EC-Council

C|CSE™

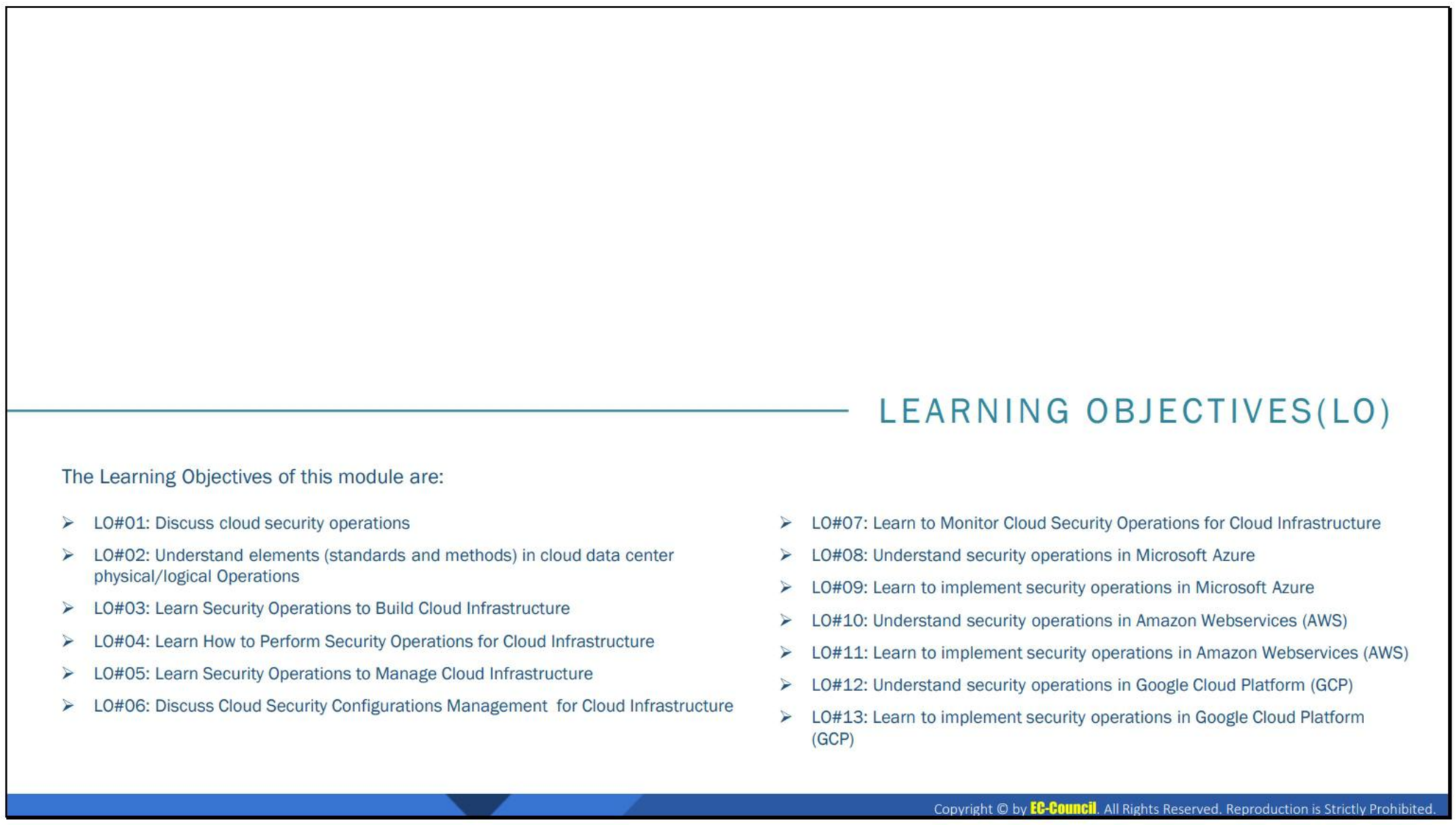
Certified Cloud Security Engineer

Security Operations in Cloud

Module 05

This page is intentionally left blank.

hide01.ir



Learning Objectives

After transferring the workload and sensitive information in a cloud ecosystem, an organization must efficiently operate the cloud infrastructure and services to satisfy customer requirements. For smooth facilitation of business, the organization should identify, investigate, and mitigate the cybersecurity threats in cloud operations using various tools, disciples, and protocols.

Cloud security engineers should have a complete understanding of cloud operation security, including the operation security provided by major cloud service providers such as AWS, Azure, and Google Cloud to secure organizations from internal and external attacks. This module will provide important and relevant information about cloud operation security to cloud security engineers. The module also explains the implementation of cloud operation security in AWS, Azure, and Google Cloud. At the end of the module, cloud security engineers would be able to effectively implement cloud operation security in their organizations.

The learning objectives of this module are:

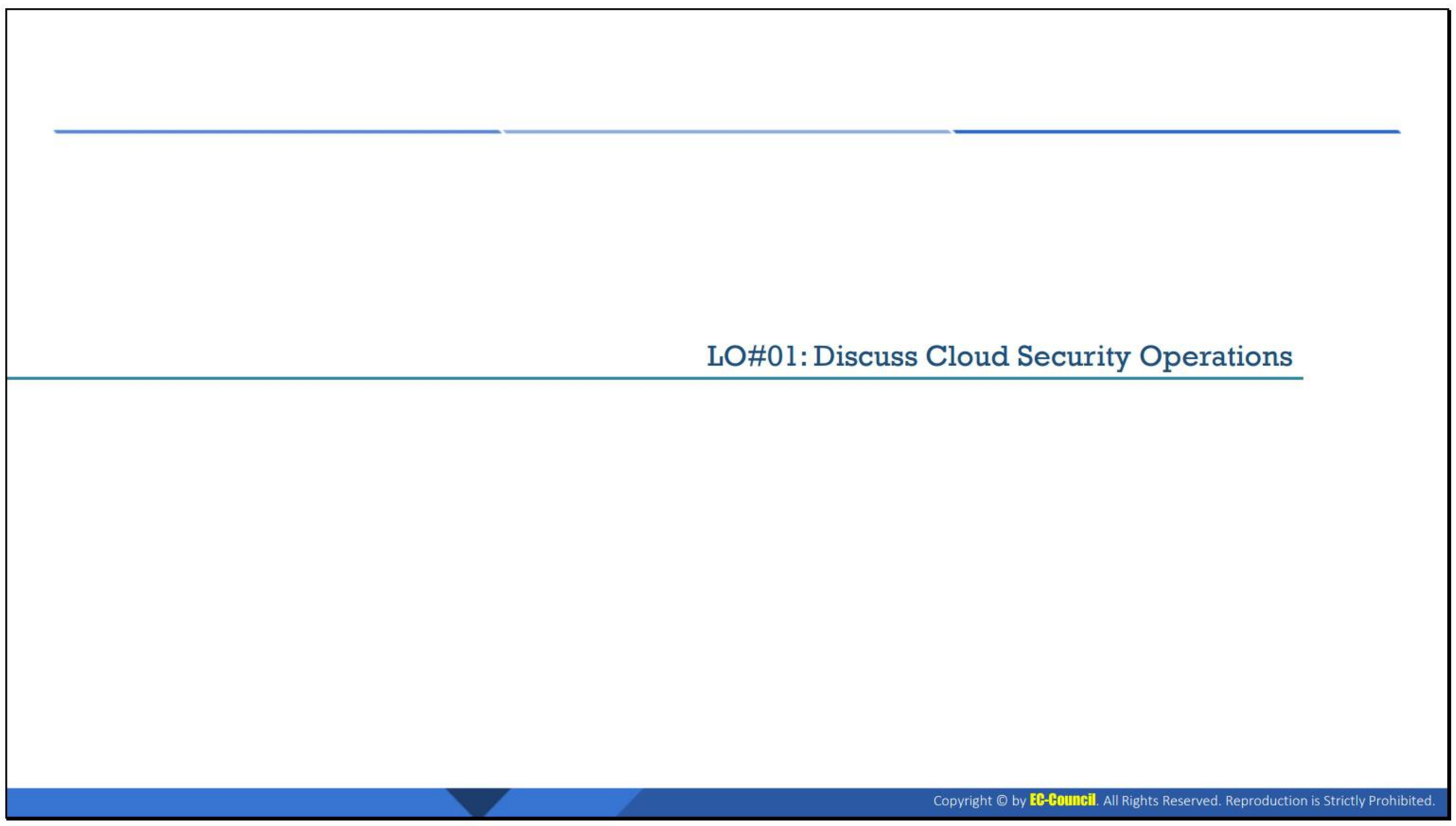
- Discuss cloud security operations
- Understand elements (standards and methods) in cloud data center physical/logical Operations
- Learn Security Operations to Build Cloud Infrastructure
- Learn How to Perform Security Operations for Cloud Infrastructure
- Learn Security Operations to Manage Cloud Infrastructure
- Discuss Cloud Security Configurations Management for Cloud Infrastructure

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

- Learn to Monitor Cloud Security Operations for Cloud Infrastructure
- Understand security operations in Microsoft Azure
- Learn to implement security operations in Microsoft Azure
- Understand security operations in Amazon Webservices (AWS)
- Learn to implement security operations in Amazon Webservices (AWS)
- Understand security operations in Google Cloud Platform (GCP)
- Learn to implement security operations in Google Cloud Platform (GCP)

hide01.ir

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

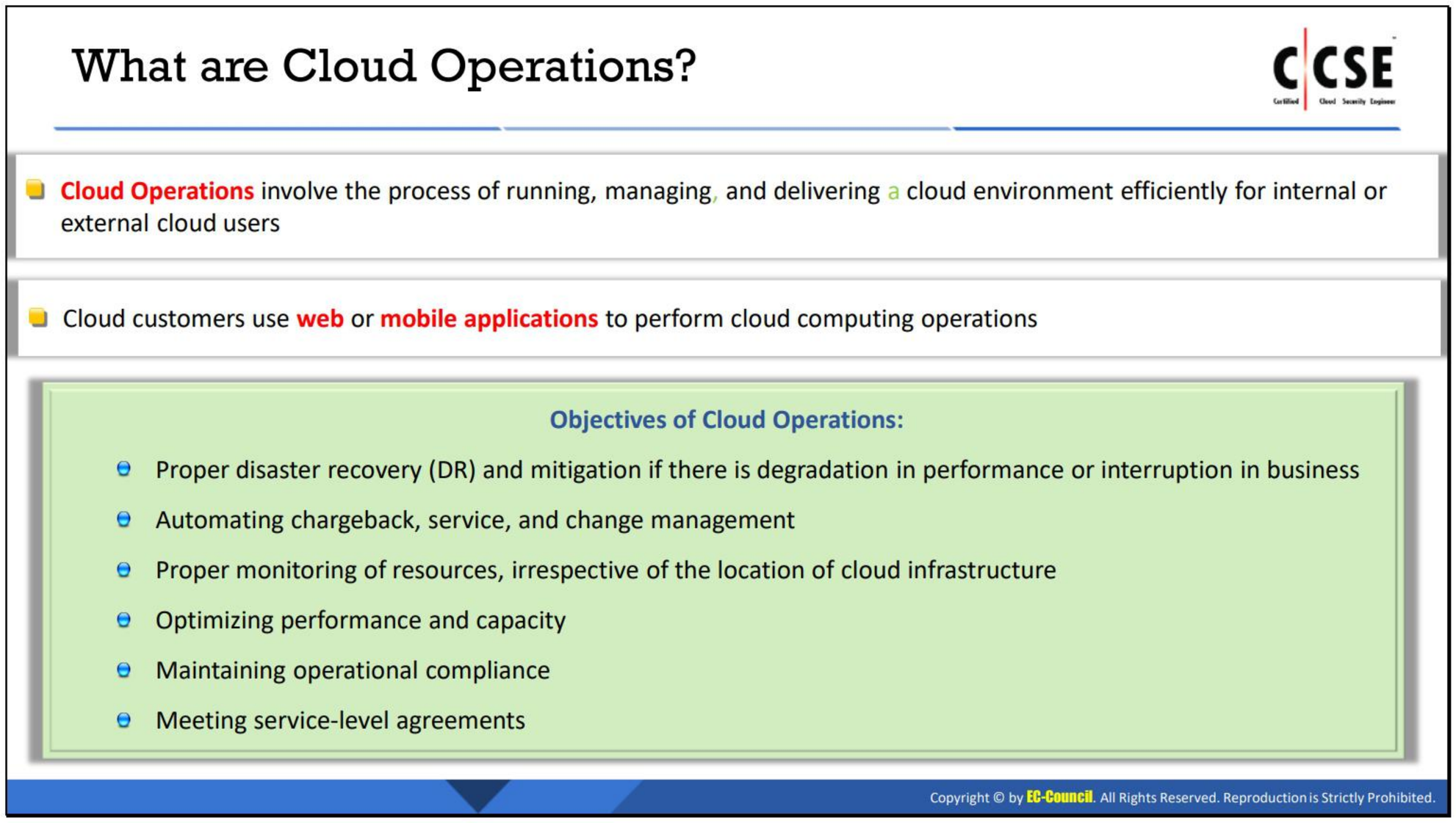


LO#1: Discuss Cloud Security Operations

The objective of this section is to understand cloud operations, cloud operation security, and the strategies involved in securing cloud operations. This section explains the basics of cloud operation security and how cloud operations can be secured. This section will help cloud security engineers in learning the strategies that can reduce security and compliance risks.

hidoi.ir

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



What are Cloud Operations?

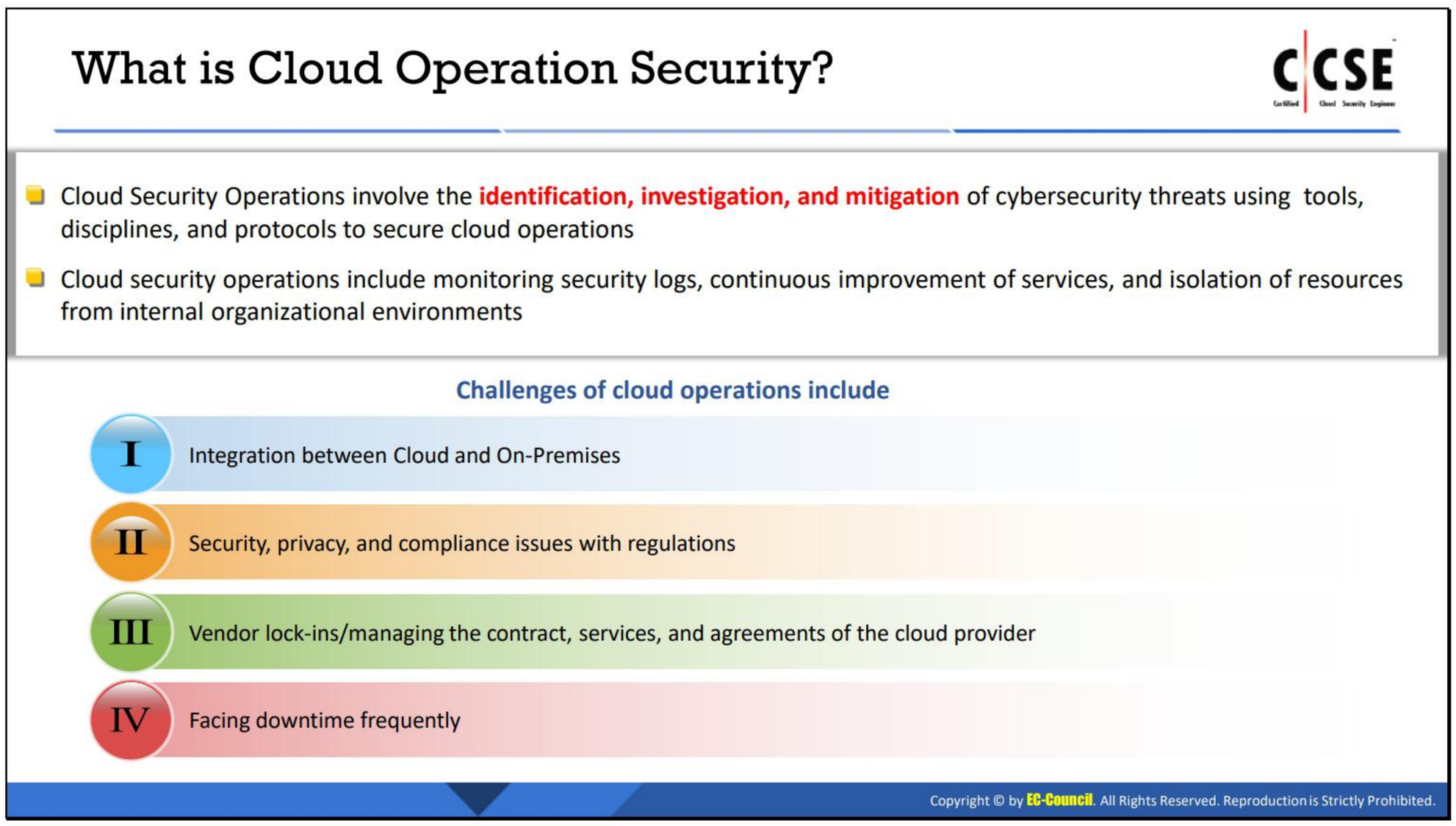
Cloud Operation is the process of running, managing, and delivering the cloud infrastructure and cloud services/environment efficiently to internal or external cloud users. It ensures maximum performance while maintaining availability to satisfy customer requirements and service level agreement standards, managing operational costs, and security and compliance. Cloud customers use the web or mobile applications to perform cloud computing operations.

Cloud operations include handling the database or application server of an organization hosted on a public/private cloud as well as managing and designing networks for the VPC (Virtual Private Cloud) of an organization.

The objectives of cloud operations include:

- Delivering the cloud infrastructure and/or services
- Properly monitoring resources irrespective of platform or infrastructure location
- Maintaining operational compliance
- Automating chargeback, service, and change management
- Maintaining configuration
- Enabling transparency
- Proper disaster recovery (DR) and mitigation if there is degradation in performance or interruption in business
- Meeting service-level agreements
- Optimizing performance and capacity

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



What is Cloud Operation Security?

Securing the data and networks in a cloud environment is different from ensuring their security in an on-premises environment. In a cloud, the static on-premises infrastructure elements are abstracted to virtual or software, and the organization focuses more on applications, application program interfaces, and user roles in securing cloud operations.

Cloud Operation Security involves identifying, investigating, and mitigating cybersecurity threats in cloud operations. It includes tools, disciplines, and protocols that ensure the security of cloud operations. The common ground between the consumer and provider must be anchored in clear contractual and agreement languages in cloud security operations.

For example, monitoring security logs, continuous improvement of services, isolating records, confidentiality of records, and isolation of resources from internal organizational environments.

The concerns involved with cloud computing security from an organizational cloud operations perspective include

- **Availability**

  In cloud, availability refers to the time that can be guaranteed by the cloud service provider for which the customer data and services are available. Cloud service providers should provide an uptime of 99.999 (or five nines), allowing cloud customers to access their resources with downtime for no more than approximately 5 min per year.

- **Integrity**

  In cloud, integrity refers to allowing authorized people to make changes to the organizational data.

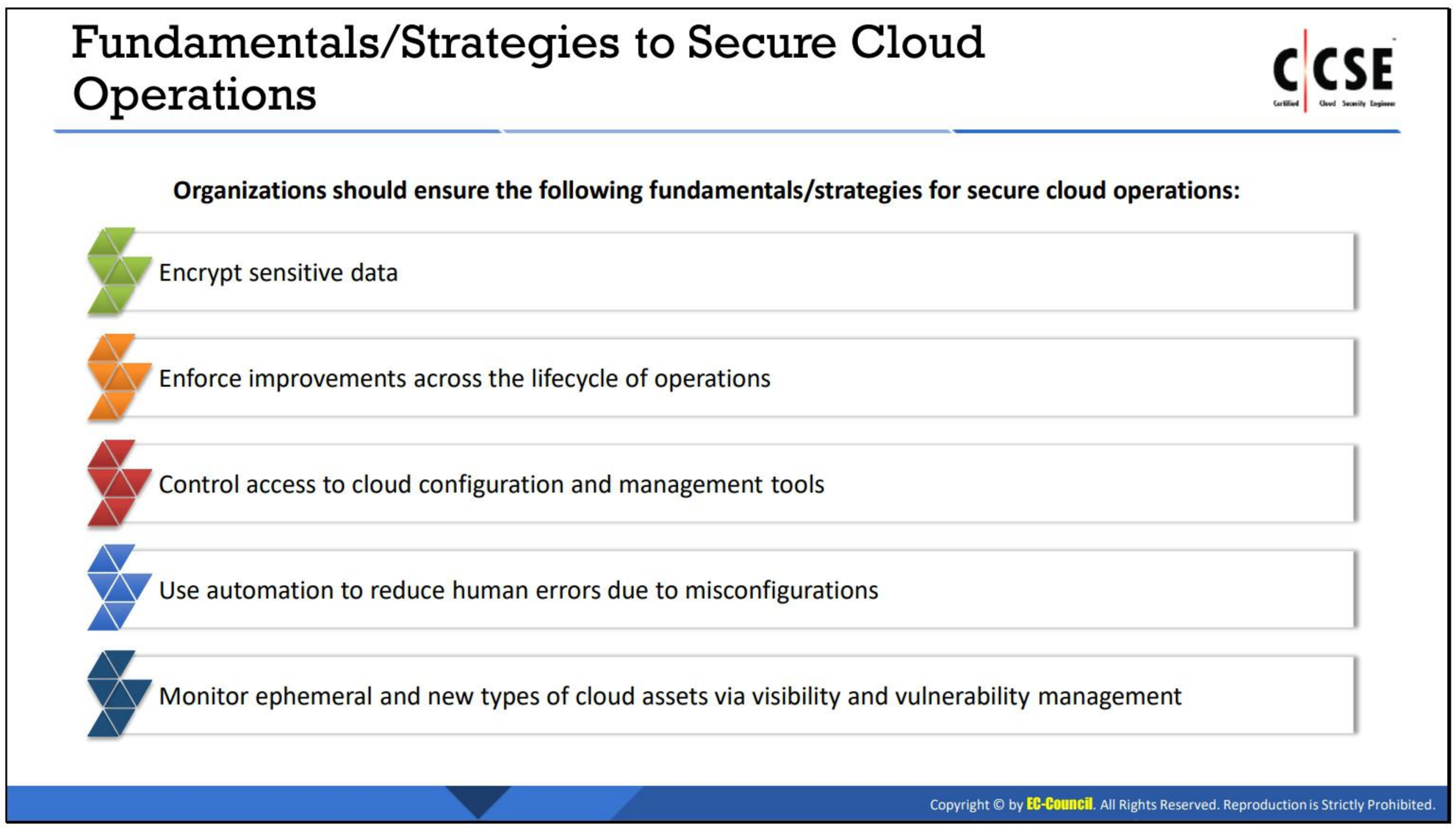
- **Confidentiality**

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

In cloud, customers data are stored on remote servers that are operated by cloud service providers using an internet connection. In this context, confidentiality refers to preventing unauthorized access to these data and ensuring that only permitted users can access the data.

hide01.ir

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



Fundamentals/Strategies to Secure Cloud Operations

The fundamentals/strategies that can reduce the security and compliance risks *or* ensure secure cloud operations include:

hide01.ir

- **Encryption of sensitive data**

  Use encryption to protect data in transit because data leaks and data spillage are unavoidable.

  - To reduce the impact of a compromised key, encrypt sensitive data while segmenting the data using multiple keys
  - Rotate keys with strong access control policies regularly
  - Implement encryption for the data in transit and at rest
  - Review CSP network encryption
  - Evaluate third-party encryption solutions
  - Evaluate native cloud solutions

- **Monitoring ephemeral and new types of cloud assets using visibility and vulnerability management**

  Organizations may have less visibility to monitor threats and ensure compliance with a cloud solution. Legacy methods that include human vulnerability detection and remediation management may work slowly. Therefore, the vulnerability tools for container architectures, serverless architectures, rapid infrastructure deployment cycles, and other new cloud services should be extended, and in-line services should be used. For

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

example, using network overlays and proxies for replicating network traffic to transparent security services.

Additionally, the following should be known before moving to the cloud.

- Can the infrastructure enable visibility (using a system of logs, reports, and dashboards) across the cloud environment?
- Are the incident response service-level agreements of the vendor transparent?
- Is there sufficient information for integrating incident response service-level agreements into processes?

- **Using automation to reduce human errors due to misconfigurations**

  Manual configurations may cause human errors in cloud computing. The consequences of such errors could be inadvertent data spillage, inconsistent deployment configurations, and vulnerabilities. To prevent human errors,

  - Deploy and configure the cloud infrastructure correctly using automation with pretested and audited configurations
  - Automate the infrastructure and platform builds
  - Automate security testing
  - Automate security guardrails
  - Automate baseline configurations
  - Reduce the risks of unavailable zones due to provider errors using high-availability configurations
  - Perform configuration checks regularly
  - Perform routine compromise assessments

- **Enforcing improvements across the lifecycle of operations**

  Continuous improvements should be made to the implementation of cloud. In this case, the DevSecOps approach can be used. If the DevSecOps approach is implemented, ensure the following:

  - Enable ops staff to continue upgrading the cloud environment by enforcing site reliability engineer functions
  - Integrate DevSecOps with the staff in development
  - Integrate DevSecOps with the staff in operations
  - Track new products and services using road maps for future integrations

- **Controlling access to cloud configuration and management tools**

  Organizations should be protected against internal and external threats using cloud management and configuration tools; for example, tools such as APIs, CSP consoles, and

hide01.ir

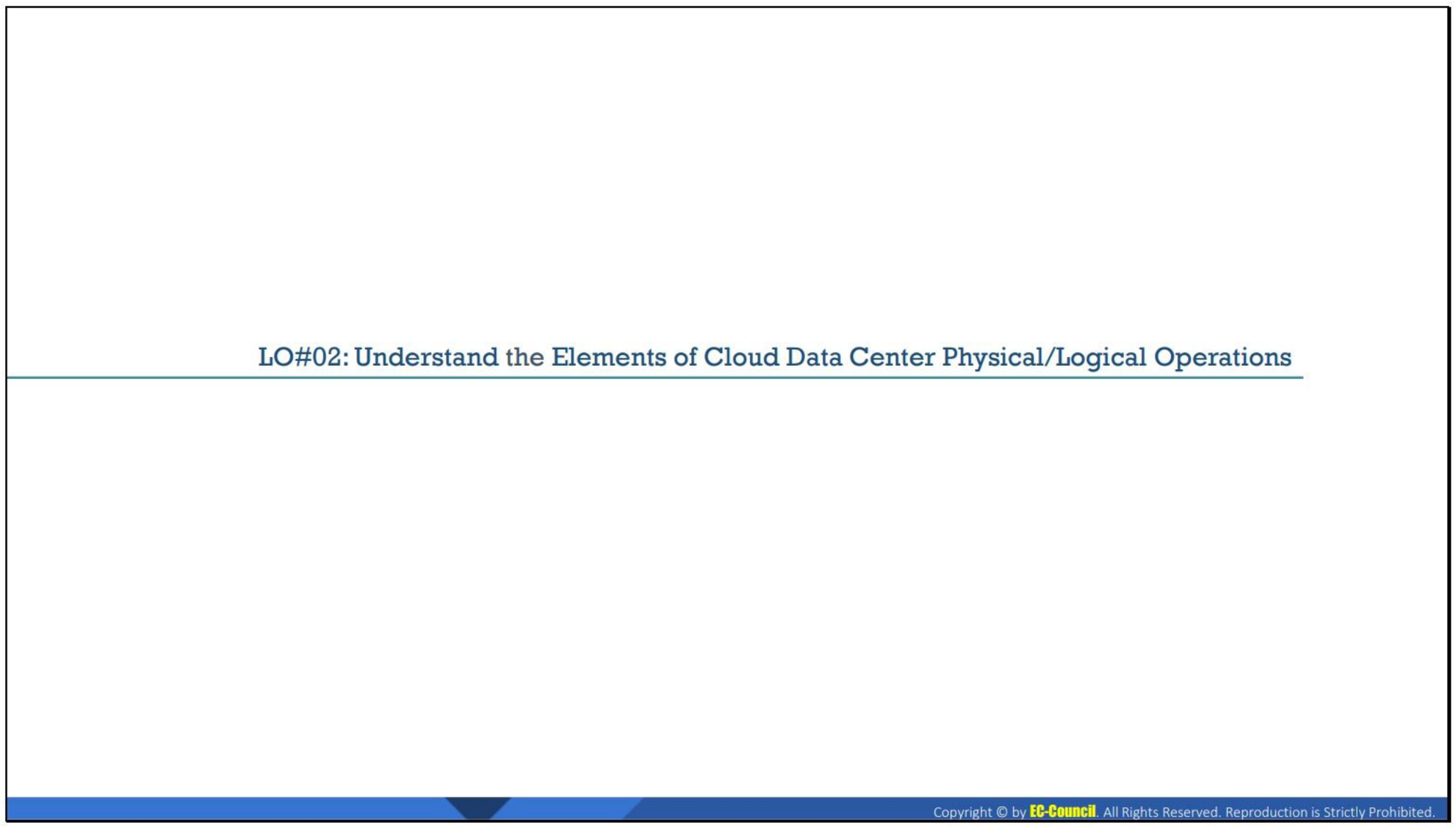
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CLIs enable efficient role-based control. To control the access to such cloud configuration and management tools,

- Use two-factor authentication, certificates, and digital signatures for authentication and authorization
- Ensure that training and skill evaluation are mandatory before cloud roles are granted
- Separate user and admin credentials
- Restrict user access for production systems
- Ensure process standardization for account lifecycle management

hide01.ir

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



LO#2: Understand the Elements of Cloud Data Center Physical/Logical Operations

Organizations that adopt the cloud environment must understand the perspective of cloud service providers (CSPs) in cloud operations. The objective of this section is to understand the various standards and methods used by CSPs for the physical and logical operations of their cloud data centers. This section explains the important physical/logical operation mechanisms used by CSPs in their data centers, including facilities and redundancy, virtualization operations, storage operations, and physical and logical isolation. In this section, cloud security engineers will become aware of the various standards and methods utilized by CSPs in data centers and use them efficiently to secure their organizations.

hide01.ir

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

Cloud Data Center Physical/Logical Operations

- To some extent, organizations must understand the perspective of CSPs in cloud operations
- **Physical Operations** include barriers and detection mechanisms intended to prevent intruders from accessing the cloud data center and alerting the security personnel
- **Logical Operations** include specific controls that manage the access to systems and physical spaces within the cloud data center
- A robust data center can provide continuous system operation and access to data (**uptime (highest is 99.999%)** to numerous customers with various services
- The standards and methods helpful in achieving an uptime of 99.999% in the physical/logical operations of a data center include:
  - **Facilities and Redundancy**
  - **Virtualization Operations**
  - **Storage Operations**
  - **Physical and Logical Isolation**

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

Cloud Data Center Physical/Logical Operations

Physical Operations include barriers and detection mechanisms such as biometric access control, heat-sensing, infrared CCTV, and electric fence. These mechanisms are intended to prevent intruders from accessing the data center and alerting the security personnel.

Logical Operations involve specific controls that are established to manage access to systems and physical spaces within the data center. For example, using a locked door is a physical security operation that involves safeguarding the server room entrance of the data center, but two-factor authentication for opening the door is a logical operation.

Figure 5.1: Physical/Logical Operations

To some extent, organizations must understand the perspective of CSPs in cloud operations. Accordingly, the internal working of the data center of CSPs should be understood by examining the physical/logical operations.

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

The data center of a CSP should be resilient to all threats from cyber attacks and natural disasters. A robust data center can provide continuous system operation and access to data (uptime) for numerous customers with various services. The Uptime of the data center is as follows:

- TIER I: availability of 99,671%
- TIER II: availability of 99.741%
- TIER III: availability of 99.982%
- TIER IV: availability of 99.995%

The industry standard for uptime in cloud service provision is 99.9%, implying that the providers should possess:

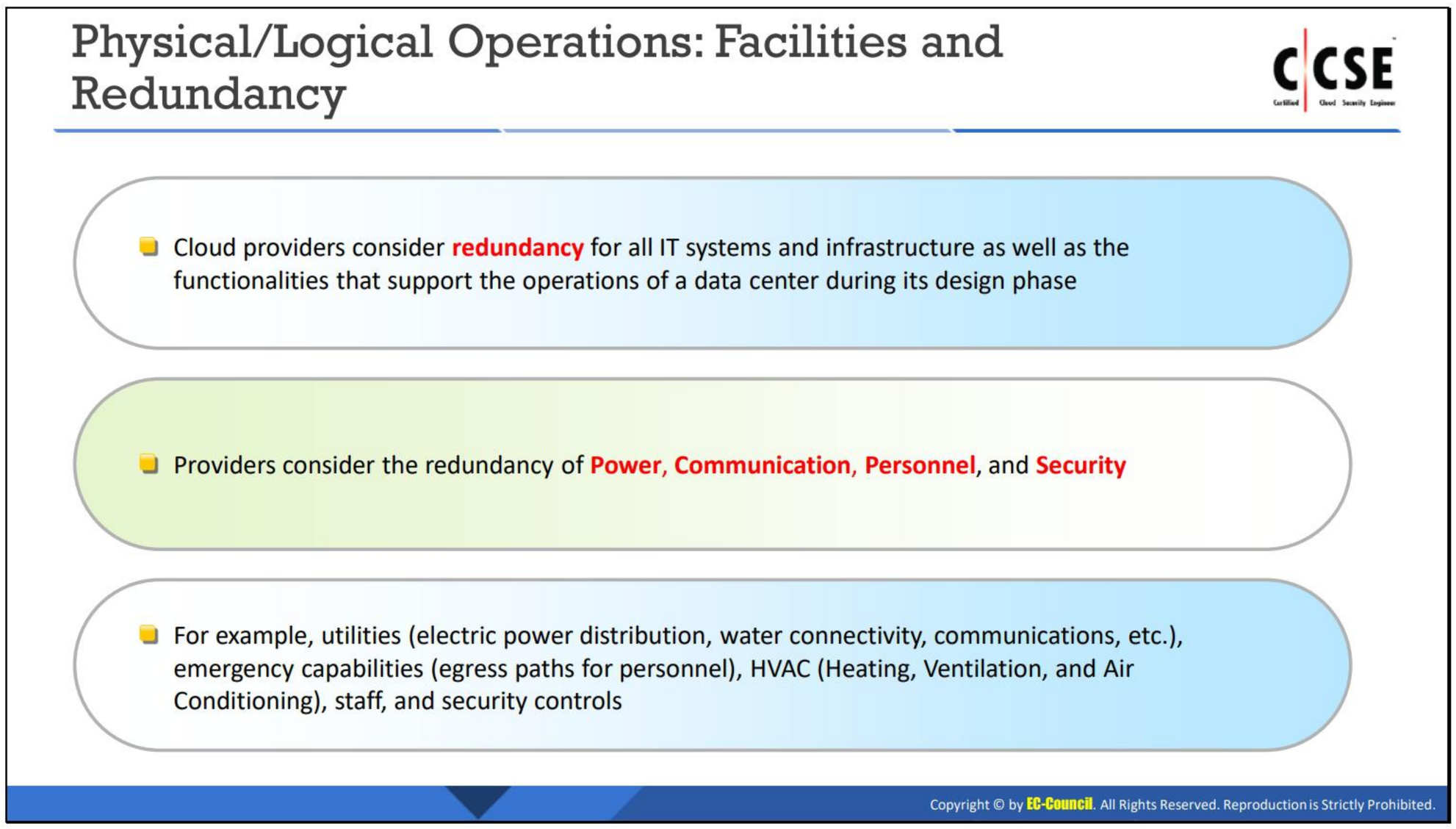
- Downtime of less than 90 s in a day
- Downtime of less than 45 min in a month
- Downtime of less than 9 h in a year

The standards and methods helpful in achieving an uptime of 99.999% in the physical/logical operations of a data center include

- Facilities and Redundancy
- Virtualization Operations
- Storage Operations
- Physical and Logical Isolation

hide01.ir

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



Physical/Logical Operations: Facilities and Redundancy

CSPs should consider redundancy for all IT systems and infrastructure as well as the functionalities that support the operations of a data center when it is being designed. For example, utilities (electric power distribution, water connectivity, communications), emergency capabilities (egress paths for personnel), HVAC (heating, ventilation, and air conditioning), staff, and security controls.

- **Power Redundancy:** Data centers require sufficient power for operating the processing and storage systems for cloud customers and the systems (HVAC and lighting) that run the data center. CSPs consider energy utility providers and actual physical connections (from provider to data center) for the primary power requirements.
- **Communication Redundancy:** Data centers increase the demand for internet services at their geographic location. In such cases, ISPs build infrastructure to serve the internet requirements of data centers.
- **Personnel Redundancy:** The following techniques can be adopted to enhance the robustness of personnel who administer and support IT components.
    - **Cross-Training:** Personnel should be trained considering their primary duties and employee duties. This technique is expensive because it requires a significant training budget and high salaries for top-level personnel. Moreover, this technique can result in personnel redundancy.
    - **Water:** Water provides cooling, fire suppression, and drinking for personnel and the systems in a data center. Multiple pumping facilities should be included for sufficient pressure and power for running the pumps when designing redundancy for water supply.

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

- **Egress:** Data centers should have multiple points of escape in the case of an emergency. Thus, fire suppression systems should be designed over egress paths and the ingress should be strictly controlled.
- **Lighting:** When the lighting system fails in a data center, employee productivity will decrease. Therefore, it is important to install emergency lights and ensure that the lighting system is connected to the backup power supply.

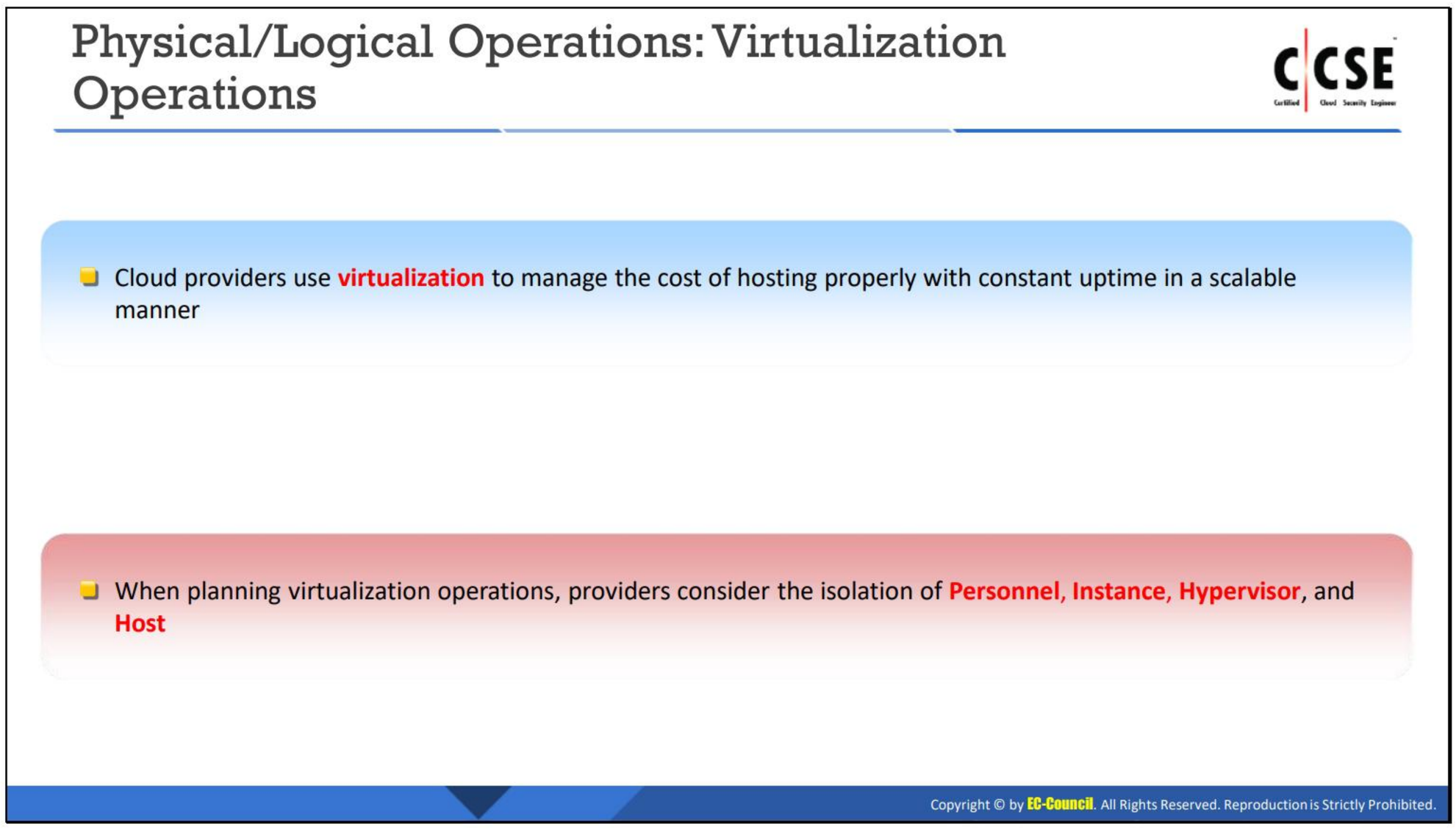
- **Security Redundancy:** This ensures that the process of breaching becomes complicated. To implement this, include all basic protective measures for a cloud data center. In the form of layering, include monitoring the fence line, installing video surveillance, and electronic monitoring of tampering on the fence, etc.

  In addition to perimeter security in data center design, include physical security measures such as guest/visitor access through a controlled entry point, interior physical access controls (turnstiles, badging, keys, etc.), and RFIDs.

- **Holistic Redundancy - The Uptime Institute (UI) Tiers:** The advisory organization for matters related to IT service "Uptime Institute (UI)" provides a standard for data center design and certifies data centers for compliance. The UI standard comprises four tiers, among which, the tier 4 data center is an expensive selection and fits any organization when considering cloud migration irrespective of the sensitivity of information assets/uptime requirements.

hide01.ir

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



Physical/Logical Operations: Virtualization Operations

Virtualization is the only method to manage the cost of hosting customers properly with constant uptime in a scalable manner in a cloud data center. This section discusses the aspects considered by a CSP when planning virtualization operations.

hi0001.ir

- **Personnel Isolation**

  CSP administrators can access devices that run customer instances physically. In such cases, the provider should ensure that impropriety and conflict of interest do not affect customer service. For example, if any two competing customers exist on a host and if some contingency forces the administrator to stop one instance to maintain the functionality of a device, the administrator should choose based on data center performance and operation. Theoretically, customer business details should be masked from the admins. Practically, this might be less than ideal and may be impossible to implement.

- **Hypervisor Hardening**

  Controlling the hypervisor could enable attackers to access the data of every instance. Thus, the hypervisor should be updated and patched as per vendor standards and it should be ensured that it contains no default account. It should be monitored using automatic sensors. For providers, the bare-metal (Type 1) hypervisor is preferable to the hypervisor because it provides less attack surface.

- **Instance Isolation**

  VMs should be logically isolated from each other with strict logical controls. It should be ensured that the raw data and metadata are not leaked between instances, and an

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

instance should not reveal what other instances present on the same host and their operations.

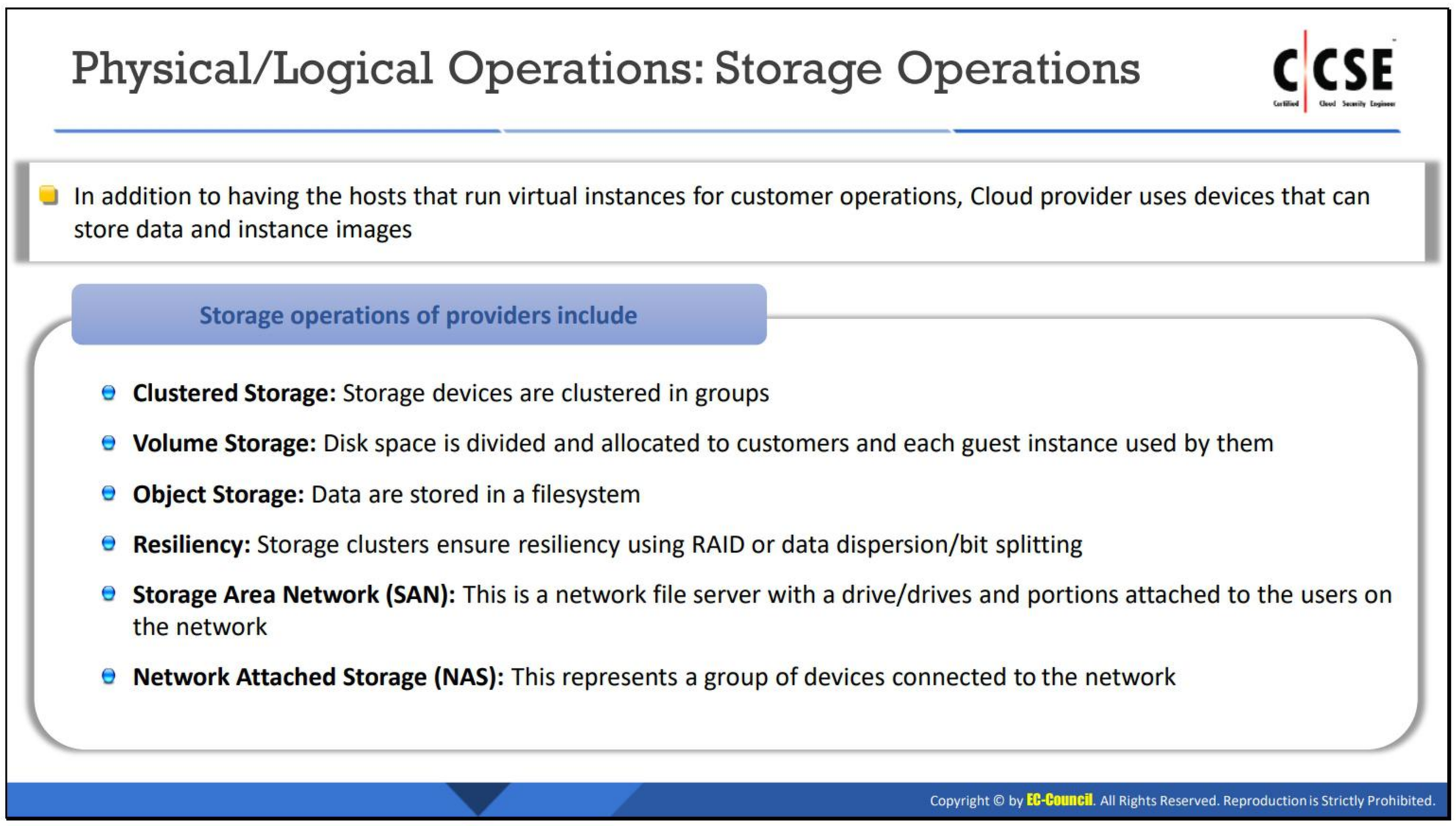
Instance isolation should be tested and monitored using controls in the sandbox and live environment. Moreover, reduce the possibility of guest escape in which a user escalating a privilege can leave the virtual instance and access the host machine itself.

- **Host Isolation**

  All hosts should be physically and logically isolated from each other as much as possible. The hosts are still connected to the network and can communicate with each other; thus, these connections should be minimized and secured. Moreover, host escape activities should be recognized via thorough network monitoring.

hide01.ir

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



Physical/Logical Operations: Storage Operations

In addition to the hosts that run virtual instances for customer operations, a data center comprises devices that store data and instance images. The storage operations include the following.

hide01.ir

- **Clustered Storage and Coupling**

  Storage devices are often clustered in groups. This enhances the reliability, performance, and flexibility of storage operations. Clustered storage architectures accept either of the following two types.

  - **Tightly coupled cluster:** All storage devices are connected to a shared physical backplane directly (tightly). Every component of the cluster connects with other components and subscribes to the same policies and rule sets. This type of clustered storage architecture enhances the performance as it scales. Because the performance of every element is added to the overall cluster performance, the performance is enhanced as the architecture is scaled.
  - **Loosely coupled cluster:** Each node/device of the cluster is independent of other nodes and connected logically (loosely). This allows for greater flexibility, but the cluster performance does not necessarily scale because the nodes/devices do not build on one another. New nodes can be added as per requirement.

- **Volume vs. Object**

  The way the data are stored offer different storage options. The options include:

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

- **Volume storage/Block storage:** In volume storage, the disk space is divided and allocated to the customer as well as each guest instance used by the customer. The virtualized OS of the guest implements a filesystem on the allocated volume.
- **Object storage:** In this type, all data are stored in a filesystem. The customers get access to different parts of the hierarchy to which they are assigned.

- **Resiliency**

  In cloud storage clusters, data security can be implemented via two methods that provide a level of resiliency.

  - **Redundant Array of Independent Disks (RAID):** In RAID configurations, data are stored across disks using "stripping" method thus allowing efficient data recovery because if any drive fails, other drives fill in the missing data. A few RAID schemes (RAID 0-10) enable data recovery after a drive fails by adding parity bits to the raw data.
  - **Data dispersion/Bit splitting:** In data dispersion, data are turned into encrypted pieces along with parity bits. Later, the pieces are written to the drives in the cluster.

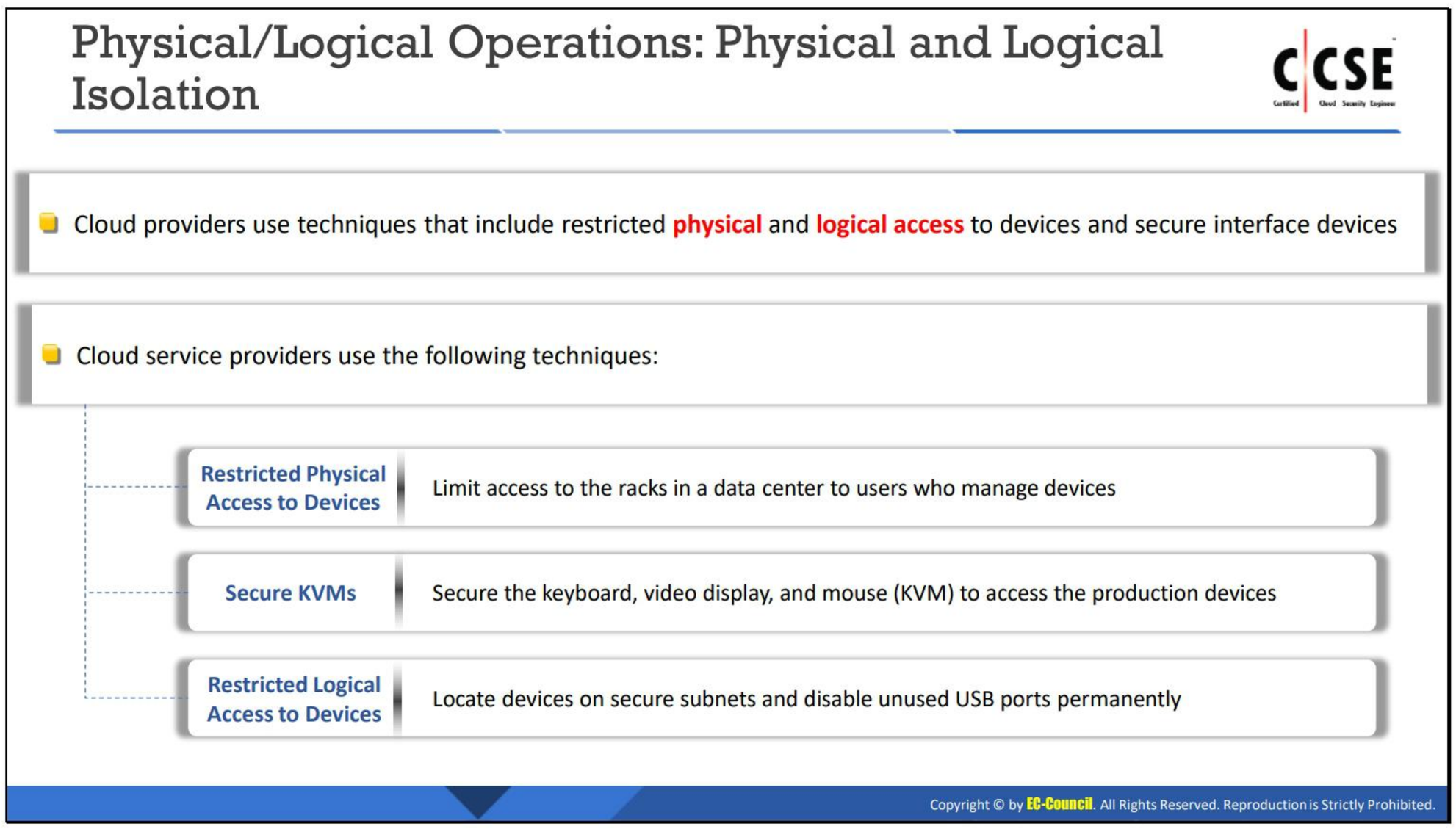
- **SAN vs. NAS**

  Network-attached storage (NAS)/storage area network (SAN) can be used in storage architectures. Both NAS and SAN should be transparent to the user.

  - **NAS:** This is a network file server with a drive/drives and portions attached to users on the network. NAS uses TCP/IP generally.
  - **SAN:** This network represents a group of devices connected to the network, providing storage space to users. Generally, the storage is partitioned and allotted like an empty drive to the user machine. The filesystem is formatted and implemented according to user preferences. SAN uses iSCSI/Fibre Channel protocols. The storage space should be available to users regardless of the device/storage component location.

hacker1.ir

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



Physical/Logical Operations: Physical and Logical Isolation

The principles applied to the physical and logical isolation of personnel, virtualized instances, and storage devices in a cluster should be applied to the data center to include other isolation techniques. Cloud providers use techniques that include restricted physical and logical access to devices and secure interface devices.

- **Restricted Physical Access to Devices**
  - Limit access to racks in the datacenter to who (admins and maintainers) needs to deal with devices to perform their functions
  - Control, monitor, and log entry and egress
  - Lock racks and check keys for each rack
  - Check keyboards, video displays, and mice (KVMs) to use them for a specific task
- **Secure KVMs**

  Secure KVMs to access production devices (processing and storage). Secure KVMs have the following traits.
  - **Secure Data Ports:** These reduce the chances of data leaks between systems connected through a KVM.
  - **Tamper Labels:** These labels show visual indications if the unit housing got opened or breached.
  - **Fixed Firmware:** It cannot be reprogrammed.

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

- **Soldered Circuit Board:** Its components cannot be removed because they are soldered.
- **Reduced Buffer:** Data cannot be stored if a device does not need them immediately.
- **Air-Gapped Pushbuttons:** The current connection will be broken physically before a newer one is established during switching between devices connected to a data center.

- **Restricted Logical Access to Devices**
  - Locate devices on secure subnets, which will reduce the potency of intruders.
  - Control the use of USB ports and eliminate them wherever possible by disabling unused ports permanently.

hide01.ir

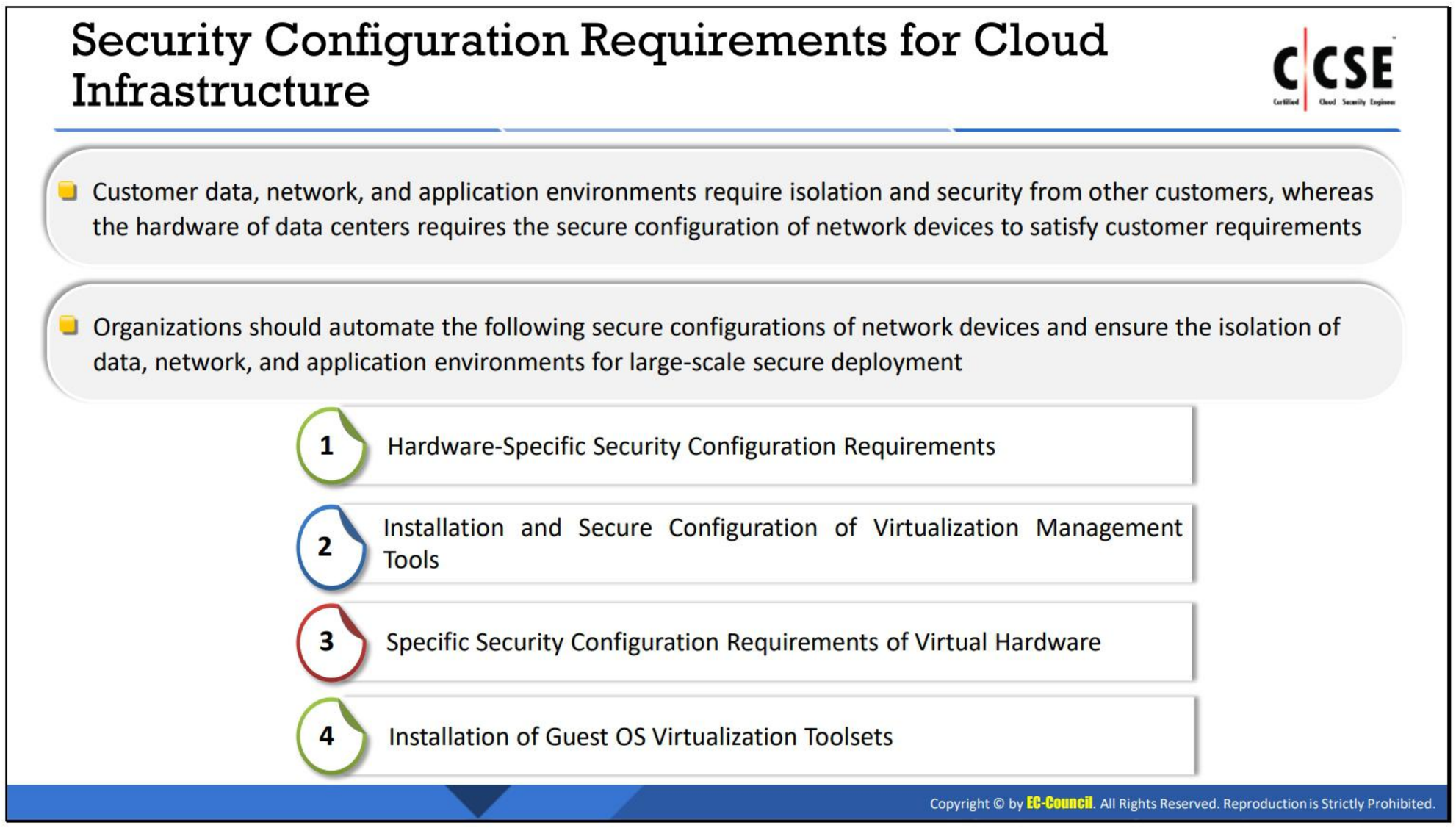
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

LO#3: Learn Security Operations to Build Cloud Infrastructure

The objective of this section is to understand how data, networks, and cloud environments are isolated and secure configurations for network devices are implemented. This section describes the hardware-specific security configuration requirements, installation and secure configuration of virtualization management tools, and virtual hardware-specific security configuration requirements in detail. In this section, cloud security engineers will learn about building and implementing secure physical and logical infrastructure in cloud environments.

hiddn01.ir

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



Security Configuration Requirements for Cloud Infrastructure

The **physical cloud infrastructure** comprises the components of networks, storage, and servers. These components require planning to operate together in the cloud by concentrating on security models and cloud considerations.

hide01.ir

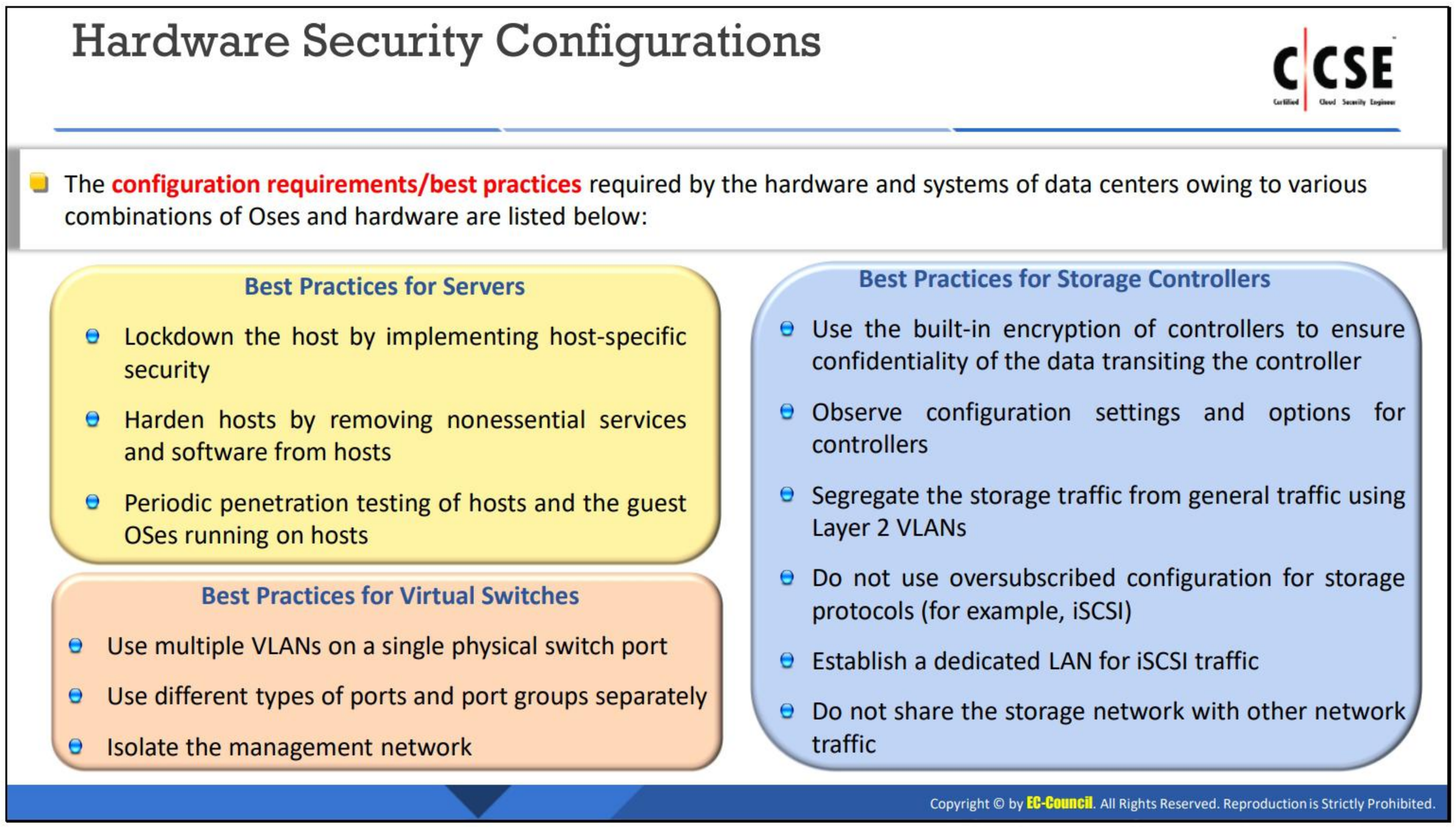
In contrast, the **logical cloud infrastructure** is more abstract and removes the platform and software specifics. Instead, it focuses on logical infrastructure aspects such as processes, regulations, locations, and roles.

Enterprises that want to migrate their environments to cloud architectures require the secure isolation of resources while delivering the management operations and advantages of shared resources. The customer data, network, and application environments require isolation and security from other customers across any private and public CSP. The hardware inside a data center requires secure configuration of network devices, servers, storage controllers, and any other device to meet customer requirements.

Organizations should automate such configurations (given below) for large-scale deployments.

1. **Hardware Specific Security Configuration Requirements**
2. **Installation and Configuration of Virtualization Management Tools**
3. **Virtual Hardware Specific Security Configuration Requirements**
4. **Installation of Guest OS Virtualization Toolsets**

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



Hardware Security Configurations

Generally, a cloud data center has unique and specific requirements for its cloud environment. However, the security of the hardware and systems in a cloud data center is like that in a traditional data center. The hardware and systems of a data center have several configuration requirements owing to the possibility of numerous combinations of OSes and hardware and the specific OSes that run on hardware appliances and hypervisors.

- **Best Practices for Servers**

  Implement the following requirements/best practices to secure servers within the cloud.

  - To secure host servers,
    - Secure the build by following the specific recommendations offered by the OS vendor to deploy the OS securely.
    - Secure initial configuration. This involves the OS vendor, workloads, operating environment, risk assessment, business requirements, risk appetite, and regulatory requirements hosted on the system.
  - Harden hosts by removing nonessential services and software from hosts.
  - Patch hosts by installing all necessary patches provided by hardware and software vendors. For example, patching may include BIOS/firmware updates, driver updates, and OS security patches.
  - Lockdown the host by implementing host-specific security measures. These measures may change with vendors.
    - Block non-root access to the host.

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

- Allow the use of secure communication protocols and tools (for example, Putty and SSH) to connect with the host remotely.
- Configure the host-based firewall to examine and manage communications from and to the host as well as the guest OSes and workloads running on the hosts.
- Use role-based access controls (RBAC) to restrict user access to hosts and user permissions.

○ Secure ongoing configuration maintenance using vendor-provided mechanisms along with other mechanisms.

- Patch management and periodic vulnerability assessment scan of hosts, guest OSes, and applications workloads running on hosts
- Periodic penetration testing of hosts and guest OSes running on hosts periodically

▪ **Best Practices for Virtual Switches**

The core networking component on a host, virtual switches, connect the physical NIC (Network Interface Controllers in the host server to the virtual NICs in VMs. Follow the below configurations/best practices for virtual switches.

○ Decide how engineers should use physical NICs while planning virtual switch security architecture to assign virtual switch port groups to ensure security, segmentation, and redundancy.

○ Use multiple VLANs on a single physical switch port to reduce the number of required physical NICs in a host.

○ Use different types of ports and port groups separately instead of using them together on a single switch.

○ Achieve redundancy by

- Assigning at least two physical NICs to a virtual switch. Here, each NIC connects to a different physical switch.
- Using port channeling that can enhance the available bandwidth between two devices.
- Creating a logical path out of multiple physical paths.

○ Isolate the management network through which the host connects with other hosts and management systems.

○ Isolate the management physically and virtually in a virtual infrastructure.

○ Secure traffic by connecting all hosts, management systems, and clients to a separate physical network.

○ Create isolated virtual switches for the host management network.

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

- Do not club virtual-switch traffic with normal VM network traffic.
- Create a separate isolated virtual switch with its own physical NICs while dealing with internal and external networks.
- Do not club the internal and external traffic on a virtual switch.
- Lock down the access to virtual switches to prevent attackers from moving VMs from one network to another.

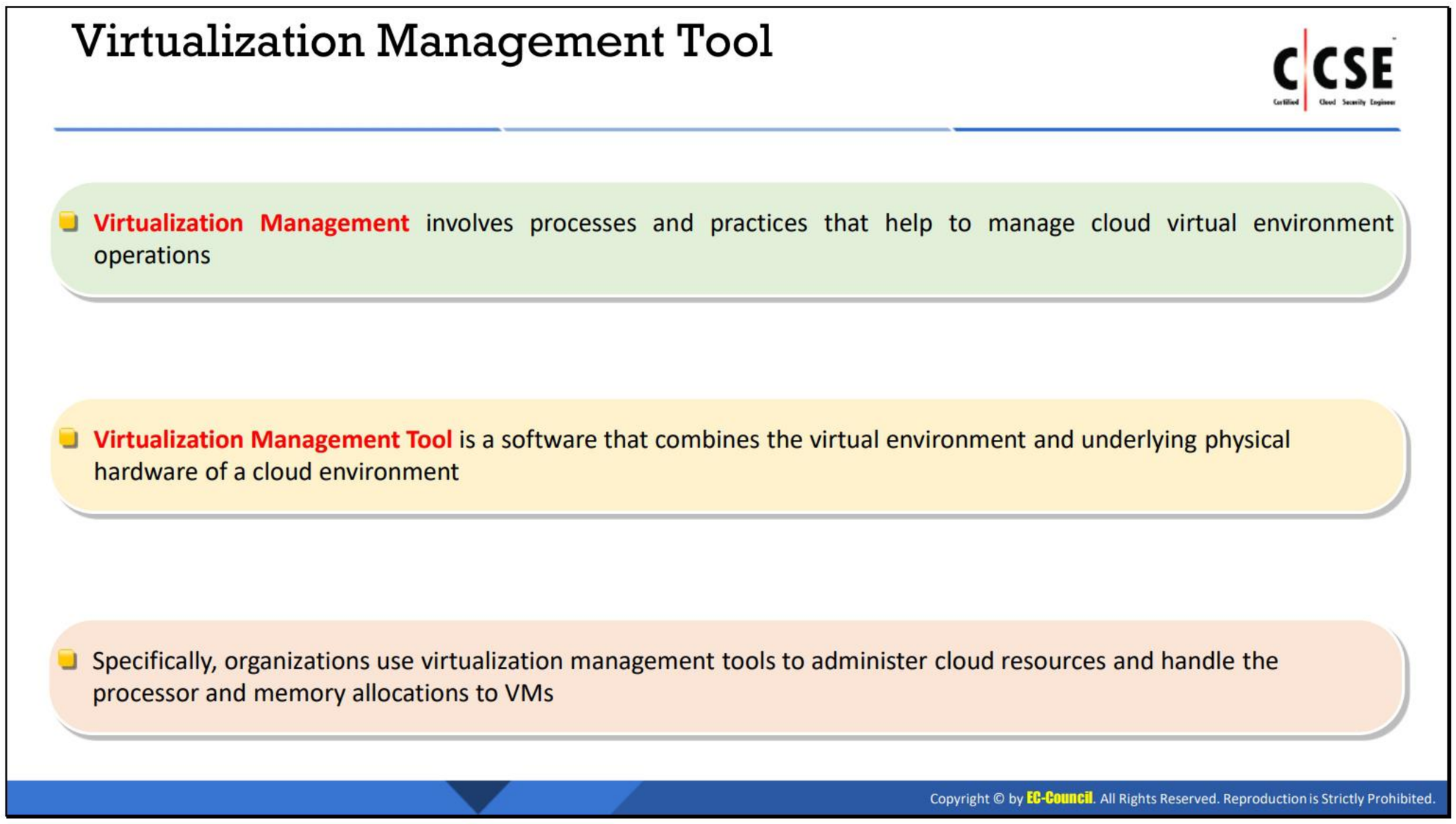
- **Best Practices for Storage Controllers**

  A cloud storage controller is an appliance that can move data from on-premises to the cloud automatically. These controllers use hard-disk drives, solid-state drives, or both to store data on-premises. These controllers can be secured using the following best practices irrespective of the storage protocols (iSCSI, FC, or FCoE) being used.

  - Use the built-in encryption of controllers to ensure confidentiality of the data transiting the controller.
  - Observe the configuration settings and options of controllers because there may be options for disabling services and enabling insecure settings.
  - Segregate the traffic of storage protocol (for example, iSCSI (Internet small computer system interface)) from the general traffic using Layer 2 virtual local area networks (VLANs).
  - Do not use oversubscribed configuration for storage protocols (for example, iSCSI). Instead,
    - Have a dedicated LAN for iSCSI traffic.
    - Do not share the storage network with other network traffic, including management and fault tolerance.

hidoc1.ir

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

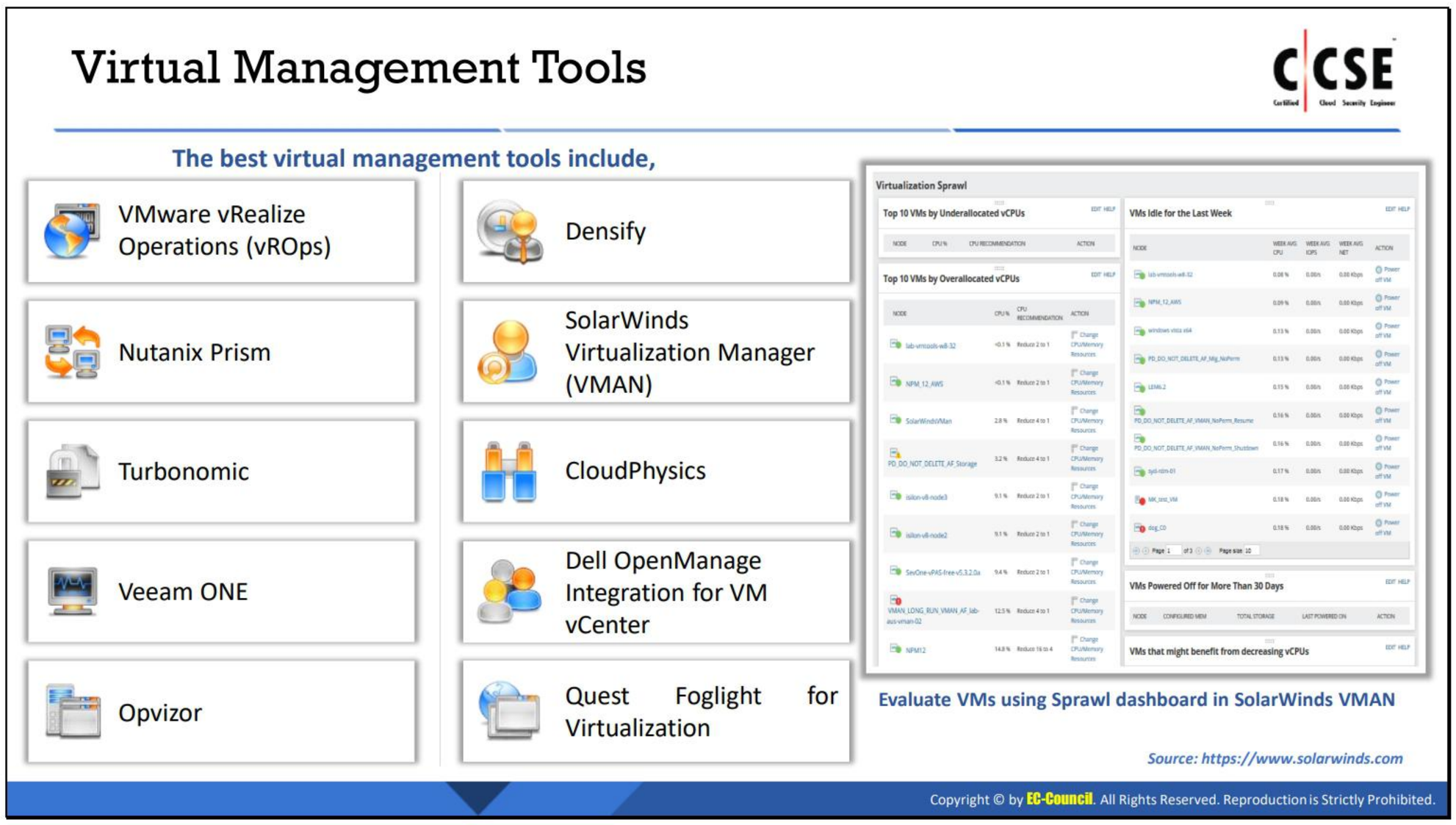


Virtualization Management Tool

Virtualization Management involves processes and practices that help in managing virtual environment operations. It involves controlling operations and applications and acts as an interface between VMs/cloud environments and the physical hardware they run on. Virtual management includes creating, updating, or deleting VMs, infrastructures, and networks and tracking their functioning.

Virtualization Management Tool is a software that combines the virtual environments of a cloud environment and the underlying physical hardware at one point. It enables monitoring of operations and processes, thus providing visibility into cloud virtualization environments to analyze the overall performance and security status of the cloud. These tools enhance data analyses and streamline cloud operations. Specifically, organizations use virtualization management tools to administer cloud resources and handle processor and memory allocations to VMs. Other key features of these tools include dynamic resource allocation and VM performance monitoring. It is important to select the right management tools to meet the required efficiency without increasing cloud operation expenses.

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



Virtual Management Tools

Virtualization management tools are installed based on the selected virtualization platform, and the latest tools are installed on each host. The configuration management plan should include the rules for updating these tools.

hide01.ir

The best virtual management tools include

- VMware vRealize Operations (vROps)
- Nutanix Prism
- Turbonomic
- Veeam ONE
- Opvizor
- Densify
- SolarWinds Virtualization Manager
- CloudPhysics
- Dell OpenManage Integration for VM vCenter
- Quest Foglight for Virtualization

SolarWinds Virtualization Manager

Source: https://www.solarwinds.com

SolarWinds Virtualization Manager (VMAN) helps in fixing and optimizing cloud environment performance issues. One of the key features of this virtualization management software enables

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

monitoring VMware, Nutanix, AHV, and Microsoft Hyper-V problems with virtualization management. This feature of VMAN provides

- Built-in dashboards, reports, and alerts to see the immediate ROI in the virtual management software
- Tools to analyze storage I/O performance with VM
- Virtualization capacity planning can allow the use of data and trends pulled from specific virtualized environments to project future resource growth and needs

Evaluate VMs using Sprawl dashboard in SolarWinds VMAN:

Use the Sprawl dashboard of VMAN to list the top issues in resource views with captured metrics. With the scalability of VMs, cloud environments tend to sprawl timely. This causes resource overallocation and stale VMs misuse resources. Here, the Sprawl dashboard helps to identify the key areas of VM resource usage and metrics, and provides options to manage VMs directly.

Steps to resolve issues with over and under-allocated systems:

- Open Sprawl dashboard. Open **My Dashboard -> Virtualization -> Sprawl.**
- The Sprawl dashboard appears with VM data that provide a historical view of the cloud environment.

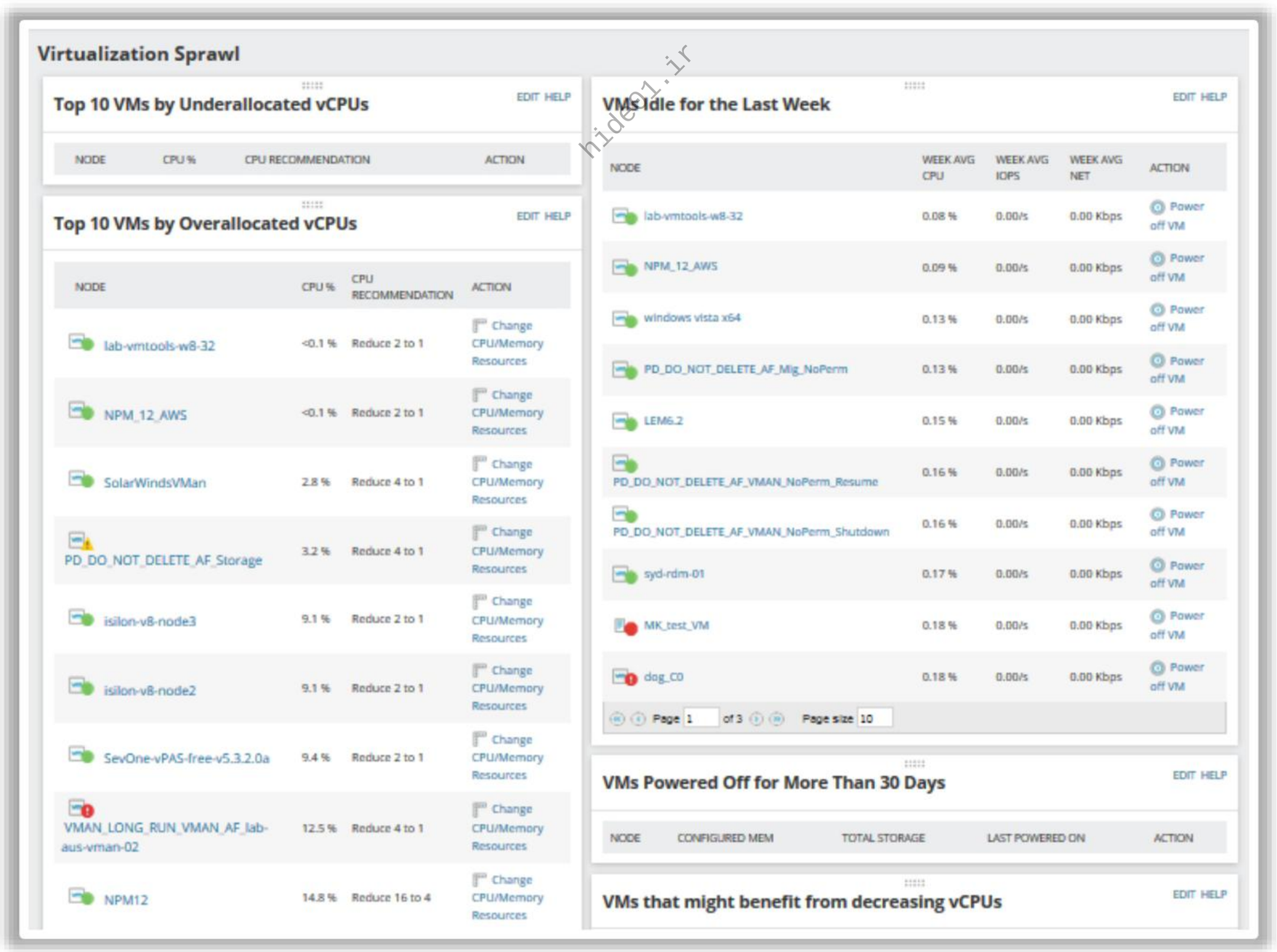


Figure 5.2: Sprawl Dashboard

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

- Observe the **Top 10 VMs by Over-allocated vCPUs** resource to identify the VMs with over-allocated CPU. Here, this resource displays powered-on VMs with two or more CPUs with a peak sum of CPU load that has not exceeded 30% in the last seven days. Balance CPU allocation and free resources for under-allocated systems.

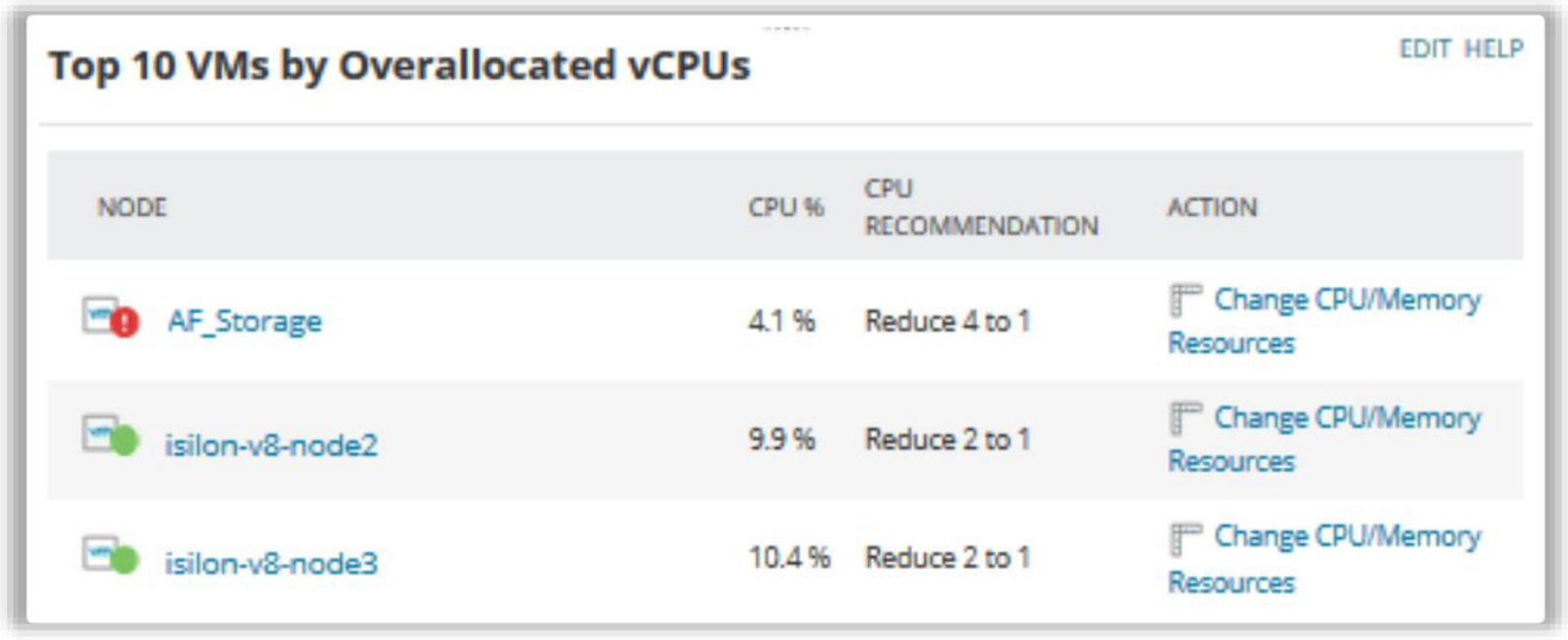


Figure 5.3: Top 10 VMs by Over-allocated vCPUs

- Click **Change CPU/Memory Resources** for a virtual system to free up CPUs. The recommended CPU allocation is listed based on the usage.
- Here, the VM **AF_Storage** has three CPUs over-allocated based on the historical CPU load data.

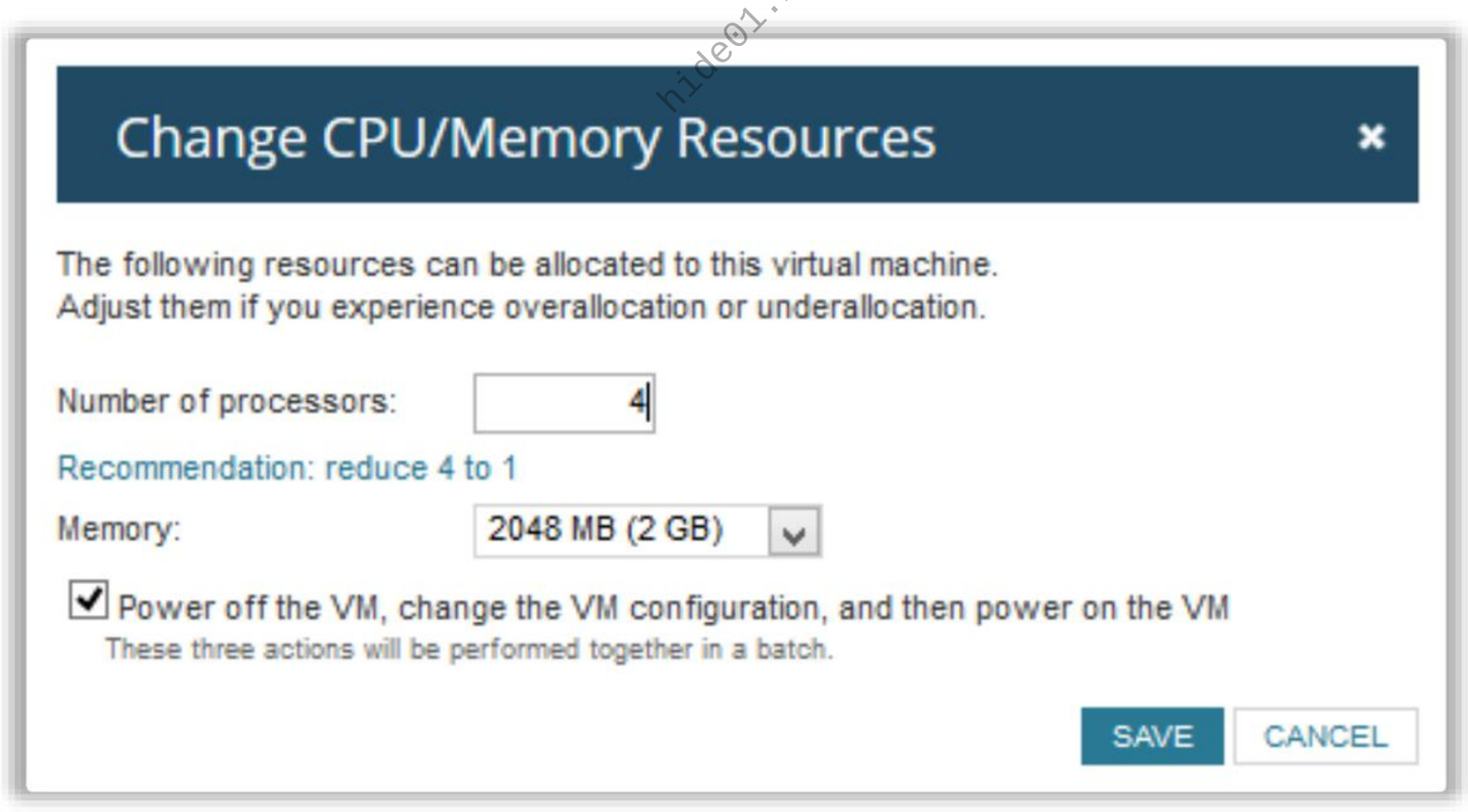


Figure 5.4: Change CPU/Memory Resources

- Enter 1 for in the field "**Number of processors.**" Select **Power off the VM, change VM configuration, and then power on the VM,** and click **Save**.
- Observe the **Top 10 VMs by Over-allocated Memory** resource to determine the VMs with over-allocated memories. This resource displays powered-on VMs with two or more MBs of memory and the average memory usage has not exceeded 30% in the last seven days. Balance the memory allocation and free the resources for under-allocated systems.

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

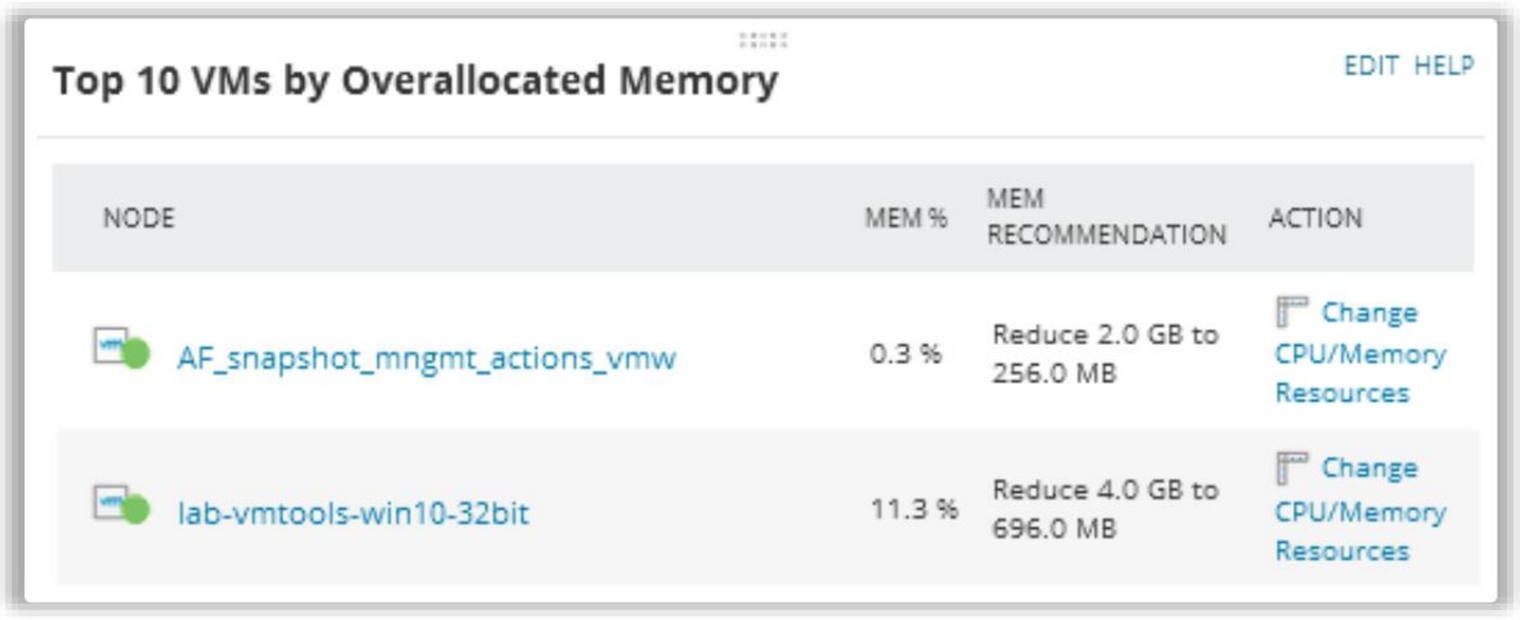


Figure 5.5: Top 10 VMs by Overallocated Memory

- Click **Change CPU/Memory Resources** for a virtual system to free up memory.
- A recommended number of CPUs is listed based on the usage. The **lab-vmtools-win10-32bit** VM has 3 GB of over-allocation that could be used by under-allocated systems.

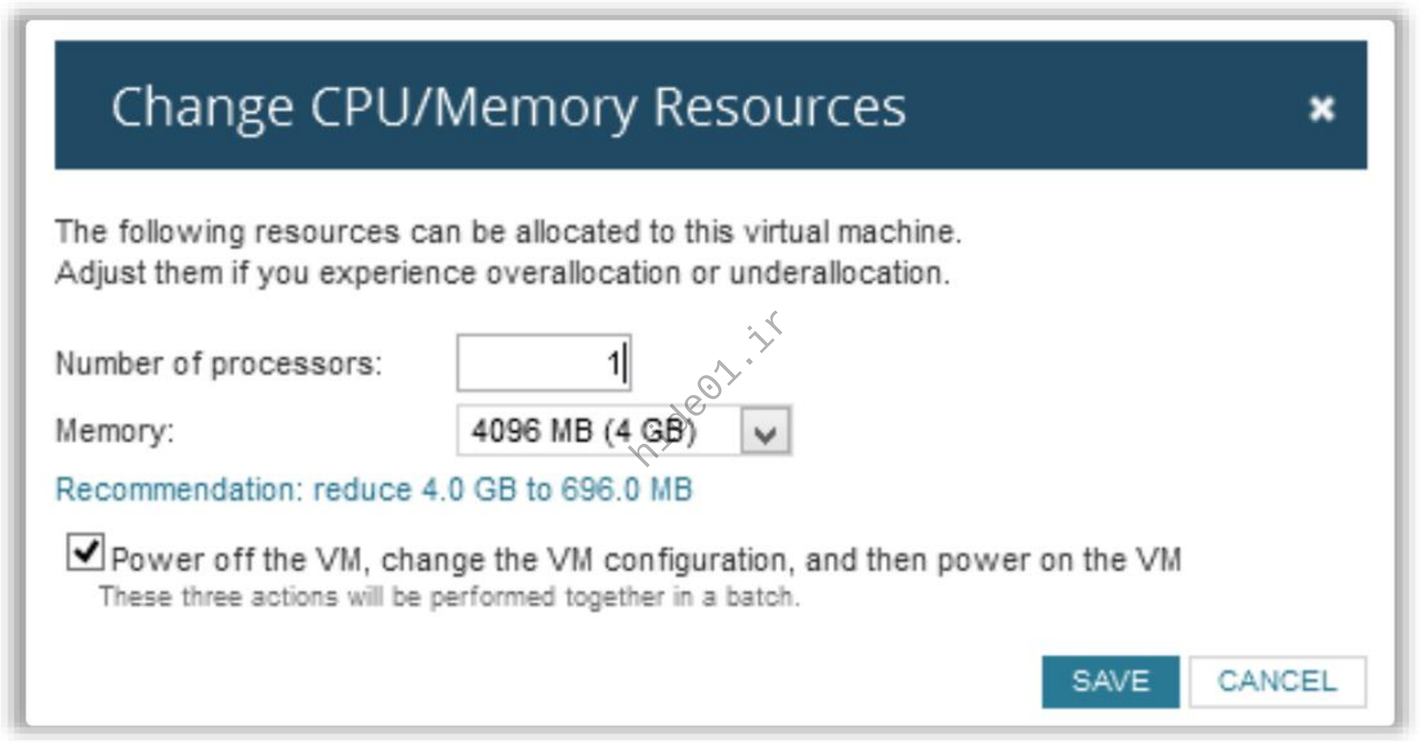


Figure 5.6: Change CPU/Memory Resources

- Select **1024 MB (1 GB)** for the **Memory** field and click **Save**.

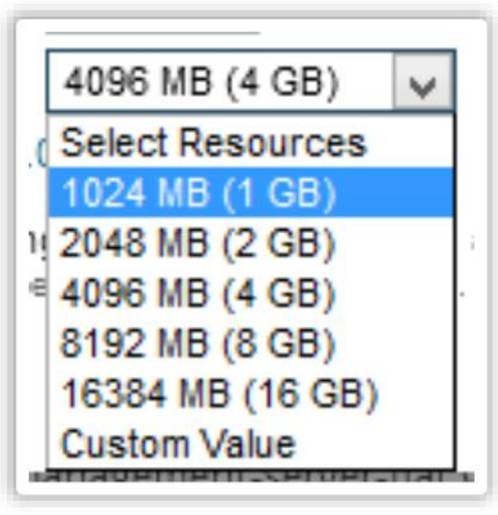
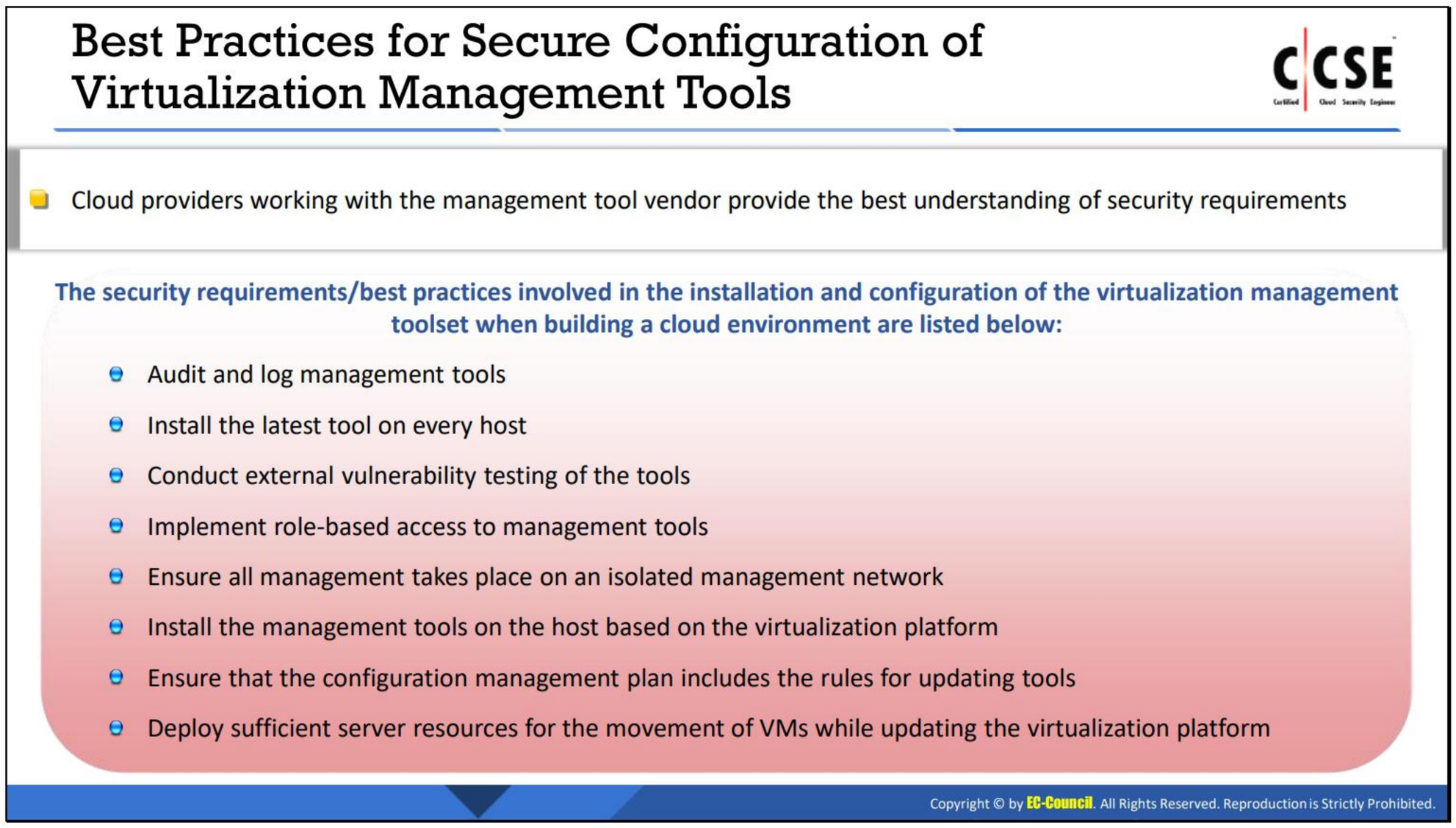


Figure 5.7: Select Memory

The Sprawl dashboard updates with the under- and over-allocated systems after the next polling. Allocate the released resources to other VMs on the hosts.

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

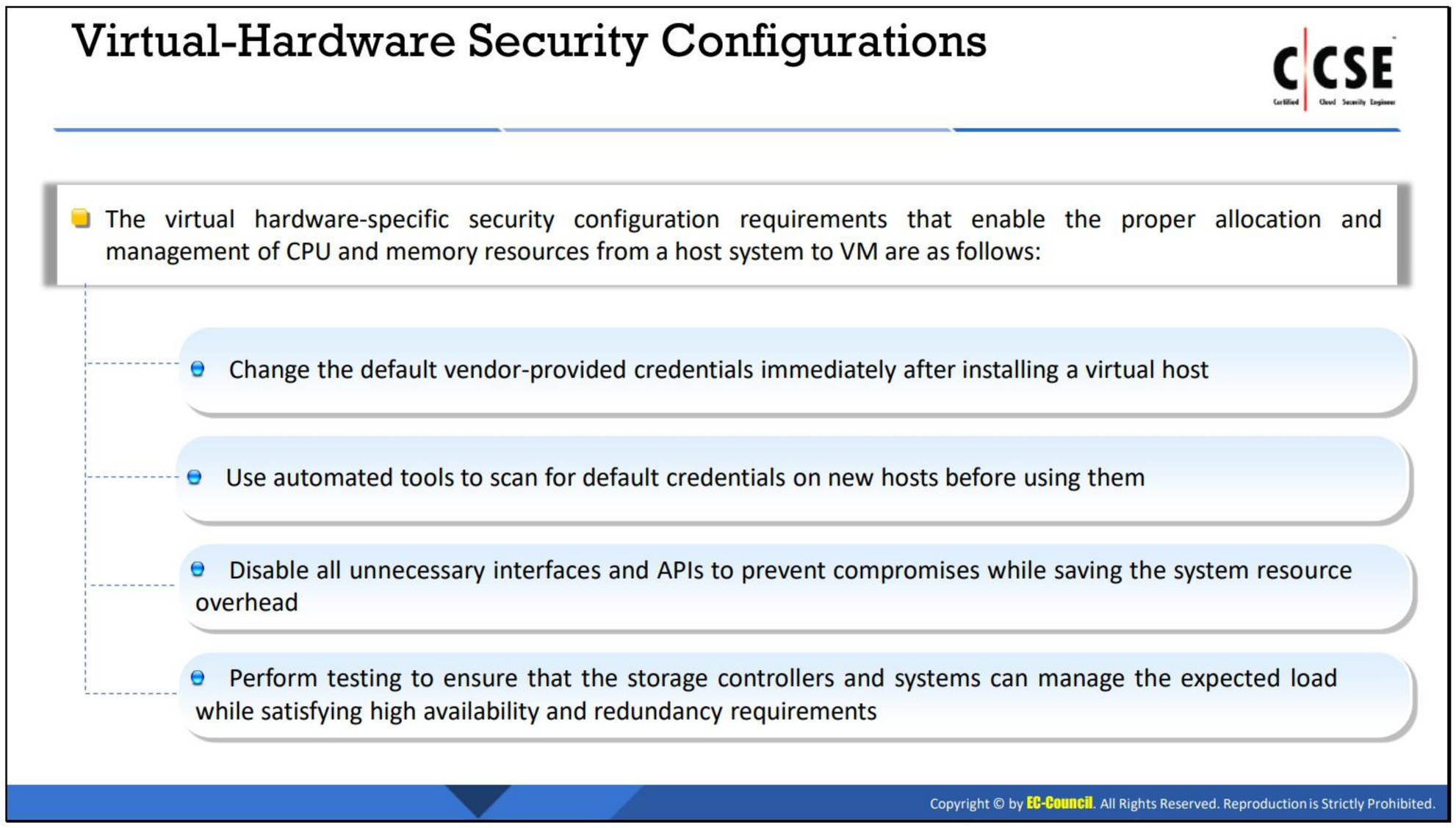


Best Practices for Secure Configuration of Virtualization Management Tools

There are various virtualization management tools, and each vendor has specific guidelines to secure their implementation. The cloud provider working with the management tool vendor provides the best understanding of security requirements. Attackers may compromise management tools and try to get unlimited access to hosts, VMs, and the cloud network. Install and configure the virtualization management toolset securely when building a cloud environment and monitor them later.

- Ensure all management takes place on an isolated management network.
- Install management tools on the host based on the virtualization platform.
- Install the latest tool on every host.
- Ensure that the configuration management plan includes the rules on updating tools.
- Deploy sufficient server resources for the movement of VMs while updating the virtualization platform because updating those tools might require server downtime.
- Conduct external vulnerability testing of the tools.
- Follow the security guidance provided by the vendor while configuring and deploying management tools.
- Implement role-based access to management tools.
- Audit and log management tools.
- Understand the management tools provided by the vendor and how to install and configure them securely based on system configuration.

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



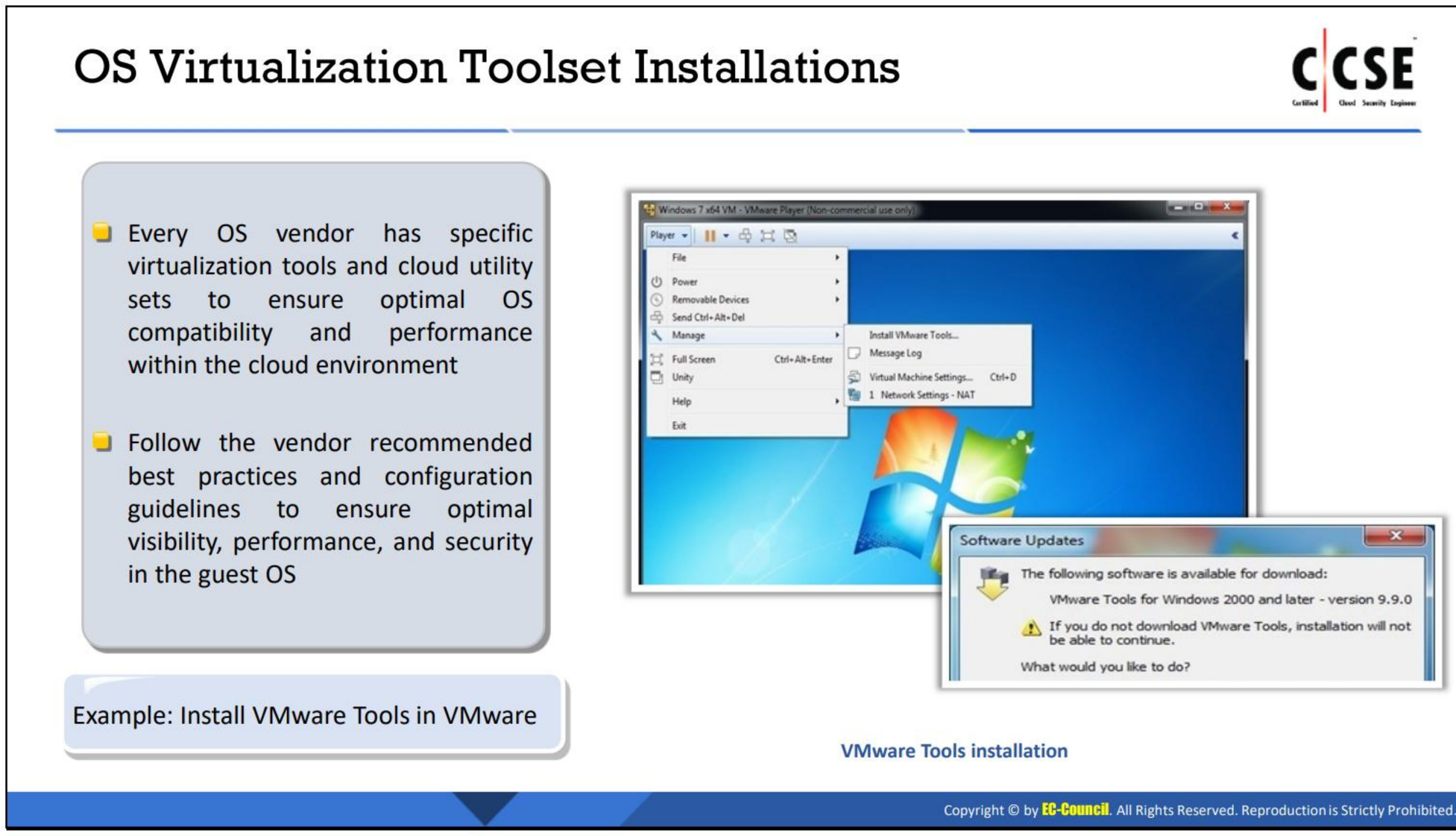
Virtual-Hardware Security Configurations

Virtual hardware-specific security configuration requirements enable the proper allocation and management of CPU and memory resources from a host system to a VM that runs on the host. These specific settings and configurations on VMs should match the physical hardware/host requirements and capabilities. The requirements of the underlying host systems should be known while configuring virtual hardware in a cloud data center. Virtual host vendors articulate these requirements. Later, the requirements are matched by those building and configuring images for virtual devices.

For storage-side secure configuration,

- Change the default vendor-provided credentials immediately after installing a virtual host because attackers could obtain the default credentials to compromise a system.
- Use automated tools to scan for default credentials on new hosts before using them and ensure continuous vulnerability assessments.
- Disable all unnecessary interfaces and APIs to prevent compromises while saving system resource overhead.
- Perform testing to ensure that the storage controllers and systems can manage the expected load while meeting high availability and redundancy requirements.

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



VMware Tools installation

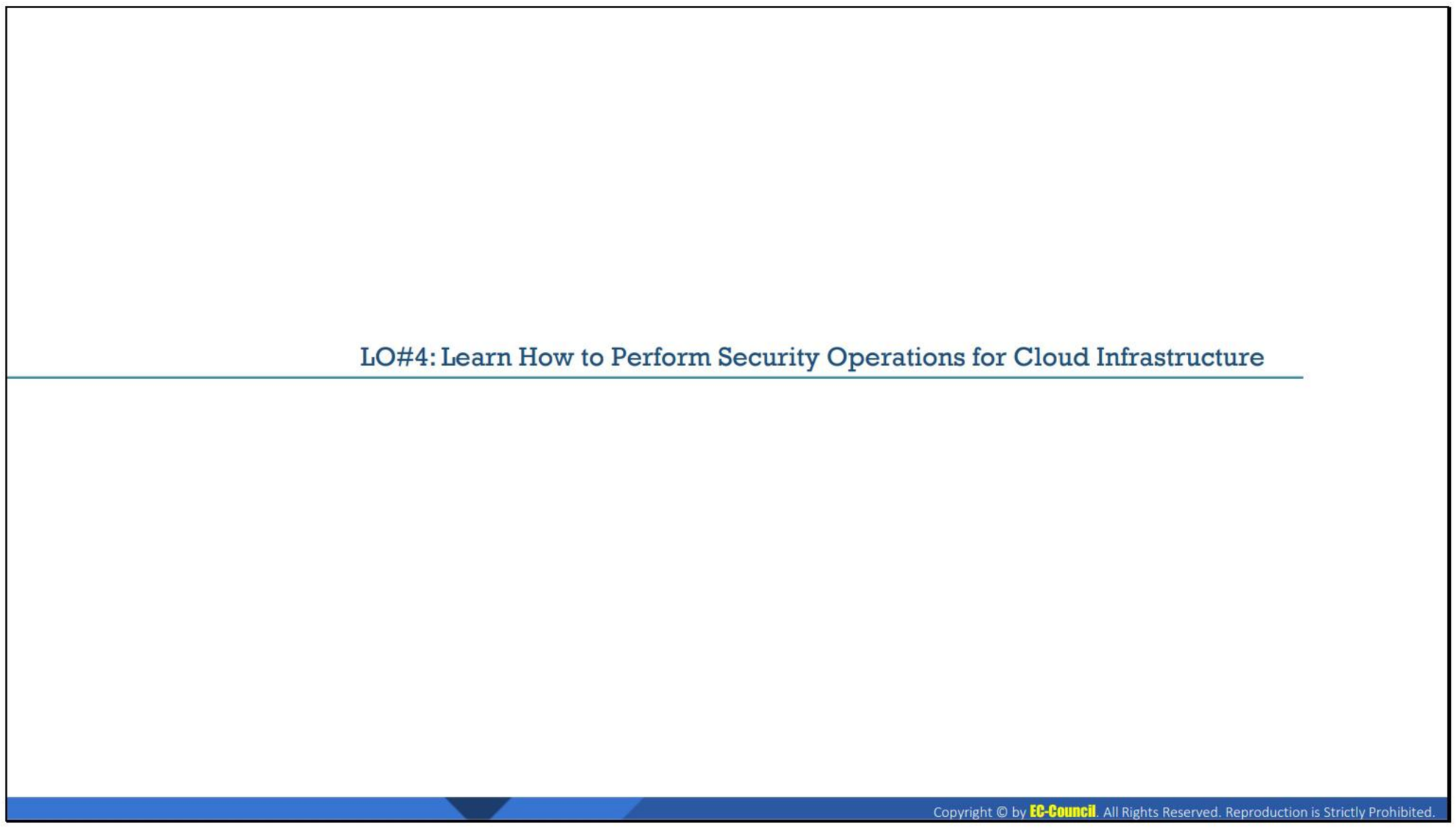
OS Virtualization Toolset Installations

Cloud virtualized environments run different OSes. Appropriate toolsets should be installed for these environments. Each OS vendor has specific virtualization tools and cloud utility sets to ensure optimal OS compatibility and performance within the cloud environment. Follow the best practices and configuration guidelines recommended by the vendor to ensure optimal visibility, performance, and security for the guest OS.

Generally, installing a guest OS virtualization toolset can eliminate/improve the following issues:

- Restricted movement of the mouse
- Inadequate color depth
- Missing sound
- Low video resolution
- Unable to copy and paste files
- Unable to drag-and-drop files
- Incorrect display of network speed

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

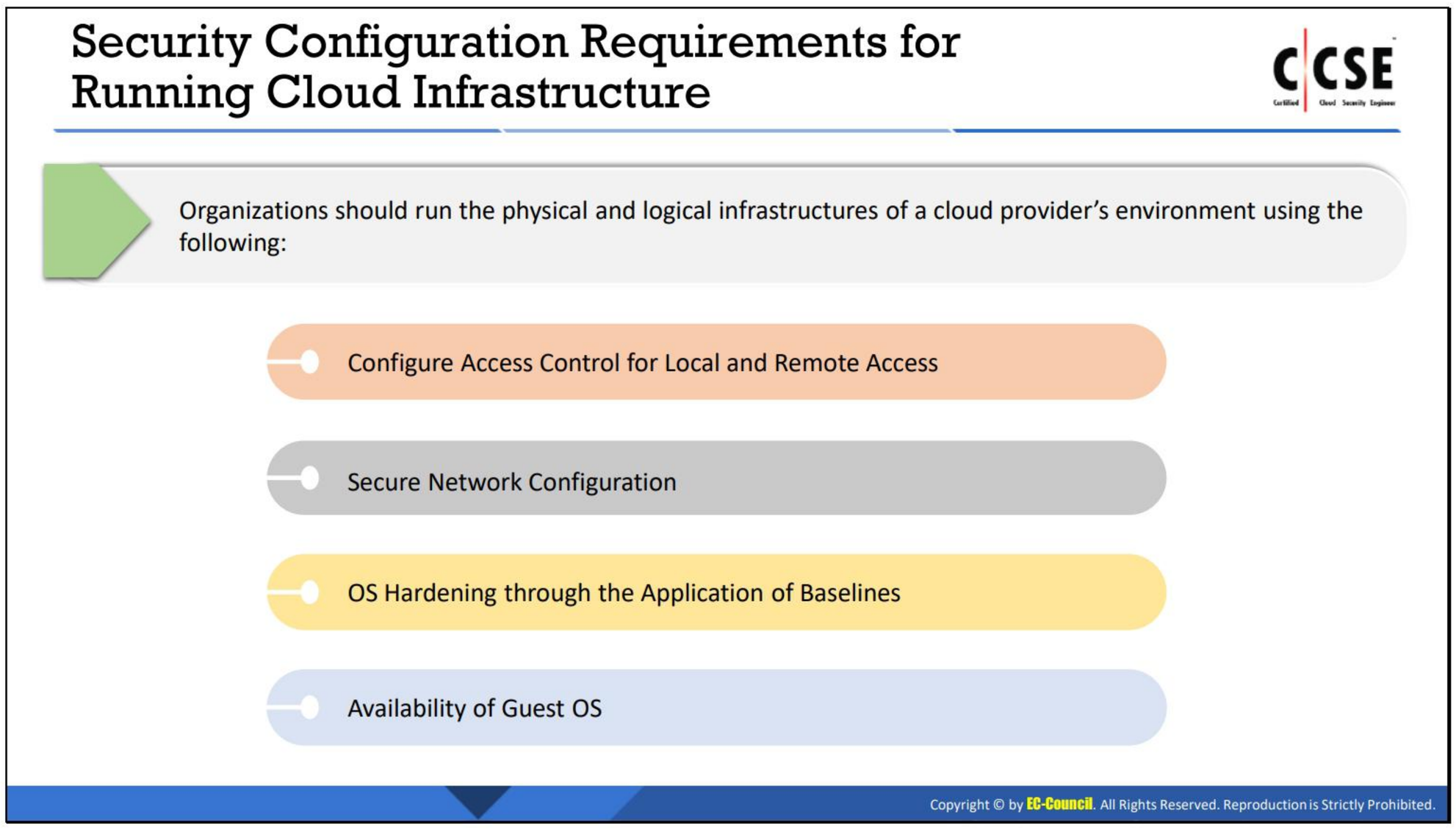


LO#4: Learn How to Perform Security Operations for Cloud Infrastructure

The objective of this section is to demonstrate how to operate the physical and logical infrastructure of a cloud environment. This section focuses on the security considerations of configuring access control for local and remote access, secure network configuration, operation system hardening through the application of baselines, and achieving high availability in the cloud. In this section, cloud security engineers will learn to operate securely in a cloud environment.

hide01.ir

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



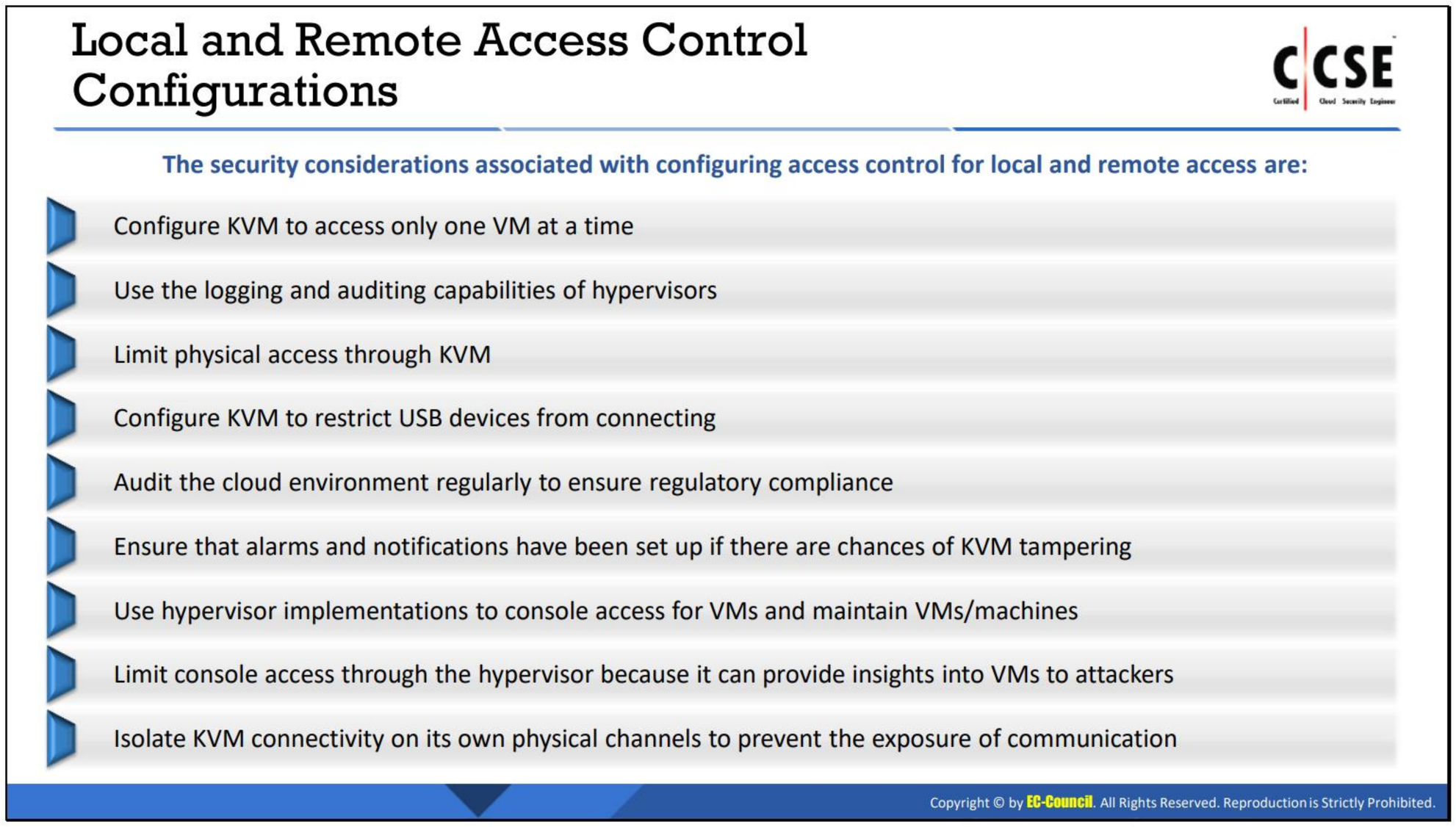
Security Configuration Requirements for Running Cloud Infrastructure

Organizations should run the physical and logical infrastructure of a cloud provider environment using the following:

hade01.ir

- **Configure Access Control for Local and Remote Access**
- **Secure Network Configuration**
- **OS Hardening Through the Application of Baselines**
- **Availability of Guest OS**

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



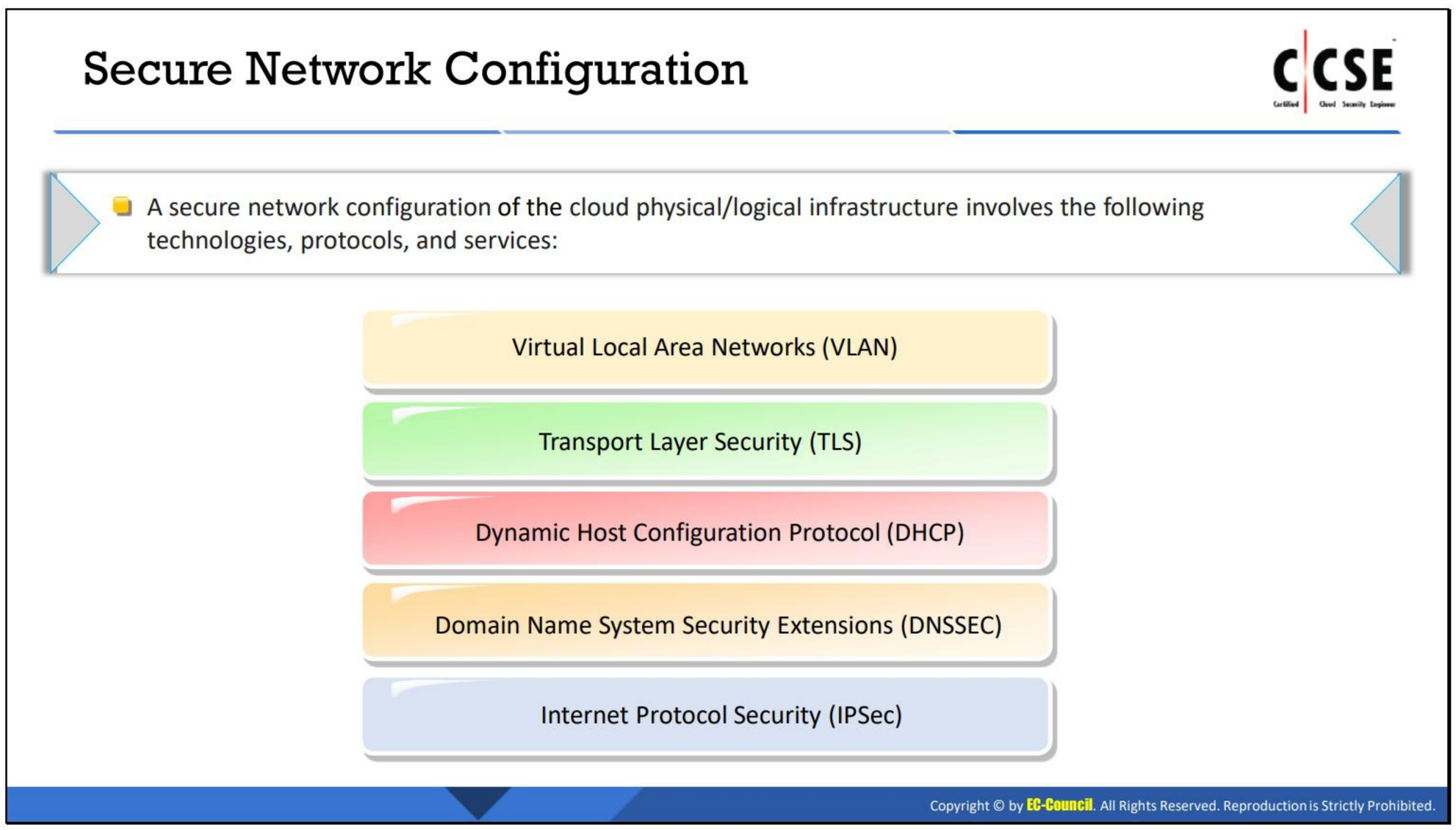
Local and Remote Access Control Configurations

In a cloud data center, access control generally focuses on the VMs and the underlying infrastructure and components of the data center. Limiting the physical access to hardware in a cloud data center includes personnel access to data centers, where the physical servers and other hardware are installed, and to hardware components through the terminal.

The security considerations of configuring access control for local and remote access include

- Limiting physical access through KVM
- Isolating KVM connectivity on its physical channels to prevent exposure of communication
- Ensure that alarms and notifications are set up if there are chances of tampering KVM
- Configure KVM to access only one VM at a time
- Configure KVM to not allow USB devices from connecting
- Use multi-factor authentication (MFA) regardless of the type of local access used
- Use hypervisor implementations to provide console access for VMs and maintain VMs/machines in the event of crash/troubleshooting
- Limit console access through the hypervisor because it can provide insights into VMs to attackers
- Use the logging and auditing capabilities of hypervisors
- Audit the cloud environment regularly to ensure regulatory compliance of the environment and privileged user access
- Use remote desktop protocol (RDP) to control, audit, and log the remote access

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



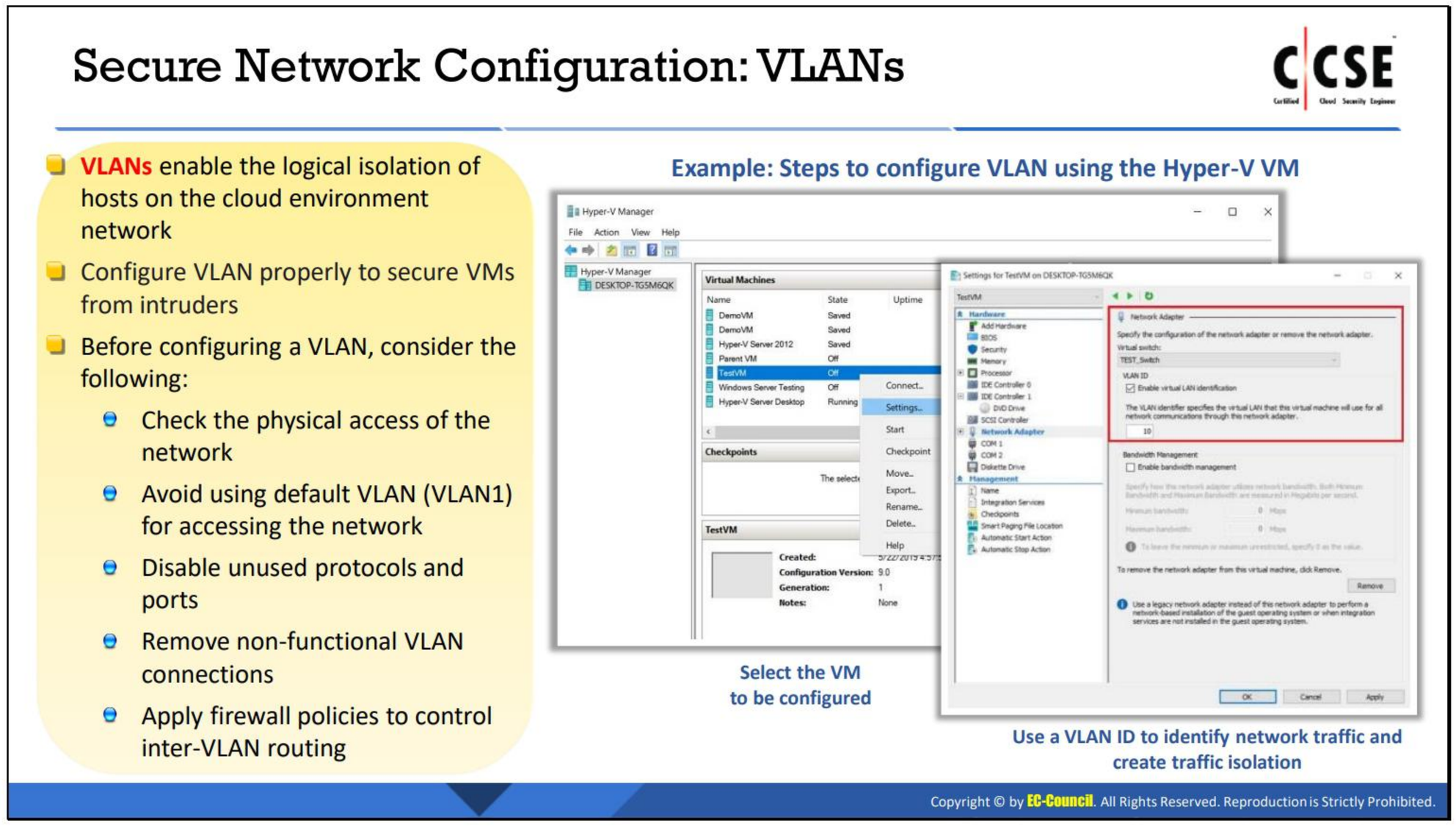
Secure Network Configuration

A secure network configuration involves the following technologies, protocols, and services:

- **Virtual Local Area Networks**
- **Transport Layer Security**
- **Dynamic Host Configuration Protocol**
- **Domain Name System Security Extensions**
- **Internet Protocol Security**

hide01.ir

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



Secure Network Configuration: VLANs

A LAN is a collection of devices connected to a server within an area via a communication line. **Virtual Local Area Network (VLAN)** allows the logical isolation of hosts on the network in a cloud environment. VLANs are logical groupings of workstations, servers, and other network devices that behave like they are on a single and isolated LAN. The purpose of VLAN is to create a simple network with improved security and better traffic management. VLAN allows combining systems on separate local networks into a VLAN, spanning corporate network segments.

Use VLAN to implement physical network isolation in a cloud environment. A VLAN operates like a physical LAN and groups the hosts that are not connected to the same switch. Configure VLAN properly to secure VMs from intruders. Configure VLAN through multiple approaches such as MAC address, port assignment, protocols, and IP subnets.

VLAN offers the following benefits:

- VLAN allows segmentation and helps in reducing issues related to network management and scalability.
- It saves cost because devices within a VLAN do not require routers to communicate with each another.
- VLAN facilitates the creation of flexible network designs and provides better flexibility.
- Less administrative maintenance is required to manage VLANs.
- VLAN minimizes latency and traffic load on the network and maximizes performance.

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

How VLAN configuration works

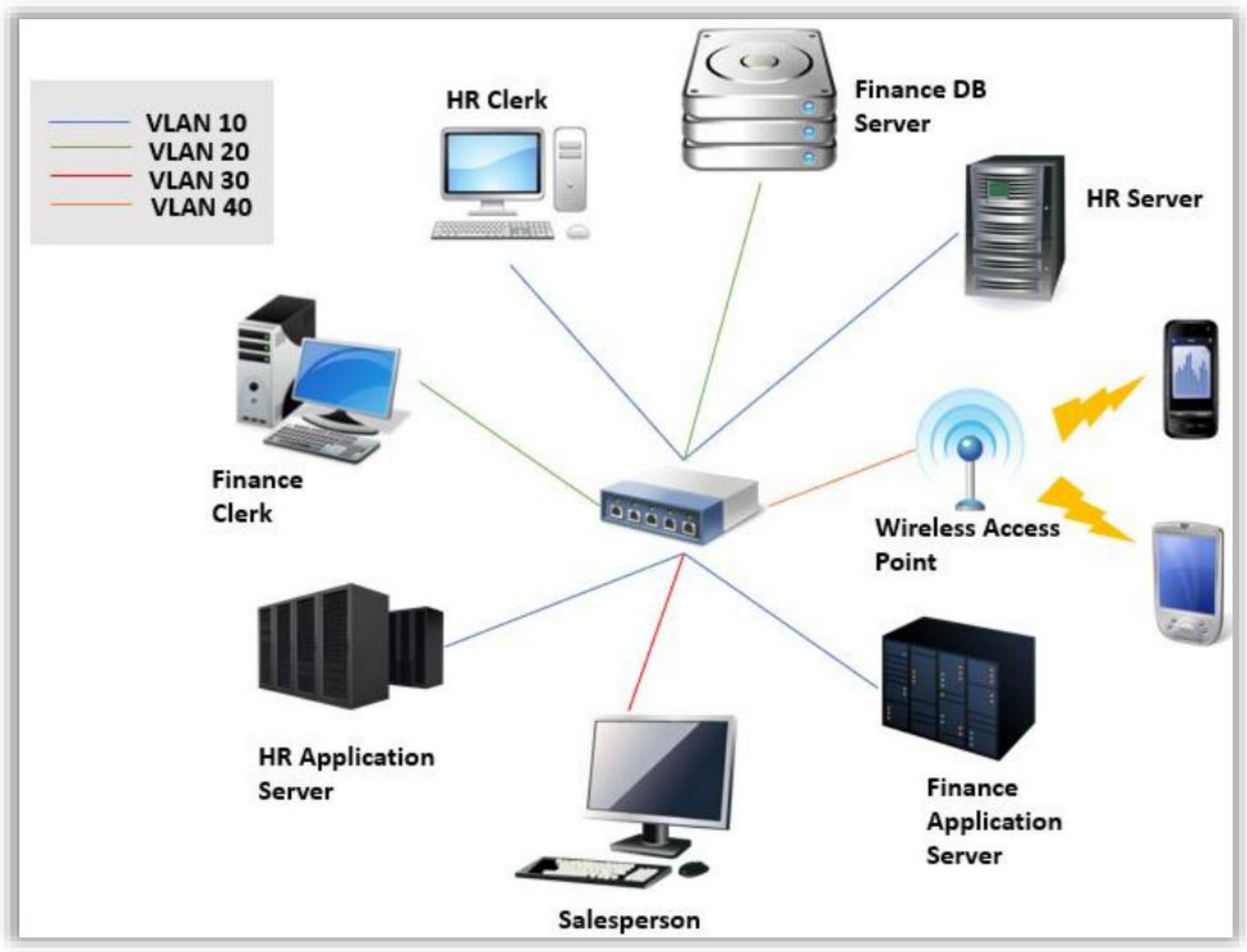


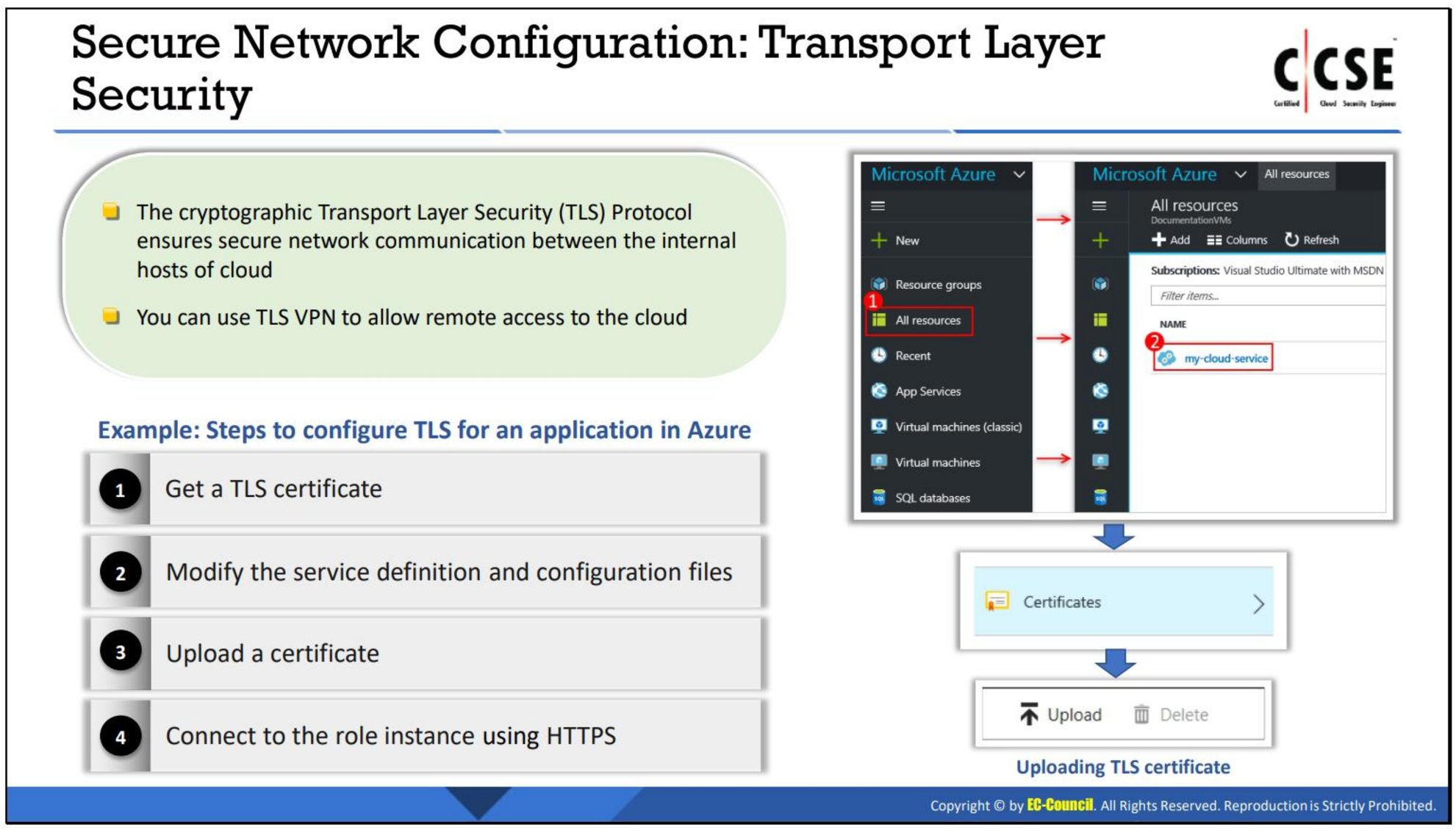
Figure 5.8: Basic VLAN Configuration

As shown in the above image, all HR servers and the HR clerk are assigned to some switch ports configured as VLAN 10. Devices connected to these VLAN ports can freely communicate with each other but they cannot communicate with devices that are not a part of that VLAN. In this example, the salesperson's computer is on another VLAN (VLAN 30), thus not allowing communication with the HR clerk's computer because they both belong to different VLANs.

Check the below points before configuring a VLAN network.

- Check the physical access of the network
- Avoid using default VLAN (VLAN1) for accessing the network
- Disable unused protocols and ports
- Remove the VLAN connections not being used
- Apply firewall policies to control inter-VLAN routing

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



Secure Network Configuration: Transport Layer Security

The cryptographic protocol, transport layer protocol (TLS), is responsible for secure network communication between cloud hosts. TLS uses X.509 certificates issued by the Certificate Authority (CA) for communication authentication and encryption between hosts. Implementing TLS for internal networks can prevent traffic sniffing and provide confidentiality and integrity of information. It can provide security for e-mail communication, voice over IP (VoIP) communication, web traffic, messaging clients, file transfers, internet services (domain name service, and network time protocol (NTP)), among other. Cloud customers can use TLS VPN to allow remote access to the cloud environment.

TLS has two different layers.

- **TLS Handshake Protocol**: This protocol initially attempts to establish a TLS connection between hosts or any two parties in the cloud environment. Later, it enables a secure communication channel to handle data transmission. This protocol works before data transmission. To establish secure communication, TLS uses key exchange and Session ID for communication between hosts. At this stage, TLS uses certificates (for example, X.509) to authenticate and establish a connection between hosts. Here, the encryption algorithms are negotiated.
- **TLS Record Protocol:** This protocol works once communication is established by the TLS handshake protocol. It is the actual protocol that can secure data transmission. It is responsible for data authentication and encryption throughout data transmission between hosts.

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

Steps to configure TLS in Azure cloud:

Source: www.microsoft.com

Note: Assume that cloud services are already created and deployed in Azure.

- Login to **Azure portal**.

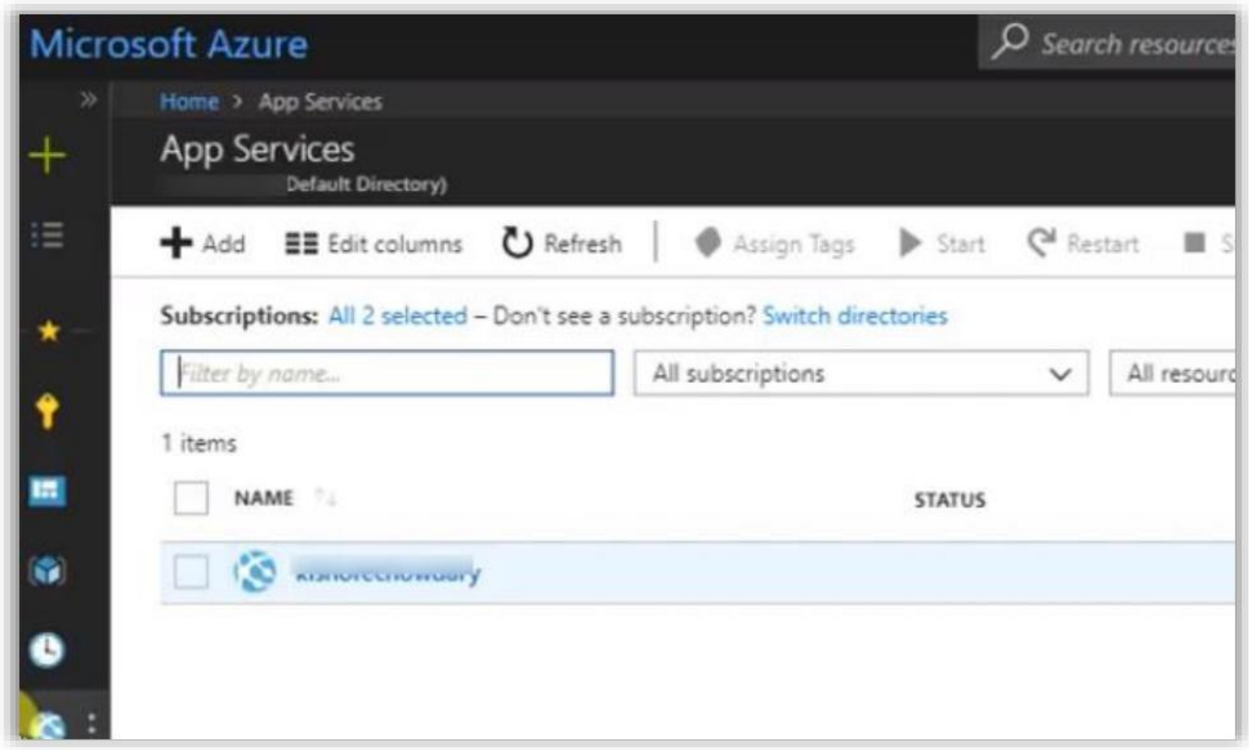


Figure 5.9: Azure Portal

- Click on **All Resources** and select the cloud service.

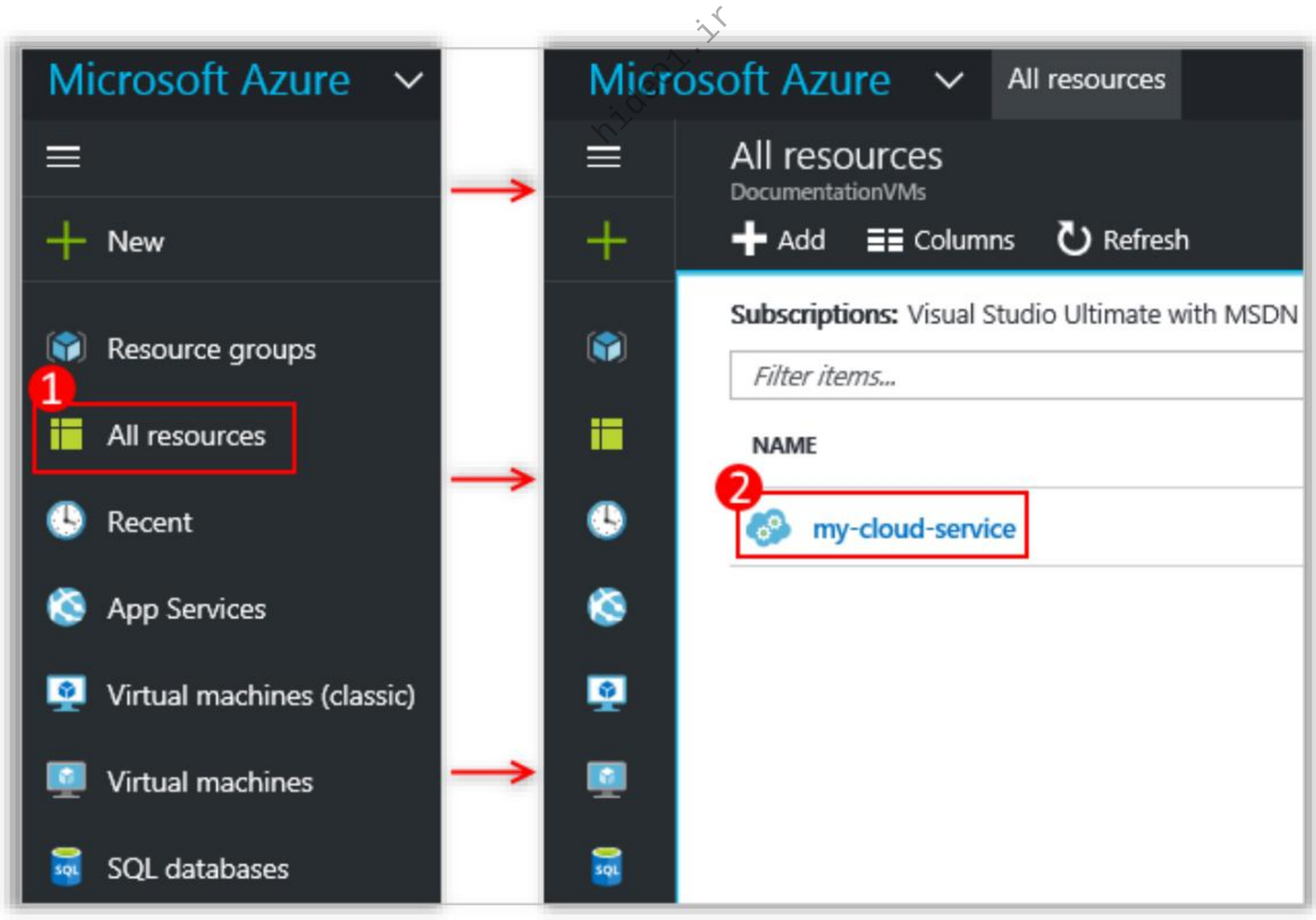


Figure 5.10: All Resources

- Scroll down the left side pane and click on **SSL settings**; then, the SSL configuration page appears.

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

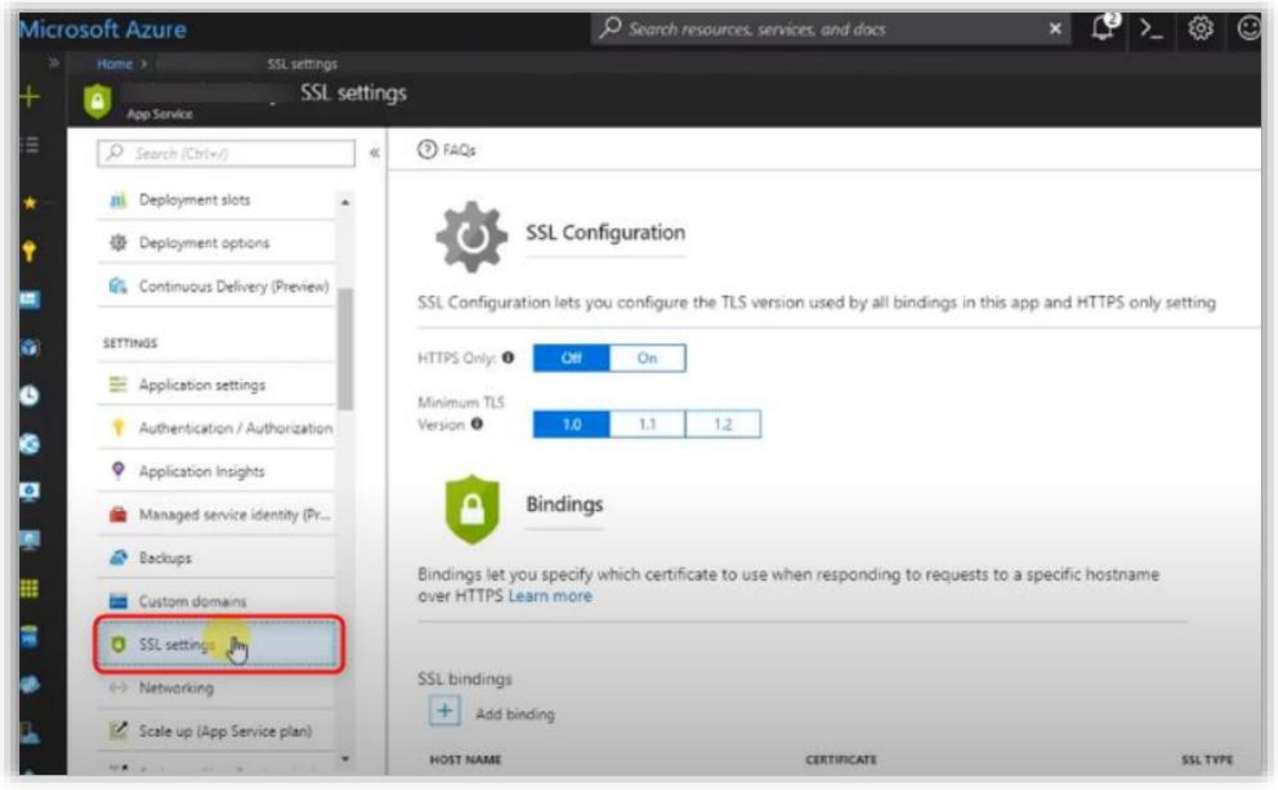


Figure 5.11: SSL Settings

- Scroll down the page, click on **Upload Certificate**.

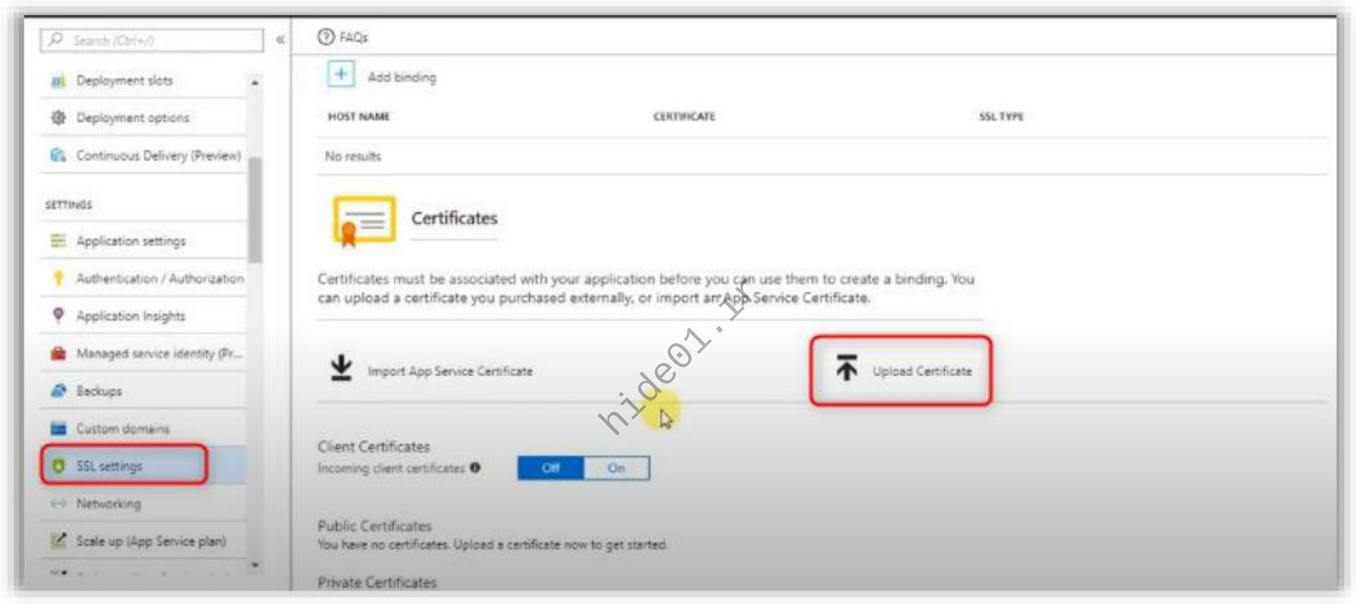


Figure 5.12: Upload Certificate

- Choose **Private** or **Public** as the type and select certificate in the .pfx format file.

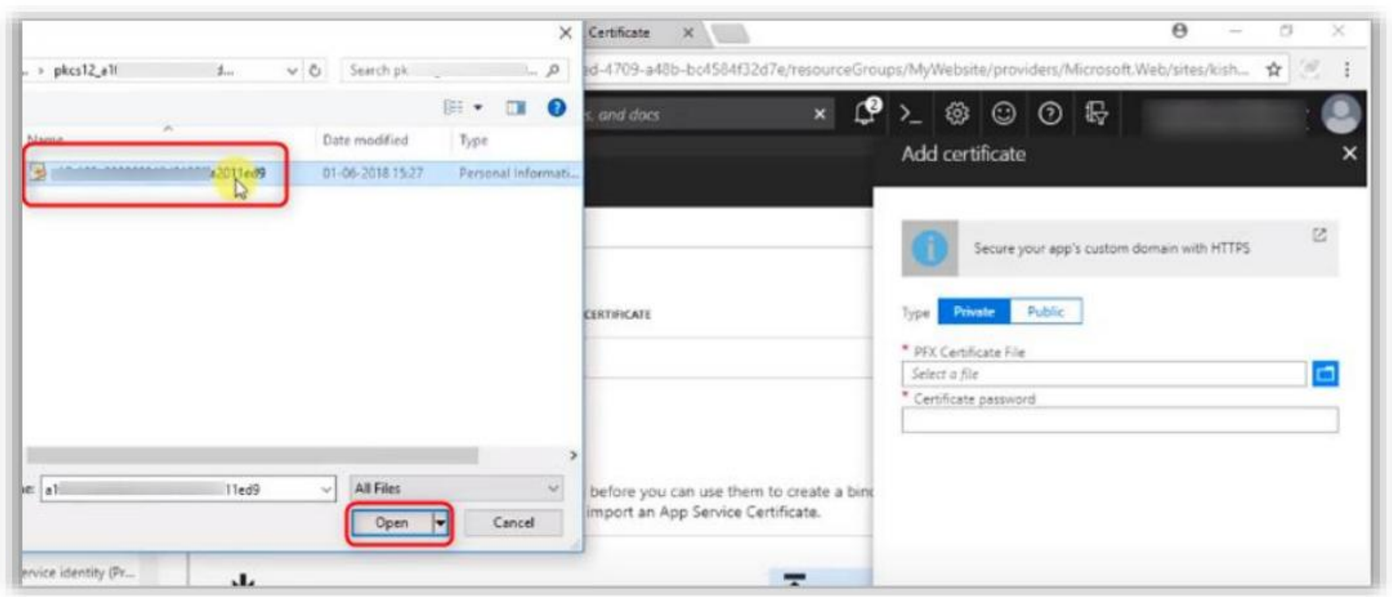


Figure 5.13: Choose Type & Select Certificate

- Type the certificate password and click **Upload**.

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

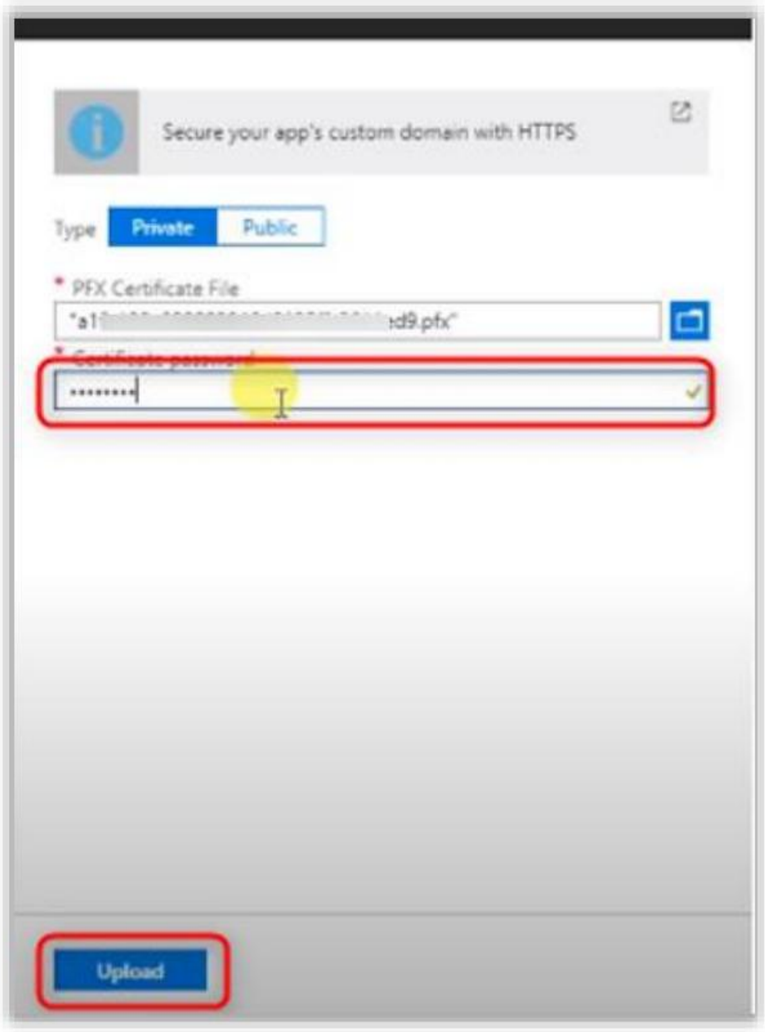


Figure 5.14: Upload

- A message stating that the certificate has been uploaded successfully appears.

Figure 5.15: Uploaded

- Click **+Add binding** under the **SSL bindings** section.

Figure 5.16: Add Binding

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

- The **Add SSL Bindings** pane appears. Select **Hostname**, **Certificate**, and **SSL Type**. Click on **Add Binding**.

Figure 5.17: SSL Bindings

- You can see the added certificate in the notification.

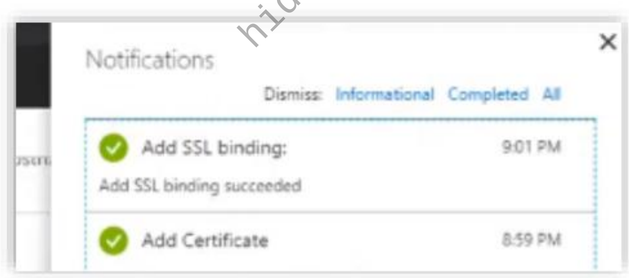
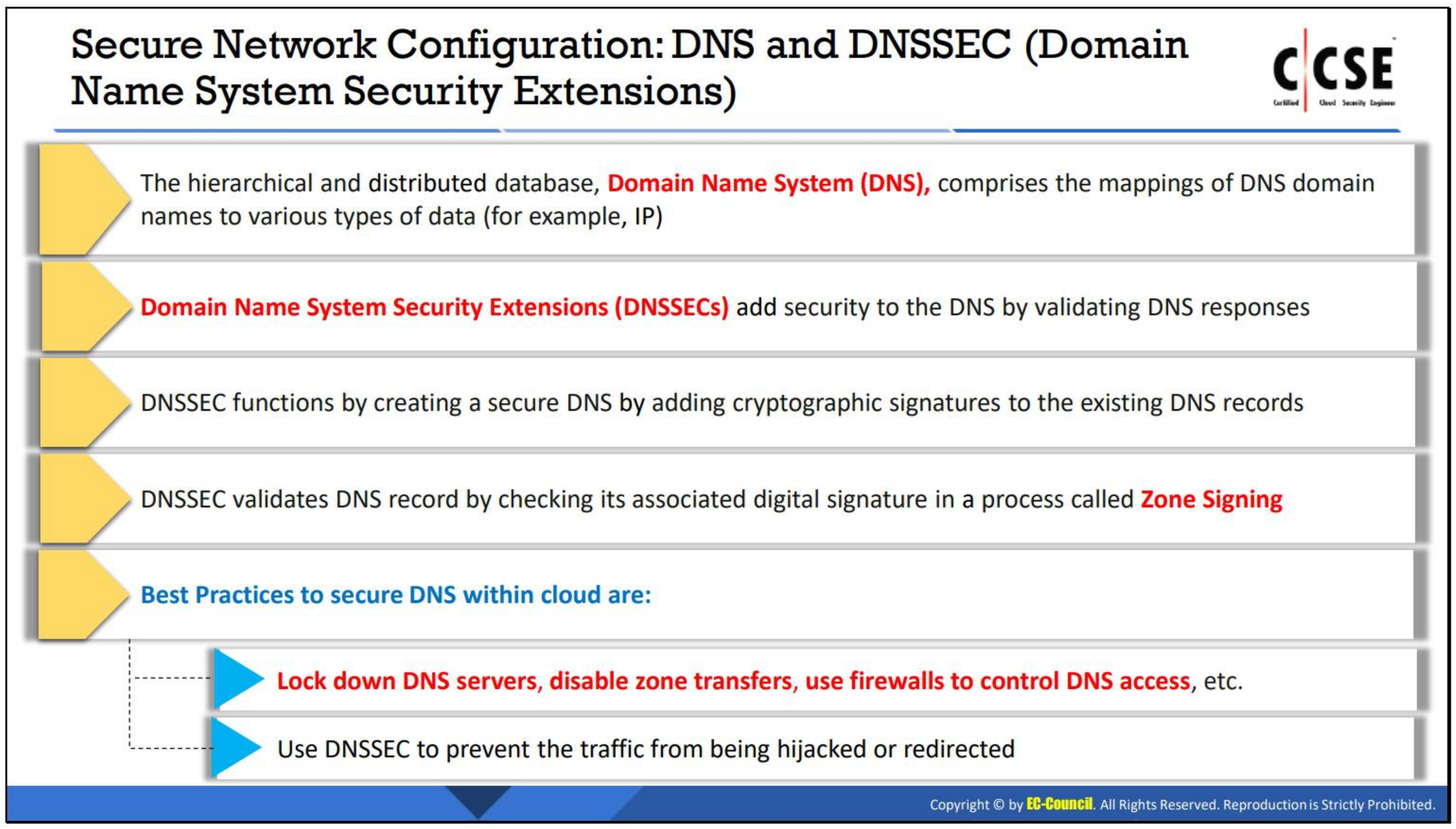


Figure 5.18: Notification

- Now you can access the application with SSL configuration.

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



Secure Network Configuration: DNS and DNSSEC (Domain Name System Security Extensions)

The hierarchical and distributed database, **Domain Name System (DNS),** comprises the mappings of DNS domain names to various types of data (e.g., IP). The internet cannot function in the absence of DNS because web browsers only use IP addresses to access any device or website. DNS can be useful for routing messages to web-mail services and e-mail servers, peer-to-peer sharing programs, or connecting IoT devices.

Domain Name System Security Extensions (DNSSEC) add security to the DNS by validating DNS responses. It is a secure implementation of DNS because it ensures the trust and integrity of DNS records via cryptographic signatures. DNSSEC ensures that DNS records are only obtained from authenticated servers. DNSSEC does not ensure confidentiality but provides origin authority, data integrity, and authenticated denial of existence.

DNSSEC functions by creating a secure DNS by adding cryptographic signatures to the existing DNS records. DNSSEC validates DNS records by checking their associated digital signature through a process called Zone Signing.

DNSSEC offers the following benefits:

- Prevents man-in-the-middle attacks
- Provides safe and secure web browsing
- Verifies the authenticity and origin of DNS requests
- Preserves data integrity

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

Best practices to secure DNS within the cloud

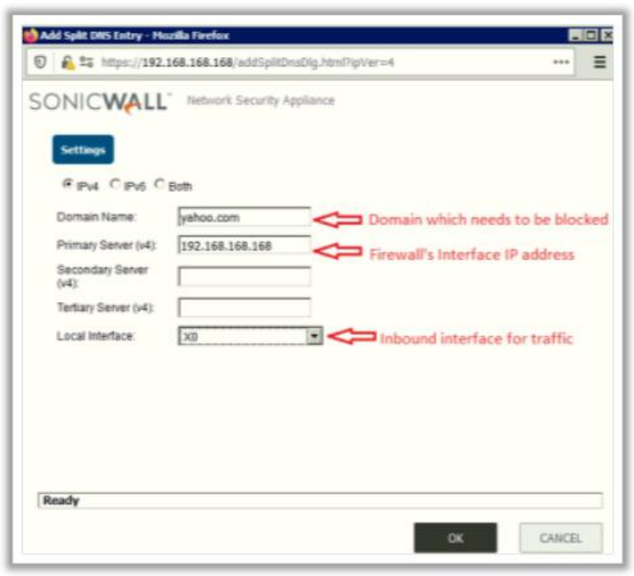
- **Lockdown DNS servers**: Ensure the security of DNS servers from the beginning by following security measures such as not changing the default settings of Active Directory-integrated DNS and securing data transfer between clients and DNS server.
- **Disable zone transfers**: Disable zone transfers to secure key infrastructure services from attackers.
- **Use firewalls to control DNS access**: Always use firewalls to control DNS access. Block connections from external hosts to DNS servers that are meant for internal client queries only.
- **Use of DNSSEC can prevent hijacking and redirection of traffic**: DNSSEC provides a secure web browsing experience by validating the authenticity and origin of DNS requests, thereby preventing hijacking and redirection of traffic.

hide01.ir

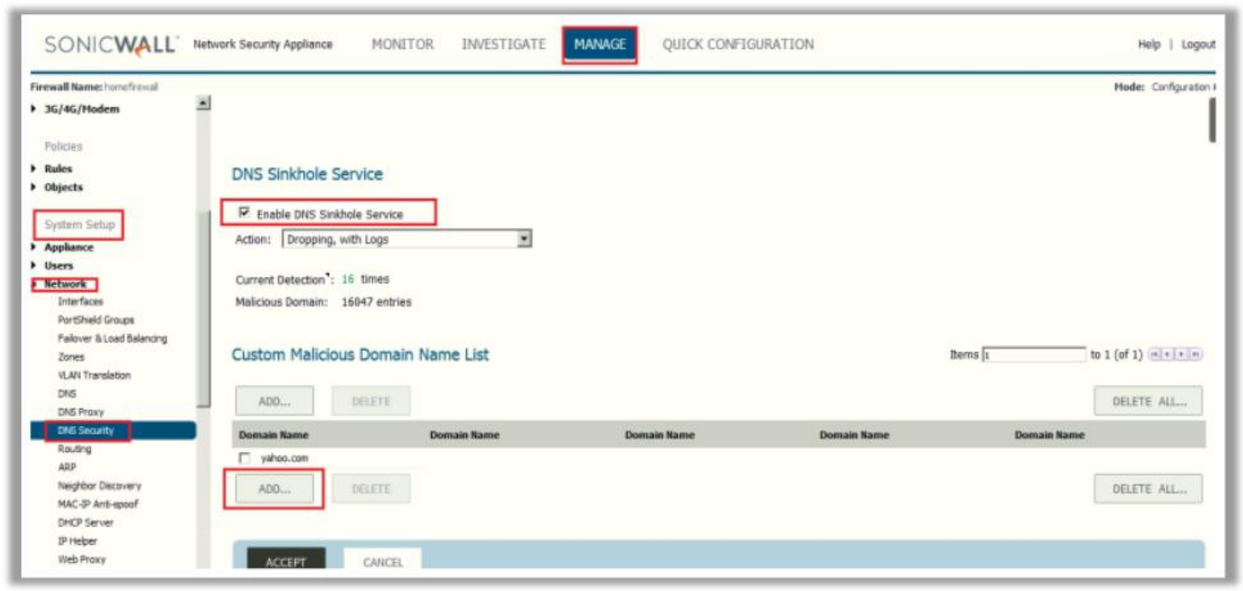
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Example: SonicWall's DNS Sinkhole to Block DNS Queries

Example: Use SonicWall's **DNS Sinkhole** feature to block DNS queries to a domain



Configure Firewall and point the DNS query for the domain towards the firewall



Enabling DNS Sinkhole and configuring it

Source: www.sonicwall.com

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

Example: SonicWall's DNS Sinkhole to Block DNS Queries

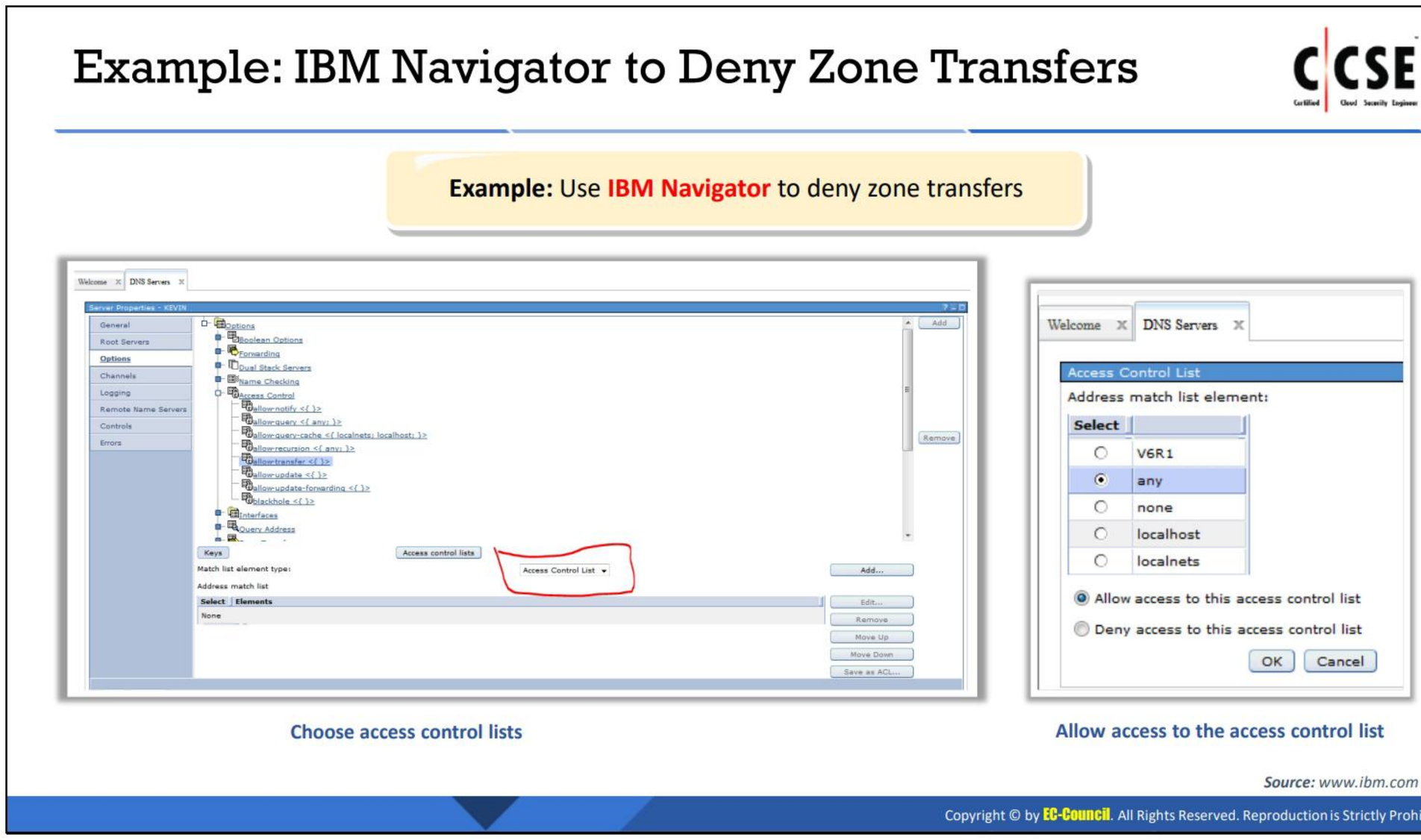
Example: Use SonicWall's DNS Sinkhole feature to block DNS queries to a domain

Source: https://www.sonicwall.com

ide01.ir

Use the Sinkhole feature of a firewall to block DNS queries to particular domains. Use split DNS tunneling to achieve this requirement. It will allow the firewall to take proper action upon receiving the DNS queries rather than forwarding them to the internal DNS server.

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



Example: IBM Navigator to Deny Zone Transfers

Example: Use IBM Navigator to deny zone transfers

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

ride01.ir

DNS zones can be transferred only for name servers designated within each zone by NS (Name Server) records. The cloud admin can restrict zone transfers for all zones to specific hosts by adjusting the restrictions.

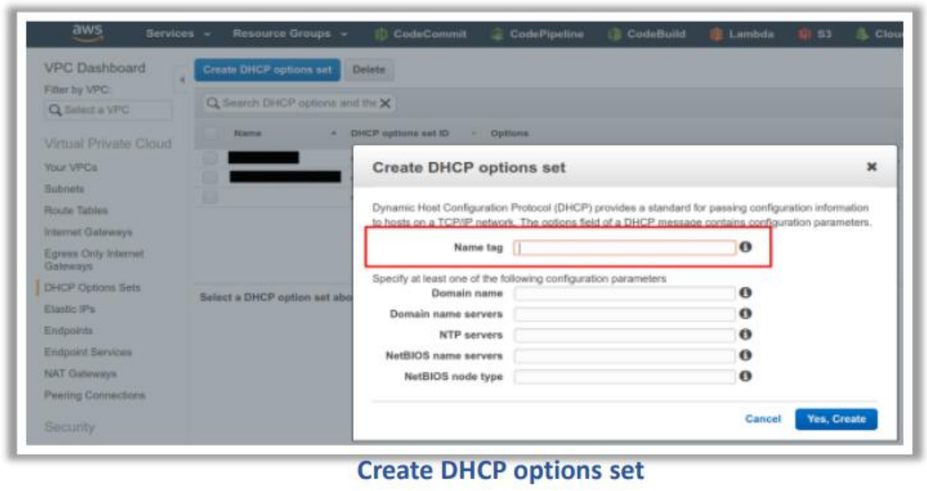
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Secure Network Configuration: Dynamic Host Configuration Protocol

- The Dynamic Host Configuration Protocol (DHCP) centralizes the assignment of IP addresses and maintains IP addresses in a static manner
- Assign configuration details such as IP, MAC address, hostname, and node names that are always assigned to VMs, thus allowing great speed and flexibility with automation and orchestration

Use the DHCP options set in AWS

- The DHCP with a standard enables configuration management to hosts on a TCP/IP network
- The **options** field refers to configuration parameters (domain name, netbios-node-type, and domain name server)
- AWS automatically creates a set of DHCP options and associates the options with the VPC when creating it (VPC)
- Organizations can determine their own DHCP options sets for their VPC



Create DHCP options set

Source: www.aws.amazon.com

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

Secure Network Configuration: Dynamic Host Configuration Protocol

Source*: https://www.aws.amazon.com*

The dynamic host configuration protocol (DHCP) distributes IP addresses to the client to configure the network. It enables assigning an IP address, subnet mask, and default gateway. While configuring the network in a cloud environment, IP addresses and other network parameters (MAC address, hostname, and node name) should be assigned to the device. Manual configuration of network parameters may reduce the network speed and flexibility in the cloud; moreover, it often conflicts with the IP address over the network.

DHCP enables automation and orchestration within the cloud. It allows to assign network parameters automatically and helps in avoiding network IP collisions. Enabling DHCP for cloud platforms allows the administration of network settings centrally and assigning IP addresses in a static manner. Here, DHCP provides great speed and flexibility with its automation and orchestration. Moreover, it removes configuration requirements (for example, network settings at the host level) because they are administered centrally.

For example, use the DHCP options set in AWS

DHCP configuration helps in setting network parameters for the host on the network. DHCP with a standard enables configuration management to host on a TCP/IP network. Here, the options field refers to configuration parameters (domain name, netbios-node-type, and domain name server). AWS automatically creates a set of DHCP options and associates them with the VPC when creating it (VPC). The organization can configure its own DHCP option sets for their VPC.

Steps to set up DHCP options set in AWS:

- Log into AWS Console. Open VPC dashboard.

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

- Select VPC from the left-side pane.

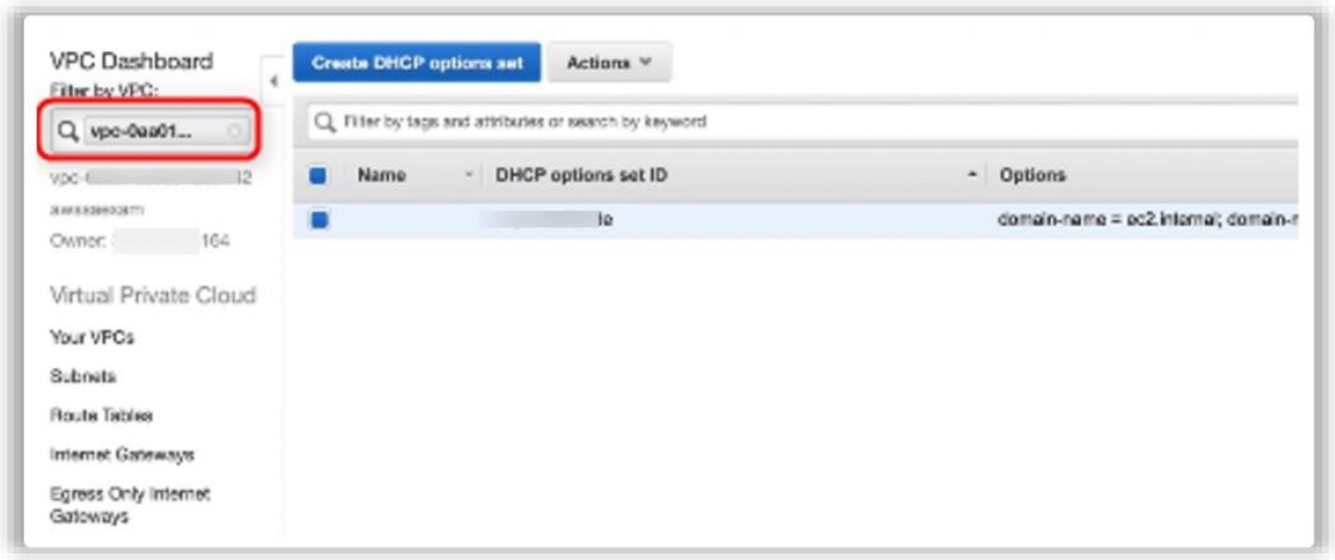
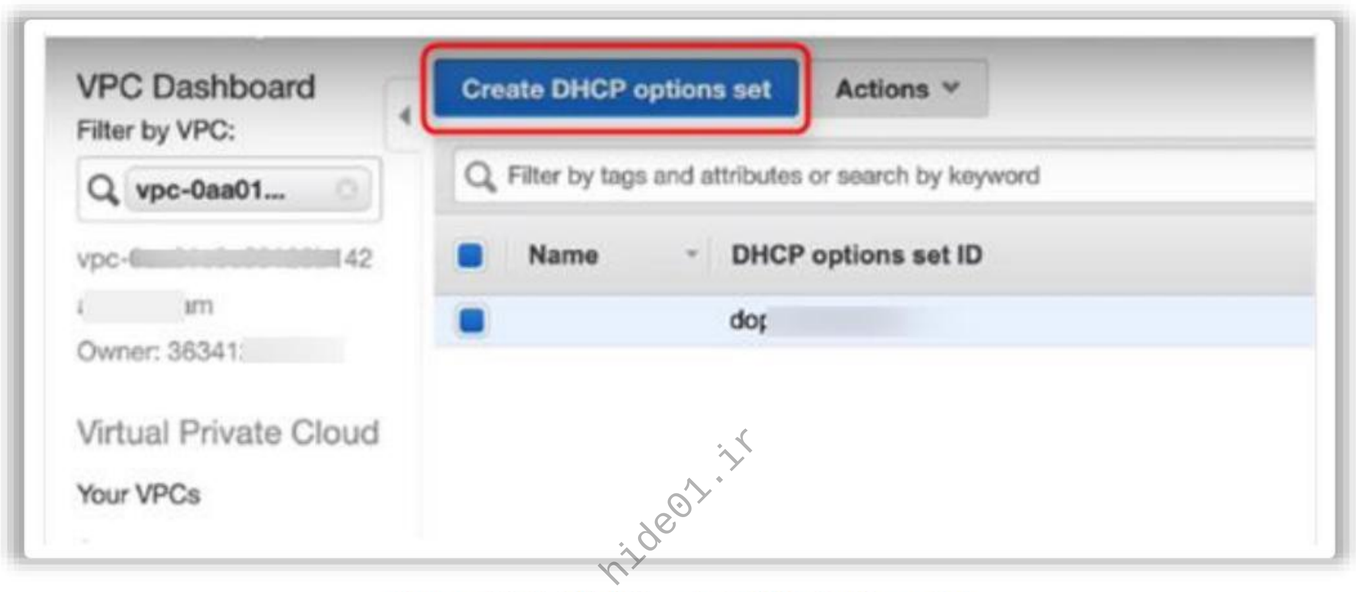


Figure 5.19: VPC

- Click **Create DHCP options set** button from the top.



hide01.ir

Figure 5.20: Click Create DHCP Options Set

- The **Create DHCP options set** page appears. Type the **Name** and **Domain Name.**

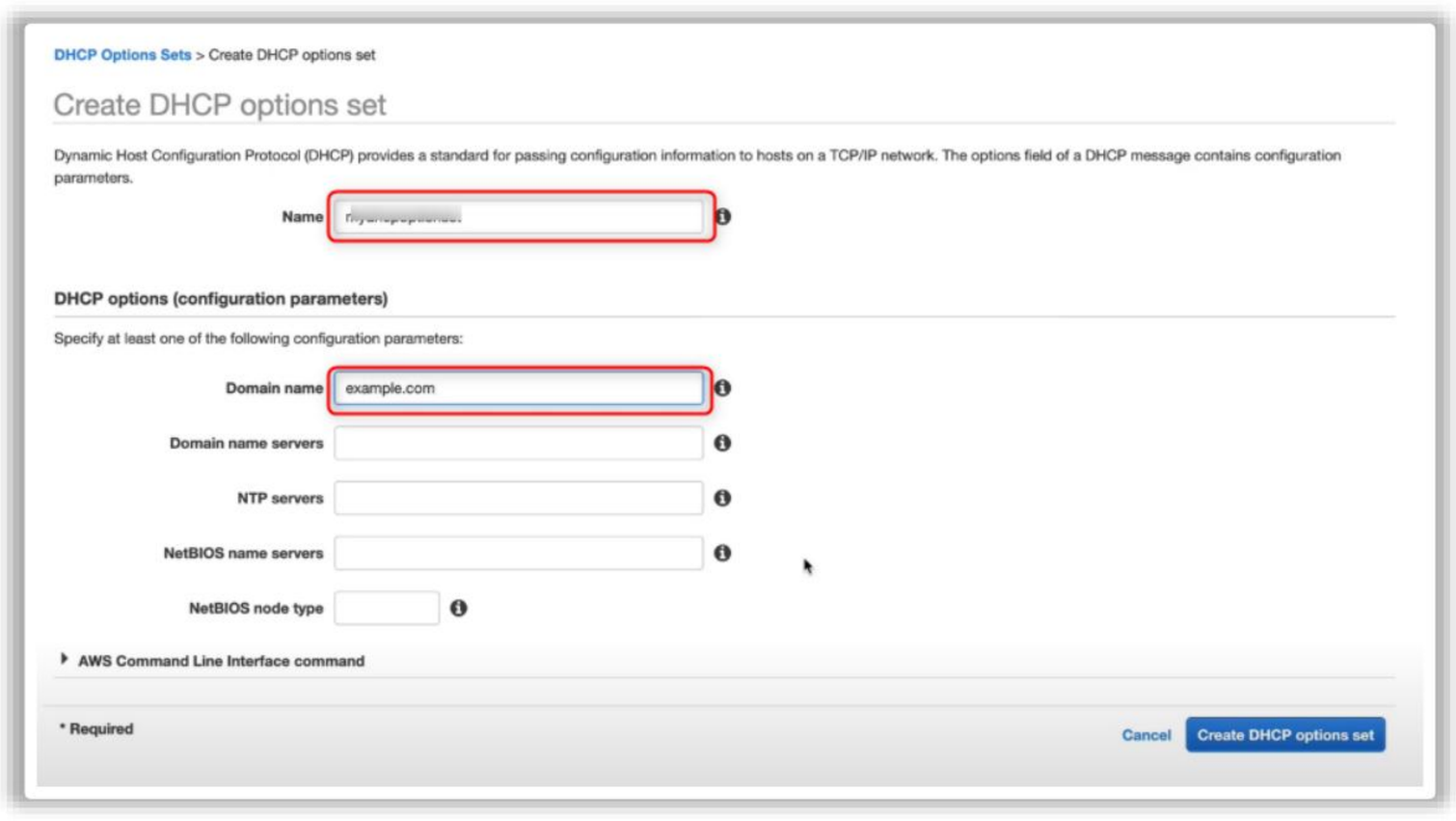


Figure 5.21: Create DHCP Options Set

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

- Click on **Create DHCP options set**. The Create DHCP options set succeeded page appears, then click on **Close**.

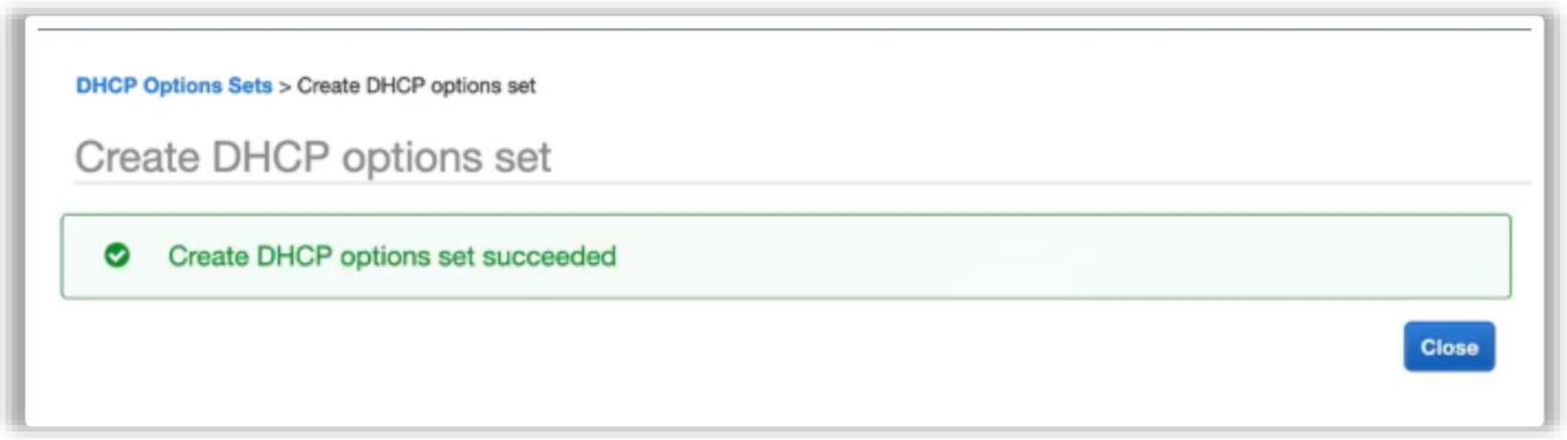


Figure 5.22: Click Close

- You can see the **DHCP options set ID** below the DHCP options set pane.

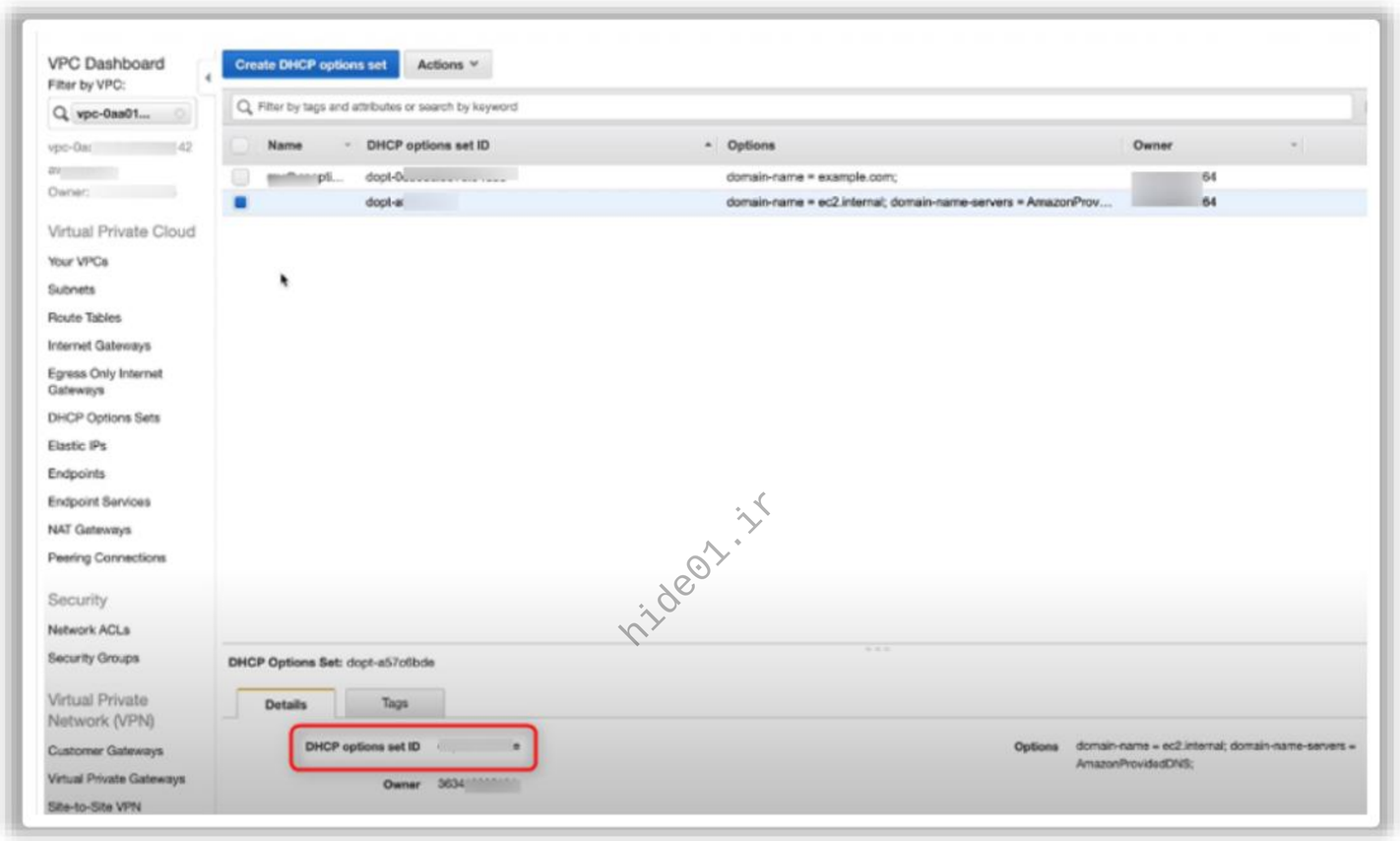
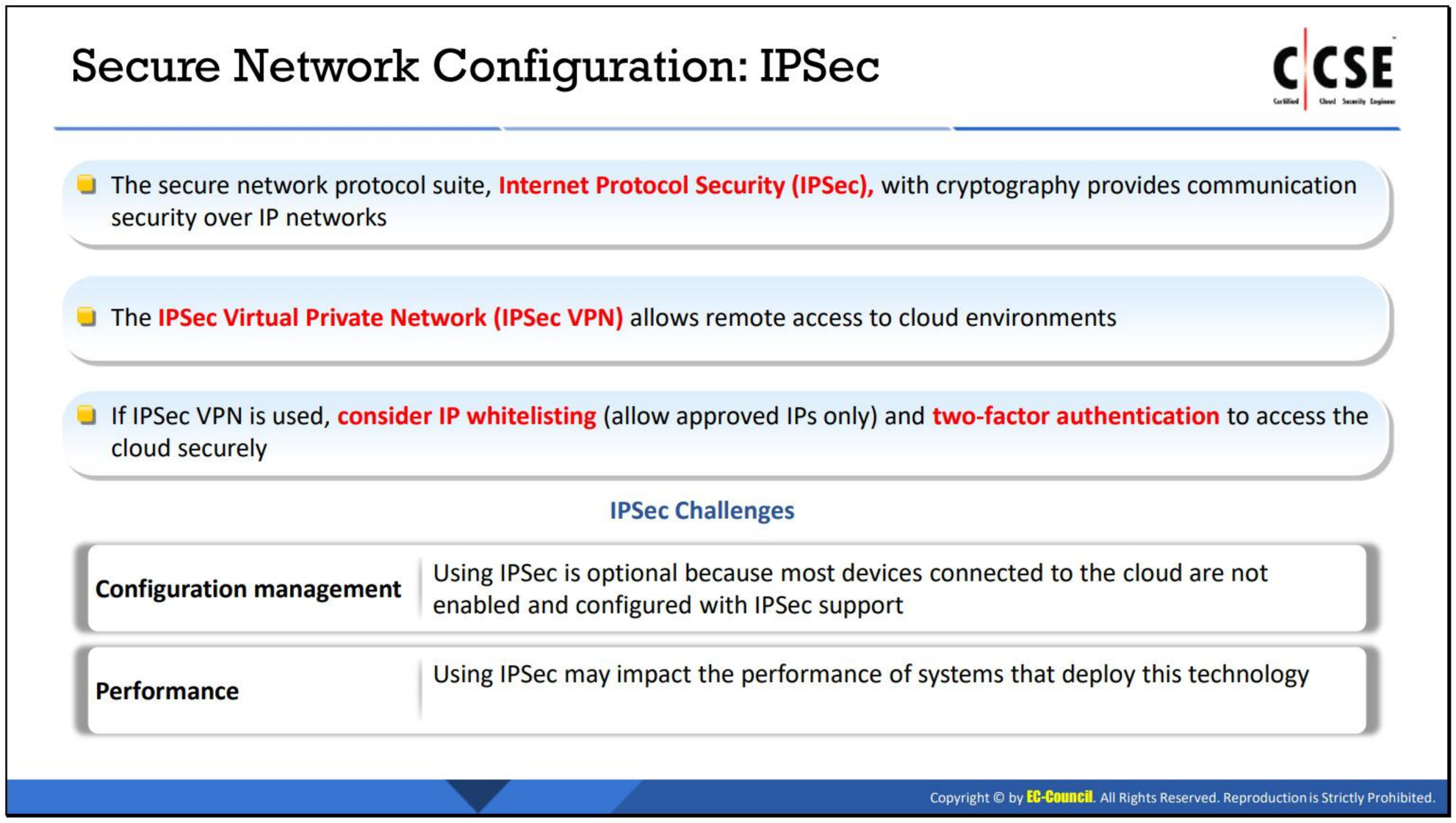


Figure 5.23: DHCP Options Set ID

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



Secure Network Configuration: IPSec

Internet Protocol Security (IPSec) is a protocol that provides network-level peer authentication, data authenticity, confidentiality, replay security, encryption, and integrity between two communication points across the IP network. It is a suite of protocols that include the Authentication Header (AH), Encapsulating Security Protocol (ESP), and Security Association (SA). Using cryptography, IPSec provides communication security over IP networks. It employs various cryptographic algorithms to encrypt information such as SHA, AES, 3DES, and CBC.

It commonly finds its application in VPNs, but it can also be implemented in routers and application-level security. It works faster and better in VPN configurations. It adds value to the network configuration that requires data security while transiting the network.

IPSec Virtual Private Network (VPN) allows remote access to cloud environments. If IPSec VPN is used, consider **IP whitelisting** (allow approved IPs only) and **two-factor authentication** methods to access the cloud securely. IPSec is a common element of many VPNs.

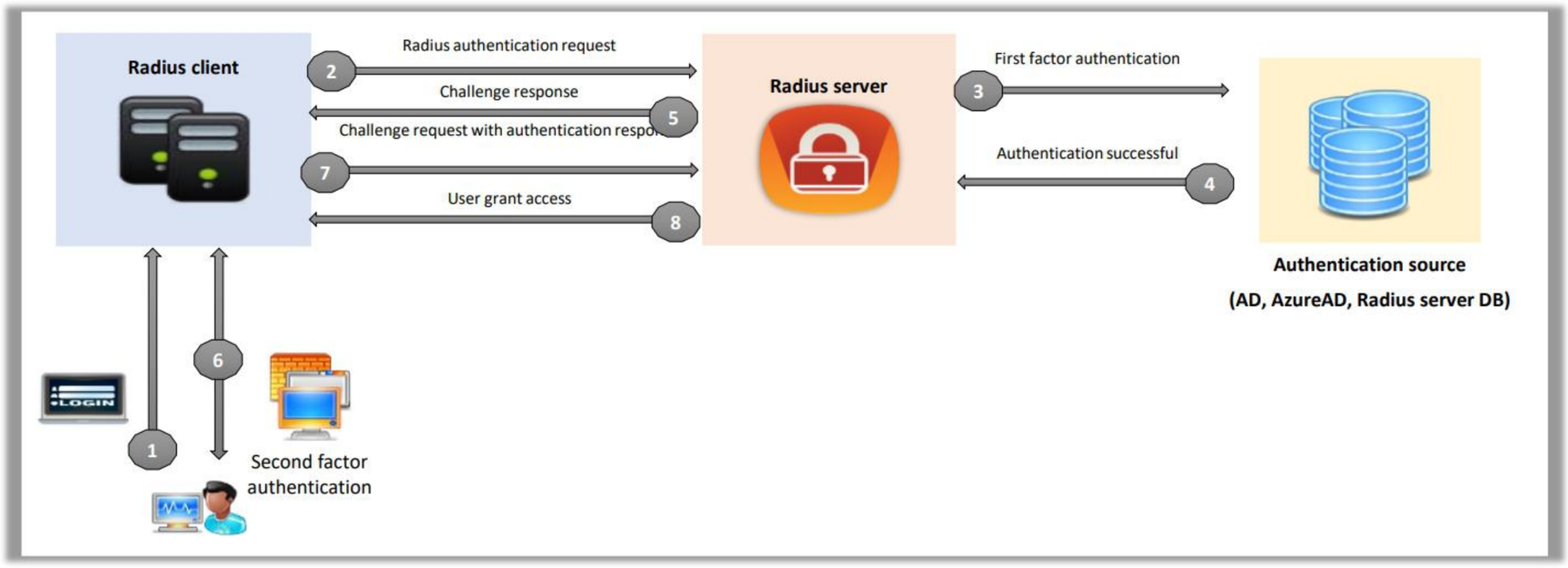
IPSec challenges:

- **Configuration management**: Using IPSec is optional because most devices connecting to the cloud do not have IPSec support enabled and configured.
- **Performance**: Using IPSec may impact the performance of the systems that deploy this technology.

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

Example: miniOrange 2FA for Fortinet FortiGate VPN

For example: Use **miniOrgane 2FA for the Fortinet FortiGate VPN client platform**



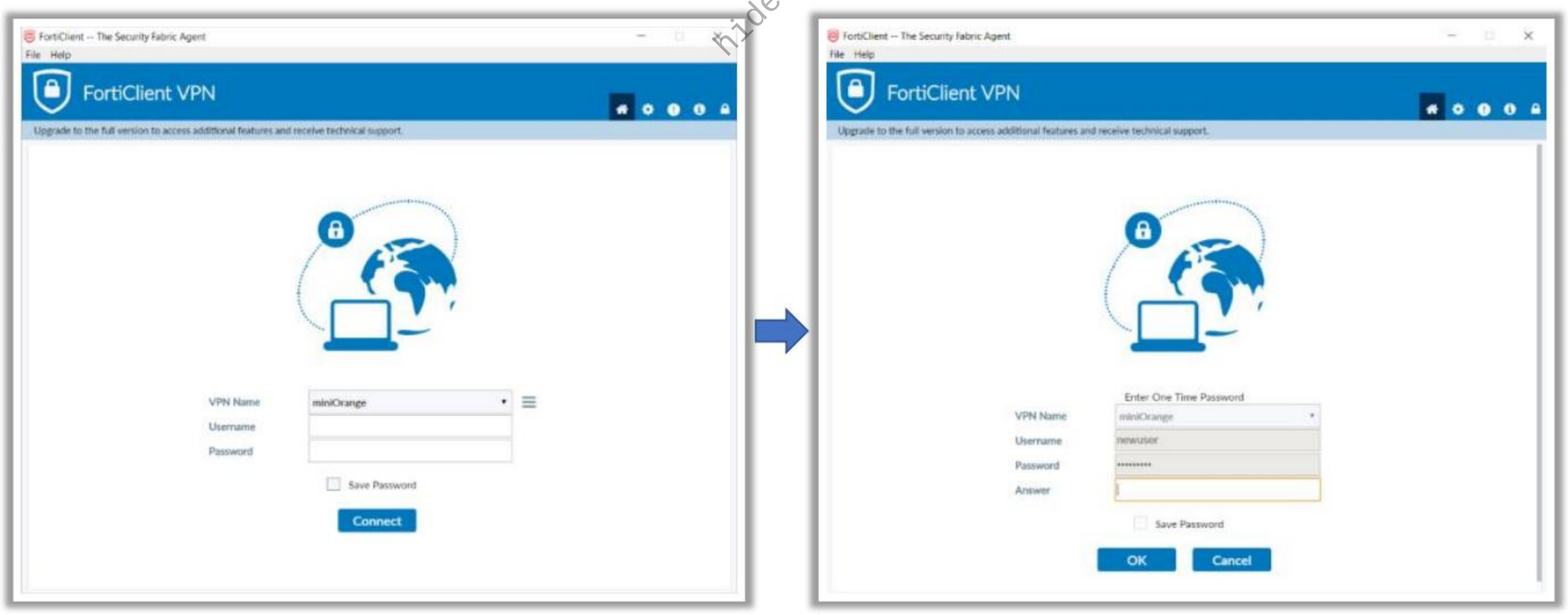
Steps involved in miniOrgane 2FA for Fortinet FortiGate VPN client platform

Source: www.miniorange.com

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

Example: miniOrange 2FA for Fortinet FortiGate VPN (Cont'd)

hide01.ir



Test miniOrange 2FA setup for Fortinet VPN Login

Source: www.miniorange.com

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

Example: miniOrange 2FA for Fortinet FortiGate VPN

For example: miniOrange 2FA for Fortinet FortiGate VPN client platform

Source: https://www.miniorange.com

Fortinet FortiGate VPN provides physical and virtualized security designs and appliances for key information and workloads. Two-factor authentication (2FA) provided by miniOrange can be used for Fortinet FortiGate-managed active directories to enhance security. If 2FA is enabled,

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

users enter a username and password (first factor), followed by an authentication code (second factor) that will be shared to the virtual/hardware 2FA solution.

Enable 2FA in Fortinet FortiGate VPN by enabling RADIUS authentication in Fortinet. Later, configure policies in miniOrange to enable/disable 2FA for users.

The miniOrange ensures 2FA for VPN login by acting as a RADIUS server. Here, this RADIUS server accepts the username and password of users as a RADIUS request. Later, it validates users against the Active Directory (AD), prompts user 2FA, and grants access (see the below diagram). The type of 2FA (software tokens, OTP over e-mail, or push notifications) depends on VPN clients support or do not support the RADIUS challenge.

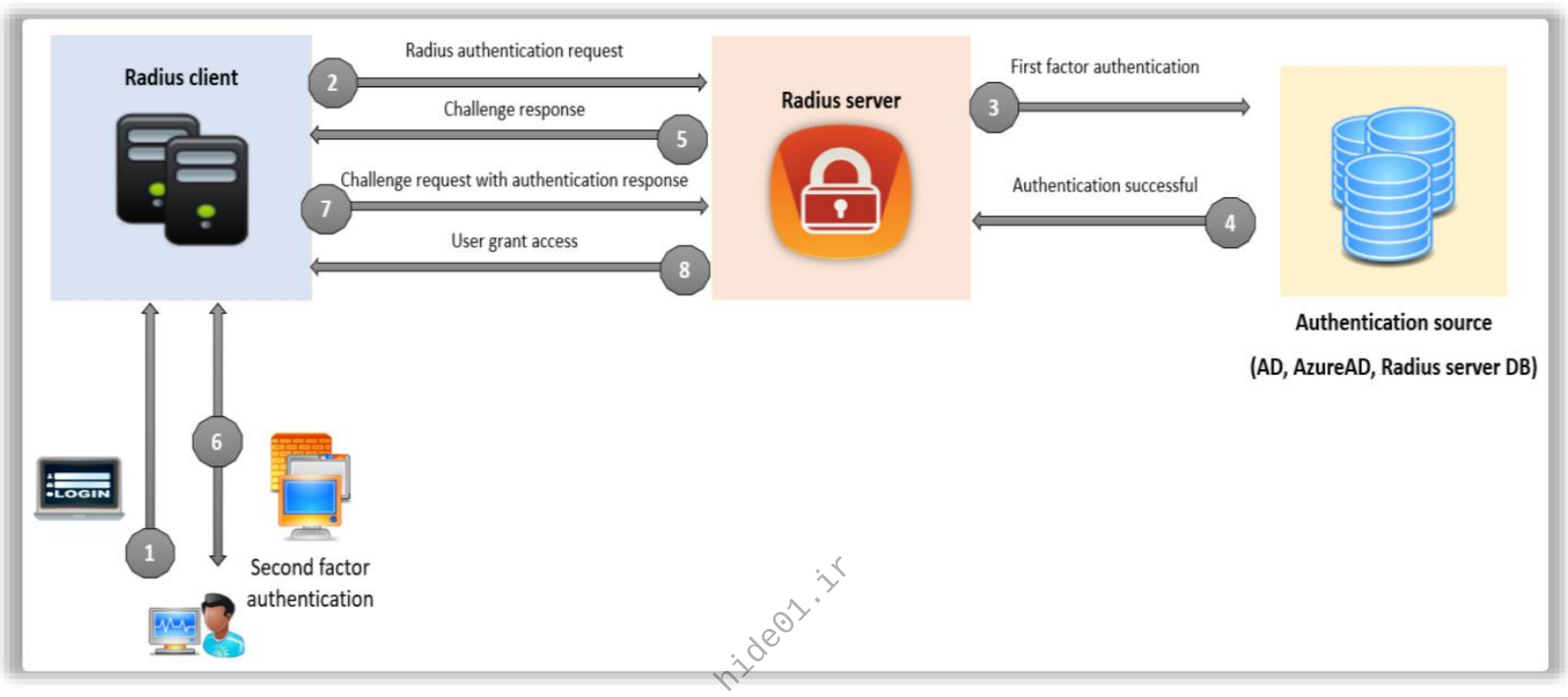
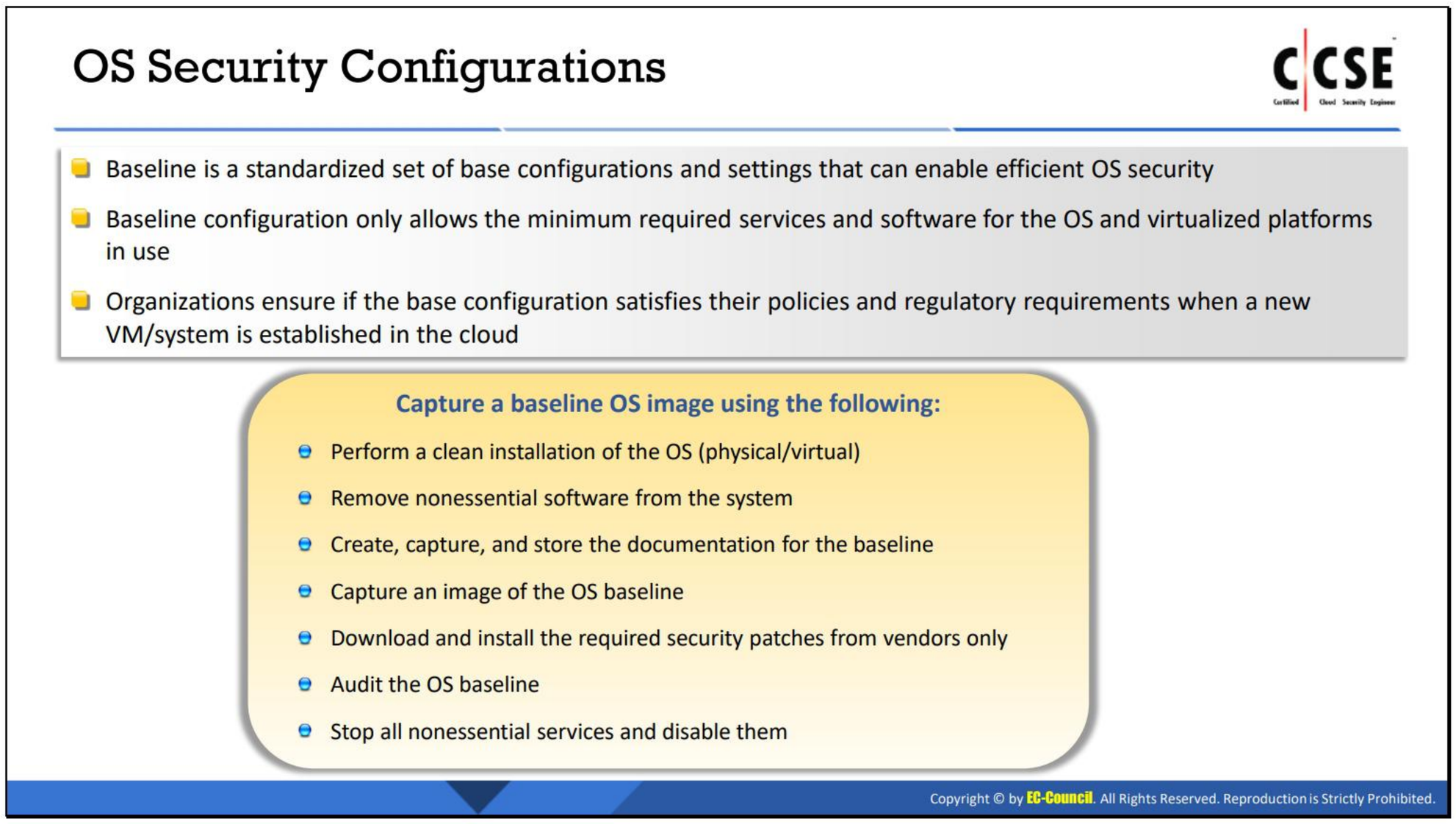


Figure 5.24: 2FA in VPN clients that support the RADIUS challenge

(OR)

miniOrange 2FA for Fortinet FortiGate VPN client platform

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



OS Security Configurations

Baseline is a standardized set of base configurations and settings that can enable efficient OS security. When building a new system or establishing a new VM, organizations apply baselines to a new image to ensure that the base configuration satisfies the organizational policies and regulatory requirements. Before a virtual image is used, organizations apply baselines to such images, enabling new hosts to be started with the already configured standards. In a cloud environment, baselines enable rapid deployment and auto-scaling. Based on the types of OS, technologies, and organizational requirements, baselines are applied to hosts differently.

Organizations should use baseline configuration to only allow the minimum required services and software for the OS and virtualized platforms that are being used. The baseline should be used to satisfy the maximum requirements of cloud customers, and they can detect deviations from the baseline. It should be ensured that the baseline configuration satisfies the organizational policies and regulatory requirements when a new VM/system is established in the cloud. Systems such as AD (Windows) or Puppet (for multiplatform) can be used to manage baselines for servers and hosts under organizational control; they can also detect deviations from such systems.

Establish a functional baseline for the organization. To create or capture a baseline image for the organization, consider the organizational regulatory or policy requirements.

Capture a baseline OS image (OR) OS hardening through the application of baselines using the following:

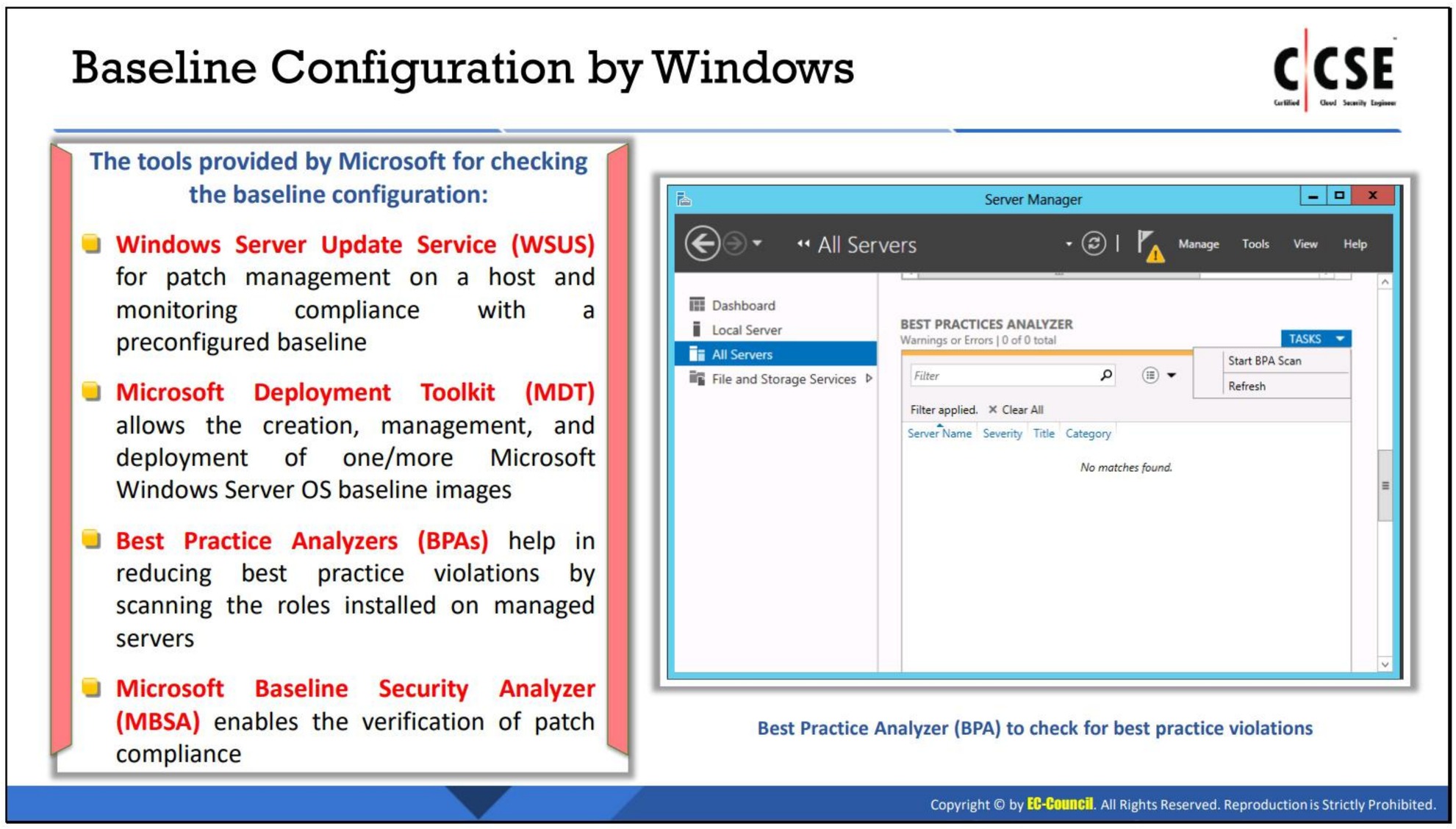
- Ensure that the required configuration of the host OS meets the requirements of the baseline being created.
- Perform a clean installation of the OS for physical or virtual environment.
- Stop nonessential services and disable them to ensure that they are nonfunctional.

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

- Remove nonessential software from the system.
- Place the baseline OS image under configuration management (CM) and treat it for continuous integration (CI).
- Set a schedule and update the baseline OS image for regular security patches and additional required configurations.
- Enforce strong passwords so that users are not allowed to set weak passwords or those that can be estimated easily. Enforce the changing of passwords and disabling user accounts if repeated logins fail.
- Download the required security patches and install them only from the vendor repository.
- Audit the baseline to know whether the required configurations are covered.
- Create, capture, and store a document for the baseline that is being created.
- Capture an image of the OS baseline and store it for future deployments.
- Place the OS baseline image under change management control and ensure the application of all access controls.
- Disable unused user accounts or remove them from the OS.
- Enforce access control lists (ACLs) and file permissions for files and directories.
- Disable unnecessary file sharing.

hide01.ir

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



Baseline Configuration by Windows

The tools provided by Microsoft for checking baseline configuration include:

- **Microsoft Deployment Toolkit (MDT)** allows the creation, management, and deployment of one/more Microsoft Windows Server OS baseline images.
- **Windows Server Update Service (WSUS)** allows patch management on a host and monitors for compliance with a pre-configured baseline.
- **Microsoft Baseline Security Analyzer (MBSA)** enables the verification of patch compliance.
- **Best Practice Analyzers (BPAs)** help in reducing best practice violations by scanning the roles installed on managed servers.

Steps to use BPA to scan roles for best practice violations:

- Open Server Manager.
  - On the Windows taskbar, click on **Server Manager**.

    (OR)
  - On the **Start** screen, click on **Server Manager**.
- In the navigation pane, open a role or group page. The BPA scans from a role or a group page scans all roles installed on the servers in the group.

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

- In the **Tasks** menu of **Best Practices Analyzer** tile, click on **start BPA Scan**.

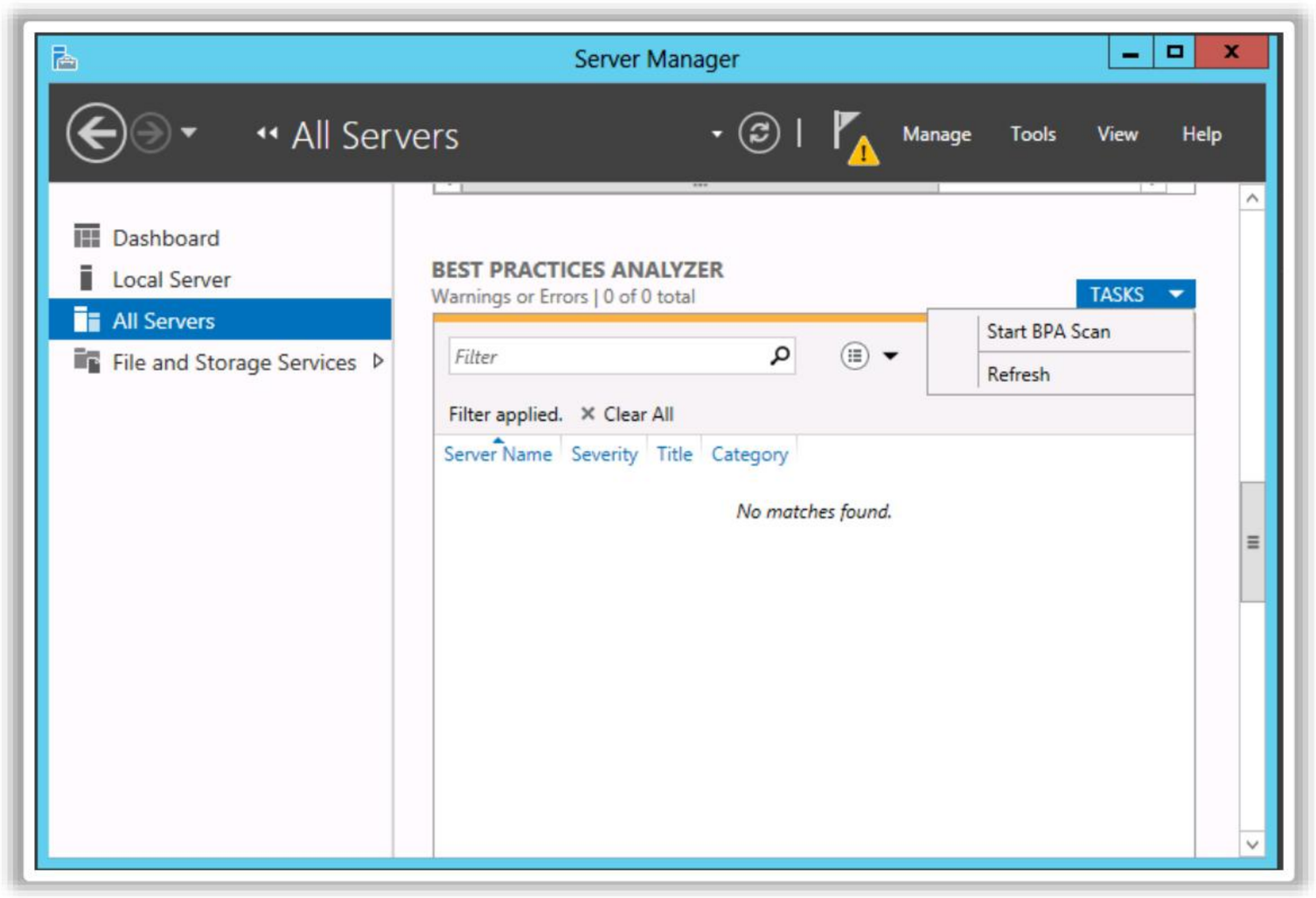


Figure 5.25: Start BPA Scan

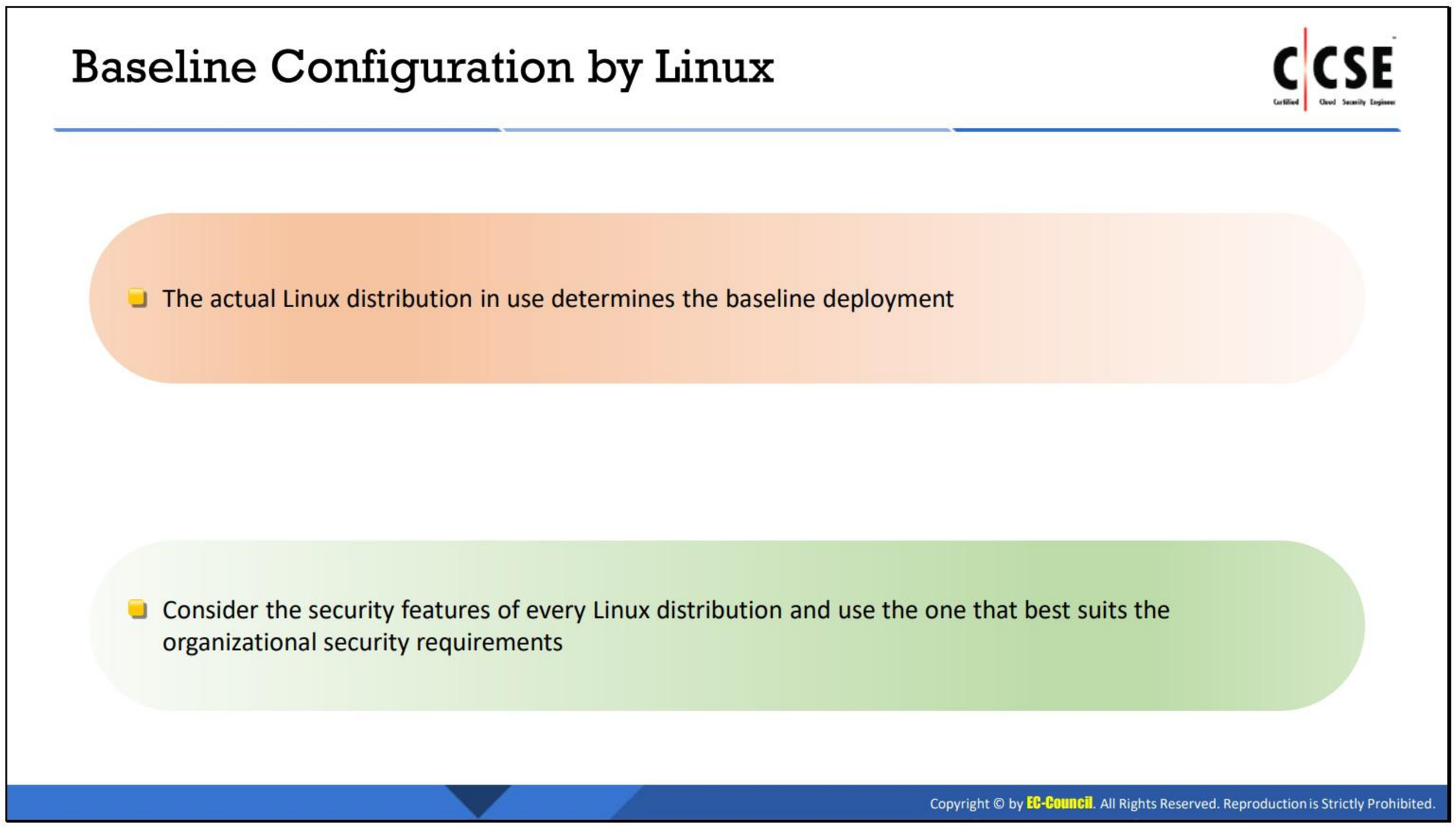
- Depending on the number of rules evaluated for the selected role or group, BPA scan will take a few minutes.

  Here, the scan results are categorized into three different security levels.

  - **Error results:** These are returned if a role fails to satisfy a best practice rule. There may be functionality problems due to these errors.
  - **Information results:** These are returned if a role satisfies the conditions of a best practice rule.
  - **Warning results:** These are returned if noncompliance causes problems.

hide01.ir

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

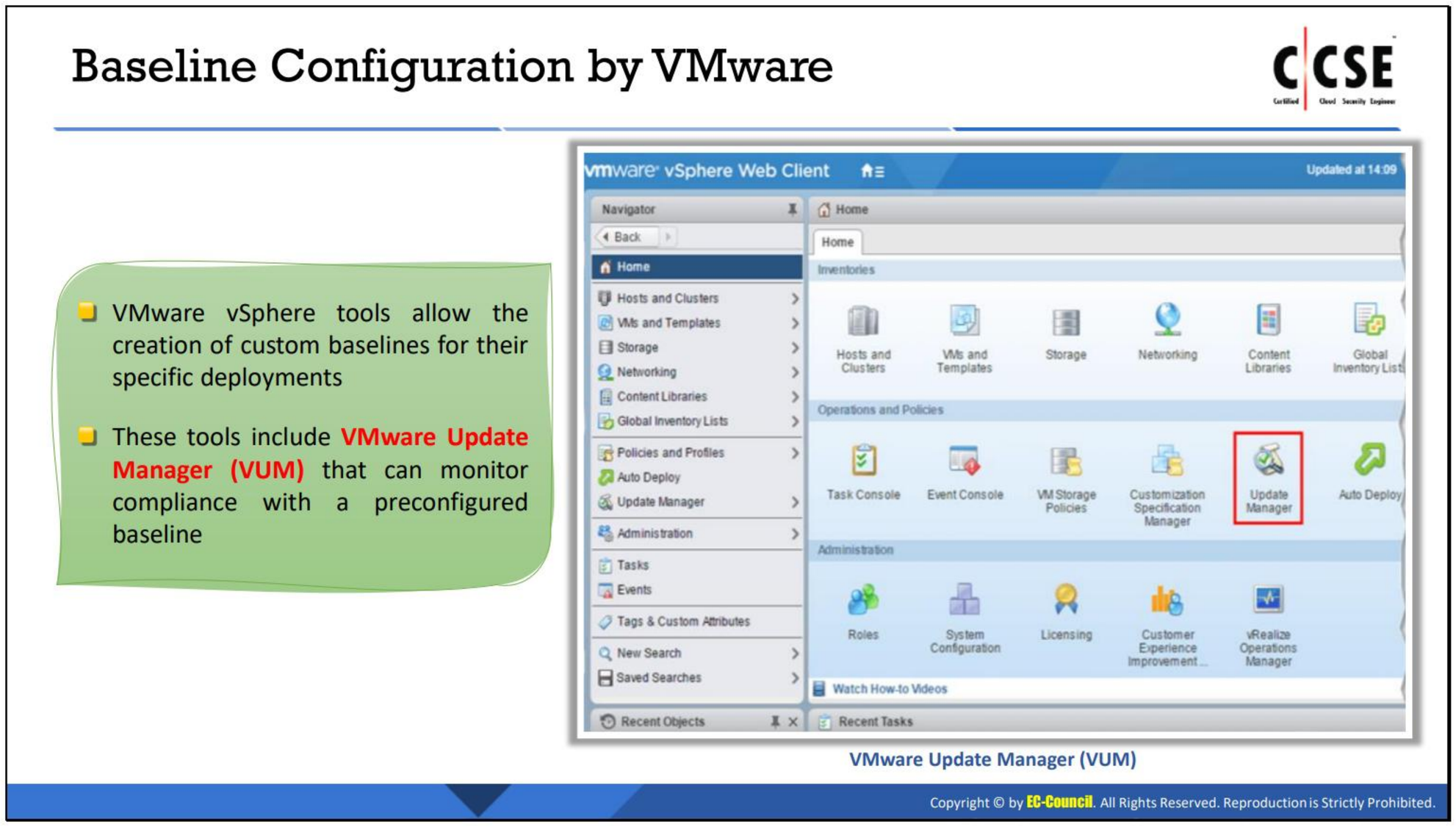


Baseline Configuration by Linux

OS baseline deployment depends on the actual Linux distribution being used. Consider the security features of every Linux distribution and use the one that best suits the organizational security requirements.

hide01.ir

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



VMware Update Manager (VUM)

Baseline Configuration by VMware

VMware vSphere tools enable the creation of custom baselines for their specific deployments. These tools include

- **Host and storage profiles** that enable the **configuration of an ESXi host** to mirror preconfigured baseline options
- **VMware Update Manager (VUM)** that can monitor compliance with a pre-configured baseline

Steps to update an ESXi/ESX host using VMware vCenter Update Manager (VUM):

Source: https://www.vmware.com

- **Set up the frequency of the repository update**
  - Click on **Home**, followed by **Update Manager**.

hdle01.ir

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

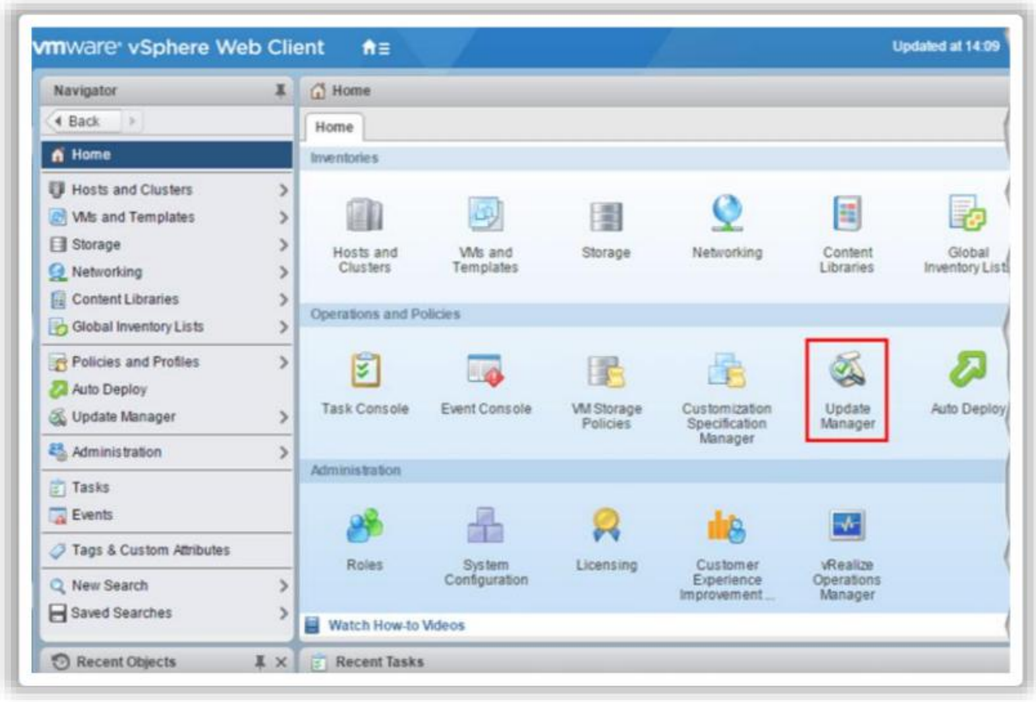


Figure 5.26: Update Manager

- Under the **Configuration** tab, click on **Patch Download Schedule**.

- **View the Patch Download scheduled task:**
  - Click on **Home**, followed by **Scheduled Tasks**.
  - Click on **VMware vCenter Update Manager Update Download**.

    Notes: To manually run, right-click the task and click **Run**. While running the task, see the Download Patch Definitions task in **Recent Tasks**.

- **Attach the baselines to the ESX host:**
  - Click **Home** -> **Hosts and Clusters**.
  - Select the ESX host to be updated and click on **Update Manager**.
  - Click on **Attach**.
  - Select **Critical Host Patches** and **Non-Critical Host Patches baselines**.
  - Click on **Attach**.

    Note: To create custom baselines, click **Home** -> **Update Manager** -> **Baselines and Groups** > **Create**.

- **Scan the ESX host for missing patches against the repository:**
  - Right-click the ESX host and navigate to **Scan for Updates** -> **Patches and Extensions** -> **Scan**.

    Notes: See the scan progress in Recent Tasks by the Scan Entity task.
  - Host scan does not affect the running VMs.
  - If the scan fails, make sure that the ports between Update Manager and ESX host are opened.
  - If the scan is complete, see the number of patches missing on the ESX host. If no patches are missing, see if it is **Compliant**.

hide01.ir

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

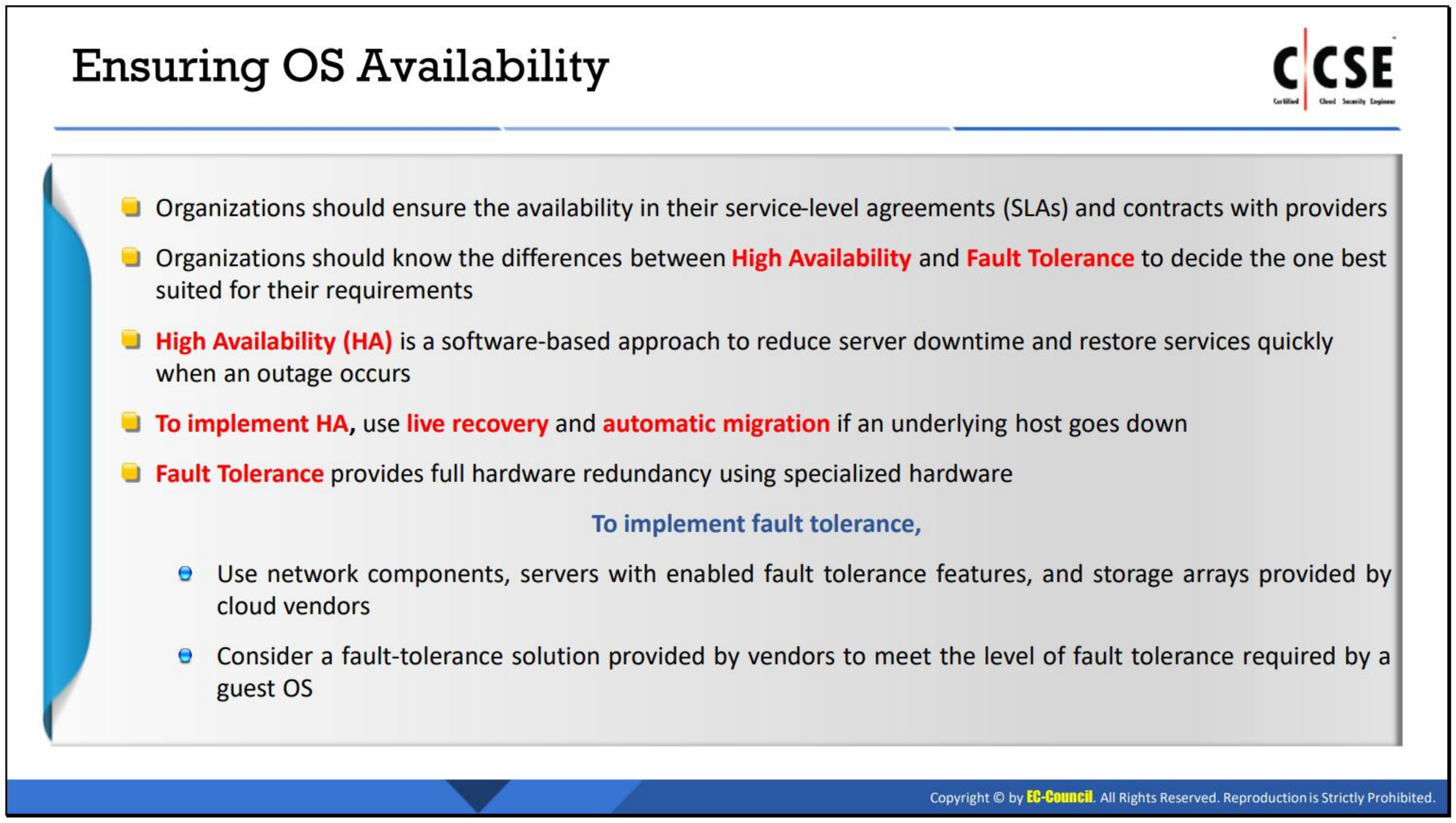
- **Remediate the missing patches to the ESX host:**
  - Power-off all VMs or vMotion them to a different ESX host.
  - Place the ESX host into maintenance mode.
  - Right-click the ESX host, select **Enter Maintenance Mode**, and click on **Yes**.
  - Right-click the ESX host and select **Remediate** -> **Critical Host Patches** and **Non-Critical Host Patches baselines** and click on **Next**.
  - Select which updates or patches to install and click on **Next** -> **Next** -> **Finish**.

    Notes:

    - See the progress of Remediate in Recent Tasks by the Remediate Entity task.
    - Wait for a while until the Update Manager finishes downloading patches from vmware.com.
    - If remediation fails, see if the ports between Update Manager, ESX host, and vmware.com are open.
    - The ESX host may reboot after remediation completes.
- **Initiate a scan in the inventory:**
  - In the vSphere Web Client object navigator, select an ESX/ESXi host or host folder.
  - Click the **Monitor** tab, click on **Update Manager**, followed by **Scan**, and select the types of updates to scan for. Choose to scan for Patches and Extensions or Upgrades if you want.
  - Click on **OK**.

hidedot.ir

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



Ensuring OS Availability

Generally, cloud environments ensure availability by providing redundancy and fault tolerance in systems. Here, the level of redundancy is high in the cloud, and redundancy is possible to a higher degree to ensure availability. As per their requirements, organizations should ensure availability in their service-level agreements (SLAs) and contracts with providers.

The mechanisms to ensure the availability of the guest OS running on a cloud host include the following. Organizations should know the differences between these while deciding the suitable ones.

- **Redundant system hardware:** It can address system outages due to hardware failure. For example, backup power supplies or generators can ensure continuous power supply to hosts if power is cut off for some time.
- **High availability (HA):** It is a software-based approach to reduce server downtime. It reduces the downtime and restores services quickly during an outage. To reduce the impact of system downtime, HA uses the available shared and pooled resources. The HA can limit the downtime as well as maintain the system performance at optimum levels. However, it leads to downtime lag, which results in the unavailability of applications to clients. For example, if a client requests a website hosted on a high-availability platform and if a node crashes, the client will see a 500 error message; this is because if the primary server fails to respond due to an OS error/node crash, the error will not be replicated in the HA system.

  To implement HA,

  - Organizations can use live recovery or automatic migration if an underlying host goes down for their availability requirements.

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

- Use vendor-provided specific toolsets to ensure HA.
- Understand the vendor capabilities within the HA and document them during the disaster recovery plan (DRP)/business continuity plan (BCP) process.

- **Fault tolerance:** It provides full hardware redundancy. It involves specialized hardware to detect faults. Depending on the identified fault, it automatically switches to redundant systems. Organizations use this when they want to remove system downtime as a threat to system availability.

  Although fault tolerance provides a higher degree of availability, it is still limited, and organizations must pay higher costs on standby hardware. Software failures are responsible for maximum system availability issues in the cloud. Moreover, fault tolerance can only address hardware failures, not software failures.

  Unlike HA, fault tolerance maintenance of system performance is not the greatest priority. If an error occurs in a fault-tolerant system during an active action, the system will accept its end state; this is not the case with HA systems. For example, if a client requests a website hosted on a high-availability platform and if a node crashes, the client will see a 500 error message.

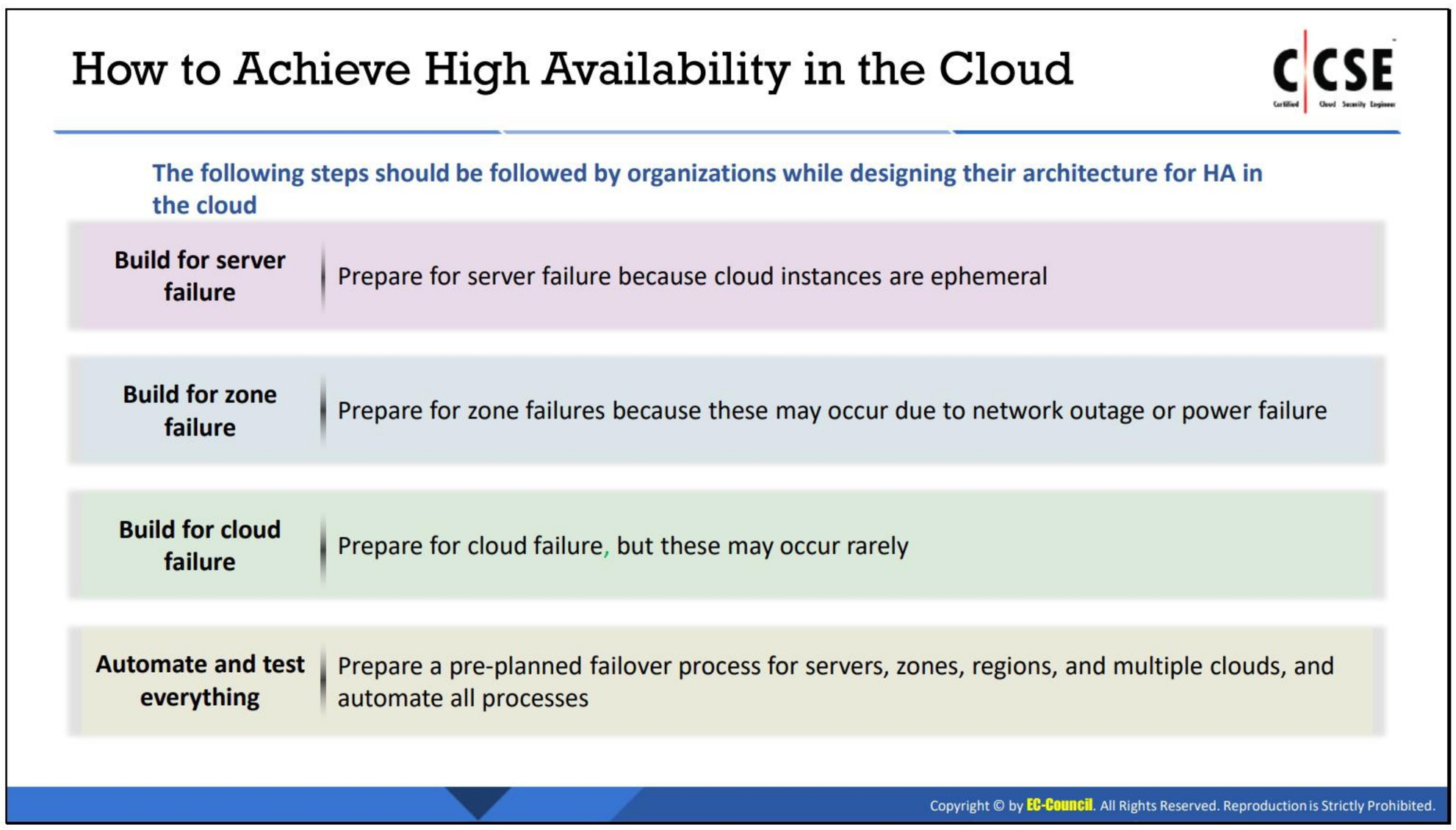
  With a fault-tolerant system, the system can still be operational and respond to new requests. It is the key difference between HA and fault tolerance.

  To implement fault tolerance,

  - Organizations can use network components, servers with enabled fault tolerance features, or storage arrays provided by cloud vendors.
  - Consider a fault-tolerance solution provided by the vendors to meet the level of fault tolerance required by a guest OS.

hiccc01.ir

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



How to Achieve High Availability in the Cloud

Every component of the cloud will fail at some point in time. Organizations should automate processes to handle such failures. To manage such failures or downtime, HA strategies can be implemented.

hide01.ir

Organizations should follow the steps given below while designing their architecture for HA in the cloud.

- **Build for server failure**

  Prepare for server failure because cloud instances are ephemeral. First, address the issue of server failure by designing stateless applications that are resilient through server/service reboot/relaunch.

  - Mirror the databases, configurations of master/slave, and/or data integrity and ensure minimum downtime.
  - Consider performance metrics and set up auto-scaling to enable organizational applications to respond to dynamic traffic.
  - Use dynamic DNS and static IPs.

- **Build for zone failure**

  Owing to power failures, network outages, lighting, or earthquakes, more than one server can fail.

  - Organizations should ensure that their applications are prepared for zone failures.
  - Distribute or replicate organizational data across multiple zones.

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

- Spread the servers in every application tier across at least two different zones.

- **Build for cloud failure**

  Rarely, multiple zones in a region may face cloud-wide issues. Every region is an independent system of resources. Building for cloud failure is difficult because APIs, services, and configurations are different from each other.

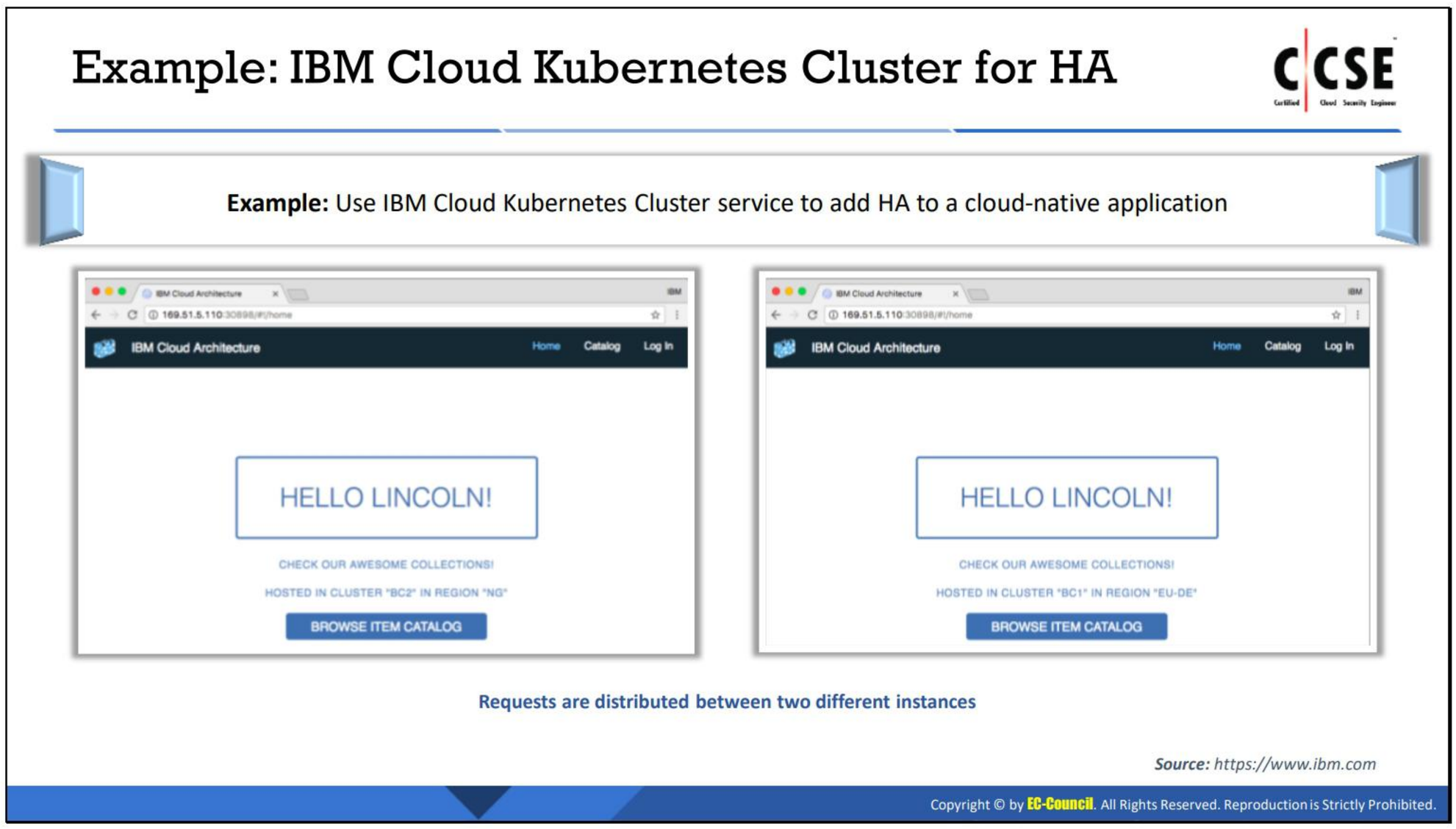
  - To achieve multiple 9s of availability, design the architecture using generic concepts such as durable storage and deploy cloud specifics such as EBS volumes.
  - Implement a fault-tolerant strategy to move across different regions of the same provider and across different infrastructure providers.
  - Backup data across different regions/providers.
  - Secure and authenticate user communication across regions.
  - Build HA across zones and expand HA to multiple cloud providers.

- **Automate and test everything**

  Organizations should automate their processes in the event of a failure. Determine pre-planned failover processes across servers, zones, regions, and multiple clouds.

  - Automate backups to make the organization available during downtime.
  - Use monitoring and alerts to issues or problems when they occur because the cloud customers may not receive timely notifications from providers sometimes.
  - Test the organizational infrastructure to determine if it can withstand failure. For testing purposes, use high loads on production servers and disable other servers, zones, and services.

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



Example: IBM Cloud Kubernetes Cluster for HA

IBM Cloud Kubernetes Service allows the creation of a cluster of compute hosts and deployment of HA containers. Its key features include security cluster infrastructure, isolating computing resources, and ensuring security compliance in container deployments. It enables the configuration of custom Kubernetes clusters that can auto-scale and recover containers based on defined policies.

Source: www.cloud.ibm.com

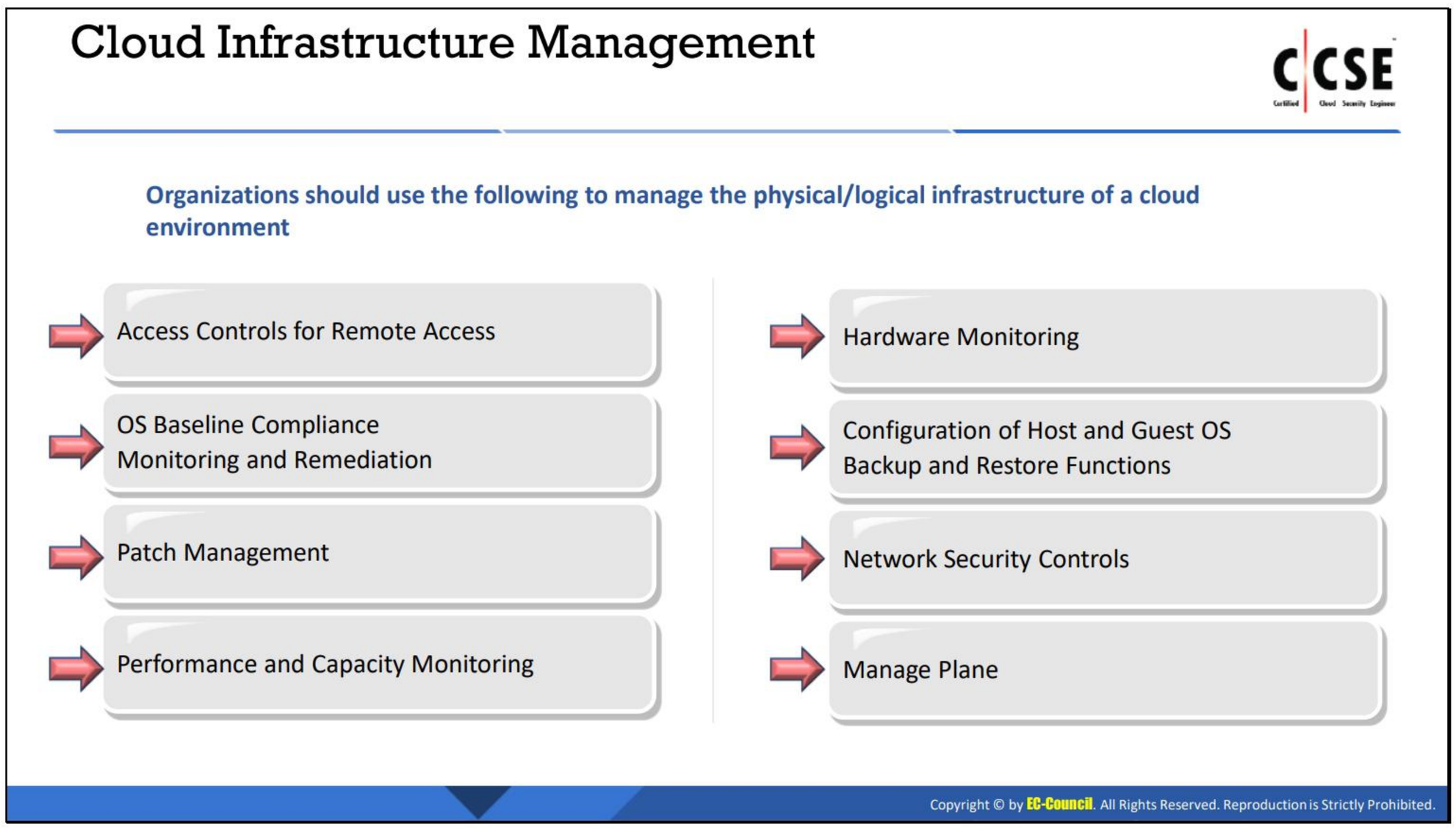
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

LO#5: Learn Security Operations to Manage Cloud Infrastructure

The objective of this section is to understand the management of the physical and logical infrastructures of cloud using various methods. In this section, cloud security engineers will learn about access control for remote access, various types of updates in the cloud, patching methodologies, applying security patches, patch management, hardware monitoring, and network security controls. This section will help in understanding the management of the physical and logical infrastructures of the cloud environment and using them efficiently for securing cloud environments.

vid01.ir

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

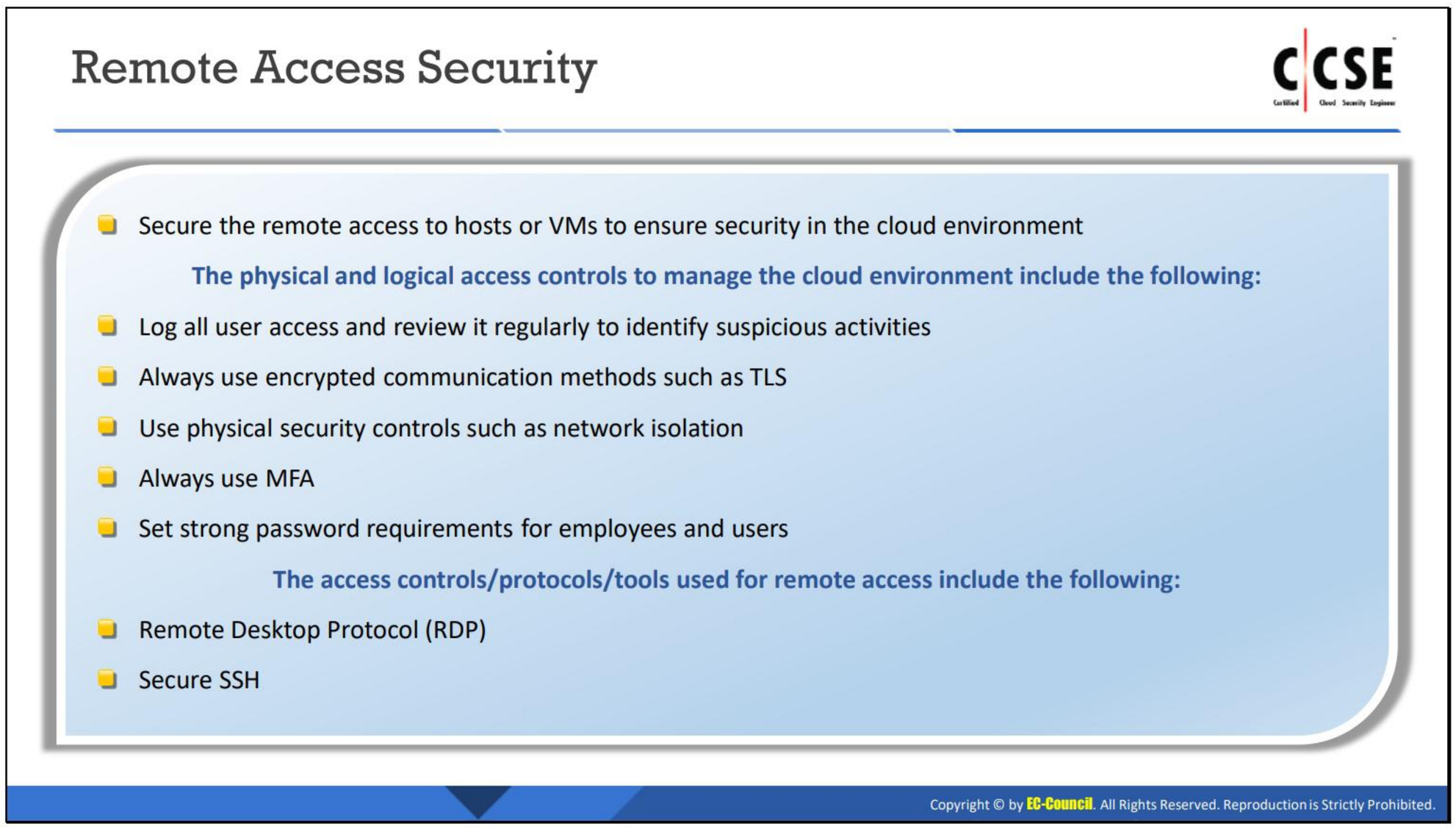


Cloud Infrastructure Management

- Access controls for remote access
- OS baseline compliance monitoring and remediation
- Patch management
- Performance and capacity monitoring
- Hardware monitoring
- Configuration of host and guest OS backup and restore functions
- Network security controls

hide01.ir

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



Remote Access Security

Cloud users need remote access to manage cloud hosts and applications. In a cloud environment, customers do not get physical access to their systems; they rely entirely on remote access to manage cloud infrastructure. Secure remote access to the hosts and ensure the security of the cloud platform and customer data.

hiu01.ir

Ensure secure access to cloud hosts and applications by allowing only appropriate users to use them after proper authentication and authorization. Meanwhile, ensure that organizational policies are followed and users are provided with the least privileges. This will ensure data confidentiality and integrity.

Controlling remote access provides the following benefits:

- Preserves privileged credentials
- Restricts remote access to the cloud environment
- Provides session control over workflow enforcement and access permissions
- Prevents sufficient isolation between the desktop of the remote user and the target system to which the user connects to prevent the spread of malware
- Allows real-time monitoring to see privileged activities in the cloud

Physical and logical access controls to manage a cloud environment include the following:

- Because location-based controls or physical controls cannot manage a cloud environment, use remote desktop technologies such as Citrix, Splashtop, or ConnectWise Control to monitor cloud infrastructure remotely and securely. Use such technologies to reduce attack vectors and improve the security of remote access.

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

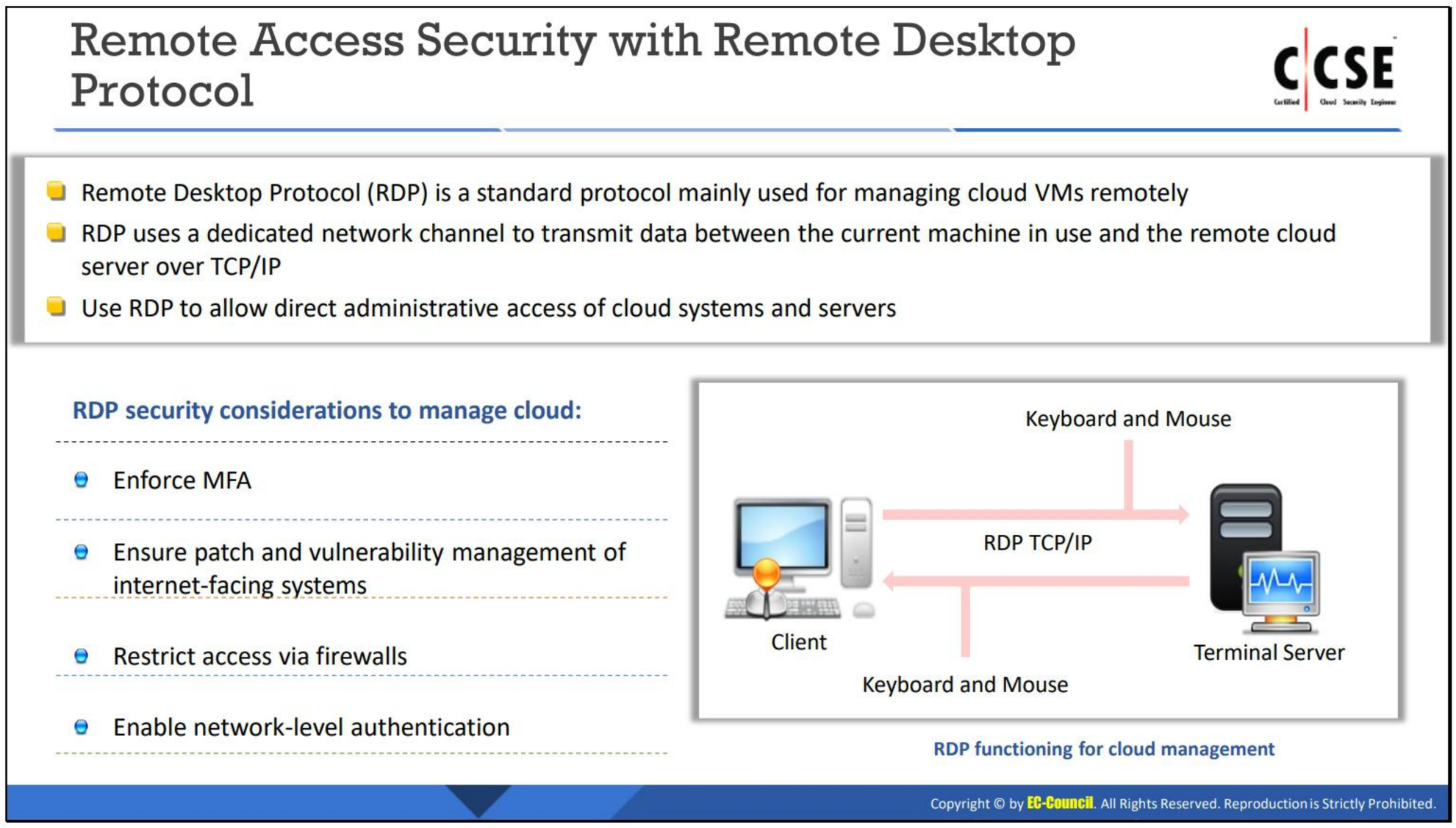
- Integrate strong logging and monitoring with a centralized access method, which will help admins and providers in enforcing strict access requirements and limitations when necessary.
- Log all user access and review it regularly to identify suspicious activities.
- Configure alerts for incidents such as multiple login failures and login attempts from different IP addresses within a short period.
- Always use encrypted communication methods such as TLS.
- Use physical security controls such as network isolation.
- Always use multi-factor authentication.
- Set strong password requirements for employees and users.
- Use a centralized access method.

The access controls/protocols/tools used for remote access are

- **Remote Desktop Protocol (RDP)**
- **Secure SSH**

hide01.ir

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



Remote Access Security with Remote Desktop Protocol

Remote Desktop Protocol (RDP) is a standard protocol mainly used for managing cloud VMs remotely. For secure remote administrator access, use RDP to allow direct administrative access of cloud systems and servers. It offers secure data transfer without VPN and secure storage of data on-premises.

RDP transmits user activities on their current computer to the remote desktop. These activities include keystrokes and mouse movements (as shown in the below image). A dedicated network channel is used to transmit data between the current machine in use and the remote cloud server over TCP/IP. This transmission happens with a delay of few milliseconds because all actions (keyboard strokes and mouse movements) are encrypted before transmission. RDP helps in transmitting screen events, keystrokes, mouse activity, and updates to manage the cloud environment.

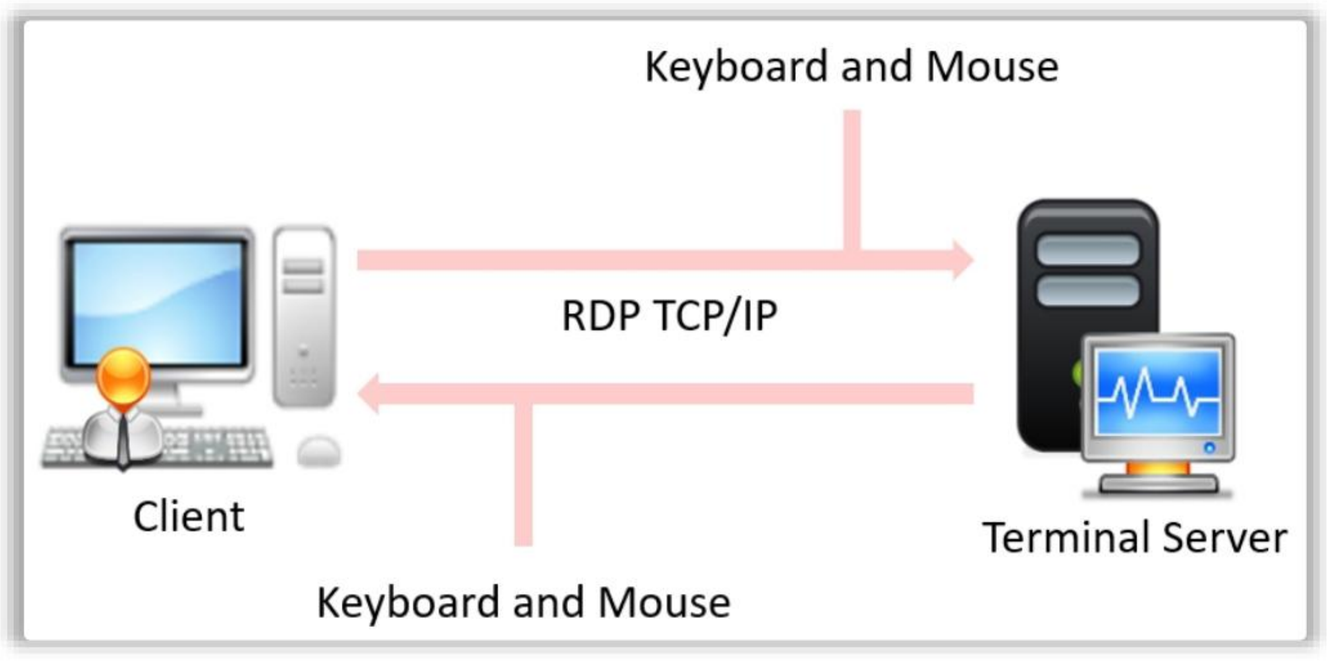


Figure 5.27: RDP functioning for managing cloud

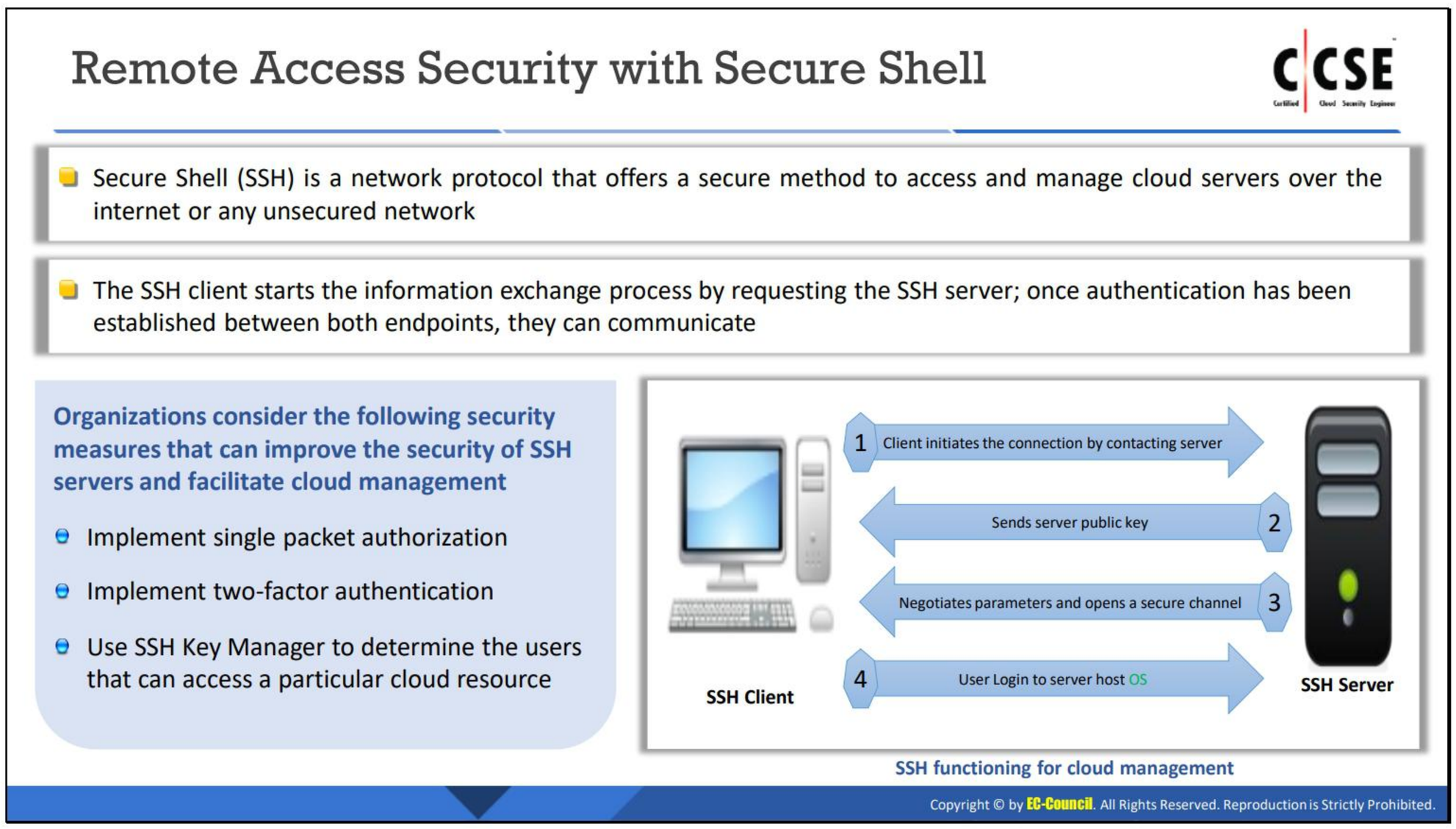
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The security considerations offered by the RDP to manage the cloud infrastructure include:

- Implementation of session security
- Enforcement of multi-factor authentication
- Patch and vulnerability management of internet-facing systems
- Control, log, and audit of remote access
- Direct accessibility of systems over the internet
- Restricted access via firewalls
- Enablement of network-level authentication

hide01.ir

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



SSH functioning for cloud management

Remote Access Security with Secure Shell

The Secure Shell (SSH) network protocol offers a secure way to access and manage cloud servers over the internet or any unsecured network. It provides the following while managing the cloud infrastructure:

- Data authentication, data integrity, and data encryption for transmitted data
- Security of remote terminals over the internet
- Prevention of DNS spoofing, IP spoofing, eavesdropping, and data manipulation

The SSH client starts the information exchange process by requesting the SSH server. Once the authentication between both endpoints is completed, communication can be established. SSH uses a cryptography system for work session and authentication; thus, it is widely used for access control and remote administration of the cloud.

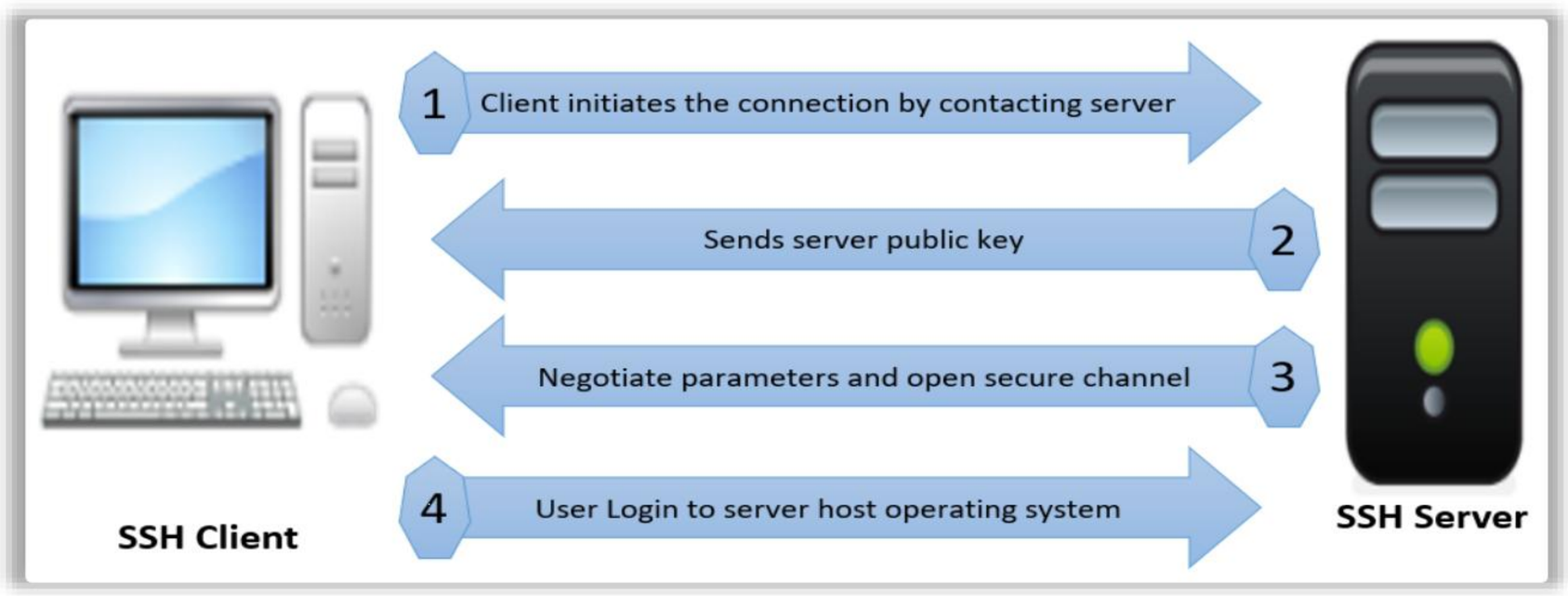


Figure 5.28: SSH Functioning

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

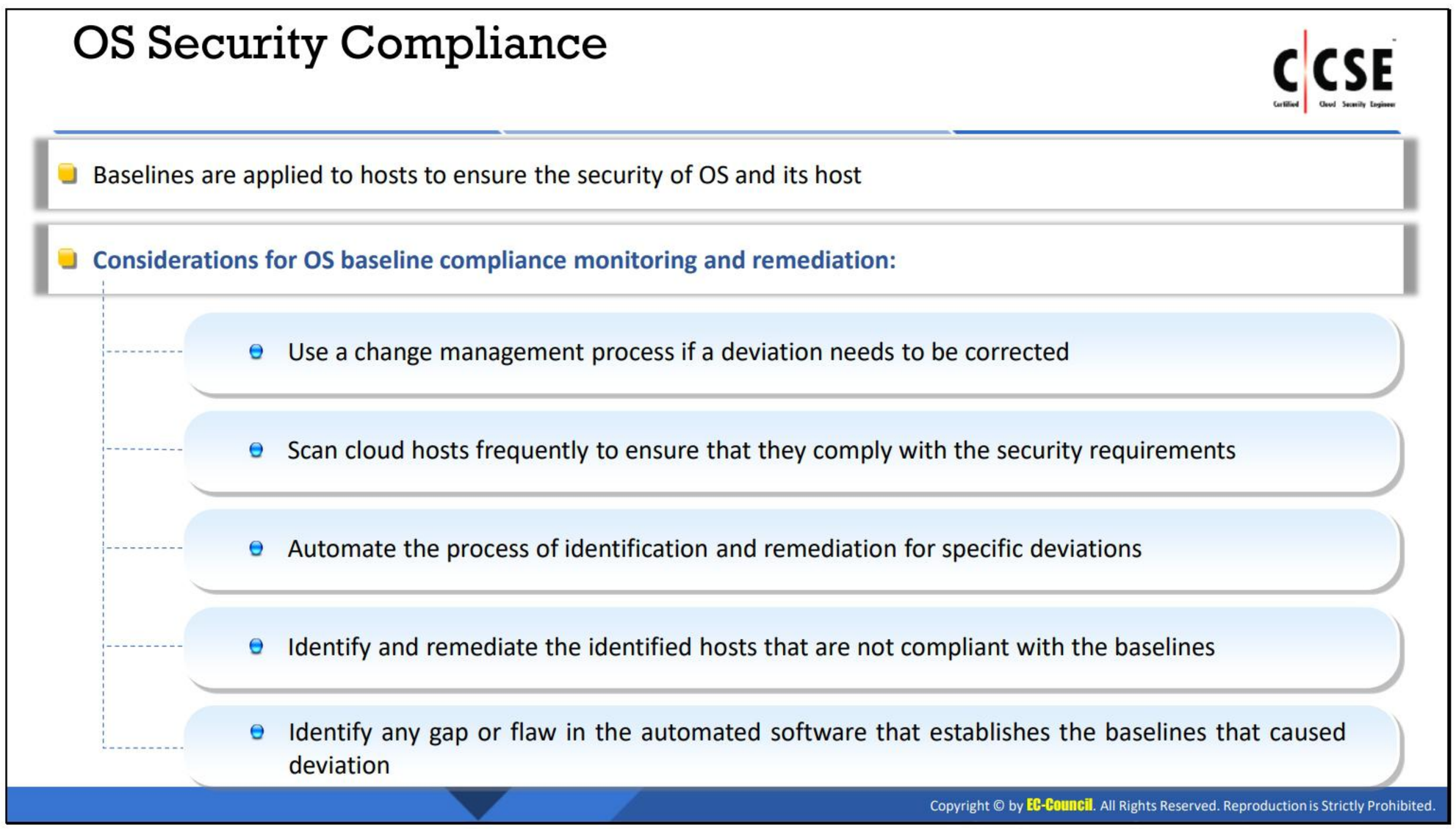
Hardening SSH

The security measures that can improve the security of SSH servers and enable easy management of the cloud include:

- Using TCP wrapper to define a list of IP addresses that are denied or allowed access to the SSH server
- Using port knocking to secure the SSH server from various attacks
- Implementing single packet authorization
- Implementing 2FA
- Using SSH Key Manager to know which user can get access to a particular cloud resource

hide01.ir

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



OS Security Compliance

Baselines are applied to hosts to ensure the security of the OS and its host. After applying baselines to a particular host, ensure that they have been correctly installed and enabled. With new installations, configuration changes, and updated software versions, the baseline changes and new baselines may be set according to organizational policies.

Considerations for OS baseline compliance monitoring and remediation include the following,

- In a cloud environment, use an automated scanning software tool to perform scans to identify and flag hosts that are not compliant with the baseline configurations loaded into the scanning software. Use the tools provided by cloud providers or external providers.
- Identify and remediate the identified hosts that are not compliant with the baselines. This can help in detecting unauthorized changes made by developers or administrators, if any.
- Identify any gap or flaw in the automated software that sets baselines causing deviations.
- Automate the process of identification and remediation for specific deviations.
- Use a change management process if a deviation requires correction.
- Document the approved deviations based on organizational policies and get them approved by the organization's change management.
- Scan cloud hosts often to remain in compliance with security requirements.
- Perform scanning when the host encounters change in configuration, new software installation, upgrades, or patching because these activities may introduce new vulnerabilities or deviations from the defined baselines.

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

Managing Updates in Cloud Infrastructure

- Updates in a cloud environment help to repair the security holes, remove or fix bugs, remove outdated features, and add the latest features
- The various types of updates commonly observed in a cloud ecosystem are as follows:

Hotfix

- It is a software update that is designed to resolve a particular problem instantly with a quick-release procedure
- Hotfix is mostly a bug fix that is released without following normal quality assurance
- Because the installation of hotfix could introduce new issues in the environment, immediate actions need not be taken against the bug until testing is completed

Patch

- A known bug or issue can be fixed with a patch update
- A patch is a piece of software code that is designed to update an application or OS to fix any security vulnerability or operational bug

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

Managing Updates in Cloud Infrastructure (Cont'd)

hide01.ir

Version Update

- In this type of update, a software product is replaced with a new version of the same product
- Version update can add the latest features, update the system, and deliver a roll-up of earlier patches

Rollback

- In this type of update, the software is returned to its previous state
- Rollback update is performed if a software fails to update, the issues were not fixed as expected, or new issues were observed in the environment; thus, the original state of the system needs to be restored

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

Managing Updates in Cloud Infrastructure

Updates in a cloud environment help in repairing the security holes, removing or fixing bugs, removing outdated features, and adding the latest features.

The various types of updates that are commonly observed in a cloud ecosystem are as follows:

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

- **Hotfix**

  It is a software update that is designed to resolve a particular problem instantly with a quick-release procedure. Hotfix is also referred to as quick-fix engineering (QFE) update because it fixes a problem (bug) in a software product immediately. Normally, hotfix updates are customer-specific that are meant to address specific customer situations. This implies that they may not be released to everyone.

  Hotfix is often a bug fix that is released without following the normal quality assurance procedures because it is meant for quick deployment. A hotfix update poses a higher-risk factor than other software patching approaches owing to its quick nature of providing a bug fix to a critical issue. Hotfixes are risky because they are applied to systems that are live or running in production.

  A hotfix package may have multiple encompassed bug fixes that increase the risk of regression. A subset of full QA test suites is normally used to quickly test hotfix patches. New and unknown issues can be introduced into an environment when a hotfix is applied. Hotfixes are less likely to fix problems and may even cause an immediate loss of services.

  Because the installation of the hotfix could introduce new issues in your environment, do not immediately take any action against the bug until all testing procedures have been performed. Accordingly, compare the risk of applying a hotfix for fixing a bug and introducing new issues against the risk of living with the bug without taking any action.

- **Patch**

  Patch refers to an update that is released publicly to fix a software bug or problem. A known bug or issue can be fixed with a patch update. A patch is a piece of software code that is designed to update an application or OS to fix any security vulnerability or operational bug to improve its operation.

  Software vendors release patches as temporary fixes in between full releases of software packages. Patches are meant to fix both large and small issues that may or may not require immediate attention such as installing new drivers, fixing a bug, upgrading the software, fixing new security vulnerabilities, and addressing new software stability issues.

  Usually, patches are updates of various sizes that are automatically installed on the software. They provide performance enhancement or fixes but do not offer feature enhancements. Patches are mostly delivered on a set schedule and can be included in the new version release of a software product along with additional fixes and updates.

- **Version Update**

  In this type of update, the software product is replaced with a new version of the same product.

  Version updates can add the latest features, update the system, and deliver a roll-up of earlier patches to improve the software product. To upgrade a software product, its current version must be replaced with its latest version.

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

A software version update is different from a software update because software updates are made to the existing software program, whereas version updates (software upgrades) are new versions of the same existing product. In addition, software updates demand less attention and are free, but software upgrades are provided for a cost and are bigger than updates. Unlike software updates, software upgrades are not always compulsory to keep the product running.

Software vendors introduce major feature capabilities and enhancements through version updates. They may charge for these version updates because they improve the overall product functionality and experience. A software version update is also called a software upgrade because it involves purchasing a new version of the same existing product.

- **Rollback**

When a software update applied to address or fix a software issue fails to successfully solve the problem, it is often required to downgrade the software to its previous state. This can be achieved via a rollback. It is the process of bringing back the updated version of software to its original state. Contrary to a version update, the software is brought back to its earlier version in a rollback update.

Normally, rollback update is performed if a software fails to update, the issues are not fixed as expected, or new issues are observed in the environment. Rollback updates help to restore the previous version of the software when the newer version cannot be used to provide the expected results.

Depending on individual systems, the process of performing a rollback varies. For example, a snapshot of an existing VM is taken before installing a patch to it so that if there is any issue with the new update, the snapshot can be used to roll back the software to its earlier version. Some OSes and applications allow the patch to be rolled back with the help of scripts and utilities. However, in some cases, the original package has to be installed to overwrite the patch.

Similarly, rollback is prevalent in database operations. Rollback is an operation that can help the database to return to its previous state to ensure database integrity. A rollback can be performed in the case of a critical database issue so that the database is returned to the point before the issue.

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

Cloud Patching Methodologies

- Ensure that all systems in an organization are updated with the latest security patches to minimize the attack footprint and safeguard the organization by addressing the known bugs that could affect operations
- The various patching methodologies to patch systems are as follows:

Production Systems

- Before rolling out the patches to be applied on production systems, they should be tested in a non-production environment
- After patching the production systems, perform testing to ensure that it is successful and the system is performing operations as expected

Development Systems

- Before rolling out a product, the DevOps team must evaluate the patches and integrate them into the product

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

Cloud Patching Methodologies (Cont'd)

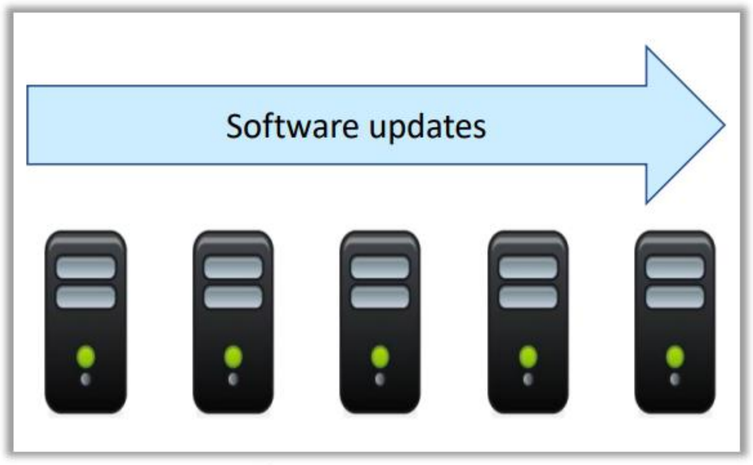
guide01.ir

Quality Assurance

- Establish a quality assurance testbed to test a particular patch in your environment to determine dependencies, concerns with interoperability, and ascertain the patch updates that can resolve the problem of the organization

Perform Rolling Updates

- Rolling updates are small and frequent updates, which are performed sequentially
- In rolling updates, a system is patched; when the first system is patched successfully, the next system is patched



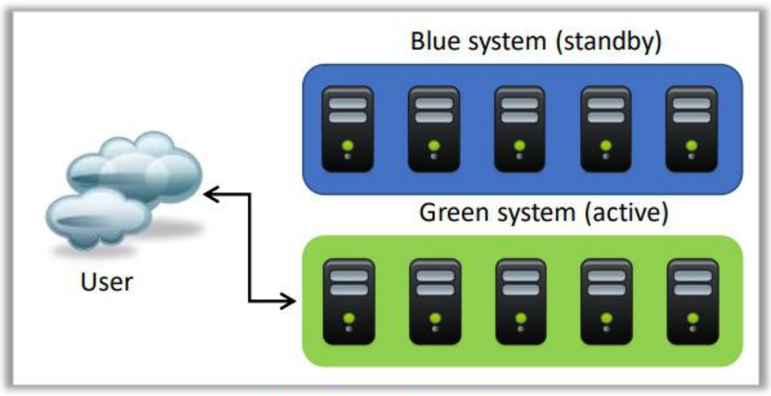
Performing Rolling Updates

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

Cloud Patching Methodologies (Cont'd)

Blue-Green

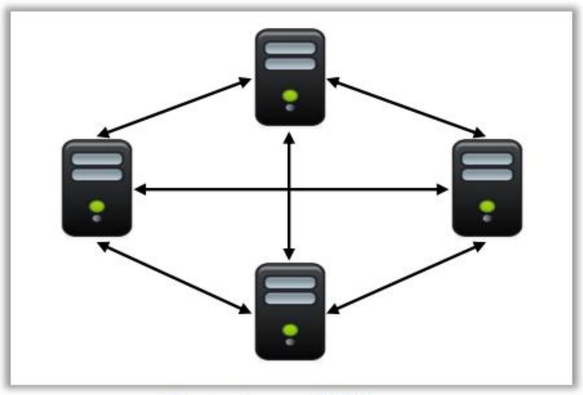
- In the Blue-Green methodology, two identical configurations are used in the production environment; one environment is referred to as Blue and the other as Green
- One environment remains active while the other becomes inactive; thus, security patches and software updates can be implemented in the inactive side



Blue-Green Deployment

Clustering and Failover

- Security patches or updates can be installed on the master nodes of a cluster; they push and install the patches or updates on all systems in a cluster
- If any node in the cluster fails, another node assumes the operational functionality of that node without any downtime



Clustering and Failover

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

Cloud Patching Methodologies

To ensure ongoing cloud operational support, patching is essential. There are various patching methods that can be used for patching. It should be ensured that all systems in an organization are updated with the latest security patches to minimize the attack footprint and safeguard the organization by addressing the known bugs that could affect its operations.

Patch management can be complex if systems have different versions or levels of patches. It is recommended to have the same version, revision, or patch level for all related systems. This will help IT admins to have a known security baseline that can help them operate and troubleshoot systems conveniently. Admins can keep track of cloud system versions using spreadsheets (to manually track version levels) or applications (to automatically track them).

Different types of patches are released every month and it can be cumbersome to decide which patch should be applied first. The prioritization of patches becomes a challenge when several patches are released simultaneously. It is essential for admins to know the order in which patches must be applied and their application process based on the criticality of security issues. Assessing the level of risk to different systems can help in identifying the systems that require patches instantly and those that can wait.

Various methodologies can be used to patch cloud systems, as explained below:

Production Systems

The application of patches to systems in production is risky because newly applied patches may cause operational issues in the systems. Additionally, other steps must be considered to ensure successful patch operation such as:

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

- Ensure that the change management process is followed by production updates and a plan is developed that describes the upgrade steps, testing and validation processes, and the process to rollback patches under undesirable results.
- Before rolling out patches to be applied on production systems, they should be tested in a non-production environment. Automate the patching and updating processes if there are numerous servers to ensure consistency. To automate the process, use automation systems such as Chef, Puppet, Ansible, or OpenStack.
- After patching the production systems, perform testing to ensure that patching is successful and the system is performing the expected operations.
- Use the rollback plan to restore the system to its previous state if issues occur after patching.

Although patching production systems is risky, it is sometimes necessary to apply patches to fix security bugs. This should be done only when there is no other choice and with robust planning. Ensure that your organization has a robust architecture network in which the production servers are not adversely affected during patching. It is advisable to have redundant and HA systems because they can allow patching without any service disruption.

Development Systems

Development systems can be created by duplicating production systems. These development systems can then be patched to determine their performance after the update. Patching in development systems enables the full integration of patches into systems before further processes such as QA testing and application rollout.

For better product release, the DevOps team must evaluate the patches and integrate them into the product. The application of patches to development systems helps to identify functional errors or security issues caused by patching. If any problem is identified, it can be fixed easily. The main advantage of using this method is that patching does not affect the production systems or services; thus, it is a preferred method.

Quality Assurance

It is the responsibility of the software vendor, organizational staff, and cloud provider to validate updates to determine the performance of patches in the production environment. Quality assurance is an important tool that helps to verify the operation of an applied patch in a test environment and then estimate its performance in production.

Establish a quality assurance testbed to test a particular patch in your environment to determine dependencies, concerns with interoperability, and understand if the patch update can resolve the problem experienced by the organization. This will help in fixing the issue that may arise and make improvements. The testbed or testing environment must closely simulate the production environment and facilitate software compatibility testing.

It is essential for the software vendor that developed the patch to perform a full suite of QA tests of the patch package to verify whether the patch fixes the problem or issue for which it was designed. In addition, the vendor can use QA tests to evaluate if other processes are getting

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

affected by the applied patch or the patched version of software is experiencing any buffer or memory issues.

Perform Rolling Updates

Rolling updates are small and frequent updates that are performed sequentially. In rolling updates, software patches or updates are delivered constantly to applications or OSes. Because updates are delivered continuously, this patching method is also known as continuous delivery or rolling releases.

These updates are common in Linux and are delivered mostly as a package that can be accessed remotely over the internet. In rolling updates, one system will be patched at a time; after the first system is patched, the next system will be patched. Because updates are installed on one system or server at a time, the rolling updates method reduces application downtime and avoids unexpected errors in software updates.

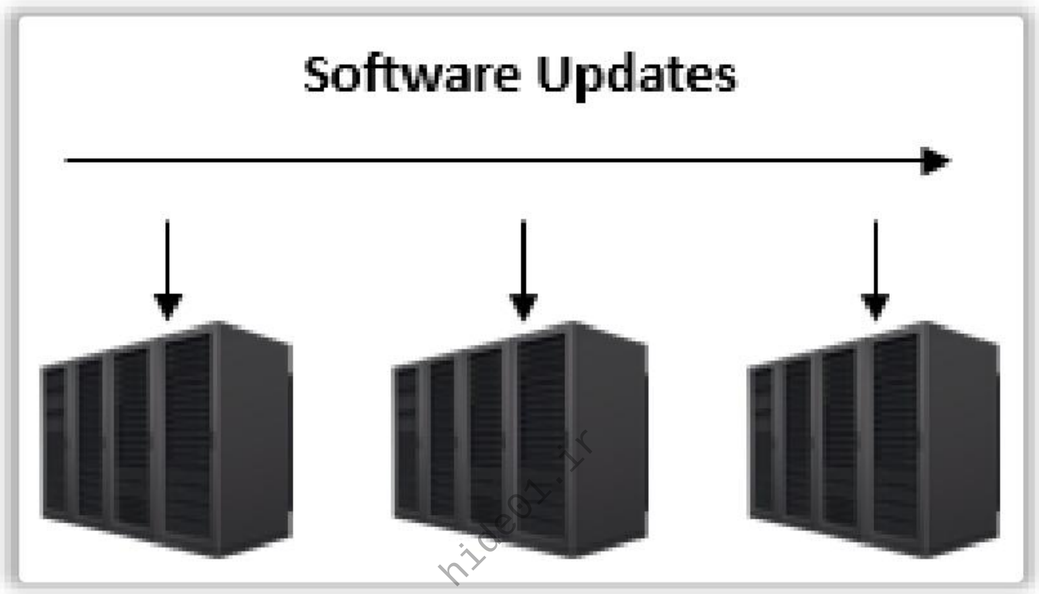


Figure 5.29: Rolling updates

The rolling updates method may include a testing phase in which only limited test traffic is directed to the patched server by the load balancer to confirm that the update is working as intended. Once the software is successfully tested in one server, the server assumes the service, and another server is taken offline and patched. This continues till all servers are patched and tested successfully.

Blue-Green

In the Blue-Green methodology, two identical configurations are used in the production environment; one environment is referred to as Blue and the other as Green. Each configuration can handle the full workload independently without the support of the other configuration. Either (Blue or Green) configuration can serve as the active configuration while the other will be on standby.

The Blue-Green deployment method ensures that user traffic is served continuously in production with reduced risk and downtime. Because one environment is active while the other is inactive, the software and security patches can be updated on the inactive side. After the updates or patches are applied, the inactive side can be made functional if no issue occurs owing to the application of new updates. The previously active side must be made inactive once the newly patched side is live. Then, the same updates must be applied to this side.

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

Even though every time one side is active and serving traffic, updating the inactive side does not affect the active side; thus, thorough testing can be performed on the inactive side before making it active. For new application deployments in critical implementations that require high availability, the Blue-Green method works efficiently. With this approach, rollbacks are fast and easy. The major drawback of this approach is that it requires numerous servers because the standby side should have the same number of servers as the active side to manage resources.

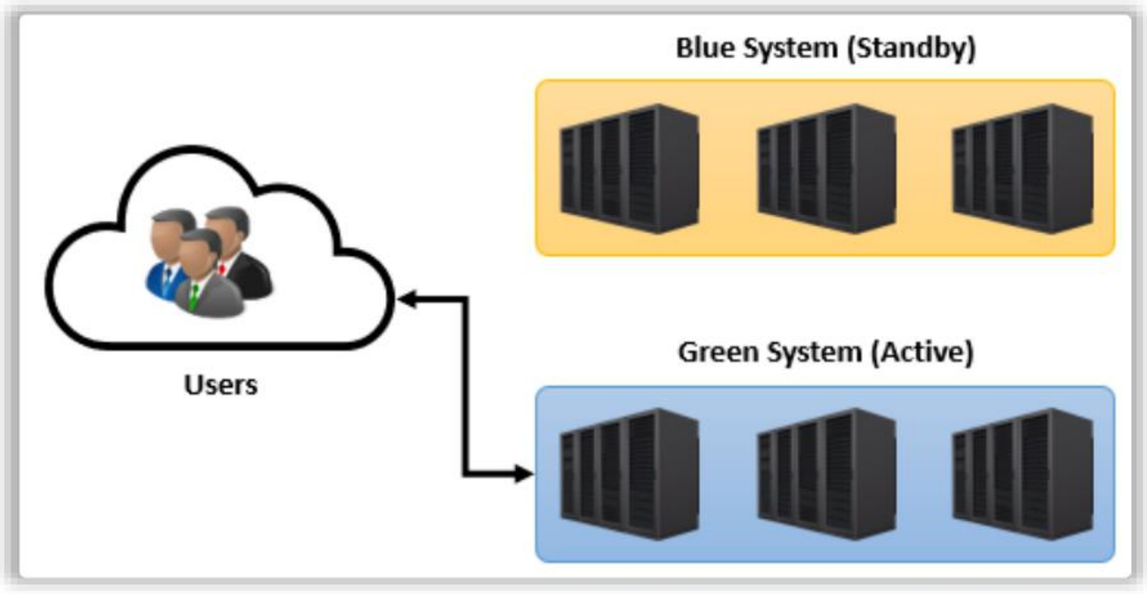


Figure 5.30: Blue-Green deployment

Clustering and Failover

A cluster refers to a collection of servers that are interconnected and operate as a single large system. Clusters can be managed as a single larger system rather than several smaller interconnected servers. This helps in simplifying operations via a central point of management.

Cloud admins can manage a cluster in the same way as a single large system without worrying about individual systems. Patching is easier with clusters because it eliminates the need for applying updates or patches separately to individual systems. Security patches or updates can be installed on the master nodes of a cluster and they will push and install the patches or updates on all systems in a cluster.

When a cluster is fully functional, upgrades can be implemented without affecting its operations. The devices grouped together in a cluster provide high availability for services and applications. If any node in the cluster fails, another node takes the operational functionality of that node without any downtime.

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

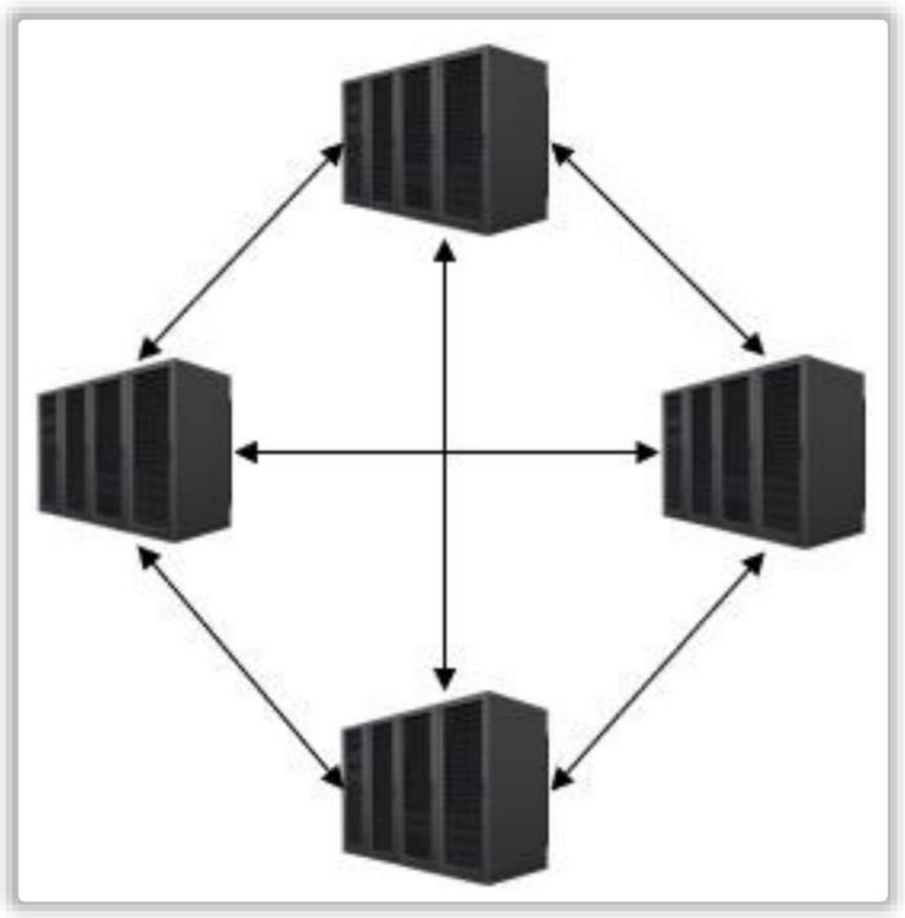
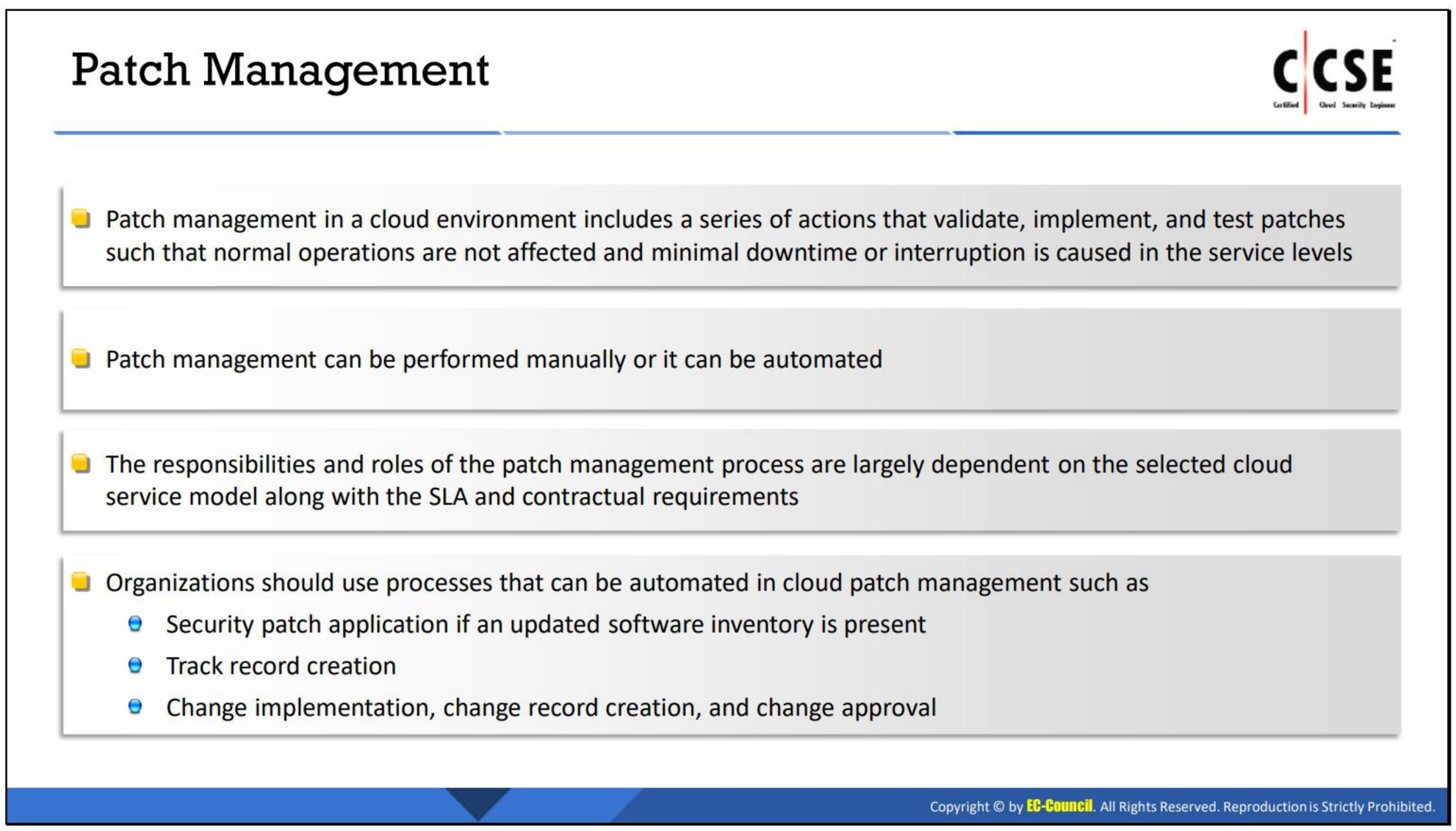


Figure 5.31: Cluster updates on servers with no downtime

hide01.ir

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



Patch Management

Regular patching is essential for the software and firmware of cloud hosts and servers to ensure cloud operational security. Patching helps in fixing bugs, solving stability issues, fixing security vulnerabilities, and introducing new features. Patch management in a cloud environment includes a series of actions that validate, implement, and test patches in a way that does not affect normal operations and causes minimal downtime or interruption in service levels. It is performed repeatedly to track new patch releases, verify hosts that require them, test the patches, install them, and verify the working of hosts after patch application.

Within a logical or virtualized environment, the responsibilities and roles of patch management are largely dependent on the selected cloud service model as well as the SLA and contractual requirements. Cloud customers are responsible for patching in IaaS cloud service models. In PaaS models, cloud providers are liable for patching with the coordination of customers. For SaaS cloud models, cloud providers are responsible for patch management.

The patch management process can be manual or automated. Manual patch management involves IT admins applying patches to systems, applications, and network equipment manually, which is more time consuming (hours or days) for huge organizations. Organizations can automate the application of patches using specific tools such as Faronic's Deep Freeze Cloud, ManageEngine Patch Manager Plus, and SolarWind's Cloud Patch Management Software.

The processes that can be automated in cloud patch management include

- Security patch application if an updated software inventory is present
- Track record creation
- Change implementation, change record creation, and change approval

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

- Verification of the implementation of patches
- Creating documentation after successful implementation of patches

Patch Management Cycle in Cloud

The patch management cycle involves the following phases.

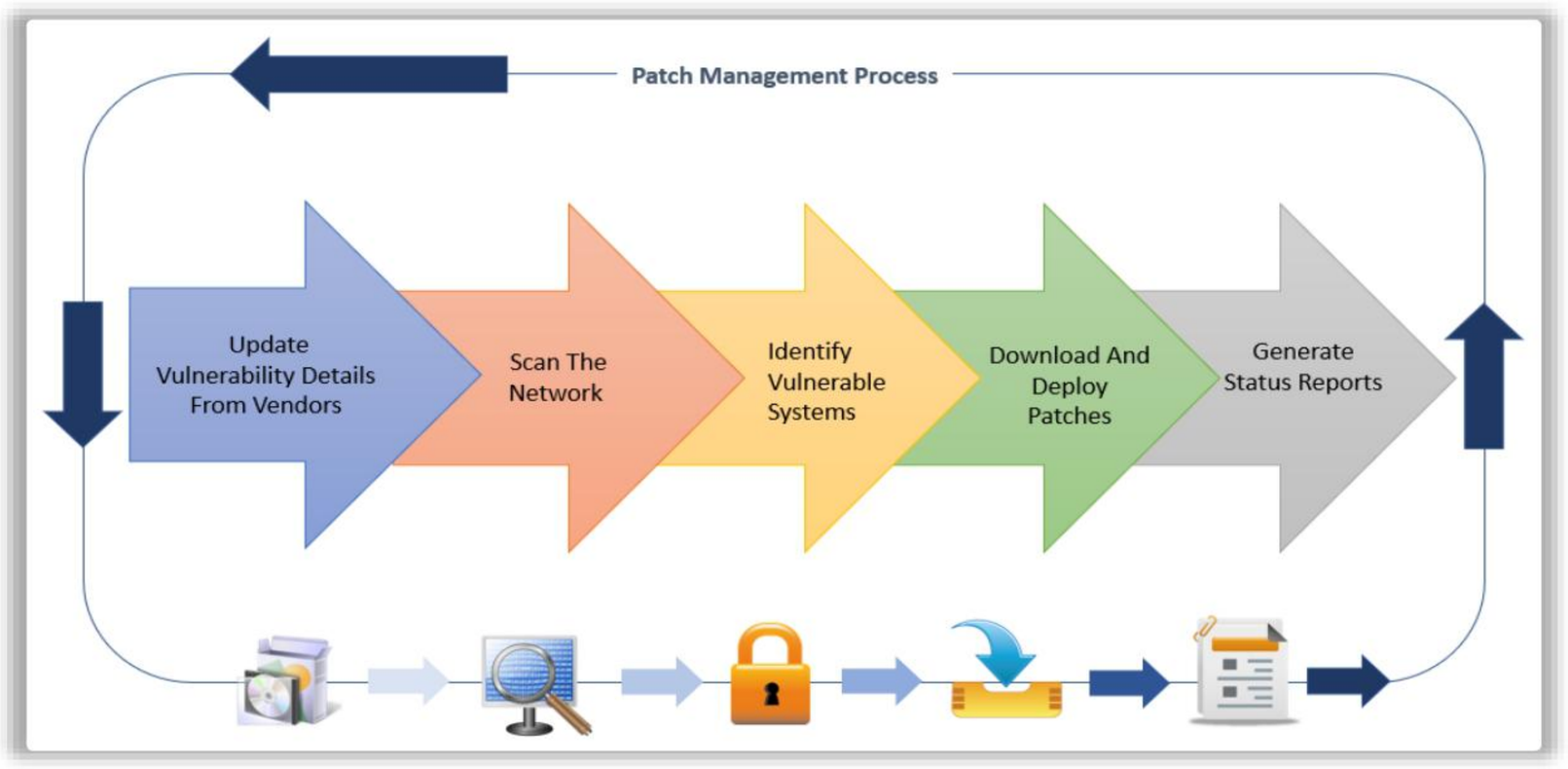


Figure 5.32: Example patch management process

Example of patch management process

- **Identification**: Being aware of new patches is the first step in patch management. Identify the cloud hosts and servers that require patches. Vendors send notifications to security personnel whenever new patches are introduced. They have a separate notification mechanism to notify the release of new patches and the components included in them. Based on this information, organizations can effectively implement patches. A well-established patching cycle at regular intervals helps in including new patches. However, organizations should apply security patches that are immediately required to prevent vulnerabilities from being exploited. It is important to have well-established and documented procedures even for emergency patching. A vulnerability scanner can be used to highlight new vulnerabilities in cloud systems and servers. The hosts and network should be scanned to detect any new, unpatched vulnerability.
- **Acquiring**: Acquire patches for software and systems from respective vendors. Patches are of different forms depending on software implementation and vendors. Usually, they come in a downloadable format such as ZIP files, script, proprietary format, or binary executable. Patches can also be directly downloaded and applied on cloud hosts and servers by the patching utilities of vendor systems. This approach is not good for the security setup and must be avoided because it requires hosts and servers to have open outbound connectivity via the internet to outside systems that are not in the organization's control.
- **Implementation**: Once patches are acquired and evaluated, they should be applied to a non-production environment to check their performance and impact on that

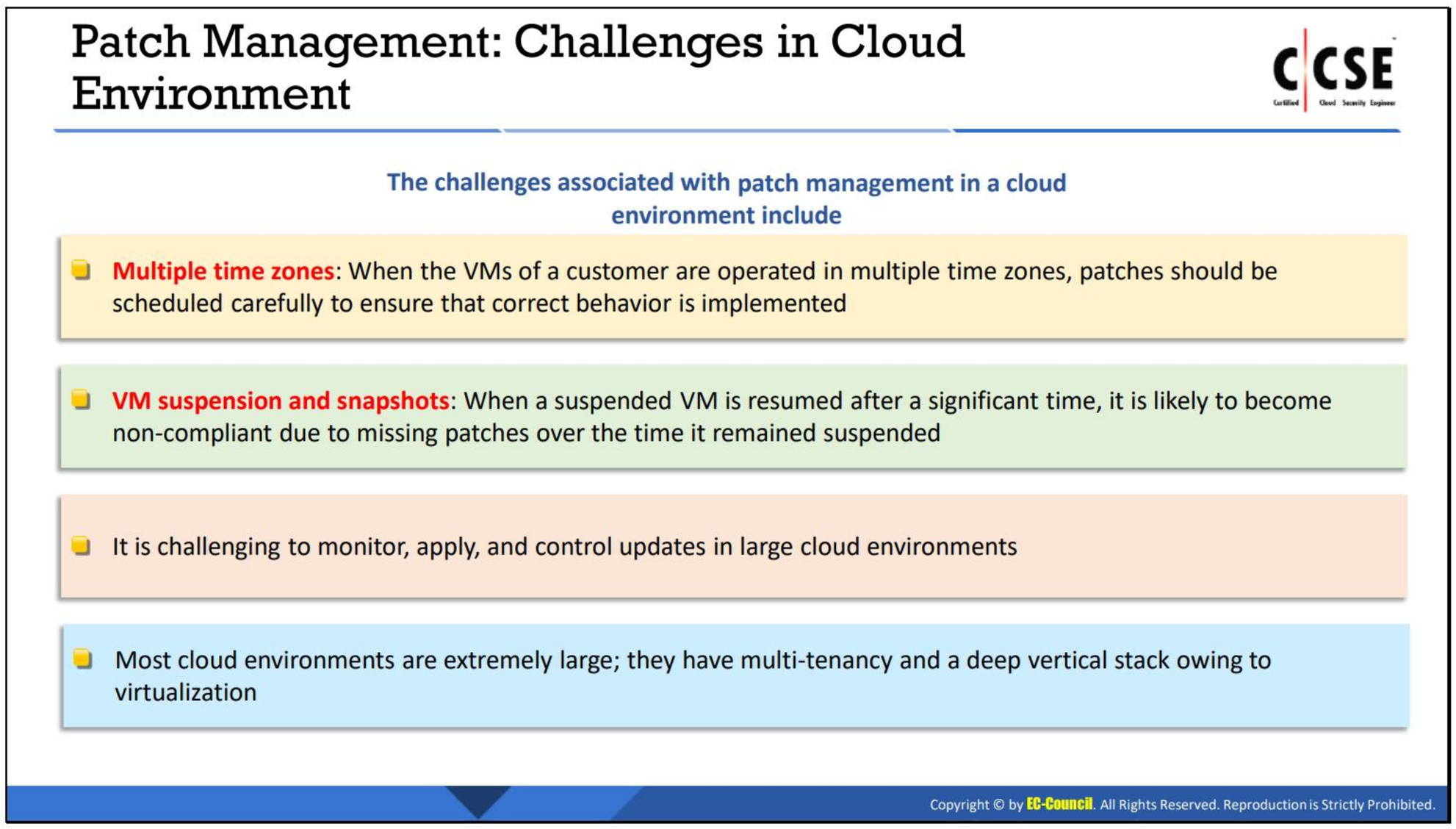
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

environment. Only after thorough testing in the non-production environment, they can be applied to a production environment. Monitor the implementation and successful completion of patches in the cloud where automated software utilities are responsible for implementation.

- **Validation and verification**: Validate and verify the applied patches. Use vendor instructions or documentation for particular patches while validating and verifying them. Several software vendors provide instructions or documentation and patches that must be used while validating and verifying the patches. After successful validation, ensure that cloud applications and software work as intended. Generate status report after completing the patch management process.

hide01.ir

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



Patch management: Challenges in Cloud Environment

It is challenging to monitor, apply, and control the updates in a large cloud environment. Usually, cloud environments are huge, have multi-tenancy, and a deep vertical stack owing to virtualization.

hide01.ir

VMs can be used in various time zones. Patch scheduling on VMs can interrupt the maintenance of the physical infrastructure of data centers because VMs run on hypervisors. Additionally, a snapshot of a VM can be taken by a customer to restore the VM from that snapshot in the cloud environment. From the perspective of patching, it is challenging to restore a VM from its snapshot because a compliant VM that is being restored from a previous snapshot can become non-compliant.

Following are the important challenges associated with patch management in a cloud environment:

- **Multiple time zones**: In a cloud environment, customers can use VMs from various time zones throughout the world. When the VMs of a customer are operated in multiple time zones, patch scheduling should be carefully performed to ensure that the correct behavior is implemented. The correct behavior, for some patches, involves the application of these patches at the same local time of each VM. For example, applying the MS10-071 update from Microsoft to all Windows machines at 12 am of their respective local time. The correct behavior for other patches is to apply them simultaneously to prevent the mixed-mode problem, which results in data corruption.
- **VM suspension and snapshots**: In a virtualized environment, users and administrators can perform operations such as snapshot, revert, VM suspension, and resume. The management console through which users can perform these operations should be

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

closely integrated with the compliance processes and patch management. Failure to do so can make a VM non-compliant unexpectedly. For example, when a suspended VM is resumed after a significant time, it is most likely to become non-compliant due to missing patches over the time it remained suspended. Similarly, baselining a VM to the latest patch is necessary before the VM is reverted to an earlier snapshot.

hide01.ir

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

Applying Security Patches

- The key elements in a cloud environment that require patch installation to mitigate security issues are as follows:

Hypervisors

- Before performing patching on a hypervisor, migrate every VM on the hypervisor to another server to prevent operation disruption
- After migrating all active services from the hypervisor to another server, initiate patching on the hypervisor while it is offline
- Periodically update the hypervisor code to address security vulnerabilities and add the latest functionalities and features

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

Applying Security Patches (Cont'd)

hide01.ir

Virtual Machines

- Use automation software to patch VMs
- Cloned images and snapshots can be utilized to create a master copy of the VM with the necessary patches installed and tested

Virtual Appliances

- Virtual appliances can be managed by the CSP; therefore, it is the responsibility of the CSP to update the managed virtual appliances
- The virtual appliance vendor offers security and patch management

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

Applying Security Patches (Cont'd)

Network Systems

- Many CSPs provide network systems such as firewalls, routers, DNS servers, IDSs/IPSs, and load balancers as managed services; CSPs also allow cloud consumers to install and manage systems by themselves
- The entity with control over the system is responsible for updating the device with the latest security patches

Applications

- Configure automation software such as Chef or Puppet to patch applications
- Run automated scripts on the server to check and update the latest security patches
- If you purchase a SaaS solution from the CSP, it is the responsibility of the provider to secure and update the application with the latest patches
- If you developed the application internally or run it on IaaS/PaaS, it is your responsibility to secure and update it with the current patches

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

Applying Security Patches (Cont'd)

hide01.ir

Storage Systems

- Cloud storage systems are redundant and facilitate the application of latest security updates and patches
- One part of the storage system can be removed for temporary offline maintenance and the backup system performs all operational functionalities

Clusters

- All clusters are created for high availability and patches can be easily installed on a cluster with zero downtime
- Based on the capabilities of the cluster software, every component in a cluster can be taken offline
- The individual system of a cluster can be easily updated with security patches while the entire cluster remains functional

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

Applying Security Patches

All software programs have bugs that can be exploited by attackers to launch attacks. When a new bug is identified, its details soon become public. When attackers gain information about the bug, they try to exploit it for personal gains.

Organizations must assign patch management the top priority and incorporate a planned approach toward it. CSPs are liable for securing the cloud infrastructure as per the shared

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

responsibility model, and the customer organization must address security issues based on the selected cloud service model. To prevent security breaches, the organization must develop, implement, and adhere to a comprehensive patch management approach.

Cloud Element Security

Various cloud elements require patches for security. The key elements in cloud environments that require patch installation to alleviate security concerns are as follows:

Hypervisors

Hypervisor (also known as VMM) is the most important component of a cloud IT system because it enables several VMs to run concurrently on the host computer. Like any other IT infrastructure component, hypervisor also possesses vulnerabilities that require periodic patching. Therefore, organizations that use virtualization or cloud computing must incorporate hypervisor security updating/patching into their patch management process.

Hypervisor is responsible for providing a virtual operating platform to various VMs and monitoring them to ensure that they are working as intended. Because multiple VMs are deployed on a single host in a cloud environment, hypervisor security concerns (such as different forms of attacks) are increasing. If the hypervisor is compromised owing to any vulnerability, attackers can easily access all VMs running on it along with their data.

Guest OS or VMs do not have any indication to know that they are operating on a compromised hypervisor without strong security controls. Patching a compromised hypervisor is the only way to secure the entire virtual environment. The main challenge while patching the hypervisor is that updates to the hypervisor may adversely affect the VMs running on it, and in worse cases, the applied patches may bring the whole environment to a halt.

Because multiple VMs run on the hypervisor, the application of updates directly to the hypervisor while allowing the operation of these VMs is not advisable. This is because updates might affect the working of these VMs, which may result in unexpected business loss. Before performing patching on the hypervisor, migrate every VM on the hypervisor to another server to prevent any operational disruption.

After migrating all active services from the hypervisors to another server, initiate patching on the hypervisor while it is offline. This ensures that any patch/update applied to the hypervisor does not affect the services that were running on the hypervisor and they can run without causing any problem on another server.

Periodically update the hypervisor code to address security vulnerabilities and add the latest functionalities and features. This will help in keeping the system up to date, which in turn prevents the hypervisor and their VMs from encountering various security issues.

Virtual Machines

A VM comprises the software that includes the guest OS, hypervisor, and applications or workloads running on it. Like any other software, VMs also have security flaws, bugs, and performance improvements that require updates and patches to ensure that they are fixed and the VM performance is improved.

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

Ideally, there may not be a fixed schedule to apply patches on VMs or hosts. However, patches can be released by software developers on a regular basis and critical patches can be expected at any time. In a cloud environment, it is a challenge for IT professionals to determine the availability of patches and verify if they work or solve problems as expected.

Organizations must include VMs in their patch management process. To reduce the overhead of tracking patches and updates when they are available, use automation software to patch VMs. The automation of VM patch management ensures that patches are tracked, downloaded, implemented, and validated automatically. It is recommended to apply patches to VMs in a lab (test) environment to validate their functionality so that the patched VMs do not cause any problem or disruption when deployed in production. VMs that are patched without being tested in a test environment may cause service disruption or other performance issues that will affect the business.

Cloned images and snapshots can be utilized for creating a master copy of a VM with the necessary patches installed and tested. While updating VMs, these cloned images can be leveraged as master templates. Organizations must ensure that their cloud environments have updated and patched VMs because this will help them to keep their cloud environment secure.

Virtual Appliances

A virtual appliance refers to a VM image file that comprises a preconfigured OS environment and one application. Virtual appliances contain the preconfigured software stacks required by applications for smooth operation. They simplify the delivery and operation of applications. Software vendors use virtual appliances to distribute their products to customer organizations because these appliances can be deployed easily in private data centers as well as public clouds. However, most vendors have outdated or unpatched software components in their virtual appliances.

Moreover, virtual appliances must be kept up-to-date and patched like other software components. Virtual appliances run on Linux; thus, they have their own vulnerabilities and flaws that require proper patch management. Virtual appliances can be managed by CSPs; therefore, it is the responsibility of CSPs to update all managed virtual appliances. In cloud computing, vendors of virtual appliances that offer firewalls, IDS/IPS, or load balancers license their products to customer organizations. Thus, the organizations become responsible for maintaining these appliances. However, several vendors sign support agreements with customers, allowing them to access their technical support teams, vendor support forums, and software updates.

Various virtual offerings exist for different organizations. Each virtual appliance vendor has its own patch management and security offerings depending on its product offerings.

Network Systems

Similar to traditional IT infrastructures, the cloud infrastructure also consists of various network systems that help in ensuring its security by protecting from several types of cyber threats. Network systems also have vulnerabilities, flaws, and other performance issues that should be patched or updated to ensure that they continue their secure and smooth functioning.

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

Many CSPs provide network systems such as firewalls, routers, DNS servers, IDSs/IPSs, and load balancers as managed services. CSPs also allow cloud consumers to install and manage the systems by themselves. The entity with control over the system is responsible for updating the device with the latest security patches. This implies that if network devices are controlled by organizations, they are liable for handling all maintenance and patch management processes, and if organizations use these systems as a part of managed services provided by CSPs, the providers are responsible for maintenance and patch management.

Because most network elements reside at the core of the cloud fleet of servers and data pass through them, it is essential to keep them updated and patched to prevent them from being exploited or compromised. Failure to keep them patched and updated will lead to compromised network, which will allow attackers to attack all systems present on the network.

Applications

Similar to any software product, vulnerabilities and security issues are present in cloud applications as well that must be timely patched to prevent them from becoming a target by attackers. In the context of cloud computing, there are different levels of responsibilities and control for SaaS and PaaS/IaaS.

- **Patching in SaaS**

  If you purchase a SaaS solution from a CSP, it is the responsibility of the provider to secure and update the application with the latest patches. The provider handles all application maintenance tasks (including patching) and updates users with the end results. Because patch management in SaaS is vendor-driven rather than customer-driven, customer organizations face fewer or no issues with patch management. Thus, the provider decides and manages SaaS application patches to address security concerns, new features, or performance issues.

- **Patching in PaaS/IaaS**

  If an organization develops an application internally or runs the application on IaaS/PaaS, then the organization is responsible for securing and updating the application with the current patches. In PaaS, the application is controlled by the organization but the OS or hypervisor stack is controlled by the provider. System admins perform patch management functions in PaaS.

Most applications can ensure that they are up to date by automatically checking with a central repository. If they are not updated, they will download and install the updates or notify users or admins that updates are available so that they can handle the process further. This is possible with automation software that allows the automation of the patch management process. Applications can be patched by configuring automation software such as Chef or Puppet. Additionally, automated scripts should be run on the server to check and update the latest security patches.

Storage Systems

Various elements of cloud storage systems such as SAN FC (Storage Area Network Fibre Channel) switches, host bus adapters, storage controller heads, and RAID controller software require

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

updates and patches, similar to other systems that run on software. Storage systems are critically important because they must provide constant uptime for cloud servers.

Cloud storage systems are redundant and allow the application of latest security updates and patches with ease. Redundant storage is required, especially when some part of the storage system has security flaws or vulnerabilities that must be patched. Redundant storage helps to keep the storage services running during patching to provide constant uptime.

While patching a part of the storage system, services running on that part are temporarily transferred to another part of the system (backup system). Then, that part of the storage system can be taken out for temporarily offline maintenance and the backup system will perform all operational functionalities. This ensures no service disruption while applying patches or updates to storage systems.

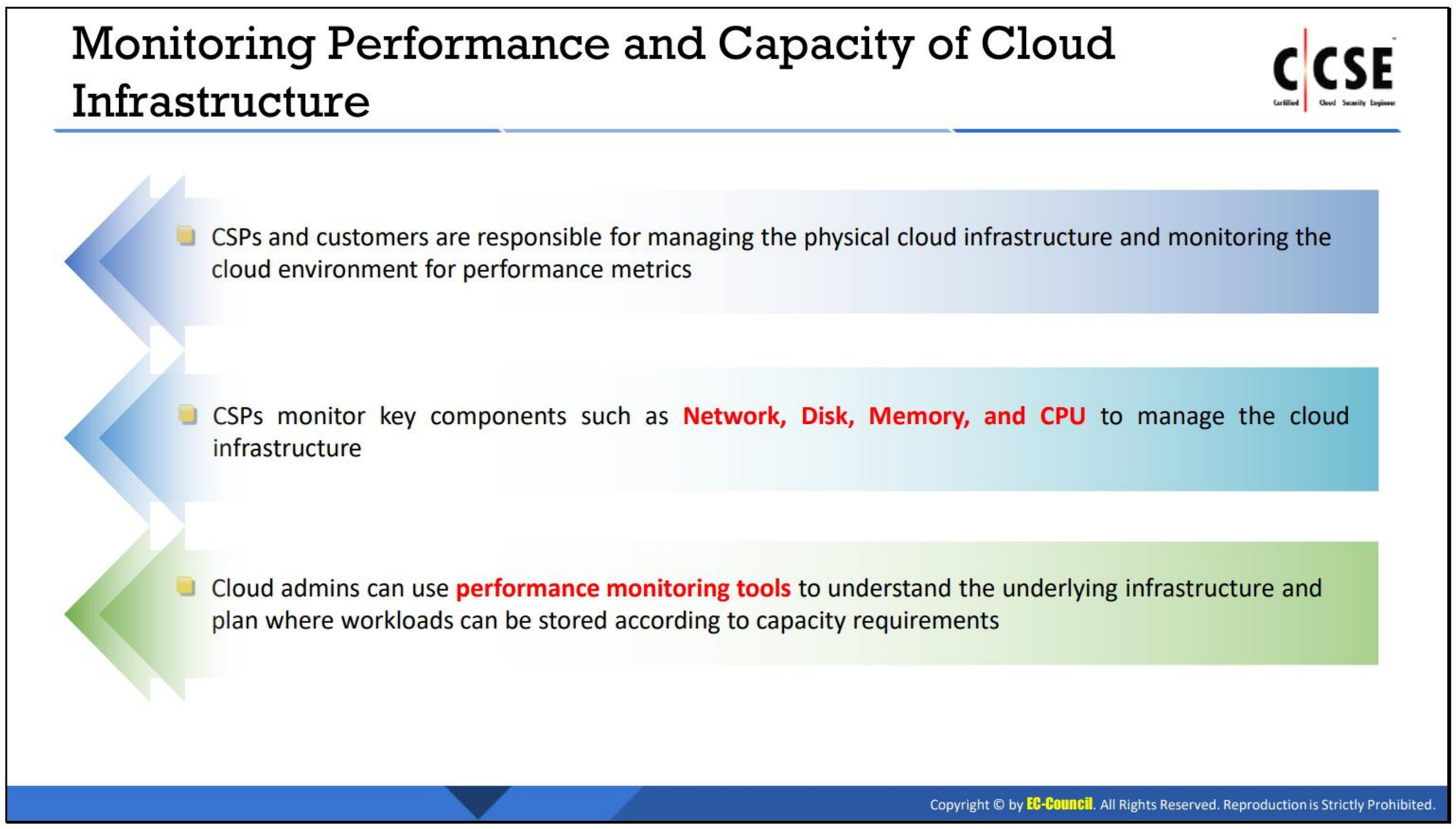
Clusters

A group of servers or computers that are interconnected via a LAN is called a cluster. Updating or patching individual systems is time-consuming, difficult, and may cause downtime. The use of clusters can help address these issues. Depending on the solutions that clusters are designed for and their use cases, clusters can be configured in various topologies.

All clusters are created for high availability and patches are easily installed on them with zero downtime. Patches and updates can be applied to individual systems present in a cluster. Based on the capabilities of the cluster software, every component in a cluster can be taken offline. This eliminates the need for taking the entire cluster down. Thus, each system of the cluster can be updated easily while the entire cluster remains operational.

Alternatively, IT admins can use the master or controller node to perform upgrades. With the help of cluster management software, they can upload a patch to the controller node in a cluster and apply it to all systems internally.

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



Monitoring Performance and Capacity of Cloud Infrastructure

While managing the physical cloud infrastructure, it is the responsibility of the CSPs and customers to monitor the cloud environment for performance metrics. Performance metrics are important components of the contract between cloud consumers and CSPs. The performance capabilities of virtualized resources depend on the underlying physical infrastructure. This makes performance monitoring important for cloud providers as well as customers. Cloud providers charge cloud consumers for the resources they request and use as per the selected service model; thus, proper resource allocation must be performed to ensure better performance. SLAs and contracts must contain detailed information about the resources to be allocated by the provider to the customer. This makes the provider accountable for their services and ensures that they remain compliant.

The important performance metrics related to the key physical components of the physical cloud environment include disk, CPU, memory, and network. Cloud providers must ensure that sufficient resources are provided to customers according to the SLA agreement, which should satisfy the present and possible future requirements as well. Moreover, the resources must respond with the acceptable reliability speed defined in the agreement. The key components that should be monitored to ensure cloud operational security are

- **Network**: Monitor the cloud network for excessive dropped packets.
- **Disk:** Monitor the disks of cloud servers for slow reads/writes to disks (IOPS) and full disk. In other words, monitor the response time.
- **Memory:** Monitor the cloud storage for exhaustion of allocated memory and excessive memory usage.
- **CPU:** Monitor the CPU of cloud servers for excessive CPU utilization.

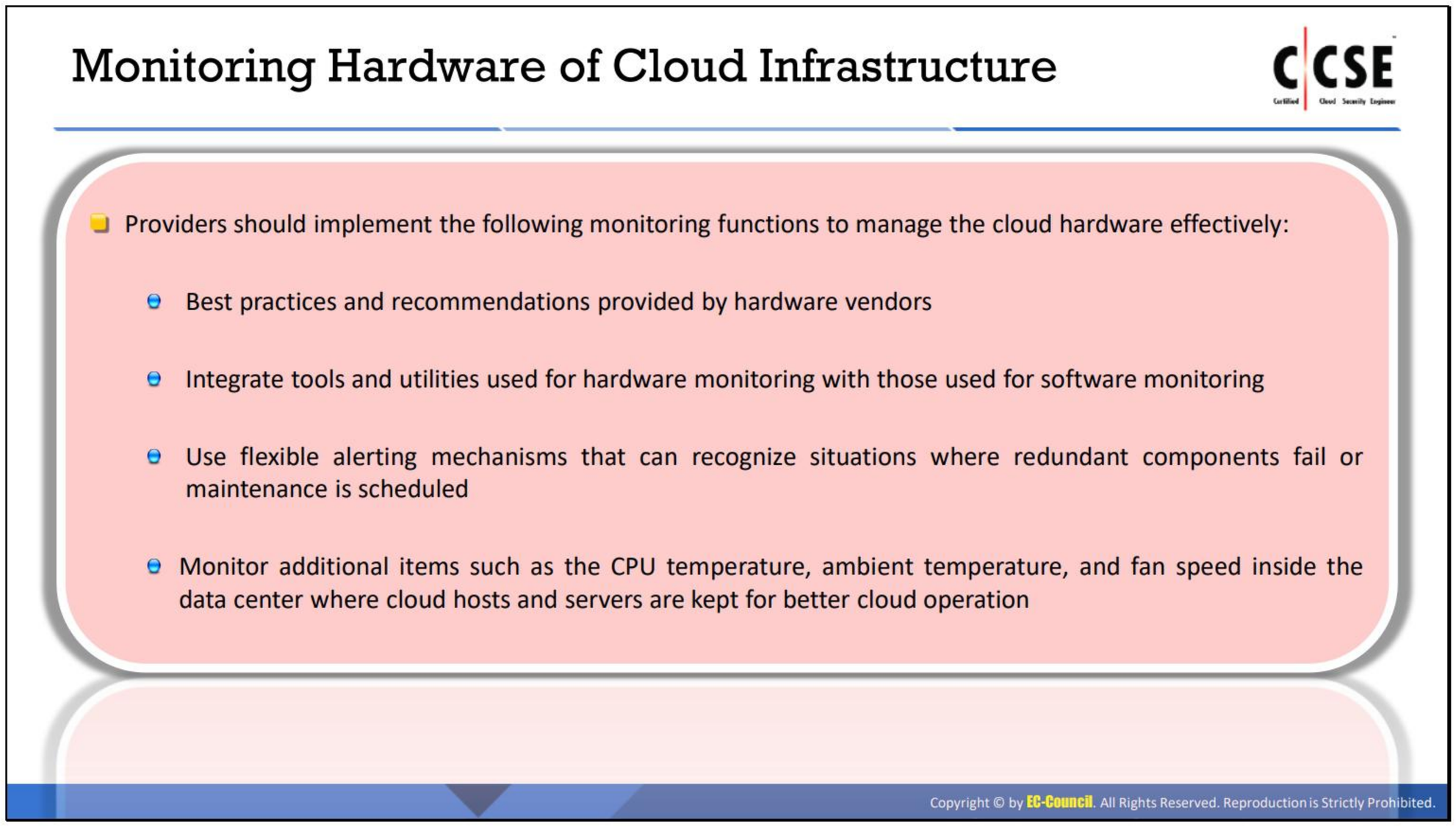
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

By considering these four key components, vendors of cloud systems and software establish their own set of monitoring capabilities, performance metrics, and security best practices for planning and implementation. The parameters and best practices set by vendors are crucial in setting the resource thresholds and planning for possible requirements and improvements. CSPs are responsible for supporting the current resource requirements of customers as well as providing potential growth and auto-scaling. Here, auto-scaling helps in meeting demands when traffic loads increase suddenly. When there is an increase in traffic, capacity requirements will rise.

Performance monitoring is directly related to capacity management. Cloud admins can use performance monitoring tools to determine the underlying infrastructure and plan the storage of workloads based on capacity requirements. Capacity requirements often vary with business growth and other factors. Capacity management ensures that the IT infrastructure of an organization is capable of delivering the agreed SLA targets in a cost-effective and timely manner by considering all resources needed to deliver IT services. The capacity of cloud hosts should be monitored and some thresholds should be defined to prevent cloud hosts from reaching a situation in which their capacity is over-utilized.

hide01.ir

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



Monitoring Hardware of Cloud Infrastructure

Managing and monitoring the underlying physical infrastructure is important because it is responsible for running a cloud or virtual environment. The issues encountered by the physical cloud infrastructure are the same as those experienced by hosts in a traditional data center. Monitoring the hardware of cloud hosts is a part of performance monitoring and mainly involves monitoring the following important physical components and other parameters:

- **Network**: Monitor the cloud network for excessive dropped packets.
- **Disk:** Monitor the disks of cloud servers for slow reads/writes to the disks (IOPS) and full disk.
- **Memory:** Monitor the cloud storage for exhaustion of allocated memory and excessive memory usage.
- **CPU:** Monitor the CPU of cloud servers for excessive CPU utilization.
- **Fan speed**: Monitor the fan speed in cloud servers and hosts.
- **Ambient temperature**: Monitor the temperature of the data center where cloud servers are installed to keep it at an acceptable level.
- **CPU temperature**: Monitor the CPU temperature at an acceptable level to ensure proper cloud operations.

To manage the cloud environment effectively, providers should implement the following monitoring functions and redundant system architecture.

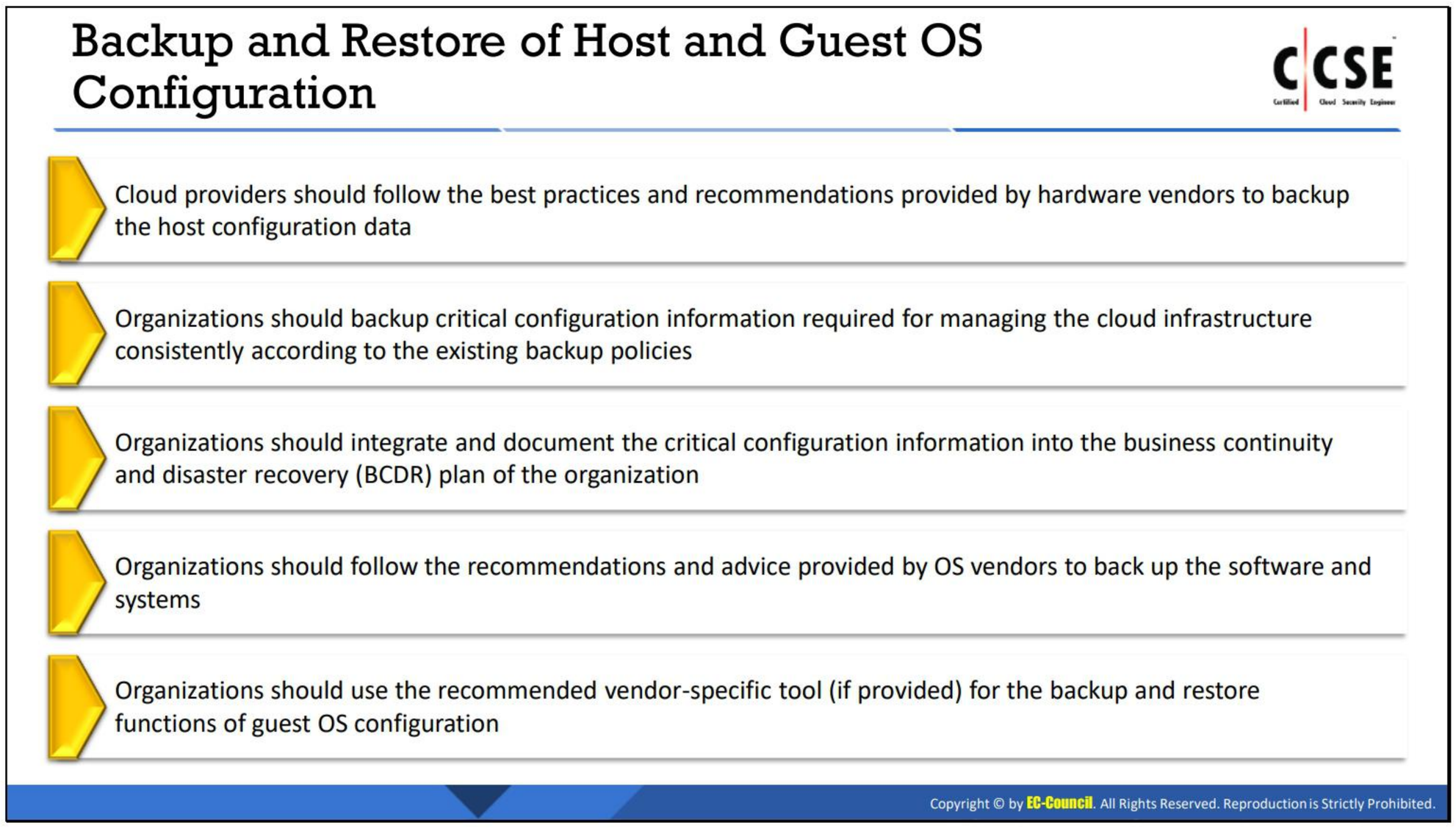
- Best practices and recommendations provided by hardware vendors.
- Use the tools and utilities provided by respective hardware vendors to monitor hardware.

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

- Integrate the tools and utilities used for hardware monitoring with those used for software monitoring. This provides a clear picture of the cloud environment and helps to manage it.
- Use flexible alerting mechanisms that can recognize situations where redundant components fail or maintenance is scheduled.
- Monitor additional items such as CPU temperature, ambient temperature, and fan speed inside the data center where the cloud hosts and servers are kept for better cloud operations.

hide01.ir

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



Backup and Restore of Host and Guest OS Configuration

The backup and restore operations inside a cloud data center must include configuration data along with other data. In a cloud environment, backing up configuration data is as important as backing up any other kind of data because configuration data are also valuable. Cloud providers should closely follow the best practices and recommendations provided by hardware vendors to backup the host configuration data. Vendors expose APIs or services that enable backup systems to capture configuration data to ensure that backups work smoothly and optimally with physical devices. Exposure of such information to any utility or service increases the risk of unauthorized access. Therefore, hardware vendors must thoroughly understand the parts that can be exposed and how to secure them.

Cloud consumers should negotiate with cloud providers about exposing configuration data based on their service model in the contract or SLA. The contract must clearly define the chances of any data exposure and the steps to ensure that systems exposing configuration data are properly secured and isolated from other systems or tenants.

Cloud security professionals must backup critical configuration information required for managing the cloud infrastructure consistently based on the existing backup policies of the organization. It is recommended to integrate and document this information into the business continuity and disaster recovery (BCDR) plan of the organization. Security professionals should understand their scope of access to hosts and accordingly implement configuration management. The important capabilities that will enable these operations include:

- **Control**: It refers to how confidently a security professional decides who (user) and what (applications) are allowed to access customer data and programs; accordingly, necessary actions (such as deleting data) are performed.

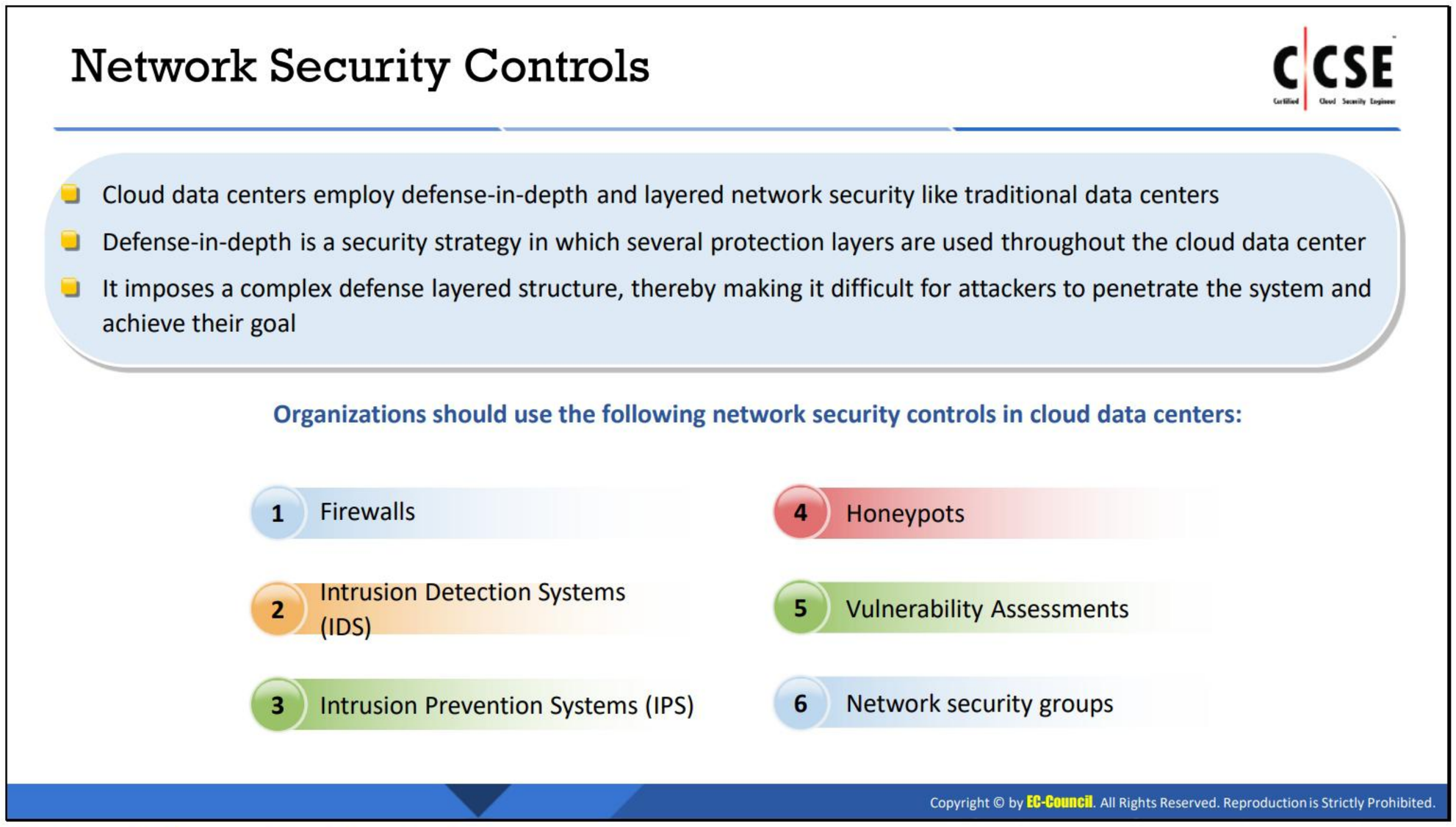
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Visibility**: It refers to the ability of a cloud security professional to confidently monitor the status of customer data and programs and how others access those data and programs.

For the backup of virtualized hosts or VMs, cloud security professionals may use any tool or utility, but they must ensure that backups are successfully performed and the restore process is tested successfully. The recommendations and advice for backing up software and systems provided by vendors should be followed and the vendor-specific tool (if provided) recommended by the vendor should be used to backup and restore the functions of guest OS configuration. If the security professional wants to use a third-part tool or utility, they must validate and support it independently because the OS vendor will not be liable for ensuring its success.

hide01.ir

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



Network Security Controls

Cloud data centers employ defense-in-depth and layered network security, similar to traditional data centers. A cloud data center is designed using a defense-in-depth strategy to ensure that all cloud operations and services remain secure.

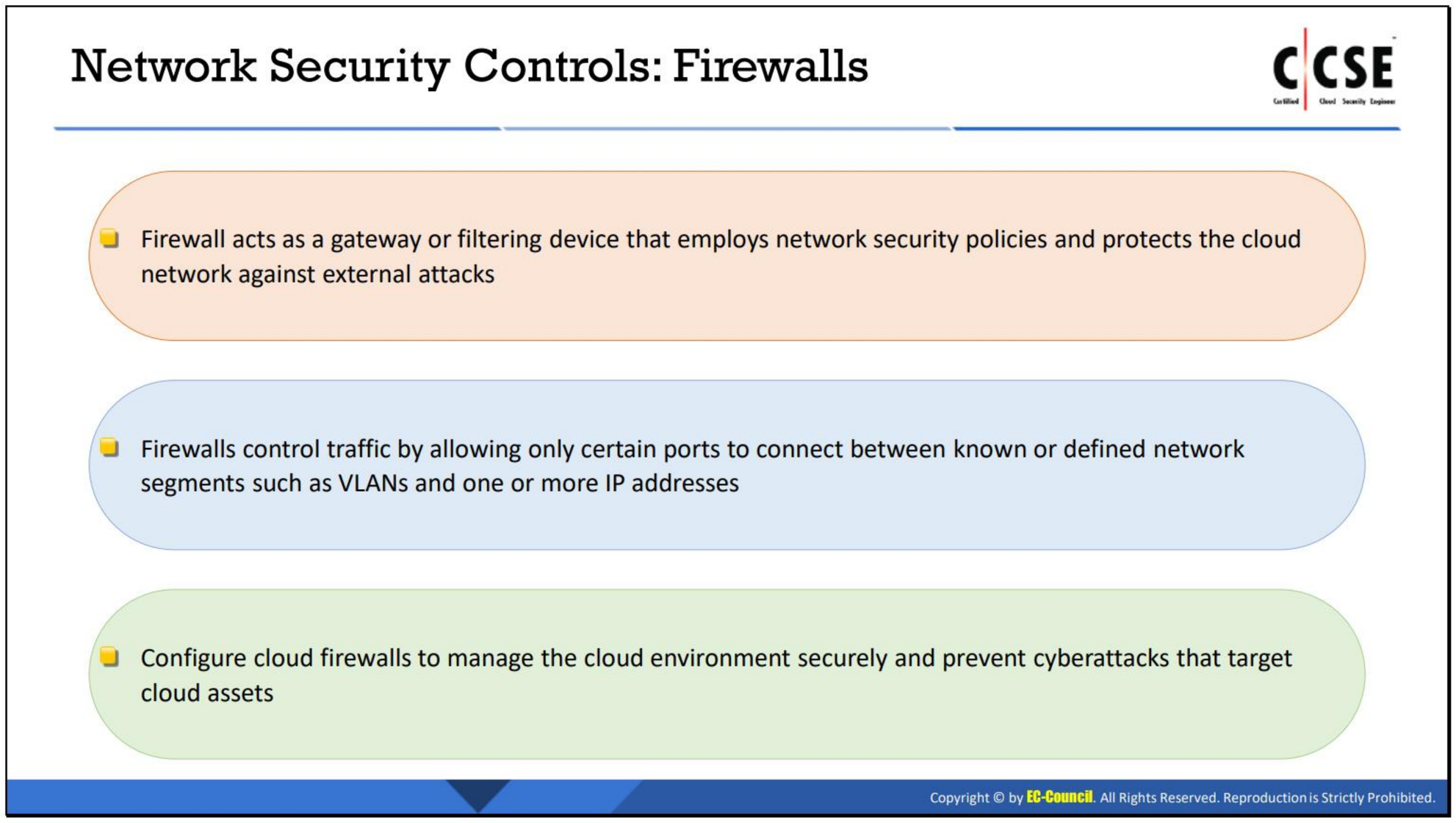
Defense-in-depth is a security strategy where several protection layers are used throughout the cloud data center. Defense-in-depth security involves implementing security controls at different layers of the cloud network stack. It imposes a complex defense layered structure, making it difficult for attackers to penetrate the system and achieve their goals.

Implementing one protection layer is not sufficient to prevent attacks in a cloud environment, but multiple layers of security can help prevent attacks. If an attacker successfully penetrates through a security layer, other layers will prevent them from exploiting the cloud network. A cloud environment can be accessed from any part of the world, thus making it an easy target for attackers. With defense-in-depth layered security, cloud security professionals can securely manage attacks in a cloud environment. It includes various security controls such as technical controls, physical controls, and administrative controls. Cloud security professionals must ensure proper data isolation and protection by testing and validating the VLAN implementations utilized by the cloud provider.

Following are some essential security controls used in cloud data centers.

- **Firewalls**
- **Intrusion Detection Systems (IDS)**
- **Intrusion Prevention Systems (IPS)**
- **Honeypots**
- **Vulnerability Assessments**
- **Network security groups**

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



Network Security Controls - Firewalls

A firewall is considered the first line of defense for an organizational cloud network. It acts as a gateway or filtering device employing network security policies and protects the network against external attacks. Firewalls are mainly used to control the traffic flow in a cloud environment according to the rules configured. They regulate the flow of traffic between trusted networks and untrusted networks. Firewalls help in keeping the cloud environment secure by restricting unauthorized access from external sources. Based on the needs and resources of a cloud environment, software or hardware implementations of firewalls can be used.

Inside a cloud environment, host-based or virtual firewalls are implemented. Virtual firewalls mostly work in the same manner as hardware firewalls. Host-based software firewalls are included with the OS from the vendor and provide additional protection to the hosts and VMs running on them. Firewalls inspect the network traffic and filter it based on the preconfigured rules. They control traffic by allowing only specific ports to connect between known or defined network segments such as VLANs and one or more IP addresses. For improved security of the cloud environment, both hardware- and software-based firewalls must be used.

- **Hardware firewall**: A hardware firewall is a dedicated firewall device placed on the perimeter of the cloud network. It can read the header of a packet to determine the source and destination address and compares it with a set of predefined and/or user created rules that determine whether it should forward or drop the packet.
- **Software firewall**: A software firewall is similar to a filter. It sits between the normal application and the networking components of the operating system. A software firewall implants itself in the key area of the application/network path. It analyzes data flow against the ruleset. It intercepts all requests from a network to VMs to determine if they are valid and protects the VMs from illicit attacks that attempt to access them. It

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

incorporates user-defined controls, privacy controls, web filtering, and content filtering to restrict unsafe applications from running on individual VM.

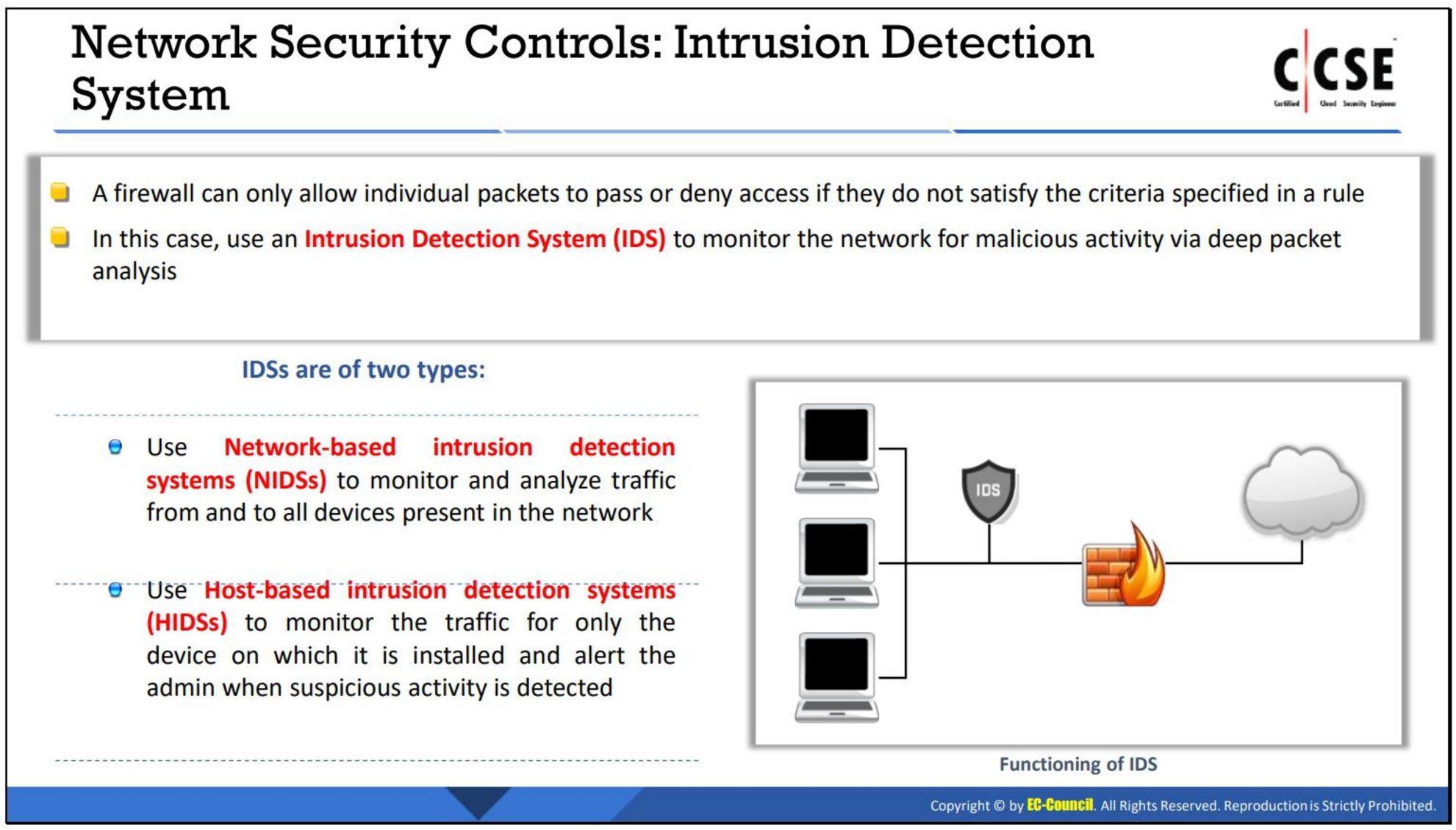
Cloud security professionals can configure the ports of cloud hosts via firewalls according to security requirements. They can use the rule-set configuration file to know the firewall rules and the relationship of each rule with the ports and protocols. Cloud firewalls should be configured to manage the cloud environment securely and prevent cyberattacks that target cloud assets.

Firewalls offer the following benefits in a cloud environment:

- Scalability
- Control network traffic
- Perform traffic logging
- Prevent malware attacks
- Filter protocols, services, and packets
- Provide secure access

hide01.ir

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



Network Security Controls: Intrusion Detection System

Relying solely on a firewall for network security can provide a false sense of security. A firewall is implemented in the IT security policy by allowing or denying traffic based on policy rules. It allows individual packets to pass through or denies access if they do not meet specific criteria specified in a rule. It does not check the content of legitimate traffic and allows based on a ruleset. Legitimate traffic may contain malicious content that is not evaluated during inspection by a firewall. In this case, use **Intrusion Detection Systems (IDSs)** for the deep analysis of packets to detect a broader range of cyber threats. IDS includes network security appliances used to monitor a network for malicious activity. Use an IDS in the cloud environment to analyze network packets, compare the packet content with a defined set of signatures or configurations, and receive notifications if threat is detected. However, IDS often generates false positives. Therefore, reduce the false positives by continuously evaluating IDS functions and tuning them.

IDS Benefits

An IDS can be used to

- Detect and alert if an intrusion is detected
- Monitor network traffic for malware or virus
- Log all unauthorized access attempts
- Record information about events
- Generate reports

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

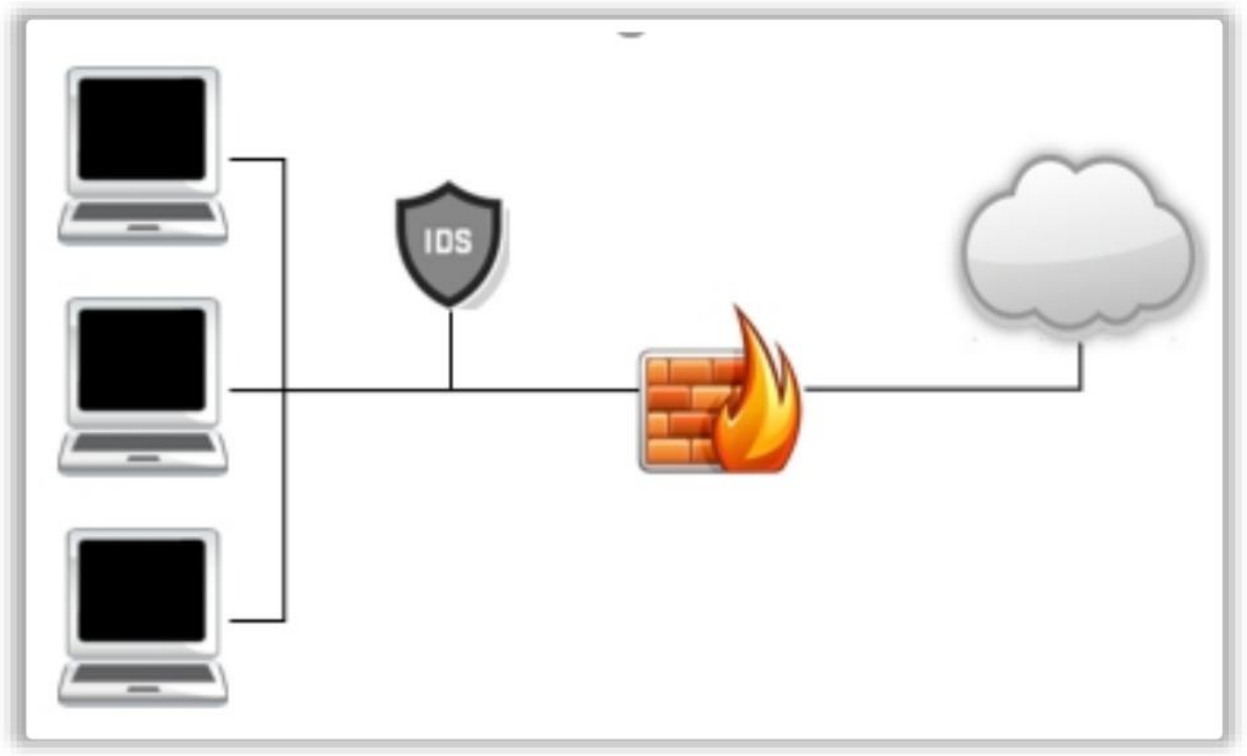


Figure 5.33: IDS Functioning

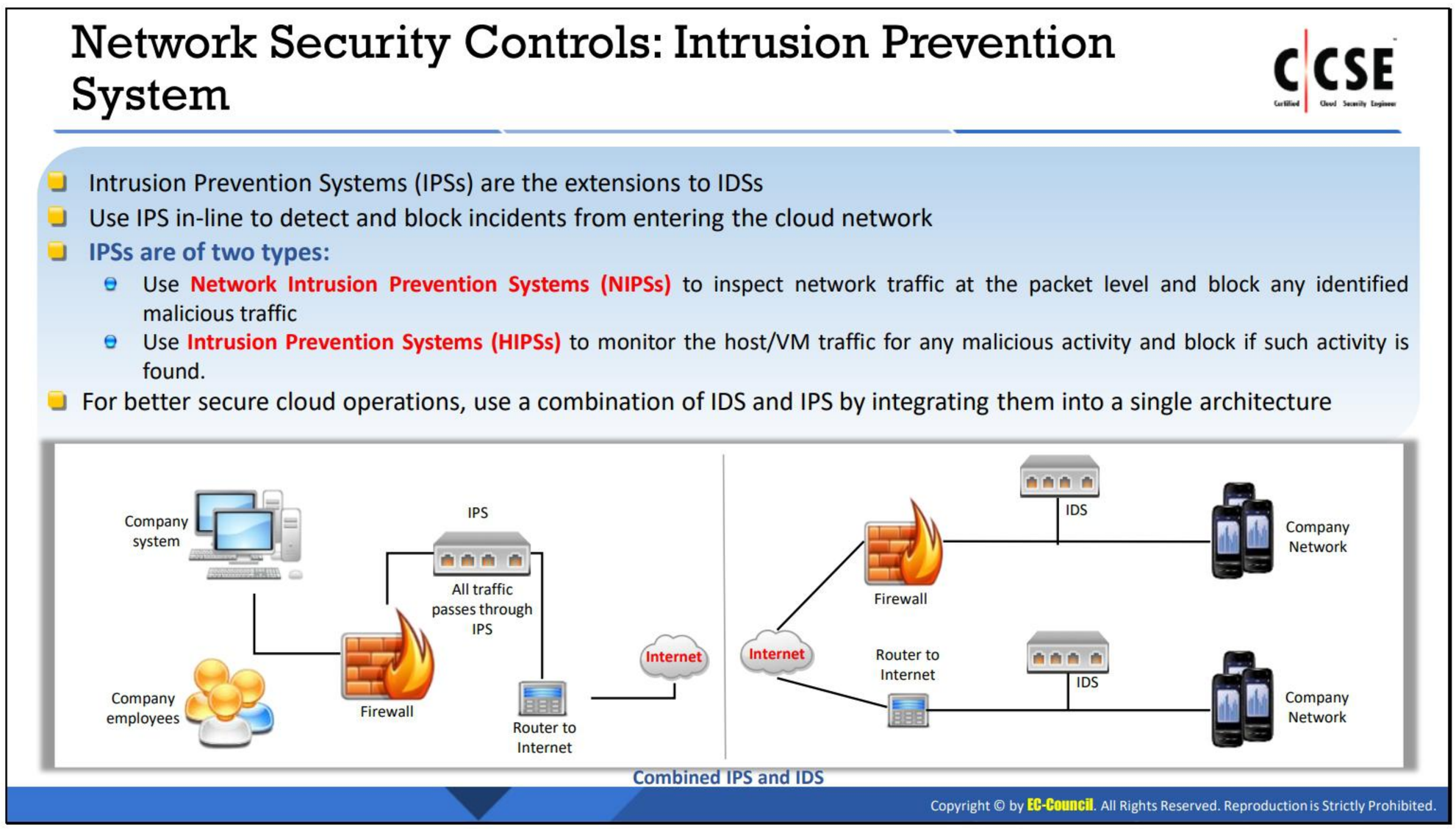
IDS Types

IDSs are of two types:

- **Network-based intrusion detection systems (NIDSs)**: NIDSs are security appliances that are installed at strategic points of a cloud network to monitor and analyze network packets for threats. Use NIDS systems to monitor and analyze traffic from and to all devices present in the network.
- **Host-based intrusion detection systems (HIDSs)**: HIDSs are installed on a single cloud host to monitor and analyze traffic for that particular host. This includes both inbound and outbound traffic. Use HIDS systems to
    - Monitor configuration files and critical system files for any modification
    - Monitor the traffic for only the device on which it is installed and alert the admin when it detects any suspicious activity
    - Check and compare previous snapshots of system files with the current system files to detect any modification
    - Send out alerts to the admin to investigate the issue if any modification is found
    - Use on mission-critical machines that have fixed or stable configurations
    - Detect any modification attempts or suspicious activity that originates from within the organization, unlike NIDS

ridel.ir

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



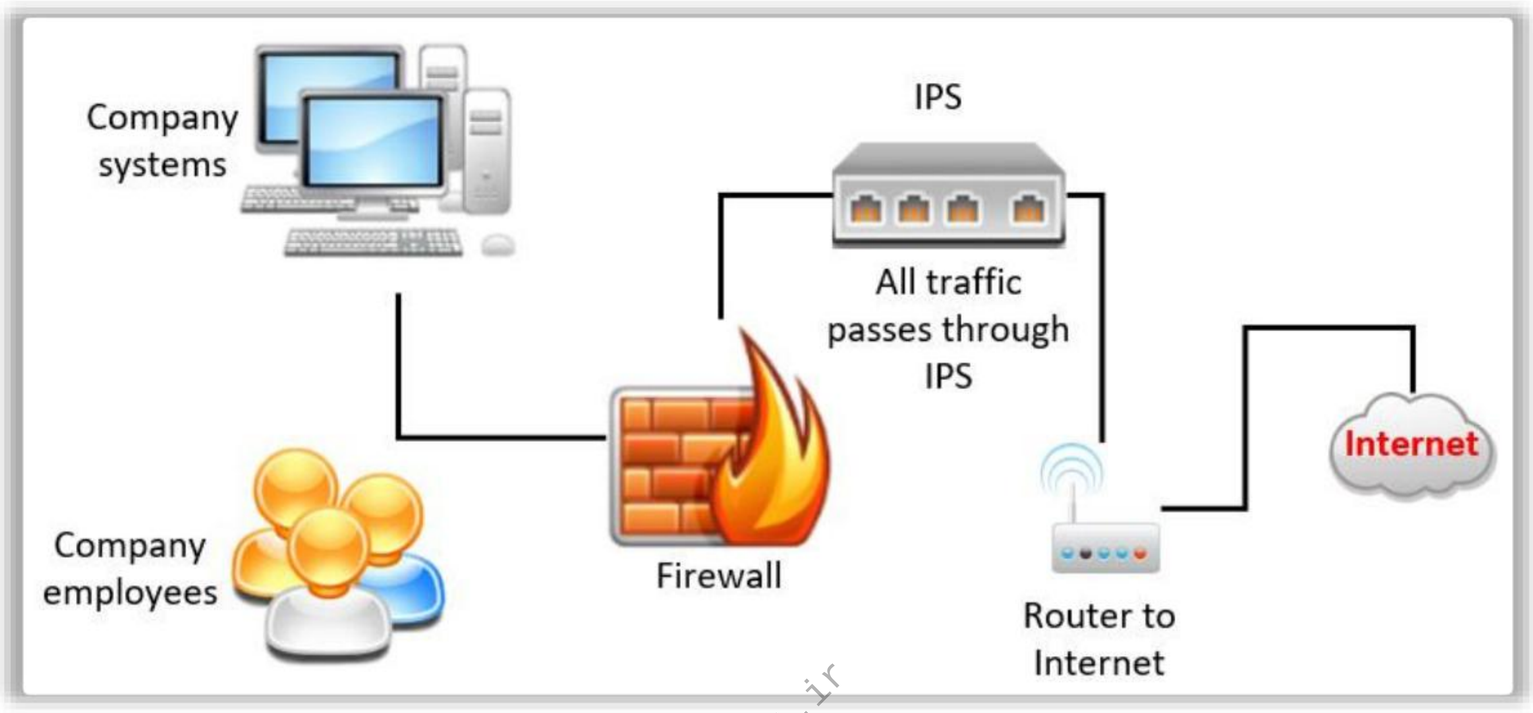
Network Security Controls: Intrusion Prevention Systems

Intrusion Prevention Systems (IPSs) are considered to be the extensions of IDSs. Unlike IDS, an IPS is placed in-line and detects any incident and blocks it from reaching the cloud network. An IDS can be used to identify and get alerts on intrusion attempts in the cloud. However, an IPS can be used to

- Detect and stop intrusion attempts
- Correct cyclic redundancy check (CRC) errors, defragment packet streams, TCP sequencing issues, and manage the options in the transport and network layers
- Analyze all inbound network traffic and decide whether a specific connection is allowed based on the packet content. If it is identified that a specific connection is malicious, then it will take predefined actions or generate alerts to notify users.
- Respond to a cloud security incident in two ways:
  - Make configuration changes to other cloud security controls such as router or firewall to prevent an attack; here, IPS can apply patches to hosts with certain vulnerabilities
  - Eliminate malicious packet content to prevent an attack
- Prevent OS fingerprinting attempts
- Defragment packet streams
- Drop identified malicious packets
- Reset a connection

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

- Block traffic from a malicious IP address
- Correct CRC errors
- Clean the transport and network layer options that are not required
- Prevent DDoS/DoS attacks
- Prevent attacks on the SSL protocol
- Ensure privacy of cloud users



hi1le01.ir

Figure 5.34: IPS setup

IPS Types

IPSs are of two types:

- **Network Intrusion Prevention Systems (NIPSs)**: NIPSs are installed at particular points on the cloud network to monitor and protect it from various threats. Use NIPSs to inspect network traffic at the packet level and block any identified malicious traffic.
- **Intrusion Prevention Systems (HIPSs)**: HIPSs are installed on individual hosts/VMs to monitor their activities and take necessary actions to detect any malicious behavior. Use these systems to monitor the host/VM traffic for any malicious activity and block if such activity is found.

Difference between IPS and IDS

The key difference between an IPS and IDS is that IPS is implemented in-line, but IDS sits off to the side. An IPS can be used to block the traffic directed through IPS or allow it depending on the configured policy. An IDS is connected via network tap and it monitors traffic but cannot act directly. Unlike IDS, IPSs are reactive in nature; thus, they are used to act automatically and immediately to prevent attack attempts.

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

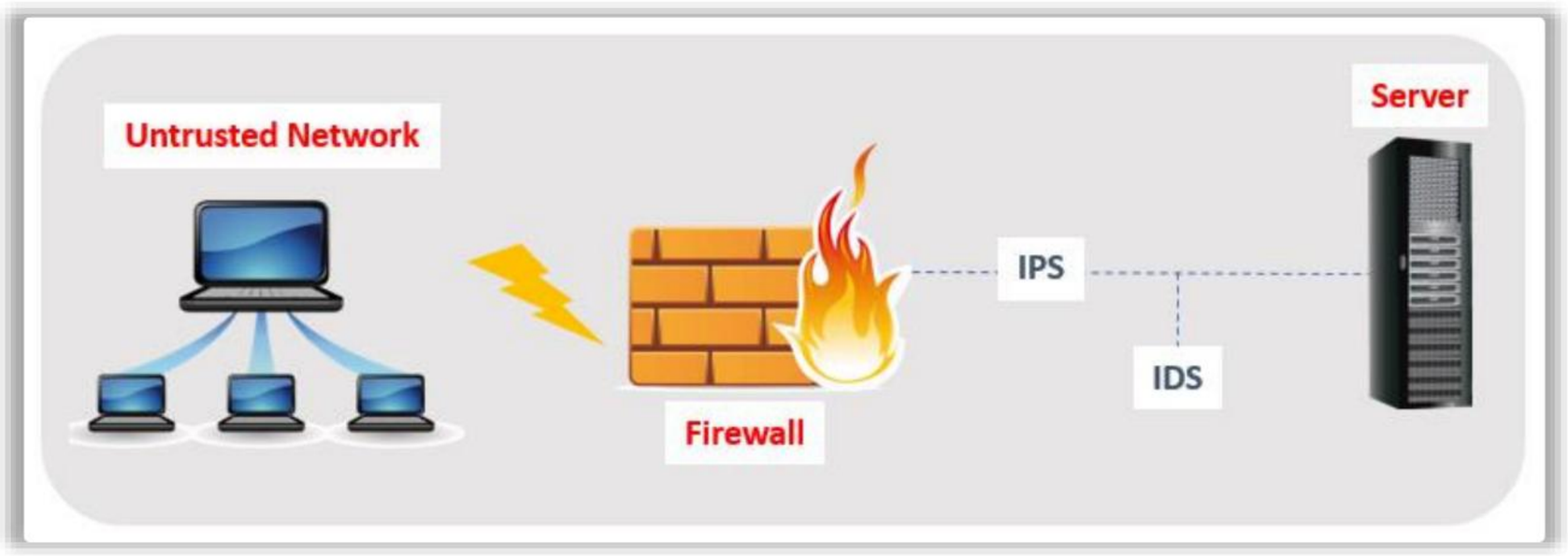


Figure 5.35: Difference between IPS and IDS

IDS vs IPS

For better secure cloud operations, use a combination of IDS and IPS by integrating them into a single architecture.

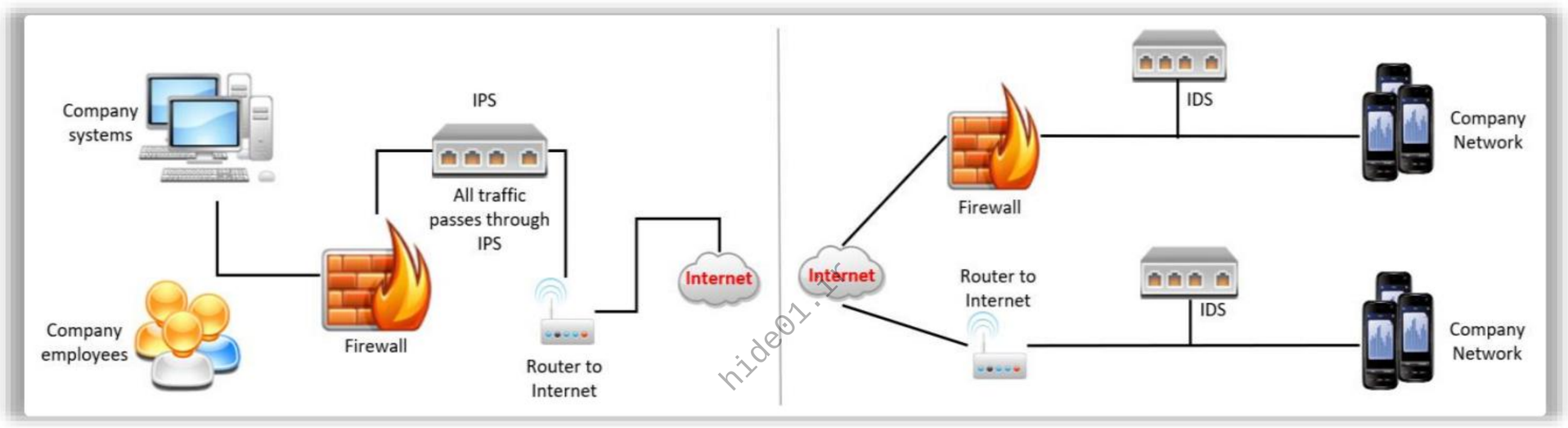
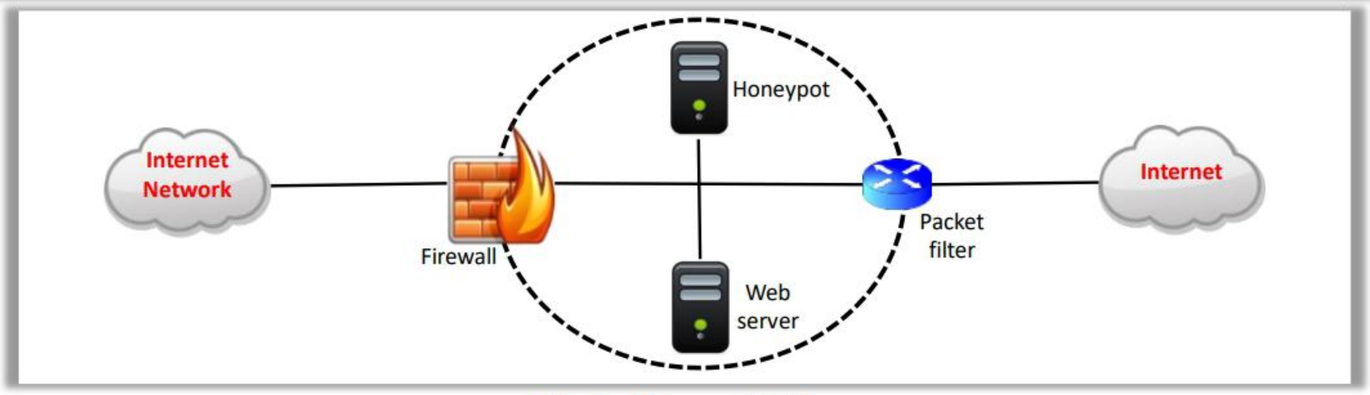


Figure 5.36: Combined IPS and IDS

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

Network Security Controls: Honeypots

- Honeypot is a fake proxy that can be executed to frame attackers by logging traffic through it and sending complaints to victim ISPs
- Honeypot seems to be a part of the production network but it is located on an isolated network with bogus data meant to lure attackers
- Use Honeypot to collect and analyze the information provided to understand the tools, tactics, and procedures (TTPs) of attackers and how they can bypass the security controls of actual production systems using these TTPs



A typical honeypot setup

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

Network Security Controls: Honeypots

A honeypot is an information resource system that is explicitly set up to attract and trap attackers who attempt to penetrate an organizational cloud network for unauthorized utilization of cloud hosts or resources. It is a fake proxy that can be implemented to frame attackers by logging traffic through it and sending complaints to ISPs. It acts as a part of the cloud network but it is actually located on an isolated network with bogus data meant to lure attackers. The actions of attackers are recorded when they use honeypots, considering them as target production systems. Honeypots also record newly dropped and modified files on systems by attackers.

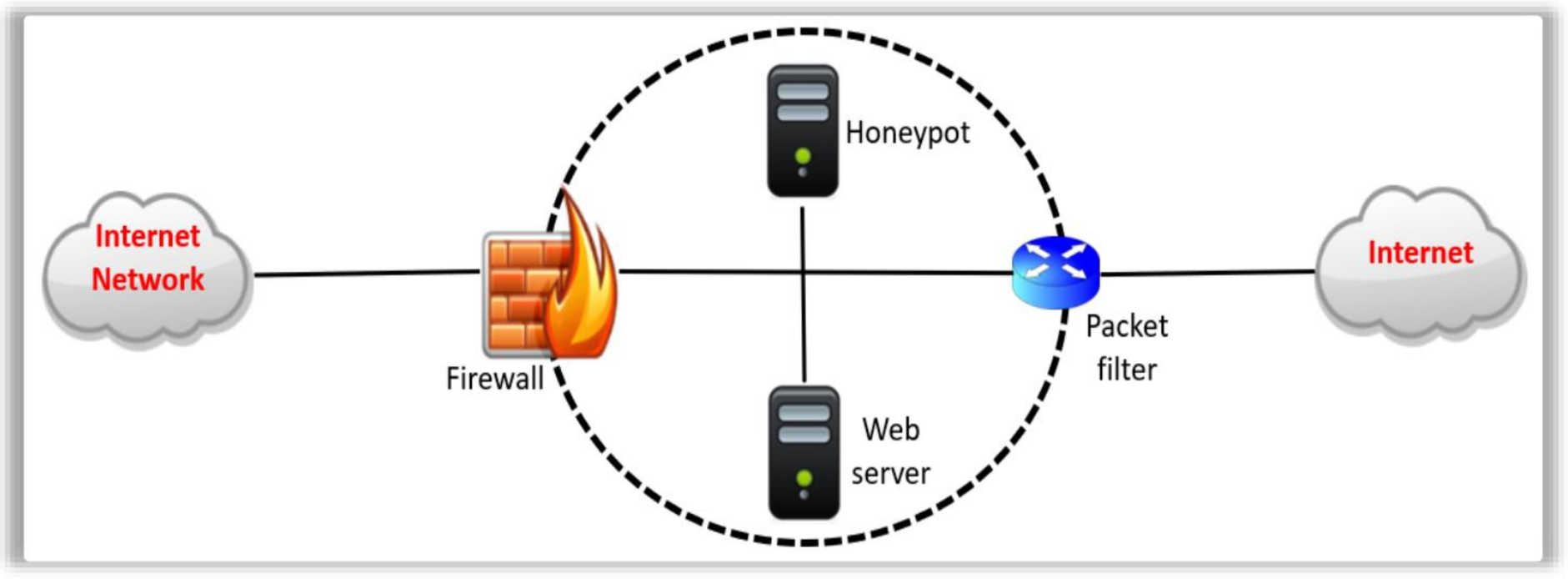


Figure 5.37: Typical honeypot setup

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

Honeypots Benefits

Use honeypot systems to

- Collect and analyze the information provided to understand the tools, tactics, and procedures (TTPs) of attackers and how they can bypass the security controls of actual production systems using these TTPs.
- Track the activities performed by attackers and build countermeasures for those attacks.
- Form a network called Honeynet by grouping multiple honeypot systems. Honeynet works in the same way as honeypots, but it provides more scalability and functionality.
- Detect insiders (employees) misusing the system.
- Record activities even when they are encrypted.

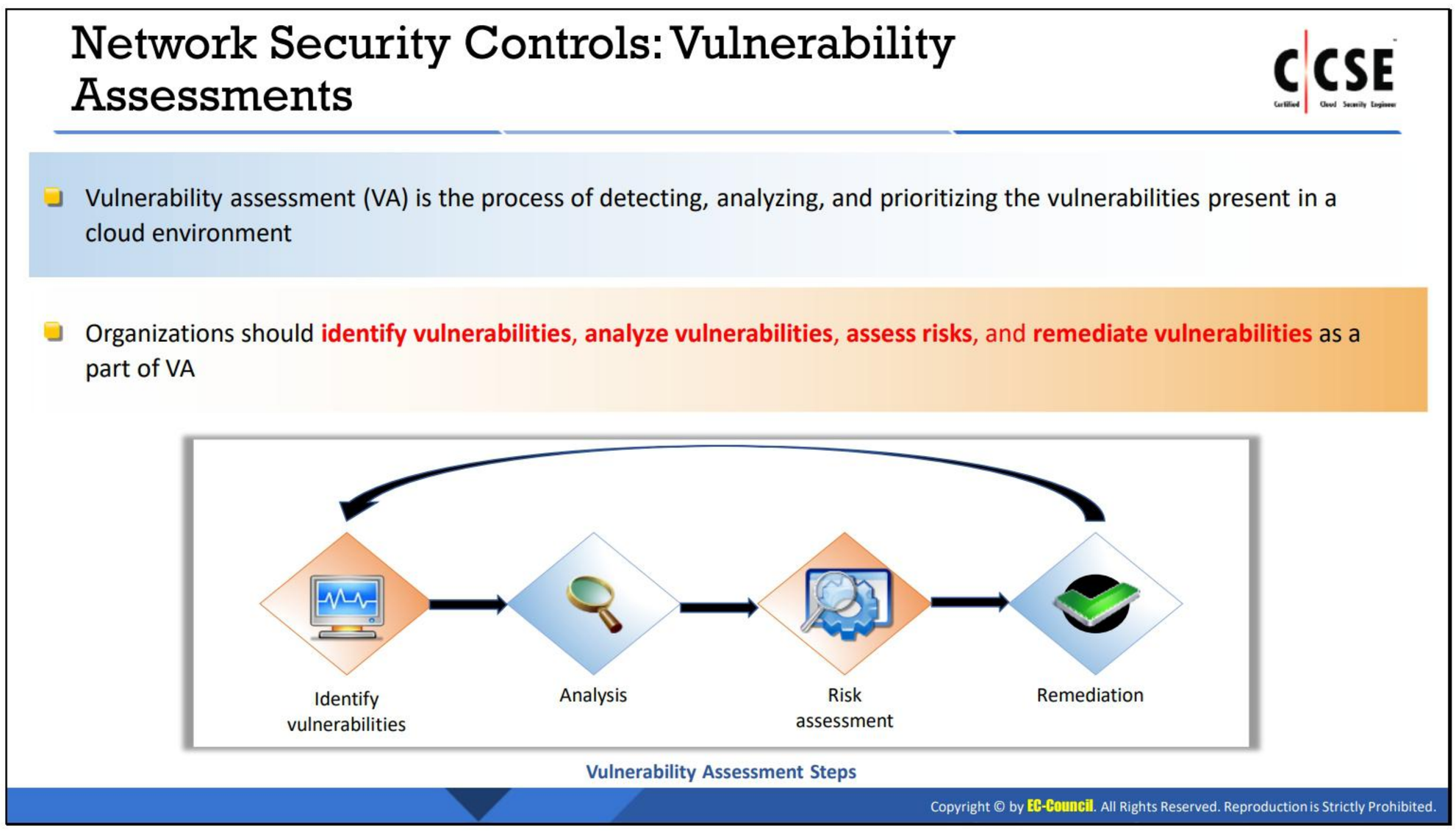
Honeypot Security Considerations

Follow the below security considerations while using honeypots:

- Understand the legal and compliance issues associated with using honeypots in an enterprise.
- Ensure that honeypots are isolated from the production cloud network to restrict the potential damage by attackers.
- Use a public cloud system for hosting a honeypot because it ensures proper isolation from the production network.

hide01.ir

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



Network Security Controls: Vulnerability Assessments

Vulnerability assessment (VA) refers to the process of detecting, analyzing, and prioritizing the vulnerabilities present in a cloud environment.

hide01.ir

VA Benefits

Organizations should perform VA to

- Test their cloud environment during VA for known vulnerabilities. The vulnerabilities identified during this process are not exploited to ensure that the assessment does not cause any destruction; thus, the vulnerabilities may require additional validation to eliminate false positives.
- Perform VA on cloud hosts based on the type of data stored in them and the regulatory requirements applicable to that data.
- Detect vulnerabilities in cloud environments using manual or automatic techniques based on organizational needs.

VA Steps

Organizations should follow the steps listed below as a part of VA.

- **Identify Vulnerabilities**: Scan the cloud hosts and servers to identify known vulnerabilities using cloud-based or external tools.
- **Analyze Vulnerabilities**: Analyze the root cause of the identified vulnerabilities. It includes identifying system components that are responsible for vulnerabilities and finding their root cause.

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

- **Assess Risk**: Prioritize vulnerabilities based on their potential impact. Risk assessment is mainly performed to assign priorities to identify vulnerabilities according to their severity.
- **Remediate**: Mitigate the identified vulnerabilities.

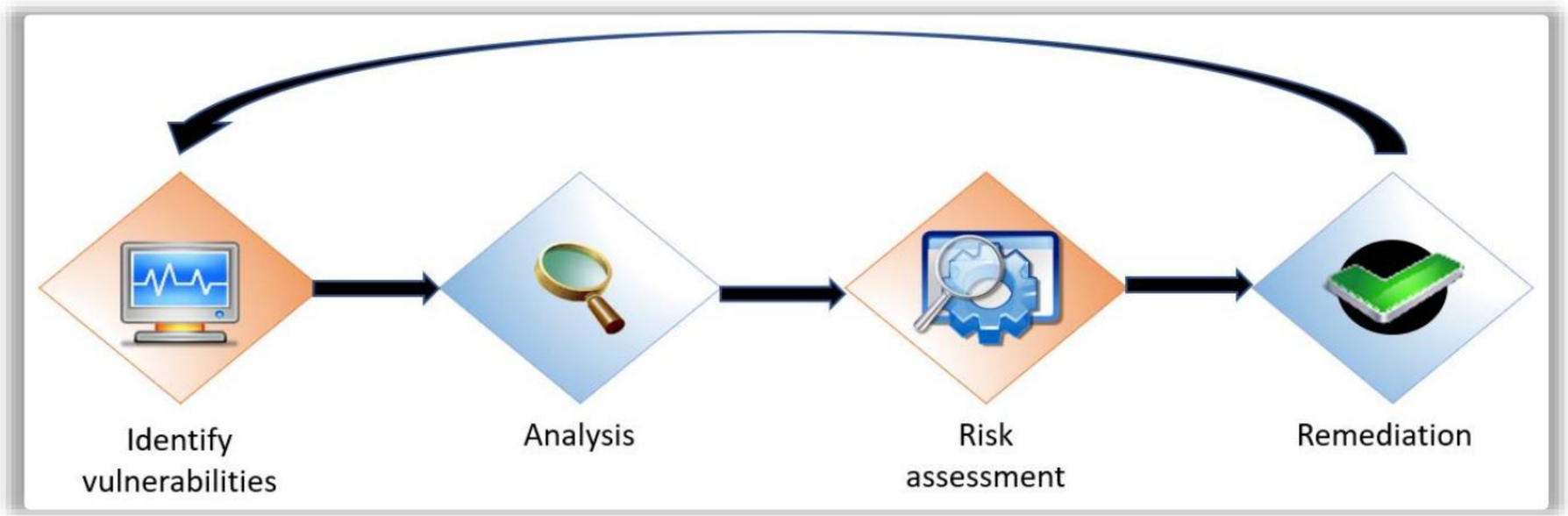


Figure 5.38: Vulnerability assessment process

VA Security Recommendations

The security recommendations for conducting VA in cloud environments include the following:

- Conduct regular VA and establish a process to track and remediate the identified vulnerabilities. The process must adhere to the compliance and regulatory requirements.
- Conduct different levels of testing based on the type of data stored in cloud systems. For example, when medical information is stored on cloud servers, conduct checks for compliance with the relevant regulatory policies such as HIPAA.
- Store the vulnerable data securely using proper access controls to ensure that they are not disclosed.
- Provide access to vulnerable data only for authorized parties that require access.
- Cloud provider must have a clear policy on disclosing vulnerable data, a timeline to remediate the identified vulnerabilities, and remediation steps. This policy will help them when cloud users demand scanning reports as proof of conducting an assessment by providing necessary information in the report.
- Ensure all required and essential policies are documented as part of the contract.
- Conduct external VAs to validate internal assessments.
- Understand how to use and manage cloud-based VA tools.
- Understand the tools used by third-party auditors when a third-party vendor is involved in validating internal assessment findings via an independent assessment and audit.

VA Limitations

Cloud consumers may often have contractual requirements for cloud providers to conduct vulnerability scans regularly for their systems. The reports and data of VAs contain data that are sensitive for cloud providers and cloud consumers. Unintentional disclosure of such reports or

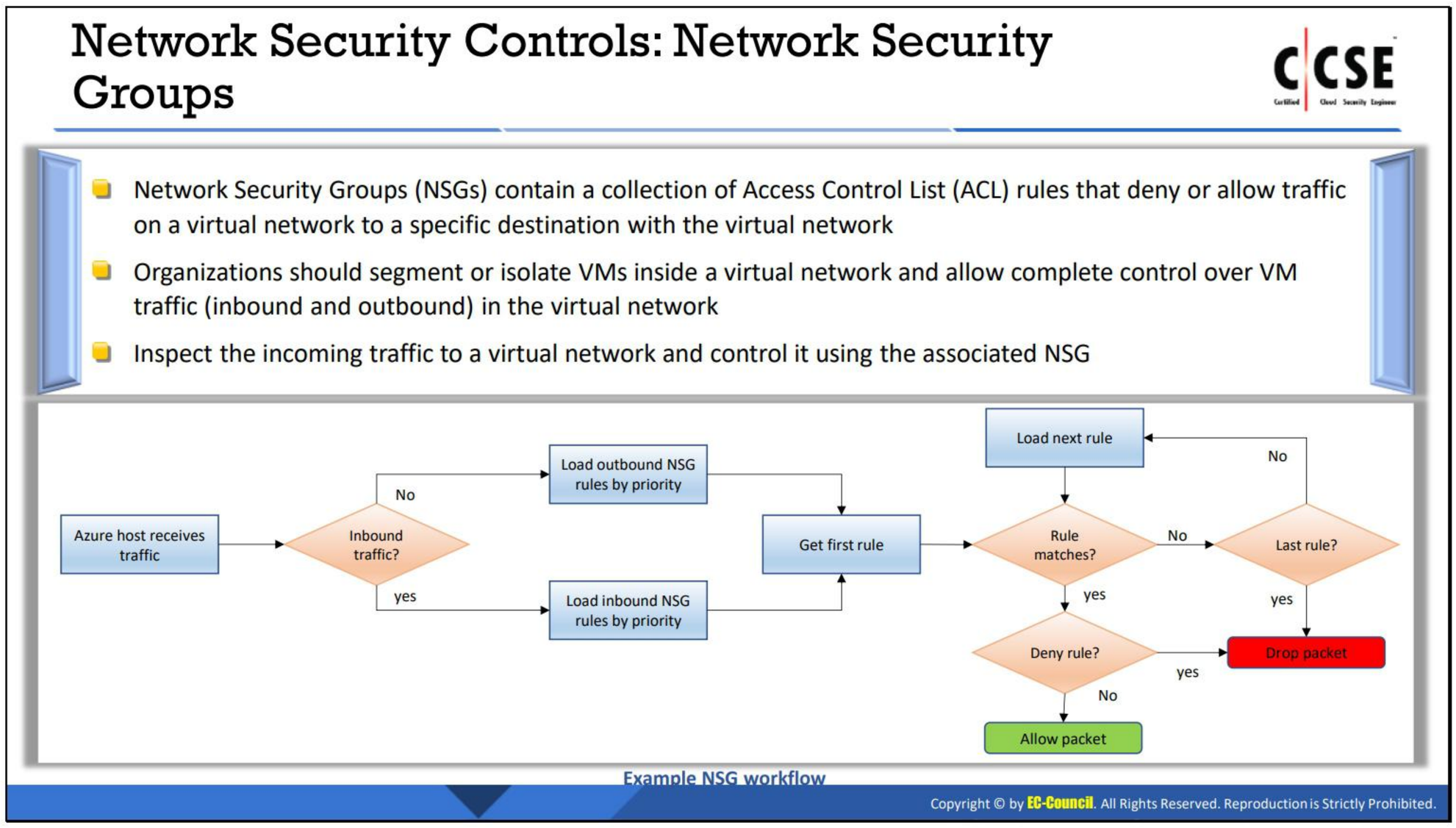
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

data may be risky for both parties. Generally, the tools and procedures to be used for VA are defined in the contract or SLA signed between the cloud provider and consumer.

Cloud security professionals should be aware of using VA tools and must know the tools that can be used for specific assessment processes. Cloud providers often appoint independent third-party auditors to perform VA to ensure transparency and trust. Additionally, they obtain various certifications for their cloud data centers and the underlying infrastructure from government authorities to ensure the trust of their consumers. Cloud consumers who wish to perform independent audits and VA for their cloud environment and its infrastructure must clearly define it in the agreement because most providers do not allow individual audits by their consumers owing to security issues.

hide01.ir

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



Network Security Controls: Network Security Groups

A network security group (NSG) includes a set of access control lists (ACLs) or security rules to allow or deny traffic on a VNet to a specific destination within the virtual network. Cloud customers can overrule/modify the default NSG rules provided by the provider but cannot delete them.

hi@91.ir

NSGs Benefits

NSGs allow cloud customers to

- Segment or isolate VMs inside a virtual network and allow complete control over VM traffic (inbound and outbound) in the virtual network.
- Create scenarios such as demilitarized zones (DMZs) to secure backend services such as application and database servers.
- Apply one NSG to several subnets or VMs.
- Control direct internet connection, network connectivity to cloud from an on-site environment, and communication on a virtual network between different workloads.

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

How NSGs Work

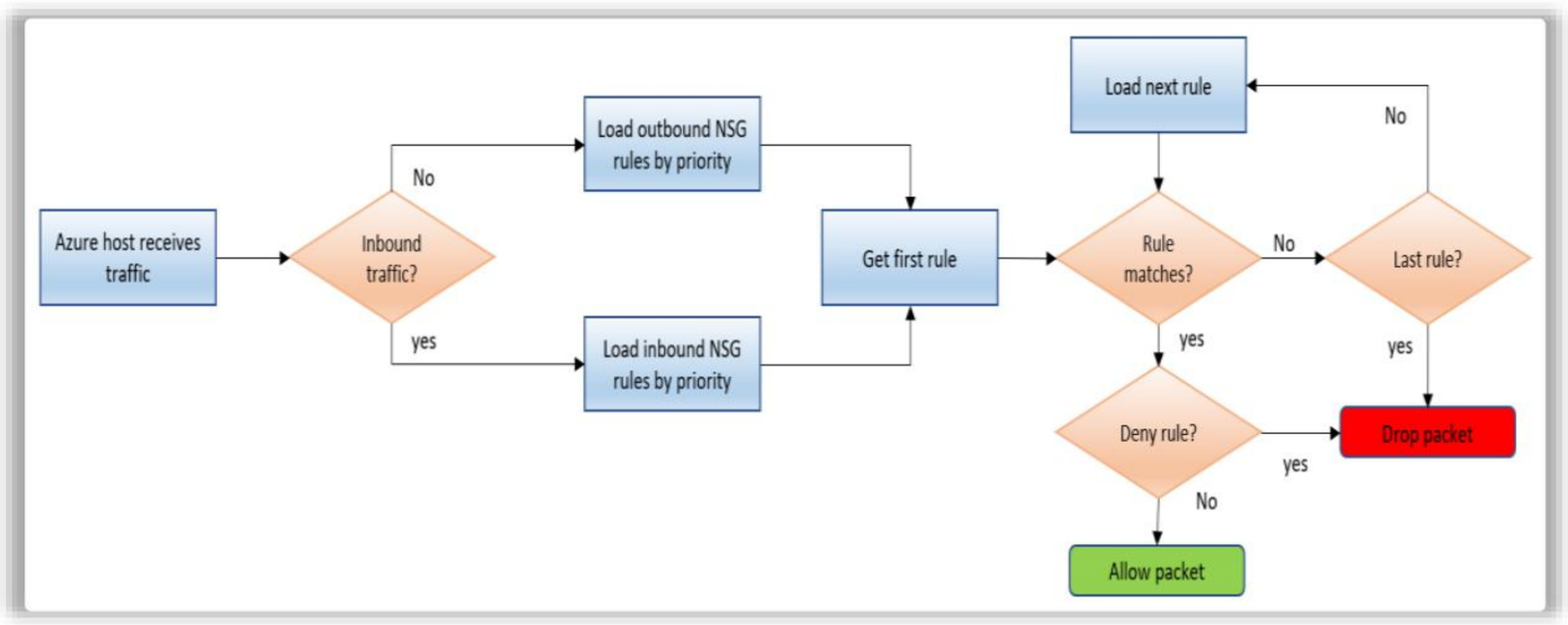


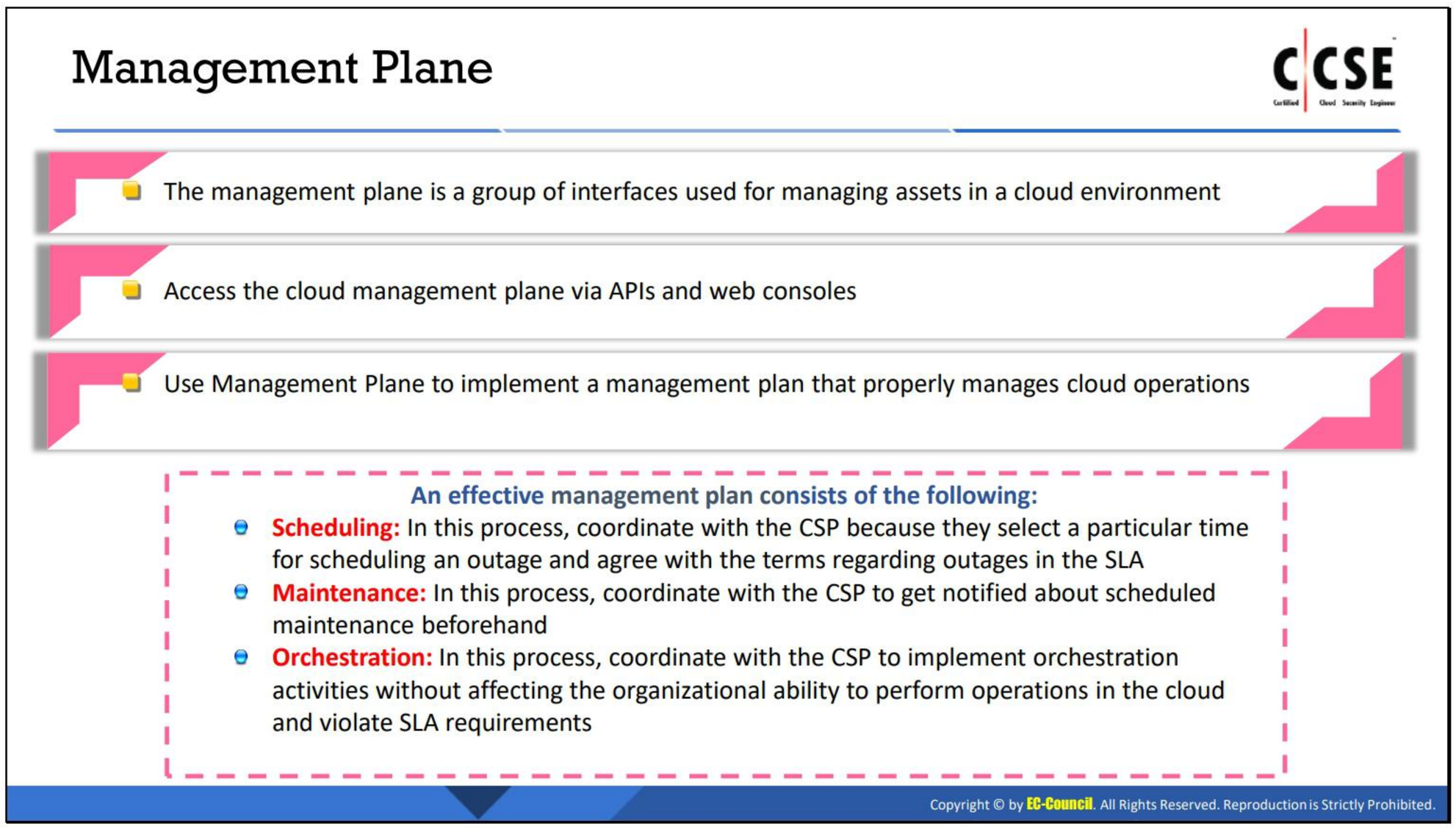
Figure 5.39: Example NSG workflow

Inspect the incoming traffic to a virtual network and control it by the associated NSG. Check all packets against the NSG rules and allow or deny them based on these rules.

Apply NSGs to a subnet, which are then applied to all VMs inside that subnet. Apply an NSG to a VM; accordingly, the NSG rules are applicable for that VM only. Use an NSG to control inbound and outbound access to subnets, VMs, and network interfaces (NICs).

hide01.ir

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



Management Plane

The management plane is a group of interfaces used for managing assets in a cloud environment. It is used to control and configure the meta structure (management plane components). The management plane includes the interfaces used to build and manage the cloud and those used to manage the allocated cloud resources for cloud consumers. For SaaS, the management plane is the user interface admin tab where users can configure components such as users or settings for an organization. It helps in enabling and enforcing isolation in multi-tenancy. Cloud customers use the management plane to configure and manage cloud resources such as launching instances and configuring VNets.

Use Management Plane to implement a Management Plan

Design and implement all aspects of the cloud security architecture of an organization. Know the mitigation techniques and hardware vendor recommendations to be applied in the cloud infrastructure. Create an effective management plan that can facilitate smooth cloud operations. Use the cloud management plane to implement a management plan effectively.

An effective management plan consists of the following:

- **Scheduling**

  Scheduling an outage is significantly easier in a traditional data center owned by a single customer because it can be performed when the data center is least used. However, it is difficult to schedule an outage in a cloud data center because cloud users are located in different time zones and access cloud all the time. There is no particular time when cloud usage is low. If an outage is scheduled in a cloud environment, it will result in downtime or unavailability of cloud services, which may impact the business.

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

Cloud providers effectively plan their operations based on the available cloud resources during downtime or repair and knowledge of their customers. Coordinate with the providers because they select the time for scheduling an outage and agree with the terms related to outages in the SLA.

- **Maintenance**

  Cloud systems also need maintenance like other systems. In a cloud environment, a maintenance mode is required to patch or upgrade a virtualized host. No VM can run on a host under maintenance.

  Stop the VMs running on a host under the maintenance mode or transfer to another host to avoid any downtime or service disruption. Coordinate with the cloud provider to get notified about the scheduled maintenance beforehand. Know the steps taken to prevent downtime, period of maintenance window, and its possible impacts it may have with the inputs of the provider.

  During a maintenance window, VMs are moved to another host to avoid downtime and disruption of services; the cloud environment does not have the set of resources it had (running on the host under maintenance) for that particular duration. Cloud providers ensure that they can meet the possible demands during the maintenance window with the help of auto-scaling and self-provisioning of systems in the cloud. Additionally, the provider checks how many cloud systems can be put under maintenance without affecting customer requirements for that duration before scheduling a maintenance activity.

  hide01.ir

  The security considerations for secure maintenance of cloud systems include

  - Ensure that the cloud provider has sufficient resources to meet SLA requirements and the expected demands during maintenance.
  - Ensure that the required change management processes are followed for all systems and all concerned parties that may be affected by the maintenance work are notified.
  - Use automated system tools to notify the concerned parties.
  - Ensure that all hosts are properly secured during maintenance.

- **Orchestration**

  Orchestration in a cloud environment refers to automating tasks such as provisioning, scaling and assigning resources, and customer billing and reporting. The main objective of cloud orchestration is to automate the configuration, management, and configuration of software and its interactions. This process involves automating the tasks and workflows necessary for service delivery. Tasks that can be automated through this process include those that manage server runtimes and process flow between applications. The orchestration capabilities of a cloud platform must satisfy the SLA requirements of the provider.

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

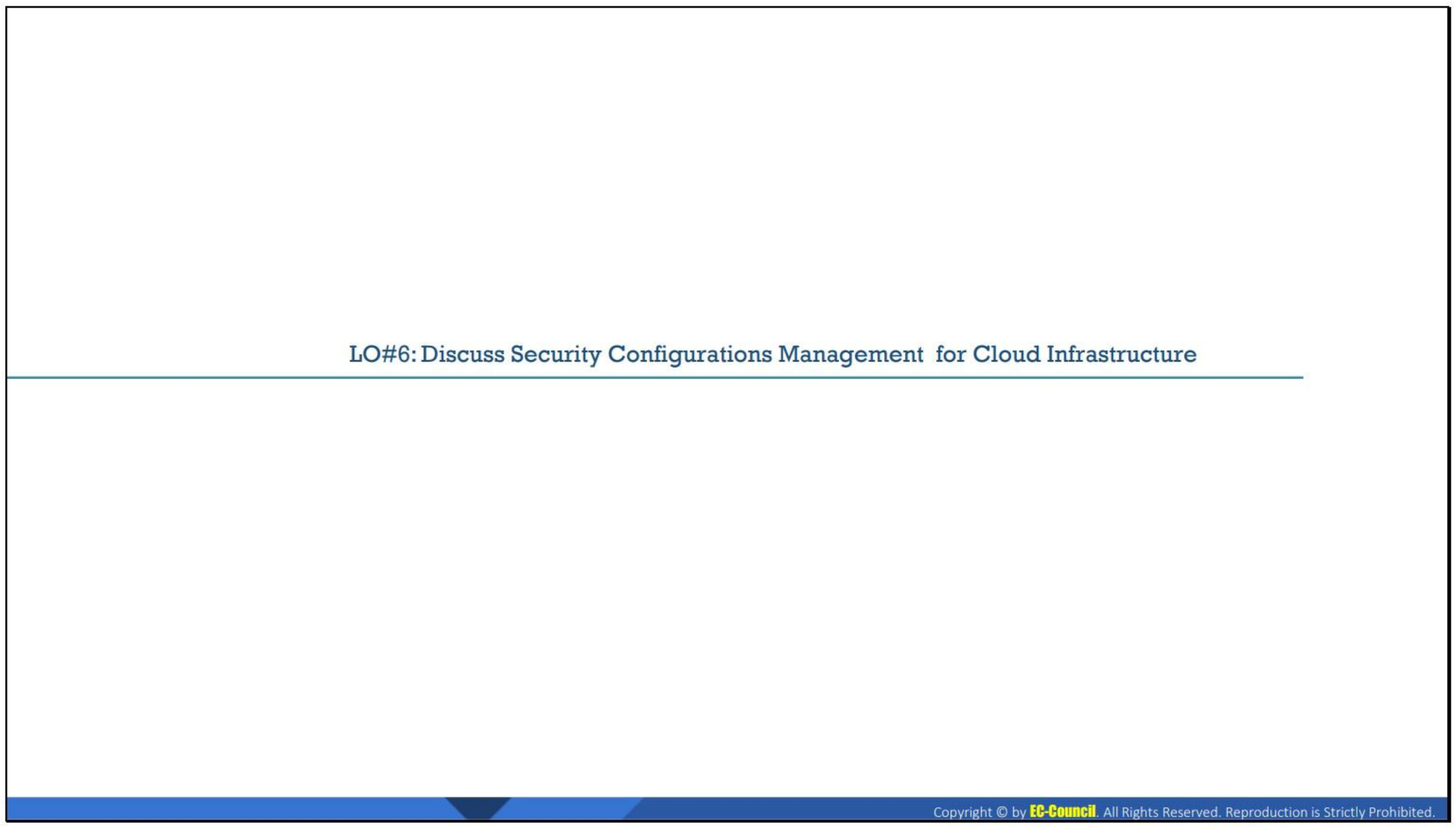
Within a cloud environment, orchestration is crucial while planning or performing operation activities because it facilitates cloud customers to scale their environments and make configuration changes at any time without involving cloud providers. Coordinate with the cloud provider to implement orchestration activities without affecting the organizational abilities to perform operations in the cloud and violate SLA requirements.

Implement cloud orchestration for the following:

- To obtain increased speed of delivery
- To minimize the chances of errors during provisioning, scaling, and other processes
- To eliminate the involvement of personnel to a great extent
- To enforce security policies and standardize templates
- To review and modify (improve) automation scripts
- To provide better visibility and control over cloud resources

hide01.ir

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

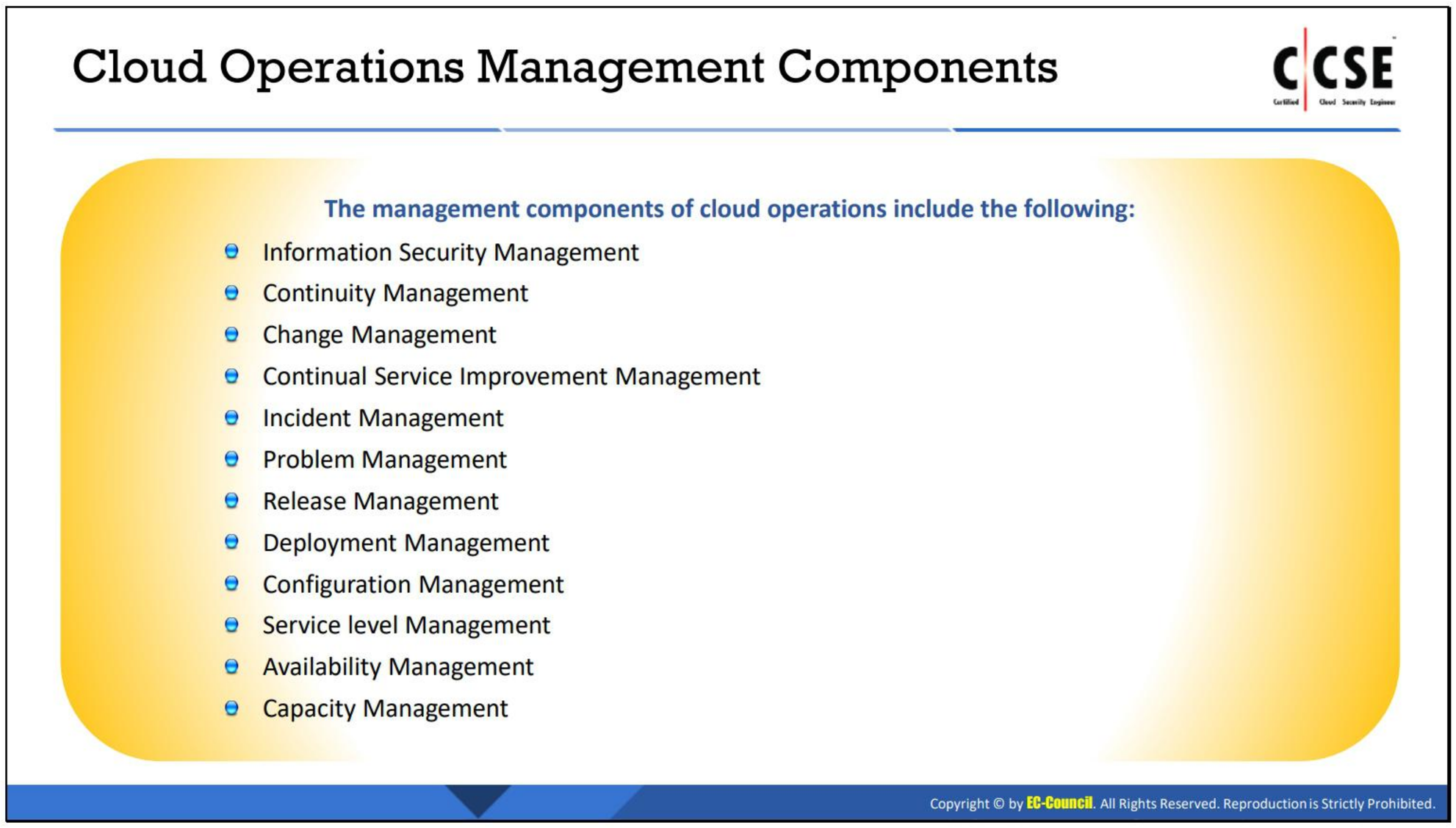


LO#6: Discuss Security Configurations Management for Cloud Infrastructure

The objective of this section is to understand the various management components of cloud operations such as information security management, continuity management, change management, evidence management, problem management, deployment management, and configuration management. In this section, cloud security engineers will learn about the different management components of cloud operations and use the acquired knowledge to securely manage cloud operations.

hiddi01.ir

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

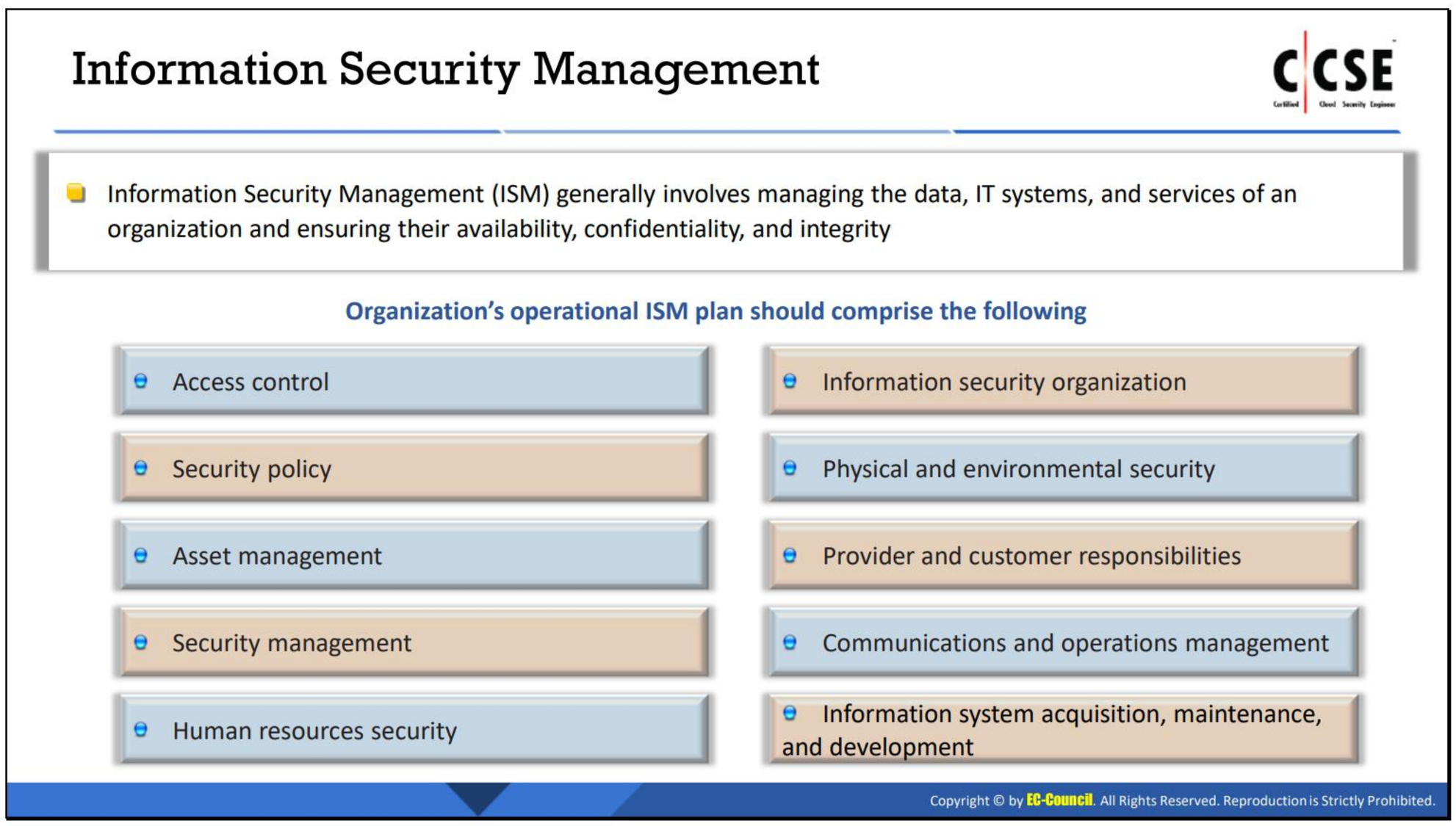


Cloud Operations Management Components

Organizations should manage multiple processes and aspects in a cloud environment. These processes ensure compliance with regulations and organizational internal policies and form a structured operation management program to manage processes. The management components of cloud operations include the following:

- Information Security Management
- Continuity Management
- Change Management
- Continual Service Improvement Management
- Incident Management
- Problem Management
- Release Management
- Deployment Management
- Configuration Management
- Service Level Management
- Availability Management
- Capacity Management

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



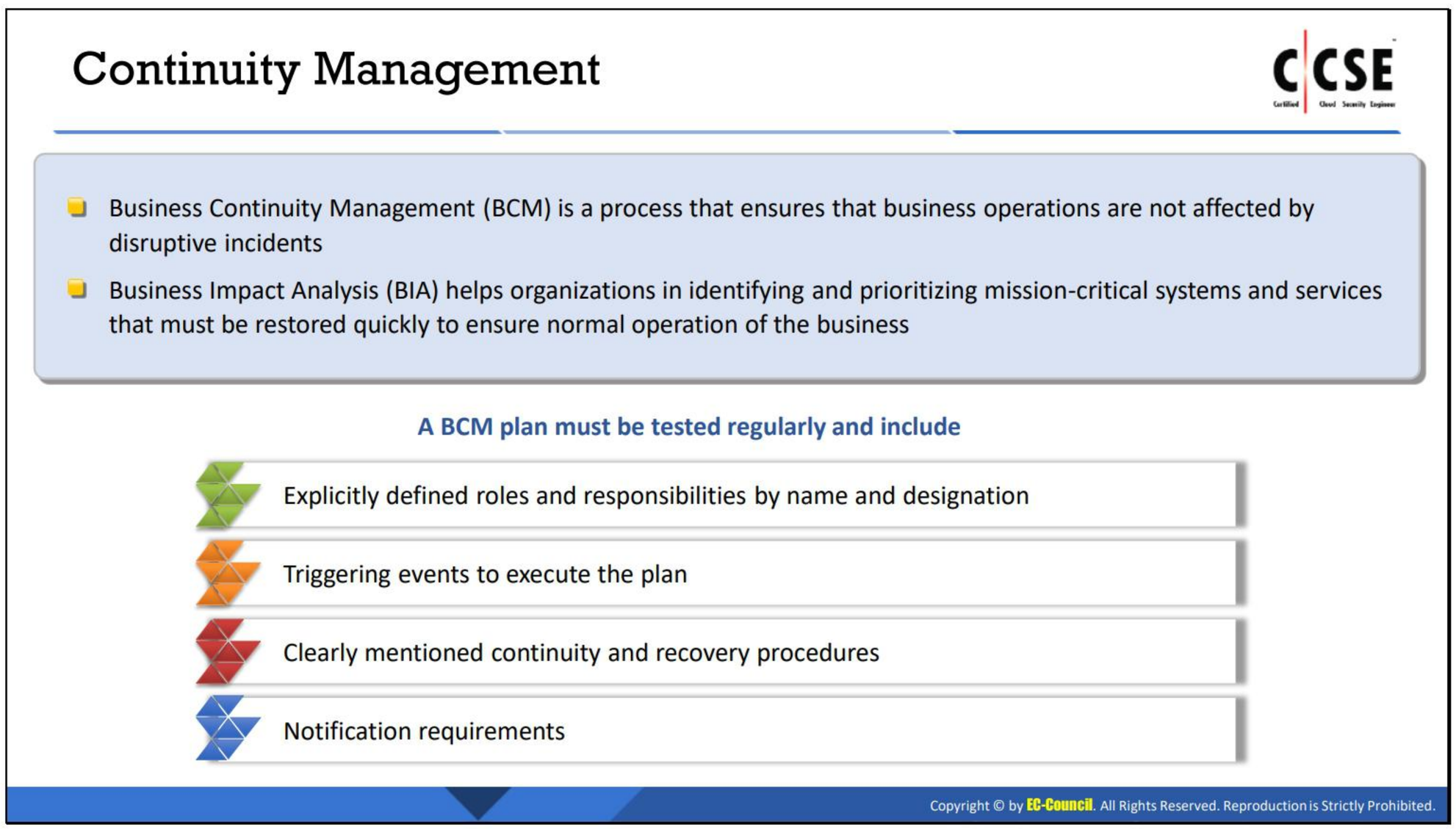
Information Security Management

Information security management (ISM) involves managing the data, IT systems, and services of an organization and ensuring their availability, confidentiality, and integrity. It includes the design of security controls, testing, managing incidents, continually reviewing, and maintaining security controls and processes. The implementation of security management in an organization as an integral part ensures that security is embedded in all projects and discussions (from planning till implementation).

Organizations should have an operational ISM plan. It should comprise the following:

- Access control
- Security policy
- Asset management
- Security management
- Human resources security
- Information security organization
- Physical and environmental security
- Provider and customer responsibilities
- Communications and operations management
- Information systems acquisition, maintenance, and development

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



Continuity Management

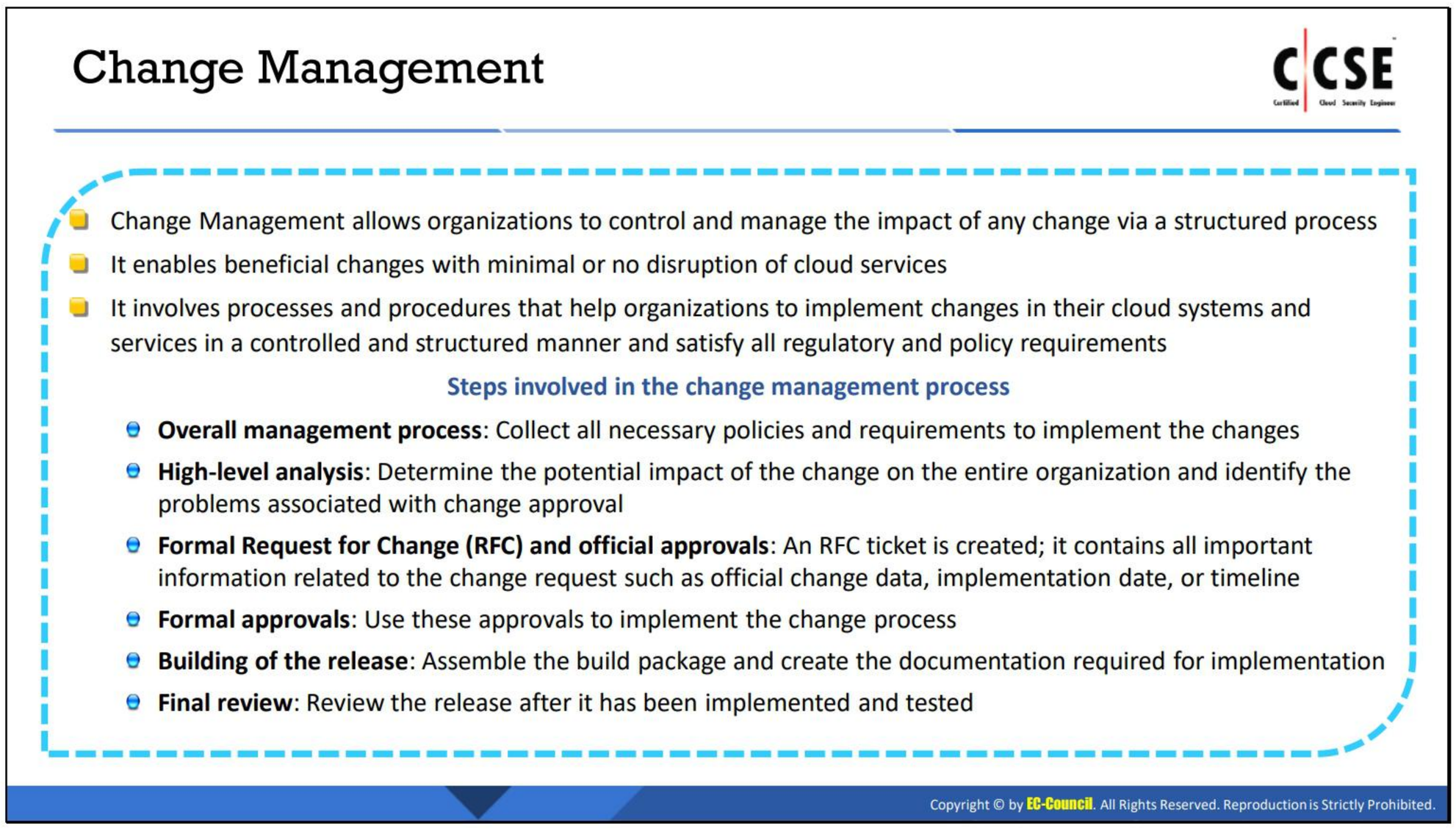
Business continuity management (BCM) or continuity management is a process that ensures that business operations are not affected by disruptive incidents. Continuity management involves the successful restoration of cloud systems and services after a sudden disaster, incident, or outage. Unexpected events include security incidents that demand service or system shut down, loss of network connectivity, physical problems with system hardware or data centers, and natural disasters. In such cases, the BCM framework enables organizations to anticipate the internal and external threats.

To develop a BCM plan, an organization must prioritize its systems and services (mission-critical services) to make inventory services and their underlying technologies and systems that support them. This will help the organization identify the systems that need to be restored quickly and those that can be restored later or when the primary hosting facility becomes functional again. To implement BCM, business impact analysis (BIA) is used. Using BIA, cloud security professionals can create plans and strategies that will help the organization recover from any service disruption and continue normal business operations.

A BCM plan must be tested regularly and must include

- Required capacity and capability of backup systems
- Explicitly defined roles and responsibilities by name and designation
- Triggering events to execute the plan
- Clearly mentioned continuity and recovery procedures
- Notification requirements

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



Change Management

Change management allows organizations to control and manage the impact of any change via a structured process. It includes processes and procedures that help organizations to implement changes in their cloud systems and services in a controlled and structured way and satisfy all regulatory and policy requirements for auditing and documenting the change processes and actors. It enables beneficial changes that must be implemented with minimal or no disruption of cloud services.

Objectives of Change Management

The main objectives of change management are:

- Respond to varying business requirements of customers while reducing disruption, rework, and incidents and maximizing value.
- Respond to IT and business requests for changes that help services with business needs.
- Ensure that the changes are properly evaluated and recorded.
- Ensure that the authorized changes are carefully planned, prioritized, properly tested, implemented, documented, and then reviewed in a structured manner.
- Ensure that changes to CIs are documented or recorded in the configuration management system (CMS).
- Optimize business risks.

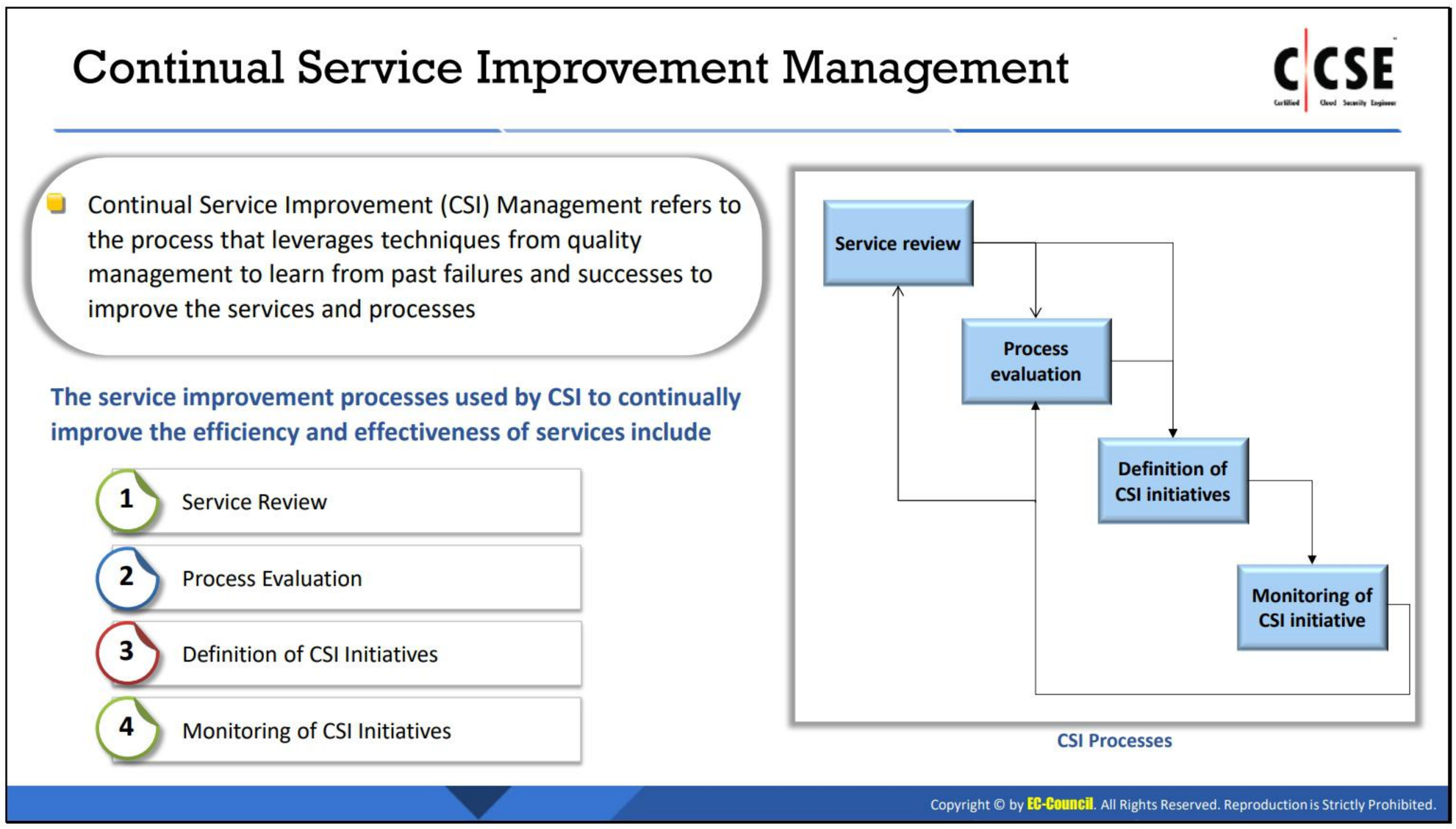
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Change Management Process

The steps involved in a change management process include:

- **Overall management process**: At this stage, gather all necessary policies and requirements to implement changes. Organizations with documents and processes should standardize the entire change management program. Management allows to decide and approve the changes.
- **High-level analysis**: Once the management decides the changes to be implemented, the change proposal requires high-level analysis to determine the potential impact of these changes on the organization and identify any problem associated with change approval. Here, organizations should address those problems. At this stage, discover potential dependencies and analyze them.
- **Formal Request for Change (RFC) and official approvals**: The formal RFC and official approval process starts after the completion of high-level analysis and dependency checks with no major identified problems. An RFC ticket is created following the process suitable for the organization. Most organizations use software for handling the formal RFC process. The RFC ticket contains all important information related to the change request such as official change data and implementation date or timeline. Stakeholders are required to approve the change request formally. Stakeholder in an organization refer to the system and operations teams, development teams, project managers, and management. Stakeholders approve the RFC request after carefully evaluating it to ensure that the required information is present and valid, and the proposed timeline is in-line with the management policies. The RFC requests are officially approved once stakeholders give their approval, and this approval is recorded for audit purposes.
- **Formal approvals**: The change process requires two formal approvals: change manager and change advisory board (CAB). These two approvals are required to implement the change process. The CAB comprises representatives with different roles across the organization. The CAB can approve major modifications to the change request, but the change manager can only approve minor modifications.
- **Building of the release**: The process of scheduling and building the release starts after formal approvals are obtained. This phase involves assembling the build package and creating the documentation required for the implementation. After scheduling and assembling, formal authorization is implemented to deploy the release and make the configuration changes. The deployment process involves functional testing and validation of the build package; it ensures that all components are working as desired.
- **Final review**: This involves reviewing the release after it has been implemented and tested. The final review improves the change management process and ensures that the release documentation is finalized for regulatory compliance or future audits.

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



Continual Service Improvement Management

Continual service improvement (CSI) management refers to the process that leverages techniques from quality management to learn from past failures and successes to improve the services and processes. CSI ensures continual IT service improvement; it based on ISO 20000 standards. It combines a wide range of metrics and data with quality management principles to create a formal analysis process that identifies areas that need improvement within the operations and systems to improve performance, cost effectiveness, and user experience.

With CSI management, organizations can enhance the service quality and customer experience and make processes more efficient and effective. CSI can be applied to all aspects of the ITIL (Information Technology Infrastructure Library) framework or other lifecycle management and can be utilized to review and evaluate improvement recommendations for every part of the lifecycle. Now, collect and analyze metrics on all processes and services to check if improvements can be made using a formal process. Monitor the performance of these services and processes using various tools (e.g., ITIL framework).

CSI Processes

ITIL CSI uses the following service improvement processes to improve the efficiency and effectiveness of services continually:

- **Service Review:** Service reviews are performed to assess the IT infrastructure and services regularly. These reviews uncover the need for discontinuation of service, new services, and other quality demands.
- **Process Evaluation**: Process evaluations help IT teams to determine if services are meeting the desired goals. Process evaluation includes audits, establishing benchmarks, evaluating metrics, and performing other assessments.

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

- **Definition of CSI initiatives**: CSI adopters can specify initiatives based on service reviews and process evaluations to improve the processes and services.
- **Monitoring CSI initiatives**: This process helps to track the effectiveness of initiatives, troubleshoot issues, and refine changes. It helps in taking corrective measures where the specified initiatives are not working as intended.

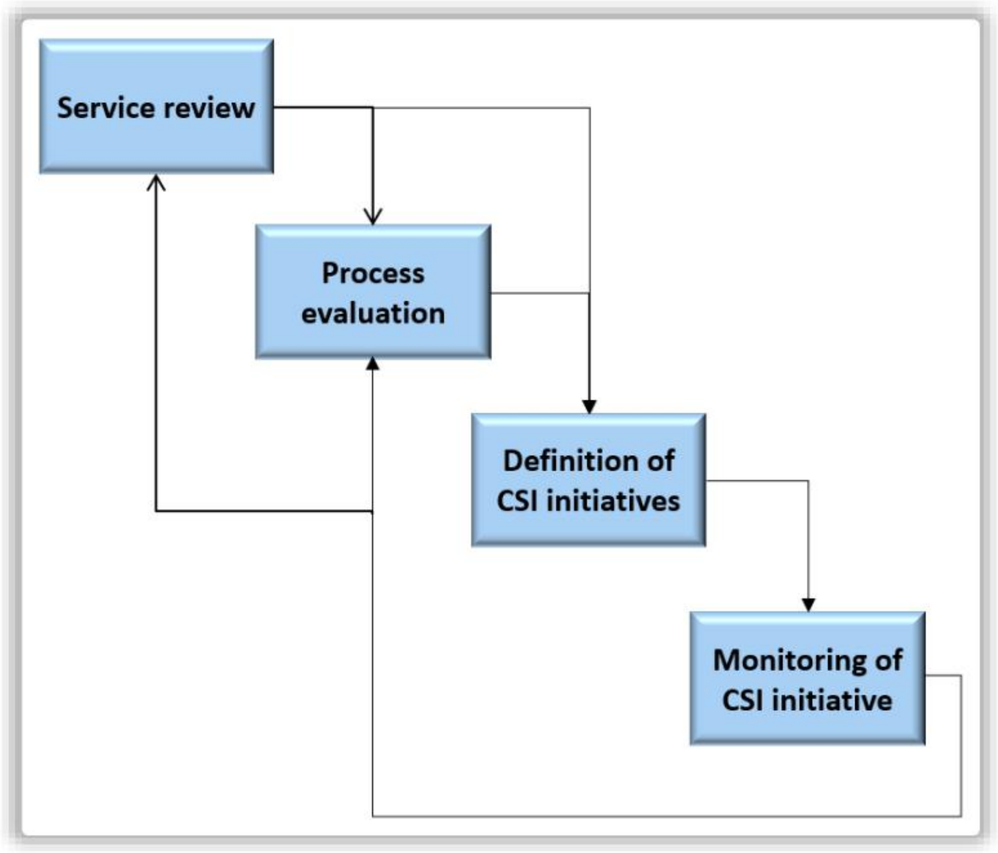
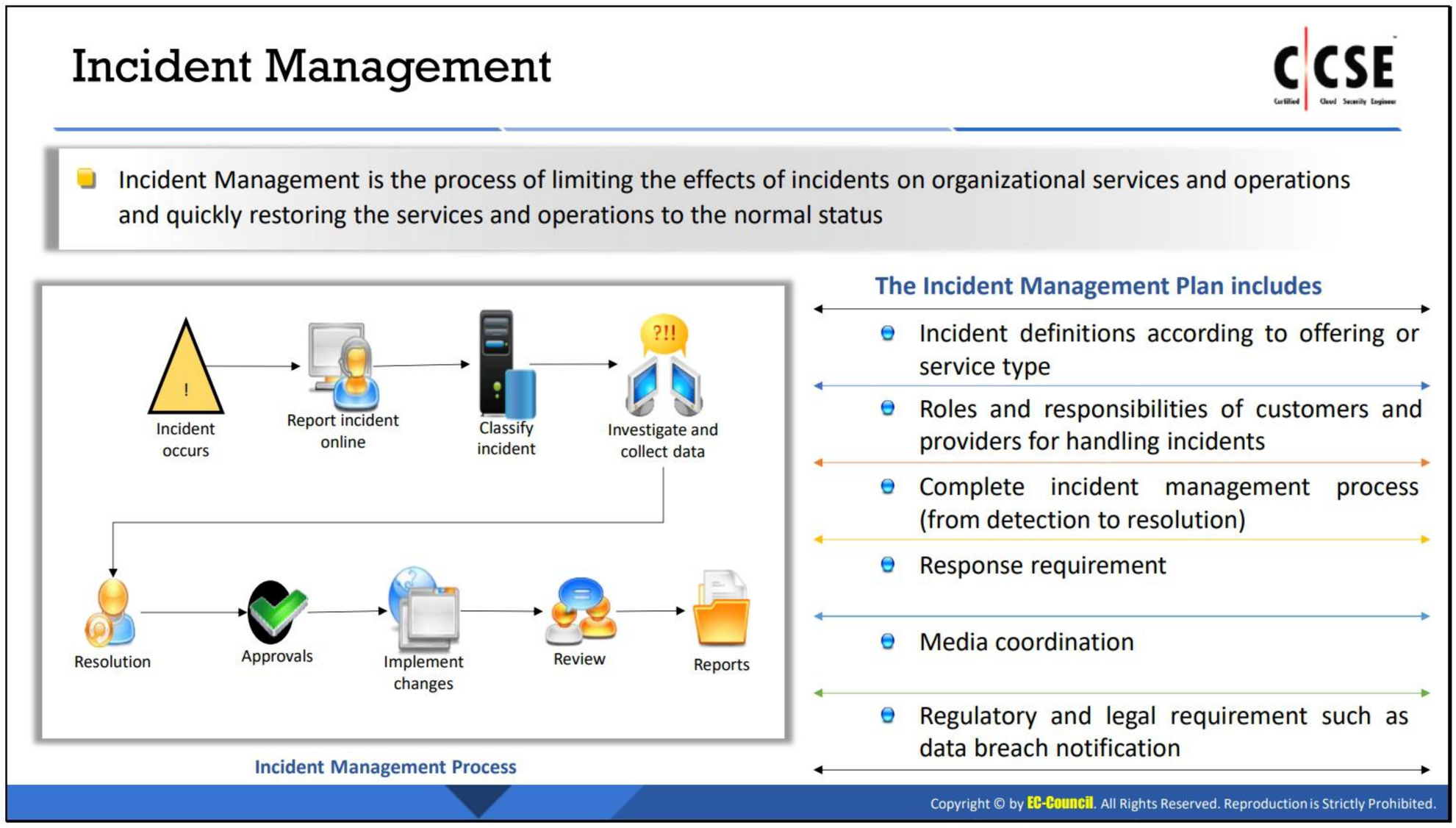


Figure 5.40: CSI processes

hide01.ir

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



Incident Management

Incident management is a process of limiting the effects of incidents on organizational services and operations and quickly restoring them to the normal or functional status. The main objective of incident management in cloud is to respond to events quickly and prevent them from becoming a larger cause of disruption. An important part of incident management includes performing a complete analysis and learning from past incidents. It will help the organization to handle incidents effectively and eliminate factors that may cause harm.

Purpose of Incident Management

There are three main purposes for having incident management:

- Quickly restoring normal service operations
- Reducing the negative impact on business operations
- Maintaining service availability and quality

Objectives of Incident Management

Following are the main objectives of incident management:

- Ensure that only standardized procedures and methods are utilized to respond to, analyze, and report incidents.
- Improve communication and visibility of incidents to IT support staff.
- Improve business perception of IT using a standard approach in rapidly communicating and solving incidents.
- Align the activities of incident management with those of business.

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

- Maintain user satisfaction.

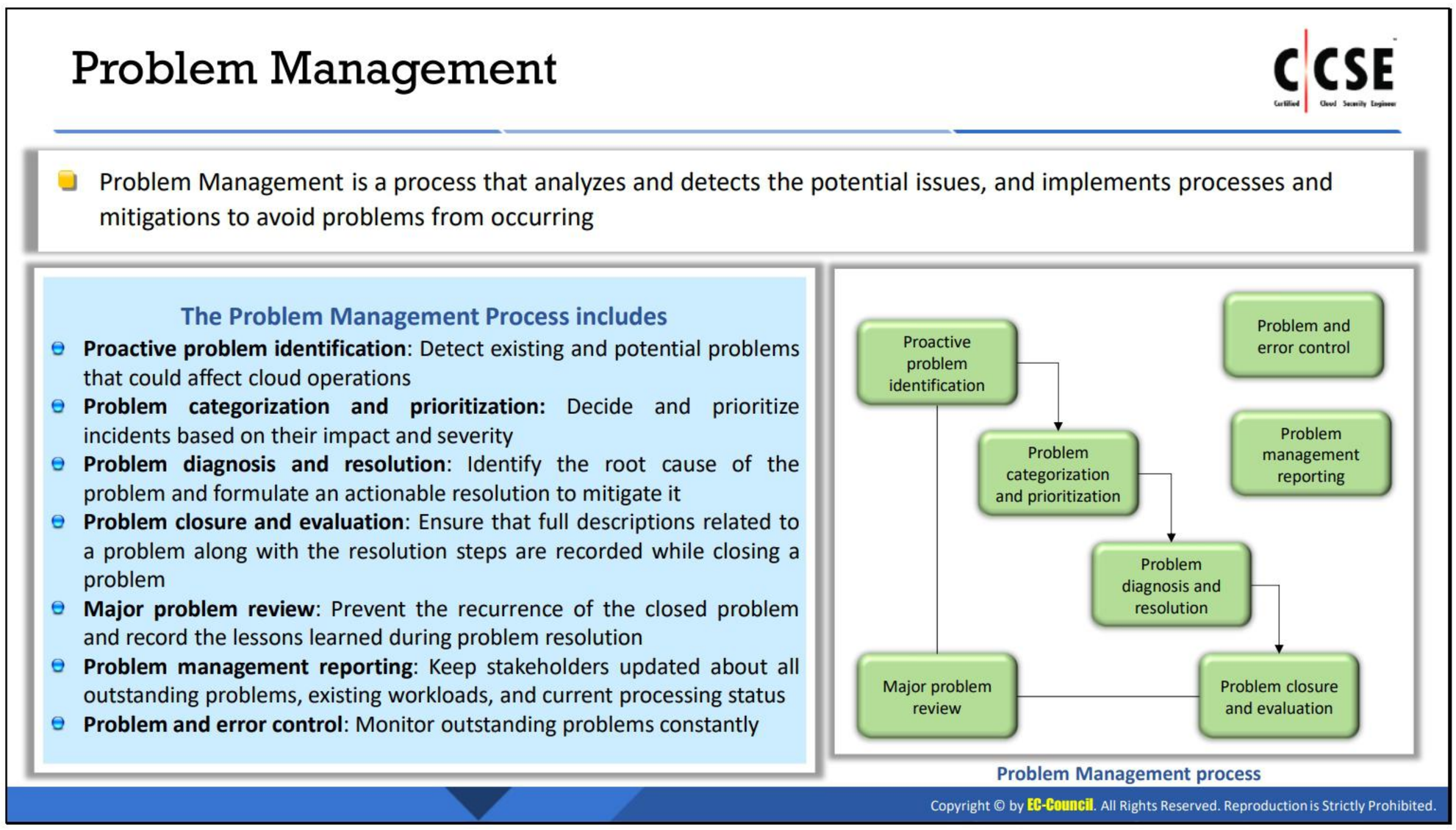
Incident management plan

For proper incident management in cloud, cloud security professionals should establish a well-documented incident management plan. The plan must include the following:

- Incident definitions by offering or service type
- Roles and responsibilities of customers and providers for handling incidents
- Complete incident management process (from detection to resolution)
- Response requirement
- Media coordination
- Regulatory and legal requirement such as data breach notification

Figure 5.41: Incident Management Process

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



Problem Management

Problem management is a process that analyzes and detects potential issues and implements processes and mitigations to avoid the occurrence of problems. This is usually performed by gathering and analyzing reports and data from apps and systems along with reports of past incidents. The problem management process utilizes this information to prevent potential problems. The main goal of problem management is to avoid the occurrence of predictable problems by establishing processes that can identify problems and prevent them. If it cannot prevent specific problems, it attempts to minimize the effect of those problems and strives to recover from them.

It detects the root cause of predictable problems and minimizes their effects on organizational operations. Organizations use problem management to gain greater agility, reliability, and efficiency in their cloud operations. Problem management processes help in the improvement of organizations and predict their operational performance.

Objectives of Problem Management

Problem management has the following objectives:

- Eliminate underlying issues that may cause the same problem
- Minimize the number of incidents that affect service performance or cause service outages
- Reduce the costs associated with incident response
- Increase productivity for both IT and business
- Quick resolution of service outages

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

Problem Management Process

Organizations require a problem management process to respond to problems or issues reactively and proactively. This process can differ for various organizations according to their requirements. A typical problem management process defined by the Information Technology Infrastructure Library (ITIL) is shown below.

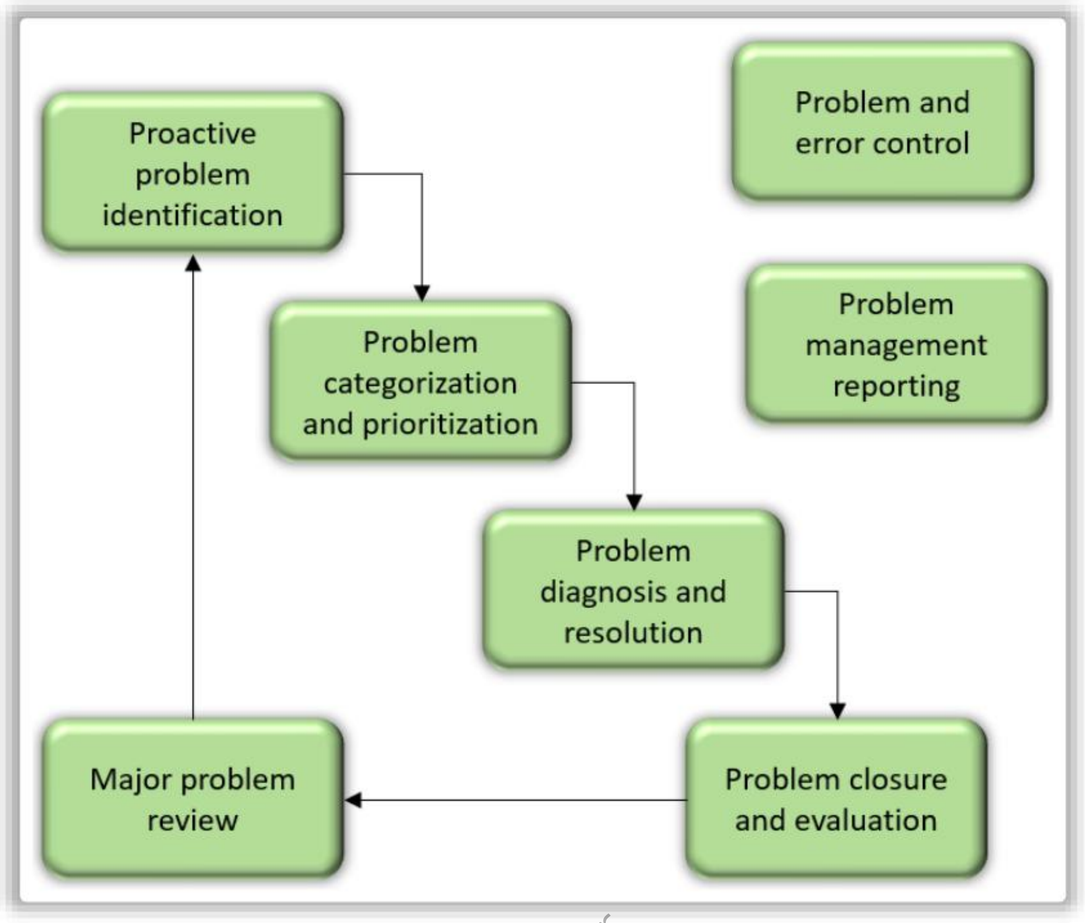


Figure 5.42: Problem Management process

Proactive problem identification: It helps to detect the existing and potential problems that could affect cloud operations by correlating several incidents or outages into a single underlying problem.

Problem categorization and prioritization: This step helps the problem management team to decide and prioritize incidents based on their impact and severity.

Problem diagnosis and resolution: It helps the team to identify the root cause of the problem and take an actionable resolution to mitigate it.

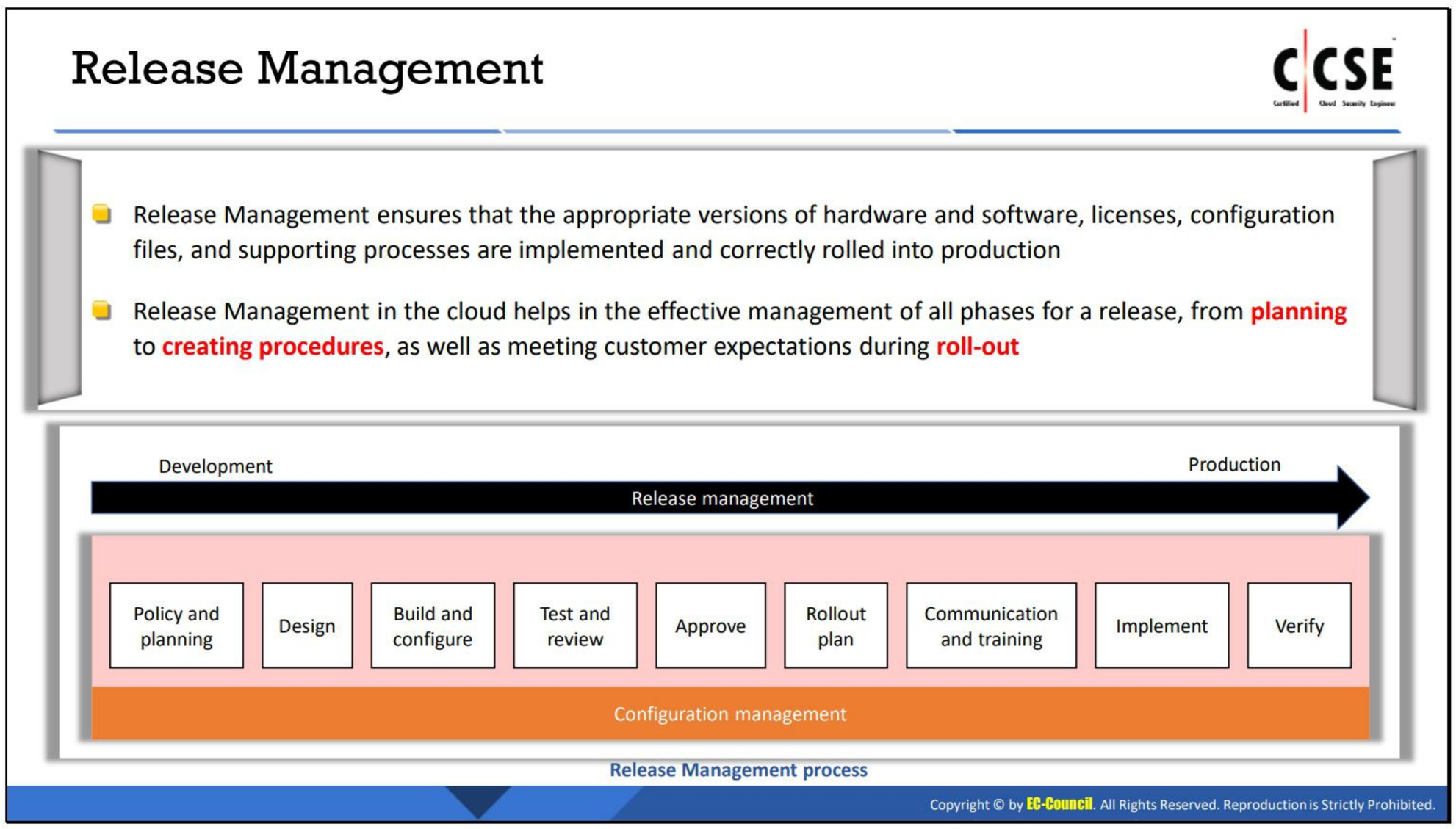
Problem closure and evaluation: This step ensures that full descriptions related to a problem along with the resolution steps are recorded while closing a problem. It helps in detecting incidents that are related to the closed problem.

Major problem review: It mainly focuses on preventing the recurrence of a closed problem and the collection of lessons learned in the problem resolution process. It helps in improving the problem management process.

Problem management reporting: It helps organizations to keep stakeholders updated about all outstanding problems, existing workloads, and current processing status.

Problem and error control: This step helps the problem management team to monitor the outstanding problems constantly. This helps them decide when to apply fixes or workarounds to the problems.

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



Release Management

Release management is a process that ensures that appropriate versions of hardware and software, licenses, configuration files, and supporting processes are implemented and correctly rolled into production. "Release" here refers to a newer version of a component or service. Release management in cloud helps in the effective management of all phases for a release, from planning to creating procedures and meeting customer expectations during roll-out.

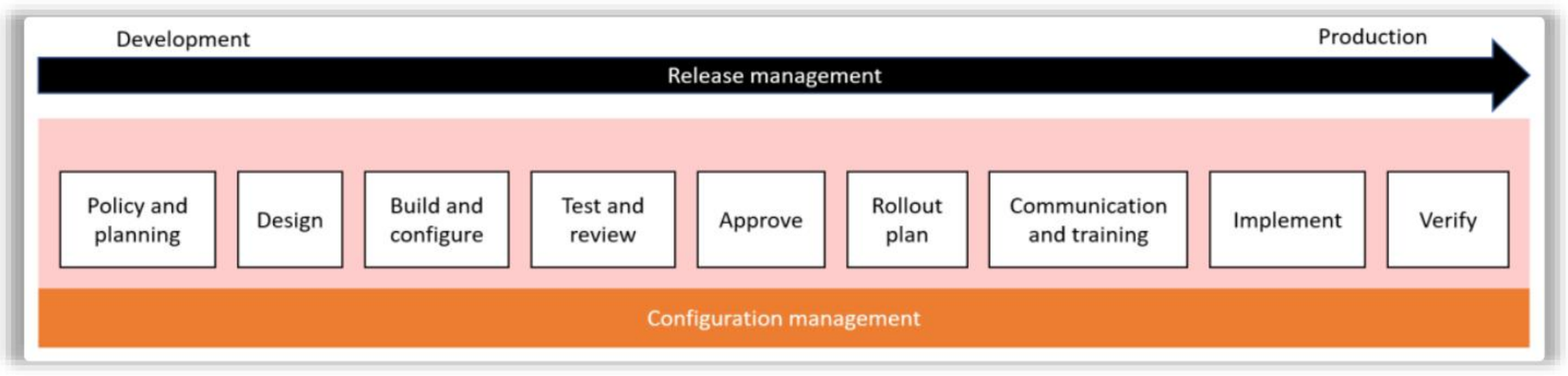


Figure 5.43: Release Management process

New software releases must be in accordance with the configuration plan. Release management is crucial for PaaS and SaaS providers. Security testing should be conducted on all new releases before they are deployed into production.

Objectives of Release Management

The main objectives of release management include

- Fast delivery of modified or new services at low cost
- Ensure that only authorized releases are deployed to minimize risk
- Maintain the integrity of release packages

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

- Knowledge transfer and manage risks
- Create and test release packages

Release Categorizations

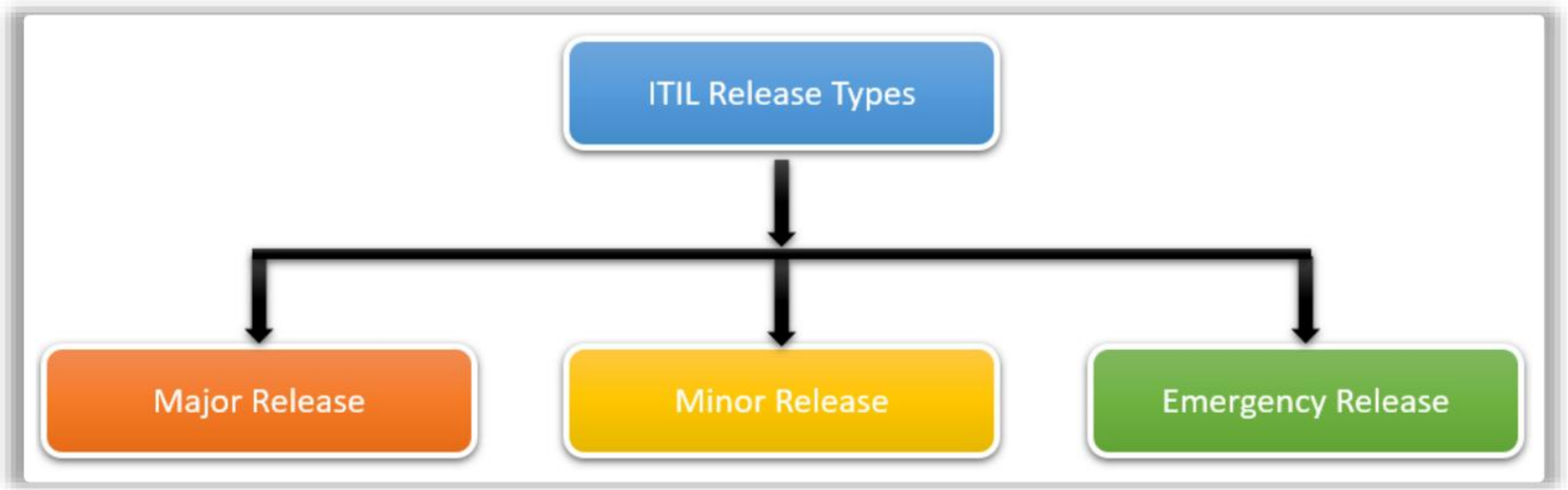


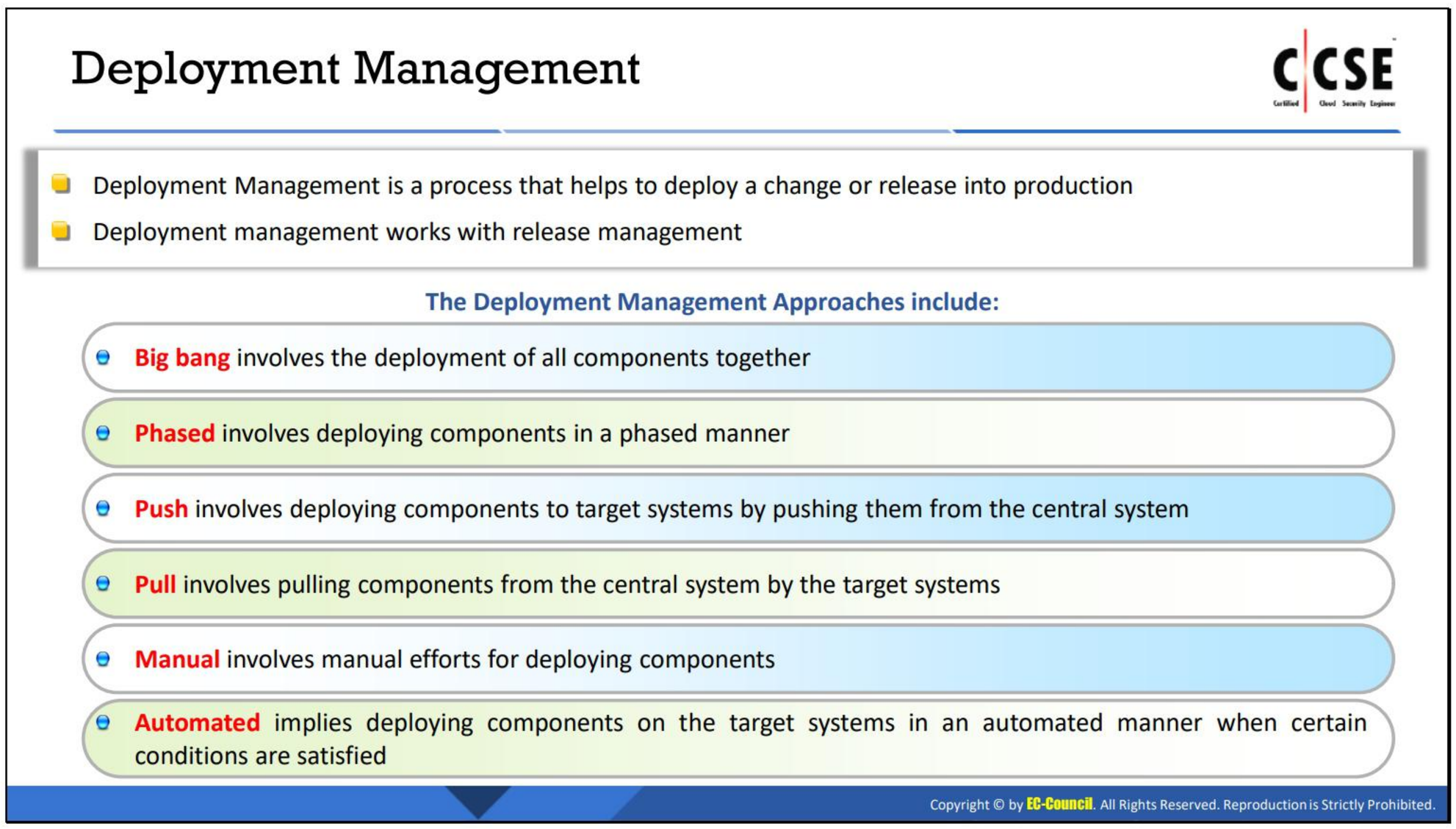
Figure 5.44: Types of releases

Releases may include emergency fixes as well as major or minor hardware or software changes.

- **Major release**: Major releases commonly include new software or hardware components or completely new functionality.
- **Minor release**: Minor releases commonly include improvements in the existing functionality and may contain fixes.
- **Emergency release**: Emergency releases are meant for fixing security bugs that require immediate attention.

hide01.ir

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



Deployment Management

Deployment management works with release management. After new releases are tested, they are deployed into production. Deployment management is a process that helps to deploy a change or release into production. It helps in deploying the new or modified service or component/feature based on the schedule proposed in the change request approved by a change authority. The main goal of deployment management involves moving new or modified processes, service components, software, or hardware into a live environment (production).

Objectives of Deployment Management

- Ensure the successful deployment of release package according to schedule
- Ensure that the deployment has minimal or no effect on production processes
- Specify and agree upon plans for deployment

Deployment Management Approaches

Various approaches can be used to perform deployment:

- **Big bang**: This deployment approach involves deploying all components together.
- **Phased**: This approach involves deploying components in a phased manner. It is the most commonly used deployment approach.
- **Push**: This approach involves deploying components to the target systems by pushing them from the central system.
- **Pull**: In this approach, the target systems pull components from the central system for deployment.

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

- **Manual**: This deployment approach requires manual efforts to deploy components.
- **Automated**: This approach involves deploying components on the target systems in an automated manner when certain conditions are met or satisfied.

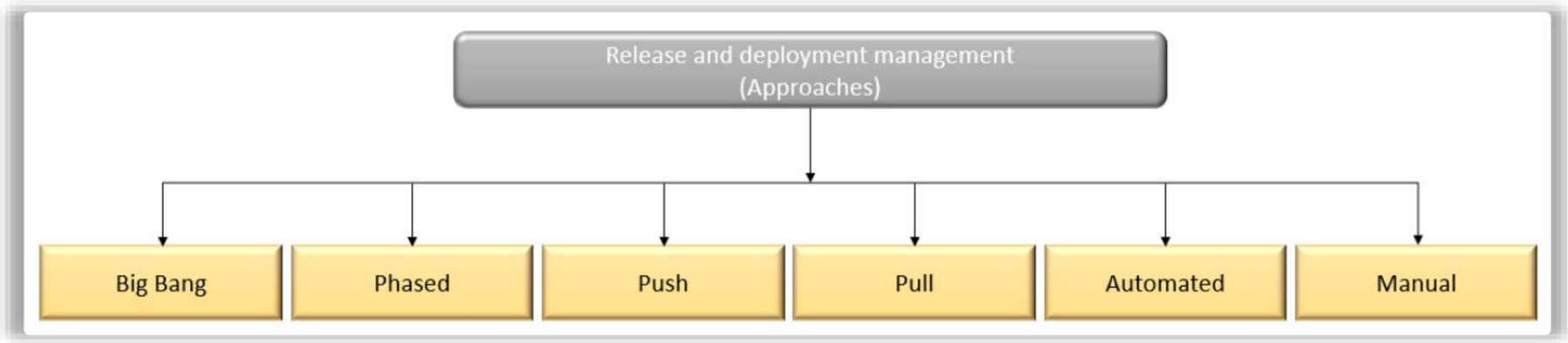
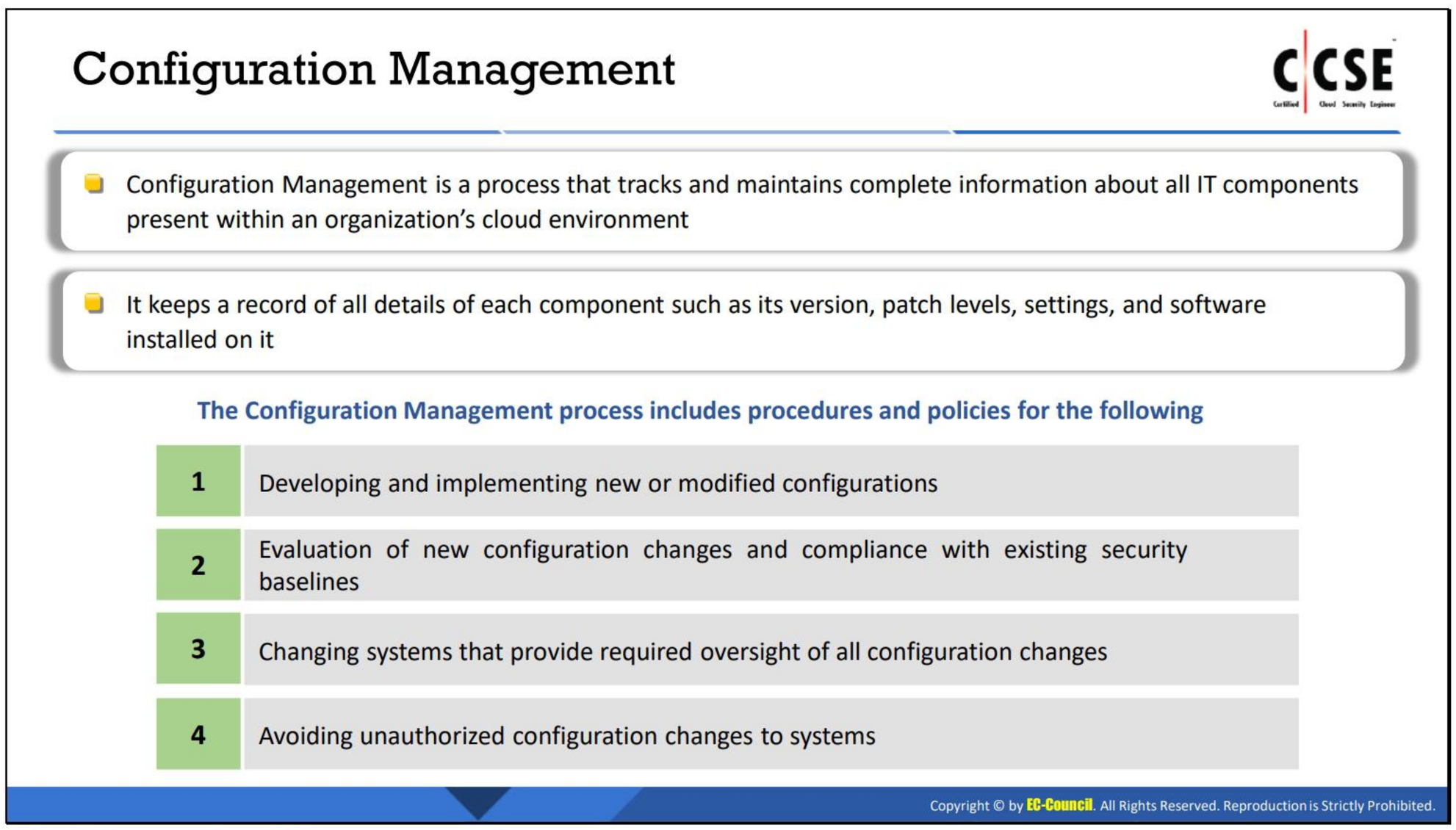


Figure 5.45: Deployment approaches

hide01.ir

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



Configuration Management

Configuration management is a process that tracks and maintains all information about the IT components present within an organization's cloud environment, including appliances, servers, and devices. It maintains a record of all details of each component, such as its version, patch levels, settings, and software installed on it. The main objective of configuration management is to maintain all information related to service configurations and configuration items (CIs).

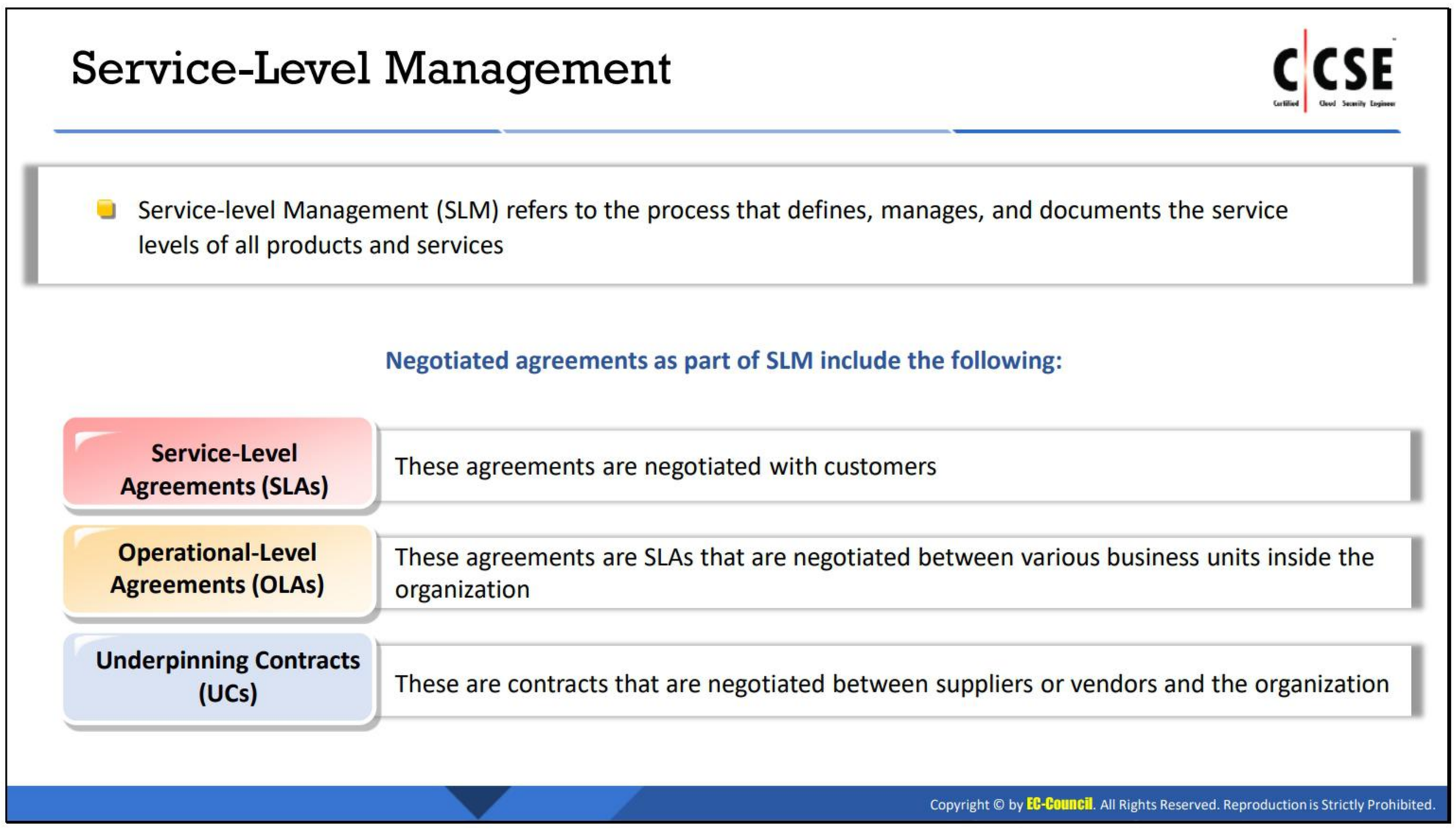
It is an iterative process that tracks changes to the configuration of cloud systems as and when they occur. When new devices or systems are configured and added to a cloud environment, they are added to the configuration database immediately. The configuration database, a key part of configuration management, stores data about all CIs and their relationships. All hardware, software, documents, and users that form a service are called CIs.

The configuration database should be regularly updated while updating a service or implementing a change and the integrity of all CIs and their configurations should be maintained. Configuration management helps organizations to monitor configuration changes in their cloud environments and detect unauthorized changes easily. Configuration management is closely related to change management and availability management.

Cloud security professionals must create a configuration-management process for cloud infrastructure, which must include procedures and policies for the following:

- Development and implementation of new or modified configurations that must apply to the existing software and hardware configurations of the cloud environment.
- Evaluation of new configuration changes and compliance with the existing security baselines.
- Changing systems (e.g., deployment and testing procedures). They should provide the required oversight of all configuration changes.
- Avoiding unauthorized configuration changes to systems.

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



Service-Level Management

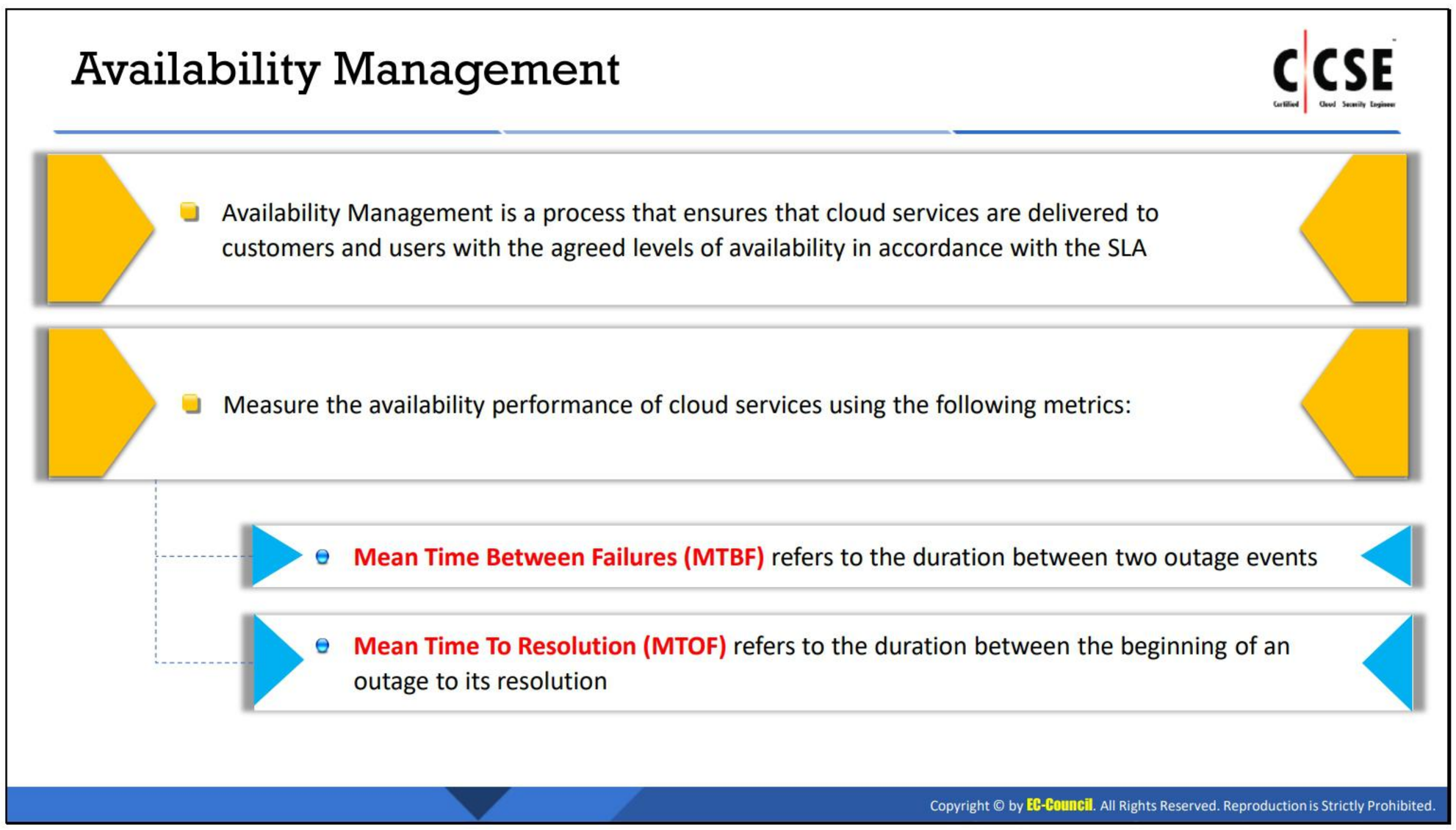
Service-level management (SLM) refers to the process that defines, manages, and documents the service levels of all products and services. It helps to negotiate agreements with multiple parties to provide services based on the agreed-upon service-level targets. SLM sets realistic expectations (or SLAs) for clients and makes cloud service providers accountable for meeting those expectations.

Negotiated agreements as a part of SLM include the following:

- **Service-Level Agreements (SLAs)**: These agreements are negotiated with customers.
- **Operational-Level Agreements (OLAs)**: These agreements are SLAs that are negotiated between various business units inside an organization.
- **Underpinning Contracts (UCs)**: These are contracts that are negotiated between suppliers or vendors and the organization.

The main aim of SLM is to monitor and manage the performance of services against the agreed-upon targets between clients and cloud service providers. Understand the nature of business while setting SLAs. Ensure that the SLM process helps to understand the concerns and requirements correctly. Organizations must incorporate SLM practices to set clear business-based targets for the performance of their services. This will help them to assess, monitor, and manage the delivery of services against these targets. Establish appropriate policies, tools, and procedures to ensure that the organization meets the service levels as agreed in the SLA with its customers.

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



Availability Management

Availability management is a process that ensures that cloud services are delivered to customers and users with the agreed levels of availability according to the SLA. It strives to define, analyze, measure, and improve each aspect of cloud service availability. It ensures that all IT infrastructure, processes, roles, and tools work according to the agreed-upon availability targets. The main objective of availability management is to ensure that the business requirements are satisfied with the expected level of service availability. Cloud systems provide better availability than non-cloud systems.

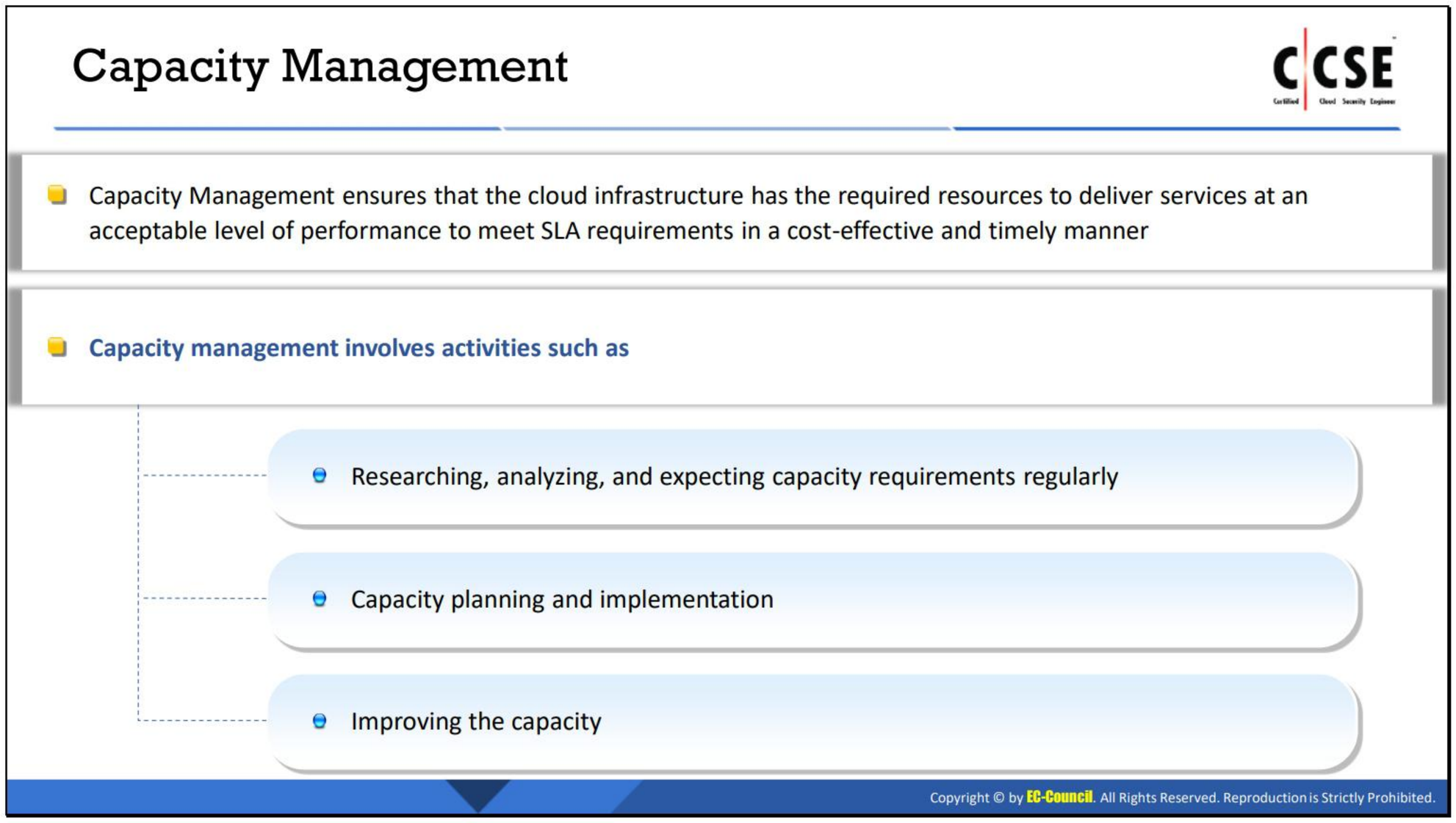
Ensure that all systems are designed to meet the availability requirements mentioned in SLAs. Availability management activities must help to

- Negotiate and agree upon the targets that are achievable for availability
- Build infrastructure and apps in a way in which they can deliver the expected availability levels
- Ensure that components and services can gather the data required to determine availability
- Ensure proper monitoring, analyzing, and reporting on availability
- Plan to improve the availability of services continually

Measure the availability performance of cloud services using the following metrics.

- **Mean Time Between Failures (MTBF)**: It is the distance in time or duration between two outage events. A larger MTBF is desired for high availability performance.
- **Mean Time To Resolution (MTOF)**: It is the distance in time or duration from the beginning of an outage to its resolution.

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



Capacity Management

Capacity management ensures that the cloud infrastructure has the required resources to deliver services at an acceptable level of performance to meet the SLA requirements in a cost-effective and timely manner. It considers all resources that are necessary to deliver IT services inside the scope of specified business requirements. The system capacity should be monitored and it should be ensured that systems do not reach an over-capacity situation by setting thresholds. Moreover, the availability of sufficient capacity should be ensured with systems to deliver services at the expected performance level.

Ensure that systems are not under-provisioned or over-provisioned because both result in loss of reputation/business or low profits. Capacity management ensures that this balance is maintained and systems are adequately provisioned. Cloud services and performance become slow when cloud systems are under-provisioned, resulting in loss of business. When cloud systems are over-provisioned, maintaining them will incur more cost, which will result in low profits.

Capacity management involves activities such as

- Researching, analyzing, and expecting capacity requirements regularly
- Capacity planning and implementation
- Improving the capacity

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

Evidence Management

- Digital forensics refers to the application of science to identify, collect, examine, and analyze data while ensuring information integrity and a strict chain of custody for the data
- Cloud forensics refers to the application of all digital forensics processes in the cloud environment
- Cloud forensics involve the below processes:
  - **Forensic Data Collection Methodologies**
  - **Evidence Management**
  - **Collect, Acquire, and Preserve Digital Evidence**
- Evidence Management refers to managing the evidence (while preserving its integrity, authenticity, and admissibility) from collection to trial in cloud forensics
- Only collect the requested or required data because it helps in minimizing data exposure and ensures compliance with the regulatory requirements
- Do not disclose any evidence collection requests, requirements, or activities with other tenants

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

Evidence Management (Cont'd)

hide01.ir

Forensic Data Collection Methodologies

- Cloud consumers can undertake forensic data collection with the support of providers
- The cloud forensics process has the following phases

Cloud Forensics Process Flow

Collect, Acquire, and Preserve Digital Evidence

- Ensure a clear understanding of how CSPs will handle, format, and preserve data in a legal case
- There should be clauses related to data collection and preservation as well as the specific roles and responsibilities on behalf of both parties (CSP and cloud consumers) in the contract for legal purposes
- Ensure that data handling and moving are performed according to contractual terms to avoid any legal complications and fines

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

Evidence Management

Digital forensics refers to the application of science to identify, collect, examine, and analyze data while ensuring information integrity; moreover, a strict chain of custody is maintained for the data.

Cloud forensics refer to the application of all digital forensics processes in a cloud environment. All customers in a cloud environment do not have uniform ownership or access to data owing to

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

different service models. IaaS customers have a high degree of ownership over VMs and the components hosted on them. However, PaaS and SaaS customers have limited ownership and control over their data and access.

The following processes support cloud forensics:

- Forensic Data Collection Methodologies
- Evidence Management
- Collect, Acquire, and Preserve Digital Evidence

Forensic Data Collection Methodologies

The contract and SLA between cloud consumers and providers must clearly define the access, support, and response timelines to collect forensic data irrespective of the cloud service model. Cloud consumers can undertake forensic data collection with the support of providers.

The cloud forensics process has the following phases:

Figure 5.46: Cloud Forensics Process Flow

hide01.ir

Identification of Evidence

In the first phase of the cloud forensics process, identify the evidence after confirming the occurrence of a security event. Identifying the evidence is a difficult process in cloud environments because they have various deployment and service models, and the devices cannot be physically confiscated. Thus, identify all possible data sources where evidence can be found and ensure that the integrity of evidence is not lost.

Evidence Collection

Acquire data from different sources (e.g., VMs, routers, hosts, servers, etc.). Identify the potential data sources to collect evidence data.

Follow the procedure mentioned below to collect evidence.

- **Develop a plan to collect evidence data**

  Multiple data sources are present in a cloud environment; thus, it is crucial to identify and prioritize potential data sources suitable for evidence collection. Additionally, establish the order in which data must be collected. Consider the following factors to prioritize potential data sources.

  - **Likely value**: Evaluate the relative likely value of every potential data source based on the understanding of the existing situation and previous experience with similar situations.

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

- **Volatility**: Give priority to volatile data first for evidence collection. Volatile data include the data present on a running system that can be lost owing to any action performed on the system, shutting down the system, or with time.
- **Efforts needed**: Consider the efforts required to collect evidence. The amount of effort required to gather evidence data from different sources differs. This includes the time spent on collecting evidence by security professionals and the cost of services (e.g., external experts) and equipment used.

- **Collect data**

  Use forensic tools to acquire volatile data, collect non-volatile data by duplicating their data sources, and secure the original non-volatile data sources. Collect data locally or over a network (remotely). Although it is better and recommended to collect data locally (because it offers greater control over the data and systems), it is not always possible. While collecting data (remotely) over a network, understand the type of data that should be collected and the amount of effort utilized. For example, collecting data from multiple systems may be required via different network connections in some cases, but in some cases, copying a logical volume from a single system may be sufficient.

- **Verify data integrity**

  Verify the integrity of collected data to prove that it is not tampered with or modified, especially for legal purposes. Use tools to verify the integrity of collected data. These tools compute the message digests of copied and original data and then compare these digests to ensure that they are the same (not tampered with).

hiteo.ir

- **Decide how to preserve the collected evidence before collecting it**

  Preserve the evidence so that it supports its use (it remains valid and useful) in internal disciplinary or legal proceedings in the future. Follow a clearly defined chain of custody in such situations to prevent allegations of tampering or mishandling of evidence. This chain of custody includes logging the activities of people who have physical custody of the evidence, storing it in a secure location when not in use, and using only the evidence copy for examining and analysis.

- **Use network forensics to capture, store, and analyze network events**

  Use network forensics because they can capture every network packet and store it in a searchable database to examine them in detail whenever required. Use network forensics to trace actions or conversations back to physical devices by exposing the low-level address of the communicating systems. It helps to reconstruct the entire content of emails, instant messaging conversations, file transfers, and web-surfing activities to reveal the original transaction.

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

Network forensics helps investigators to:

- Disclose the proof of an attack
- Troubleshoot performance issues
- Source data leaks
- Ensure compliance with policies by monitoring activities
- Create audit trails for business transactions

Collect evidence from various sources

Collect evidence from the following sources:

- **Host OS**

  Collecting evidence from a host OS requires physical access. A VM hosted on a host may be transferred to one or more hosts after an incident; thus, collect evidence from the host OS where the VM resides.

- **Guest OS**

  - Collect a forensic image by taking a snapshot of the guest OS.
  - Use write blockers to prevent unintentional writing of data to the host OS or guest OS while collecting evidence.
  - Use various tools to collect evidence from the guest OS.

hidedn.ir

- **Collect Metadata**

  Metadata are present at every stage of the cloud architecture as users create them. Establish a plan and policy to manage and collect metadata.

- **Cloud log analysis**

  Logging helps to identify various operational issues, fraudulent activities, and incident violations. It also helps in investigating various types of attacks. Use cloud log analysis to detect the source of evidence from various devices and components such as hard disk, VM instances, and RAM images. Analyze the following logs to get information related to various types of attacks:

  - Application logs
  - System log
  - Firewall log
  - Network log
  - Web server log
  - Audit log
  - VM log

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

- **Cloud storage**

  Collect evidence from cloud storage such as Google Drive, Dropbox, and SkyDrive using web browsers and downloading files via the existing software tools. Detect unauthorized modification or illegal access to cloud storage and check if the attacker modified the timestamp information in any user account.

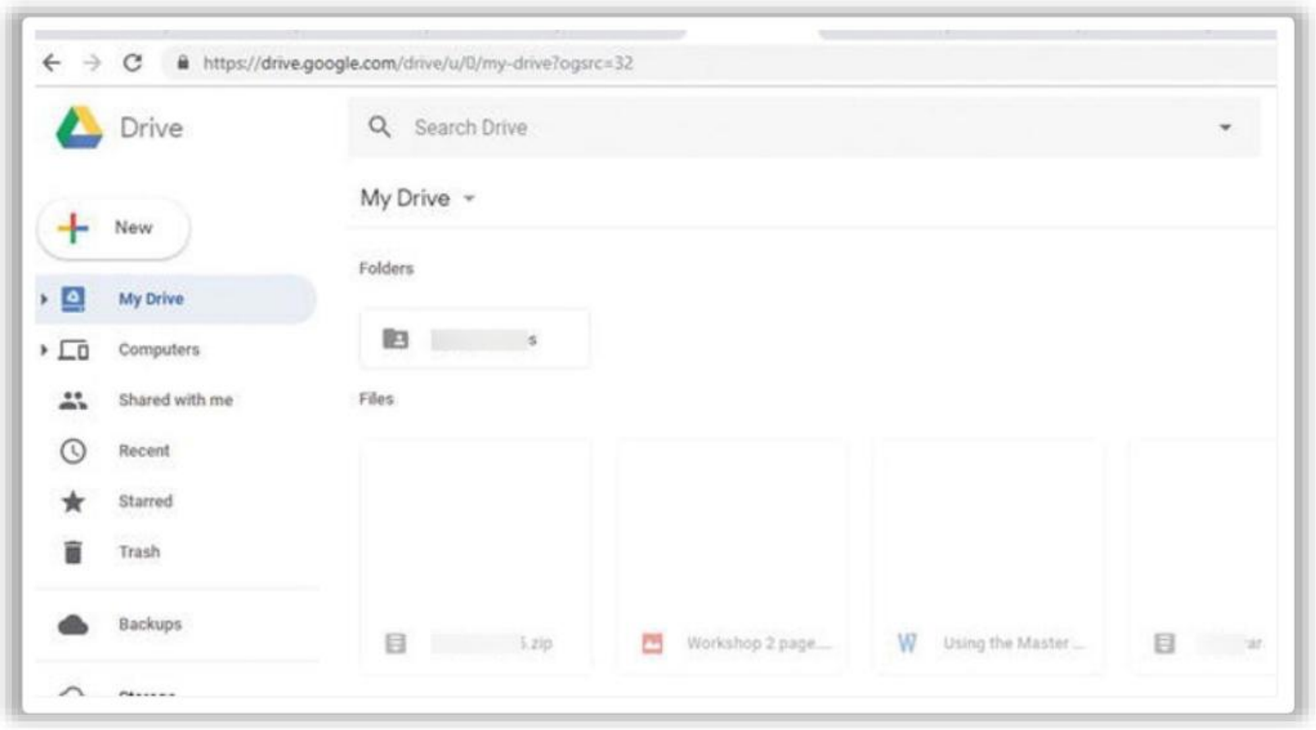


Figure 5.47: Google drive evidence

- **Web browser**

  Consumers or clients use web browsers to communicate with the cloud servers in a cloud environment. They perform multiple tasks on their web browsers such as accessing emails, news, or shopping online. Collect evidence by analyzing website URLs from the web browser history, user browsing behavior, and timeline analysis. For example, use a Chrome forensic tool to record and analyze the Google web browser data. This tool analyzes the data from web logins, history, cookies, bookmarks, and archived history.

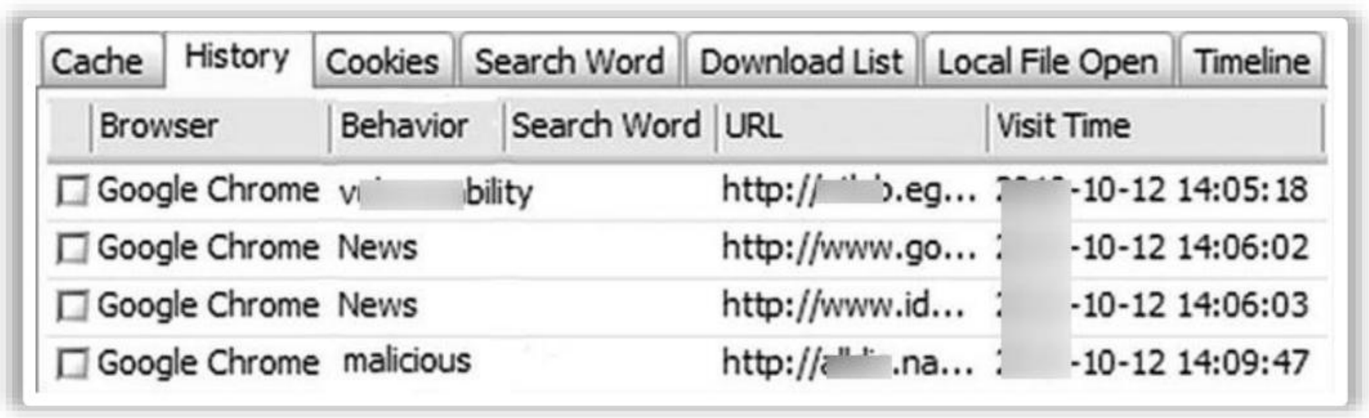


Figure 5.48: Google Chrome forensic tool

- **Physical memory analysis**

  Acquire caches of cloud usage such as encryption keys, network socket information, and in-memory database. Analyze them using the “pslist” function from the physical memory dump. The “pslist” function recovers the process identifier, process name, parent process identifier, and process initiation time.

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

Examination and analysis of data

Once data are collected, they are examined. Extract information from the collected data. The examination phase may involve the following processes:

- Bypass OS or app features that hide data and code such as encryption, data compression, and access control mechanisms.
- Use pattern or text searches to detect relevant data; for example, finding documents that contain a particular subject.
- Utilize tools that can detect the type of contents contained in each data file such as graphics, text, and music.
- Utilize databases that contain information about the known files to exclude or include files from further consideration.
- Analyze the collected data to correlate data between various sources. It includes identifying items, people, places, and events and finding the relationship between them to infer a conclusion.
- Use tools such as security event management software and centralized logging because they can speed up this process by collecting and correlating data. To detect different types of changes made to the system, compare system characteristics with the known baselines.

ide01.ir

Presentation and Reporting

In the final phase of the cloud forensics process, prepare and present the information derived from the previous (analysis) phase. Prepare all reports related to the entire cloud forensics process. Usually, reports contain relevant information about the case such as the details of CSP, people involved in the investigation, and analysis methods used.

Consider the following factors while preparing reports.

- **Alternative explanation**

  If complete information about an event is not available, precise conclusions about the event cannot be made. If there is more than one reasonable explanation for an event, each explanation must be given equal consideration in the reporting process. Ensure the use of a methodological approach to approve or reject every possible explanation proposed in the report.

- **Audience consideration**

  Know and understand the audience to which the information will be presented. Different audiences require different types of reports.

- **Actionable information**

  Reporting should include the detection of actionable information extracted from the data to gather new sources of information. For instance, prepare a list of contacts from the

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

data, which may provide extra information regarding an incident. Additionally, prevent future security events from using information from the data.

Evidence Management

Evidence management refers to the management of evidence (while preserving its integrity, authenticity, and admissibility), from collection to trial, in cloud forensics. Maintaining data integrity and chain of custody is crucial for managing and preserving the collected evidence. Ensure that appropriate policies and procedures are implemented for collecting and maintaining the evidence. Failing to ensure proper processes and controls, the evidence data might be later deemed inadmissible in the court of law during scrutiny. Ensure that data are collected within the scope of the requesting legal document. This allows to limit the disclosure of data collected and minimizes the changes in sensitive data exposure. Some legal discovery orders bound CSPs to prevent the information of activities performed (for that order) by them from being exposed.

Only collect the data requested or required because it helps in minimizing data exposure and ensures compliance with the regulatory requirements. Keep the evidence management process confidential when the requester is a government body or the request is a part of sensitive criminal investigation by limiting the staff working on it and taking necessary measures.

Do not disclose any evidence collection requests, requirements, or activities with other tenants. Cloud consumers are bounded via SLAs or contracts to not disclose any confidential information regarding evidence management shared with them by the CSP through multiple channels.

Collect, Acquire, and Preserve Digital Evidence

ride01.ir

Digital forensics deals with the application of science to identify, collect, examine, and analyze evidence data without compromising the integrity of information and maintaining a chain of custody for the data. Organizations have multiple data sources that generate and store a huge amount of data. Data are shared between various devices in an organization for operational purposes; moreover, data are often subjected to regulatory and security requirements and must be secured from attackers.

Digital forensics can be used to investigate internal policy violations, crimes, troubleshooting operational issues, reconstructing computer security incidents, and recovering from accidental system damage. Organizations must be capable of performing digital forensics to identify the events that occurred in their systems and networks such as sensitive information exposure. They must have a clear understanding of how the cloud service providers will handle, format, and preserve data in a legal case. There should be clauses related to data collection and preservation as well as the specific roles and responsibilities of both parties (the CSP and cloud consumers) in the contract for legal purposes. Data handling and moving must be performed according to the contract terms and court orders (if received) to avoid any legal complication and fine.

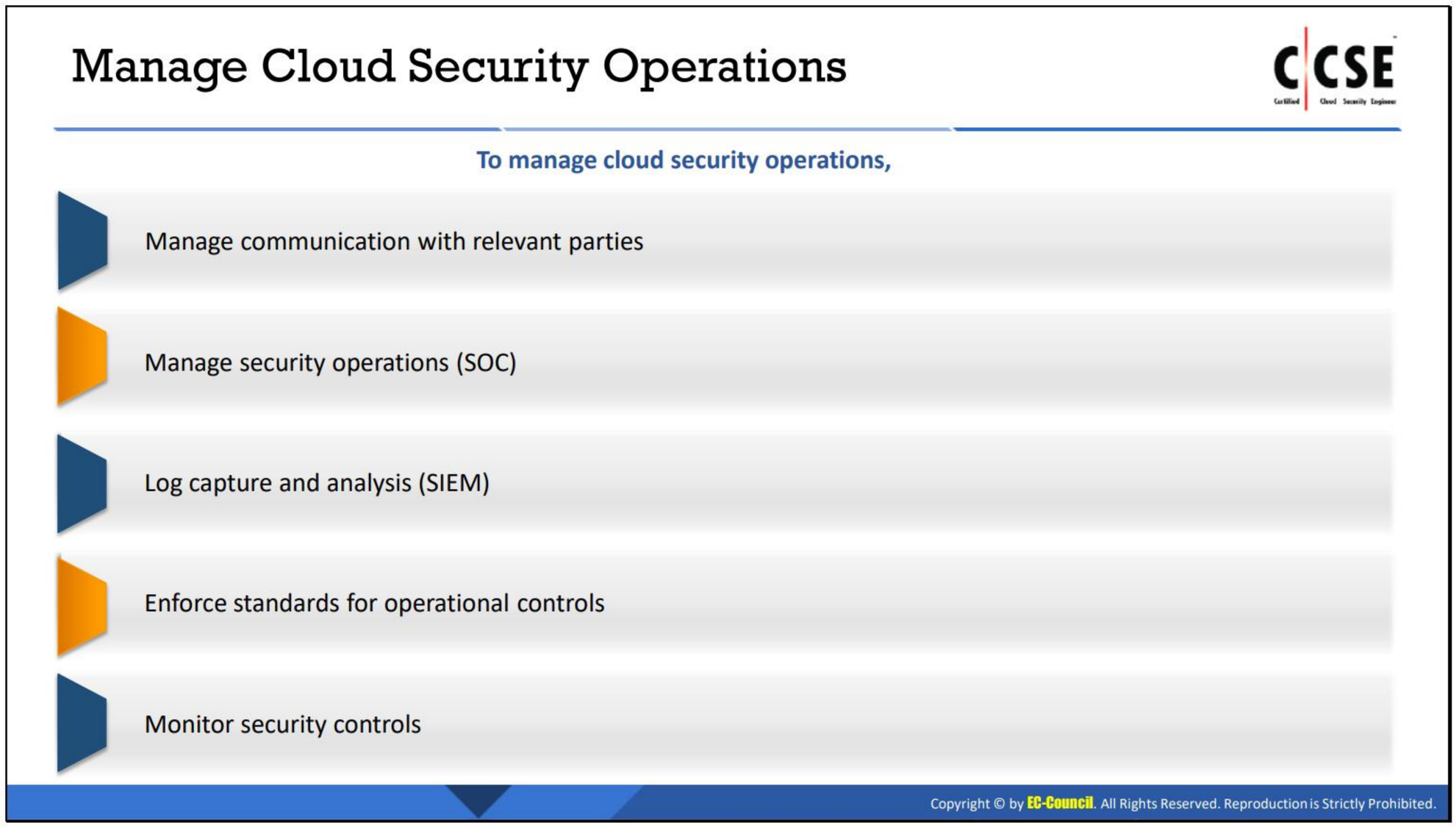
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

LO#7: Learn to Monitor Security Operations for Cloud Infrastructure

The objective of this module is to understand the management of cloud security operations using various tools and strategies. This includes maintaining proper communication between parties, managing security operations using the security operations center (SOC), and log capture and analysis using security information and event management (SIEM). From this section, cloud security engineers can learn how to implement standards for operational controls using various tools and monitor security controls to secure the organizational cloud environment.

hidd01.ir

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



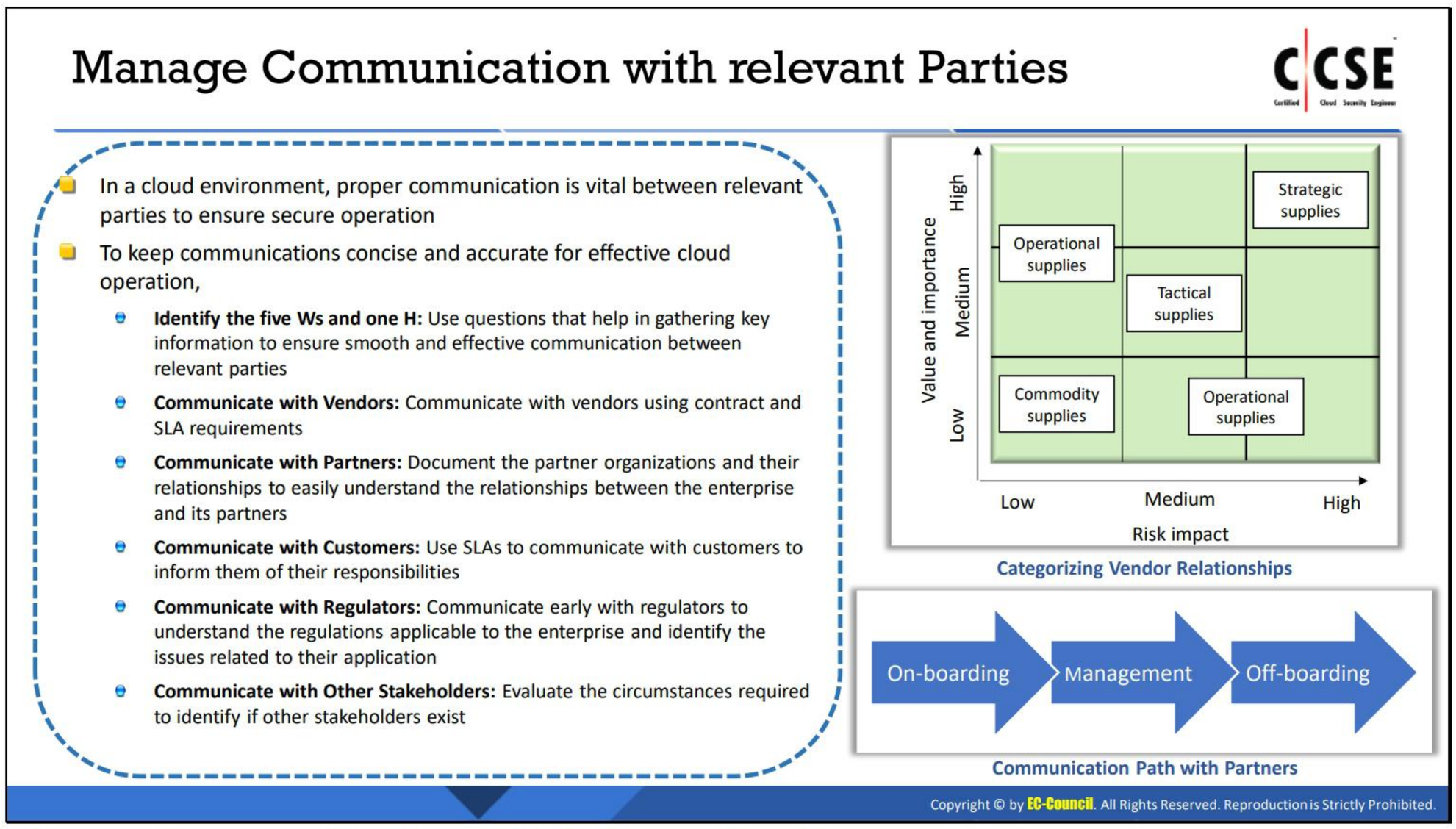
Manage Cloud Security Operations

To manage cloud security operations, implement the following:

- Manage communication with relevant parties
- Manage security operations (SOC)
- Log capture and analysis (SIEM)
- Enforce standards for operational controls
- Monitor security controls

hidedr.ir

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



Manage Communication with Relevant Parties

In a cloud environment, proper communication is vital between relevant parties to ensure secure operations. Keep communications concise and accurate to make cloud operations effective.

Identify five Ws and one H

Identify the need for 5 Ws and 1 H to communicate because it directly impacts the governance across the organization. They include questions that help in gathering key information to ensure smooth and effective communication between relevant parties.

The 5 Ws and 1 H of communication indicate the following:

- **Who** indicates "Who is the main target of the communication?"
- **What** indicates "What is the communication designed to get?"
- **When** indicates "When is the communication most likely to reach its desired target?"
- **Where** indicates "Where is the communication pathway best managed from?"
- **Why** indicates "Why is the communication being started?"
- **How** indicates "How is the communication being transmitted and received?"

Communicate with Vendors

Use contract and SLA requirements to define ways to communicate with vendors effectively. Both parties (the organization and vendor) can have policies in the contract regarding communication requirements, type of communication (reports), and their frequency. Throughout the relationship with the vendor, vendor communication is essential and must cover everything, from initial on-boarding to off-boarding.

Understand the policies and capabilities of the supporting vendors and ensure to create and test emergency communication paths with them. While managing vendors/suppliers, rank them on a suitable scale. This will help in effectively managing the relationship with them.

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

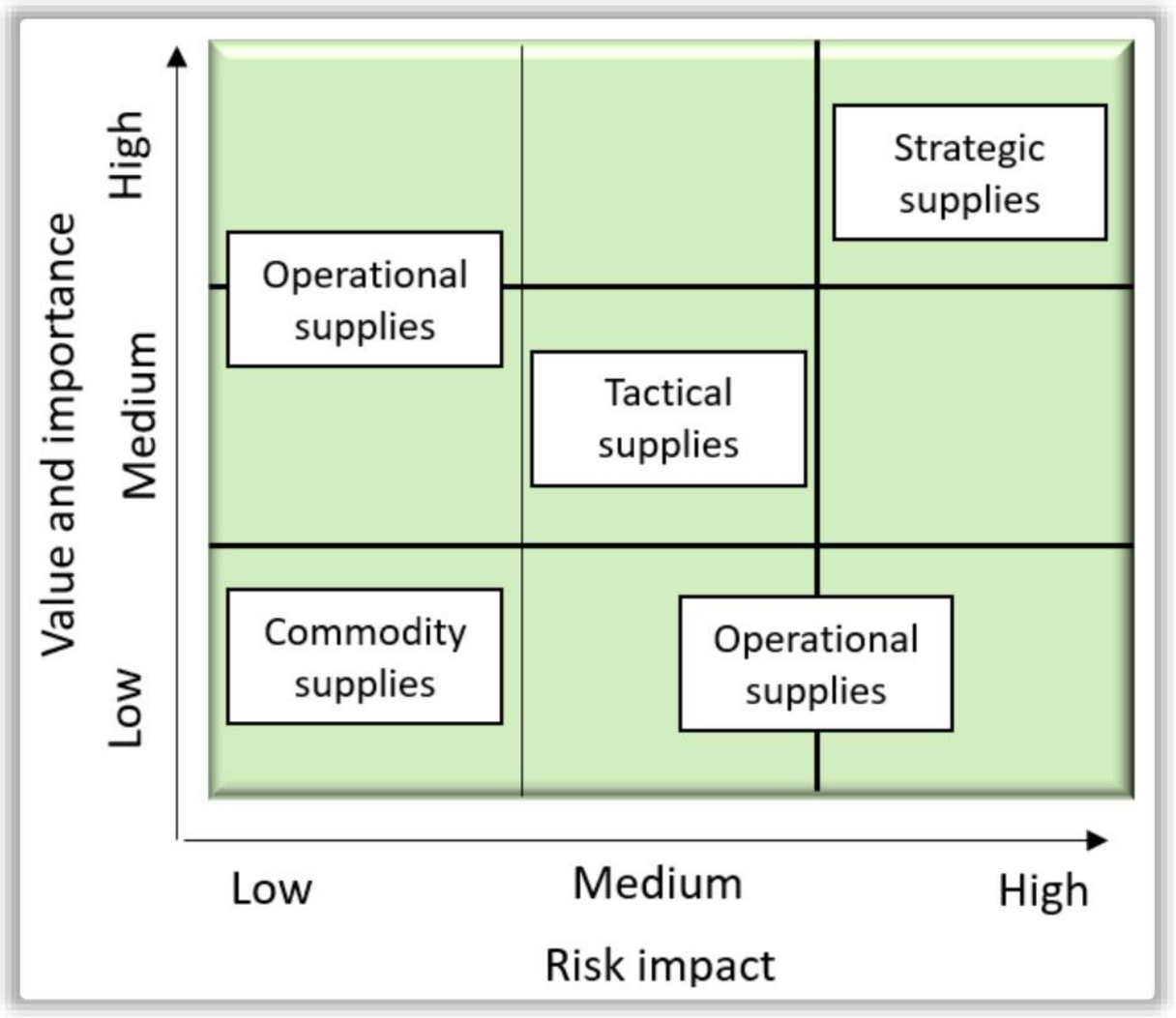


Figure 5.49: Categorizing vendor relationships

The above graph clearly shows that strategic suppliers are the most crucial and cannot be replaced by other suppliers easily. This type of suppliers may be few, but they are vital for the success or failure of the organizational cloud architecture. In contrast, commodity suppliers hold the lowest rank because they provide commodities that can be sourced from other suppliers easily; thus, they are easily replaceable.

Communicate with Partners

Partners are somewhat different from vendors in terms of communication because partner organizations do not have the same type of contractual relationships as cloud providers and consumers. Partners can have federated relationships within a cloud environment via federated services and federated access to cloud resources. Federated organizations have a formal agreement between them that articulates the requirements and expectations for their partnership.

Ensure that communication paths are established with all partners that support or use cloud services in the enterprise. Document the partner organizations and their relationships to easily understand the relationships between the enterprise and its partners. Partners can be federated or non-federated, and both have different levels of access to cloud services. Ensure that a proper on-boarding process is implemented for all partners to be thoroughly tested before they are granted access to systems.

Figure 5.50: Communication path with partners

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

Manage the partners under the current enterprise security infrastructure until the relationship is in force and never provide access by exception. When a partnership with a partner is terminated, ensure that proper off-boarding policy and procedures are communicated to the partner and their access to enterprise systems (cloud or non-cloud) is terminated.

Communicate with Customers

There are two types of customers in an enterprise: internal and external customers. Both types of customers consume cloud services differently and are important for the success of a cloud environment. Understand the customer audience that consumes cloud services to determine how various audiences use cloud services, their goals, requirements, and issues. These things must be documented, managed, and tracked over the cloud environment lifecycle.

Use SLAs as a way to communicate with customers to inform them about their responsibilities. Establish appropriate SLAs to manage the cloud services used by each type of customer. These SLAs must specify the service levels required by customers and specific metrics that differ for customers based on their type and needs. SLAs provide detailed information about the roles and responsibilities of both customers and providers to understand their responsibilities and ensure secure cloud operations. SLAs must contain the following metrics:

- Availability of services for what percentage of time
- Number of users who can use services at a time
- Performance benchmarks against which actual performance are compared
- Schedule for notification before making network changes that might affect users
- Service/help desk response time for solving different types of problems
- Usage statistics that are to be provided
- Remote access availability

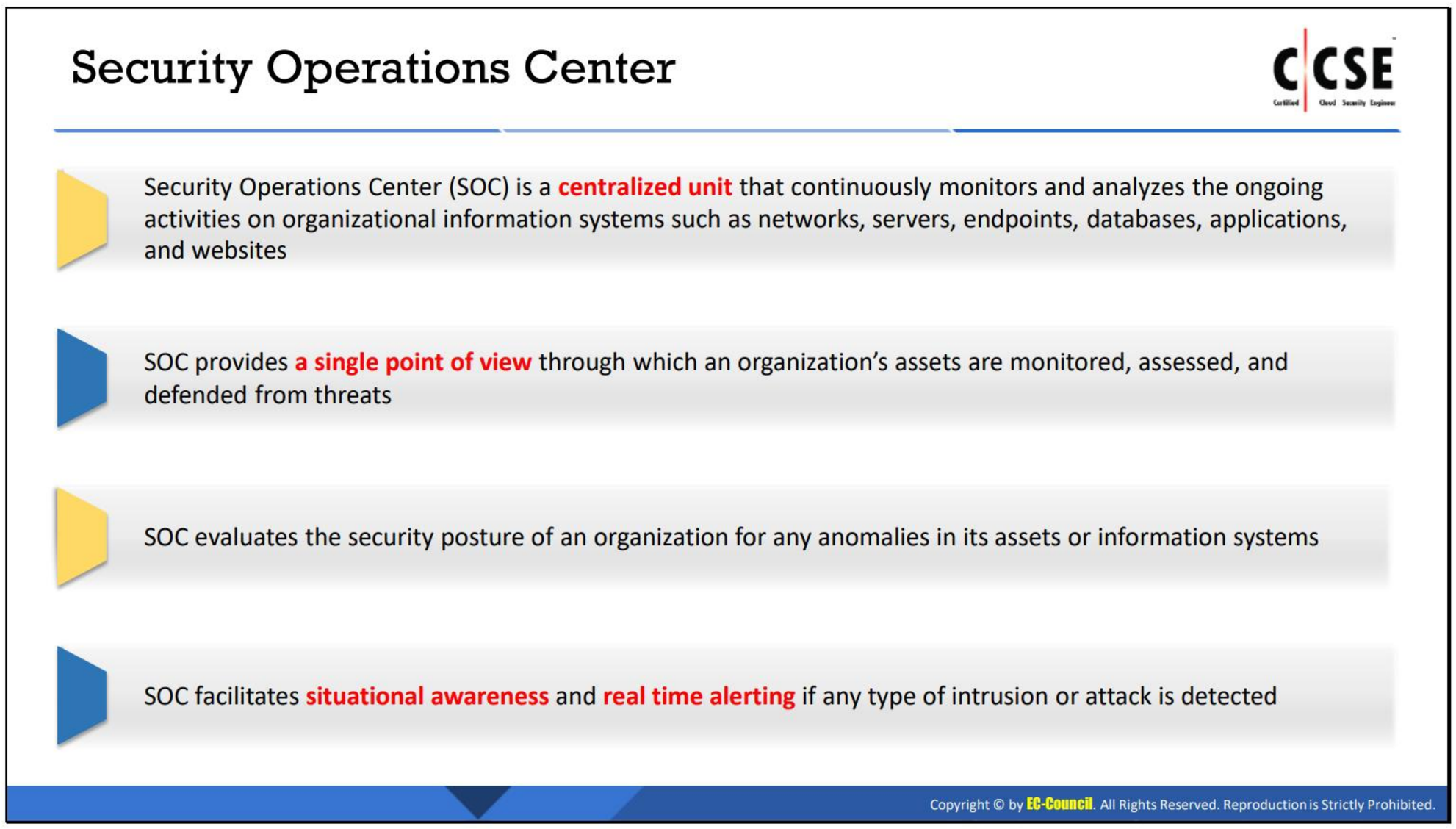
Communicate with Regulators

While developing a cloud environment, communicate with regulators early to understand the regulations that are applicable to the enterprise and identify any issues related to their application. As a cloud security professional, ensure that the cloud infrastructure complies with the applicable regulatory requirements. Regulatory requirements are different for different organizations based on their geography, business type, and services provided. Several regulatory authorities often publish their regulatory recommendations and requirements to help organizations know about them easily.

Communicate with Other Stakeholders

Other relevant stakeholders may have to be involved in the communication process based on a particular project or regulatory requirements. Evaluate the circumstances to identify if other stakeholders exist. If other stakeholders are identified, determine what type of communication is required and its frequency.

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



Security Operations Center

Security operations are handled and managed with the help of the security operations center (SOC). SOC is a centralized unit that continuously monitors, manages, and analyzes the ongoing activities on organizational information systems such as networks, servers, endpoints, databases, applications, and websites. Its end-goal is to maintain the continuity of an organization by determining, preventing, detecting, and responding to intrusion events before they affect the business. It is also sometimes referred to as security defense center (SDC), security analytics center (SAC), cyber security center, network security operations center (NSOC), threat defense center, and security intelligence and operations center (SIOC). It provides a single point of view through which the organizational security and assets are monitored, assessed, and defended. It collects data from logs, IDS/IPS, firewalls, endpoint devices, and network flows and facilitates incident detection, investigation, and response. It evaluates the security posture of an organization for any anomalies/organizational assets or information systems and facilitates situational awareness and real-time alerting if any intrusion or attack is detected.

hide01.ir

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

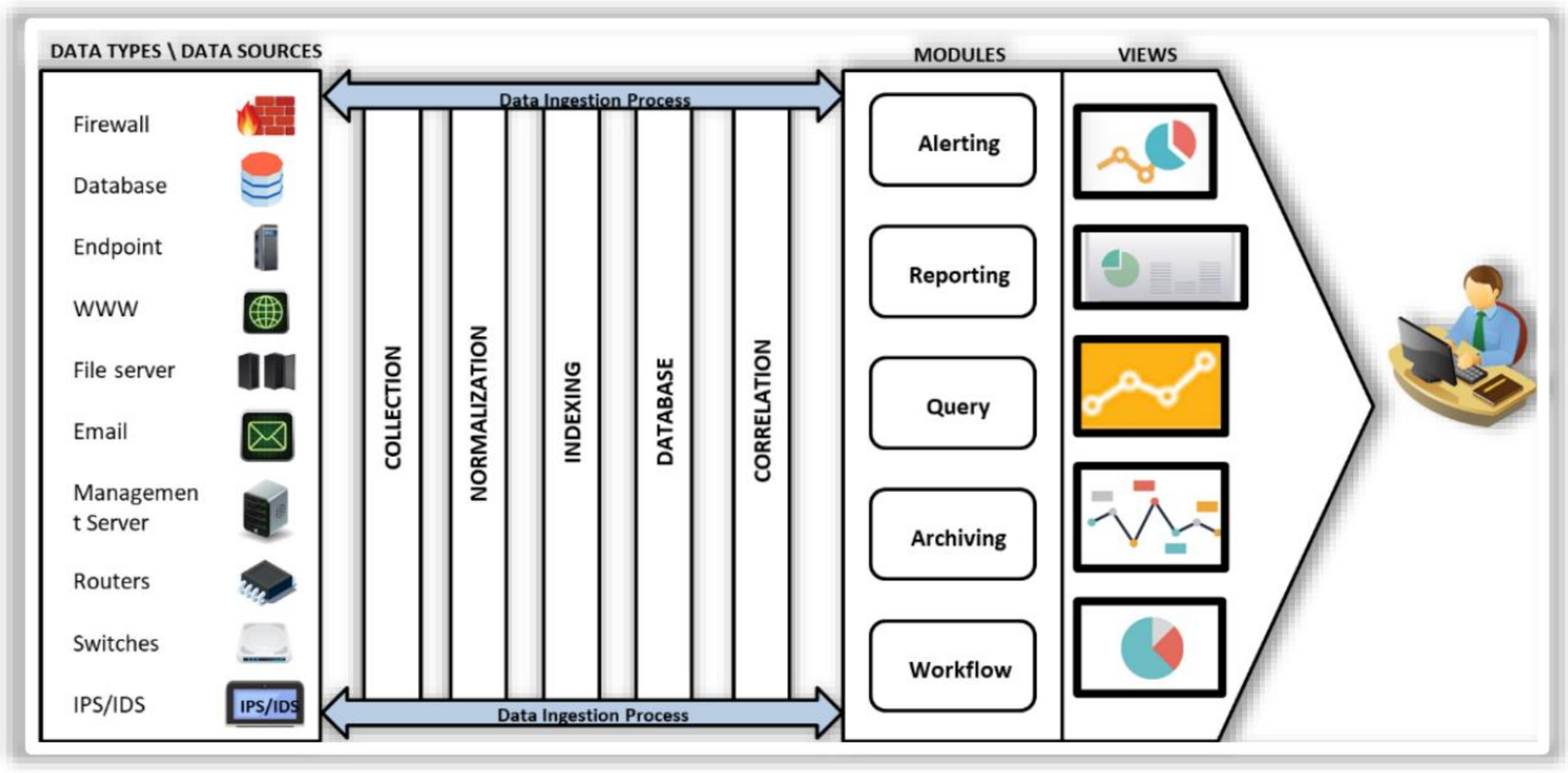
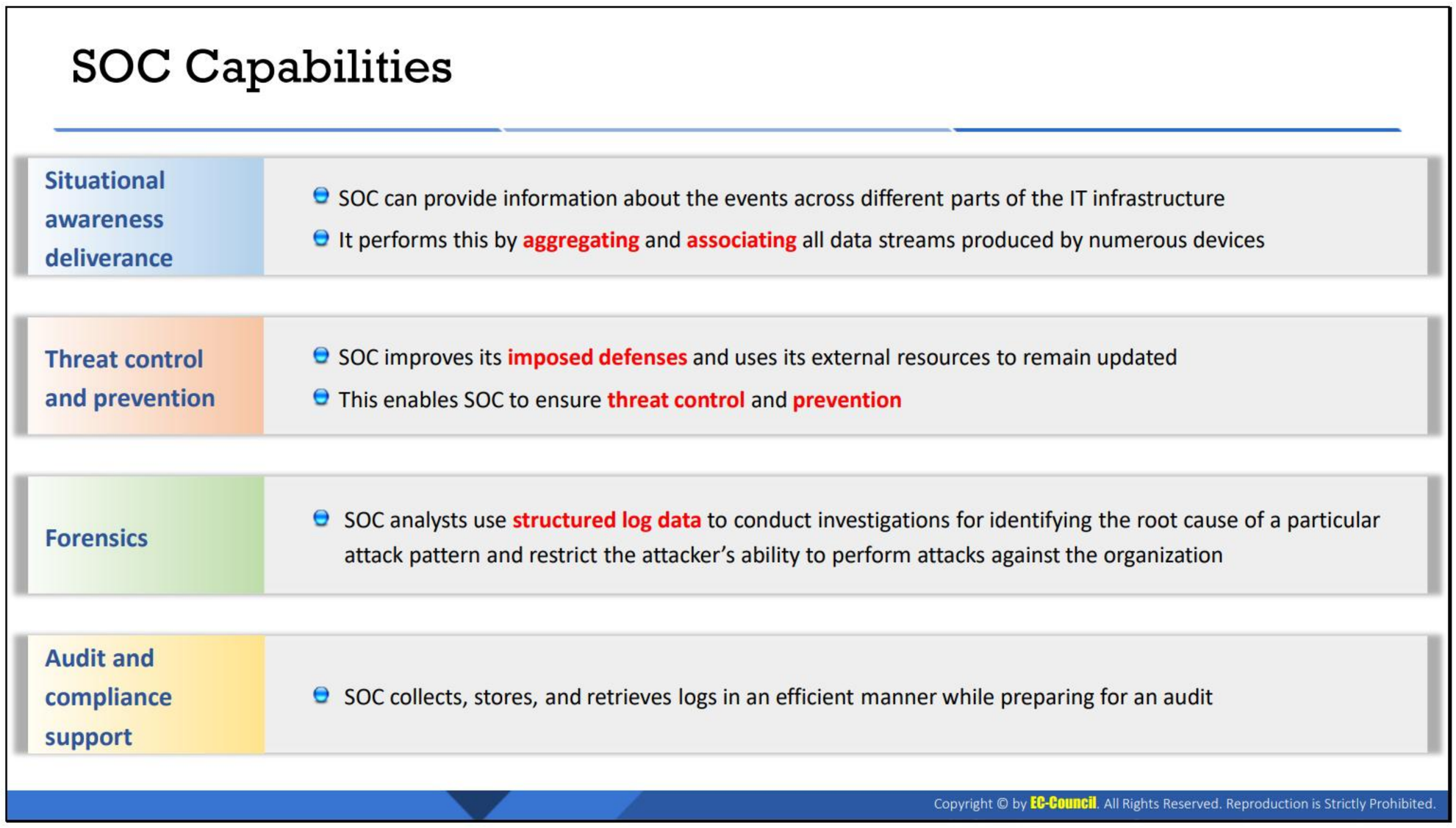


Figure 5.51: soc -Single Point View

hide01.ir

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



SOC Capabilities

The basic capabilities of an SOC include preventing, detecting, responding, and reporting security incidents.

hide01.ir

- **Preventing Capability**

  It refers to stopping an attack from being successful. To prevent an attack, SOC uses fine-tuning and maintenance tools. It also directs the incident response team to perform security monitoring. It uses the detection rules effectively and considers the indicators of compromise (IoC) detected by the incident response team. Thus, SOC detects risks and identifies their harmful impact on the organization to design a well-defined and vigilance plan.

- **Detection Capability**

  It refers to monitoring a system or network to identify suspicious activities and security breaches. To fulfill this purpose, SOC collects, analyzes, and correlates security events, and triggers alerts when suspicious activities are observed. It also informs clients of issues through notification and communication.

- **Responding Capability**

  It refers to analyzing and handling the documented alerts and security incidents instantly with security teams.

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

- **Reporting Capability**

  SOC offers various reports, which keep you updated about various assets and their security events, level of compliance, and alarms generated. SOC uses the security dashboard to display service indicators, technical indicators, and trend indicators.

- **Forensics**

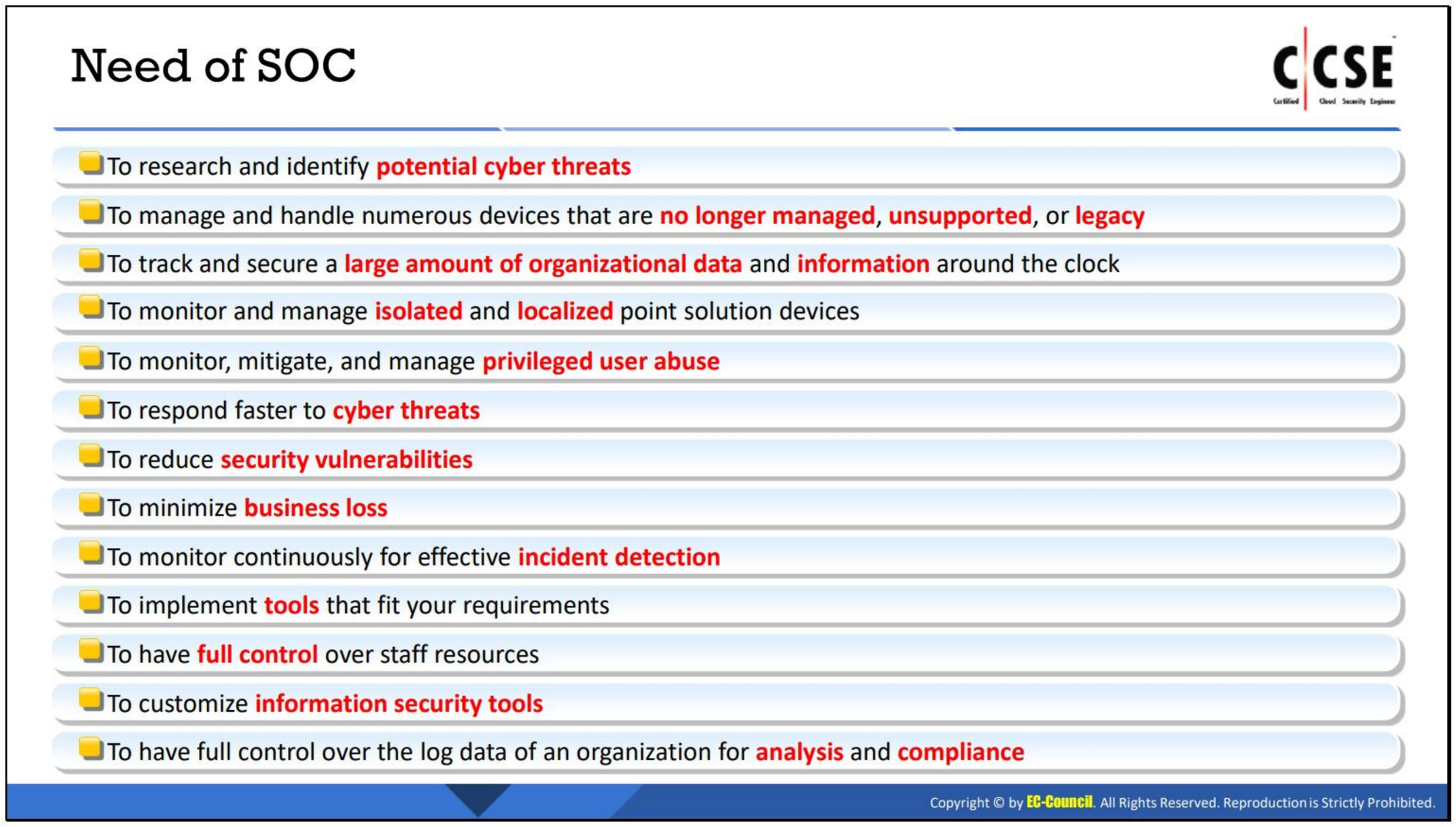
  SOC analysts use structured log data to investigate the root cause of a particular attack pattern and restrict the attacker's ability to perform attacks against the organization.

- **Audit and compliance support**

  SOC collects and stores logs, and efficiently retrieves them while preparing for an audit.

hide01.ir

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



Need of SOC

Organizations use various security measures such as intrusion detection/prevention system, firewall, email filtering, URL filtering, and antivirus to protect the organizational network from threats. However, in recent times, these security measures have been proven to be insufficient to provide enough security because hackers are inventing new trends and techniques to penetrate networks by evading such security measures. Thus, there is an increased demand for security measures that can ensure that the security perimeter is always updated with respect to new and developing threats and vulnerabilities. This is possible through SOC.

SOC is responsible for performing the following types of activities:

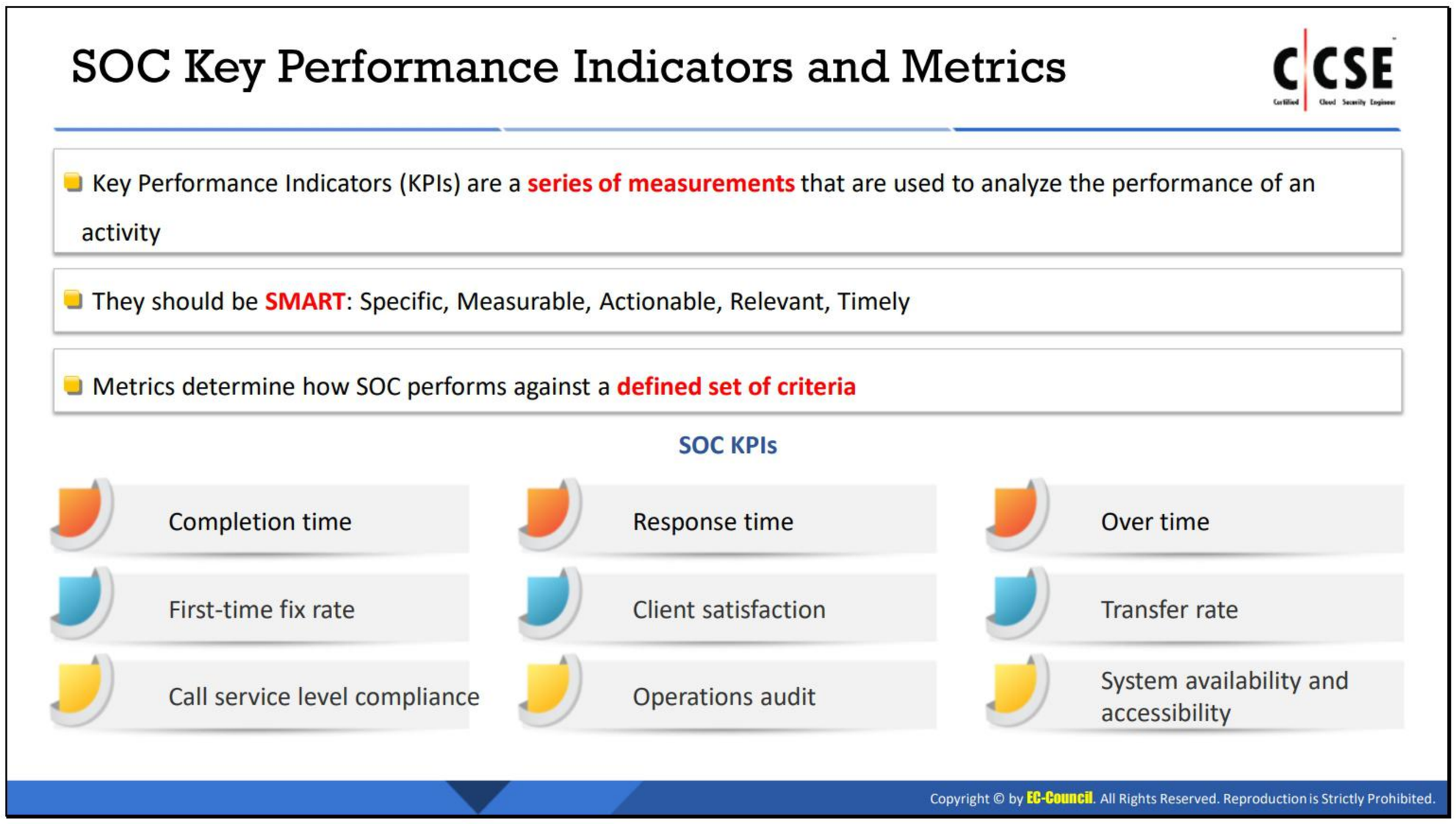
- Proactively identifying suspicious activities in the network and system
- Performing vulnerability management to identify activities that are vulnerable to the network
- Becoming aware of the hardware and software assets working in the network
- Performing log management that facilitates forensics during security breach
- Evaluating the policies and procedures required for business operations
- Checking whether the organization has appropriate internal controls and processes to provide proper services to clients
- Strengthening the environment of the organization
- Eradicating internal blinders
- Managing and handling numerous devices that are no longer managed, unsupported, or legacy

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

- Tracking and securing a large amount of organizational data and information around the clock
- Monitoring and managing isolated and localized point solutions devices
- Monitoring, mitigating, and managing privileged user abuse
- Responding faster to cyber threats
- Minimizing business loss
- Continuous monitoring for effective incident detection
- Implementing tools that fit your requirements
- Having full control over staff resources
- Customizing information security tools

hide01.ir

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



SOC Key Performance Indicators and Metrics

Key performance indicators (KPIs) are a series of measurements that are used to analyze the performance of an activity. It should be SMART: Specific, Measurable, Actionable, Relevant, Timely. Specific indicates that it should evaluate the attributes of a system directly; it should not depend upon the measurements of other systems as well as the integration of different systems. Measurable indicates that KPIs should provide accurate and complete information. Actionable implies that it should provide information that can be easily reviewed to determine the actions that can be performed. Relevant implies that it should be able to provide relevant data from the collected information. Timely indicates that it should provide information during requirement. The SOC has the following KPIs:

- **Completion Time**

  Time spent in completing the project as near as possible to 100%. It should be completed on the date demanded by the client.

- **Response Time**

  Time taken to respond to security incidents. It should be given as quickly as possible.

- **Over Time**

  Over time refers to organizing the staffing levels according to the expected volumes of calls and service delivery. It should be done in a manner that can reduce the unbillable over time and increase the profit and productivity of the system.

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

- **First-Time Fix Rate**

  It indicates the provision of the necessary information to the staff to monitor and respond to a site effectively. The information given to the client should be accurate enough such that they can take appropriate action against security incidents.

- **Client Satisfaction**

  It denotes the time taken to answer client questions and satisfy them. It should be done quickly, and to ensure this, the system should be properly automated.

- **Transfer Rate**

  These are incidents that are not handled properly by the first incident responder and are transferred to another incident responder. The transfer rate should be as minimum as possible.

- **Operation Audit**

  It is a scheduled or unannounced deep dive performed by the security team to validate the efficiency and effectiveness of the organization.

- **System Availability and Accessibility**

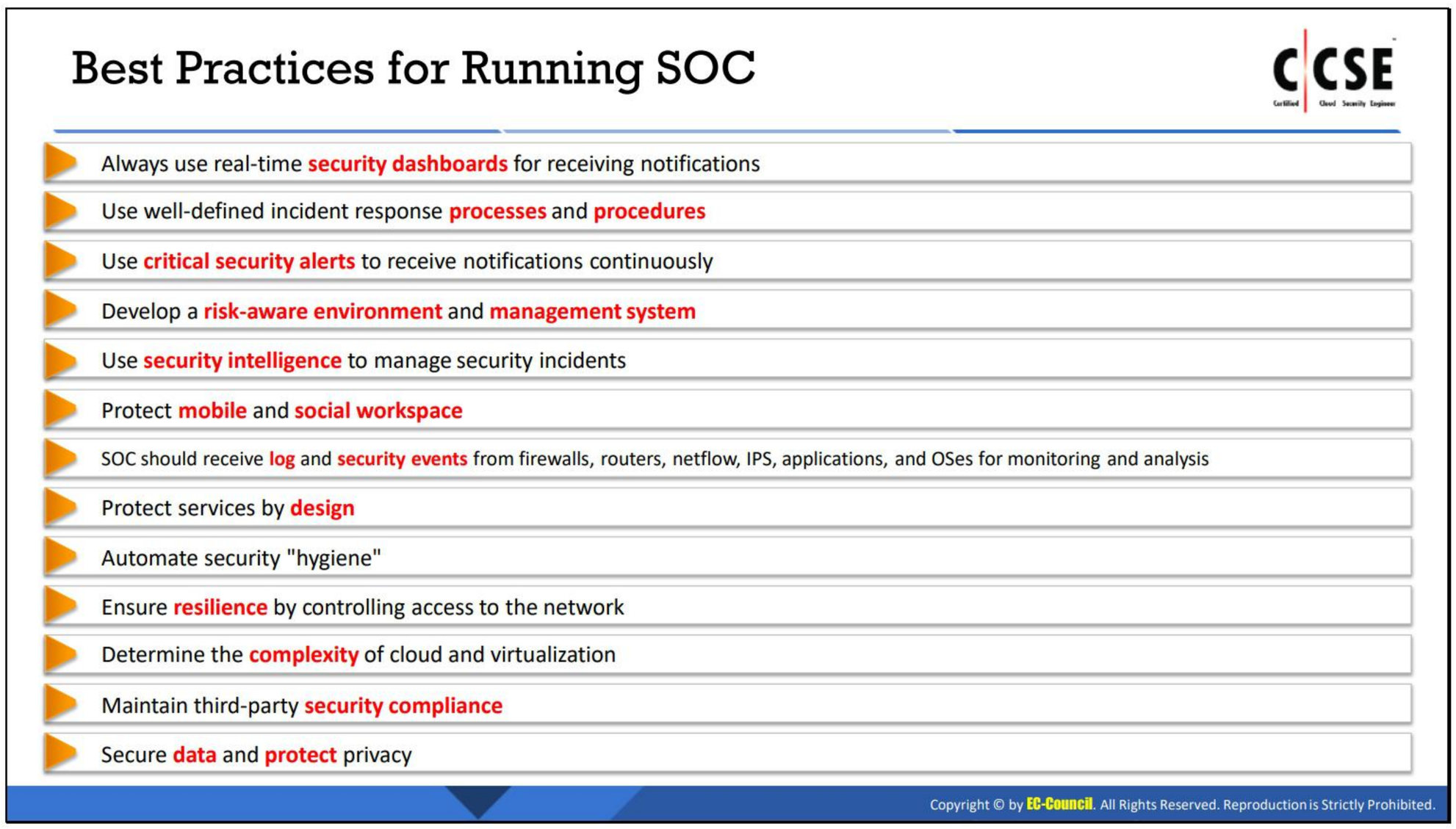
  It means measuring the up-time reliability of the critical system, subsystem, or process.

Metrics determine how an SOC performs against a defined set of criteria. It helps security analysts to make decisions and enhance performance and accountability. It provides an overview of the levels of regulatory compliance and validates whether security controls are implemented according to the policy, process, and procedure. It also facilitates the identification of security program effectiveness and the capabilities of people to handle issues as well as security trends, both inside and outside the organizational control.

In addition to this, the following metrics can be used to evaluate the performance of SOC:

- Number of security events given into SOC
- Number of data points gathered and analyzed
- Types of data collected and assessed
- Number of use cases
- Outcomes
  - Correlated events
  - Incidents/cases

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



Best Practices for Running SOC

SOCs use various security tools and technologies; however, security is not only dependent upon the tools and technologies but also requires a security team to focus on different factors such as scope of security team and their roles and responsibilities, organizational security budget, skills and knowledge of security analysts, business requirements, detecting and defending perimeters, building incident response systems, and right organization infrastructure.

Moreover, there are various other best practices that are required for running an SOC:

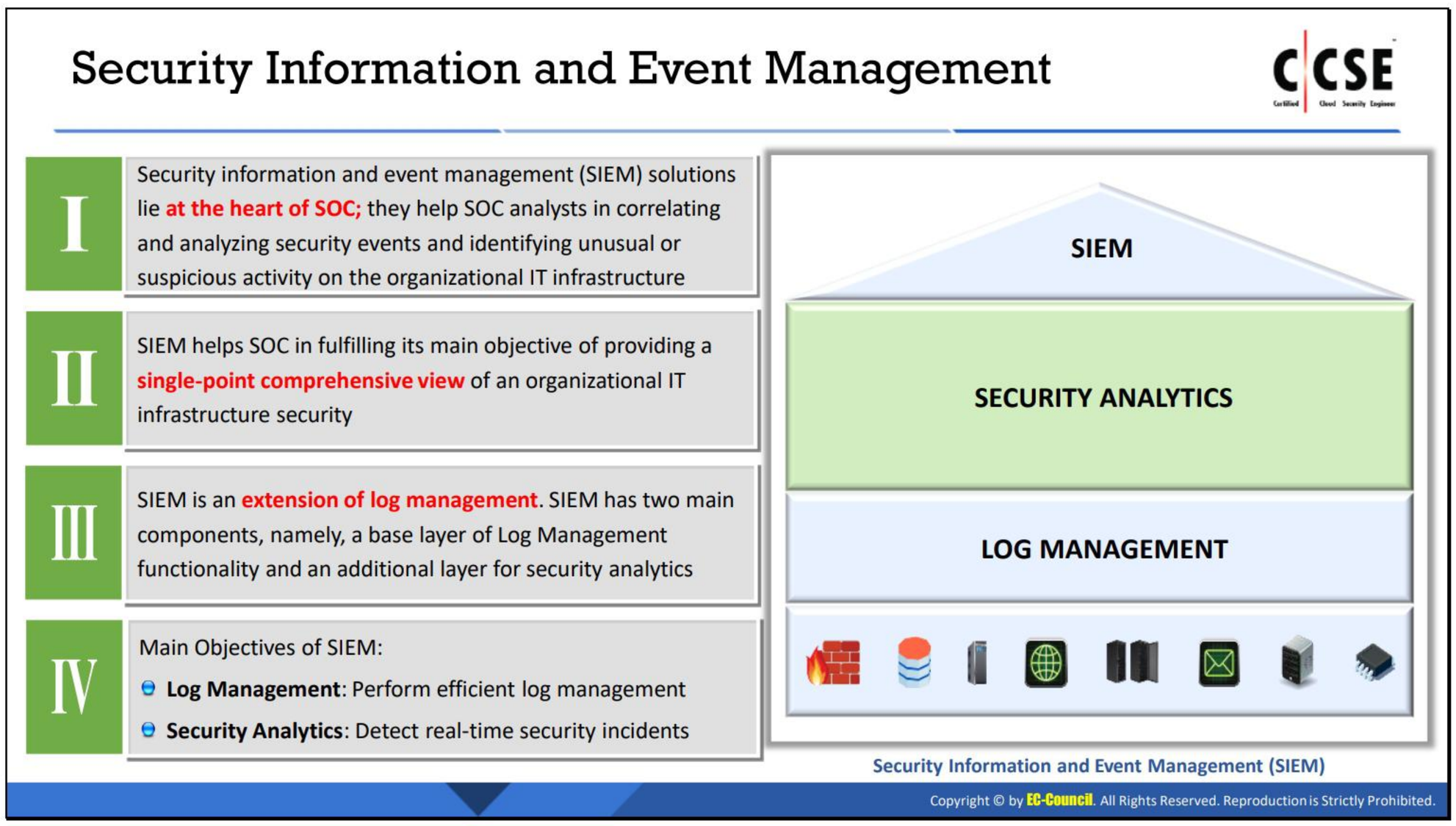
- Always use real-time security dashboards for receiving notifications
- Use well-defined incident response processes and procedures
- Use critical security alerts to receive notifications continuously
- Develop a risk-aware environment and management system
- Use security intelligence to manage security incidents
- Protect mobile and social workspace
- SOC should receive log and security events from firewalls, routers, NetFlow, IPS, applications, and OSes for monitoring and analyzing
- Protect services by design
- Automate security "hygiene"
- Ensure resilience by controlling access to the network
- Determine the complexity of cloud and virtualization
- Maintain third-party security compliance

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

- Secure data and protect privacy
- Understand the working of SOC and how it monitors the endpoints and networks, detects security threats and vulnerabilities, and handles them appropriately
- Use correct tools and technologies such as firewalls, data monitoring tools, automated application security, asset discovery systems, and endpoint protection system
- Use skilled and dedicated security specialists for monitoring and managing alerts, proposing security actions, and detecting threats internally
- Build an incident response team to provide effective responses to security incidents
- Form a team to collect information regarding security incidents

hide01.ir

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



Security Information and Event Management

Every organization requires expansion to maintain its business. Increasing the infrastructure implies adding more devices to the network. Monitoring and managing these devices become challenging for organizations because these devices perform different tasks in a distributed manner. Moreover, owing to the increased number of devices, systems, and data, the threat from newly evolved attacks also increases. Attackers are getting smarter and traditional security tools are not suitable for the latest requirements. Thus, managing the security of organizational infrastructure has become a difficult task for organizations. To alleviate the effect of advanced cyberattacks and manage the increasing volumes of log data from multiple sources, security information and event management (SIEM) is used.

SIEM facilitates security management because it provides a single point comprehensive view of the IT infrastructure security of an organization.

SIEM helps the SOC to collect the external and internal data from devices and monitor and analyze them. The SIEM solution is at the heart of SOC, which helps SOC analysts in correlating and analyzing network security events and identifying unusual or suspicious activity on the organizational IT infrastructure.

The main aim of SIEM is to analyze the log data and detect threats. This process is made easier by collecting all logs in one centralized location. SIEM detects threats that cannot be detected by traditional methods such as signature-based techniques. By communicating and reconfiguring the rules of firewalls and intrusion prevention systems, SIEM can take certain actions on the detected threats.

SIEM has two layers, a base layer of log management functionality and an additional layer for security analytics. The activities in both layers are distributed between the security information

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

management (SIM) and security event management (SEM) components of SIEM. SEM performs real-time monitoring, correlation of events, and incident response, whereas SIM collects, stores, analyzes, and reports the log data.

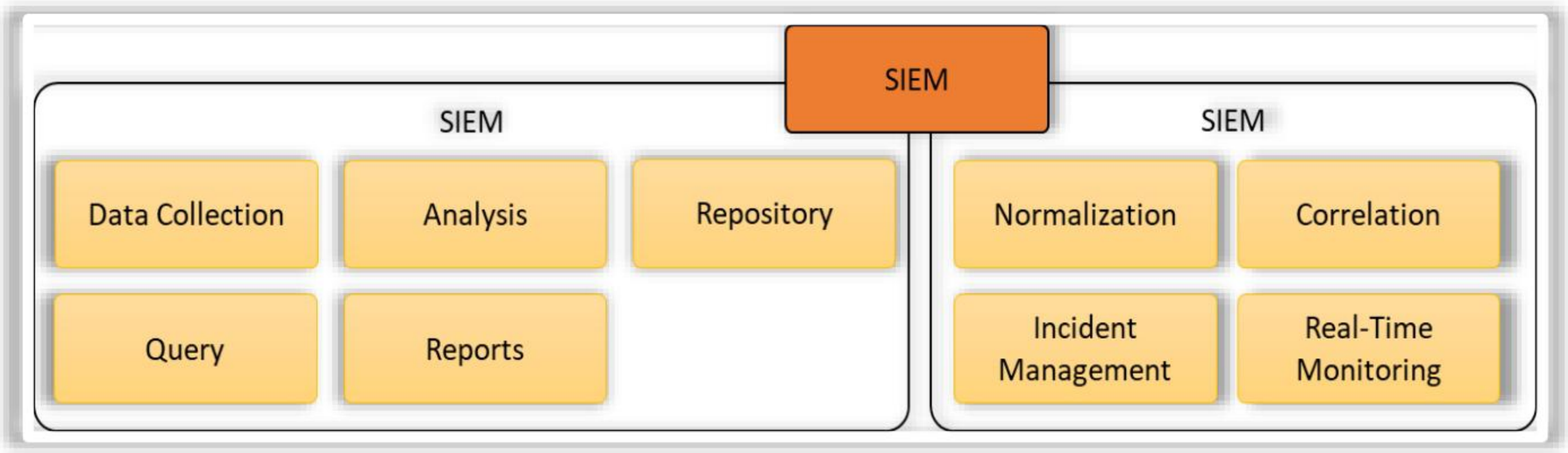
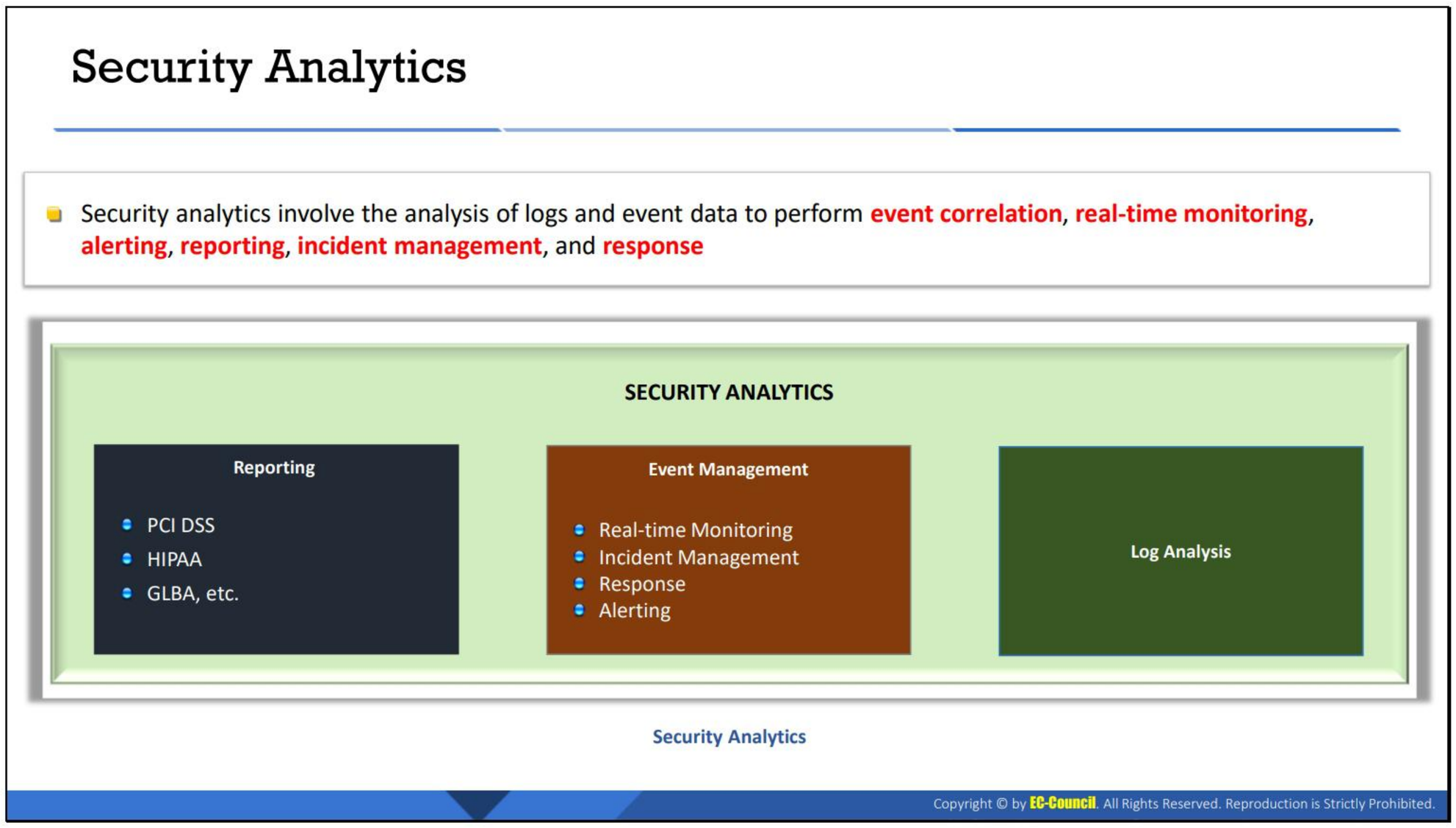


Figure 5.52: SIEM

Correlated logs and context data are ingested to SIEM to identify what is happening on the organization's IT infrastructure.

hide01.ir

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

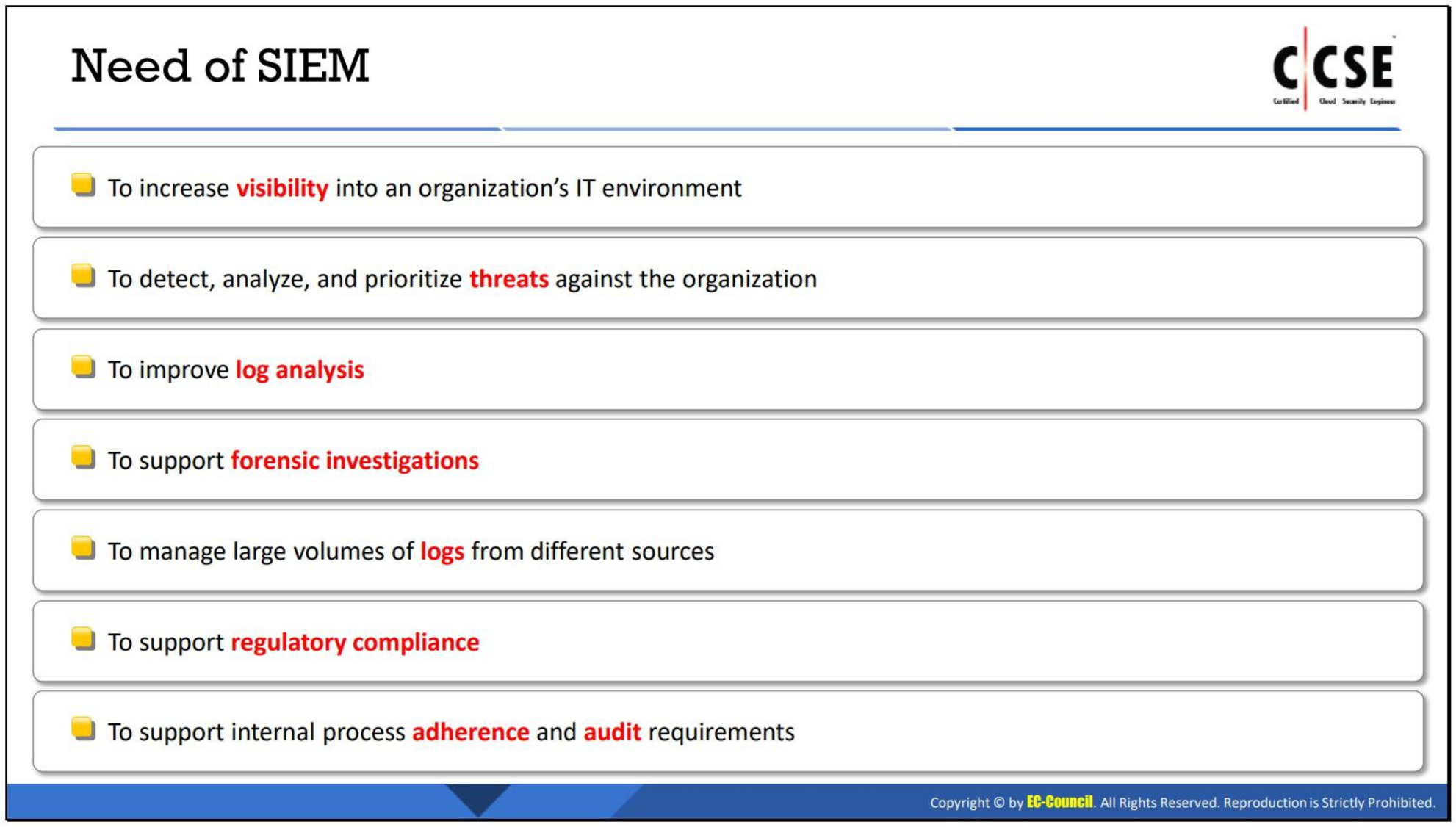


Security Analytics

Security analytics is a component of SIEM responsible for performing SEM, log analysis, and reporting. In SEM, real-time monitoring and incident management are performed. In log analysis, patterns are identified; the anomalies in correlated log data signify the activities of any intrusion attempt or policy violation. Automated or user-driven methods can be used for log analysis. In automated log analysis, log analysis is performed using systems and software without the involvement of human resources. In user-driven log analysis, the data collected from different devises are manually monitored and examined to determine suspicious events in a network. Manual log analysis is not preferred in real-time situations because it is a time-consuming process.

Figure 5.129: Security Analytics Components

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



Need of SIEM

The implementation of SIEM can help in numerous ways:

- **Increase visibility over the network**

  If the organization that implements SIEM is aware of the activities in its network, then the organization is said to have good visibility over its network. Accordingly, the organization can closely monitor user actions, the data accessed, number of login attempts, and other information such as the addition of new users, installation of new application, and network performance. If there is good visibility over a network, then all malicious behaviors and alert-causing incidents can be observed strictly. Thus, organizational network security can be enhanced.

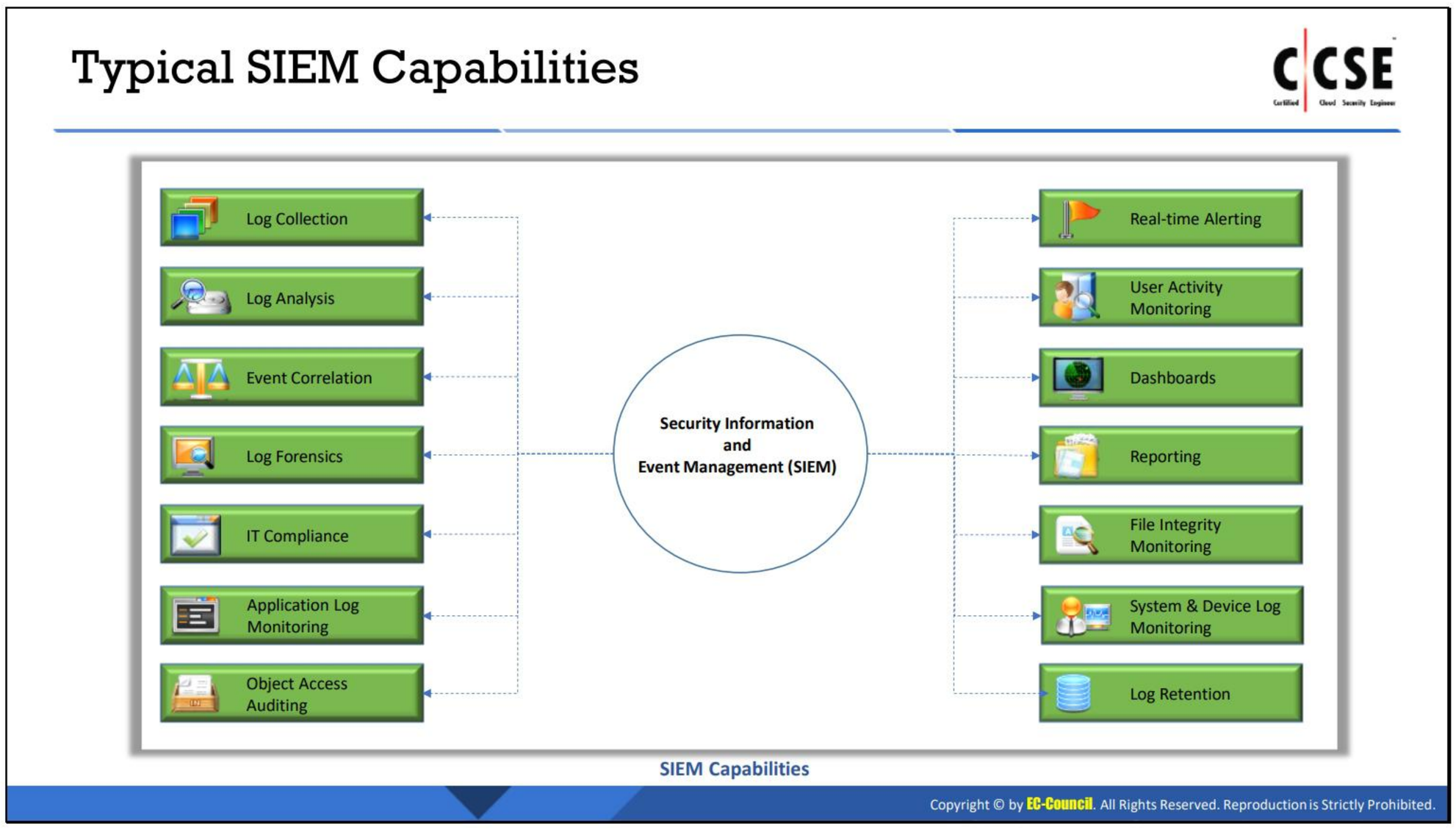
- **Incident management**

  If the number of devices and applications on a network is huge, then the log data produced by these event sources will be humongous. In such cases, a malicious incident cannot be found by collecting numerous events at a centralized location. SIEM performs different types of techniques to find alert-causing incidents. This will help the organization in increasing the efficiency of their network.

- **Forensics**

  SIEM can be used during forensic investigation to find the event that initiated the attack by analyzing previous records. Thus, when a similar incident occurs, SIEM alerts the intrusion detection systems and firewalls and makes them reconfigure the rules to stop the ongoing attack by taking necessary actions. These automatic defensive steps are used to prevent ongoing malicious attacks without human involvement. It can also be used to support regulatory compliance.

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



Typical SIEM Capabilities

The figure depicts the typical capabilities of SIEM.

hide01.ir

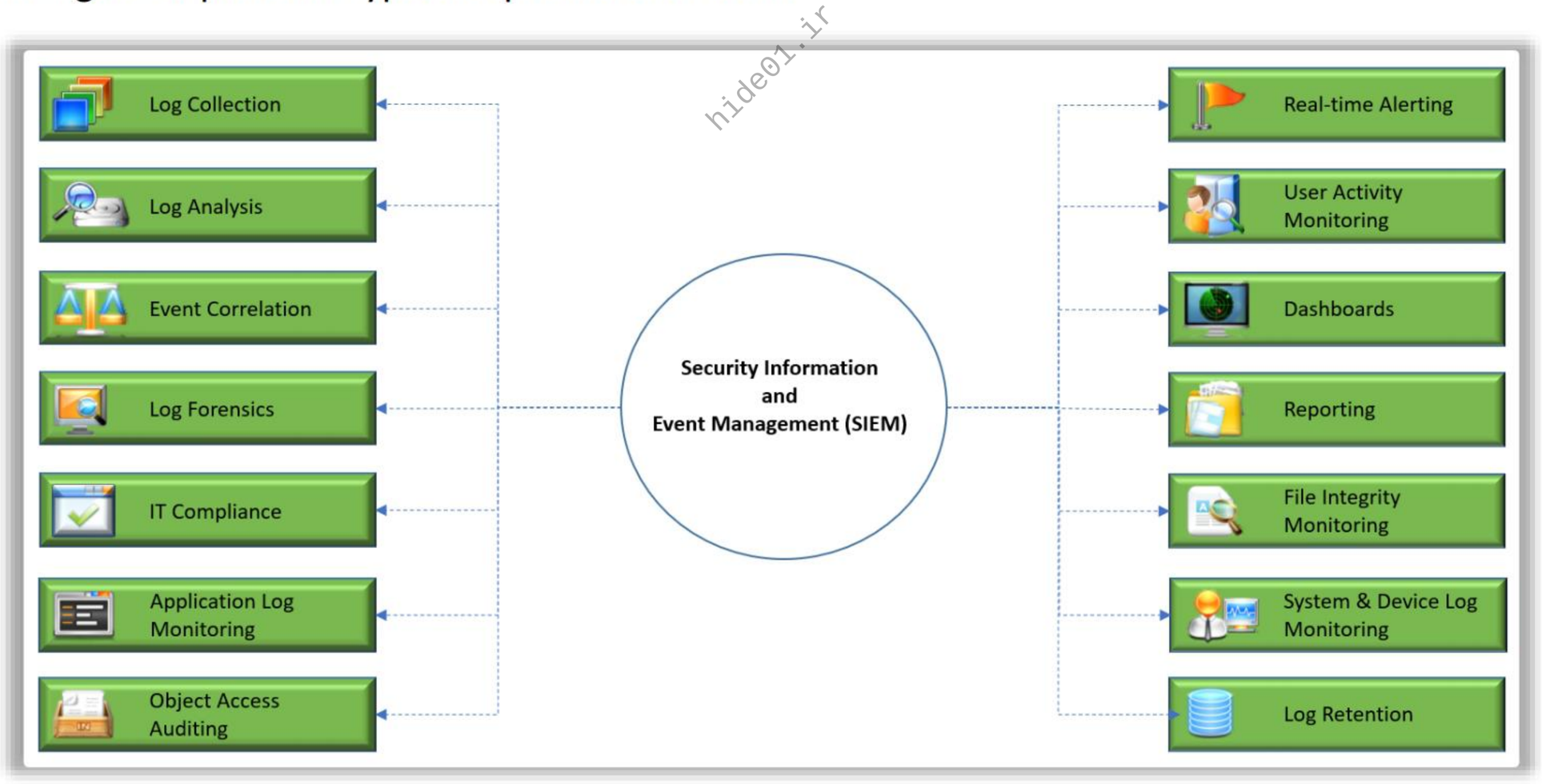


Figure 5.53: Typical capabilities of SIEM

- **Log collection**

  SIEM collects logs from heterogeneous sources such as Windows systems, Unix/Linux systems, applications, databases, routers, switches, and other devices. It uses both agent-based and agentless log collection methods.

- **Correlation**

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

It links events and related data into meaningful bundles that describe real security incidents, threats, vulnerabilities, or forensic findings. It is performed based on log search, rules, and alerts.

- **Real-time alerting**

  It analyzes events and sends alerts to SOC analysts to inform them about the immediate issues, either by messaging, email, or dashboards.

- **IT compliance**

  SIEM includes regulatory compliance reports such as PCI DSS, FISMA, GLBA, SOX, and HIPAA. It can also customize and create new compliance reports for future regulatory acts.

- **Threat hunting**

  It enables the security team to run queries on data and analyze and filter the data to identify threats or vulnerabilities.

- **Threat intelligence**

  SIEM can analyze data and identify threats in a network. It identifies threats and understands their possible relation to events.

- **Log forensics**

  It enables users to track event activities or an attacker through log search.

hide01.ir

- **Application log monitoring**

  It can monitor application logs, log files, event logs, service logs, and system logs on Windows, Linux, and Unix servers.

- **Object access auditing**

  SIEM notifies users about their files and folders (who accesses, deleted, edited, or moved them). It represents object access reports in human-readable formats and sends alerts if unauthorized users access any file/folder.

- **User activity monitoring**

  This feature of SIEM enables the tracking of suspicious behavior in users.

- **Dashboards**

  SOC analysts use dashboards to perform the right actions at the right time and make correct decisions during network anomalies.

- **Reporting**

  It notifies users about security-related incidents and events such as malware activities, successful and failed logins, and various other malicious activities.

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

- **File integrity monitoring**

  SIEM facilitates real-time file integrity monitoring (FIM) by securing sensitive files and folders and satisfying regulatory compliances.

- **Log data retention**

  This feature enables users to retain the historical log data and perform log forensics investigation and internal audits.

hide01.ir

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

Types of SIEM Solutions

In-House SIEM

- In-House SIEM: Customers **buy the software and hardware** and manage them on-premises

Advantages

- It provides full control over the system
- It can be customized based on organizational requirements

Disadvantages

- It is expensive to set up and operate

Cloud-Based SIEM

- In this type of SIEM, customers **subscribe to SIEM as a service**

Advantages

- The SIEM platform is updated constantly. There is no need to depend on a third party to maintain the implementation

Disadvantages

- Customers may fail to realize complete SIEM functionalities or benefits

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

Types of SIEM Solutions (Cont'd)

hide01.ir

Managed SIEM

- This type of SIEM can be implemented either **on-premises or on-cloud**
- It includes all technology features required for do-it-yourself implementation and satisfying security objectives

Advantages

- It removes the load of hiring, training, and keeping special personnel because it comes with advanced technology and skilled people
- It provides compliance support and data security assistance

Disadvantages

- Data security is managed by third party. If a wrong company has been selected, there is a chance of more risks or unwanted hassles

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

Types of SIEM Solutions

There are three different methods of implementing SIEM:

- **In-House SIEM**

  If SIEM is implemented in an organization or company without the involvement of external sources, it is known as in-house SIEM. In this type of SIEM, the organization buys and installs the required software and hardware and manages them at their physical

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

location by themselves. For this type of implementation, the organizational staff must have managerial skills or a team should be recruited and educated.

Advantages

- It provides full control over the system.
- It can update rules according to user preferences.
- SIEM can be customized according to the security requirements of organizations.

Disadvantages

- It is expensive to set up and operate.
- The process of training the staff and explaining the working of SIEM is time consuming.
- It is difficult to provide the necessary tools.

- **Cloud-based SIEM**

  In cloud-based SIEM, a third-party vendor supplies the required features of SIEM without any organizational involvement. In this type of SIEM, the organization subscribes to a plan for a particular period with specific features. To obtain more features, the company has to pay more money.

  Advantages

  - The SIEM platform is updated constantly.
  - Operational support is provided when needed.
  - This provides numerous features such as unlimited data storage.
  - No further installation of hardware equipment is required.

  Disadvantages

  - Customers may fail to realize complete SIEM functionalities.
  - To utilize all benefits of SIEM, customers have to pay a large amount of money, which can be expensive.

- **Managed SIEM**

  This type of SIEM can be implemented either on-premises or on-cloud. Managed SIEM is introduced with via a third party. SIEM includes all technology features that are required for do-it-yourself implementation and satisfy security objectives. In this type of SIEM, the features and possibilities can be managed. Managed SIEM can be equipped with necessary elements that help the organization in finishing a particular task. Because the features are expandable, managed SIEM is highly encouraged in real-world scenarios.

  Advantages

  - It removes the load of hiring, training, and keeping special personnel because it includes advanced technology and skilled people.

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

- It costs less in comparison to other types of SIEMs.
- It includes the implementation and maintenance cost, and no additional cost is required.
- This takes less space compared to the in-house mechanism.
- It provides continuous compliance support and data security assistance.

Disadvantages

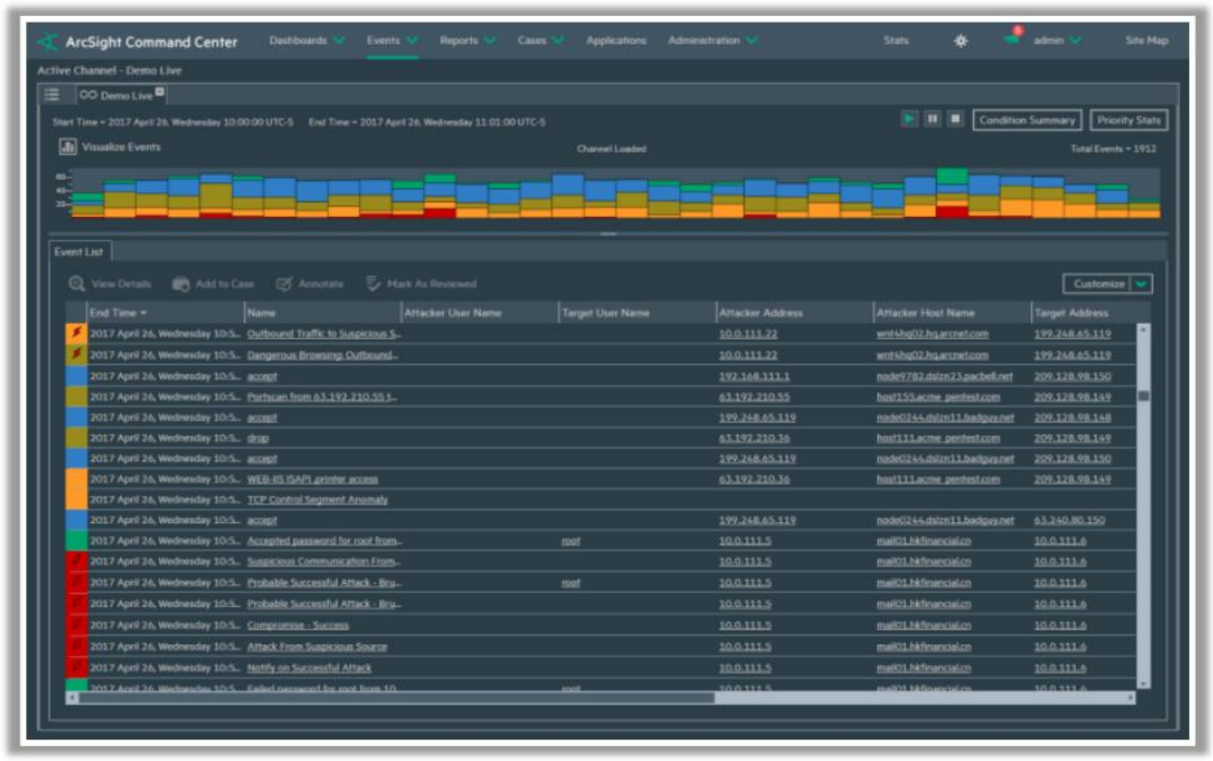
- Because a third party manages data security, if a wrong company has been selected, then there is increased chances of risks or unwanted hassles.
- As an SIEM system is introduced with raw data, the chances of getting false positives increases. Analyzing a false positive will consume the same amount of time as a real incident.

hide01.ir

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

SIEM Solutions: Micro Focus ArcSight Enterprise Security Manager

- It is a comprehensive **threat detection**, **analysis**, and **compliance management** SIEM solution
- Using ArcSight ESM, SOCs gain the agility to expand their cyber security footprint and respond faster to evolving threats at massive scale
- It empowers SOC monitoring teams to triage detected alerts through ArcSight ESM integration commands



ArcSight command center dashboard

Source: https://software.microfocus.com

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

SIEM Solutions: Micro Focus ArcSight Enterprise Security Manager

Source: https://www.microfocus.com

Micro Focus ArcSight Enterprise Security Manager (ESM) is a comprehensive threat detection, analysis, and compliance management SIEM solution. With ArcSight ESM, SOCs gain the agility to expand their cybersecurity footprint and respond faster to the evolving threats at a massive scale. It empowers SOC monitoring teams to triage detected alerts using ArcSight ESM integration commands.

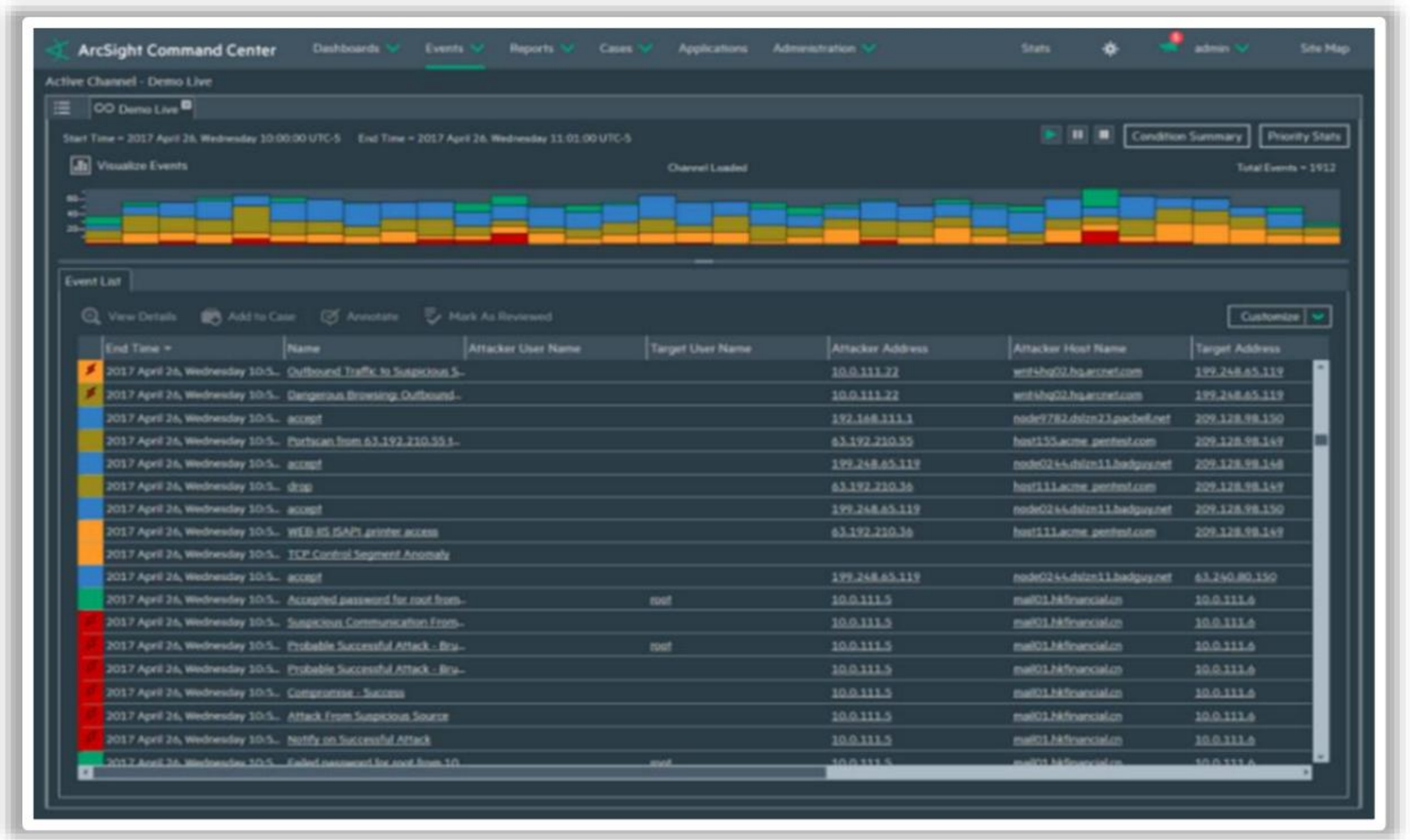


Figure 5.54: Screenshot of Micro-Focus ArcSight ESM

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

Key Features

The following are the key features of ArcSight ESM.

- **Real-time correlation**: ArcSight ESM correlates events and alerts to identify high priority threats within environments. The correlation engine of ESM allows for the collection of data and real-time correlation of events to accurately escalate threats that violate the internal rules within the platform. ESM can correlate up to 100,000 events per second within an enterprise.
- **Categorization and normalization**: Categorization and normalization convert collected original logs into a universal format for use inside an SIEM product.
- **Powerful and modular content development**: Once custom content (rules, trends, dashboards, and reports) has been created to address a security use case, it can be easily packaged up and deployed on other systems or shared with other business units or the ArcSight community. In tiered ESM architectures, multiple ESMs can be set to automatically sync content systems dynamically.
- **Integration with ArcSight Data Platform event broker**: Addressing the challenges imposed by big data for massive scale, openness, and speed, ArcSight ESM fully integrates with ArcSight Data Platform (ADP) event broker. It is an open, massively scalable intelligent data ingestion and delivery bus for modern SOCs. ESM can send and receive events from the EB open architecture of ADP, which enables data sharing to third-party applications such as Hadoop, data lakes, or even proprietary in-house applications.
- **Integration with ArcSight Investigate**: ArcSight ESM integrates with ArcSight Investigate to create extremely fast and intuitive search and data visualization within the security operation environment. ArcSight Investigate is a companion next-generation hunt and investigation solution built on a new advanced analytics platform to serve the evolving needs of security teams.
- **Workflow automation:** ArcSight ESM creates an easy way for SOC teams to efficiently and effectively triage the detected alerts through real-time triaging channels and its built-in case management system.
- **Automated response within the console or as rule actions**: Action connectors (CounterAct) allow integrations between ArcSight and third-party devices; this enables third-party devices to be controlled from the ArcSight Console. You can execute commands on third-party devices from within ArcSight and send the output of these commands back to the console for analysts to examine.
- **Multi-tenancy**: With multi-tenancy capabilities and access-control permissions configurable down to the event level, enterprises can use a centralized set of management abilities, including rule-based thresholds and unified permissions role, rights, and responsibilities matrix.

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

SIEM Solutions: Splunk Enterprise Security

Source: https://www.splunk.com

Splunk Enterprise Security (ES) is an analytics driven SIEM solution that provides users with what they need to detect and responds to internal and external attacks quickly.

- It automates the collection, indexing, and alerting of real-time machine data that are critical to organizational operations.
- It discovers actionable insights from all data (structured or unstructured).
- It leverages AI powered by machine learning for actionable insights.

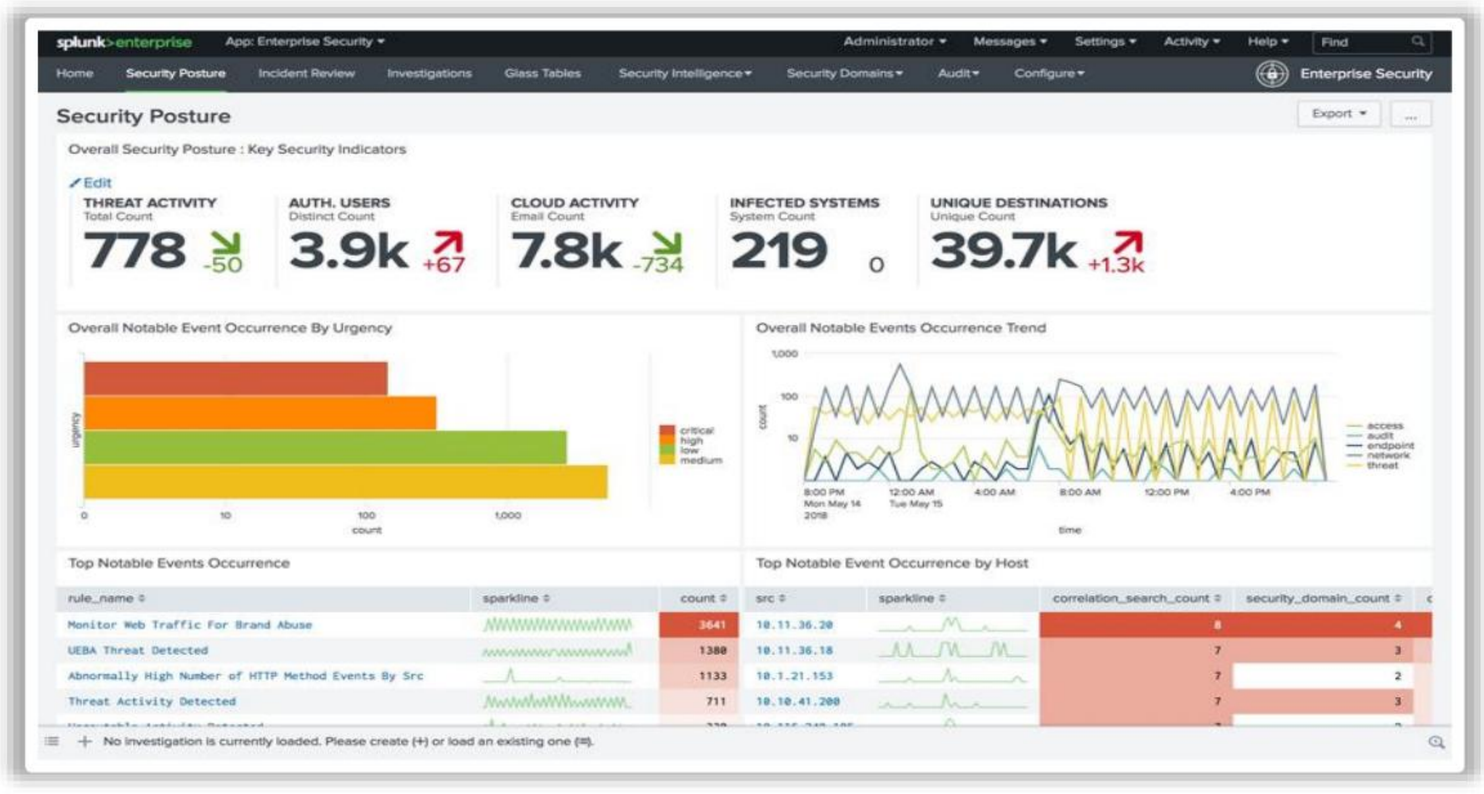


Figure 5.55: Screenshot of Splunk ES

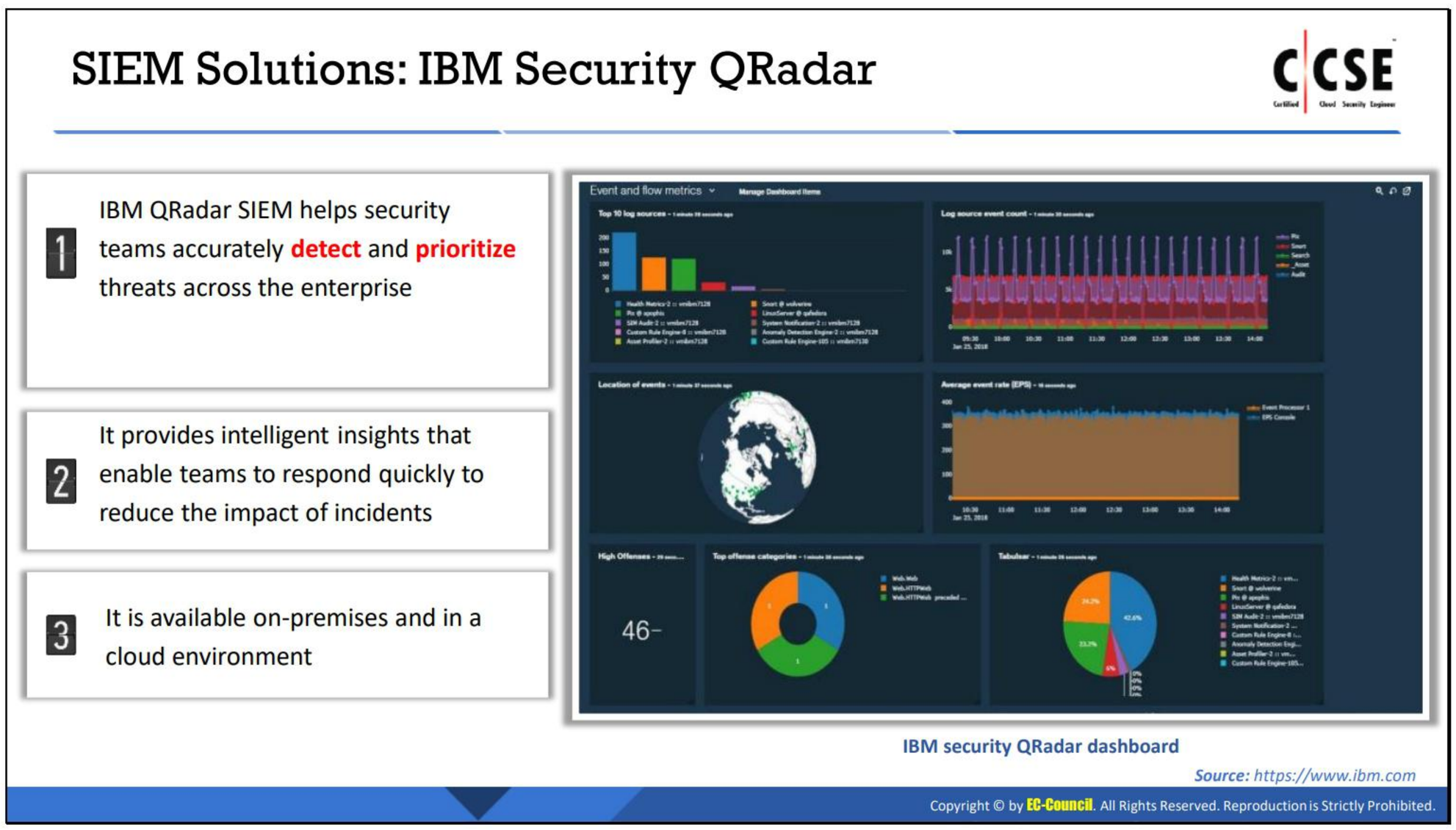
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Splunk ES provides organizations the ability to

- Improve security operations with faster response time
- Improve security posture by getting end-to-end visibility across all machine data
- Increase detection and investigation capabilities using advanced analytics
- Make better informed decisions by leveraging threat intelligence

hide01.ir

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



IBM security QRadar dashboard

Source: https://www.ibm.com

SIEM Solutions: IBM Security QRadar

Source: https://www.ibm.com

IBM QRadar SIEM helps security teams accurately detect and prioritize threats across the enterprise. It provides intelligent insights that enable teams to respond quickly to reduce the impact of incidents. It is available on-premises and in cloud environments.

Key Features

The following are the benefits of QRadar:

Comprehensive visibility: It gains centralized insight into logs, flow, and events across on-premises, SaaS, and IaaS environments.

Eliminate manual tasks: It centrally analyzes all events related to a particular threat in one location to eliminate manual tracking processes and enable analysts to focus on investigation and response.

Real-time threat detection: It leverages out-of-the-box analytics that automatically analyzes logs and network flows to detect threats and generate prioritized alerts as attacks progress through the kill chain.

Easily manage compliance: It complies with internal organizational policies and external regulations by leveraging prebuilt reports and templates.

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

Figure 5.56: Screenshot of IBM security QRadar

hide01.ir

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

SIEM Solutions: AlienVault Unified Security Management

Source: https://www.alienvault.com

AlienVault unified security management (USM) delivers threat detection, incident response, and compliance management across cloud, on-premises, and hybrid environments.

Features

- Vulnerability assessment and remediation
- Manages detection and response
- Threat and malware detection
- Log management, monitoring, and archiving
- Manages SIEM or SIEM-as-a-service
- Continuous compliance management
- Cloud security monitoring

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

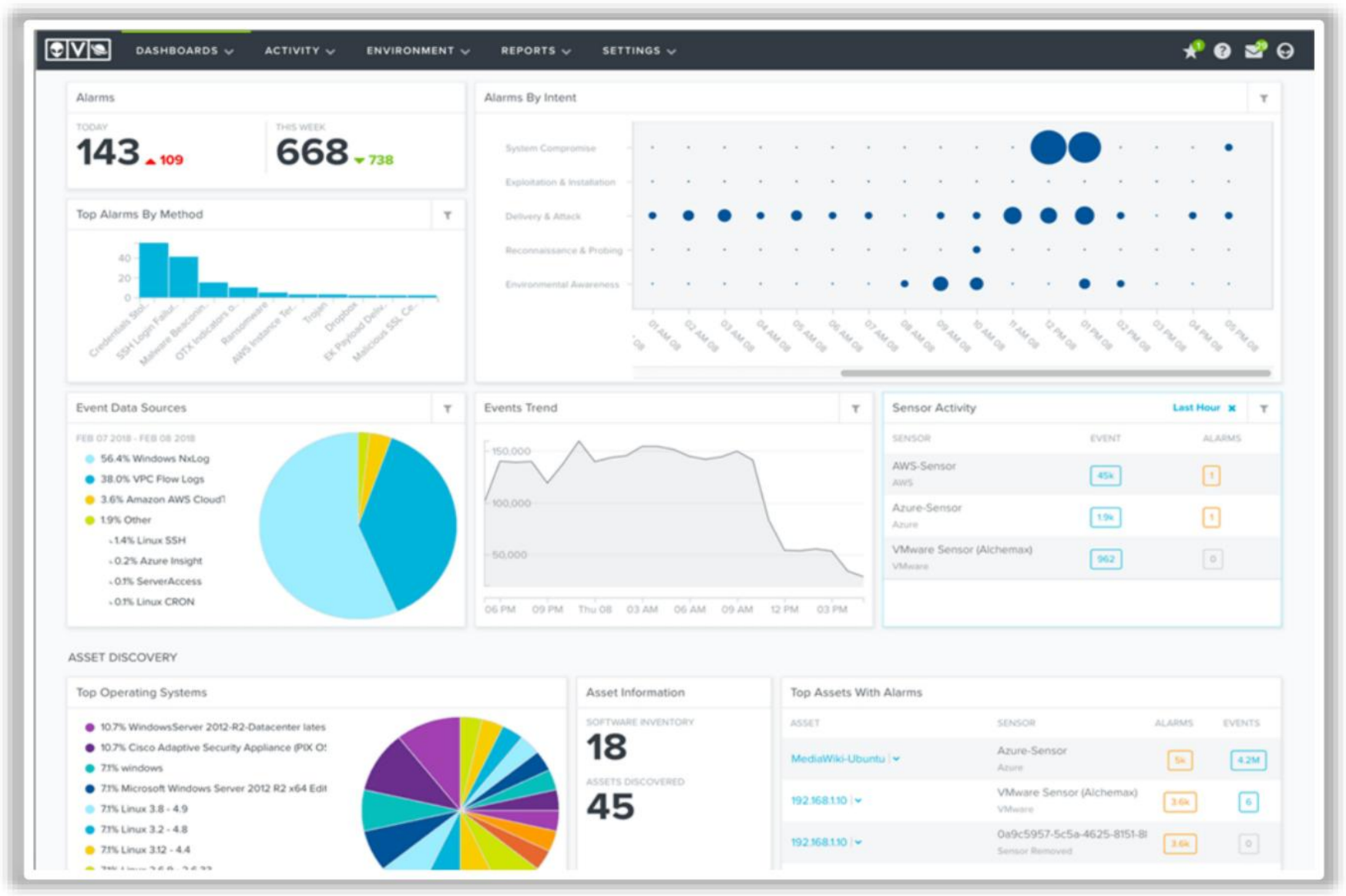


Figure 5.57: AlienVault unified security management (USM)

Essential Security Capabilities of Alien Vault USM

The AlienVault USM appliance provides the following five essential security capabilities in a single console:

- **Asset discovery**: It utilizes active network scanning, passive network monitoring, asset inventory, and service inventory to determine who and what is connected to on-premises environments continuously.
- **Vulnerability assessment**: It can perform authenticated/unauthenticated vulnerability scans and continuous vulnerability monitoring to determine the location of vulnerabilities on assets to avoid easy exploitation and compromise.
- **Intrusion detection**: It utilizes network IDS, host IDS, and FIM to determine the occurrence of suspicious activities.
- **Behavioral monitoring**: It uses NetFlow analysis, service availability monitoring, and full packet inspection to identify suspicious behavior and potentially compromised systems.

SIEM: It performs log management, event correlation, incident response, reporting, and alarming to correlate and analyze security event data from across a network and respond.

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

Additional SIEM Solutions

Following are some additional SIEM solutions:

- **Elastic Stack**

  Source: https://www.elastic.co

  hide01.ir

  Elastic Stack is a group of open-source products that lets users reliably and securely take data from any source in any format, and search, analyze, and visualize them in real-time. The products in Elastic Stack are designed to be used together and releases are synchronized to simplify the installation and upgrade process.

  A full stack consists of

  - **Beats**: Beats is a platform for lightweight shippers that send data from edge machines to Logstash and Elasticsearch.
  - **Elasticsearch**: Elasticsearch is a distributed, JSON-based search and analytics engine designed for horizontal scalability, maximum reliability, and easy management.
  - **Kibana**: Kibana gives shape to user data; it is an extensible user interface for configuring and managing all aspects of Elastic Stack.
  - **Logstash**: Logstash is a dynamic data collection pipeline with an extensible plugin ecosystem and strong Elasticsearch synergy.

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

- **LogRhythm SIEM**

  Source: https://logrhythm.com

  LogRhythm SIEM is a unified, scalable solution designed to help organizations to achieve monitoring and analytics capabilities. Its end-to-end solution identifies threats and quickly mitigates and recovers from security incidents. It is a detection and response framework for SOCs.

- **McAfee ESM**

  Source: https://www.mcafee.com

  McAfee ESM is an SIEM solution that delivers actionable intelligence and integrations to prioritize, investigate, and respond to threats. It provides continuous visibility into threats and risk, actionable analysis to guide triage and speed investigations, and orchestration of security remediation. It prioritizes alert surface potential threats before they occur while analyzing data for patterns that may indicate a larger threat.

- **Micro-Focus Sentinel Enterprise**

  Source: https://www.netiq.com

  Sentinel® is a full-featured SIEM solution that simplifies the deployment, management, and day-to-day use of SIEM; readily adapts to dynamic enterprise environments; and delivers true "actionable intelligence" to security professionals who need to understand their threat posture and prioritize responses quickly.

- **SolarWinds Log and Event Manager**

  Source: https://www.solarwinds.com

  SolarWinds Log and Event Manager is a full-featured SIEM tool to help simplify IT security with advanced event log analysis, threat detection, and response. It identifies threats faster with event-time detection of suspicious activities. It conducts security event investigations and forensics for mitigation and compliance. It demonstrates compliance with audit-proven reporting for HIPAA, PCI DSS, SOX, and DISA STIG. It maintains continuous security with encryption capabilities.

- **Trustwave SIEM Enterprise and Log Management Enterprise**

  Source: https://www.trustwave.com

  Trustwave Log Management Enterprise helps to simplify the collection and processing of logs and understanding data. It is an appliance-based solution that can be easily deployed, operated, and managed. It includes support for hundreds of auditing devices from a myriad of vendors and offers a primarily agent-less approach, which simplifies the ongoing operational maintenance requirements and reduces the total cost of ownership.

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

- **RSA NetWitness Suite**

  Source: https://www.rsa.com

  The RSA NetWitness Suite provides pervasive visibility across a modern IT infrastructure, enabling better and faster detection, investigation, and response to security incidents. RSA NetWitness Suite takes security "beyond SIEM," extending the traditional log-centric, compliance-focused approach to security to include state-of-the-art threat analytics and visibility into cloud, network, and endpoints.

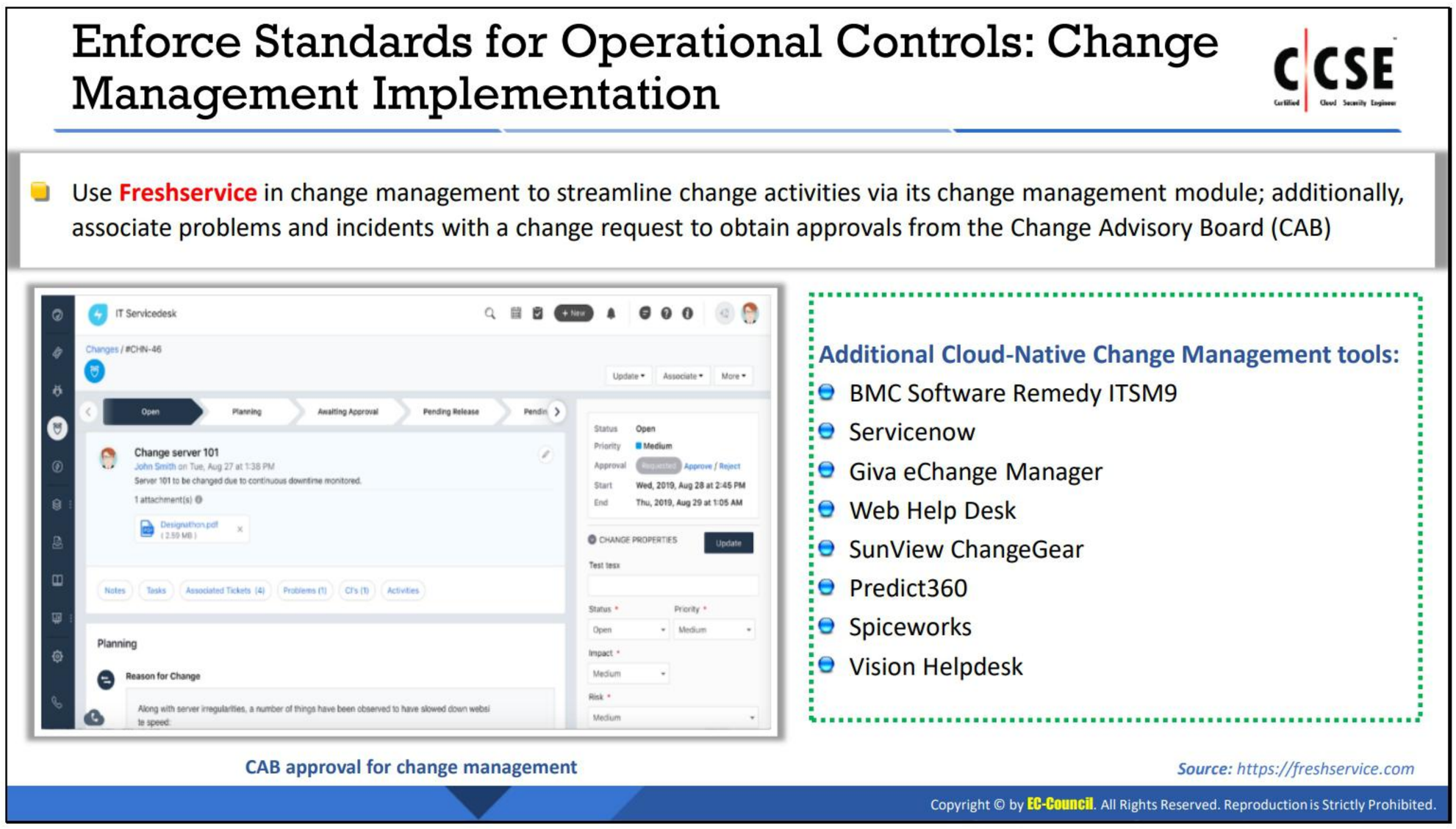
- **LogPoint**

  Source: https://www.logpoint.com

  An SIEM solution is central in a risk management toolkit. A great SIEM tool allows businesses to improve threat detection and response by providing real-time data analysis, early detection of data breaches, data collection, data storage, and accurate data reporting.

hide01.ir

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



Enforce Standards for Operational Controls: Change Management Implementation

Freshservice

Source: https://freshservice.com

hide01.ir

Freshservice helps in change management by allowing to streamline change activities via its change management module, associate problems and incidents with a change request, and obtaining Change Advisory Board (CAB) approvals.

Key features

- Visually tracks changes through their lifecycle. Ensures fulfillment of mandatory checks and requirements before progressing to the next stage.
- Automates change approvals and notifications to agents and end-users alike about any event related to a change.
- Views tasks and changes scheduled for the day that are automatically added to the calendar of an agent, with the ability to view the schedules of other agents for easy planning. Sets up hierarchical approvals, notifies the CAB, and approves or rejects changes based on their recommendations and comments from the portal.
- Monitors changes upon implementation, adds notes to review the change rollout process, and continuously improves the procedure.

Additional Cloud-Native Change Management tools

Following are the most common third-party tools used for change management in cloud environments:

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

- BMC Software Remedy ITSM9
- ServiceNow
- Giva eChange Manager
- Web Help Desk
- SunView ChangeGear

hide01.ir

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

Enforce Standards for Operational Controls: Incident Management Implementation

Source: https://www.sunviewsoftware.com

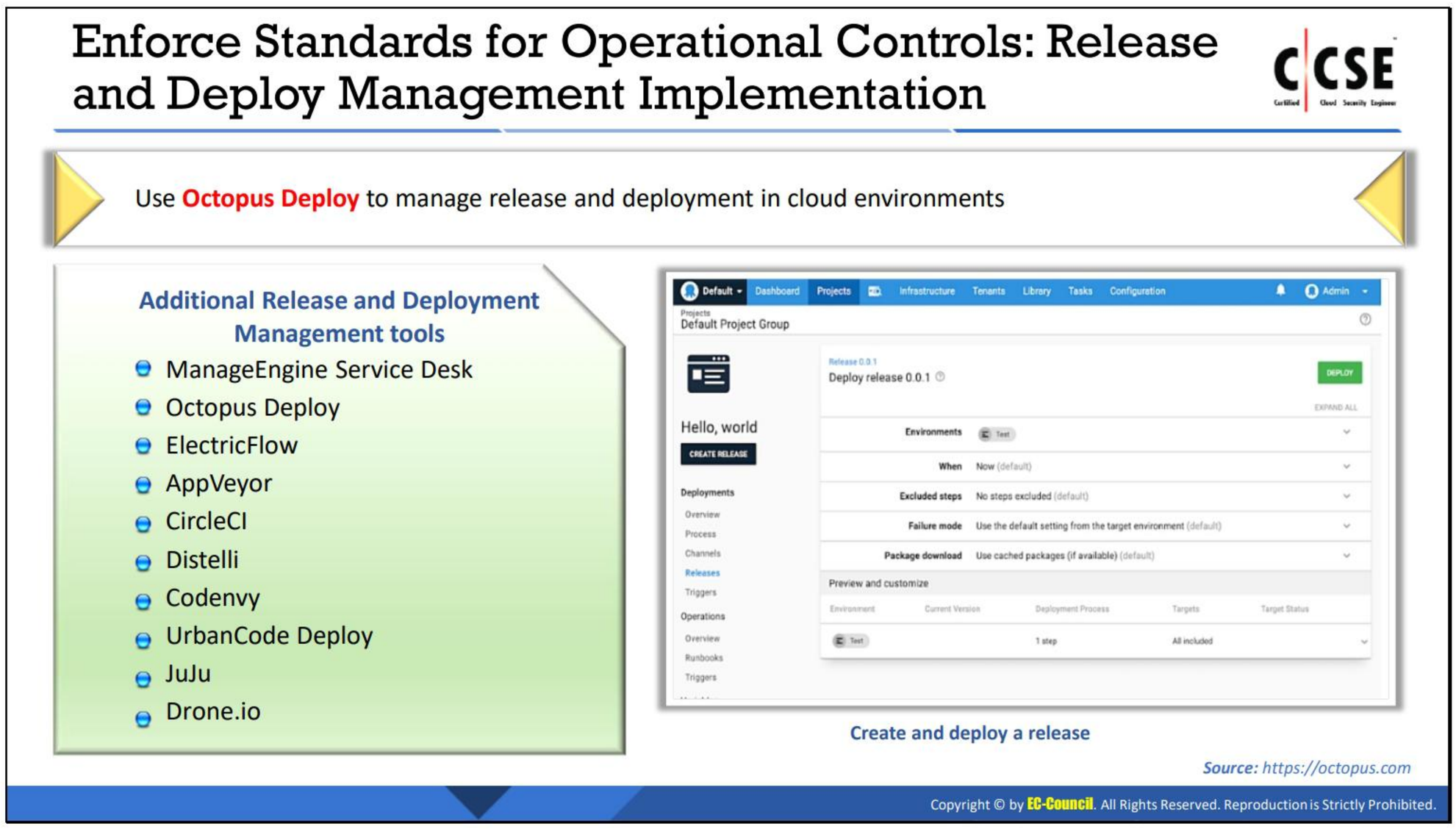
SunView ChangeGear provides change management, incident management, problem management, release management, and configuration management functions on the cloud. It helps to manage incidents effectively on the cloud by allowing cloud admins to create, edit, and delete lookup lists. Cloud admins can use these incident management lookup lists to manage incidents. This list contains some important criteria such as summaries, categories, change types, and close types.

hide01.ir

Additional incident management tools

- Freshservice
- Predict360
- SolarWinds Service Desk
- LogicGate Risk Cloud
- IBM Cloud Event Manager
- SunView ChangeGear
- IssueTrak
- C2 Atom
- New Relic One
- Onspring

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



Enforce Standards for Operational Controls: Release and Deploy Management Implementation

Source: https://www.octopus.com

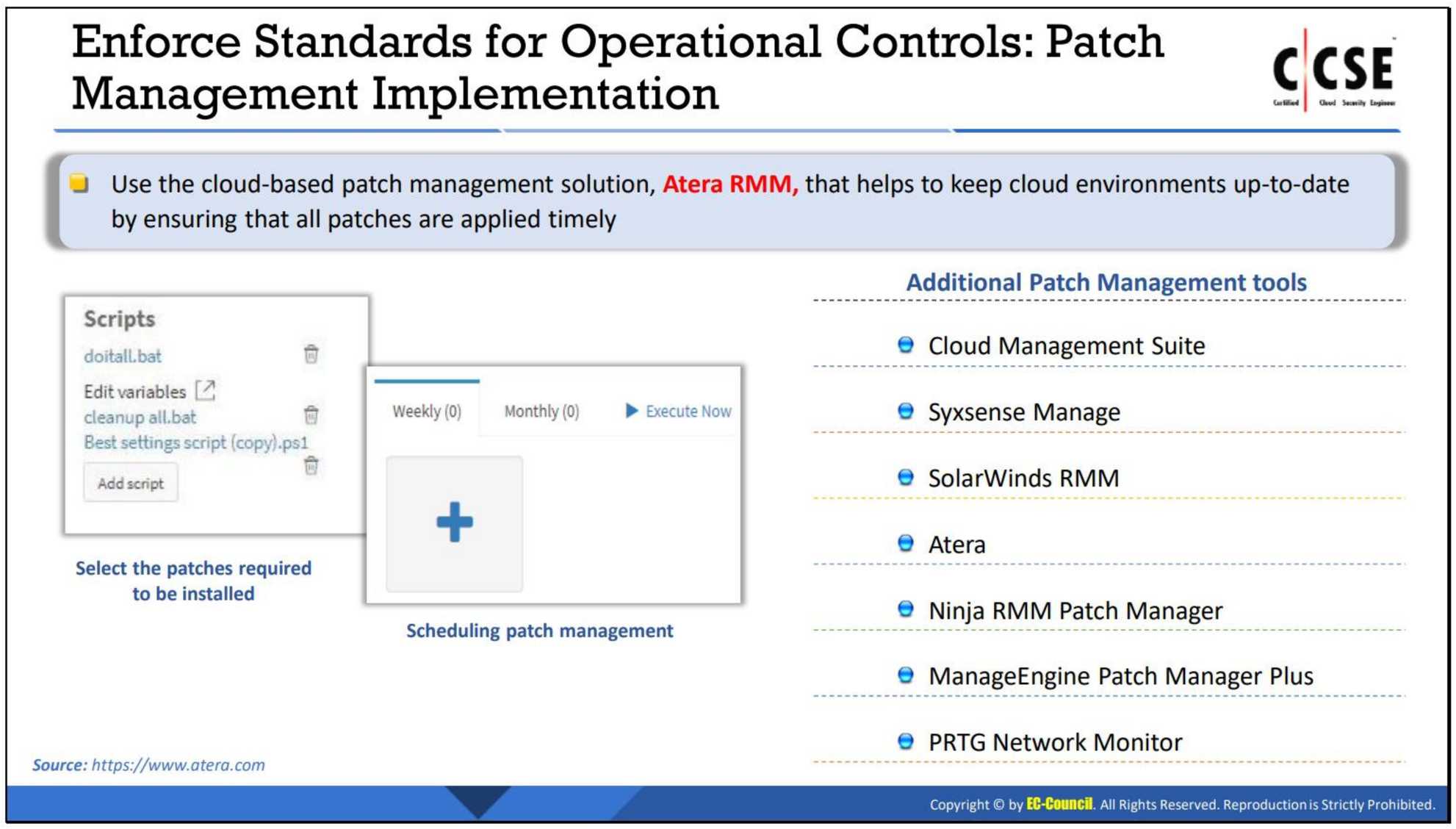
hade01.ir

Octopus Deploy helps to manage release and deployment in cloud environments. It provides release management, deployment, and runbook automation with multi-tenancy support, thus enabling the management of deployments to a single customer or group without duplication.

Additional release and management tools

- ManageEngine Service Desk
- Octopus Deploy
- ElectricFlow
- AppVeyor
- CircleCI
- Distelli
- Codenvy
- UrbanCode Deploy
- JuJu
- Drone.io

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



Enforce Standards for Operational Controls: Patch Management Implementation

Source: https://www.atera.com

hide01.ir

Atera is a cloud-based patch management and RMM (Remote Monitoring and Managaement) solution that helps to keep cloud environments up to date by ensuring that all patches are applied timely.

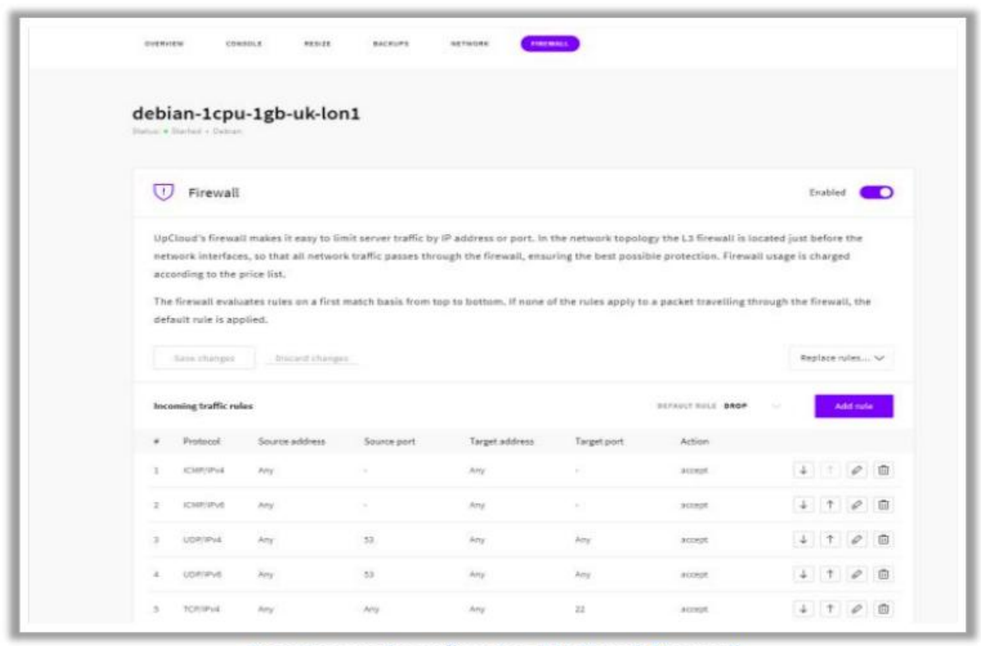
Additional Patch Management tools

- Cloud Management Suite
- Syxsense Manage
- SolarWinds RMM
- Atera
- Ninja RMM Patch Manager
- ManageEngine Patch Manager Plus
- PRTG Network Monitor

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

Monitor Security Controls Example: Configure UpCloud Firewall

- **UpCloud Firewall** is placed between the cloud server and internet to protect all connections in the cloud environment



Creating and configuring UpCloud Firewall

Source: https://upcloud.com

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

Monitor Security Controls Example: Configure UpCloud Firewall

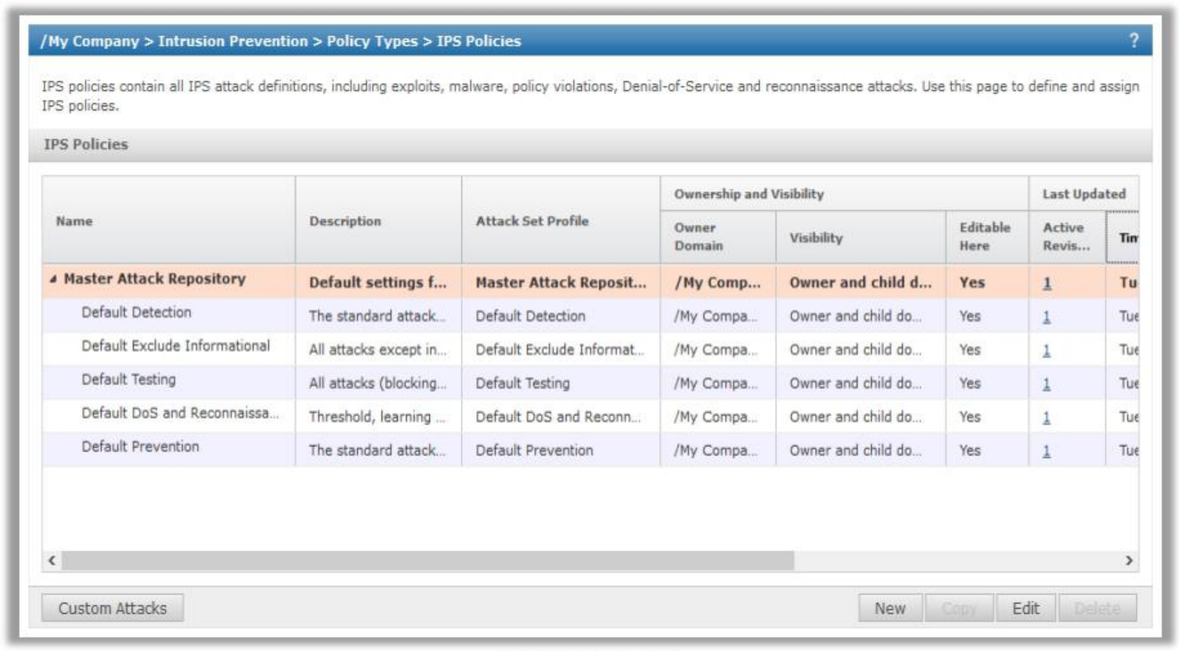
UpCloud Firewall is placed between the cloud server and internet to protect all connections in a cloud environment. It is a stateless firewall that does not store a record of connections.

hide01.ir

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

Monitor Security Controls Example: Add IPS Policy in McAfee Network Security Platform

- **McAfee Network Security Platform** can stop new and unknown attacks with signature-based and signature-less intrusion prevention systems



IPS Policies page

Source: https://www.mcafee.com/

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

Monitor Security Controls Example: Add IPS Policy in McAfee Network Security Platform

McAfee Network Security Platform can stop new and unknown attacks with signature-based and signature-less intrusion prevention systems. Signature-less intrusion detection finds malicious network traffic and stops attacks with no signatures. It supports VMware NSX and OpenStack. Integration with VMware NSX allows administrators to scale security with virtual workloads in private clouds as they are created and moved.

Source: https://www.mcafee.com

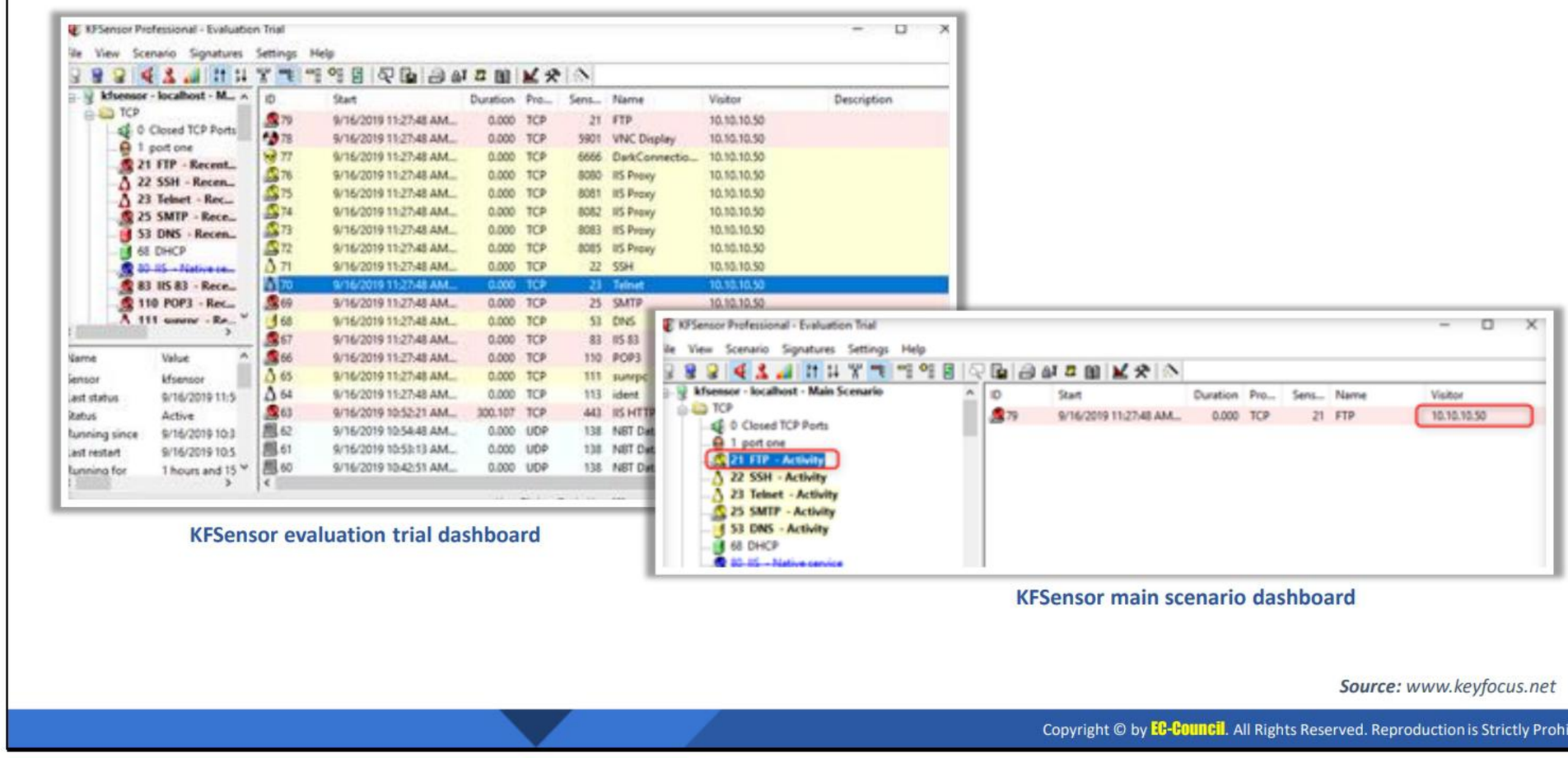
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Monitor Security Controls Example: Use Nessus Assessment for Vulnerability Assessment

Nessus Vulnerability Assessment tool can be used to identify vulnerabilities in a cloud network and issue alerts for the security team. It reduces the attack surface area and performs high-speed asset discovery and configuration auditing.

Source: https://www.tenable.com

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



Monitor Security Control Example: Implement Honeypot - KFSensor

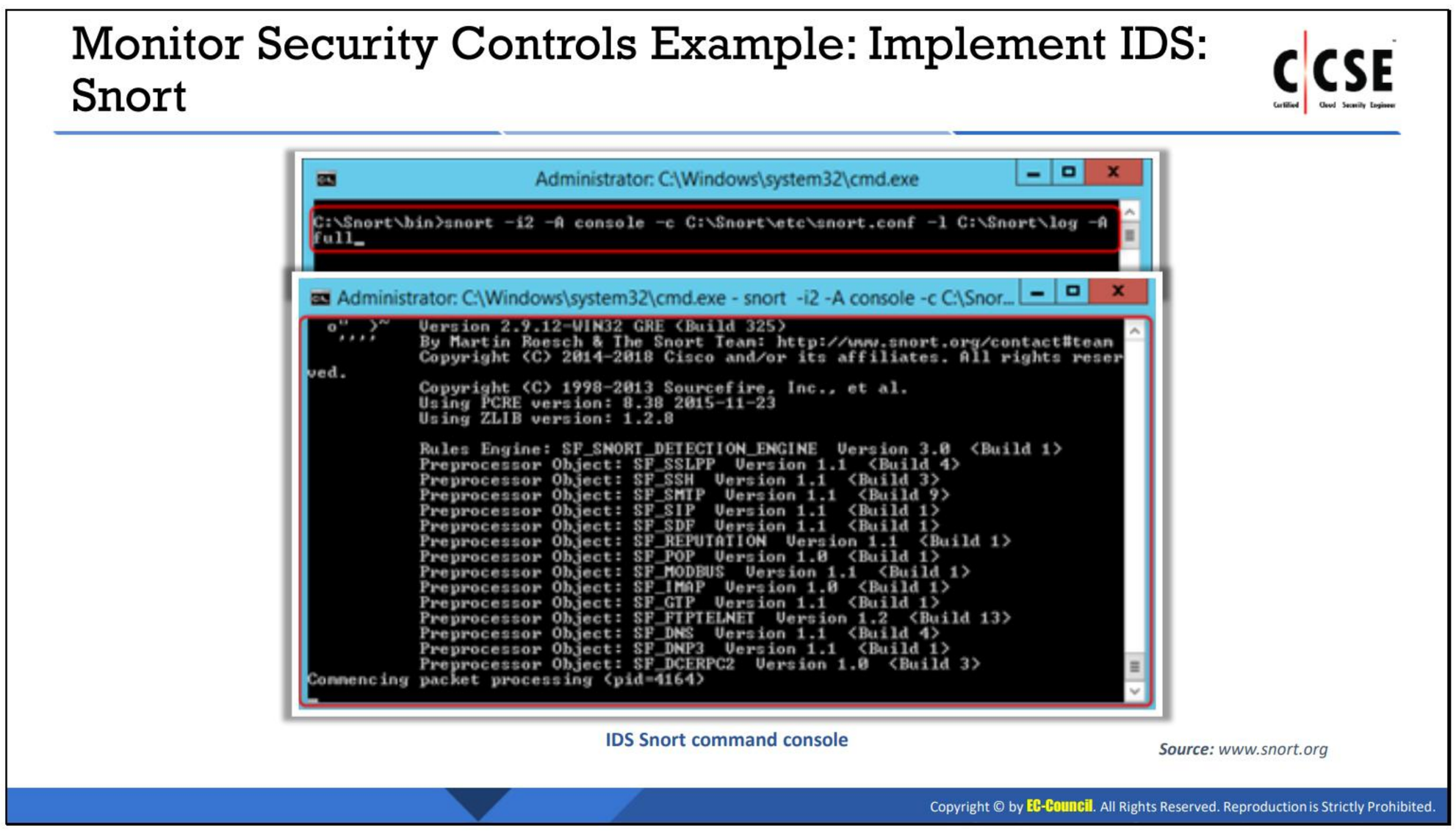
KFSensor

Source: https://www.keyfocus.net

ride01.ir

KFSensor acts as a honeypot designed to attract and detect hackers and worms by simulating vulnerable system services and trojans.

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



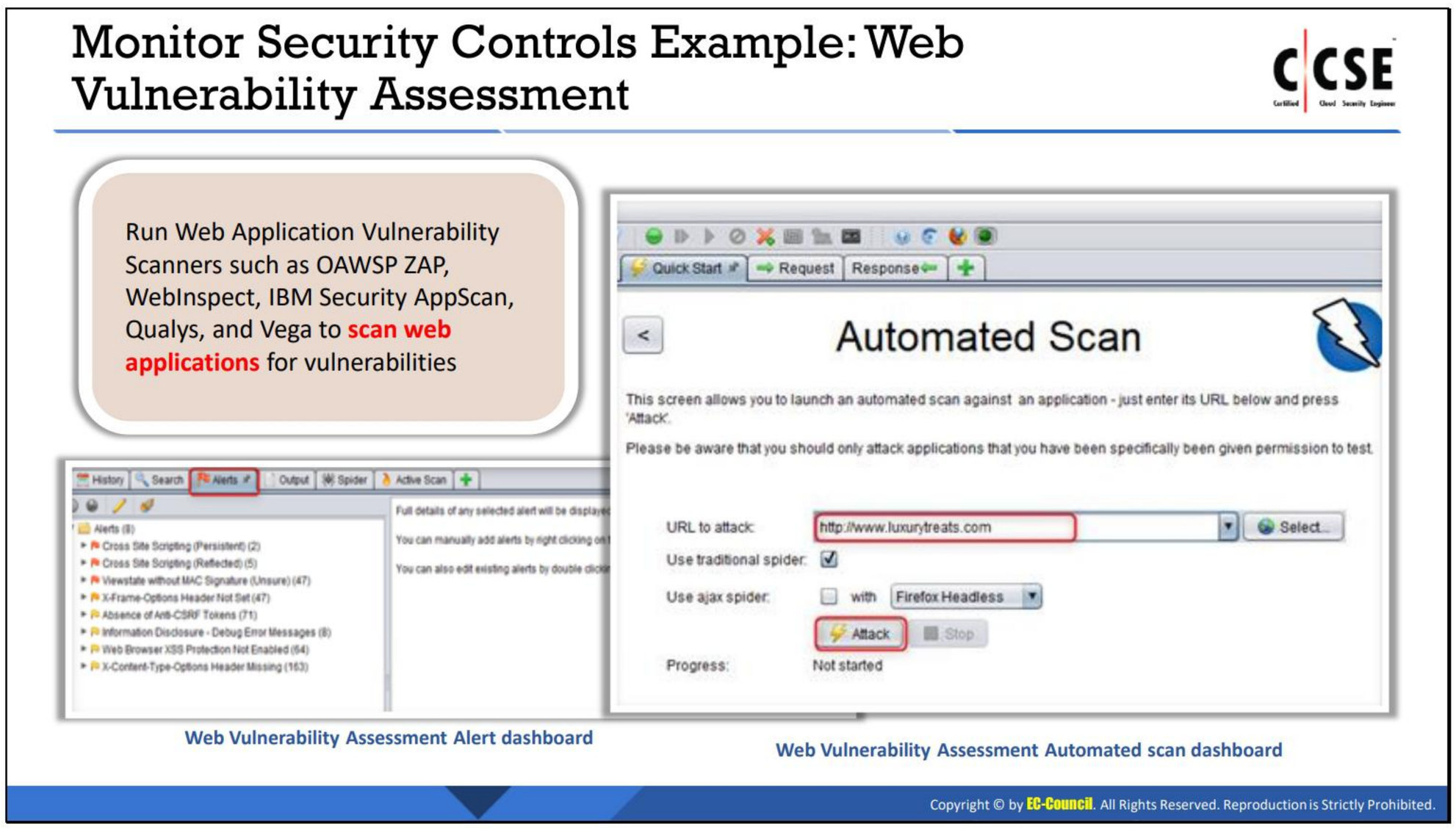
IDS Snort command console

Monitor Security Control Example: Implement IDS: Snort

Source: https://www.snort.org

Snort is an open-source network intrusion detection system (NIDS) software for Linux and Windows to detect the emerging threats. It is capable of real-time traffic analysis and packet logging on IP networks, protocol analysis, content searching, and matchings against a rule set defined by the user. The program performs an action based on the identified element. It uses a rule-based language that combines signature, protocol, and anomaly inspection methods to find malicious activity. It can be used to find attacks such as DoS attacks, OS fingerprinting attempts, buffer overflows, semantic URL attacks, stealth port scans, server message block probes, CGI attacks, and SMB probes.

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



Monitor Security Control Example: Web Vulnerability Assessment

Web vulnerability assessment involves crawling a website to discover potential vulnerabilities and reporting these results. Various open source and commercial vulnerability scanning tools are available to perform vulnerability assessment. The main aim of web vulnerability assessment is to make a website free from vulnerabilities. Look for the following vulnerability assessment functions while selecting a web application vulnerability scanner:

- User friendly interface
- Assessment process should be automated
- Should easily assign priorities and grouping
- Accurate Reports

Web Application Vulnerability Scanners

OWASP ZAP

Source: https://www.owasp.org

OWASP ZAP is an open source, easy to use, integrated tool for finding vulnerabilities in web applications.

WebInspect

Source: https://www.microfocus.com

HPE WebInspect is a web application security assessment solution designed to thoroughly analyze the latest complex web applications and web services for security vulnerabilities.

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

It provides the broadest dynamic application security testing coverage and detects new types of vulnerabilities that often remain undetected by black-box security testing technologies.

IBM Security AppScan

Source: https://www.ibm.com

IBM Security AppScan® Standard is a security vulnerability testing tool for web applications and web services. It features the most advanced testing methods to help protect websites from the threat of cyberattacks with a complete range of application data output options.

Qualys Web Application Scanner (WAS)

Source: https://www.qualys.com

Qualys is a robust cloud solution for continuous web app discovery and detection of vulnerabilities and misconfigurations.

Vega

Source: https://subgraph.com

Vega vulnerability scanner is an open-source web security tool to test the security of web applications. Vega can help you find and validate SQL Injections, Cross-Site Scripting (XSS), inadvertently disclosed sensitive information, and other vulnerabilities.

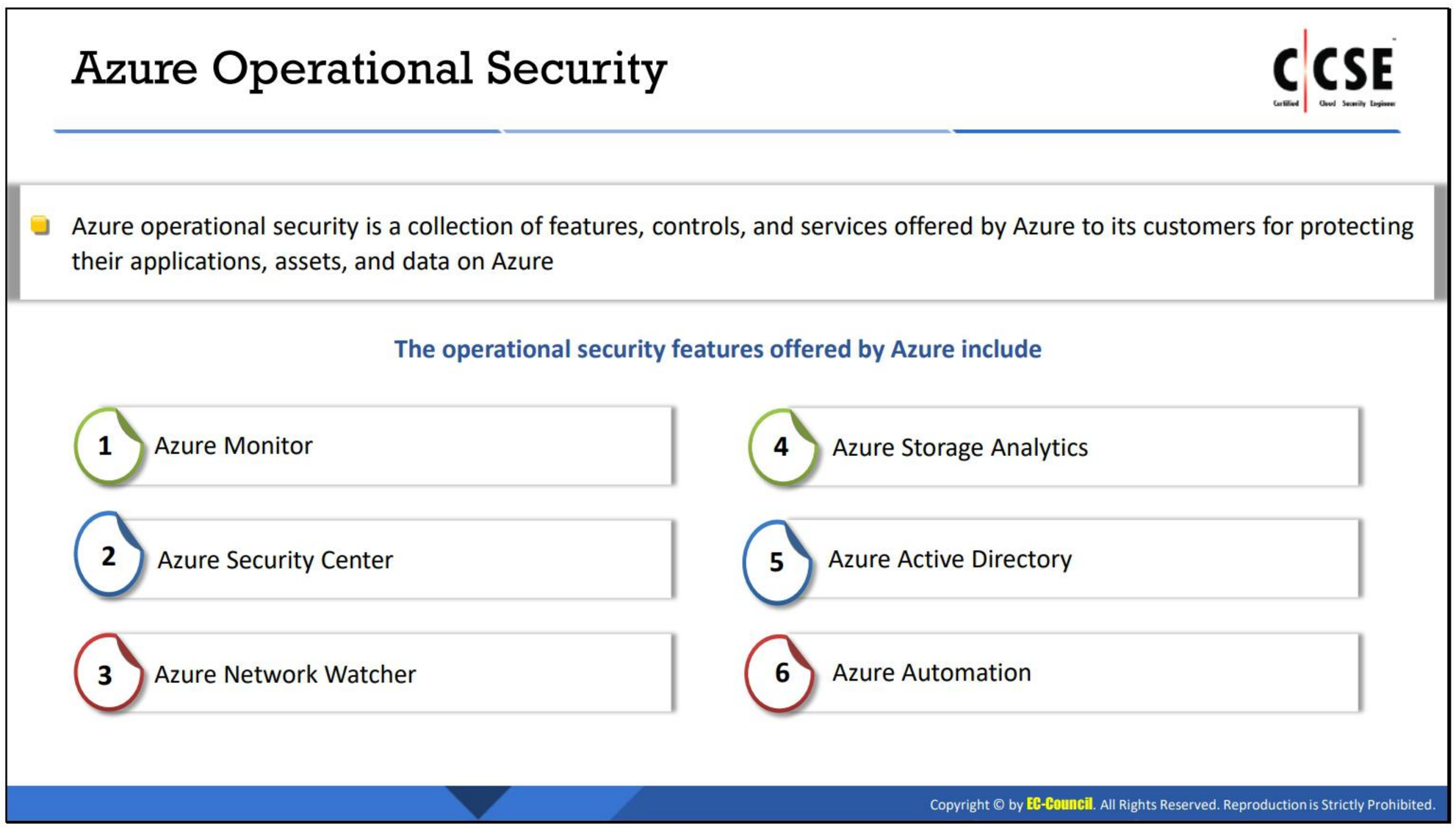
hide01.ir

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

LO#8: Understanding Security Operations in Microsoft Azure

The objective of this section is to understand the various features and services provided by Microsoft Azure for operational security. This section describes Azure services such as Azure Monitor, Azure Security Center, Azure Network Watcher, Azure Storage Analytics, Azure Active Directory, and Azure Automation. In this section, cloud security engineers will learn the various features and services offered by Microsoft Azure and use them effectively and efficiently to secure the Microsoft Azure environment of organizations.

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



Azure Operational Security

Azure operational security is a collection of features, controls, and services offered by Azure to its customers for protecting their applications, assets, and data on Azure. Azure operational security ensures that all cloud operations are secure and satisfy the customer requirements.

Azure operational security depends on the framework that contains Microsoft capabilities such as the Microsoft Security Response Center (MSRC) program, Microsoft Software Development Lifecycle (SDL), and in-depth awareness of the cybersecurity threat landscape.

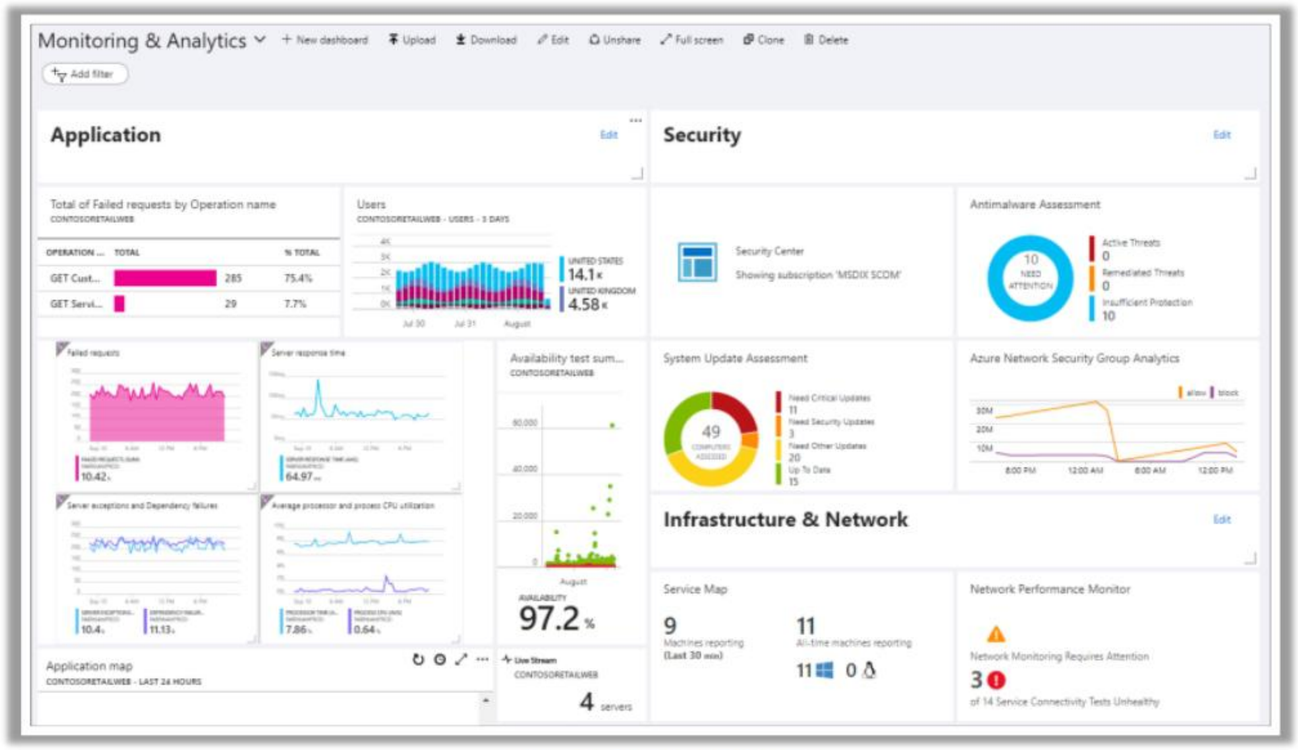
The operational security features offered by Azure include

- Azure Monitor
- Azure Security Center
- Azure Network Watcher
- Azure Storage Analytics
- Azure Active Directory
- Azure Automation

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

Azure Monitor

- **Azure Monitor** can be used to collect, analyze, and act on security telemetry received from cloud environments
- It can be used to understand the performance of applications and proactively detect issues that affect apps and resources on which they depend to ensure effective and safe cloud operations



Azure Monitor Dashboard

Source: https://azure.microsoft.com

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

Azure Monitor

Azure Monitor is a comprehensive service that can be used to collect, analyze, and act on security telemetry received from on-premises and cloud environments. It helps in maximizing the performance and availability of applications and services by collecting and analyzing performance metrics, activities, and diagnostics logs from the cloud environment. It enables cloud admins to understand the performance of applications and proactively detect issues that affect this application and the resources on which they depend to ensure effective and safe cloud operations.

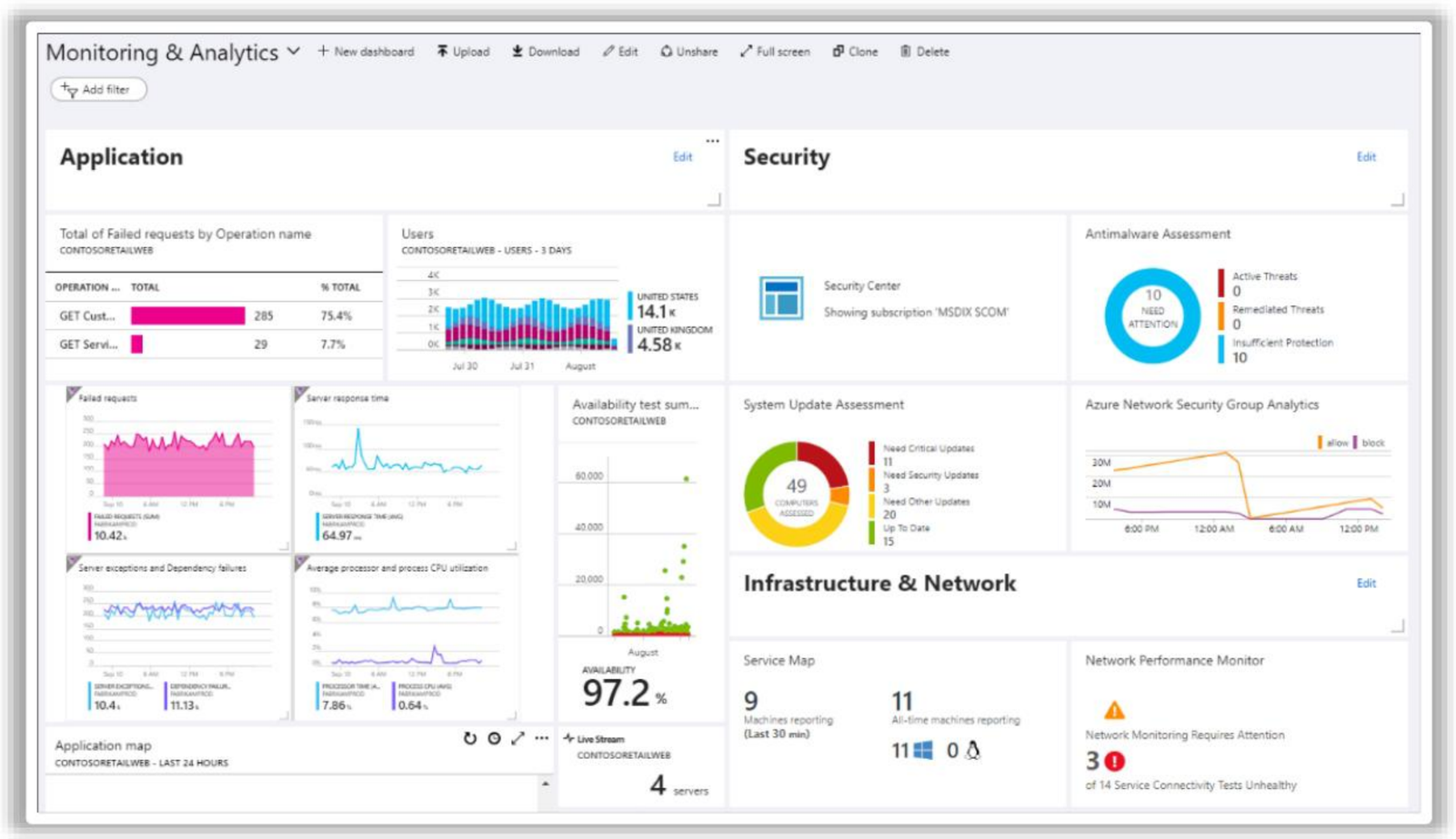


Figure 5.58: Azure Monitor Dashboard

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

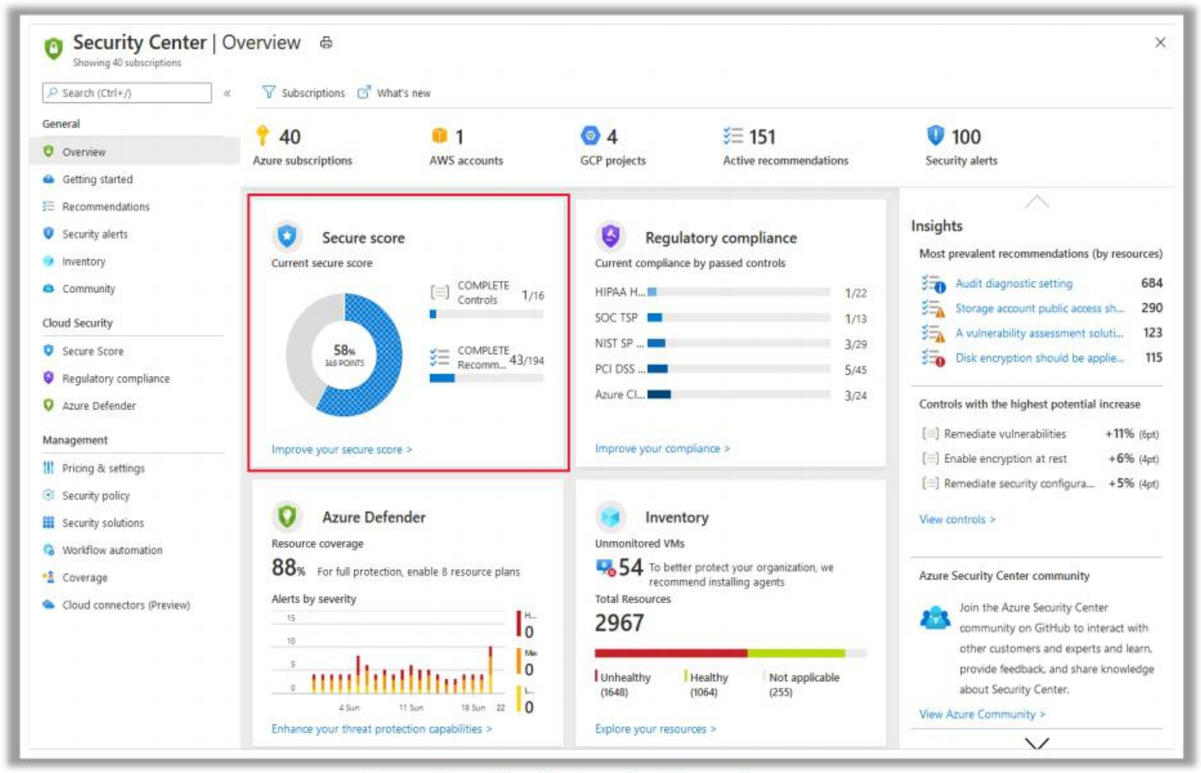
Azure Monitor offers the following operational security features/services:

- **Azure Monitor logs**: These logs help to analyze and monitor the availability and performance of various resources.
- **Automation**: It allows to automate manual processes and enforce configurations for physical and virtual machines.
- **Backup**: Azure Monitor provides a backup service to back up and restore the critical data on Azure.
- **Site Recovery**: Azure Monitor provides the Site Recovery service that ensures high availability of critical applications.
- **Azure Activity Log**: Azure Activity Log (formerly known as Operational log) provides information regarding the operations performed on the resources of any given subscription.
- **Azure Diagnostic Logs**: These logs provide insights into operations performed by a resource in a given subscription.
- **Application Insights**: With the Application Insights feature, Azure Monitor allows monitoring of the performance, availability, and usage of applications hosted on Azure.
- **Infrastructure monitoring**: Azure Monitor helps to analyze and optimize the infrastructure performance by allowing to monitor the health of VMs and their dependencies.
- **Network monitoring**: It helps in diagnosing and monitoring networking issues in VMs without logging into them. Cloud admins can trigger a packet capture, analyze NSG flow logs, detect routing issues, and obtain control and visibility into the Azure network.

ide01.ir

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

Azure Security Center



Azure Security Center dashboard

- **Azure Security Center (ASC)** is a security management system that helps in preventing, detecting, and responding to threats by providing visibility and control on Azure resources
- Use it to gain granular control over subscriptions via integrated security monitoring and policy management across subscriptions

Source: *https://azure.microsoft.com*

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

Azure Security Center

Azure Security Center (ASC) is a security management system that helps in preventing, detecting, and responding to threats by providing visibility and control on Azure resources. It ensures cloud operational security by strengthening the security posture of data centers and securing hybrid workloads. It allows monitoring and improving the security posture of applications, machines, storage, networks, and data services on Azure.

ASC detects security vulnerabilities by constantly analyzing the security state of all Azure resources and provides recommendations to fix them. It helps cloud admins to have granular control over their subscriptions by providing integrated security monitoring and policy management across their subscriptions.

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

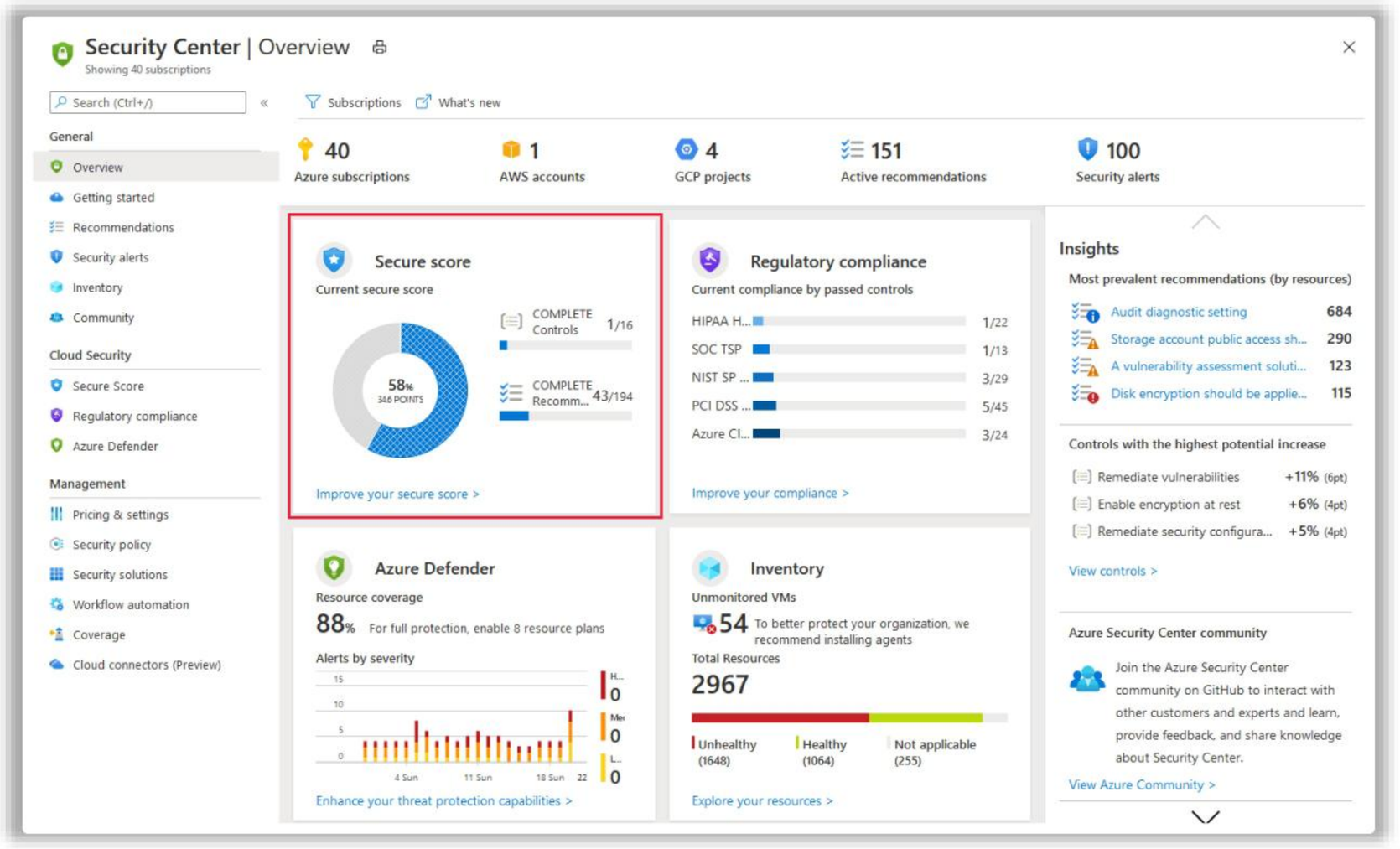


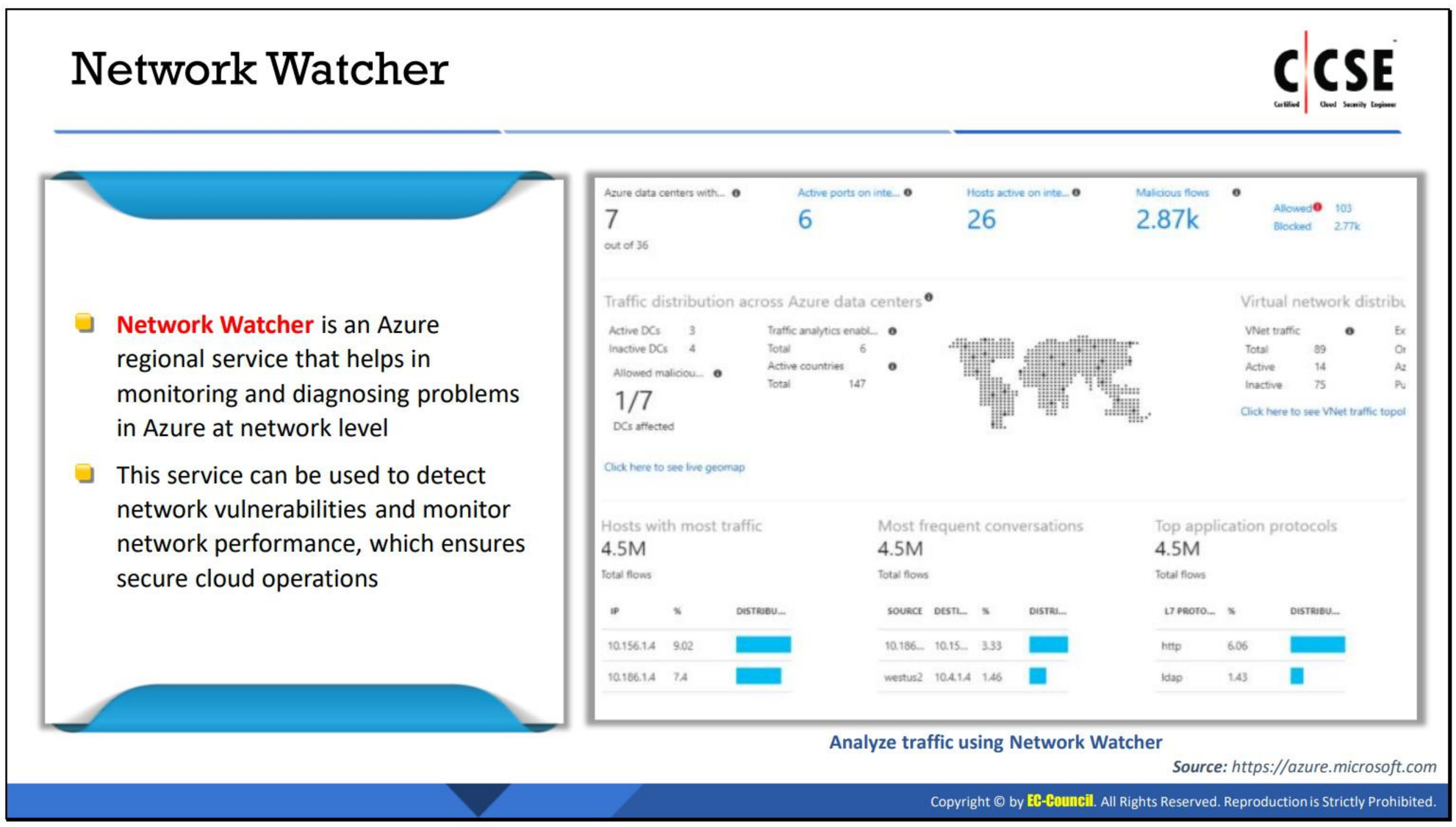
Figure 5.59: ASC overview (main dashboard)

ASC offers the following operational security features:

- **Security policies and recommendations**: ASC allows to define security policies based on organizational security requirements. It also recommends policies that are necessary to be implemented.
- **Data protection**: It gathers and secures security-related data (metadata, configuration information, event logs, etc.) to help customers in detecting, preventing, and responding to threats.
- **Data collection**: It collects data from the VMs running on Azure to evaluate their security posture and provide security recommendations to strengthen their security.
- **Data sources**: It displays the security state of resources, detects threats and vulnerabilities, and recommends mitigations by gathering data from different sources such as Azure services, VMs, network traffic, and partner solutions.
- **Azure secure score**: ASC provides a secure score by visualizing the security state of cloud resources, including networks, applications, and servers. This score helps in assessing and improving the security posture of Azure resources.
- **Azure Defender**: Azure Defender is integrated into ASC; it helps to secure hybrid cloud workloads such as IoT, servers, storage, and data.
- **Streamline threat investigation**: ASC helps to detect, streamline threat investigation, and automate remediation using AI and automation.

hide01.ir

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



Analyze traffic using Network Watcher

Source: *https://azure.microsoft.com*

Network Watcher

Network Watcher is an Azure regional service that helps in monitoring and diagnosing problems associated with Azure at a network level. It contains network diagnostic and visualization tools that help to understand, diagnose, and obtain visibility into the Azure network. This service helps cloud admins to detect network vulnerabilities and monitor network performance, ensuring secure cloud operations.

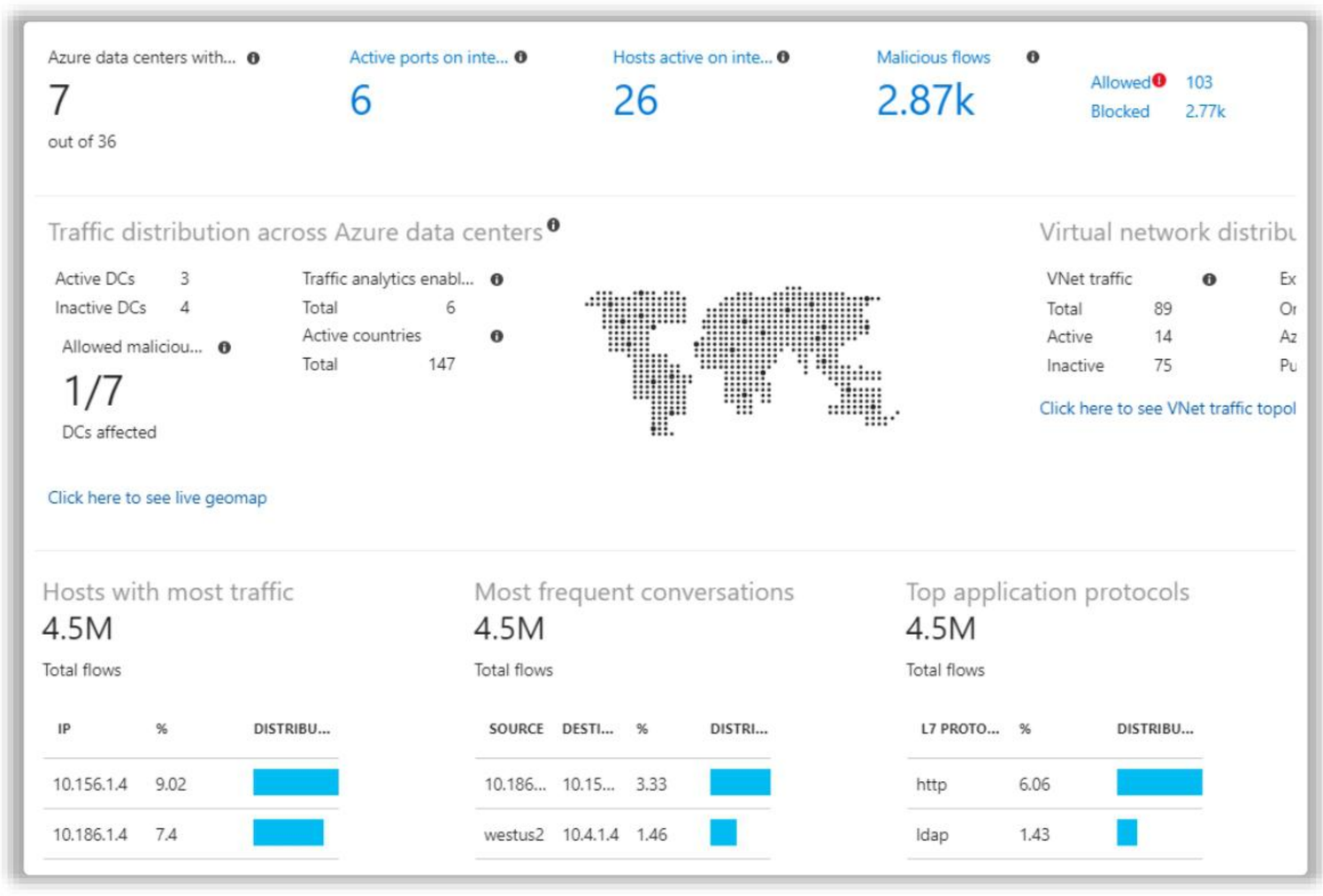


Figure 5.60: Analyze traffic using Network Watcher

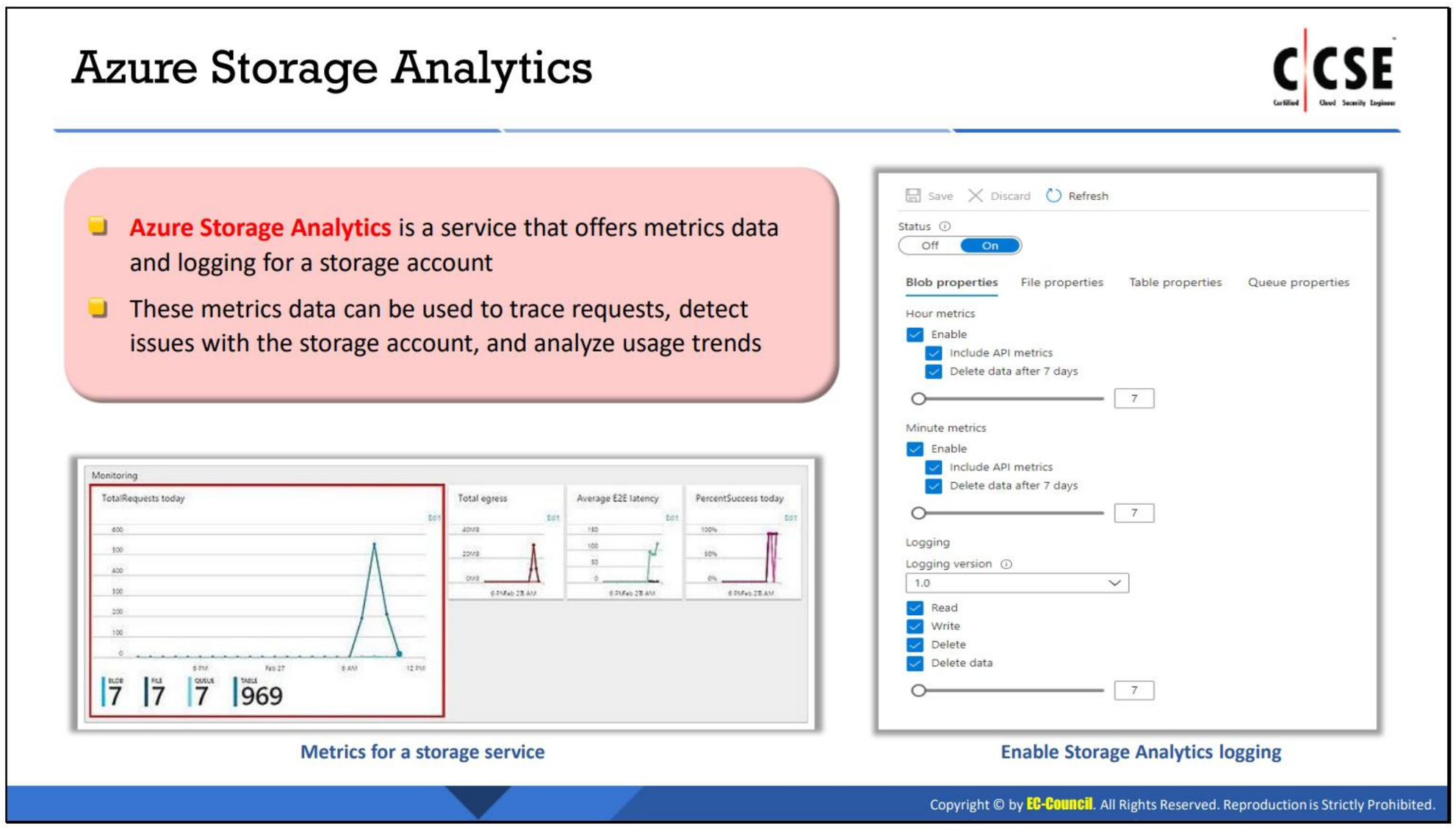
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following operational security features are provided by Network Watcher:

- **Audit logs**: These logs are available for operations performed on all network resources in Azure. Audit logs log operations performed as a part of network configuration.
- **IP flow verifies**: This feature of Network Watcher checks if a packet is denied or allowed according to flow information 5-tuple packet parameters (Source IP, Destination IP, Protocol, Source Port, and Destination Port).
- **Next hop**: Network Watcher helps to diagnose misconfigured user-defined routes by determining the next hop for routed packets in Azure Network Fabric.
- **Security group view**: It provides information regarding security rules that are effective and applied on a VM.
- **NSG flow logging**: NSG flow logging helps in capturing traffic logs that are denied or allowed by the security rules in a group.
- **Remote network monitoring**: Network Watcher enables the automation of remote network monitoring via packet capture to detect networking issues without logging into VMs.
- **VPN connectivity issues**: Network Watcher helps in diagnosing common VPN gateway and connectivity issues. It facilitates the detection of issues and investigates them via logs.

hide01.ir

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



Azure Storage Analytics

Storage Analytics is an Azure service that offers metrics data and logging for a storage account. These data can be used to trace requests, detect issues with the storage account, and analyze usage trends. This service logs complete information about all requests (both failed and successful) to the storage account. This service should be enabled for every service that needs to be monitored individually. Azure Storage Analytics logging can be used for the Queue, Blob, and Table services.

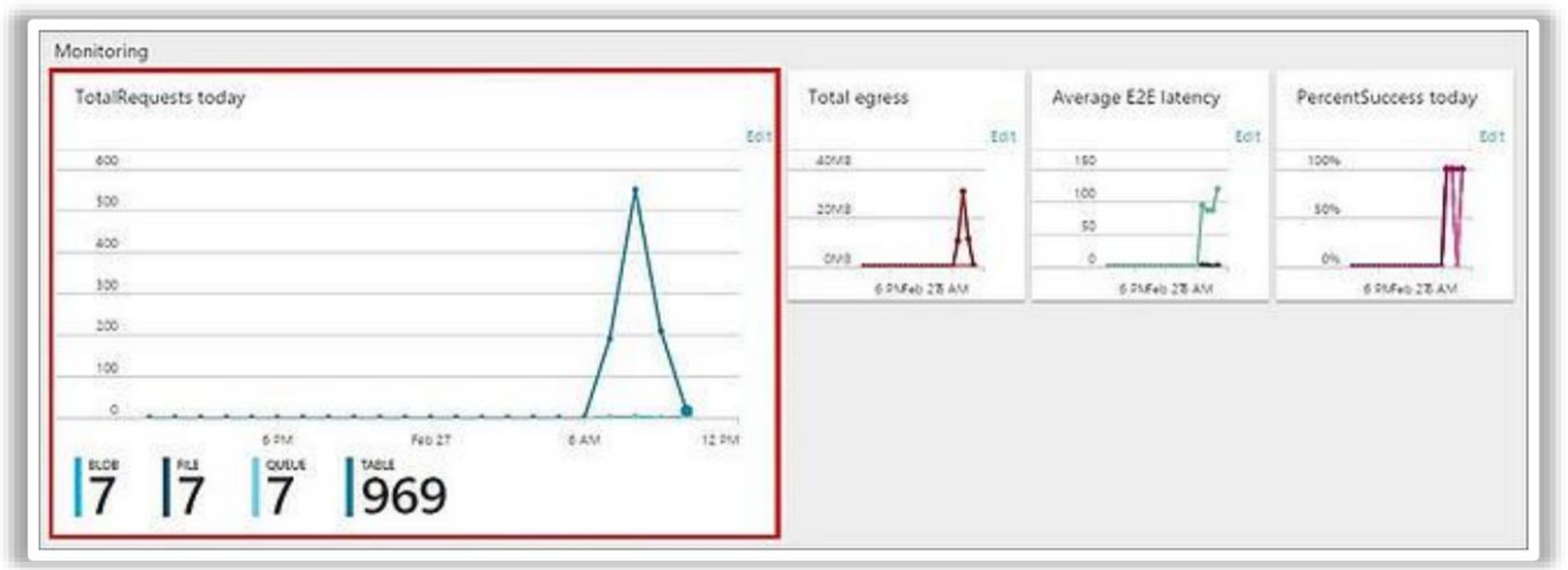


Figure 5.61: Metrics for a storage service

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

The aggregated data of requests to a storage account are stored in a popular blob for logging and in popular tables for metrics; these data can be accessed via the Blob and Table service APIs, respectively.

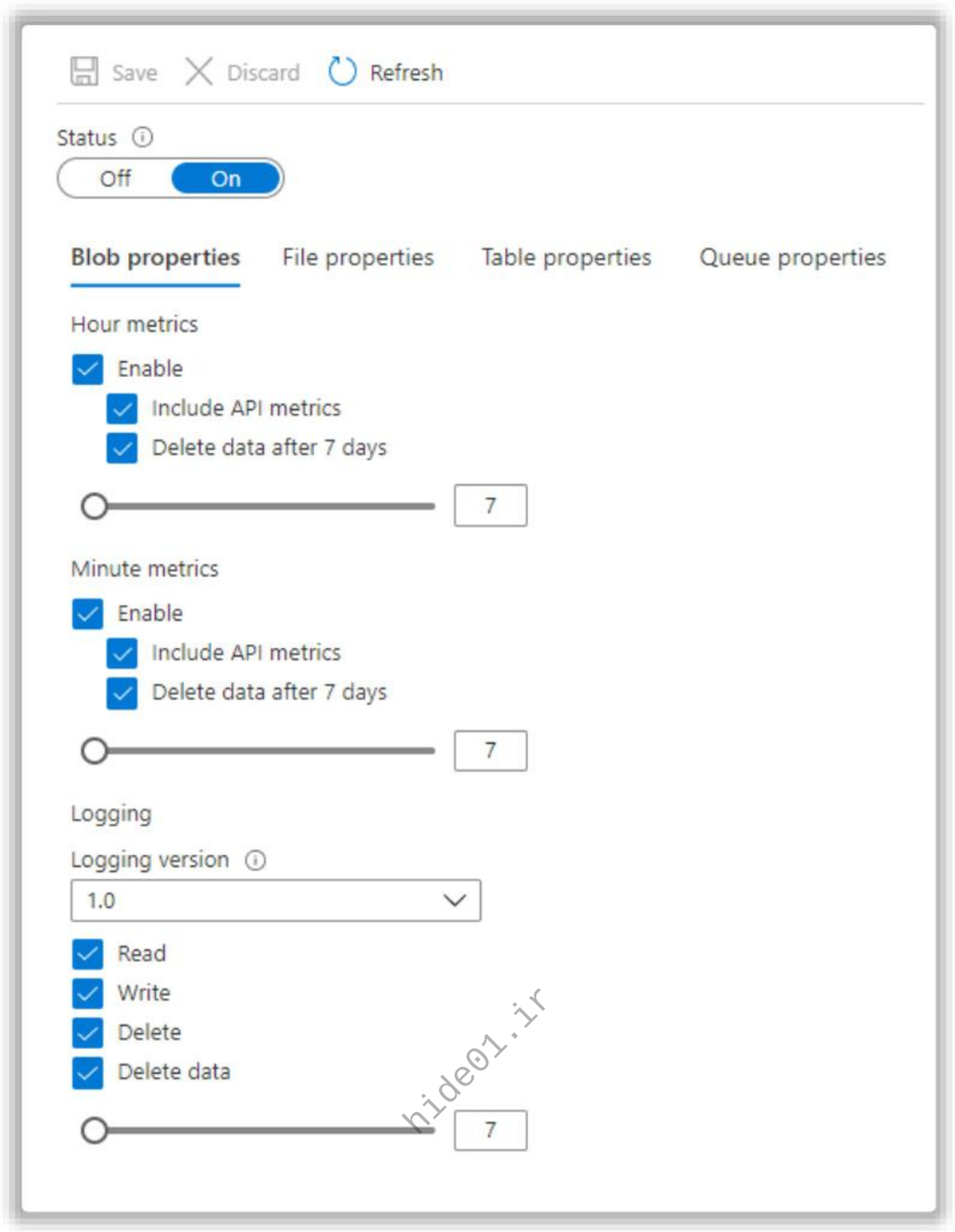
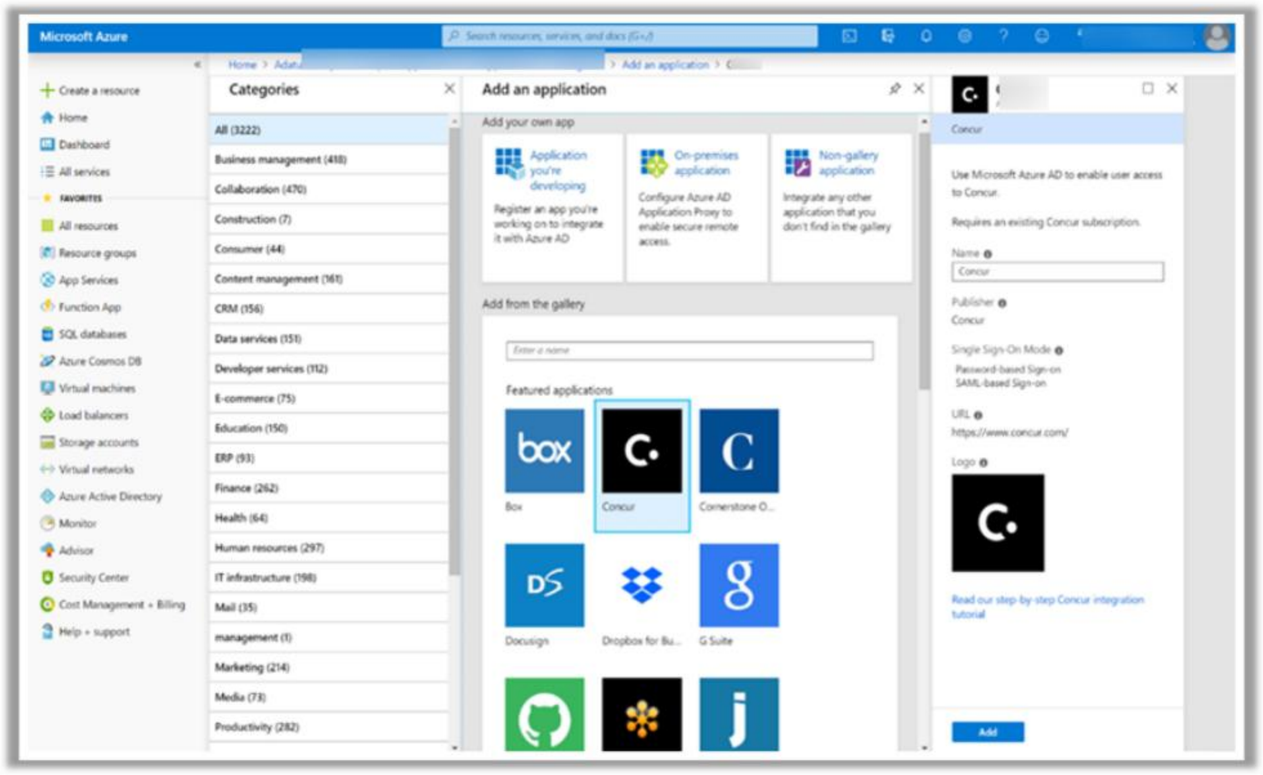


Figure 5.62: Enable Storage Analytics logging

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

Azure Active Directory

- **Azure Active Directory (AD)** provides identity management capabilities such as MFA, self-service password management, privileged account management, self-service group management, role-based access control, rich auditing, application-usage monitoring, and security monitoring and alerting
- Get complete details about the actions/events that occurred in Azure AD via these audit reports



Azure Active Directory dashboard

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

Azure Active Directory

Azure Active Directory (AD) consists of a collection of identity management capabilities such as device registration, multi-factor authentication (MFA), self-service password management, privileged account management, self-service group management, role-based access control, rich auditing, application-usage monitoring, and security monitoring and alerting. Azure AD improves application security by offering MFA and conditional access. It also offers security reporting and monitoring, which helps in monitoring application usage and preventing advanced threats.

Azure AD provides security reports, activity reports, and audit reports for a directory. Audit reports help in detecting privileged actions in Azure AD, including changing policy configuration, elevation changes, and directory configuration changes. Cloud admins can obtain complete details about the actions/events in Azure AD via these audit reports.

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

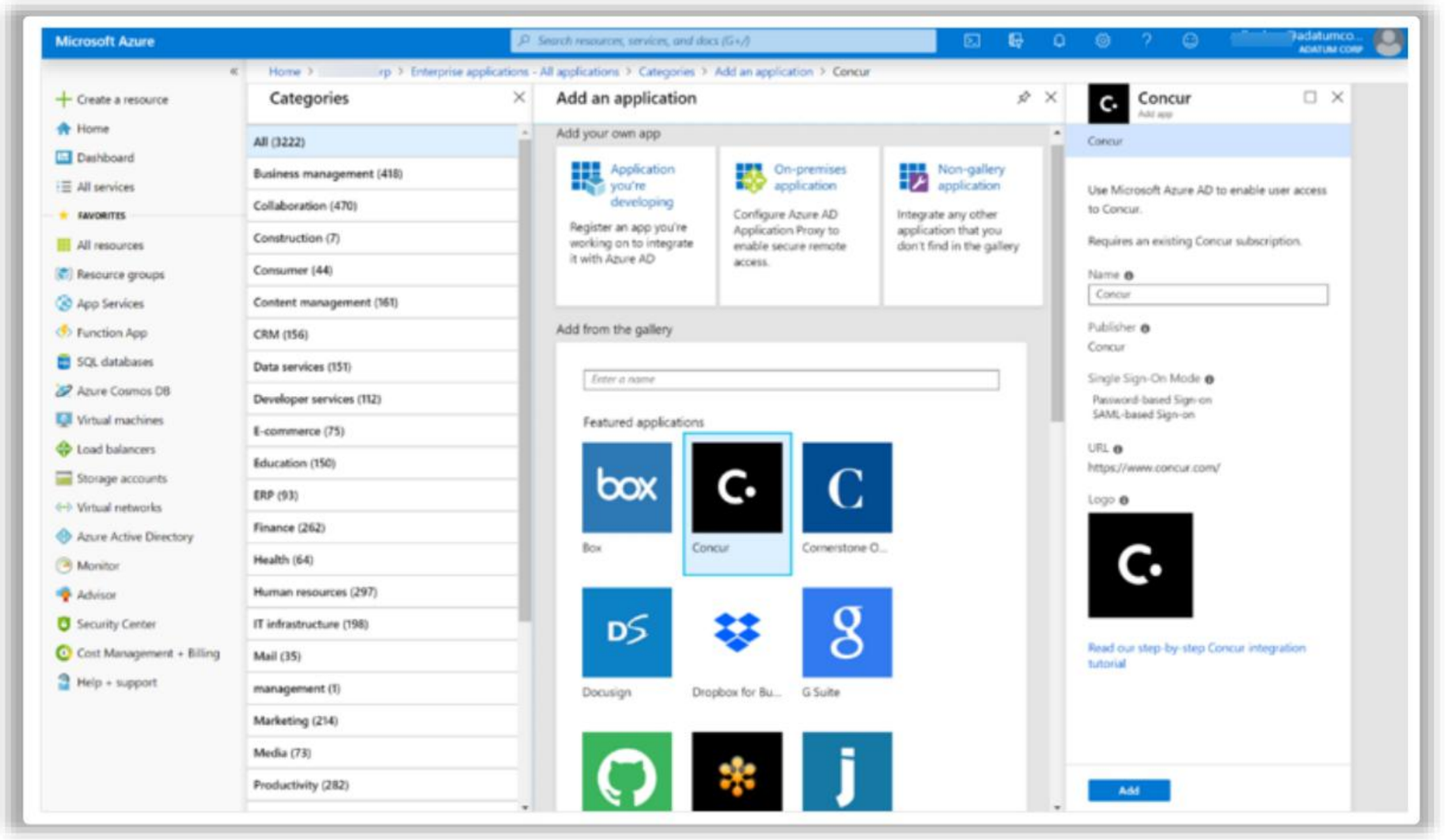
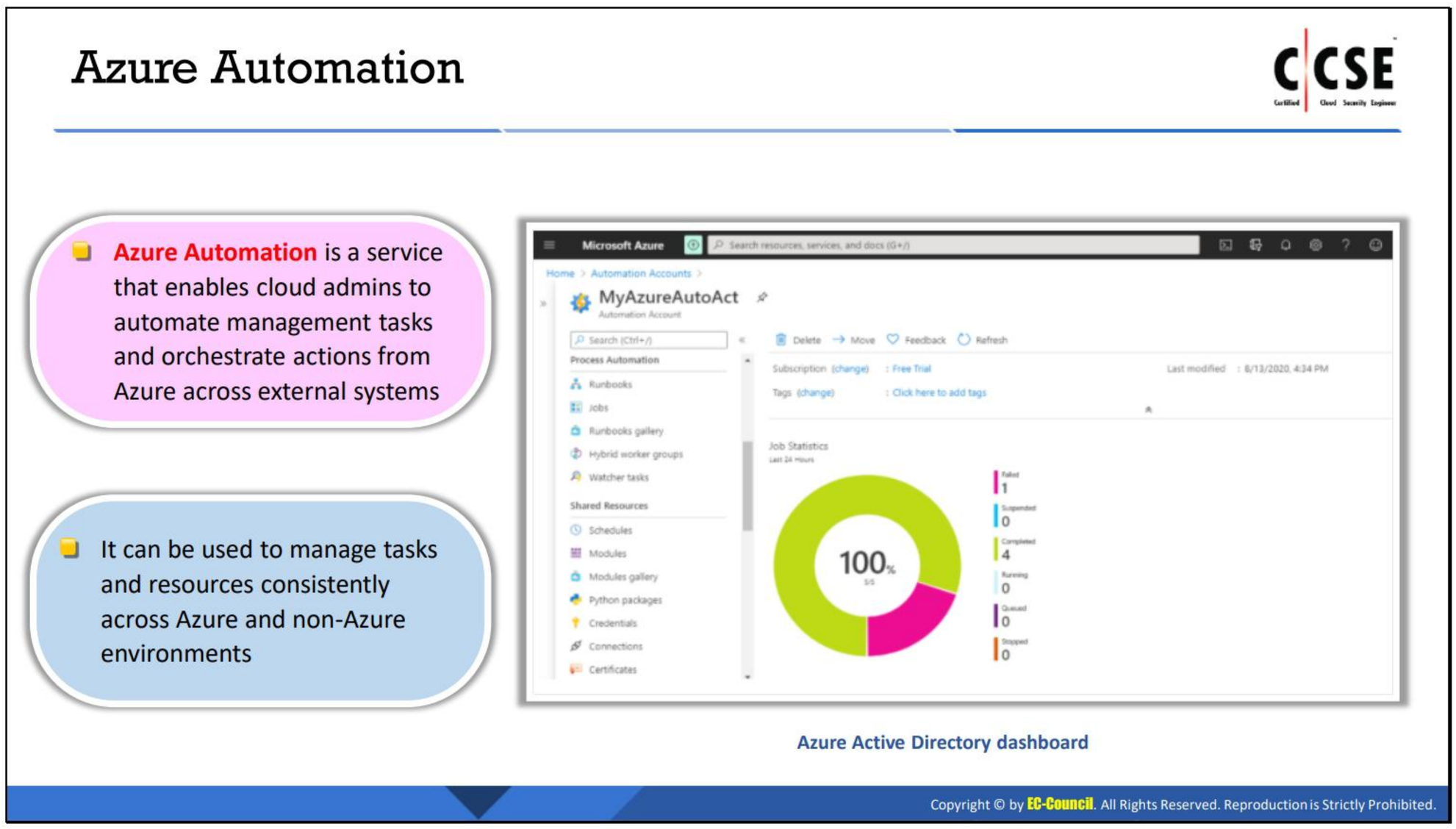


Figure 5.63: Azure AD dashboard

Azure AD offers the following features for operational security:

- **Authentication**: Azure AD ensures operational security by allowing cloud admins to manage MFA, self-service password reset, smart lockout, and custom-banned password list.
- **Application management**: Azure AD helps to manage on-premises and cloud apps via single sign-on (SSO), Application Proxy, SaaS apps, and My Apps portal.
- **Conditional access**: It helps cloud admins to manage access to cloud applications.
- **Device management**: Cloud admins can use Azure AD to manage and control how on-premises and cloud devices access corporate data.
- **Identity Protection**: Azure AD Identity Protection allows cloud admins to identify the potential vulnerabilities that affect the identity of their organization, configure policies that help in responding to malicious actions, and resolve them by taking appropriate actions.
- **Privileged identity management (PIM)**: The PIM feature helps to manage, control, and monitor access to resources in Azure, Azure AD, and other Microsoft Online Services (e.g., Microsoft 365).
- **Reports and monitoring**: With the reporting and monitoring feature, Azure AD provides insights into the usage and security patterns in a cloud environment.

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



Azure Automation

Azure Automation is a service that enables cloud admins to automate management tasks and orchestrate actions from Azure across external systems. It provides a cloud-based automation and configuration service that consistently manages tasks and resources across Azure and non-Azure environments. Azure Automation provides complete control during resource/workload deployments, operations, and decommissioning.

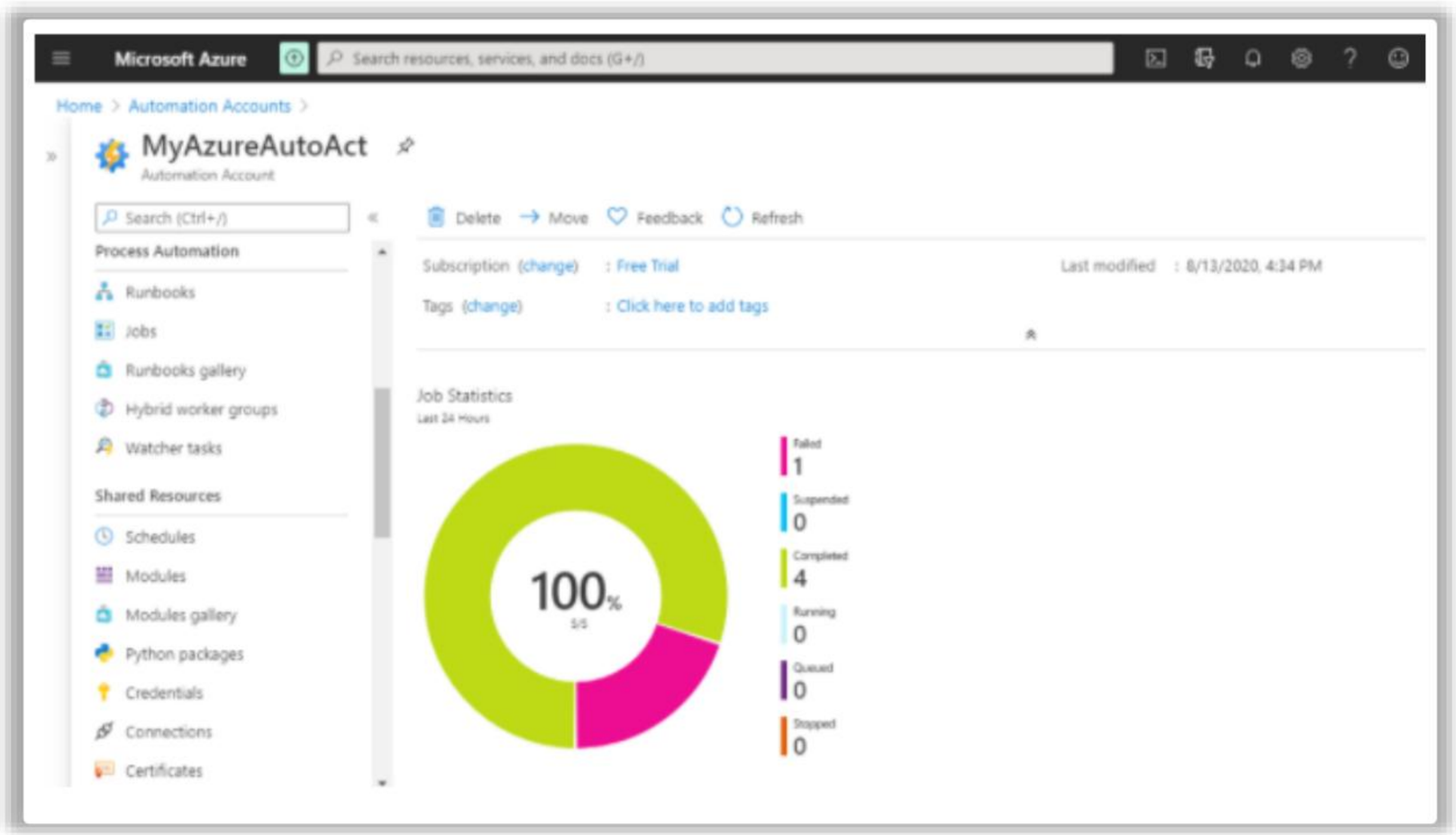


Figure 5.64: Azure Automation dashboard

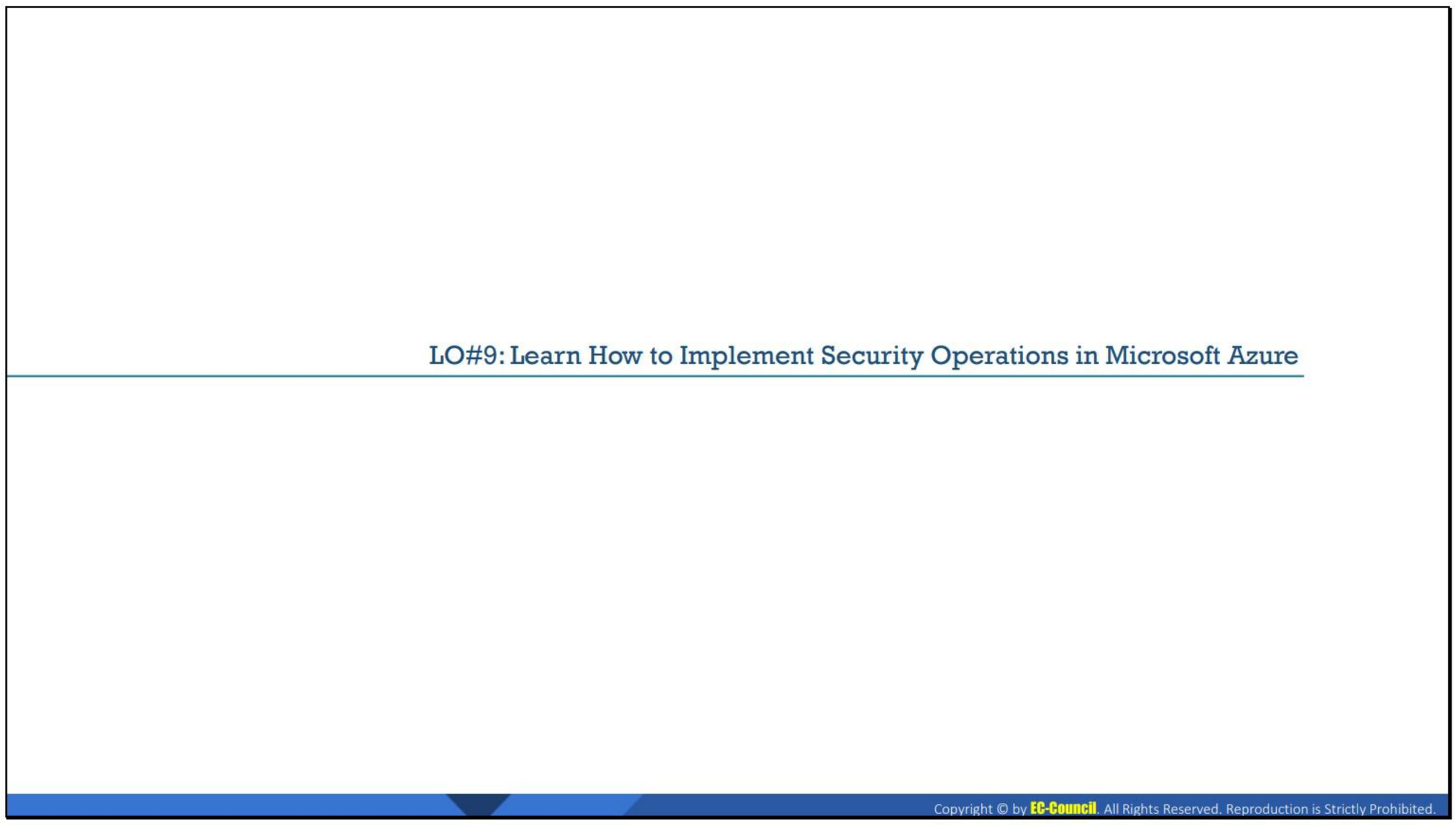
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Features of Azure Automation

- **Process automation**: Azure Automation allows to automate error-prone and time-consuming Azure management tasks. This feature helps in managing runbooks (that orchestrate processes) graphically using Python or PowerShell. Process automation saves time and minimizes overhead costs.
- **Configuration management**: It supports configuration management by providing change tracking, inventory collection, and state configuration.
- **Update management**: This feature allows visibility into update compliance across Azure and non-Azure environments and helps to create scheduled deployments.
- **Heterogenous support**: It works well across hybrid cloud environments as well as Linux and Windows systems by providing automation and configuration for deployed workloads and their OS.
- **Shared capabilities**: Automation supports shared capabilities that help in automating and configuring cloud environments securely and easily. These capabilities include RBAC, shared resources, flexible scheduling, tagging, auditing, and source control integration.
- **Faster and reliable services**: With serverless runbooks, Azure Automation provides faster and reliable services.

hide01.ir

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



LO#9: Learn How to Implement Security Operations in Microsoft Azure

The objective of this section is to implement operational security in the Azure environment using various Azure features and services. In this section, cloud security engineers will learn how to manage and monitor user passwords, configure Azure service health alerts, manage subscription utilizing management groups, monitor Azure storage services for unexpected behavioral changes, monitor Azure AD reports, and enable Microsoft defender for endpoint detection integration. This section will help clous security engineers in safeguarding the Azure cloud environment of their organization.

mid001.ir

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

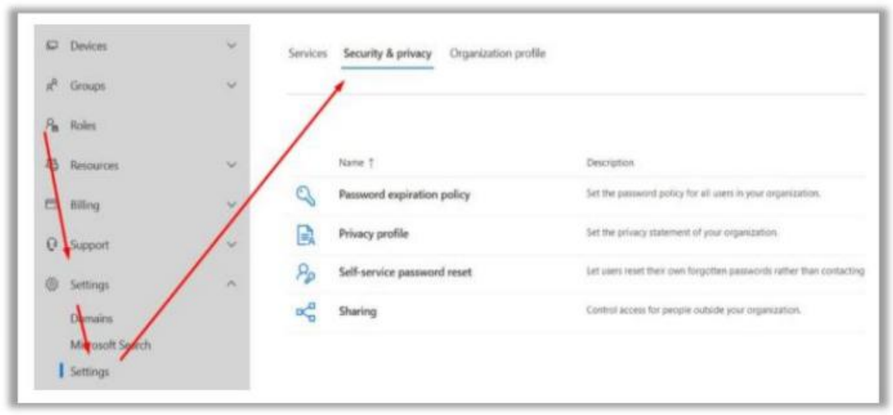
Manage and Monitor User Passwords

Manage and monitor user passwords in Azure using the following best practices:

1. Follow the guidelines stated in Microsoft Password Guidance for proper password protection in Azure

Steps for the guidelines provided by Microsoft Password Guidance:

1. Configure password complexity in Azure AD



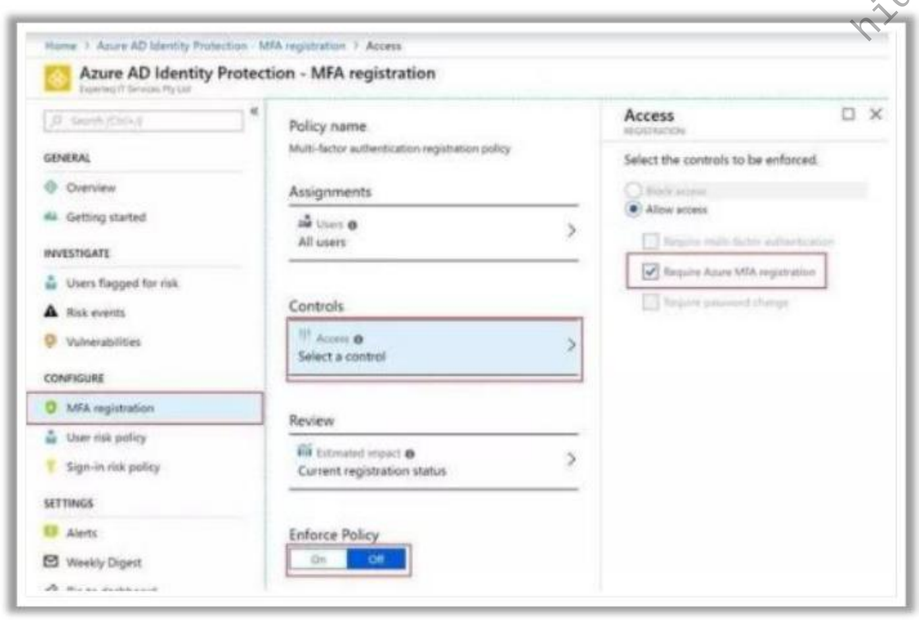
2. Disable the password expiration rule

3. Prevent custom banned passwords

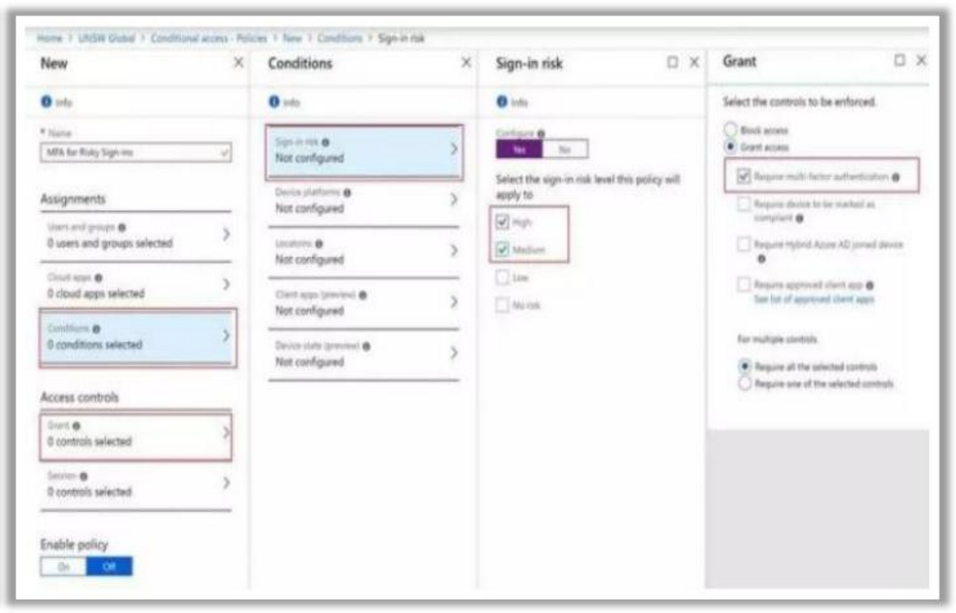
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Manage and Monitor User Passwords (Cont'd)

hide01.ir



4. Setting Identity Protection policy



5. Enable risk-based MFA challenges

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

Manage and Monitor User Passwords

To manage and monitor user passwords in Azure, implement the following best practices.

Follow the guidelines stated in Microsoft Password Guidance

Follow the guidelines stated in **Microsoft Password Guidance** for proper password protection in Azure. These guidelines are meant for the users of Microsoft Identity platforms (e.g., Microsoft account, Active Directory (AD), and Azure AD).

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

Steps for the guidelines provided by Microsoft Password Guidance:

- **Configure password complexity in Azure AD:**
  - Log into the **Azure Portal** and select **Directory + Subscription** on the toolbar of the portal.
  - Choose the directory containing the Azure AD B2C tenant.
  - On the Azure portal, search for **Azure AD B2C** and select it.
  - Click on **User flows** and select a user flow. Then, click on **Properties**.
  - Modify the password complexity requirements for this user flow under **Password complexity** to **Simple, Custom,** or **Strong**. Ensure that it is at least 8 up to 65 characters long.

    Password complexity is as follows:

    Simple: A password of length between 8 to 64 characters.

    Strong: A password of length between 8 to 64 characters with the requirement of one lowercase, uppercase, symbol, or number.

    Custom: A customized password that can be configured based on the complexity rules established by admins. It offers better control over complexity rules and password length.

hide01.ir

Figure 5.65: Reset Password

- **Disable character-composition requirements**:

  Do not keep character-composition requirements (e.g., (,*,$,&,^,%) while setting up password complexity rules. Disable the character-composition requirements to prevent users from setting commonly attacked passwords that can be easily estimated. These complexity requirements make users set passwords that are less secure and difficult to remember. Disable it to allow users to keep more secure and memorable passwords.

- **Disable the password expiration rule to remove mandatory periodic password resets for user accounts:**
  - Go to **Microsoft 365 Admin Center** and sign in as global administrator.

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

- Choose **Settings** and then click on **Security and Privacy**.

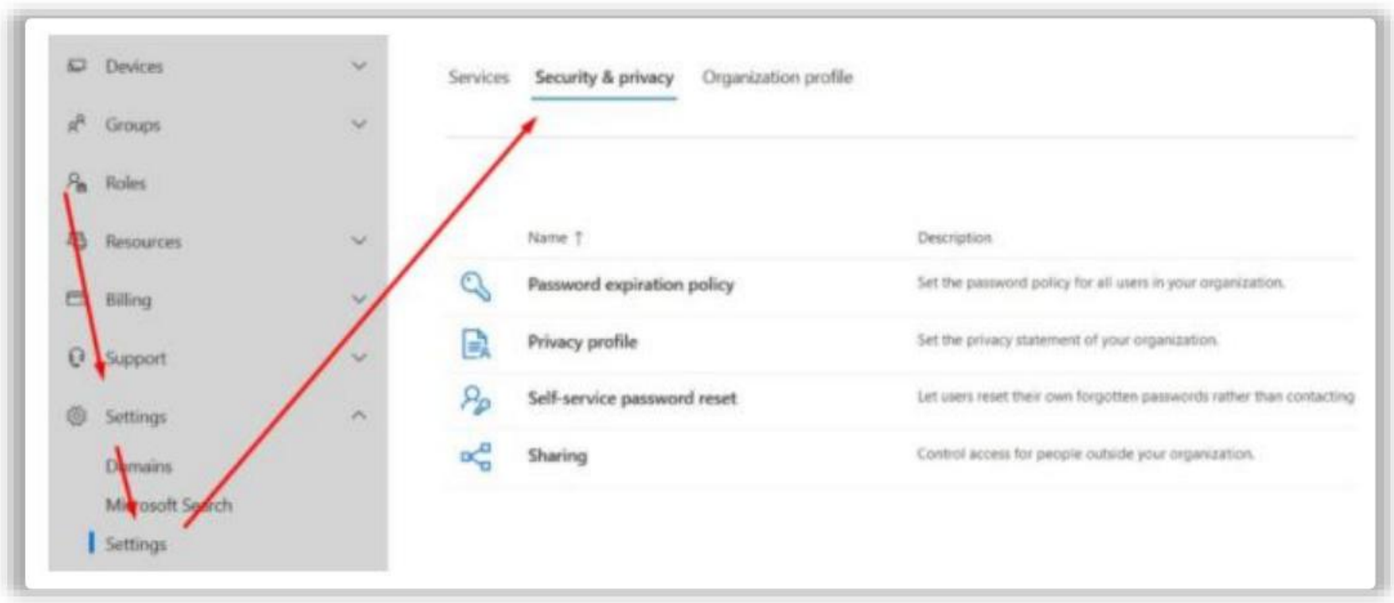


Figure 5.66: Security & Privacy

- Click on **Password expiration policy** and deselect **Set user passwords to expire after a number of days.**

- **Use Azure AD password protection to prevent custom banned passwords**

  Prevent users from using commonly used passwords such as "**password**," "**monkey**," or "**abcdefg.**" If a user selects a password banned by the admin, they get the following error message.

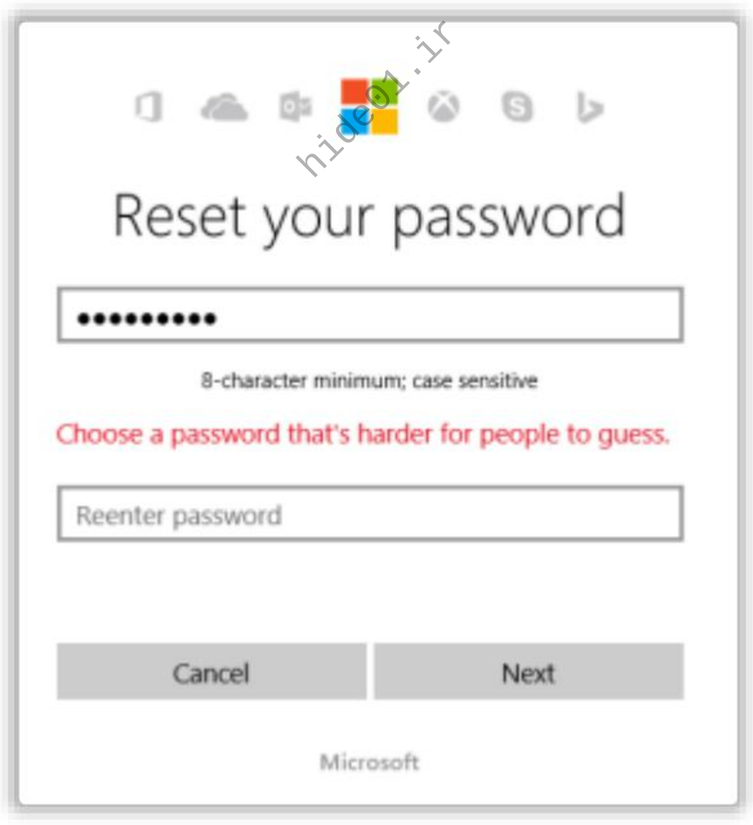


Figure 5.67: Reset Password

Use **Azure AD password protection** to prevent setting custom banned passwords. It is enabled by default for all Azure users but contains only 1000 words in the default banned list.

- Navigate to **Azure AD Settings**.
- Under **Security**, click on **Authentication methods**.
- Click on **Password protection**, followed by **Yes** for **Enforce custom list**.

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

- Enter your customized list of common passwords in **Custom banned password list**.
- Choose **Yes** for **Enable password protection on Windows Server AD** to ensure that the password protection feature is extended to on-premises AD (this is optional).
- For **Mode**, choose **Enforced**.

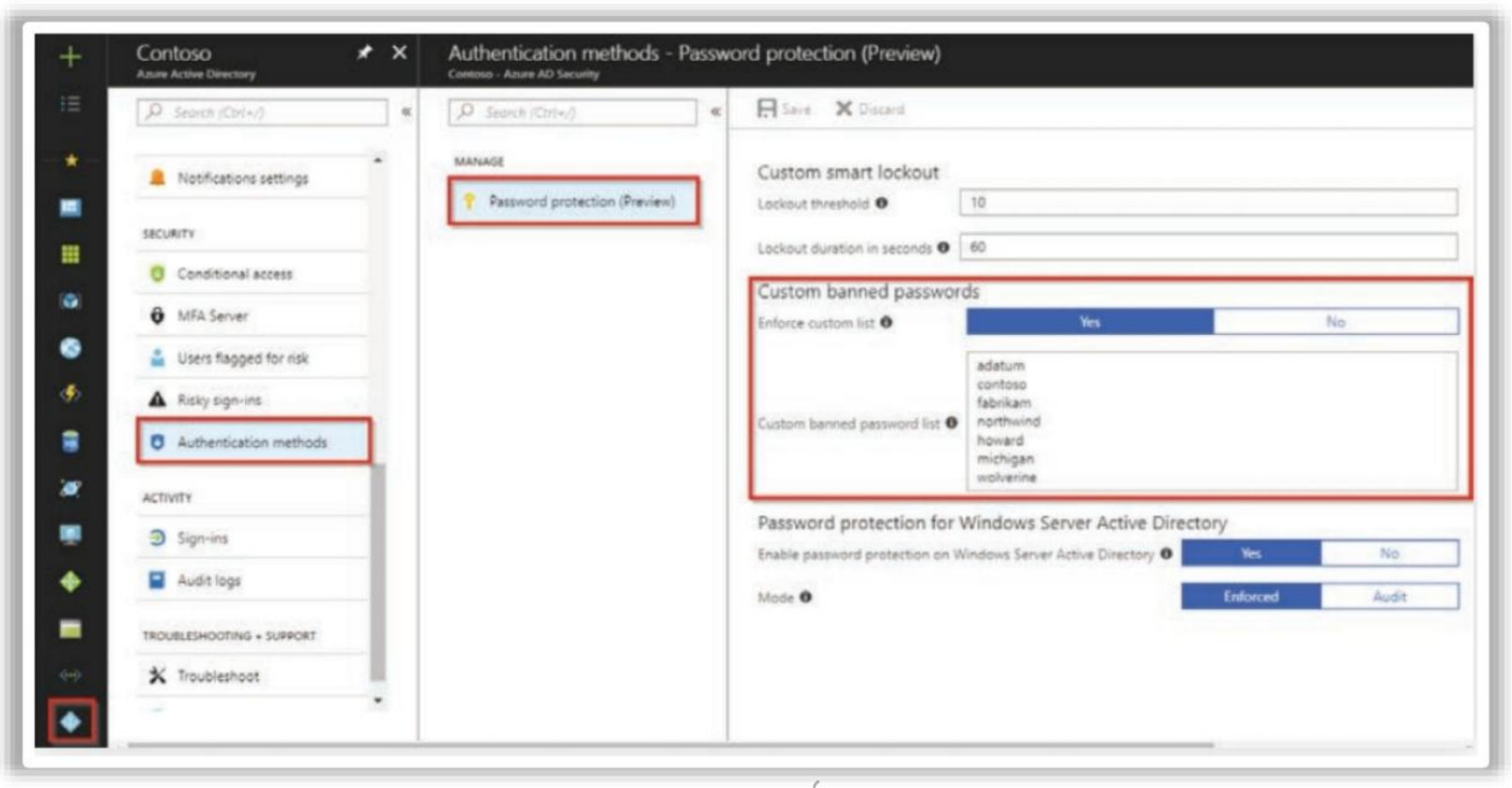


Figure 5.68: Choose Enforced

video01.ir

- **Set up Identity Protection policy to mandate users to register for MFA:**

  Organizations must mandate employees and users to register for MFA to ensure cloud operational security. Ensure that all cloud users update the current security information such as alternate email address, phone number, or device to receive push notifications. This allows users to respond to security challenges successfully and know about security events.

  Update current security information for users to verify their identity when they forget their password or someone else tries to log into their accounts. Moreover, use timely notifications when any security event (e.g., login attempts or modifying password attempts) occurs.

  - Log into the Azure portal and choose **Azure AD**.
  - Select **Security**, **Identity protection,** followed by **MFA registration policy**.
  - Choose **Select individuals and groups** or **All users** under **Assignments**.
  - Under **Controls**, select the checkbox beside **Require Azure AD MFA registration**.
  - Select **On** for **Enforce Policy** and click on **Save**.

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

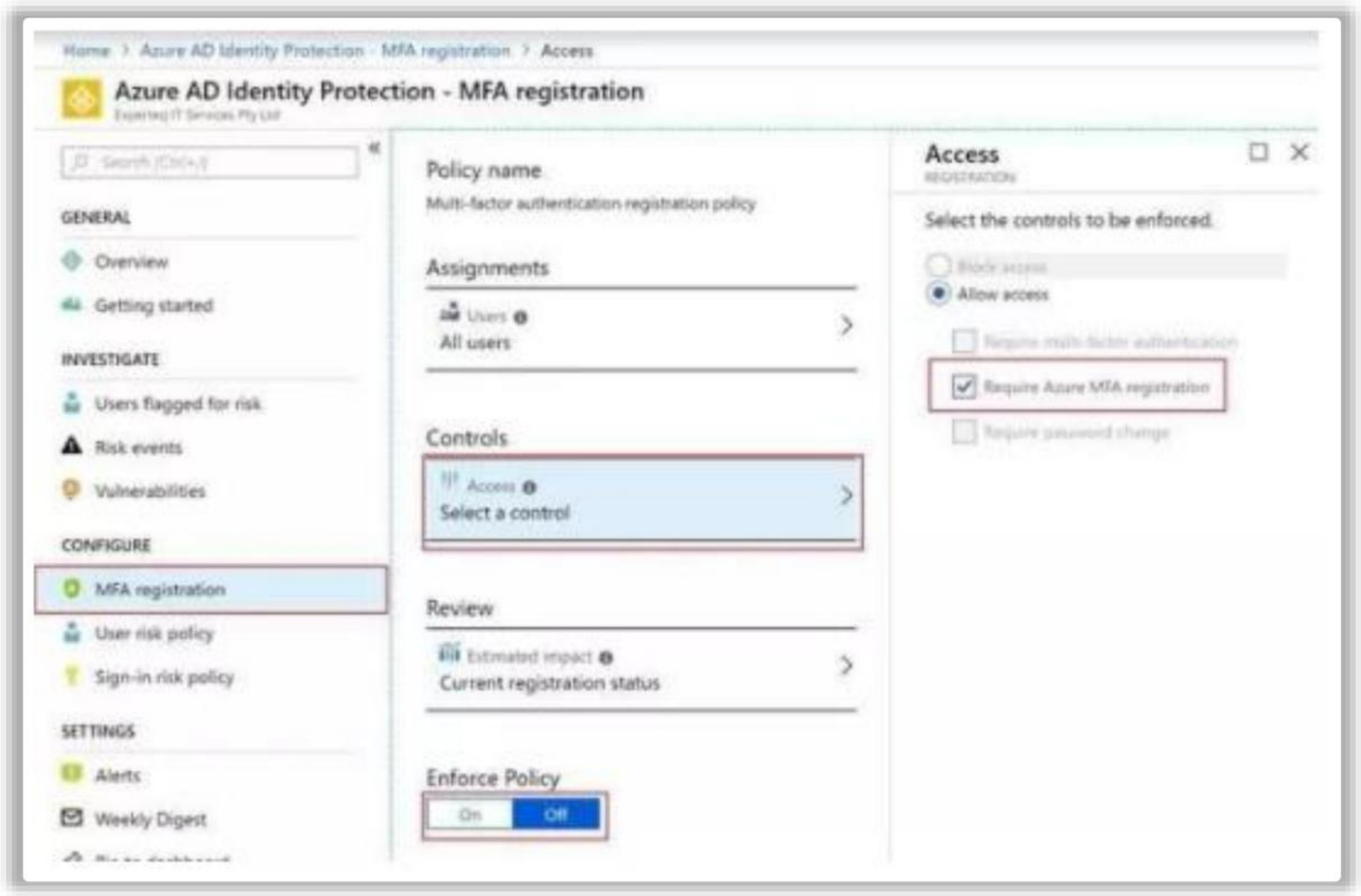


Figure 5.69: MFA Registration

- **Enable risk-based MFA challenges**:

  Enable risk-based MFA to improve the security posture of cloud environments. Accordingly, enforce sign-in risk policies for users with suspicious behaviors so that they can authenticate themselves using risk-based MFA challenges. Ensure that users are already registered for Azure AD MFA because it is required to implement sign-in risk policy. Sign-in risk policy detects and responds to suspicious sign-in attempts by allowing users to verify their identity via Azure AD MFA.

  Steps to enable the sign-in risk policy:

  - Log into the Azure portal as a global administrator and search for **Azure AD** and select it.
  - Choose **Security** and select **Identity Protection** under the **Protect** menu.
  - Choose Sign-in risk policy on the left side of the menu.
  - The policy is applied to **All users** by default but can be changed to apply to only selected individuals or groups by going to **Assignments.**
  - Click on **Select conditions** under **Conditions**, followed by **Select a risk level**.
  - Choose **Medium and above** and click on **Select**. Click on **Done**.
  - For **Access controls**, click on **Grant access** and **Require multi-factor authentication** under **Select the controls to be enforced**.

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

- Select **On** for **Enforce Policy** and click on **Save**.

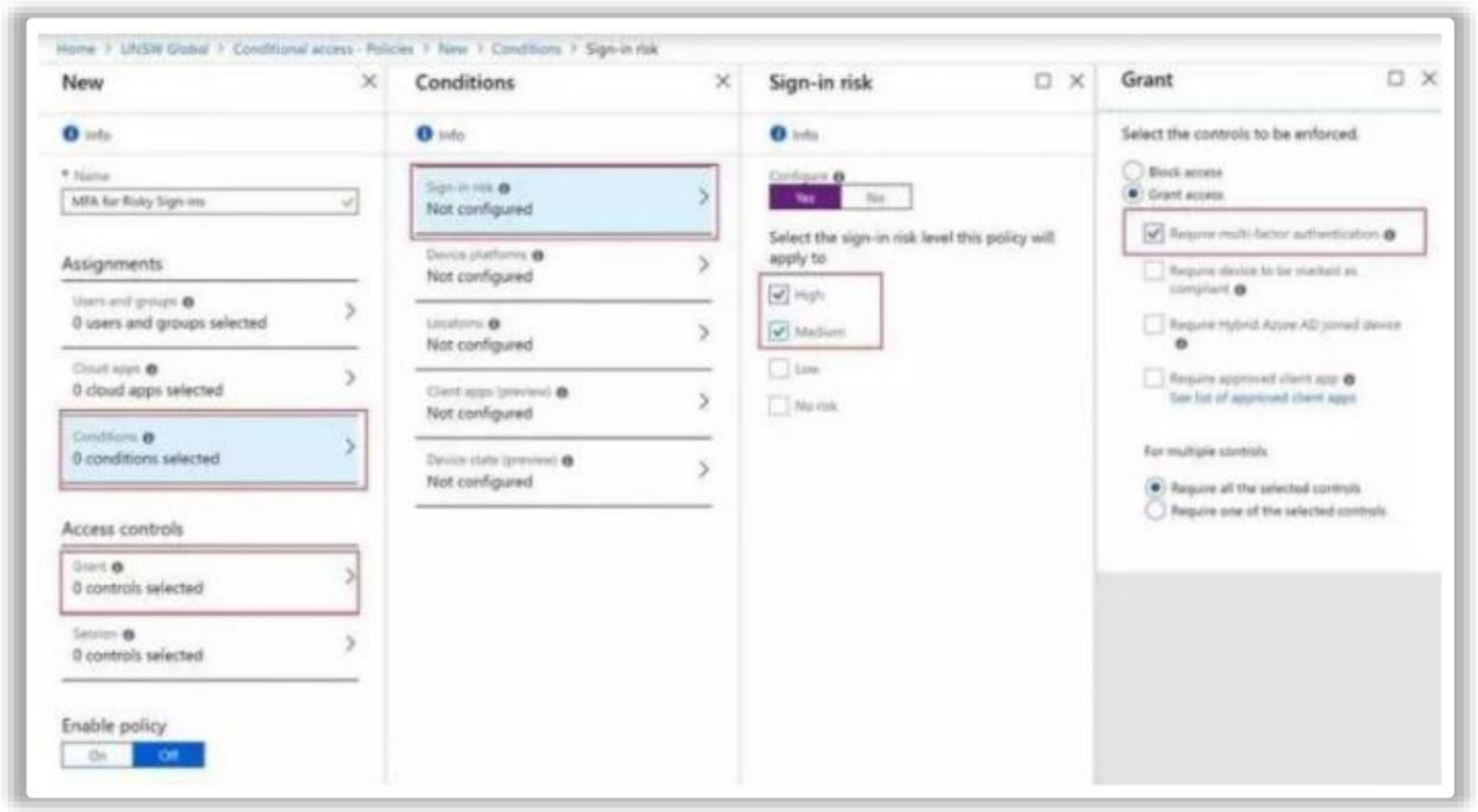


Figure 5.70: Enforce Policy

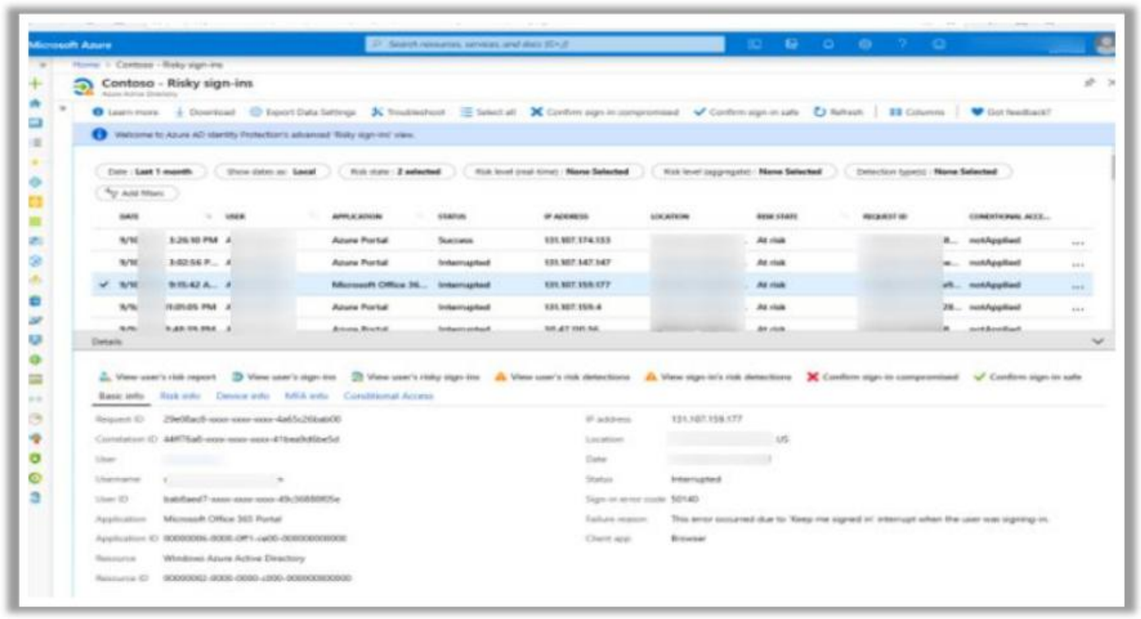
hide01.ir

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

Manage and Monitor User Passwords (Cont'd)

2 Detect suspicious activities by accessing reports related to risky sign-in and risky users

Use the **Azure Identity protection feature** that offers three reports (risky users, risky sign-ins, and risk detections) to help organizations investigate the identity risks present in their environment



Azure Security reports

Source: https://azure.microsoft.com

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

Manage and Monitor User Passwords

Detect Suspicious Activities by Accessing Reports of Risky Sign-ins and Risky Users:

Detect suspicious activities by accessing the reports of risky sign-ins and risky users. Azure identity protection offers three reports (risky users, risky sign-ins, and risk detections) to help organizations investigate the identity risks present in their environment.

These reports can be downloaded in .CSV format and used for further investigation and analysis. Risky sign-in and risky user reports can contain 2500 recent entries, whereas risk detection reports can contain 5000 recent records.

Steps to access the reports:

- Log into the Azure portal as a global administrator, search for **Azure AD,** and select it.

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

- Click on **Security** to access the reports.

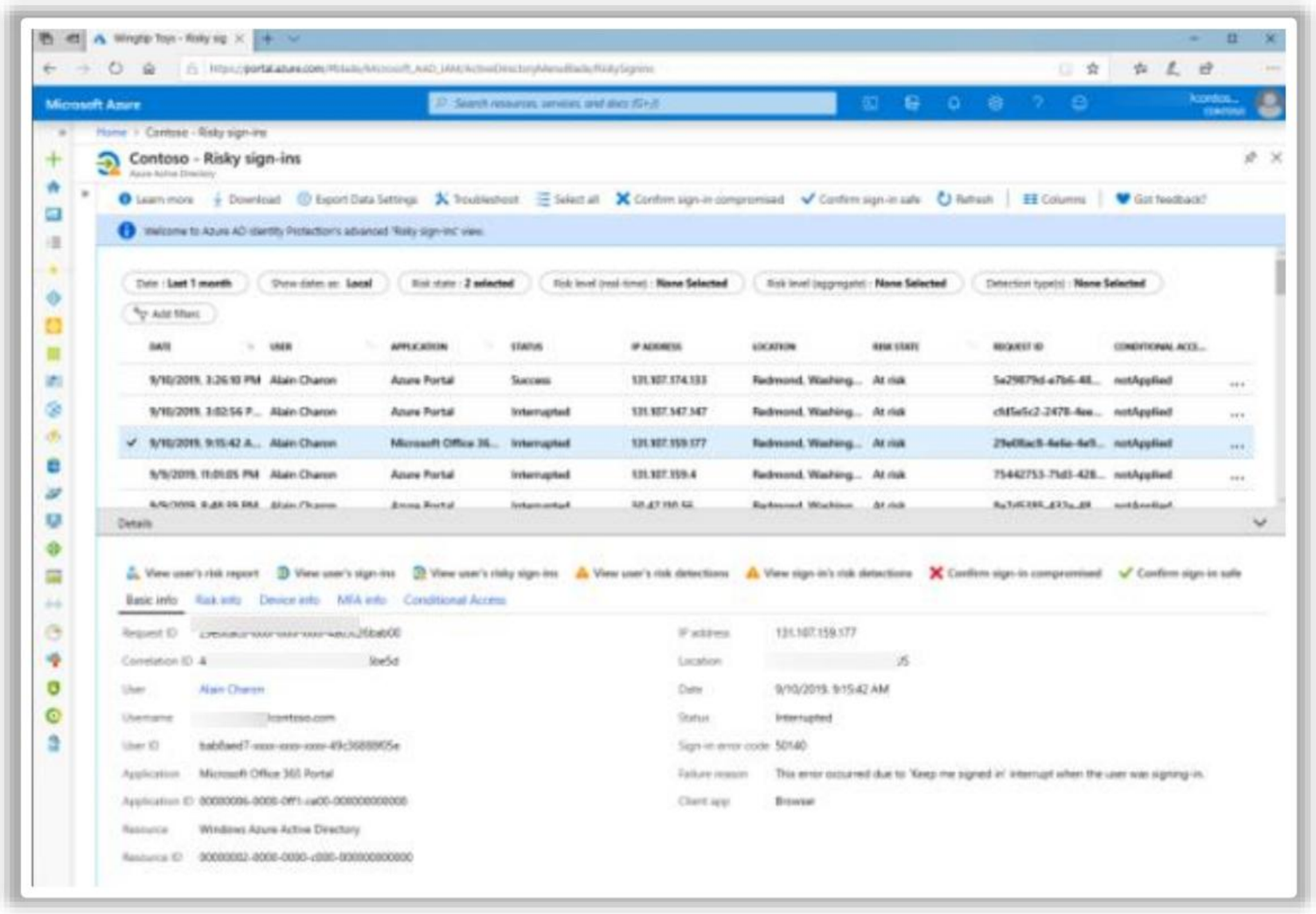
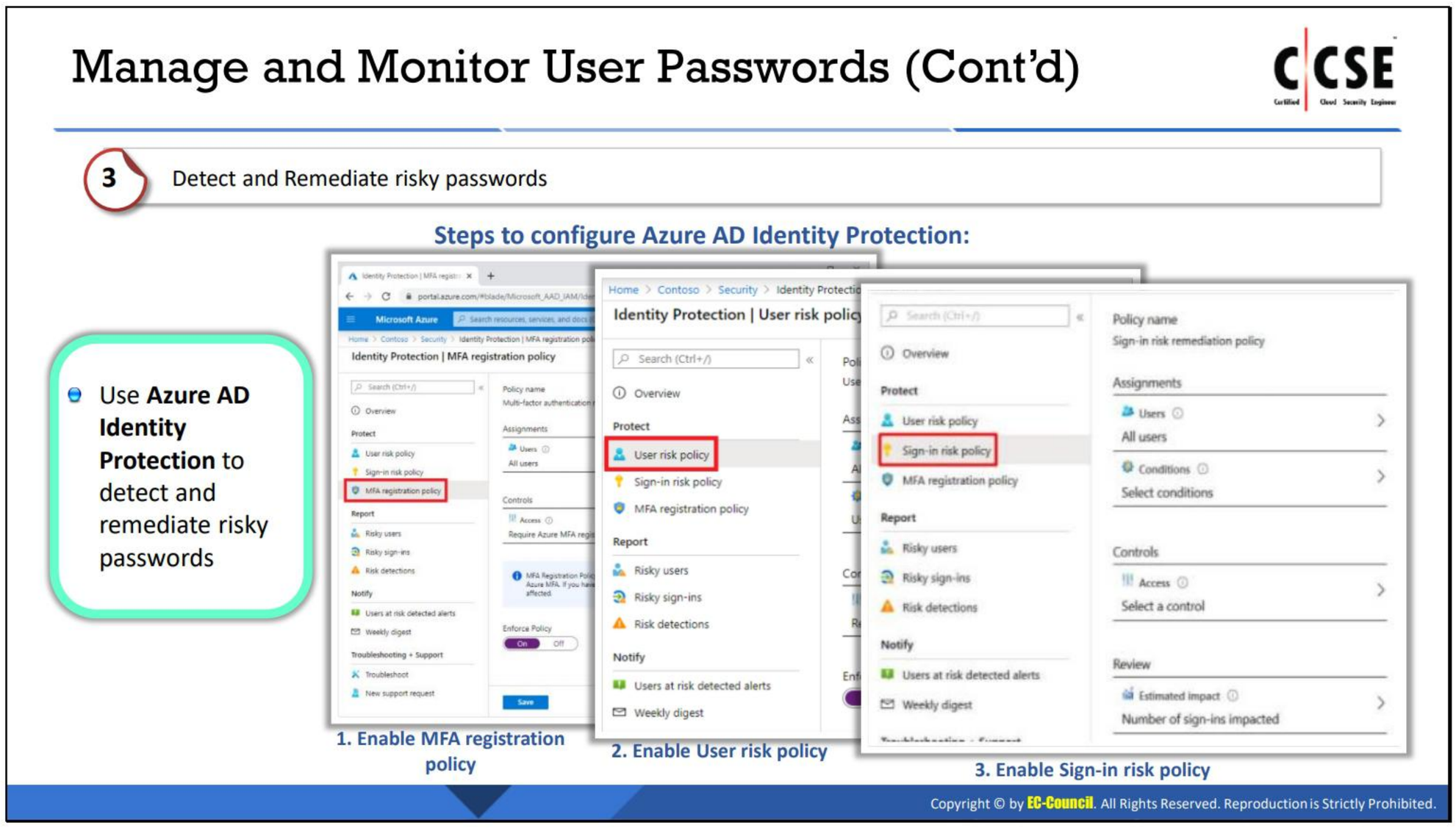


Figure 5.71: Reports

Every report has a list of findings or detections, which admins can access for a particular period (shown at the top of the report). Reports can be downloaded in.CSV or JSON format and columns can be added or deleted based on requirements. Admins can use the filters provided in the reports to find desired detections.

Additional entries may appear at the top of the report while selecting individual entries. These entries include confirm sign-in compromised, troubleshoot, confirm sign-in safe, etc. A details window opens up at the bottom when an entry is selected. It helps admins to investigate and take necessary actions on every detection.

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



Manage and Monitor User Passwords

Detect and Remediate Risky Passwords Automatically

Use **Azure AD Identity Protection** to

- Determine vulnerabilities that could affect the identities of an organization.
- Generate automated responses to the identified malicious actions of organizational identities.
- Examine the identified suspicious incidents and execute appropriate actions to solve them.

Steps to configure Azure AD Identity Protection

Source: https://www.microsoft.com

Three main policies are used in Identity Protection to protect users and respond to any suspicious activity. Enable these three policies to get maximum benefits from Identity Protection capabilities.

- **Enable MFA registration policy:**

  This policy helps in rolling out Azure MFA registration. MFA registration is required even if MFA is not enabled. Ensure that this policy is configured while using Identity Protection. This policy, when enabled, does not require users to perform MFA while signing in each time. It only confirms the registration status of a given user and requires them to preregister if necessary. This policy applies to users covered under this policy.

  - Log into the Azure portal and choose **Azure AD**.

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

- Select **Security**, **Identity protection,** followed by **MFA registration policy**.
- Choose **Select individuals and groups** or **All users** under **Assignments**.
- Under **Controls**, select the checkbox beside **Require Azure AD MFA registration**.
- Select **On** for **Enforce Policy** and click on **Save.**

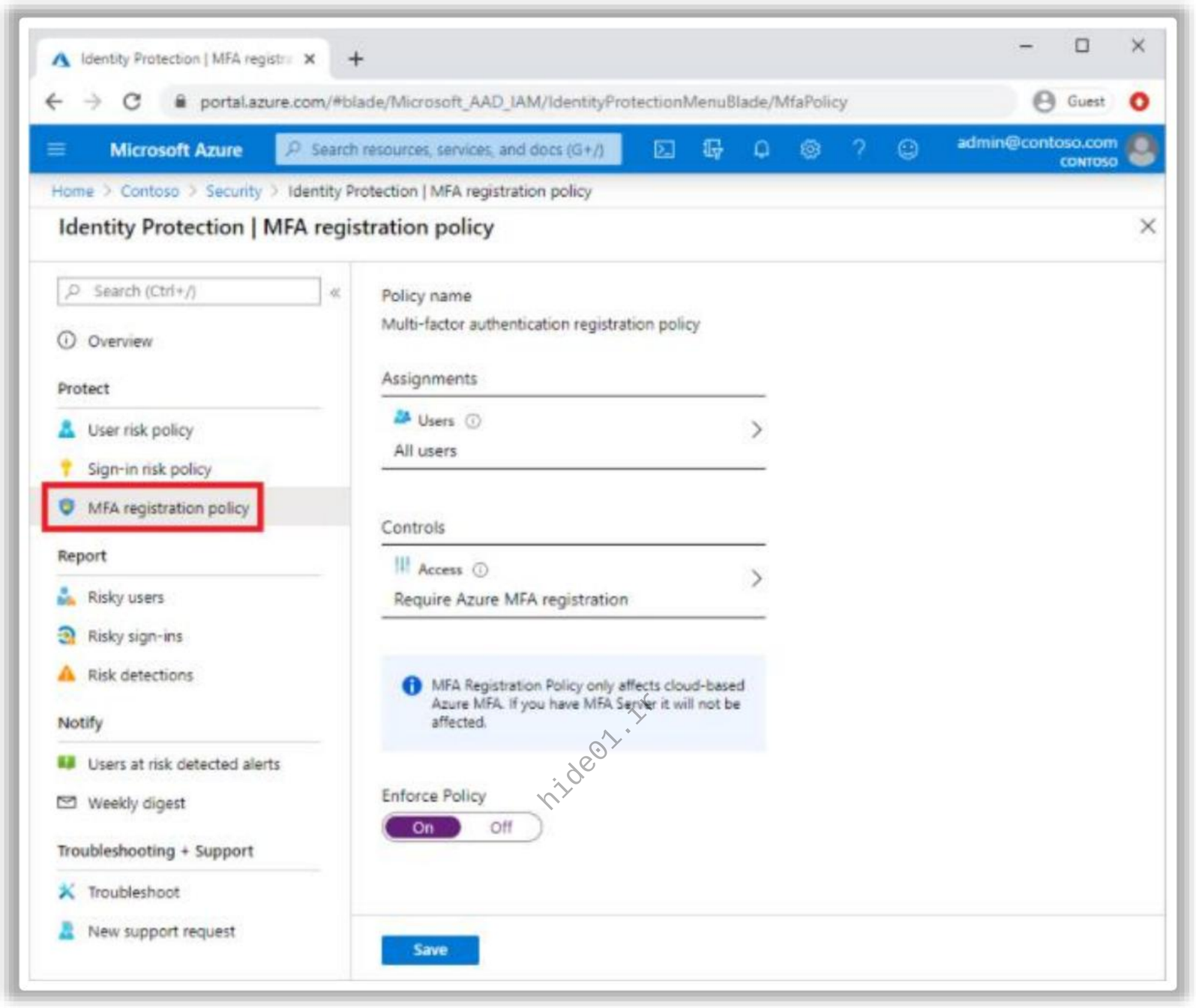


Figure 5.72: MFA Registration Policy

- **Enable User risk policy**

Use this policy to request a password change. When this policy is triggered, it asks a user to utilize MFA and change their password. Ensure that users are registered for MFA because this policy blocks users who are not registered for MFA from accessing their accounts. This policy affects users who are flagged as risky. Only the admin can unblock a user account if it gets blocked owing to this policy.

- Log into the Azure portal and choose **Azure AD**.
- Select **Security**, **Identity Protection,** followed by **User risk policy**.
- Choose **Select individuals and groups** or **All users** under **Assignments**. By default, the policy applies to all users.
- Under **Conditions**, select the suitable user risk level as **Medium and above.**
- Click on **Select** and then **Done**.

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

- Under **Access controls**, click on **Access** and select **Allow access** and **Require password change** options. Click on **Select**.
- Select **On** for **Enforce Policy** and click on **Save.**

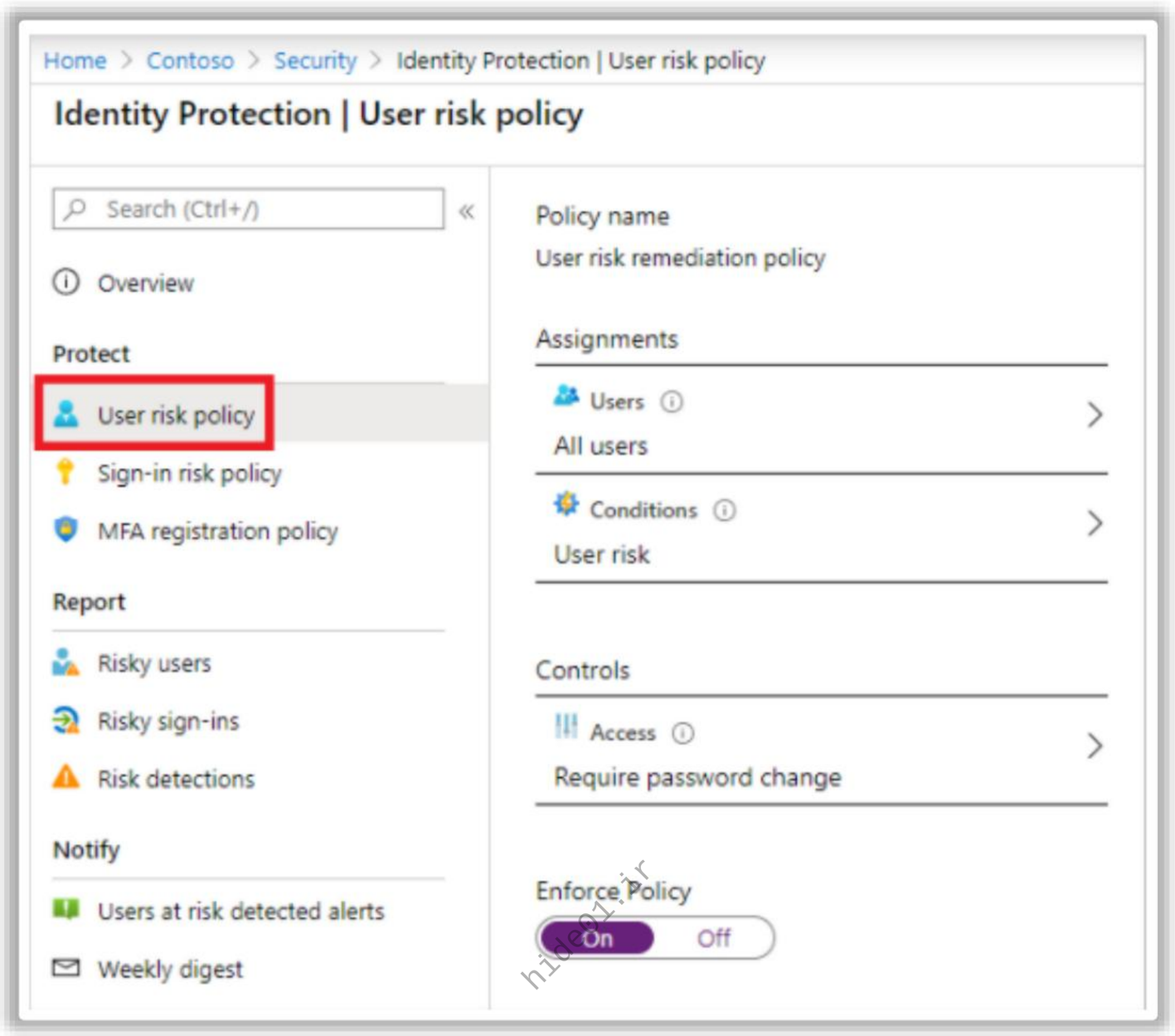


Figure 5.73: Enforce Policy

- **Enable Sign-in risk policy**

  Enforce sign-in risk policy for users whose behavior is suspicious. Ensure that users are already registered for Azure AD MFA because it is required to implement a sign-in risk policy. This policy blocks users who are not registered for MFA. The sign-in risk policy detects and responds to suspicious sign-in attempts by allowing users to verify their identity via Azure AD MFA. Enabling this policy makes it mandatory for users to leverage MFA before they access their accounts. This policy will affect users who are flagged as risky. Only an admin can unblock the account that is blocked due to this policy.

  - Log into the Azure portal as a global administrator and search for **Azure AD** and select it.
  - Select **Security**, followed by **Identity Protection** under the **Protect** menu.
  - Choose Sign-in risk policy on the left side of the menu.
  - The policy is applied to **All users** by default but can be changed to apply to only selected individuals or groups by going to **Assignments.**
  - Click on **Select conditions** under **Conditions** and then **Select a risk level**.

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

- Choose **Medium and above** and click on **Select**. Click on **Done**.
- For **Access controls**, select **Grant access** and **Require multi-factor authentication** under **Select the controls to be enforced**.
- Choose **On** for **Enforce Policy** and click on **Save**.

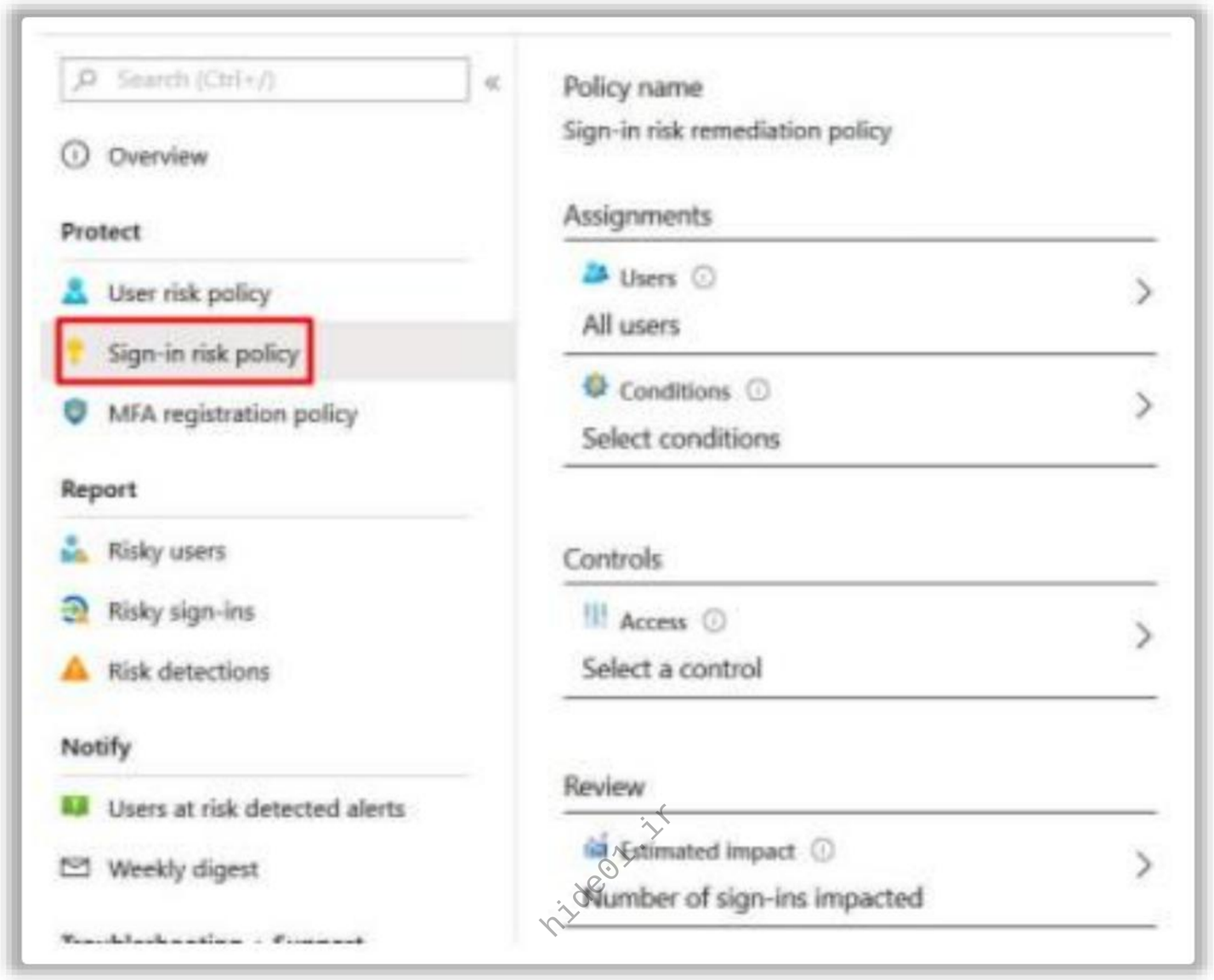
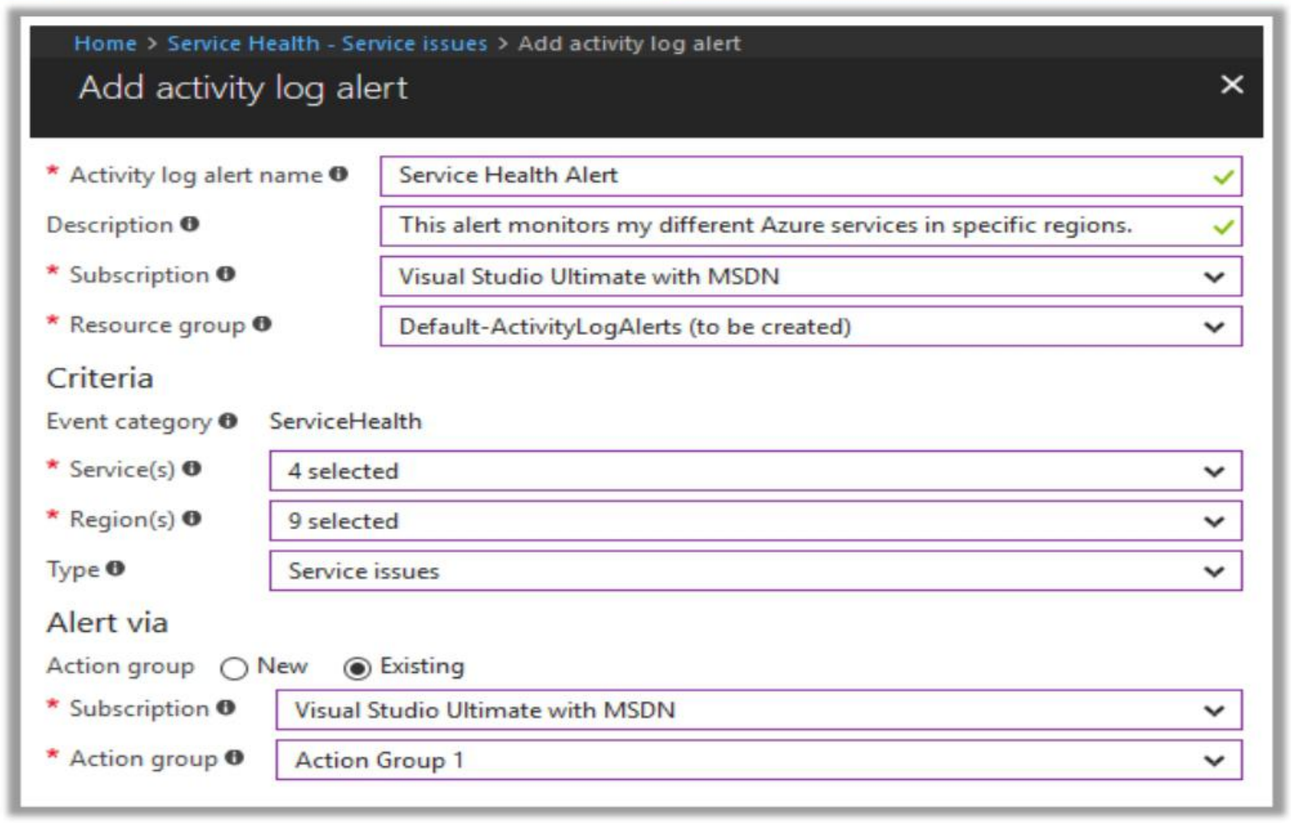


Figure 5.74: Sign-in Risk Policy

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

Configure Azure Service Health alerts to receive incident notifications

- Ensure that Azure incident notifications are received by the security operations team from Microsoft
- Use **Azure Service Health** to configure alerts to receive notifications when incidents occur.



Configure Azure Service Health alerts to get notified when service incidents occur

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

Configure Azure Service Health Alerts to Receive Incident Notifications

Ensure that the security operations team receives azure incident notifications from Microsoft. These incident notifications help the team know whether Azure resources are compromised, thus helping to respond and quickly remediate the potential risks.

Ensure that the Azure enrolment portal's admin contact details contain the required details (email address and phone number) to notify security operations. Cloud admins can select an alert type (email alert, SMS push alerts, or integrate alerts with their IT service management tools) based on their requirement. They can use Azure Service Health to configure alerts to get notified when service incidents occur.

Steps to create service incident alerts:

- If the personalized Azure Service Health map on the Azure portal shows issues with services, click on the map to obtain more information about the issue. After clicking on the issue, a personalized health dashboard appears with relevant information. Notify or warn your customers and engineering team about the potential impact of that service incident.

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

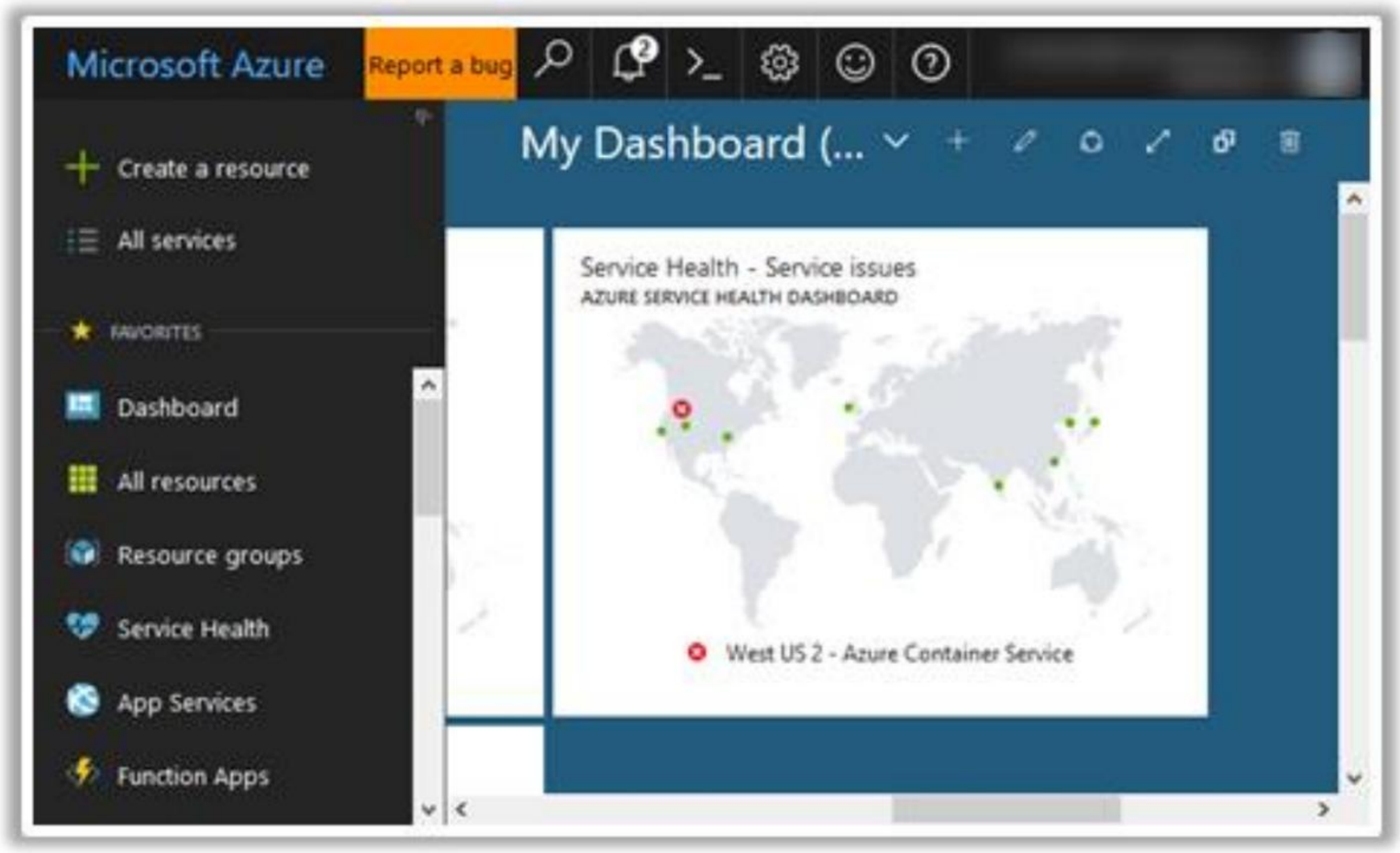


Figure 5.75: Dashboard

- Here, we noticed the health status passively by going to the portal, but a health alert can be created to notify us the next time such incidents occur. Based on the existing filters, create a new alert via a single click. Select **Create service health alert**.

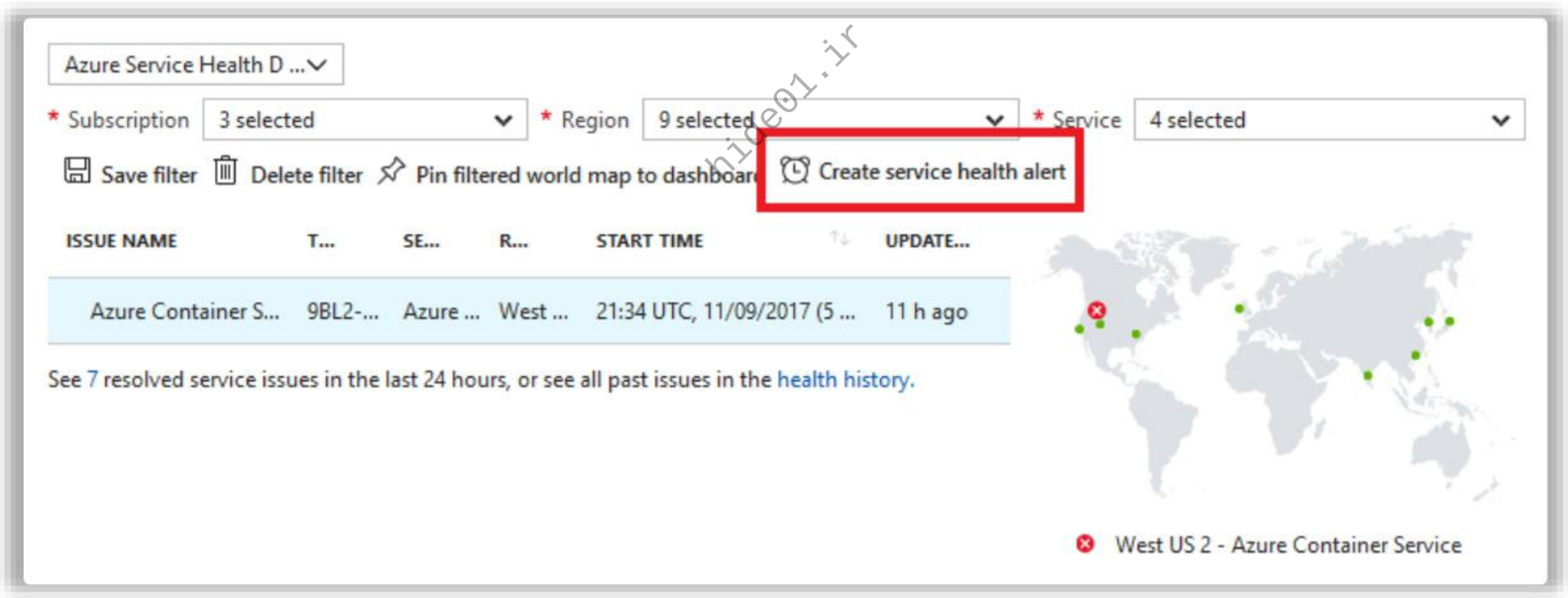


Figure 5.76: Create Service Health Alert

- A new window with existing filter settings will appear. Ensure that the settings are as expected and name the alert. Use the existing action group or create a new action group to notify when this alert is triggered.

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

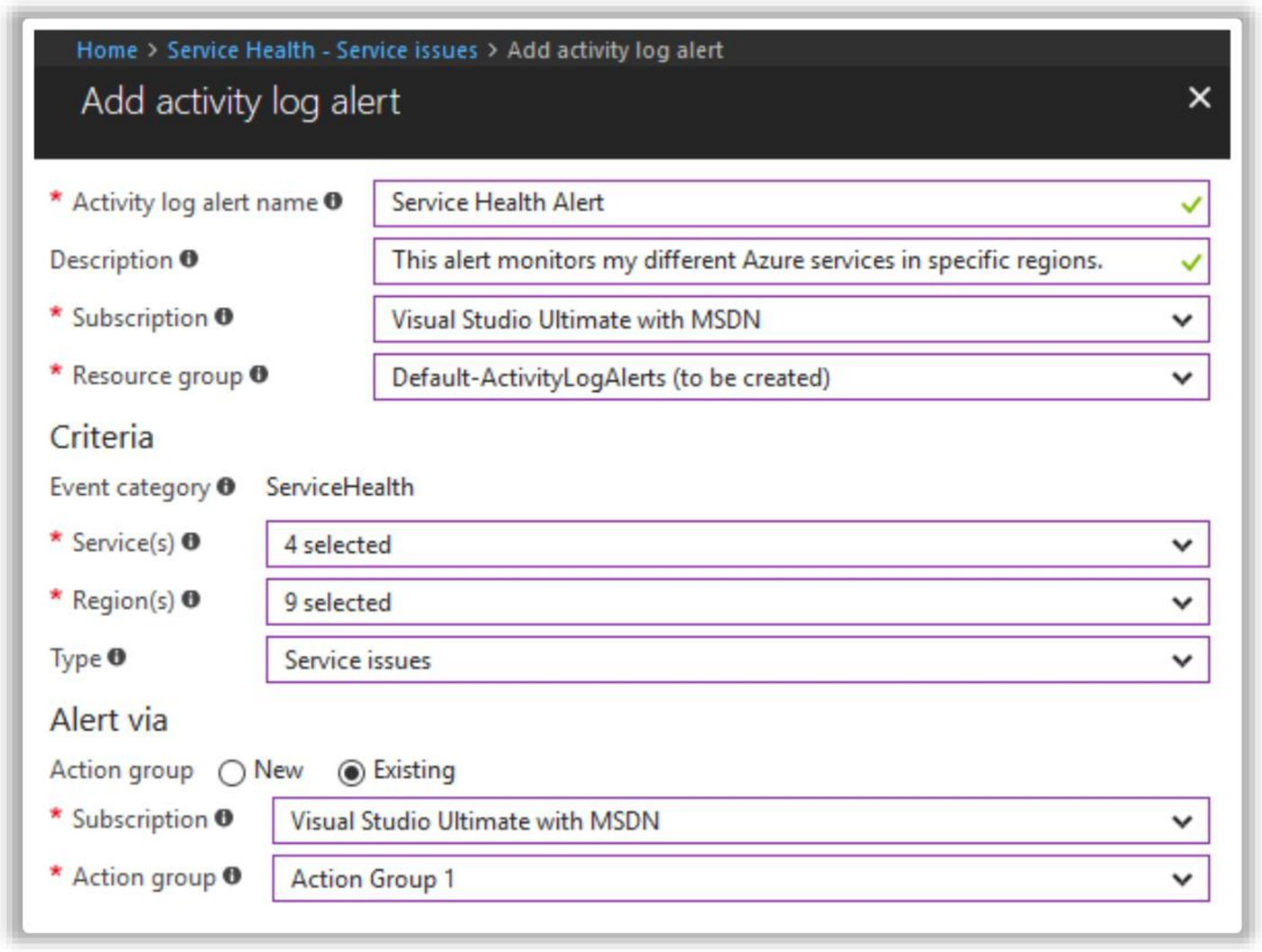


Figure 5.77: Add Activity Log Alert

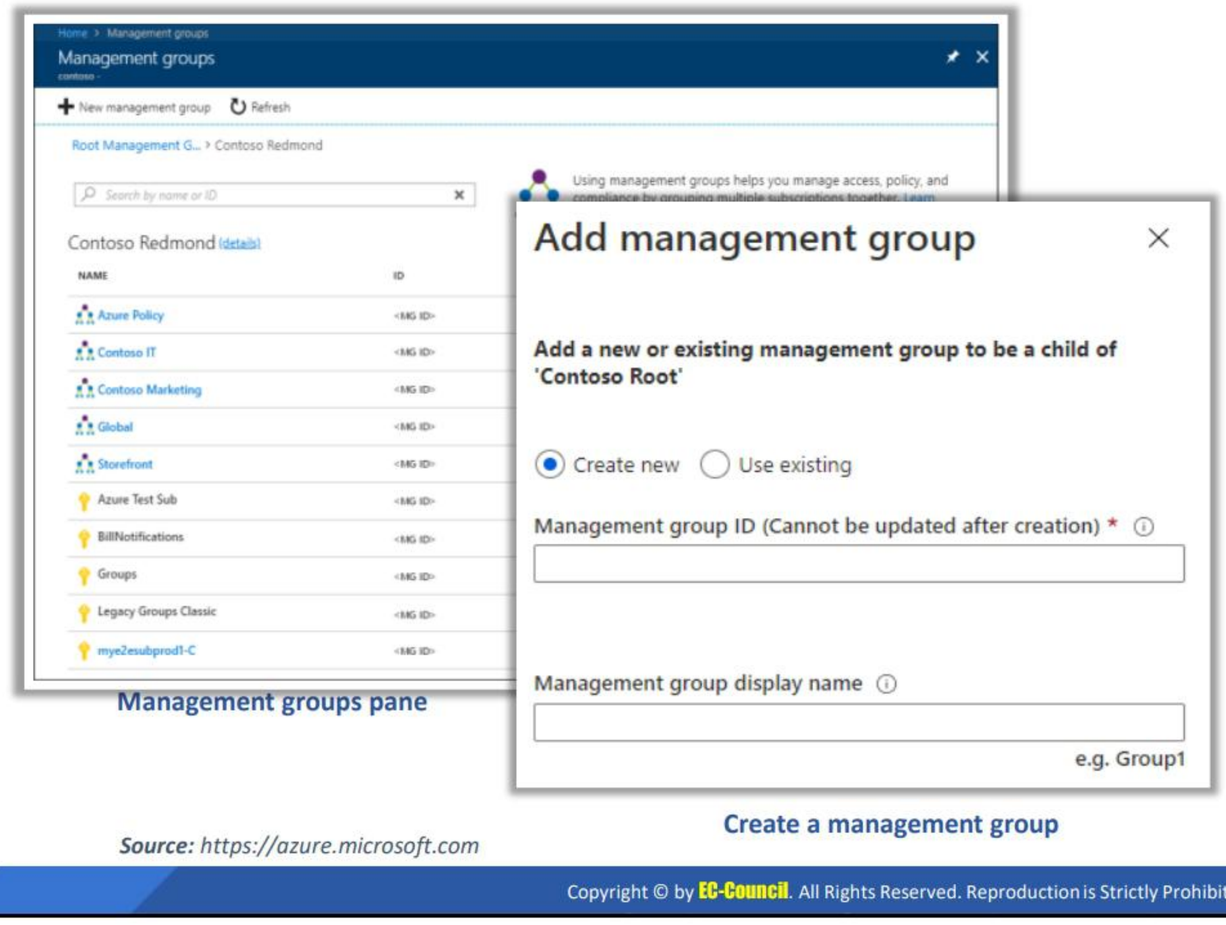
- Click on **OK.** You will be redirected to the dashboard and receive confirmation regarding new alert creation.

hide01.ir

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

Manage Subscriptions using Management Groups

- If the organization possesses multiple subscriptions, their policies, access, and compliance can be efficiently managed
- Use **Azure Management groups** to manage the multiple subscriptions of the organization



Management groups pane

Create a management group

Source: https://azure.microsoft.com

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

Manage Subscriptions Using Management Groups

If an organization possesses multiple subscriptions, it should manage the policies, access, and compliance for these subscriptions efficiently. Azure management groups can help in managing them. The organization can organize multiple subscriptions into containers, known as management groups, and apply its governance conditions. Conditions applied to a management group will automatically apply to all subscriptions under that group.

Management groups and subscriptions can be used to build a directory. The root management group is the top-level management group for every directory. This root management group has all management groups and subscriptions under it in a hierarchy. At the directory level, this root management group helps to enforce global policies and role assignments.

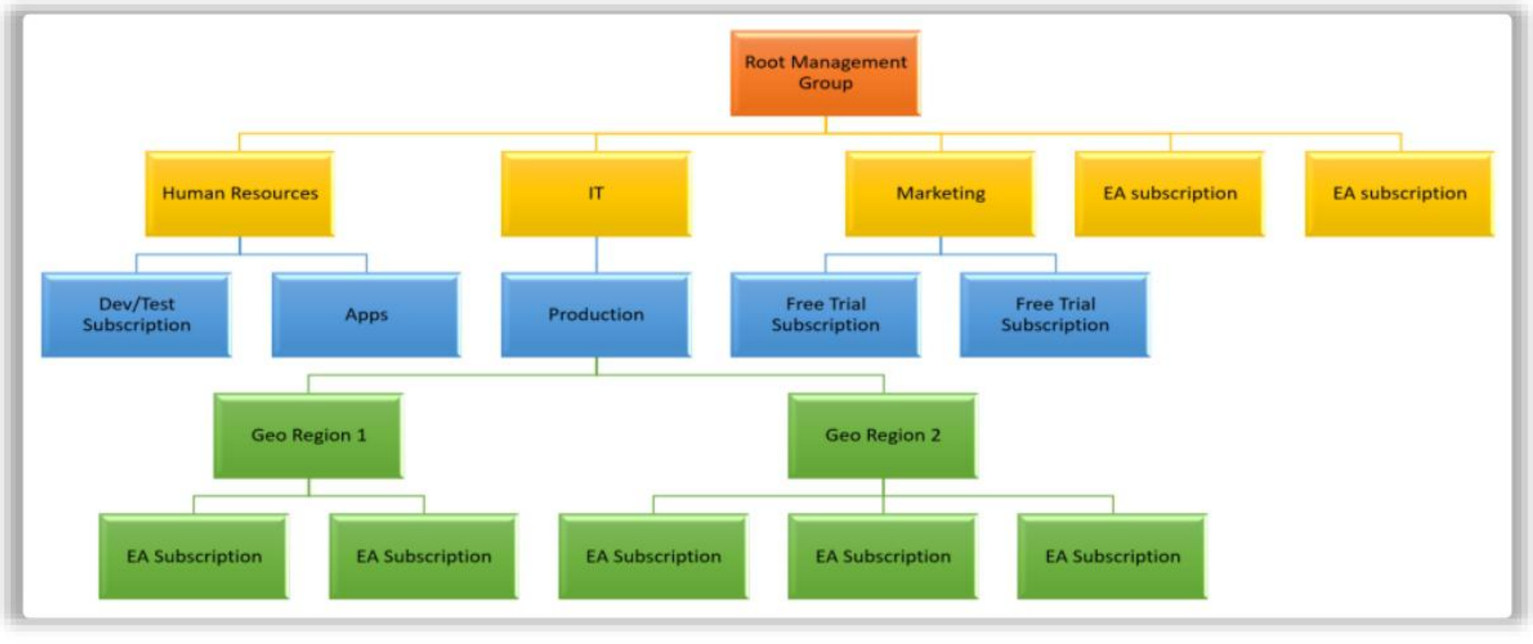


Figure 5.78: Azure Management Groups

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

Best practices for using management groups are as follows:

- **Ensure that all new subscriptions should have the necessary governance elements such as policies and permissions**

  Use the root management group for assigning organization-wide policies and permissions that are applicable to all Azure assets.

- **Top-level management groups should be arranged utilizing segmentation strategies to apply control and policy strategies to every segment**

  Under the root management group, create a single management group for every segment. Avoid creating multiple management groups under that root.

  Steps to create a management group:

  Source: https://www.microsoft.com

  - Log into the Azure portal and choose **All Services**.
  - Select **Management + governance** and click on **Management Groups.**
  - Select **+ Management group**.

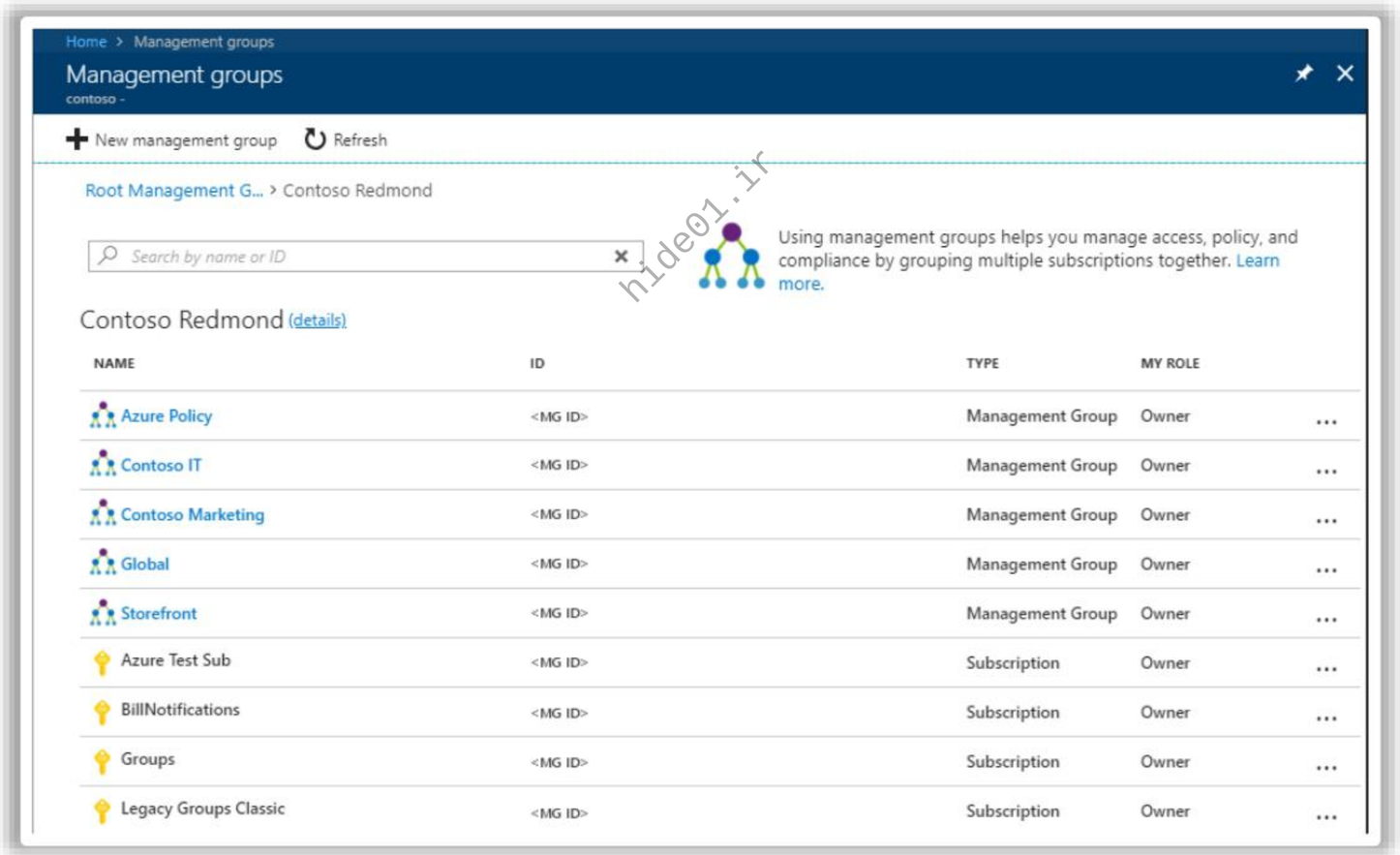


Figure 5.79: +Management Group

- Enter the management group ID (it is a unique directory identifier used to submit commands) and display name.

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

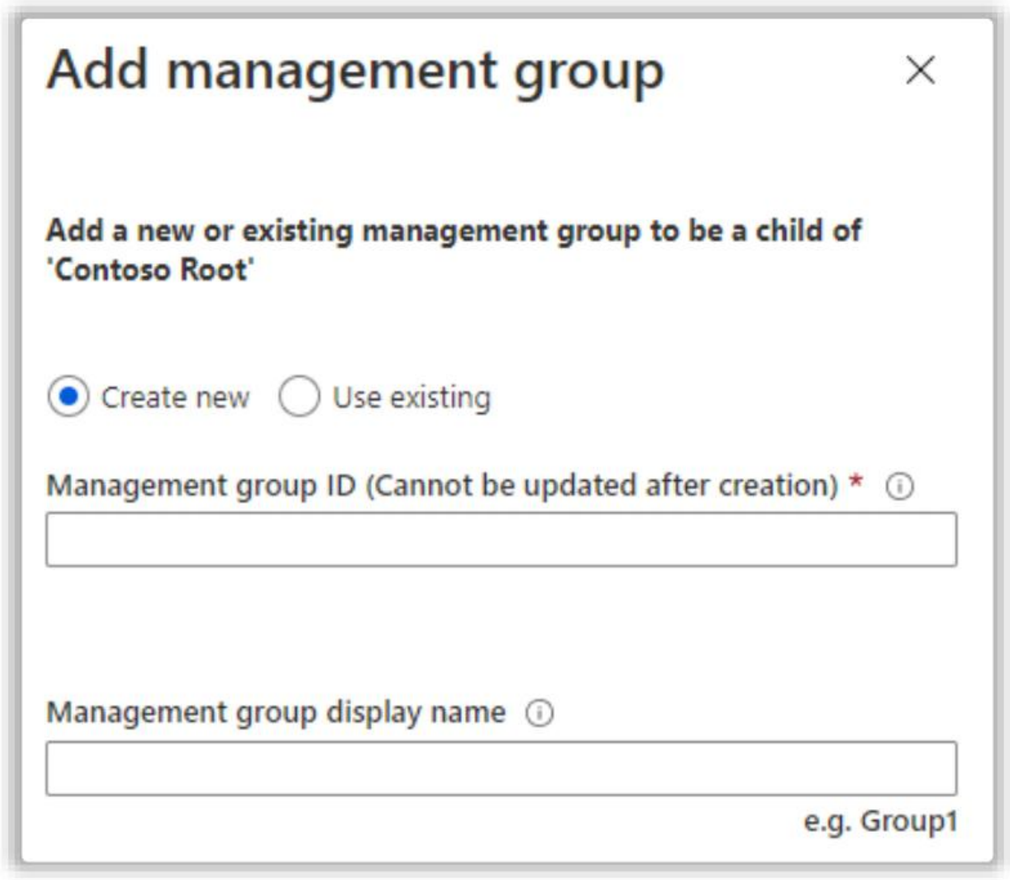


Figure 5.80: Add Management Group

- Click on **Save**.

- **Restrict management group depth to prevent confusion that can affect operations and security**

  Limit the overall hierarchy to three levels to avoid confusion. These hierarchy levels include the root management group along with subscriptions and management groups. Increasing the levels to more than three can create confusion, thereby directly affecting the operations and security.

- **Select the management group elements carefully that should be applied to the entire organization**

  To apply root management elements such as policies and permissions to every resource, there should be clarity in requirement with less impact.

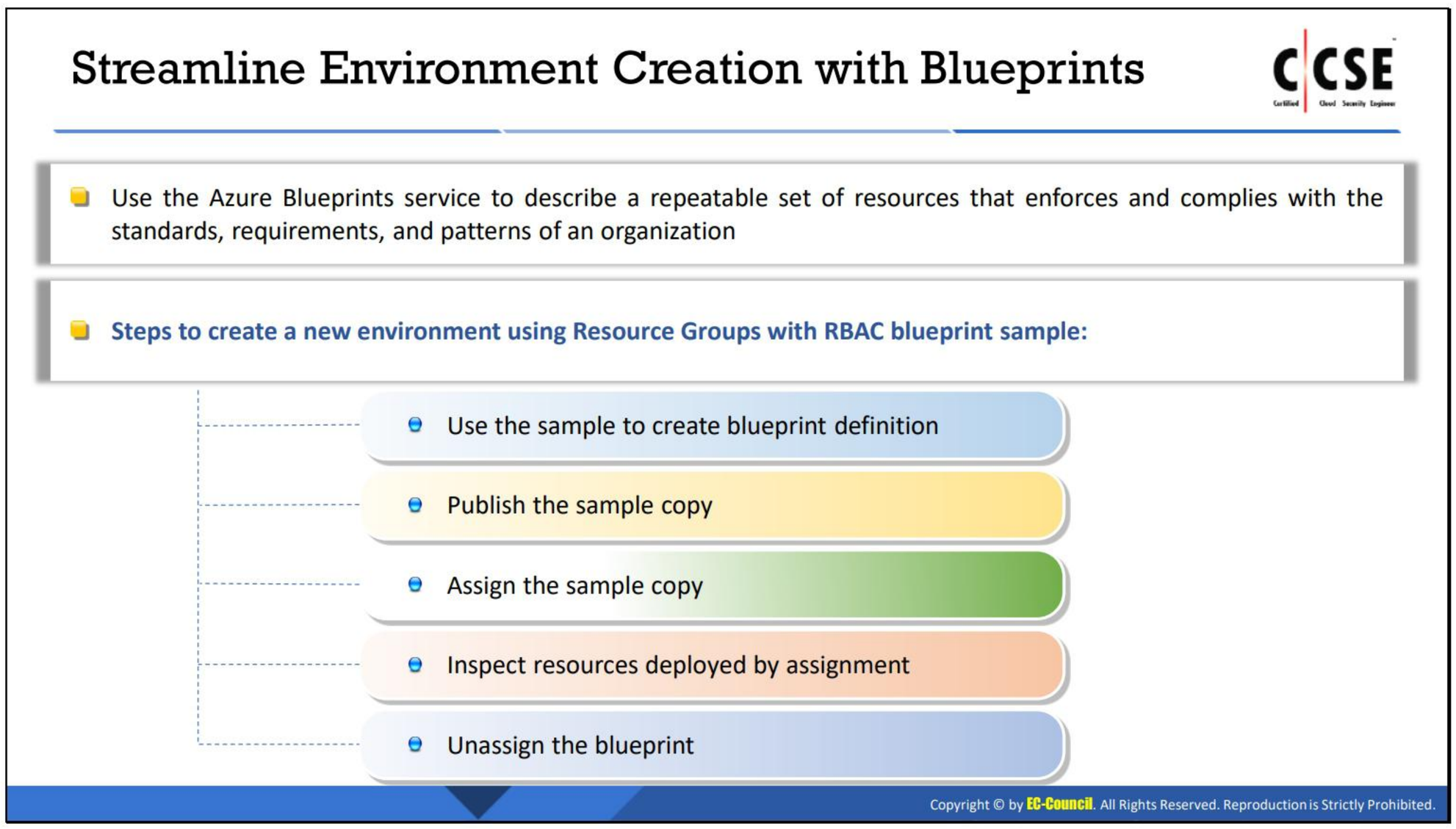
  This includes:

  - Regulatory requirements that can directly affect the business such as the restrictions and policies associated with data sovereignty.
  - Requirements that do not have any negative effect on operations such as a policy that affects audit and appropriately reviewed RBAC role assignments.

- **All organization-level changes on the root management group should be properly planned and tested before application**

  Organization-wide changes on the root group affect each resource present on Azure. Careful planning and testing of such changes are crucial before they are applied. These changes provide consistency across the organization when implemented correctly. However, when they are implemented incorrectly or with errors, they can negatively affect the production operations. Therefore, test all changes made to the root management group in a production pilot or test lab before they are applied.

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



Streamline Environment Creation with Blueprints

Use the Azure Blueprints service to build and run new environments rapidly. The Blueprints service helps IT groups and cloud architects in defining a repeatable set of resources that follows and adheres to the standards, requirements, and patterns of an organization. It ensures that the new environment is created within organizational compliance.

The deployment of different resource templates and artifacts can be orchestrated via Blueprints. These templates and artifacts include

- Role assignment
- Policy assignment
- Resource groups
- Azure ARM templates

Sample blueprints offer some examples of actions that can be performed using Azure Blueprints. They are samples with a specific purpose or intent, but they cannot create a complete environment. This example shows the creation of a new environment using Resource Groups with RBAC blueprint sample.

Steps to create an environment from a sample blueprint

Source: https://www.microsoft.com

- **Use sample to create blueprint definition:** Implement the sample blueprint. Create a new blueprint in the environment (based on the blueprint sample) via importing.
    - Choose **Select All** and search for **Blueprints** and select it.

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

- On the **Getting started** page, click on **Create** under **Create a blueprint**.
- Under **Other samples**, select **Resource Groups with RBAC**
- Fill out the **Basics** of the sample: **Blueprint name** (e.g., **two-rgs-with-role-assignments**) and **definition location** (choose the management group or subscription using ellipsis where the sample copy will be saved).
- Choose Next: Artifacts and review the artifact list that makes up the sample. Two resource groups (**ProdRG** and **PreProdRG**) are defined in the sample, whose final name and location are set during blueprint assignment. The **Contributor** role is assigned to **ProdRG,** whereas the **Owner and Readers** roles are assigned to PreProdRG.
- Click on **Save Draft** after reviewing the sample to create a copy of the sample in the selected subscription or management group.
- Move to the next step (publish the sample copy) after receiving the notification "**Saving blueprint definition succeeded**."

- **Publish the sample copy**: The sample copy is created in the environment in the draft mode. It should be published so that it can be assigned and deployed later. This copy is customizable. Follow the steps given below to publish the sample copy:
  - Choose **Select All,** search for **Blueprints,** and select it.
  - Go to the **Blueprint definitions** page and search for blueprint definition (**two-rgs-with-role-assignments**) using filters to select it.
  - Click on **Publish blueprint**. Enter the **version** as 1.0 in the new pane for the sample copy. After providing **Change notes**, click on Publish.

  Changes can be made after publishing but with different versions to track differences between various versions of the same blueprint definition. Move to the next step once the notification "**Publishing blueprint definition succeeded**" appears.

- **Assign the sample copy**: After publishing the sample copy, the sample copy can be assigned to a subscription inside a management group where it was saved. Follow the steps below to assign the sample copy.
  - Choose **Select All** and search for **Blueprints** and select it.
  - Go to the **Blueprint definitions** page and search for blueprint definition (**two-rgs-with-role-assignments**) using filters to select it.
  - On the **blueprint definition** page, click on **Assign blueprint**.
  - Enter the parameter values for the assignment:

    Basics

    - **Subscription**- Select the subscription where the sample copy is saved.

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

- **Assignment name**- Name is automatically taken according to the blueprint definition name.
- **Location**- Select a region where the managed identity has to be created.
- **Blueprint definition version**- Select **version 1.0** of the sample blueprint definition copy.
- **Lock Assignment**: Select **Read-Only.**
- **Managed Identity**: Keep the default **System assigned** option.
- **Artifact parameters**: Select an appropriate value.

  - Choose **Assign** after entering all parameters.

Assigning the sample copy deploys the specified resources and configures the Lock Assignment selected. It may take up to 30 min to apply blueprint locks. Move to the next step once the notification "Assigning blueprint definition succeeded" appears.

- **Inspect resources deployed by assignment:** The artifacts defined in the definition are created and tracked by blueprint assignment. The status of resources can be viewed on the blueprint assignment page or by directly viewing the resources.

  - Choose **Select All,** search for **Blueprints,** and select it.
  - Go to the **Assigned blueprints** page; search and select **Assignment-two-rgs-with-role-assignments.**
  - Choose the **ProductionRG** resource group.
  - Go to the **Access control (IAM)** page and click on **Role assignments**. This tab shows that the **Contributor** role is assigned to the account and the **Owner** role has been assigned to the **Assignment-two-rgs-with-role-assignments** blueprint assignment.
  - To go back one page, click on **Assignment-two-rgs-with-role-assignments** from the Azure portal breadcrumb. Select the resource group "**PreProductionRG."**
  - Go to the **Access control (IAM)** page and click on the **Role assignments** tab. We can see here that the account is granted **Owner and Reader** roles.
  - Click on the **Deny assignment** tab. Deny assignment prevents users on the **Role assignment** page from taking particular actions by enforcing **Read Only** blueprint lock mode.
  - Select the deny assignment and click on the **Denied permissions** page.
  - Choose **PreProductionRG - Access Control (IAM)** from the Azure portal breadcrumb. Go to the **Overview** page and click on **Delete resource group**. Confirm deletion by entering **PreProductionRG** and selecting **Delete**.

A notification **"Delete resource group PreProductionRG failed**" appears, which implies that the Read-Only blueprint lock mode is successfully preventing accounts with

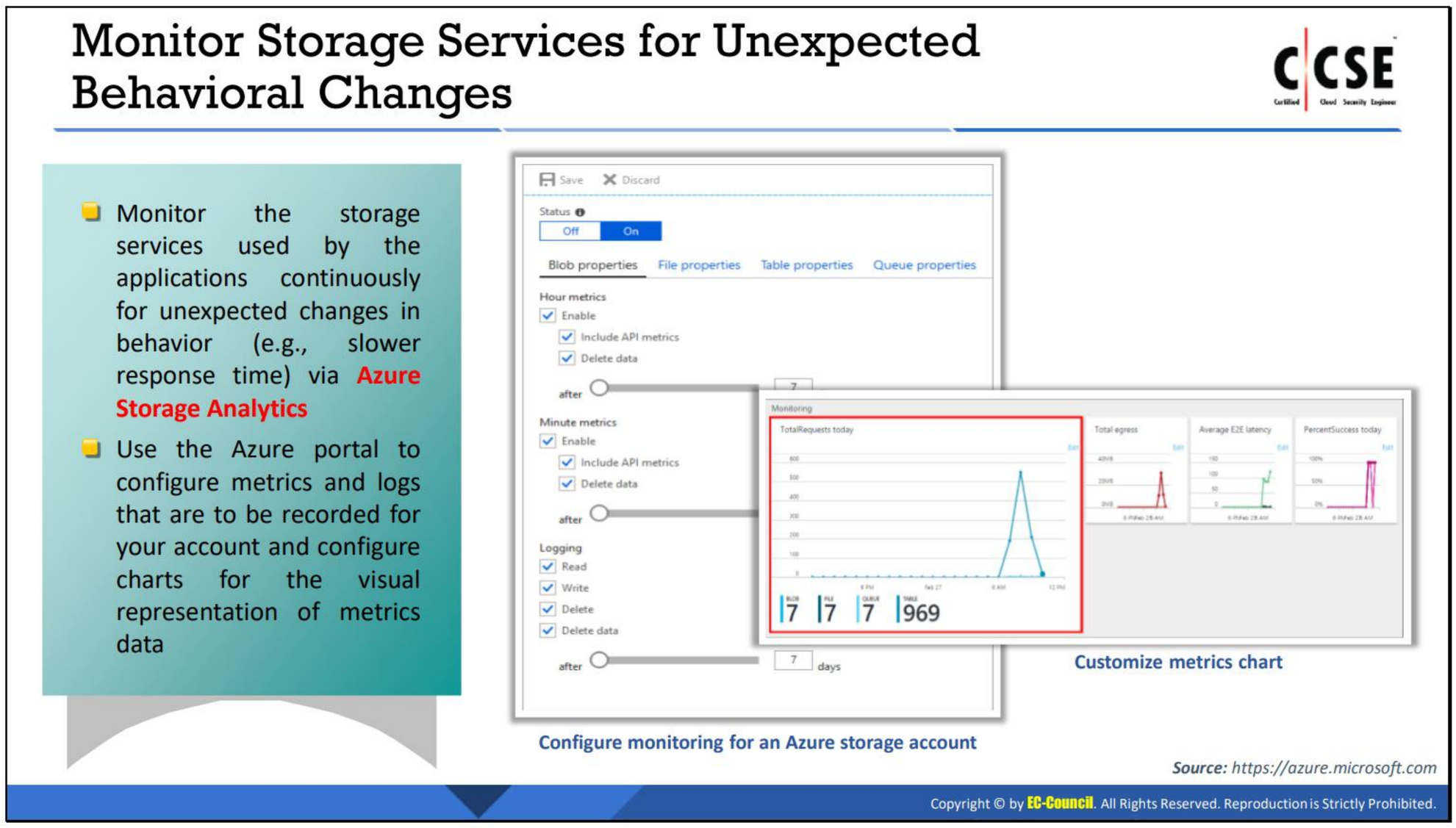
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

permission (even Owner) from deleting the resource group because this lock mode was applied during blueprint assignment.

- **Unassign the blueprint**: Remove the assignment of blueprint and the deployed resources. Follow the given steps::
  - Choose **Select All,** search for **Blueprints,** and select it.
  - Go to the **Assigned blueprints** page; search and select **Assignment-two-rgs-with-role-assignments.**
  - Choose **Unassign blueprint** and confirm by clicking on **OK**. This removes the blueprint and blueprint locks, implying that the created resources can be deleted by accounts with permissions.
  - From the Azure menu, choose **Resource groups** and select **ProductionRG.**
  - Go to the **Access control (IAM)** page and click on the **Role assignments** tab. Here, we can see that blueprint assignment does not possess the Owner role, but resource groups still have the deployed role assignments.
  - After blueprint assignment is removed, a notification "**Removing blueprint assignment succeeded**" appears.

hide01.ir

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



Monitor Storage Services for Unexpected Behavioral Changes

Monitor the storage services used by the applications continuously for unexpected changes in behavior (e.g., slower response times) via **Azure Storage Analytics**. Use logging to gather detailed information and analyze an issue in depth. Use the information collected through logging and monitoring to identify the root cause of the issue faced by an application. This will further help in taking appropriate steps to remediate the cause or issue.

For an Azure storage account, use Azure Storage Analytics to perform logging and offer metrics data. Cloud admins can use the information derived from Storage Analytics to **trace security requests**, **know usage trends**, and **detect issues with their storage accounts**. Azure Storage Analytics offers metrics (for storage services) and logs (for tables, queues, and blobs).

Use the Azure portal to configure metrics and logs that are to be recorded for your account and configure charts for the visual representation of metrics data.

Source: https://www.microsoft.com

Steps to configure monitoring for an Azure storage account:

- On the Azure portal, choose **Storage accounts,** followed by the name of the storage account.
- On the account dashboard, select **Diagnosis** under the **MONITORING** section.

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

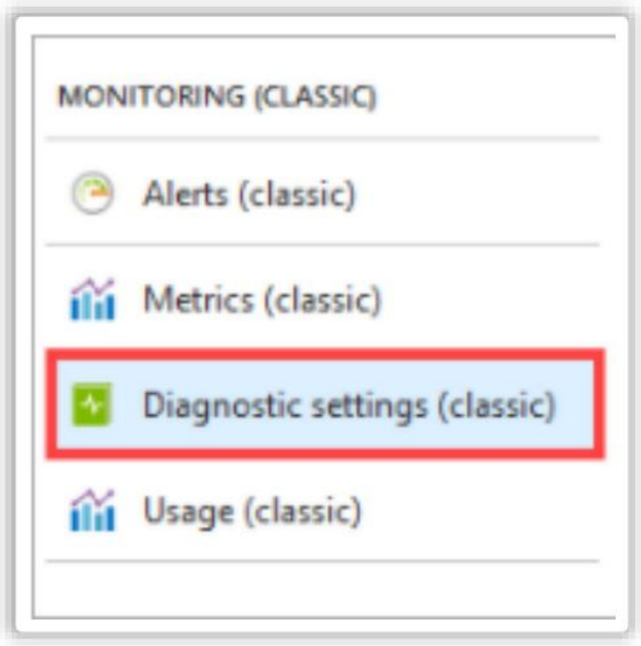


Figure 5.81: Diagnostic Settings

- Select the **type** of metrics data for each service that must be monitored and select the **retention policy** for these data. Set the retention policy using the slider or entering the number of days (from 1 to 365 days). The default retention days are seven for a new storage account.

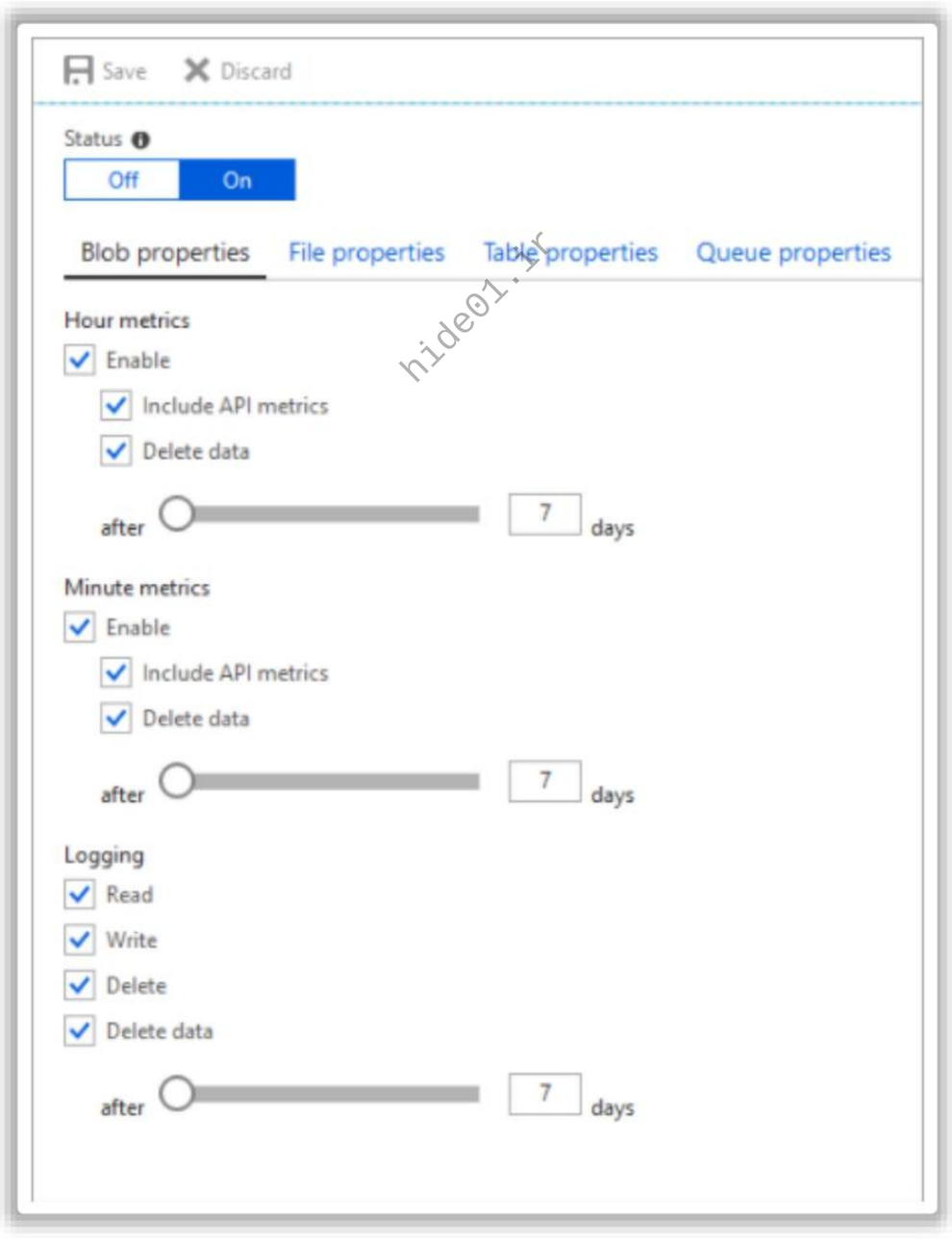


Figure 5.82: Blob Properties

- Click on **Save** after completing the monitoring configuration.

  On the storage account blade and individual service blades, a default set of metrics appears in charts. To customize or configure the metrics that should be displayed in the

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

chart, click **Edit** on any metric chart. By selecting **Off** for **Status**, metrics collection and logging can be disabled.

Steps to customize metrics chart

To select the metrics to be displayed on the chart, follow the procedure given below:

- Go to the storage account blade or metrics blade for individual services to see the chart.

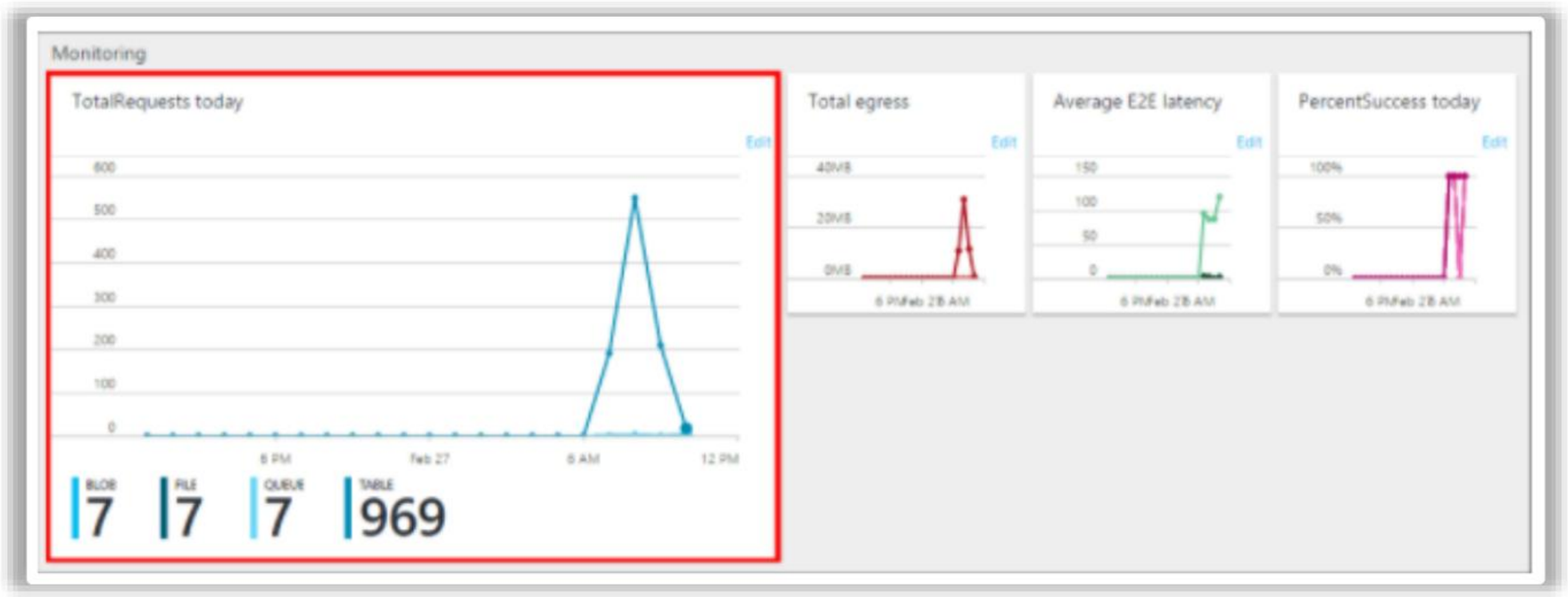


Figure 5.83: Monitoring

- To edit the chart, click anywhere on it.
- Choose the service whose metrics have to be displayed and the **Time range** of the metrics.

hide01.ir

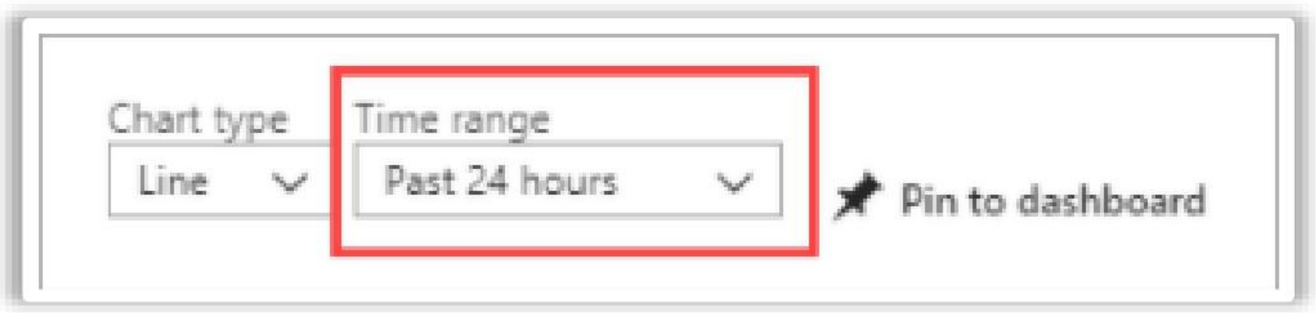


Figure 5.84: Time Range

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

- Select the individual **metrics** to be displayed in the chart and click **OK.**

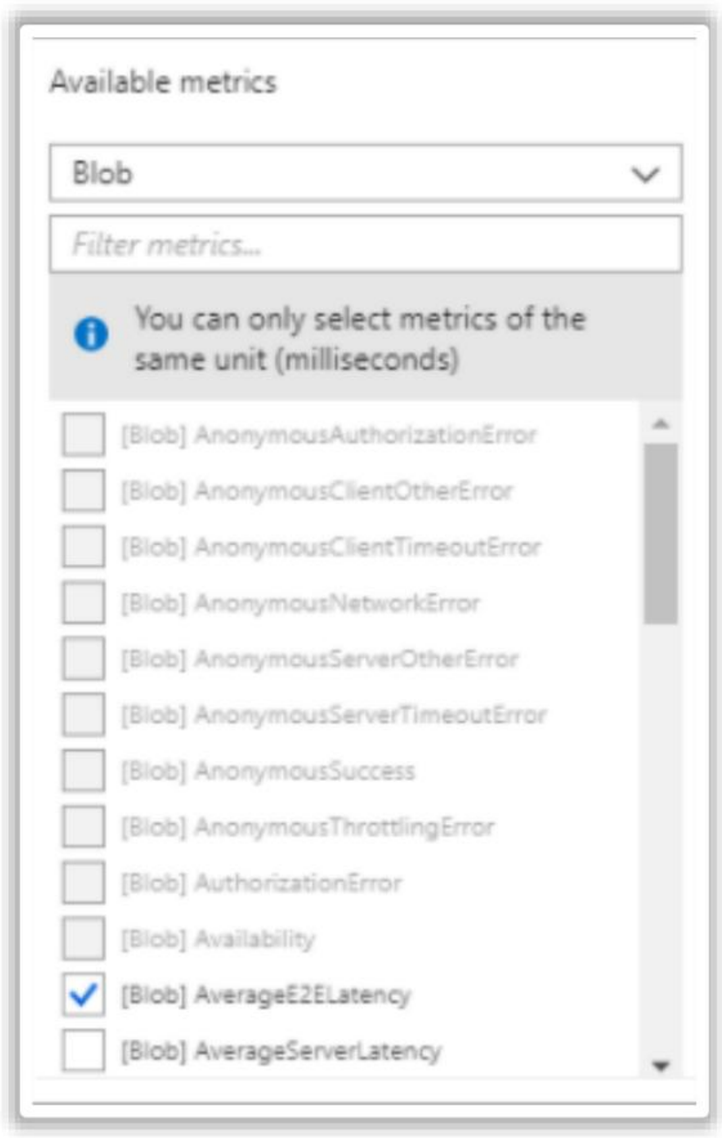


Figure 5.85: Select Metrics

hide01.ir

Steps to configure metrics alerts:

- Go to the **Alert rules** blade and move to the **MONITORING** section. Choose **Alerts (classic).**
- Choose **Add metric alert (classic)**. Provide a **Name** and **Description** for the new alert.
- Choose the **Metric** for which an alert is being configured, an alert **Condition**, and **Threshold.**

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

- Choose the **Period**. An alert is triggered whenever the metrics reach or exceed the threshold.

Figure 5.86: Alert

- Configure **Webhook** and **Email** notifications (optional).

Steps to add metrics charts to the dashboard:

- On the dashboard, click on **Edit dashboard**.
- Under the **Tile Gallery,** select options as shown below.
    - **Find titles by**- Type
    - **Type**- Storage accounts

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

- **Resources**- Select the storage account whose metrics should be added to the dashboard
- Drag-and-drop the tile on the dashboard

Figure 5.87: Tile Gallery

- After adding charts, click on **Done customizing** on the dashboard.

Steps to configure logging

- On the Azure portal, choose **Storage accounts**, followed by the name of the storage account.
- On the account dashboard, click on **Diagnosis settings** under the **MONITORING** section.

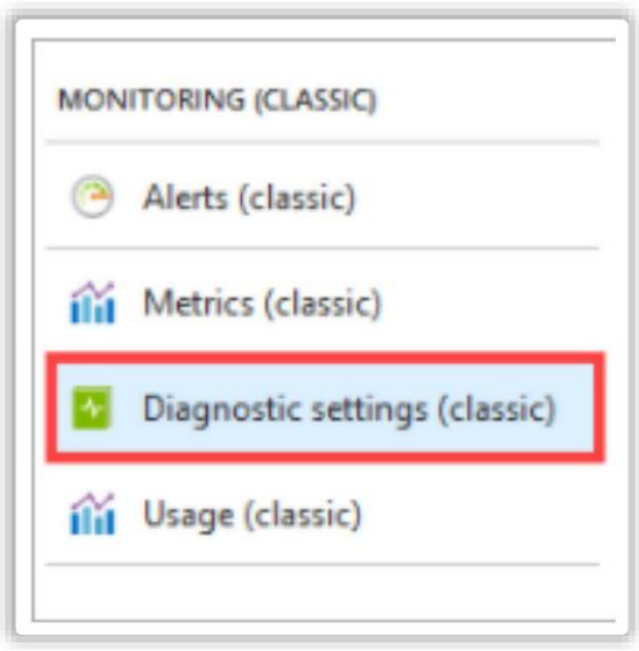


Figure 5.88: Diagnosis Settings

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

- Set the **Status** as **On** and choose the services for which logging has to be enabled.

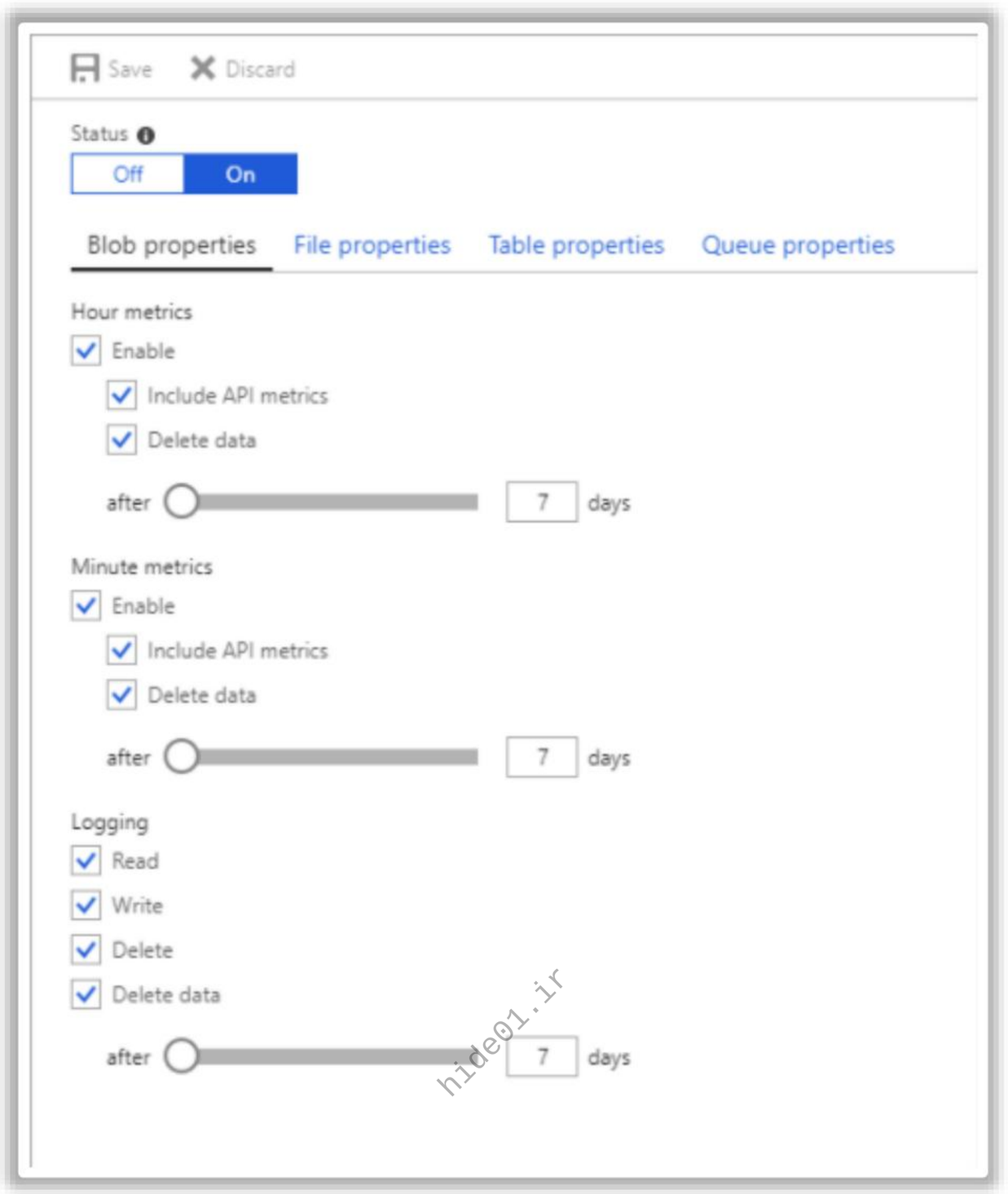


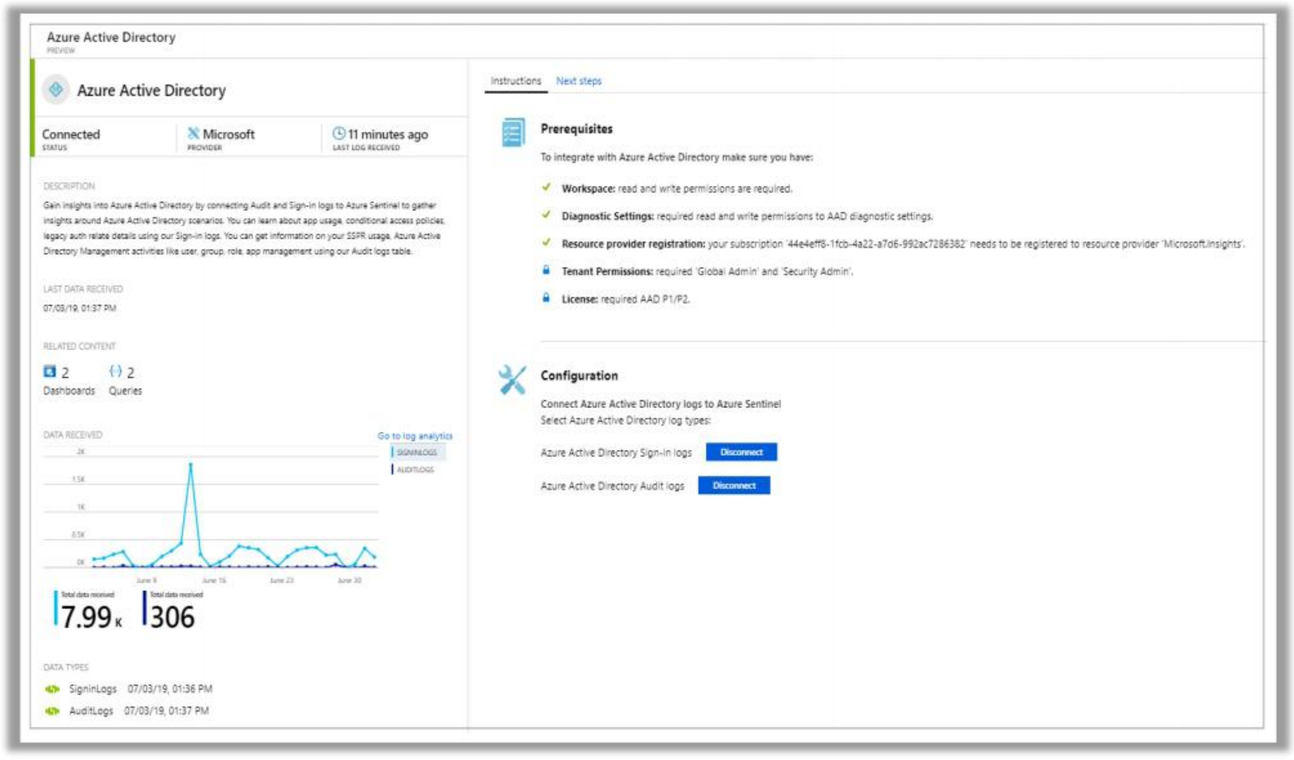
Figure 5.89: Status

- Click on **Save.**

The diagnostic logs are stored inside your storage account in a blob container ($logs) that can be accessed via storage explorers (such as Azure Storage Explorer), storage client library, or PowerShell.

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

Prevent, Detect, and Respond to Threats using Azure Sentinel



Selecting the types of logs (audit logs or sign-in logs) to be delivered to Sentinel

- **Use a cloud-based SIEM (Azure Sentinel) to improve the speed and scalability of your SIEM solution:**
  - Cloud admins need to enable Sentinel and connect all data sources to Sentinel to start using it

Source: https://azure.microsoft.com

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

Prevent, Detect, and Respond to Threats Using Azure Sentinel

To prevent, detect, and respond to threats in Azure, **utilize a cloud-based SIEM to enhance the performance and scalability of the on-premises SIEM solution:**

Consider using cloud-based SIEM (Azure Sentinel) to improve the speed and scalability of your SIEM solution if it meets the requirements of your organizational SIEM solution. Azure Sentinel is a cloud-based SIEM and SOAR solution that provides threat intelligence and intelligent security analytics throughout an organization. It serves as a single solution for proactive hunting, alert detection, threat visibility, and threat response.

Cloud admins must enable Sentinel and connect all data sources to Sentinel to start using it.

Steps to enable Azure Sentinel

- Log into the Azure portal and select the subscription that has Sentinel.
- Search for **Sentinel** and select it.

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

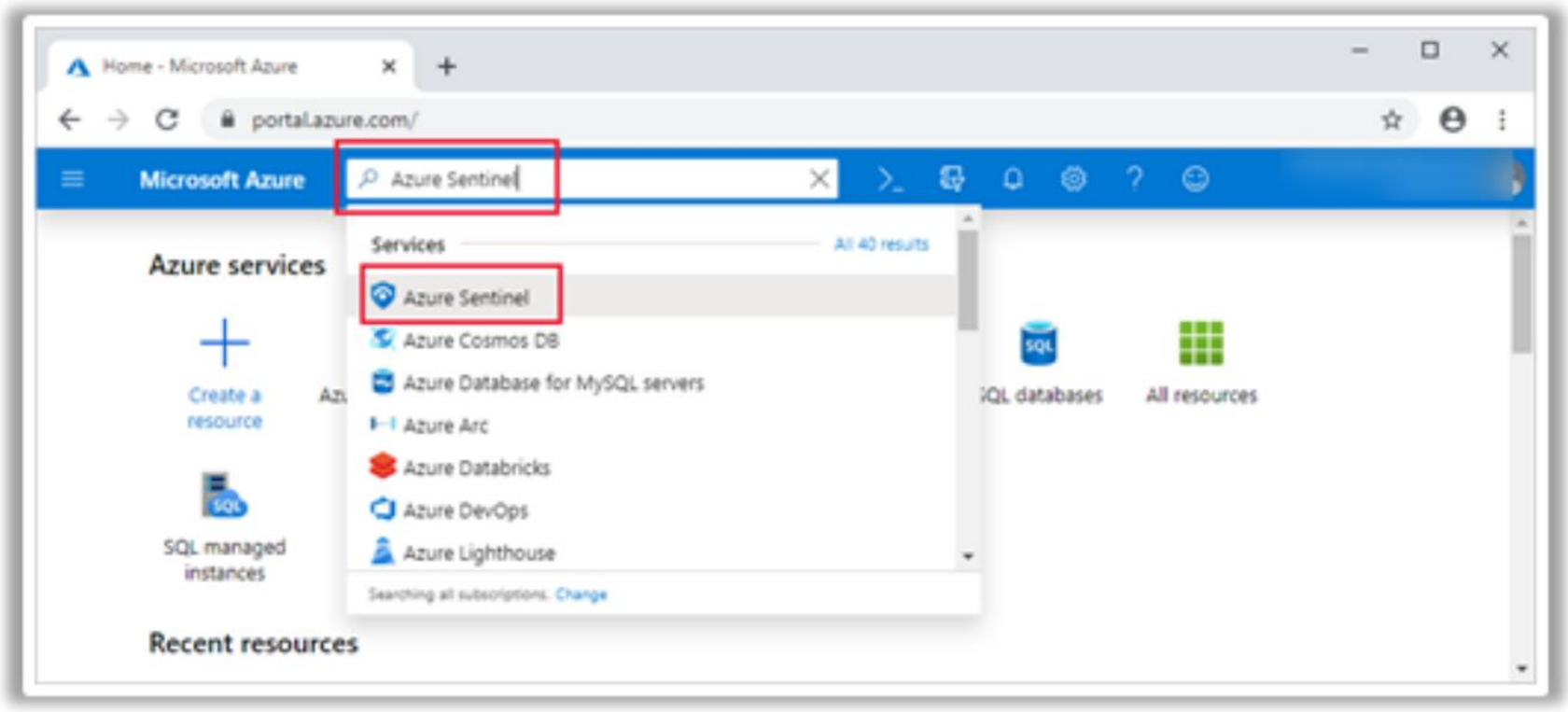


Figure 5.90: Select Azure Sentinel

- Click on **Add** and select an existing workspace or create a new one.

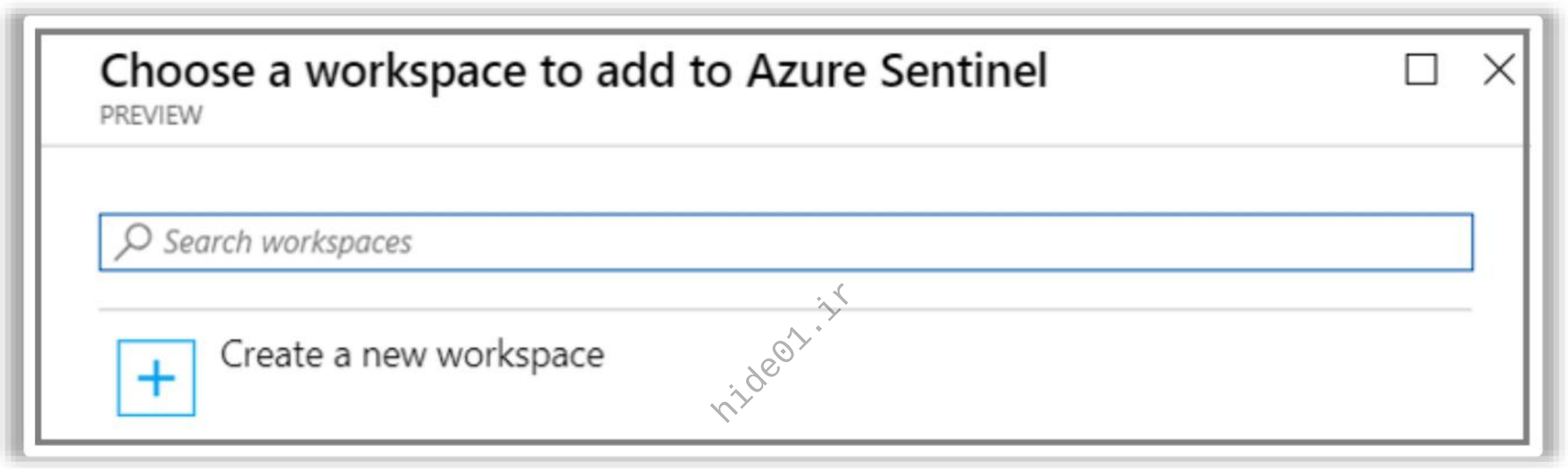


Figure 5.91: Add Workspace

- Choose **Add Azure Sentinel.**

Connecting data sources: Data are forwarded to Azure Sentinel from multiple apps and services. Install Log Analytics agents on VMs and physical machines to collect logs and events and send them to Sentinel. Install the Logs Analytics agent on Linux Syslog server for firewall and proxies so that the agent sends the log files to Sentinel. Follow the steps given below to connect data sources with Sentinel.

- Select **Data connectors** from the **main menu**.

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

- In the **data connectors gallery**, select a data source, followed by the **Open connector** page. The data connector gallery has all data sources that can be connected to Sentinel.

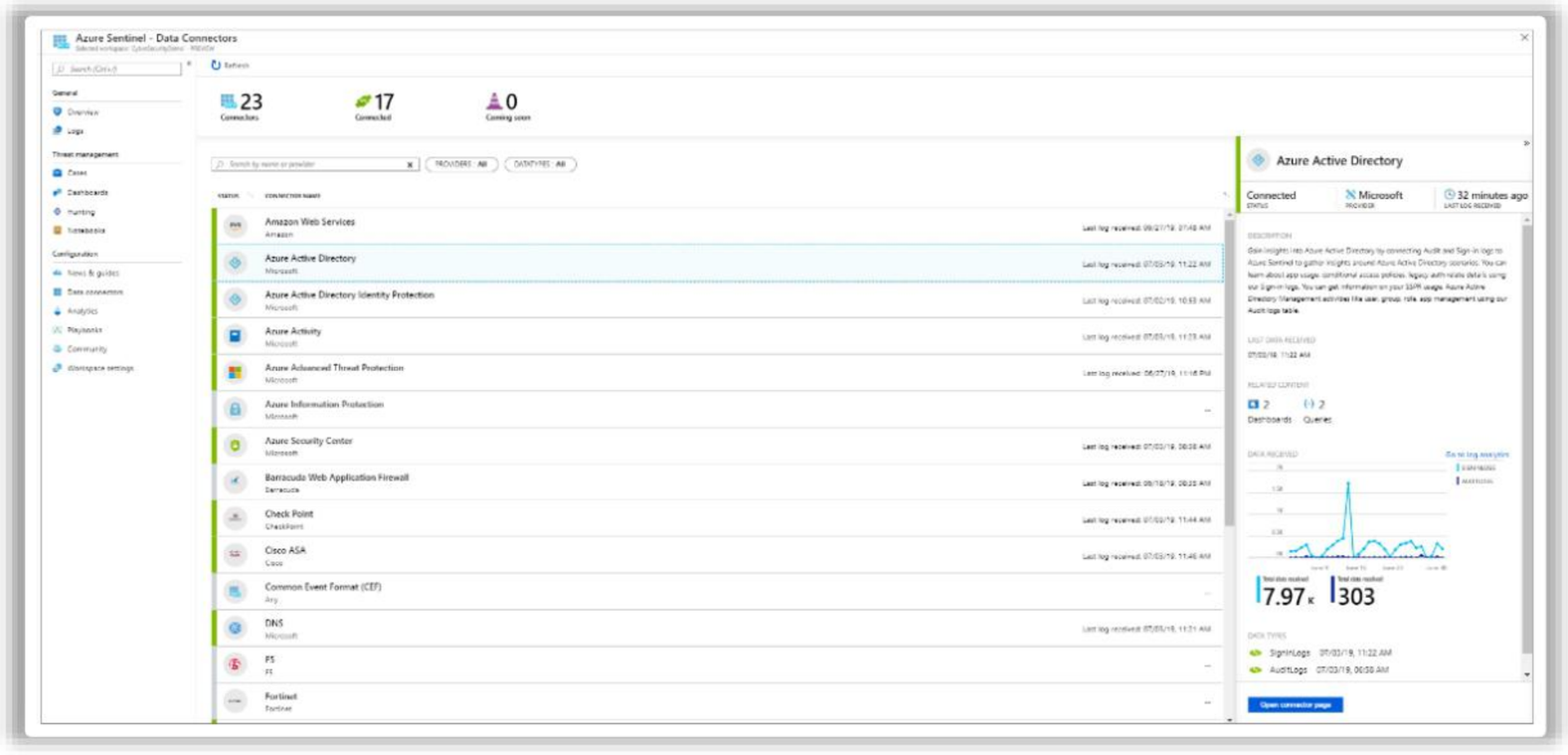


Figure 5.92: Data Connectors Gallery

- Choose appropriate options on the **connector** page. It displays instructions for configuring the connector and other important instructions. For example, if the **Azure AD** data source is selected, select the **types of logs** (audit logs or sign-in logs) to be delivered to Sentinel.

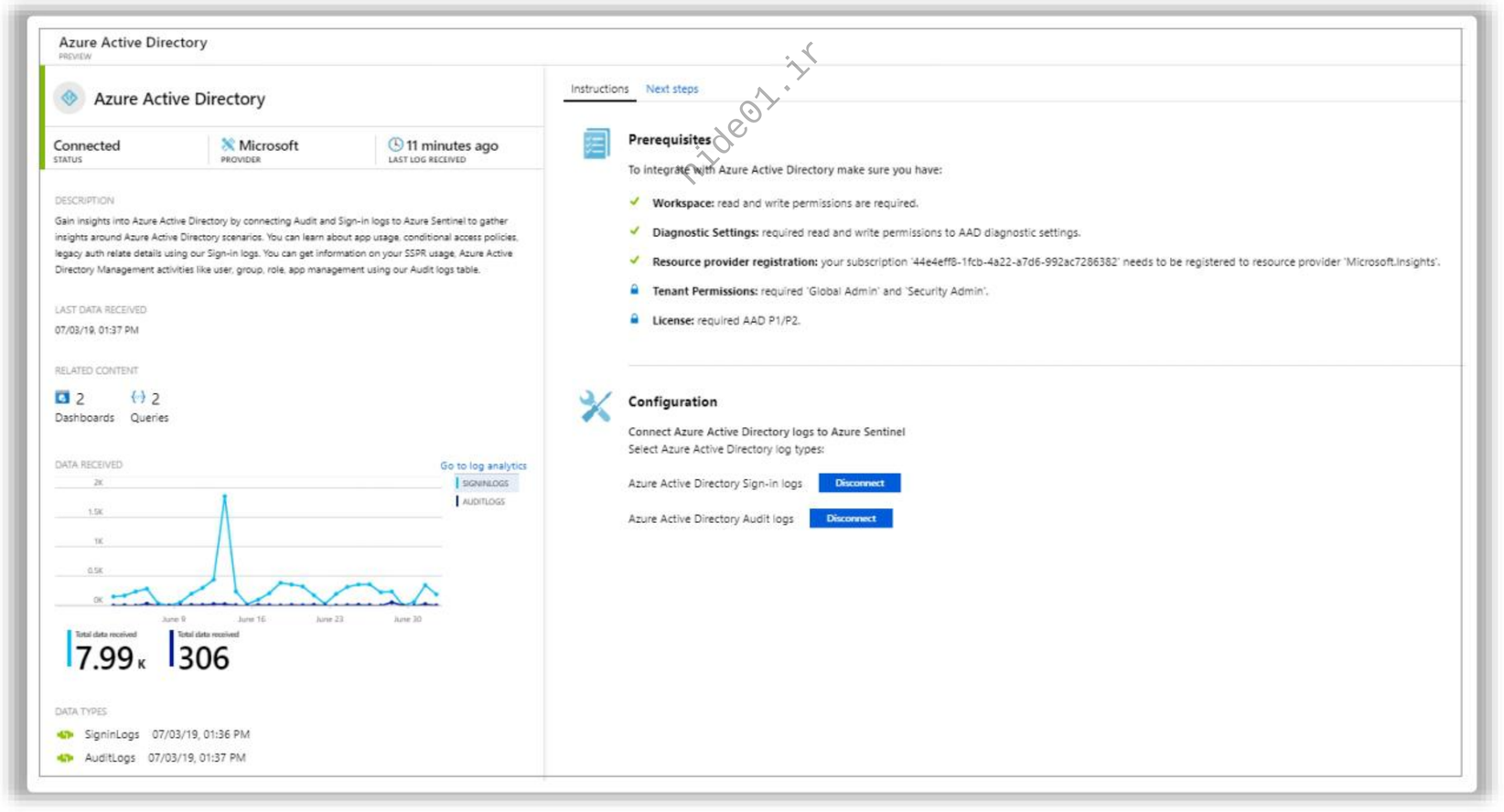


Figure 5.93: Azure AD

- Click on **Next steps** on the **connector** page. It will display in-built workbooks, analytics rule templates, and sample queries. Use them as they are or modify them as required to get insights across data.

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

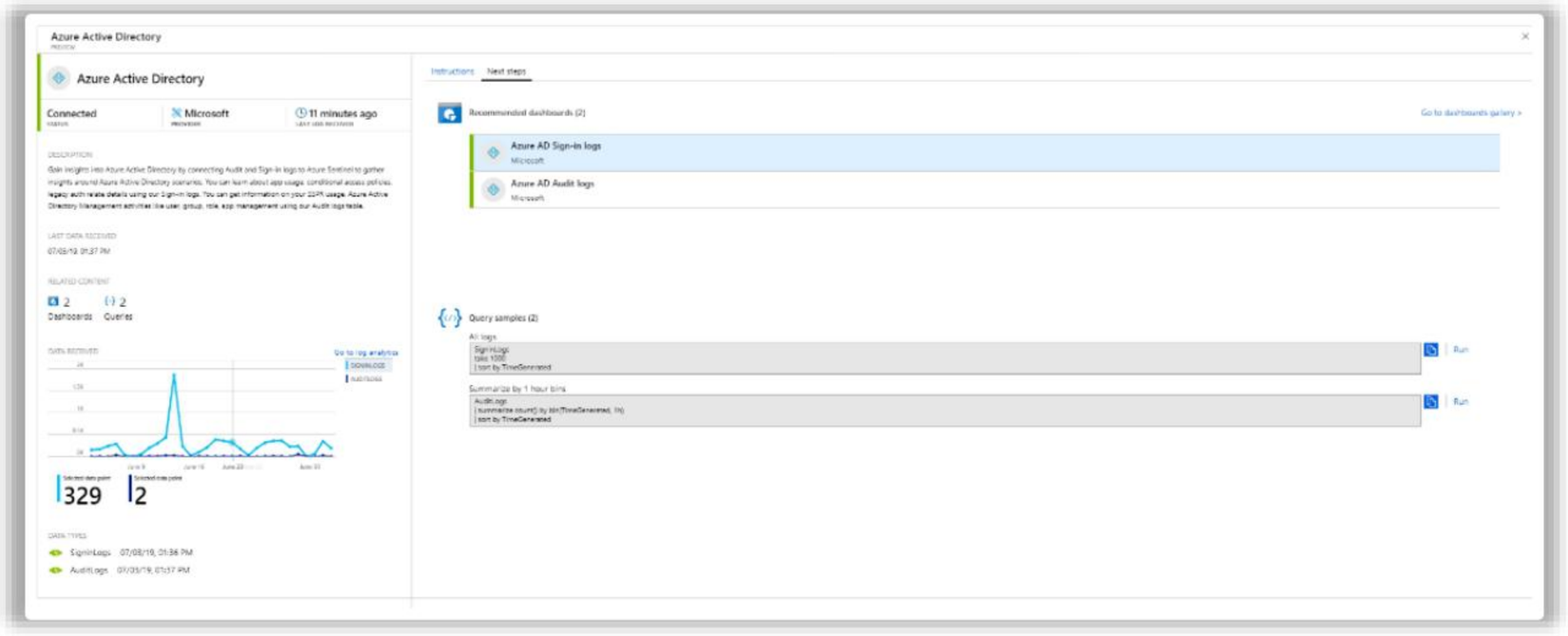
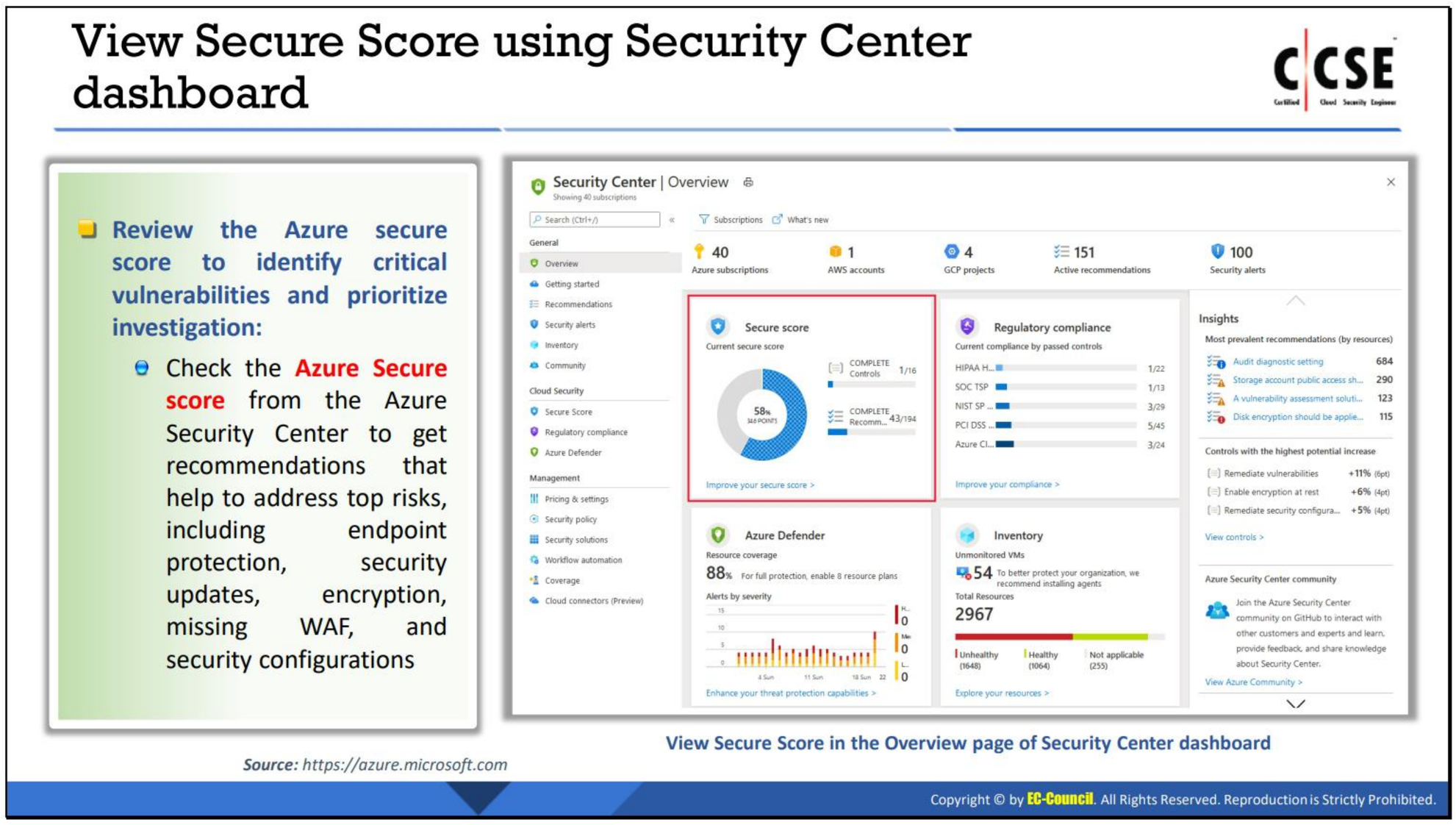


Figure 5.94: Connector Page

After connecting the required data sources, the data get streamed into Sentinel.

hide01.ir

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



View Secure Score Using Security Center Dashboard

Check the Azure secure score from the Azure Security Center to get recommendations that help to address top risks, including endpoint protection, security updates, encryption, missing WAF, and security configurations. Secure score helps customers to assess or evaluate their workload security posture. It can be accessed by customers from their dashboard. Secure score helps in achieving better security by offering recommendations that should be implemented.

Source: https://www.microsoft.com

Steps to check the secure score in three ways:

- **First method**: Go to the **Overview** page in the **Security Center** dashboard to see the secure score.

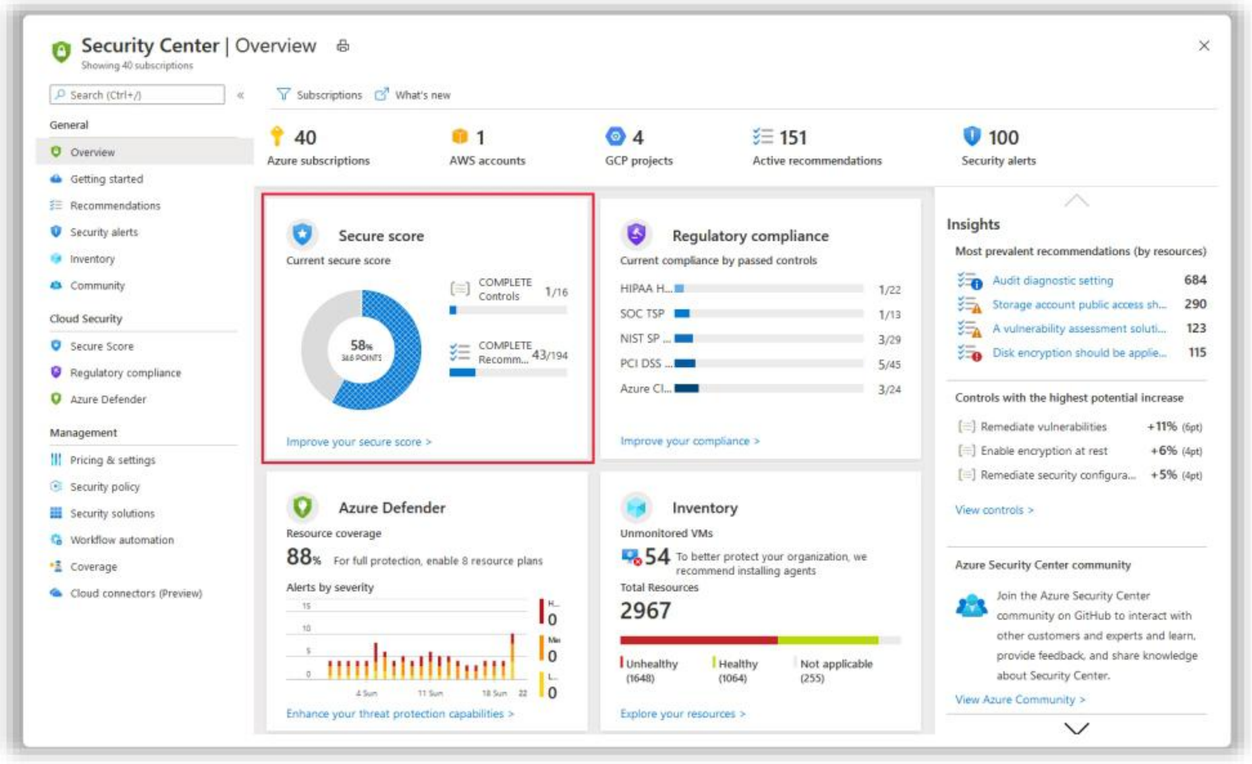


Figure 5.95: Security Center

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

- **Second method**: Choose **Secure score** on the main dashboard.

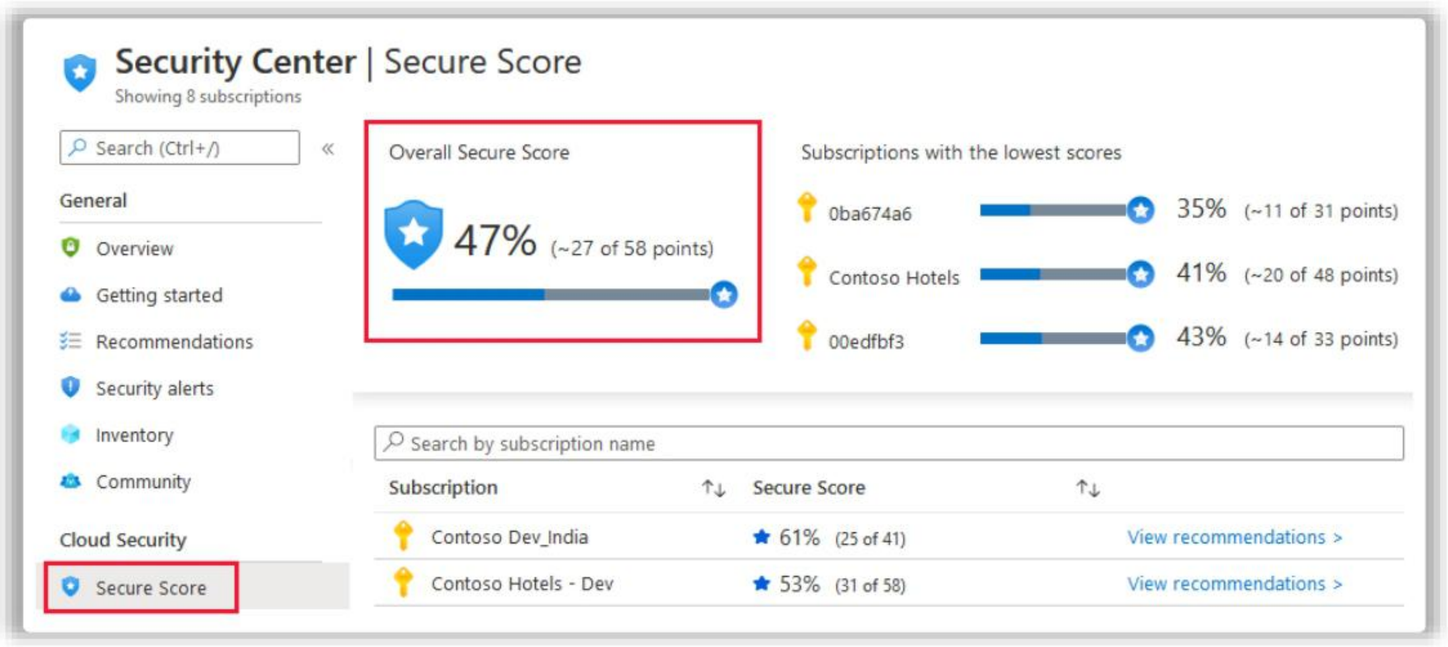


Figure 5.96: Secure Score

- **Third method**: Choose **Recommendations** on the main dashboard.

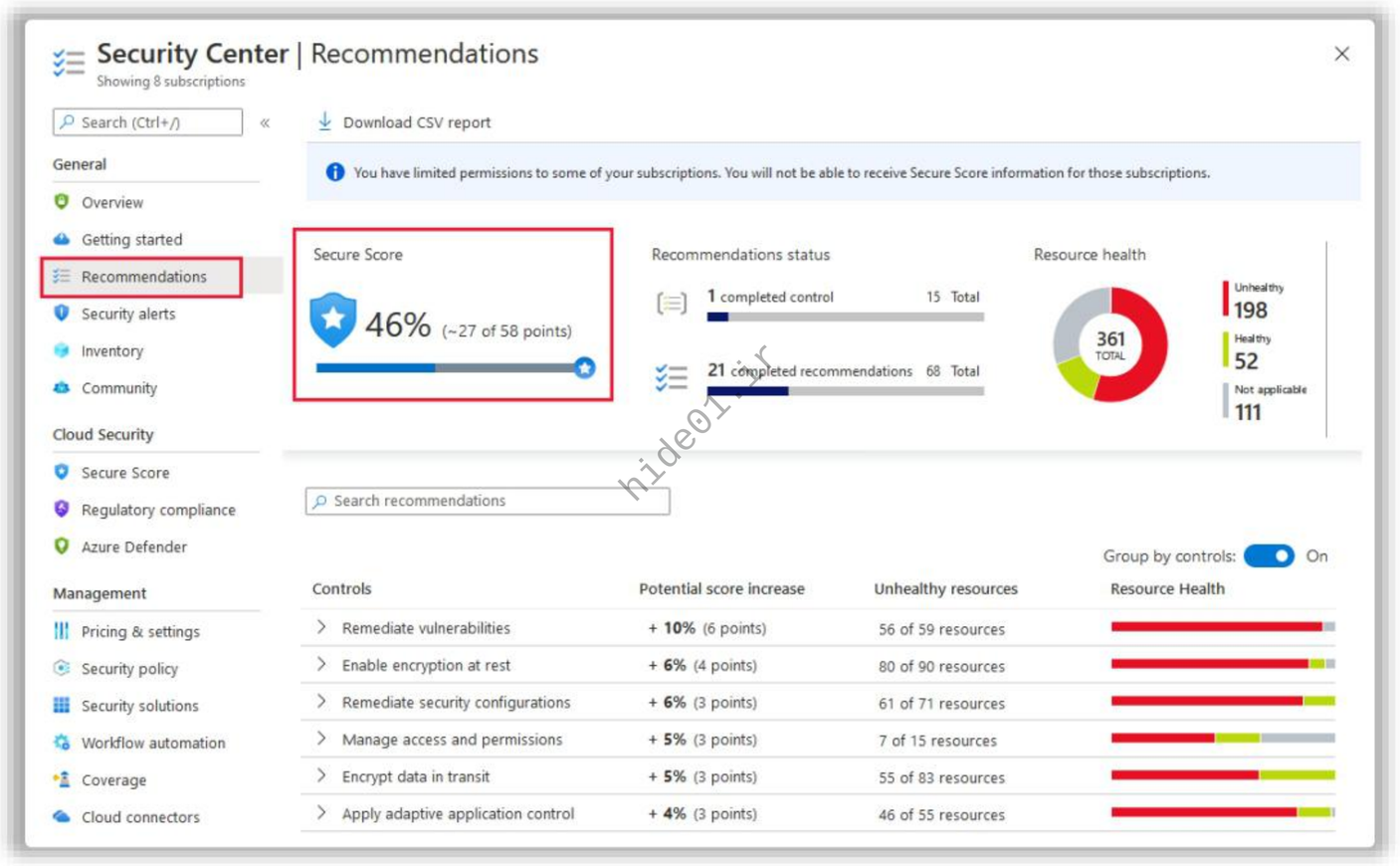
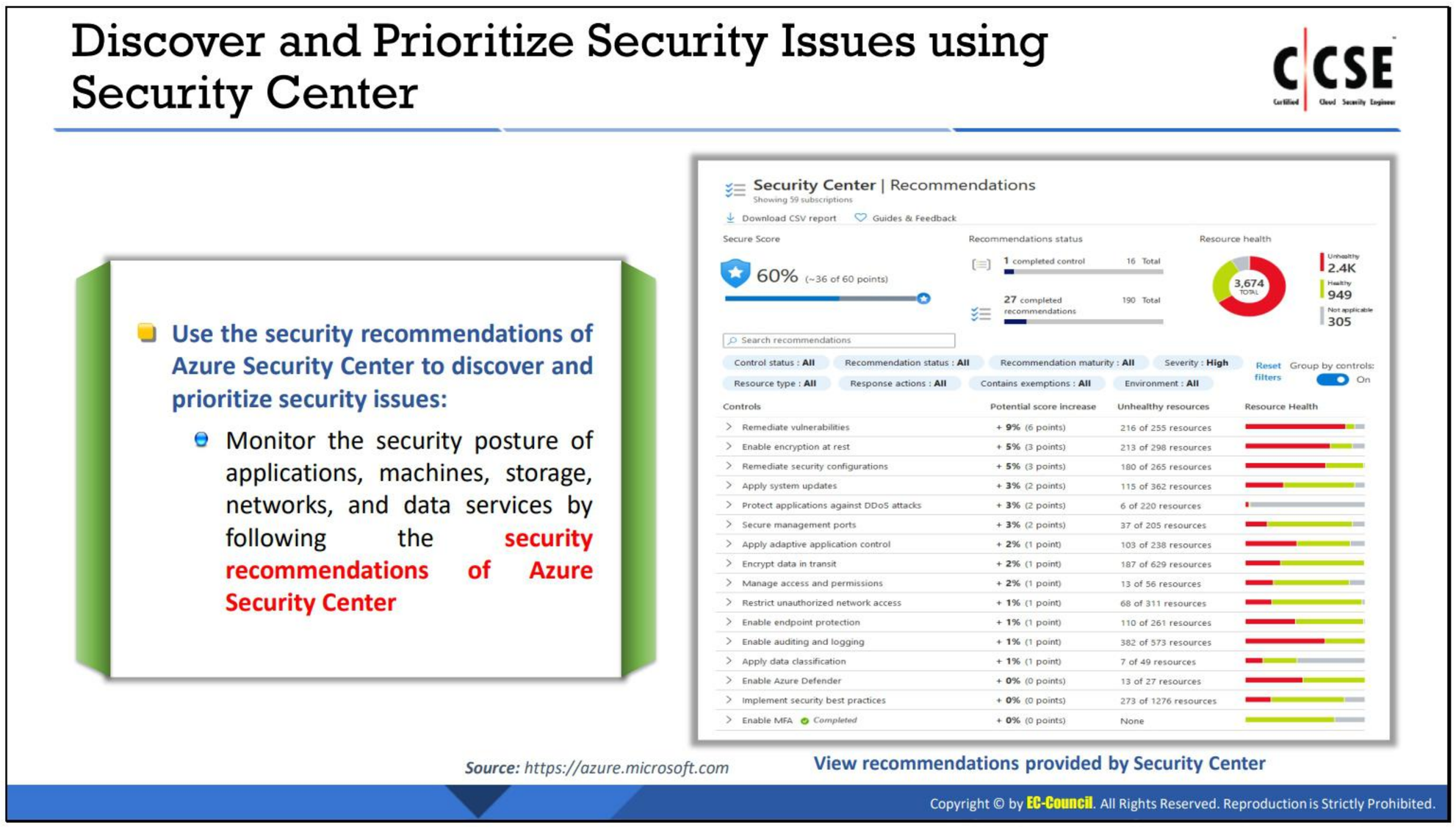


Figure 5.97: Recommendations

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



Discover and Prioritize Security Issues Using Security Center

Monitor the security posture of applications, machines, storage, networks, and data services by following the security recommendations of Azure Security Center. High priority items are shown first in the security recommendation list. Azure Security Center detects security vulnerabilities by constantly analyzing the security state of all Azure resources and provides recommendations to fix those vulnerabilities.

Source: https://www.microsoft.com

Steps to view recommendations provided by Security Center

Follow the steps given below to view the recommendations provided by Security Center:

- Click on **Recommendations** on the **Security Center dashboard** to see the recommendations that apply to your environment. They are grouped into security controls.

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

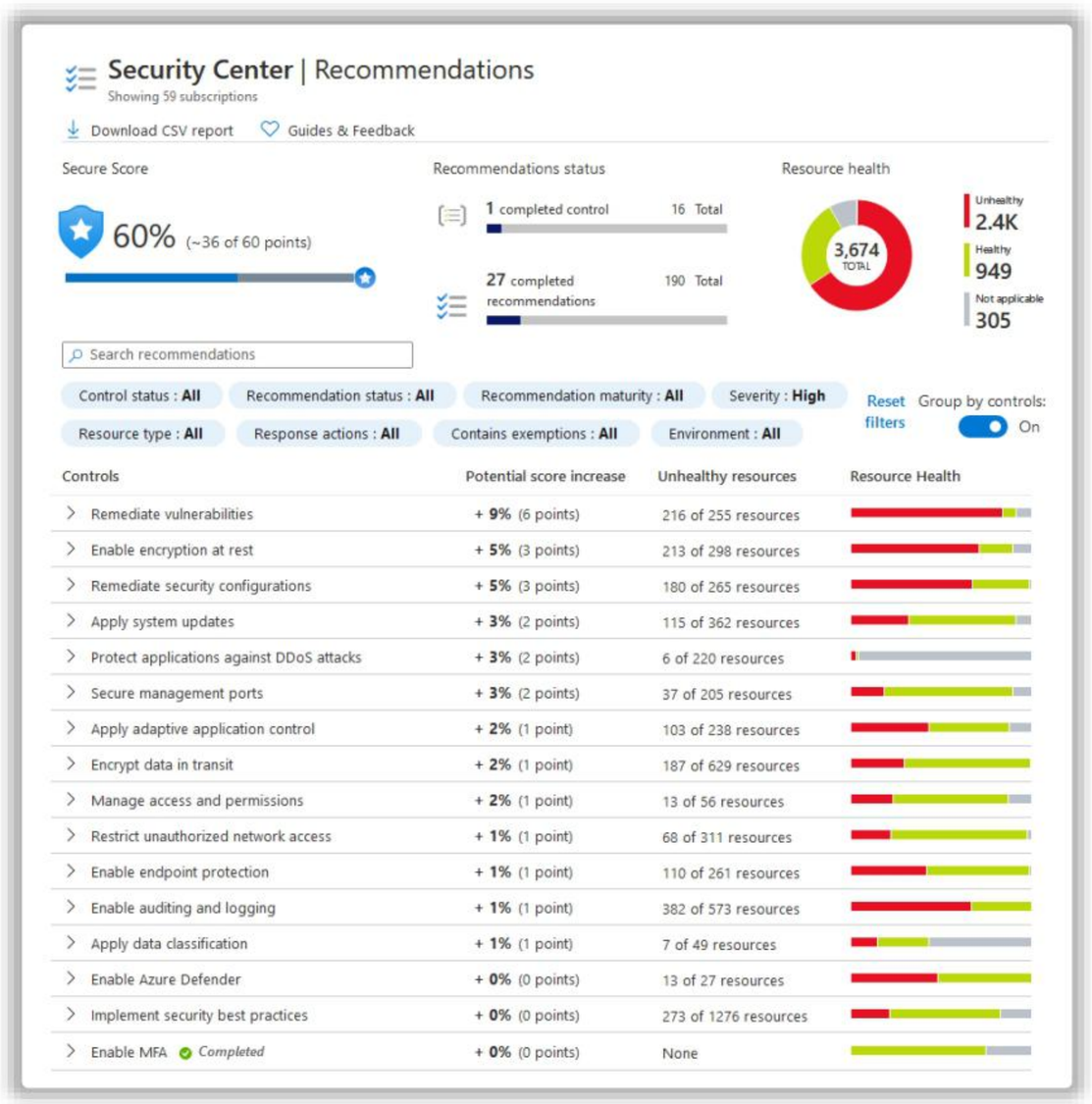


Figure 5.98: Recommendation

- Use filters to find recommendations specific to the environment, severity, resource type, or other important criteria.

hide01.ir

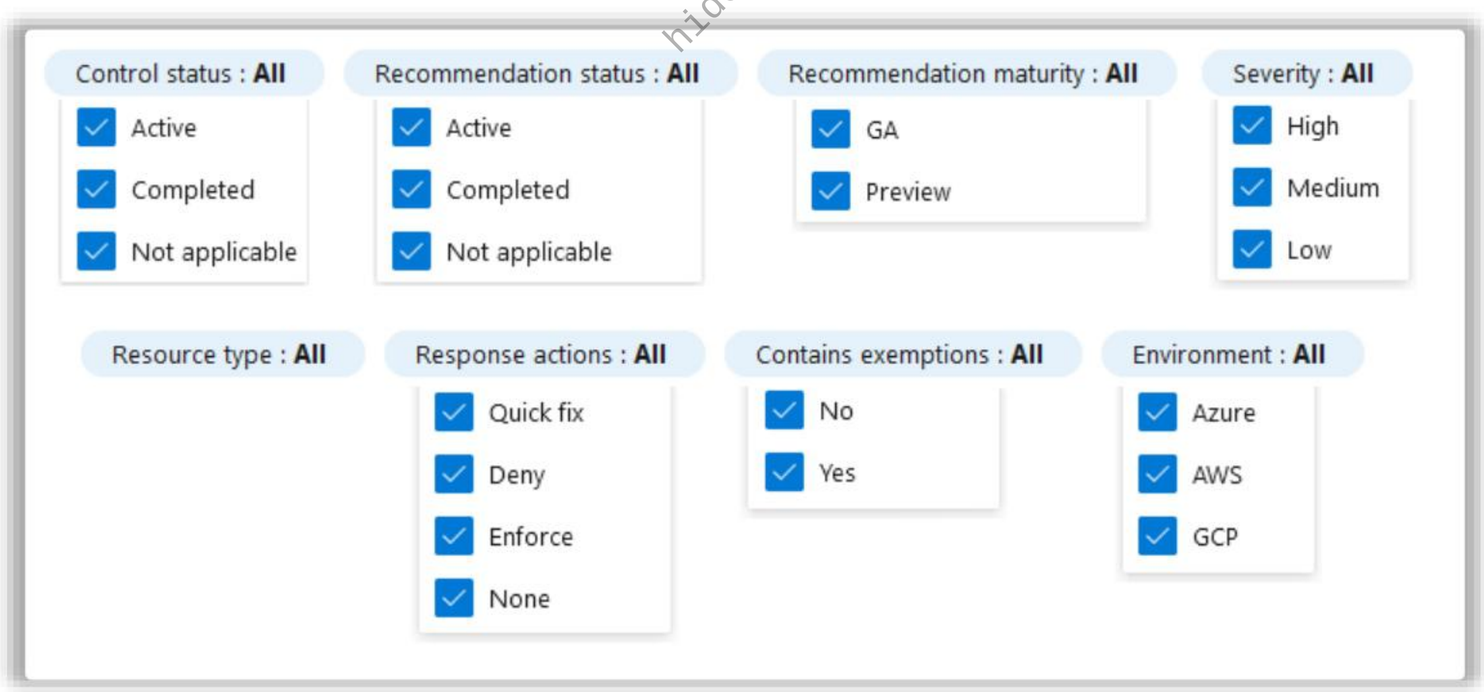


Figure 5.99: Filters

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

- To view recommendation details, expand a control and then select a specific recommendation.

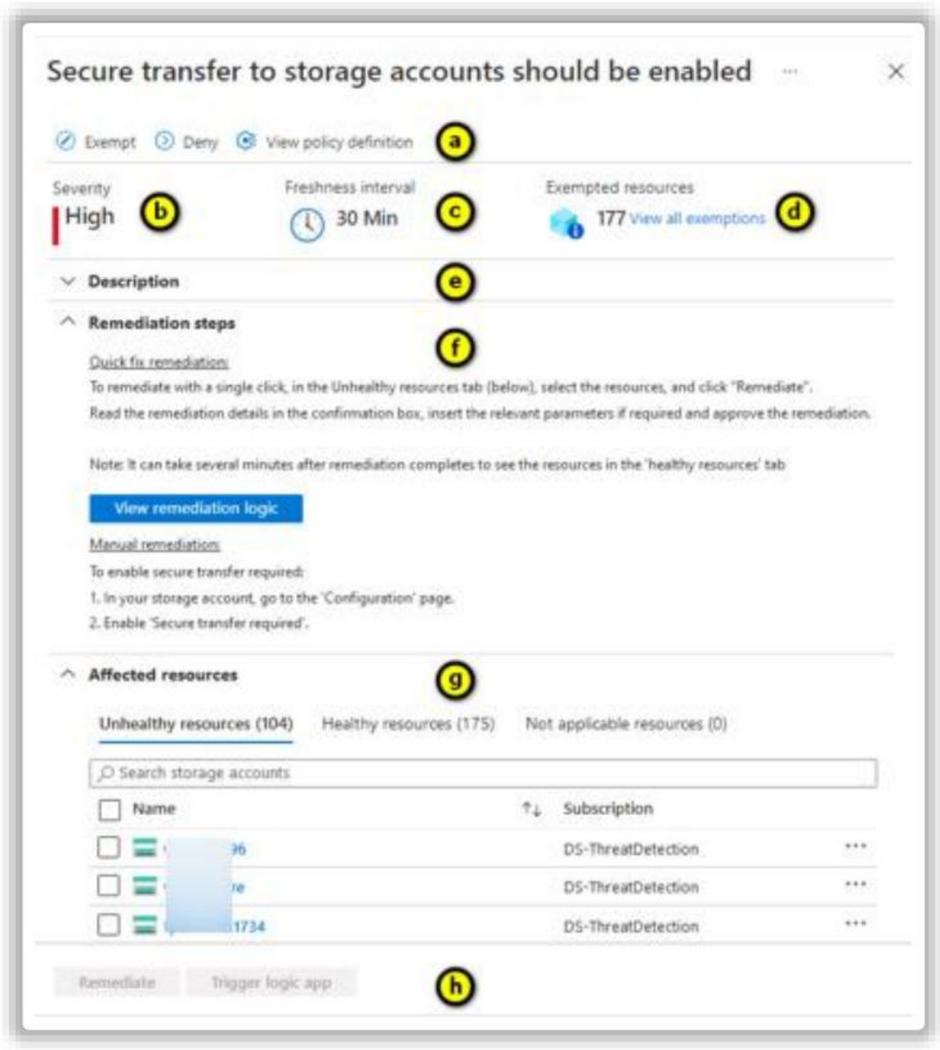


Figure 5.100: Recommendation Details

As shown in the above screenshot, the following options are available:

- Deny or enforce option for recommendations
- Severity indicator
- Freshness interval
- **Description**: Contains a brief description of the issue.
- **Remediation steps**: This option contains a short description of the manual steps required to remediate or fix issues. Select View remediation logic for recommendations before applying them to resources.
- **Affected resources**: Resources are classified into three tabs: Healthy resources (that are not impacted or already remediated), Unhealthy resources (impacted by the detected issues), and Not applicable resources (no definite recommendations for these resources).

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

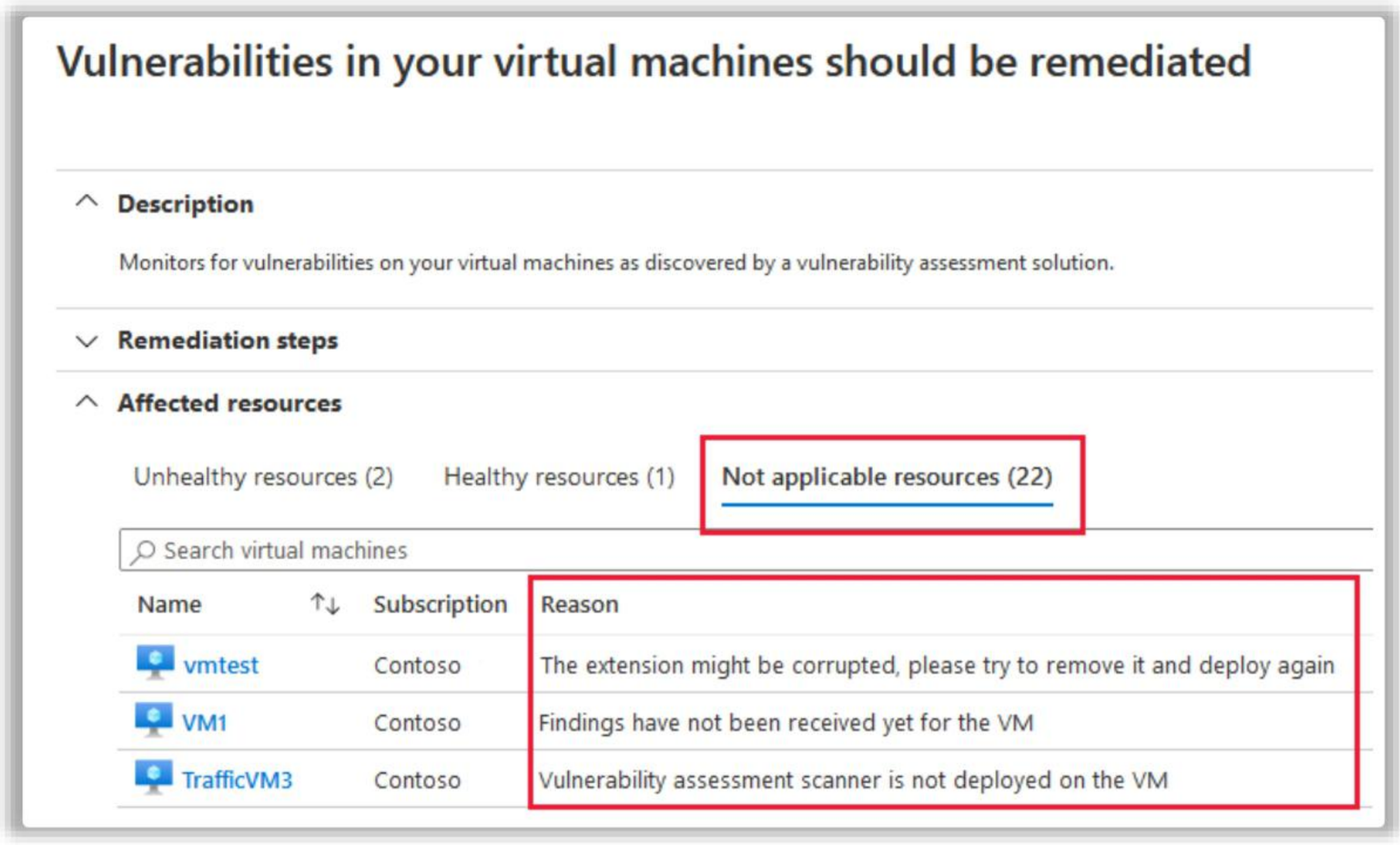
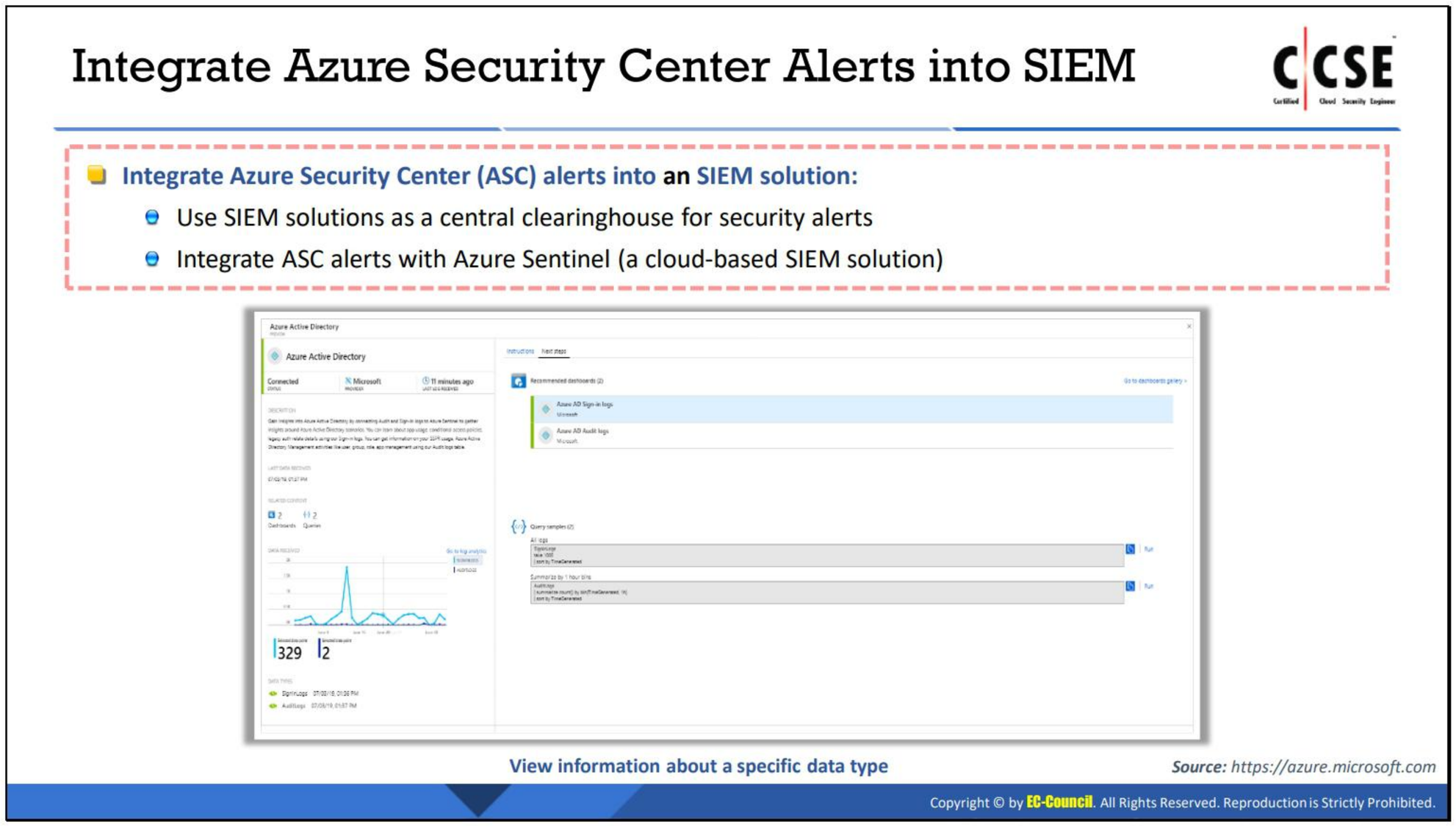


Figure 5.101: Not applicable Resources

- Action buttons that are used to remediate an issue.

hide01.ir

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



Integrate Azure Security Center Alerts into SIEM

Use SIEM solutions as a central clearinghouse for security alerts. The events processed by the Azure Security Center (ASC) are sent to Activity Log (in Azure Monitor). Azure Monitor then provides a consolidated pipeline to route monitoring data into SIEM tools. Integrate ASC alerts with Azure Sentinel (a cloud-based SIEM solution).

Source: https://www.microsoft.com

Steps to integrate ASC alerts into SIEM solutions

To stream alerts from ASC into Sentinel, use Azure Defender.

- **Connect Azure Defender to Sentinel**
  - Select **Data connectors** from the menu of Azure Sentinel.
  - Select **Azure Defender alerts from ASC** from **data connectors gallery** and select **Open connector page**.
  - Under **Configuration**, select the **Connect** button next to the subscription whose alerts are to be streamed in Sentinel.
  - To enable alerts from the Defender to generate incidents in Sentinel automatically, turn on the default analytics rule. For this, click on **Enabled** under **Create incidents**. This rule can be edited under the **Analytics** section on the **Active rule** tab.
  - Search for **SecurityAlert** to utilize the relevant schema for Defender alerts in Log Analytics.
- **Integrate Azure logs into an SIEM solution (Azure Sentinel)**

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

Utilize Azure Monitor to collect and export data to an SIEM solution. This helps in security incident investigation. Azure logs can be integrated with on-premises SIEM solutions and cloud-native SIEM solutions such as Sentinel, but integration is simpler and quicker between Azure Monitor and Sentinel.

- Choose **Data connectors** from the **main menu.** A comprehensive list of connectors provided by Sentinel will be displayed.
- Select the desired connector you need to connect, followed by the **Open connector page**.

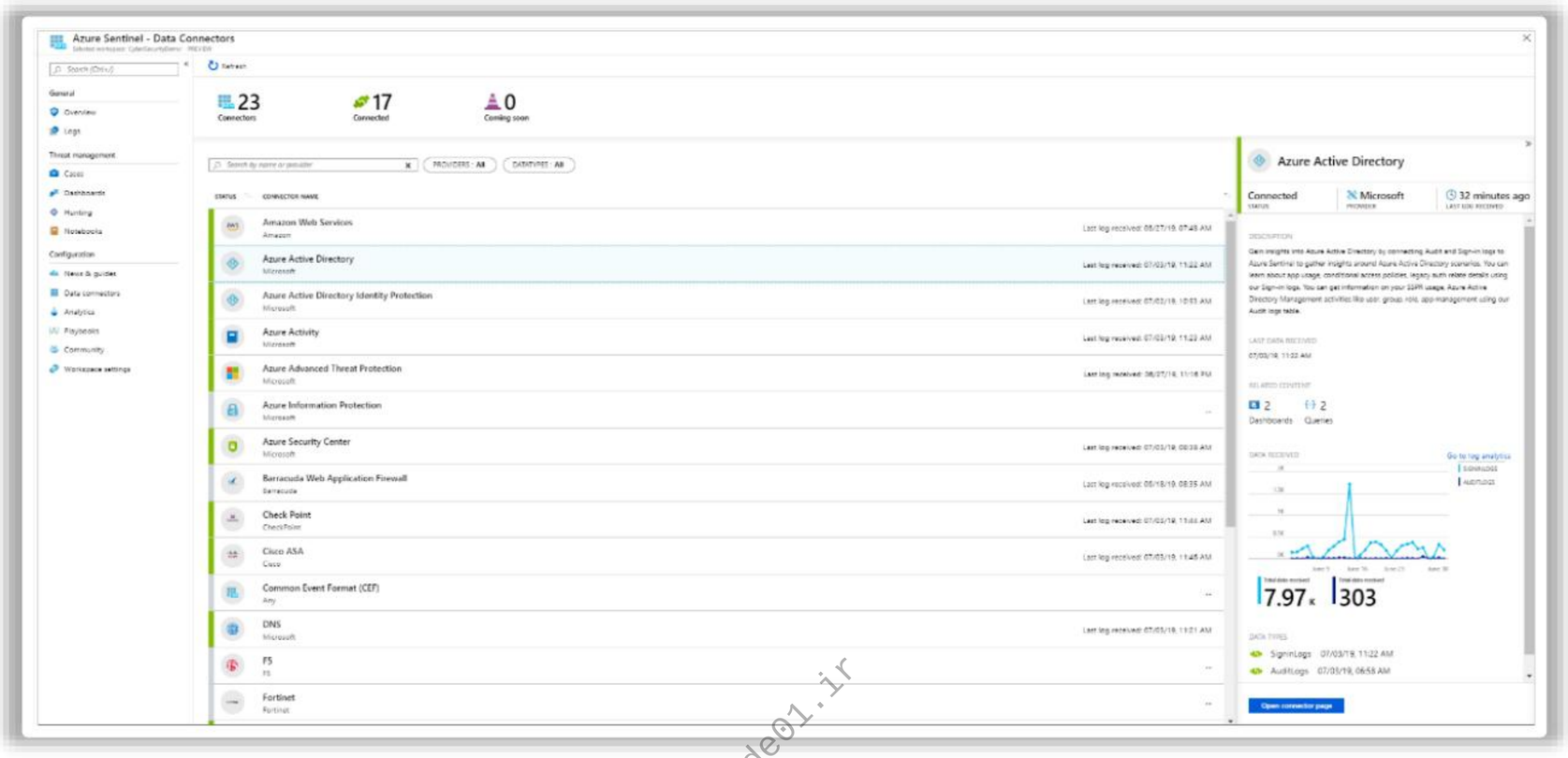


Figure 5.102: Data Connector

- Follow all instructions on the specific connector page to connect data to Sentinel. Logs may start syncing with Sentinel after some time. Data summary can be viewed in the **Data received** graph; connectivity status is displayed after connecting.

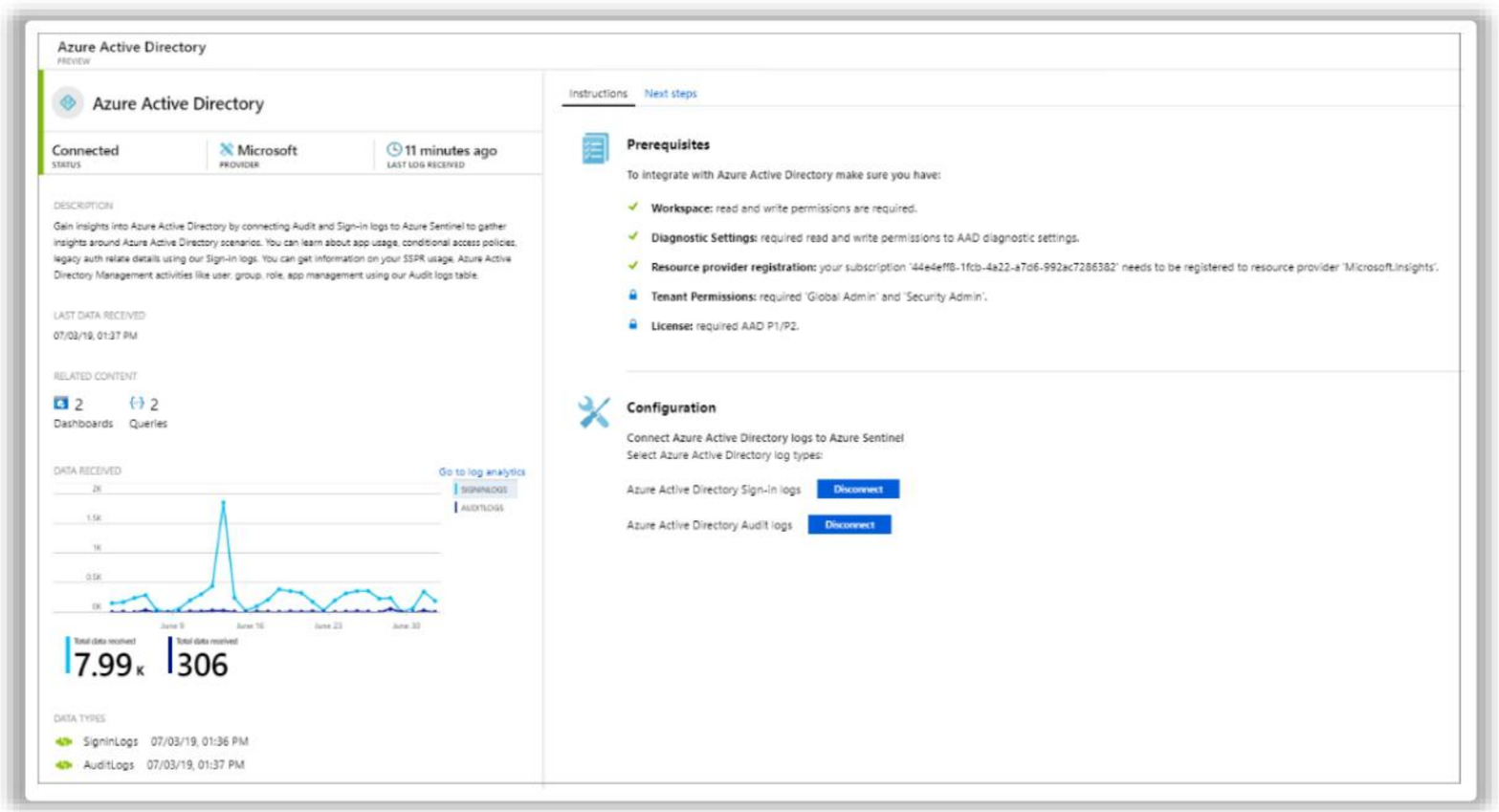


Figure 5.103: Azure AD

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

- Choose the **Next steps** tab to view information about a specific data type.

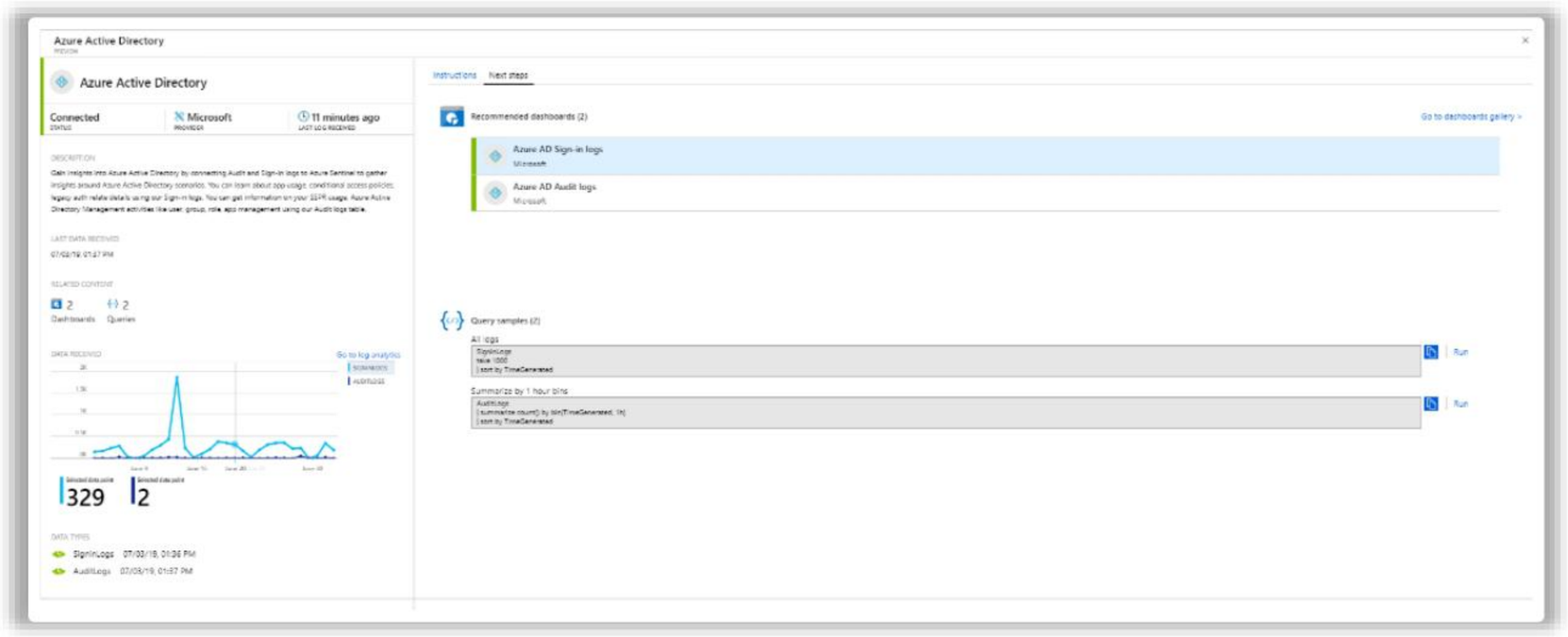


Figure 5.104: Azure AD

- **Integrate Azure logs into an SIEM solution (Azure Sentinel)**

  Utilize Azure Monitor to collect and export data to an SIEM solution. This helps in security incident investigation. Azure logs can be integrated with op-premises SIEM solutions and cloud-native SIEM solutions such as Sentinel, but integration is simpler and quicker between Azure Monitor and Sentinel.

  Steps to integrate Azure logs into Azure Sentinel

  - Select **Data connectors** from the **main menu.** A comprehensive list of connectors provided by Sentinel will be displayed.
  - Choose the desired connector you need to connect, followed by the **Open connector page**.

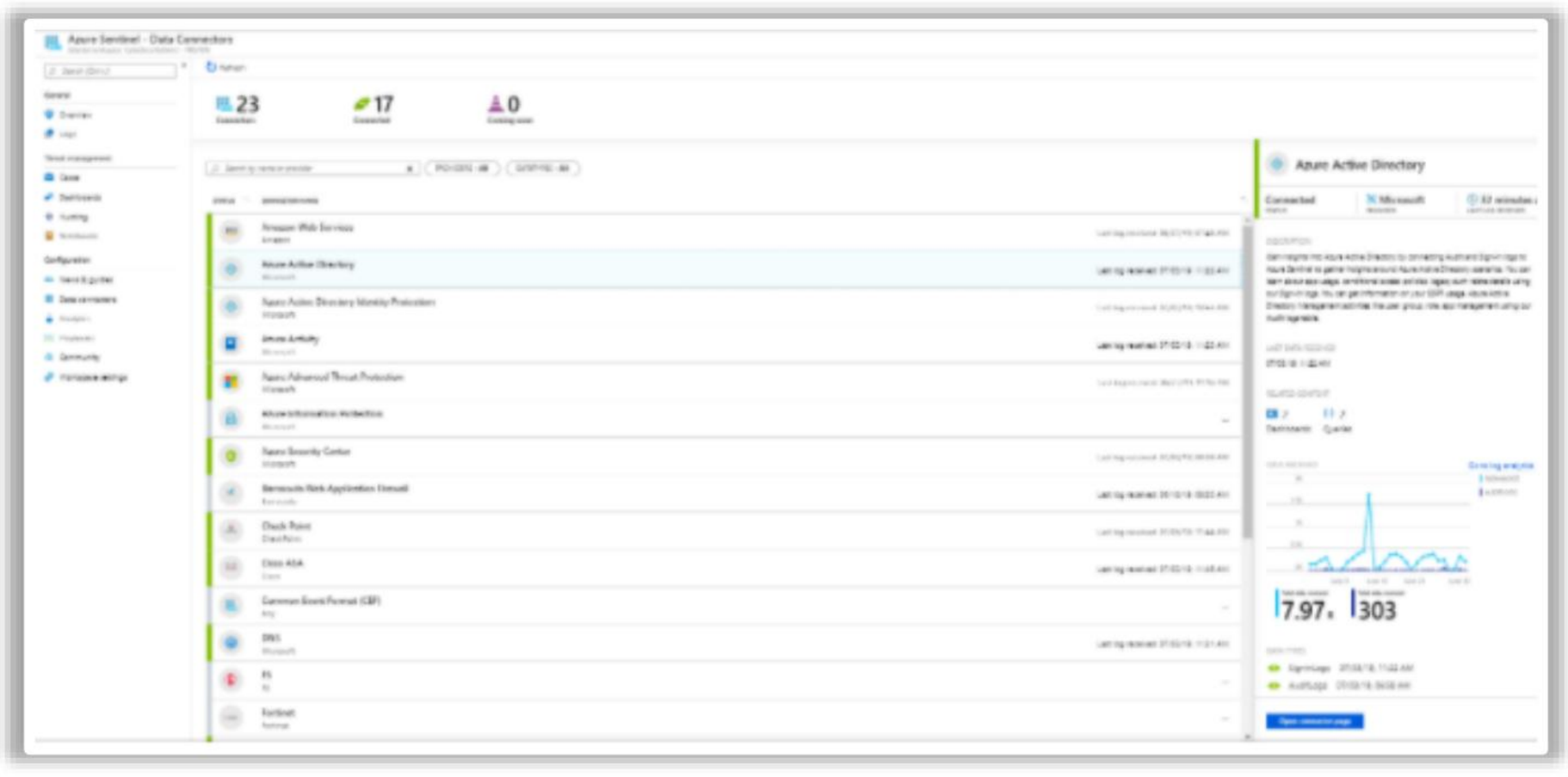


Figure 5.105: Data Connector

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

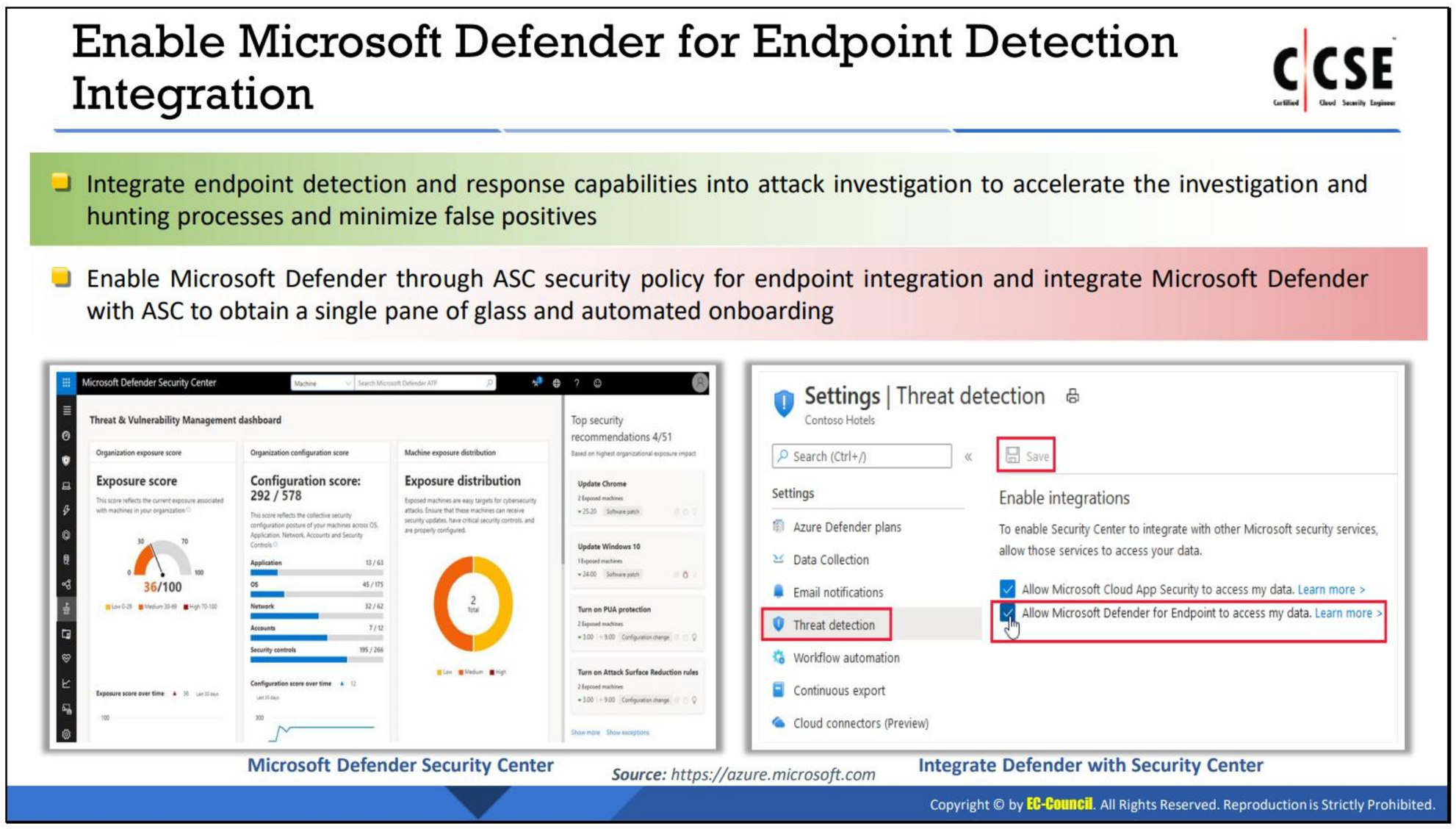
- Follow all instructions on the specific connector page to connect data to Sentinel. Logs may start syncing with Sentinel after some time. Data summary can be viewed in the **Data received** graph; connectivity status is visible after connecting.
- Choose the **Next steps** tab to view information about a specific data type.

Azure Sentinel supports the streaming of logs from various data sources. Consider an example of connecting data from Azure Activity logs to stream into Sentinel. The Activity log records and shows subscription-level events throughout Azure, including Azure Resource Manager operational data and updates regarding Service Health events. Cloud admins can use Azure Activity logs to identify write operations (POST, PUT, and DELETE) performed on their subscription resources and obtain information about the operational status and other related properties.

Steps to set up the Azure Activity connector

- Choose **Data connectors** from the menu of Azure Sentinel.
- Select **Azure Activity** from the list of connectors, followed by the **Open connector page**.
- Click on **Configure Azure Activity logs>** under the **Instructions** tab.
- Now, select the subscription whose logs need to be streamed into Sentinel on the **Azure Activity log** pane.
- Click on **Connect** on the subscription pane.
- Enter **AzureActivity** in the query window to use the relevant schema for Azure Activity alerts in Log Analytics.

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



Enable Microsoft Defender for Endpoint Detection Integration

Source: https://www.azure.microsoft.com

Integrate endpoint detection and response capabilities for attack investigation to accelerate the investigation and hunting processes and minimize false positives. Enable Microsoft Defender through Security Center security policy for endpoint integration. Integrate Microsoft Defender with Security Center to get a single pane of glass (Defender alerts are displayed on Security Center console) and automated onboarding (Security Center will enable the Defender sensor for the Windows servers monitored by it).

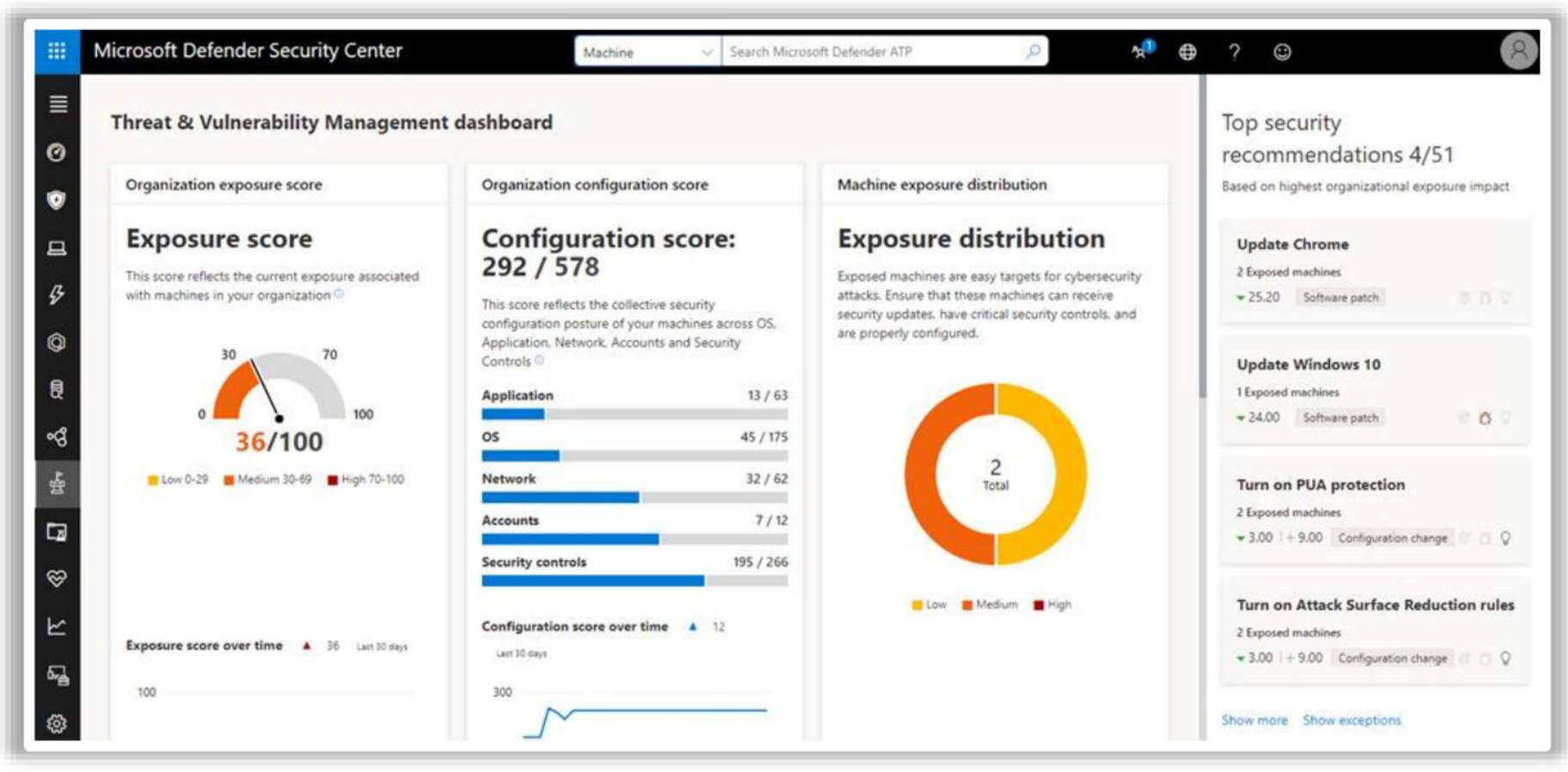


Figure 5.106: Microsoft Defender

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

Microsoft Defender for Endpoint refers to a cloud-based endpoint security solution that provides the following features:

- Automatic investigation and remediation
- Attack surface reduction
- Risk-based vulnerability assessment and management
- Endpoint detection and response (EDR)
- Cloud-powered and behavioral-based protection
- Managed hunting services

Steps to enable Microsoft Defender for Endpoint integration:

- First, enable **Azure Defender for servers**.
- Remove the existing Microsoft Defender for Endpoint if already deployed and licensed.
- Choose **Pricing & settings** from the Security Center menu and select the subscription that needs to be changed.
- Choose **Threat detection** on the **Settings** page.
- Then, select **Allow Microsoft Defender for Endpoint to access my data** and click on **Save**.

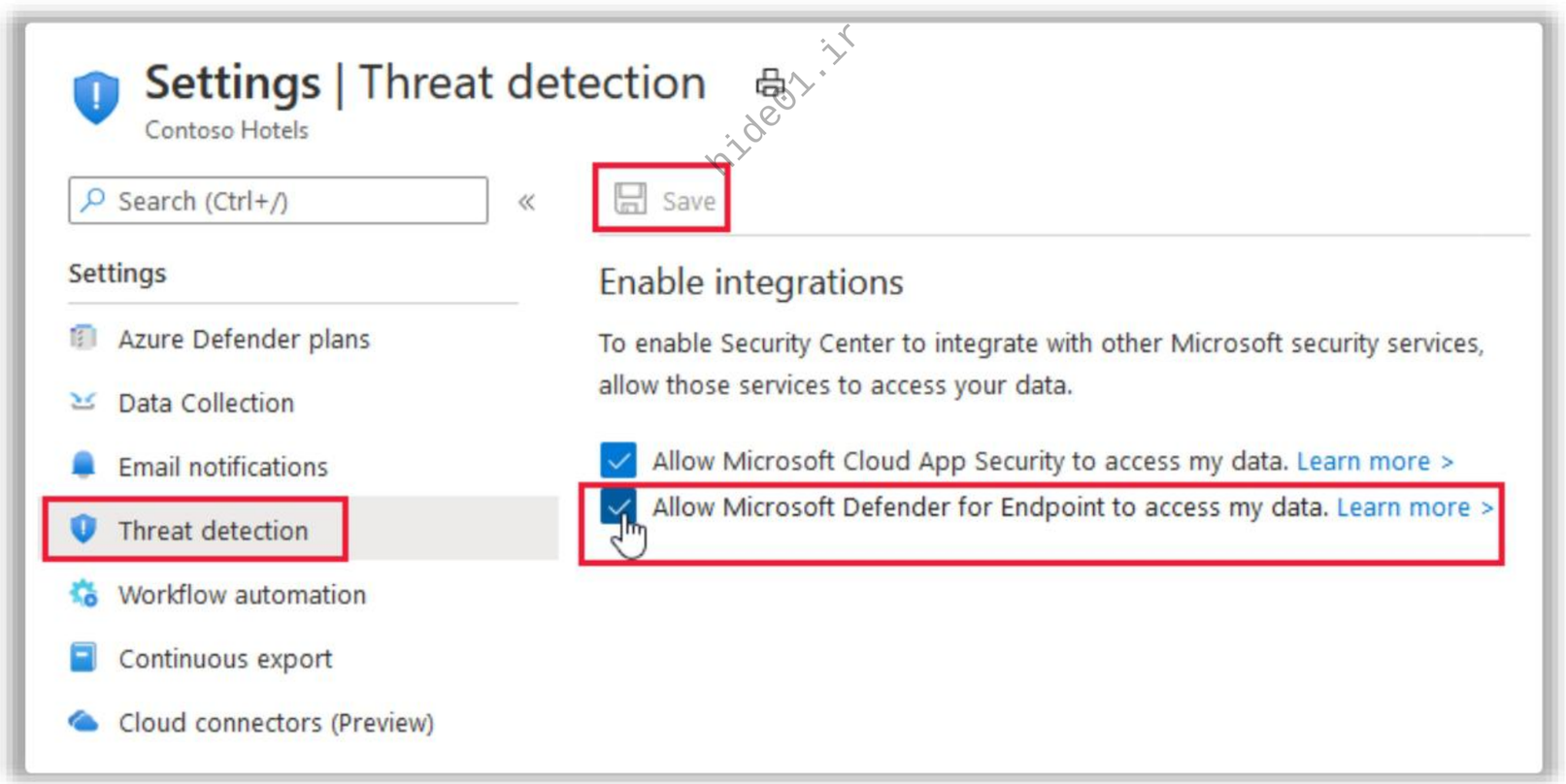
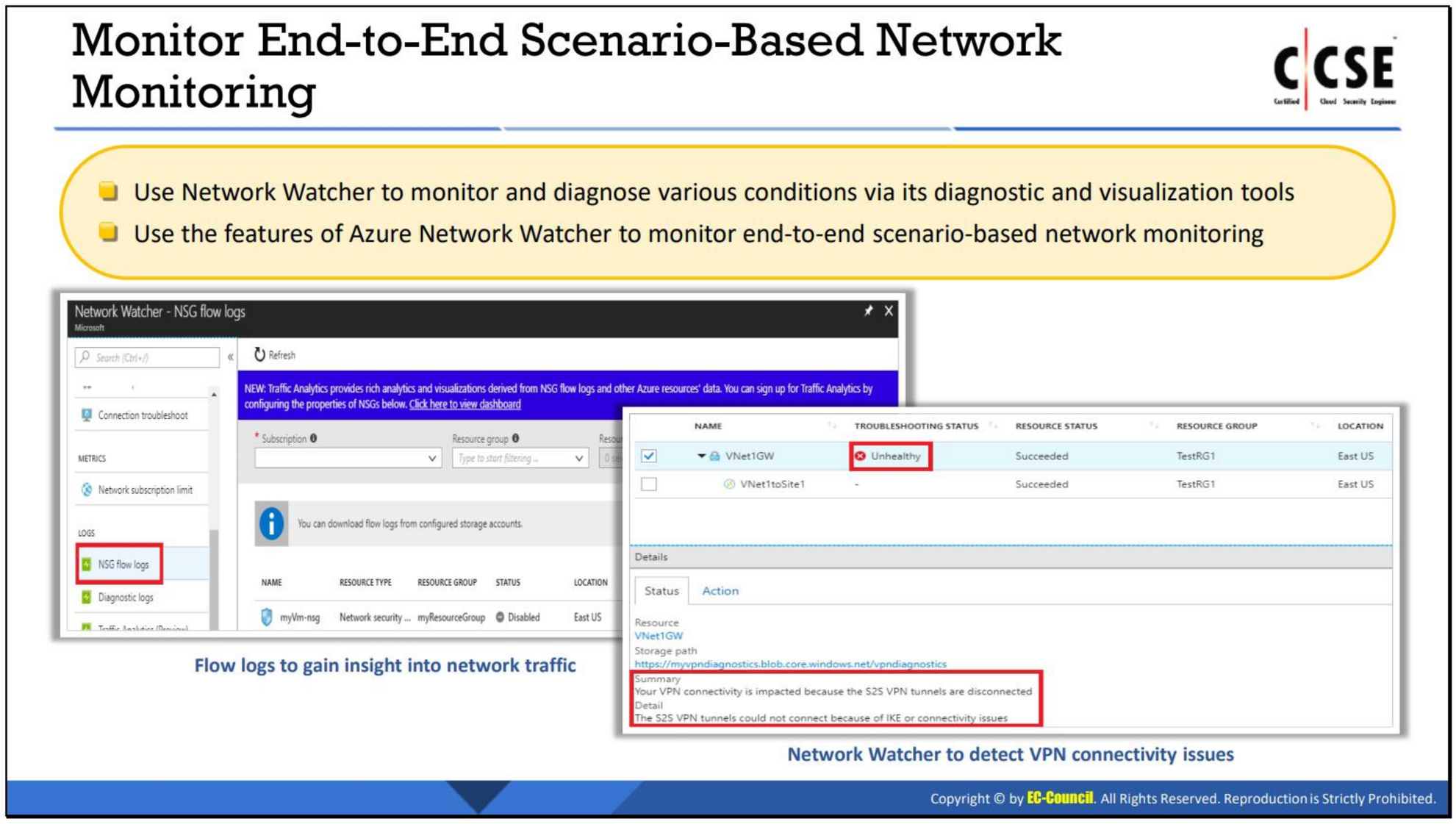


Figure 2.107: Threat Detection

Servers will automatically get installed on Microsoft Defender for Endpoint by ASC, but it may take up to 24 h. Microsoft Defender for Endpoint can be accessed via the Microsoft Defender Security Center portal.

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



Monitor End-to-End Scenario-Based Network Monitoring

In Azure, an end-to-end network is established using various network resources such as Load Balancer, ExpressRoute, and Application Gateway. Every network resource supports monitoring. Use Network Watcher to monitor and diagnose various conditions via its diagnostic and visualization tools.

Azure Network Watcher is used to monitor the network health of IaaS products such as VMs, VNet, and load balancers. The features of Azure Network Watcher are listed below:

- The packet data of VM are remotely captured.
- Using flow logs and security group view, the VM security network is monitored.
- VPN connectivity issues are diagnosed.

Steps for effective end-to-end scenario-based network monitoring

- **Use flow logs to gain insight into network traffic**

  Use NSG flow logs to better understand network traffic patterns. Azure Network Watcher provides the flow logs feature, which allows to record information about the IP traffic traveling via NSG. Flow data can be accessed from Azure storage accounts or sent to any SIEM, IDS, or visualization tools from storage accounts. Steps to enable NSG flow logs include:

  - Create an Azure Storage account (because flow log data are sent to the storage account) by selecting **+ Create a resource** on the portal.
  - Choose **Storage** and click on **Storage account- blob, file, table, queue**.

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

- Fill in the required information as shown below, accept the defaults, and choose to **Create**.
  - **Name**- Enter a name (3-24 characters)
  - **Location**- Select East US.
  - **Resources group**- Click on **Use existing**, followed by **myResourceGroup.**
- After the storage account is created, choose **All services** on the left top of the portal. Search for **Network Watcher** and select it via the filter box.
- Choose **NSG flow logs** under **LOGS**.

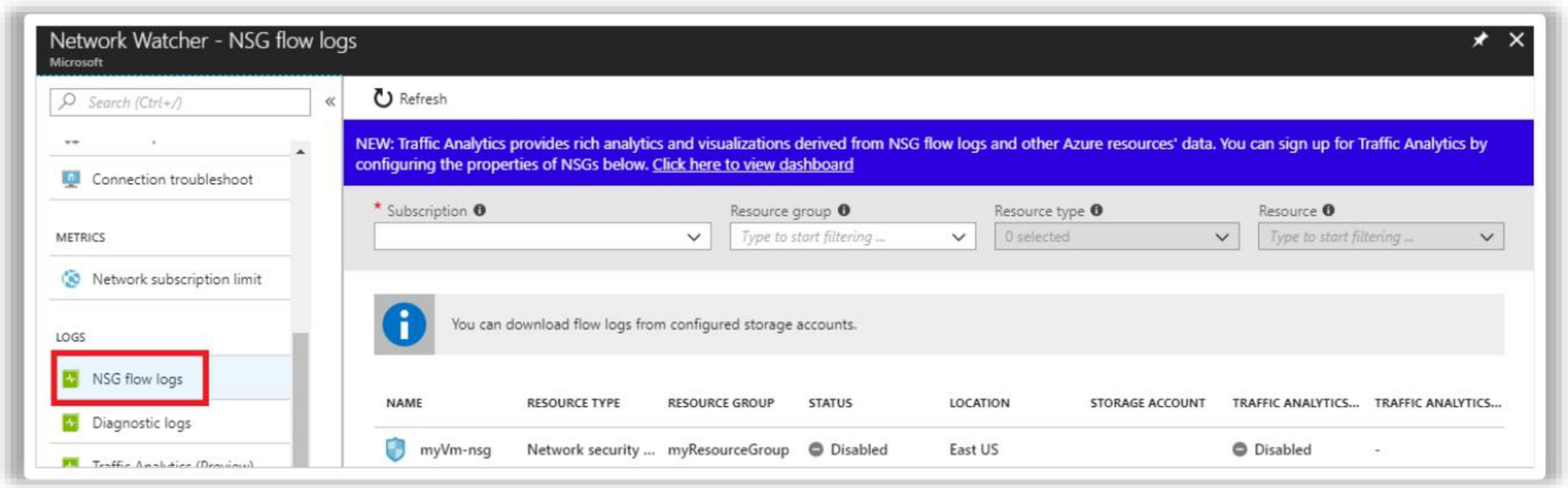


Figure 5.108: NSG Flow Logs

- Select the suitable NSG (**myVm-nsg**) from the list of NSGs.
- Select **On** under the **Flow log settings**; then, select the appropriate flow logging version.

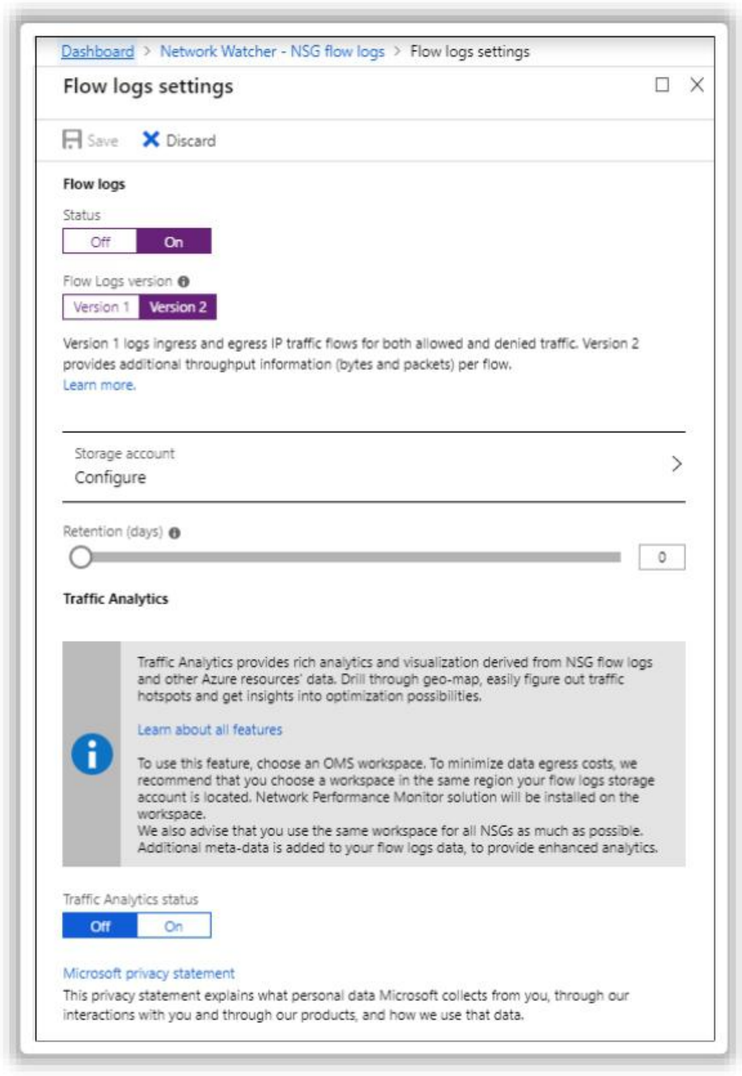


Figure 5.109: Flow Logs Settings

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

- Choose the newly created storage account.
- Choose **All services** on the top left corner of the portal. Search for **Network Watcher** and select it via the filter box.
- Set **Retention** period to 5 days and click on **Save**.

- **Use packet capture to automate remote network monitoring**

  Use Network Watcher to diagnose and monitor networking issues without logging into VMs. Create capture sessions with Network Watcher to monitor traffic from and to a VM. Packet capture allows cloud security professionals to diagnose anomalies reactively and proactively, collect network statistics, and obtain information about network intrusions. Packet captures can be triggered remotely on a particular VM, which reduces the burden of executing a packet capture manually and saves time.

  Steps to set up a packet capture include:

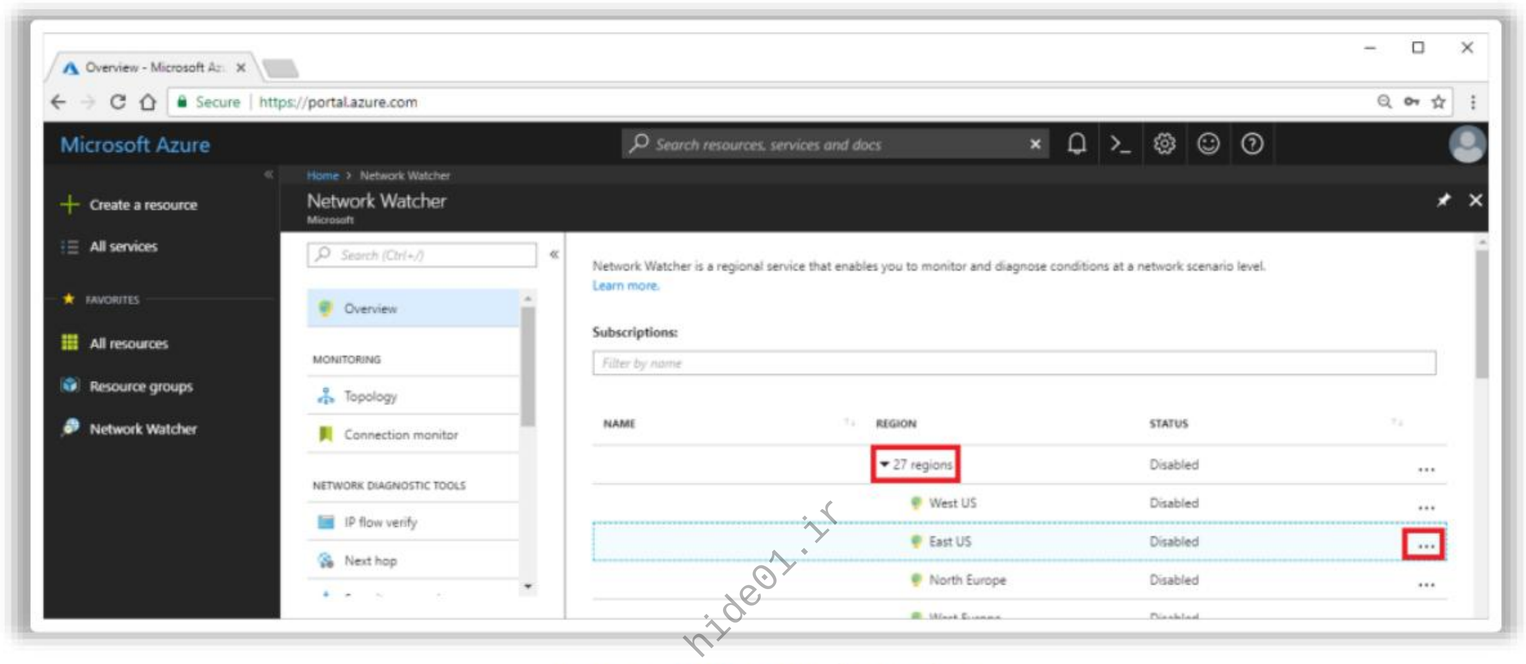
  - Go to the Azure portal and choose **All services**. In the **Networking** section, click on **Network Watcher**.
  - Under **Network diagnostic** tools, select **Packet capture**.
  - Click on **Add** to create a new packet capture by selecting appropriate values as shown:
    - **Subscription**- Select the subscription that contains the VM for which packet capture is being created.
    - **Resource group**- Resource group of the VM.
    - **Target virtual machine**- The VM for which packet capture is being created.
    - **Packet capture name**- Enter a name for packet capture.
    - **Storage account or File**- Select Storage account, File, or both. The capture is saved with the VM if File is selected.
    - **Local file path**- The local path where the capture will be stored on VM (if File is selected).
    - **Storage accounts**- If storage account is selected in the previous step, select an existing storage account.
    - **Max bytes per packet**- The number of bytes captured from each packet. All bytes get captured if it is left blank.
    - **Max bytes per session**- It refers to the total number of bytes captured. Packet capture stops once the maximum value is reached.
    - **Time limit**- Packet capture stops after the set time limit (in seconds) is reached.
  - Click on **OK.**

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

- **Use Network Watcher to detect VPN connectivity issues**

  Diagnose the standard VPN gateway and connection issues using Network Watcher because it helps to detect issues and view detailed logs for further investigation. Steps to detect VPN connectivity issues via Network Watcher include:

  - Log into the Azure portal.
  - Enable **Network Watcher** if not already enabled. Go to the next step if already enabled.
    - Select **All services** and search for **Network Watcher** and select it via the filter box.
    - Expand **Regions** and choose the icon at the right of East US as shown below



hide01.ir

Figure 5.110: Network Watcher

  - Diagnose a gateway after enabling Network Watcher:
    - Select **All services** and search for **Network Watcher;** select it via the filter box.
    - Choose **VPN Diagnostics** under **NETWORK DIAGNOSTIC TOOLS**.
    - Choose **Storage account** and select the storage account where the diagnostic information should be stored. Create a storage account if it does not exist by selecting **+ Storage account**, entering the required information, and clicking on **Create**.
    - Select a container from the list of **Containers** and click on **Select**. Create a container if there are no existing containers by selecting **+ Container**, typing a name for it, and clicking on **OK**.
    - Choose a gateway and click on **Start troubleshooting,** as shown in the screenshot (**Vnet1GW** gateway is selected to be tested).

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

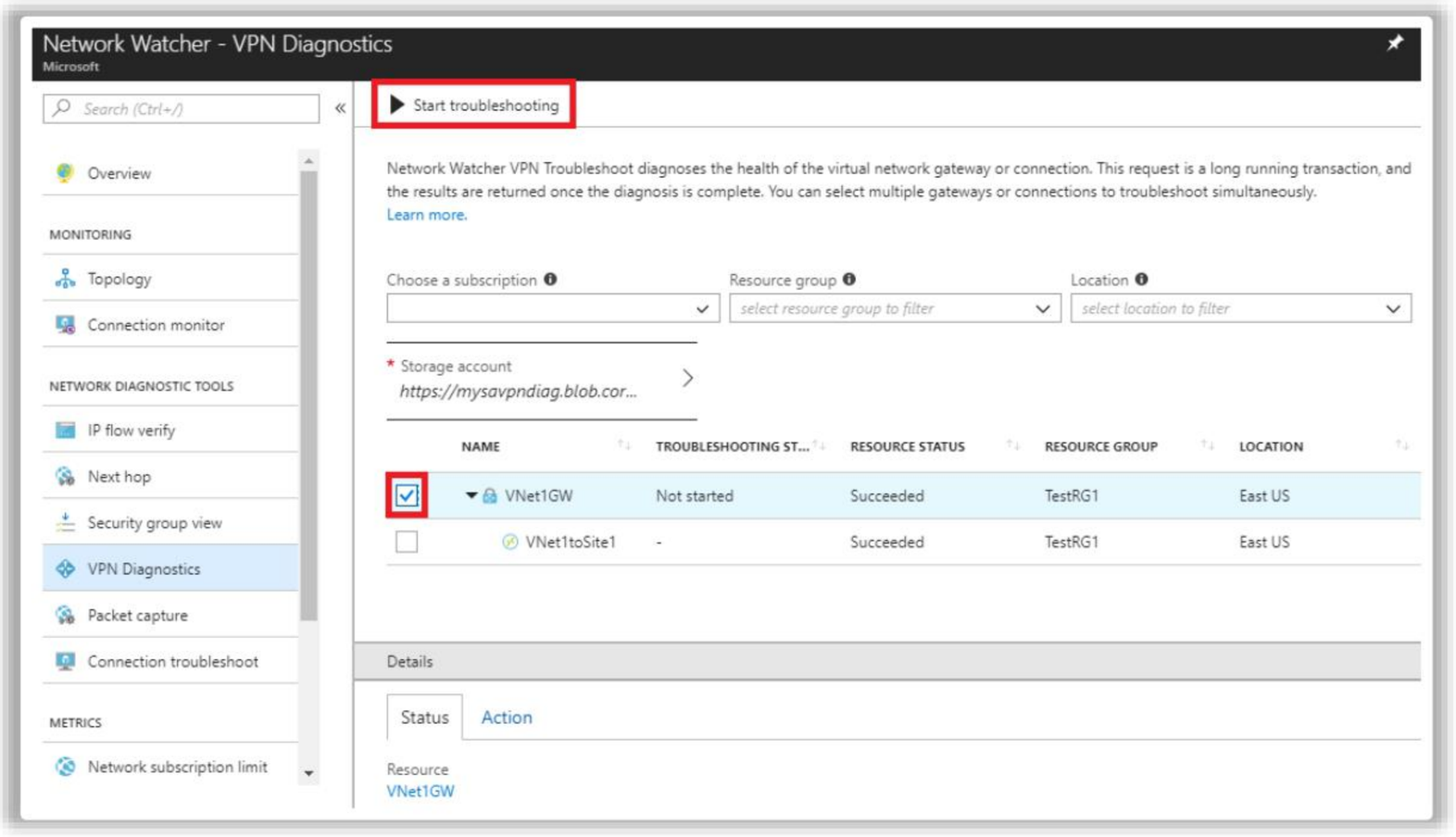


Figure 5.111: VPN Diagnostics

- **RUNNING** is shown in the **TROUBLESHOOTING STATUS** column when the test is in progress. See the status of the test once it is complete. The results of the completed diagnostic test are shown in the following screenshot.

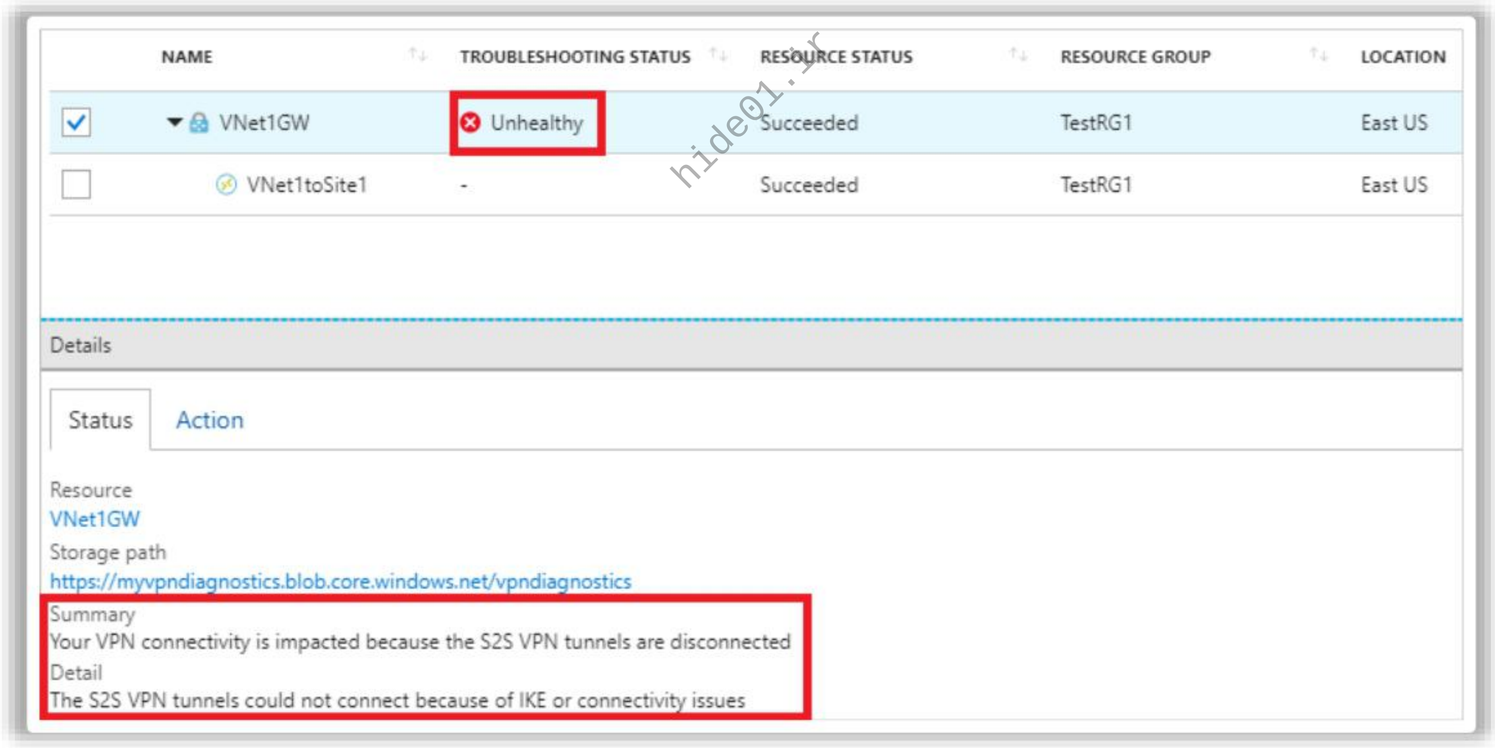


Figure 5.112: Troubleshooting Result

- Check additional information from the Action tab for the Unhealthy gateway. In the below screenshot, according to VPN diagnostics, the health of each connection should be checked.

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

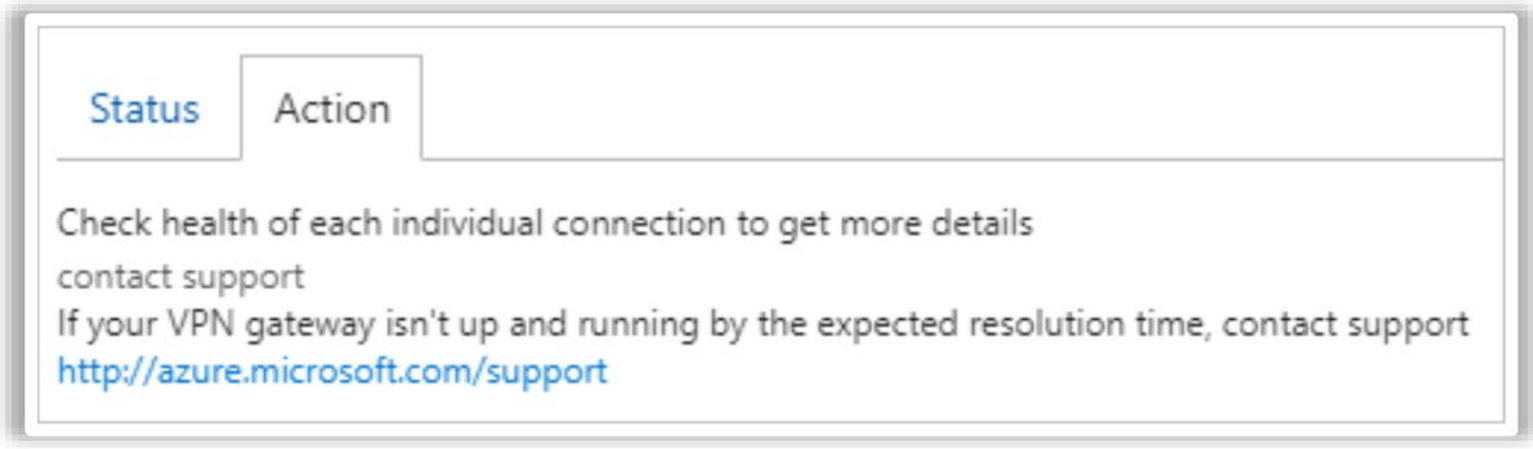


Figure 5.113: Actions

- Diagnose a gateway connection after detecting an Unhealthy gateway:
  - Choose a gateway connection and click on **Start troubleshooting,** as shown in the following screenshot (VNet1toSite1 connection is tested).

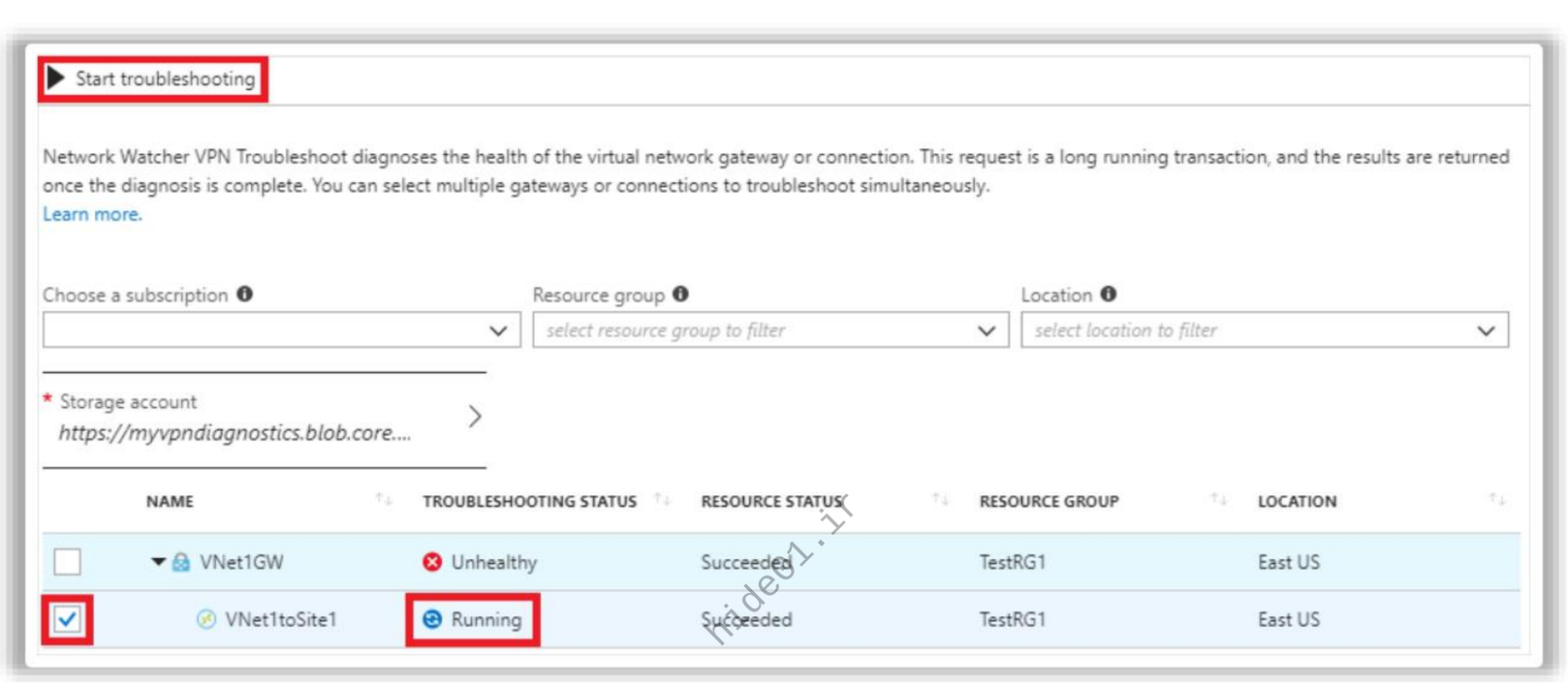
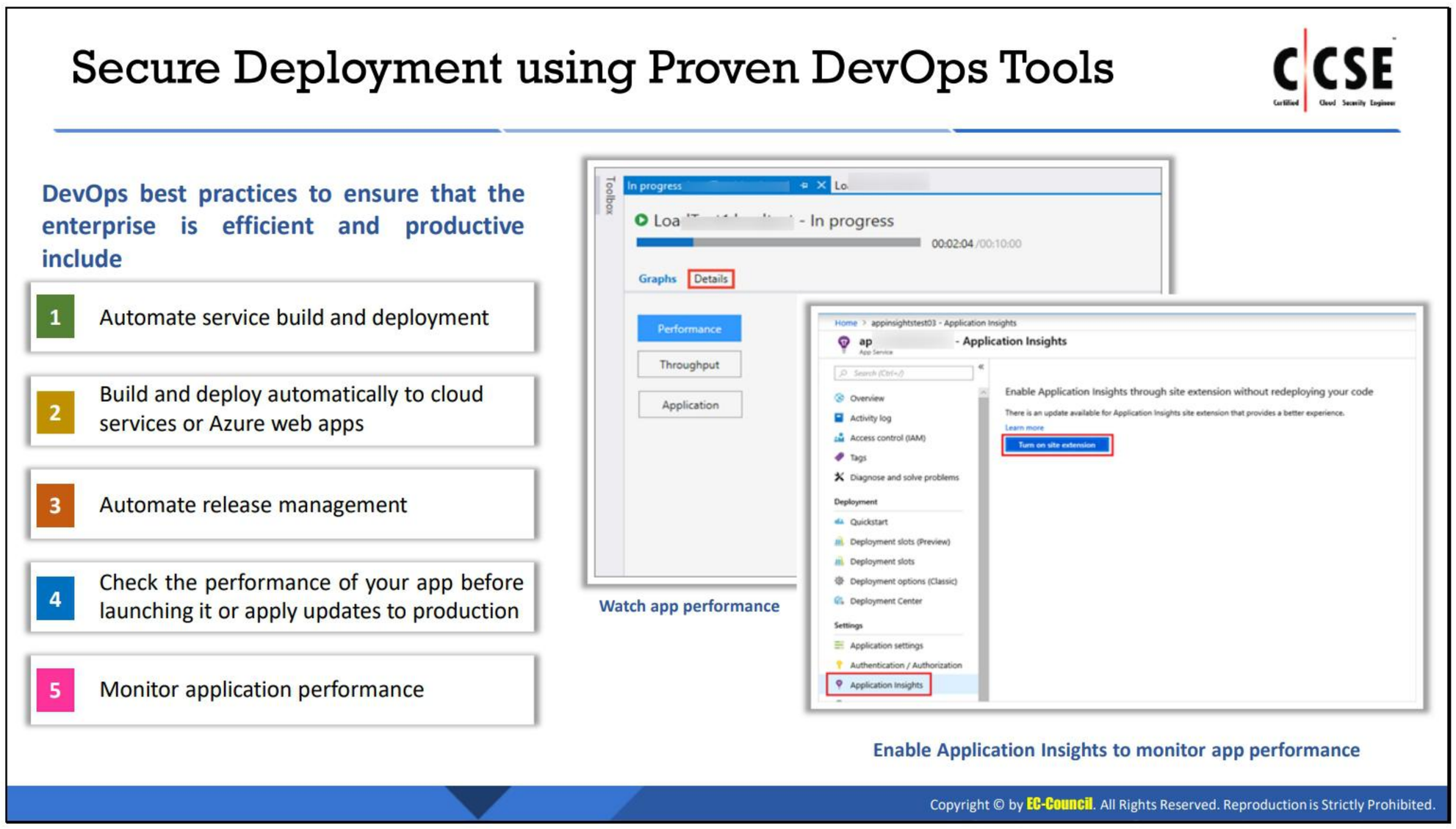


Figure 5.114: Start Troubleshooting

- After test completion, check the **Status** and **Action** tabs for more details regarding connection issues. The **Status** tab provides information about connection problems whereas the **Action** tab suggests the causes of the problem.

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



Secure Deployment using Proven DevOps Tools

Enforce the following DevOps best practices to make the organization efficient and productive.

Automate service build and deployment

Use the infrastructure as code to build and deploy services. It is a collection of best practices and techniques that help IT professionals offload their burden of building and managing modular infrastructure. Provision applications using a declarative template with the help of Azure Resource Manager (ARM). Use the same template multiple times to deploy an application in each stage of the application lifecycle. You can deploy multiple services along with the dependencies in a single template.

Build and deploy automatically to cloud services or Azure web apps

Configure Azure DevOps Projects to build and deploy automatically to Azure cloud services and web apps. After doing a build, the binaries are automatically deployed to Azure by Azure DevOps after every code check-in. The package build process in Azure DevOps is similar to the Package Command in Visual Studio. The publishing steps are similar to the Visual Studio Publish Command.

Automate release management

Manage and automate the release process using Azure pipelines. Azure pipelines help IT professionals by building and testing code projects automatically and providing them to others. They can be used to consistently and constantly check and build code and send it to any target. Azure pipelines allow IT professionals to establish predefined approval workflows and automate the release process.

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

Check the performance of your app before launching it or apply updates to the production

Run a cloud-based load test to check the performance of your application. Running cloud-based load testing helps to

- Detect performance issues in the application
- Improve deployment quality
- Ensure the availability of application
- Ensure that the application is capable of handling traffic

Monitor application performance

Monitor live web applications using Azure Application Insights. The application performance management service, Azure Application Insights, can detect anomalies automatically. This service helps in diagnosing performance issues and improving usability and performance. Enable Azure Application Insights to monitor ASP.Net and ASP.Net Core web applications that run on Azure App Services.

Steps to enable Application Insights

- Go to the Azure control panel for your app service and select **Application Insights**. Click on **Turn on site extension**.

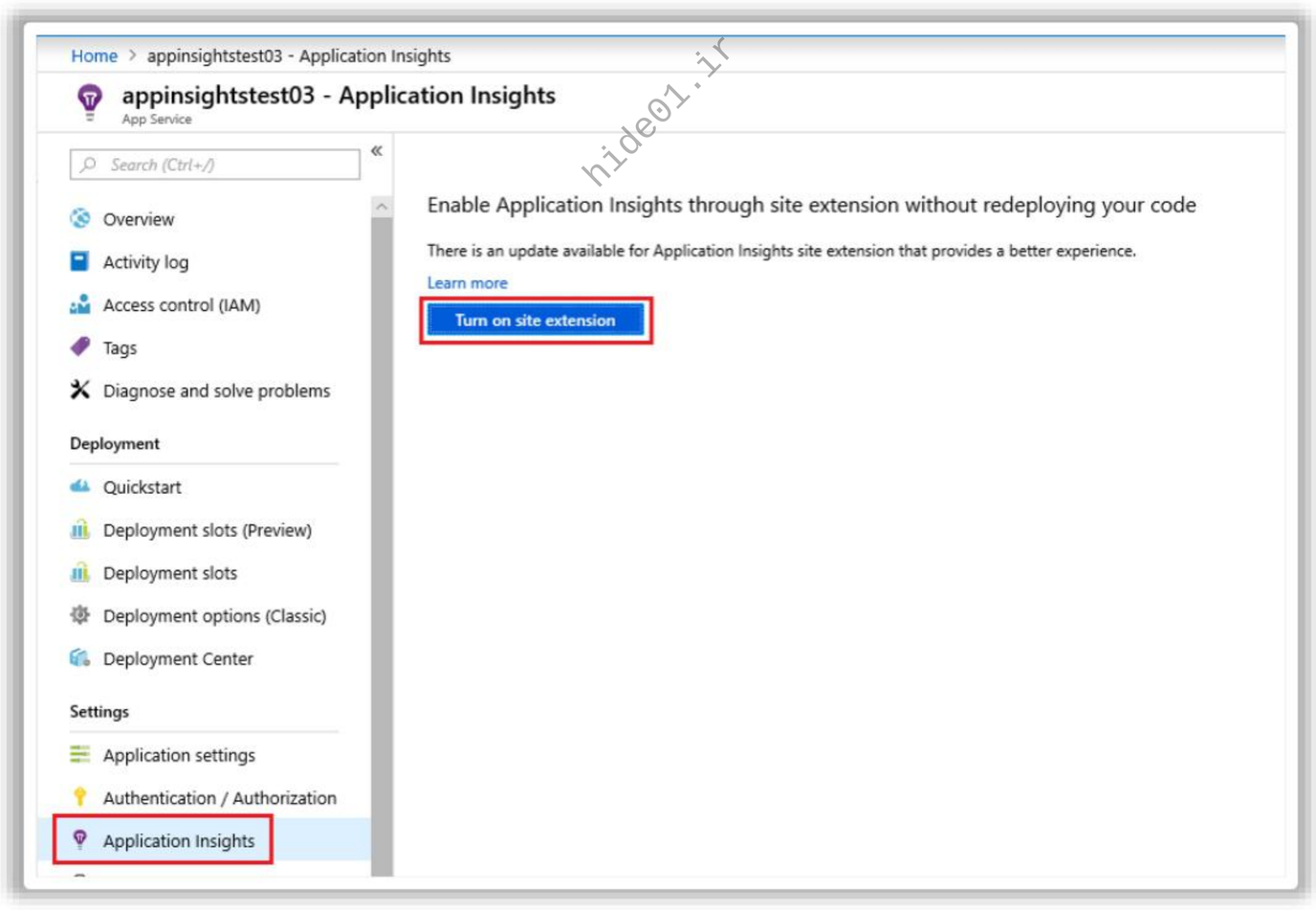


Figure 5.115: Application Insights

- Create a new resource if you have not already set up an Application Insights resource for your application. After creating the resource, you will be directed to **Apply monitoring settings**. Click on **Continue** to link the new Application Insights resource to the app service.

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

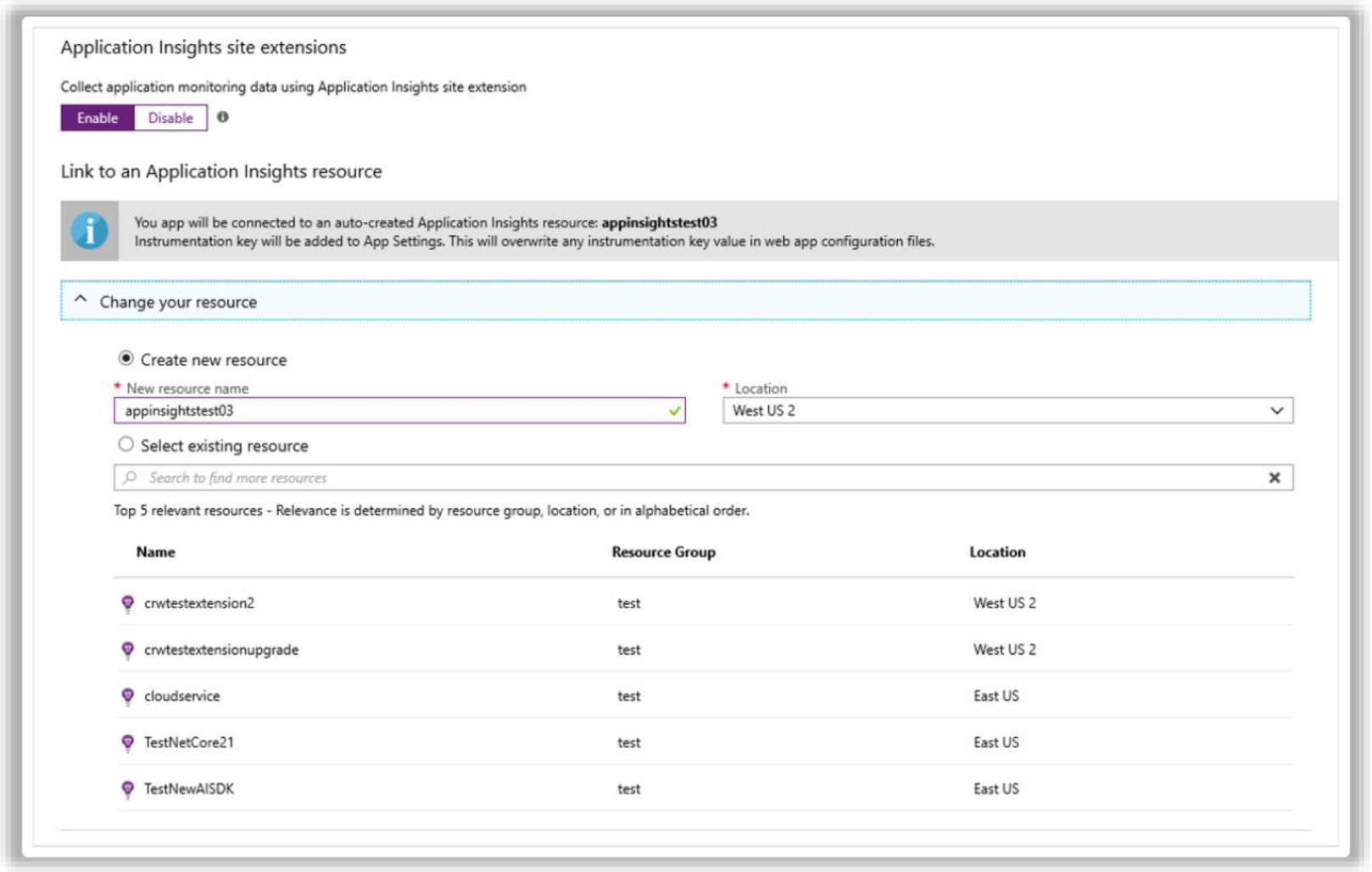


Figure 5.116: Setting

- Select how Application Insights should collect data for the application. ASP.Net monitoring is enabled by default and supports two different levels of data collection. Choose one from these two based on the requirements.

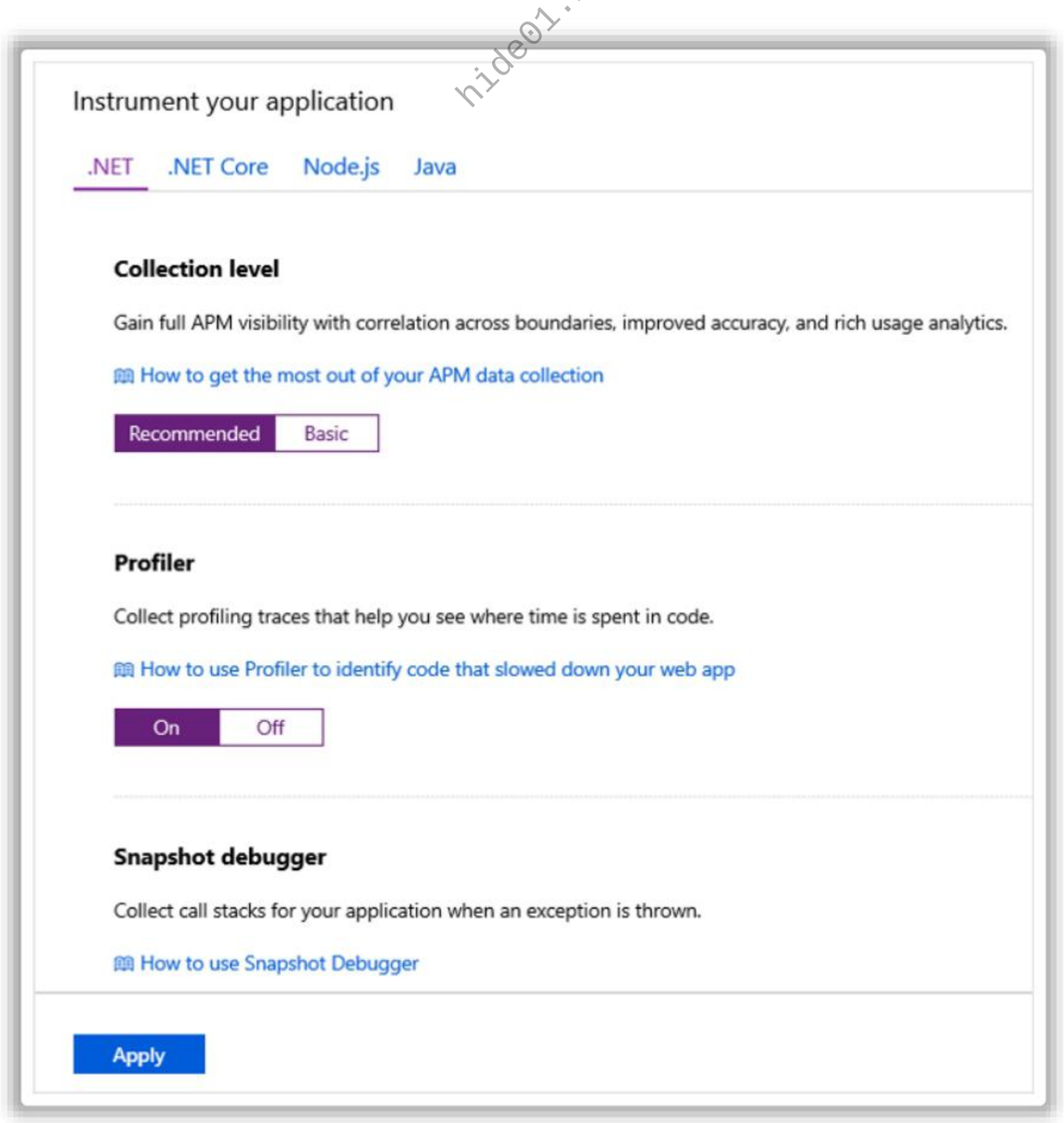
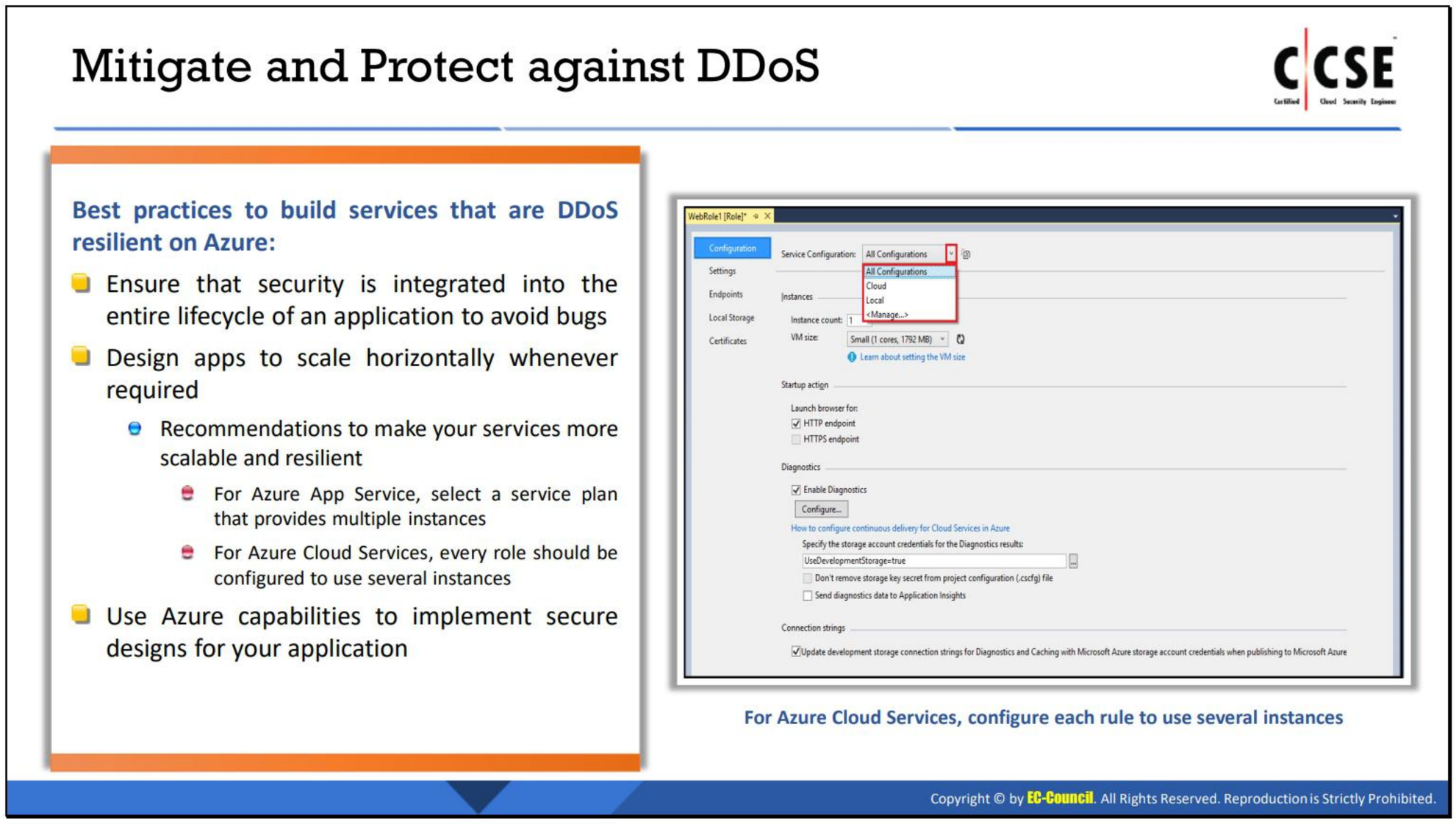


Figure 5.117: .NET

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



Mitigate and Protect against DDoS

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. Thorough planning and designing are required while building applications and services for DDoS resiliency.

To safeguard the Microsoft Azure Environment against network-based attacks, Azure offers the following services:

- **Basic protection**: This protection is provided by Azure without any additional cost because it is integrated into Azure by default. With basic protection, Azure protects against common network-layer attacks by continuous traffic monitoring and real-time mitigation. Azure basic protection does not require any application change or user configuration. It helps to secure all Azure services, and even PaaS services such as Azure DNS.
- **Standard protection**: This Azure service offers advanced DDoS mitigation capabilities to prevent network attacks. It offers protection to specific Azure resources. Standard protection can be enabled while creating virtual networks or even after creating them without any resource or application change.

Azure best practices for building services that can mitigate DDoS attacks

- **To prevent bugs, integrate security throughout the application lifecycle**

  Some low-volume requests are allowed by applications that are affected by bugs, which lead to the consumption of numerous resources and cause service outages. Understand the application architecture of a service running on Azure to protect it from security issues. Ensure that the application has DDoS resiliency and does not get affected by DDoS

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

attack attempts. Ensure that security is integrated into the entire lifecycle of the application so that no bugs or errors can make DDoS attacks successful.

Azure provides privacy and security as its in-built platform features. Use the security features provided by Azure to protect the services on Azure.

- **Design apps to scale horizontally whenever required**

  Ensure that applications are designed to scale horizontally when there is an increased load to meet the demand. It is essential to handle DDoS attacks. Applications with only one instance of service can encounter a single point of failure whereas providing many instances for service will make the system resilient and easily scalable.

Recommendations to make your services more scalable and resilient

- For Azure App Service, select a service plan that provides multiple instances.
- For Azure Cloud Services, roles should be configured such that they can use multiple instances.

  Follow the steps given below to change the number of instances for a particular role:

  - In VS, open or create an Azure cloud service project.
  - Expand the project node in **Solution Explorer**. Under **Roles**, right-click a role and select **Properties** from the context menu.

hadeo_ir

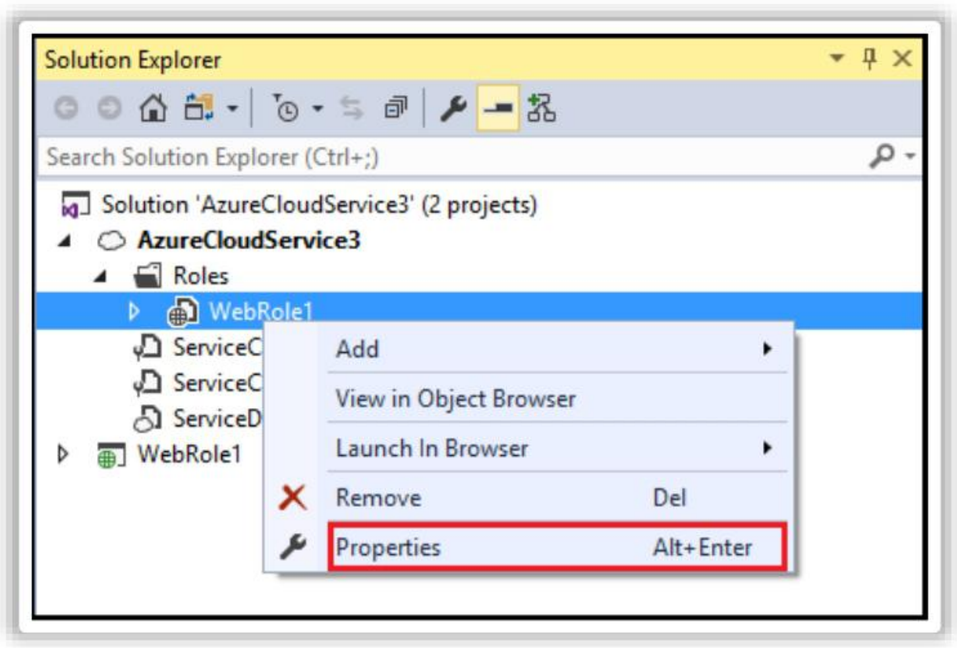


Figure 5.118: WebRole1

- Click on **Configuration**.

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

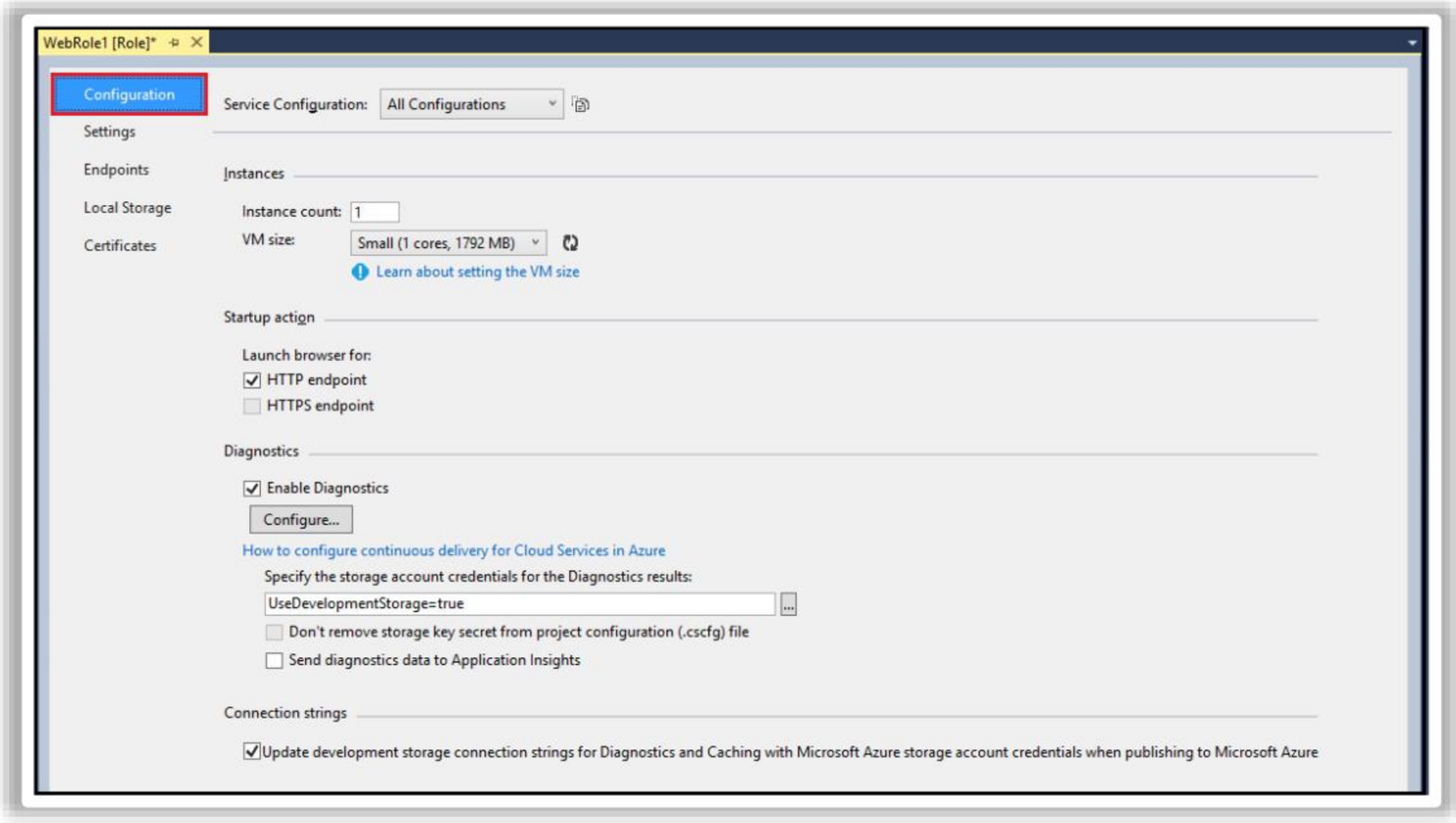
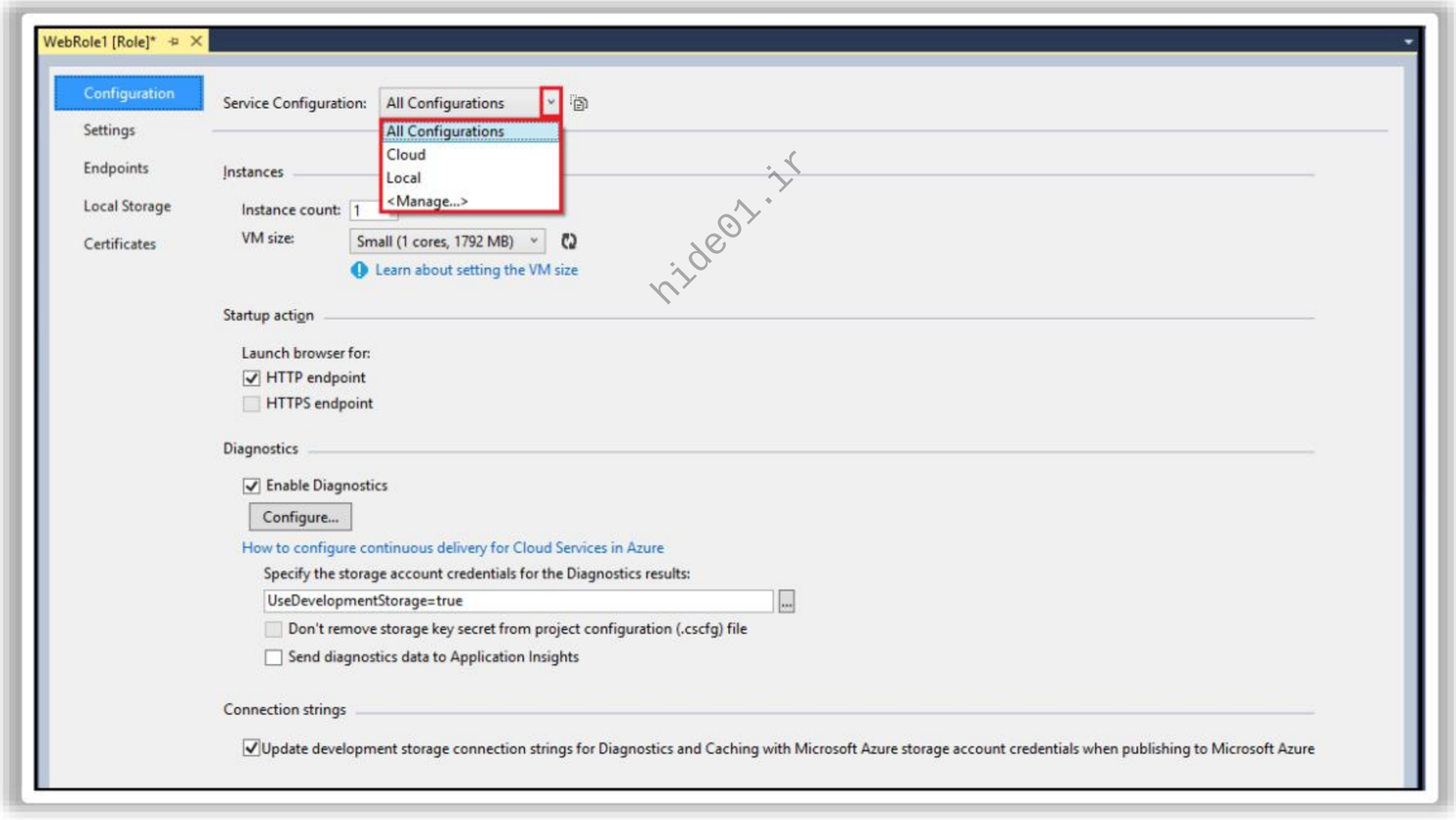


Figure 5.119: Configuration

- Choose the service configuration that needs to be updated from the **Service Configuration** list.



hide01.ir

Figure 5.120: All Configuration

- Enter the number of instances that should be started for this role in the **Instance count** box. When the cloud service is published to Azure, each instance will run on a separate VM.

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

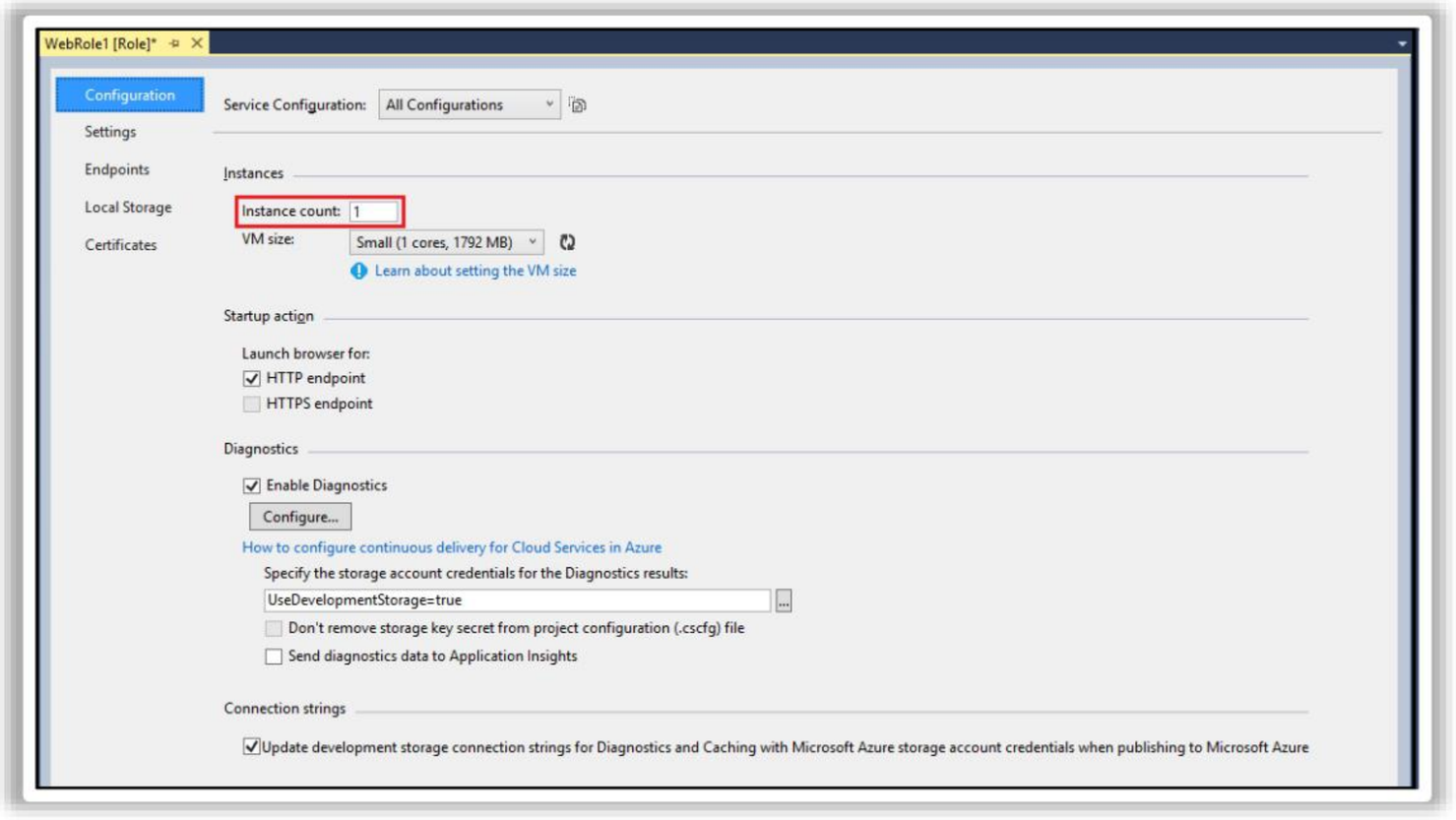


Figure 5.121: Local Storage

- Click on **Save** from the toolbar in VS.

- For Azure VMs, make sure that your VM architecture contains multiple VMs and each VM must be included in an availability set. For auto-scaling capabilities, use VM scale sets.

- **Use Azure capabilities to implement secure designs for your application**

  Reduce the attack surface by layering security defenses in the application. Security recommendations that use Azure capabilities to implement security include:

  - Use an approval list to disable the listening ports and exposed IP address space that are not required on load balancers.
  - Reduce the exposure of on-premises resources to the internet while connecting those resources to Azure to protect them from being attacked.
  - Deploy Azure services in a VNet (wherever possible) to keep them secure because service resources can communicate via private IP addresses.
  - Use Network Security Groups (NSGs) to configure network security.
  - Use NSGs to monitor and filter network traffic and reduce the attack surface. NSGs can filter network traffic to and from a VNet subnet. NSGs contain security rules that filter traffic based on ports, protocols, and IP addresses.

Source: https://www.microsoft.com

Steps to create NSG to filter traffic

Follow the steps to create an NSG and associate it to a subnet.

- Log into the Azure portal. To create a VNet, follow the steps given below:
  - Select **Create a resource** from the portal menu.

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

- Select **Networking** and click on **Virtual network**.
- Enter the name (myVirtualNetwork) and other requested details. Click on **Create.**

- Create an application security group via the following steps:
  - Choose **Create a resource** from the portal menu.
  - Type "application security group" in the **Search the Marketplace** box. Select it when it appears in the result. Under **Everything**, followed by **Application security group,** and click on **Create**.
  - Provide the name (myAsgWebServers) and other details. Click on **Create**.
  - Repeat the above step with a different name (myAsgMgmtServers).
- Create an NSG by following these steps:
  - Click on **Create a resource** from the portal menu.
  - Choose **Networking** and click on **Network security group**.
  - Enter the name (myNsg) and other details. Click on **Create**.
- Now, associate the NSG to a subnet:
  - Type 'myNsg' in the **Search** box at the top of the portal. Select it when it appears in the result.
  - Choose **Subnets** under **SETTINGS** and select **+ Associate**.

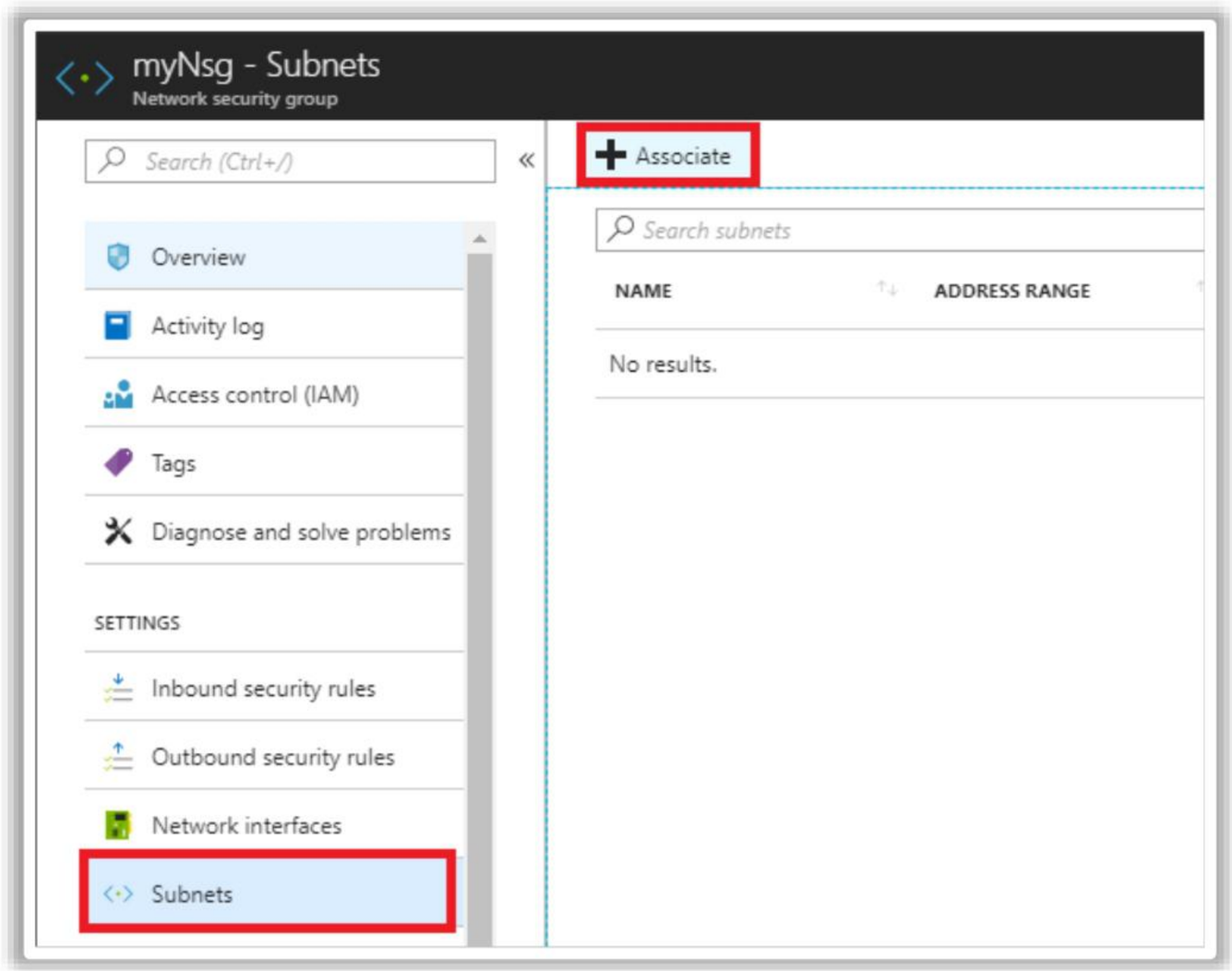


Figure 2.122: Subnets

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

- Select **Virtual network** under **Associate subnet** and click on **myVirtualNetwork**. Select **Subnet**, followed by **mySubnet**, and click on **OK**.

○ Create security rules using these steps:

- Choose **Inbound security rules** under **SETTINGS** and click on **+ Add.**

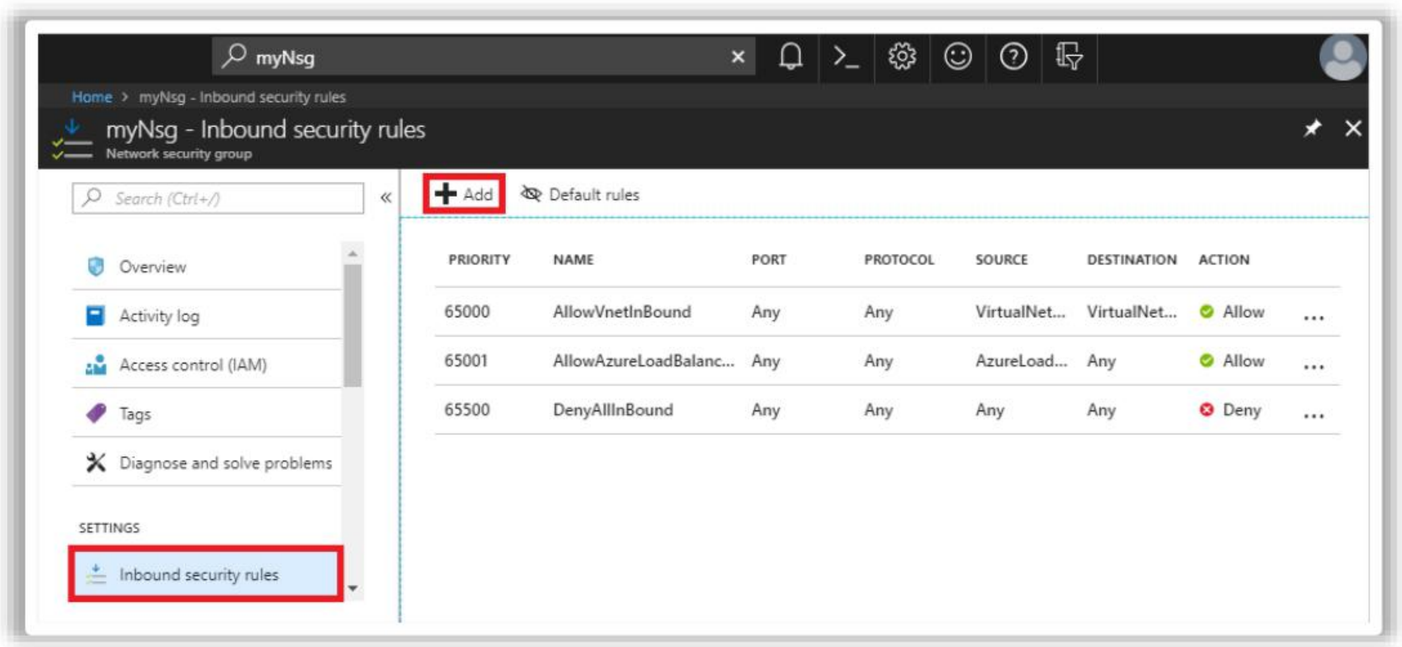


Figure 5.123: Add

- Create a security rule that provides ports 443 and 80 to the (myAsgWebServers) ASG. Enter the following information under **Add inbound security rules** and click on **Add**.
  - **Destination**- Select myAsgWebServers for App security group
  - **Destination port ranges**- 80, 443
  - **Protocol**- TCP
  - **Name**- Allow-Web-All
- Repeat the above step with the following values:
  - **Destination**- Select myAsgMgmtServers for App security group
  - **Destination port ranges**- 3389
  - **Protocol**- TCP
  - **Priority**- 110
  - **Name**- Allow-RDP-All
- The rules created in the above steps look similar to the list shown in the screenshot below:

hide01.ir

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

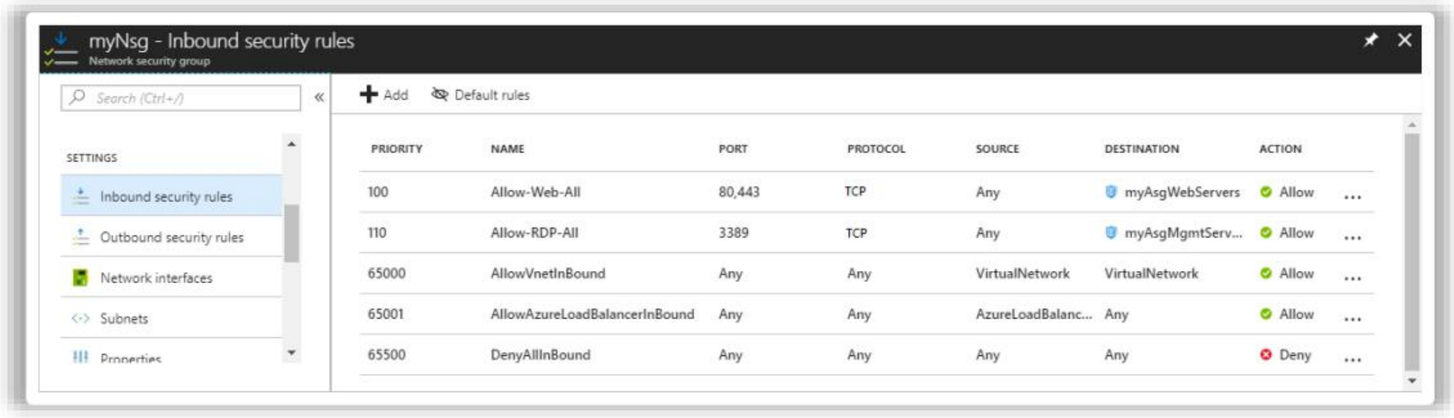


Figure 5.124: Inbound Security Rules

- Create two VMs in VNet:
  - Click on **Create a resource** from the portal menu.
  - Click on **Compute** and choose **Windows Server 2016 Datacenter.**
  - Enter the name (myVmWeb) and other details.
  - Choose the VM size and click on **Select**.
  - Under **Networking**, accept the defaults and select the following given values:

    a. **Virtual network**- myVirtualNetwork

    b. **NIC NSG**- none
  - Choose **Review + Create** and click on **Create** to begin VM deployment.
  - Similarly, create another VM with the name "myVmMgmt."
- Associate each VM network interface to an ASG:
- Search for and select "myVmWeb" in the **Search** box available at the top of the portal.
- Choose **Networking** under **SETTINGS**. Click on **Configure the application security groups;** for **Application security groups**, choose **myAsgWebServers**.

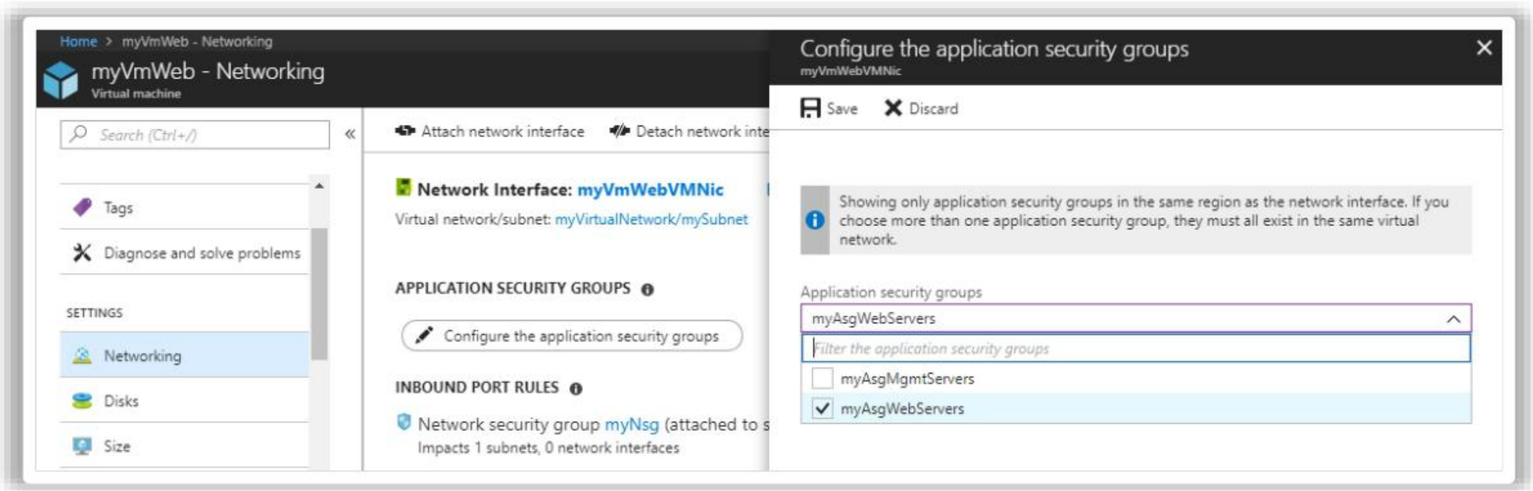
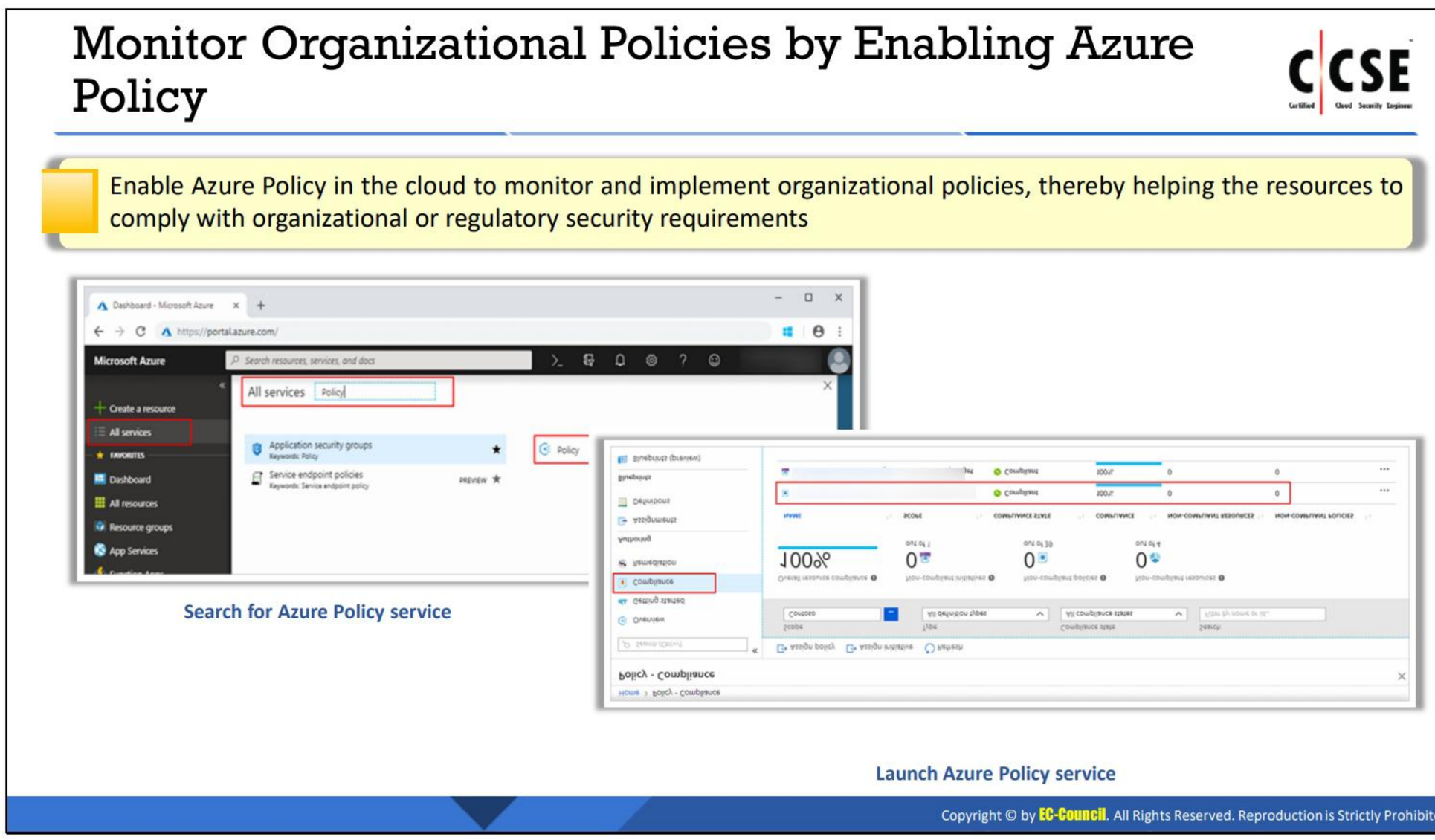


Figure 5.125: Networking

- Now, search and select "**myVMMgmt"** VM, repeat the above step, and choose **myAsgMgmtServers** for **Application security groups**.

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



Monitor Organizational Policies by Enabling Azure Policy

The Azure service "Azure Policy" is used to create, assign, and manage policies that are applied to resources. These policies ensure that cloud resources remain compliant with SLAs and corporate standards. With the help of assigned policies, Azure Policy evaluates resources for non-compliance.

Enable Azure Policy in the cloud to monitor and implement organizational policies. This will help the resources to comply with organizational or regulatory security requirements.

Steps to identify non-compliant resources with Azure Policy

Source: https://www.microsoft.com

Create a policy assignment with the policy definition "Audit VMs that do not use managed disks."

- Choose **All services** on the Azure portal; search and select **Azure Policy** to launch Azure Policy service.

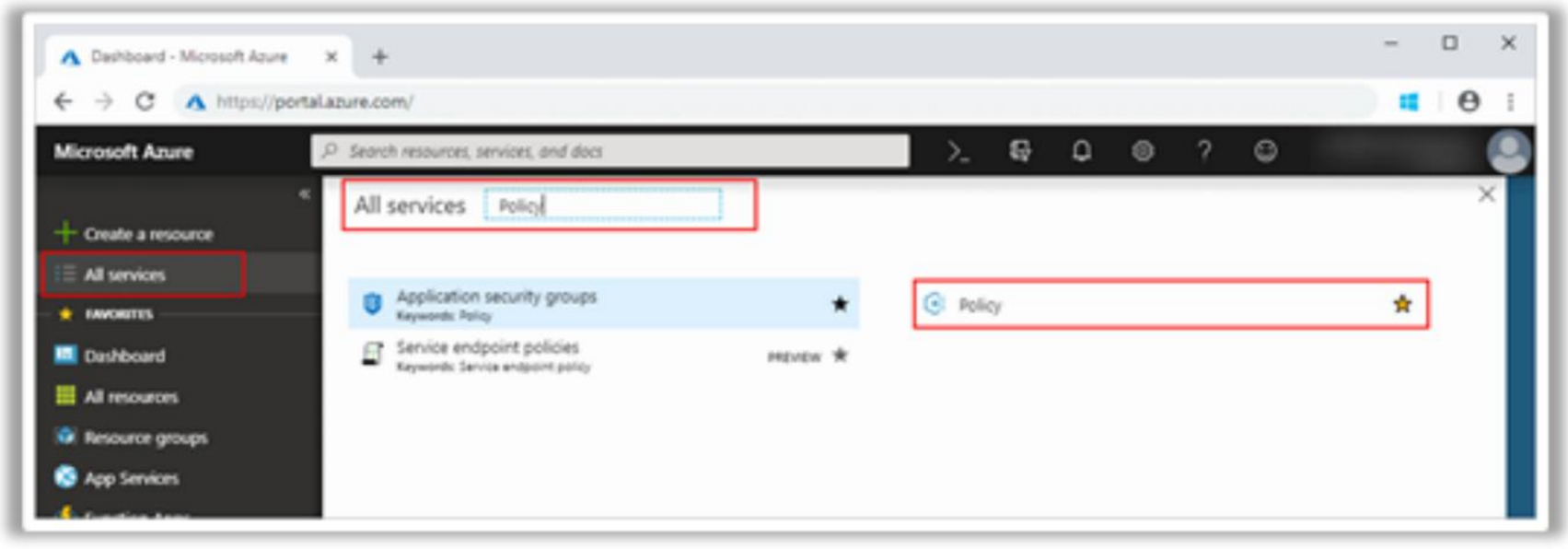


Figure 5.126: Policy

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

- Select **Assignments** on the **Azure Policy** page.

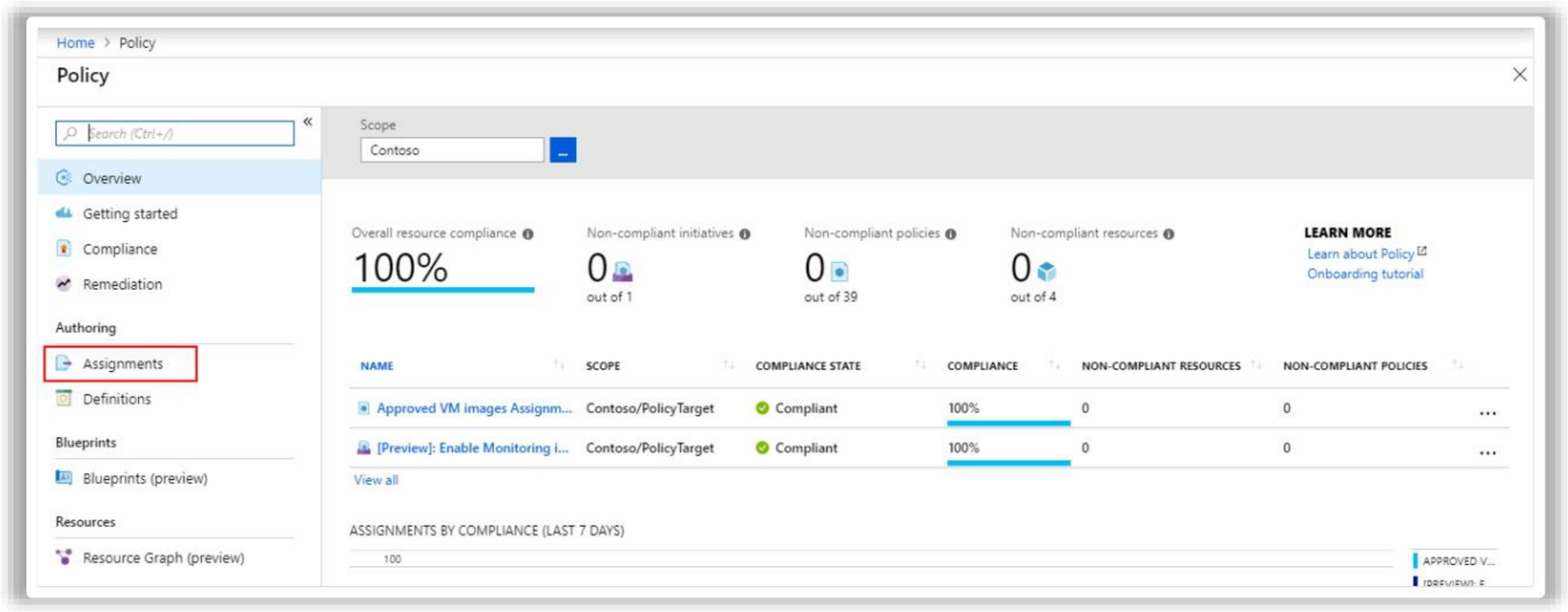


Figure 5.127: Policy

- On the **Policy - Assignment** page, select **Assign Policy**.

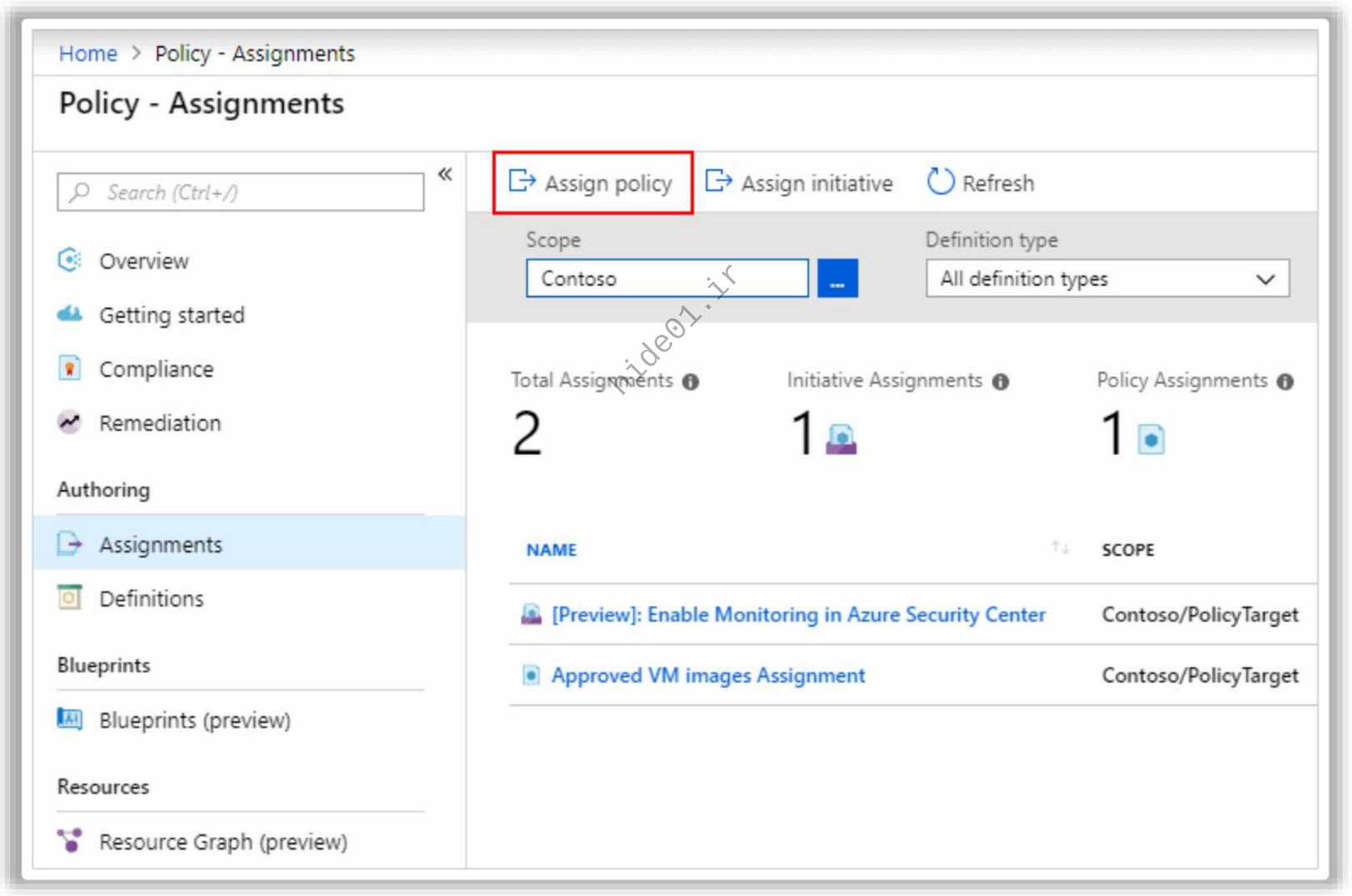


Figure 5.128: Assign Policy

- Set the **Scope** on the **Assign Policy** page by selecting **ellipsis;** either select a **subscription** or **management group**. The scope determines the resources on which policy assignment will be enforced.
- Choose the **Policy definition** ellipsis to view the available definitions. Find the policy definition "**Audit VMs that do not use managed disks**" and select it. Click on **Select**.

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

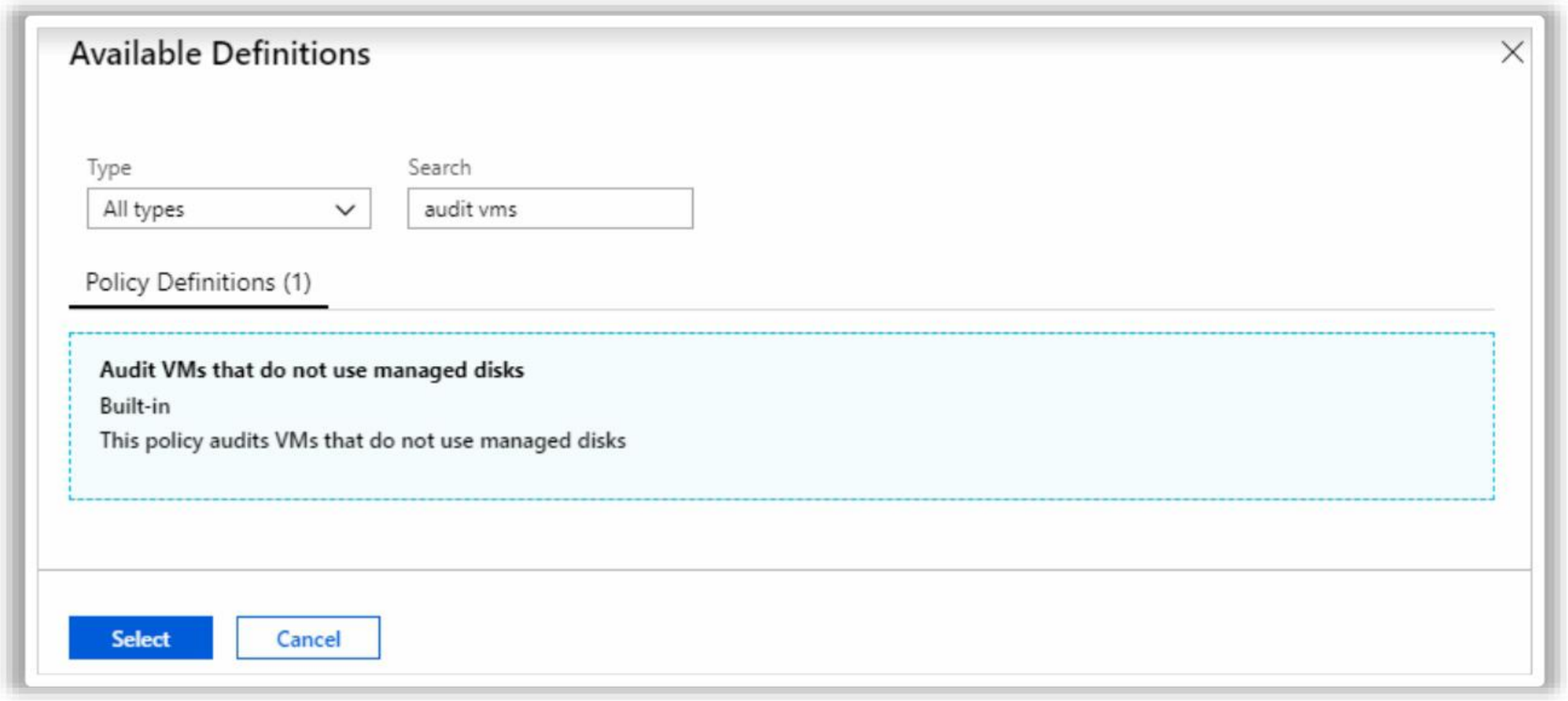


Figure 5.129: Available Definitions

- The **Assignment name** is the same as that of the selected policy, but it can be changed. Optionally, add **Description** for policy assignment.
- Ensure that policy enforcement is **Enabled** and click on Next to move to the **Parameters** tab.
- On this tab, the parameters included in policy definition selected on the **Basics** tab are configured. Click on **Next** (because the selected policy definition has no parameters) to go to the **Remediation** tab.
- Keep **Create a Managed Identity** unchecked and click on **Next** to move to the **Non-compliance messages** tab.
- Set "**Virtual machines should use a managed disk**" for the Non-compliance message. This custom message is displayed for non-compliance resources during evaluation. Click on **Next** to move to the **Review + Create** tab.
- Click on **Create** after reviewing the selected options; the assignment process can now identify non-compliant resources.
- Choose **Compliance** on the **Policy - Compliance** page and select "Audit VMs that do not use managed disks" policy assignment. Resources that are non-compliant with this policy assignment will appear under **Non-compliant resources.**

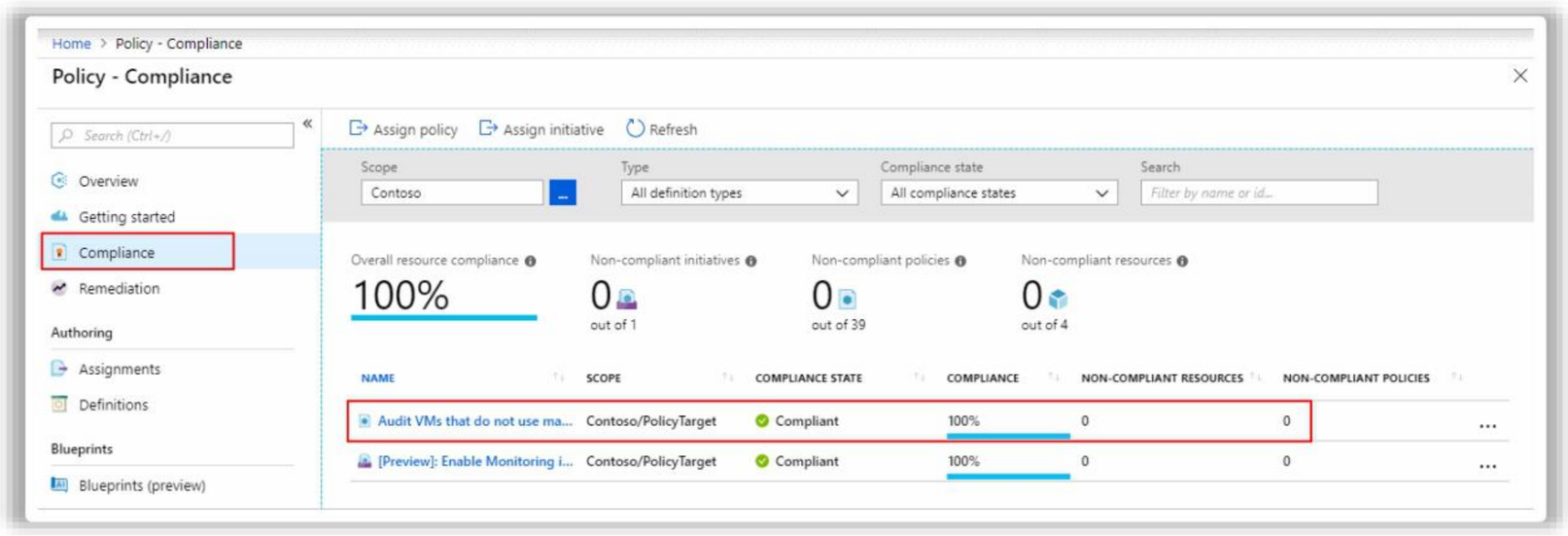


Figure 5.130: Compliance

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

After adopting the Azure Policy, follow these best practices:

- **Start policy deployments with the audit mode and later move to deny and remediate effect:**

  Azure Policy supports different types of effects such as append, audit, deny, and disabled. Avoid using deny and remediate effects while deploying Azure Policy because they may negatively affect business operations. Always start with the audit effect during policy deployment.

  - **Deny effect**: This effect fails the request and creates an event in the activity log.
  - **Audit effect**: This effect does not fail the request but generates a warning event in the activity log.
  - **Remediate effect**: This effect makes resources (that are non-compliant to a modify or deployIfNotExists policy) compliant.
  - Always start policy deployments with the audit effect and progress to remediate or deny effect. Before moving to deny and remediate effects, test and review the results of audit effects.

- **Identify the roles that should be monitored for policy violations and ensure that correct remediation actions are taken instantly:**

  Make the assigned role to monitor compliance using the Azure portal. To monitor compliance via the Azure portal, click on **Overview** on the **Policy** page. It displays the information for available scopes on the compliance of initiatives and policies. It has a chart that shows compliance over the past seven days along with the compliance state and count per assignment. This information can also be accessed on the **Compliance** page, except for the chart.

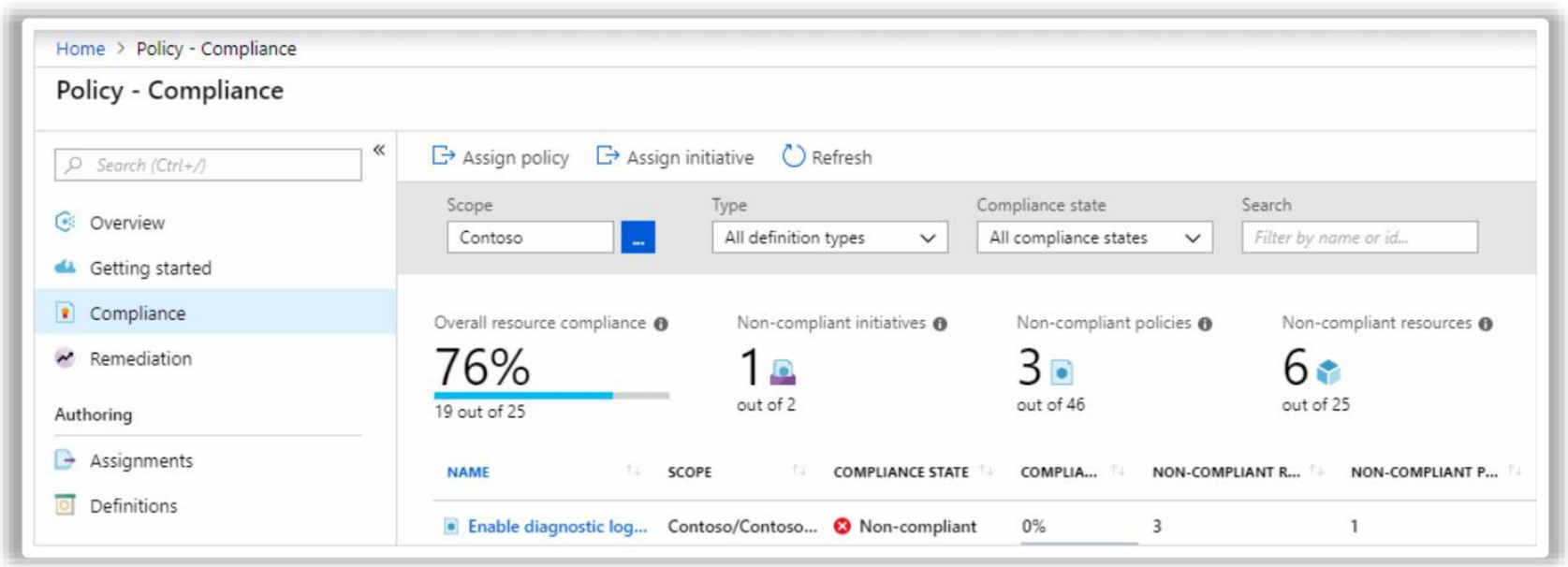


Figure 5.131: Compliance

- Choose a policy or initiative in the table to obtain more details regarding compliance for a particular assignment.

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

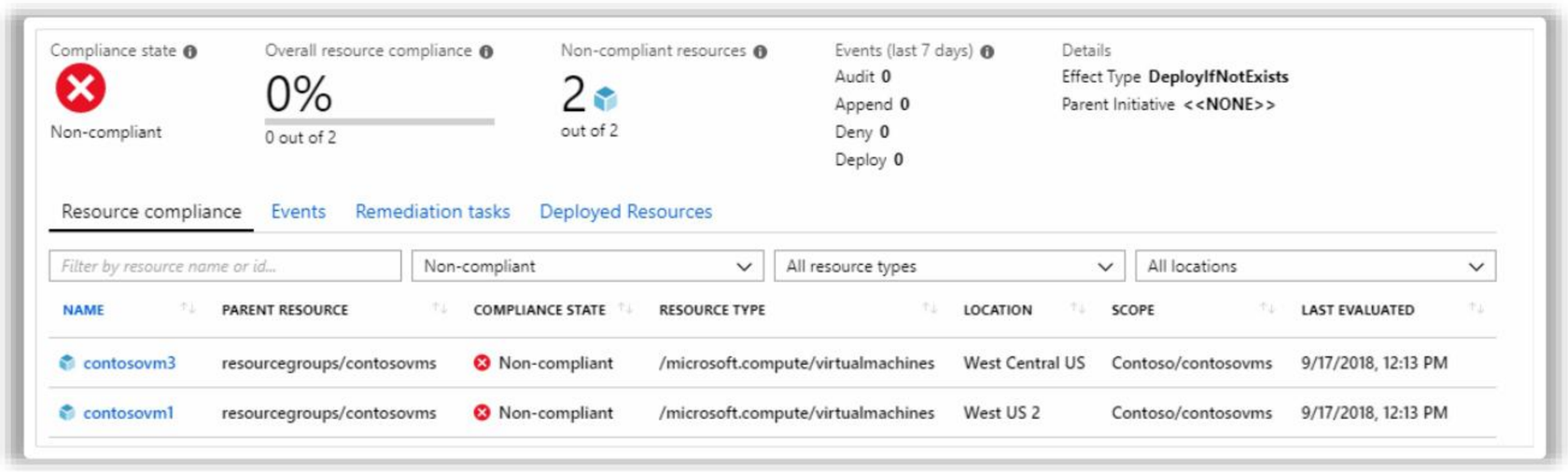


Figure 5.132: Resource Compliance

- The **Resource** tab contains a list of resources that displays the evaluation status for the assignment process. The **Events** tab shows the events that are triggered by requests to create a resource.

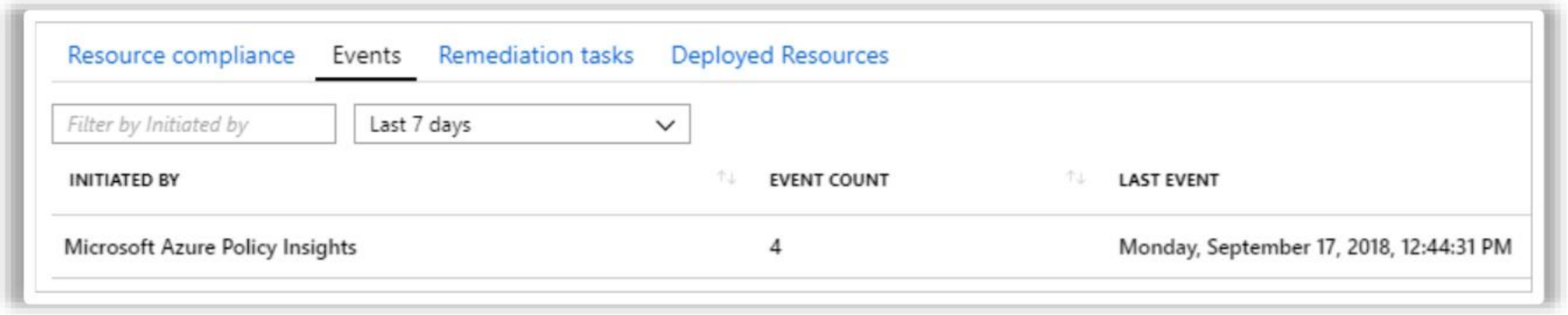


Figure 5.133: Events

- On the **Resource compliance** tab, select a resource, followed by **View compliance details** to view component compliance details, policies, events, component events, and change history.

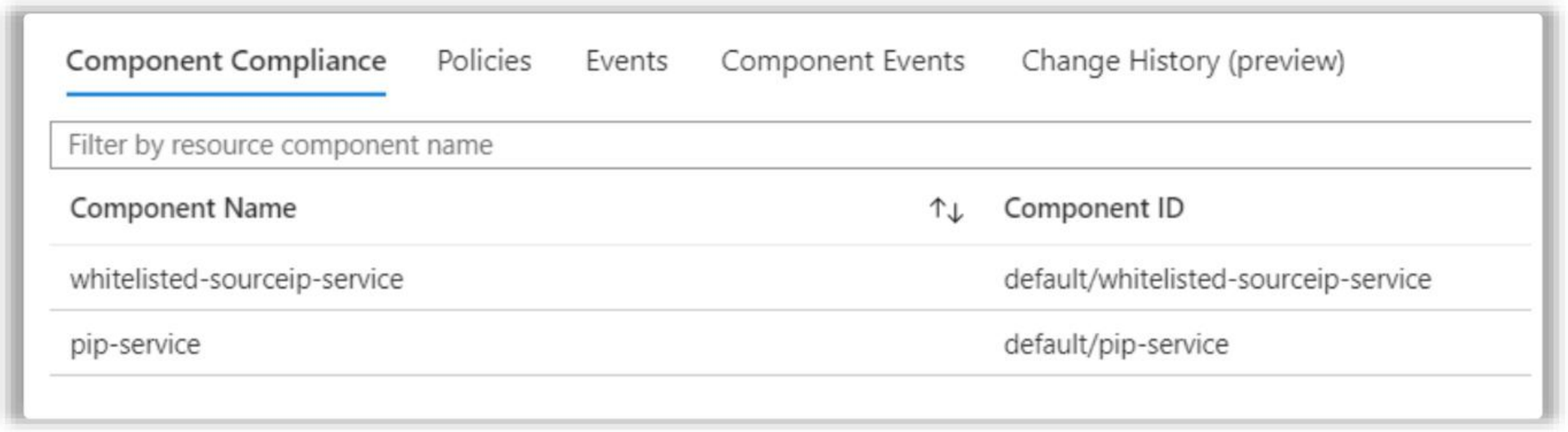


Figure 5.134: Components Compliance

- Click on **Show activity logs** on the **Resource compliance** page to know additional context and information about events.

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

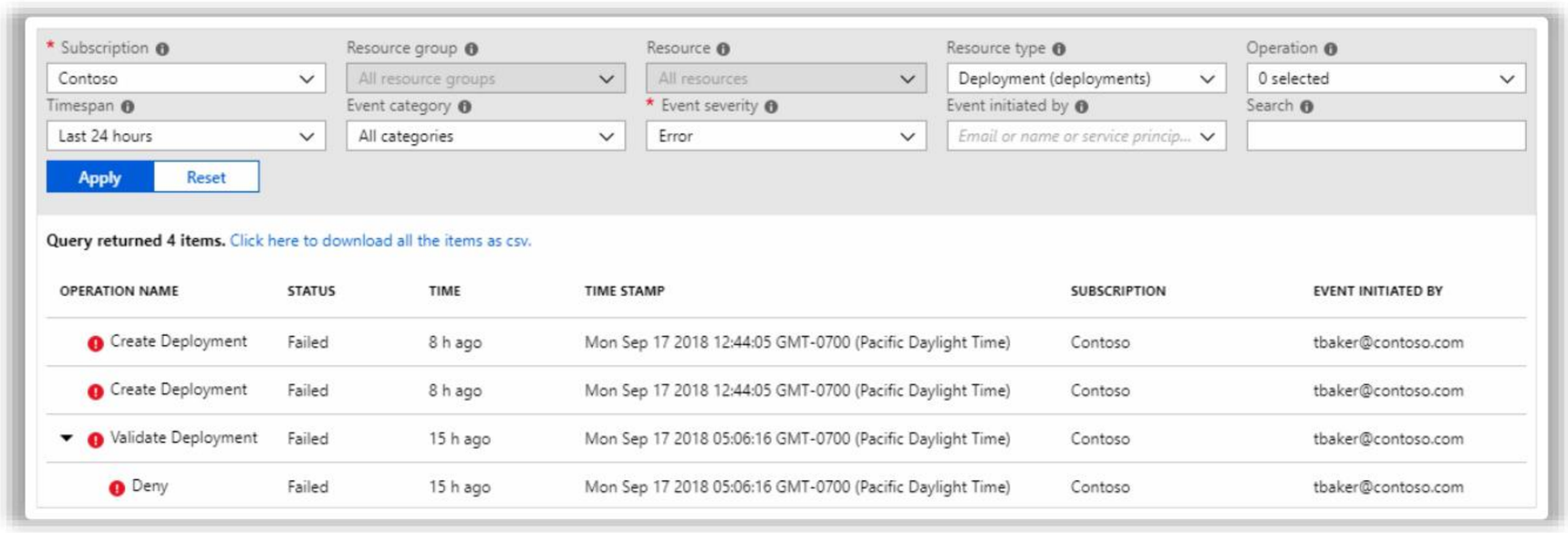


Figure 5.135: Apply

- **Map Azure policy definitions to your organizational policies to increase consistency and avoid confusion**

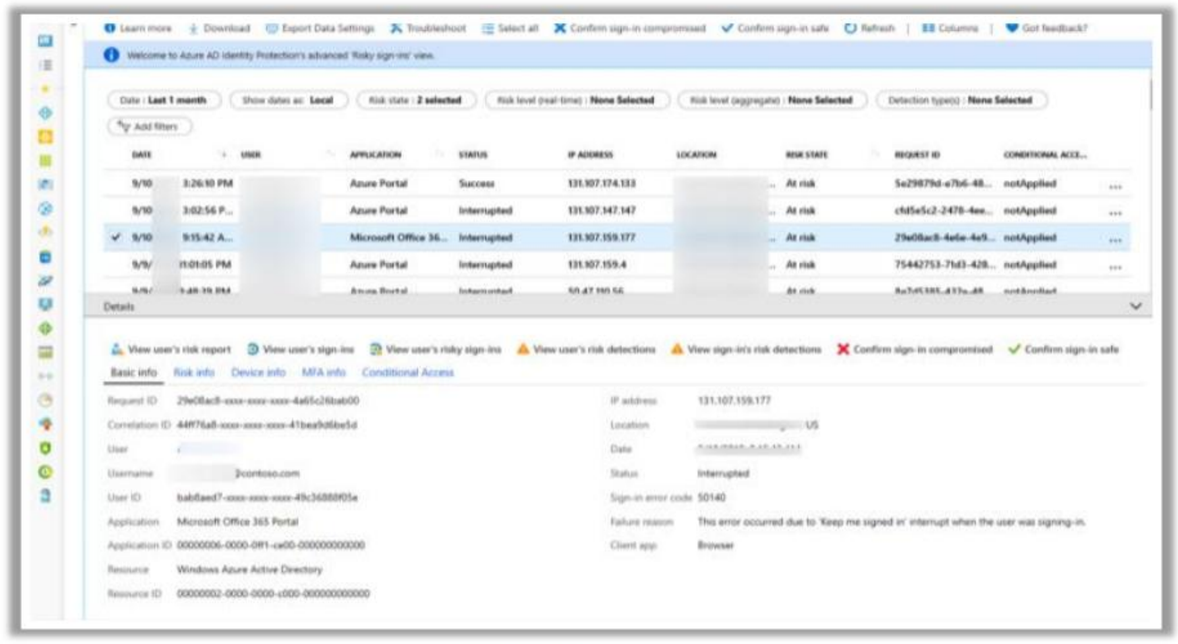
Because Azure Policy is a form of technical representation of the written policies of an organization, map all policy definitions to organizational policies. This will improve the consistency and prevent confusion. Ensure that this mapping is documented in organizational documentation or Azure Policy definition. It can be achieved by adding a reference to the organizational policy in the policy or initiative definition description.

hide01.ir

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

Monitor Azure AD Reports

- Use Azure AD reports (risky users, risky sign-ins, and risk detections) to record all suspicious actions, which are stored in a risk detection record
- Identify the three reports in **Azure portal -> Azure Active Directory -> Security**



Viewing Risky sign-ins

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

Monitor Azure AD Reports

Security breaches occur when an adversary steals user identity to perform suspicious actions. It is not easy to detect such malicious activities. However, Azure AD can effectively identify suspicious actions related to a user account using its advanced machine learning algorithms. All suspicious actions are stored in a risk detection record. The detection of these risks is recorded in AD security reports.

Azure Identity Protection offers three reports (risky users, risky sign-ins, and risk detections) to help organizations investigate the identity risks present in their environment. Risk detection reports contain data from up to the past three months. Cloud admins can find important information such as type of risk detected, sign-in attempt location, and other associated risks from risk detection reports.

Access Azure AD security reports by following these steps:

- Log into the Azure portal as a global administrator, search for **Azure AD,** and select it.
- Click on **Security** to access the reports.

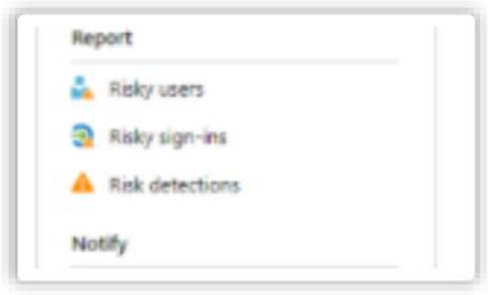


Figure 5.136: Report

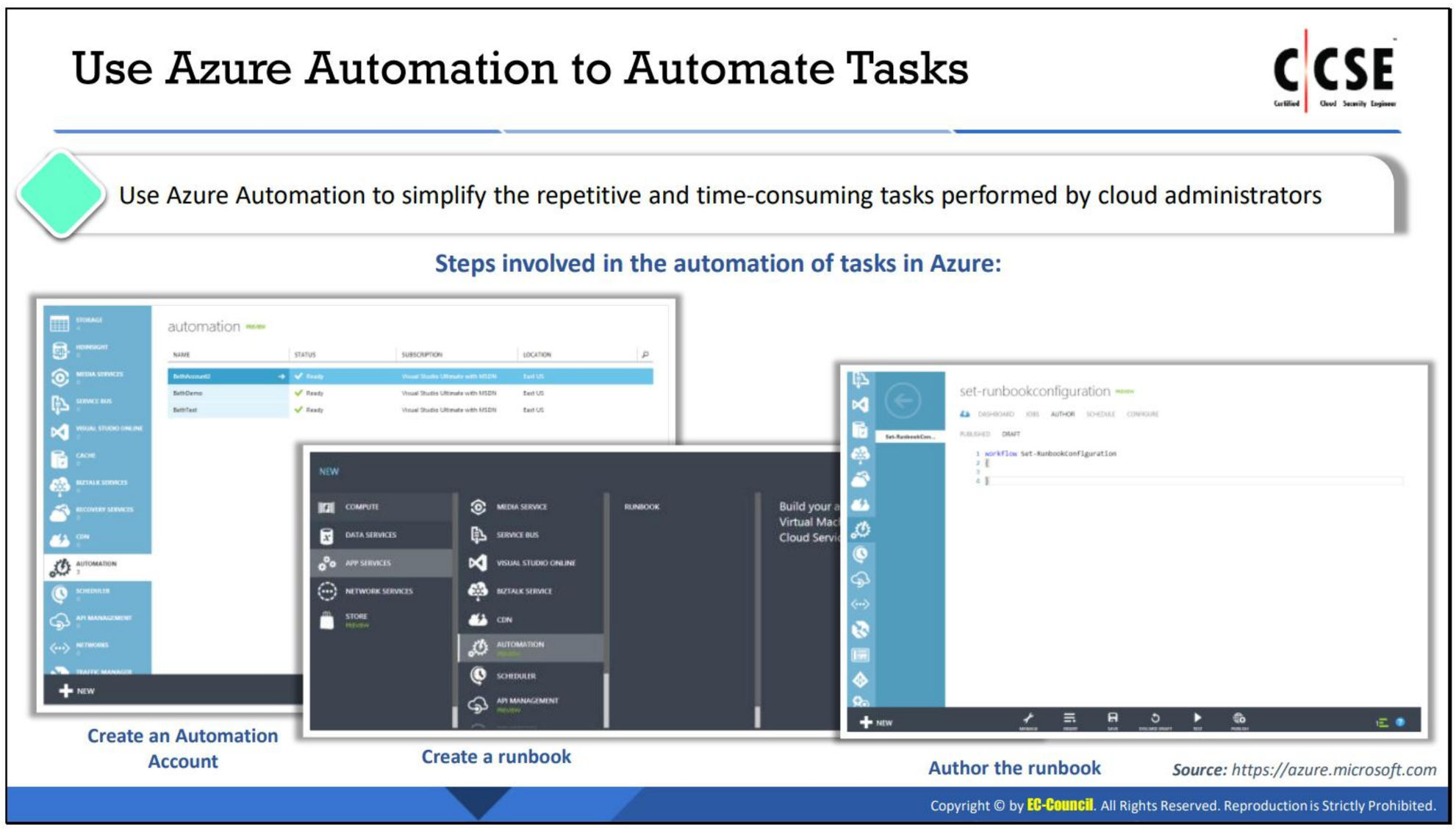
Download the reports in .CSV format for further investigation and analysis. risky sign-in and risky user reports can contain 2500 recent entries, whereas risk detection reports can

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

contain 5000 recent records. Next, access reports that contain a list of findings or detections for a particular period.

hide01.ir

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



Use Azure Automation to Automate Tasks

Azure Automation helps in creating and scheduling workflows to simplify the repetitive and time-consuming tasks performed by cloud administrators. It uses runbooks to perform repetitive tasks such as backup management, resource management, server patching, and log management.

Source: https://www.microsoft.com

Steps to use Azure Automation to automate tasks

- **Enable Azure Automation service**
  - Login to your Azure subscription.
  - Type "**Automation**" in the search bar and press **Enter**. Choose **Automation Accounts** from the search results.

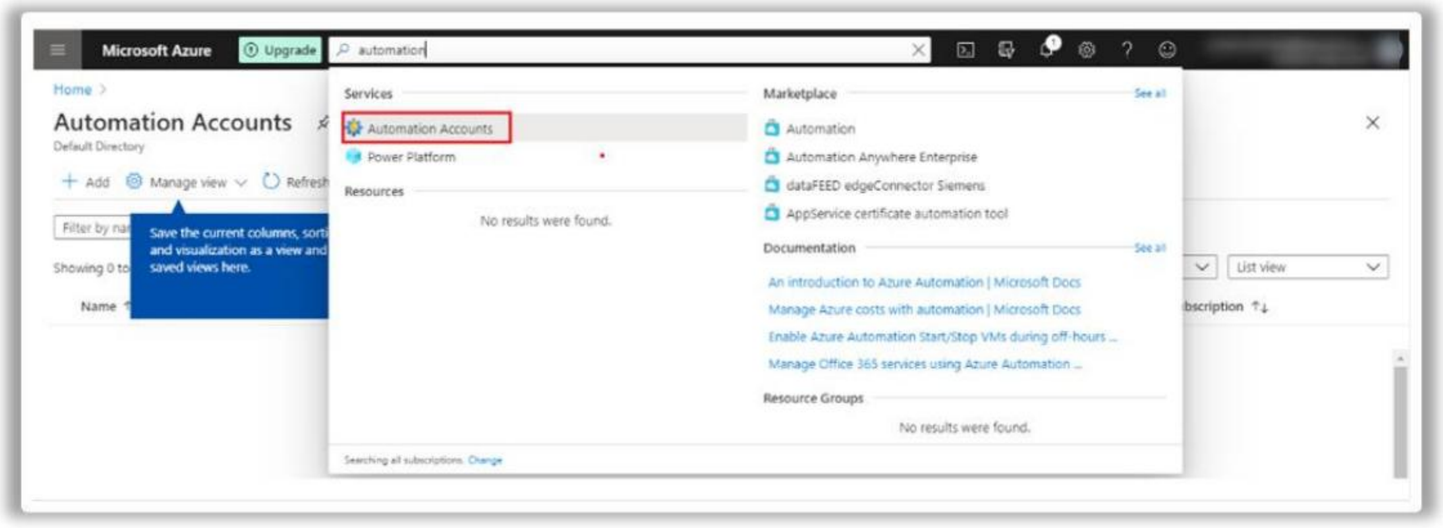


Figure 5.137: Automation Account

- Click on **Add.**

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

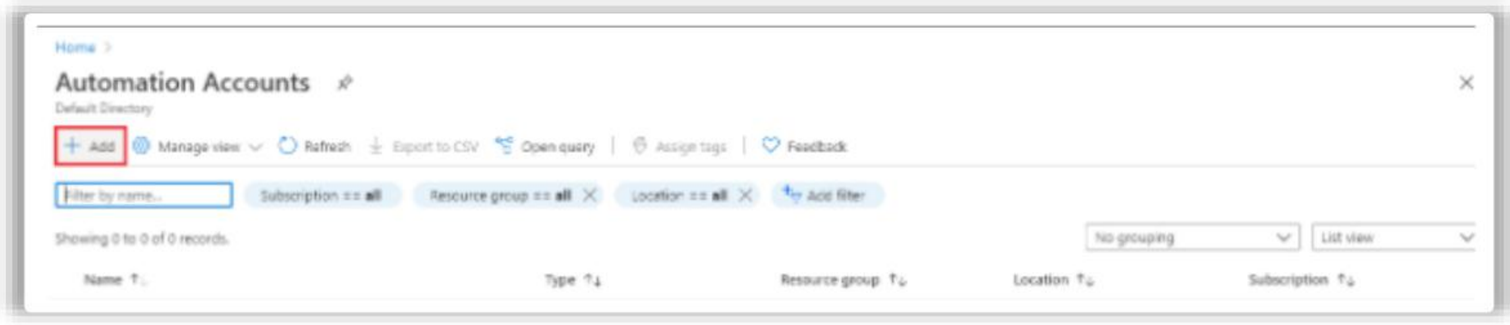


Figure 5.138: Add

- Provide name and other details in the **Add Automation Account** window. Choose "**Yes**" for **Create Azure Run As Account** and click on **Create**.

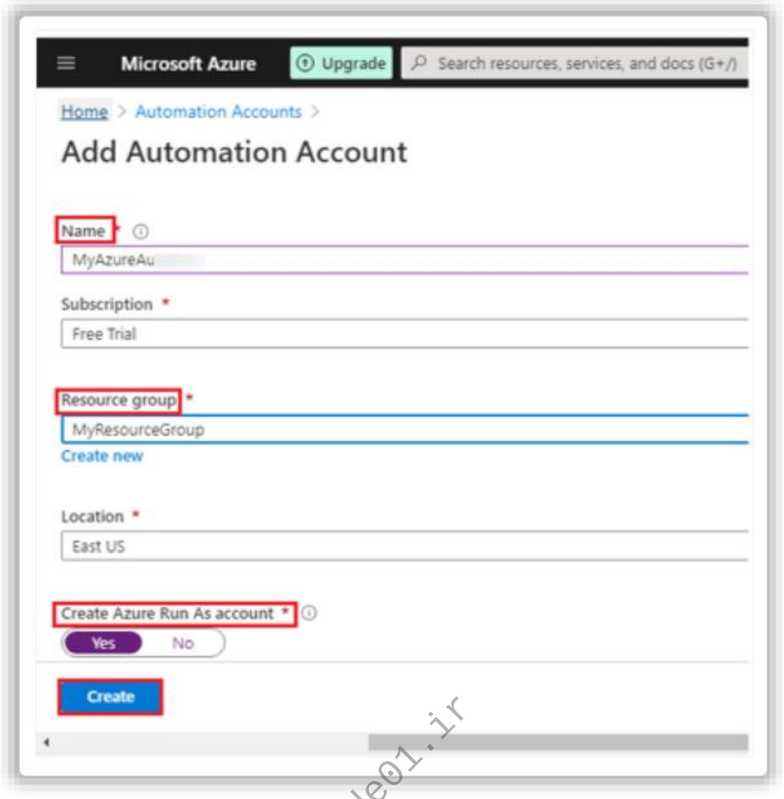


Figure 5.139: Add Automation Account

- An **automation** icon will appear on the left side of the portal after the registration process is completed.
- Azure Automation dashboard displays the job, diagnostic, and usage information for the executed automation jobs, indicating the status of jobs for a time period of 1 h to 30 days.

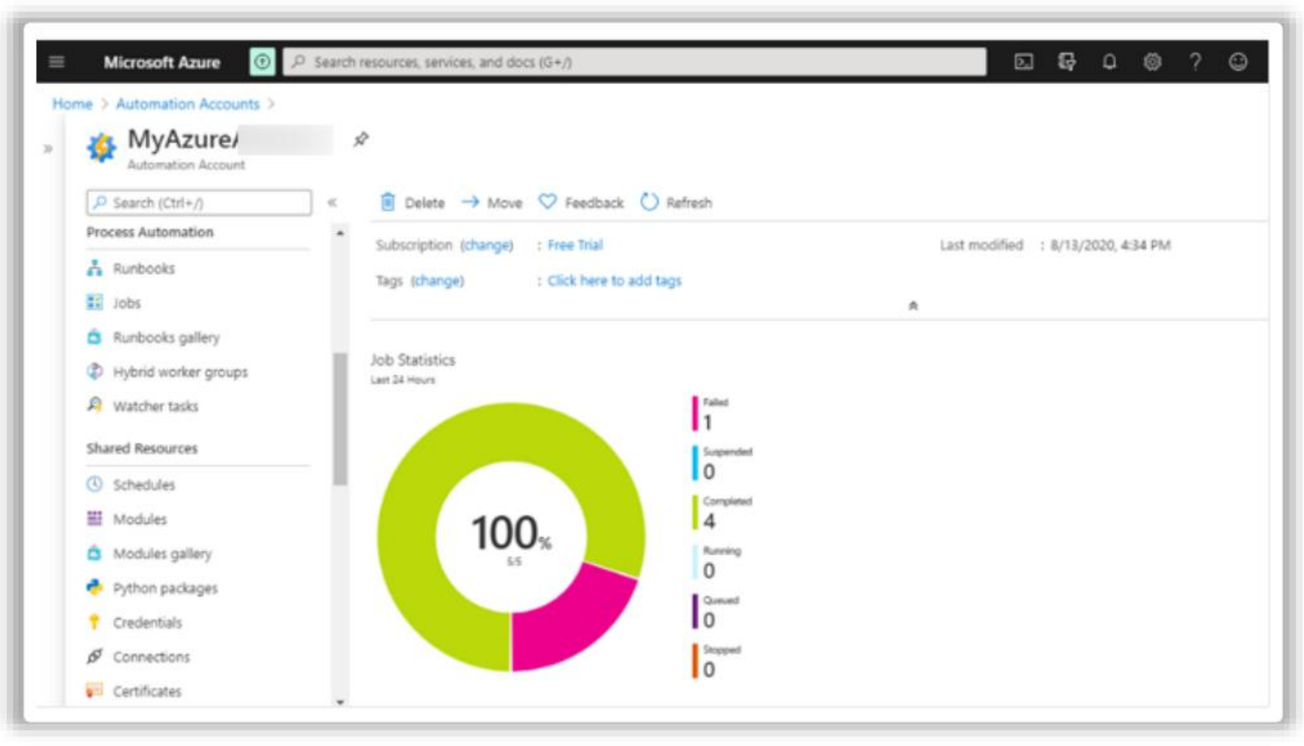


Figure 5.140: Automation Account

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

- The **Runbooks** tab on the dashboard provides several runbooks and their status. To filter the job status by time and date, use the **search** bar.

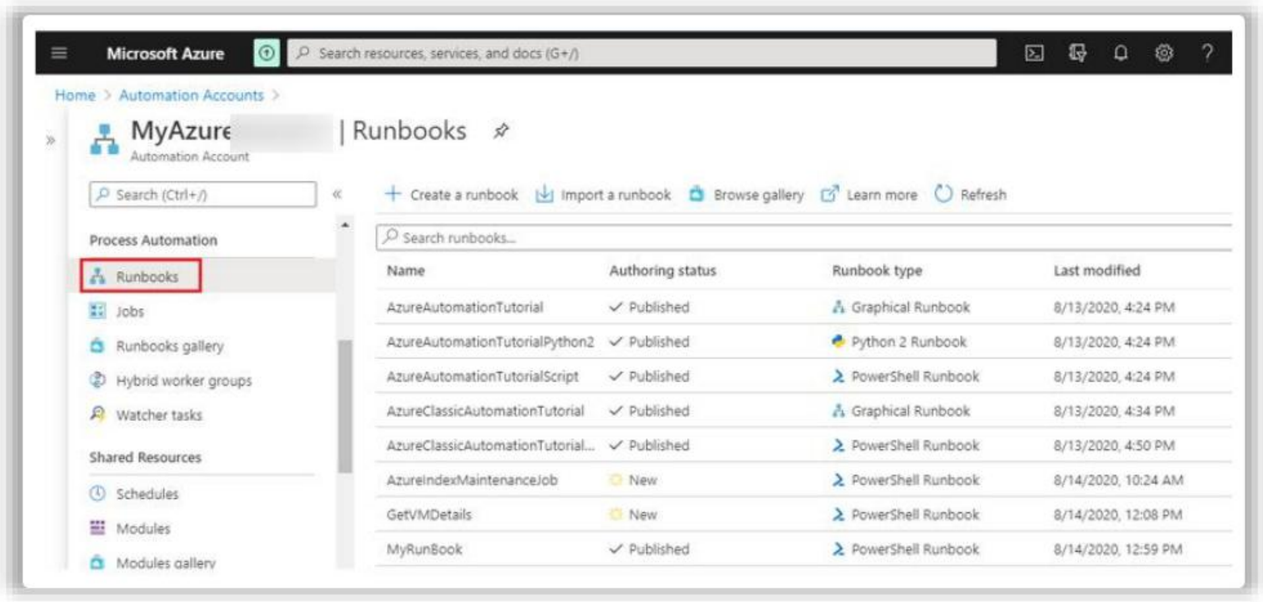


Figure 5.141: Runbooks

- Import a runbook or export it to a file on the **Runbooks** page.

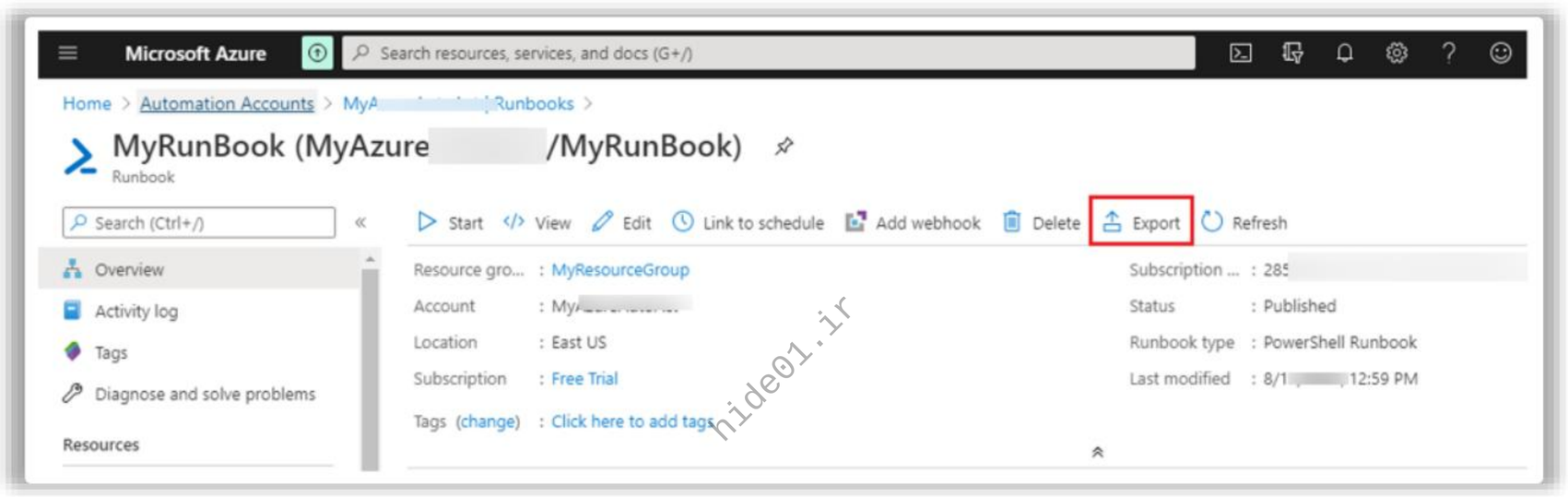


Figure 5.142: Export

- Create variables, connections, and certificates using the **Assets** tab. Import additional modules that contain Windows PowerShell workflows to be used in runbooks if required.

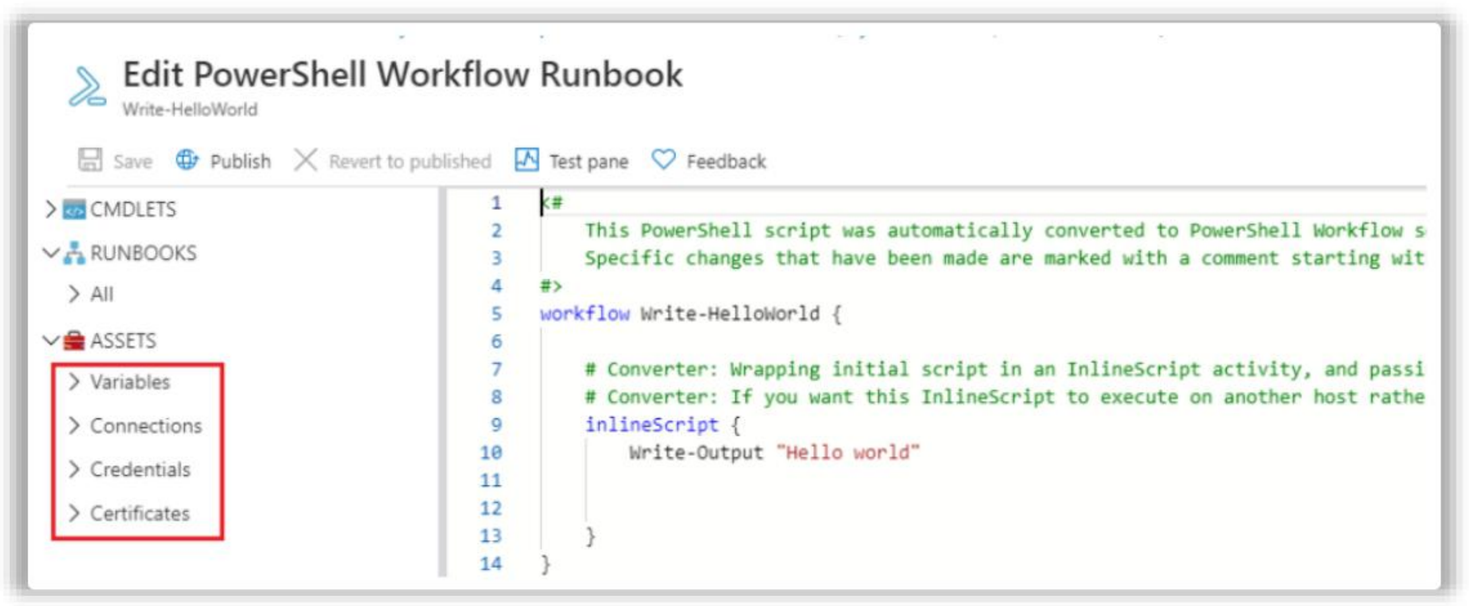


Figure 5.143: Assets

- **Create a runbook**
  - Log into the Azure Management Portal and select the Automation account.

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

- Choose **Runbooks** and click on **Create a runbook.**

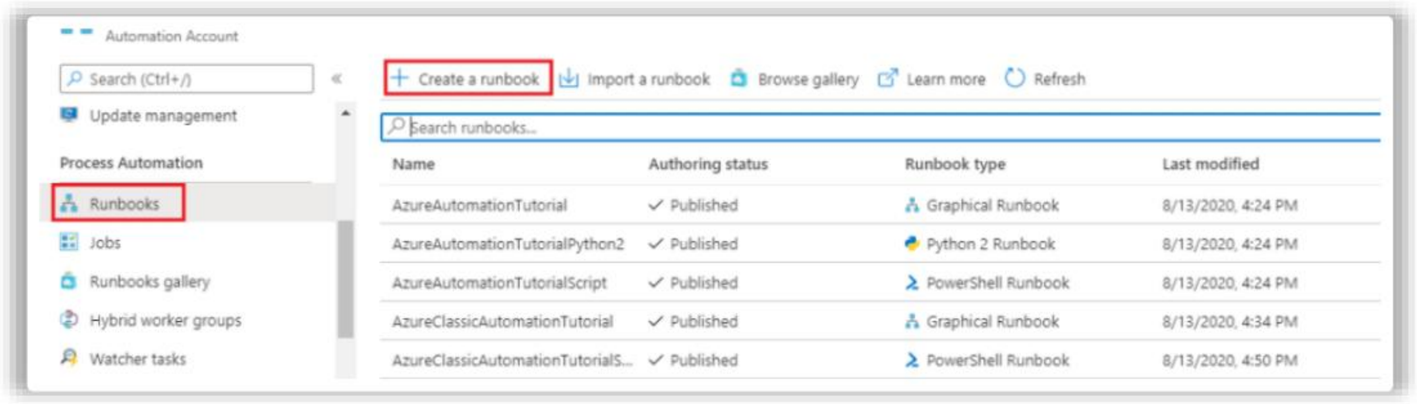


Figure 5.144: Runbooks

- Enter the requested information as shown in the screenshot below.

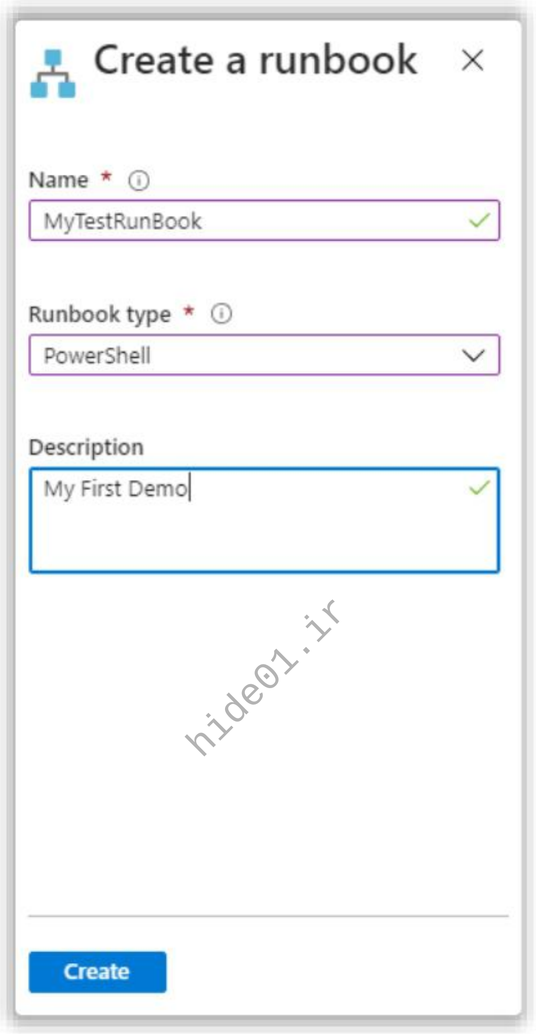


Figure 5.145: Create Runbook

- Click on **Create** to create the runbook.
- Add the following sample code to the empty runbook:

```
Write-output "My First Automation Example"
Write-output "Get Started"
```

Figure 5.146: Sample Code

- Click on Save after entering the code. The runbook job is now ready to start.

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

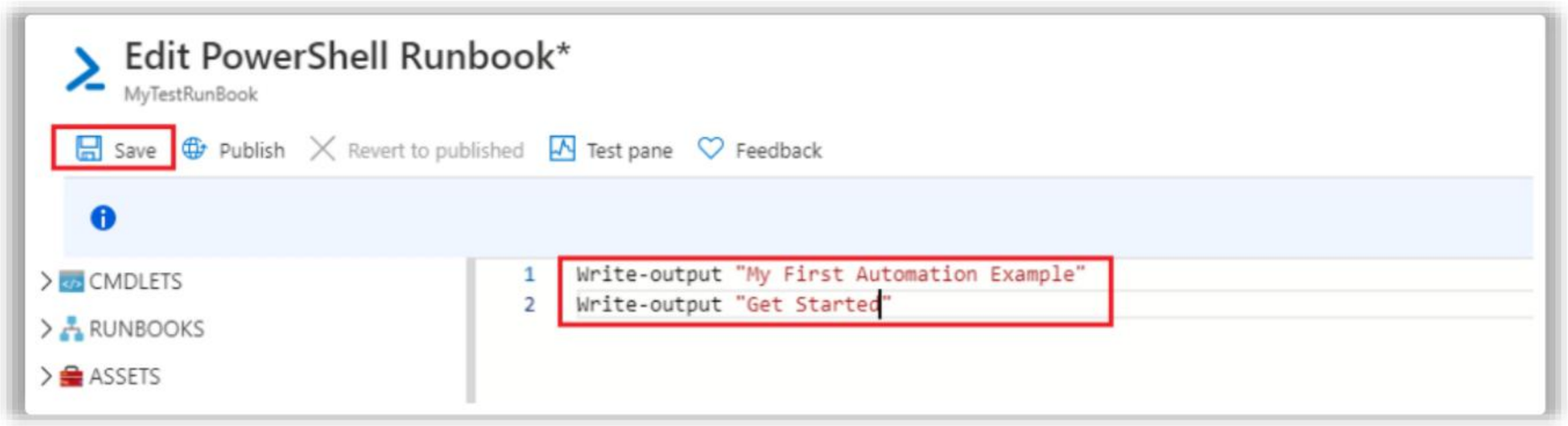
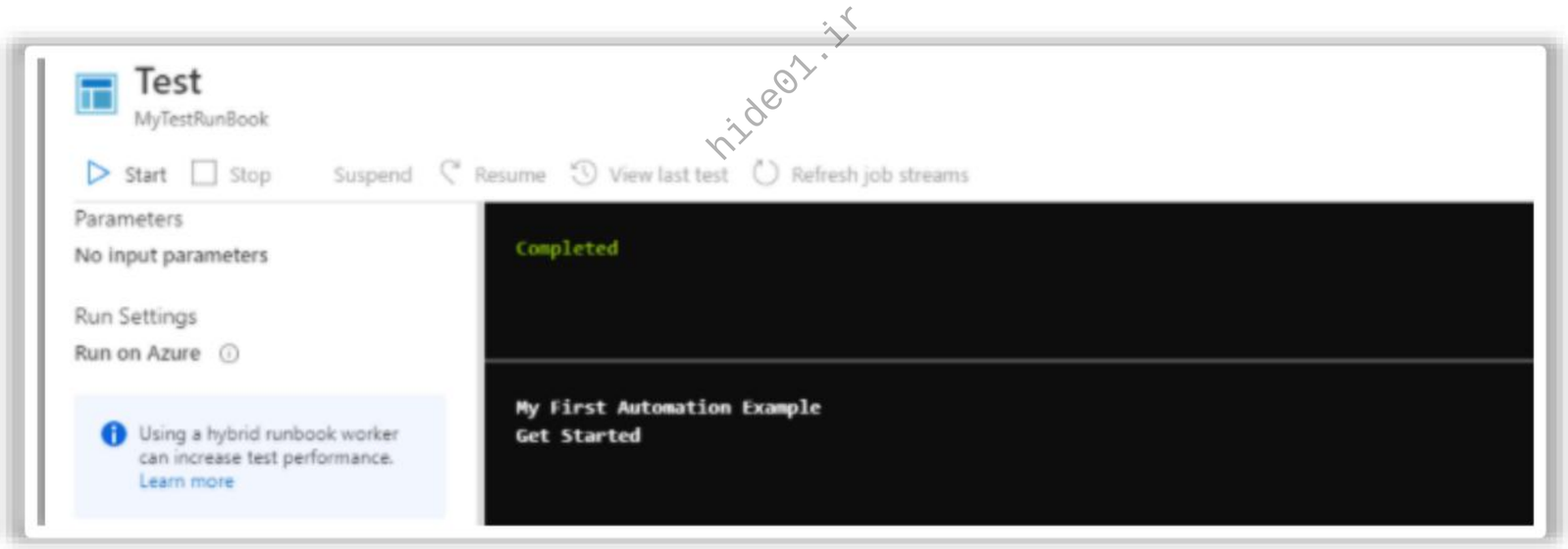


Figure 5.147: Edit

- To test the runbook, choose **Edit**. Then, click on the **Test pane** to test the code.

Figure 5.148: Edit

- Click on **Start** to begin the test. The runbook job is created and the output is shown in the result pane. The runbook is tested and validated successfully.



hide01.ir

Figure 5.149: Test

- **Publish the runbook**
  - To publish the runbook, click on the **Publish** icon and select **Yes** when prompted.
  - On the **Runbooks** page, the status will be shown as **Published**.
  - On the same page, select **Start,** followed by **Yes** to initiate the runbook. You will be taken to a Job pane.

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

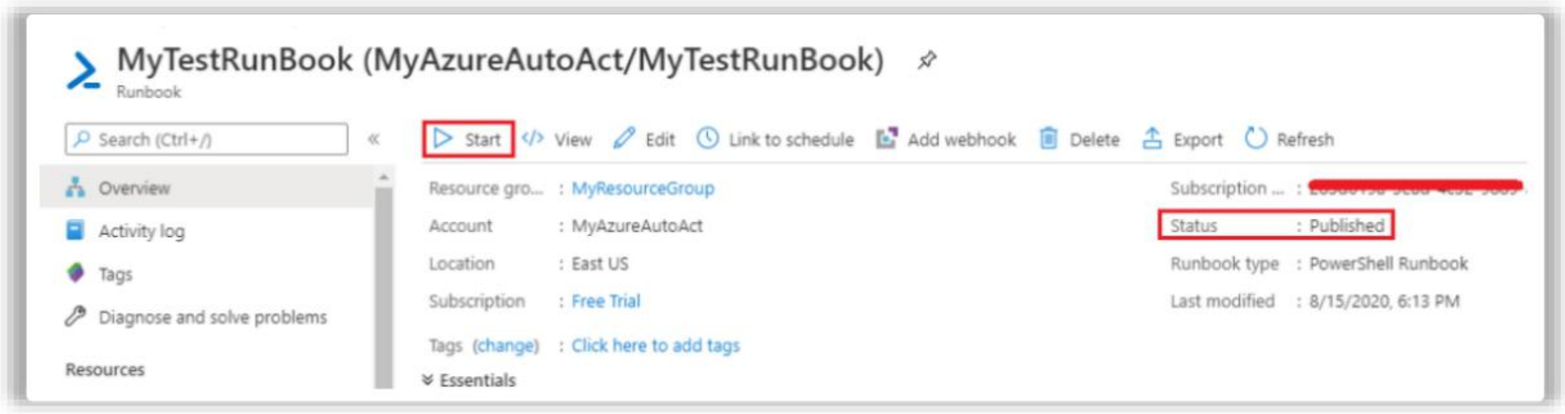


Figure 5.150: MyTestRunBook

- Check the job status on the Job pane. Keep refreshing the page using the **Refresh** icon to check the status.

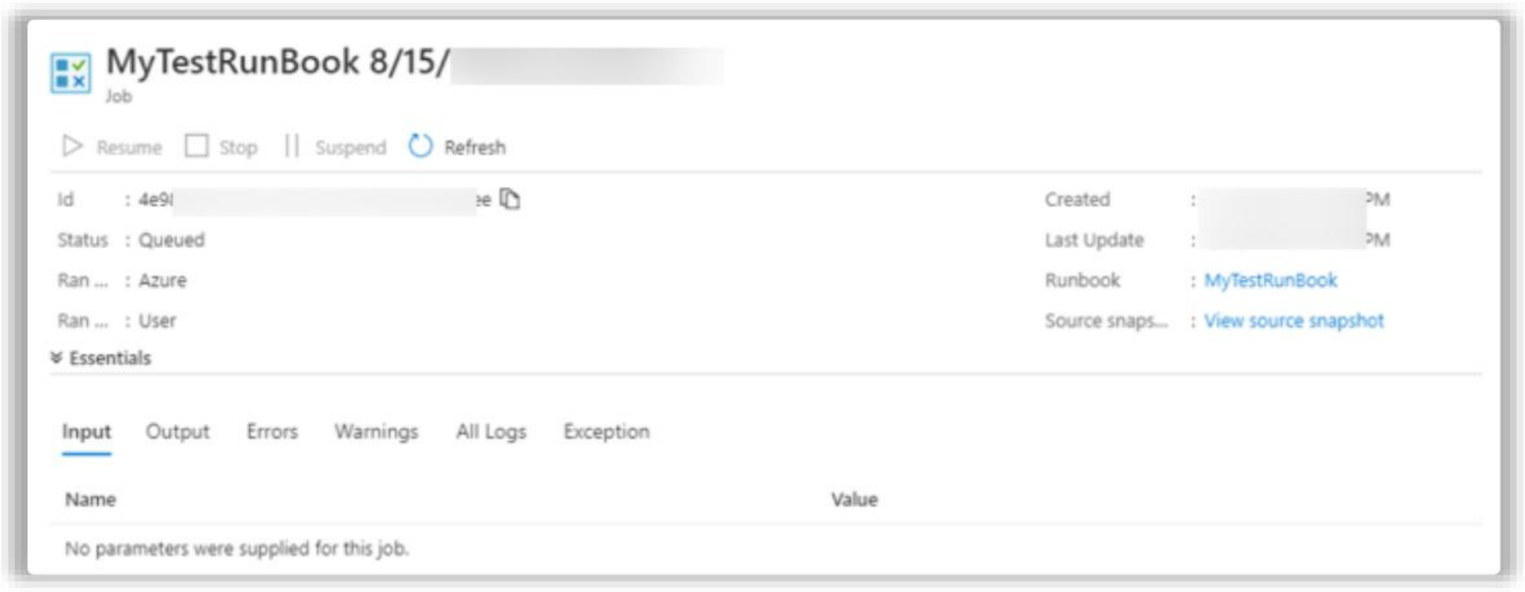


Figure 5.151: Status

- The status is now changed to **Completed,** as shown in the screenshot below:

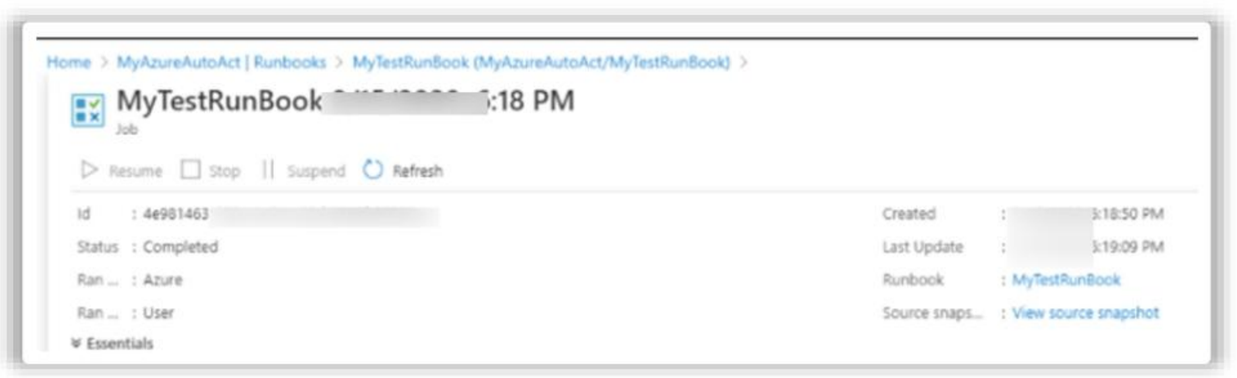


Figure 5.152: Completed

- Check the result summary by clicking on **Output**. The output pane shows the result as shown below.

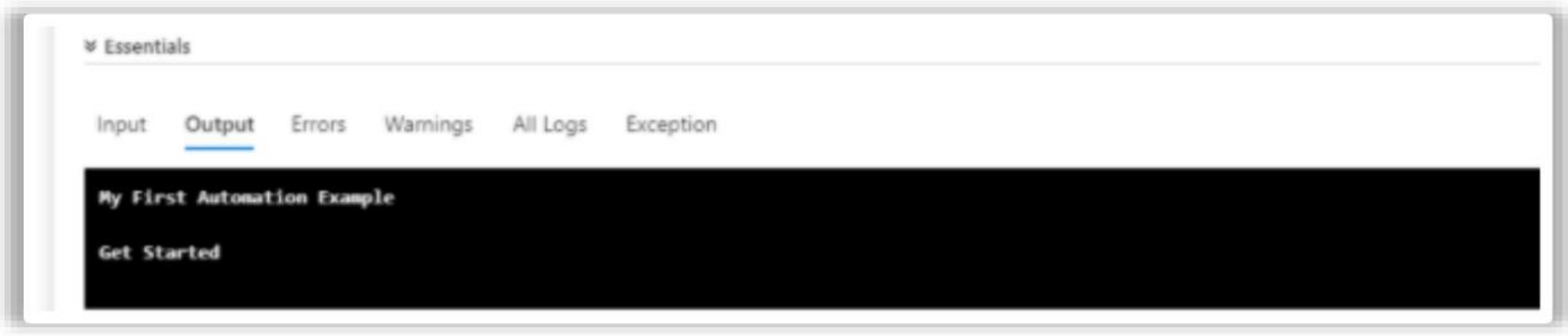


Figure 5.153: Output

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

- Select **All Logs** to view the output streams of the runbook job.

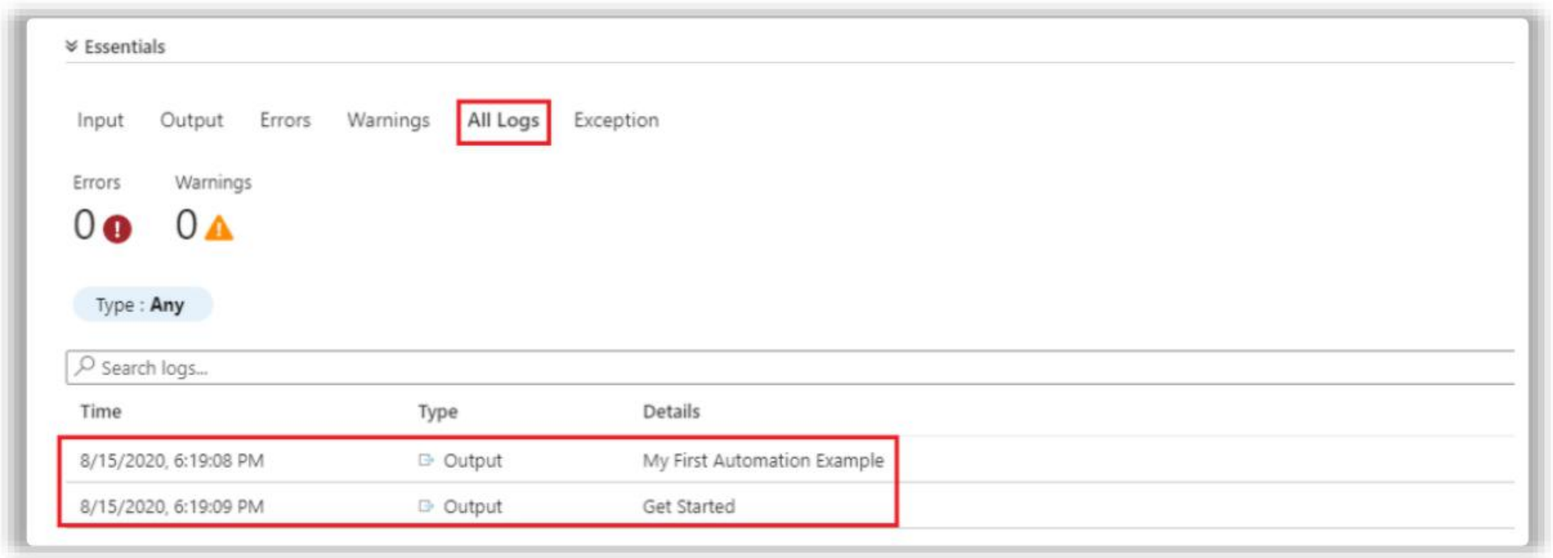


Figure 5.154: All Logs

hide01.ir

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

Azure Operational Security Best Practices

Azure operational security best practices include the following:

Best practices	Description
1. Manage and monitor user passwords	▪ Implement proper password protection in the cloud ▪ Monitor for suspicious activities related to user accounts ▪ Detect and remediate risky passwords automatically
2. Get incident notification from Microsoft	Ensure that Azure incident notifications are received by the security operations team from Microsoft
3. Arrange subscriptions into management groups	▪ Ensure that all new subscriptions have sufficient governance elements (policies and permissions) when they are added ▪ The highest level of management groups should be arranged using segmentation strategies to provide a point for control and policy ▪ Restrict management group depth to prevent confusion that can affect operations and security ▪ Carefully select the components that are applied to the entire organization with the root management group ▪ Plan and test all organization-wide changes on the root management group before they are applied
4. Streamline environment creation with blueprints	Use the Azure blueprints service to build and run new environments rapidly
5. Monitor storage services for unexpected behavioral changes	Monitor the storage services used by the application continuously for unexpected changes in behavior (e.g., slower response time) via Azure Storage Analytics
6. Prevent, detect and respond to threats	▪ Use cloud-based SIEM to increase the speed and scalability of the on-premises SIEM solution ▪ Identify critical vulnerabilities to prioritize investigation ▪ Discover and prioritize security issues by monitoring the security posture of applications, machines, storage, networks, and data services ▪ Integrate Azure Security Center alerts into your current SIEM solution ▪ Integrate Azure logs into your current SIEM solution ▪ Integrate endpoint detection and response capabilities into attack investigation to accelerate the investigation and hunting processes and minimize false positives

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

Azure Operational Security Best Practices (Cont'd)

hide01.ir

Best practices	Description
7. Monitor end-to-end scenario-based network monitoring	▪ Use packet capture to automate remote network monitoring ▪ Use flow logs to gain insight into network traffic ▪ Detect VPN connectivity issues
8. Secure deployment by using proven DevOps tools	▪ Automate service build and deployment ▪ Build and deploy automatically to cloud services or Azure web apps ▪ Automate release management ▪ Check the performance of your app before launching it or apply updates to production ▪ Monitor your application performance
9. Mitigate and protect against DDoS	▪ Ensure that security is integrated into the entire lifecycle of an application to avoid bugs ▪ Design apps to scale horizontally whenever required ▪ **Use Azure capabilities to implement secure designs for your application**
10. Enable Azure Policy	▪ Start policy deployments with the audit mode and later move to the deny and remediate effects ▪ Identify the roles that should monitor for policy violation and ensure that correct remediation actions are taken instantly ▪ Map Azure policy definitions to your organizational policies to improve consistency and avoid confusion
11. Monitor Azure AD reports	Use Azure AD security reports to detect suspicious actions related to user accounts
12. Automate Tasks	Use Azure Automation to automate tasks

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

Azure Operational Security Best Practices

Azure operational best practices work with the existing Azure platform features and capabilities to provide Azure operational security. These best practices are listed below.

Best practices	Description

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

Manage and monitor user passwords	▪ Implement proper password protection in the cloud. ▪ Monitor for suspicious activities related to user accounts. ▪ Detect and remediate risky passwords automatically.
Get incident notification from Microsoft	Ensure that Azure incident notifications are received by the security operations team from Microsoft.
Arrange subscriptions into management groups	▪ Ensure all new subscriptions have sufficient governance elements (policies and permissions) when they are added. ▪ The top-level management groups should be arranged utilizing segmentation strategies to apply control and policy strategies to every segment. ▪ Management group depth should be restricted to avoid confusion that would impact security and operations. ▪ Select management group elements carefully that should be applied to the entire organization. ▪ Plan and test organization-wide changes on the root management group carefully before they are applied.
Streamline environment creation with blueprints	Use the Azure Blueprints service to build and run new environments rapidly.
Monitor storage services for unexpected behavioral changes	Monitor the storage services used by applications continuously for unexpected changes in behavior (e.g., slower response time) via Azure Storage Analytics.
Prevent, detect, and respond to threats	▪ Use cloud-based SIEM to improve the speed and scalability of on-premises SIEM solution. ▪ Identify critical vulnerabilities to prioritize investigation. ▪ Discover and prioritize security issues by monitoring the security posture of applications, machines, and storage, networks, and data services. ▪ Integrate Azure Security Center alerts into your current SIEM solution. ▪ Integrate Azure logs into your current SIEM solution.

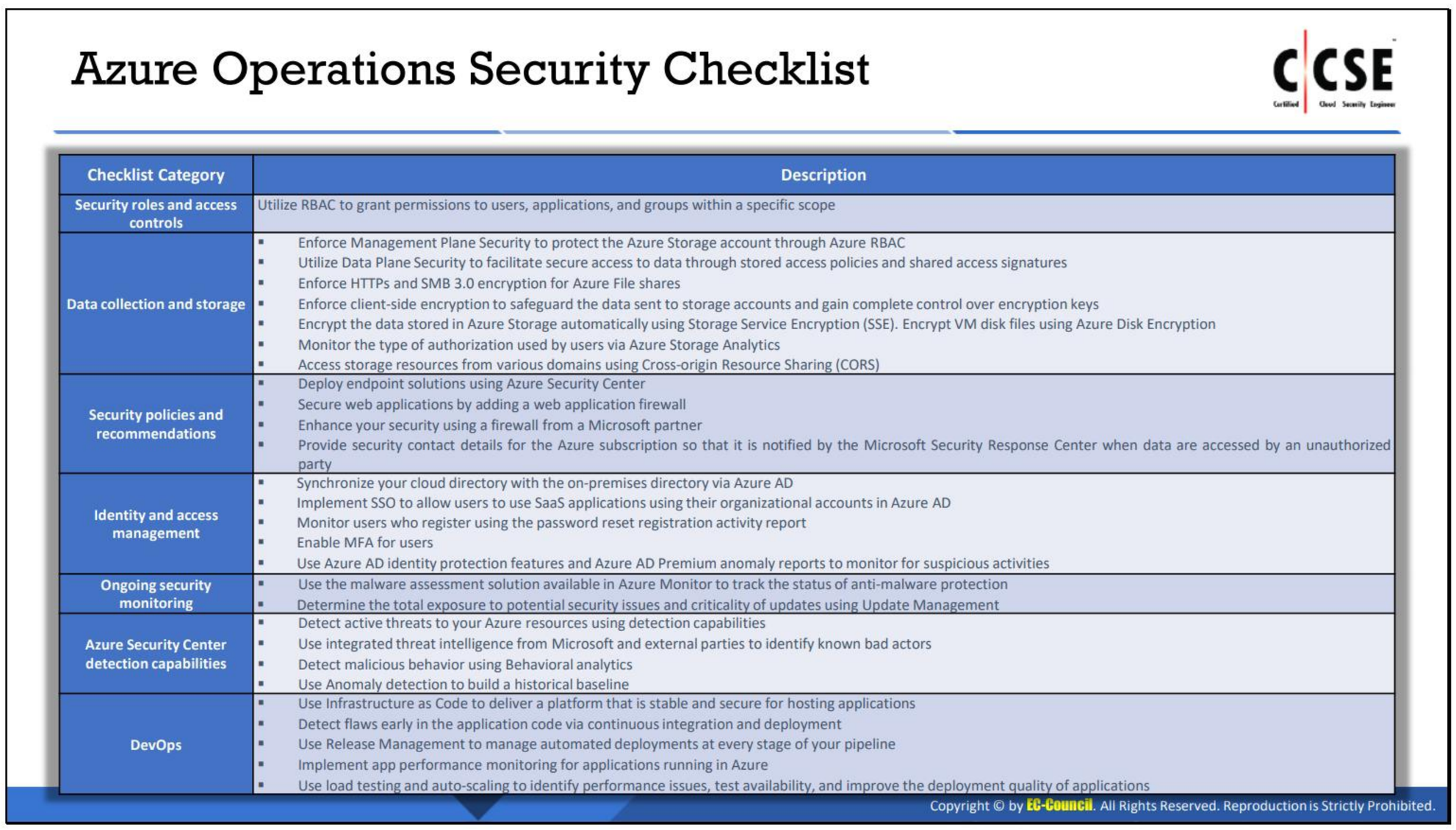
hidemy.name

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

	▪ Integrate endpoint detection and response capabilities with attack investigation to accelerate the investigation and hunting processes and minimize false positives.
Monitor end-to-end scenario-based network monitoring	▪ Use packet capture to automate remote network monitoring. ▪ Use flow logs to gain insight into network traffic. ▪ Detect VPN connectivity issues.
Secure deployment using proven DevOps tools	▪ Automate service build and deployment. ▪ Build and deploy automatically to cloud services or Azure web apps. ▪ Automate release management. ▪ Check the performance of your app before launching it or applying updates to the production. ▪ Monitor your application performance.
Mitigate and protect against DDoS	▪ Ensure that security is integrated into the entire lifecycle of an application to avoid bugs. ▪ Design apps to scale horizontally whenever required. ▪ Use Azure capabilities to implement secure designs for your application.
Enable Azure Policy	▪ Start policy deployments with the audit mode and later move to the deny and remediate effects. ▪ Identify the roles that should be monitored for policy violation and ensure that correct remediation actions are taken instantly. ▪ Map Azure policy definitions to your organizational policies to improve consistency and avoid confusion.
Monitor Azure AD reports	Use Azure AD security reports to detect suspicious actions related to user accounts.
Use Azure Automation	Use Azure Automation to automate tasks.

TABLE 5.1: Best Practices

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



Azure Operations Security Checklist

The checklist that can help organizations to review operational security considerations includes the following. Use this checklist to build a secure cloud migration and operations strategy.

hide01.ir

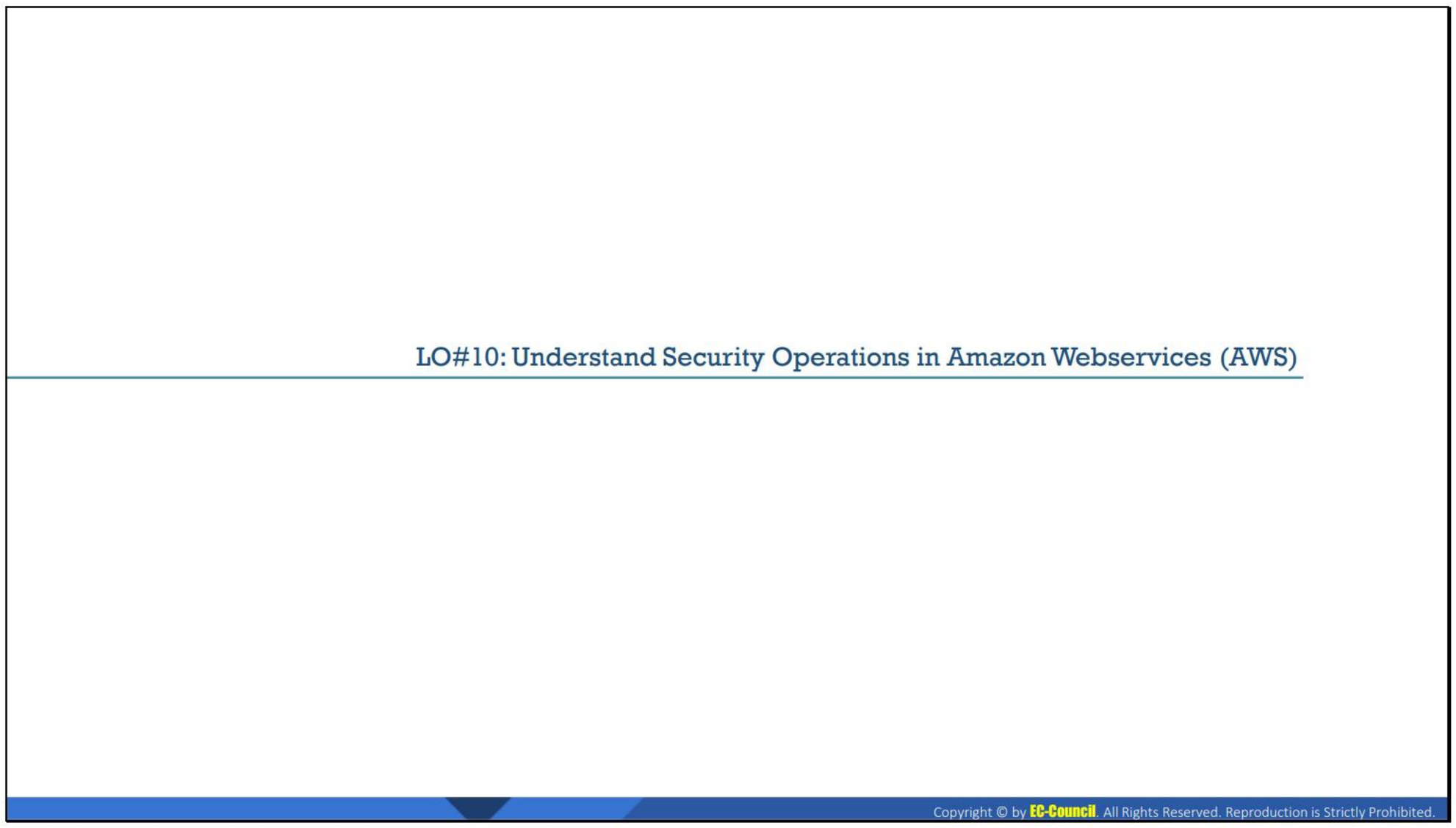
Checklist Category	Description
Security roles and access controls	Utilize Azure role-based access control (RBAC) to assign permissions to users, applications, and groups at a specific scope.
Data collection and storage	▪ Implement Management Plane Security to secure Azure Storage account via Azure RBAC. ▪ Use Data Plane Security to secure data access via Stored Access policies and Shared Access Signatures (SAS). ▪ Implement HTTPs and SMB 3.0 encryption for Azure File share. ▪ Implement client-side encryption to protect the data sent to storage accounts when complete control is desired over encryption keys. ▪ Encrypt the data stored in Azure Storage automatically using Storage Service Encryption (SSE). Encrypt VM disk files using Azure Disk Encryption. ▪ Monitor the type of authorization used by users using Azure Storage Analytics. ▪ Access storage resources from various domains using Cross-

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

	origin Resource Sharing (CORS).
Security policies and recommendations	▪ Deploy endpoint solutions using Azure Security Center (ASC). ▪ Secure web applications by adding a web application firewall. ▪ Enhance your security using a firewall from a Microsoft partner. ▪ Provide security contact details for the Azure subscription to get notified by the Microsoft Security Response Center when your data are accessed by an unauthorized party.
Identity and access management	▪ Synchronize your cloud directory with the on-premises directory via Azure AD. ▪ Implement SSO to allow users to use SaaS applications using their organizational accounts in Azure AD. ▪ Monitor users who register using the password reset registration activity report. ▪ Enable MFA for users. ▪ Use Azure AD identity protection features and Azure AD premium anomaly reports to monitor suspicious activities.
Ongoing security monitoring	▪ Use the malware assessment solutions available in Azure Monitor to track the status of anti-malware protection. ▪ Determine the total exposure to potential security issues and criticality of updates via Update Management.
Azure Security Center detection capabilities	▪ Detect active threats to your Azure resources using detection capabilities. ▪ Use integrated threat intelligence from Microsoft and external parties to identify known bad actors. ▪ Detect malicious behavior using Behavioral analytics. ▪ Use Anomaly detection to build a historical baseline.
DevOps	▪ Use Infrastructure as Code to deliver a platform that is stable and secure for hosting applications. ▪ Detect flaws early in the application code via continuous integration and deployment. ▪ Use Release Management to manage automated deployments at every stage of your pipeline. ▪ Monitor the performance of applications running in Azure. ▪ Use load testing and auto-scaling to identify performance issues, test availability, and improve the deployment quality of applications.

TABLE 5.2: Checklist

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



LO#10: Understand Security Operation in Amazon Webservices (AWS)

The objective of this section is to understand various AWS tools and services to secure cloud operations in AWS. This section describes AWS, including AWS System Manager OpsCenter, Systems Manager Explorer, CloudWatch, and CloudTrail. Cloud security engineers will learn about AWS tools and services in this section and use them effectively to secure organizational operations in the AWS cloud environment.

hide01.ir

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

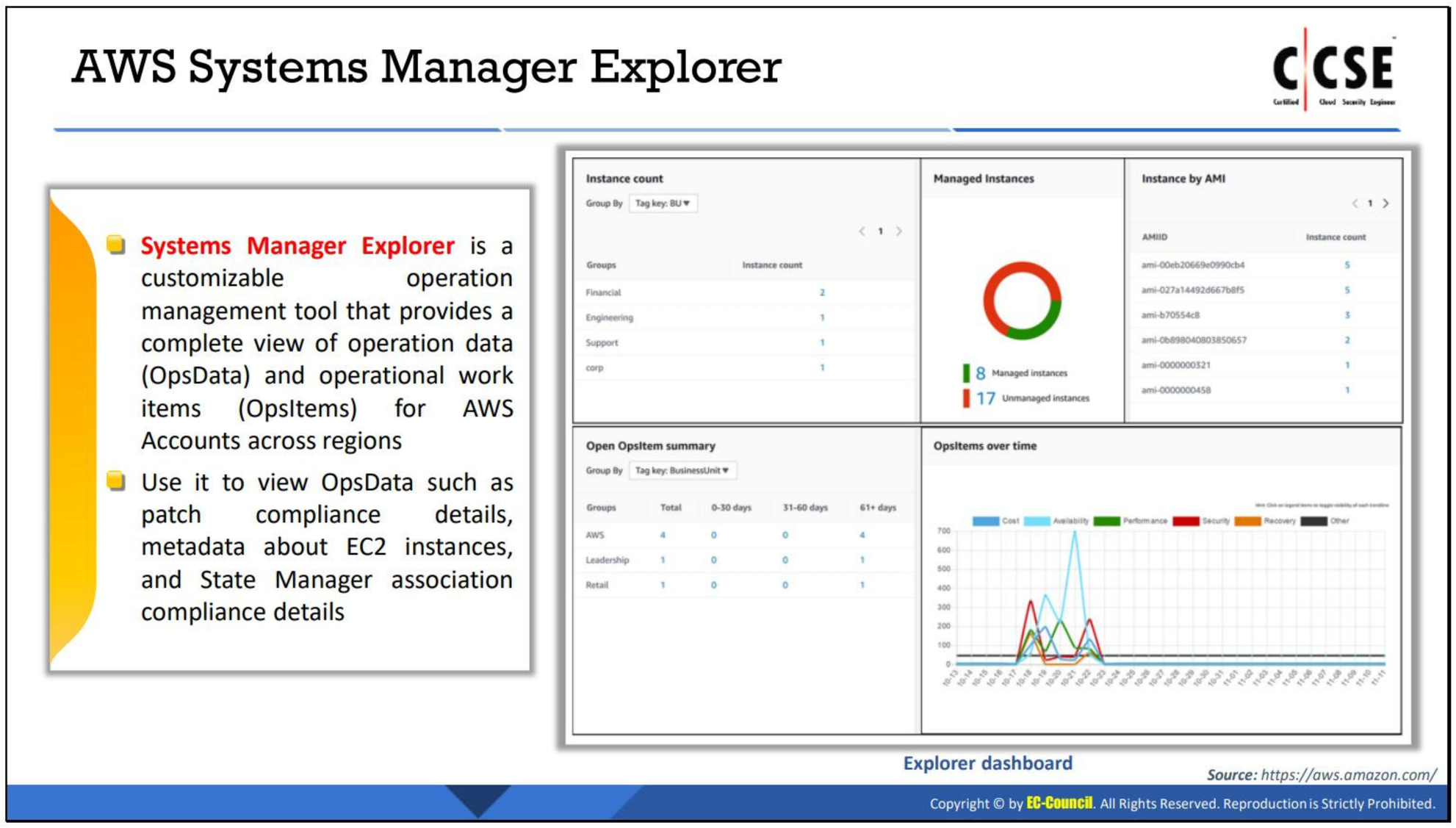
AWS Security Operation Features/Services

AWS provides various features/services to manage organizational security operations. Use these features to implement security checks and analyses automatically, gain insights into events by monitoring logs, perform security assessments to prevent common vulnerabilities, and apply security best practices.

The key features of AWS security operations include

- AWS Systems Manager Explorer
- AWS System Manager OpsCenter
- Amazon CloudWatch
- Trusted Advisor and Personal Health Dashboard (PHD)
- AWS CloudTrail
- AWS Config
- Amazon GuardDuty
- Amazon Inspector
- AWS Security Hub
- AWS CloudFormation

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



AWS Systems Manager Explorer

Systems Manager Explorer is a customizable operations management tool that presents a holistic view of operations data (OpsData) and operational work items (OpsItems) for AWS accounts across regions. It displays OpsData such as patch compliance details, metadata about EC2 instances, and State Manager association compliance details. In addition, OpsData include information from other supporting services such as AWS Compute Optimizer, AWS Trusted Advisor, and data of AWS support cases.

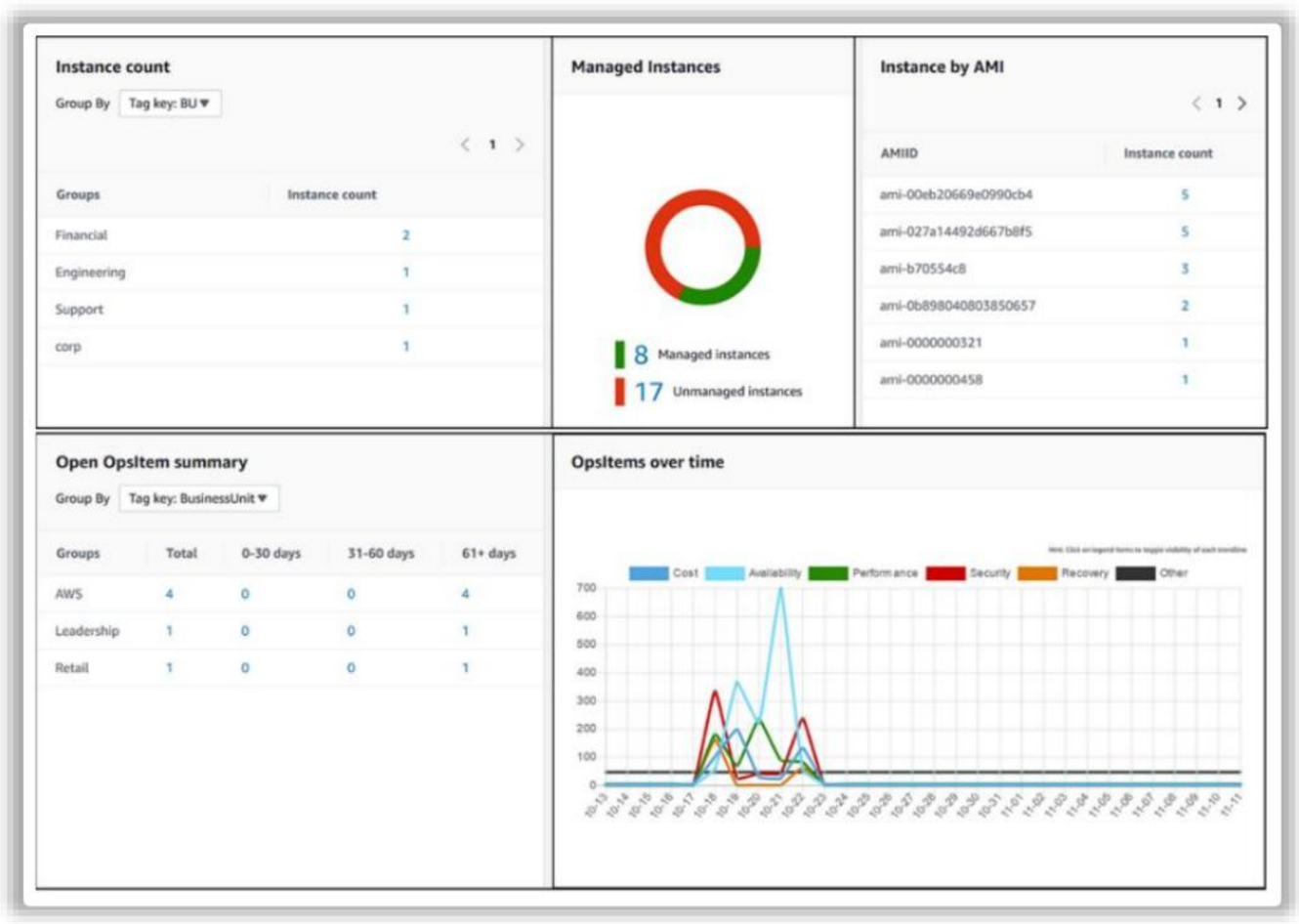


Figure 5.155: Explorer dashboard

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

Key features of System Manager Explorer

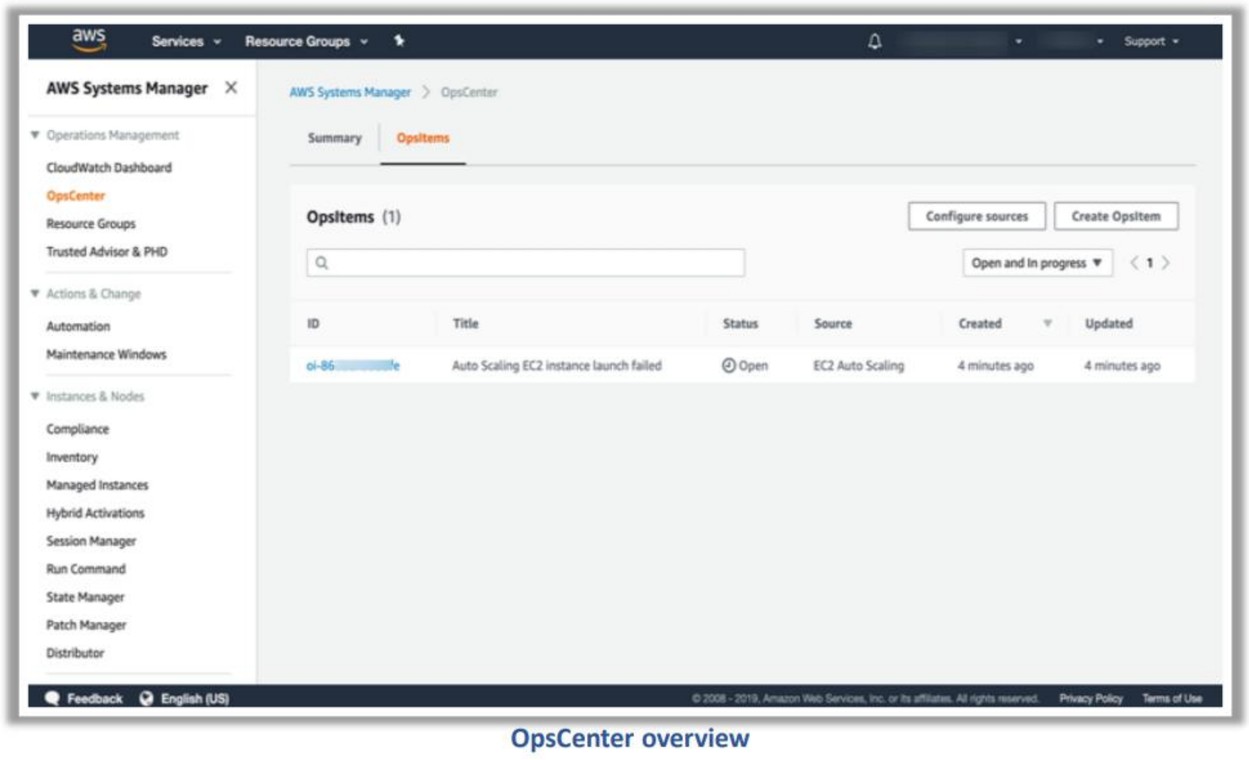
- **Customizable view of actionable information**: Explorer displays actionable information about AWS resources automatically in widgets. These widgets include OpsItem widgets and Informational widgets.
- **Direct links to service screens**: Explorer widgets have direct links to relevant service screens to facilitate the smooth investigation of issues with AWS resources.
- **Reporting**: Explorer supports exporting of reports in the form of .csv files to Amazon S3 buckets so that they can be used for further investigation.
- **Reporting tag keys**: While setting up Explorer, up to five keys can be specified. These tag keys help to filter and group data in Explorer to help in operation management.
- **Groups**: Explorer widgets allow to group operational issues across an organization based on the tag, account, and region.
- **Modes**: Explorer supports three different modes of AWS account and region display for better operation management.

hide01.ir

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

AWS System Manager OpsCenter

- **System Manager OpsCenter** allows operations engineers and IT professionals to view, investigate, and fix OpsItems that are related to AWS resources
- Use it to view the summary reports of OpsItems (by source and status) that are generated automatically
- Use it to eliminate the need to navigate multiple consoles during an investigation by aggregating information from AWS CloudTrail logs, AWS Config, and CloudWatch events



OpsCenter overview

Source: https://aws.amazon.com/

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

AWS System Manager OpsCenter

System Manager OpsCenter allows operation engineers and IT professionals to view, investigate, and fix OpsItems related to AWS resources. It reduces the mean time required to resolve issues that impact AWS resources. Use OpsCenter to view the summary reports of OpsItems (by source and status) that are generated automatically. OpsCenter eliminates the need to navigate multiple consoles during an investigation by aggregating information from AWS CloudTrail logs, AWS Config, and CloudWatch events.

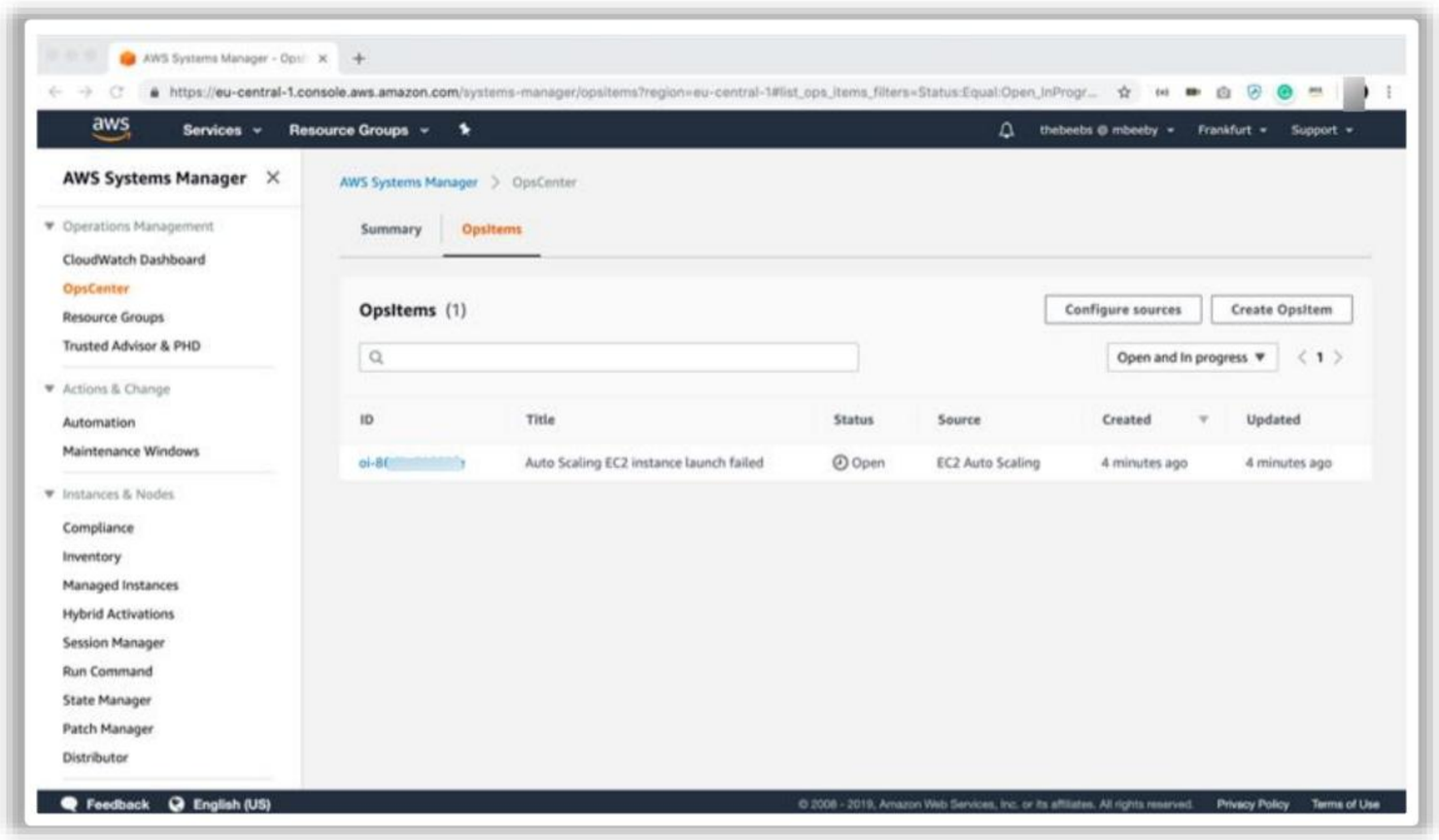


Figure 5.156: OpsCenter overview

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

Key features of OpsCenter

OpsCenter provides the following features:

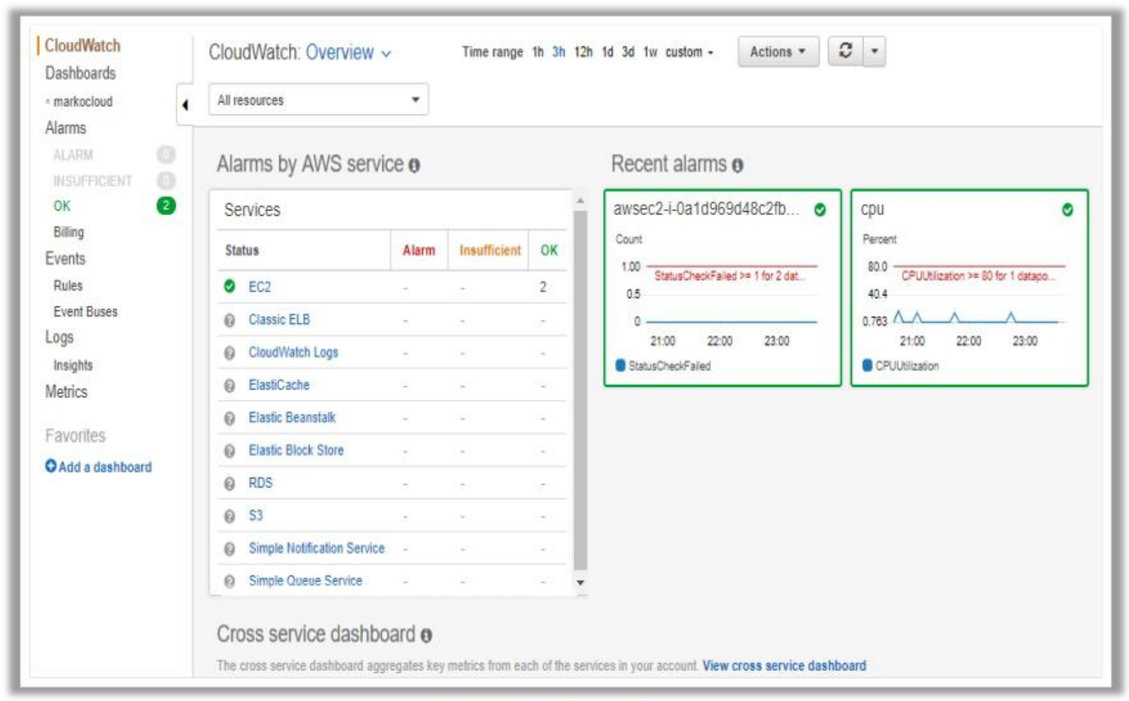
- **Manual and automated OpsItem creation:** OpsCenter allows the manual creation of OpsItems and automates their creation through CloudWatch.
- **Easy remediation:** OpsCenter remediates the common issues related to AWS resources automatically using Runbooks.
- **OpsItem summary reports:** OpsCenter provides summary reports that contain important information such as the status summary of OpsItems, OpsItems by age and source, and sources with the most open OpsItems.
- **IAM access control:** OpsCenter allows the use of IAM policies to control who can create, view, list, and update OpsItems in an organization.
- **Supports logging and auditing:** OpsCenter can be integrated with other AWS resources to log and audit OpsCenter user actions in AWS accounts.

hide01.ir

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

CloudWatch Dashboards Hosted by Systems Manager

- In a CloudWatch console, cloud security engineers can utilize **CloudWatch dashboards** to monitor all AWS resources of the organization
- Utilize dashboards to monitor resources in various regions
- Utilize dashboards for creating customized views of metrics and alarms



CloudWatch dashboard

Source: https://aws.amazon.com/

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

CloudWatch Dashboards Hosted by Systems Manager

In a CloudWatch console, CloudWatch dashboards are customizable homepages that can be used to monitor resources. They can even monitor resources present in different Regions.

Create customized views of metrics and alarms using CloudWatch dashboards for AWS resources.

hade01.ir

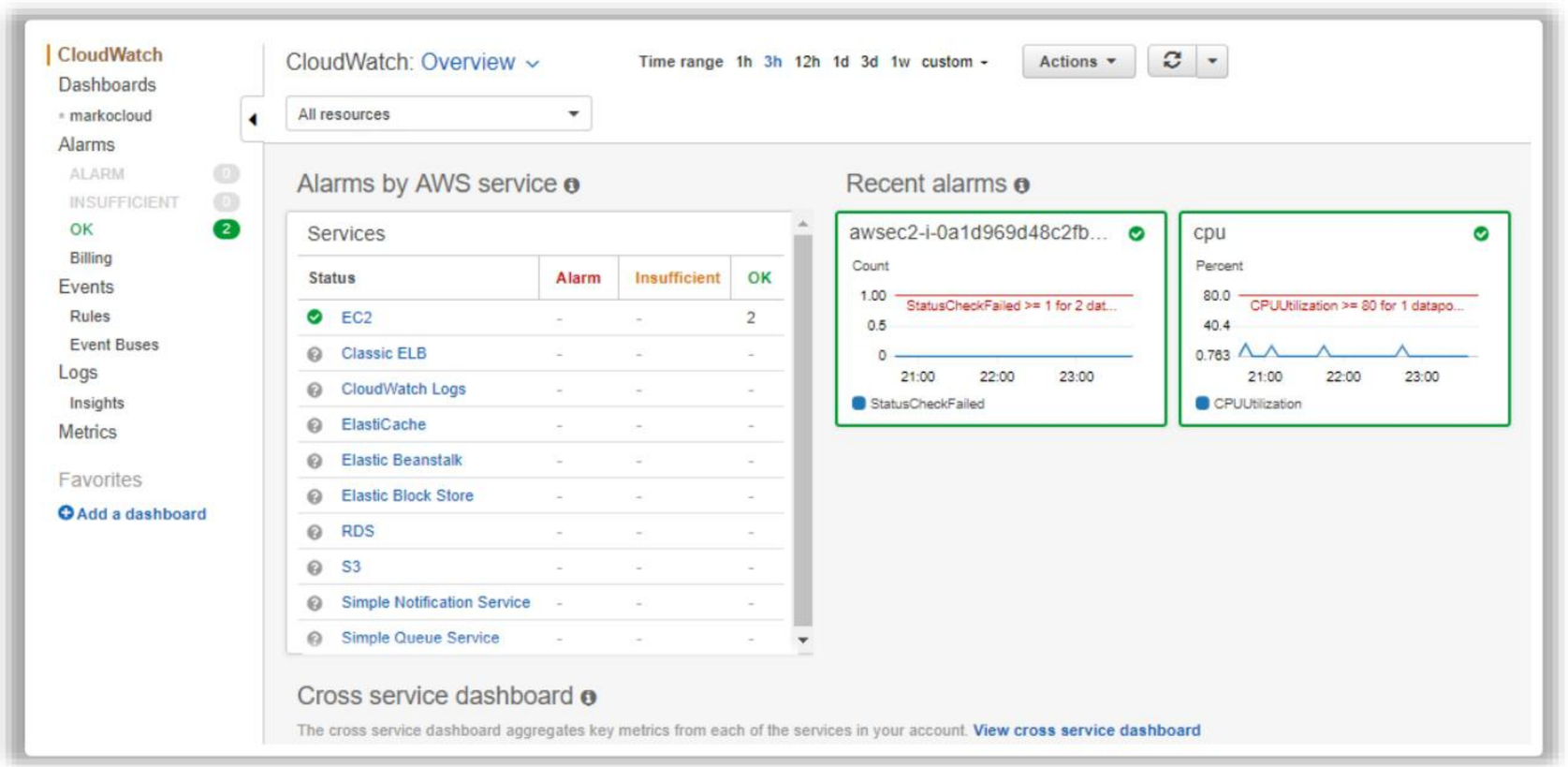


Figure 5.157: CloudWatch dashboard

CloudWatch dashboards provide the following features:

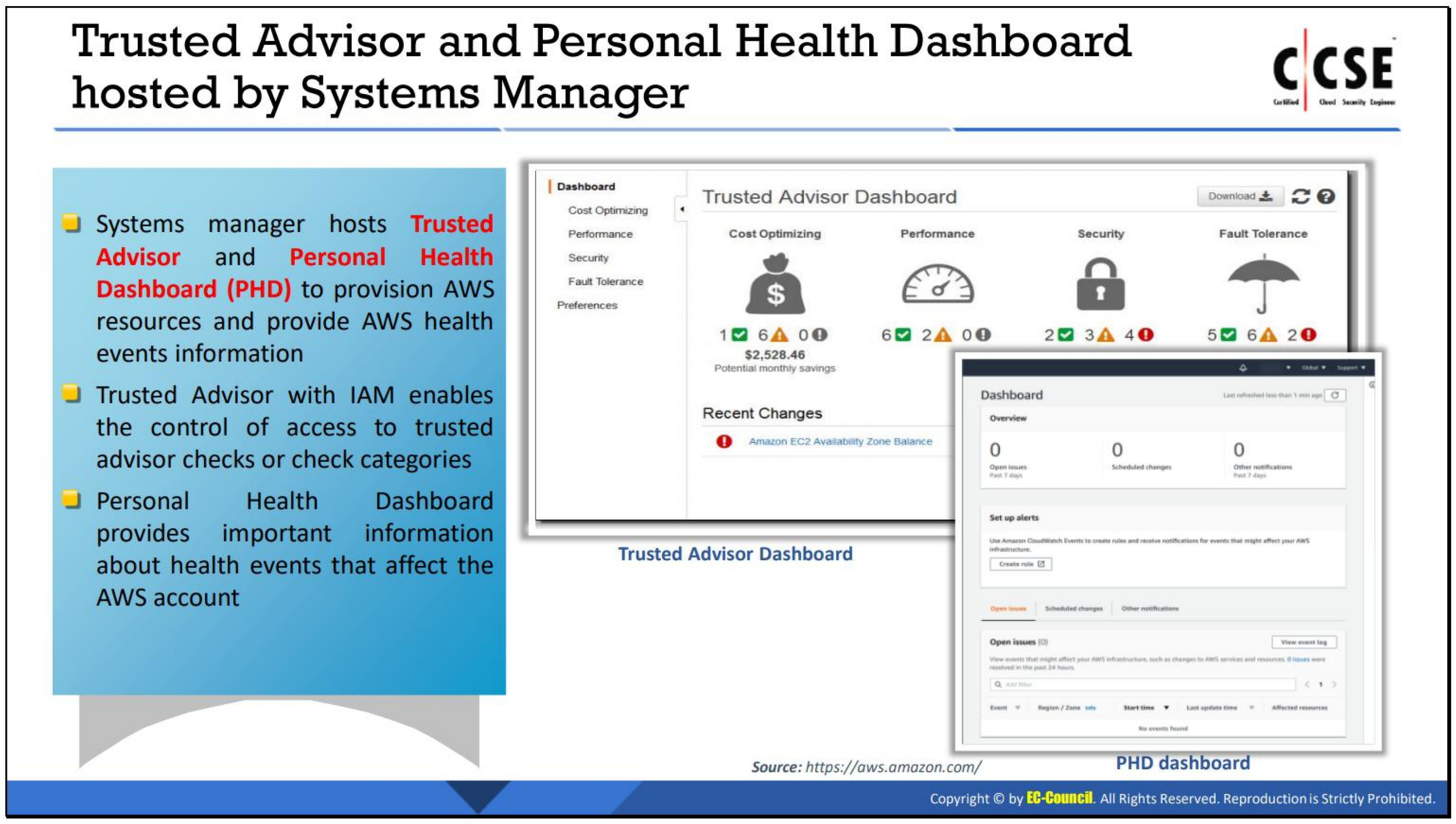
- Help to assess the health of applications and resources across regions.
- Guide the response to particular incidents via operational playbooks.

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

- Allow sharing a common view of application measurements and critical resources with team members to improve and accelerate communication flow during operational events.

hide01.ir

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



Trusted Advisor and Personal Health Dashboard hosted by Systems Manager

Trusted Advisor and Personal Health Dashboard (PHD) are two online tools hosted by Systems Manager to provision AWS resources and monitor AWS accounts for health events. Trusted Advisor is a tool that offers real-time assistance to provision AWS resources considering AWS best practices. Trusted Advisor checks can be used to improve the performance and security, optimize AWS infrastructures, monitor service limits, and minimize the overall cost.

Trusted Advisor offers the following features:

- **Access management**: Trusted Advisor allows the use of IAM to control access to particular trusted advisor checks or check categories.
- **Action links**: Trusted Advisor report items contain hyperlinks to the console where actions can be taken on Trusted Advisor recommendations.

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

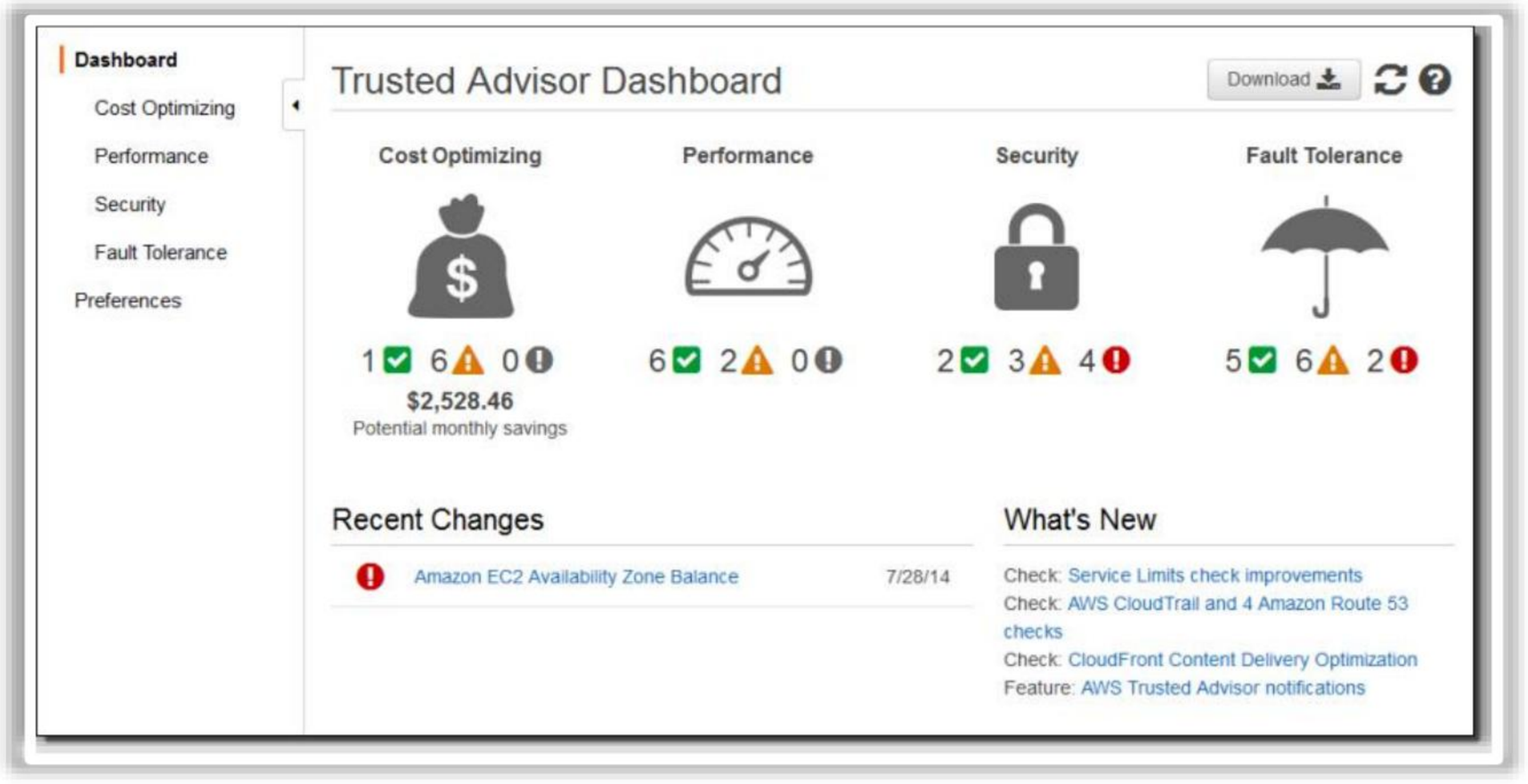


Figure 5.158: Trusted Advisor dashboard

Personal Health Dashboard is an AWS service that provides important information about health events affecting AWS accounts. This information is displayed in two forms: a dashboard that displays the upcoming and recent events and a full event log that contains all events from past 90 days. It organizes issues into three categories, namely, open issues, scheduled changes, and other notifications (shown below).

hide01.ir

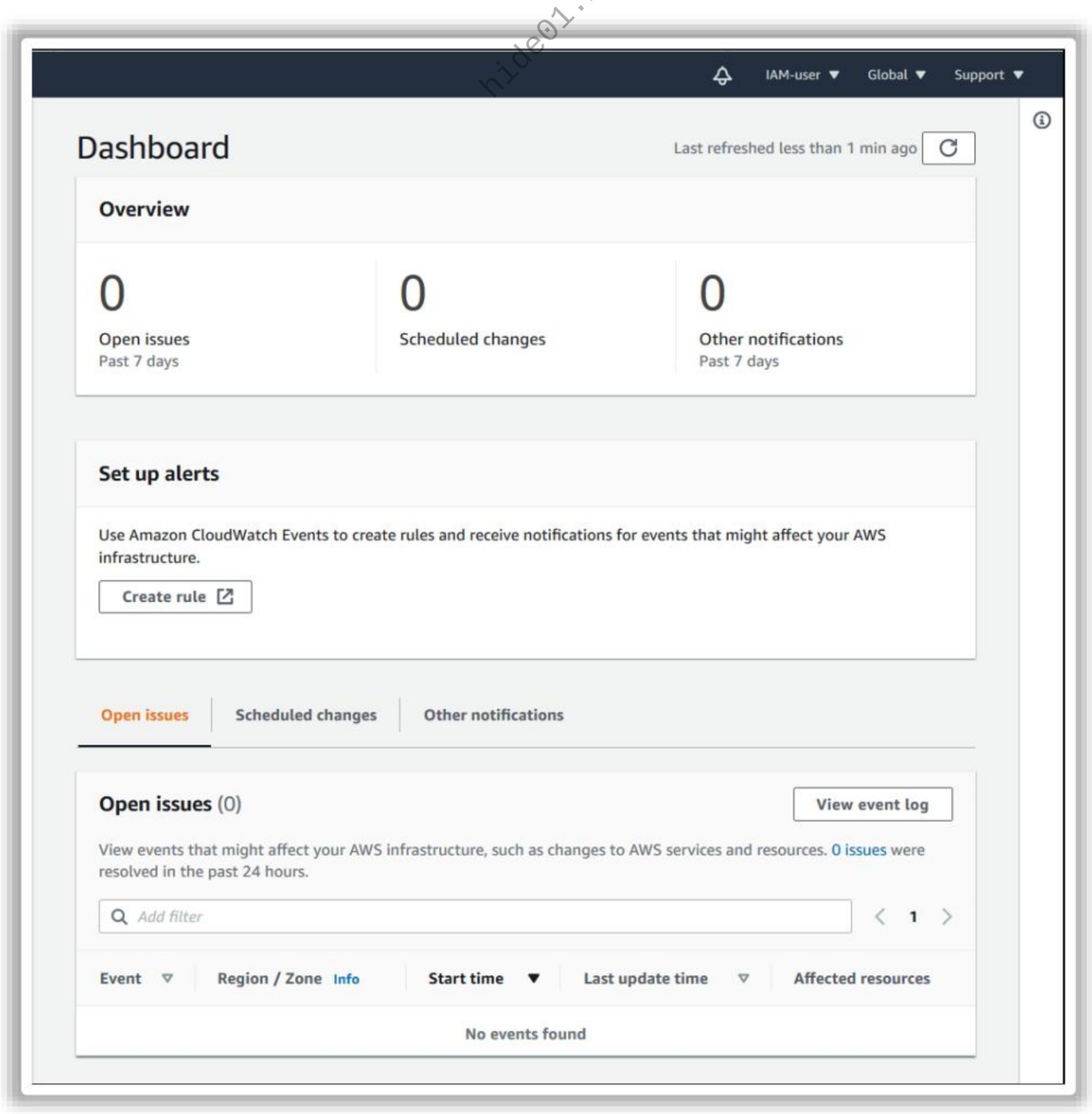
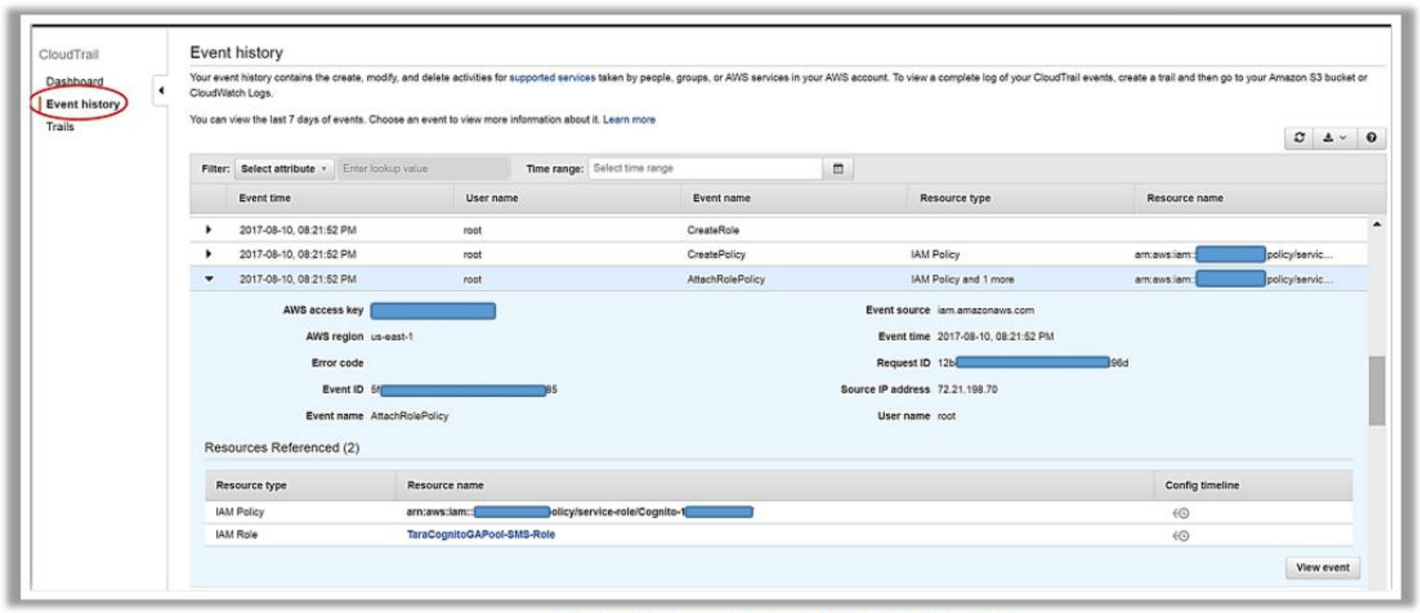


Figure 5.158: PHD dashboard

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

AWS CloudTrail

- **AWS CloudTrail** provides the event history of AWS account activities that can simplify security analysis, resource change tracking, and troubleshooting
- It is utilized to detect malicious activity in AWS accounts, operational analysis, and troubleshooting



Viewing customers' event history in CloudTrail

Source: https://aws.amazon.com/

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

AWS CloudTrail

AWS CloudTrail enables risk auditing, compliance, operational auditing, and governance of an AWS account. It enables organizations to log, continuously monitor, and retain account activities related to actions across the AWS infrastructure. It provides the event history of AWS account activities that can simplify security analysis, resource change tracking, and troubleshooting. It can be used to detect unusual activity in AWS accounts, thus facilitating the simplification of operational analysis and troubleshooting.

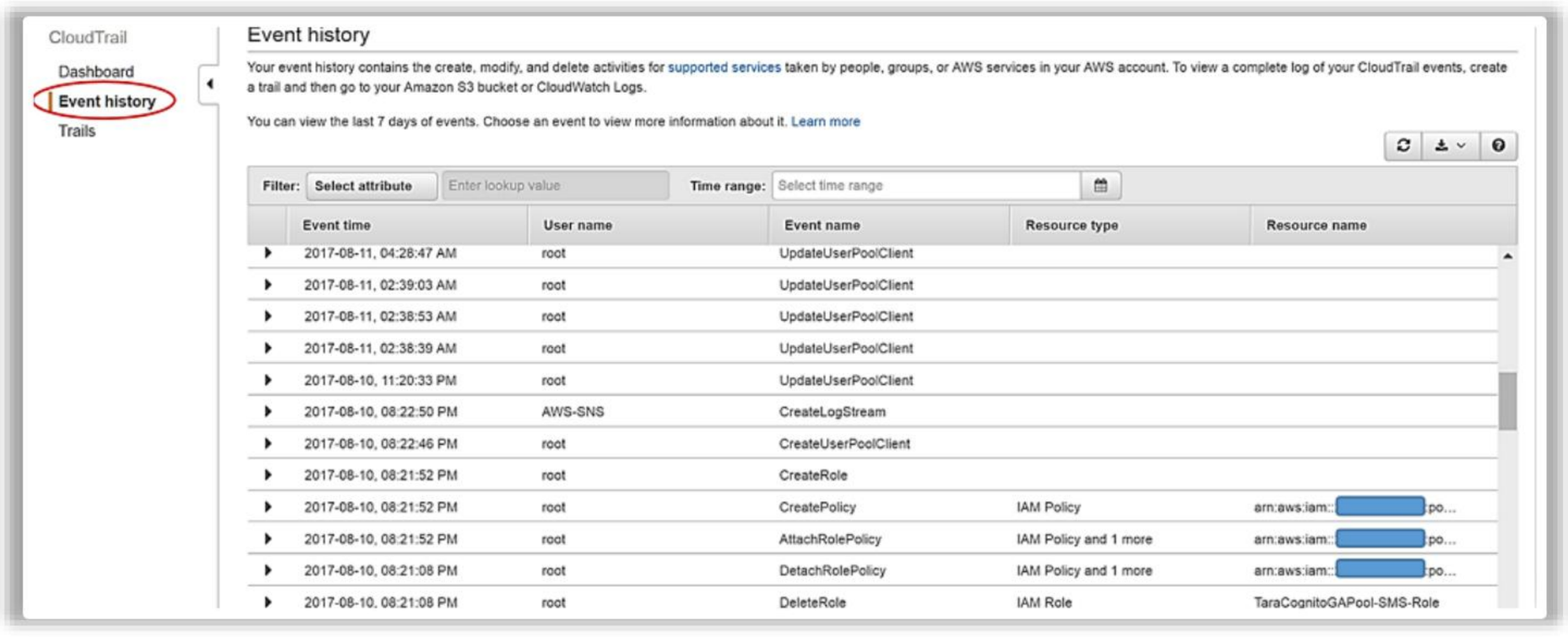


Figure 5.159: Viewing customers' event history in CloudTrail

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

Key Features

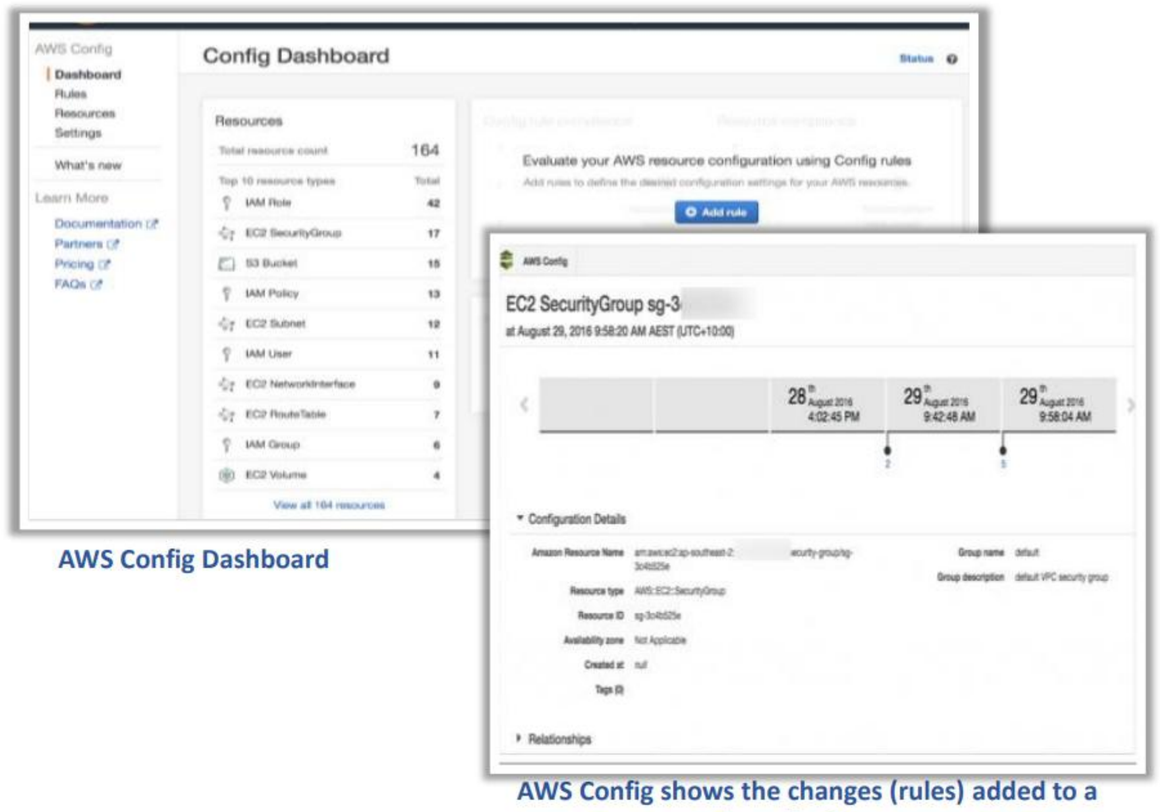
- **Validates the integrity** of AWS CloudTrail log files stored in Amazon S3 buckets and detects whether the log files were unchanged, modified, or deleted.
- **Data events** provide insights into the resource ("data plane") operations performed on or within the resource itself. Additionally, they record the activity of lambda functions and receive details regarding lambda function executions.
- **Management events** provide insights into the management ("control plane") operations performed on the resources in an AWS account. Administrative actions such as creation, deletion, and modification of Amazon EC2 instances are logged.
- **CloudTrail Insights** identify unusual activities in AWS accounts. They can identify the spikes in resource provisioning, bursts of AWS IAM actions, or gaps in periodic maintenance activity.
- **Integration with CloudWatch Events, CloudWatch Logs, and Amazon S3 bucket** to automatically respond to the changes in AWS resources, send management and data events, and invoke lambda function, respectively.

hide01.ir

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

AWS Config

- Use **AWS Config** to review the changes in configurations and relationships between resources, history of resource configuration, and compliance adherence of a particular configuration
- Utilize AWS Config for operational troubleshooting, compliance auditing, security analysis, and change management



AWS Config Dashboard

AWS Config shows the changes (rules) added to a Security Group

Source: https://aws.amazon.com/

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

AWS Config

Using AWS Config, cloud security engineers can assess, audit, and evaluate the configurations of AWS resources. It helps in reviewing the changes in the configurations and relationships between resources, detailed resource configuration histories, and determining overall compliance against the specified configurations. It enables operational troubleshooting, compliance auditing, security analysis, and change management.

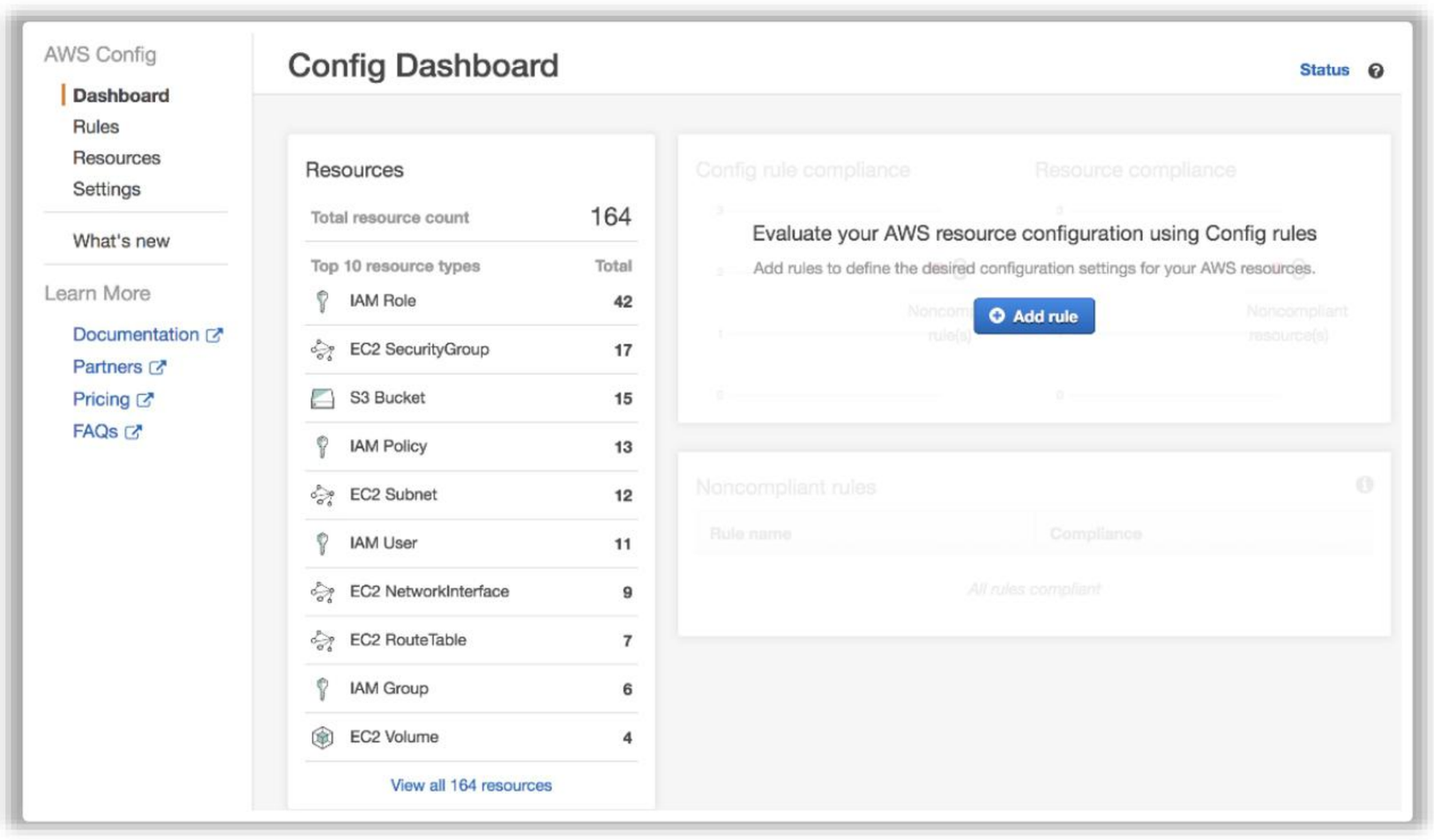


Figure 5.160: AWS Config Dashboard

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

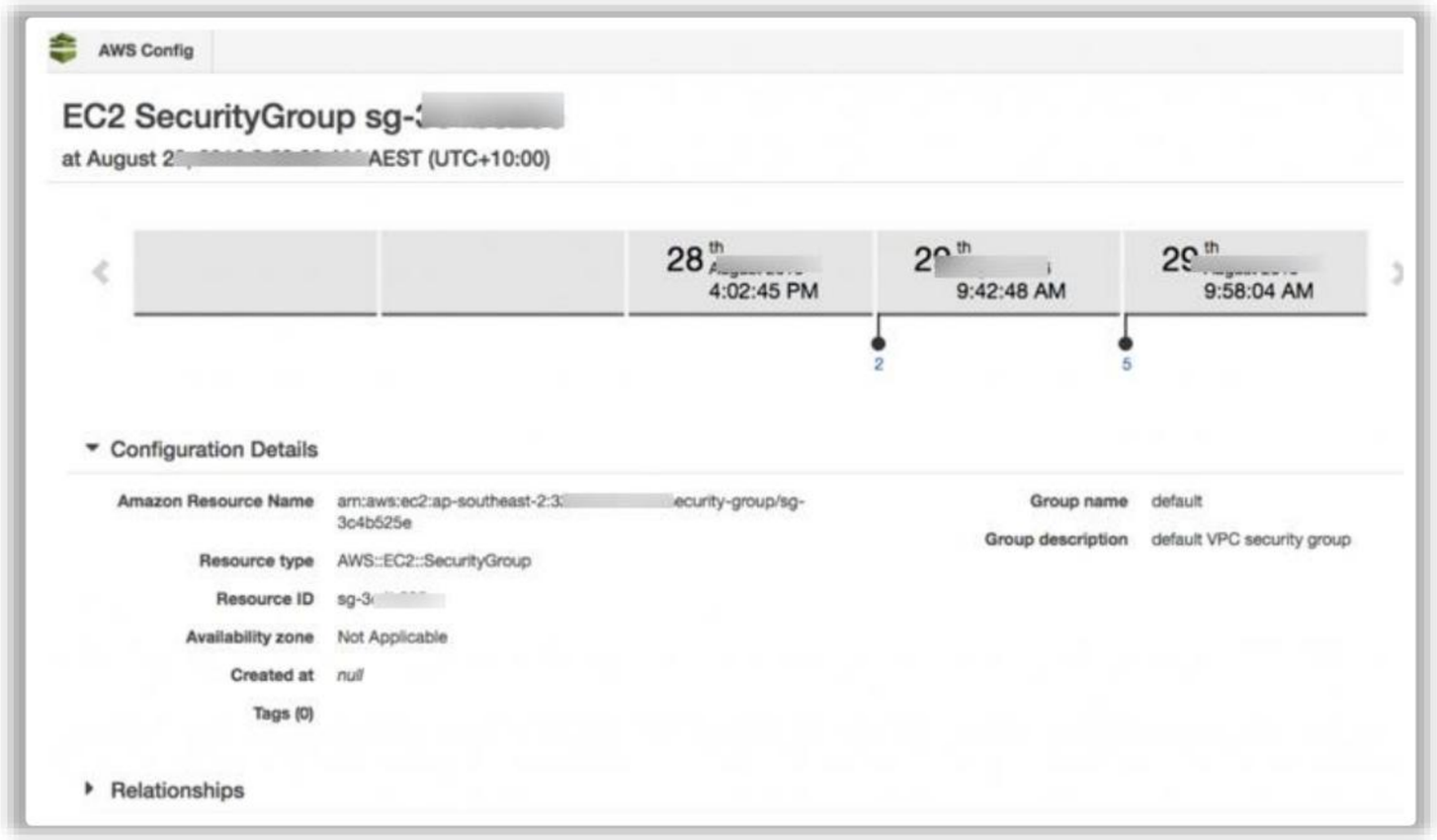
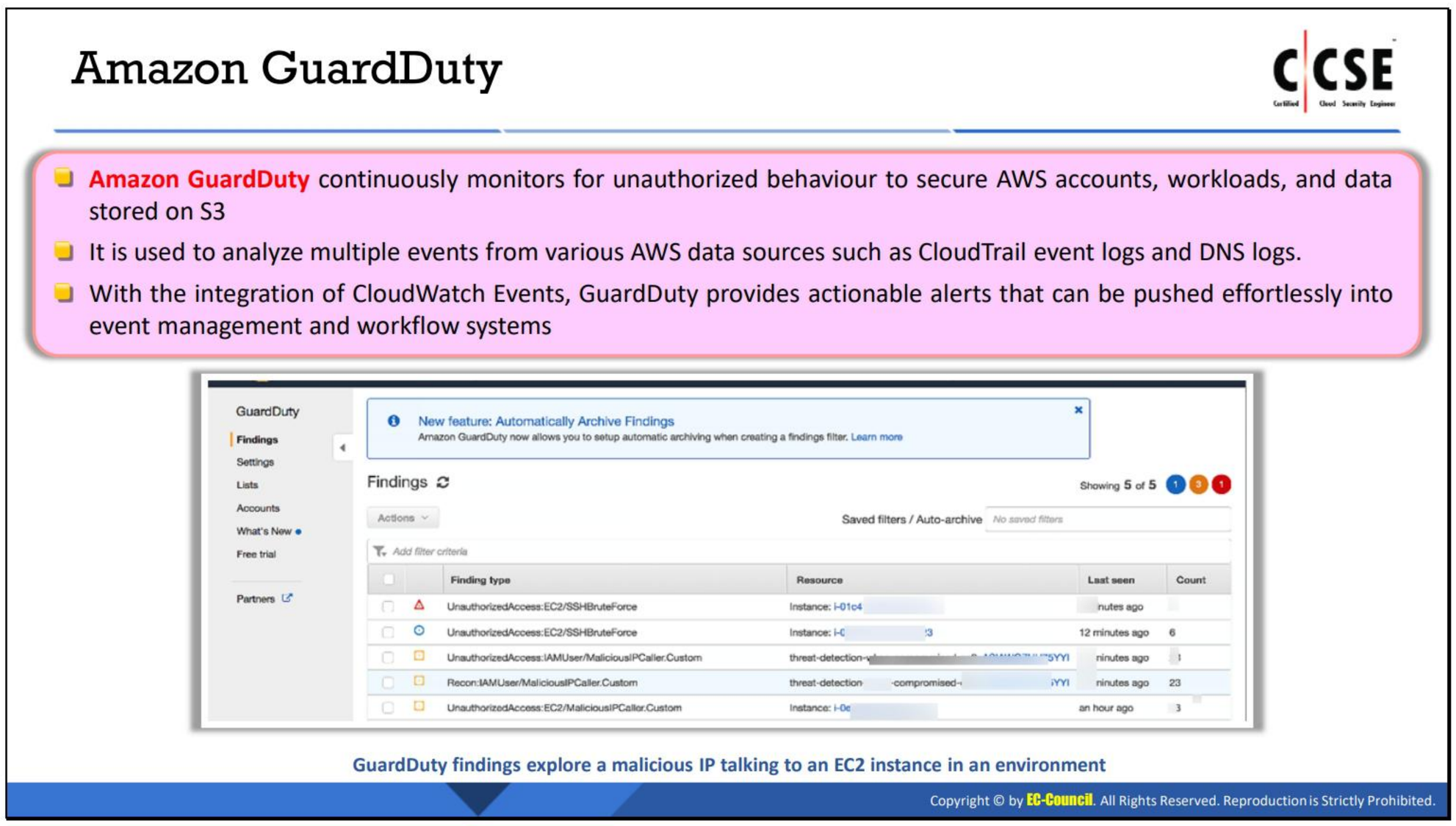


Figure 5.161: AWS Config shows the changes (rules) added to a Security Group

Key Features

- **Configuration history of AWS resources:** AWS Config records the changes in AWS resources to provide configuration history. Additionally, it automatically delivers configuration history files to the specified Amazon S3 bucket.
- **Resource relationships tracking:** AWS Config discovers, maps, and tracks AWS resource relationships in an AWS account.
- **Configurable and customizable rules:** These help to assess resource configurations and resource changes for compliance against the built-in or custom rules.
- **Conformance packs:** These help in managing the compliance of AWS resource configuration at scale (from policy definition to auditing and aggregated reporting) using a common framework and packaging model.
- **Multi-account and multi-region data aggregation:** It enables centralized auditing and governance. It provides an enterprise-wide view of AWS Config rule compliance status and allows associating an organization to quickly add to AWS accounts.
- **Cloud governance dashboard:** It helps to spot non-compliant resources and take appropriate action quickly.

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



GuardDuty findings explore a malicious IP talking to an EC2 instance in an environment

Amazon GuardDuty

The threat detection service, Amazon GuardDuty, continuously monitors for unauthorized behavior to secure AWS accounts, workloads, and data stored on S3. It enables the analysis of billions of events across AWS data sources such as CloudTrail event logs, VPC Flow Logs, and DNS logs. With CloudWatch Event integration, GuardDuty provides actionable alerts that can be pushed effortlessly into event management and workflow systems.

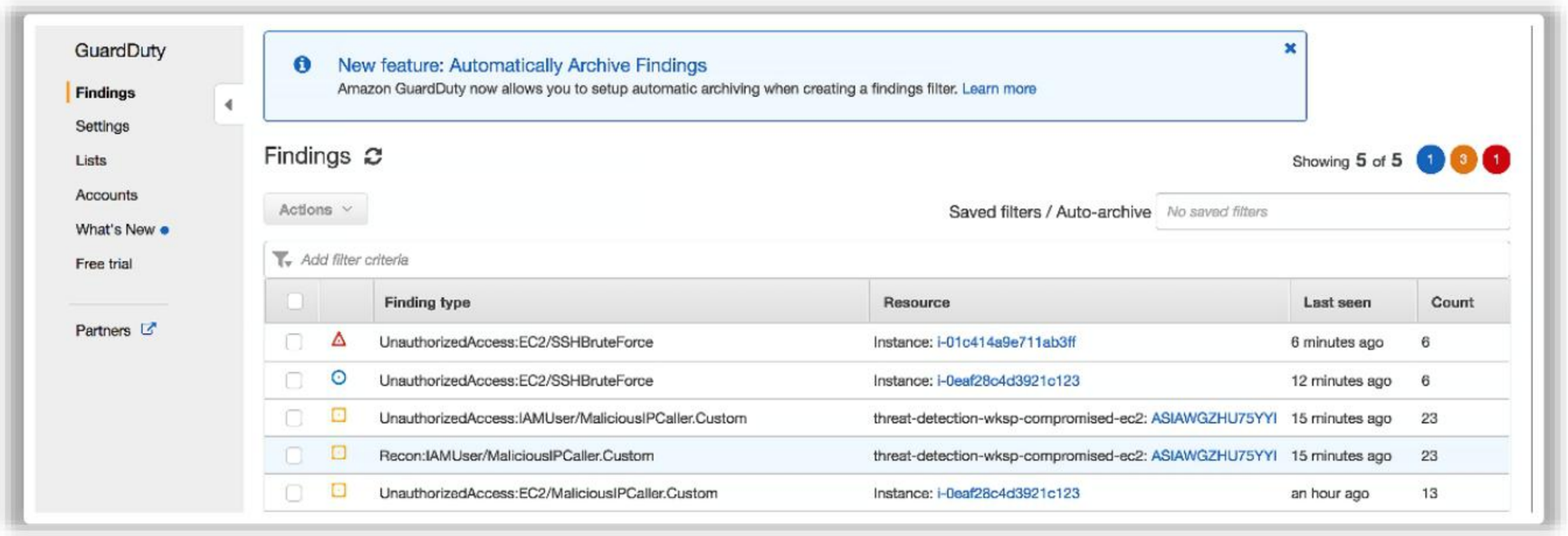


Figure 5.162: GuardDuty Findings explores a malicious IP talking to an EC2 instance in an environment

Key Features

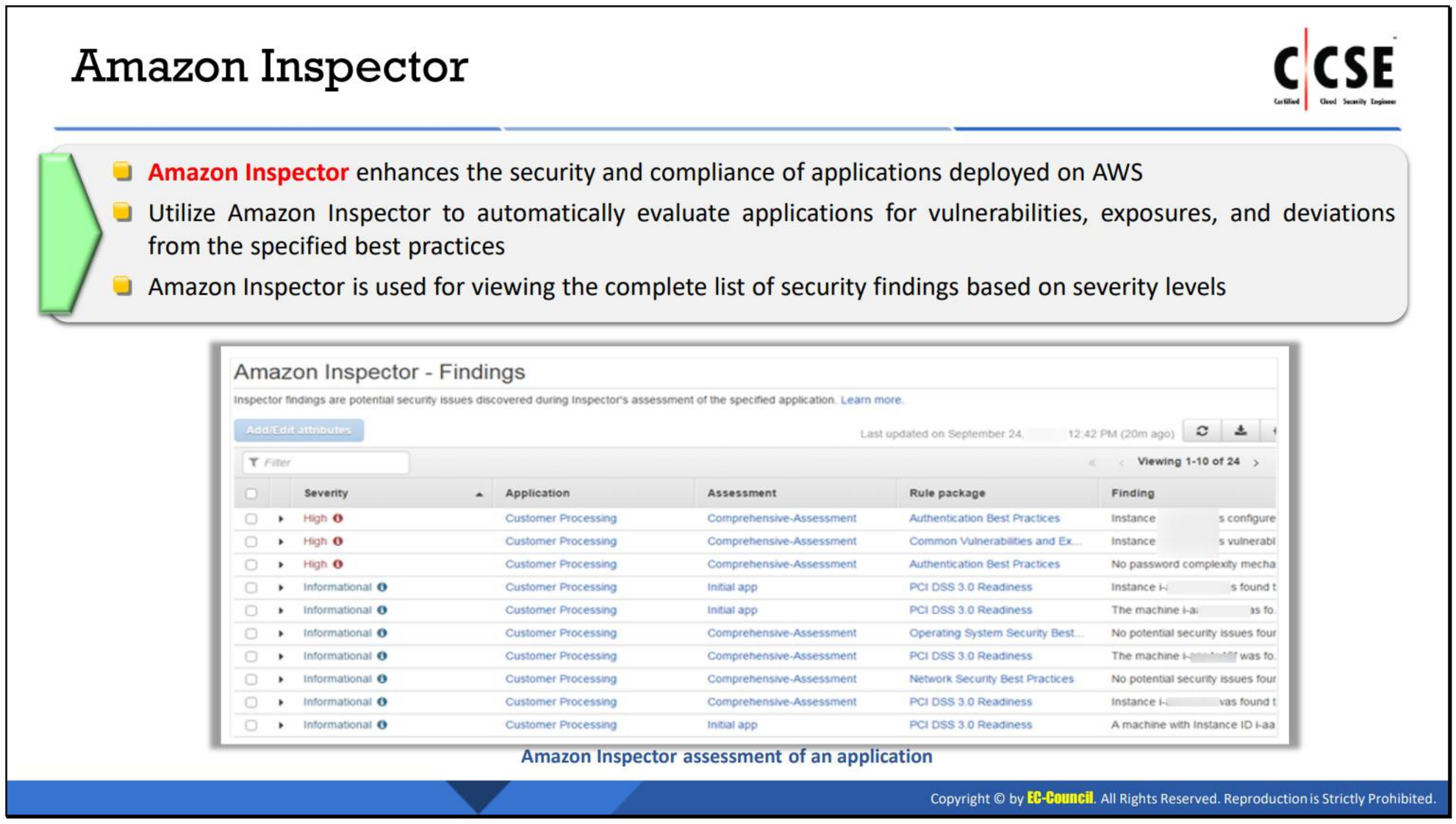
- **Account-level threat detection:** GuardDuty can detect signs of compromised account such as accessing AWS resources from an unusual geo-location at a typical time of day. For programmatic AWS accounts, GuardDuty checks for unusual API calls such as attempts to obscure account activities by disabling CloudTrail logging or taking snapshots of a database from a malicious IP address.

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

- **Continuous monitoring across AWS accounts:** GuardDuty continuously monitors and analyzes AWS accounts and the workload event data found in AWS CloudTrail.
- **Threat detection developed and optimized for the cloud:** Amazon GuardDuty provides access to built-in detection techniques optimized for the cloud. They are
    - **Reconnaissance:** Activity suggesting reconnaissance by an attacker such as unusual API activity, intra-VPC port scanning, unusual patterns of failed login requests, or unblocked port probing from a known bad IP.
    - **Instance compromise**: Activity indicating instance compromise such as cryptocurrency mining, backdoor command and control (C&C) activity, and malware using domain generation algorithms (DGA).
    - **Account compromise**: Common patterns indicative of a compromised account include API calls from unusual geolocation or anonymized proxy, attempts to disable AWS CloudTrail logging, and changes that weaken the account password policy.
    - **Bucket compromise**: Activity indicating bucket compromise such as suspicious data access patterns indicating credential misuse, unusual S3 API activity from a remote host, and unauthorized S3 access from known malicious IP addresses.
- **Threat severity levels for prioritization:** Severity levels (Low, Medium, and High) help to prioritize the response to potential threats.
    - **Low severity level** indicates a malicious activity that was blocked before it compromised a resource.
    - **Medium severity level** indicates a suspicious activity. For example, a large amount of traffic being returned to a remote host that is hiding behind the Tor network or activity that deviates from the normally observed behavior.
    - **High severity level** indicates that the resource in question (e.g., an EC2 instance or set of IAM user credentials) is compromised and actively being used for unauthorized purposes.
- **Automate threat response and remediation:** Amazon GuardDuty offers HTTPS APIs, CLI tools, and Amazon CloudWatch Events to support automated security responses to security findings. For example, you can automate the response workflow using CloudWatch Events as an event source to trigger an AWS lambda function.

hide01.ir

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



Amazon Inspector

Amazon Inspector enhances the security and compliance of applications deployed on AWS. It is used to automatically evaluate applications for vulnerabilities, exposures, and deviations from the specified best practices. After assessment, it displays a detailed list of security findings prioritized by severity levels. Its security assessments help to check for vulnerable software versions.

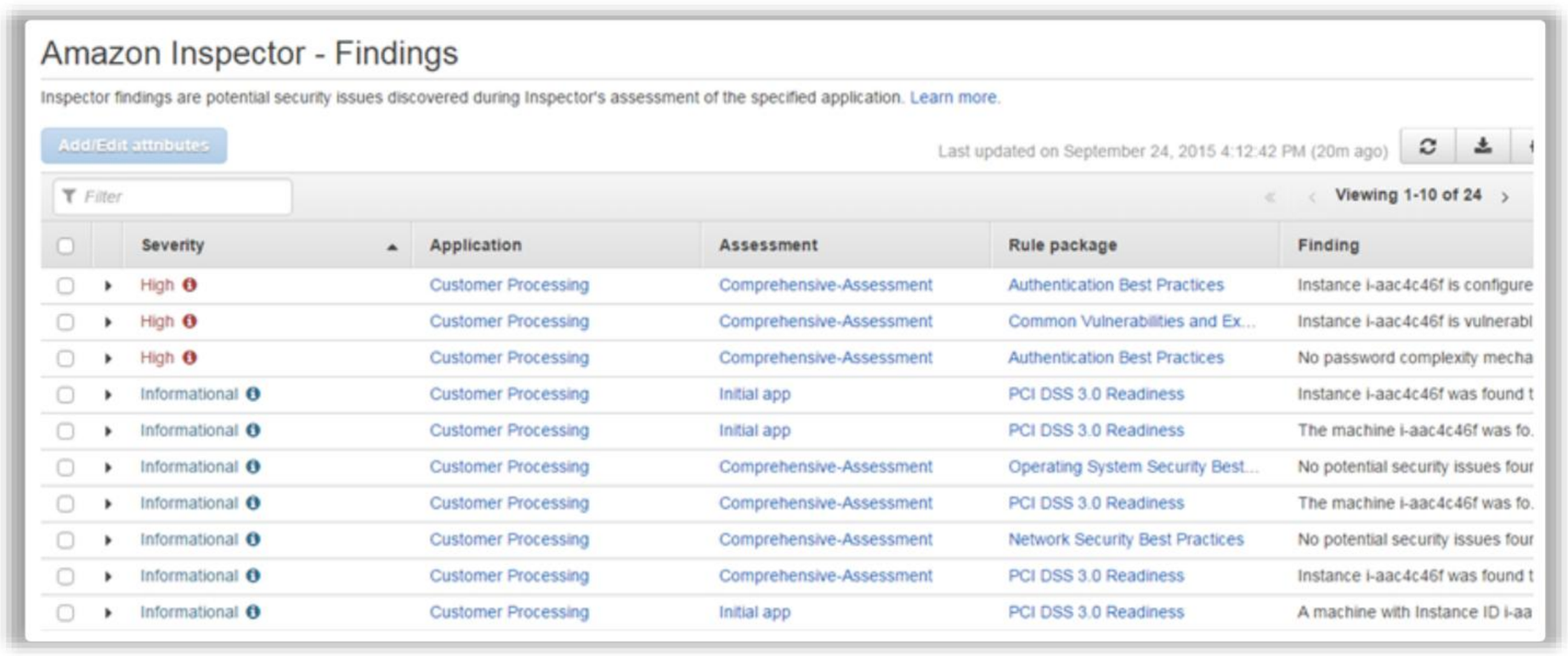


Figure 5.163: Amazon Inspector assessment of an application

Key Features

- **Integrate security into DevOps:** Amazon Inspector analyzes the network configurations in an AWS account and uses an optional agent for visibility into Amazon EC2 instances. This helps in building Inspector assessments into the existing DevOps process,

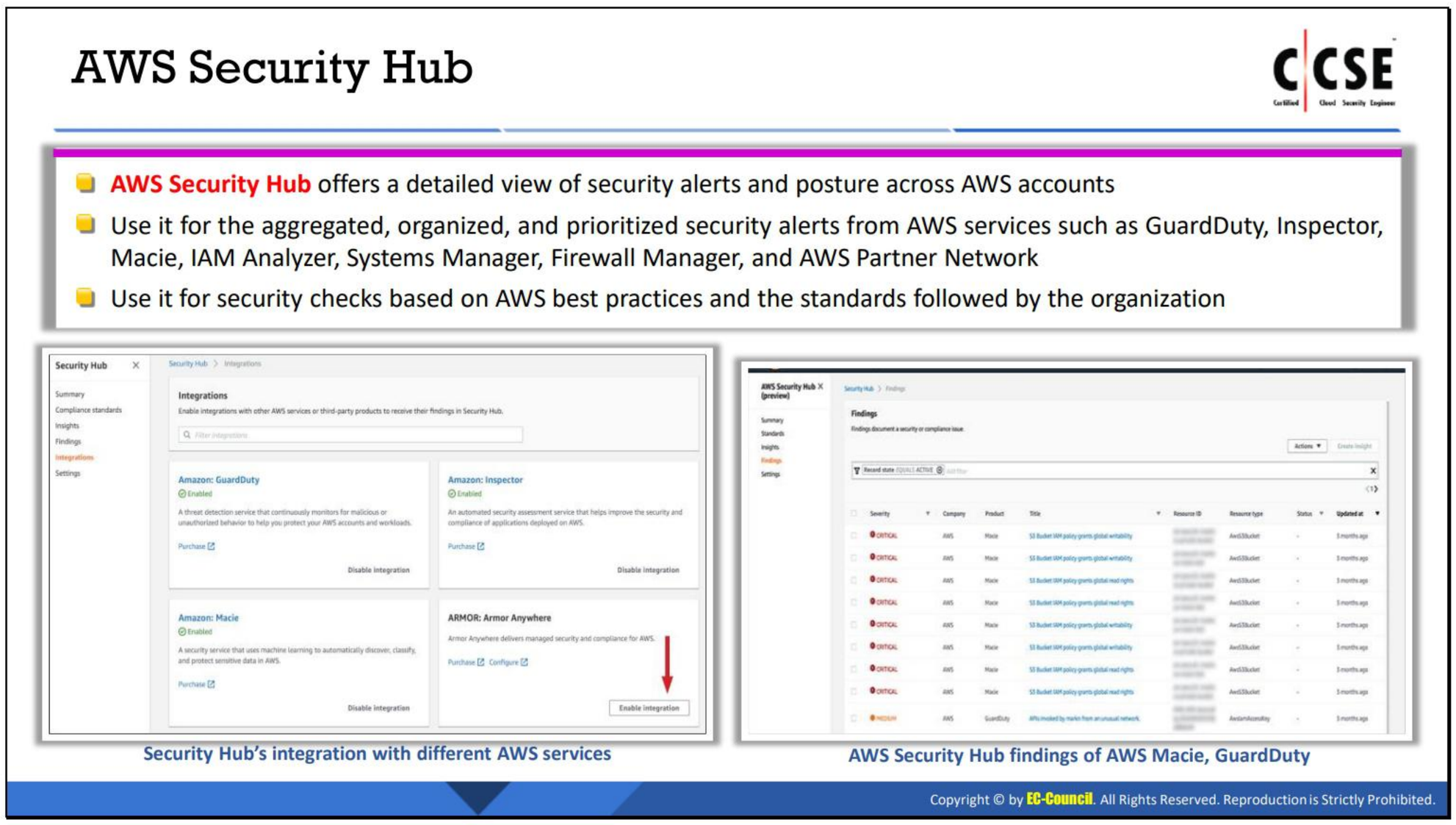
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

decentralizing and automating vulnerability assessments, and empowering the development and operation teams to make security assessments an integral part of the deployment process.

- **Increase development agility:** Amazon Inspector helps to automate the security assessment of applications and identify vulnerabilities. This enables development and iteration on new applications quickly and assessment of compliance with best practices and policies.
- **Streamline security compliance:** Amazon Inspector provides visibility into security testing performed during the development of applications on AWS. This streamlines the process of validating and demonstrating that security, compliance standards, and best practices are being followed throughout the development process.

hide01.ir

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



AWS Security Hub

AWS Security Hub provides a view of security alerts and security posture across AWS accounts. It provides different tools, ranging from firewalls to vulnerability and compliance scanners. Security Hub provides aggregated, organized, and prioritized security alerts from AWS such as GuardDuty, Inspector, Macie, IAM Analyzer, Systems Manager, Firewall Manager, and AWS Partner Network. AWS Security Hub monitors the environment of an organization continuously using security checks based on AWS best practices and organizational standards. It acts on security findings by investigating them according to Amazon Detective/CloudWatch Event rules.

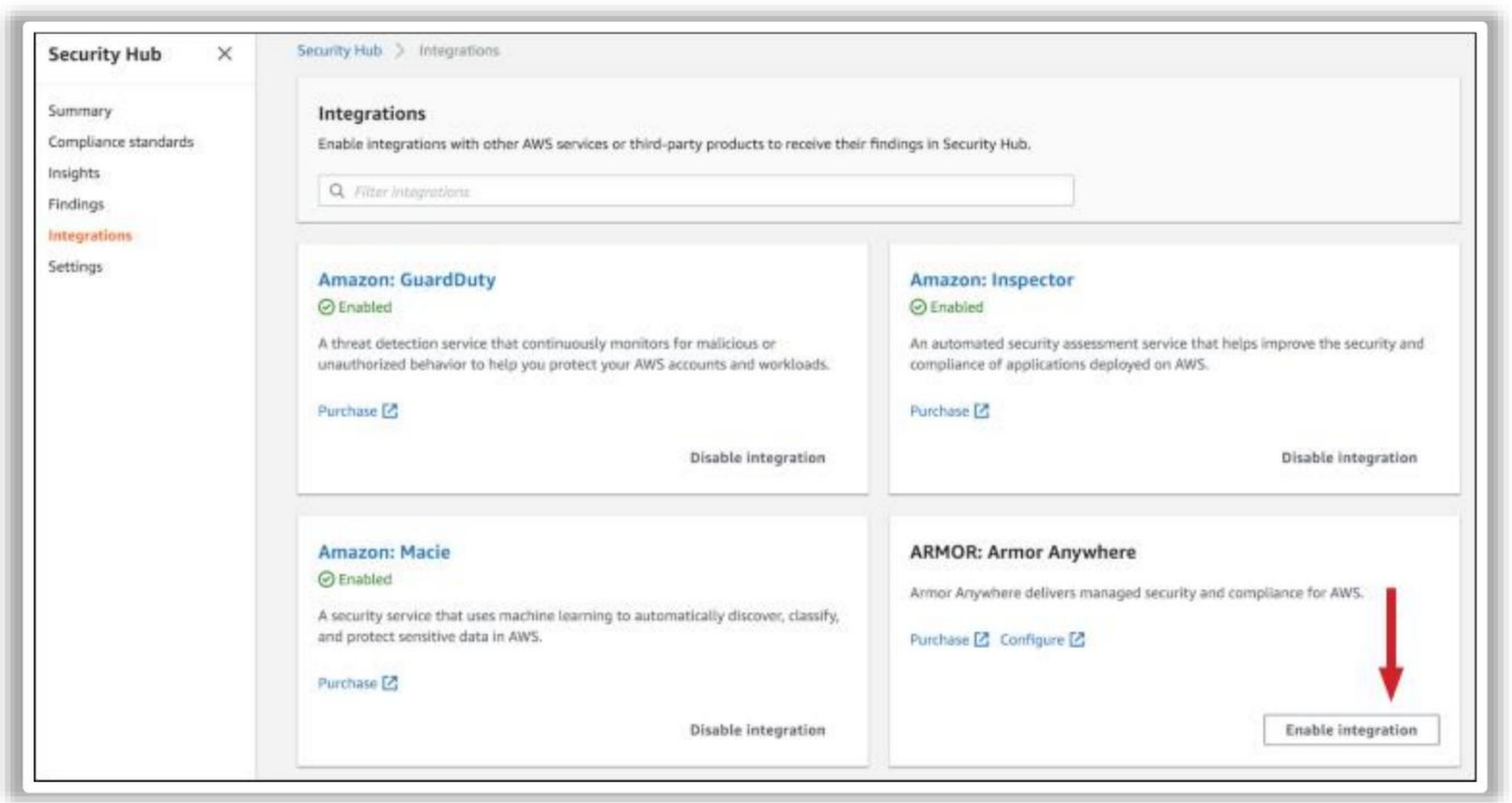


Figure 5.164: Security Hub integration with different AWS resources

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

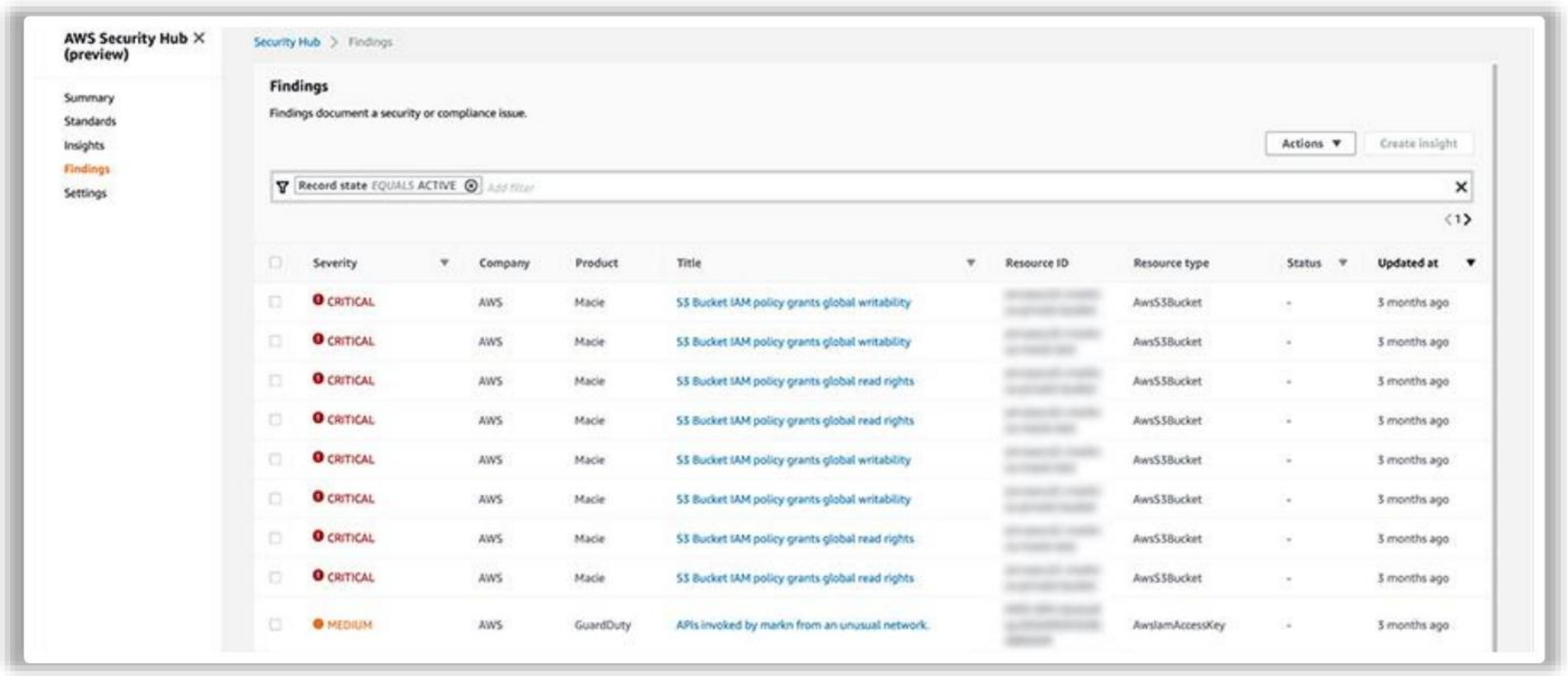


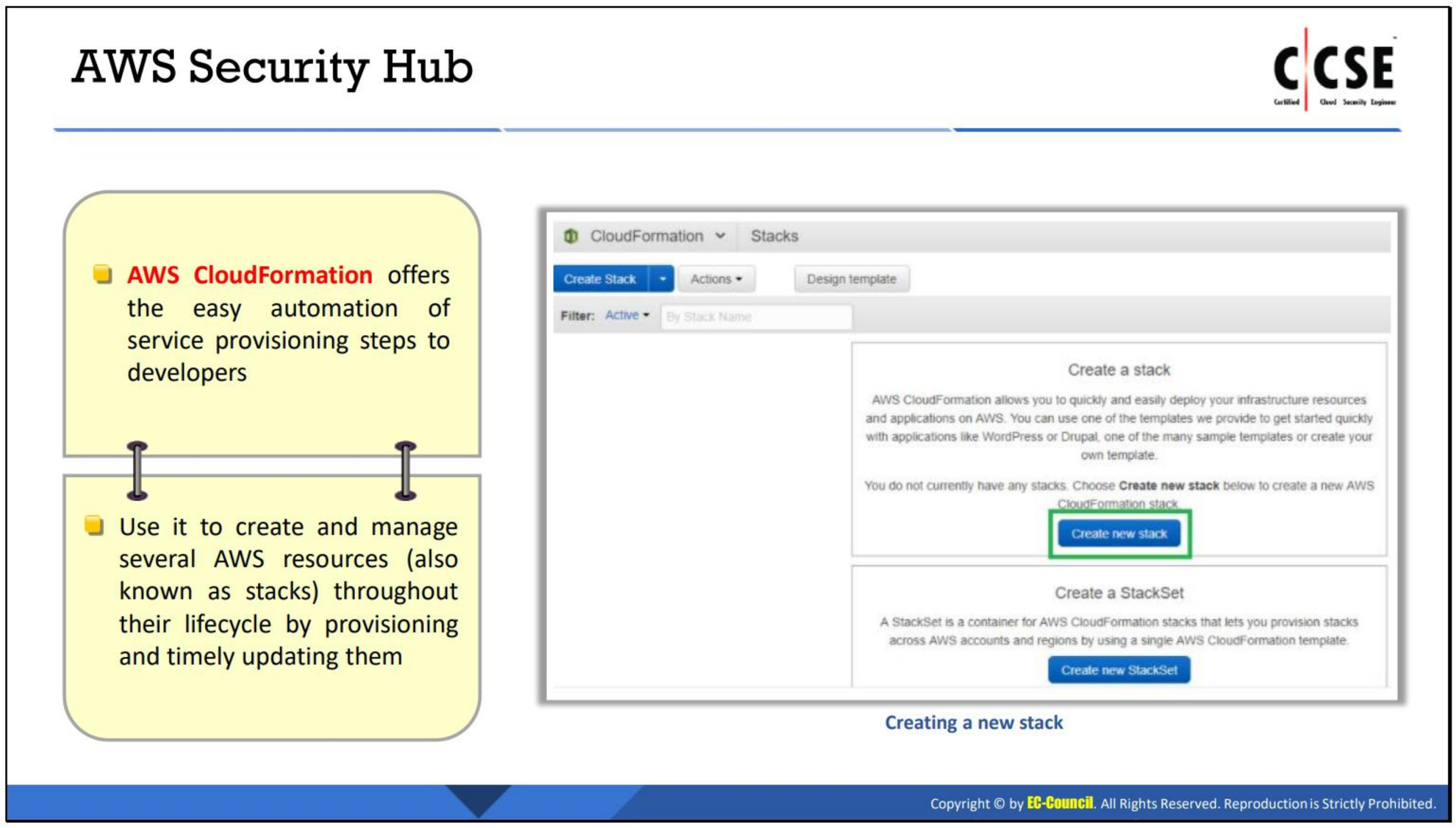
Figure 5.165: AWS Security Hub findings of AWS Macie, GuardDuty

Key Features

- **Automated and continuous security checks:** It automates continuous, account, and resource-level configuration and security checks using industry standards and best practices. For example, AWS Security Hub automates the Payment Card Industry Data Security Standard (PCI DSS) and Center for Internet Security (CIS) AWS Foundations Benchmark, a set of security configuration best practices for AWS. If any account or resource deviates from a best practice, AWS Security Hub flags a problem and recommends remediation steps.
- **Custom response and remediation actions:** AWS Security Hub integrates with Amazon CloudWatch events, thus enabling the creation of custom response and remediation workflows. You can easily send the findings to SIEM, chat tools, ticketing systems, Security Orchestration Automation and Response (SOAR) tools, and on-call management platforms. AWS System Manager Automation documents, AWS Step Functions, and AWS lambda functions can be used to build automated remediation workflows that can be initiated from Security Hub.
- **Visual summary dashboard:** Monitor the security posture and quickly identify security issues and trends using the summary dashboard of AWS Security Hub. For example, drill down into a trendline graph to discover that a set of Amazon EC2 instances with a high number of findings were created using the same Amazon Machine Images (AMI).

hide01.ir

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



AWS Security Hub

AWS CloudFormation is a service of AWS that offers the tools required to create and manage the infrastructure needed for applications to run on AWS. Developers can use AWS CloudFormation to automate service provisioning steps easily. CloudFormation can create and manage several AWS resources (also known as stacks) throughout their lifecycle by provisioning them and timely updating them. It allows to manage these resources or the infrastructure in a template or text file. Templates can be used to deploy the resources required for an application and are reusable.

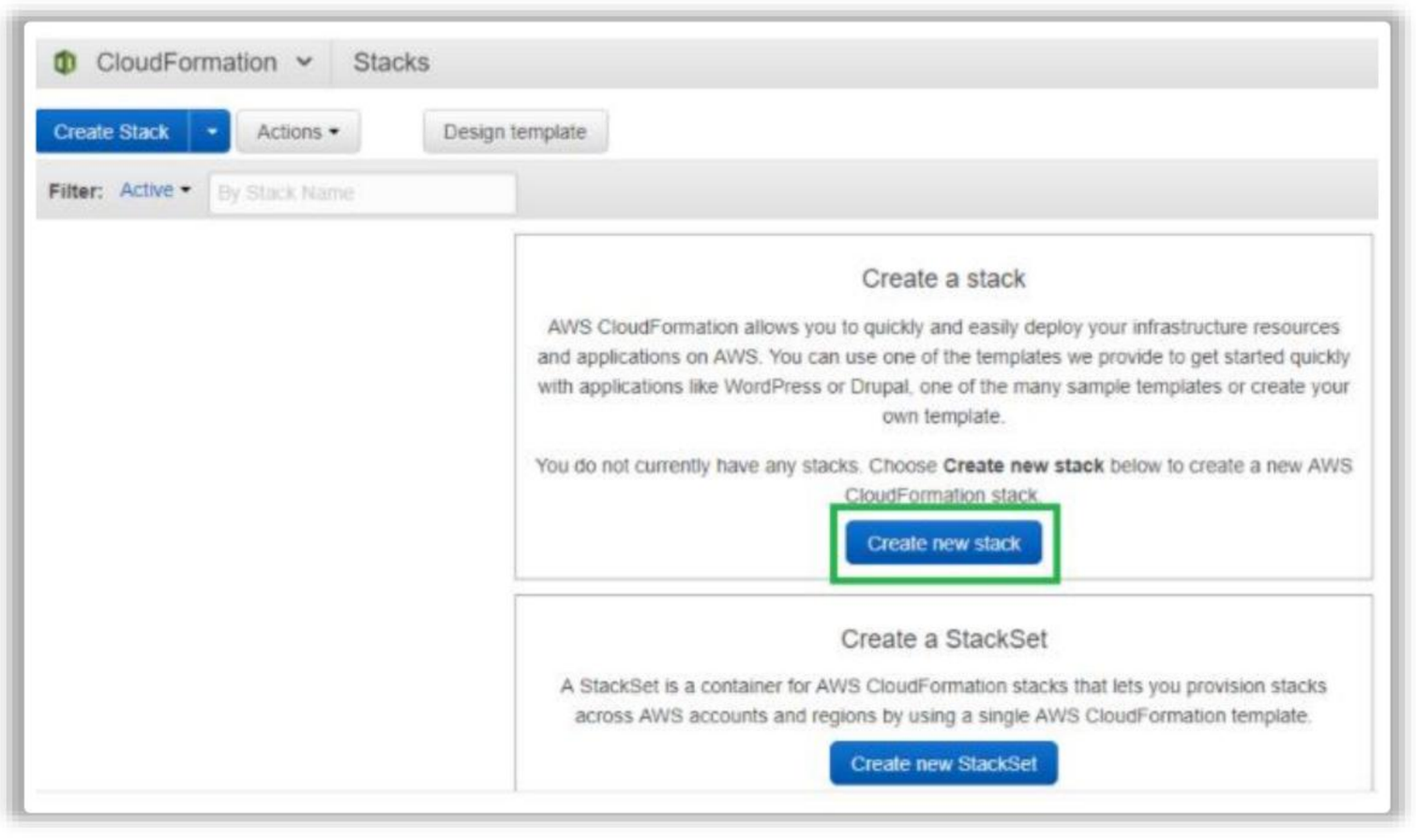


Figure 5.166: Creating a new stack

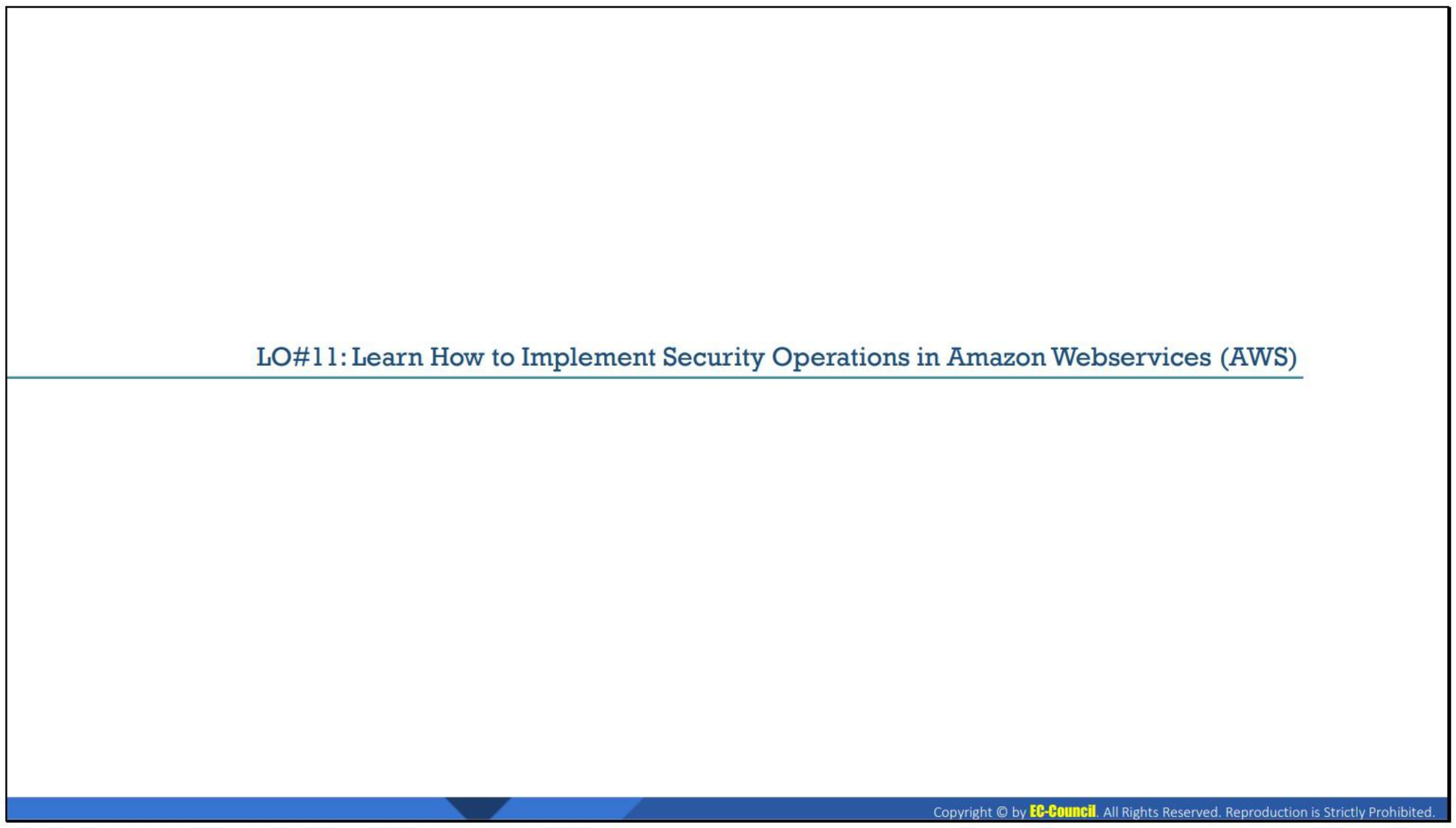
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Features of AWS CloudFormation

- **Extensibility**: AWS CloudFormation Registry helps to create and provision AWS and third-party resources such as incident management tools, team productivity tools, and version control tools.
- **Cross-account and cross-region management**: With CloudFormation StackSets, a common collection of AWS resources can be provisioned across several accounts and regions via a single CloudFormation template.
- **Serverless applications**: AWS SAM allows to build serverless applications easily. Applications can be defined and modeled using YAML with a few lines per resource.
- **Safety controls**: The changes proposed by CloudFormation that are to be applied to the infrastructure and application resources should be previewed before they are executed with the help of ChangeSets. Similarly, changes made to resources outside CloudFormation should be tracked using Drift Detection.
- **Dependency management**: CloudFormation manages the dependencies between various resources during stack management actions automatically. While performing stack operations, it determines the correct series of actions required for each resource.

hide01.ir

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

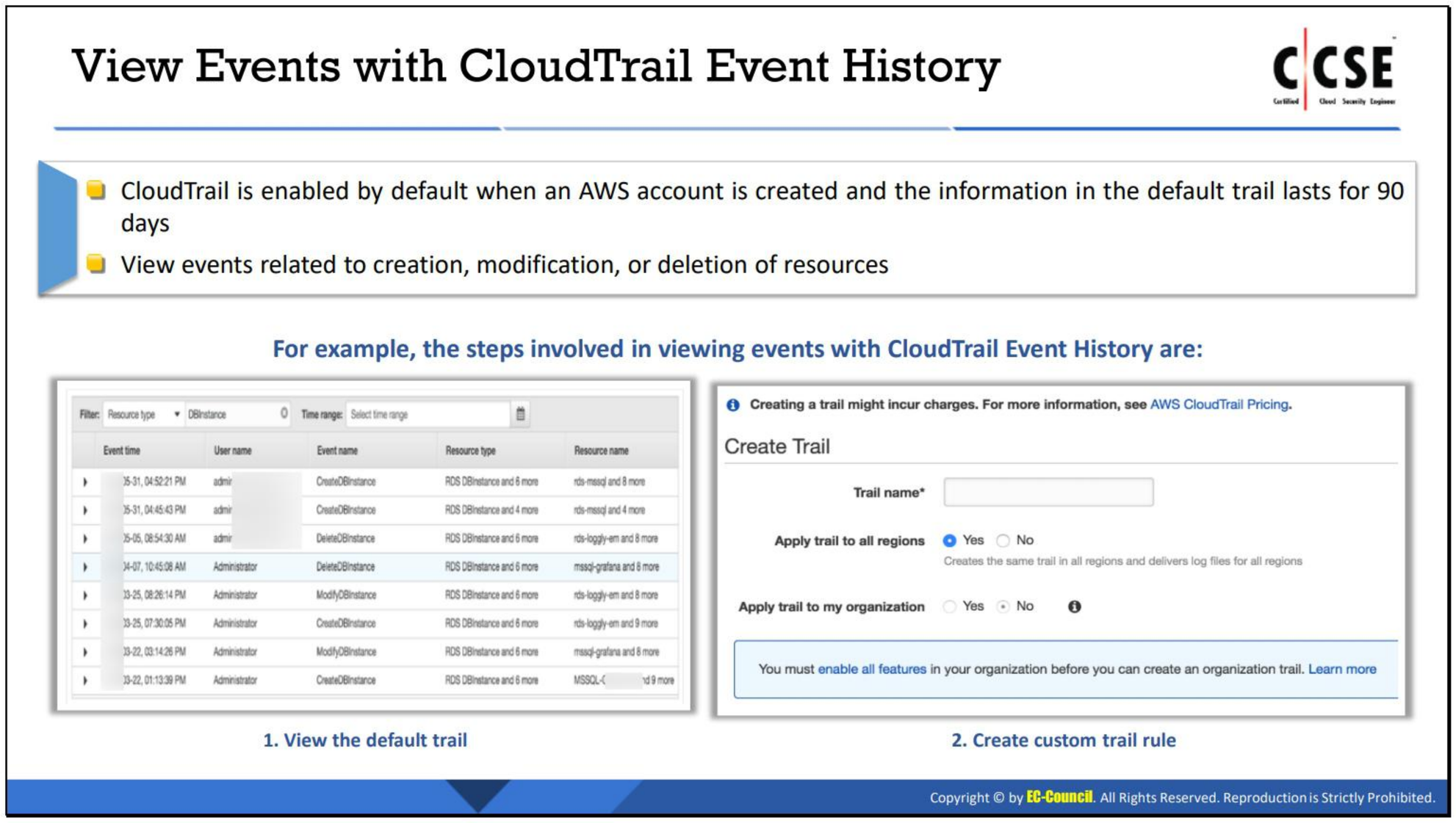


LO#11: Learn How to Implement Security Operations in Amazon Webservices (AWS)

The objective of this section is to implement operational security in AWS using various services. In this section, cloud security engineers will learn how to view events, monitor and record AWS resource configurations, monitor AWS resources, and enable and analyze VPC flow logs. This section will help cloud security engineers in securing their AWS cloud environment.

ehid91.ir

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



View Events with CloudTrail Event History

CloudTrail is enabled by default when an AWS account is created. The information in this default trail lasts for 90 days. Thus, the events related to creation, modification, or deletion of resources can be viewed. Moreover, admins can customize the display of event history in the console.

Steps to view events with CloudTrail Event History

- **View the default trail**
  - Open the CloudTrail console and select **Event history** from the navigation pane.

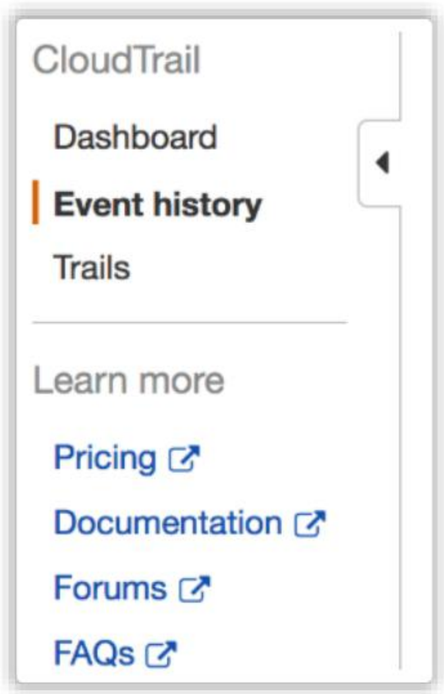


Figure 5.167: Event History

  - Select a date range, particular resource type or resource name, event name, AWS access key ID, and other filters for specific search results. For example, the image below view events related to RDS DBInstance type resource.

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

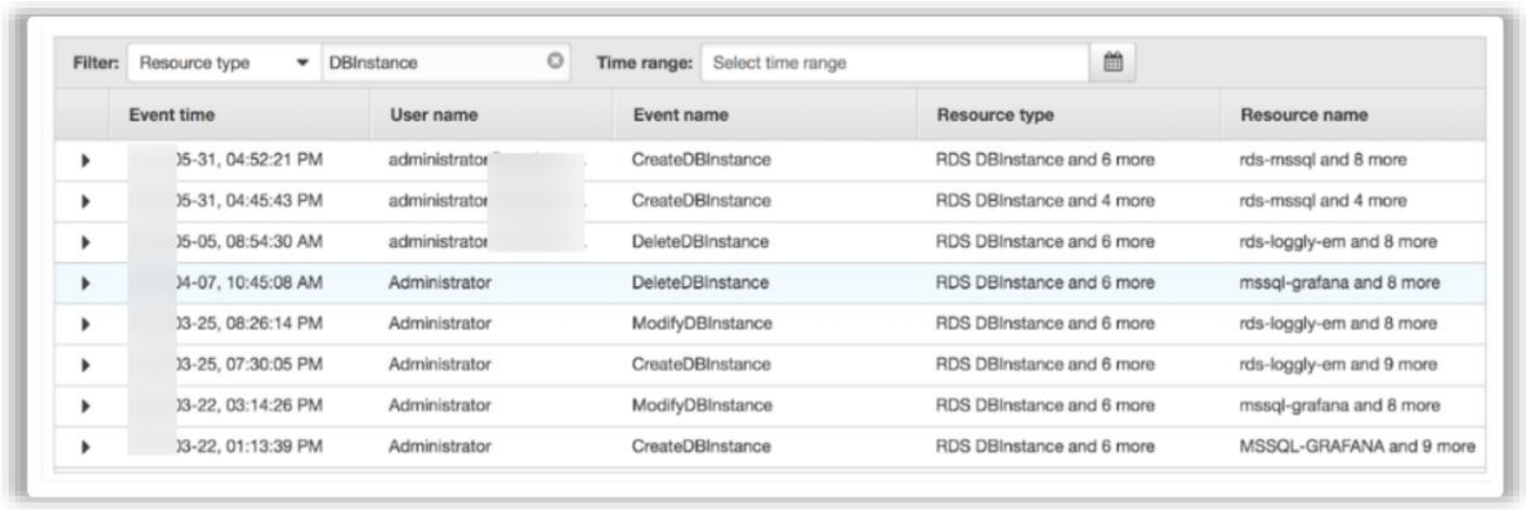


Figure 5.168: Event History

- Click on a particular event record for more information. The following image shows a part of the JSON record for the DeleteDBInstance event.

Figure 5.169: JSON Record

It can be observed that the IAM user **Administrator** has deleted the **mysql-db** instance at a particular date and time in **US-East-1** region. The user did not take a snapshot before deleting the instance. The user could log into the console without MFA. Use this information to start using MFA to review access to RDS.

- **Create a custom trail**

  Create custom trails or user-created audit definition to capture one or more types of events. Unlike Event History, these CloudTrail trail logs are not limited to 90 days. Deliver

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

these to S3 bucket/AWS CloudWatch Logs and configure to send SNS notifications when an event occurs.

- Here, ensure that **Trail1**'s log files are delivered to an S3 bucket, **athena-cloudtrails**.

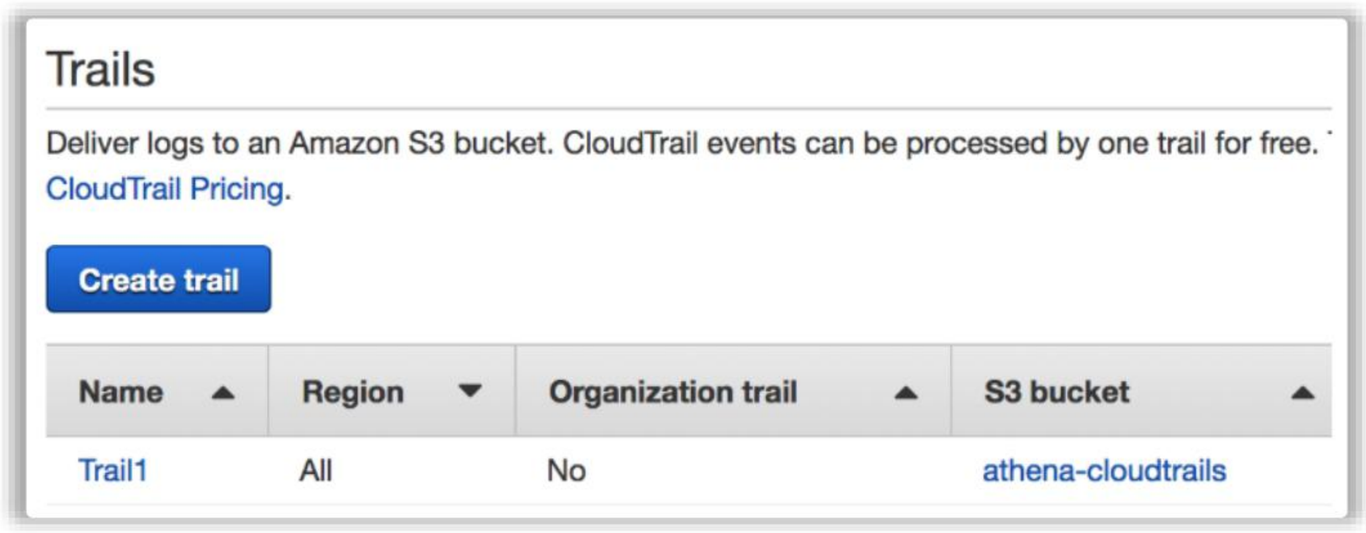


Figure 5.170: Trails

- To define a trail, define the following parameters.

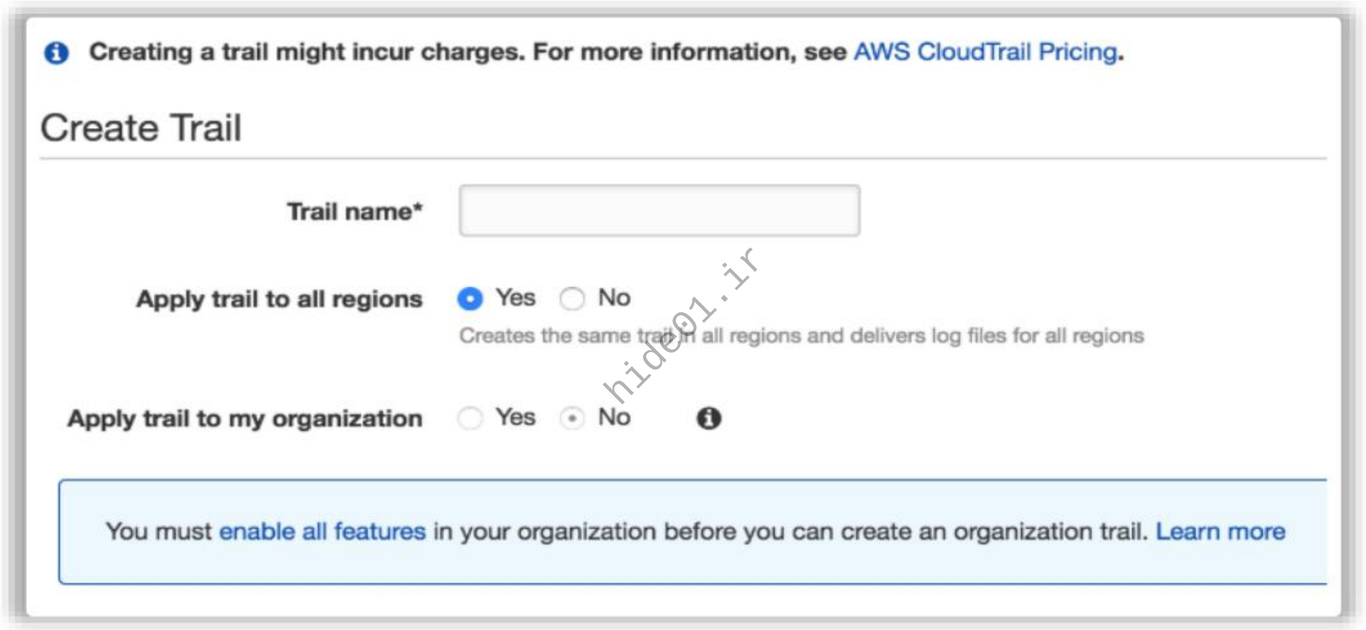


Figure 5.171: Create Trail

- Specify the events to be tracked: **read events** such as **Describe** or **List** API operations, **write events** such as **Create** or **Delete** operations, both type of operations, or **None**. These "management events" are related to the actions performed on resources, not actions happening within the resources.

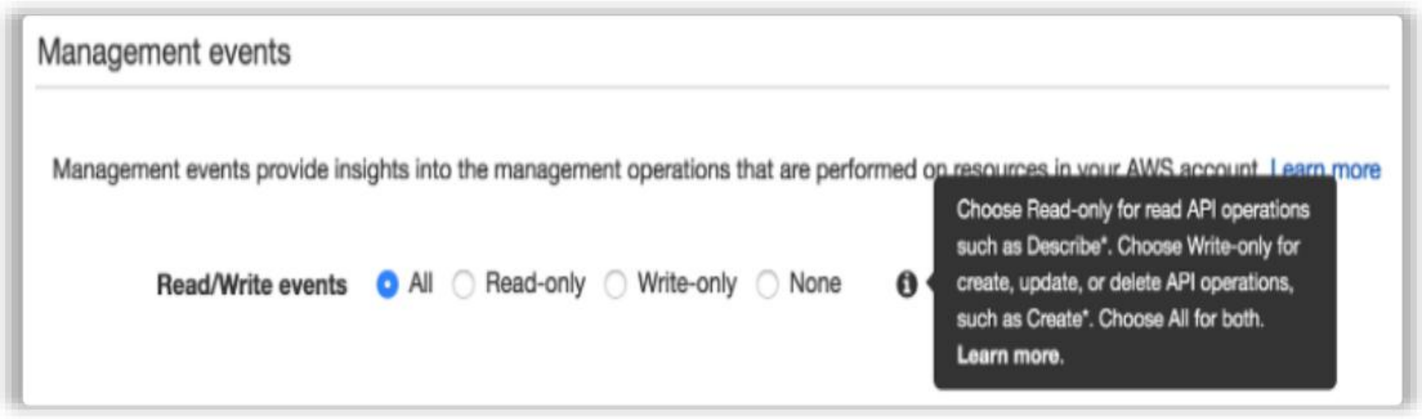


Figure 5.172: Management Events

- Next, track data events because these data events track API operations within a specific resource. It supports two types of resource operations during writing,

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

namely S3 and lambda. With data events, track S3 bucket level operations such as **PutObject**. Track it for all or specific buckets.

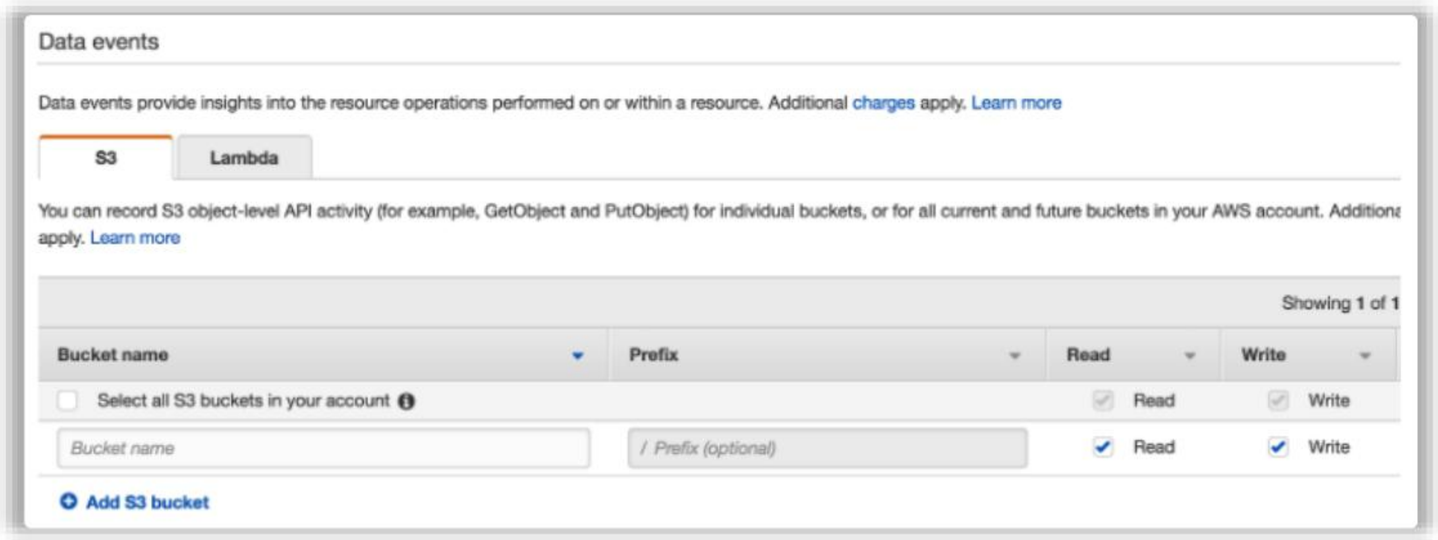


Figure 5.173: Data Events

- For lambda, use the trail to capture an event each time a function is invoked.

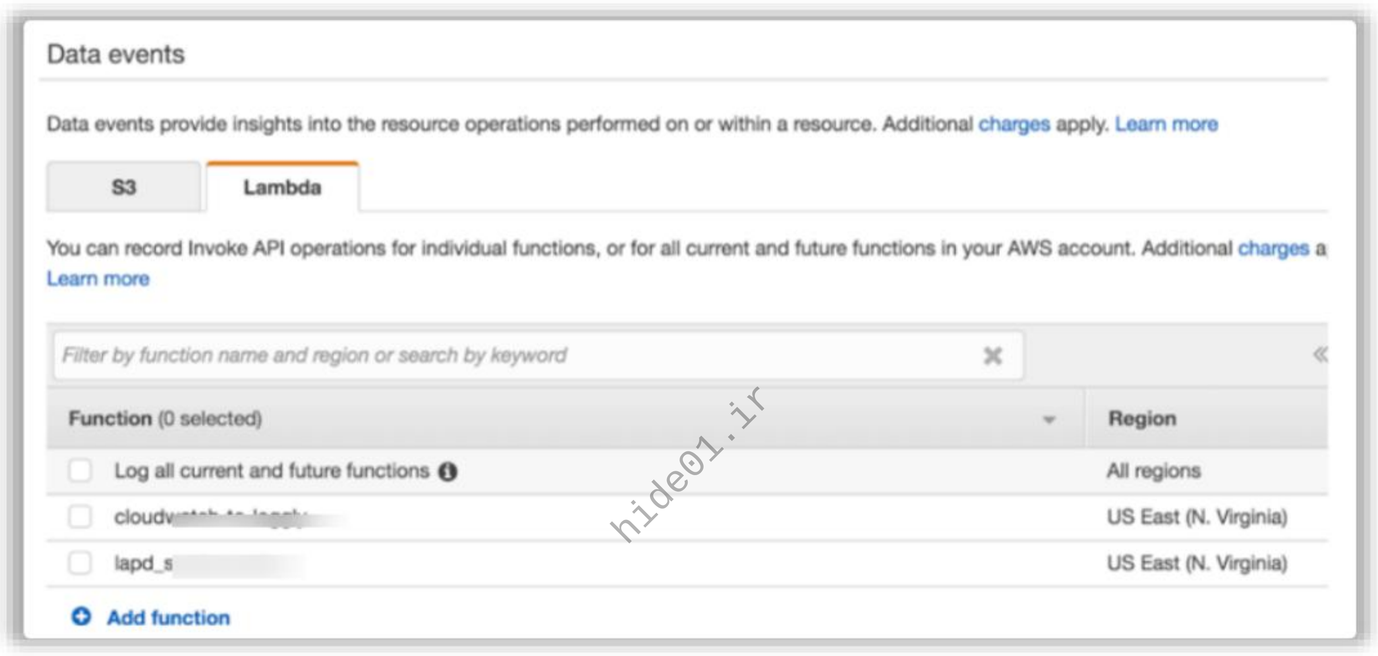


Figure 5.174: Lambda

- Specify where the data will be stored.

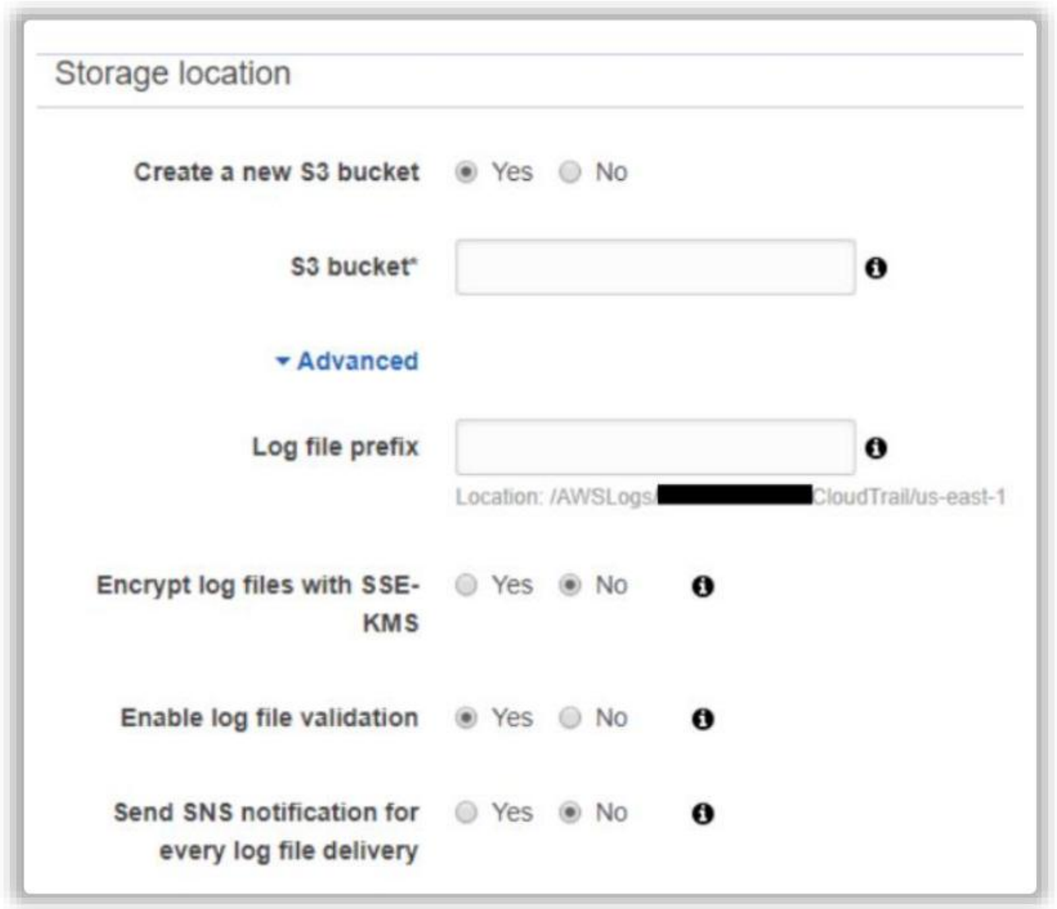


Figure 5.175: Storage Location

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

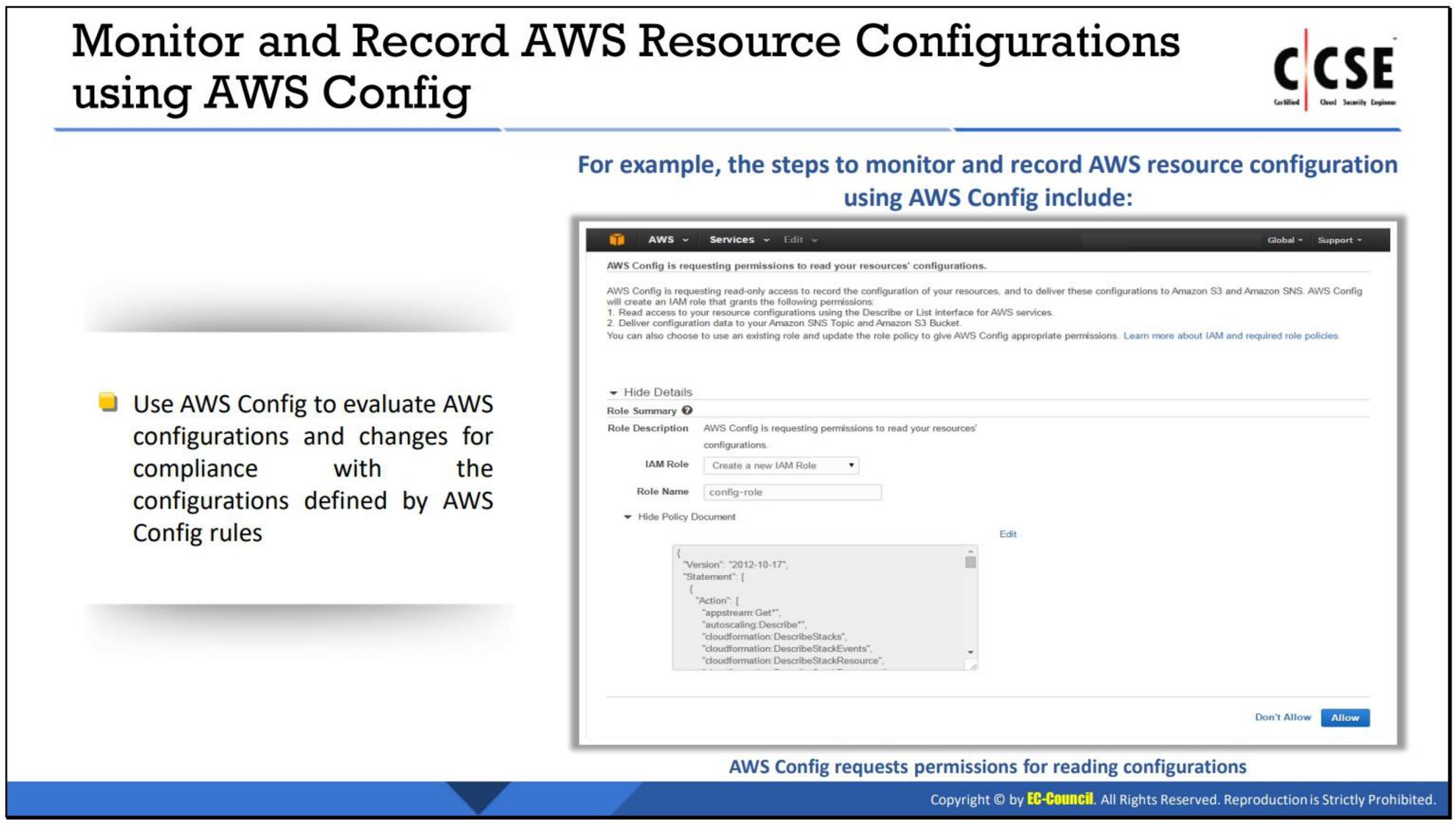
- Create a new bucket or select an existing bucket to store the trail log files. The log files will be saved under a folder in the S3 bucket. The folder structure has the following naming style.

```
/AWSLogs/<account-id>/CloudTrail/<region>/yyyy/mm/dd/.
```

  Select the option to include a file name prefix. Admins can also get notified via SNS alerts every time a CloudTrail log file is created.

hide01.ir

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



Monitor and Record AWS Resource Configurations using AWS Config

Use AWS Config to evaluate AWS configurations and changes for compliance with the configurations defined by AWS Config Rules.

h1de01.ir

Steps to monitor and record AWS resource configuration using AWS Config

- In the **Set-up AWS Config** page, specify tracking in all resources in a defined region or you can add certain types of AWS resources.
- Select **Record all resources in this region,** specify the new bucket name (here, it is **config-test-bucket-18dec2015**), and provide a new topic (here, it is **config-test-topic-18dec2015**). Track all global resources such as IAM users, groups, roles, and managed policies. Click on **Continue**.

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

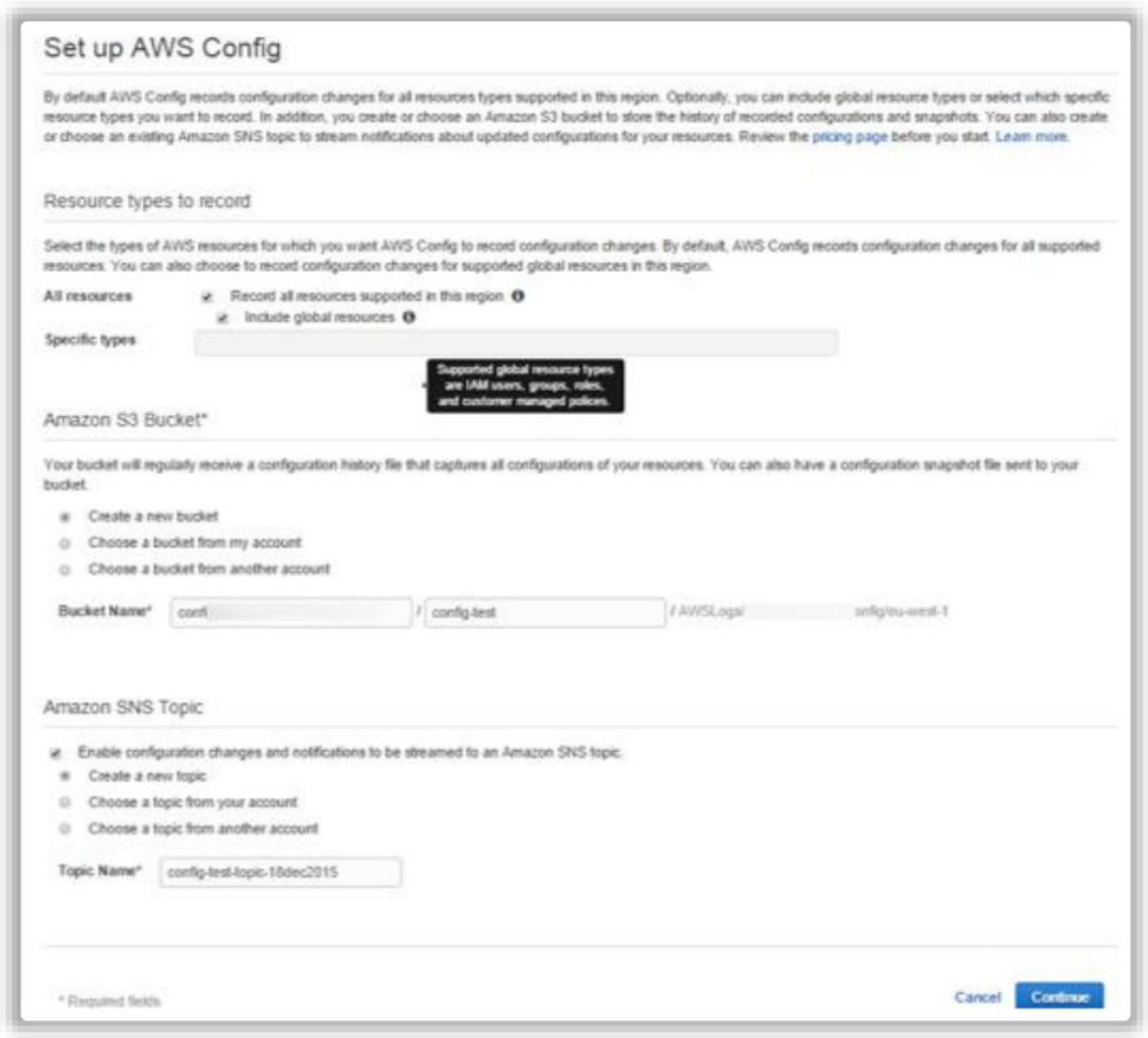


Figure 5.176: Set Up AWS Config

- A new IAM role will be created. Click on **Allow**.

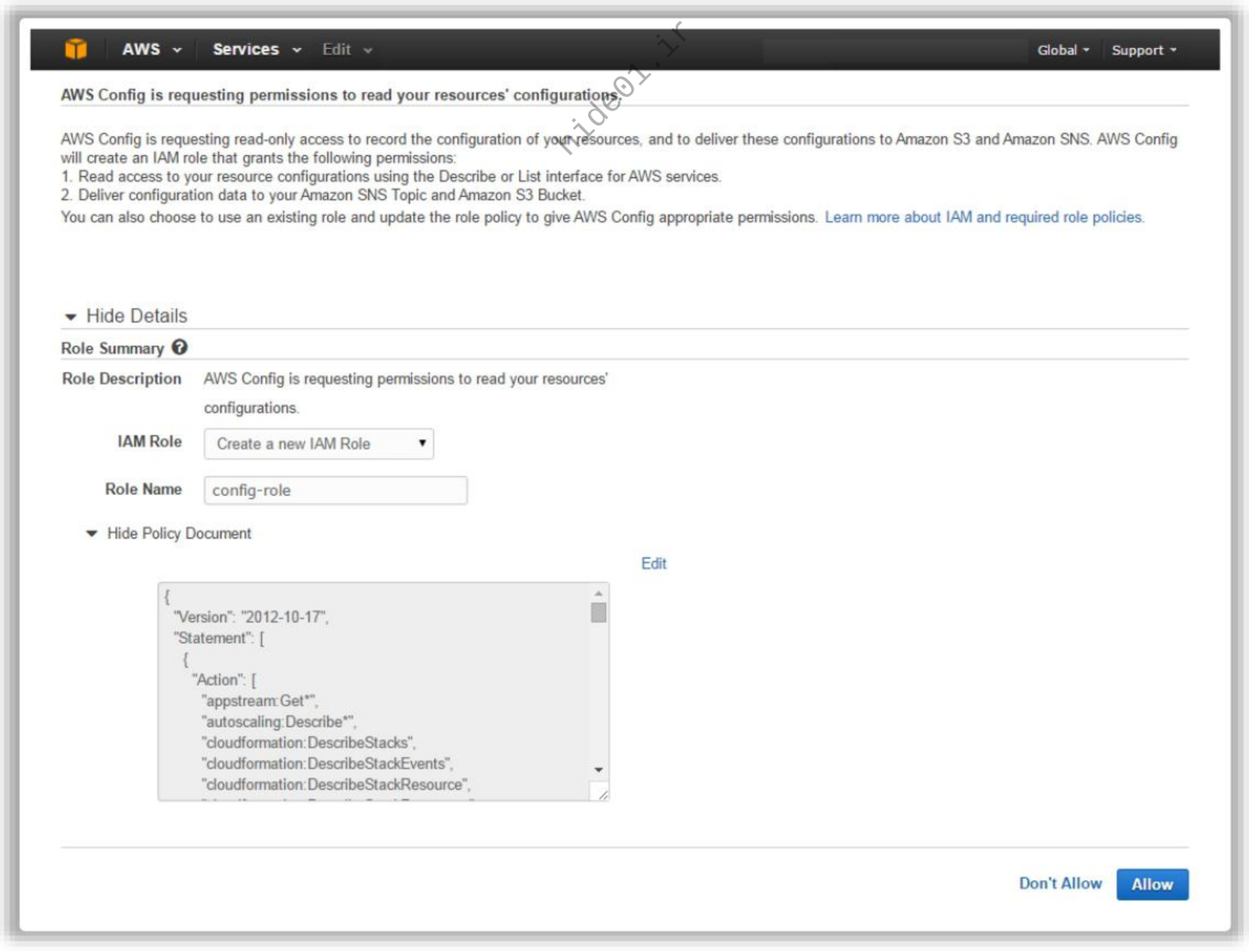


Figure 5.177: IAM Role

- In the next page, select **Resources** and click on **Look Up** to view the resources. Here, **IAM User Group** is selected.

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

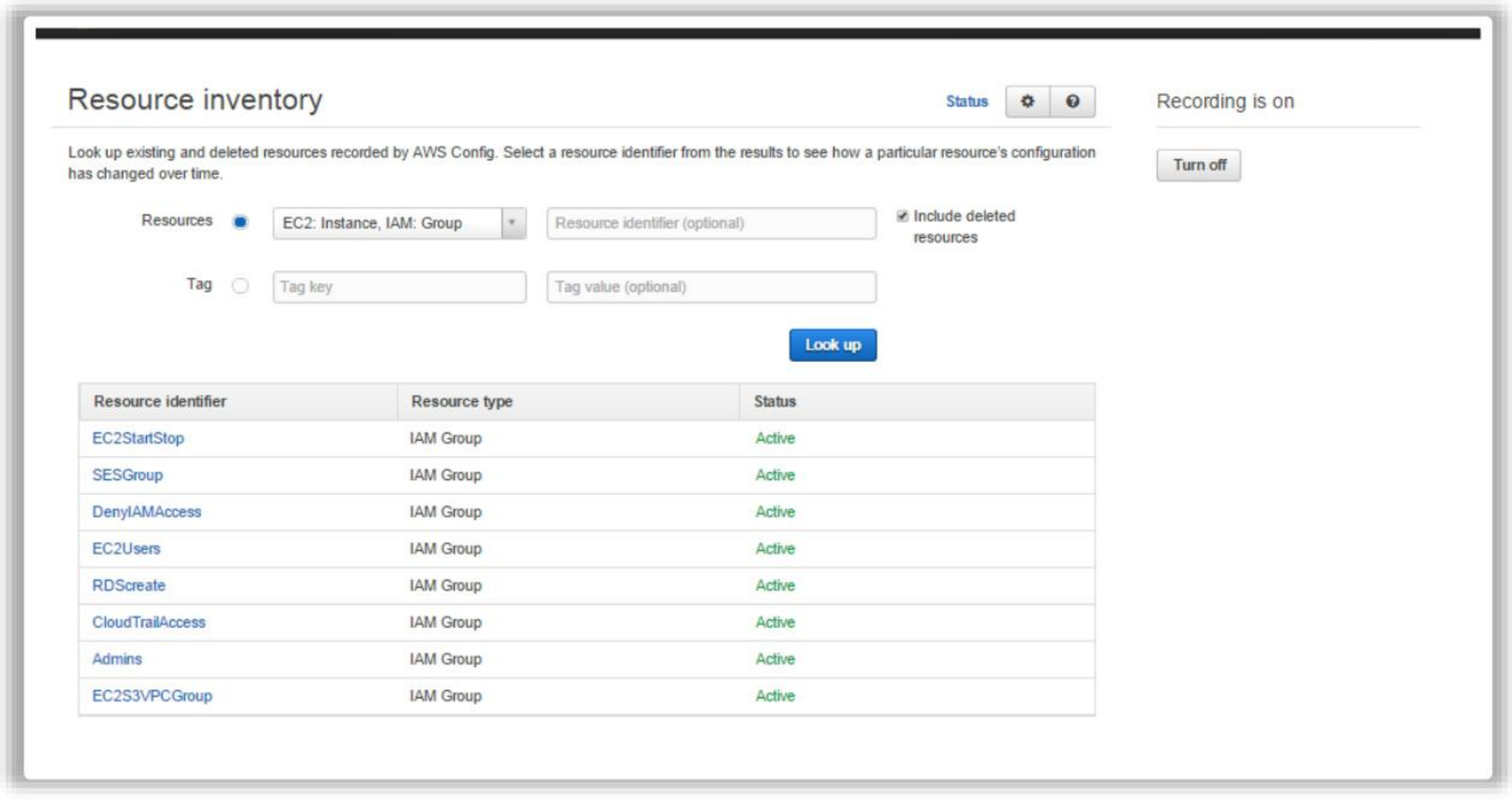


Figure 5.178: Resource Inventory

- Click on one resource to see the timeline page of the recorded configuration items. If this is the first time, start from today.

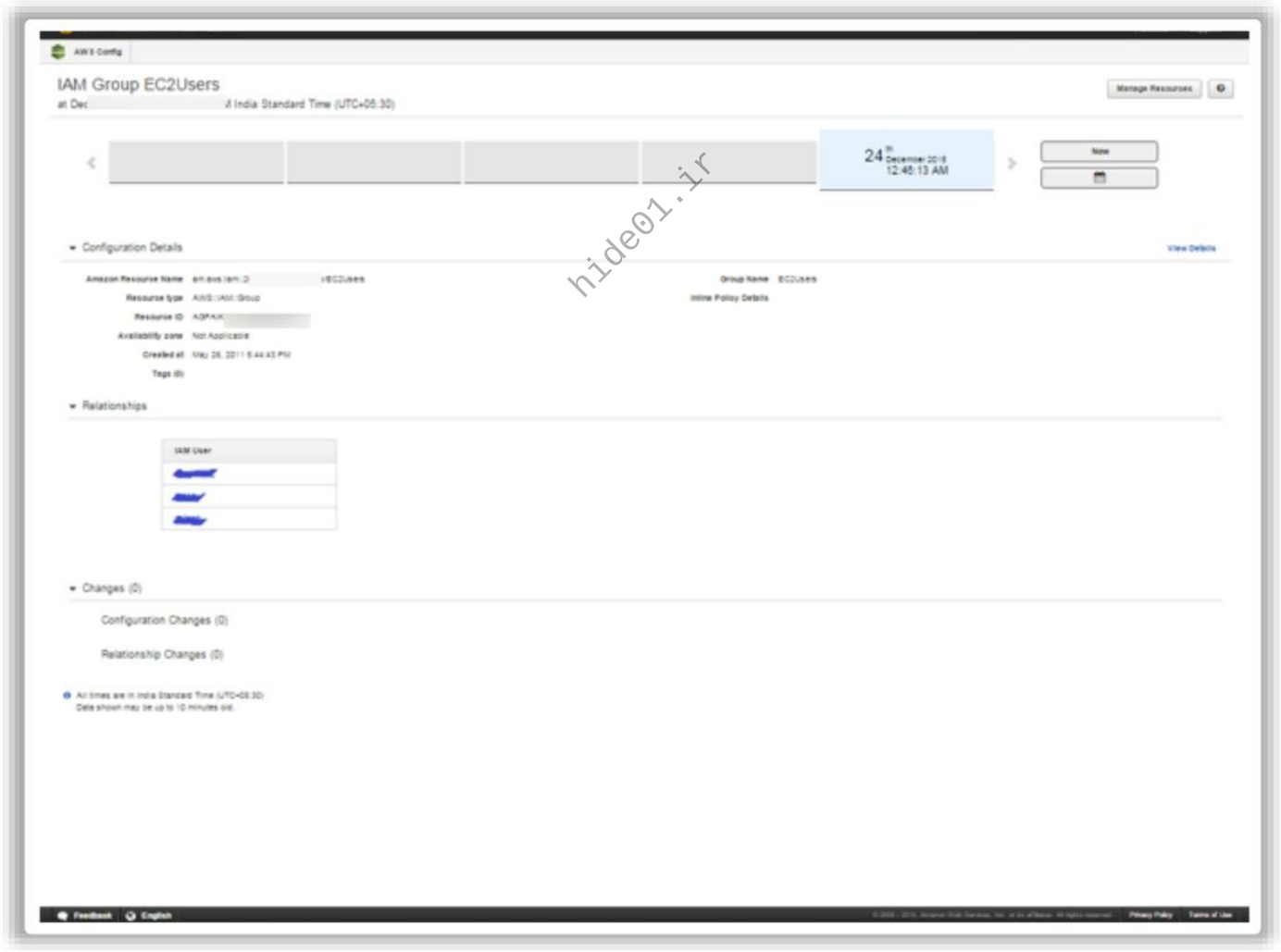


Figure 5.179: Timeline

- If attempts are made to access from an earlier date before the recording was turned **ON**, an error message (shown below) will be displayed.

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

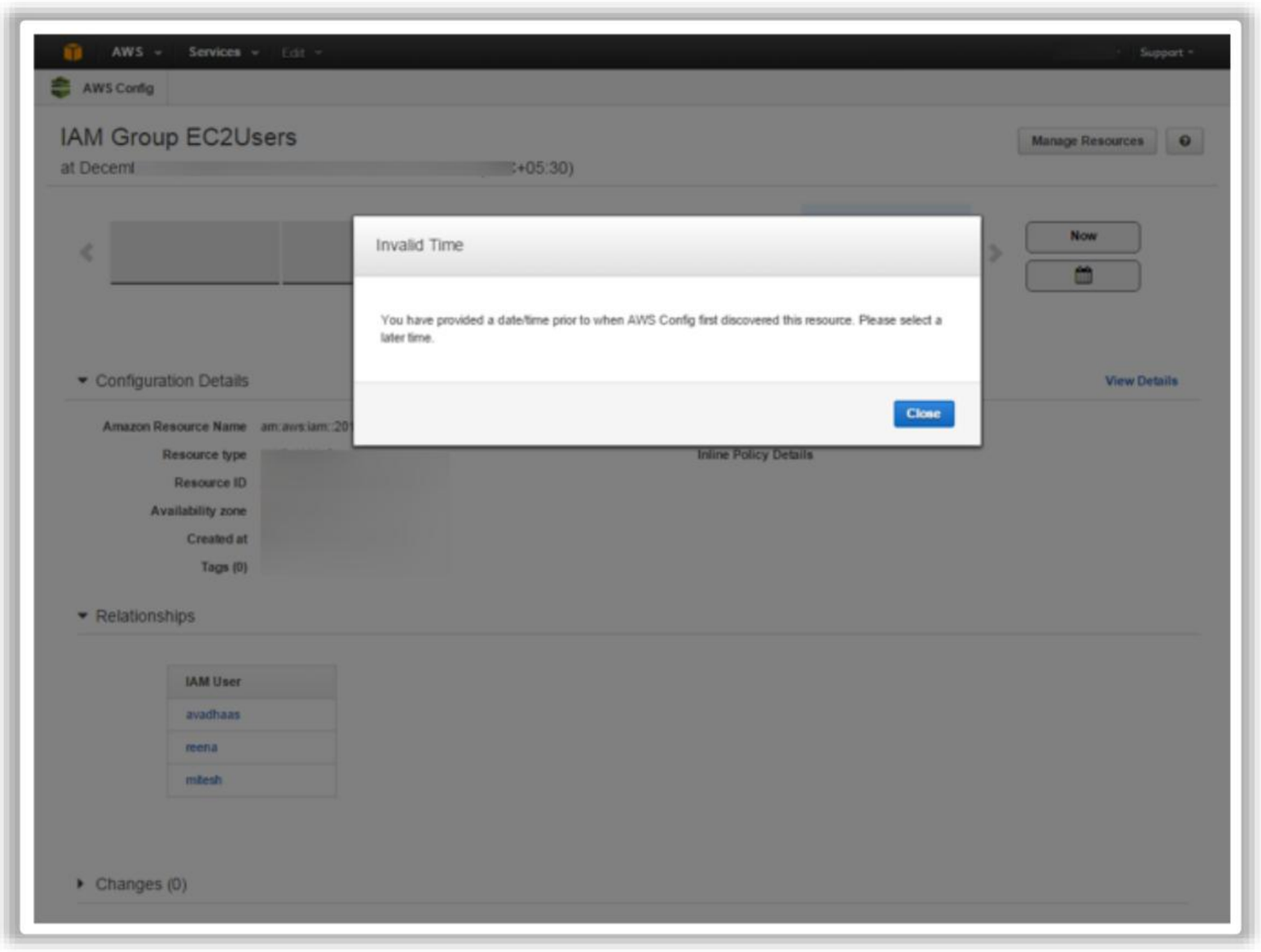


Figure 5.180: Alert

- If the above steps are successful, select **SNS service** from the **Services** menu and go to the **SNS Home** page. From **Topics**, select the created topic (here, it is **config-test-topic-18dec2015**). Select and copy the ARN of the topic.
- Select the **Subscription** menu and click on **Create Subscription**.

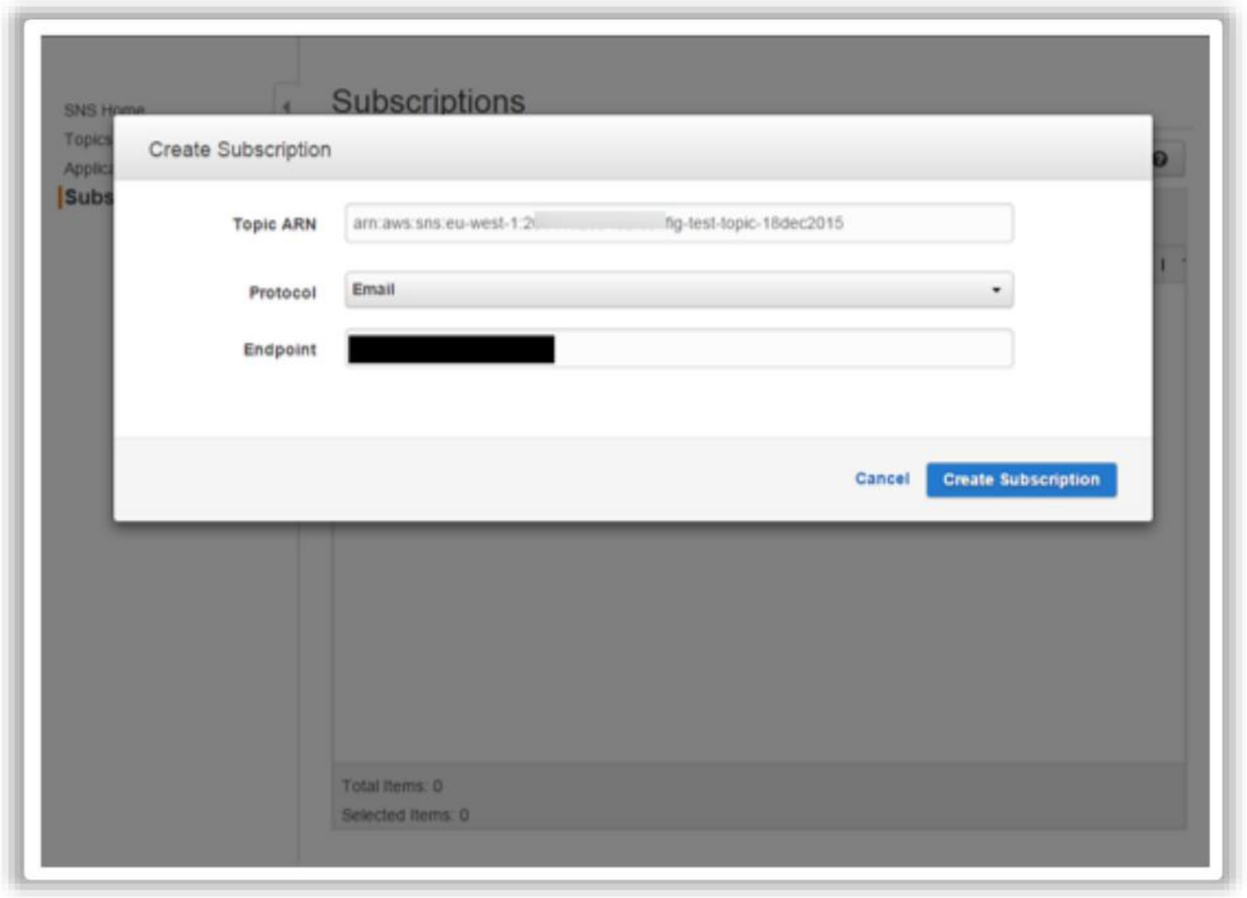


Figure 5.181: Create Subscription

- After completing these steps, you will be requested to confirm your subscription from an email sent to your email address. Confirm the request to receive email notifications.

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

- Go to the **AWS IAM** service page and select the created IAM role. Click on the **Attach Policy** button and attach **AWSConfigRole**.

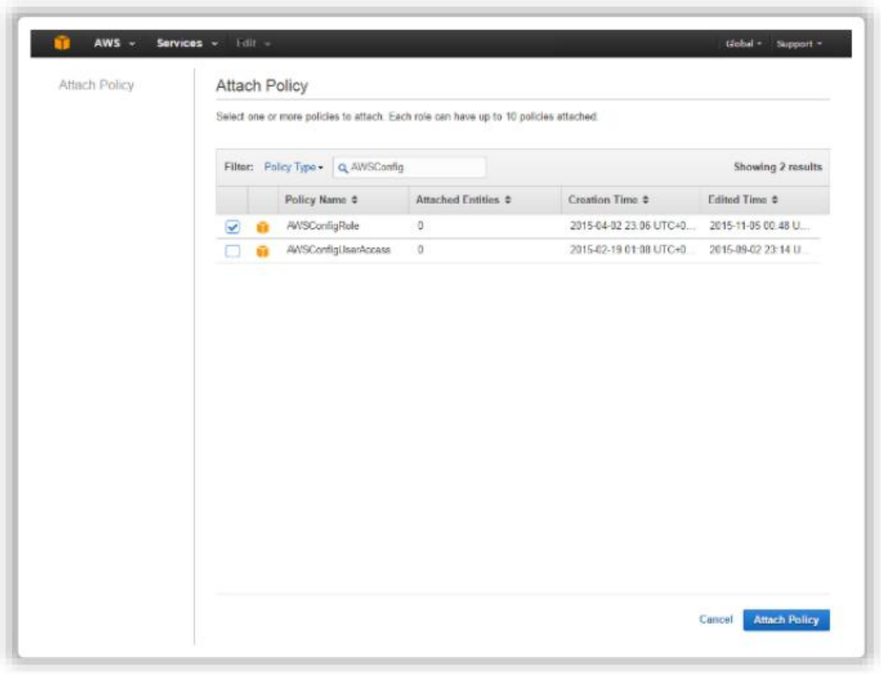


Figure 5.182: Attach Policy

- Now, add a user to the group you have been tracking. In this example, the IAM Group named **EC2User** is being tracked. Add a new user to the group. A message will be received when a new user is added, and the change will be reflected on the timeline page.

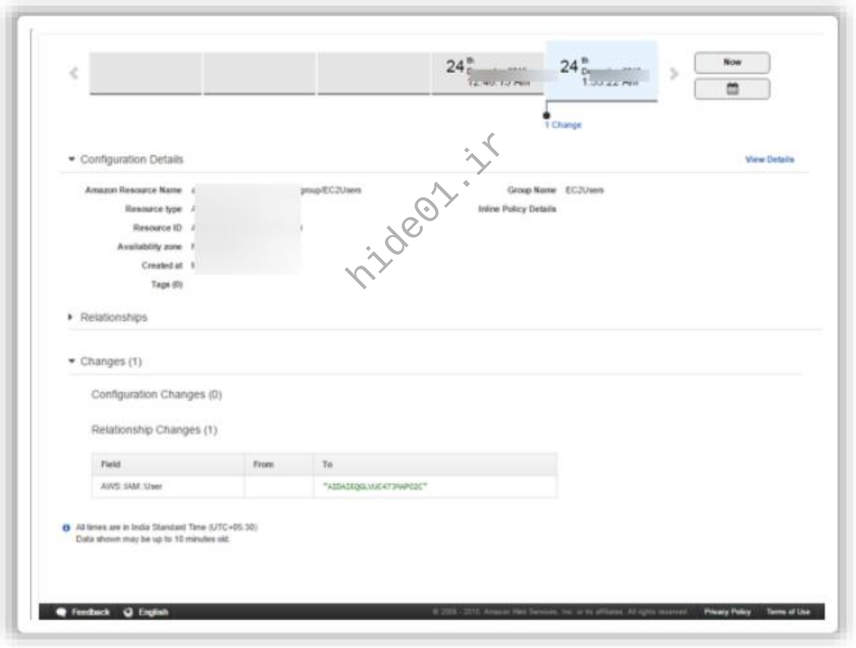


Figure 5.183: Add User to Group

- The email message is shown in the following screenshot.

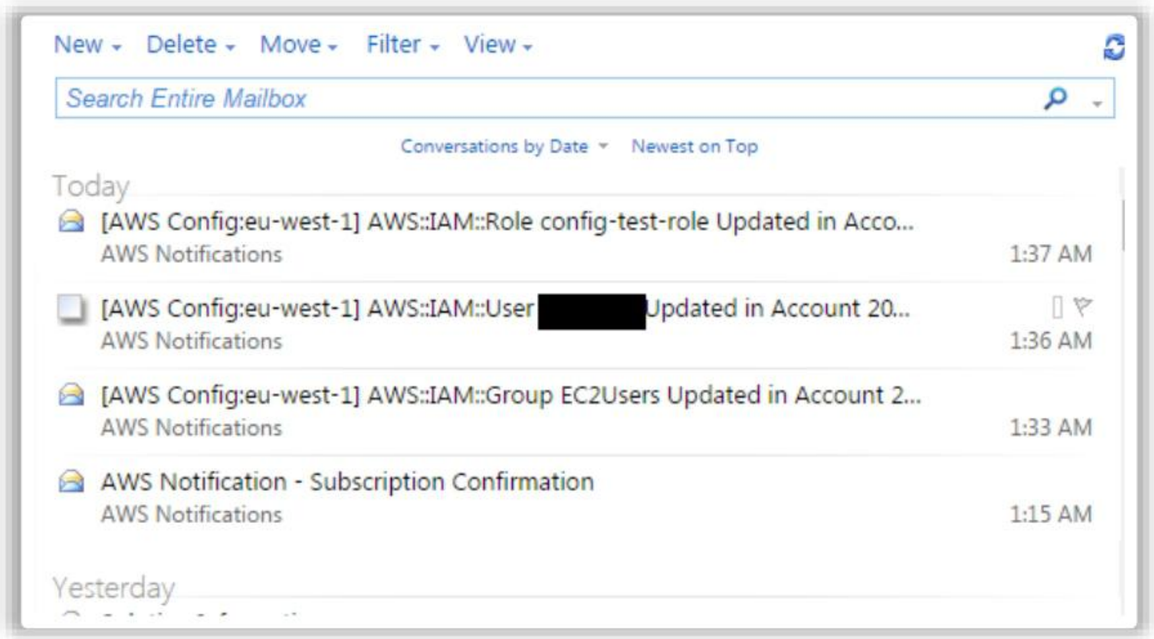
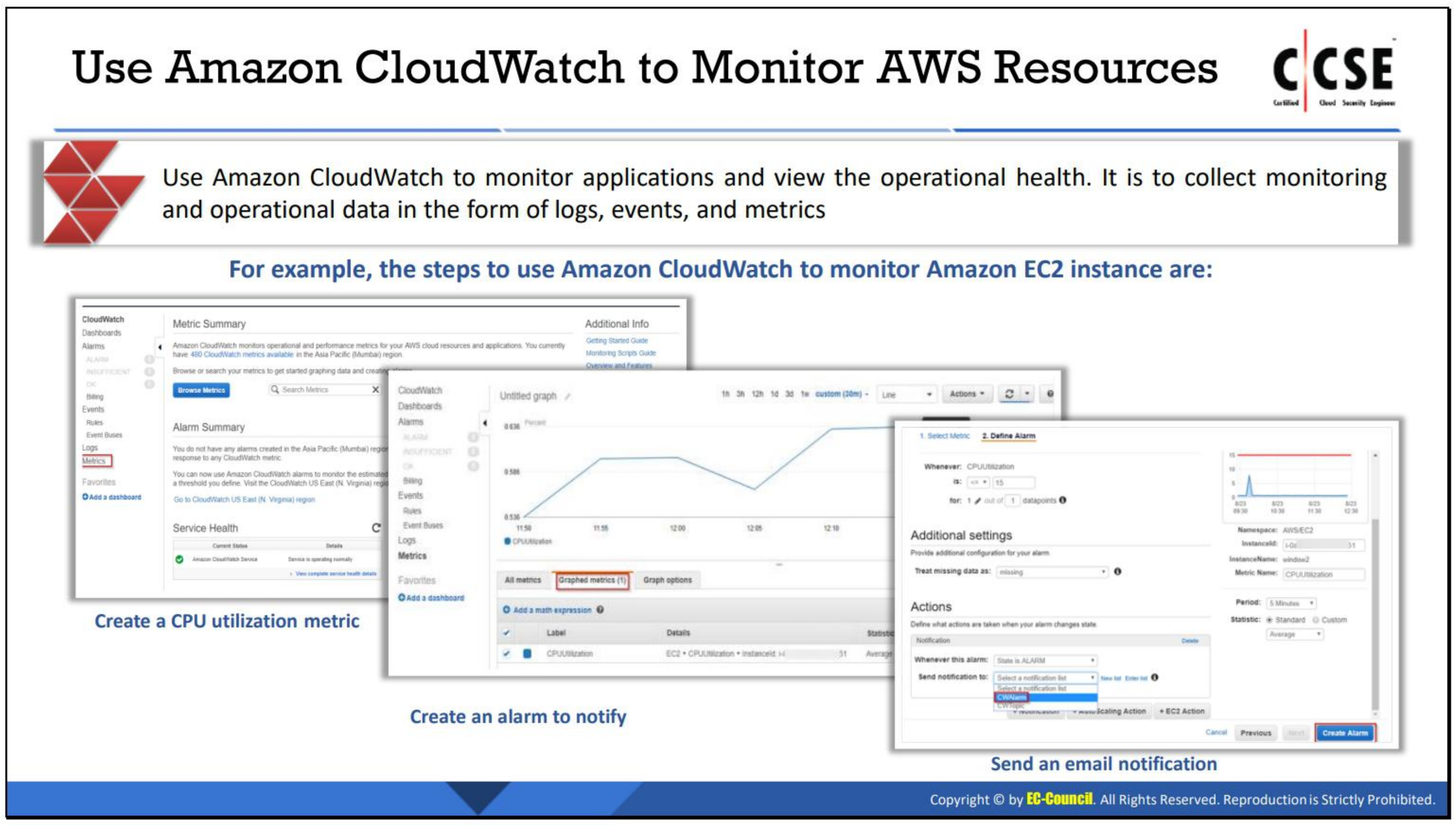


Figure 5.184: Email

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



Use Amazon CloudWatch to Monitor AWS Resources

Use Amazon CloudWatch to monitor applications and obtain a view of operational health. Use it to monitor operational data in logs, metrics, and events.

For example, the steps to use Amazon CloudWatch to monitor Amazon EC2 instance are as follows:

Configure Amazon CloudWatch to send a notification when the CPU utilization of an instance is lower than 15%.

- **Create a CPU utilization metric**
  - Go to Amazon CloudWatch Management Console. Select **Metrics** from the navigation pane.

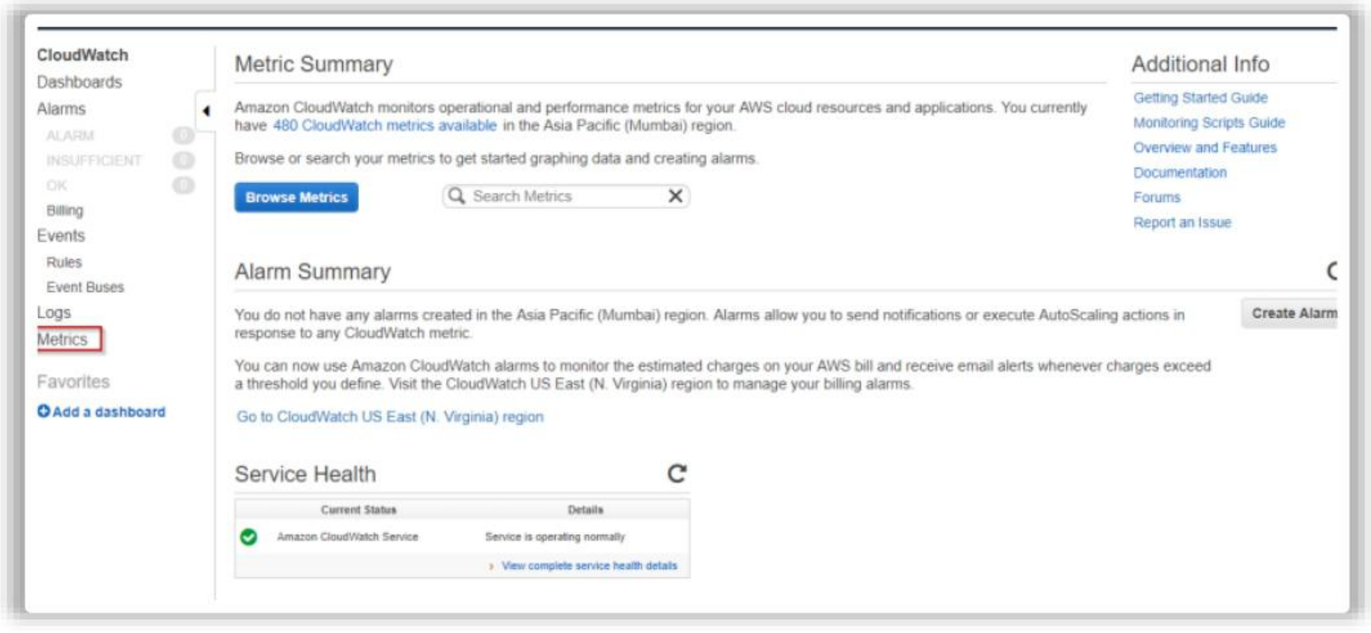


Figure 5.185: Metric Summary

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

- On the metrics page, type CPU utilization in the search bar. From the displayed list of instances, select the instance for which you want to create a metric.

- **Create an alarm to notify when the CPU utilization metric of the instance is lower than 15%**

  - Select the **Graphed metrics** option on the same page. Set the period according to requirement. Then, select the alarm icon located beside the selected instance.

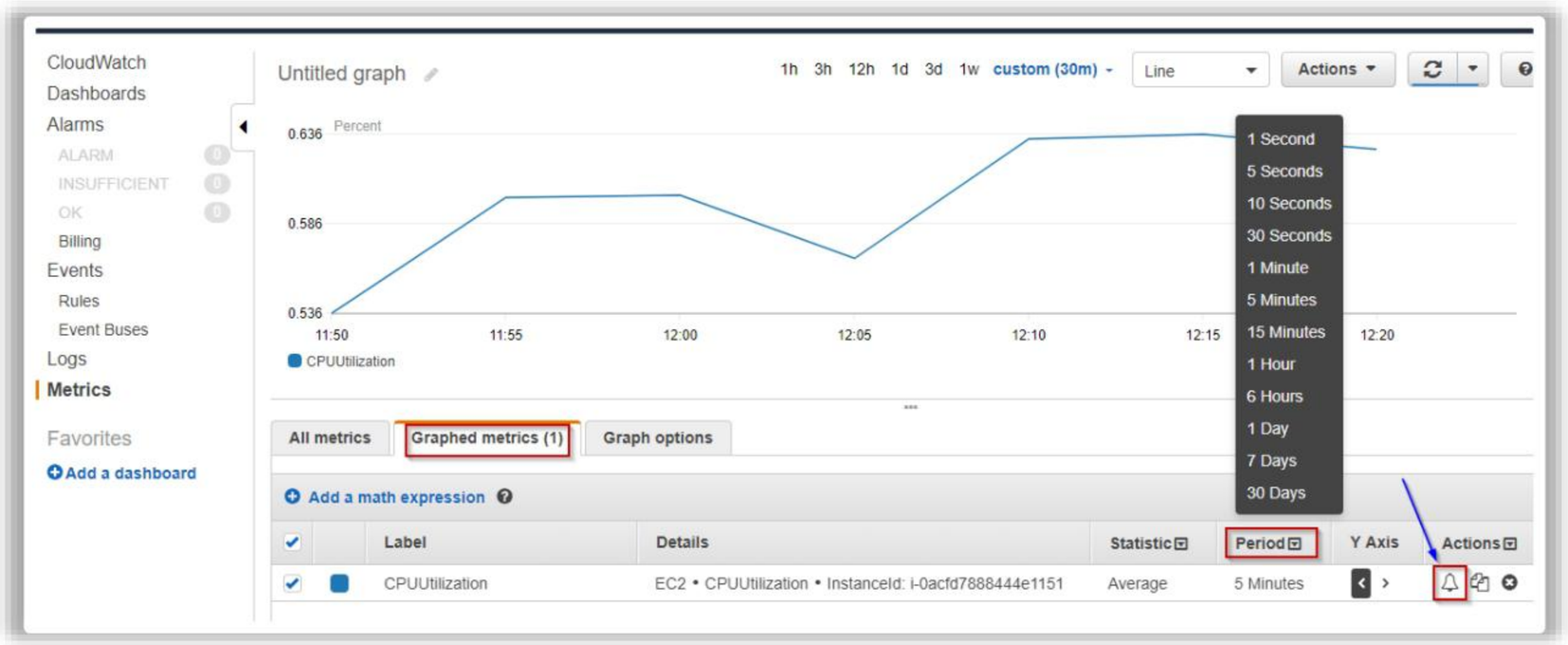


Figure 5.186: Graphed Metrics

- A metric with the label **CPUUtilization** is created.

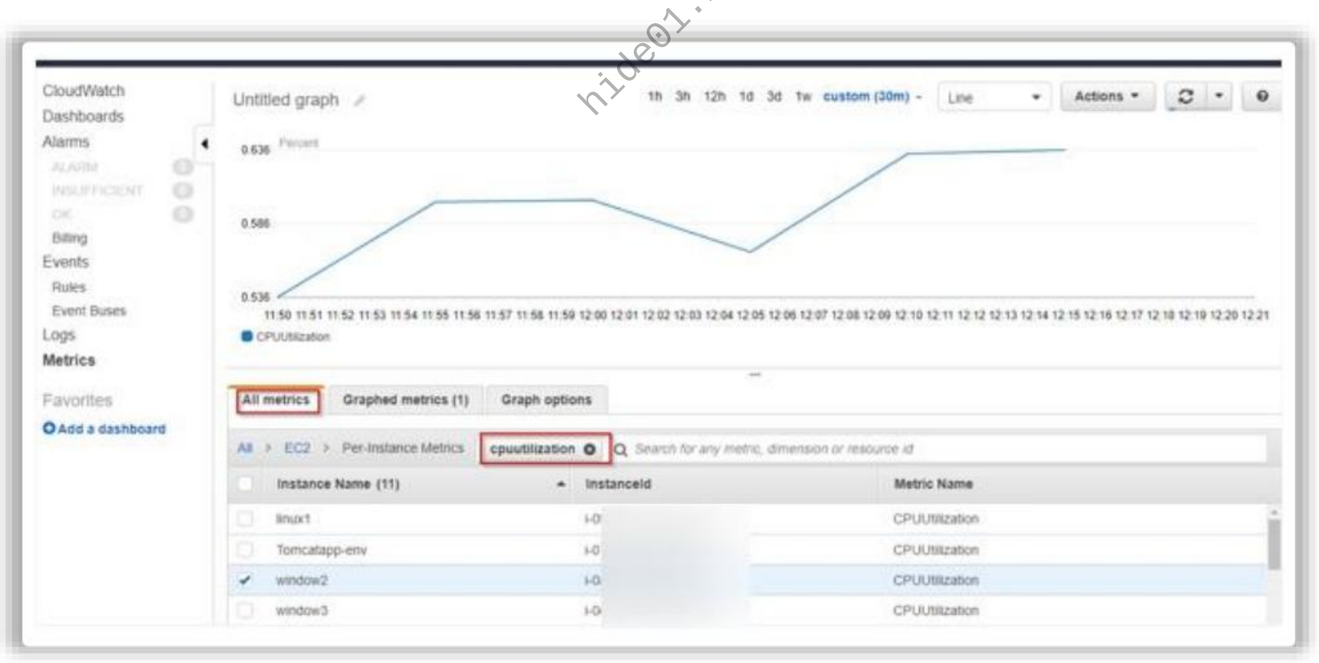


Figure 5.187: CPUUtilization

- Configure the alarm in the displayed dialog box. Assign it a name and description. Set the **Alarm Threshold** condition.

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

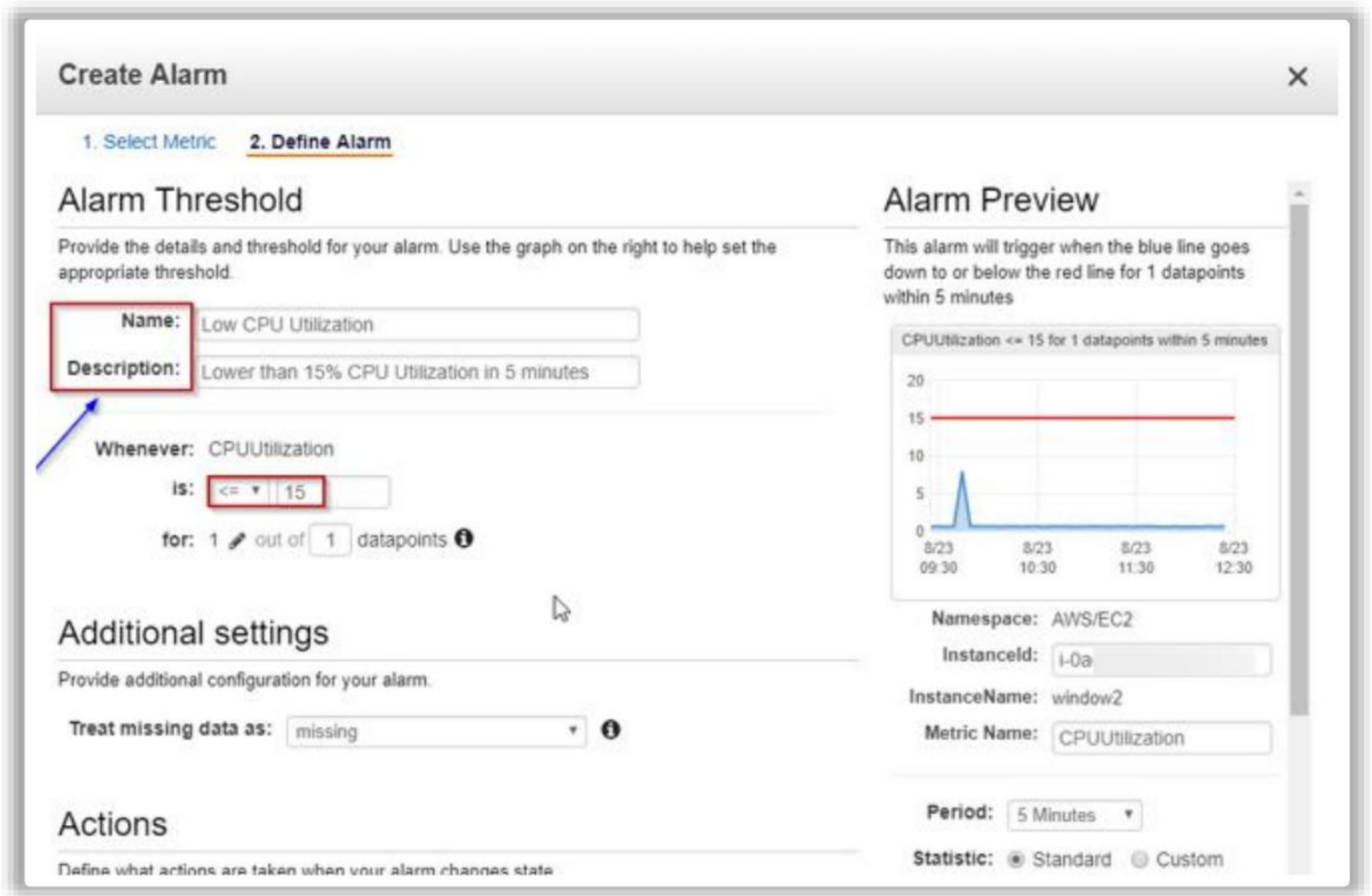


Figure 5.188: Create Alarm

- **Set AWS to send an email notification when the alarm condition is satisfied. The notification will be sent through Amazon SNS Topic.**
  - Select the **New List** option to add a new email recipient or select **Enter List** if you want to select an existing recipient; next, enter the name of SNS topic. Click on **Create Alarm**.

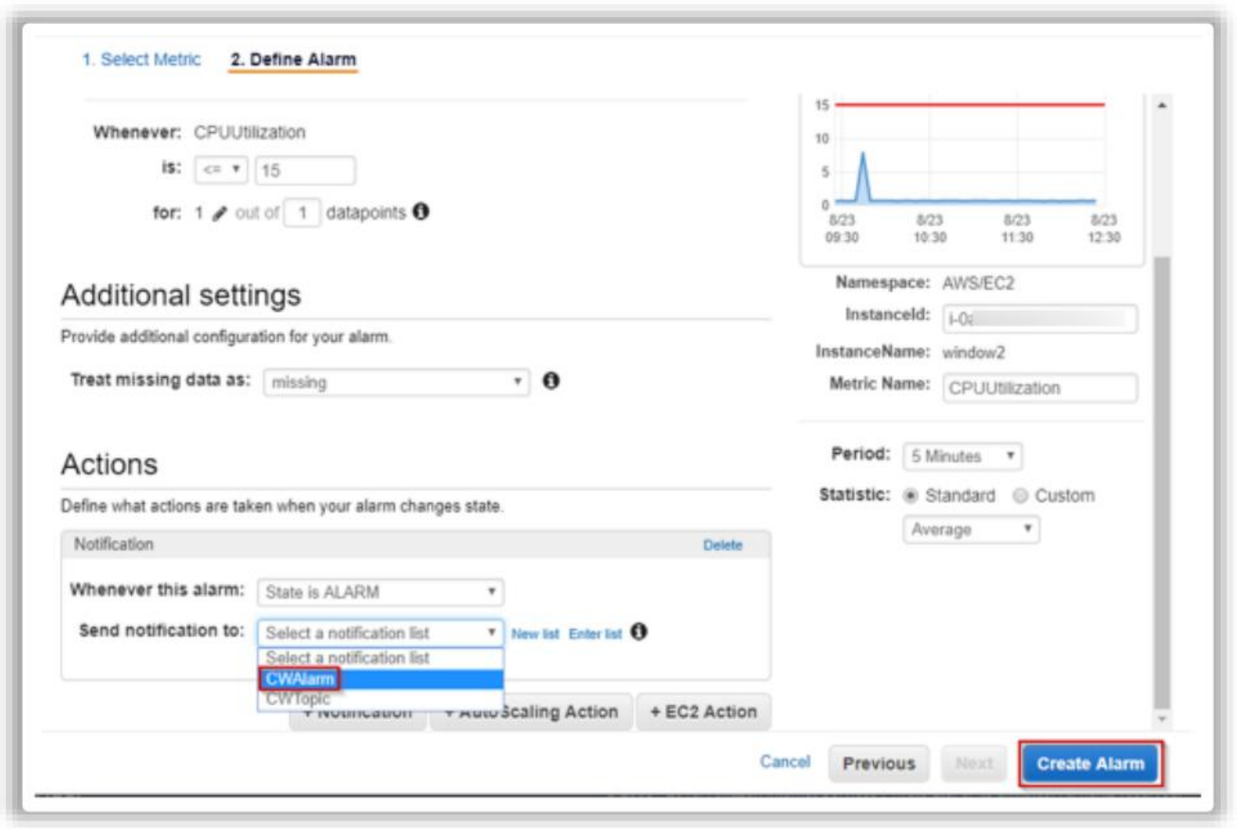


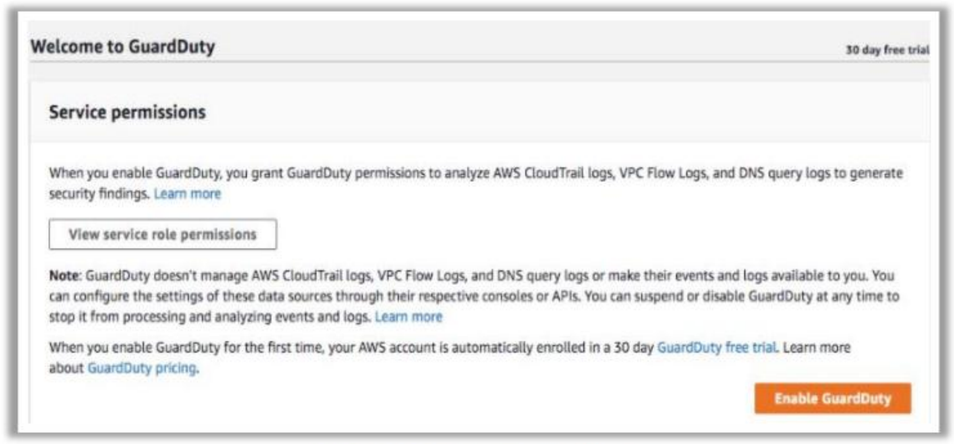
Figure 5.189: Define Alarm

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

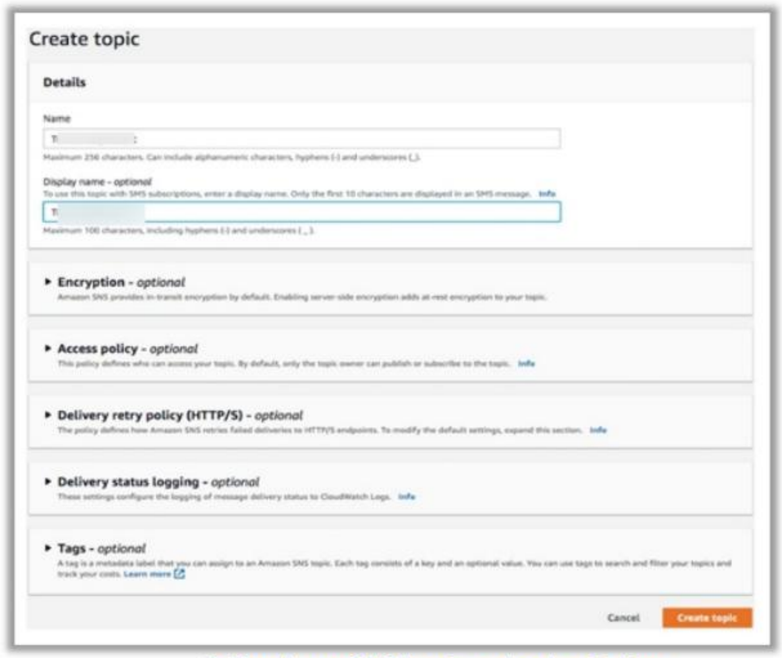
Monitor GuardDuty Findings with Amazon CloudWatch Events

- Receive notifications through email regarding GuardDuty findings based on the severity levels using SNS topics and CloudWatch Events automatically

For example, the steps to monitor GuardDuty Findings with Amazon CloudWatch Events are:



1. Enable Amazon GuardDuty

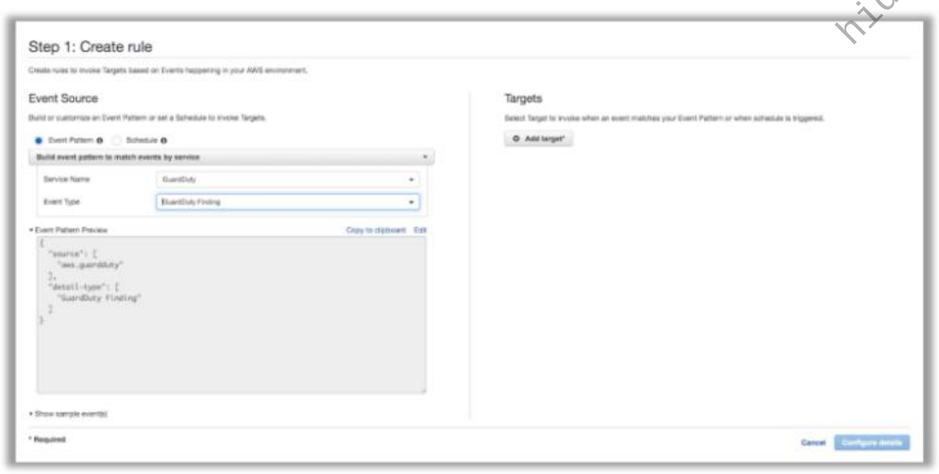


2. Create an SNS topic and subscription

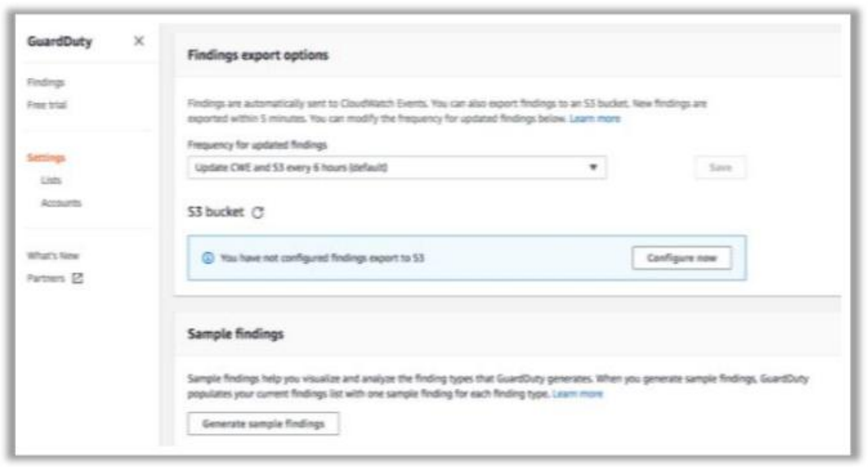
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Monitor GuardDuty Findings with Amazon CloudWatch Events (Cont'd)

hide01.ir



3. Configuring a CloudWatch Events rule for sending a message to the SNS topic



4. Generate sample finding

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

Monitor GuardDuty Findings with Amazon CloudWatch Events

Use Amazon GuardDuty to ingest data across different services of AWS such as CloudTrail, DNS Logs, and VPL flow logs; in addition, use integrated threat intelligence to find and prioritize attacks. For example, use SNS topics and CloudWatch Events to automatically receive notifications through email for GuardDuty findings based on severity levels.

Steps to monitor GuardDuty Findings using Amazon CloudWatch Events

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

These steps include enabling Amazon GuardDuty, creating an SNS topic and subscription, configuring a CloudWatch Events rule to send a message to the SNS topic based on the results of GuardDuty, and adjusting the CloudWatch rule and target SNS configuration depending on the requirements.

- Go to the GuardDuty console and click on **Enable GuardDuty**.

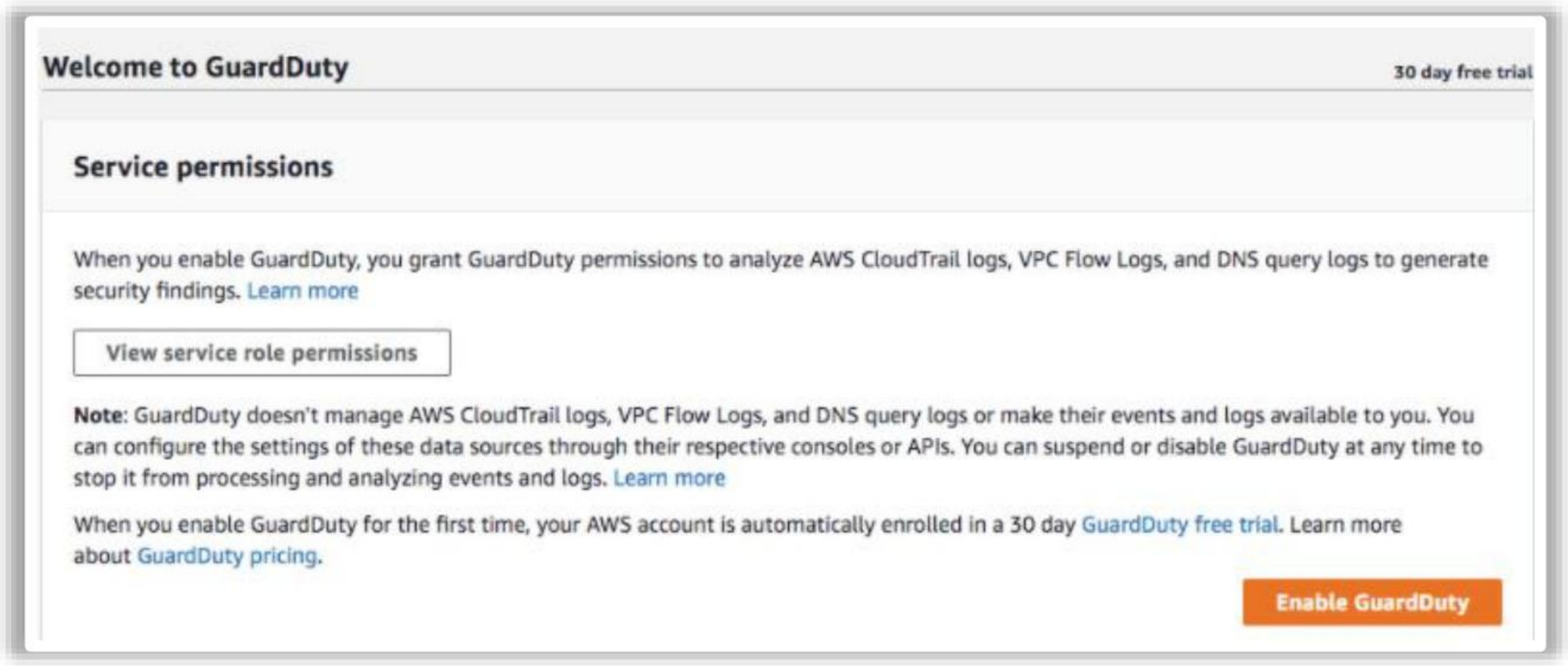


Figure 5.190: Service Permissions

- The GuardDuty console is probably empty, especially when being launched on a fresh account.

hide01.ir

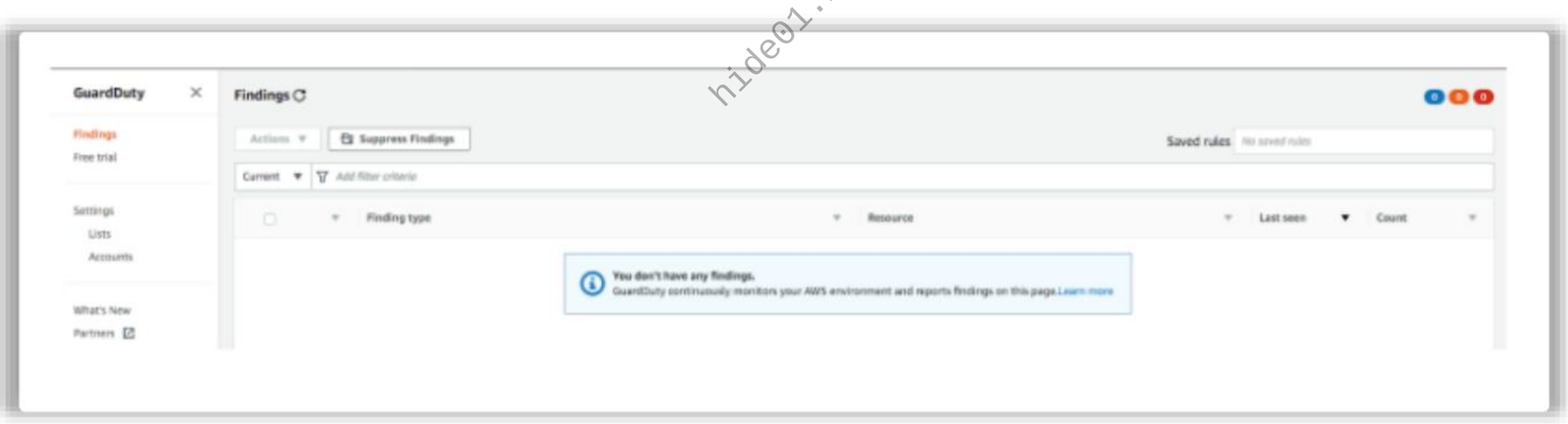


Figure 5.191: Console

- Create an SNS topic, thus allowing to send notifications.
  - Head over to **SNS**
  - Create and name a topic.
  - Click on **Create topic**

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

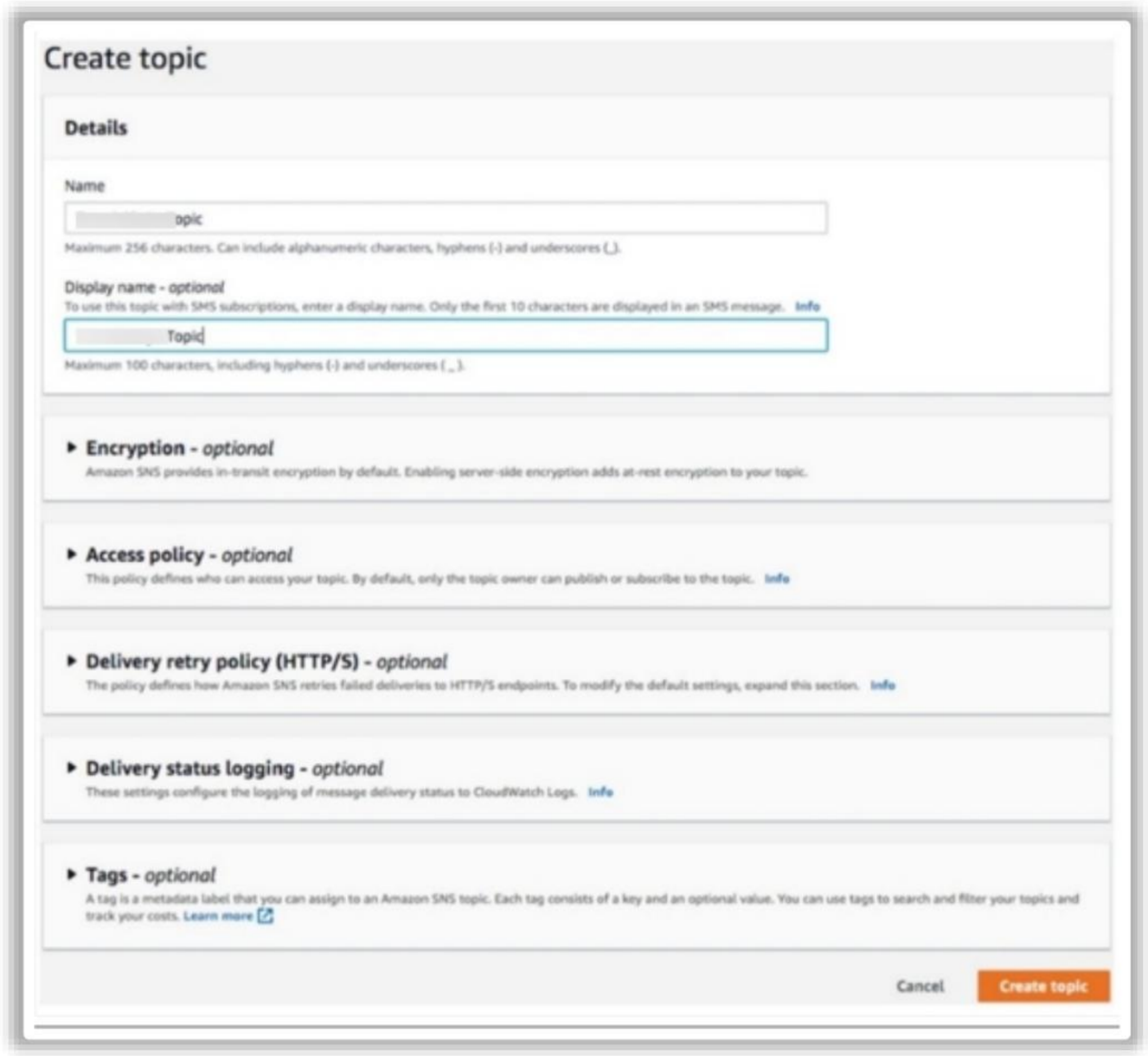


Figure 5.192: Create Topic

- Create an SNS subscription for the topic
  - Specify the SNS topic created previously
  - Under **protocol**, select **Email**
  - In the **Endpoint** field, enter the email address that will receive the CloudWatch events.
  - Click on **Create subscription**

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

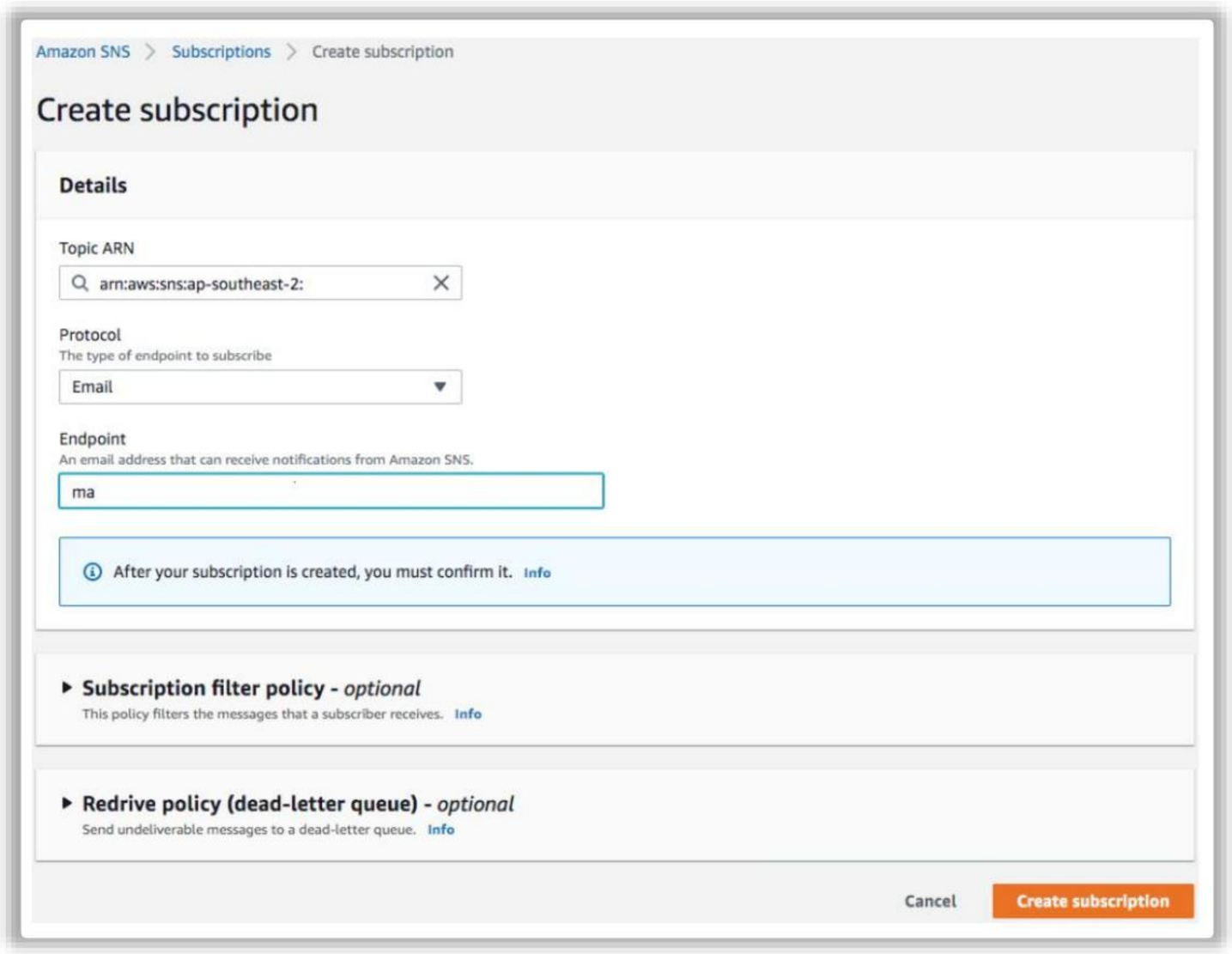


Figure 5.193: Create Subscription

- Create a CloudWatch Events rule to send events to the SNS topic.
  - Move to CloudWatch and click on the **Rules** tab .

hide01.ir

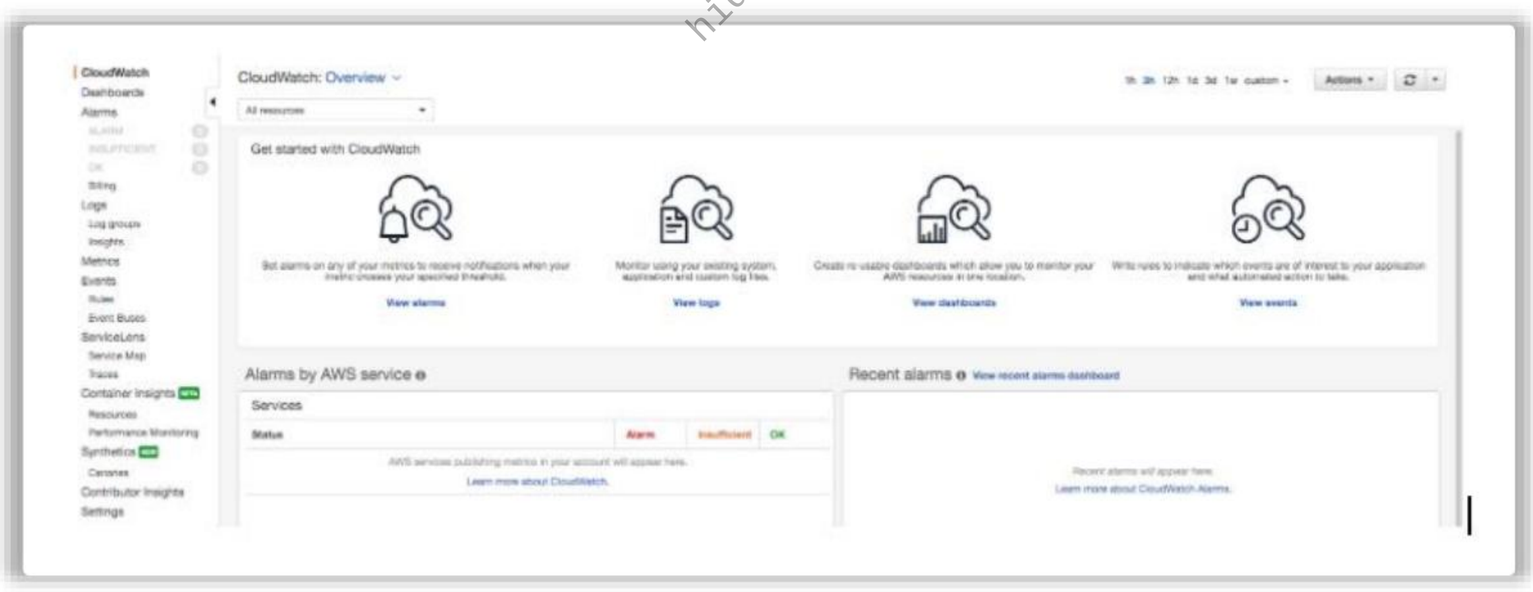


Figure 5.194: Rules

- Create a CloudWatch Events Rule.

Figure 5.195: Create Rule

  - Click on **Create Rule** and toggle to **Event Pattern.**
  - For the **Service Name** menu, search for GuardDuty.

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

- For the **Event Type** menu, select **GuardDuty Finding**.
- Click on **Edit** to modify the **Event Pattern Preview**, paste the following JSON code, and click on **Save**. This code can alert for findings ranging from medium to high.

```
{
  "source": [
    "aws.guardduty"
  ],
  "detail-type": [
    "GuardDuty Finding"
  ],
  "detail": {
    "severity": [
      4, 4.0, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9,
      5, 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9,
      6, 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9,
      7, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9,
      8, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9
    ]
  }
}
```

hide01.ir

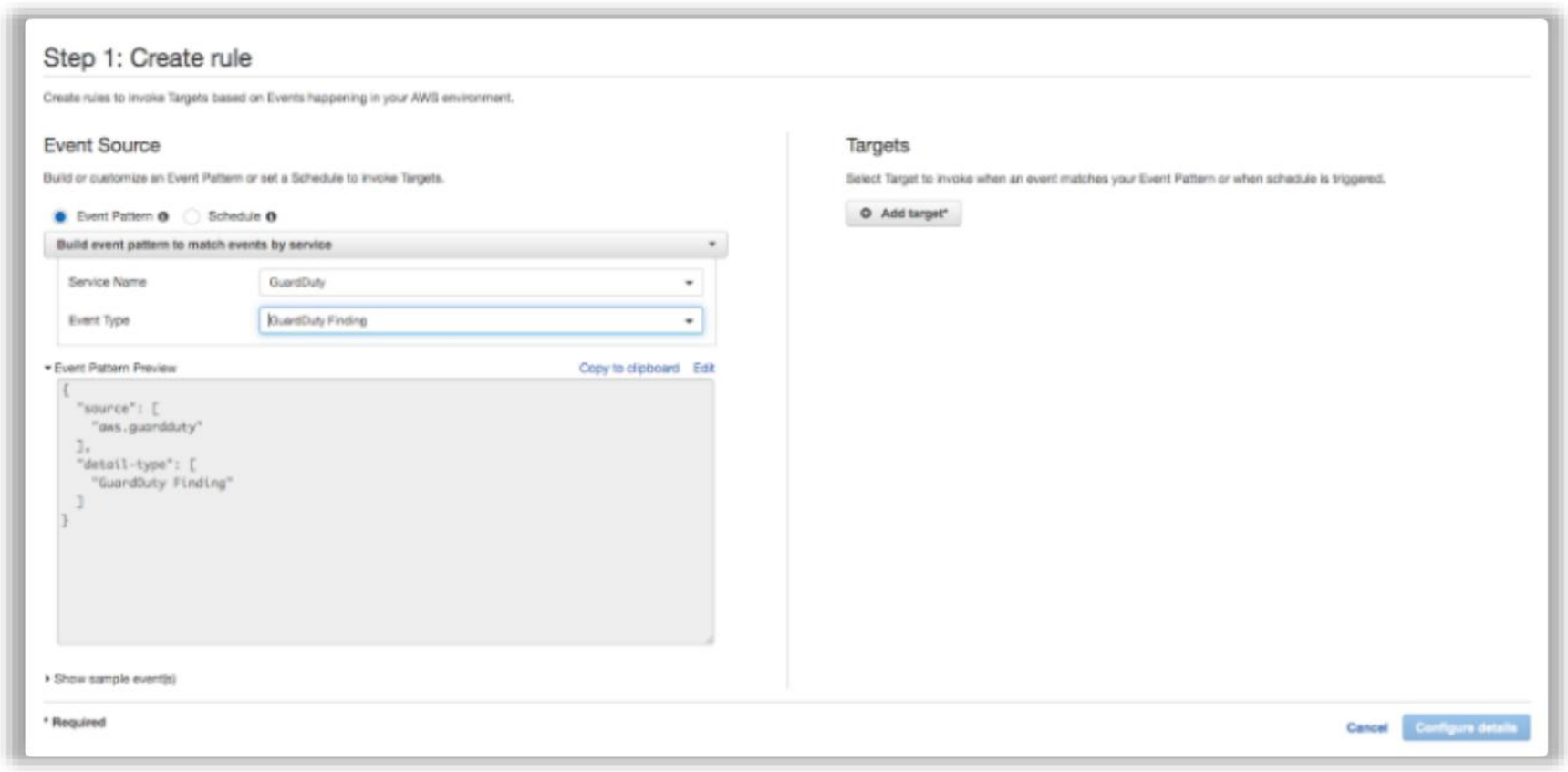


Figure 5.196: Create Rule

- Click on **Add Target** in the **Target** section.
  - In the **Targets** section, click on **Add target** and specify the created SNS topic.

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

- Under **Configure Input**, click on **Input Transfer**.
- Paste the following JSON code for **Input Path** and **Input Template**. Click on **Configure Details**.

For input path field,

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_description": "$.detail.description"
}
```

For input template,

```
"AWS <Account_ID> has a severity <severity> GuardDuty
finding type <Finding_Type> in the <region> region."

"Finding Description:"

"<Finding_description>. "

"For more details open the GuardDuty console at
https://console.aws.amazon.com/guardduty/home?region=<regio
n>#/findings?search=id=<Finding_ID>"
```

hileon.ir

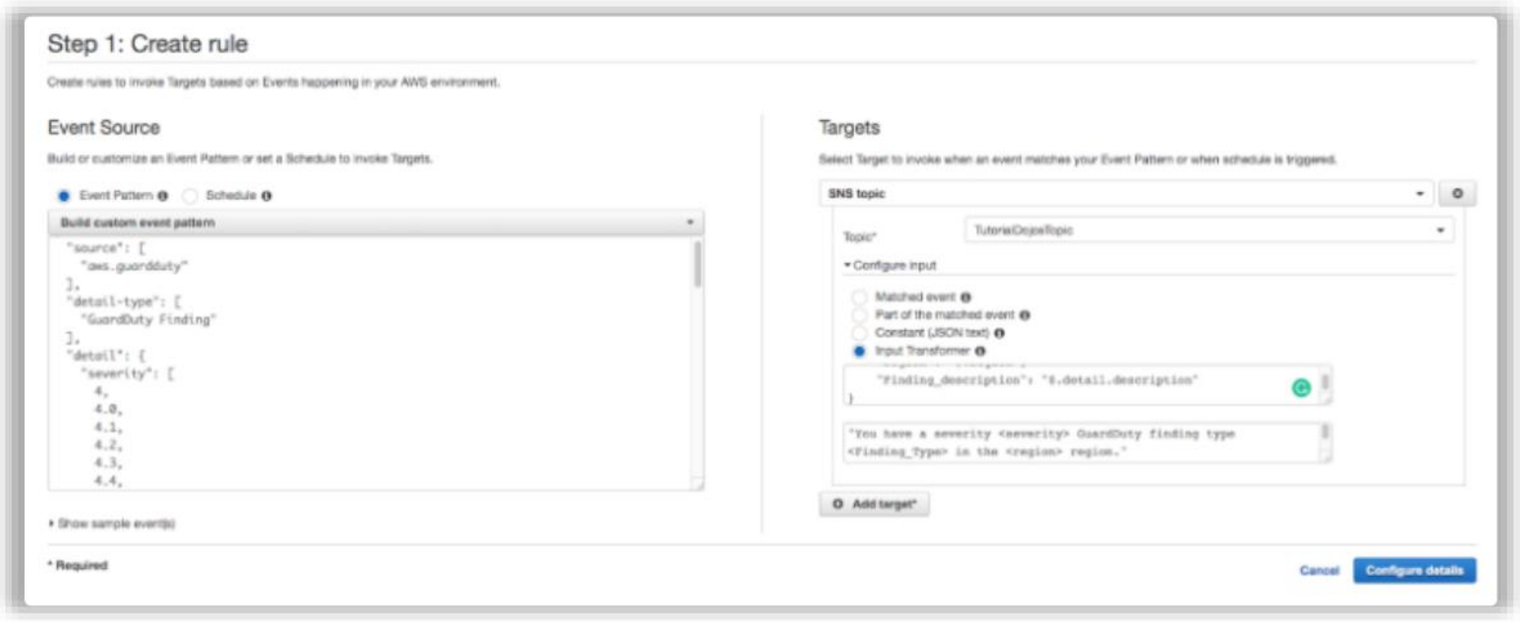


Figure 5.197: Create Rule

- In the **Configure rule details** page, **Name** the rule definition, tick the **Enabled** box under **State**, and click on **Create rule**.

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

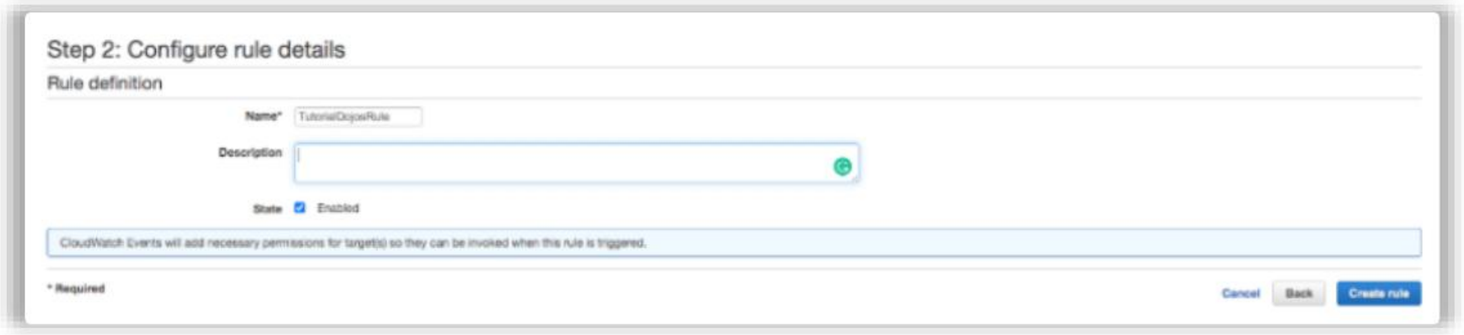


Figure 5.198: Configure Rule Details

- Populate GuardDuty.
  - Go to **Settings.**
  - Under **Sample findings**, click on **Generate sample findings.**
  - You will receive the notifications sent by GuardDuty within 5 min of a finding or receive an email 5 min after generating a sample finding.

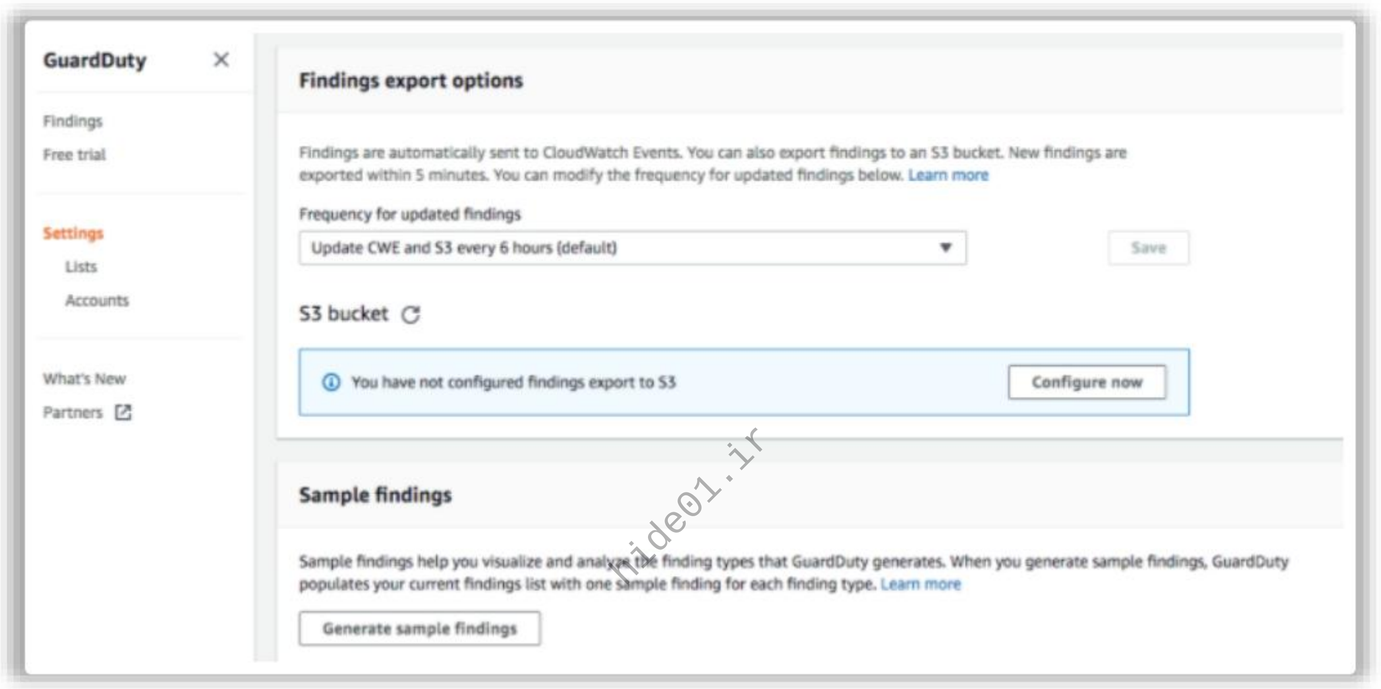


Figure 5.199: Sample Finding

- You will receive an email from AWS regarding the findings of GuardDuty.

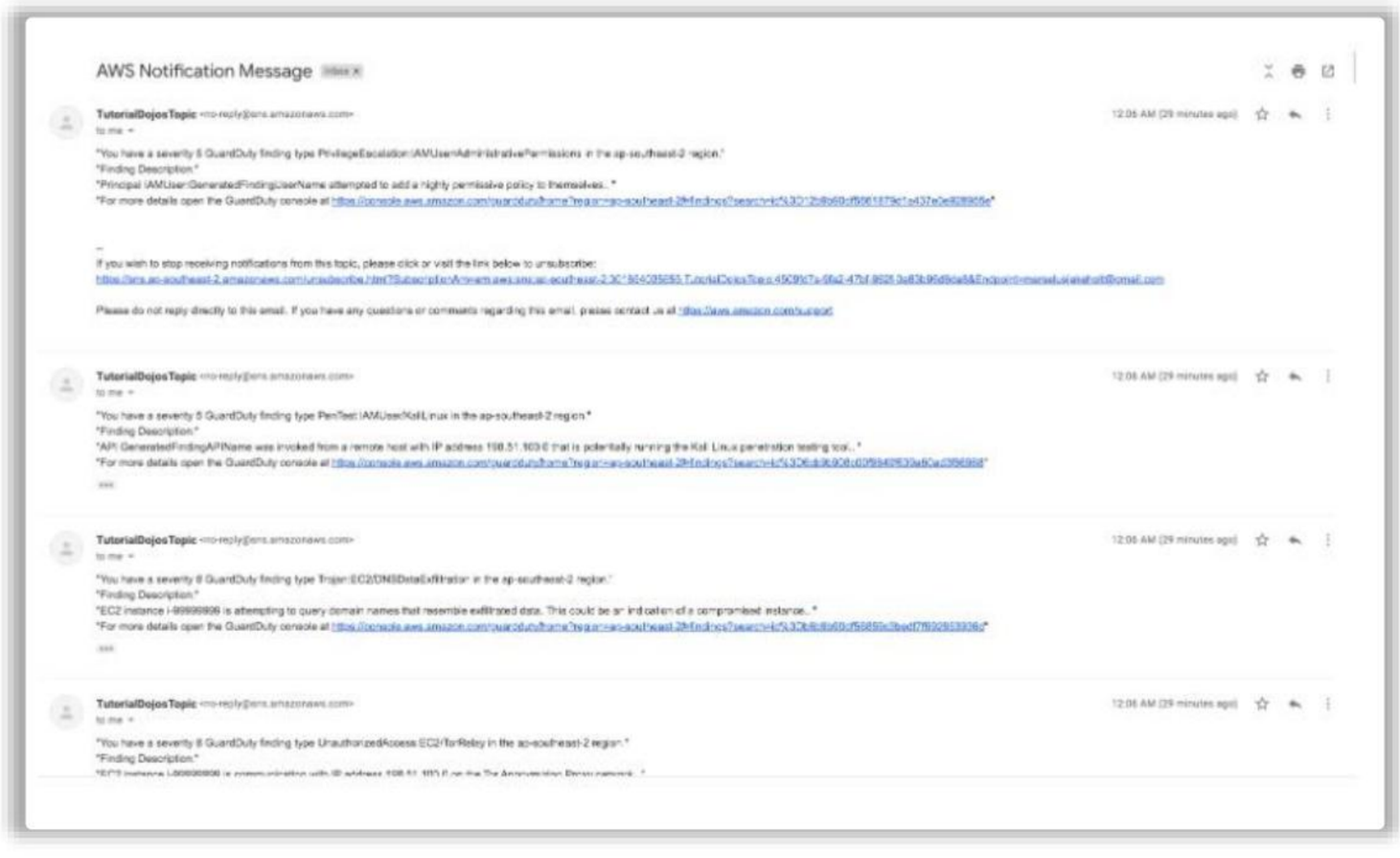
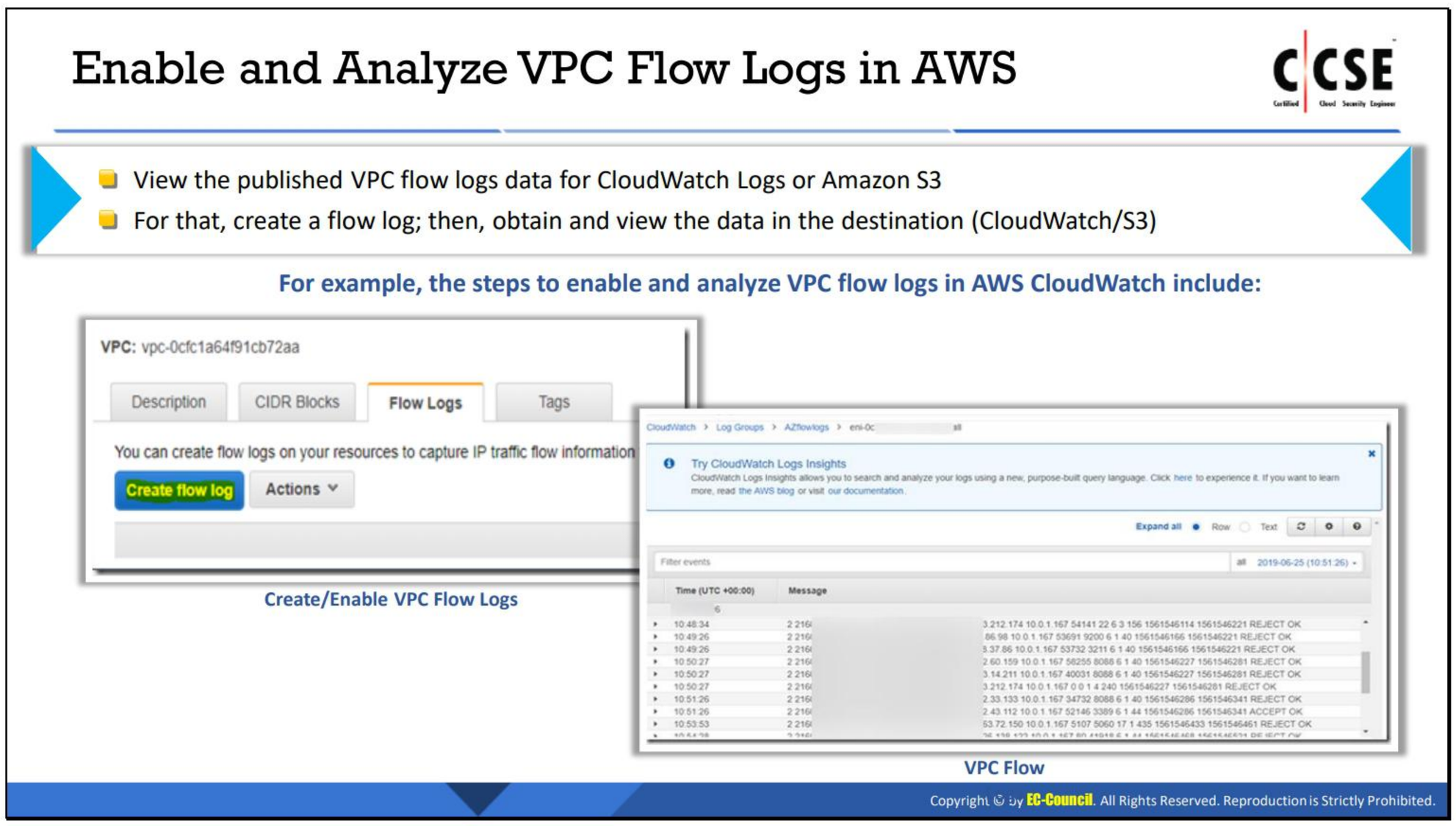


Figure 5.200: Email

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



Enable and Analyze VPC Flow Logs in AWS

View the published VPC Flow Logs data regarding CloudWatch Logs or Amazon S3. To view this, create a flow log and retrieve and view its data in the destination (CloudWatch/S3).

Steps to enable and analyze VPC Flow Logs in AWS

- For this example, a VPC with two subnets has already been created in different availability zones.

Figure 5.201: AZ-VPC

Figure 5.202: Two Subnets

- Additionally, a windows EC2 instance has already been created for this example.

Figure 5.203: EC2 Instance

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

- **Enable Flow Logs**
  - Open the VPC dashboard. Click on **Your VPCs**.

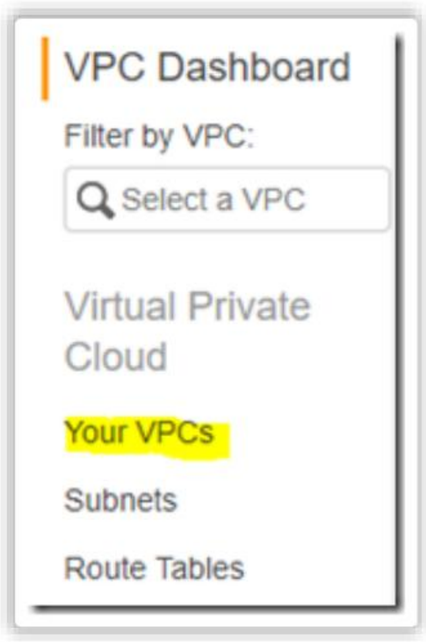


Figure 5.204: VPC Dashboard

  - Select the VPC and click on the **Flow Logs** tab.

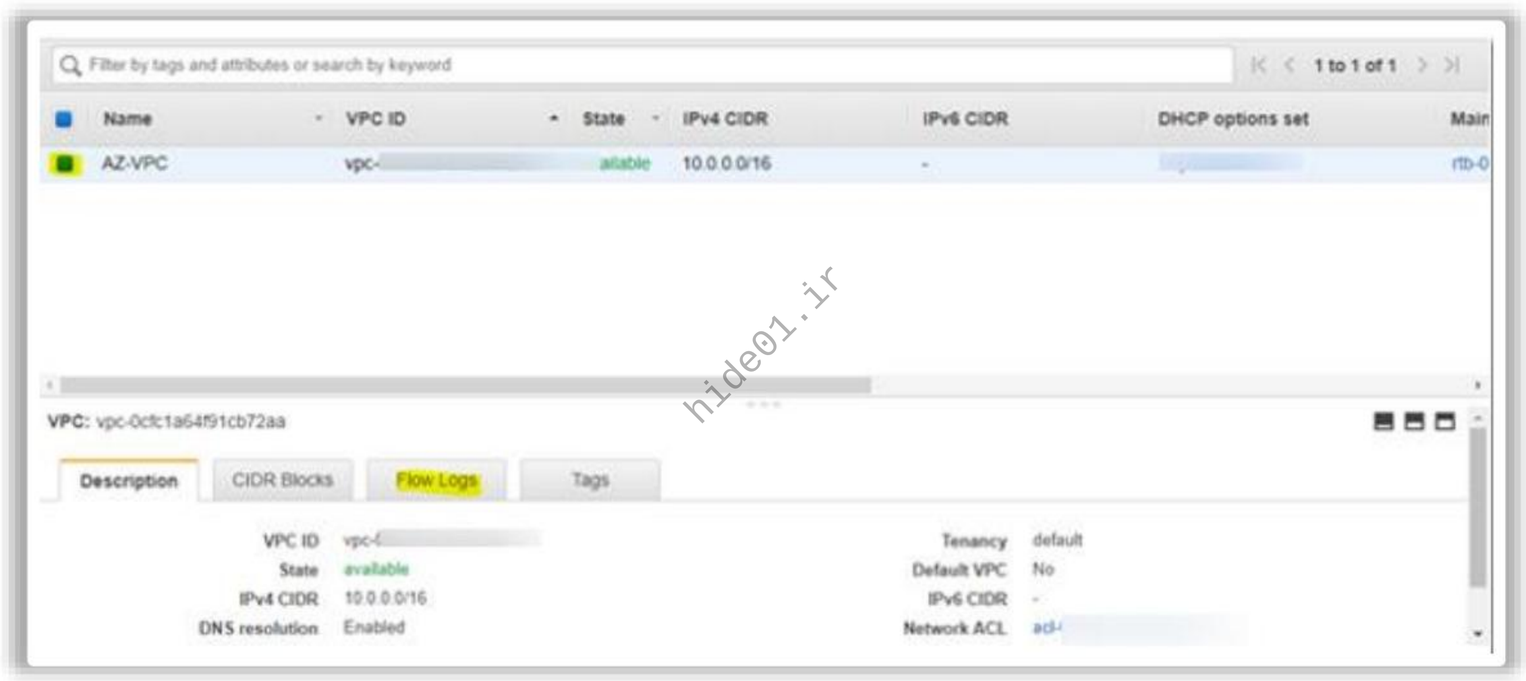


Figure 5.205: Flow Logs

  - Click on **Create flow log**.

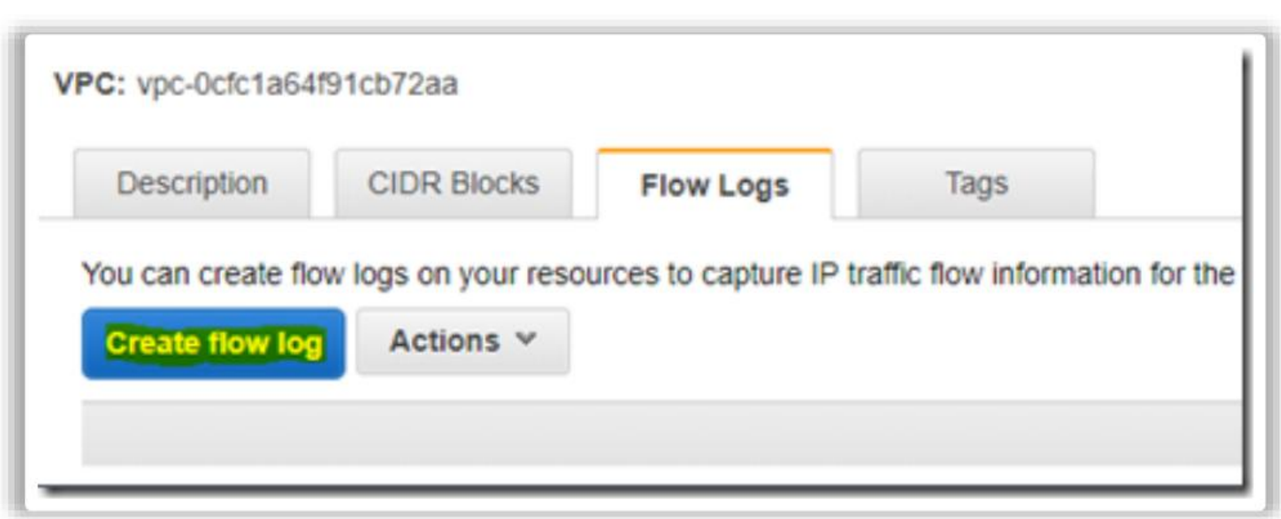


Figure 5.206: Create Flow Log

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

- Select on **All** for **Filter*** and **CloudWatch** as the **Destination**.

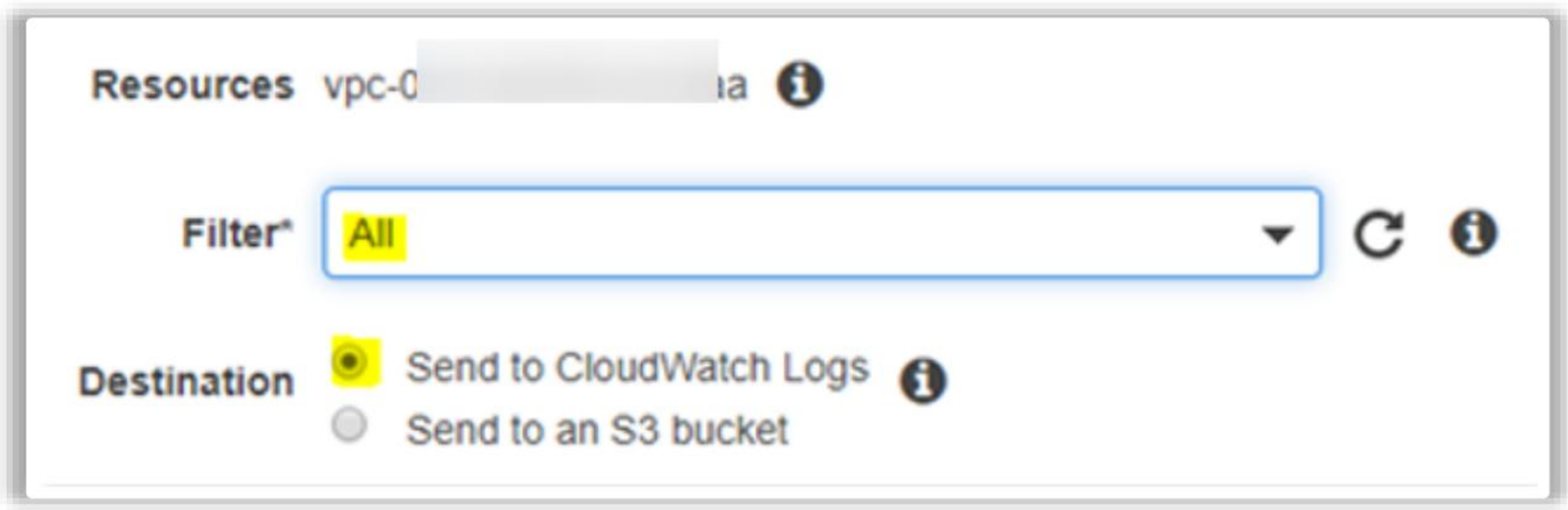


Figure 5.207: Select All Filter

- Provide the **Destination log group*** name and click on the **Set Up Permissions** link.

Figure 5.208: SetUp Permission

- (For this example) Leave the default settings and click on **Allow**.

hide01.ir

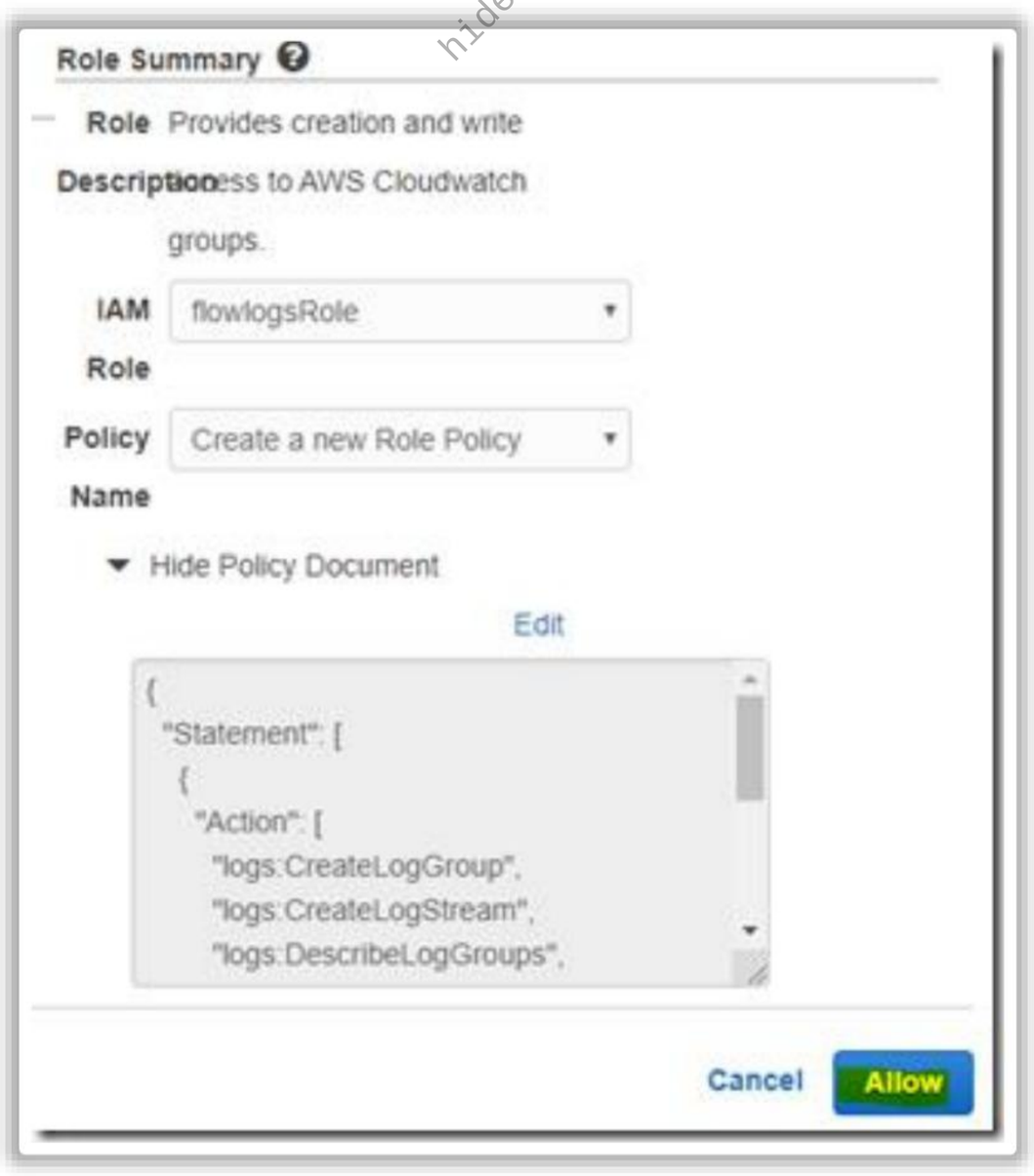


Figure 5.209: Role Summary

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

- Select the IAM Role named **flowlogsRole** from the drop-down list. Click on **Create.**

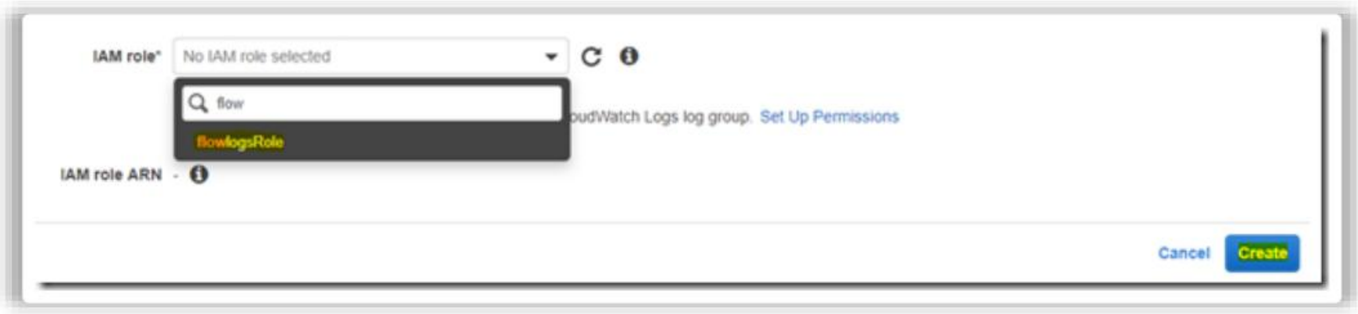


Figure 5.210: IAM Role

- Flow log is created successfully.

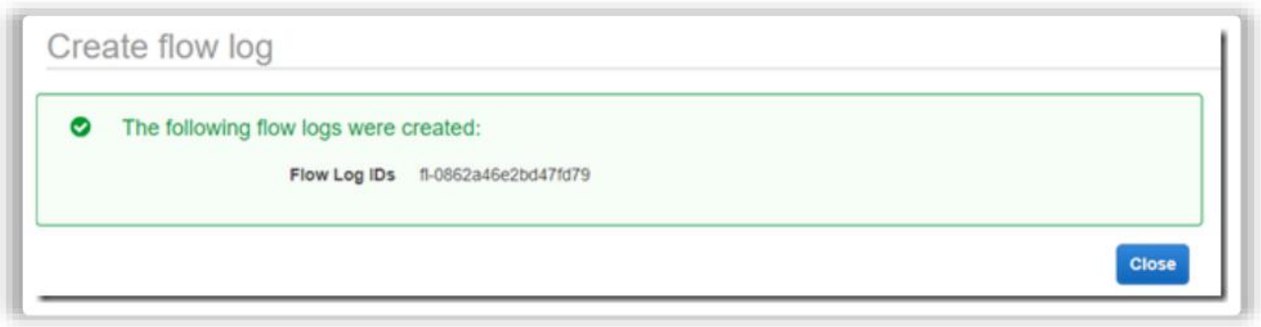


Figure 5.211: Flow Log is Created

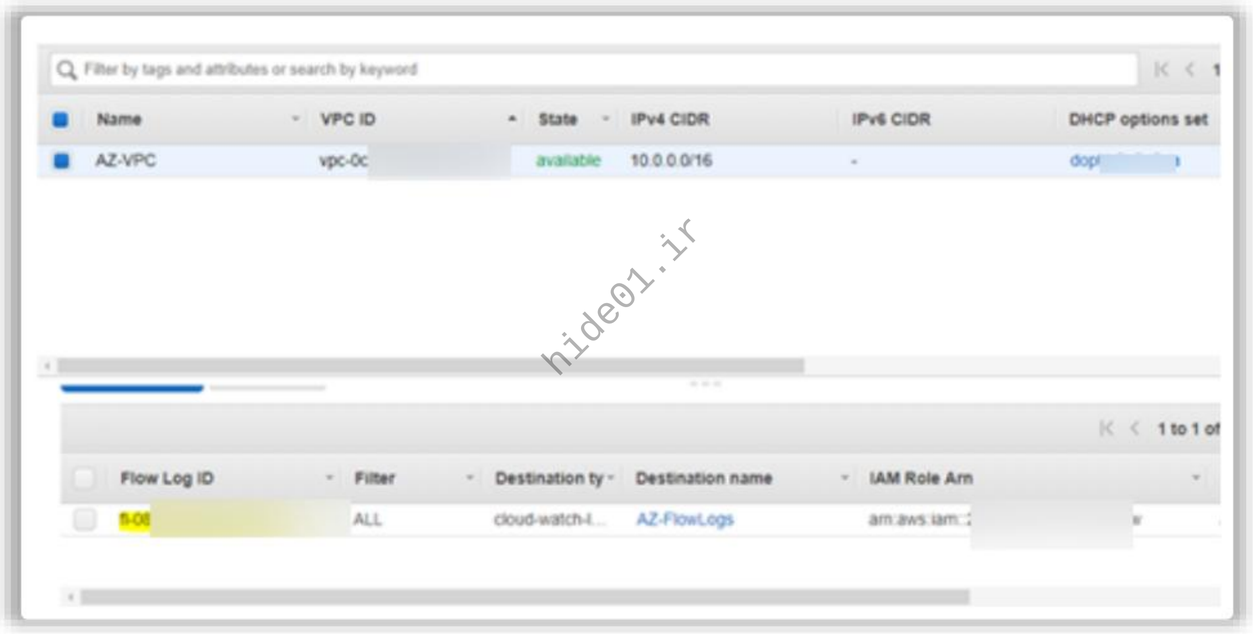


Figure 5.212: Flow Log

▪ Verification

- (For this example) Try to telnet a few ports to gather logging.

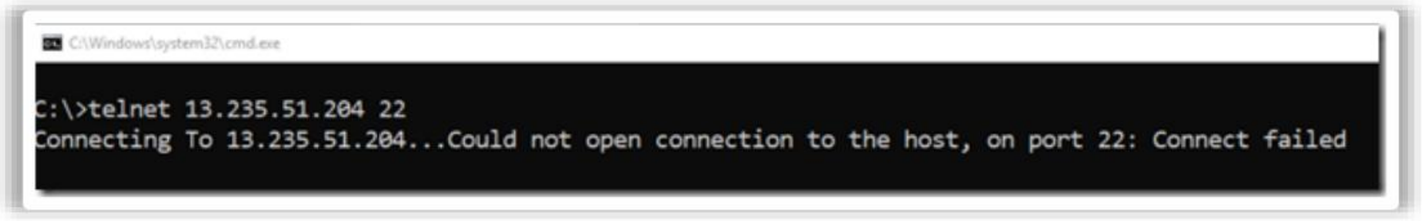


Figure 5.213: Telnet

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

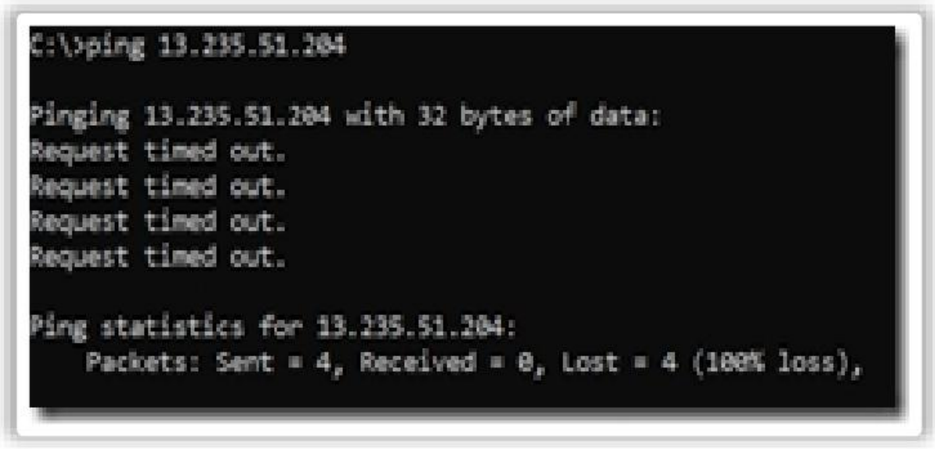


Figure 5.214: Output

- Go to CloudWatch and click on **Logs**.

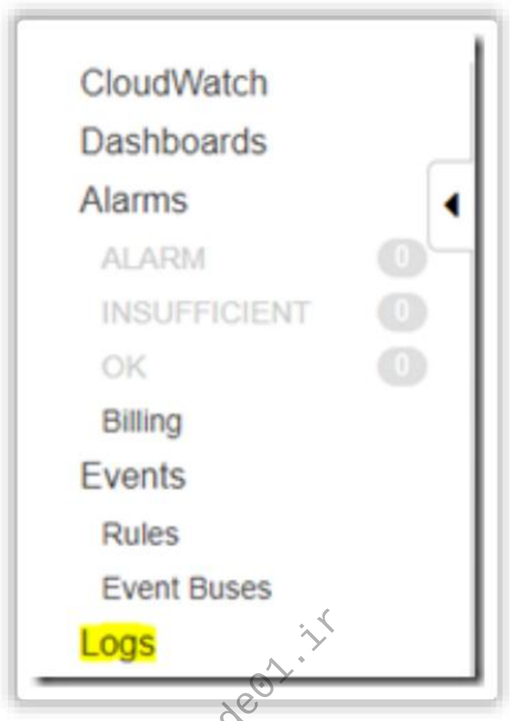


Figure 5.215: Logs

- See the VPC log group in the cloud watch.

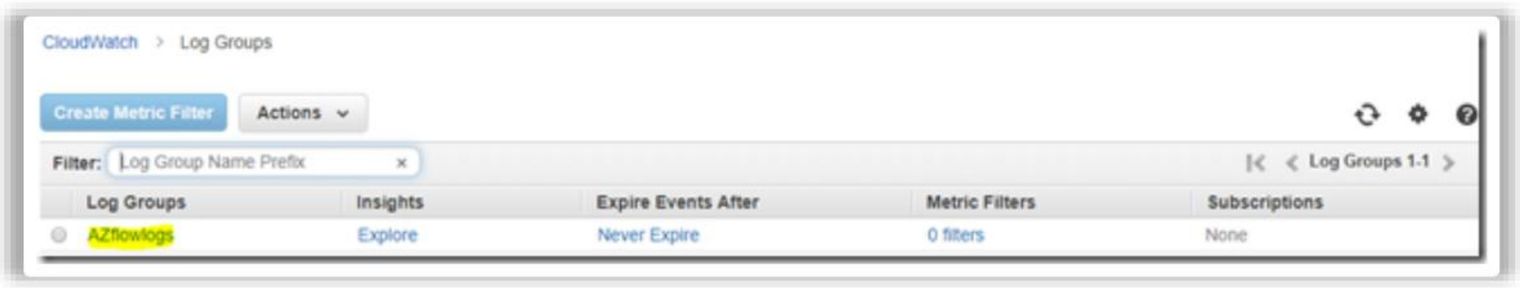


Figure 5.216: VPC Log Group

- The VPC flow logs can be viewed as shown in the following screenshot.

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

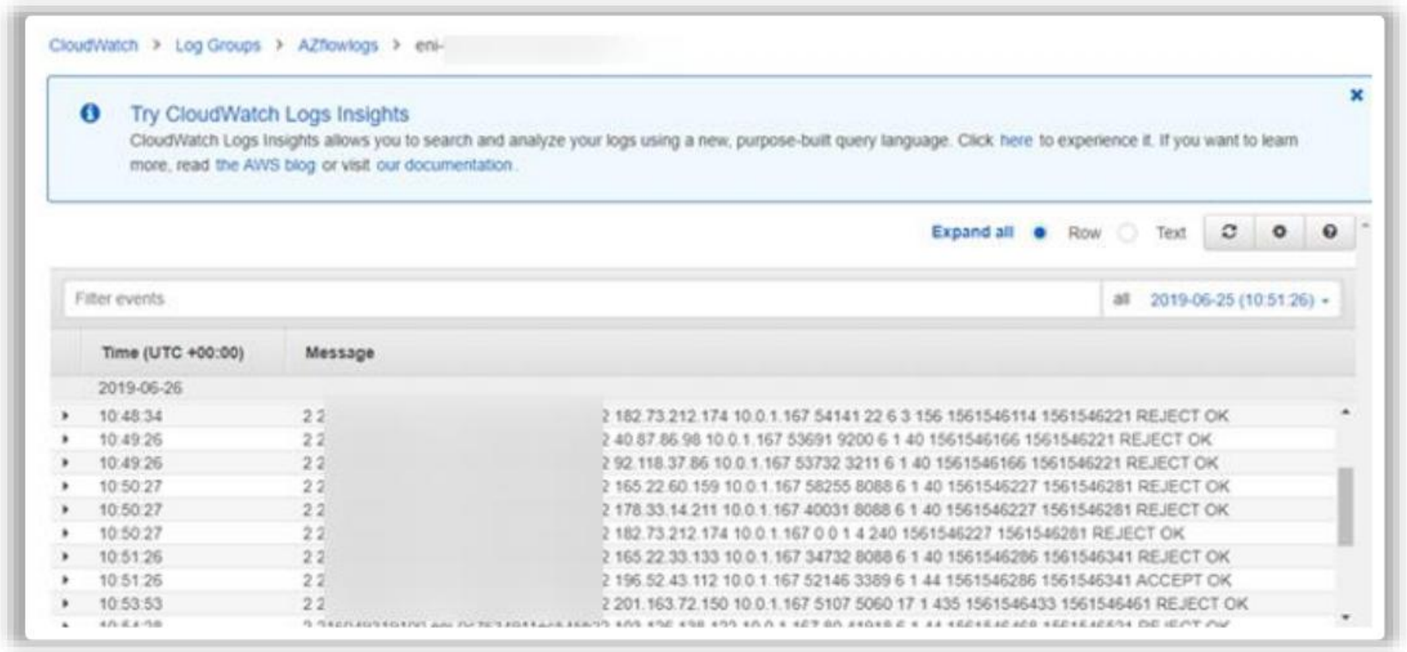


Figure 5.217: VPC Flow Logs

- Here, ports 3306 and 3389 are tested; the flow log results are shown in the following screenshot.

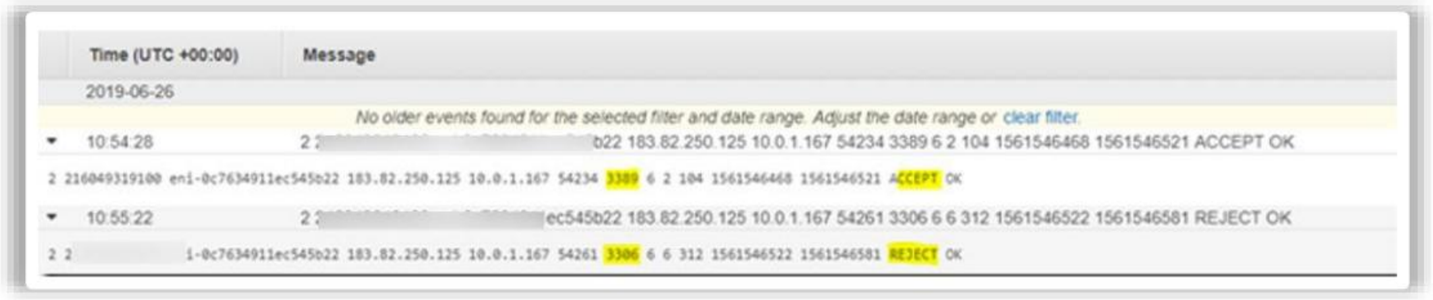
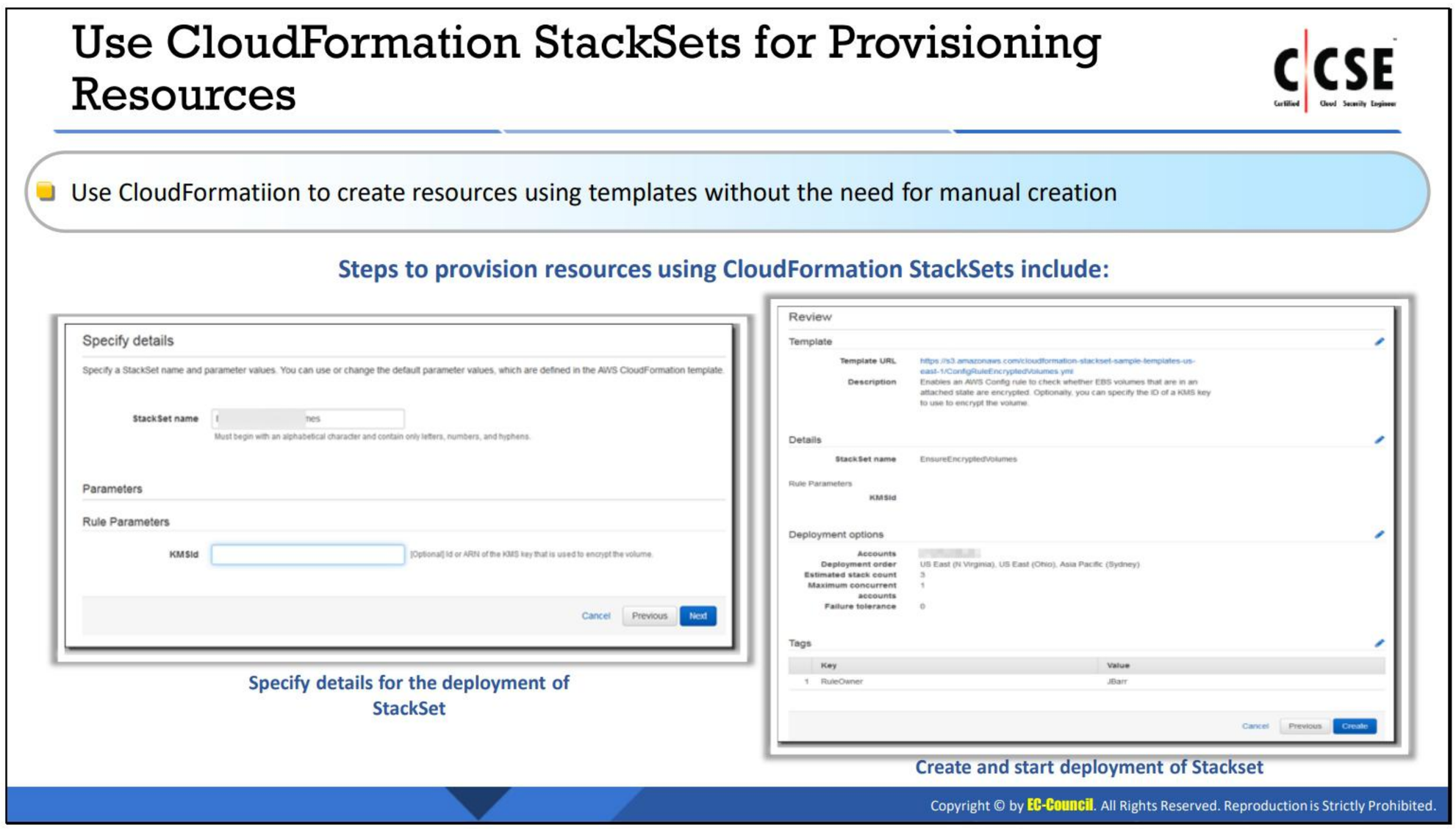


Figure 5.218: Flow Log Result

hide01.ir

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



Use CloudFormation StackSets for Provisioning Resources

CloudFormation enables the creation of resources using templates without the need for manual interference. It eliminates the chances of manual errors, increases efficiency, and provides consistent configurations while creating and provisioning environments and resources. These resources can be provisioned in multiple accounts/regions.

hidoo1.ir

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

Steps to provision resources using CloudFormation StackSets

- Go to the AWS Console and choose **Create StackSet**. Use a sample template or your own template. For example, select "**Add config rule encrypted volumes**."

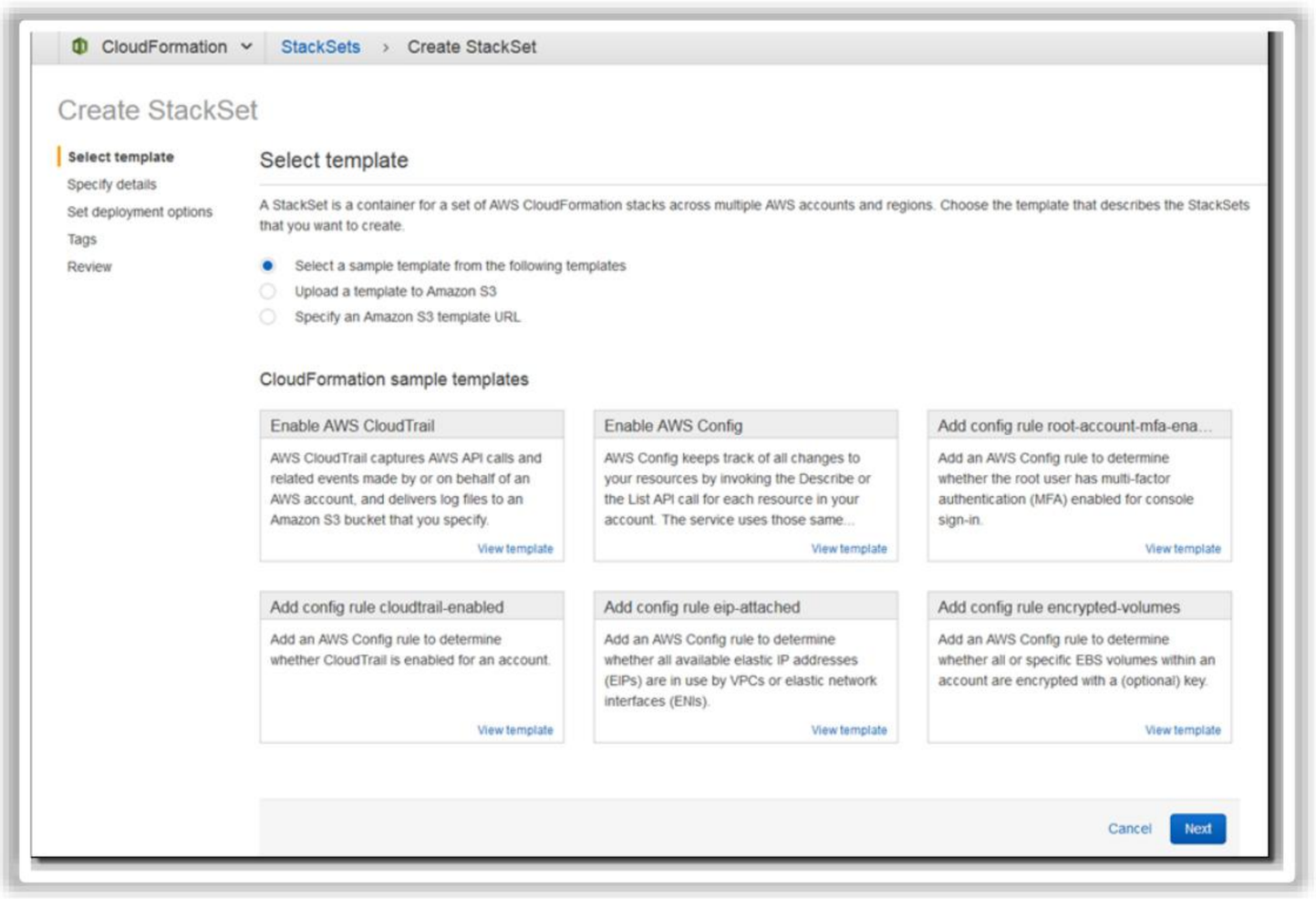


Figure 5.219: AWS Console

- To know more about the template and rule, click on **View template**.

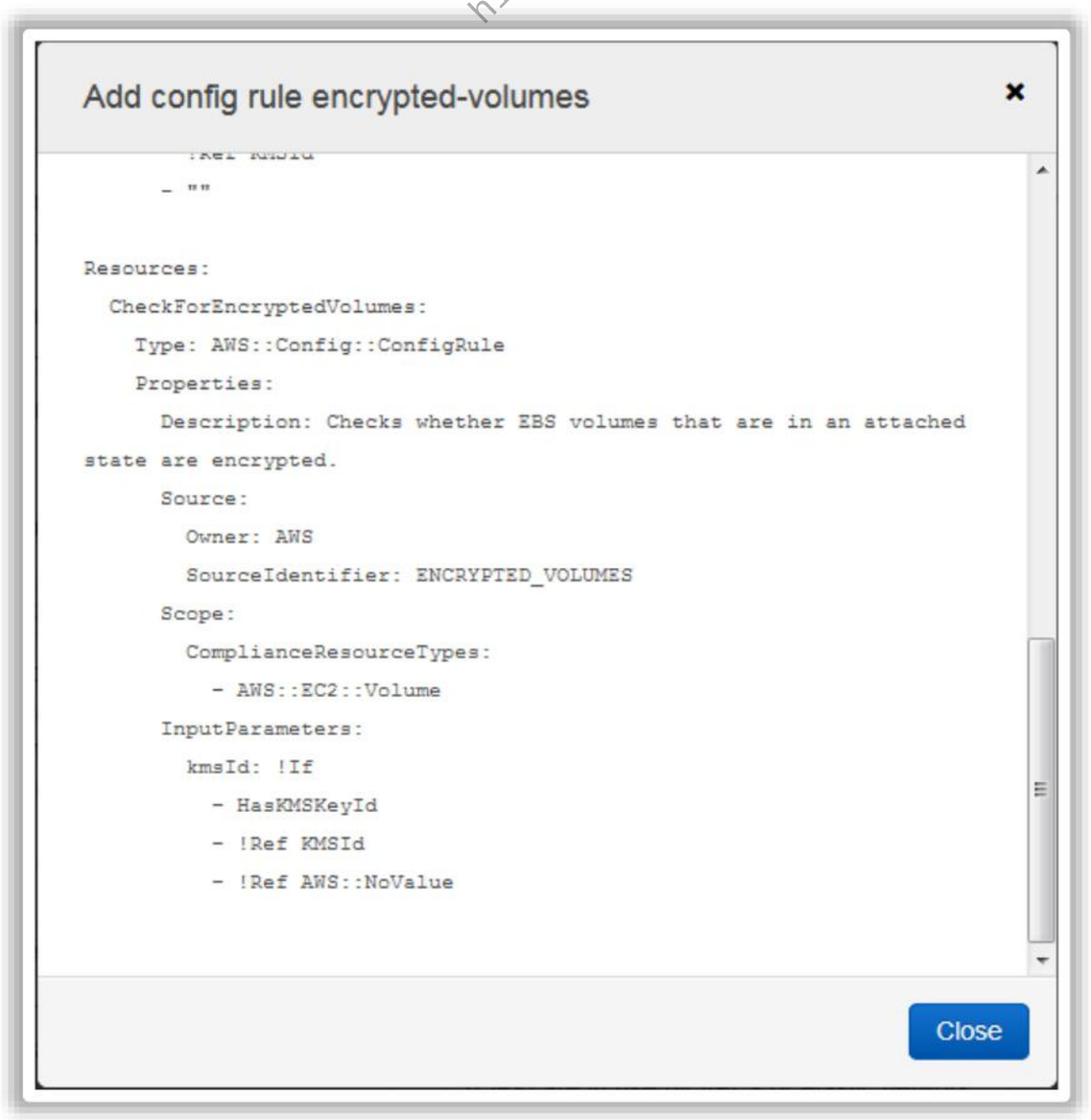


Figure 5.220: View Template

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

- Provide a name to the StackSet and an optional parameter in the relevant field.

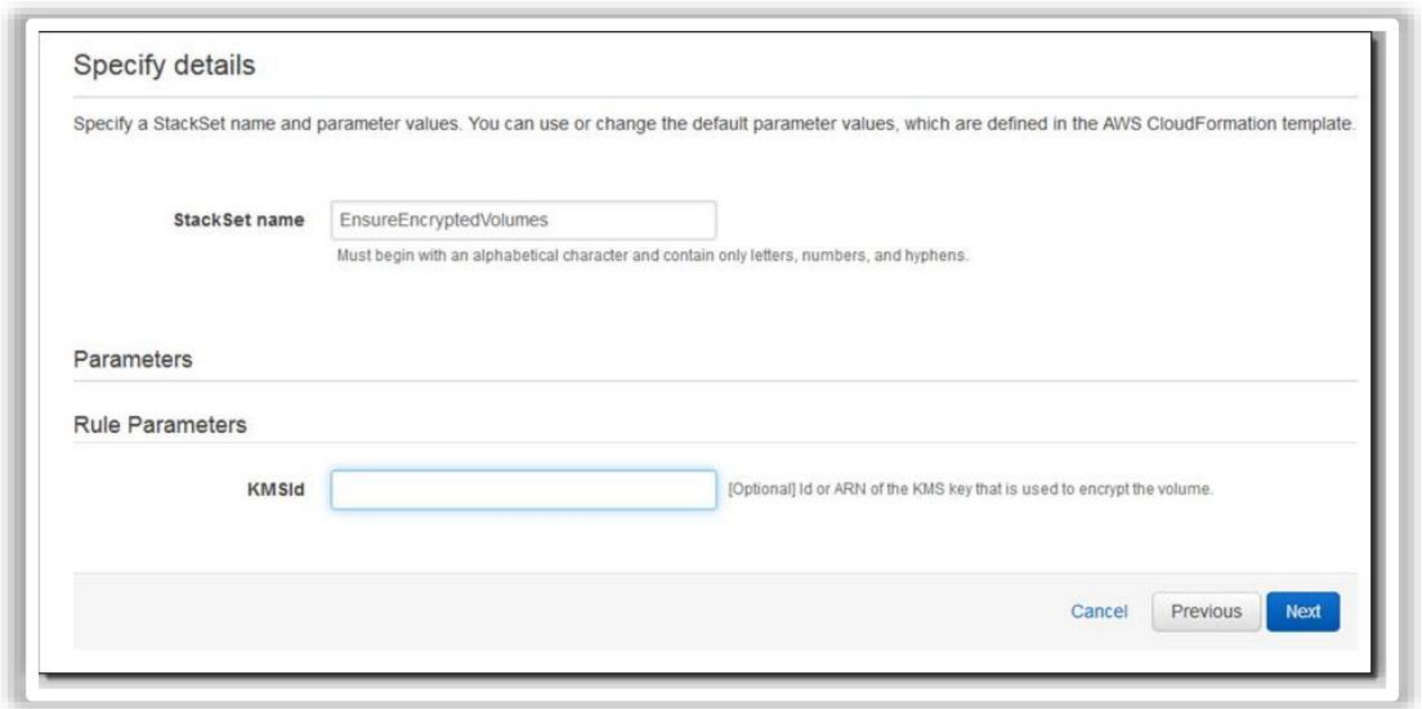


Figure 5.221: Specify Details

- Select the accounts under **Deployment Options** by entering account numbers, uploading a list of account numbers, or referencing an organizational unit.

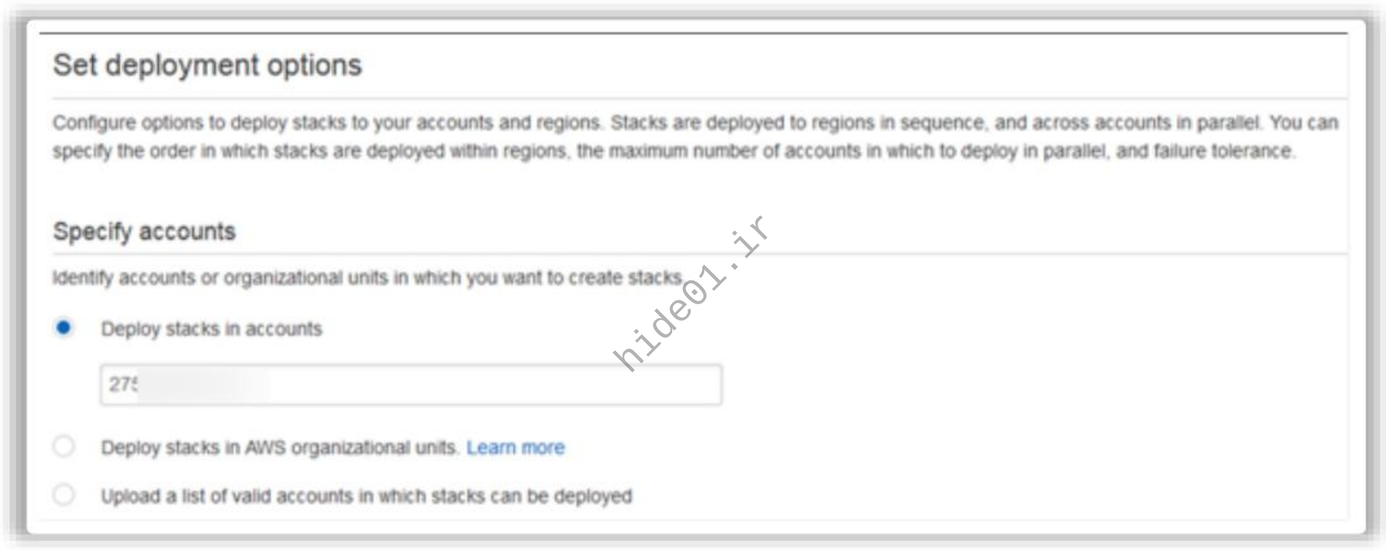


Figure 5.222: Set Deployment

- Choose the regions and control the deployment order.

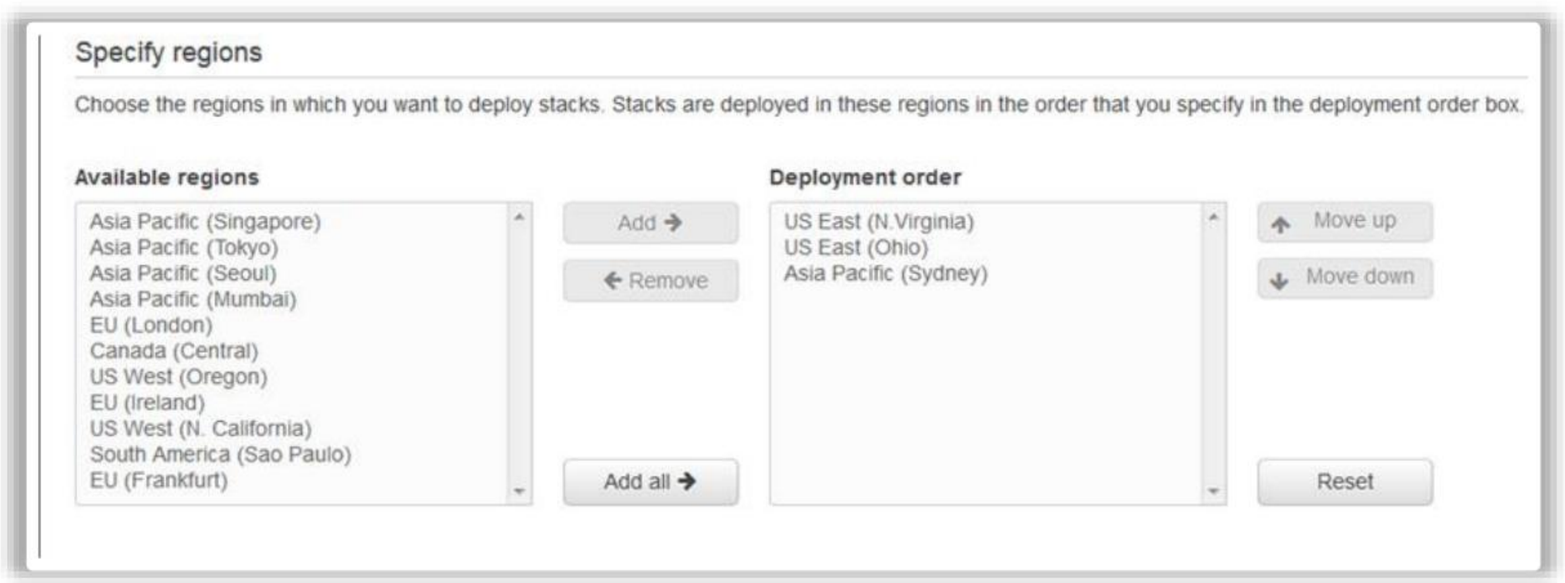


Figure 3.223: Specific Regions

- Select the deployment options (for **Failure tolerance** and **Max. Concurrent accounts**) and click on **Next**.

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

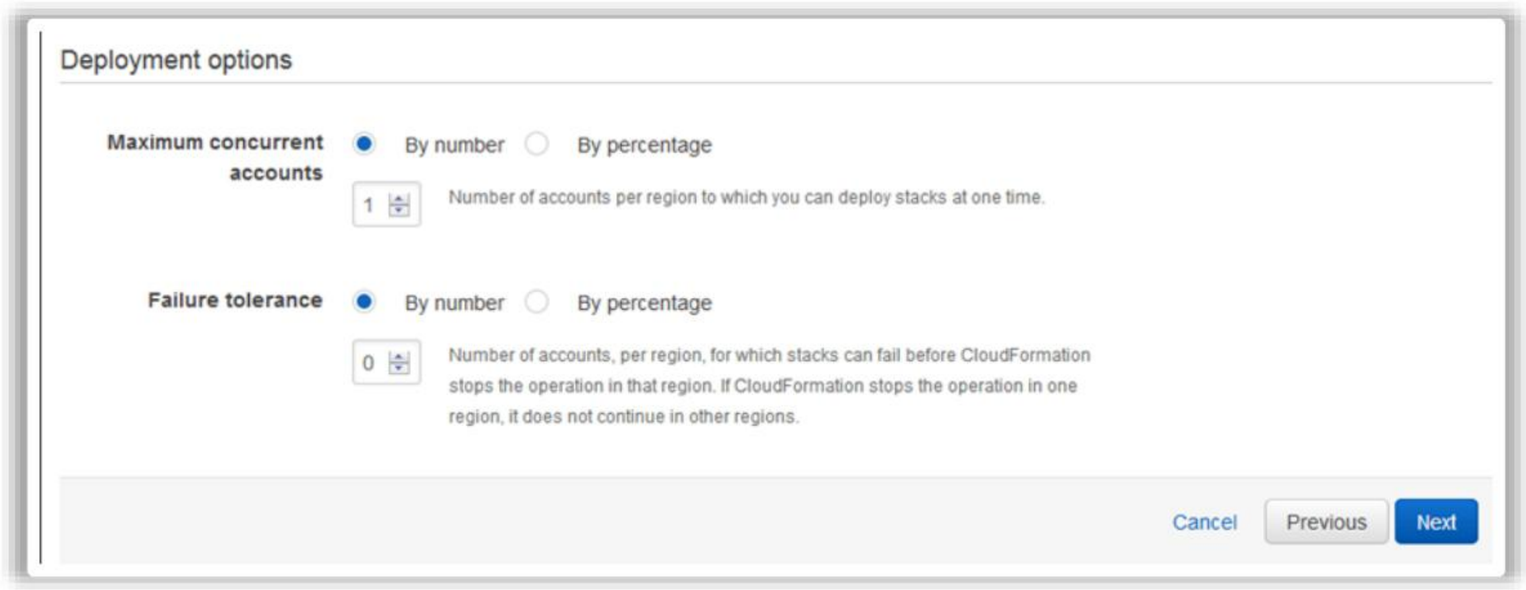
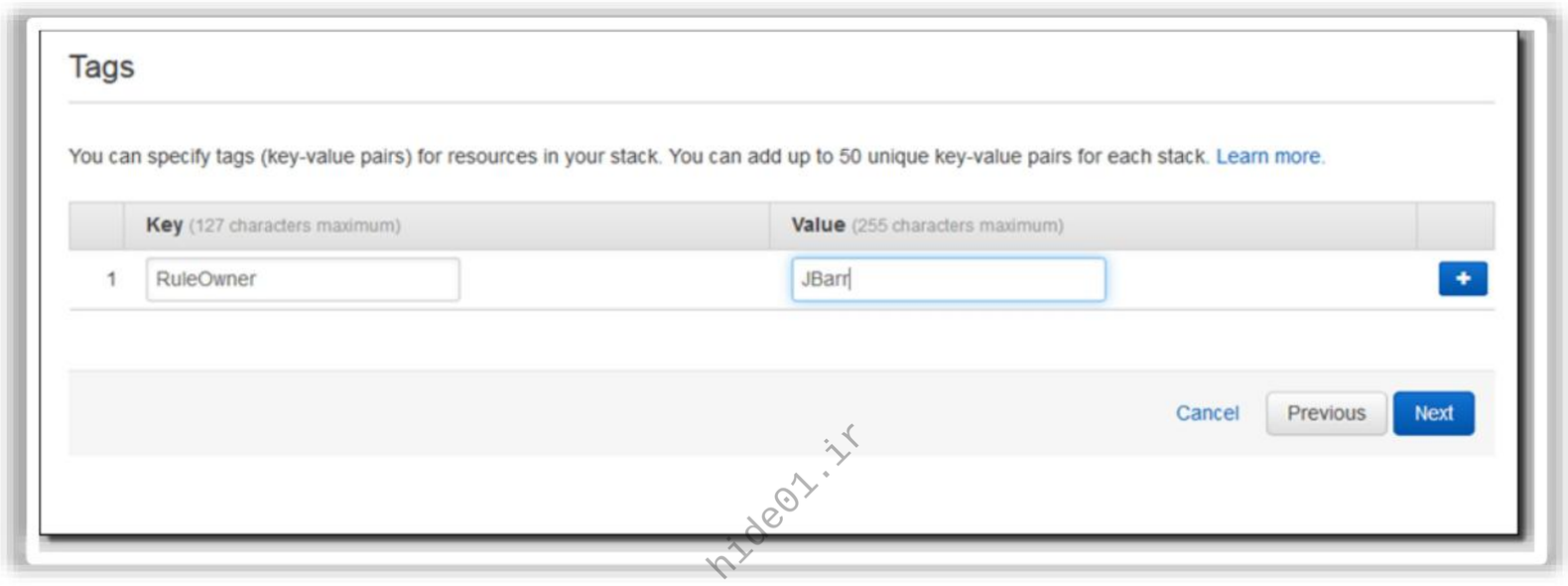


Figure 5.224: Deployment Options

- Add tags to the StackSet, which will be applied to resources created during deployment, and click on **Next**.



hide01.ir

Figure 5.225: Tags

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

- Review all details before deployment and click on **Create**. Thus, deployment will start.

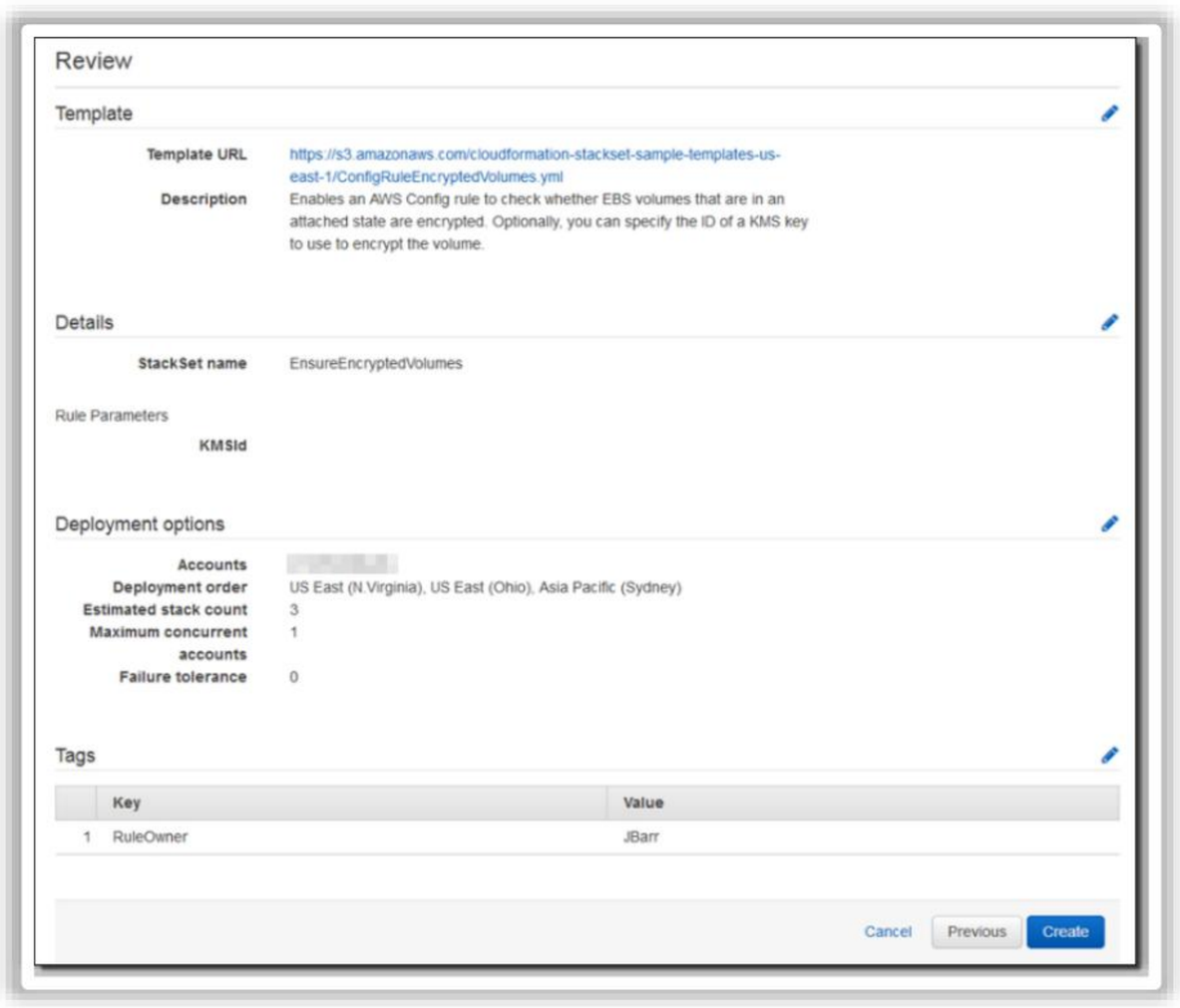


Figure 5.226: Review

- Track the deployment status via the Console. The status of stacks is shown to be **OUTDATED**. It indicates that the template is yet to be deployed to the stack. The status will change to **CURRENT** once deployment is successful. When a stack cannot be deleted, the status is shown as **INOPERABLE**.

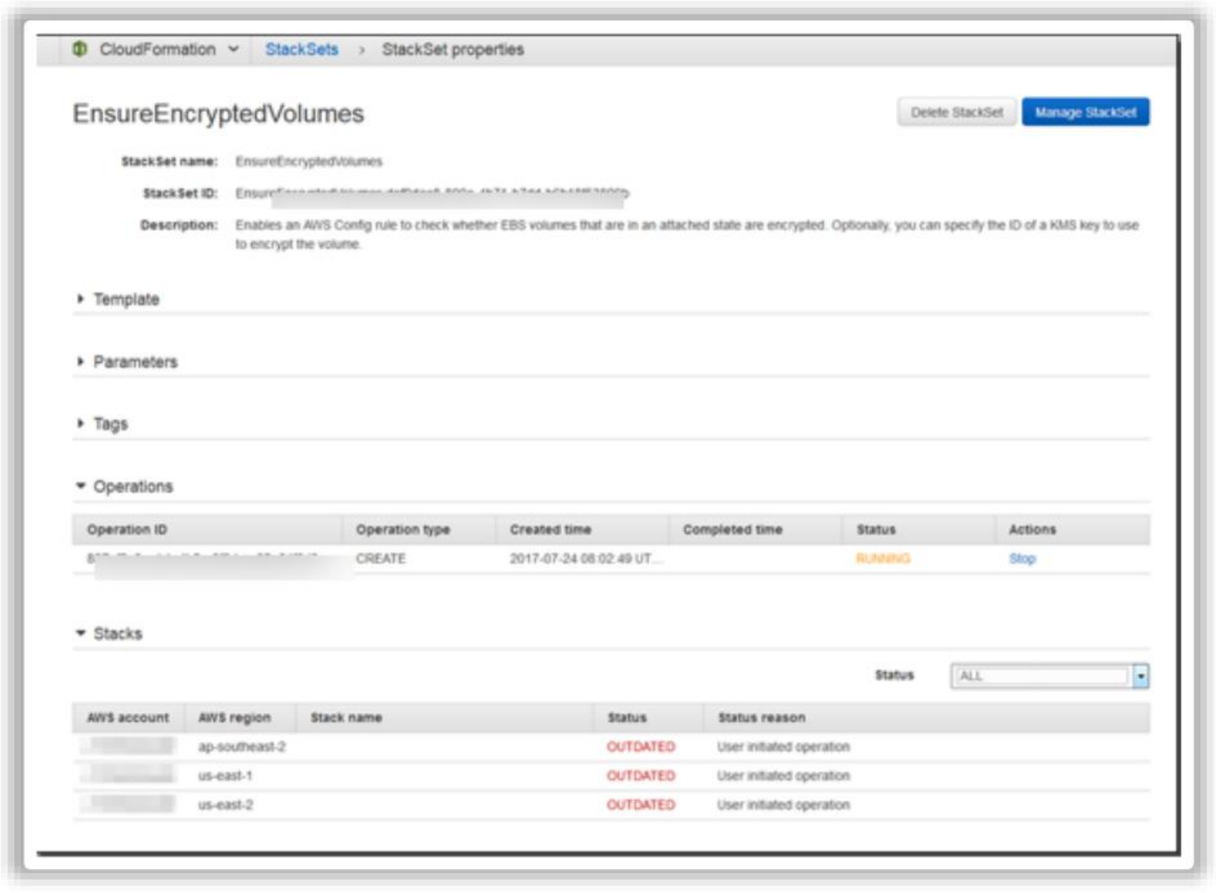


Figure 5.227: EnsureEncryptedVolume

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

- Click on **Manage StackSet** after deployment to add more accounts/regions or create additional stacks.

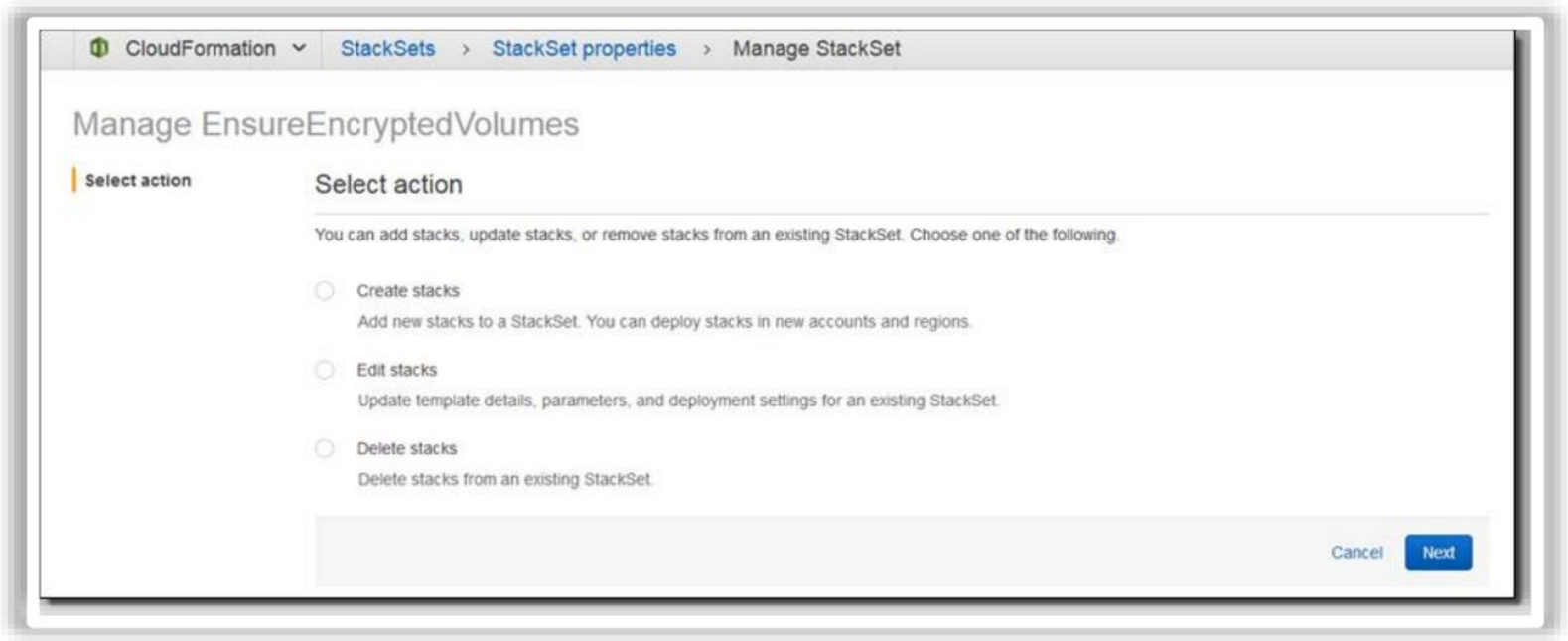
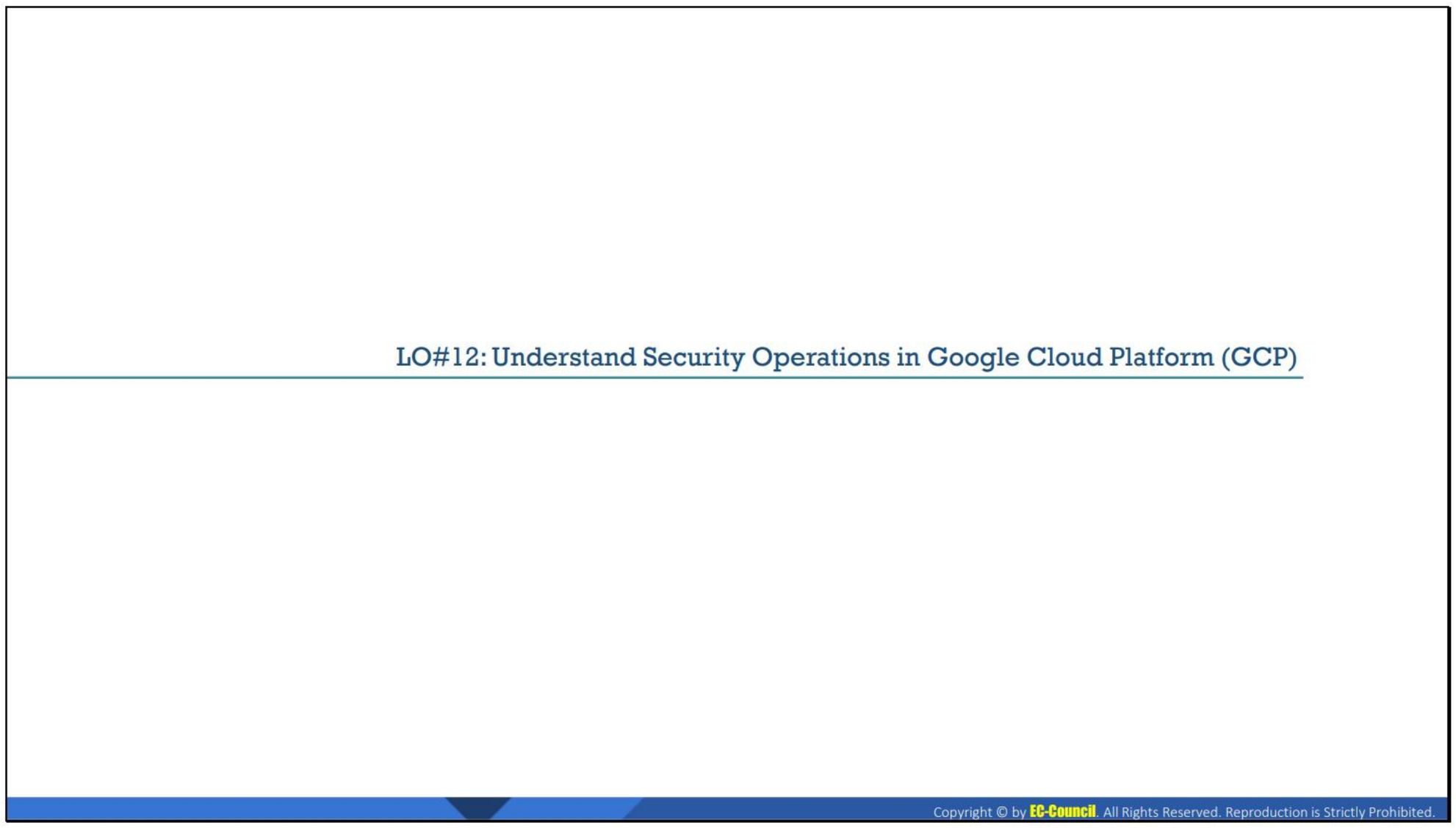


Figure 5.228: Manage StackSet

hide01.ir

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

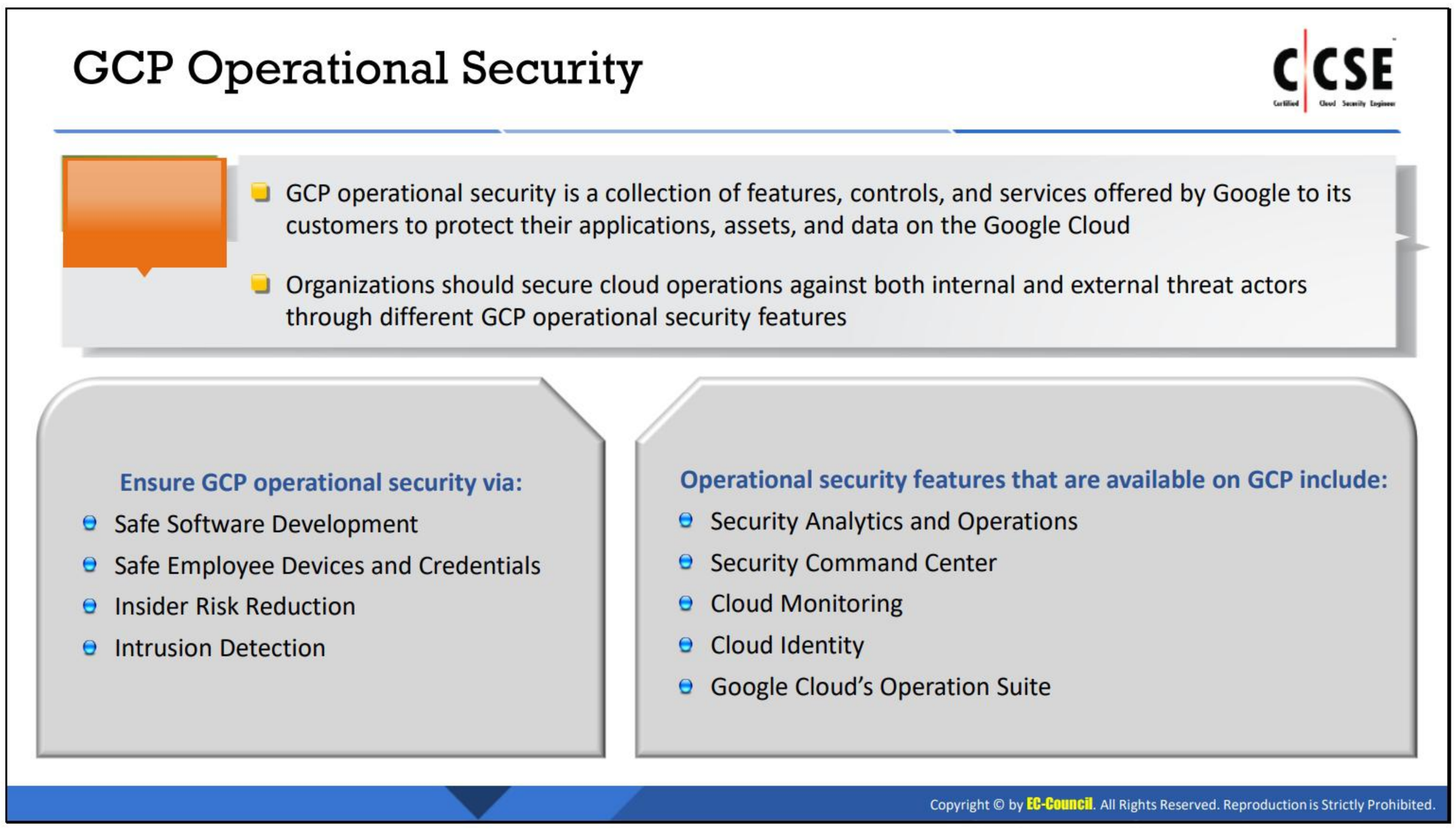


LO#12: Understand Security Operations in Google Cloud Platform (GCP)

The objective of this section is to understand the features and services in GCP (Google Cloud Platform) that can be used to ensure operational security. This section discusses GCP features and services such as Security Analytics and Operations, Cloud Monitoring, Security Command Center (SCC), Cloud Identity, and Google Cloud's Operation Suite. By understanding these features, cloud security engineers can secure cloud operations in their GCP environments.

hiu01.ir

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



GCP Operational Security

GCP operational security is a collection of features, controls, and services offered by Google to its customers to protect their applications, assets, and data on Google Cloud. GCP operational security ensures that all cloud operations are secure and satisfy customer requirements.

Implement the following to ensure GCP operational security:

- **Safe Software Development**: Implement safe software development on GCP using libraries and frameworks provided by GCP to eliminate XSS vulnerabilities, ensuring manual security reviews, and conducting vulnerability reward programs.
- **Keep Employee Devices and Credentials Safe**: Monitor and protect employee devices and credentials continuously to protect them from being compromised by keeping the devices up-to-date and implementing application-level access management controls.
- **Reduce Insider Risk**: Reduce risks by assigning the least privilege to employees and automating tasks. Monitor the activities of employees who have admin privileges.
- **Intrusion Detection**: Detect intrusions on GCP using advanced data processing pipelines that integrate signals from various sources such as devices, and monitor points and infrastructure services.

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

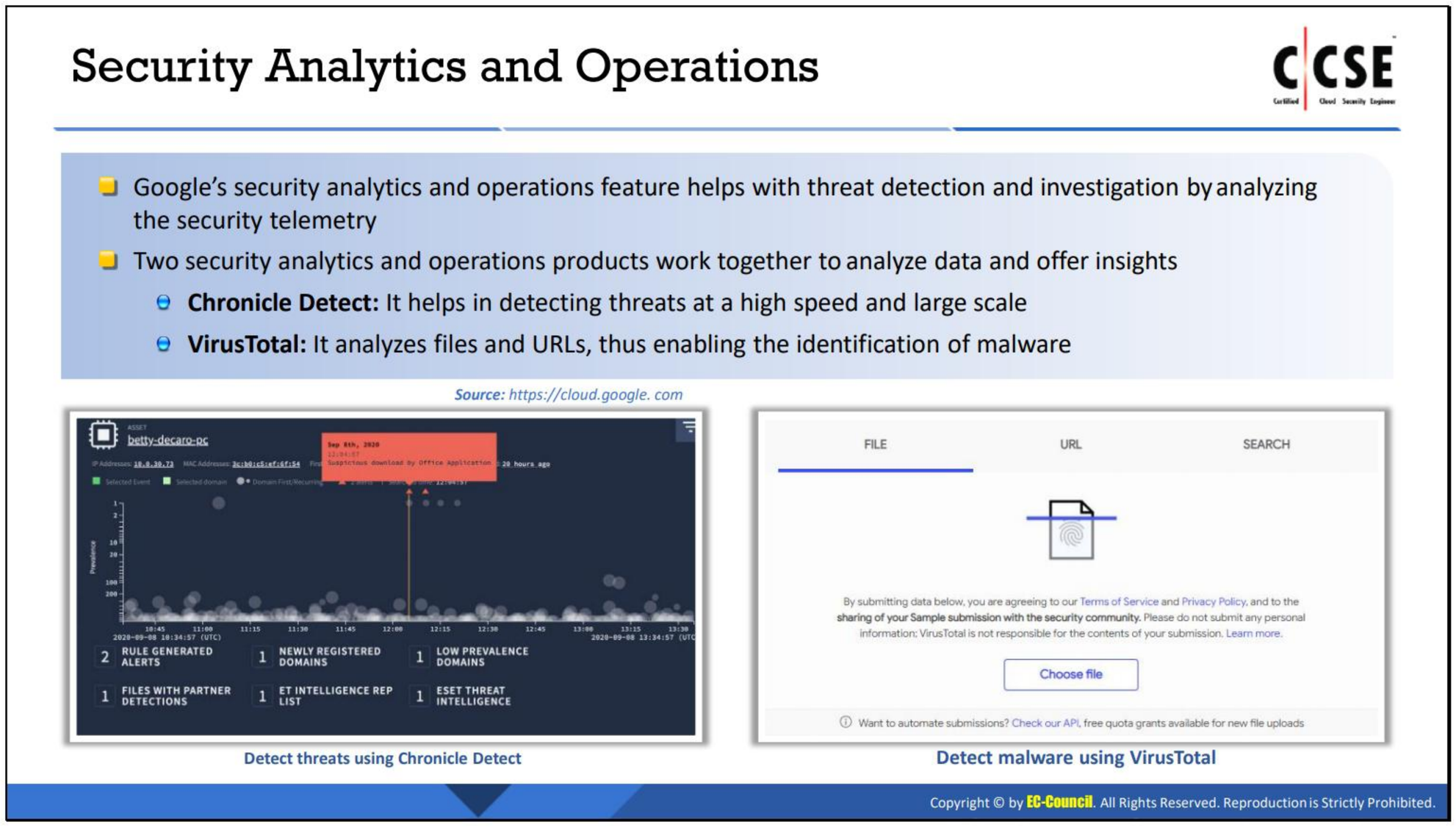
GCP Operational Security features

Following are the operational security features provided on GCP:

- Security Analytics and Operations
- Security Command Center
- Cloud Monitoring
- Cloud Identity
- Google Cloud's Operation Suite

hide01.ir

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



Security Analytics and Operations

The security analytics and operations feature of Google help with threat detection and investigation. It mainly focuses on detecting threats and investigating by analyzing security telemetry. This feature can be used to store and analyze petabytes of security telemetry to detect and investigate threats rapidly.

The key features of Security Analytics and Operations include:

- **Intelligent data fusion**: This feature improves threat investigation and detection by providing timelines and enriched data models.
- **Modern threat detection**: It helps in detecting complex threats using YARA (Yet Another Recursive/Ridiculous Acronym) rules.
- **Continuous IoC matching**: It analyzes security telemetry data along with threat intelligence and provides continuous IoC matching to detect threats.

Google provides two security analytics and operations products that work together to analyze data and offer insights.

- **Chronicle Detect**: It is a threat detection solution on the Google infrastructure that detects threats at a high speed and large scale. It employs a rule engine that helps to edit and create detection rules to detect threats based on requirements.

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

Figure 5.229: Detect multi-event attacks using Chronicle Detect

- **VirusTotal**: VirusTotal is a free online web-based scanner offered by Google that analyzes files and URLs, thus enabling malware identification. It filters malicious content from uploaded files, URLs, and domains using more than 70 antivirus scanners, URL/blacklisting services, and other tools.

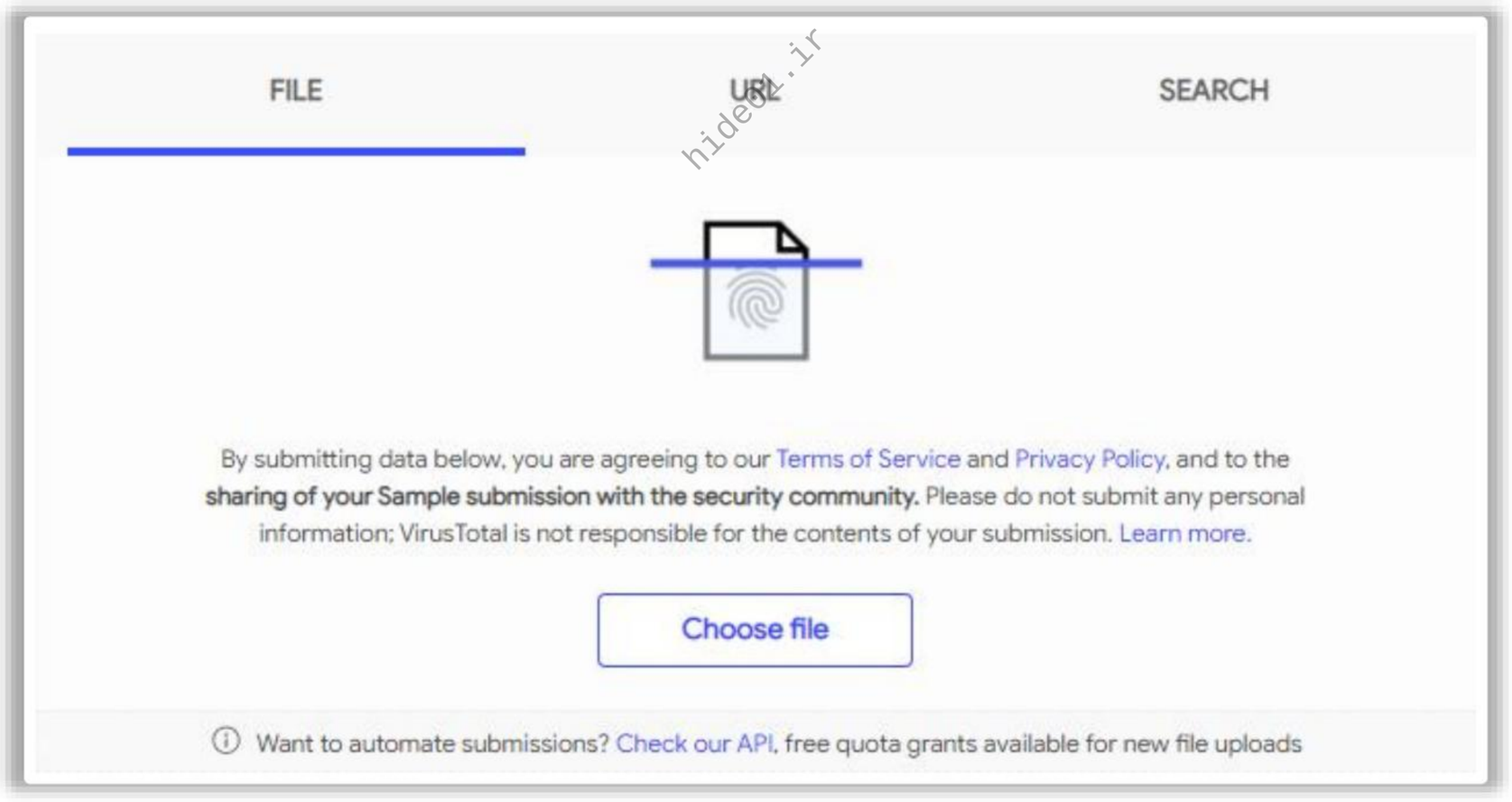
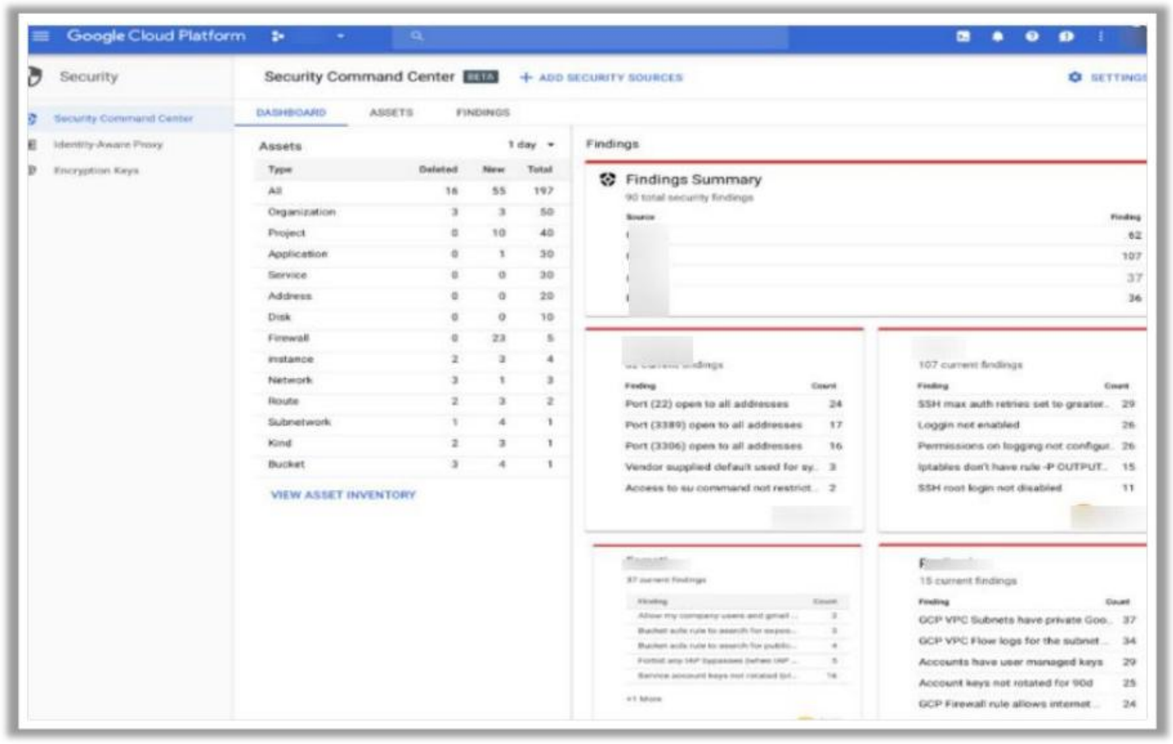


Figure 5.230: Detect malware using VirusTotal

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

Security Command Center (SCC)

- **Google Cloud Security Command Center (SCC)** helps cloud security professional to collect and analyze data, detect threats, and respond to them before they impact cloud operations
- Use it to obtain insights into data and application risk via its dashboard, thereby enabling quick and easy threat detection, and response and helping in fixing misconfigurations and maintaining compliance



Google Cloud SCC dashboard

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

Security Command Center

Security Command Center (SCC) helps cloud security professionals in collecting and analyzing data, detecting threats, and responding to them before they impact cloud operations. It provides deep insight into data and application risks via its dashboard, thereby enabling quick and easy threat detection and response, fixing misconfigurations, and maintaining compliance. Use Google SCC to secure cloud operations by viewing and monitoring cloud assets, identifying common web vulnerabilities, scanning storage systems for sensitive data, and reviewing the access rights to critical resources via a single centralized dashboard.

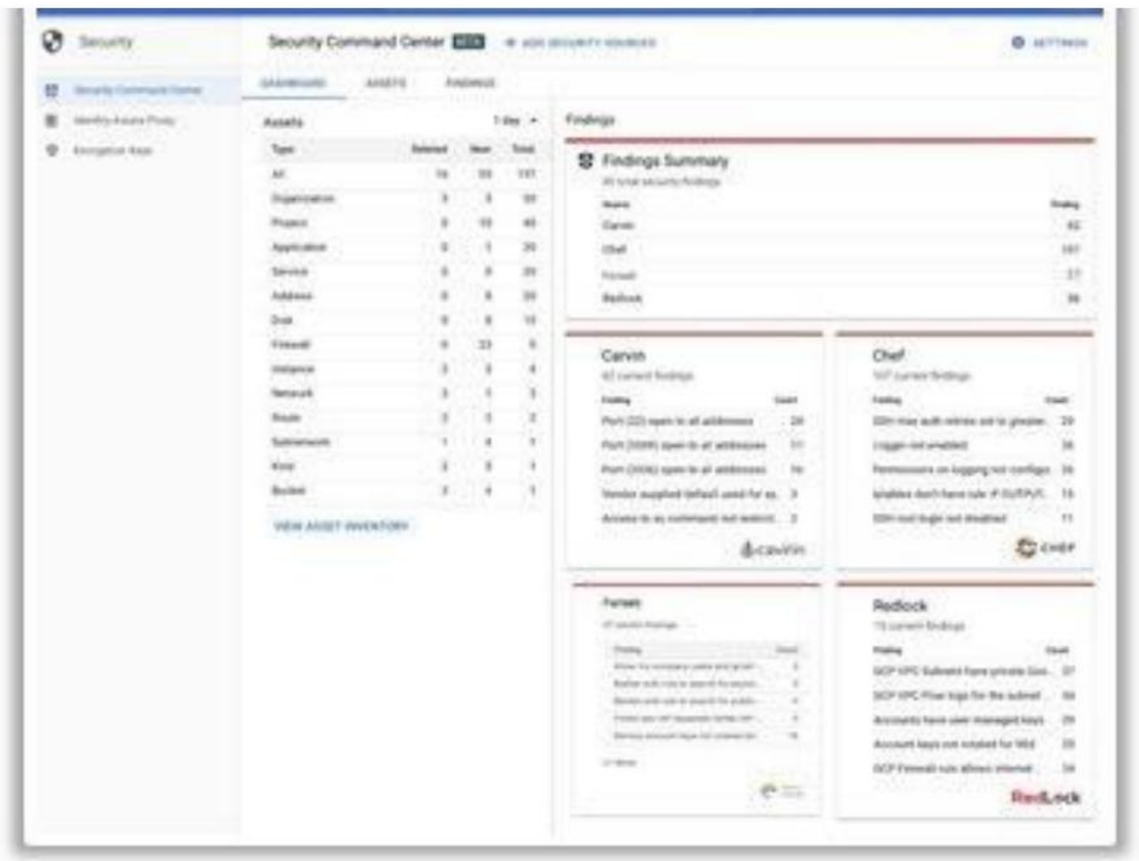


Figure 5.231: Google Cloud SCC dashboard

SCC offers the following operational security features:

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

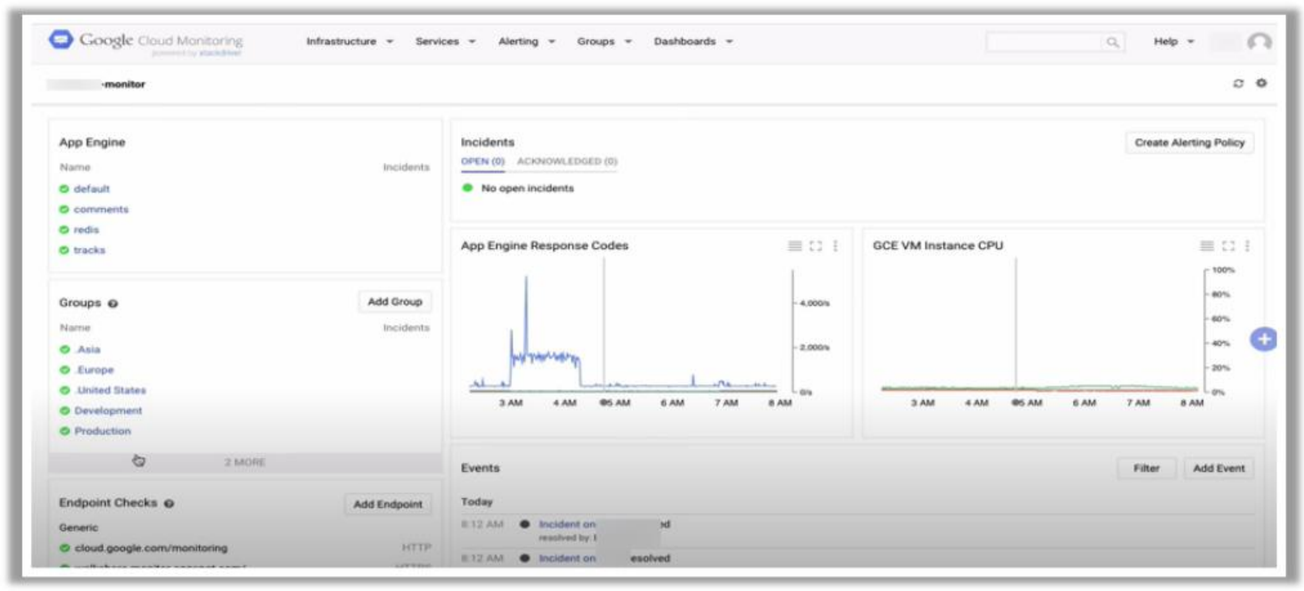
- **Asset discovery and inventory**: SCC helps cloud security professionals to discover and view their assets in near-real-time across Cloud Storage, Compute Engine, Cloud IAM, and App Engine. Security professionals can review historical discovery scans to determine new, deleted, or modified assets.
- **Threat prevention**: SCC helps in understanding the security posture of Google Cloud assets by revealing common web application vulnerabilities or outdated libraries present in web applications that run on GKE, App Engine, and Compute Engine. SCC allows security professionals to quickly fix these vulnerabilities by clicking on the impacted resources directly and following the specified procedure.
- **Threat detection**: SCC uses the logs running in the GCP to detect threats. It detects common threats such as reverse shell, suspicious library, and suspicious binary.

hide01.ir

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

Cloud Monitoring

- **Google Cloud Monitoring** provides enhanced visibility into the availability, health, and performance of cloud infrastructure and applications
- Use it to visualize insights through charts and dashboards and generate alerts



Cloud Monitoring GUI

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

Cloud Monitoring

Google Cloud Monitoring is a collection of tools that provides enhanced visibility into the availability, health, and performance of the cloud infrastructure and applications. It helps in monitoring apps and services in real-time on GCP via its dashboard by collecting metrics from various sources, including hybrid and multi-cloud infrastructures. Cloud Monitoring helps cloud security professionals by visualizing insights using charts and dashboards and generating alerts.

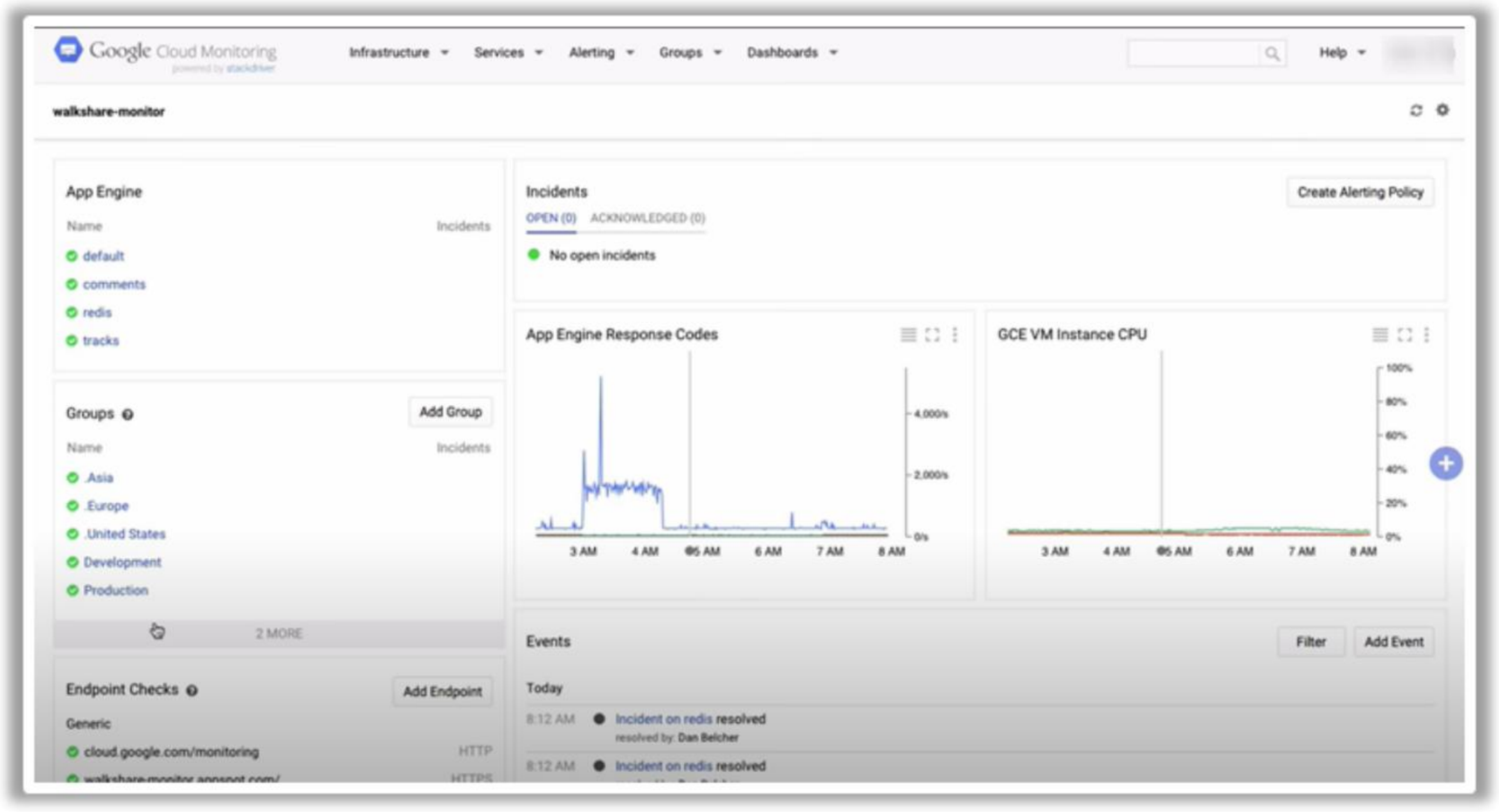


Figure 5.232: Cloud Monitoring GUI

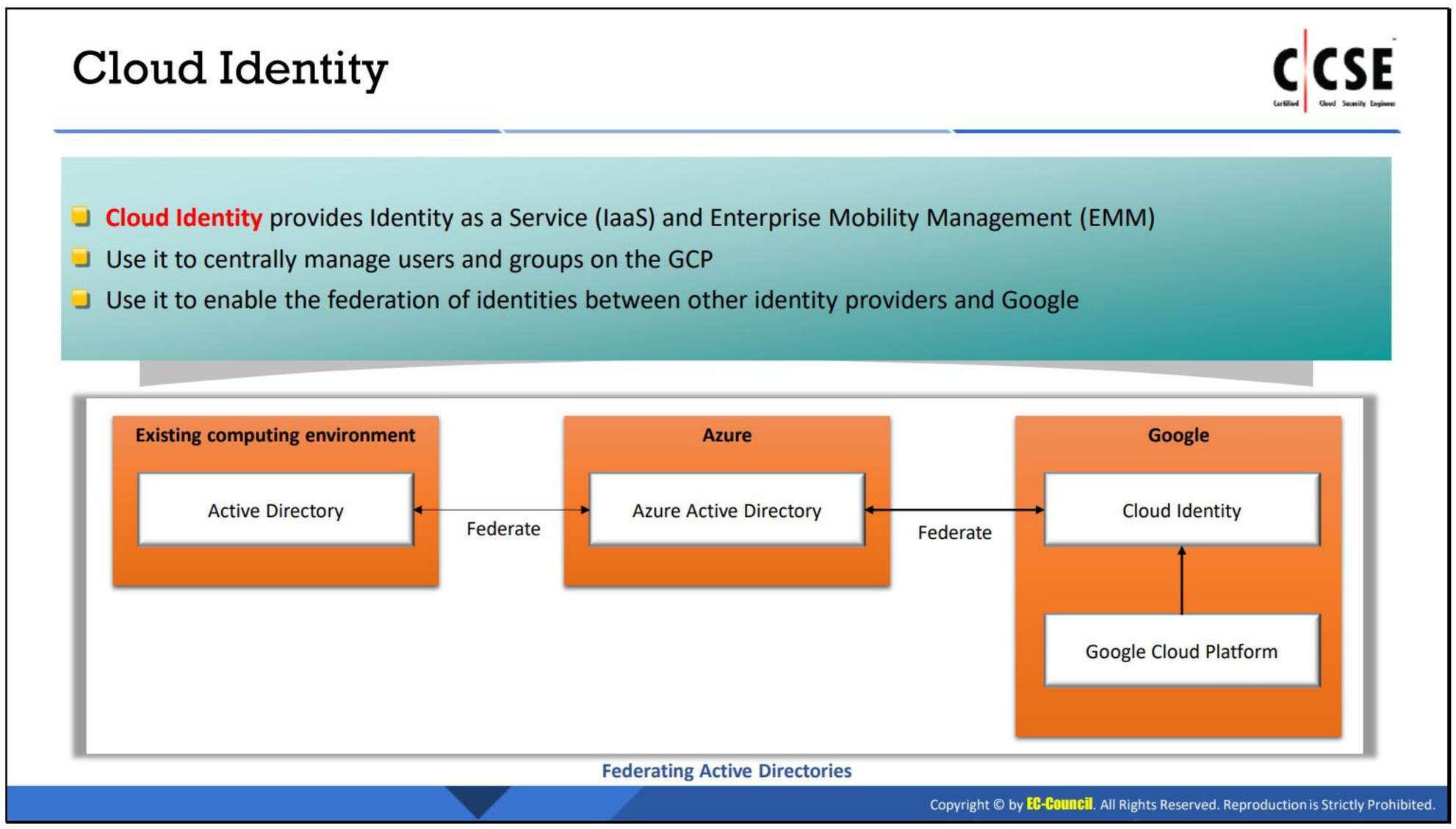
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cloud Monitoring offers the following operational security features:

- **SLO monitoring**: Cloud Monitoring allows security teams to define custom service-level objectives (SLOs) for applications to ensure that they receive alerts in the case of SLO violation.
- **Logging integration**: It provides deep insights across dashboard and charts to logs.
- **Uptime monitoring**: It helps in monitoring the availability of internet-accessible VMs, URLs, APIs, and load balancers across the world. Cloud admins can use Cloud Monitoring alerts to receive notifications during outage.
- **Alerting**: It enables the definition of alerting policies; thus, when an event occurs or the custom metrics violate the defined rules, security teams are notified via emails, SMS, or Slack.

hide01.ir

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



Cloud Identity

Cloud Identity is a service provided by Google that helps cloud administrators to centrally manage users and groups on GCP. Cloud Identity provides identity as a service (IDaaS) and enterprise mobility management (EMM). Use Cloud Identity to retain more control over the accounts used in an organization. Cloud Identity helps to manage access and compliance across users in the organization who use their accounts, such as Gmail accounts. It allows the federation of identities between other identity providers and Google. Cloud admins can use Cloud Identity for managing all apps, users, and devices from a central location (Google Admin console).

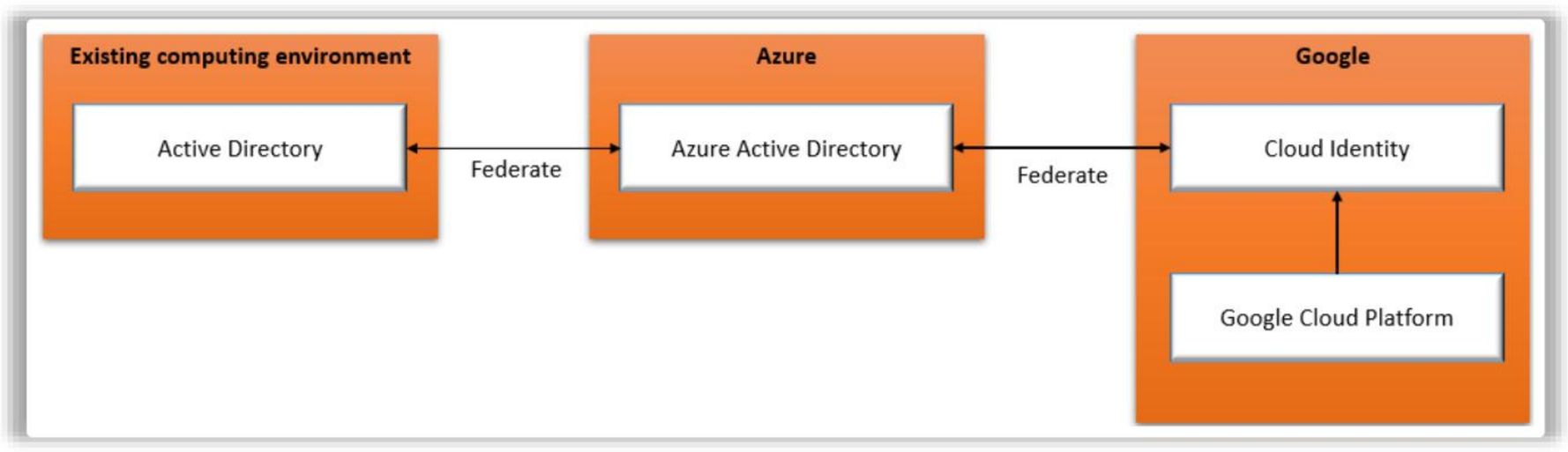


Figure 5.233: Federating Active Directories

Some operational security features offered by Cloud Identity include:

- **Password management**: Cloud Identity helps with password management by allowing cloud admins to monitor and enforce user password requirements.
- **Automated user provisioning**: It allows cloud admins to automatically save the changes to user identities in the Google Admin console via automated user provisioning.

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

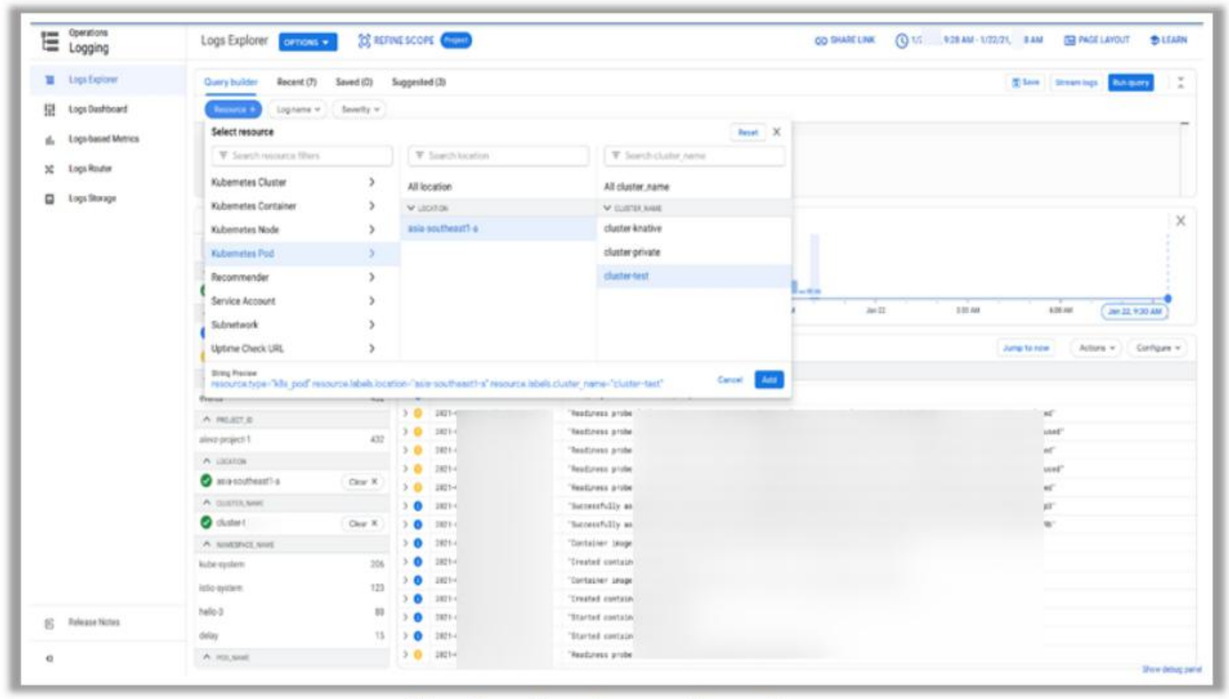
- **Security reports**: It allows cloud admins to monitor the exposure of users to data compromise via security reports. These reports provide a clear view of how users share and access data.
- **Account activity reports**: Using Cloud Identity, cloud admins can check the status and account activity of users using account activity reports.

hide01.ir

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

Google Cloud's Operation Suite

- **Google Cloud's Operation Suite** is a collection of management tools that help in securing cloud operations
- Use it to collect metrics, traces, and logs across applications and Google cloud and determine a unique dashboard that helps cloud admins to monitor the GCP and applications easily



Cloud Logging via operation suite

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

Google Cloud's Operation Suite

Google Cloud's operation suite is a collection of management tools that help in securing cloud operations. It consists of Cloud Logging and Error Reporting, Cloud Monitoring, and Application Performance Management tools (Cloud Trace, Cloud Profiler, and Cloud Debugger). It gathers metrics, traces, and logs across applications and Google cloud and provides an unique dashboard that helps cloud admins to monitor the GCP and its applications easily. They can set alerts and notification rules along with performance and availability indicators using the operation suite.

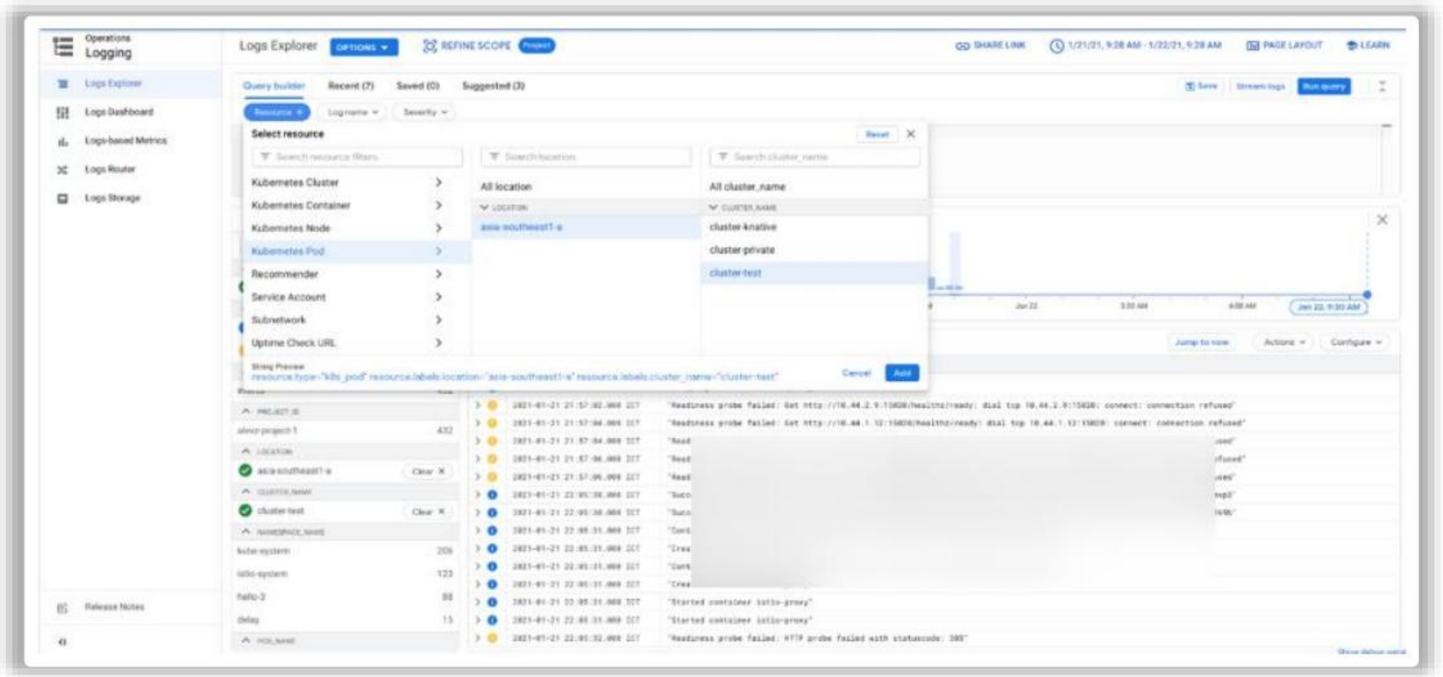


Figure 5.234: Cloud Logging via operation suite

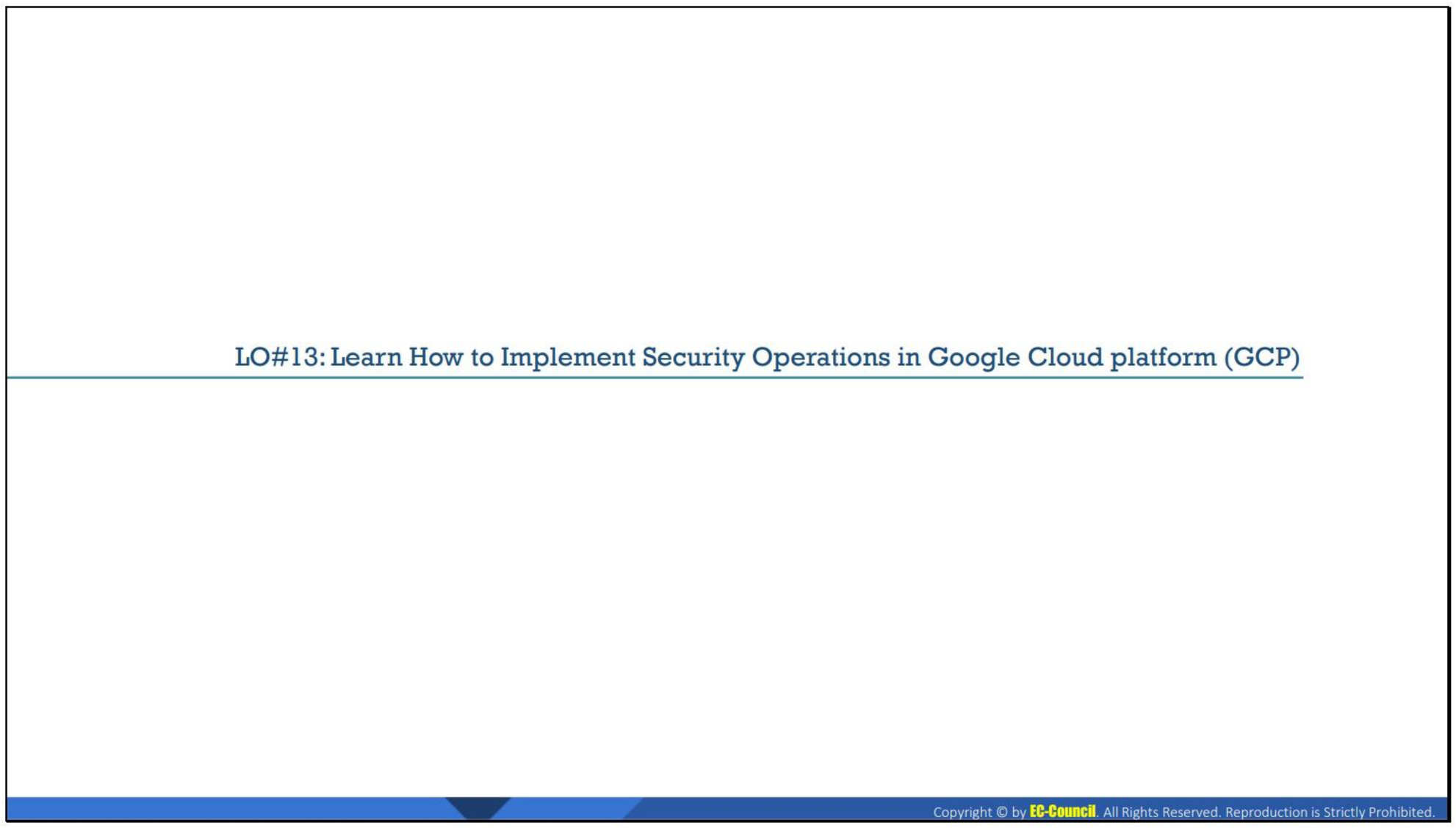
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Google Cloud's operation suite offers the following features:

- **Real-time log management and analysis**: The operation suite provides real-time log management and analysis. The Cloud Logging service of the suite uses the application and system log data and custom log data from VMs, GKE environments, and Google Cloud services. Cloud admins can use cloud logging to analyze the selected logs and accelerate the application troubleshooting process.
- **Monitor and improve app performance**: The operation suite helps in reducing cost and latency with its capabilities and services, which helps in running more efficient applications.
- **Health check monitoring**: Cloud Monitoring provides health check monitoring; it also provides endpoint checks to internet access services that run in the cloud, including web applications. Cloud Monitoring enables cloud admins to configure uptime checks related to groups, URLs, or resources such as load balancers and instances.
- **Security management**: The Cloud Audit Logs service of the suite provides security management by offering near-real-time visibility into user activity across the Google Cloud.
- **Log insights**: The error reporting service of the operation suite aggregates and analyzes errors in cloud applications and notifies when new errors are identified.
- **Latency management**: Cloud Trace offers latency management by providing latency sampling and reporting for Google App Engine.
- **Debugging**: The Cloud Debugger service of the suite inspects the status of applications at any code location (in production) without slowing down or interrupting requests while connecting the application production data to the source code.
- **Performance and cost management**: This feature is provided by Cloud Profiler, which continuously profiles resource consumption in production applications. This helps in detecting and eliminating potential performance issues.
- **Service monitoring**: The Service Monitoring feature of the suite offers security telemetry and dashboards to facilitate troubleshooting in various situations via topology and context graphs; moreover, it automates health monitoring via error budget management and SLOs.

hide01.ir

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

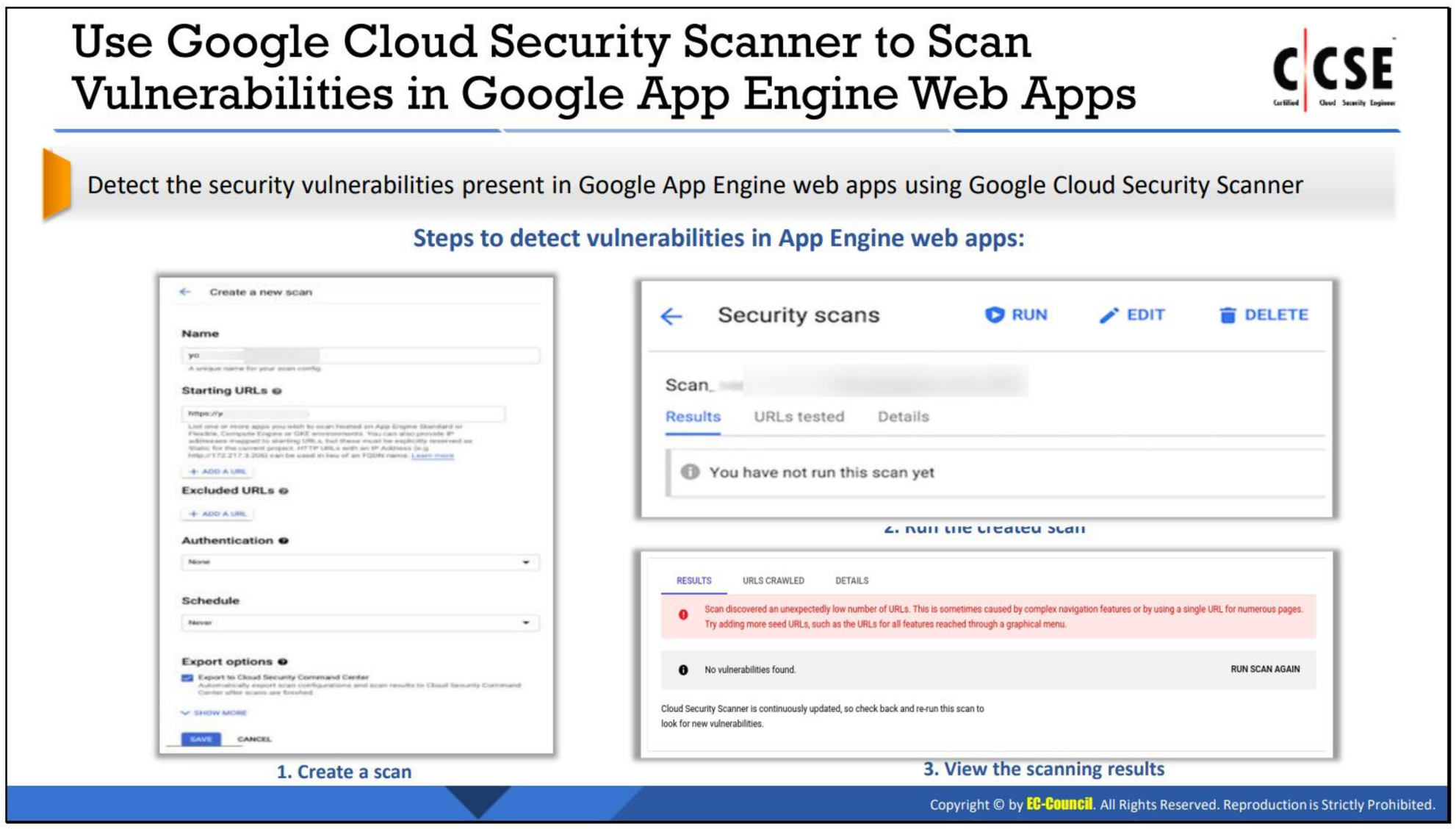


LO#13: Learn How to Implement Security Operations in Google Cloud Platform (GCP)

The objective of this section is to understand the implementation of operational security in GCP using GCP features and services. This section explains how GCP features such as Google Cloud Scanner, VPC Flow Logs, and Google SCC dashboard can be used to secure cloud operations. This section will help cloud security engineers in detecting vulnerabilities, capturing network flow, and analyzing incidents.

hid001.ir

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



Use Google Cloud Security Scanner to Scan Vulnerabilities in Google App Engine Web Apps

Use Google Cloud Security Scanner to detect the security vulnerabilities present in Google App Engine web apps. It complements the existing secure design and development processes to enhance security.

hi0901.ir

Steps to run the scan to identify vulnerabilities

The steps involved in creating and running a scan include:

- Navigate to the GCP Console.
- Select **App Engine** from the navigation menu and click on **Security scans**.

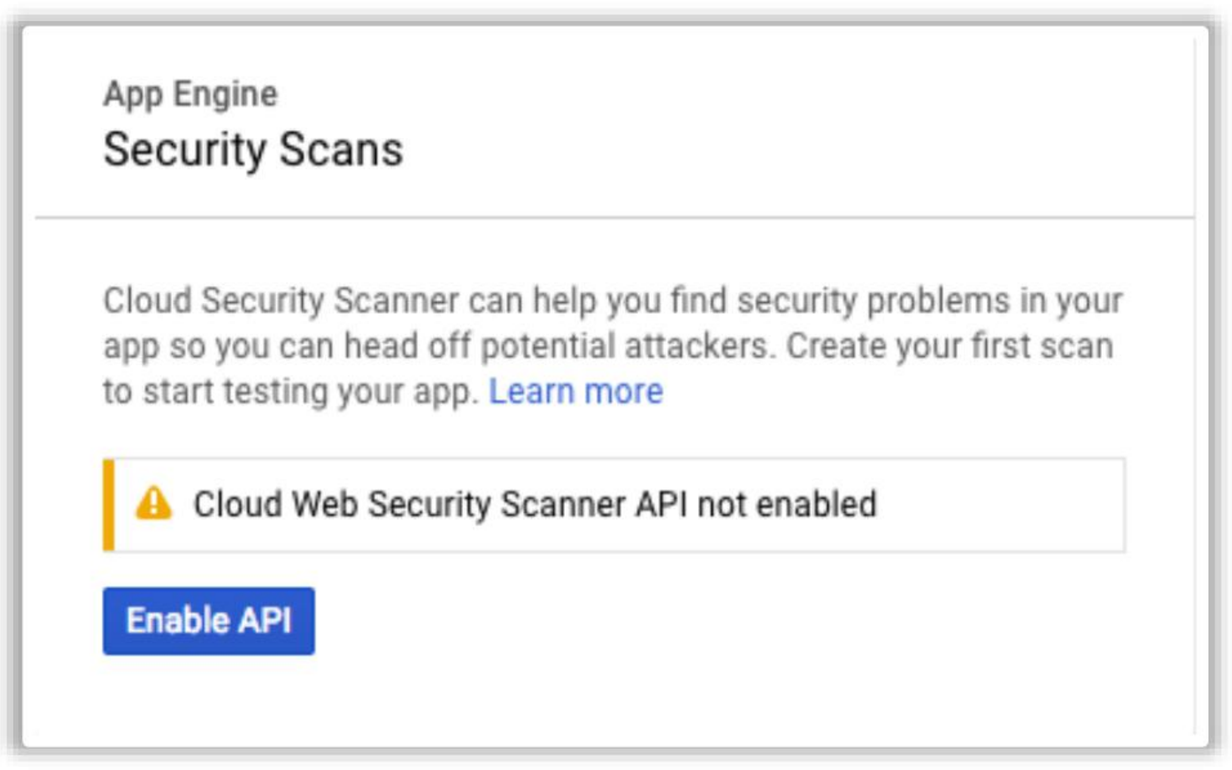


Figure 5.235: Security Scan

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

- Click on **Enable API**, followed by **Create scan**.
- Provide the URL of the application that needs to be scanned under **Starting URLs**. Click on **Save** to create the scan.

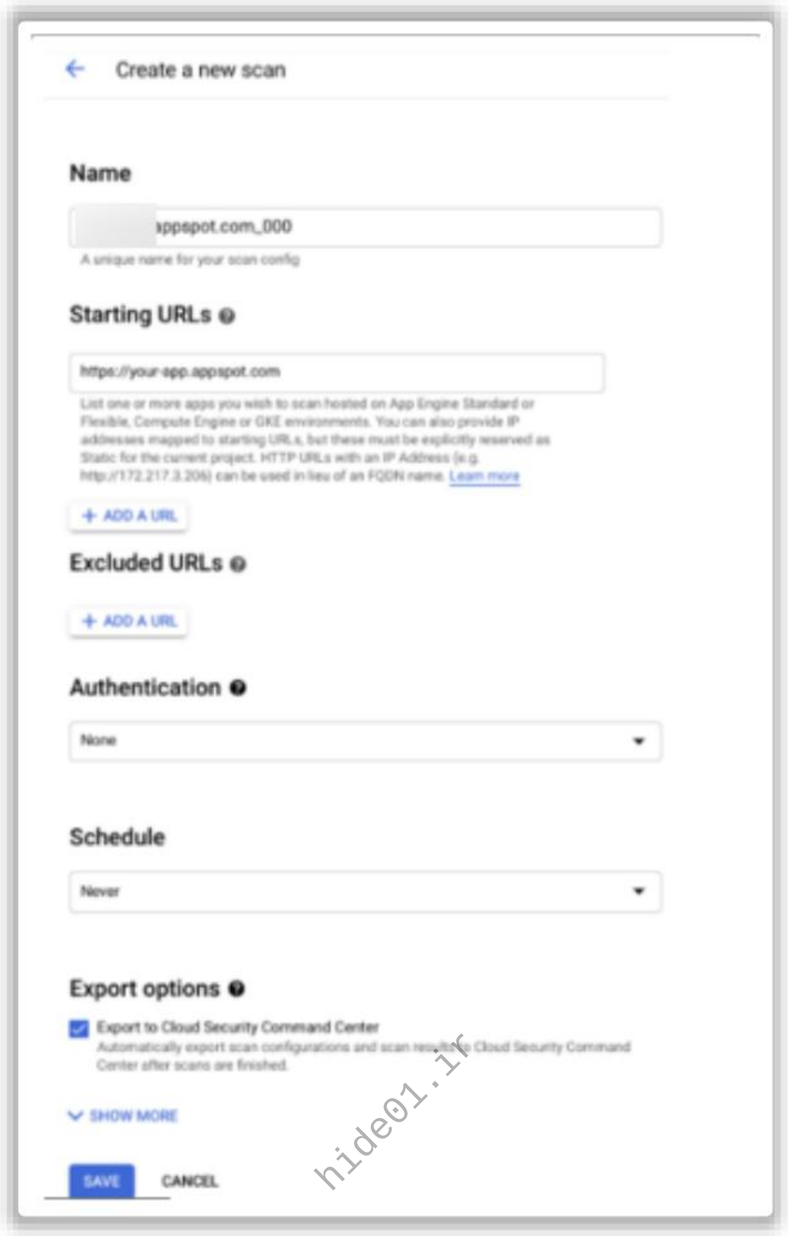


Figure 5.236: Create New Scan

- Start the scan by clicking on **RUN**.

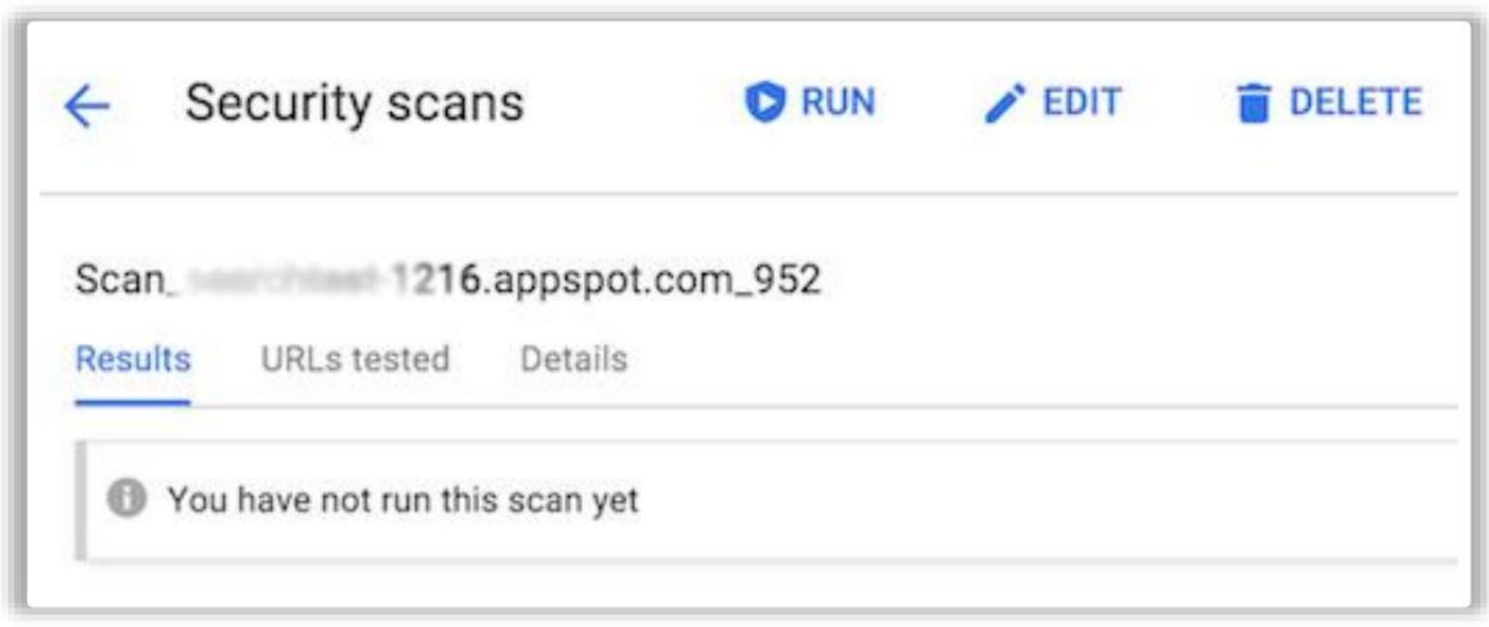


Figure 5.237: Security Scan

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

- Subsequently, the scan is queued and will run after some time. View the progress of the status bar when the scan starts. See the results in the **RESULTS** tab.

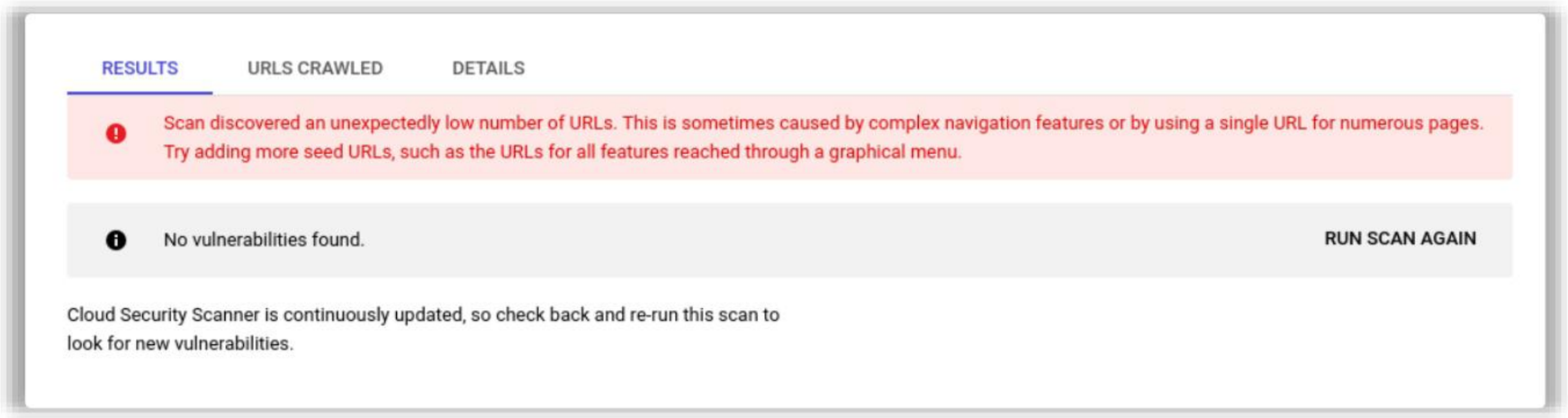
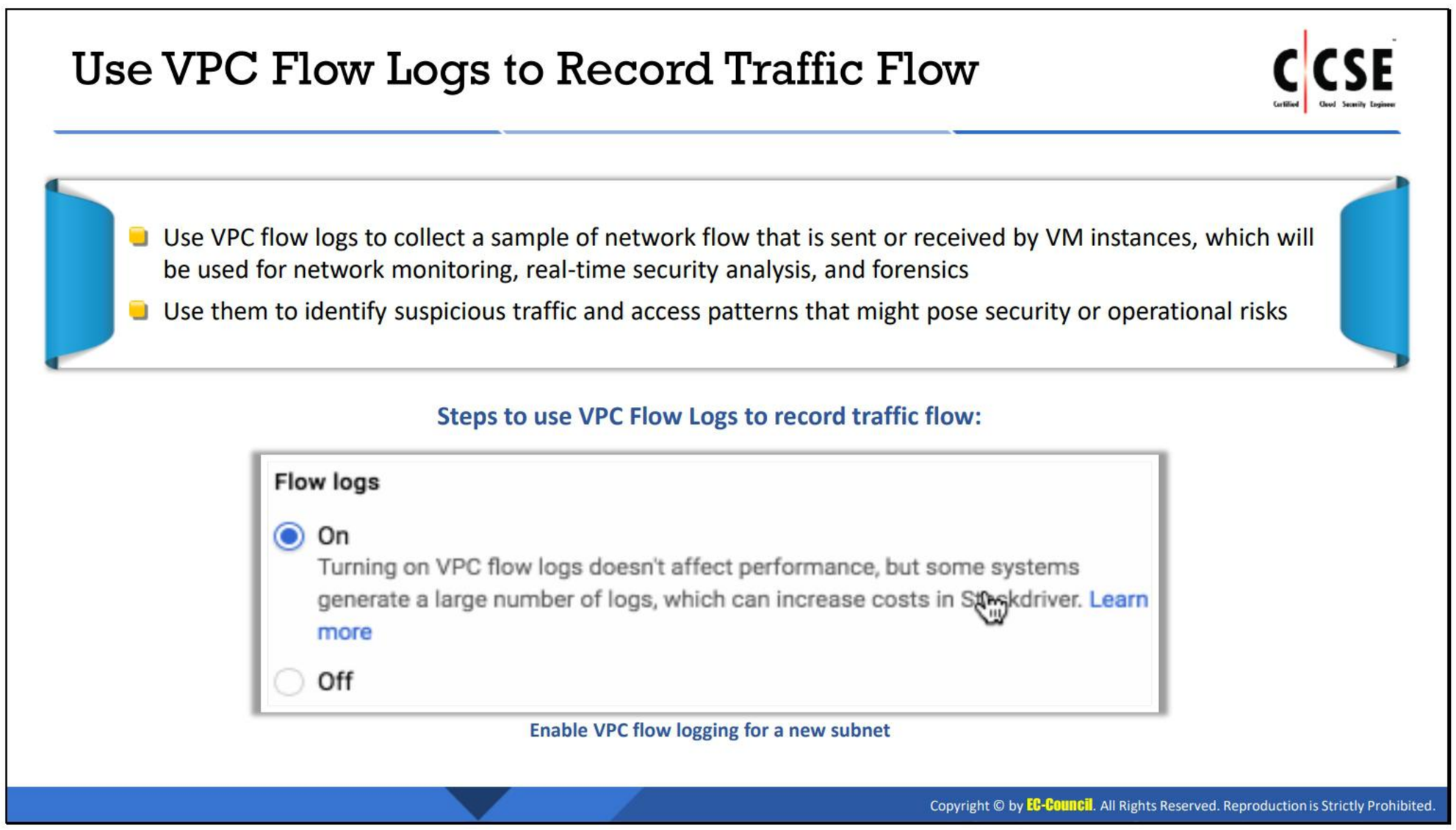


Figure 5.238: Results

hide01.ir

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



Use VPC Flow Logs to Record Traffic Flow

Use VPC Flow Logs to collect a sample of network flow sent or received by VM instances, which will be used for network monitoring, real-time security analysis, and forensics. Use these logs in network logging and monitoring for VMs. Cloud admins can use them to identify suspicious traffic and access patterns that might pose security or operational risks. To use VPC Flow Logs, enable flow logging.

Source: https://console.cloud.google.com

Steps to use VPC Flow Logs to record traffic flow

- **Enable VPC flow logging for a new subnet**
  - On the GC console, go to the **VPC networks** page.
  - Click on the network where the subnet is to be added.
  - Click on **Add subnet** and select **On** under **Flow logs**.

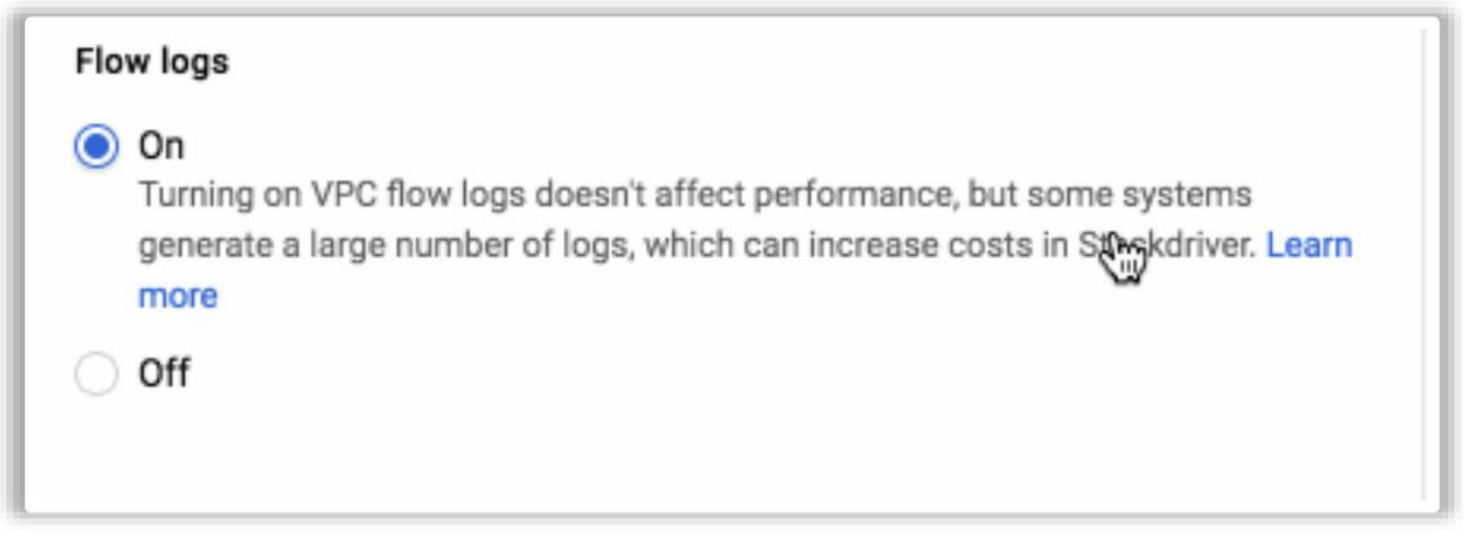


Figure 5.239: Flow Logs

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

- To adjust log sampling and aggregation, choose **Configure logs** and then adjust the following:
  - **Aggregation interval**
  - Inclusion of **metadata**
  - **Sample rate** (it should be set as 100% to include all entries)

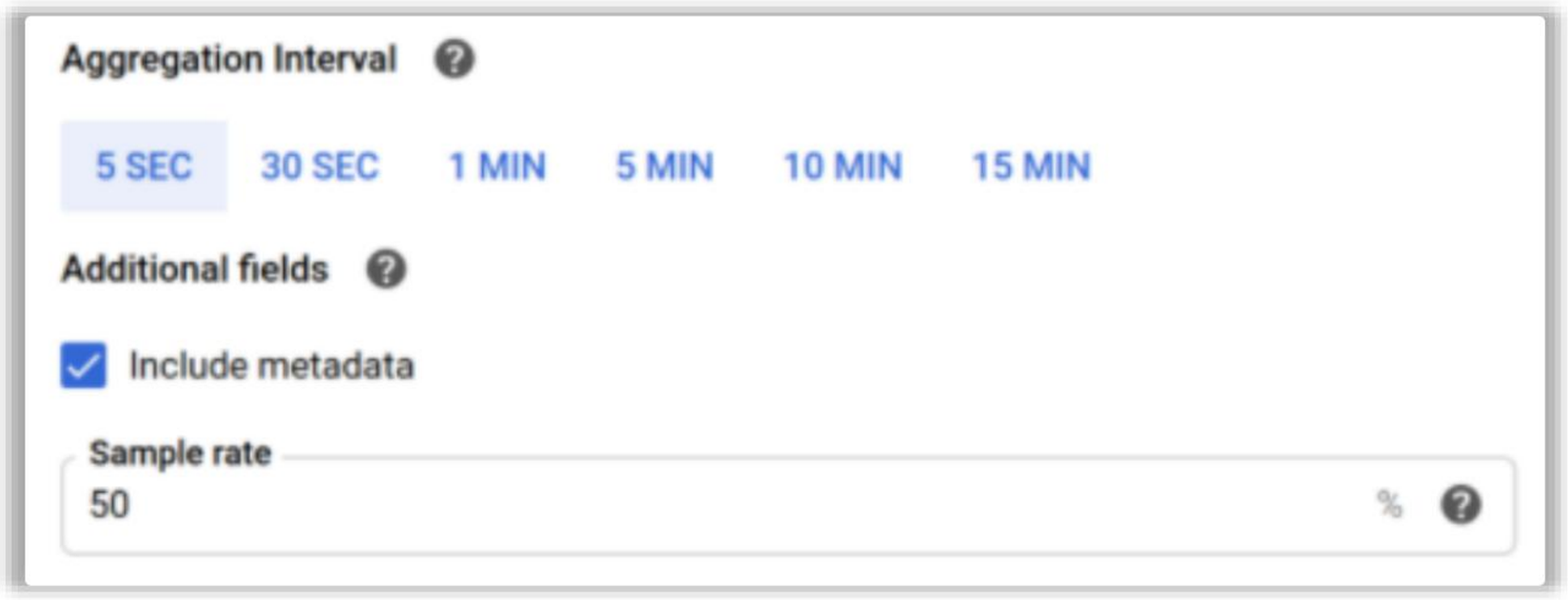


Figure 5.240: Aggregational Interval

- Fill other relevant fields with suitable information and click on **Add**.

- **Turn on VPC flow logging for an available subnet**
  - On the GC console, go to the **VPC networks** page.
  - Choose the subnet that has to be updated and click on **Edit**.
  - Select **On** under **Flow logs**.

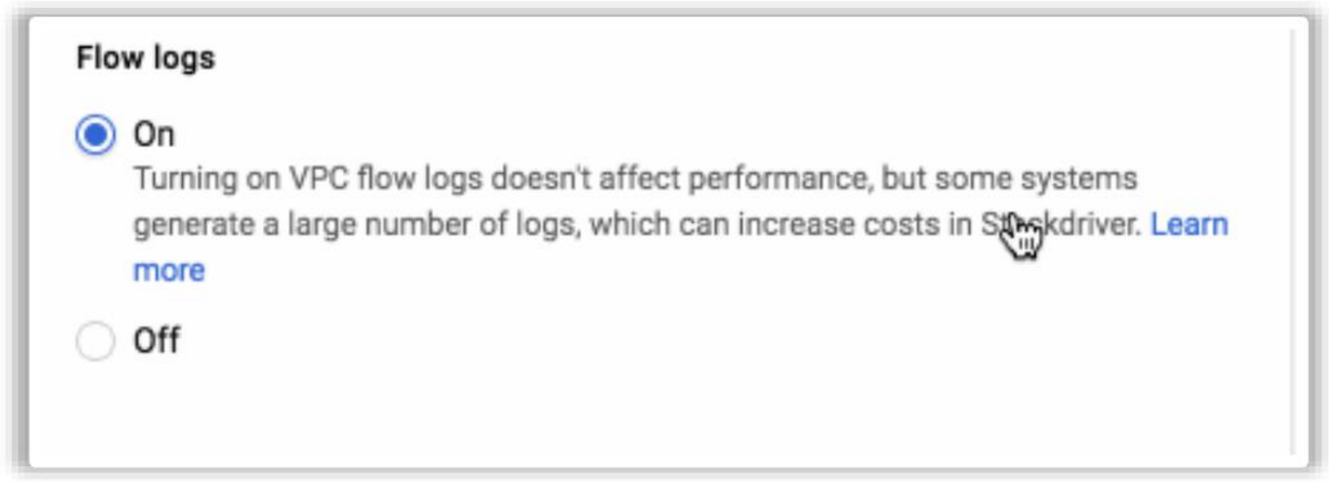


Figure 5.241: Flow Logs

- To adjust log sampling and aggregation, select **Configure logs** and then adjust the following:
  - **Aggregation interval**
  - Inclusion of **metadata**
  - **Sample rate** (it should be set as 100% to include all entries)

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

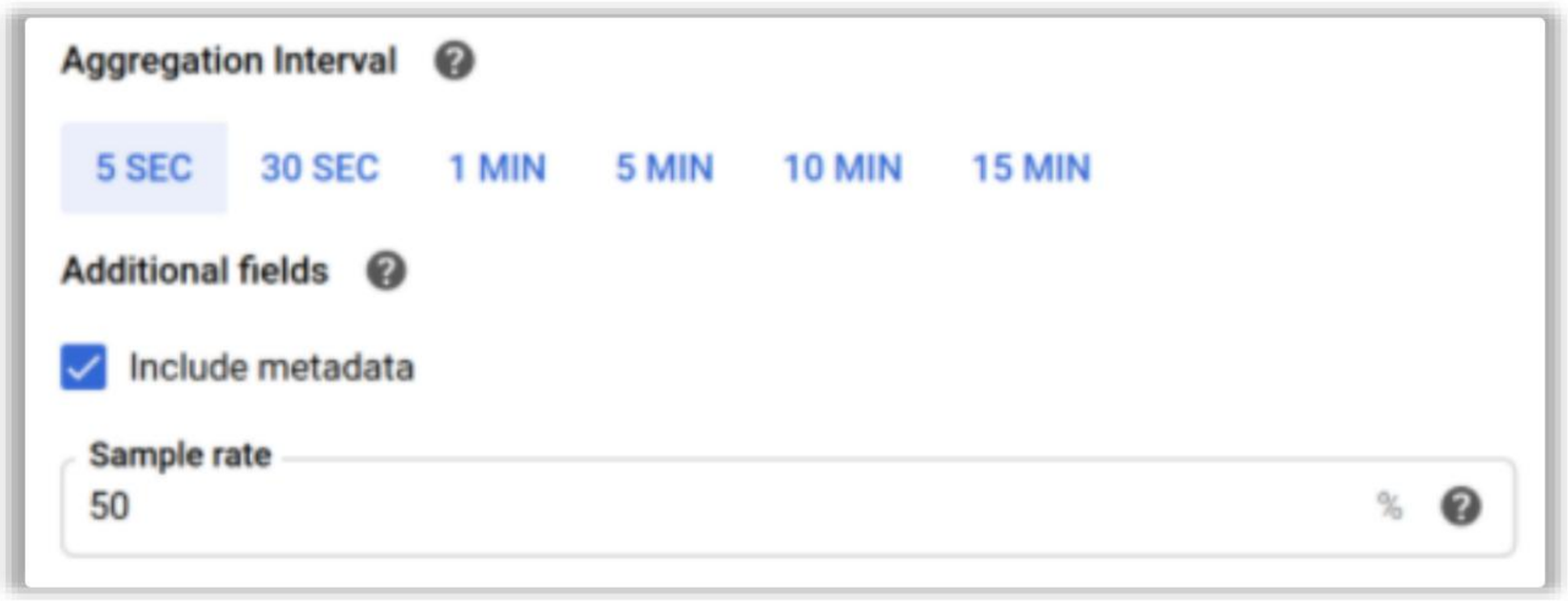
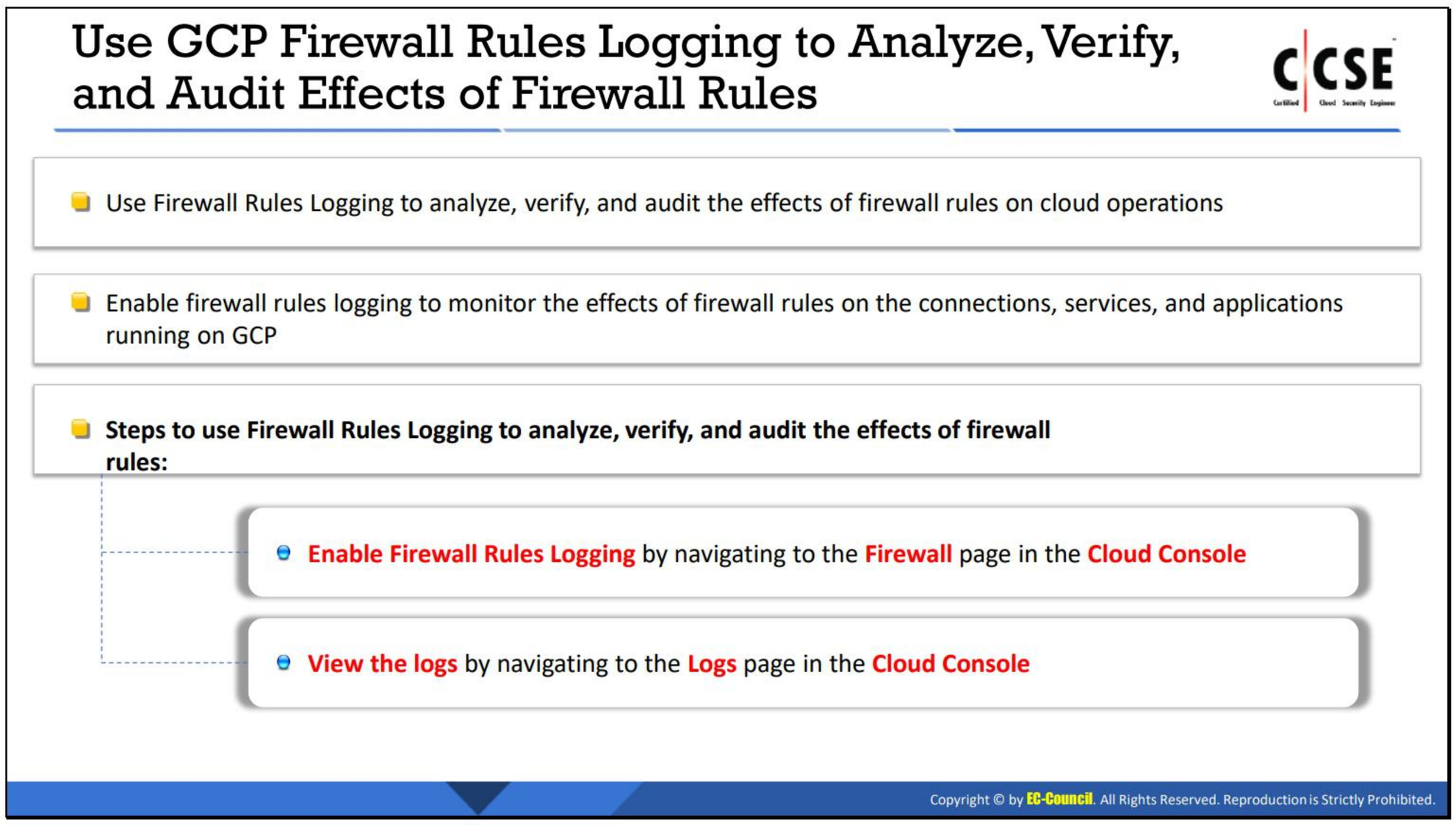


Figure 5.242: Aggregation Interval

- Click on **Add.**

hide01.ir

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



Use GCP Firewall Rules Logging to Analyze, Verify, and Audit Effects of Firewall Rules

Use GCP Firewall Rules Logging to analyze, verify, and audit the effects of firewall rules on cloud operations. Monitor how these rules impact GCP operations and services. Verify whether these rules are working as intended to ensure secure cloud operations. Enable firewall rules logging to monitor the effects of firewall rules on the connections, services, and applications running on the GCP.

Source: https://console.cloud.google.com

Steps to use Firewall Rules Logging to analyze, verify, and audit the effects of firewall rules:

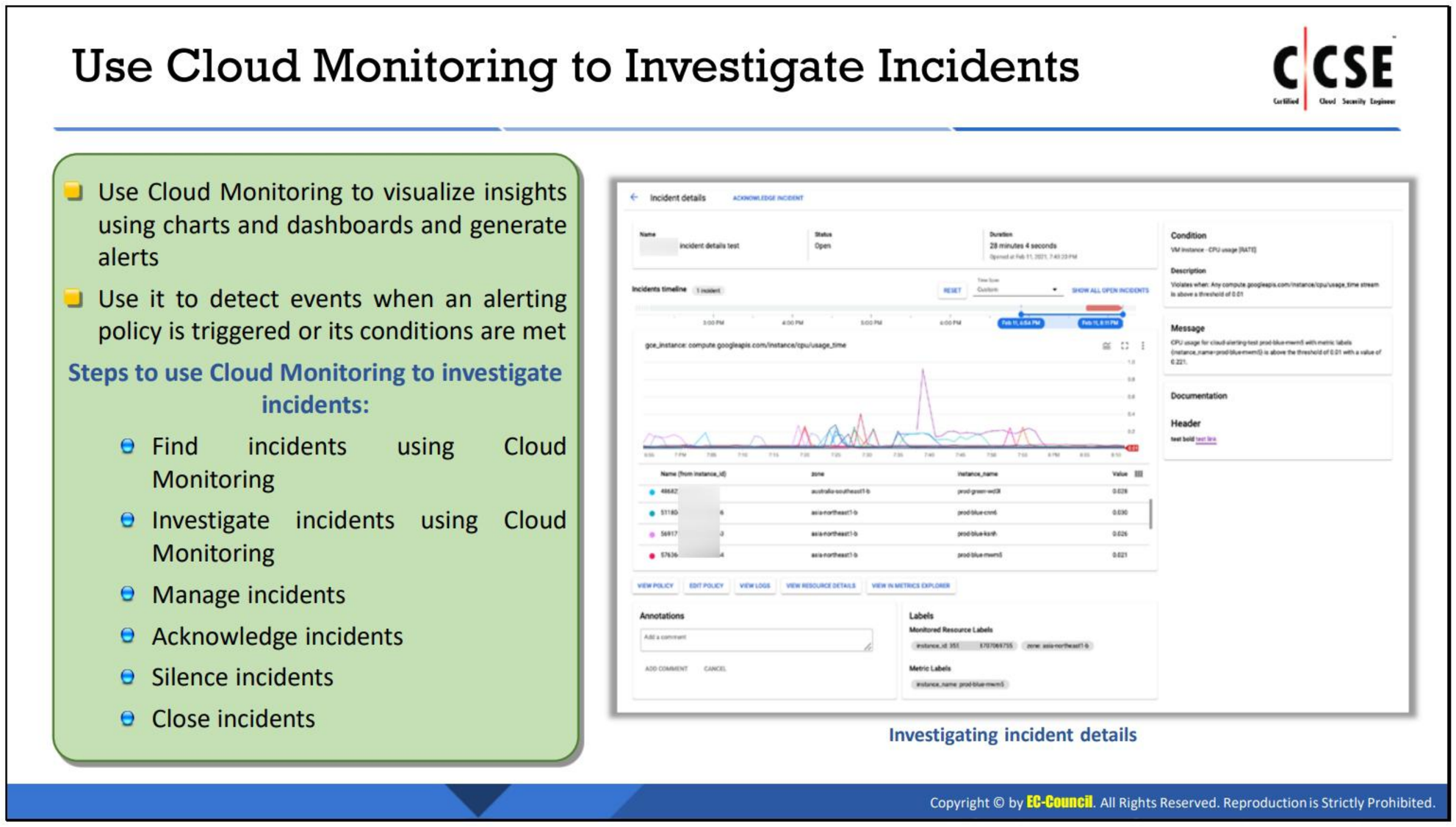
- **Enable Firewall Rules Logging**
  - Navigate to the **Firewall** page in the **Cloud Console**.
  - Check if firewall logging is disabled or enabled for each firewall rule in the **Logs** column.
  - Select the checkbox for the rules in which you want to enable logging.
  - Choose **Configure logs** in the **Firewall rules** page.
  - Select **On** in the **Configure logs** window.
  - To remove metadata fields, clear **include metadata** after expanding the **Logs details**.
  - Now, click on **Save configuration**.
- **View the logs**

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

- In the **Cloud Console**, go to the **Logs** page.
- Click on **Subnetwork** from the first pull-down menu.
- From the second pull down menu, choose **compute.googleapis.com/firewall**.
- Click on **OK.**

hide01.ir

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



Use Cloud Monitoring to Investigate Incidents

Use Cloud Monitoring to visualize insights using charts and dashboards and generate alerts; it can be used to detect events when an alerting policy is triggered or its conditions are met.

Source: https://console.cloud.google.com

Steps to use Cloud Monitoring to investigate incidents

- **Find incidents using Cloud Monitoring**
  - Select **Navigation Menu** in the **Cloud Console** toolbar and click on **Monitoring**.
  - Click on **Alerting** in the **Monitoring navigation** pane. The alerting dashboard page consists of all open incidents in the **Summary** pane; the most recent incidents are displayed in the **Incidents** table.
- **Investigate incidents using Cloud Monitoring**

  Investigate an incident after determining its details from the **Incident details** page. Click on incident summary (to view incident details) in the table of incidents on the **Incidents** or **Alerting** page.

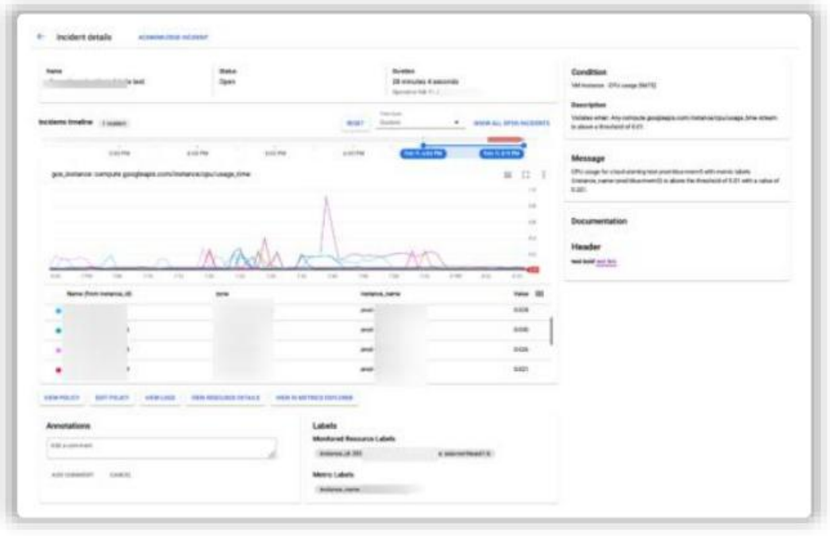


Figure 5.243: Incident Details

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

The **Incident details** page displays labels, status information, information about alerting policies that created the incident, annotations, and tools for investigation.

- **Manage incidents**

  Incidents can be categorized into three states:

  - **Open**: Incidents are in Open state when the policy conditions are satisfied or no data are available to show that the condition is no longer satisfied.
  - **Acknowledged**: It shows that incidents are open and manually marked as acknowledged. Usually, this indicates that the incident is under investigation.
  - **Closed**: It indicates that the policy condition is no longer satisfied or has not been satisfied for the past seven days.

- **Acknowledge incidents**

  To acknowledge an incident, ensure the following:

  - On the **Alerting** dashboard, click on **See all incidents** in the **Incidents** pane; the **Incidents** window will appear.
  - On the incident that must be marked as acknowledged, click on **More options**, followed by **Acknowledge**.
  - Similarly, the incident can be acknowledged by going to the **Incident details** page and clicking on **Acknowledge incident**.

hide01.ir

- **Silencing incidents**

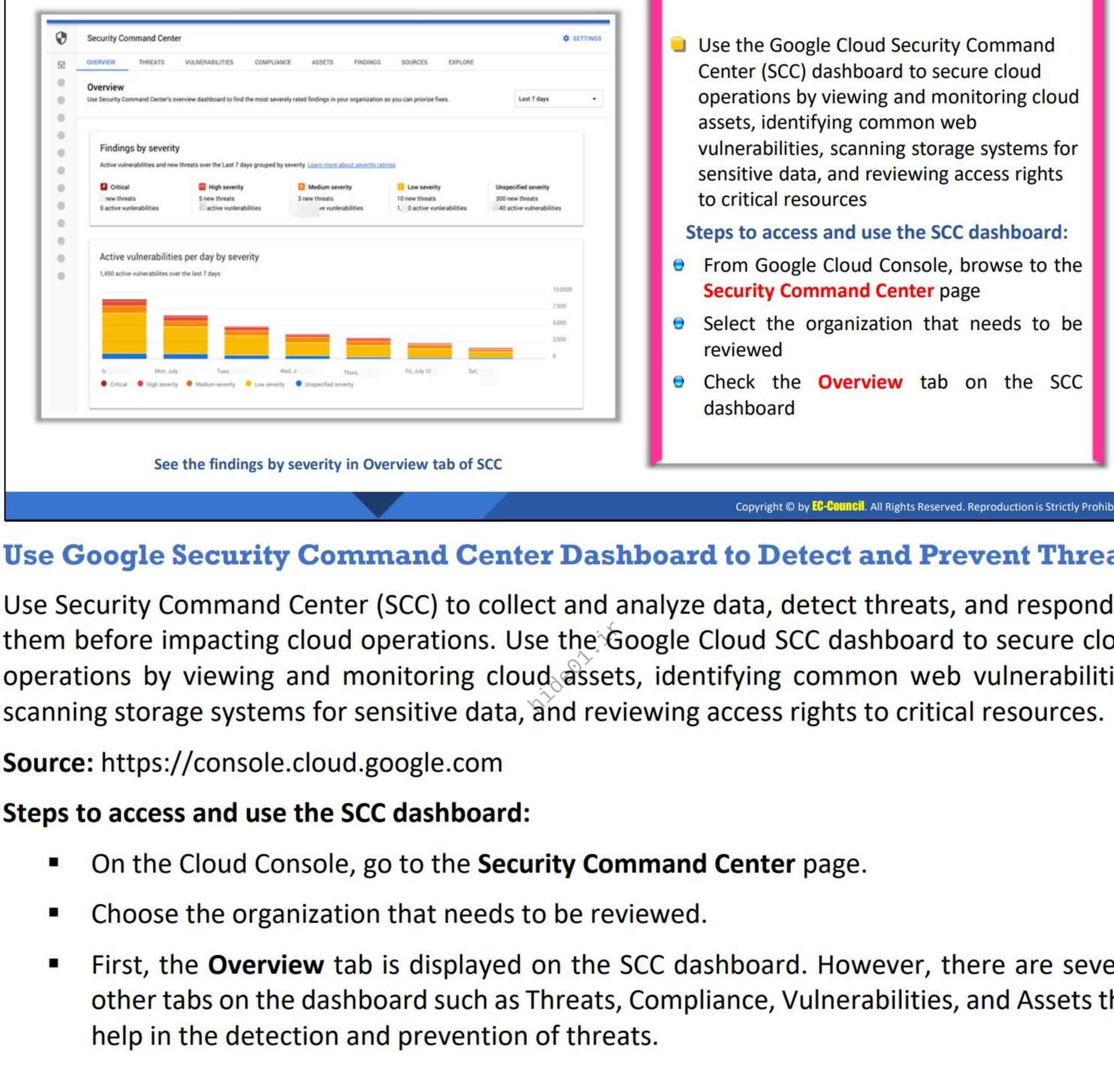
  Incidents can be silenced by silencing a condition. When a condition is silenced, all associated incidents will be silenced and no alert will be generated for that incident. An incident can be silenced by the following:

  - On the **Alerting** dashboard, select **See all incidents** in the **Incidents** pane**.** The **Incidents** window will appear.
  - On the incident that needs to be marked as silenced, click on **More options** and select **Silence associated condition.**

- **Close incidents**

  An incident is automatically closed when the policy condition is no longer satisfied or has not been satisfied for seven days.

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



Use Google Security Command Center Dashboard to Detect and Prevent Threats

Use Security Command Center (SCC) to collect and analyze data, detect threats, and respond to them before impacting cloud operations. Use the Google Cloud SCC dashboard to secure cloud operations by viewing and monitoring cloud assets, identifying common web vulnerabilities, scanning storage systems for sensitive data, and reviewing access rights to critical resources.

Source: https://console.cloud.google.com

Steps to access and use the SCC dashboard:

- On the Cloud Console, go to the **Security Command Center** page.
- Choose the organization that needs to be reviewed.
- First, the **Overview** tab is displayed on the SCC dashboard. However, there are several other tabs on the dashboard such as Threats, Compliance, Vulnerabilities, and Assets that help in the detection and prevention of threats.

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

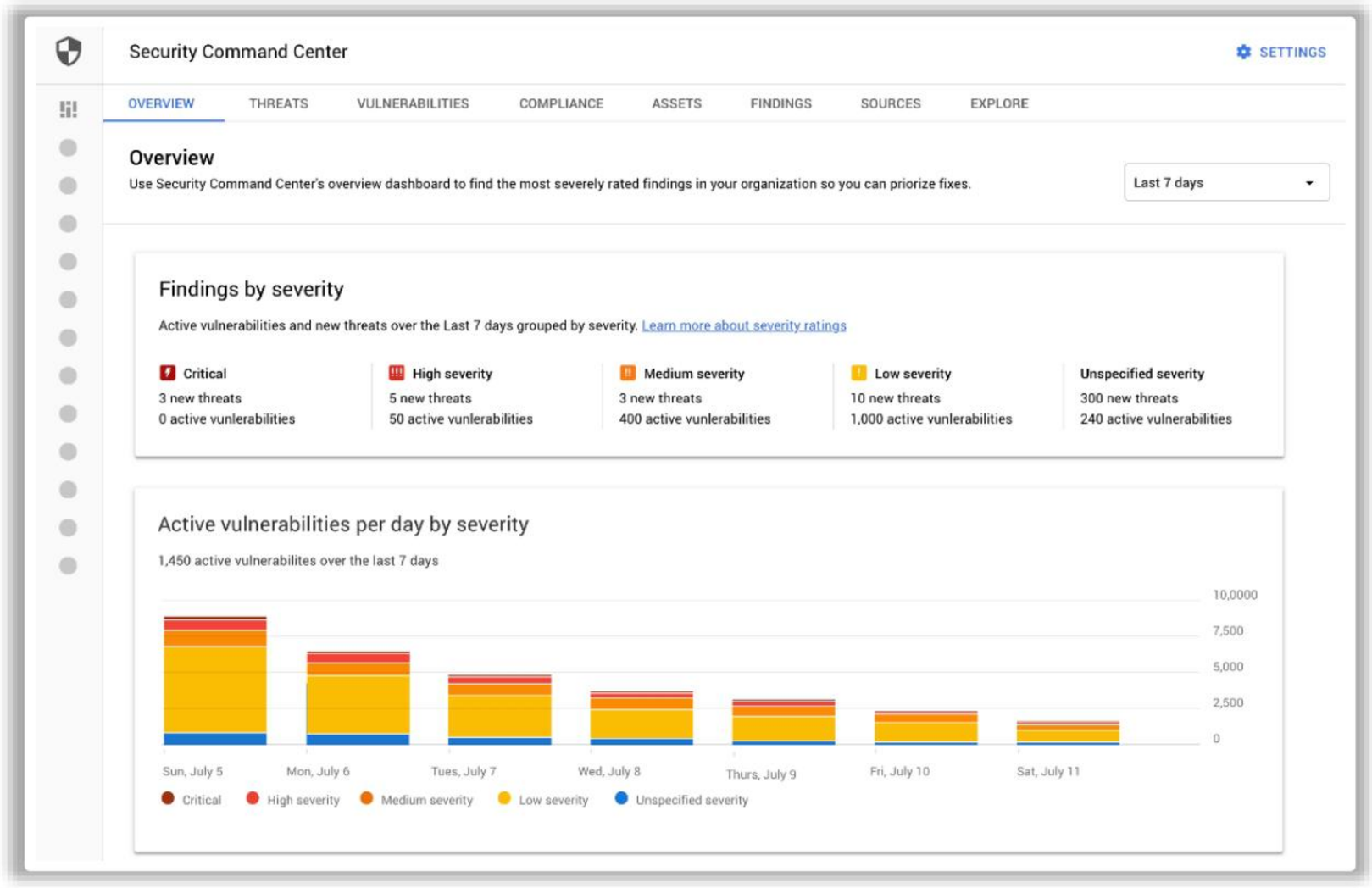


Figure 5.244: Security Command Center

hide01.ir

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

Module Summary

In this module, the concepts of cloud operation security; elements involved in the physical/logical operations of cloud data centers; how to build, implement, operate, and manage physical and logical infrastructures; implementation of operations controls and standards; Azure operation security and the implementation of operational security in Azure; AWS operation security and the implementation of operational security in AWS; and GCP operation security and the implementation of operational security in Google Cloud were discussed in detail. Owing to this module, cloud security engineers can effectively implement operation security in their organization.

The key points discussed in this module are stated below:

- Cloud operation security involves the identification, investigation, and mitigation of cybersecurity threats in cloud operations using various tools, processes, and features.
- Cloud data centers should be resilient to all threats, including cyberattacks and natural disasters, to provide continuous system operation and access to data (uptime).
- To securely manage the physical and logical infrastructures of cloud, organizations must implement important security measures such as patch management, hardware monitoring, network security controls, performance and capacity monitoring, and access controls for remote access.
- To manage cloud security operations, organizations should take necessary measures, including managing communication with relevant parties, monitoring security controls, and enforcing standards for operational controls.

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

- Microsoft Azure provides operational security to Azure customers through Azure Security Center, Azure Monitor, and Azure Network Watcher.
- AWS provides operational security to AWS customers through services such as AWS System Manager OpsCenter, Systems Manager Explorer, CloudWatch, and CloudTrail.
- Google Cloud provides operational security to its consumers by offering services such as Security Command Center (SCC), Security Analytics and Operations, and Cloud Monitoring.

hide01.ir

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