EC-Council

C|CSE™

Certified Cloud Security Engineer

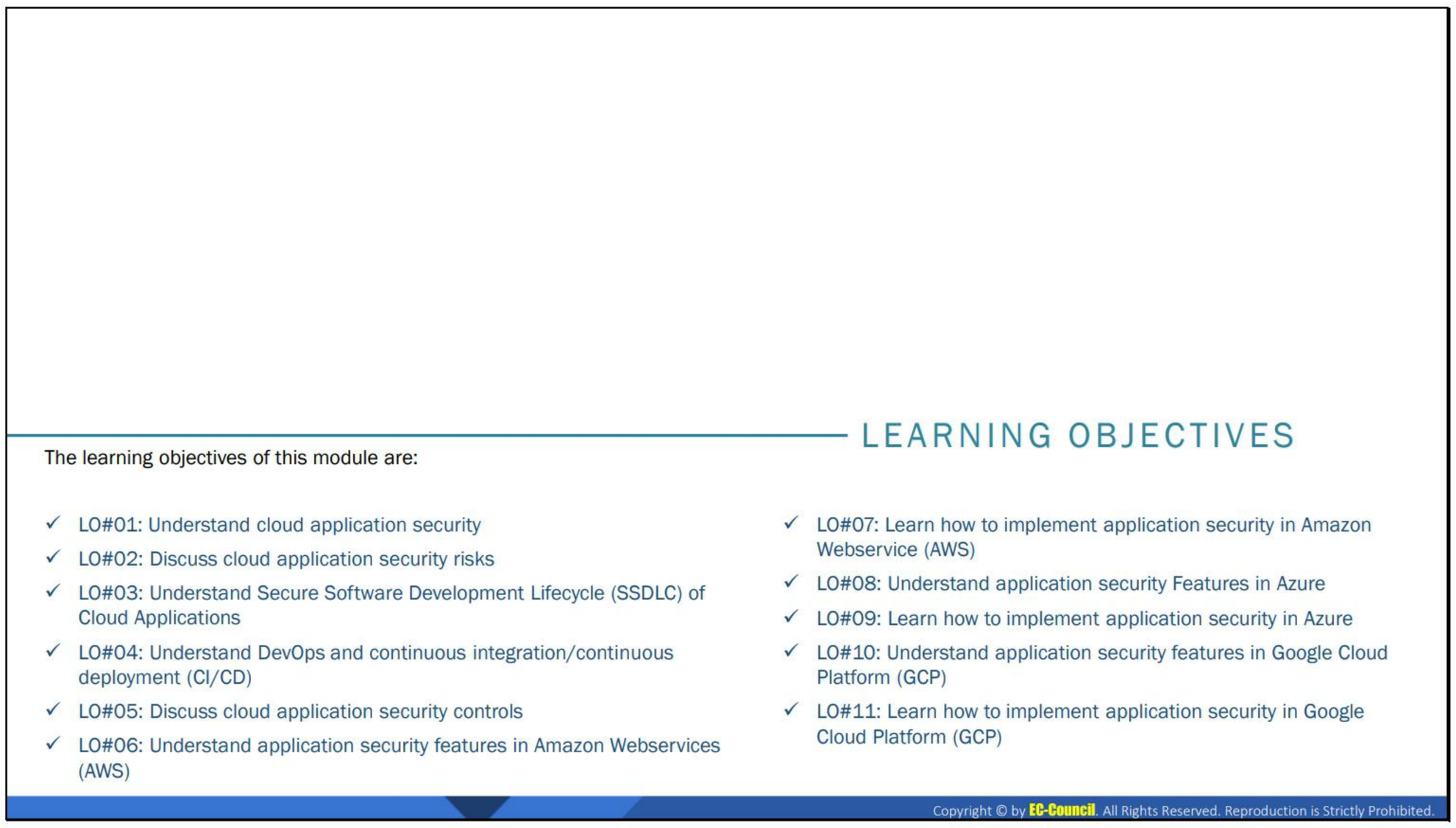


Application Security in Cloud

Module 03

This page is intentionally left blank.

hide01.ir



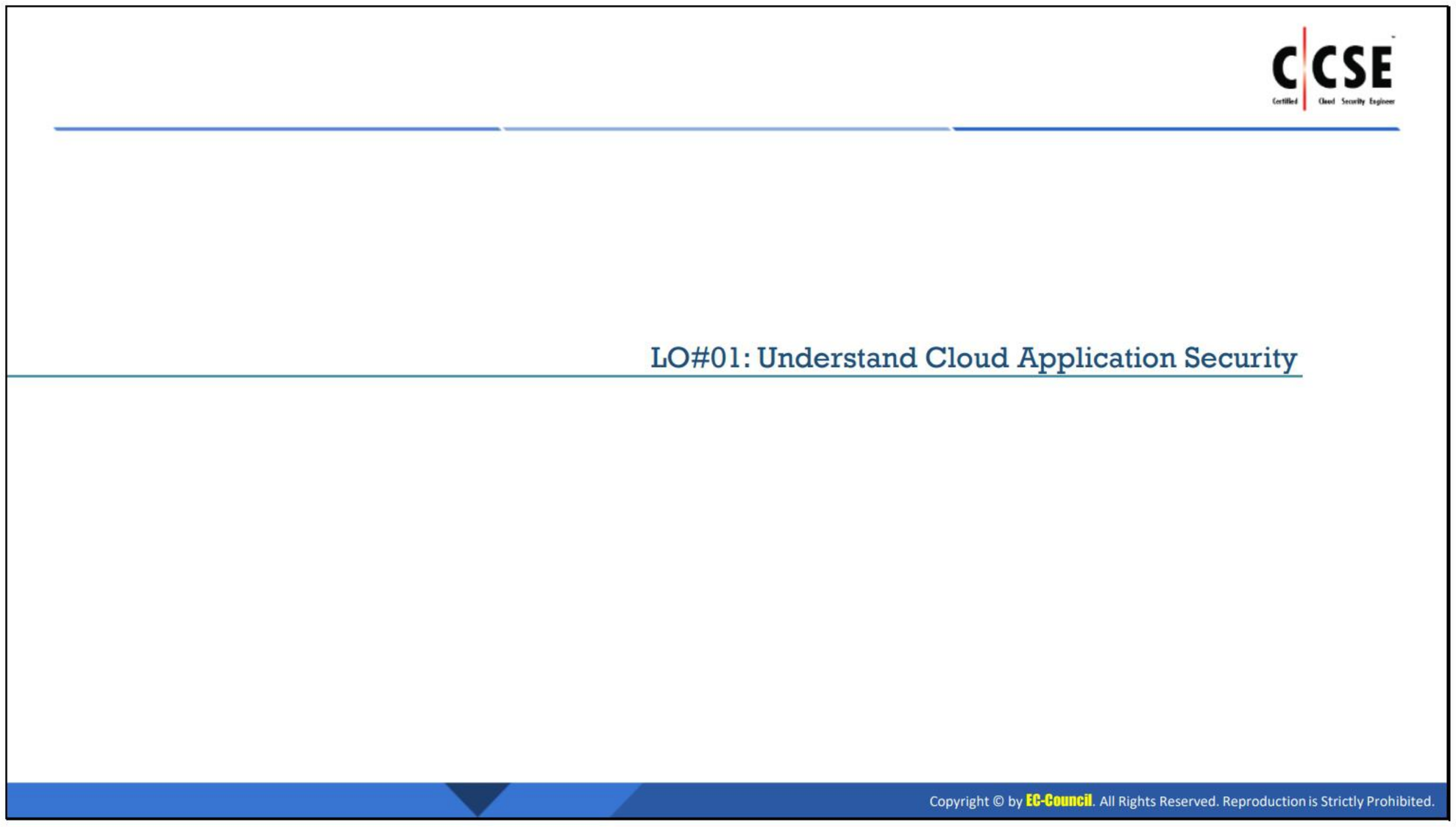
Learning Objectives

Cloud security engineers should have sufficient knowledge of cloud application design and architecture. They should understand the importance of testing and validating various cloud applications. Knowledge of secure system development life cycle and the access management features used will enable cloud security engineers to ensure that which are consumed. This module covers various aspects such as secure software development life cycle, and it shows implementation of DevOps and integration of security to the CI/CD pipeline for secure deployment of applications. Cloud application architecture and various cloud application security controls are also discussed. It also highlights the various application security features provided by AWS, Azure, and GCP.

The objectives of the module include:

- Understand cloud application models and cloud application security
- Understand the various phases of SSDLC for designing secure cloud applications
- Usage of IAM for managing user roles and permissions to cloud applications
- Secure design of cloud applications
- Implementation of security devices for enhancing cloud application security
- Various application security features in AWS, Azure, and GCP along with their implementation

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

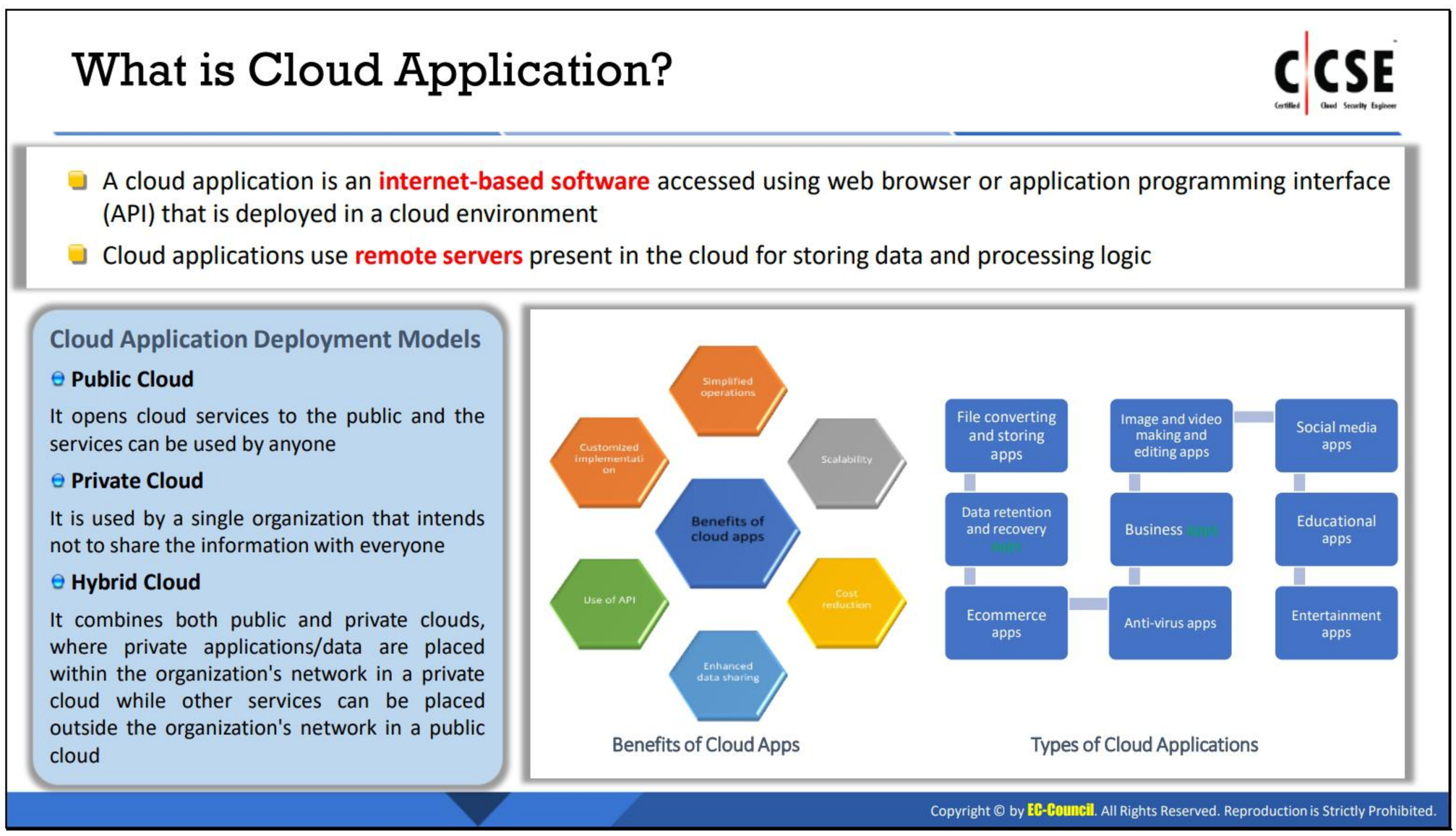


LO#01: Understand Cloud Application Security

The objective of this section is to understand cloud application security. This section describes the basic models of cloud applications, security benefits, and security challenges of cloud applications. It also describes the cloud application security responsibilities for various cloud service models.

hid01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Cloud Application?

A cloud application is a software application deployed and developed in a cloud environment that can be accessed through the internet. Users interact with the application online through the browser or with the help of a mobile application. The data is processed or handled by the local device as well as cloud computing solutions. From a user perspective, the applications that are deployed in the cloud behave like a standard website. However, the data that is processed and computing are controlled by the cloud via application program interface (APIs) or a hybrid of both.

Examples of cloud applications include Google Docs, Microsoft 365, etc. They can be accessed with any machine that can run a web browser with an internet connection. The interface and all the necessary functionalities, including data storage, are provided from a remote server. With the help of cloud application servers, users can host hundreds of different cloud applications for their business.

Advantages of Cloud Applications

- **Reliability:** Cloud service providers can guarantee a high level of service and availability for users' applications with good infrastructure, including easily available backup servers in the event of a disaster. Service providers are responsible for any system crash and they must fix it.
- **Instantly scalable**: Cloud applications can scale instantaneously without an increase in costs; moreover, the scaling is dynamic. Dynamic scaling can further reduce costs as users use resources only when they need to.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Cost efficiency:** Cloud application deployment can be completed in a short period without any initial investment in IT infrastructure. Companies bear the cost of purchasing servers and other equipment and save on administrative, electrical, air conditioning, and other maintenance costs. Cloud services offer flexible cost models where organizations can pay only for the storage and capacity they use.
- **Ease-of-management:** To streamline the management of cloud applications, organizations have implemented cloud management platform (CMPs). CMPs use a comprehensive list of APIs to extract data from entire cloud environments and feed it into a comprehensive system where users can monitor the performance, security, and compliance of an organization.
- **Improved security and data sharing**: Data stored in the cloud is always available and can be accessed by authorized users. Due to their large scale, cloud providers can hire world-class security professionals and implement infrastructure security measures, which are usually only achieved by large companies. Centralized data maintained by IT operations personnel is backed up more efficiently in normal times and can be easily restored in case of a disaster.
- **Use of APIs:** Cloud applications allow access to third-party data resources and storage services via APIs. APIs can be used to handover data to applications or API-based backend services for computation, the results of which are returned to the cloud applications. Vetted APIs impose passive consistency, which accelerates development and produces predictable results.
- **Faster response to organization needs**: It is easier to update, run, and test cloud applications, allowing more time for marketing and agility, which leads to a cultural change in business operations.

Disadvantages of Cloud Applications

- **Security:** As increasing number of companies are moving to the cloud, it is difficult to constantly monitor the security status of the IT infrastructure and ensure safety of cloud applications. Certain cloud management platforms, such as AWS, Azure Cloud, and GCP, allow IT companies to collect data from applications within the cloud and use it to monitor for security threats and risks in a secure manner.
- **Downtime**: When the organization is using the cloud as a service, an internet connection is required to access the data. Thus, a random web outage may cause a big business interruption by disrupting access to cloud applications. Additionally, cloud service providers may experience technical outages from time to time, during which time all the organization's data may not be available.
- **Control**: Control is one of the major trade-offs that companies make to save on the cost of cloud application deployment. Cloud infrastructure is owned, operated, and maintained by the CSP; the company has no real control over the backend infrastructure, which makes cloud application deployment ideal for companies that only want to manage applications, data, and services, but not the physical aspect of their IT.

Cloud Application Deployment Models

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

There are various cloud models for application deployment that may be suitable to the requirements of an organization. These cloud deployment models are categorized into three types.

- **Public Cloud**

  This type of model opens cloud services to the public and anyone can use their services. Virtualization is a method used to build cloud services that are accessible to the public.

  Advantages:

  - Cost efficiency: No need to buy software or hardware, and organizations pay for the service they use.
  - Scalability: Dynamic scalability allows organizations to use unlimited resources.
  - Reliability: It is secure against massive network failure of servers.
  - No maintenance: Service providers take care of maintenance.

- **Private Cloud**

  This type of model is used by a single organization that intends not to share the information with everyone. A private cloud resides within the organization and stays behind a firewall so that only limited organization employees can access the data.

  Advantages:

  - Highly secure: All private cloud resources are not accessible by every user with a high level of control and security.
  - Flexibility: Organizations can adapt according to the cloud environment to meet specific business needs.
  - Scalability: Private clouds are scalable and efficient.

- **Hybrid Cloud**

  This type of model can combine both public and private clouds. In this model, private applications and data are placed within the organization's network in a private cloud, while other services are placed outside the organization's network in a public cloud. Developers can access private and public cloud services in their daily activities.

  Advantages:

  - Control: Organizations can manage private infrastructure for sensitive data and assets.
  - Cost-efficient: Organizations pay for extra computation power only when they need it.
  - Flexibility: Organizations can use additional public cloud resources when they need them.
  - Ease-of-management**:** Transition to the cloud will not be complex because they may gradually migrate the workload over time.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

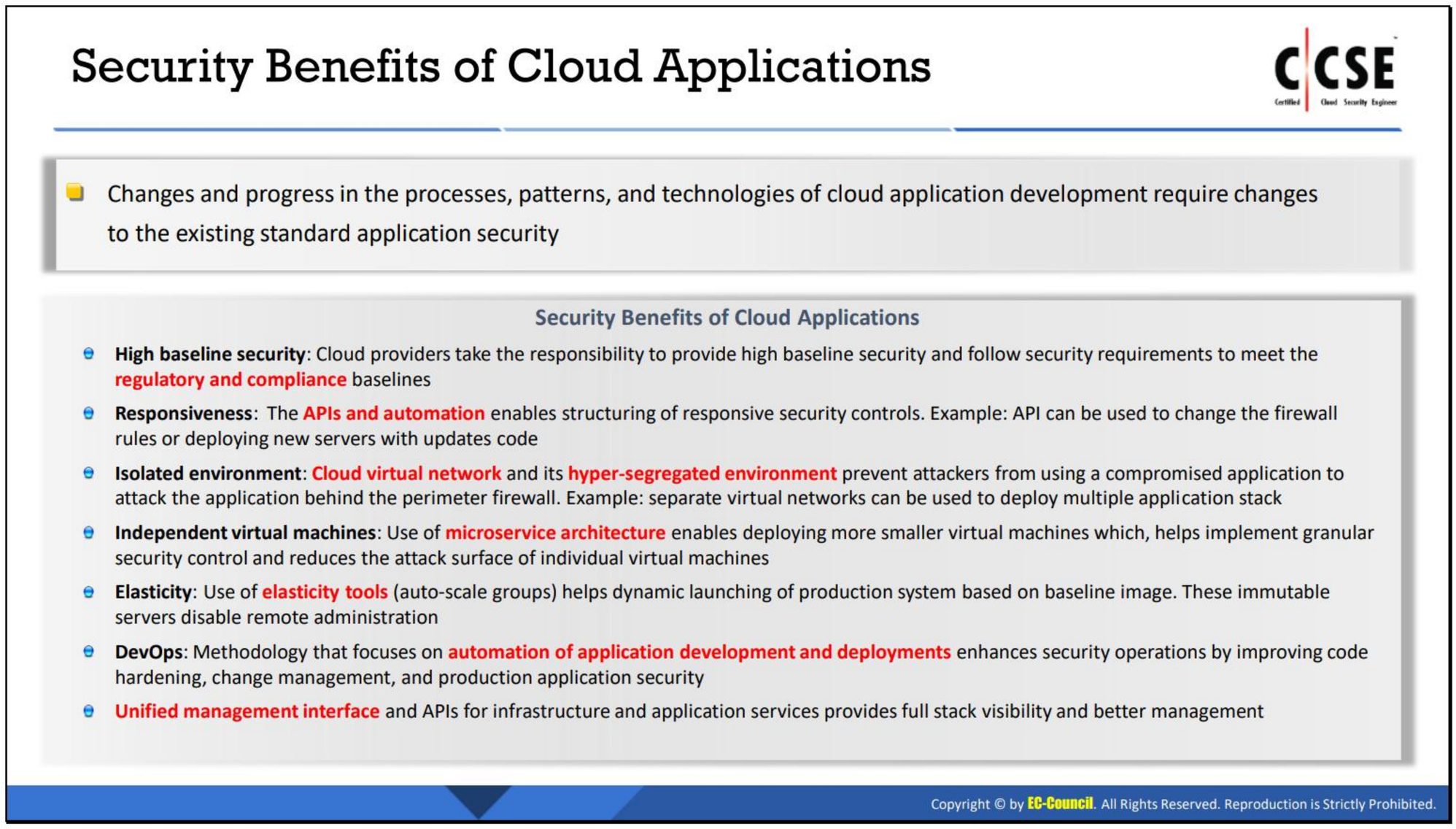
Types of Cloud Applications

Cloud applications can be of various types, including the following:

- File converting and storing apps
- Image and video making and editing apps
- Social media apps
- Data retention and recovery apps
- Business apps
- Educational apps
- E-commerce apps
- Antivirus apps
- Entertainment apps

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Security Benefits of Cloud Applications

Changes and progress in the processes, patterns, and technologies of cloud application development require changes to the existing application security standards. The following are some of the security benefits of cloud applications.

hiteo.ir

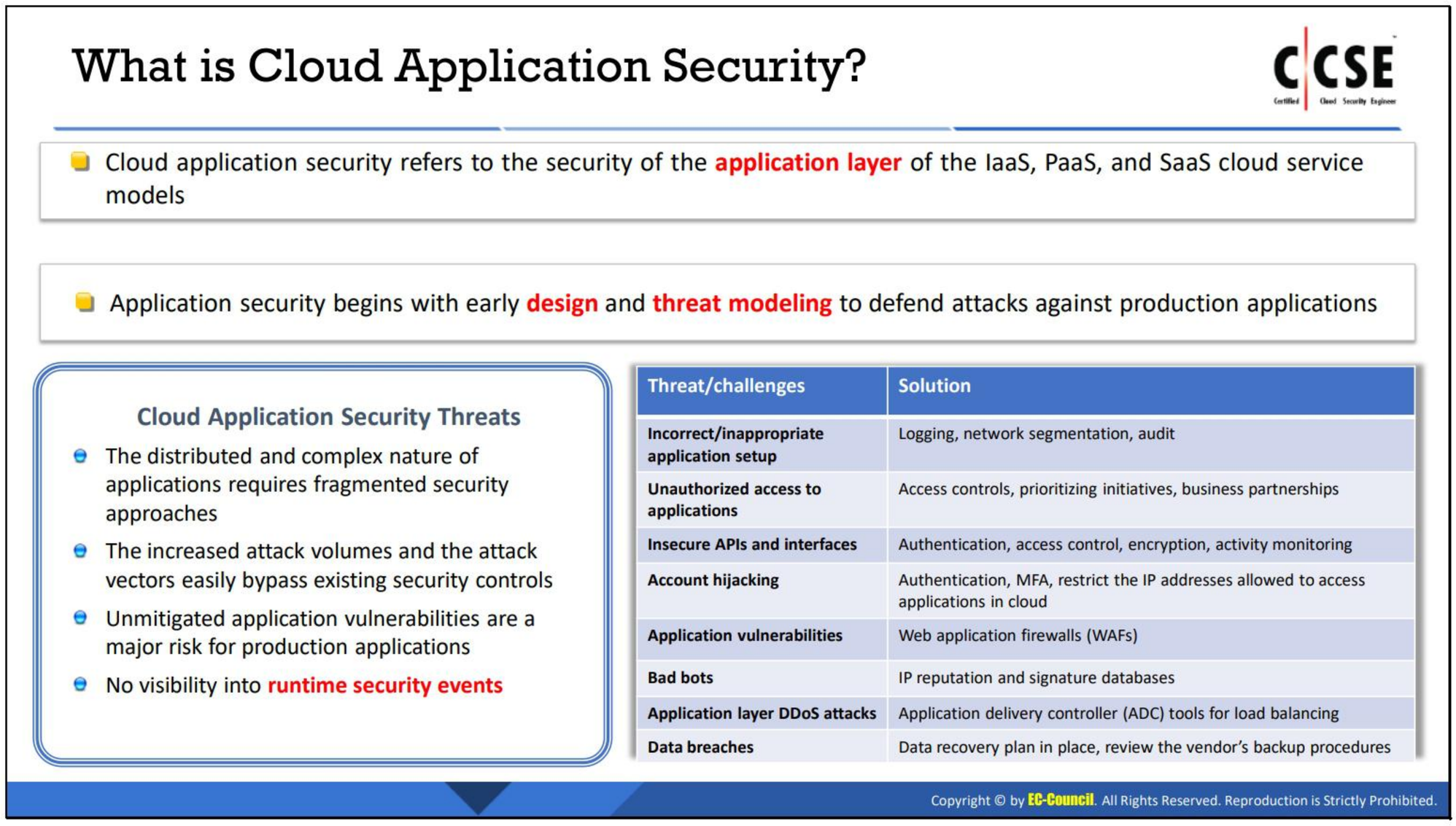
- **High baseline security**: Cloud providers take the responsibility to provide high baseline security and follow security requirements to meet the regulatory and compliance baselines.
- **Responsiveness**: The APIs and automation enable structuring of responsive security controls. Example API can be used to change the firewall rules or deploying new servers with updates code.
- **Isolated environment**: Cloud virtual network and its hyper-segregated environment prevent attackers to use a compromised application to attack application behind perimeter firewall. Example separate virtual networks can be used to deploy multiple application stack.
- **Independent virtual machines**: Use of microservice architecture enables deploying more smaller virtual machines, which helps implement granular security control and reducing the attack surface of individual virtual machines.
- **Elasticity**: Use of elasticity tools (autoscale groups) helps dynamic launching of production system based on baseline image. These immutable servers disable remote administration.
- **DevOps**: Methodology that focuses on automation of application development and deployments enhances security operations by improving code hardening, change management, and production application security.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Unified management interface and APIs** for infrastructure and application services gives full stack visibility and better management.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Cloud Application Security?

Application security involves security measures at the application level. These security measures can prevent data or code within the app from being stolen by attackers. Additionally, it covers the security considerations for application development and design and involves systems and approaches to secure applications after their deployment. It is a set of defined processes, policies, techniques, and controls used for ensuring secure data transmission within the cloud environment.

Application security in the cloud refers to the security of the application layer in the IaaS, PaaS, and SaaS cloud service models. This is the fundamental control layer of cloud security. Adding cloud application security to a zero-trust security infrastructure can be a security advantage if organization employees access applications frequently. The application security in cloud computing comprises appropriately programmed cloud applications to prevent vulnerabilities such as cross-site scripting (XSS), poor authentication and session management, SQL injection, cross-site request forgery (CSRF), etc. Cloud applications are distributed and complex; moreover, their security approaches are also fragmented. Common attack vectors are becoming sophisticated enough to bypass current security controls. Moreover, unmitigated vulnerabilities put critical production apps at risk. In a cloud environment, there is no visibility into runtime security events.

Why is Cloud Application Security Needed?

Listed below are the reasons why cloud application security is needed.

- It enables organizations to know what apps are in use by their employees and what type of access to the application is granted because traditional security solutions cannot detect threats associated with the employees' access to cloud applications.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- It is as prevalent as the antivirus within the workforce because an organization's data is distributed across a cloud vendor that hosts hundreds of different applications.
- It is a part of security compliance because cloud application threats are a focused security control effort.

Cloud Application Security Threats

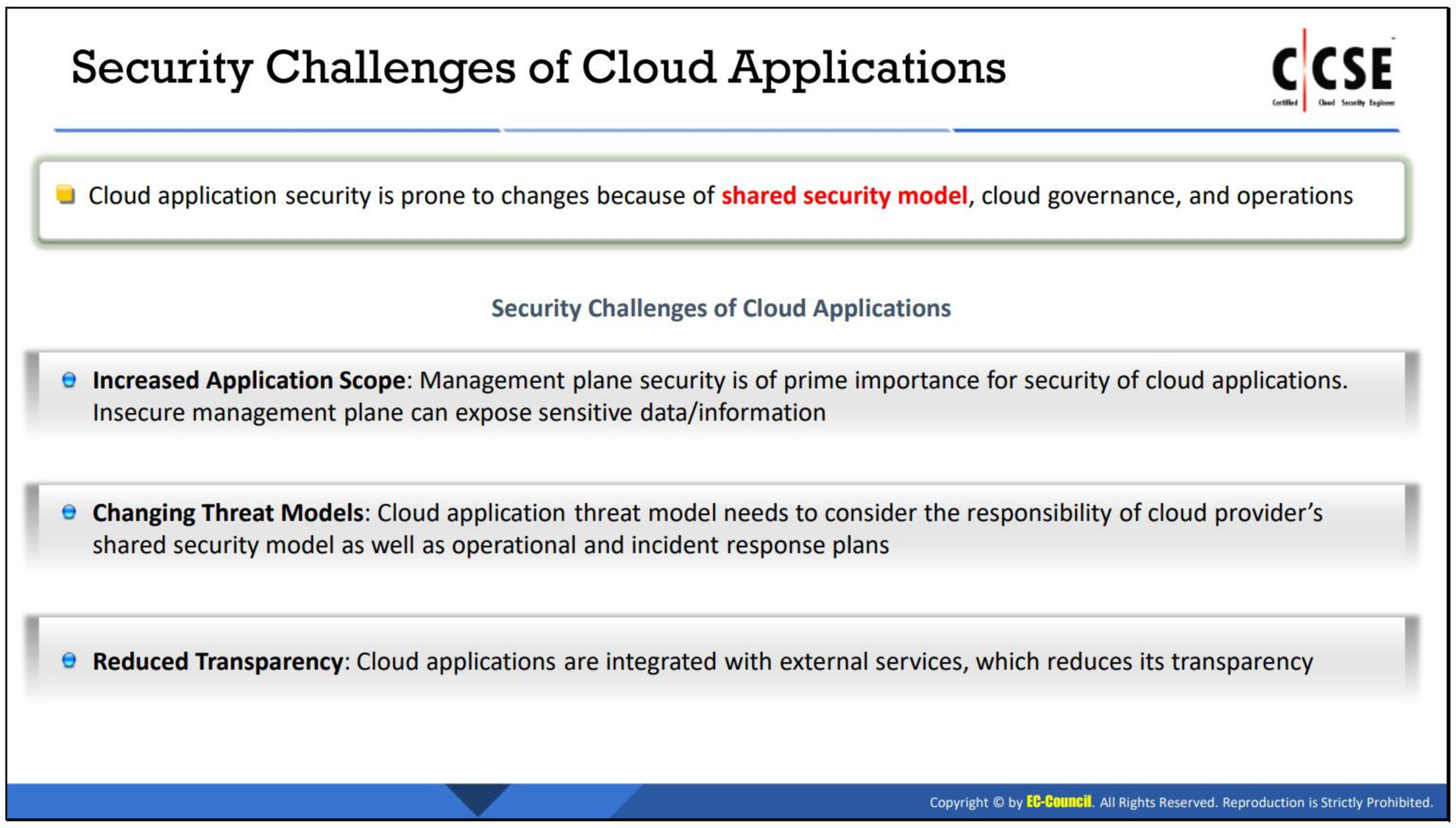
The following table summarizes the cloud application security threats along with their solutions.

Threats/Challenges	Solutions
Incorrect/inappropriate application setup	Use logging, network segmentation, and audits
Unauthorized access to applications	Use access controls, prioritizing initiatives, and business partnerships
Insecure APIs and interfaces	Implement authentication, access control, encryption, and activity monitoring
Account hijacking	Implement authentication, multi-factor authentication (MFA), and restrict IP addresses allowed to access applications in the cloud
Application vulnerabilities	Implement web application firewalls (WAFs)
Bad bots	Use IP reputation and signature databases
Application-layer DDoS attacks	Leverage application delivery controller (ADC) tools for load balancing
Data breaches	Keep data recovery plan in place and review the vendor's back up procedures

Table 3.1: Cloud Application Security Threats

hideo1.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Security Challenges of Cloud Applications

Cloud application security offers numerous changes due to its shared security model, governance, and operations. These changes may cause the following security challenges for cloud applications during platform sharing.

hide01.ir

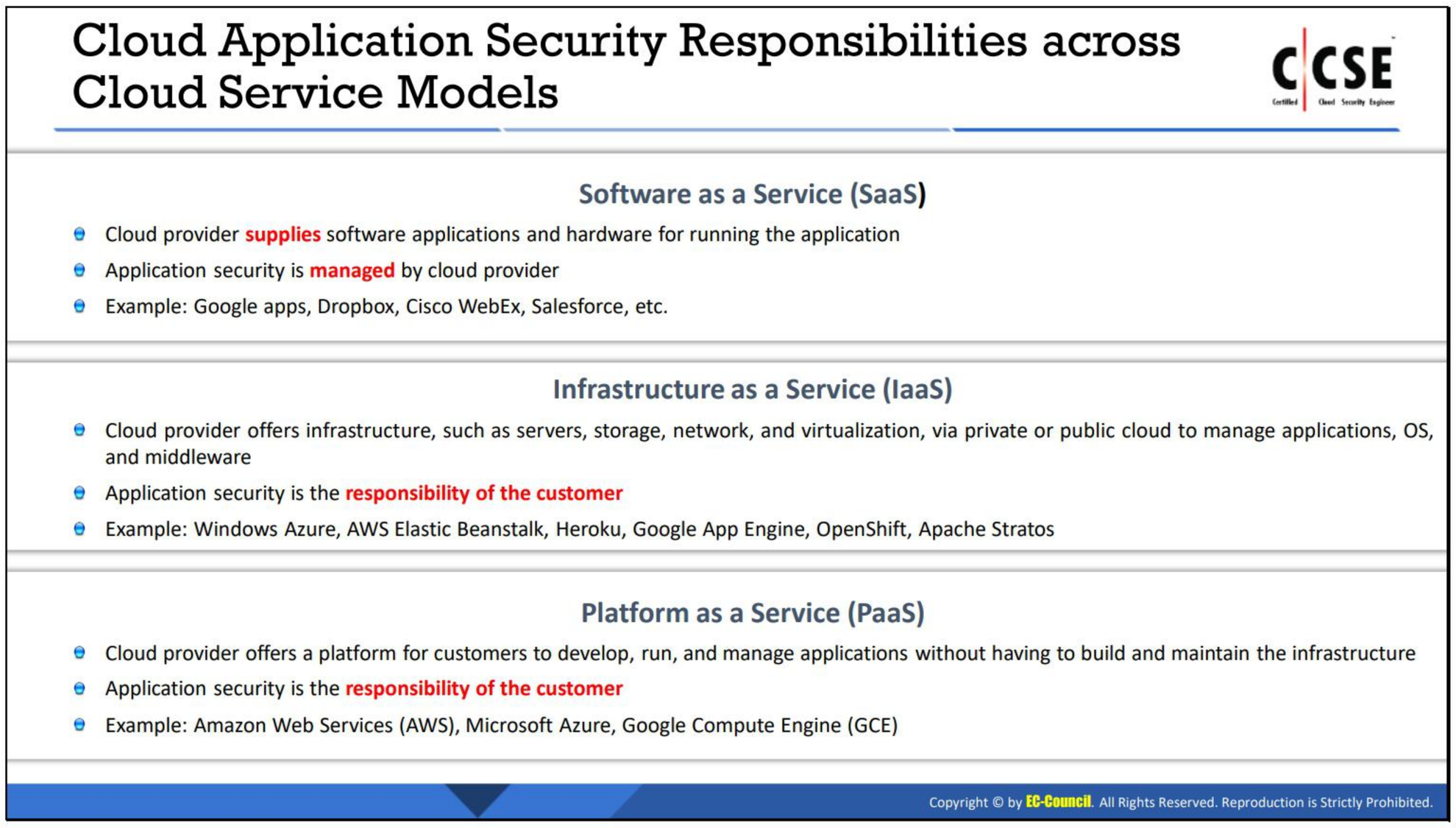
- **Limited detailed visibility**: Changes in cloud applications impact the monitoring and logging of visibility and availability, leading to new approaches for security-related data that limit PaaS accessibility (commonly available logs such as system or network logs) for cloud users.
- **Increased application scope**: The management plane or metastructure security affects the application security for cloud accounts. Developers and operations also require access to the management plane instead of using different team account to access the cloud application. Multiple access can cause exposure of sensitive data and information within the management plane. Modern cloud applications where PaaS is involved need to connect with the management plane for triggering various automated actions. This issue implies that management plane security is a part of the application's security, due to which failure in any part can cause security breaches for others as they are mutually connected.
- **Changing threat models**: Threat models should consider cloud provider relationships and the shared security model for operational and incident response plans. It should reflect the technical differences of the cloud provider or platform in use.
- **Reduced transparency**: Transparency about ongoing processes in an application is reduced because of its integration with external services. For example, the cloud user

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

does not know the entire set of security controls for an external PaaS service integrated with the application.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Application Security Responsibilities across Cloud Service Models

Cloud application services are divided into one of the three below-given categories:

hadeel_ir

- **Software as a Service (SaaS):** SaaS provides organizations with not only the hardware to run an application but also the software application. The cloud provider supplies software applications and hardware for running the application. SaaS also provides support for applications and systems. In SaaS, application security is managed by the cloud provider. A good example of this is Google Workspace, which provides all Google services. SaaS reduces the cost of additional equipment and licenses for software.

  Examples: Google Apps, Dropbox, Cisco WebEx, Salesforce, etc.

- **Infrastructure-as-a-Service (IaaS):** IaaS provides infrastructure and infrastructure support within the cloud. The cloud provider offers infrastructure such as the actual servers, storage, network, and virtualization via the private or public cloud to manage applications, OS, and middleware. Middleware is the software that exists between OS and application and provides extended features for OS functions to simplify programming. In IaaS, application security is the responsibility of the customer. For example, Google Compute Engine, a by-product of the Google Cloud Platform, provides developers access to the same infrastructure that Google uses to maintain spikes in its products.

  Other examples: Windows Azure, AWS Elastic Beanstalk, Heroku, Google App Engine, OpenShift, Apache Stratos

- **Platform as a Service (PaaS):** Both PaaS and IaaS are similar services that provide the same resources; however, PaaS also provides OS, middleware, and other software. PaaS suppliers provide full support for software and hardware that they provide by updating the software daily. It also provides developer application and application support. In PaaS,

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the customer is not required to build or maintain the IT infrastructure, and is provided a platform to develop, run, and manage the customer's applications. Application security is the responsibility of the customer in this model. Example: Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine (GCE)

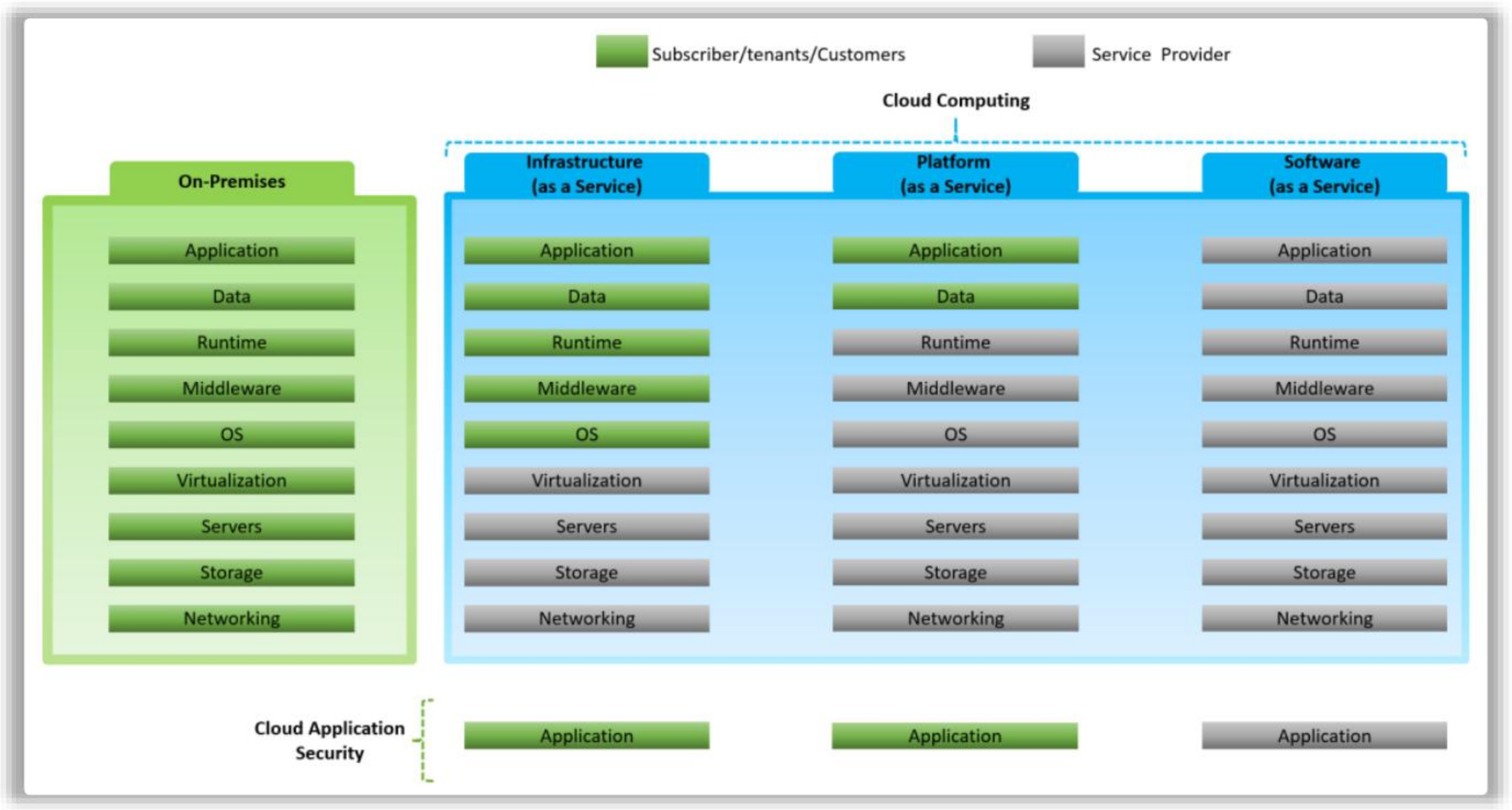
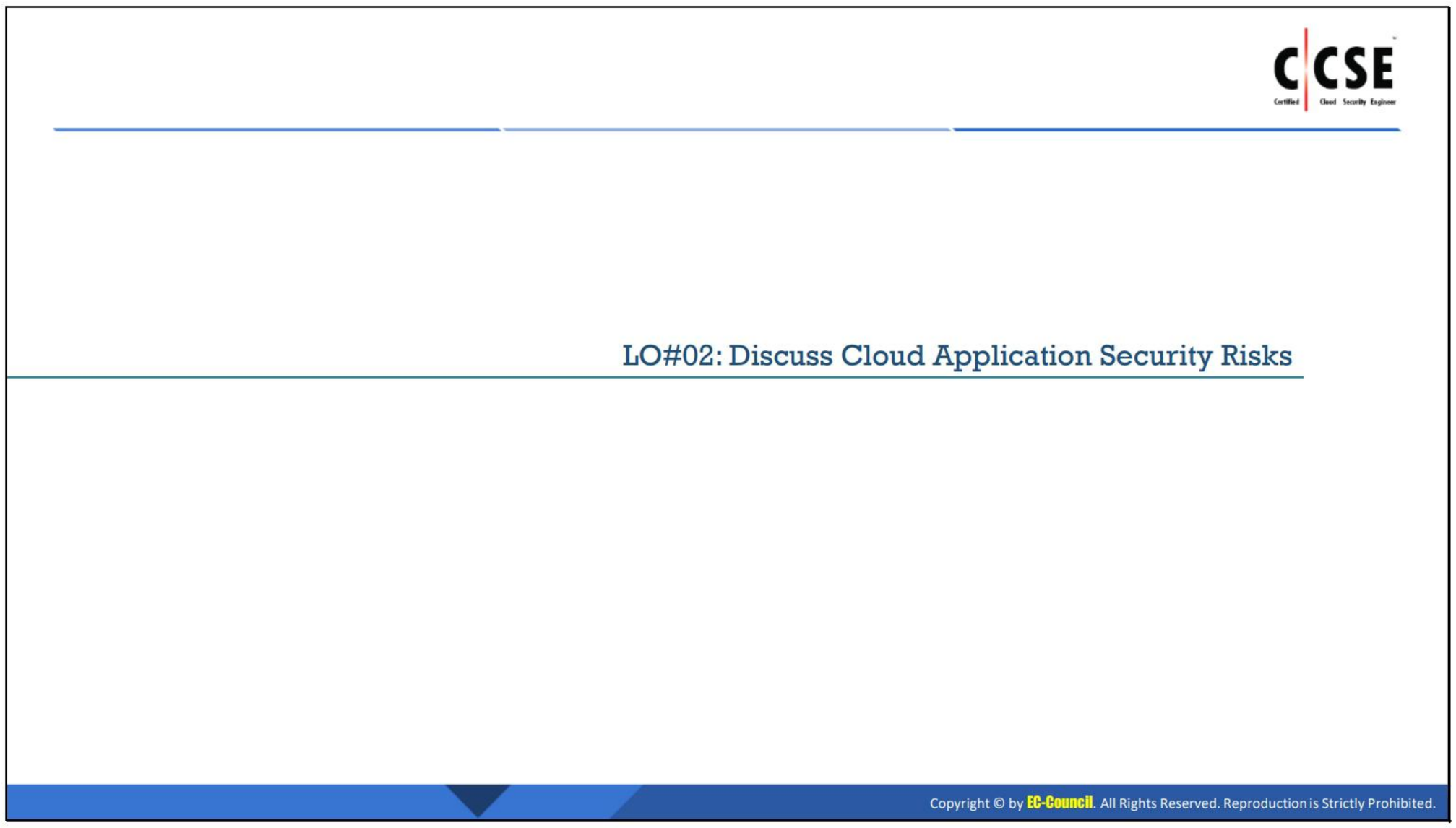


Figure 3.1: Cloud Application Security across Different Cloud Service Models

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#02: Cloud Application Security Risks

Understanding cloud vulnerabilities and risks is required to analyze and assess the risks associated with migrating to the cloud. This section describes the common cloud application vulnerabilities and risks and discusses the cloud-specific risks that need to be focused on. It also explains the scope of cloud application security.

h1de0_ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Common Cloud Application Vulnerabilities and Risks – OWASP Top 10

Vulnerability and Risks	Description
Injection	When untrusted data is sent to an interpreter as part of a command or query, it results in injection flaws, such as SQL, NoSQL, OS, and LDAP injection. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
Broken Authentication	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
Sensitive Data Exposure	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
XML External Entities (XEE)	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
Broken Access Control	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
Security Misconfiguration	Security misconfiguration is the most seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.
Cross-Site Scripting (XSS)	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
Insecure Deserialization	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
Using components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
Insufficient Logging and Monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Source: *https://owasp.org*

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

Common Cloud Application Vulnerabilities and Risks – OWASP Top 10

hide01.ir

Vulnerability and risks	Description
Injection	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
Broken authentication	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
Sensitive data exposure	Many web applications and APIs do not properly protect sensitive data such as financial, healthcare, and personally identifiable information (PII). Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
XML external entities (XEE)	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial-of-service attacks.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Broken access control	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
Security misconfiguration	Security misconfiguration is the most commonly observed issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.
Cross-site scripting (XSS)	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser, which can hijack user sessions, deface websites, or redirect the user to malicious sites.
Insecure deserialization	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
Using components with known vulnerabilities	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
Insufficient logging and monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems; maintain persistence; pivot to more systems; and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

TABLE 3.2: OWASP Top 10

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Focus on Cloud-Specific Risks

Threat	Description
Data Breaches	Data breach incidents occur when confidential information is stolen or accessed by unauthorized person
Weak Identity, Credential and Access Management	Lack of proper identity access management, failing to implement multi-factor authentication, using weak passwords, lack of automation of rotating cryptographic keys, data breaches can enable such attacks
Insecure Interfaces and APIs	Providers can expose the customer's software user interfaces (UI)/Application Programming Interfaces (API) that are intended for interacting with cloud services
System and Application Vulnerabilities	System vulnerabilities can be exploited to infiltrate systems to steal data or taking control over the system or disrupting services
Account Hijacking	If the attackers get credentials, they can eavesdrop activities, corrupt data, return false information to let the clients to redirect to malicious sites
Malicious Insiders	A malicious individual (former employee, business partners, current employee, etc.) who have access to the organization's data/system/network can misuse their authorized access to spoil the organization's integrity or data confidentiality
Advanced Persistent Threats (APTs)	This parasitical form of attack enter systems to set their foothold in the organization's system infrastructure and steal data
Data Loss	Accidental deletion of data by provider or physical catastrophe can cause loss of data unless the cloud service provider and customer backup their data
Insufficient Due Diligence	Rushing to adopt cloud technologies and selecting a provider without proper due diligence can expose the customer to technical, legal, compliance and commercial risks
Abuse and Nefarious Use of Cloud Services	Poor security of service deployments, malicious account sign-ups, free trials of cloud services, etc can expose cloud service models to attacks
Denial of Service	These are the attacks that can prevent cloud service users from accessing their data/apps on cloud
Shared Technology Issues	The underlying infrastructure components like the CPU, caches, etc. may not be designed to provide secure service delivery models (IaaS, PaaS, ad SaaS) resulting in shared technology vulnerabilities

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

Focus on Cloud-Specific Risks

Threat	Description
Data breaches	A data breach is an incident in which sensitive, protected, or confidential information is released, viewed, stolen, or used by an individual who is not authorized to do so.
Weak identity, credential, and access management	Data breaches and other similar attacks can occur because of a lack of scalable identity access management systems, failure to use multi-factor authentication, weak password use, and a lack of ongoing automated rotation of cryptographic keys, passwords, and certificates.
Insecure interfaces and APIs	Cloud computing providers expose a set of software user interfaces (UIs) or application programming interfaces (APIs) that customers use to manage and interact with cloud services.
System and application vulnerabilities	System vulnerabilities are exploitable bugs in programs that attackers can use to infiltrate a computer system for the purpose of stealing data, taking control of the system, or disrupting service operations.
Account hijacking	If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites.
Malicious insiders	A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused

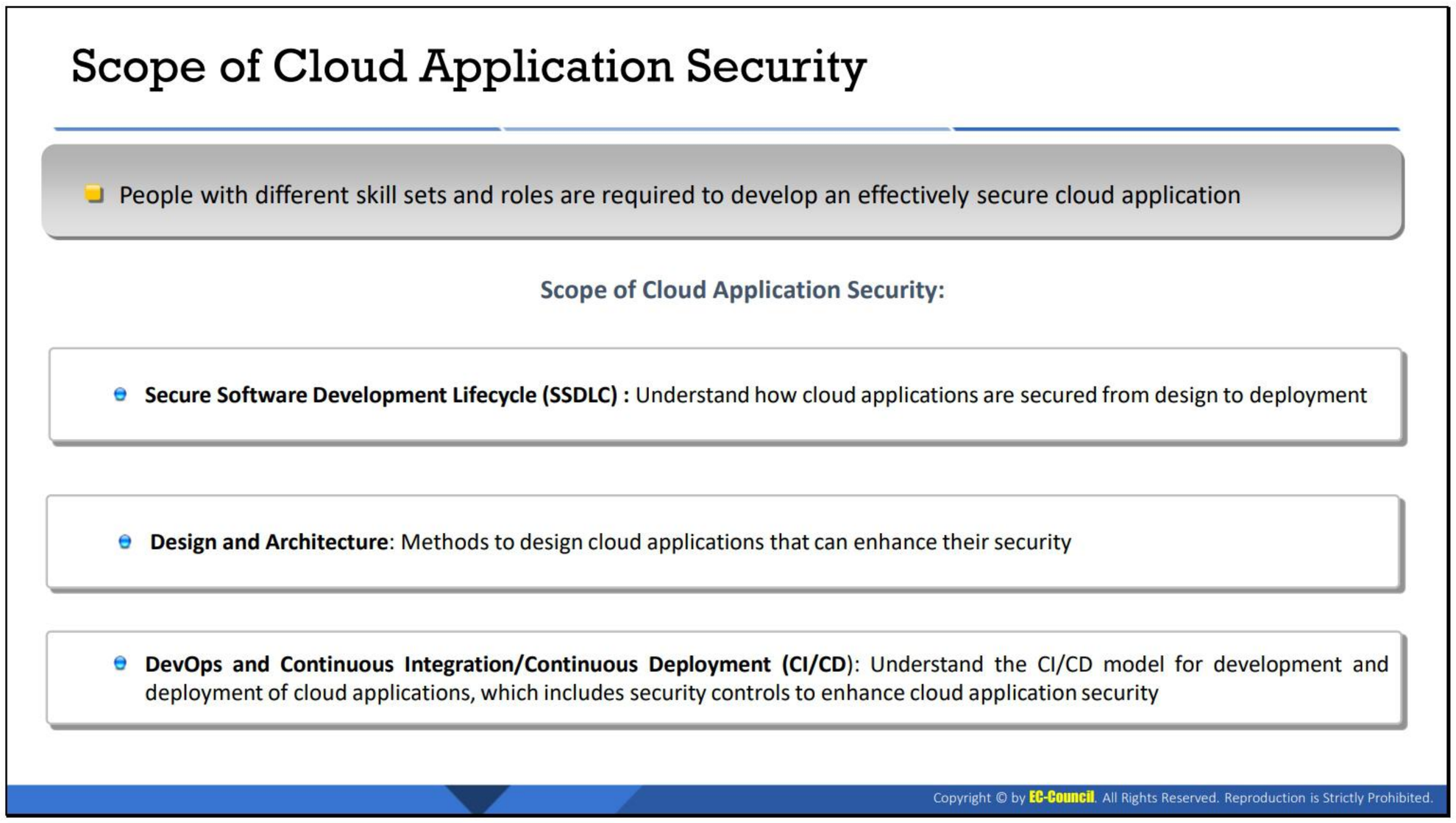
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

	that access in a manner that negatively affects the confidentiality, integrity, or availability of the organization's information or information systems.
Advanced persistent threats (APTs)	APTs are a parasitical form of cyberattack that infiltrates systems to establish a foothold in the computing infrastructure of target companies from which they smuggle data and intellectual property.
Data loss	An accidental deletion by the cloud service provider or, worse, a physical catastrophe such as a fire or earthquake, can lead to permanent loss of customer data unless the provider or cloud consumer takes adequate measures to back up data.
Insufficient due diligence	An organization that rushes to adopt cloud technologies and choose CSPs without performing due diligence exposes itself to a myriad of commercial, financial, technical, legal, and compliance risks that jeopardize its success.
Abuse and nefarious use of cloud services	Poorly secured cloud service deployments, free cloud service trials, and fraudulent account sign-ups via payment instrument fraud expose cloud computing models such as IaaS, PaaS, and SaaS to malicious attacks.
Denial of service	Denial-of-service (DoS) attacks are meant to prevent users of a service from being able to access their data or their applications.
Shared technology issues	Underlying components (e.g., CPU caches, GPUs, etc.) that comprise the infrastructure supporting cloud services deployment may not have been designed to offer strong isolation properties for a multitenant architecture (IaaS), redeployable platforms (PaaS), or multicustomer applications (SaaS). This can lead to vulnerabilities related to shared technology.

hidel1.ir

TABLE 3.3: Cloud Application Specific Risks

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Scope of Cloud Application Security

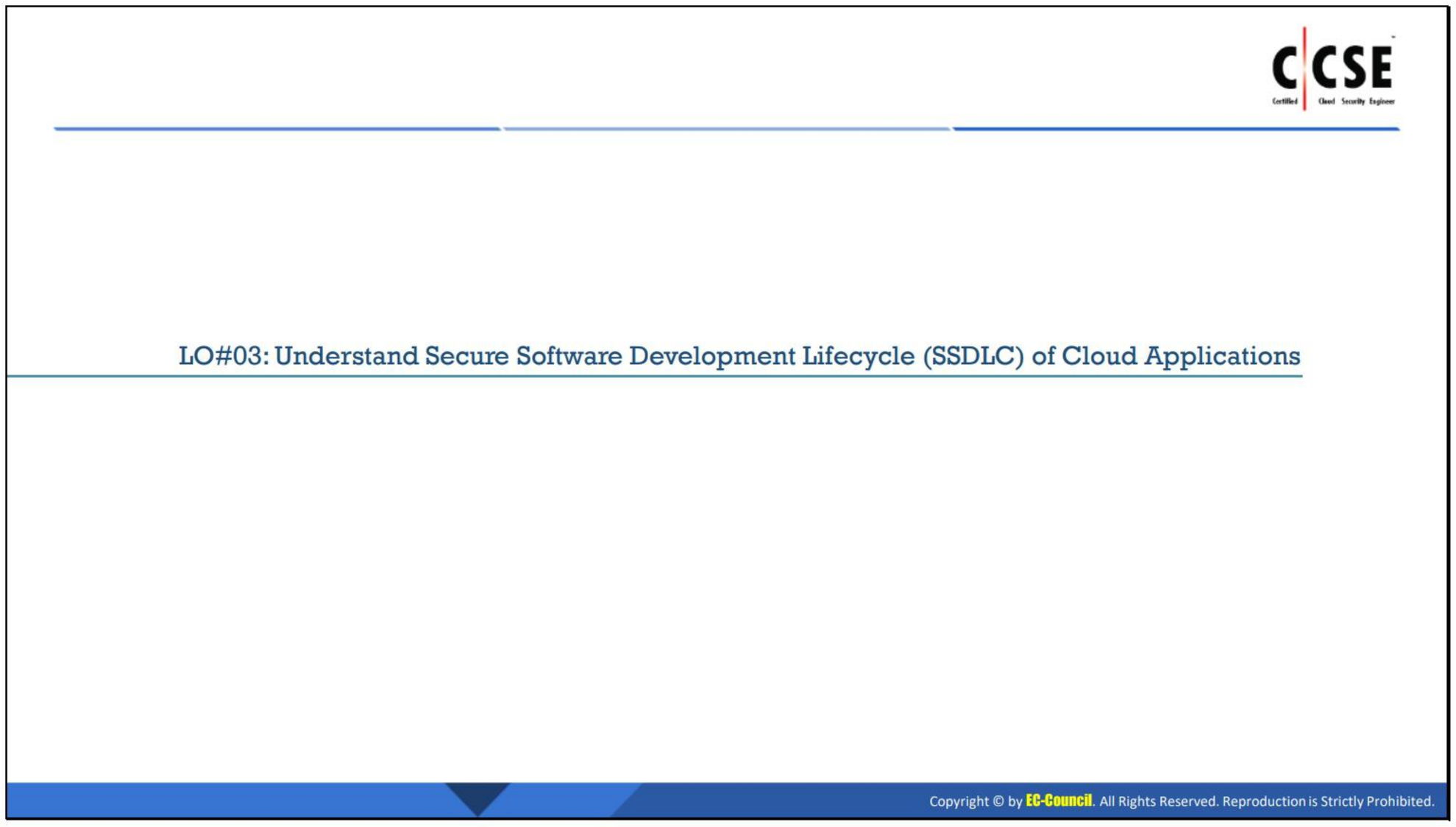
People with different skill sets and roles are required to develop an effective secure cloud application. The nature of application security is very broad; thus, various factors are to be considered to develop secure cloud applications.

hidn01.ir

The scope of cloud application security can be categorized into the following:

- **Secure software development lifecycle (SSDLC):** SSDLC is a process that ensures security assurance activities are added and implemented as an integral part of the software development process. Security assurance activities include architecture analysis, code review, and penetration testing. While developing applications in the cloud, these activities are added to the existing software development life cycle (SDLC) process to develop secure applications. Understand how cloud applications are secured from design to deployment. Additionally, understand how application security is affected by cloud computing at all stages of its development.
- **Design and architecture:** Methods to design cloud applications that can enhance their security. The design and architecture of cloud apps must ensure that they are protected from commonly known threats. Including certain methods and trends while designing cloud apps can improve their security.
- **DevOps and continuous integration/continuous deployment (CI/CD):** CI and CD are fundamental DevOps best practices that developers use while developing software applications. CI/CD are best practices that support DevOps. CI/CD encourages the use of automated tools to integrate and test apps to improve their security. Understand the CI/CD model for development and deployment of cloud applications, which includes security controls to enhance cloud application security.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

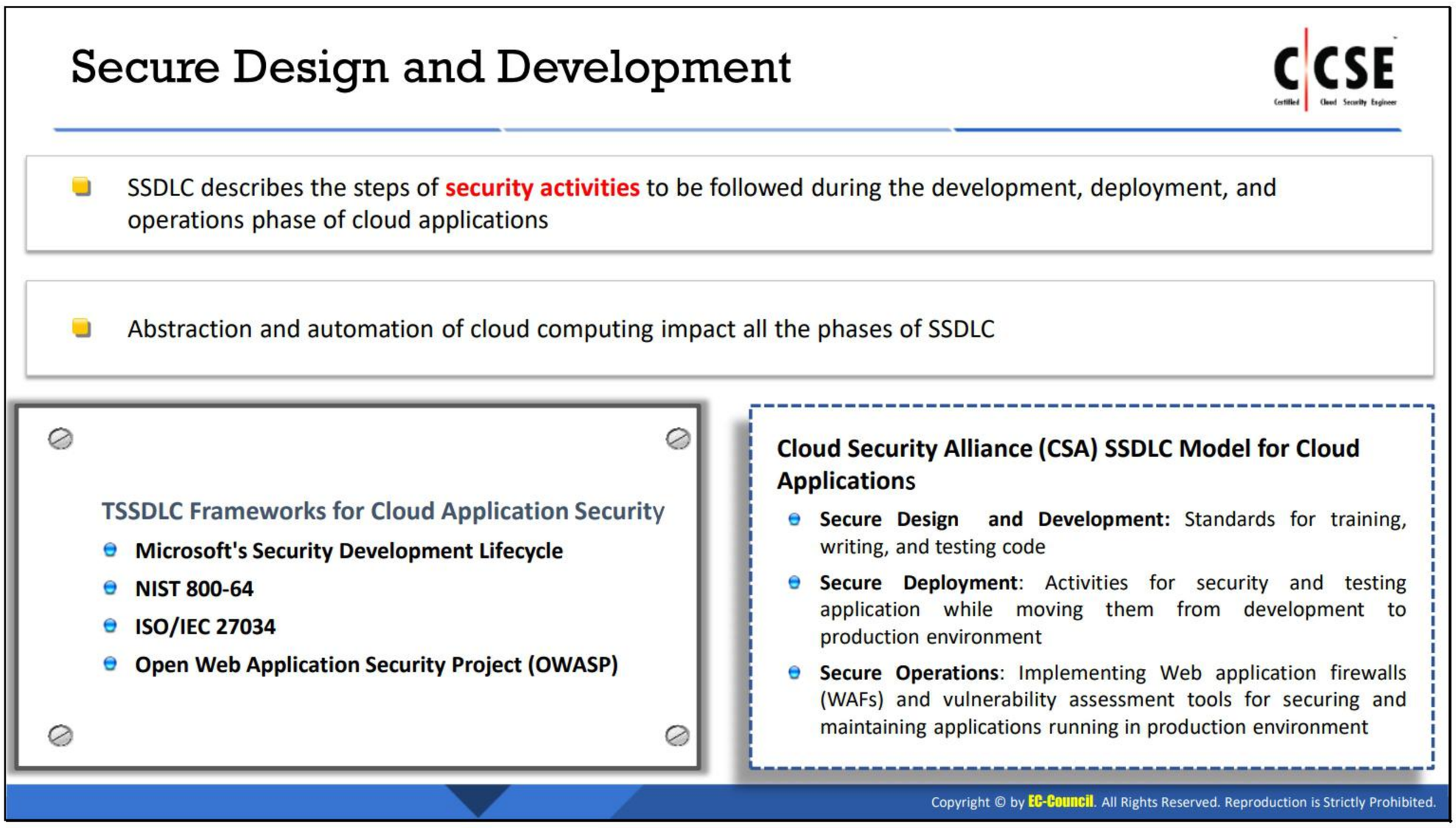


LO#03: Understand Secure Software Development Lifecycle(SSDLC) of Cloud Applications

The objective of this section to explain secure design and architecture of cloud applications. This section explains different architectures of cloud applications and factors to consider when designing a secure application in the cloud. It also explains the PaaS security features and best practices for designing secure cloud applications. Finally, this section explains SSDLC for cloud applications, that is, the **security activities** to be followed during various phases of cloud applications.

vid01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Secure Design and Development

SSDLC describes the security activities to be followed during the development, deployment, and operations phases of cloud applications. These activities help keep cloud applications secure from various cyber threats. Abstraction and automation of cloud computing impact all the phases of SSDLC, no matter which SSDLC is being used. In addition, there is a greater dependence on the CSP in public clouds due to which cloud computing affects SSDLC. It can be understood through the following points:

- With a shared responsibility model in cloud computing, cloud customers are dependent on the CSP for certain security aspects based on the selected cloud service model.
- In cloud computing, there are major changes in visibility and control that differ based on the technology and provider.
- The overall application security plan must be developed considering the CSP's capabilities such as services, features, and security.
- Now, metastructure and the management plane may come under the application security scope.

SSDLC Frameworks for Cloud Application Security

Various frameworks are used for cloud application security such as:

- Microsoft's Security Development Lifecycle
- NIST 800-64
- ISO/IEC 27034
- Open Web Application Security Project (OWASP)

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

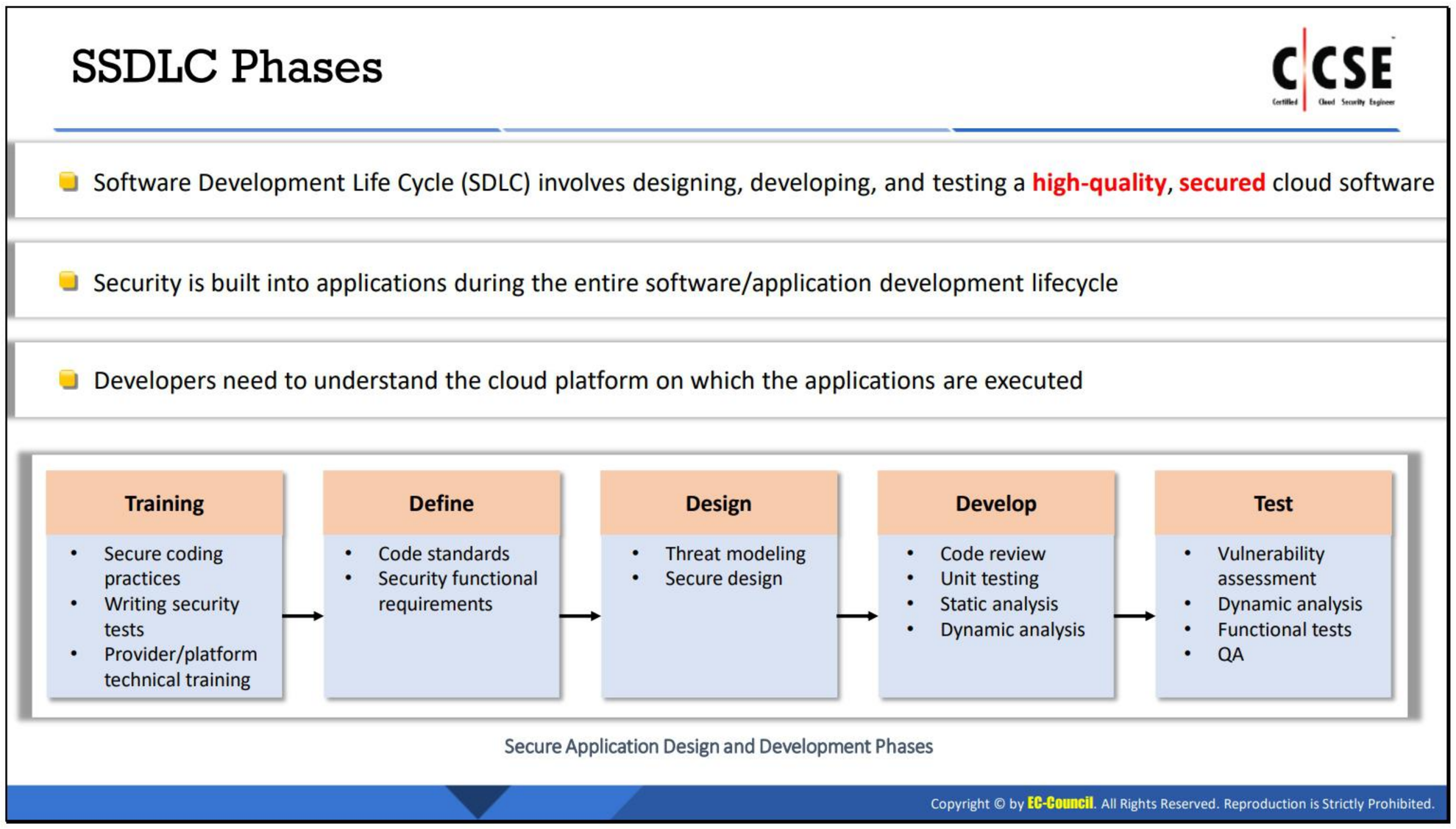
Cloud Security Alliance (CSA) SSDLC Model for Cloud Applications

Because there are various frameworks and terminology differences, the CSA describes these into meta-phases to define the standard set of activities observed across these frameworks. The CSA's SSDLC model offers a descriptive model that can be used to address major activities, no matter which lifecycle an organization uses.

- **Secure design and development**: Activities ranging from training and developing enterprise-wide standards to writing and testing code.
- **Secure deployment**: It includes security and testing activities performed while moving code from a development environment to the production environment.
- **Secure operations**: These operations include activities that secure and maintain production apps such as implementing web application firewalls (WAF) and using vulnerability assessment tools for securing and maintaining applications running in the production environment.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SSDLC Phases

SDLC involves designing, developing, and testing high-quality secured cloud software. Secure application design and development, or SSDLC, consists of five key phases that are affected by cloud computing.

hide01.ir

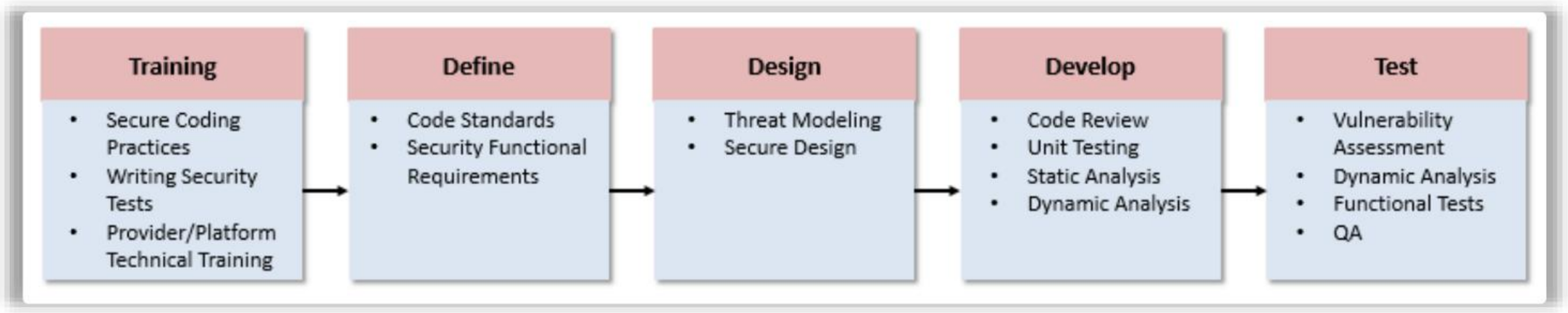


Figure 3.2: Secure App Design and Development Phases

These five SSDLC phases are explained below:

- **Training**: The staff of development, security, and operations departments in an organization must get additional training on cloud security fundamentals and technical security training on the particular cloud platform used for the organization's projects. As the development and operations teams are directly involved in architecting and managing the cloud infrastructure, they must be provided with baseline security training on the tools that will be used by them.
- **Define**: The approved security standards, architectures, and other requirements for the provider is determined by the cloud consumer or user. The cloud user determines them based on their compliance requirements and listing. For example, they determine what kind of data can be stored on which cloud services. Deployment processes are to be defined at this phase; however, they can be finalized later in some cases. Additionally,

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

security standards must include pre-approved configurations, tools, technologies, and design patterns as well as the initial entitlements for who can manage what services on the cloud platform.

- **Design**: During the application design process in PaaS, the main focus for security is on cloud architecture, platform features, provider's baseline capabilities, and automating and managing security for application deployment and operations. By leveraging the provider's security capabilities, integrating security into the application architecture offers significant security benefits.
- **Develop**: To configure services, networks, and other settings, developers may often require a development environment with admin access to the cloud management plane. They must not be given access to a production environment or hold production data. It is likely that developers use CI/CD pipelines (e.g., the code repository) so these pipelines must be secured. If developers use PaaS, they must build logging into their apps so that they can compensate for any loss of service, system, or network logs.
- **Test**: It is required to integrate security testing into the deployment process and pipeline. Security testing involves security functional tests, security unit tests, SAST, and DAST. In the cloud, organizations must use automated testing. The scope of application testing often involves infrastructure because of IaaS where templates and automation are used to define and implement the infrastructure. It is essential to have flagging features as part of security testing for security-sensitive capabilities that need deeper security review (e.g., encryption code and authentication).

Security is built into an application during the entire software/application development lifecycle. It is essential for developers to understand the cloud platform on which the applications will be executed. Having a clear understanding will help them to use appropriate security controls provided by the provider to securely develop cloud applications.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Application Architecture

- The four different types of cloud application architectures are

Microservices Architecture

- Microservices architecture is an approach where a single application is composed of many **smaller components** or services
- The best practices for securing the microservices architecture include the following:
  - Build secure API gateways
  - Use **OAuth/OAuth2** as the standard for authorization
  - Scan dependencies to detect and remediate vulnerabilities
  - Integrate application security testing tools throughout the DevSecOps pipeline
  - Implement container security

Cloud-based architecture

- Cloud-based architecture provides scalability, high availability, and resource elasticity for building web applications
- It consists databases, web servers, load balancers and application servers
- Cloud-based architecture provides security features such as **redundancy, resilience,** and **scalability**
- To secure cloud-based architecture, we should:
  - Implement **end-point encryption**
  - Use intrusion detection system and intrusion prevention system
  - Define the **policy of cloud usage** for all users

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

Cloud Application Architecture (contd.)

hide01.ir

Event Driven Serverless Architecture (EDA)

- EDA provides a **decoupled system** to run and respond to events that trigger and communicate between services
- The distributed serverless EDA enables codes to automate scale for REST API or event trigger
- Best security practices include:
  - Implement **environment variable** to store configuration
  - Enable strict network access controls using security groups and ACL
  - Implement **one-role-per-function** practice

Cloud Native Architecture

- Cloud native architecture offers planning to build and run application in public, private, and hybrid cloud
- The cloud native architecture model uses **DevOps, continuous integration (CI), continuous delivery (CD), microservices, and containers**
- Best security practices include:
  - Integrate security at container and microservices level
  - Ensure that the feedback of automated security processes is in place
  - Define security policies and ensure that no vulnerabilities exist

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

Cloud Application Architecture

The main focus of application design is on features such as agility, statelessness, and user experience. Different application architectures provide different features. Organizations must adopt the right application architecture based on their business requirements.

The four different types of cloud application architectures are described below.

Microservice Architecture

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Microservice architecture is a design that divides single applications into smaller components and services tested and deployed separately according to business requirements. Each service uses different storage and is written in different programming languages. Services communicate using lightweight protocols. Sidecar, Ambassador, and Adapter are examples of frameworks that support microservice architecture.

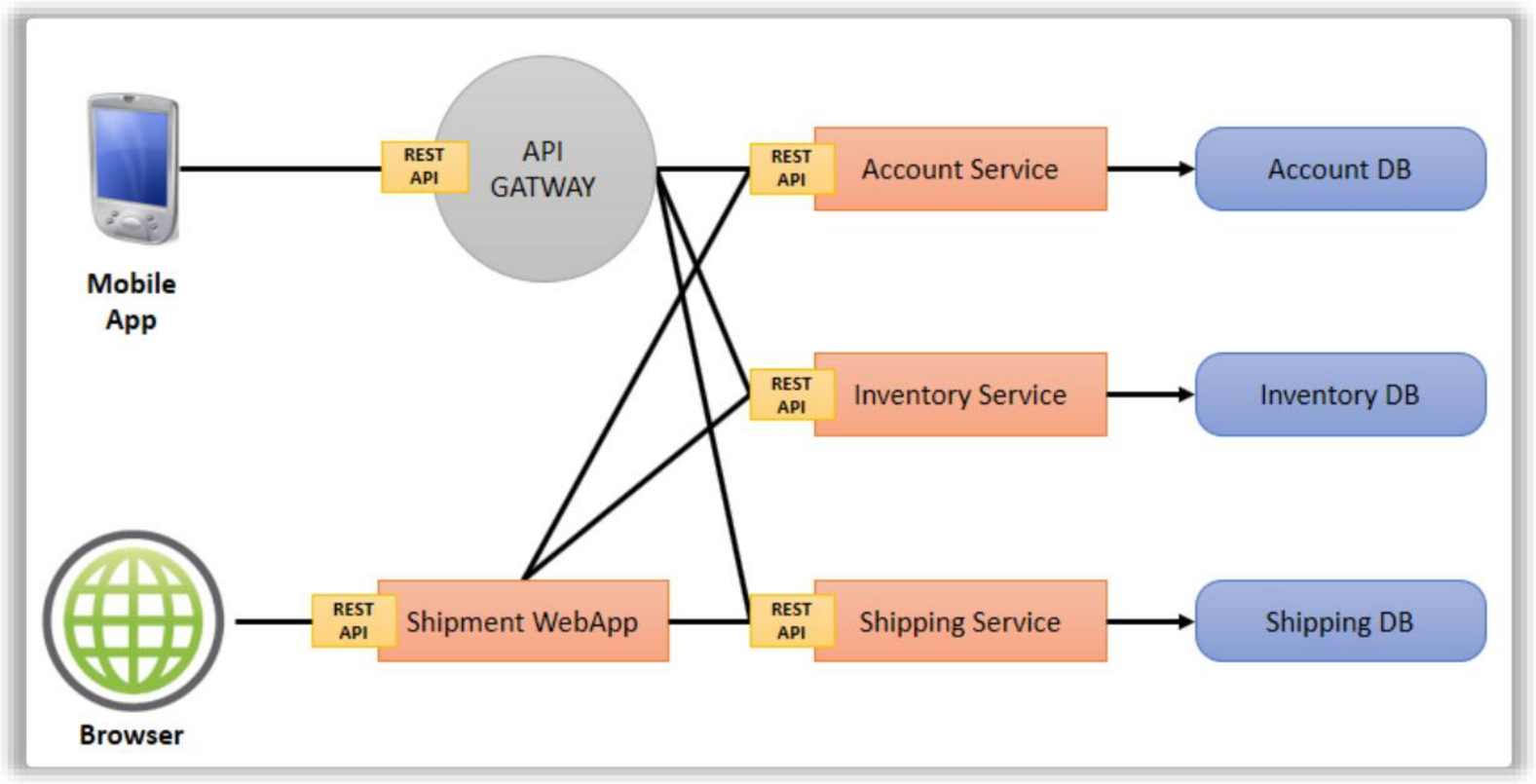


FIGURE 3.3: Microservice Architecture

Described below are the best practices for microservices architecture.

- **Built secure API gateway:** APIs are the most vulnerable areas of a microservice architecture. An API gateway acts as a single point of entry for all services, and handles external requests, helps clients get direct access to microservice, and prevents attacks from malicious actors.
- **Use authentication and access control:** It offers authentication and access control for endpoint security in microservices through security planes. It implements OAuth/OAuth2 authentication for securing services. MFA is effective for prevention and detection as it blocks malicious users and provides warning about intruders.
- **Scan dependency:** Third-party and open-source components create a tangled dependency on the web that is impossible to track and cause security vulnerabilities. Establish connection to third-party components and their dependency to detect and remediate security vulnerabilities.
- **Application security test tools:** Implement integration on black-box and white-box application security testing tools on DevSecOps pipelines that include static application security testing (SAST), dynamic application security testing (DAST), runtime application self-protection (RASP), and software composition analysis tools (SCA).
- **Container security:** It implements in a cloud-native environment where microservices reside and offers an entire container environment that includes container images, registration, and orchestration. DevSecOps provide automated container security tools and technologies for integration.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud-based Architecture

The cloud-based architecture builds a modern web application that deploys web applications to connect databases and analyze user behavior. A traditional cloud-based architecture contains load balancers, application servers, and databases. It provides cloud features such as resource elasticity, software-defined networking, auto-provisioning, high availability, and scalabilities that make it suitable for maintaining organizations' servers. It supports different programming languages like PHP, Java, .NET, Node.js, Python, Ruby, Docker, and Go. It provides an API gateway to create and publish secure APIs, which are the front gate for applications. APIs ensure authentication and access control and invoke serverless functions for API calls.

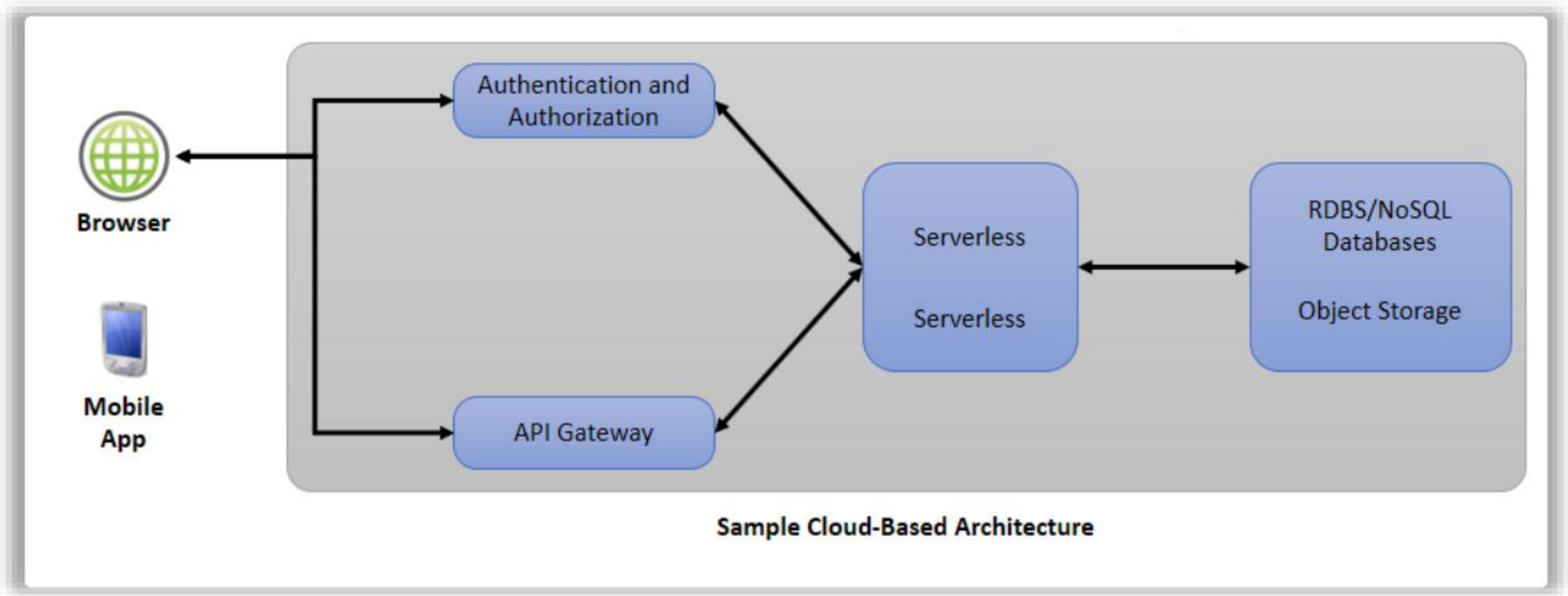


FIGURE 3.4: Cloud-based Architecture

Described below are the best practices for cloud-based architecture.

- **Implement endpoint security:** Endpoint protection protects end-user devices such as laptops, desktops, and mobile devices. Enhancing endpoint security prevents risk activities that provide entry points to malicious users. Protection and compliance provide organizations to gain robust control over their services.
- **Implement intrusion detection and prevention system:** It is the third most effective cloud security system that monitors corporate networks for intrusion signs, prevents unauthorized access, and alerts security administrators of the attempt. It deploys mitigation solutions and increases the response capability for blocking access from the source.
- **Define cloud usage policy for all users:** Enable cloud utilization for implementing security strategies to the cloud. Implement monitoring on cloud resources and activities of users to maintain cloud security. Through this, activities of suspicious users get denied, thereby minimizing security risks on cloud data and applications.

Event-driven Serverless Architecture

It provides a decoupled system to run event response and establish communication on decoupled services. EDA provides agility, cost-saving, and operational benefits. The distributed serverless EDA implements codes that automatically respond to REST API without any management systems to offer a scalable model for updates and deployment.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Described below are the best practices for event-driven architecture.

- **Implement environment variable to store configuration**: Enable environment variables to store configuration such as hostnames as it is accessible to change deployments and source codes. Moreover, it decreases the risk of data exposer.
- **Enable strict network access controls using security groups and access control lists (ACLs):** Ensure strict network access control by implementing API gateways. Implement function-specific API authentications that establish capabilities to provide multiple authentication and authorization mechanisms.
- **Implement one-role-per-function practice:** This implements single role for multiple functions. It enables a single function with an identity and access management (IAM) role. For example, if a user is supported to read the data, it should only have read access. Providing higher privileges increases the chances of leverage attacks.

Cloud-native Architecture

Cloud-native architecture provides design to deploy cloud from application planning. It builds and runs applications that exploit the advantages of the delivery model. It describes a container-based environment to create and deploy applications. Cloud-native architecture implements applications in public, private, and hybrid clouds. It helps people, processes, and technologies to build, deploy, and manage apps for the cloud. The cloud-native architecture model uses DevOps, continuous integration (CI), continuous delivery (CD), microservices, and containers.

hide01.ir

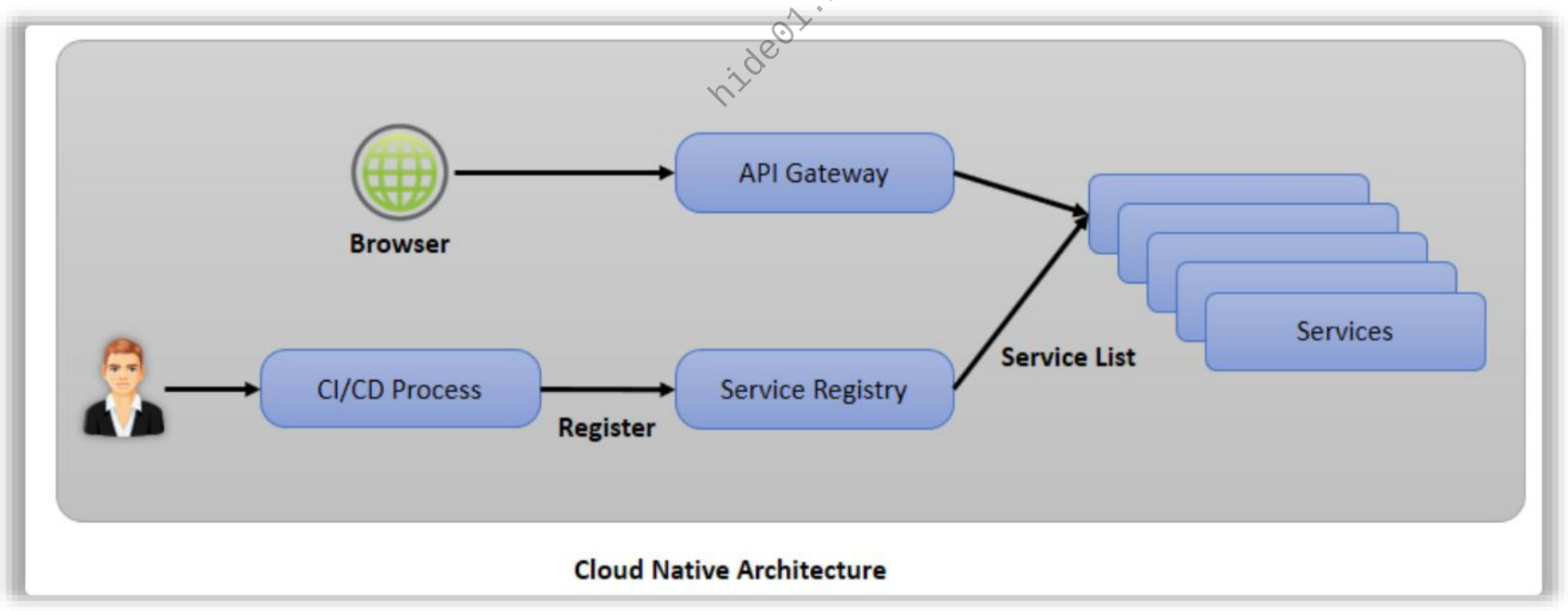
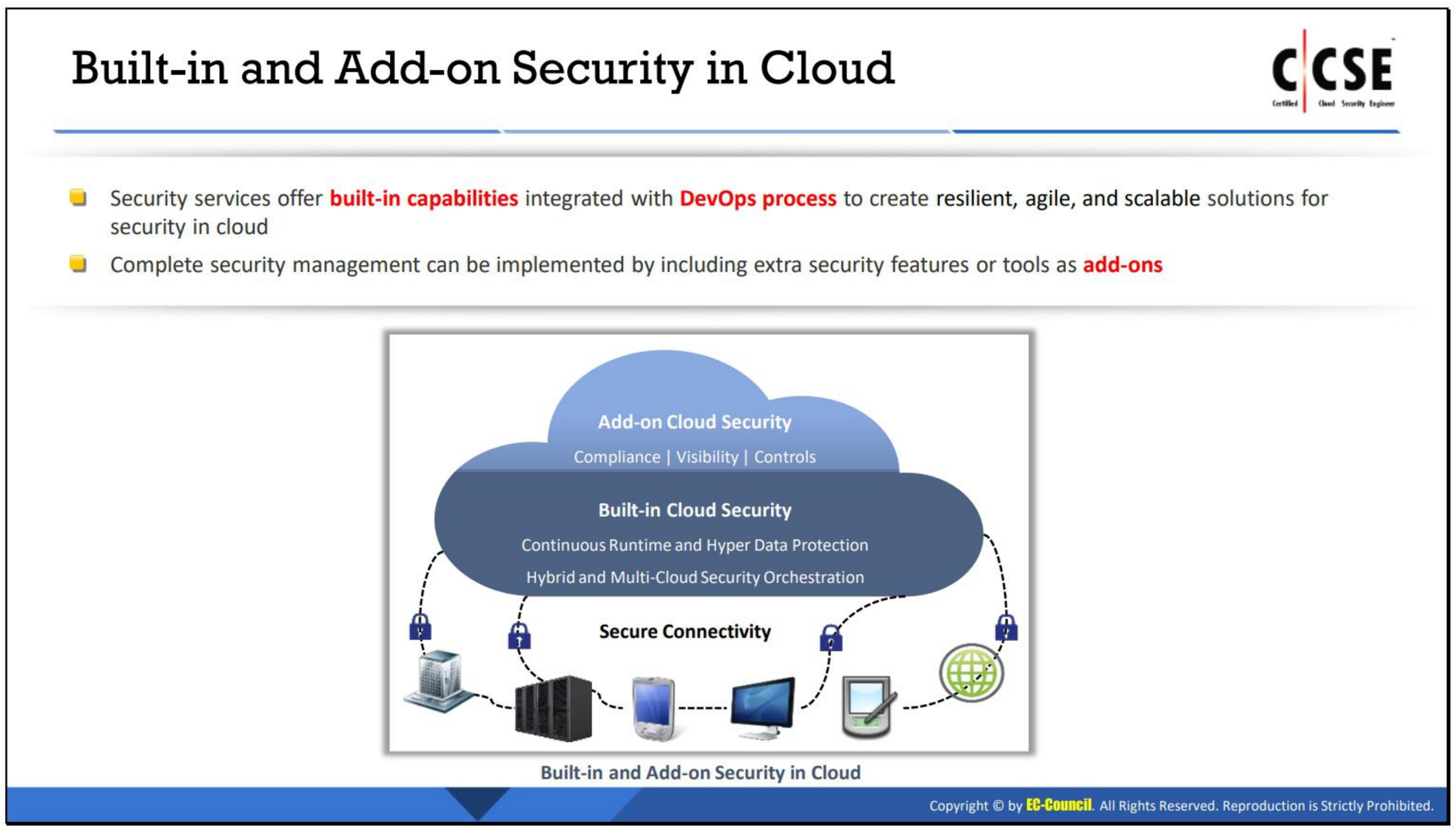


FIGURE 3.5: Cloud Native Architecture

Described below are the best practices for cloud-native architecture.

- Implement security at the container and microservices level to create a secure cloud application architecture as the containers secure development engineer code directly.
- Enable automation to control assets and enable immediate feedback on failed or successful tests to implement automatic security.
- Security policies should be applied to ensure that there are no vulnerabilities. Security should become a repeated required step in the ongoing development cycle of the application.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Built-in and Add-on Security in the Cloud

Cloud developers use simple and effective ways to secure their cloud-native applications in organizations. Security services offer built-in capability services for the cloud integrated with the DevOps process to create resilient, agile, and scalable solutions for security in the cloud.

Security experts use security investments to implement complete security management that provides extra security features or tool add-ons for organizations in the cloud.

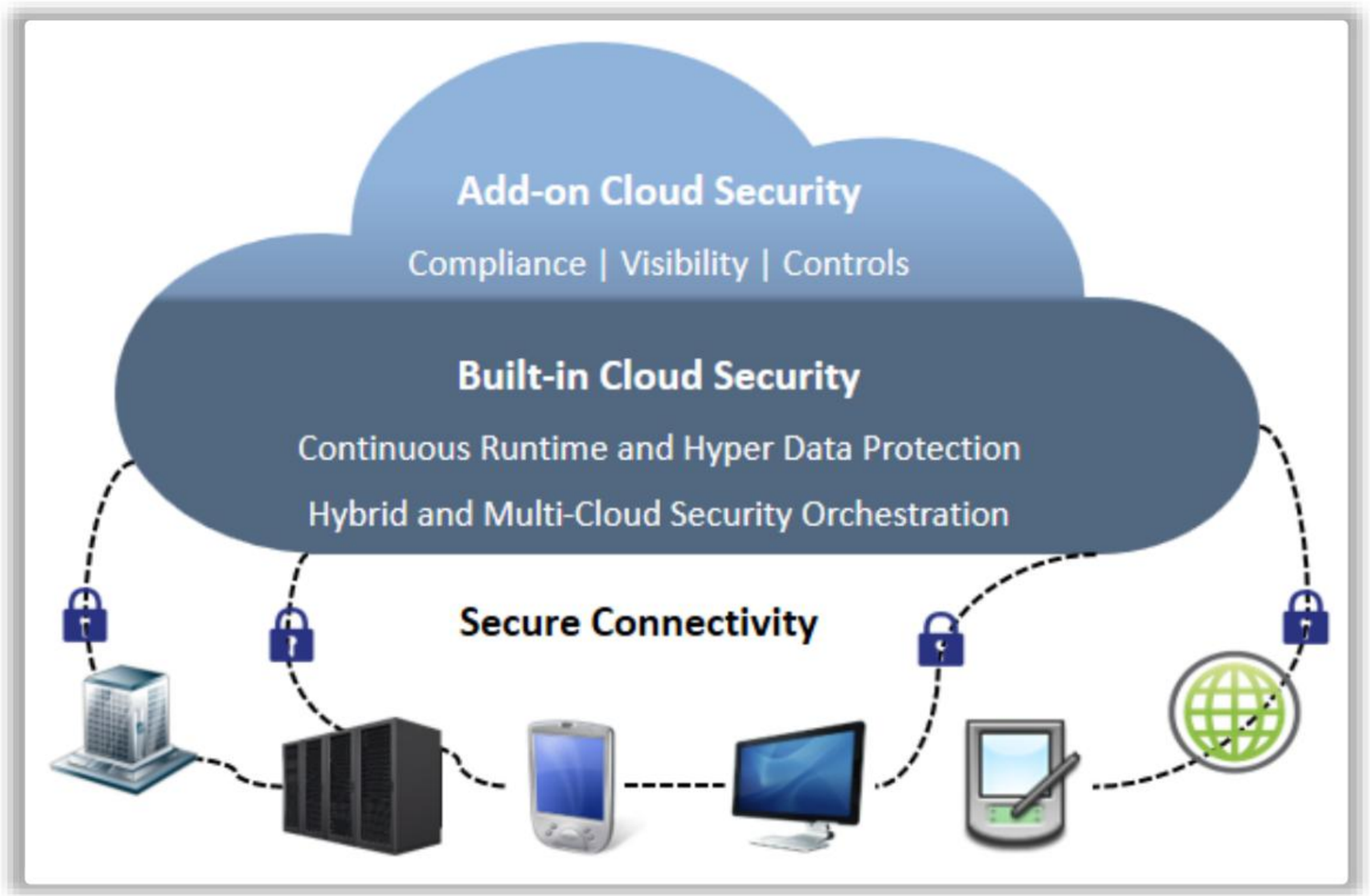


FIGURE 3.6:Built-in Add-on Security in the Cloud

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Key components to create a secure cloud solution include the following.

- **Managing identities and access:** Implement identity management to control user access on cloud resources associated with privilege activities done by cloud administrators. Enable activity tracking for people involved in development and operations to establish access control on user managing and customer access for cloud applications.
- **Protecting infrastructure, application, and data**: Provide tenant-specific network isolation to protect cloud infrastructure in traditional data centers. Implement a secure development and operations process design for application protection, including identifying and managing vulnerabilities in VM, container, and application code. Implement encryption techniques for data protection on files, objects, storage, and data in motion, including data activity monitoring and add processes to verify and audit outsourcing data on the cloud.
- **Gaining visibility across the environment**: Offer activity monitoring to provide complete visibility in on-premises and cloud-based environments. Establish security and visibility on virtual infrastructure through log collection and analyzing various services and components in the cloud.

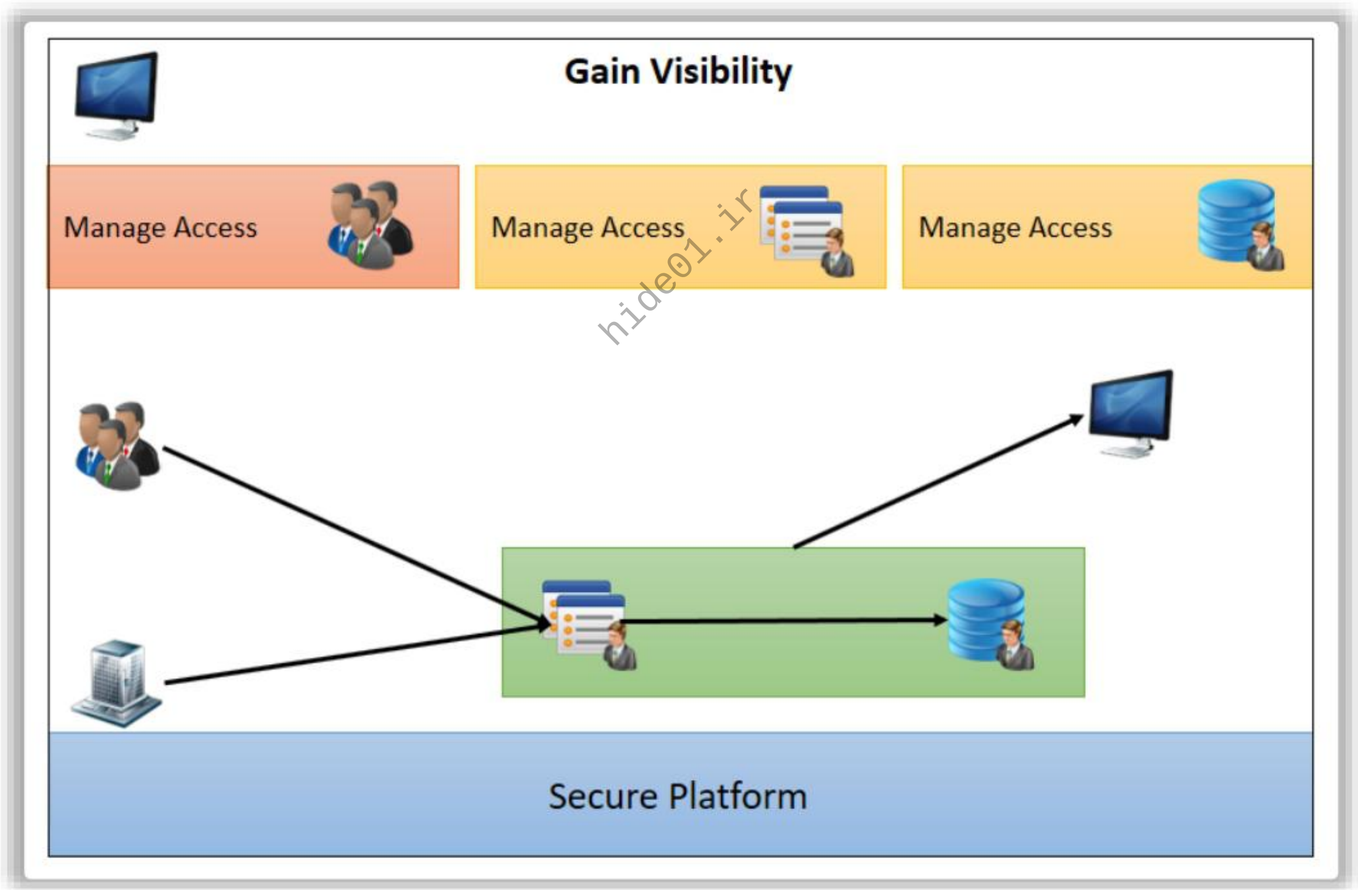
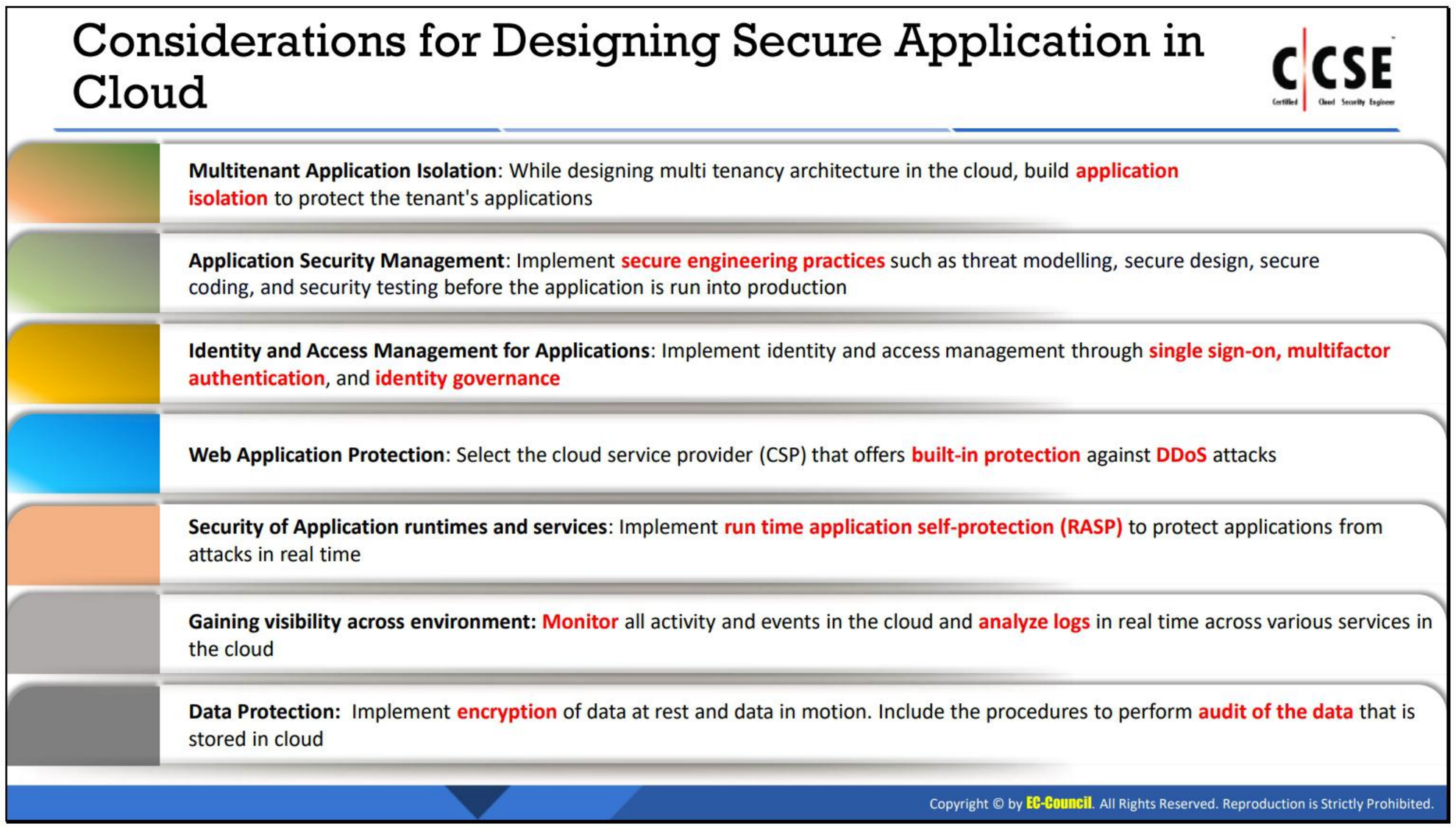


FIGURE 3.7: Gain Visibility

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Considerations for Designing Secure Application in Cloud

Cloud application security provides data privacy and ensures that applications are working fast.

Described below are the application security types.

- **Multitenant application isolation**: Clouds use multitenant architecture where a single software application serves multiple tenants. It is cost-efficient, and establishes efficient application isolation through container isolation and network isolation to protect tenant data and application.
- **Application security management**: Implement secure engineering practices to ensure security foundation before developing application. The following practices prevent applications and services from vulnerabilities:
    - Enable threat modeling to identify weaknesses and threat patterns.
    - Implement a secure mitigation design.
    - Implement secure coding guides and practices to prevent vulnerabilities.
    - Enable security testing to fix problems before deployment to validate that product is risk-free.

  Ensure that applications follow development lifecycle components to ensure secure development of the application.

Identity and Access Management for Applications

Implement used authentication model for identity and access management of an application.

- Unprotected websites or mobile application do not require authentication.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- SAML and Open ID Connect-based repository handle authentication for API, including cloud functions for existing customers, business partners or supplies, and internal employees and users .
- Cloud directory handles authentication for API, including cloud functions for new customers.

Web Application Protection

Implement built-in DDoS protection provided by the CSPs against DDoS attacks to ensure security for web applications.

Security of Application Runtimes and Services

Implement RASP for securing application runtime and services. It is a technology that runs on the server and detects an attack in real-time. It monitors applications and mitigates attacks without human intervention.

Gaining Visibility Across the Environment

Offer activity analyses to ensure visibility and security on virtual infrastructure through secured log collection, services, and components in the cloud.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Best Practices for Secure Cloud application Design and Architectures

Segregation by default

- **Isolate** cloud environment to run applications by using virtual network
- Use **account/sub account structures** to enable management plane segregation

Immutable infrastructure

- Disable **remote logins** to immutable servers/containers
- Use **immutable techniques** for implementing incident recovery plans
- Implement **file integrity checking** and **monitoring**

Increased use of micro-services

- Ensure that the communication between the **microservices** and the discovery, scheduling, and routing of microservices is configured securely

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

Best Practices for Secure Cloud application Design and Architectures (Cont'd)

hide01.ir

PaaS and Serverless Architectures

- Running workloads directly on the cloud platform reduces the attack surface as it does not require managing services and operating system
- Cloud service provider should secure the **platform/serverless setup**
- **Serverless platform** prevents direct network attacks by utilizing providers network communication using **API** or **HTTPS traffic**

Event-driven Security

- Event-driven code execution in cloud platform can define events and perform security actions such as **automated notification, assessment, remediation, etc.**

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

Best Practices for Secure Cloud Application Design and Architectures

Cloud computing is making changes to the preferred application architectures, designs, and patterns. Though most of these changes do not directly affect application security, certain ones offer chances to minimize common security issues.

Following are some of the application design and architecture practices that can enhance the security of cloud applications.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Segregation by default**: Applications can run easily in their own separated cloud environments. A separate cloud environment can be an isolated virtual network or account/subaccount depending on the provider. Use account/sub account structures to enable management plane segregation. Organizations can allow more rights in development accounts when running production accounts that are highly restrictive.
- **Immutable infrastructure**: In cloud computing, immutable infrastructure is becoming popular due to various operational reasons. Enhance cloud application security by
  - Turning off remote logins to immutable containers/servers.
  - Using immutable techniques for implementing incident recovery plans.
  - Implementing file integrity checking and monitoring.
- **Increased use of microservices**: Using microservices enhances workload security. Ensure that the communication between the microservices and the discovery, scheduling, and routing of microservices is configured securely.
- **PaaS and serverless architectures**: Running workloads directly on the cloud platform reduces the attack surface as it does not require managing services and operating systems. With PaaS and serverless architectures, the responsibility to secure the platform/serverless setup lies with the cloud provider.

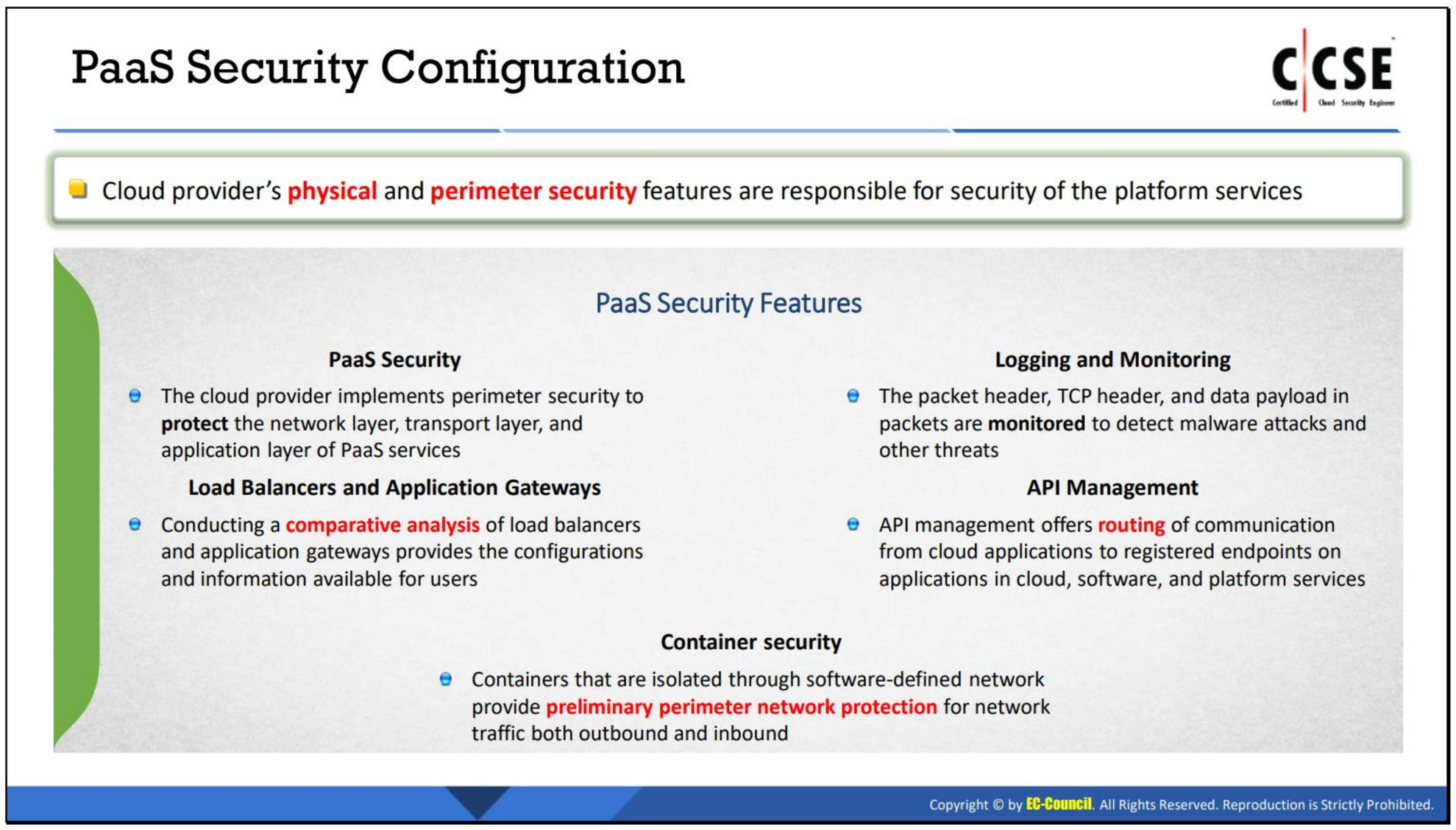
  Serverless platforms prevent direct network attacks by utilizing the provider's network to have communication with the consumer's components using API or HTTPS traffic. The attacker can only try making API calls or access HTTPS traffic but cannot scan ports, utilize common techniques, and detect other servers.

hide01.ir

- **Software-defined security**: It enables automating security operations such as incident response, change management, and their integration into the application stack. Security teams can use software-defined security to perform activities such as automating cloud incident response, remediating unapproved infrastructure changes, and automating dynamic entitlement changes.
- **Event-driven security**: Event-driven code execution is supported by certain cloud providers. In event-driven cases, various activities (e.g., a configuration change to identity management or the network or a file being uploaded to an assigned object storage location) are detected by the management plane, which results in triggering code execution via serverless hosted code or a notification message.

  Events can be defined for security actions and event-driven capabilities can be used to trigger automated assessment, notification, remediation, or various other security processes.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



PaaS Security Configuration

The cloud providers physical and perimeter security offers the security context for cloud provider platform services:

hide01.ir

PaaS Security

PaaS services implement protection through cloud perimeter security measures on the network, transport, and application layers. The cloud providers perimeter comprises of the following:

- Implement network-layer DDoS before internet traffic reaches cloud provider virtual network, VMs, and subnets. It provides a physical network layer that protects the cloud provider platform from large-scale internet-based attacks. These are not user-configurable and applied before public IP NAR address translation.
- The cloud provider network DDoS would not detect small-scale DDoS attacks that target a specific network weakness. Customers should implement application layer DDoS protection.

The network perimeter subnet directly communicates to the internet. The routing tables are responsible for providing communication from and to the on-premises and back-end networks. Cloud application traffic moves from the cloud provides application layer WAF. All WAFs are not able to offer the evaluation on the level of protection. You may enable fine-grained access management using the cloud provider's role-based access control (RBAC) on cloud service offerings.

Load Balancer and Application Gateway

Implement analysis of load balancers and application gateway to include available configuration level. Customers can access information from operational dashboards. It forms functions for each provides that describes their set of terms.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Logging and Monitoring

Monitor incident security events of management operations by implementing analysis on TCP header and data payload in network packets that allow or deny connections with application-layer contents. It offers to counteract the growing number, type, and nature of threats and attacks from malware.

API Management

An API management capability allows users to use APIs to publish self-service portals used by application developers to consume APIs. It provides communication routing from cloud applications to registered endpoints on the cloud provider-hosted applications, software, and platform services. API management services provide a part of tokens that pass parameters from the cloud application to the cloud provider services. API management policy types include the following:

- Access restrictions such as token validation and API call rate limits.
- Enable request forwarding, conditional evaluation, execution, and call logging.
- Authentication
- Message transformation
- Configuration of cross-domain calls

Container Security

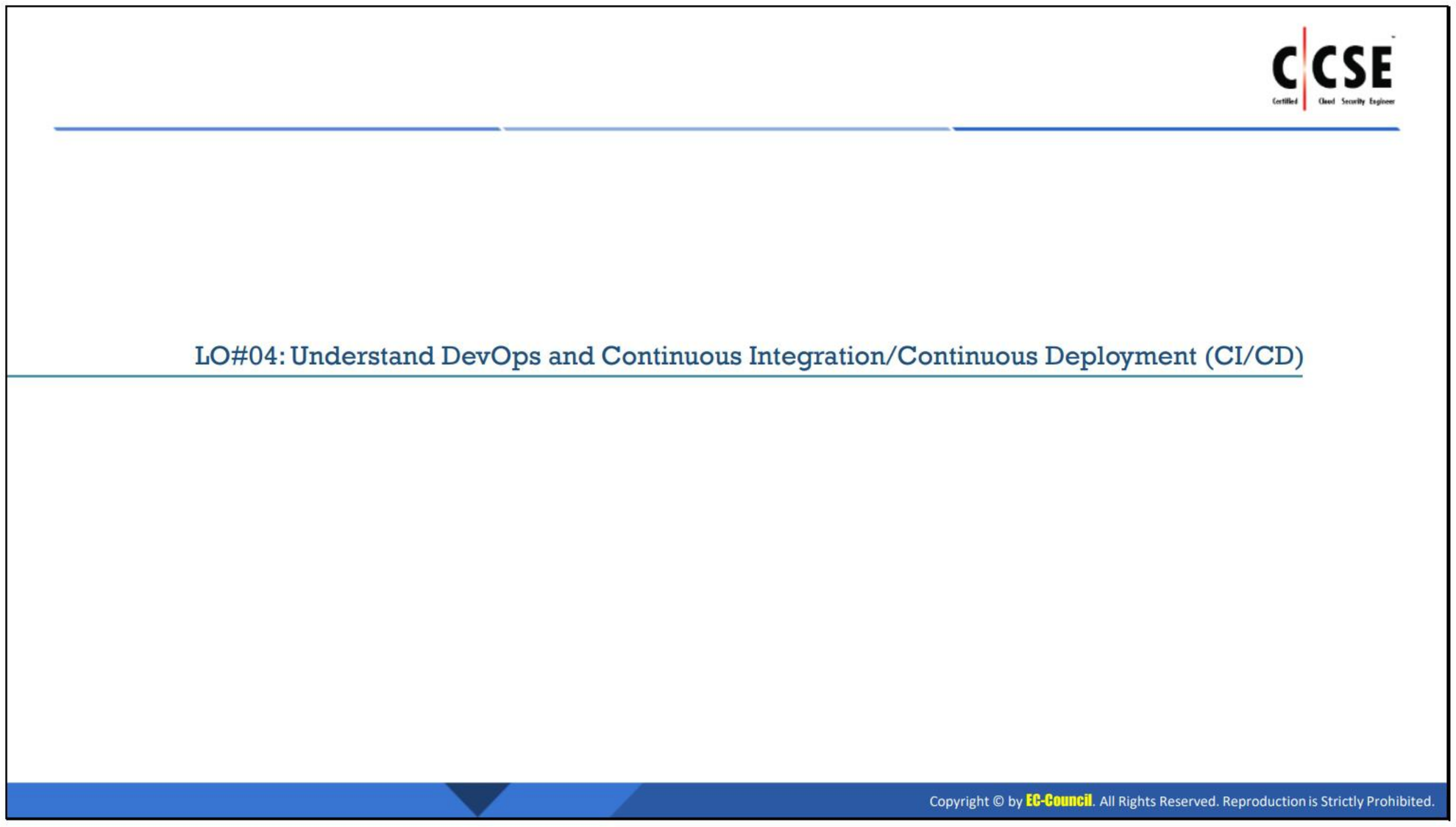
hide01.ir

It deploys cloud applications as microservices through a development model suited for SaaS. Containers get isolated by a software-defined network that provides network security for inbound and outbound traffics. Configure pipeline endpoints for using the cloud provider's file storage. Configure access control for code repository access. Container orchestration provides coordination of the management, control, and data planes for containers. Linux control groups provide the basis for container operations and vulnerabilities that include access to Linux filesystems. Agents provide container health care data that offer performance management and coordination, aggregate data for preventive management, and raise alerts and alarms. Fine-grained access control configures and manages the identity management services of a cloud provider. Container services provide schedule management, resource management, and service management for distributed Linux nodes to deploy container clusters.

Security features for containers are listed below.

- **Identity management**:
  - Establish control on access to management interfaces using IDM access control.
  - Implement authentication on connections to the cluster.
  - Enable access control on communication routing.
- **Network security**:
  - Implement software-defined networking to configure design for cloud provider's standard network templates.

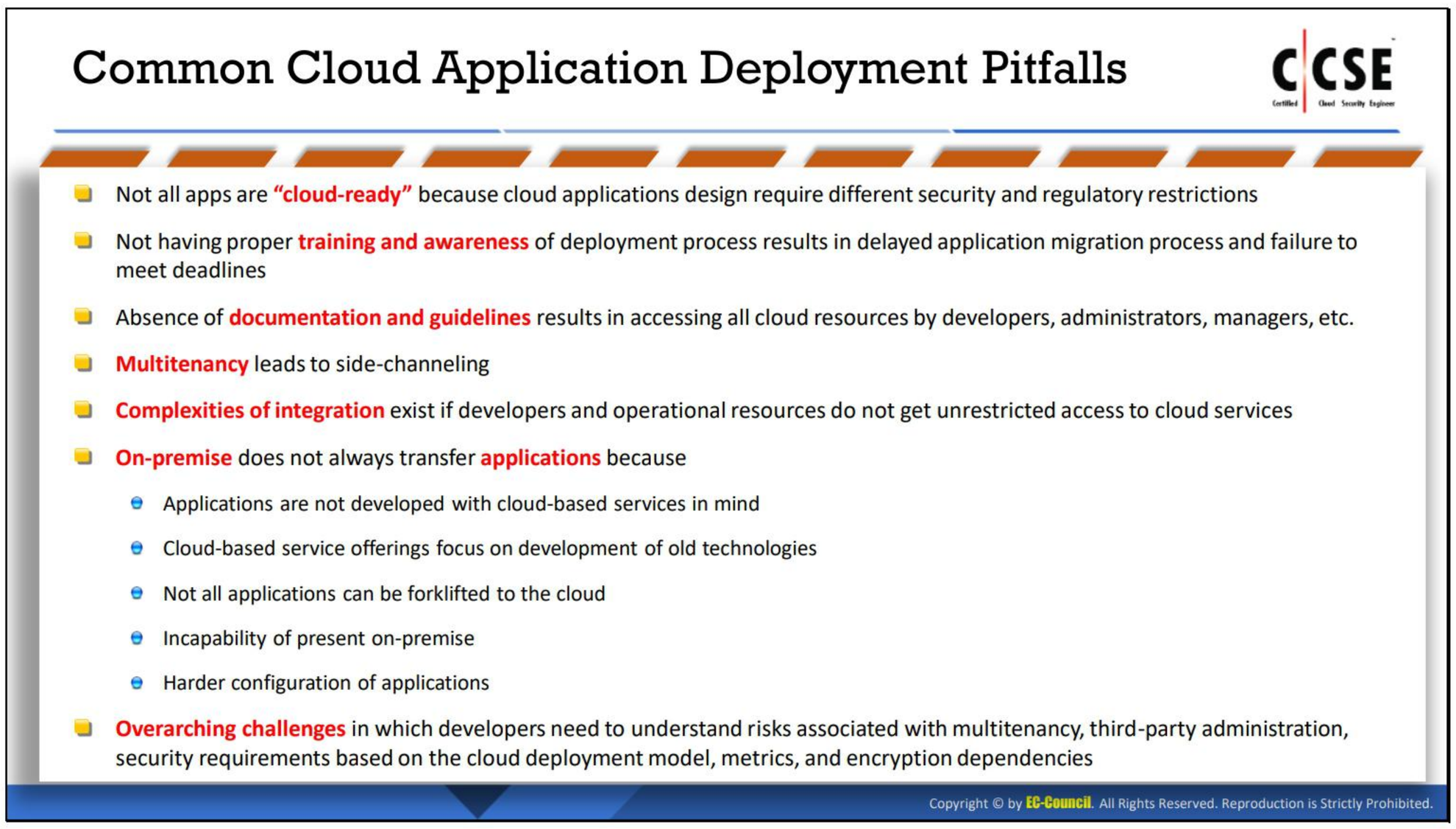
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#04: Understand DevOps and Continuous Integration/ Continuous Deployment (CI/CD)

This section explains integration and importance of security during continuous integration, development, testing, deployment, and operations. It discusses how security of cloud applications can be enhanced while using Infrastructure-as-Code (IaC) and DevSecOps.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Common Cloud Application Deployment Pitfalls

Common pitfalls that can affect organizations when cloud applications are deployed/migrated to the cloud are listed below:

hide01.ir

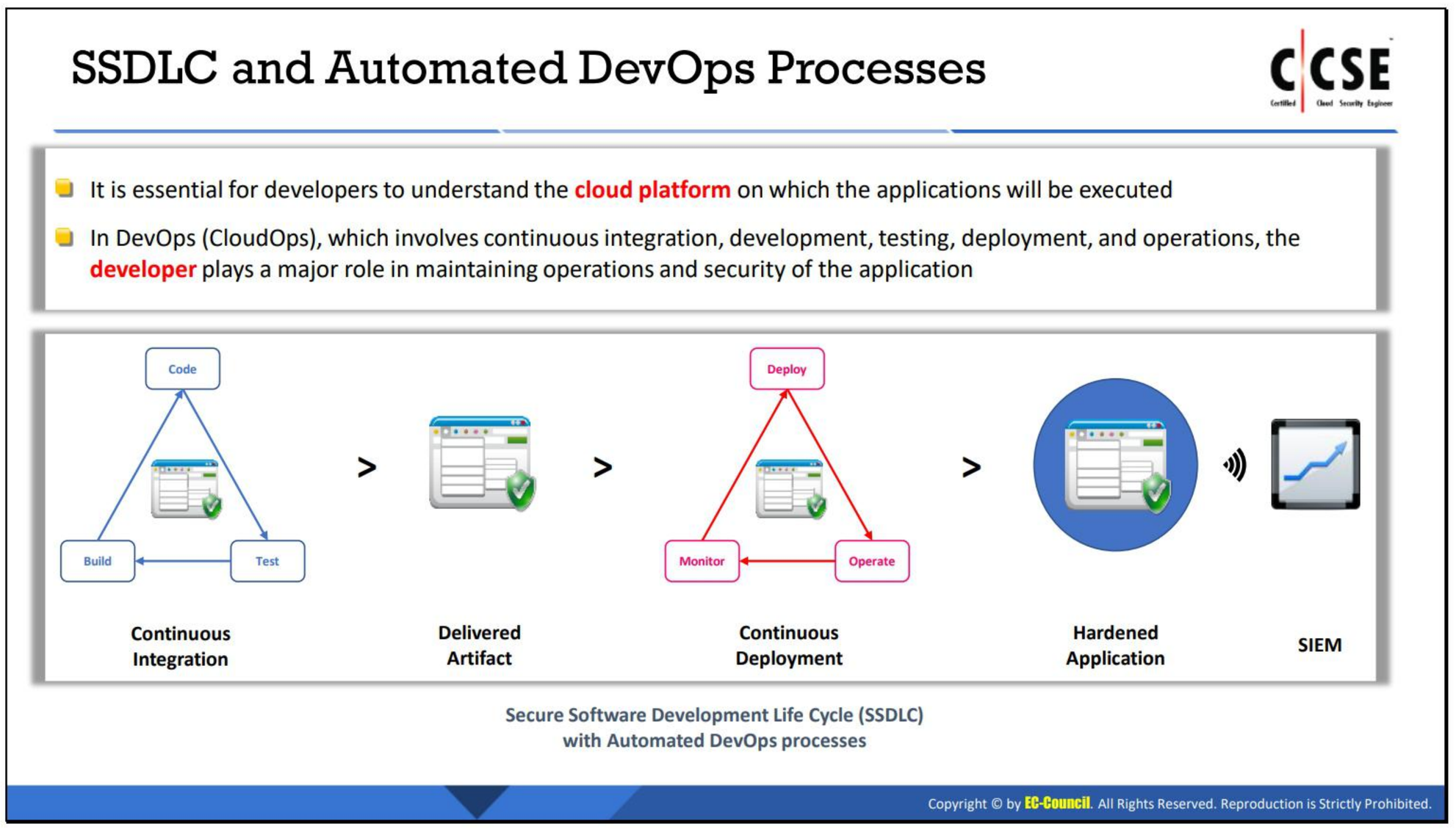
- **Not all applications are cloud-ready**: It is because many high-end applications come with
  - Multiple and distinct security and regulatory restrictions
  - Relying on traditional coding practices
- **Lack of training and awareness**: Training and awareness are needed for employees to work with new development techniques and approaches and utilize new services. Without experienced staff or proper training
  - The migration process would require considerable time, resulting in failing to meet deadlines or facing any additional issues.
  - There would be a higher risk of bringing the legacy into the cloud.
- **Absence of documentation and guidelines**: In the absence of policy implementation, there is a chance of accessing all cloud services by developers, managers, or administrators. The developer should follow the required methodologies, processes, documentation, lifecycles, and guidelines to prevent risks.
- **Multitenancy/tenancy separation**: Many public cloud service providers use multitenancy to optimize server workload and reduce costs by sharing the workload across multiple cloud environments. This practice leads to side-channeling, which occurs when an attacker can access information through a shared tenant's node.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Complexities of integration:** Complexities of integration exist if developers and operational resources do not get unrestricted access to cloud services and supporting components. This might exist particularly if the cloud provider manages infrastructure, apps, and integration platforms. If this is the case or reduces such complexities, use a secure and validated cloud provider's API.
- **On-premise does not always transfer applications and vice versa:** The reasons why on-premises do not always transfer applications included are
  - Applications are not developed with cloud-based services in mind.
  - Expansion of cloud-based service offerings
    - Focus only on enhancing old technologies and development.
    - Do not always maintain support for more development and systems.
  - Not all applications can be forklifted to the cloud. Here, forklifting is the migration process of the entire application the way it runs on on-premises (traditional infrastructure) with minimal changes in its code.
  - Present performance and functionality of a system may not be transferable.
  - Applications and their configurations may be hard to replicate through cloud services.
- **Overarching challenges:** Developers should understand
  - Risks associated with cloud applications: **multitenancy** and **third-party administrators**
  - Security requirements based on the **cloud deployment model** that the application will run in **cloud service model.**
  - **Metrics** because cloud applications may have a higher reliance on metrics than internal applications to provide visibility into who is accessing and what action is performed on applications.
  - Encryption dependencies for **encryption of data at rest**, **encryption of data in transit**, and **data masking/data obfuscation**.

hade01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SSDLC and Automated DevOps Processes

In a cloud environment, deployment automation often involves security activities that can also be implemented in the design and development phase. Deployment automation in the cloud environment requires integrating automated security testing in a deployment pipeline. Automated security testing is conducted outside of direct developer control. Secure deployment involves security and testing activities that are performed while moving application code from a development environment into the production environment.

Application security tests that can be integrated into application cloud development and deployment are described below.

- **Code review:** Code review is a manual activity that is not part of automated testing. It helps examine specific areas that need special attention. Communications between an application and the management plane (e.g., API calls to the cloud service that can modify the infrastructure) should be scrutinized.

  Security teams must enable only the least-privilege entitlements for a part of the application and validate them with the configuration of the management plane, besides reviewing the code. They should conduct additional reviews for issues related to authentication and encryption. Moreover, security teams can automate the deployment process to notify security in case any modification to these parts of code is detected that requires manual approval or soon after-the-fact change review.

- **Unit testing, regression testing, and functional testing**: These are the standard tests developers use in their normal processes. These tests should be integrated with security testing to make sure that the application's security features continue to work as intended. These tests should be updated to include API calls.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Static application security testing (SAST):** SAST tests incorporate checks on API calls to the cloud service. SAST helps developers in analyzing the source code, binaries, and byte code of a cloud application when it is coded and designed. It uncovers the security vulnerabilities of the application. SAST tools or solutions analyze applications from the inside out in a nonrunning state. They help create applications that are less vulnerable to threats by educating developers about security flaws in cloud applications while creating them.
- **Dynamic application security testing (DAST)**: DAST is performed while cloud applications are running, and it uses penetration testing, fuzzing, and web vulnerability testing to identify security problems. DAST evaluates a cloud application from the outside-in by actually attacking it as a real attacker would do. DAST is performed from outside without any access to the application source code. Pretesting permission may be required from the provider due to contractual obligations. With the help of automated pipelines, an entirely functional test environment that uses IaaS can be set up and deep assessments can be performed prior to approving changes for production.

SSDLC and Automated DevOps Processes

It is essential for developers to understand the cloud platform on which the applications will be executed. In DevOps (CloudOps), which involves continuous integration, development, testing, deployment, and operations, developers play a major role in maintaining the operations and security of the application. Developers need to have a well-defined, robust application security program for building security into the SDLC. A robust application security program requires interworking and exchanging of information among several domains and resources. Apart from technical components (infrastructure tools, applications, and security controls), two teams are involved in ensuring application security: builders and developers.

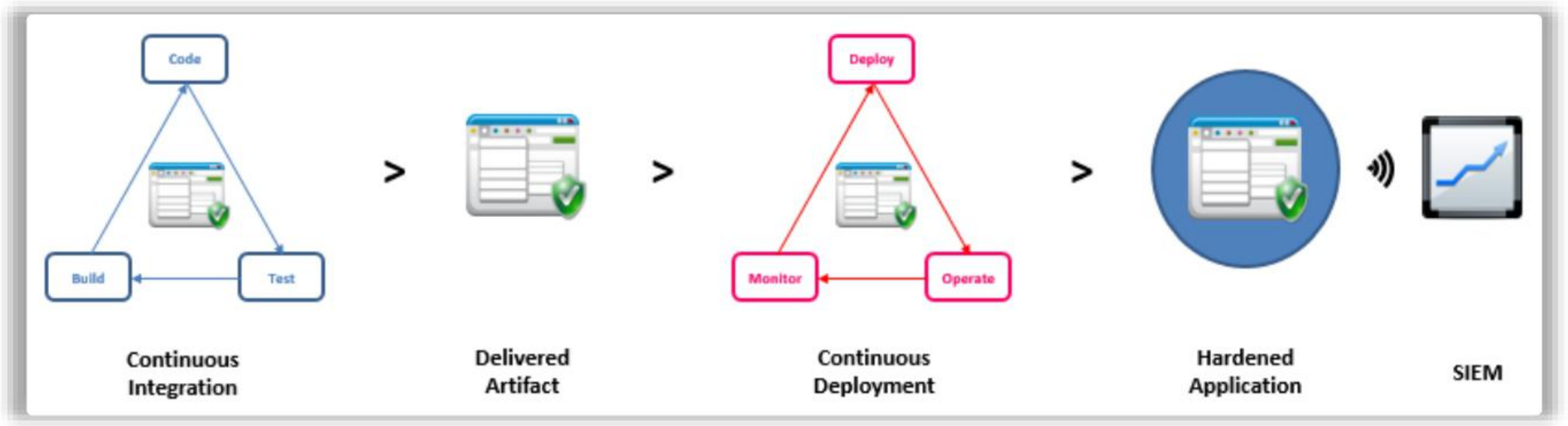


Figure 3.8: SSDLC Aligning with Automated DevOps

The above figure represents different components that contribute to application security. The teams/organizations involved in ensuring application security can be mainly categorized as described below.

Builders

Builders are the teams that normally stay within the product, technology, and business units with the aim to move applications into production as soon as possible. Builders work in an environment that has the following disruptions:

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **IT changes**: Builders often face challenges that prevent them from building applications fast. These challenges arise due to virtualization, software-defined data centers, on-demand VMs, cloud apps, and containerization.
- **DevOps**: Application development teams are now adopting an agile DevOps environment. Though the agile DevOps environment offers fast, agile development and feedback, it introduces unknown risks to the conventional software development model.
- **DevSecOps**: To fix vulnerability backlogs, builders often need to work with security administrators or defenders. Despite having various processes (scanning tools, SDLC, and penetration testing) that detect issues present in the application, builders are often under pressure to quicken application release, which forces them to push the code into production while neglecting known risks.

Builders insist on having the following requirements for application security and control:

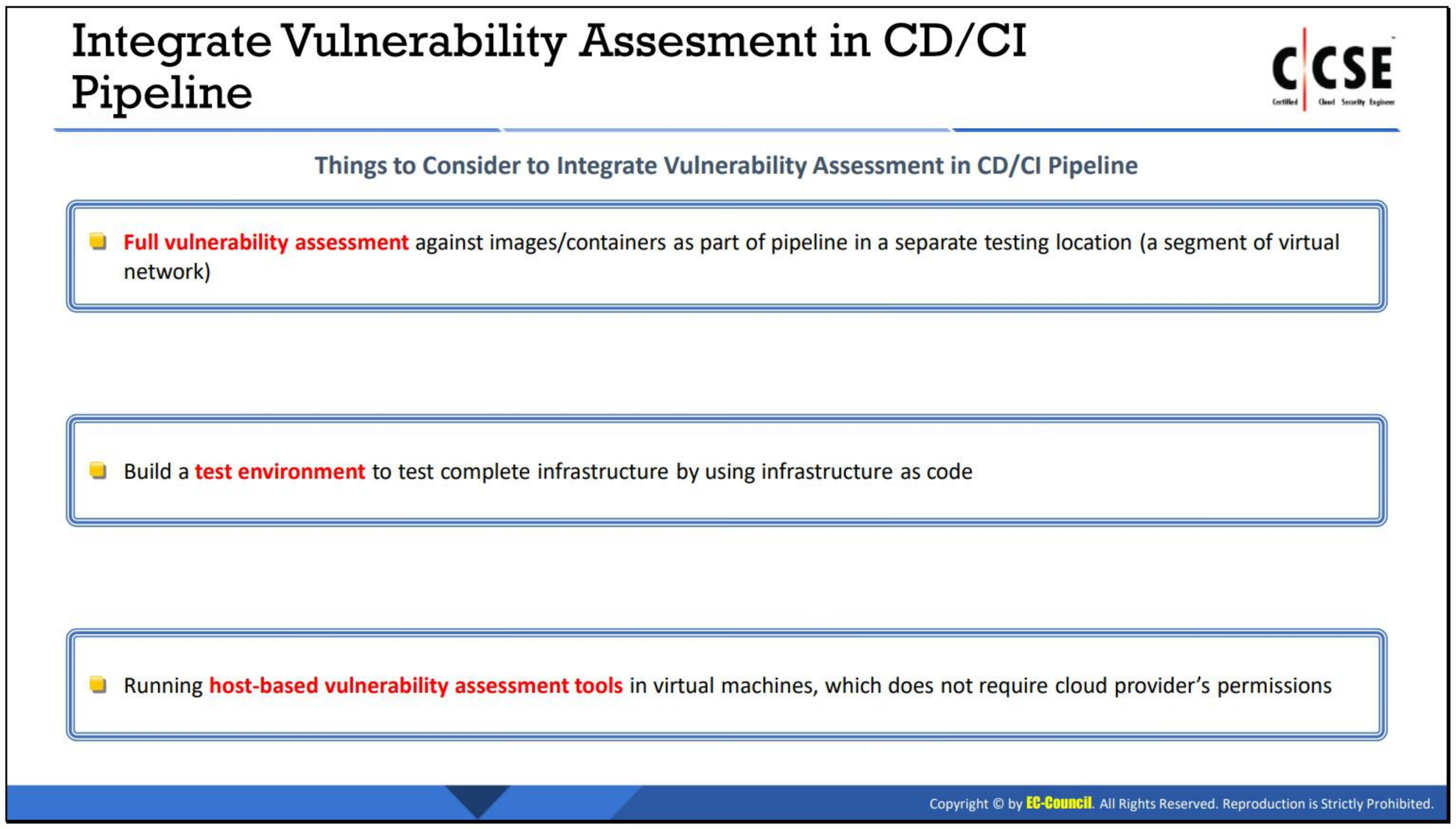
- A security tool must not impact the performance of an application.
- Vulnerabilities must be prioritized based on their criticality and real attack data must be provided from production environments by the CISO's office.
- The CIO's office should make infrastructure changes transparent to applications.

Defenders

Defenders are teams that reside within the CISO/CIO organizations with the goal of addressing enterprise security and minimize risk holistically. These teams are responsible for managing penetration-testing programs, overseeing RASP and WAF technologies, and managing application security testing solutions. Defenders have access to SIEM technologies. The following challenges are faced by information security executives, who oversee the efforts of defenders:

- Applications are complex and distributed and have fragmented approaches for application security. It is almost impossible to monitor applications and data accurately and consistently due to the cloud, virtualization, and microservices. Additionally, security strategies are mostly a collection of tools and services that are not portable or flexible.
- There is an increase in attack volumes and common attack vectors are getting sophisticated enough to bypass current controls. To prevent modern, common attack vectors, pragmatic, simple application security controls are needed.
- Because of unmitigated vulnerabilities, critical production apps are at risk. When builders move code to production without mitigating known risks, critical production apps are at risk. It is essential to use vulnerability mitigation tools and security controls to avoid such risk.
- Absence of visibility into runtime security events. Defenders are not able to access useful runtime attack data even after conducting analysis at the preproduction stage or gathering intelligence at the network layer.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Integrate Vulnerability Assesment in CD/CI Pipeline

A continuous integration/continuous delivery (CI/CD) pipeline refers to a series of actions that are performed to deliver a new version of software. CI/CD pipelines mainly focus on making software delivery better using a site reliability engineering (SRE) or DevOps approach. To improve the application development process at the integration, testing, delivery, and deployment phases, a CI/CD pipeline supports automation and monitoring. Though the steps/actions of the pipeline can be automated, they can also be executed manually.

A CI/CD pipeline hosted and managed using cloud-native tools in the cloud can best serve cloud-based applications. With these pipelines, applications can also integrate security and compliance in a manner that suits the cloud environment. These pipelines help to enable DevSecOps, which is a process of continuously integrating security into the SDLC.

It is easy to integrate vulnerability assessment into CD/CI pipelines and then implement it the cloud. However, it essentially requires compliance with the terms of service of the provider. To accelerate software delivery, organizations can use these pipelines. With vulnerability scanning, software security improves and individuals working in various teams (engineering and product teams) are responsible for the processes they own or work on.

The following patterns can be used to integrate vulnerability assessment in CD/CI pipelines:

- **Assessments against images**: This pattern requires running full assessments against containers/images as part of the pipeline in a specific testing area of the cloud (e.g., a virtual network segment) that is specially defined for this purpose. The image is approved for production only when it passes this assessment.

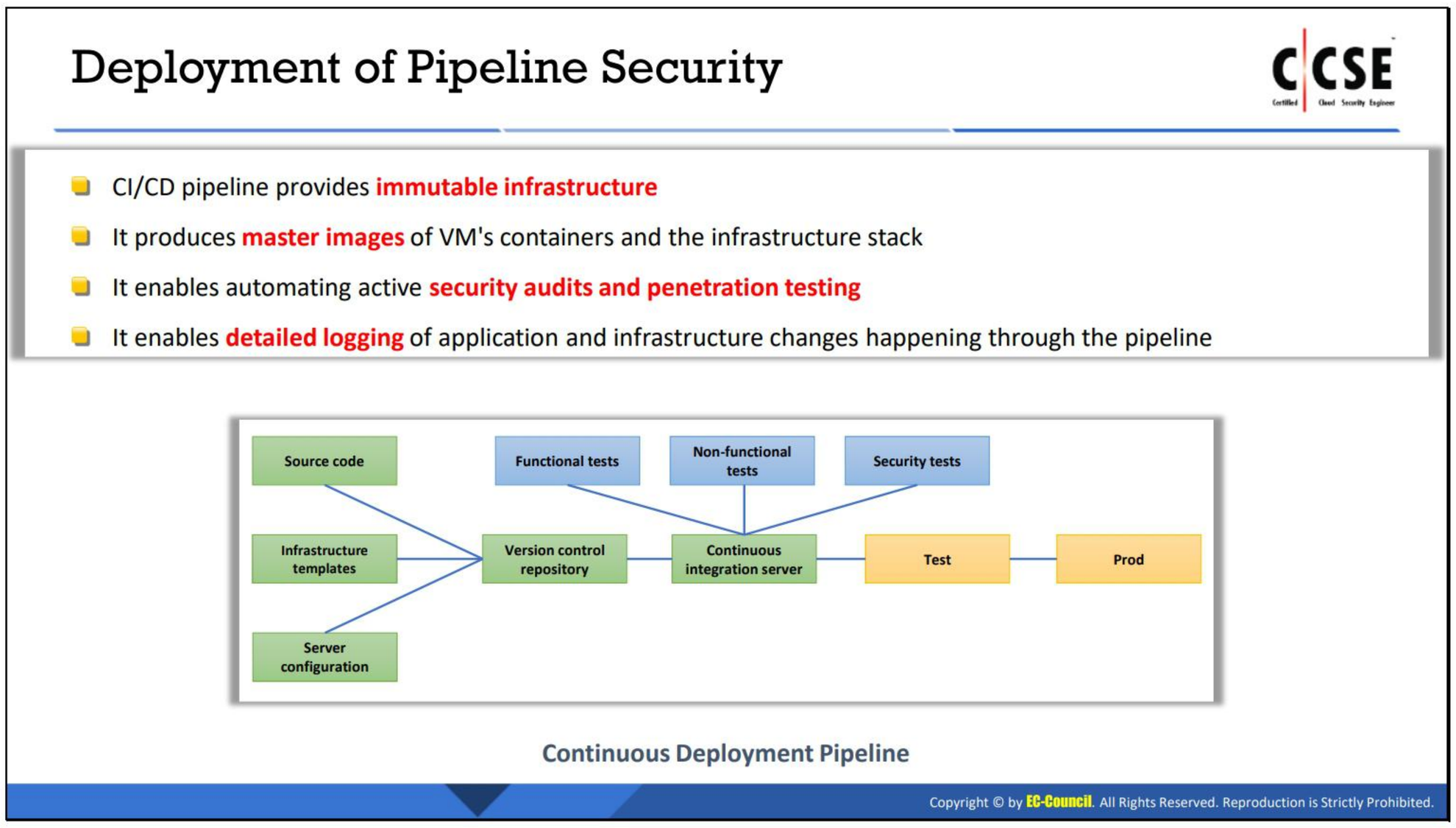
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Testing entire infrastructure**: This pattern requires building a test environment to test the complete infrastructure by using IaC. Unlike the "assessments against images" pattern, this pattern can easily test the entire infrastructure to identify vulnerabilities.

In these patterns, the production environment is not tested at all or tested less because it is immutable and exactly like the test environment. Both environments are based on the same definition files. Host-based vulnerability assessment tools can also be used by organizations. These tools run locally in VMs and do not require any permission of or coordination with the provider.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Deployment of Pipeline Security

A CI/CD pipeline provides immutable infrastructure. It produces master images of VM's containers and the infrastructure stack. With immutable infrastructure (where fewer manual changes are needed to production environments), extensive logging of infrastructure and application changes (while the changes are across the pipeline), and automating security testing, the CI/CD pipeline improves security. It enables automating active security audits and penetration testing.

The logging feature of CI/CD pipelines allows security teams to easily check and identify changes and the users who are responsible for them. When these pipelines are properly configured, every configuration, code, and infrastructure change can be tracked with the help of logs. Moreover, logs help to trace whoever submitted the change and approved it. Testing results are also included in the logs.

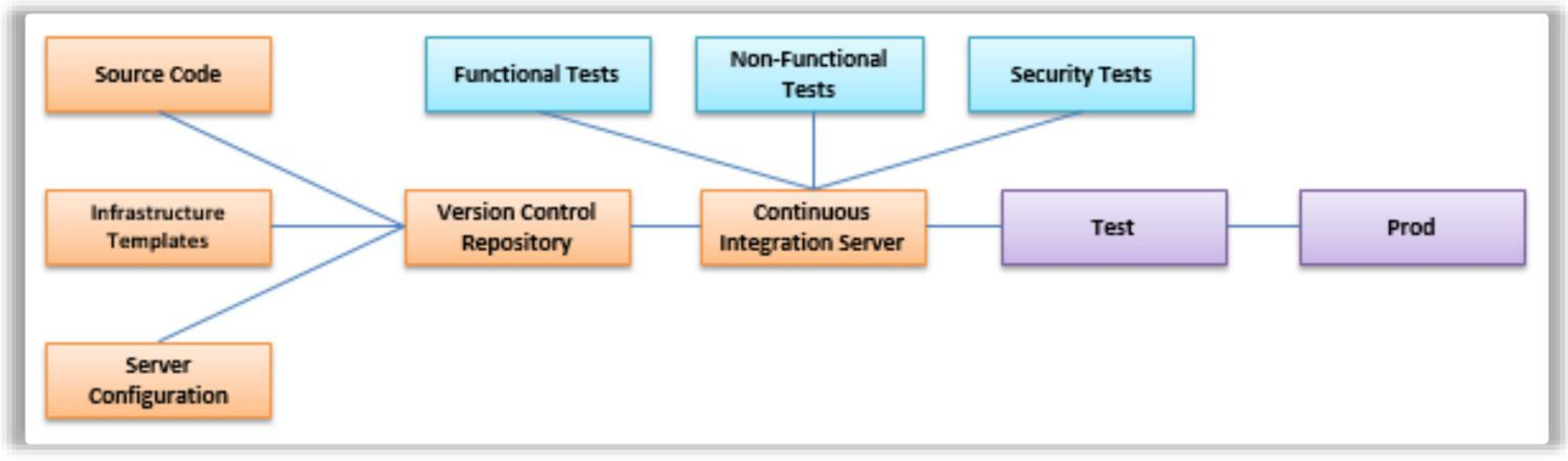


Figure 3.9: Continuous Deployment Pipeline

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

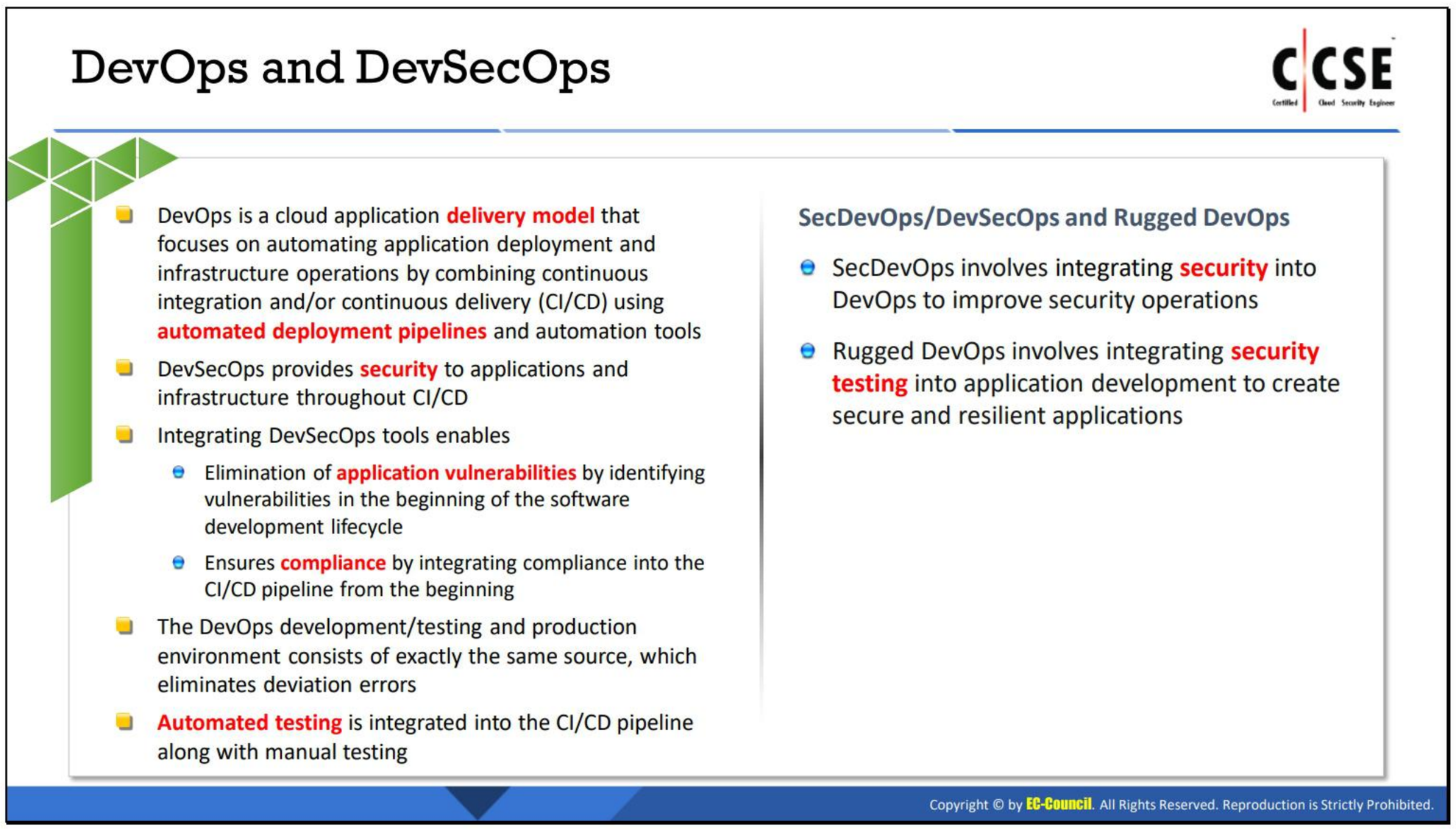
It is essential to tightly secure the pipeline itself. The pipeline can be secured by hosting it in an isolated cloud environment having very limited access to the infrastructure or cloud that hosts the pipeline components.

Securing the Build and Deployment Pipeline

To secure the build and deployment pipeline, implement the following:

- **Use a trusted pipeline**: Always use a trusted, secure pipeline by considering how the pipeline is managed and administered. If the security of the pipeline is compromised, trust cannot be asserted in code that is to be built and deployed through it.
- **Peer review code before the deployment**: Peer review code servers as a quality control measure that must be followed before the pipeline deployment. It is necessary to use technical controls to secure it from being bypassed.
- **Control how deployments are triggered**: Carefully manage the code that triggers automated deployment to production environments. Ensure that untrusted code repositories or branches are not used to make production deployments.
- **Run automatic testing as part of the deployment process**: Automate testing wherever possible to support the deployment pipeline. Never ignore tests that fail and re-evaluate testing that does not work.
- **Manage credentials and secrets carefully**: Secret keys or tokens are required by the deployment pipeline to launch and run code. Manage credentials and secrets carefully to prevent them from being exposed. Inadvertently exposed credentials can allow unauthorized access to systems. Additionally, consider rotating keys and ensure that this process is automated.
- **Ensure deployment pipeline controls cannot be bypassed**: Implement security controls like cryptographic signing and verification at every stage from development through to deployment processes. This will ensure that these controls cannot be bypassed.
- **Scan Infrastructure-as-Code (IaC) templates**: IaC templates (e.g., Azure Resource Manager and Amazon CloudFormation) are commonly used by DevOps teams along with automation to quickly deploy, manage, and tear down infrastructure. Using templates that contain misconfigurations to deploy infrastructure can lead to breaches and exploits. Scanning these templates before the infrastructure deployment will significantly reduce the chances of security incidents in the runtime environment.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DevOps and DevSecOps

DevOps

DevOps literally is a combination of two terms: development and operations. Development here refers to software development, whereas operations refer to information technology operations. DevOps is a cloud application delivery model that focuses on automating application deployment and infrastructure operations by combining CI/CD using automated deployment pipelines and automation tools. The main goal of DevOps is to establish closer collaboration between administrators and programmers in the software development process to facilitate faster software delivery.

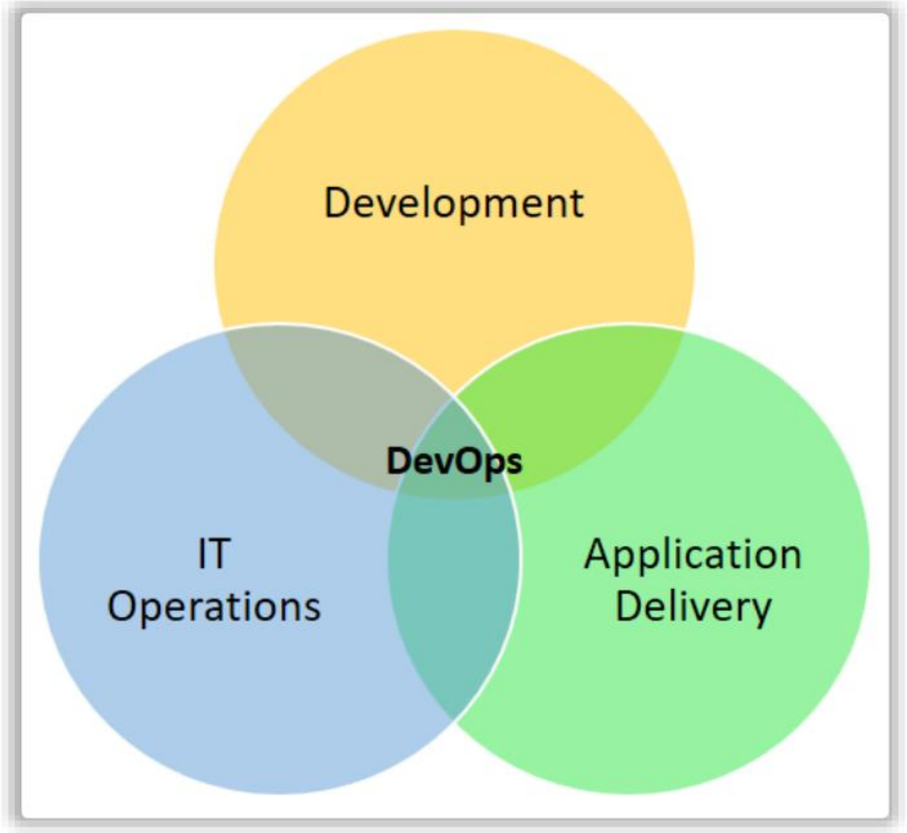


FIGURE 3.10: DevOps

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

By applying DevOps throughout the development pipeline, developers can gain control over the production infrastructure. This helps them achieve faster software delivery as they can prioritize software delivery over other goals. A DevOps engineer works on the intersection of these fields (development and operations) with the primary objective of taking the efficiency, predictability, and security of software development to the optimum level possible.

DevOps includes the following:

- Continuous integration (where processes such as coding, integration, building, and testing are performed).
- Continuous delivery (includes continuous integration but emphasizes on product delivery).
- Continuous deployment (tries to automate product deliveries).

DevSecOps

DevSecOps is a combination of three elements: Development, Security, and Operations. It is also known as SecDevOps or DevOpsSec. DevSecOps is a process of integrating security in all SDLC processes right from the beginning till the end. It places security at the forefront throughout the software development process. DevSecOps introduces various security measures such as code analysis, vulnerability assessment, compliance monitoring, etc. in the DevOps ecosystem.

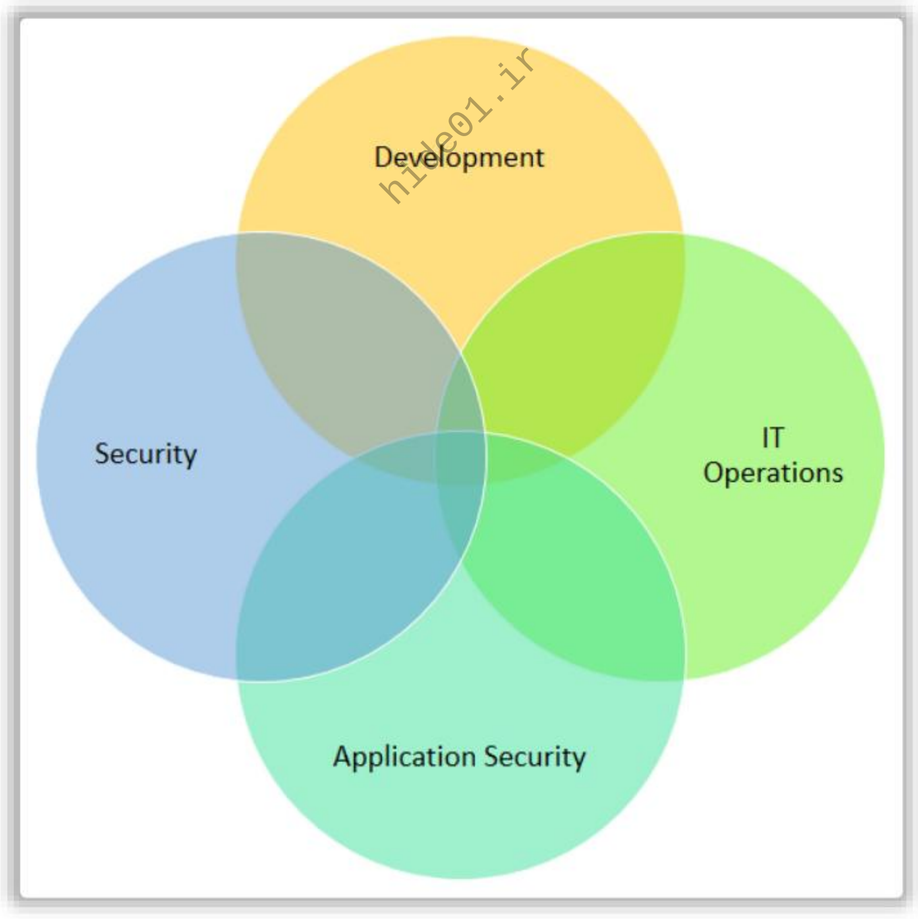


FIGURE 3.11: DevSecOps

DevSecOps provides security to applications and infrastructure throughout the CI/CD pipeline. Like DevOps, DevSecOps also depends on automation to a great extent. DevSecOps introduces various security techniques from the very start of the SDLC to ensure application security. DevSecOps helps security professionals and developers to strike a healthy balance between security and development speed.

Integrating DevSecOps tools provides the following advantages:

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

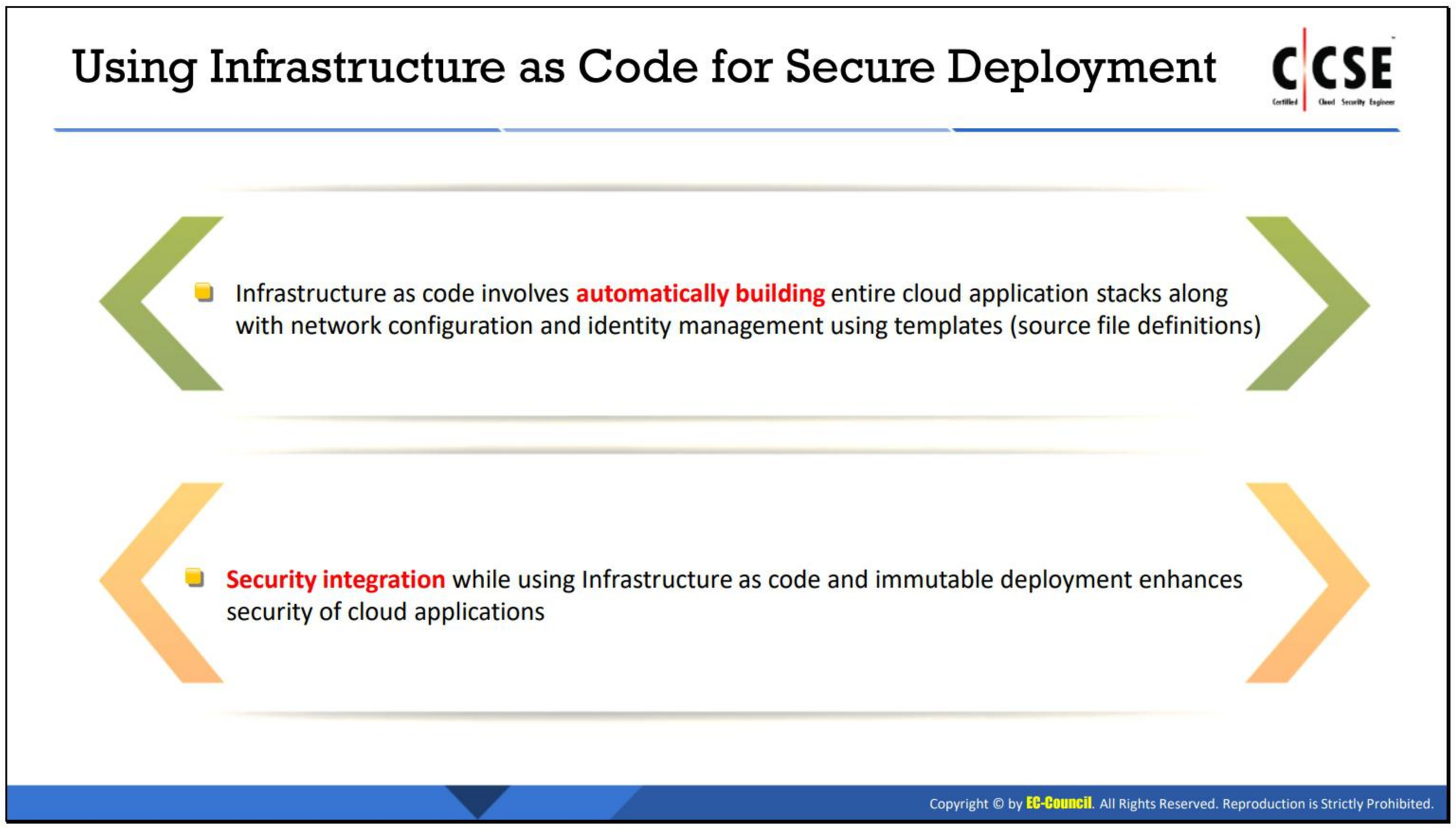
- Eliminate application vulnerabilities by identifying vulnerabilities in the beginning of the software development lifecycle.
- Ensure compliance by integrating compliance into the CI/CD pipeline from the beginning.

DevSecOps and Rugged DevOps

SecDevOps and rugged DevOps describe the integration of security into DevOps. Sometimes, DevSecOps refers to using DevOps automation techniques to improve security operations. The integration of security testing into the app development process to build more secure, harder, and more resilient applications is called rugged DevOps.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Using Infrastructure as Code for Secure Deployment

Infrastructure-as-Code (IaC) includes automatically building the entire cloud application stacks along with network configuration and identity management using templates (source file definitions). It enables locking down of the production environment. IaC is an important part of DevOps that uses a collection of human-editable files (templates) that define infrastructure resource configurations to provision and manage resources in public clouds.

In cloud computing, a complete environment can be defined using templates. IaC tools translate these templates into API calls that build the environment automatically. For example, a server configuration can be built using a template. IaC tools ingest these templates and then create, modify, or delete resources to keep the cloud infrastructure in compliance with the desired state. These tools are capable of managing the (explicit and implicit) dependencies between resources to ensure the resource creation, updating, and removal are performed logically by considering these resource dependencies.

The environments built using IaC are immutable because they are automatically created from a set of source file definitions. If an environment is automatically built from a template (e.g., CI/CD pipeline), changes made in production will not last and will be overwritten by the following template or code change. Therefore, the production environment can be locked down more tightly than in non-cloud application deployment. This is because a non-cloud application deployment involves configuring the infrastructure manually to a specification. Security integration while using IaC and immutable deployment enhances the security of cloud applications.

IaC offers the following benefits:

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

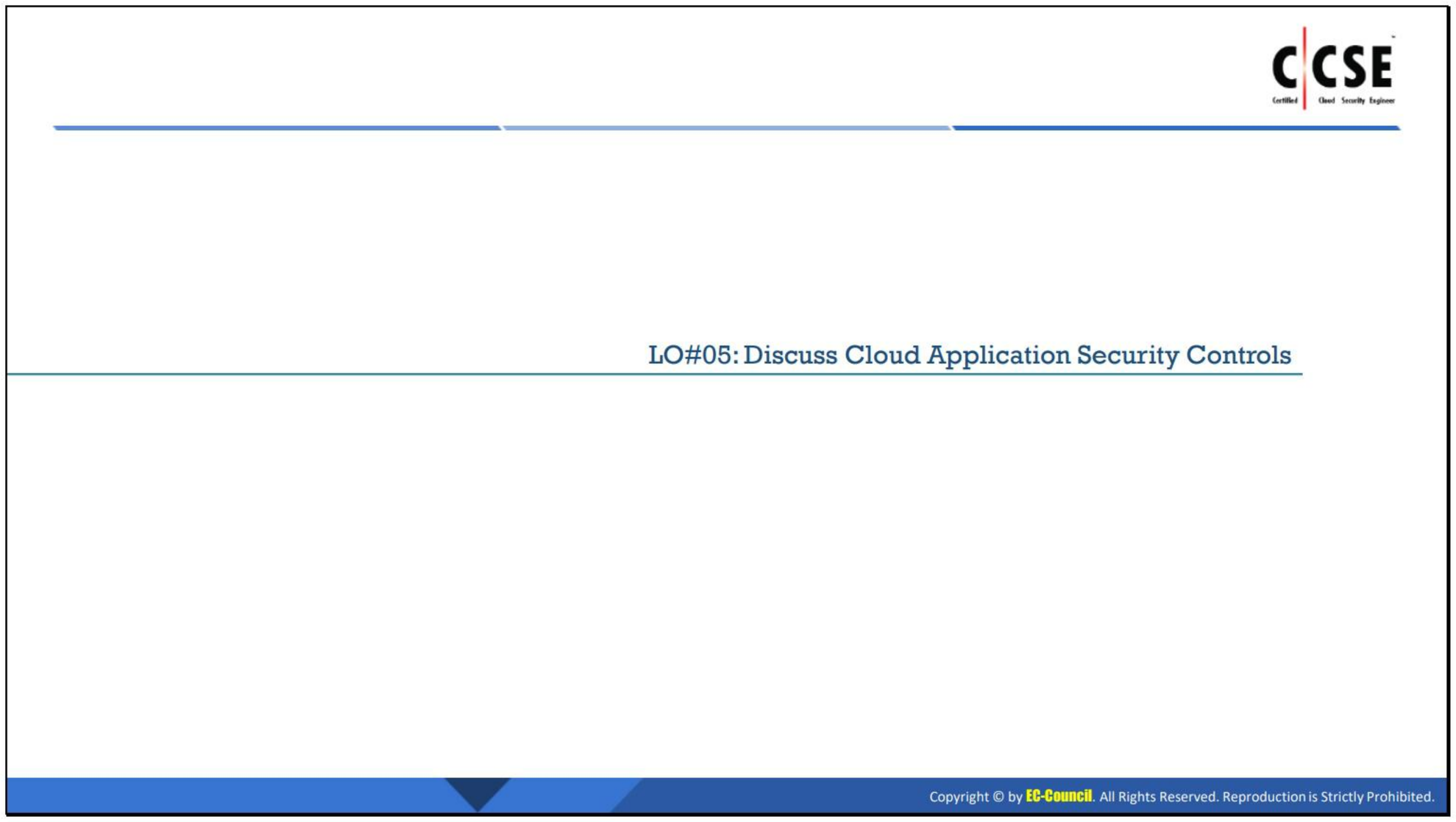
- Allows representing the desired state of an environment using scripts for perfect reproducibility.
- Provides an option to save the scrips in Git. This helps in maintaining a history of the infrastructure.
- Allows the scrips to be treated as documentation.
- Extends the likelihood of continuous deployments to provision and manage resources.

Organizations can use IaC solutions for secure deployments in their cloud environments. Some of the IaC solutions offered by leading CSPs are mentioned below:

- AWS CloudFormation (offered by AWS).
- Azure Resource Manager (offered by Microsoft Azure).
- Cloud Deployment Manager (offered by GCP).

hide01.ir

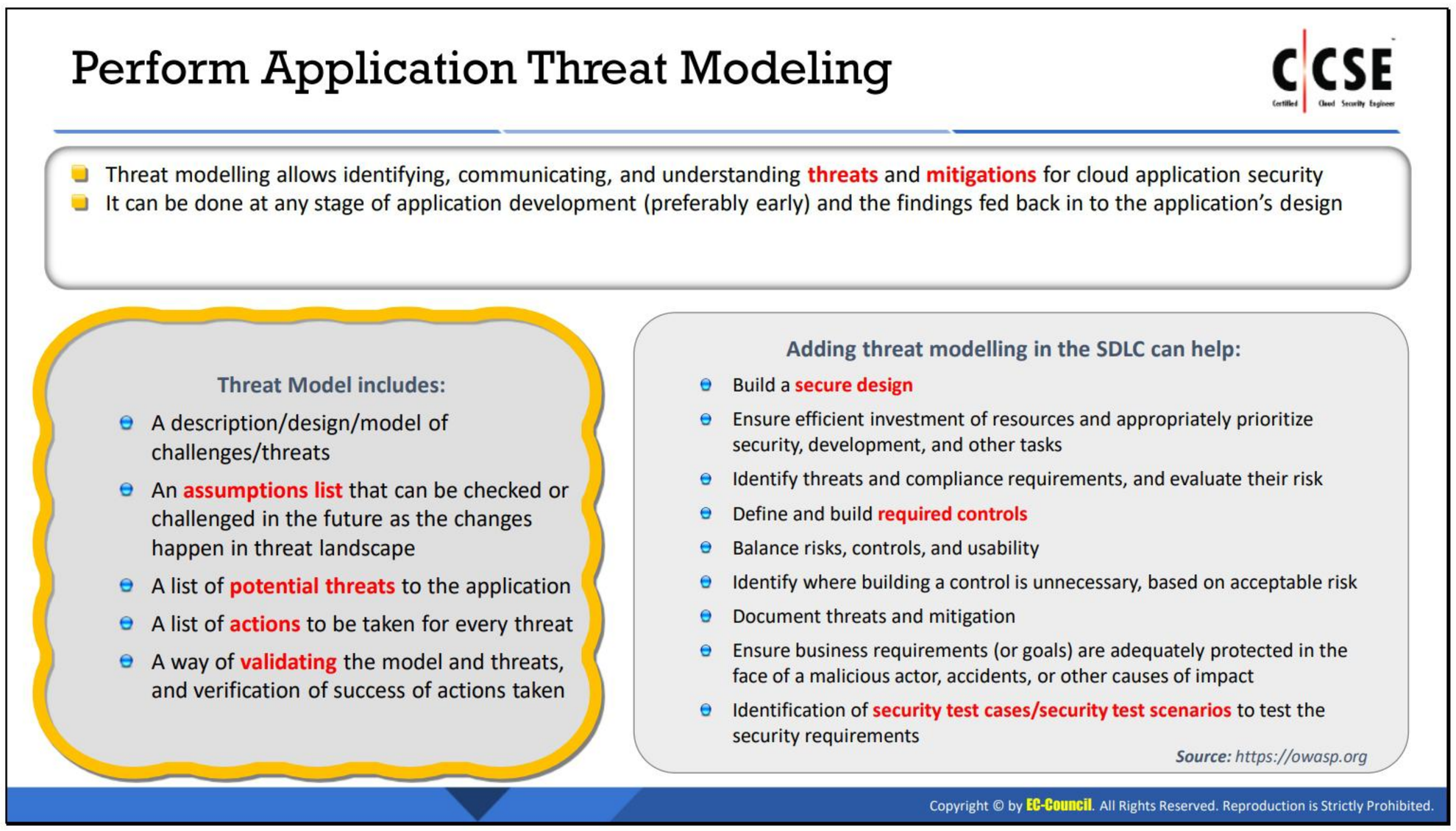
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#05: Cloud Application Security Controls

Securing cloud applications by implementing security at all stages (from development to deployment) is critical to secure them. This section discusses the various practices and tools that can secure cloud applications. The objective of this section is to explain the security controls of cloud applications that can be used for enhancing the security and performance of cloud applications. It also describes application security solutions that can be used for enforcing compliance, governance, and security policies for cloud applications. This section also includes security recommendations for cloud applications, cloud providers, and checklist for cloud application security audit.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Perform Application Threat Modeling

Threat modeling provides the application development team a view on conditions, actions, or behaviors that affect cloud applications and lead to security incidents. Cloud application development should address the identified threats during threat modeling. Additionally, threat modeling enables the development team to prevent the identified threats through secure design, secure coding, secure configuration, secure integration, and security testing practices.

Threat Model Types

A threat model acts as an input to operational security control validation and penetration testing. Threat model is of two types:

- **Simple threat model**: A simple threat model is a list of common programming errors based on the information published by SANS25 and the OWASP Top 10. A simple threat model guides coding, integration, and testing. It is sufficient for application development or running applications on a secure cloud platform.
- **Complex threat model**: Cloud applications that process or store critical data pursue the complex threat model. It involves
  - Identifying the targets of attack. For example, cloud applications, systems, and the other digital assets.
  - Documenting the motivations of bad actors.
  - Documenting the actions that are taken by bad actors to cause risks.
  - Assessing the risks of operational.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

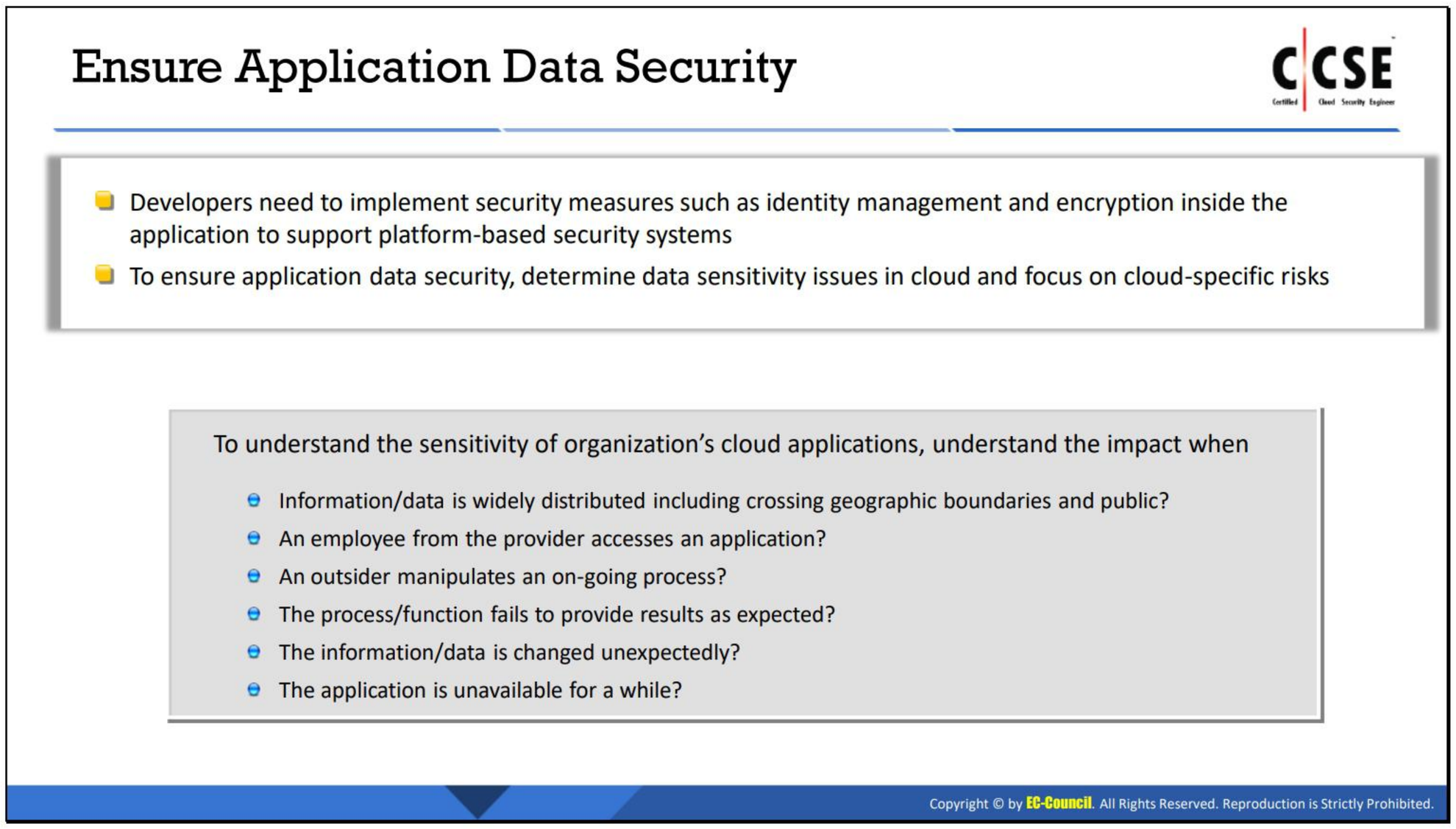
Guidelines for application design, development, and integration are created after cross-referencing the above information with known methods of attack and known software weaknesses.

Use Threat Intelligence Sources

Use multiple threat intelligence sources such as SolarWinds Security Event Manager, ManageEngine Log360, CrowdStrike Falcon X, etc. to identify active and relevant threats to applications. These sources provide an insight into current threats and the methods used for compromising cloud applications and cloud environments. Use this information to keep the required countermeasures in place to prevent breaches, and ensure that the right detection and response processes are in place to limit impact. Continuously monitor cloud applications to understand the changing thread landscape in addition to threat modeling.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Ensure Application Data Security

Determine Data Sensitivity Issues in Cloud/Focus on Cloud-Specific Risks

To determine the sensitivity and importance of applications that are to be deployed in a cloud environment, organizations should ask themselves what the impact would be if

- **Information/data was widely distributed and public, including crossing geographic boundaries?**

  Widely distributed data/information typically needs more effort to protect it. It can be subject to potentially malicious behavior if it is accessed public widely.

- **An employee of the cloud provider accessed the application?**

  Improper cloud service agreement or lack of specificity about the rights of cloud providers to use customer data is a major risk and results in data loss and password theft.

- **The process/function was manipulated by an outsider?**

  Outsider threats include cybercriminals, hackers, or malicious individuals unrelated to the organization, leading to reputation and legal issues. The most frequent outside attacks are ransomware attacks: malware is installed into companies' data on devices containing sensitive information data. The data is then encrypted and access is blocked until the organization pays a certain amount as ransom.

- **The process/function failed to provide the expected result?**

  Failure of cloud services would impact organizations financially though downtime incidents that last for days. Complete failure of cloud could end the businesses permanently and may lead to bankruptcy.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **The information/data was unexpectedly changed?**

  Without sophisticated monitoring and auditing systems, organizations cannot track when sensitive data of an organization is changed, manipulated, deleted, or moved to another location. This may result in reputational damage and legal ramifications.

- **The application or information was unavailable for a period of time?**

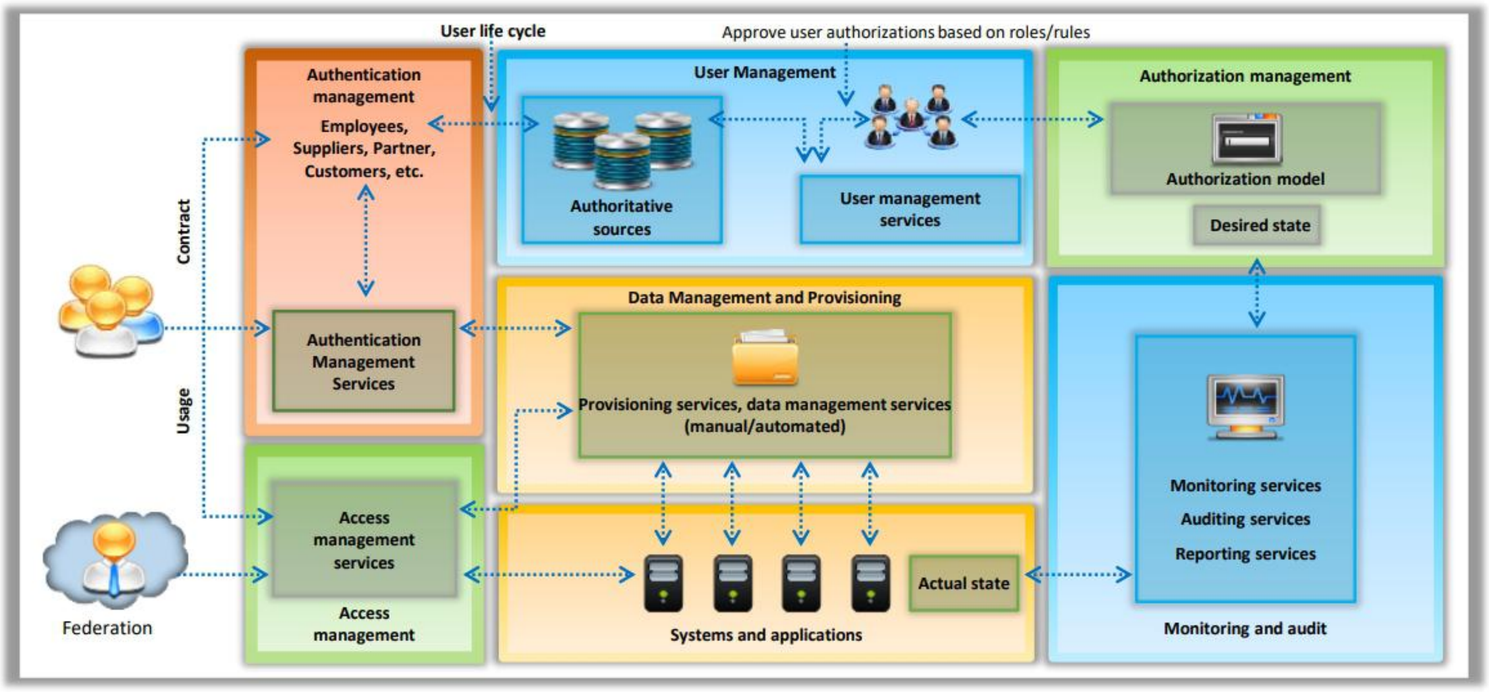
  Unavailability of data could block the delivery of services, which creates a chain reaction that compromises other users' data as well. Therefore, organizations should take steps to ensure availability of data.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Design Appropriate Identity and Access Management (IAM) Solutions

- IAM refers to management of **roles, permissions**, and **access privileges** of users to cloud applications
- IAM can authenticate and authorize a user to provide access to the cloud applications



Cloud Identity and Access Management

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

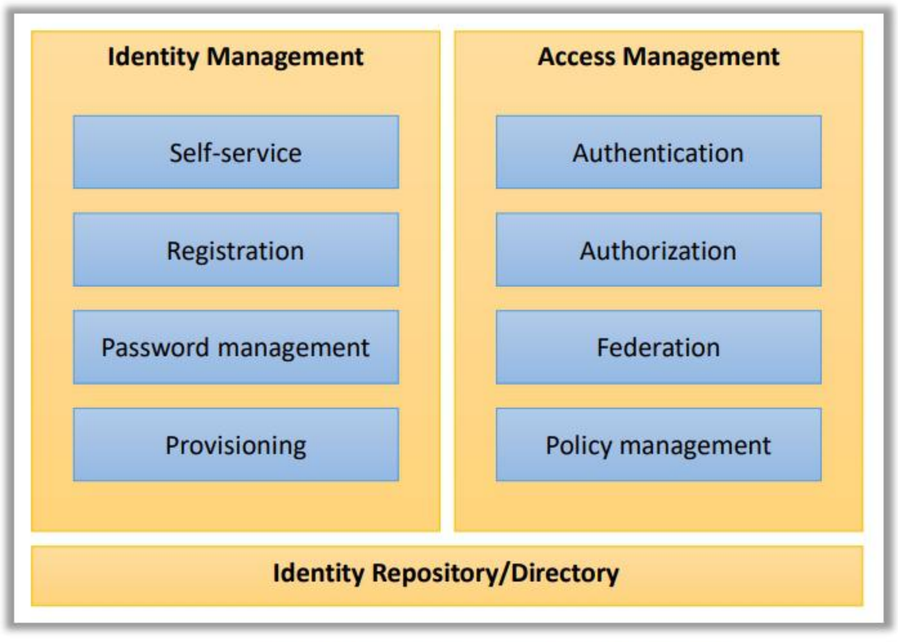
Design Appropriate Identity and Access Management (IAM) Solutions

hi1e01.ir

- An identity and access management (IAM) solution verifies the identity of an entity and allows administrators to manage access to cloud user's applications; it then grants proper access levels to protected applications

- **Identity Management** involves
  - Self-service
  - Registration
  - Password management
  - Provisioning

- **Access Management** involves
  - Authentication
  - Authorization
  - Federation
  - Policy management



Cloud Identity and Access Management

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

Design Appropriate Identity and Access Management (IAM) Solutions

Generally, IAM includes people, processes, and systems. It helps administrators manage access to enterprise cloud applications by verifying the identity of an entity and then granting the correct level of access based on the protected applications.

As part of IAM, an administrator should ensure the following:

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

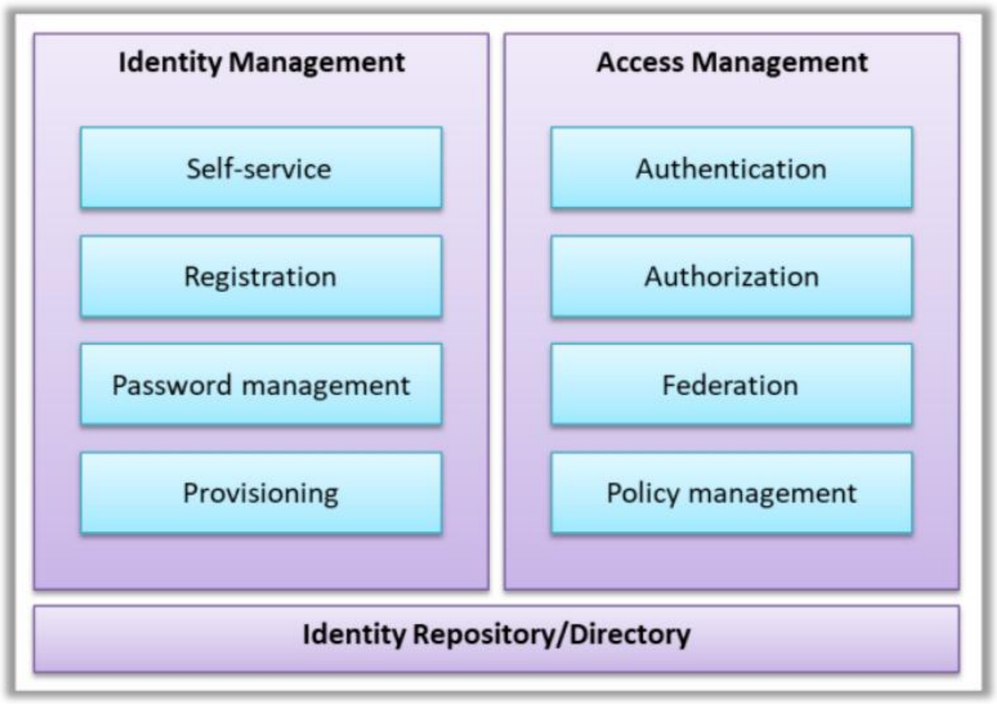


FIGURE 3.12: IAM

Identity Management

Identity management enables identification of users/employees in a system and control of their access to cloud applications within the system by associating the employee's rights and restrictions with the established identity.

As part of identity management, the administrator should focus on the following.

- Self-service
- Registration
- Password management
- Provisioning

hide01.ir

Access Management

Access management involves management of access rights of identities. It includes important decision-making activities related to access rights. Controlling access rights is more important than controlling the number of identities.

IAM is used to grant or deny rights to cloud applications and authenticate users, services, or devices. IAM can be used within an organization or outside of it in a business-to-business relationship or even between a cloud provider and an organization. It has a vast organizational area that deals with identification of cloud entities, objects, and controlling access to cloud applications on the basis of certain predefined policies.

Administrators can effectively handle access managements by using the following controls.

- **Authentication**

  Authentication is the process of verifying and establishing the identity of an entity. It is a function of the identity provider that is established through certain factors such as passwords, biometrics, and key generators. It is often recommended to implement MFA for administrative functions.

  There can be two types of authentication mechanisms:

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

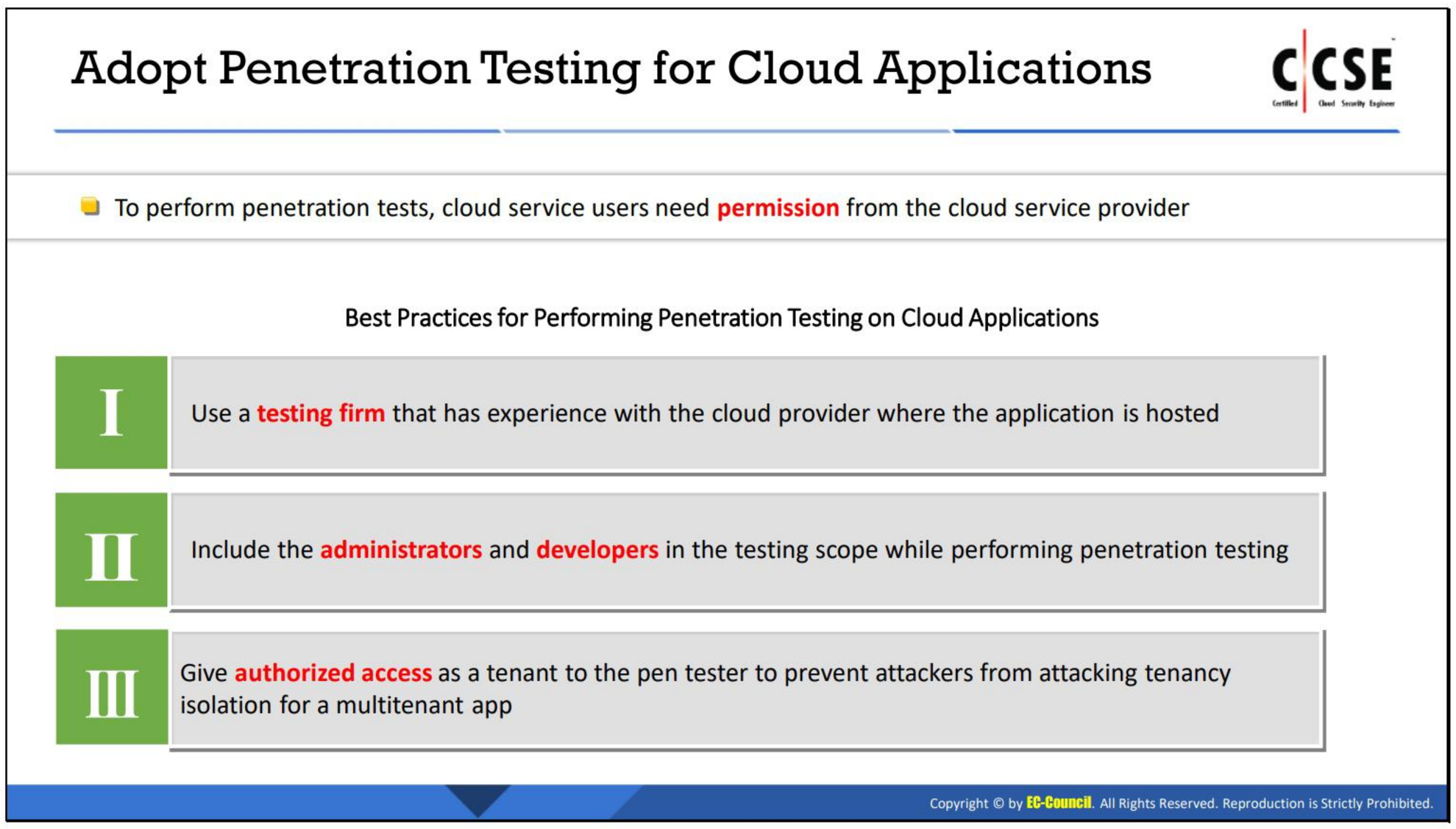
- **Physical security mechanisms**: Implement physical security mechanisms such as access cards and biometrics to protect cloud resources (applications) and facilities from unauthorized user access. As part of data center security, use access cards and biometric authentication methods such as fingerprint recognition, IRIS recognition, face recognition, etc. In addition, implement certain usage and governance policies along with physical security mechanisms to prevent data leakage from insiders.
- **Digital security mechanisms:** Digital security mechanisms include credentials, secure shell keys, MFA, etc.
  - **Credentials**: Use credentials to secure the system from malicious users. The most common mechanisms used to manage access credentials for the cloud environment are Microsoft Active Directory and Lightweight Directory Access Protocol technologies. When credentials are compromised, hackers can manipulate or monitor data in the cloud along with malicious redirects.
  - **Secure shell (SSH) keys**: Use SSH keys to identify the SSH server through challenge-response authentication or cryptography. Use them in performing authentication to the server without passing the password over the network and eliminate the chances of password cracking through brute-force attacks during authentication. SSH keys and static credentials are commonly used for cloud web service authentication.
- **Multi-factor authentication (MFA)**: This includes the use of OTPs, patterns, captchas, etc. as an additional secondary authentication mechanism along with the traditional credential-based authentication. Some of the various types of multi-factor authentication (MFA) mechanisms include
  - **OTP**: One-time-password (OTP) is mainly used to authenticate the user while performing a transaction. The server generates the OTP, which is sent to the user either on his registered email or mobile number. OTP can provide better security when used to authenticate cloud service users who want to access cloud resources or applications.
  - **Captcha**: To secure web applications from programmatically driven malware attacks, captchas are used. A captcha can be an image, a mathematical equation, or an alphanumeric combination.
  - **Patterns**: Patterns are a form of authentication that have different formats. In mobile applications, dotted patterns are widely used, whereas matching image selection is mostly used in web applications.
  - **Security or challenge questions**: Another form of multi-factor authentication is the use of security questions. In this form of authentication, the user is offered a predefined list of security questions that they want to answer. During the authentication process, the login screen displays the security questions so that the user types the answers that they entered previously along with their credentials to login successfully.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Biometric verification**: Biometric authentication methods include fingerprints, iris, facial scans, etc. These methods can be used with traditional password-based authentication to add extra security. Administrators can setup biometric authentication along with credential-based authentication to avoid unauthorized access to cloud resources or apps.
- **Step-up authentication**: It is a form of authentication where the user needs to produce additional forms of authentication to prove his identity. This authentication is usually required when users request access to sensitive data.
- **Out-of-the-band authentication**: This authentication enhances security and prevents hacking or unauthorized access by requiring the user to make a call or send a SMS from their registered number or respond to a call from the concerned authority. This type of authentication is widely used in financial institutions and organizations that have higher security requirements to ensure better security.
- **Push notification**: This type of authentication involves sending a push message to a secure app on the user's mobile phone to confirm the login attempt. This notification is sent to the user to alert them about the authentication attempt. The login attempt will be successful only when the user approves the notification.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



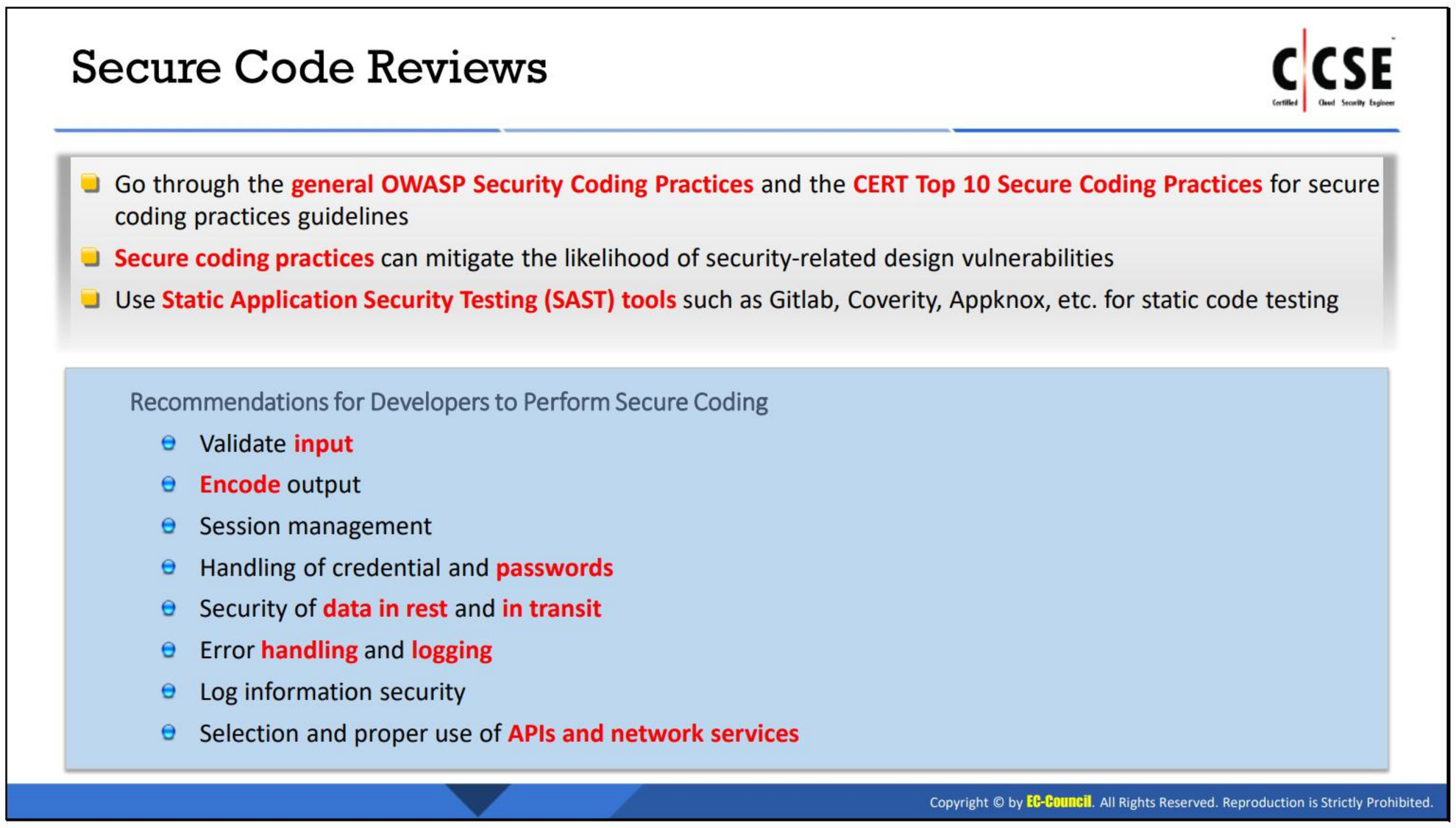
Adopt Penetration Testing for Cloud Applications

To perform penetration tests, cloud service users need permission from the cloud service provider. The following are some of the best practices for performing penetration testing on cloud applications.

hide01.ir

- Use a testing firm who is experienced on the cloud provider where the application is hosted.
- Include administrators and developers in the testing scope while performing penetration testing.
- Give authorized access as a tenant to the pen tester to prevent attackers from attacking tenancy isolation for a multitenant app.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Secure Code Reviews

The main goal of a code review is to detect security flaws in an application related to its design and features along with the root cause. Code review is an effective way that ensures the application is developed such that it can be self-defending in a given environment. Secure code reviews are part of static testing.

hidd91.ir

Secure coding practices can mitigate the likelihood of security-related design vulnerabilities. Application developers should go through the general OWASP Security Coding Practices and the CERT Top 10 Secure Coding Practices for secure coding practices guidelines.

The cloud application developers should perform secure coding using the below design recommendations and prevent harmful programming, insecure software configuration, and application integration errors.

- Validate input
- Encode output
- Session management
- Handling of credential and passwords
- Security of data in rest and in motion
- Error handling and logging
- Log information security
- Selection and proper use of APIs and network services

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

During application development, developers should focus on static code testing throughout application development to identify source code vulnerabilities. For this purpose, developers can use SAST tools such as GitLab, Coverity, Appknox, HCL AppScan, etc to identity weaknesses such as SQL injection and buffer overflows.

Developers should ensure that manual code reviews complement static code testing to ensure comprehensive vulnerability analysis.

As an enhancement to the standard code review process, a secure code review is introduced where security considerations such as company security standards are kept at the forefront while making decisions. Secure code review includes the process of examining or auditing an application's source code to verify that proper security and logical controls are in place, that they work as expected, and that they are used/invoked in the right places. A secure code review can identify potential security vulnerabilities in cloud applications by reviewing or examining their application code. It not only helps identify and fix vulnerabilities introduced into the application during the planning and development phase but also improves the overall quality of the cloud application and skills of the developer.

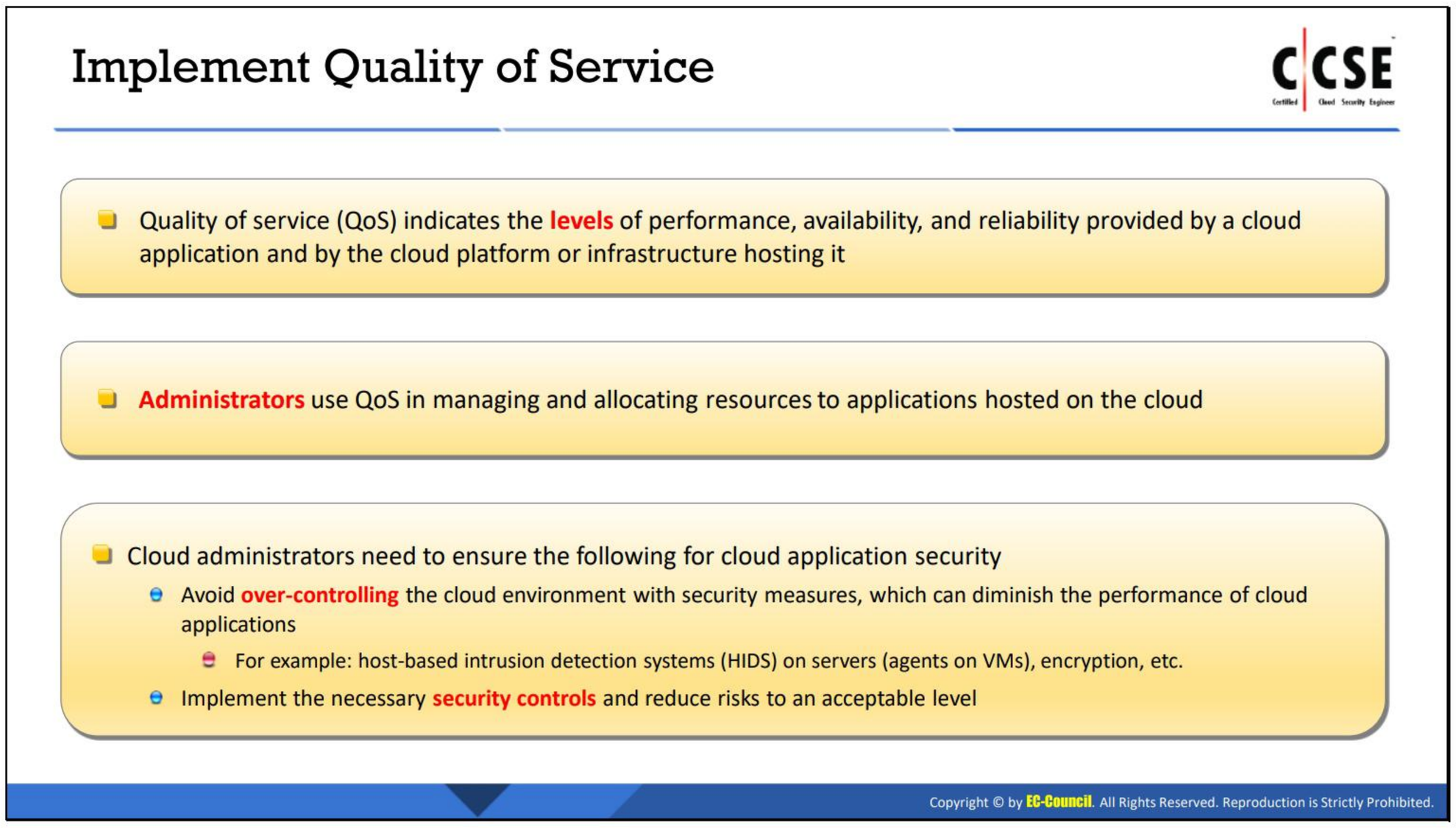
An organization can use a secure code review to ensure that its application developers are following secure application development techniques. A proper secure code review will eliminate most vulnerabilities in the application source code. All secure code reviews involve both the human effort and technology support. Application security tools such as SAST tools can be used for secure code reviews but still human verification is required. These tools do not understand context, which is an essential part of a secure code review.

Cloud application security tools can assess large amounts of code and can identify possible security issues but it is essential that a person verifies each result to determine whether it is a real security issue, whether it is exploitable, and to estimate the risk to the organization. Moreover, human reviewers are necessary for filling the blind spots that automated security tools cannot see.

Secure code reviews can take various forms such as walkthrough and formal inspection.

- **Code walkthrough:** It is an informal process of reviewing an application code. It is a form of software peer review where the code developer leads the development team members and other interested parties through an application or software and people participating in the review ask questions and make comments about possible security issues/errors, violation of development standards, etc. The objective of having a code walkthrough is to provide assurance about the fitness of the application code and occasionally to evaluate the competence/output of a team. Code walkthroughs can be conducted at any time during the project.
- **Formal inspection:** It is an organized review or formal evaluation exercise that involves finding defects in the code, design, and specifications of an application. Such reviews are planned and controlled by a moderator. In the review meeting, the errors identified by QA analysts or the developers are discussed and documented in the formal review report.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Implement Quality of Service

Quality of Service (QoS) indicates the levels of performance, availability, and reliability provided by a cloud application and by the cloud platform or infrastructure hosting it. QoS is critical for both cloud users and providers.

hide01.ir

Network performance is an element that has a direct impact on its users and providers. QoS represents the ability of a network to achieve or utilize maximum bandwidth and manage other network elements such as error rate, latency, and uptime. It includes the management of network resources by assigning priorities to a particular type of data such as files, audios, and videos.

Administrators use QoS in managing and allocating cloud resources to applications hosted on the cloud. Cloud administrators need to implement QoS to ensure a service level along dimensions such as reliability, performance, and availability. It is very important to consider QoS while developing a cloud application (software). Administrators can use techniques such as scheduling, admission control, and dynamic resource provisioning to provide QoS to cloud applications.

Cloud administrators need to ensure that the following two points are implemented:

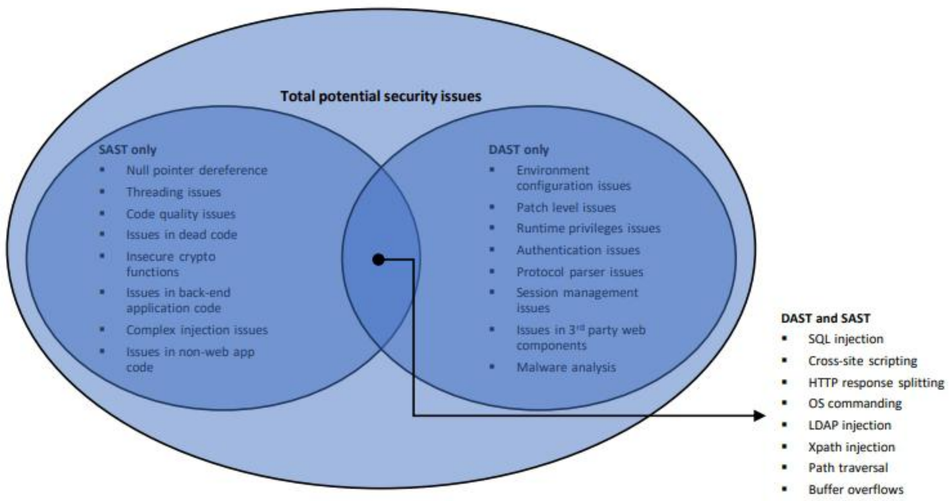
- Avoid over-controlling the cloud environment with security measures that can diminish the performance of cloud applications. For example, encryption, host-based intrusion detection systems on servers (agents on VMs), etc. Implement security measures in a way that does not interrupt or affect the performance of cloud applications.
- Implement the security controls that are required to reduce the risk to acceptable levels. The administrator should ensure that all security controls that are necessary must be implemented to avoid risk or keep it under control.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Application Security Testing

- Security testing helps identify **vulnerabilities** in cloud applications
- OWASP **Application Security Verification Standard** (ASVS) provides the basis for testing application technical security controls to protect against XSS and SQL injection attacks

- Cloud application security testing should focus on
  - **Attack surface review**, in which original and final attack surface of application are compared to identify changes
  - **Fuzz testing/fuzzing**, in which the application code gets checked
  - **Web application scanning**, in which web apps are scanned for identified vulnerabilities
  - **Penetration testing**, in which vulnerabilities are validated and the extent of exposure is identified



Security Issues in Cloud Applications

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

Application Security Testing (Cont'd)

hi0001.ir

- Application security testing in the cloud includes three important areas:

User Interaction

Application testing should include

- Applications' analysis that includes platform, data flow, and logic vulnerabilities
- Vulnerabilities to client attacks that include **XSS attacks**, data leakage, binaries runtime, etc.
- Network attack vulnerabilities that include encryption and traffic analysis

Defensive Coding Practices

- Identify severe issues while performing code review by reviewing the **OWASP Top 9 Coding Security Flaws**

DevOps Security

- DevOps needs **risk analysis** of the security practices of cloud applications
- Document the **DevOps configuration information** of cloud applications

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

Application Security Testing

An effective security testing helps identify vulnerabilities in cloud applications. Go through OWASP ASVS to focus on relevant threats and to ensure that the correct and effective security measures are in place as part of security testing.

Cloud application security testing focuses on the following.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Attack surface review**: Here, the original attack surface identified during application design and the final attack surface identified after finishing code development are compared to identify changes in applications. In an attack surface review, the threat model is updated with the required changes. This information is considered while security testing process.
- **Fuzz testing/fuzzing**: Here, the application code gets tested. The code generally processes the input across trusted boundaries such as file exchange, service interfaces, and network sockets.

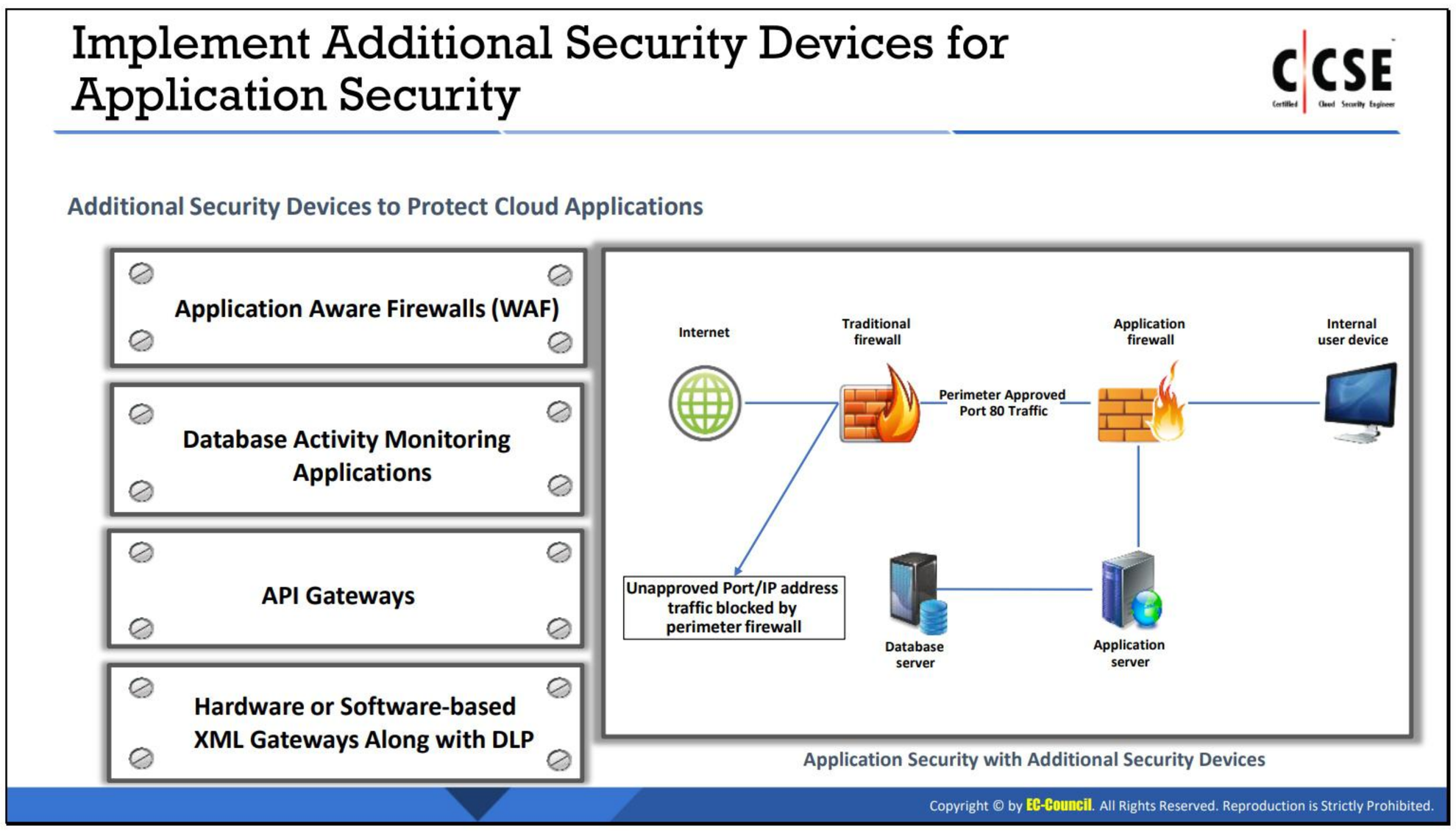
  For testing purposes, fuzz testing methods are used, including black-box testing, beta testing, or any other debugging method that injects invalid or malformed data (fuzz) to identify exploitable privilege level elevation vulnerabilities such as unhandled exceptions, buffer overruns, and other weaknesses.

  Use fuzz testing tools such as Peach Fuzzer, Burp Suite, Webscarab, OWASP WSFuzzer, etc to enhance security testing of cloud applications.

Application security in a cloud environment includes the below three aspects.

- **User interaction**: Application testing in the user interface should include the below points.
  - Applications should be analyzed based on logical data flow and platform to ensure no security breaches are caused.
  - Conduct vulnerability assessments to detect data leakage, data storage, file system, and binary runtime XSS attacks on clients
  - Determine network attack vulnerabilities that include traffic analysis and encryption
- **Defensive coding practices**: Ensure identification of critical security issues during code review by reviewing the OWASP Top 9 Coding Flaws, which includes data validation, authentication, session management, authorization, cryptography, error handling, etc
- **DevOps security**: Application testing in DevOps security should include the below points.
  - DevOps requires risk analysis of cloud application security practices to ensure that DevOps security measures are met.
  - Ensure documenting the DevOps security configuration information for further references.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Implement Additional Security Devices for Application Security

Securing cloud applications by implementing security at all stages (from development to deployment) is critical to secure them. However, having a layered security (consisting of additional security devices) enhances the overall application security by providing defense in depth. These devices limit and monitor traffic and access before reaching actual applications as part of a layered security approach.

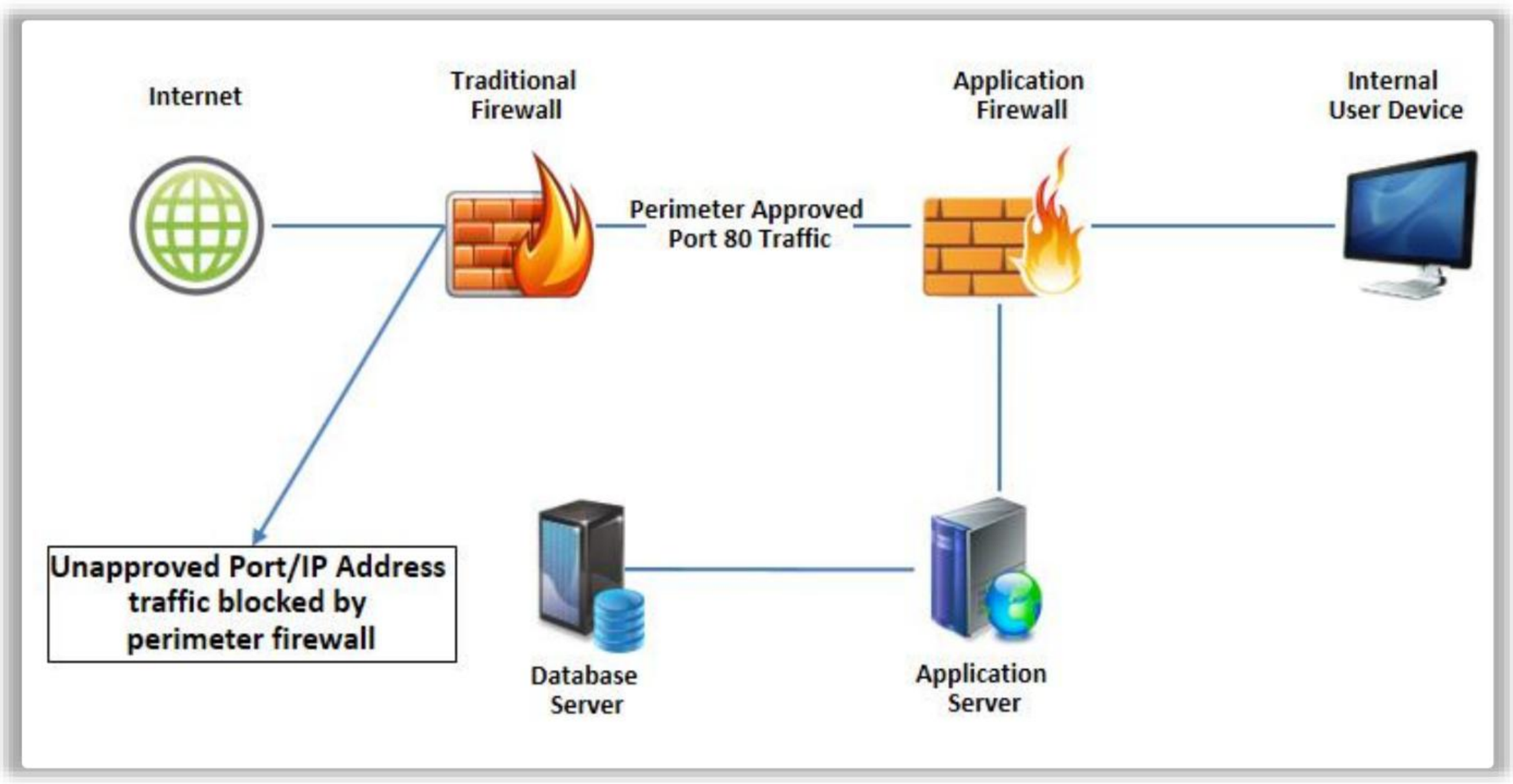


FIGURE 3.13: Cloud Application Security

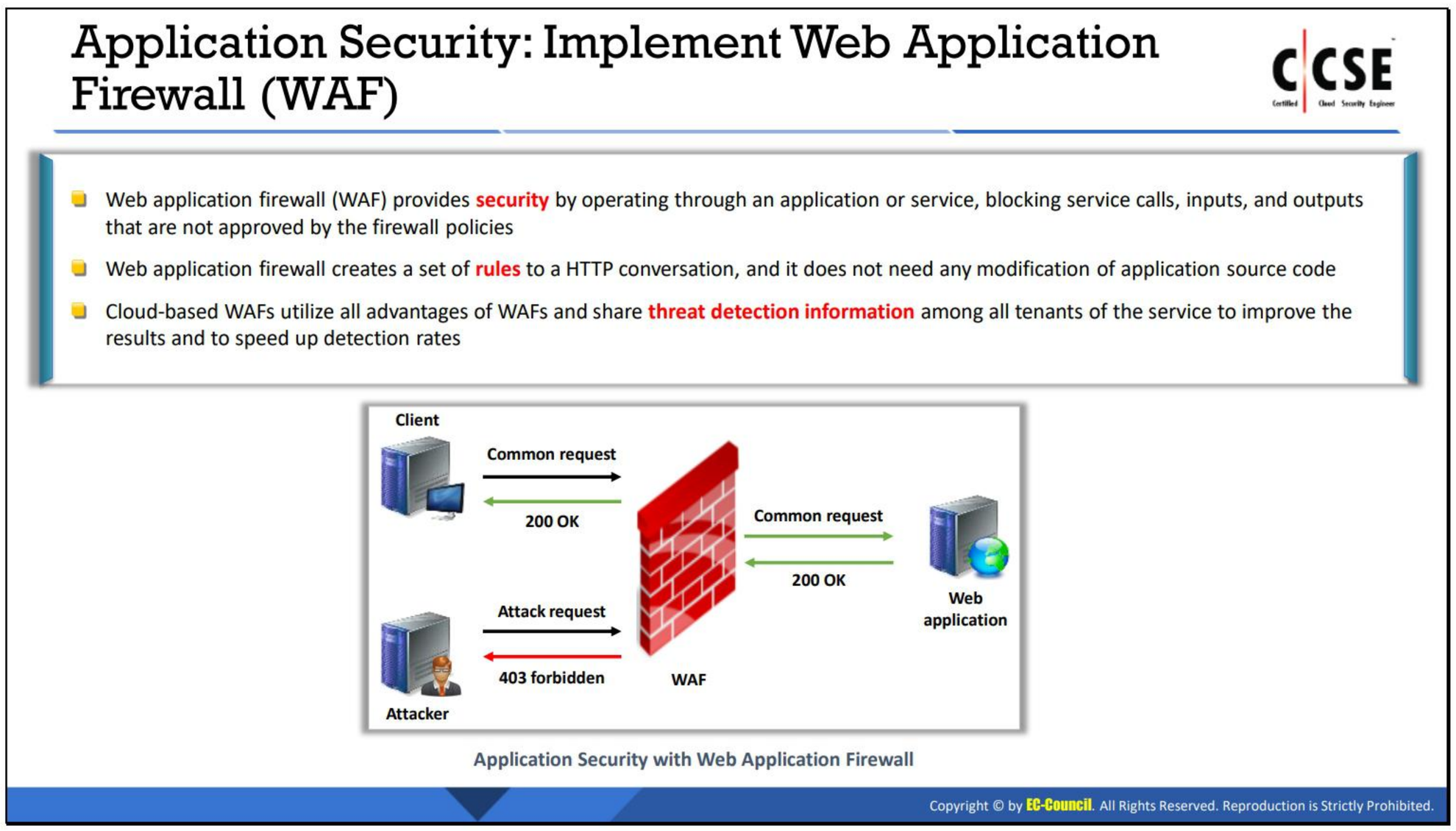
Application security with additional security devices

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud applications must be protected by employing additional security devices such as:

- **Application-aware firewalls (AWFs):** AWFs can inspect application-level messages and protect against various attacks such as XML, API, and other application-level attacks. Most applications are not secured against these types of attacks, which allows attackers to exploit them. AWF provides security at the application level by analyzing and inspecting application traffic to detect threats.
- **Database activity monitoring:** This helps monitor, capture, and record database activities in real-time and send alerts about policy violations. It enables organizations to actively monitor and analyze database activity. All user actions that are performed on the database via a cloud application are logged and can be used for further analysis. Database activity monitoring (DAM) logs can be sent to SIEM systems to perform real-time threat analysis when any security threat happens or is suspected.
- **API gateways**: Application APIs are most vulnerable to attacks and abuse. Building API gateways is critical because they can serve as a single point of entry that manages external user requests. These gateways can stop direct access of users to app services and prevent them from potential attacks. API gateways can integrate with IAM, logging and monitoring, and various other cloud security features to provide enhanced application security.
- **Hardware or software-based XML gateways along with DLP**: XML gateways (or XML firewalls) offer secure cloud applications by inspecting and analyzing SOAP, REST, JSON, and XML traffic to detect any malicious attempts that may compromise the security of cloud apps. They can help apps that are not designed to handle XML assertions and web services traffic that normal cloud apps use. These gateways can be hardware or software-based, and they can be used along with DLP systems to prevent sensitive information disclosure.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Application Security: Implement Web Application Firewall (WAF)

A WAF is designed to offer web security for online apps or services against various malicious attacks such as XSS, SQL injection, butter overflow, etc. WAF technology detects and eliminates potential threats that can degrade, compromise, reveal online applications to DoS attacks. It inspects network traffic before it reaches the application server and prevents unauthorized data transfer from the server.

The main function of a WAF is to provide security by operating through an application or service, thereby blocking service calls, inputs, and outputs that are not approved by the firewall policies. The WAFs provides protection against these vulnerabilities by filtering, monitoring, and blocking malicious traffic (both HTTP/HTTPS) that goes to applications and blocks any unauthorized data that leaves applications.

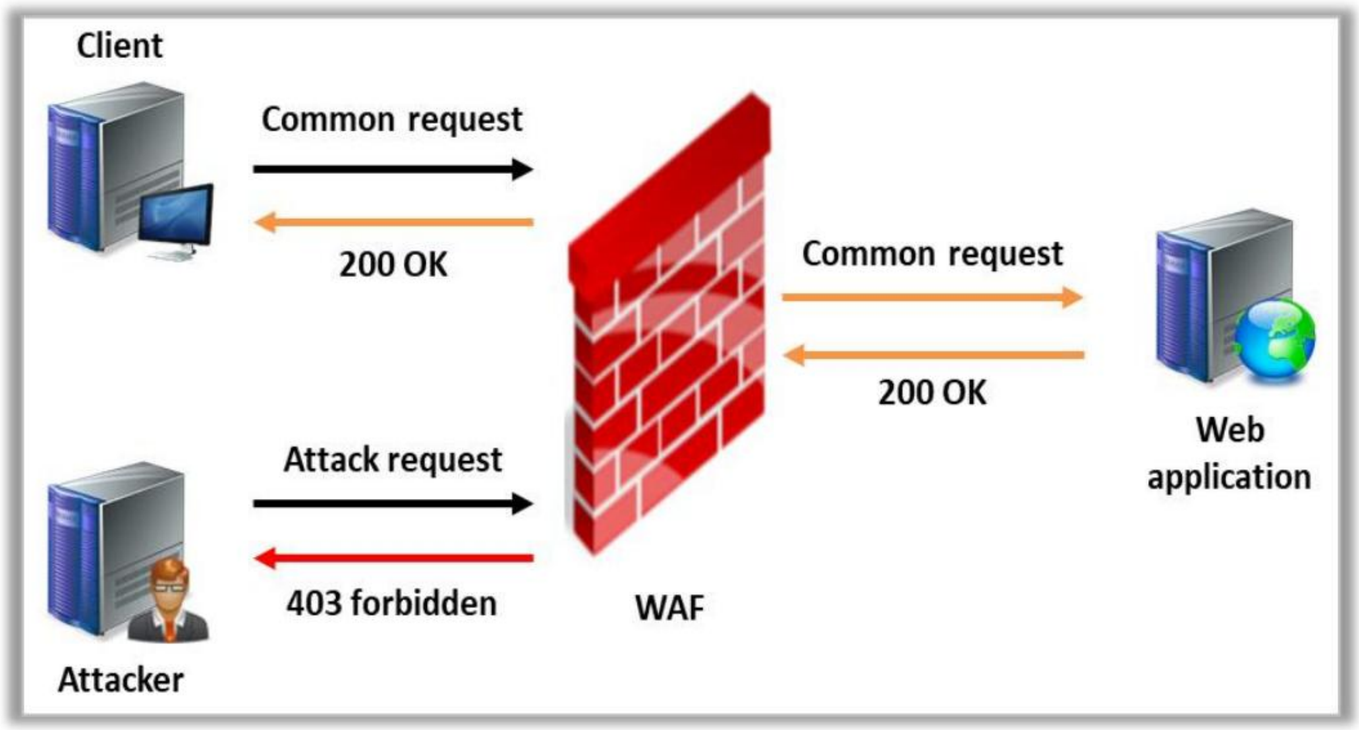


Figure 3.14: Application Security With Web Application Firewall

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

WAF creates a set of rules for an HTTP conversation, and it does not need any modification of application source code. WAF can be configured to work as per a set of policies (WAF policies) that help it to determine what kind of traffic is malicious and should be blocked. These policies can be customized as per requirements. WAF helps in securing web applications without any code modifications.

Cloud-based WAFs serve as a low-cost solution for organizations requiring a ready-made product that needs minimal resources for its implementation and management. These are easy-to-deploy, elastic, scalable, and fast firewalls that are available on the basis of subscription and only require a simple DNS or proxy change to redirect application traffic. To improve the results and speed up detection rates, cloud-based WAFs utilize all advantages of WAFs and share information related to threat detection among all tenants of the service.

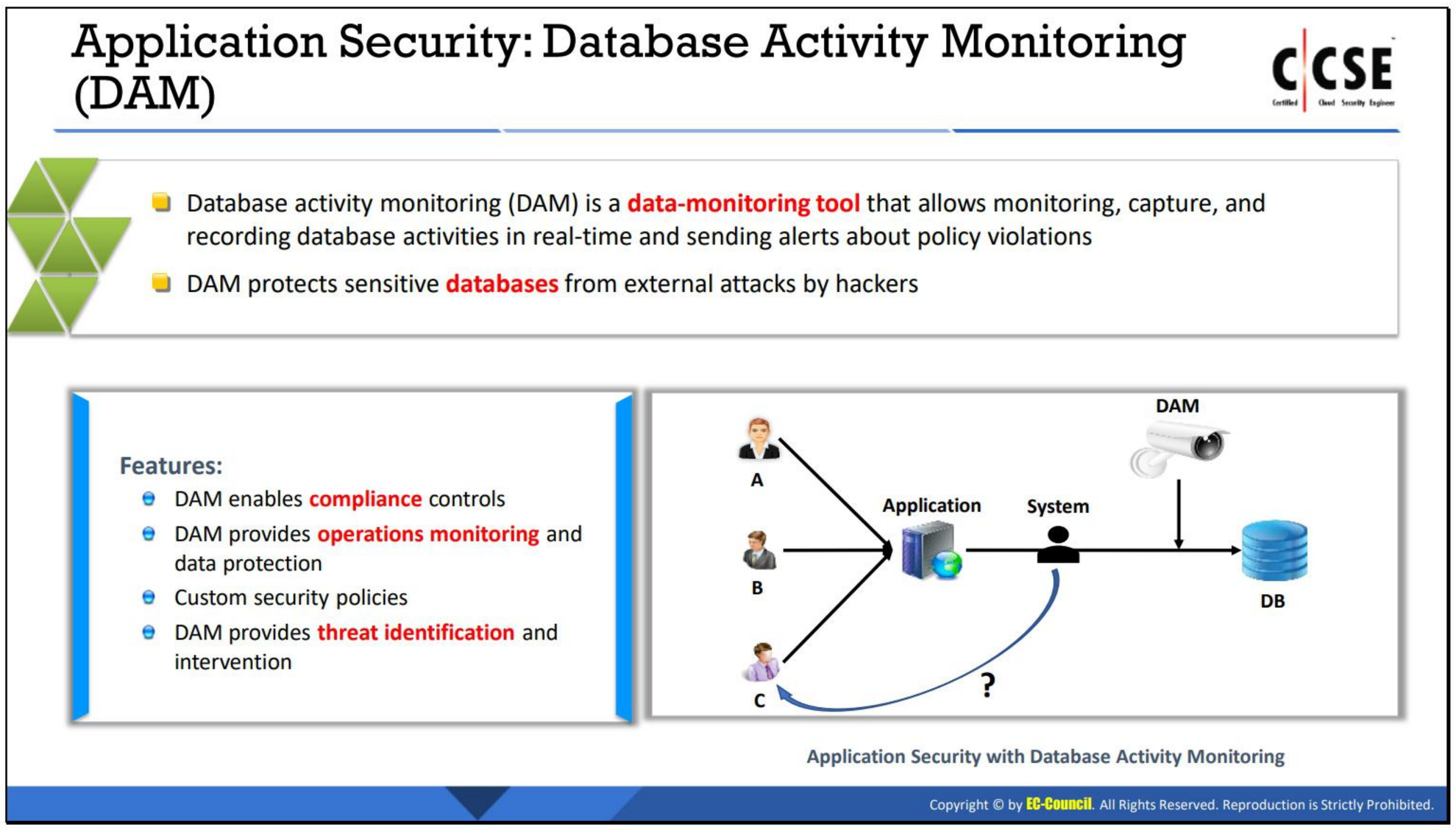
Cloud WAF services provide more elastic, responsive, and customizable security options on the basis of predefined security policies that respond automatically to threats. By customizing cloud-based WAFs as per requirements, cloud administrators can save time spent on manual tuning of security systems, perform proactive threat detection (instead of reactive threat detection), get real-time visibility and insights, and ensure compliance with various regulations as well as provide centralized application security.

Benefits of Using Cloud-based WAFs

Cloud-based WAFs offer the following security benefits:

- Prevent cookie poisoning and identity theft
- Prevent vulnerable component exploits
- Secure apps from XSS and SQL injection attacks
- Prevent sensitive data exposure
- Prevent access to unauthorized/confidential data
- Offer protection against layer 7 DoS attacks
- Prevent web scraping
- Protect applications against unvalidated redirects and forwards
- Secure apps from falsified transactions and broken authentication sessions
- Protect against forged requests to access functionality

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Application Security: Database Activity Monitoring (DAM)

Most databases by default do not provide activity logging. Even if some databases provide activity logs, they cannot help organizations carry out full investigations of historical breaches. The databases that log activity data store the data in a table inside the database itself. If an attacker gets access to database credentials having write access, the attacker can manipulate the activity data present in the table after performing malicious actions to hide the database compromise. That is why the database activity logs available in the database cannot be considered a source of truth. Relying only on the activity logging provided by databases will make many attacks and breaches go unnoticed.

DAM is a data monitoring tool that helps monitor, capture, and record database activities in real-time and send alerts about policy violations. It enables organizations to actively monitor and analyze database activity. A DAM solution offers a comprehensive picture of database activity by combining network-based monitoring data and native audit information. The data collected by the DAM solution can then be utilized to analyze and report on database activity, alert against anomalies, and support breach investigations.

Attackers target databases because they contain the most valuable information of organizations. To avoid loss of financial and critical business data, every database must have continuous monitoring and layered protection. DAM solutions can be used to ensure the security of databases because they are designed to inspect the way applications consume data and database resources to fulfill user requests. DAM protects sensitive databases from external attacks by hackers.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How DAM works?

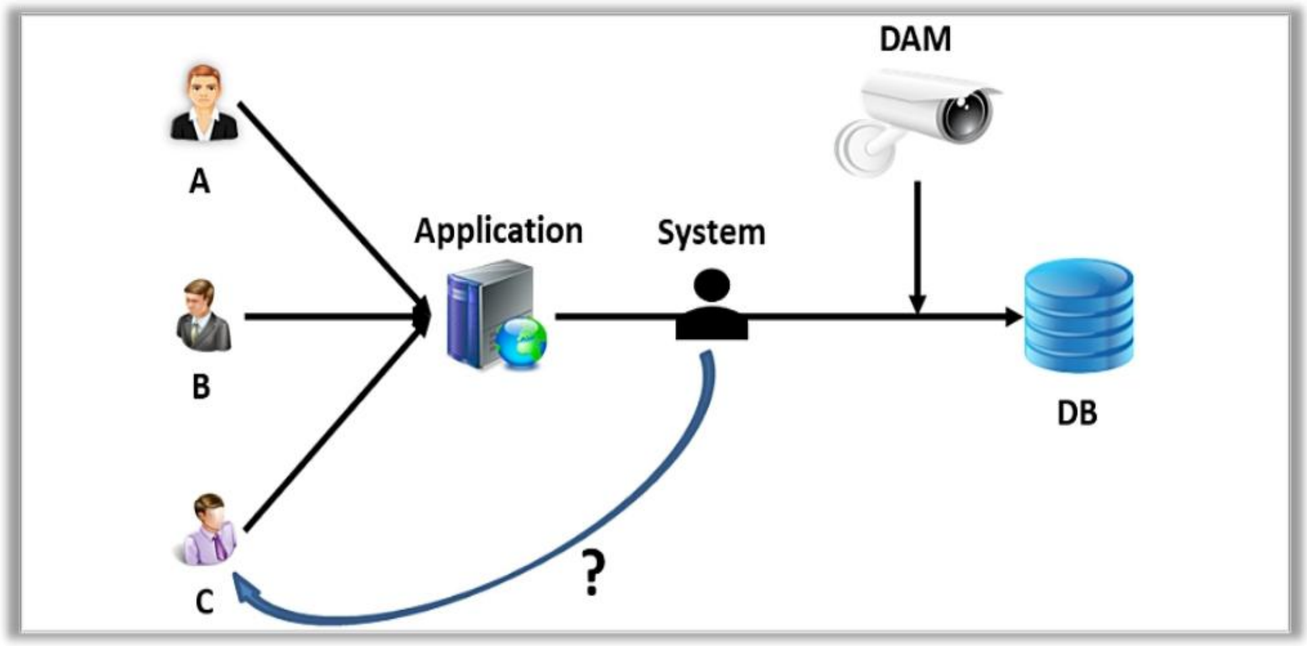


FIGURE 3.15: DAM Working

Organizations can use DAM for capturing and recording their database events in real-time. DAM provides a conceptual understanding of transactions and how several database operations lead to a specific business function. Organizations can keep track of actions their administrators perform such as accessing sensitive data or making unauthorized changes by using DAM because DAM can easily identify suspicious behavior.

Database security monitoring consists of various components, including inventory, auditing, monitoring, configuration, protection, etc. DAM uses all these components to provide both a qualitative and quantitative analysis of events across various apps and databases.

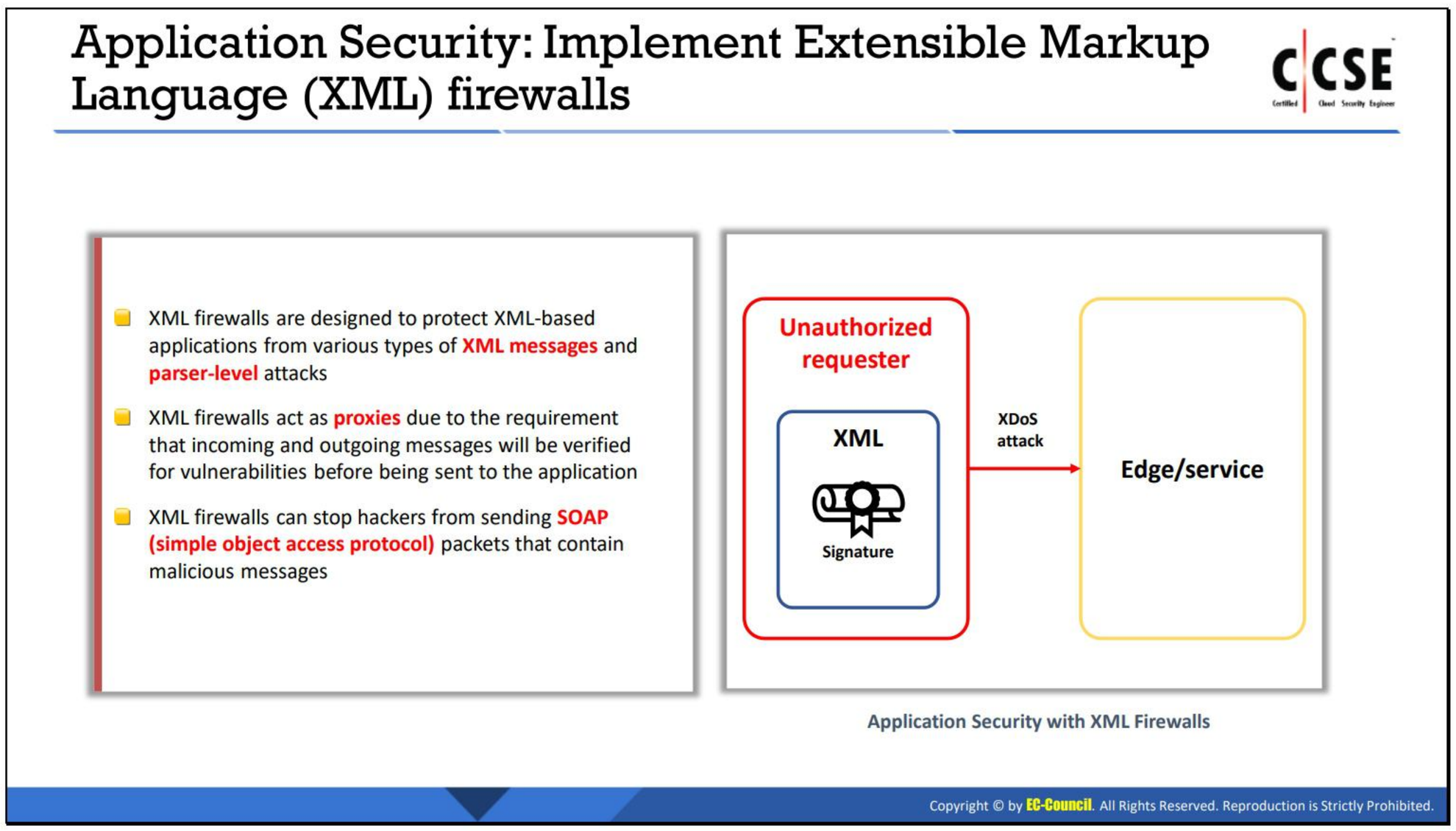
hide01.ir

Features of DAM

Following are the features offered by DAM solutions:

- Enables compliance controls
- Provides operations monitoring and data protection
- Offers custom security policies
- Provides threat identification and intervention
- Offers behavior monitoring
- Provides database activity monitoring and protection
- Provides audit logs for investigations
- Offers regular virtual patching updates for new vulnerabilities
- Supports third-party integration and advanced reporting functionality

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Application Security: Implement Extensible Markup Language (XML) Firewalls

Traditional firewalls have been proved as inadequate to secure certain application services in a cloud environment. Modern attackers use network packets that contain malicious content such as hostile payloads and executables that conventional firewalls are not able to filter out, making applications vulnerable. To secure cloud applications from such threats, advanced application-layer firewalls are required that can deeply scan packets' payload and inspect SOAP, SAML, UDDI, and other web service protocols for attacks.

An XML firewall refers to a specialized device that can protect applications exposed via XML-based interfaces (e.g., REST and WSDL) and examine XML traffic entering and leaving an organization's cloud environment. It is commonly used to validate XML traffic, filter XML content, control access to XML-based resources, and rate limit requests to backend apps that are exposed via XML-based interfaces. XML firewalls are designed to protect XML-based applications from various types of XML messages and parser-level attacks.

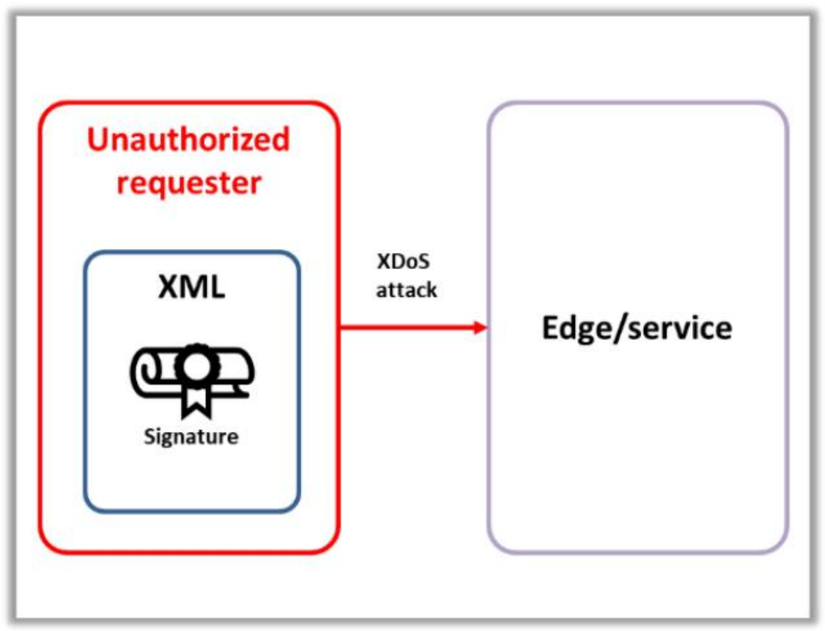


FIGURE 3.16: XML Attack

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

XML firewalls can prevent coercive parsing attacks where a particular format of SOAP messages is sent to the XML parser that results in the depletion of the parser's processing capabilities, making it vulnerable to a DoS attack. XML firewalls can stop hackers from sending SOAP packets that contain malicious messages. The above figure shows an XML DoS (XDoS) attack where a malicious attacker sends a message containing multiple digital signatures and the parser starts examining each signature, which in turn causes the service to slow down under the load.

How does an XML firewall work?

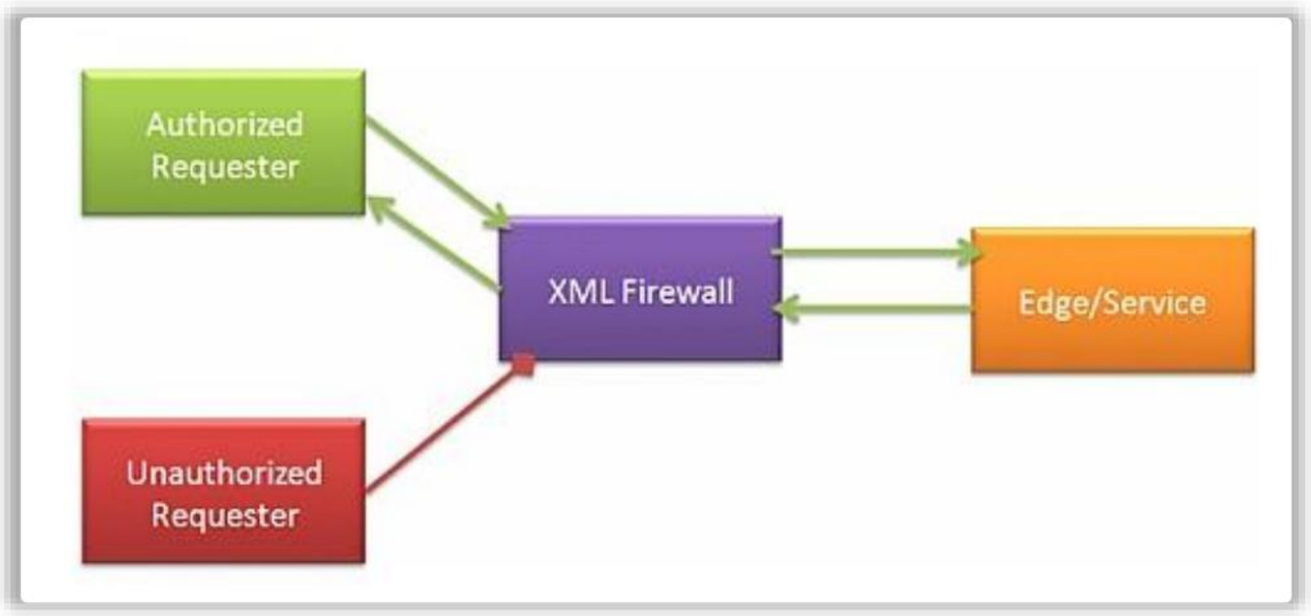


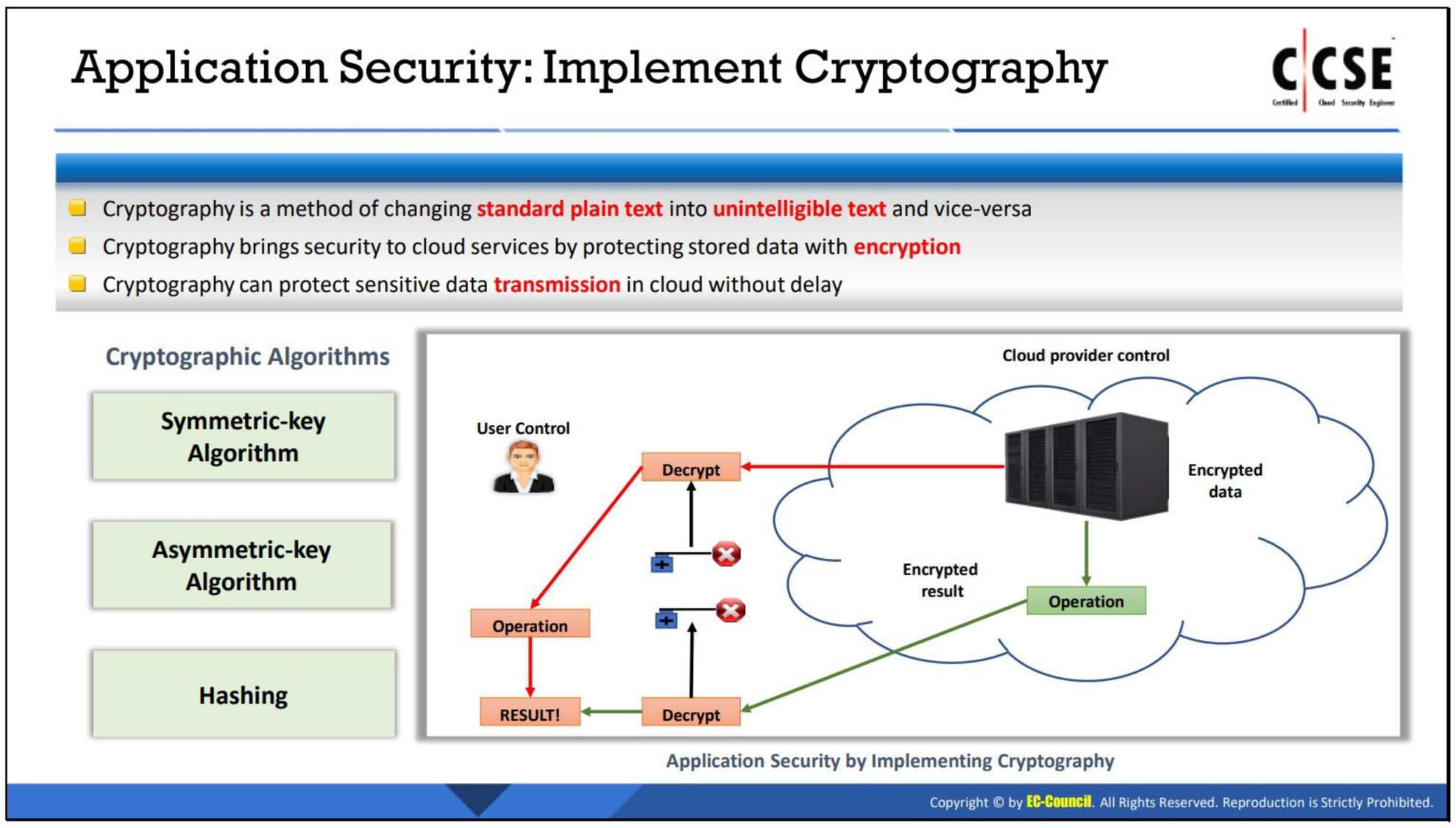
FIGURE 3.17: XML Firewall

An XML firewall acts as the first line of defense for the cloud application service. When the XML firewall receives a request, it checks the request's validity (e.g., it can check whether the XML matches the predefined XSD). It then allows authorized requests to move to the service and rejects unauthorized requests.

The firewall intercepts each message packet and scans it for malicious content (e.g., XDoS or virus attacks). If it is free from any malicious content, it will be forwarded to the application service. The firewall logs the message if it contains something that is malicious and then filters it out or removes the malicious content to forward it. XML firewalls act as proxies due to the requirement that incoming and outgoing messages will be verified for vulnerabilities before being sent to the application.

hid-01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Application Security: Implement Cryptography

Organizations can use cryptography to secure application data stored in the cloud. They can encrypt data before uploading it to the cloud or use cloud capabilities to encrypt it in the cloud environment. Cryptography is used in various digital currencies (e.g., Bitcoin and Ethereum) to verify asset transfer, protect transactions, and control additional unit creation.

It provides the same level of security to cloud services by securing the data stored in the cloud with encryption. Organizations can define cryptographic protocols for their cloud environments to maintain a healthy balance between efficiency and security. Organizations cannot have physical control over their data stored in cloud storage. However, they can secure the data stored in cloud storage by using cryptography and control the cryptographic keys.

Encryption is the application of cryptography and uses an algorithm to encrypt data or communication between applications in the cloud. An organization takes the decision regarding encryption based on the organizational or regulatory requirements to maintain the confidentiality and integrity of critical data.

Encryption can protect an organization's critical data in the following ways.

- **Encryption in transit**: Encryption data in transit can be done using techniques like Transport Layer Security (TLS). It secures communication between two applications using certificate checking and prevents man-in-the-middle (MITM) attacks. If TLS is not feasible, use the other secure options such as SFTP in place of FTP, point to point IPSEC tunnels, etc.
- **Encryption at rest**: Encryption of data at rest needs organizational requirements such as **where the encryption is to be applied** and its **scope**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Where to apply encryption at rest**: Application-level encryption is applied in the application code itself. It has the advantage of providing more fine-grained data protection because the application developer knows exactly which data is critical for organization. The application developer knows the various users, roles, and entitlements, and provides access to applications accordingly. While implementing application-level encryption, use industry standard cryptographic implementations such as data encryption standard (DES), advanced encryption standard (AES), digital signature algorithm (DSA), etc.
- **Scope of encryption**: Application-level encryption should be architected in the early stage of the development cycle. It is required if the architecture of the application requires encryption at rest outside of the data center or on the end-user system, which may cache data locally on the client side. For example, if a cloud application involves accessing a client app, client-side encryption can protect application data.

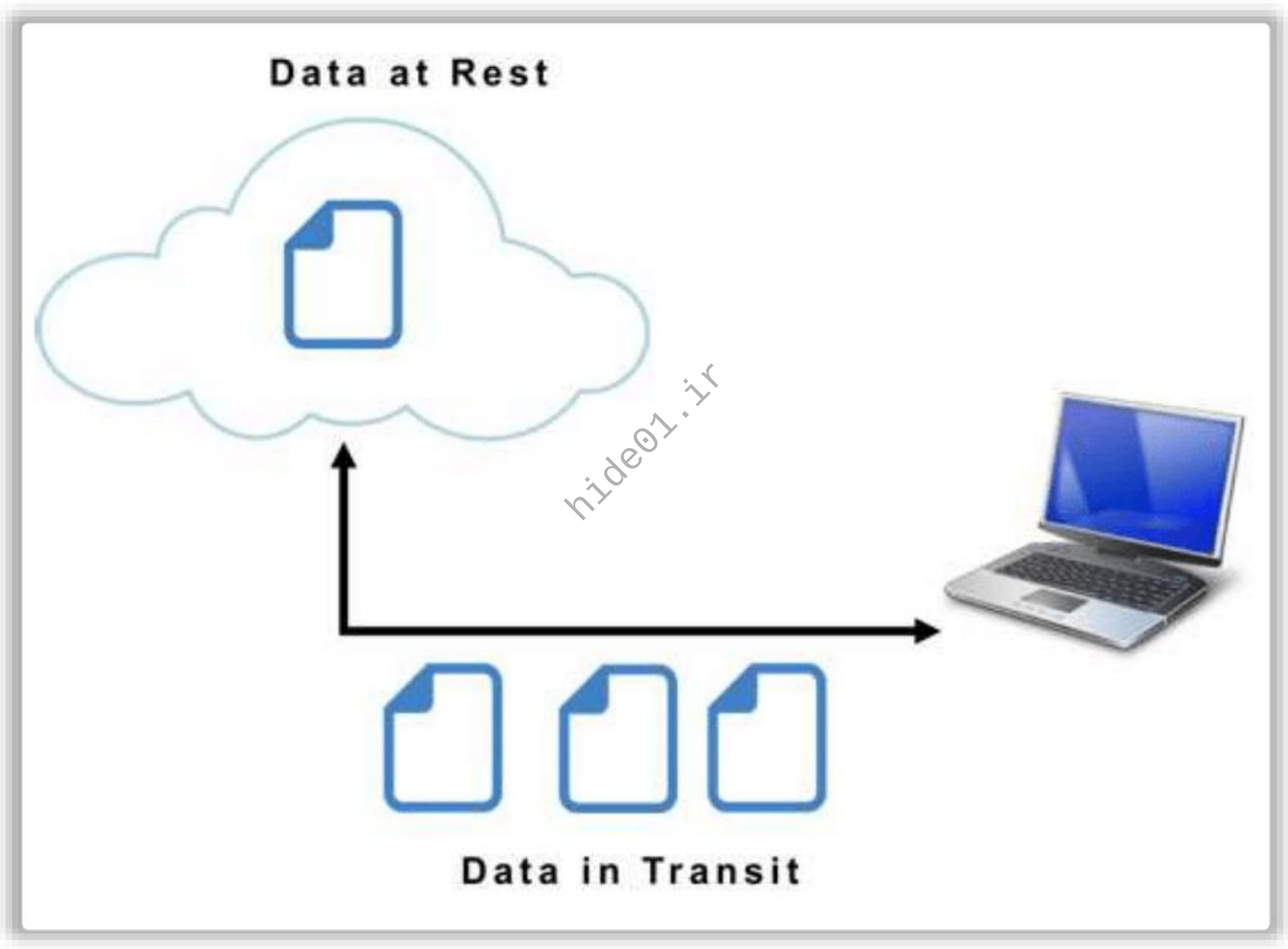


FIGURE 3.18: Application-Level Encryption

Key Management

Key management involves creation, deletion or rotation, secure storage, auditing, and access control of keys. Unprotected keys can make them vulnerable to malicious access. For key management, use key management solutions such as Openstastack's Barbican, Harshicorp's Vault, Amazon Web Service Key Management Service, Azure Key Vault, etc.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Application Security Best Practices

The best practices that can ensure cloud application security and enhance cloud security operations are discussed below.

- **Avoid ignoring due diligence in cloud app selection**: In the case of SaaS applications hosted and accessed in the cloud, it is difficult for information security teams to monitor what access is granted for vendors to their IT system without the right set of cloud security tools in place. Ensure that information security should be involved in helping teams perform their due diligence in identifying and selecting the required safe SaaS app selection. The steps for selecting a safe SaaS app included are
    - **Focus on the design and architecture** of security solutions first and choose the technology later.
    - **Know the source** of the app to know whether it is offered by a credible developer. Ensure that the developer is active in providing updates and patches to the app.
    - **Limit excessive app permission requests**. Check whether the app really needs those permissions for the intended purpose.
    - Check whether the app requires credit card info for **in-app purchases** and it is needed for its intended purpose.
    - Know how the app can handle **authentication and encryption**. Know the method of encryption used for storing and accessing data.
    - Know about **licensing flexibility,** which should include consumption-based billing options. This enables IT teams to deploy the required instances and allows paying for the traffic that is secured through those cloud applications.
- Manage access to cloud applications and user behavior**:**
    - **Integrate cloud-based IAM solutions with enterprise security** from the outset.
    - **Set up MFA and SSO** for access management of cloud applications and user behavior.
    - **Set up user groups** within main applications to manage who needs access and what type of access.
    - **Put a block on IP address locations for logins** to reduce the risk of user account takeover.
    - **Monitor for increase in the number of failed login attempts** to identify attacks on the IT environment.
    - **Monitor for abnormal user behavior** to identify a user account takeover and to detect if information is handled improperly.
    - **Monitor for internal threats** because disgruntled employees may prove to be as harmful as external threat actors.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Malware threat protection and cloud phishing:
    - Ensure that the security teams secure email. **Add a cloud-specific security layer** using platforms such as Google Workspace, Microsoft 365 Cloud Security, etc. for cloud-based email applications to secure cloud infrastructure.
    - **Know security regulations and compliance requirements** to determine the needed encryption type.
- **Automate and remediate cloud application security risks**:

  Use a cloud access security broker (CASB)-based tool to
    - Automate cloud app security risk detection and remediation.
    - Set up DLP rules and policies for automatic detection of
        - Abnormal behavior
        - Improper information use
        - Malware and phishing threats
        - Shadow cloud IT, etc.

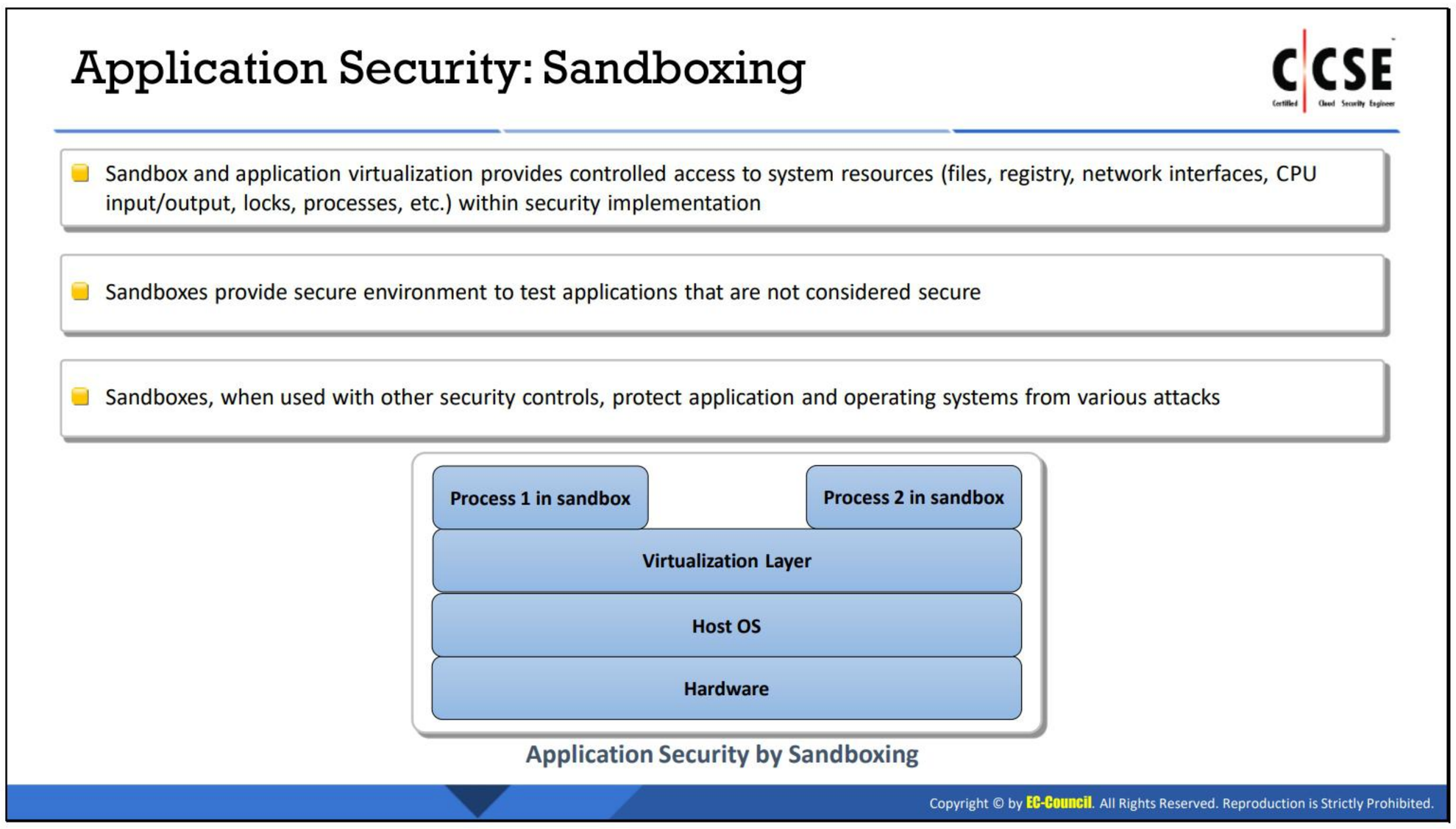
      Here, the CASB remediates automatically based on the selected option (quarantine, delete, revoke access, etc).
- **Audit and optimize**:
    - Ensure consistent auditing of cloud security using a CASB. Set up audit reports to run periodically to identify where new vulnerabilities have emerged, detect unsanctioned apps sneaking back into environment, etc.
    - Monitor the risks and trends timely, helping to optimize the already set up rules and policies and making a CASB work even better timely.
- **Reduce application vulnerabilities**:

  Implement a set of policies for continuous security, continuous vulnerability management, and remediation practices. Ensure these practices are automated and the changes in cloud applications do not open known vulnerabilities.
- **Build security testing into DevOps automation:**

  Validate whether the applications are properly secured and up to the outlined and scripted specifications by building security testing into DevOps automation.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Application Security: Sandboxing

When applications are developed, different types of errors occur, which are fixed after testing and real-life usage. Applications that are not sufficiently tested before launch cause various types of security issues such as OS infected with malware. To ensure that applications remain secure, it is essential to thoroughly test them to rule out any errors and vulnerabilities.

Organizations use sandboxing because of various reasons, including internal policies and regulatory requirements. In cloud computing, sandboxing refers to a protected area that is used for testing untrusted/untested code or application to confirm if the application is working as intended. Sandboxes are isolated, protected areas in memory that do not allow the processes or apps running inside to run outside the environment as well as prevent access of other processes to the sandbox environment. A sandbox can be defined as the software that provides a controlled and monitored environment where no untested/unknown app can damage the environment it is running in as well as no outside program can access or affect the sandbox environment.

Sandboxing provides controlled access to resources by isolating them from one another. With the help of virtualization, VMs can be used as sandbox environments where untested applications can be run and checked for possible improvements. Use sandboxing and application virtualization to provide controlled access to system resources (files, registry, network interfaces, CPU input/output, locks, processes, etc.) within security implementation. Sandboxes provide a secure environment to test applications which are not considered secure. Most developers want to leverage cloud platforms that provide sandboxing for testing apps or code because it helps them avoid security issues later.

Developers can use sandboxes to open suspicious files, run untrusted apps, and download files from URLs without affecting the device they run on. Sandboxes can be used anytime and for any situation to securely examine a file or code that is suspicious or malicious by keeping it isolated

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

from systems and corporate networks. Sandboxing helps organizations and developers categorize applications as “safe” or “unsafe.” Releasing applications without sandboxing them may result in allowing attackers access to the network and data stored on it. Sandboxing can be effectively utilized as a tool to identify malware attacks and stop them before they enter and damage the devices and network. Sandboxes when used with other security controls help protect applications and operating systems from various attacks.

How does Sandboxing Work?

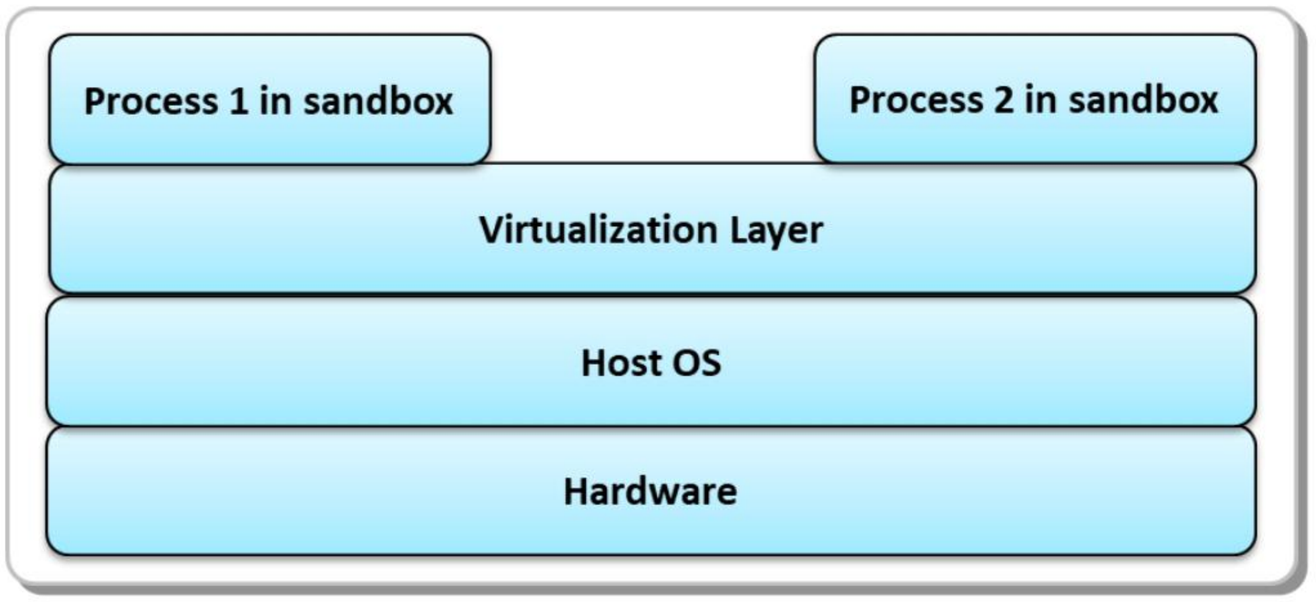


FIGURE 3.19: Sandbox

Various processes can be run securely in sandbox environments (VMs) without affecting the host they are running on. VMs serve as an efficient platform for sandboxing because virtualization offers proper isolation between VMs or a VM and the host environment. Potentially dangerous operations can be executed in VM instances without affecting the host or other VMs operations. This is because VMs are by default fully isolated from one another, and the virtualization layer provides sufficient isolation between VMs and host OS and hardware. It makes sandboxes a secure and safe environment for testing the functioning of apps or processes.

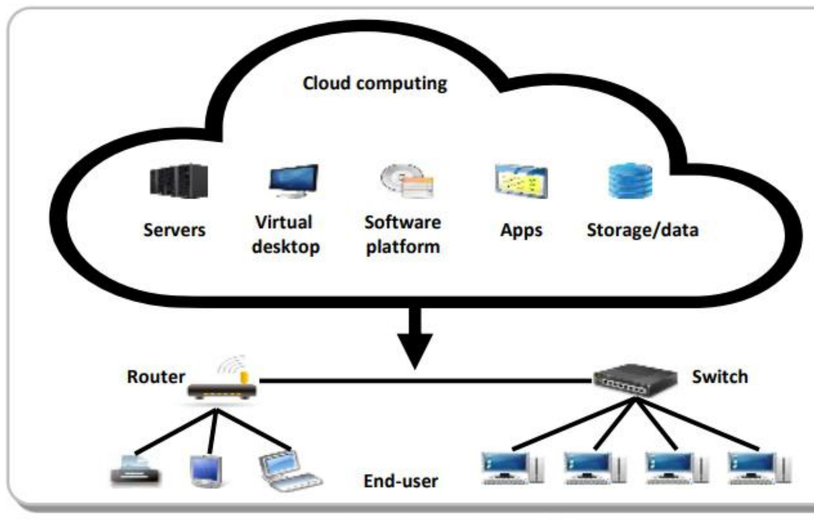
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Application Security: Application Virtualization and orchestration

C|CSE Certified Cloud Security Engineer

Application Virtualization

- Application virtualization is a technology that enables **access** to an application without needing to install it on the target device
- It allows IT administrators to implement **remote applications** on a server inside an organization's data center or via a hosting service
- It provides application management, scalability, and security



Application Virtualization

Application orchestration

- It refers to the process of integrating multiple applications or services to automate a process or perform synchronization in real time
- It provides decoupling of applications from each other, message routing, security transformation, and reliability
- It helps to centrally manage and monitor application integrations

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

Application Security: Application Virtualization and Orchestration

Application virtualization refers to a technology that enables a user to access an application without requiring to download/install it on their device. It encloses the application from the underlying OS on which it is run. Applications that are fully virtualized behave as if they are installed on the device, but they are not. The user can have a seamless experience that is much similar to that of running an application on their device. With application virtualization, the user can perform all functions on virtualized apps that they used to do with traditional apps running on the device.

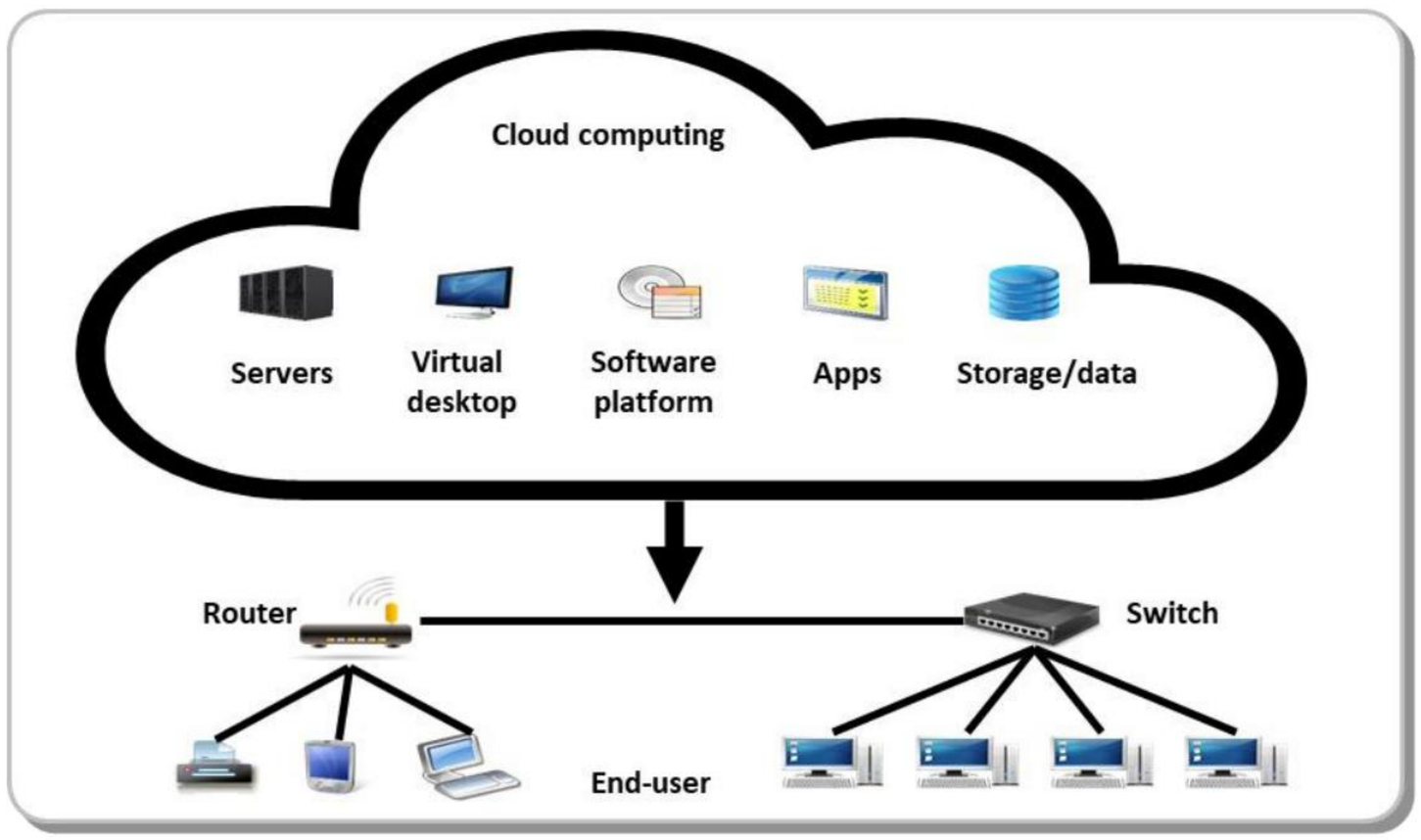


FIGURE 3.20: Application Virtualization

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

It allows IT administrators to implement remote applications on a server within an organization's data center or via a hosting service. Application virtualization makes the maintenance of applications easier where changes can be applied to the applications without the user even noticing them. It is a cost-effective solution that minimizes data transfer, thereby reducing the impact on hardware. Additionally, it offers easier access and authentication management when compared to desktop virtualization where desktops are virtualized and the OS is installed on a remote client (system).

Organizations can use application virtualization and desktop virtualization to centralize the management of the entire desktop environment ecosystem. Application virtualization enables organizations to easily apply updates to applications by patching the application images stored in the data center, unlike applying updates to applications on all endpoints. This helps in applying updates and patches rapidly, easily, and consistently.

How Does Application Virtualization Work?

Applications can be virtualized using a server-based approach where the IT administrator can implement remote apps on a server within the data center of an organization or by using a hosting service. Then, the administrator leverages application virtualization software to deliver the apps to endpoints where users can use them as if they are installed on their devices. The actions taken by the users on the apps are conveyed back to the server for execution.

Benefits of Application Virtualization

Though application virtualization offers multiple benefits, the most important ones are discussed below:

hide01.ir

- **App management**: Application virtualization enables an organization's IT department to easily manage and maintain applications across the organization. They need not install or update apps individually on each user's system. Instead, they can install and manage apps on the central server and deploy the virtualized apps on user devices as required. Additionally, they can save time and effort spent on installation as well as updating and patching.
- **Scalability**: Because the central server hosts applications, users do not have to use powerful computers or devices with high computational power. This helps organizations achieve scalability and saves cost by provisioning thin clients as basic devices to access and use these apps.
- **Security**: With application virtualization, IT administrators can have centralized control over access to applications. They can modify access permissions easily for applications.
- **Simple and easy installation**: Apps can be installed to a server once and can be virtualized to be used on multiple endpoints without reinstalling them on these endpoints.
- **Better portability:** Apps that are virtualized offer better portability as they can be used on any endpoint from anywhere without worrying about the endpoint if they are lost or compromised.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Easier updates**: Updates applied to the application running on the central server will be reflected on all endpoints running its virtualized version.
- **Independence from the OS support**: As the virtualized applications are independent of the OS being used, any endpoint device (e.g., Android, Microsoft, or iOS) can be used to access and use them.
- **Reduced conflicts between apps**: Because applications run on endpoints in their virtualized version, there is no conflict between applications.
- **Easier rollback**: Apps can be reverted to rolled back easily if they do not work as intended.
- **Simplified support:** Helpdesk personnel can easily fix issues with the working of applications from the central location if any issue is detected with virtual applications.

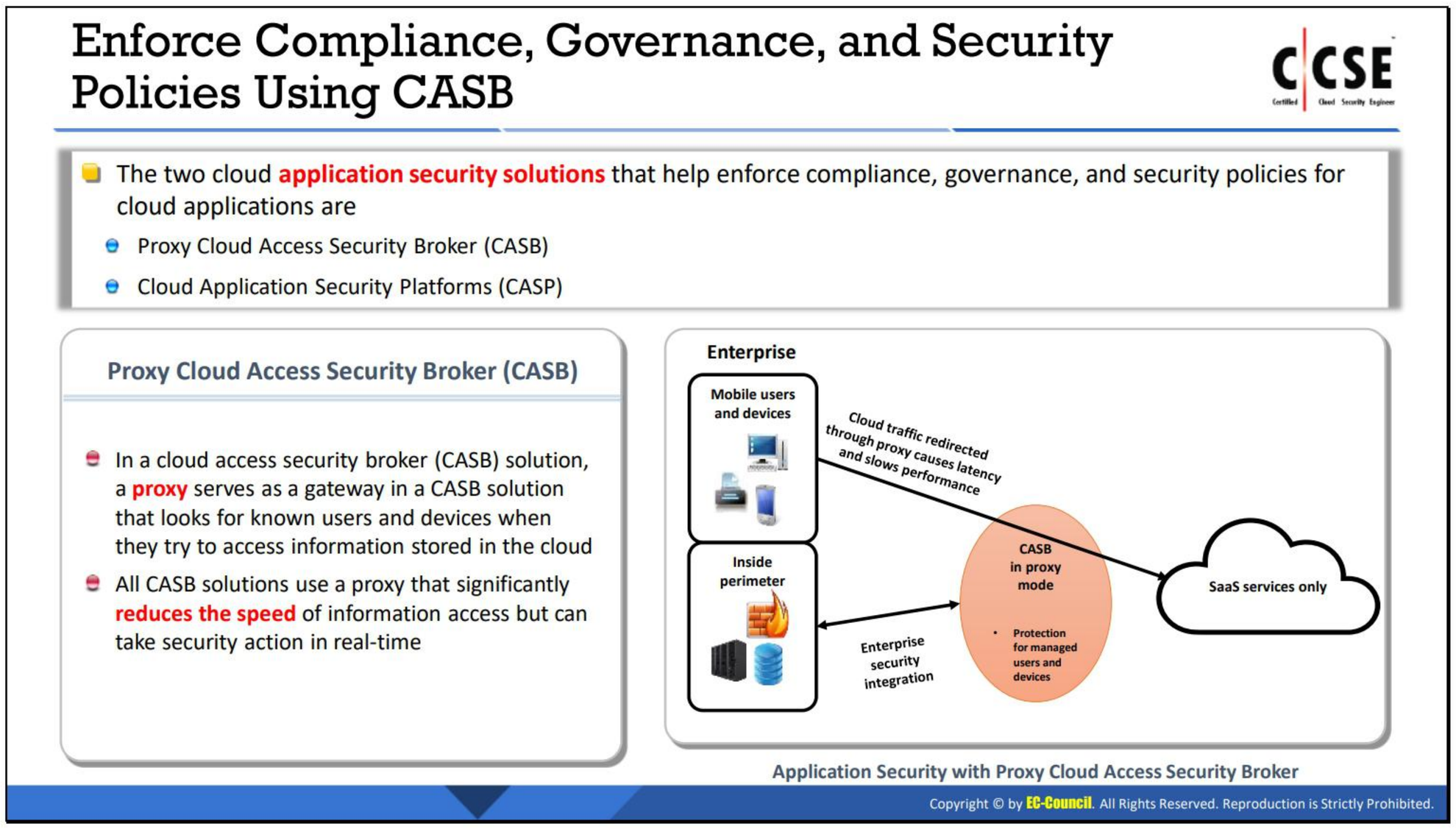
Application Orchestration

Application orchestration offers an automated process that synchronizes data between two or more applications or services by integrating them in real-time and establishing efficient management and monitoring. It provides a design of integration to decouple applications or services from each other. Application orchestration involves designing, creating, and delivering integration services. It offers features such as message routing, security, transformation, and reliability.

Application orchestration securely connects multiple application ecosystems and orchestrates workloads across multi-cloud and multi-vendor environments to deploy and manage integration between the applications and services with flexibility and scalability to secure the cloud environment. It provides access to network capabilities and data such as positioning, QoS and SLA assurance, traffic isolation, and data integrity.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enforce Compliance, Governance, and Security Policies using CASB

Cloud Application Security Solutions - CASB

Cloud access security mainly involves securing the interaction between cloud applications and cloud users in a SaaS solution. Controlling an organization's information present in cloud applications is referred to as cloud access security. Cloud access security includes having control over who is downloading and uploading files, which documents contain sensitive information, which documents are exposed to the internet, which cloud applications are potentially risky, which users possess anomalous behavior, and several other variables.

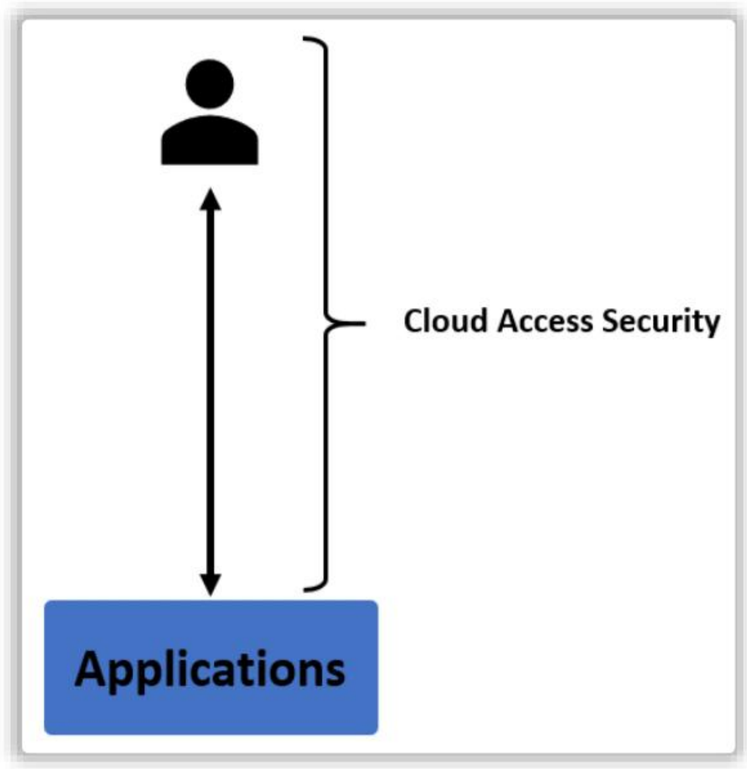


Figure 3.21: Cloud Application Security Solutions

There are two cloud application security solutions that take care of cloud access security. These solutions ensure that interactions between users and cloud applications remain secure in a SaaS

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

deployment. One of these solutions (CASB) uses a proxy browser extension to secure cloud applications. The other solution (CASP) uses the cloud application's native APIs to control, monitor, and secure activities that happen inside them. CASPs are API-based CASB solutions.

Proxy Cloud Access Security Broker (CASB)

CASB refers to security software (both on-premise or cloud-based) that is used between CSPs and cloud service users to enforce compliance, governance, and security policies for cloud applications. This software monitors all activities happening inside the applications and offers several other services such as warning administrators about possible hazardous actions, preventing malware automatically, enforcing security policies, etc.

A proxy-based CASB solution just performs the function of a firewall and sits between cloud users and cloud applications. However, it slows down user experience. This solution can secure multiple cloud-based SaaS applications.

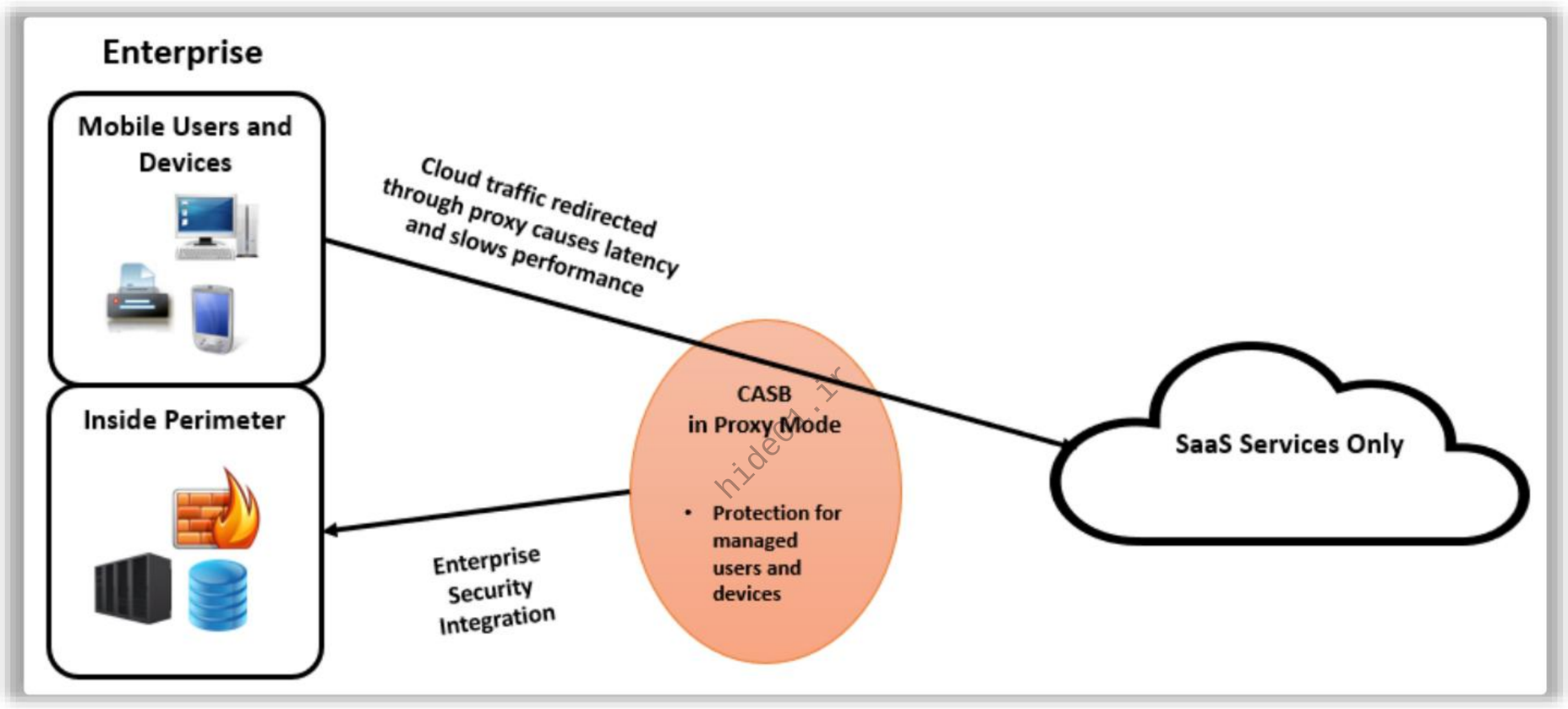


Figure 3.22: Proxy Cloud Access Security Broker (CASB)

A proxy serves as a gateway in a CASB solution that looks for known users and devices when they try to access information stored in the cloud. The advantage of using a proxy is that it can take security action in real-time.

Functions of CASB

CASB solutions provide three main functions.

- **Data-loss prevention (DLP):** DLP forms the most critical function of all data security strategies. Securing data in the cloud is very different when compared to securing data in traditional on-premises infrastructures. The main challenge faced in securing data in the cloud is the openness and accessibility of the cloud; therefore, data stored, shared, and accessed in the cloud is vulnerable to both malicious and accidental leaks. This increases concerns for IT and InfoSec managers.

  A CASB solution can help an organization quickly identify the leaks in its cloud environment and close them. It also offers the IT team with more robust policy controls

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

and rules, which enable the IT team to set and apply specific content-level sharing and remediation policies. As they configure the systems, DLP becomes more automatic.

- **Threat protection:** Organizations often become a victim of cyberattacks due to lack of adequate security. Smaller organizations are often easy targets for attackers but big and popular organizations are prone to attacks as well.

  CASB solutions help IT teams of organizations secure sensitive data stored in the cloud via acquisitions, partnerships, and homegrown threat protection technology. Organizations need to select their CASB wisely. Proxy-based CASBs provide protection against threats, similar to a firewall, whereas API-based CASB solutions, also known as CASP, provide an additional layer of security by working along with the existing InfoSec stack. The cloud environment can be effectively protected against malicious threats by using API-based CASB solutions. Cloud threat protection should also include securing unsanctioned cloud applications, shared files, browser plugins, etc., which could be used by attackers to gain access to the information infrastructure.

- **Account monitoring and compliance**: When an organization moves to the cloud-based software (e.g., Google Workspace or Microsoft 365) from on-premises software, the system administrators often cannot detect account activities due to lack of visibility. The visibility to identify who is logging in, from where they are logging in, what all they are accessing, etc. is not available unless the organization purchases enterprise-level licensing. Without proper visibility and control over account activities, it is very difficult to thwart phishing and malware threats, and prevent data loss.

- **Compliance**: This is also an essential element that demands account monitoring. All schools, government agencies, companies, and NGOs are required to protect personally identifiable information (PII) stored in their databases. They should inform the affected people whose information was stored in the databases in case of a data breach.

While most proxy-based CASBs use forward proxies, certain CASBs use reverse proxies. However, these proxies significantly increase the time required to access information, which in turn slows down the user experience. Moreover, using a proxy-based CASB solution is meaningless when a next-gen firewall or security gateway is in place because the proxy-based CASB solution just duplicates the functionality of a firewall without providing any additional protection while adding cost.

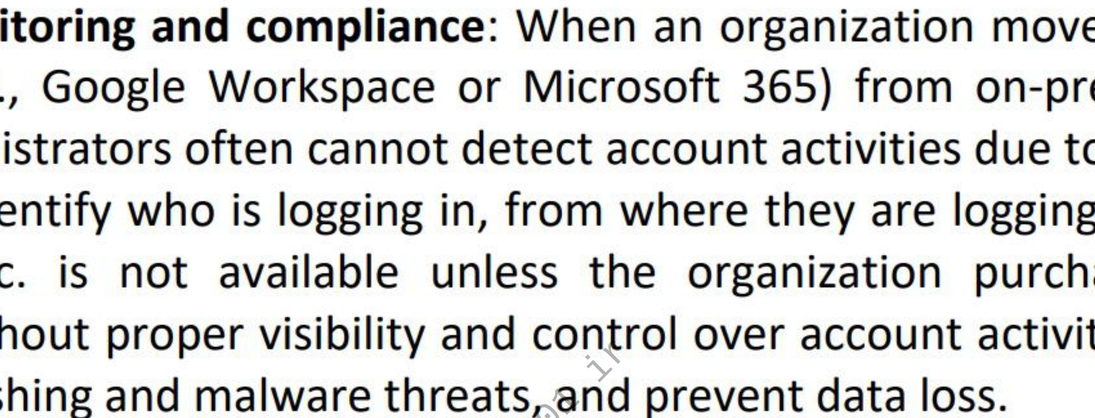


Figure 3.23: Proxy Deployment

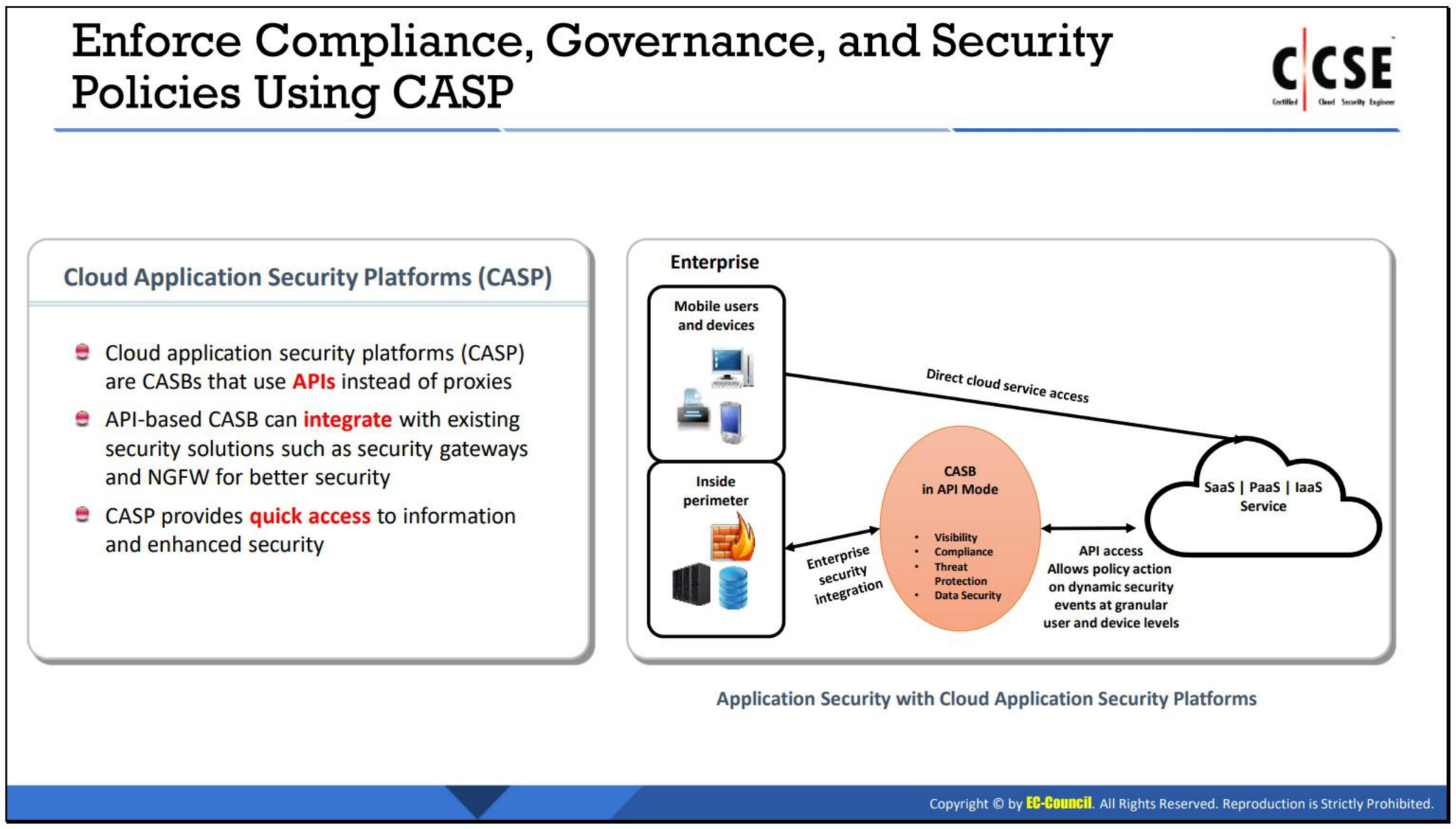
Most cloud application providers such as Google and Microsoft have advised against using proxy-based CASB solutions because of the inability of such solutions to stay updated with changes and

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

updates applied to application infrastructures. Application developers (such as Google and Microsoft) often make changes and updates to authentication methods and protocols and they do not inform CASB vendors regarding any updates or changes made to the application infrastructure; thus, CASB vendors do not get to know what changes are needed when updates happen. This creates gaps in the security infrastructure that need to be filled by CASB developers.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enforce Compliance, Governance, and Security Policies using CASP

Cloud application security platforms (CASPs) are CASBs that use APIs instead of proxies. Using API-based CASBs is a better way to secure data that is shared and stored in the cloud. These solutions provide users with secure, direct access to the cloud from anywhere, any device across the world without having any impact on network performance. IT and InfoSec teams can use CASPs to customize access rules, automate compliance policies, and do other things. By using CASP solutions, they can also gain visibility into account activity in the cloud. This makes it easy for them to achieve compliance, data security, and threat protection.

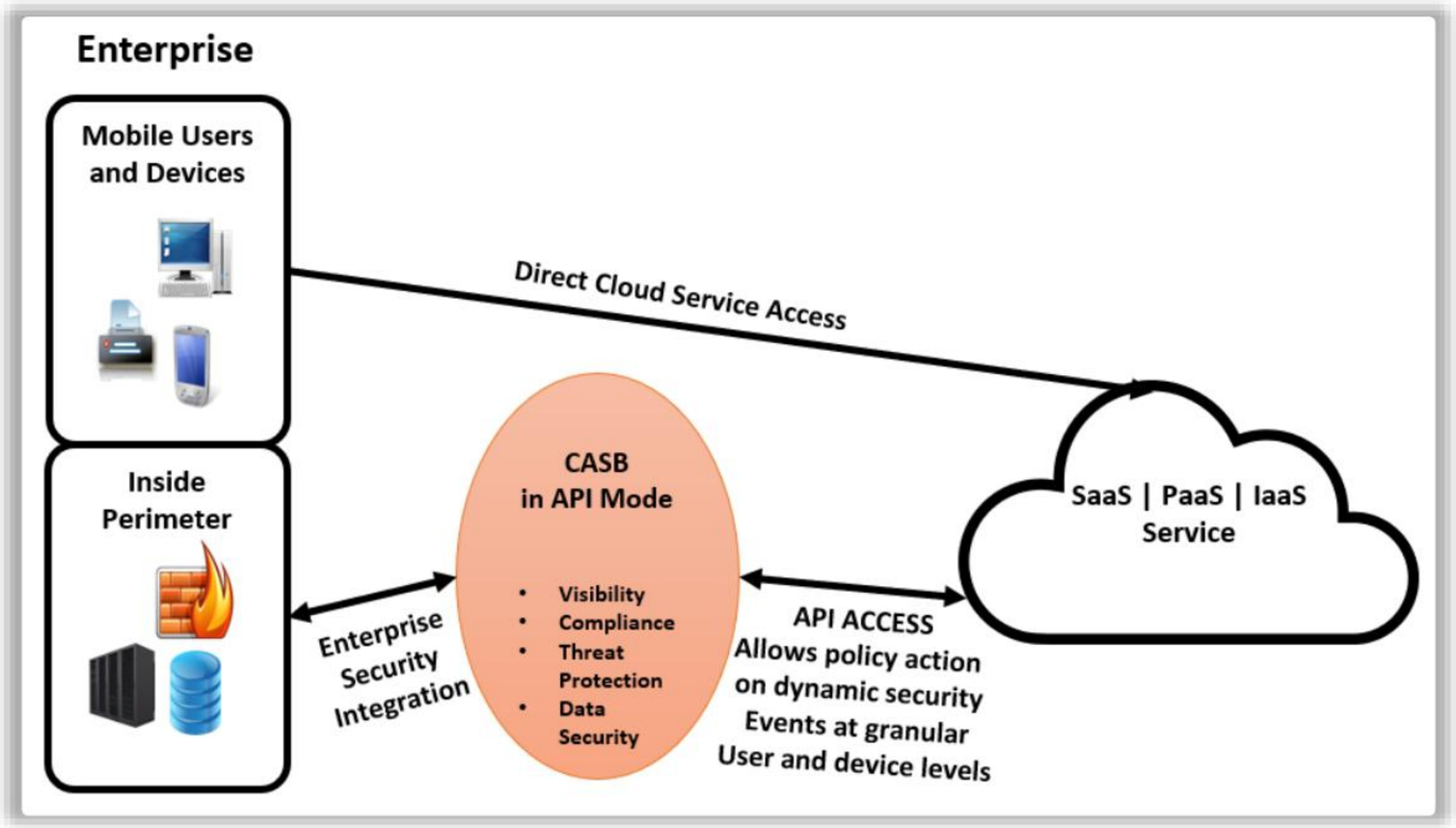


Figure 3.24: CASP (or) API-Based CASB

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Unlike proxy-based CASB solutions, API-based CASB can integrate with existing security solutions such as security gateways and NGFWs for better security. They provide an additional layer of security rather than just duplicating a functionality (unlike proxy-based CASBs). CASPs work as a nearly native feature within every cloud application because these solutions develop one-to-one integrations by using cloud applications APIs. The effectiveness of a CASP is impacted only by changes in API protocols and these changes are regularly documented and updated for developers.

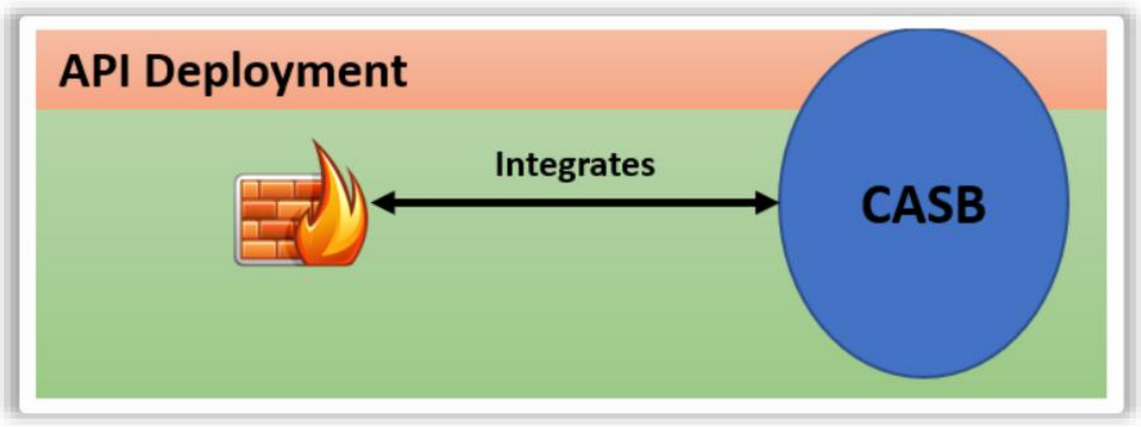
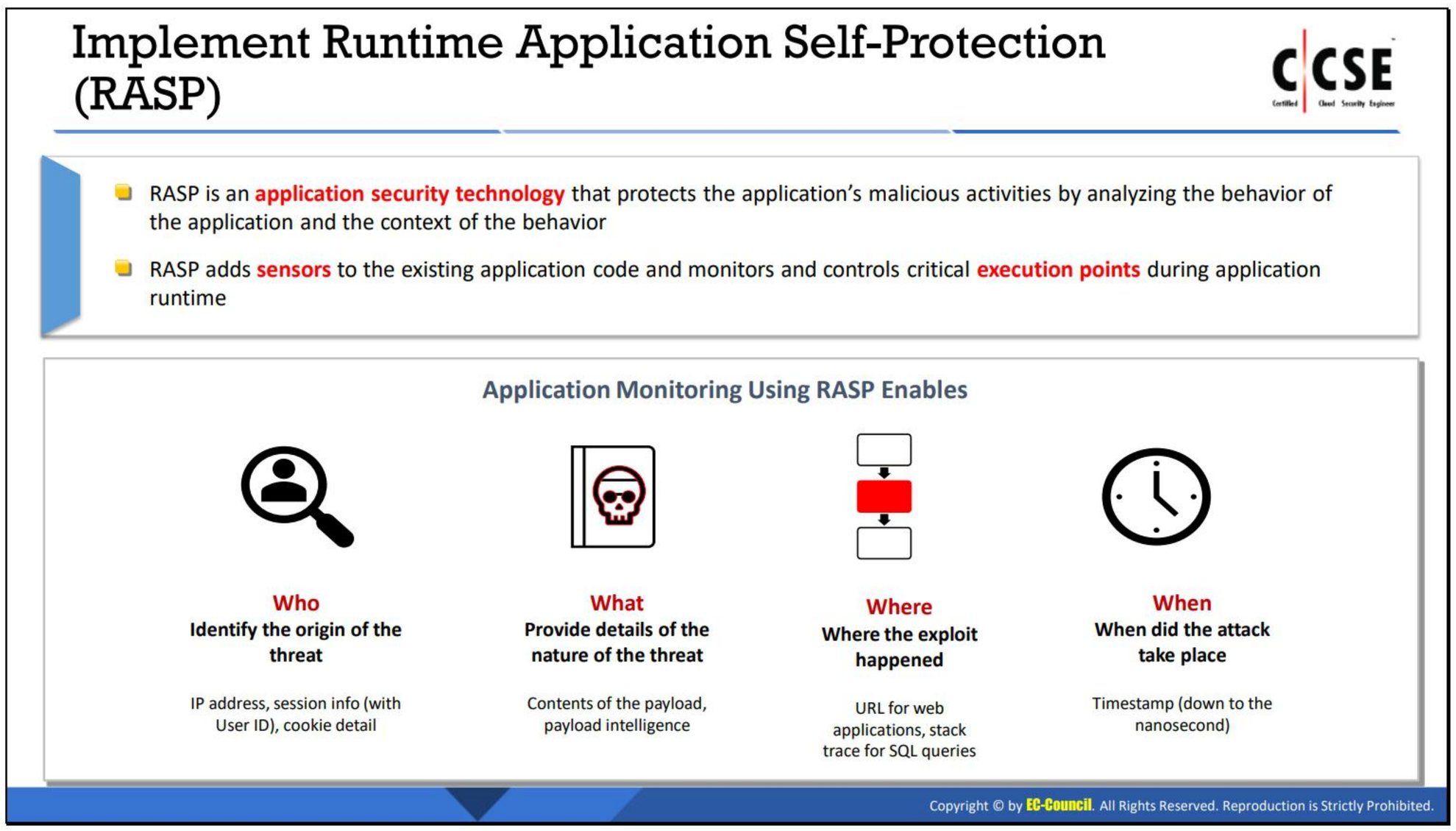


Figure 3.25: Integration of API-based CASB with Security Solution

API-based CASB models are getting more popular compared to their proxy-based counterparts because they provide quick access to information and enhanced security. Moreover, they are more user-friendly and easier to use. Instead of inline inspection of cloud application traffic, they focus on detection, remediation, and user education.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Implement Runtime Application Self-Protection (RASP)

RASP is one of the latest security technologies used to protect cloud applications from attacks during runtime. While WAFs protect applications from the outside, RASPs protect them from the inside. RASPs provide better visibility of the dataflow and the consequences of each input received by the application. They protect applications and APIs by preventing attackers from exploiting vulnerabilities such as XSS, SQL injection, and insecure deserialization.

RASP is an application security technology that protects applications from malicious activities by analyzing the behavior of the applications and the context of the behavior. Certain latest RASP solutions also provide protection from design flaws or business logic flaws such as workflow abuse, parameter tampering, etc. They provide in-depth security and significantly reduce the chances of security breaches. Developers can use RASP solutions to detect vulnerabilities inside their apps. RASP adds sensors to the existing application code and monitors and controls critical execution points during application runtime.

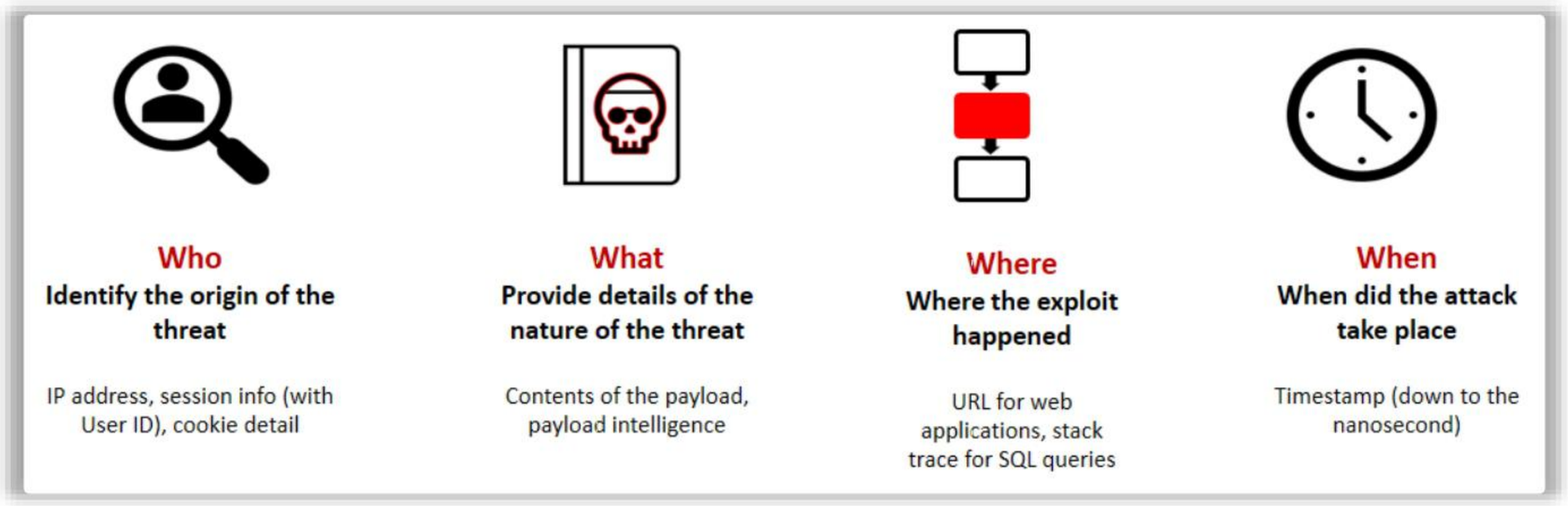


Figure 3.26: Application Monitoring using RASP

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

RASP works well when deployed with WAFs to provide better security for cloud applications. While WAFs block known exploit payloads, RASP blocks unknown exploit payloads. A RASP solution can also prevent zero-day attacks and provide cloud-native application protection; it also protects from other types of attacks. For deep visibility into an organization's actual runtime exposure to risk and faster/smarter responses, RASP provides correlated application, network, and database security logs. Additionally, it supports detailed audit trails and root cause analysis for data breaches.

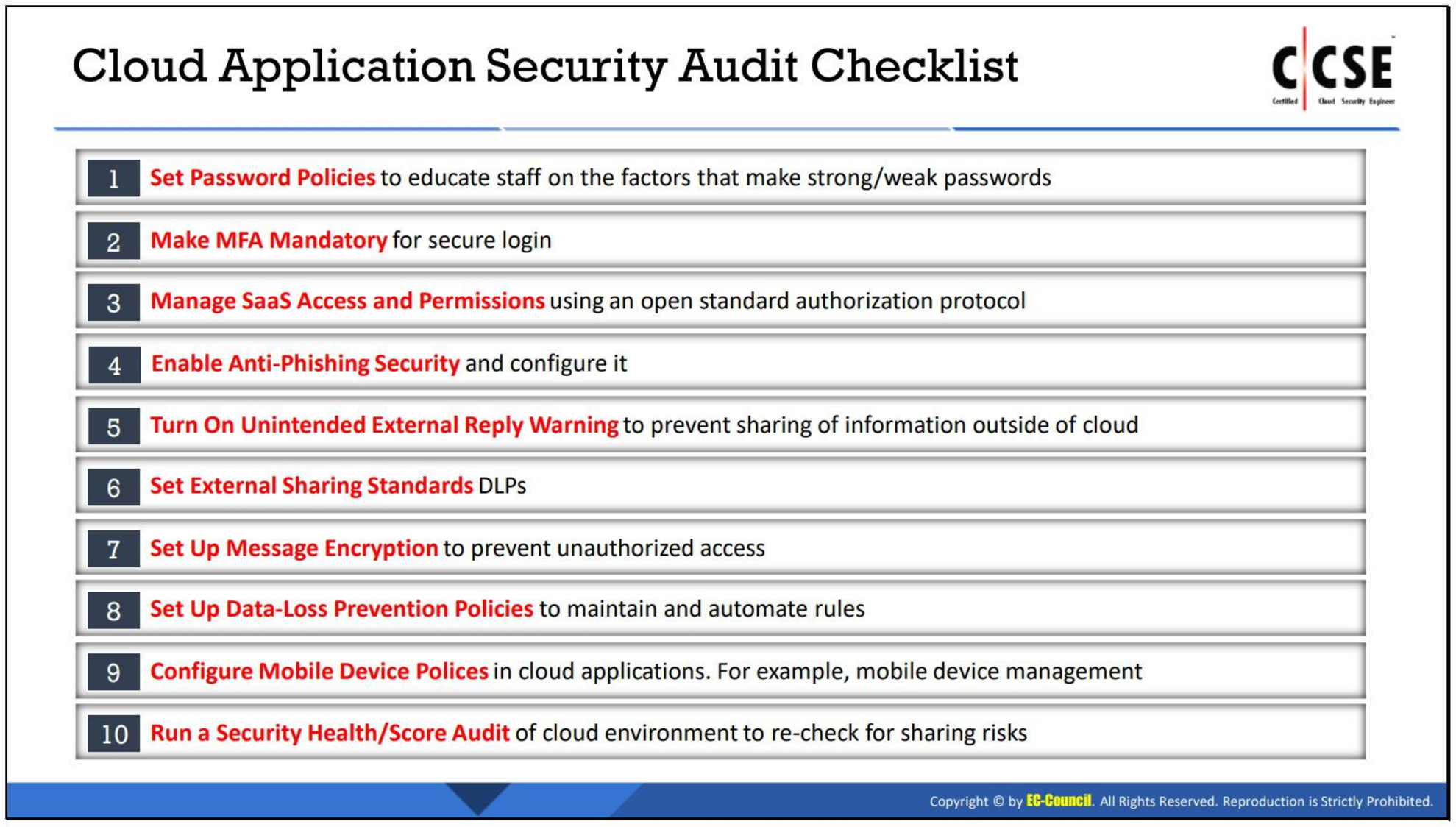
RASPs work in two modes:

- Diagnostic mode: In this mode, RASP will raise an alarm to indicate something is wrong with the application.
- Protection mode: In this mode, RASP will try to prevent malicious actions such as the execution of certain instructions that appear to be a SQL injection attempt.

RASP inserts sensors into existing application code to monitor and control critical execution points. It also reduces false positives, provides strong protection, and has easy maintenance.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

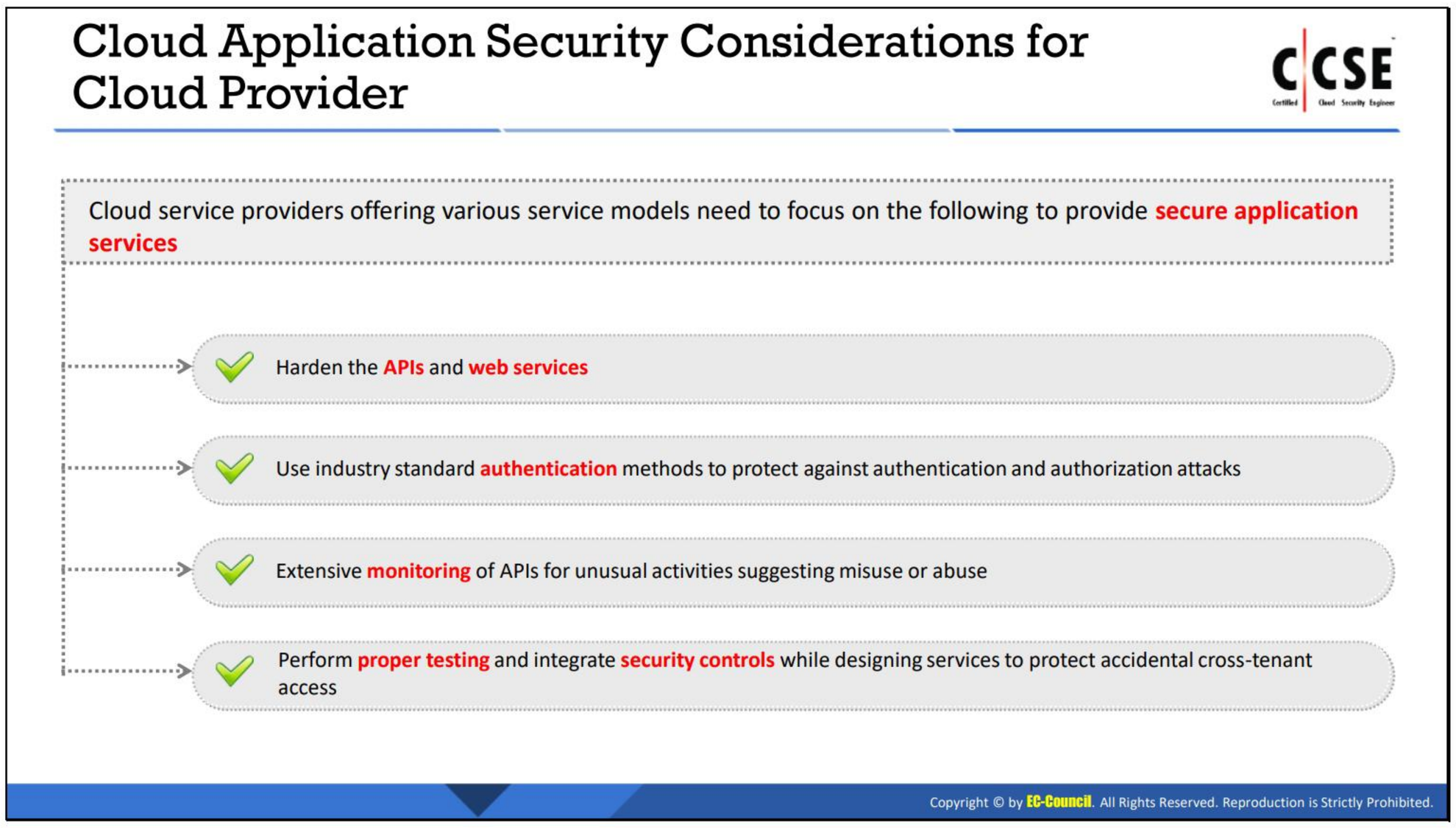


Cloud Application Security Audit Checklist

The audit checklist of cloud application security involves:

- **Set password policies** to educate staff on the factors that make strong/weak passwords.
- **Make MFA mandatory** for secure login.
- **Manage SaaS access and permissions** using an open standard authorization protocol.
- **Enable anti-phishing security** and configure it.
- **Turn on unintended external reply warning** to prevent sharing of information outside of the cloud.
- **Set external sharing standards** DLPs.
- **Set up message encryption** to prevent unauthorized access.
- **Set up data-loss prevention policies** to maintain and automate rules.
- **Configure mobile device polices** in cloud applications. For example, mobile device management.
- **Run a security health/score audit** of the cloud environment to re-check for sharing risks.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

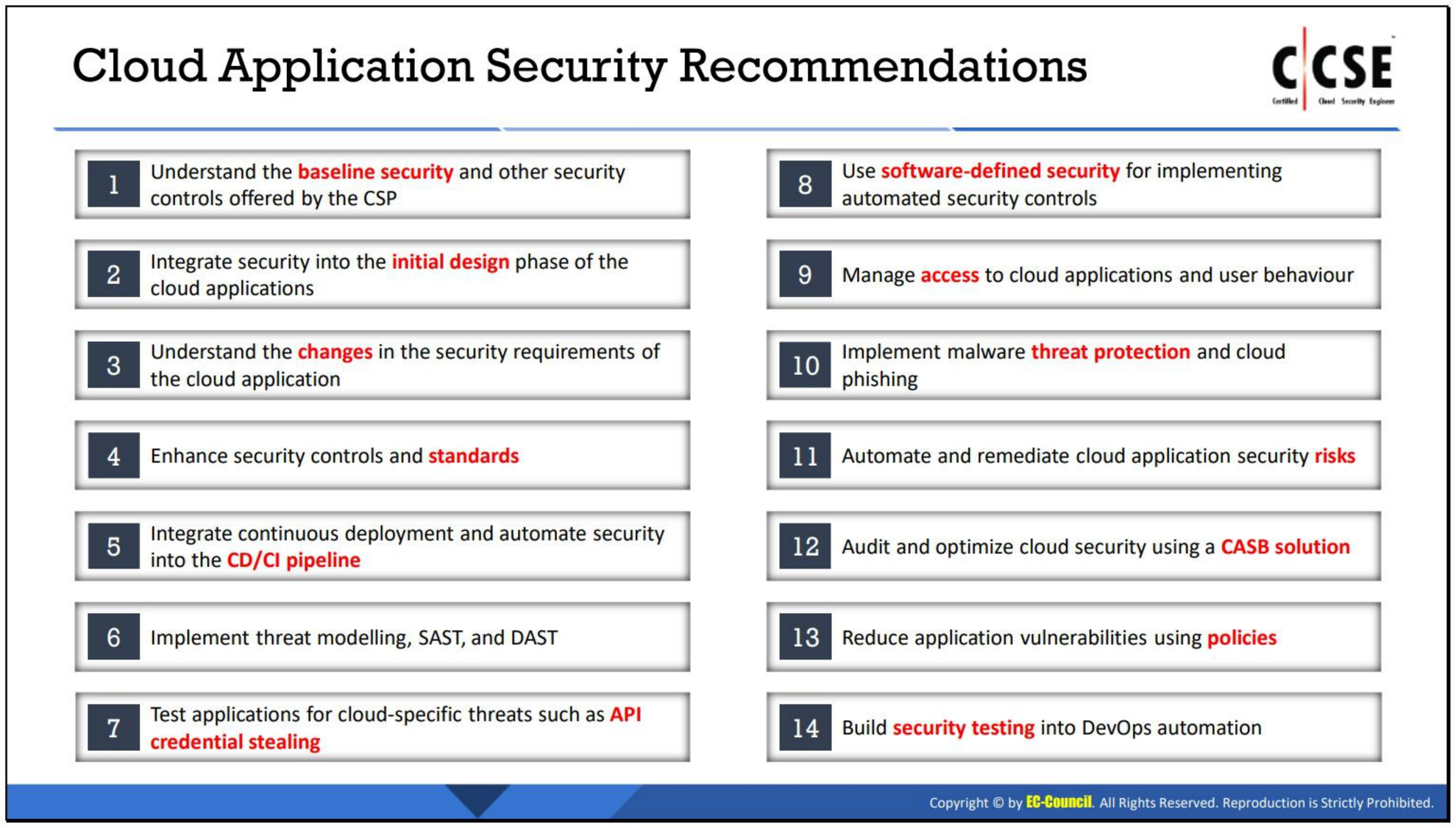


Cloud Application Security Considerations for Cloud Provider

Cloud providers are responsible for providing a secure cloud platform for their customers. To ensure a secure and safe cloud platform, they need to implement certain security measures that help protect cloud resources, applications, and data. CSPs offering various service models need to focus on the following to provide secure application services:

- **Harden APIs and web services**: Attackers target APIs and web services as cloud APIs and web services are exposed to the public and are easily accessible. To protect cloud resources and provide secure cloud services, CSPs need to harden APIs and web services.
- **Use industry-standard authentication methods to protect against authentication and authorization attacks:** Industry-standard authentication methods are tested and proven to provide the level of security that is essential to secure cloud applications. CSPs must use only industry-standard authentication methods to secure cloud apps from authentication and authorization attacks.
- **Extensive monitoring of APIs for unusual activities suggesting misuse or abuse**: APIs are the easiest targets of attackers and they can expose the whole cloud environment if not secured. Monitoring APIs for unusual activities is a part of API security because it helps detect misuse or exploitation. Providers must implement extensive monitoring to secure APIs.
- **Perform proper testing and integrate security controls while designing services to protect accidental cross-tenant access**: It is the responsibility of the cloud provider to ensure there is no cross-tent access in its cloud platform. While designing cloud services, they should integrate security controls and perform proper testing of these controls to prevent any accidental cross-tenant access. Cross-tenant access may allow attackers to steal information and abuse tenants.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Application Security Recommendations

Implement the following cloud application security best practices to improve cloud security operations.

hade01.ir

- **Implement due diligence in selecting and sanctioning cloud apps**: A new risk is introduced every time a new application or platform is connected to a company's cloud environment. Therefore, manage which vendor can access their IT ecosystem. Use the right set of security tools to manage SaaS applications hosted and accessed in the cloud. Help teams cautiously select vendors. The below steps are useful in safe SaaS app selection.
    - **Know the source of the app**: Check if a popular developer offers the app and whether the developer is active in providing patches and updates.
    - **Limit additional permissions**: Check what type of permissions are requested by the app and whether those permissions are needed to perform their intended purpose.
    - **Be careful of the application's name**: This is required because criminals often create look-alike applications to trick people into downloading them.
    - **In-app purchases**: Check whether the app requires credit card details for in-app purchases and whether it is required for its intended purpose.
    - **Authentication and encryption**: Check whether the app supports authentication and encryption and which encryption methods are used for accessing and storing data.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Read reviews**: To know what other users of the app have experienced, read the reviews carefully. Read overly complimentary reviews as they could be fake.

- **Manage access to cloud apps and user behavior**: Set up and configure MFA and SSO properly if they are not present for the organization's cloud applications. Ensure that user groups are set within the main application (Microsoft 365 and/or Google Workspace) to manage who can access what.

  To improve the data security posture, segment information and allow access to sensitive information only for specific users who need access to them.

  To reduce the risk of an account takeover, put a block on IP address locations for logins. Monitor for a spike in the number of failed login attempts to detect when their organization is under attack. Educate employees on how to be vigilant for phishing emails can help organizations to prevent attacks.

  Monitor for abnormal user behavior. Abnormal behavior includes phishing emails sent from any internal account, importing files that contain malware links to the shared drives, and bulk downloading of files. The aim is to identify whether external threat actors and internal users are potentially misusing the information.

- **Cloud phishing and malware threat protection**: Attackers still use emails as the primary threat vector. Protect emails (even if they are hosted in the cloud, such as Gmail). Cloud malware threat protection works differently than normal perimeter-based security technology. Criminals try to find ways to bypass the perimeter-based security for companies that leverage cloud-based email platforms.

  The native email filters offered by Microsoft and Google are also prone to vulnerabilities because these filters are designed to whitelist the links that come from their domains automatically. The number of incidents where attackers upload malicious files to SharePoint and Google Drive and then send the file link in emails is increasing. Therefore, add a cloud-specific protective layer.

- **Automate and remediate cloud app security risks**: Use CASB solutions to automate cloud app risk detection and remediation. Use these solutions to set up DLP rules and policies to detect improper use of information automatically, abnormal behavior, malware and phishing threats, shadow IT threats, etc. The technology automatically takes remediation actions selected to quarantine, delete, restrict access, etc. making their job much easier and simpler.

- **Audit and optimize**: Regularly audit and optimize the organizations' security infrastructure and posture depending on their size and complexity of their data environment. Security teams can use CASBs to set up audit reports that they want CASBs to run periodically. This ensures that they get the reports directly without requiring them to set up the same report repeatedly. Auditing helps security teams know about new vulnerabilities, whether unsanctioned apps are sneaking back into the environment, etc. Keep a close watch on these risks and trends over time to optimize how they have set up their rules and policies to make CASB solutions work even better.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Apply cloud governance policies**: When working inside the cloud environment, cloud governance policies are required to ensure that security standards are present for all users to follow. Use monitoring mechanisms to ensure all the established policies are followed. Establish hardening standards for containers, VMs, approved repositories, etc. Implement some other cloud security and cloud governance policies to ensure strict monitoring of sharing, usage, and storage.
- **Identify, categorize, and secure sensitive data**: As cloud users are allowed to share files and folders in the cloud environment, organizations must be proactive in using the right cloud security policies around sensitive data and file sharing. To do this, identify sensitive data such as organizational policies, customer data, hardcoded passwords, etc. Such data needs to be stored securely in separate folders with limited access. After sensitive data is identified, categorize such data into different sections and encryption or other protective mechanisms to ensure that only intended users can access it.
- **Use DLP with CASBs**: Use a DLP policy along with CASBs. CASB solutions are very helpful in preventing data loss. The main goal of CASBs is to extend an enterprise's security controls from its on-premises infrastructure to the cloud.

  By using CASBs, the organization can

  - Detect which cloud services are being used, who is using them, what type of security risks they introduce to the application data and the organization.
  - Evaluate and choose cloud services that satisfy its compliance and security requirements by using a database of cloud services and security controls.
  - Detect unauthorized or improper use of the cloud, including activity that may compromise user accounts both from inside the organization (by employees) and outside (by end-users).
- **Restrict downloading sensitive data to insecure or risky devices**: Even after having strict access controls, data loss occurs mostly through downloading files to devices. Ensure to make security policies that block and protect downloads to untrusted devices and monitor low-trust sessions while sharing data externally.
- **Use real-time session controls to have secure collaboration with external users**: Create a session policy that allows an organization to monitor sessions between internal and external users is necessary to ensure secure collaboration and gain better visibility in the cloud environment. This will allow tracking of every session between users and restricting particular activities against compliance standards and application security.

  Prevent data exfiltration by disabling functions such as copying, pasting, downloading, cutting, or printing confidential data. When users share or upload files containing sensitive data, these files must have appropriate labels and protection.
- **Integrate cloud-based IAM solutions with enterprise security**: Integrate cloud-based identity management solutions with enterprise security to enhance the overall cloud applications security.

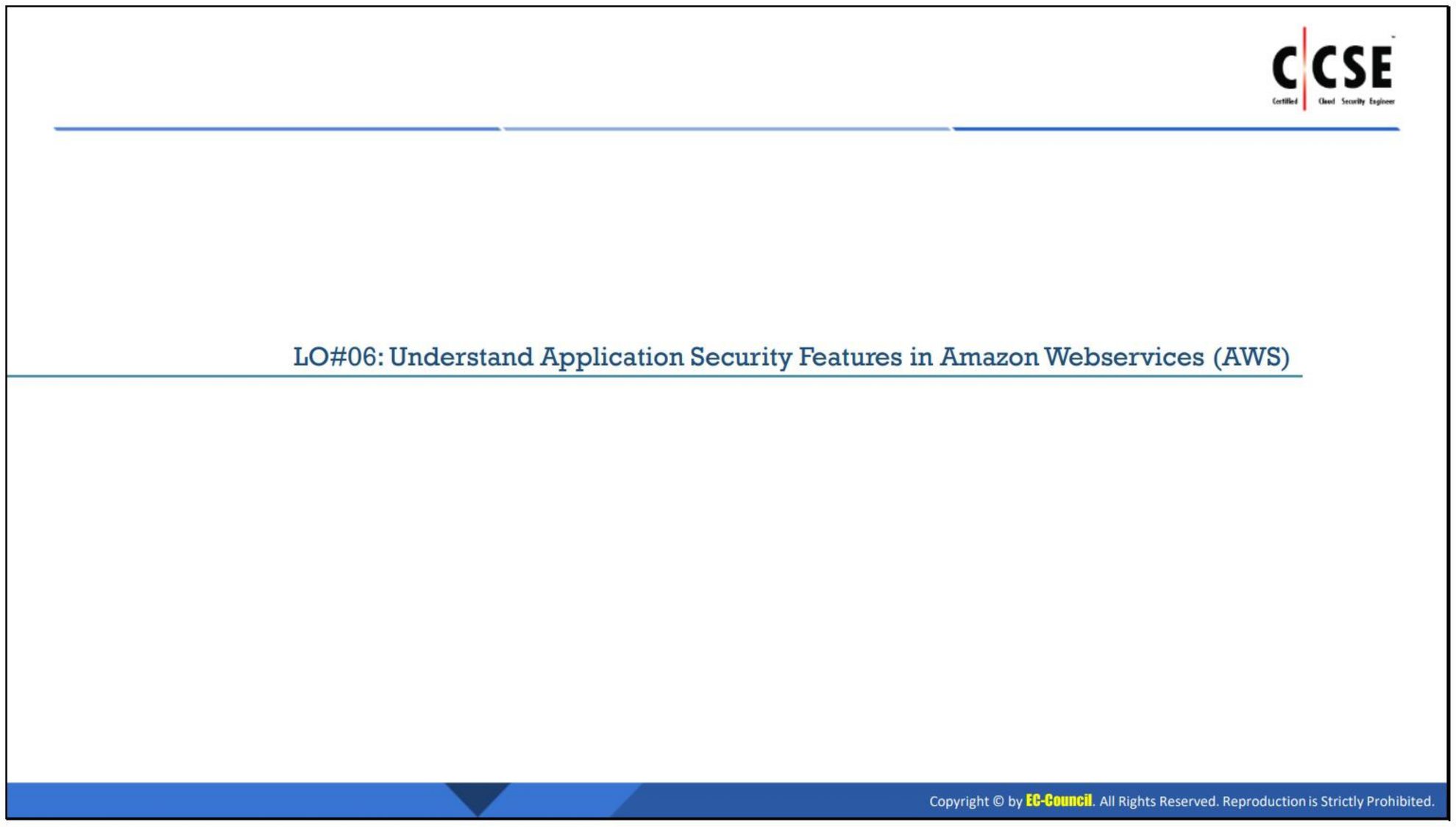
h1e0i.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Build security testing into DevOps automation:** Validate that applications are secured properly and are as per the outlined and scripted specifications. To facilitate consistent deployment of secure cloud-based applications, automate these tests and checks.
- **Train users**: Train staff and users on following security policies because human errors constitute the most common reasons for cloud security initiatives' failure. Train in-house users about the risk of shadow IT and its consequences.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

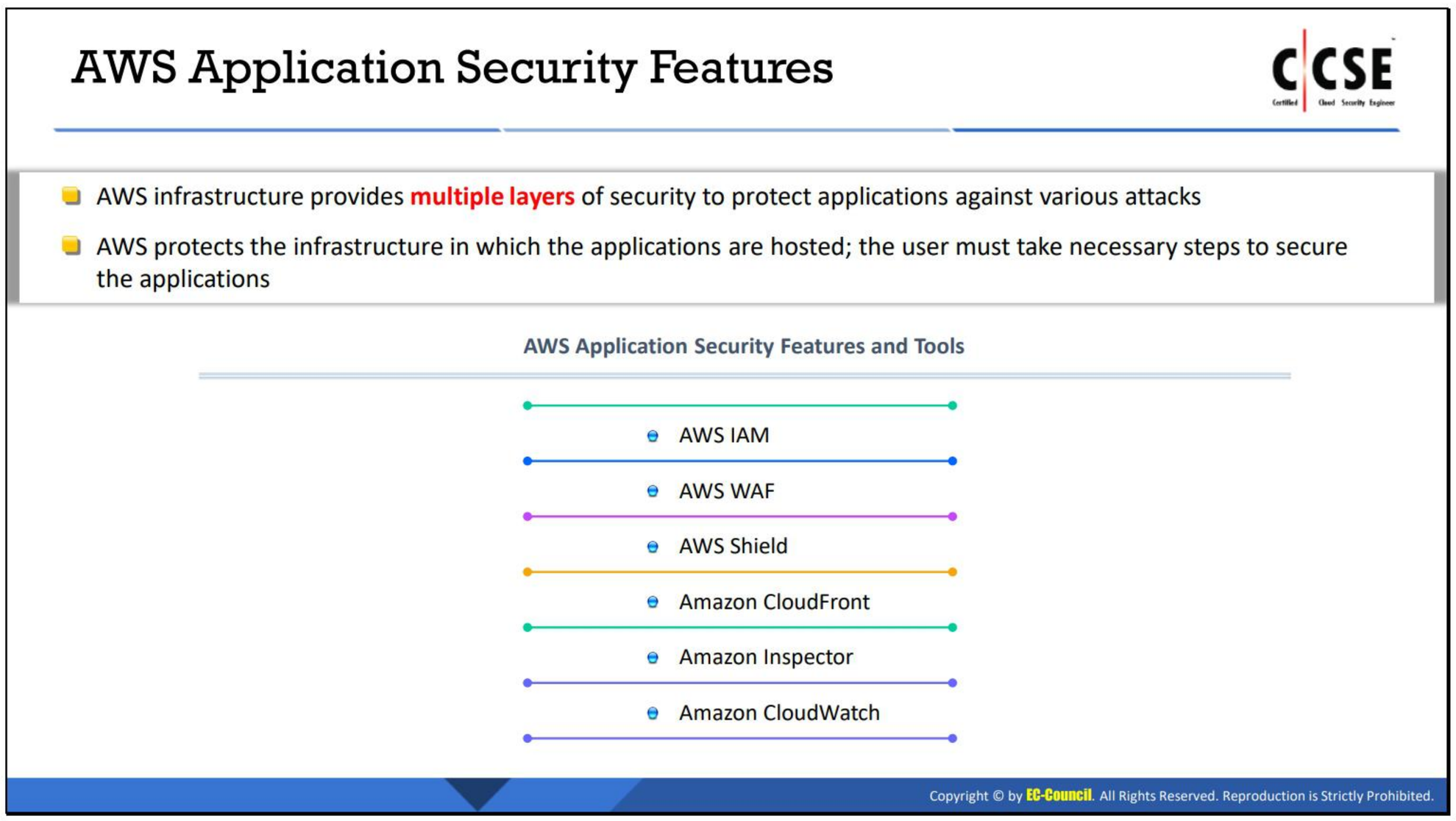


LO#06: Understand Application Security Features in AWS

AWS provides a wide range of services and tools to enable cloud users secure their applications. Knowledge of how to configure these services to enhance the security of the hosted applications is very important for cloud security engineers. This section explains the different application security features in AWS and how they can be used to protect the AWS cloud applications. It also describes the best practices for securing AWS cloud applications.

hid01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



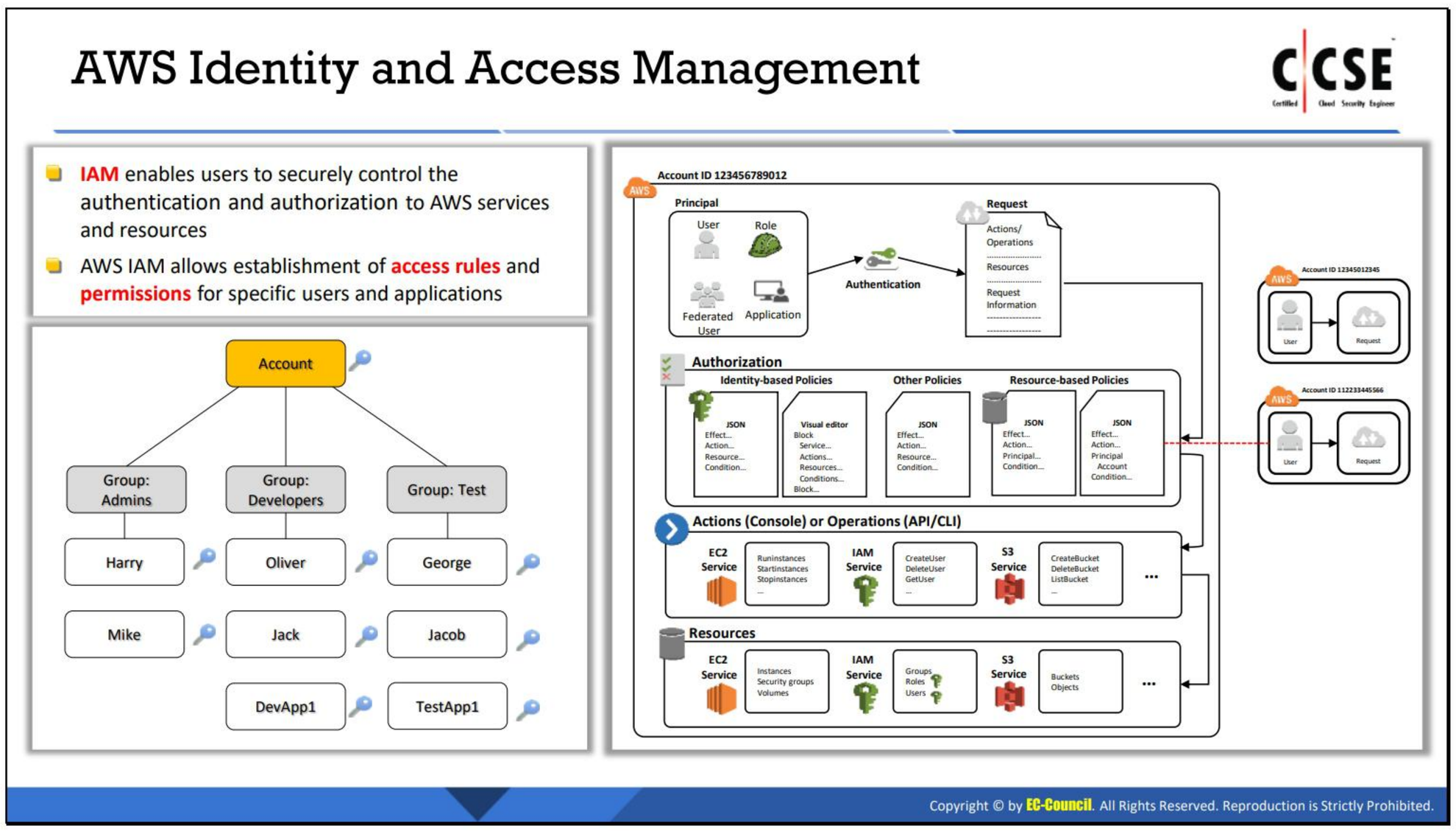
AWS Application Security Features

For security and performance to go hand in hand, AWS provides the best features for application security. AWS provides a layered security approach that can protect the application from multiple attacks. To protect applications from the OWASP Top 10 vulnerabilities and the common vulnerability exposures, CloudFront and WAFs and AWS Shield Advanced do the job. Although AWS protects the infrastructure in which the applications are hosted, the user must take the necessary steps to secure the applications.

AWS Application Security Services

- **Amazon CloudFront**: Amazon CloudFront is a content delivery network (CDN) that is highly secure.
- **AWS Web Application Firewall (WAF):** Common web attacks can be prevented by setting up the network traffic rules in AWS WAF.
- **AWS Firewall Manager:** AWS Firewall Manager is the service where firewall rules can be centrally configured and managed.
- **AWS Shield:** DDoS attacks can be prevented by AWS Shield and AWS Shield Advanced.
- **Amazon Inspector:** The automated security checking service Amazon Inspector can check for vulnerabilities or exposures in the applications deployed on AWS.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AWS Identity and Access Management

AWS identity and access management (IAM) is a web service that enables you to control access to AWS services and resources securely. It allows establishment of access rules and permissions to specific users and applications. It controls who is authenticated (signed in) and authorized (has permissions) for resource access.

hi0001.ir

IAM Features

Key features of IAM are listed below.

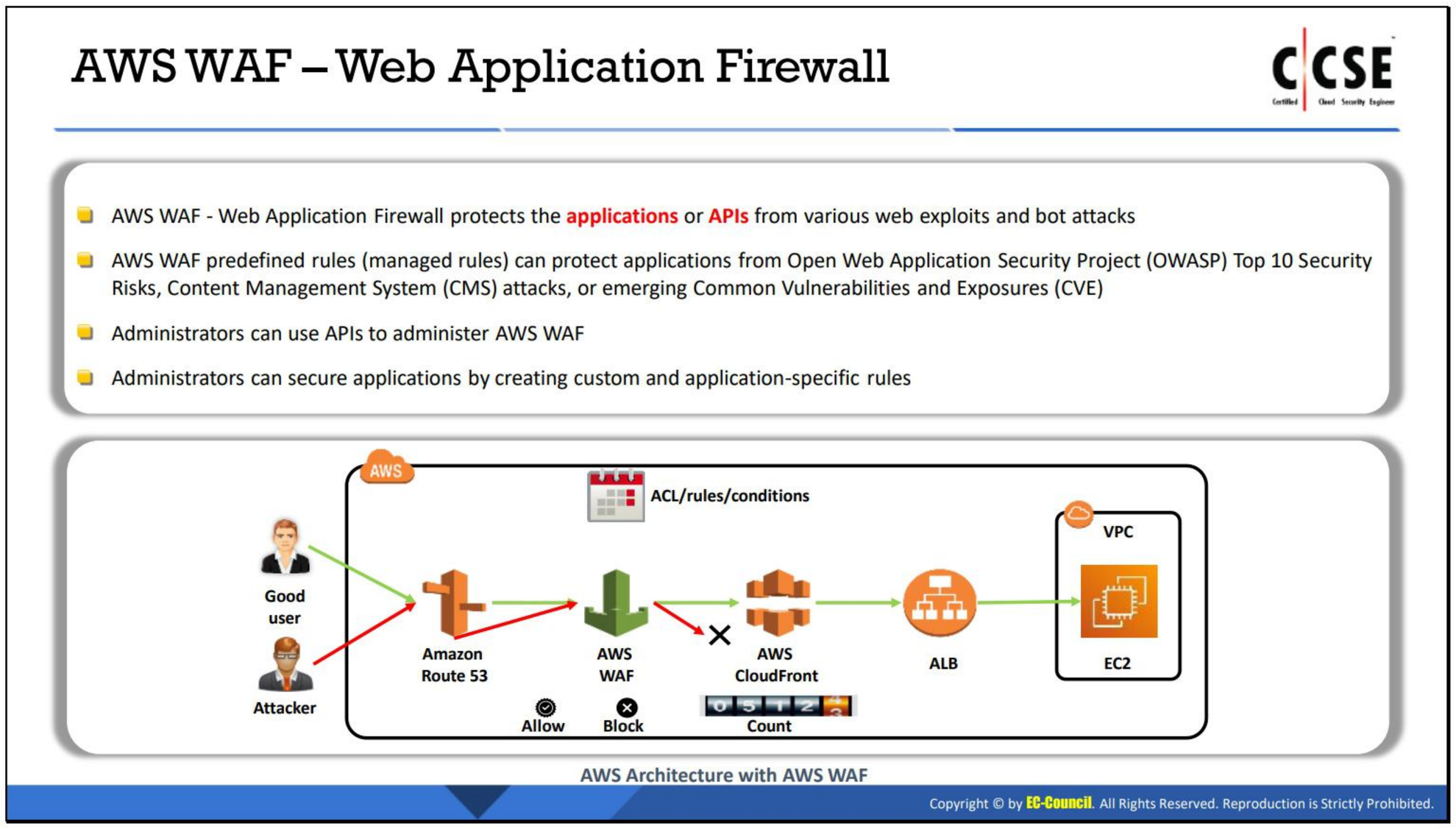
- **Shared access to AWS account/enhanced security**: Creating usernames and passwords for other users/groups to delegate access to specific AWS service APIs and resources without sharing your password or access key.
- **Granular permissions**: Granting different permissions to different people for different resources to provide the granularity to control a user's access to specific AWS services and resources.
- **Secure access to AWS resources for applications that run on Amazon EC2**: Providing credentials for applications that run on EC2 instances to permit applications to access other AWS resources.
- **MFA**: Adding two-factor authentication to your account and to individual users for additional security.
- **Identity federation**: Allowing users who already have passwords elsewhere and allowing users to have just one password for on-premises and cloud environment work.
- **Identity information for assurance**: Receiving log records if you use AWS CloudTrail.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **PCI DSS compliance:** Supporting the information security standard Payment Card Industry Data Security Standard (PCI DSS) for organizations that handle branded credit cards from the major card schemes.
- **Integrated into AWS services**: Allowing to define access controls from one place in the AWS Management Console that will take effect throughout your AWS environment.
- **Password policy**: Allowing to reset a password or rotate passwords remotely and setting rules for passwords' usage.
- **Policies and groups**: Use IAM groups for easier permissions management and to follow IAM best practices. IAM allows organizing IAM users into IAM groups and applies a policy to that group. Individual users still possess their credentials.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AWS WAF- Web Application Firewall

The AWS Web Application Firewall can protect APIs or applications deployed on AWS from common web exploits such as SQL injection, cross-site scripting, etc, thereby ensuring that security and availability of the application is not compromised. The AWS WAF can filter out the network traffic based on certain predefined rules. Managed rules for AWS WAF contain certain predefined rules that can be used for defining the rules.

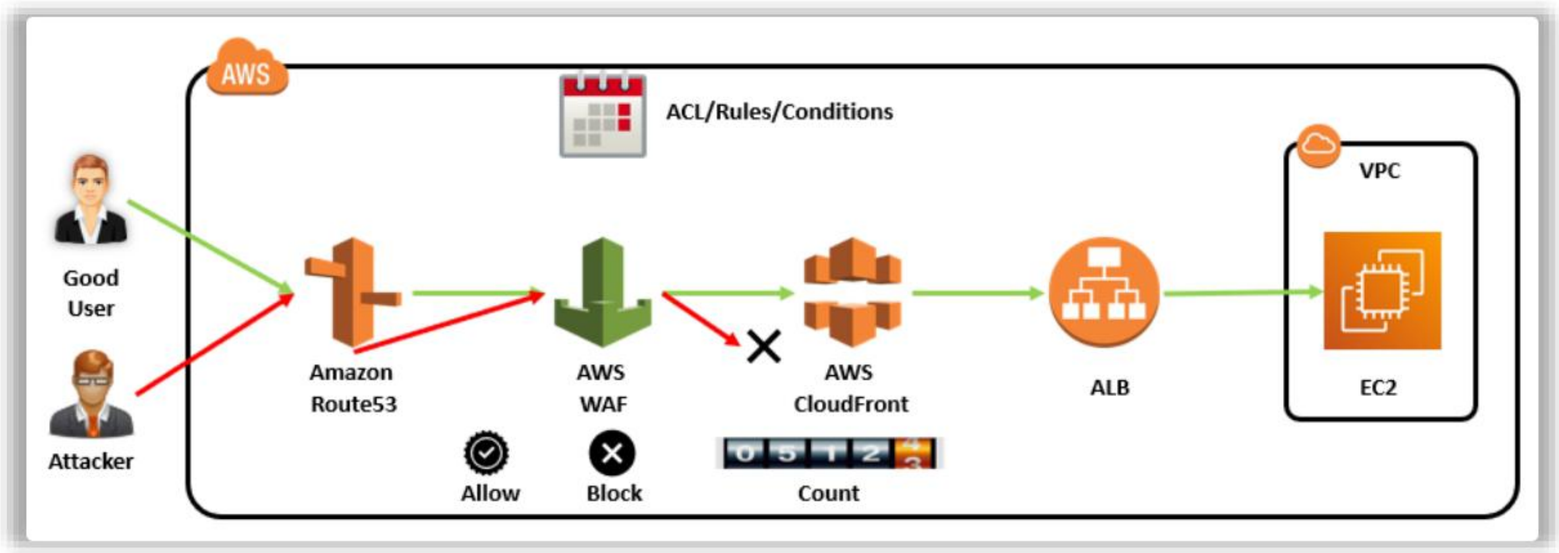
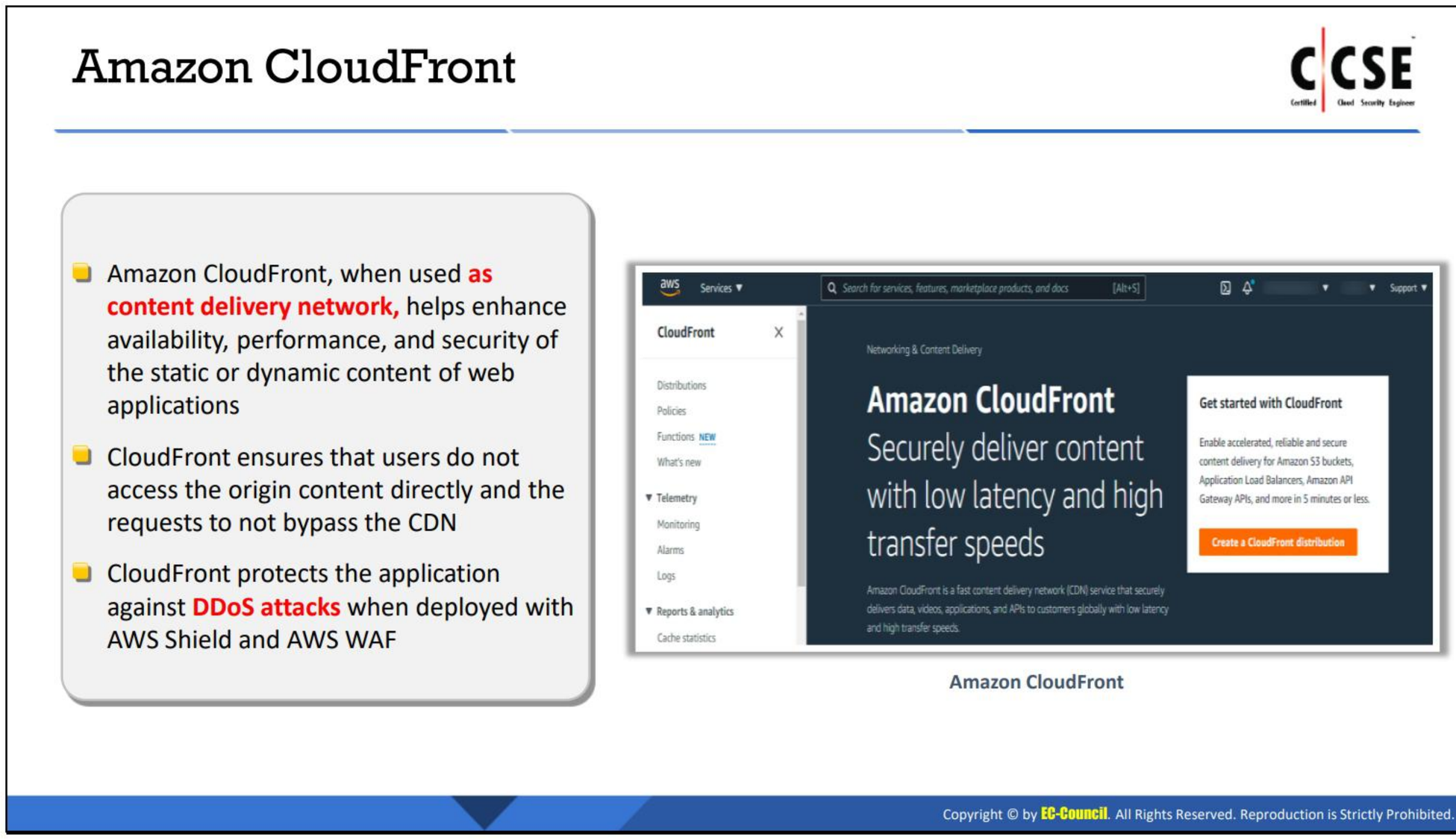


Figure 3.27: AWS WAF

When new security issues emerge, the managed rules for AWS WAF will get updated. The managed rules can protect against OWASP Top 10 Security Risks as well as common vulnerabilities and exposures (CVE). Security policies can be updated quickly across the whole infrastructure as the updates take less than a minute when any issues arise. Web requests can be filtered based on features such as IP address, origin country, malicious scripts, malicious SQL code, etc. Rules can be defined to allow/block requests or count requests based on certain properties. APIs are used to administer AWS WAF. Administrators can create custom, application-specific rules to protect applications from common attacks.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Amazon CloudFront

Amazon CloudFront

CloudFront is a fast content delivery service that can deliver data at high speeds and securely without any data loss. Network and application layer DDoS attacks can be prevented as it offers field-level encryption and HTTPS support. Amazon CloudFront can be integrated with AWS Shield, AWS WAF, and Route 53, which protect against most web attacks. However, it needs to be ensured that users do not access the origin content directly and the requests not to bypass the CDN.



FIGURE 3.28:Amazon Cloud Front

Amazon CloudFront can work with Amazon EC2, Amazon S3, and Elastic Load Balancing to deliver a seamless experience. When used as a CDN, Amazon CloudFront helps enhance the availability, performance, and security of web applications' static or dynamic content. It can deliver faster and high availability services to the users, so that availability in the CIA Triad can be met with CloudFront. CloudFront can be integrated with AWS Shield Advanced and AWS WAF to add extra layers of defense, which protects against most CVEs. CloudFront has security compliance certifications such as PCI DSS, HIPAA, SOC 1/2/3, etc.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

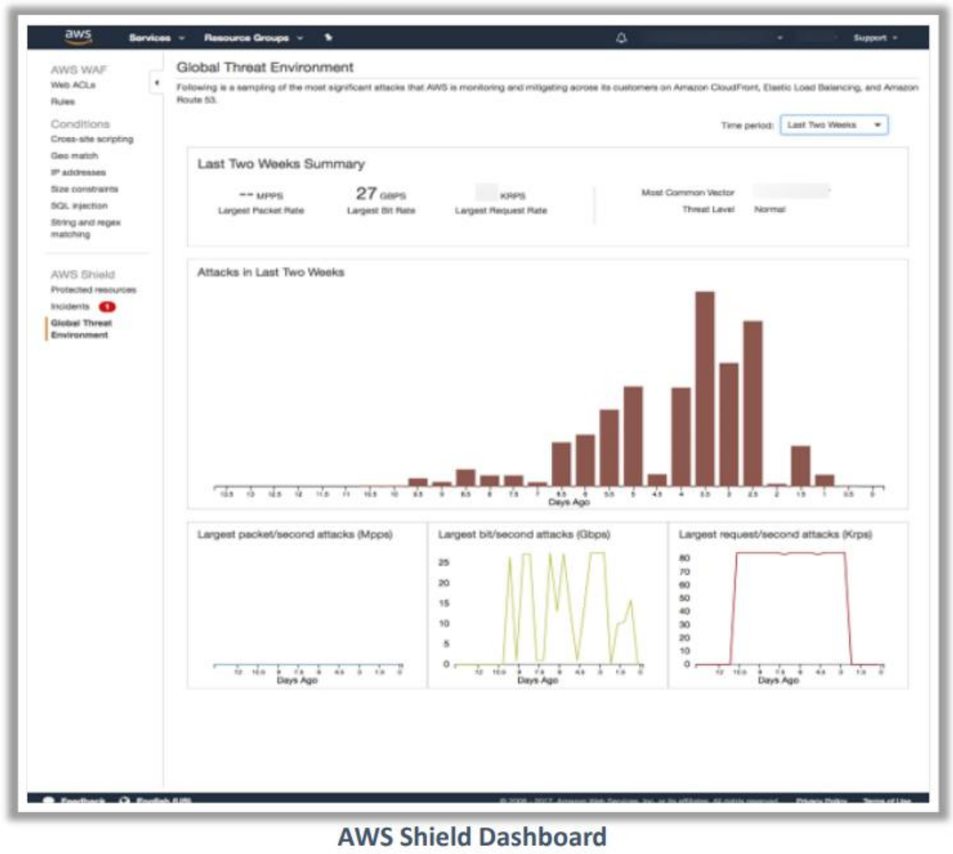
and high availability services to the users, so that availability in the CIA Triad can be met with CloudFront. CloudFront can be integrated with AWS Shield Advanced and AWS WAF to add extra layers of defense, which protects against most CVEs. CloudFront has security compliance certifications such as PCI DSS, HIPAA, SOC 1/2/3, etc.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

AWS Shield

- AWS Shield is a **managed DDoS protection** service to protect the applications on AWS
- All network layer and transport layer attacks can be prevented by using **AWS Shield standard** along with **AWS CloudFront** and **Route 53**
- AWS Shield reduces the **downtime** and latency of applications by providing always on detection and automatic inline mitigations
- **AWS Shield Advanced**, an advanced version of AWS Shield, can protect applications against major DDoS attacks, including a 24 ×7 response team



AWS Shield Dashboard

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

AWS Shield

The most critical attack that affects applications is a DDoS attack. AWS Shield is a service in AWS that can protect the application against DDoS attacks. It provides always-on detection and automatic inline mitigation, which can reduce the application's latency and downtime. AWS Shield Standard can protect the web application against most network layer and transport layer DDoS attacks.

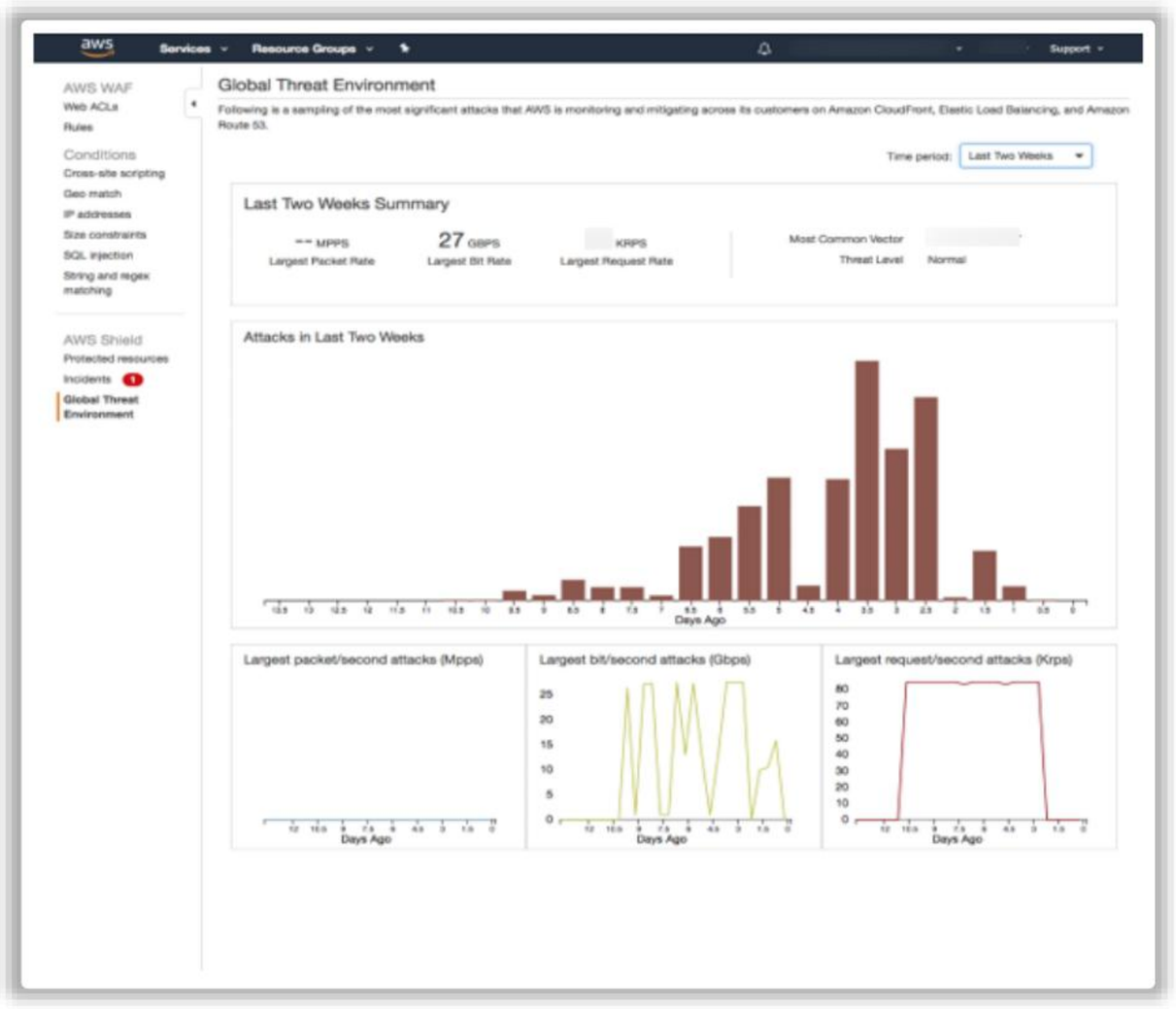


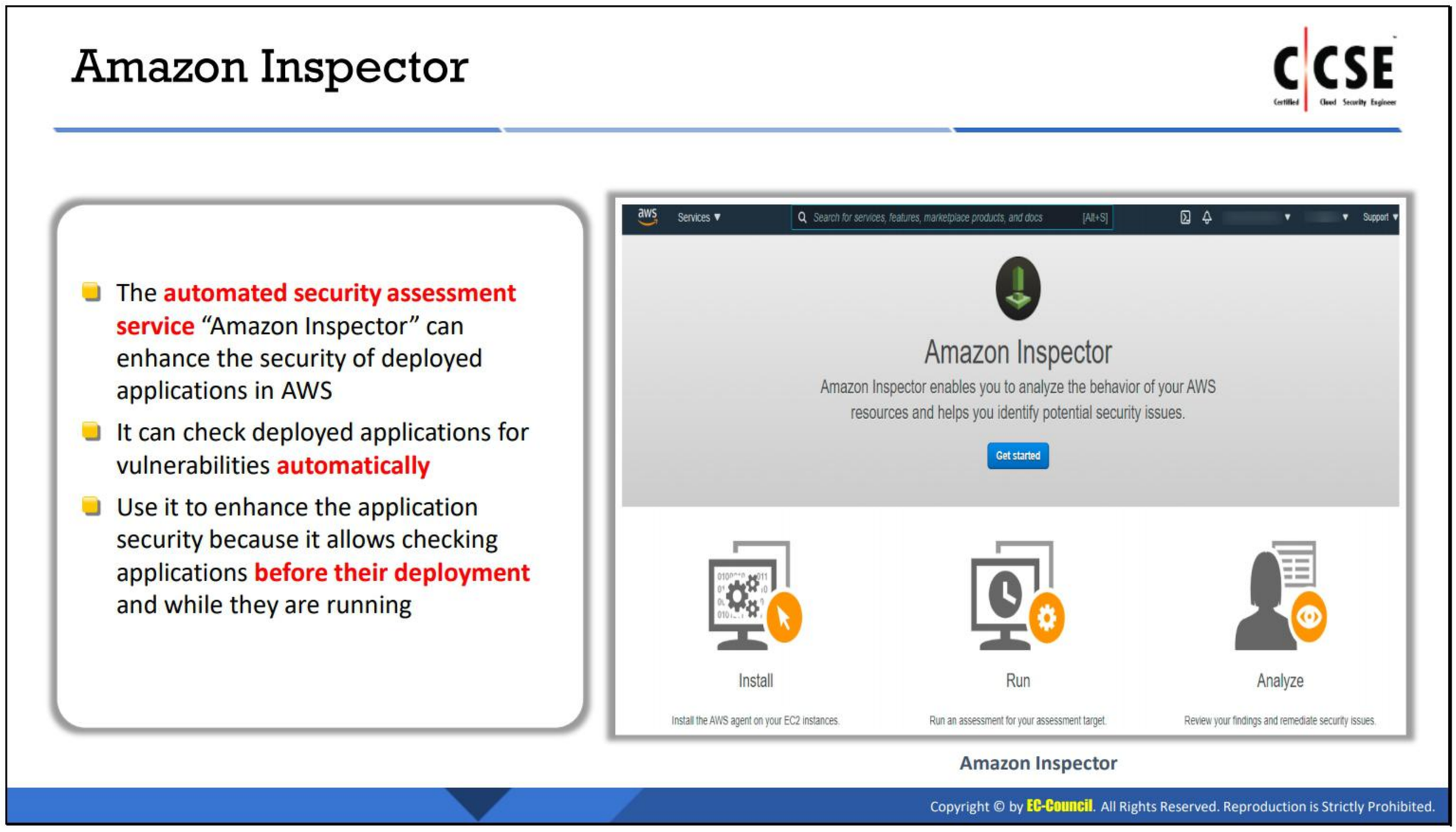
FIGURE 3.29: AWS Shield Dashboard

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

When AWS Shield is implemented along with CloudFront & Route 53 can protect the application against all layer 3 and layer 4 attacks. AWS Shield Standard is an advanced version of AWS Shield that can be used for DDoS protection if the applications are running on Amazon EC2, Elastic Load Balancing, CloudFront, or Route 53. AWS Shield Advanced has an additional capability of detecting and mitigating even the most complex DDoS attacks. It can also protect resources such as Amazon EC2 and Amazon Route 53 against DDoS-related traffic. Shield Advanced also provides a 24×7 AWS DDoS Response Team (DRT). With AWS Shield Advanced, all DDoS logs can be reviewed by AWS CloudWatch.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Amazon Inspector

An automated security assessment service to improve application security is Amazon Inspector. It can check the application for any kind of vulnerabilities or deviation from best practices automatically. Security vulnerabilities are listed based on the level of severities in Amazon Inspector.

hide01.ir

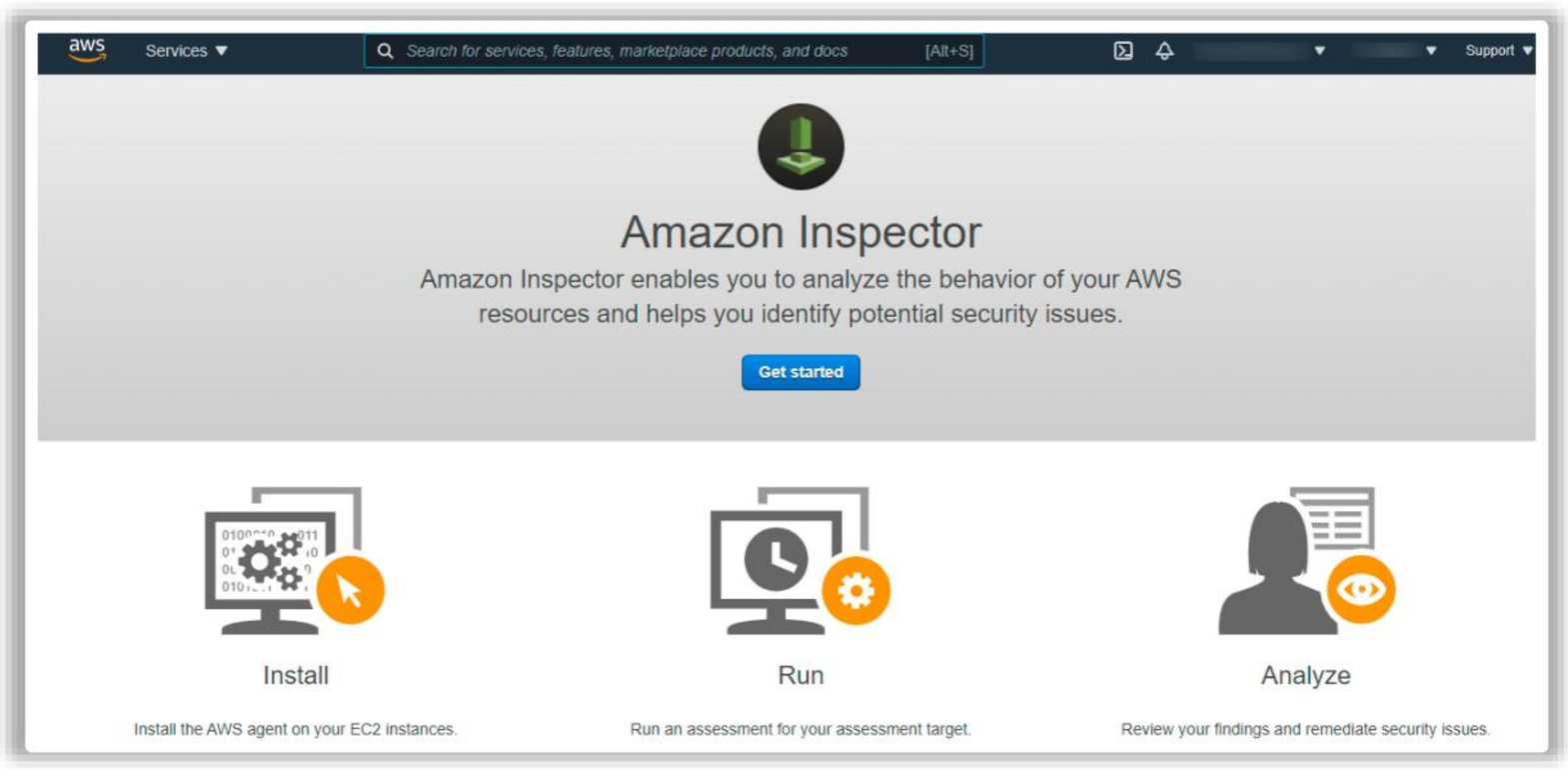


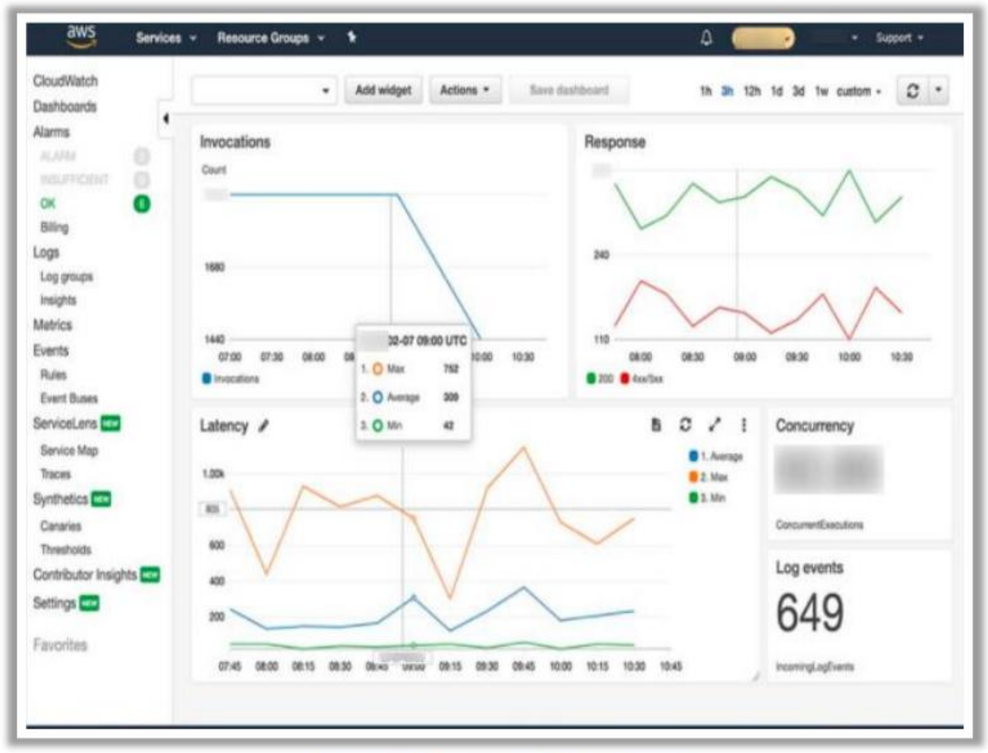
FIGURE 3.30: Amazon Inspector

Complete security of an application can be ensured as Amazon Inspector protects the application before deployment and in the running environment. Amazon Inspector provides the functionality of enforcing the best security standards and policies for the application. It can check for vulnerabilities or network accessibility issues in the application. Amazon Inspector has a database that consists of plenty of rules that are updated by security researchers.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Amazon CloudWatch

- Amazon CloudWatch provides the **data** and other insights for monitoring the applications
- The large data that is generated by applications that are running on AWS can be **collected, assessed,** and **correlated**
- CloudWatch provides data in the form of logs, metrics, and events about applications that run on AWS
- CloudWatch can detect any deviation of the application from normal behaviour as well as troubleshoot security issues
- The **health** and **performance** of the applications can be monitored; thus, smooth application performance is ensured



Amazon CloudWatch Dashboard

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

Amazon CloudWatch

Amazon CloudWatch provides the data and other insights for monitoring the applications. The extensive data that is generated by applications that are running on AWS can be collected, assessed, and correlated. CloudWatch provides data in the form of logs, metrics, and events about applications that run on AWS. CloudWatch can detect any deviation of the application from normal behavior as well as troubleshoot security issues. The health and performance of the applications can be monitored; thus, smooth application performance is ensured.

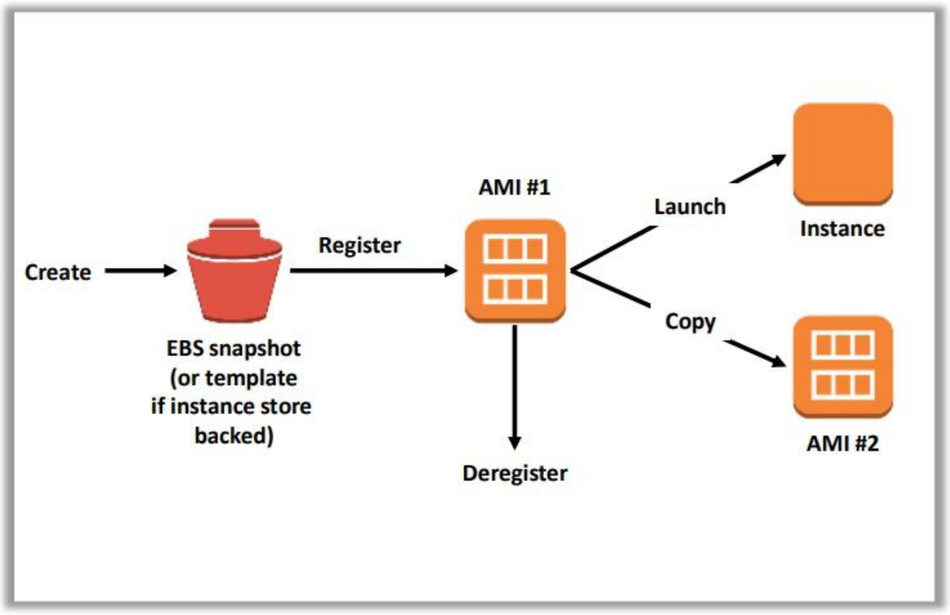
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Securing Amazon Machine Images (AMI)

- Amazon EC2 provides **scalable computing**, eliminating the need for hardware
- Amazon Machine Images (AMI) provides **preconfigured templates** for EC2 instances, which pack the bits required for the server

How to Secure the AMI

- Disable the insecure applications by disabling the services and protocols that **authenticate** the users insecurely
- Enable **essential services** on startup
- Delete all the AWS credentials and third-party credentials from the disk and configuration files
- Ensure that the installation of software is not done using **default** account names and passwords
- Ensure the system agrees to the **Amazon Web Services Acceptable Use Policy** (e.g., use of open SMTP relays/proxy servers)
- Control the incoming traffic to an instance using **Security Groups**



AMI Life Cycle

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

Amazon Machine Images (Contd.)

hide01.ir

Securing Linux /Unix AMIs

- Public key authentication must only be allowed by configuration of sshd
- In **sshd_config**, PubkeyAuthentication can be set to Yes and Password Authentication to No
- If AMI uses cloud-init, a unique **SSH host key** is generated on creation of instance
- For each user account, passwords can be disabled by running **passwd – l <USERNAME>**
- All user SSH public and private key pairs should be deleted
- The shell history and log files containing sensitive information must be deleted

Securing Windows AMIs

- Make sure that upon creation of a new instance, all the enabled user accounts have new **randomly** generated passwords
- For **Administrator** accounts, random passwords can be generated upon boot by the **EC2 Config Service**
- The **guest account** should be disabled
- All the windows event logs must be cleared
- The AMI should not be part of the Windows Domain
- All **nonessential services** such as file sharing, print spooler, and RPC should be disabled

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

Securing Amazon Machine Images (AMI)

Amazon Machine Image provides the essential information for launching an instance that includes

- One or more Amazon Elastic Block Store snapshots required for instance-store-backed AMIs with a root volume template of instance.
- Launch permission to control the use of AWS accounts to launch the instance.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- It requires block device mapping to specify the launch of the instance.

After creating and registering, the AMI can launch the instance and copy it into the same AWS region or another AWS region. After completing the task, you can deregister the AMI and search for other AMI that meets the required criteria of instance.

How to Secure AMI?

Following are the requirements to secure AMI:

- Disable the insecure application by disabling the services and protocols used to provide authentic access to the uses and create insecurity in the AMI environment.
- Enable essential services on startup to avoid confusion.
- Delete the AWS credentials and third-party credentials from the disk and configuration files that create a security breach.
- Avoid using default account names and passwords for installing software because they are easily detected and misused by the attackers.
- Ensure that the system does not violate the Amazon Web Service Acceptable Use Policy uses such as open SMTP relays or proxy servers.
- Ensure the use of security groups for controlling incoming traffics to the instance

How to Secure Linux/Unix AMIs?

Following are the steps used to secure Linux/Unix AMIs:

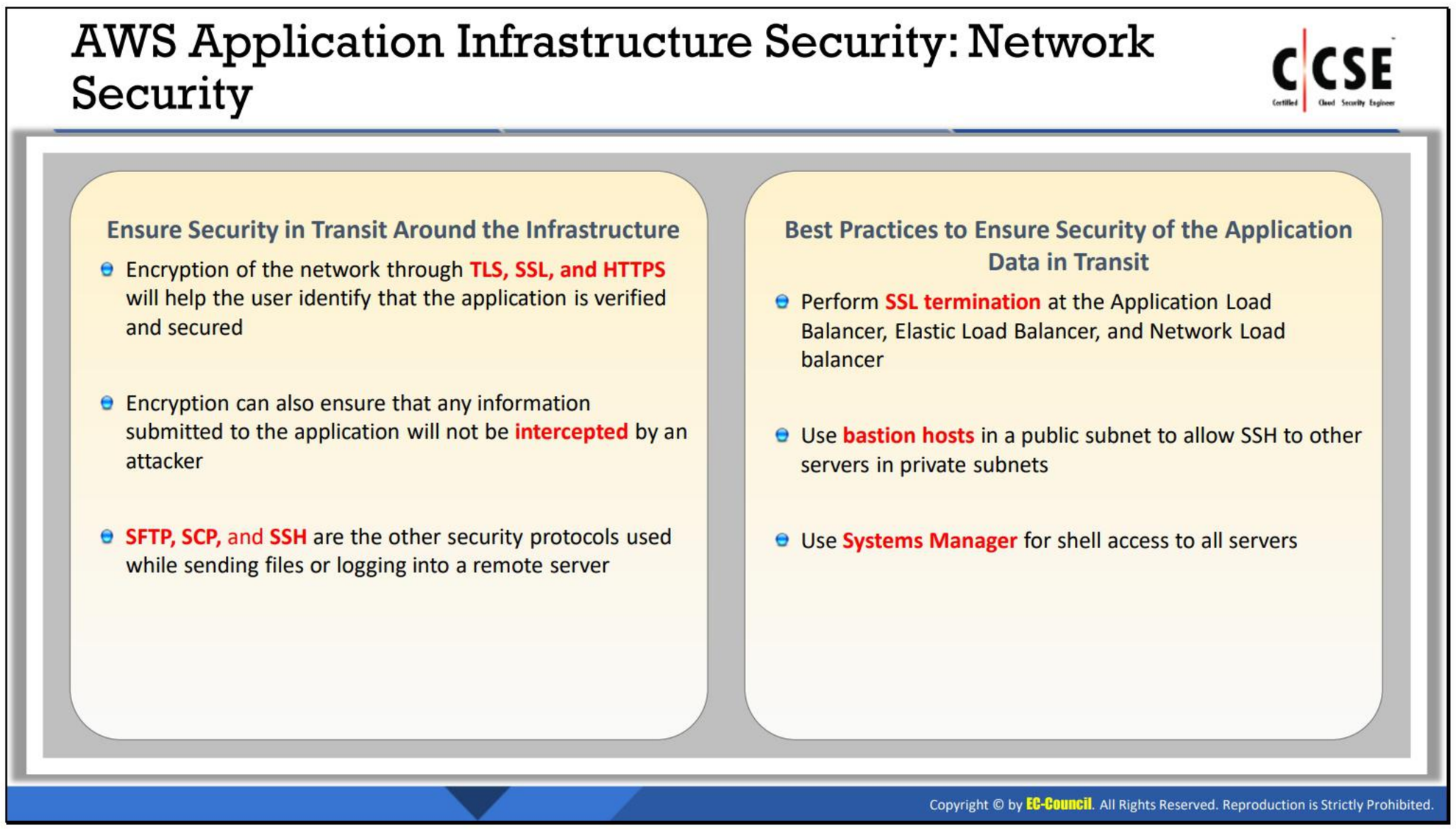
- Ensure that public-key authentication must be allowed by SSHD configurations only.
- Ensure that PubkeyAuthentication can be set to Yes and Password Authentication to No in the sshd_config.
- Generate a unique SSH host key while creating an instance when AMI uses cloud_init.
- Run `passwd -l <USERNAME> fo`r disabling user account passwords.
- Delete all user SSH public and private key pairs.
- Delete the shell history and log files containing sensitive information about the AMI.

How to Secure Windows AMIs?

Following are the steps to secure windows AMIs:

- Ensure that users get new randomly generated passwords while creating new instance.
- Ensure that random password is generated for administrator accounts by the EC2 Config service.
- Disable the guest accounts from the AMI.
- Delete windows event logs from the system for security.
- Ensure that AMI should not be a part of the windows domain.
- Ensure that nonessential services such as file sharing, print spooler, and RPC should not be enabled.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AWS Application Infrastructure Security: Network Security

To prevent security exploits on applications deployed in AWS, it is important to protect the infrastructure hosting the application. Application security should enforce the best practices for both security in transit and security at rest:

hide01.ir

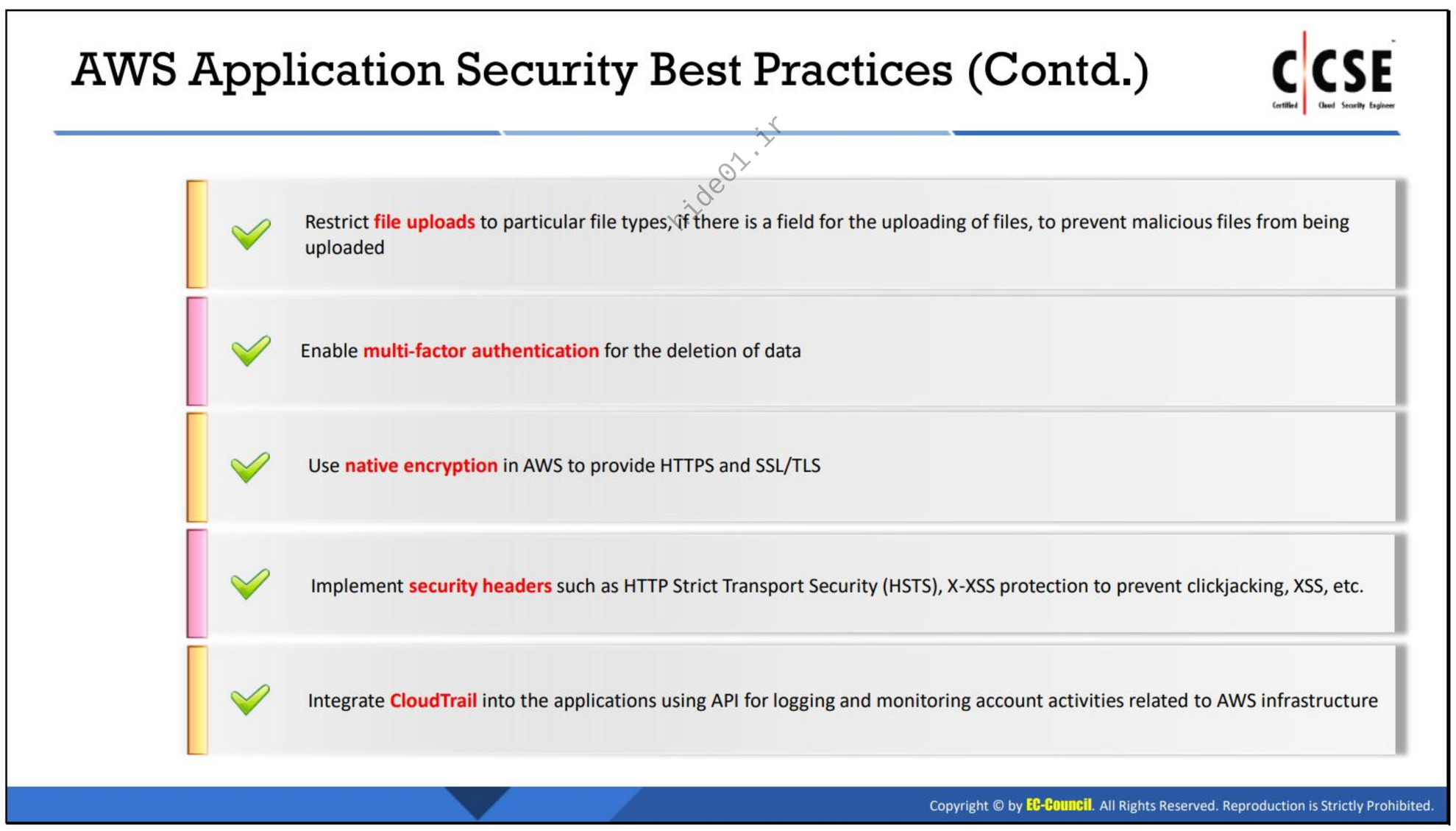
- For every point in the infrastructure, there should be security in transit.
- Wherever data is stored, there should be security of data at rest.
- Security exploits should be detected and responded proactively.

Application data while flowing through the internet is exposed to attackers listening to the network traffic to find and exploit the data. Internet traffic should be encrypted with HTTPS, SSL, and TLS to ensure that the application is verified and is protected from an attacker who might try to exploit it. Protocols such as SFTP, SCP, and SSH can be used when logging into a server automatically. The best practices for protecting the application infrastructure for security in transit are described below.

- **SSL termination at ALB, ELB, and NLB**: Enabling HTTPS listener can cause encryption between the load balancer and clients.
- **TLS encryption for all services**: TLS can be used to encrypt the communication between an application and Amazon Document DB cluster
- **Bastion hosts**: Bastion hosts can be used to allow SSH access to all other servers in private subnet.
- **Systems Manager for shell access to all servers**: Systems Manager provides secure access to EC2 instances.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





AWS Application Security Best Practices

To ensure applications that run on AWS are safe and secure, it is essential to follow security best practices related to cloud applications. Some of the best practices that ensure application security are described below.

- **Prevent information disclosure**: The leakage of user credentials and source code is due to insecure security practices on the application. To mitigate the disclosure of the version

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

of the operating system, it should be ensured that the services running on open ports do not reveal that information. Sensitive information that is not necessary to display on the web application interfaces should not be uploaded. Strong password policies and proper access control mechanisms are also necessary for protection against information disclosure.

- **Detect code vulnerabilities**: An insecure code can lead to vulnerabilities in the application even though all the security resources are deployed on the application. Synk, a SaaS platform, can fix and monitor open-source applications' vulnerabilities. Synk can fix vulnerabilities in containers and Kubernetes applications. Synk has an updated vulnerability database supported by machine learning and crowdsourcing. Thus, applications can be kept secure.
- **Perform penetration testing**: Even if all the security measures are deployed, a single vulnerability can make the application insecure. It is always better to do a vulnerability assessment and a penetration test on the application to find and fix any security loophole.
- **Restrict the file upload types**: Web applications having fields for uploading certain files must be restricted only to that file type. Allowing uploads of any type of file may compromise the webserver on which applications are deployed.
- **Enforce MFA**: MFA can be enabled for account logins and for the deletion of data. This can prevent accidental deletion of data by administrators as well as prevent unauthorized access and information disclosure.
- **Encrypt sensitive information**: AWS native encryption provides HTTPS and SSL/TLS for application security. It is always recommended to use encrypted connections when exchanging sensitive information.
- **Utilize security headers**: Various attacks, such as clickjacking and XSS, can be prevented by the implementation of security headers. They can provide an improved layer of security against those risks. These headers are sent along with the HTTP response of the server that informs the browser how to handle the content of the website. Security headers include HTTP Strict Transport Proxy (HSTS), X-XSS protection, and content security policy.
- **Integrate CloudTrail with apps**: It is essential to perform logging and monitoring of activities in the AWS account to ensure its overall security. This can be achieved by integrating CloudTrail into apps that use APIs. CloudTrail helps in ensuring governance, compliance, risk auditing, and operational auditing of the AWS account. Actions across the AWS infrastructure can be continuously logged and monitored, including actions performed through the AWS Management Console.

hi1e01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#07: Learn How to Implement Application Security in AWS

The objective of this section is to explain the implementation of application security in AWS using various AWS products and services.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AWS IAM: Lock Your AWS Account Root User Access Keys

The access key (an access key ID and secret access key) allows making programmatic requests to AWS. But it is not recommended to use the AWS account root user access key as it can provide full access to all your resources for all AWS services. You cannot reduce the permissions associated with your AWS account root user access key.

hidx01.ir

Secure Root User Access Key

To protect root user access key, use the following guidelines.

- **Do not create AWS account root user access key unless required or if you do not have it already**. Use the email address and passwords of account to sign-in to the AWS Management Console and create an administrative IAM user.
- **Change the AWS account root user access key regularly or delete** it if you already have.

  Steps to delete or rotate root user access keys, include the following:

  - Go to the My Security Credentials page in the AWS Management Console.
  - Sign-in with your account's email address and password.
  - Manage access keys in the Access keys section.
- **Never share the AWS account root user password or access keys** to avoid having to embed them in an application.
- **Use strong passwords for logging into AWS Management Console**.

  Steps to use strong passwords:

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select your account name or number and then choose “My Account” in the upper right corner of the AWS Management Console.
- Select **Edit** on the right side of the page next to the **Account Settings** section.
- Select **Edit** to change your password on the **Password** line.
- AWS requires that your password must meet the following conditions:
  - Password has a minimum of 8 characters and a maximum of 128 characters.
  - Password should include a minimum of three of the following mix of character types: uppercase, lowercase, numbers, and ! @ # $ % ^ & * () <> [] {} | _+-= symbols.
  - Password should not be identical to your AWS account name or email address.

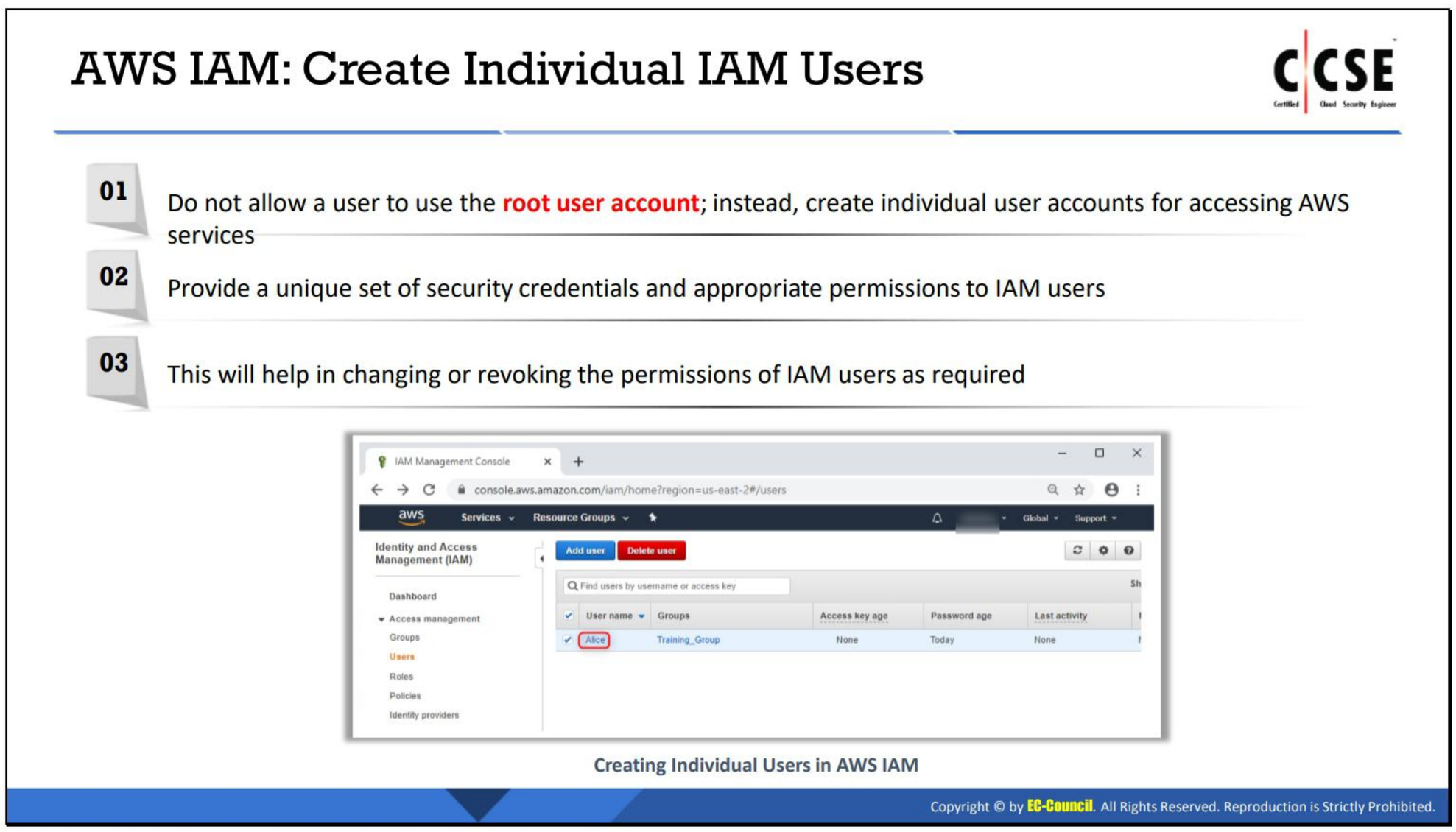
- **Enable AWS MFA on AWS account root user account.**

  Steps for enabling MFA devices are described below:

  - Get an MFA device such as one of the following. You can enable only one MFA device per AWS account root user or IAM user.
    - Virtual MFA device
    - U2F device
    - Hardware-based MFA device
    - Mobile phone
  - Enable the MFA device.
    - For IAM users with virtual or hardware MFA devices, enable from the AWS Management Console, AWS CLI, or the IAM API.
    - For IAM users with U2F security keys or a mobile phone that can receive SMS text messages, enable from the AWS Management Console only.
    - For AWS account root users with any type of MFA device (except SMS MFA), enable from the AWS Management Console only.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AWS IAM: Create Individual IAM Users

It is recommended to avoid using the AWS root user account to access AWS. Instead, create individual user accounts for accessing AWS. Create an IAM user for yourself as well, give that user administrative permissions, and use that IAM user for all your work. Give the IAM user a unique set of security credentials and different permissions to each IAM user. Change or revoke an IAM users' permissions if needed.

Steps to create a new IAM user are described below:

- Select **Users** from the **Identity and Access Management (IAM)** section and click **Add user** to create a new user.

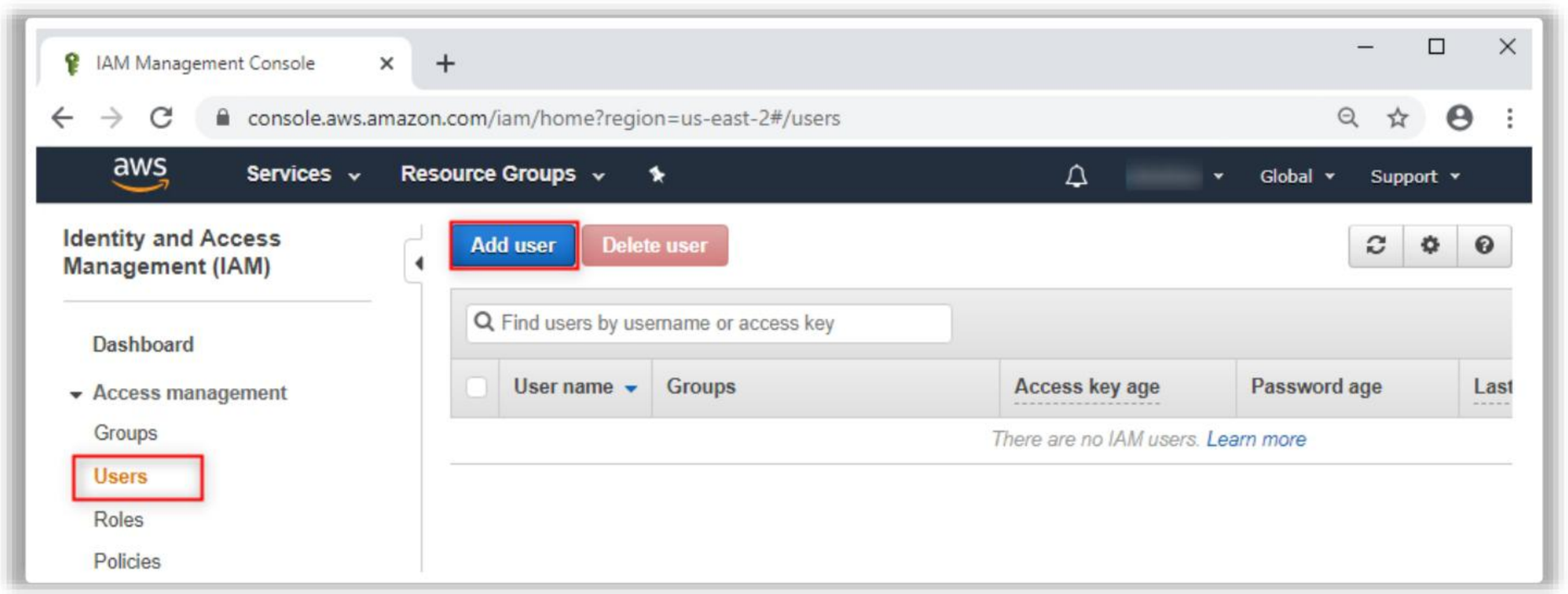
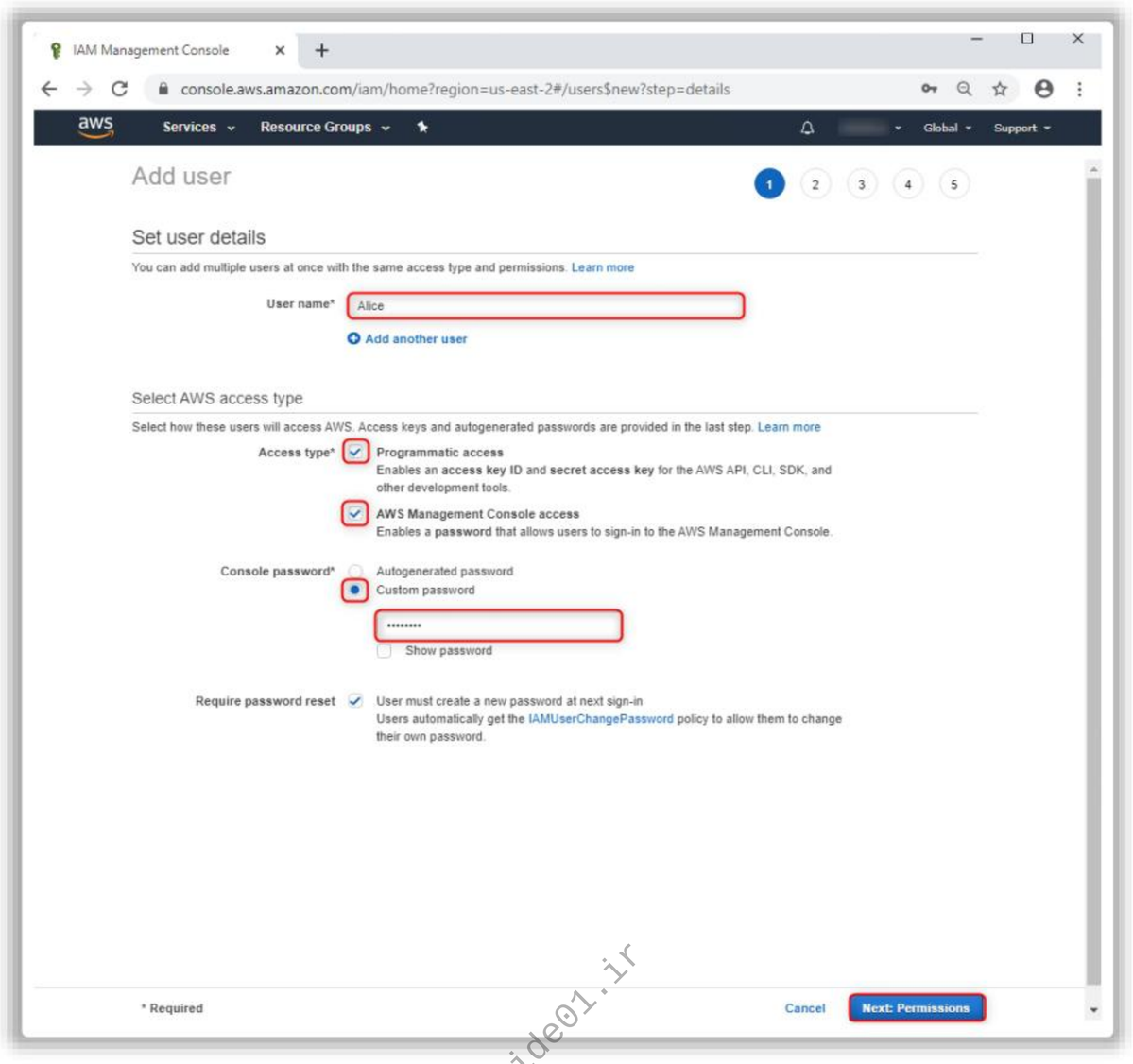


FIGURE 3.31: AWS IAM

- In the **User** name field, provide any name (here, **Alice**).

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- For **Access type**, give Alice **AWS management Console access** under **Select AWS access type** section. Choose the **Custom password** radio button and provide the password in the Password field. The **Require password reset** is optional; however, enable this setting. Click **Next Permission.**



hide01.ir

FIGURE 3.32: AWS Access Type

- Under **Set permissions** section, **Add user to group** option is selected by default. Check newly created group (here, **Training_Group**), which will allow you to add the user to the group. Click **Next: Tags**.

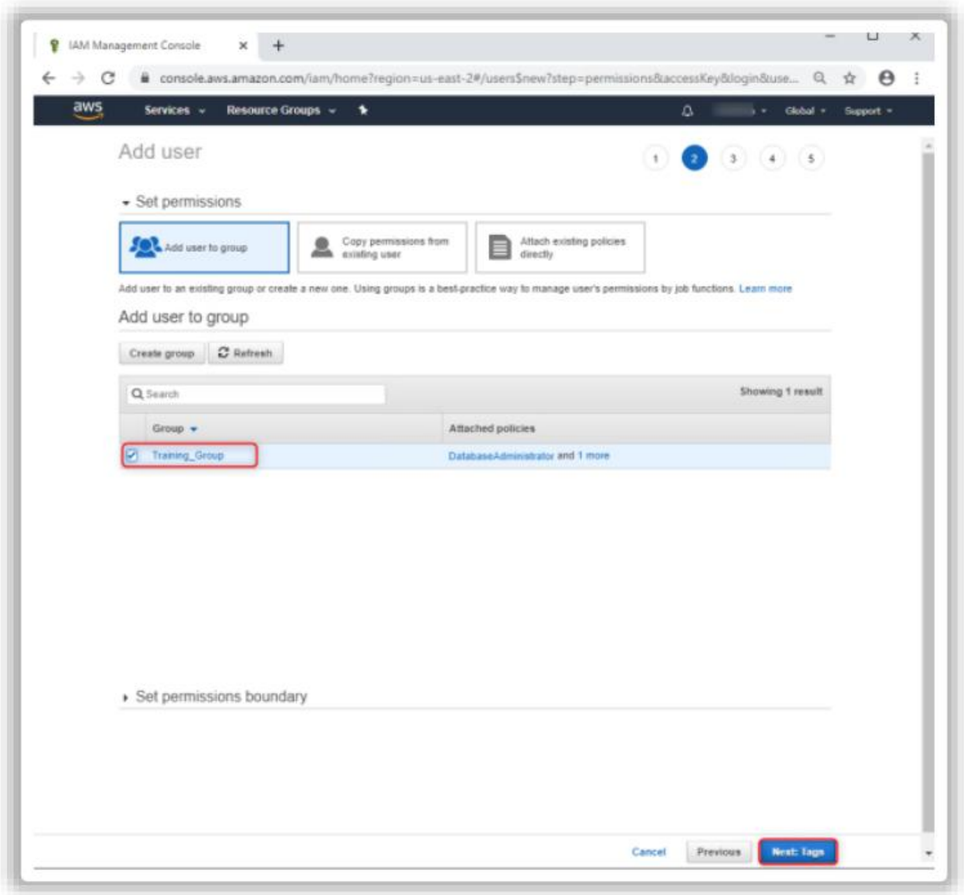


FIGURE 3.33: Set Permissions

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Tags are optional; however, tagging allows searching for tag keys later on easily. Specify **Department** as **Tag Key** and **Key-Value** as **Training**. Click **Next: Review** to proceed with reviewing IAM user creation.

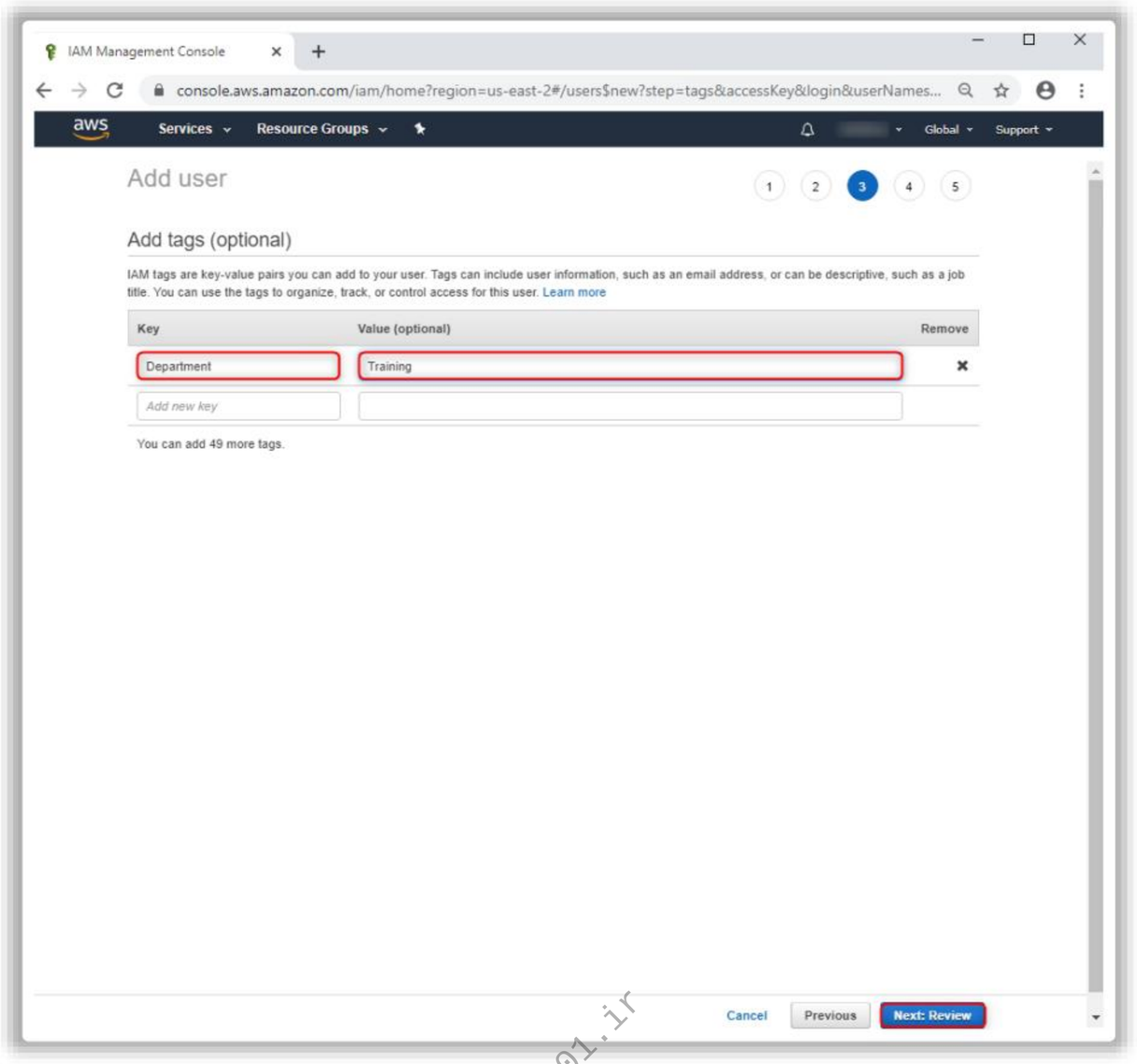


FIGURE 3.34: Adding Tags

- Having verified the settings on the Review page, click **Create user**.

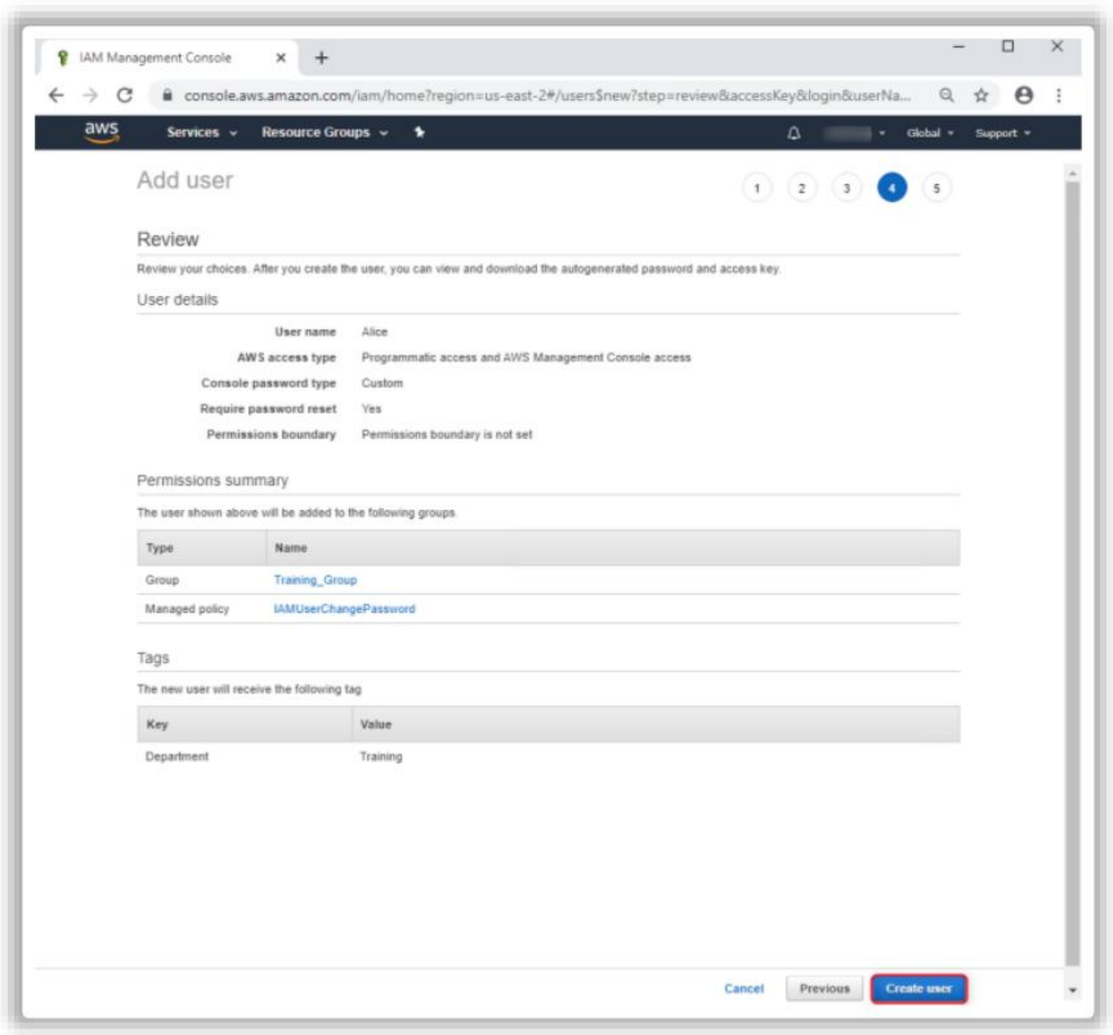


FIGURE 3.35: Review

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- After clicking **Create user**, a success message is displayed.

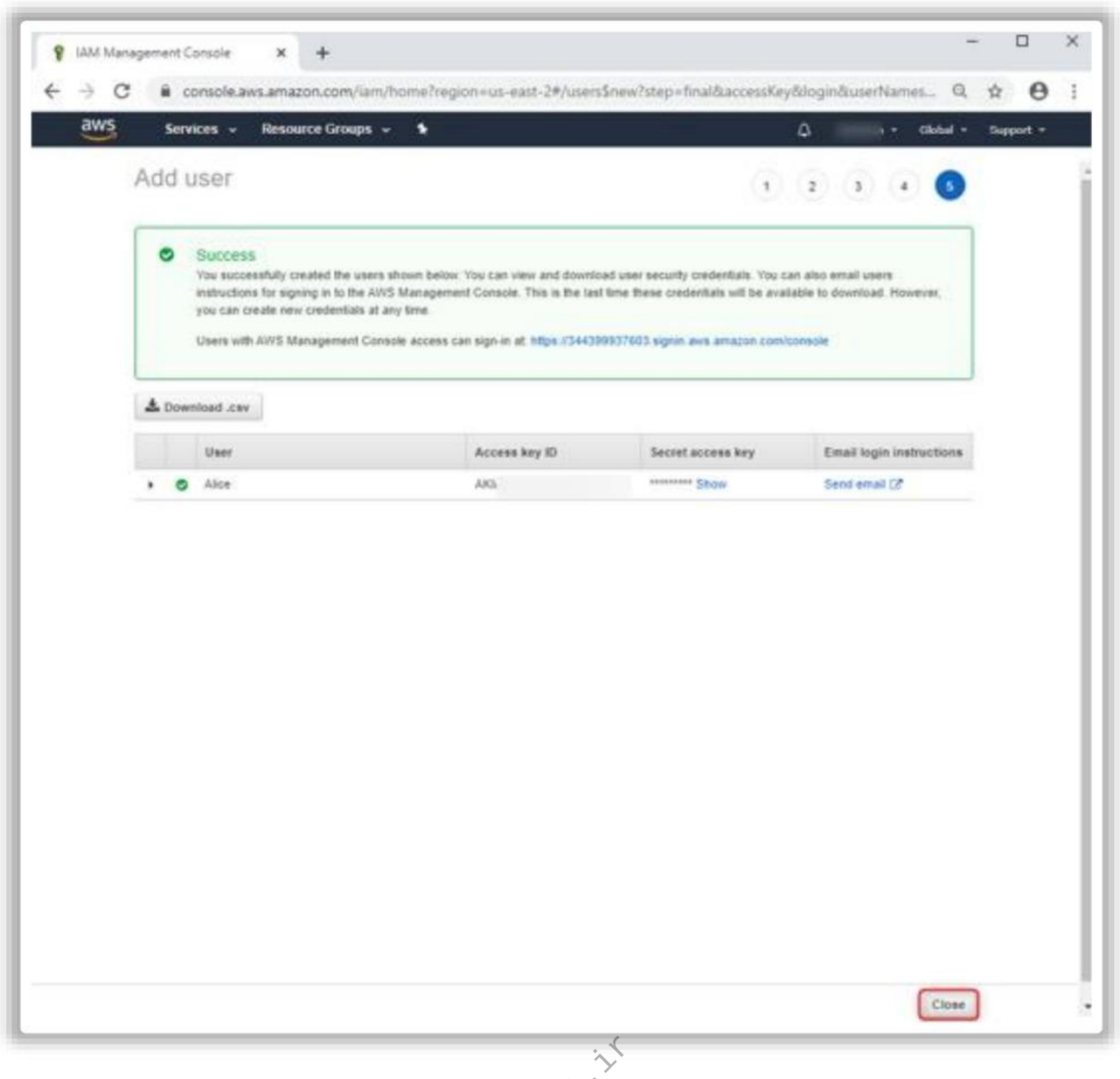
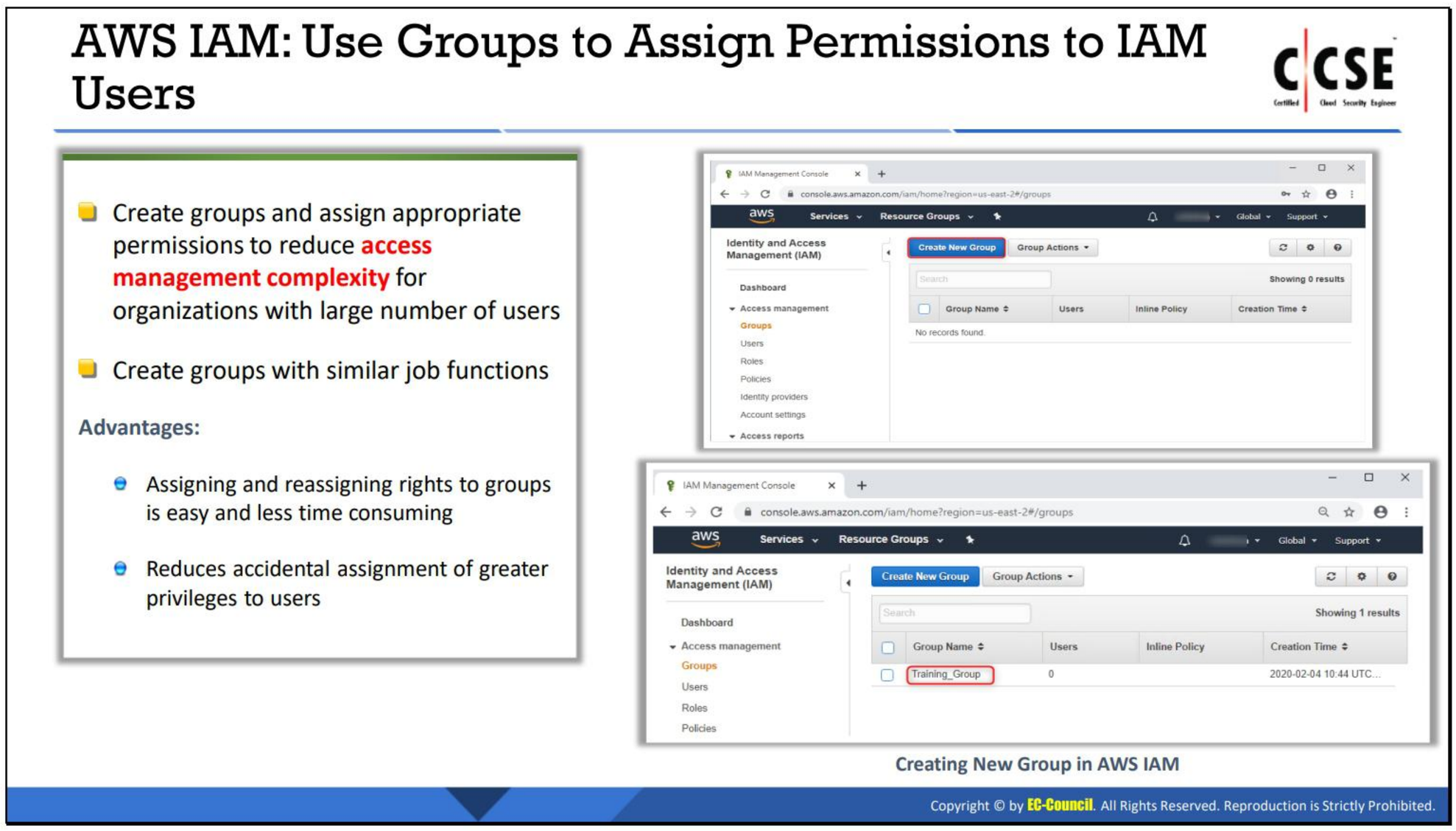


FIGURE 3.36: Created New User

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Creating New Group in AWS IAM

AWS IAM: Use Groups to Assign Permissions to IAM Users

Granting permissions for each individual IAM user can be a hard task. Instead, create groups and define them specific rights and permissions. Add IAM user accounts to those groups based on their job functions. Through this, modification to the IAM users of specific group can be done at one place. It reduces access management complexity for organizations with large number of users and also reduces accidental assigning of greater privilege to users. Assigning and reassigning rights to groups is easy and less time consuming. If the user is changed from one role to the other role, then IAM user account in one group can be changed to that specified group.

Steps to create a new IAM Group are described below:

- Click **Groups** in the left pane under **Identity and Access Management (IAM)** in Identity and Access Management.

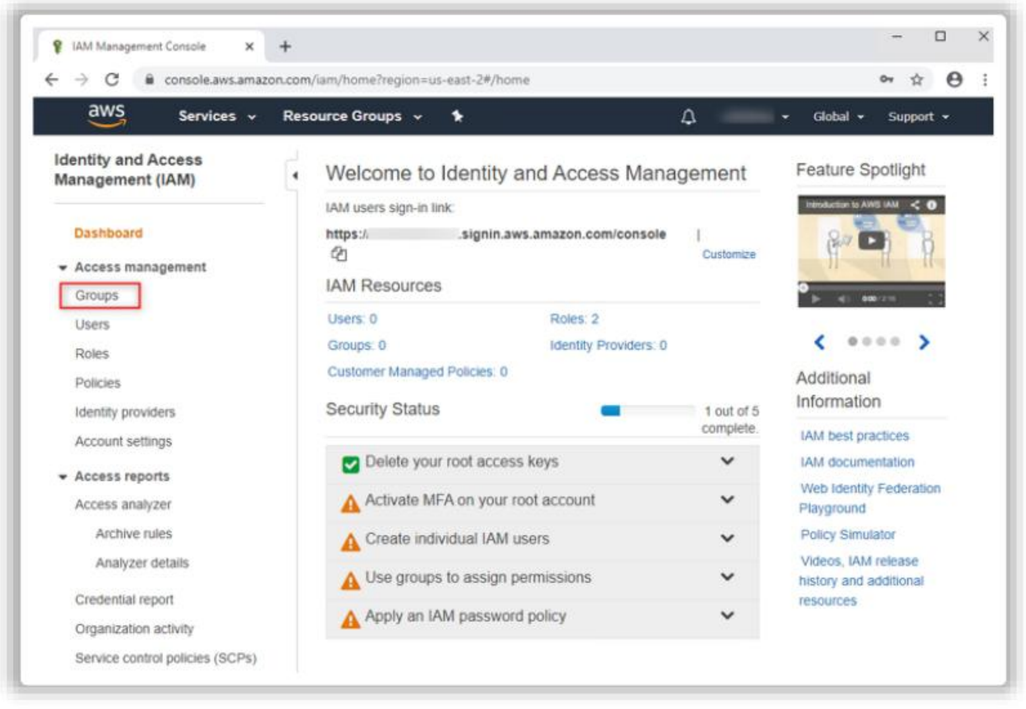


FIGURE 3.37: AWS IAM

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click **Create New Group**.

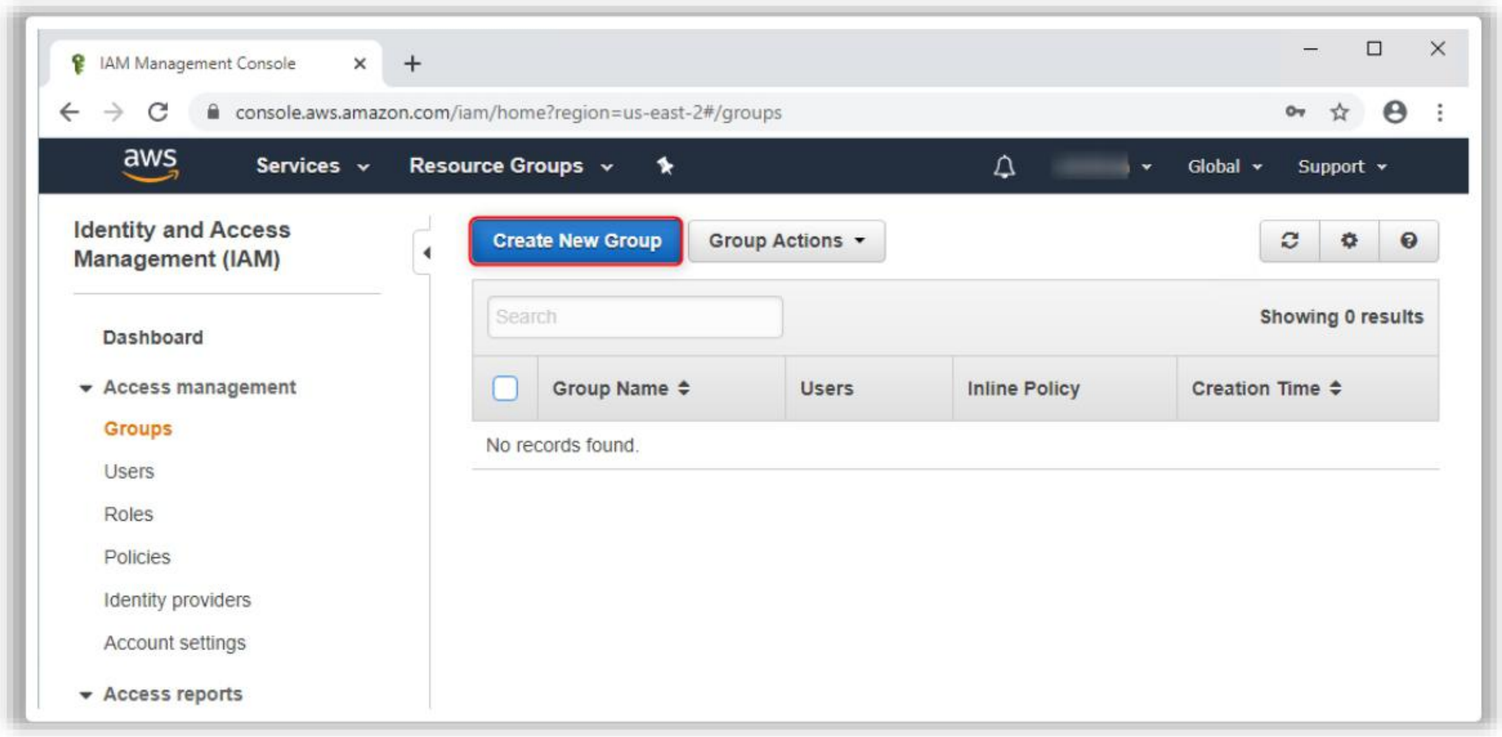


FIGURE 3.38: Create New Group

- Under **Set Group Name** section, type the group name in the **Group Name** field (here, **Training_Group**) and click **Next Step**.

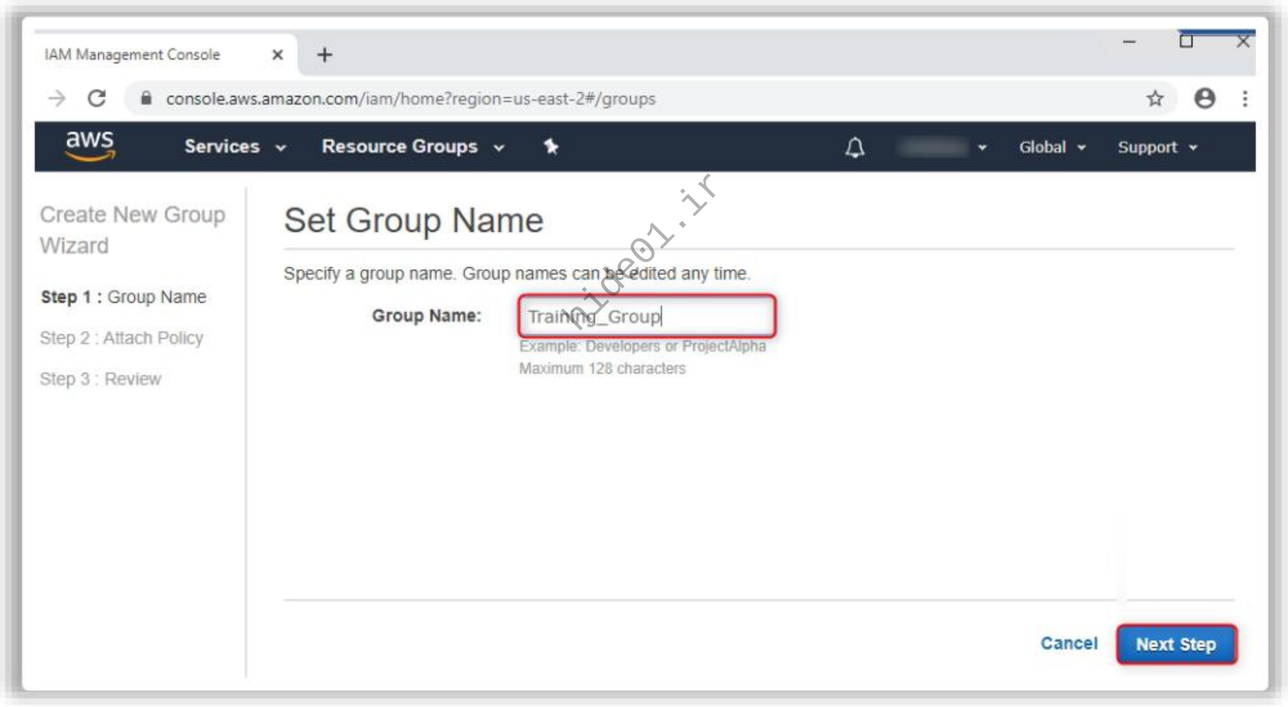


FIGURE 3.39: Set Group Name

- In the **Attach Policy** section, search for **iamuserchangepassword** and the match record gets filtered, check **IAMUserChangePassword**.

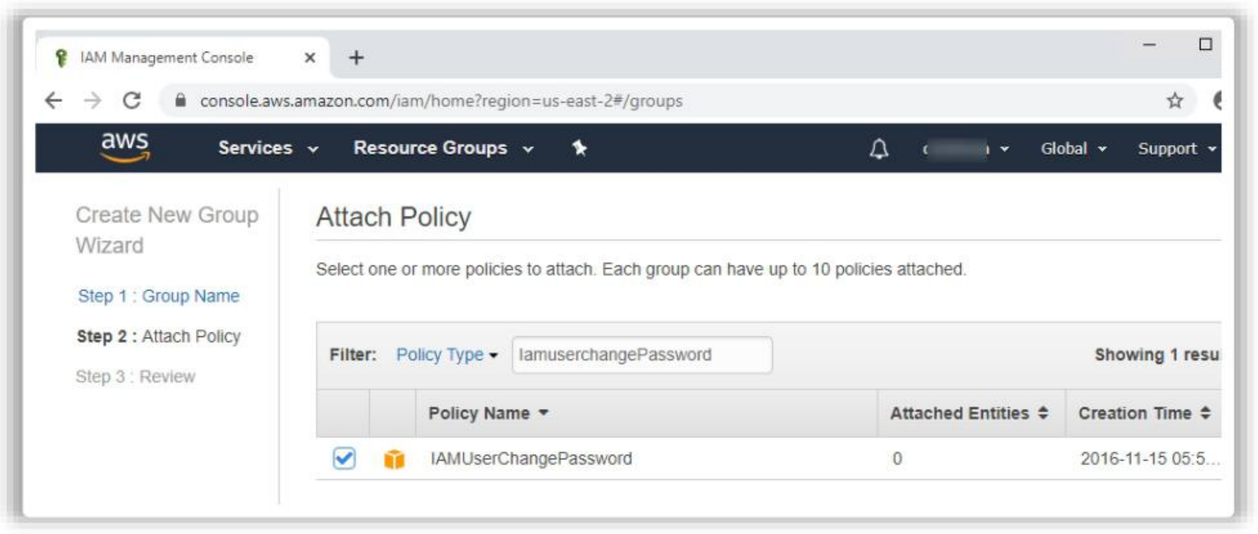


FIGURE 3.40: Attach Policy

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Search for **databaseadministrator** and the match record gets filtered, check **DatabaseAdministrator**, click **Next**.

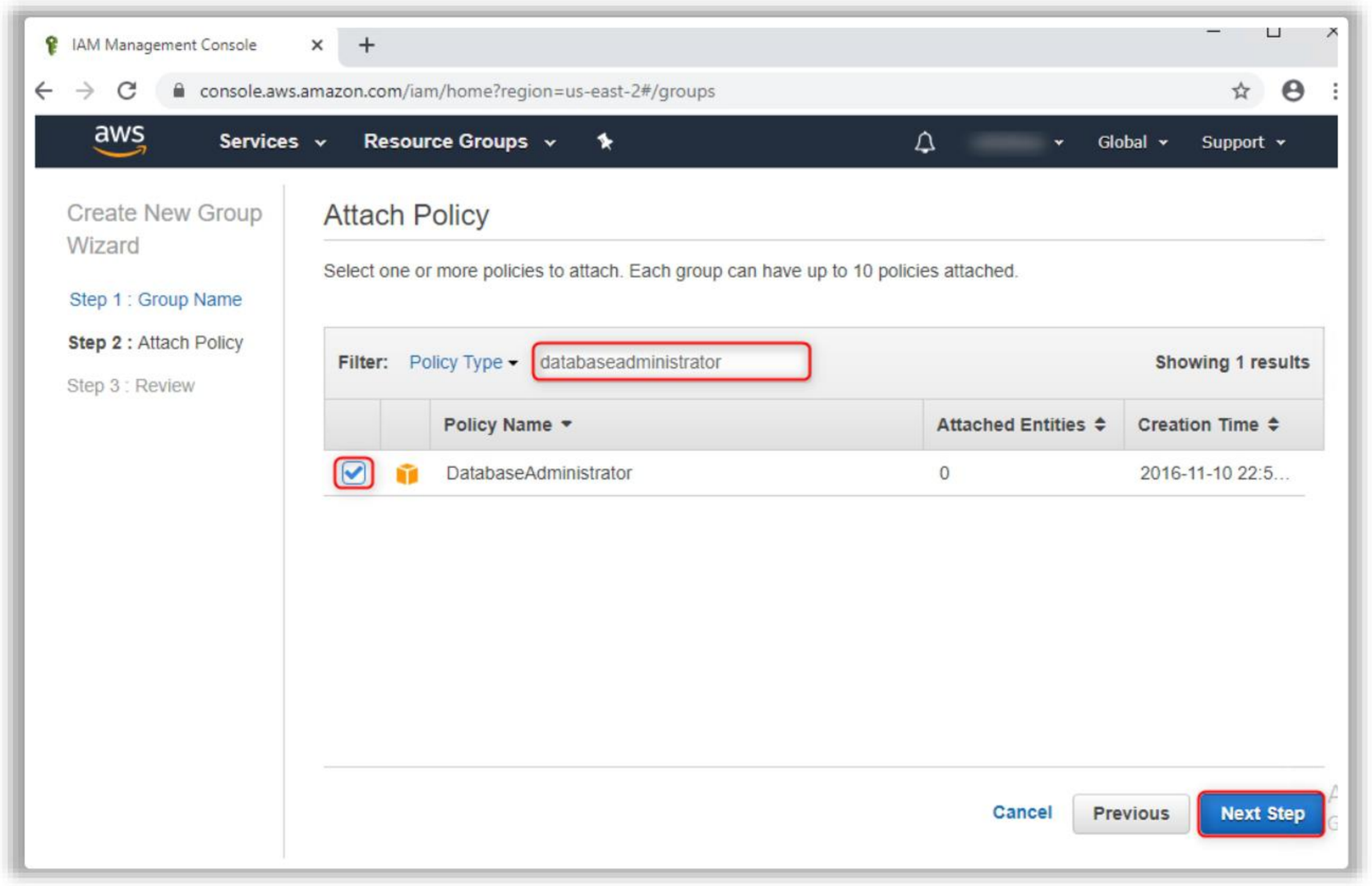


FIGURE 3.41:Search Databaseadministrator

- In the **Review** section, two policies are added. Click **Create Group**.

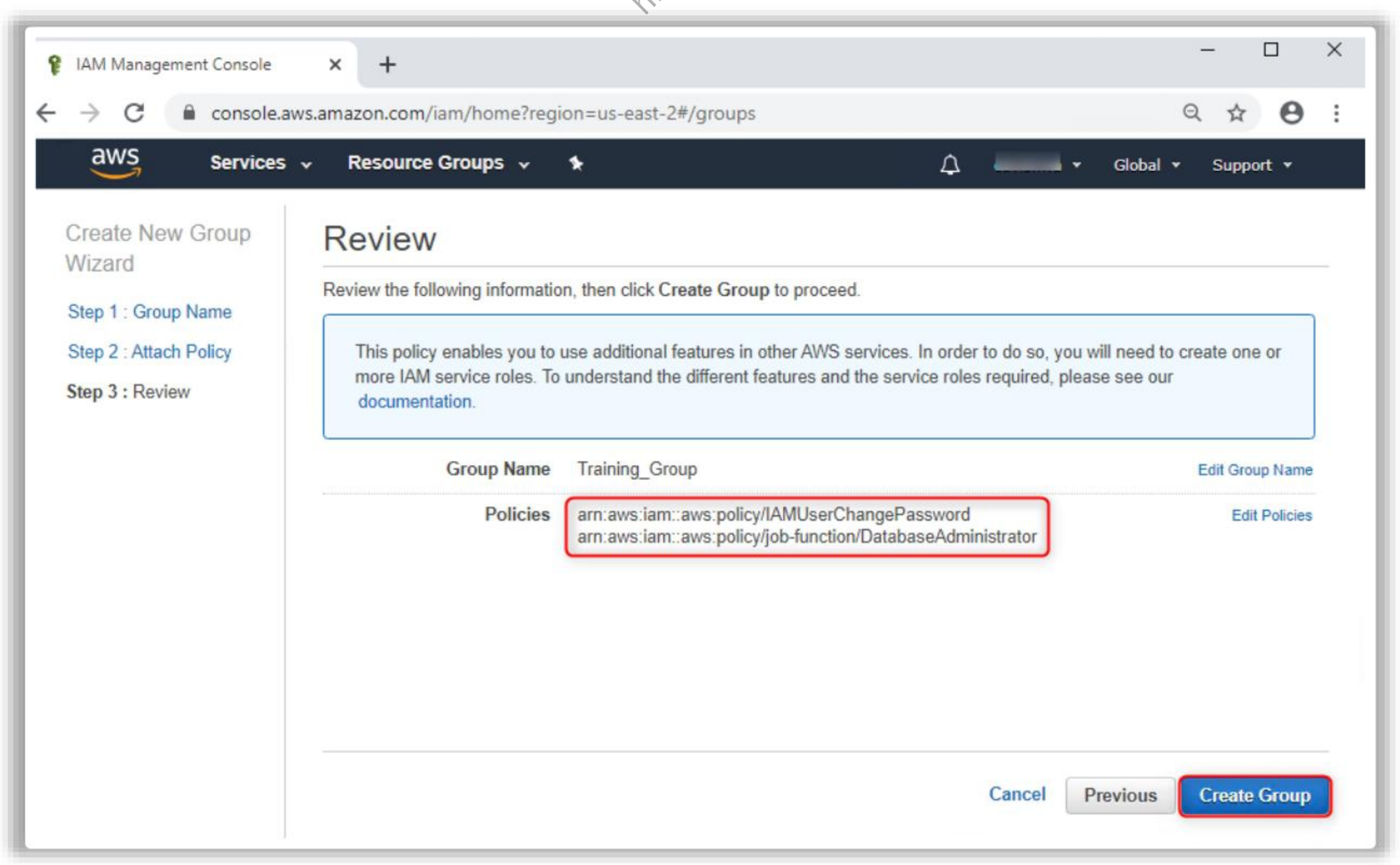


FIGURE 3.42: Review

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The **Training_Group** is created under **Groups**.

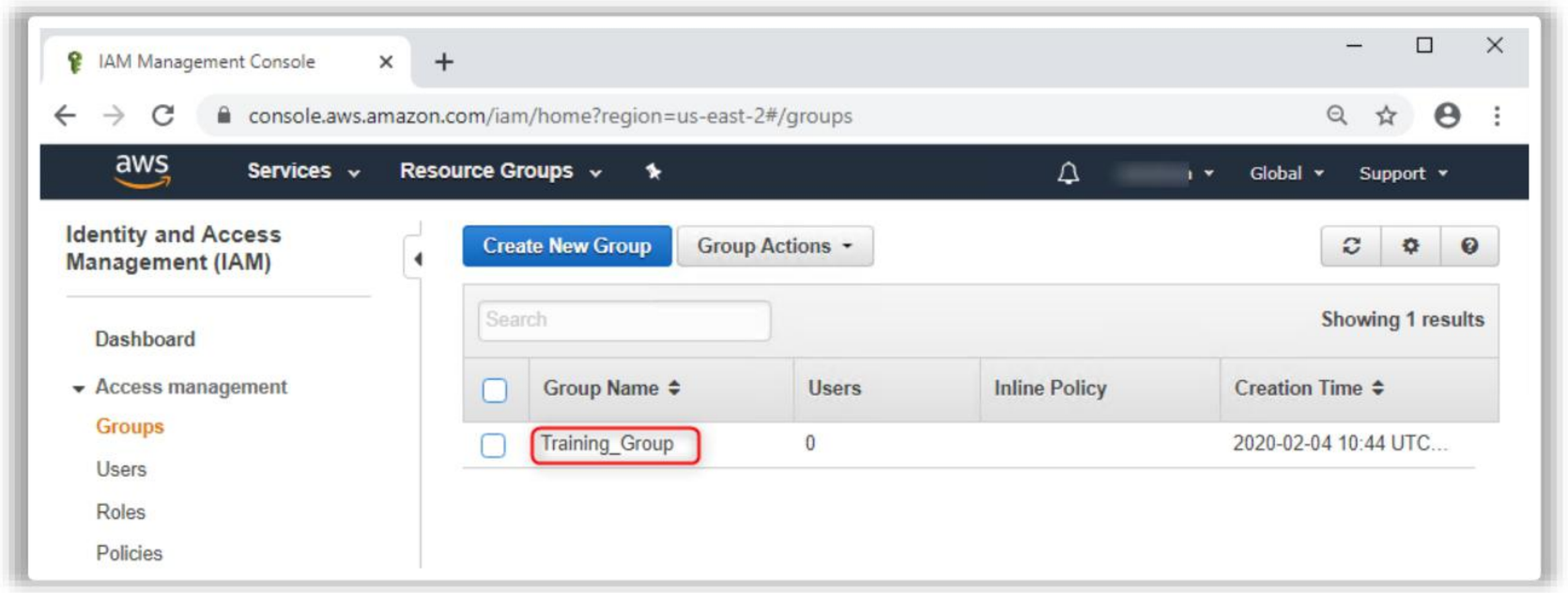
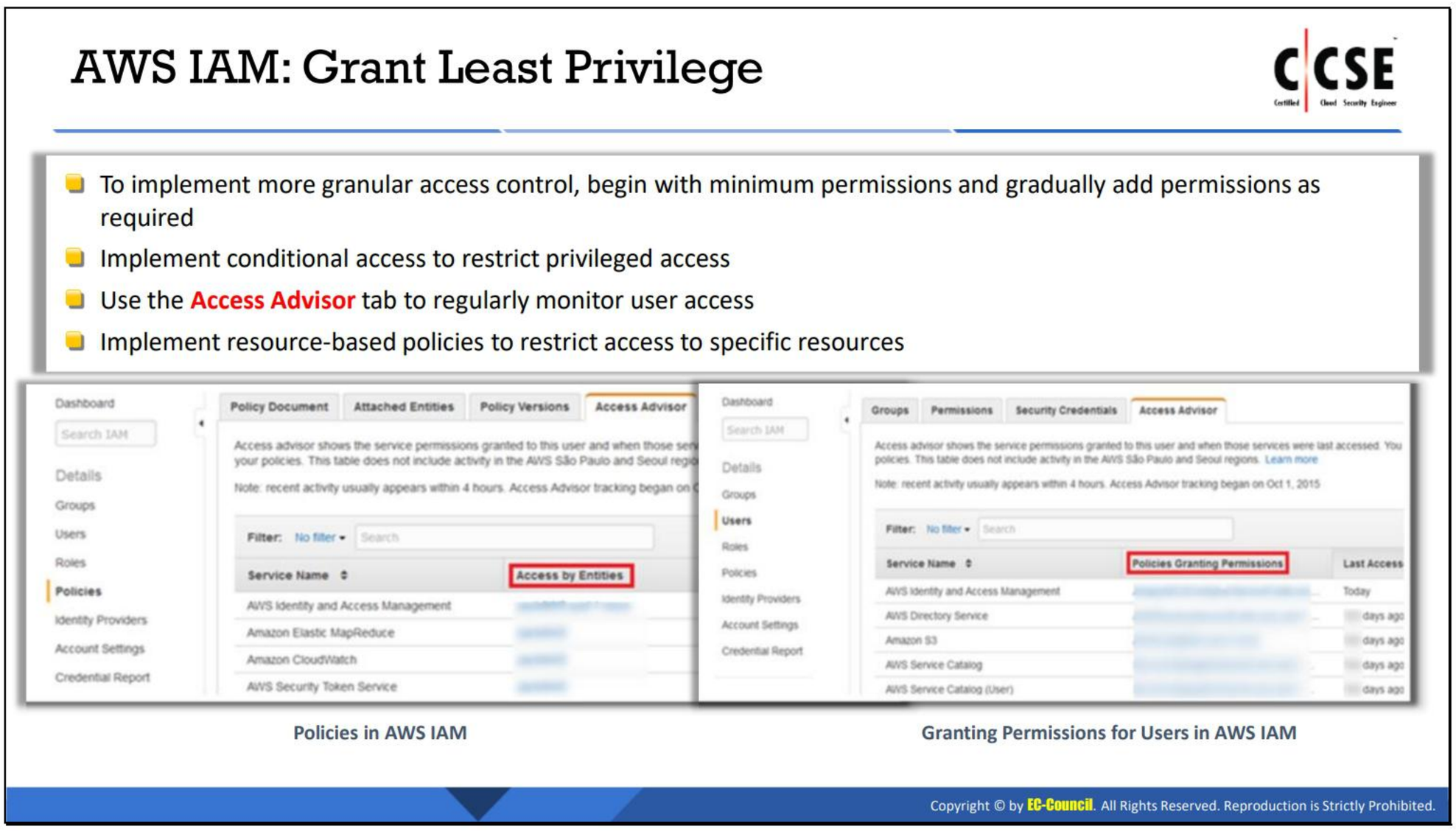


FIGURE 3.43: Created New Group

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Policies in AWS IAM

Granting Permissions for Users in AWS IAM

AWS IAM: Grant Least Privilege

When IAM policies are created, the permissions need to be granted only to perform required tasks. Determine the roles of the users and craft the policies accordingly. Starting by giving minimum permissions can be more secure. Extend the permissions later if needed. Types of policy actions include List, Read, Write, and Permissions management, and Tagging. For example, if the actions are chosen from the List and Read access levels, they are used to grant read-only access to your users. The following are examples of the actions of policies and their descriptions.

The service last accessed data feature can be used to view the data on the Access Advisor tab on the IAM console. The same data can be viewed on the AWS Organizations section of the IAM console if the user is logged in with master account credentials. Use this information to view the unnecessary permissions so that they can be refined accordingly. Use the account's events in AWS CloudTrail Event History to apply further granular permissions.

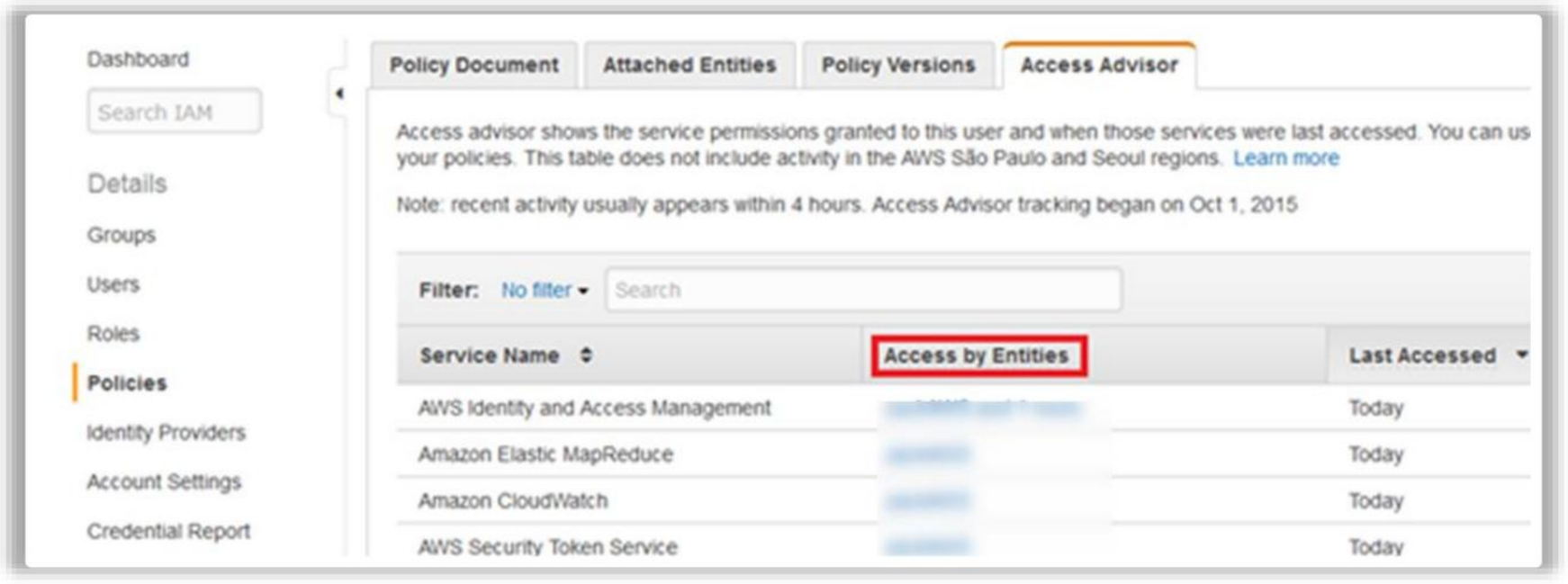


FIGURE 3.44: Access by Entities

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

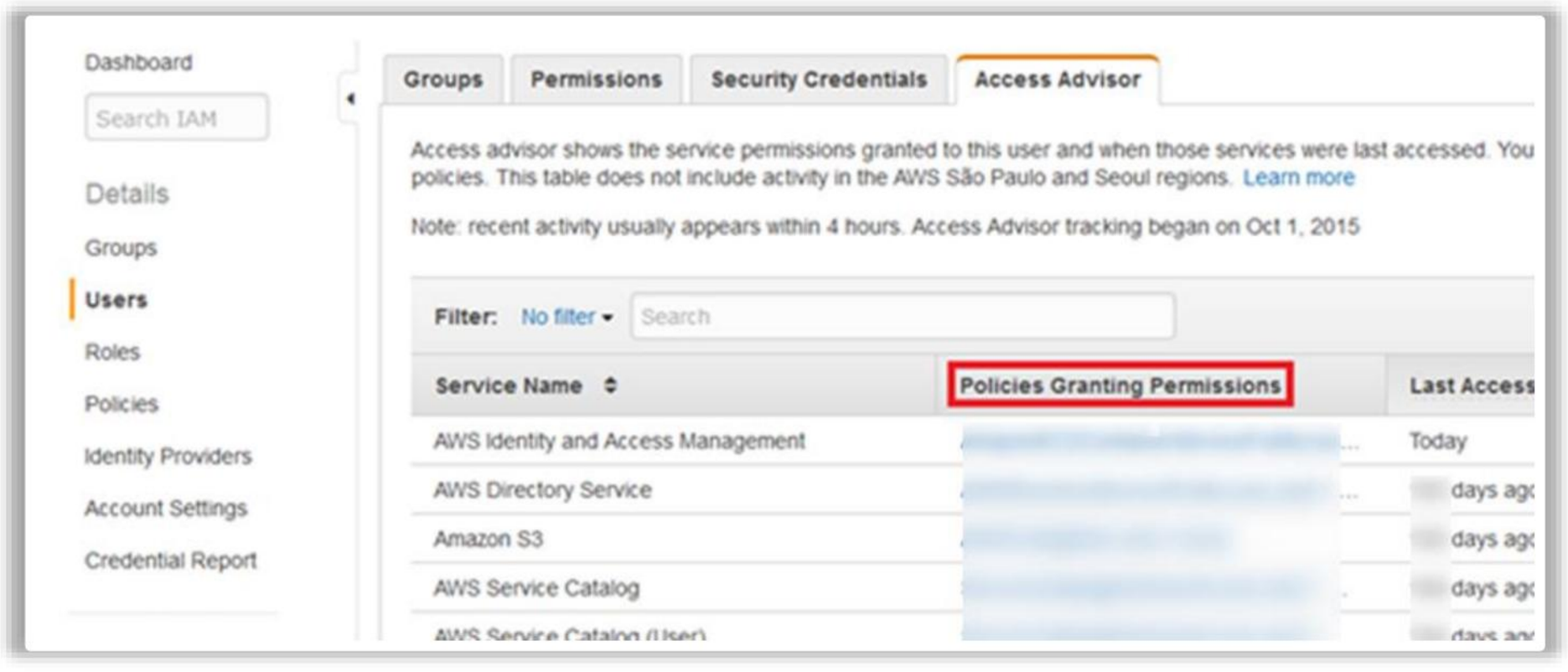
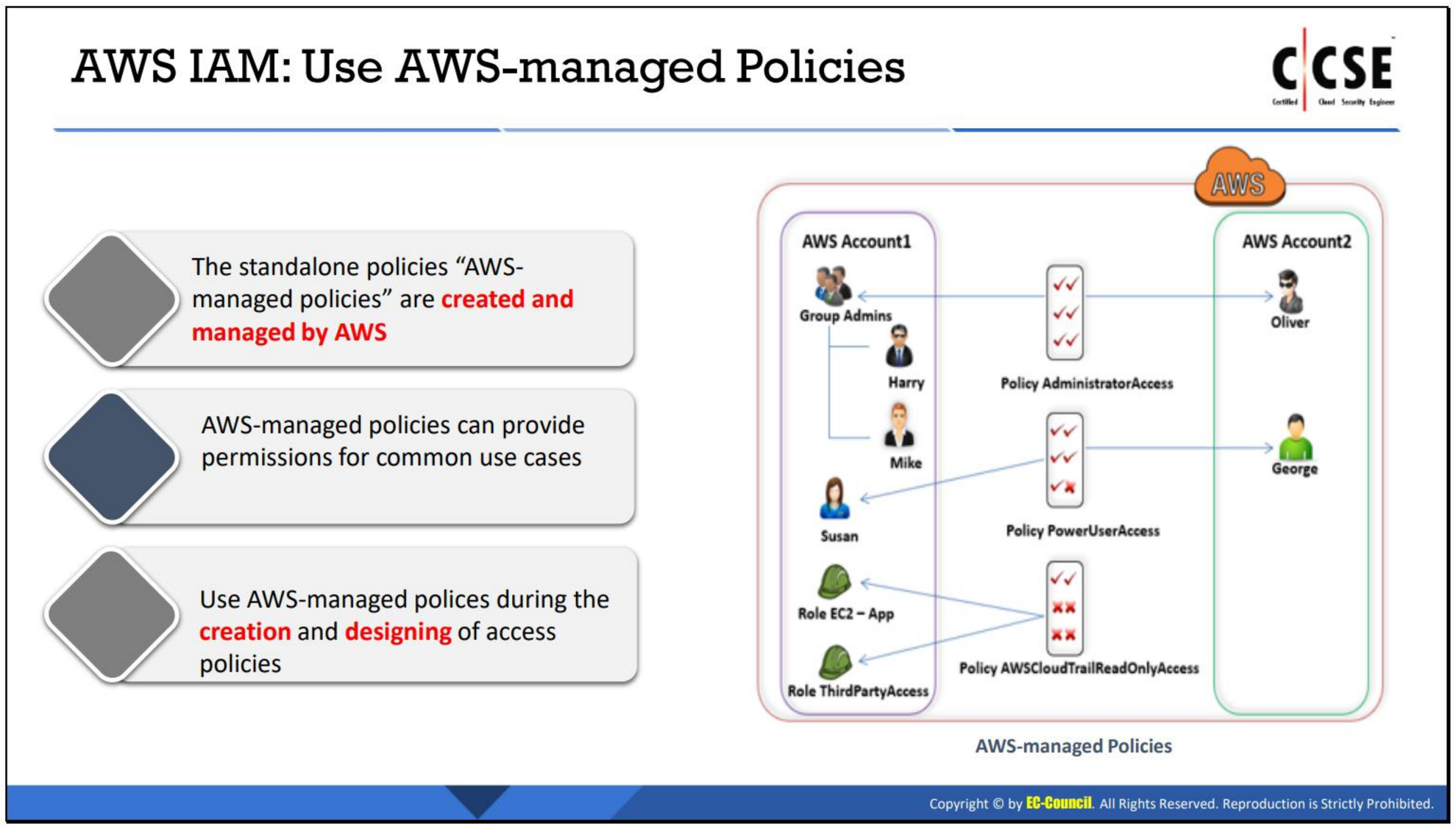


FIGURE 3.45: Policies Granting Permissions

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AWS IAM: Use AWS-Managed Policies

Administrators need some time to understand the policies and provide them to the employees to perform the required tasks. They need to have a better understanding of the IAM policies and they should test IAM before implementation. Users also need to be aware of the tasks they need to perform and understand the permissions they are granted.

For a better understanding, AWS-managed policies provide permissions to the users and make them familiar with the tasks they need to perform with the granted permissions. AWS-managed policies (standalone policies that are created and administered by AWS) are helpful in designing and creating access policies.

The AWS-managed policies provide permissions for many common use cases:

- **Full access AWS-managed policies** define permissions for service administrators by granting full access to a service. For example policies, AmazonDynamoDBFullAccess and IAMFullAccess.
- **Power-user AWS-managed policies** provide multiple levels of access to AWS services without allowing permissions management permissions. For example, AWSCodeCommitPowerUser and AWSKeyManagementServicePowerUser policies.
- **Partial-access AWS-managed policies** provide specific levels of access to AWS services. For example policies, AmazonMobileAnalyticsWriteOnlyAccess and AmazonEC2ReadOnlyAccess.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

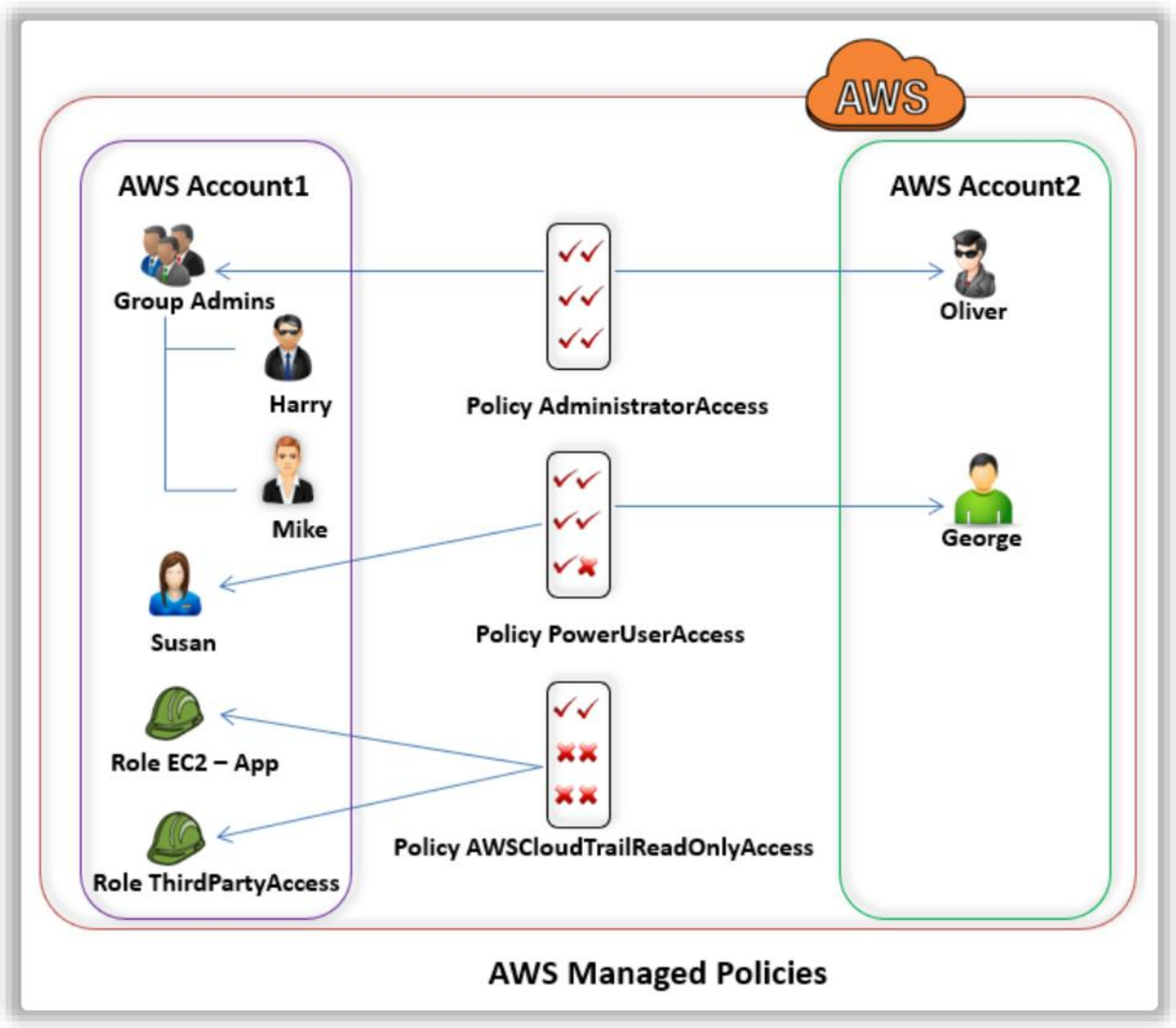


FIGURE 3.46: AWS Managed Policies

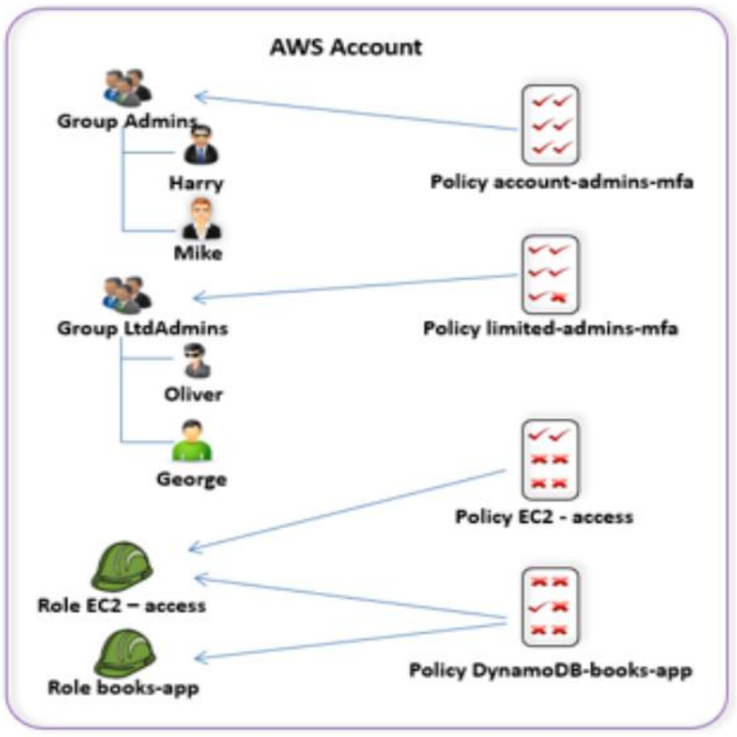
The above diagram shows three AWS-managed policies: AdministratorAccess, PowerUserAccess, and AWSCloudTrailReadOnlyAccess. Here, a single AWS-managed policy is attached to principal entities in different AWS accounts and different principal entities in a single AWS account.

hidden.if

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

AWS IAM: Use Customer-managed Policies Instead of Inline Policies

- The policies **"Inline Policies"** exist only on an IAM identity (user, group, or role)
- Customer-managed policies are **standalone policies** created by the administrator to administer their AWS account
- Customer-managed policies can be attached to multiple principal entities in an AWS account
- You can view all managed policies in one console



Customer-managed Policies

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

AWS IAM: Use Customer-managed Policies Instead of Inline Policies

Customer-managed policies are standalone policies created and added to multiple principal entities in an AWS account, allowing the entity the permissions defined in the policy. The better way to use a customer manage policy is to copy the existing AWS-managed policy and customize it if needed.

hide01.ir

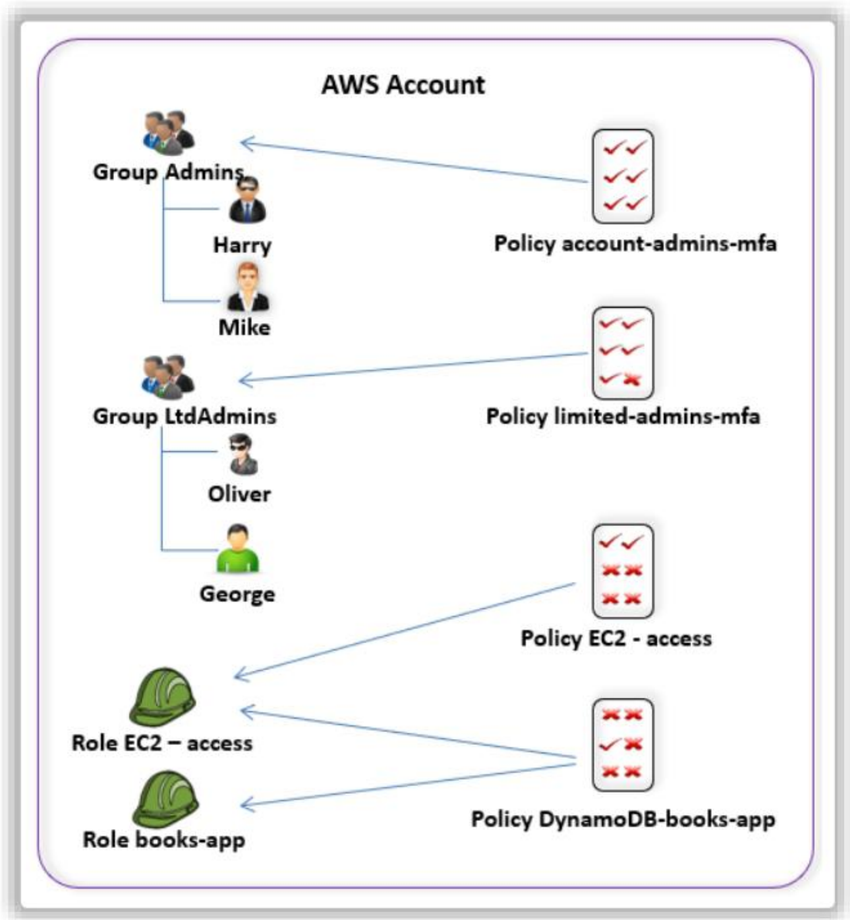


FIGURE 3.47: Customer Managed Policies

The above diagram shows that each customer-managed policy is an entity in IAM with its own Amazon resource name (ARN) that includes the policy name. Here, the same policy same (DynamoDB-books-app) is attached to multiple principal entities or two different IAM roles.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Managed Policies Features

- **Reusability:** A single managed policy can be attached to multiple principal entities.
- **Central change management:** A change in a managed policy also applies to all principal entities that the policy is attached to.
- **Versioning and rolling back:** A change to a customer-managed policy/a changed customer-managed policy does not overwrite the existing policy. Instead, IAM creates a new version of the managed policy. These policy versions help revert a policy to an earlier version when needed.
- **Delegating permissions management:** Users in your AWS account can be allowed to attach and detach policies while maintaining control over the permissions defined in those policies.
- **Automatic updates for AWS-managed policies:** AWS manages policies by updating them automatically when needed. These updates are applied to the principal entities to which the AWS-managed policy is attached.

Inline Policies

Inline policies refer to policies that are embedded in principal entities (user, group, or role). These policies are an inherent part of the principal entities. It is possible to create an inline policy and embed it in a principal entity while creating the principal entity or later. These policies help maintain a strict one-to-one relationship between a policy and the principal entity that it is applied to.

hide01.ir

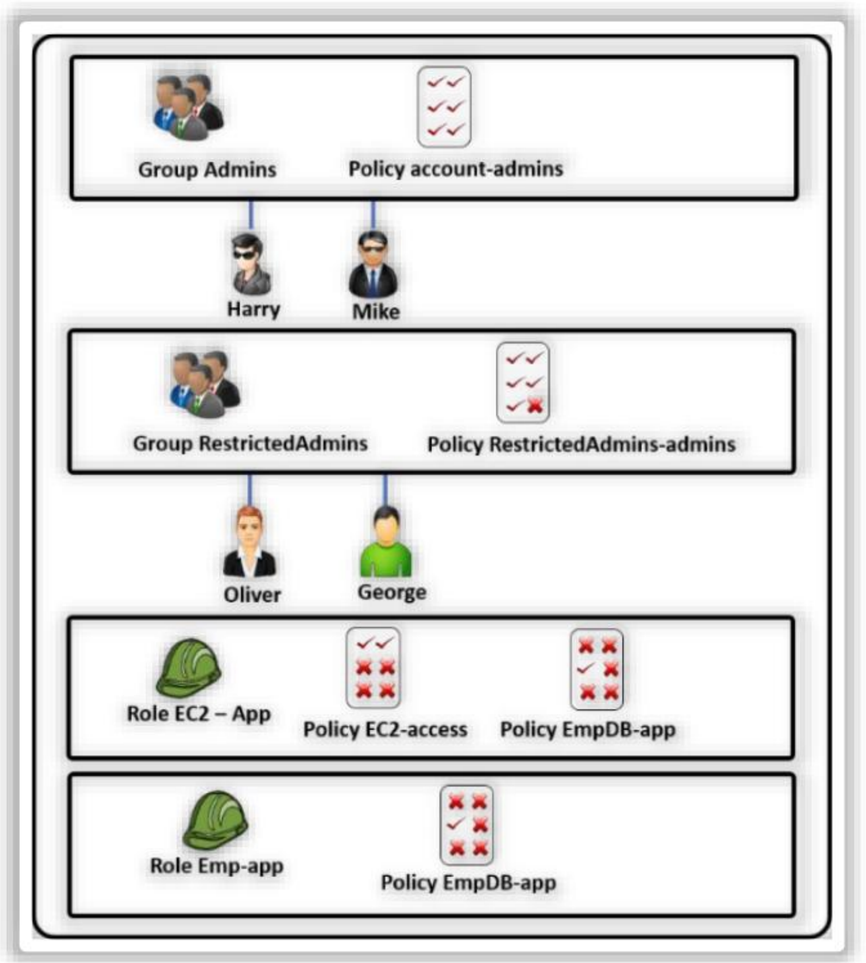


FIGURE 3.48: Inline Policies

The above diagram shows that each policy is an inherent part of the principal entity. Here, two roles have the same policy (the Policy EmpDB-app policy) while they are not sharing a single policy. Each role comprises its own copy of the policy.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Use Customer-managed Policies Instead of Inline Policies

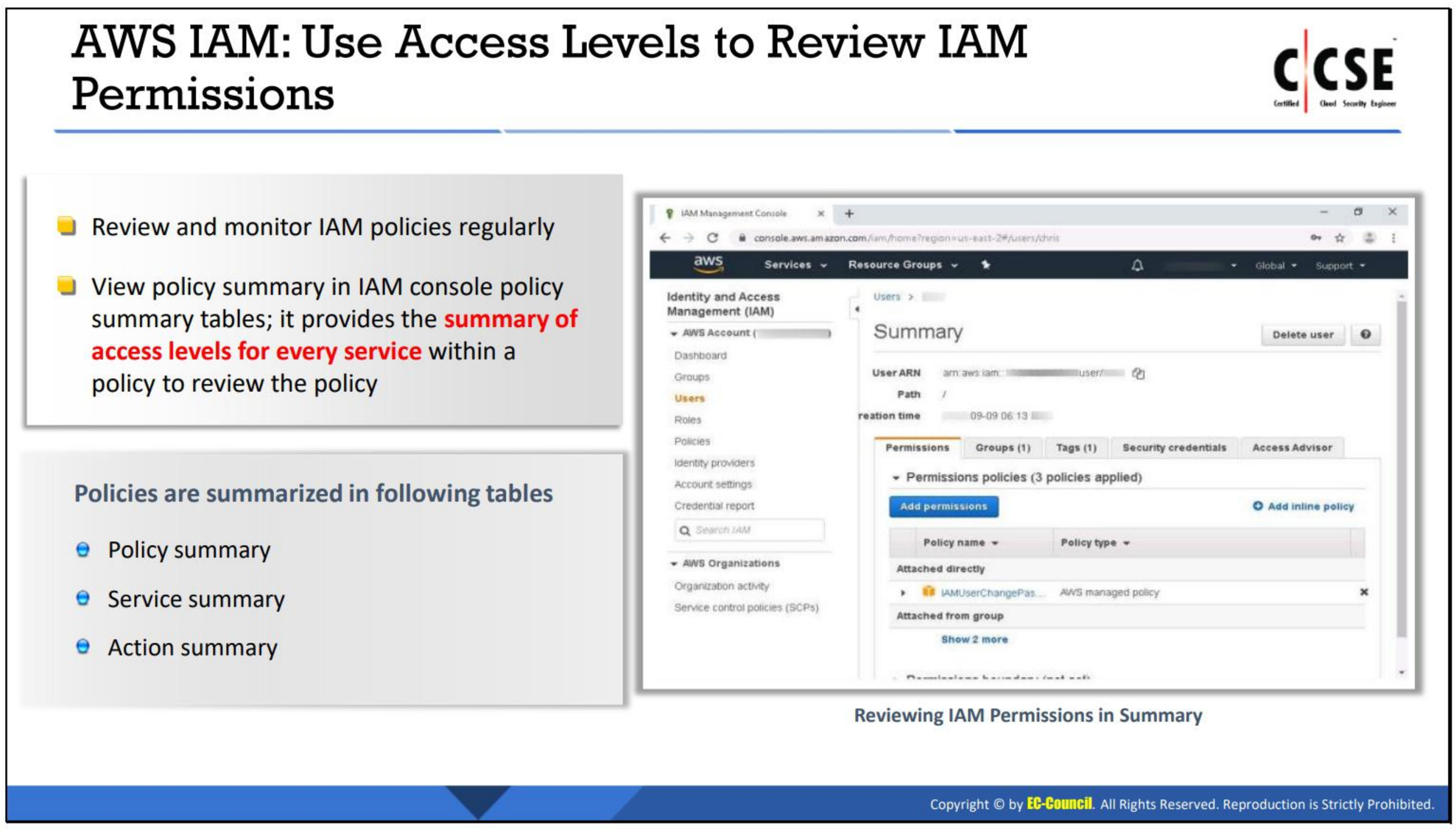
Generally, it is recommended to use customer-managed policies instead of inline policies because AWS-managed policies allow viewing all the managed policies in a single AWS CLI or AWS API operation and can separate IAM resources that can be attached to multiple identities. However, inline policies exist only on an IAM identity. It is possible to convert the inline policies to managed policies.

Source: https://aws.amazon.com

Steps to convert the inline policies to managed policies are as follows:

- In the navigation pane of the IAM console, select **Groups, Users**, or **Roles**.
- Select the name of the Group, User or Role with the policy to remove.
- Select the **Permissions** tab.
- Choose **Show Policy** next to the inline policy that you want to remove for **Groups**.
- Copy the JSON policy document for the policy.
- Select **Policies** in the navigation pane and select **Create policy** and then choose the **JSON** tab.
- Replace the existing text with your JSON policy text and select **Review policy.**
- Enter a name for your policy and select **Create policy**.
- Choose Groups, Users, or Roles in the navigation pane and select the name of the **group**, **user**, or **role** that has the policy you want to remove.
- Select **Attach Policy** for groups. Select **Add permissions** for users and roles**.**
- Select the checkbox next to the name of your new policy and select **Attach Policy** for groups. For users or roles, select **Add permissions**.
- On the next page, select **Attach existing policies directly**, select the checkbox next to the name of your new policy, choose **Next: Review**, and then select **Add permissions.**
- You will be returned to the **Summary** page for your group, user, or role.
- Select **Remove Policy** next to the inline policy that you want to remove for groups. For users or roles, choose **X** next to the inline policy that you want to remove.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AWS IAM: Use Access Levels to Review IAM Permissions

Review and monitor IAM policies constantly to maintain AWS account security and make sure the least privileges are granted for the individual accounts.

To view the summary of access level while reviewing a policy, view the policy summary; it is included on the **Policies** page for managed policies and on the **Users** page for policies that are attached to users. AWS classifies service actions into five access levels based on what each action does: **List**, **Read**, **Write**, **Permissions management**, or **Tagging**. Using these access levels, you can decide which actions are needed in policies.

Policies are summarized in three tables:

- **Policy summary table** includes a list of services and summaries of the permissions that are defined by the chosen policy.
- **Service summary table** includes a list of the actions and summaries of the permissions that are defined by the policy for the chosen service.
- **Action summary table** includes a list of resources and the associated conditions that apply to the chosen action.

Steps to view the policy summary from the Policies page are as follows:

- Select **Policies** in the navigation pane in the AWS Management Console.
- Select the name of the policy that you want to view in the list of policies.
- View the **Permissions** tab to see the policy summary on the **Summary** page for the policy.

Steps to view the summary for a policy attached to a user are as follows:

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select **Users** from the navigation pane in the AWS Management Console.
- Select the name of the user that you want to view in the list of users.
- View the **Permissions** tab to see the list of policies that are attached to the user directly or from a group on the **Summary** page for the user.
- Expand the row of the policy that you want to view in the table of policies for the user.

Steps to view the summary for a policy attached to a role are as follows**:**

- Select **Roles** in the navigation pane.
- Select the name of the role whose policy you want to view in the list of roles.
- View the **Permissions** tab to see the list of policies that are attached to the role on the **Summary** page for the role.
- Expand the row of the policy that you want to view in the table of policies for the role.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AWS IAM: Configure a Strong Password Policy for Users

Create a strong password policy and allow IAM users to change their own passwords periodically. You can create a password policy for your AWS account on the **Account Settings** page of the IAM console.

hide01.ir

Any strong password policy should include the following**:**

- The user can specify the **minimum number of characters** allowed in an IAM user password. That can be any number from 6 to 128.
- IAM user passwords must contain **at least one uppercase character** (A-Z).
- IAM user passwords must contain **at least one lowercase character** (a-z).
- IAM user passwords contain **at least one numeric character** (0 to 9).
- IAM user passwords contain at least one of the following non-alphanumeric characters: ! @ # $ % ^ & * ( ) _ + - = [ ] { } | '
- Allow users to change their own password.
- Enable password expiration.
- Prevent password reuse.
- Password expiration requires administrator reset.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



FIGURE 3.49:Password Policies

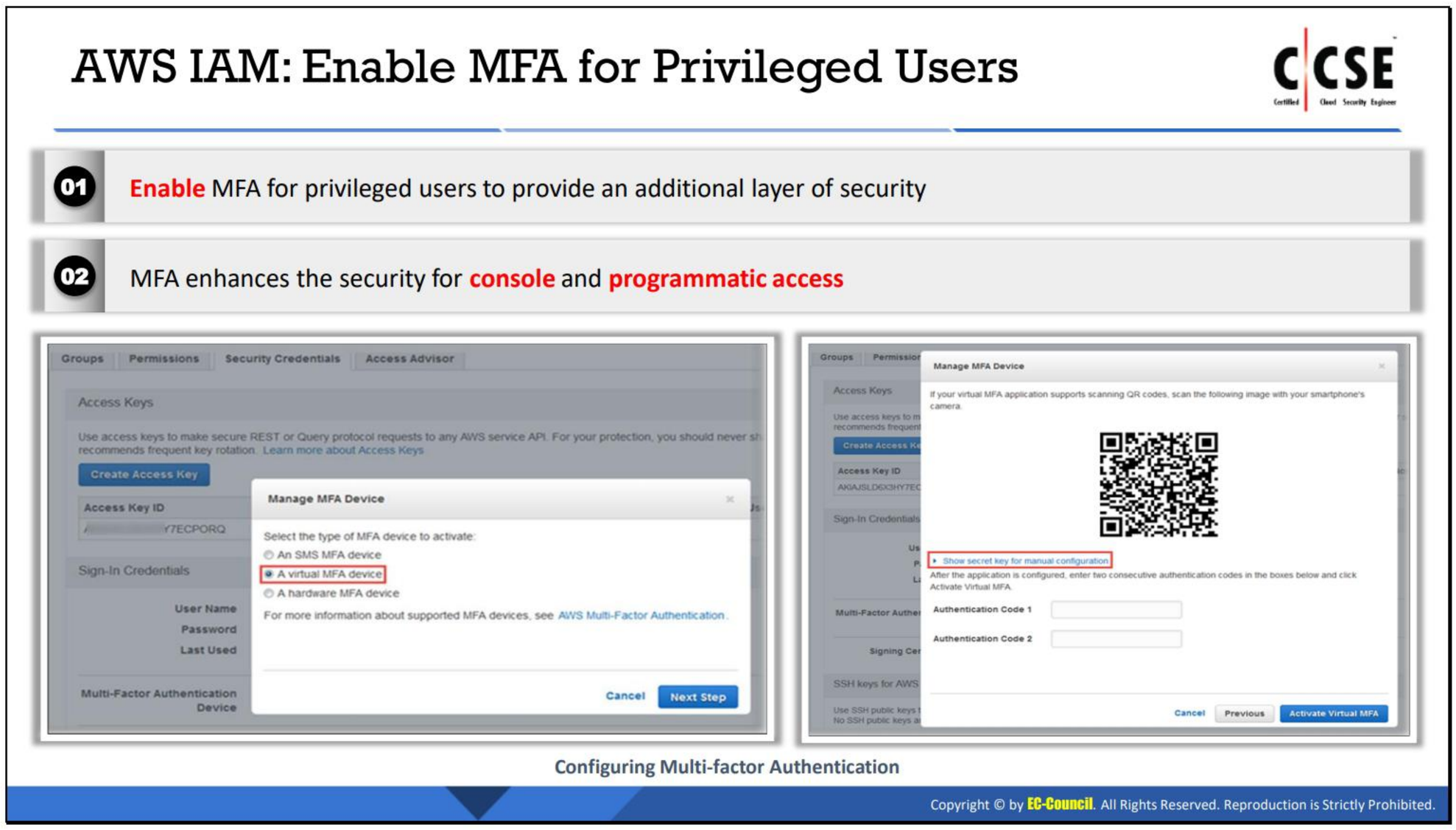
Steps to create or change a password policy are as follows**:**

- Click **Account Settings** in the navigation pane of the IAM console.
- Select the options you want to apply in the **Password Policy** section.
- Click **Apply Password Policy**.

To delete a password policy Click Delete Password Policy in the Password Policy section of Account Settings.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AWS IAM: Enable MFA for Privileged Users

For extra security, it is recommended to enable MFA for privileged users. The MFA enabled users to use a device-generated response for authentication. Both the user's credentials and the device-generated response are required to complete the sign-in process. With the implementation of MFA, the user account can be secured even if the credentials or access keys are compromised.

The response is generated in one of the following ways. You can use either way for the privileged IAM users who are allowed to access sensitive resources or API operations.

- **Virtual and hardware MFA devices** that generate a code on the app/device and allow IAM users to enter the code on the sign-in screen.
- **U2F security keys** that generate a response when you tap the device and allow the IAM users to finish the sign-in process automatically.

Steps to enable a virtual MFA device for an IAM user are as follows**:**

- Select **Users** in the navigation pane of the IAM console.
- Choose the intended MFA user in the **User Name** list.
- Select the **Security credentials** tab and choose **Manage** next to **Assigned MFA device**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In the **Manage MFA Device** wizard, choose **Virtual MFA device**, and choose **Continue**.

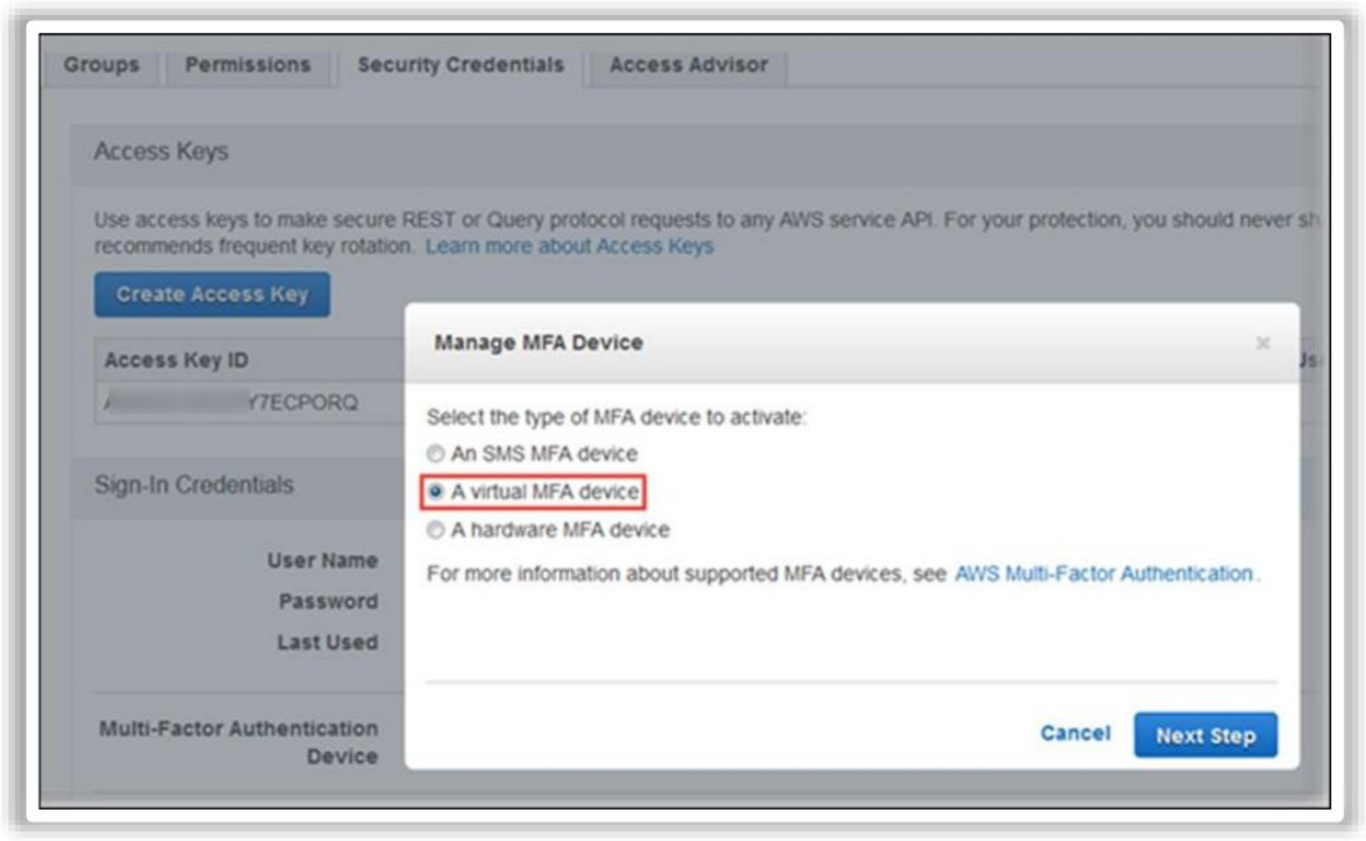


FIGURE 3.50: Choose Virtual MFA Device

- Open your virtual MFA app. For a list of apps that you can use for hosting virtual MFA devices, see the section on multi-factor authentication
- Decide whether the MFA app supports QR codes, and do one of the following:
  - Choose **Show QR code** from the wizard, and use the app to scan the QR code.

hide01.ir

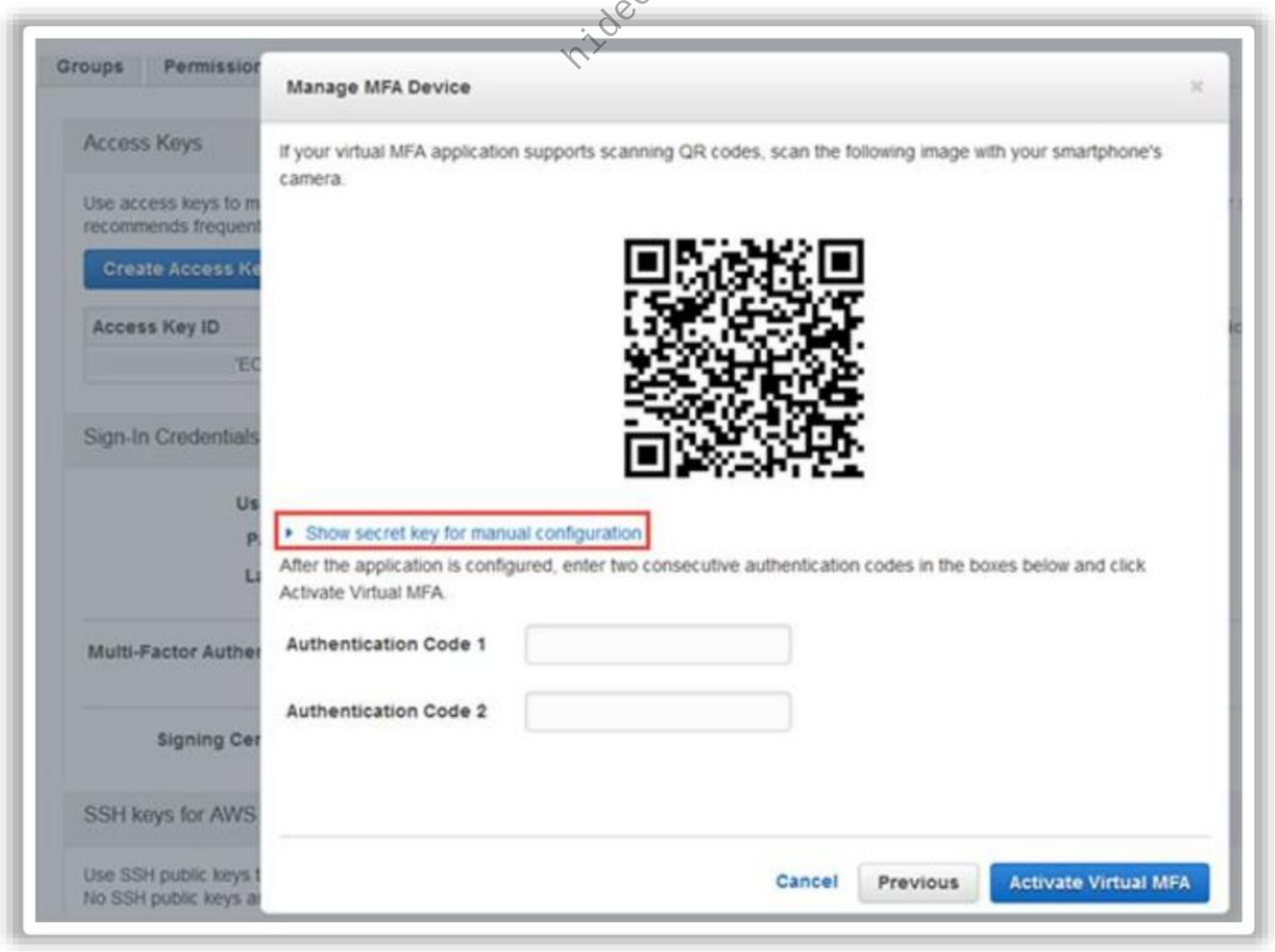


FIGURE 3.51: QR Code

  - Select **Show secret key** in the **Manage MFA Device** wizard, and type the secret key in the MFA app.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In the **Manage MFA Device** wizard, type the OTP that currently appears in the virtual MFA device in the **MFA code 1** box.
- Wait for 30 seconds for the device to generate new OTP. Then type the second OTP into the **MFA code 2** box. Select **Assign MFA**.

Steps to enable a U2F security key for your own IAM user are as follows**:**

- In the navigation bar on the upper right, select your username, and select **My Security Credentials**.

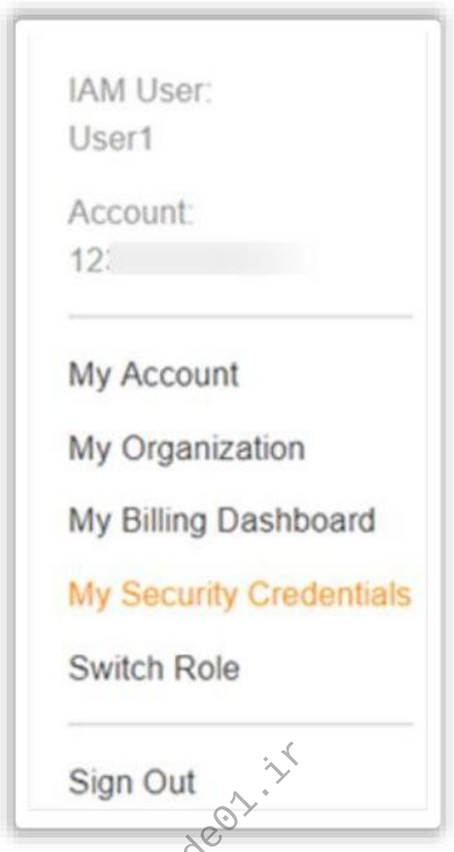


FIGURE 3.52: Navigation Bar

- On the **AWS IAM credentials** tab and in the **Multi-factor authentication** section, select **Manage MFA device**.
- Select **U2F security key**, and then select **Continue** in the Manage MFA device wizard.
- Insert the U2F security key into your computer's USB port.
- Tap the U2F security key, and select **Close** when U2F setup is complete.

Steps to enable a hardware MFA device for your own IAM user are as follows**:**

- In the navigation bar on the upper right, select your username, and select **My Security Credentials**.
- On the **AWS IAM credentials** tab and in the **Multi-factor authentication** section, and select **Manage MFA device**.
- In the **Manage MFA device** wizard, select **Hardware MFA device** and select **Continue**.
- Type the device serial number (see the back of the device for number).
- Type the six-digit number displayed by the MFA device in the **MFA code 1** box. Press the button on the front of the device to view the number.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

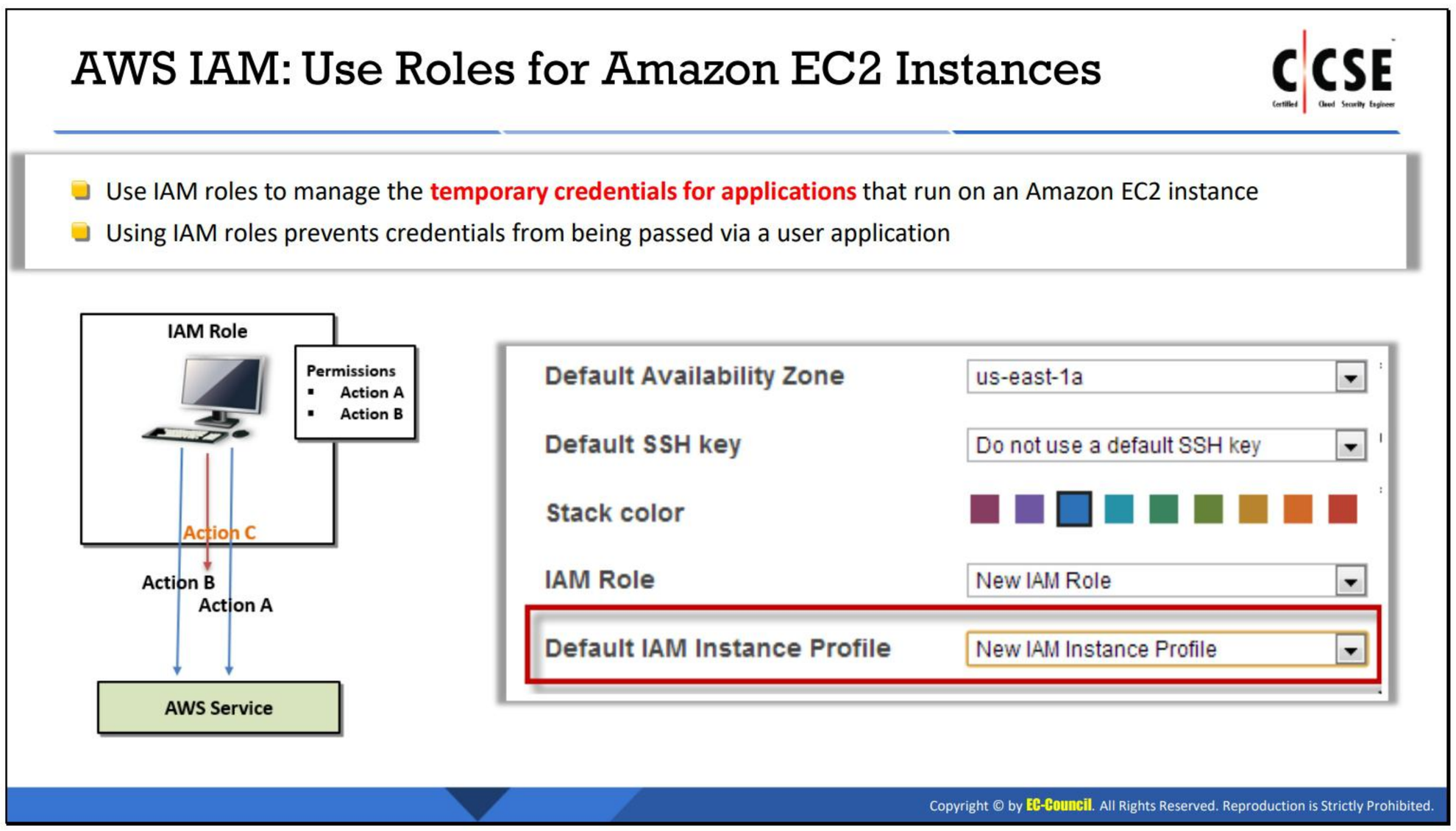
- Wait 30 seconds while the device refreshes the code, and type the next six-digit number into the **MFA code 2** box. Press the button on the front of the device again to display the second number and select **Assign MFA**.

Steps to enable SMS MFA for an IAM user are as follows**:**

- Select **Users** in the navigation pane.
- Select the name (not the checkbox) of the intended MFA user in the User Name list.
- Select the **Security credentials** tab. Select **Manage** next to **Assigned MFA device**.
- Select **An SMS MFA device**, and select **Continue** in the **Manage MFA Device** wizard.
- Type the phone number to which you want to send MFA codes for this IAM user, and choose **Continue**.
- Type the six-digit authentication code that is immediately sent to the specified phone number for verification, and then choose **Continue**.
- The wizard ends if AWS successfully verifies the code. Otherwise, choose **Finish** to close the wizard.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AWS IAM: Use Roles for Amazon EC2 Instances

To access other AWS services, applications that run on an Amazon EC2 instance require credentials. The IAM roles securely provide credentials (a username and password or access keys) for these applications. An IAM role is not a user or group, and it does not have its own permanent set of credentials like IAM users. However, it is an entity that has its own set of permissions. IAM dynamically provides temporary credentials to EC2 instances and these credentials are automatically rotated. Use IAM roles to manage the temporary credentials for applications that run on an Amazon EC2 instance. Using IAM roles prevents credentials from being passed via a user application. A role can be specified as a launch parameter for an instance when launching it, and the specified role permission determines the tasks that an application is allowed to perform.

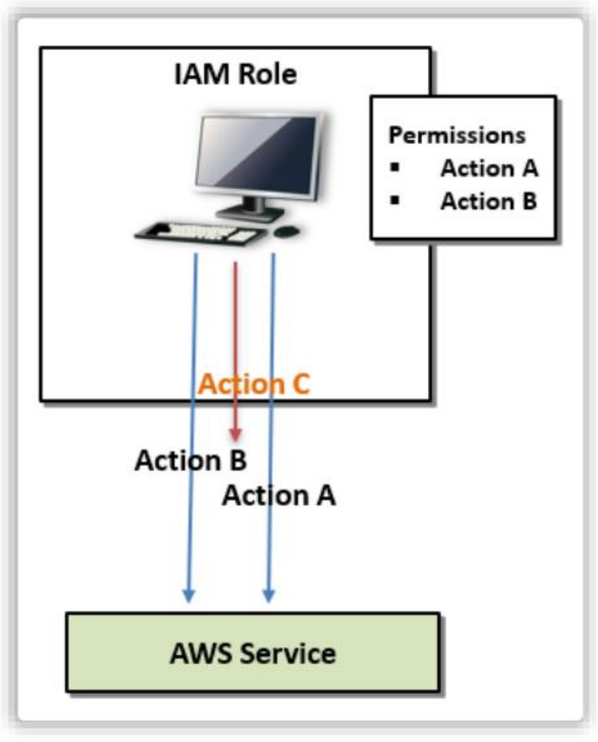


Figure 3.53: Use Roles for Amazon EC2 Instances

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For example, an application is run by a developer on an EC2 instance that needs access to the S3 bucket (photos). A Get-pics service role is created and attached to the EC2 instance by the administrator. This service role comprises a permission policy that allows read-only access to the S3 bucket and a trust policy that allows the instance to assume the role and retrieve temporary credentials. The application uses the temporary credentials of the role to access the photo bucket when it runs on the instance. For this, the developer does not need to share or manage his credentials and the administrator is not required to grant permission to the developer to access the photo bucket.

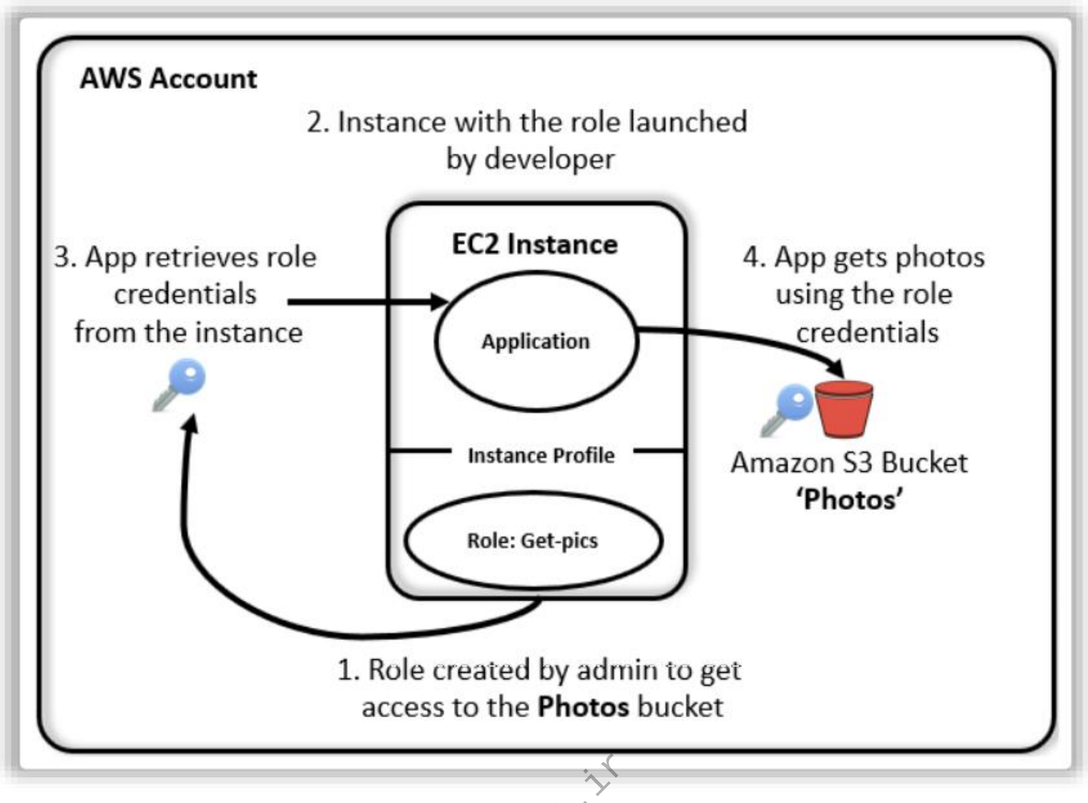


FIGURE 3.54: Access the Photo Bucket

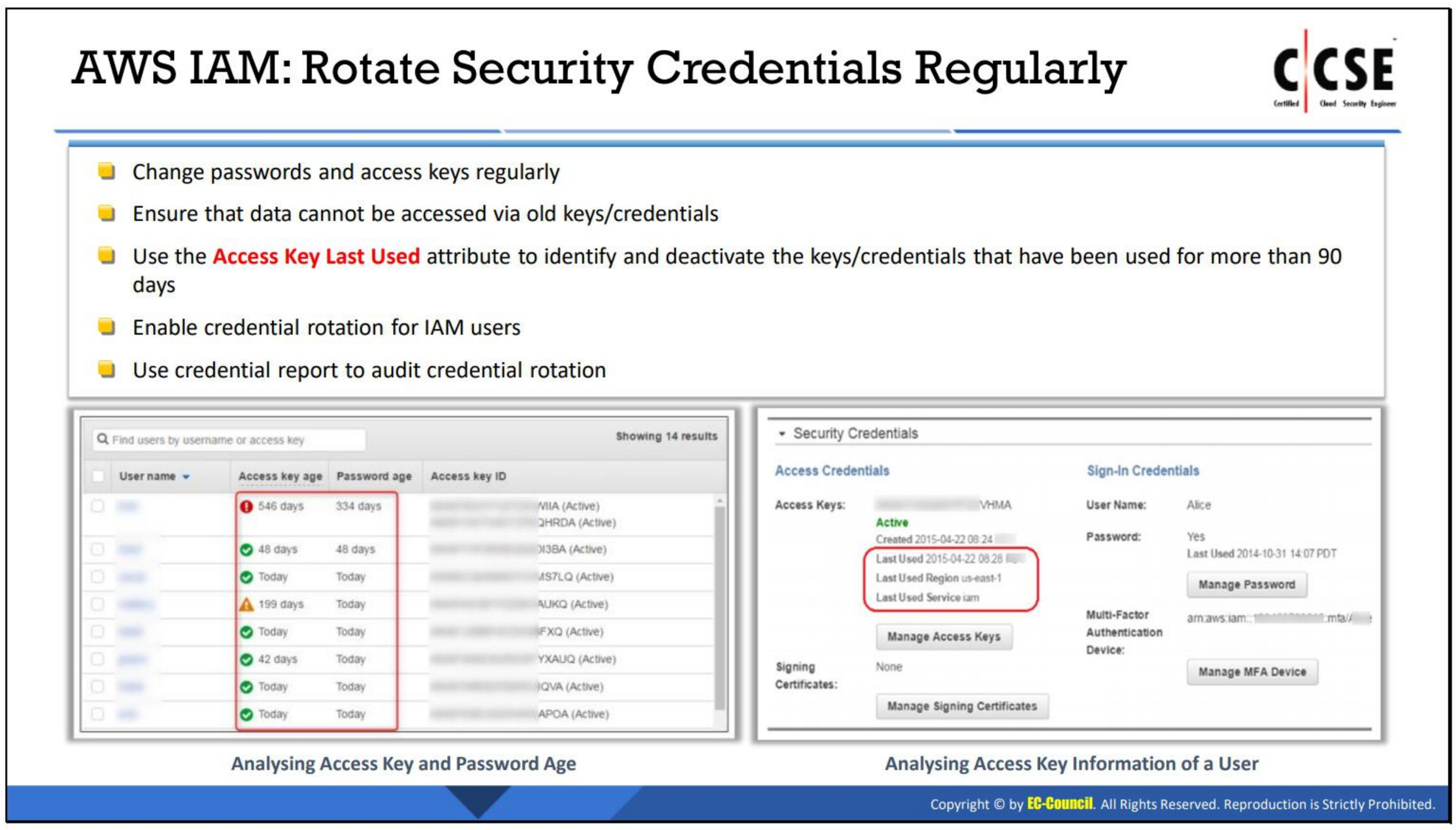
Permissions for EC2 Instance Apps

If applications running on a particular EC2 Instance's stack want to access other AWS resources, they should have appropriate permissions to do so. An EC2 instance profile can be used to grant those permissions. While creating an AWS OpsWorks Stacks stack, an instance profile for every instance can be specified. The profile specifies an IAM role that can be assumed by the apps running on the instance to access AWS resources as per the permissions the role's policy grants.



FIGURE 3.55: Instance Profile

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AWS IAM: Rotate Security Credentials Regularly

To prevent unauthorized access, follow the guidelines prescribed below:

- Change passwords and IAM user access keys regularly and ensure that all IAM users in your account do the same.
- Ensure that data is not accessible using old keys/credentials. Identify and deactivate the keys/credentials used more than 90 days using the Access Key Last Used.
- If a password or access key is compromised unknowingly, limit how long the credentials can be used to access resources.
- Apply a password policy to your account to require all IAM users associated with your account to rotate their passwords regularly and decide how often they must do so.
- Use Credential Report to audit credential rotation.

Source: https://aws.amazon.com

Steps to rotate access keys for an IAM user without interrupting your applications are as follows:

- Create a second access key while the first set of credentials is still active.
  - Choose **Users** in the navigation pane of the IAM console.
  - Select the **Security credentials tab** after selecting the name of the intended user.
  - Select **Create access key** and select **Download .csv file** to save the access key ID and secret access key to a .csv file on your computer in a secure location. After

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

downloading the .csv file, select **Close**. The new access key is active by default and the user now has two active access keys.

- Update all applications and tools to use the new access key.
- Check whether the first access key is still in use by reviewing the **Last used** column for the oldest access key. One way is to wait several days and then check the old access key for any use before proceeding.

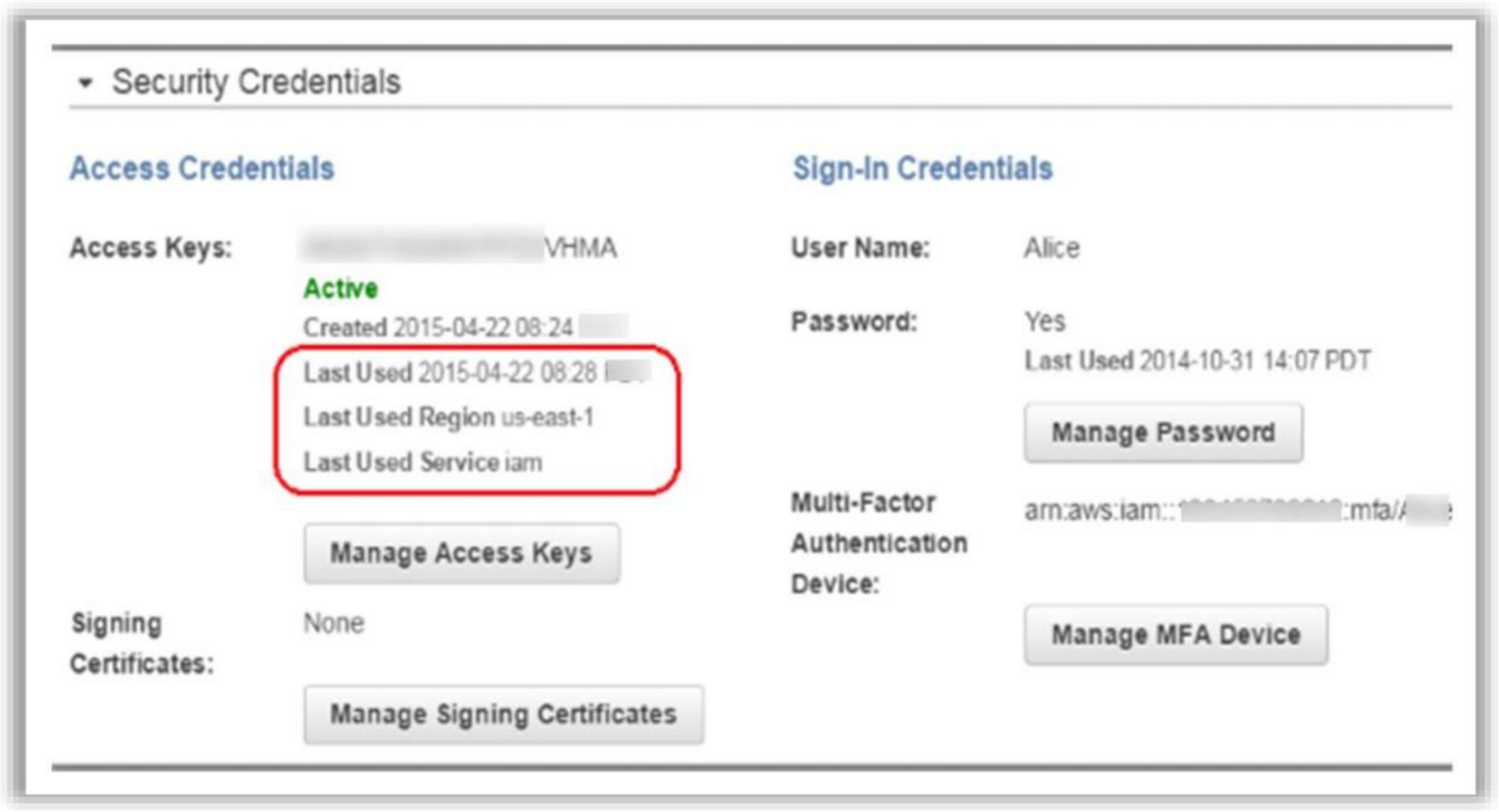


FIGURE 3.56: Security Credentials

- If the **Last used** column value shows that the old key has never been used, it is recommended to do not immediately delete the first access key. Instead, select **Make inactive** to deactivate the first access key.
- Using only the new credentials, confirm that the applications are working fine.
- Delete the first access key after ensuring that all applications and tools have been updated.
  - Select **Users** in the navigation pane of the IAM console.
  - Select the name of the intended user, and select the **Security credentials** tab.
  - Locate the access key to delete by selecting its **X** button, and **Delete** to confirm.

Steps to determine when access keys need rotating are as follows**:**

- Choose **Users i**n the navigation pane of the IAM Console.
- Add the **Access key age** column to the users' table if needed by completing the following steps:
  - Select the settings icon above the table on the far right.
  - Select **Access key age** in **Manage columns**.
  - Select **Close** to return to the list of users.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

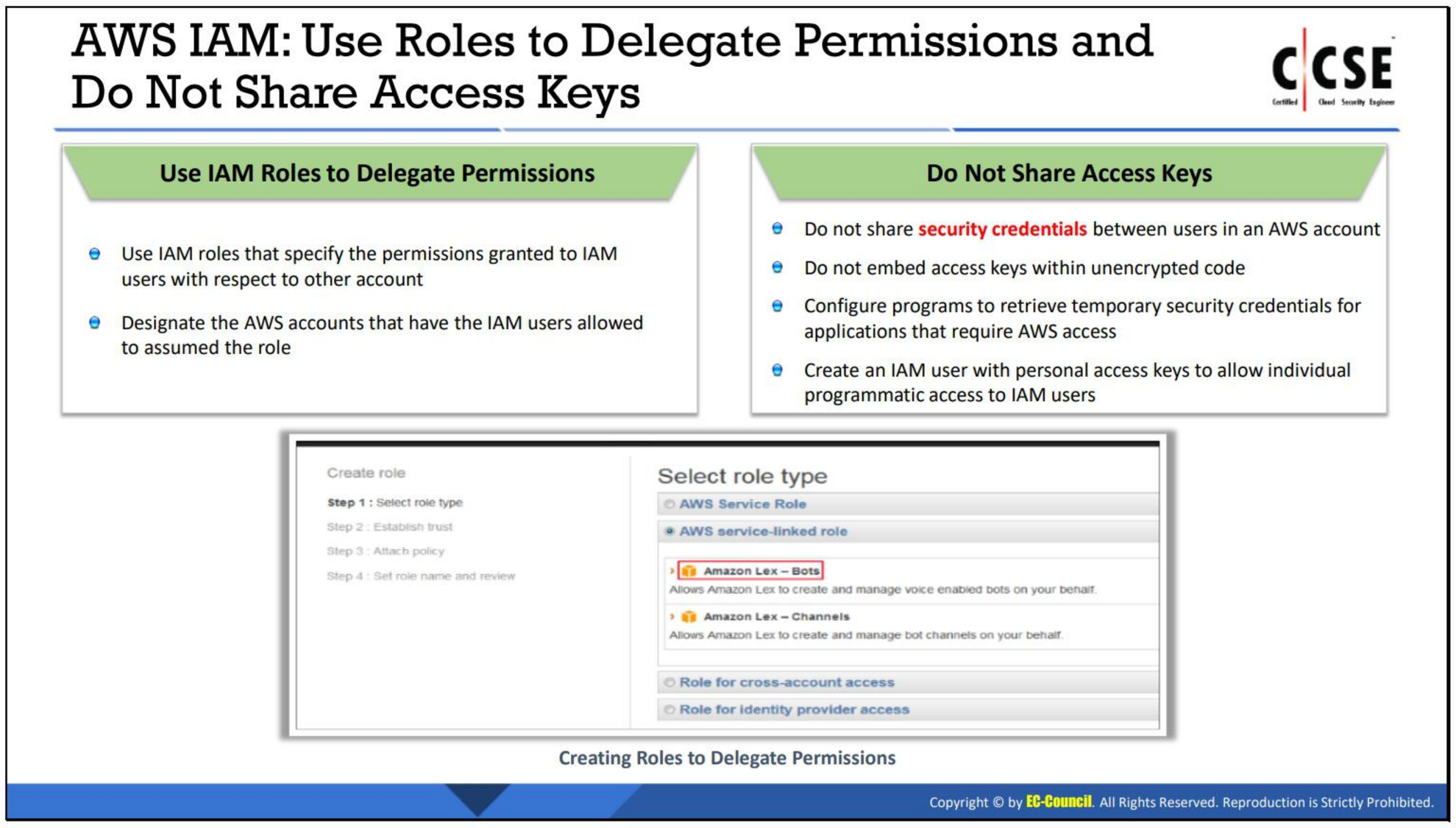
- The **Access key age** column shows the number of days since the oldest active access key was created, which is useful for finding users with access keys that need rotating. The column displays **None** for users with no access key.

Steps to download a credential report are as follows**:**

- Choose **Credential report** in the navigation pane of the IAM console.
- Choose **Download Report**.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Creating Roles to Delegate Permissions

AWS IAM: Use Roles to Delegate Permissions and Do Not Share Access Keys

Instead of sharing the security credentials between accounts to avoid users of one AWS account to access another AWS account's resources, use IAM roles. An IAM role specifies what permissions (delegation) are allowed for IAM users to access another account or designates which AWS accounts have IAM users that are allowed to assume the role. Delegation sets up a trust between two accounts. Of the two accounts, the first is the **trusting account** that owns the resource, and the second is the **trusted account** that comprises the users that need to access the resource. Trusted and Trusting accounts can be any of the following:

- Same account
- Separate accounts under organization's control
- Two accounts owned by different organizations

Before delegating permission to access a resource, create an IAM role in the trusting account that has two policies attached. These attached policies are described below:

- **Permission policy** that allows the user of the role to perform their tasks on the resources with the needed permissions and is one-half of the permissions.
- **Trust policy** specifies which trusted account members are allowed to assume the role and is the second half of the permissions. The user who assumes the role temporarily gives up his own permissions and takes the permissions of the role. Once the user stops using the role, the user's original permissions are restored.

Source: https://aws.amazon.com

Steps to create a role to delegate permissions to an IAM user are as follows:

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select **Roles** and then select **Create role** in the navigation pane of the IAM console.
- Select **Another AWS account** role type.
- Type the AWS **Account ID** to which you want to grant access to your resources.
- To grant permission to assume this role to any IAM user in the specified account, the administrator attaches a policy to the user or a group that grants permission for the `sts:AssumeRole` action. That policy should specify the role's ARN as the Resource.
- In the case of granting permissions to users from an account that you do not control, the users will assume this role programmatically. Then, select the addition parameter **Require external ID**, which ensures secure use of roles between accounts that are not controlled by the same organization by adding a condition to the trust policy that allows the user to assume the role when only the request includes the correct `sts:ExternalID`. This can be any word or number that is agreed between you and the administrator of the third-party account.
- In the case of restricting the role to users who sign-in with MFA, select **Require MFA**, which adds a condition to the role's trust policy that checks for an MFA sign-in.
- Select **Next: Permissions**.
- Select the policy (AWS-managed/customer-managed policies) to use for the permissions policy or select **Create policy** to create a new policy.
- Set a permissions boundary. Open the **Set permissions boundary** section and select **Use a permissions boundary to control the maximum role permissions**. Select the policy to use for the permissions boundary.
- Select **Next: Tags**.
- Add metadata to the role by attaching tags as key value pairs.
- Select **Next: Review**.
- Type a name for **Role name**.
- Type for **Role description**.
- Review the role and select **Create role**.

hadeer.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Steps to delegate permissions to AWS Services: Service-Linked Roles are as follows:

- Select **Roles** in the navigation pane of the IAM console.

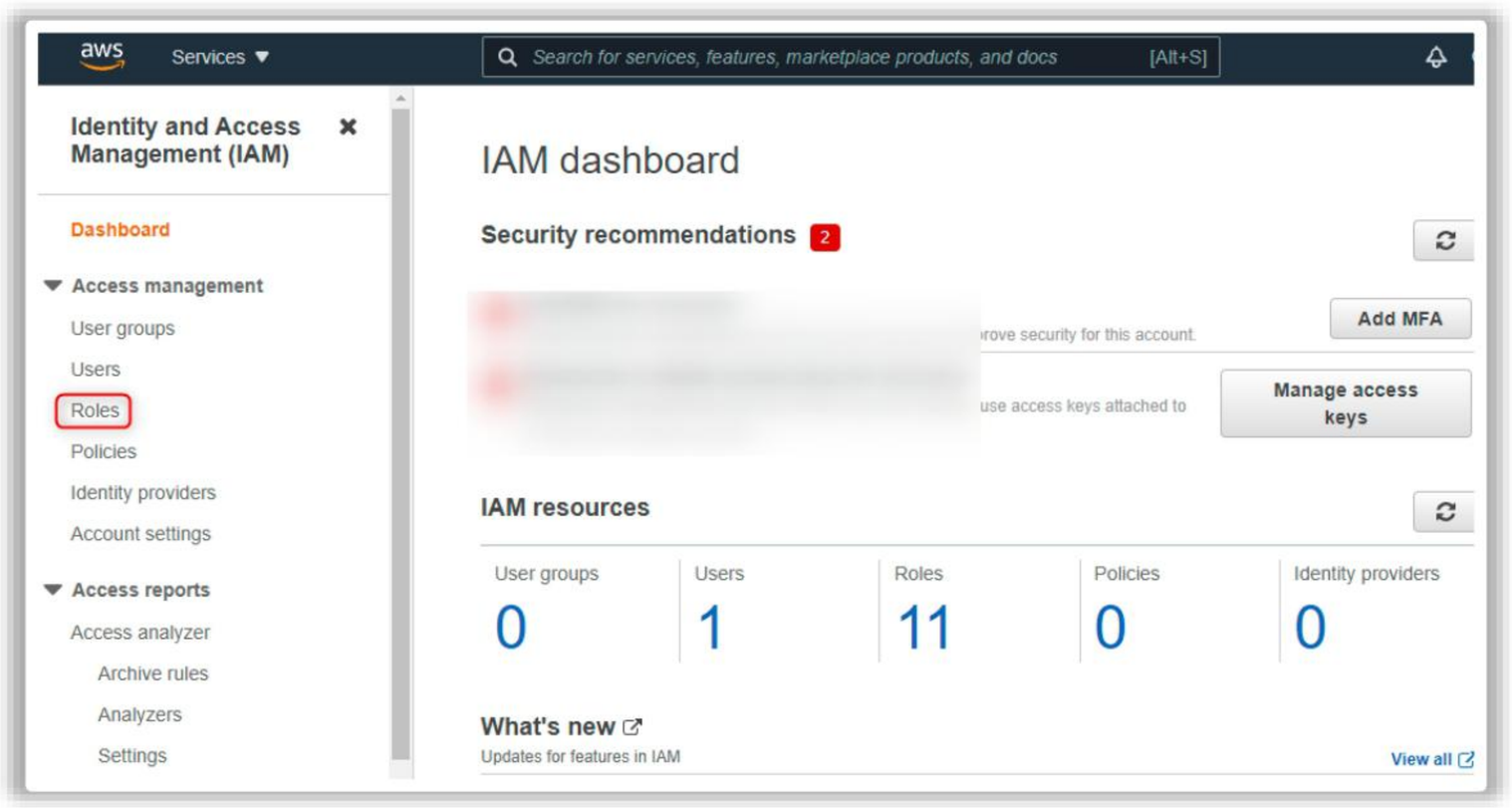


FIGURE 3.57:Select Roles

- Choose **Create new role**.

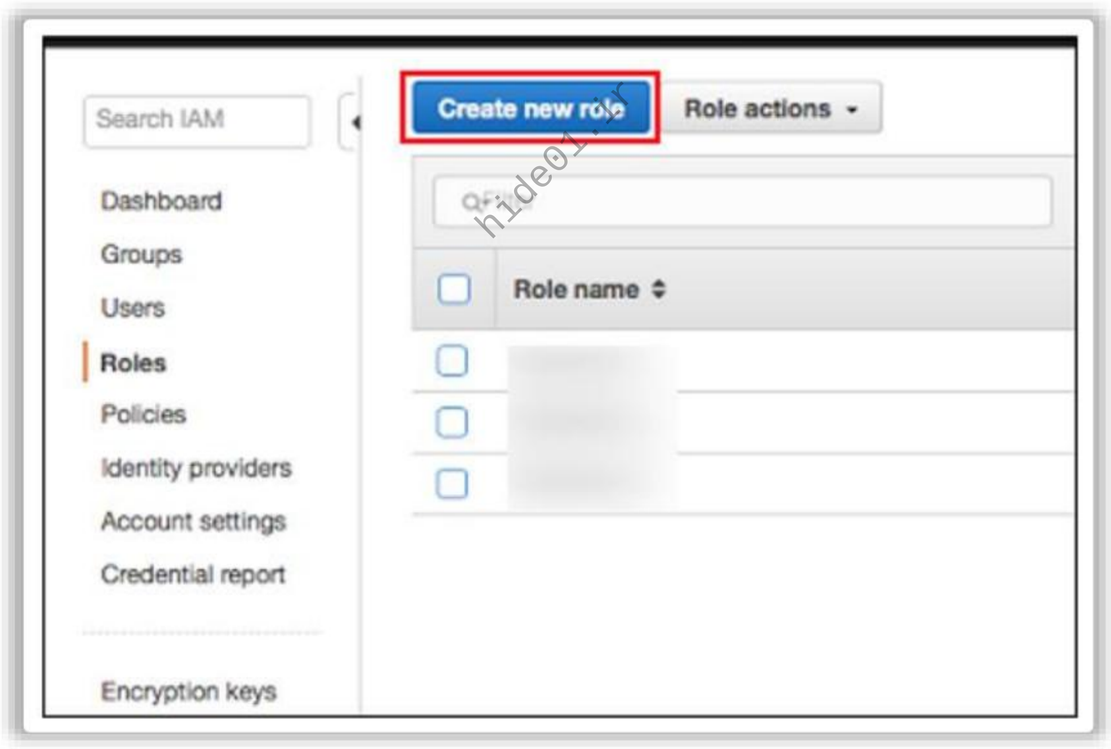


FIGURE 3.58: Create New Role

- In the **AWS service-linked role** section of the **Select role type** page, select the AWS service for which you want to create the role.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

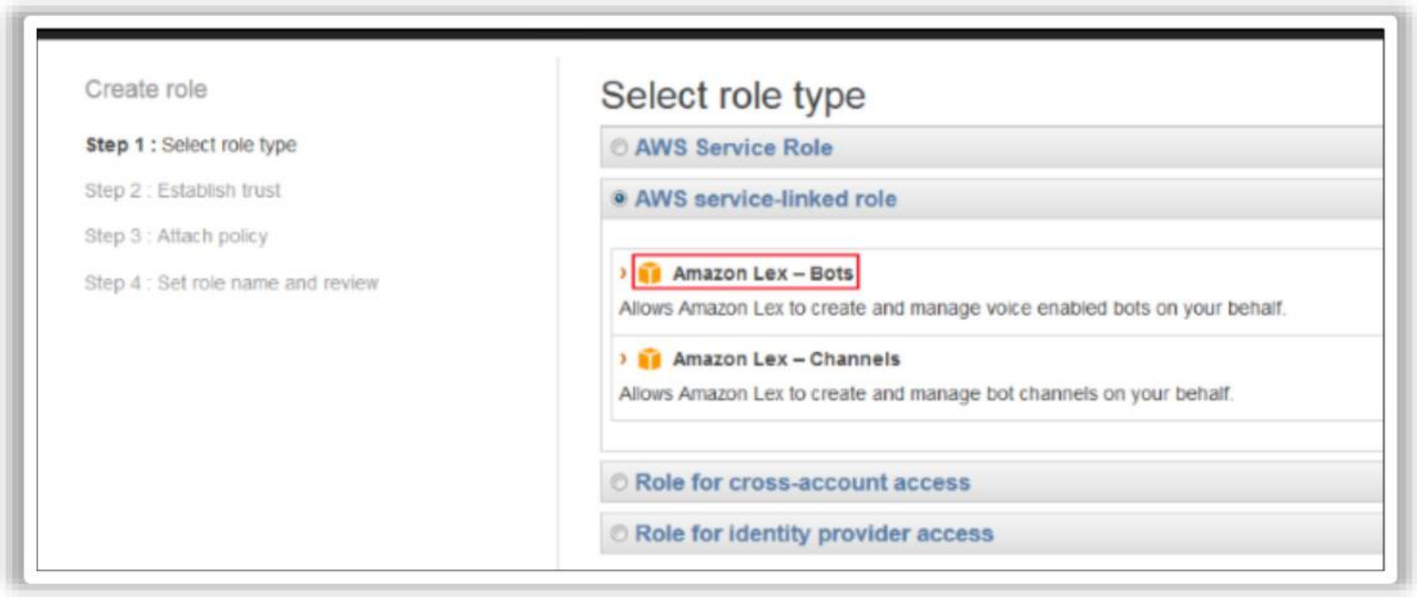


FIGURE 3.59: Select Role Type

- Observe that the role name prefix is automatically populated. Type the role name suffix for the service-linked role. Leave the role name suffix box blank if the AWS services such as Amazon Lex do not support custom suffixes.
- Give a description of the new role. IAM suggests a description for a role, which you can edit.

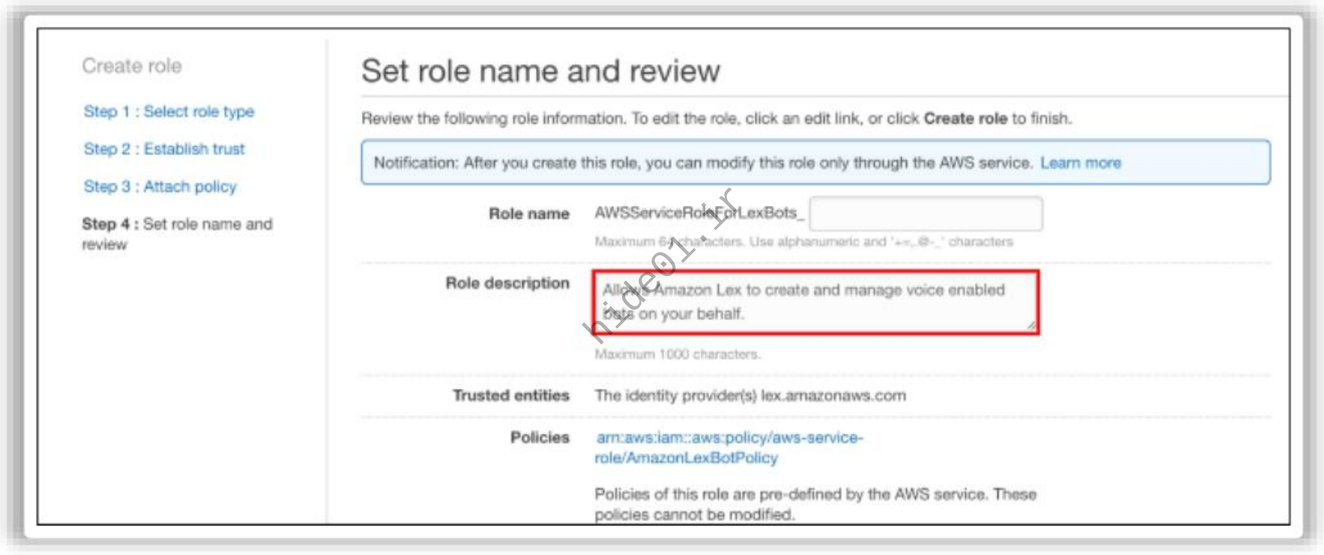


FIGURE 3.60: Role Description

- Select **Create role**. The service-linked roles are marked with a cube-shaped icon in the IAM console.

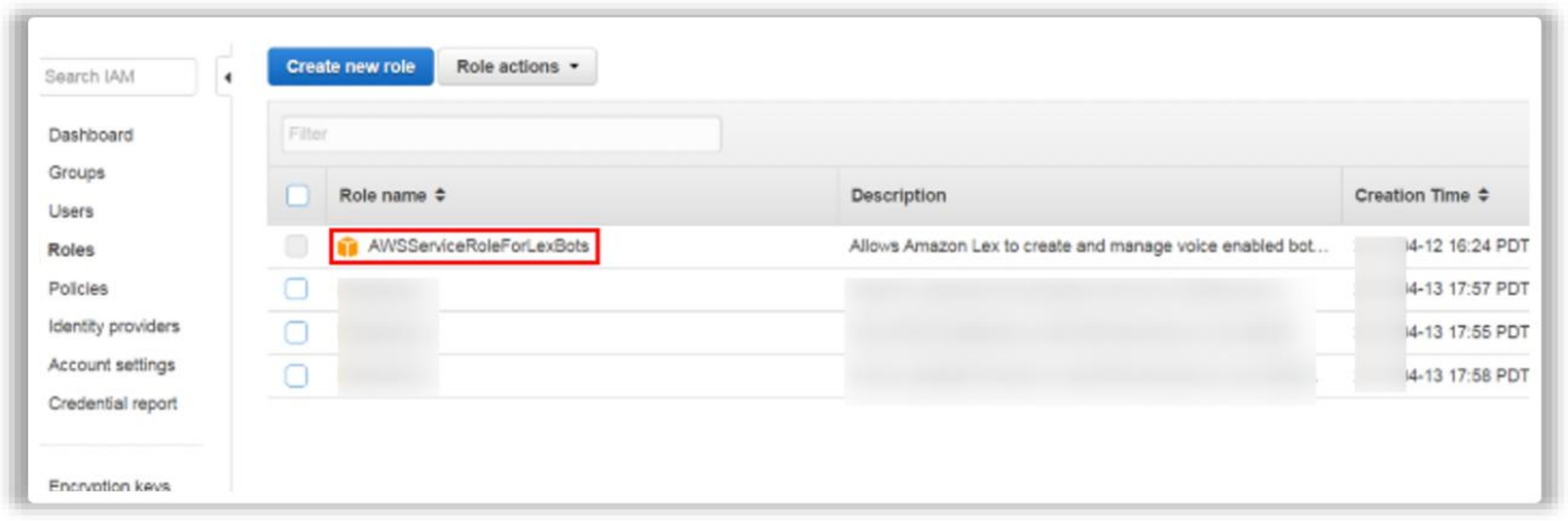


FIGURE 3.61:Create Role

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Do Not Share Access Keys

Access keys give programmatic access to AWS. It is recommended to not share the security credentials between the users in the AWS account and do not embed access keys within the unencrypted code. Configure the program to retrieve temporary security credentials for applications that need AWS access. Create an IAM user with personal access keys to allow IAM users for individual programmatic access.

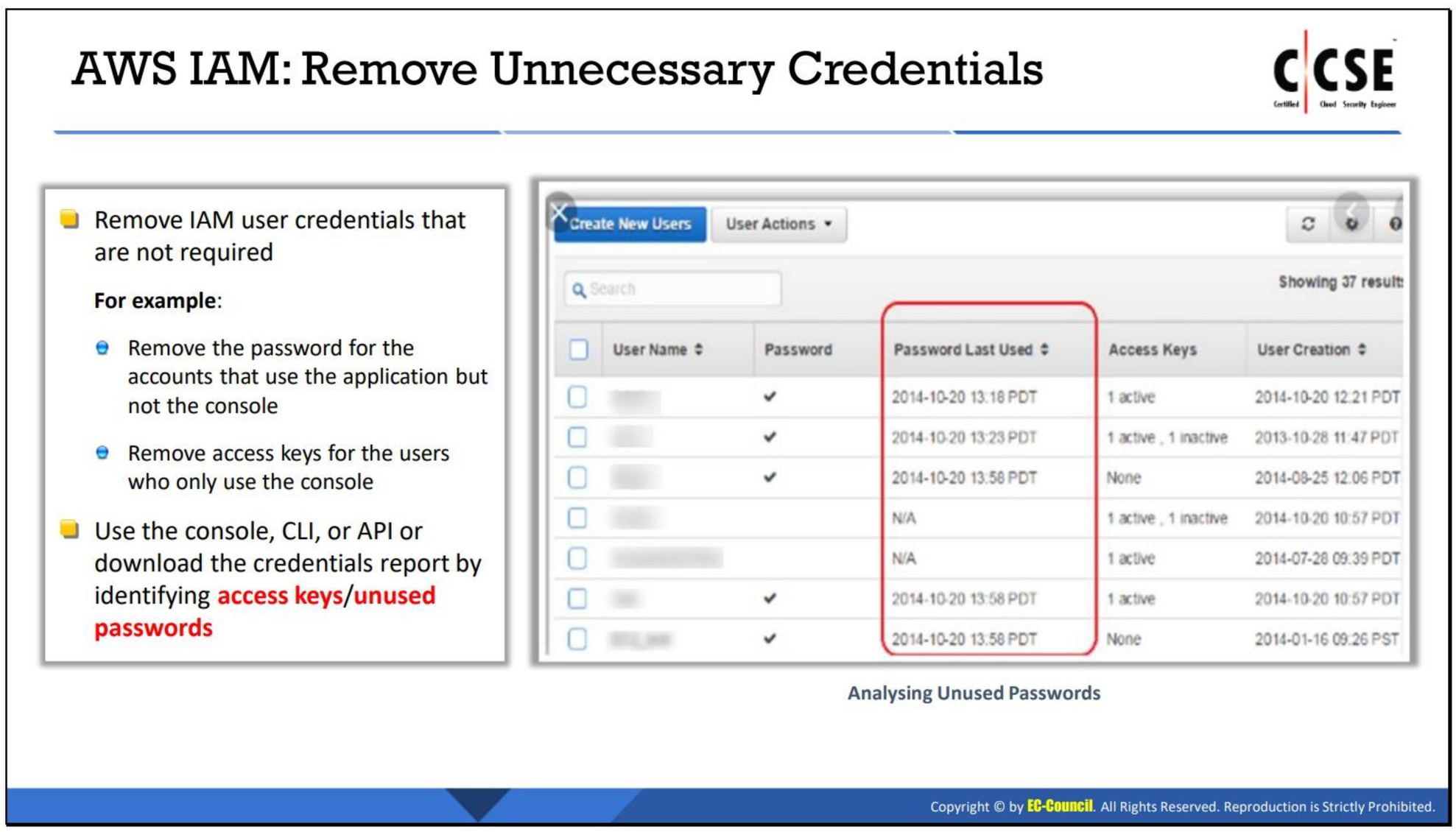
Source: https://aws.amazon.com

Steps to create an IAM user with personal access keys to allow IAM users for individual programmatic access are as follows:

- Select **Users** and then select **Add user** in the navigation pane of the IAM console.
- Type the username for the new user. In case to add more users, select **Add another user** and type their usernames.
- Select the type of access (programmatic access, access to the AWS Management Console, or both) this set of users will have.
  - Select **Programmatic access** when the users need access to the API, AWS CLI, or Tools for Windows PowerShell, which will create an access key for each new user.
- Select **Next: Permissions**.
- On the **Set permissions** page, specify how you want to assign permissions to this set of new users by selecting any one of the following options:
  - Select **Add user to group** if to assign the users to one or more groups that already have permissions policies.
  - Select **Copy permissions from existing user** to copy all the group memberships, attached managed policies, embedded inline policies, and any existing permissions boundaries from an existing user to the new users.
  - Select **Attach existing policies to user directly** to see a list of the AWS-managed and customer-managed policies in your account.
- Select **Next: Tags**.
- Select **Next: Review** to see all the choices made and select **Create user**.
- Provide users credentials and then select **Send email** next to each user. Local mail client opens with a draft to allow customization. The email template includes the following details to each user: Username and URL to the account sign-in page.

hidd1.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AWS IAM: Remove Unnecessary Credentials

Remove IAM user credentials (passwords and access keys) that are not required; for example:

- Remove unused passwords and access keys using the console, CLI, API, or by downloading the credentials report.
- Remove passwords for users who use the application but not the console.
- Remove access keys for users who only use the console. The AWS IAM Console displays when the access keys were last used.

hidedo.ir

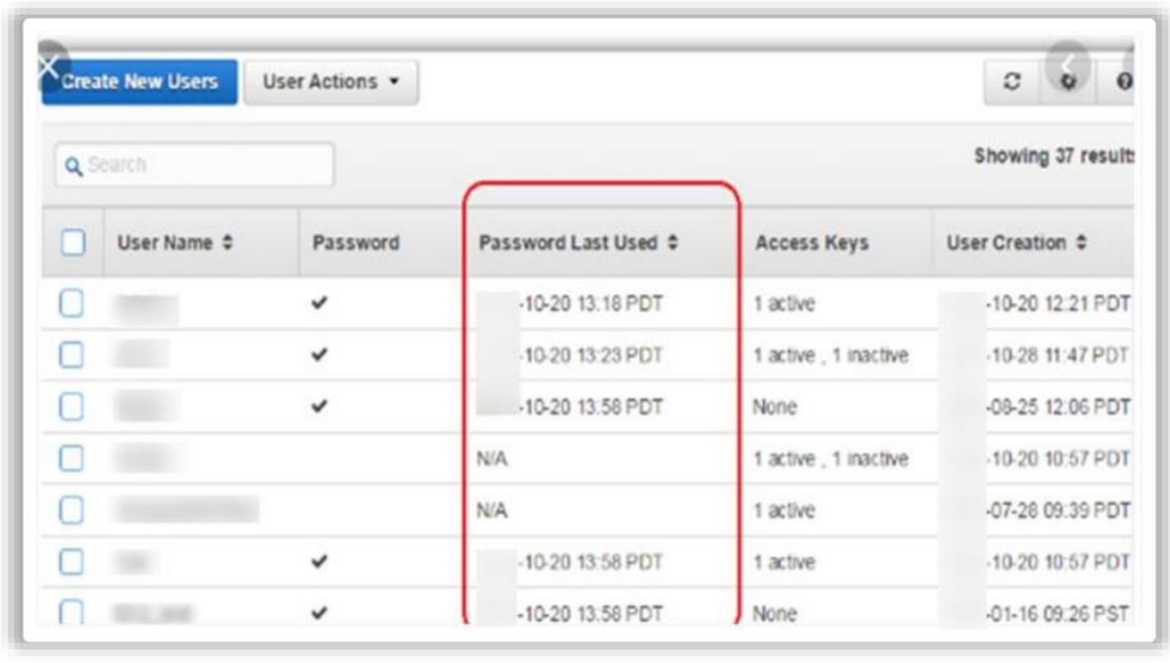


FIGURE 3.62: Analysing Unused Password

Source: https://aws.amazon.com

Steps to find unused passwords are as follows:

- Select **Users** in the navigation pane of the IAM console.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Add the **Console last sign-in** column to the users table if needed.
- Above the table on the far right, choose the settings icon.
- Select the Settings icon.
- Select **Console last sign-in** in **Manage Columns**.
- Select **Close** to return to the list of users.
- The **Console last sign-in** column displays the number of days since the user last signed into AWS through the console. The column displays **Never** for users with passwords that have never signed in and **None** for users with no passwords.

Steps to find unused passwords by downloading credentials report are as follows:

- Select **Credential report i**n the navigation pane.
- Select **Download Report** to download a comma-separated value (CSV) file. The password_last_used column shows the following:
  - **N/A**: Users that do not have a password.
  - **no_information**: Users that have not used their passwords since IAM began tracking the password age (date).

Steps to remove (disable) password for users who use the application but not console are as follows:

hide01.ir

- Select **Users** in the navigation pane.
- Select the name of the user whose password you want to delete.
- Select the **Security credentials** tab, and then under **Sign-in credentials**, Select **Manage password** next to **Console password**.
- For **Console access**, select **Disable** (delete), followed by **Apply**.

Steps to remove access keys for users (own IAM user) who only use the console are as follows:

- Select your username in the **navigation** bar on the upper right, followed by **My Security Credentials**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

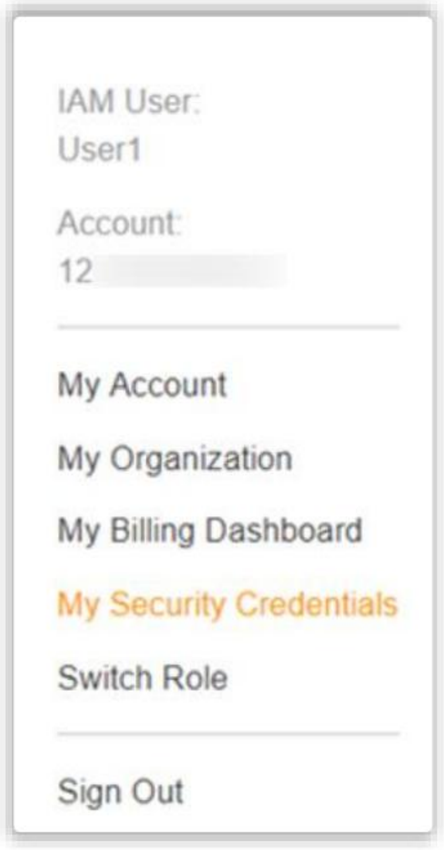


FIGURE 3.63: Navigation Bar

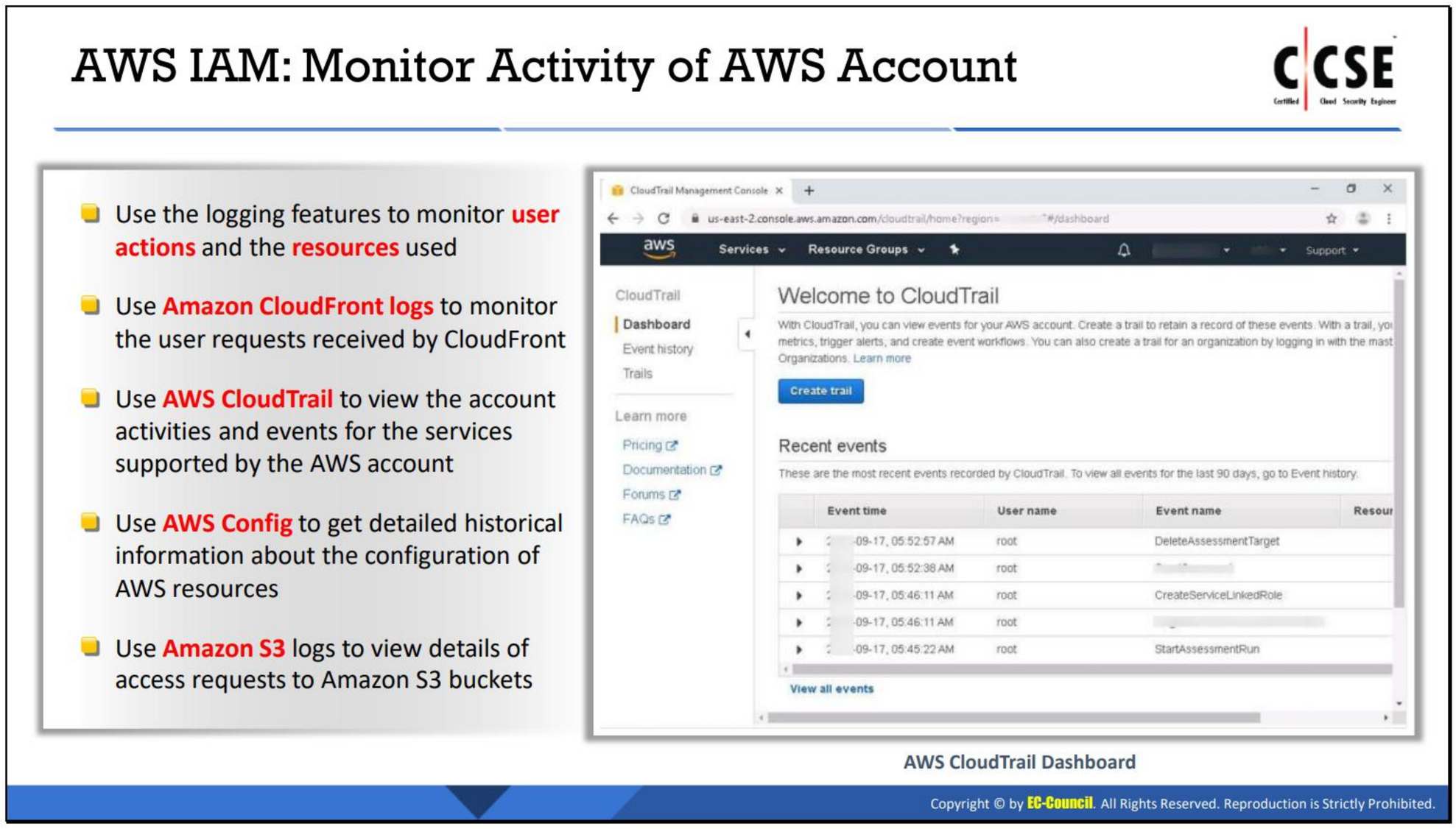
- In the **AWS IAM Credentials** tab in the **Access keys for CLI, SDK, and API access** section, select the **X** button. Then, select **Delete** to confirm.

Steps to remove access keys for users (another IAM user) who only use the console are as follows:

- Select the name of the user whose access keys you want to delete, and then click on the **Security credentials** tab.
- In the **Access keys** section, select the **X** button to delete the access key, and then select **Delete** to confirm.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



AWS IAM: Monitor Activity of AWS Account

Use logging features to decide the users' actions in the AWS account and the resources used by the users. These log files display the following:

hide01.ir

- Time and date of actions
- Source IP for an action
- Which actions failed due to inadequate permissions, and more.

Use the following AWS services for logging:

- **Amazon CloudFront:** Use Amazon CloudFront logs to monitor user requests received by CloudFront. These access logs are available for web and RTMP distributions. You can enable logging when you create or update a distribution. To enable logging, choose an **Amazon S3 Bucket** for access logs. After enabling logging for a distribution, specify the Amazon S3 Bucket that the CloudFront to store log files in. It is possible to store the log files for multiple distributions in the same bucket. After enabling logging, specify an optional prefix for file names to keep track of which log files are associated with which distributions. It is recommended to do not use the same bucket for log files if using Amazon S3 as your origin. Use a separate bucket for simplified maintenance.
- Use **AWS CloudTrail** to view account activity and events for supported services made by the AWS account. If it is already created, CloudTrail is enabled on AWS account. It records the activity of AWS account in a CloudTrail event. View the recent events in the CloudTrail console by viewing Event history. Create a trail for ongoing record of activity and events in AWS account.

  Features:

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Event history** allows one to view, search, and download recent AWS account activity.
- **Log file integrity validation** helps in log file integrity validation in IT security and auditing processes.
- **Log file encryption** allows encryption of all log files delivered to specified Amazon S3 Bucket using Amazon S3 server-side encryption (SSE).
- **Data events** provide an insight into the resource ("data plane") operations performed on or within the resource itself.
- **Management events** provide an insight into the management ("control plane") operations performed on resources in your AWS account.
- **CloudTrail Insights** helps identify unusual activity in AWS accounts.

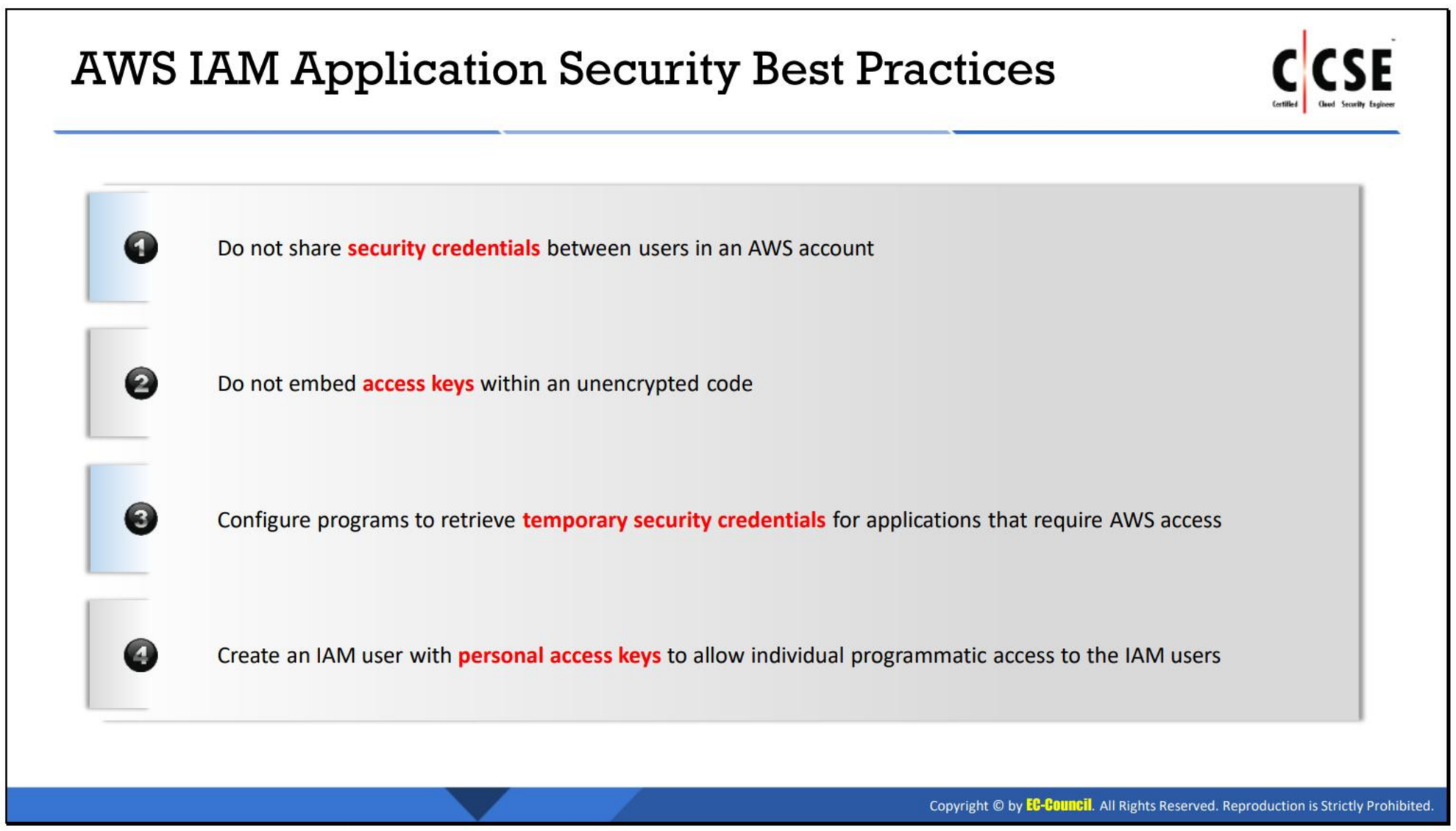
- **AWS Config**: Use AWS Config to get detailed historical information about the configuration of AWS resources, including IAM users, groups, roles, and policies.

  Features:

  - **Configuration history of AWS resources** provides the configuration history.
  - **Configuration history of software** allows one to record software configuration changes within your Amazon EC2 instances and servers running on-premises, as well as servers and virtual machines in environments provided by other cloud providers.
  - **Resource relationships tracking** allows discovering, mapping, and tracking AWS resource relationships in your account.

- **Amazon Simple Storage Service (Amazon S3):** Use Amazon Simple Storage Service (Amazon S3) logs to view details of access requests to Amazon S3 buckets. Amazon S3 also supports audit logs that list the requests made against S3 resources for complete visibility into who is accessing what data.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

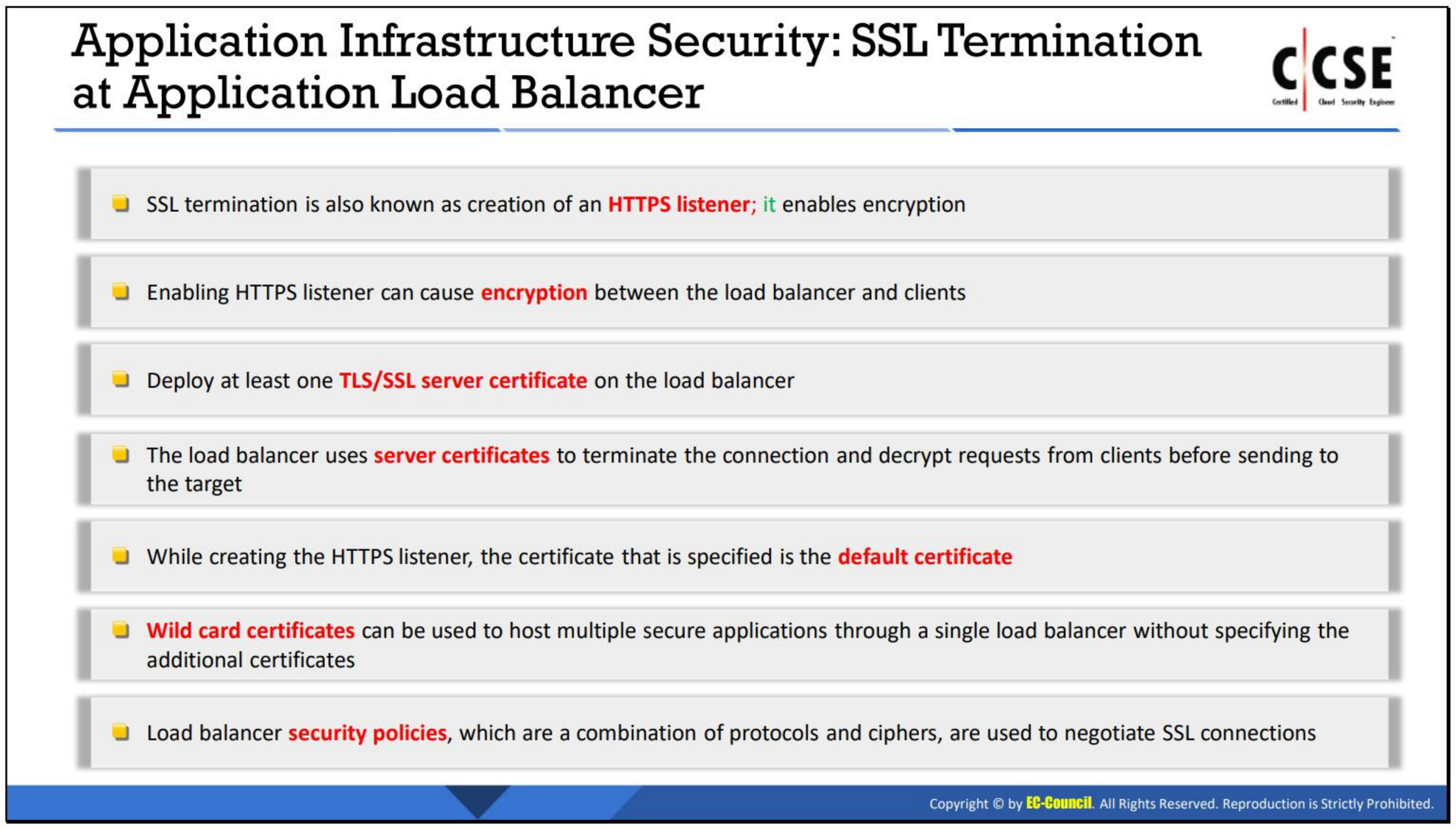


AWS IAM Application Security Best Practices

The following are some of the AWS IAM Application security best practices:

- Do not share security credentials between users in an AWS account.
- Do not embed access keys within an unencrypted code.
- Configure programs to retrieve temporary security credentials for applications that require AWS access.
- Create an IAM user with personal access keys to allow individual programmatic access to the IAM users.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Application Infrastructure Security: SSL Termination at Application Load Balancer

To prevent security exploits on applications deployed in AWS, it is important to protect the infrastructure hosting the application. Application security should enforce the best practices for both security in transit and security at rest.

hidori.ir

- For every point in the infrastructure, there should be security in transit.
- Wherever data is stored, there should be the security of data at rest.
- Security exploits should be detected and responded to proactively.

SSL Termination at Application Load Balancer

- SSL termination, also known as the creation of an HTTPS listener, enables encryption.
- Enabling an HTTPS listener can cause encryption between the load balancer and clients.
- At least one TLS/SSL server certificate should be deployed on the load balancer.
- Using server certificates, the load balancer can close a connection and decrypt the client requests before sending them to the targets.
- While creating the HTTPS listener, the certificate that is specified is the default certificate.
- Wild card certificates can be used to host multiple secure applications through a single load balancer without specifying the additional certificates.
- Load balancer security policies, which are a combination of protocols and ciphers, are used to negotiate SSL connections.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

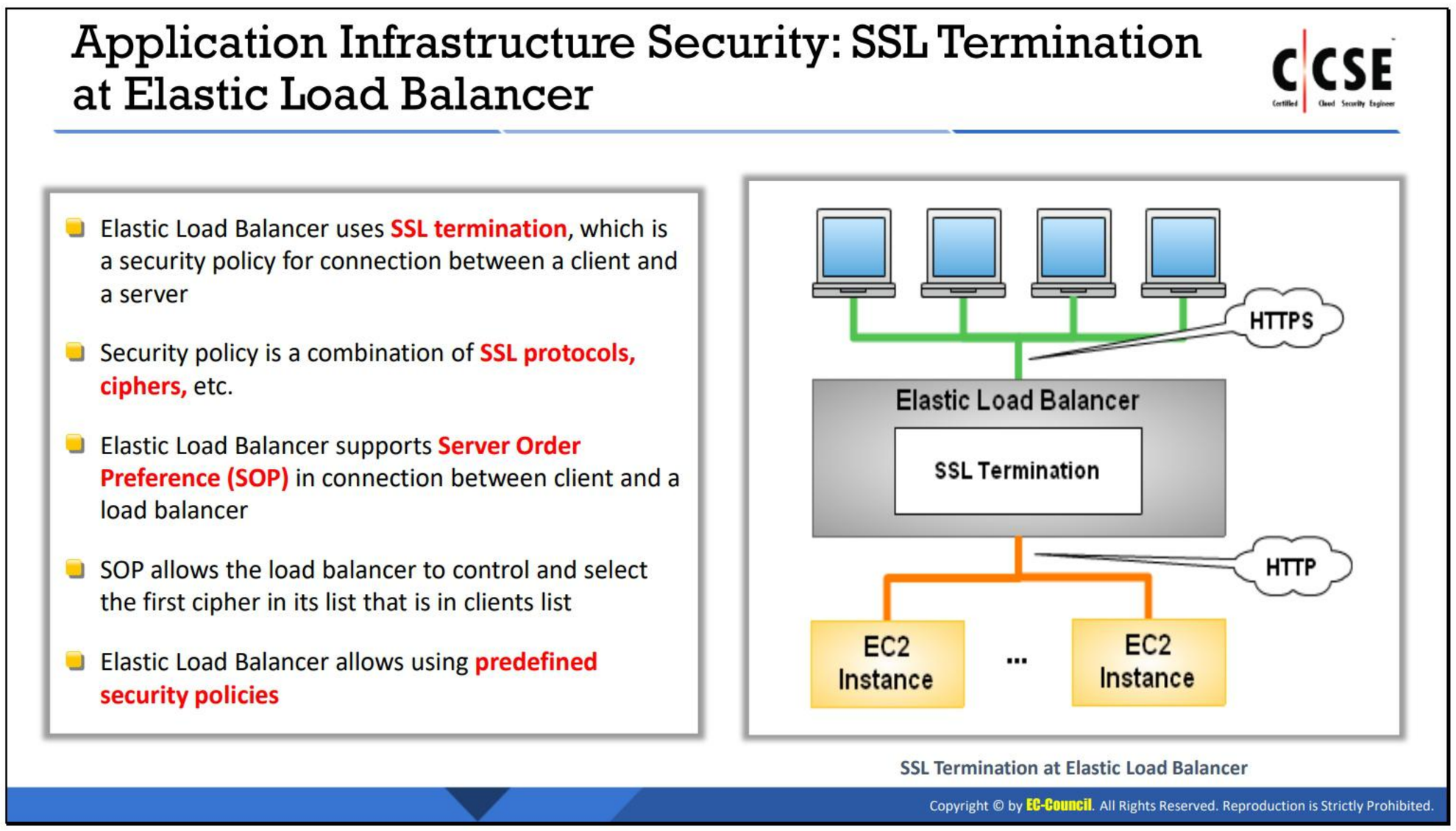
Source: https://aws.amazon.com

Adding an HTTPS Listener at Application Load Balancer

- Open the Amazon EC2 Console.
- On the **Navigation** pane under **Load Balancing**, select **Load Balancers**.
- Select a load balancer.
- Choose **Listeners, add listener**.
- In **Protocol: Port**, select **HTTPS** and enter a port.
- For Default actions
  - Choose **Add Action, Forward To** and select a target group.
  - Choose **Add Action, Redirect To**, give the URL for redirection.
  - Choose **Add Action, Return Fixed Response**, give a response code.
  - Choose checkmark icon to save.
- Keep the Default Security Policy for **Security Policy.**
- For **Default SSL Certificate**
  - **From ACM** choose the certificate, if a certificate is created or imported.
  - Choose **From IAM** and choose the certificate, if uploaded using IAM.
- Select **Save.**

video1.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Application Infrastructure Security: SSL Termination at Elastic Load Balancer

Elastic Load balancer uses SSL termination, a security policy to connect both a client and a server. A security policy comprises SSL protocols, ciphers etc. Elastic load balancer with server order preference (SOP) support allows negotiating connections from a client to a load balancer. The load balancer is allowed by SOP to control and select the first cipher in SOP's list (in clients list). Elastic load balancer allows the use of predefined security policies.

Use the following steps for adding SSL termination to Elastic Load Balancer:

- Create or purchase a certificate.
- Upload the certificate to the AWS account and retrieve ID.
- Create a new Load Balancer that has an HTTPS listener and supply the retrieved certificate ID.

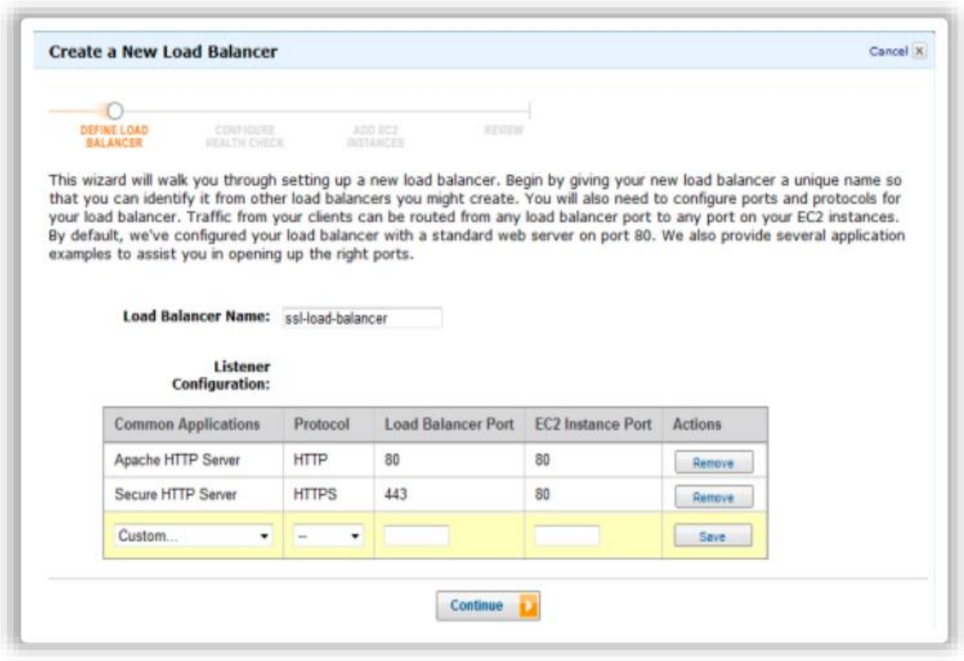


FIGURE 3.64: Listener Configuration

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

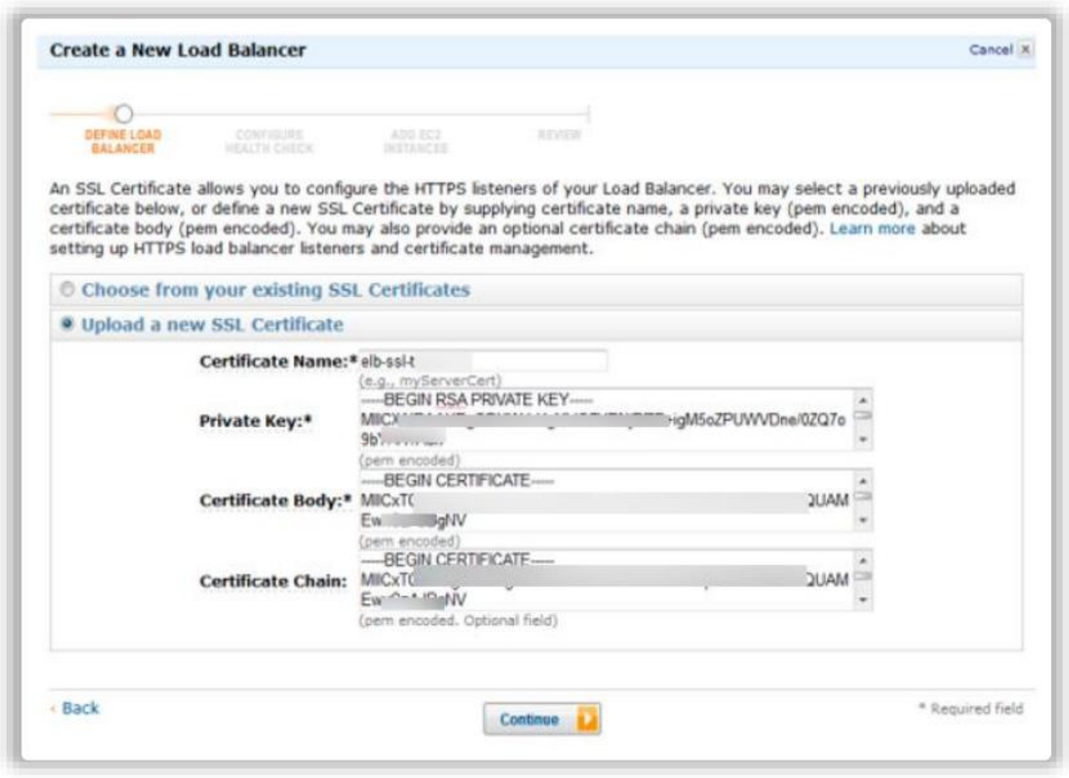


FIGURE 3.65: New SSL Certificete

- Perform a health check and associate EC2 instances with the load balancer.

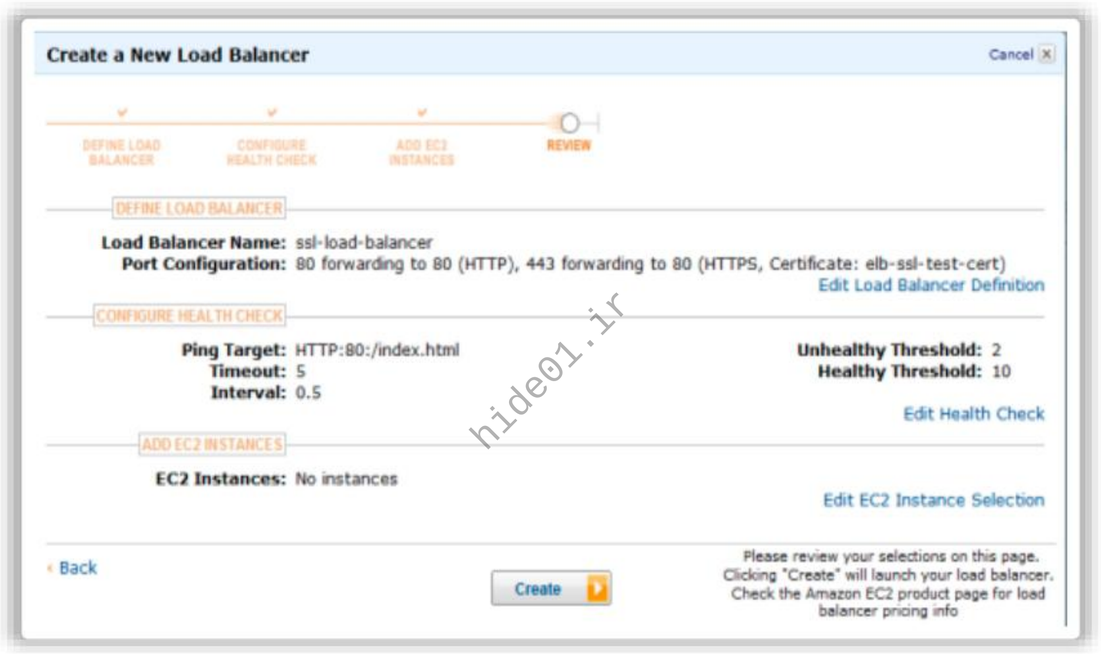


FIGURE 3.66: Review

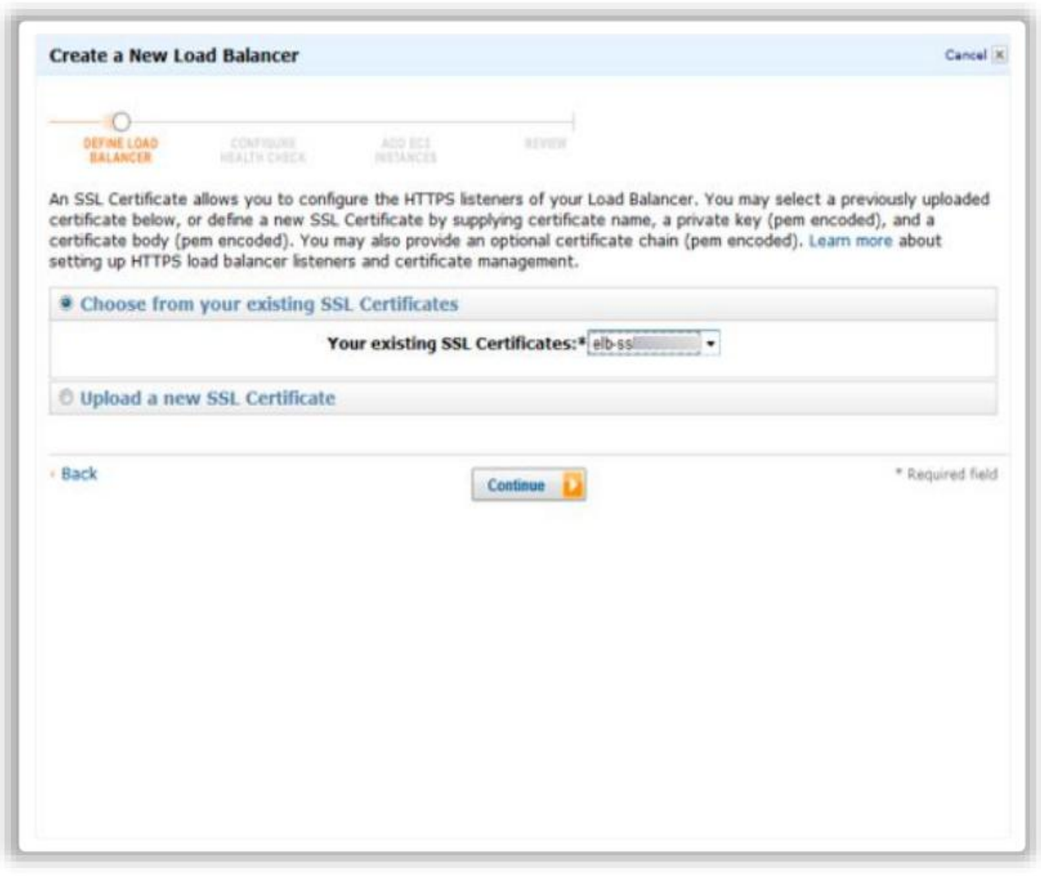
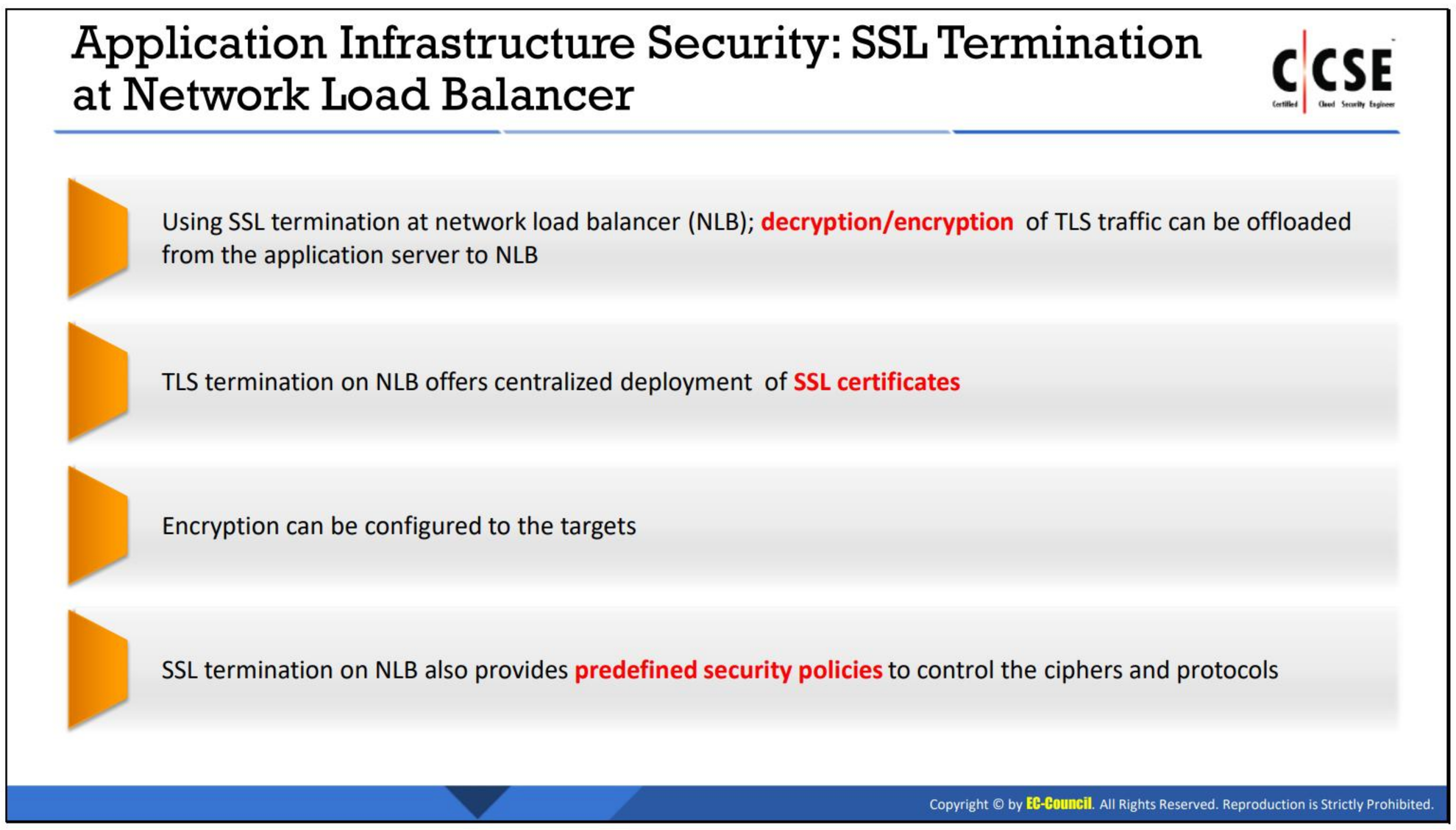


FIGURE 3.67: Choose Existing SSL Certificate

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

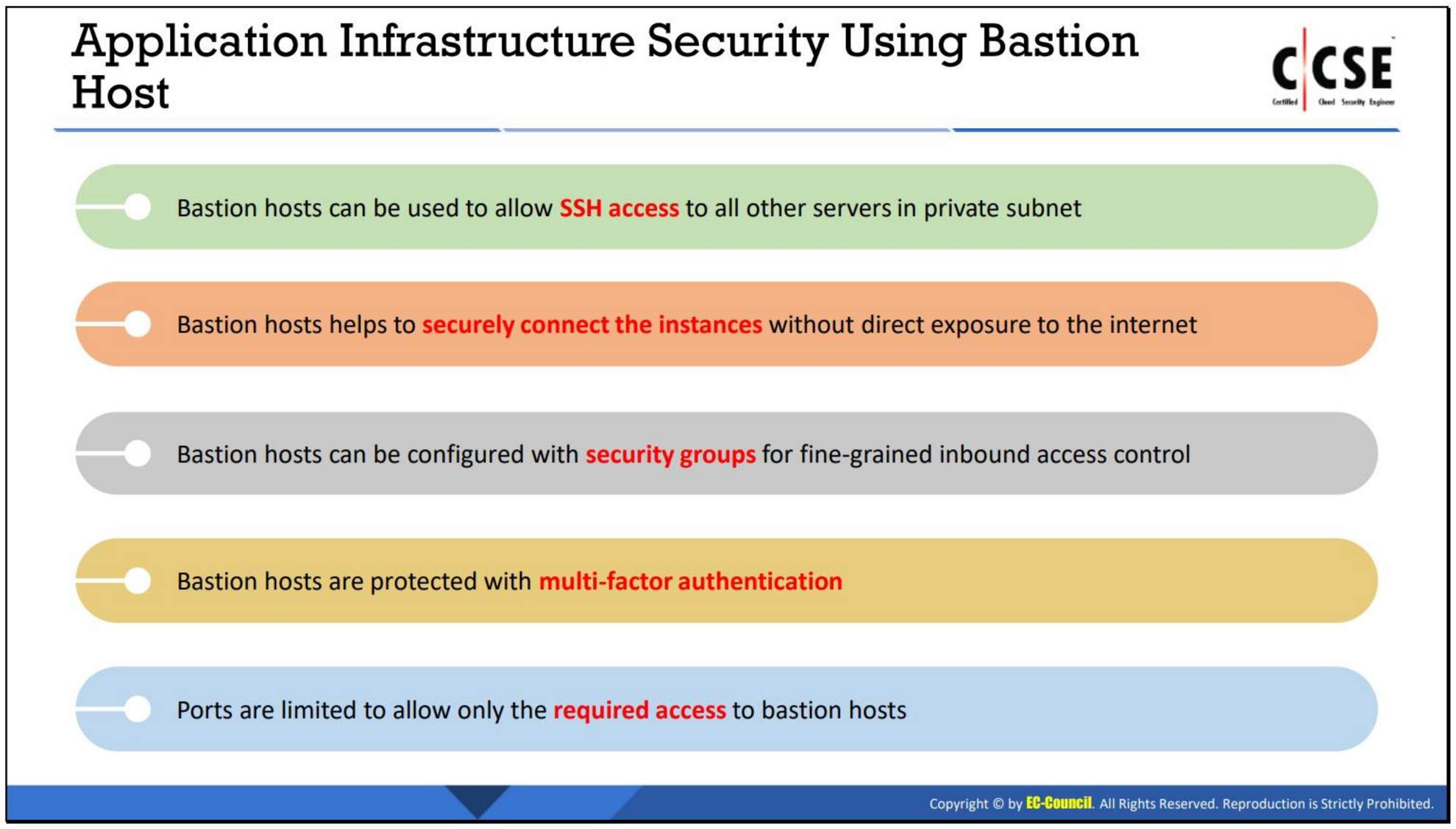


Application Infrastructure Security: SSL Termination at Network Load Balancer

- Using SSL termination at network load balancer (NLB); decryption/encryption of TLS traffic can be offloaded from the application server to NLB.
- TLS termination on NLB offers centralized deployment of SSL certificates.
- Encryption can be configured to the targets.
- SSL termination on NLB also provides predefined security policies to control the ciphers and protocols.

h3le01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Application Infrastructure Security using Bastion Host

- Bastion hosts can be used to allow SSH access to all other servers in a private subnet.
- This helps connect the instances without direct exposure to the internet securely.
- Bastion hosts can be configured with security groups for fine-grained inbound access control.
- Bastion hosts are protected with MFA.
- Ports are limited to allow only the required access to bastion hosts.

Source:https://aws.amazon.com

Bastion Hosts Deployment Steps

Step 1: Prepare account.

- Creating a user account at aws.amazon.com.
- Choose the AWS region.
- Creating a key pair in preferred region. In the navigation pane, select **Key Pairs, Create Key Pair,** type a name and choose **Create.**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

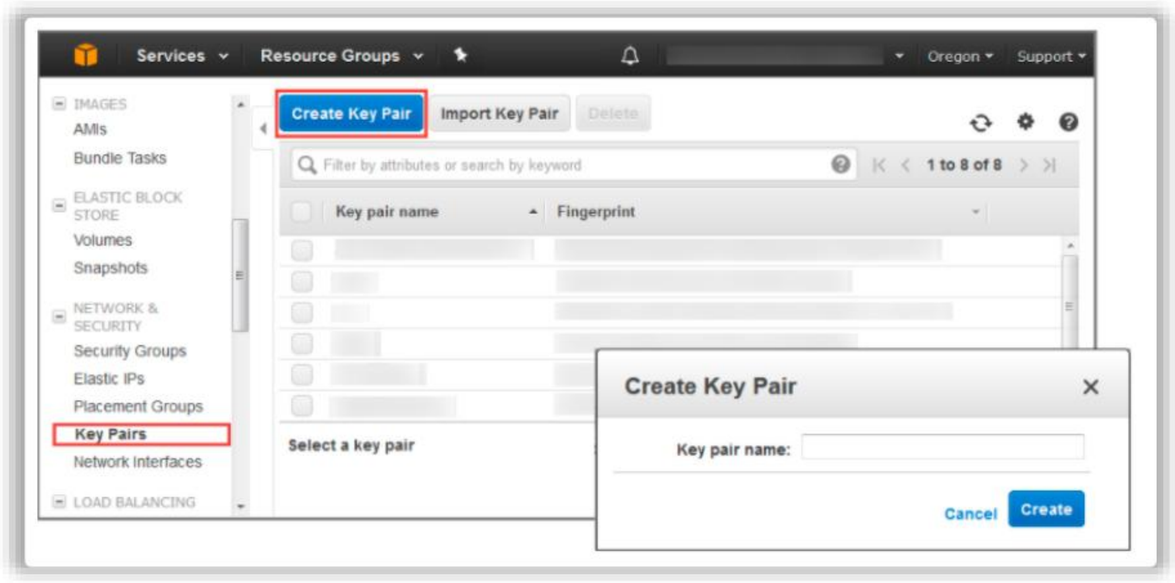


FIGURE 3.68: Create Key Pair

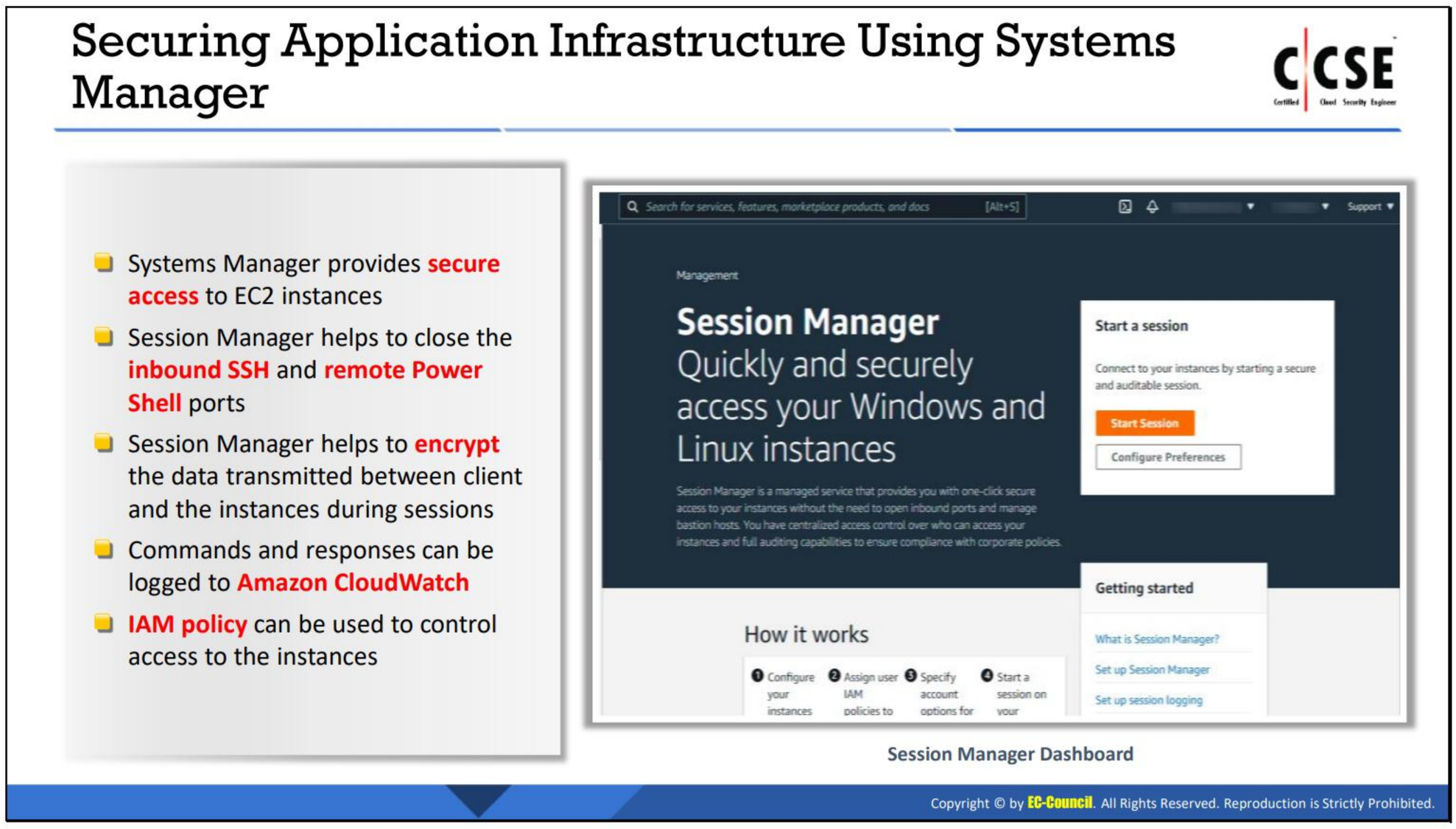
Step 2: Launch the stack.

- Subscribe to CentOS AMI in AWS Marketplace if the CentOS operating system is used.
- Two options can be used to launch the AWS CloudFormation Template
  - Launch Quick Start (for new VPC)
  - Launch Quick Start (for existing VPC)
- Keep default settings for Amazon S3 template URL on **Select Template** page and click **Next.**
- Review the parameters for the template on **Specify Details** page, provide value for parameters and click **Next.**
- On **Options** page, specify tags for resources and set advanced options, and click **Next.**
- Review and confirm the template settings on **Review** page.
- Select the checkbox to acknowledge that the template will create IAM resources under **Capabilities.**
- Choose **Create** to deploy the stack.
- Monitor the status, if it is **CREATE_COMPLETE**, the stack is ready.
- Login to the bastion host using one of the following usernames based on parameter setting.
  - Amazon Linux – **ec2-user**
  - CentOS – **centos**
  - Ubuntu – **ubuntu**

Step 3: Deploy applications on top of this AWS infrastructure.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Securing Application Infrastructure using Systems Manager

- Systems Manager provides secure access to EC2 instances.
- Session Manager helps close inbound SSH and remote PowerShell ports.
- Session Manager helps encrypt the data transmitted between client and the instances during sessions.
- Commands and responses can be logged to Amazon CloudWatch.
- IAM policy can be used to control access to the instances.

Session Manager Configuration

- Open the **AWS System Manager** and click **Preferences.**
- Enter the name of S3 bucket and CloudWatch Log Group, to log the commands.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

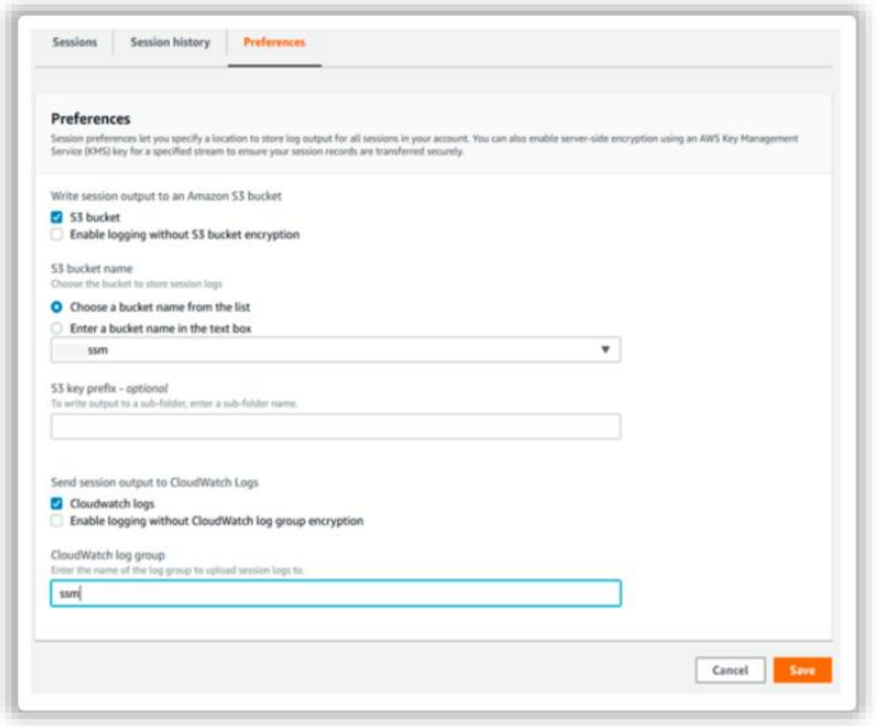


FIGURE 3.69: Naming S3Bucket & CloudWatch

- Click **Session**, and then click on **Start Session.**

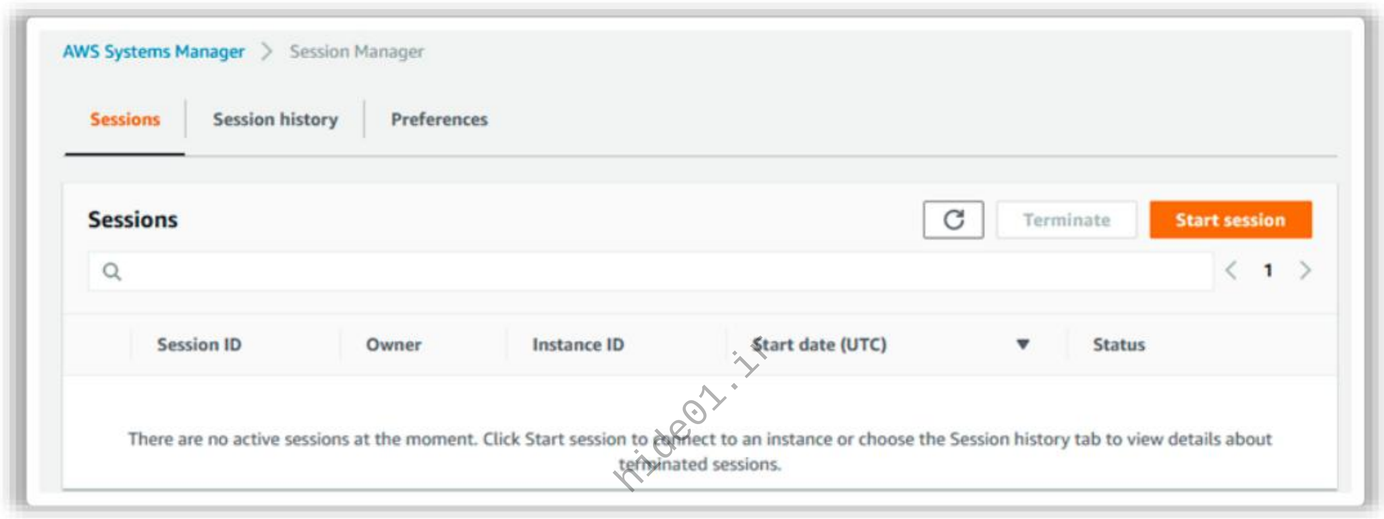


FIGURE 3.70: Session

- Select an instance and click **Start Session** again.

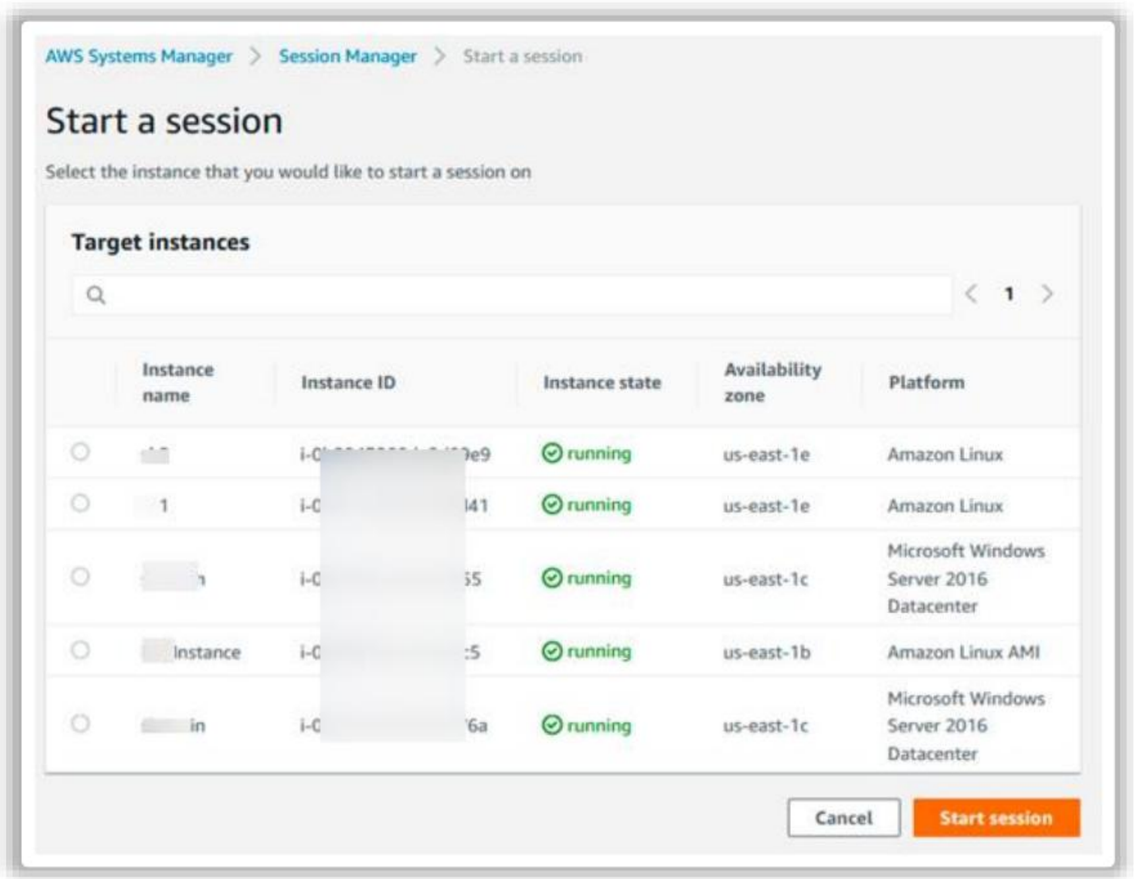


FIGURE 3.71:Start Session

- The session will open up.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

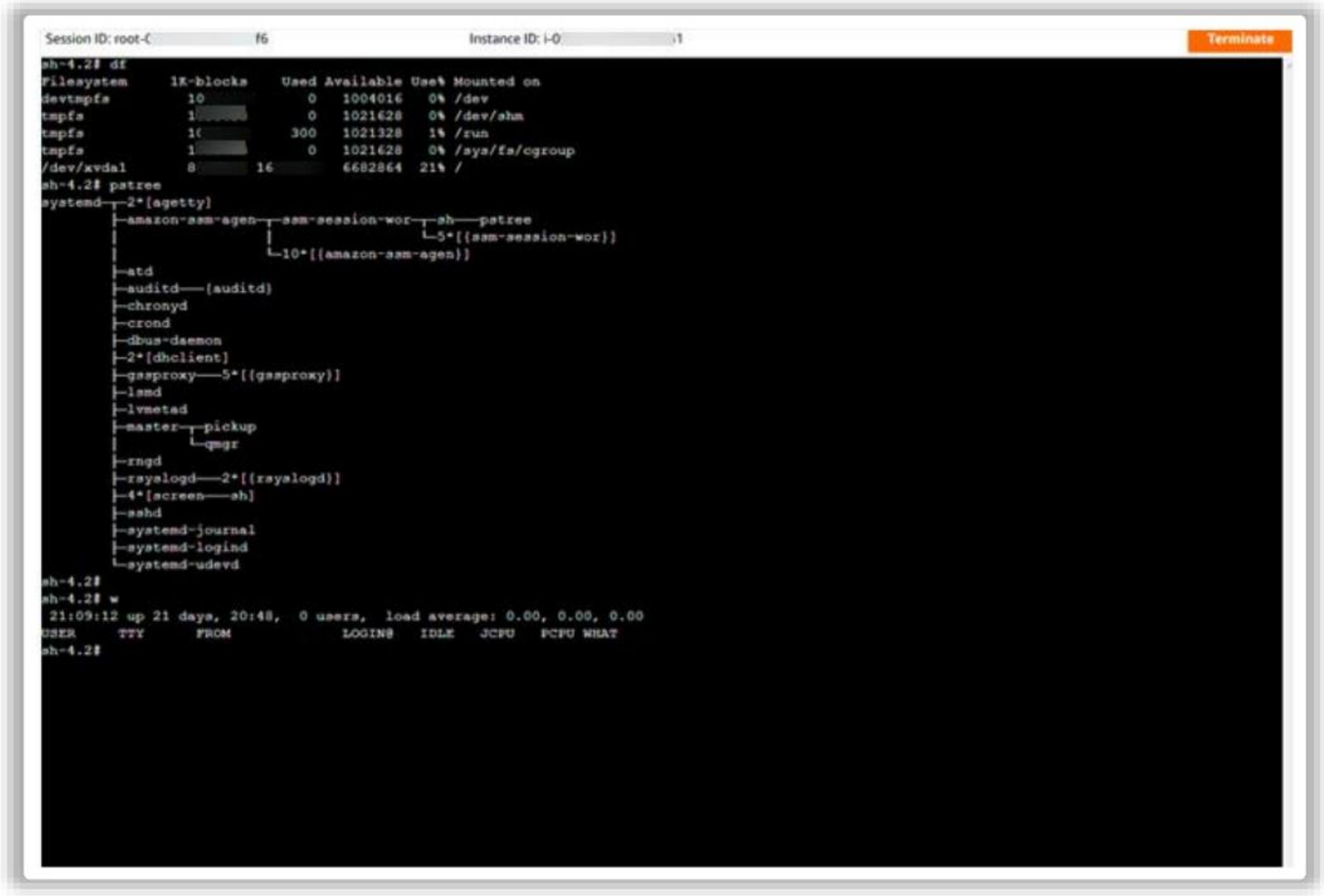


FIGURE 3.72: Session Open Up

- Log streams are available in CloudWatch.

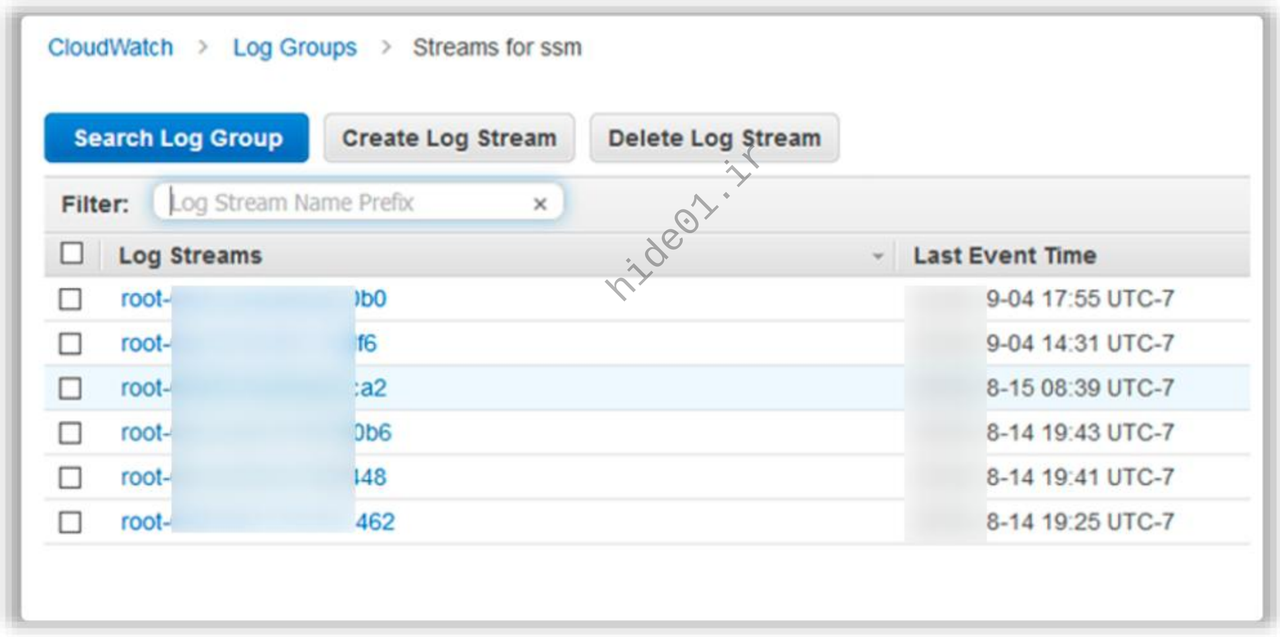
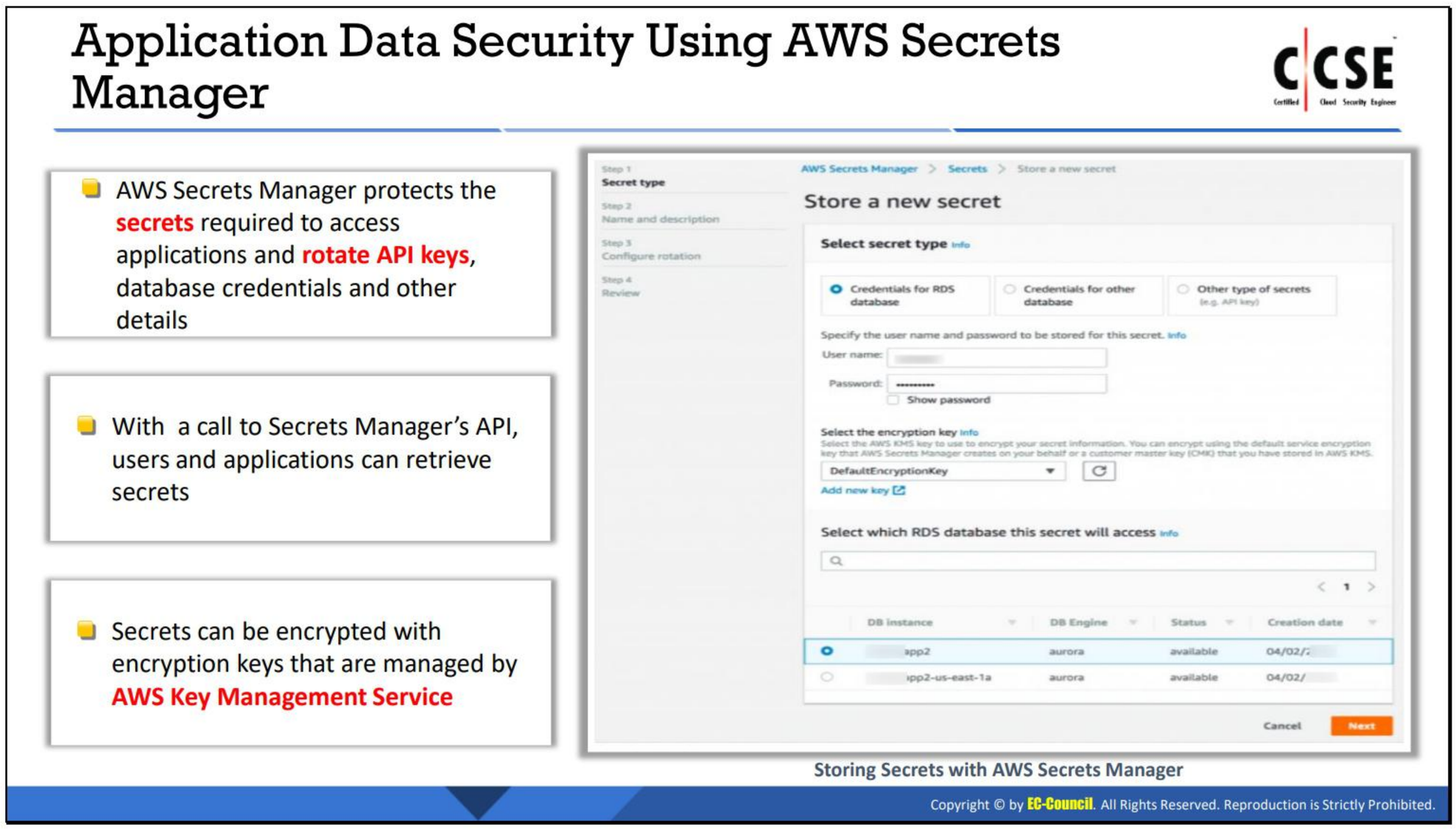


FIGURE 3.73: Log Stream

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Storing Secrets with AWS Secrets Manager

Application Data Security using AWS Secrets Manager

All data should be encrypted, whether stored in databases or servers, to prevent it from being accessed by an attacker. Application secrets, such as passwords, can be protected using certain AWS features. AWS Secrets Manager can protect the secrets needed to access the application. It enables users to easily rotate, manage, and retrieve database credentials, API keys, and other secrets. With a call to Secret Manager APIs, the applications can retrieve the secrets. The access to the secrets can be controlled using fine-grained permissions. The security and compliance requirements of the application can be met by enabling rotation of secrets in a safe manner. For centralized auditing, Secrets Manager can be integrated with AWS logging and monitoring services. Parameter Store can be used to provide application access to third-party API keys, and database credentials to EC2 instances.

Using AWS Secrets Manager Console for Storing Secrets

- Click on **Store a New Secret.**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select the instance and provide the initial username and password.

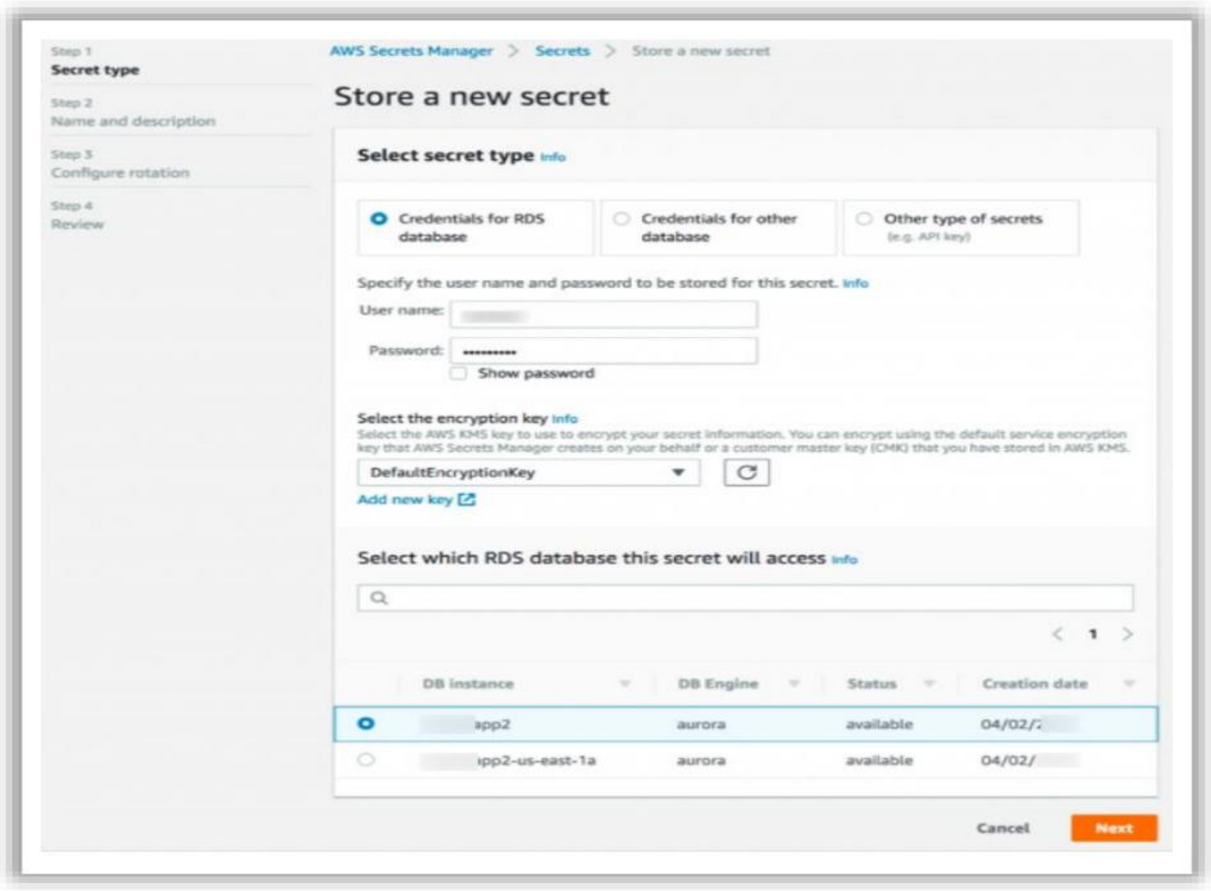


FIGURE 3.74:Instances

- Fill in the description and name to access the secret.

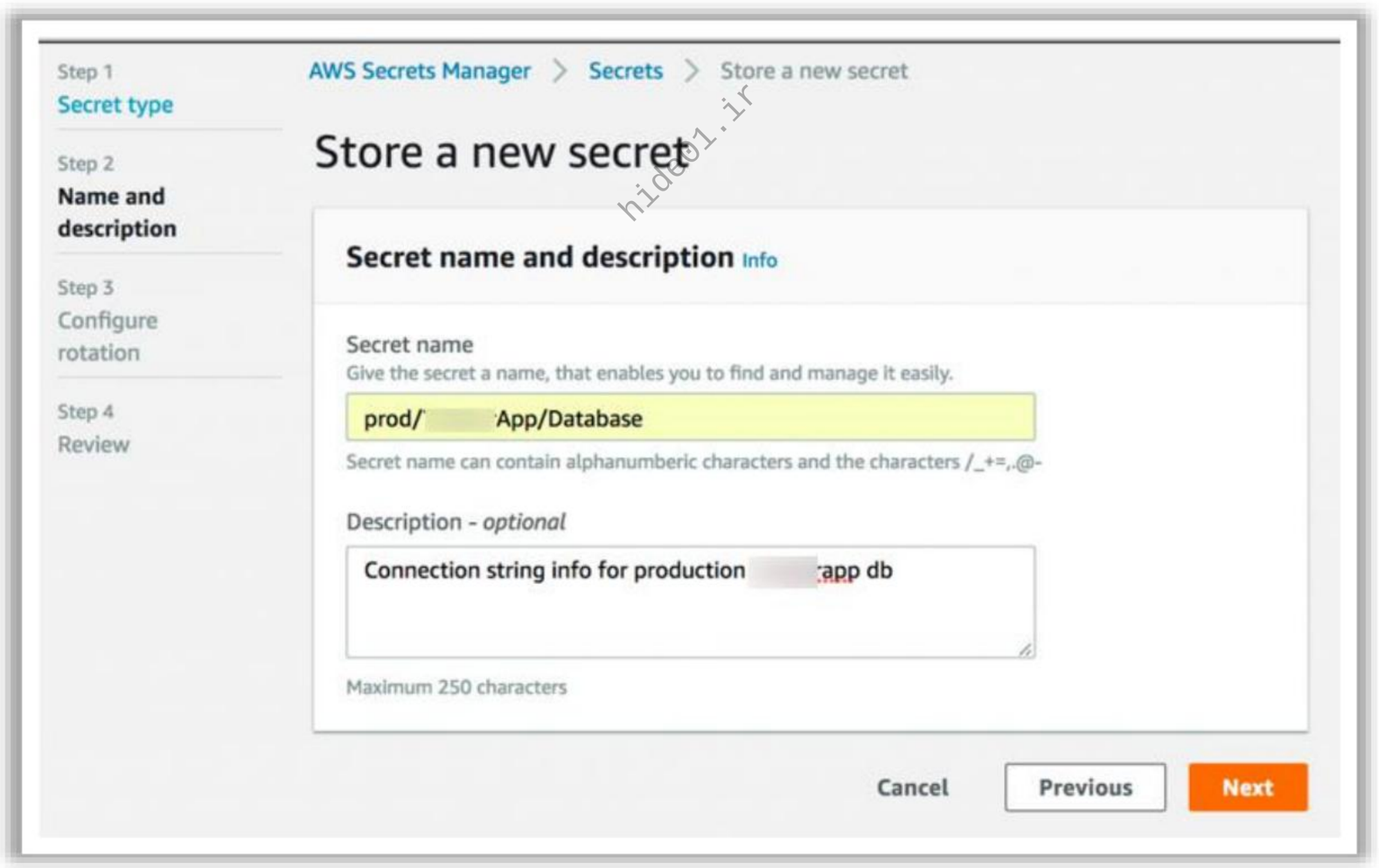


FIGURE 3.75: Secret Name & Description

- Configure rotation to rotate the password every 10 days.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

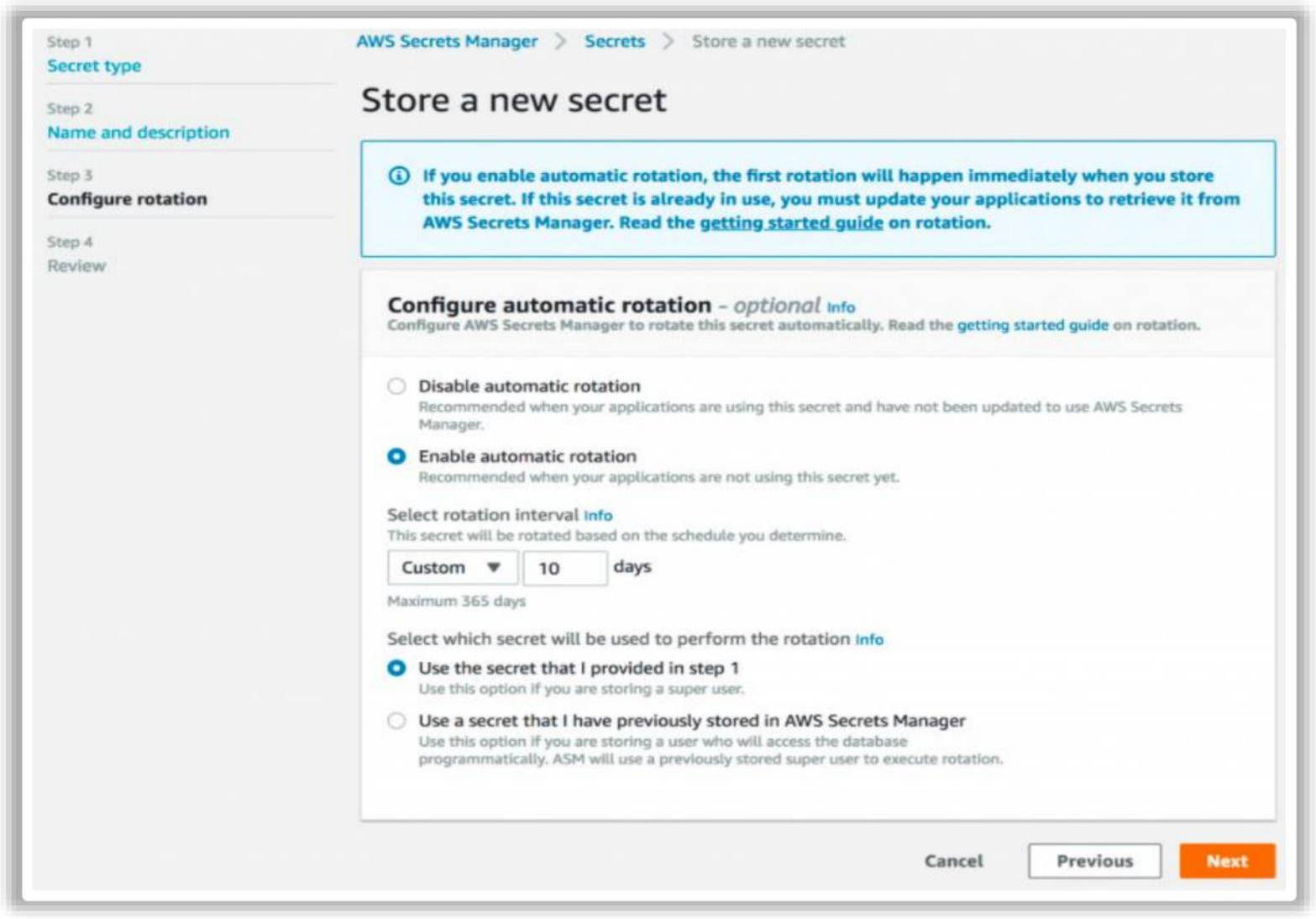


FIGURE 3.76: Configure Password

- Review all the details and check the code for storing and retrieving the secret.

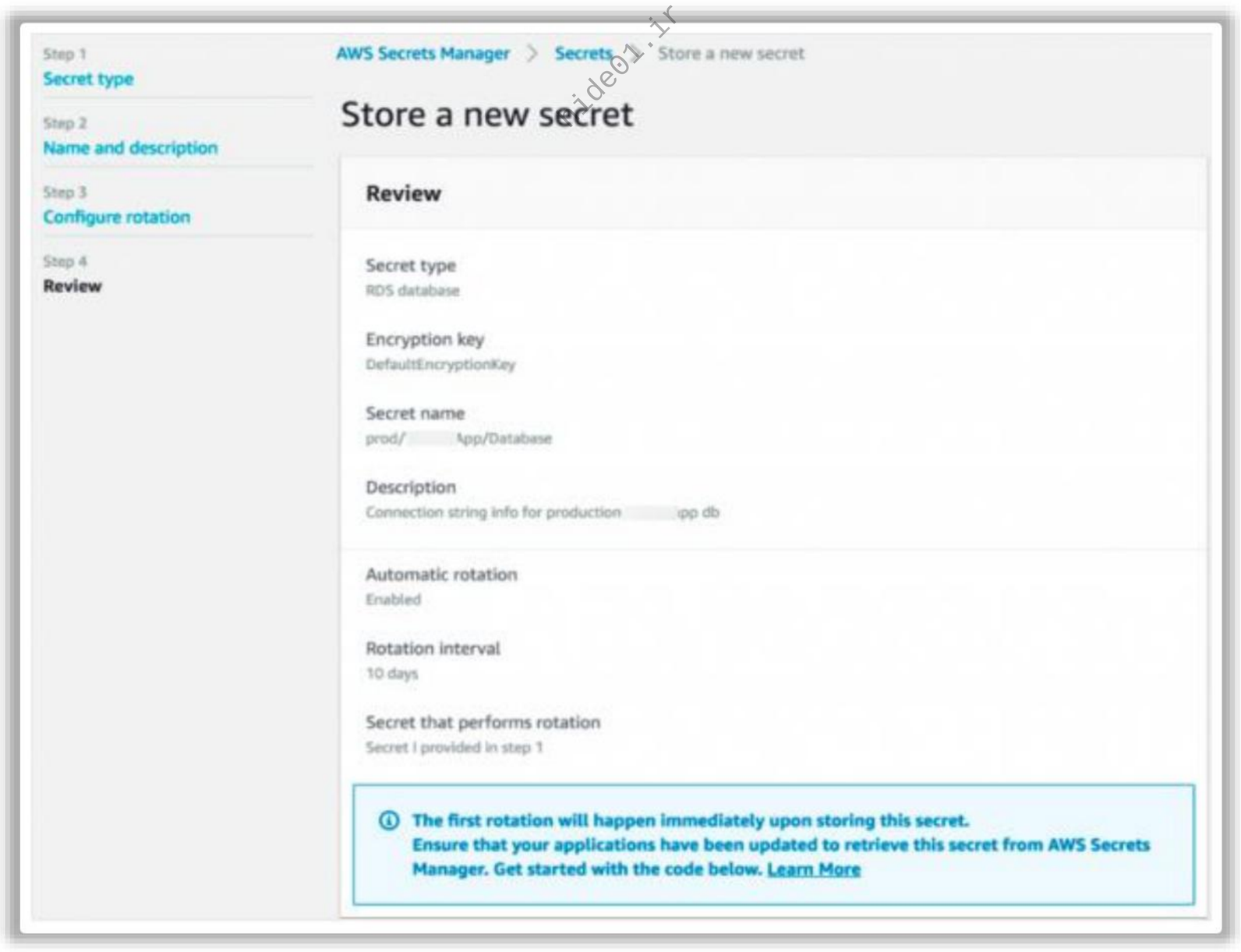


FIGURE 3.77: Review

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

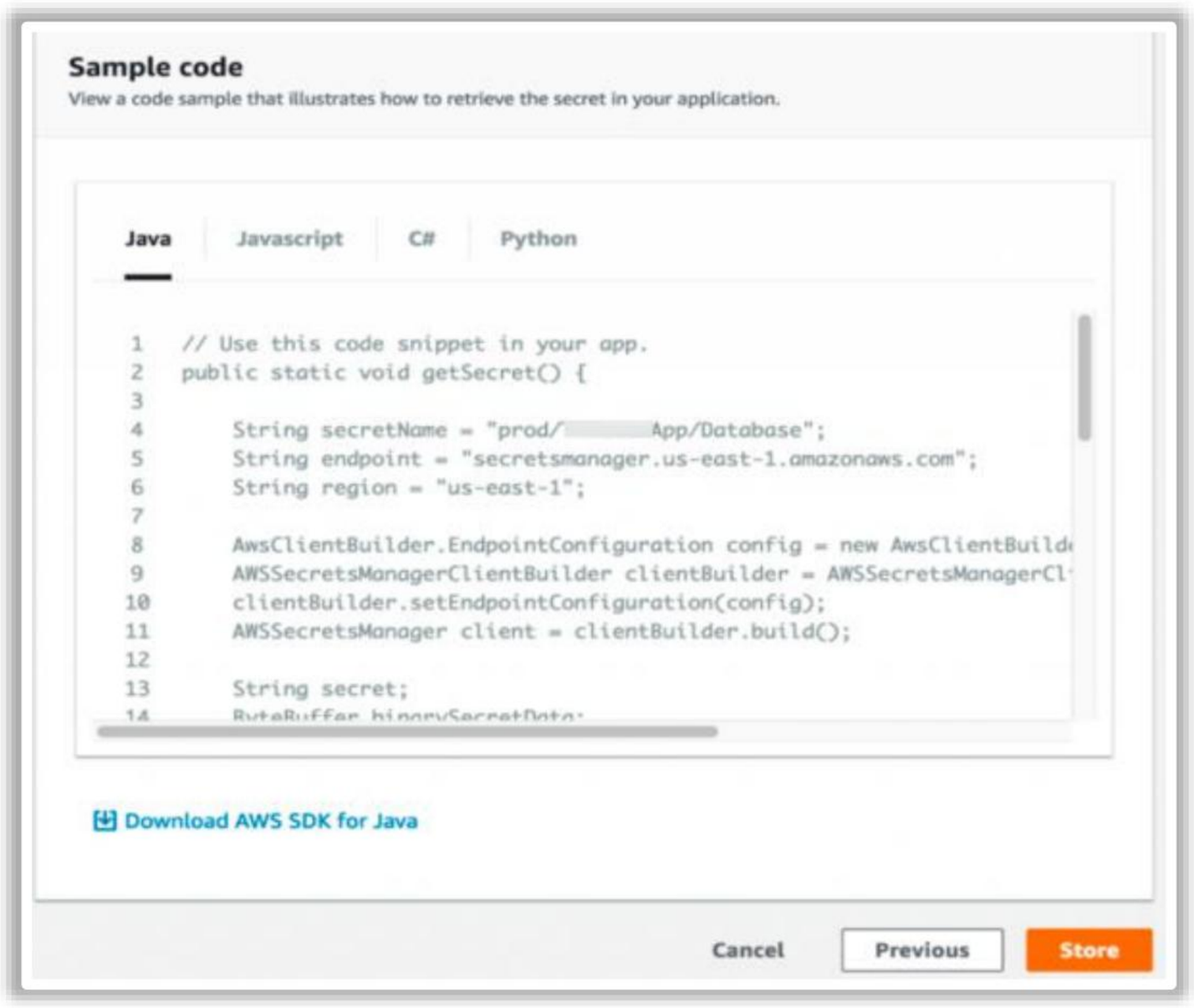


FIGURE 3.78: Sample Code

hide01.ir

- The secrets can be reviewed in the console.

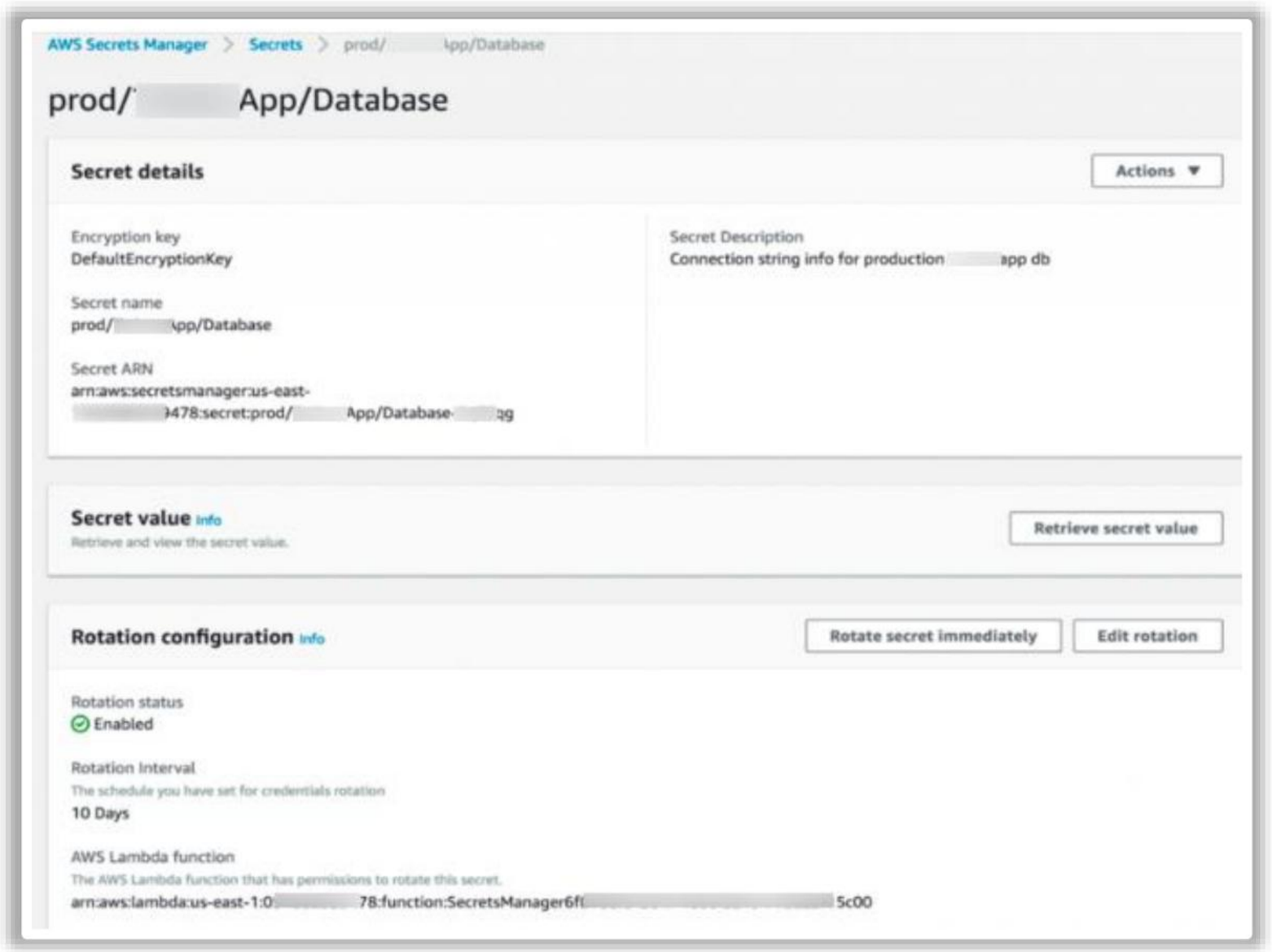


FIGURE 3.79: Review Secret

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Store OAuth Application keys.

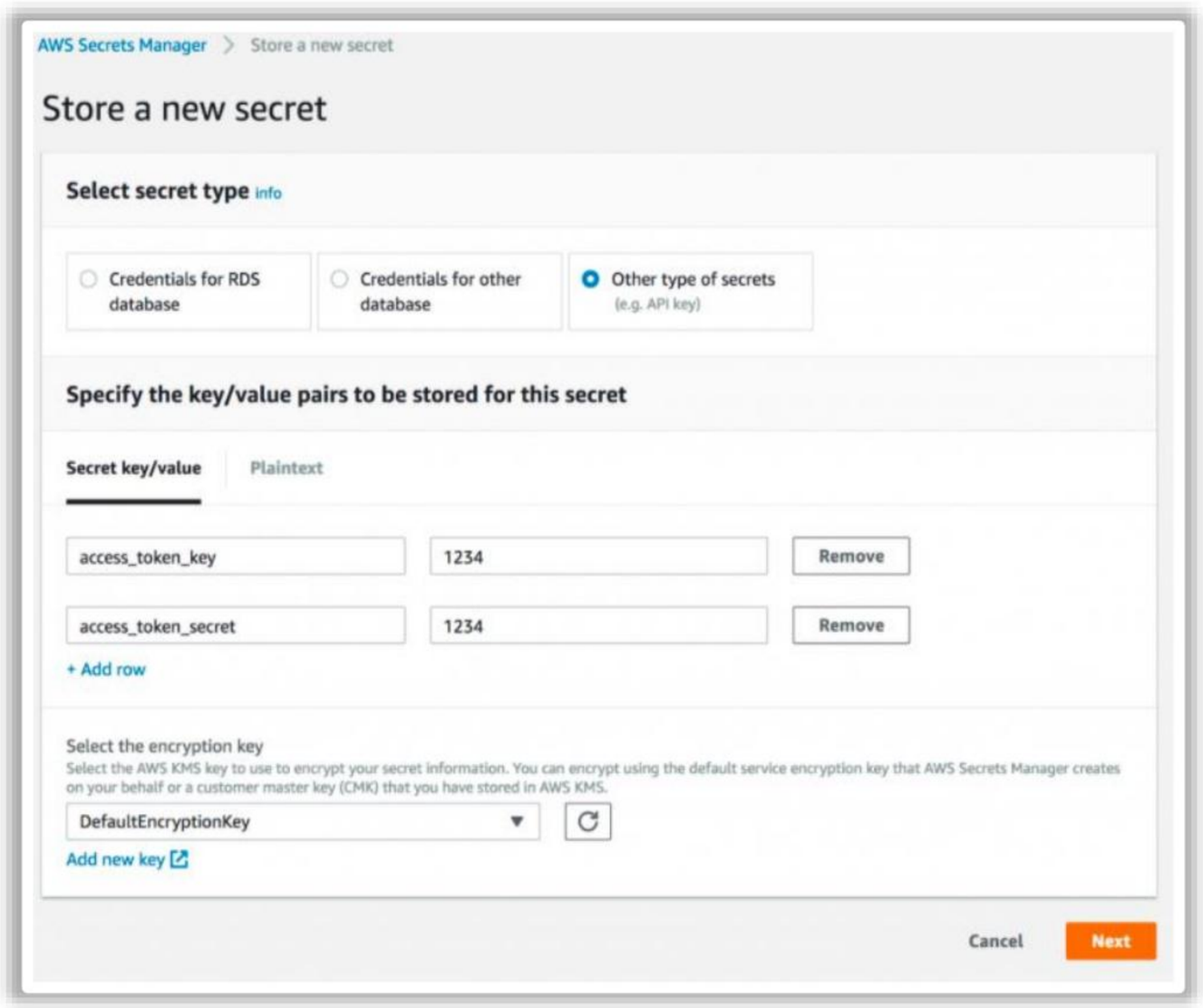


FIGURE 3.80: Store OAuth Application Key

hide01.ir

- Enable third-party OAuth credentials with custom AWS Lambda Function that can call the application to rotate the credentials.

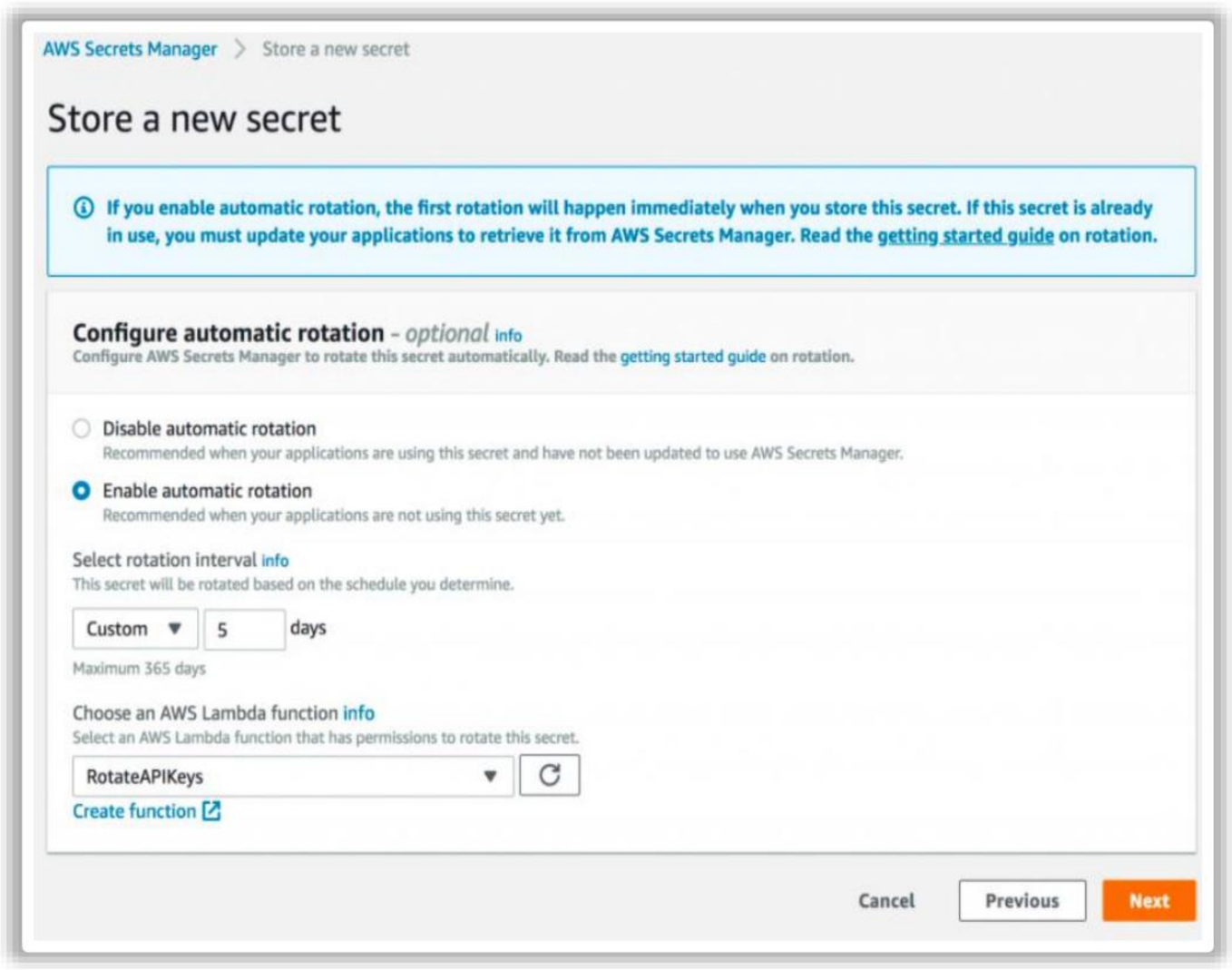
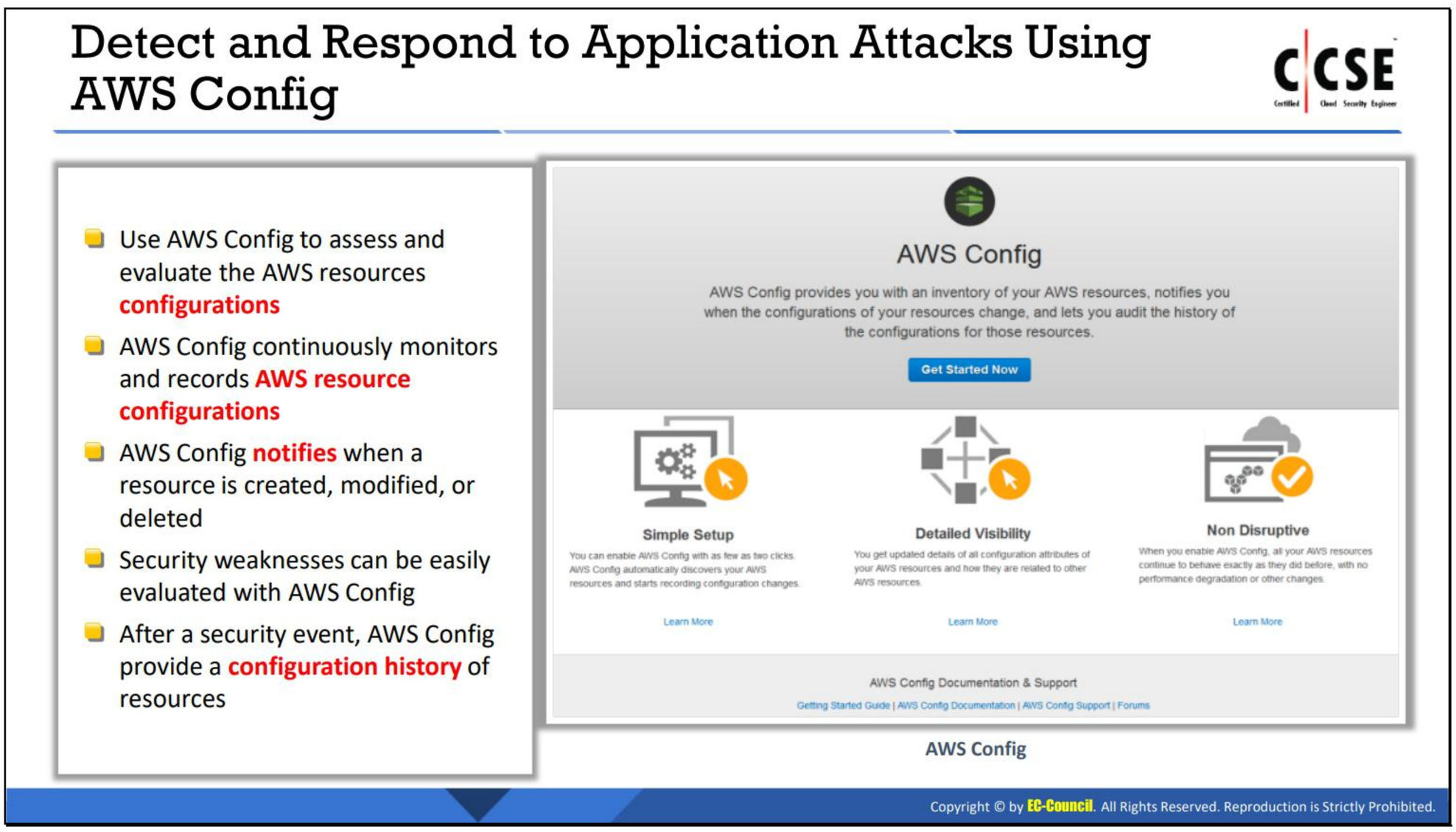


FIGURE 3.81: Enable third-party OAuth Credential

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Detect and Respond to Application Attacks using AWS Config

AWS Config is used to assess and evaluate the configurations of AWS resources. It continuously monitors and records the configurations and automates it to check whether it meets the desired configuration. With Config, the configuration changes can be reviewed. It notifies when a resource is created, modified, or deleted. If a change from a previous state is detected, the Amazon Simple Notification Service (SNS) will be delivered and actions can be taken accordingly. It defines the rules for provisioning and configuring AWS resources. AWS Config can be integrated with Amazon CloudWatch Events so that alerts can be monitored continuously. As it helps monitor resources continuously, any security weaknesses can be evaluated. The virtual dashboard can be checked whether the overall security requirements are met. After a security event, AWS Config provides a configuration history of resources. AWS Config can be integrated with AWS CloudTrail, which records events related to API calls, and hence the main cause of an issue can be identified.

How AWS Config Works

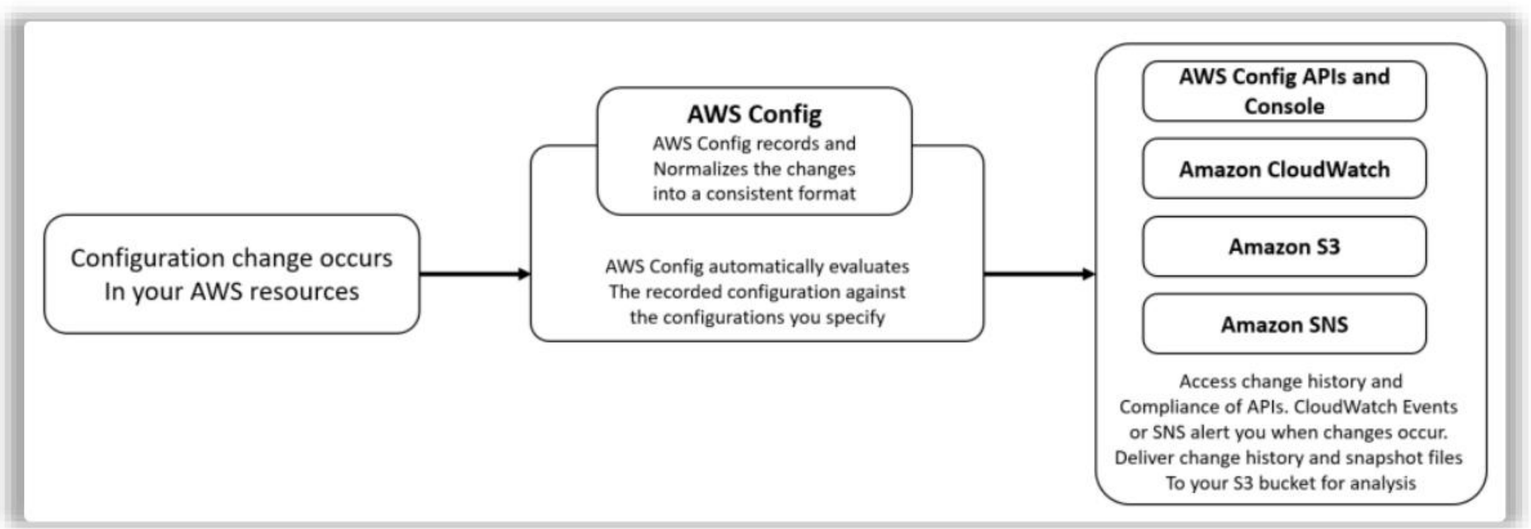


Figure 3.82: How AWS Config Works

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Steps to detect and respond to application attacks using AWS Config are as follows:

Step 1: Set up AWS Config.

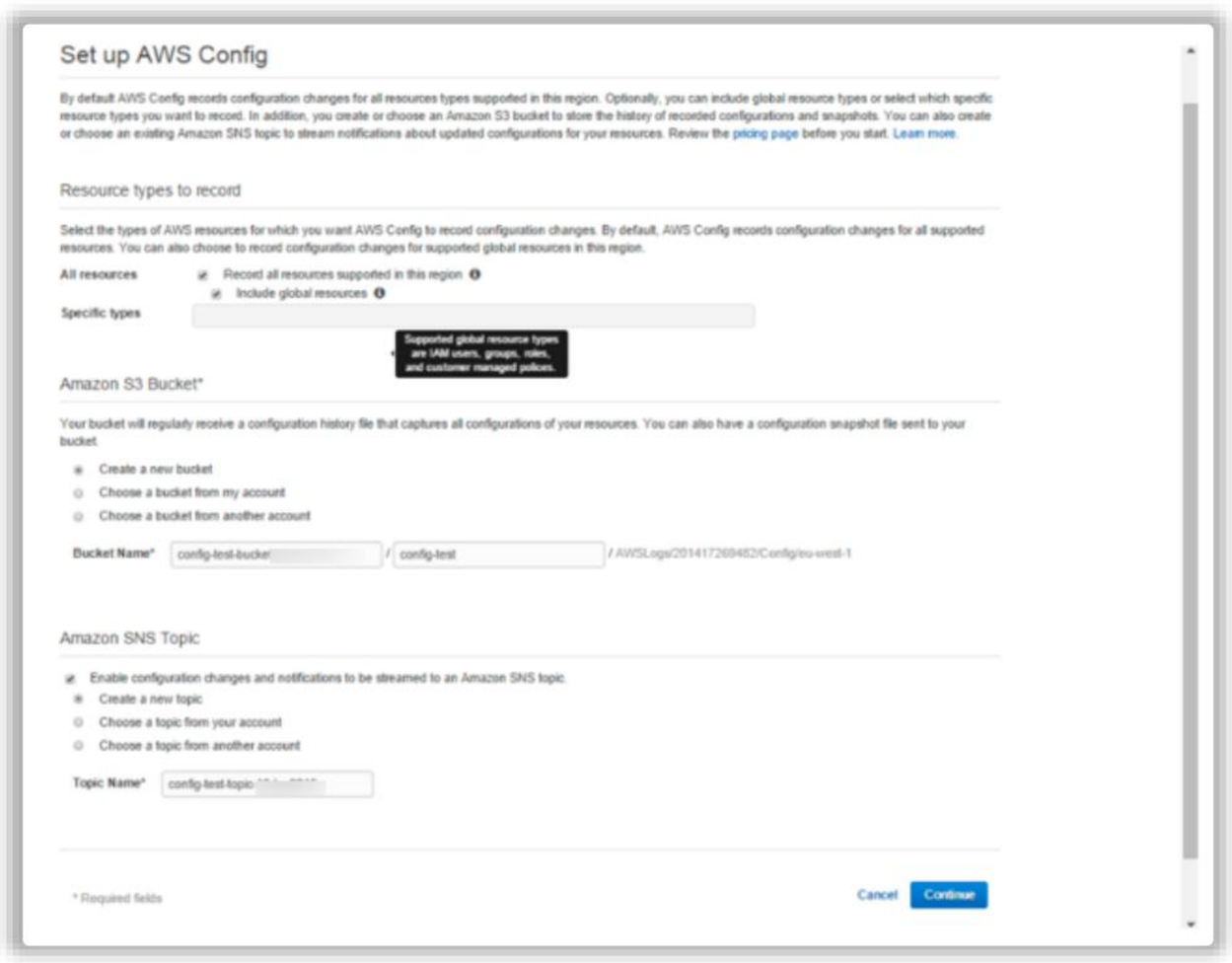


FIGURE 3.83: AWS Configuration

- Select **Record All Resources in this region.**
- Specify the bucket name and topic name.
- Click **Continue.**

hide01.ir

Step 2: Create IAM role.

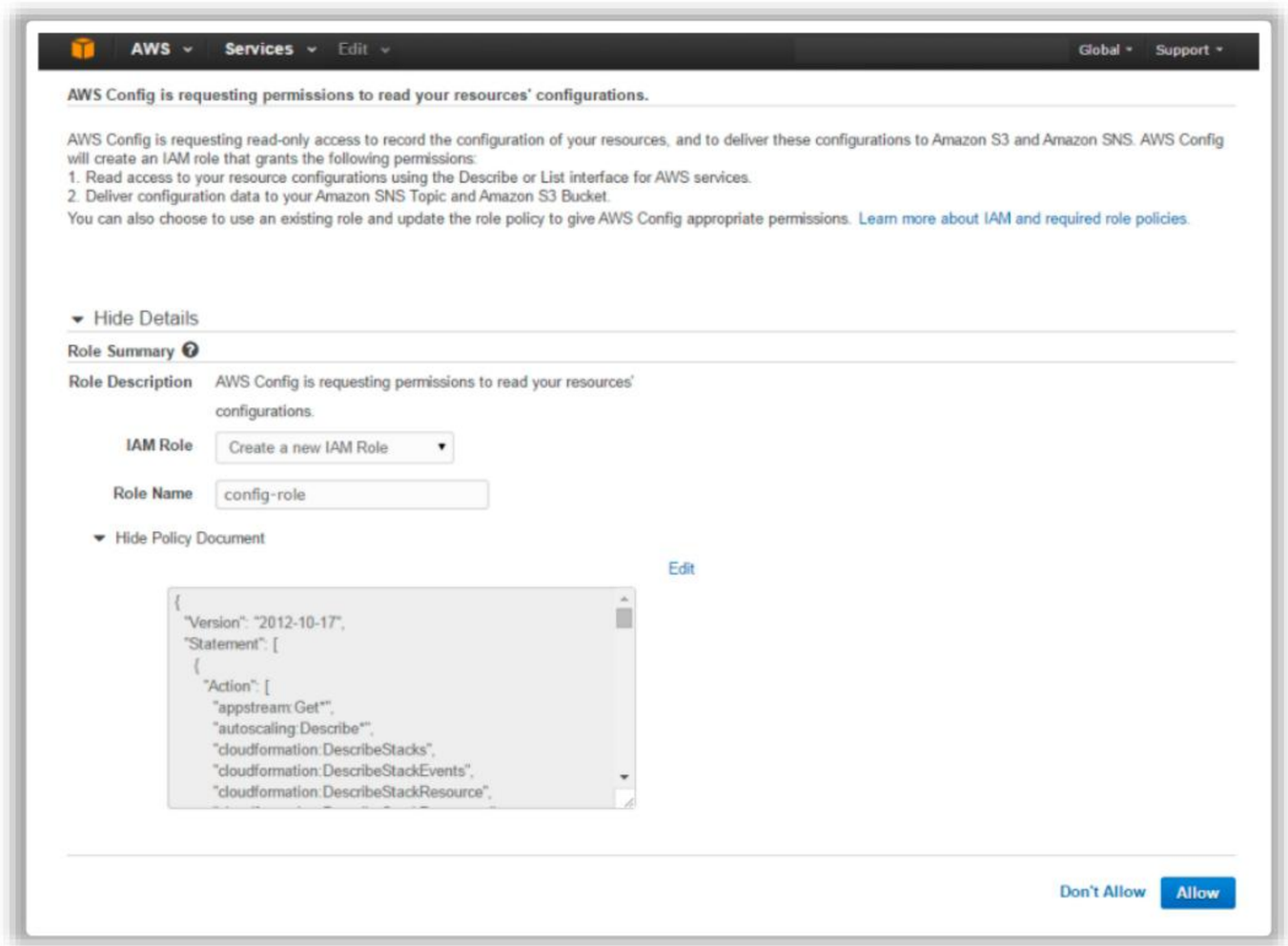


FIGURE 3.84: Create IAM Role

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click **Allow.**

Step 3: Resource inventory.

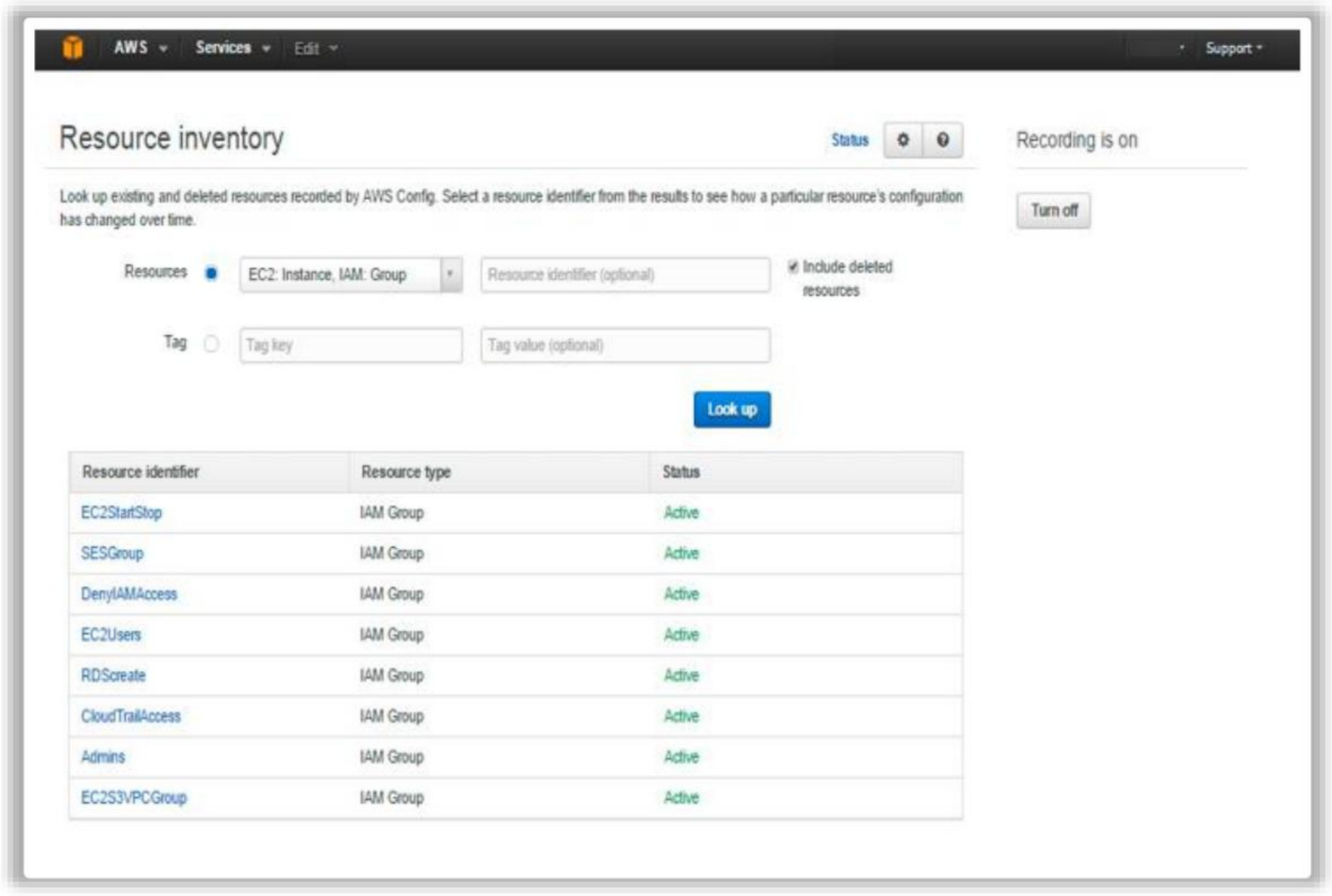


FIGURE 3.85: Resource Inventory

- Select **Resources** and click **Look Up** to view resources.

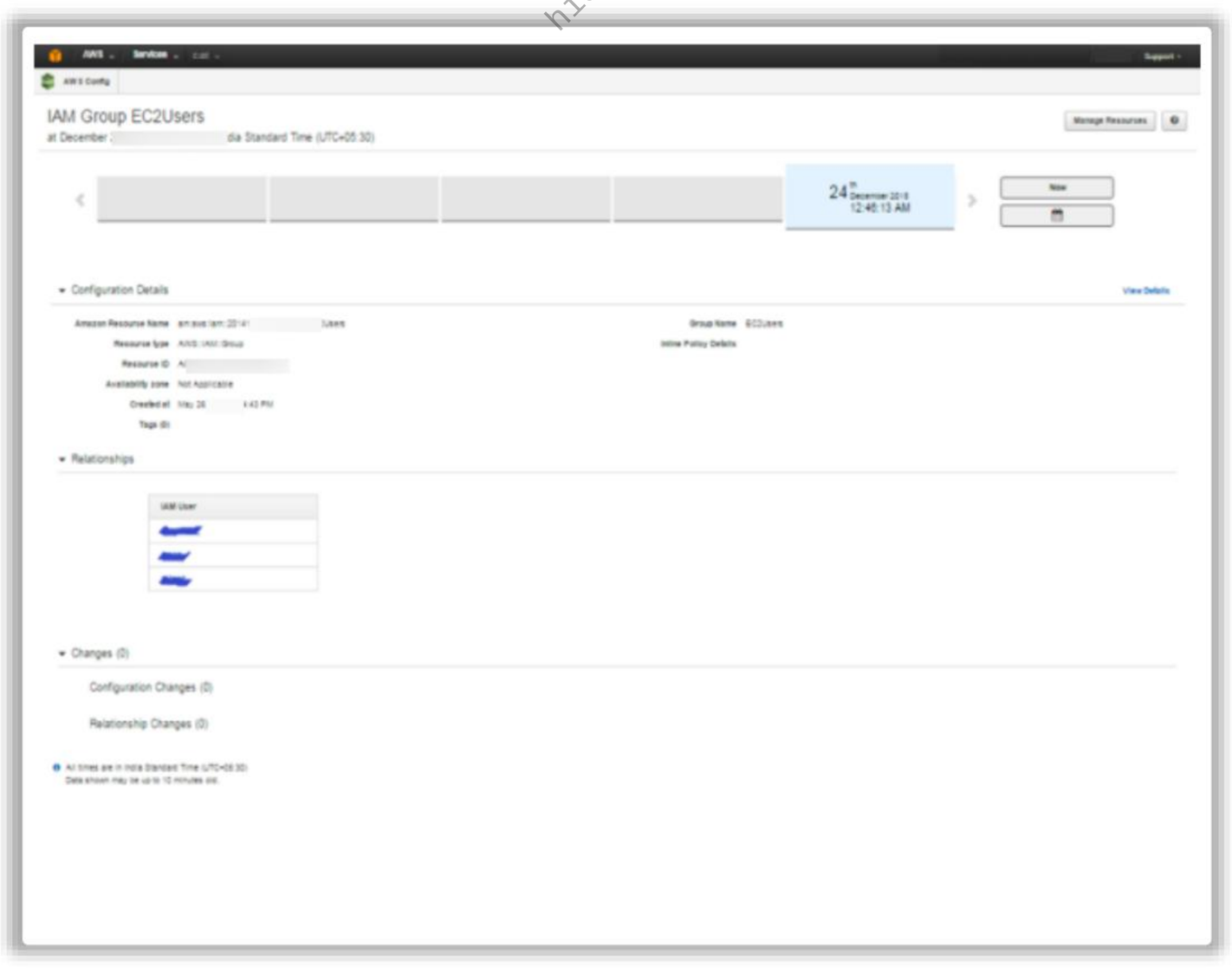


FIGURE 3.86: Create Resource

- Select **SNS service** from the **Services** menu and go to **SNS Home Page.**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- From **Topic,** select the topic recently created.
- Select and copy the ARN of the topic.

Step 4: Subscription.

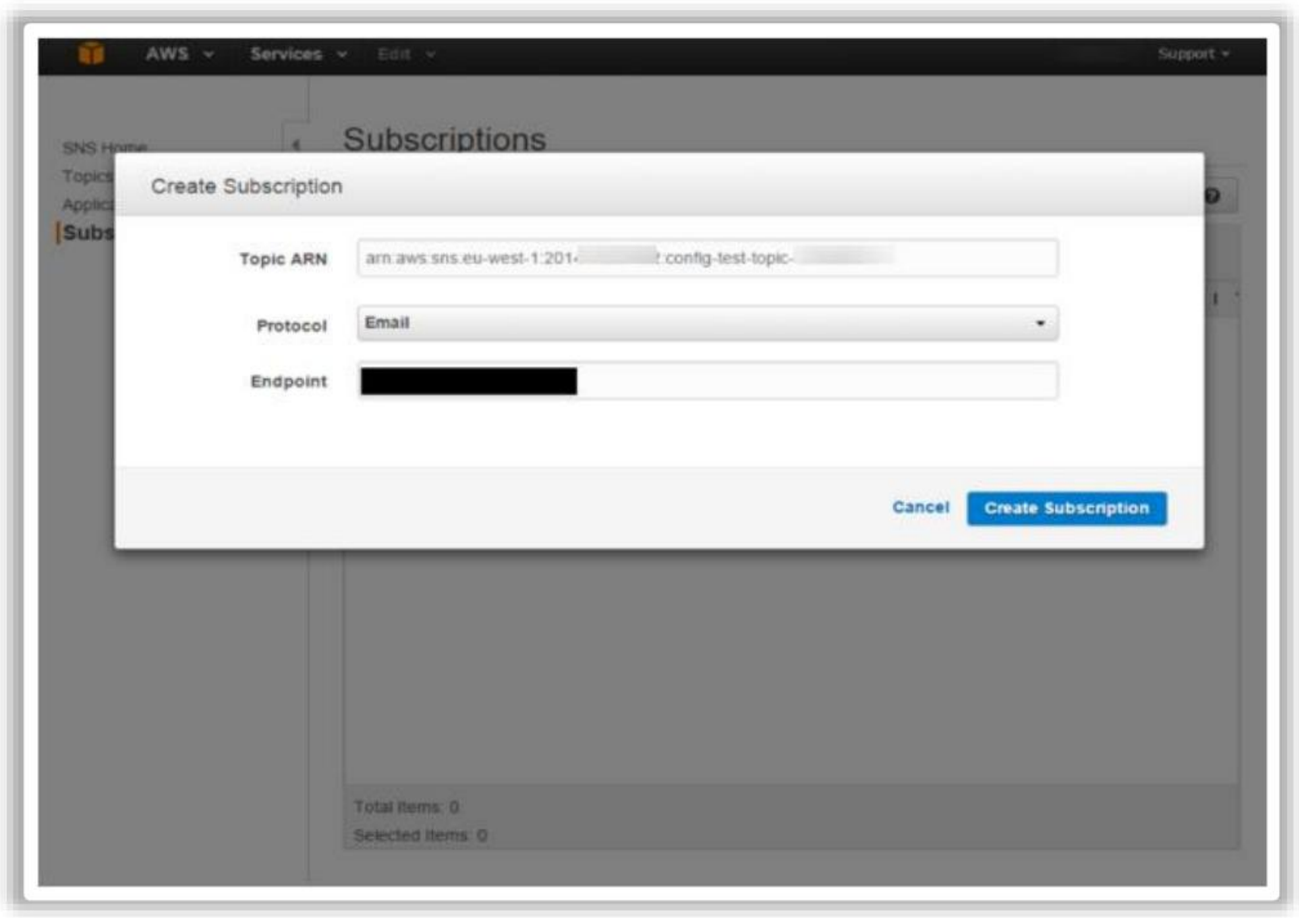


FIGURE 3.87:Create Subcription

- From the **Subscription** menu, click **Create Subscription.**
- After that, confirm the subscription from an email sent to the provided email address.

Step 5: Attach policy.

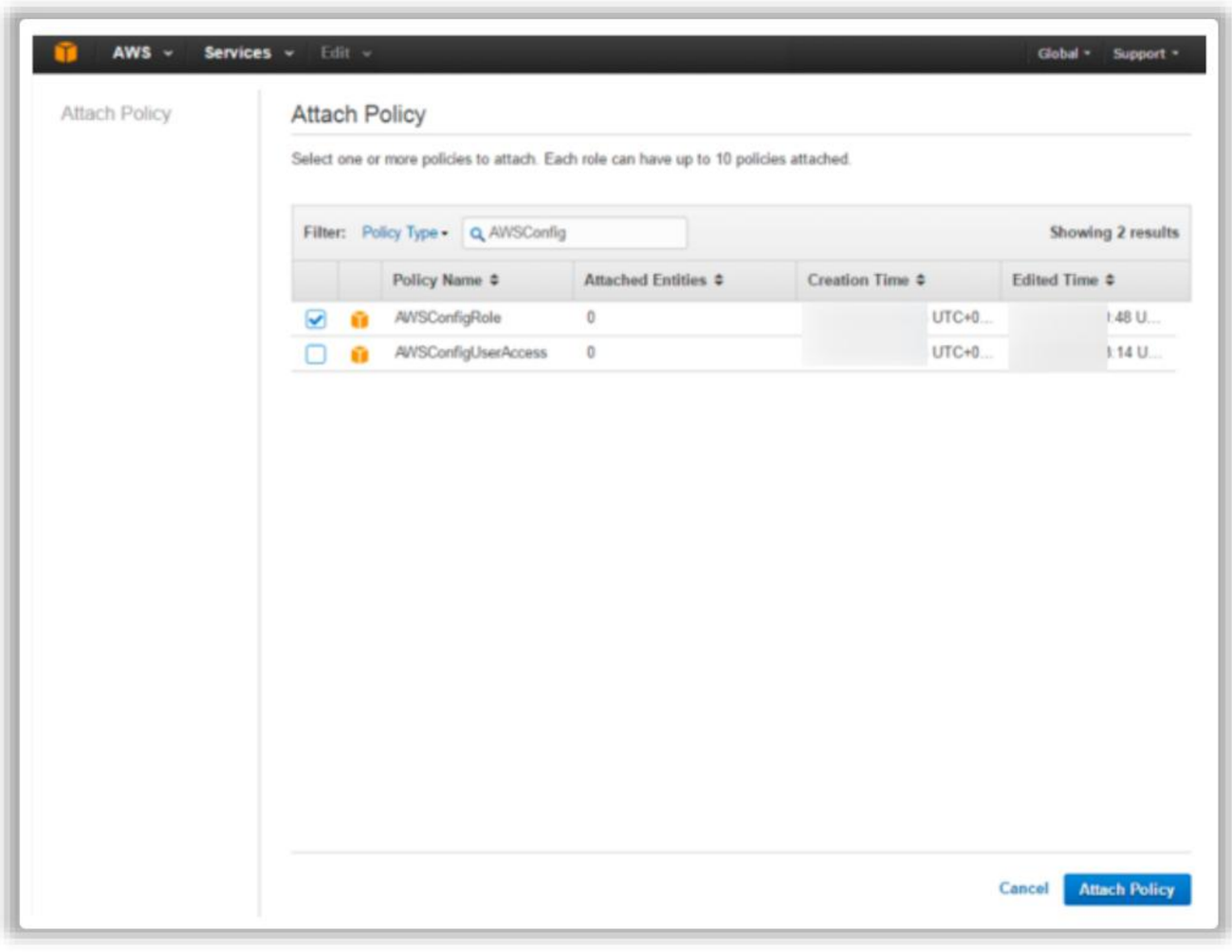


FIGURE 3.88: Attach Policy

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In the **AWS IAM service** page, select the created IAM role and click it.
- Click **Attach Policy** button and attach **AWS Config Role.**
- Add a user to the group, and the changes will be shown in **timeline** page.

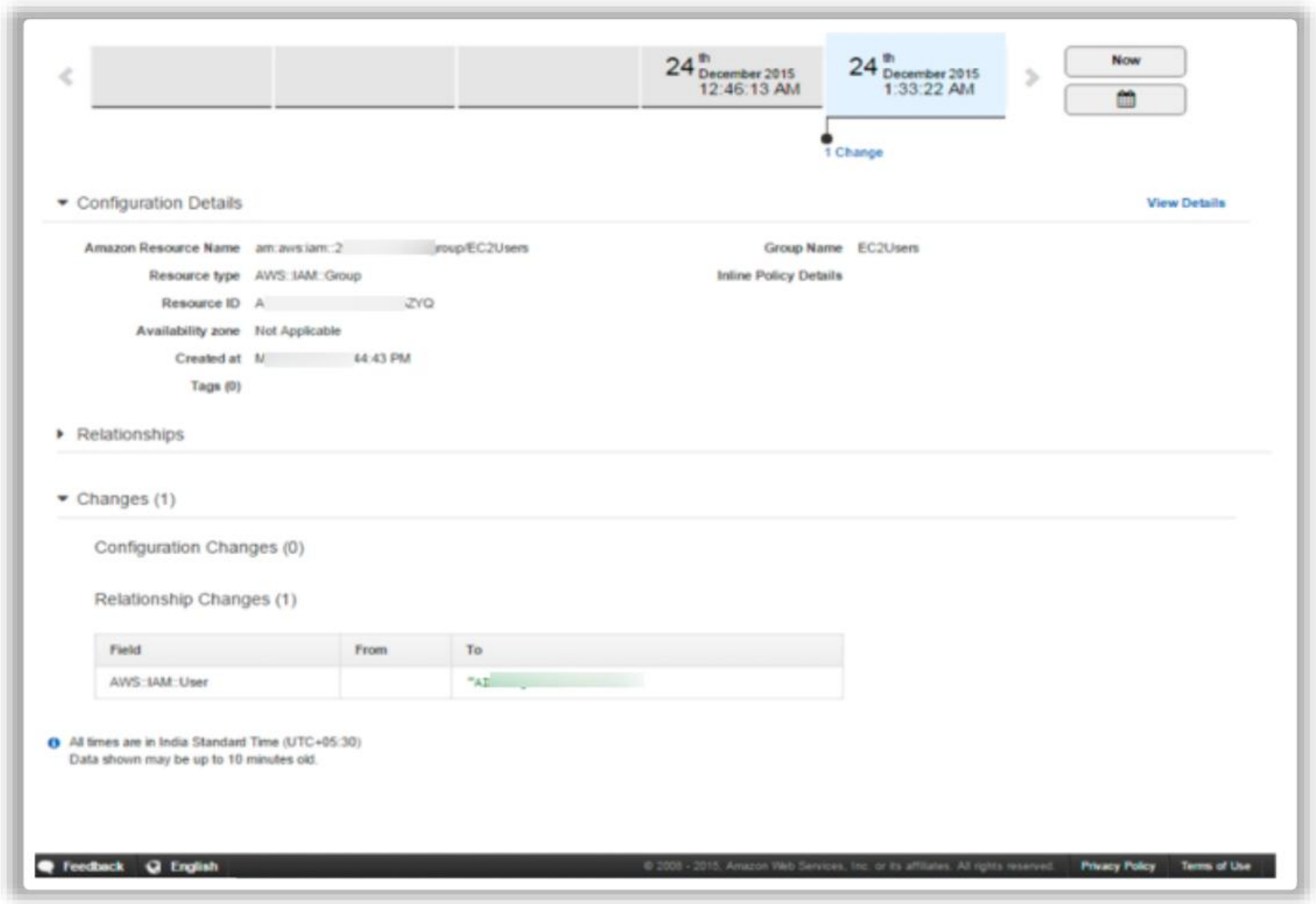


FIGURE 3.89:Timeline Page

hide01.ir

- Email message.

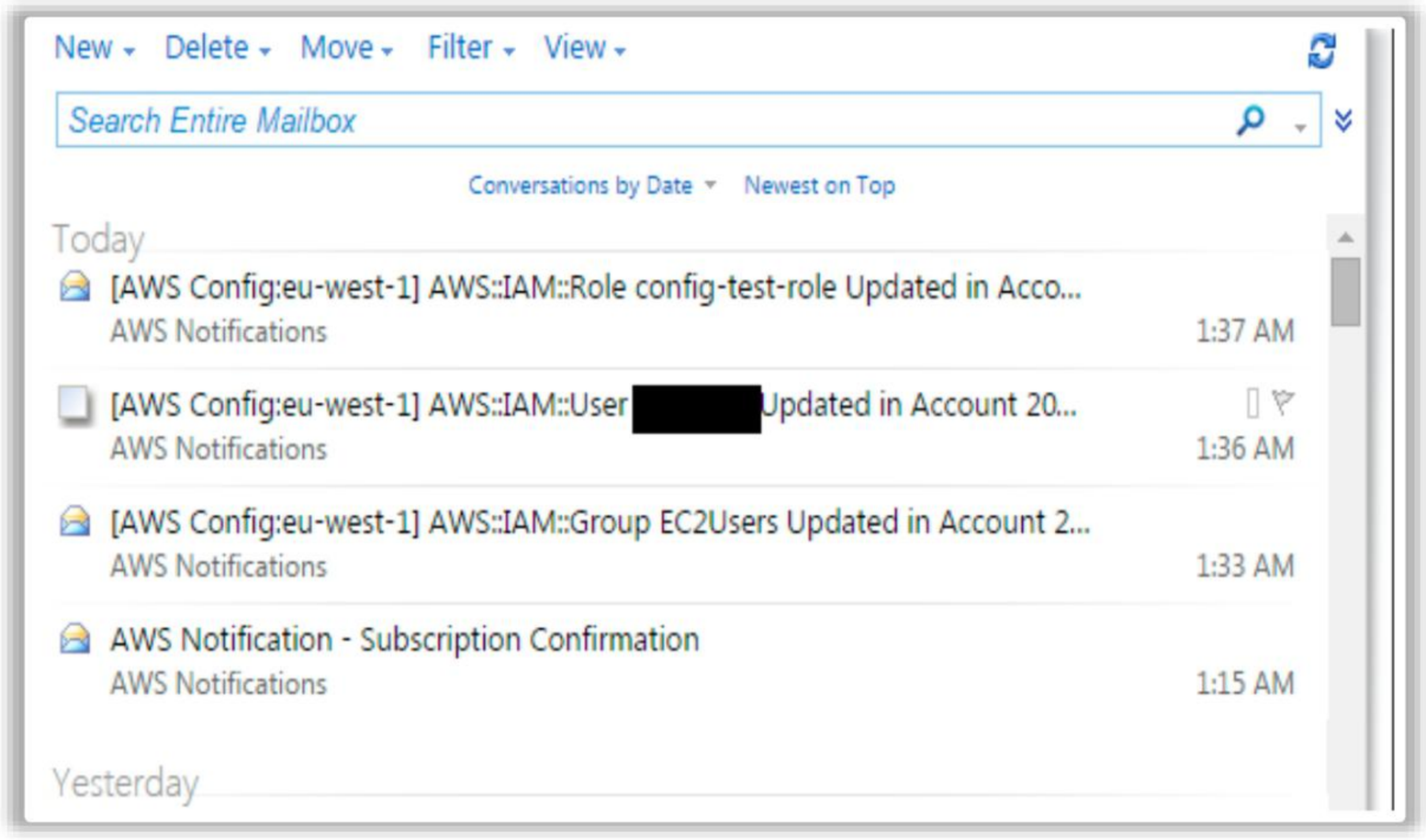
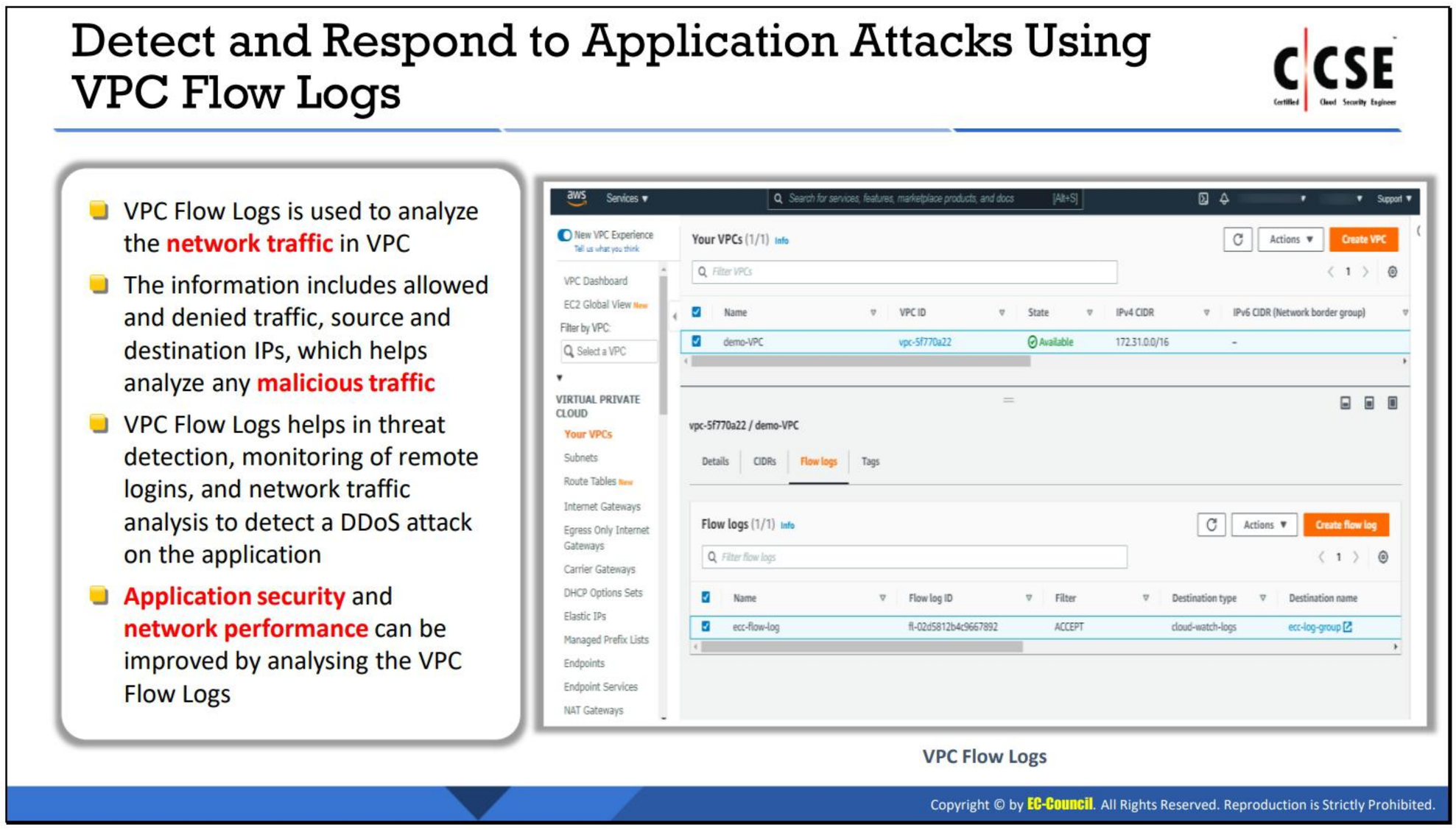


FIGURE 3.90: Email Message

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Detect and Respond to Application Attacks using VPC Flow Logs

VPC Flow Logs can capture information of the IP traffic that goes to and from the VPC network interfaces. Enabling VPC Flow Logs will enable logging network traffic to CloudWatch Logs for storage and analysis by applications. These logs contain important information. The information includes allowed and denied traffic as well as source and destination IPs, thereby analyzing all malicious traffic.

Alarms can be created for some specific traffic patterns. It can identify botnet activity, vulnerability scans against the network can be detected and blocked. VPC Flow Logs helps in detection of threats, monitoring of remote logins, DDoS attack detection. Application security and network performance can be improved by analyzing the VPC Flow Logs

Enabling VPC Flow Logs

- Enable VPC Flow Logs from the AWS Management Console or AWS Command Line Interface or making calls to EC 2 API.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click on **Create Flow Log** for the VPC.

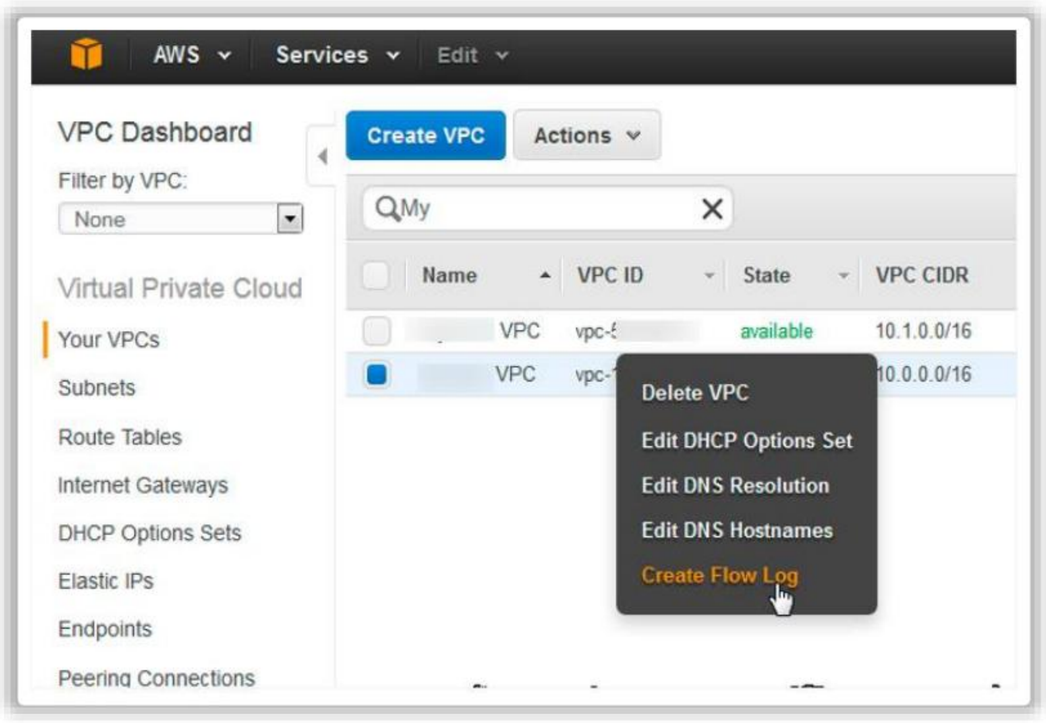


FIGURE 3.91: VPC Dashboard

- Click on **Create Flow Log** in **Create Flow Log** wizard.

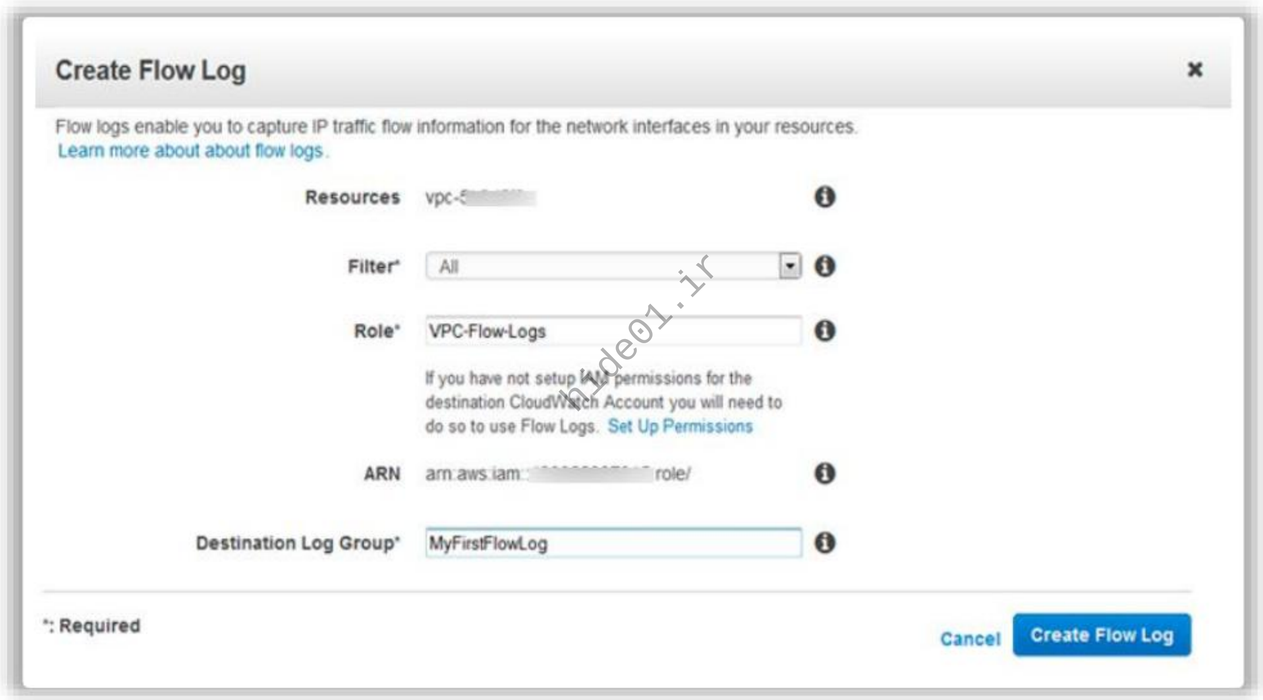


FIGURE 3.92:Create Flow Log

- New Flow Logs will appear in the **Flow Logs** Tab of the **VPC Dashboard**.

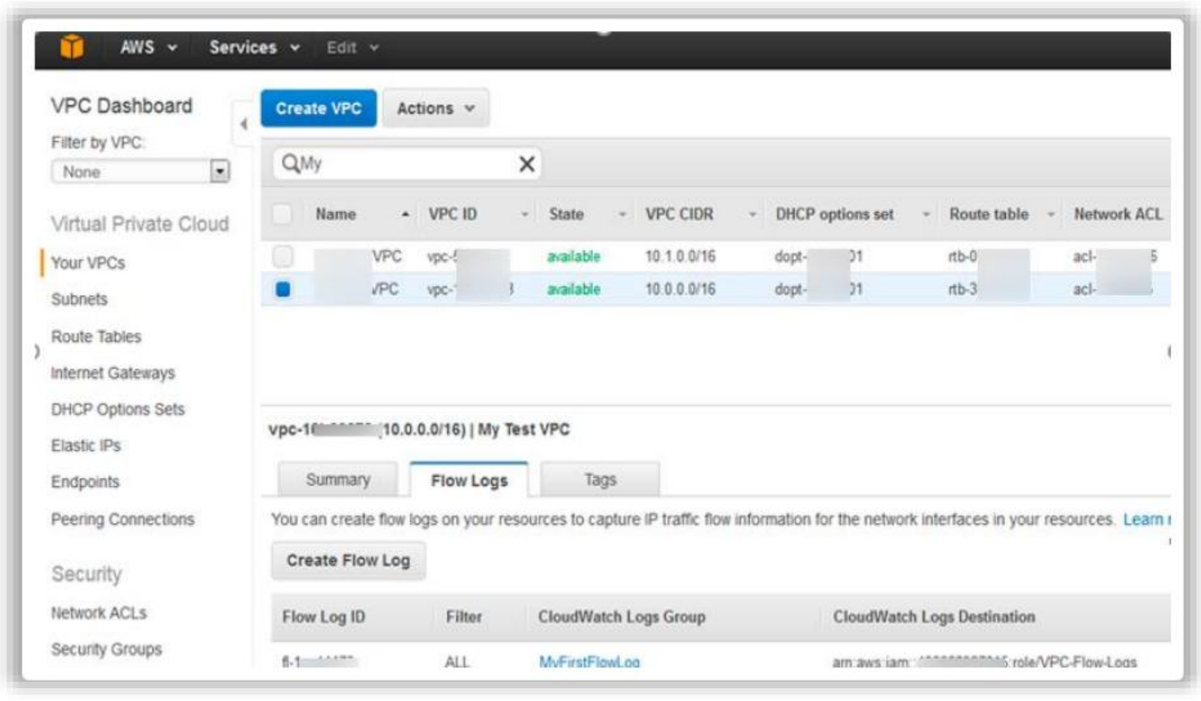


FIGURE 3.93: New Flow Log

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Flow Logs will be saved to log groups in CloudWatch Logs. Access them from **CloudWatch Logs** dashboard.

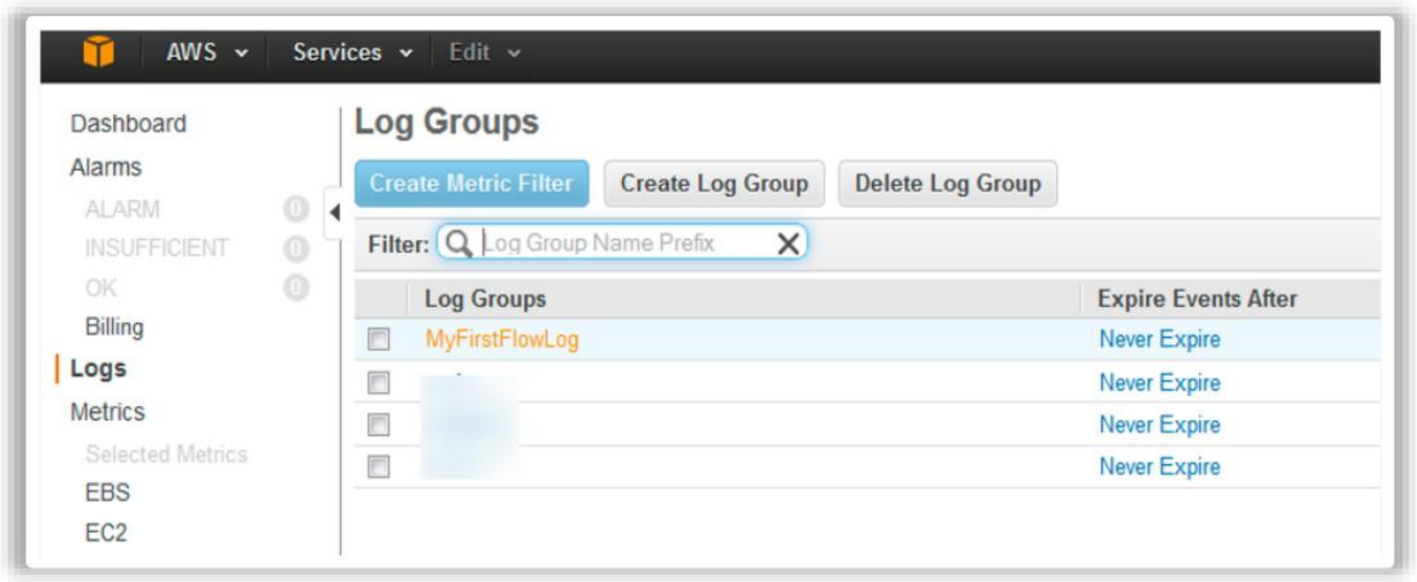


FIGURE 3.94: CloudWatch Logs

- Every Log Group consists of a separate stream for elastic network interface (ENI).

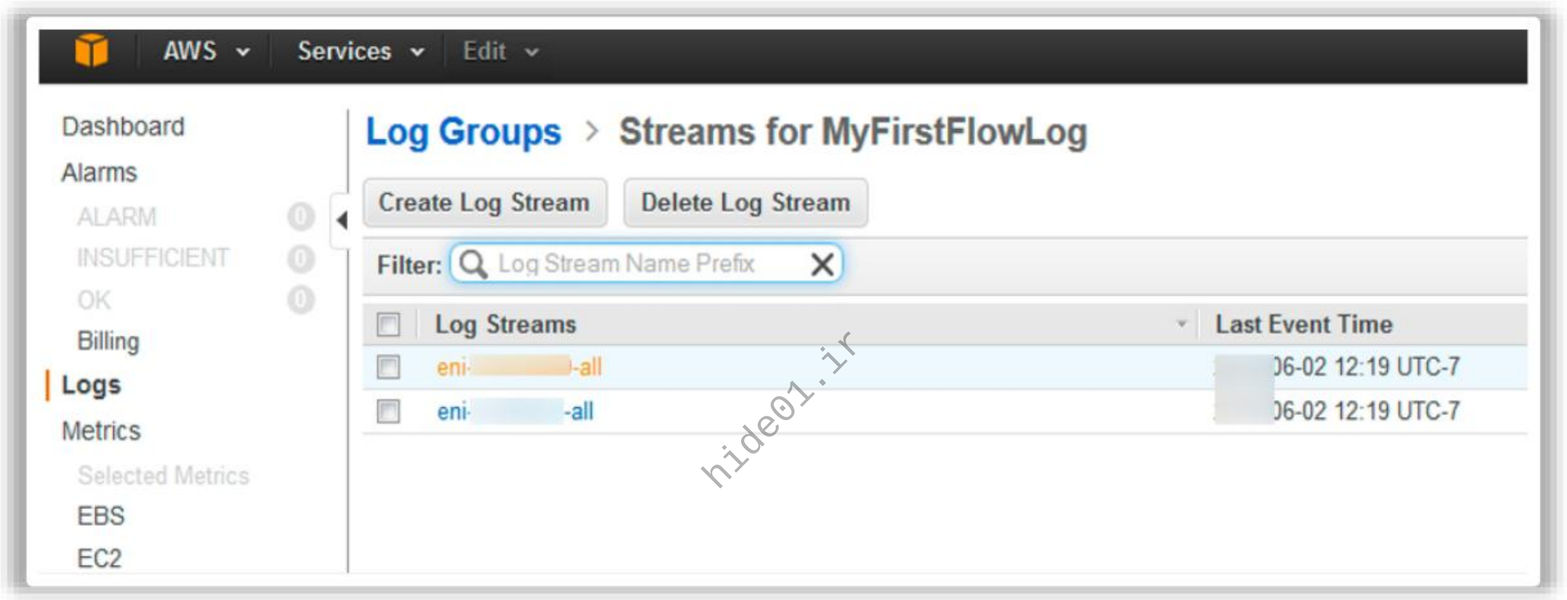


FIGURE 3.95: Log Group

- Every stream consists of a series of Flow Log Records.

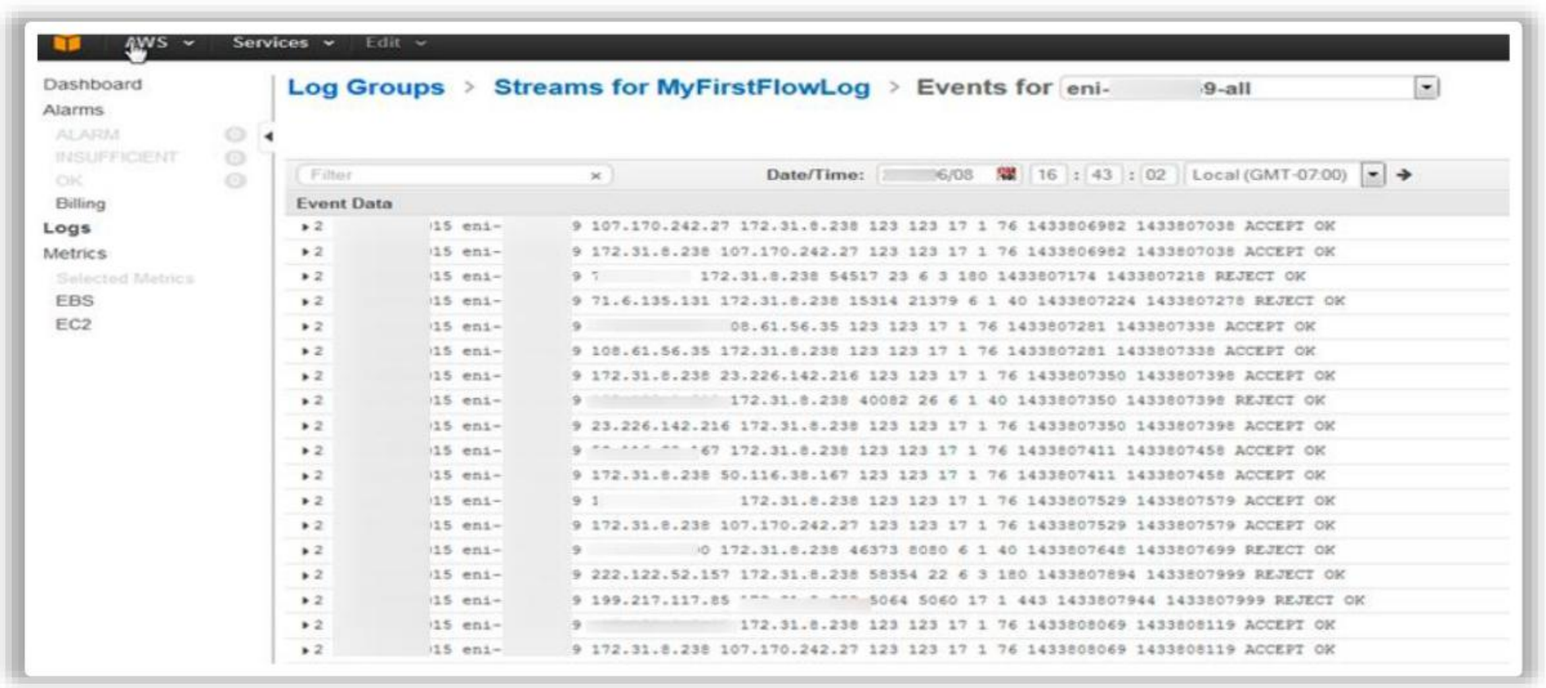
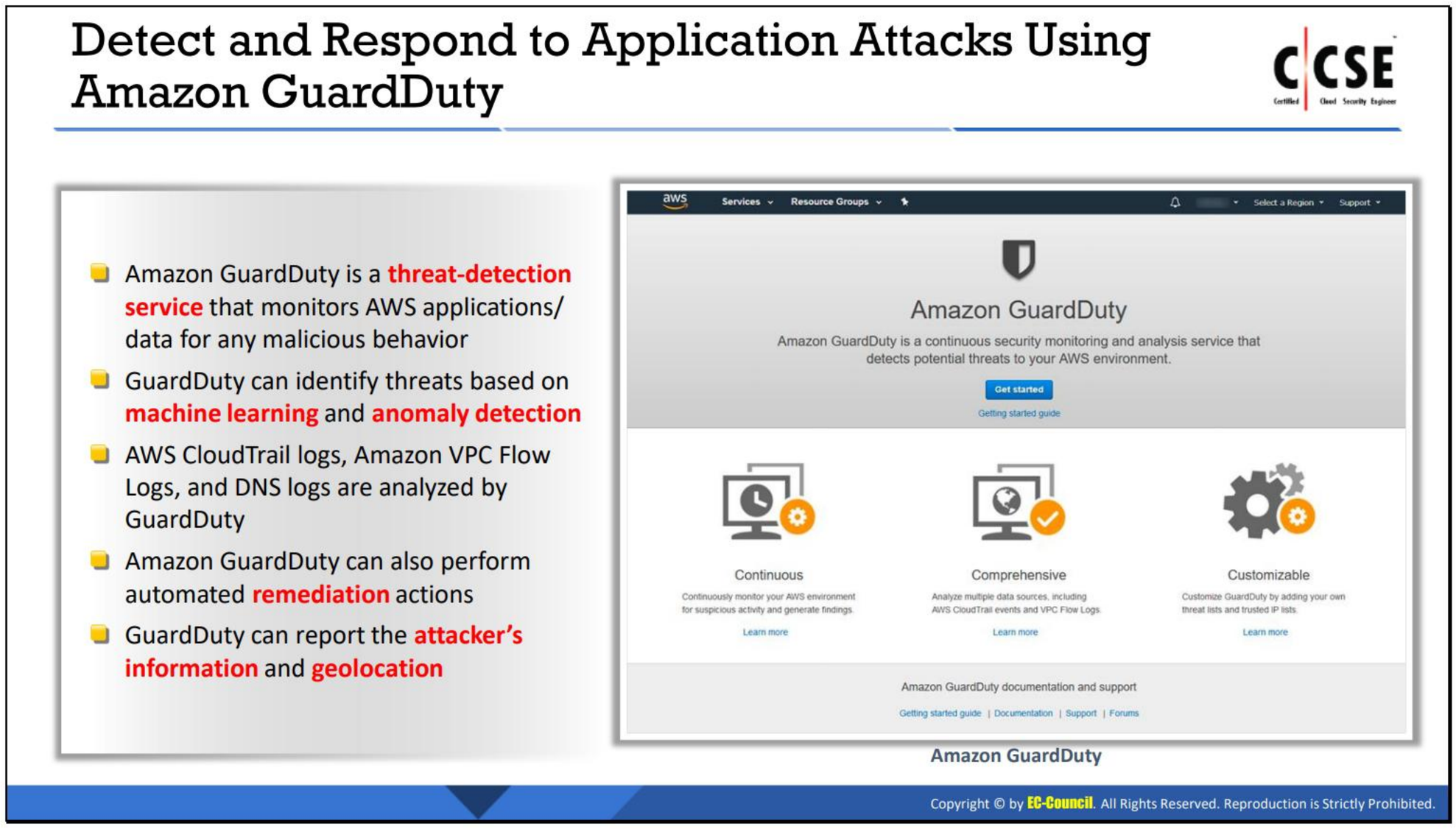


FIGURE 3.96: Flow Log Records

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Detect and Respond to Application Attacks Using Amazon GuardDuty

Amazon GuardDuty is a threat detection service that is responsible for monitoring applications for any malicious and unauthorized activities continuously. To identify threats, Amazon GuardDuty uses machine learning, anomaly detection, and advanced threat intelligence. GuardDuty can analyze events from AWS CloudTrail, VPC Flow Logs, and DNS logs. Amazon GuardDuty can be integrated with Amazon CloudWatch Events and AWS Lambda and performs automated mitigation of threats. GuardDuty's findings include attacker's information such as IP address and location.

How Amazon GuardDuty Works

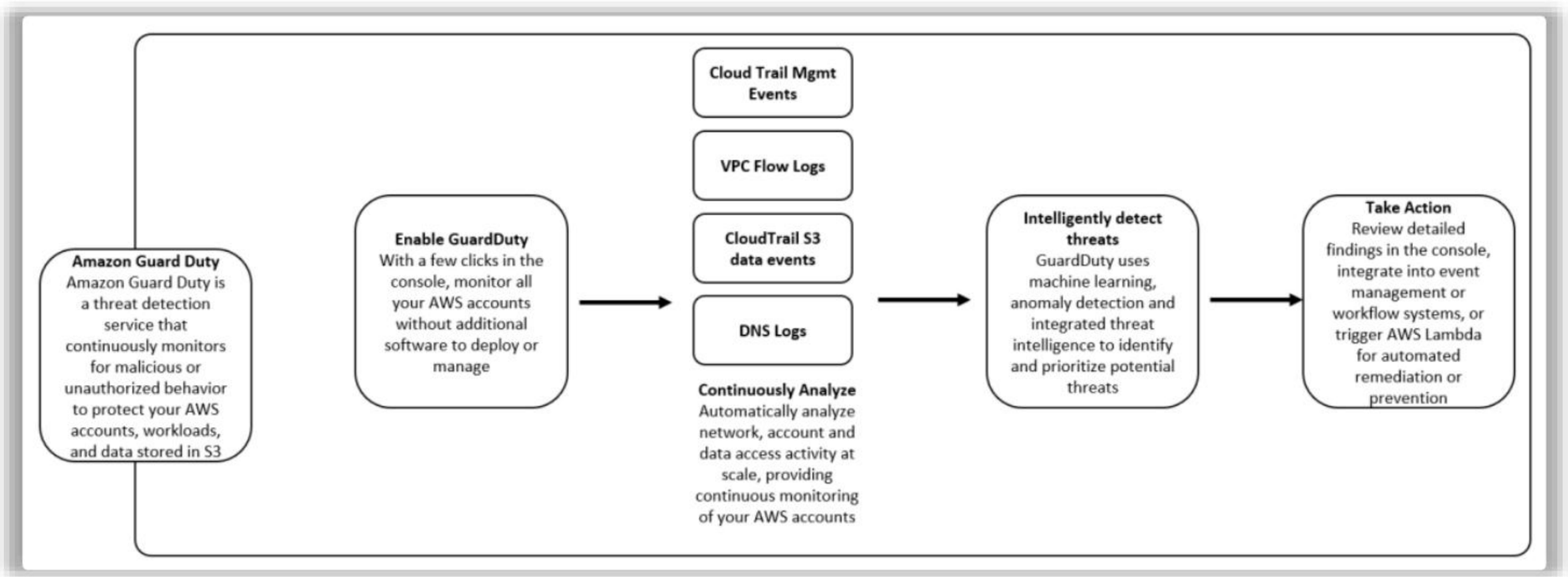


Figure 3.97: Working of Amazon GuardDuty

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Enabling Amazon GuardDuty

- Go to GuardDuty Console and click on **Get Started.**



FIGURE 3.98: GuardDuty Console

- On the next screen, click **Enable GuardDuty.**

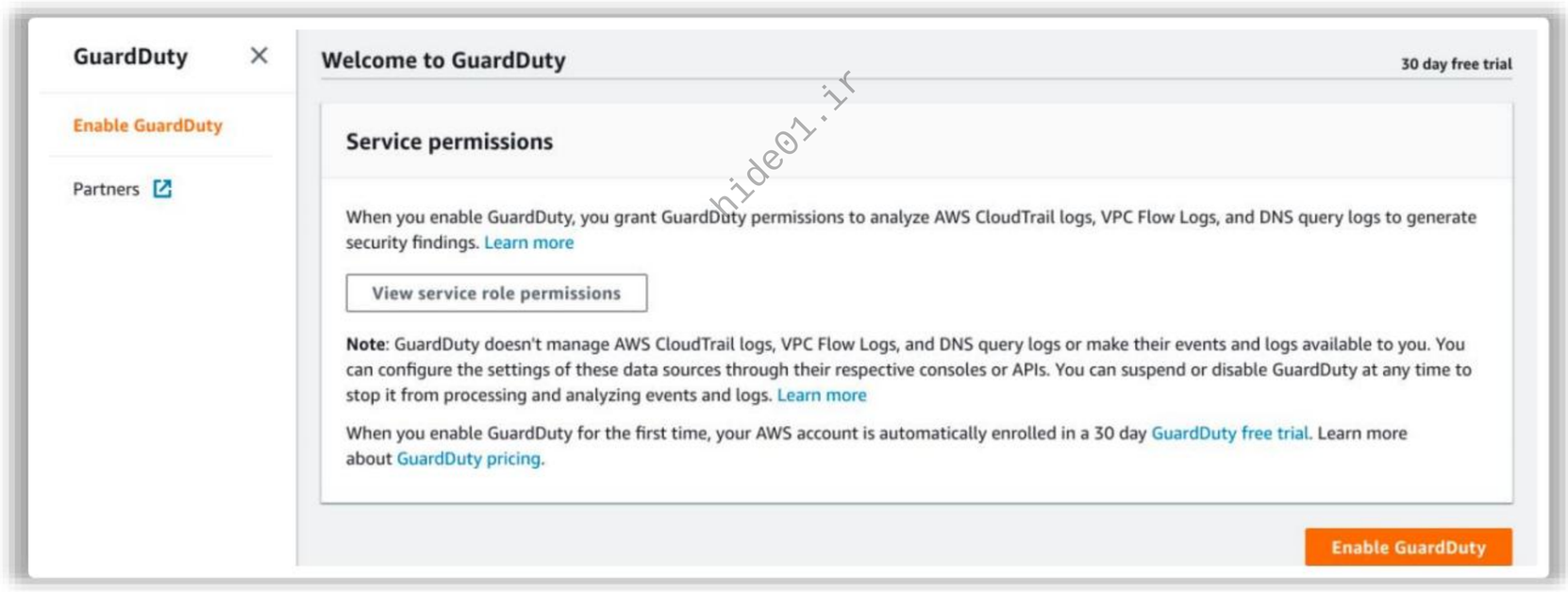


FIGURE 3.99:Enable GuardDuty

- Click **deploy to AWS** to launch the CloudFormation Stack.
- Click **Next** on the **Specify Template** page.
- On the **Specify Stack details** page under **Parameters,** enter the email address to receive notifications.
- Click **Next** on the **Configure Stack options** page.
- Under **Capabilities,** acknowledge that the template will create IAM roles and click on **Create Stack.**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

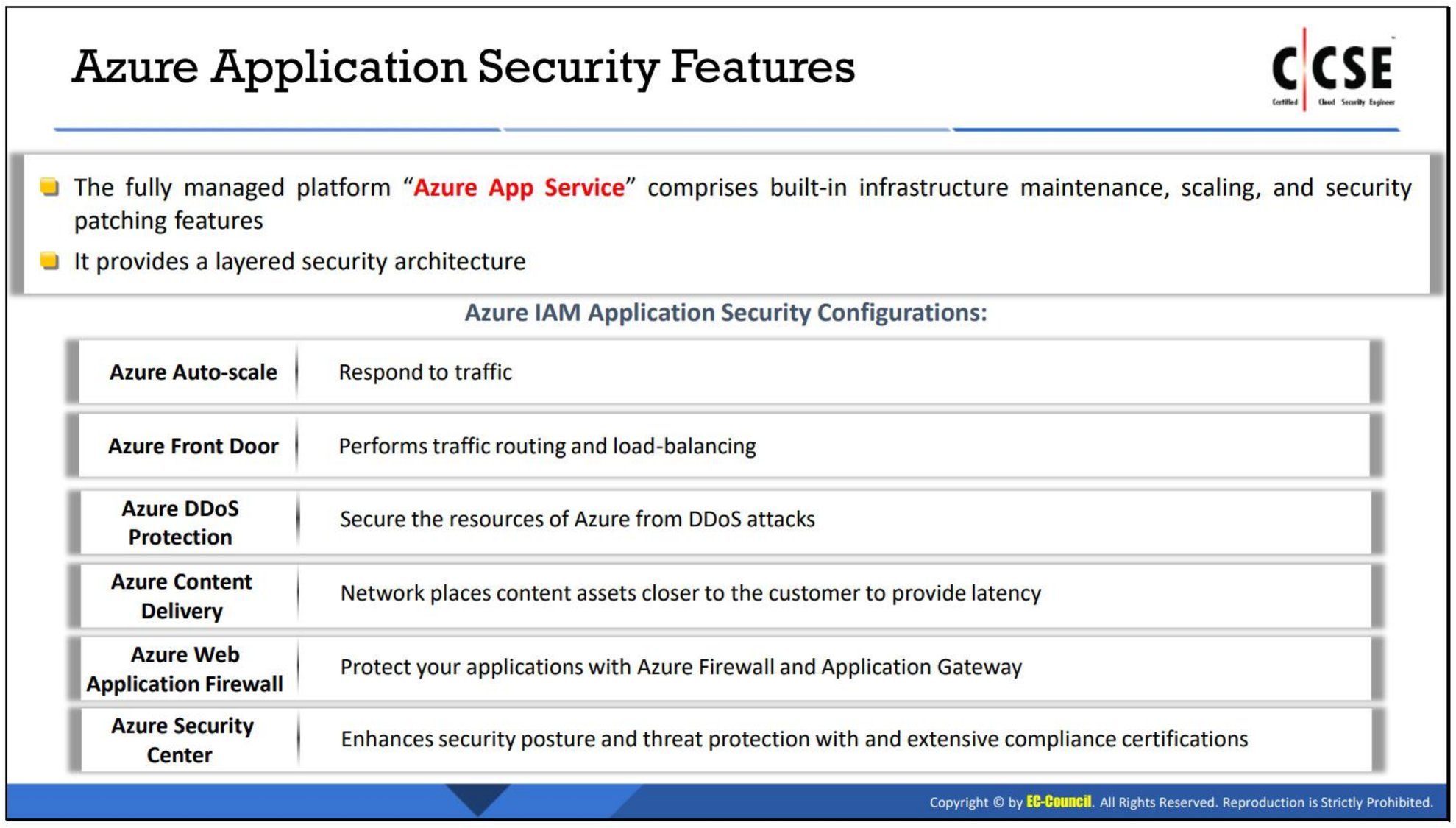


LO#08: Understand Appication Security Features in Azure

Understanding the various tools and services provided by Azure to protect the applications and services is very important. This section explains the various application security features in Azure and best practices for application security in Azure.

hi@01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



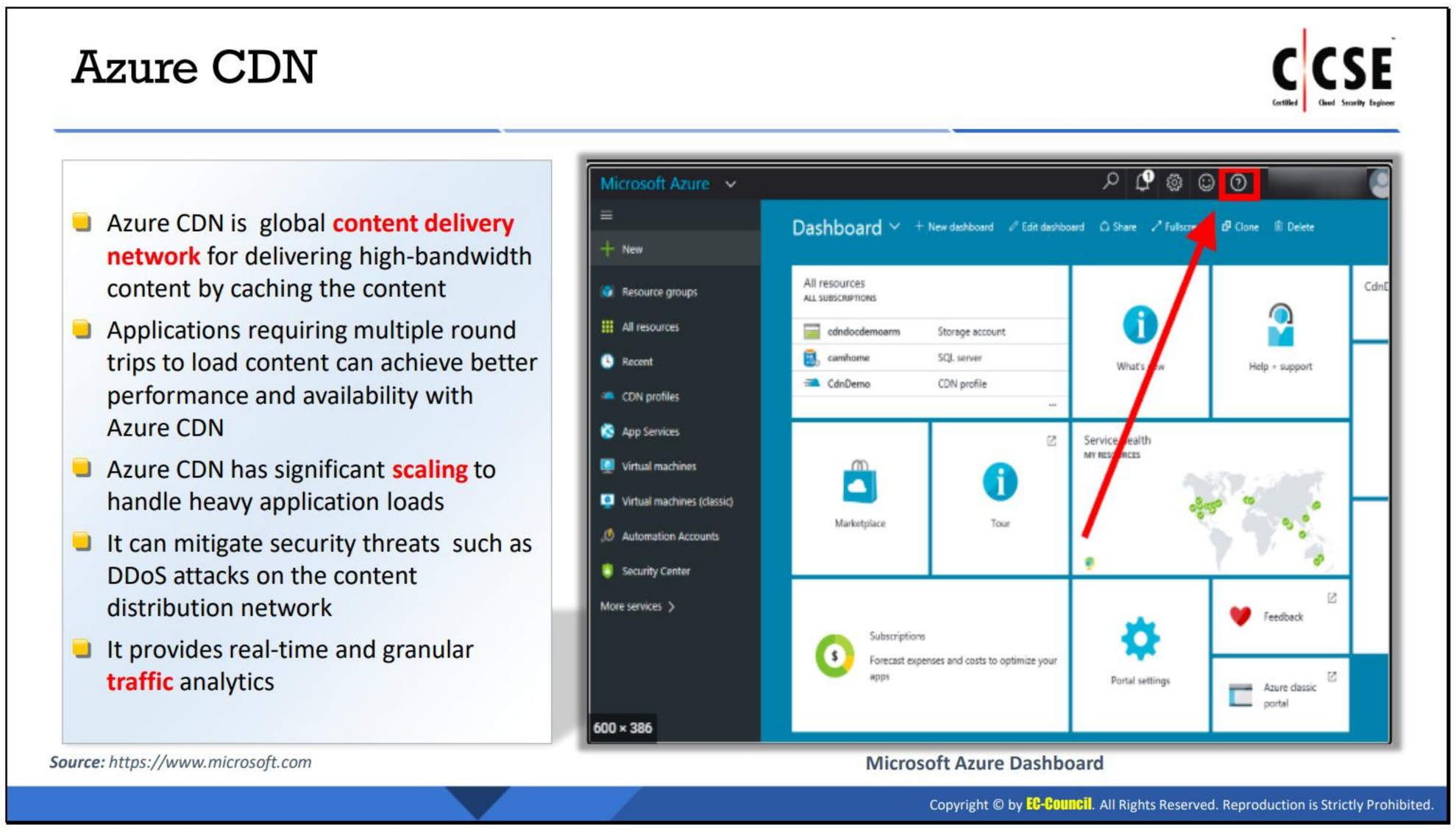
Azure Application Security Features

Azure App Service is a fully managed platform that provides infrastructure maintenance, security patching, and scaling. It provides a layered security architecture. Administrators can use the built-in features provided by the Azure Platform to manage the security of applications. Organizations can use these configurable security options and their capabilities to customize the security of applications and meet the requirements of the organization's deployments. The Azure application service provides a layered security architecture.

The Azure application security capabilities/features that can help the organizations to fulfill their requirements are as follows:

- **Azure Auto-scale:** Respond to traffic
- **Azure Front Door:** Performs traffic routing and load balancing
- **Azure DDoS Protection:** Protect Azure resources from DDoS attacks
- **Azure Content Delivery:** Network places content assets closer to the customer to provide latency
- **Azure Web Application Firewall:** Protect your applications with Azure Firewall and Application Gateway
- **Azure Security Center:** Enhances security posture and threat protection with and extensive compliance certifications

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Azure CDN

Azure Content Delivery Networks (CDN) is a network server located at various points of presence (POP) locations to facilitate efficient content delivery to users. They store cached content on edge servers in POP locations that are close to end-users to reduce latency. CDNs shorten the physical distance between the users and content on origin servers by storing the cached content, which can be provided to users with minimal latency upon their requests.

Azure CDN is a global solution that caches content at physical nodes that are placed strategically across the world to deliver high-bandwidth content to users. Use Azure CDN to accelerate dynamic content because it accelerates content that cannot be cached (dynamic content) by employing various network optimizations. Use Azure CDN to secure applications hosted on Azure, protect websites/applications from DDoS attacks, reduce bandwidth consumption, manage high traffic loads, increase page-load speed, etc.

Azure CDN offers the following benefits:

- Better performance and enhanced user experience, especially for end-users that use applications that need multiple round-trips to load content.
- Large scaling to manage high instantaneous loads in a better way.
- Directs minimal traffic to the origin server by distributing user requests and providing content to users directly via edge servers.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

How Azure CDN Works

Working of Azure CDN is illustrated in the below image and explained later:

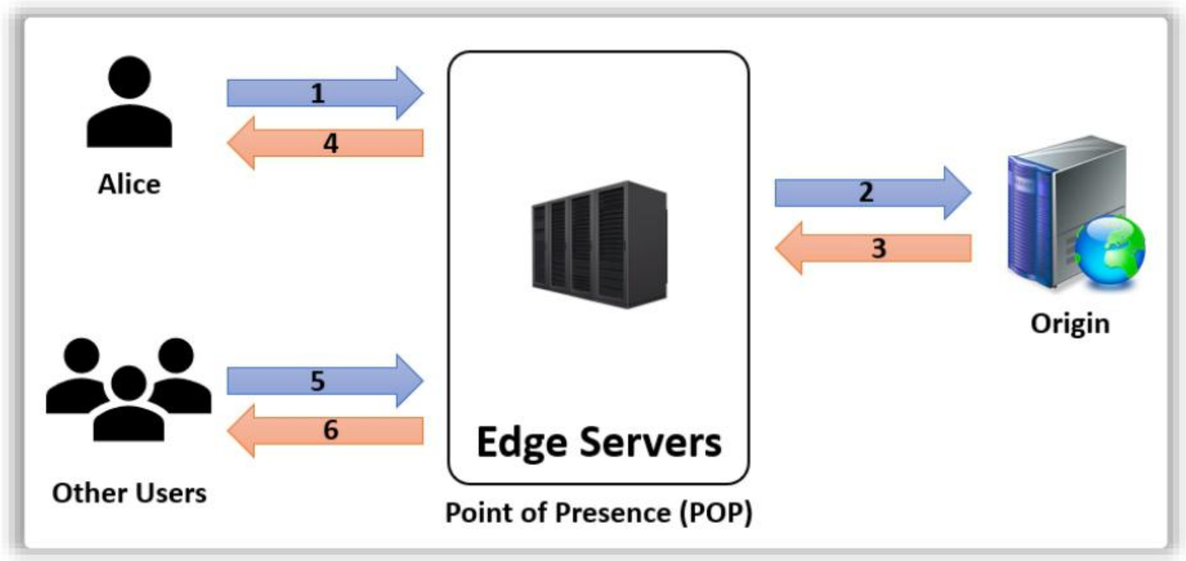


Figure 3.100: Working of Azure CDN

- When a file is requested by a user (Alice) via a URL having a special domain name, the request is routed to the best performing POP location that is geographically closest to the user by DNS.
- If the POP does not have the file available in any of its servers, it requests the origin server to provide the file. The origin server may be an Azure storage account, Azure cloud service, Azure web app, or any other web server.
- The origin server provides the file to an edge server present on the POP.
- The edge server then caches the files and sends them to the user (Alice). Until the time-to-live (TTL) defined in its HTTP header expires, the file is kept cached on the edge server. The default TTL time is 7 days if the origin server does not specify a TTL time.
- Other users can request the same file via the same URL used by Alice. The users will be directed to the same POP.
- The edge server provides the file from the cache directly if the TTL of the file has not expired. This entire process provides a faster and more responsive user experience.

At least one Azure subscription and one CDN profile are needed to use Azure CDN. A CDN profile refers to a set of endpoints having configurations of content access and delivery. Based on the CDN profile, Azure pricing is set.

Source: https://www.microsoft.com

Features of Azure CDN

Azure CDN offers the following important security features to secure the delivery of applications:

- Geo-filtering
- HTTPS custom domain support
- Azure diagnostics logs
- CDN caching rules

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Steps to Use the Azure CDN Features to Secure Content Delivery

Use the following Azure CDN features to deliver content securely.

- **Restrict Azure CDN content by locations (Geo-filtering):** Azure CDN usually delivers content to all users who request content across all locations (regions/countries). Use the geo-filtering feature of the CDN to restrict access to content by regions/countries. The geo-filtering feature allows creating rules on particular paths on a CDN endpoint. Additionally, it allows setting rules to block or allow content in selected regions/countries.

  Restrict CDN content by locations for Azure CDN Standard from Akamai/Verizon profiles and Azure CDN Premium profile from Verizon using the below-given procedure.

1. **Azure CDN Standard from Akamai/Verizon profiles**
   - **Define the directory path:**
     - Choose a CDN endpoint inside the portal. Under **SETTINGS**, choose **Geo-filtering**.

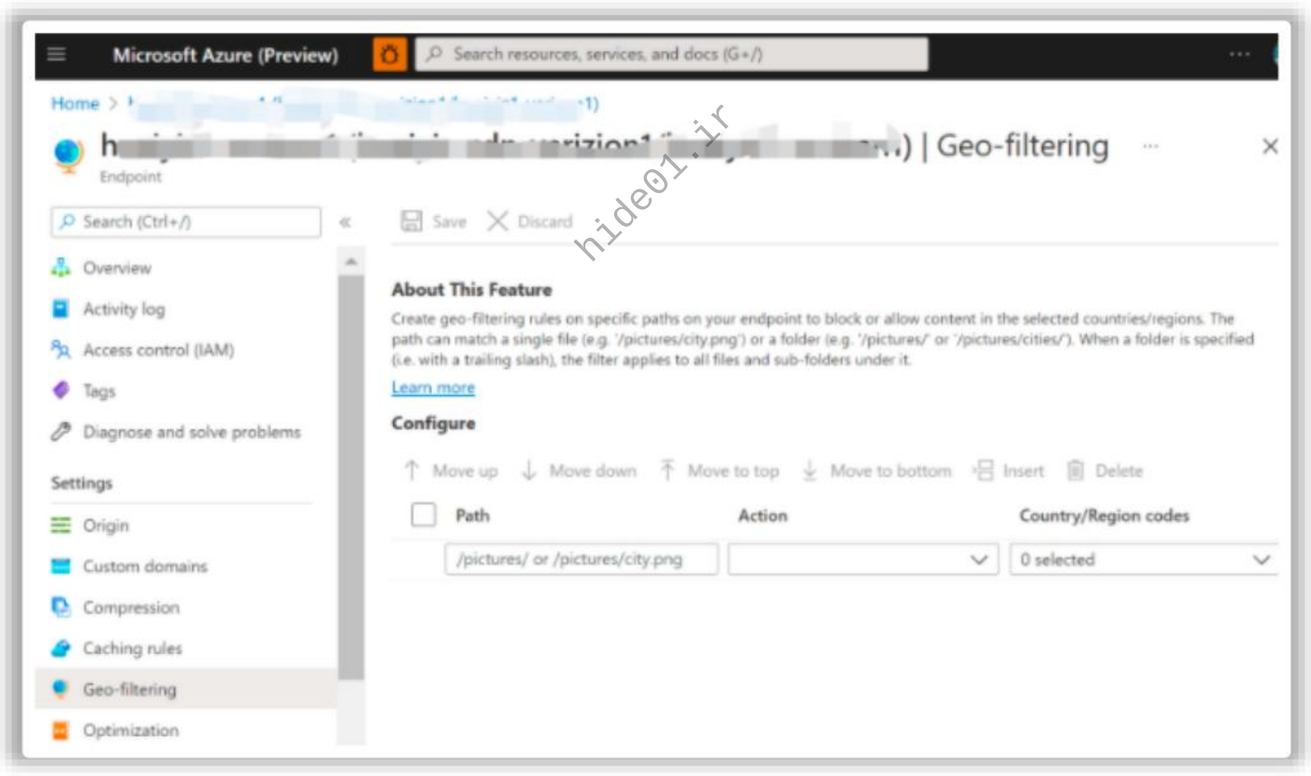


FIGURE 3.101: Selecting Geo-filtering

- In the **PATH** box, define the path to the location to which the access is denied or allowed for users. Geo-filtering can be applied for all files either with a forward slash (/) or by selecting particular folders by specifying directory paths (e.g., **/pictures/**).
- Define the action type by choosing **Block** or **Allow** from the **ACTION** list. If you choose Allow, users from the specified locations (regions/countries) can only access the assets requested from that path. If you choose Block, users from the specified locations are denied access to assets requested from that path.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Define the regions/countries by choosing them from the **COUNTRY CODES** list that must be allowed or blocked for the path. Click on **Save** after selecting the locations.

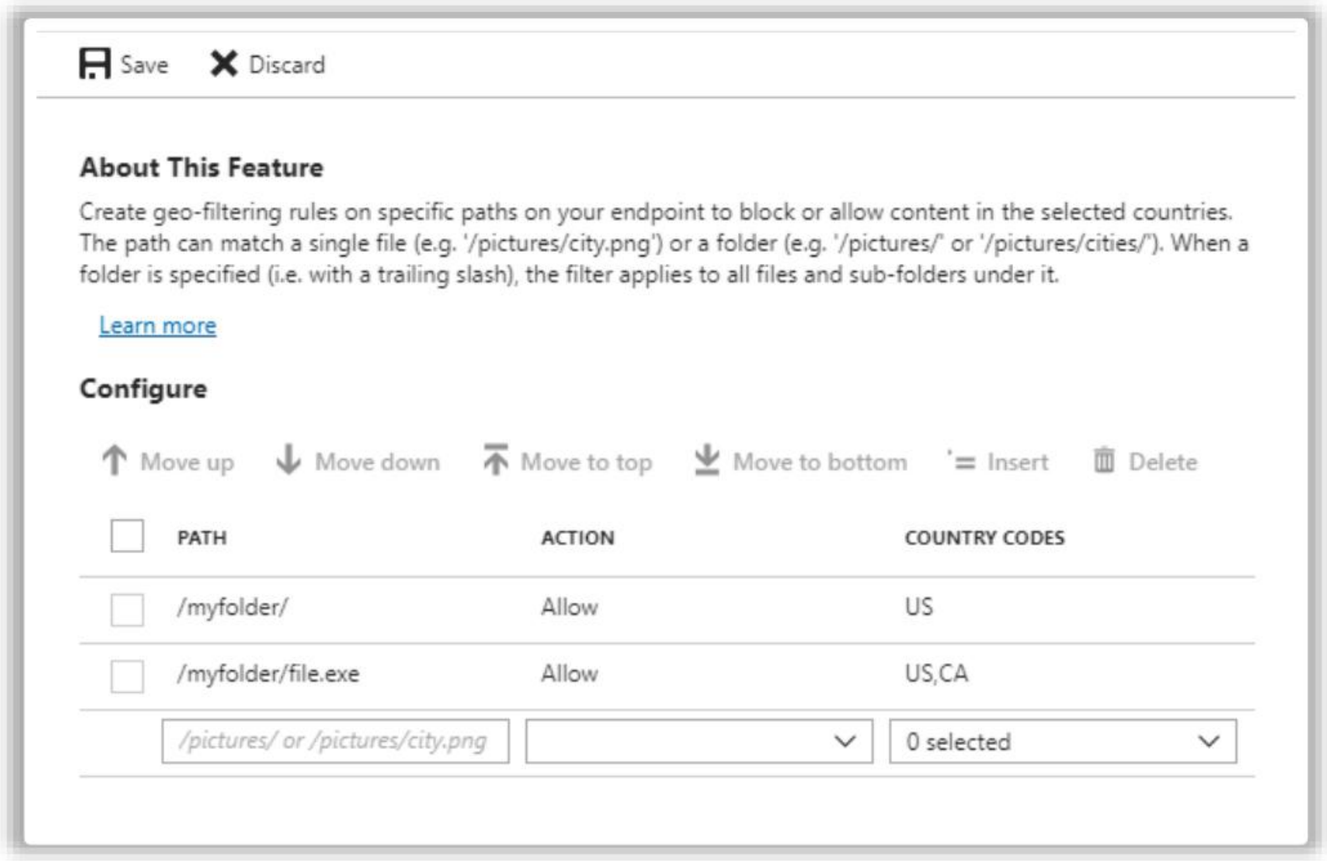


FIGURE 3.102: Choosing Country Codes

2. **Azure CDN premium from Verizon**
   - Choose **Manage** from the menu in the Azure CDN profile.
   - Choose **HTTP Large** from the Verizon portal and then click on **Country Filtering**.

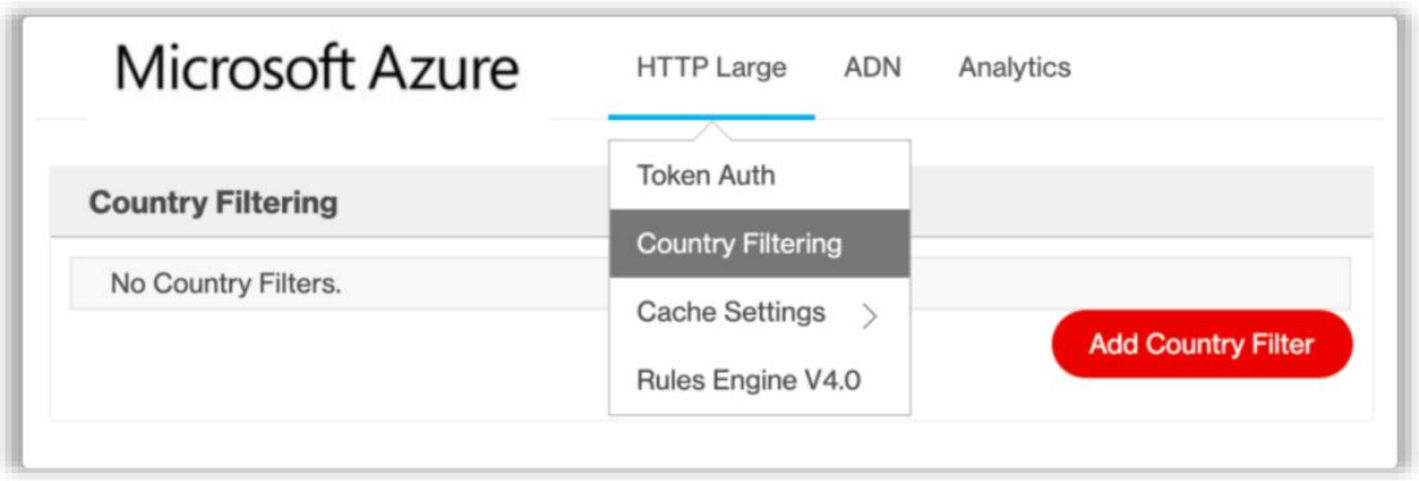


FIGURE 3.103: Choose Country Filtering

   - Choose **Add Country Filter.**
   - Enter the directory path in the first step. Choose **Add** or **Block** and then click on **Next**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Choose one or more countries/regions in the second step. To activate the rule, choose **Finish**. The new rule can be seen on the **Country Filtering** page in a table.

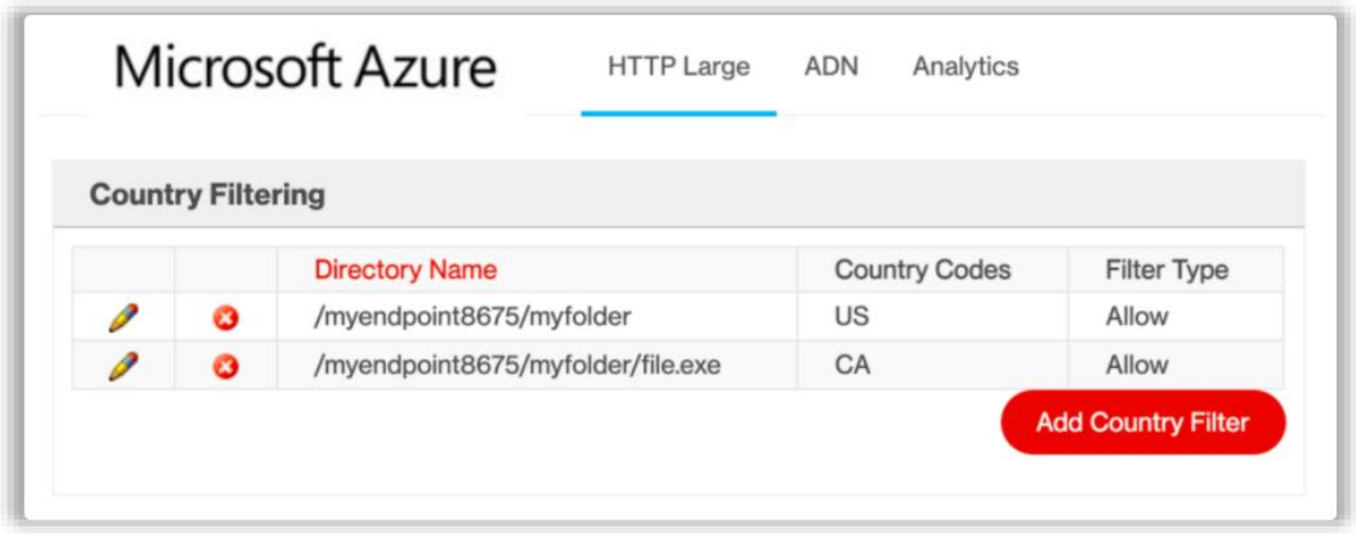


FIGURE 3.104: Country Filtering

- **Implement HTTPS on an Azure CDN custom domain:** Implement HTTPS on a custom domain associated to an Azure CDN endpoint to ensure sensitive data is securely delivered via TLS/SSL. A website's certificate is validated by a browser when the browser is connected through HTTPS. This process of validating the certificate if a legitimate certificate authority issues it ensures security by protecting cloud applications from attacks.

  Azure CDN automatically enables HTTPS by default on a CDN endpoint hostname. HTTPS is enabled automatically when a CDN endpoint is created. Create a CDN profile and a CDN endpoint and then associate a custom domain to that CDN endpoint.

  - **Enable TLS/SSL**

    Steps to enable HTTPS on the CDN custom domain by choosing the TLS/SSL certificate managed by Azure CDN.

    - Log in to the Azure portal and search for **CDN profiles** and select it.
    - Select your profile.
    - Choose the endpoint that has your custom domain from the list of CDN endpoints. The **Endpoint** page will open.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

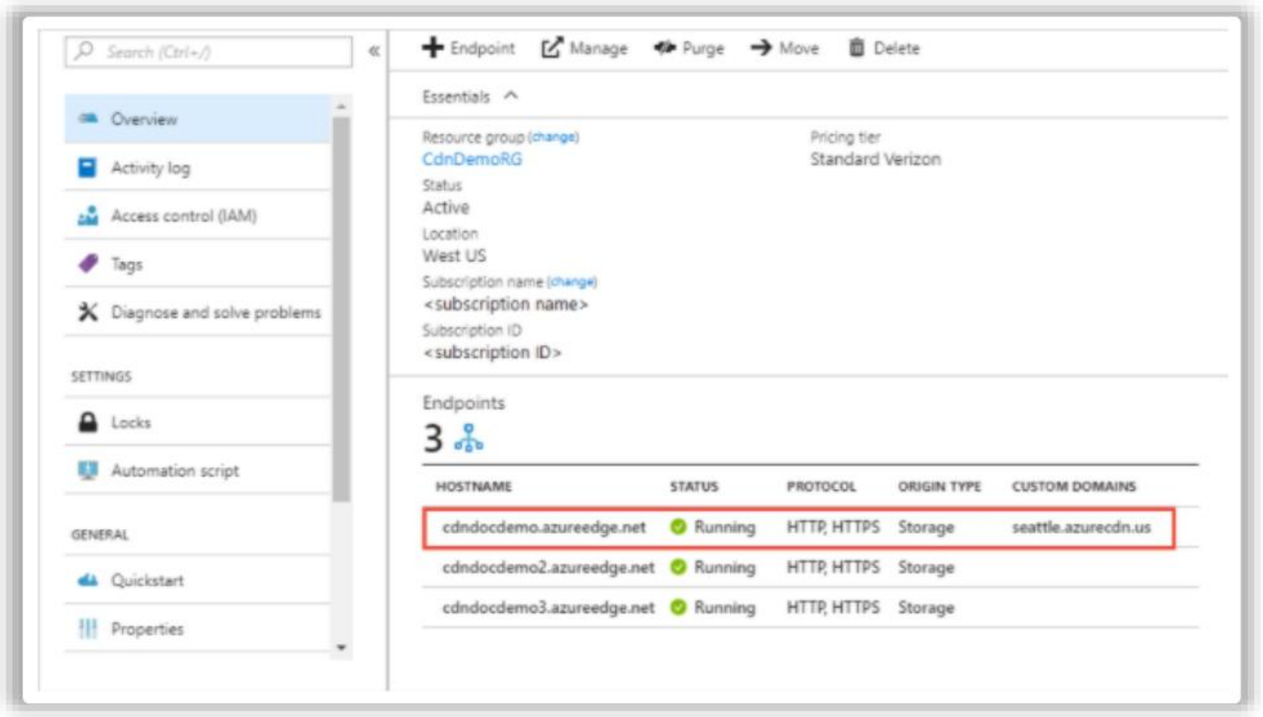


FIGURE 3.105: List of CDN Endpoint

- Choose the custom domain for which HTTPS needs to be enabled from the list of custom domains. The **Custom domain** page will open.

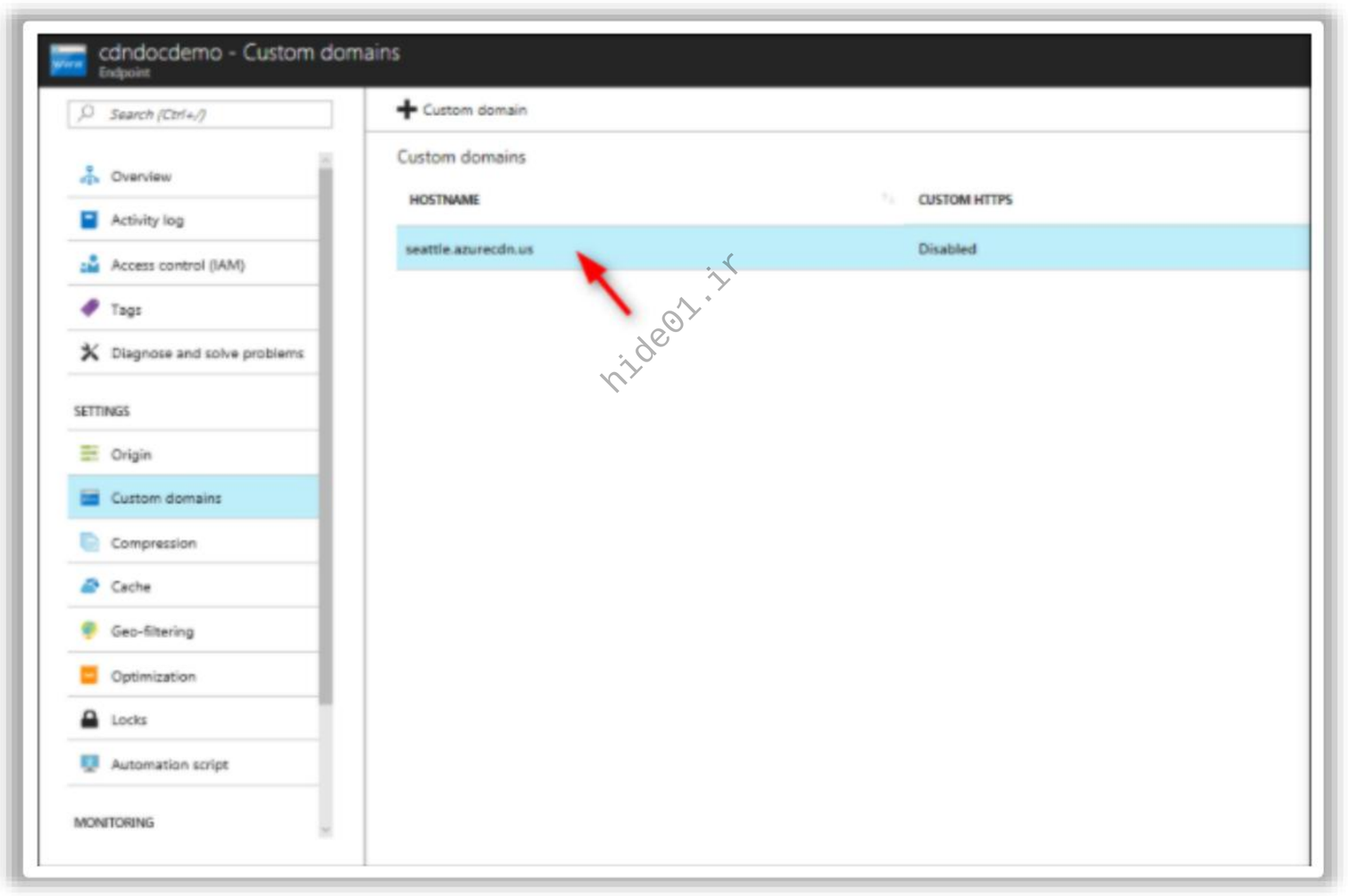


FIGURE 3.106: Custom Domain Page

- Choose **CDN managed** under **Certificate management type**.
- To enable HTTPS, select **On**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

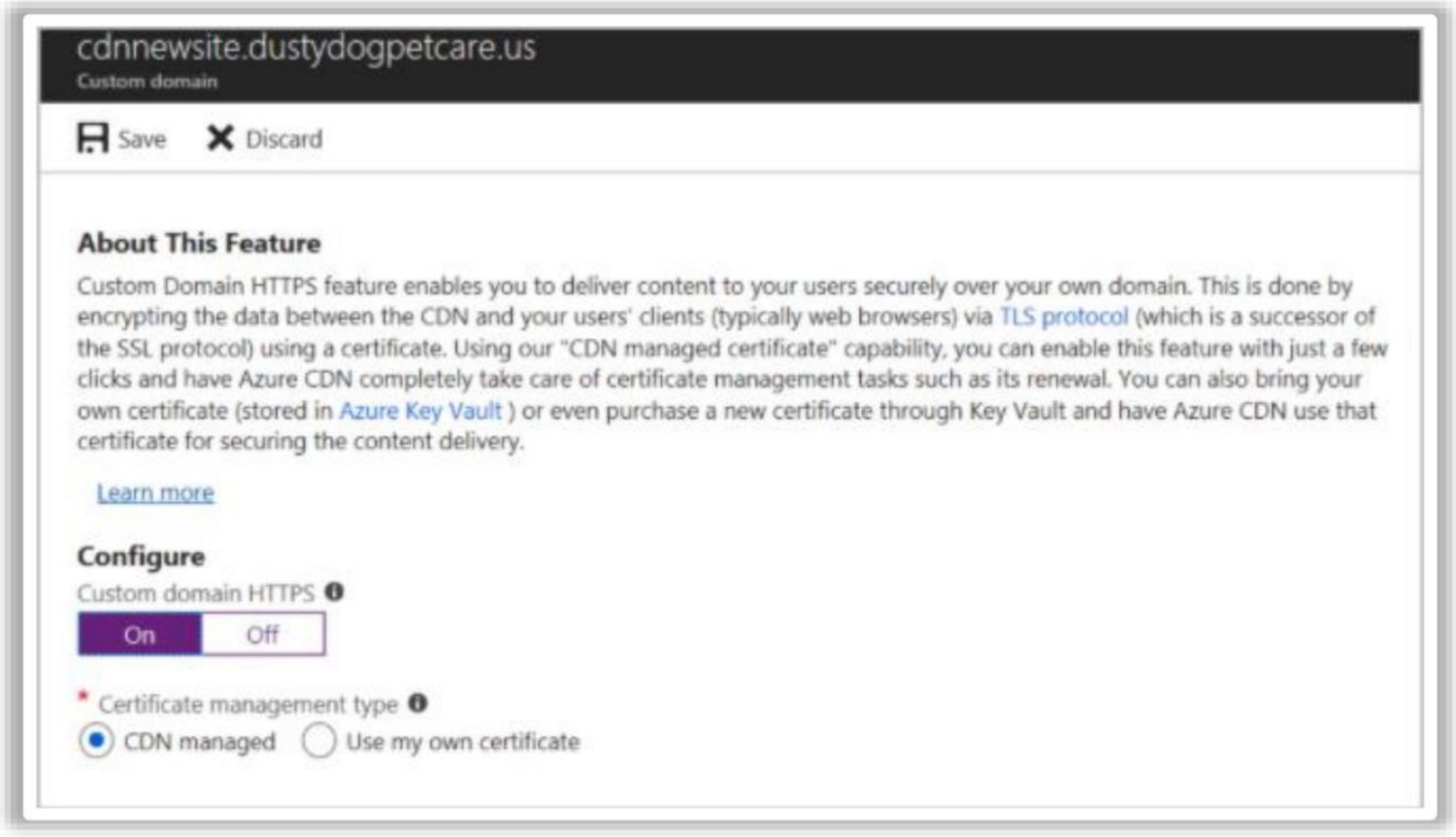


FIGURE 3.107: Configure Custom Domain

- Move ahead to **validate the domain**.

- **Validate the domain**

  - While a custom domain is added to your endpoint, a CNAME record is created in the DNS domain registrar which is mapped to the CDN endpoint hostname. The DigiCert CA leverages the CNAME record (if it exists without containing the cdnverify domain) to automatically validate the custom domain ownership. Domain validation is not required if own certificate is used. The CNAME record should be in the following format.



Name	Type	Value
<www.contoso.com>	CNAME	contoso.azureedge.net

FIGURE 3.108: CNAME Record

Name: It is the custom domain name

Value: It is the CDN endpoint hostname

DigiCert CA verifies the custom domain name if the CNAME record is in the right format and creates a certificate (valid for one year) for the domain, but it does not send any verification email for the same.

- If the cdnverify domain is present in the CNAME record, DigiCert CA sends a verification email (as shown below), which needs to be approved.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



From: DigiCert [mailto:admin@digicert.com]
Sent: Wednesday, September 6, 2017 5:49 PM
To: [redacted]
Subject: Please validate ownership of your domain seattle.azurecdn.us -- DigiCert order [redacted]

digicert

Verizon Digital Media Services, Inc.

DigiCert recently received a certificate request that requires approval prior to the certificate's issuance.

To review and approve this request, visit the following link:

https://www.digicert.com/link/approve.php?t=vrg6wz2gvv97vx95hg

Domain names requiring your approval: seattle.azurecdn.us

The certificate was requested by:

Verizon Digital Media Services
VDMS
ssl-orders@verizondigitalmedia.com
+1 (877) 334-3236

If you do not approve of this request, or if you have any questions or concerns please contact us directly.

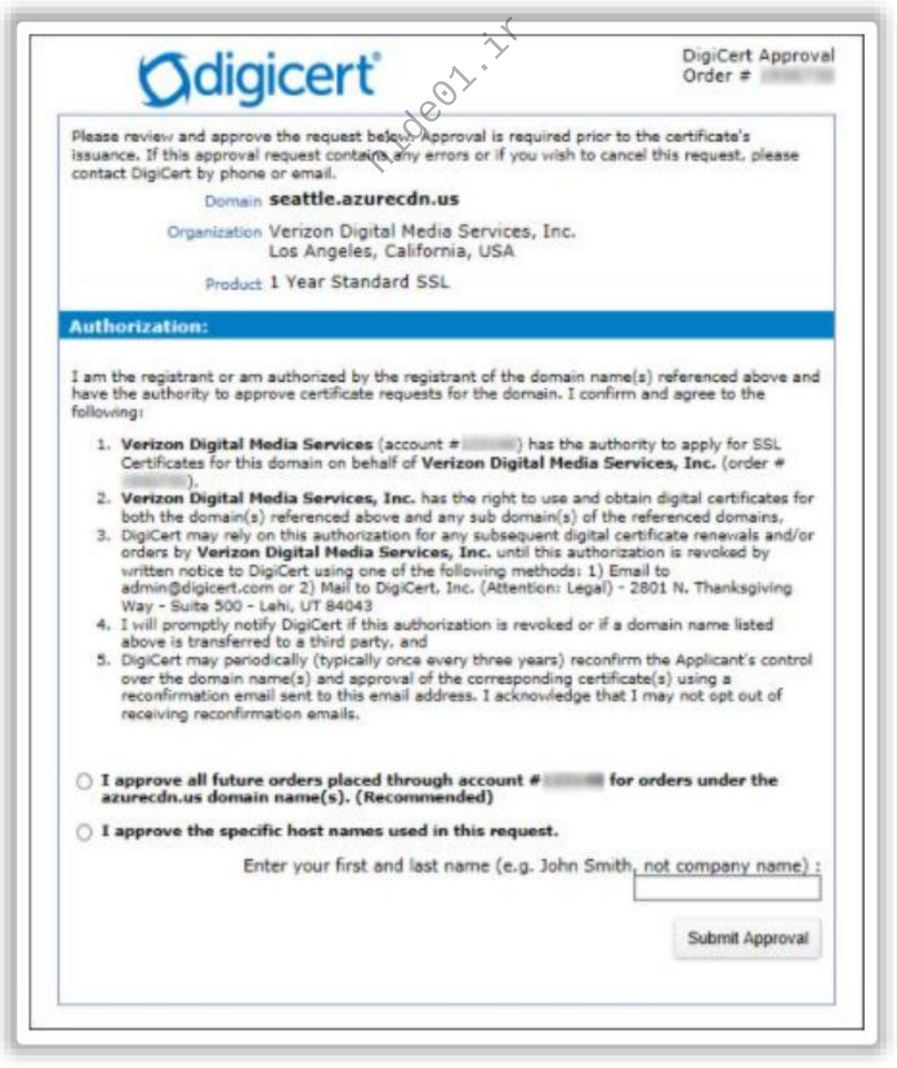
Thanks!

The DigiCert Team

Phone: 1-801-701-9600
Email: support@digicert.com
Live Chat: www.digicert.com

FIGURE 3.109:Verification E-mail

- The approval link will redirect you to an online approval form, as shown below.



digicert

DigiCert Approval
Order # [redacted]

Please review and approve the request below. Approval is required prior to the certificate's issuance. If this approval request contains any errors or if you wish to cancel this request, please contact DigiCert by phone or email.

Domain **seattle.azurecdn.us**
Organization Verizon Digital Media Services, Inc.
Los Angeles, California, USA
Product 1 Year Standard SSL

Authorization:

I am the registrant or am authorized by the registrant of the domain name(s) referenced above and have the authority to approve certificate requests for the domain. I confirm and agree to the following:

1. **Verizon Digital Media Services** (account # [redacted]) has the authority to apply for SSL Certificates for this domain on behalf of **Verizon Digital Media Services, Inc.** (order # [redacted]).
2. **Verizon Digital Media Services, Inc.** has the right to use and obtain digital certificates for both the domain(s) referenced above and any sub domain(s) of the referenced domains.
3. DigiCert may rely on this authorization for any subsequent digital certificate renewals and/or orders by **Verizon Digital Media Services, Inc.** until this authorization is revoked by written notice to DigiCert using one of the following methods: 1) Email to admin@digicert.com or 2) Mail to DigiCert, Inc. (Attention: Legal) - 2801 N. Thanksgiving Way - Suite 500 - Lehi, UT 84043
4. I will promptly notify DigiCert if this authorization is revoked or if a domain name listed above is transferred to a third party, and
5. DigiCert may periodically (typically once every three years) reconfirm the Applicant's control over the domain name(s) and approval of the corresponding certificate(s) using a reconfirmation email sent to this email address. I acknowledge that I may not opt out of receiving reconfirmation emails.

○ **I approve all future orders placed through account # [redacted] for orders under the azurecdn.us domain name(s). (Recommended)**

○ **I approve the specific host names used in this request.**

Enter your first and last name (e.g. John Smith, not company name) :

Submit Approval

FIGURE 3.110: Approval link

- Choose an appropriate verification option and click on **Submit Approval** to complete the certificate creation.

- **Wait for propagation**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

It may take up to 8 hours for the custom domain HTTPS feature to get activated after the validation. The custom HTTPS status will be changed to Enabled in the Azure portal once the process is completed. This indicates that the custom domain is ready to use HTTPS.

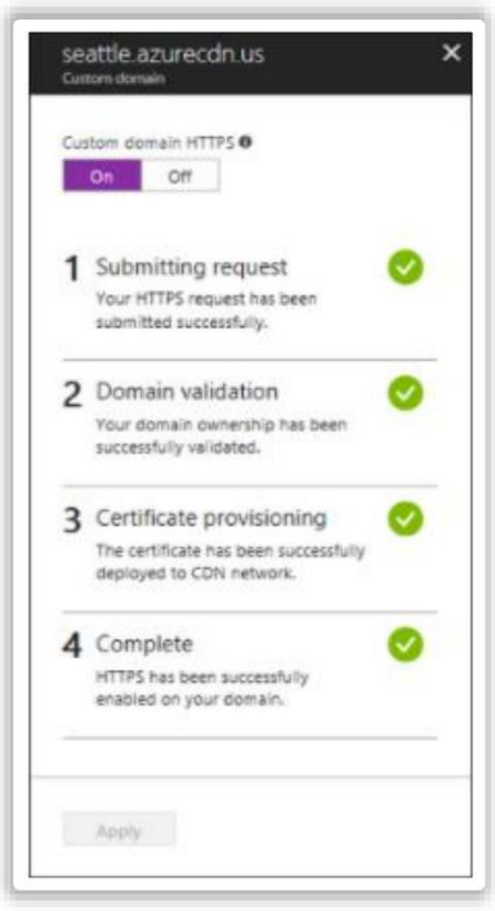


FIGURE 3.111: Propagation

- **Enable diagnostic logs in Azure CDN**: Enable diagnostic logs on CDN endpoints to monitor and view core analytics. These logs can be saved into one or more destinations (e.g., Azure Storage account). Export basic usage metrics to various sources from the CDN endpoint to use them in a customized way.
    - **Enabling logging**
        - Log in to the Azure portal and go to **All resources**. Select **your-cdn-profile**.
        - Choose the **CDN endpoint** to enable diagnostic logs.

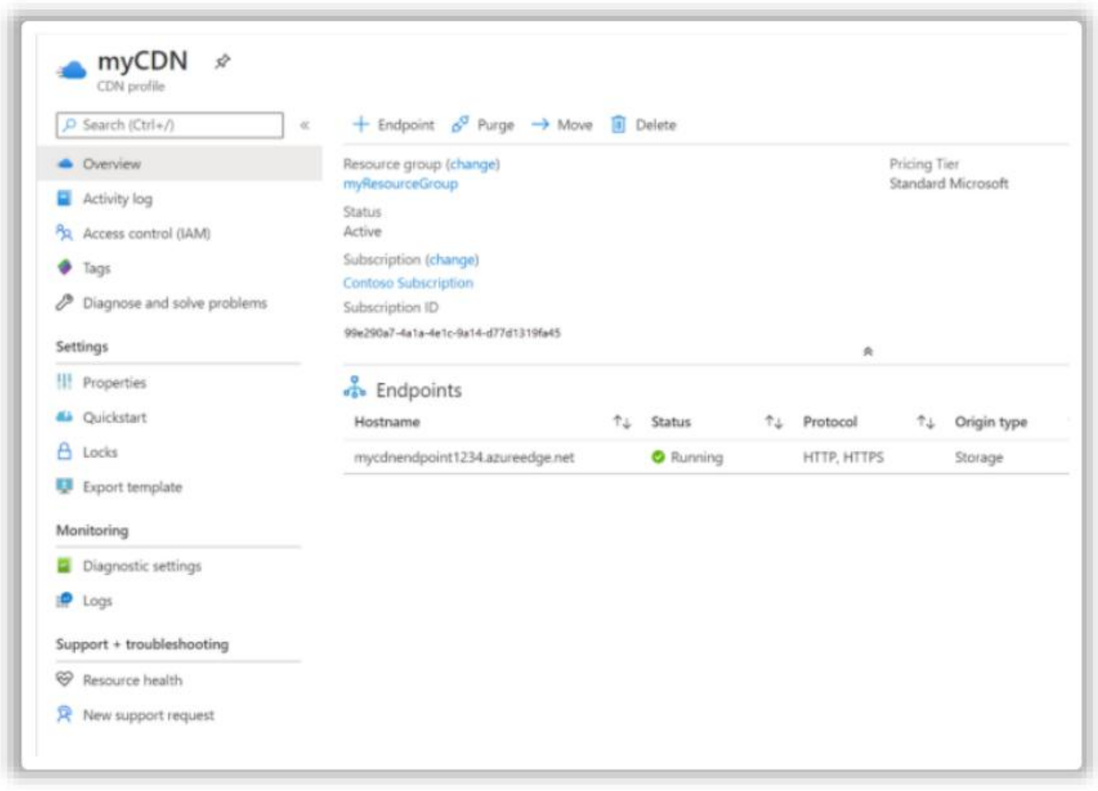


FIGURE 3.112: Choose CDN Endpoint

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Under **Monitoring** section, choose **Diagnostics logs**.

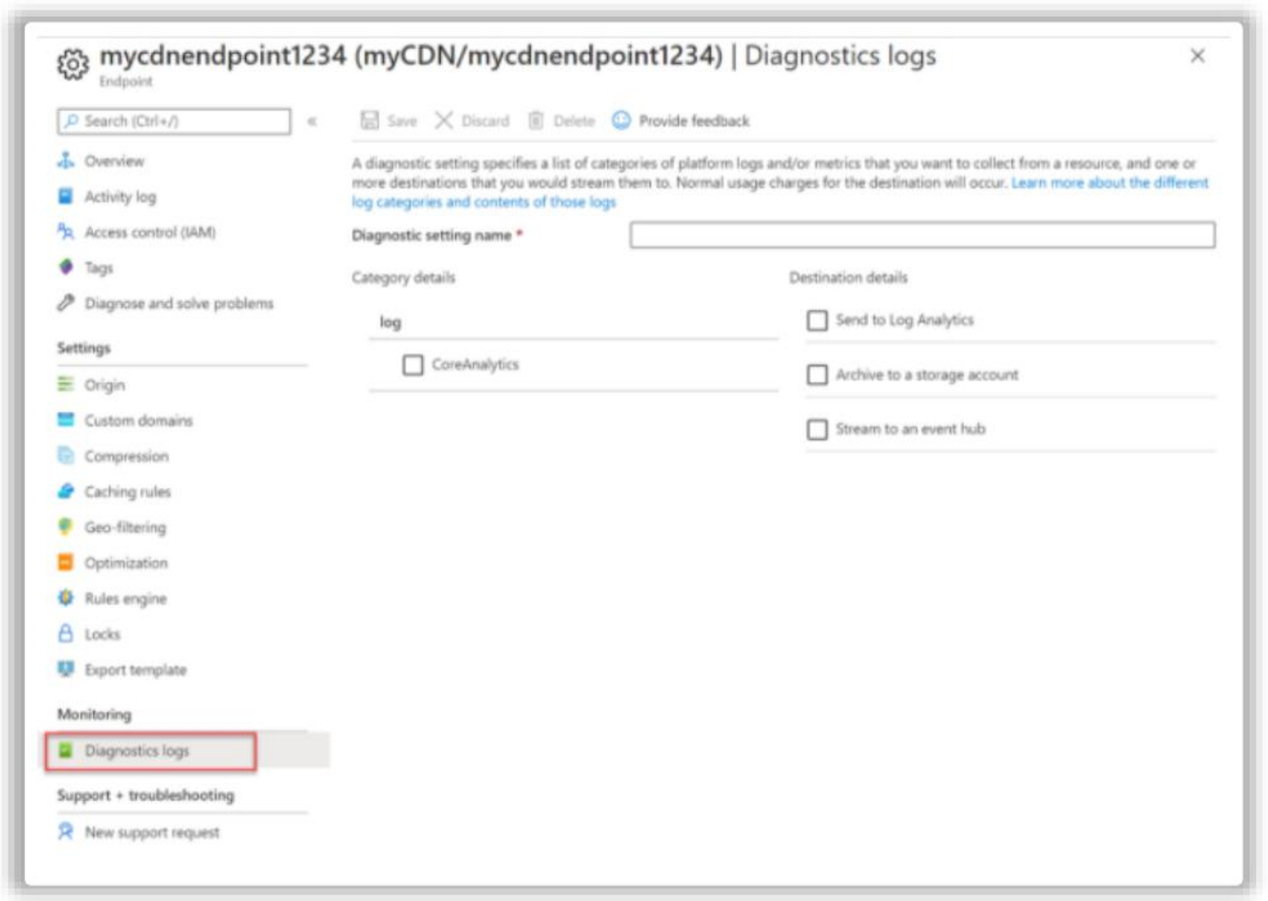


FIGURE 3.113: Diagnostics Logs

- **Enable logging with Azure storage**

  Steps to store diagnostic logs in a storage account are listed below.

  - Provide a name for the diagnostic log settings for **Diagnostic setting name**.
  - Choose **Archive to a storage account** and choose **CoreAnalytics**.
  - Select the number of retention days for **Retention**.
  - Choose the subscription and then select the storage account for the logs.

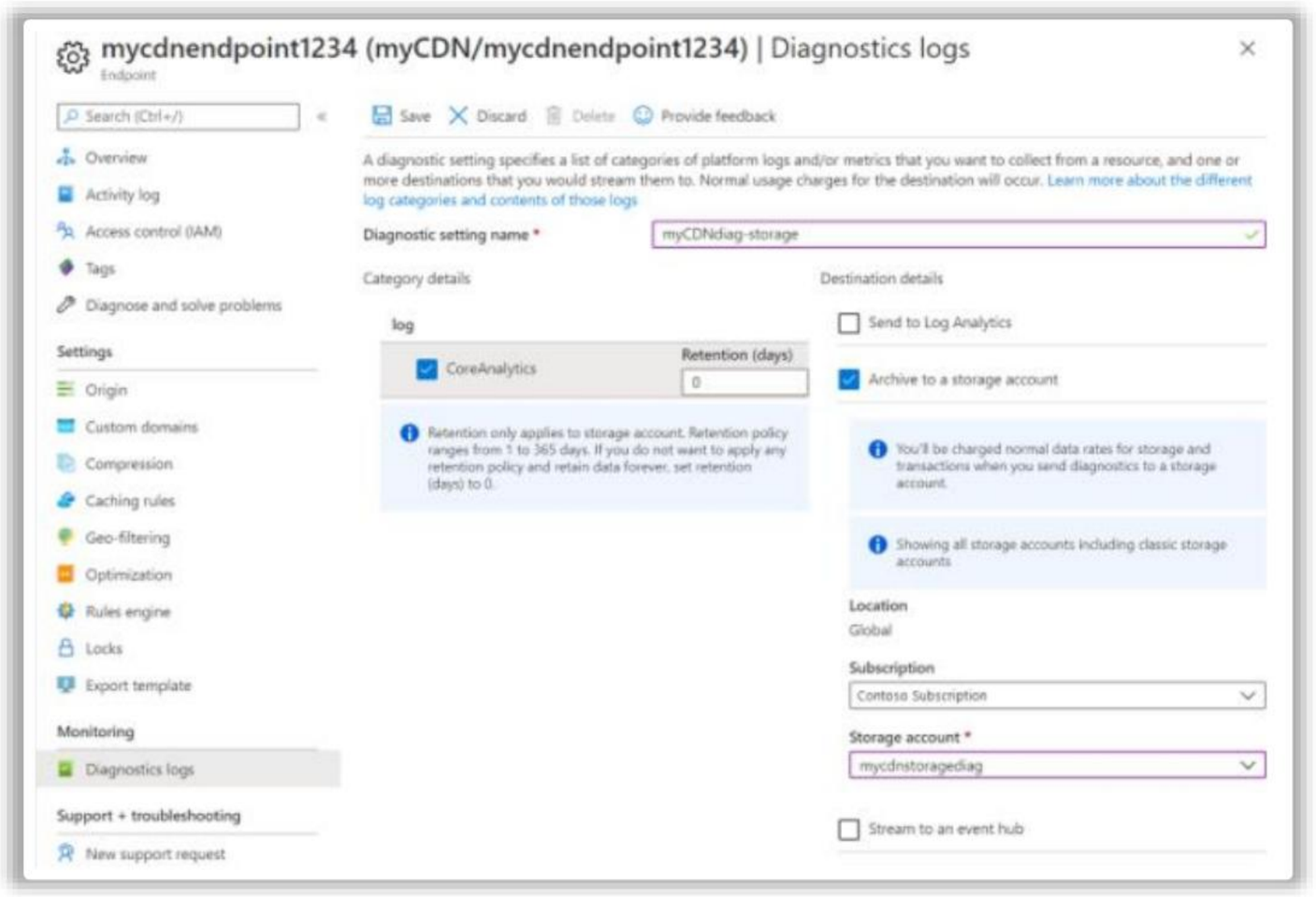


FIGURE 3.114: Choose Subscription

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click on **Save**.

- **Use caching rules to control Azure CDN behavior:** Control Azure CDN behavior by using caching rules. Caching rules are used to modify or set default cache expiration behavior globally as well as with custom conditions like a URL path and file extension. These rules are available for Azure CDN Standard from Akamai/Verizon profiles.

  Two types of caching rules are provided by Azure CDN:

  - **Global caching rules**: Only one global caching rule can be set for an endpoint in a profile. This rule will affect all requests received by the endpoints and override HTTP cache-directive headers.
  - **Custom caching rules**: Each endpoint in a profile can have one or more custom caching rules. These rules are processed in order and are used to match specific file extensions and paths. These rules can override global caching rules.

Configure CDN Caching Rules

Steps to access Azure CDN caching rules are as follows:

- Choose a CDN profile on the Azure portal and select an endpoint.
- Choose **Caching rules** under **Settings**.

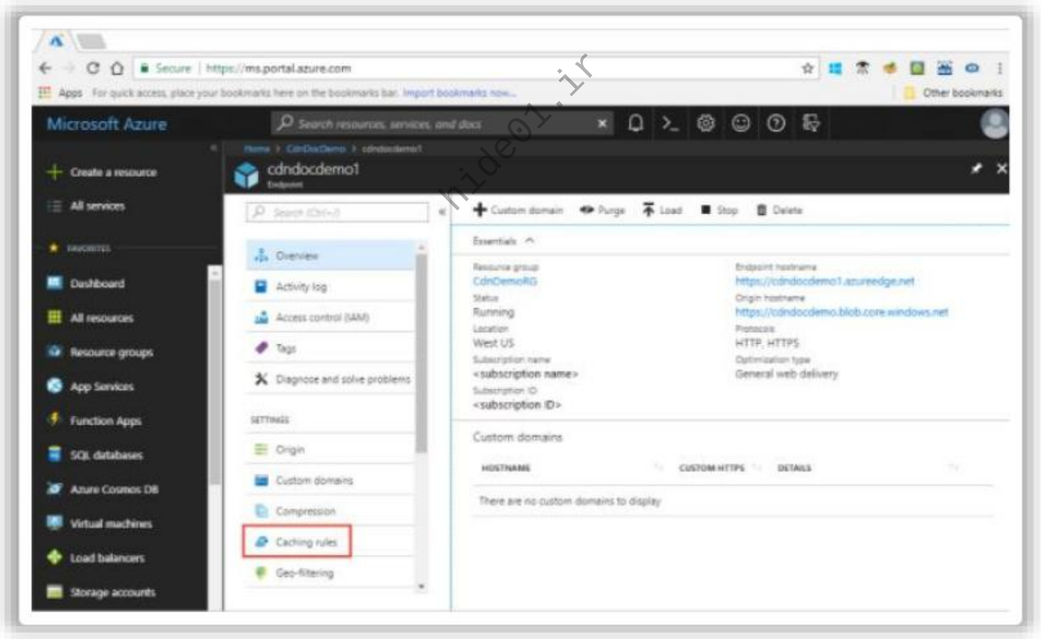


FIGURE 3.115: Settings

- The **Caching rules** page will open.

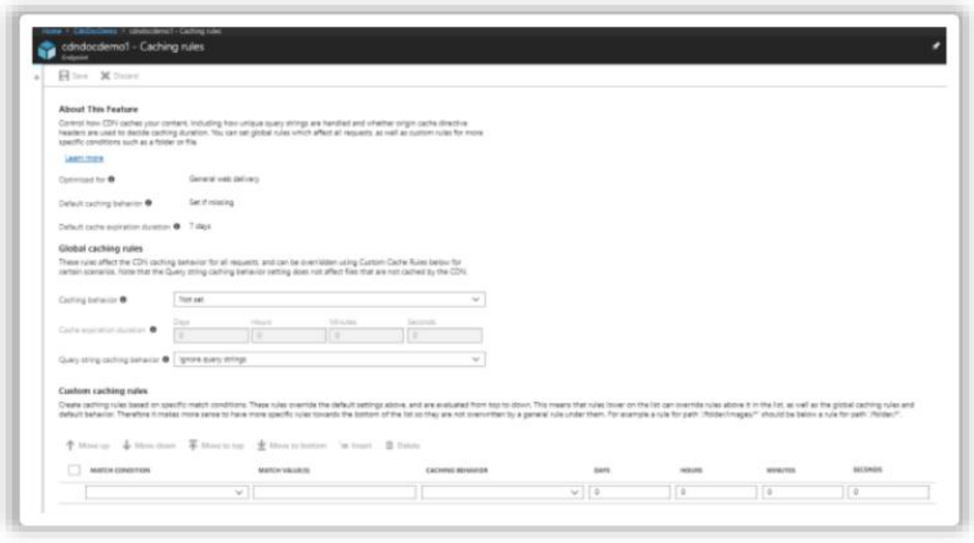


FIGURE 3.116: Caching Rules

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Under **Global caching rules**, select a suitable option for **Caching behavior** from the three options: **Bypass cache**, **Override**, and **Set if missing**.

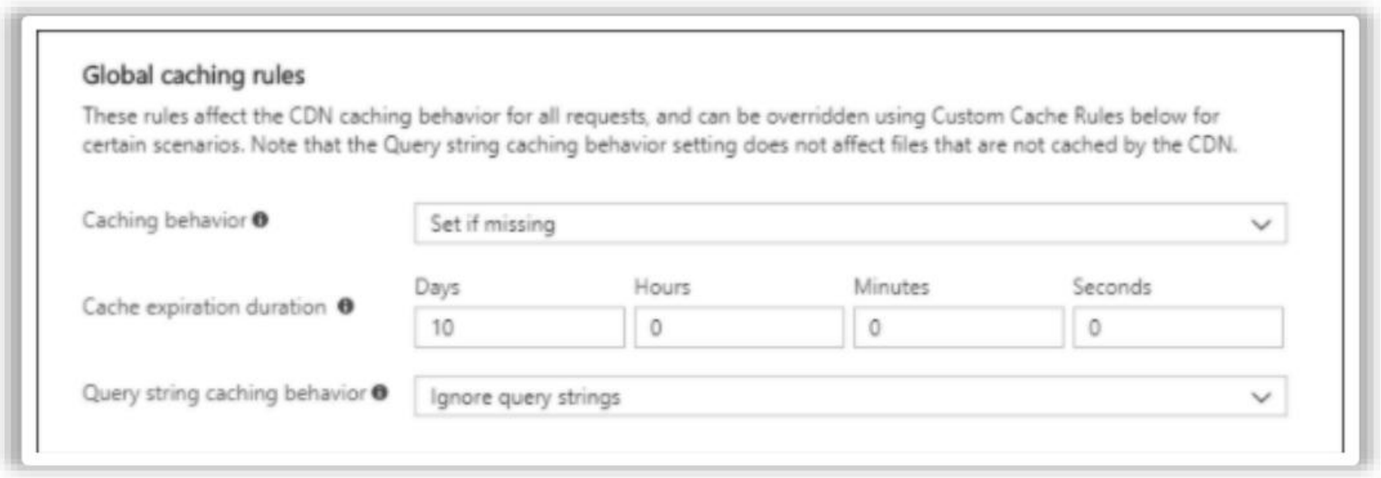


FIGURE 3.117: Global Caching Rule

Set the **Cache expiration duration** between 0 seconds to 365 days for the **Set if missing** and **Override** Caching behavior settings. The cache duration for the **Bypass cache** setting will be automatically set to 0 seconds and cannot be modified.

- Under **Custom caching rules**, choose a match condition from the two conditions: **Path** and **Extension**.

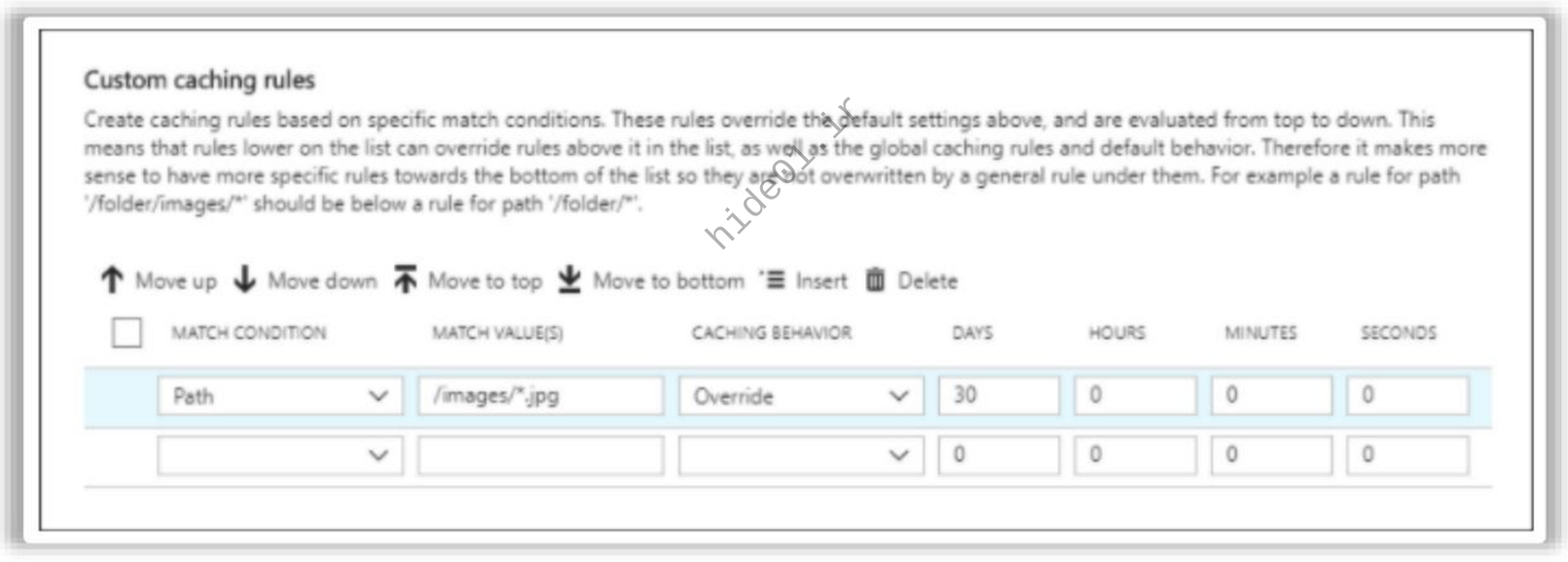


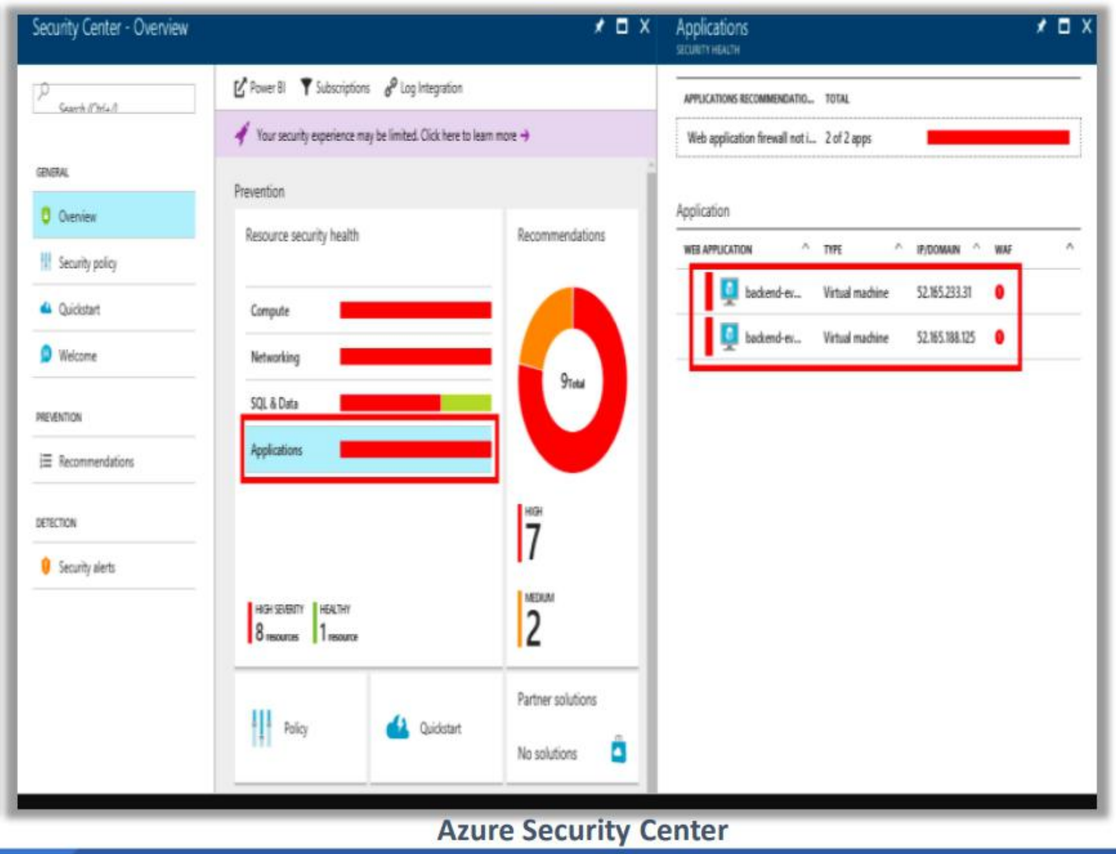
FIGURE 3.118: Custom Caching Rule

- Global caching rules are given priority over default CDN caching behavior, whereas custom caching rules are given priority over global caching rules.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Azure Web Application Firewall

- The Azure Web Application Firewall (WAF) can secure web applications from attacks and **common web vulnerabilities** such as SQL injection, cross-site scripting, etc.
- It can be integrated with **Azure Front Door** for protection from network and application layer attacks
- It can be integrated with **Azure Monitor** to provide real-time visibility and alerts
- Azure WAF centrally **patches** known vulnerabilities instead of each application



Azure Security Center

Source: https://www.microsoft.com

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

Azure Web Application Firewall

Azure Web Application Firewall (WAF) offers centralized protection to cloud applications against vulnerabilities and exploits. Cloud applications with commonly known vulnerabilities become the most common targets of attacks, such as XSS and SQL injection. It is challenging to prevent such attacks as it involves rigorous patching, maintenance, and monitoring at different layers of the app's topology. Azure WAF centrally patches known vulnerabilities instead of each application.

Azure WAF provides effective and faster protection to cloud applications from various attacks. **Azure WAF on Azure Application Gateway** effectively protects cloud applications from common attacks such as session hijacking, XSS, SQL injection, etc. It provides effective protection from the top 10 common vulnerabilities identified by the OWASP. It can be integrated with Azure Front Door for protection from network and application-layer attacks. It can be integrated with Azure Monitor to provide real-time visibility and alerts.

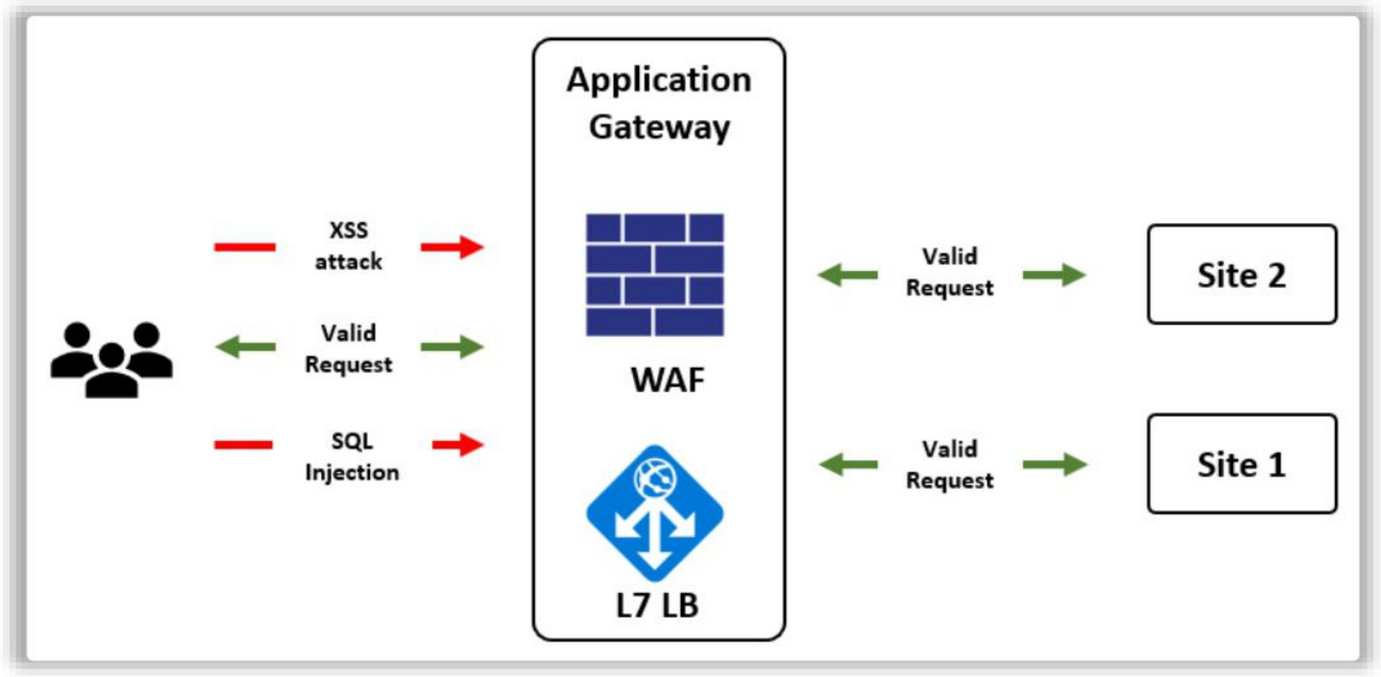


Figure 3.119: Azure WAF on Azure Application Gateway

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Benefits of Using Azure WAF on Application Gateway

- Secure cloud apps without modifying backend code from vulnerabilities and attacks.
- Secure apps with IP Reputation ruleset from malicious bots.
- Protect several cloud apps at the same time.
- Monitor attacks that target cloud apps via real-time WAF logs.
- Have custom WAF policies for different sites.
- Create custom rules that suit your application needs.

Steps to Create Azure WAF on Application Gateway

Source: https://www.microsoft.com

Steps to create Azure WAF on Application Gateway include the following:

- **Create an application gateway:**
  - Log in to the Azure portal and select **Create a resource**.
  - In the new window, choose **Networking** and then choose **Application Gateway** from the **Featured** list.
  - On the **Basics** tab, enter the following application gateway settings.

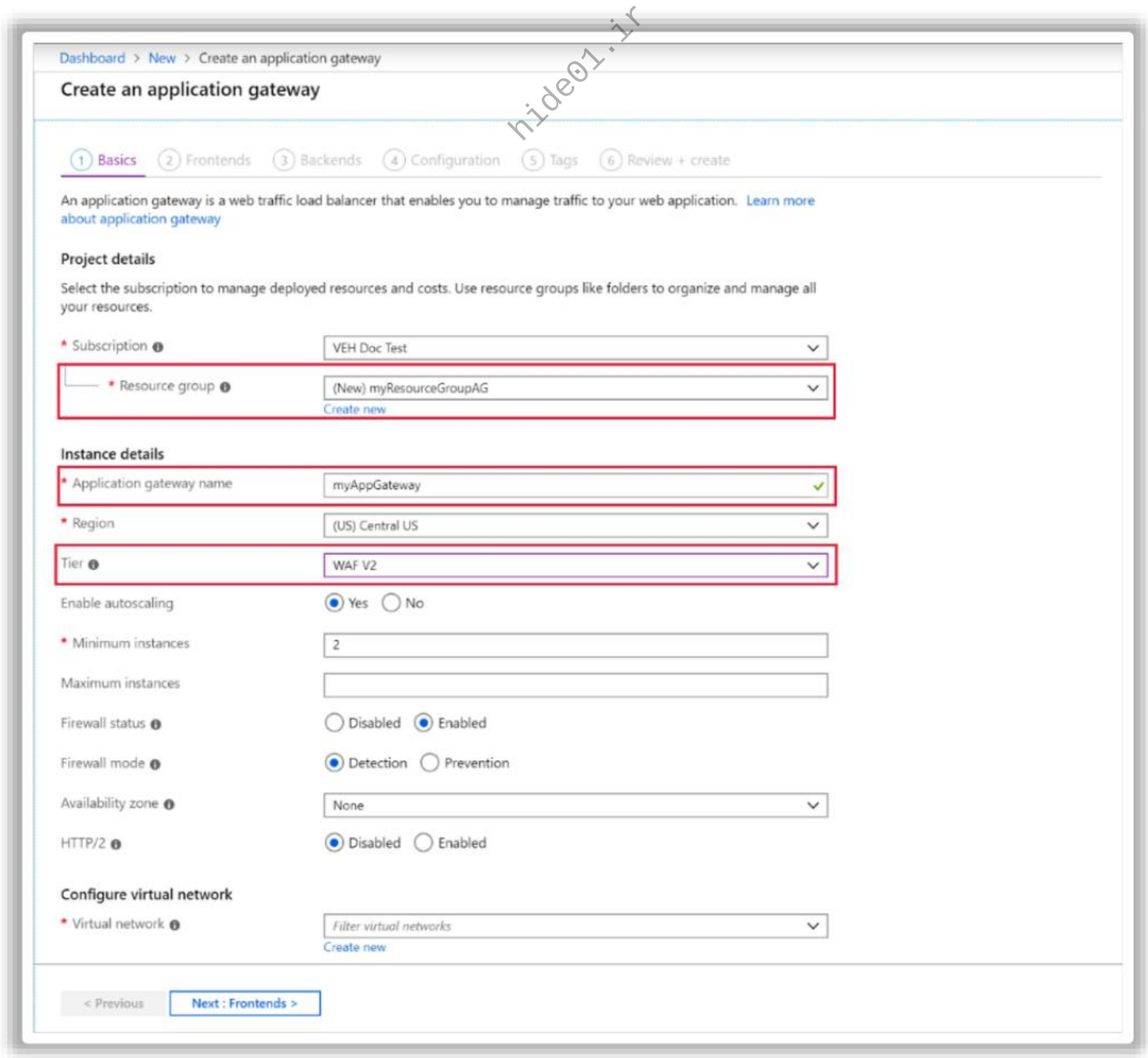
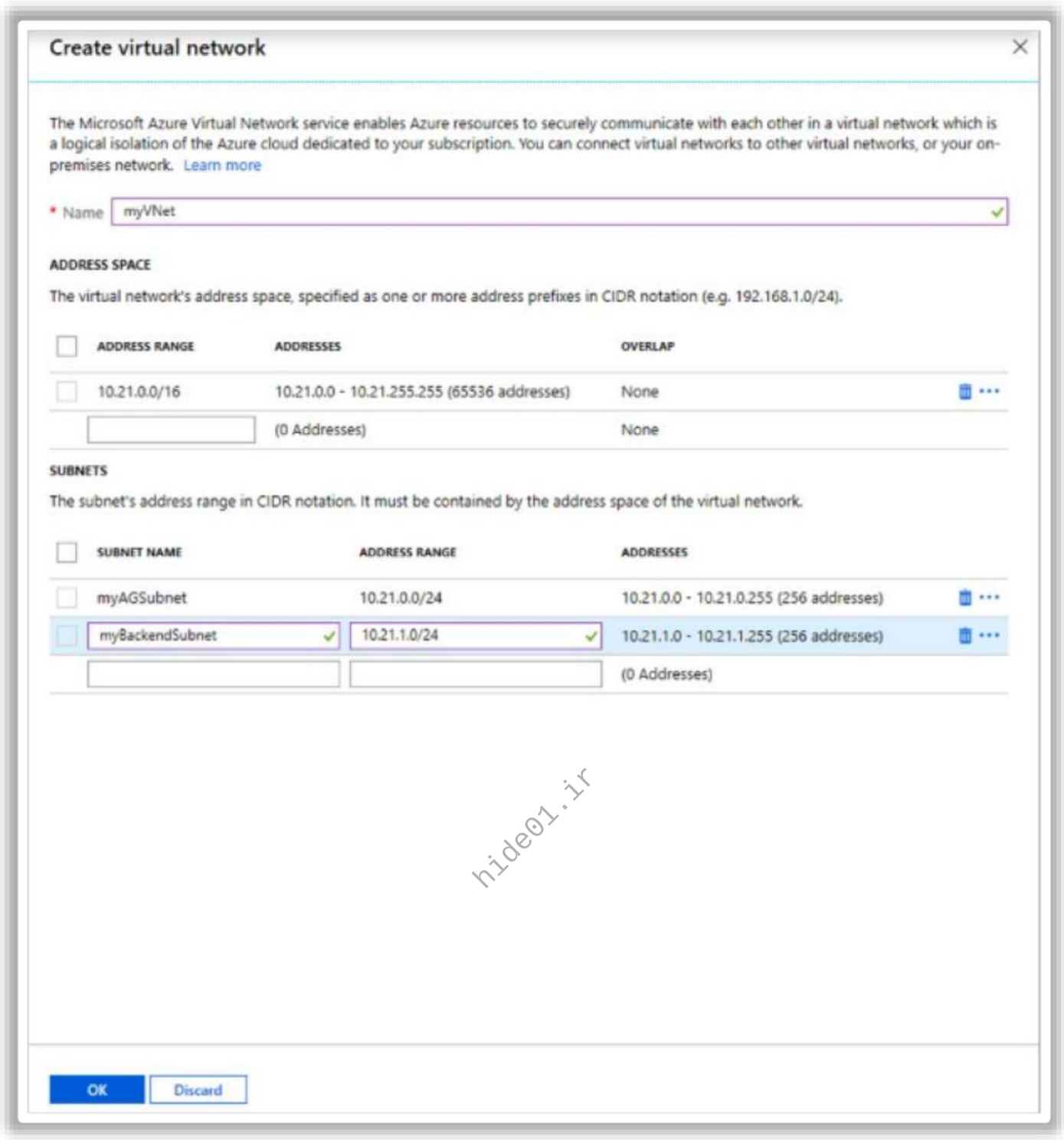


FIGURE 3.120: Basic Tab

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- A virtual network (VNet) is required for resources to communicate. Create or use an existing virtual network. If a VNet does not exist or you want to create a new one, click on **Create new** under **Configure virtual network**. Enter the following information. Click **OK** to save virtual network settings and close the window.



hide01.ir

FIGURE 3.121: Create Virtual Network

- Leave the default values on the **Basics** tab for other settings and click **Next: Frontends**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- On the **Frontends** tab, ensure that the **Frontend IP address type** is **Public**. For the **Public IP address**, select **Create new** and enter the public IP address name (myAGPublicIPAddress). Click **OK**.

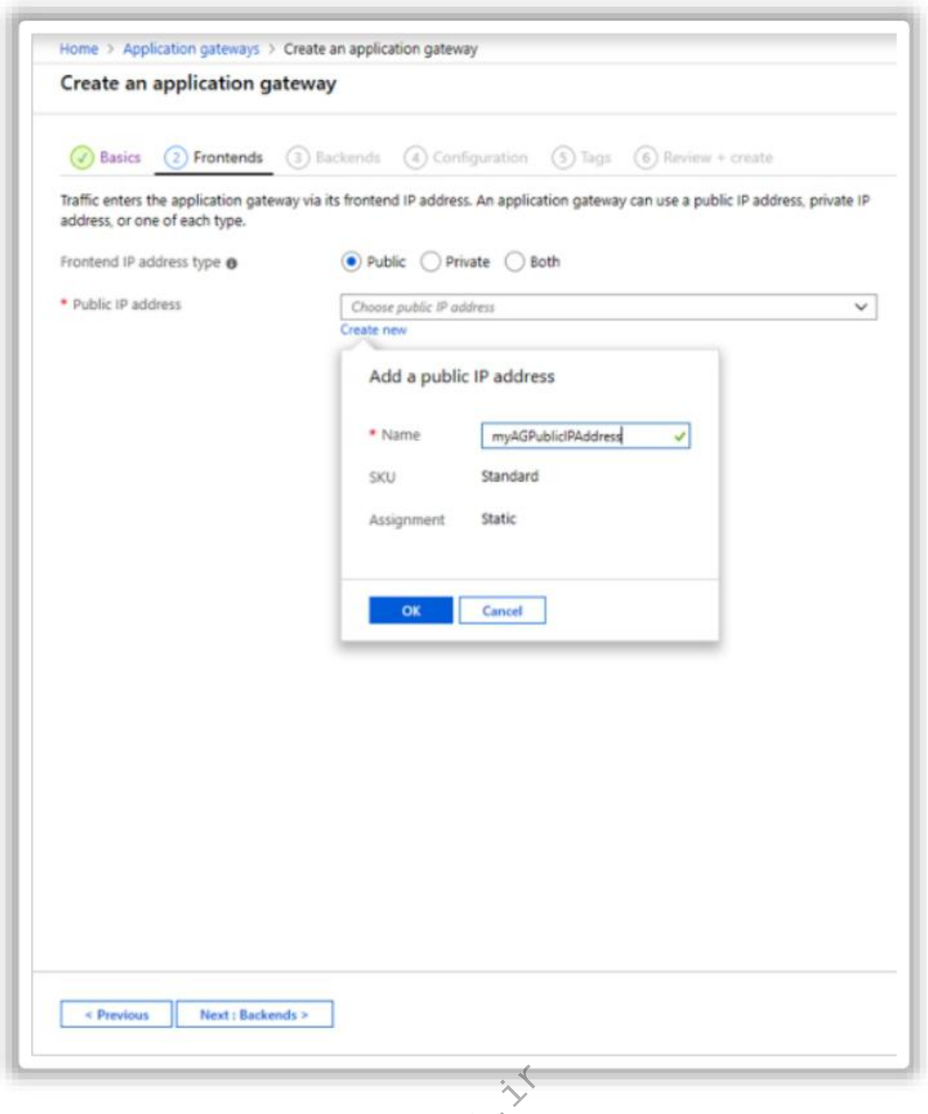


FIGURE 3.122: Add Public IP

hidd01.ir

- Click **Next: Backend**.
- On the **Backends** tab, choose **+Add a backend pool**.
- In the **Add a backend pool** window, create an empty backend pool by entering the name and choosing **Yes** for **Add backend pool without targets** and choose **Add**.

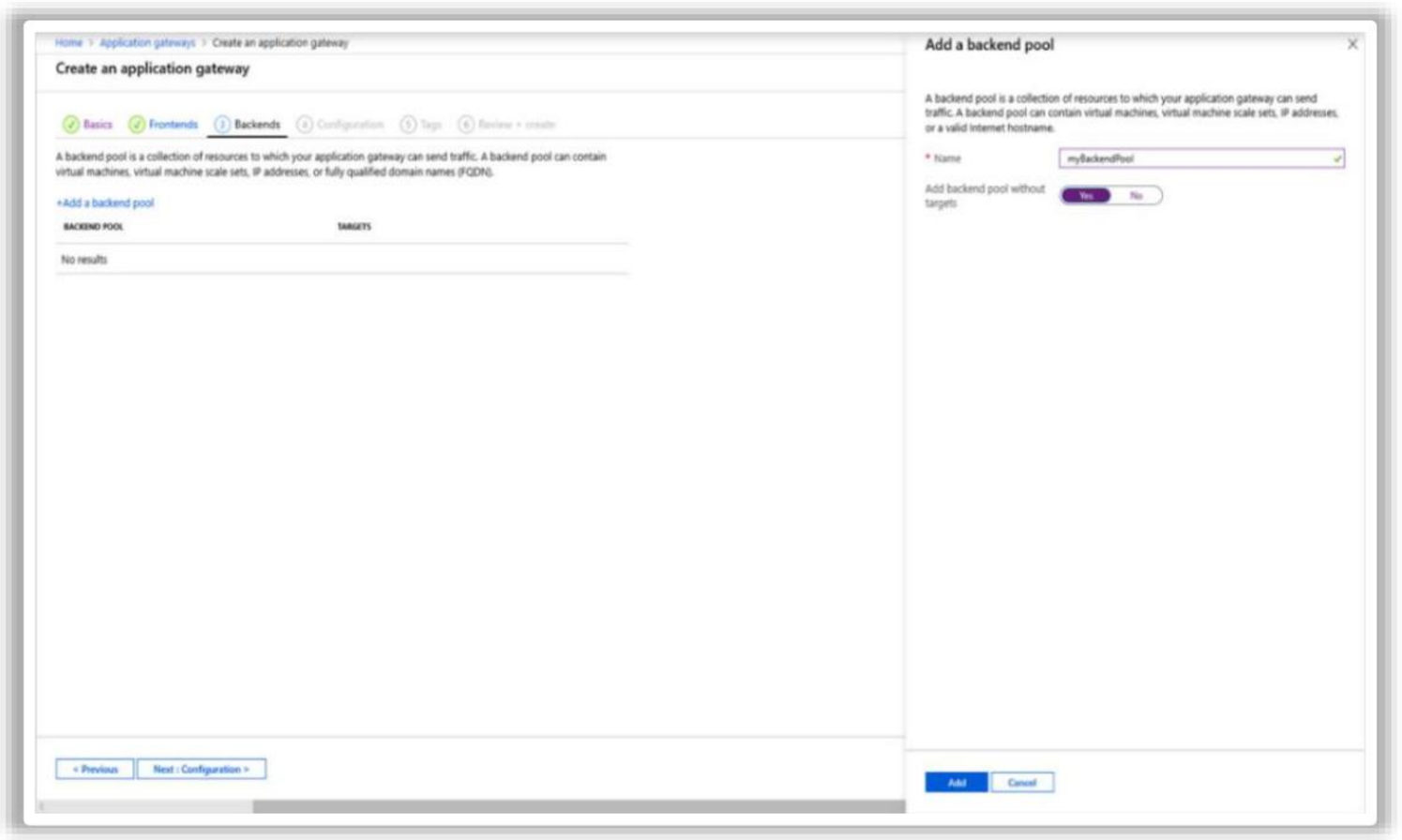


FIGURE 3.123: Add Backend Pool

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Choose **Next: Configuration** on the **Backend** tab.
- On the **Configuration** tab, the frontend and backend pool are connected using a routing rule.
- In the **Routing rules** column, choose **Add a rule**.
- Enter the rule name (myRoutingRule) for the **Rule name** in the **Add a routing rule** window.
- Enter the name (myListener), choose **FrontendIP** as **Public** and keep default values for other settings on the **Listener** tab. Choose **Backend targets** tab.

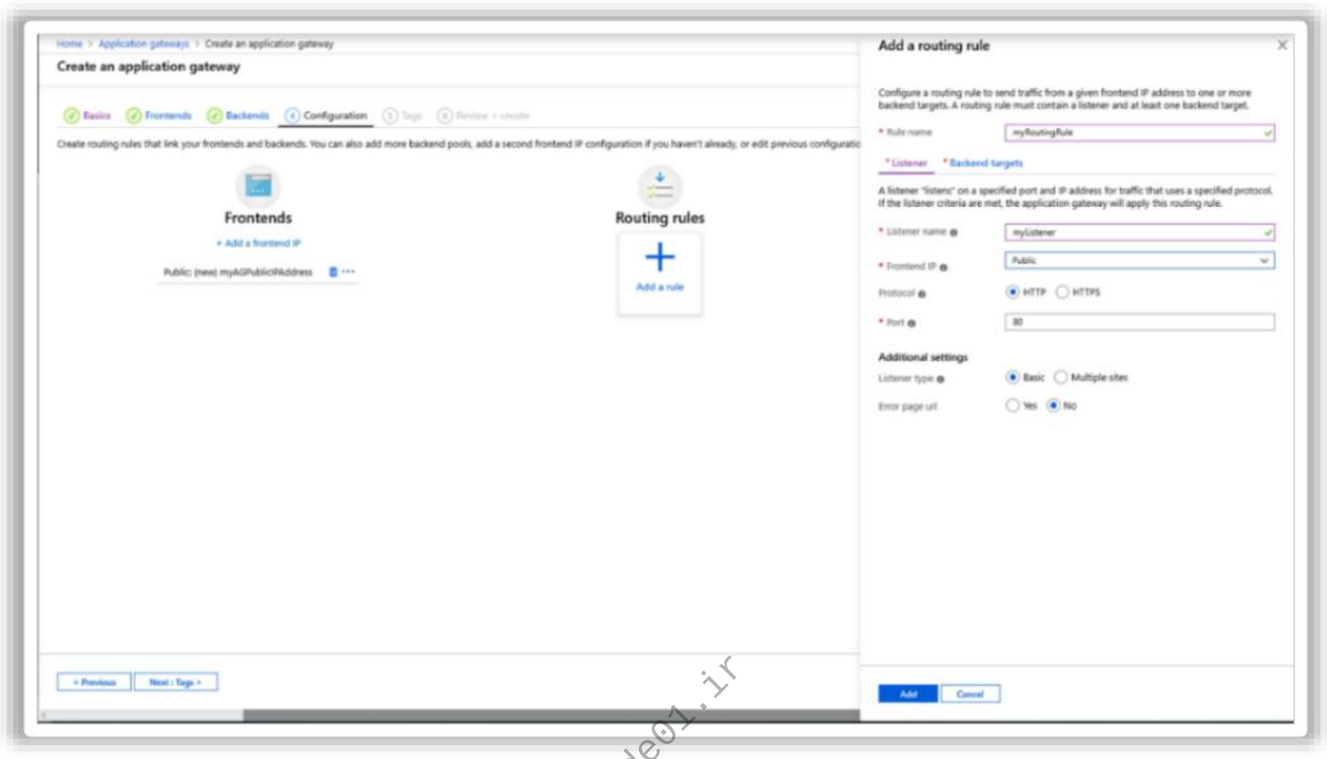


FIGURE 3.124: myListener

- For the **Backend target**, choose **myBackendPool** on the **Backend targets** tab.
- Choose **Create new** for the **HTTP setting**. This setting will determine the routing rule's behavior. On the **Add an HTTP setting** page, enter the name (myHTTPSetting) and accept default values for all other settings. Click on **Add** to go back to the **Add a routing rule** page.

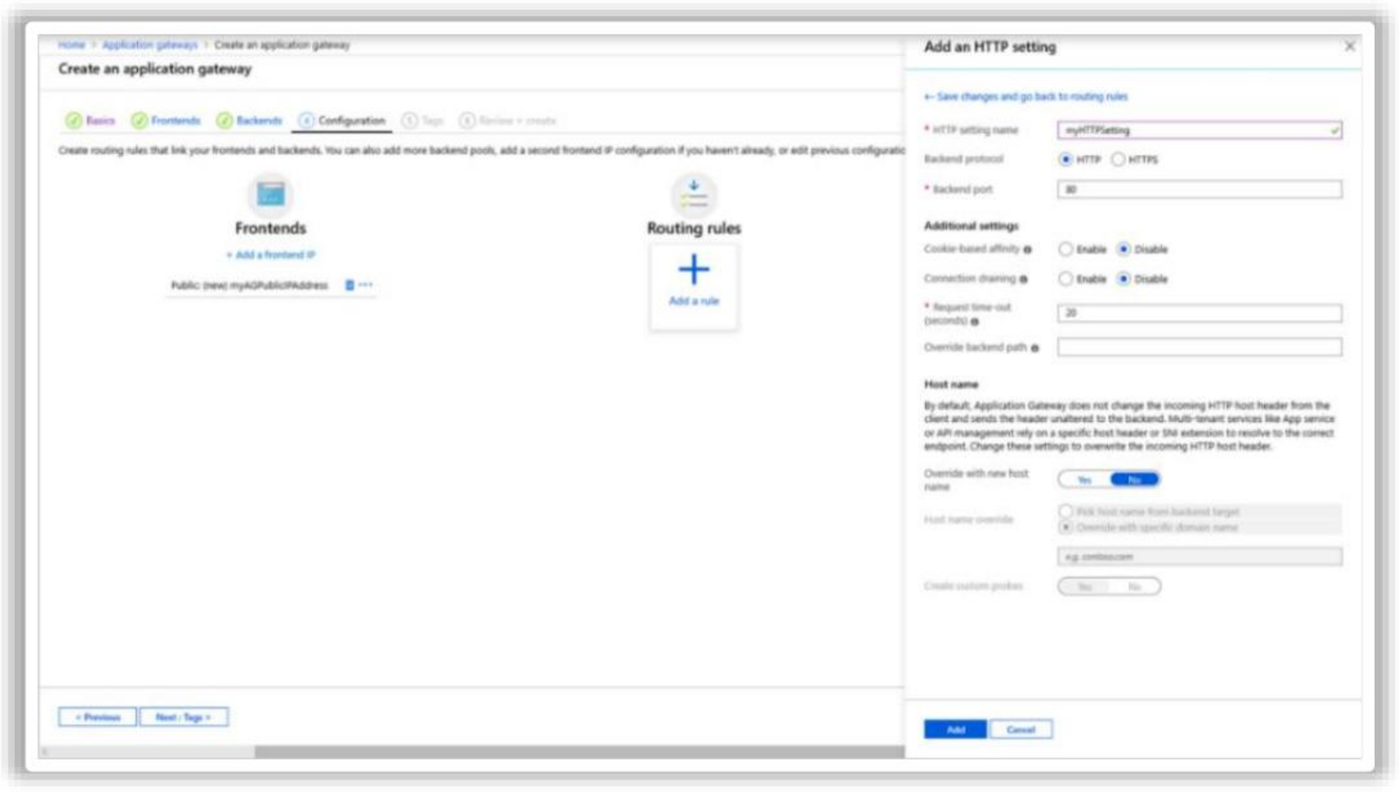


FIGURE 3. 125: HTTP Setting

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Choose **Add** on the **Add a routing rule** page to save the rule and go back to the **Configuration** tab.

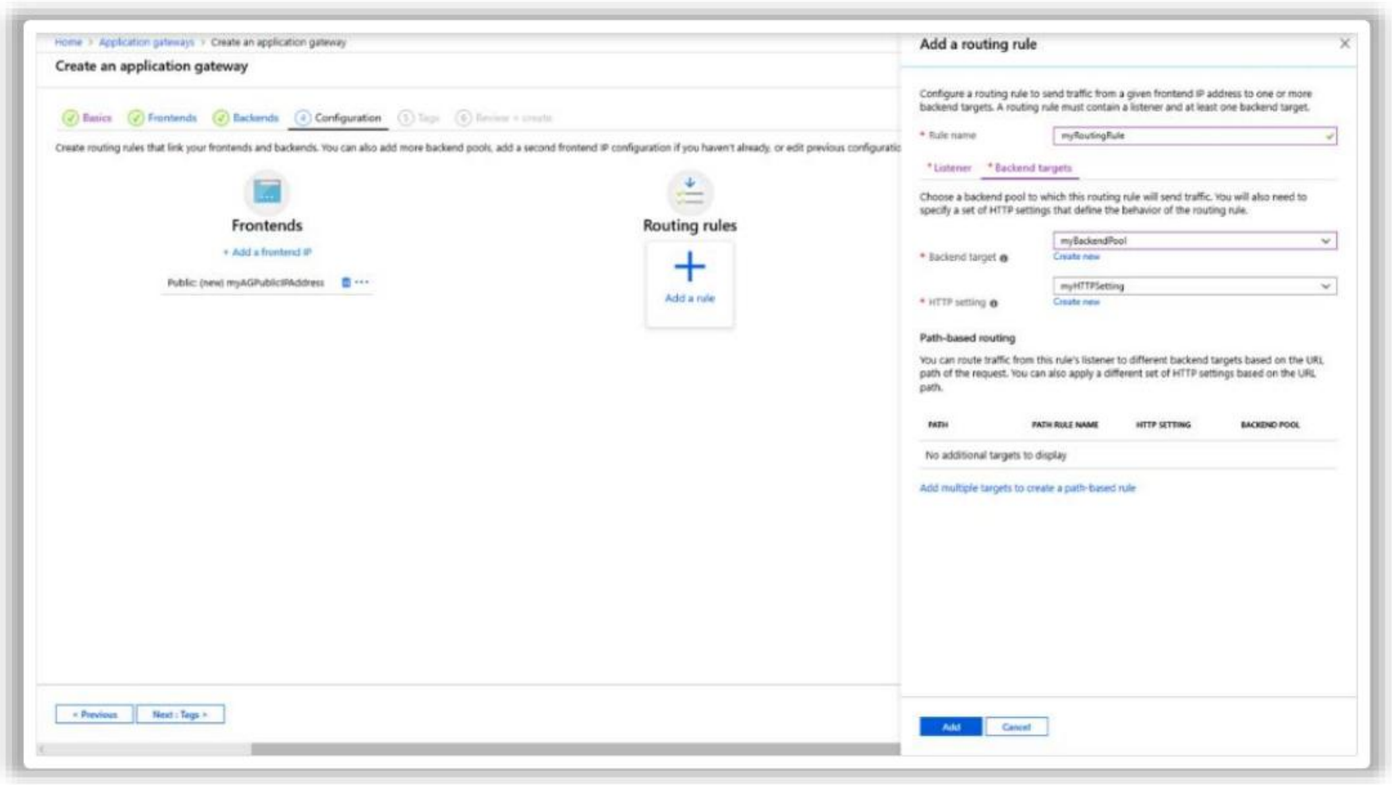


FIGURE 3.126: Add Routing Rule

- Choose **Next: Tags** and select **Next: Review + create**.
- On the **Review + Create** tab, review the settings and then choose **Create**. This will create a VNet, the application gateway, and the public IP address.

- **Add backend targets:** Use existing or new VMs as target backend targets. Here, two new VMs are being created to be used as backend servers for the app gateway and they are added to the backend pool.
  - **Create VMs**
    - On the Azure portal, choose **Create a resource**.
    - In the **Popular** list, choose **Windows Server 2016 Datacenter**. Then, a new window '**Create a virtual machine**' will open.
    - For the VM settings, enter these details on the Basics tab: the **Resource group name** (myResourceGroupAG), **VM name** (myVM), **Username** (azureuser) and **Password** (Azure123456!).
    - Choose **Next: Disks** after leaving other defaults. Keep the default settings on the **Disk** tab and click on **Next: Networking**.
    - On the **Networking** tab, ensure that **myVNet** is chosen for **Virtual network** and **myBackedSubnet** is chosen for the **Subnet**. Choose **Next: Management** after accepting other defaults.
    - Ensure that **Boot diagnostics** is **Off** on the **Management** tab. Choose **Review + Create** after accepting other defaults.
    - Review the settings on the **Review + Create** tab and click on **Create**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Once the VM is created. Repeat the above process to create another VM with a name myVM2.

- **Add backend servers to the pool**
  - Choose **All resources** and then choose **myAppGateway**.
  - Choose **Backend pools** and then select **myBackendPool**.
  - Select **Virtual machine** under **Targets**.
  - Choose **myVM** and **myVM2** under **VIRTUAL MACHINE**. Choose their associated network interfaces under **NETWORK INTERFACES** from the dropdown list.

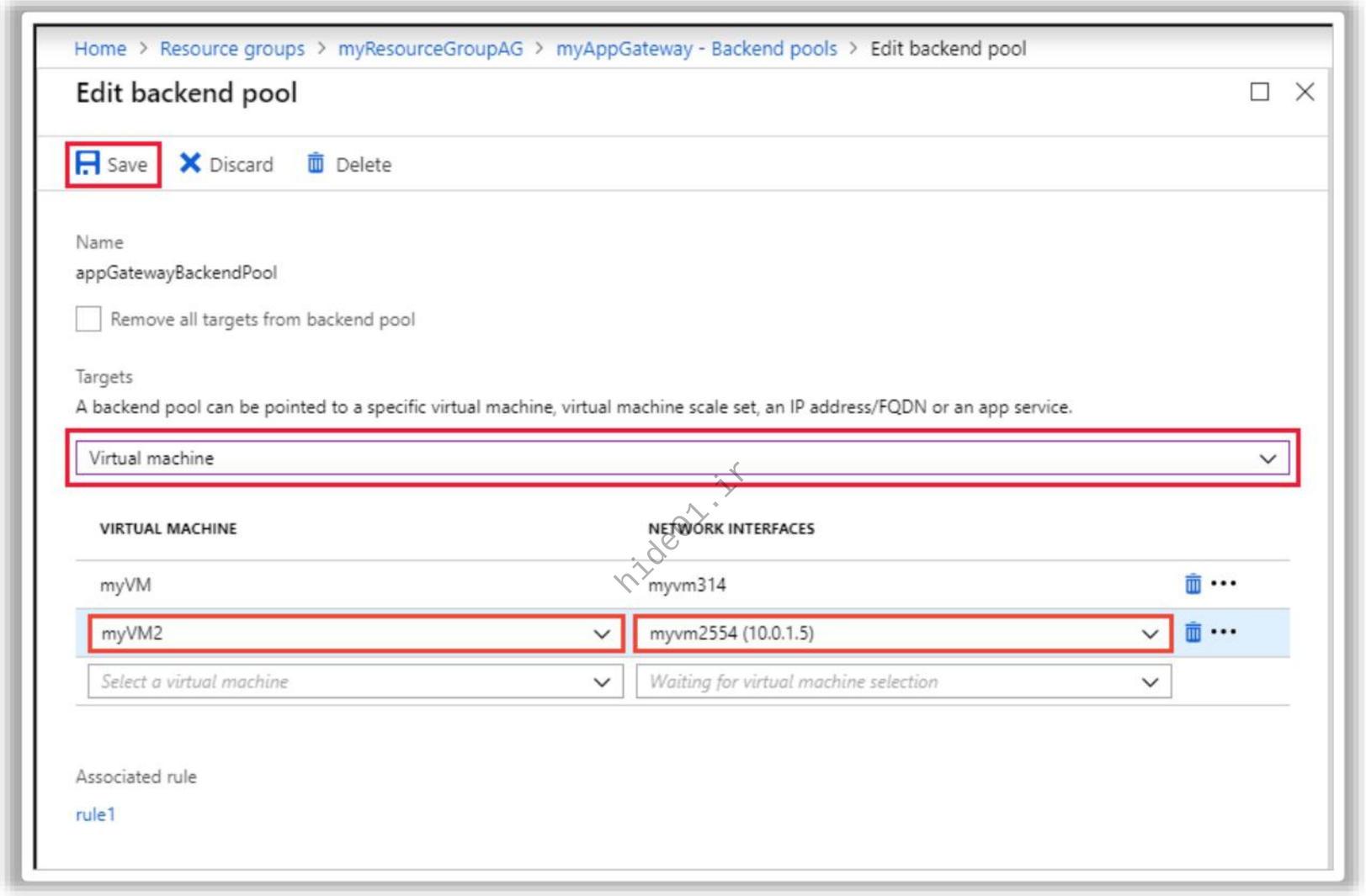


FIGURE 3.127:Edit Backend Pool

- Click on **Save** and wait for the deployment.

- **Create a storage account and configure diagnostics:** A storage account is required for the application gateway to store data for the purpose of detection and prevention. Configure diagnostics to store data into the ApplicationGatewayAccessLog and other logs.
  - **Create a storage account**
    - On the Azure portal, choose **Create a resource**.
    - Choose **Storage** and then click on **Storage account**.
    - Choose myResourceGroupAG for **Resource group**. For name of the account, enter myagstore1 and keep the default values for other settings.
    - Choose **Review + Create** to review settings and then select **Create**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Configure diagnostics**
  - Choose **All resources** on the left side of the menu and the select **myAppGateway**.
  - Choose **Diagnostics settings** under **Monitoring**.
  - Click on **Add diagnostics settings** and enter the name (myDiagnosticsSettings) for the **diagnostics settings**.
  - Choose **Archive to a storage account**. Select **Configure** to choose the newly created (myagstore1) storage account and click on **OK**.
  - Select the application gateway logs and choose **Save**.

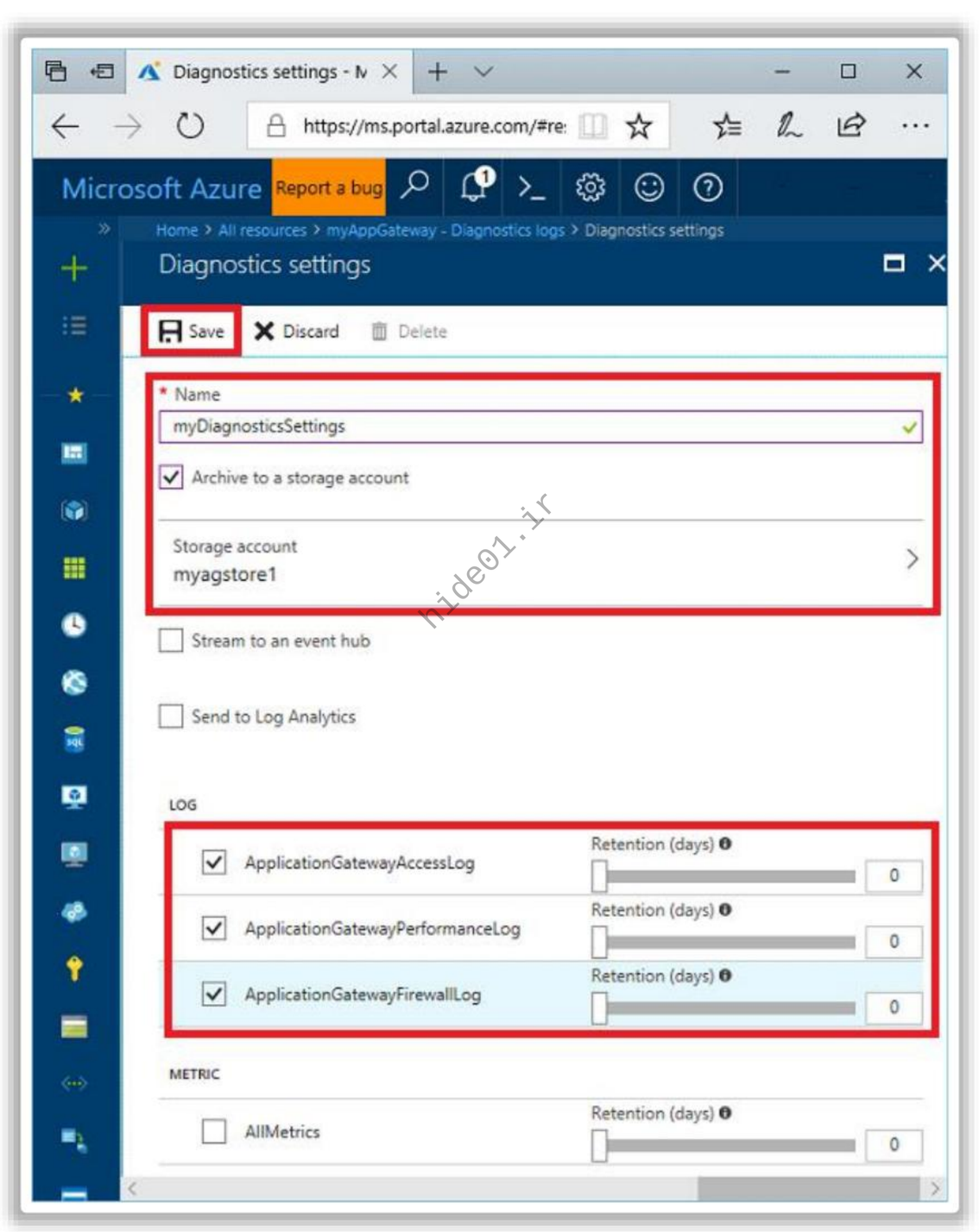


FIGURE 3.128:Diagnostics Settings

- **Link a WAF policy to the WAF**

  Link a WAF policy to the WAF by selecting a WAF policy from the **Associated Application Gateways** tab.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

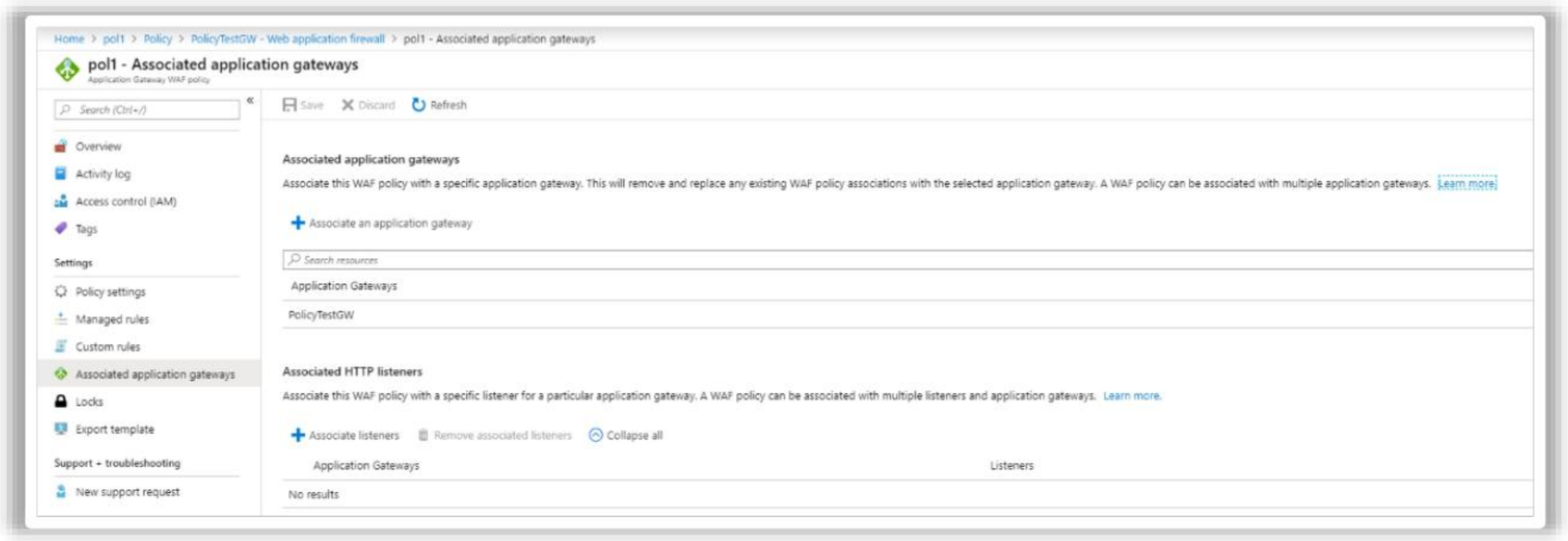


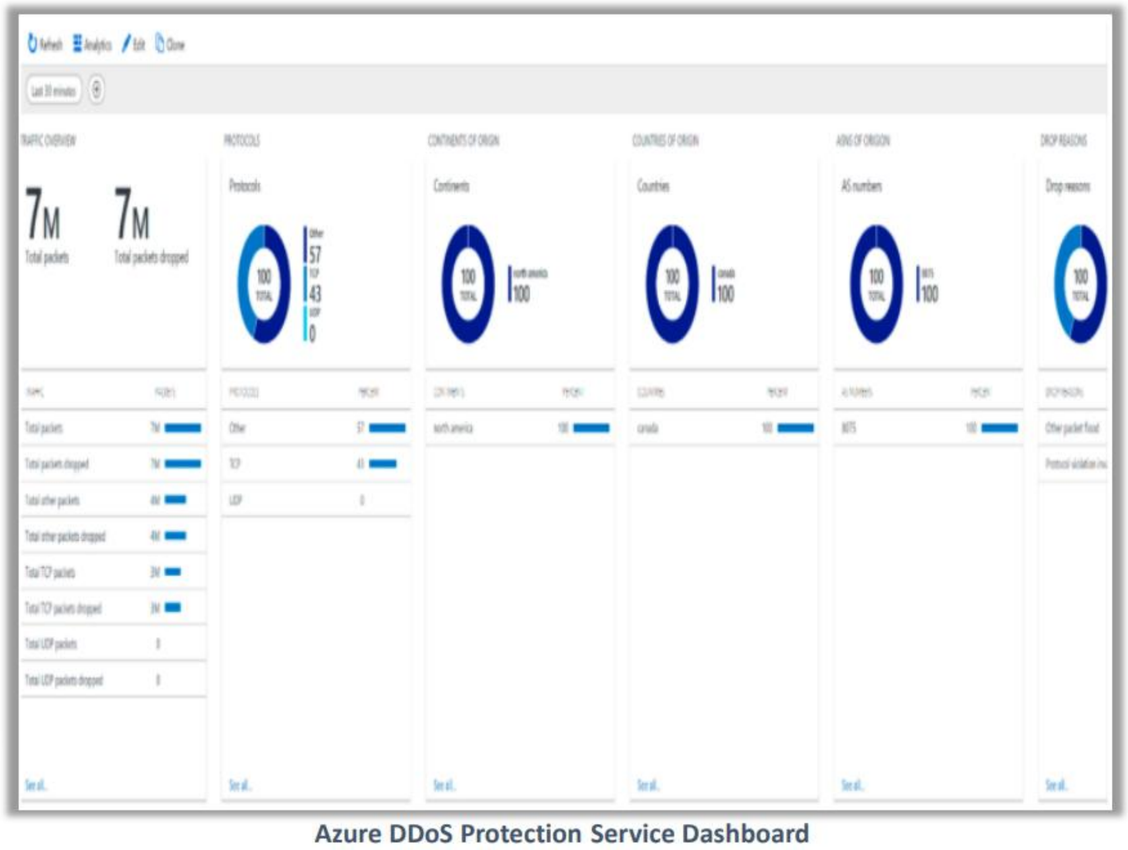
FIGURE 3.129:Associated Application Gateway

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Azure DDoS Protection Service

- Azure DDoS Protection Service, which is always-on, helps monitor and automatically mitigate network attacks
- Azure DDoS protection understands the resources and configurations to analyse the **traffic patterns** of applications over time
- DDoS protection service can be integrated with **Azure Application Gateway** to protect the application from XSS, SQL injection, and session hijacking attacks



Source: https://www.microsoft.com

Azure DDoS Protection Service Dashboard

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

Azure DDoS Protection Service

DDoS attacks mainly affect the availability and ability of cloud applications to handle legitimate requests. Endpoints that are easily reachable via the internet become the main target of DDoS attacks. Azure DDoS protection understands the resources and configurations to analyze the traffic patterns of applications over time. The DDoS Protection service can be integrated with Azure Application Gateway to protect the application from XSS, SQL injection, and session hijacking attacks.

Azure provides two DDoS protection offerings on its platform to secure cloud applications and resources:

- **Azure Basic DDoS Protection**: This protection is offered by Azure without any additional cost as it is integrated into Azure by default. Azure Basic Protection protects against common network-layer attacks by continuous traffic monitoring and real-time mitigation. It does not require any application change or user configuration. This DDoS protection features automatic attack mitigations, and always-on traffic monitoring and detection. It helps secure all Azure services, even PaaS services such as Azure DNS. IPv4 and IPv6 public IP addresses are protected under Basic Protection.
- **Azure Standard DDoS Protection**: This Azure service offers advanced DDoS mitigation capabilities to prevent network attacks. It offers protection to specific Azure resources. Enable the Standard Protection while creating virtual networks or after creating them without any resource or application change. The Standard Protection includes advanced features, including logging, alerting, and telemetry. This protection can effectively prevent protocol attacks, volumetric attacks, and resource layer attacks. Cloud security admins can use this protection to configure alerts at the beginning and end of an attack to protect IPv4 and IPv6 IP addresses.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Azure DDoS Standard Protection Features

Azure DDoS Protection offers the following features:

- **Native platform integration**: Azure DDoS protection is natively integrated into Azure. It easily manages and understands cloud applications and their configuration.
- **Turnkey protection**: DDoS protection protects all cloud applications as soon as the protection is enabled without requiring any user intervention.
- **Always-on traffic monitoring**: It monitors all cloud applications 24×7 for DDoS attempts. Attacks are mitigated as soon as they are detected.
- **Adaptive tuning**: Azure intelligent traffic profiling examines the traffic of your application and chooses a profile that suits your service best. As traffic changes over time, the profile is adjusted.
- **Multi-layered protection**: When DDoS protection is deployed with a WAF, it provides protection at the network layer as well as the application layer.
- **Extensive mitigation scale**: It can mitigate more than 60 different types of DDoS attacks.
- **Attack analytics**: Cloud security administrators can obtain detailed reports with Azure DDoS protection in 5-min increments during an attack and a full summary after the attack is over. For real-time monitoring during attacks, cloud administrators can stream mitigation flow logs to Sentinel or an on-premises SIEM solution.
- **Attack metrics and alerting**: It provides attack metrics from every attack via Azure Monitor. Cloud administrators can configure alerts at the beginning and end of an attack by using built-in metrics. They can also integrate the alerts into Azure Monitor logs, Azure Storage, email, Splunk, and the Azure portal.
- **DDoS Rapid Response**: Cloud administrators can obtain help from the DDoS Rapid Response team to investigate and analyze attacks.

Steps to Enable Standard DDoS Protection

Enable the Standard DDoS Protection so that protection policies are applied to public IP addresses associated with resources deployed in a VNet. Create a Standard DDoS Protection plan and associate various VNets inside multiple subscriptions to this plan. Follow the procedure to do so:

- Log in to the Azure portal. Search for **DDoS protection plan** after clicking on **add resource**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

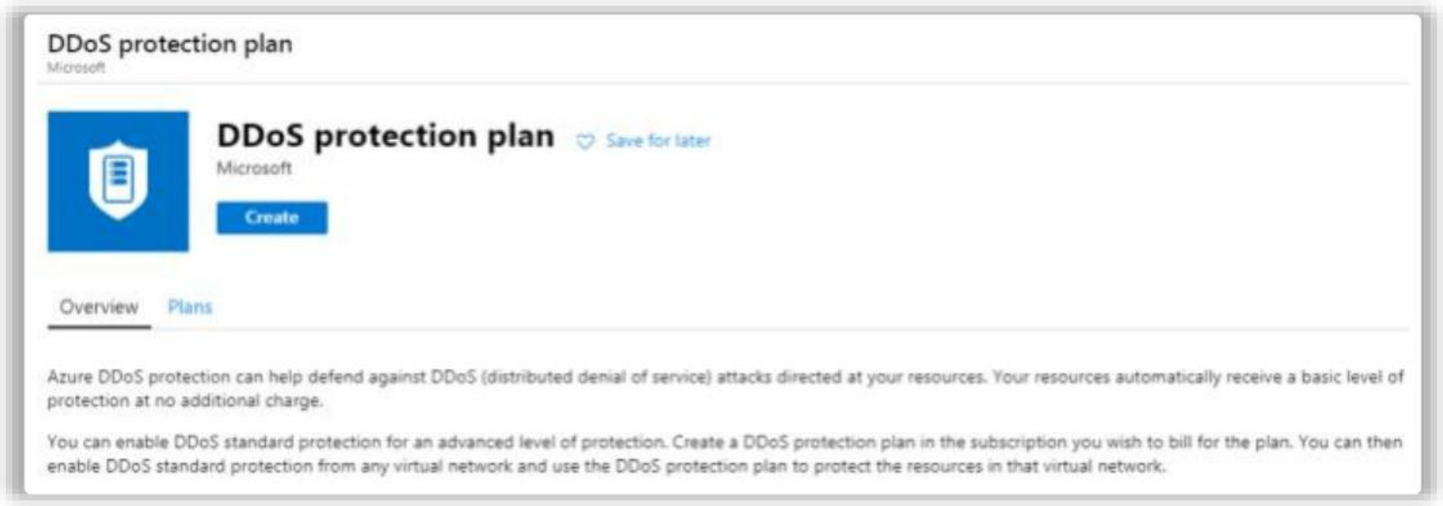


FIGURE 3.130: DDoS Protection Plan

- Select **Create** after entering all requested details.

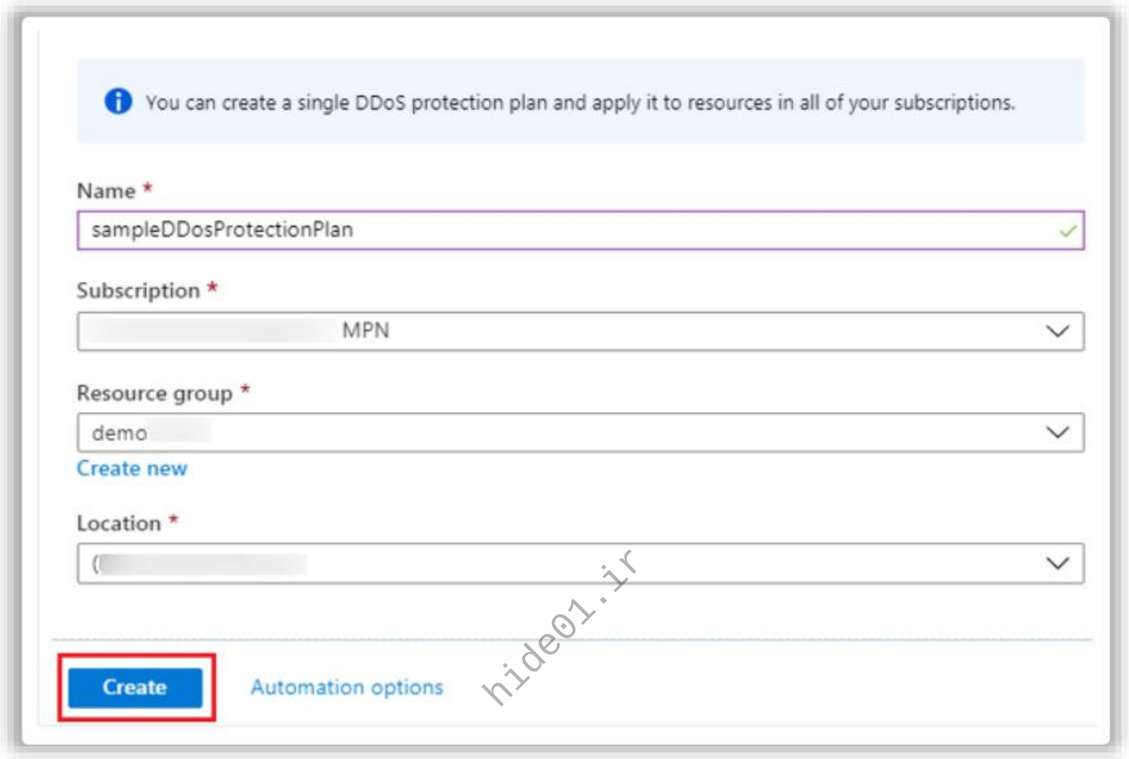


FIGURE 3.131:Create

- Go to your resource group and verify if the protection plan is created. To protect a VNet against DDoS attacks, go to the VNet and choose **DDoS protection** under **Settings**. Choose the plan details and click on **Save**.

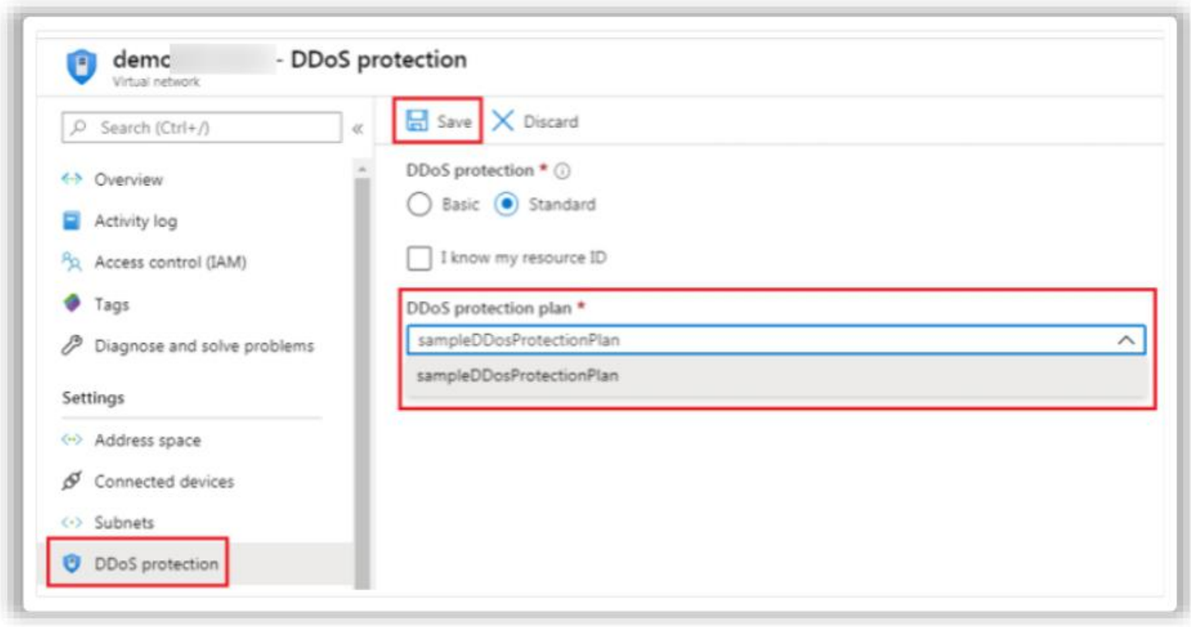
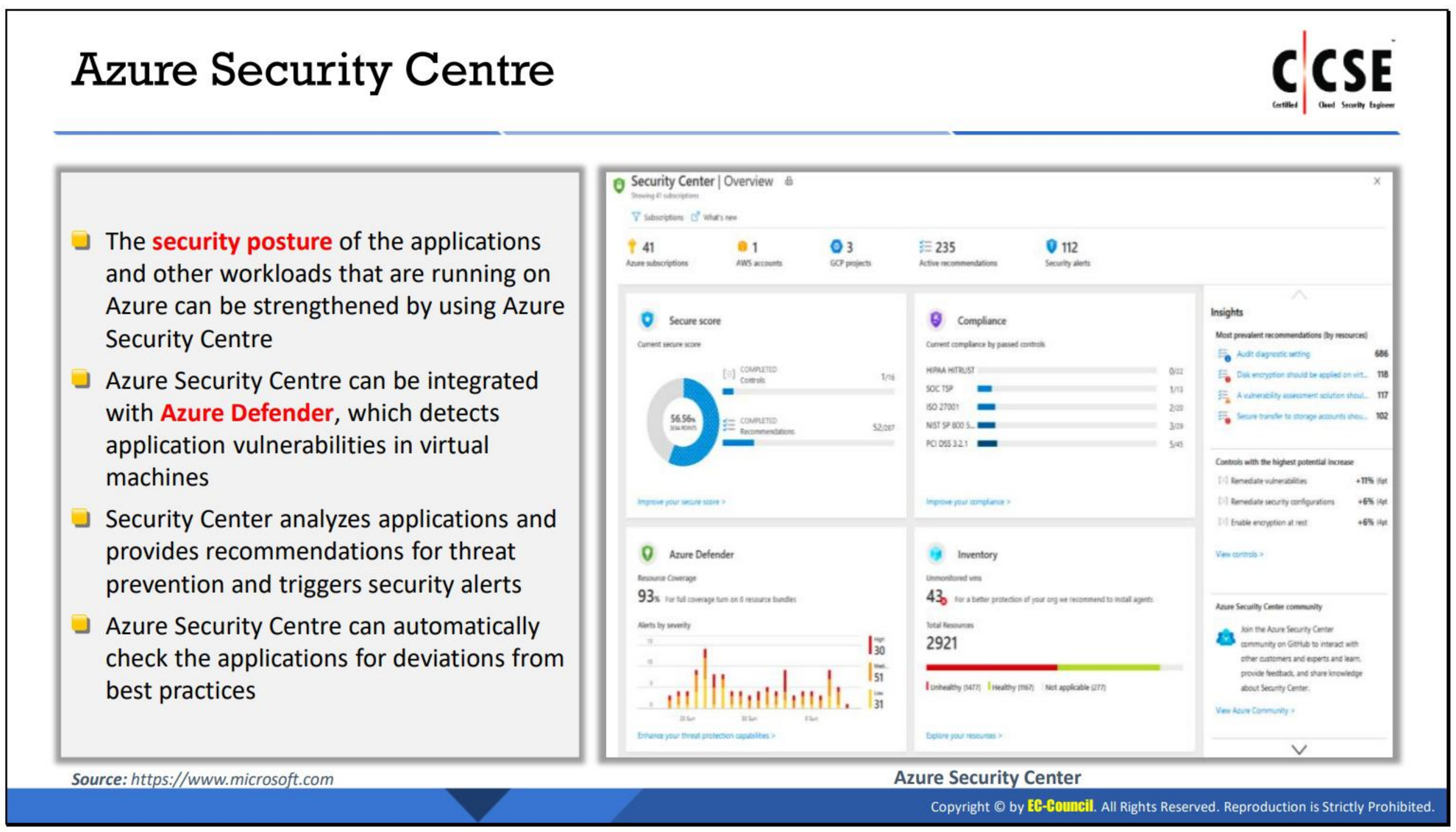


FIGURE 3.132: Settings

- The VNet is protected under the DDoS protection plan from DDoS attacks after saving the configuration.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Azure Security Centre

Azure Security Center (ASC) is a security management system that helps in securing the data center and offers advanced threat protection to workloads/applications in the cloud and on-premises. It detects security vulnerabilities by constantly analyzing the security state of all Azure resources and provides recommendations to fix those vulnerabilities. The security posture of the applications and other workloads that are running on Azure can be strengthened by using Azure Security Centre. Applications are analyzed and recommendations are provided for threat prevention and security alerts.

ASC is integrated with Azure services. For example, use Azure Defender that is integrated with ASC to secure hybrid cloud applications. The administrator can utilize it to enforce security policies across applications, get security alerts and security recommendations about the environment, reduce the threat exposure, and identify and respond to cyberattacks. ASC can automatically check applications for deviations from best practices.

Steps to use Azure Defender that is integrated with ASC are as follows:

Enable Azure Defender and install the Log Analytics agent on machines to monitor security vulnerabilities.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Source: https://www.microsoft.com

- **Enable ASC on your subscription:**
  - Log in to the Azure portal and choose **Security Center** from the menu.

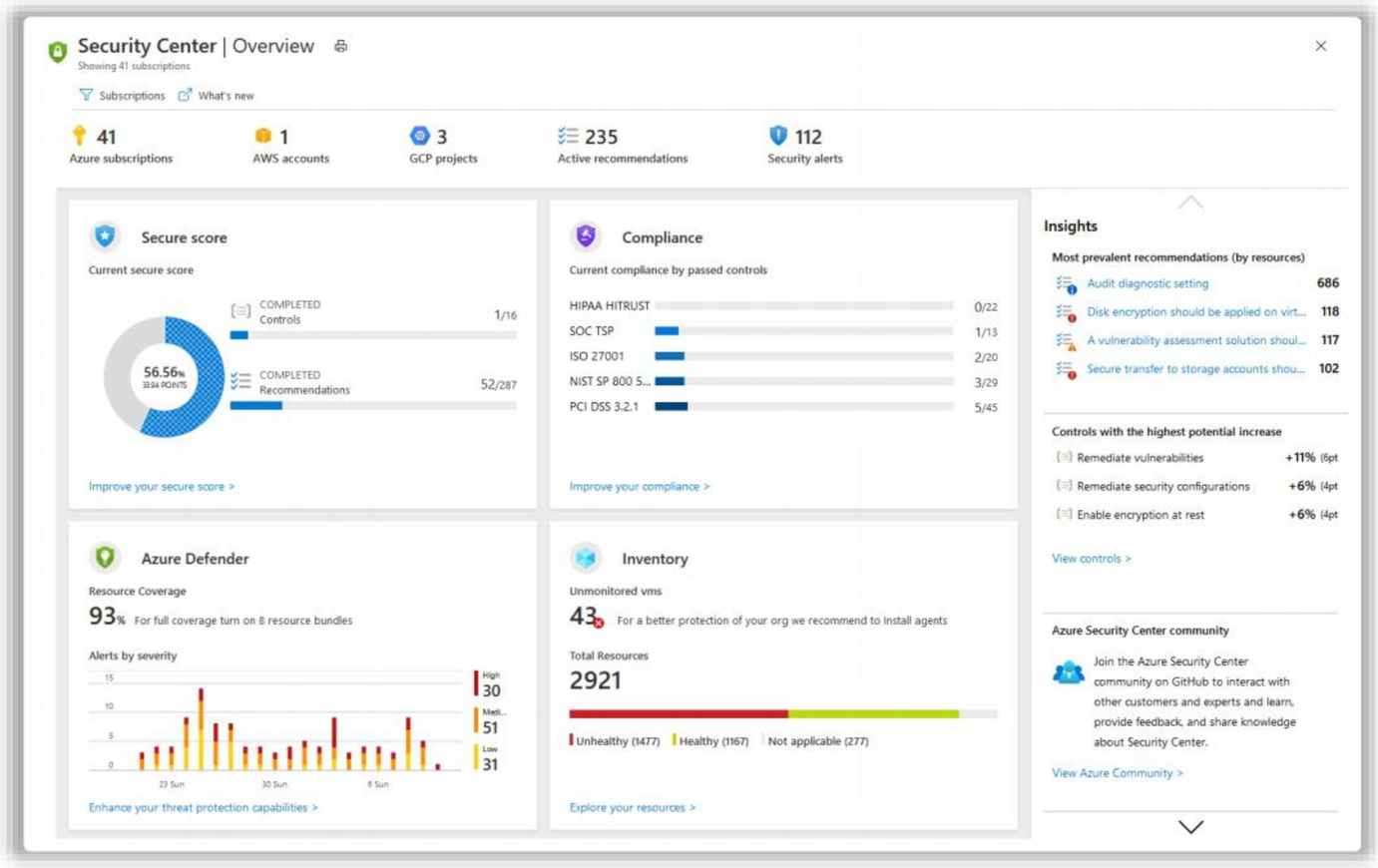


FIGURE 3.133: Security Center

Security Center | Overview offers recommendations and shows security posture of each resource along with the resource inventory. It allows to detect and mitigate risks by displaying the security posture of applications.

Customer security recommendations across all workloads are reviewed by the ASC. It determines how critical each recommendation is by applying advanced algorithms and then calculates the Secure Score based on them. The Secure Score helps customers to assess or evaluate their workload/application security posture. Customers can access it from their dashboard.

- **Enable Azure Defender:**
  - Choose **Getting started** on the **Security Center's sidebar**. Choose the **Upgrade** tab that shows all workspaces and subscriptions that can be on-boarded.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

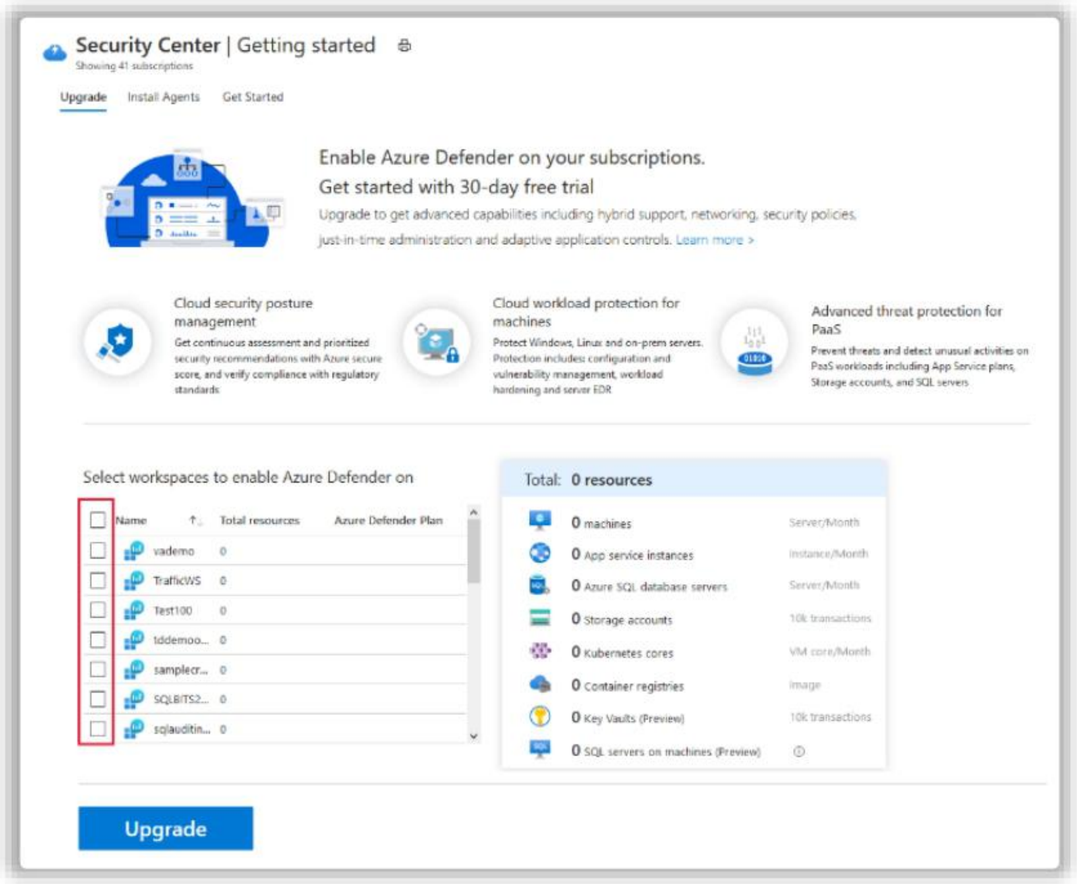


FIGURE 3.134: Security Center

- Choose the workspaces that are to be upgraded under **Select workspace to enable Azure Defender on**.
- Click on **Upgrade** for enabling Azure Defender.

- **Enable automatic data collection:** Log Analytics agents are installed on all supported machines by ASC when auto-provisioning is enabled. Through Log Analytics agents, data is collected from machines by ASC to monitor for threats and vulnerabilities. To enable auto-provisioning of the Log Analytics agent on machines, follow these steps:
  - Choose **Pricing & settings** from the ASC's menu.
  - Choose the relevant subscription.
  - Enable auto-provisioning by setting **Auto provisioning** to **On** in the **Data collection** page and click on **Save**.

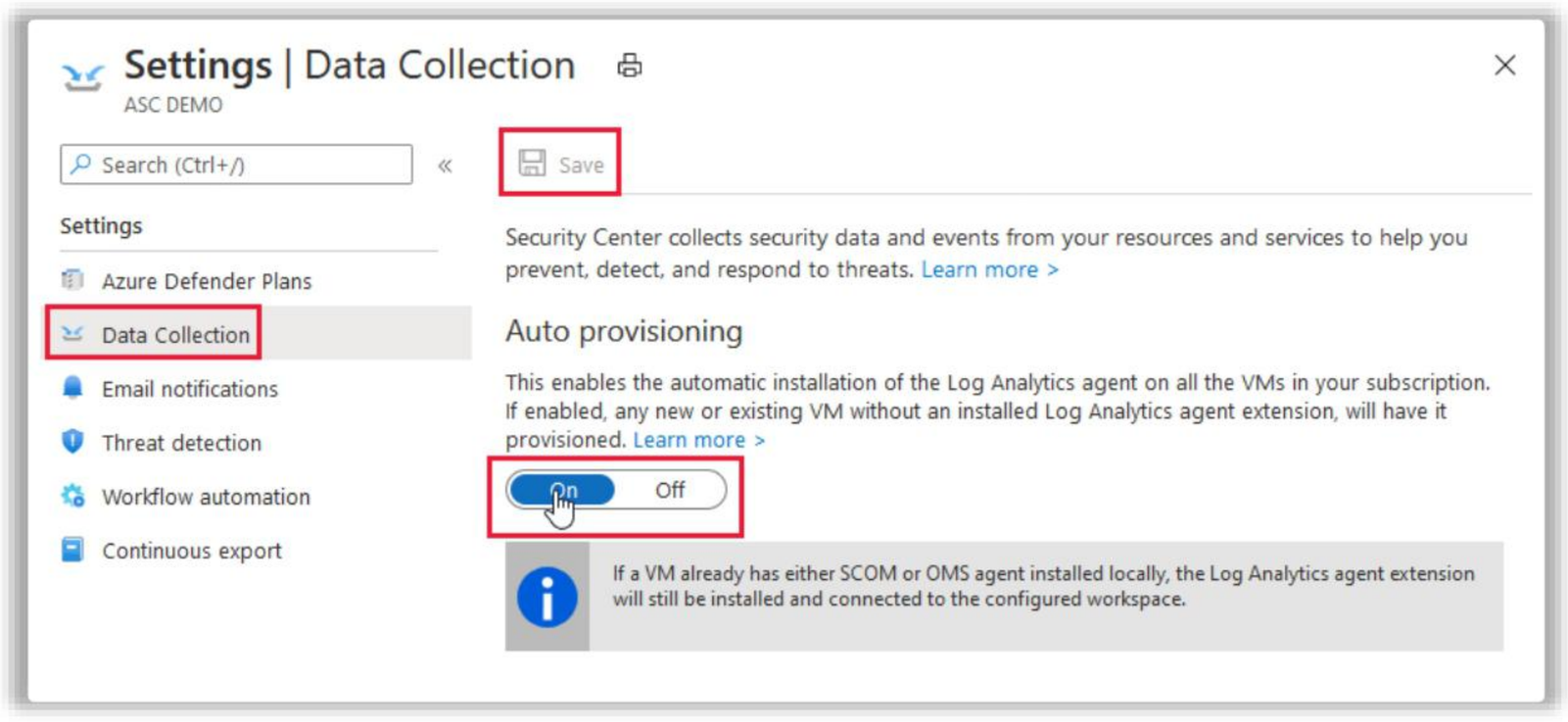
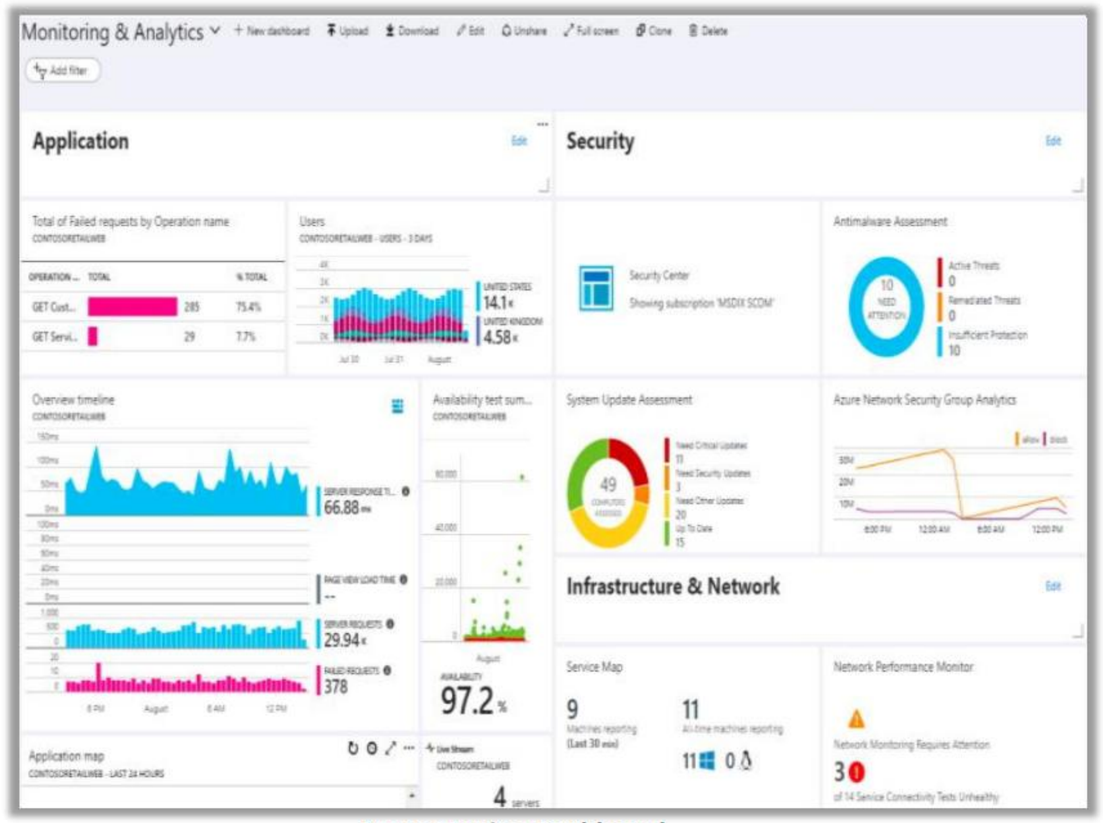


FIGURE 3.135:Auto Provisioning

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Azure Monitor

- The performance and availability of the applications can be maximized and the problems within applications can be identified proactively with Azure Monitor
- Azure Monitor provides data on **performance** and functionality of the application code
- It is a combined solution to collect analyse and act on **telemetry data**
- Azure Monitor also collects **Azure Automation** and **Azure Security Centre data**
- The data can be analysed, alerts can be setup, and an **end-to-end view** of the application can be viewed with Azure Monitor



Azure Monitor Dashboard

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

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

Azure Monitor

Azure Monitor maximizes the performance and availability of applications and services by collecting and analyzing performance metrics and activity and diagnostics logs from the cloud environment. It is a combined solution to collect, analyze, and act on telemetry data. It enables cloud administrators to understand the performance of applications and proactively detect issues that affect the apps and resources on which they depend. The data can be analyzed, alerts can be set up, and an end-to-end view of the application can be viewed with Azure Monitor. Azure Monitor provides data about the performance and functionality of the application code. Azure Monitor also collects Azure Automation and Azure Security Centre data.

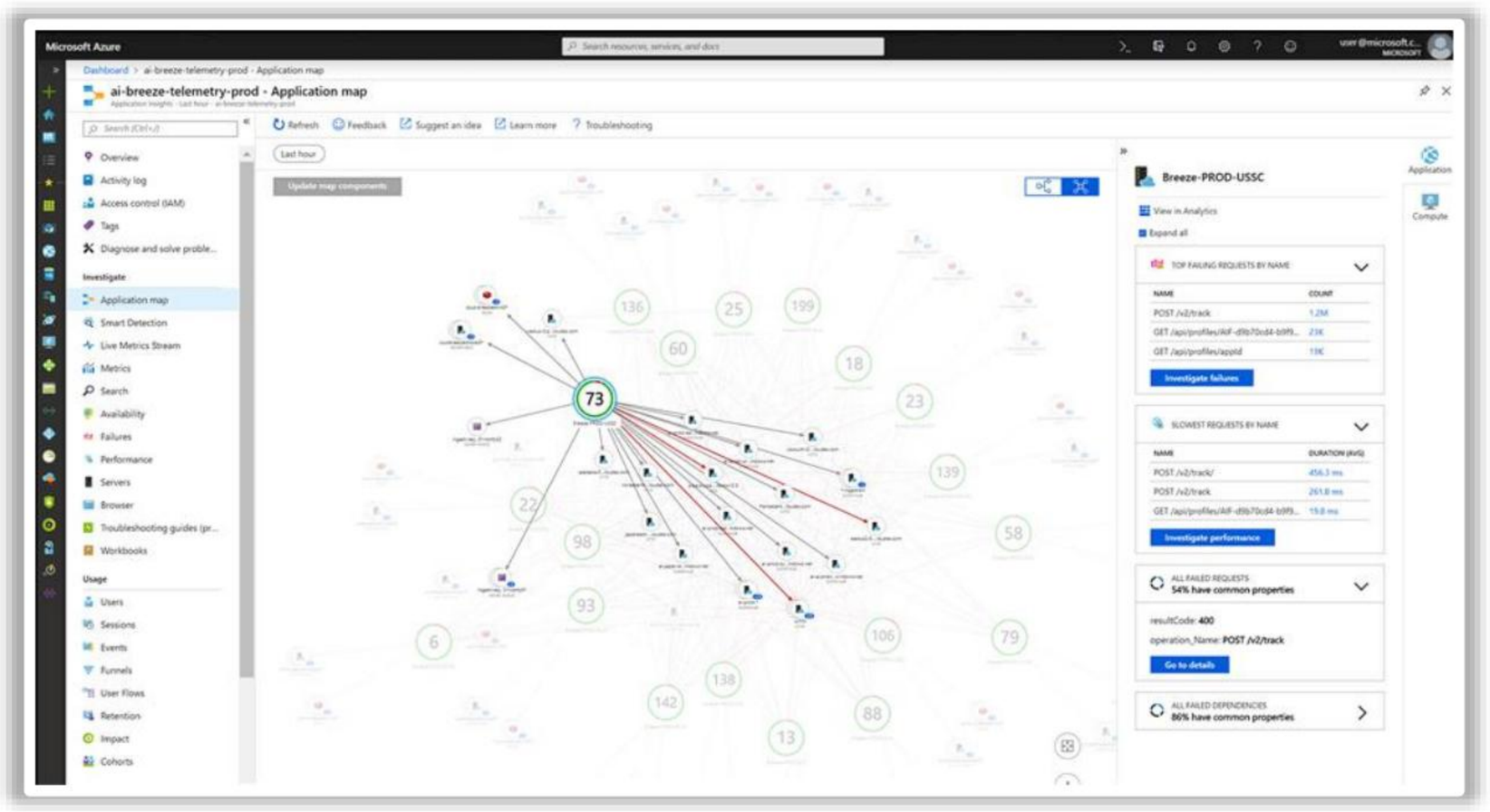


FIGURE 3.136: Monitor Applications

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Source: https://www.microsoft.com

How Does Azure Monitor Work?

Azure Monitor receives telemetry data from multiple sources, including both Azure and on-premises sources. It also receives log data from management tools such as those available in Azure automation and ASC. It stores this telemetry data into a log data store. This data is then used by Azure Monitor to perform various actions such as visualizing and analyzing data, responding to threats, and integrating with other tools to stream log data to external systems.

Key Features

The key features provided by Azure Monitor include the following.

- **Application Insights:** Use this feature of Azure Monitor to monitor the performance, availability and usage of applications hosted on Azure or on-premises. It provides deep insights into the operations of applications by using the powerful data analysis platform of Azure Monitor. Use Application Insights to identify errors and flaws in application performance before they are found by users.



FIGURE 3.137: Application Insights' deep insights into application's operations

- **Alerts:** Azure Monitor proactively sends alerts to notify cloud administrators about critical conditions and tries to take corrective actions. Alert rules based on metrics provide near real-time alerts and alert rules based on logs provide complex logic across data received from multiple data sources, including applications.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

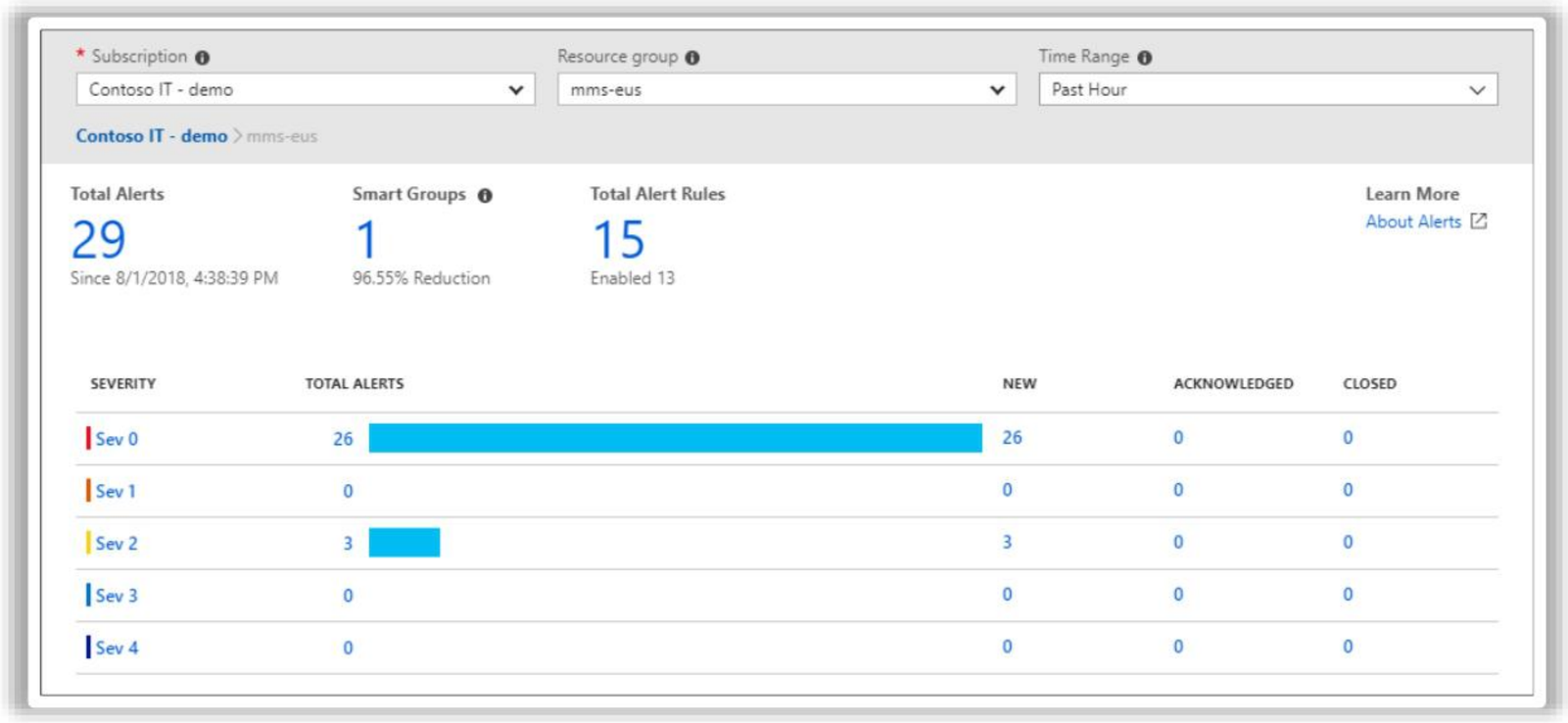


FIGURE 3.138: Alerts

Alert rules utilize action groups in Azure Monitor. These groups have unique sets of actions and recipients that can be shared across several rules. Action groups can perform actions, such as using webhooks to make alerts begin external actions, based on requirements.

- **Visualizing monitoring data:** Azure Monitor leverages charts and tables to summarize monitoring data to be effectively presented to various audiences. It uses its features to visualize monitoring data. However, Azure Monitor uses other Azure services for publishing that data to different audiences.
- **Dashboards:** In the Azure portal, Azure dashboards present different types of data into a single pane. Azure dashboard can be shared with other Azure users. Add the output of a metrics chart or log query to the dashboard. For example, a cloud administrator can combine different tiles on an Azure dashboard that display a table of activity logs, a graph of metrics, the output of any log query, and a chart from Application Insights.

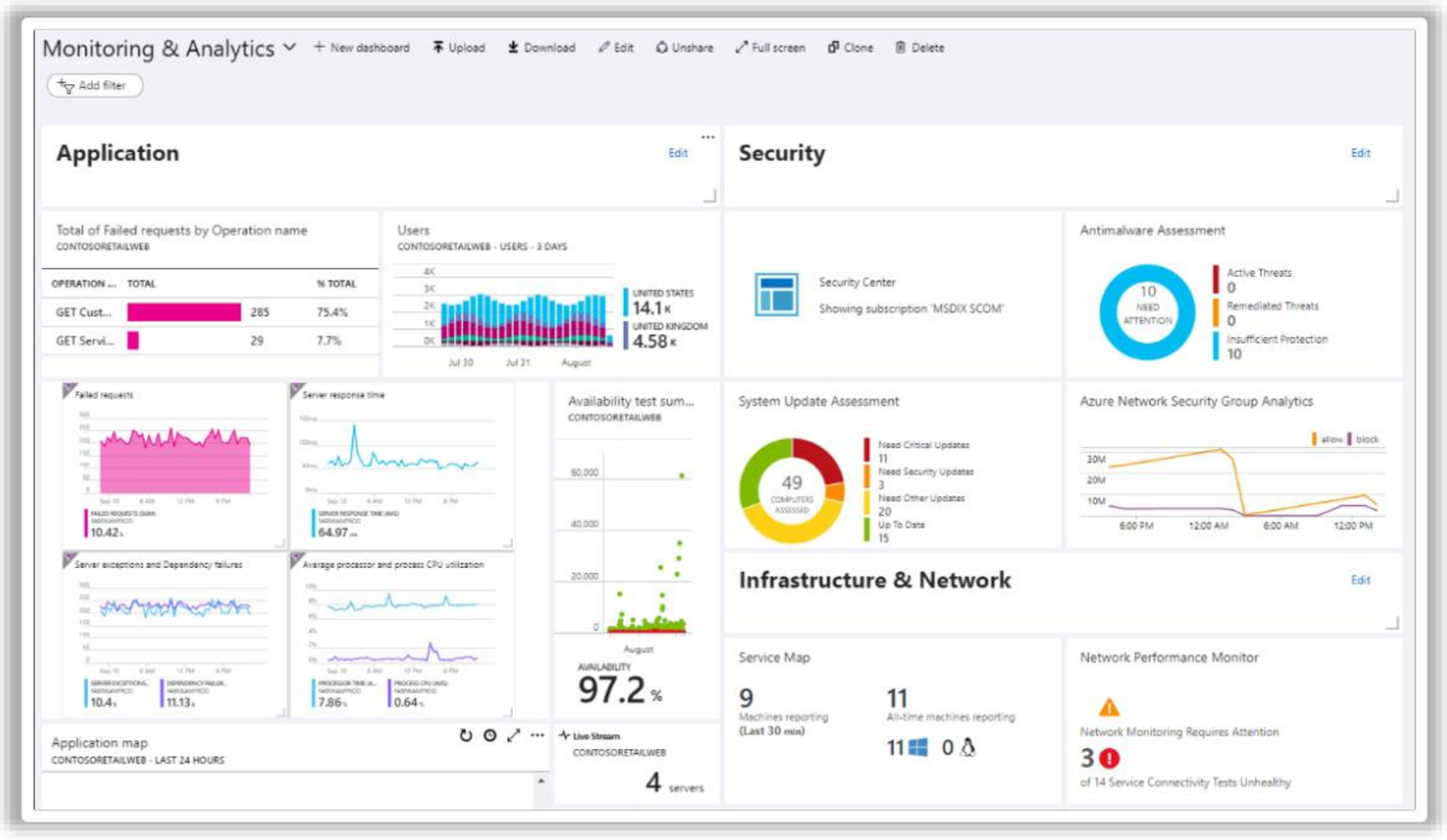
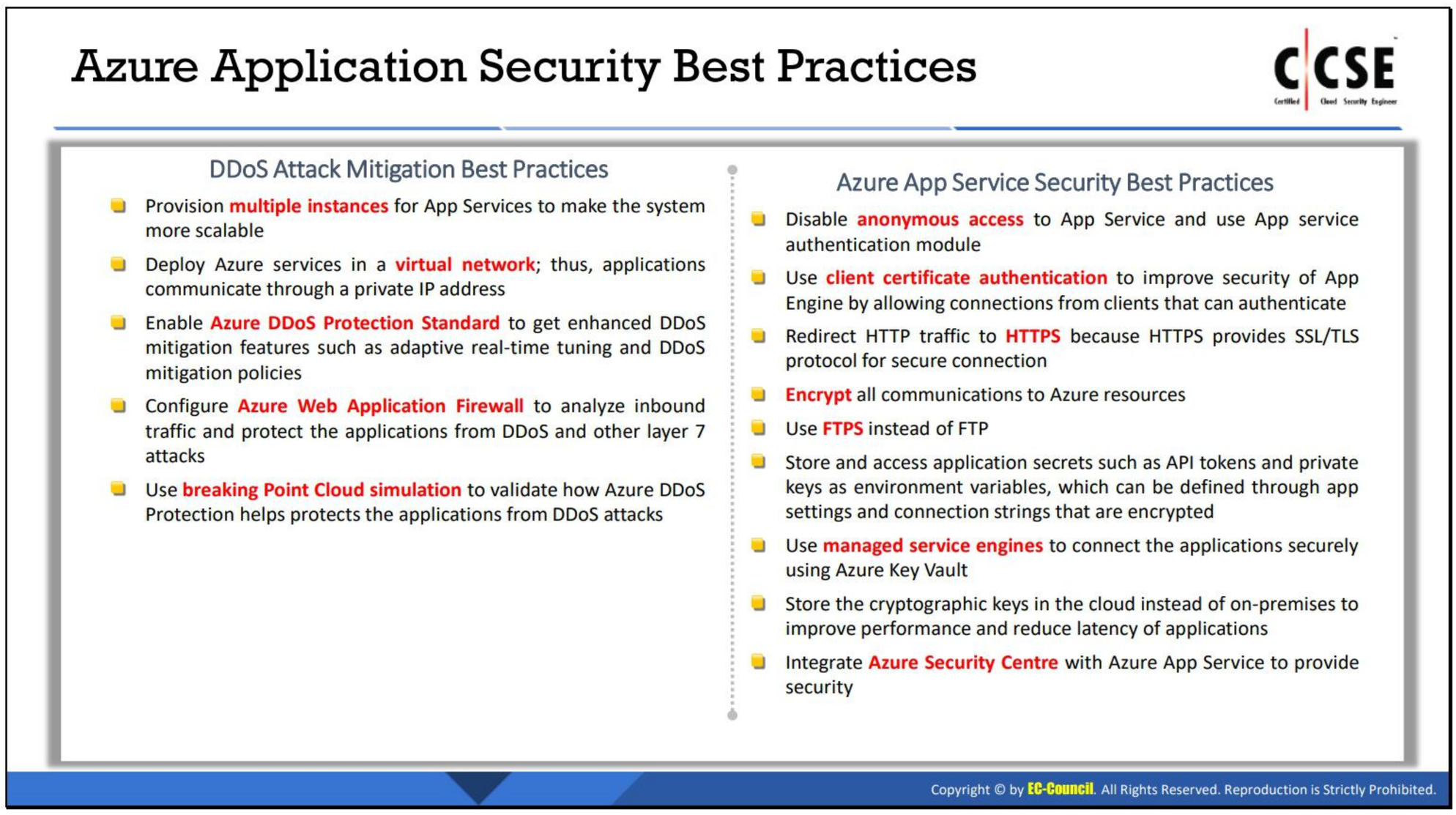
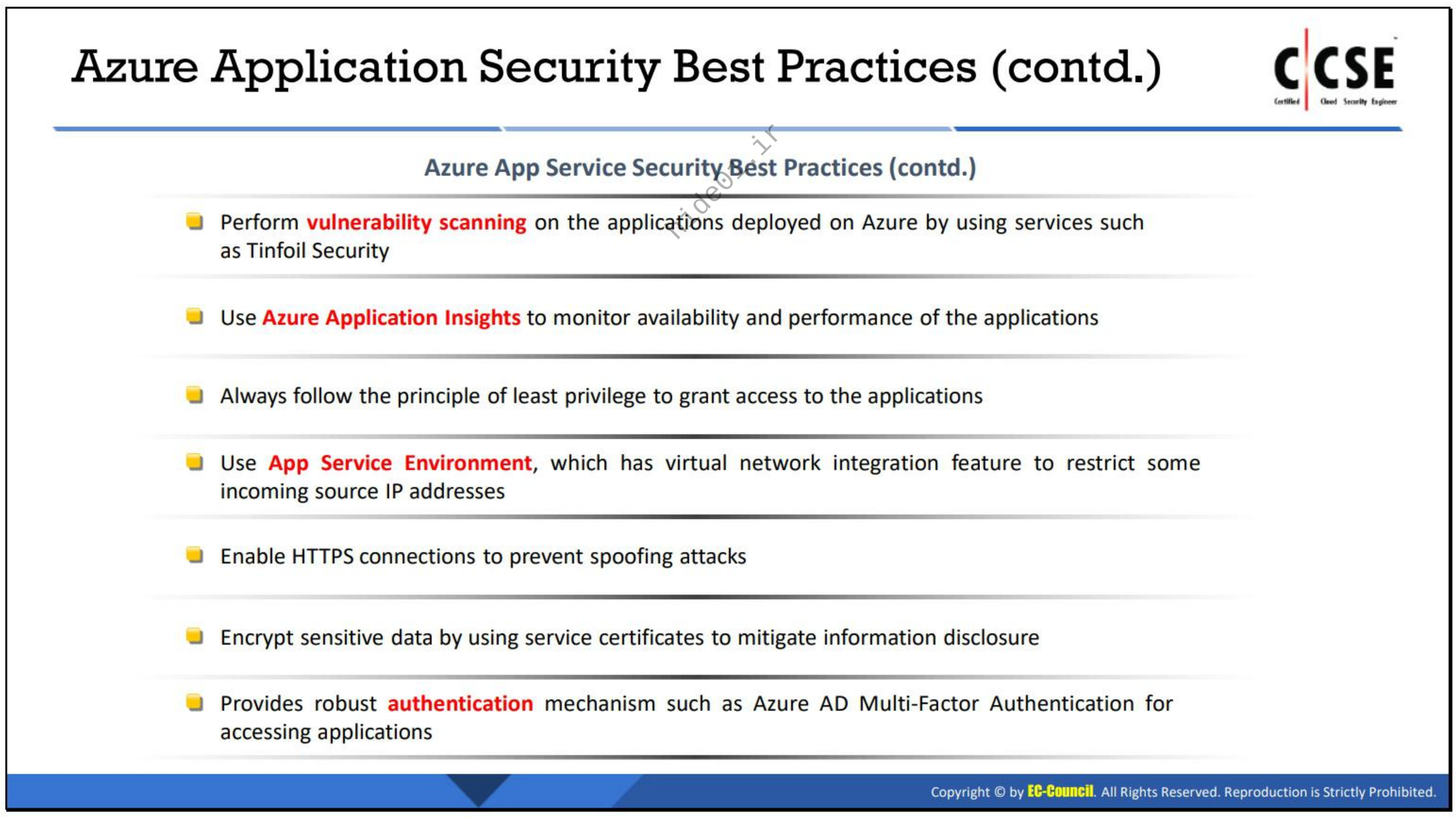


FIGURE 3.139: Dashboard

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Azure Application Security Best Practices

Azure provides best practices for its customers to adopt and apply to securing enterprise applications. They are described below.

DDoS Attack Mitigation Best Practices

- Provision multiple instances for App Services to make the system more scalable.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Deploy applications in a virtual network so that the applications can communicate through a private IP address.
- Implement enhanced DDoS mitigation features of Azure DDoS Protection Standard such as adaptive real-time tuning and DDoS mitigation policies.
- Configure Azure Web Application Firewall to analyze inbound traffic and protect the applications from DDoS and other layer 7 attacks.
- Enable DDoS Protection Standard on WAF Virtual Network to protect from volumetric and protocol attacks.
- Use Breaking Point Cloud simulation to validate how Azure DDoS Protection protects the applications from DDoS attacks.
- DDoS Protection Service starts DDoS mitigation only if metric value Policy to Trigger DDoS Mitigation is lower than the traffic on protected public application.

Azure App Service Security Best Practices

- Disable anonymous access to App Service and also use the app service authentication module.
- Use the client certificate authentication to improve App Engine's security by allowing connections from clients that can authenticate.
- Redirect HTTP to HTTPS because HTTPS provides SSL/TLS protocol for secure connection.
- Encrypt all communications to Azure resources.
- Use FTPS instead of FTP.
- Access the application secrets such as API tokens, private keys as environment variables. Define these variables through app settings and connection strings.
- Integrate Azure Security Centre with the Azure App Service to run assessments and provide security recommendations.

Storing of Application Secrets Best Practices

- Use Azure Key Vault to store application secrets, keys, and certificates securely.
- Use Key Vault to retrieve the secrets.
- Use Managed Service Engines to connect applications securely to Azure Key Vault.
- Instead of storing the cryptographic keys on-premises, store them in the cloud to improve performance and reduce the latency of applications.

Mitigation of SQL Injection and XSS Attacks Best Practices

- Implement a WAF to prevent SQL Injection and XSS attacks.
- Enable Azure Front Door's WAF feature because it acts as a gateway to applications and filters traffic, and set routing rules.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

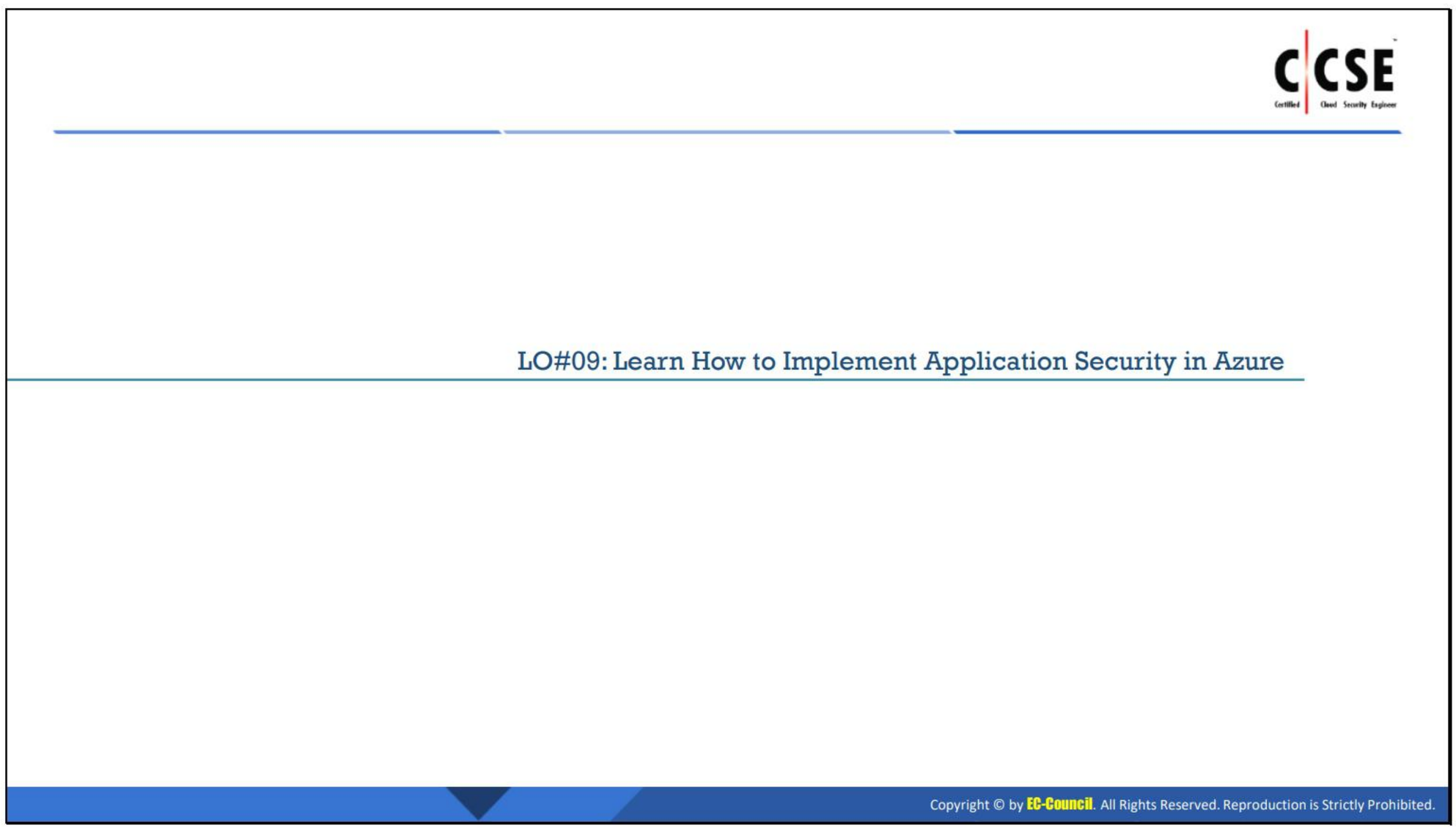
- Enable Azure Application Gateway's WAF feature to protect against OWASP vulnerabilities.
- Set up WAF rules to restrict IP addresses that are allowed to access web applications.

Other Best Practices

- Perform vulnerability scanning on the applications deployed on Azure by using services such as Tinfoil Security.
- Use Azure Application Insights to monitor the availability and performance of the applications.
- Follow the principle of least privilege to grant access to the applications.
- Restrict some incoming source IP addresses using the virtual network integration feature of App Service Environment.
- Prevent spoofing attacks by enabling HTTPS connections.
- Mitigate information disclosure by encrypting the sensitive data by using service certificates.
- Enforce Azure AD MFA for a strong authentication mechanism to access applications.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

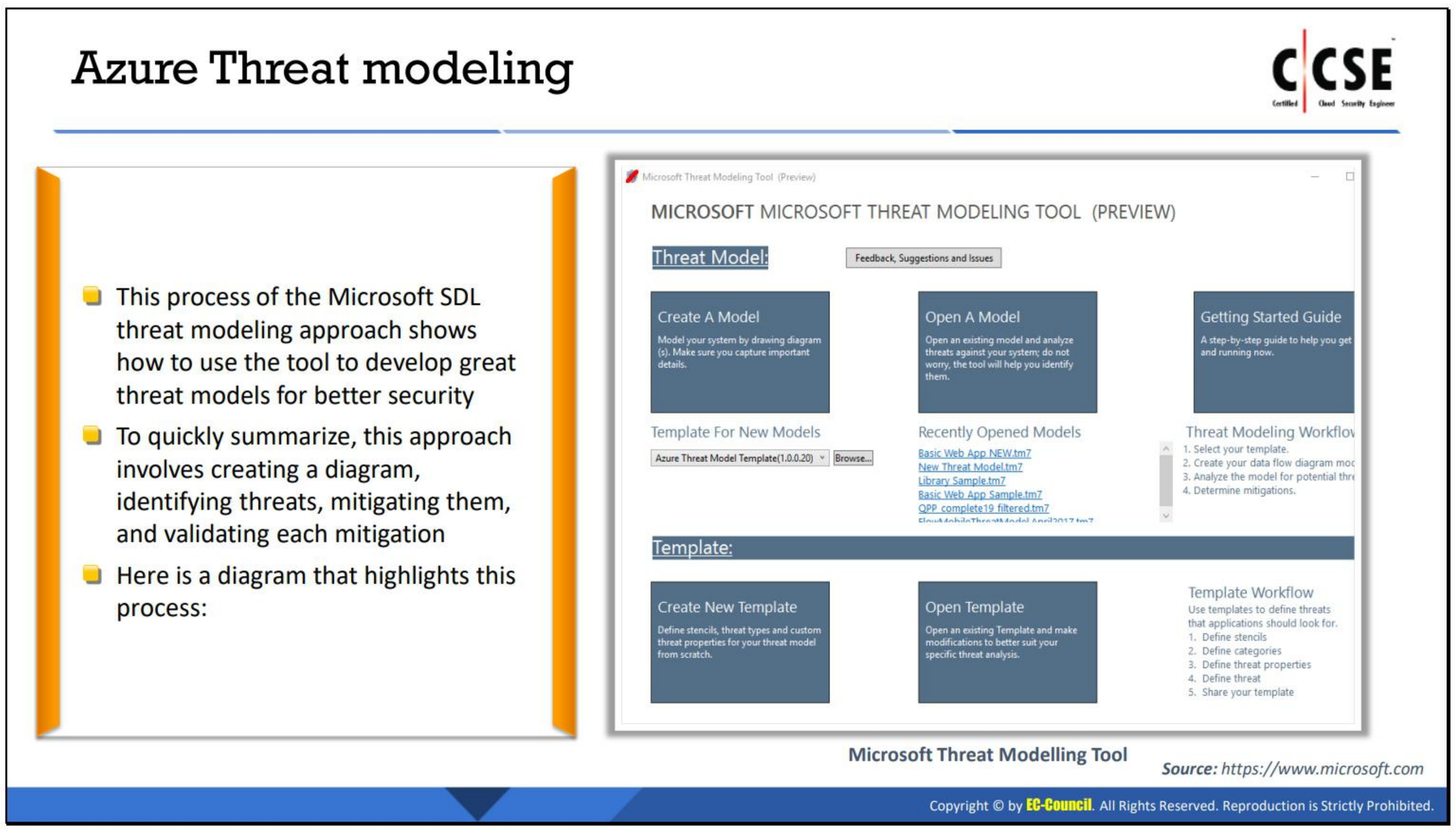


LO#09: Learn How to Implement Application Security in Azure

The objective of this section is to explain the implementation of application security in Azure using different Azure products and services. It also describes the various Azure services that provide advanced threat detection functionalities.

hidd01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Azure Threat Modeling

- This process of the Microsoft SDL threat modeling approach shows how to use the tool to develop great threat models for better security.
- This process of the Microsoft SDL threat modeling approach shows how to use the tool to develop great threat models for better security.
- Here is a diagram that highlights this process:

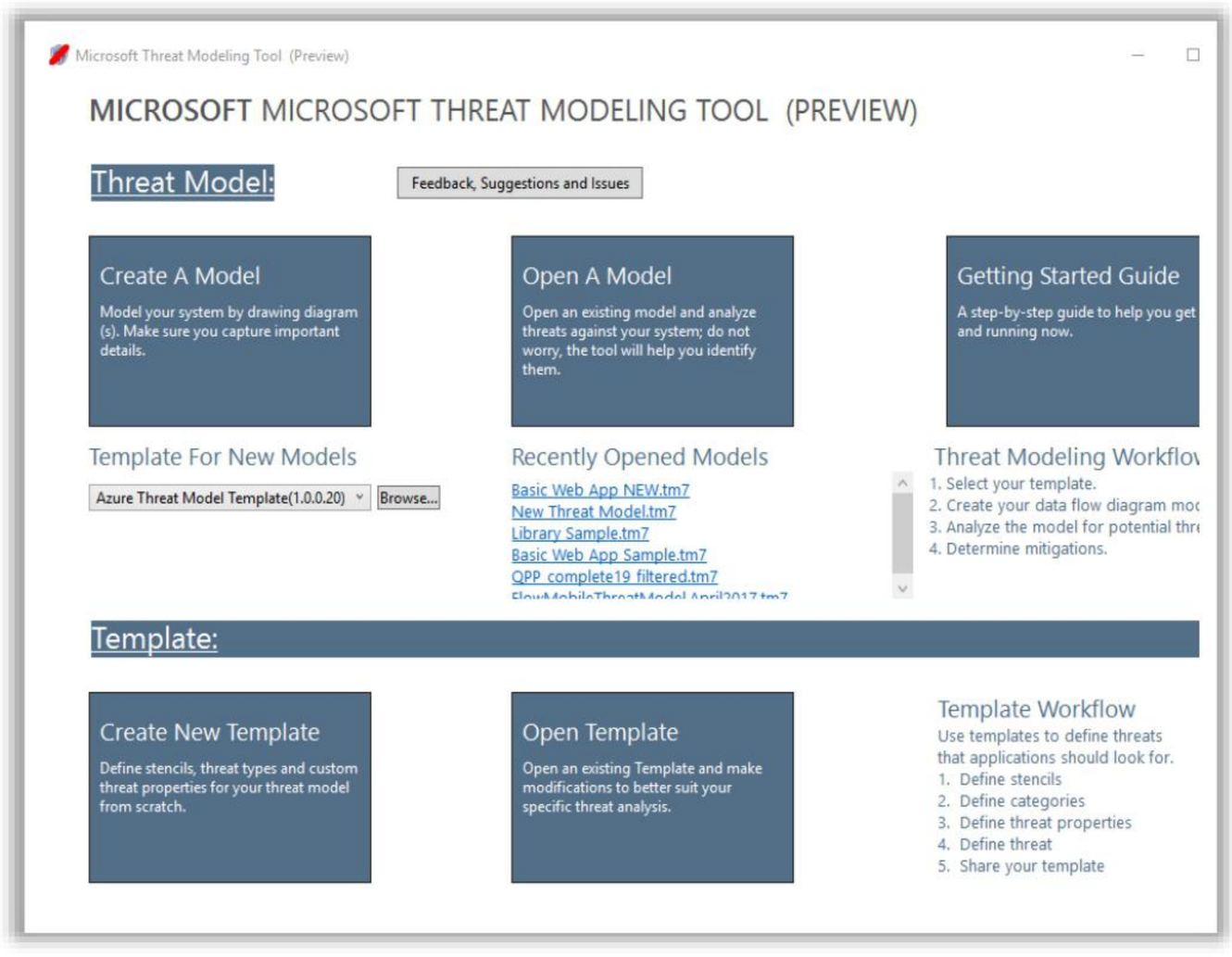
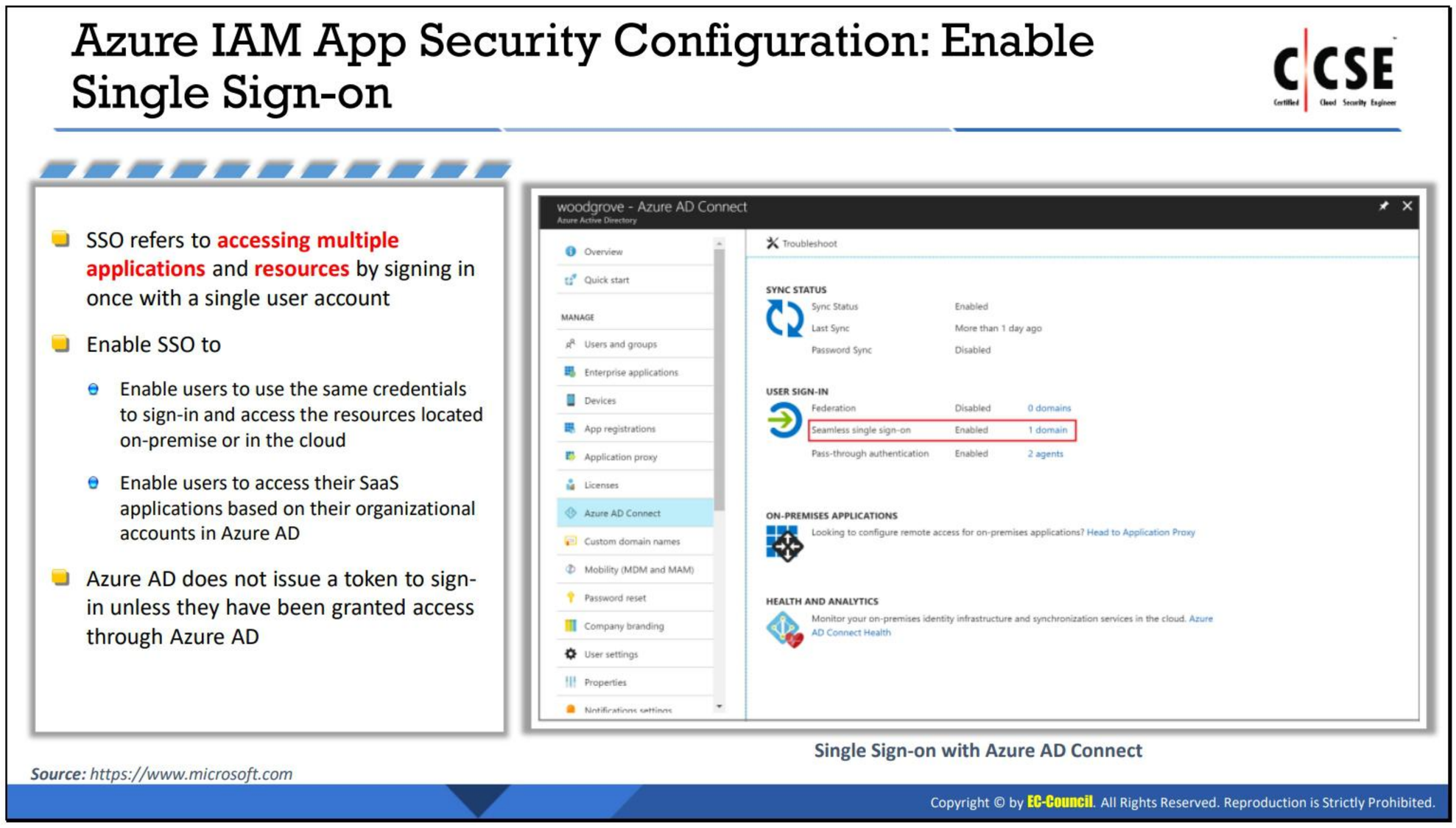


FIGURE 3.140: Microsoft Threat Modelling Tool

Source:https://www.microsoft.com

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Single Sign-on with Azure AD Connect

Azure IAM App Security Configuration: Enable Single-Sign-on

SSO refers to accessing multiple applications and resources by signing in once with a single user account. Azure AD Seamless SSO automatically signs-in corporate desktops users connected to a corporate network. Azure AD does not issue a token to sign-in unless they have been granted access through Azure AD. It allows users to access cloud-based applications easily.

- Implement SSO to provide security and convenience to users.
- Enable users to utilize the same credentials to sign-in and access the resources located on-premise or in the Azure cloud.
- Enable users to access SaaS applications based on the organization account in Azure AD.

Source: https:// www.microsoft.com

To enable SSO in Microsoft Azure, use the following steps:

- Go to **Azure AD Active Directory settings.**
- Click on **Azure AD connect.**
- Under **USER SIGN-IN**, enable **Seamless single sign-on.**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

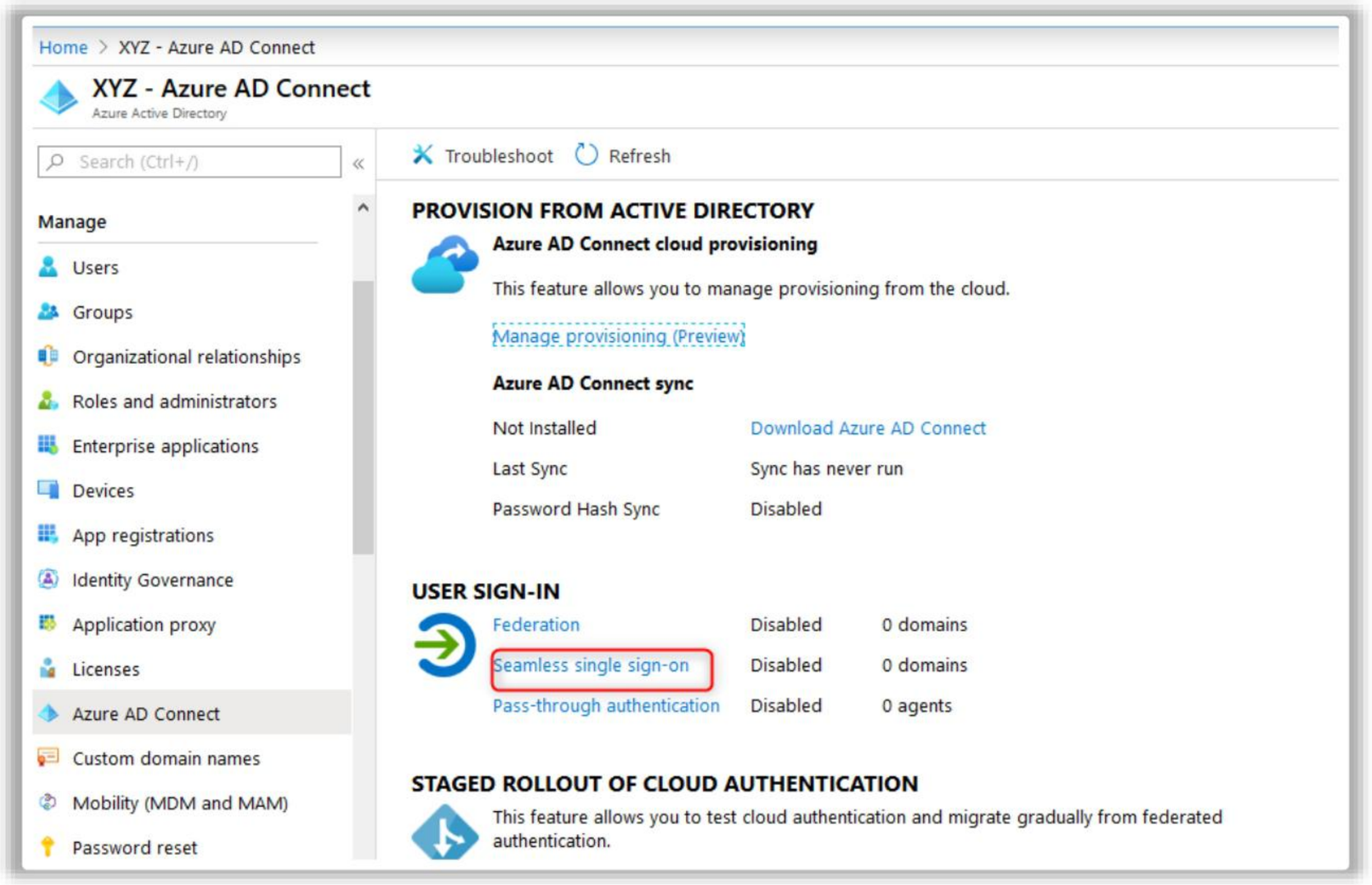
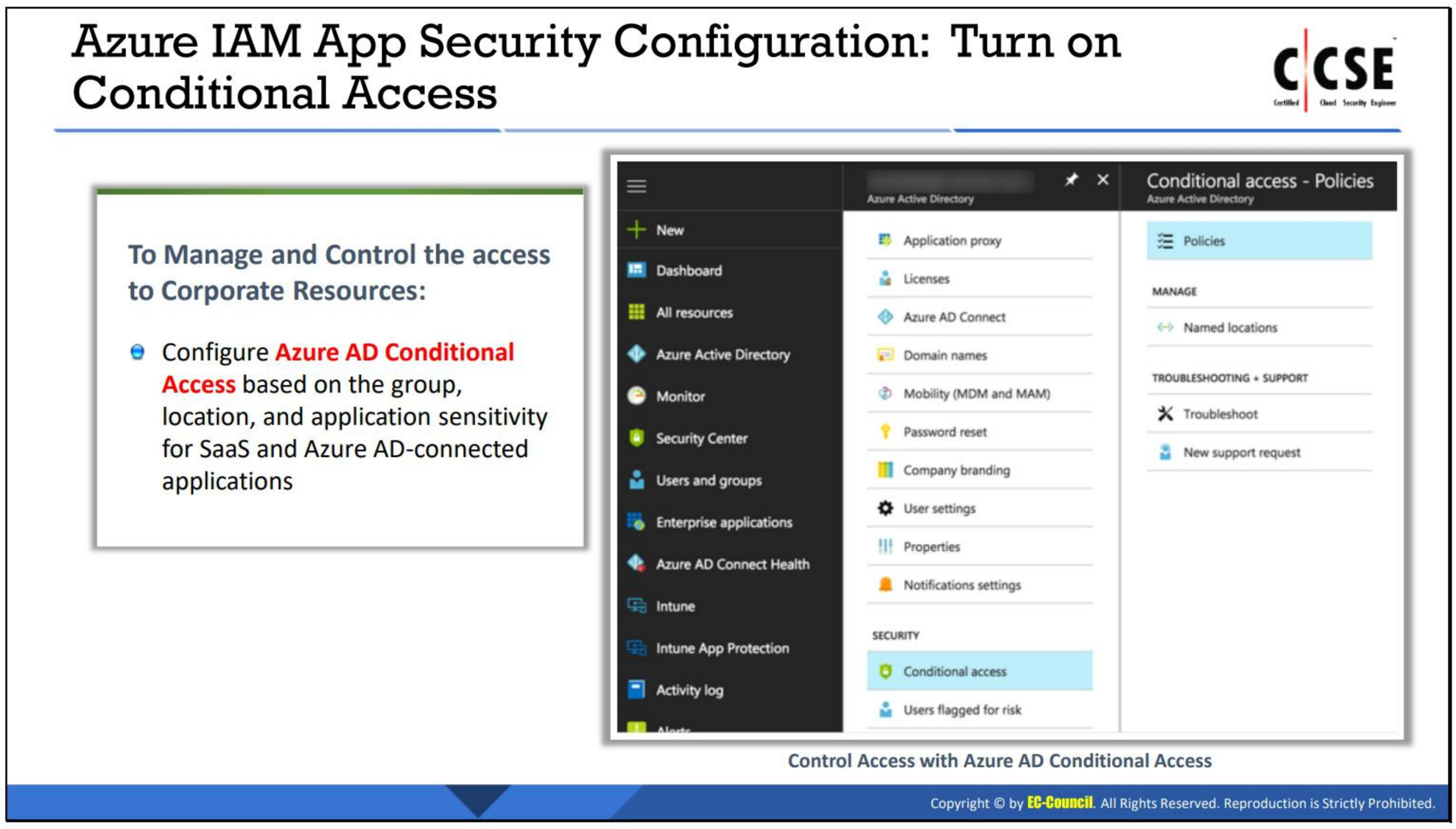


FIGURE 3.141:Azure AD Connect

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Azure IAM App Security Configuration: Turn on Conditional Access

Azure AD uses a tool called Conditional Access for enforcing organizational policies to manage and control access to corporate resources. The organizations use conditional access policies for security and right access control. These policies are implemented after the first factor's authentication.

Azure AD Conditional Access is configured based on the group, location, application sensitivity for SaaS apps, and Azure AD connected apps. These policies are prepared and implemented for on-premise and Azure cloud applications.

To enable Conditional Access in Microsoft Azure, use the following steps:

- Go to **Azure AD Active Directory settings** and click on **Security.**
- Under **Protect** section, click on **Conditional Access.**

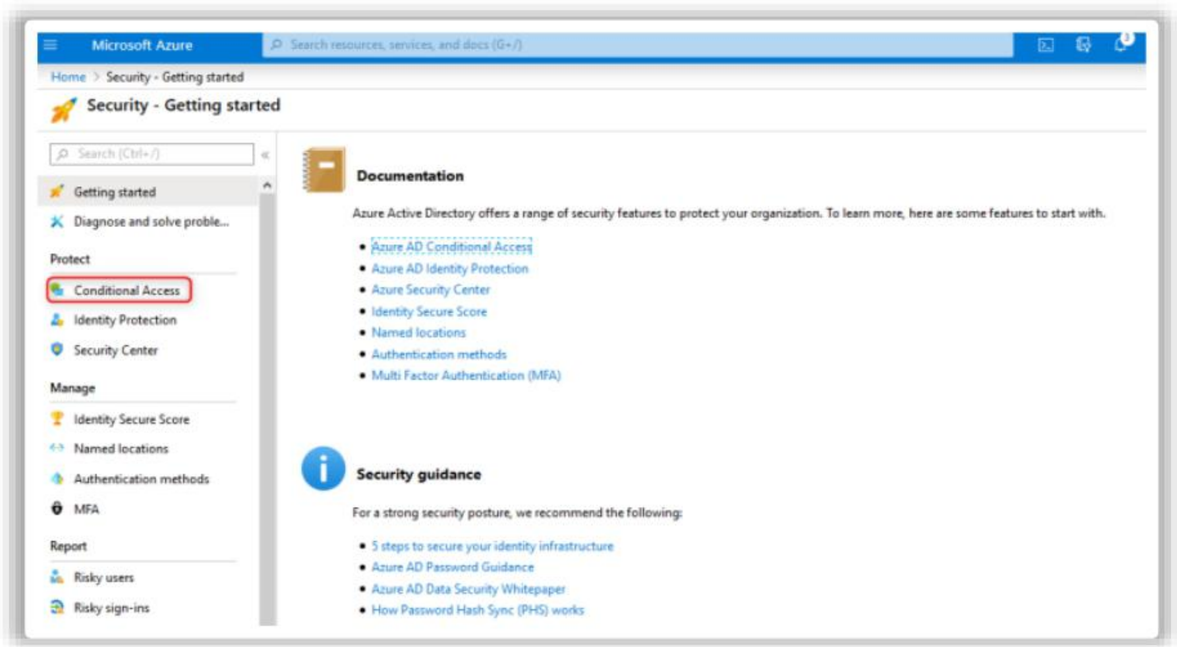


FIGURE 3.142: Conditional Security

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click on **Policies** and set the policy.

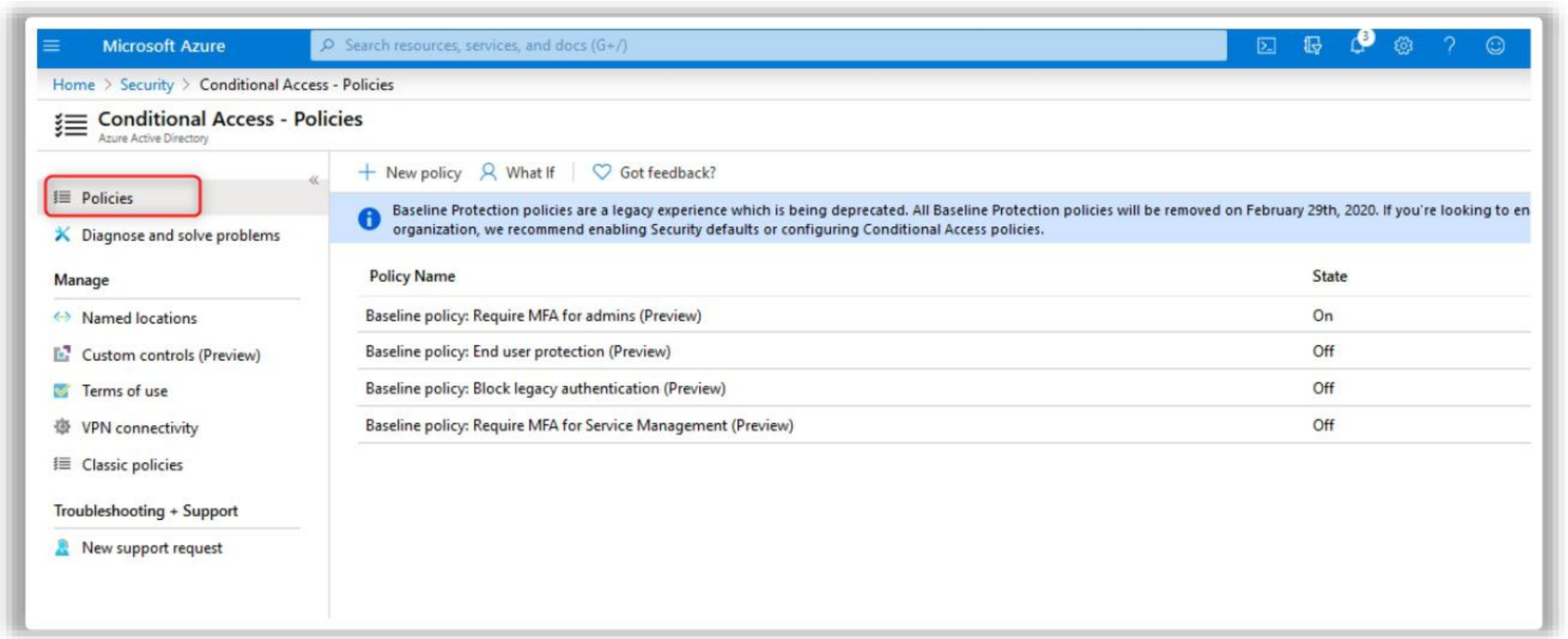
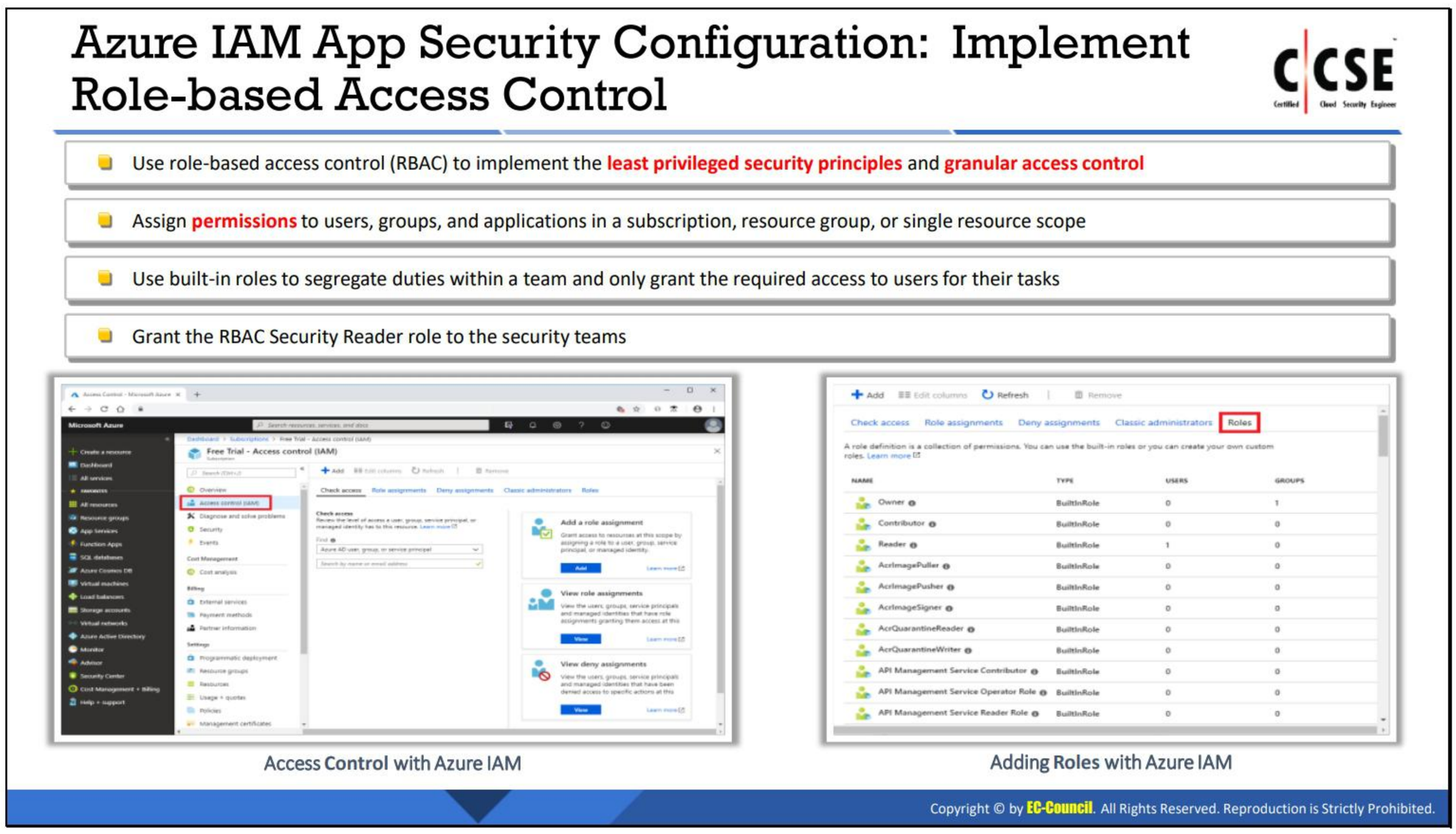


FIGURE 3.143: Policies

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Azure IAM App Security Configuration: Implement Role-based Access Control

ASC uses RBAC to assign various built-in roles to users, groups, and services to access the Azure resources. The assignment of roles helps in controlling access to resources. If the built-in roles do not meet the requirements of an organization, then the customer can create custom roles for the Azure resources.

- To implement the least-privilege security principles and granular access control, use RBAC.
- Assign permissions to users, groups, and applications on a subscription, resource group, or single resource scope.
- Use built-in roles to segregate duties within the team and only grant users the required access to their job.
- Grant the RBAC security reader role to security teams.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

To enable RBAC in Microsoft Azure, use the following steps:

- From the Microsoft Azure Portal, navigate to **All Services.**

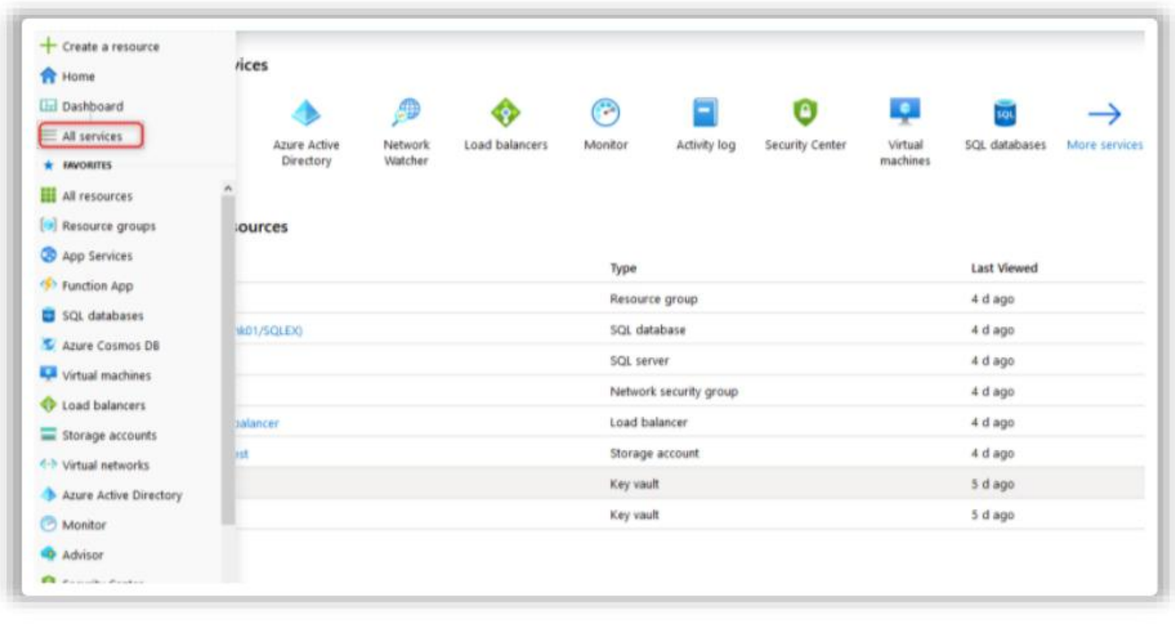


FIGURE 3.144:Microsoft Azure Portal

- Under the **Categories** section, navigate to **Storage** and select **Storage accounts.**

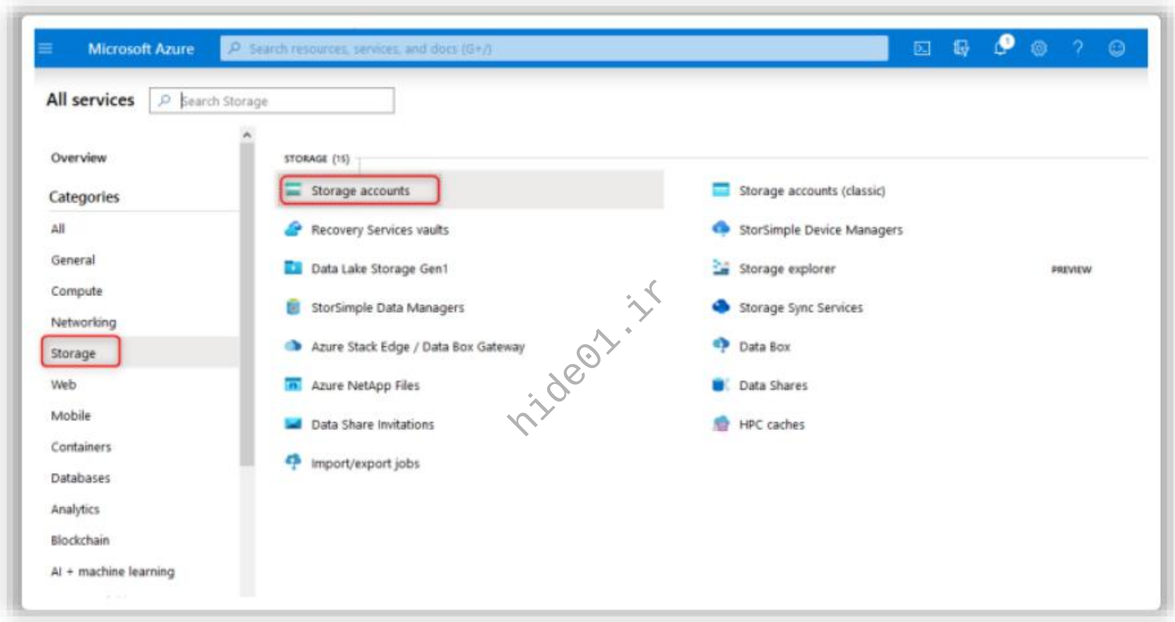


FIGURE 3.145: Select Storage Accounts

- Create a **Storage Account,** fill in the details, and click on **Review + create.**

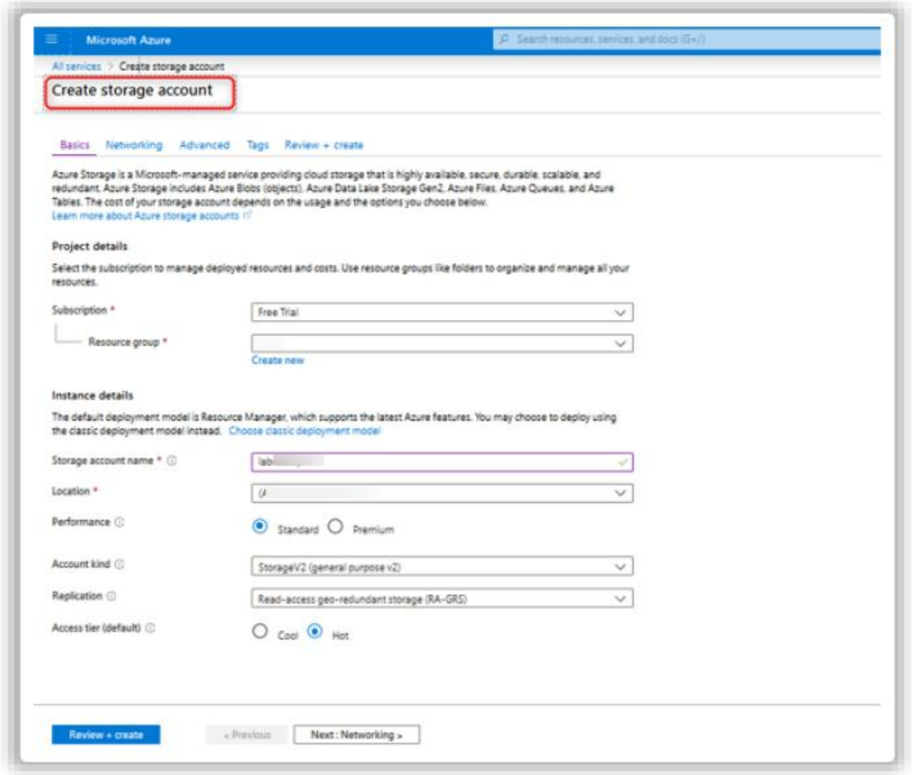


FIGURE 3.146: Create Storage Account

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- After deployment is completed, click on **Go to Resource.**

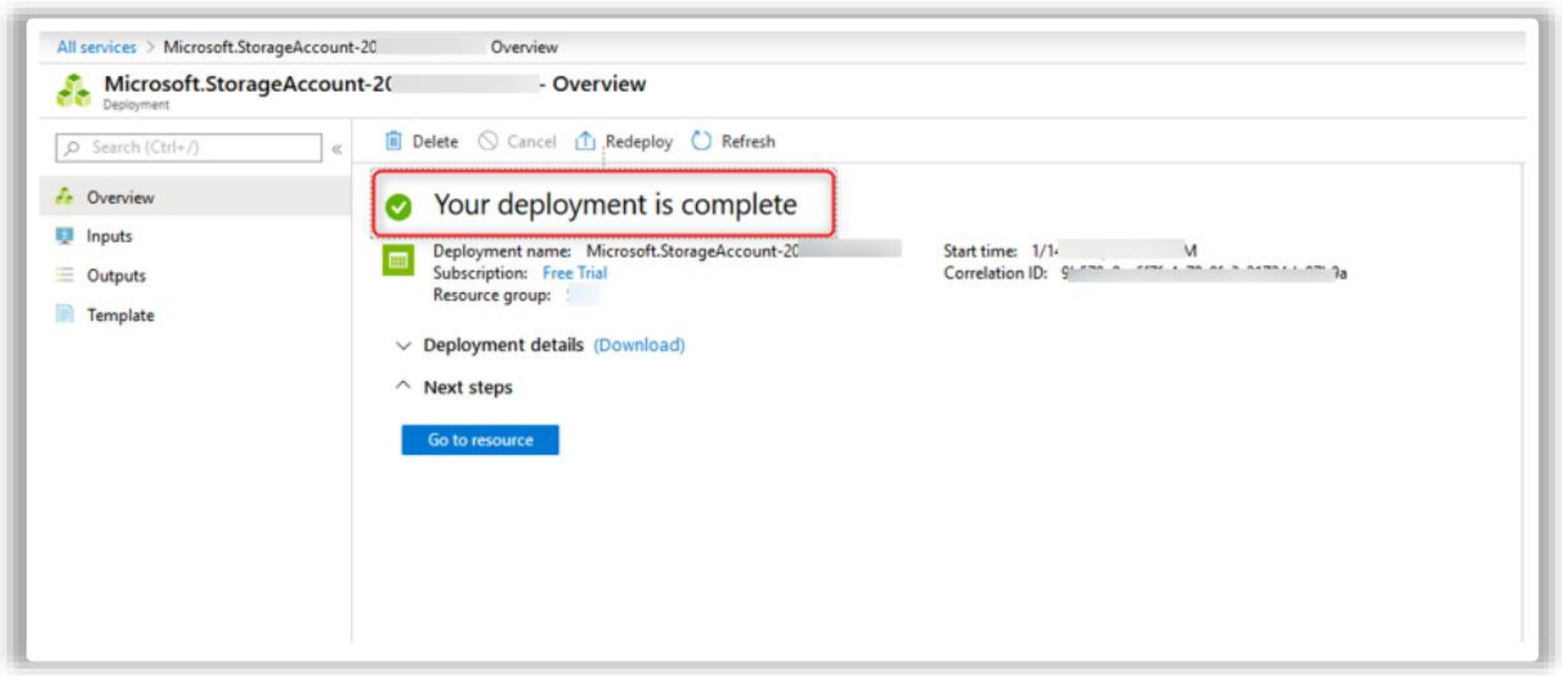


FIGURE 3.147: Deployment Complete

- Click **Access control (IAM)** and **Add a role assignment** by clicking on **Add.**

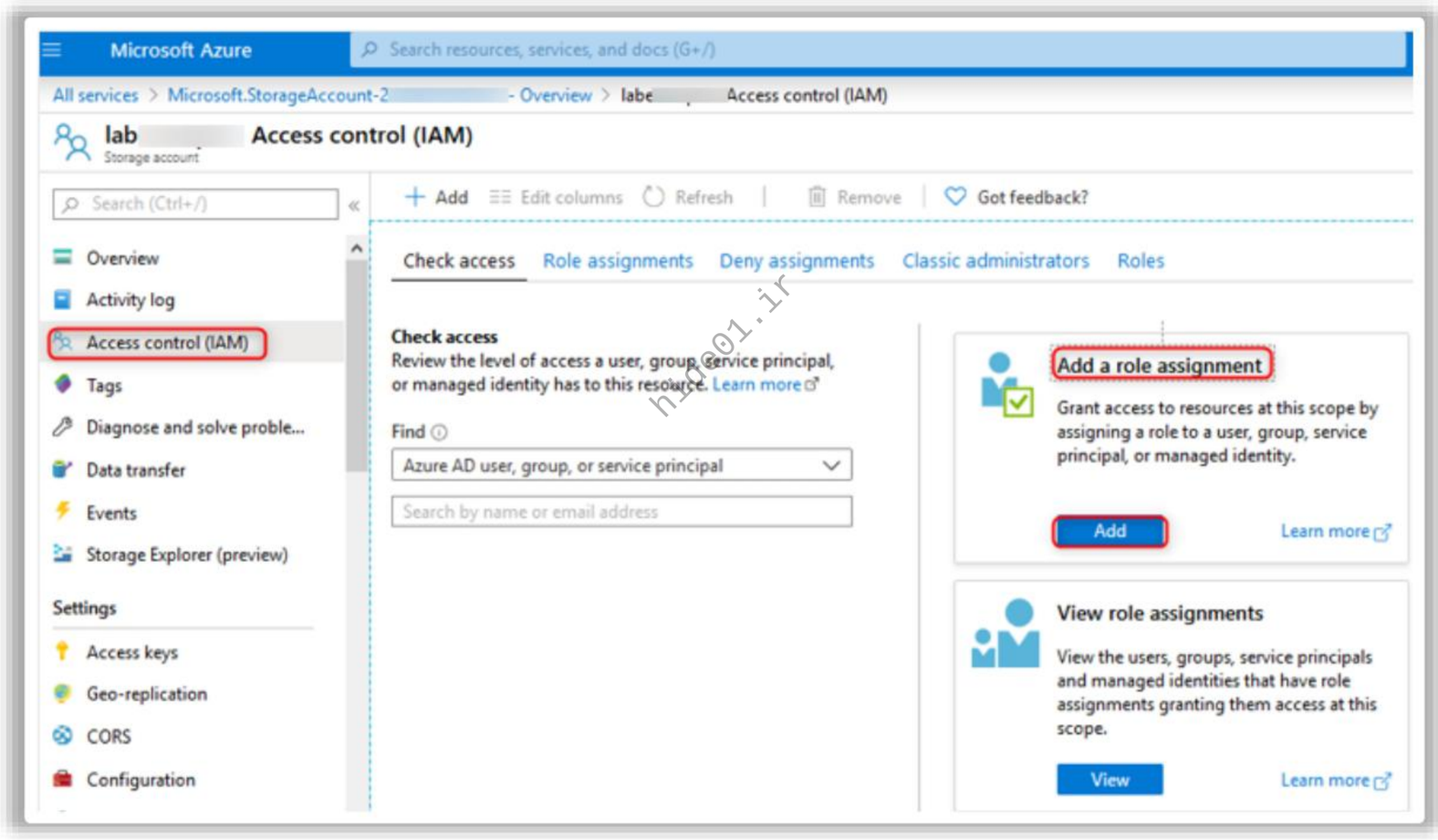


FIGURE 3.148: IAM

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enter the details in **Add role assignment** and **Save.**

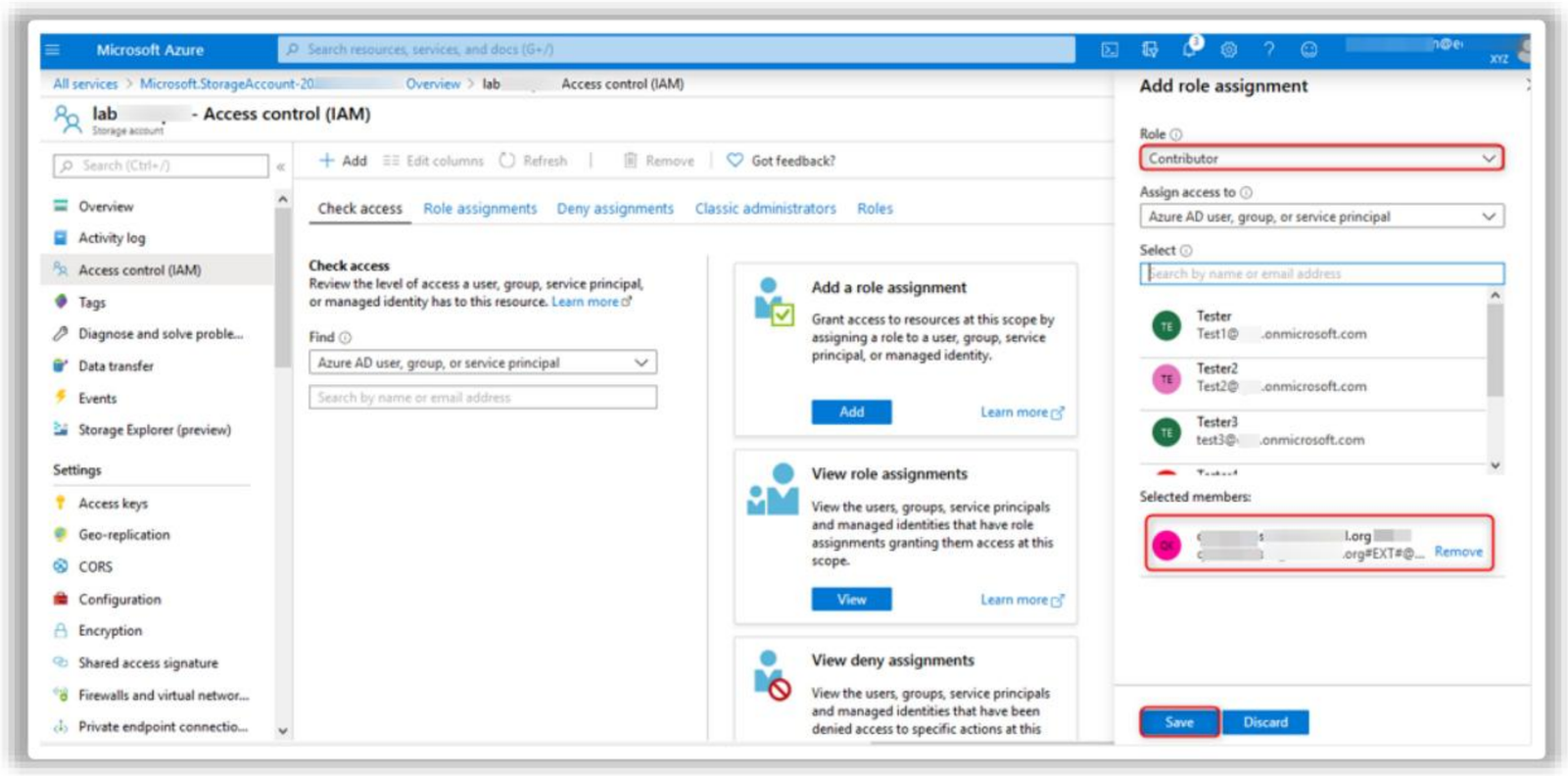


FIGURE 3.149: Add Role Assignment

- To view the assigned role, click on **View.**

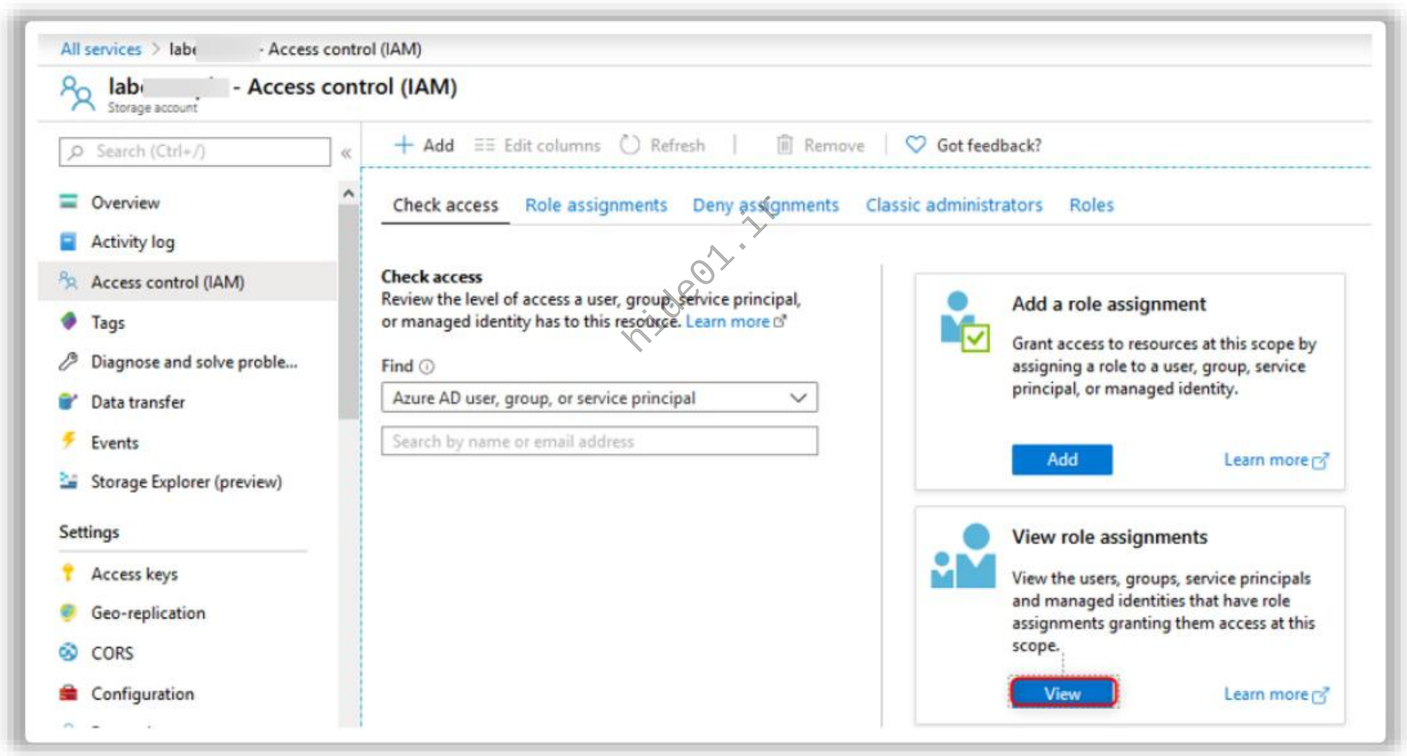
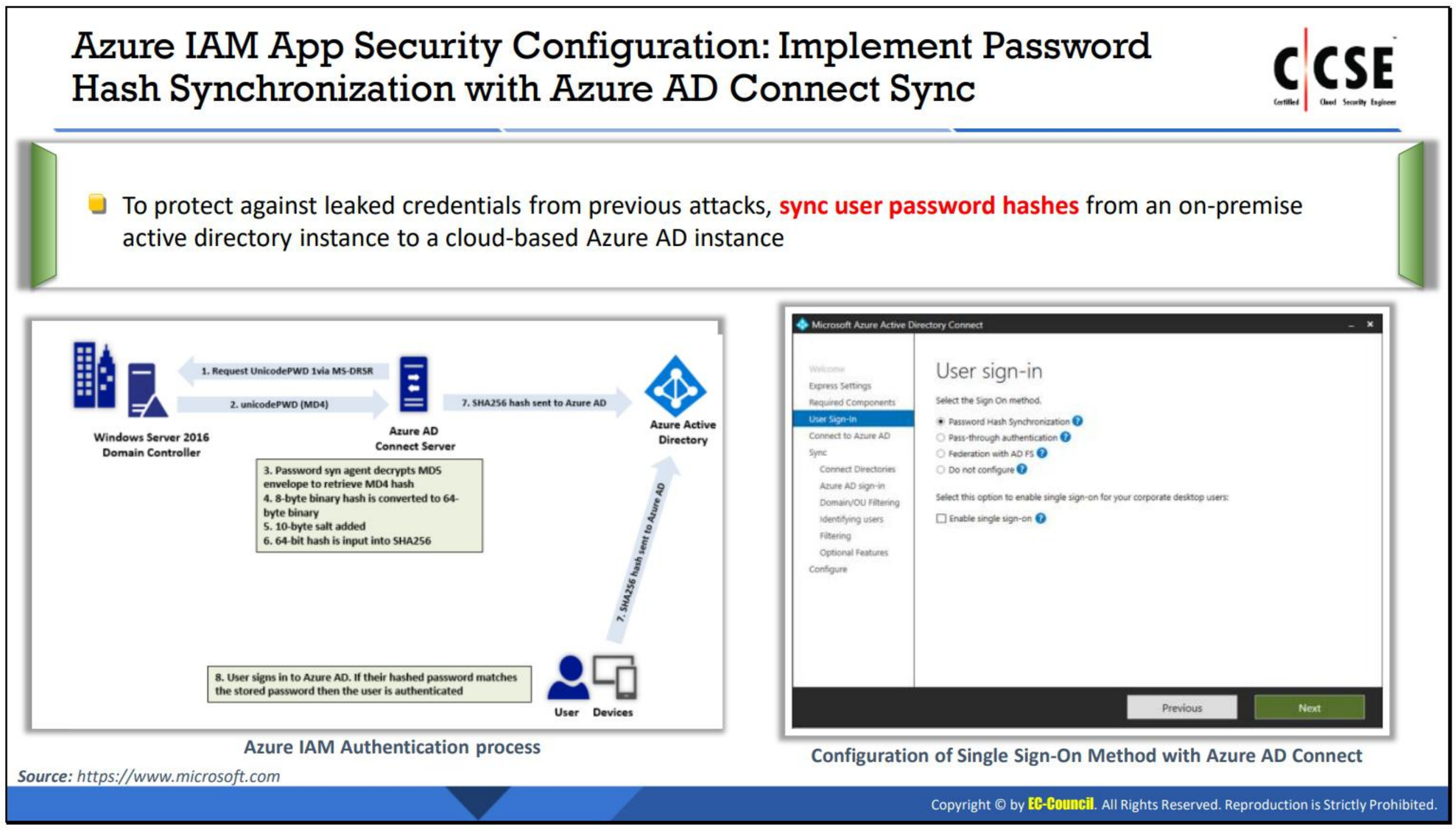


FIGURE 3.150:Access Control(IAM)

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



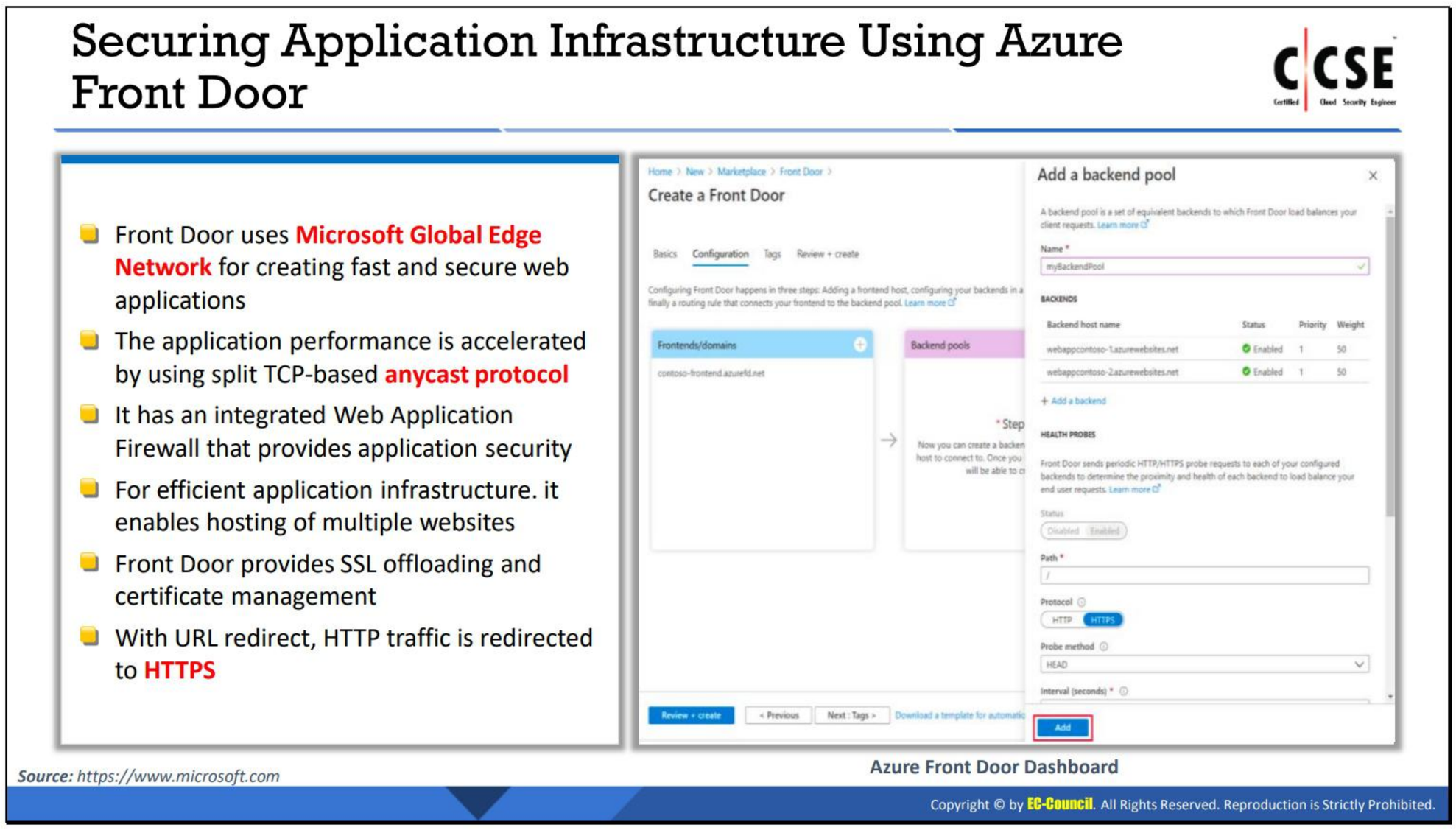
Azure IAM App Security Configuration: Implement Password Hash Synchronization with Azure AD Connect Sync

The implementation of password hash synchronization protects leaked credentials. This feature synchronizes user password hashes from an on-premise AD instance to a cloud-based Azure AD instance.

Password hash synchronization minimizes the number of passwords, and the users can maintain only one password for multiple accounts in Microsoft Azure. Thus, it not only improves the productivity of users but also reduces helpdesk costs.

Users can optionally set up password hash synchronization as a backup when on-premise servers become temporarily unavailable or fail.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Securing Application Infrastructure Using Azure Front Door

The global and scalable entry-point, Azure Front Door, uses the Microsoft global edge network to create secure web applications. Use Front Door to transform enterprise apps into high-performing personalized apps with the contents through Azure. It works at Layer 7 (HTTP/HTTPS layer) using anycast protocol with split TCP and the global network of Microsoft. It routes the client's requests to the most available application backend based on the routing method.

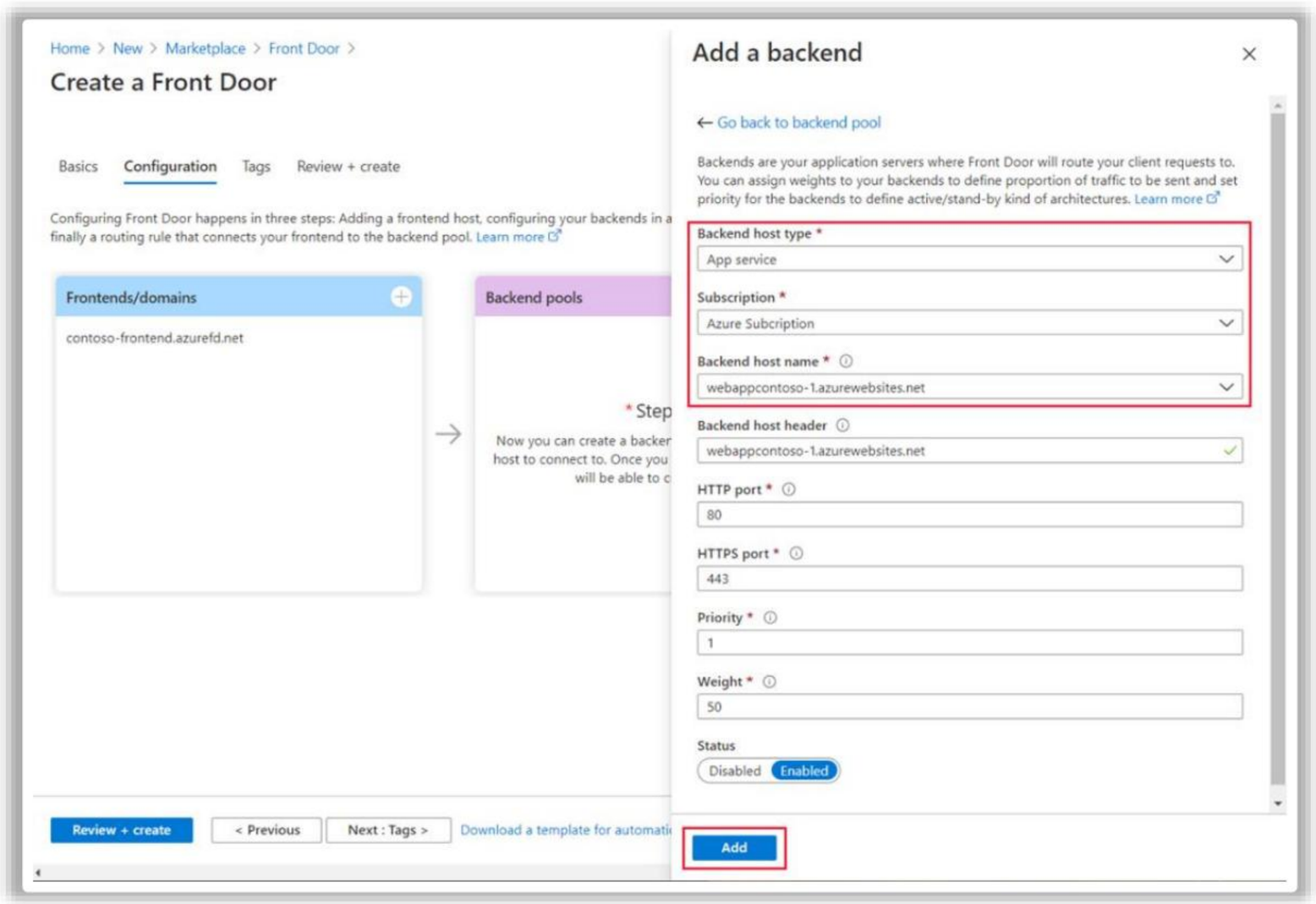


Figure 3.151: Create a Front Door for Your Application

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Source: https://www.microsoft.com

Key Features

Key features of Front Door include the following:

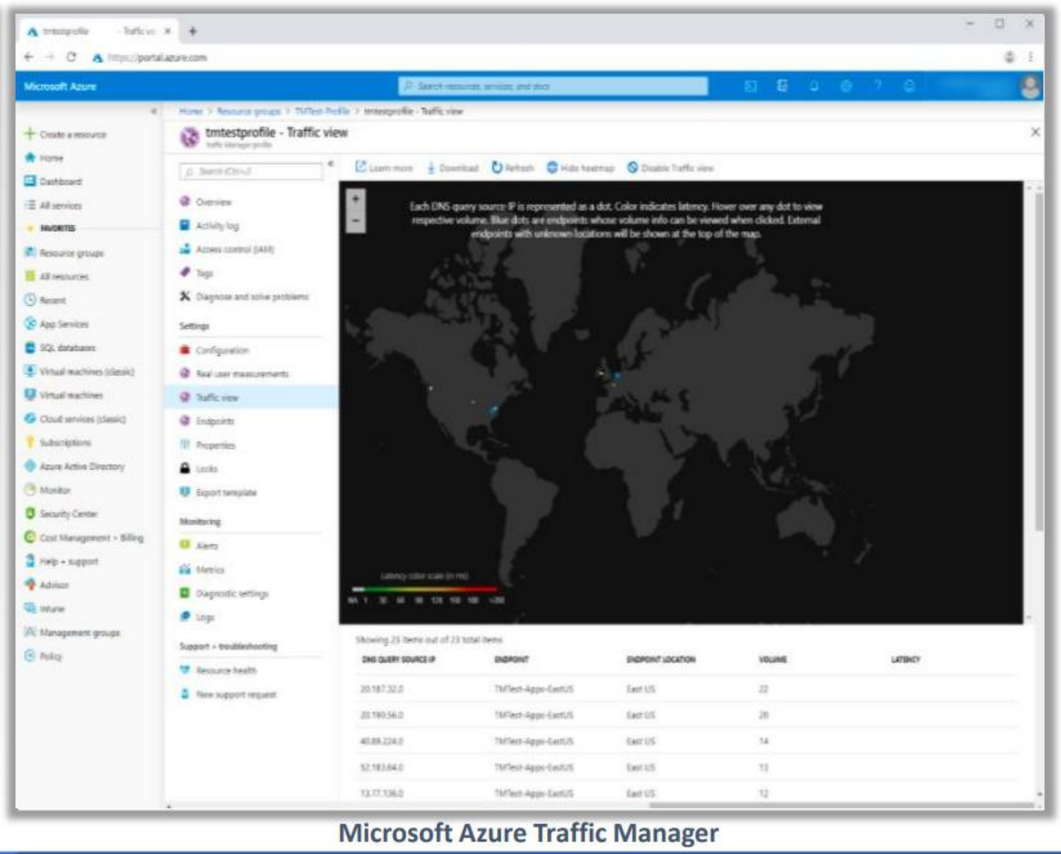
- **Split TCP**-based **anycast protocol** to accelerate application performance.
- **Health probe** monitoring for backend resources.
- **URL-path based** routing for requests.
- Hosting websites for efficient application infrastructure.
- Cookie-based **session affinity**.
- **SSL offloading** and certificate management.
- Allowing to define customer's own **custom domain**.
- Custom forwarding path with **URL rewrite**.
- Application security with integrated **Web Application Firewall (WAF)**.
- Native support of end-to-end IPv6 connectivity and **HTTP/2 protocol**.
- Redirect HTTP traffic to HTTPS with **URL redirect**.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Securing Application Infrastructure Using Traffic Manager

- Azure Traffic Manager is a **DNS-based traffic load balancer** that allows distributing the traffic to public-facing applications across global regions
- Endpoints are monitored and provides **automatic failover**, thereby delivering high availability
- Application performance is improved by directing the traffic to the endpoint with lowest latency
- Planned maintenance can be done to the applications without downtime
- **Nested traffic manager** policies can be used to distributing traffic for complex deployments



Microsoft Azure Traffic Manager

Source: https://www.microsoft.com

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

Securing Application Infrastructure Using Traffic Manager

The DNS-based traffic load balancer, Azure Traffic Manager, distributes traffic to applications that face the internet across the global Azure regions. It provides public endpoints with high availability. It uses DNS to move client requests to the appropriate service endpoints depending on the traffic-routing method.

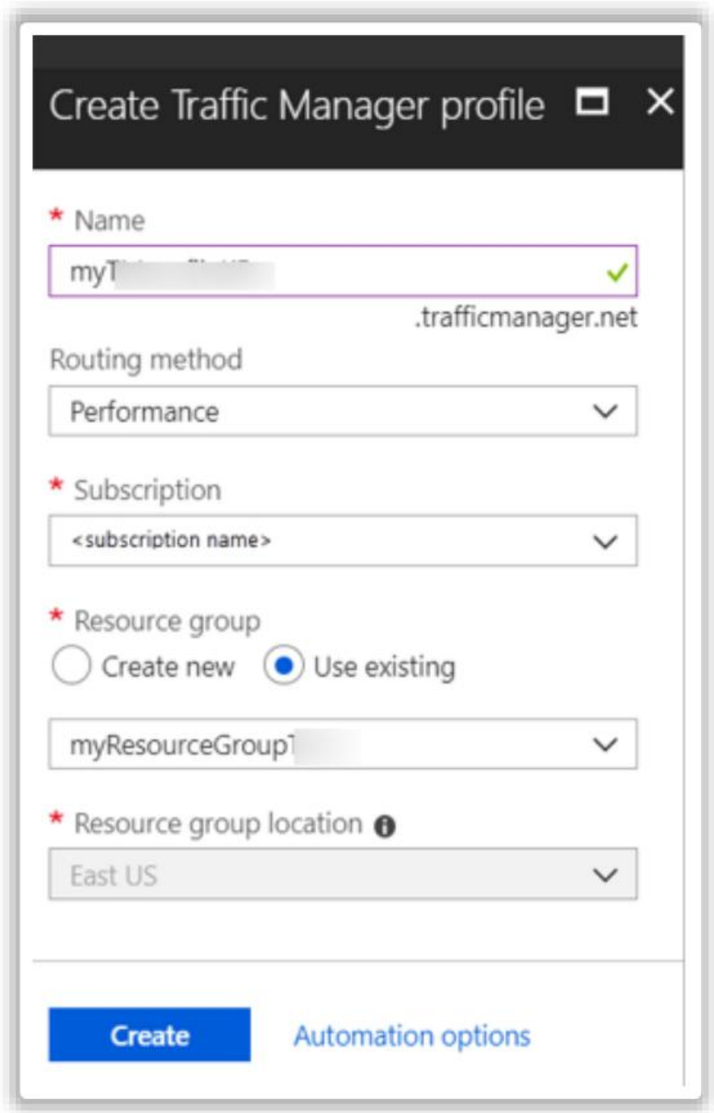


Figure 3.152: Create a Traffic Manager Profile

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Key features

The key features offered by Azure Traffic Manager include the following:

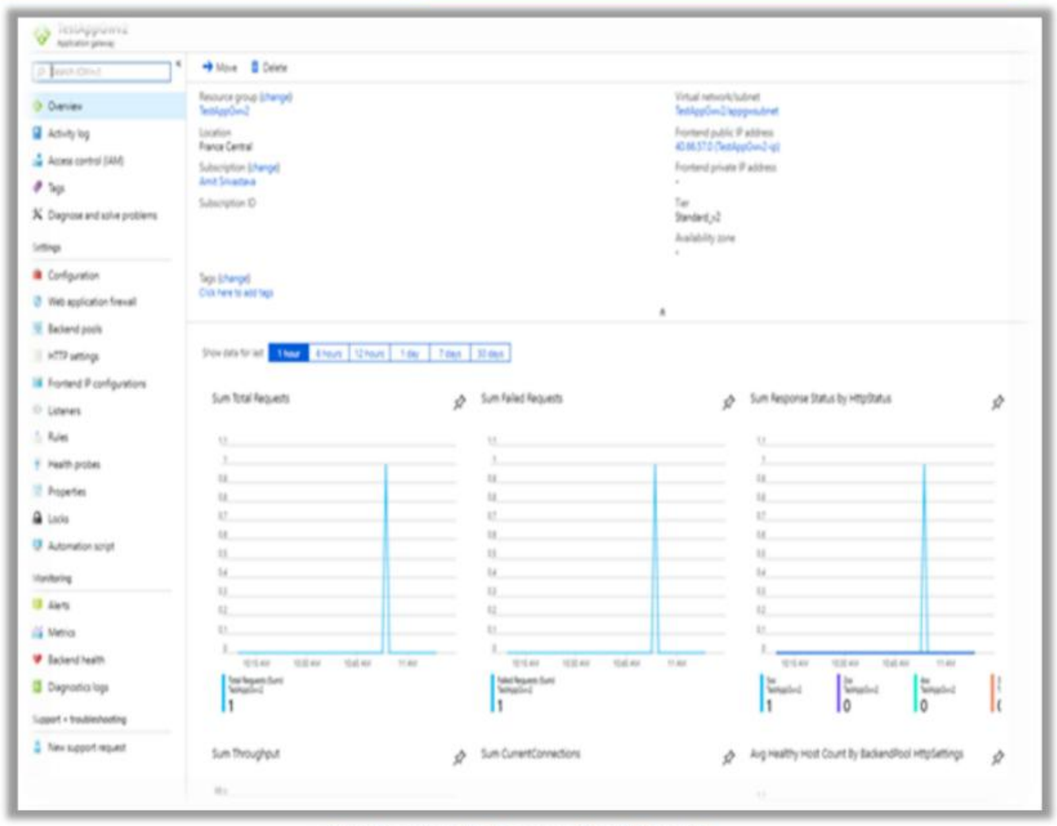
- High availability for critical applications by monitoring enterprise endpoints.
- Automatic failover when an endpoint goes down.
- Service maintenance without downtime.
- Directing traffic to alternative endpoints while the maintenance is in progress.
- Combine hybrid applications.
- Combine nested Traffic Manager profiles and multiple traffic-routing methods to create rules and to scale to the needs of larger, more complex deployments.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Securing Application Infrastructure Using Application Gateway

- Application Gateway is a **web traffic load balancer** to manage traffic to web applications
- Application Gateway supports end-to-end SSL/TLS termination
- Supports **autoscaling** and can scale up or down based on changing traffic load
- Application gateway has a **Web Application Firewall** that patches a known vulnerability at a central location
- Application Gateway supports multiple site hosting
- Supports rewriting of HTTP headers and URL for adding security-related header fields



Application Gateway Dashboard

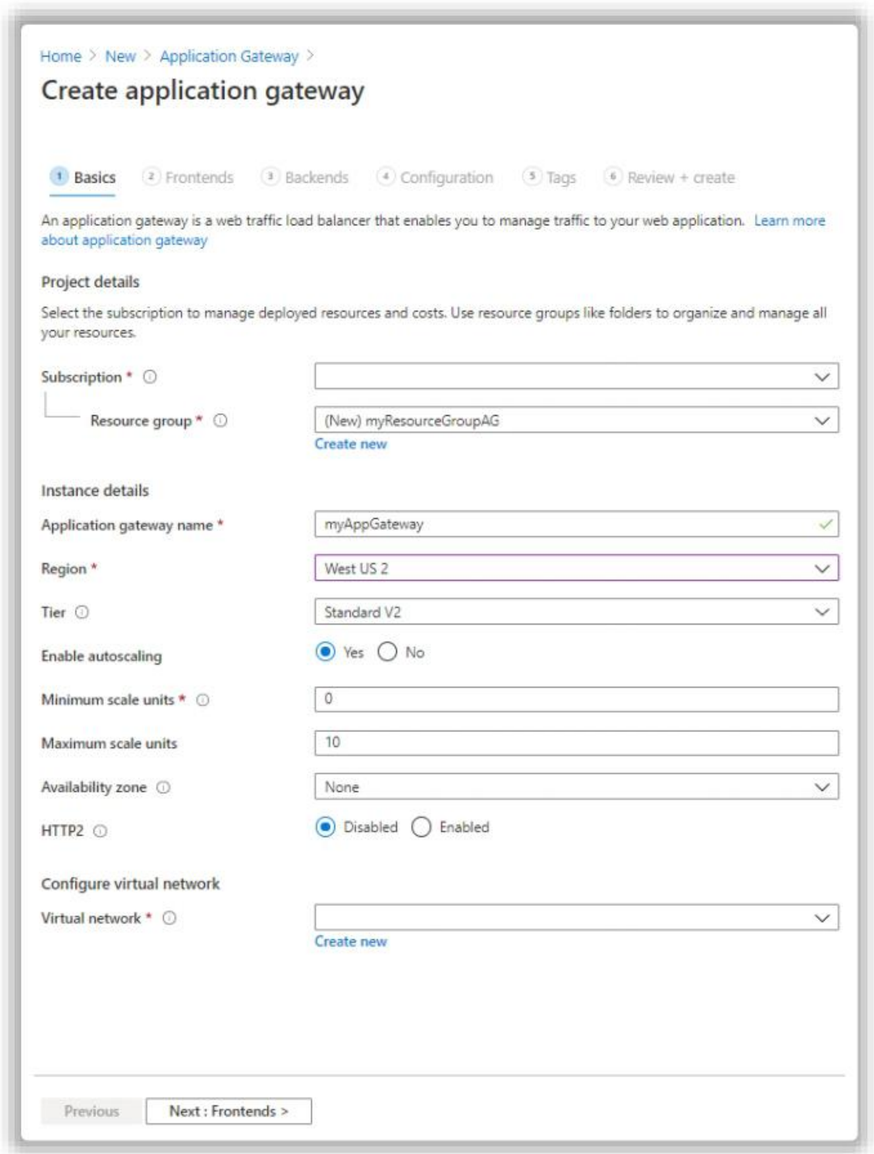
Source: https://www.microsoft.com

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

Securing Application Infrastructure Using Application Gateway

The web traffic load balancer, Azure Application Gateway, enables management of traffic to web applications. It supports end-to-end SSL/TLS termination, multi-site hosting, and autoscaling (can scale-up and scale-down as per traffic load). It also allows rewriting of HTTP headers and URLs to add security-related header files.

hid001.ir



Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 3.153: Create an Application Gateway

Source: https://www.microsoft.com

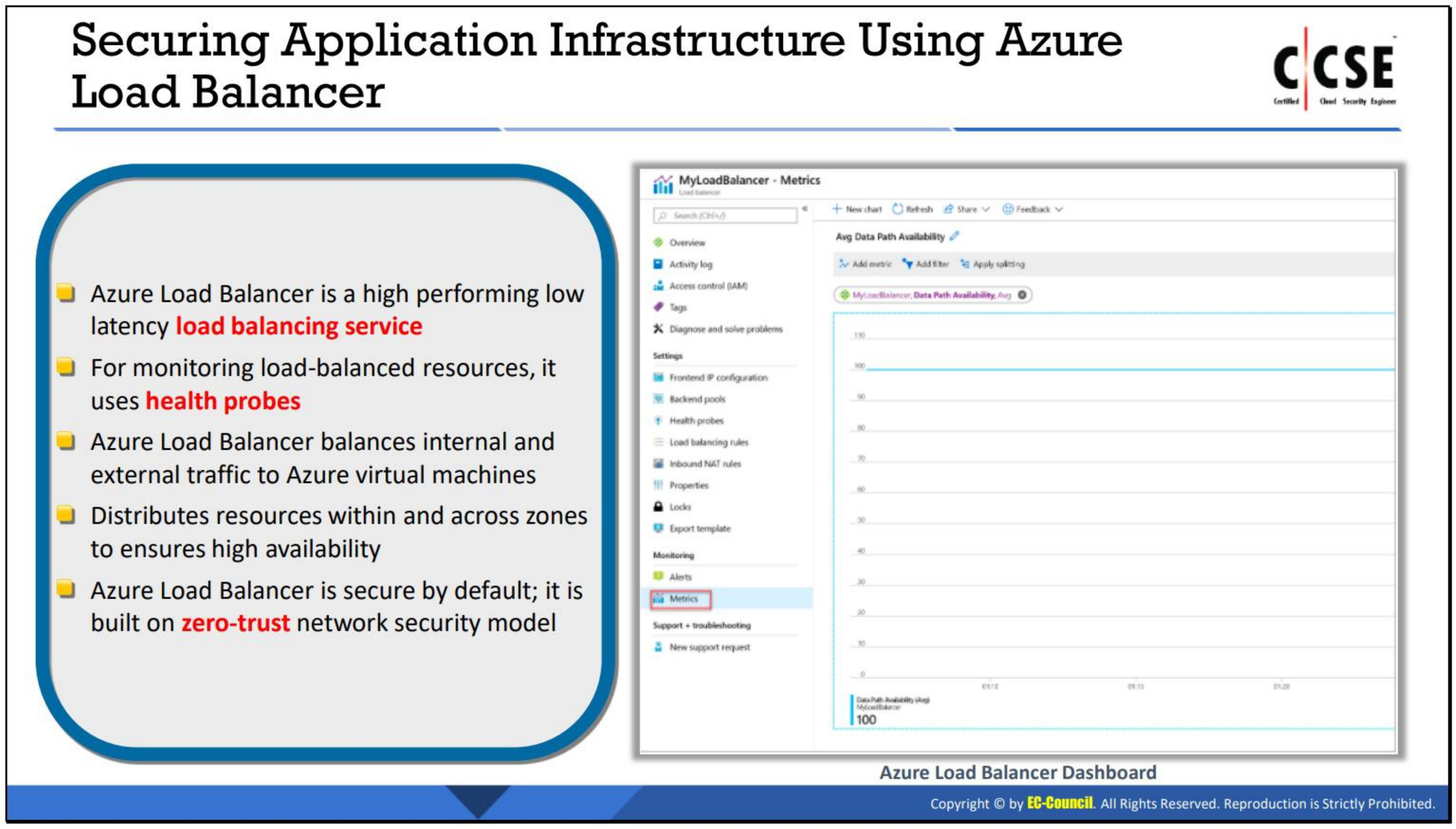
Key Features

Application Gateway includes the following features:

- Supports **Secure Sockets Layer (SSL/TLS) termination** at gateway after which traffic flows unencrypted to the backend servers.
- **Zone redundancy** in which it offers multiple availability zones, providing fault resiliency and preventing the need of provisioning separate application gateways in each zone.
- Offers **Web Application Firewall** to protect web apps from common vulnerabilities.
- **URL-based routing** to route traffic to backend server pools based on URL paths of the request.
- **Multiple-site hosting** to configure routing based on hostname/domainname for more than one web application on the same application gateway.
- **Rewrite HTTP headers and URL** to allow the client and server to pass information with request and response.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Securing Application Infrastructure Using Azure Load Balancer

Azure Load Balancer is a high-performing low-latency load balancing service. It allows scaling of applications and creating highly available services. Azure Load Balancer is secure by default because it is built on the zero-trust network security model. It supports both inbound and outbound scenarios and balances internal and external traffic to Azure virtual machines. It provides low latency and high throughput and scales up to millions of flows for all TCP and UDP applications. By distributing resources within and across zones, it ensures high availability.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

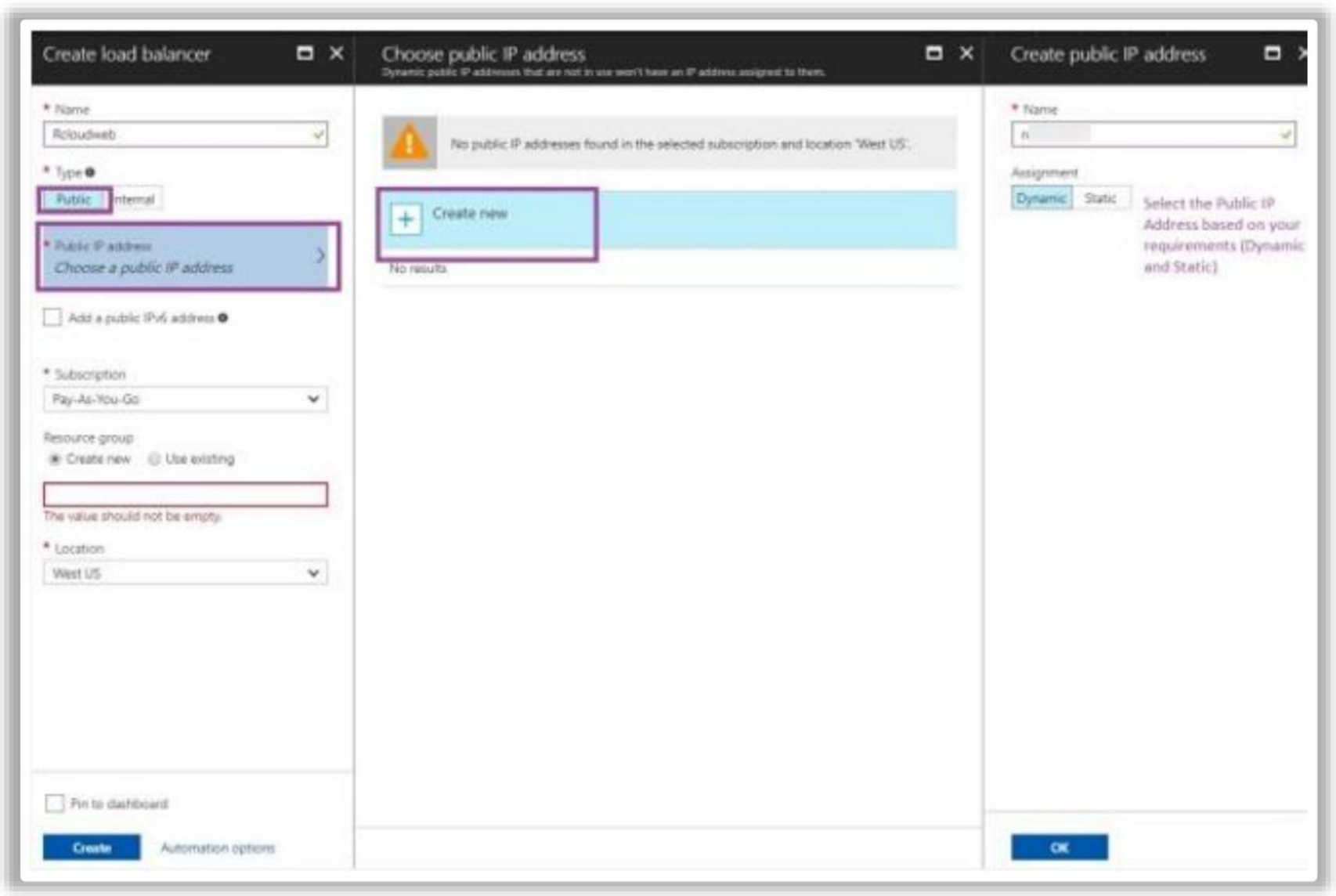


FIGURE 3.154:Create Azure Load Balancer

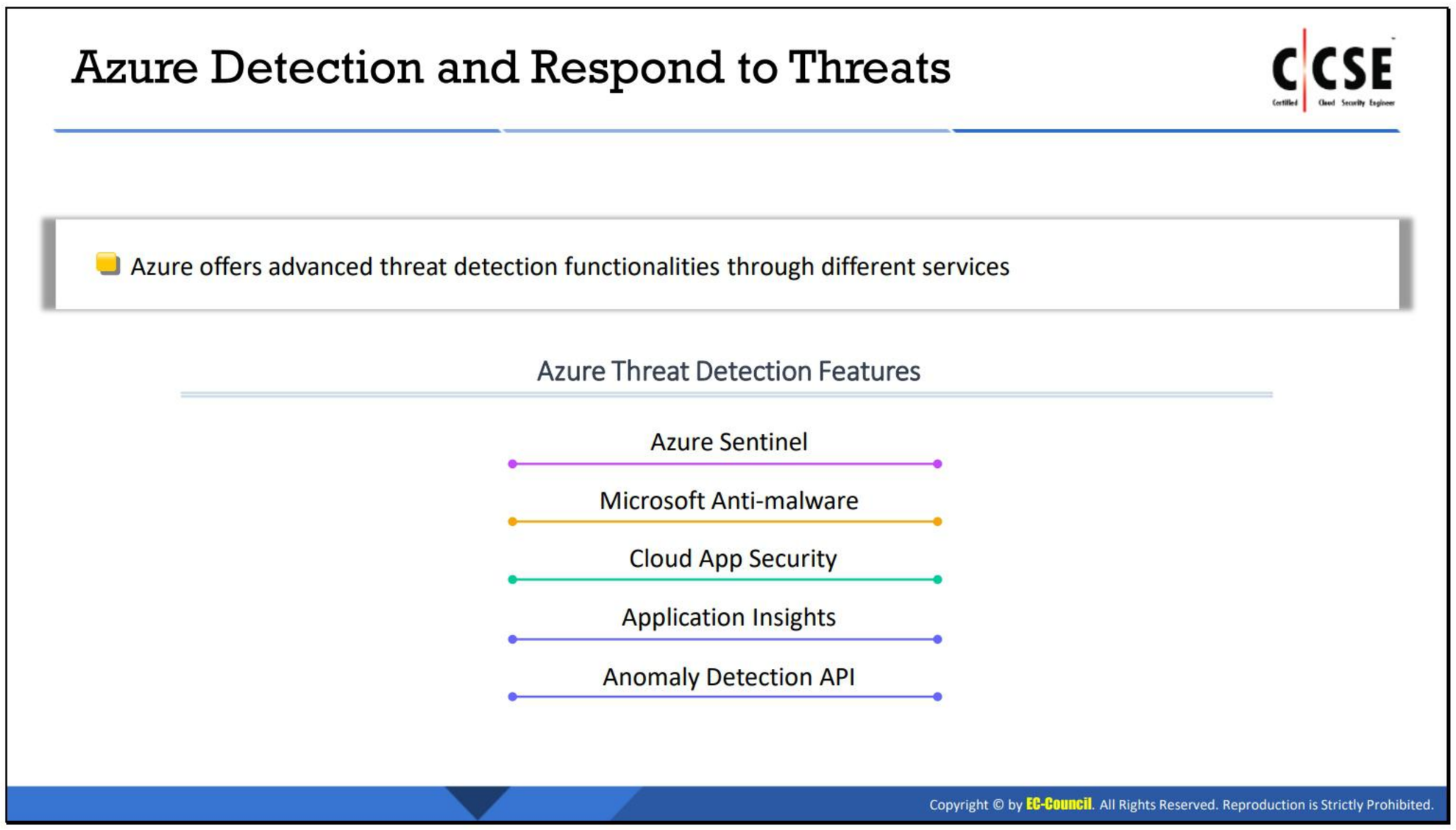
Key Features

The key features of Azure Load Balancer are as follows:

- Create highly available and scalable applications. Azure Load Balancer supports TCP/UDP-based protocols (HTTP, HTTPS, and SMTP, and protocols for voice and video messaging applications).
- Automatically scale with increasing application traffic, preventing reconfiguring/managing the load balancer.
- Use the internal load balancer for traffic among VMs inside private VNets or create multi-tiered hybrid apps.
- Probe the health of application instances, take unhealthy instances out of rotation automatically and reinstate the instances when they become healthy again. Use Global Load Balancer for latency-based traffic distribution across multiple regional deployments/improve application uptime with regional redundancy.

hi0001.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Azure Detection and Response to Threats

Azure offers advanced threat detection functionalities through different services. Azure threat detection features are.

hade01.ir

- **Azure Sentinel**: The cloud-based, scalable SIEM and SOAR solution, Azure Sentinel, provides threat intelligence and intelligent security analytics.

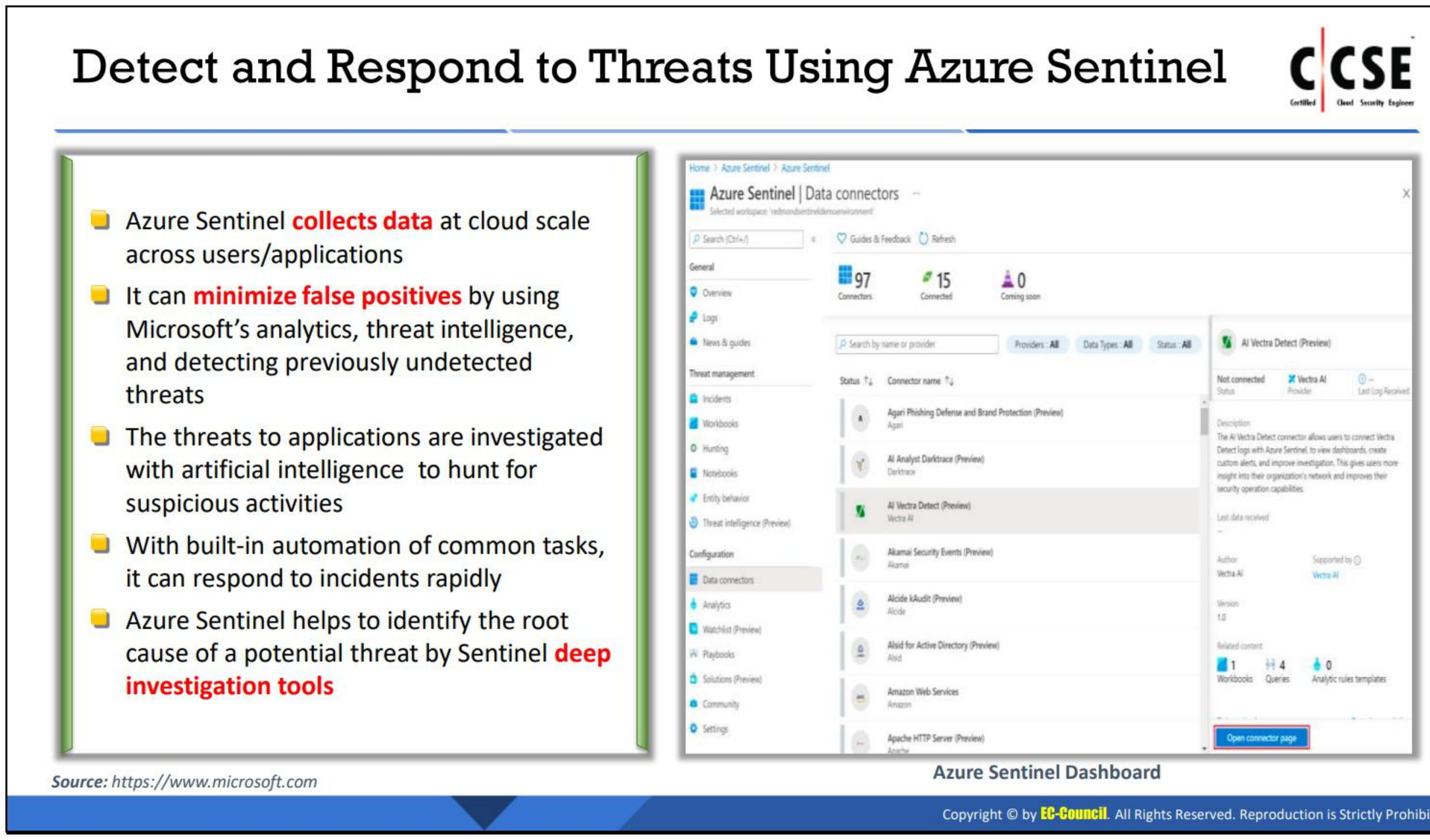
- **Microsoft Anti Malware**: Microsoft Anti-malware offers real-time protection that detects and removes spyware, viruses, and malicious software from Azure cloud applications and services.

- **Cloud App Security**: Microsoft Cloud App Security (MCAS) refers to a CASB that offers enhanced visibility into and control over data travel and advanced analytics to detect and remediate security threats across all cloud services and applications.

- **Application Insights**: Azure Monitor's Application Insights feature increases visibility into how applications function or perform. Use Application Insights to monitor the performance, availability, and usage of applications hosted on Azure or on-premises.

- **Anomaly Detection API**: Anomaly Detector API is an (AI-based) Azure service that helps monitor and detect abnormalities in time-series data without requiring any knowledge of machine learning.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Detect and Respond to Threats Using Azure Sentinel

The cloud-based, scalable SIEM and SOAR solution, Azure Sentinel, provides threat intelligence and intelligent security analytics. It is a single solution for threat visibility, alert detection, threat response, and proactive hunting. It provides a birds-eye view across the organization, reduces the number of attacks, and provides high volumes of alerts as well as the long time frames required for resolution.

Azure Sentinel offers the following security benefits:

- Gathers security data at cloud-scale across all applications
- Detects threats that were previously undetected and minimize false positives via threat intelligence and the Microsoft's analytics.
- Threat investigation with artificial intelligence.
- Respond rapidly to threat incidents with the help of in-built orchestration and automation of common tasks.

Key Features

Source: https://www.microsoft.com

Use Azure Sentinel features to ensure the security of cloud applications:

- **Analytics:** Azure Sentinel leverages Microsoft's analytics to correlate alerts into security incidents. This saves the time required to review and investigate a security alert to confirm it is a security incident. Create new correlation rules or use the existing ones to ensure Sentinel detects security incidents precisely. Sentinel also offers machine learning rues to map the behavior of a network and then search for anomalies across the

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

resources. These analytics help in connecting the dots to detect potential high-fidelity security incidents by combining low-fidelity alerts about various entities.

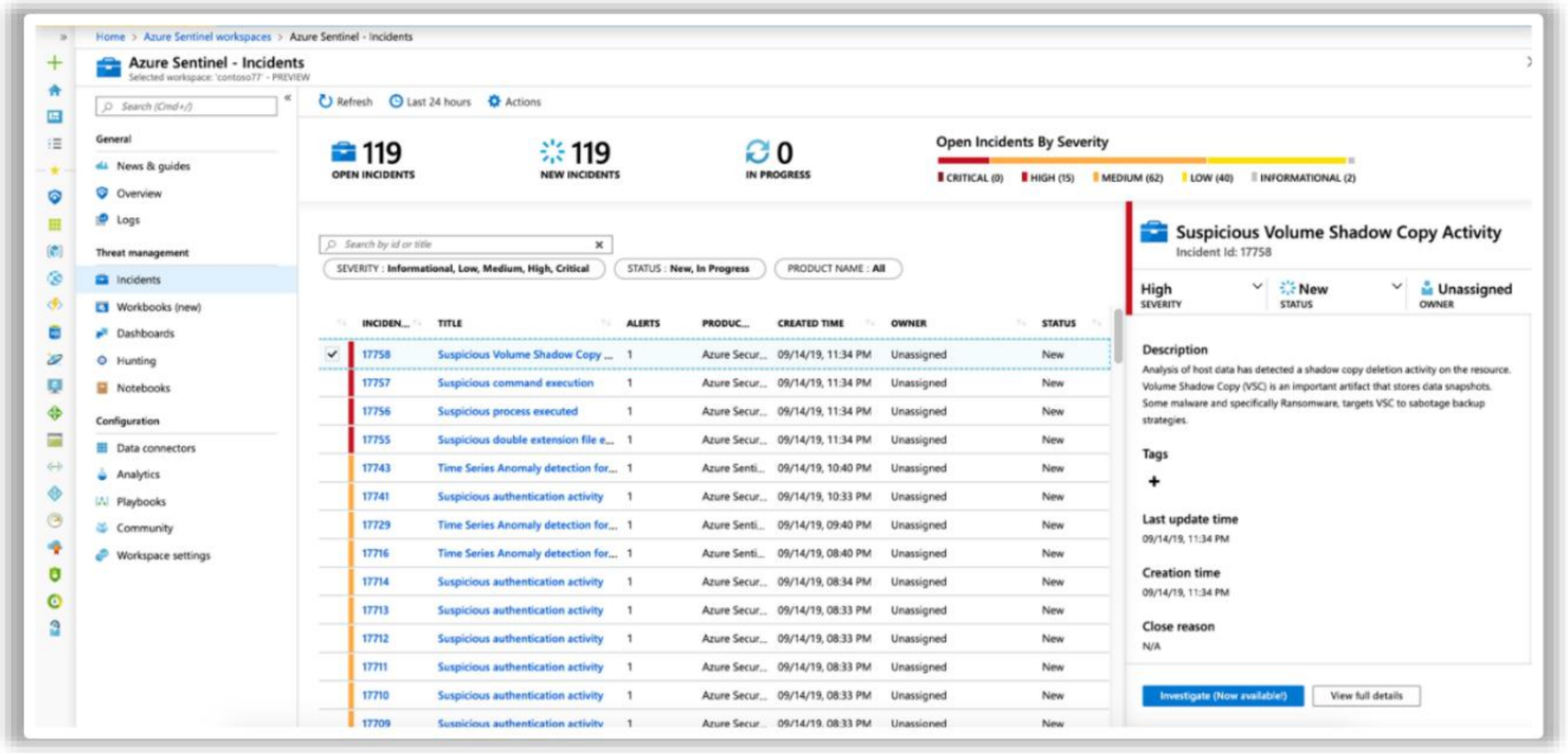


FIGURE 3.155:Azure Sentinel-Incidents

- **Security automation and orchestration:** Azure Sentinel allows cloud administrators to automate common tasks and make security orchestration simple with playbooks. These playbooks integrate with existing tools and Azure services. The security automation and orchestration feature of Sentinel enables scalable automation as new threats and technologies emerge. Choose existing playbooks that are built-in to create new playbooks with Azure Logic Apps.
- **Investigation:** Azure Sentinel provides deep investigation tools that help cloud administrators understand the scope of a potential threat and identify its root cause. A cloud administrator can select an entity on the interactive graph to know more about that entity and dig deep into that entity and its connections to identify the root cause of the threat.

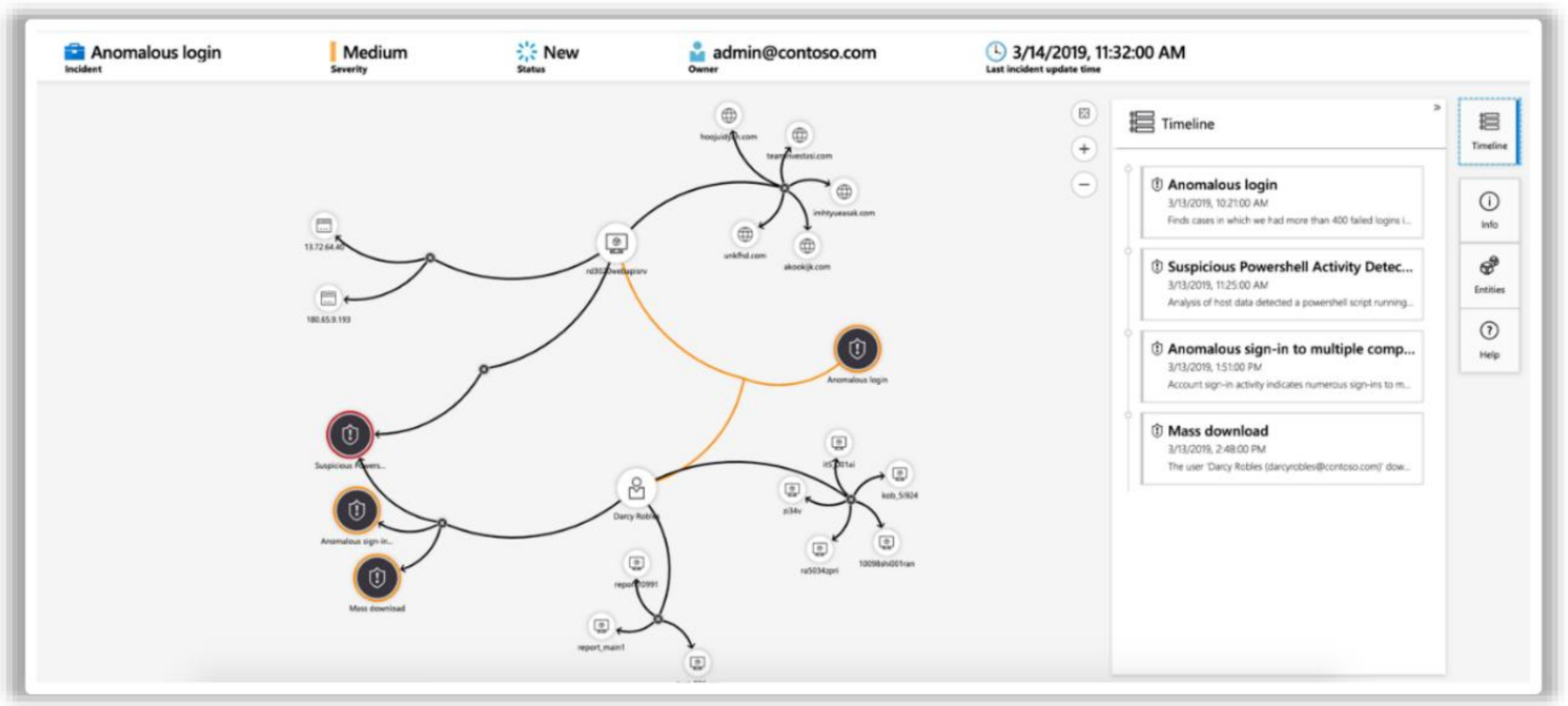


FIGURE 3.156:Anomalous Login

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Hunting:** Sentinel offers powerful search-and-query tools that are based on the MITRE framework. These tools help cloud administrators proactively hunt for threats across all organization data sources before an alert is raised. Create custom detection rules based on queries that provide high-value insights into potential attacks and inform security incident responders about those insights in the form of alerts. Sentinel allows cloud administrators to bookmark interesting events while hunting to check them later, share them with others and use them for investigation purposes.

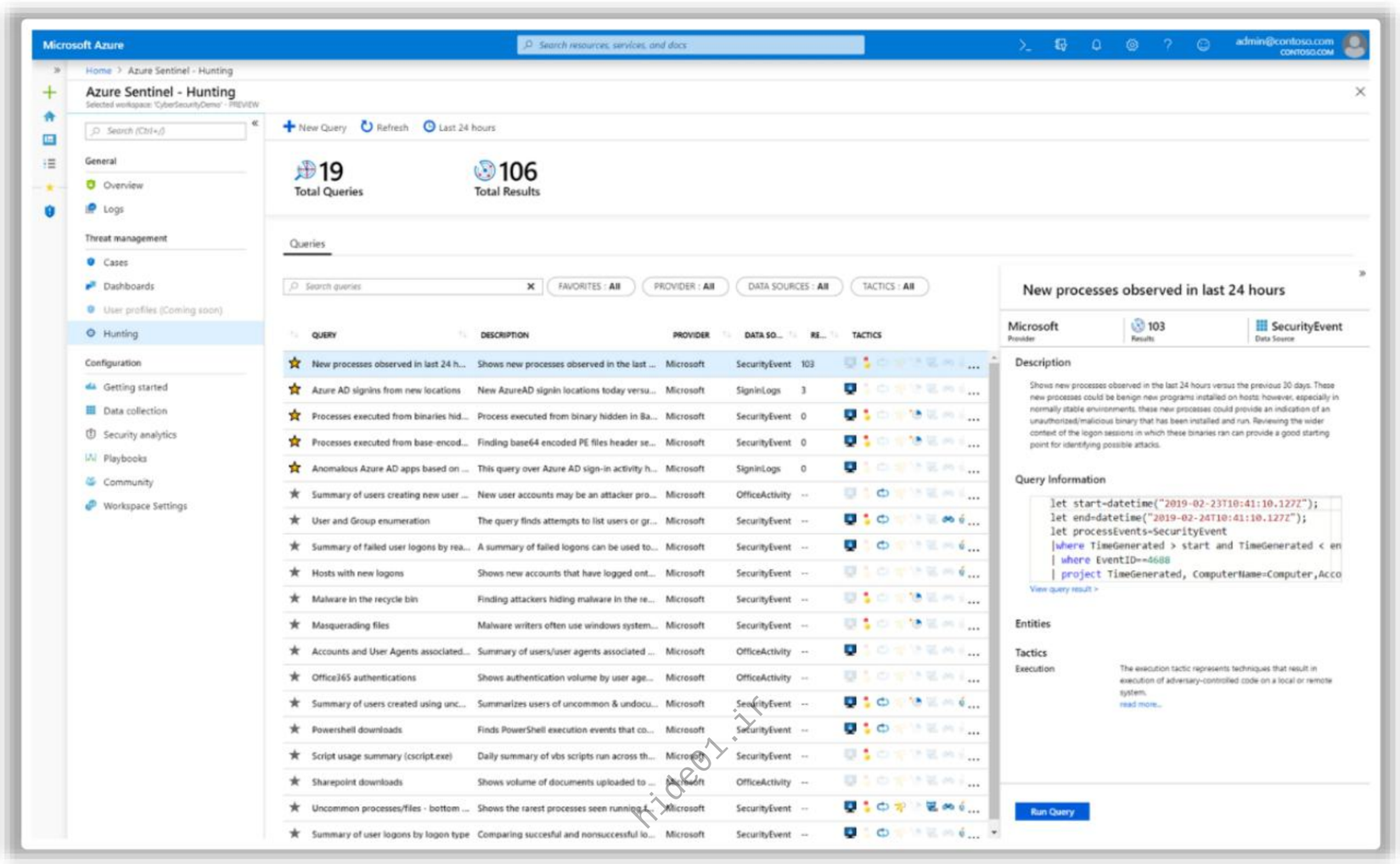
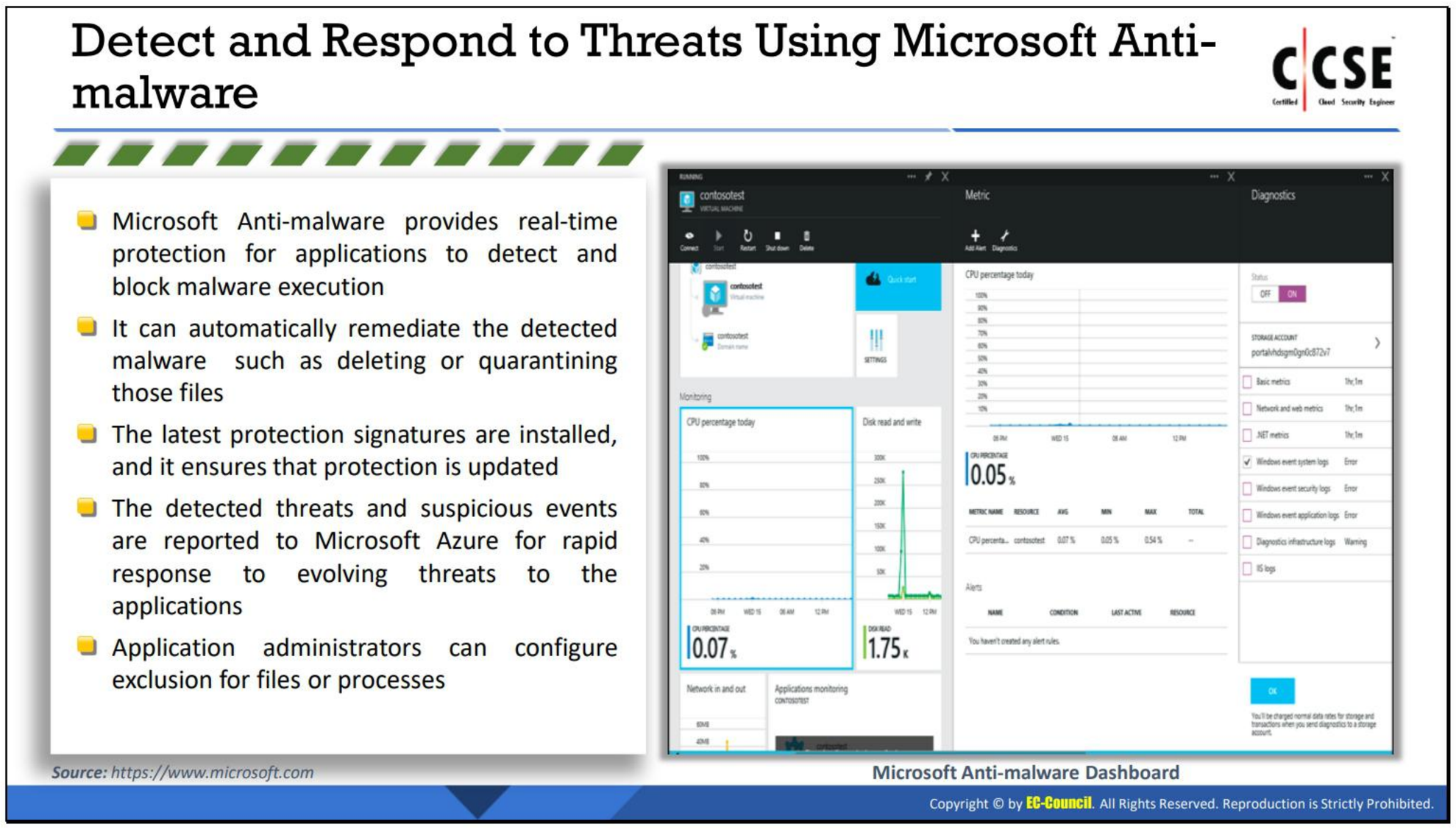


FIGURE 3.157:Azure Sentinel-Hunting

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Detect and Respond to Threats Using Microsoft Anti-malware

Microsoft Anti-malware offers real-time protection that detects and removes spyware, viruses, and malicious software from Azure cloud applications and services. When known malicious software or unknown software attempts to run or install on Azure systems, Microsoft Anti-malware generates alerts. Microsoft Anti-malware acts as a single-agent solution for Azure applications and tenant environments that run in the background to protect them without any human intervention. Based on the application needs, deploy protection and monitoring to enable real-time protection, protection updates, scheduled scanning, active protection, and malware remediation. The detected threats and suspicious events are reported to Microsoft Azure for rapid response to evolving threats to the applications. This service can be enabled by default or custom configuration settings depending on the application requirements. Application administrators can configure exclusion for files and processes.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

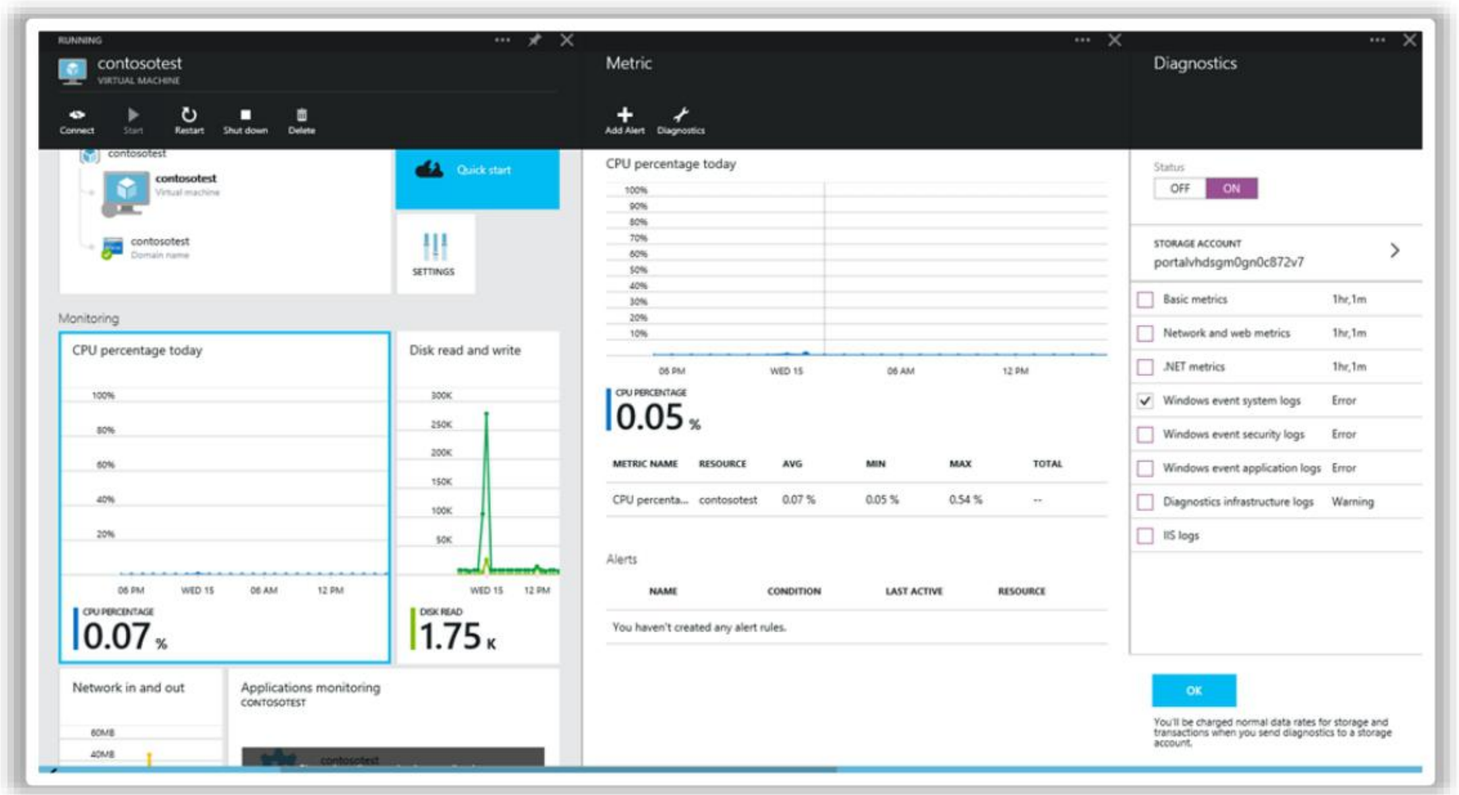


Figure 3.158: Anti-malware Events Collected from Windows Event System Logs to Azure Storage Account

Source: https://www.microsoft.com

Key Features and Advantages

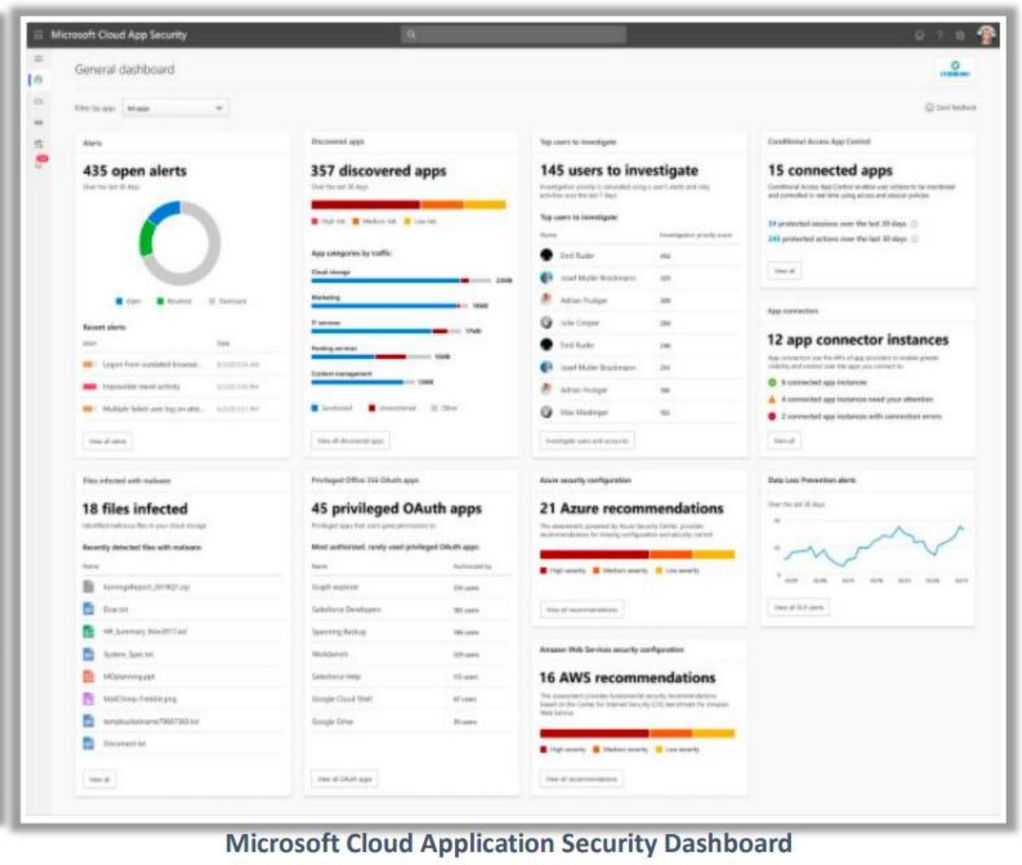
The features provided by Microsoft Anti-malware includes the following:

- **Real-time protection**: Detects and blocks malware by monitoring activity in cloud applications and services, and VMs.
- **Scheduled scanning**: Scans software or programs periodically to detect malware.
- **Malware remediation**: Takes action automatically on detected malware by either deleting files containing malware or quarantining them and removing malicious registry entries.
- **Signature updates**: Installs the latest virus definitions or protection signatures automatically to keep protection up-to-date.
- **Active protection**: Reports telemetry metadata of suspicious resources and detected Azure threats to ensure instant response to threats and enable real-time synchronous signature delivery via MAPS (Microsoft Active Protection System).
- **Sample reporting**: Provides sample to the anti-malware service to improve the service and enable troubleshooting.
- **Anti-malware event collection**: Records suspicious activities, the anti-malware service health, and remediation actions taken in the OS event log and stores them into the storage account of the customer.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Detect and Respond to Threats Using Cloud App Security

- Microsoft Cloud App Security is a **Cloud Access Security Broker (CASB)** that supports log connection, API connectors, and reverses proxy
- It has **sophisticated analytics** to identify and defend cyber threats against applications
- CASB can ensure security by acting as a doorkeeper to broker access between users and applications
- CASB monitors **user activities** for unusual behavior, controlling access, and preventing sensitive information disclosure
- CASB assesses the applications whether they meet **security compliance**
- Analyzes high-risk usage and mitigates automatically



Microsoft Cloud Application Security Dashboard

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

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

Detect and Respond to Threats Using Cloud App Security

Microsoft Cloud App Security (MCAS) refers to a CASB that offers enhanced visibility into and control over data travel and advanced analytics to detect and remediate security threats across all cloud services and applications. It offers centralized management, easy integration with other Microsoft solutions, simple deployment, and advanced automation capabilities. It supports multiple deployment modes such as reverse proxy, log collection, and API connectors. It enforces the organization's security policies to secure the use of cloud services.

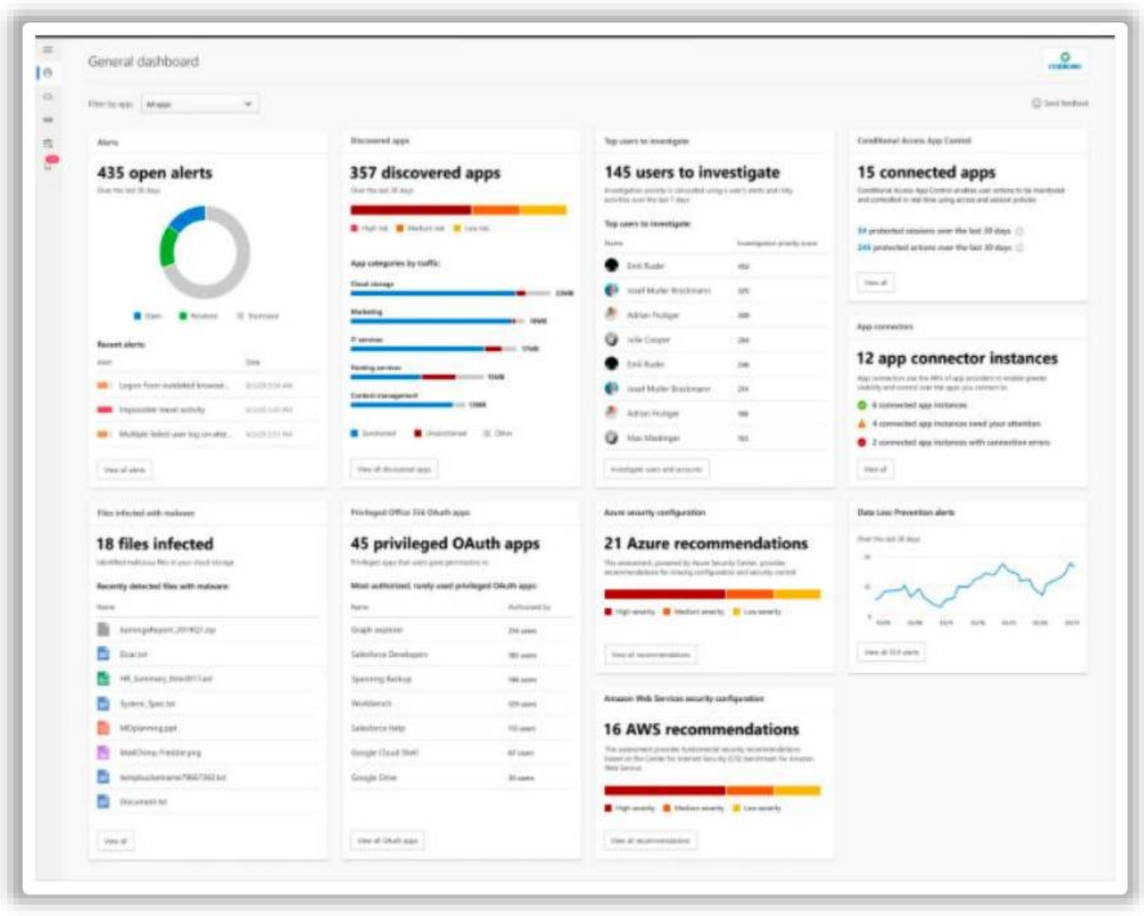


FIGURE 3.159: Microsoft Cloud App Security

Source: https://www.microsoft.com

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

MCAS embeds visibility into the cloud by

- Leveraging Cloud Discovery to detect and map the cloud environment and apps used by it.
- Sanctioning and unsanctioning applications in the organization's cloud environment.
- Employing simple App connectors for governance and visibility of apps.
- Leveraging Conditional Access App Control protection to gain real-time control and visibility into activities and access inside cloud apps.
- Allowing continuous control via setting and managing policies.

Key Features and Advantages

The features provided by MCAS are listed below.

- **Cloud Discovery:** MCAS allows cloud administrators to detect cloud services and apps used by their organizations. Cloud administrators can assess the risk levels and business readiness of the apps against more than 90 risk factors and manage them to ensure they are in compliance and security.

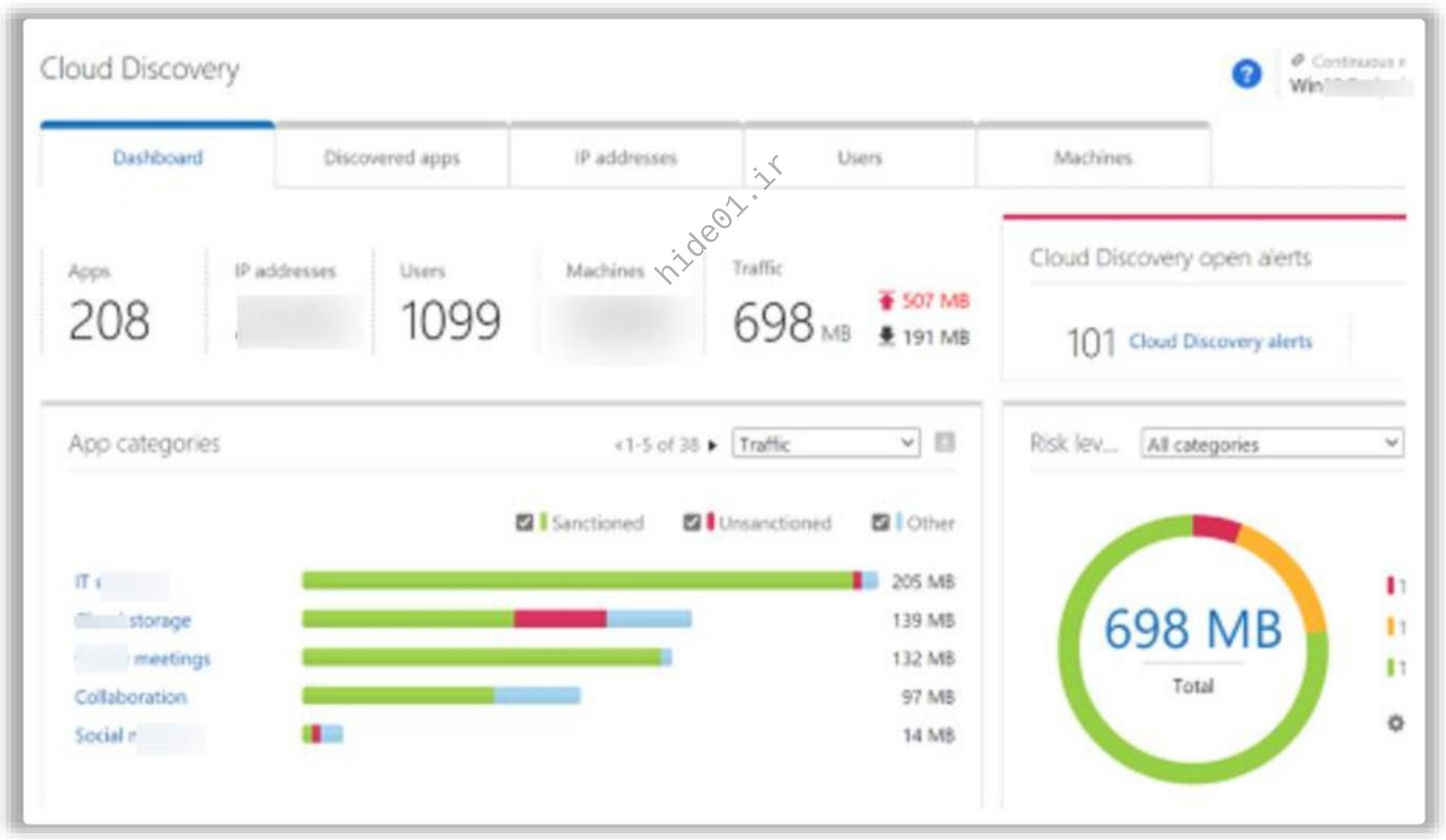


FIGURE 3.160:Cloud Discovery

- **Secure sensitive information:** With MCAS, cloud administrators can understand and classify sensitive information at rest and prevent it from exposure. They can use out-of-the-box policies and automated processes to apply controls at rest and in real-time across all cloud applications with MCAS.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

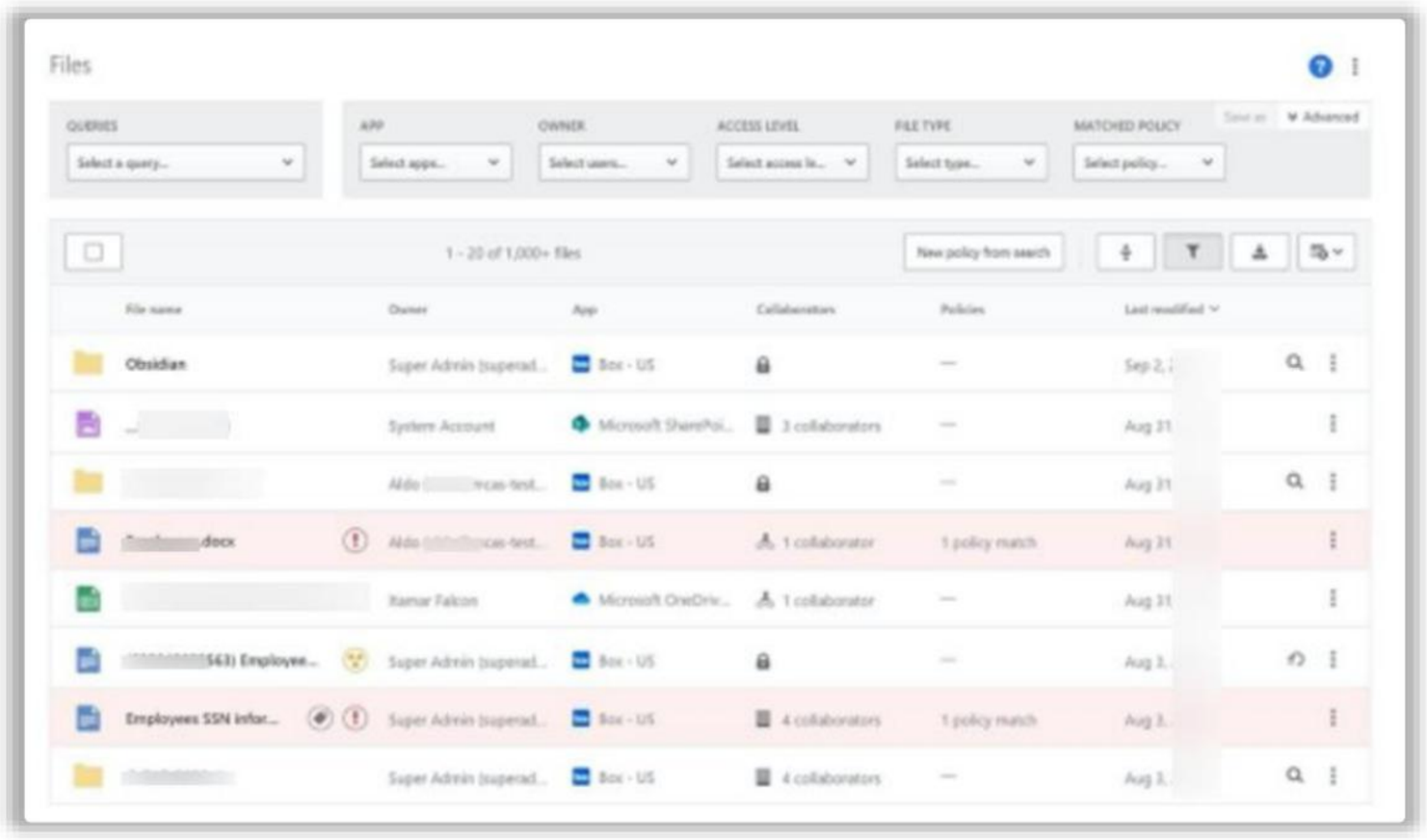


FIGURE 3.161: Files

- **Protect against anomalies and threats:** MCAS helps cloud administrators detect suspicious behavior across cloud applications so that ransomware, rouge apps, or compromised users can be identified. The use of MCAS limits the risk to the organization by analyzing high-risk usage and remediating automatically.

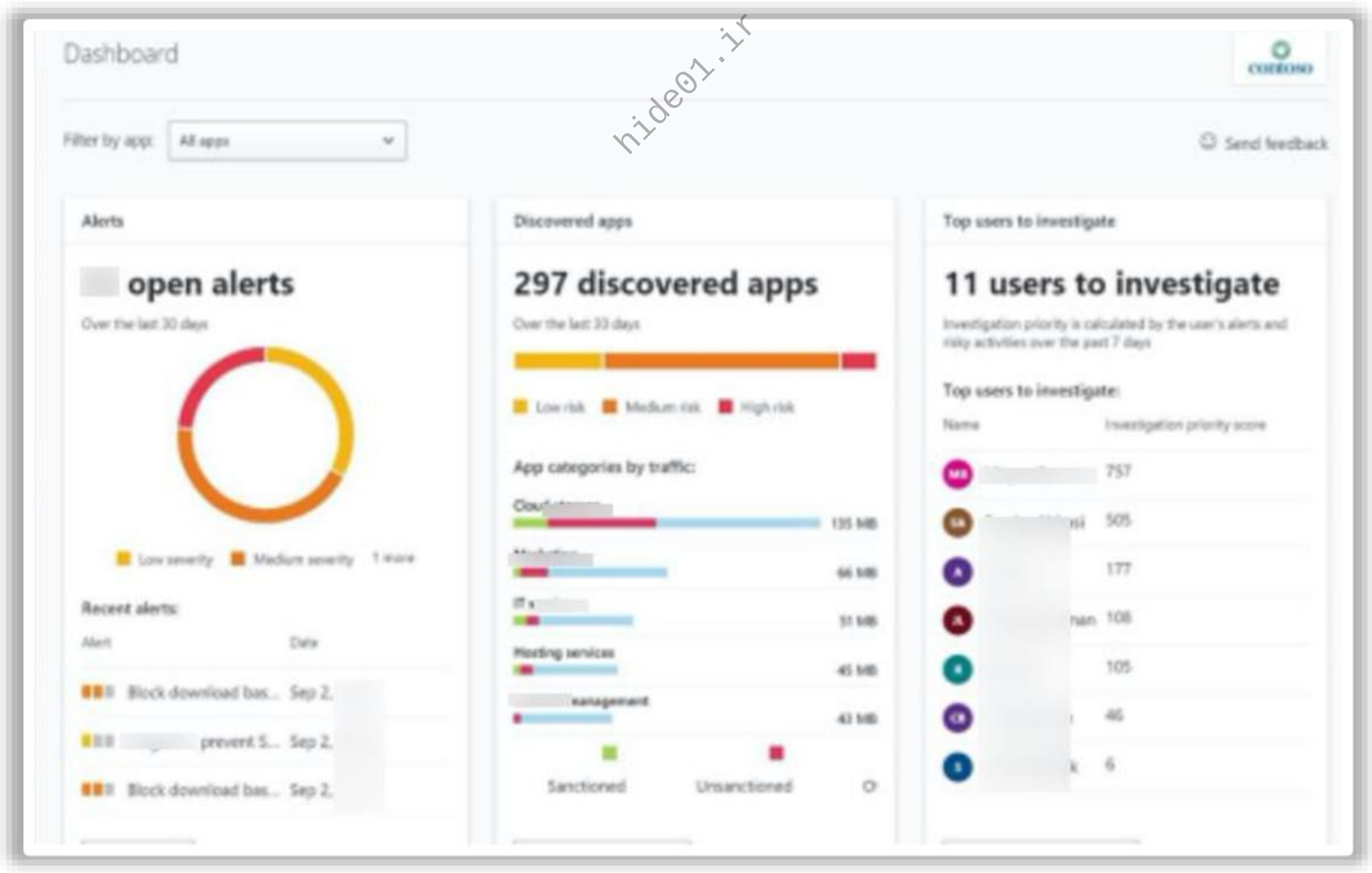


FIGURE 3.162:Dashboard

- **Assess the compliance of apps:** MCAS allows cloud administrators to assess the compliance of cloud apps to ensure they meet relevant compliance requirements. Use MCAS to prevent data leaks to the apps that are non-compliant and restrict access to regulated data.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

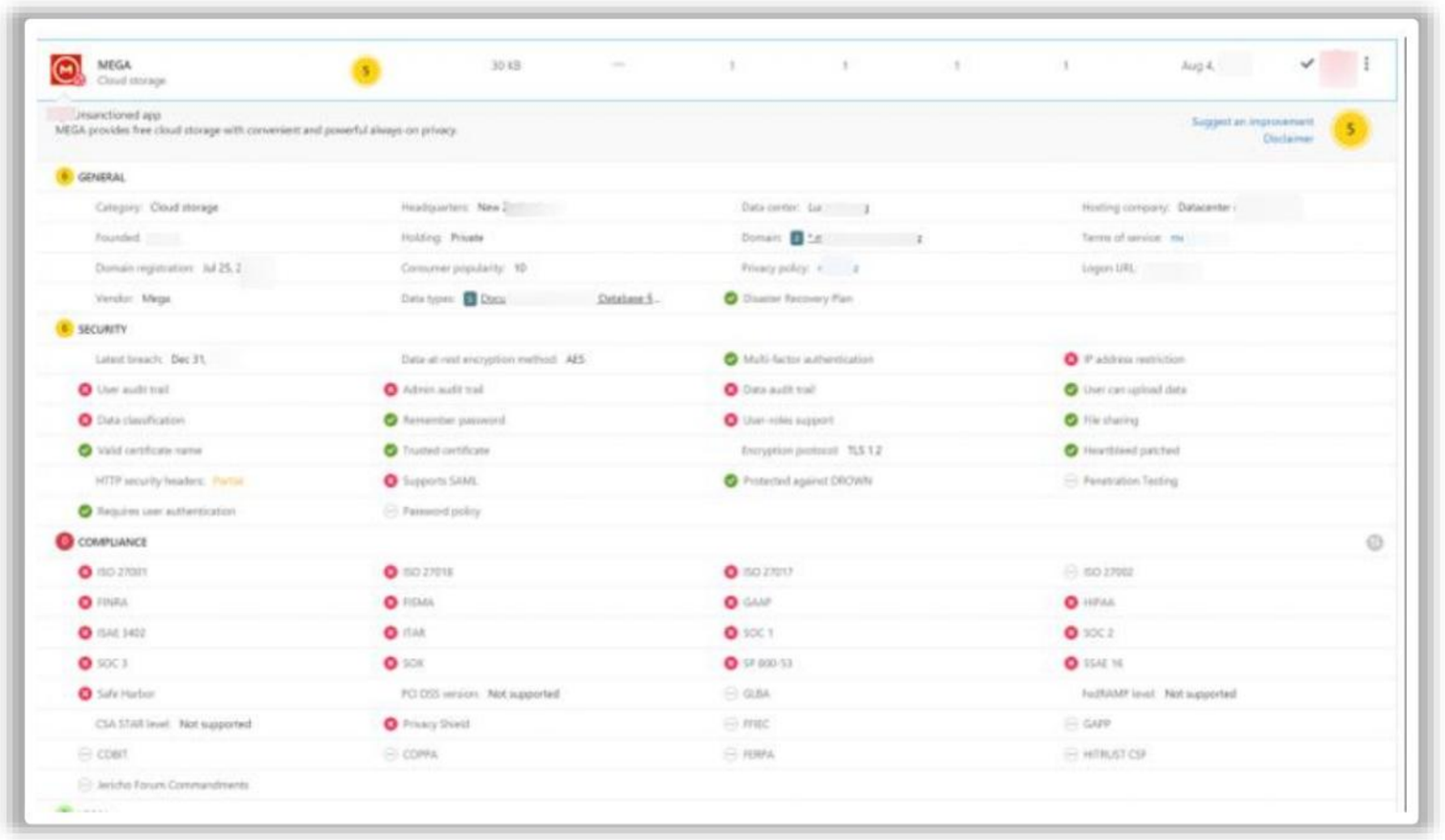


FIGURE 3.163: Cloud Storage

- **Cloud security posture management:** Use MCAS to detect and investigate all security configuration gaps by considering all cloud platform security configuration recommendations.

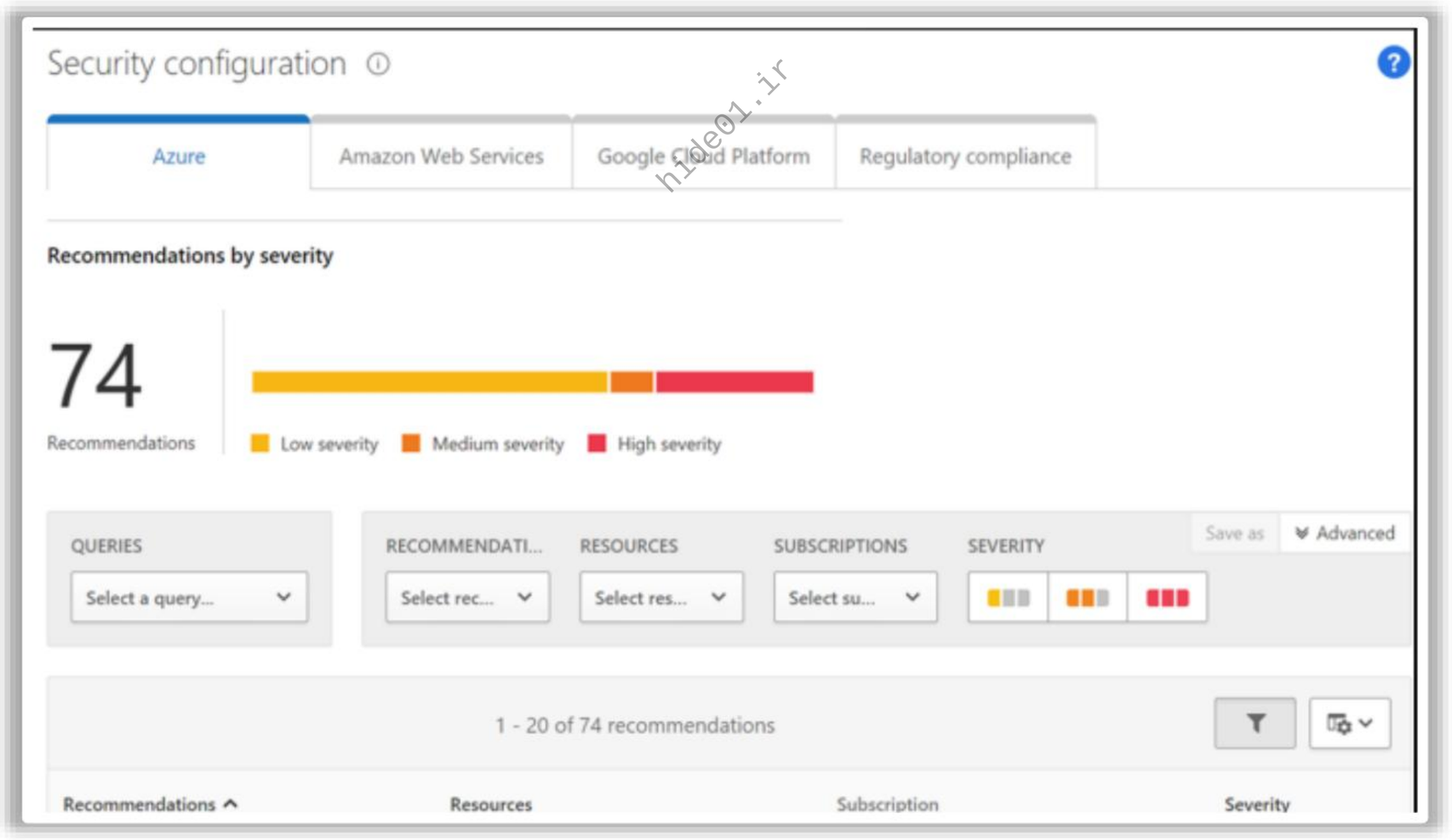
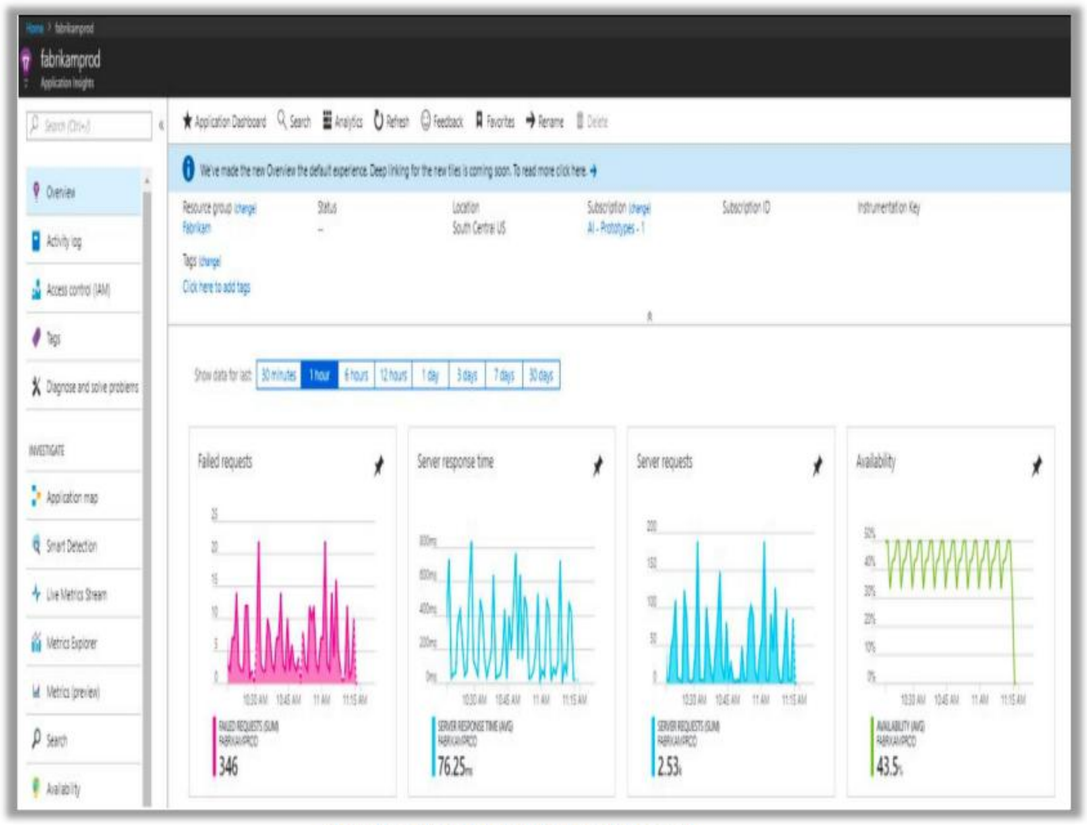


FIGURE 3.164: Security Configuration

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Detection and Respond to Threats Using Application Insights

- The application performance management (APM) Service "Application Insights" is a feature of Azure Monitor
- It monitors live applications and detects performance anomalies
- Application Insights monitors the response time and failure rates to find whether external services are slowing the application
- The performance and page views are monitored by Application Insights, which are reported by user browsers
- It provides smart detection and manual alerts to detect the applications deviation from expected behavior



Application Insights Dashboard

Source: https://www.microsoft.com

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

Detect and Respond to Threats Using Application Insights

Azure Monitor's Application Insights feature increases visibility into how applications function or perform. Use Application Insights to monitor the performance, availability, and usage of applications hosted on Azure or on-premises. It provides deep insights into operations of application by using the powerful data analysis platform of Azure Monitor. Use Application Insights to identify errors and flaws in application performance before they are found by users. It provides smart detection and manual alerts to detect the applications' deviation from normal behavior. Application Insights monitors the response time and failure rates to find whether external services are slowing the application.

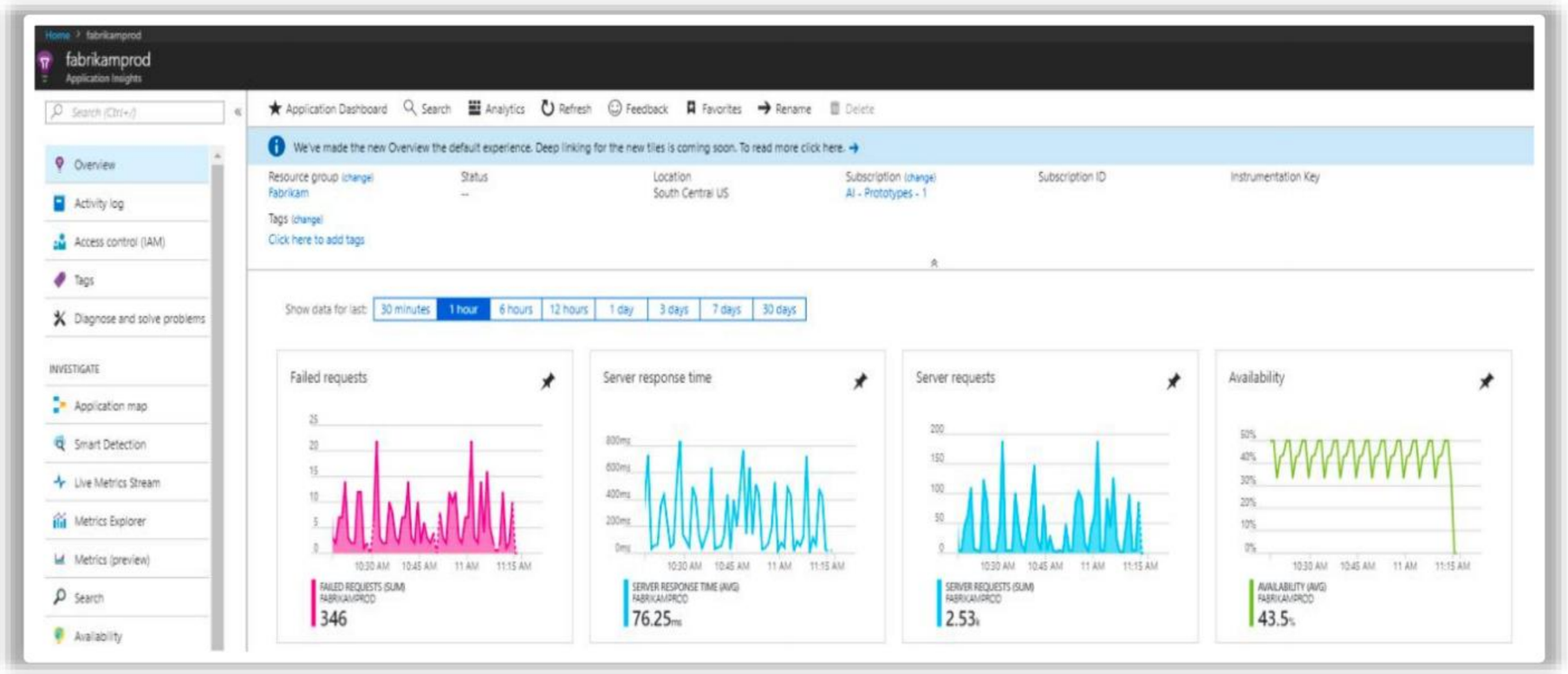


FIGURE 3.165:Application Insights

Source: https://www.microsoft.com

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Key Features and Advantages

The features Application Insights offers are listed below.

- **Continuous monitoring**: Monitors apps and servers when they slow down to identify the problem. It sends the performance statistics to the Azure portal after collecting them from the Windows performance counter. It monitors live applications and detects performance anomalies.
- **Host and performance diagnostics**: Provides host and performance diagnostics, which helps in understanding what is happening in applications.
- **Trace logs**: Monitors diagnostic trace logs from applications to correlate trace events with requests.
- **Monitoring and logging of user sessions**: Enables monitoring and logging of user logins and user sessions. The performance and page views are monitored by Application Insights, which are reported by user browsers.
- **Custom alert configuration**: Allows creation of custom alert configurations as per requirements.
- **Performance testing**: Provides performance testing based on web tests to detect threats.
- **Smart detection**: Provides a recommendation functionality that is powered by machine learning algorithms to detect problems in apps.

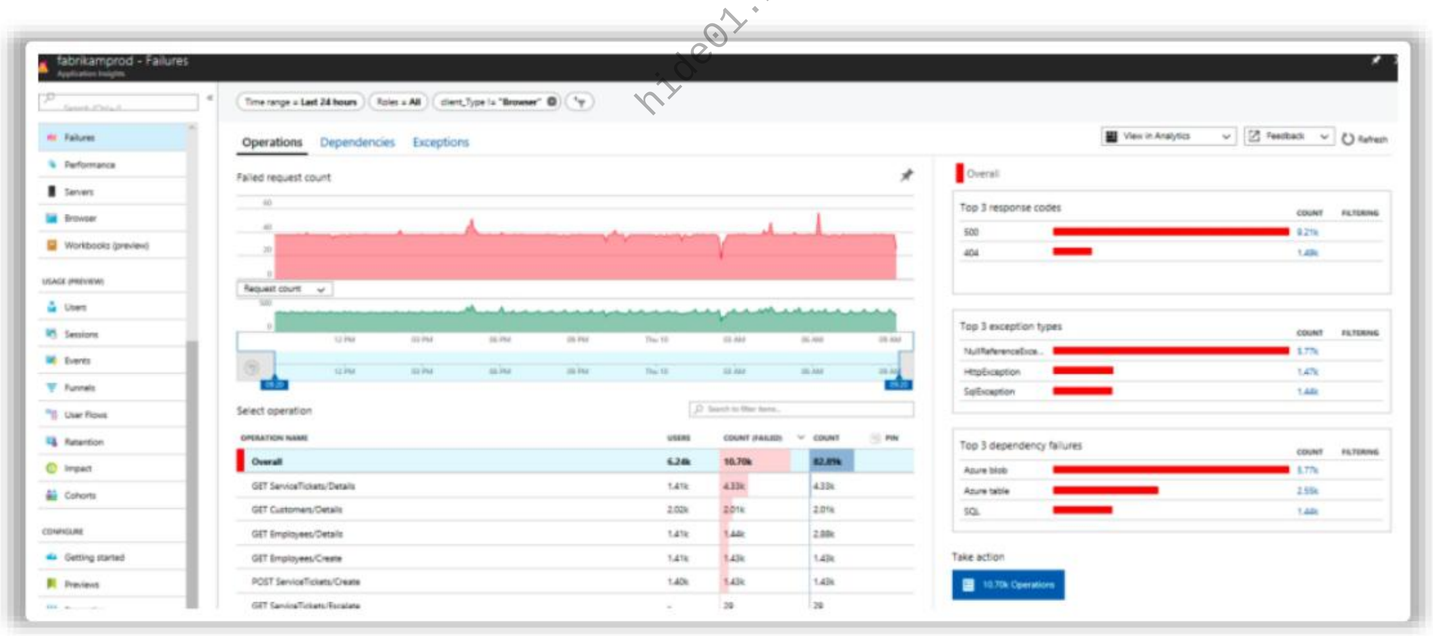
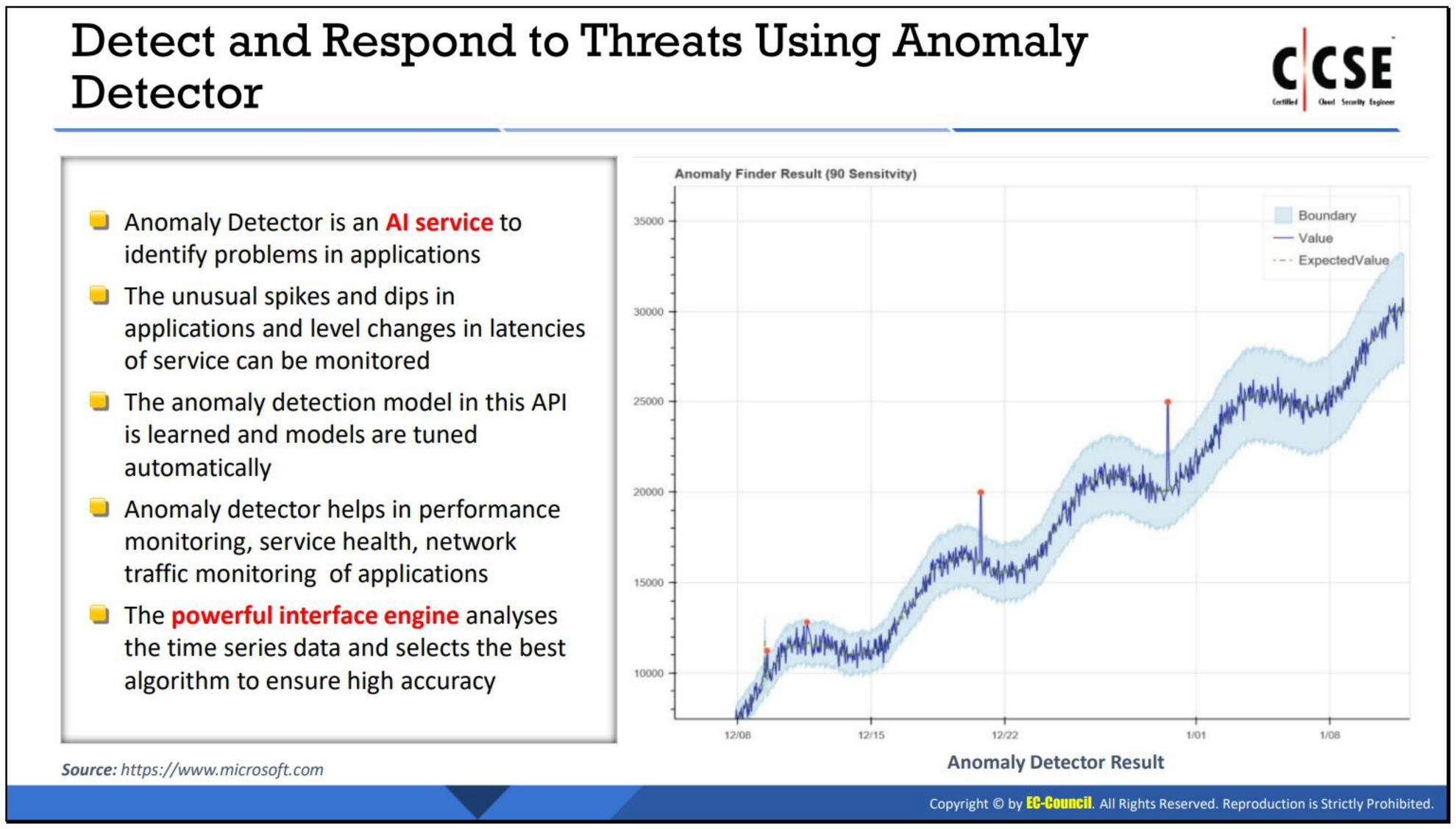


Figure 3.166: Check App Performance with App Insights

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Detect and Respond to Threats Using Anomaly Detector

Anomaly Detector API is an (AI-based) Azure service that helps monitor and detect abnormalities in time-series data without requiring any knowledge of machine learning. Embed anomaly detection capabilities into cloud applications to allow users to identify problems quickly. Any unusual spikes and dips in applications and level changes in latencies of a service can be monitored.

To ensure high accuracy, Anomaly Detector consumes multiple types of time-series data via API and chooses the best fitting detection model for a customer's data. Anomaly detector helps in performance monitoring, service health monitoring, and network traffic monitoring of applications.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

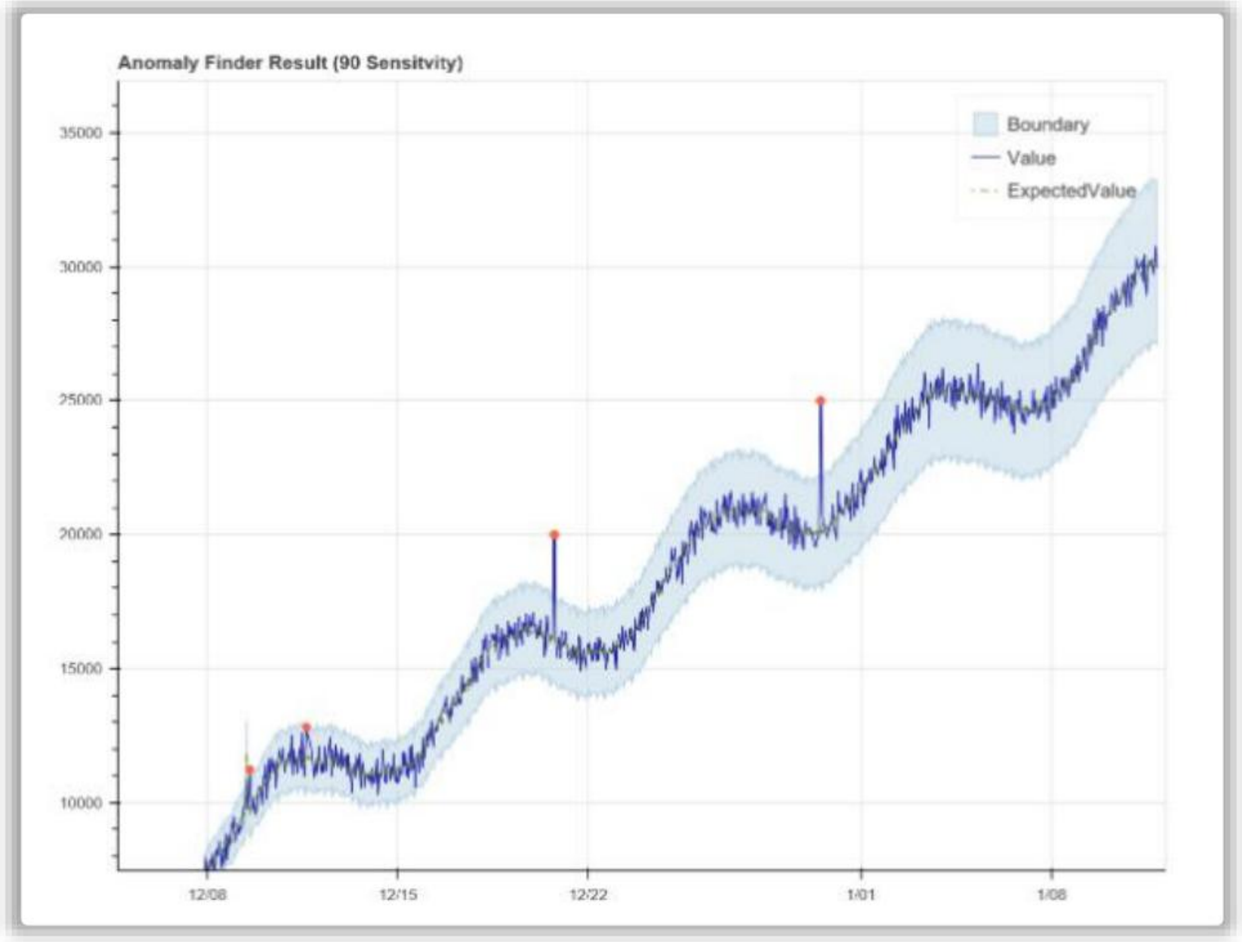


Figure 3.167: Anomaly Detector Results

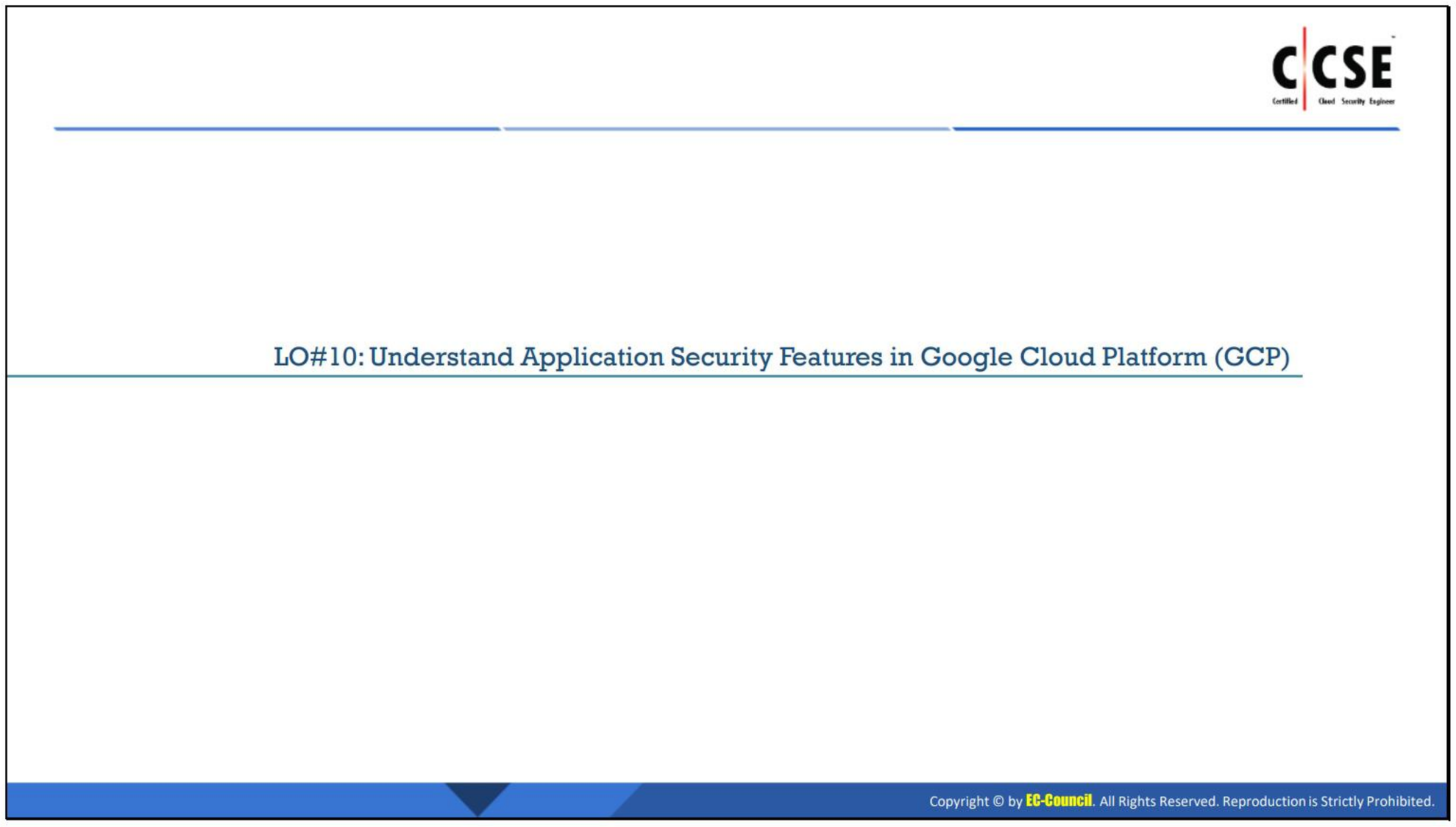
Source: https://www.microsoft.com

Key Features and Advantages

The features the Azure Anomaly Detector offers are listed below.

- **Real-time anomaly detection**: Anomaly Detector helps determine anomalies in data streaming by comparing the previously seen data point with the latest one.
- **Detect anomalies across the data set**: By using your time series, Anomaly Detector can detect anomalies present throughout your data.
- **Identify change points throughout the data set**: Identify trend change points that are present in your data by using your time series.
- **Provide detailed information about identified anomalies**: Anomaly Detector provides important information about your data and identified anomalies such as anomaly boundaries and positions, expected values, etc.
- **Create and adjust boundaries for anomaly detection**: Boundaries are created by Anomaly Detector automatically, which can be adjusted as per requirements by increasing or decreasing API's sensitivity to detect data anomalies.
- **Identify problems for any scenario**: Anomaly Detector analyzes your time-series data set and chooses an algorithm from the model gallery that is most suitable to ensure high accuracy for a particular scenario.
- **Provide automatic detection**: Anomaly Detector allows automatic detection, which removes the need for labeled training data, thereby saving time.

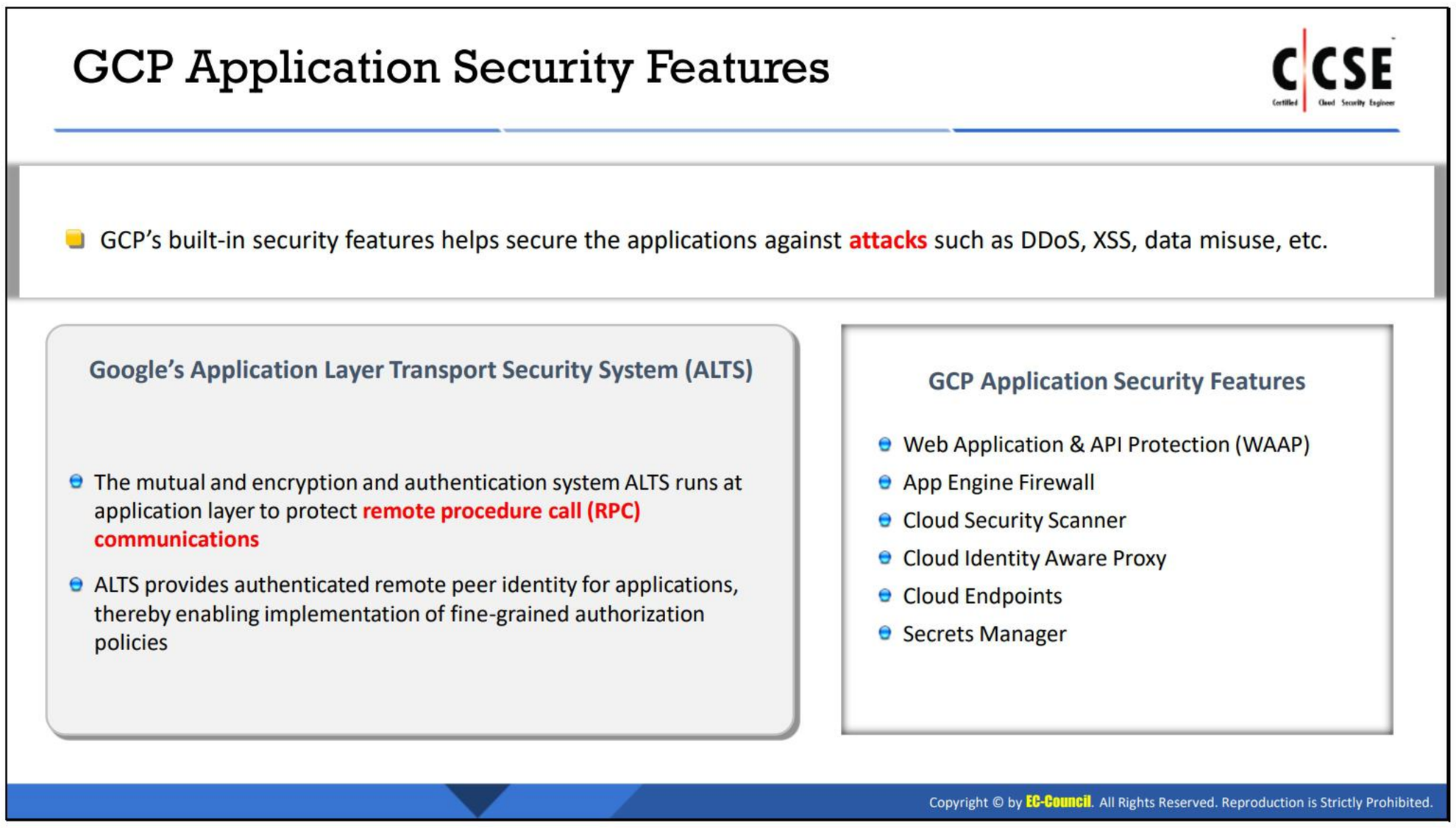
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#10: Understand Application Security Features in GCP

An understanding of how to protect App Engine apps and detect various vulnerabilities is very important to secure Google Cloud apps. The objective of this section is to explain the different security features of the App Engine to protect applications from various attacks. It describes Web Application and API Protection (WAAP), App Engine Firewall, Cloud Security Scanner, Cloud Endpoints, and Secrets Manager.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



GCP Application Security Features

Applications on GCP are prone to various attacks such as DDoS, XSS, data misuse, etc. Certain built-in security features are available with GCP, which help secure the applications against attacks. The application-level security of GCP uses Google's Application Layer Transport Security System (ALTS), a mutual authentication and transport encryption system to secure RPC communications. Implementation of application-level security allows applications to have authenticated remote peer identity, and thus fine-grained authorization policies can be implemented. ALTS is easier to monitor for security vulnerabilities and bugs than TLS. The features and services available in GCP for application security are listed below.

- **Web Application & API Protection**: WAAP includes Cloud Armor, reCAPTCHA Enterprise, and Apigee, which help keep applications secure from DDoS and bot attacks.
- **App Engine Firewall**: The App Engine Firewall can be used to control access to the App or engine app, or to deny or permit certain web requests.
- **Cloud Security Scanner**: Cloud Web Security Scanner identifies application vulnerabilities in App Engine, Google Kubernetes Engine (GKE), and Compute Engine applications.
- **Cloud Identity Aware Proxy**: Cloud Identity Aware Proxy can be used to control access to cloud-based applications.
- **Cloud Endpoints**: Cloud Endpoints can protect and monitor the APIs.
- **Secrets Manager**: The sensitive information like API keys, passwords can be stored securely by the Secrets Manager.

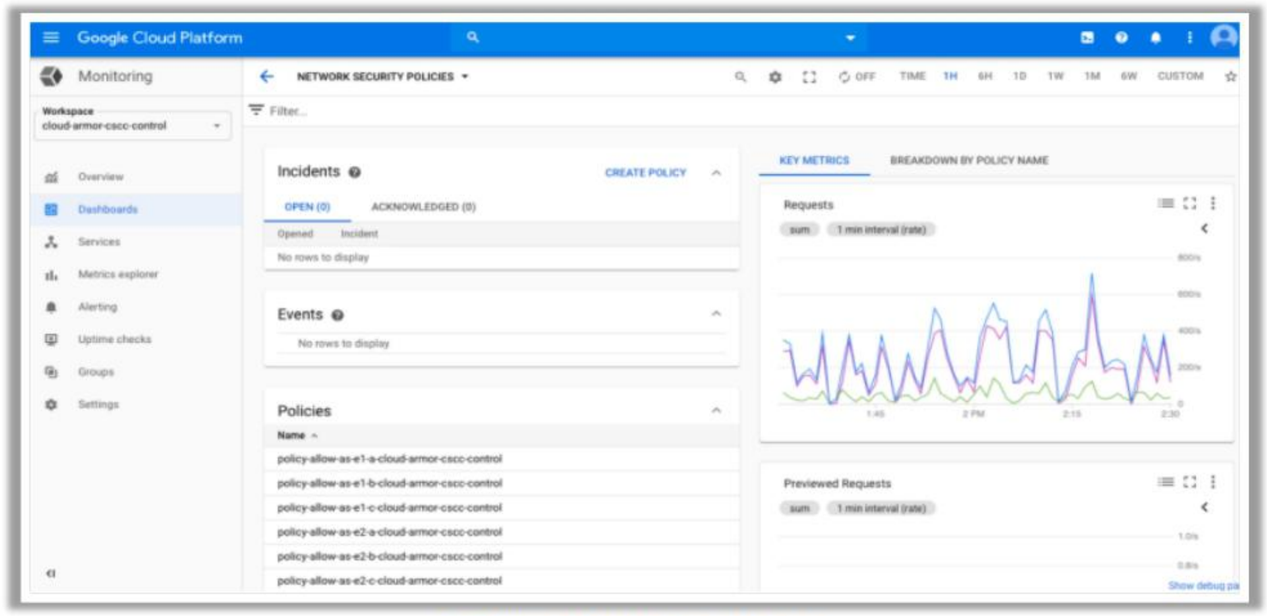
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Web Application and API Protection (WAAP)

- Web Application and API Protection (WAAP) protect web applications and APIs against existing and emerging threats
- WAAP consists of anti-DDoS, anti-bot, WAF, and API protection capabilities
- **Cloud Armor, reCAPTCHA enterprise, and Apigee** provide web applications with Anti-DDoS, anti-bot, WAF, and API protection

Cloud Armor

- The incoming web requests are **filtered** by Cloud Armor based on IP or location
- Cloud Armor can protect the applications from **DDoS attacks**
- It can mitigate most of the **OWASP Top 10 Security Risks**
- Cloud Armor also has a fully operational **Web Application Firewall (WAF)** to prevent the vulnerability exploit attempts



GCP Cloud Monitoring Dashboard

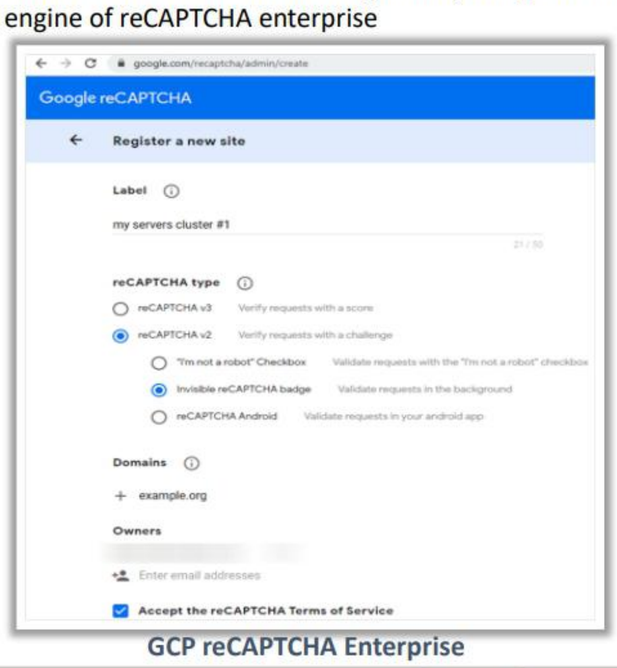
Source: *https://cloud.google.com*

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

Web Application and API Protection (WAAP) (Cont'd)

reCAPTCHA enterprise

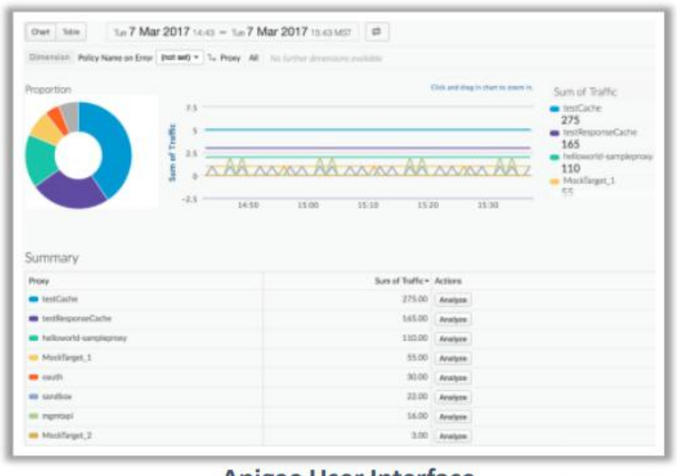
- Helps to protect the **website** against spam, abuse, and fraudulent activity
- Scraping, credential stuffing, automatic account creation can be prevented by reCAPTCHA enterprise
- Abusive activities in the site can be mitigated by using the adaptive risk analysis engine of reCAPTCHA enterprise



GCP reCAPTCHA Enterprise

Apigee

- Apigee provides an intelligent **API defence**. It can address security needs for data protection, threat detection, and access control
- It has granular role-based access controls to prevent unauthorized access to API's
- It monitors the health and security status of the API
- The Regular Expression Protection Policy can protect the applications against SQL injection attacks
- Using SAML as an authentication mechanism ensures that only the valid applications get access to the APIs



Apigee User Interface

Source: *https://cloud.google.com*

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

hide01.ir

Web Application and API Protection (WAAP)

The applications and APIs can be protected against threats and frauds and availability and compliance requirements can be met by implementing WAAP. It has anti-DDoS, anti-bot, WAF and API protection, which can protect applications against upcoming and current threats and vulnerabilities. Thus, the applications and APIs can be made security complaint and continuously available.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Armor

Cloud Armor can protect applications from web attacks and DDoS attacks. Cloud Armor provides certain predefined rules to protect the applications from XSS attacks and SQL injection. The incoming traffic can be filtered based on IPv4 or IPv6, and location-based access controls can be setup. All the metrics related to the configured security policies can be monitored on the cloud Monitoring dashboard. It can mitigate most of the OWASP Top 10 Security Risks. Google Cloud Armor allows or denies an incoming web request based on the configured security policy rule. Cloud Armor also has a fully operational WAF to prevent vulnerability exploit attempts.

Setting Up Cloud Armor to Secure the Application

Step 1: Set up Google Cloud Armor.

- Open Google Cloud Console, go to **Network Security** and click on **Cloud Armor.**
- Click **Create Policy**

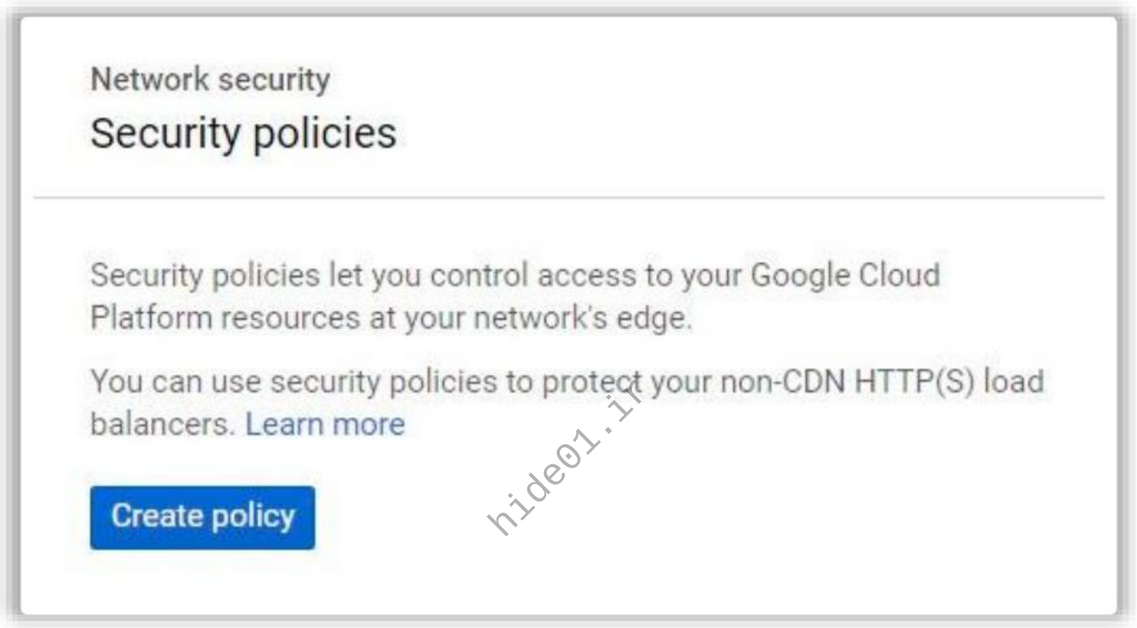


FIGURE 3.168: Create Policy

Step 2: Create Cloud Armor security policy.

- Enable the reCAPTCHA Enterprise API.
- In the name field, type the name of the policy.
- Type a description of the policy.
- Select **Allow** or **Deny** for the **Default Rule Action.**

  (**Note**: If a deny rule is creating choose Deny Status.)
- Click **Next Step.**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

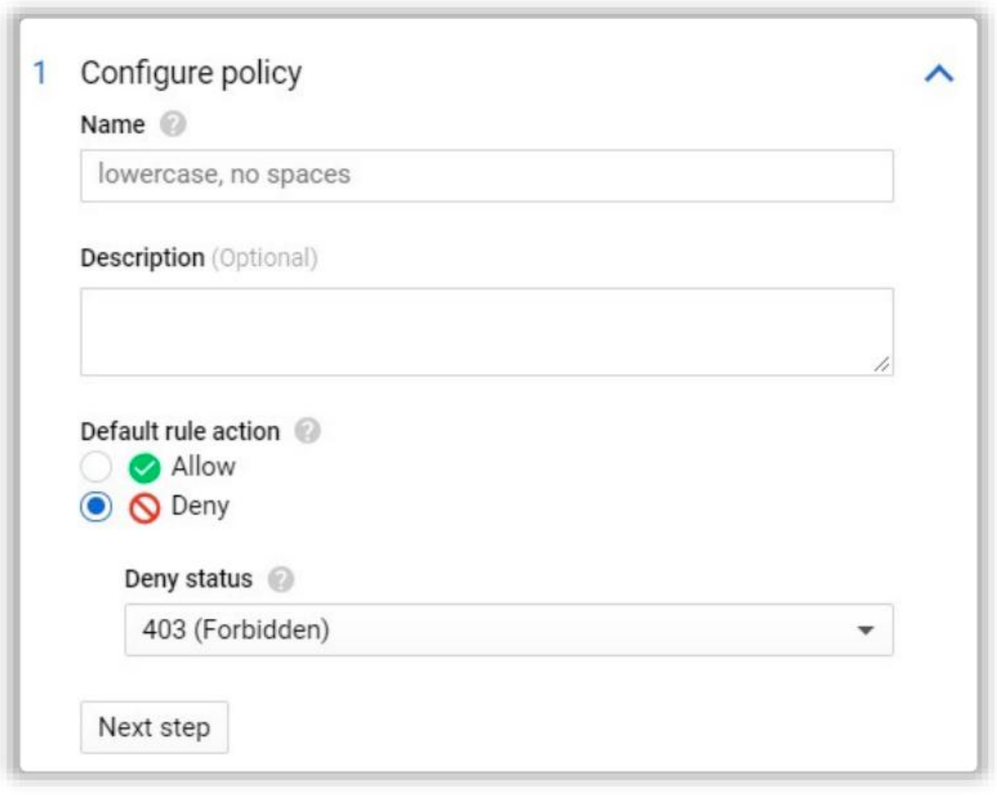


FIGURE 3.169: Configure Policy

Adding More Rules

- Type a description of the rule.
- In **Match** field, type 1 to 5 IP address ranges to match the rule.
- Depending upon the rule, choose **Allow** or **Deny.**
- To enable the rule, click the checkbox **Enable**.
- Give priority for the rule in the **Priority** field.
- Click **Done.**
- If more rules are to be added, Click **Add Rule.**
- Click **Next Step.**

Step 3: Apply policy to targets.

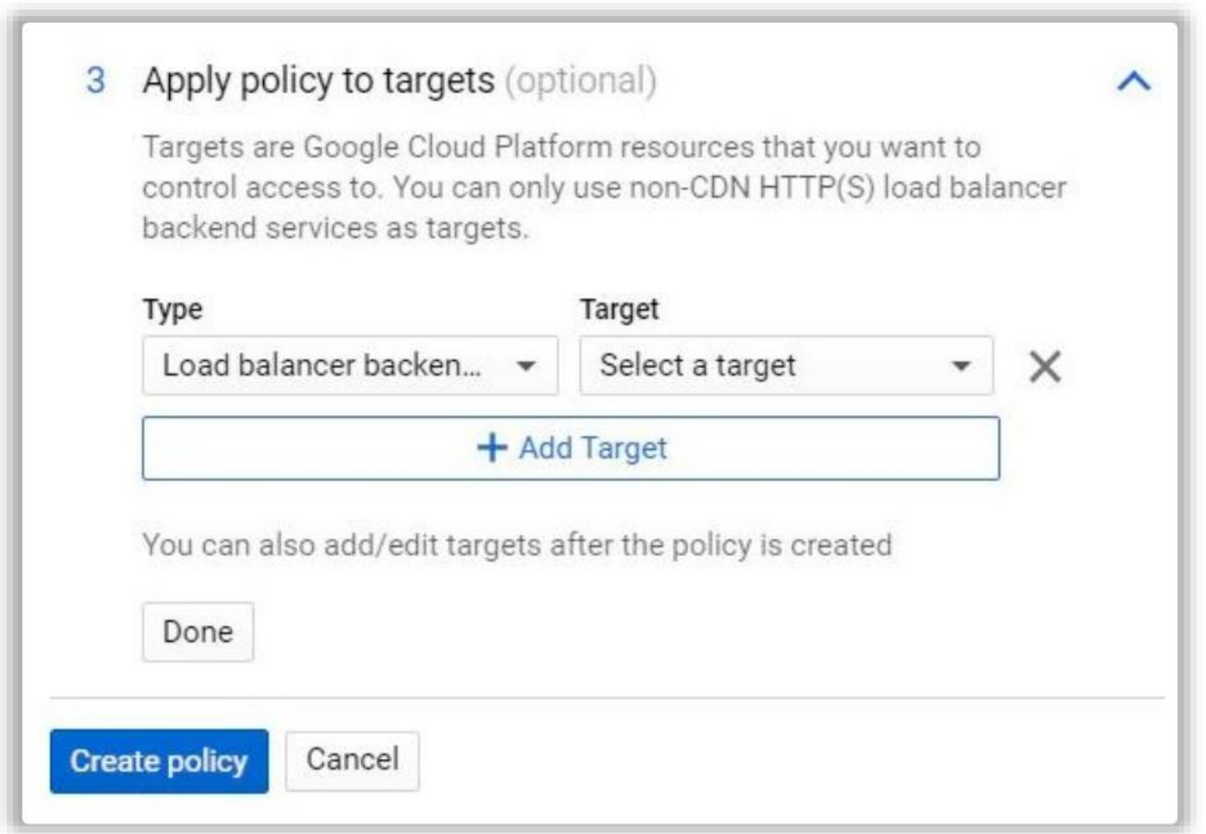


FIGURE 3.170: Apply Policy

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

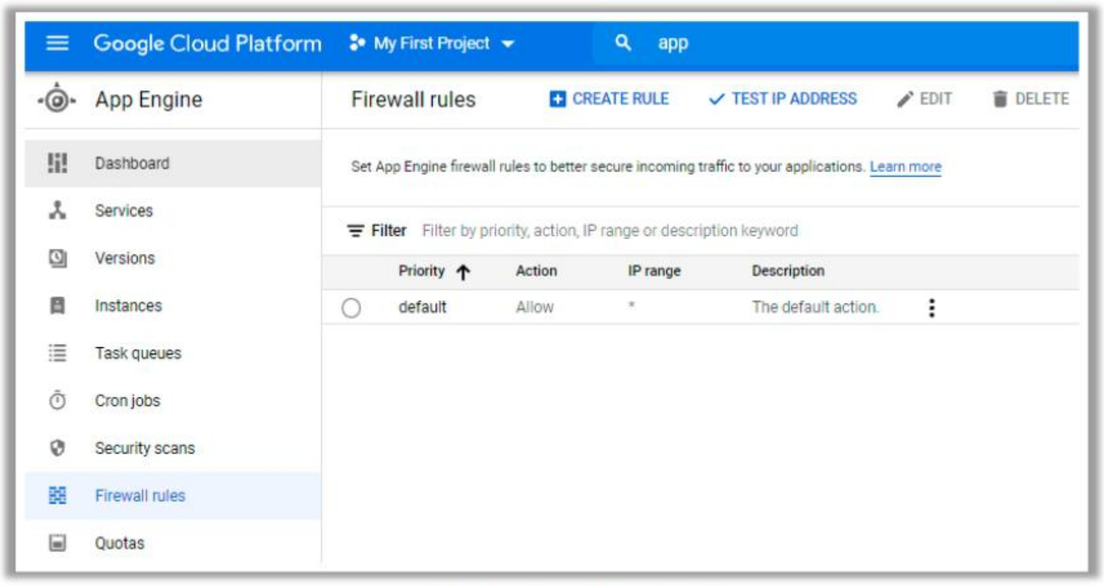
- Enable the reCAPTCHA Enterprise API.
- Click on **Add Target.**
- From the dropdown list, select a target.
- Click **Add Target** if more targets need to be added.
- Click **Done** and click **Create Policy.**

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

App Engine Firewall

- The App Engine Firewall can be used to control access to the **App engine app** and to deny or permit certain web requests
- It can be configured to allow traffic from within a network, traffic from a specific service, and blocking abusive IP addresses
- App Engine Firewall allows up to **1000 unique firewall rules**



Setting App Engine Firewall Rules

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

App Engine Firewall

The App Engine Firewall can control access to the App Engine App with a set of rules that deny or allow requests from a specified range of IPs. App Engine Firewall allows up to 1000 unique firewall rules. The Firewall can be created to do the following:

hide01.ir

- **Allow traffic from a specific network:** Certain ranges of IP addresses from specific networks can access the application. For example, during the testing phase of the application, rules can be created to allow only the IP address range within the private network of the organization. Then, the rules can be modified during the release accordingly.
- **Allow traffic from a specific service:** The traffic to the App Engine App should be proxied through a WAF to proxy the requests to the application.
- **Block abusive IP addresses:** Applications can be protected from IP addresses with malicious intent. They can be protected from DDoS attacks by blocking traffic to the application using the App Engine Firewall.

Ingress Controls

Applications receive requests only from specific sources if they are configured with network ingress controls.

- **All**: The applications receive all traffic.
- **Internal only**: Applications receive requests sent from VPC networks in the same project.
- **Internal and Cloud Load Balancing**: The application receives requests routed through Cloud Load Balancing or VPC networks in the same project.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Source: https://console.cloud.google.com

Creating Firewall Rules in Console

Following are the steps to create firewall rules:

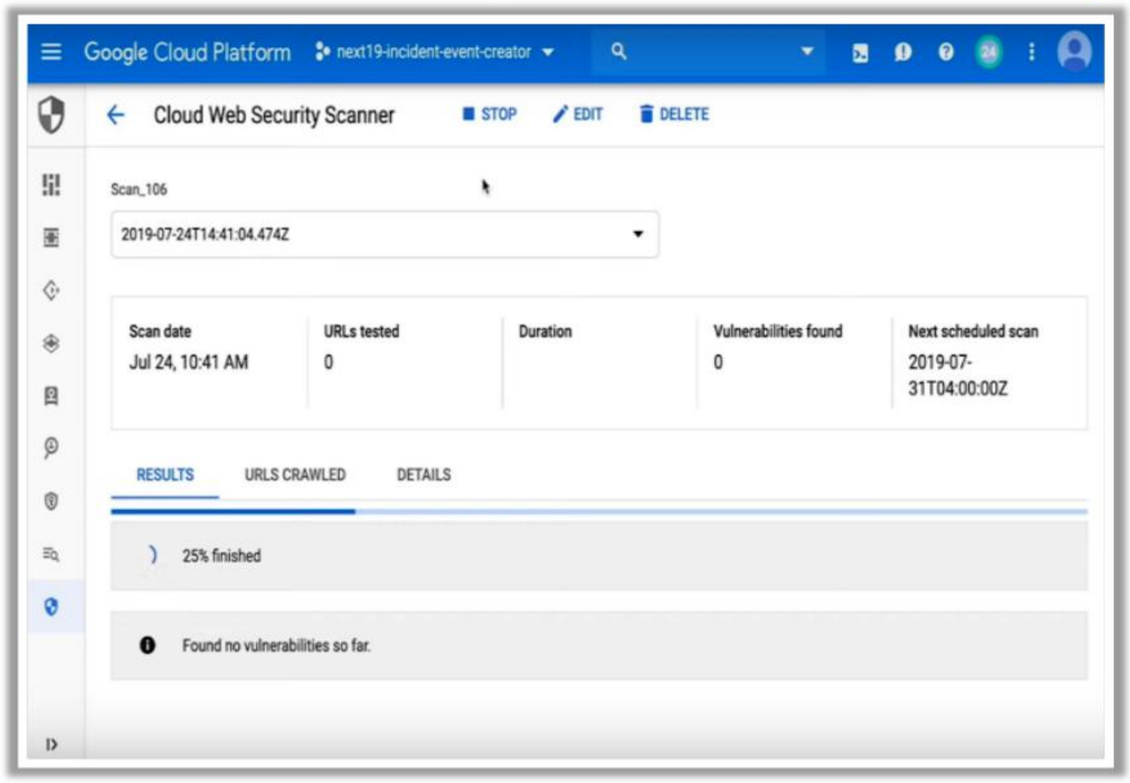
- Select **Go To the create a firewall rule page** in the console.
- Give the details of the firewall rule:
  - Under **Priority,** give the value to specify the importance of the rule and define the order of when rule is evaluated
  - Under **Action on Match,** specify allow or deny access for requests that match the rule.
  - Under **IP Range,** define the IP address range.
  - Under **Description** (optional), including the description of the rule.
- Click **Save**.
- Test the rule.
  - Click **Test IP Address.**
  - Enter the IP address that needs to be evaluated.
  - Click **Test**.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Security Scanner

- Cloud Web Security Scanner identifies **application vulnerabilities** in App Engine, Google Kubernetes Engine (GKE), and Compute Engine applications
- It crawls the application within the scope of the starting URLs
- Web Security Scanner does not display low-confidence alerts; thus, there are no false positives
- Managed scans in Security Scanner provide management of basic web application vulnerabilities
- The custom scans in Web Security Scanner provide information about outdated libraries, cross site scripting, etc.



Google Cloud Web Security Scanner

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

Cloud Security Scanner

The vulnerabilities and threats in the web applications hosted in App Engine, GKE, and Compute Engine are identified by the Web Security Scanner. The Scanner crawls the web applications by including the links associated with the URL, the user input and event handlers. Web Security Scanner does not display false positives. It does not display low-confidence alerts and hence there is no under reporting.

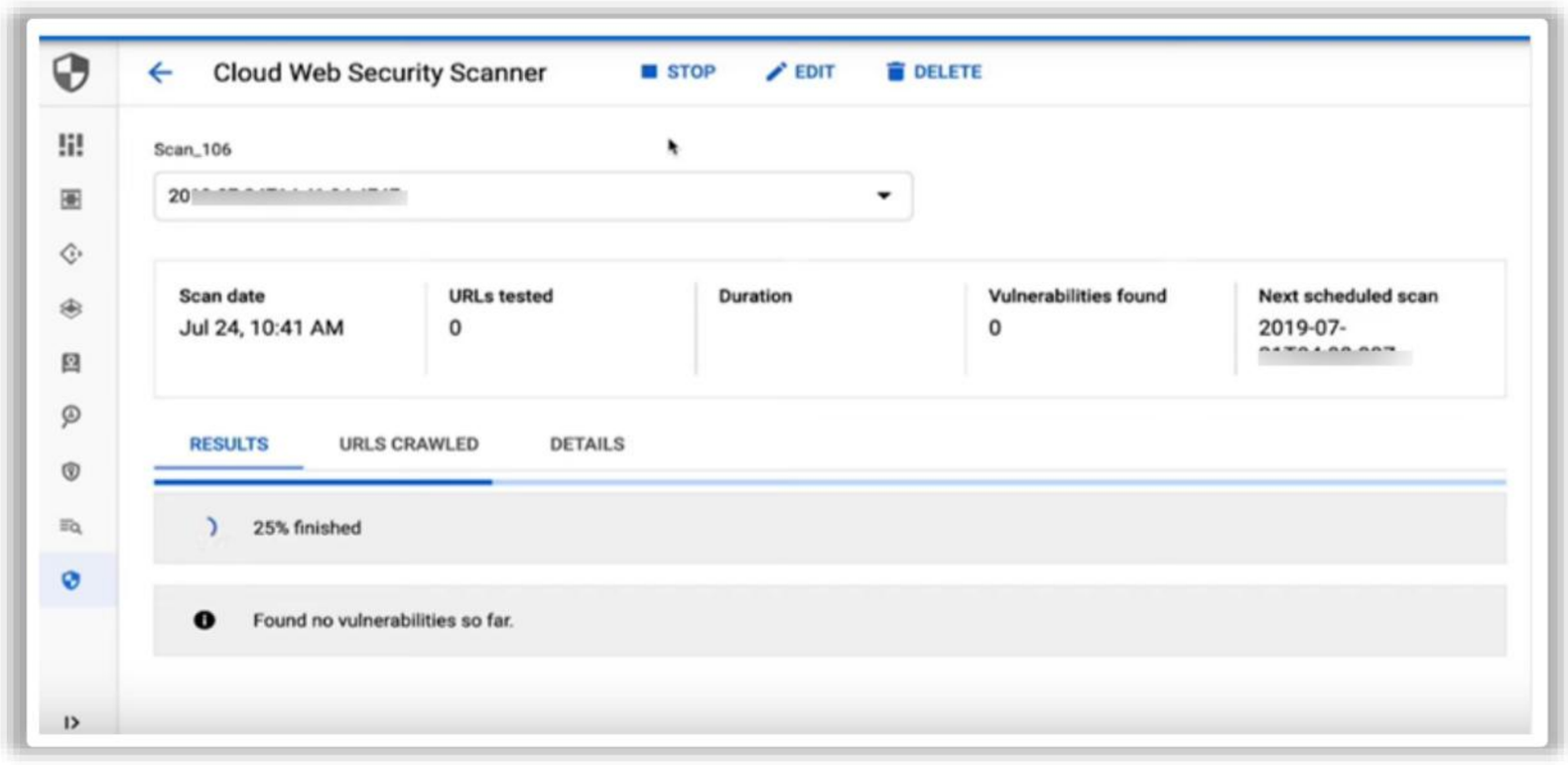


FIGURE 3.171: Cloud Web Security Scanner

Web Security Scanner provides two scan types: **Managed** and **Custom** scans**.**

Managed Scans

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Managed scans are configured by the Security Command Center and it scans public facing endpoints. Managed scans do not use any authentication. Managed Scans send GET requests and they will not submit forms in live websites. Managed Scans are used for central management of web application vulnerability detection.

Reviewing Managed Scans in Security Command Center

Managed scans in Security Scanner provide management of basic web application vulnerabilities. Managed Scan reports are available in Security Command Center vulnerabilities tab and related reports, when the Web Security Scanner is enabled as a service.

Source: https://console.cloud.google.com

Steps to Review Managed Scans

- In the Google Cloud Console, go to Security Command Center **Findings** Tab.
- Select **View By** and click **Source Type.**
- Select **Web Security Scanner** in the **Source Type** list.
- Click the finding name under **Category**. The finding details display information such as:
  - What was the event.
  - When the event occurred.
  - Event Severity.
  - Affected URL.

hide01.ir

Viewing Managed Scans Configuration for a Project

- Click on the **Web Security Scanner** page in the console.
- Select a project, a page appears with a list of managed and custom scans.
- Click Managed Scans under **Scan Configs.**
  - The page that appears shows scan status, crawled URLs, and vulnerabilities.

On-Demand Scans

  - Select **Web Security Scanner** page in Console.
  - Select Projects.
  - Click managed scans under **Scan Config.**
  - Click **Run.**
  - In the results tab, click on **Run Scan Again.**

Custom Scans

Custom scans help identify application vulnerabilities such as outdated libraries, cross-site scripting, etc.

Enabling Web Security Scanner to run Custom Scans

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 1: Deploy a test project.

Step 2: Assign IAM roles.

- Move to the **IAM & Admin** page in the console.
- Click the **Project Selector** dropdown list
- Select the project to scan from the **Select From** dialog box.
- On the **IAM** page, Click **Edit** to edit username.
- Click **Add Another Role** in **Edit Permissions** panel and select either
  - **Project > Owner**
  - **Project > Editor**
- Click **Save.**

Step 3: Run the scan.

- Move to the **Web Security Scanner** page.
- Select the project with the application which is to be scanned.
- Click **New Scan**.
- The **Create a New Scan** page loads,
  - Enter the URL of the application to be scanned under **Starting URLs.**
  - Select **Weekly,** under **Schedule.**
  - Select a date under **Next Run on.**
- Click **Save.**
- Click **Scan Name** to load the overview page, click **Run Scan.**

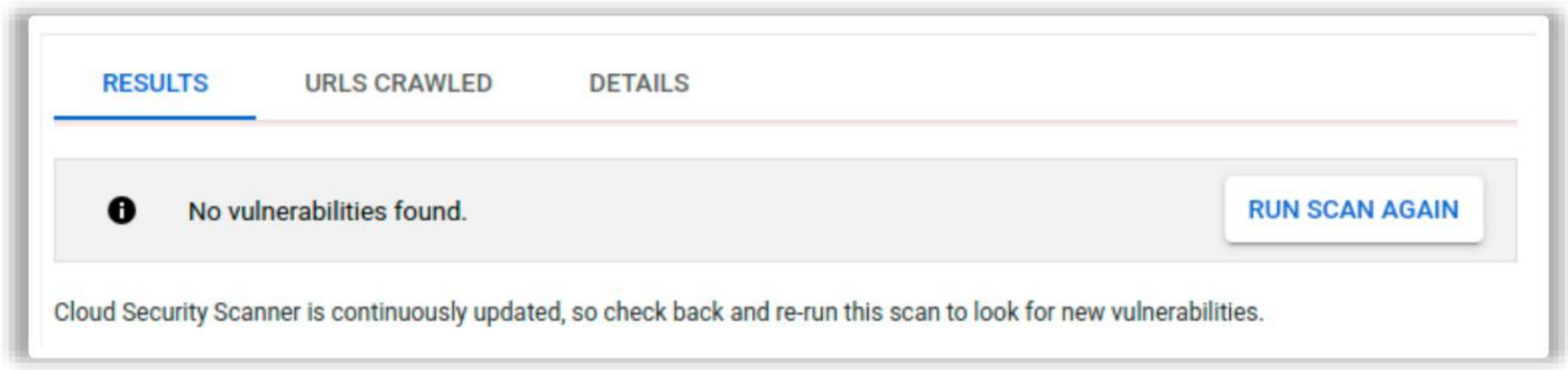


FIGURE 3.172: Run Scan

Scanning an Application Using Test Account

Following are the steps to scan an application using test account:

Step 1: Create a test account.

- The test account is the best to use for scanning the application as it does not have access to sensitive data.

Step 2: Create a scan.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Move to **Web Security Scanner**.
- Click on **Select** and select a project that already has an application deployed.
- Click **Create Scan** or **New Scan.**
- Add new values to the new scan form.
- Click **Create.**

Step 3: Run the scan.

- Sign into the test account.
- Move to the **Web Security Scanner** Page.
- Click **Select** and select the project that is created the scan in.
- Choose the name of the scan under **Scan Configs.**
- Click **Run.**

Viewing Custom Scan Results

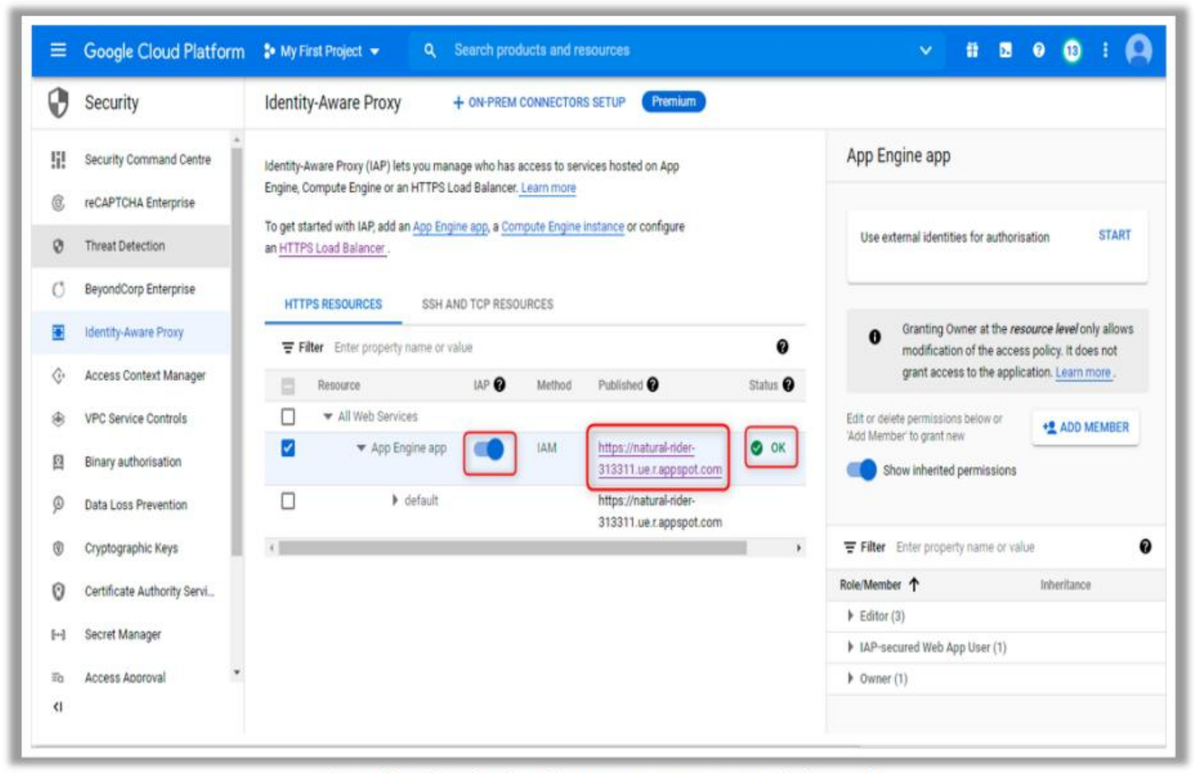
- Sign into the test account.
- Move to the **Web Security Scanner** Page.
- Click **Select** and select the project that contains the scan.
- Choose the name of the scan to be reviewed under **Scan Configs.**

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Identity Aware Proxy

- Cloud Identity Aware Proxy can be used to control **access** to cloud-based applications
- Based on user identity, device security status granular access control policies can be enforced
- Cloud IAP is a fast and reliable way to access the application without the use of a VPN
- Simple access control policies can be applied to the web applications by selecting users
- Cloud IAP can be used with IAP Connector to protect own premises applications



Google Cloud Identity Aware Proxy Dashboard

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

Cloud Identity Aware Proxy

Cloud Identity Aware Proxy manages access to applications by verifying the user identity and context. It provides secure access to the applications without the use of a VPN. It allows only authorized users to access an application by intercepting the requests made to the application and authenticating the user. Granular access control policies can be implemented on the application based on the identity of the user, device security, and IP address. Simple access control policies can be applied to the web applications by selecting the users. Cloud IAP can be integrated with IAP connector to protect on-premises applications.

Source: https://console.cloud.google.com

Enabling Cloud Identity Aware Proxy

Following are the steps to enable Cloud IAP:

Step 1: Select project.

- Move to the **Identity Aware Proxy** page.
- Select the project to which the application is deployed to enable IAP.

Step 2: Configure the OAuth consent screen.

- Move to the **OAuth Consent** screen.
- Select the email address to display as a contact under **Support email**.
- Give the **Application Name.**
- Click **Save.**

Step 3: Set IAP access.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

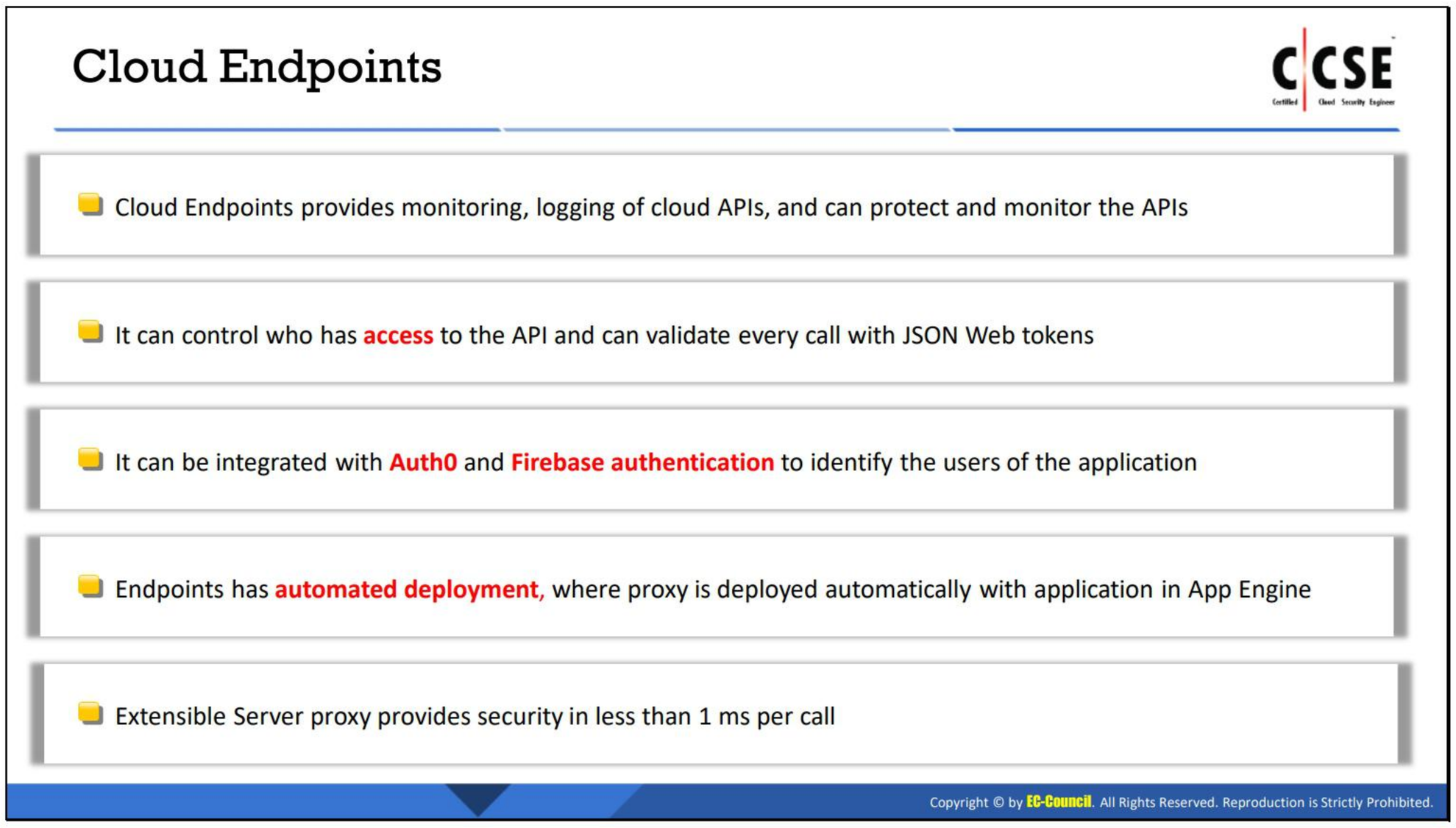
- Move to the **Identity Aware Proxy** page.
- Select the resource to be modified by checking the box.
- Click **Add Member.**
- In the **Add Members** dialog box that appears, add the email addresses to which **IAP Secured Web App User** role is to be granted.
- Click **Add**.

Step 4: Turn on IAP.

- Move to the **Identity Aware Proxy** page.
- Under **HTTPS Resources,** search for the App Engine application to which the access has to be restricted.
- The Published column will show the URL of the app.
- To turn on IAP for the application, toggle the **ON/OFF** switch.
- Click **Turn on** in the **Turn on IAP** window to confirm.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cloud Endpoints

Cloud Endpoints helps in protecting and managing APIs. Cloud Endpoints is an NGINX-based proxy that provides better performance. Using Cloud Endpoints, access to APIs can be controlled and every call is validated with JSON Web tokens and Google API keys. The users of the application can be identified by integrating Endpoints with Auth0 and Firebase Authentication. Cloud Endpoints can provide insights about the usage with Cloud Trace and Cloud Logging. Extensible Server proxy provides security in less than 1 ms per call. The proxy is deployed automatically with the application while using App Engine. Containerized ESP can be used for GKE or Compute Engine.

Source: https://console.cloud.google.com

Deploying Endpoints Configuration

Follow these steps to deploy Endpoints configuration:

Step 1: Start Cloud Shell.

- Ensure you are in the project that needs to be used for the Sample API.
- Open Cloud Shell.



FIGURE 3.173: Cloud Shell

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 2: Get sample code.

- To get the sample API and scripts, enter the below command.

git clone https://github.com/GoogleCloudPlatform/endpoints-quickstart

- Change the directory which contains sample code.

```
cd endpoints-quickstart
```

Step 3: Deploy Endpoints Configuration.

- Enter the command below in the endpoints-quickstart directory.

```
cd scripts
```

- Run the below script:

```
./deploy_api.sh
```

- Endpoints uses host field in **Open API configuration** file to identify service.
- The Open API configuration can be deployed to service management by using the below command.

```
gcloud endpoints services deploy openapi.yaml
```

Step 4: Enable the required services.

- To confirm the required services are enabled, run this script:

```
gcloud services list
```

- Enable Endpoints service by using

```
gcloud services enable YOUR-PROJECT-ID.appspot.com
```

Step 5: Deploy API backend.

- Run the below script in Cloud Shell endpoints-quickstart/scripts:

```
./deploy_app.sh
```

- To deploy the sample API to App Engine, run the command:

```
gcloud app deploy
```

Step 6: Send requests to the API.

- Requests can be sent to the API by the following script:

```
./query_api.sh
```

Thus, the API is tested and deployed in Endpoints.

Tracking API Activity

Monitor the critical operations and analyze the usage with Cloud Logging by following these steps:

- Run the traffic generation script to display graphs and logs:

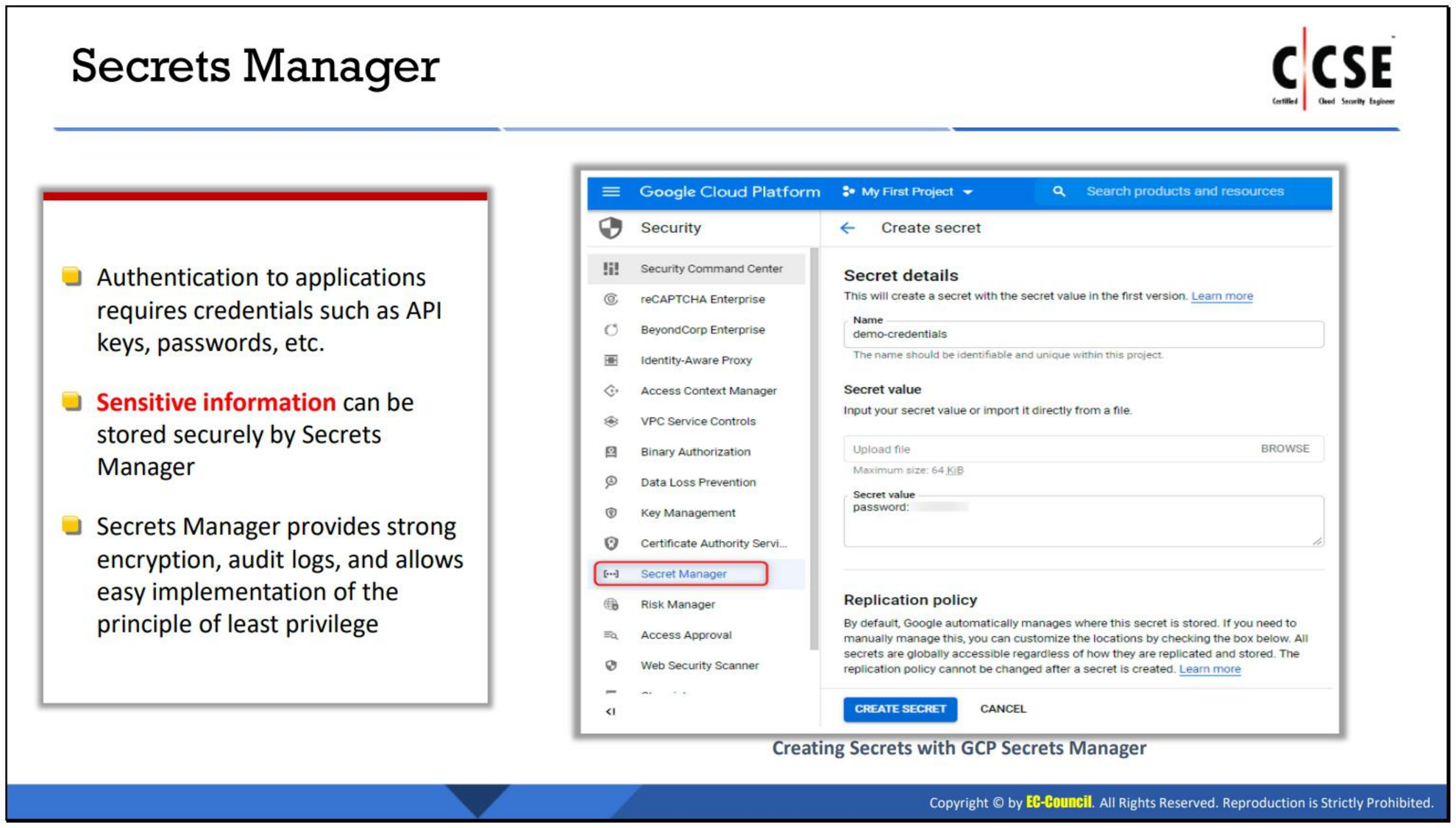
```
./generate_traffic.sh
```


Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click **+Permissions** to view who has access control to the API.
- **Deployment History** displays the history of the API deployments.
- The incoming traffic can be viewed by clicking **Overview.**
- By scrolling down to the table below graphs, Click **View Logs** for **GET.**
- The requests logs for API will be displayed by **Logs Viewer** page.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Secrets Manager

Secrets Manager can securely and conveniently store API keys, passwords, and certificates. With Secret Manager Cloud IAM role, the principle of least privilege can be effectively followed. Secrets Manager can be integrated with Cloud Audit Logs, which generates an audit log for every interaction. The logs can be ingested into anomaly detection systems to alert administrators regarding security threats and deviations from best practices. The data at rest is secured with AES 256-bit encryption and in transit with TLS encryption.

Source: https://console.cloud.google.com

Creating Secret and Secret Version

Follow these steps to create a secret and secret version:

- Go to the **Secret Manager** page via Console.
- Click **Create Secret** on the **Secret Manager** page.
- On the **Create Secret** page, under **Name,** enter my – secret.
- In the **Secret Value** field enter my super-secret data.
- Click **Create Secret.**

Accessing Contents of the Secret Version

- On the **Secrets Manager** page, click **My secret.**
- Locate version 1 in the **Secret Details** page in **versions** table.
- Click **View More** in **Actions** column.
- Click **View Secret Value.**
- Click **Done.**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Enabling API Access

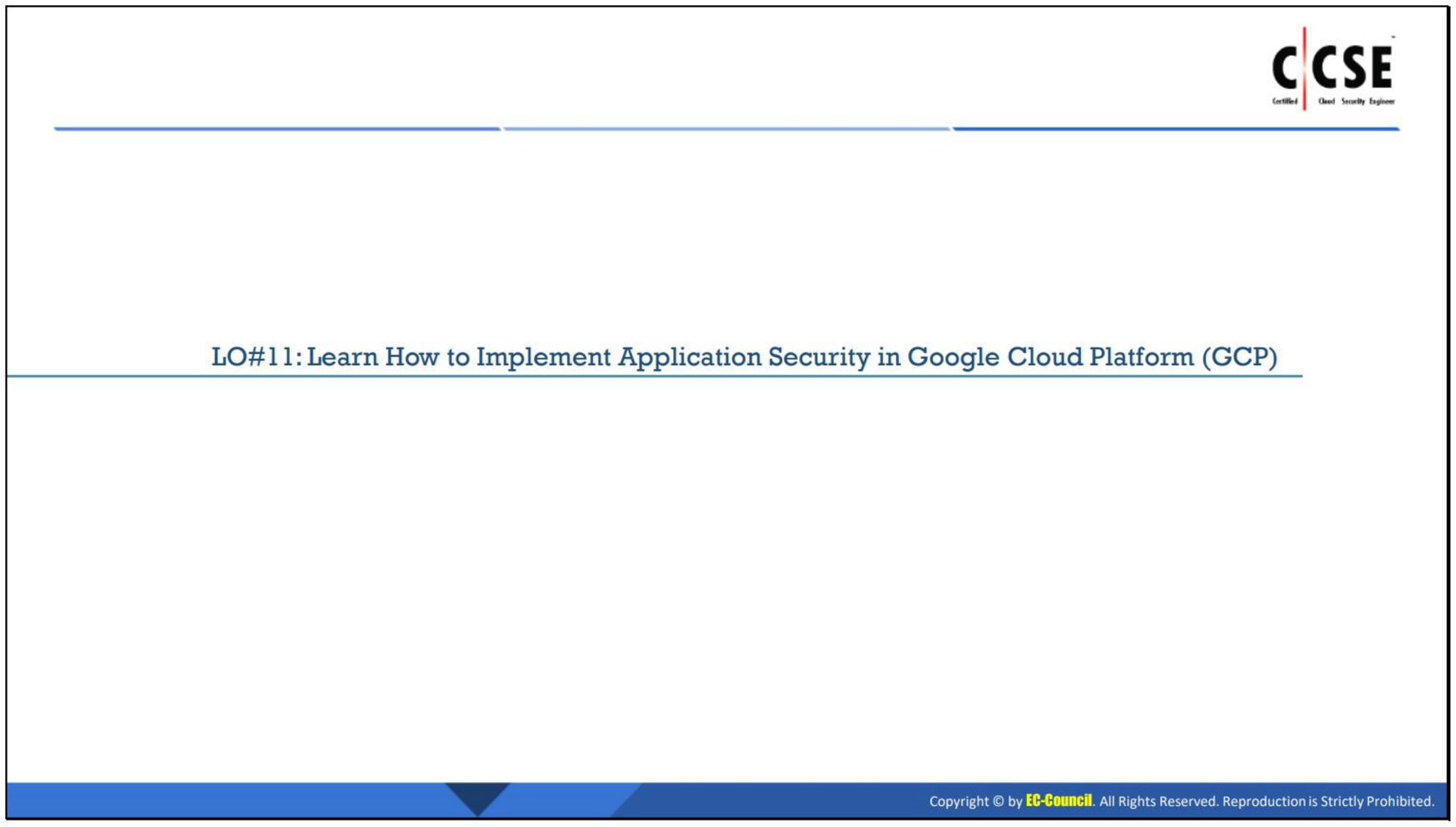
- Sign into the Google account.
- Select or create a **Google Cloud Project** on the project selector page.
- The billing should be enabled for the Cloud Project.
- Enable the API.
- Install and initialize Cloud SDK.

Additional Configuration

- To access secret manager resources from Compute Engine Instance, grant the instance OAuth scope.
- To access secret manager from App Engine, grant App Engine Service required roles.
- After the Secret Manager API is enabled to integrate Secret Manager into applications, Cloud SDK can be used. Idiomatic client libraries that permit use of secrets in applications without using Secret Manager API directly can be used.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

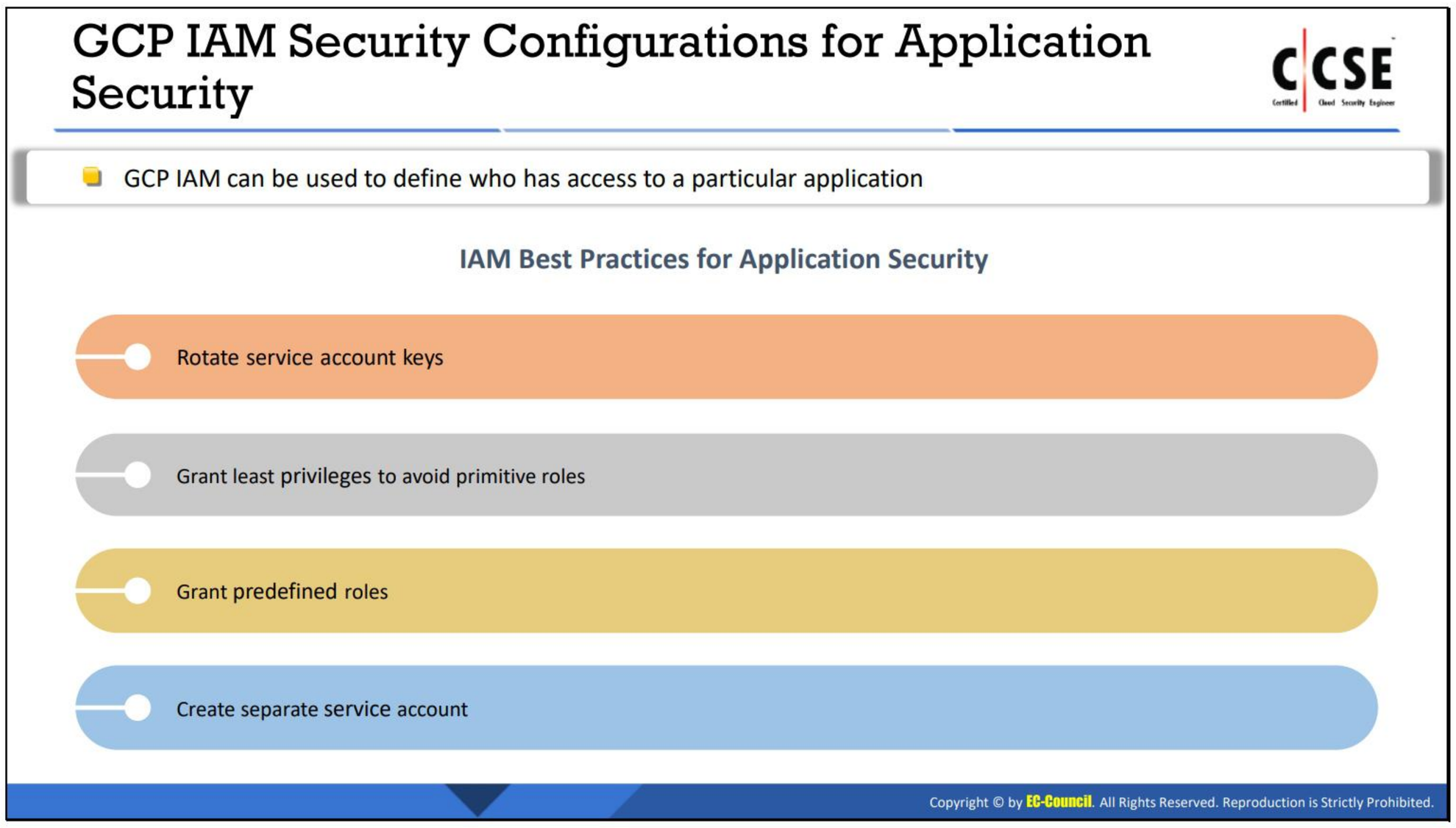


LO#11: Learn How to Implement Application Security in GCP

The objective of this section is to describe implementation of application security in Google Cloud using various services of GCP such as IAM, load balancers, and Operations Suite. It also describes the various tools and best practices for application security.

hidden1.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



GCP IAM: Security Configurations for Application Security

- The applications that run on Google Cloud are deployed securely, which delivers real defense in depth.
- Implementation of some best practices can protect the application from attacks such as DDoS, SQL injection, XSS, etc.

hade01.ir

The application security implementation can be done in GCP by considering the following factors:

- **IAM security configurations**: To implement the principle of least privilege.
- **Securing application infrastructure**: The infrastructure on which the application is hosted can be protected.
- **Detection and response**: To detect and mitigate attacks during the running of the application without compromising availability for legitimate users.

IAM Security Configurations for Application Security

GCP IAM provides granular access to users with PoLP (principle of least privilege) security for the essential Google Cloud resources.

GCP IAM model consists of three major divisions:

Member

A member of GC IAM could be a Google account, service account, Google group, Google Workspace, or cloud identity domain with an identity to access the Google Cloud resource. In Google account, Google group, and service account, the identity is an email address, whereas in Google Workspace and cloud identity domain, the identity is the domain name.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In cloud IAM, the following members are included:

- Google account: Google account constitutes a developer, an administrator, or any individual who connects to the Google Cloud with an identity such as an email address.
- Service account: A service account is a special account that belongs to an application or VM instance, but not to end-user, to run the specified account code hosted in Google Cloud. Multiple service accounts can be created for different logical components of an application.
- Google group: Google group consists of Google accounts and service accounts. It has a unique email address, which can be viewed by clicking on About on the Google group homepage. It is not possible to establish an identity for a Google group to access resources because it does not have login credentials.

  It is easy to apply a policy to the whole group through the Google group. The access control of the entire group can be easily set and members can be added or removed from the Google group without updating the GCP IAM policy.
- Google Workspace domain: The Google Workspace account of an organization has a Google Workspace domain, which is a virtual group comprising all Google accounts of an organization. The Google Workspace is an internet domain of an organization such as example.com. If you add a user to the Google Workspace domain, then a new Google account is created in the virtual group such as **username@example.com**
- Cloud identity domain: The cloud identity domain of an organization is a virtual group of all Google accounts. The users of the cloud identity domain cannot access the Google Workspace domain applications.

ridery.ir

Role

Role is a set of permissions. Note that permissions cannot be directly assigned to a user; instead, they are granted by assigning roles to the user, group, or service account.

Permissions

Permissions determine the accessibility of resource operations. They can be represented as <service>.<resource>.<verb>. For example, pubsub.subscriptions.consume.

Permissions are generally correlated one-to-one with the REST API method and each Google Cloud service is associated with the collection of permissions for each exposed REST API method. Therefore, the users need permission to call that method. For example, Google Cloud Pub/Sub exchanges messages between independent applications. If a user wants to use Pub/Sub and call the *topics.publish()* method, then they should have the pubsub.topics.publish permission related to that topic.

If a user wants access to Google Cloud resources such as projects, Compute Engine instance, and cloud storage bucket, then a role limited to that resource is granted to the user.

For some service support, there is a need to grant cloud IAM permissions at fine-grained levels instead of the project level. For example, the user of a specific cloud storage bucket is given the

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

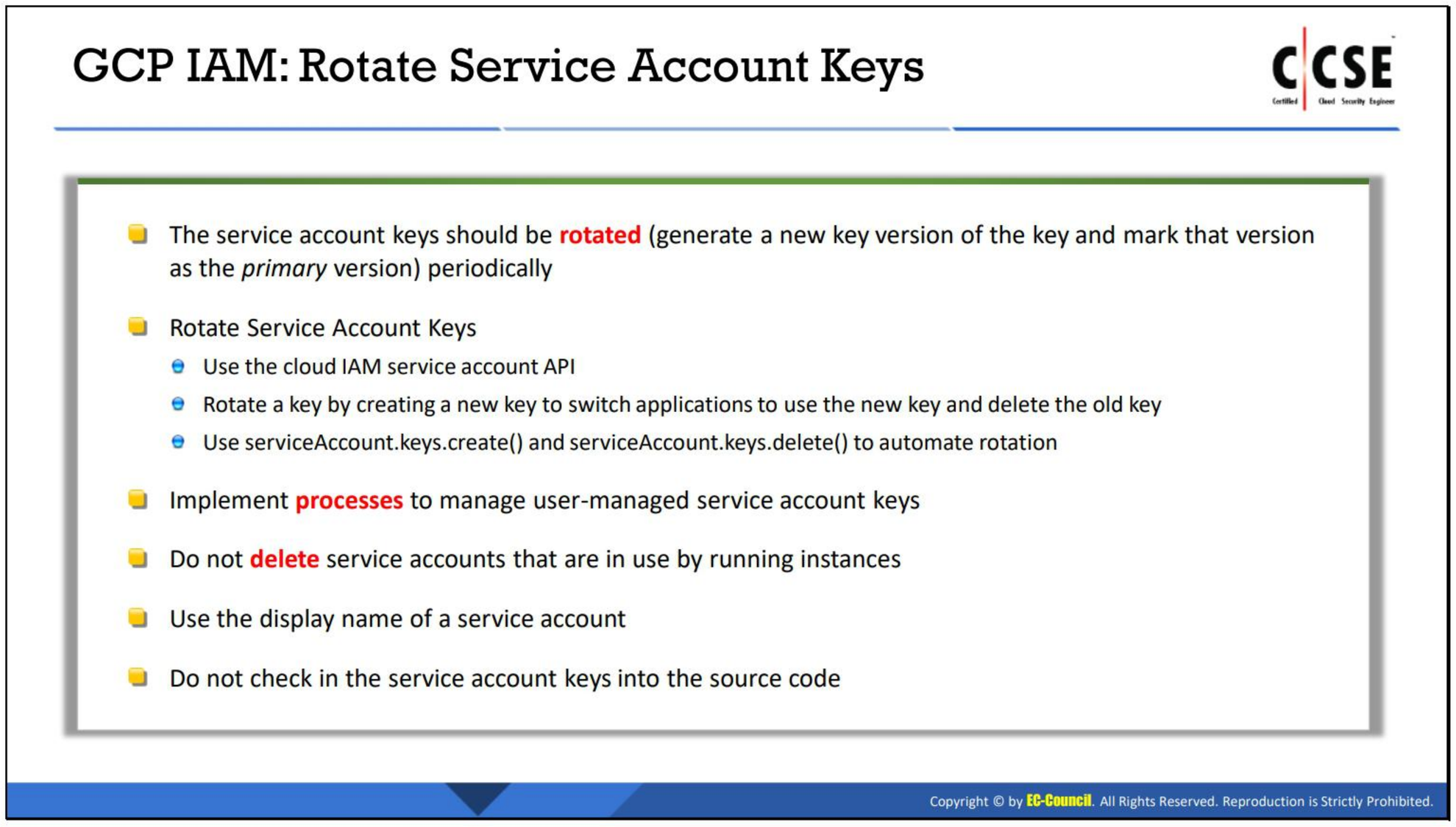
role of Storage Admin (roles/storage.admin) and the user of a particular Compute Engine instance is given the role of Compute Instance Admin (roles/compute.instanceAdmin). However, in other scenarios, the permissions should be granted at the project level, which is inherited by all resources of that project. For example, access to all cloud storage buckets of a project will be granted at the project level instead of the individual bucket level. Similarly, access to all Compute Engine instances of a project will be given at the project level instead of an individual instance.

IAM Best Practices for Application Security in GCP

- Rotate service account keys
- Grant least privileges to avoid primitive roles
- Grant predefined roles
- Create separate service account

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



GCP IAM: Rotate Service Account Keys

Service account keys are categorized into two types:

- **GCP-managed keys**: These keys cannot be downloaded or automatically rotated, and should be used within two weeks. GCP-managed keys are utilized by GCP services such as App Engine and Compute Engine.
- **User-managed keys**: Users can create, download, and manage the keys. The keys expire after ten years.

hide01.ir

The service account keys should be rotated (generate a new key version of the key and mark that version as the primary version) periodically. For key rotation, the user should have the cloud IAM role (roles/cloudkms.admin, roles/owner, or roles/editor).

Key-Rotation Methods

Following are the key-rotation methods:

- **Automatic key rotation**: To automatically rotate a key, the user should set a rotation schedule that determines when the key should be automatically rotated through the gcloud tool:
  - gcloud kms keys update **key-name**\
  - --location **location**\
  - --keyring **keyring-name**\
  - --rotation-period **rotation-period**\
  - --next-rotation-time **next-rotation-time**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Manual key rotation:** To manually rotate a key, the user needs to generate a new key version, disable automatic rotation, and set the new key version as the primary key version. This too is accomplished using the gcloud tool:

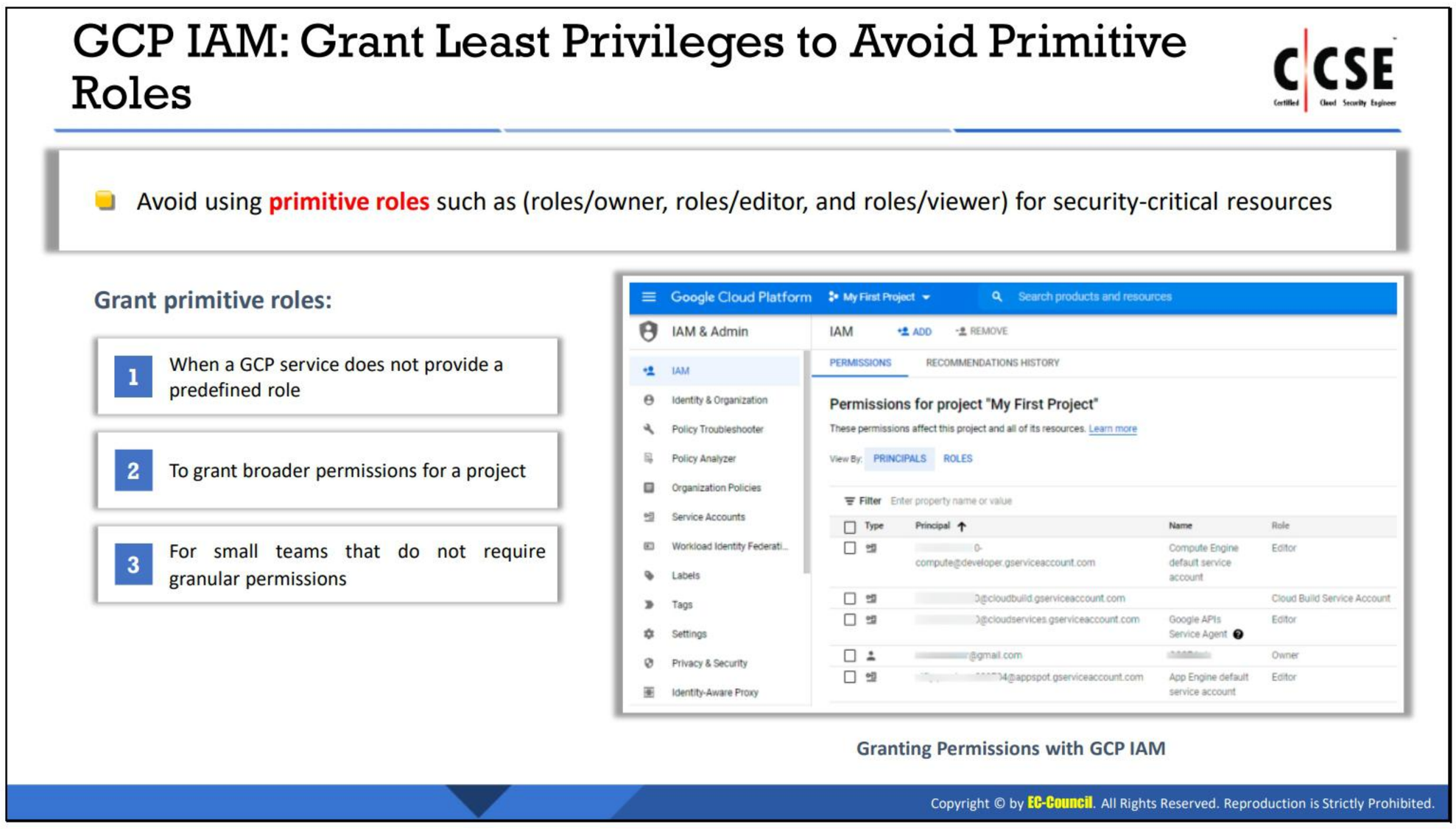
```
gcloud kms keys versions create\
  --location location\
  --keyring keyring-name\
  --key key-name\
  --primary
```

Rotate Service Account Keys

Consider the following while rotating service account keys:

- Use the cloud IAM service account API.
- Rotate a key by creating a new key to switch applications to use the new key and delete the old key.
- Use serviceAccount.keys.create() and serviceAccount.keys.delete() to automate rotation.
- After key rotation, the previous versions of the keys are neither disabled nor destroyed. This feature prevents data loss. For example, if the user rotates the key, the data encrypted with the old key version would not be automatically decrypted and re-encrypted with the new key version. Hence, for re-encrypting the data, the user should decrypt and re-encrypt with the new key version. Then, the user can schedule the old key version to be destroyed if it is not protecting any data.
- Implement **processes** to manage user-managed service account keys.
- Do not **delete** service accounts that are in use by running instances.
- Use the display name of a service account.
- Do not check in the service account keys into the source code.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Granting Permissions with GCP IAM

GCP IAM: Grant Least Privileges to Avoid Primitive Roles

Cloud IAM roles are of three types:

Primitive role: It consists of Owner, Editor, and Viewer roles.

- **Roles/owner**: It has all editor permissions, project billing setup permissions, and permissions for managing all resources in a project.
- **Roles/editor**: It has viewer permissions. For most of the Google Cloud services, this role provides permissions to modify resources.
- **Roles/viewer**: Permissions for read-only and viewing.

Owing to security concerns, it is better to avoid the use of primitive roles.

Primitive roles are granted in the following scenarios:

- When a GCP service does not provide a predefined role.
- Requiring broader permissions for a project such as in development or test environments.
- When the team size is small and team members do not require granular permissions.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Granting Primitive Roles in GCP

- Open the Google Cloud Console, navigate to **IAM & admin**, and click on **IAM** on the Menu tab.

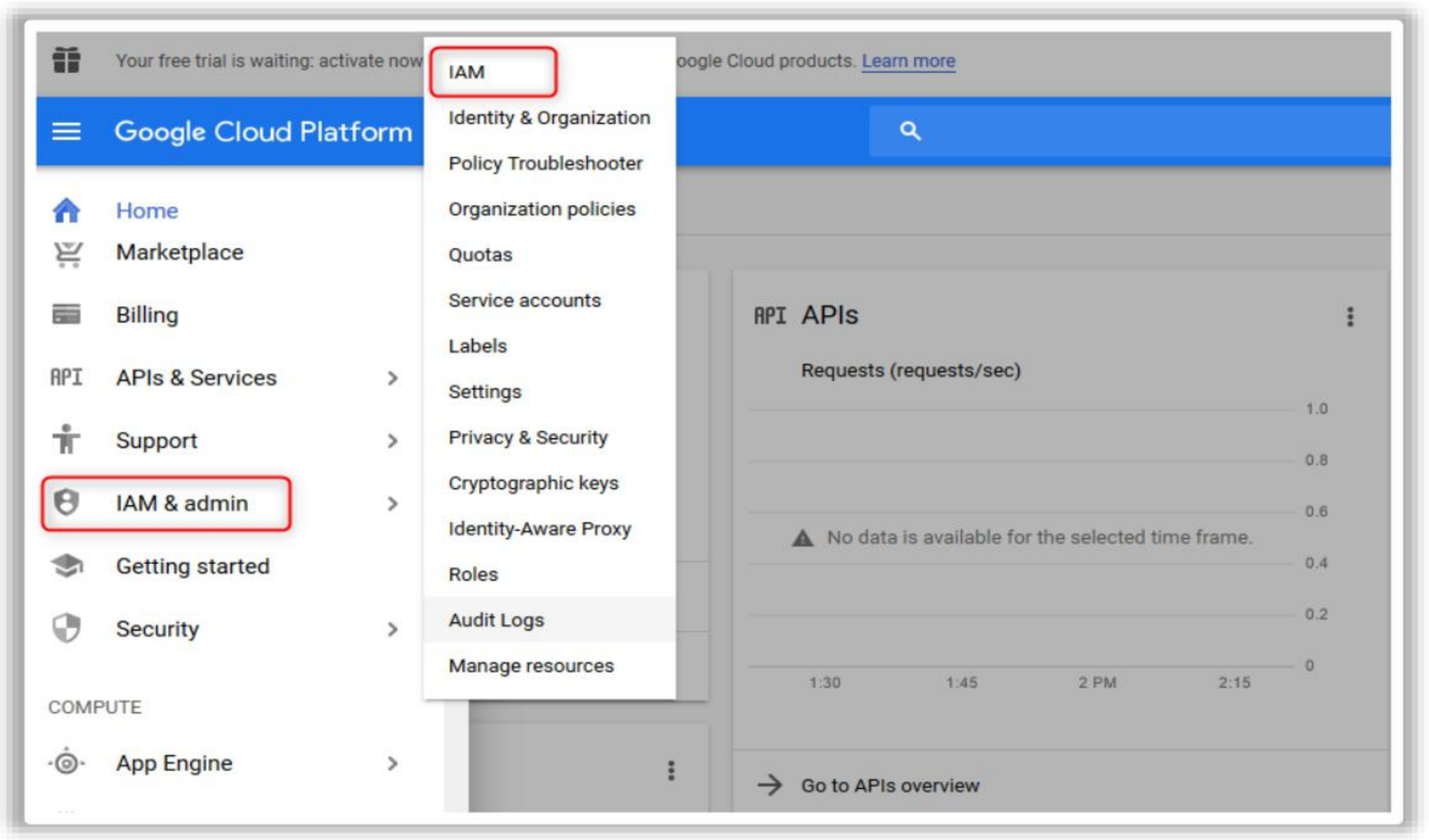


FIGURE 3.174:Open IAM & Admin

- Select **Add** to assign a role, enter one or more members in the **New members** field, select the role from the **Role** dropdown menu, and click on **Save.**

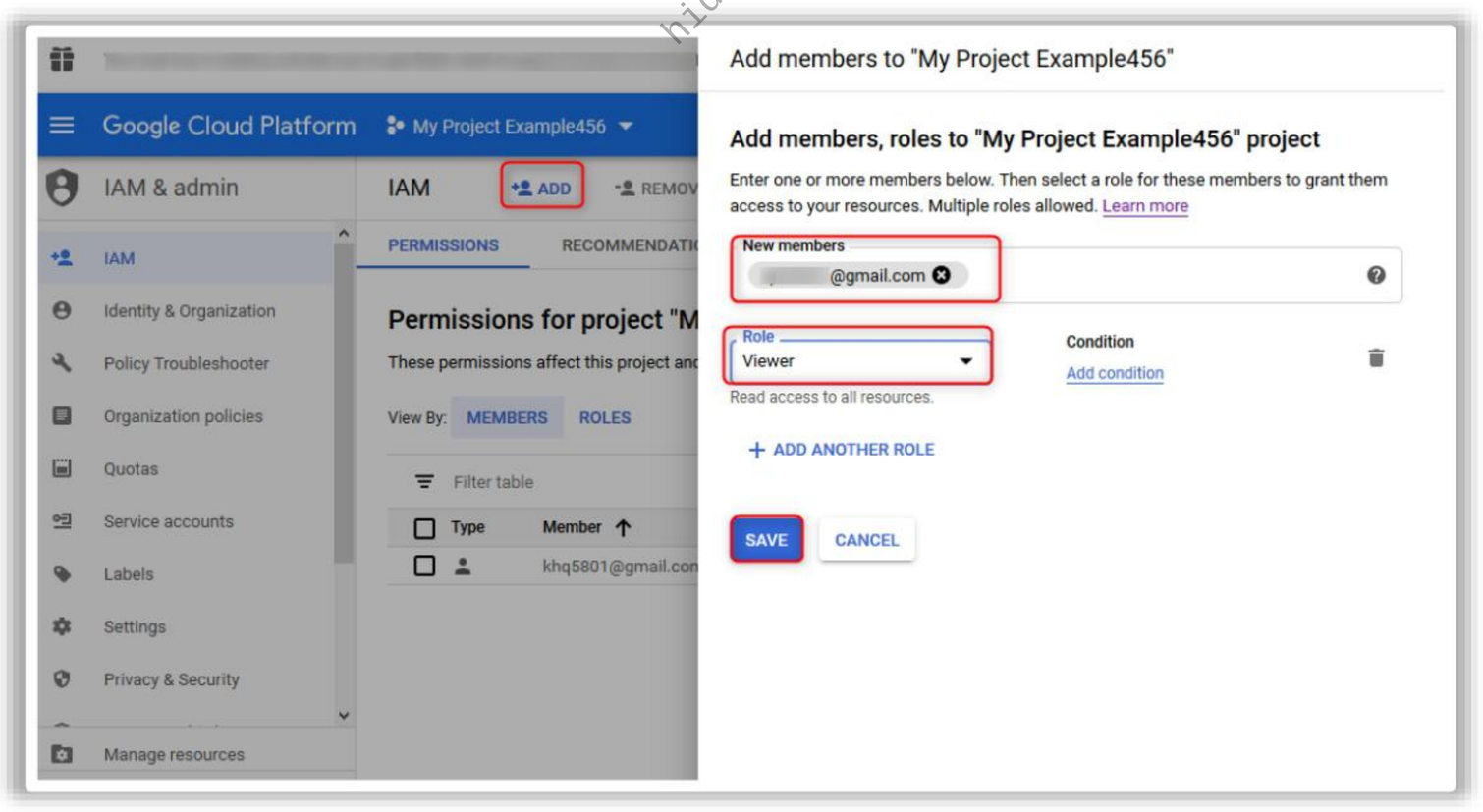


FIGURE 3.175:Add New Member

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The selected role will be granted and can be viewed in **PERMISSIONS** in the horizontal menu.

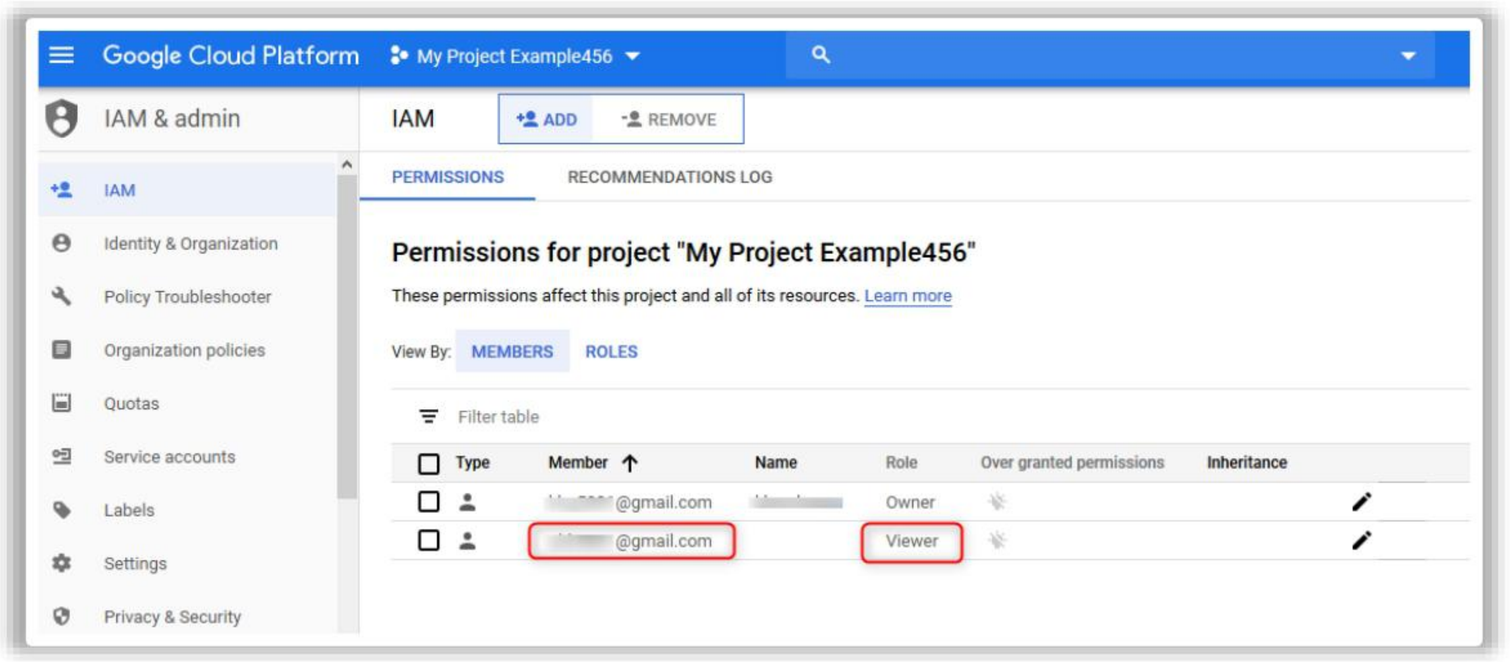


FIGURE 3.176:Permissions

hide01.ir

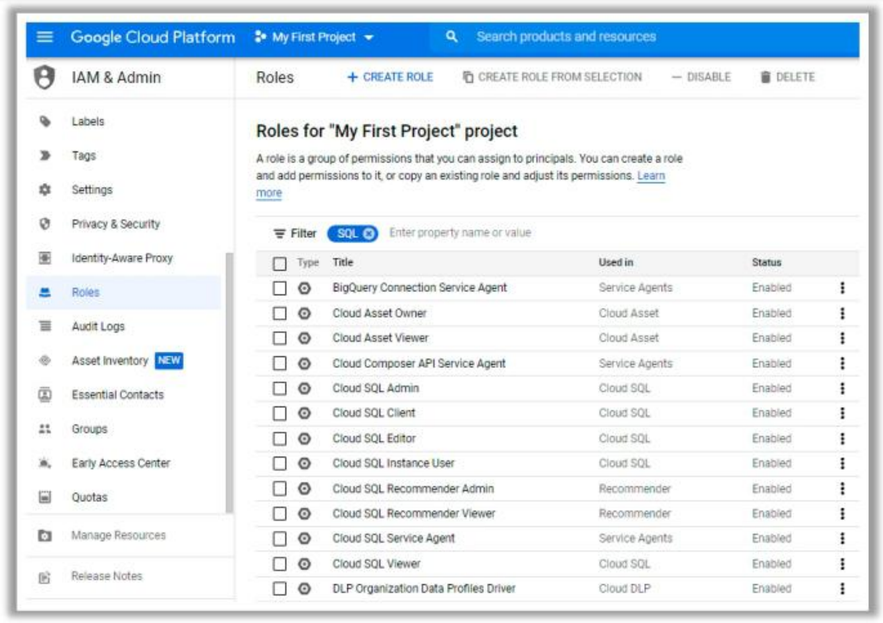
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

GCP IAM: Grant Predefined Roles

- To implement **granular access** to specific Google Cloud Platform resources and prevent unwanted access to other resources, grant predefined roles instead of primitive roles

List of Actions Roles

Role	Title	Description	Permissions
roles/actions.Admin	Actions Admin	Access to edit and deploy an action	actions.* firebase.projects.get firebase.projects.update resourcemanager.projects.get resourcemanager.projects.list
roles/actions.Viewer	Actions Viewer	Access to view an action	actions.agent.get actions.agentVersions.list firebase.projects.get resourcemanager.projects.get resourcemanager.projects.list



Granting Roles with GCP IAM

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

GCP IAM: Grant Predefined Roles

Predefined roles provide fine-grained access control. For example, the predefined role of Pub/Sub Publisher (roles/pubsub.publisher) will allow permission only to publish messages related to Pub/Sub topic. To implement granular access to specific Google Cloud Platform resources and prevent unwanted access to other resources, grant predefined roles instead of primitive roles.

hi0701.ir

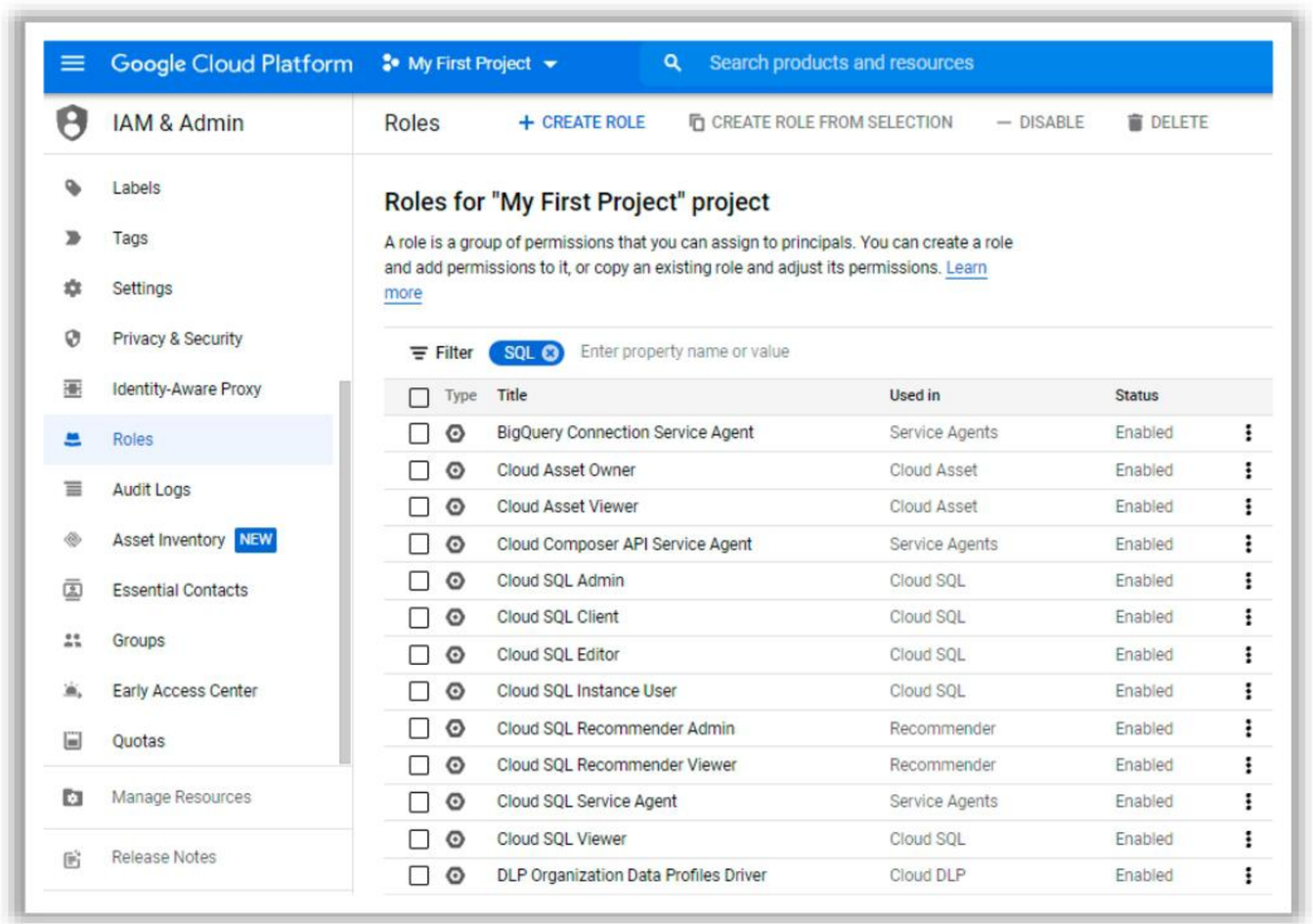


FIGURE 3.177:Granting Roles with GCP IAM

A specific role is given to a resource type. Multiple roles can also be given to the same user.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For example, the role of `roles/action.Admin is` given to the Action Admin to edit and deploy an action; it contains the following permissions:

- actions.*
- firebase.projects.get
- firebase.projects.update
- resourcemanager.projects.get
- resourcemanager.projects.list

Granting Predefined Roles in GCP

- From the Google console dropdown menu, navigate to **IAM & admin** and select **Roles** in the menu.

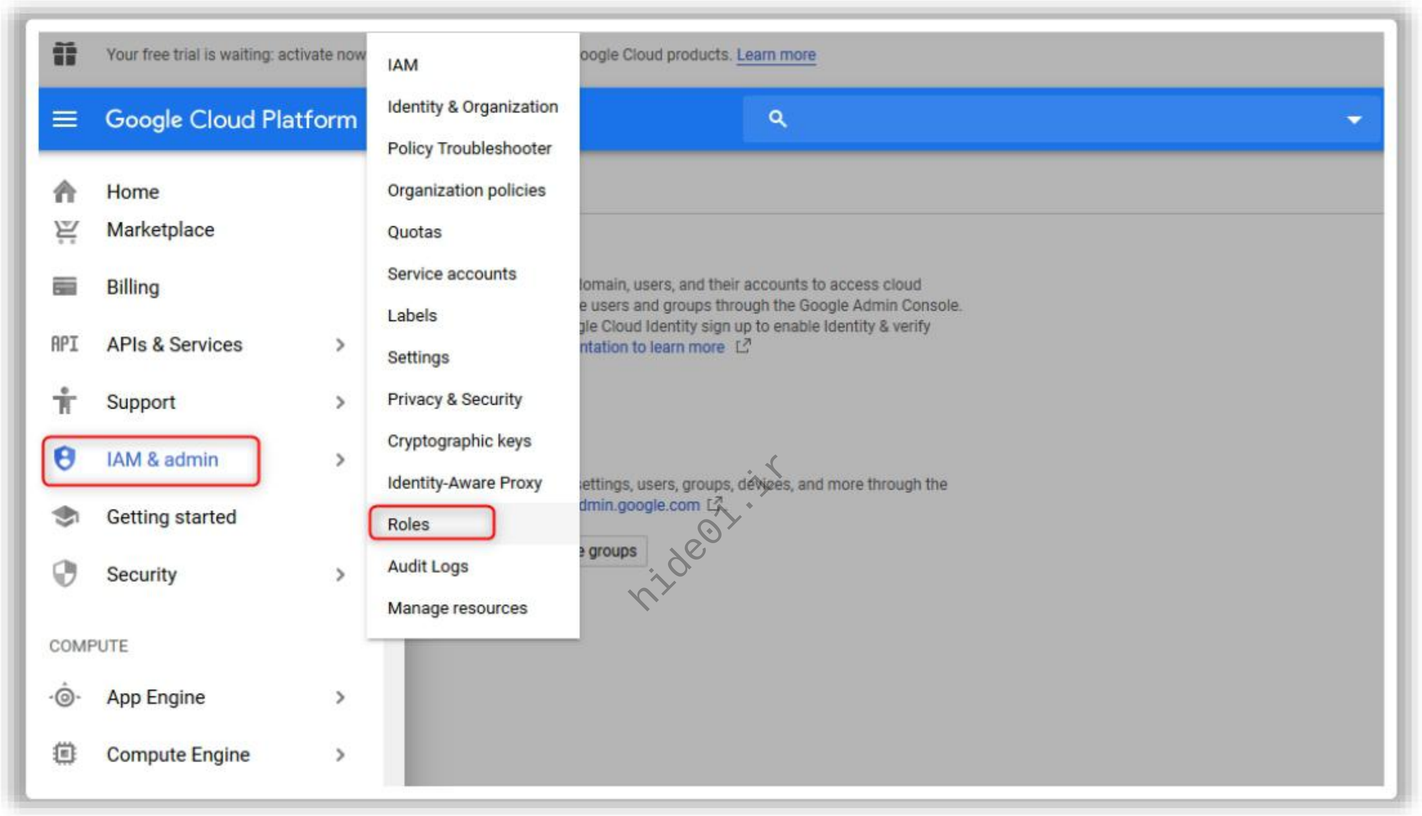


FIGURE 3.178: Navigate IAM & Admin

- Select the filter from filter table (**Name**) and search the role (**actions.Admin**). Click on the context menu to see the assigned permissions.

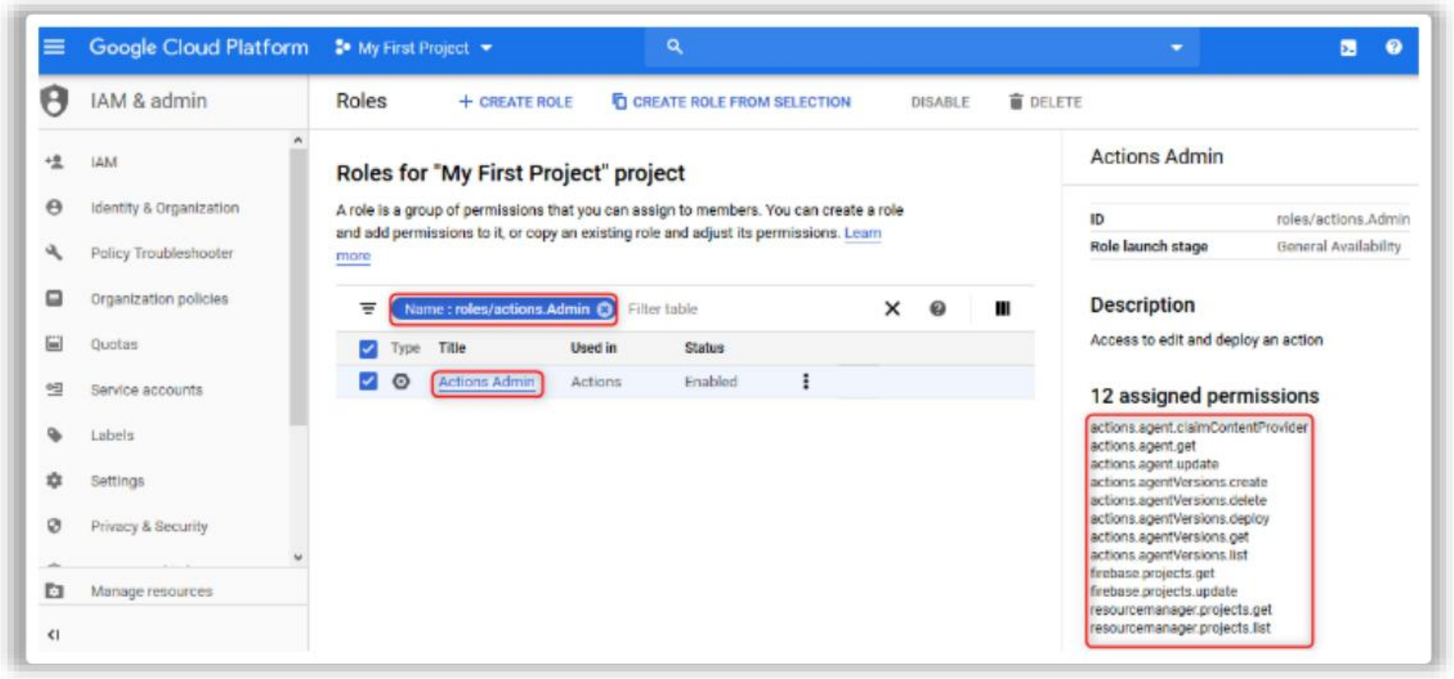


FIGURE 3.179:Assigned Permission

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click **IAM** on the **Menu** tab, select **Add** to assign role, enter the email id of the user, select Actions Admin from the **Role** dropdown menu, and click on **Save.**

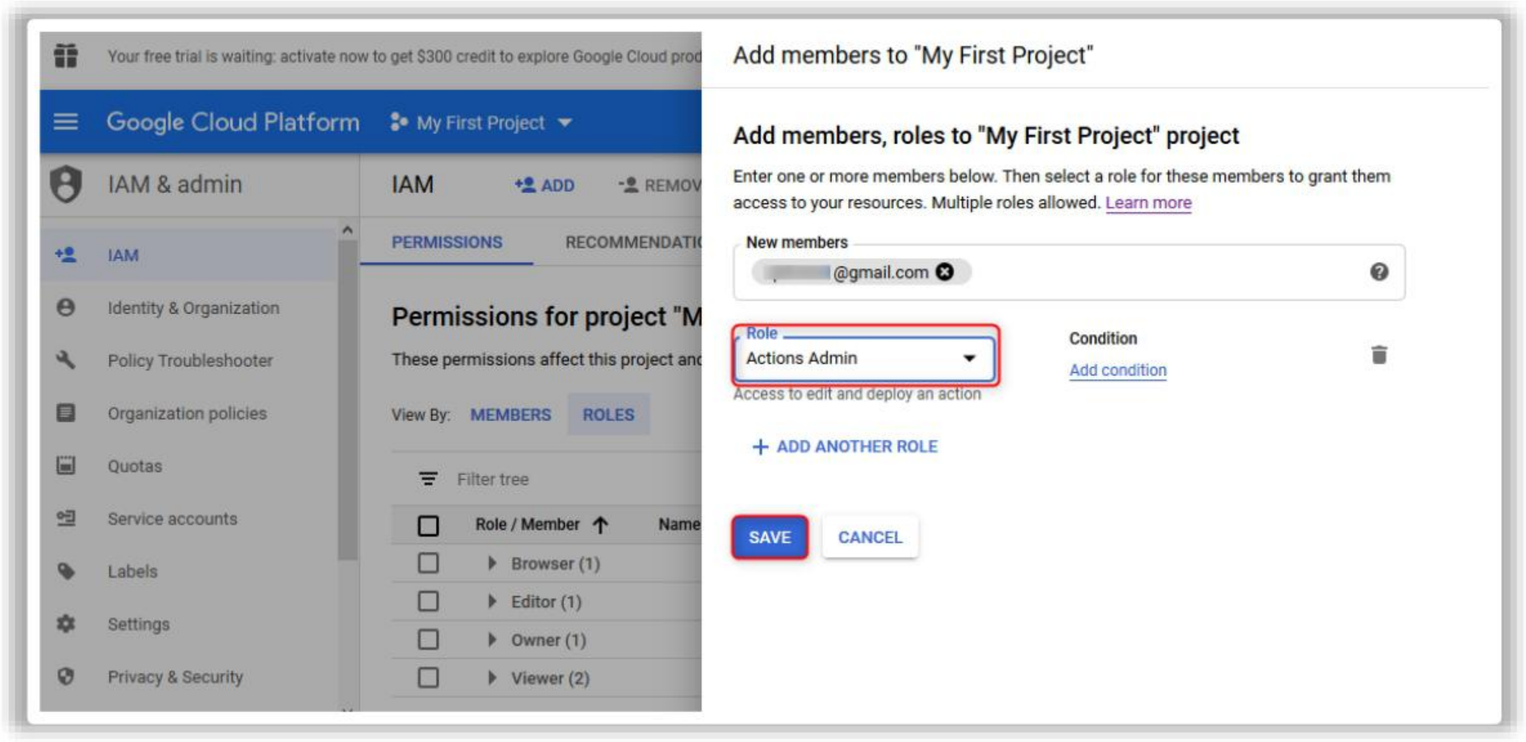


FIGURE 3.180:Assign Role

- Thus, a predefined role is granted in the GCP.

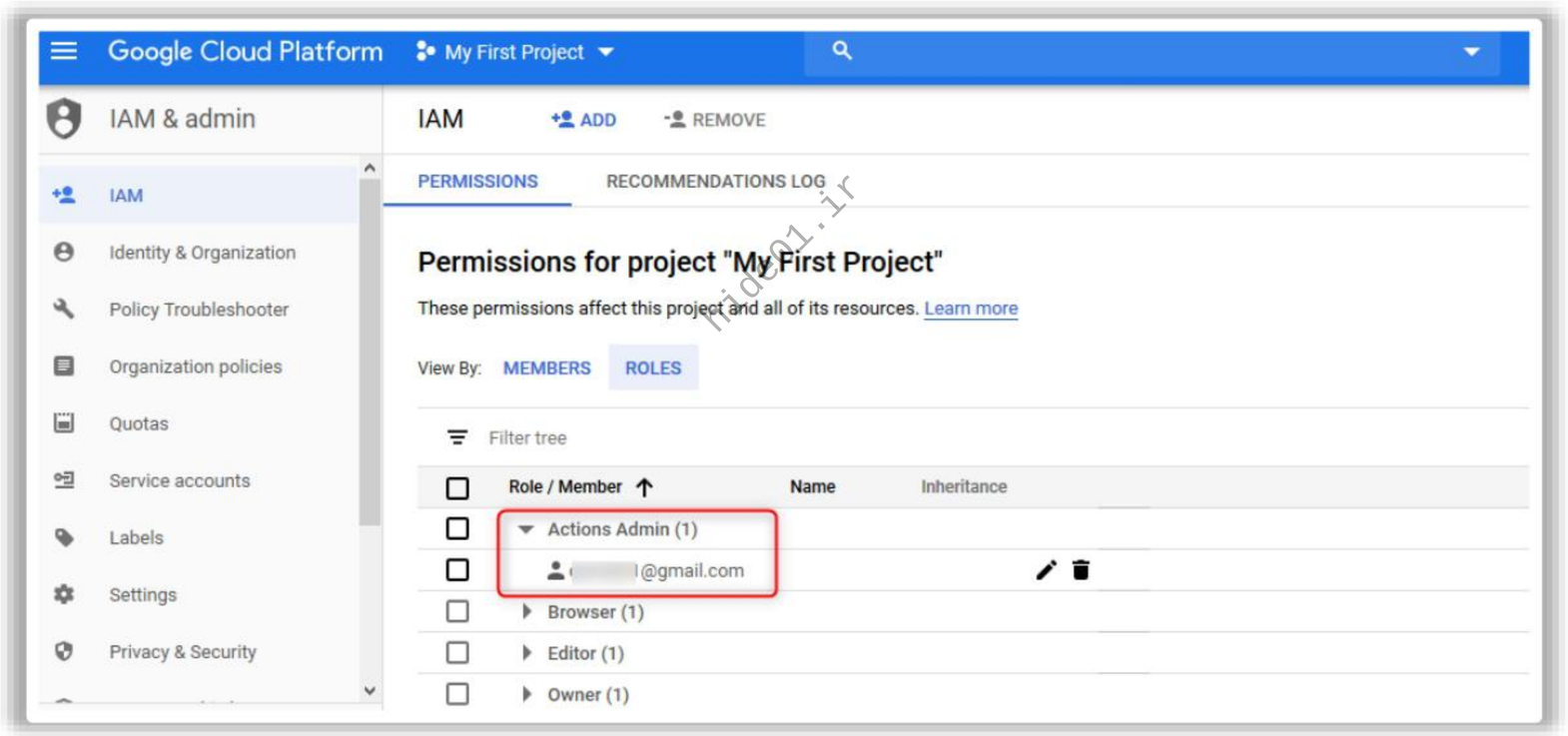


FIGURE 3.181: Predefined Role Granted

Custom Roles

When predefined roles do not satisfy the requirements of the organization, then custom roles are created to according to the permissions.

A custom role is a user-defined role that allows the collection of supported permissions to satisfy the requirements of an organization. Because Google does not maintain custom roles, these roles are not updated automatically by the GCP. Custom roles can be created at the organization and project level; however, they cannot be created at the folder level.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Granting Custom Roles in GCP

- From the Google console dropdown menu, navigate to **IAM & Admin** and select **Roles** in the menu.
- Select a role from the filter table, click on the **context** menu, and select **Create role from this role.**

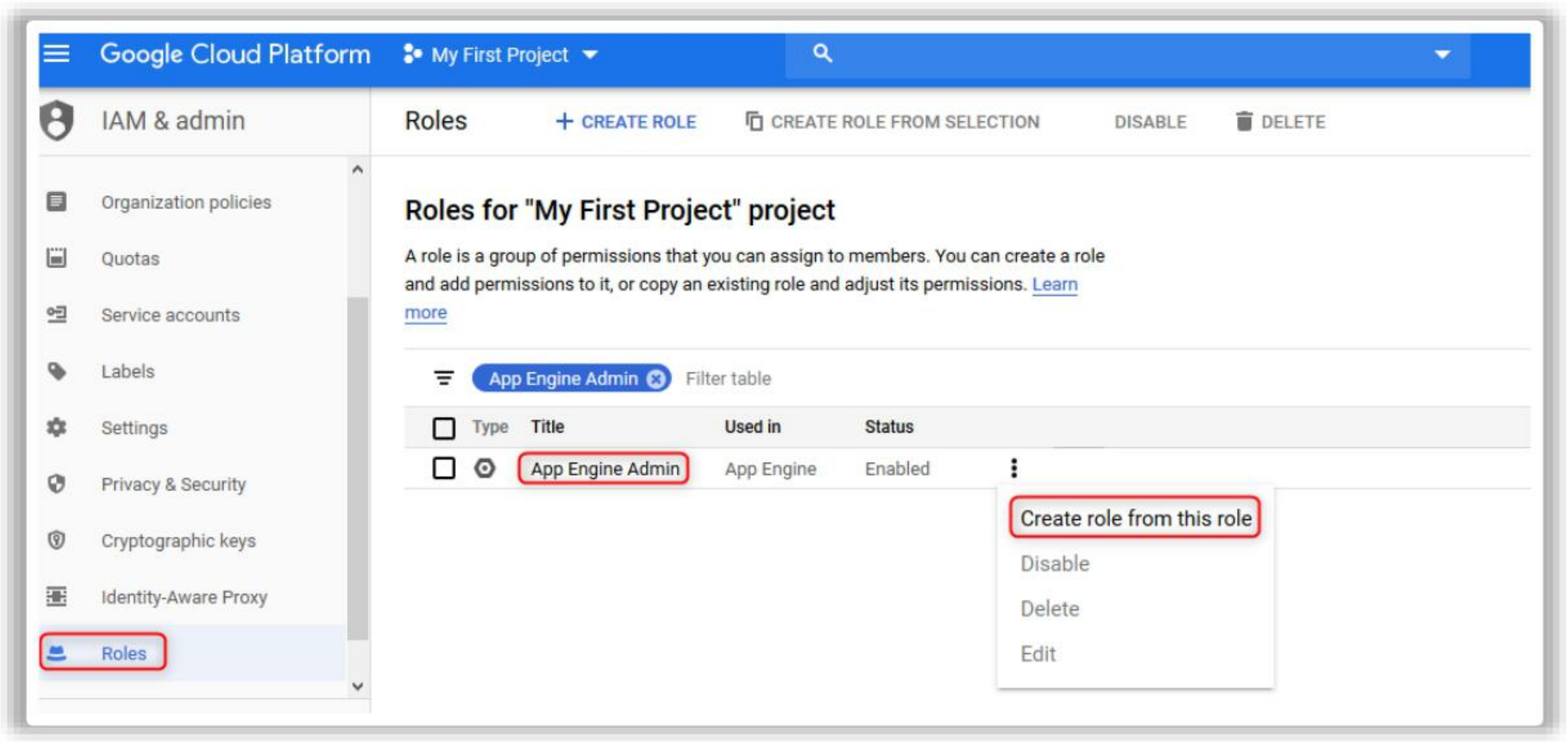


FIGURE 3.182:Create Role from Role

- Create a custom role and click on **ADD PERMISSIONS.**
- Select the required permissions and click on **ADD.**

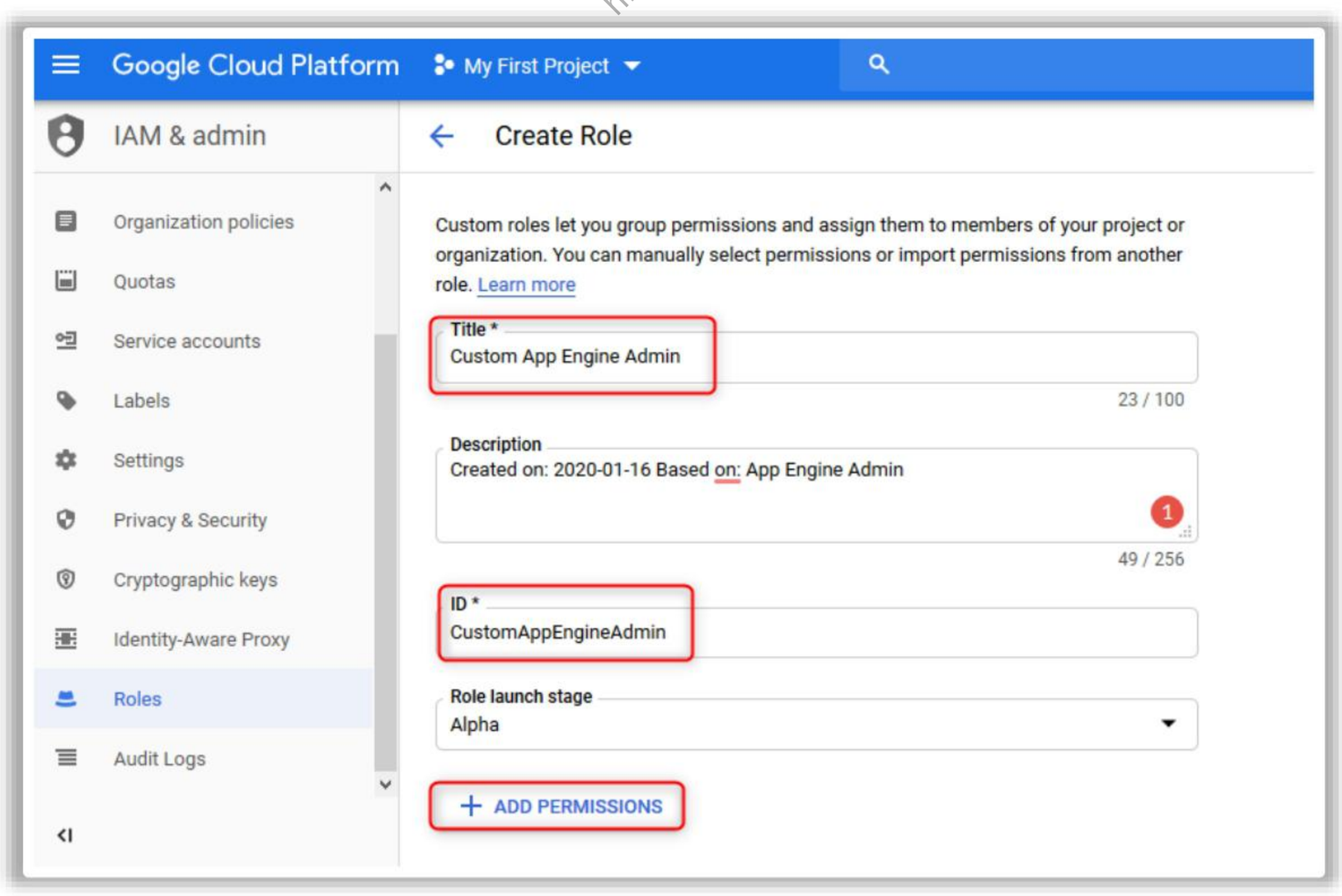


FIGURE 3.183: Click Add

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

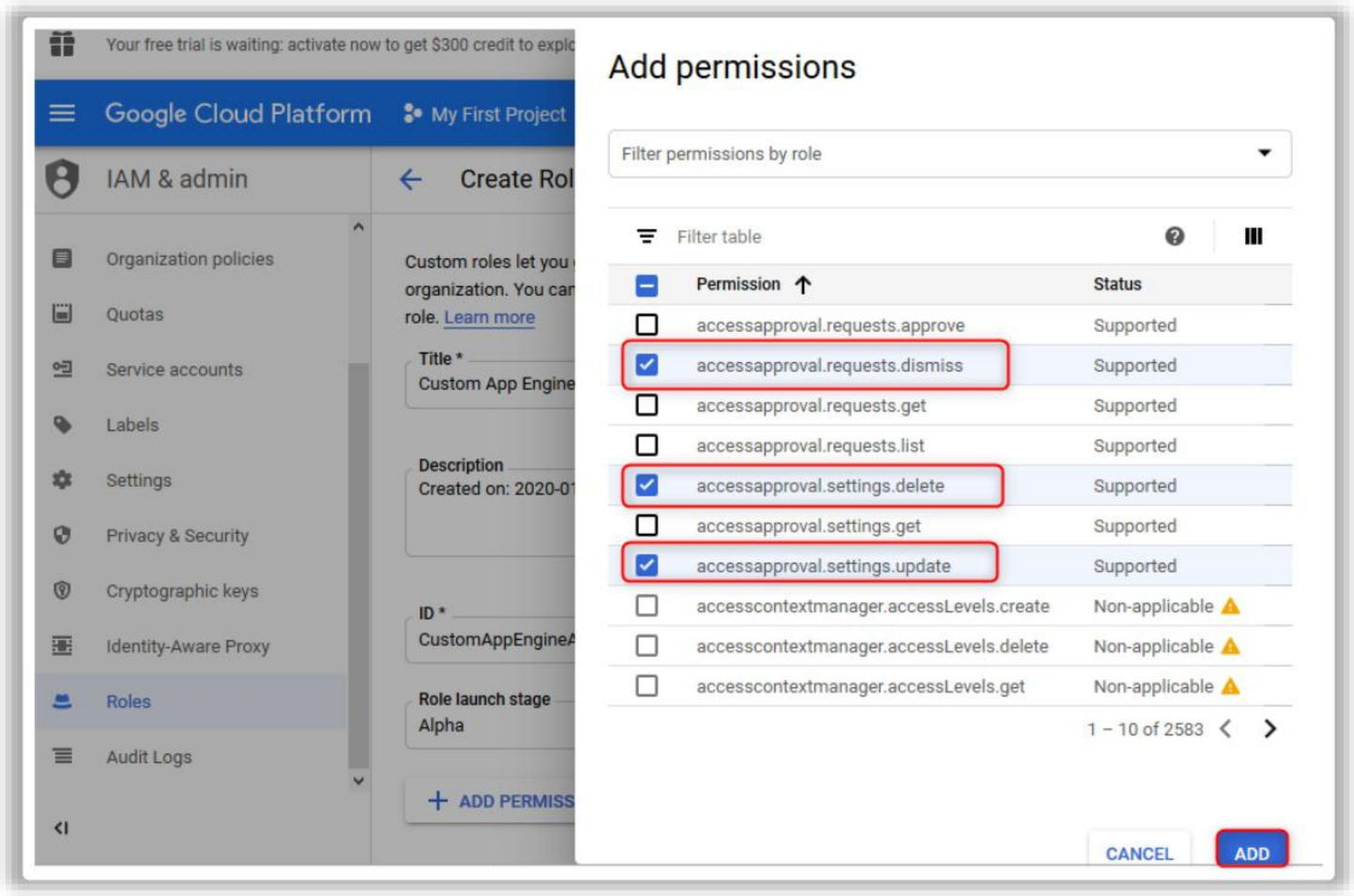


FIGURE 3.184: Add Permision

- Thus, the custom App Engine Admin roles are created.

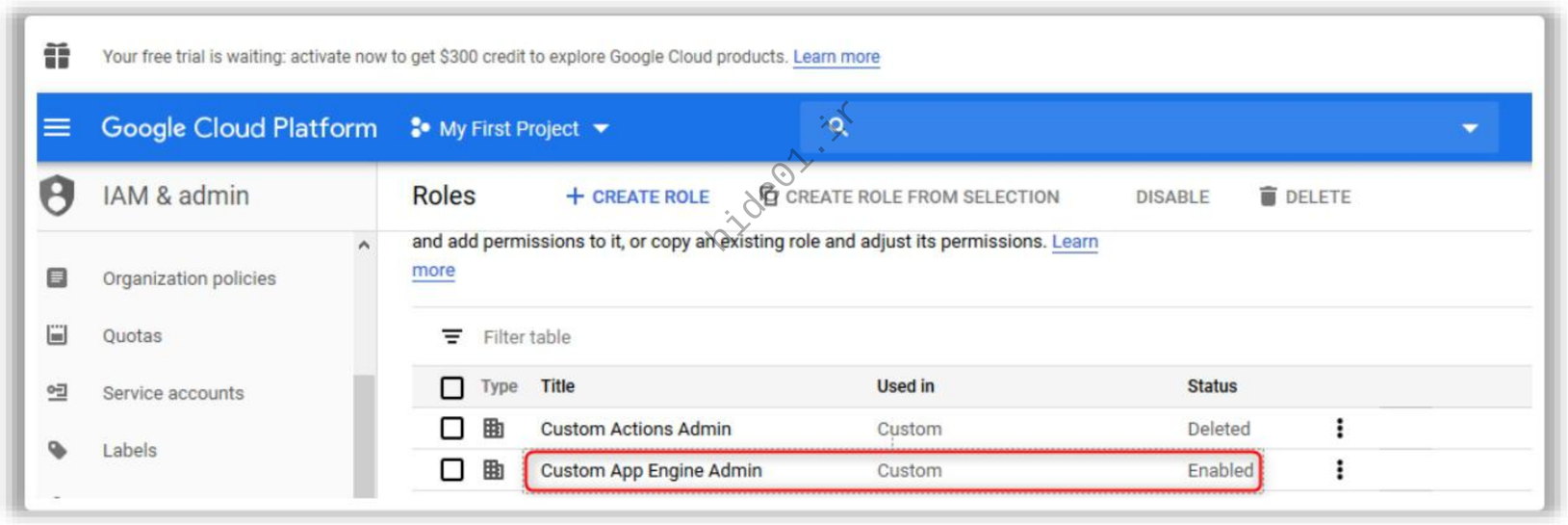


FIGURE 3.185:Custom App Engine Admin Role

- Click on **IAM** in the **Menu** tab, select **Add** to assign role, enter the email ID of the user, select **Custom App Engine Admin** from the **Role** dropdown menu, and click on **Save.**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

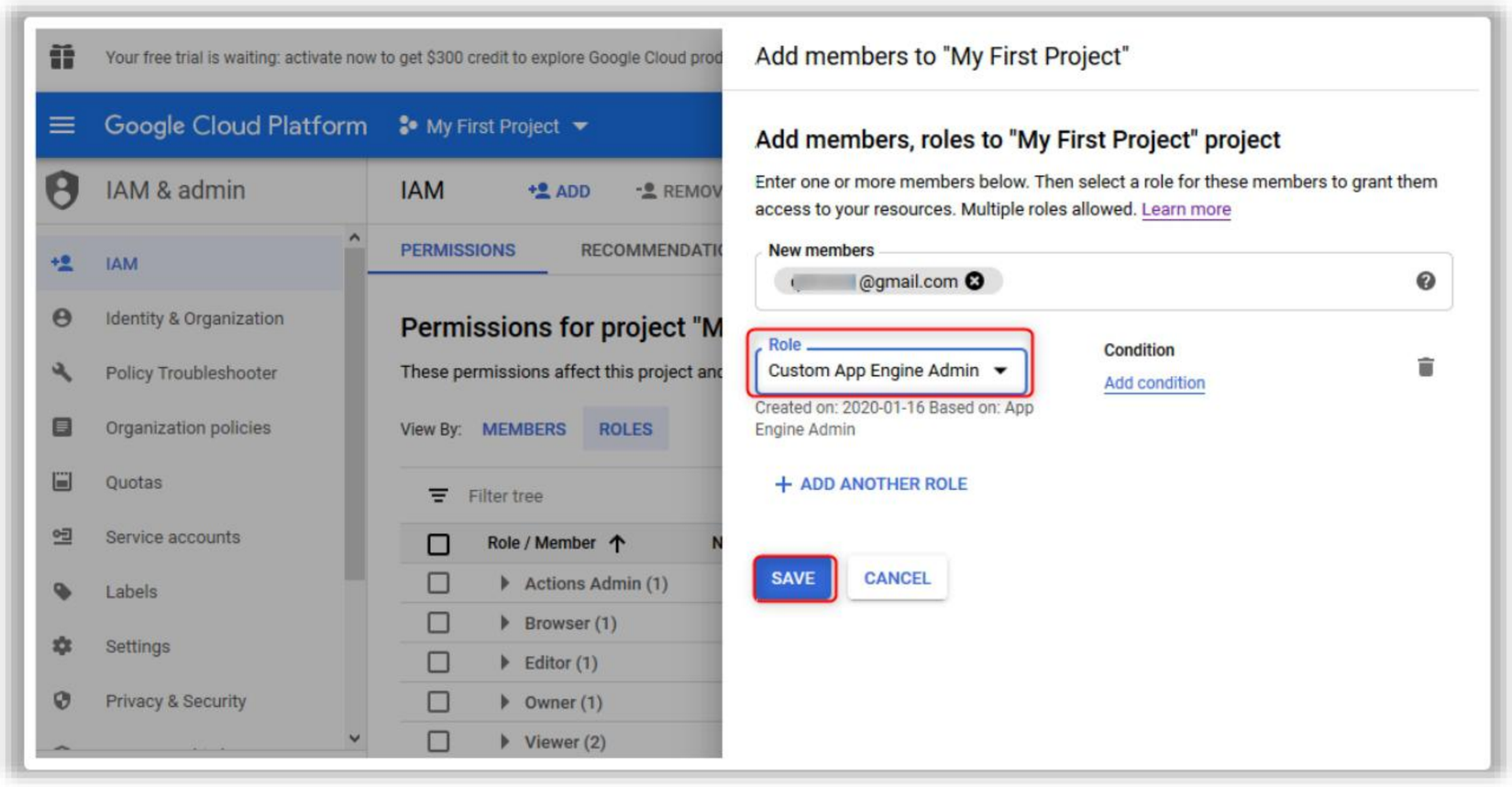


FIGURE 3.186:Assign Role

- Thus, custom roles are granted to the user.

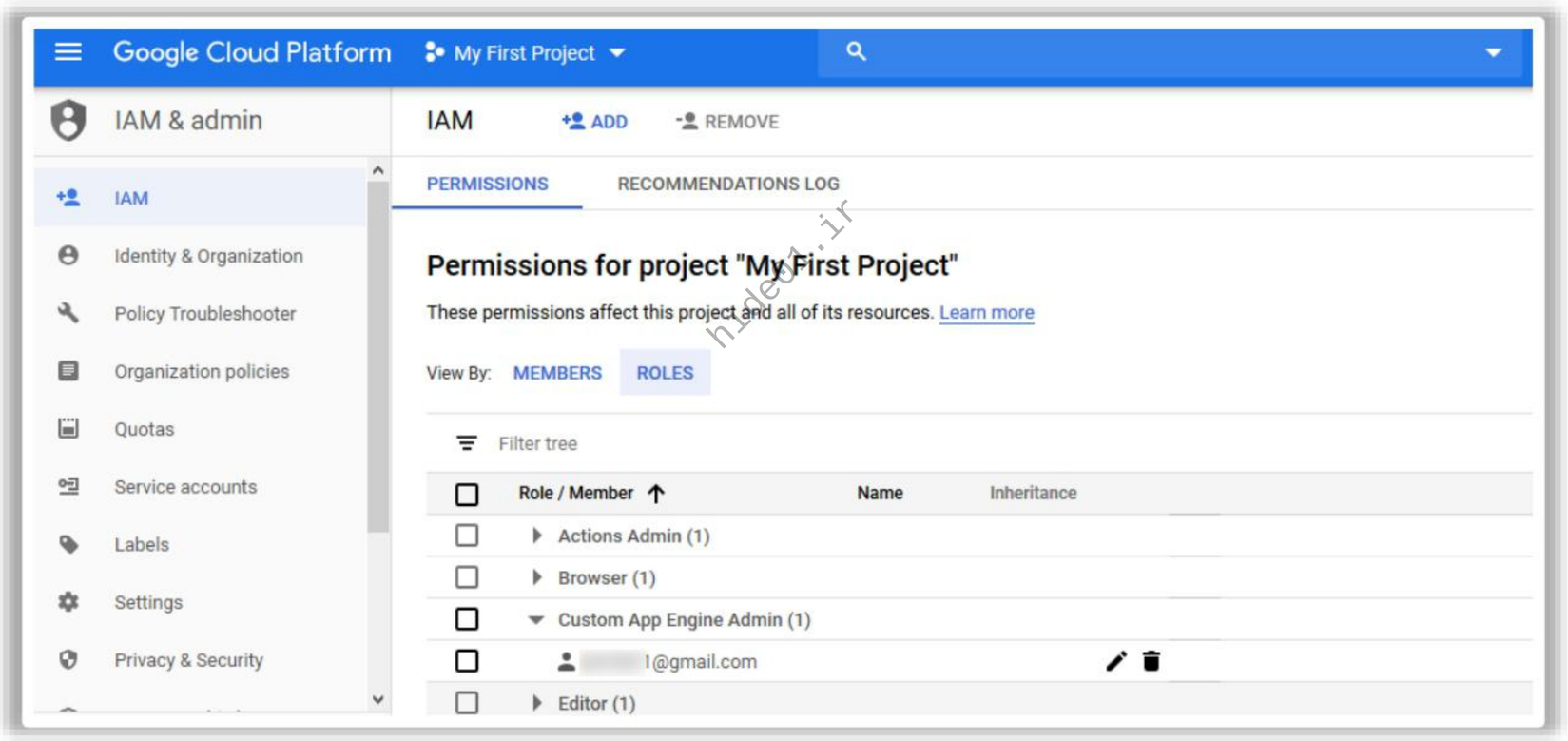
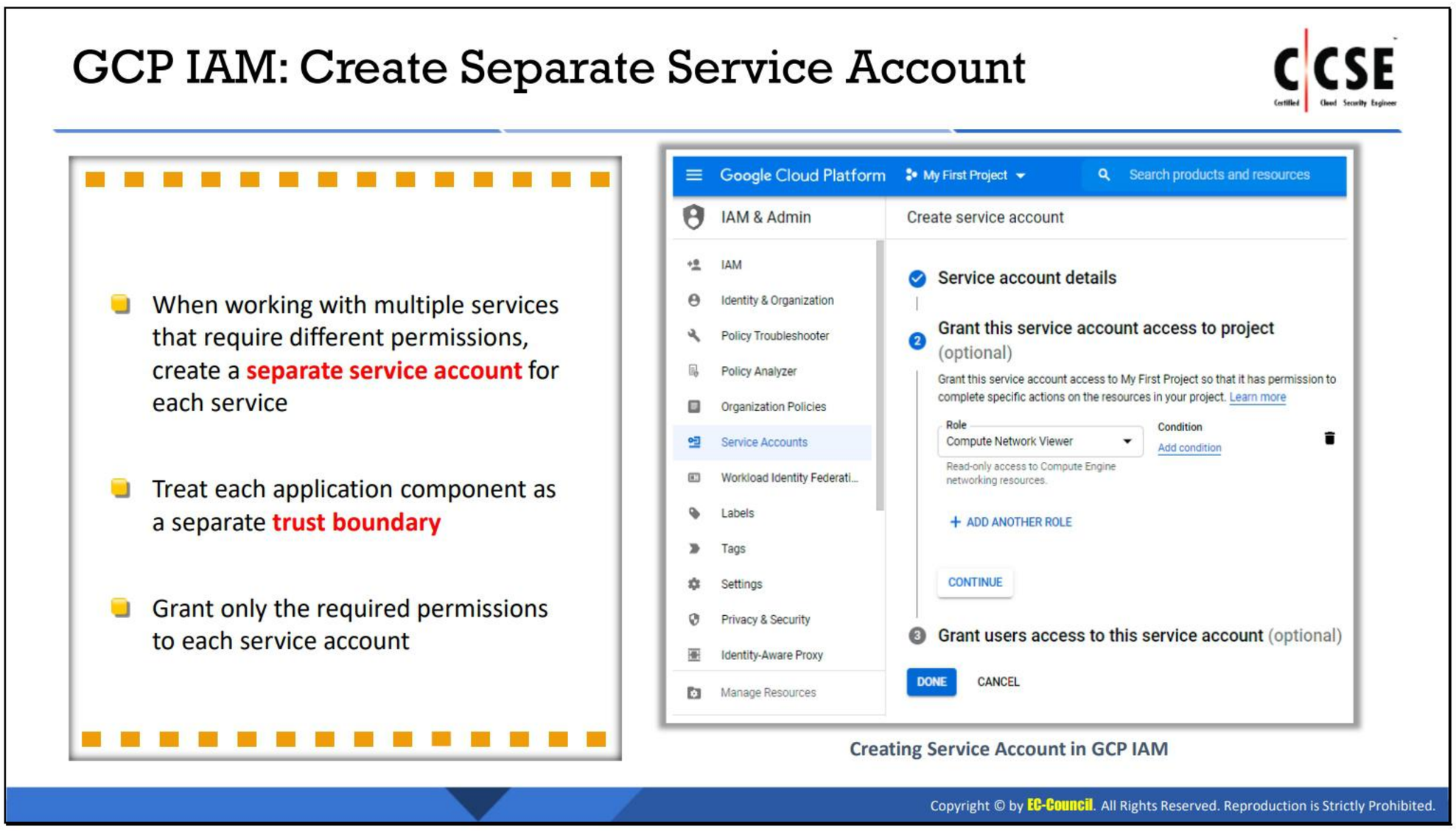


FIGURE 3.187: Custom Roles Granted

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Creating Service Account in GCP IAM

GCP IAM: Create Separate Service Account

Service accounts are accounts created to access the cloud platform APIs using applications. They perform tasks according to the role assigned to specific service accounts. It is possible to create up to 100 service accounts per project.

hide01.ir

Service account user roles can be granted at the project level or service-account level. If a service-account user role is granted at the project level, then the user can access all service accounts in the project. If a service-account user role is granted at the service-account level, the user can only access that service account. It is important to practice caution while granting service account user roles because the service account users indirectly have access to all resources of the service account. Minimum permission should be granted to service accounts based on the requirement.

Implementing Minimum Privileges to Service Accounts

- Every component of the application should be treated as a discrete trust boundary. If there are many services and each service requires different permissions, then create a separate service account for each service and give permission to the required service account.
- Restrict the actions of users to modify the service accounts of a project. Grant only the required permissions to each service account.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Creating Service Accounts in GCP IAM

Follow these steps to create service accounts:

- From the Google Cloud Console, navigate to **IAM & admin** and select **service accounts** from the menu.

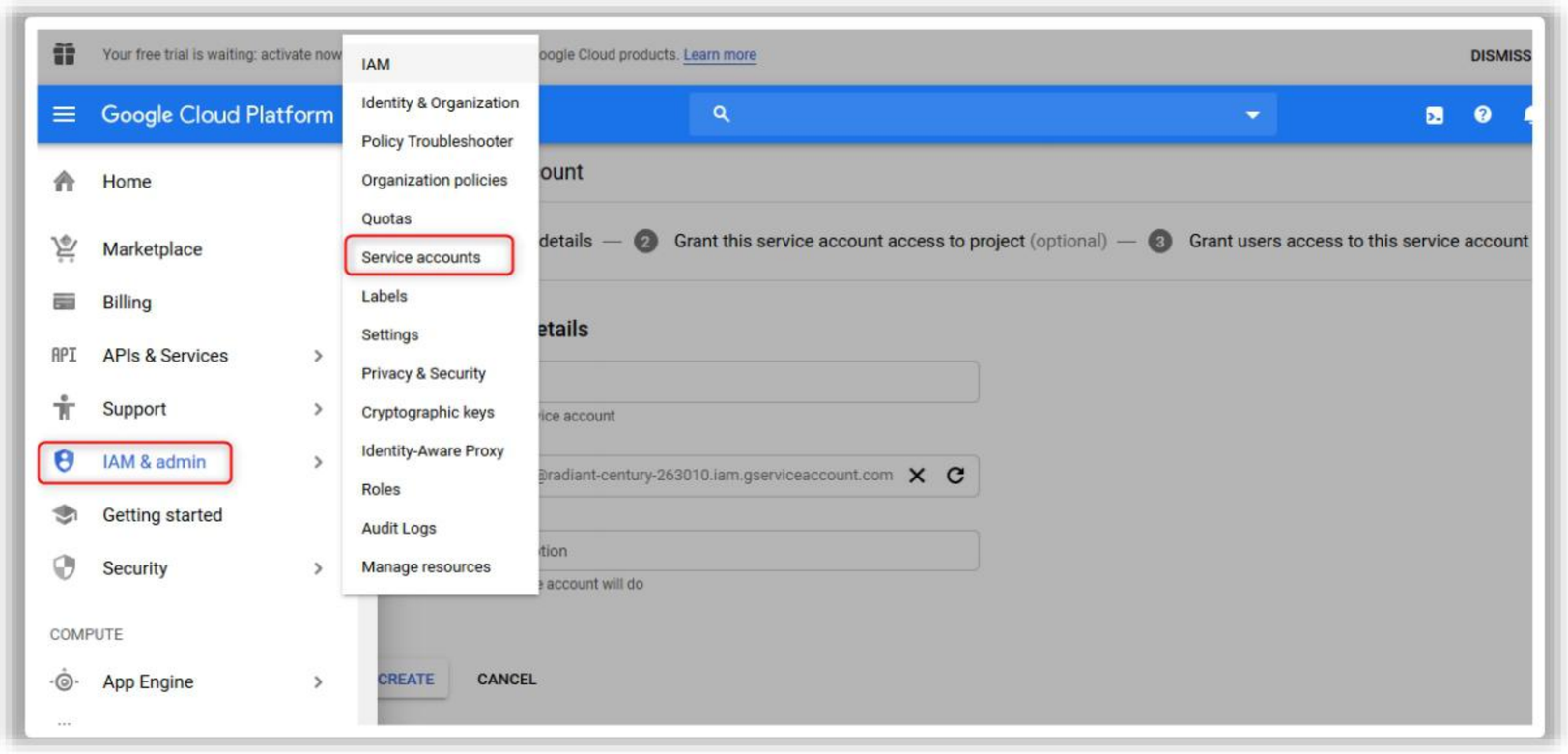


FIGURE 3.188: Google Cloud Console

- To create a service account, click on **CREATE SERVICE ACCOUNT** on the horizontal menu.

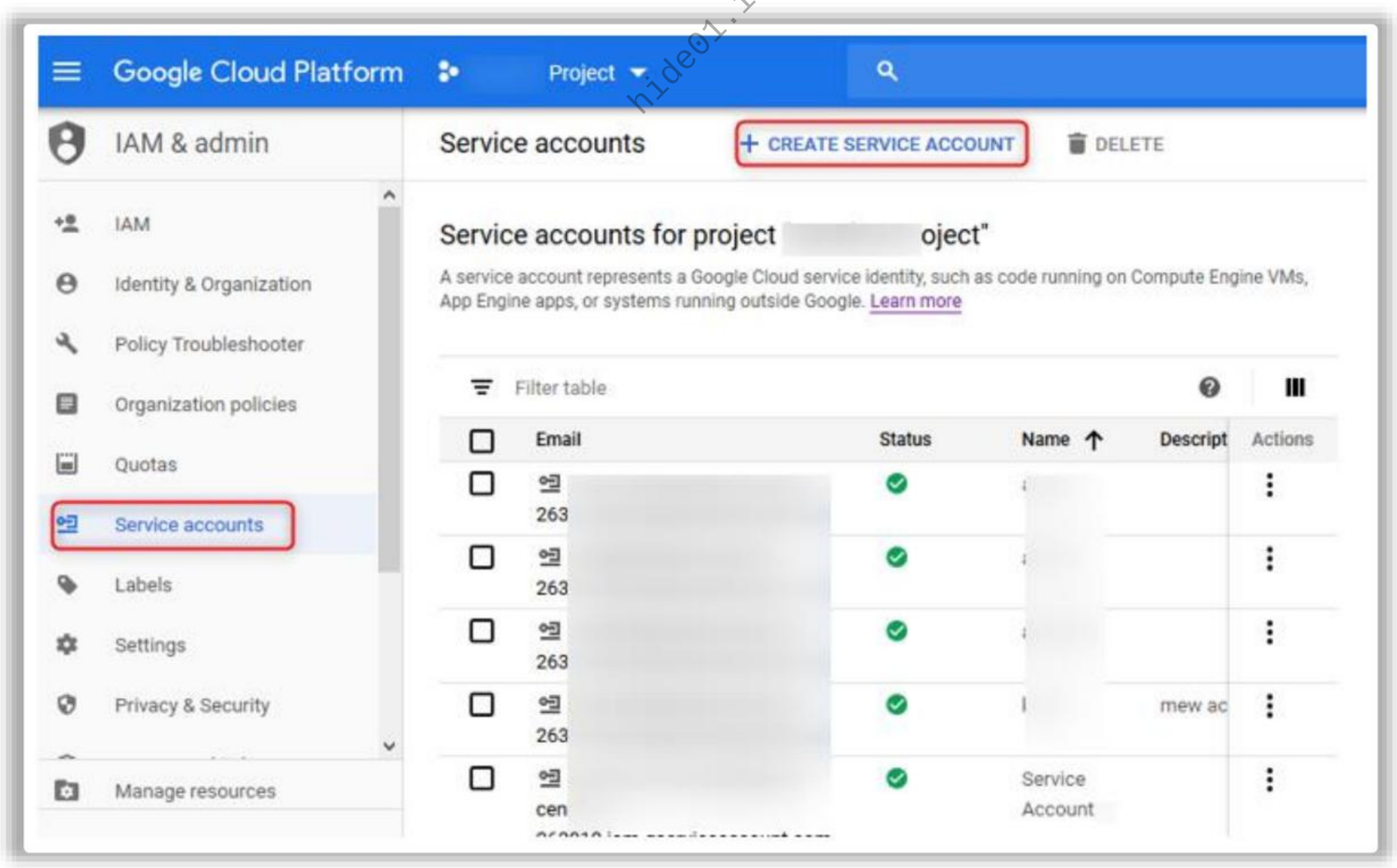


FIGURE 3.189: Create Service Account

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enter the **service account details** and click on **Create.**

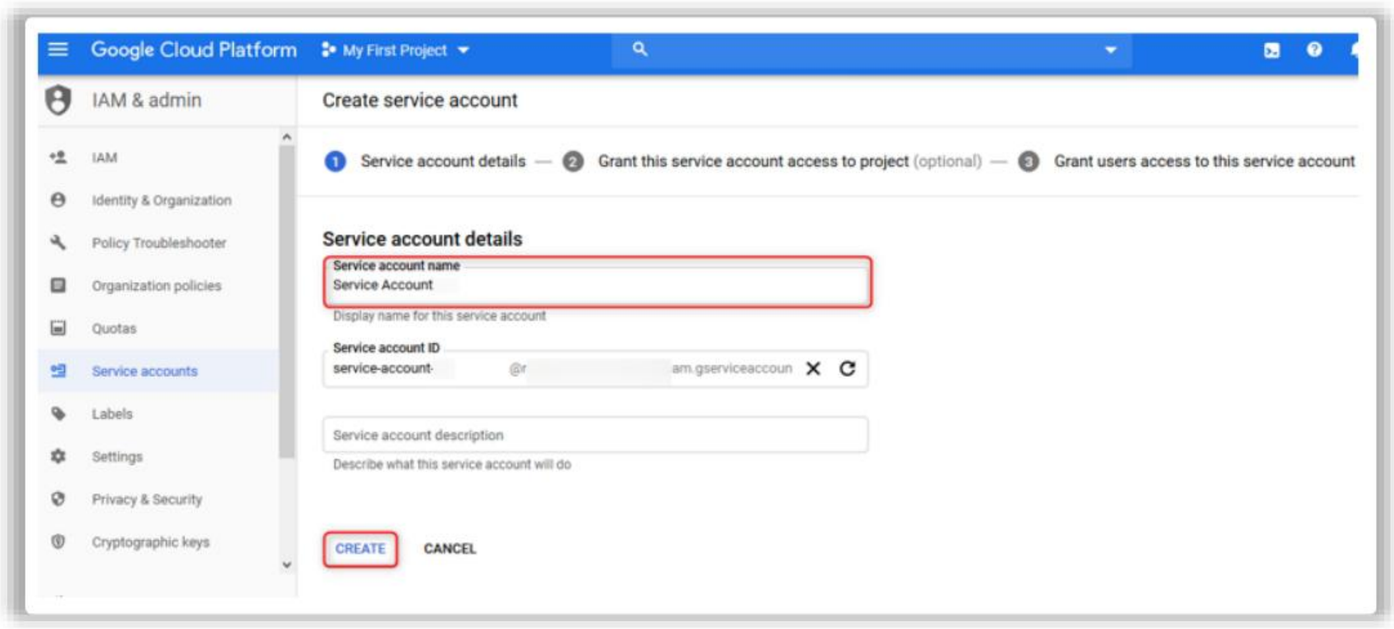


FIGURE 3.190: Enter Service Account Details

- Select the role for **service account permissions** and click on **CONTINUE.**

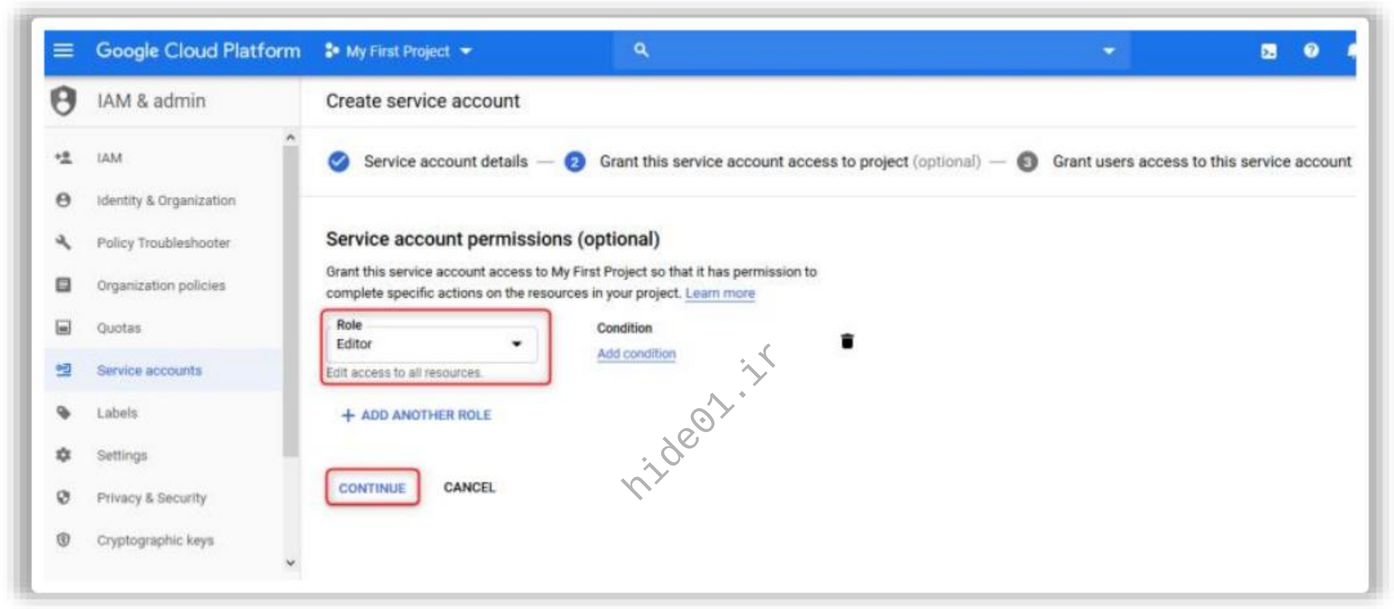


FIGURE 3.191: Service Account Permissions

- Click on **CREATE KEY** and select the **JSON** file that contains the private key.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

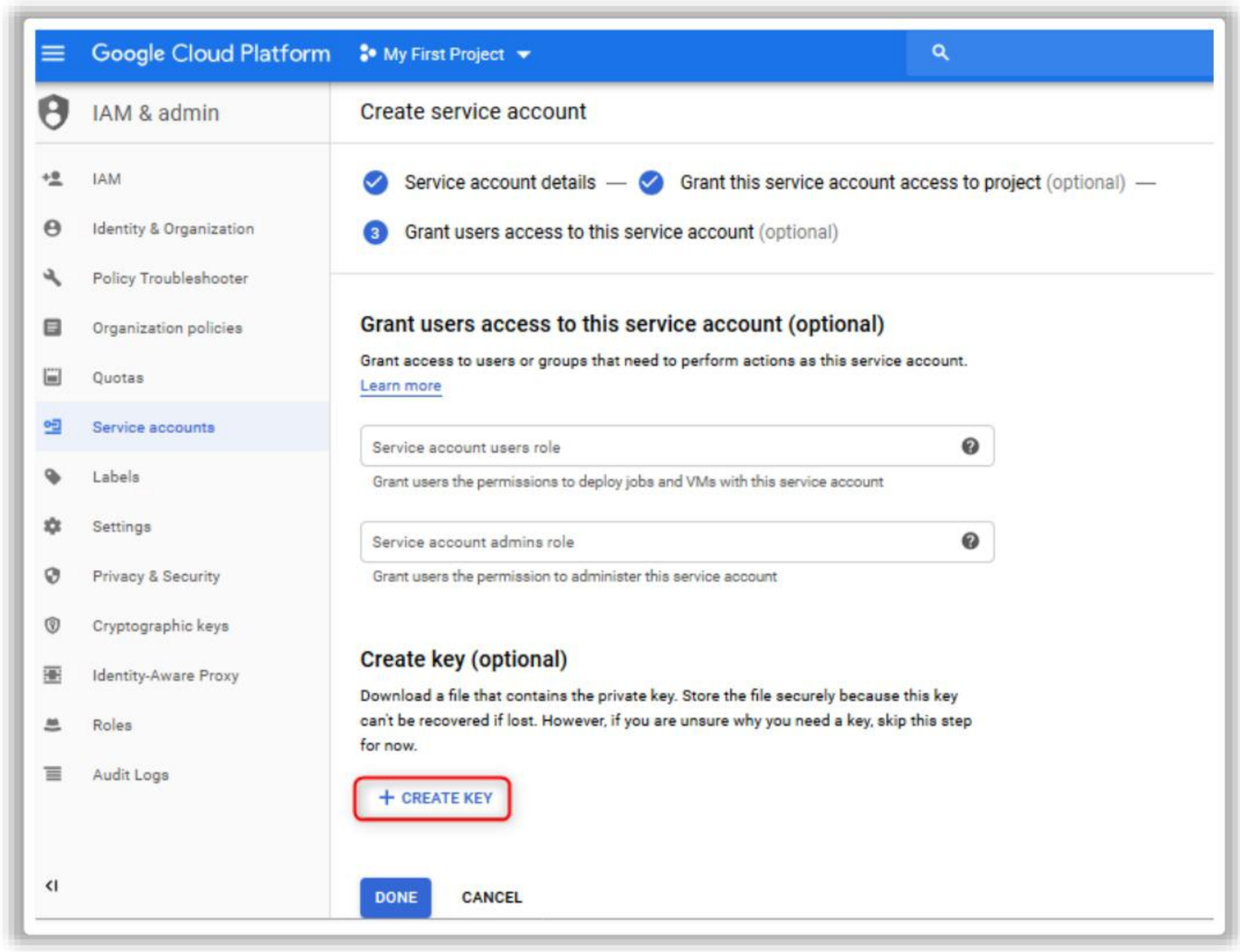


FIGURE 3.192: Create Key

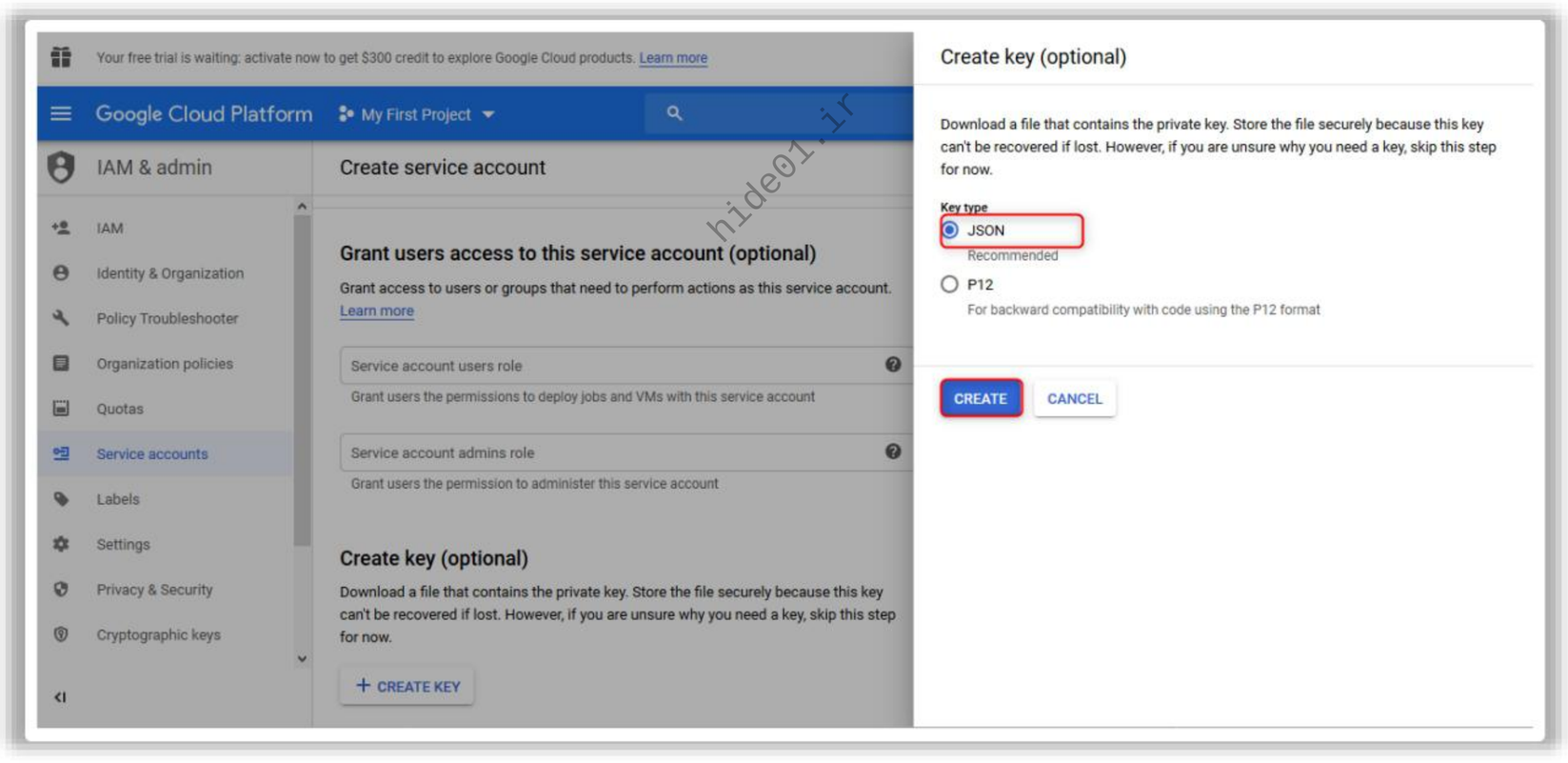


FIGURE 3.193: Select JSON

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- After the private key is saved, click on **DONE.**

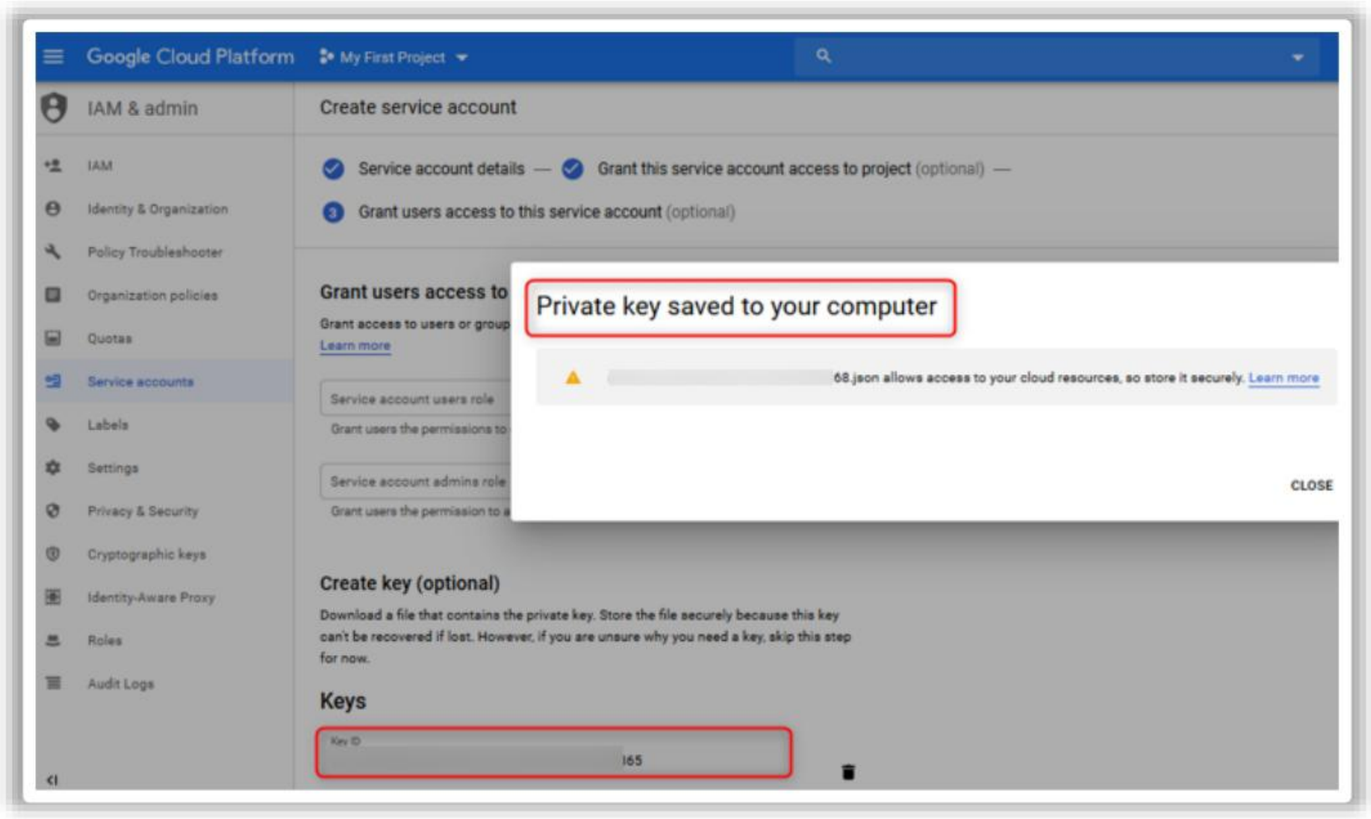


FIGURE 3.194: Save Private Key

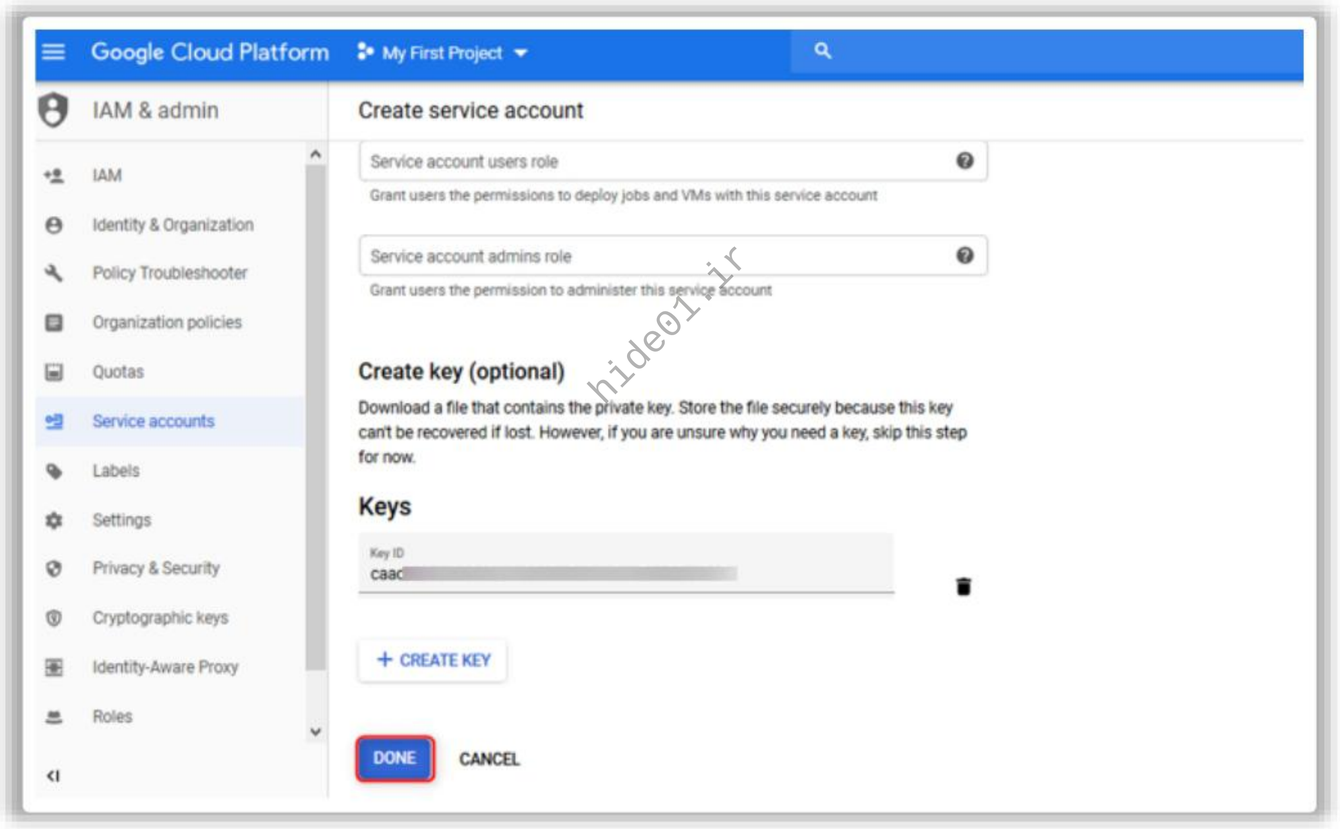


FIGURE 3.195: Click Done

- Thus, service account with the assigned role is created and can be viewed in the **IAM** menu **PERMISSIONS** tab.

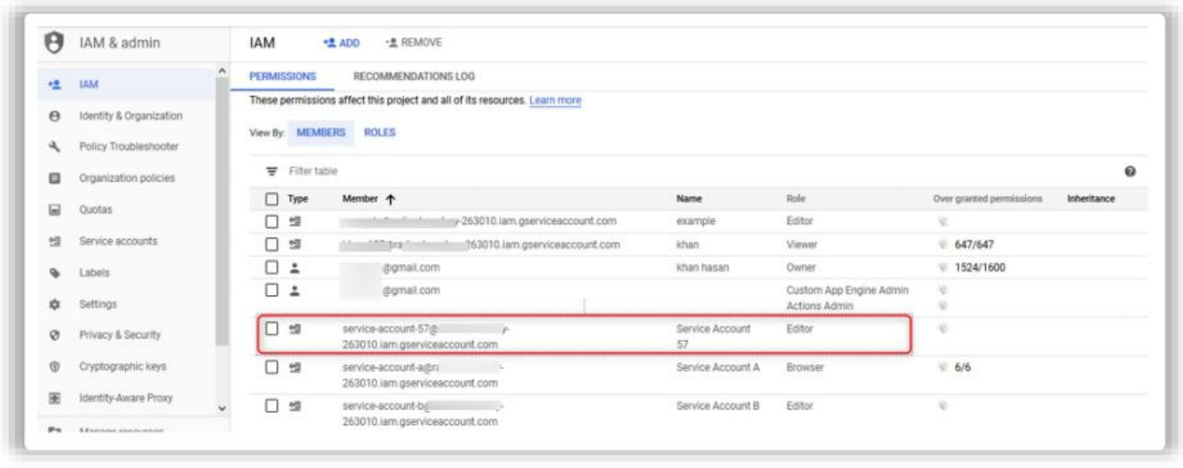
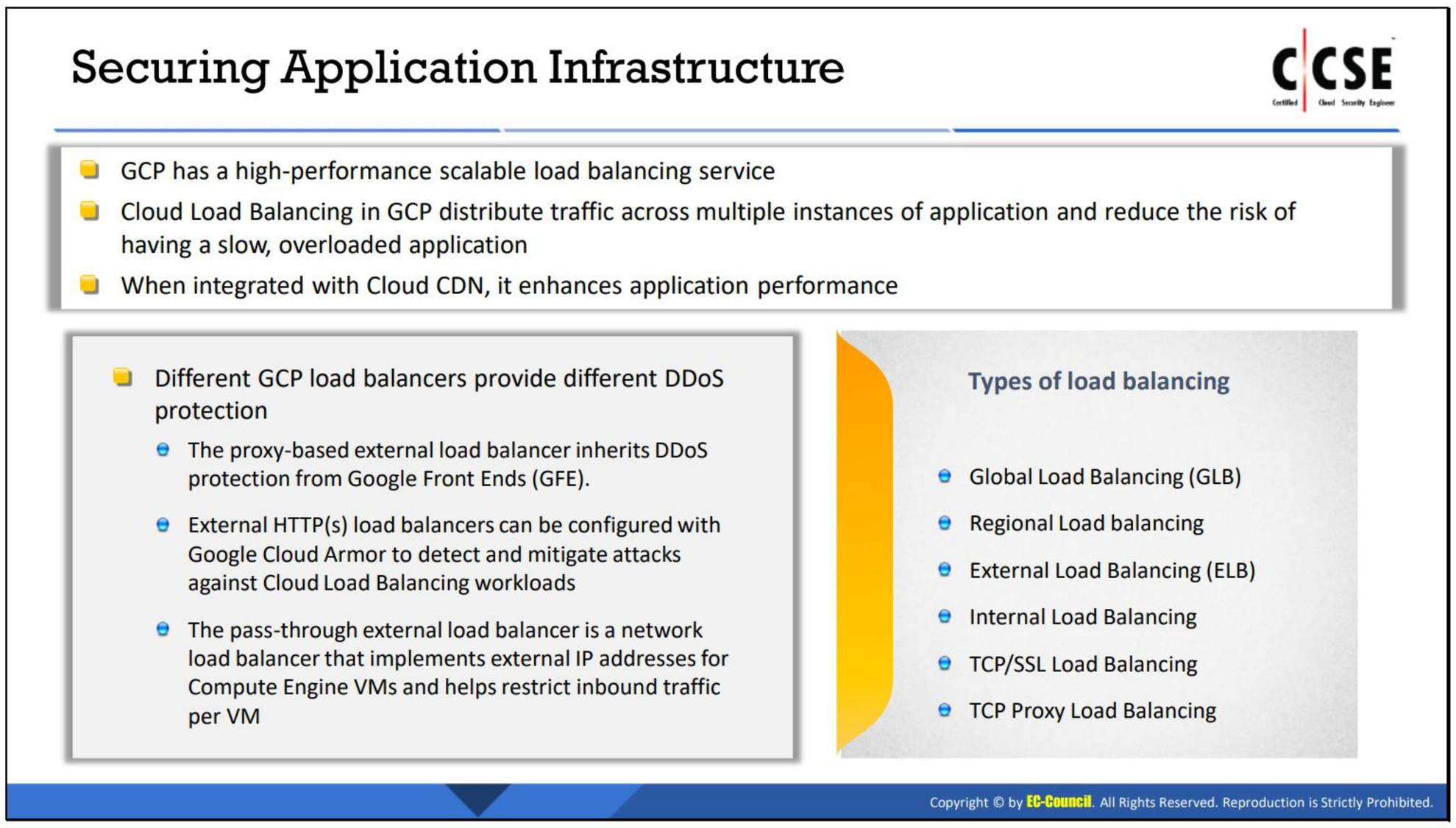


FIGURE 3.196:Permissions

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Securing Application Infrastructure

The servers on which the applications are deployed can get overloaded, which can be prevented in GCP through load balancing techniques. The traffic can be distributed across the instances in GCP if there is heavy traffic to the resources. GCP has a high-performing scalable load balancing service known as **Cloud Load Balancing**. With Cloud Load Balancing, the applications on Compute Engine can perform with full throttle.

Cloud load balancing can be integrated with Cloud CDN for better application performance. Cloud load balancing is software-based load balancing where load balancing can be applied to HTTPS, SSL, and UDP well as to terminate SSL traffic with HTTPS load balancing and SSL proxy. CLB provides health checking to ensure that the connections to the backend are load balanced.

Cloud Load Balancing's autoscaling feature can help applications in handling excess traffic based on the load. The user traffic on the application can be analyzed by Cloud Logging, which records all the requests sent to the load balancer.

Types of Google Cloud Load Balancing

- **Global load balancing**: The network traffic will be distributed across different geographical regions.
- **Regional load balancing**: The traffic can be distributed to a group of backend servers in the same region.
- **External load balancing:** ELB can be used to distribute traffic from the internet to a Google Private Cloud.
- **Internal load balancing:** Internal load balancing is used to distribute traffic within the network.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **TCP/SSL load balancing**: Within a Compute Engine, TCP traffic can be distributed across VMs.
- **HTTPS load balancing**: HTTP and HTTPS traffic can be balanced between multiple instances in multiple regions.
- **TCP proxy load balancing:** TCP Proxy Load Balancing is implemented on Google Front Ends for non-HTTP traffic.

Global Load Balancing

With GCP Global Load Balancing, traffic can be distributed across all connected servers located in different locations. The users of the applications will be dispersed, i.e., they will be accessing the application from different locations. When the distance between the application infrastructure and users increases, it takes more time to transmit data back and forth. Global load balancers help in connecting the user to the application server close to them. All the global backend instances will be front-ended by a single anycast IP. GLB ensures better disaster recovery solutions and better traffic management for optimal performance of the application. GCP Global Load Balancing does not need a VPN. The global load balancing products are HTTPS load balancing, SSL proxy load balancing, and TCP proxy load balancing.

Regional Load Balancing

- Regional load balancing can be used in cases that require IPv4 termination and all the backend servers are in the same region.
- Regional load balancing is for cases that are specific to a particular region, and the traffic is very high.
- The layer 4 traffic can be load balanced and redirected to this endpoint.
- With regional load balancers, the user IP address can be protected.
- TLS termination can be performed at the backend using regional load balancing.

hide01.ir

External Load Balancing

- External load balancers can be used to distribute the traffic from the internet to virtual private networks in GCP.
- External load balancing supports content-based cross region-based load balancing.
- External load balancing supports instance groups and cloud storage buckets.

Internal Load Balancing

- Internal load balancers are used when the users are outside GCP.
- It distributes traffic to instances inside the cloud.
- The applications can be deployed behind an internal IP address.
- The traffic can be redirected to the back end deployed in Kubernetes or Compute Engine.
- With internal load balancing, the traffic can be redirected to virtual machines.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In certain cases, internal load balancers consist of multiple backends to forward traffic.
- Internal load balancers perform health checks for load balancing.
- Internal load balancers use URL maps.

Load Balancing Based on Traffic Types

Google Front End (GFE) constitutes software-defined systems distributed in points of presence and performs global load balancing.

Andromeda is a software-defined Network Virtualization stack in GCP.

Maglev can be used for network load balancing.

Envoy Proxy, which is designed for native applications, is an open-source edge and service proxy.

For HTTP and HTTP(S) Traffic

External HTTPS load balancing: HTTPS load balancing deployed on GFE.

Internal HTTPS Load Balancing: Built on GCP's Andromeda Network virtualization stack and a managed service on open-source Envoy Proxy.

For Handling TCP Traffic

TCP proxy load balancing: Deployed on GFE and traffic can be distributed to the nearest region.

Network load balancing: Load balancing is done based on incoming IP protocol data.

Internal TCP/UDP load balancing: Provides proxy-based load balancing of layer 7 application data which is built on Andromeda.

For UDP Traffic

Network load balancing: Network load balancing can be used for UDP traffic based on the IP protocol data.

Internal TCP/UDP load balancing: Provides proxy-based load balancing of layer 7 application data.

External HTTPS Load Balancing

External HTTPS load balancing distributes traffic to the backends deployed in Compute Engine and Kubernetes Engine. External HTTPS load balancers are reverse proxy load balancers. External HTTP(S) load balancing is deployed on GFE, which offers cross region load balancing, directing traffic to the nearest healthy backend. External HTTP(s) load balancers can be configured with Google Cloud Armor to detect and mitigate attacks against Cloud Load Balancing workloads. External HTTPS load balancing supports backends such as:

- Instance groups
- Zonal network endpoint groups
- Serverless network endpoint groups; App Engine, cloud run

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Internet network endpoint groups
- Buckets in cloud storage

An external load balancer blocks the client requests and backend responses from reaching the back end. For HTTP /1.1 Compliance, external load balancer blocks

- Headers or first line containing invalid character.
- If the content length number is invalid.
- Unrecognized transfer encoding values.
- When an unparseable chunk is received load balancer blocks the connection to the client and back end.

External HTTPS Load Balancer Architecture

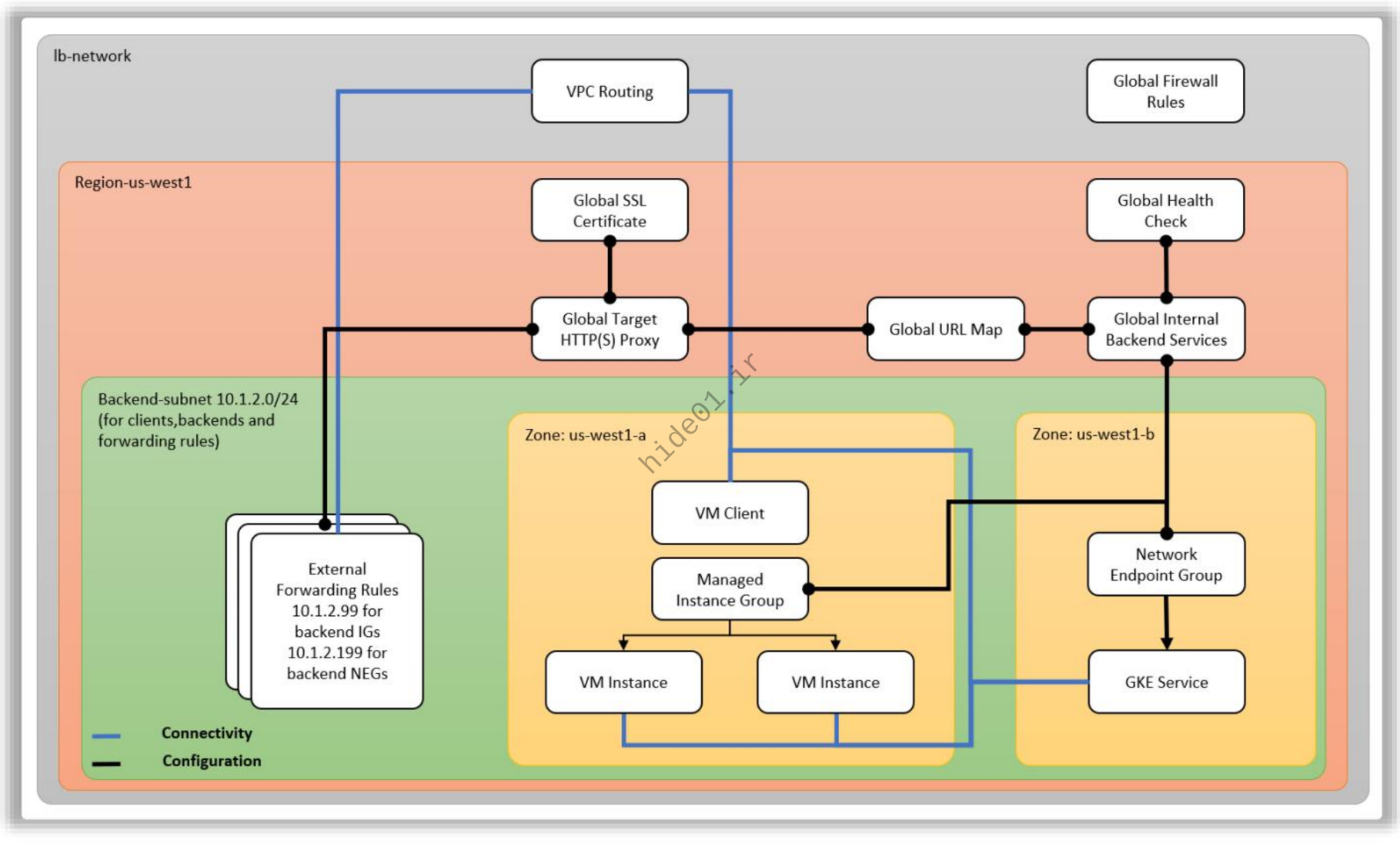


Figure 3.197: External HTTPS Load Balancer Architecture

- The external IP address, port and global target HTTPS proxy is defined by the **External Forwarding Rule**.
- The request from the user is received by the **global target HTTPS proxy** and by using the URL map it takes decision on traffic routing.
- The target HTTPS proxy uses **Global SSL certificates** to prove the identity.
- The **Global URL Map** make routing decisions based on cookies and headers.
- The **back end service or bucket** redirect the traffic to healthy back ends. The back ends can be:
  - Managed instance groups

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Unmanaged instance groups
- Network zonal end point groups
- Network internet end point groups
- Cloud storage buckets

- **Global Health Check** monitors back ends.
- Health check probes are accepted by **firewall**.

Source: https://cloud.google.com

Setup External HTTP Load Balancer

Step 1: Create a managed instances group

- In GCP, navigate to **Instance Groups** page.
- Click **Create Instance Group,** select **New Managed Instance Group.**
- Enter the **Name** lb-backend-example.
- Select **Single Zone** under **Location.**
- Select the preferred region under **Region** and select **us-east1-b** for **Zone**.
- Under **Instance Template,** select **Create a new instance template.**
- Enter the **Name** lb-backend-template.
- Set Boot disk to Debian Image like **Debian GNU Linux9.** The instructions use command available on Debian, like apt-get.
- The below script can be inserted in the **Startup Script Field** on the **Management** tab

```
#! /bin/bash
  apt-get update
  apt-get install apache2 -y
  a2ensite default-ssl
  a2enmod ssl
  vm_hostname="$(curl -H "Metadata-Flavor:Google" \
  http://169.254.169.254/computeMetadata/v1/instance/name)"
  echo "Page served from: $vm_hostname" | \
  tee /var/www/html/index.html
```

- On the **Networking** tab add the network tags: allow-health-check.
- Click **Save and Continue.**
- Select **Don’t autoscale** under **Autoscaling mode.**
- Enter 2 under **Number of Instances.**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click **Create.**

Step 2: Add named port to instance group.

- In console, navigate to **Instance groups** page.
- Click the name of the instance group and click **Edit Group**.
- Click **Specify Port Name Mapping.**
- Click **Add Item.**
- For port name enter http and port no enter 80.
- Click **Save.**

Step 3: Configure firewall rule.

- Navigate to **Firewall** page in Cloud Console.
- Click on **Create Firewall Rule**.
- Enter fw-allow-health-check for name.
- Under **Network**, select **Default.**
- Under **Targets,** select **Specified Target Tags.**
- The **target tags** field is populated with allow-health-check.
- Change the **Source Filter** to **IP ranges**.
- Set **Source IP ranges** to 130.211.0.0/22 and 35.191.0.0/16.
- Select **Specified Protocols and Ports** under **Protocols and Ports.**
- Check box **tcp** and enter port no 80.
- Click **Create.**

Step 4: Reserve an external IP address.

- In console, navigate to **External IP addresses** page.
- Click **Reserve Static address.**
- Enter lb-ipv4-1 for **name.**
- Change the **Network Service Tier** to **Premium, IP Version** to **IPv4,** and the **Type** to **Global.**
- Click **Reserve.**

Step 5: Setup load balancer.

- In console, navigate to the **Load balancing** page.
- Click **Create Load Balancer.**
- Under **HTTPS Load Balancing,** click **Start Configuration.**
- Select **from Internet to my VMs** and click **Continue.**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enter the load balancer name as web-map-http.
- Click on **Backend Configuration.**
  - Under **Create or select backend services and backend buckets,** select **Backend services > Create a backend.**
  - Give a name to the backend service such as web-backend-service.
  - Select **HTTP** as **Protocol.**
  - Give the **Port Number** as http.
  - Under **Backends > New Backends > Instance Group,** select the instance group lb-backend-example.
  - Enter the **Port Numbers** 80.
  - Keep the other default settings as such.
  - Under the option **Health Check,** click **Create a health check** and enter a name as http-basic-check.
  - Change the protocol to **HTTP.**
  - Click on **Save and continue.**
  - Keep the other default settings as such.
  - Click **Create.**
- Keep the default settings as such under **Host and Path Rules.**
- Under **Front end Configuration.**
  - Change the **Protocol** to **http.**
  - Change the **IP address** to lb-ipv4-1 created earlier.
  - Change **Port** to 80.
  - Click **Done.**
- Click **Review and Finalize.**
- Click **Create.**
- Click the name of the load balancer after the load balancer is created.
- Note the **IP:Port** of the load balancer on **Load Balancer Details.**

Step 6: Test the traffic.

- Navigate to the **Load Balancing** page in the console.
- Click on the created load balancer.
- Ensure whether the VMs are healthy by checking.
- Check whether the VMs are healthy.

video01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The **Healthy** column populates and shows both are healthy (2/2).
- Reload the page if it is not found in the above way.
- Check the firewall configuration and network tag assigned to the backend VM.

- If the result is healthy, the load balancer can be tested from a web browser by typing http://*IP_ADDRESS* (replace IP address by load balancer's IP address.
- The browser will display a page with the name of the instance with the zone.

Internal HTTPS Load Balancing

The applications can be deployed behind an internal IP address with the proxy-based internal HTTPS load balancer. The HTTPS and HTTP traffic will be redirected to the backends deployed on Compute Engine and Kubernetes Engine. The internal HTTPS load balancer is based on the open-source Envoy Proxy. It consists of the following.

- **Internal IP address:** The internal IP address that can be accessed by the users who are in the same region of the load balancer.
- **Multiple backend services:** The load balancer forwards the traffic to the backends located in the same region as the load balancer.

An internal HTTPS load balancer can improve the capabilities of legacy applications by deploying the internal load balancer in the frontend of the application. Thus, the traffic can be routed to some microservices using the load balancers capability. The URL map of the load balancer can be updated to redirect the traffic to new services.

Architecture of Internal HTTPS Load Balancer

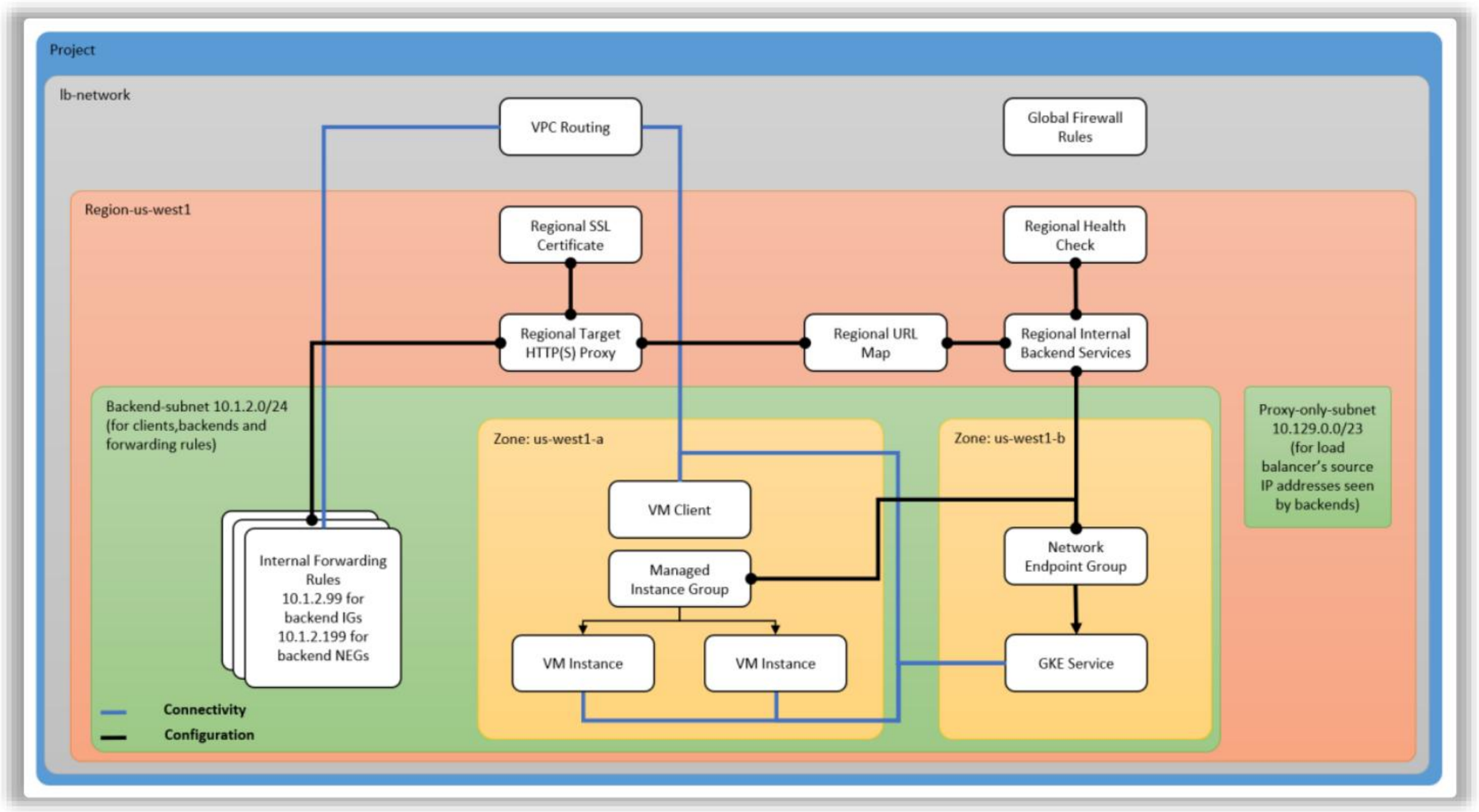


Figure 3.198 : Architecture of Internal HTTPS Load Balancer

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Proxy-only Subnet:** The IP addresses to run Envoy Proxy will be provided by Proxy-only Subnet. The same Proxy-only subnet is shared by all the regional internal HTTPS load balancers and VPC network because they share a pool of envoy proxies.
- **Forwarding Rule and IP Address:** The internal managed forwarding rule manages the IP address, port for the internal HTTPS load balancer. Users will use this IP address and port to connect to envoy proxies.
- **Regional Target HTTPS Proxy:** The HTTPS connections from users are terminated by the target proxy by checking the URL map. For user authentication, the target proxy uses SSL certificates.
- **SSL Certificates:** For secure communication between the internal HTTPS load balancer, SSL certificates can be used. Thus, end-to-end encryption can be ensured.
- **URL Map:** The routing of the traffic can be based on the URL map based on the cookies and header information. URL map provides additional functionalities such as rewriting the headers, timeout policies, etc.
- **Backend Services:** Traffic will be distributed to the healthy backends by the regional backend services. The users and backend endpoints must be in the same region in internal HTTPS load balancer.
- **Health Check:** The backends must be monitored periodically to reduce risks such as handling requests it cannot service.
- **Firewall Rules:** The internal HTTPS load requires an ingress allow rule to permit traffic from Health Check and Proxy-only Subnet.

hiddn01.ir

Steps to Set Up Internal HTTPS Load Balancing

Source: https://cloud.google.com

Step 1: Configure network and subnet for backends.

- In console, navigate to the **VPC Network** page.
- Click **Create VPC Network.**
- Enter “lb-network” for the **Name.**
- Under the **Subnet** section
  - Change **Subnet creation mode** to **Custom.**
  - Under **New Subnet,** enter
    - **Name:** backend-subnet
    - **Region**: us-west1
    - **IP address range:** 10.1.2.0/24
  - Click **Done.**
- Click **Create.**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 2: Configure firewall rules.

- Navigate to the Firewall Rules page in Console.
- The incoming SSH connections can be allowed by clicking on **Create Firewall Rule.**
  - **Name:** fw-allow-ssh
  - **Network:** lb-network
  - **Direction of Traffic:** Ingress
  - **Action on Match:** Allow
  - **Targets:** Specified target tags
  - **Target tags:** allow-ssh
  - **Source Filter:** IP Ranges
  - **Source IP Ranges:** 0.0.0.0/0
  - **Protocols and Ports:**
    - Select **Specified protocols and ports.**
    - Checkbox **tcp,** give the port no 22.
- Click **Create.**
- Click **Create Firewall Rule** again to allow GCP health checks.
  - **Name:** fw-allow-health-check
  - **Network:** lb-network
  - **Direction of Traffic: Ingress**
  - **Action on Match: Allow**
  - **Targets: Specified target tags**
  - **Target tags:** load-balanced-backend
  - **Source Filter: IP ranges**
  - **Source IP ranges:** 130.211.0.0/22 and 35.191.0.0/16
  - **Protocols and Ports:**
    - **Select Specified Protocols and Ports.**
    - Checkbox **tcp** and enter port no 80.
  - Click **Create.**
- To allow load balancers proxy servers to connect the backends, click on **Create firewall rule** for the third time.
  - **Name:** fw-allow-proxies

hide0.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Network:** lb-network
- **Direction of traffic: Ingress**
- **Action on Match: Allow**
- **Targets: Specifies target tags**
- **Target tags:** load-balanced-backend
- **Source Filter: IP ranges**
- **Source IP ranges:** 10.129.0.0/23
- **Protocols and Ports:**
  - Select **Specified protocols and ports.**
  - Check box **tcp** and enter port numbers 80,443,8080.

- Click **Create.**

Step 3: Create managed instances group.

- Navigate to **Instance Groups** in the console
- Click **Create Instance Group.**
- Select **New Managed Instance Group.**
- Enter the **Name** as l7-ilb-backend-example.
- Select **Single zone** under location.
- Select us-west1 as **Region.**
- Select us-west1-a as **Zone.**
- Choose to **Create a new instance template** under the **Instance template.**
  - Enter l7-ilb-backend-template for **Name.**
  - Set the boot disk to the Debian image like **Debian GNU/Linux 9 (stretch).**
  - Under **Management** tab in **Management, security, disks, networking, sole tenancy,** enter the following into the **Startup Script.**

```
#! /bin/bash
apt-get update
apt-get install apache2 -y
a2ensite default-ssl
a2enmod ssl
vm_hostname="$(curl -H "Metadata-Flavor:Google" \
http://169.254.169.254/computeMetadata/v1/instance/name)"
echo "Page served from: $vm_hostname" | \
```


Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
tee /var/www/html/index.html
systemctl restart apache2'
```

- Under **Networking,** select lb-network as the **Network** and for **Subnet** choose backend-subnet**.**
- Add the network tags: allow-ssh and load-balanced-backend.
- Click **Save and Continue.**

- Enter the number of instances that are to be created in the group.
  - Select **Don't configure autoscaling** under **Autoscaling mode.**
  - Under **Number of Instances,** enter 2.
- Click **Create.**

Step 4: Configuration of the load balancer.

Selecting the type of load balancer

- Navigate to the Load Balancing page in the console.
- Click on **Start Configuration** under **HTTPS Load Balancing.**
- To set the internal load balancer select **Only between my VMs.**
- Click **Continue.**

hide01.ir

Preparing the Load Balancer

- **Provide** l7-ilb-map as the **Name** of the load balancer.
- Choose us-west1 as the **Region.**
- Choose lb-network as the **Network.**
- Do not close the window.

Reserving a proxy-only subnet

- Choose **Reserve a Subnet.**
- Provide proxy-only-subnet as the **Name.**
- Provide 10.129.0.0/23 as the **IP address range.**
- Select **Add.**

Configure backend service

- Choose **Backend configuration.**
- Choose **Create a backend service** from the **Create or select backend services** menu.
- Keep the **Name** as **l7-ilb-backend-service**.
- Keep **Backend type** as **instance groups**.
- Set the following values in **New backend** section.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Instance Group: l7-ilb-backend-example.**
- **Port numbers:** 80.
- **Balancing Mode: Utilization.**
- Click **Done.**

- Choose **Create a health Check** in **Health Check** section.
  - **Name:** l7-ilb-basic-check.
  - **Protocol:** HTTP.
  - **Port:** 80.
  - Click **Save & Continue.**
- Select **Create.**

Configuration of URL Map

- Click on **Host and Path rules.**
- Ensure that the backend service is **l7-ilb-backend-service**.

Configuration of Frontend

Configuration for HTTP:

- Click **Frontend Configuration.**
- Click **Add frontend IP and Port.**
- Set the **Name: l7-ilb-forwarding-rule**.
- Set **Protocol: HTTP.**
- Set **Subnetwork** to **backend-subnet**.
- Select **Reserve a static internal IP address** under **Internal IP.**
- Give the following details in the panel.
  - **Name: l7-ilb-ip.**
  - Select **Let me Choose** under **Static IP address.**
  - Enter 10.1.2.99 under **Custom IP address.**
  - Click **Reserve.**
- Set **Port** as 80.
- Click **Done.**

Configuration for HTTPS

- Click on **Frontend Configuration.**
- Click **Add Frontend IP and port.**

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enter the **Name:** l7-ilb-forwarding-rule.
- Select **Protocol** as HTTPS (includes HTTPS/2).
- Set the **Subnetwork** as backend-subnet.
- Select **Reserve a static internal IP address** under **Internal IP.**
- Enter the following details in the panel.
  - **Name:** l7-ilb-ip.
  - **Static IP address: Let me choose.**
  - **Custom IP address:** 10.1.2.99.
  - Click **Reserve.**
- Set the **Port:** 443.
- Click **Certificate** drop down.
  - Select the SSL certificate from the dropdown if there is a self-managed SSL certificate resource.
  - Or Click **Create a New certificate**
    - **Name:** l7-ilb-cert.
    - Upload the PEM formatted files like **Public Key Certificate, Certificate Chain, Private Key.**
    - Click **create.**
- To add additional certificate resources
  - Click **Add certificate.**
  - Select a certificate from the list or click on **Create a New certificate** and follow the above steps.
- Click **Done.**
- Click **Create.**

hide01.ir

TCP Proxy Load Balancing

TCP proxy load balancer is a reverse proxy load balancer. Here, the TCP traffic is distributed to the VM instances in the VPC network. In the TCP proxy load balancer, the TCP traffic is terminated at the load balancing layer and forwarded to the nearest backends. The **proxy-based external load balancers** inherit DDoS protection from GFE. The features of TCP proxy load balancer are briefly described below.

- **IPv6 termination:** The IPv6 requests after terminating at the load balancing layer are proxied to the backends over IPv4.
- **Intelligent routing:** Intelligent routing of requests to the backend locations with capacity.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Security patching:** Cloud load balancing applies patches to the TCP stack during vulnerabilities.
- **Support TCP ports:** It supports well-known TCP ports.

Architecture of TCP Proxy Load Balancer

- **Forwarding rules and IP addresses:** The forwarding rules route traffic based on IP address, port, and protocol. This eliminates the need for DNS-based load balancing as the forwarding rules provide an IP address.
- **Target proxies:** The TCP connections are terminated from users, and new connections are created to the backends. By proxy protocol, the user IP address and port no can be preserved.
- **Backend services:** The incoming traffic can be routed to more backends using backend services. TCP proxy load balancers have single backend service resources, and it specifies the health checks to be performed. The TCP proxy load balancer use only the specified protocol for communication with backends.
- **Firewall Rules:** A firewall rule can be created for allowing connections from the load balancer/GFE health check ranges. The ports used by each forwarding rule and ports used by health checks configured for backend service must be allowed.
- **Source IP addresses:** The source IP addresses are in the range 35.191.0.0/16 and 130.211.0.0/22.
- **Open Ports:** The TCP proxy load balancers are reverse proxy load balancers that terminate the incoming connections and start new connections from the load balancer to backends, which is provided by GFE.

hade01.ir

Steps to Setup TCP Proxy Load Balancer

Source: https://cloud.google.com

Follow these steps to set up a TCP proxy load balancer:

Step 1: Configuring instance.

- Navigate to the **VM instances** page in the console.
- Click on **Create Instance.**
- Give **Name** as 'ig-us-central1-1'.
- Give the **Region** as 'us-central1'.
- Give the **Zone** as 'us-central1-b'**.**
- Under the **Management** option in **Management, security, disks, networking, sole tenancy,** click on **Networking.**
- Enter in the tags field 'tcp-lb'.
- Click on **Management** and type the given script in **Startup Script** field:

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
sudo apt-get update
sudo apt-get install apache2 -y
sudo sed -i '/Listen 80/c\Listen 110' /etc/apache2/ports.conf
sudo service apache2 restart
echo '<!doctype html><html><body><h1>ig-us-central1-
1</h1></body></html>' | sudo tee /var/www/html/index.html
```

- Keep the default values as such and click on **Create.**
- With the same settings, create 'ig-us-central1-2' and type the below script in the Startup script:

```
sudo apt-get update
sudo apt-get install apache2 -y
sudo sed -i '/Listen 80/c\Listen 110' /etc/apache2/ports.conf
sudo service apache2 restart
echo '<!doctype html><html><body><h1>ig-us-central1-
2</h1></body></html>' | sudo tee /var/www/html/index.html
```

- With the same settings, create 'ig-us-east1-1' with the **region** set as 'us-east1' and **Zone** as 'us-east1-b'. In the **Startup script** field, type

hide01.ir

```
sudo apt-get update
sudo apt-get install apache2 -y
sudo sed -i '/Listen 80/c\Listen 110' /etc/apache2/ports.conf
sudo service apache2 restart
echo '<!doctype html><html><body><h1>ig-us-east1-
1</h1></body></html>' | sudo tee /var/www/html/index.html
```

- With the same settings, create 'ig-us-east1-2', with the **region** as 'us-east1' and **Zone** as 'us-east1-b'. In the **Startup Script** field, type

```
sudo apt-get update
sudo apt-get install apache2 -y
sudo sed -i '/Listen 80/c\Listen 110' /etc/apache2/ports.conf
sudo service apache2 restart
echo '<!doctype html><html><body><h1>ig-us-east1-
2</h1></body></html>' sudo tee /var/www/html/index.html
```

Step 2: Create Instance Group for each zone and Adding Instances.

- Navigate to **Instance groups** in GCP Console.
- Click on **Create instance group.**
- Click on **New Unmanaged Instance group.**
- Set the **Name** as 'us-ig1'.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Set the **zone** as 'us-central1-b'.
- Click on **Specify Port mapping,** i.e., creating a named port to map incoming traffic to a port number. Set the following,
  - **Port Name:** tcp110
  - **Port Numbers:** 110
- For **VM Instances,** choose **ig-us-central1-1** and **ig-us-central1-2**.
- Keep the other settings as such and click **Create.**
- The above steps can be repeated by setting the following values,
  - **Name:** us-ig2
  - **Region:** us-east1
  - **Zone:** us-east1-b
  - **Port name:** tcp110
  - **Port Numbers:** 110
  - **Instances: ig-us-east1-1** and **ig-us-east1-2**.

Step 3: Configuration of load balancer.

- Navigate to the **Load Balancing page** in Console.
- Click **Create Load balancer.**
- Configure the load balancer as follows
  - Click **Start configuration** under **TCP Load balancing.**
  - Choose **From Internet to my VMs** under **Internet Facing or internal only**.
  - Change **Multiple regions or single region** to **Multiple regions.**
  - Click **Continue.**
  - Give the **name** as 'my-tcp-lb'.
  - Click on **Backend configuration.**
  - Select **Instance Groups** under **Backend Type.**
  - Select **TCP** under **Protocol.**
- Configure the first backend as follows
  - Select instance group **us-ig1** under **New backend.**
  - Keep the other values as such.
- Configure the second backend as follows
  - Click **Add backend.**

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The instance group should be selected as **us-ig2**.
- In **Port Numbers** delete 80 and add 110.

- Configure health check as follows
  - Select **create health check,** under **Health Check.**
  - Give the health check **name** as my-tcp-health-check.
  - Select **TCP** as the **Protocol.**
  - Give **Port** as 110.
- Keep the other values as such.
- Click on **Save and Continue.**
- Verify a checkmark near **Backend Configuration.**

Step 4: Configuration of frontend services.

- Click on **Frontend configuration.**
- Setup the first forwarding rule.
  - Give the **Name** as my-tcp-lb-forwarding-rule.
  - **Protocol: TCP**
  - Select **Create IP address** under **IP address.**
    - Enter **Name** of tcp-lb-static-ip.
    - Click **Reserve.**
  - Set **Port** as 110.
  - Under **Proxy Protocol,** click **ON.**
  - Click **Done.**
- Setup the second forwarding rule.
  - Click on **Add Frontend IP and Port.**
  - Enter the **Name** as my-tcp-lb-ipv6-forwarding-rule.
  - Select **TCP** as **Protocol.**
  - Set the **IP Version** as IPv6.
  - Click **Create IP Address** under **IP address.**
    - Give the name of tcp-lb-ipv6-static-ip.
    - Click **Reserve.**
  - Set the **Port** as 110.
  - Under **Proxy Protocol,** click **On.**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click **Done.**
- Verify checkmark near **Frontend Configuration.**

- Click **Review and Finalize.**
- Click **Create.**

Step 5: Configuration of firewall rule to load balancer.

- Navigate to the firewall page in console.
- Click on **Create Firewall Rule.**
- Provide the name of allow-tcp-lb-and-health.
- Select default under **Network.**
- Under targets, select **Specified target tags**.
- Assign the **Target tags** to tcp-lb.
- Assign **Source Filter** to IP ranges.
- Assign the **Source IP ranges** as 130.211.0.0/22 and 35.191.0.0/16.
- Assign **Allowed protocols and ports** to tcp:110.
- Click **Create.**

Network Load Balancing

ide01.ir

GCP external TCP/UDP network load balancer is a regional, pass-through load balancer. The TCP/UDP traffic is distributed among VM instances in the same region. The features of network load balancer are listed below:

- Network load balancer is a managed service that is implemented using Andromeda virtual networking and Google Maglev.
- Network load balancers are not proxies, providing direct server return in which the responses from the VM travel directly to the users.
- Network load balancers can be used to load balance a TCP port not supported by other load balancers.
- The backend service-based network load balancer gives fine-grained controls.
- Backend service-based load balancer can perform health checks, session affinity, and timeouts.

Network Load Balancer Architecture

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

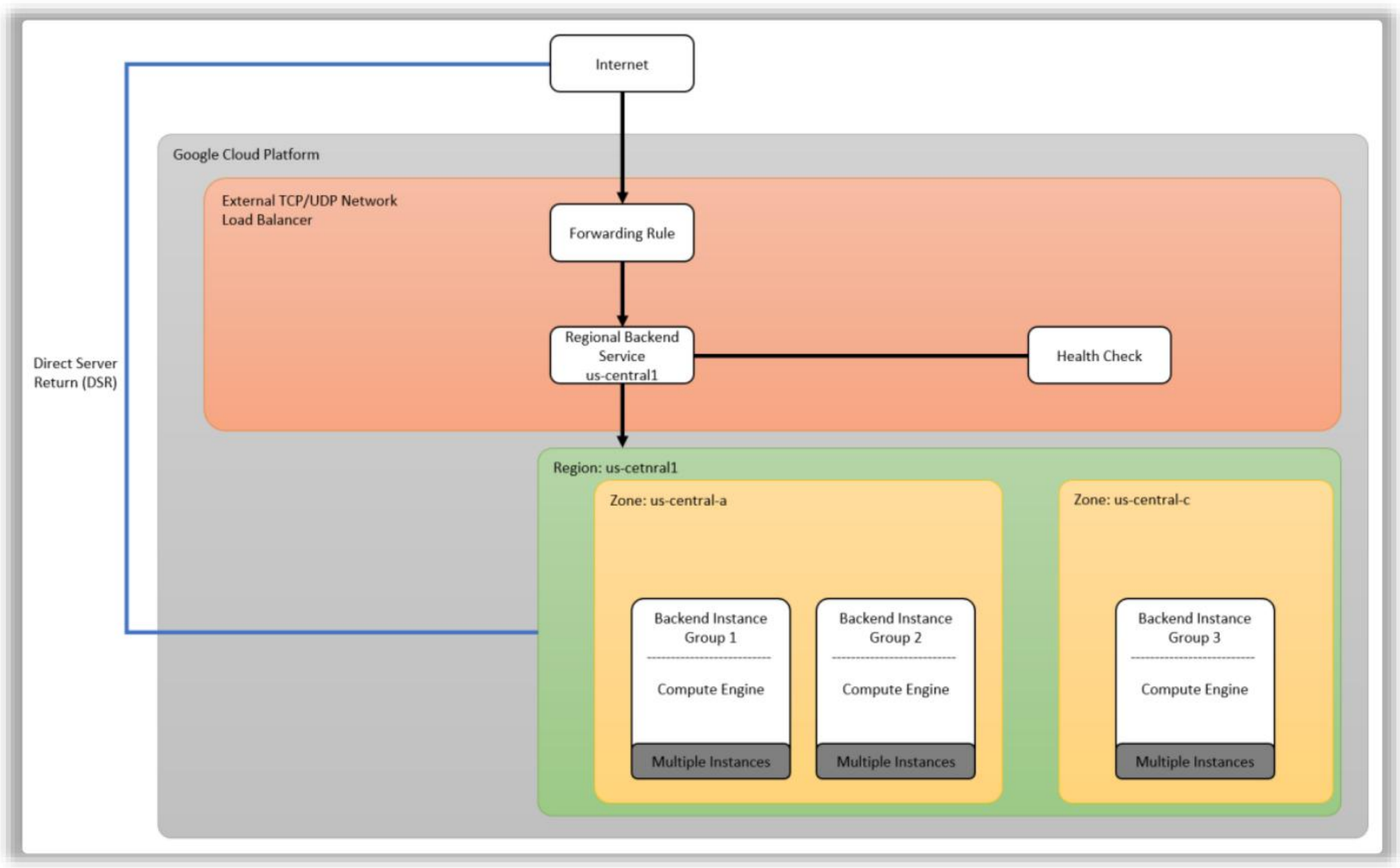


Figure 3.199: Network Load Balancer Architecture

- **IP address:** The network load balancer requires a forwarding rule which defines a single regional external IP address.
- **Forwarding rule:** The protocols and ports on which the load balancer accepts traffic is specified by the regional external forwarding rule.
- **Regional backend service:** The regional backend service of the network load balancer defines its behavior and the traffic distribution. The backend services have the backend parameters such as
  - **Protocol:** Based on the IP address and ports specified by the external forwarding rules backend services accept either TCP or UDP traffic but not both.
  - **Traffic distribution:** Based on a configured session affinity backend services allow traffic distribution.
  - **Health check:** A regional health check is associated with backend services.
- **Backend instance groups:** The connection is distributed by backend VMs within managed or unmanaged instance groups which can be regional or zonal.
  - **Regional managed instance groups:** The traffic is automatically distributed among multiple zones.
  - **Zonal managed or unmanaged instance groups:** In the same region in different zones zonal instance groups can be used for protection.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Health checks**: The regional health checks provided by network load Balancing check for which instances can receive new connections. Network load balancing supports HTTP, HTTPS, HTTP/2, SSL, or TCP health checks.
- **Firewall rules:** An ingress allow firewall rule can be created to accept traffic from internet for the protocols and ports using 0.0.0.0/0 source range.

- **Return path:** Network load balancer has direct server return, that is, the response from backend VM's travel directly to users.

Steps to Setup Network Load Balancer with Backend Service

Source: https://cloud.google.com

Follow these steps to set up a network load balancer with backend service:

Step 1: Setup the instances.

- Navigate to **Instance Groups** page in console.
- Click **Create Instance Group.**
- Select **New managed instance group.**
- Type the **Name** as 'ig-us-1'.
- Choose **Single Zone** as **Location.**
- Choose **us-central1** as **Zone.**
- Click **Create a new instance template** under **Instance template.**
  - Enter the **name** as 'ig-us-template'.
  - Set the boot disk to Debian image like **Debian GNU/Linux9 (stretch).**
  - The given script can be inserted into the **Management** tab:

```
#! /bin/bash
apt-get update
apt-get install apache2 -y
a2ensite default-ssl
a2enmod ssl
vm_hostname="$(curl -H "Metadata-Flavor:Google" \
http://169.254.169.254/computeMetadata/v1/instance/name)"
echo "Page served from: $vm_hostname" | \
tee /var/www/html/index.html
systemctl restart apache2
```

  - Under **Networking** enter the **tags** field with network-lb tag.
  - Click **Save & Continue.**

hade01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Specify the number of instances.
- Click **Create.**
- A second managed instance group can be created in the us-central1-c zone with the details:
  - **Name:** ig-us-2
  - **Zone:** us-central1-c

Step 2: Configuration of firewall rules.

- Navigate to the firewalls page in the console.
- Choose **Create Firewall Rule.**
- Assign the name as allow-network-lb.
- Select default under **Network.**
- Choose **Specified target tags** under targets.
- Assign the **Target tags** as network-lb.
- Assign the **Source IP ranges** as 0.0.0.0/0.
- In **specified protocols and ports** check box **tcp** and enter 80**.**
- Click **Create.**

hide01.ir

Step 3: Configuration of load balancer.

- Navigate to **Create a Load Balancer Page** in GCP Console.
- Under TCP Load balancing, click **Start Configuration.**
- Under **Internet Facing or Internal Only,** select **From my internet to VMs.**
- Select **Single region only** for **Multiple regions or single region.**
- Select **backend service** for **backend type**.

Configuration of Backend

- On the window of **New TCP Load Balancer,** type the **Name** as tcp-network-lb.
- Click on **Backend configuration** and set the following,
  - Select the **Region** as **us-central1.**
  - In **Backends,** from **instance group** dropdown, select 'ig-us-1' and click **Done.**
  - Click on **Add backend** and repeat the above steps to add ig-us-2.
  - Select **Create health check** under **Health Check** and enter the given information:
    - **Name:** tcp-health-check
    - **Protocol:** TCP

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Port:** 80

- Click on **Save & Continue**
- Verify checkmark next to **Backend configuration.**

Configuration of Frontend

- Click on **Frontend configuration.**
- Enter the **Name** as network-lb-forwarding-rule.
- From the **IP** dropdown menu click on **Create IP address.**
  - Give the name as network-lb-ip on the **Reserve a new static IP address.**
  - Click **Reserve.**
- Give **Port** as 80.
- Click **Done.**
- Verify a blue circle with checkmark near **Frontend Configuration.**
- Click **Review and Finalize.**
- Click **Create.**

Internal TCP/UDP Load Balancing

To run the applications behind an internal load balancing IP address that can be accessed by the internal VM instances, an internal TCP/UDP load balancer can be used. An internal TCP/UDP load balancer routes traffic from the users to the backends that are healthy without any single point of failure.

Architecture of Internal TCP/UDP Load Balancing

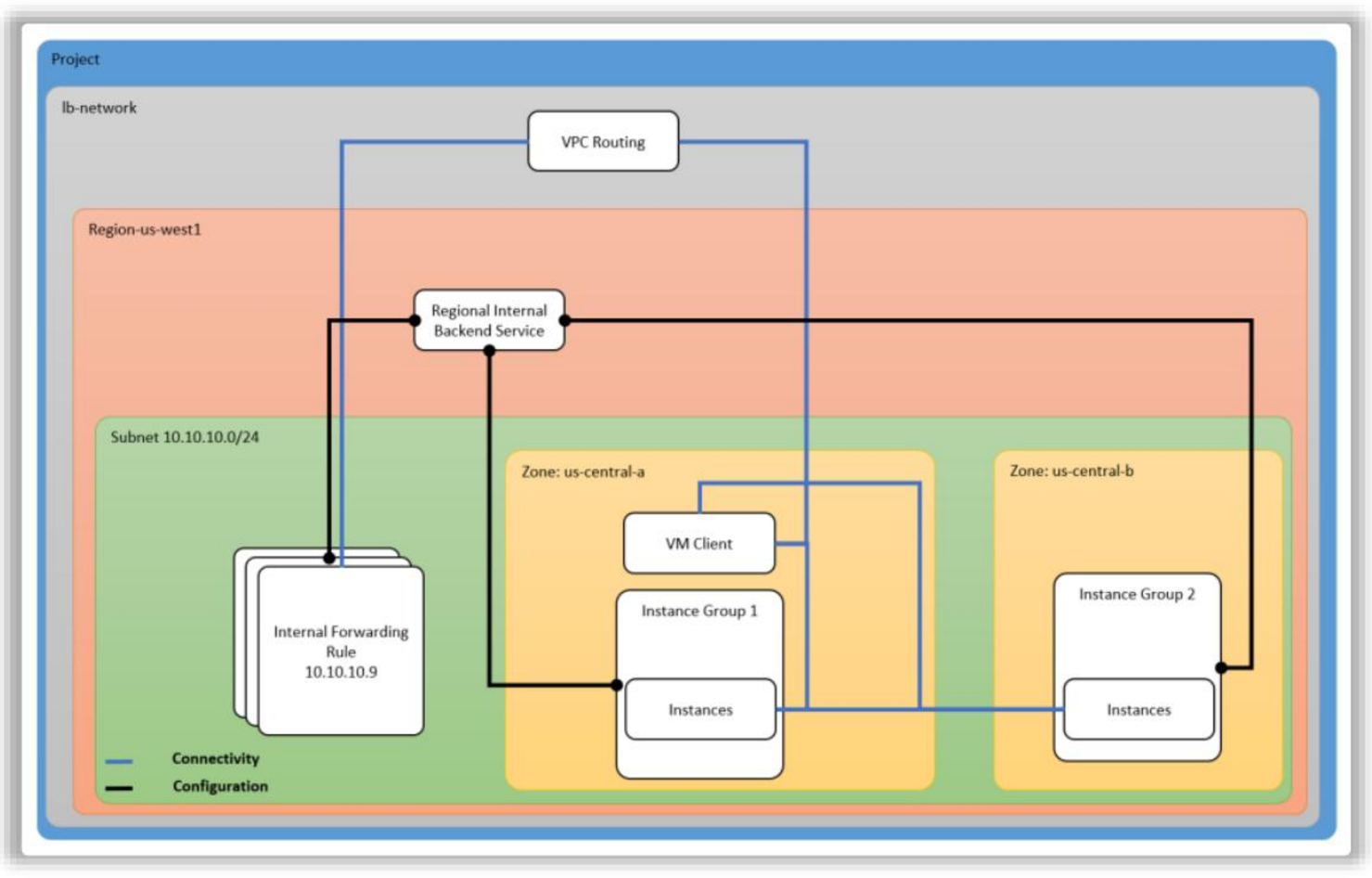


Figure 3.200: Architecture of Internal TCP/UDP Load Balancing

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Internal IP address:** The IP address of the internal TCP/UDP load balancer is an internal IPv4 address from the primary IP range of subnet. The internal IP address can be created while creating the internal forwarding rule.
- **Firewall rules:** The internal TCP/UDP load balancer requires an ingress allow rule to allow traffic from the internal IP address of users and traffic from health check ranges.
- **Forwarding rules:** The protocols and ports in which the load balancer accepts traffic are specified by the forwarding rule. The internal forwarding rule should specify a subnet in the same VPC network and region as the backend components.
- **Backend service:** The internal TCP/UDP load balancer has a regional internal backend service that defines the backend characteristics. The backend parameters are
  - **Protocol:** The traffic to be delivered to the backend VMs must be the same port used for sending traffic.
  - **Traffic distribution:** Based on a configurable session affinity backend service, allow traffic distribution.
  - **Health check:** The backend service must have a health check functionality.
- **Health check:** The new connections routed by Internal TCP/UDP load balancers are based on a health check status. The health check protocols that can be used are HTTP, HTTPS, HTTP/2, and SSL/TCP.

hide6.ir

Steps to Setup Internal TCP/UDP Load Balancing

Source*: https://cloud.google.com*

Step 1: Configuring network, region, and subnet.

- Navigate to **VPC Networks Page** in GCP Console.
- Click on **Create VPC Network.**
- Assign the name as 'lb-network'.
- Under the section **Subnet.**
  - Change the **Subnet Creation Mode** to **Custom.**
  - Provide the below information under **New Subnet** section.
    - **Name:** lb-subnet
    - **Region:** us-west1
    - **IP address range:** 10.1.2.0/24
    - Click **Done**
  - Select **Add Subnet** and type the following.
    - **Name:** europe-subnet
    - **Region:** europe-west1

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **IP Address range:** 10.3.4.0/24
- Click **Done**

- Click **Create**

Step 2: Configuration of firewall rules.

- Navigate to the **Firewall Page** in console.
- Click on **Create Firewall Rule** and give the following information.
  - **Name:** fw-allow-lb-access
  - **Network:** lb-network
  - **Priority:** 1000
  - **Direction of Traffic:** Ingress
  - **Action on Match:** Allow
  - **Targets:** All instances in the network
  - **Source Filter:** IP ranges
  - **Source IP ranges:** 10.1.2.0/24 and 10.3.4.0/24.
  - **Protocols and Ports:** Allow all
- Click **Create.**
- To allow incoming SSH connections again click on **Create Firewall Rule** and give the following information
  - **Name:** fw-allow-ssh
  - **Network:** lb-network
  - **Priority:** 1000
  - **Direction of Traffic:** Ingress
  - **Action on Match:** Allow
  - **Targets:** Specified target tags
  - **Target tags:** allow-ssh
  - **Source Filter:** IP ranges
  - **Source IP Ranges:** 0.0.0.0/0
  - **Protocols and Ports:** Select Specified Protocols and Ports and enter tcp:22
- Click **Create.**
- To allow Google Cloud Health Checks, click again on **Create Firewall Rule.**
  - **Name:** fw-allow-health-check

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Network:** lb-network
- **Priority:** 1000
- **Direction of Traffic:** Ingress
- **Action on Match:** Allow
- **Targets:** Specified target tags
- **Target tags:** allow-health-check
- **Source Filter:** IP ranges
- **Source IP Ranges:** 130.211.0.0/22 and 35.191.0.0/16
- **Protocols and Ports:** Allow all

- Click **Create**

Step 3: Creating backend VM's and instance groups.

Creating Backend VMs

- Navigate to the **VM Instances Page** in Console.
- Create four VMs with the below names and zones.
  - **Name**: vm-a1, zone: us-west1-a
  - **Name**: vm-a2, zone: us-west1-a
  - **Name**: vm-c1, zone: us-west1-c
  - **Name**: vm-c2, zone: us-west1-c
- Click on **Create Instance.**
- Assign the **Name** as indicated in above step.
- For **Region** select us-west1 and **Zone** as in the above step
- Under the section **Boot Disk,** check whether **Debian** OS and the **10 (buster)** version are selected.
- Under the **Management, security, disks, networking, sole tenancy** tab, set the below changes.
  - Click on **Networking** and add the **Network tags:** allow-ssh and allow -health-check
  - Under **Network interfaces** click **edit,** change the following.
    - **Network:** lb-network
    - **Subnet:** lb-subnet
    - **Primary Internal IP:** Ephermal
    - **External IP:** Ephermal
  - Click **Done**

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Under **Management** tab in **Startup Script** field enter the below values

```
#! /bin/bash
if [ -f /etc/startup_script_completed ]; then
exit 0
fi
apt-get update
apt-get install apache2 -y
a2ensite default-ssl
a2enmod ssl
file_ports="/etc/apache2/ports.conf"
file_http_site="/etc/apache2/sites-available/000-default.conf"
file_https_site="/etc/apache2/sites-available/default-ssl.conf"
http_listen_prts="Listen 80\nListen 8008\nListen 8080\nListen 8088"
http_vh_prts="*:80 *:8008 *:8080 *:8088"
https_listen_prts="Listen 443\nListen 8443"
https_vh_prts="*:443 *:8443"
vm_hostname="$(curl -H "Metadata-Flavor:Google" \
http://169.254.169.254/computeMetadata/v1/instance/name)"
echo "Page served from: $vm_hostname" | \
tee /var/www/html/index.html
echo "Page served from: $vm_hostname" | \
tee /var/www/html/index.html
prt_conf="$(cat "$file_ports")"
prt_conf_2="$(echo "$prt_conf" | sed "s|Listen
80|${http_listen_prts}|")"
prt_conf="$(echo "$prt_conf_2" | sed "s|Listen
443|${https_listen_prts}|")"
echo "$prt_conf" | tee "$file_ports"
http_site_conf="$(cat "$file_http_site")"
http_site_conf_2="$(echo "$http_site_conf" | sed
"s|*:80|${http_vh_prts}|")"
echo "$http_site_conf_2" | tee "$file_http_site"
https_site_conf="$(cat "$file_https_site")"
https_site_conf_2="$(echo "$https_site_conf" | sed
"s|_default_:443|${https_vh_prts}|")"
echo "$https_site_conf_2" | tee "$file_https_site"
```

hidel.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
systemctl restart apache2
touch /etc/startup_script_completed
```

- Click **Create.**

Create Instance Groups

- Navigate to **Instance Groups** page in console.

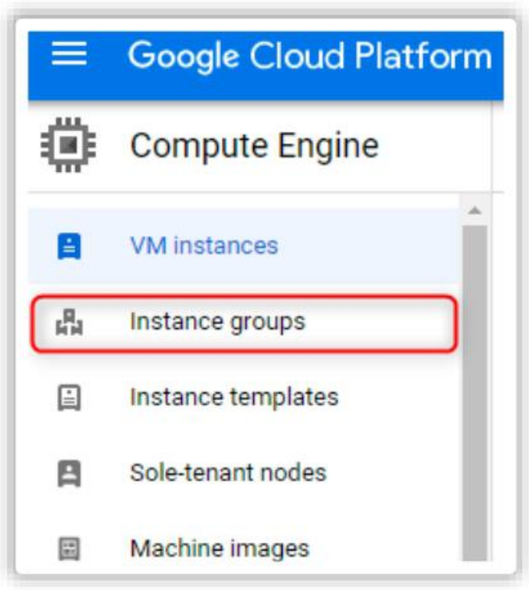


FIGURE 3.201: Instance Group

- The two unmanaged instance groups can be created by using the below combinations.
  - **Instance group**: ig-a, Zone:us-west1-a, VMs:vm-a1 and vm-a2
  - **Instance group**: ig-c, Zone:us-west1-c, VMs:vm-c1 and vm-c2
- Click **Create Instance Group.**
- **Click New Unmanaged Instance Group.**
- Give the **Name** as mentioned in the above step.
- For **location,** select us-west1 as the **Region**, **Zone** mentioned in the above step.
- **In Network,** type lb-network.
- **In Subnetwork,** type lb-subnet.
- For **VM Instances,** the VMs can be added as indicated in the above step.
- Click **Create.**

Step 4: Create a client VM.

- Navigate to the **VM Instances** page in GCP console.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

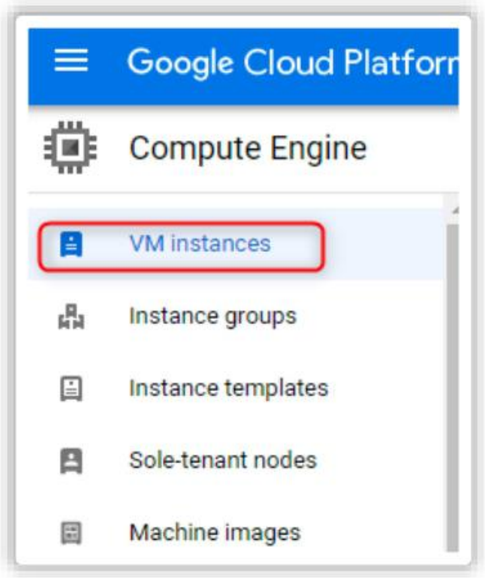


FIGURE 3.202: VM Instances

- Select **Create Instance.**
- Type the **Name** as 'vm-client'.
- Name the **Zone** as 'us-west1-a'.
- Under **Management, security, disks, networking, sole tenancy** tab
  - Click on **Networking,** for **Network tags** add allow-ssh.
  - Under **Network Interfaces** Click on the edit button and change the following:
    - **Network:** lb-network
    - **Subnet:** lb-subnet
    - **Primary Internal IP:** Ephermal
    - **External IP:** Ephermal
  - Click **Done.**
- Click **Create.**

Step 5: Configuration of load balancer.

- In console, navigate to the **Load Balancing** page.

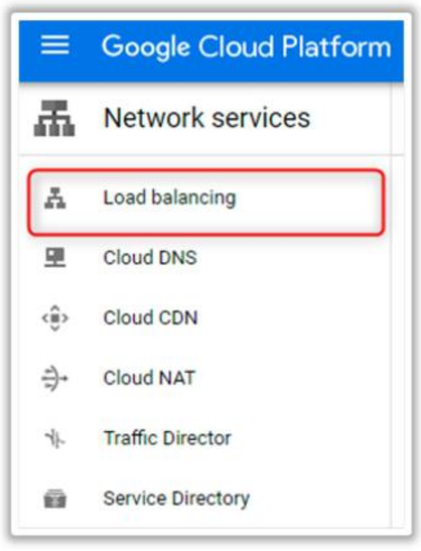


FIGURE 3.203:Load Balancing

- Click **Create Load Balancer.**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click **Start Configuration** under **TCP Load Balancing.**
- For **Internet Facing or Internal Only,** choose **Only between my VMs.**
- Click **Continue.**
- Type the name as be-ilb.
- Click **Backend configuration** and change the following.
  - **Region:** us-west1
  - **Network:** lb-network
  - For **Backends** under **New Item,** select on **ig-a** instance group.
  - Click **Done.**
  - Click **Add backend.** Select the **ig-c** instance group under **New Item**.
  - Click **Done.**
  - For **Health Check,** select **Create another health check** and change the following.
    - For **Name,** select hc-http-80.
    - For **Protocol,** select HTTP.
    - Choose **Port** as 80.
    - For **Proxy Protocol,** select None.
    - For **Request Path,** select /.
    - Click on **Save and Continue.**
- Identify a blue check mark near to **Backend Configuration.**
- Click on **Frontend Configuration,** under **New Frontend IP and Port,** change the following:
  - **Name:** fr-ilb
  - **Subnetwork:** lb-subnet
  - Select **Reserve a static internal IP address** under **Internal IP** and give the following information.
    - **Name:** ip-ilb
    - **Static IP address: Let me choose**
    - **Custom IP address:** 10.1.2.99
    - Click **Reserve.**
  - Ports**:** Select **Multiple** and for the **Port Number** enter 80,8008,8080,8088
  - Check for a blue check mark near to **Frontend Configuration.**
- Click on **Review and Finalize.**

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click **Create.**

SSL Proxy Load Balancing

SSL proxy load balancers are implemented on GFE to distribute the SSL traffic to VM instances in the GCP VPC network. They are reverse proxy load balancers. The SSL proxy load balancers can be used for SSL traffic where the SSL connections will get terminated at the load balancing layer and will get proxied to the nearest back end. The SSL proxy load balancers can be configured as regional load balancer and as global load balancer. SSL proxy balancing is for non-HTTPS traffic. SSL proxy load balancer has the following features:

- **IPv6 termination:** SSL proxy load balancers support IPv6 termination where the user requests are terminated at load balancing layer and routed as IPv4.
- **Intelligent routing:** The smarter routing of SSL proxy load balancer can route the requests to the backends with capacity.
- **Better utilization of backends:** As SSL processing is an intensive task the ciphers used should be CPU efficient. ECDSA SSL certificates and TLS 1.2 can be used for better CPU performance. For SSL connection between the load balancer and backends, ECDHE-ECDSA-AES128-GCM-SHA256 cipher suites can be used.
- **Certificate management:** Google managed SSL certificates, which support multiple domains, can be used for load balancer and self-signed certificates can be used on VMs.
- **Security patching:** Automatic patches can be applied to the load balancer if vulnerabilities occur.
- **Support well-known ports:** It supports the ports 25, 43, 110, 143, 195, 443, 465, 587, 700, 993, 995, 1883, 3389, 5222, 5432, 5671, 5672, 5900, 5901, 6379, 8085, 8099, 9092, 9200, and 9300.
- **SSL policies:** The features of SSL can be controlled by the SSL Policies.
- **Geographic control:** To minimize the latency between users and load balancer, the ssl proxy load balancer terminates TLS in global locations.

hide01.ir

Architecture of SSL Proxy Load Balancer

- **Forwarding rules and IP address:** The traffic can be routed by an IP address, port, and protocol to a load balancing configuration with a target proxy and backend service by using forwarding rules. As the forwarding rules provides a single IP address DNS-based load balancing is not required.
- **Target proxies:** The terminated SSL connections from user are routed to the backend service using target proxy.
- **SSL certificates:** For a secure communication between GFE and user, SSL certificates must be installed on target SSL proxy.
- **Backend services:** The backend services conduct health check to route the incoming traffic to one or more backends.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Firewall rules:** For the traffic to reach the endpoints the firewall rule must be configured to allow traffic from load balancer GFE/health check ranges.
- **Source IP addresses:** The source IP address is in the range of 35.191.0.0/16 and 130.211.0.0/22 as seen by backends.
- **Open ports:** SSL proxy load balancers are reverse proxy load balancers that have multiple open ports to support other services. The port scan on the external IP address of load balancer shows additional ports, which does not affect SSL proxy load balancers. The external forwarding rules will only reference specific TCP ports.

Steps to Setup SSL Proxy Load Balancer

Source: https://cloud.google.com

The setting up procedure for a global SSL proxy load balancer that exists in two regions is as follows:

Step 1: Configuration of instances.

Creating Instances

- Navigate to the **VM Instances page** in GCP.



FIGURE 3.204: VM Instances

- Click **Create Instance.**
- Enter the **Name** as 'ig-us-central1-1'.
- Choose the **Zone** as 'us-central1-b'**.**
- Click **Management, security, disks, networking, sole tenancy.**
- In **Management** section, fill **Tags** field ssl-lb.
- The **Startup script** can be set to

```
sudo apt-get install apache2 -y
sudo a2ensite default-ssl
sudo a2enmod ssl
sudo service apache2 restart
```


Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
echo '<!doctype html><html><body><h1>ig-us-central1-
1</h1></body></html>' | sudo tee /var/www/html/index.html
```

- Keep the other default values as such and click **Create.**
- ig-us-central1-2 can be created with the above steps with the below **startup script:**

```
sudo apt-get update
sudo apt-get install apache2 -y
sudo a2ensite default-ssl
sudo a2enmod ssl
sudo service apache2 restart
echo '<!doctype html><html><body><h1>ig-us-central1-
2</h1></body></html>' | sudo tee /var/www/html/index.html
```

- ig-us-east1-1 can be created with the above steps with the **Zone** as us-east1-b and startup script as

```
sudo apt-get update
sudo apt-get install apache2 -y
sudo a2ensite default-ssl
sudo a2enmod ssl
sudo service apache2 restart
echo '<!doctype html><html><body><h1>ig-us-east1-
1</h1></body></html>' | sudo tee /var/www/html/index.html
```

- ig-us-east1-2 can be created with the above steps with **Zone** as us-east1-b and the **startup script** as

```
sudo apt-get update
sudo apt-get install apache2 -y
sudo a2ensite default-ssl
sudo a2enmod ssl
sudo service apache2 restart
echo '<!doctype html><html><body><h1>ig-us-east1-
2</h1></body></html>' | sudo tee /var/www/html/index.html
```

Step 2: Creating instance groups.

- In the console, navigate to the **Instance Groups page**.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

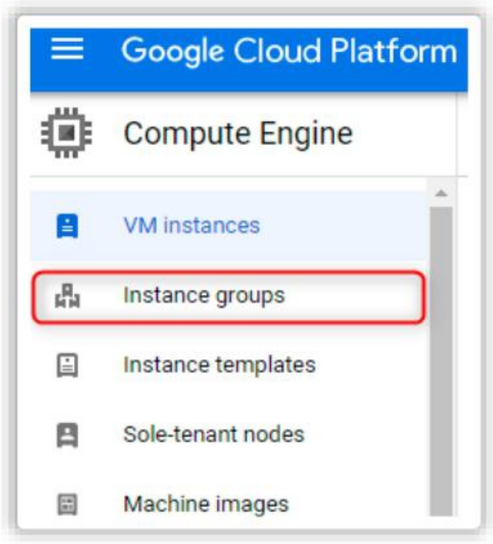


FIGURE 3.205:Instances Group

- Click **Create Instance Group.**
- Enter the **Name** as 'us-ig1'.
- Set the **Zone** as 'us-central1-b'
- Click on **Specify port name mapping.**
  - Click on **Add Item** under **Port Name Mapping.**
  - Type the **Port name** ssl-lb and **Port Numbers** 443.
- Click **Select Existing Instances** under **Instance Definition.**
- For **VM Instances** select ig-us-central1-1 and ig-us-central1-2
- Keep the other settings as such and click on **Create.**
- The above steps can be repeated with the following parameters.
  - **Name:** us-ig2
  - **Zone:** us-east1-b
  - **Port name:** ssl-lb and **Port Numbers:** 443
  - **Instances:** ig-us-east1-1 and ig-us-east1-2.

Step 3: Configuration of load balancer.

- From the GCP console, navigate to the **Load Balancing Page**.

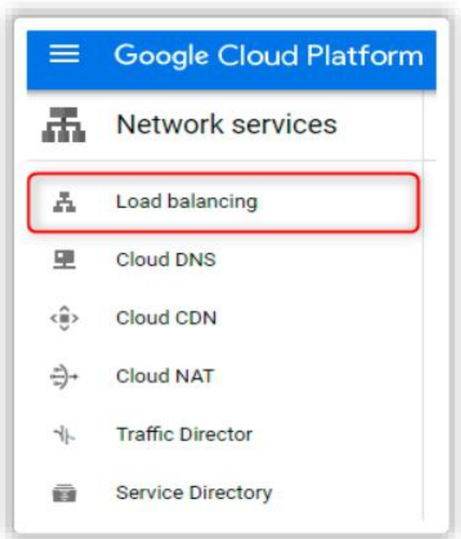


FIGURE 3.206: Load Balancing

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click **Create Load Balancer.**
- Click **Start Configuration** under **TCP Load Balancing.**
- Choose **From Internet to my VMs** under **Internet Facing or internal only.**
- For **Multiple Regions or Single Region,** choose **Multiple regions.**
- Give the **Name** of the load balancer as 'my-ssl-lb'.
- Click on **Backend Configuration.**
- Set the **Protocol** as **TCP.**
- Type ssl-lb for **Named Port.**
- For **Timeout** keep the default value.
- Set the **Backend type** to **Instance Groups.**
- Select **Instance Group** us-ig1 under **New backend.**
- Give the **Port numbers** as 443.
- Keep the other settings as such.
- For **New Backend,** choose **Instance Group** us-ig2.
- The **Port number** as 443.
- Keep the other settings as such and click **Done.**
- For **Health Check,** choose **Create Health Check**
  - Give the health check **Name** as 'my-ssl-health-check'.
  - The **Protocol** should be set as SSL.
  - Keep the other settings as such and Click **Save and Continue.**
- Check for a green mark near to **Backend Configuration.**

Step 4: Configuration of frontend services.

- Click on **Frontend Configuration.**
- For **New frontend IP and Port,** type the name my-ssl-lb-forwarding-rule.
- The **Protocol** should be set as SSL.
- For **IP Address,** click on **Create IP Address**
  - **Name:** ssl-lb-static-ip
  - Click on **Reserve.**
- For **Certificate,** choose **Create a New Certificate.**
- Type the **Name** of my-ssl-cert.
- If **Upload My Certificate** is selected

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In the fields, upload
  - **Public Key Certificate** (.crt file)
  - **Certificate Chain** (.csr file)
  - **Private Key** (.key file)
- To add other SSL certificates, click on **Add Certificate,** choose from the dropdown or click **Create a New Certificate** and repeat the above steps.
- If necessary, turn on Proxy Protocol and click **Create.**

- A **Domain** should be entered if **Create Google Managed Certificate** is selected
- Click **Done.**
- Click on **Add Frontend IP and Port**
- Give the **Name** of my-ssl-lb-ipv6-forwarding-rule.
- The **IP Version** can be selected as IPv6.
- For **IP Address,** click on **Create IP address**
  - Give the **Name** of ssl-lb-static-ipv6.
  - Click **reserve.**
- For **Certificate,** select **my-ssl-cert**.
- Click **Done.**
- To add certificate resources
  - Choose a certificate from the **Certificates** list or click on **Create a New certificate** and the above steps can be repeated.
- Click **Done.**
- To create an SSL policy
  - Click on **Create policy** under **SSL Policy.**
  - Give the **Name** of my-ssl-policy.
  - Choose **TLS 1.0** for **Minimum TLS Version.**
  - Choose **Modern** for **Profile** which displays the **Enabled features** and **Disabled Features.**
  - Click **Create.**
- Check for a green mark next to **Frontend Configuration.**
- Click on **Review and Finalize**
- Click **Create.**

hide01.ir

Step 5: Creating a firewall rule.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Navigate to the **Firewall Page** in the console.

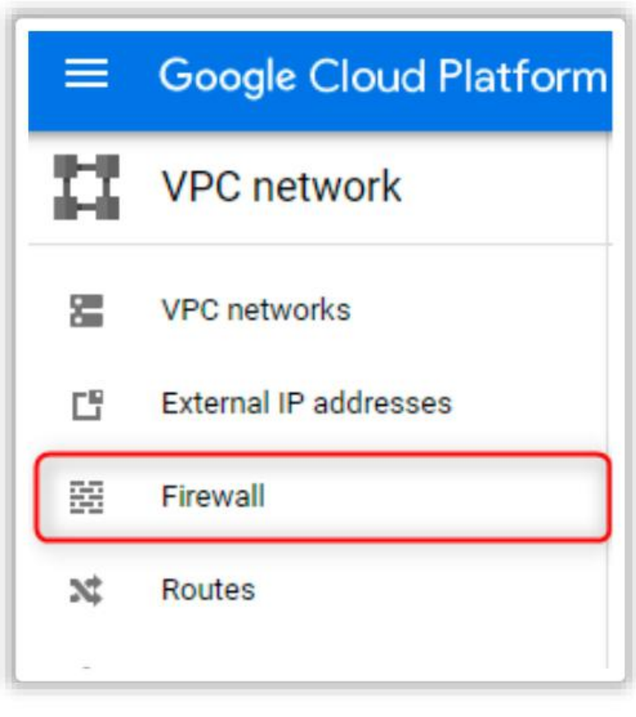
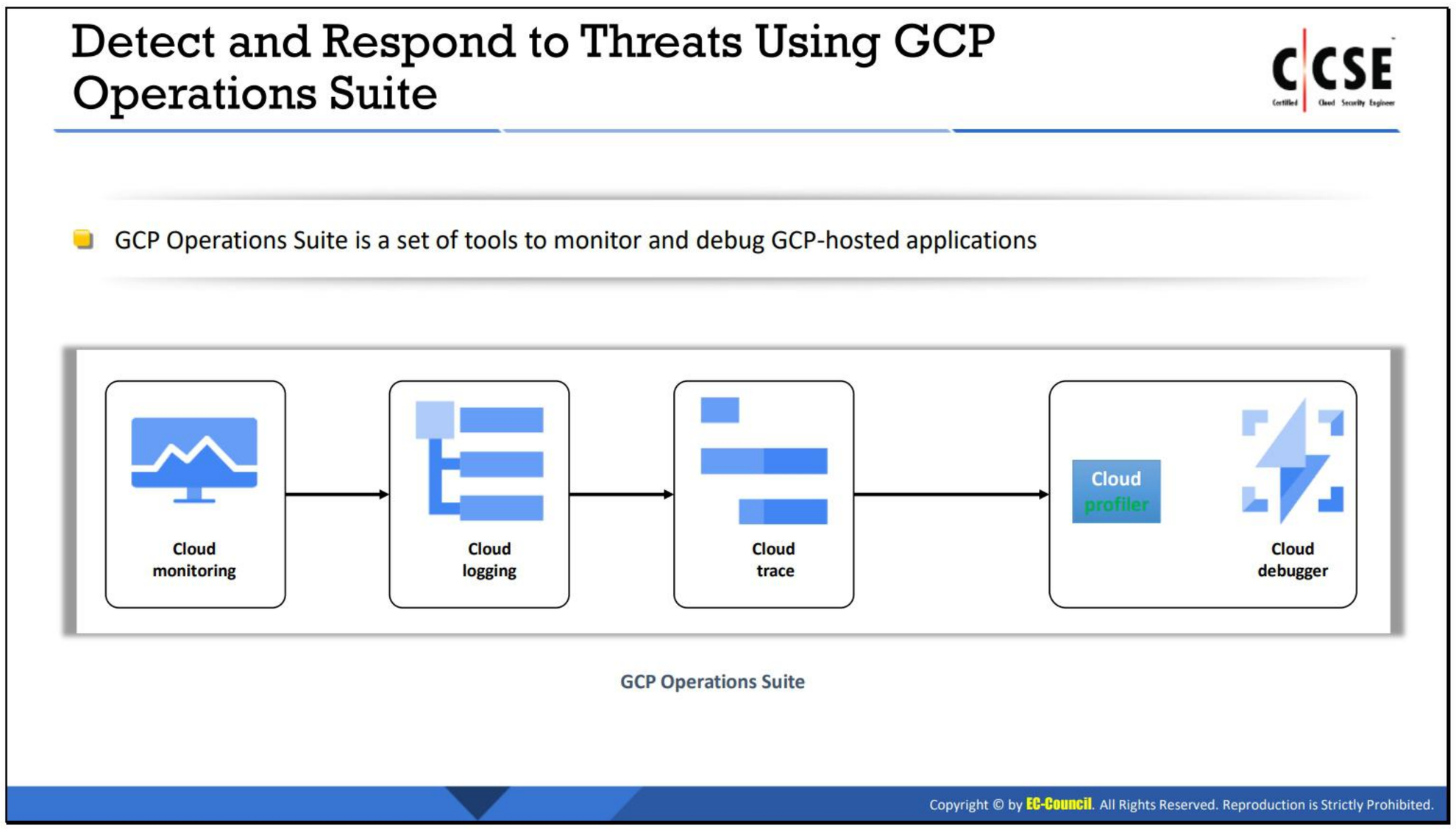


FIGURE 3.207: Firewall

- Click on **Create Firewall Rule.**
- Give the **Name** of allow-ssl-lb-and-health.
- Choose default under **Network.**
- Choose **Specified Target Tags,** under **Targets.**
- The **Target Tags** can be set to **ssl-lb**
- The **Source Filter** can be set to IP ranges.
- The **Source IP ranges** can be set to 130.211.0.0/22 and 35.191.0.0/16.
- The **Allowed Protocols and Ports** can be set to tcp:443.
- Click **Create.**

hid001.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Detect and Respond to Threats Using GCP Operations Suite

With all the security implementations, the application still needs to be protected and monitored properly to avoid an attack or deviation from the best practices. GCP Cloud Operations Suite (formerly Stack Driver) is a logging and monitoring tool that provides insights regarding the system with the help of dashboards, charts, and alerts. It is a set of tools that help monitor and debug GCP-hosted applications. The various features are described below.

- **Log management:** The Logs Router feature in GCP logs all the audit logs, platform logs, and user logs, which are sent to the Cloud Logging API and then they are passed through the Logs Router. Based on the existing rules, Logs Router will check the logs and decide whether to discard, ingest or route to other destinations.
- **Log insights:** A centralized error management service that can identify application errors and reports them instantly. It will display error details such as occurrences and affected users.
- **Proactive monitoring:** The policies for alerts can be created by using Cloud Monitoring to check the metrics, health checks, and uptime. Alerting policies have conditions that are continuously monitored to check whether the resources require any action. It has notification channels such as email, cloud mobile app, PagerDuty, SMS, slack, webhooks.
- **Service monitoring:** Service monitoring and service level objectives (SLO) API can measure the performance, provide a statement of desired performance and a measurement of the difference between the real and actual performance.
- **Latency management:** The Cloud Trace service available with GCP Operations Suite gives the latency sampling and reporting for App Engine.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Debugging:** Without stopping the end-user experience, the Cloud Debugger service included with GCP Operations Suite connects the application production data with source code by analyzing the application state at any code location.
- **Performance Management:** The performance issues with applications can be detected and mitigated by the Cloud Profiler service, which actively provides the consumption of resources in the applications.

All these features of GCP Operations Suite are provided by the following services:

- Cloud Monitoring
- Cloud Logging
- Cloud Trace
- Cloud Debugger
- Cloud Profiler

The application performance can be improved and the mean time to discover (MTTR) can be reduced by using the full services available with the Cloud Operation Suite. The dashboard provides metrics and alerts, which provide an insight into the application. The following functionalities are provided by the services available within Operations Suite to protect the application.

- **Cloud Monitoring:** Cloud Monitoring collects the performance metrics, analyzes the trends, and sets alert thresholds.
- **Cloud Logging:** It generates outlier signals; logs will be analyzed to troubleshoot the applications.
- **Cloud Trace:** The latency distribution across the microservices is analyzed.
- **Cloud Profiler and Cloud Debugger:** The application performance can be improved, and debugging can be performed during production.

hide01.ir

Cloud Monitoring

Cloud Monitoring helps in monitoring the performance, availability, and health of the application by collecting the metrics, events, and metadata from the application infrastructure in real-time. The SLO for applications can be defined in custom or automatically and the alerts will be generated when violations occur. The Cloud Monitoring agent, an open-source agent on GCP hosts collects the metrics from VM instances can be deployed to monitor all the applications. The targeted dashboards and alerting policies can be created based on resource names, projects, regions etc. The applications uptime can be monitored with Cloud Monitoring. The metrics data of the Compute Engine instances can be collected by creating an agent policy that automatically maintains the GCP Operations Suite services.

Monitoring a Compute Engine Instance with Cloud Monitoring

Source: https://cloud.google.com

Follow these steps to monitor a CE instance via Cloud Monitoring:

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 1: Create a Compute Engine instance.

- In GCP Console navigate to the **Compute Engine.**
- Click on **create.**
- Fill the fields with the given parameters.
  - **Name:** lamp-1-vm
  - **Machine type,** select small
  - The **Boot disk** is to be configured as **Debian GNU/Linux.**
  - The **Firewall** should be selected as **Allow HTTP Traffic** and **Allow HTTPS Traffic.**
  - Keep the other values as such.
- Click **Create.**
- To open the terminal, click on **SSH** in the **Connect** column.
- To update the package list, run

```
sudo apt-get update
```

- The Apache2 HTTP server can be set up by

```
sudo apt-get install apache2 php7.0
```

- Connect to the Apache2 HTTP server by the URL http:// [External IP]. The [External IP]can be replaced with the external IP of the Compute Engine instance. The Apache2 default page opens.

hide01.ir

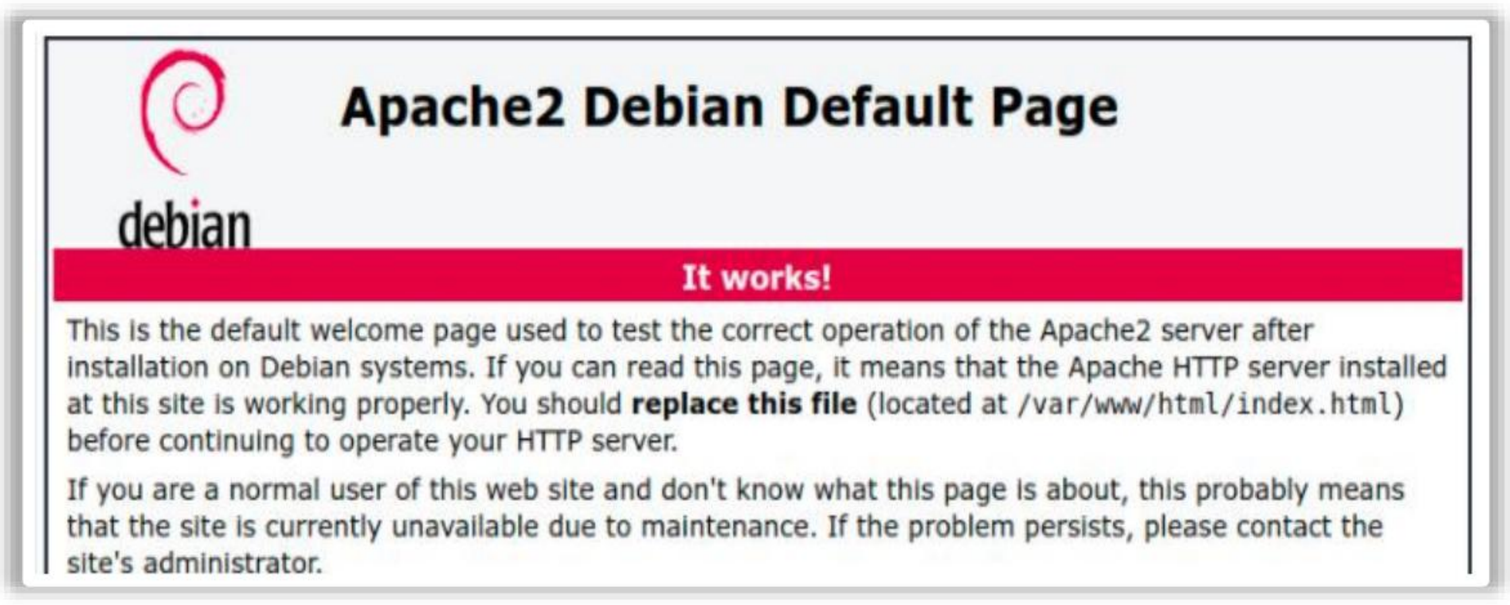


FIGURE 3.208: Apache2 Debian

Step 2: Install the agents.

- Open the terminal connected to the VM instance or create new one.
- The Cloud Monitoring agent can be installed and started.
  - To add the package repository and update the package list, the following script can be used:

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
curl -sSO https://dl.google.com/cloudagents/add-monitoring-
agent-repo.sh
sudo bash add-monitoring-agent-repo.sh
sudo apt-get update
```

- Install the agent

```
sudo apt-get install stackdriver-agent
```

- Start the agent

```
sudo service stackdriver-agent start
```

- Install, start, and configure the Cloud Logging agent
  - The package list can be updated by the given script

```
curl -sSO https://dl.google.com/cloudagents/add-logging-agent-
repo.sh
sudo bash add-logging-agent-repo.sh
sudo apt-get update
```

  - Install the cloud agent by using

```
sudo apt-get install google-fluentd
```

  - Install the default agent configuration for ingesting data by running

```
sudo apt-get install google-fluentd-catch-all-config-
structured
```

  - Start the agent

```
sudo service google-fluentd start
```

hide01.ir

Step 3: Create an uptime check and alerting policy

- Navigate to **Monitoring** in cloud console.
- Click on **Uptime checks.**
- Click on **Create Uptime Check.**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

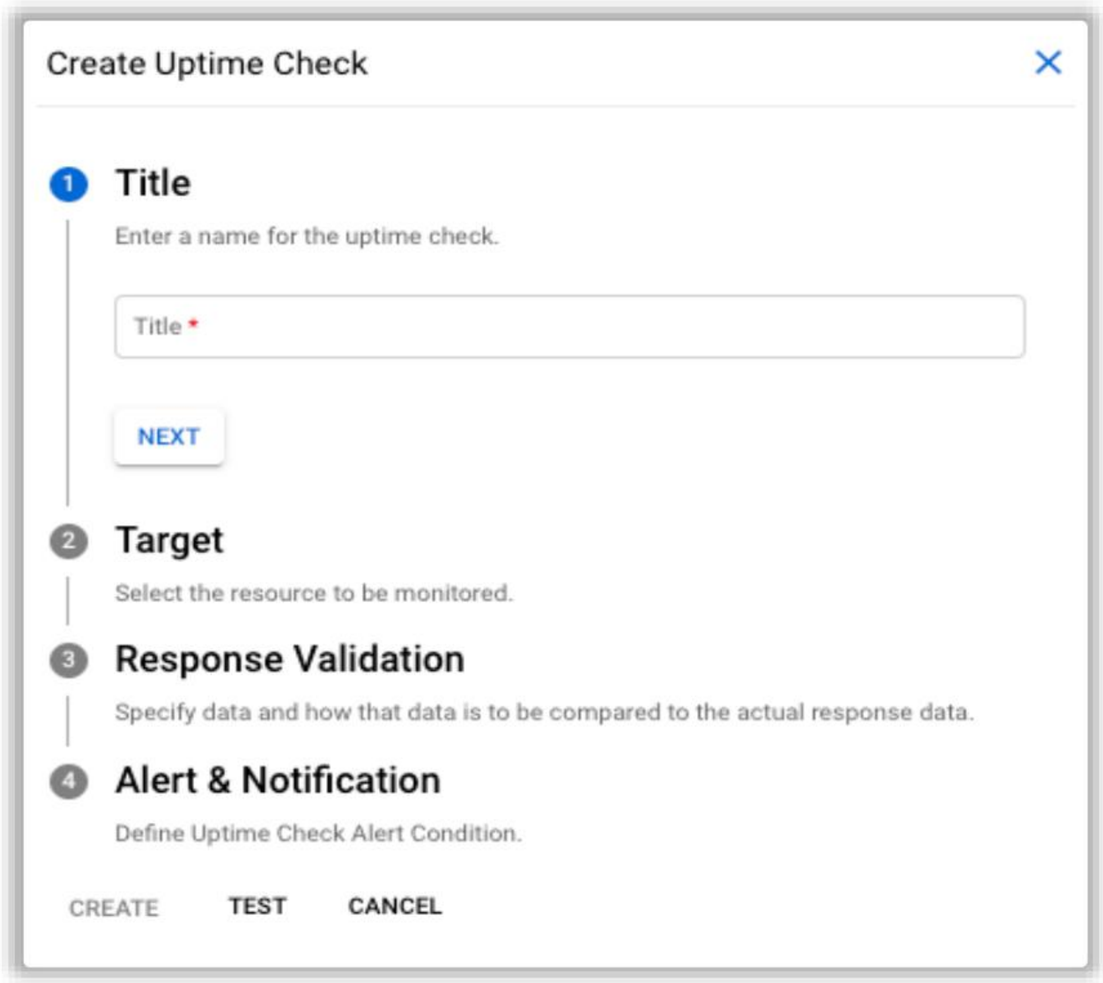


FIGURE 3.209: Create Uptime Check

- Enter 'My Uptime Check' as the **title** and click **Next.**
- **Target:**
  - Protocol: **HTTP**
  - **Resource Type: Instance**
  - **Applies To: Single** and select 'lamp-1-vm' as the instance name.
  - Keep the default values as such and click **Next.**
- **Response validation:** Keep the default values as such and click **Next.**
- **Alert and Notification:**
  - The toggle's label should be such that **Alerting is enabled.**
  - Keep the default values for name and duration fields.
  - Under **Notification Channels,** click **menu,** select the channels to add for alerting policy and click **OK.**
  - Click on **Manage Notification Channels** to add an entry to the checkbox and the instructions can be followed. Click **Refresh.**
- Click on **test** to verify the uptime check.
- Click **Create.**

hide01.ir

Step 4: Creating dashboard and chart

- Navigate to **Monitoring** in console.
- Click on **Create Dashboard** in the **Dashboards Overview** page.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- It should be ensured that the **Preview** is displayed.
- A **Line Chart** can be added to the dashboard by dragging that from **Widget Library.**
- For the section **What data do you want to view?**
  - The resource type can be selected as **GCE VM Instance.**
  - Enter **CPU,** select **CPU Utilization.**

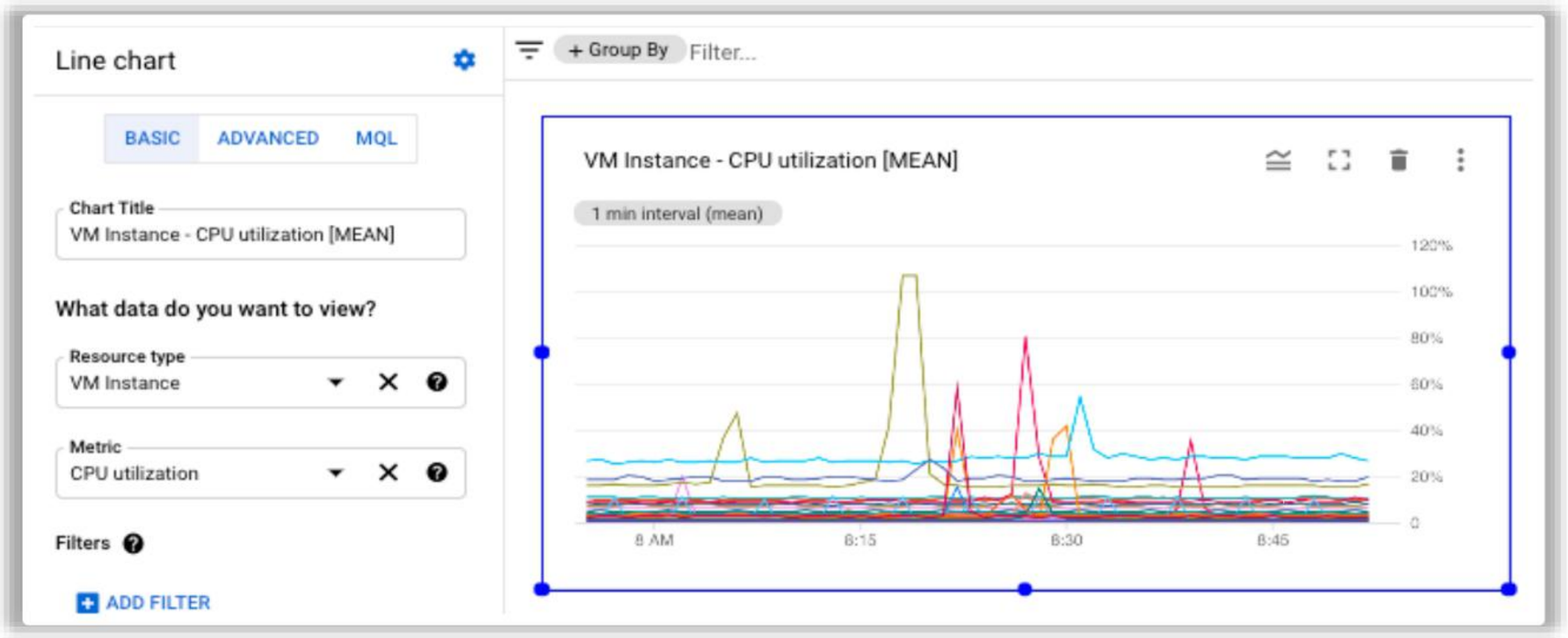


FIGURE 3.210: CPU Utilization

- To add a second **Line Chart,** click the dashboard toolbar to enable **Widget Library.** Select the plot type and drag the entry from **Widget Library.**
- Click **Save Dashboard.**

Cloud Logging

Cloud Logging is a feature available with the GCP Operations Suite that helps with real-time log management and analysis. The Logs Explorer feature with Cloud Logging helps in searching, sorting, and analyzing the logs with histograms and simple field explorers. Custom logs from any source can be written using public write APIs. Cloud Logging can be integrated with Cloud Monitoring to configure alerts on the metrics defined. With Logs Router, different retention periods for logs can be defined. Errors from the applications, which are sent to Cloud Logging, help in automatic analyzing of the errors and can be aggregated into groups. Cloud Audit Logs help in analyzing all the data access events within GCP.

Using Logs Explorer for Viewing Logs

Source*: https://cloud.google.com*

For analyzing the logs data, the Cloud Logging Interface called Logs Explorer can be used:

- Navigate to the **Google Cloud navigation** menu and select **Logging > Logs Explorer.**

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

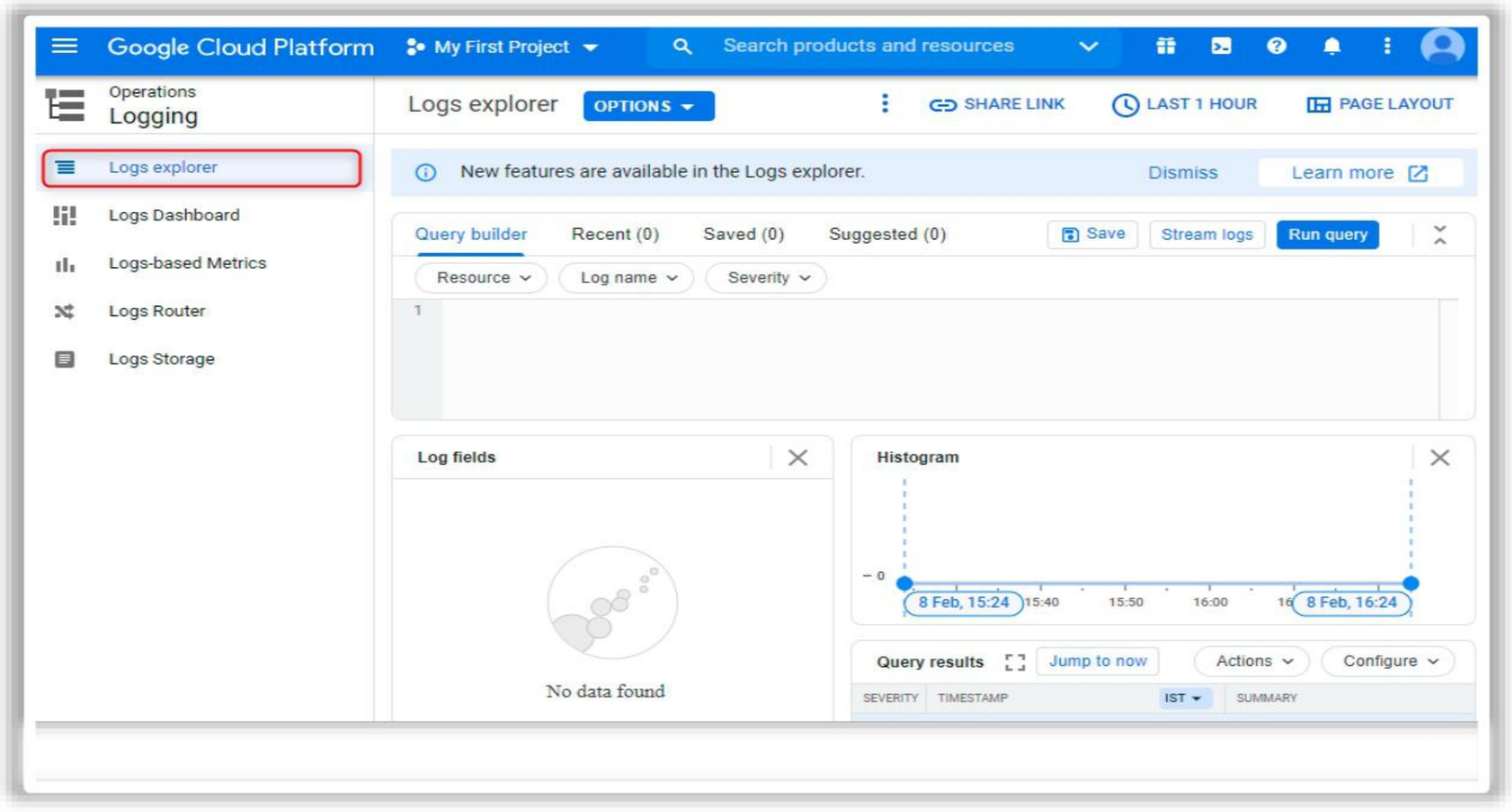


FIGURE 3.211:Select Log Explorer

- Select a Cloud Project.
- In the **Upgrade** menu, change from **Legacy Logs Viewer** to **Logs Explorer.**
- The Logs Explorer window appears.

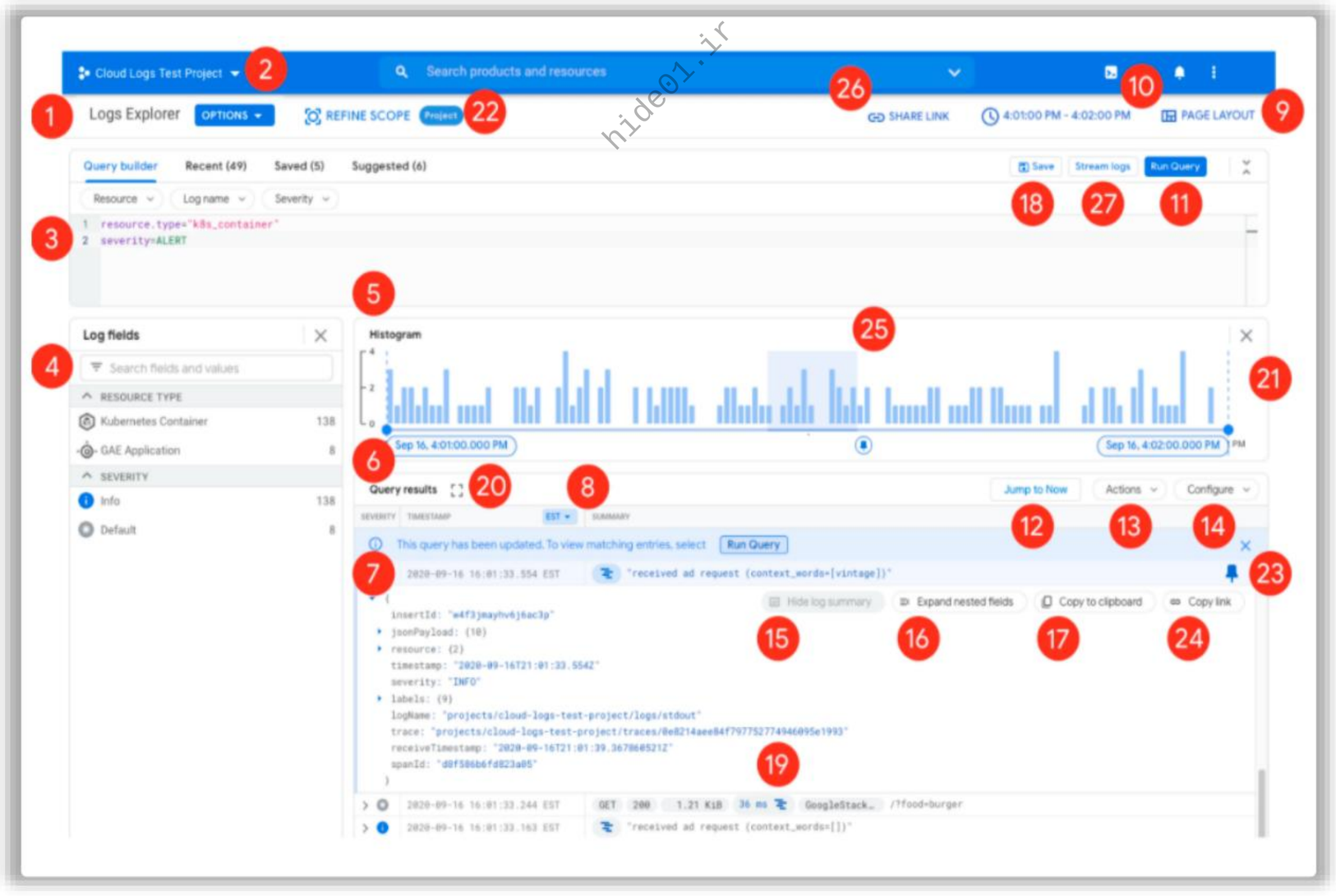


FIGURE 3.212:Log Explorer Window

- **Logs Explorer page:** To build, analyze, and refine the queries.
- **Organization and project selector:** The logs can be viewed at an organization level or project level.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Query builder:** The queries can be built from the drop down or query builder language.
- **Log fields:** Provides aggregation-based results.

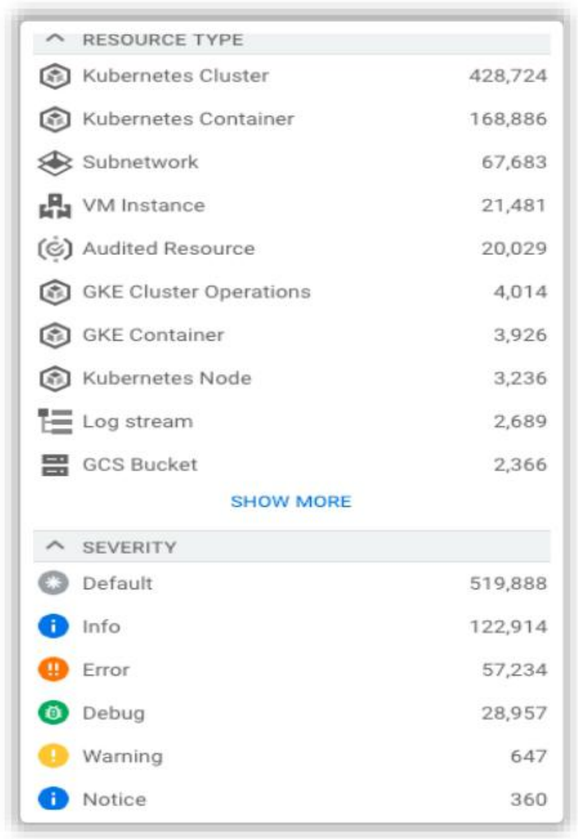


FIGURE 3.213: Log Fields

- **Histogram:** Helps analyze the frequency of the logs.

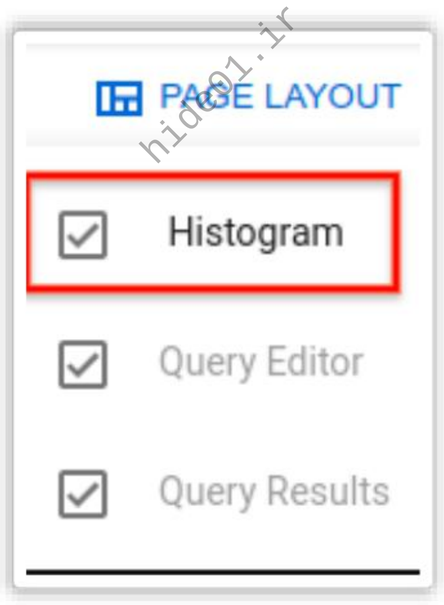


FIGURE 3.214:Histogram

- **Query results:** The logs can be viewed based on the query.
- **Log entries:** The logs can be viewed in structured JSON format.
- **Time zone:** The time zones of the displayed logs can be changed.
- **Page layout:** The **Histogram** and **Logs field explorer** panel can be enabled or disabled.
- **Time range selector:** Helps to refine the results based on the time range.
- **Run query:** The queries can be run after building them.
- **Jump to now:** Helps perform a forced refresh to include the present time.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Actions:** A log-based metric can be created, and the logs can be downloaded.

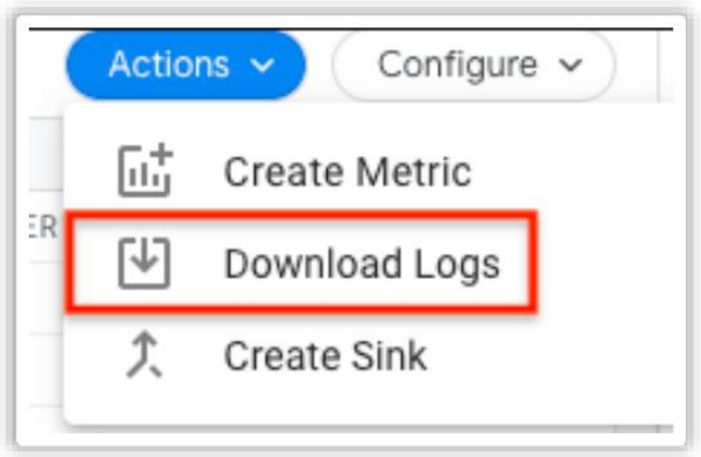


FIGURE 3.215:Download Logs

- **Configure:** Adds the value of the log field to the summary line.
- **Hide log summary:** The log summary line can be hidden from query results.
- **Expand or collapse nested log fields:** The nested fields can be collapsed or expanded.
- **Copy to clipboard:** The log entry can be copied in the JSON format.
- **Save:** Saves the queries
- **Trace data:** The trace details can be viewed, and the query can be modified.
- **Expand and collapse query results:** To expand the query results pane to view more.
- **Adjust time range:** The time range used for queries can be changed by adjusting the handles.
- **Refine scope:** The search can be limited to the logs in the current project by one or more storage views.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

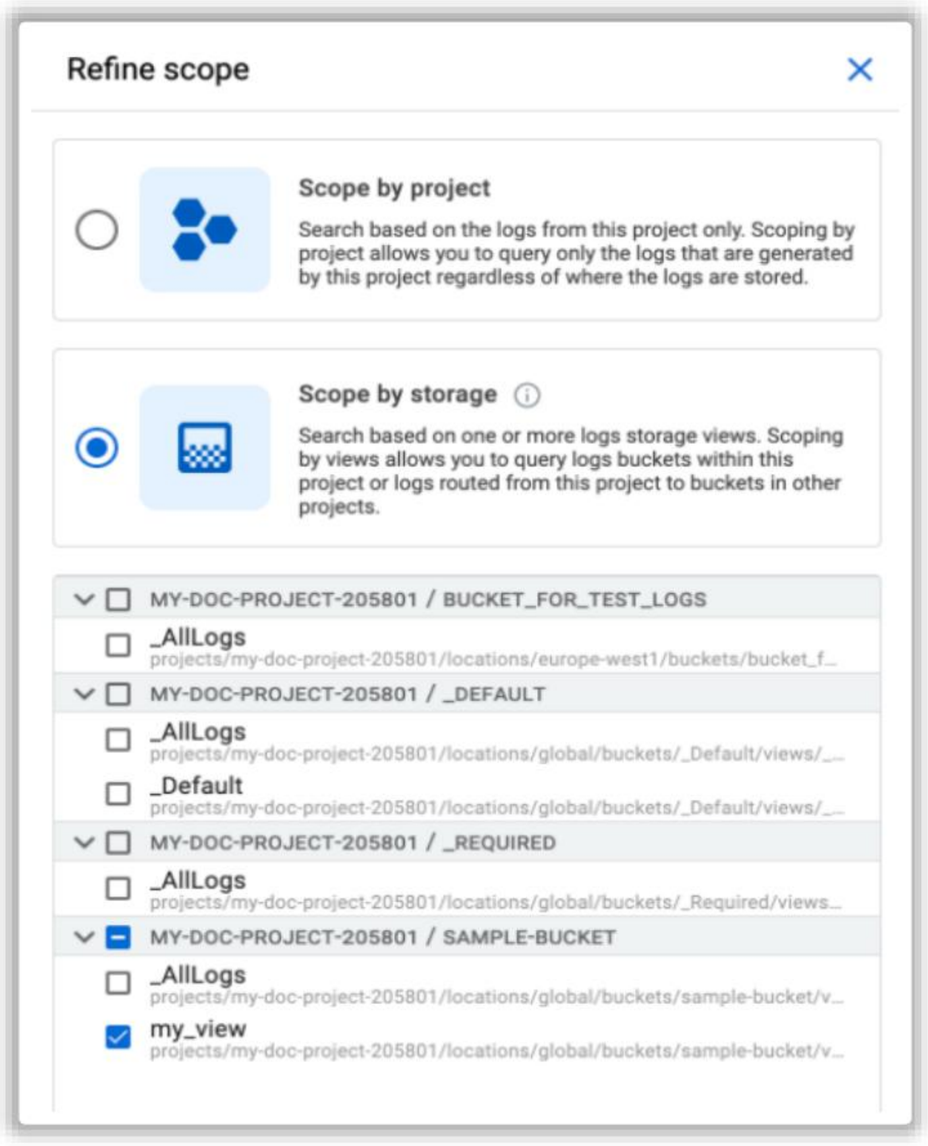


FIGURE 3.216:Refine Scope

- **Pin log entry:** The log entry can be pinned to the Query results or histogram panes.
- **Copy link to a log entry:** It allows sharing of a log entry as a link.

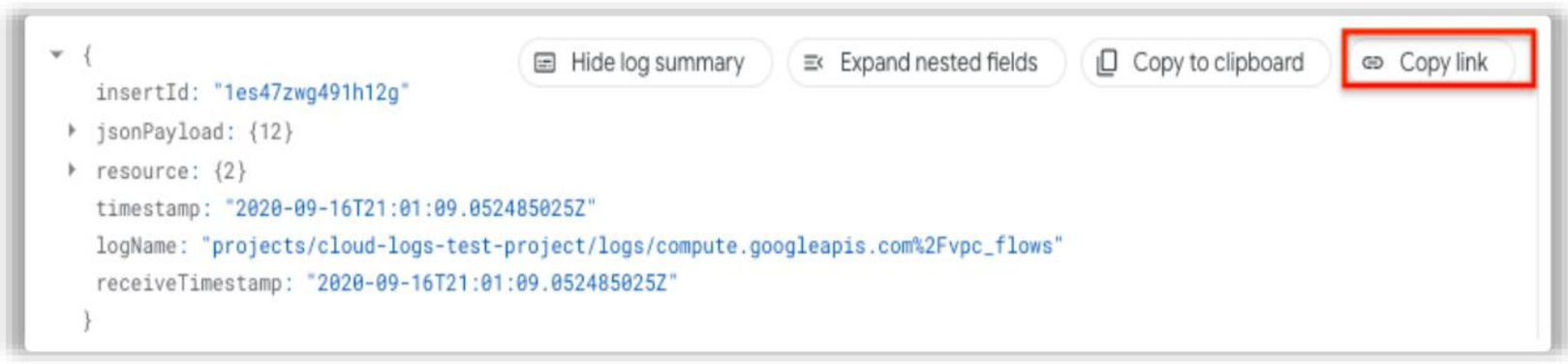


FIGURE 3.217: Copy Link to a Log Entry

- **Histogram viewport:** Helps to view the time frame of the presently displayed logs.
- **Share link:** A URL can be created for the current query.
- **Stream logs:** When logging ingests logs, the log entries can be viewed.

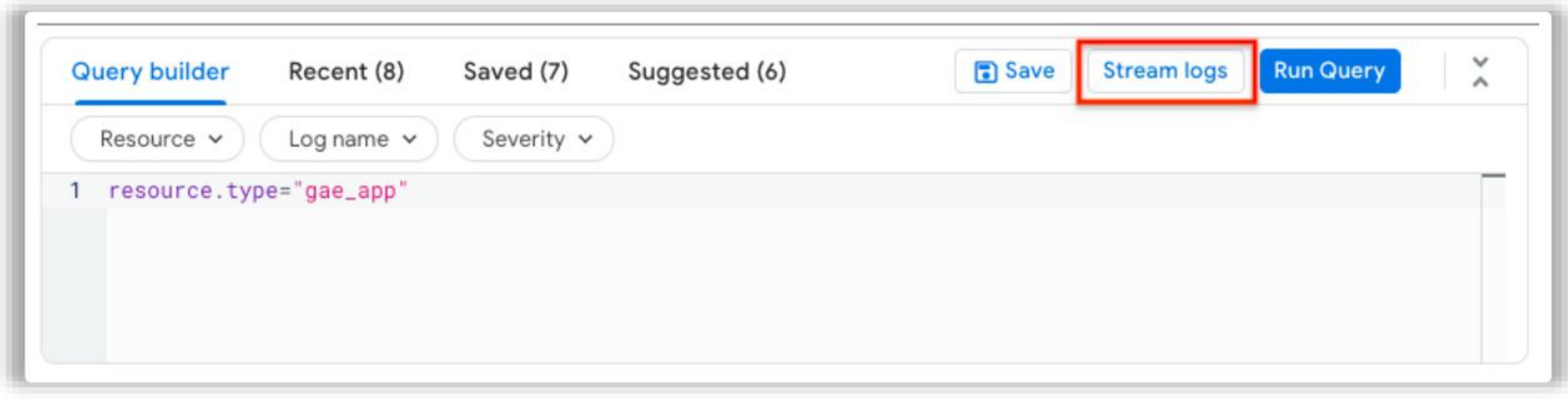


FIGURE 3.218: Stream Logs

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Trace

The latency data from the applications is collected and displayed in the console by the distributed tracing system known as Cloud Trace. With Cloud Trace, the real-time performance of the application and the performance bottlenecks can be monitored. For each traced application, automatic performance reports are created. The App Engine applications are automatically traced, and other applications running elsewhere can be traced by libraries. The latency reports are provided by the Analysis Reports feature and Cloud Trace will generate alerts for deviation in application latency. Trace API can retrieve trace data from any source.

Deploying an Application and Creating a Trace

Source: https://cloud.google.com

Follow the below steps for deploying an application in GKE cluster and the traces being captured and analyzed to view the latency information.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 1: Download and deploy the application.

- Open Cloud shell and click on **Activate Cloud Shell.**

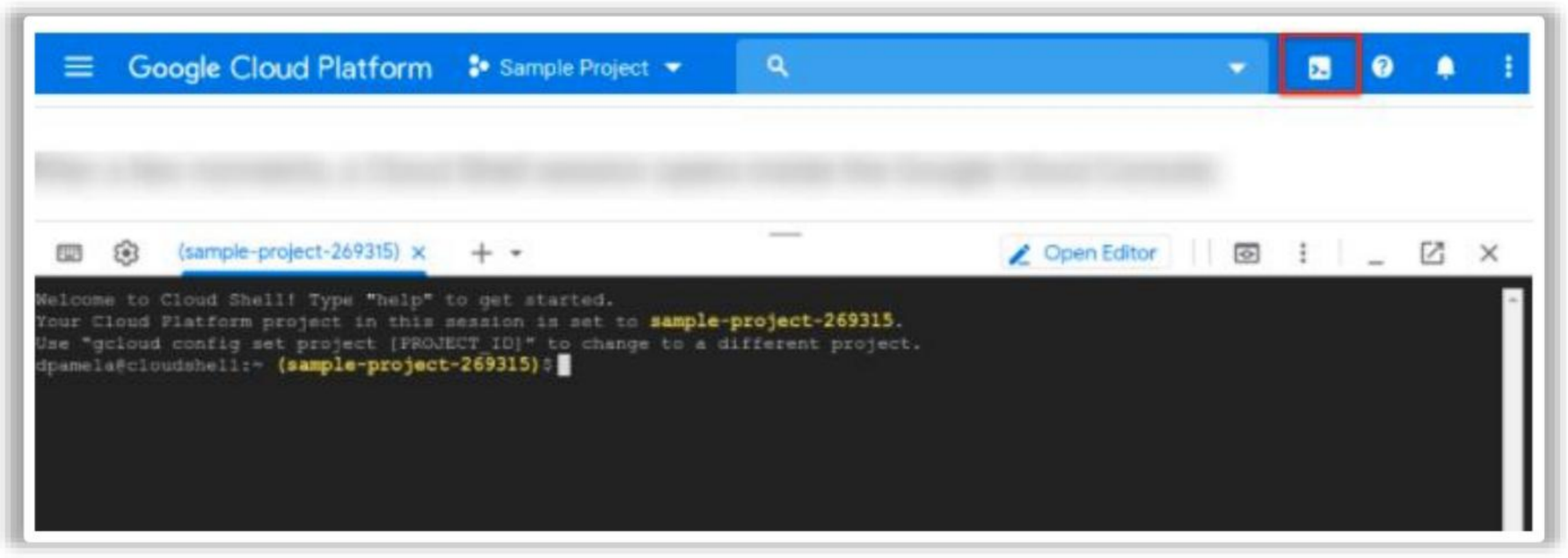


FIGURE 3.219:Active Cloud Shell

- To download the source code

  git clone https://github.com/GoogleCloudPlatform/python-docs-samples.git

- To enable the GKE API

  ```
  gcloud services enable container.googleapis.com
  ```

- To create the GKE cluster

  ```
  gcloud container clusters create demo --zone us-west1-b
  ```

hid001.ir

- To verify the creation, use

  ```
  kubectl get nodes
  ```

- The sample application can be deployed by running

  ```
  cd python-docs-samples/trace/cloud-trace-demo-app && ./setup.sh
  ```

Step 2: Create the trace.

The trace describes the time span it takes to process an incoming request and return response. Span describes the time span for a complete sub operation. For an application it describes completing a single operation. To create a trace

```
curl $(kubectl get svc cloud-trace-demo-c -
ojsonpath='{.status.loadBalancer.ingress[0].ip}')
```

Step 3: View trace data.

- Navigate to **Trace** in console.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The default view in trace is **Overview** window. The **Recent Traces** pane will show the trace details of a new project.

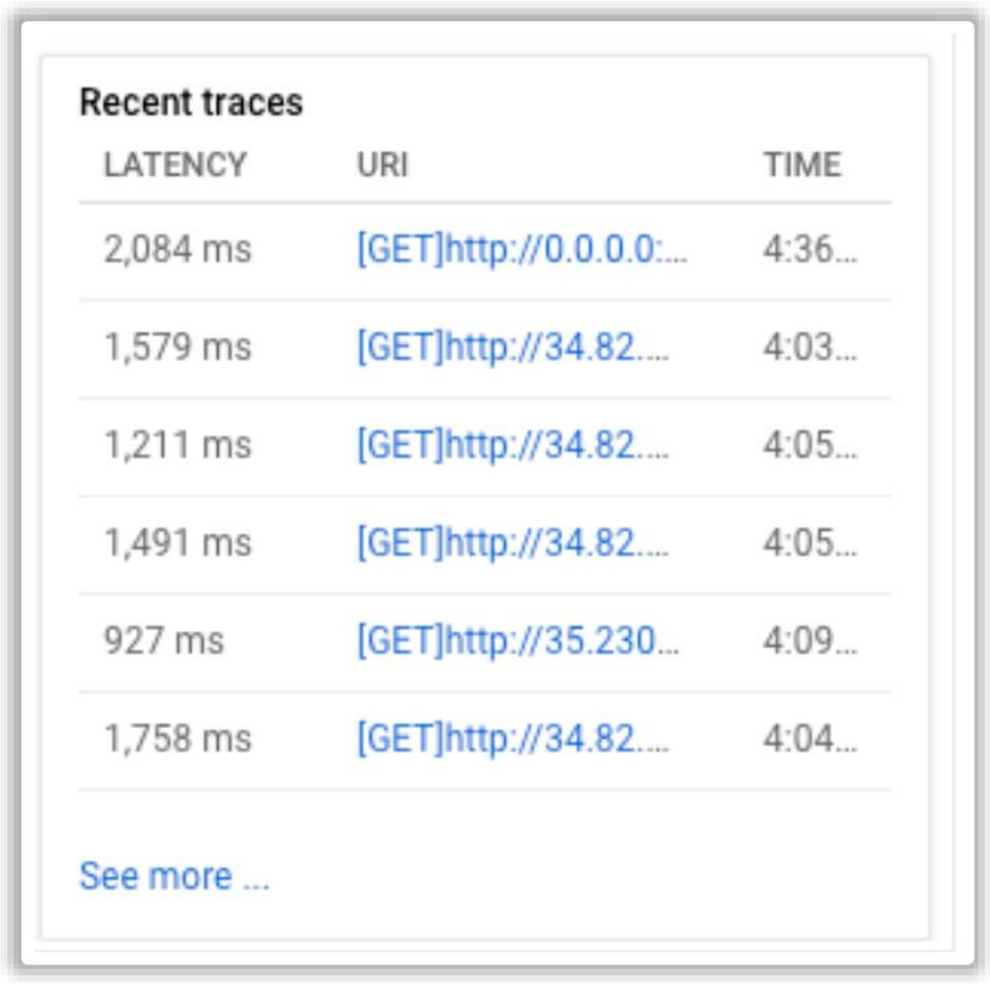


FIGURE 3.220:Recent Traces

- Click on **Trace List.**



FIGURE 3.221:Select Trace

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The graph and table are displayed on the **Trace List** window. The dot on the graph represents a trace. The trace in detail can be viewed by selecting a dot in the graph or a row in table.

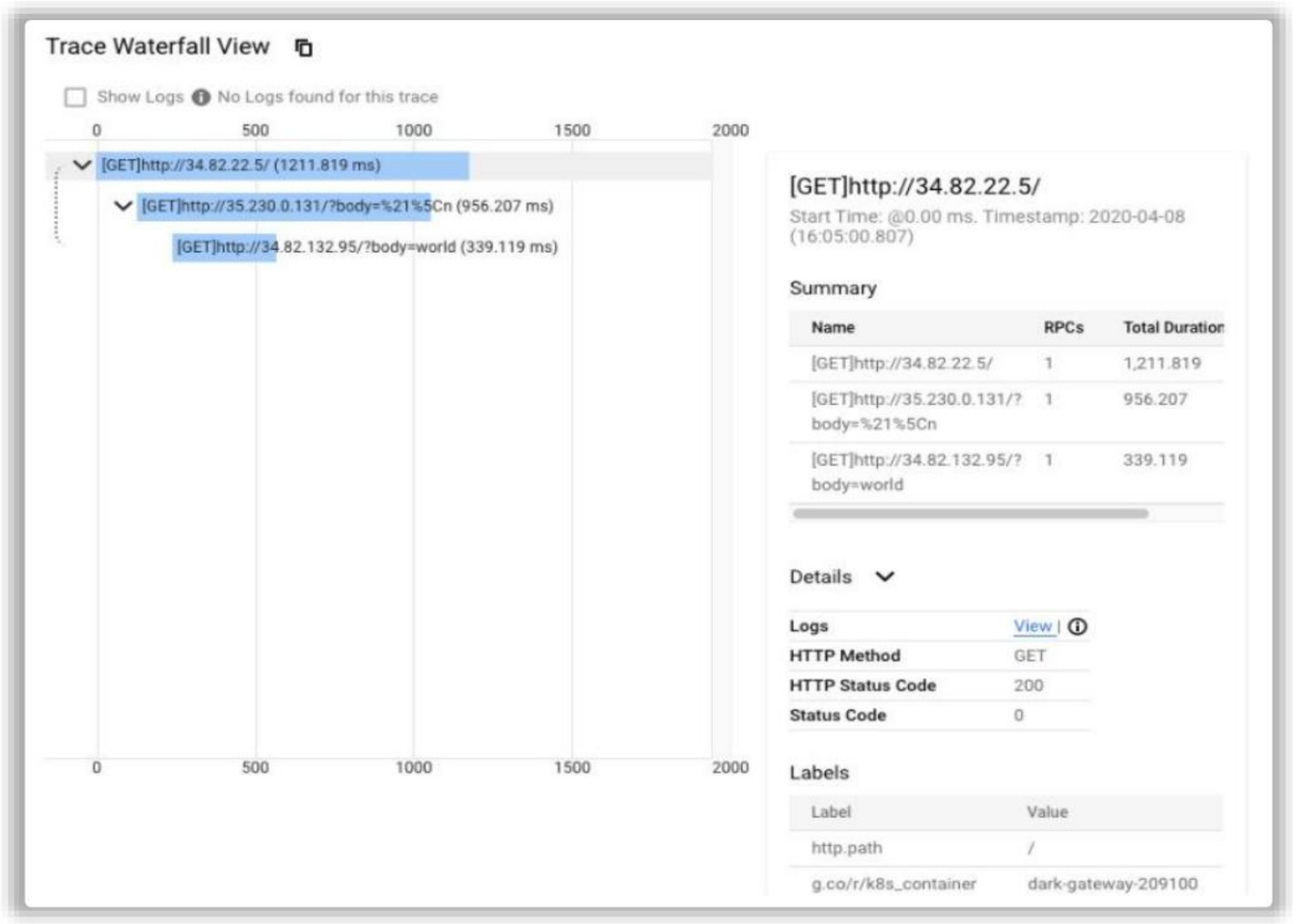


FIGURE 3.222:Trace List

In the waterfall graph, each row represents a span. The span details are displayed on the details table. The HTTP request received can be viewed from this trace.

hiboy1.ir

Cloud Debugger

The current state of a running application can be inspected in real-time using the Cloud Debugger service. The running application will not get stopped or get slowed down. The end-user experience is not compromised while the call stack and variables are captured at any location in source code with a snapshot. The highlight here with Cloud Debugger is that the debugger adds only less than 10 ms to the latency of the request while taking snapshot, which will not be noticed by users. The injected log point behaves the same as that of the deployed code. Cloud Debugger is automatically enabled for App Engine applications.

Canary Snapshots and Log Points

A canary snapshot and log point is used by the python debugger agent to protect large jobs from bugs in debugger agent when applying a snapshot or log point. To avoid this, the debugger canaries the snapshots and log points on a subset of running instances. The snapshot and log point are applied to all instances by the debugger only after it verifies that it does not affect the running instances. Canarying is disabled by default. For protecting deployment and production critical workload canarying can be enabled while debugging. Canarying should be enabled for workloads that have an execution time of less than 40 seconds and also for a faster snapshot triggering cycle.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Setting Up Cloud Debugger for Python

Source: https://cloud.google.com Step

1: Enable debugger for GKE.

- Creating cluster access
  - https://www.googleapis.com/auth/cloud-platform, grants cluster access to all GCP APIs.
  - https://www.googleapis.com/auth/cloud_debugger, grants cluster access to only debugger API.
  - To improve the security of the cluster

```
gcloud container clusters create example-cluster-name \
--scopes=https://www.googleapis.com/auth/cloud_debugger
```

- Adding Debugger package to the application
  - For the requirements.txt file, run

```
google-python-cloud-debugger
```

  - For the Docker file, run

```
pip install google-python-cloud-debugger
```

- While using Django Framework, the below lines can be used in initialization code.
  - Debugging with canarying enabled

```
try: import googleclouddebugger
  googleclouddebugger.enable(
    breakpoint_enable_canary=True
  )
  except ImportError:
  pass
```

  - With canarying not enabled

    breakpoint_enable_canary=**False**

Step 2: Enable debugger for Compute Engine.

- The Compute Engine VM instances should be running a 64-bit Debian Linux Image and Python 3.
- The Compute Engine VM Instances should be created with access **Allow Full Access to All Cloud APIs.**
- Download the debugger agent by using

```
pip install google-python-cloud-debugger
```

- The below lines can be added in the initialization code for Django Framework
  - Debugging with canarying enabled

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
try:
  import googleclouddebugger
  googleclouddebugger.enable(
    module='[MODULE]',
    version='[VERSION]'
    breakpoint_enable_canary=True
  )
except ImportError:
 pass
```

- Debugging with canarying not enabled

  breakpoint_enable_canary=**False**

Cloud Profiler

The CPU usage and memory allocation information of the applications will be collected continuously by Cloud Profiler. It is a statistical low overhead profiler to improve the performance of the applications. It attributes to the information regarding the source code of the application. Thus, it to detect application parts that consume resources using an interactive time flame graph. Cloud Profiler provides an overall picture of application performance without slowing it down using statistical techniques and low impact instrumentation.

Setting Up Cloud Profiler

Source: https://cloud.google.com

hi0001.ir

- In the GCP console, select or create a Google Cloud Project.
- Navigate to Profiler in the GCP Console.
- Open the Cloud Shell by clicking on **Activate Cloud Shell.**

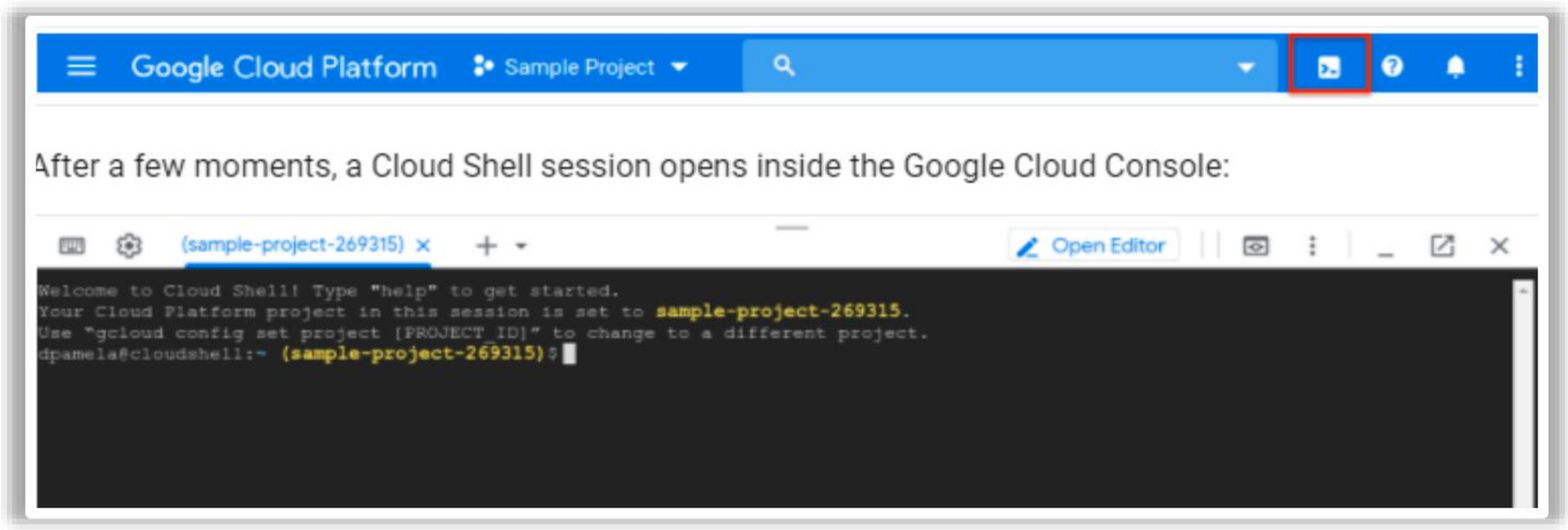


FIGURE 3.223:Active Cloud Shell

- To get a program for profiling

  ```
  go get -u github.com/GoogleCloudPlatform/golang
   samples/profiler/...
  ```

- Profiling the code
  - Open the directory of sample code for profiler

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
cd ~/gopath/src/github.com/GoogleCloudPlatform/golang-
samples/profiler/profiler_quickstart
```

- A CPU intensive workload should be created to provide data to the profiler which is done by main.go program

```
go run main.go
```

- After the application gets started, Profiler starts displaying the data with a flame graph.

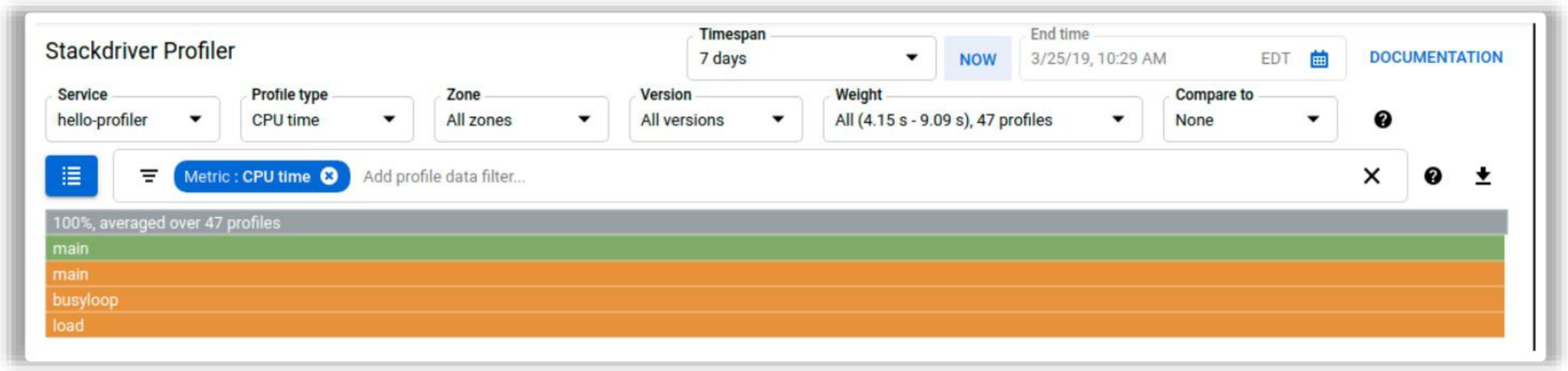
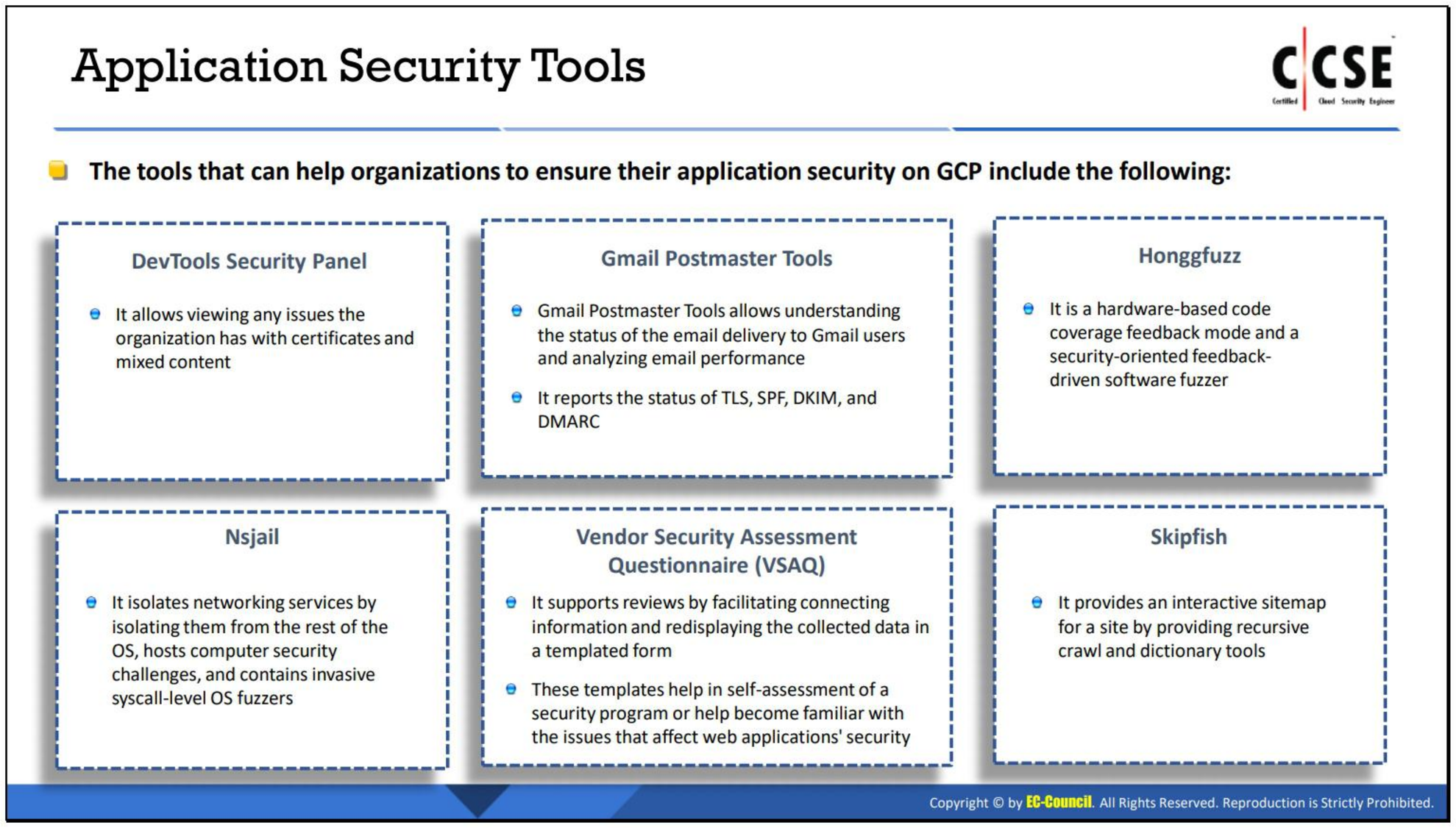


FIGURE 3.224:Stackdriver Profiler

- While profiling multiple applications, **Services** can be used to select the origin of profiled data.
- The type of profile data to be displayed can be selected by **Profile Type.**
- To restrict data from Compute Engine zones or versions of the application, **Zone Name** and **Version** can be used.
- To select profiles captured during excess consumption, use **Weight.**
- The gray frames represent 100% resources consumed.
- Green main frame represents the GO runtime.main.
- Orange main frame represents the main routine.
- Orange busyloop frame represents routine called from the program's main.
- Orange main.load frame represents routine called from the program's main.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Application Security Tools

The tools that can help organizations ensure their application security on GCP include the following:

hide01.ir

DevTools Security Panel

Source: https://developers.google.com

DevTools Security Panel allows viewing any issues the organization has with certificates and mixed content. To do so, go to DevTools and click on the URL bar's lock icon and click **Details** link. On the Security Overview page, click the link that appears to have a filtered view of the Network Panel and know the offending requests.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

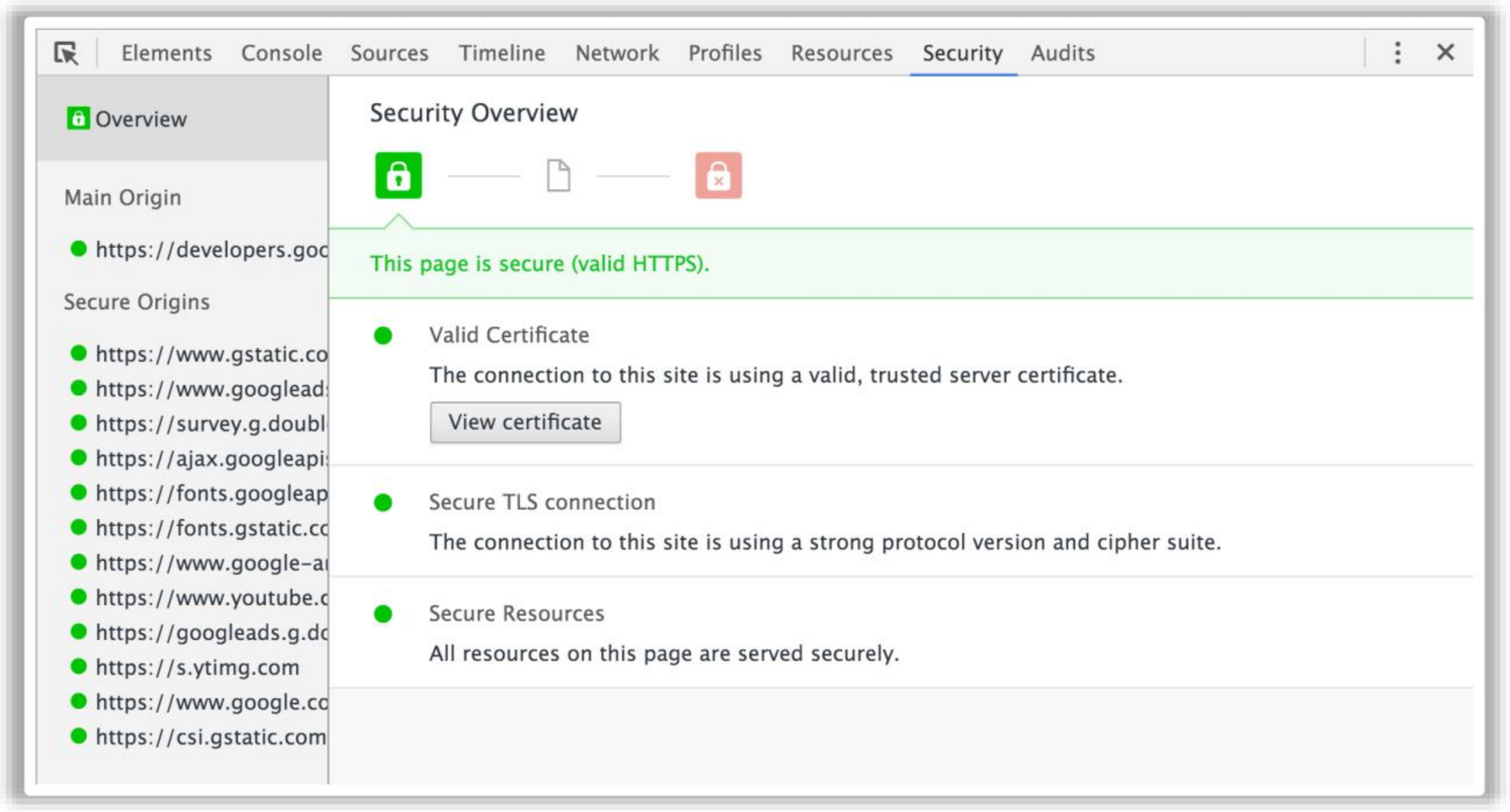


FIGURE 3.225:Checking Certificates Of URL For Issues

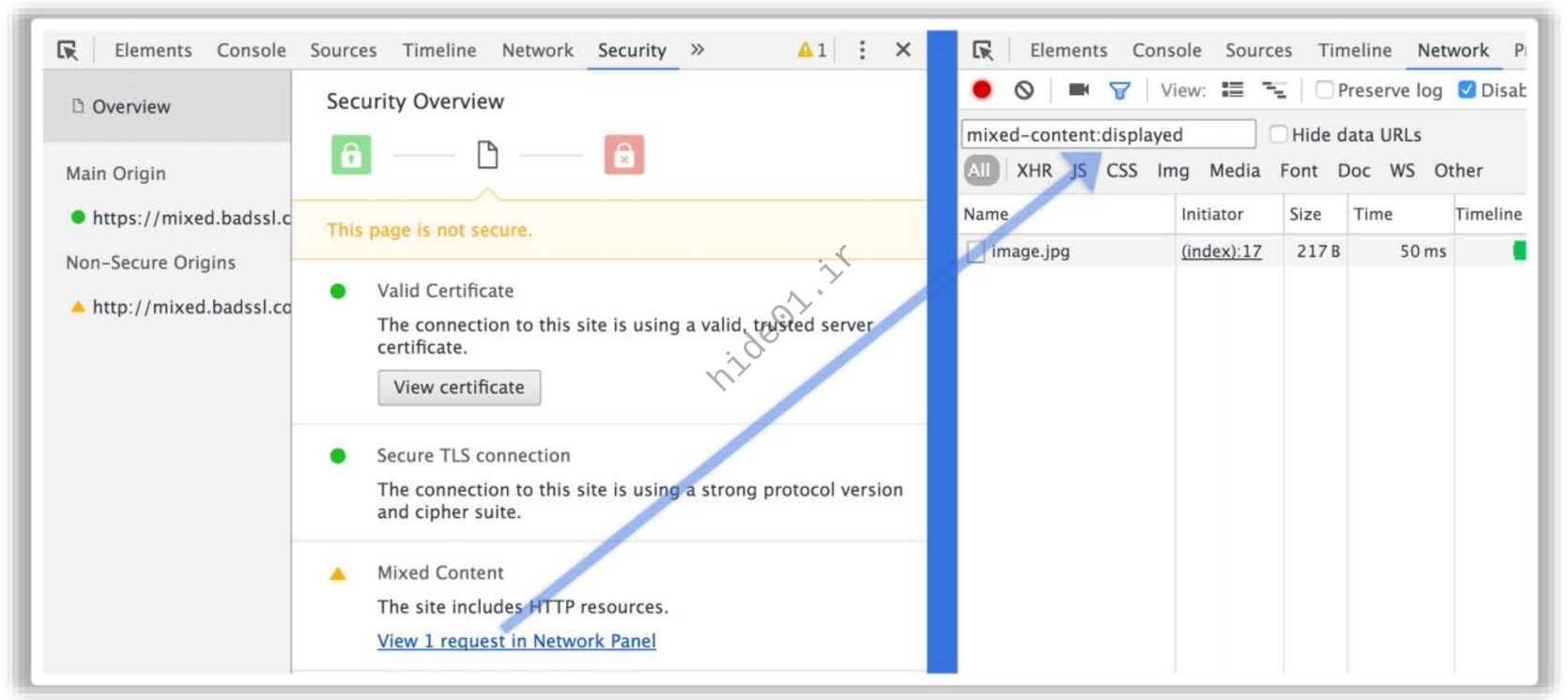


Figure 3.226: Viewing Mixed-content on the Security Overview Page

Gmail Postmaster Tools

Source: https://www.gmail.com

Gmail Postmaster Tools shows the status of the email delivery to Gmail users and analyzing email performance. It reports the status of TLS, SPF, DKIM, and DMARC. It enables gathering of metrics on bulk emails sent to Gmail users and import data into/merge that data with other systems. Here, the metrics include the percentage of an email marked as spam by users and delivery errors.

Honggfuzz

Source: https://honggfuzz.dev

Honggfuzz is a hardware-based code coverage feedback mode and a security-oriented feedback-driven software fuzzer.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The features of Honggfuzz include the following:

- Unlock potential of all your available CPU cores with a single running instance.
- Test a simple/empty **LLVMFuzzerTestOneInput** function with up to 1mo iterations per second on a relatively modern CPU (e.g., i7-6700K).
- Uncover security bugs such as vulnerability in OpenSSL with the critical score mark.
- Low-level interfaces to monitor processes (e.g., **ptrace** under Linux and NetBSD).
- Discover and report hijacked/ignored signals from crashes (intercepted and potentially hidden by a fuzzed program).
- Supports the new qemu mode for black-box binary fuzzing.

Nsjail

***Source*:** https://nsjail.dev

The Linux containerization/isolation tool Nsjail utilizes the Linux namespace subsystem, resource limits, and the seccomp-bpf syscall filters of the Linux kernel. It isolates networking services (e.g., web, time, DNS) by isolating them from the rest of the OS, hosts computer security challenges (so-called CTFs), and contains invasive syscall-level OS fuzzers. Its key features include utilizing kafel seccomp-bpf configuration language for flexible syscall policy definitions, and ProtoBuf-based configuration file.

Skipfish

hide01.ir

Source: https://tools.kali.org

The active web application security reconnaissance tool "Skipfish" provides an interactive sitemap for a site by providing recursive crawl and dictionary tools. Annotate the resulting map with the output from many active security checks. The final report serves as a foundation for professional web app security assessments.

Its key features include highly optimized HTTP handling, minimal CPU footprint, on-the-fly wordlist creation and form autocompletion, and spotting flaws such as blind injection vectors.

VSAQ (Vendor Security Assessment Questionnaire)

Source: https://vsaq-demo.withgoogle.com

The interactive questionnaire application VSAQ (Vendor Assessment Questionnaire) supports reviews by facilitating connecting information and redisplaying the collected data in a templated form. In Google, the questionnaires help assess the security programs of third parties. The templates help with the self-assessment of a security program or when trying to become familiar with the issues that affect web applications' security.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

GCP Application Security Best Practices

Web Security Scanner Best Practices

- Perform the scan in a **test environment** by creating a separate App Engine project and loading the application and data there
- Create a test user account time that does not have access to sensitive data as many applications present a special workflow during a users first login
- Block individual user interface elements that do not wants to be activated
- Perform a backup of the data before scanning
- Specify URL patterns that need not be crawled or tested
- Carefully **audit** the application before the scan for any feature that may affect data/users beyond the scope

Security Best Practices for Protecting App Engine

- Use HTTPS requests to access the App Engine app more securely
- Set up access controls in the App Engine to define who has access to a particular service
- Set up App Engine Firewall to control access to the App Engine app through a set of rules:
  - Allow only traffic within a network
  - Allow only traffic from a specific service
  - Block abusive IP addresses
- Use network ingress control to control the network traffic

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

GCP Application Security Best Practices (cont'd)

hide01.ir

Cloud Identity Aware Proxy Best Practices

- Do not use third-party content delivery network in front of the application as CDNs cache content and serve unauthenticated users with cached page
- Ensure use of **signed headers** for App Engine Standard Environment, Compute Engine, and GKE applications for properly securing the application
- Route all requests to the Compute Engine through a **load balancer**
- Configure firewall rule to allow health checking
- Check the source IP of requests in the application to ensure that the IP range is the same that is allowed in the firewall rule

Secrets Manager Best Practices

- The authentication to applications requires API keys, passwords, etc., which are stored in Secrets Manager and the following best practices can help in secure storage of sensitive information:
  - Use **Cloud IAM** to grant roles and permissions to access the resources
  - Apply permissions by following the principle of least privilege
  - Enable **Secrets Manager API** before using Secrets Manager
  - Enable **automatic replication** if there is no preference where to store the secret data
  - Enable **manual replication** to pick regions to store data

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

GCP Application Security Best Practices

Google has the best mechanisms in place to protect applications from DDoS attacks. Handling and mitigation of DDoS attacks are a shared responsibility between Google Cloud Platform and users. The DDoS protection on applications in GCP includes the deployment of detection systems, scaling, and implementing protection barriers. Some of the best practices to protect the applications deployed in AWS are described below:

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Reduce the attack surface:
  - An isolated and secure network can be created with Google Cloud Virtual Network.
  - Firewall rules and port forwarding can be used for opening access to ports and protocols.
  - The applications can be isolated by using subnetworks, firewall rules, and IAM.
  - Anti-spoofing protection is enabled by default for private networks in GCP.
- Isolate the internal traffic:
  - NAT gateway or SSH bastion Host can be used to limit the instances facing the internet.
  - Deploy Internal Load Balancing to internal client instances.
  - Setup instances without Public IP addresses.
- Enable proxy-based load balancing:
  - Layer-4 and below attacks such as SYN floods and IP fragment floods can be mitigated if HTTPS load balancing is enabled.
  - Deploy HTTPS load balancing in multiple regions to disperse attacks.
- Scaling:
  - Deploying GFE Load Balancing, the front end automatically scales to absorb attacks and terminates user traffic.
  - Implementing HTTPS load balancing and SSL proxy enables a single anycast IP frontend and the deployed backend instances to increase the surface area to absorb the attack.
  - Along with configuring HTTPS or SSL proxy load balancing, configure autoscaling to handle sudden traffic spikes.
- CDN offloading:
  - Google Cloud CDN acts as a proxy between the users and origin servers. During DDoS attacks for cacheable content, the flood requests are sent to points of presence close to the users and hence protecting the backend servers. Thus, the attack is absorbed from multiple locations.
  - CDN interconnect can be used to direct traffic from VPC networks to providers' network, providing extra DDoS protection.
- API rate limiting:
  - API rate limits can limit the number of requests that can be made to the Google Compute Engine API.
- Deployment of App Engine:
  - Block a set of IPs/IP networks, which can be specified with a dos.yaml file, from accessing the application.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The App Engine sits behind GFE, which defends against most layer-4 attacks.

Best Practices for App Engine Protection

- **HTTPS requests** can be used to access the App Engine app more securely.
  - For **appspot.com** domains, use HTTPS URL prefix to send requests to the default service of a cloud project.
  - To convert HTTP URL to HTTPS, the periods between each resource shall be replaced.
  - For **custom domains,** SSL certificates provisioned by App Engine can be used to send requests.
- **Access control**
  - Access control can be configured in App Engine to determine who can access the services within the project.
  - Following the PoLP, different accounts can be given different roles to ensure that they have the necessary permissions to support the application.
- **App Engine Firewall**
  - Access to the App Engine can be controlled with the App Engine Firewall by denying or allowing requests from certain IP addresses.
  - **Allow traffic from specific network:** Certain ranges of IPs from selected networks can access the application.
  - **Allow traffic from a specific service:** All the requests to the App Engine app can be proxied before they reach the App Engine.
  - **Block IP addresses:** The application can be secured from DDoS attacks by blocking the traffic from specific IPs with malicious characters.
- **Ingress controls**
  - The application receives only HTTPS requests from specific sources if network ingress controls are used.
  - **All**: Receives all traffic.
  - **Internal only**: The requests that are sent from VPC networks in the same project will be received.
  - **Internal and Cloud Load Balancing**: The applications receive request through Cloud Load Balancing or the request from VPC networks in the same project.
- **Google Cloud Security Scanner**
  - Cloud Security Scanner identifies vulnerabilities and threats in the application by crawling the App Engine application.

Best Practices for Web Security Scanner

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Web Security Scanner should be used with utmost caution to prevent it from producing false positives. The best practices are described below.

- **Perform scans in test environment**: The application can be loaded into an App Engine project to develop a test environment for performing vulnerability scans. The scan can be done in a test environment by creating a separate App Engine project and loading the application and data there.
- **Create a test account**: A test account should be created for performing the scan operations, without access to the sensitive data to get the desired scan result. As many applications present a special workflow during a user's first-time login, a test user account can be created that does not have access to sensitive data.
- **Blocking individual user interface elements**: The individual user interface elements that need not to be activated can be blocked by CSS class (inq-no-click). During the scanning operation, event handlers attached to this are not activated.
- **Backup data**: It is a good practice to back up the data before the scan operation.
- **Exclude URLs**: The URL patterns can be defined, which will not be scanned.
- **Audit the app:** Carefully audit the application before the scan for any feature that affects data and users beyond the scope.

Cloud Identity Aware Proxy Best Practices

- **Caching**: A third-party CDN shall not be used in front of the application. Third-party CDNs cache content and serve the content to unauthenticated users.
- **Securing application**: Signed headers can be used for the App Engine flexible environment and App Engine standard environment to secure the application.
- **Configuring the firewall:** A network load balancer can be used to route the request to the Compute Engine.
  - Firewall rules can be configured for checking the application health.
  - Check the source IP of incoming requests to check whether they are from the allowed IP range.

GCP Secret Manager Best Practices

Applications require credentials for authentication, such as API keys, passwords, and certificates. The authentication details can be stored securely as a text file by implementing protection. That information can be securely stored in the Secret Manager. Before using the Secret Manager, enable the Secret Manager API. The Secret Manager has several built-in best practices.

- **Cloud IAM:** Cloud IAM can be used to grant roles and permissions to access the resources.
- **Global names and replication**: Secrets Manager has a replication policy in which it addresses the customers who want full control in regions where the secrets are stored, and some others do not have such preferences. This can be met with automatic replication and user-managed replication in GCP.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Automatic replication**: Google itself can select the region to store the secrets. Automatic replication can be enabled if there is no preference where to store the secret data.
- **User-managed replication**: The secret data will be replicated to the specified regions by the user. Manual replication can be enabled to pick regions to store data.

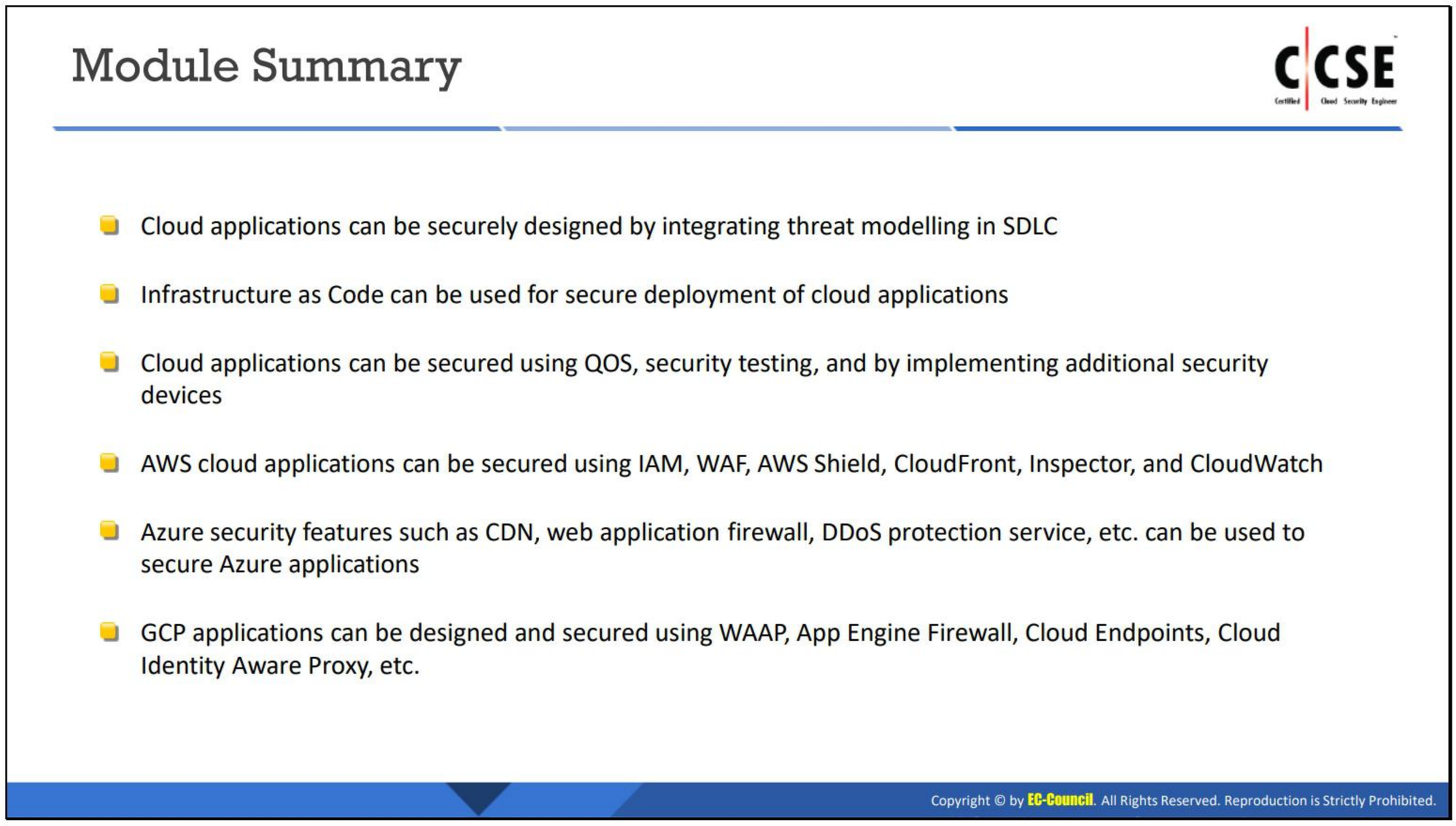
- **First-class versioning**: The secret data is automatically versioned by the secret's manager using the secret versions as most operations take place on the secret version.
- **Principle of Least Privilege (PoLP):** The secrets can be accessed by the owners only. Others must be granted the permissions for access by using Cloud IAM. Apply permissions by following the PoLP.
- **Audit logging:** Cloud audit logging records all interactions with the Secret Manager. These audit logs can be ingested into anomaly detection services to detect threats or deviation from normal functioning.
- **Strong encryption**: Data is encrypted with TLS and AES-256-bit encryption.

Other Best Practices

- Secret Manager does not have automatic rotation feature. Google Cloud Functions and Secret Manager API can be used to perform rotations automatically.
- Data access audit logs should be enabled to log all interactions to Secrets Manager.

hide01.ir

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

This module discussed the importance of application security to secure the cloud environment. It highlighted the various security controls that can be added to secure the applications consumed in SaaS model. It described the SSDLC of cloud applications as well as the designing of a secure cloud application architecture. It also demonstrated the various security features provided by AWS, Azure, and GCP Cloud for securing the hosted applications.

It highlighted the following points:

- Cloud applications can be securely designed by integrating threat modeling in the SDLC
- IaC can be used for secure deployment of cloud applications.
- Cloud applications can be secured using QoS, security testing, and by implementing additional security devices.
- AWS cloud applications can be secured using IAM, WAF, AWS Shield, CloudFront, Inspector, and CloudWatch.
- Azure security features such as CDN, WAF, DDoS protection service, etc. can be used to secure Azure applications.
- GCP applications can be designed and secured using WAAP, App Engine Firewall, Cloud Endpoints, Cloud Identity Aware Proxy, etc.

Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.

hide01.ir