EC-Council

C|CSE™

Certified Cloud Security Engineer



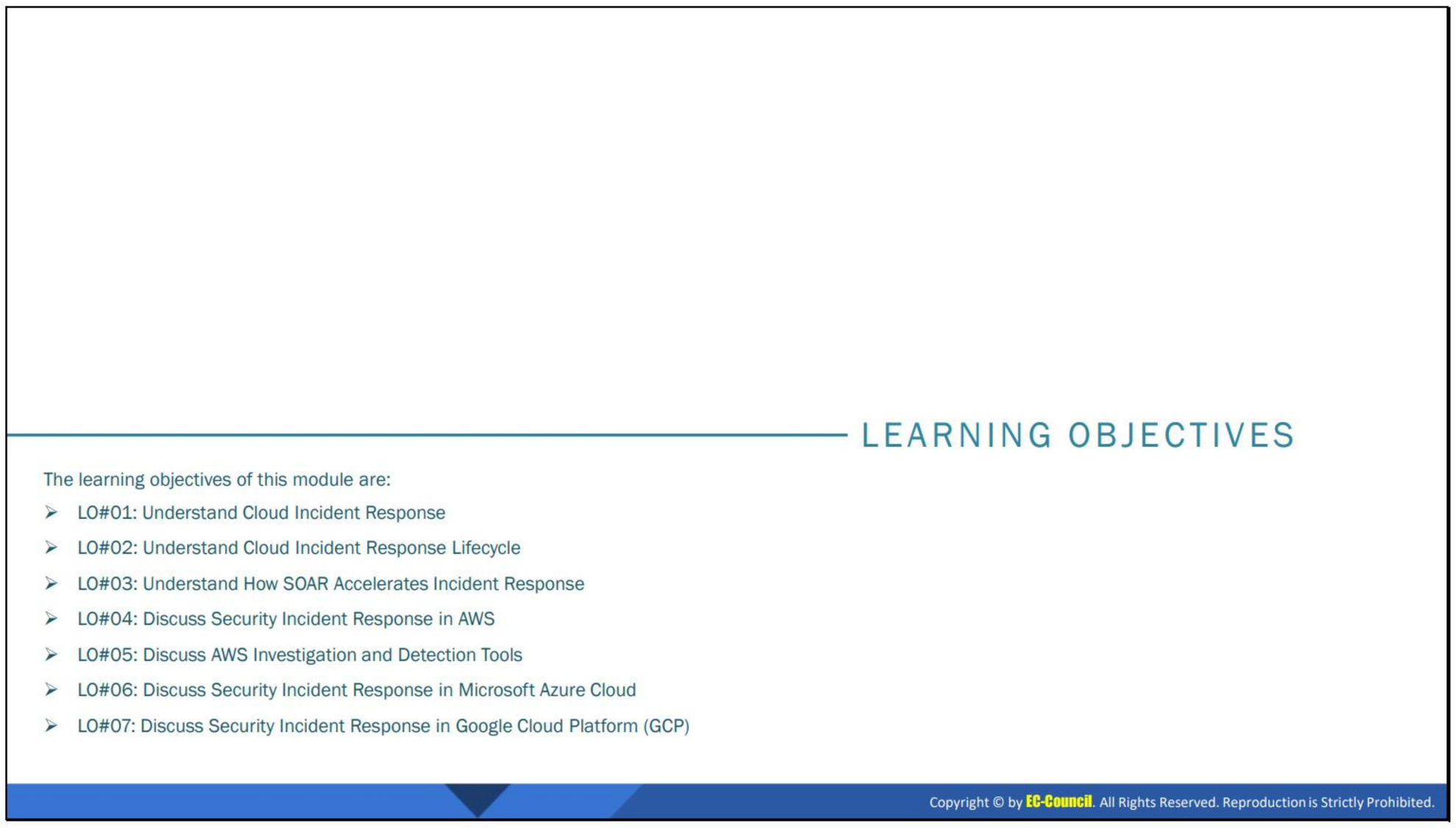
hide01.ir

Incident Response in Cloud

Module 07

This page is intentionally left blank.

hide01.ir

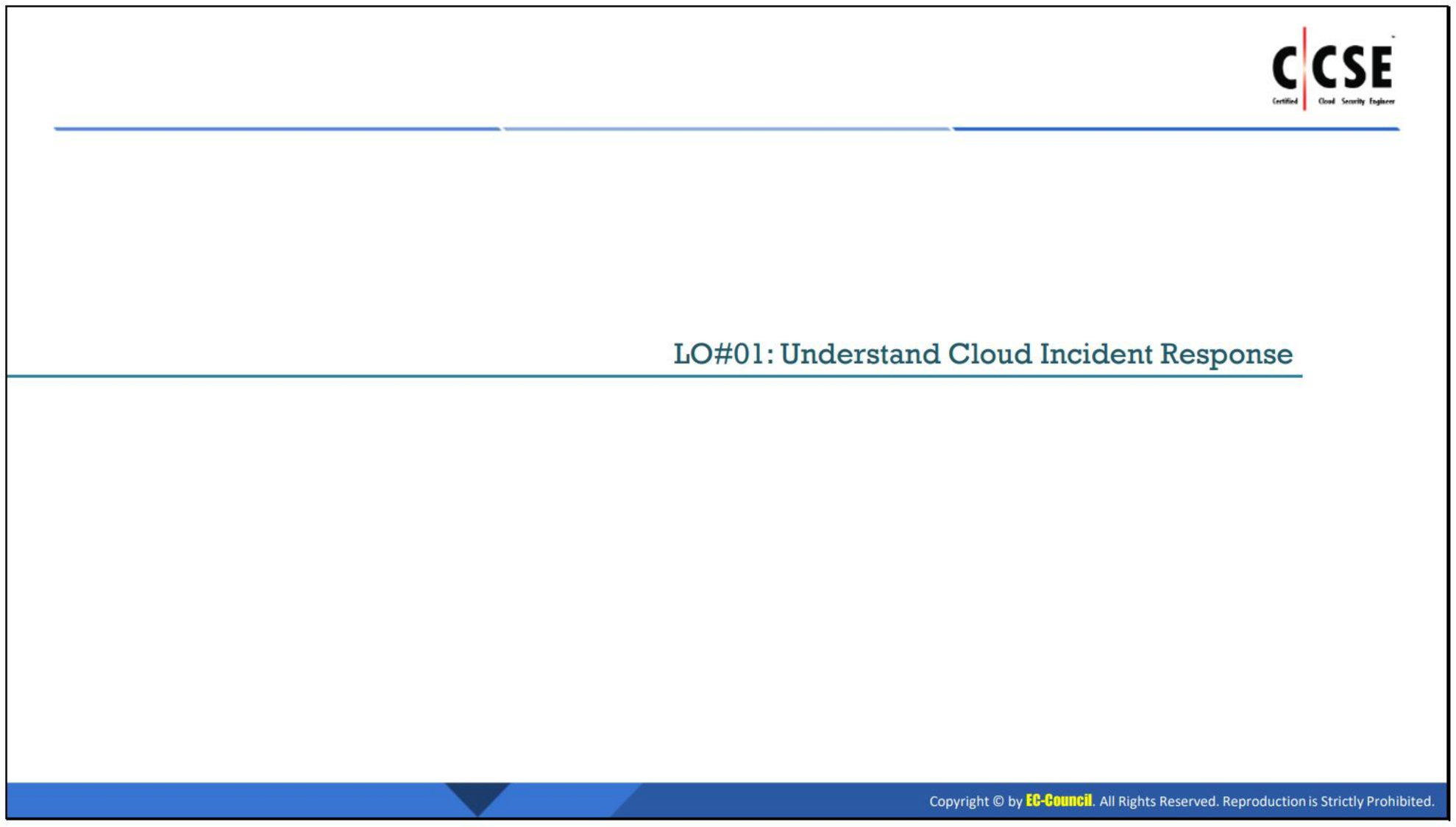


Learning Objectives

Preventive security controls cannot guarantee a complete protection against attacks. Gaining visibility into the various services hosted on the cloud and identifying and responding to the possible security issues in advance is a major concern. A proper incident response plan which helps in investigating attacks along with governance and forensic investigation can help an organization secure their cloud services. This module focuses on the various aspects of incident detection and response in the cloud. It explains the incident response characteristics specific to the cloud environment. It helps security professional to understand the phases of incident response in the cloud. Additionally, it highlights the various recommendations for both the user and the service provider in each phase of the incident response lifecycle. They can understand how implementing security orchestration, automation, and response (SOAR) tools accelerates incident response. This module explains the incident detection and response process and tools in AWS, Microsoft Azure, and GCP cloud. The learning objectives of this module are as follows.

- Understand cloud incident response
- Understand the cloud incident response lifecycle
- Understand How SOAR accelerates incident response
- Discuss security incident response in AWS
- AWS investigation and detection tools
- Discuss security incident response in Microsoft Azure Cloud
- Discuss security incident response in Google Cloud Platform (GCP)

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

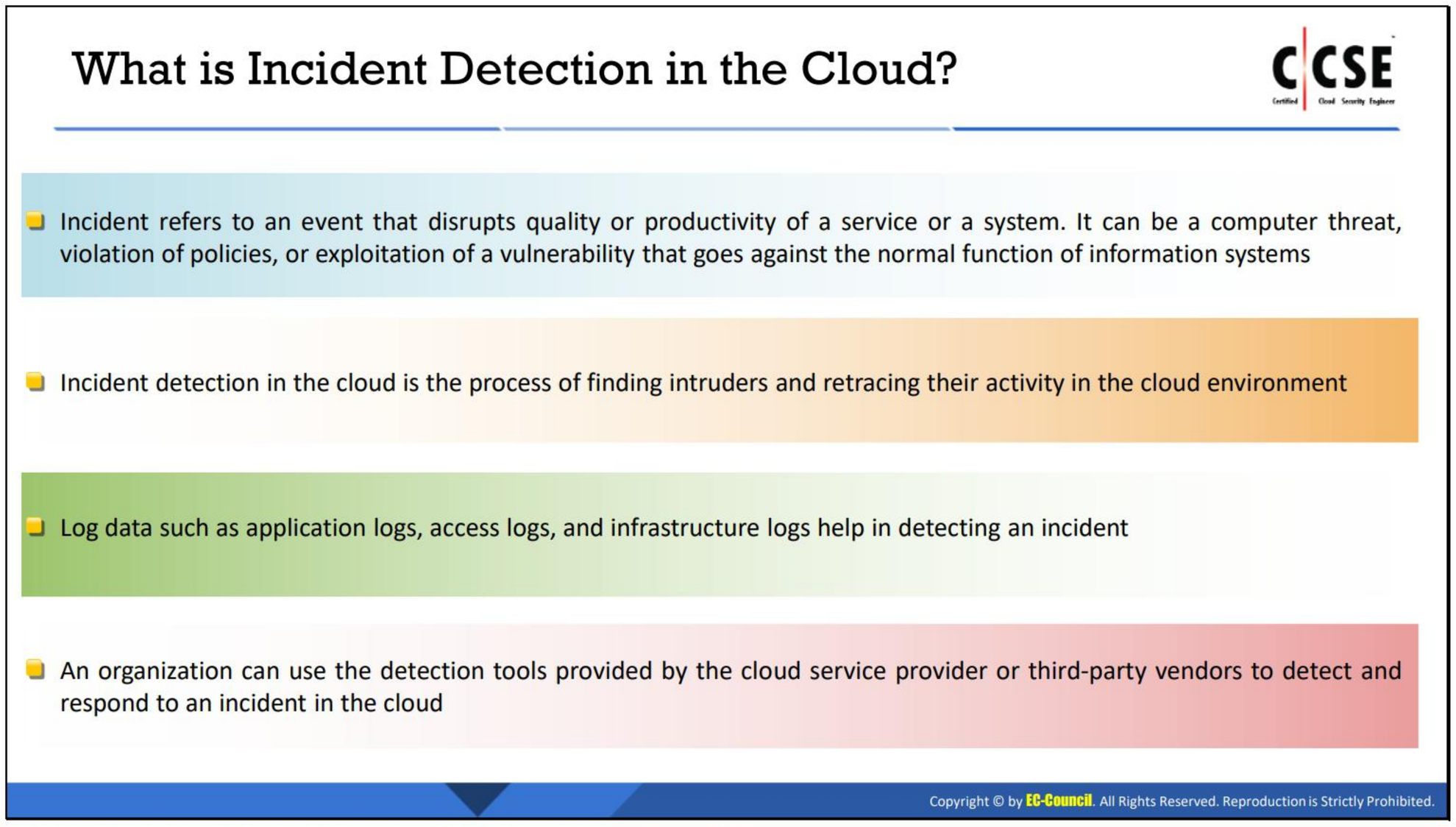


LO#01: Understand Cloud Incident Response

The objective of this sections is to explain incident detection and response in cloud and the importance of cloud incident response (CIR). You can understand the requirements of incident response specific to the cloud environment.

hide01.ir

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



What is Incident Detection in the Cloud?

Owing to the numerous benefits of cloud computing, many organizations are moving their workloads to the cloud. Because various organizations deploy their sensitive data and workloads on the cloud, attackers extensively target the cloud environment. Cloud-specific security problems have been increasing because of multi-tenancy, shared resources, third-party hosting, access from any place, etc. The recommendations, standards, and laws are not enough to secure a cloud environment. The cloud-specific security issues have not been addressed because of the frequent changes in the cloud infrastructure.

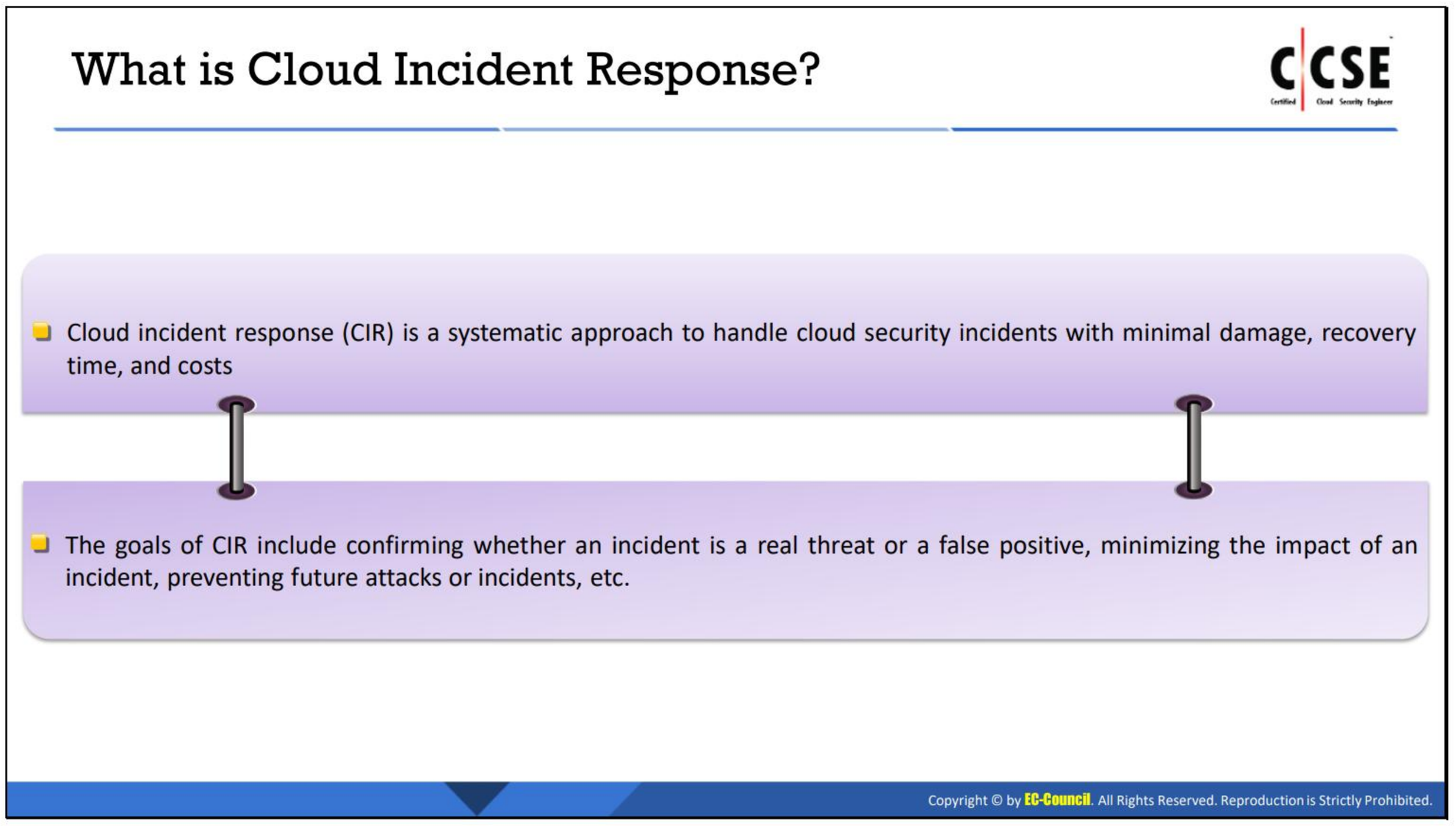
Incident detection in the cloud is a process of findings intruders and retracing their activity in the cloud environment. By detecting intruders, security analysts can safeguard their organization.

Incident detection plays a significant role in the cloud environment because sensitive data stored in the cloud environment can be accessed by insecure and unmanaged services, unauthorized access to data by other cloud tenants/outsiders, data breach by the cloud service provider, lack of visibility on data that is processed in the public cloud, the intrusion of malware from other cloud tenants, etc. It is possible to mitigate attacks and protect an organization by detecting various threats in the cloud environment.

Incident detection in the cloud is challenging, as the security professional needs to provide evidence that something is wrong. It requires highly skilled personnel, processes, and tools. Because of the increased threat landscape with public and regulatory scrutiny of companies, an organization cannot overlook incident detection.

Log data such as application logs, access logs, and infrastructure logs help in detecting an incident. For detecting an incident in a cloud environment, it is necessary to employ an automated technique. An organization can use the detection tools provided by the cloud service provider or third-party vendors to detect and respond to an incident in the cloud.

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



What is Cloud Incident Response?

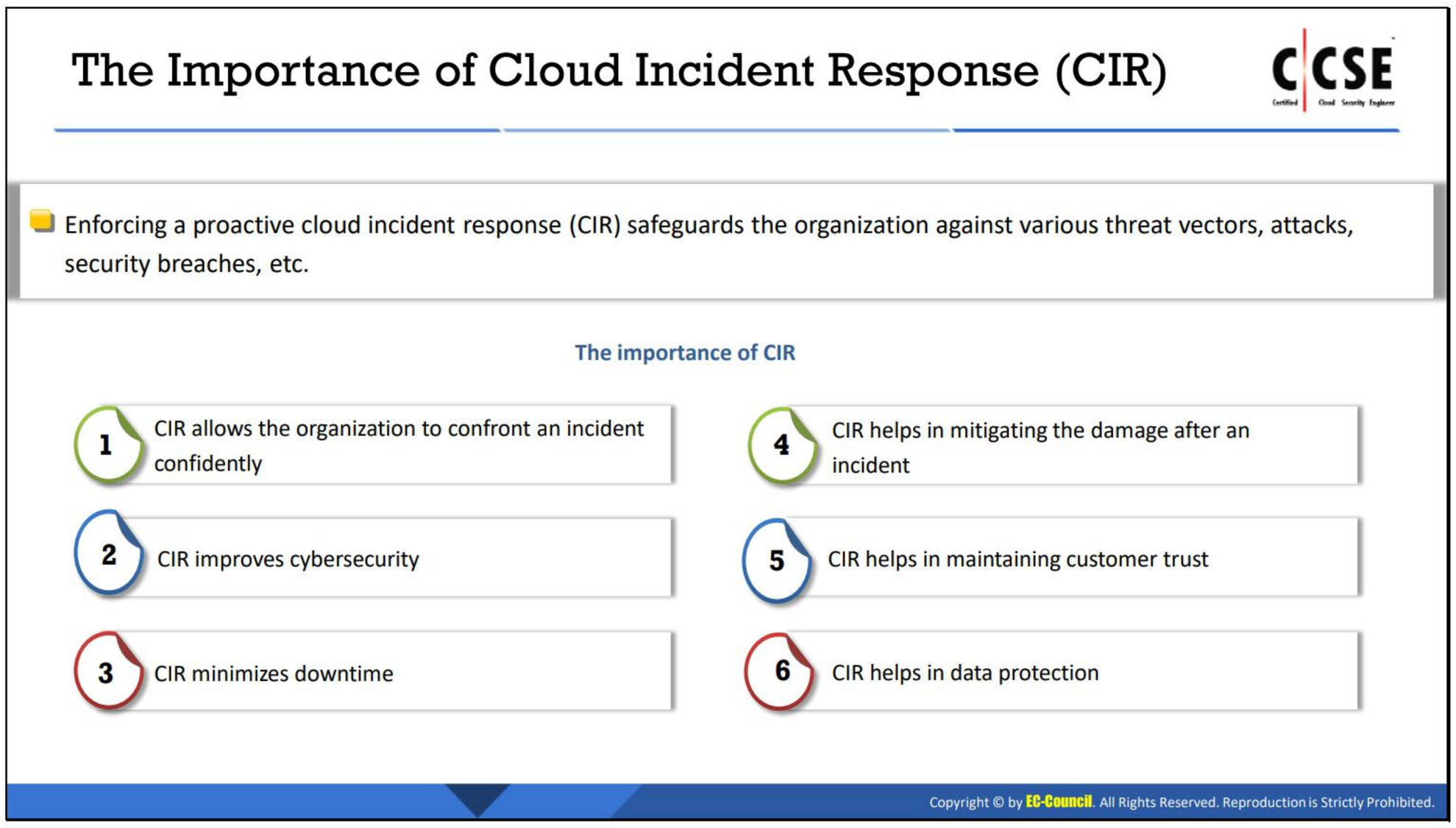
An incident is defined as an unplanned interruption or decline in the quality of a service. Cloud incident response (CIR) is a systematic approach to handle cloud security incidents with minimal damage, recovery time, and costs. When responding to an incident, information such as which network vulnerability led to the attack, who initiated the attack, and the types of affected devices and files can be known. To safeguard against security and business risks and mitigate cost-intensive downtime, every organization should have a robust incident response process. Traditional IT service management depends on various platforms and applications for monitoring, tracking, and alerting the relevant teams about various incidents. The security team must respond quickly and accurately to an incident because it can affect the entire organization's performance, security, and downtime.

The threat actors are fully aware that the sensitive data could be duplicated to an unsupervised or poorly protected cloud environment. An attacker uses cloud environments as a point of entry to harm, infect, exploit, and disrupt a business. Since the cloud environments are completely different, the cloud incident responses should also be different.

CIR combines DevOps functions such as transparency, collaboration, and rapid deployment for efficient and streamlined incident response systems. These incident response systems consist of monitoring, communication, documentation, and alerting subsystems. Consequently, the CIR teams can easily collaborate, track processes, and automate important security tasks.

The goals of CIR include confirming whether an incident is a real threat or a false positive, maintaining or restoring business continuity, minimizing the impact of an incident, analyzing the cause of an incident, preventing future attacks or incidents, and enhancing security and incident response.

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



The Importance of Cloud Incident Response (CIR)

Enforcing a proactive CIR safeguards the organization against various threat vectors, attacks, security breaches, etc. The importance of CIR is explained below.

CIR Allows the Organization to Confront an Incident Confidently: A robust CIR will alleviate fear among employees, stakeholders, and security teams at the time of an incident. In the absence of a proactive CIR, the organization's condition will worsen during an incident. Thus, organizations can confront an incident confidently if they have a robust CIR with clear and coherent post-incident instructions, incident response management guidelines, and assignment of responsibilities.

CIR Helps in Mitigating the Damage After an Incident: A cybersecurity attack on a cloud customer or cloud service provider can lead to financial loss, operational disruption, business crises, legal implications, and a loss of trust. A robust CIR will help in quickly understanding the nature of an attack, where and how the attack has occurred, the associated risks, etc., which will help the security team in promptly applying any mitigation and remediation steps. It saves time and effort, which is otherwise wasted in addressing an encountered incident. Thus, CIR can help in minimizing and limiting the impact of an attack.

CIR Improves Cybersecurity: With the help of CIR, an organization can implement certain best practices for securing its network. This will help the organization in detecting the weaknesses and vulnerabilities in their network and the current cybersecurity strategies along with developing new remedies to enhance their entire cybersecurity posture.

CIR Helps in Maintaining Customer Trust: A cybersecurity attack on the cloud environment of an organization can have a significant impact on their business relations with customers, investors, and partners. In case the organization fails to appropriately communicate the

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

incident to its stakeholders, it would lose customer trust and brand reputation. Thus, a CIR plan can help an organization maintain customer trust by assuring the stakeholders that it is proactively prepared for any type of incident.

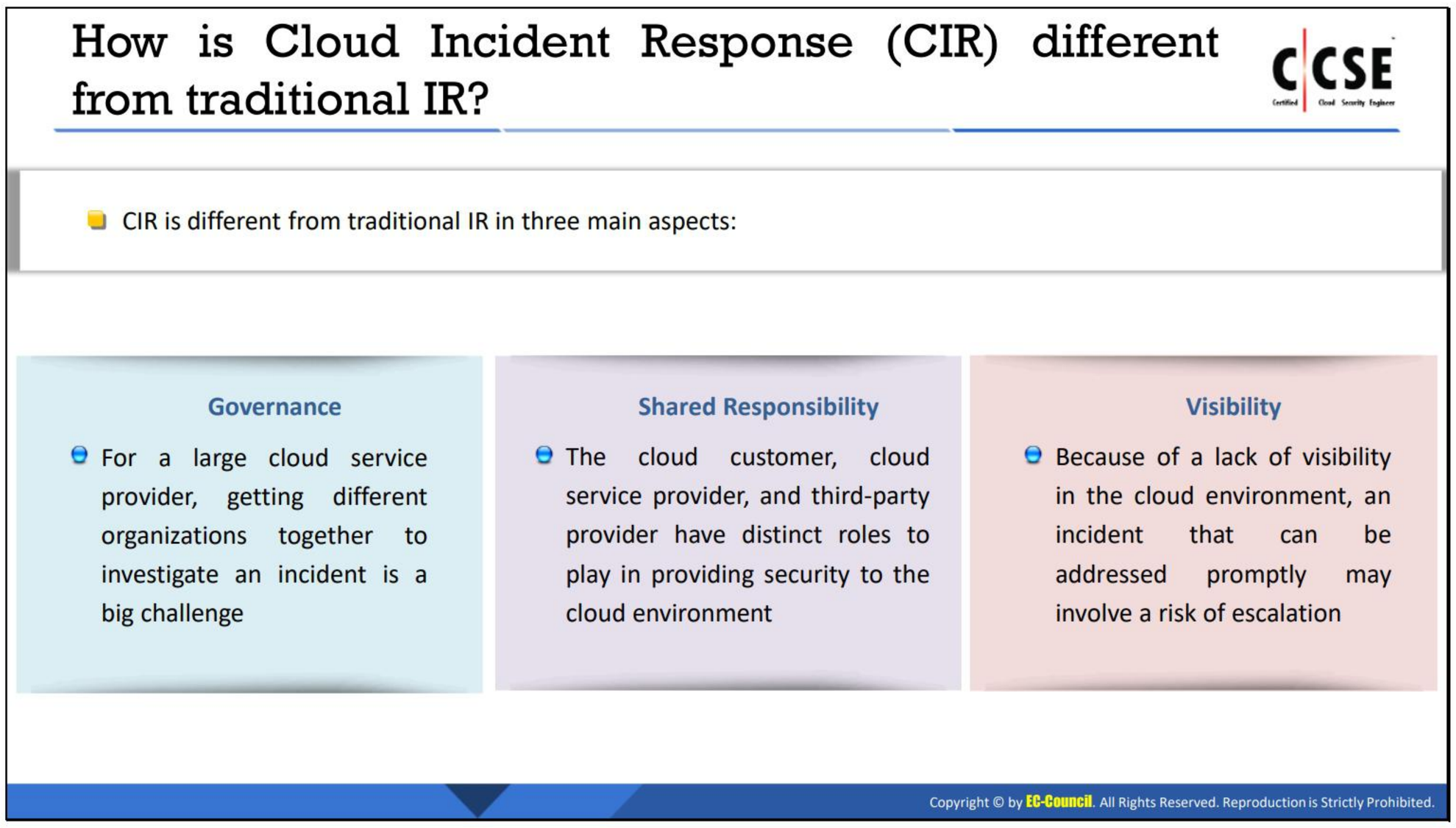
CIR Minimizes Downtime: CIR can significantly minimize the downtime of an organization.

CIR Helps in Data Protection: By implementing CIR, the security team can proactively protect the data. A robust CIR protects the data against a ransomware attack or data leak. The CIR team safeguards the data assets throughout the CIR by detecting malicious activities through logs and security alerts, securing backups, preventing insider threats using IAM, etc.

CIR Ensures Compliance: A CIR ensures an organization's statutory compliance and safeguards it against fines and expensive lawsuits. It saves the organization from the legal consequences of a severe incident.

hide01.ir

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



How is Cloud Incident Response (CIR) Different from Traditional IR?

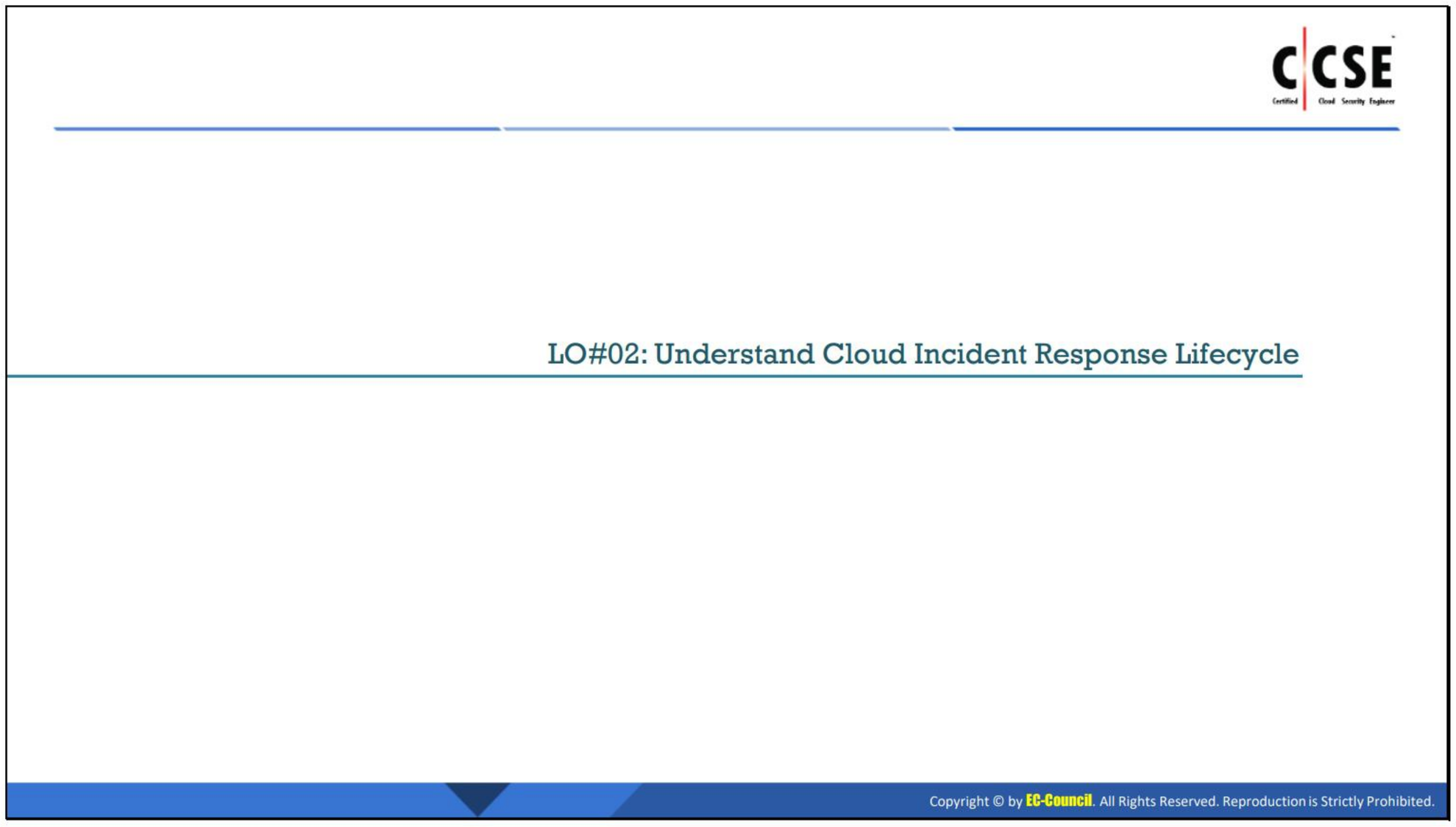
CIR is different from traditional IR in three main aspects:

Governance: In cloud computing, data resides at various geographic locations, and sometimes, with different cloud service providers. It is significantly challenging for a large cloud service provider with a large customer pool to get different organizations together to investigate an incident.

Shared Responsibility: The cloud customer, cloud service provider, and third-party provider have distinct roles to play in securing the cloud environment. The cloud service providers are responsible for their infrastructure and the services, whereas the customers are responsible for their data. The CIR should be coordinated among all parties. Before opting for the cloud services, it is essential to discuss all granular details with the cloud service provider for a clarity on governance and roles. Do not settle for a policy that you cannot implement. Every organization should clearly understand that they should not outsource shared responsibilities or governance.

Visibility: Because of a lack of visibility in the cloud environment, an incident that can be addressed promptly also includes a risk of escalation. The cloud can be leveraged appropriately to provide a faster and cost-effective incident response. When developing incident response processes and documentation, it is essential to carefully consider the benefits of a cloud architecture, which is contrary to the traditional data center models. Most tools provided by a cloud service provider can efficiently and effectively perform incident detection, response, and forensic analysis, which is possible only in the cloud environment. The CIR should be proactive and designed for failure.

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

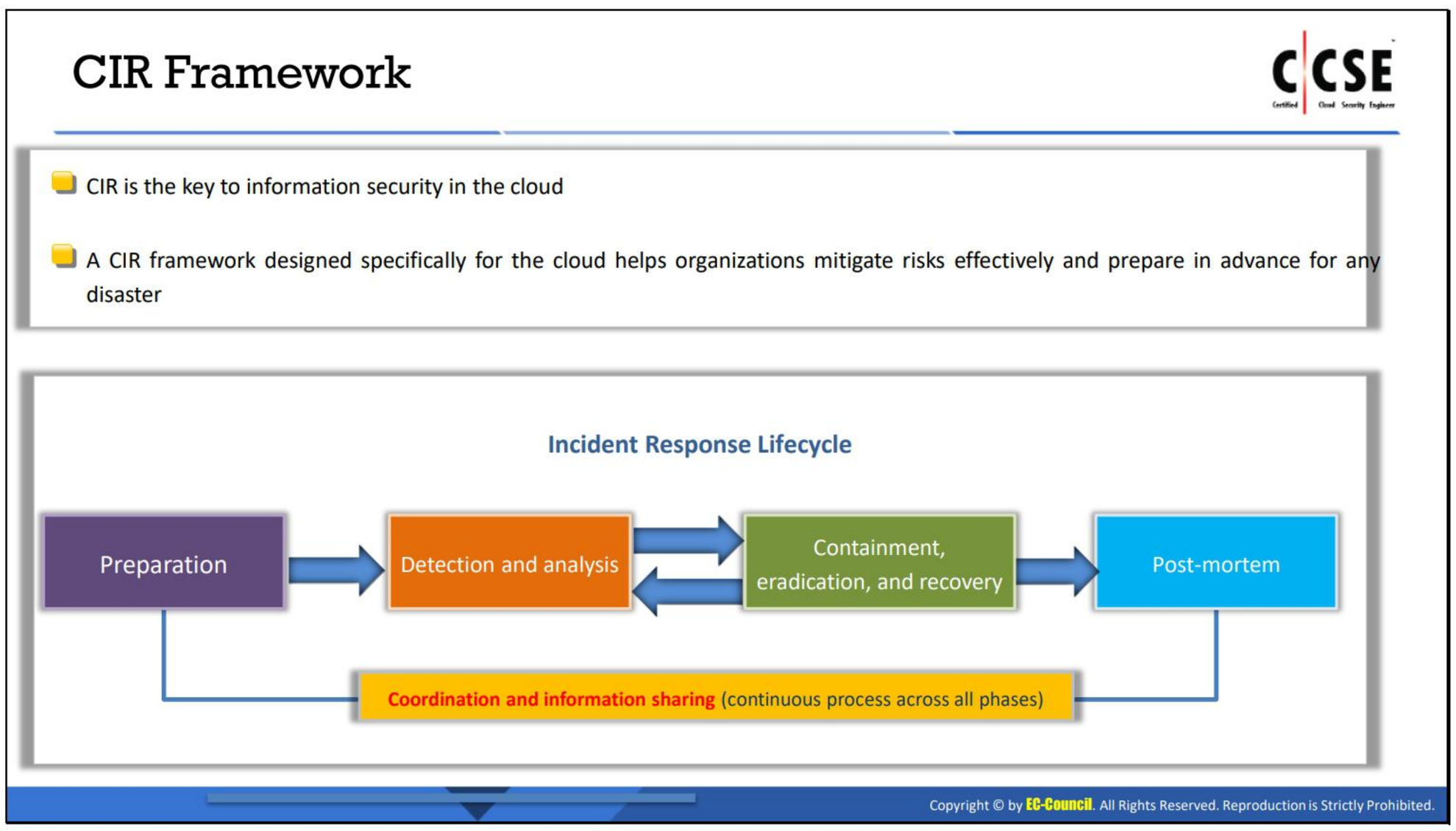


LO#02: Understand Cloud Incident Response Lifecycle

The objective of this section is to describe the various phases of CIR: preparation, detection and analysis, containment, eradication, recovery, post-mortem, and coordination, and information sharing. It provides recommendations for both users and service providers for each phase of the CIR lifecycle.

hidd01.ir

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



ClR Framework

CIR is the key to information security in the cloud. A CIR framework designed specifically for the cloud helps an organization mitigate risks effectively and prepare for any disaster in advance. This framework is applicable to all cloud incidents, whether caused by security or non-security events. These events include natural disasters, DDoS and phishing attacks, operational errors, etc. A CIR framework helps cloud users select a suitable level of incident protection to improve their BC/DR capabilities.

Incident Response Lifecycle Phases

- Preparation
- Detection and analysis
- Containment, eradication, and recovery
- Post-mortem
- Coordination and information sharing (continuous process across all phases)

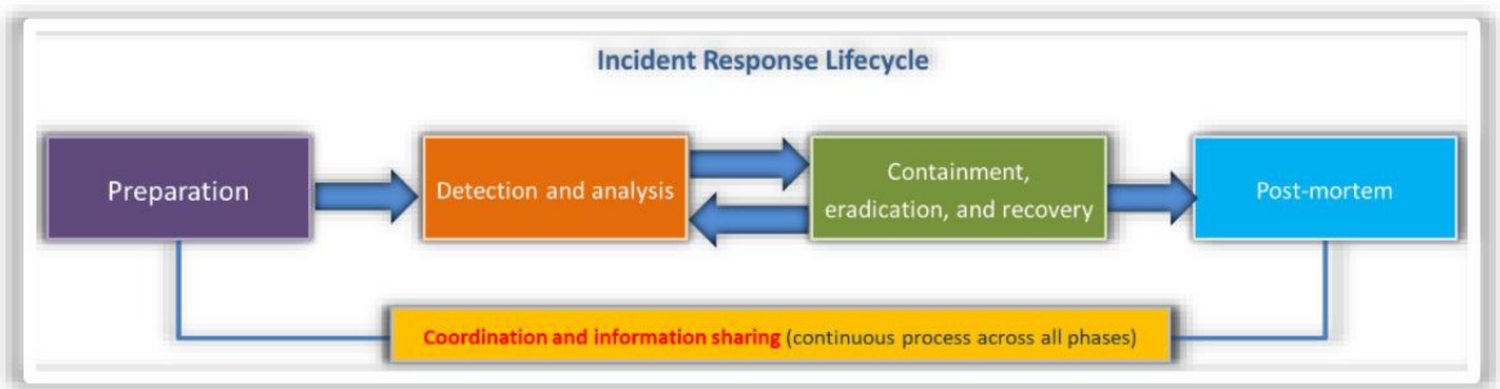
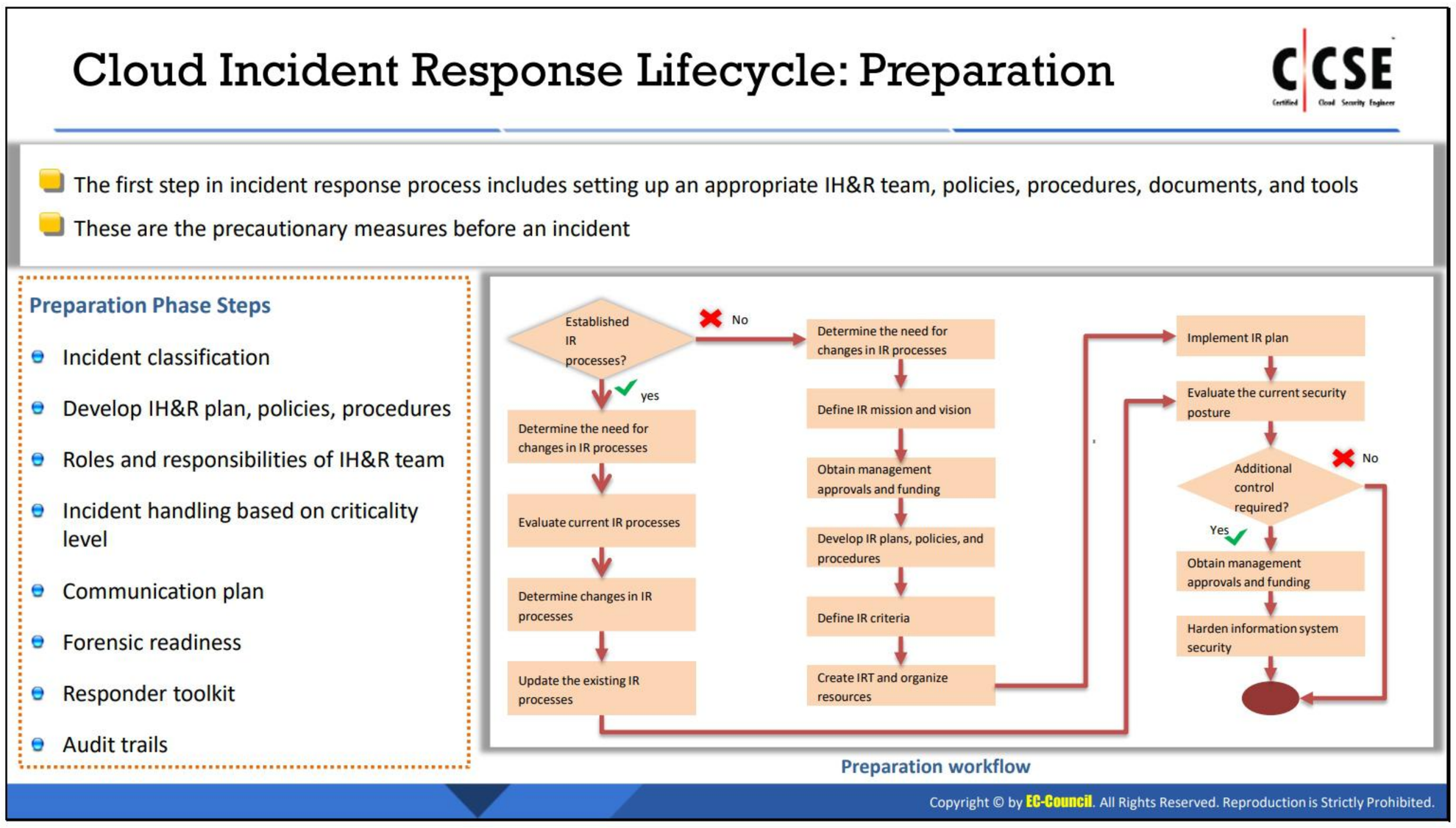


Figure 7.1: Incident Response Lifecycle Phases

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



Cloud Incident Response Lifecycle: Preparation

This is the first step in the incident response process, which includes setting up an appropriate IH&R team, policies, procedures, documents, and tools. The best solution to improve the efficiency of the incident response team is being appropriately prepared for threats. Preparation of a CIR helps in assigning responsibilities to different individuals to act on an incident. Chaos engineering methods can be deployed to build more secure systems to withstand abnormal conditions.

IAM roles can be enabled for incident response teams by following the principle of least privilege and multifactor authentication must be enabled for these accounts. A new security group can be created from incident responders for inbound connections.

The CIR team should configure the incident detection tools to respond to threats. The organization should perform risk assessments to identify the mitigating solutions for incident prevention. If the cloud infrastructure is deployed outside the control of the organization, internal policies must be created so that the cloud infrastructure is within a virtual private network (VPN). The staff should be aware of securing the cloud infrastructure. For large-scale incident handling, a face-to-face discussion with the cloud service provider and the organization's incident response team is necessary.

Cloud users must review the information, services, functionalities, and tools provided by the cloud service provider (CSP). The service level agreements (SLAs) between the users and the CSP must include their roles and responsibilities, investigation process, incident reporting process, and response time.

In case of an incident, the organization should use the CSP's business continuity and disaster recovery plans instead of its offline backups. Incident response plans should be based on

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

certain attack simulations and aimed at training the staff on appropriate actions during an incident.

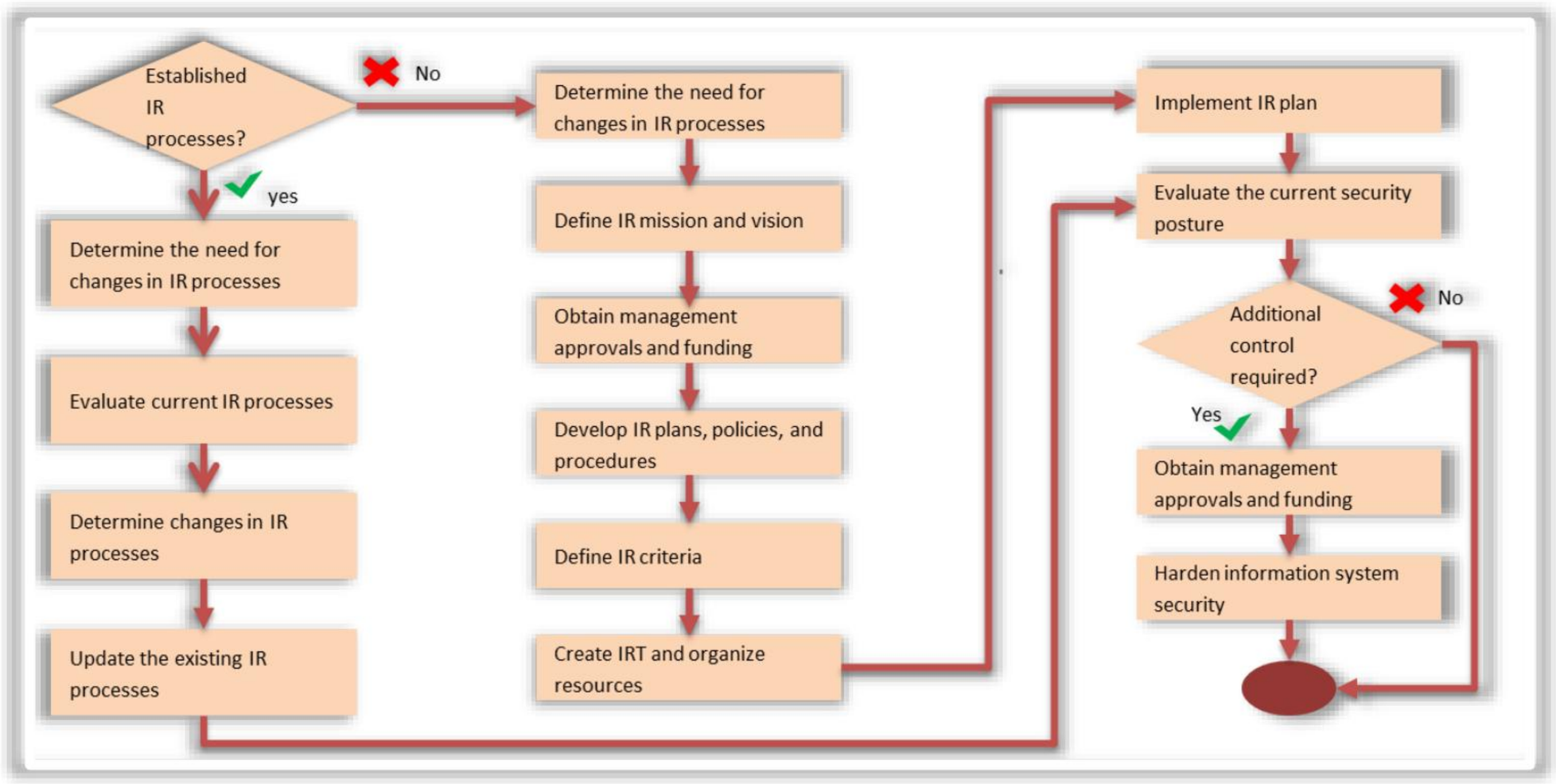
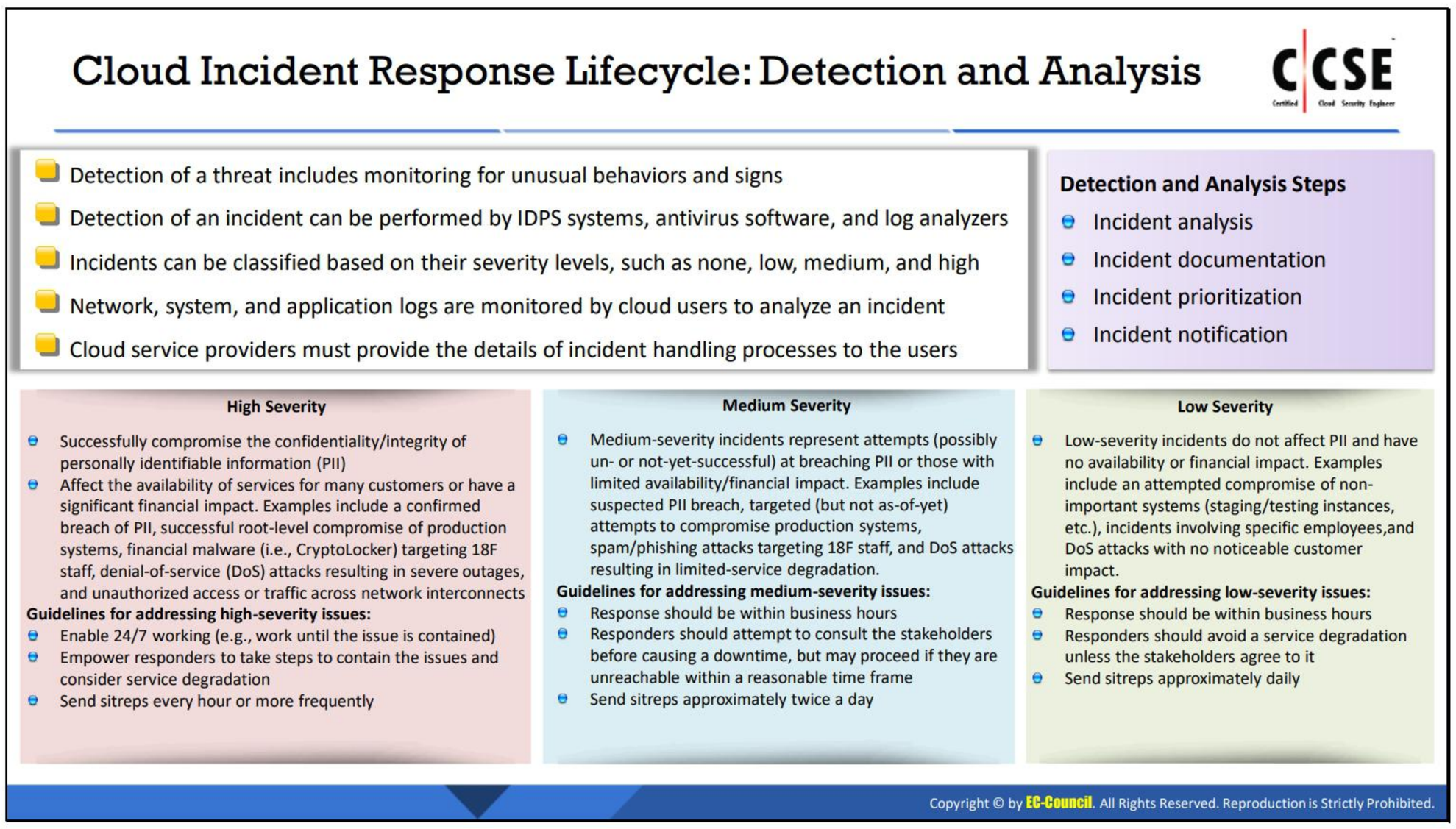


Figure 7.2: Preparation Workflow

Preparation Phase Procedures/Steps

- **Incident Classification:** The incident response team evaluates the incident details and correlates them with indicators. Incidents are then classified based on their severity, affected resources, and attack methodology. Finally, incidents are classified based on factors such as their nature, the criticality of the systems being impacted, systems impacted, and legal and regulatory requirements.
- **Develop Incident Handling and Response Plan:** The incident handling and response plan determines the future course of action for establishing, managing, and strengthening incident response capabilities.
- **Roles and Responsibilities of IH&R Team:** The incident response team comprises an incident manager, incident coordinator, threat researchers, internal auditors, etc. to detect and mitigate incidents based on their types.
- **Incidents Handling Based on Criticality Level:** Incident classification can be based on their criticality level. Incidents affecting critical systems have a high criticality level and those affecting non-critical systems have a medium criticality level. Incidents that are not time-sensitive have a low criticality level.
- **Communication Plan:** The communication plan includes emails, SMS alerts, on-call contacts, etc.
- **Responder Toolkit:** Incident responders need a collection of hardware and software tools to detect, validate, contain, and eradicate an incident in time and reduce its impact.

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



Cloud Incident Response Lifecycle: Detection and Analysis

The detection of a threat includes monitoring for threats and signs of an incident. The CSPs have their native tools for cloud monitoring. The cloud logs can be used to detect the incident time and the affected areas. The logs can be exported to an SIEM tool for alerts on incidents. The detection of an incident can be performed by intrusion detection prevention systems (IDPSs), antivirus software, log analyzers, and Impact-level classification scales can be used to classify the severity of an incident.

- **None:** The organization can provide all services to the users without any interruption.
- **Low:** The organization can provide all critical services to the users, and the impact severity will be minimal.
- **Medium:** A group of users will not be able to access the critical services.
- **High:** The organization cannot provide any service to the users.

There are two components of IaaS incident detection and response: CSP incident response and consumer incident response. A CSP incident response is applicable to backend storage, services, and networks, while a consumer incident response is applicable to consumer VMs and their associated virtual networks. Network, system, and application logs are monitored by cloud users for analyzing an incident. CSPs must provide the details of incident handling processes to the users.

The analysis of an incident is a tedious task because the incident response team may have to deal with false positives and false negatives. Profile and baseline data are important for analyzing an incident. The network, system, and application logs are important for such an analysis.

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

Detection and Analysis Procedures/Steps

- **Incident Analysis:** The incident response team needs to analyze the indicators of a security issue, and examine the security solutions, system logs, etc. This analysis will help in determining the affected resources, business impact, and incurred losses.
- **Incident Documentation:** Immediately start an incident documentation in the case of a suspected incident. The documentation must include system events, incident summary, list of evidence, actions taken, current status of the affected system, etc.
- **Incident Prioritization:** Consider the impact and urgency of an incident request to calculate its priority. Here, impact measures the effect of an incident on the cloud, and urgency indicates how quickly the organization needs a resolution.
- **Incident Notification:** The process of notifying a user or administrator about an abnormal incident, process, or action identified on a computing device or system environment is known as incident notification.

The incident levels based on their severity are as follows:

- **High-severity Incidents**

  They successfully compromise the confidentiality/integrity of personally identifiable information (PII), and affect the availability of services for a large number of customers or have a significant financial impact.

  Examples: Confirmed breach of PII, successful root-level compromise of production systems, financial malware (i.e., CryptoLocker) targeting TTS staff, denial of service (DoS) attacks resulting in severe outages, and unauthorized access or traffic across network interconnects.

Guidelines for Addressing High-Severity Issues: The work will likely be 24/7 (e.g., work until the issue is contained). Responders are empowered to take any step necessary to contain the issue, up to and including complete service degradation. Sitreps should be sent every hour or more frequently.

- **Medium-severity Incidents**

  Medium-severity incidents represent attempts (possibly un- or not-yet-successful) at breaching PII, or those with limited availability/financial impact.

  Examples: Suspected PII breach, targeted (but not as-of-yet) attempts to compromise production systems, spam/phishing attacks targeting TTS staff, and DoS attacks resulting in limited-service degradation.

Guidelines for Addressing Medium-Severity Issues: The response should be within business hours. Responders should attempt to consult the stakeholders before causing a downtime but may proceed if they cannot be contacted within a reasonable time frame. Sitreps should be sent approximately twice a day.

- **Low-severity Incidents**

  Low-severity incidents do not affect PII and have no availability or financial impact.

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

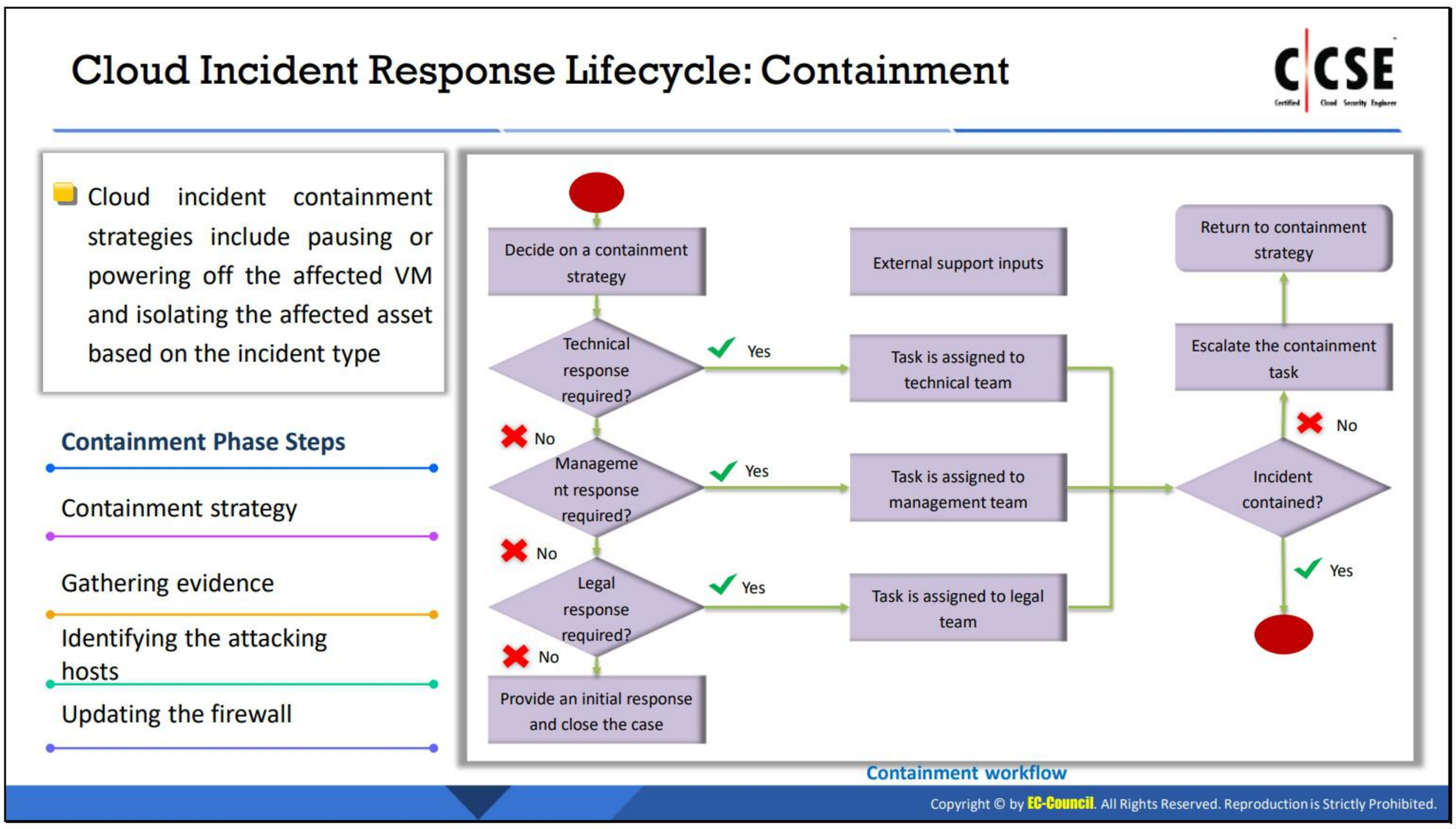
Examples: Attempted compromise of nonimportant systems (such as staging/testing instances), incidents involving specific employees, and DoS attacks with no noticeable customer impact.

Guidelines for Addressing Low-Severity Issues: The response should be within business hours.

Responders should avoid a service degradation unless the stakeholders agree to it. Sitreps should be sent approximately daily.

hide01.ir

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



Cloud Incident Response Lifecycle: Containment

Containment strategies include limiting the scope of an incident and protecting the resources. The containment process includes making the systems offline, isolating the systems, and blocking connections to the affected systems. Deleting the threats will destroy the evidence required for an investigation. Some of the containment strategies include

- **Pausing the Compromised VM:** Access to the VM, including access to all investigated valuable data residing within it, can be disabled.
- **Powering Off the VM:** The data to be investigated will be lost by powering off the VM.
- **Isolating the Compromised Asset:** Firewall rules can isolate the compromised asset.
- **Deleting the Compromised Asset:** This can be performed only after the data required for a forensic analysis has been collected and the asset is no longer required.

To recover from an incident, CSP functionalities such as like back up, disaster recovery, and business continuity plans can be used. Some common incidents are

- **Leaked Keys/ credentials:** Credentials and keys uploaded to source code repositories can be accessed by bot attacks to install malware in a system. Using cloud functionalities, these leaked keys can be revoked and a VM can be restored to an uncompromised state.
- **Firewall Rules:** Since the cloud infrastructure is deployed with firewall rules for remote access, they can easily be accessed by attackers through brute-force attempts. The firewall rules can be deleted, and more secure rules can be imposed.

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

- **Software Vulnerability:** A vulnerable software that is not patched and updated with security policies is the primary reason behind most application security incidents. The CSP's inbuilt security scanners can be used to recover from such incidents.

Containment Phase Procedures/Steps

- **Containment Strategy:** Containment strategies depend on the incident type. In other words, they are different for high-priority incidents and low-priority incidents.
- **Gathering Evidence:** The incident response team must gather evidence related to the incidents from the affected resources.
- **Identifying the Attacking Hosts:** The attacking hosts can be identified by validating the host IP address and monitoring the attacker's communication channel.
- **Updating the Firewall:** The software, firewall, or anti-malware blacklist must be updated to block attackers' IP addresses.

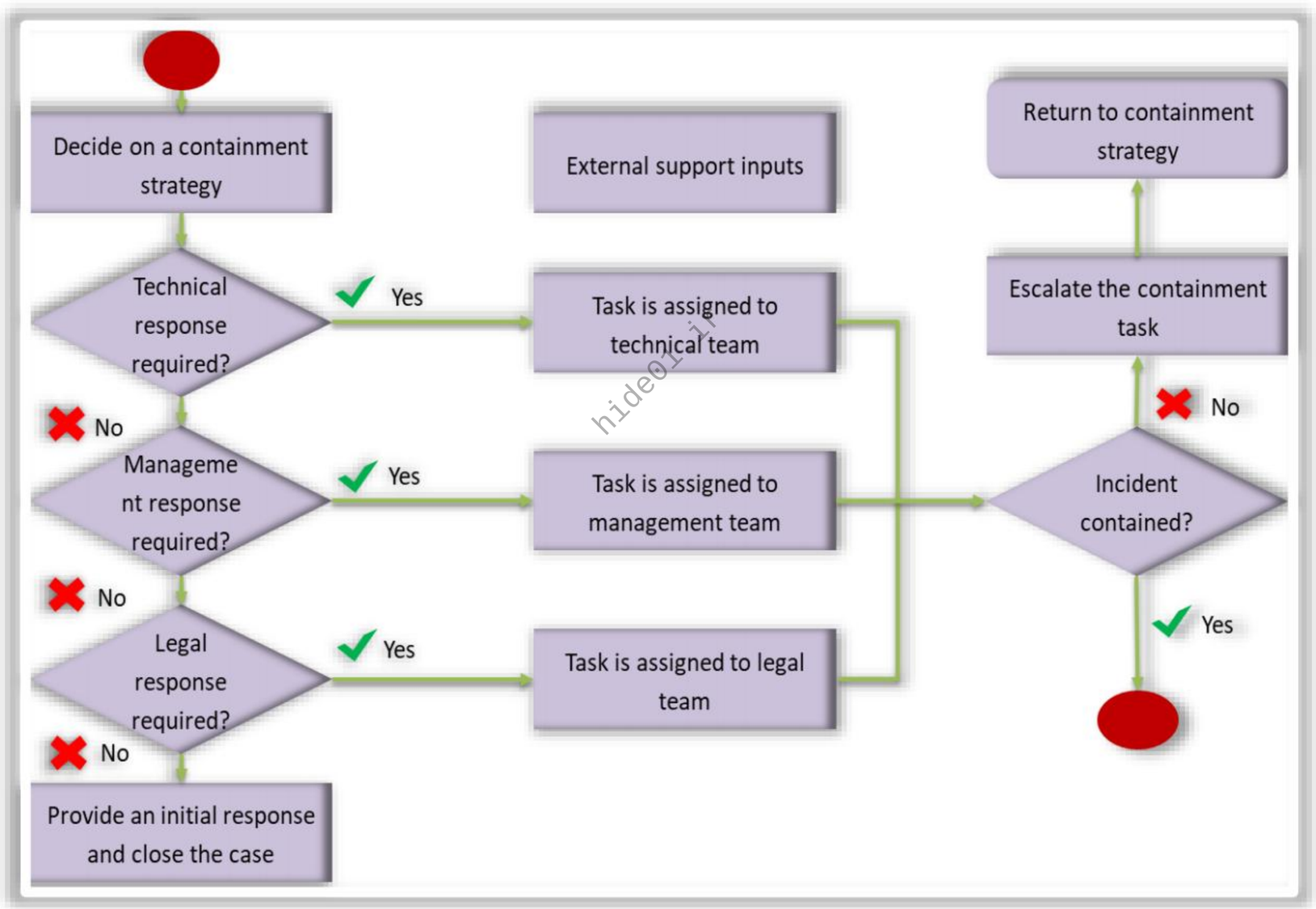
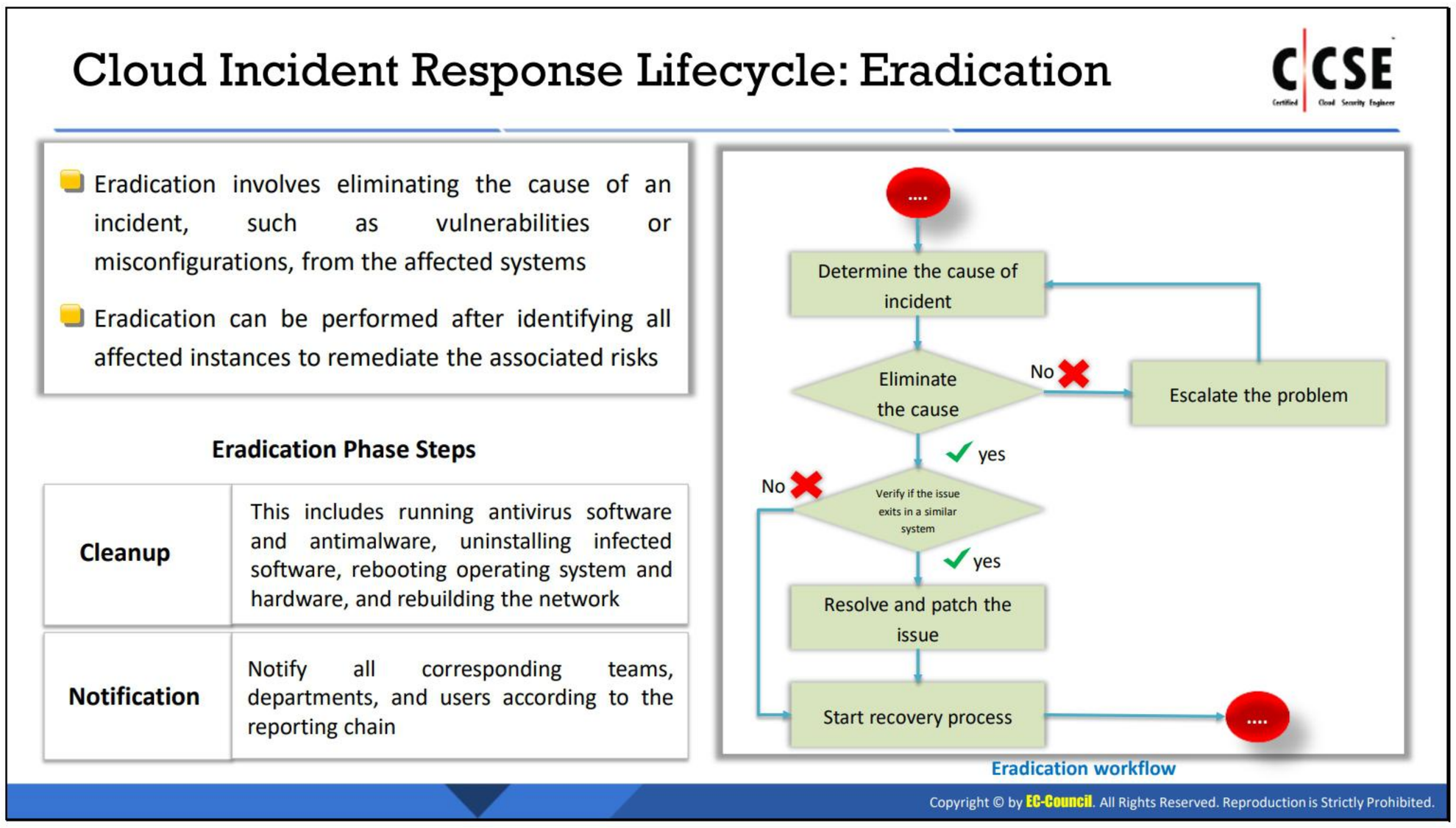


Figure 7.3: Containment Workflow

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



Cloud Incident Response Lifecycle: Eradication

Eradication involves eliminating the cause of an incident, such as vulnerabilities or misconfigurations, from the affected systems. Eradication can be performed after identifying all affected instances to remediate the associated risks.

hide01.ir

Eradication Phase Procedures/Steps

- **Cleanup:** This includes running antivirus software and antimalware, uninstalling infected software, rebooting the operating system and hardware, and rebuilding the network.

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

- **Notification:** The notification process includes notifying the incident to all corresponding teams, departments, and users according to the reporting chain.

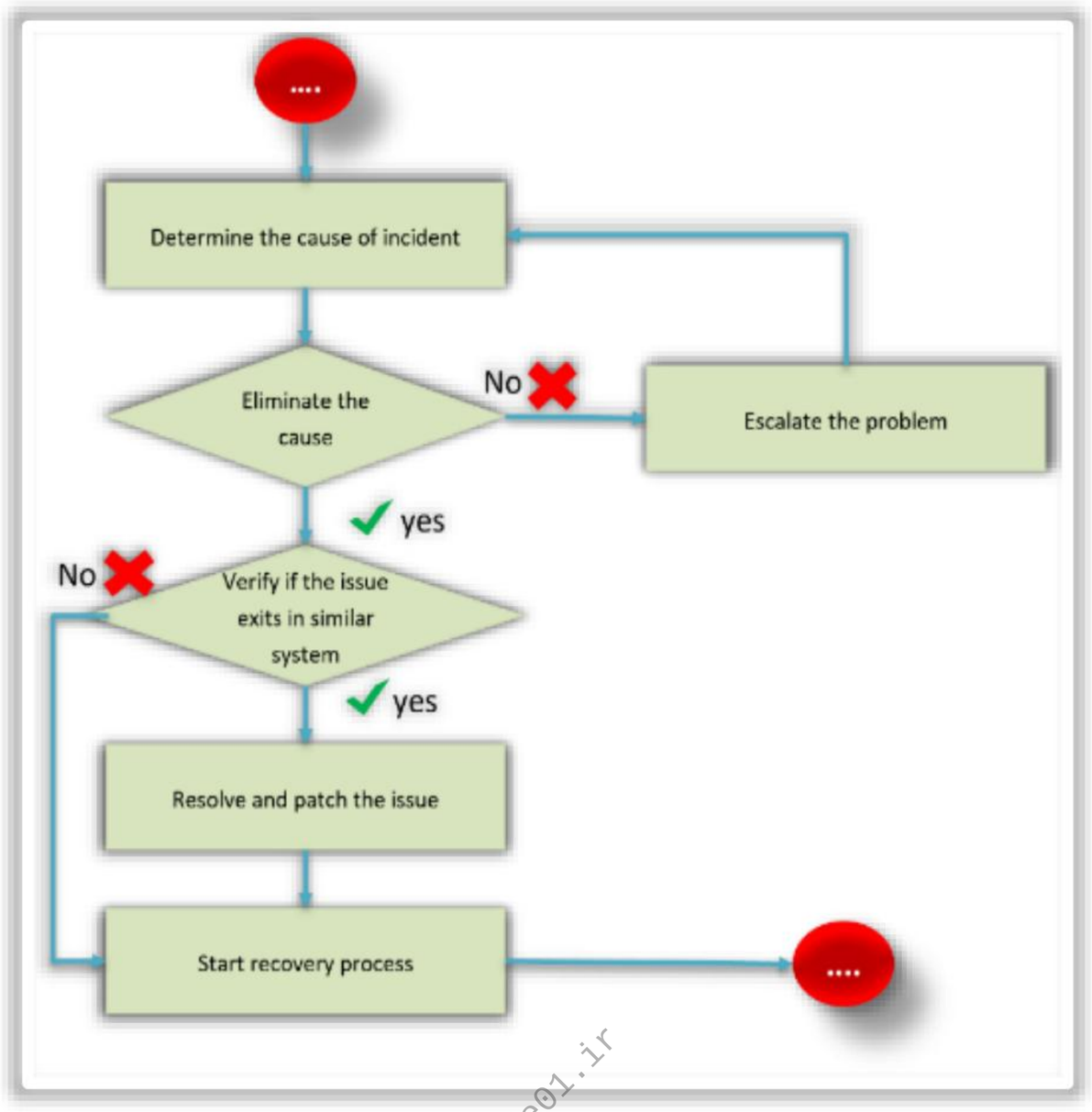
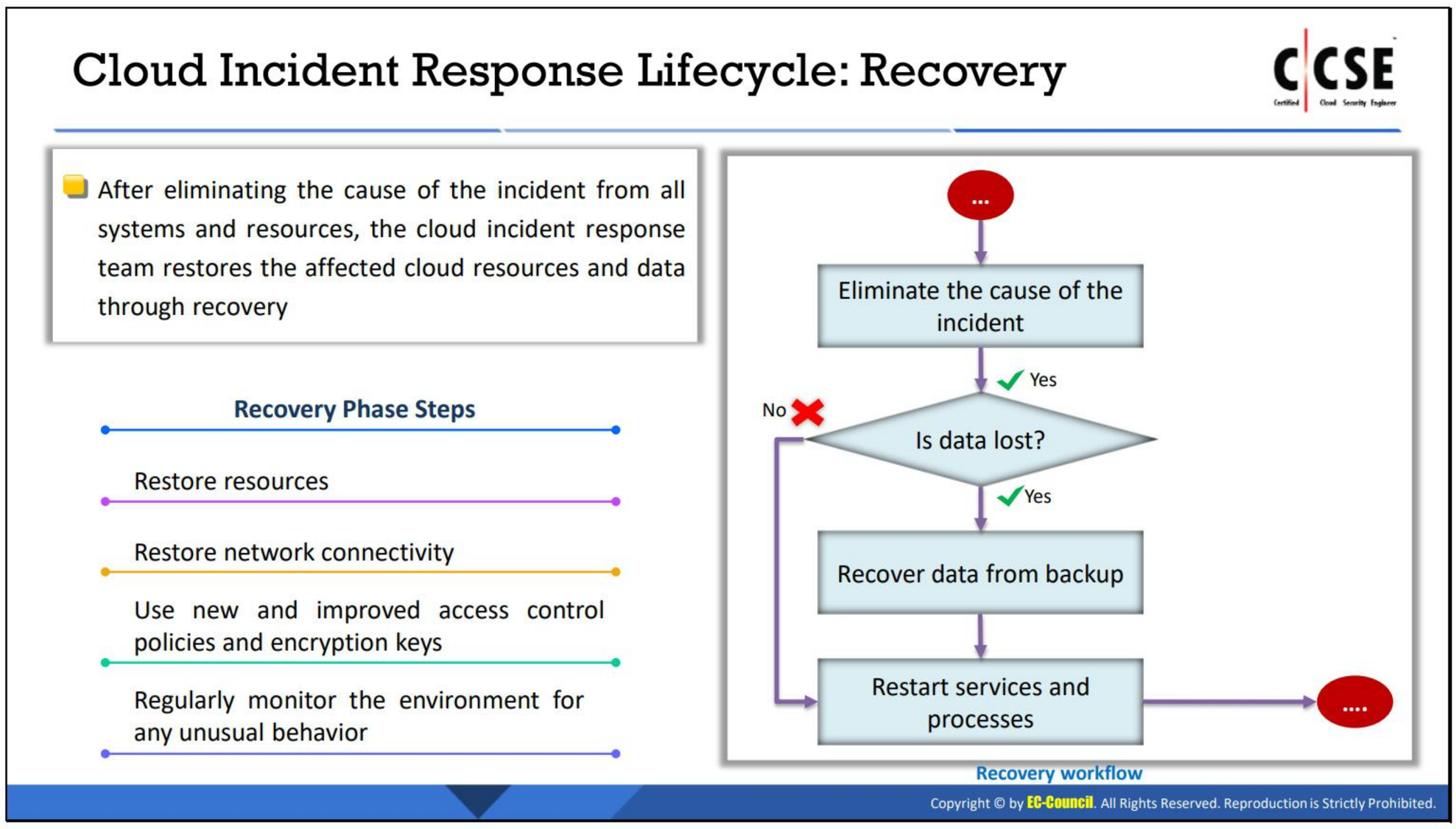


Figure 7.4: Eradication Workflow

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



Cloud Incident Response Lifecycle: Recovery

After eliminating the cause of the incident from all systems and resources, the CIR team restores the affected cloud resources and data through recovery.

hide01.ir

Recovery Phase Procedures/Steps

- **Restore Resources:** This phase restores the normal business operations by performing backups.
- **Restore Connectivity**: Restore network connectivity.
- **Access Control Policies:** This step includes the use of new and improved access control policies and encryption keys.
- **Monitoring:** Regularly monitor the environment for any unusual behavior.

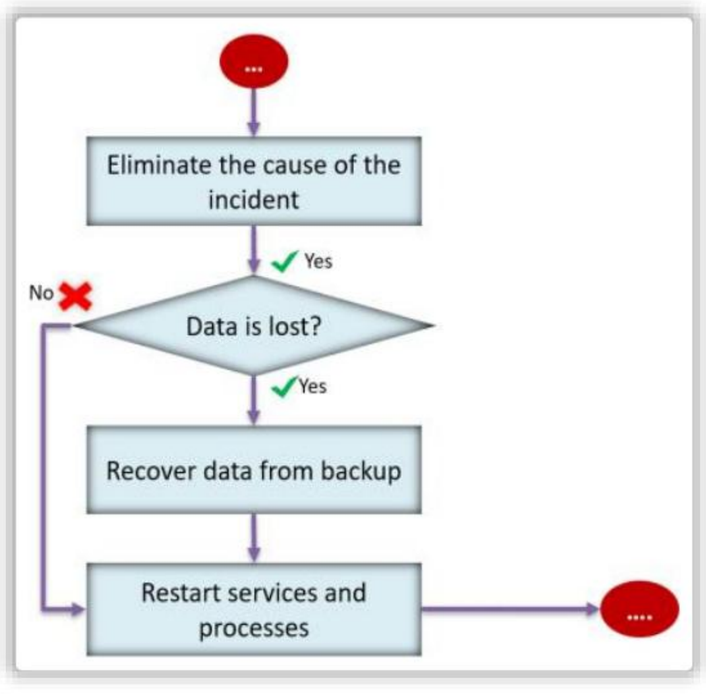
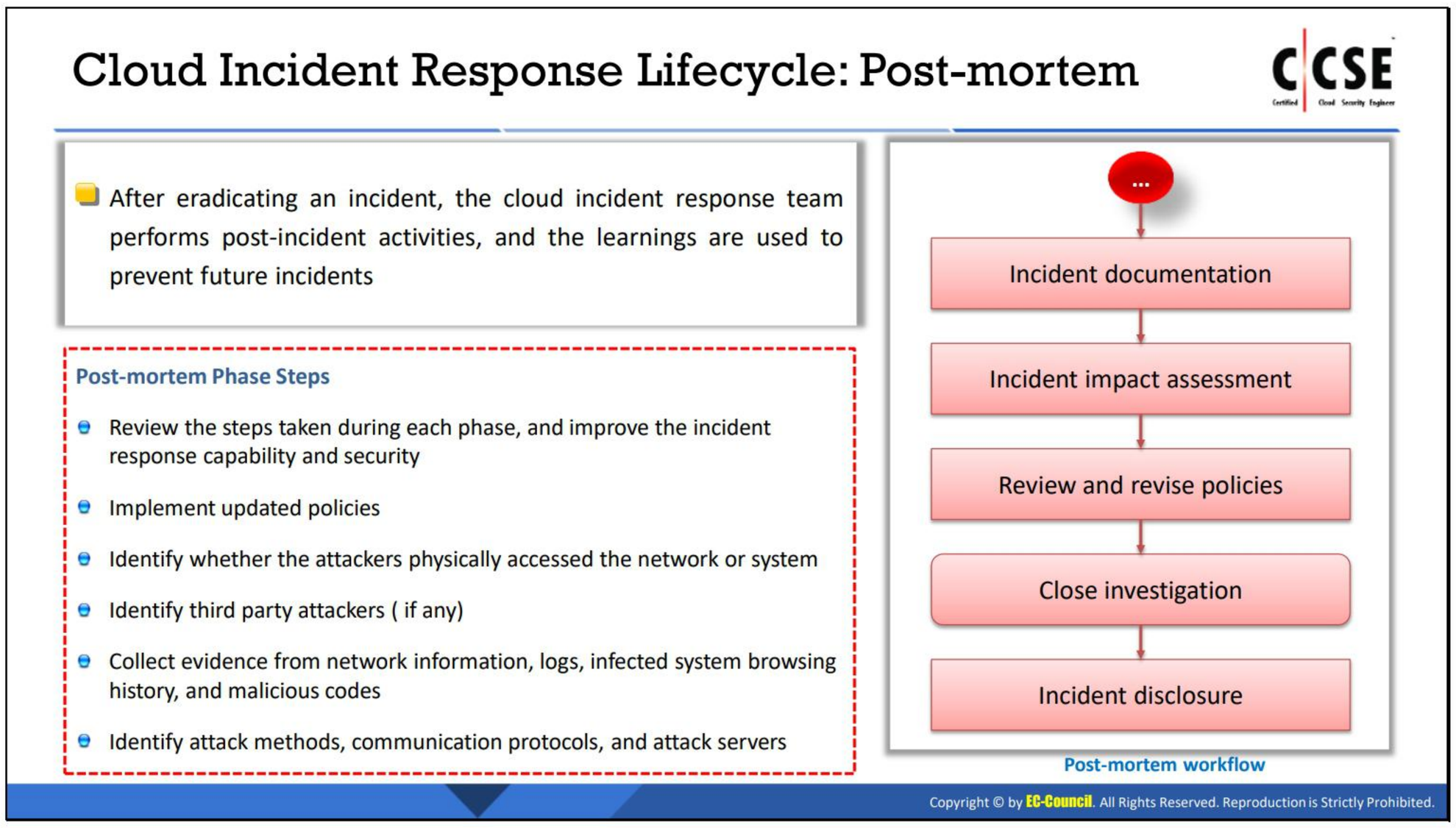


Figure 7.5: Recovery Workflow

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



Cloud Incident Response Lifecycle: Post-mortem

Post-mortem is the final phase of an incident response and is done after recovering the resources. A post-mortem should include the lessons learned from previous attacks, apart from analyzing and documenting the incident to understand the areas of improvement. After the incident is eradicated, the CIR team performs post-incident activities, and the learnings will be used to prevent future incidents. The post-mortem phase also includes patching or resolving exploited vulnerabilities to prevent future incidents. Reports from the previous phases are collected and shared with the top management, along with recommendations for improving the security posture.

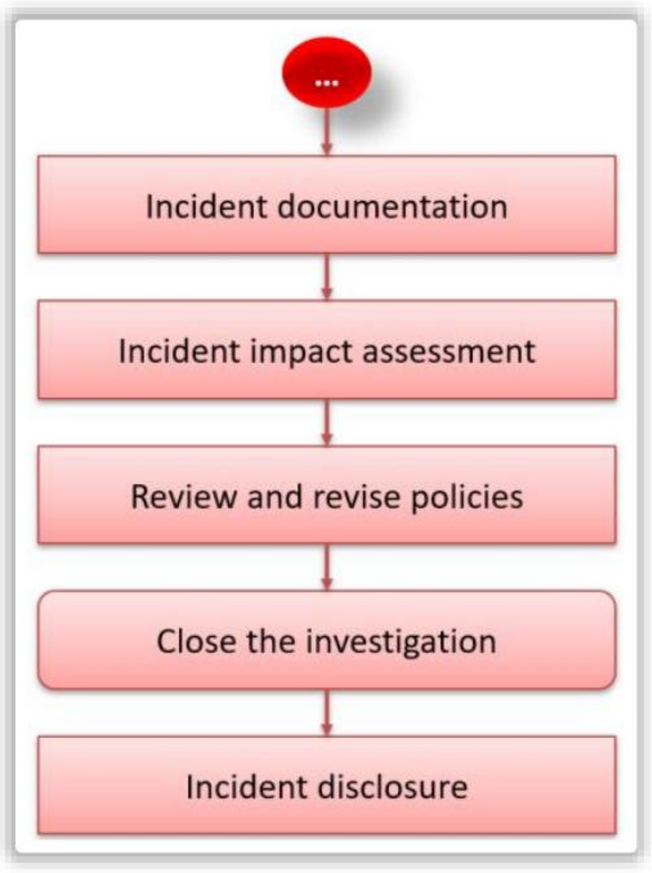


Figure 7.6: Post-mortem Workflow

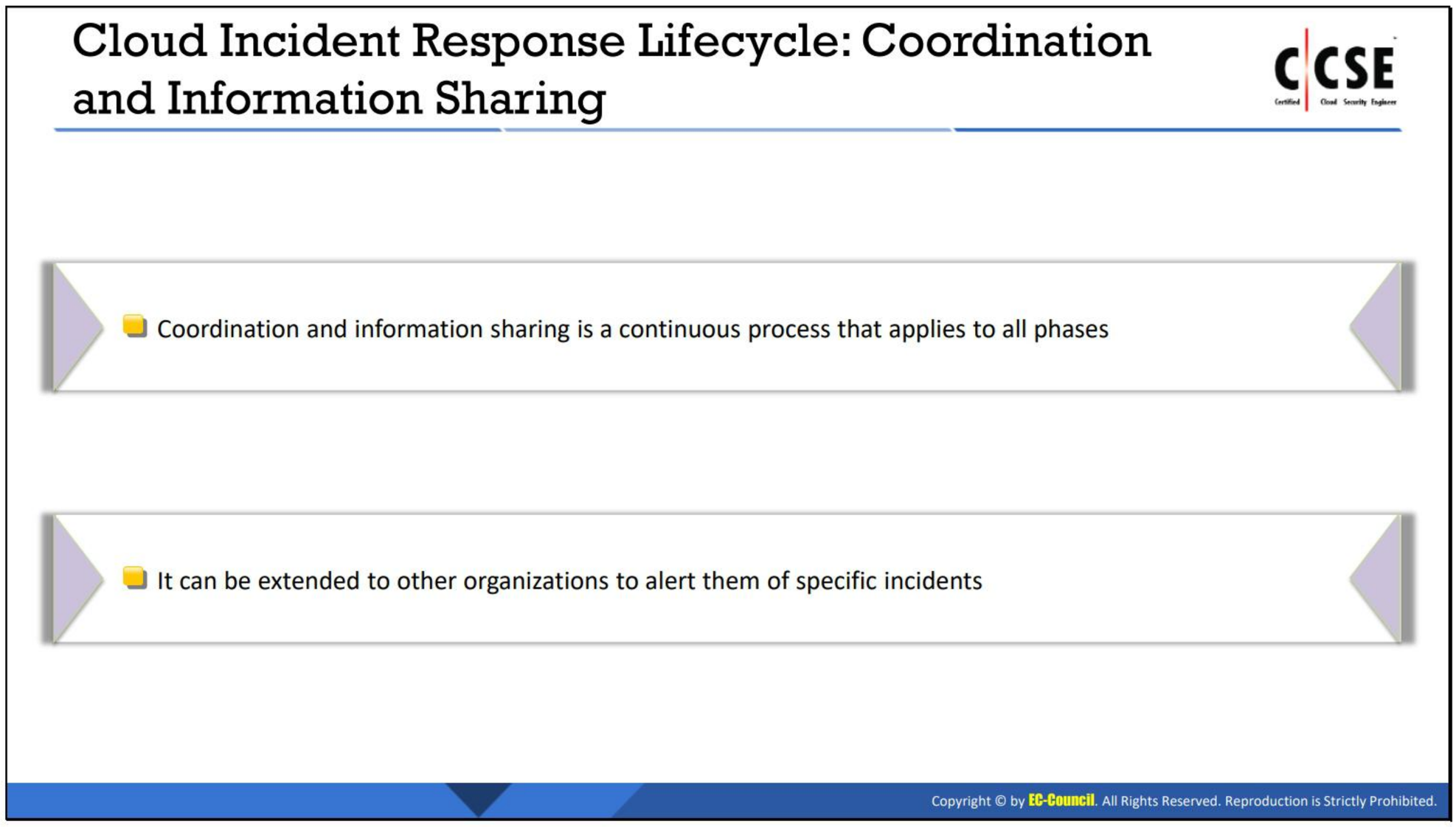
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Post-mortem Phase Procedures/Steps

- Review the steps taken during each phase and improve the incident response capability and security.
- Implement updated policies.
- Identify whether the attackers physically accessed the network or system.
- Identify third-party attackers (if any).
- Collect evidence from network information, logs, infected system browsing history, and malicious codes.
- Identify attack methods, communication protocols, and attack servers.

hide01.ir

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

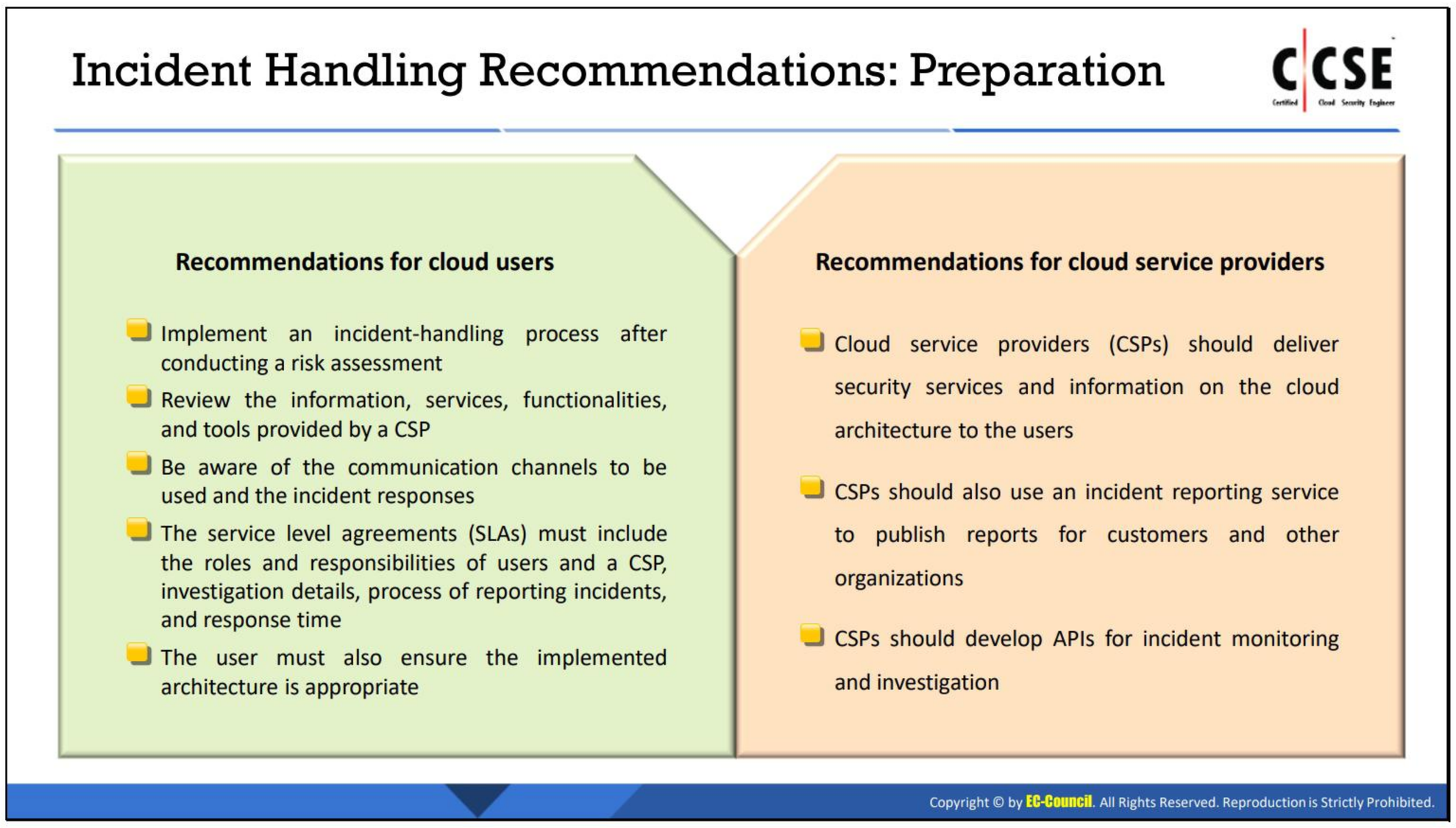


Cloud Incident Response Lifecycle: Coordination and Information Sharing

Coordination and information sharing are a continuous process and common to all phases. Proper coordination and sharing of the information between the users and CSP are essential to prevent losses and efficiently recover a business. Coordination and information sharing can be extended to other organizations to alert them of a potential incident. Different CIR teams and law enforcement agencies should also coordinate for enforcing incident response capabilities.

h1de01_ir

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



Incident Handling Recommendations: Preparation

Recommendations for Cloud Users:

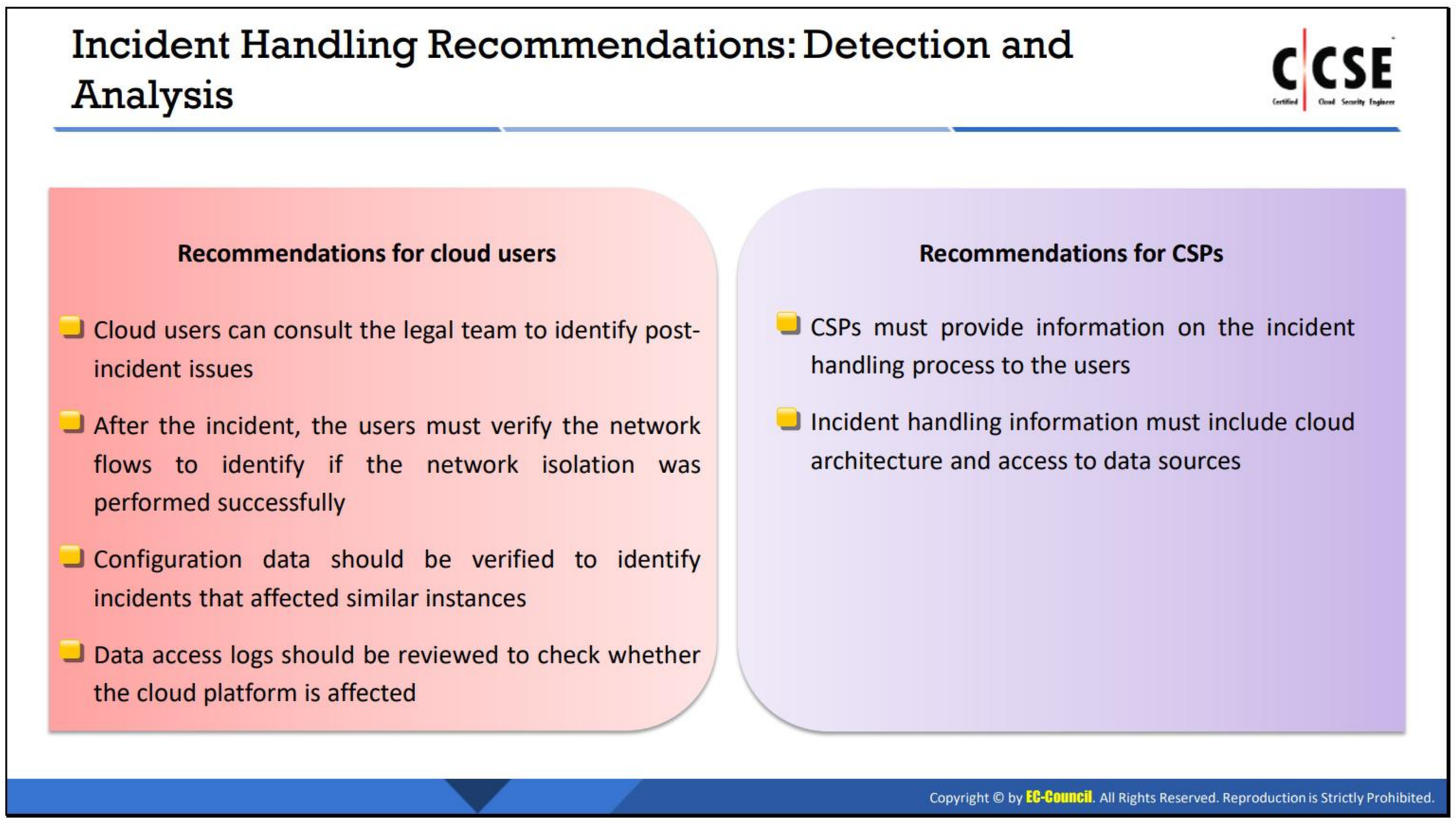
hide01.ir

- The incident handling process should be implemented after conducting a risk assessment.
- Cloud users must review the information, services, functionalities, and tools provided by a CSP.
- The user must be aware of the communication channels to be used and the incident responses.
- A service level agreement (SLA) must include the roles and responsibilities of the users and CSP, investigation details, process of reporting incidents, and response time.
- The user must also ensure the implemented architecture is appropriate.

Recommendations for CSPs:

- CSPs should deliver security services and information to users on the cloud architecture
- CSPs should also use an incident reporting service to publish reports for customers and other organizations.
- CSPs should develop APIs for incident monitoring and investigation.

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



Incident Handling Recommendations: Detection and Analysis

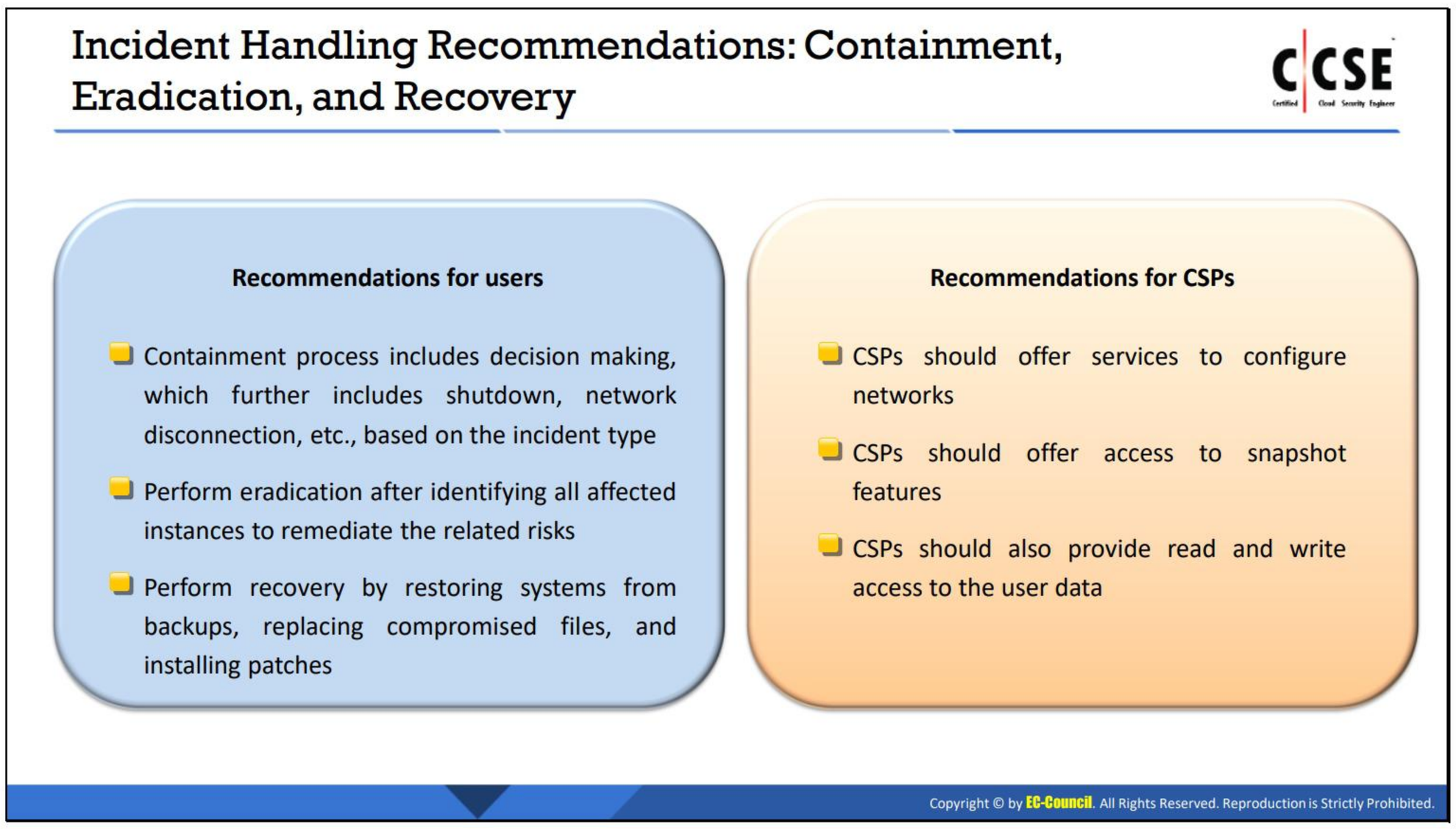
Recommendations for Cloud Users:

- Cloud users can consult the legal team to identify post-incident issues.
- After the incident, the users must verify the network flows to identify if the network isolation was performed successfully.
- The configuration data should be verified to identify incidents that affected similar instances.
- Data access logs should be reviewed to check whether the cloud platform is affected.

Recommendations for CSPs:

- CSPs must provide information on the incident handling process to the users.
- Incident handling information must include cloud architecture and access to data sources.

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



Incident Handling Recommendations: Containment, Eradication, and Recovery

Recommendations for Users:

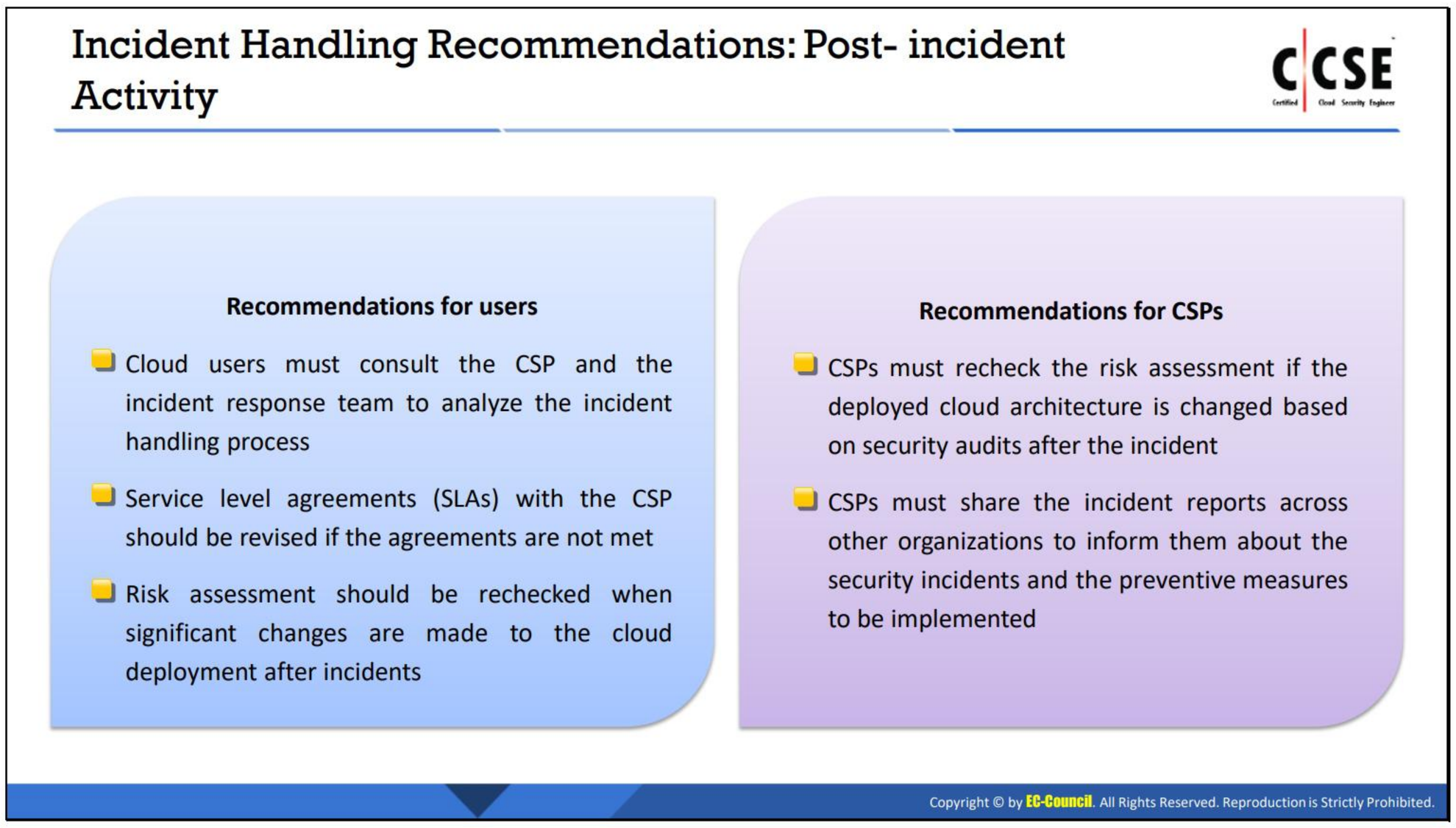
hide01.ir

- The containment process includes decision making, which further includes shutdown, network disconnection, etc., based on the incident type.
- Eradication can be performed after identifying all affected instances to remediate the related risks.
- Recovery can be performed by restoring systems from backups, replacing compromised files, and installing patches.

Recommendations for CSPs:

- CSPs should offer services to configure networks.
- CSPs should offer access to snapshot features.
- CSPs should also provide read and write access to the user data.

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



Incident Handling Recommendations: Post-incident Activity

Recommendations for Users:

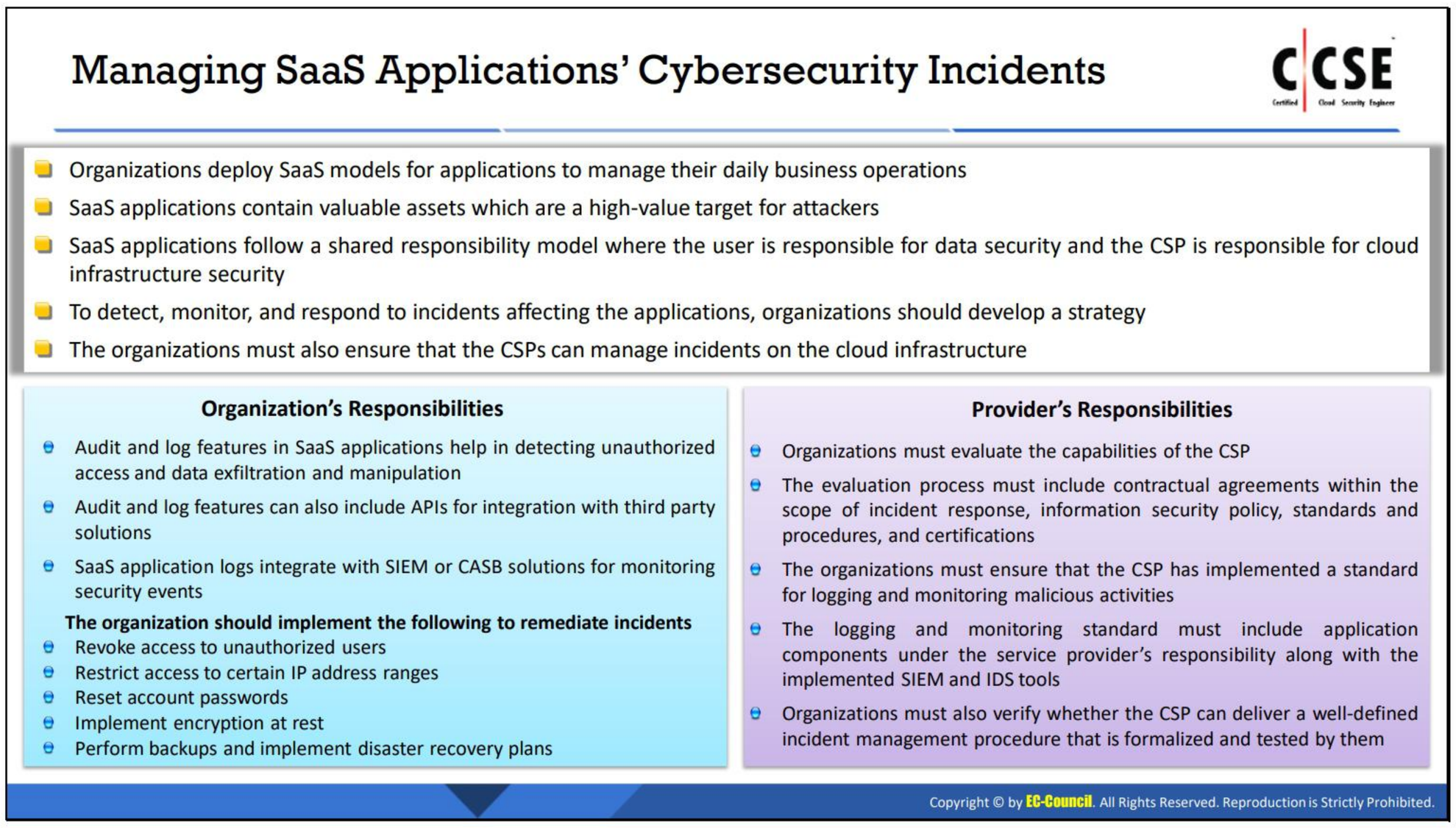
- Cloud users must consult the CSP and the incident response team to analyze the incident handling process.
- Service level agreements (SLAs) with the CSP should be revised if the agreements are not met.
- Risk assessment should be rechecked when major changes are made to the cloud deployment after incidents.

Recommendations for CSPs:

- CSPs must recheck the risk assessment if the deployed cloud architecture is changed based on security audits after the incident.
- CSPs must share the incident reports across other organizations to inform them about the security incidents and the preventive measures to be implemented.

hide01.ir

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



Managing SaaS Applications' Cybersecurity Incidents

Organizations deploy SaaS models for applications to manage daily business operations. SaaS applications contain valuable assets which are high-value targets for attackers. SaaS applications follow a shared responsibility model where the CSP is responsible for cloud infrastructure security and the users are responsible for data security.

To detect, monitor, and respond to incidents affecting the applications, organizations should develop a strategy. The organizations must also ensure that the CSPs can manage incidents on the cloud infrastructure.

Organization's Responsibilities

- Audit and log features in SaaS applications help in detecting unauthorized access and data exfiltration and manipulation.
- Audit and log features can also include APIs for integration with third-party solutions.
- SaaS application logs can be integrated with SIEM or CASB solutions for monitoring security events.

The organization should implement the following to remediate incidents

- Revoke access to unauthorized users.
- Restrict access to certain IP address ranges.
- Reset account passwords.
- Implement encryption at rest.
- Perform backups and implement disaster recovery plans.

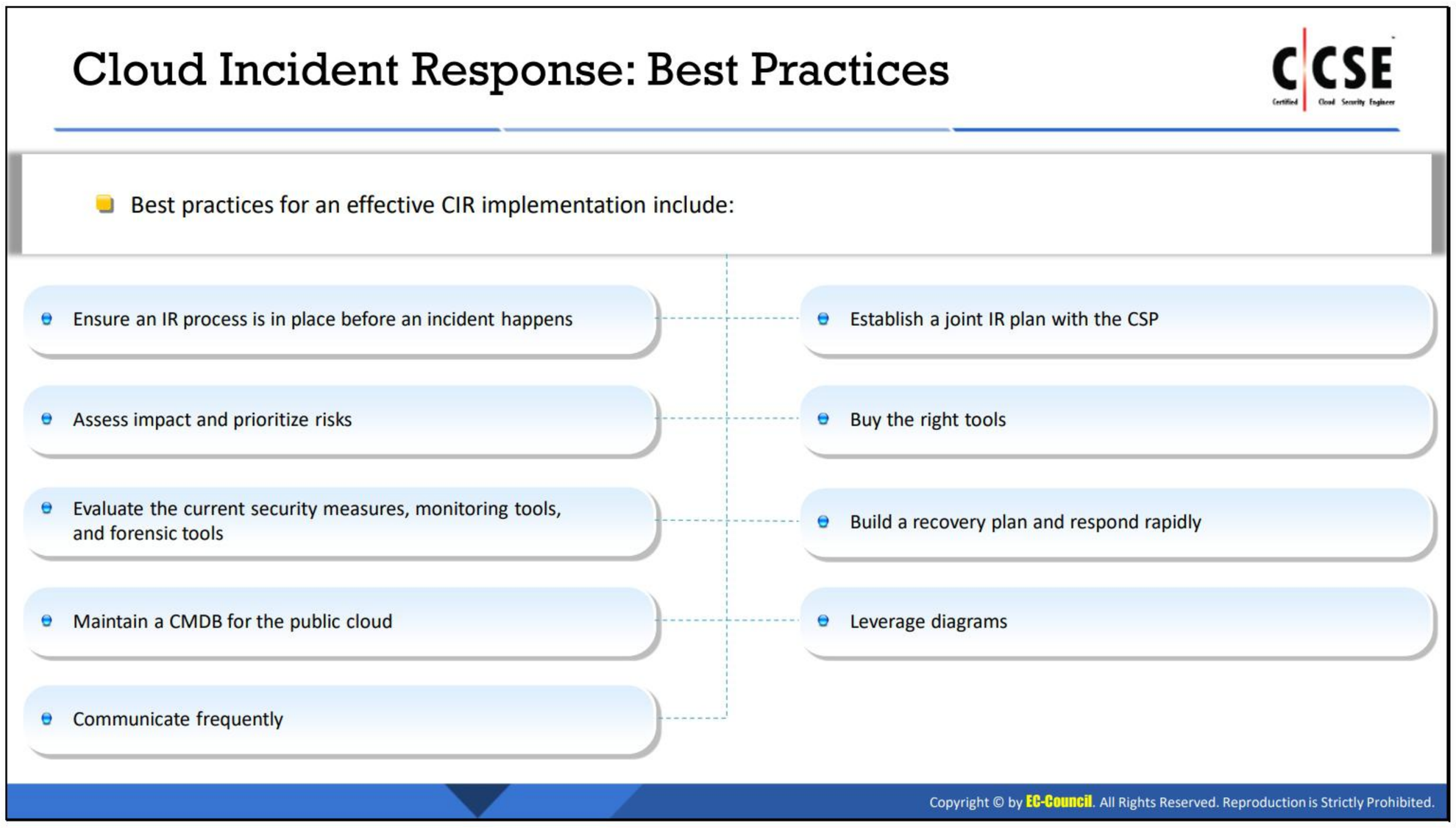
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Provider's Responsibilities

- Organizations must evaluate the capabilities of the CSP.
- The evaluation process must include contractual agreements within the scope of incident response, information security policy, standards and procedures, and certifications.
- The organizations must ensure that the CSP has implemented a standard for logging and monitoring malicious activities.
- The logging and monitoring standard must include application components under the service provider responsibility along with the implemented SIEM and IDS tools.
- Organizations must also verify whether the CSP can deliver a well-defined incident management procedure that is formalized and tested by them.

hide01.ir

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



Cloud Incident Response: Best Practices

Implement the following best practices for an effective incident response in the cloud:

- **Ensure an IR Process is in Place Before an Incident**

  Prepare a response to security incidents before they occur. Have an IR process that contains all necessary procedures and methods required to tackle and remediate security incidents. Document and develop playbooks containing standard procedures for the IR team to respond to incidents. Create scripts and materials to help the team communicate with stakeholders and customers about critical outages or incidents. In addition, ensure that the IT team is able to access the training guides and all processes are updated regularly (consider automating them if possible).

  Have an IR management process to,

  - Reduce financial loss
  - Improve response speed
  - Improve internal and external communication
  - Provide a scope for continuous improvement and learning

- **Establish a Joint IR Plan With the CSP**

  Consider establishing a joint IR plan with the CSP if your organization has not yet moved to the cloud. Define the roles and responsibilities and exchange contact information of all primary and secondary points of contact.

  Get detailed information on what can trigger the CSP's incident response and what measures they will take to handle various incidents.

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

- **Assess Impact and Prioritize Risks**

  Respond to security incidents according to their impact on the organization. Categorize and prioritize incidents as per their severity and urgency. Define all severity and priority levels before incidents occur so that they can be effectively handled without any major loss. Ensure that proper communications are established between team members responsible for handling incidents to avoid any communication gap.

- **Evaluate the Current Security Measures, Monitoring Tools, and Forensic Tools**

  Understand the security measures and monitoring tools provided by the CSP to respond to incidents. It is essential to thoroughly understand the CSP's services and tools for incident response and what type of access you have to these tools and services. Have supplemental fixes wherever there are insufficient security measures or monitoring controls in the cloud environment.

  In addition, evaluate the forensic tools from the CSP or any other source for investigating incidents. Have the appropriate tools for forensics and evidence tracking for incidents involving personally identifiable information (PII).

- **Buy the Right Tools**

  Invest in the right incident response tools in the cloud as the cloud infrastructure is complex and large with several moving parts for tracking and monitoring. Use automation tools to offload repetitive and mundane tasks. Choose incident management tools that are best suited to your cloud IR plan. Some popular incident management tools include:

  - IBM QRadar
  - Demisto
  - Confluence
  - Splunk

- **Build a Recovery Plan and Respond Rapidly**

  Discuss and decide if a recovery will be necessary in the event of a provider outage. Have a clear recovery plan that specifies the recovery options to be used (another provider or internal assets) to gather and move data.

  Respond to incidents rapidly by integrating alerts into the current workflows for policy orchestration and automated remediation.

- **Maintain a Configuration Management Database (CMDB) for the Public Cloud**

  Ensure that a configuration management database (CMDB) is maintained for the public cloud as the traditional CMBD systems cannot provide a historical context for incident response investigations in dynamic cloud environments. Maintain a CMDB for the cloud to identify users who modified database configurations and provide essential information for investigations.

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

- **Leverage Diagrams**

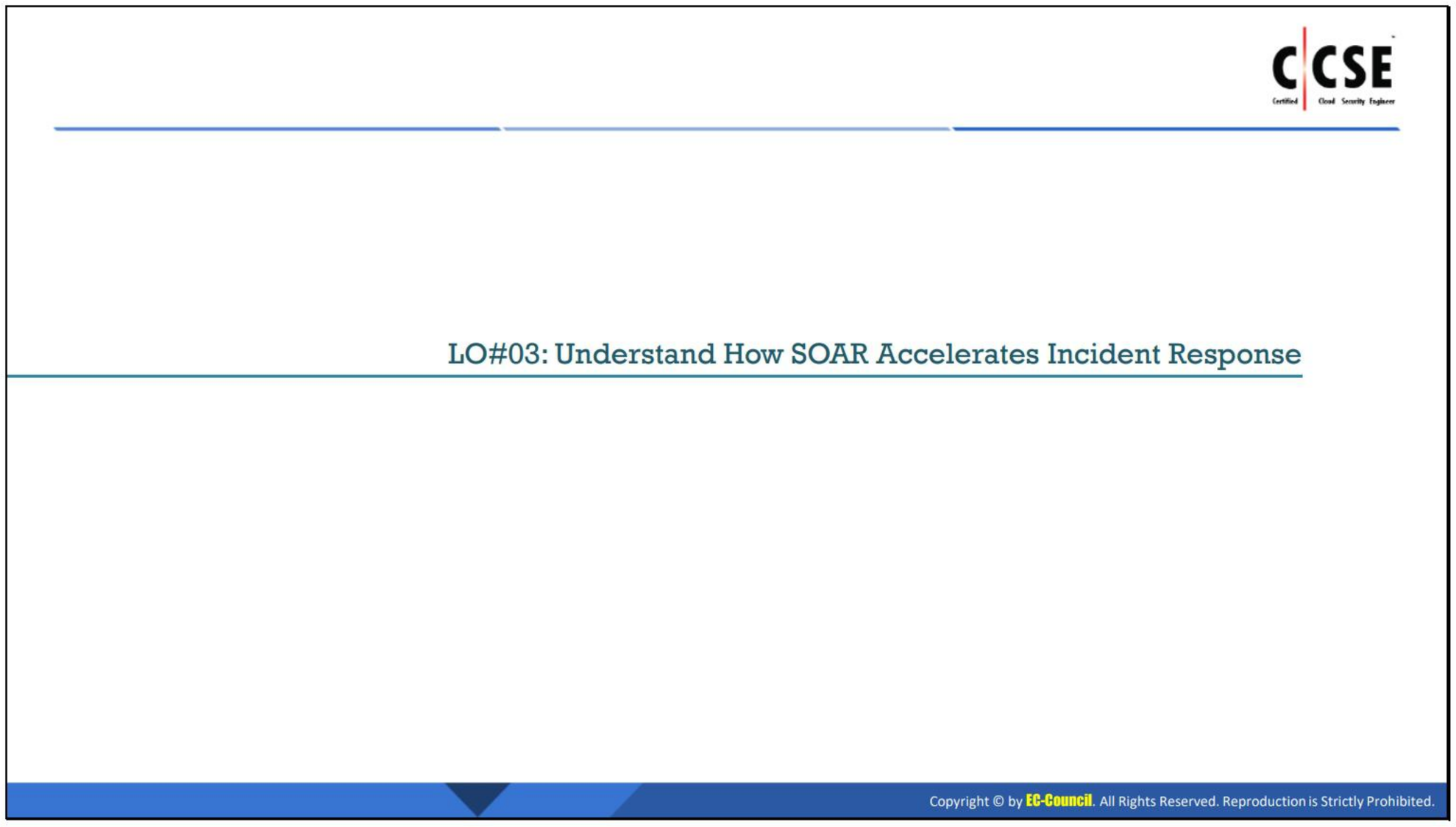
  In cloud environments, security incidents often go undetected because their high volumes, which makes it difficult to prioritize them. Use diagrams to visualize IR processes and map cloud architecture so that everyone can be alerted and made aware of the incidents and can handle them effectively. Use diagrams and maps to understand the cloud architecture and how the cloud components work together. Moreover, make the process of sharing recommendations and insights with stakeholders easier and fill the communication gaps between remote teams.

- **Communicate Frequently**

  Ensure all IR team members use IR playbooks, process flows, and messaging scripts and are on the same page. Have communication channels for team members involved in the IR process to avoid any communication gap or miscommunication. Create a status page for tracking incidents to share information with a large group of team members.

hide01.ir

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

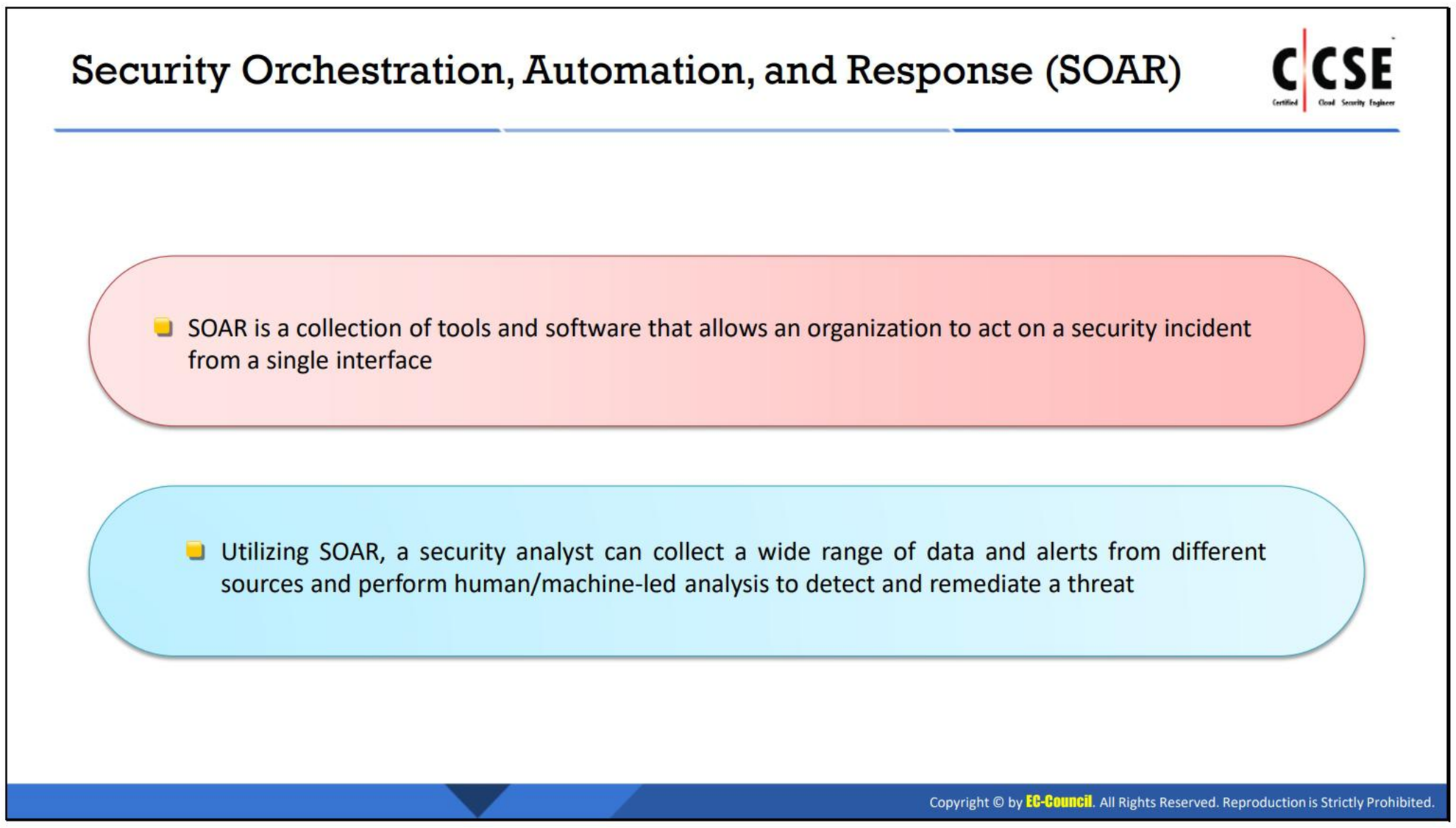


LO#03: Understand How SOAR Accelerates Incident Response

The objective of this section is to highlight the importance of security orchestration, automation, and response (SOAR) for accelerating incident response. It describes various SOAR use cases, implementations, and tools.

hide01.ir

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



Security Orchestration, Automation, and Response (SOAR)

Security orchestration, automation, and response (SOAR) is a collection of tools and software that allows an organization to act on a security incident from a single interface. Security automation is the automatic handling of security operations-related tasks, such as searching the logs or scanning for vulnerabilities, whereas security orchestration is a method to connect the security tools and integrate different security systems. Security orchestration is a connecting layer that streamlines the security process and supports security automation. SOAR allows an organization to streamline security operations in three important areas: security operations automation, threat and vulnerability management, and incident response.

A security analyst usually deals with numerous cyberattacks manually from attackers. They have to take care of thousands of alerts regularly, and it is really hard for them to decide on which alert to act on and which alerts to ignore. Even with an adequate staff, an incident response can be significantly time-consuming. In most organizations, the security team suffers from alert fatigue and fails to respond to a real alert. SOAR helps the organization in handling these tasks effectively using automation and orchestration. It allows the organization to respond quickly to a security incident, perform an investigation on an important issue, and improve the overall security posture.

Using SOAR, a security analyst can respond to multiple alarms at machine speed. The SOAR solution provides the event data and security in a single consolidated view that allows a security analyst to analyze, investigate, and act instantly. Using SOAR, a security analyst can perform automated queuing and prioritize alerts. It also helps them organize the alert details, such as IP addresses, email addresses, domain names, and other relevant fields, which helps in efficiently and effectively responding to an incident. SOAR can be easily integrated with security and infrastructure assets such as endpoint products, SIEMs, firewalls, etc. It will enhance their

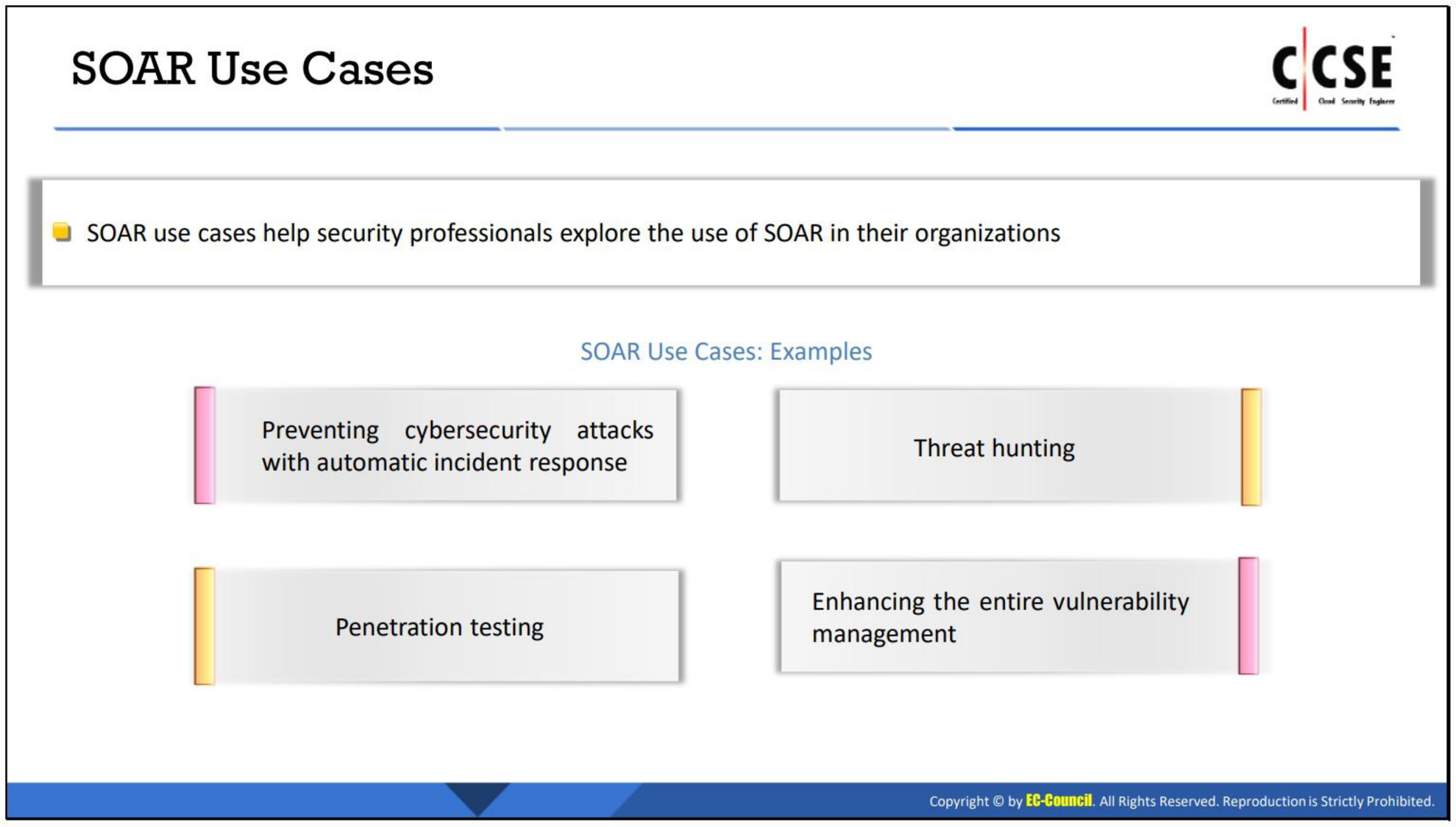
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

decision-making ability and significantly minimize their time-consuming activities by minimizing false positives, manual processes, and repetitive tasks.

Utilizing SOAR, a security analyst can collect a wide range of data and alerts from different sources and perform human/machine-led analysis to detect and remediate a threat. SOAR minimizes the mean time to detect (MTTD) and mean time to respond (MTTR) through the security alerts that should be remediated within minutes. Thus, it helps in reducing the risk of a security breach and limits the damage. SOAR helps in automating the incident response process such as blocking the IP address on the firewall or IDS system, suspension of user accounts, etc.

hide01.ir

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



SOAR Use Cases

The following SOAR use cases help security professionals explore the application of SOAR in their organizations.

hide01.ir

Preventing Cybersecurity Attacks with An Automatic Incident Response: The severity of security incidents varies in different industries. For example, the healthcare industry is subject to phishing attacks aimed at stealing the user credentials from hospital databases, whereas the retail industry is increasingly subject to ransomware attacks. A security analyst can use the SOAR platform to automatically analyze and detect the sources of these types of attacks. For instance, a security analyst can identify and examine a suspicious phishing email, find out its copies in the network, delete or quarantine them, block IP addresses, etc.

Threat Hunting: Security analysts regularly deal with numerous alerts, and thus, do not have any time to hunt for threats, perform an investigation, and develop a strategy to robustly secure the entire organization. With SOAR automation, they can quickly address most previously encountered threats, which will allow them to improve the security across the entire network. For example, the financial services industry is subject to various attacks, including security breaches and confidential data theft. Using SOAR, a security analyst can address these attacks instantly, correct the vulnerabilities, and create difficulties for the attackers to access sensitive information.

Penetration Testing: Most organizations do not conduct penetration testing consistently. Using the SOAR platforms, a security team can operationalize penetration testing and easily perform automated tasks such as target prioritization, asset discovery scans, etc.

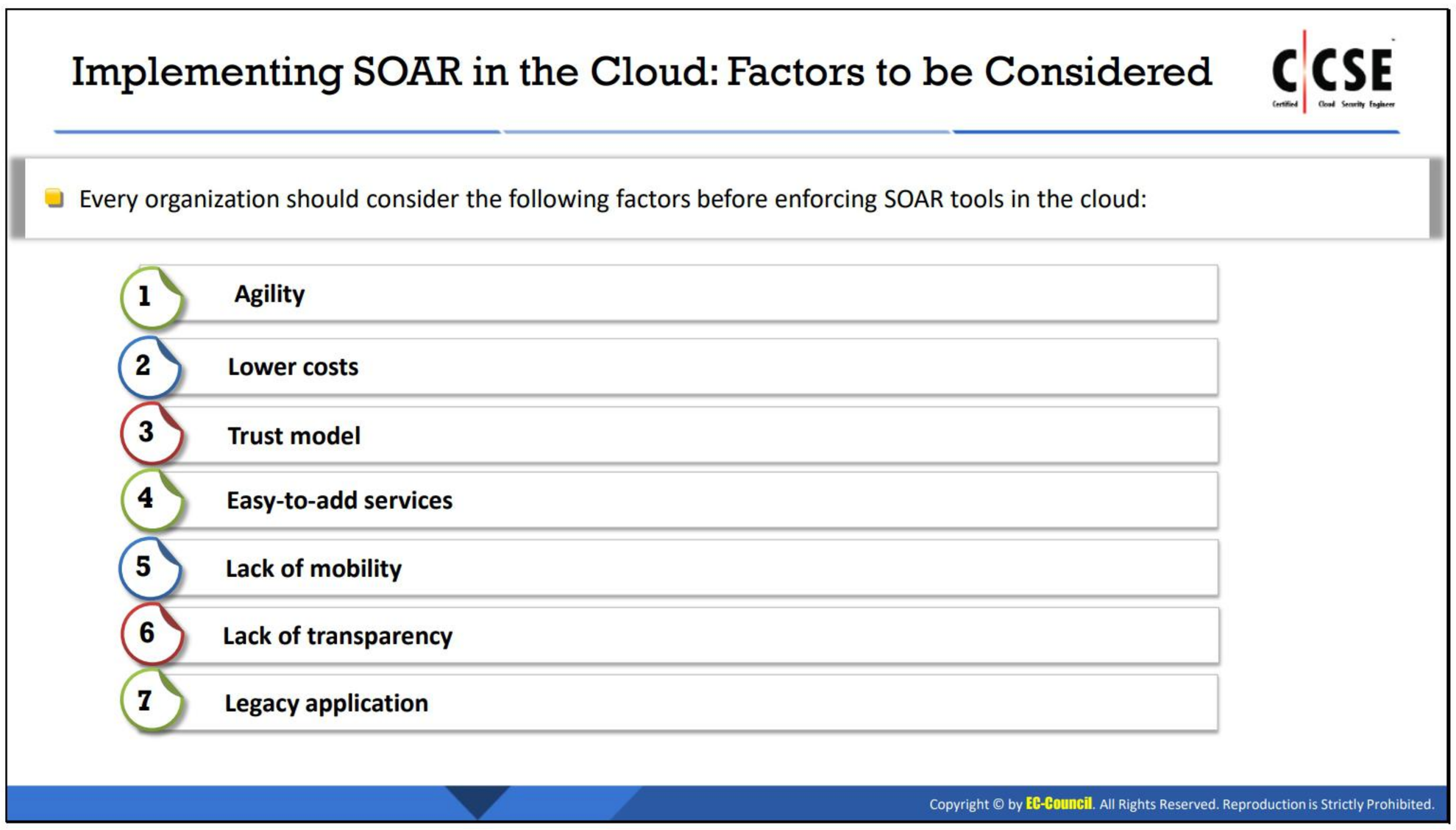
Enhancing the Entire Vulnerability Management: With SOAR, a security team can triage and properly manage the security risks launched by new vulnerabilities in the environment. SOAR

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

allows a security team to proactively collect information on the vulnerabilities, perform an investigation, and place safeguards to prevent breaches or attacks.

hide01.ir

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



Implementing SOAR in the Cloud: Factors to be Considered

The increased usage of cloud computing and the ineffectiveness of perimeter security around a traditional network has made security controls and operations complex. This complexity is further increased because of the perimeter's extension to roaming endpoints, SaaS applications, shifting of the entire workload to IaaS, etc. This increases the need to examine various aspects and accomplish various tasks to maintain the enterprise security. Owing to the numerous security benefits of SOAR, many organizations are willing to use SOAR tools in the cloud. Before using SOAR tools in the cloud, the security and the business objectives should be balanced. Every organization should consider the following factors before enforcing SOAR tools in the cloud.

Agility: In the older models, developers used to go through various rigid processes to gain access to the computing environment. With cloud models, they can spin the servers in seconds, easily deploy an application, and rapidly initiate application testing.

Lower Costs: To appropriately maintain the onsite infrastructure, there is a need for several on-prem solutions, which can significantly increase the associated costs. The cloud's "pay-as-you-use" model allows a customer to only pay for the services they use.

Trust Model: The certification process of cloud models ensures they are secure, and compliance audits check whether all the standards are satisfied. A cloud model should meet and adhere to all regulations.

Easy-to-add Services: The CSPs allow the cloud consumer to easily add services. The cloud consumer can quickly add any number of services in their environment without any complexity.

Lack of Mobility: Owing to the deployment of services and workloads, it is difficult to switch to other CSPs.

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

Legacy Applications: Some legacy applications are alluring to many organizations because of their 24/7 availability. It makes more sense to run such legacy or critical applications on a hybrid or on-prem model.

Lack of Transparency: You should know the flow of your information and understand the cloud-deployed services or products thoroughly to be able to control the cloud technology; otherwise, it will control you. You should know how your information moves, its format, its location, etc. The CSP should adhere to and meet the federal regulatory standards, but only you and your organization can ensure each security concern is addressed appropriately. Hence, you should thoroughly understand every detail of the process; otherwise, you would inevitably run into an issue.

Therefore, many organizations adopt a hybrid model to extract the benefits of both cloud and on-premises. It is recommended to identify the gaps in the current workflow before finding a SOAR platform.

hide01.ir

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

SOAR Tool: IBM Security SOAR

- IBM Security SOAR, formerly known as IBM Security Resilient, is a SOAR tool that makes a security operations center (SOC) more efficient
- With this tool, the security team can respond to cyber-threats with confidence, automate with intelligence, and collaborate with consistency

IBM Security SOAR dashboard



Source: https://www.ibm.com

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

SOAR Tool: IBM Security SOAR

Source: https://www.ibm.com

IBM Security SOAR, formerly known as IBM Security Resilient, introduces efficiency into a security operations center (SOC). It maximizes security tools by integrating with them, guides the team through the incident response (IR) process with playbooks, and leverages automation to reduce repetitive tasks, allowing the team to focus on the tasks that matter the most.

It is designed to help the security team respond to cyber threats with confidence, automate with intelligence, and collaborate with consistency. It captures and codifies the established incident response processes into dynamic playbooks to guide and empower the team with knowledge to resolve incidents. It helps the team accelerate and orchestrate their response by intelligently automating actions and integrating with other security tools. In addition, it allows the team to visualize and understand security incidents to prioritize and act accordingly.

IBM Security SOAR helps in minimizing the duration and impact of a cyberattack by automating manual tasks; thus, it allows the team to focus on high-value investigations. IBM Security SOAR's open and agnostic platform integrates with a security infrastructure and establishes a central hub to maximize security investments. IBM Security SOAR's playbooks are dynamic and additive, providing the team with guidance to resolve incidents and agility and intelligence to adapt to incident conditions.

Key Features of SOAR Tool

- It provides flexible deployment options to meet your needs.
- Use SOAR capabilities as part of Cloud Pak for Security, an open, multi-cloud platform built on Red Hat OpenShift.

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

- Realize rapid time-to-value using software-as-a-service (SaaS) early in the SOAR journey.
- On-premises deployment through a virtual machine to support limited, existing virtualized environments.

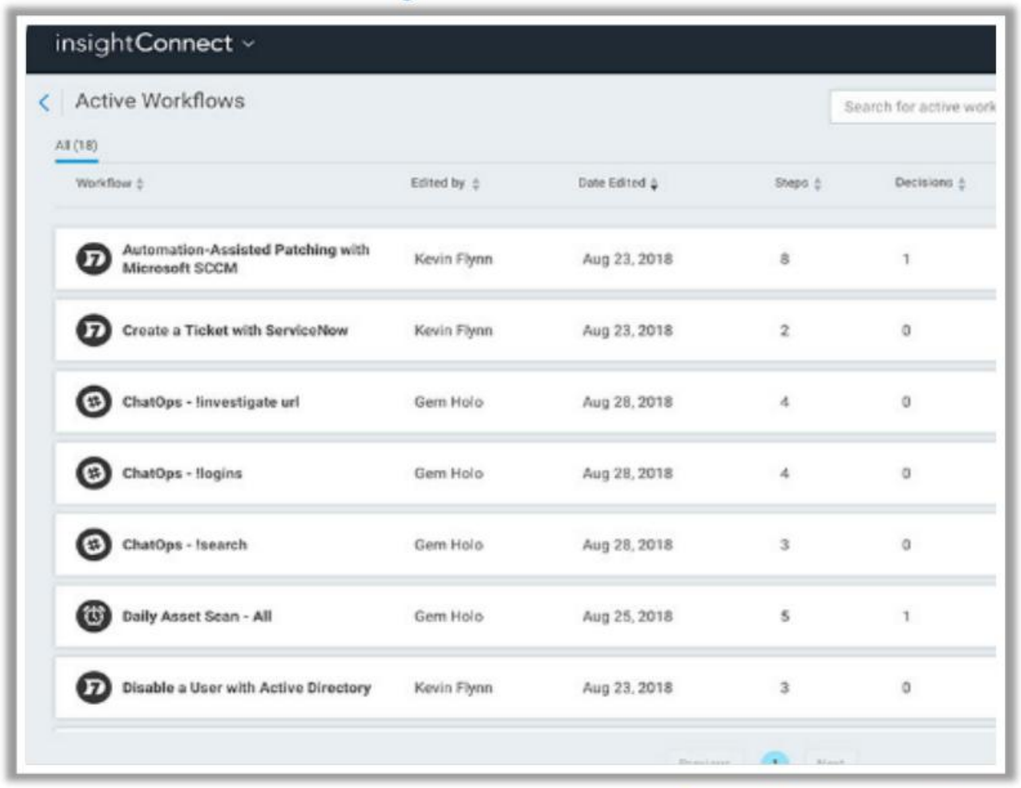
hide01.ir

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

SOAR Tool: InsightConnect

- InsightConnect is Rapid7's security orchestration and automation response (SOAR) solution to accelerate, streamline, and integrate time-intensive security processes
- With this tool, a user can create workflows from scratch and customize them to meet the team's needs

InsightConnect workflow



Source: https://www.rapid7.com

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

SOAR Tool: InsightConnect

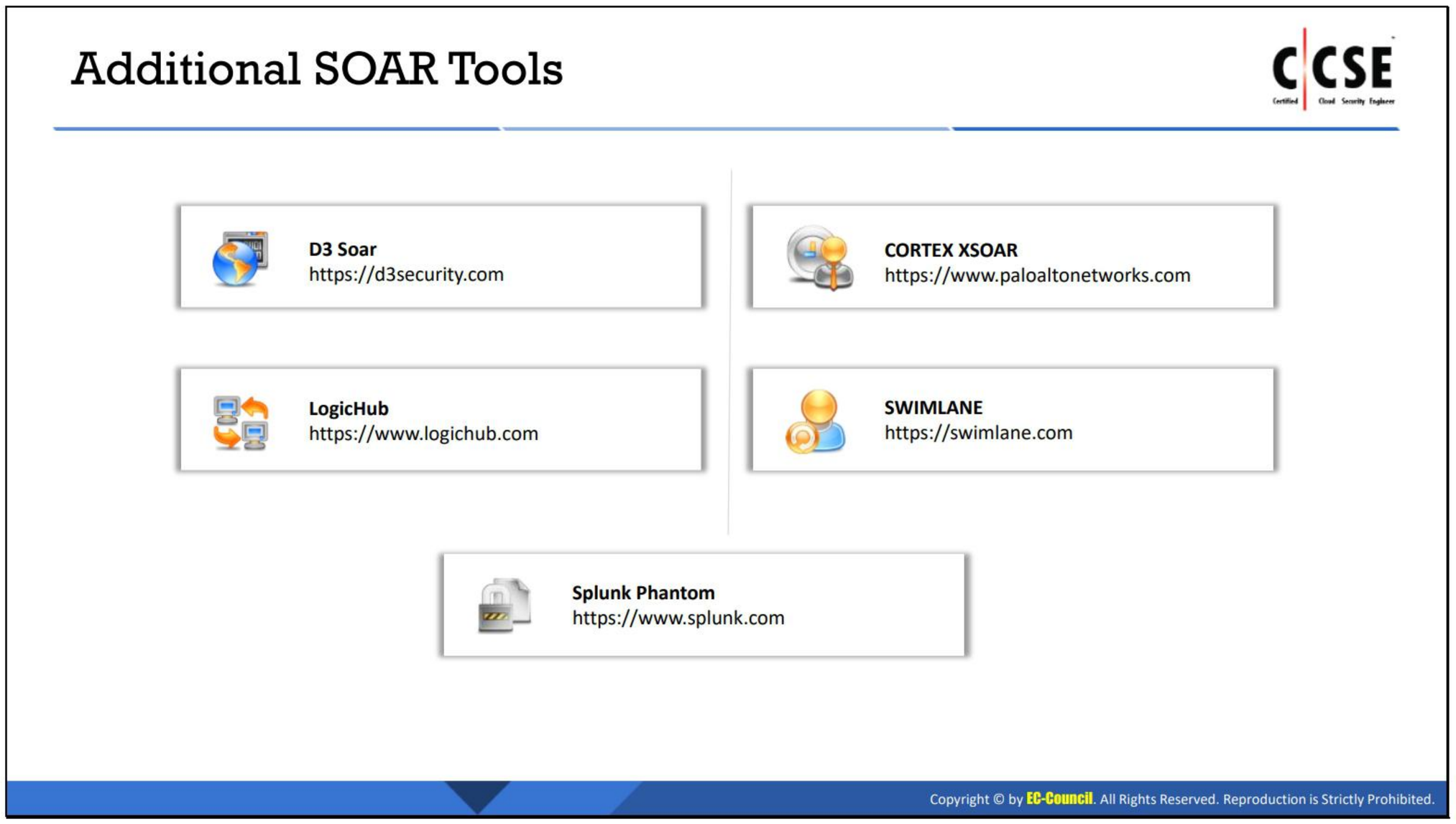
Source: https://www.rapid7.com

InsightConnect is a security orchestration and automation response (SOAR) solution by Rapid7 to streamline, fasten, and integrate time-consuming security processes.

The key features of InsightConnect are as follows:

- **Connect Your Tools**: Seamlessly connect your existing security tools with a library of 280+ plugins or import your own.
- **Build Automated Workflows**: You can also create workflows from scratch and customize them to meet your team's needs.
- **Utilize Human Decisions**: Automate manual, repetitive processes without giving up your decision-making power. Add human decision points to the automation workflow and empower your team to provide an expert insight when responding to critical security threats. With the automation of repetitive tasks, security personnel are free to focus on the strategic work they do best.
- **Improve Operational Efficiency**: Alert fatigue is real. Reduce the noise by automating your most repetitive tasks. False positives are vetted out quickly and threats are handled rapidly through the automation of enrichment tasks, investigation, and more. In addition, with automation, your team has the time and energy to play a more strategic and proactive role in protecting your organization from threats that matter the most.

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



Additional SOAR Tools

hide01.ir

D3 Soar

Source: https://d3security.com

D3 SOAR is a security orchestration and automated incident response tool with MITRE ATT&CK. You can coordinate across 260+ tools via codeless, drag-and-drop integrations and automate SOC tasks to reduce the response time by up to 95%. In addition, you can manage incidents with a library of adaptable, full lifecycle playbooks.

CORTEX XSOAR

Source: https://www.paloaltonetworks.com

CORTEX XSOAR is the industry's most comprehensive security orchestration, automation, and response platform with native threat intelligence management and a built-in marketplace. It will automate across your security stack, speed up incident investigations, break down team silos, and confidently act on threat intelligence.

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

LogicHub

Source: https://www.logichub.com

LogicHub provides a comprehensively deep detection, autonomous triage, 24x7 expertise, and automated incident response at a fraction of the associated costs. It monitors everything, integrates every tool in your security stack, detects deep threats mapped to an ATT&CK framework, fully enriches cases and not noisy alerts, responds to incidents with single-click automated actions, and automates playbooks and routine tasks.

Swimlane

Source: https://swimlane.com

Swimlane manages and automates the tasks associated with responding to security alerts and incidents so that your team can focus on higher-value work. It streamlines and accelerates incident response with centralized event data and standardized workflows. Swimlane integrates your organization's security tools with your existing people and processes to orchestrate a faster and more effective incident response and threat management. It provides an insight into your SOC's productivity and efficacy with easily customizable dashboards, granular reporting, and extensive visualization capabilities.

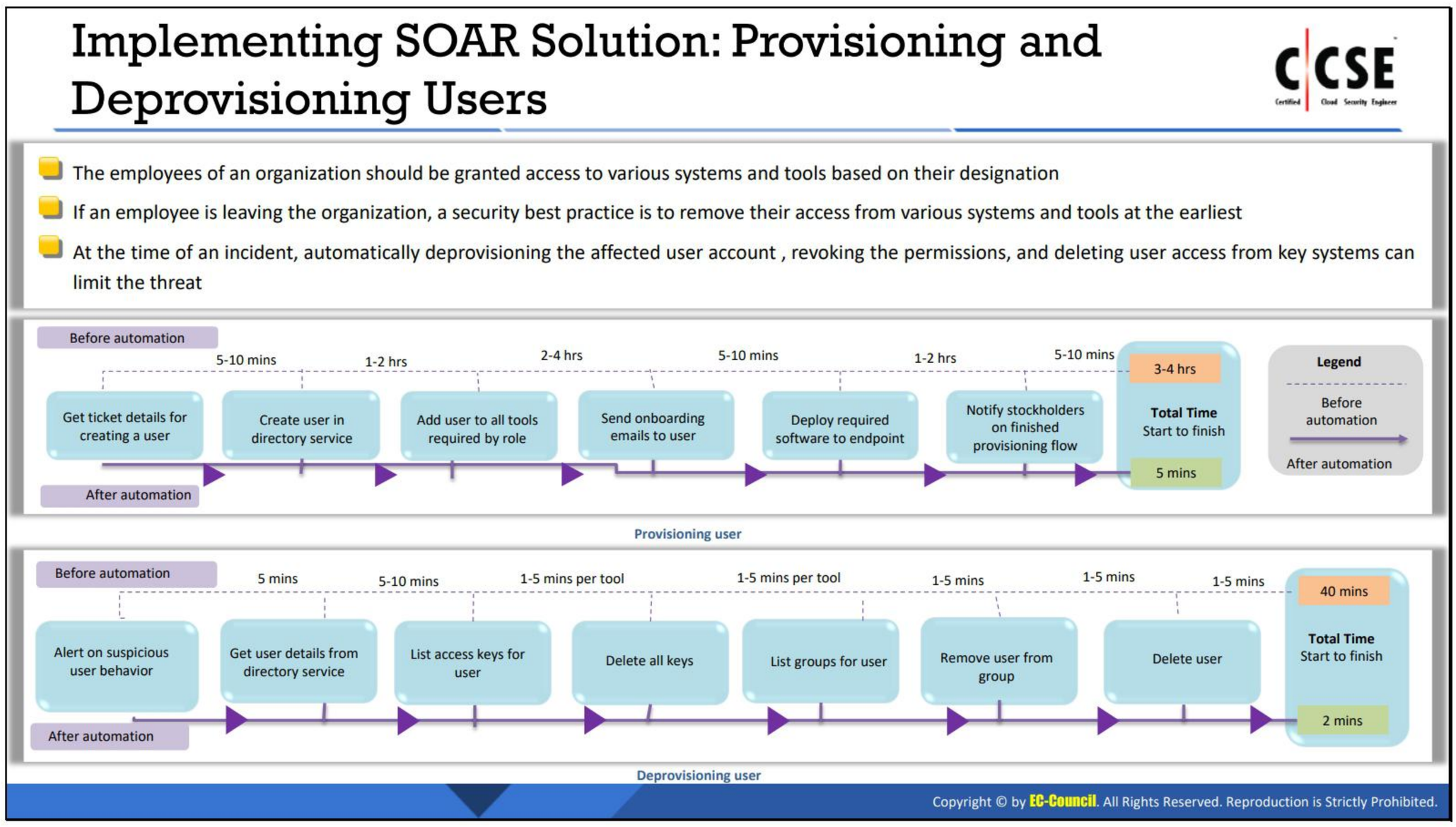
Splunk Phantom

Source: https://www.splunk.com

Splunk Phantom automates repetitive tasks to force-multiply your team's efforts and better focus your attention on mission-critical decisions. It reduces dwell times with automated investigations. It can reduce response times with playbooks that execute at machine speed. Moreover, it integrates your existing security infrastructure so that each part can actively participate in your defense strategy.

ir

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



Implementing SOAR Solution: Provisioning and Deprovisioning Users

Before using the SOAR solution, it is recommended to define the pain points that the organization wants to address. The next step is to define the most common use case or the task that the organization team spends the most time on. For instance, some organizations benefit from automating the handling of malware incidents because it is their biggest concern, whereas some organizations benefit from orchestrating threat hunting to manage the increased threats. To immediately benefit from SOAR, identify a use case to quickly resolve the problem and prioritize it.

Provisioning and Deprovisioning Users Using a SOAR Solution

User permission management is an important process that every organization must complete quickly for responding to security threats. The employees in an organization should be granted access to various systems and tools based on their designation. If an employee leaves the organization, a security best practice is to remove their access from various systems and tools at the earliest. Security and IT teams should immediately deactivate the account of an employee leaving the organization through a single automated workflow.

The attacker exploits the user's account through phishing attacks. A security analyst can use the SOAR solution at the time of the incident to limit the spread of a threat by automatically deprovisioning the affected user account, revoking the permissions, and deleting user access from key systems. Some widely used plugins for this purpose are AWS IAM, AD/LDAP, JIRA, etc.

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

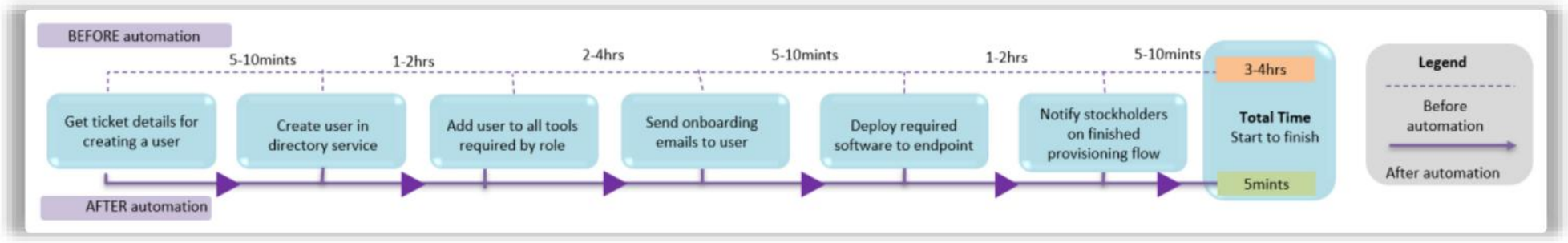


Figure 7.7: Provisioning User

For provisioning users in the RAPID7 SOAR solution, obtain the ticket details for creating users, and then create a user in a directory service. Then, based on their designated role, grant access to the required tools. Then, send onboarding emails to the user and deploy the required software to the endpoint. Finally, notify the stakeholders about the end of the provisioning flow.

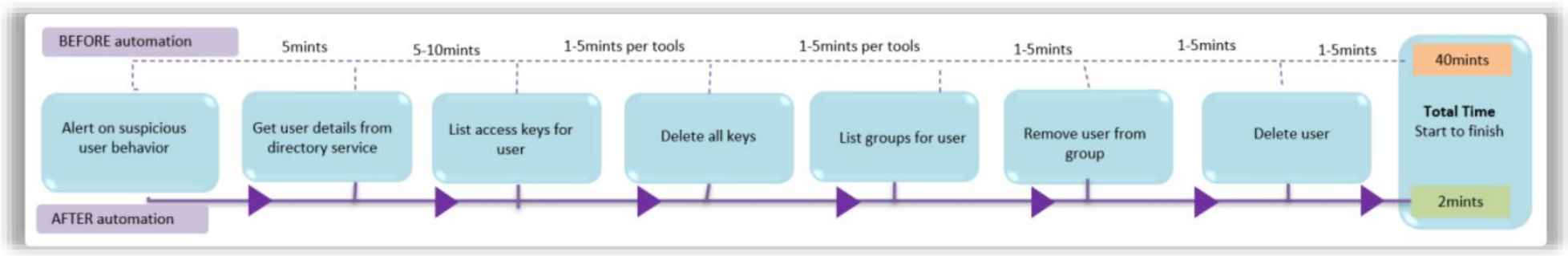
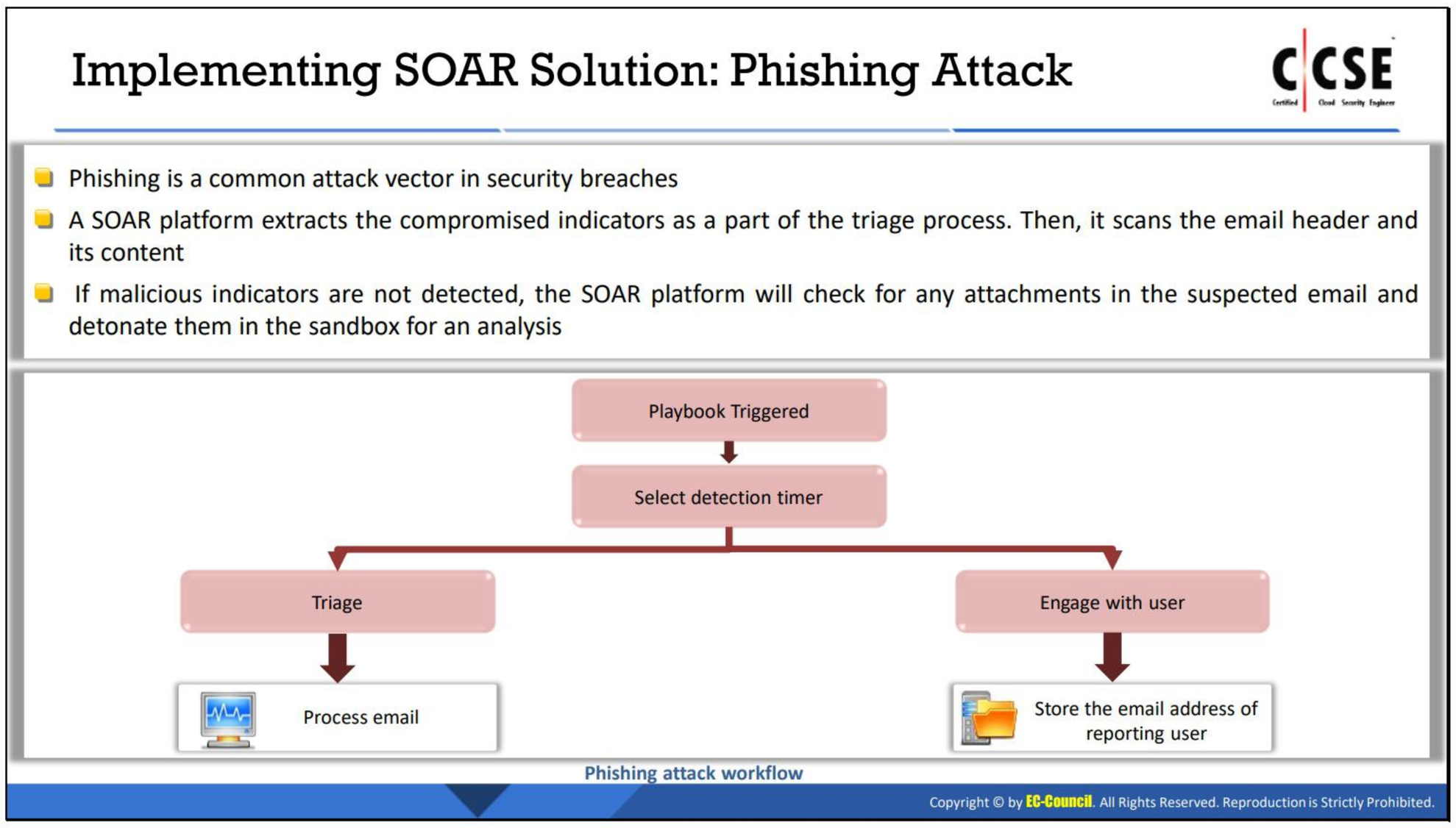


Figure 7.8: Deprovisioning User

For deprovisioning users in RAPID7 SOAR solution, after obtaining an alert on suspicious user behavior, obtain the user details from directory service, list all access keys for users, and then delete them. Next, remove the user from all listed groups they belong to. Finally, delete the user.

hide01ir

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



Implementing SOAR Solution: Phishing Attack

In most security breaches, phishing is a common attack vector. Investigating phishing emails is a time-consuming task, which involves checking URLs, investigating attachments, checking suspicious requests for sensitive information, etc. Apart from this, the volume of phishing attacks has been increasing continuously, and the security team spends a lot of time in identifying and remediating such attacks.

A SOAR platform extracts the compromised indicators as a part of the triage process. Then, it performs a scan on the email header and its content. Later, the email data is assigned an incident severity value and checked against external threat intelligence databases for reputation red flags. On detecting malicious indicators, it intimates the affected users about the remediating steps.

If malicious indicators are not detected, the SOAR platform will check for any attachments in the suspected email and detonate them in the sandbox for an analysis. If there are no malicious indicators in the email, the SOAR platform sends the incident to the IT security team for a manual investigation. The security team categorizes the email as not malicious if satisfied with its analysis. The SOAR platform will then send an email to the recipient stating that the email is a false alarm.

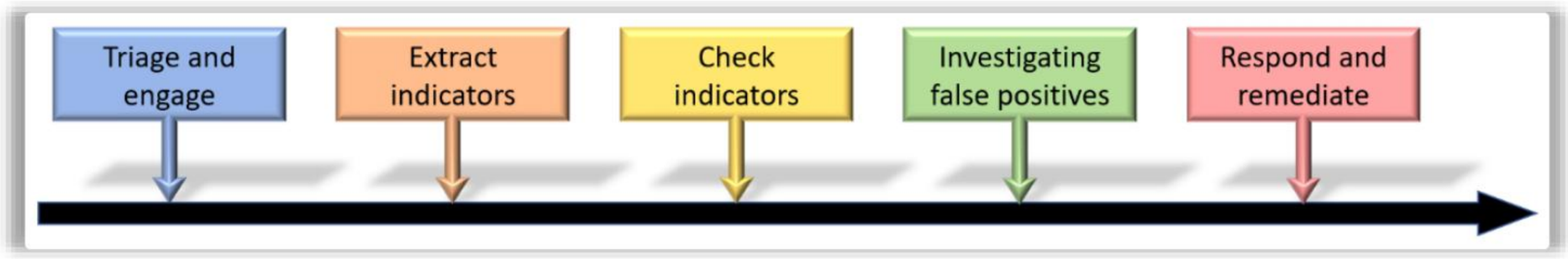


Figure 7.9: SOAR Platform Process

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

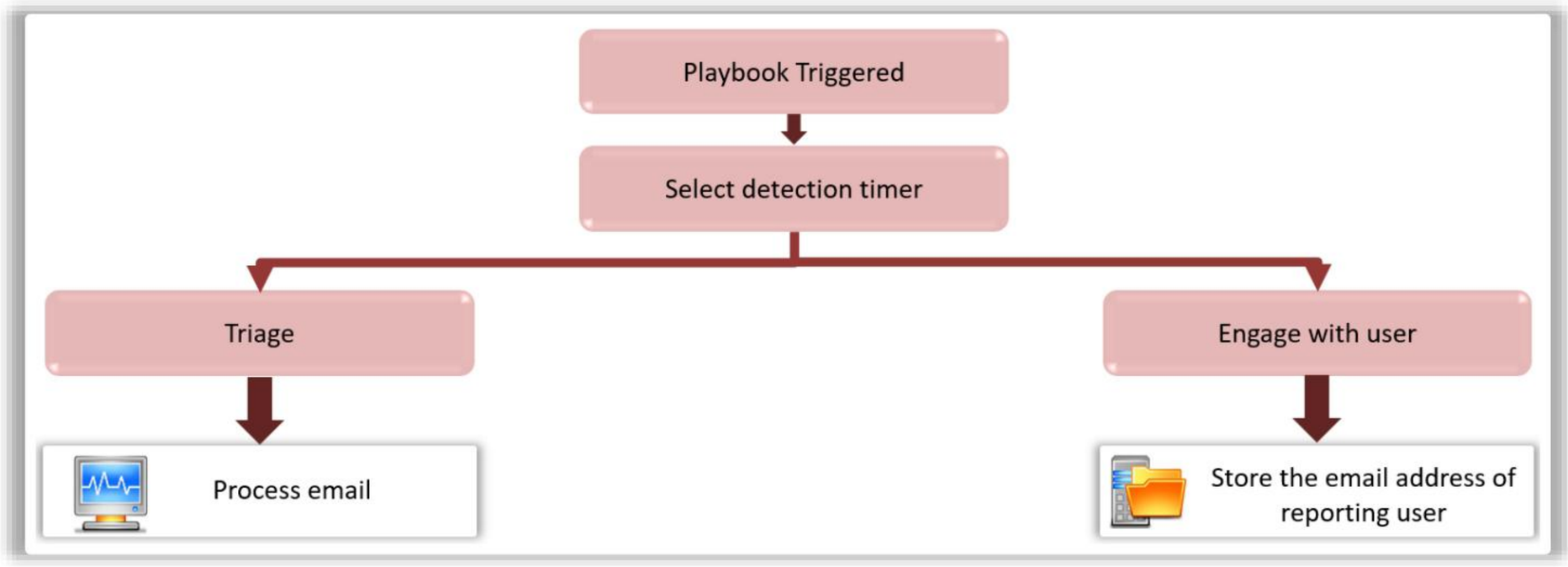


Figure 7.10: Phishing Attack Workflow

Triage and Engage

If any employee sends a suspected phishing email, it is considered malicious until proven otherwise. The employee should be apprised with an email receipt. An initial triage will help in determining the intensity of the phishing attack.

Extract Indicators

Start the investigation by obtaining common indicators that help in breaking down the phishing email into constituent parts. Obtain the URL and IP address from the email.

Check Indicators

After extracting the indicators, check whether they are malicious by enriching them with a reputation from the integrated security tools. The data can be enriched with a reputation from sources such as URL, IP, and files.

Investigate False Positives

This task is automated to increase its robustness and reduce an analyst's manual effort. The steps involved in investigating false positives are as follows:

- Execute a check-in sandbox if you do not find any malicious indicator in the initial checks
- Manually check the similarity between the sender's and the company's domains in case the sandbox results are positive.
- Check the hostname URL if you do not find anything suspicious in the domain.
- In case the email has cleared all tests, perform one more round of manual investigation; if required, take the help of another security analyst.
- If nothing malicious is observed, finish the investigation and email the employee stating the email is safe.

Responding to the Verified Phishing Attempt

The analyst should respond quickly to a verified phishing attempt. The email attachment should be investigated thoroughly to detect further threats and limit the spread of the attack. The

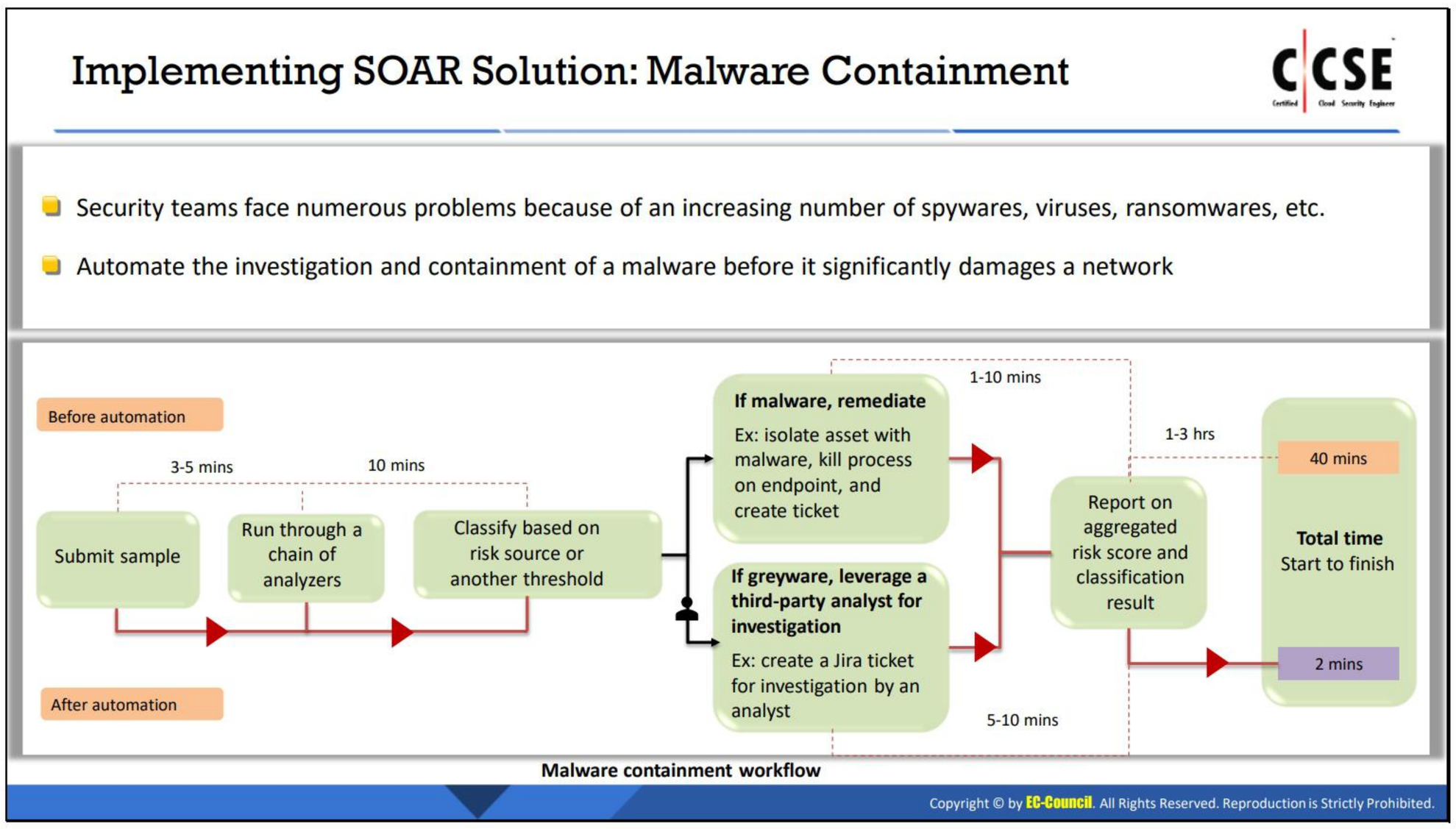
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

confirmed malice should be notified to all employees. The steps involved in responding to a verified phishing attempt are as follows:

- Send an email to the employees to notify that the email is malicious
- Search other mailboxes and delete all phishing emails
- In case the email has an attachment and has been extracted, utilize the tools to check the extracted file for malicious indicators of compromise (IoC).
- If the email does not have any attachments, close the investigation.

hide01.ir

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



Implementing SOAR Solution: Malware Containment

Security teams have been facing numerous problems due to increasing spyware, viruses, ransomware, etc. Perform automation for the investigation process and contain the malware before it causes significant damage to the network. Malware containment for a SOAR solution involves:

Malicious Activity Identification: Look for the signs of a malware and take the necessary steps to stop its spread. The processes should be automated to detect indicators such as an abnormal log activity or misspelled process names.

Threat Investigation: Analyze a detected malware using the latest plugins for sandbox tools and malware analysis solutions. This will allow you to check the malicious file in a safe environment. The most commonly used plugins are Cuckoo, JIRA, Cortex, and VirusTotal.

Containment and Removal: Perform containment or removal actions on all identified malwares. Using automation, identify the affected users and assets, leave a decision point for a security analyst to delete the affected user accounts, separate the malware, and remove the machine connected to the network.

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

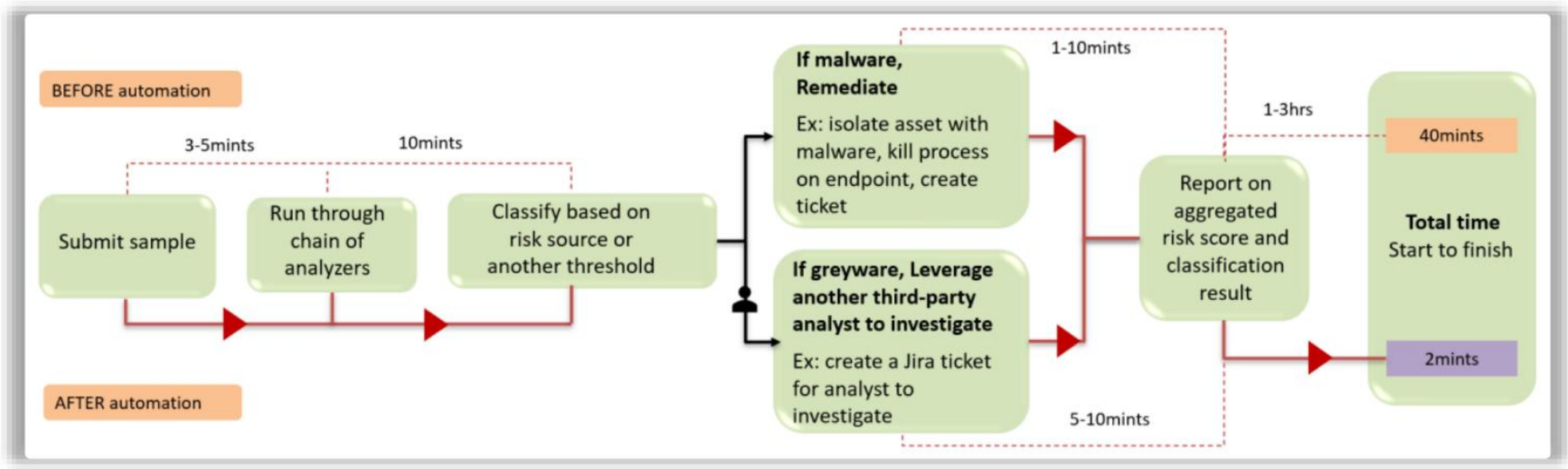
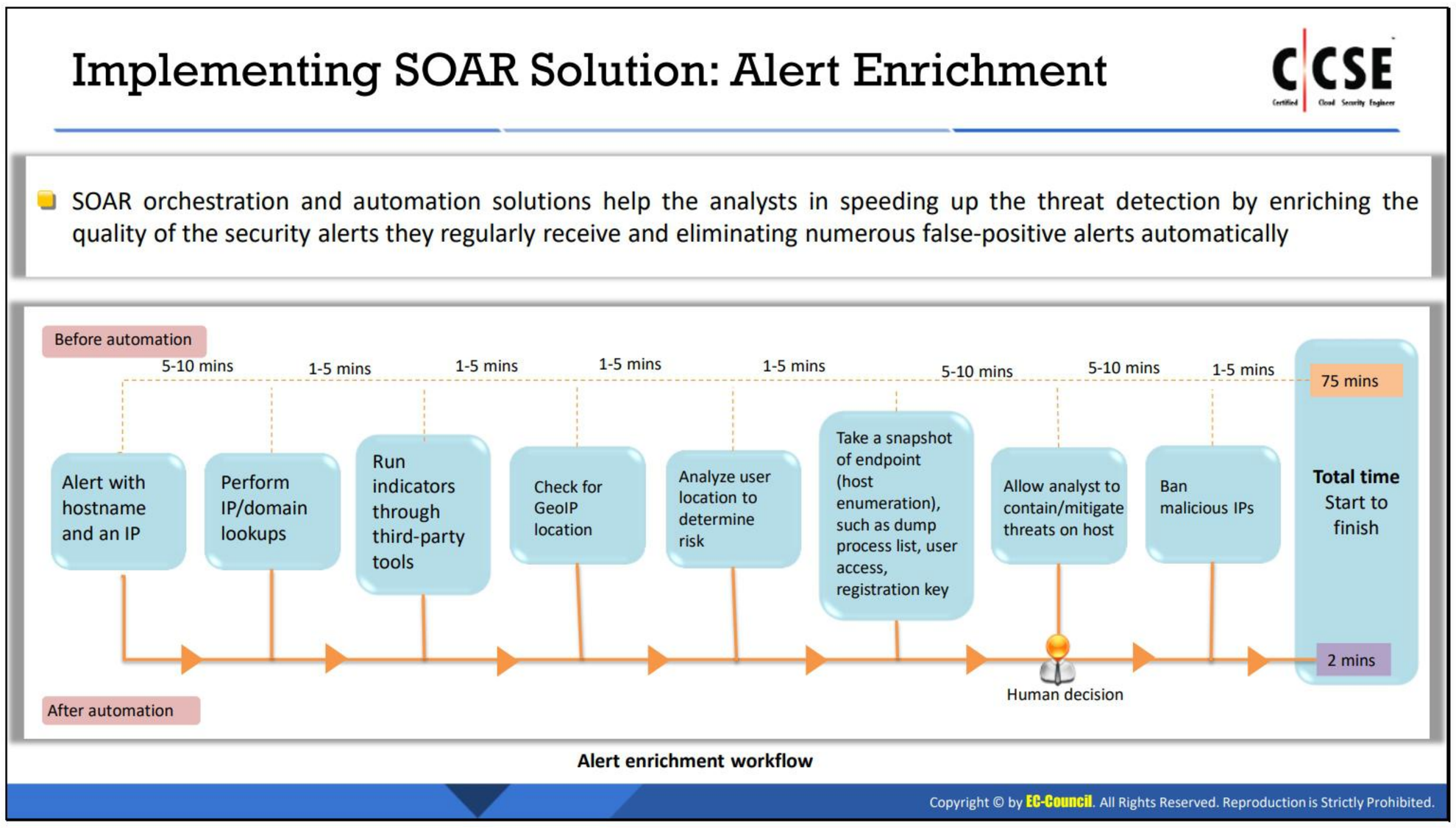


Figure 7.11: Malware Containment Workflow

For malware containment in the SOAR solution, the submitted sample should go through a chain of analyzers. Based on its risk score, the sample will be classified as a malware, greyware, etc. If identified as a malware, remediations steps such as isolating the asset with malware, creating a ticket, and killing processes on endpoints, will be performed. If identified as a greyware, it will be sent to other third-party analysis tools or for a human intervention. The classification results and aggregated risk scores of malwares and greyware will be analyzed and a suitable action will be initiated.

hide01.ir

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



Implementing SOAR Solution: Alert Enrichment

On an average, every enterprise security operation center (SOC) has 75 distinct security tools. Switching among different tools regularly because of SIEM alerts is tedious and the SOC Tier 1 analysts often fail to initiate an appropriate action on the actual threats. SOAR orchestration and automation solutions help the analysts hasten the threat detection by enriching the quality of the security alert they regularly receive and eliminating numerous false-positive alerts automatically. Thus, SOAR solutions provide a good amount of time and context to SOC analysts to deal with an actual threat.

The security team regularly receives thousands of alerts. The SOAR solution automatically collects and compiles the relevant context of a security event. This allows the security team to focus on analysis and response rather than spending a significant amount of time to manually collect the security event data.

SOAR solutions help in optimizing the operations by automating repetitive tasks. It will minimize the noise. With a SOAR solution automating enrichment tasks, the security analyst can remove false-positive alerts quickly and respond immediately to threats.

With a SOAR solution, the analyst enriches the security alerts automatically with essential information such as domain analysis, geo-IP lookups, and malware detonation. Apart from this, the analyst can also orchestrate a suitable threat intelligence platform and use various free and open-source tools to initiate an appropriate action on the threat. For alert enrichment, the analyst can use various plugins such as GeoIP2 Precision, DomainTools, and AbuseIPDB.

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

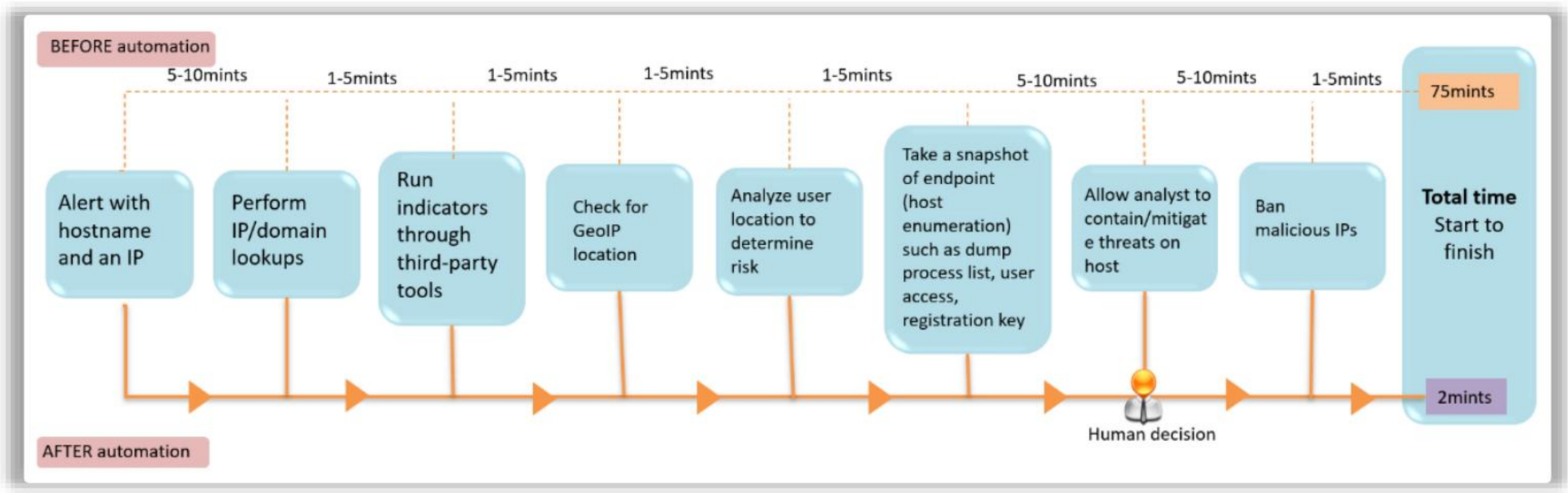
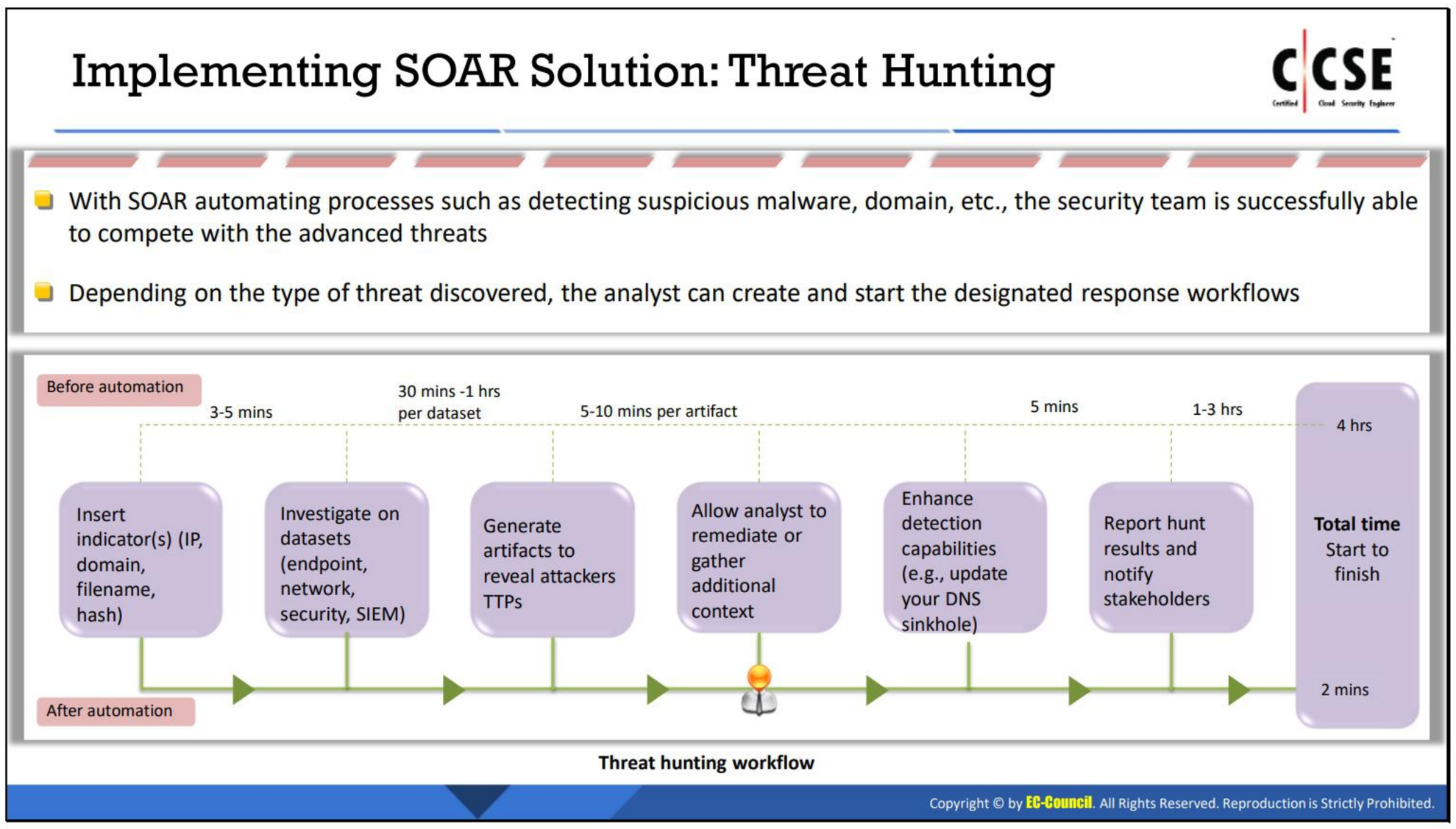


Figure 7.12: Alert Enrichment Workflow

For alert enrichment in the RAPID7 SOAR solution, the analyst needs to perform IP/domain lookups after receiving an alert with a hostname and an IP. The analyst will run the indicators through third-party tools, check for GeoIP location, and analyze the user location to determine the risk. Then, they will take a snapshot of the endpoint. Finally, they will contain or mitigate the threats to the host and ban the malicious IPs.

hide01.ir

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



Implementing SOAR Solution: Threat Hunting

Threat hunting is a time-consuming process and requires a highly skilled analyst. By being proactively involved in threat hunting, the analyst can safeguard and defend their organization against advanced persistent threats (APTs). With SOAR automating processes such as the detection of suspicious malware and domains, the security team can successfully tackle the advanced threats.

Threat hunting does not have any boundary; the more datasets that can be collected and analyzed, the more information about the threat that can be obtained to proactively defend the organization. With SOAR orchestration, the analyst would add various tools to the datasets for a robust threat hunting.

All he tasks associated with threat hunting can be automated with SOAR solutions. Thus, the security team gets more time to detect and prevent an attack. Depending on the type of the discovered threat, the analyst can develop and initiate the designated response workflows. This will ensure the security team follows an appropriate protocol and all stakeholders are notified at the earliest.

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

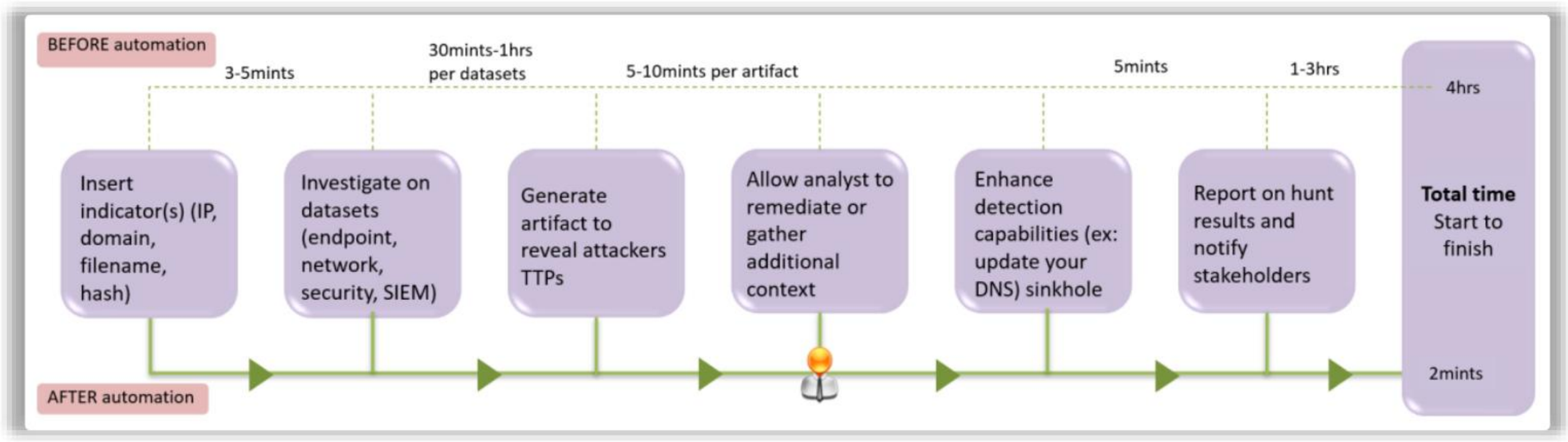
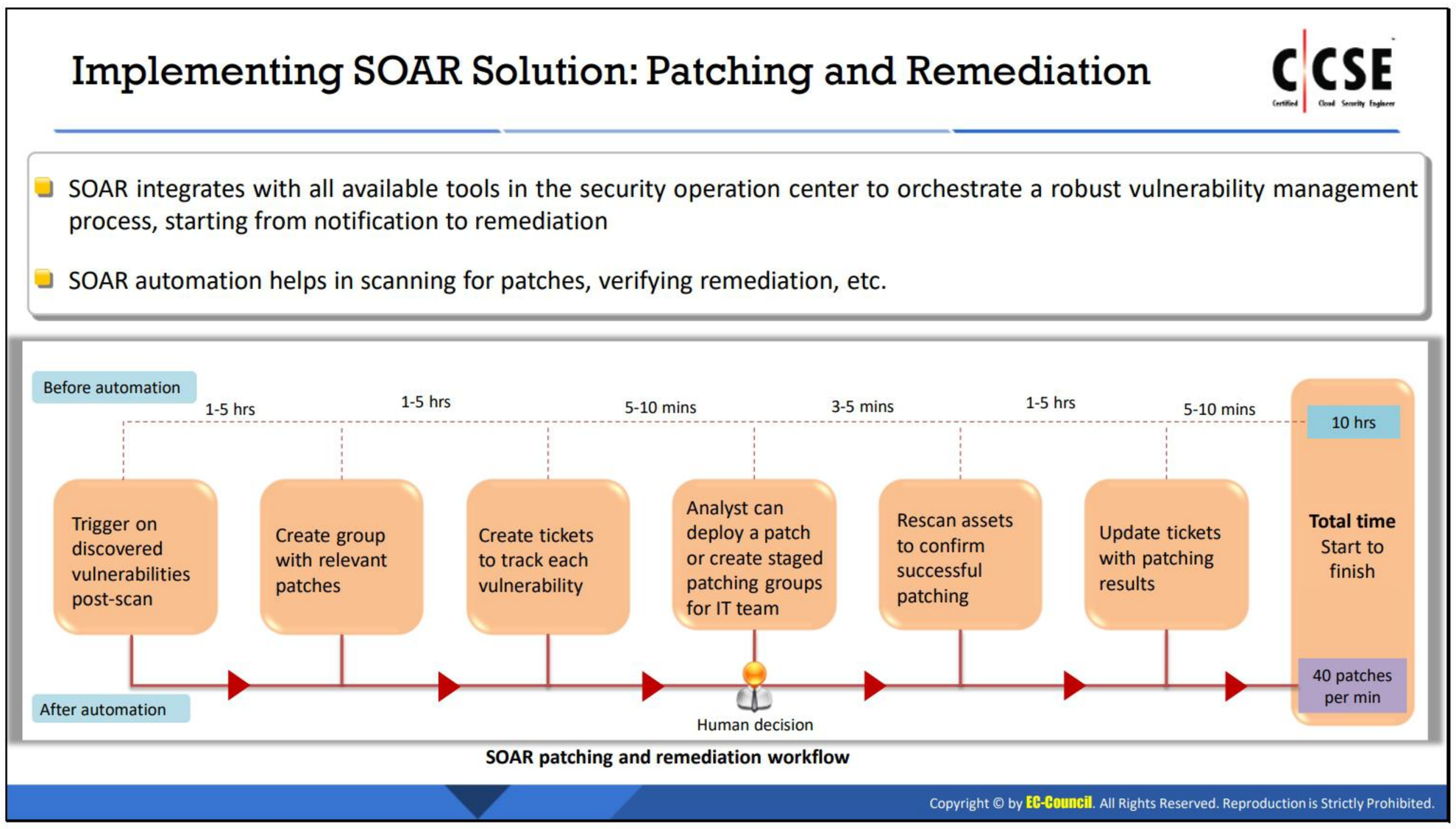


Figure 7.13: Threat Hunting Workflow

For threat hunting in RAPID7 SOAR solution, insert indicator(s) such as IP, domain, and file name/hash, and then investigate the datasets. Artifacts can be generated to reveal attacker TTPs followed by either a remediation or a collection of additional context. It can enhance the detection capabilities, report the hunt results, and notify the stakeholders as quickly as possible.

hide01.ir

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



SOAR patching and remediation workflow

Implementing SOAR Solution: Patching and Remediation

Today, security teams face numerous vulnerabilities in their environment and remediating each of them takes a significant amount of time. This leads to a mounting backlog, unintentionally neglected issues, and an increased vulnerability of organizations because certain actions are not initiated promptly.

A SOAR solution integrates with all available tools in the SOC to orchestrate a robust vulnerability management process, starting from notification to remediation. It ensures all critical issues are addressed appropriately and adds human decision points to address the most critical ones. SOAR automation helps in scanning and finding patches, verifying remediation, etc.

SOAR automation solution allows the analyst to create workflows for automatically monitoring the advisory list through RSS feed plugins. The analyst can set up decisions and action points wherever necessary.

If any vulnerability needs to be addressed, the SOAR solution automatically creates service tickets and notifies the stakeholders. SOAR solution automation allows the security team to respond effectively and efficiently within a specified timeframe. For patching and remediation, the widely used plugins are JIRA, Microsoft SCCM, ServiceNow, and IBM BigFix.

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

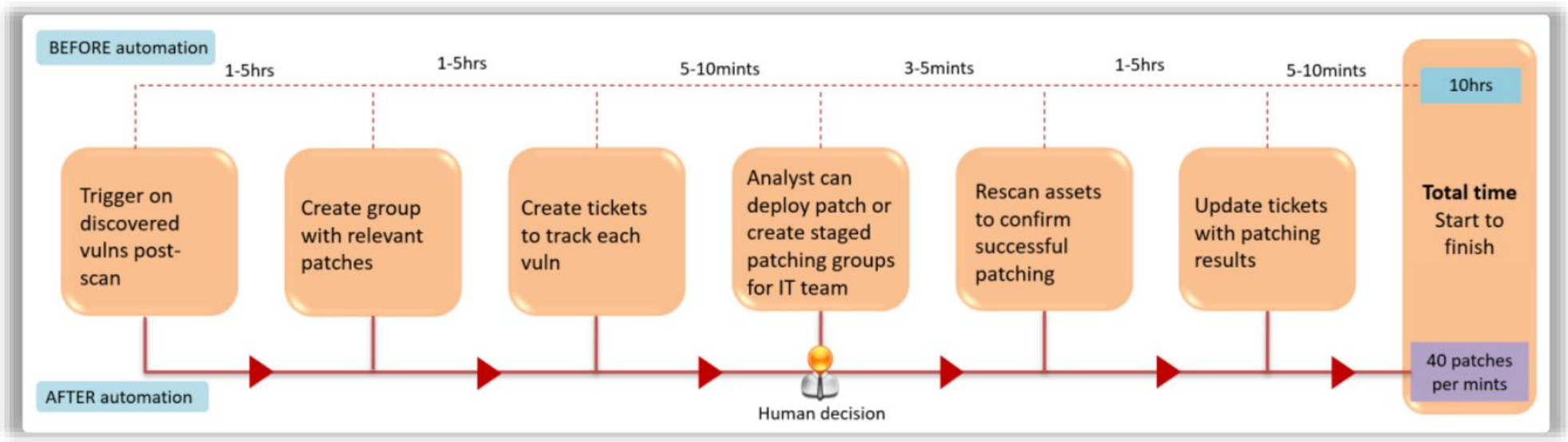


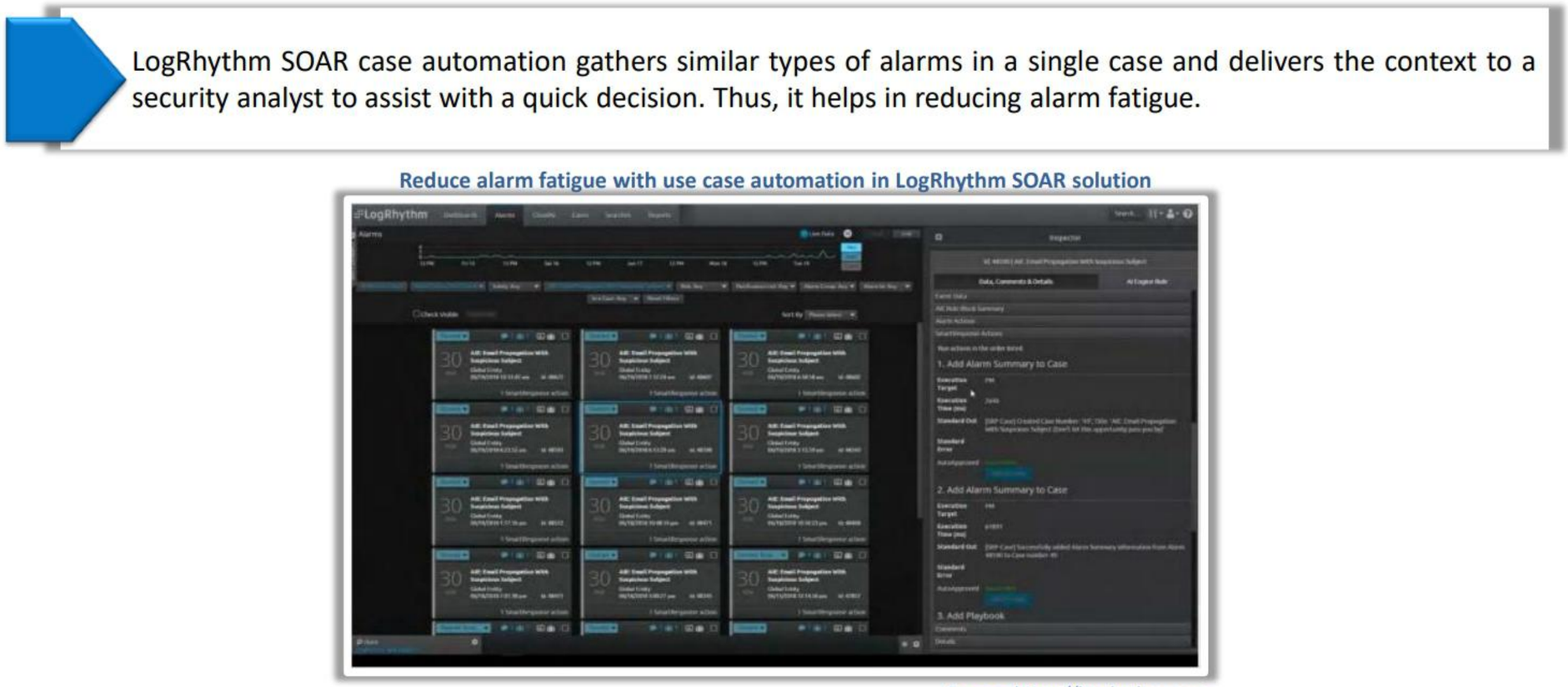
Figure 7.14: SOAR Patching and Remediation Workflow

For patching and remediation in the RAPID7 SOAR solution, after discovering vulnerabilities on a post-scan, the security analyst needs to create a group with the relevant patches and then create tickets to track each vulnerability. They can deploy a patch or create a staged patching group for the IT team, and then rescan the assets to confirm a successful patching. Finally, they can update the tickets with the patching results.

hide01.ir

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

Implementing SOAR Solution: Reduce Alarm Fatigue with Use Case Automation



LogRhythm SOAR case automation gathers similar types of alarms in a single case and delivers the context to a security analyst to assist with a quick decision. Thus, it helps in reducing alarm fatigue.

Reduce alarm fatigue with use case automation in LogRhythm SOAR solution

Source: https://logrhythm.com

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

Implementing SOAR Solution: Reduce Alarm Fatigue with Use Case Automation

Source: https://logRhythm.com

hide01.ir

Handling thousands of alarms regularly is a tedious task for a security analyst. The security analyst does not have the time to investigate and triage alarms that would turn out to be false positives. LogRhythm SOAR case automation gathers similar types of alarms in a single case and delivers the context to the security analyst for a quick decision. Thus, it helps in reducing alarm fatigue. LogRhythm integrates the SIEM and SOAR solutions to help the security team tackle threats quickly from a unified interface.

In case an alarm is triggered overnight, the security analyst will need the correct information to initiate an action. Using LogRhythm's SmartResponse automation, the analyst can automatically collect the important details and set up an action plan, thereby saving time.

The analyst can see 50 alarms for a similar campaign, but these alarms can belong to different users. The analyst does not have to waste time in investigating all alarms and creating 50 cases. The analyst just needs to aggregate the alarms with case automation, and then compress and attach them to the case automatically, which will reduce the alarm fatigue.

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

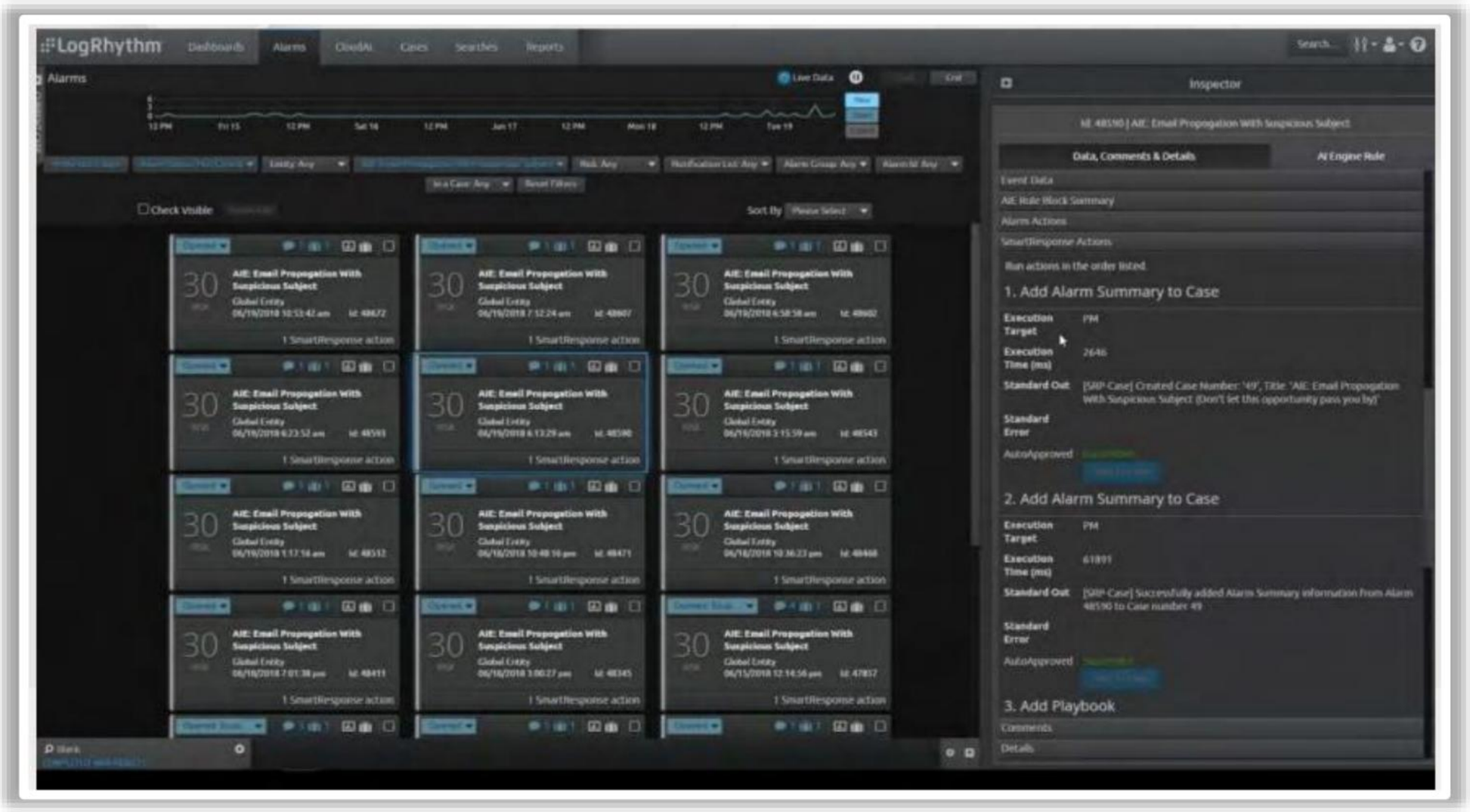


Figure 7.15: Reduce Alarm Fatigue with Use Case Automation

Using SmartResponse automation, the analyst can also group alarms from a similar campaign. Apart from this, the analyst can also review the automatically retrieved information such as alarm notes, email addresses, etc.

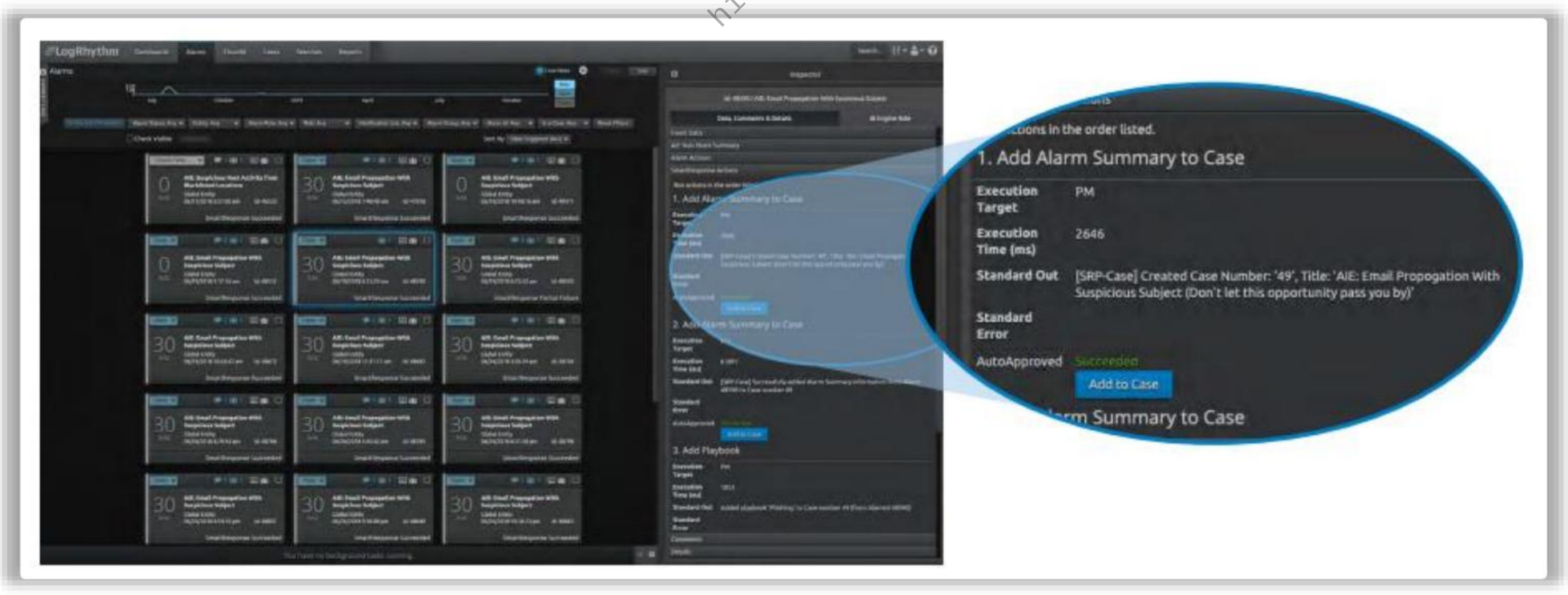


Figure 7.16: List of Alarms

Preapproved SmartResponse automation will generate the case automatically, add details and important tags to the case, allocate a Tier 1 analyst, and link the case with the suitable playbook to deliver a robust response.

The analyst can also include their colleagues to assist with a case. If the analyst adds their colleagues to a case, they will be notified of it.

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



Figure 7.17: Adding an Analyst to the Case

hide01.ir

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

Implementing SOAR Solution: Streamline the Security Operations Workflow

- The organization should streamline its security operations workflow to attain a lower MTTD and MTTR
- LogRhythm SOAR solution utilizes PowerShell scripts that change the email alerts into text logs and utilize AI to automatically send a notification
- LogRhythm SOAR solution minimizes the MTTD and MTTR from hours to minutes



SaaS alert showing malware-affected email

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

Implementing SOAR Solution: Streamline the Security Operations Workflow

The speed of threat detection and response plays a pivotal role in safeguarding an organization against a threat. Therefore, measuring the detection and response time to a threat is important. An organization should streamline its security operations workflow to attain a lower MTTD and MTTR.

For instance, a multinational bank can use a SaaS email security solution for scanning all inbound emails to detect email-borne malware and phishing attacks, but it may not have usable log messages of these alerts. Entirely depending on emails for incident alerts can be problematic.

LogRhythm SOAR solution utilizes PowerShell scripts that change the email alerts into text logs and utilize AI to automatically send a notification. The AI technology of LogRhythm has a SmartResponse action, which creates a case automatically. The details of the case are immediately populated for providing critical information to an analyst. Without using any additional applications, the LogRhythm SOAR solution minimizes the MTTD and MTTR from hours to minutes.

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

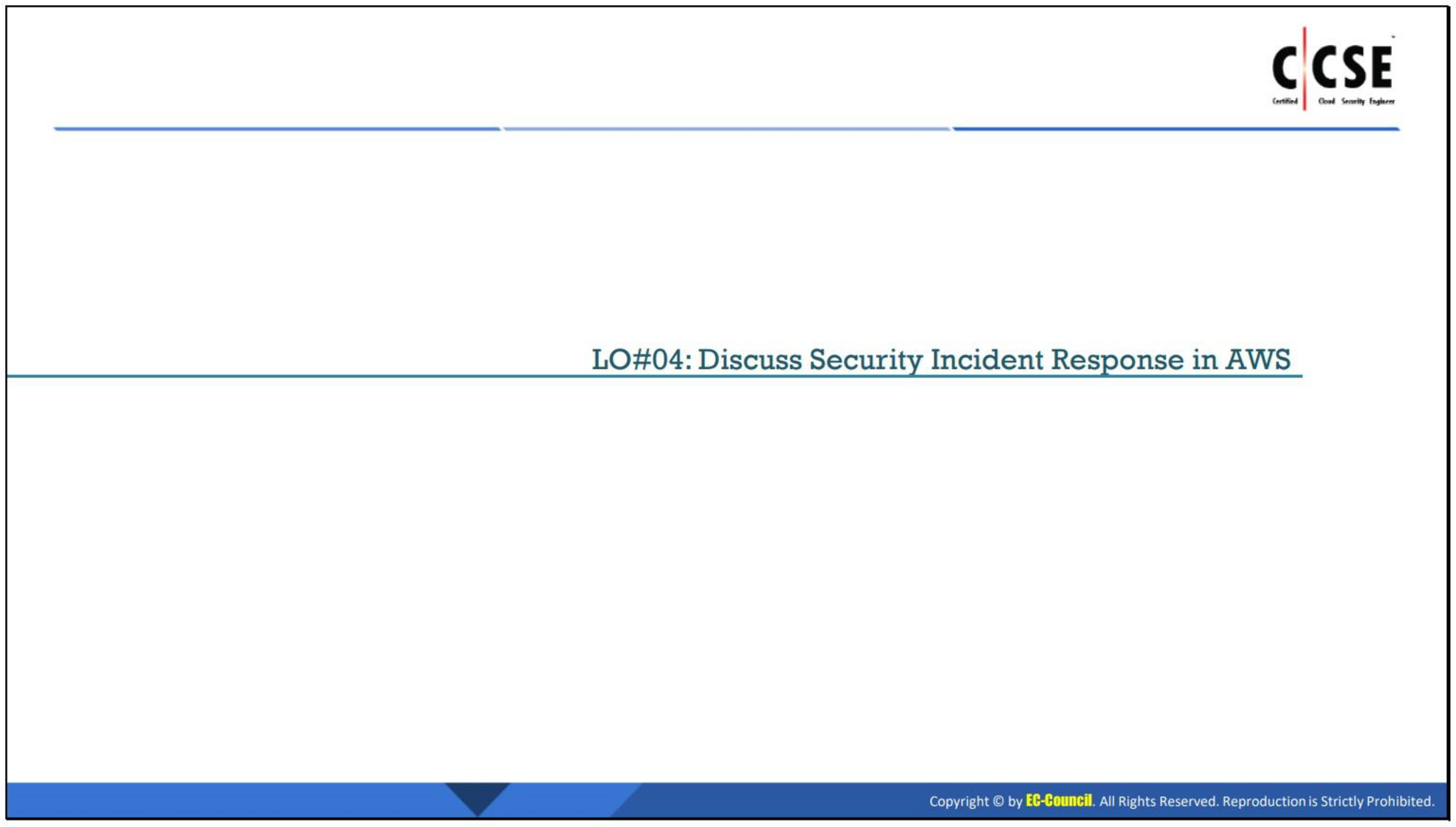
Given below is a SaaS alert showing malware-affected email:



Figure 7.18: Malware Affected Email

hide01.ir

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

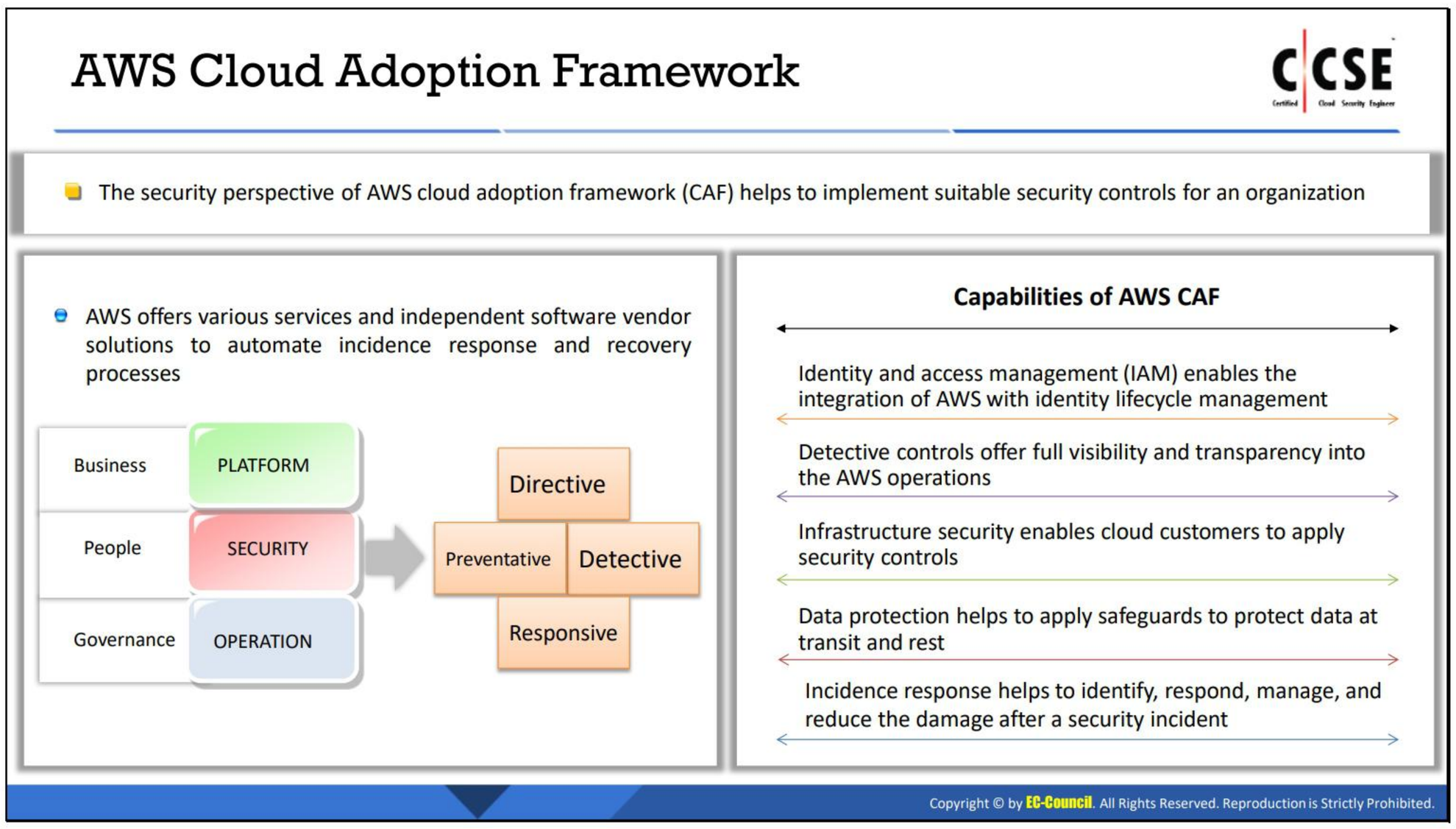


LO#04: Discuss Security Incident Response in AWS

The objective of this section is to explore the various features provided by AWS for incident response. The section explains the AWS cloud adoption framework (CAF) and shows how to implement an incident response plan in AWS.

hide01.ir

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



AWS Cloud Adoption Framework

AWS cloud adoption framework (CAF) is responsible for guiding the coordination between various parts of an organization planning to migrate to the cloud. The security perspective of AWS CAF helps cloud consumers implement appropriate security controls in their organization.

AWS CAF Security Perspective Capabilities

AWS CAF security perspective offers various capabilities, as listed below:

- Identity and incident management (IAM) enables the administrator to create appropriate roles and policies associated with relevant users and groups.
- Detective controls help make the AWS operations completely transparent and visible.
- Infrastructure security enables cloud customers to apply security controls.
- Data protection provides the ability to control the data and how it can be accessed and used in the organization.
- Incidence response helps cloud customers identify, respond, manage, and reduce the damage after a security incident. By engaging the AWS environment with an existing security posture and preparing simulated actions, the administrators will be prepared to respond to incidents when they occur.

AWS offers various services and independent software vendor solutions to automate incidence response and recovery processes. With an automated incident response and recovery in place, the security team can shift its focus from response to forensics and root cause analysis.

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

Simulating the occurred events helps determine if the established security controls and processes are reacting as expected. It also helps determine if the system can recover and respond to the events when they occur.

AWS CAF Capabilities Categories

AWS CAF capabilities are categorized into the following:

- **Business Capabilities:** These include business, people, and governance perspectives.
- **Technical Capabilities**: These include platform, security, and operational perspectives.

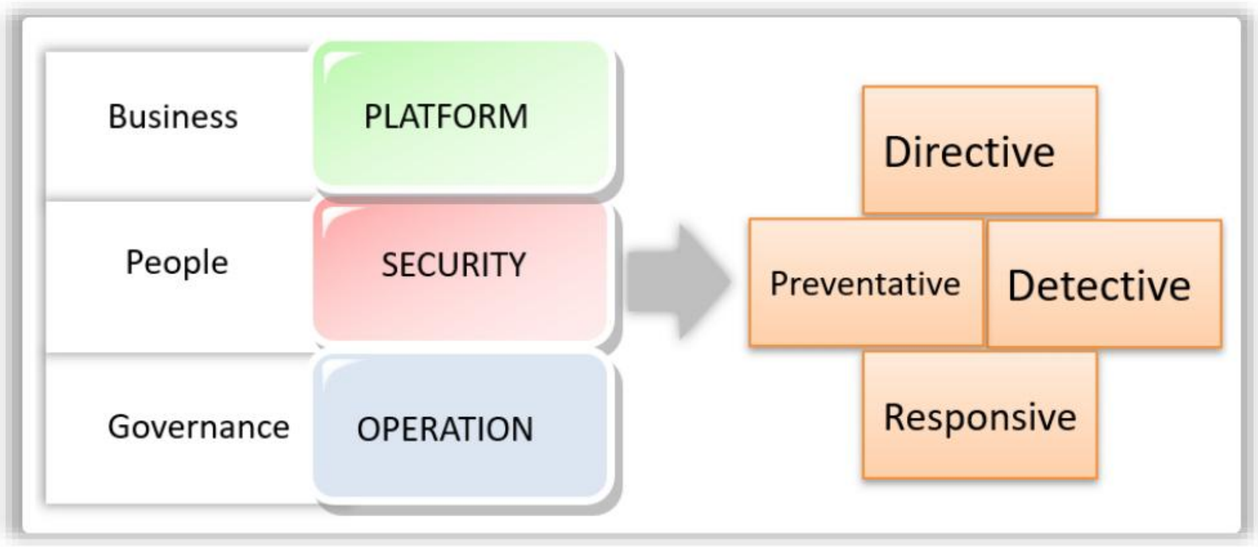


Figure 7.19: AWS CAF Capabilities Categories

AWS CAF Perspectives and Their Areas of Focus/Common Roles

AWS CAF perspectives and their areas of focus/common roles are shown in the table below.

hidego.ir

Perspective	Area of Focus
Business	Business support capabilities to optimize business value with cloud adoption Common roles: business manager, finance manager, budget owners, strategy stakeholders
People	People development, training, communications, and change management Common roles: human resources, staffing, people managers
Governance	Managing and measuring resulting business outcomes Common roles: CIO, program managers, project managers, enterprise architects, business analyst, portfolio managers
Platform	Develop, maintain, and optimize cloud solutions and services Common roles: CTO, IT managers, solution architects

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

Operations	Allow system health and reliability through the move to cloud and deliver an agile cloud computing operation Common roles: IT operations managers, IT support managers
Security	Ensure the workloads deployed or developed in the cloud align with the organization's security control, resiliency, and compliance requirements Common roles: CISO, IT security managers, IT security analysts, head of audit and compliance

Table 7.1: AWS CAF Perspectives and Their Areas of Focus

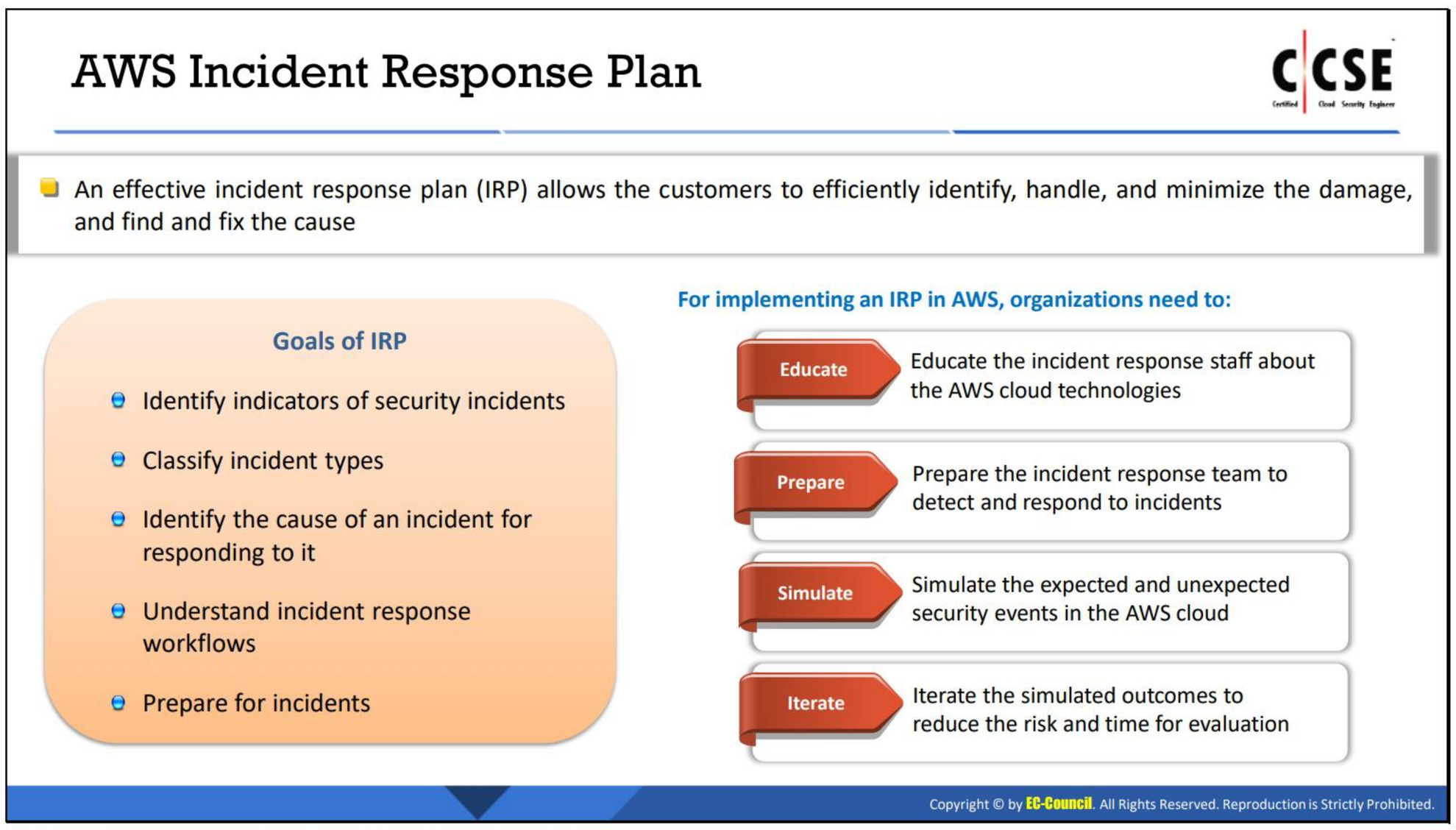
Security Perspective Components

The security perspective components organize the principles to drive the transformation of an organization's security posture. These components include the following:

- **Directive Controls:** These controls can set up governance, risk, and compliance models within the operational environment.
- **Preventive Controls:** These controls can secure workloads to help minimize vulnerabilities and threats.
- **Detective Controls:** These controls add transparency and provide a complete visibility into the AWS deployment operations.
- **Responsive Controls**: These controls can remediate the potential deviations from security baselines.

hide01.ir

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



AWS Incidence Response Plan

AWS is responsible for handling the security of the cloud, whereas cloud consumers are responsible for handling the security in the cloud. If there is any deviation from the security baseline, the cloud customers need to investigate and respond to those incidents. Incident response in AWS is a method of handling security issues or incidents, data breaches, and cyberthreats. An effective incident response plan (IRP) allows the customers to efficiently identify, handle, and minimize the damage, and find and fix the cause.

For a successful IRP, the cloud customers should have a basic idea of incident response in AWS and the issues to be considered before an incident occurs. They should be aware of the capabilities and remediation methods to be used to improve the incident response speed.

Need for Security Incident Response and IRP in AWS

The benefits of an IRP include the following:

- The primary goals of any organization are the trust and reputation of their customers. It is essential to identify and respond to even small security incidents. Regardless of the size of the breach, it is necessary to have an IRP to handle the risks associated with cyberattacks.
- An IRP usually defines the incidents, roles of security teams, tools for handling breaches, required steps to be taken for handling a security incident, and how such incidents should be investigated and communicated.
- If a security breach is not handled quickly, the trust of the customers would be affected, which may lead to a loss of confidence in the organization. Investors and shareholders also lose trust after a data breach; hence, it is essential to have an IRP in place.

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

- A well-defined IRP not only protects the data but also safeguards the organization from a potential loss of revenue. The faster an organization detects and responds to a data breach, the less likely it is to impact data, company revenue, customer trust, and its reputation.

Goals of IRP

During a security incident, the incident response (IR) team faces several problems and may fail to follow a proper incident response procedure to reduce the damage. Therefore, an IRP should be prepared in advance to prevent any damage to reputation adverse business impact. The cloud customers should develop runbooks, use the basic capabilities, and build an incident response library to iterate and improve the incidence response accordingly.

Organizations with an IRP should do the following:

- Identify the indicators of security incidents
- Classify the incident types
- Identify the cause of an incident to respond to it
- Understand the incident response workflows
- Prepare for incidents

AWS IRP Implementation Steps

hideo1.ir

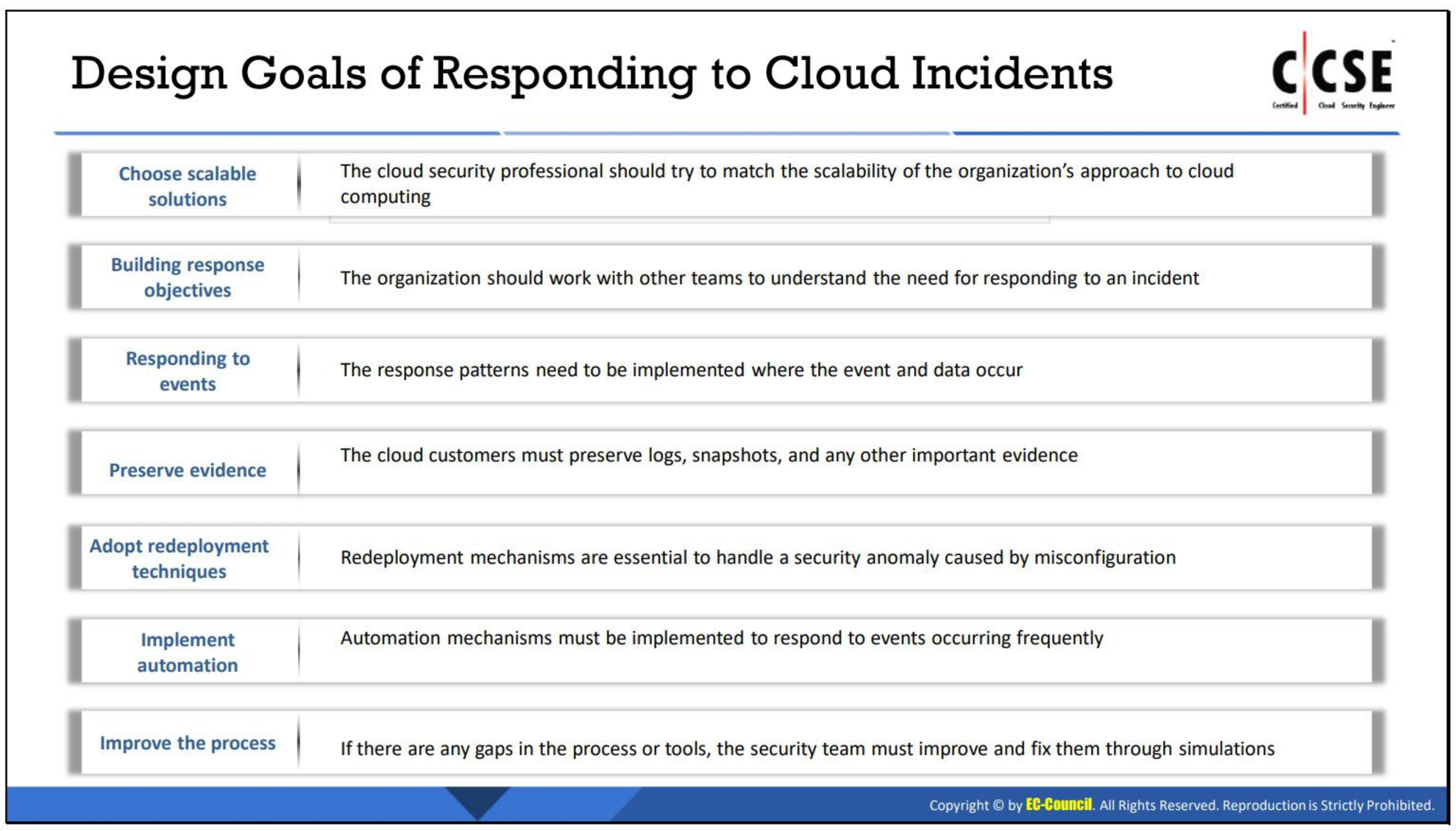
All users in the administration must be aware of the security incidence response in AWS. The security staff must also understand how to respond to security incidents. The IRP in AWS involves the following four steps:

- Educate
- Prepare
- Simulate
- Iterate

As the first step, educate the incident response staff about the AWS technologies. In the second step, detect and respond to the incidents. Now, simulate the expected and unexpected security events in the AWS cloud to ensure the developed process is working well. In the final stage, iterate the outcome of the simulation to improve the response posture and reduce the risk and time for evaluation.

For example, a user can log in into the AWS account using AWS API. The user identifies the events using the event logs generated by CloudTrail. The logs can be imported to the S3 bucket for storing the evidence. The user can make use of CloudWatch events to describe the changes in the AWS resources. By using AWS Lambda, the user can run a code for the CloudWatch events to generate responses. AWS Lambda automatically allocates the compute resources required by that code, such as allocating storage, generating notifications using simple notification service (SNS), etc. Now, the response team will be informed about the security events, and can execute the required actions.

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

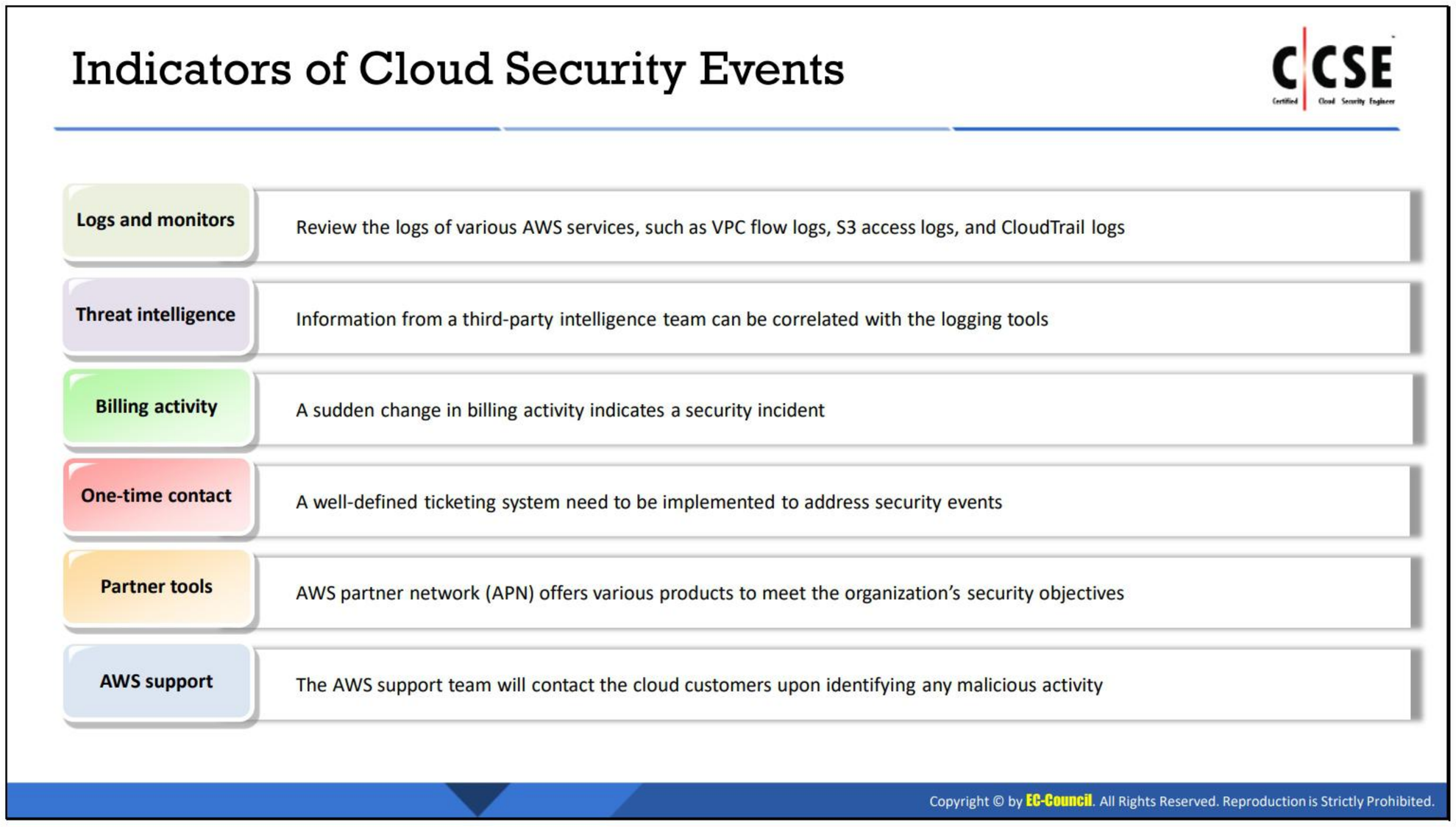


Design Goals of Responding to Cloud Incidents

The design goals relevant to incident response in the cloud are as follows:

- **Build Response Objectives:** The organization should work with the stakeholders, legal team, and enterprise leaders to understand incidence response. Some goals include mitigating issues, recovering damages, and storing forensics data.
- **Respond to Events:** Implement the response patterns where the event and data occur.
- **Preserve Evidence:** Preserve logs, snapshots, and any other important evidence. Copy the evidence to a centralized security account. Use tags and metadata to implement retention policies.
- **Adopt Redeployment Techniques:** Resolve through a redeployment with an appropriate configuration if a security anomaly is caused by a misconfiguration. If possible, ensure the response mechanism can be safely executed more than once in unknown conditions.
- **Implement Automation:** When certain incidents and issues repeat frequently, implement automation mechanisms for responding to them. This reduces the time and effort of the incident response team.
- **Choose Scalable Solutions:** Ensure you match the scalability approach adopted by the organization to cloud computing. It should minimize the incident detection and response time.
- **Improve the Process:** Improve the process, tools, and people to fix any gaps. Use simulations to achieve this.

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



Indicators of Cloud Security Events

Consider the following potential indicators to determine the security-related incidents in AWS.

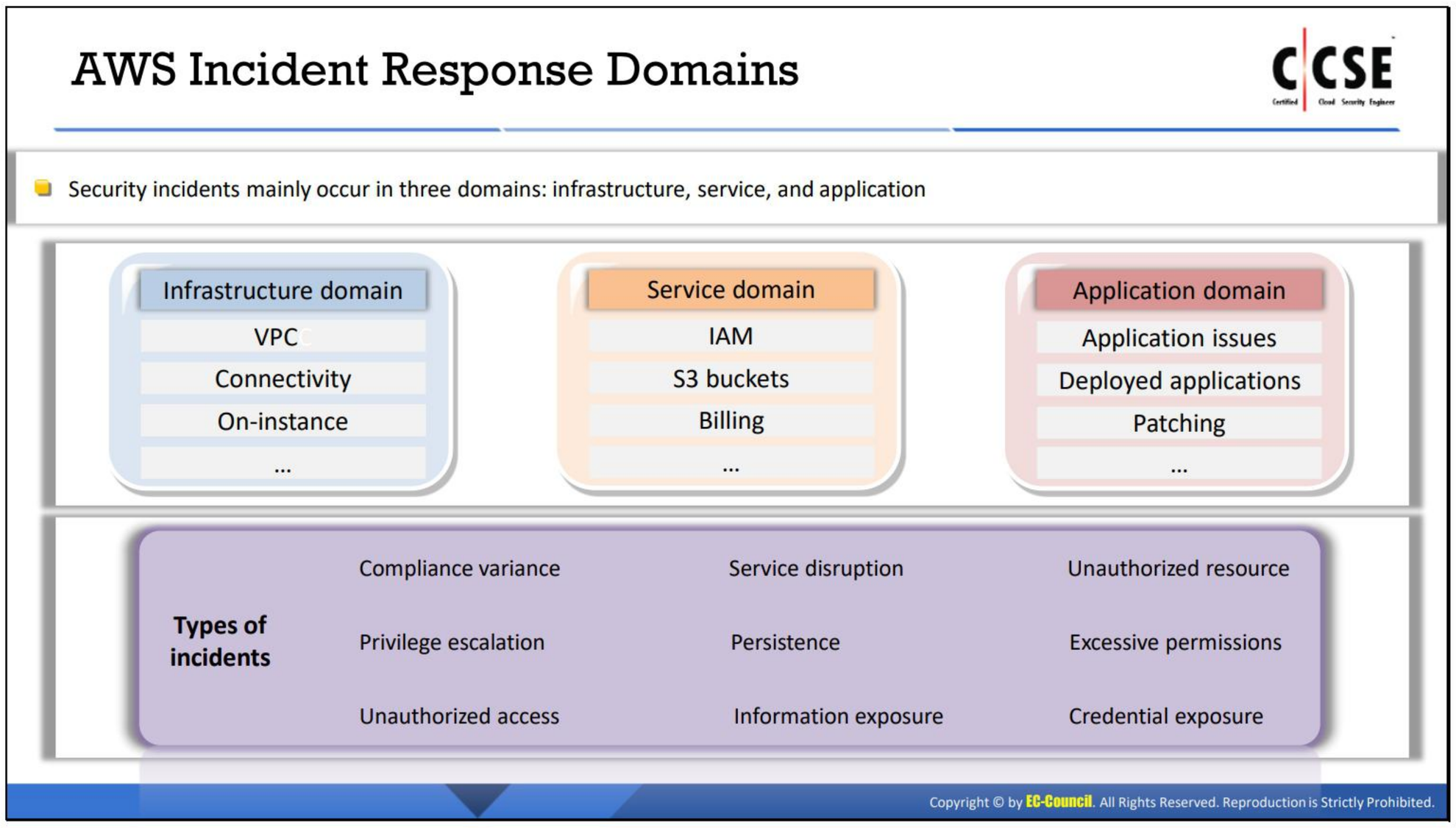
- **Logs and Monitors:** Review the logs of various AWS services, such as VPC Flow logs, S3 access logs, and CloudTrail logs. Review various AWS monitoring services such as GuardDuty, Security Hub, Detective, and Macie. Use Route 53 health checks and CloudWatch alarms to handle incidents. Use application-specific logs that can be generated within the applications.
- **Billing Activity:** A sudden decrease or increase in the billing amount may indicate a security event.
- **Threat Intelligence:** If the cloud customers have subscribed to a third-party threat intelligence team, correlate their information with the logging and monitoring tools. This helps determine the potential risk of a security incident.
- **Partner Tools:** AWS partner network (APN) offers various products to meet the security objectives of an organization. These partners have the experience and expertise in securing every stage of cloud adoption, from migration to day-to-day activities. They also specialize in providing security-based solutions to certain workloads.
- **One-time Contact:** The security events may be identified by users, customers, developers, or other organization staff. Therefore, ensure you have an established and well-defined method to contact the security team. Some common methods include ticketing systems, contact email addresses, and web forms.
- **AWS Support:** The AWS support team will contact the cloud customers upon identifying any malicious activity.

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

Take required actions on security incidents using Amazon Detective, Amazon Athena, Amazon CloudWatch Events, or Event Bus rules. Use these tools and send the findings to chat, ticketing, and incident response tools. Implement event-based automation to avoid manual responses.

hide01.ir

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



AWS Incident Response Domains

Security incidents mainly occur in three domains: service, infrastructure, and application. The tools used for responding to the incidents also differ between these domains. It is important to thoroughly understand each domain to handle the incidents accordingly.

hidori.ir

- **Service Domain:** Incidents in the service domain affect the AWS accounts of users, IAM roles and permissions, metadata, billing, among others. A service domain incident is handled using AWS API mechanisms. A service domain incident can be because of an improper configuration or AWS resource permissions.
- **Infrastructure Domain:** All network-related activities or application data are included in the infrastructure domain. This domain includes the processes that run on the EC2 instance and the traffic to the instance. A response to infrastructure domain incidents includes restoration, retrieval, and acquisition of incident-related data for forensics. The response includes an interaction with the instance's operating system. In the infrastructure domain, incidents can be handled using AWS APIs along with a digital forensic/incident response software. Such incidents may involve an analysis of the Amazon EBS volume's disk blocks, network packet captures, or volatile memory.
- **Application Domain:** Incidents found in an application code, or in a software deployed for the infrastructure or services are referred to as application domain incidents. Application domain incidents should be included in runbooks and cloud threat detection. Such incidents can be handled using cloud tools, automated recovery, deployment, and forensics.

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

In all these domains, it is crucial to identify the users who might cause a threat to resources, data, and accounts. A risk management framework must be used to determine potential risks for the organization and the necessary actions.

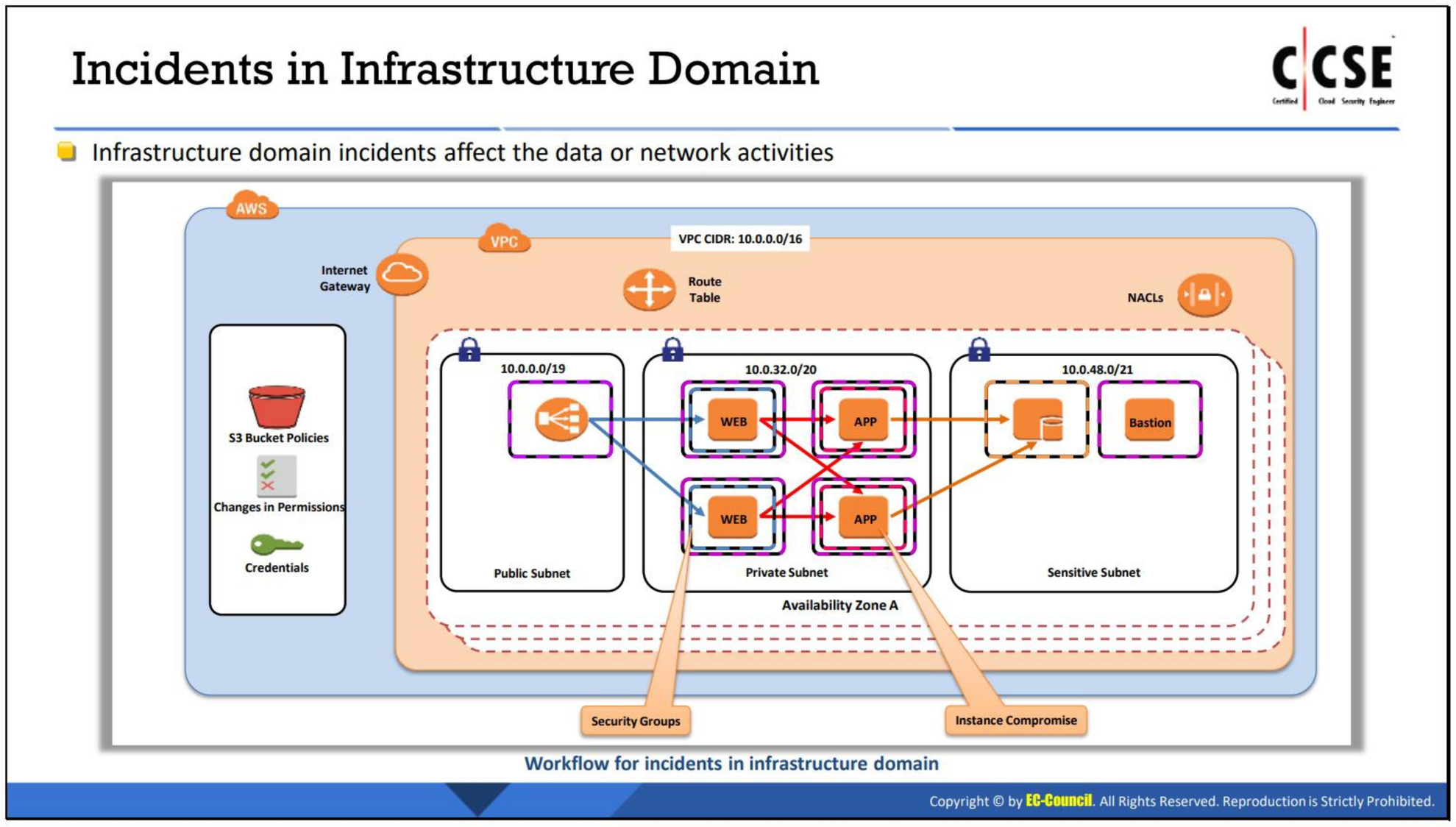
Types of Incidents

The following are the types of cloud incidents:

- **Compliance Variance**: It refers to incidents where resources or data is configured in a way that violates compliance policies.
- **Service Disruption**: Incidents where users are not able to access resources in their cloud environment.
- **Unauthorized Resources**: Incidents that involve the creation of resources in an unauthorized manner.
- **Unauthorized Access**: These incidents involve access to resources via an unauthorized user, IP address, or system.
- **Privilege Escalation**: It refers to the attempts to access resources by gaining elevated access permissions, which is otherwise not allowed.
- **Persistence**: This type of incident involves the attempts to create an access mechanism that allows attackers a future access to resources.
- **Excessive Permissions**: These incidents involve resources that have more permissions than necessary.
- **Information Exposure**: It refers to an unauthorized access to critical or sensitive data.
- **Credential Exposure**: It refers to an unauthorized access to AWS credentials.

hide01.ir

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



Incidents in Infrastructure Domain

Infrastructure domain incidents are those that affect the data or network activities. Some examples include traffic to the EC2 instance in the VPC, data on EC2 instances or containers, and so on.

hide01.ir

Steps to Address Infrastructure Domain Incidents

As an example, if a security anomaly has occurred in an EC2 instance, it can be addressed through the following steps:

- **Capture Metadata:** Before making any changes to the environment, ensure you capture the metadata from the EC2 instance.
- **Protect the Instance:** Enable termination protection for the instance to protect it from an accidental termination.
- **Isolate the Instance:** Deny any network traffic to the EC2 instance's IP address using an network access control list (NACL) or switch the VPC security group to isolate the EC2 instance.
- **Detach EC2 Instance:** Detach the instance from auto-scaling groups.
- **Deregister from Load Balancer:** Deregister the instance from any associated ELB service.
- **Snapshot:** Take snapshots of the EBS data volumes connected to the Amazon EC2 instance, which can be preserved and used for any follow-up investigations in the future.
- **Tag Instance:** Ensure the EC2 instance is tagged as "quarantined for investigation," and the relevant metadata is added to it.

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

Use AWS APIs, CLI, SDKs, and AWS console for the above steps. Control the interaction with AWS using IAM. Create new EBS volumes using the snapshots and attach to EC2 instance forensics for an in-depth analysis.

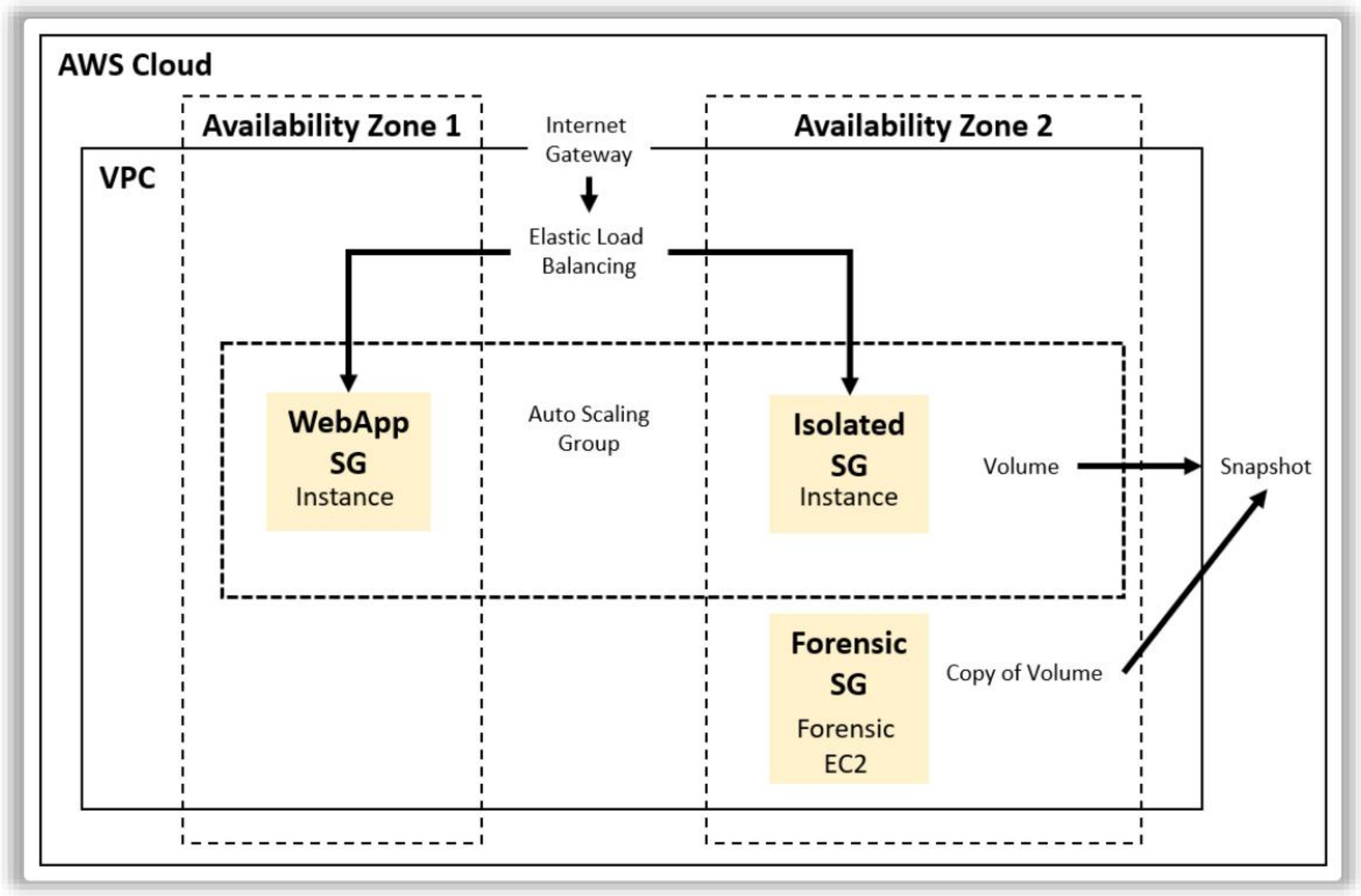


Figure 7.20: Instance Isolation and Snapshots

Decide the Investigation Method

The cloud customers can choose between offline investigation and online investigation. In an offline investigation, the instance will be immediately shut down. An online investigation is performed to keep the instance running.

In an offline investigation, the instance will not affect the environment after being shut down. Use a snapshot to create a copy of the affected instances and review the copy of the affected instance in an isolated AWS account.

The incidence response team can choose an online investigation if they need to copy unstable evidence such as network traffic from the host operating system.

Capture Volatile Data

Understand the mechanism of capturing volatile data from an EC2 instance. To perform an online investigation, the responder must communicate with the operating system running on the EC2 instance. Use the IAM service for tasks on the EC2 instance. Though the responder can directly connect to the instance using secure socket shell (SSH) or remote desktop (RDP), it is not a best practice. Using an automation tool is recommended to perform tasks on the instance.

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

Use AWS Systems Manager

AWS Systems Manager Run Command helps the responder make changes securely and remotely by running Linux shell scripts or Windows PowerShell commands on the instance. To do this, the responder must first activate the EC2 instance as a managed instance. Now, the SSM agents should be installed on the machine and then the IAM permissions should be configured. To use Run Command for automation, the responder must ensure the prerequisite activities are completed before an investigation.

The AWS Systems Manager is integrated with CloudTrail and exports log files to the specified S3 bucket. Use the log files to determine the IP address of the request, who made the request and when it was made, etc. CloudTrail generates logs of all AWS Systems Manager API actions, including the requests to execute Run Command.

An AWS Systems Manager (SSM) agent executes PowerShell commands and Linux shell scripts by leveraging the Run Command service of SSM. Specific tools can be loaded and executed using these scripts to extract additional information from the EC2 instance or host. The data can be transferred to the S3 bucket for storage or to a forensic EC2 instance.

Automate the Capture

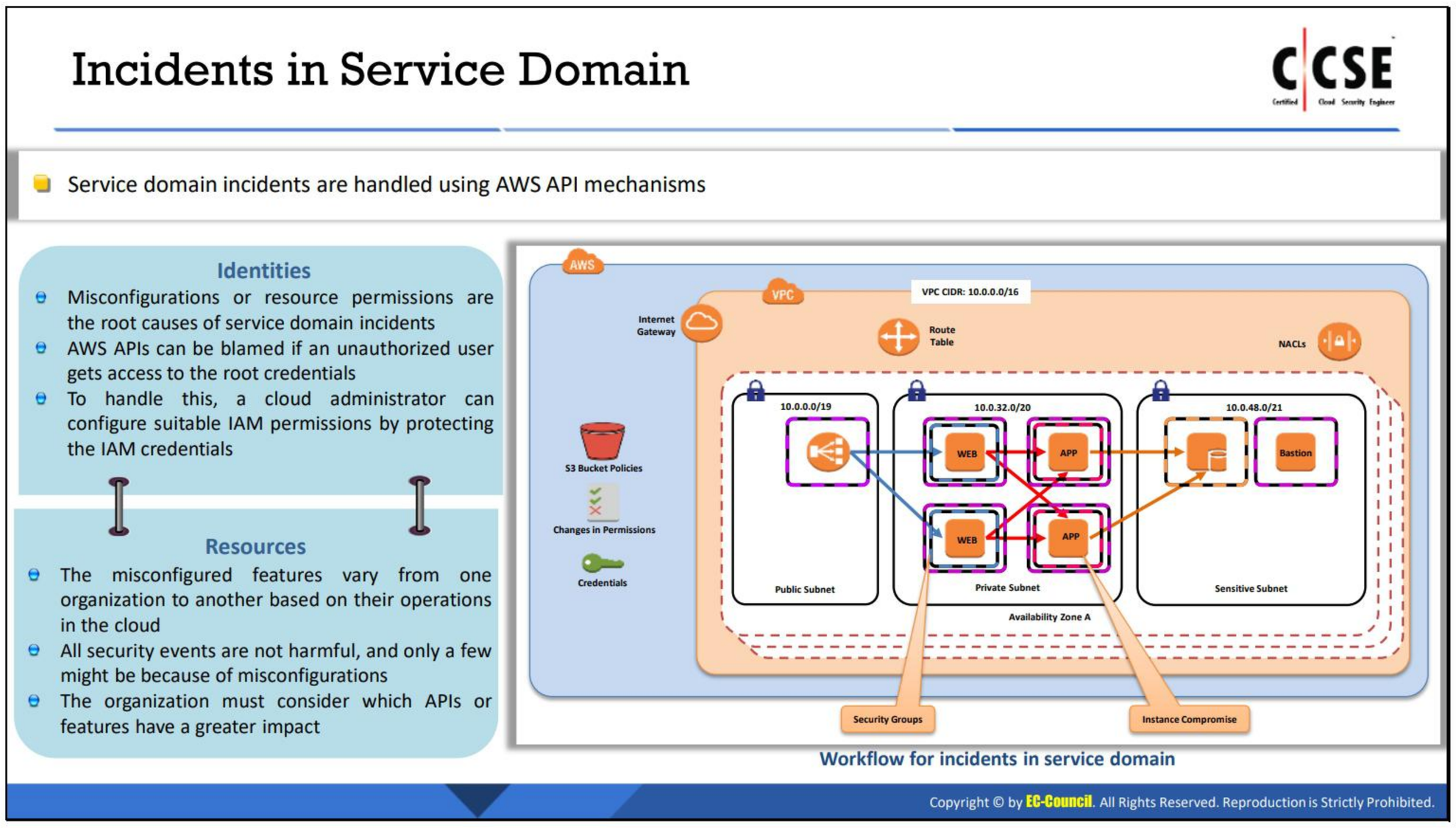
When the EC2 instance is tagged with a particular tag, CloudWatch Events can be used to target the Run Command to invoke the SSM agent. This tag-driven response is also an event-driven response.

hide01.ir

Use Hibernation for Memory Capture

Use hibernation for memory capture. An instance can be hibernated to create a copy to the EBS volume. Pre-planning is necessary for hibernation because only certain operating systems and instance types support it. Hibernation is a powerful way to capture the memory as it does not depend on other services. It supports both automation and repeatable processes.

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



Incidents in Service Domain

Service domain incidents are handled using AWS API mechanisms.

Identities

The root causes of service domain incidents can be associated with misconfigurations or resource permissions. It mainly affects a user's AWS account, resource metadata, billing, etc. AWS APIs can be revoked through various methods such as AWS command line interface (CLI), software development kits (SDKs), and AWS console. While interacting with AWS using these APIs, identity and access management (IAM) can be used to securely control the access to AWS services or resources.

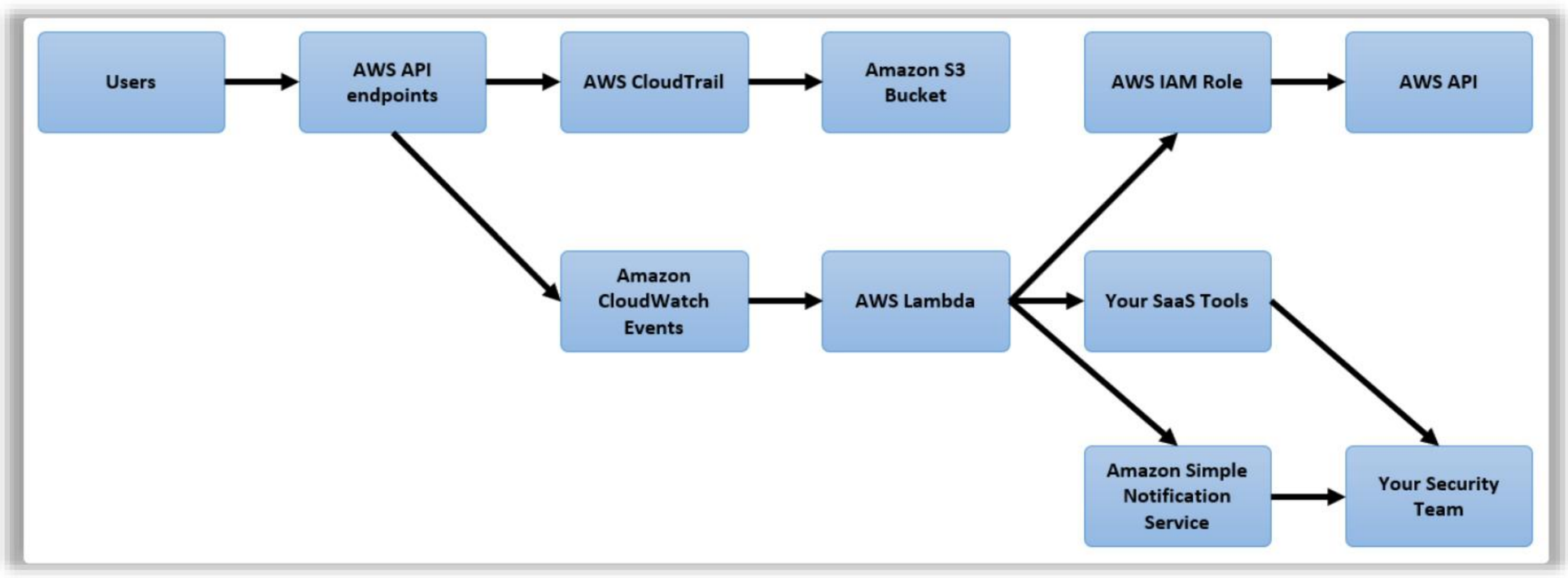


Figure 7.21: Service Domain Incident Response Workflow

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

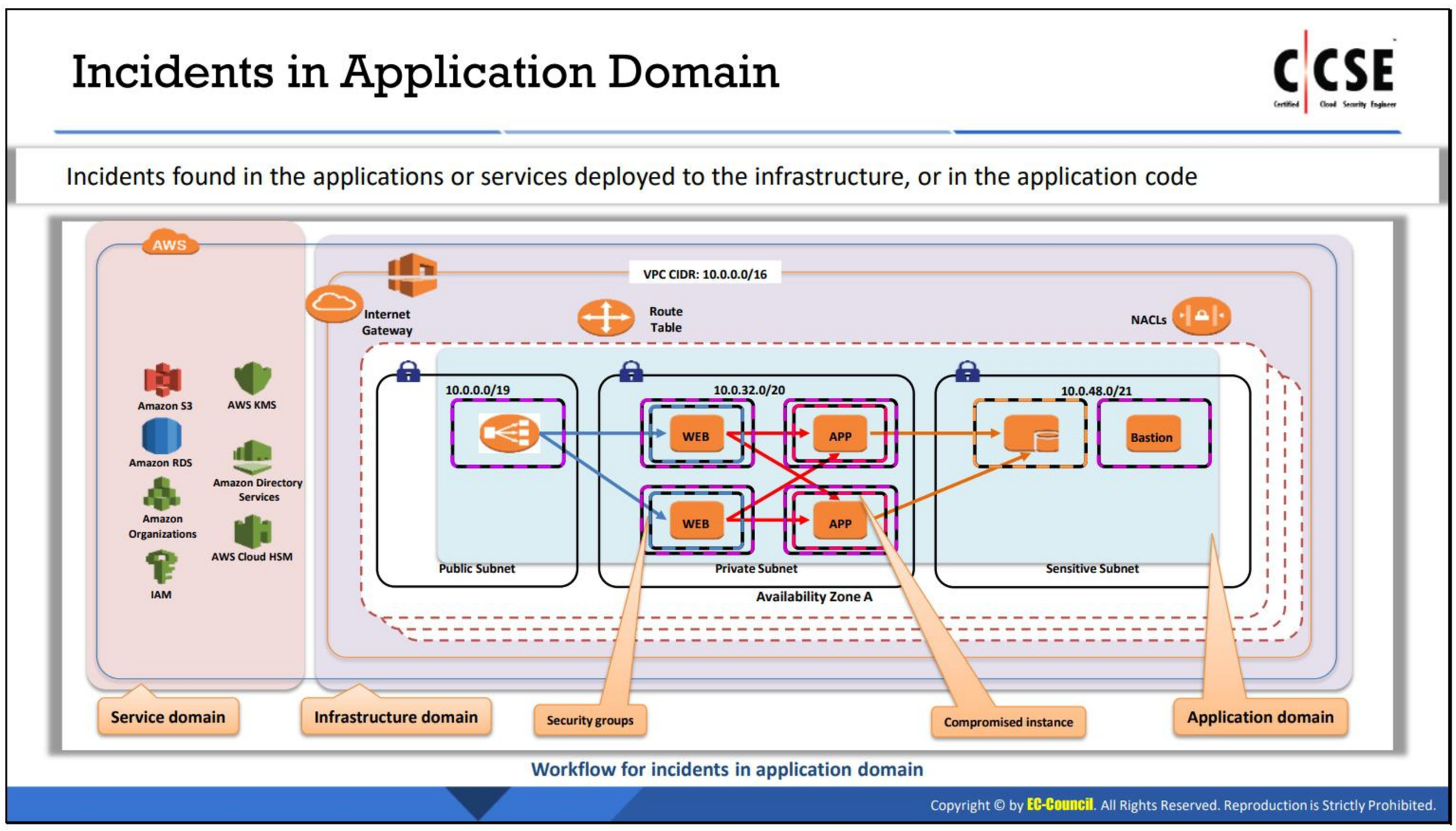
Though these APIs are valuable to millions of customers, they can be blamed if an unauthorized user gets access to the root credentials. For example, the cloud customer can use APIs to enable logging within the AWS account. If a hacker gets the credentials, they can use the API to disable those logs. To avoid these types of incidents, a cloud administrator can configure suitable IAM permissions by protecting the IAM credentials.

Resources

The misconfigured features vary from one organization to another based on their operations in the cloud. A few organizations keep data and applications accessible for everyone, whereas others keep their applications and data confidential. All security events are not harmful, and only a few might be because of misconfigurations. The organization must consider which APIs or features have a greater impact and whether they are frequently used. Use tools and services such as Trusted Advisor to detect multiple configuration issues.

hide01.ir

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

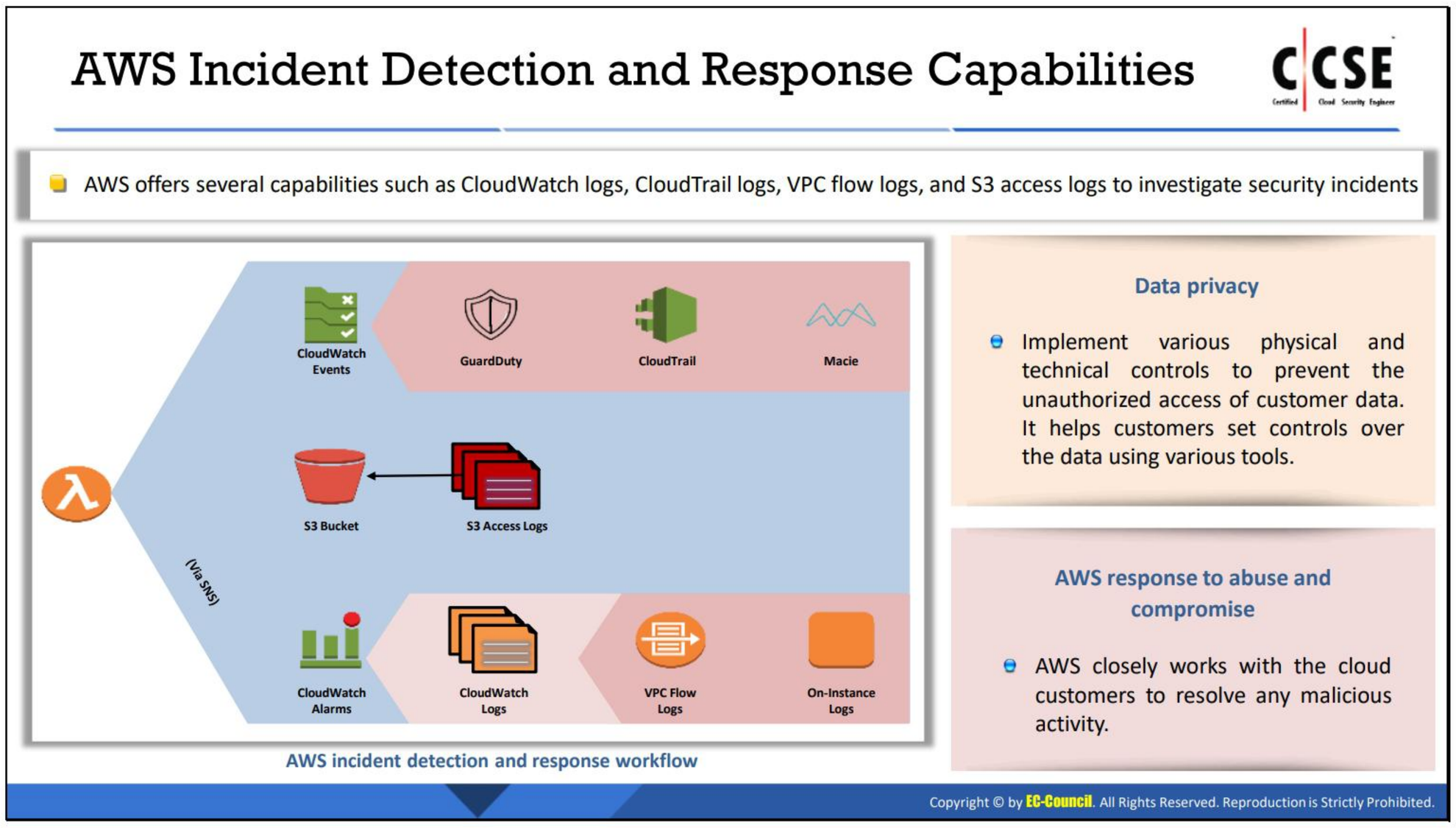


Incidents in Application Domain

Incidents found in the application code or within a software deployed to the infrastructure or services are called application domain incidents. Application domain should be included in the runbooks and cloud threat detection. The application domain incidents can be handled using cloud tools, automated recovery, deployment, and forensics.

hiddn1.ir

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

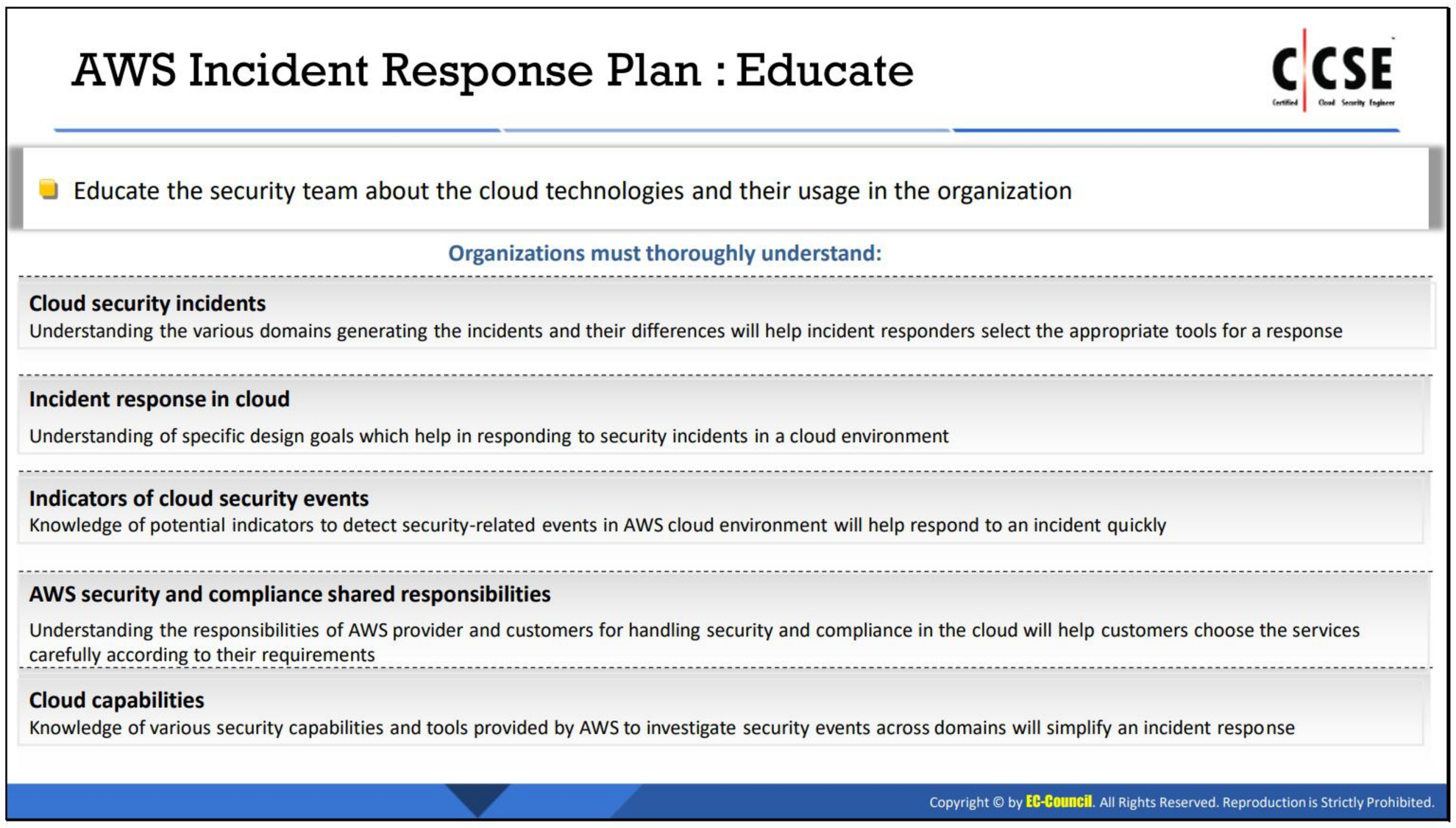


AWS Incident Detection and Response Capabilities

AWS offers the following capabilities to investigate security incidents:

- Investigate security events across the domains using AWS security capabilities. For example, use AWS logging mechanisms such as Amazon CloudWatch logs, AWS CloudTrail logs, and Amazon S3 access logs. Ensure you have enabled the logs pertaining to your used services.
- AWS centralized logging solution can consolidate and store the common types of cloud logs. We need to enable the log sources to be examined, and can use Amazon Athena to query logs stored in Amazon S3 buckets.
- Use AWS partner products to simplify the analysis of logs that are similar to those mentioned in the APN Security Competency program. Moreover, you can get valuable insights into the log data using AWS services such as Amazon GuardDuty and AWS Security Hub.

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



AWS Incident Response Plan: Educate

The incident response and security operations teams should be educated about the cloud technologies the organization intends to use. This education includes the following aspects:

hi4le01.ir

Security and Compliance Shared Responsibility

AWS and cloud customers are responsible for handling security and compliance in the cloud. Amazon controls and monitors all components from the host OS. The cloud customers are responsible for handling the host operating system and configuring security groups, network access control lists, IAM, etc. A customer has to choose the AWS services carefully as their responsibilities will vary based on the selected services.

Incidence Response in Cloud

Consider the following design goals relevant to incident response in the cloud.

- **Build Response Objectives:** The organization should work with the stakeholders, legal team, and enterprise leaders to understand incident response. Some of the goals include mitigating issues, recovering damages, and storing forensic data.
- **Respond to Events:** Implement the response patterns where the event and data occur.
- **Preserve Evidence:** Preserve logs, snapshots, and any other important evidence. Copy the evidence to a centralized security account. Use tags and metadata to implement retention policies.
- **Adopt Redeployment Techniques:** Resolve through a redeployment with an appropriate configuration when a security anomaly is caused by misconfiguration. If possible, ensure the response mechanism can be safely executed more than once under unknown conditions.

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

- **Implement Automation:** Automate when certain incidents and issues repeat frequently. This reduces the incident response team's time and effort.
- **Choose Scalable Solutions:** Develop a mechanism that can respond to the common incidents and match the scalability of the approach adopted by the organization to cloud computing. Moreover, the mechanism must minimize the time between incident detection and response.
- **Improve the Process:** Improve the process to fix any gaps in the process, tools, or people. Use simulations to find gaps and improve the process.

Cloud Security Incidents

Understanding the various domains generating the incidents and their differences will help incident responders select the appropriate tools for a response. These include service, infrastructure, and application domains.

hide01.ir

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

AWS Incident Response Plan : Prepare

- Enable appropriate access to various incident detection and response tools and cloud services to help incident response teams detect and respond to incidents
- Prepare runbooks, both manual and automated, to help the team respond to incidents quickly
- Identify the baseline operations and use these to identify deviations

Prepare people

- Define roles and responsibilities
- Define response mechanism
- Create a receptive and adaptive security culture
- Predict response

Prepare technology

- Prepare access to AWS accounts
- Prepare processes
- Cloud service provider support

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

AWS Incident Response Plan : Prepare (Cont'd.)

hide01.ir

Cloud provider support

AWS managed services	AWS managed services help with infrastructure management using best practices
AWS support	AWS support provides a set of tools, technology, and programs to optimize performance and reduce costs
DDoS response support	AWS shield offers a managed distributed denial-of-Service (DDoS) protection service to protect the web applications running on AWS cloud

AWS support escalation path

Predefined escalation path includes:

- Submission of a support case
- Technical account manager
- On-call operations manager
- Global enterprise support manager
- Director of support engineering
- VP of AWS support

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

AWS Incident Response Plan: Prepare

Prepare People

An organization can spend time on measures to increase the security of its cloud environment and applications by leveraging automated processes. Use an automated incident response process to easily handle the security incidents in an organization. However, the incident

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

responders and analysts are still required to create new response procedures, correlate events, do research, perform simulations, test and create new tools, and acquire new skills.

Preparing people involves the following:

- **Define Roles and Responsibilities**

  To effectively handle the incident response process, define the roles and responsibilities within the organization to constitute an incident response team. This team will be responsible and accountable for handling security incidents. In addition, involve trusted partners, resource and application owners, and any third parties in an incident response or investigation as per requirements.

  Educate the IR or security team on various cloud services and allow them to practice on the cloud platform used by the organization. Provide additional training to the staff on development processes, programming skills, and infrastructure automation to effectively handle the incident response process.

- **Define Response Mechanisms**

  Cloud platforms provide a greater visibility and functionalities via service APIs. Note down such APIs and learn how to use them. Moreover, collect the AWS account numbers of the team, IP address ranges of VPCs, etc., and document the incident response procedures to help remediate and investigate incidents.

- **Create an Adaptive and Receptive Security Culture**

  Ensure the organization's security team is open and accessible to all staff. Non-security staff can also help detect and respond to incidents if the security team members are receptive. If an adaptive and receptive security culture is adopted in the organization, incidents can be reported and remediated in a timely manner with the teams' collaboration. Provide a clear channel or way for all staff members to report security incidents when they find them.

- **Predict Response**

  An automated incident response plan is intended to handle recurring and simple security tasks. It is impossible to predict all potential incidents; thus, a human analysis is required. Train the staff and ensure they are prepared for an incident response. This helps the organization deal with unexpected incidents. Collaborate with trusted third-party security partners to determine unexpected security incidents.

  - **AWS Security APN Partners and Window of Response**

    Every organization using the cloud must identify and collaborate with a trusted AWS security APN partner. This provides a different perspective to handle security incidents and improves the organization's response capabilities. A trusted security APN partner also helps identify the potential risks an organization may not be familiar with.

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

Map traits using the following window of response, which consists of four quadrants. The below diagram helps simplify the difficulties in identifying the potential threats to an organization.

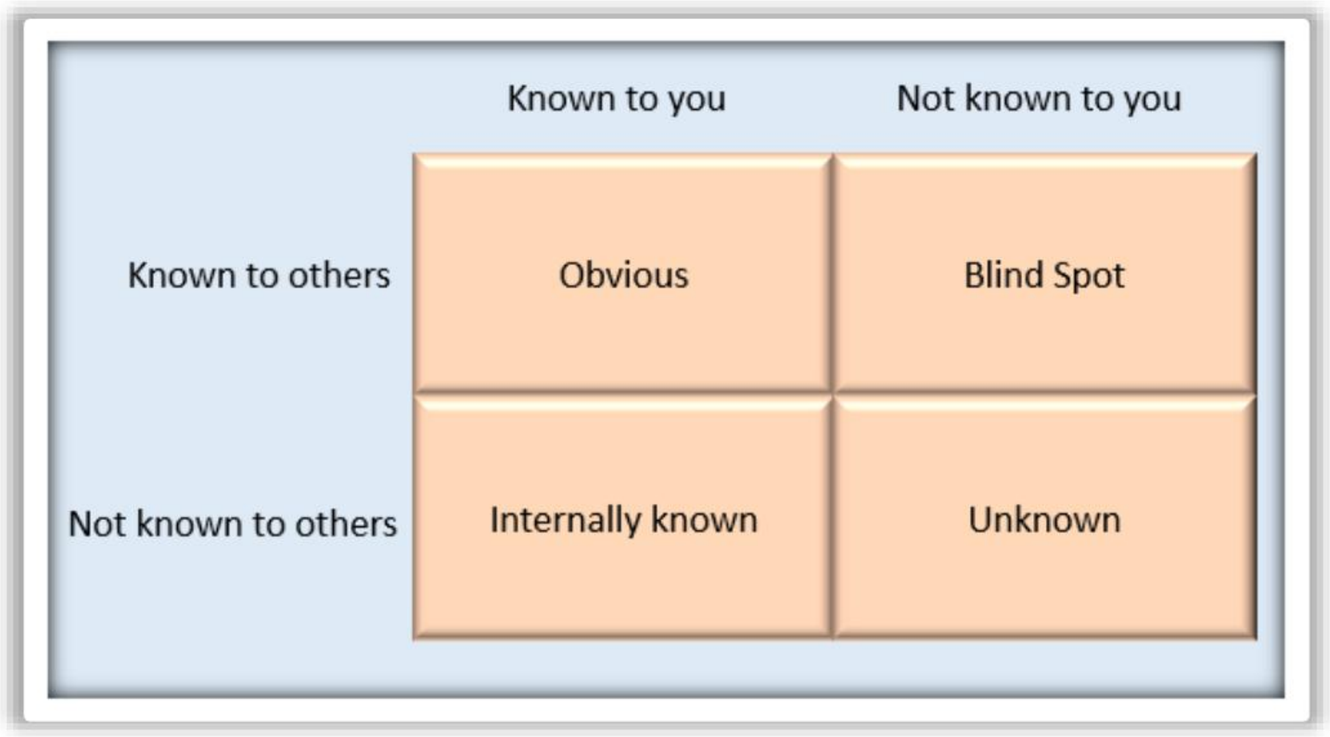


Figure 7.22: Window of Response

- **Obvious:** It includes incidents that both the incident response team and APN partner are aware of. Though the team is aware of these incidents, an APN partner with the right expertise can recommend the right controls and solutions.
- **Internally Known:** It includes incidents that the team is familiar with, but not the APN partner. When internally known risks are brought to the APN partner's notice, they can find the optimized controls to handle them.
- **Blind Spot:** It includes incidents that the APN partner is familiar with, but not the response team. A right APN partner can bring these blind spot risks to the organization's notice.
- **Unknown:** It includes incidents unknown to both the team and APN partner.

hidoc1.ir

- **Methods to Reduce Unknown Risks**

  Reduce the unknown risks using the following methods:

  - **Define Security Assertions:** Defining security assertions helps the organization to be prepared for incident response. Define security assertions in the early stages of the cloud journey instead of trying to reverse engineer the security assertions in the later stages.
  - **Educate the Team:** Include security expert partners or create cloud security experts in the team to help examine and secure the cloud environment. Ensure process feedback loops and develop mechanisms for the engineering team to communicate with the security teams. This incident response approach can also be expanded to monitor mailing lists and security disclosures.

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

- **Reduce the Attack Surface:** Keep the organization's defense strong to avoid attacks and provide more time for the security team to focus on unknown attacks. The security defense must block and slow down the attackers to detect them easily.
- **Threat Intelligence:** Ensure that the organization utilizes threat intelligence for continuous feeds or updates on current threats, indicators, and risks from different parts of the world.
- **Alerts:** Set alert notifications in the case of any unusual or suspicious activities. For instance, create notifications for activities in services or regions rarely or not used by the organization.
- **Machine Learning:** Leverage machine learning to identify complicated anomalies in the organization.

Manage issues with the services and tools provided by AWS. Leverage logging and monitoring tools such as Kibana and Elasticsearch Service for big data architectures.

Prepare Technology

Preparing technology as a part of an AWS IRP includes the following:

- **Prepare Access to AWS Accounts**

The incident response team should have access to the resources and environment where the incident occurs. Ensure that the response team has all required access to perform their duties before the occurrence of a security event. To do this, the organization must understand the required level of access and provide it in advance. Document the authentication and authorization of the team and test them before an incident occurs. This ensures the team can perform tasks immediately without any delays. Review the layout of the AWS accounts and know how the cross-functional roles are organized.

The cloud administrator must collaborate with the cloud architecture and development teams to determine the level of access required for the incident responders. Talk to the organization's cloud architects regarding the cloud identity strategy and AWS account strategy to understand the configured authentication and authorization methods (e.g., authentication, federation, and cross-account access). Grant privileged access to the user accounts created for responding to security incidents and restrict them from regular activities.

While creating a new access mechanism, the organization must work with the cloud teams to understand how the AWS accounts are organized and managed. Then, it can use the following response patterns to determine the right type of approach:

- **Indirect Access:** With indirect access, the account owners need to perform authorized remediations in their AWS accounts with the support of the incident response team. This method is beneficial when the incident responders are not familiar with the cloud environment. It is a complex and slower process.

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

- **Direct Access:** To provide direct access to responders, an incident response IAM role must be created in the AWS accounts. The responders can use this IAM role during a security event. If the security incident affects the authentication process, the responder can authenticate using a special emergency process or a normal federated process. The permissions assigned to the incident response IAM role are based on the expected actions of the responders.
- **Alternative Access:** If a security incident affects the organization's security, communication systems, or identity, it needs to look for an alternative method to investigate and handle the incident. Using a new AWS account, the incident responders can integrate and work from a safe and secure infrastructure. Use IAM policies to create appropriate access controls to grant access so that the new alternate AWS account has the same permissions as the affected AWS account. After granting sufficient access, AWS APIs in the affected AWS account can be used to share the required data (e.g., volume snapshots and logs) for an investigation in the new AWS account.
- **Automation Access:** When automation methods are used to handle security incidents, the cloud administrator must create IAM roles, especially for automation resources (e.g., EC2 instances and Lambda functions). In doing so, instead of creating new AWS accounts, the AWS resources receive temporary credentials and inherit the permissions of the assigned IAM role. These temporary credentials are sent to the AWS resources automatically and can be used to sign API requests. The cloud administrator can choose a safe method to automate authentication and execution inside the OS of the EC2 instance. Use AWS Systems Manager Run Command to administrate or monitor instances securely and remotely by installing an agent on the OS of the EC2 instance.
- **Managed Services Access:** When an organization works with an AWS managed service or a managed services partner, both have a shared responsibility to ensure the organization's security. The organization must understand the responsibilities of the partners, their access to AWS resources, the access they need, and how to contact them when required. AWS managed services help the organization minimize operational risks and overheads by implementing the best practices to maintain its infrastructure. It automates common activities such as patch management, monitoring, security, change requests, and backup services. In addition, it offers full lifecycle services for provisioning, running, and supporting the organization's infrastructure.

- **Prepare Processes**

  Once a proper access is provisioned and tested, an incident response (IR) team should develop the remediation and investigation processes. This stage is crucial for the success of the incident response plan IRP (IRP) because it is necessary to plan a proper response to security events.

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

Collaborate with the cloud services team to determine the tasks responsible for making the processes successful. The response tasks must be collaborative to ensure the required account configurations are implemented properly.

Provide the processes and essential configurations in advance for the following response capabilities:

- **Decision Trees:** The security team's actions should be based on various conditions such as the AWS account type, resource tags, and AWS configuration rules. To allow the creation and documentation of these decisions, the organization must develop decision trees with the stakeholders and other teams. A decision tree helps in decision making and identifying actions and outcomes, depending on the required conditions and inputs.
- **Use Alternative Accounts:** Though it is essential to respond to security events in an AWS account, it is better to investigate the data outside the affected account. Some cloud customers use specific processes to create isolated, separate AWS account environments using templates. Use services such as CloudFormation or Terraform to deploy the templates. These templates enable users to create a group of AWS resources and use them in an orderly manner.

  Using templates in the incident response's initial stages to preconfigure such accounts can eliminate human interactions. The teams' preparedness for incident response can be verified through an audit. Automated processes also enhance security and help keep the data in a forensic environment.

  To determine a suitable AWS account process, the organization needs to work with cloud architects and the cloud services team. For instance, use AWS Organizations to create and preconfigure new accounts using a scripted or templated method.
- **View or Copy Data**

  Incident responders must have access to logs for analysis and should be able to view and copy the data. The IAM policy for incident responders should at least provide read-only access to help them with investigations. Use pre-built AWS managed policies to enable an appropriate access for responders.
- **Share Amazon EBS Snapshots**

  Many cloud customers use Amazon elastic block storage (EBS) snapshots for investigating the security events in AWS EC2 instances. EBS snapshots are incremental backups. To investigate an EBS volume in an isolated account, modify the permissions of the snapshots (sharing of the snapshots with other AWS accounts must be allowed). The authorized users can then use these hared snapshots to create their own EBS volumes.

  If the snapshot is encrypted, share the custom AWS key management service (KMS) customer managed key (CMK) used for its encryption. Though the

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

snapshots are constrained to a region, you can share them with other regions by copying them to that region.

- **Share Amazon CloudWatch Logs**

  Amazon CloudWatch logs can be shared with another account using CloudWatch Logs subscription. Create this configuration in the early stages before a security incident takes place.

- **Use Immutable Storage**

  When logs and other important evidence are copied to another AWS account, the replicated data should also be protected. In addition, protect the integrity of the source data. Use immutable storage to protect the integrity of the data and prevent it from any tampering.

  Configure the S3 bucket to protect the integrity of data stored in it by using its native services. Restrict how data is read or written in the S3 bucket by enabling MFA, configuring S3 versioning, and managing access permission with the bucket policies. Use this type of configuration for storing investigation logs and important evidence. Use server-side encryption with AWS KMS to protect data and ensure it can be decrypted only by authorized IAM principals.

  Once the investigation is completed, use object lifecycle policies to move the collected data from Amazon S3 to S3 Glacier for a long-term storage. Here, S3 Glacier offers a durable, secure, and inexpensive storage for archiving data and creating long-term backups.

  You can also Amazon S3 Glacier Vault Lock to protect the data in S3 Glacier. This feature allows the setting of compliance controls in each S3 Glacier vault using a vault lock policy. Enforce special security controls such as WORM (write once, read many times) in the vault lock policy to protect it from future edits. A locked policy cannot be changed. Different compliance controls can be deployed in a vault lock policy using IAM policies.

- **Launch Resources Near an Event**

  Ensure the investigation is performed in the same region where the event has occurred to reduce the data transfer time. It is advisable to investigate and conduct forensics activities in the cloud environment where the data is located, instead of transferring it to a data center before investigation. The cloud customers need to create and manage separate accounts for a long-term storage in case the collected evidence needs to be retained for compliance and legal purposes.

  The organization must ensure that the incident response procedure and responders stick to data privacy laws of that specific region. In addition, consider the legal implications of moving data between jurisdictions.

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

If an event affects the organization's security, communication systems, or identity, use an alternative mechanism to investigate it. AWS offers a quick launch of new infrastructure for secure and alternate work environments. Use AWS services such as WorkSpaces, WorkMail, and Chime as they provide the required capabilities and connectivity for investigations.

- **Isolate Resources**

  During the investigation of certain security incidents, isolate specific resources as a part of the response. Such resources are isolated to reduce the impact on the affected resources, prevent the exposure of data, and limit any further unauthorized access. Consider business, regulatory, legal, and other requirements while responding to a security incident.

- **Launch Forensic Workstations**

  For some security incidents, analyze the associated disk images, file systems, and RAM dumps. The customers can create a customized forensic workstation for mounting copies of the affected data volumes.

  Once a forensic system is provisioned, the responders can use the template and create a new Amazon machine image (AMI) to launch a separate forensic workstation for each investigation. Simplify the deployment process by automating the AMI launch process. This process ensures no cross-contamination from other forensic examinations.

hide01.ir

- **Cloud Provider Support**

  - **AWS Managed Services**

    AWS managed services provides the management of infrastructure so that the cloud customers can focus on their applications. AWS managed services reduce the operational overhead of customers by using best practices to maintain the infrastructure. Common activities such as monitoring, security, change requests, backup services, and patch management are automated. AWS managed services also include lifecycle services to run, provision, and support the infrastructure.

    In addition, it is also responsible for deploying a set of security detection controls and responding to security incidents. In the case of an alert, AWS managed services (AMS) follow a set of manual and automated runbooks to initiate a response. The runbooks are shared with the customer during onboarding so that they can co-ordinate with the response.

  - **AWS Support**

    AWS support provides a set of tools, technologies, and programs to optimize the performance of AWS solutions and reduce costs. The support plans offer 24/7 access to AWS account, whitepapers, documentation, blogs, and support forums. If the customers need a technical support or resources, they can choose a suitable support plan to meet their AWS account use case.

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

Support center is the central point of contact for any issues with AWS resources. IAM is responsible for controlling the access to AWS support center. To report an Amazon EC2 abuse, customers need to contact the AWS abuse team.

- **DDoS Response Support**

  Distributed denial of service (DDoS) is a cyberattack where an attacker sends multiple requests to an application or website and prevents it from responding and functioning properly.

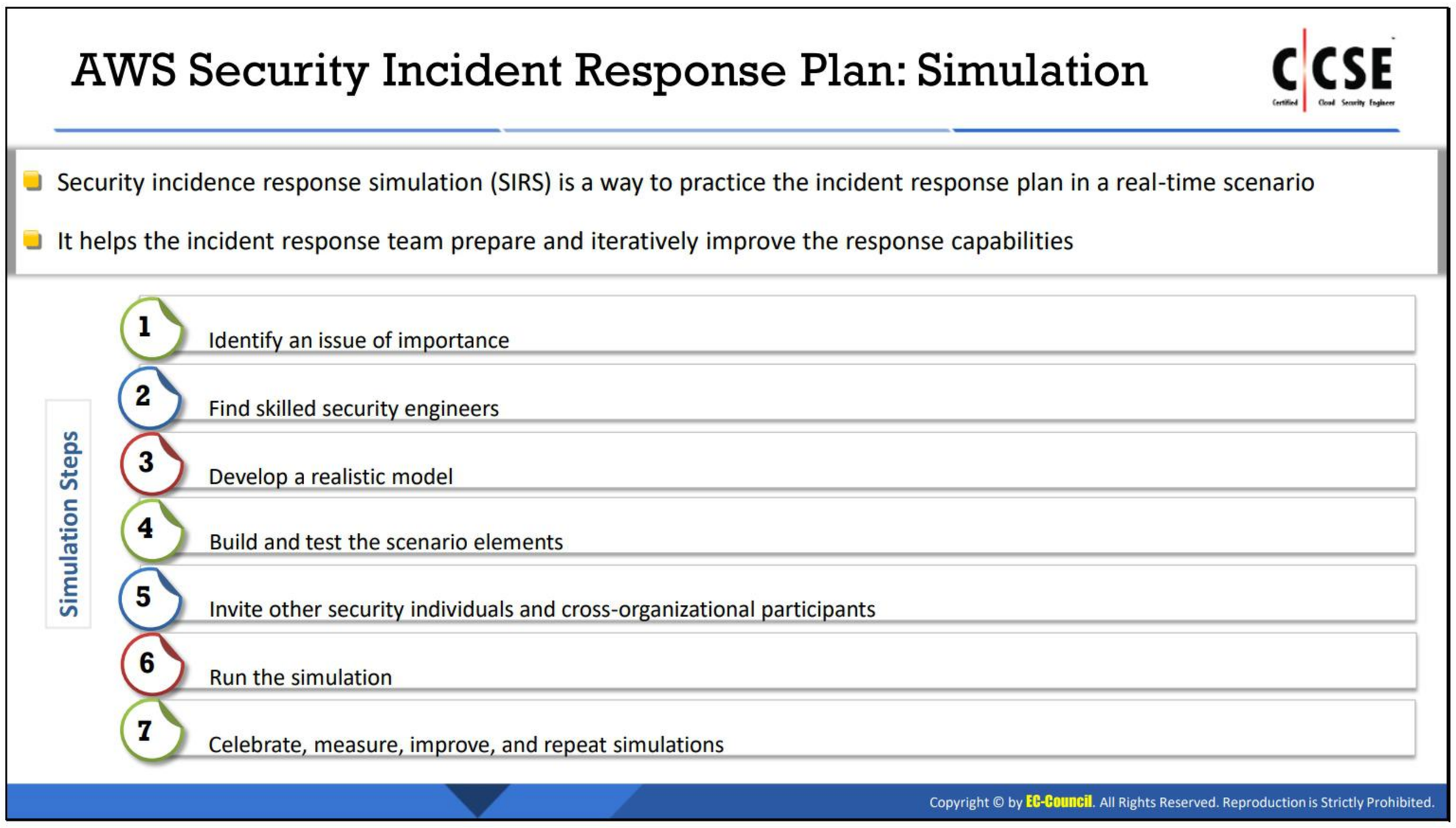
Use AWS Shield to secure web apps on AWS. It offers a managed DDoS protection service to protect the web applications running on the AWS cloud. AWS Shield offers automatic inline mitigations to reduce application downtime and latency.

AWS Support Escalation Path: Customers should follow a predefined escalation path for situations that require an escalation

- Submission of a support case
- Technical account manager
- On-call operation manager
- Global enterprise support manager
- Director of support engineering
- VP of AWS support

hide01.ir

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



AWS Security Incident Response Plan: Simulation

To simulate expected and unexpected security events within the cloud to know the effectiveness of the organization's preparation, consider the following:

hyde01.ir

Security Incident Response Simulations (SIRS)

SIRS helps in practicing the IR plan and other procedures during a real security incident. SIRS activities are internal and are concerned with preparing and iteratively improving the response capabilities.

SIRS activities include

- Validating readiness
- Learning from simulations and training the concerned teams
- Generation of artifacts for accreditation
- Improving tools to improve speed
- Simplifying communication and escalation
- Developing familiarity with unexpected and rare security incidents

Simulation Steps

The simulation steps are as follows:

- **Identify an Issue of Importance:** Identify a high-priority issue and define the trigger that will lead to a response.
- **Find Skilled Security Engineers:** Find a builder and tester for developing effective simulations.

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

- **Develop a Realistic Model:** Ensure realistic simulations so that all participants will value them. If there is a need for legal counsel, executives, and public relations, the organization must also invite them for an active participation.
- **Create and Test the Scenario Elements:** Build simulation materials such as potential runbooks, email alerts, and logging artifacts.
- **Invite Security Individuals and Participants from Other Organizations:** Invite all individuals who have a role in the simulations. For example, invite the legal counsel, public relations, and organization executives.
- **Run the Simulation:** Decide whether the organization should inform the staff about the simulations.
- **Measure, Improve, and Repeat:** Measure the performance, and improve and repeat the subsequent simulations.

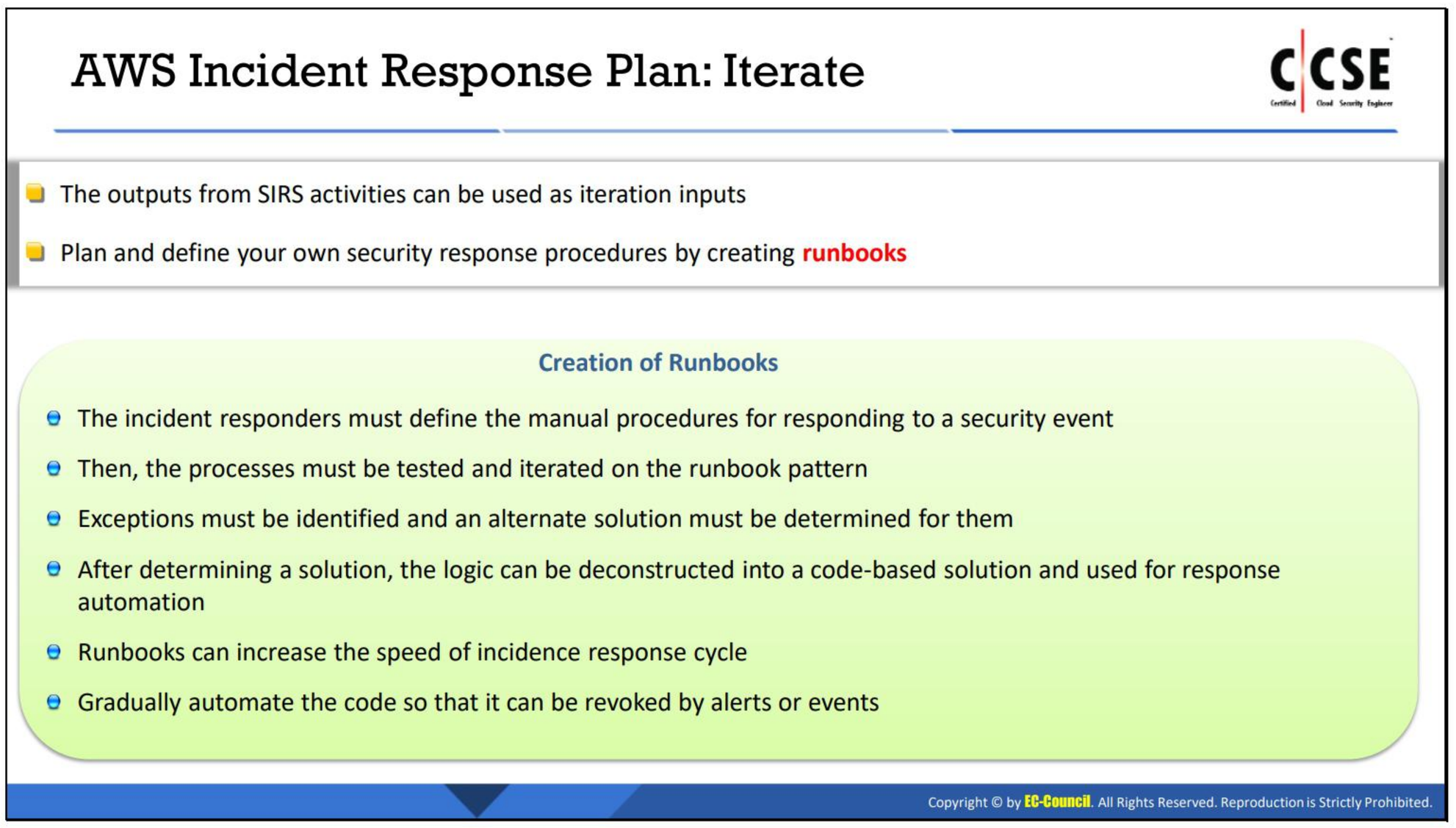
Simulation Examples

Consider past and real-world events as valuable sources for simulation exercises. The following simulation examples are helpful while developing the initial simulations:

- Unauthorized changes to resources/network configuration
- Public exposure of credentials because of misconfigurations
- Public access to sensitive data because of misconfigurations
- Isolation of a web server connected to malicious IP addresses

hide01.ir

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



AWS Incident Response Plan: Iterate

Use the simulation outcomes to improve the security response. This will also improve your agility through incremental improvements. A simulation also provides feedback to the organization on whether things are working as expected. This can help enhance the existing procedures or create new procedures incrementally to improve the security incident response.

Iterate the simulation outcomes to reduce the risk and time of evaluation using the following:

Runbooks

If a security incident is detected, return to an acceptable state as a part of the response plan. To do this, plan and define security response procedures in advance using runbooks. A runbook consists of documented organization procedures for performing tasks during a security incident. Store the runbooks in an internal digital system or as printed documents. An organization may already have runbooks. If not, create new runbooks.

Potential mistakes are possible if you manually follow the written runbooks. It is recommended to automate all repetitive tasks. This allows the response team to focus on key tasks such as practicing simulations, performing research, and building or testing new tools.

- **Create Runbooks**

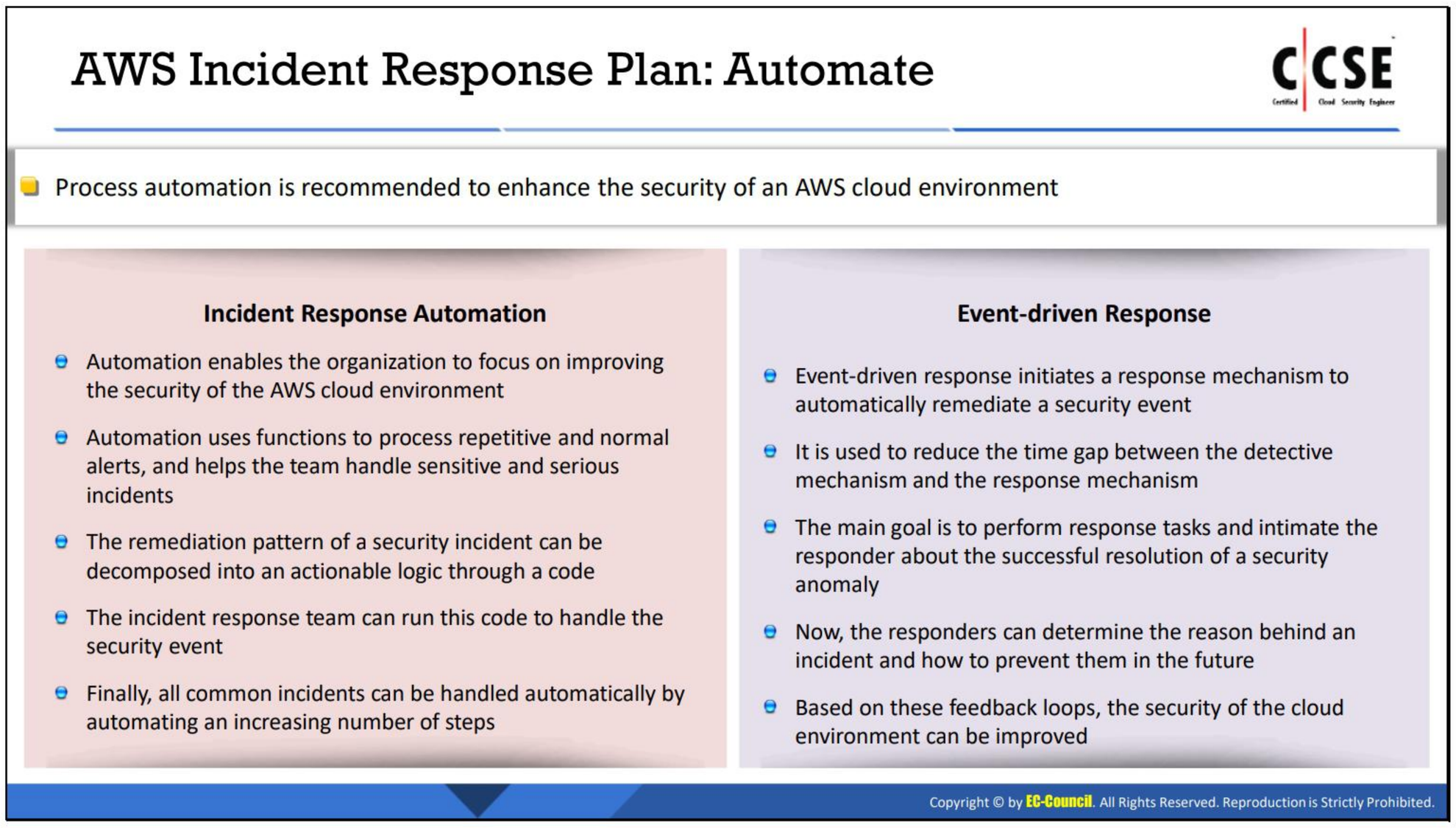
  Before creating runbooks, focus on the currently generated alerts by investigating them. To do this, define the manual procedures that need to be performed. Then, test and iterate the process on a runbook pattern to improve the primary response logic. Determine the exceptions and an alternate resolution to such scenarios.

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

After determining the best solution, the logic can be deconstructed into a code-based solution and used as a tool to automate the response. This increases the speed of the response cycle. Now, automate the code so that the alerts or events can revoke it.

hide01.ir

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



AWS Incident Response Plan: Automate

Process automation is recommended to enhance the security of an AWS cloud environment. In addition, it assists the responders' efforts to cope with the organization's speed and reduces the burden of performing repetitive tasks. The automation comprises the following:

hid001.ir

- **Incident Response Automation**

  Automation helps the organization spend more time on improving the security of the AWS cloud environment. Use the AWS APIs and tools for automating the security engineering and operations functions. Automate software development methods, identity management, network security, and data protection. By doing so, the system can automatically monitor, review, and generate a response.

  If the team continues to respond to incidents manually, they might make mistakes while handling simple incidents or even miss serious incidents. Automation uses functions to process repetitive and normal alerts, enabling the team to handle sensitive and severe incidents.

  You can improve a manual process by automating its steps. After defining a remediation pattern for a security incident, decompose it to an actionable logic by writing a code. The incident response team can run this code to handle the security event. Eventually, more steps can be automated to automatically handle all common incidents.

- **Event-driven Response**

  In an event-driven response, a detective mechanism initiates a responsive mechanism to automatically remediate a security event. This method is used to reduce the time gap between a detective mechanism and a response mechanism. Use AWS Lambda for an

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

event-driven response architecture that runs codes in response to the events. It automatically manages all underlying architectures.

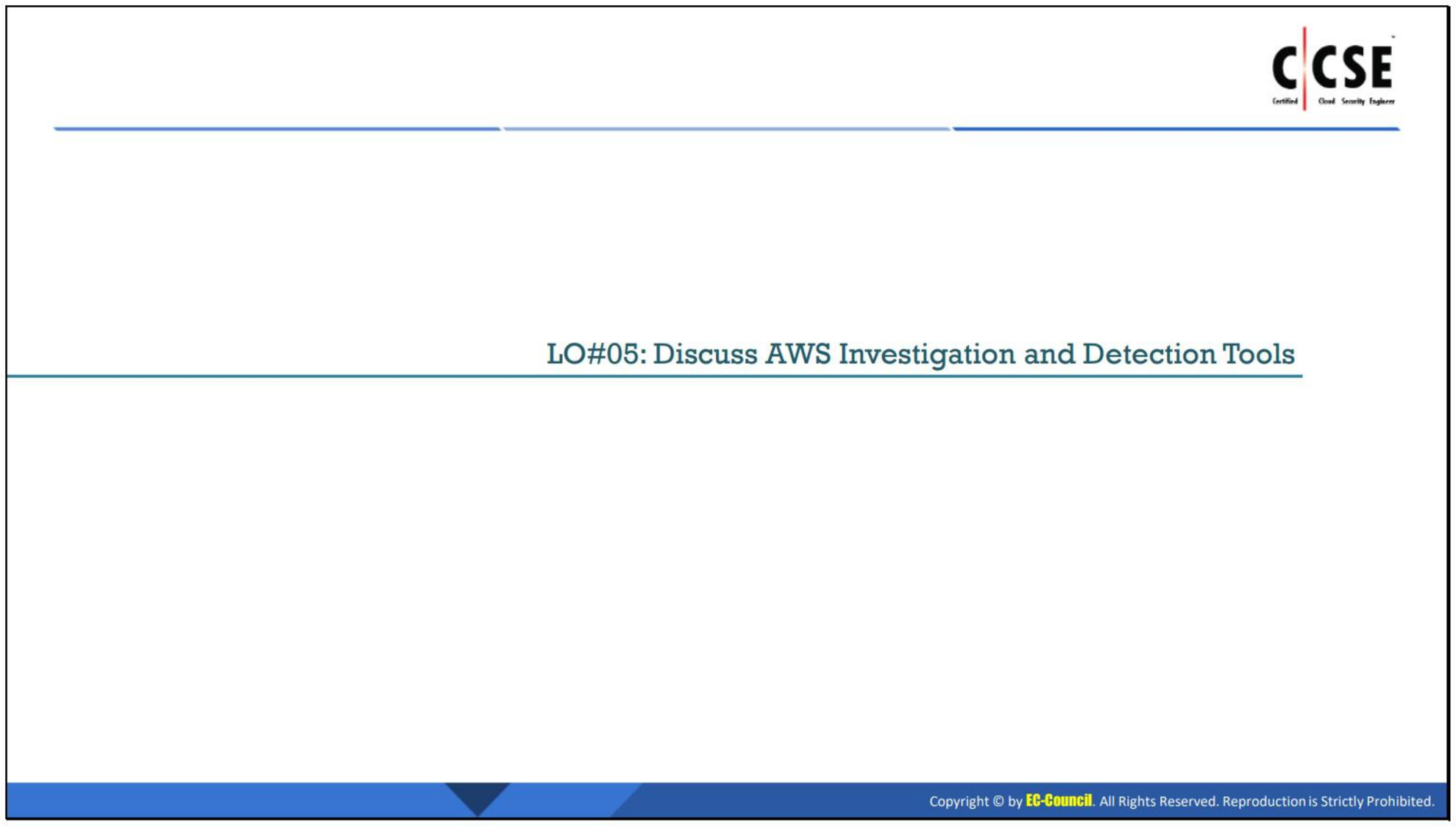
The main goal of event-driven response is to execute response tasks and intimate the responder about the successful resolution of the security anomaly. Now, the response team can determine why the incident occurred and how to prevent them in the future. Based on these feedback loops, the security of the cloud environment can be improved.

Options for Automating Response

Use various options for automating a response, such as AWS Lambda, AWS Step Functions, Auto Remediation with AWS Config Rules, SSM Agent, AWS Fargate, and Amazon EC2. Along with the automation options, consider centralization and scan period (events per second). Centralization involves a central account to perform all detection and remediation steps for an organization. Events per second (EPS) metric is used for estimating the cost. The higher the EPS, the higher the price for sending the events to centralized accounts.

hide01.ir

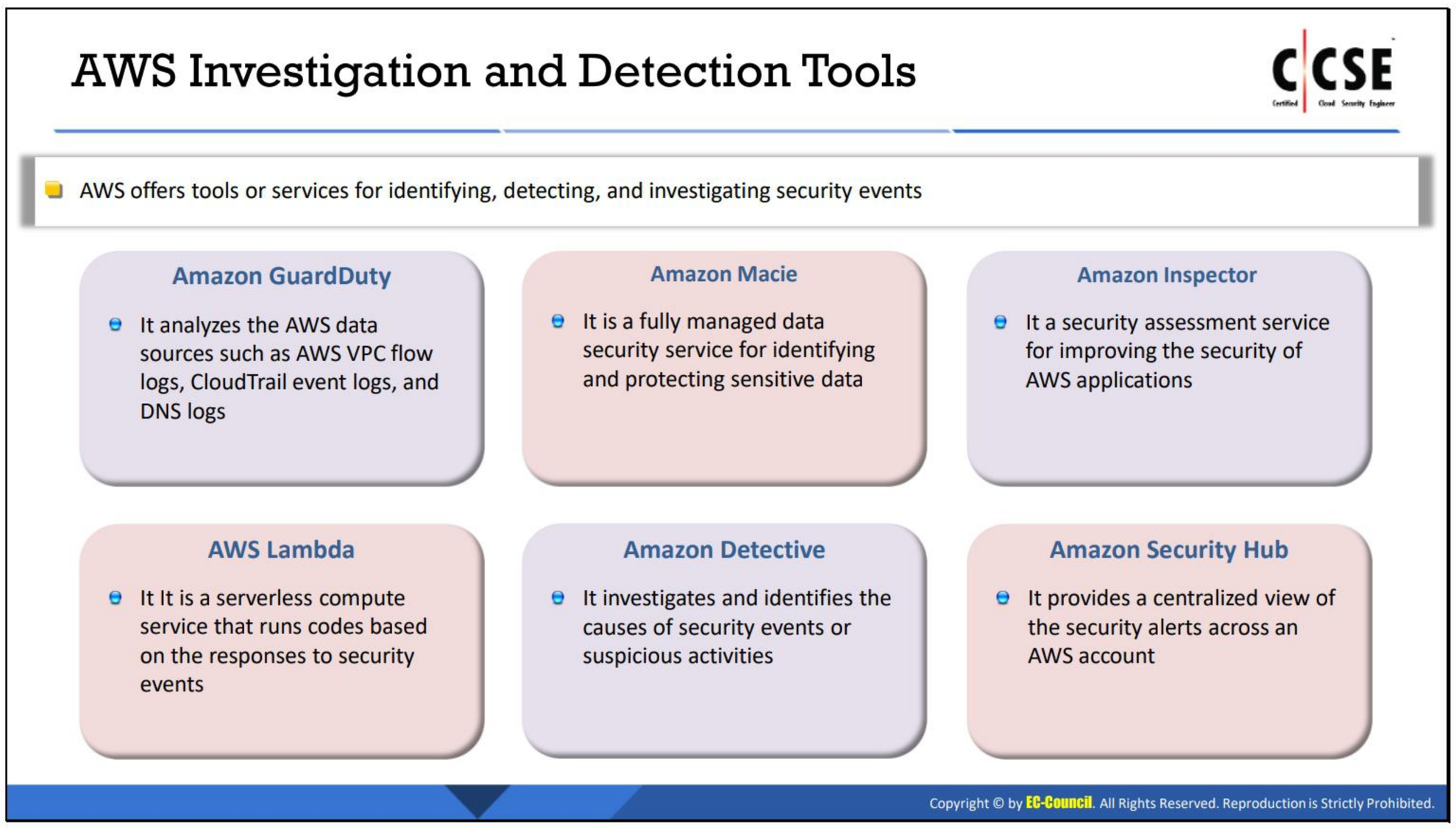
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#05: AWS Investigation and Detection Tools

This section explains various AWS investigation and detection tools. It shows you how to use tools such as GuardDuty, Macie, Amazon Inspector, AWS Lambda, Amazon Detective, and Amazon Security Hub for detecting and responding to threats. It lists the various third-party tools that can be integrated with AWS for incident detection and response.

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



AWS Investigation and Detection Tools

AWS provides various tools or services for identifying, detecting, and investigating security events.

hide01.ir

Amazon GuardDuty

Amazon GuardDuty is a detection service. It is used for monitoring malicious activities and unauthorized access to protect accounts, data, and workloads. It is a cost-effective method for continuous threat detection in AWS. It uses anomaly detection, machine learning, and integrated threat intelligence to identify and classify threats.

It analyzes the events from various AWS data sources, namely AWS CloudTrail event logs, VPC Flow logs, and DNS logs. By using this service, the responders can focus on how to respond faster and secure the organization.

GuardDuty provides HTTPS APIs, CLI tools, and CloudWatch Events for automating the responses to security findings. These include the details of affected resources and attacker information such as IP address, time, and location.

Amazon Macie

Amazon Macie is a fully managed data security service for identifying and protecting sensitive data. It automates the discovery of data and lowers its protection cost. Macie supports S3 storage and provides an inventory of publicly shared buckets, unencrypted buckets, and buckets shared with AWS accounts outside the defined AWS organization. By applying machine learning and pattern matching techniques to the selected buckets, it identifies and alerts about the sensitive data. Macie findings include details such as encryption status, public accessibility, and sensitive data type.

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

The findings or alerts of Macie can be sent to CloudWatch Events for integration with existing workflows or with other AWS services for automatic remediation actions.

Amazon Inspector

Amazon Inspector is a security assessment service for improving the security of applications in the AWS cloud environment. It automatically inspects all applications for vulnerabilities. Following an assessment, it provides a list of security findings prioritized according to their severity. The security findings include the details of security issues and recommendations on how to fix them.

AWS Lambda

AWS Lambda is a serverless compute service that runs a code based on the responses to security events in AWS services. A developer just needs to upload the code as a zip file or a container image. AWS Lambda allocates the required resources and runs the code based on the events. A cloud security professional can automatically trigger the code from AWS services or it can be called from any web or mobile application.

Amazon Detective

Amazon Detective helps investigate and identify the causes of a security event or suspicious activities. Using machine learning and statistical analysis, it automatically collects data from various AWS resources. Amazon Detective analyzes events from multiple AWS resources. It generates an interactive view of resources, users, and their interactions by analyzing the events. With this unified view, a cloud security team can easily visualize and identify the events' underlying reasons.

hide1.1

Amazon Security Hub

AWS Security Hub provides a central view of the security alerts across the AWS account. It collects and prioritizes the security findings or alerts received from various services, including Amazon Inspector, Amazon GuardDuty, and Macie. Using automated security checks, it continuously monitors the environment. Targeted actions can be taken by investigating with Amazon Detective.

All tools described above can be used together for responding to an incident in AWS. For example, Amazon Macie can be used to identify and classify the data in an AWS account. Then, using GuardDuty, the threats in the AWS account can be detected. Alarms can be generated using the on-instance logs, VPC Flow logs, and CloudWatch logs. Then, the flow logs can be imported to the S3 bucket. Now, users can run a code to generate responses to security events using AWS Lambda.

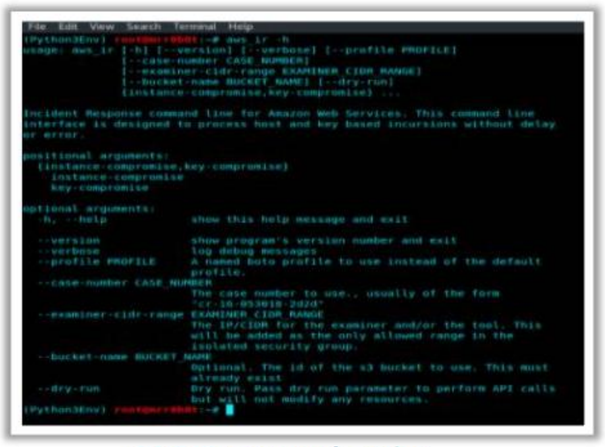
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

AWS Investigation and Detection: Third-party Tools

- Several third-party tools can be used for handling incident response

AWS IR

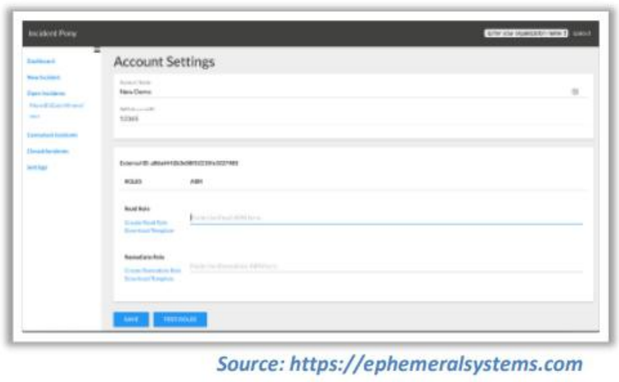
- A standalone command line for handling a response in AWS



AWS IR command section

Incident Pony

- A case management and incident response management tool specially designed for AWS

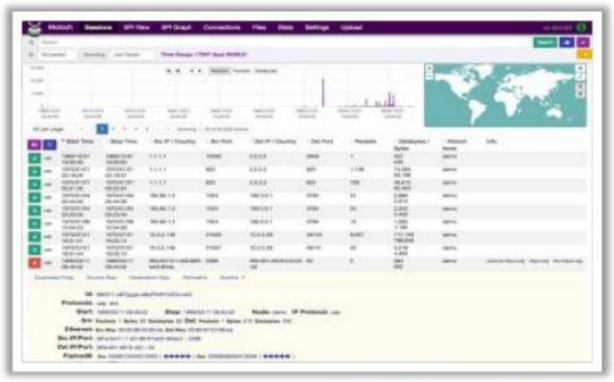


Source: https://ephemeralsystems.com

Incident Pony dashboard

Arkime

- An open-source indexed packet capture and search tool



Source: https://arkime.com

Arkime dashboard

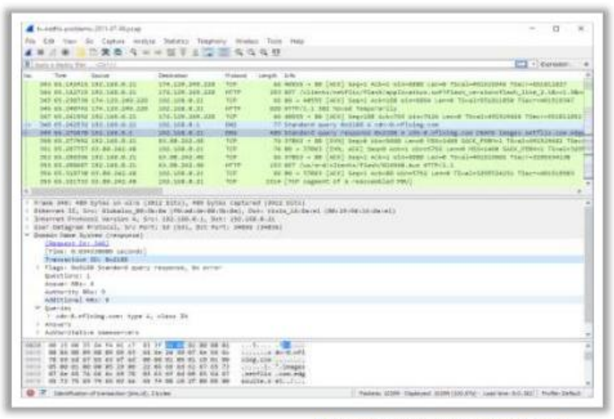
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

AWS Investigation and Detection: Third-party Tools (Cont'd.)

hide01.ir

Wireshark

- A network packet analyzer tool that helps with deep network inspection



Source: www.wireshark.org

Wireshark dashboard

Mandiant

- A leading provider of incident response and computer forensic solutions

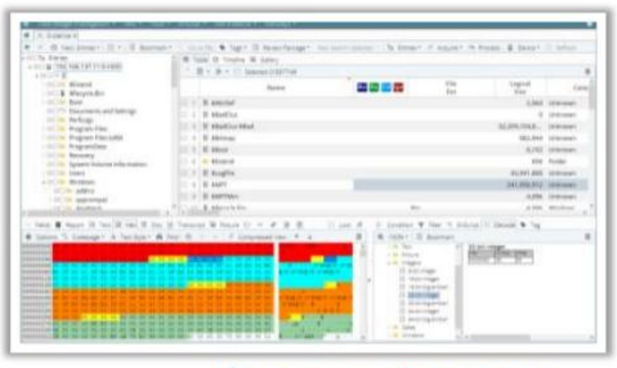


Source: www.fireeye.com

Mandiant threat intelligence dashboard

Encase Endpoint Investigator

- An effective tool for efficient digital forensic investigations



Source: www.security.opentext.com

Blank Encase Endpoint Investigator project file

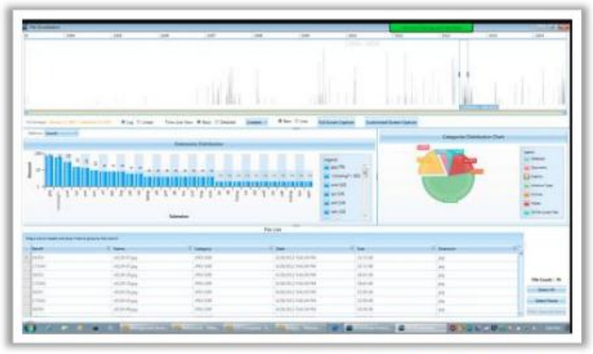
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

AWS Investigation and Detection: Third-party Tools (Cont'd.)

Forensic Tool Kit (FTK)

- A suite of tools for effective and smart digital investigations

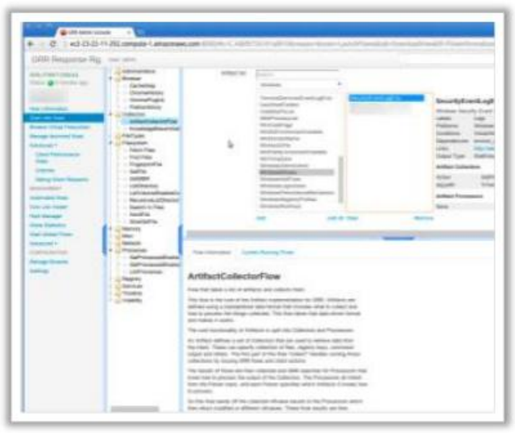


Source: www.esecforte.com

Forensic Tool Kit dashboard

Google Rapid Response (GRR)

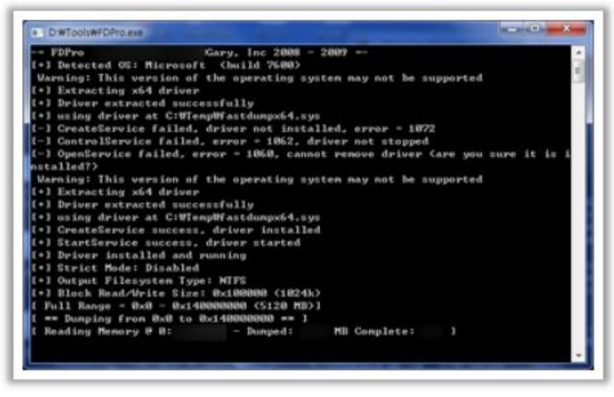
- An incident response framework for handling remote live forensics



Google Rapid Response dashboard

FastDump

- It is used for collecting physical memory data from 32-bit Windows systems



FastDump command section

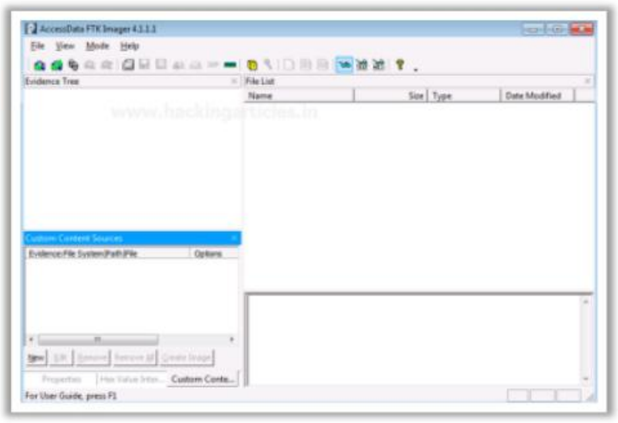
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

AWS Investigation and Detection: Third-party Tools (Cont'd.)

hide01.ir

FTK Imager

- A data preview and imaging tool for collecting evidence



Access Data FTK Imager dashboard

Linux Memory Extractor (LiME)

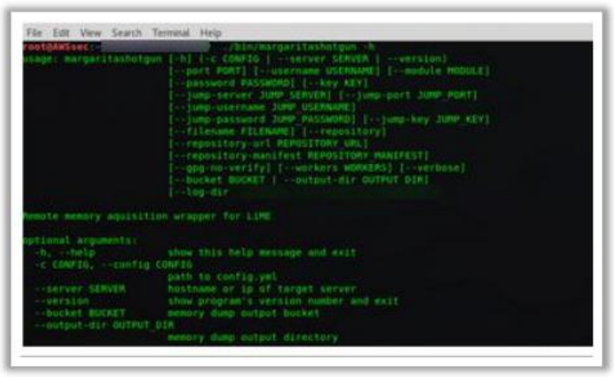
- Allows the acquisition of volatile memory from Linux-based devices



LiME command section

Margarita Shotgun

- It is used for memory capture from a running Linux instance



Margarita Shotgun command section

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

AWS Investigation and Detection: Third-party Tools

The third-party tools for handling incident response in AWS include the following:

AWS IR

Source: https://aws-ir.readthedocs.io

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

AWS IR (ThreatResponse) can be used for handling responses in AWS. It is a Python module and standalone command-line tool for collecting evidence and minimizing the impact of incidents.

Incident Pony

Source: https://ephemeralsystems.com

Incident Pony is a case management and incidence response management tool specially designed for AWS. It can be easily deployed and set up with a cross-account to manage the incidents at a single place. With Incident Pony, AWS incidents can be easily managed and response times can be minimized.

Arkime (formerly Moloch)

Source: https://arkime.com

Arkime (formerly Moloch) is an open-source indexed packet capture and searching tool. It is used for networking. It stores and exports all packets in a standard PCAP format. Moloch can be deployed across multiple systems and scaled to handle large network traffic.

Wireshark

Source: https://www.wireshark.org

Wireshark is a network packet analyzer tool. It helps with a deep inspection of the network at a microscopic level. It runs on multiple platforms such as Linux, Windows, MacOS, and Solaris. The captured network data can be browsed through the GUI or TTY-mode TShark utility. The output from Wireshark can also be exported in a CSV, plain text, or XML format.

hide01.ir

Mandiant

Source: www.fireeye.com

Mandiant is a leading provider of incidence response and computer forensic solutions. It enables an organization to optimize, measure, and improve its security programs. Mandiant enables the security team of an organization to automate their intelligence and expertise in its cloud environment.

EnCase Endpoint Investigator

Source: https://security.opentext.com

EnCase Endpoint Investigator is a useful tool for digital forensic investigation. It is used by forensic practitioners for efficient forensics and investigations using a defensible process. It helps the investigators with an in-depth analysis to collect evidence such as documents, internet history, pictures, etc. It is trusted by government agencies and corporations worldwide.

Forensic Tool Kit (FTK)

Source: www.esecforte.com

FTK provides a suite tools for effective and smart digital investigations. It provides various features to support data processing integrity and in-depth analysis.

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

Google Rapid Response (GRR)

Source: https://grr-doc.readthedocs.io

Google Rapid Response (GRR) is an incidence response framework for handling remote live forensics. It is an open-source software developed by GitHub. It consists of a Python client (agent) which is installed on the target system and a Python server infrastructure that manages and communicates with the clients. The primary goal of GRR is fast and scalable forensics and investigations to promptly triage security incidents.

FastDump

Source: http://hbgary.com

FastDump is a tool released by HBGary for collecting physical memory data from 32-bit Windows systems. FastDump Pro, a subsequent release, supports all 32-bit and 64-bit versions of Windows. FastDump allows the responders to promptly collect and analyze data during an incident.

FTK Imager

Source: https://accessdata.com

FTK Imager is a data preview and imaging tool for collecting reliable and sensible evidence. It is also used to make perfect copies (forensic images) of data without any changes to the original evidence. The forensic image is identical to the original evidence, including the unallocated space and file slack. This helps protect the original evidence from any harm during an investigation by using a copy or image of the evidence.

Linux Memory Extractor (LiME)

Source: www.github.com

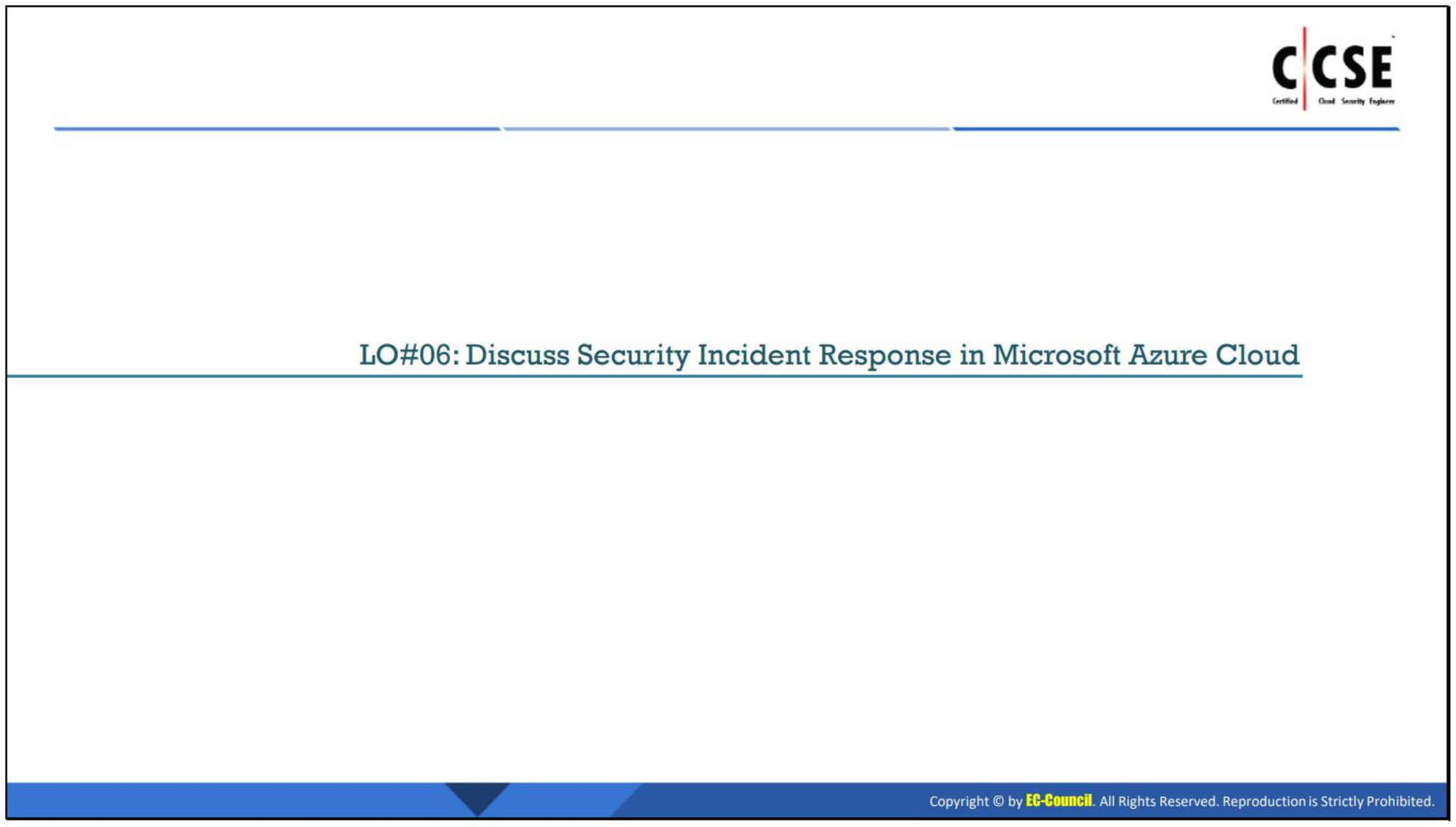
LiME is a loadable kernel module (LKM) that allows the acquisition of volatile memory from Linux-based devices, such as Android devices. It allows a full memory capture of Android devices and reduces the interaction between the user and kernel space during an acquisition. This enables a more effective memory capture than other tools.

Margarita Shotgun

Source: https://margaritashotgun.readthedocs.io

Margarita Shotgun is used for memory capture from a running Linux instance. It is also a standalone command-line to automate both on-premises and AWS memory captures. Margarita Shotgun makes use of LiME Project to capture memory. It has a pre-built repository of LiMe kernel modules to handle the memory acquisition process.

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

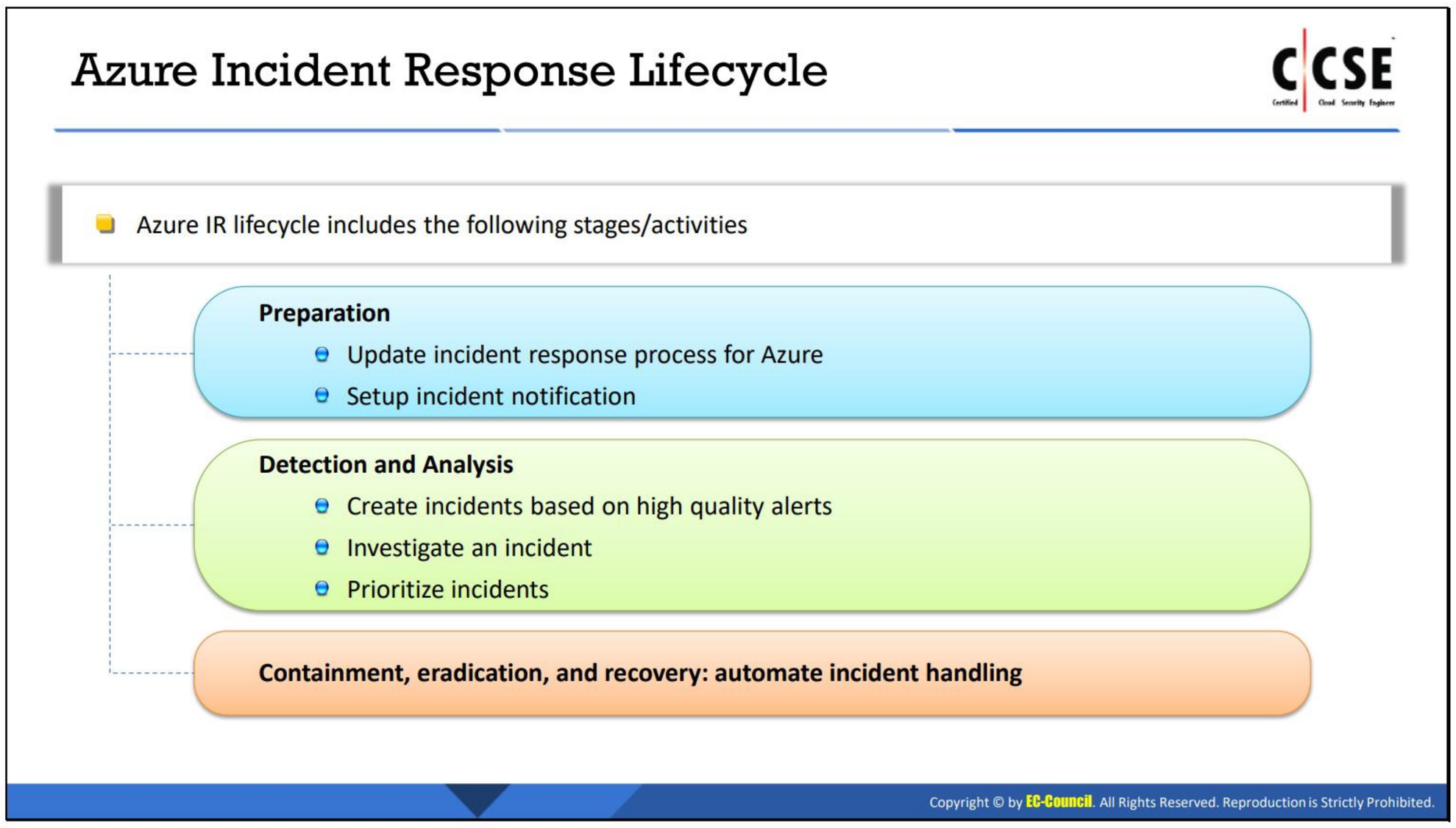


LO#06: Discuss Security Incident Response in Microsoft Azure Cloud

This section aims to detailly explain incidence response in Azure. It explains an Azure incident response plan and its implementation. It demonstrates the use of Azure Security Center, Azure Sentinel, and other tools for handling an incident response, along with the best practices for implementing Azure incident response (IR).

hidan01.ir

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



Azure Incident Response Lifecycle

Incident response includes controls throughout the IR lifecycle. It also leverages Azure services such as Sentinel and Azure Security Center (ASC) to automate the IR process.

Azure IR lifecycle includes the following stages/activities

- **Preparation**

  This stage includes the following:

  - **Update the IR Process:** Ensure the organization employs standard processes for responding to security incidents. Moreover, these processes should be regularly updated and tested to ensure readiness.
  - **Setup Incident Notification**: Ensure you set up incident contact information in ASC because Microsoft will use it to update any security incident.

- **Detection and Analysis**

  The detection and analysis stage involves the following:

  - **Create Incidents Based on High-quality Alert Guidance**: Incorporate a process to generate high-quality alerts and also to measure their quality. This helps in eliminating false positives. These alerts can be based on validated community resources, experience from previous incidents, and tools designed to create and clean up alerts.
  - **Investigate an Incident**: When investigating a potential incident, ensure the security analysts use multiple data sources (including centralized logging sources) for a better understanding.

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

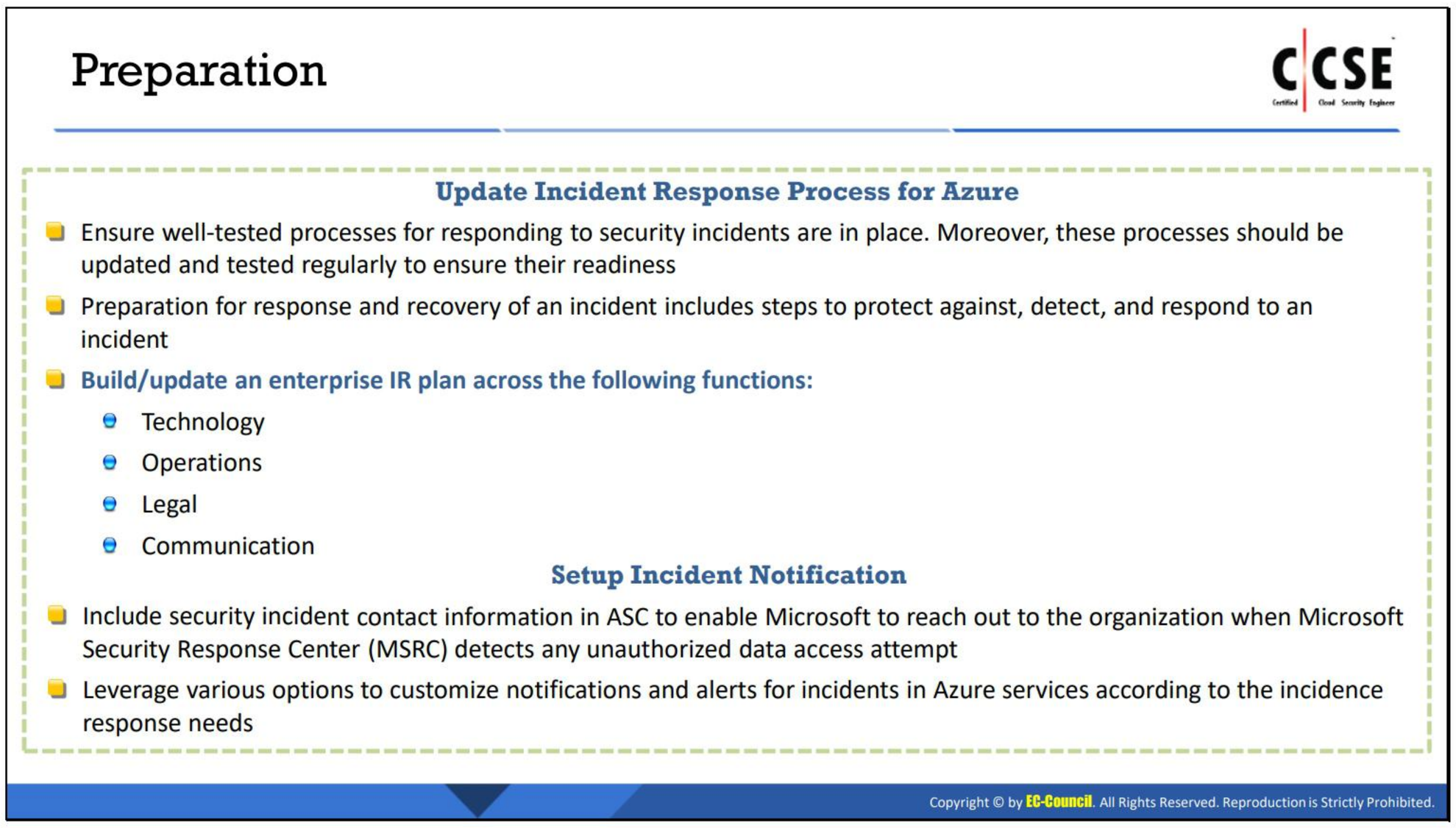
- **Prioritize Incidents**: Prioritize incidents based on their alert severity and asset sensitivity.

- **Containment, Eradication, and Recovery: Automate Incident Handling**

  Speed up the response time and offload the burden from analysts by automating repetitive tasks.

hide01.ir

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



Preparation

Organizations often face cyberattacks. An adequate preparation ensures a significant reduction in the risk/impact of an incident or attack on the business and convenient recovery and response processes. Ensure the organization has processes in place for responding to security incidents. In addition, update and test these processes regularly to ensure their readiness.

Build/update an enterprise IR plan across the following functions:

- Technology
- Operations
- Legal
- Communication

Technology

Preparation for incident response and recovery should include steps to prevent, detect, and respond to security incidents.

The following preparations are required for responding to incidents:

- **General Preparation**
  - **Identify HVA**: Identify critically important high-value assets (HVAs) such as servers, data files, and applications. This critical inventory collection helps in the recovery phase of an incident response. It also helps prioritize the protective and detective controls for HVAs and identify threats to them.

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

- **Ensure Reliable Software Deployment**: Ensure the scripts/installers can be executed rapidly on all endpoints for a recovery. Recovery efforts may be hampered because of unreliable or incomplete software deployment systems.

- **Investigation Preparation**
  - **Threat Detection and Monitoring Capabilities**: Ensure you have the required skills and tools to detect advanced attackers in the cloud environment.
  - **Forensic and Investigation Capabilities**: Ensure you have the required skills and tools to investigate targeted attacks (e.g., attack activity analysis and malware analysis).
  - **Track and Analyze the Cost of Response**: Keep a record of the cost incurred in responding to incidents to enable a better risk management. This includes direct costs (e.g., external services) and indirect costs (e.g., time spent by the team on investigation and recovery).

- **Recovery Preparation**
  - **Backup and Recovery Capabilities**: Ensure you have the required backup and recovery capabilities for critical data. For example, preparation for an attack that deletes or encrypts data needs you to have the ability to recover critical data using ransomware-resistant/ offline backups.
  - **Make Technical Documentations**: Document procedures that are often used during security incidents. This includes the following:
    - Compromised account recovery procedures
    - Compromised host recovery procedures
    - Network isolation and segregation procedures

hi4o1.ir

Operations

Handling a cybersecurity incident is challenging because it is technically complex and involves many unknown parameters. As incidents can impact business operations, an adequate planning and preparation is necessary for business continuity in the case of a cybersecurity incident.

- **Recommended Practices for Operations**

  The following are the recommended practices for operations to help reduce organizational risk:

  - **Adapt ICS for Crisis Management**: Use incident command system (ICS) in natural disasters and security incidents as it is useful in managing major incidents that could lead to a crisis.
  - **Establish a Framework**: Have a framework that specifies the IR program.
  - **Test/exercise the Crisis Process**: Ensure a recurring schedule for testing crisis processes and teams across all responsibility levels in relevant scenarios. The schedule must include exercises on individual components and tabletop exercises

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

with stakeholders. In addition, validate non-intrusive technical procedures (e.g., threat detection, and backup and recovery tools) during these exercises.

- **Emergency Approval Process:** Ensure a streamlined emergency approval process is used to handle sudden changes during an incident/emergency.
- **Have Clear Escalation Guidelines:** Have clear and documented guidelines on thresholds when the internal investigations should be escalated to specialists and third-party investigation teams.

- **Organizational Preparedness Self-Assessment**

  Organizations should self-assess their preparedness through the following:

  - **Core Strategy and Alignment:** Organizations must thoroughly understand their HVAs, the advanced controls for HVAs, and their high-probability attack vectors, along with assessing whether they can measure the impact on their business resources when not prepared for an attack.
  - **Security Operations:** Organizations must check whether they have a dedicated security operations center (SOC) for handling incidents, a designated security team for responding to known threats, a documented and tested process for incident response, and tools that are effective and useful in detecting threats.

Legal

A legal counsel plays a crucial role in the deployment, development, and execution of cybersecurity programs. Legal advisors provide legal advice on contractual, statutory, and regulatory duties. They also give recommendations on how to mitigate and manage risks resulting from investigations, audits, or litigations.

Following are some important aspects of proactive legal workflows in cybersecurity:

- **Designate a Cyber Lead from Legal:** Evaluating and managing legal risk is an integral part of IR preparation for most incidents. A legal counsel (external, internal, or both) must lead or direct certain IR preparation activities and involve external forensic and communications experts to maximize the chances of their work being covered under the attorney–client privilege.
- **Review Policies and Public Statements**: Review policies and public statements regularly to represent the current state and prevent any needless definitive statements on the organization's cybersecurity program.
- **Develop an IR Plan**: Create an IR plan as it is a key operational document that helps respond to incidents. Craft operationally effective IR processes with the help of an expert cyber counsel to reflect the latest insights from litigated cases and regulators.
- **Have Cybersecurity Assessments at Legal Counsel's Direction**: A legal counsel (internal or external) should work closely with cybersecurity consultants for vulnerability assessments, penetration testing, etc. to protect related work products,

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

communications, and deliberations under legal privilege. Prepare reports only under the direction (guidance) of a legal counsel to ensure minimal discovery risks.

- **Conduct Regular Board Briefings**: Ensure the board members/directors are briefed regularly on the important aspects of incidents and their associated risks. Without this knowledge, they cannot fulfill their fiduciary responsibilities.
- **Manage Third-Party Vendors**: Evaluate third-party vendors based on the risk they impose on the organization. Use agreements that clearly define the security standards the vendors must comply with when an incident occurs. Also, develop a process to audit, review, and certify vendors by testing their compliance with the security standards.

Communications

The main focus of communications should be on the actions that organizations take to remediate and investigate security incidents. This includes hiring forensics experts and notifying law enforcement to help investigate an incident along with any other general steps for its remediation. Communicating information on security incidents requires a deep understanding of the dynamics of cybersecurity issues and a careful planning. Disclosing or communicating initial findings early during an IR process/investigation is risky as the dynamic leads may be proved incorrect at a later stage. This results in a loss of credibility, increased negative coverage, and an additional news cycle.

Organizations must take the following steps to be prepared for a potential incident.

- **Designate a Communication Lead**: Ensure a communication lead is appointed in the core IR team. The communication lead must know about all aspects of the IR process and cybersecurity to effectively communicate the incident handling process. Inclusion of a communication lead in the core IR team facilitates communications and reputation management during a decision-making process.
- **Develop a Communications Portion**: Organizations often do not have a communications portion as a part of their IR plans. Develop a communications portion in the IR plan to ensure only the right information is disclosed. A communications-centric portion in the IR plan helps decide what, when, and to whom the information should be disclosed.
- **Map Stakeholders**: Map all stakeholders (e.g., regulators, customers, media, partners, etc.) who need to be informed about incidents. Understand the contractual obligations to inform certain customers or partners about incidents as this can save precious time during a live incident.
- **Create Draft Media-Holding Statements**: Ensure you develop draft media-holding statements and other related materials for major incidents. These statements are issued to the press when an initial investigation is under progress and facts are still unknown.
- **Have a Tabletop Exercise**: Conduct a tabletop exercise with all IR team members to test how they respond to press, customers, and regulators following security incidents. These tabletops are often conducted in collaboration with an external legal counsel to discuss the non-technical aspects of IR.

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

Preparation: Set Up Incident Notification

Set up the information of security incident contact in Azure Security Center, allowing Microsoft to connect with the organization if the Microsoft Security Response Center (MSRC) detects any unauthorized data access attempt. This helps review incidents to resolve them.

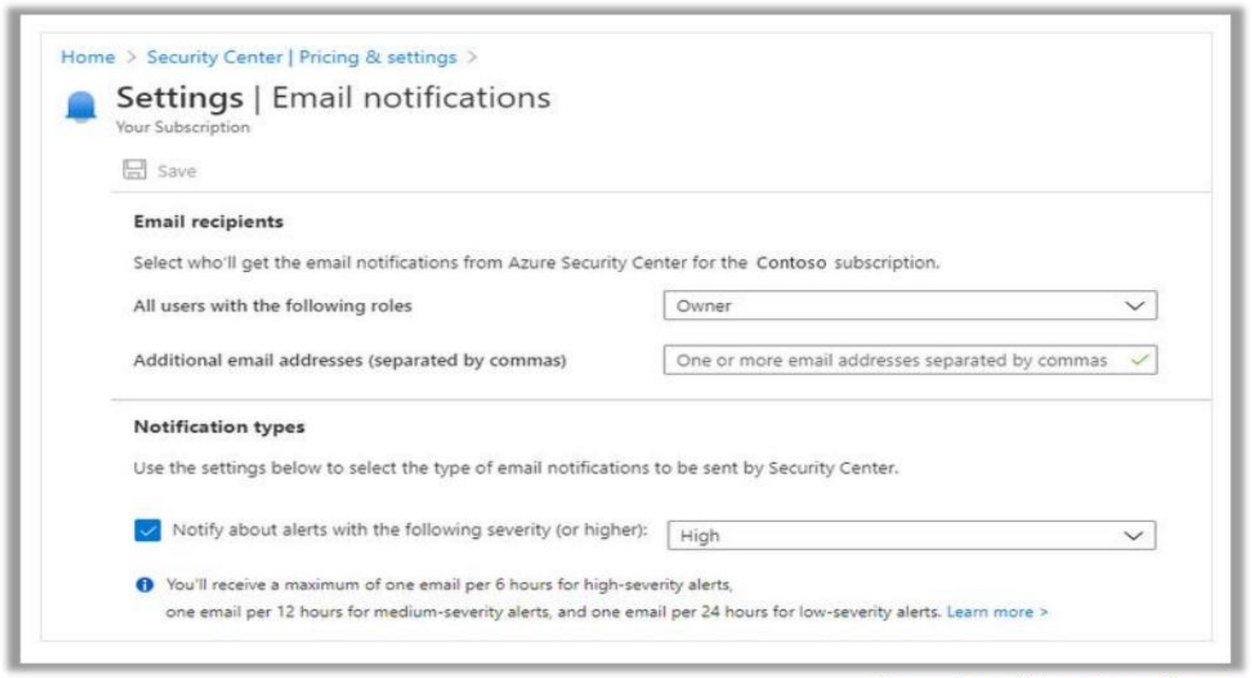
Use different options to customize notifications and alerts for incidents in Azure services according to the need of incident response.

hide01.ir

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

Set up Azure Security Center Security Contact

- By default, Azure Security Center emails the subscribers whenever a high-severity alert is triggered for their subscription
- To customize the email notifications and to know **who should be notified** and **what they should be notified about**, use Azure Security Center's **Email notifications** settings page



Source: https://docs.microsoft.com

Configure email notifications for security alerts
or
Set the Azure Security Center security contact

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

Set Up Azure Security Center Security Contact

Whenever a high-severity alert is triggered, Microsoft sends an email to the subscribers by default. You can change the email notification preferences by going to ASC's email notification settings page. The page allows you to choose the following:

- **Who Should Be Notified:** Security alerts can be sent to specified individuals or anyone with a particular Azure role for a subscription.
- **What They Should be Notified About:** Configure or modify the severity levels for which ASC will send email notifications

To avoid bulk mail alerts, ASC limits the number of outgoing email notifications for each subscription. The limits are described below:

- For high-severity alerts, it sends a maximum of 1 email per 6 hours.
- For medium-severity alerts, it sends a maximum of 1 email per 12 hours.
- For low-severity alerts, it sends a maximum of 1 email per 24 hours.

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

Steps to Set Up ASC Contact

Customize email notifications of security alerts via the portal using the following steps.

- Go to **Pricing and settings** in Security Center, choose your subscription, and then click on **Email notifications**.

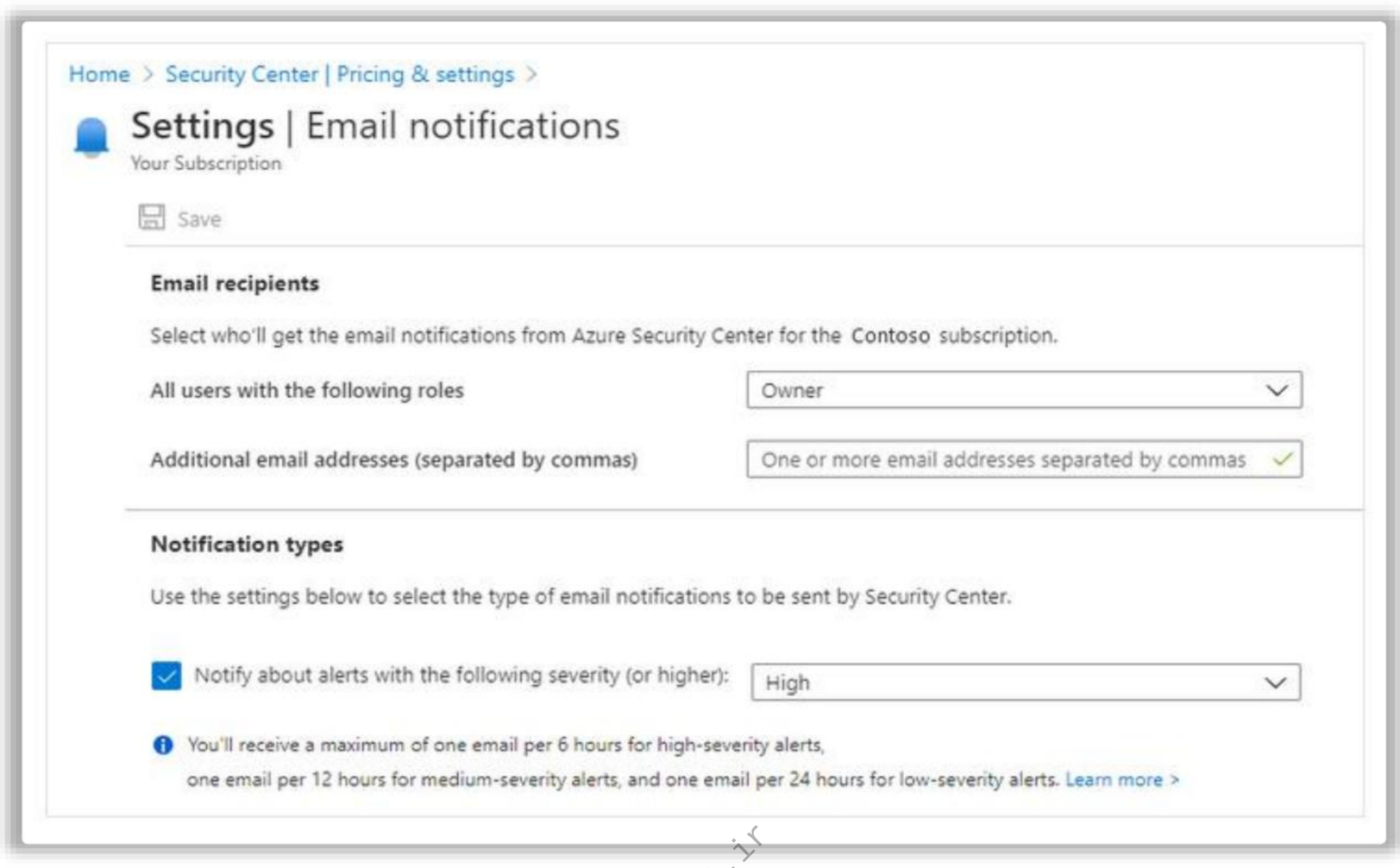


Figure 7.23: Email Notification

- Provide information about the recipient to whom the security alert notifications should be sent using any one or both options:
  - Selecting the available roles from the drop-down list
  - Manually entering the email addresses and using commas to separate them. Add any number of email addresses as there is no limit.
- Select **Save** to apply the security contact information.

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

Detection and Analysis

Generate Security Incidents based on High-quality Alerts

- Generate high-quality alerts and measure their quality to learn lessons from the past incidents and prioritize them for analysis
- **Use the below options to create incidents based on alerts:**
  - Stream alerts to Azure Sentinel via the ASC data connector, which will allow the creation of advanced alert rules for automatically generating incidents
  - Use the export feature to export ASC recommendations and alerts to detect risks to Azure resources

Investigate an Incident

- Collect logs to track the activities of attackers across the kill chain to prevent blind spots, and capture insights and learnings for future reference
- **The following data source options help to investigate an incident in Azure:**
  - **For network data:**
    - Capture network flow logs and other analytics using Azure Monitor and Network Watcher
  - **For taking snapshots of running (live) systems:**
    - Leverage the snapshot feature of Azure VMs to take a snapshot of the running system disk
    - Investigate incidents with Azure Sentinel
    - Utilize the native memory dump feature of the OS to take a snapshot of the running system memory

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

Detection and Analysis (Cont'd.)

Prioritize Incidents

hidedy.ir

Based on the alert sensitivity and alert severity, you should explain the context to analysts about incidents they must focus on initially

Use the severity levels of alerts assigned by the Azure Security Center to prioritize which alerts should be investigated first

Use tags to highlight resources and develop a naming system for identifying and categorizing the Azure resources to re-process sensitive data

Prioritize alert remediations as per

- Azure resources' criticality
- The environment where the incident has occurred

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

Detection and Analysis

Generate Incidents Based on High-Quality Alerts

Create high-quality alerts and measure their quality for a comparison with the previous incidents and prioritize them for analysis. Ensure you have a process to create these alerts because it helps analysts avoid wasting their time on false positives. These alerts can be based

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

on validated community resources, experience from previous incidents, and tools to create and clean up alerts. ASC provides high-quality alerts across multiple assets in Azure.

Options to create incidents based on alerts include:

- Streaming alerts to Azure Sentinel via the ASC data connector, which allows the creation of advanced alert rules for automatically generating incidents.
- Using the export feature to export ASC recommendations and alerts to detect risks to Azure resources.

Investigate an Incident

While investigating a potential incident, ensure the security analysts use multiple data sources to get a complete picture about what happened.

Track the activities of a potential attacker by collecting different types of logs. This helps in avoiding blind spots. Sources of data for investigation include centralized logging sources. These logs are already collected from the running systems and in-scope services. Use the below data sources to investigate an incident in Azure:

- **Network Data**: Capture network flow logs and other analytics using Azure Monitor and Network Watcher.
- **Snapshots of Running (Live) Systems**:
  - Leverage the snapshot feature of Azure VMs to take a snapshot of the running system disk.
  - Utilize the native memory dump feature of the OS to take a snapshot of the running system memory.
  - Investigate incidents with Azure Sentinel.

hide01.ir

During an investigation, intelligence on an incident can be associated with tracking and reporting. To manage the entire lifecycle of incidents, Azure Sentinel provides extensive data analytics capabilities.

Prioritize Incidents

Based on the alert sensitivity and severity, you should explain the context of incidents the analysts must focus on initially. This ensures they focus on the critical items first.

Use the severity levels of alerts assigned by the ASC to prioritize which alerts should be investigated first. The ASC assigns a severity to help prioritize alerts that necessitate an investigation.

Use tags to highlight resources and develop a naming system for detecting and categorizing Azure resources that process sensitive information.

Prioritize alert remediations according to the following:

- Azure resources' criticality
- The environment where the incident has occurred

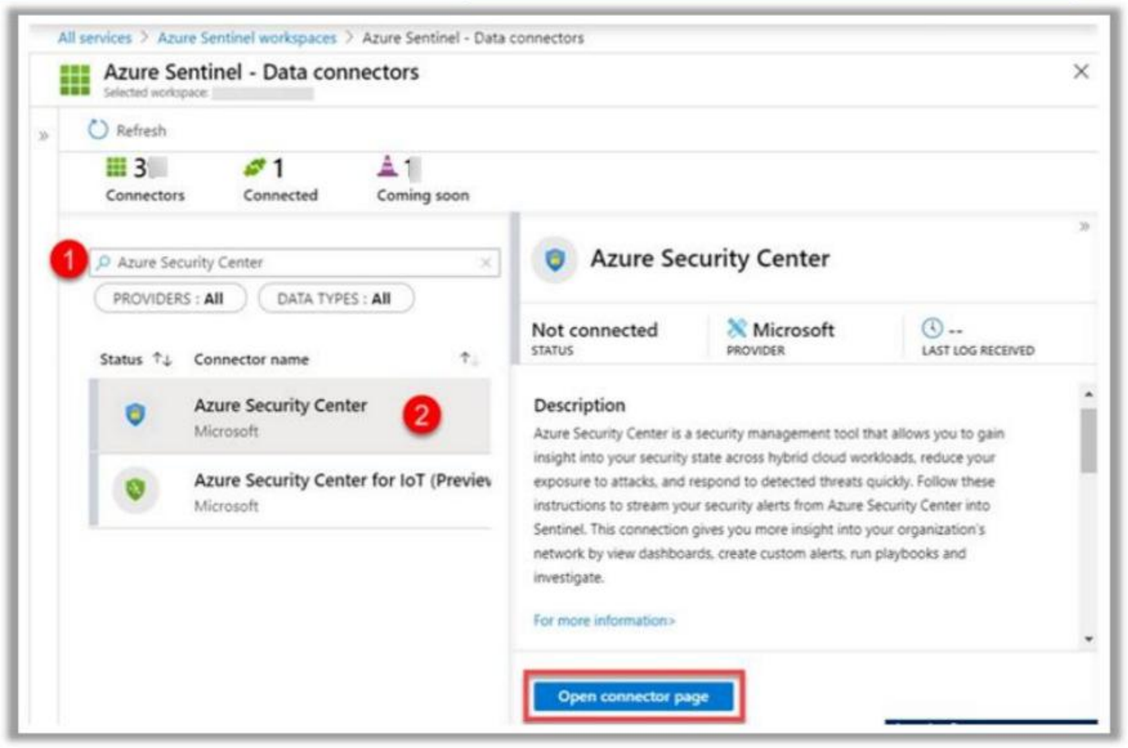
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Use ASC Data Connector to Stream Alerts to Azure Sentinel

- Use Azure Defender alert connector to take the Azure Defender alerts from Azure Security Center, and then stream them into Azure Sentinel

Steps to stream alerts into Azure Sentinel

- Enable and connect to Azure Defender
- Select Data connectors in Azure Sentinel
- Select Azure Defender alert from ASO (may still be called Azure Security Center) from the data connectors gallery and click the **Open connector page** button
- Click **Connect** next to each subscription under **Configuration**
- Click **Enabled** to turn on the default analytics rule under **Create incidents**



Open connector page of ASC

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

Use ASC Data Connector to Stream Alerts to Azure Sentinel

To stream alerts from Security Center into Sentinel, use Azure Defender. Follow the steps given below to connect Azure Defender to Sentinel.

- Choose **Data connectors** from the **Azure Sentinel** menu.
- Choose **Azure Defender alerts from ASC** from the **data connectors gallery** and select **Open connector page**.

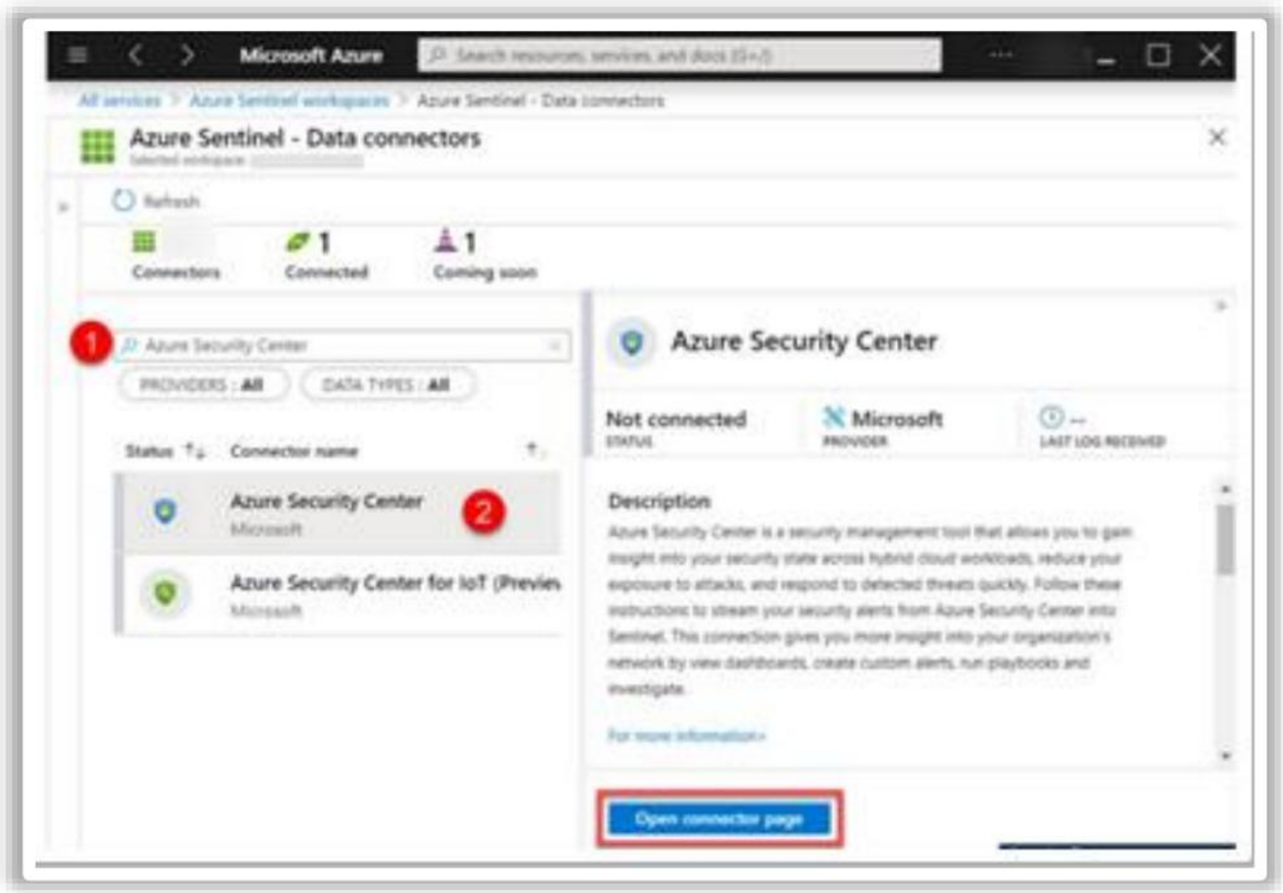


Figure 7.24: Azure Sentinel – Data Connector

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

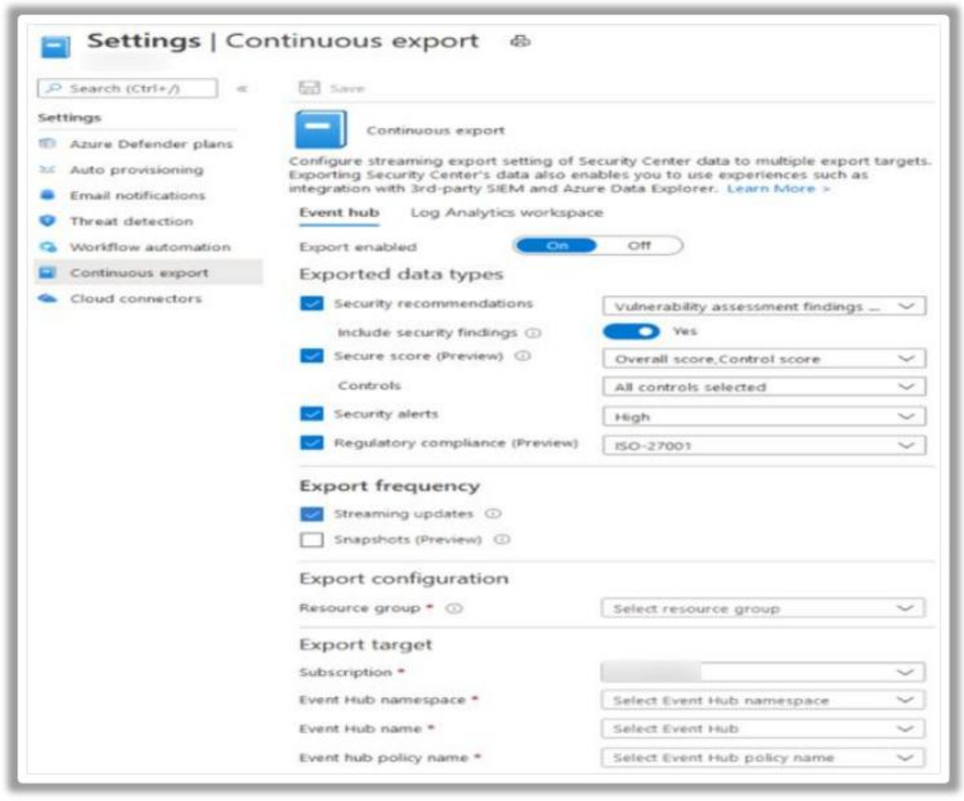
- Under **Configuration**, select the **Connect** button next to the subscription whose alerts are to be streamed in Sentinel.
- To allow alerts from Defender to automatically generate incidents in **Sentinel**, turn on the default analytics rule. To do this, choose **Enabled** under **Create incidents**. 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.

hide01.ir

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

Export ASC Alerts and Recommendations using the Export Feature to Identify Risks

- You can export some or all Azure Security Center's detailed security alerts and recommendations for tracking along with other monitoring tools in the organization's environment
- Use **Continuous export** to customize **what** will be exported and **where** it will go
- From the ASC page in the Azure portal, configure **continuous export**



Use the ASC pages in Azure portal for configuring a continuous export

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

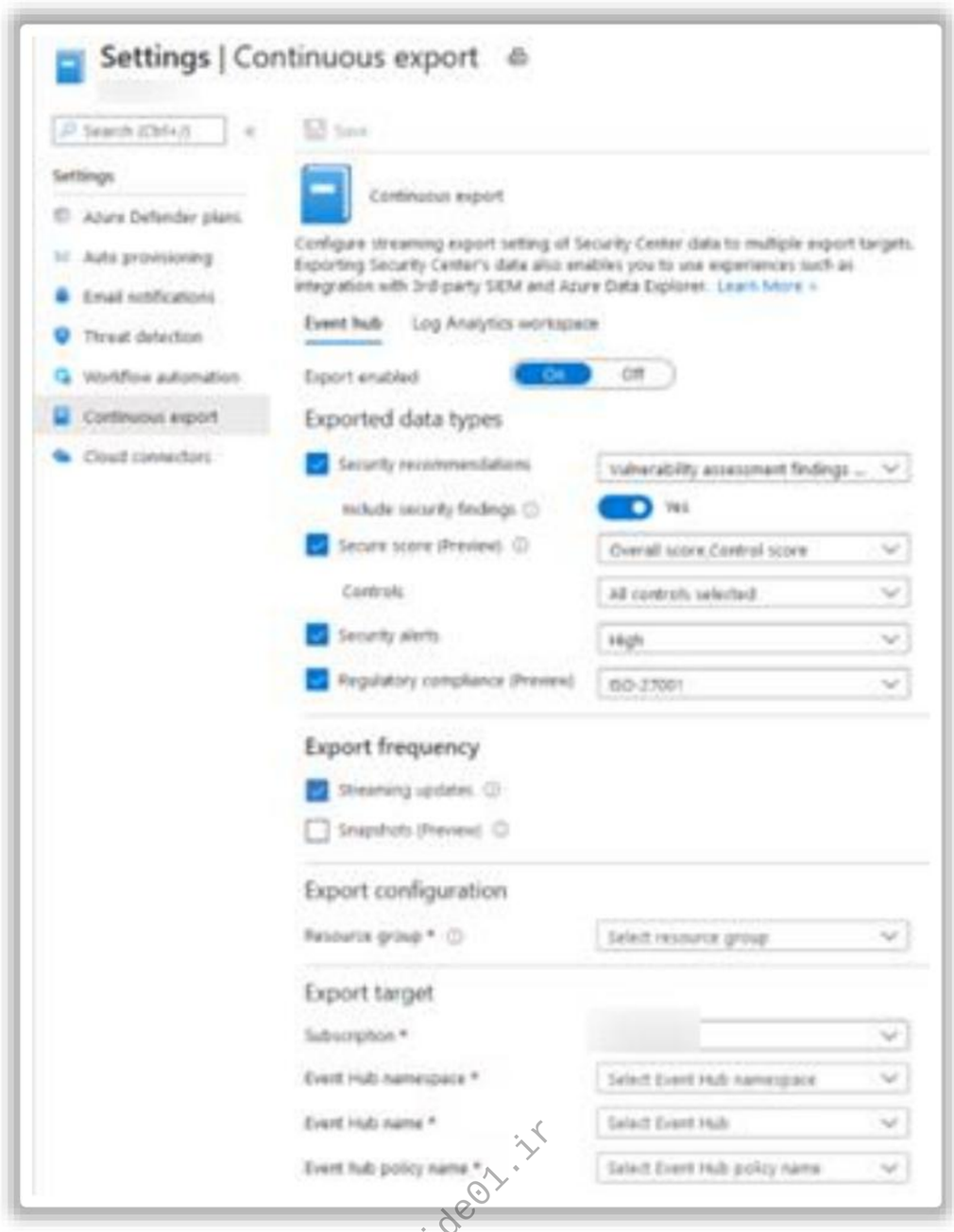
Export ASC Alerts and Recommendations using the Export Feature to Identify Risks

For a better identification of risks to Azure resources, use the continuous export feature, which exports Security Center alerts and recommendations. This feature allows the export of alerts and recommendations either manually or in a continuous mode. Follow these steps for continuously exporting to Azure Event Hubs or Log Analytics workspace:

- Choose **Price & Settings** from the ASC's side bar.
- Choose the subscription for which the data export is to be configured.

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

- Select **Continuous Export** from the settings page of that subscription.



hide01.ir

Figure 7.25: Continuous Export

- Choose the data type to export and use filters to choose from each type (e.g., export only high-severity alerts).
- Choose a suitable export frequency from **Streaming** and **Snapshots**.
- Optionally, enable **Include security findings** and click on Save.

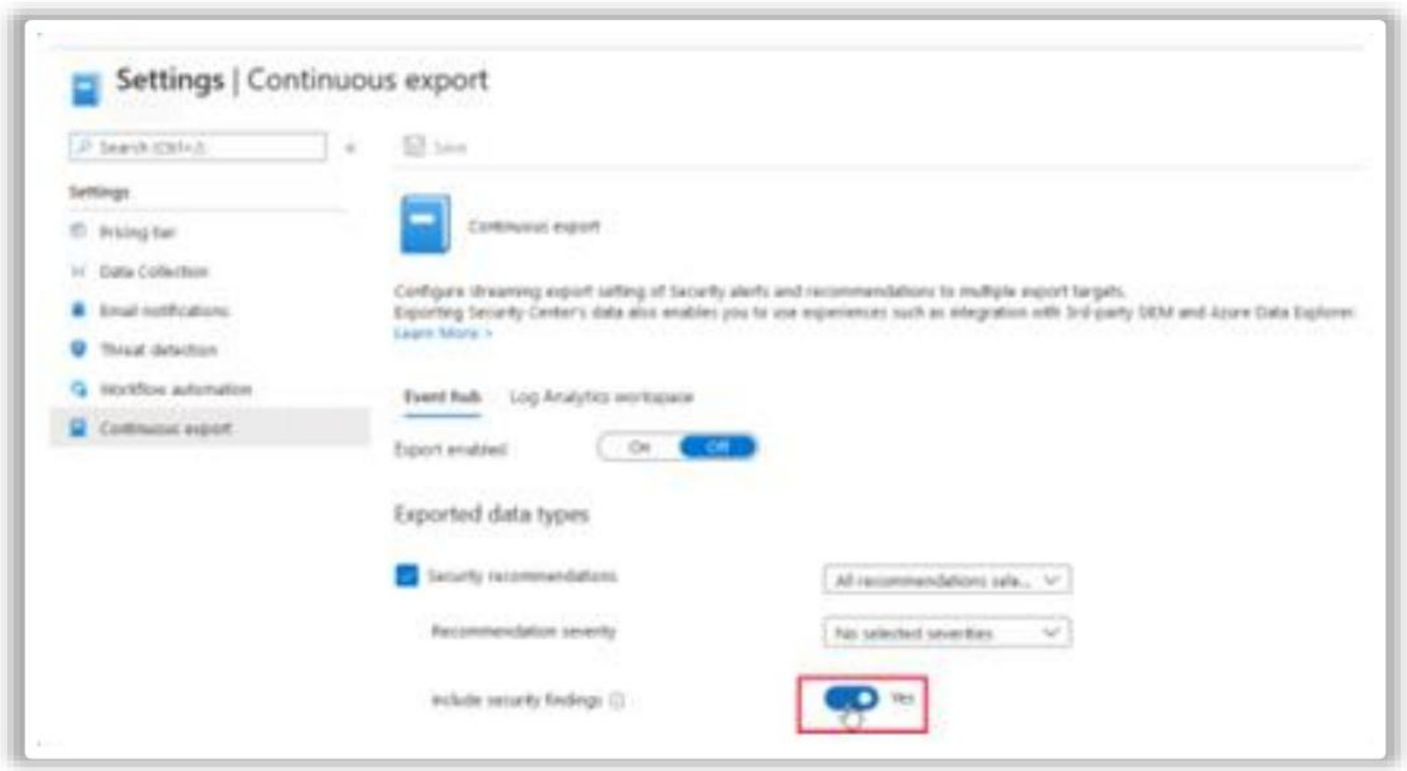
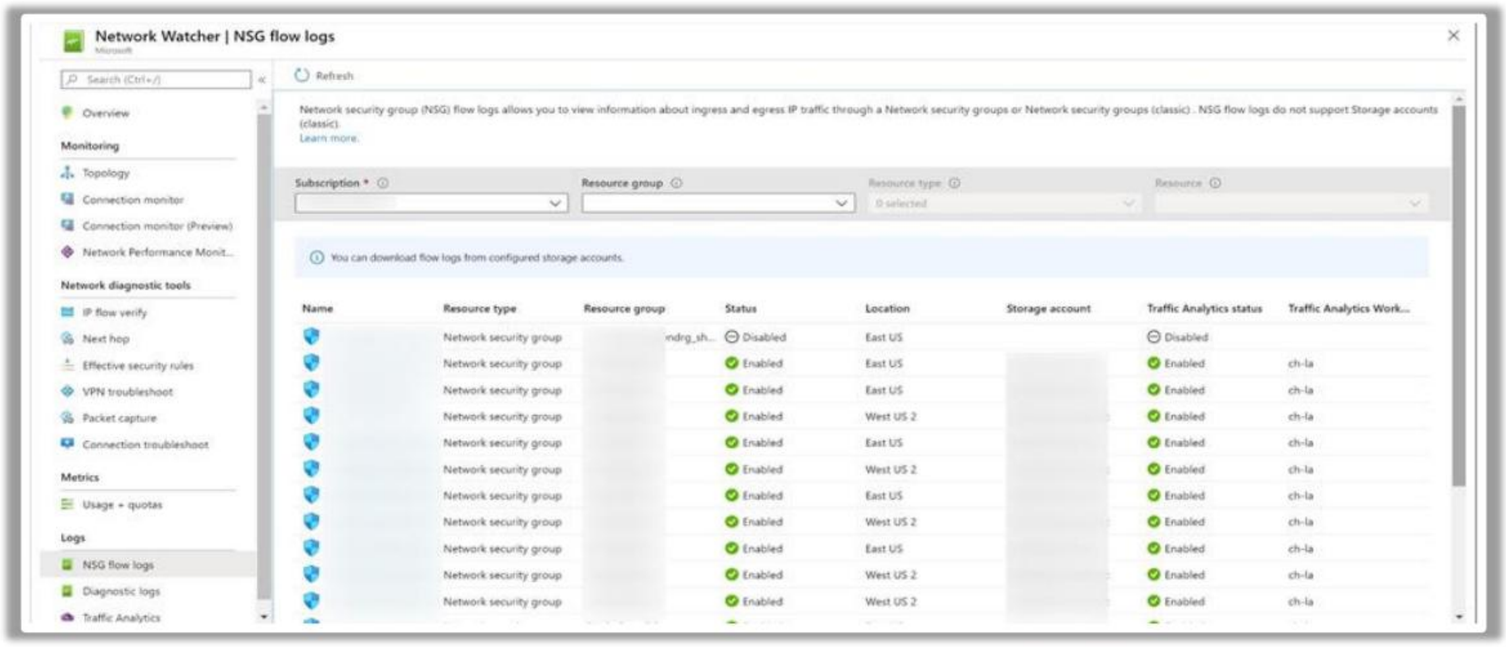


Figure 7.26: Including Security Findings

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

Capture Network Flow Logs using Azure Network Watcher

- Use the network security group (NSG) flow logs feature of Azure Network Watcher, which helps log the IP traffic flowing through an NSG



Azure Network Watcher network security group (NSG) flow logs

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

Capture Network Flow Logs Using Azure Network Watcher

Use the network security group (NSG) flow logs feature of Azure Network Watcher, which helps log the IP traffic flowing through an NSG. An NSG helps filter network traffic to and from a VM. With the flow log capability of Network Watcher, the log traffic that passes through an NSG can be captured.

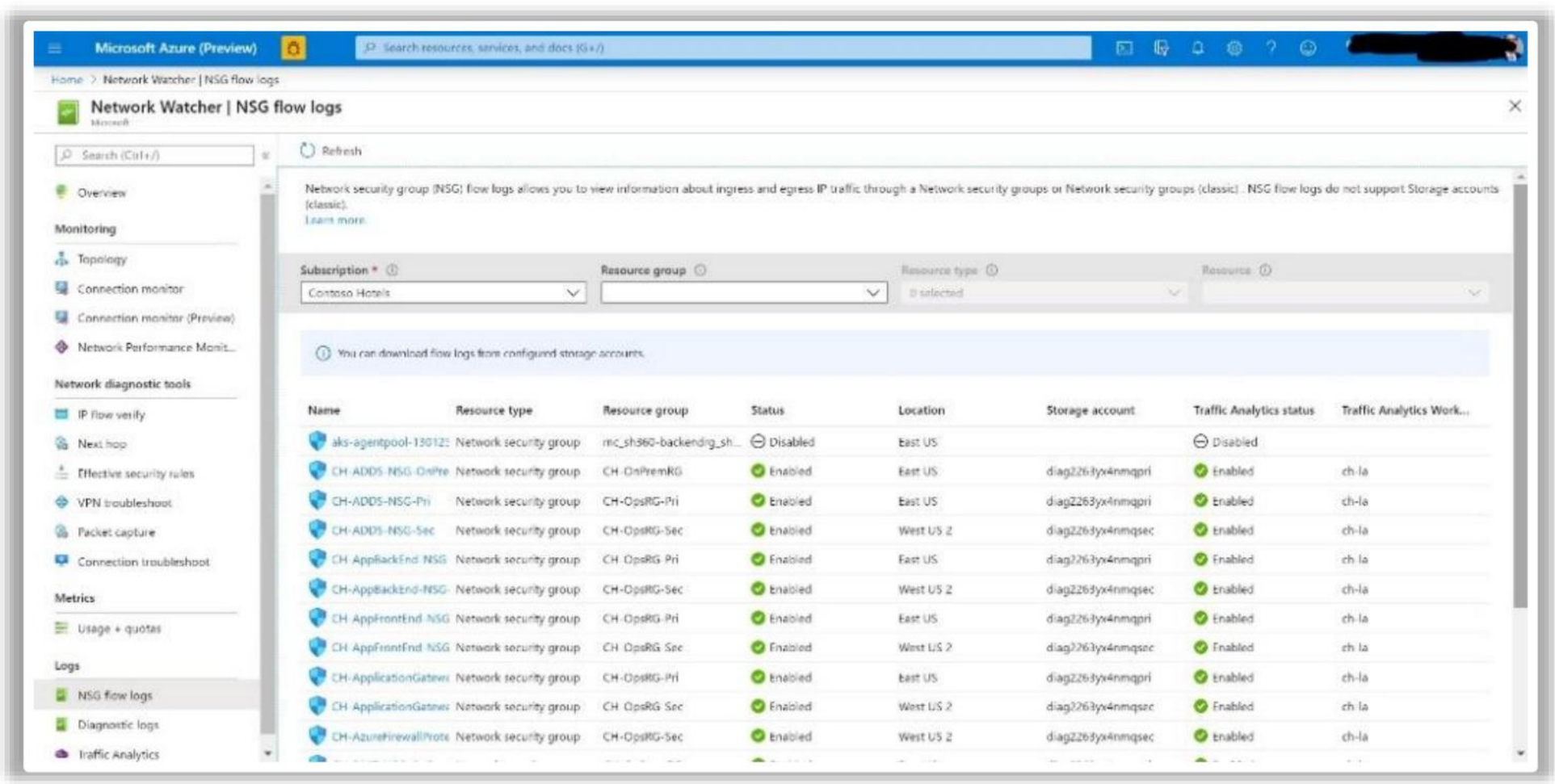


Figure 7.27: NSG Flow Logs

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

Steps to Capture Network Flow Logs Using Network Watcher

- **Create a VM**
  - Choose **+Create a resource** on the Azure portal.
  - Choose **Compute** and click on **Windows Server 2016 Datacenter** or any **Ubuntu Server** version.
  - Provide the requested information and then choose **OK**
  - Choose the VM size and click **OK**
  - Choose **Create** under **Create** of **Summary** to begin the VM deployment. The deployment will take some time.
- **Enable Network Watcher**
  - Choose **All Services** on the portal, and then type **Network Watcher** in the search box and select it.
  - Expand **Regions** and choose (**…**) on the right-side of **East US**.

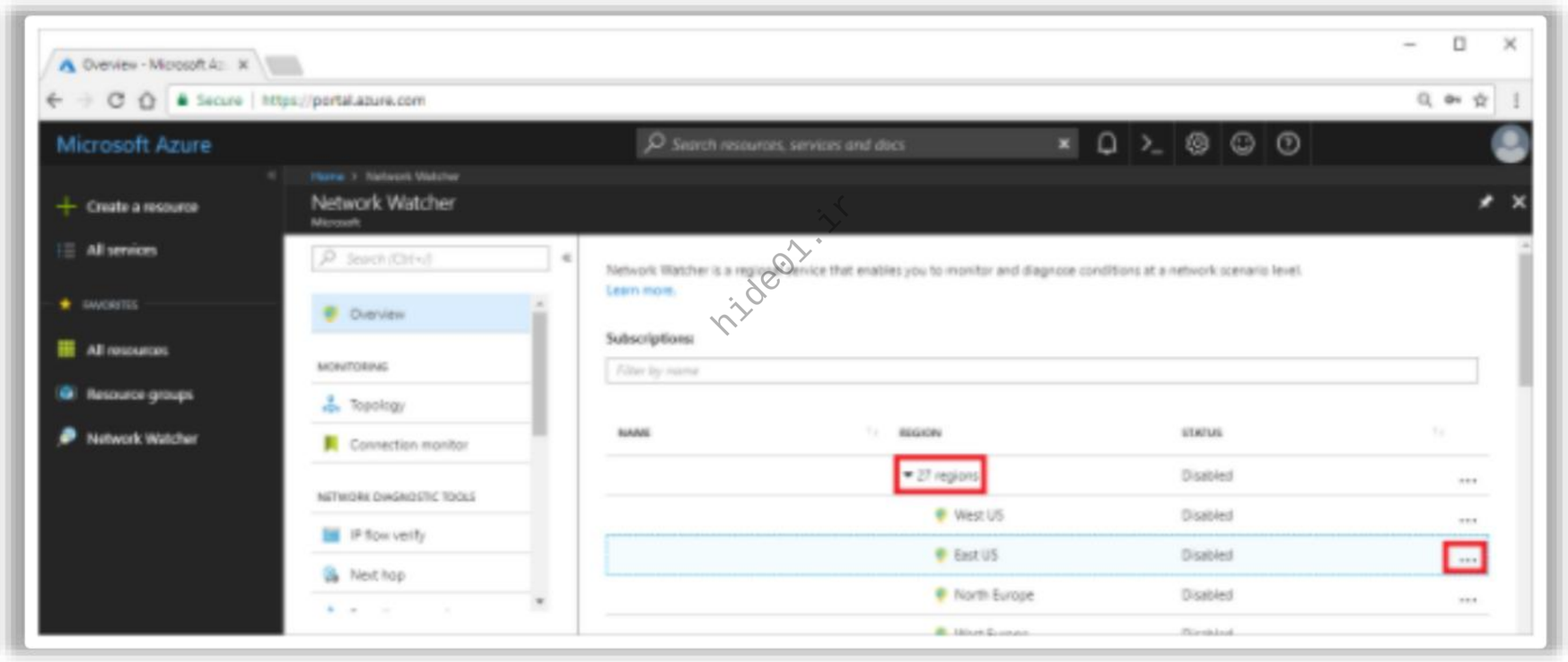


Figure 7.28: Expanding Region

  - Click on **Enable Network Watcher**.
- **Register Insights Provider**
  - Choose **All Services** on the portal, and then type subscriptions in the search box and select it.
  - Now, select the subscription for which you want to enable the provider.
  - Under **SETTINGS**, choose **Resource providers**.

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

- Ensure the status is shown as **Registered** for the **microsoft.insights** provider. Choose **Register** if the status shows **Unregistered.**

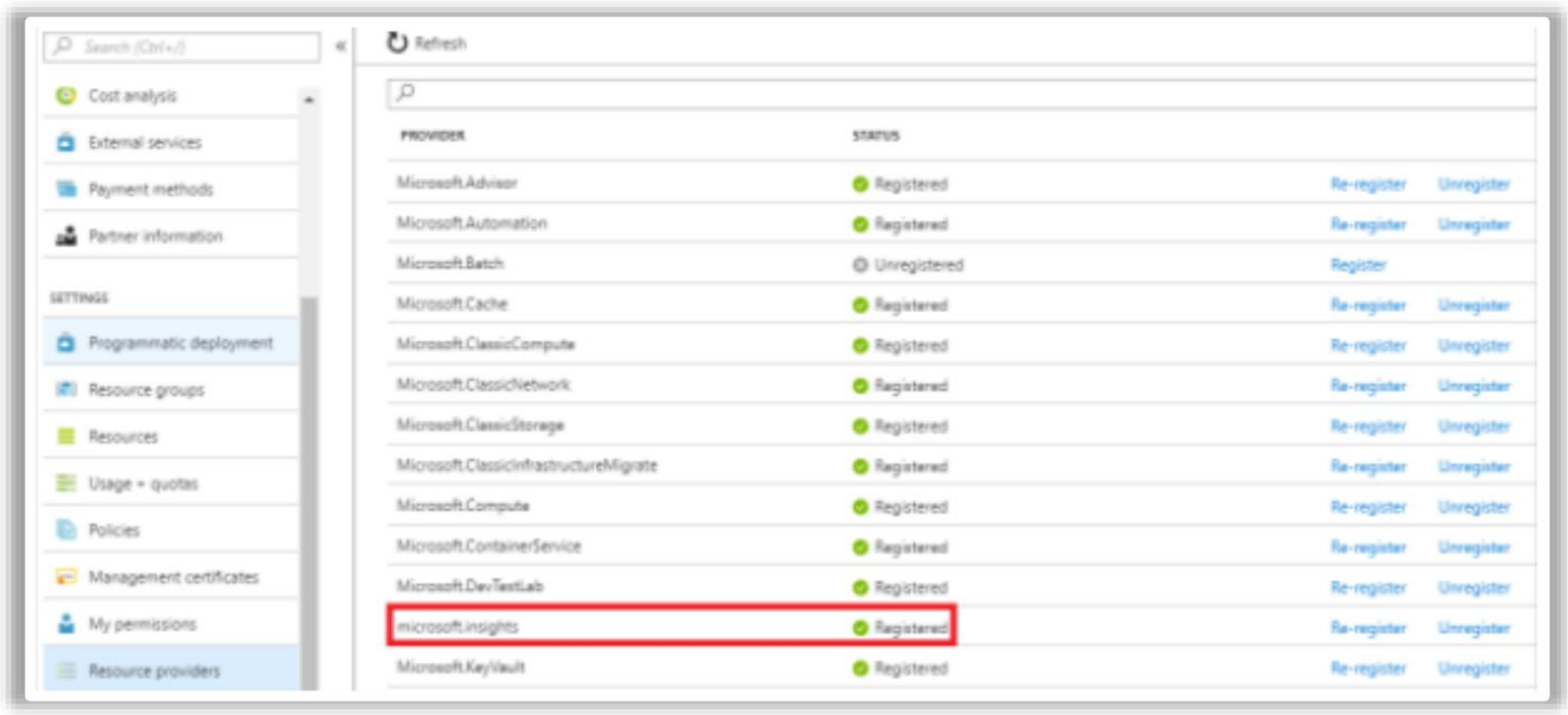


Figure 7.29: Registering for Microsoft.insights Provider

- **Enable NSG Flow Logs**
  - Create an Azure Storage account (as flow log data is sent to the storage account) by selecting **+ Create a resource** on the portal.
  - Choose **Storage** and then click on **Storage account- blob, file, table, queue**
  - Fill in the required information as shown below, accept the defaults, and choose **Create**.
    - **Name**: enter a name (3–24 characters)
    - **Location**: choose East US
    - **Resources group**: choose **Use existing** and then click on **myResourceGroup**
  - After the storage account is created, choose **All services** on the top left of the portal. Search for **Network Watcher** and select it via the filter box.

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

- Choose **NSG flow logs** under **LOGS.**

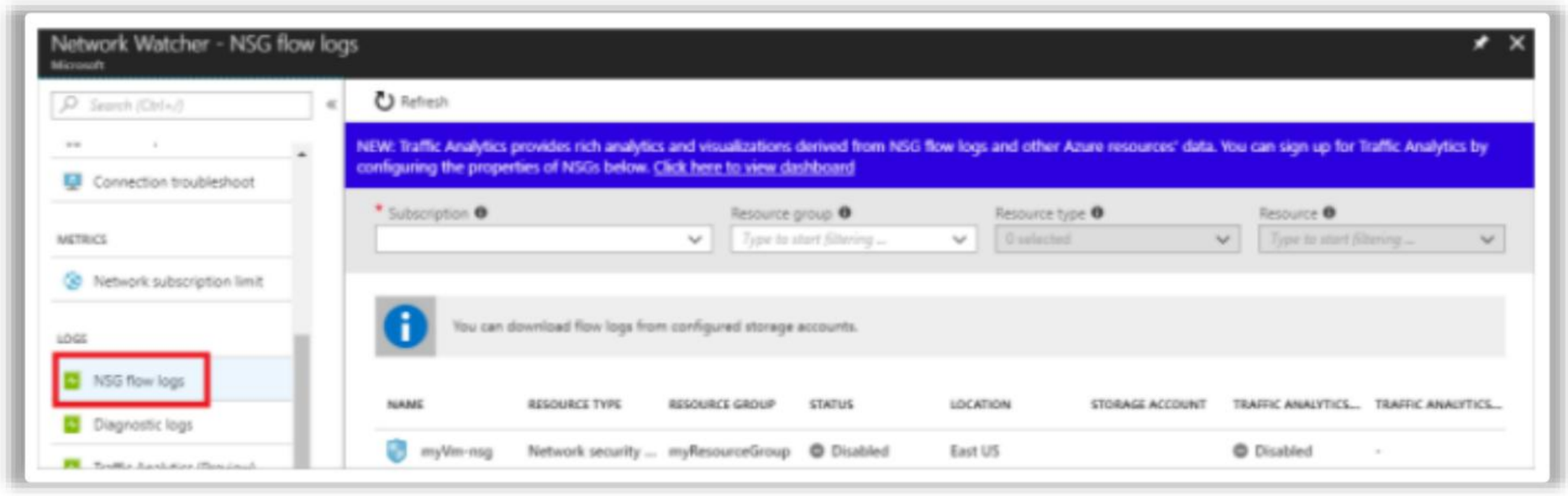


Figure 7.30: NSG Flow Logs

- Choose the NSG (**myVm-nsg**) from the list of NSGs.
- Choose **On** under the **Flow log settings** and select the appropriate flow logging version.

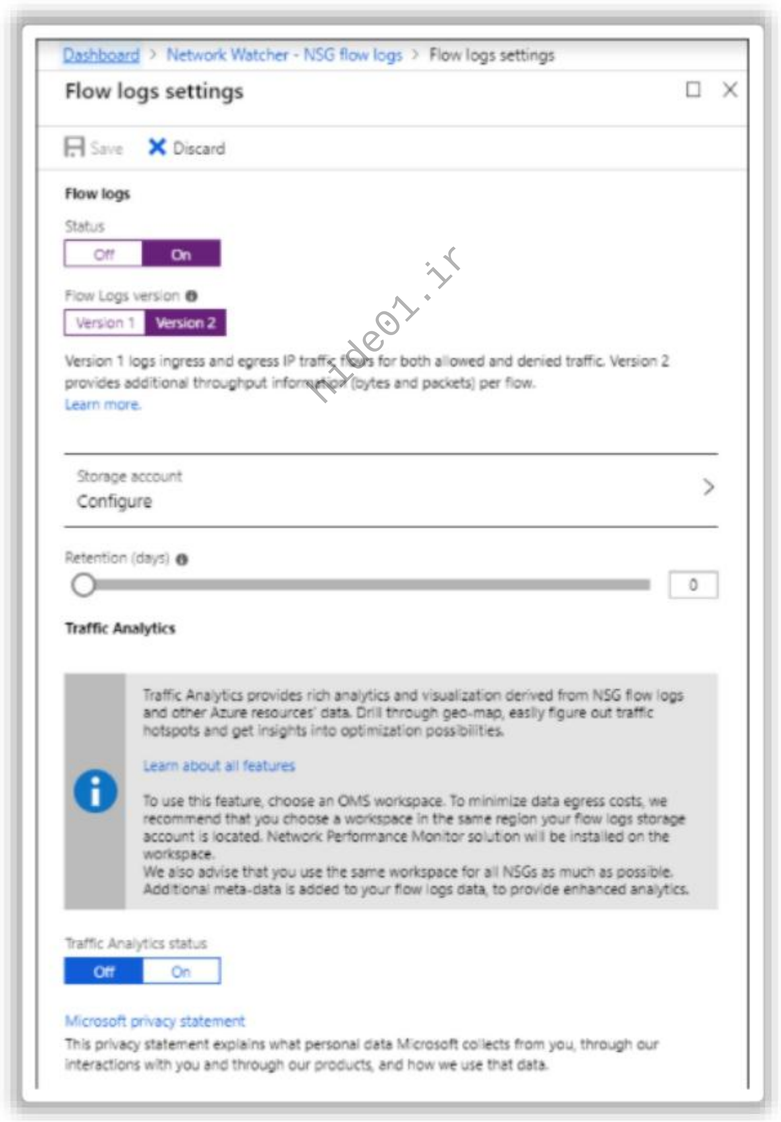


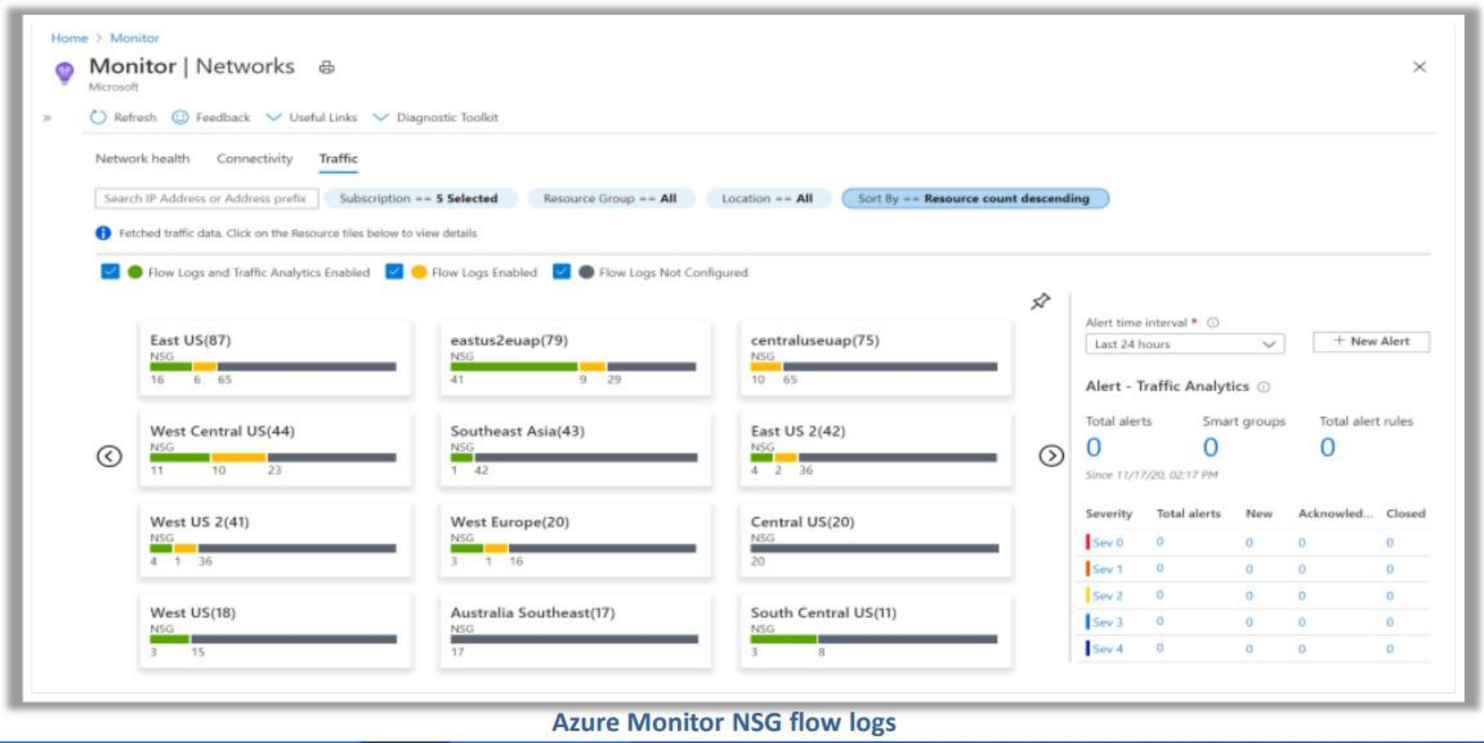
Figure 7.31: Turning On Flow Logs

- 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 then choose **Save.**

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

Capture Network Flow Logs using Azure Monitor

- Configure all NSG flow logs for the selected subscriptions grouped by location using Azure Monitor



Azure Monitor NSG flow logs

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

Capture Network Flow Logs Using Azure Monitor

Configure all NSG flow logs for the selected subscriptions grouped by location using Azure Monitor.

Steps to Capture Network Flow Logs Using Azure Monitor

- On Azure Monitor page, go to the **traffic** tab to access all NSGs configured for flow logs and Traffic Analytics for the chosen subscriptions.
- Use the search option in Azure Monitor to identify the NSGs configured for the searched IP address.

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

- NSGs will be shown along with the NSG flow logs and Traffic Analytics configuration status in a tiled regional view.

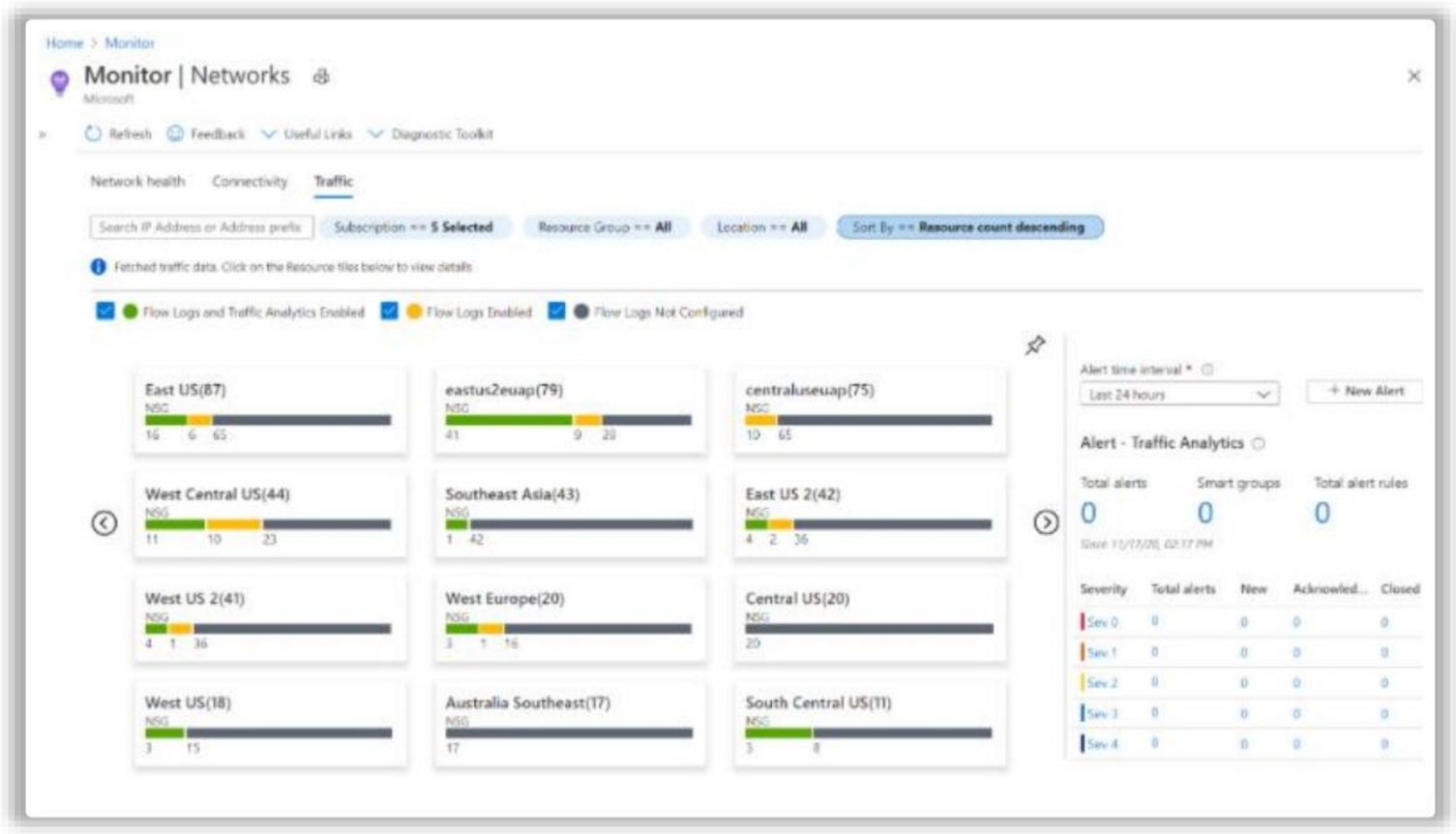


Figure 7.32: NSG Flow Logs and Traffic Analytics Configuration Status

- Select a region tile. A grid view will be shown with Traffic Analytics and NSG flow logs.

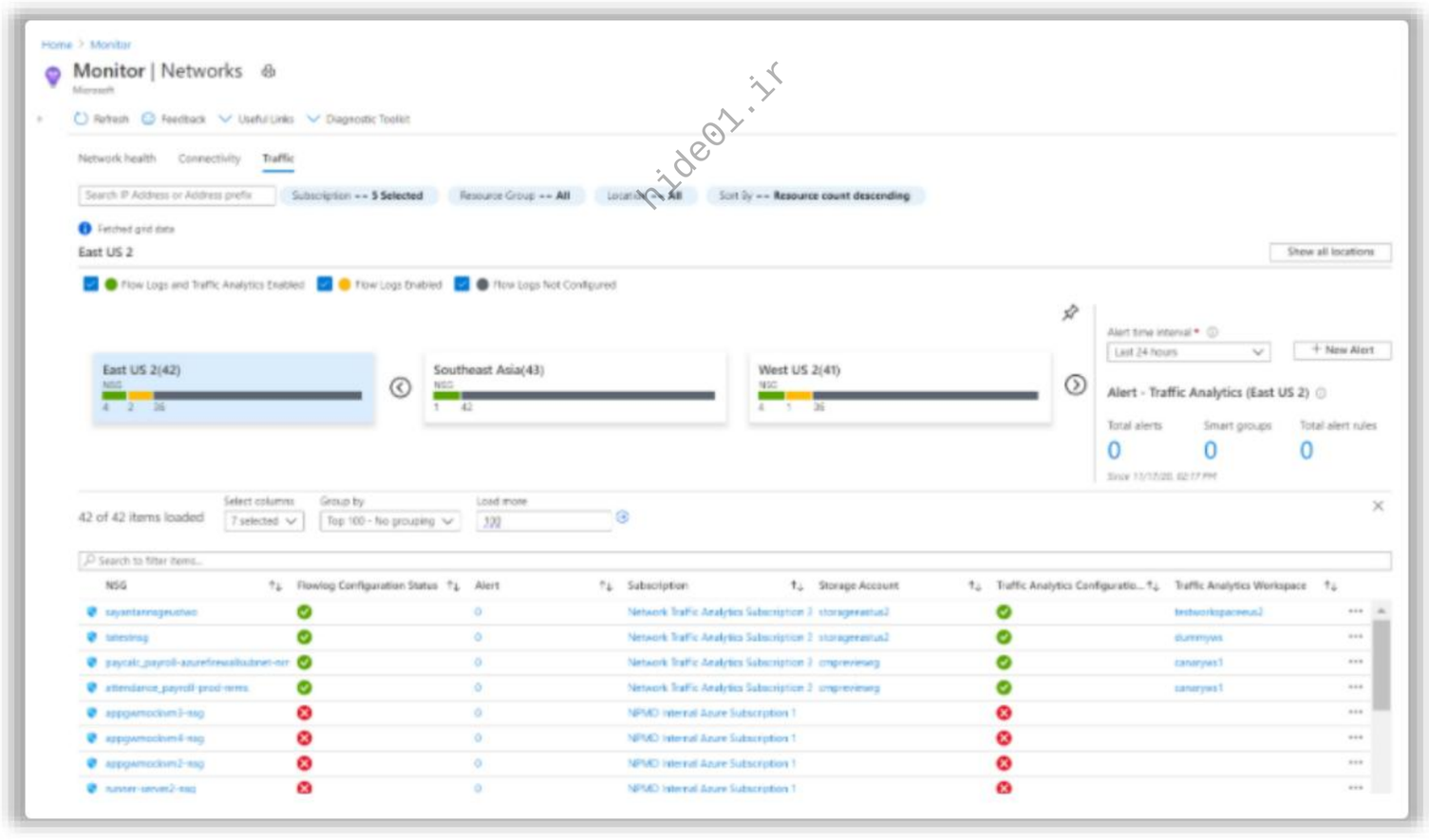
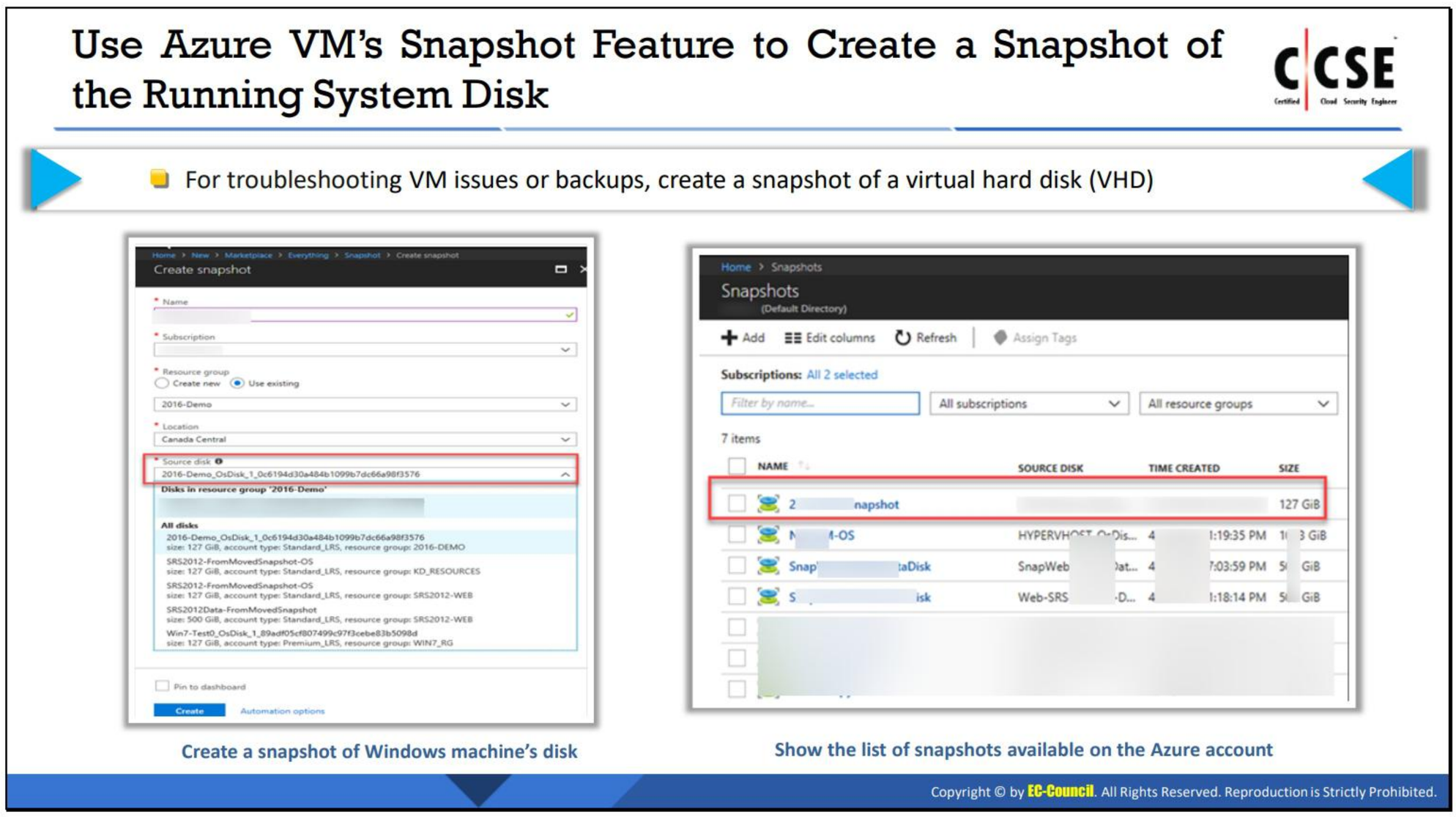


Figure 7.33: Grid View with Traffic Analytics and NSG Flow Logs

- To edit the NSG flow log and Traffic Analytics configuration, choose **Flowlog Configuration Status**.
- To go to traffic alerts configured for the chosen NSG, choose the value in the **Alert** column.
- Select **Traffic Analytics Workspace** to go to the Traffic Analytics view. The Alert box offers a view of all Traffic Analytics workspace-based alerts. To go to the detailed alerts page, select the alert counts.

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



Use Azure VM's Snapshot Feature to Create a Snapshot of the Running System Disk

Take new snapshots of a VM's virtual hard disks (VHDs) before making/testing major development changes, testing new application settings, adding Windows updates, etc., so that if anything goes wrong, the previous state can be easily restored.

Steps to Create a Snapshot of VHDs

- Choose **Create a resource** on the Azure portal.
- In the search bar, search for **Snapshot** and select it from the results.
- Choose **Create** on the **Snapshot** blade.

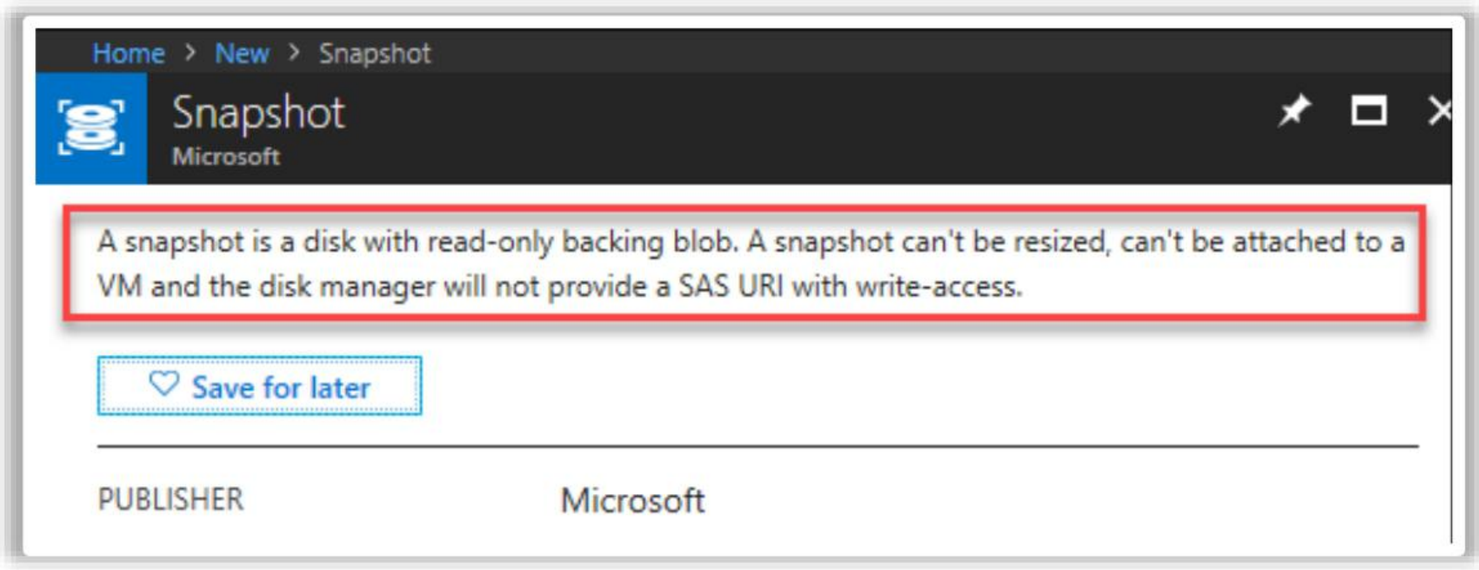


Figure 7.34: Snapshot

- Provide a name to the snapshot and select the **Resource Group**, **Subscription**, and **Location**.

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

- Choose the managed disk to snapshot for **Source disk**.
- Choose the **Account type** to store the snapshot. Choose **Standard_HDD** unless it is to be stored in a high-performing disk, and click on **Create**.

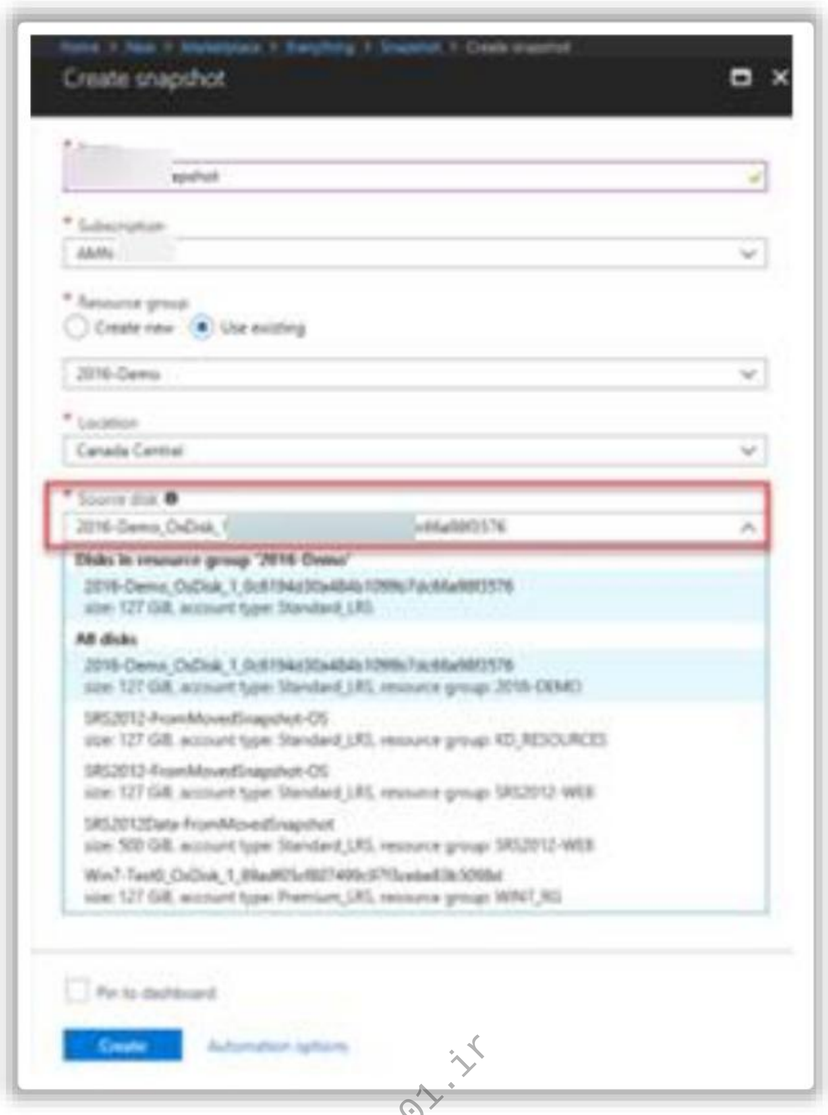


Figure 7.35: Selecting Source Disk

- The newly created snapshot will be visible in the **Snapshot** list available on the Azure account.

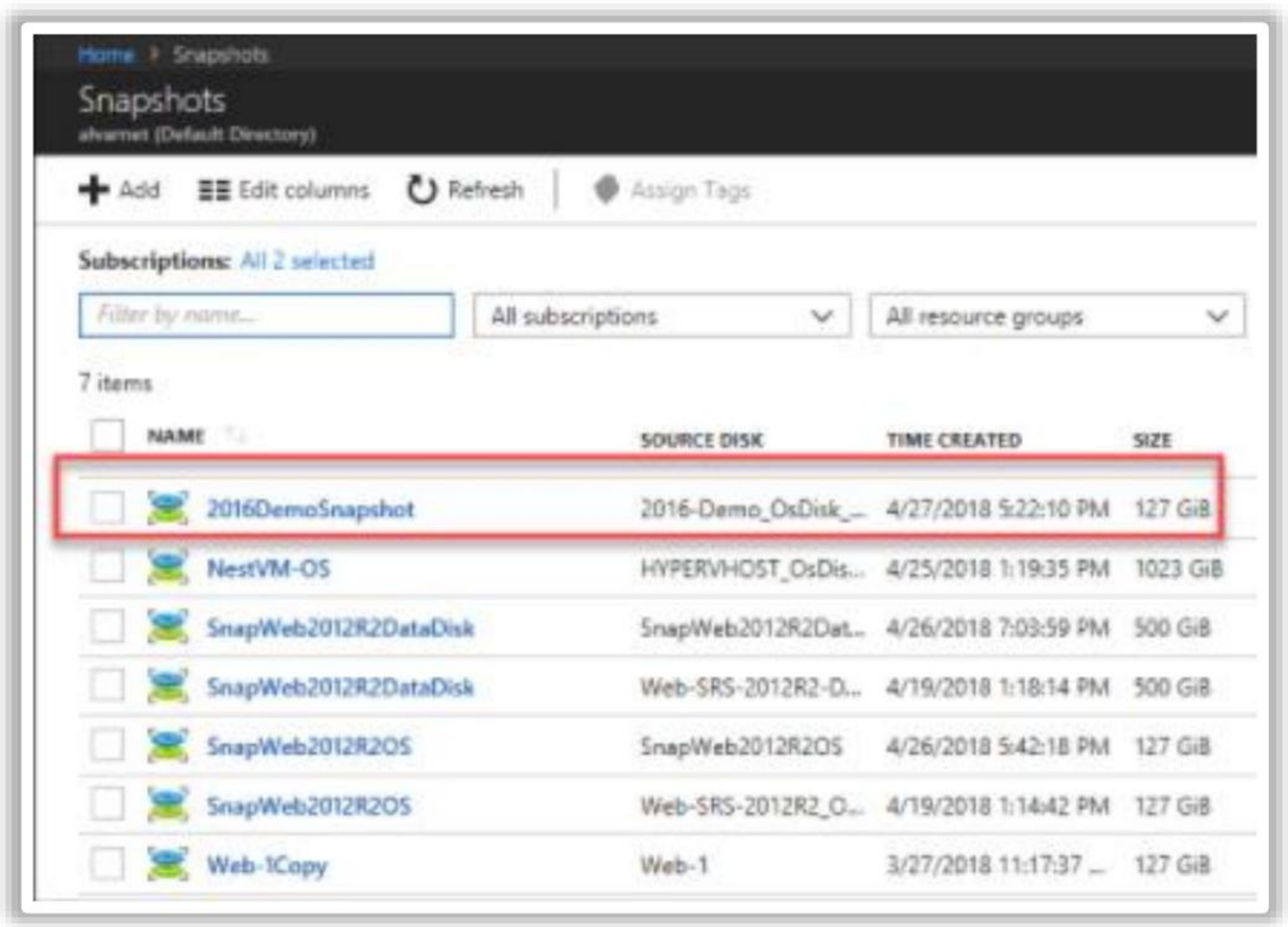
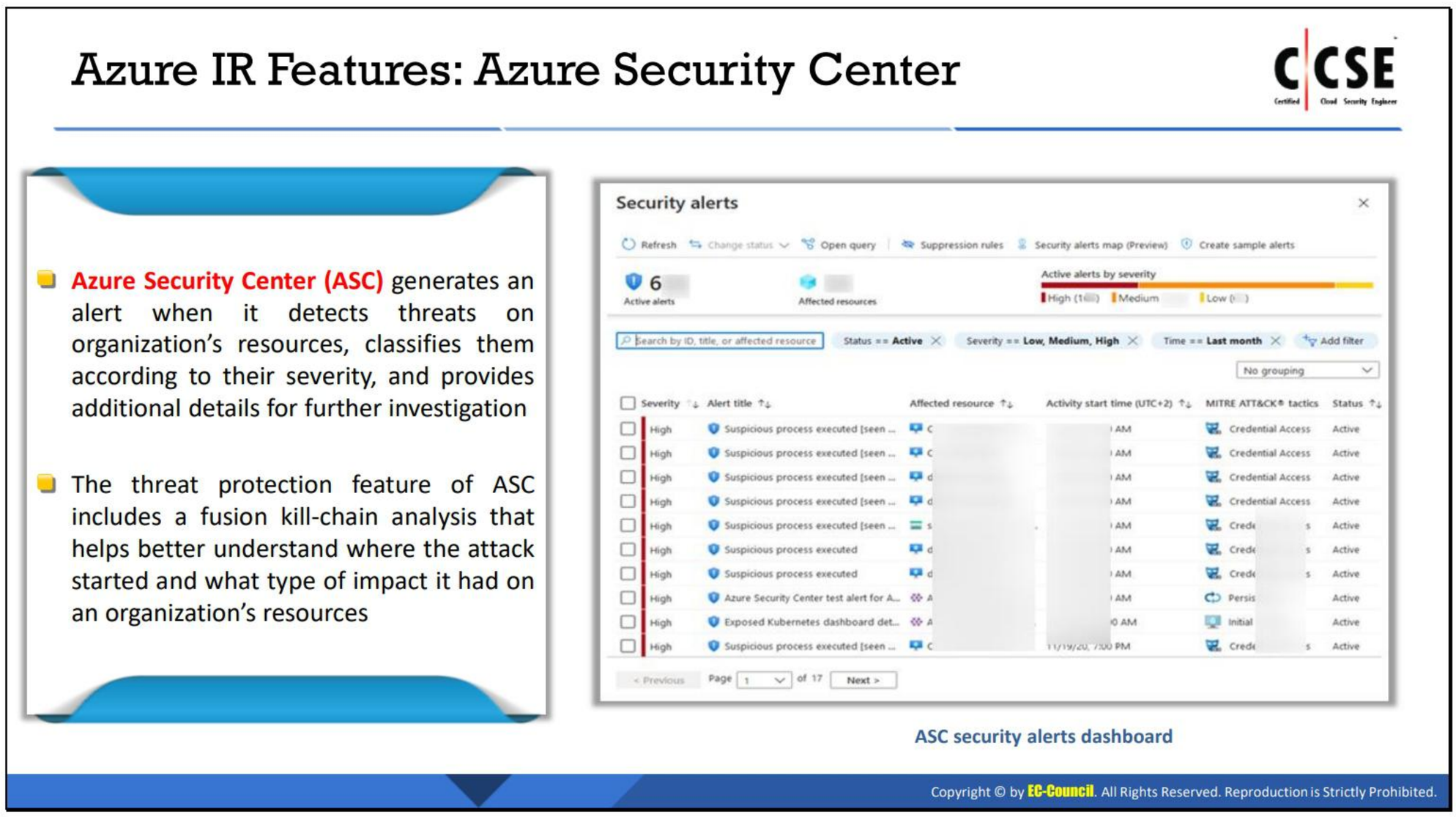


Figure 7.36: Snapshot List

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



Azure IR Features: Azure Security Center

Azure Security Center (ASC) is a security management system that helps prevent, identify, and respond to threats by offering a greater control over and enhanced visibility into Azure resources. It offers an advanced threat protection across all hybrid workloads (available on-premises and in Azure) and secures the data center by strengthening its security posture. ASC's threat protection feature includes fusion kill-chain analysis, which helps better understand the origin of an attack and its impact on an organization's resources.

It helps incident responders detect and respond to incidents easily with its security alerts feature. Moreover, it provides incident-related artifacts and information during investigations, which help in understanding the cause of threats or anomalies. It generates an alert on detecting threats to an organization's resources, classifies alerts based on their severity, and provides the additional details required for a further investigation.

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

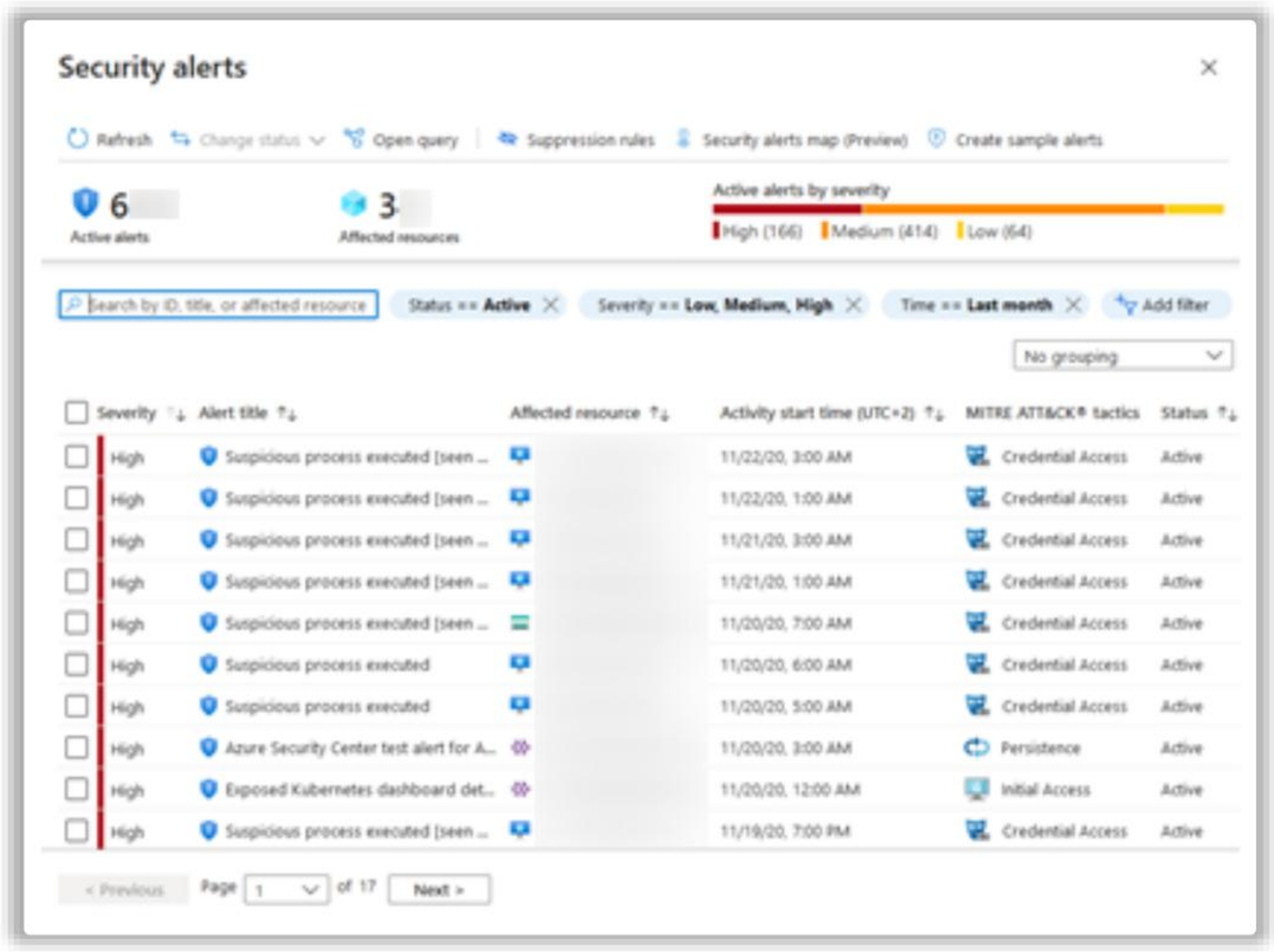


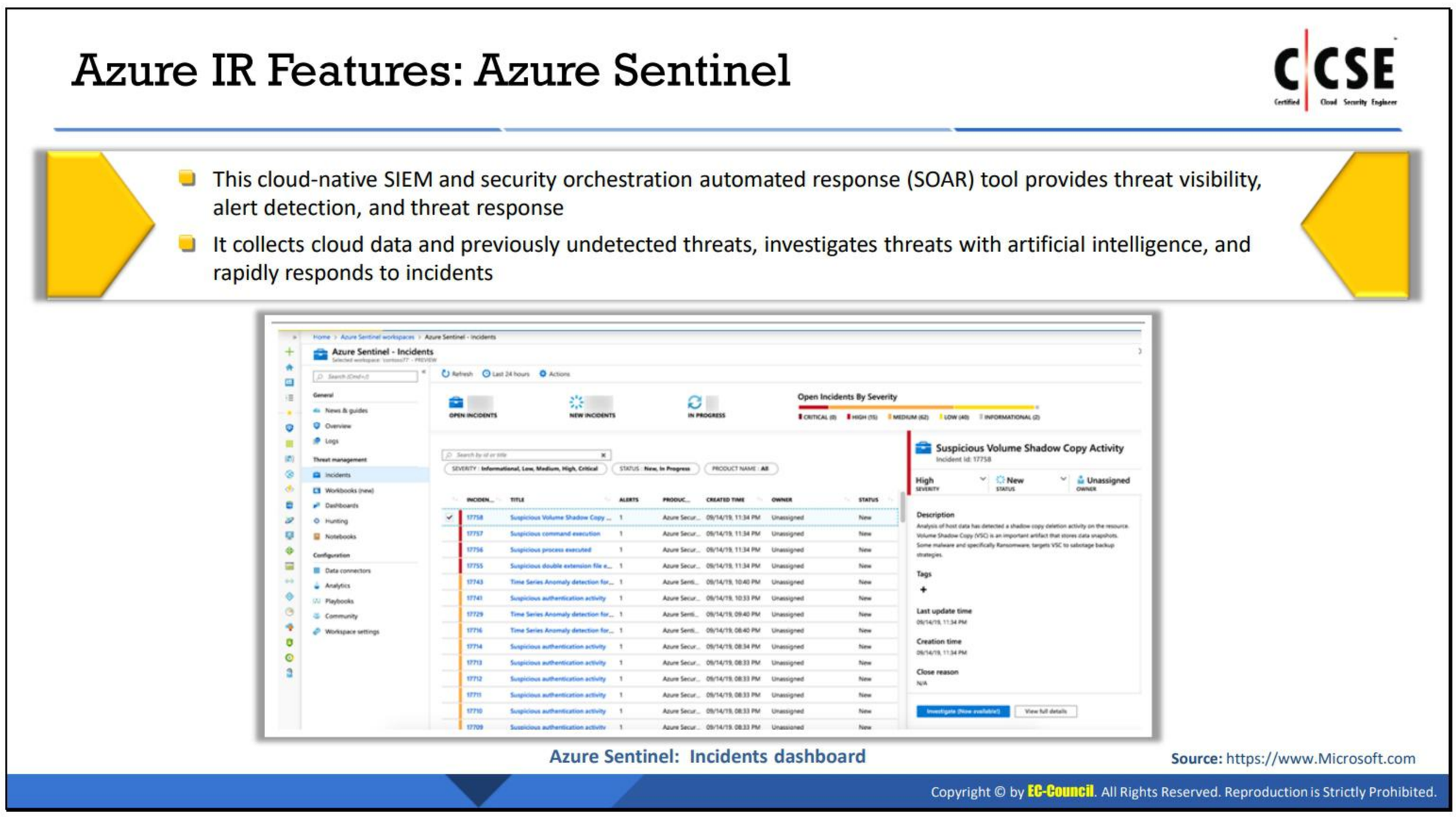
Figure 7.37: ASC Security Alerts Dashboard

ASC offers the following IR features:

- **Streamlined Threat Investigation**: ASC helps in detecting threats, streamlining threat investigation, and automating remediation with AI.
- **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.
- **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.
- **Security Policies and Recommendations**: ASC helps define an organization's security policies as per their requirements. It also recommends policies and actions to be necessarily implemented for preventing threats.
- **Workflow Automation**: This ASC feature automatically triggers incident responses via Logic Apps on security recommendations and alerts for securing Azure resources.

hide01.ir

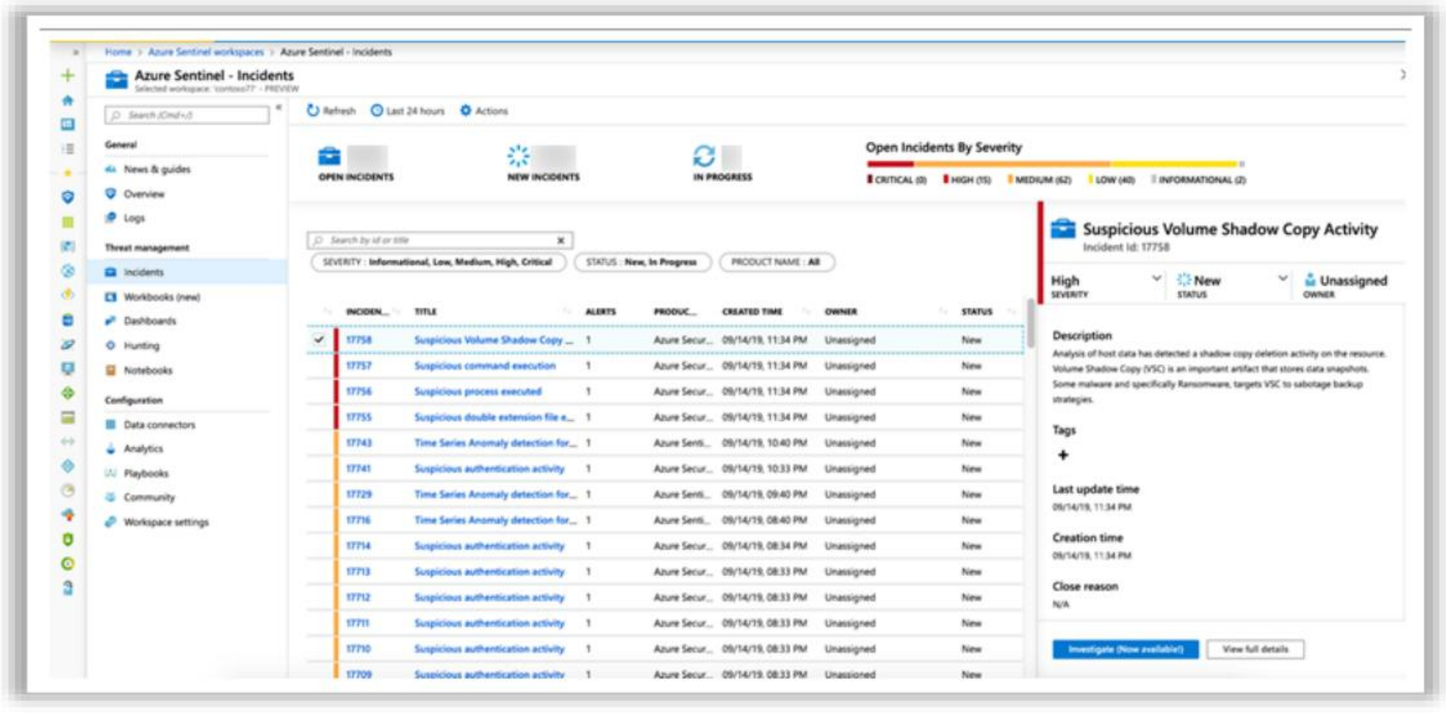
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Azure IR Features: Azure Sentinel

Azure Sentinel is a cloud-native SOAR and SIEM tool that provides threat visibility, alert detection, and threat response on Azure. Azure Sentinel helps with incident detection and investigation using artificial intelligence. It can use Microsoft's threat intelligence and any other third-party threat intelligence to detect and respond to threats. Its investigation tools help find the root cause of an incident.

Azure Sentinel uses analytics to identify incidents from multiple alerts, which reduces the number of alerts to be reviewed. Azure Sentinel provides rules using machine learning to map network behavior and check for suspicious activities in an organization's resources. It collects cloud data, detects previously undetected threats, investigates threats with artificial intelligence, and rapidly responds to incidents.



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

Figure 7.38: Azure Sentinel - Incidents Dashboard

Azure Sentinel offers the following IR features:

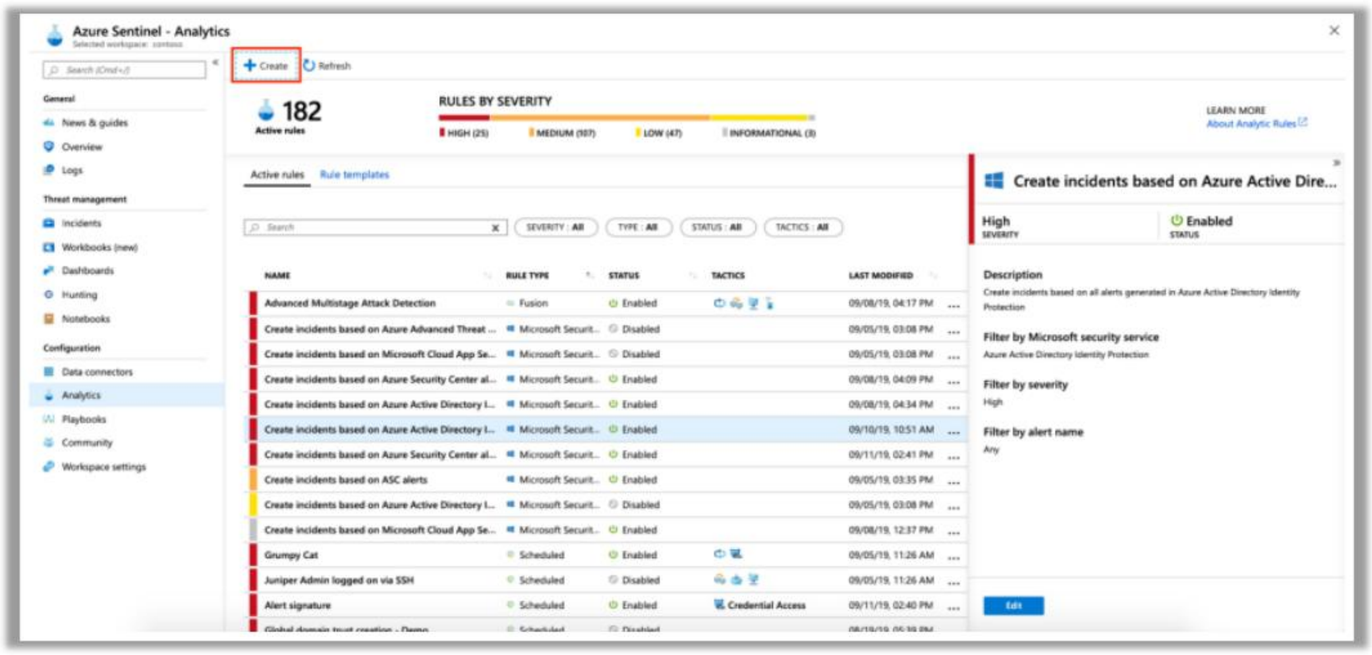
- **Cloud-scale Data Collection**: It collects cloud data of devices, users, infrastructure, and applications (both on cloud and on-premises).
- **Detect Undetected Threats**: It detects previously undetected threats and minimizes false positives with Microsoft's analytics and threat intelligence.
- **AI-aided Threat Investigation**: It helps investigate threats using artificial intelligence.
- **Rapid Incident Response**: It helps respond to incidents using its built-in orchestration and automation.

hide01.ir

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

Investigate Incidents with Azure Sentinel

- Use Azure Sentinel to create advanced alert rules and generate incidents to be investigated



Azure Sentinel: Analytics

Source: https://www.Microsoft.com

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

Investigate Incidents with Azure Sentinel

Use Azure Sentinel to investigate incidents on Azure. Azure Sentinel allows cloud admins to create advanced alert rules to generate incidents that can be assigned and investigated later.

Steps to Investigate Incidents Using Azure Sentinel

- On Azure Sentinel homepage, choose **Incidents**. This page shows incidents that are open, closed, and in progress, as well as the time of their occurrence, their status, and severity.

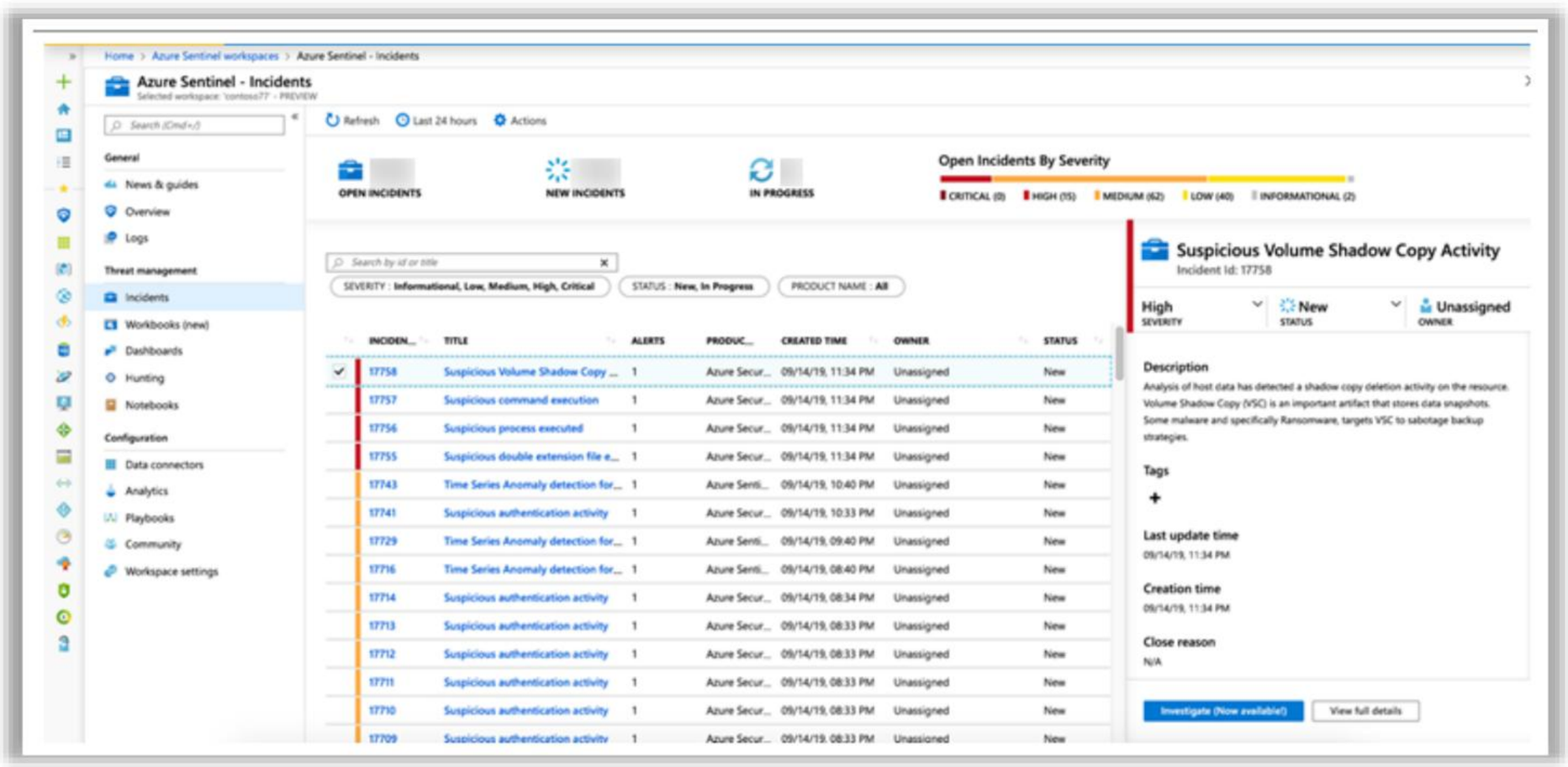


Figure 7.39: Azure Sentinel - Incidents

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

- Filter incidents as per requirements (e.g., status or severity).
- Choose a specific incident to start an investigation. The incident window will show detailed incident information such as incident ID, its severity, events that triggered this incident, and so on.
- Choose **View full details** on the incident page and check the summary of the incident information for more details on the associated entities and alerts. Go to the **Alert** tab to review the alerts. Choose the number of **Events** to further investigate the incident.

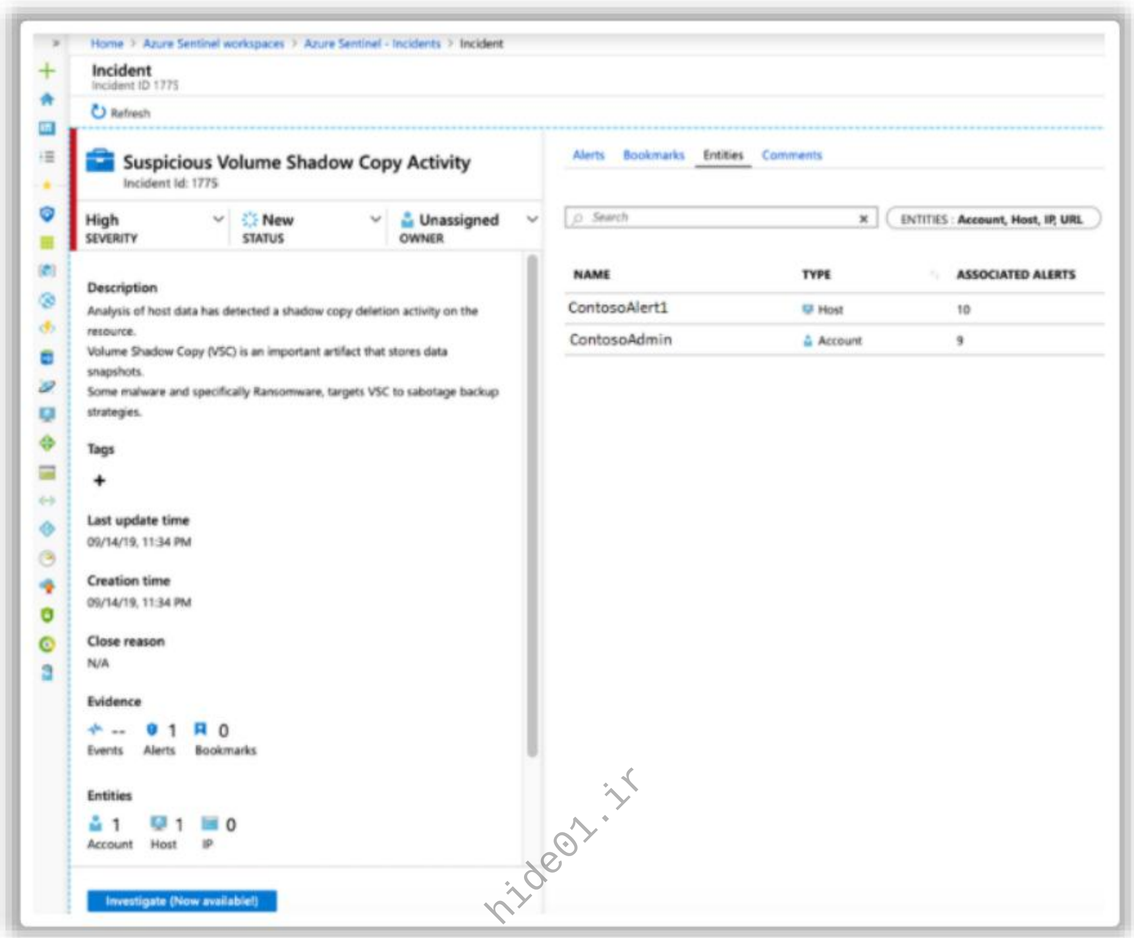


Figure 7.40: Incident Summary

- Keep the status as **In progress** while actively investigating an incident.
- Assign incidents to analysts using the **Incident Owner** field. Initially, incidents are unassigned and can be assigned to a specific user.



Figure 7.41: Assigning Incidents to Analysts

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

- Choose **Investigate** to see the investigation map.
- The investigation graph appears after selecting an incident and clicking on **Investigate**.



Figure 7.42: Investigation Graph

- Open the **Entities** pane by choosing an entity and review information on that entity.

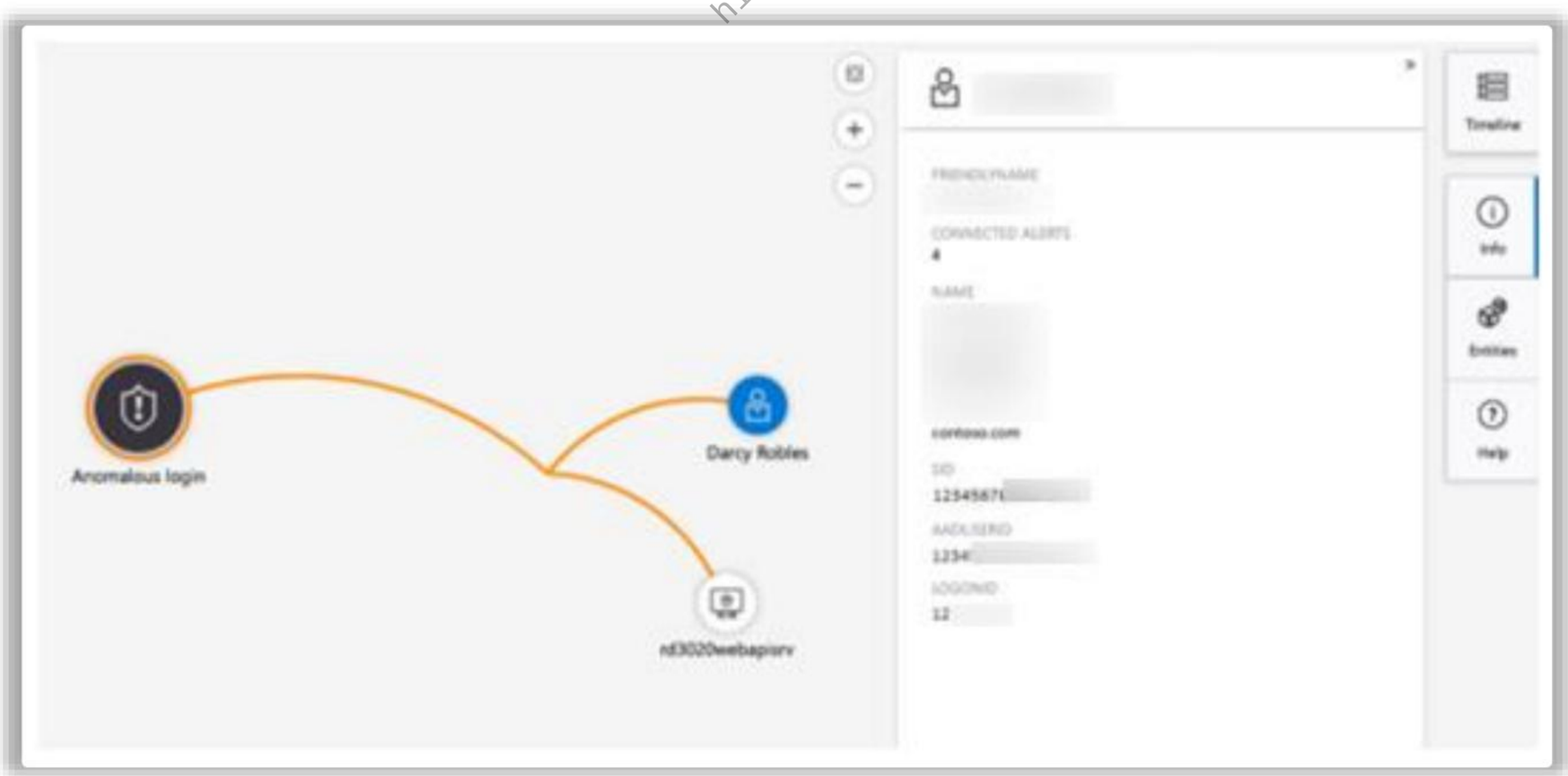


Figure 7.43: Information of an Entity

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

- Hover over each entity to see a list of questions (known as exploration queries) designed by Microsoft's experts and analysts for each entity type to deepen the investigation.



Figure 7.44: List of Questions

- Choose **Related alerts** to get alerts into a graph (as shown below).

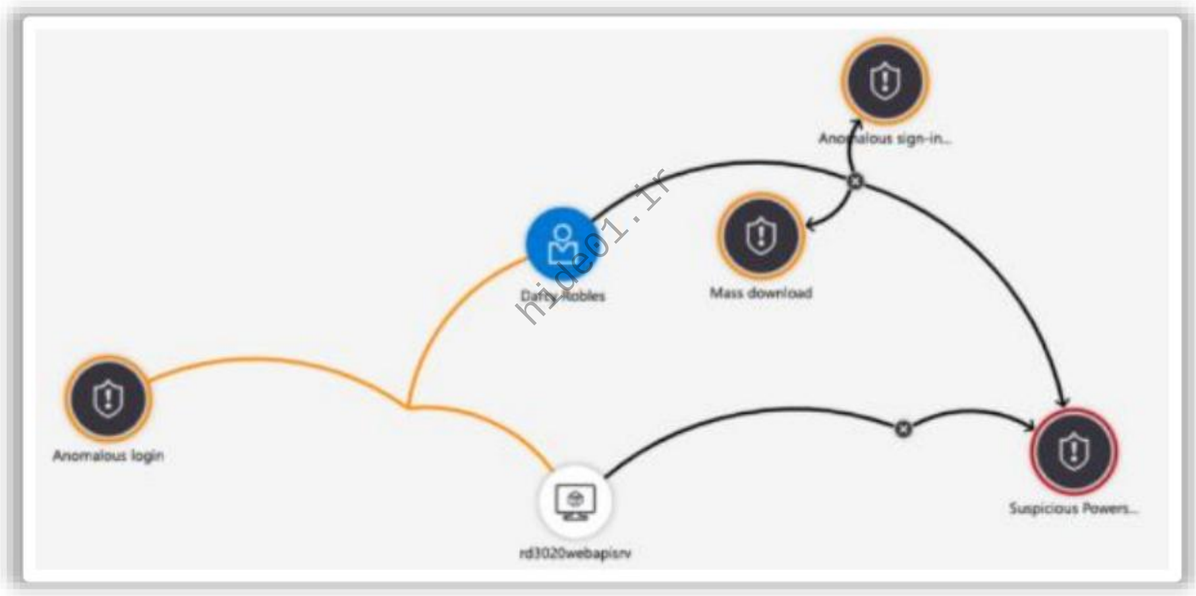


Figure 7.45: Related Alerts

- Choose **Events>** for each exploration query to open the raw event results and the query utilized in Log Analytics. A parallel timeline is provided by the graph to help understand the incident.

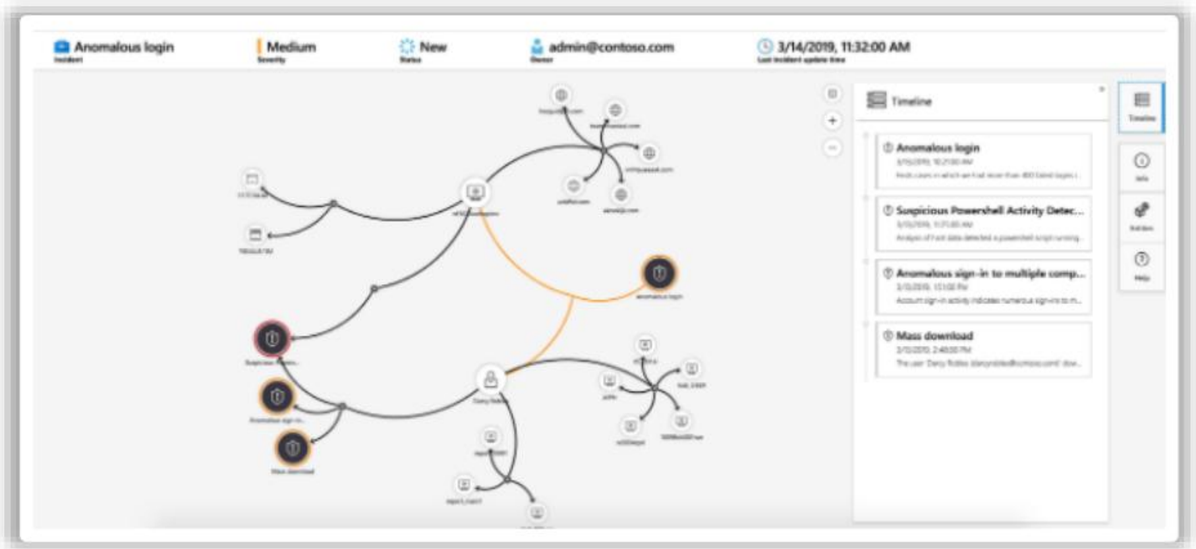


Figure 7.46: Events

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

- Hover over the timeline to check time of occurrence of the events on the graph.
- Set the status of the incident as **Closed** after resolving it. When closing the incident, choose **Select classification** to specify the reason for the incident closure. Following reasons can be chosen when closing an incident:
    - True positive: suspicious activity
    - Benign positive: suspicious but expected activity
    - False positive: incorrect alert logic
    - False positive: incorrect data
    - Undetermined

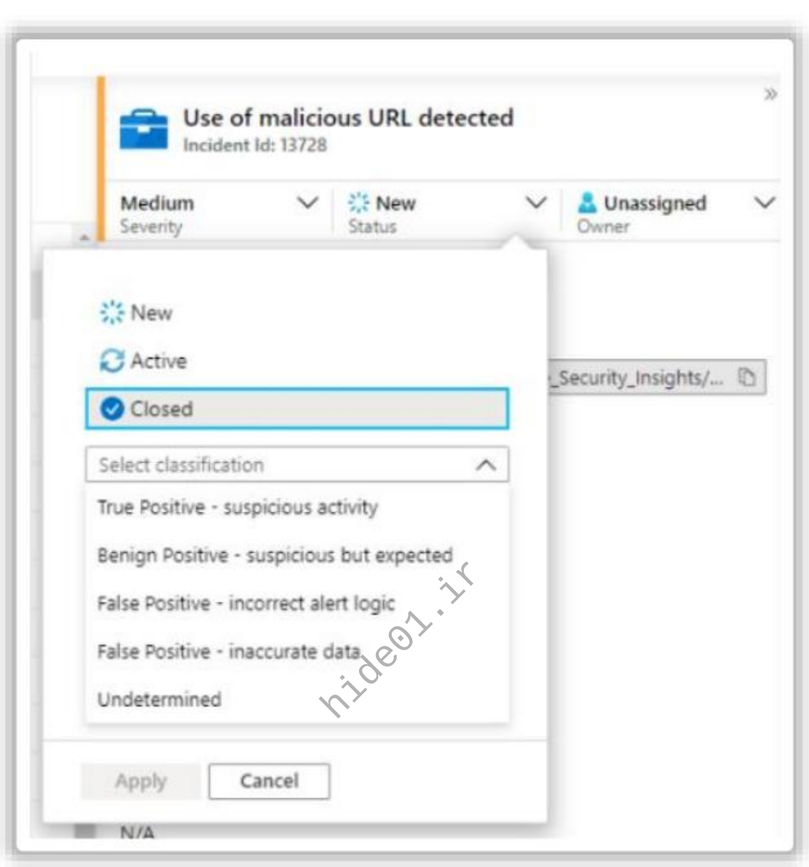


Figure 7.47: Setting the Status of the Incident as Closed

- Add a comment after choosing an incident classification and then click on **Apply** to close the incident.

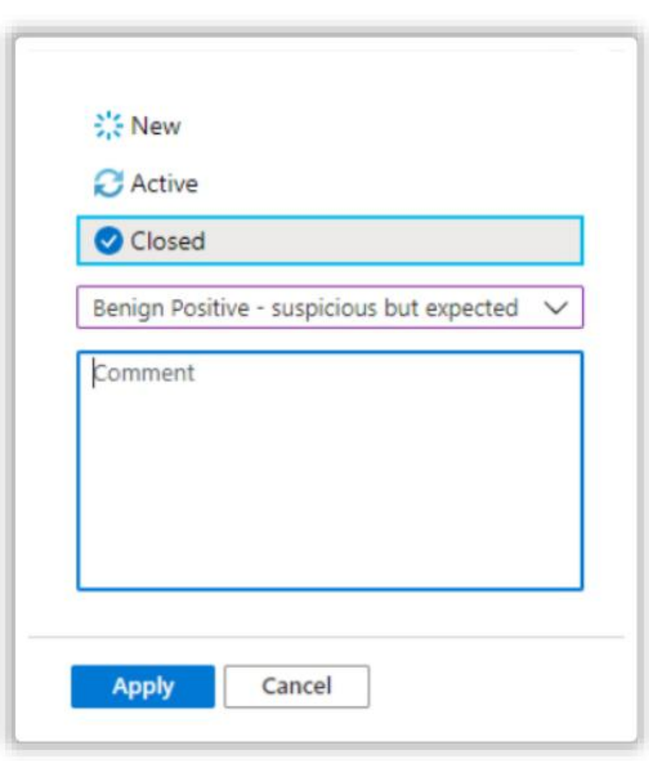
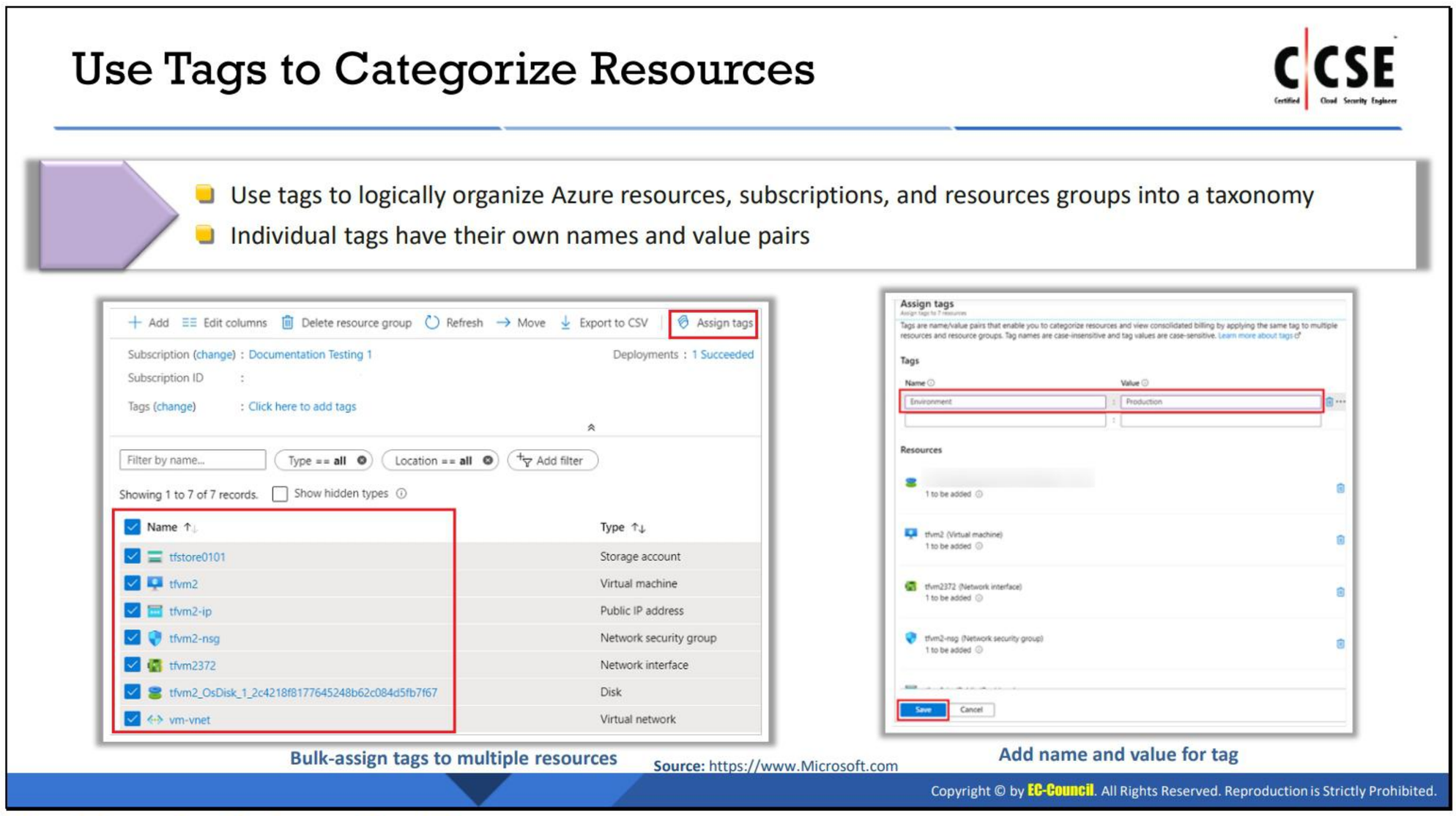


Figure 7.48: Adding a Comment

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



Use Tags to Categorize Resources

Use tags to logically organize Azure resources, resource groups, and subscriptions into a taxonomy. Tags consist of a pair of a name and a value. Follow the steps given below for using tags to categorize resources:

- Check for existing tags in the overview to see tags for a resource or a resource group. The list will be empty if tags have not been previously applied.

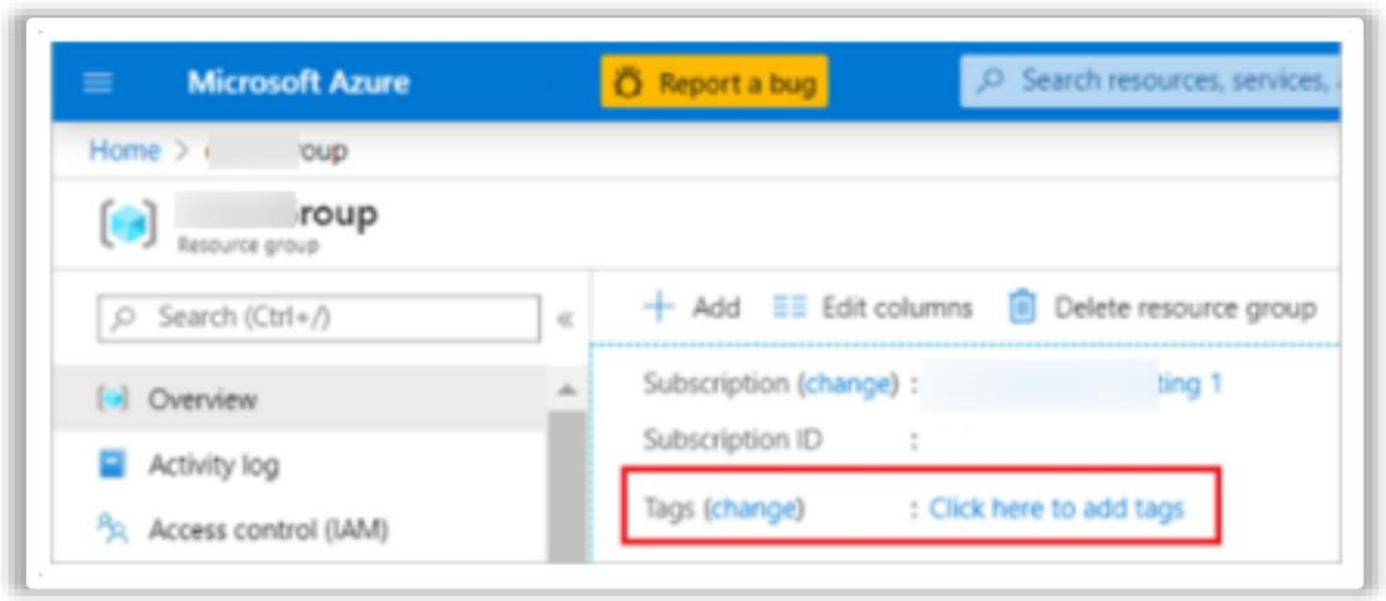


Figure 7.49: Tags

- Choose **Click here to add tags** to add a tag.

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

- Provide a name and value for the tag.

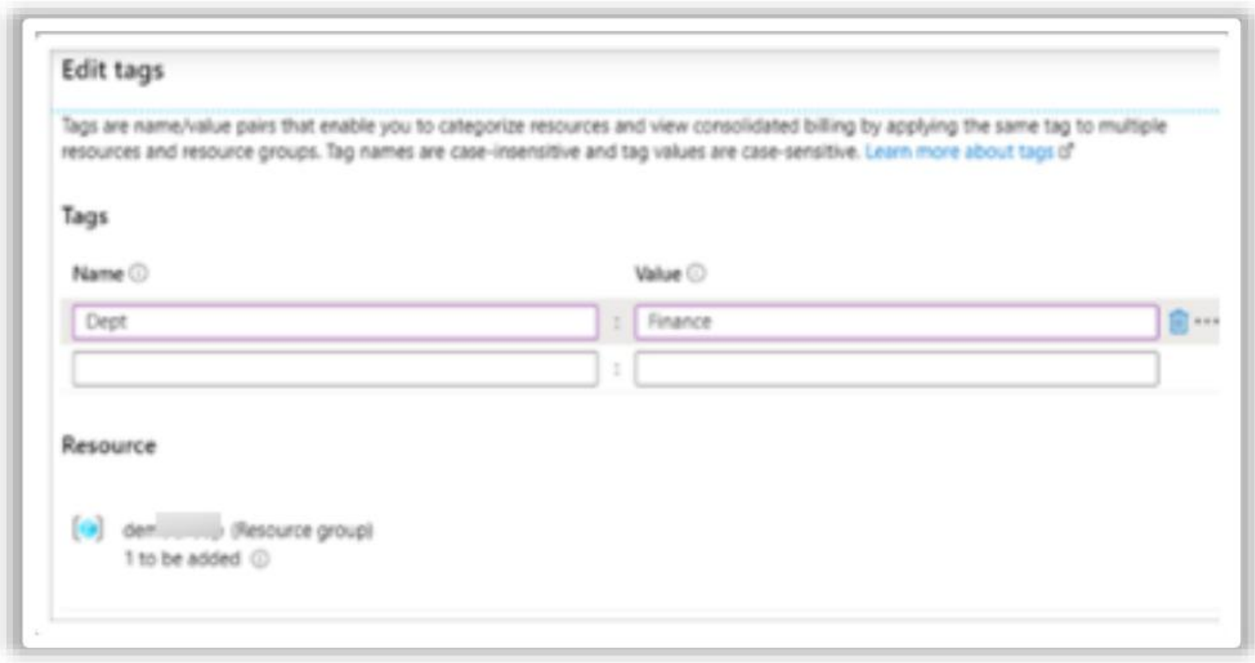


Figure 7.50: Editing a Tag

- Keep adding tags as required and click **Save** when done.

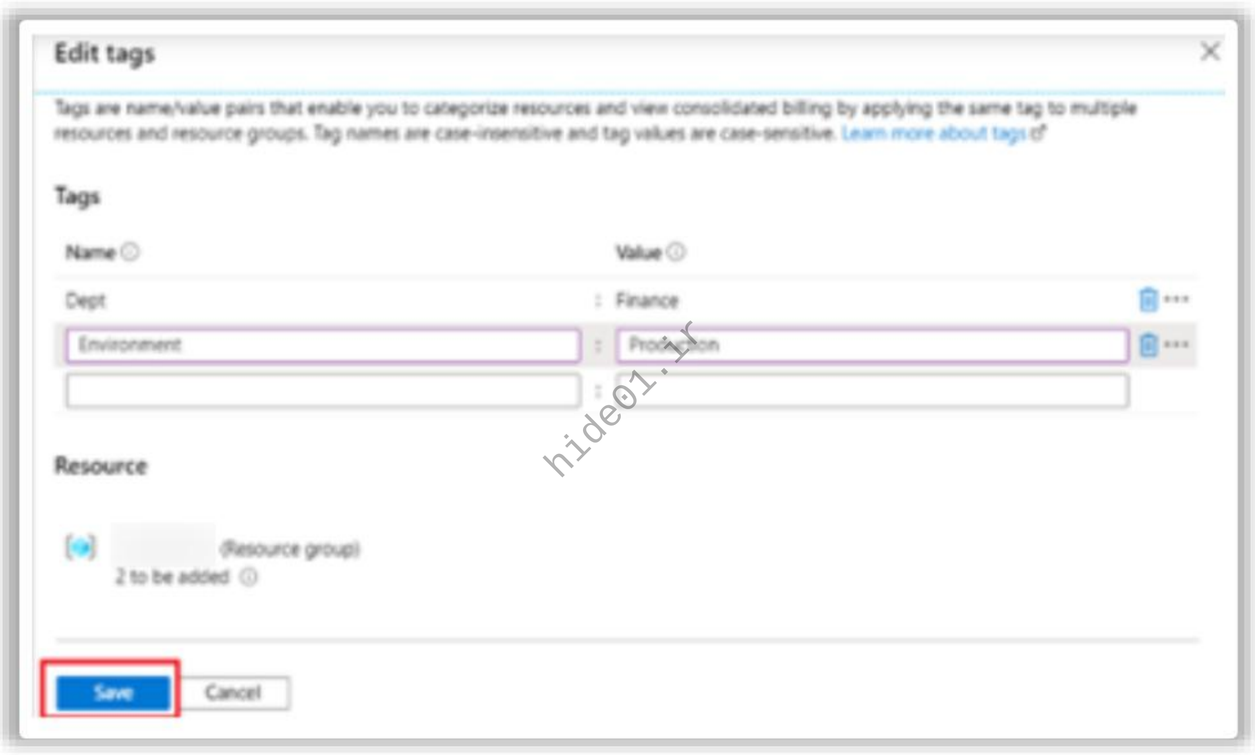


Figure 7.51: Adding Tags

- The overview now displays tags.

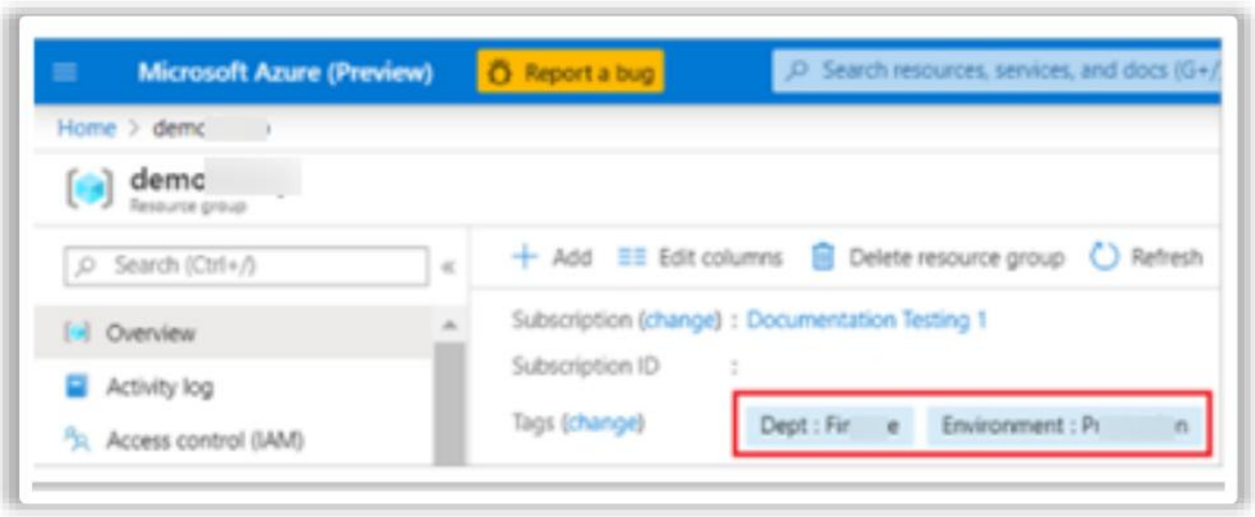


Figure 7.52: Created Tags

- Choose **Change** to add or delete a tag.

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

- Delete a tag by selecting the **trash** icon and choose **Save**.

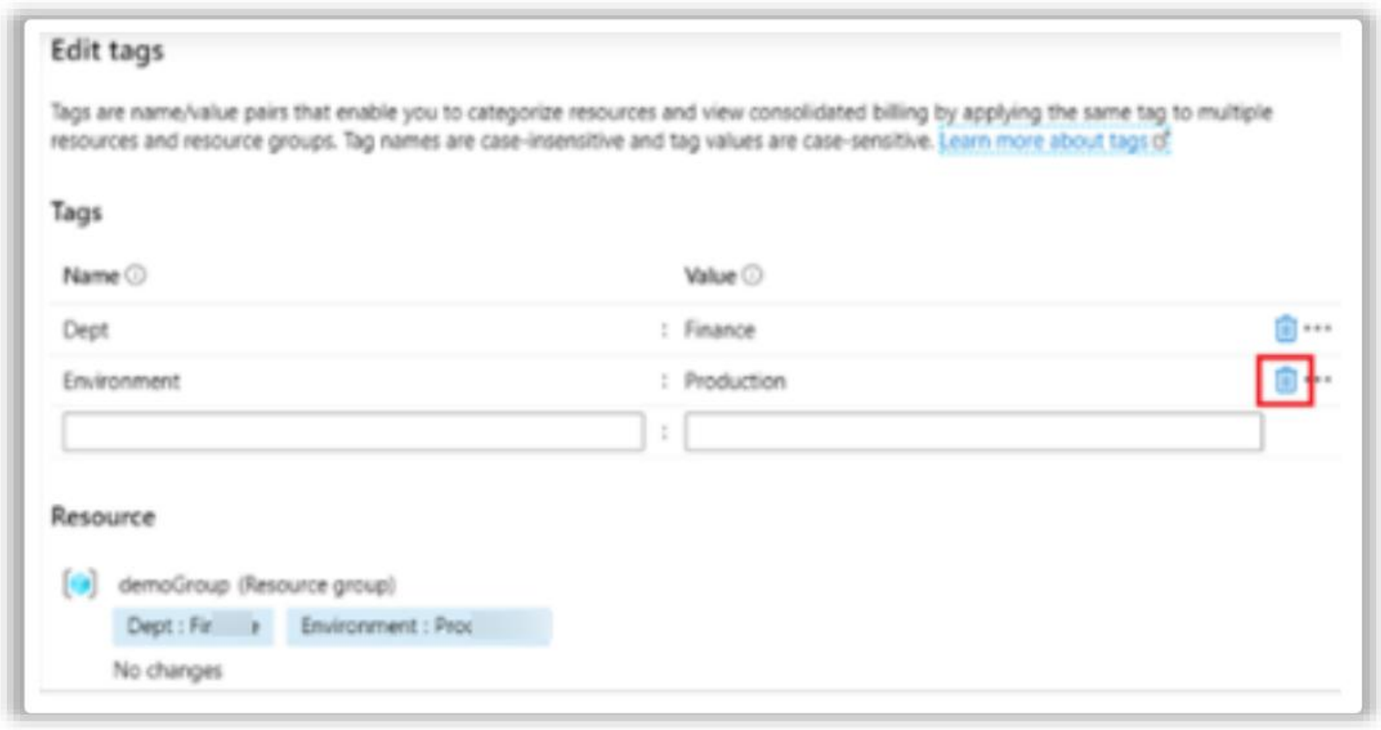


Figure 7.53: Deleting a Tag

- **Assign Tags to Multiple Resources**
  - Choose the checkbox for the resources that should be assigned a tag from a list of resources. Choose **Assign tags**.

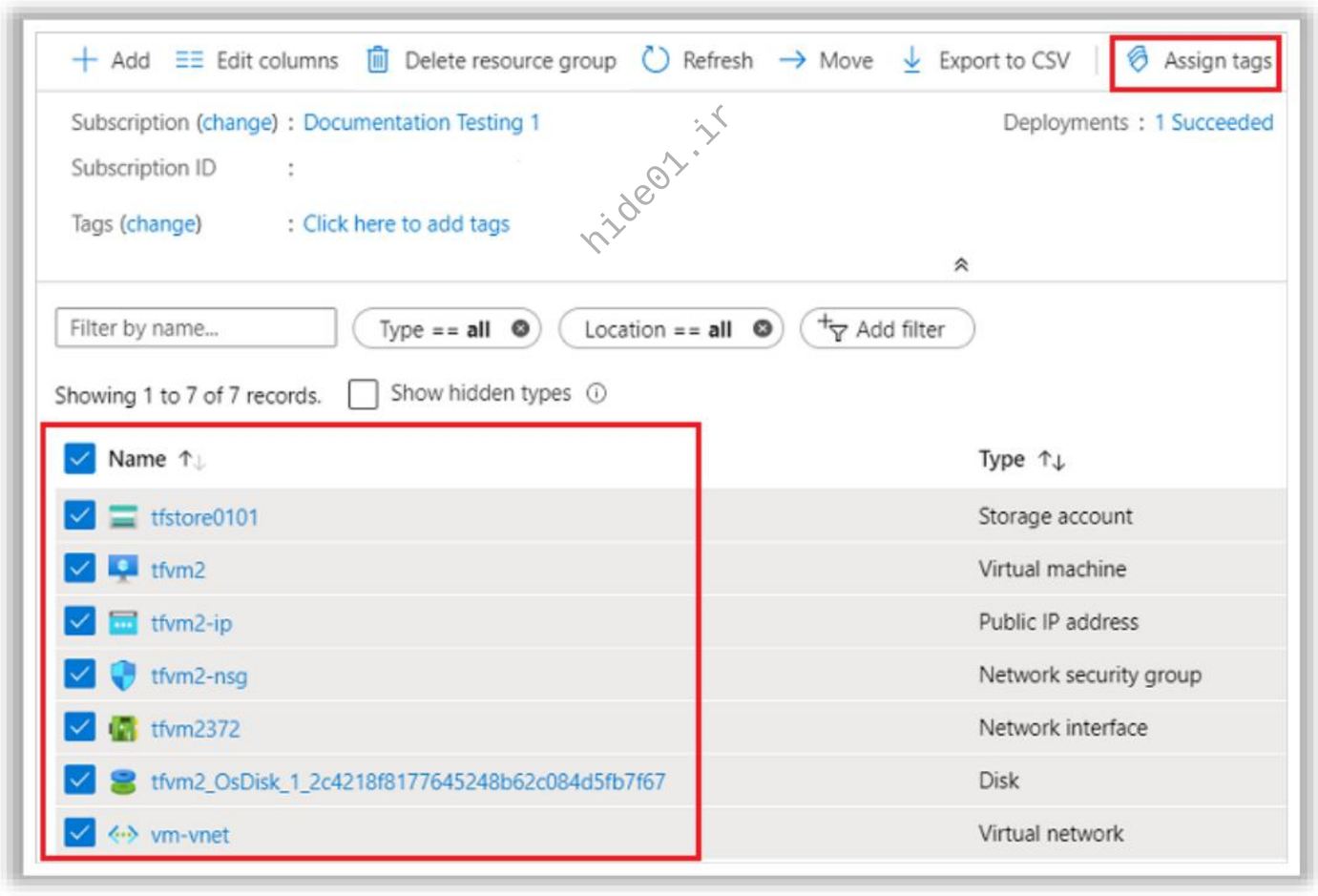


Figure 7.54: Assigning Tags to Multiple Resources

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

- Provide names and values, and then choose **Save**.

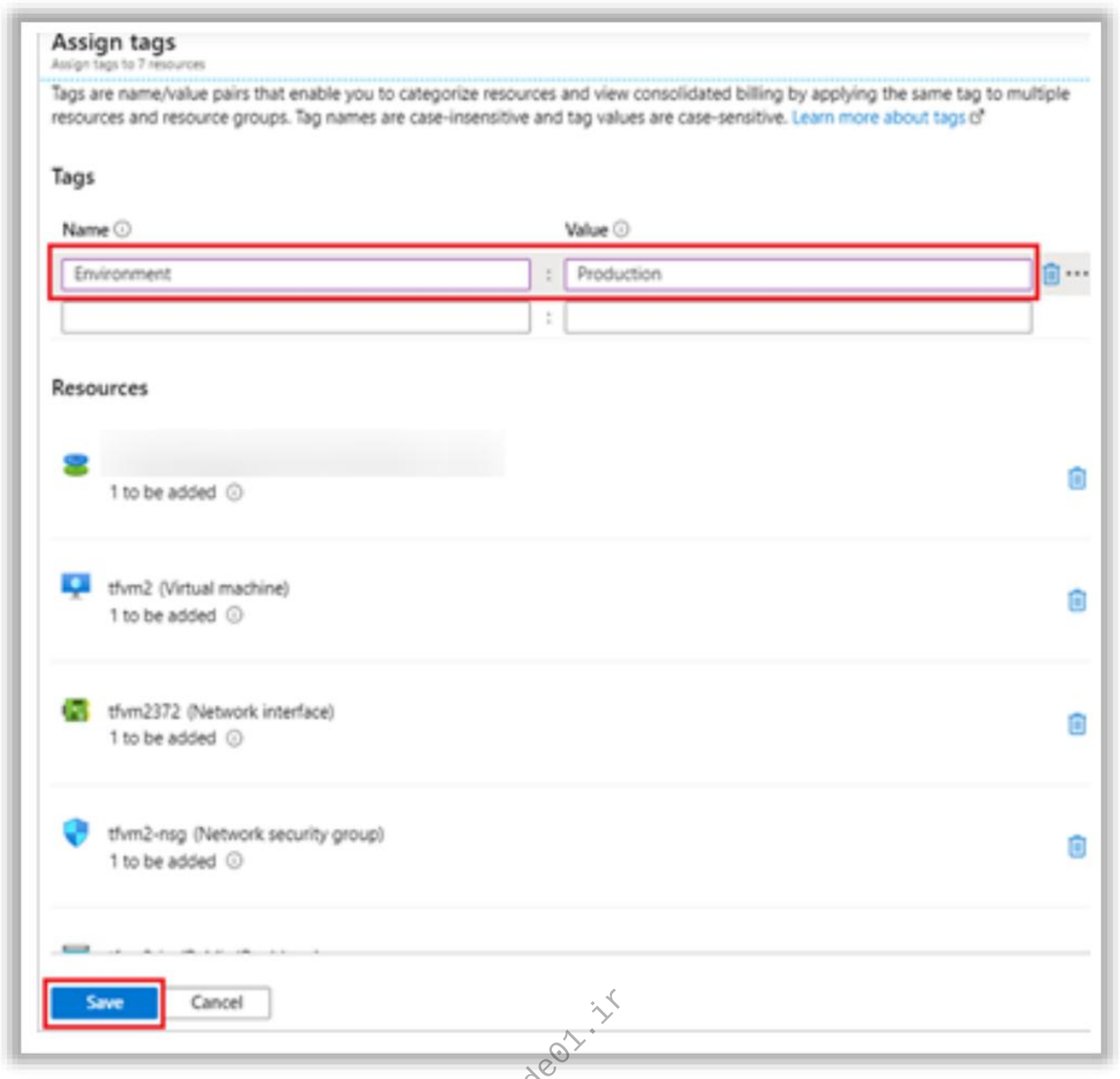


Figure 7.55: Adding Name and Value to a Tag

- **View Resources with Tags**
  - Search for **tags** on the Azure portal and select it.

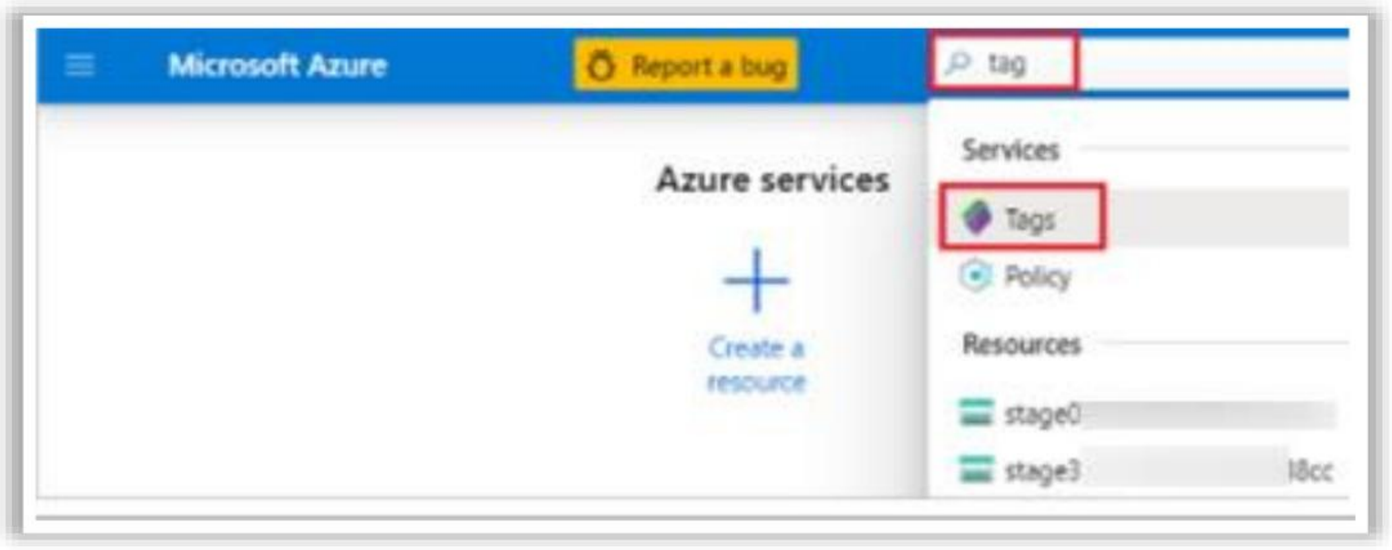


Figure 7.56: Searching for Tags

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

- Choose the tag to view resources.

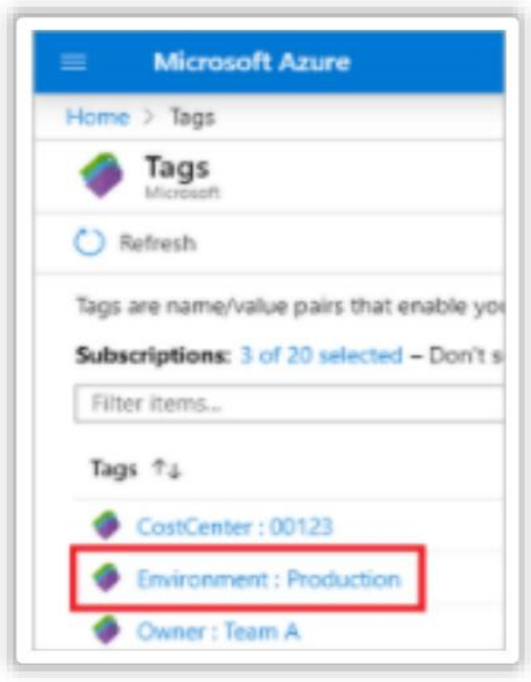


Figure 7.57: Resources of a Tag

- All resources with the relevant tag are displayed.

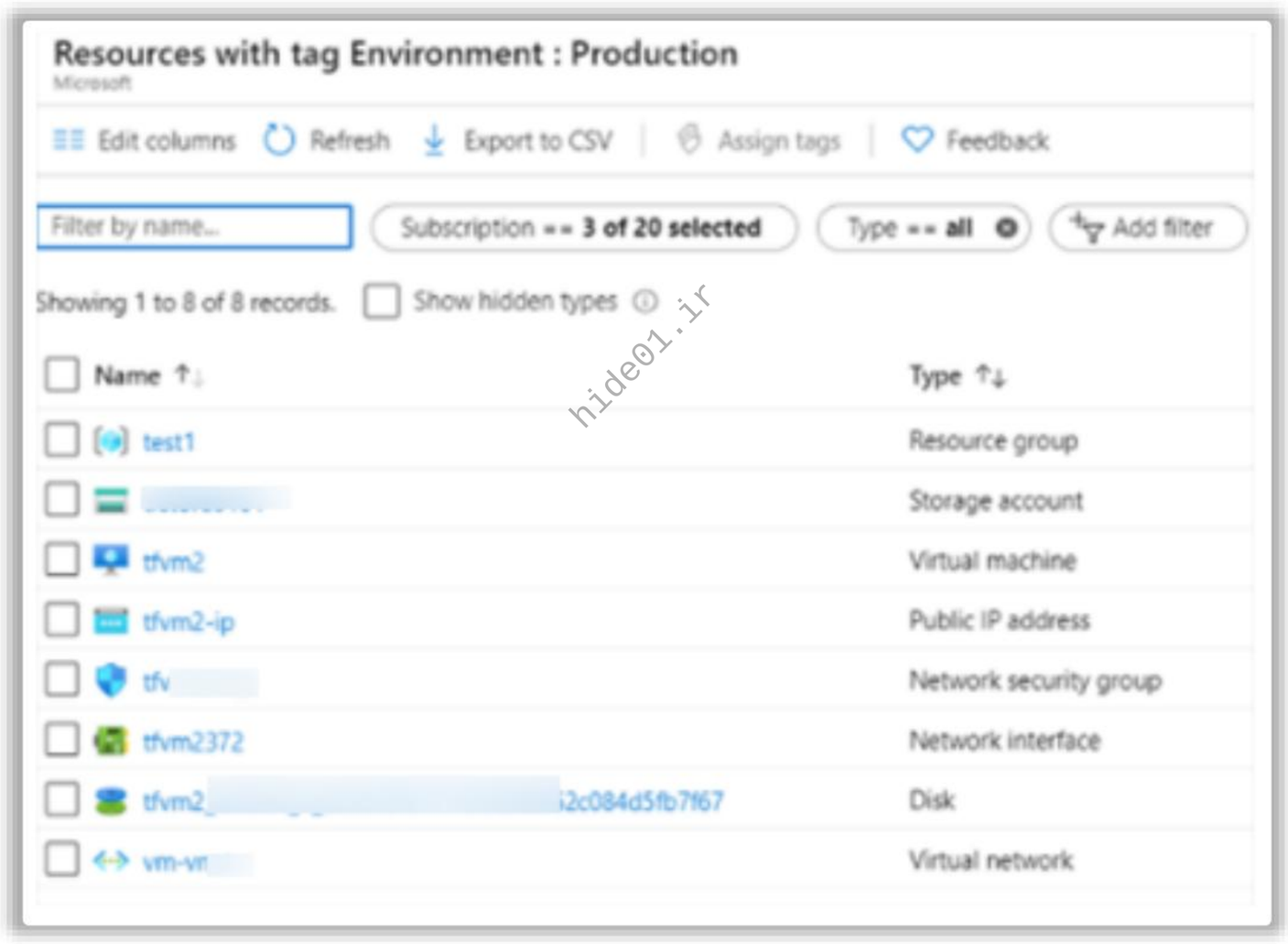
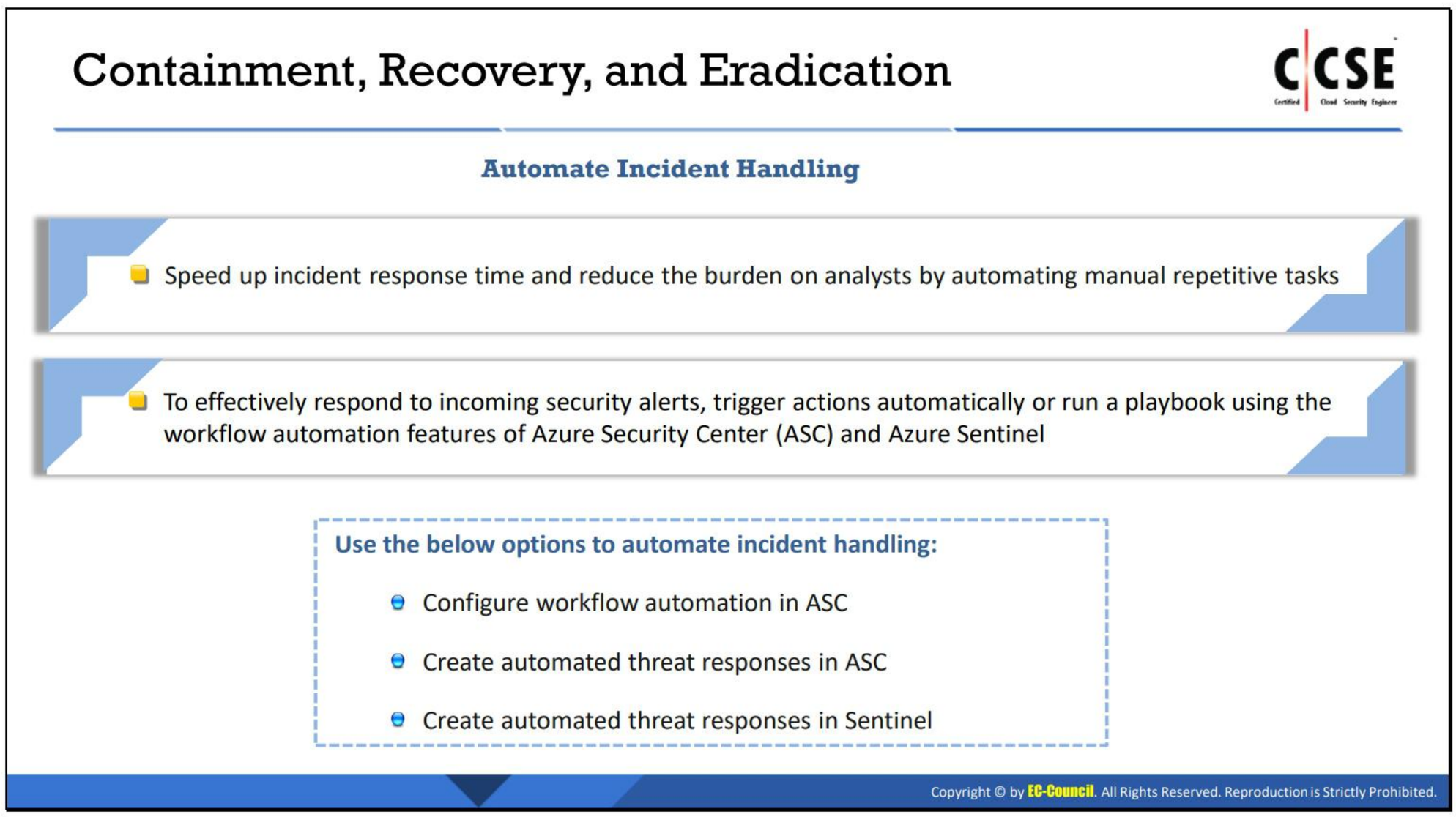


Figure 7.58: Resources with Relevant Tag

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



Containment, Recovery, and Eradication

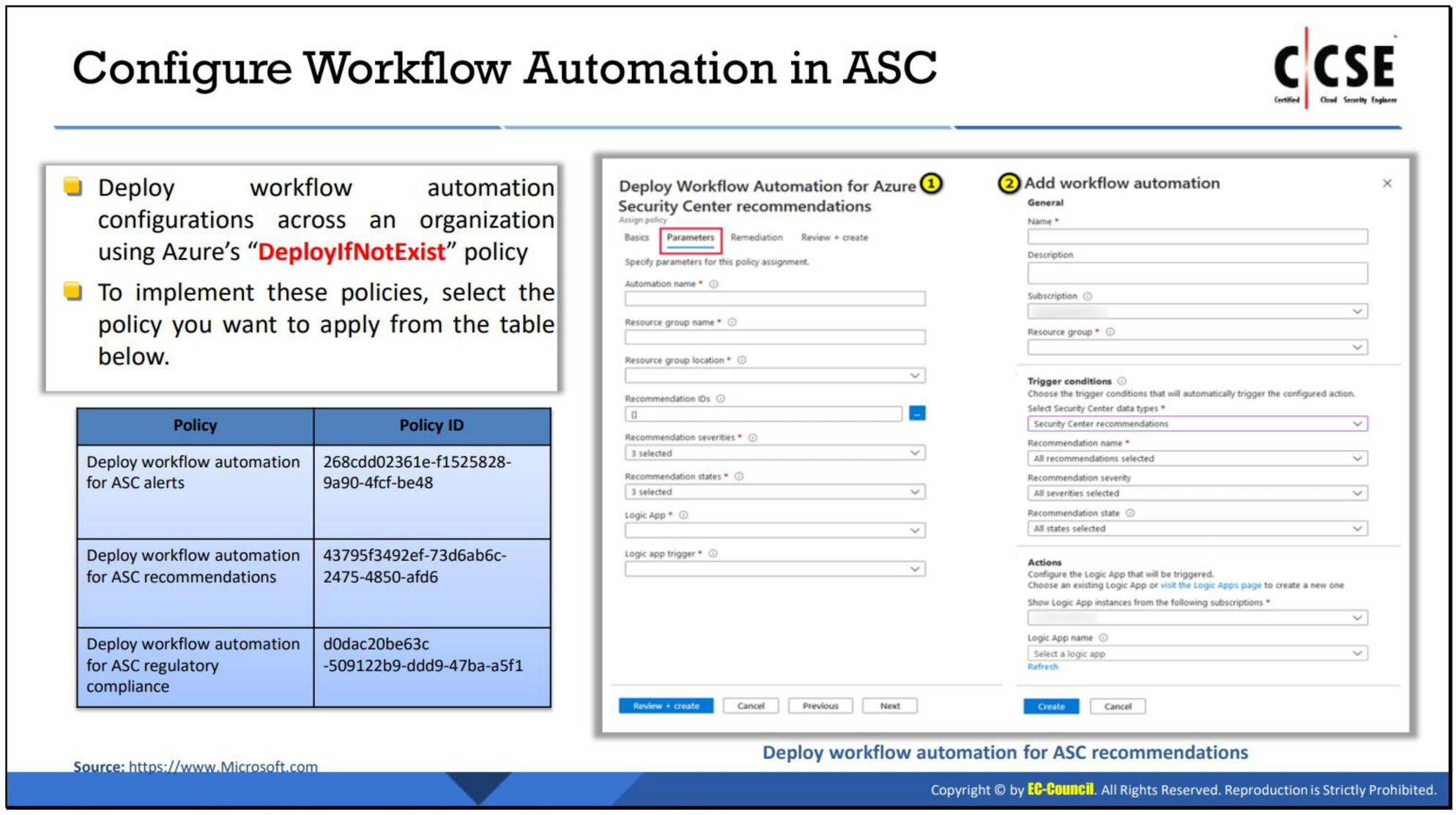
Speed up the incident response time and reduce the burden on analysts by automating repetitive manual tasks. The process of handling incidents manually may result in analyst fatigue, which, in turn, will increase the chances of human errors and lead to delays. Moreover, the chances of losing focus on complex tasks will increase, which may degrade the ability of analysts to respond to incidents.

Trigger actions automatically or run a playbook to respond to the incoming security alerts using the workflow automation features of ASC and Azure Sentinel. Playbooks can effectively take actions such as isolating problematic accounts, sending notifications, and disabling accounts.

Use the following options to automate the incident handling process:

- Configure workflow automation in ASC
- Set up automated threat responses in ASC
- Set up automated threat responses in Sentinel

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



Configure Workflow Automation in ASC

Automating the organization's monitoring and IR processes will help reduce the time taken to respond to and mitigate security incidents. Deploy workflow automation configurations across the organization using Azure's "DeployIfNotExist" policy.

Steps to Configure Workflow Automation in ASC

- To implement these policies, select the policy you want to apply from the following table.

Policy	Policy ID
Deploy workflow automation for ASC alerts	f1525828-9a90-4fcf-be48-268cdd02361e
Deploy workflow automation for ASC recommendations	73d6ab6c-2475-4850-afd6-43795f3492ef
Deploy workflow automation for ASC regulatory compliance	509122b9-ddd9-47ba-a5f1-d0dac20be63c

Table 7.2: Policy with Policy ID

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

- Alternatively, you can search for and open **Azure Policy**. Then, choose **Definitions** and search for policies by their name from the Azure Policy menu.

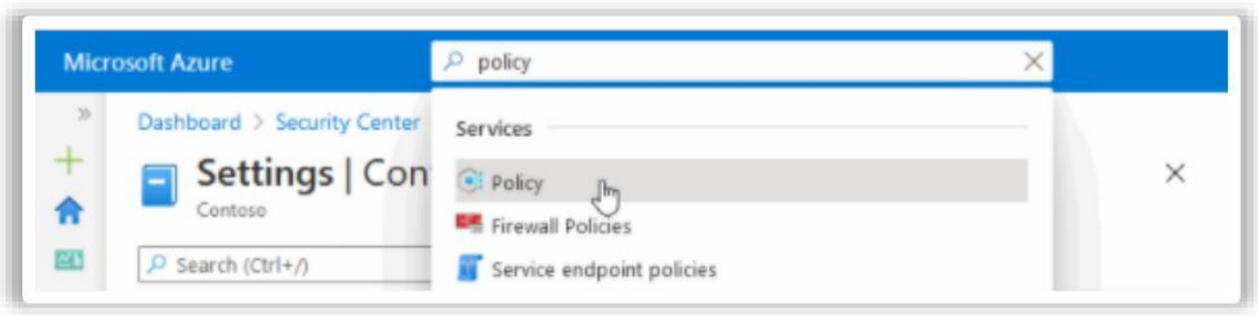


Figure 7.59: Looking for Azure Policy

- Choose **Assign** from the relevant **Azure Policy** page.

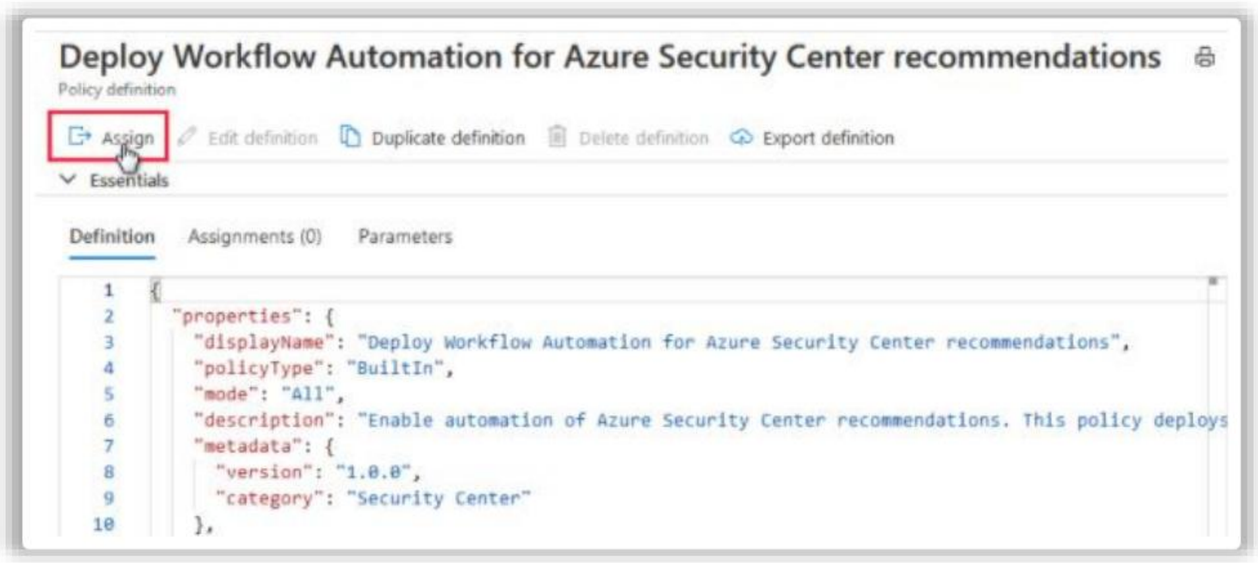


Figure 7.60: Assigning an Azure Policy

- Set the parameters as intended after opening each tab.
  - On the **Basics** tab, set the policy scope. Assign the policy to the management group with subscriptions that will leverage the workflow automation configuration.
  - On the **Parameters** tab, set the details of the resource group and data type.

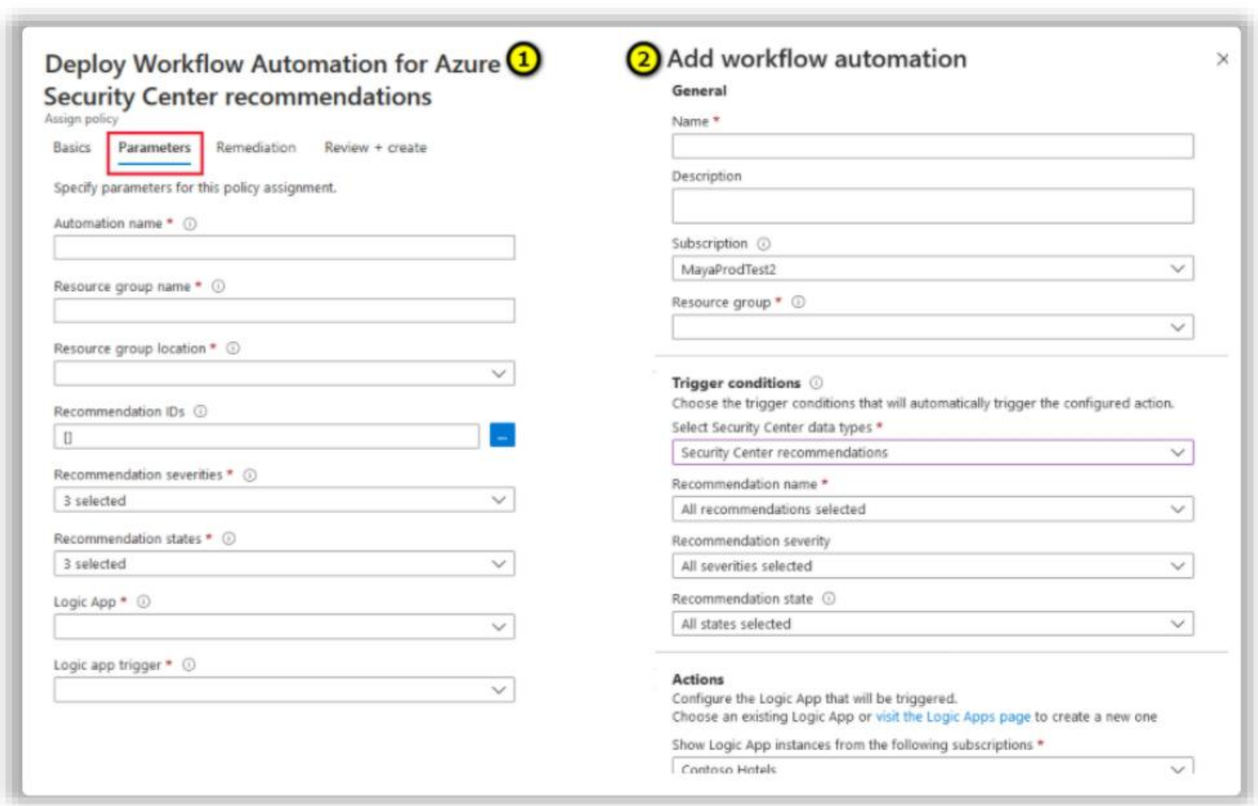


Figure 7.61: Entering Resource Group and Data Type

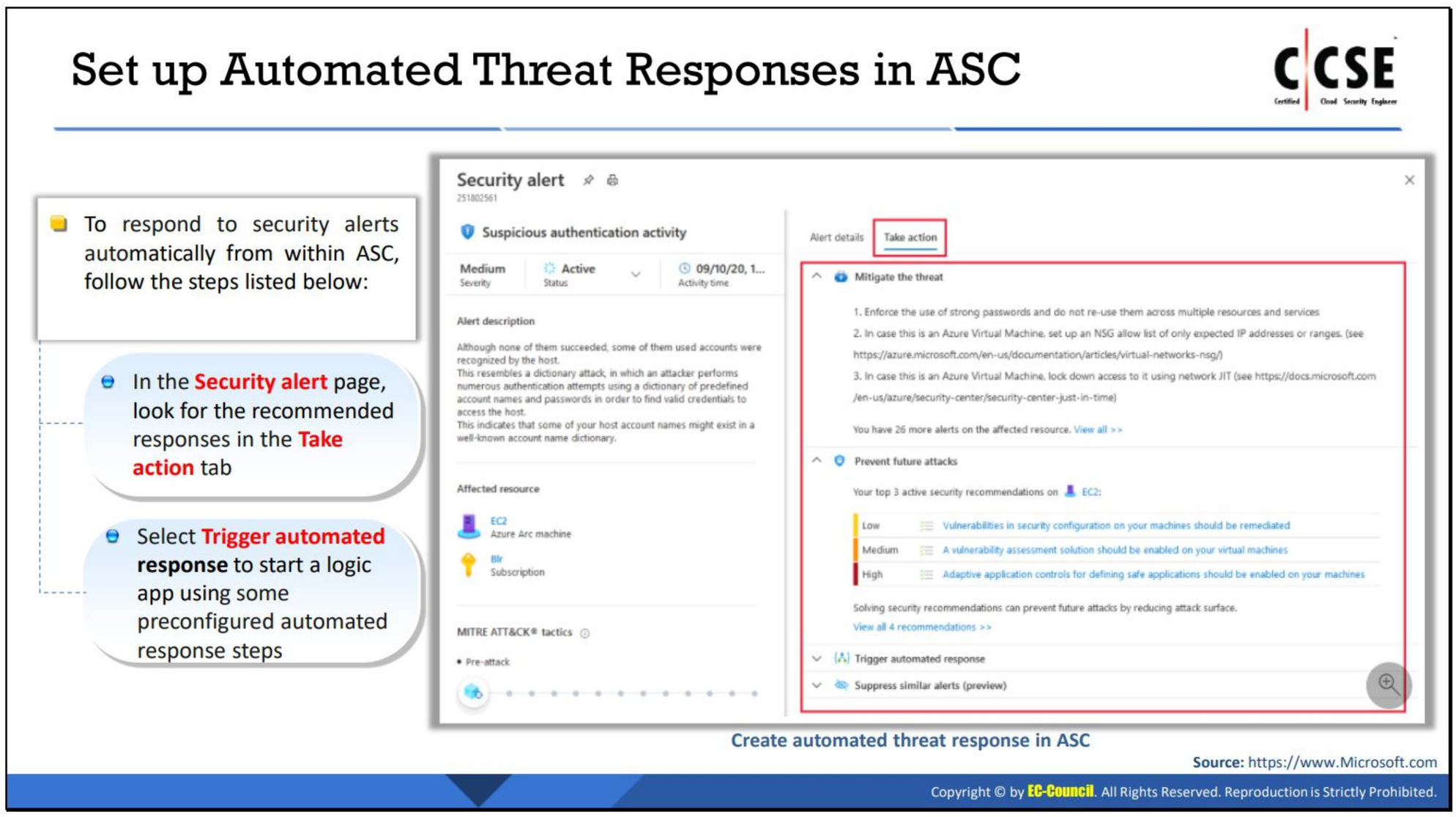
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- For applying this assignment to current subscriptions, go to the **Remediation** tab and create a remediation task (optional).

- Now, review the summary page and click on **Create**.

hide01.ir

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



Create automated threat response in ASC

Source: https://www.Microsoft.com

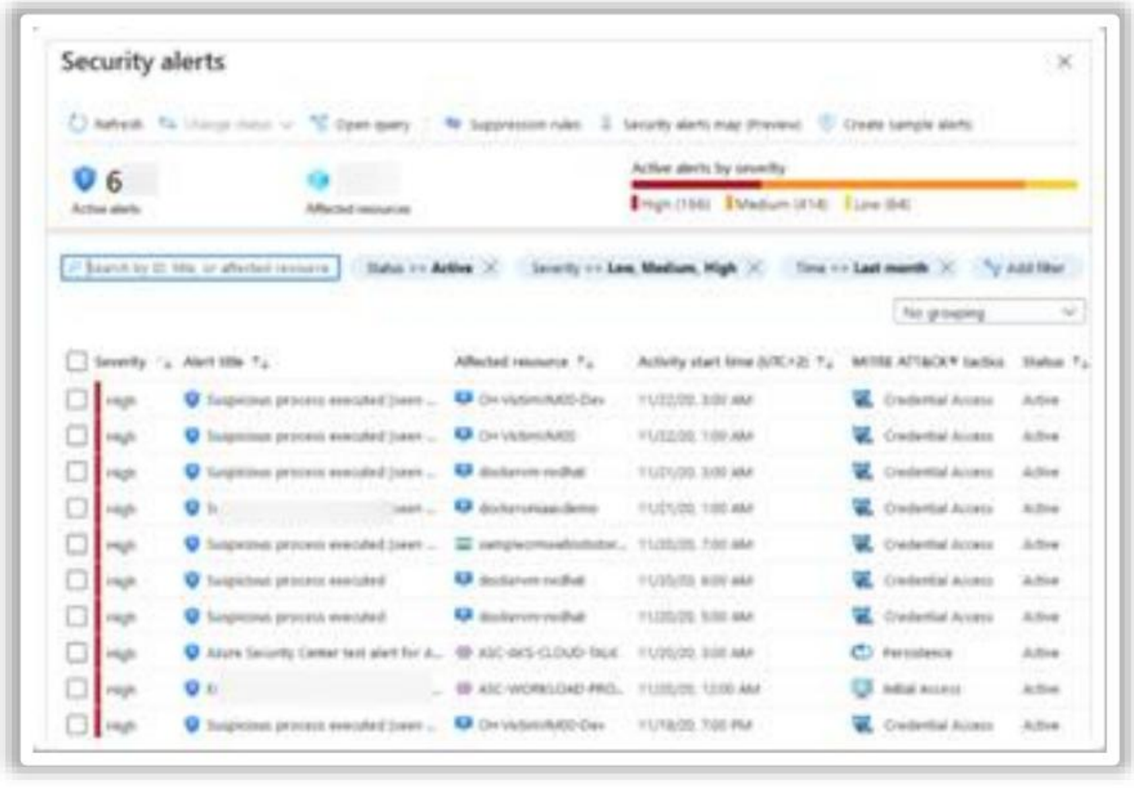
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Set Up Automated Threat Response in ASC

Azure Security Center (ASC) uses threat intelligence and advanced analytics to analyze hybrid-cloud workloads to alert or notify you about potential malicious activities within your cloud resources. Integrate security alerts from other security services and products into ASC. Quickly investigate and remediate a potential issue after an alert is raised.

Steps to Use ASC for Automated Threat Response

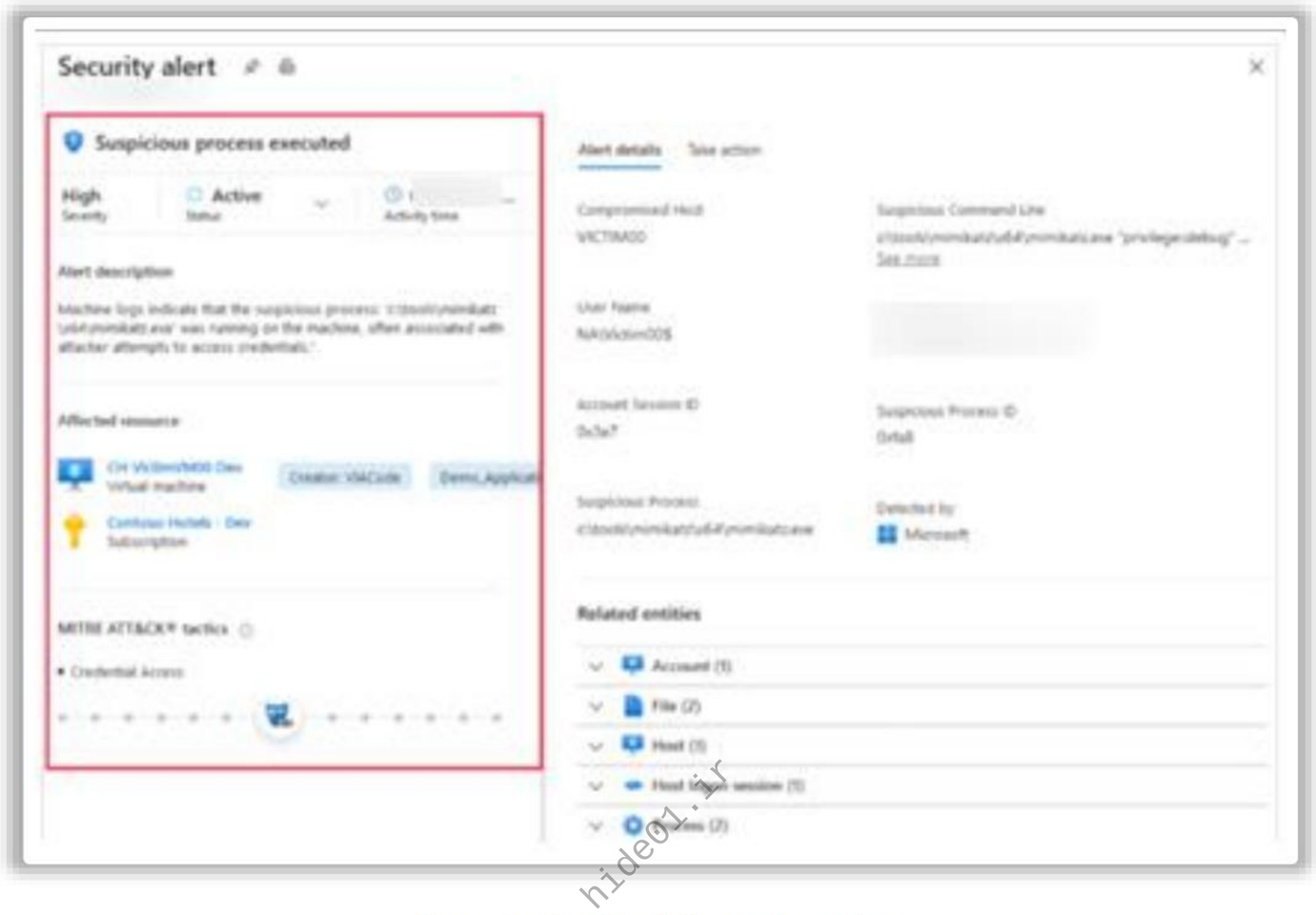
- **Check for Alerts**
  - Triage security alerts from the **Security alerts** page. Alerts are ranked based on the detected activity's severity.



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

Figure 7.62: Security Alerts

- **Investigate a Security Alert**
  - Choose the alert that needs to be investigated.
  - Choose the resource from the **Alert overview** page.
  - Start the investigation from the left pane that shows critical alert information (e.g., affected resources, description, alert severity).

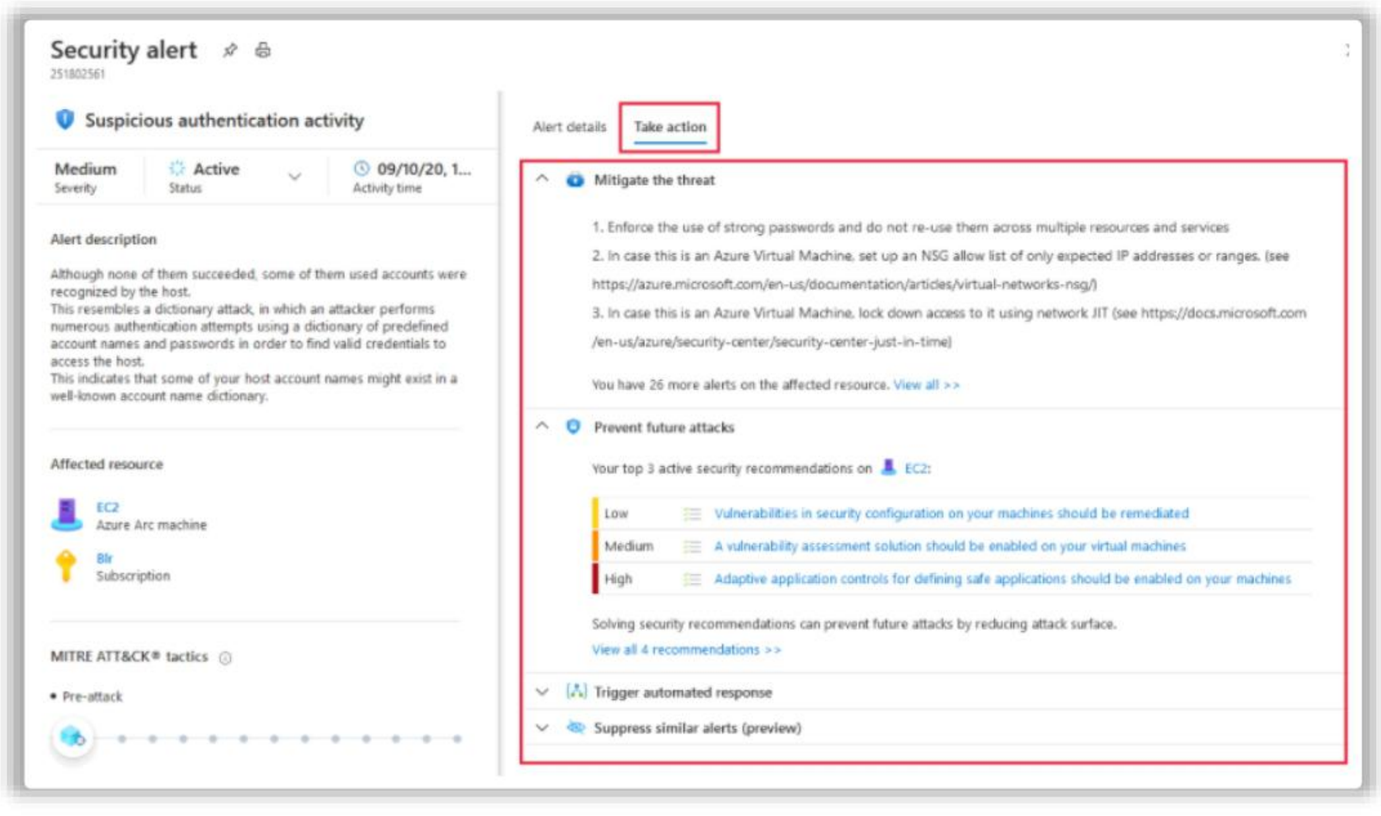


hide01.ir

Figure 7.63: Critical Alert Information

  - Check the **Alert details** tab for more information to help investigate the suspicious activity.

- **Respond to an Alert**
  - To view the recommended responses, open the **Take action** tab.



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

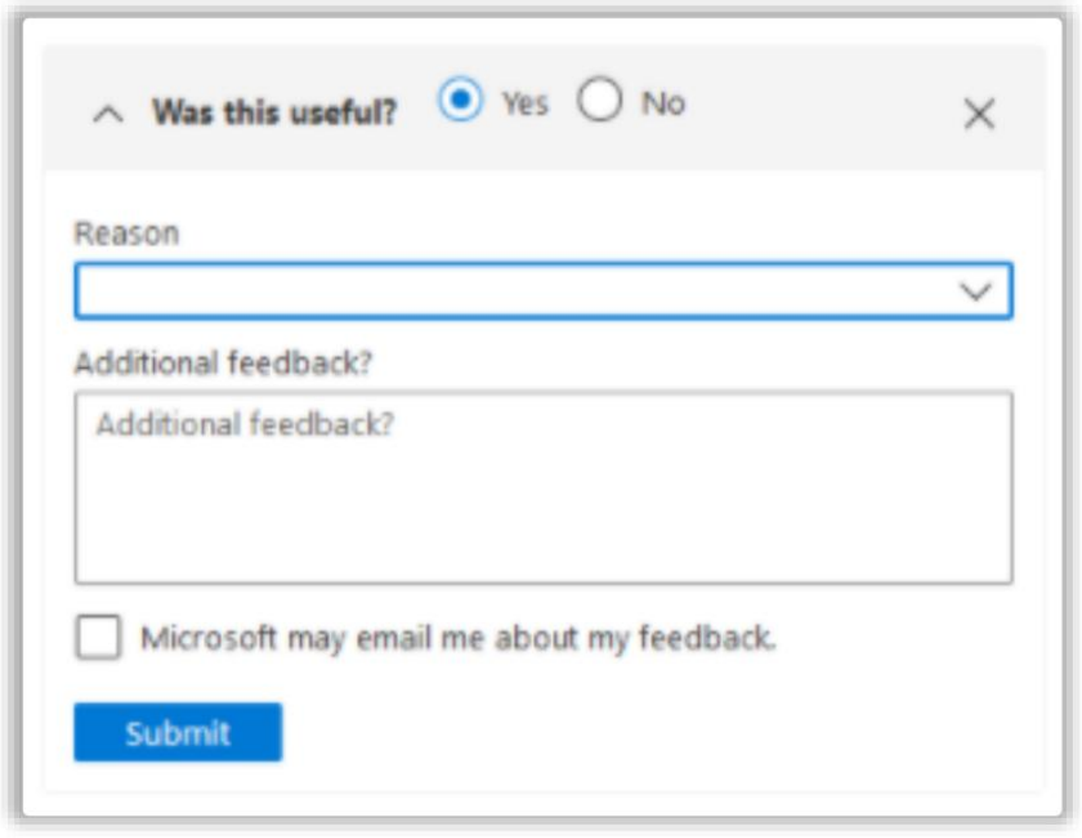
Figure 7.64: Take Action Tab

- For mitigating the issue, review the **Mitigate the threat** section.
- Follow the security recommendations in the **Prevent future attacks** section to secure resources and prevent such attacks in the future.
- Use the **Trigger automated response** section for triggering a logic app with automated response steps.
- Use the **Suppress similar alerts** section if the detected activity does not qualify as malicious to suppress such type of alerts in the future.
- Change the status of the alert to **Dismissed** once you complete the investigation. This will eliminate it from the list of main alerts.



Figure 7.65: Changing the Status of an Alert

- Provide a feedback to Microsoft on the investigated alert. It can be done by specifying the alert as **Not Useful** or **Useful** along with providing a reason and a comment.

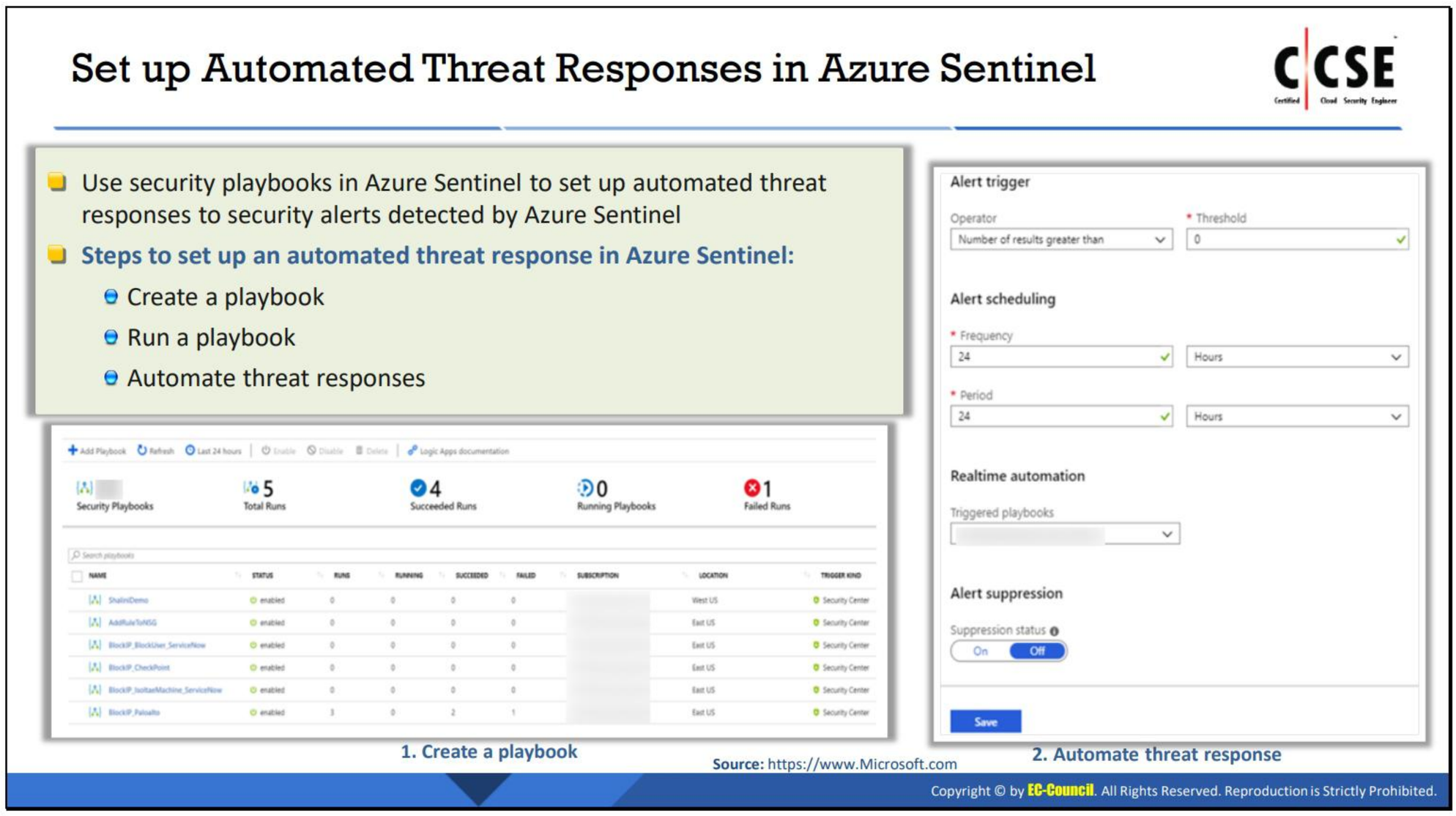


Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 7.66: Providing Feedback

hide01.ir

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



Set Up Automated Threat Response in Azure Sentinel

Use security playbooks to set up automated threat responses to security alerts detected by Azure Sentinel. Setting up an automated threat response in Azure Sentinel involves creating a playbook, running it, and automating threat responses.

Steps to Use Azure Sentinel for Automated Threat Response

- **Create a New Security Playbook**
  - Go to the **Azure Sentinel** dashboard.
  - Choose **Playbooks** under **Configuration**.

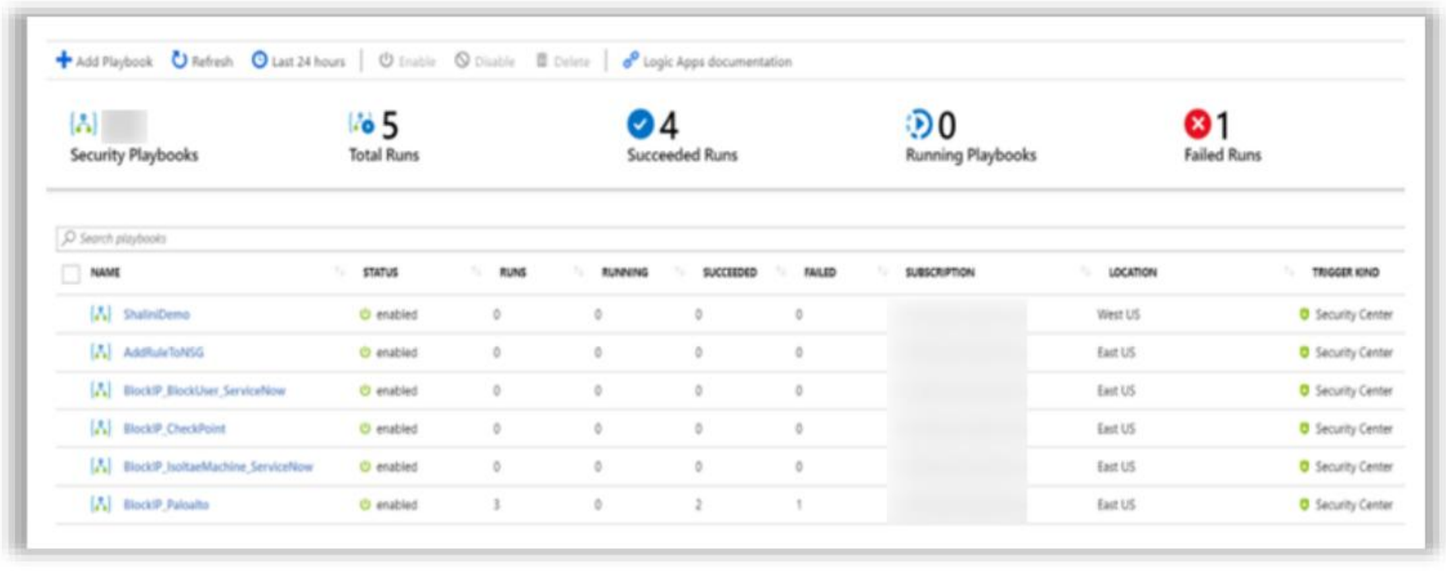


Figure 7.67: Choosing Playbooks

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

- Click on **Add** on the **Azure Sentinel- Playbooks** page.

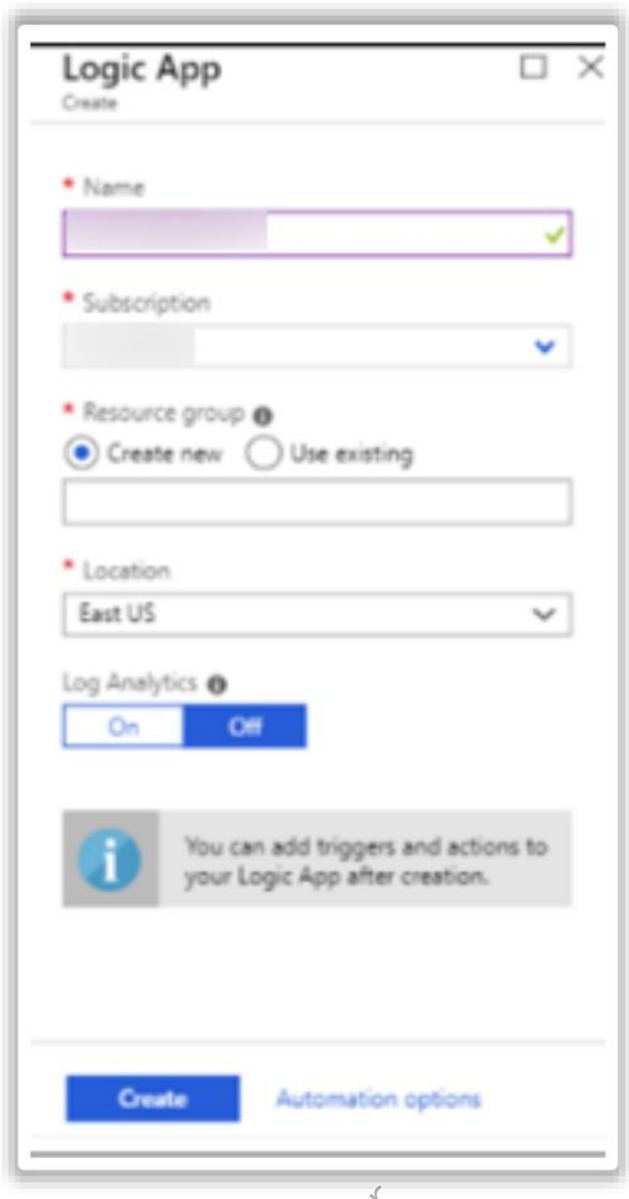


Figure 7.68: Adding Playbooks

- On the **Create Logic app** page, provide the requested information while creating a new logic app and then choose **Create**.
- Choose the template you want from the **Logic App Designer.** Provide the necessary credentials for the templates you want to use. Choose **Blank Logic App** to create a new blank playbook. The Logic App Designer allows you to either edit an existing template or create a new one.

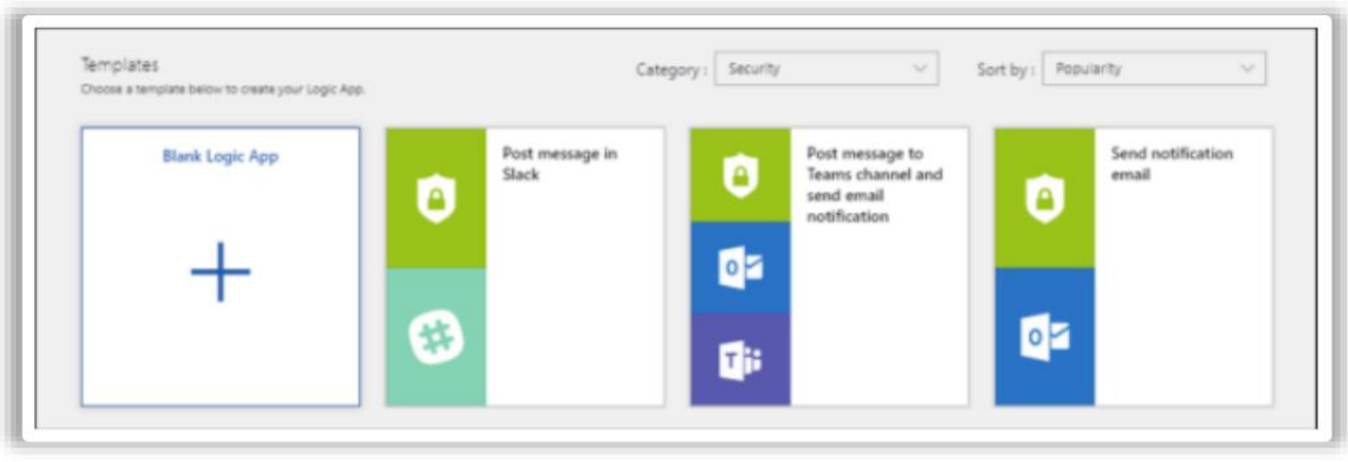


Figure 7.69: Creating a Blank Playbook

- While creating a blank playbook, type **Azure Sentinel** in the **Search all connectors and triggers** field. Then, choose **When a response to an Azure Sentinel alert is triggered**. Once a playbook is created, it is available in the **Playbooks** list. Choose **Refresh** if it is not displayed in the list.

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

- Utilize the **Get entities** function to get relevant entities from the **Entities** list like hosts and IP addresses. This helps perform/run actions on specific entities.
- Define what actions should be taken when the playbook is triggered. Add a logical condition, an action, loops, or switch case conditions.

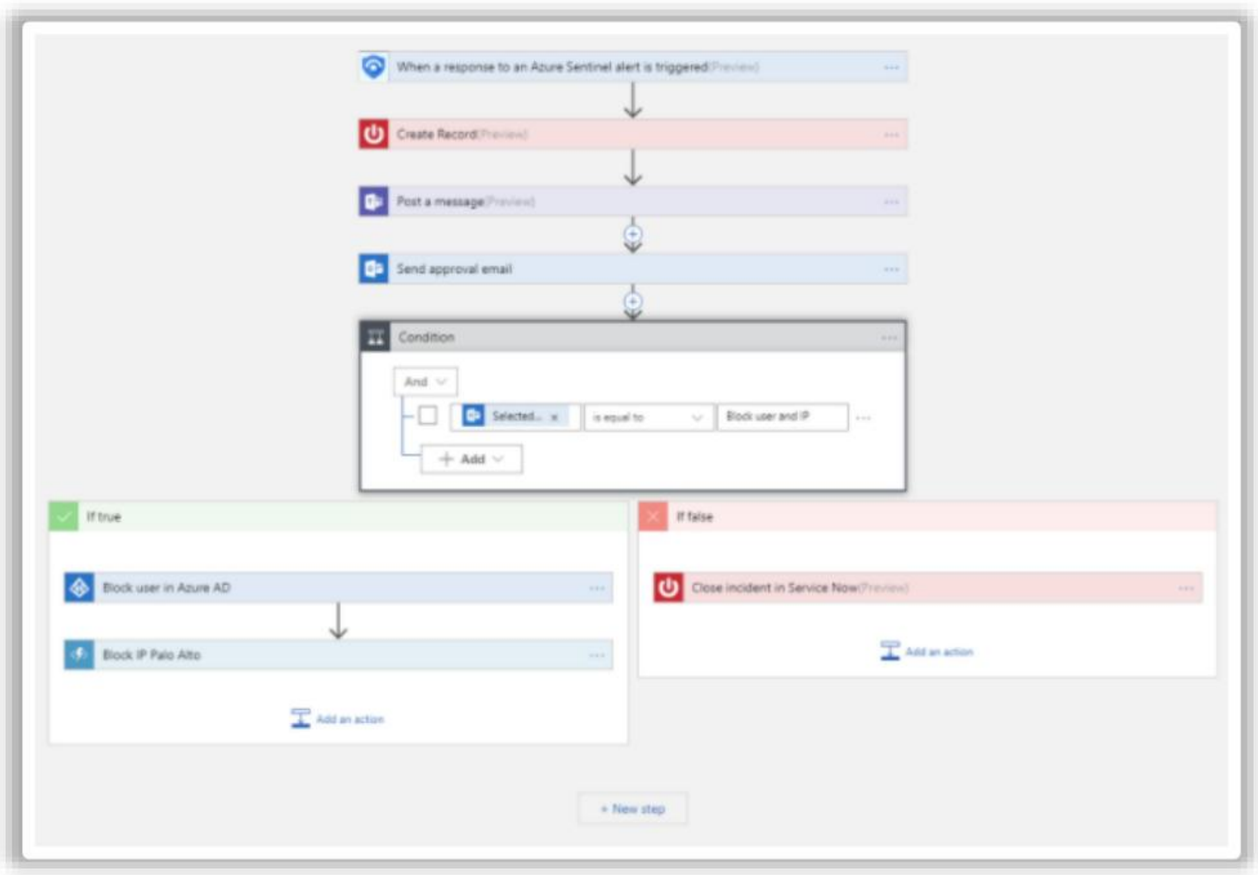


Figure 7.70: Adding Conditions

hade01.ir

- **Run a Security Playbook**
  - Choose an incident on the **incidents** page and click on **View full details**.
  - On the **Alert** tab, choose the alert on which the playbook should run. Click on **View Playbooks** and select a playbook to run from the playbook list.
- **Automate Threat Responses**
  - Choose the alert for which the response has to be automated.
  - Under **Real-time automation** on the **Edit alert rule** page, select the **Triggered Playbook** that must run when this alert rule is matched.
  - Choose **Save**.

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

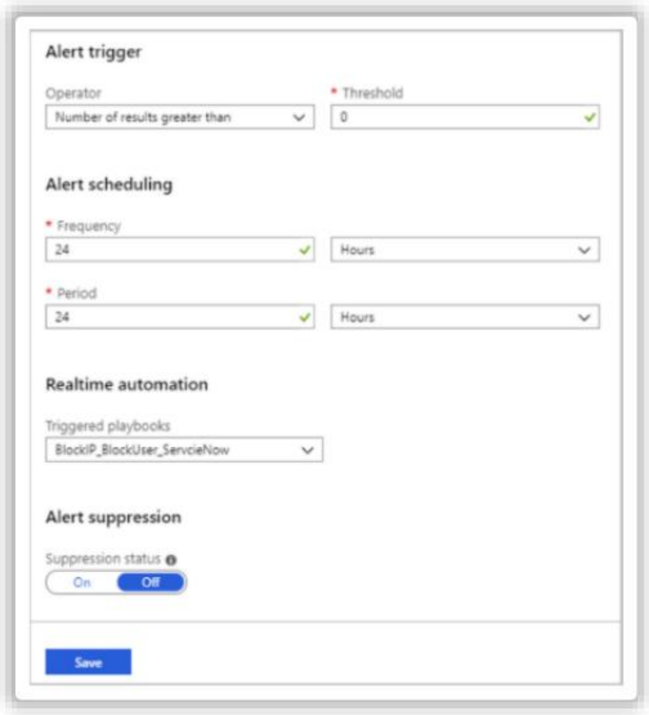
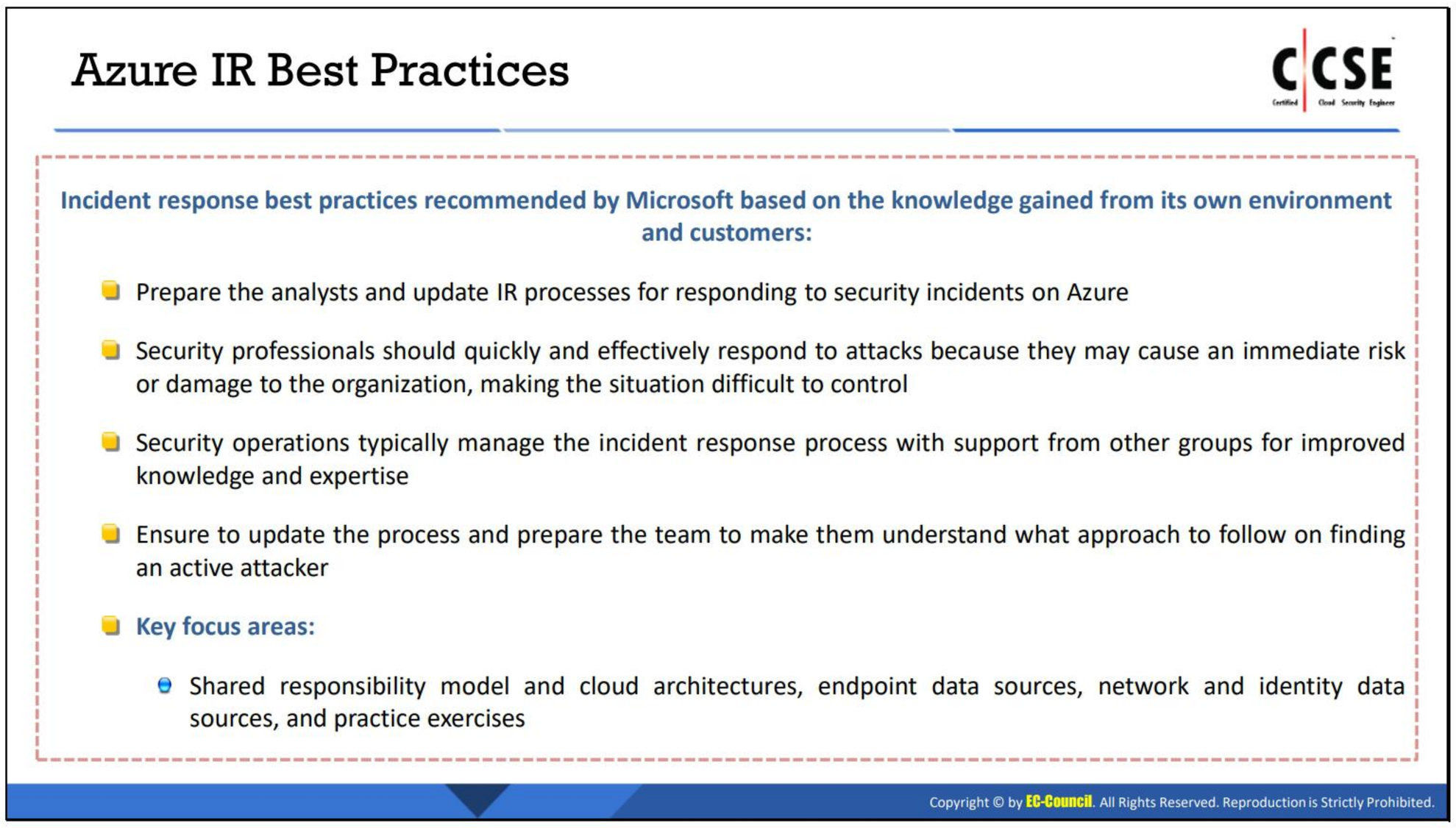


Figure 7.71: Automate Threat Responses

hide01.ir

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



Azure IR Best Practices

Azure IR best practices recommended by Microsoft based on the lessons learned from its customers and its own environment are as follows:

hade01.ir

- Prepare the analysts and update IR processes for responding to security incidents on Azure. Ensure that your team practices simulated attacks because it will help in the actual incidents, where they can provide their best performance in threat hunting, investigation, and remediation.
- Security professionals should quickly and effectively respond to the attacks as they may cause an immediate risk or damage to the organization, making the situation difficult to control. The incident response process must be effective for everything, including systems, accounts, and cloud platforms hosting enterprise data.
- Security operations typically manage the incident response process with support from other groups for improved knowledge and expertise.
    - **Sponsorship:** A security operations director or an equivalent sponsors this process modernization.
    - **Execution:** Collective efforts of multiple individuals or teams (such as security operations incident management team, security operation analysts, and central IT operations) are required to adapt the existing processes or develop them for the first time.
- Ensure process updation and prepare the team on the approach to be followed on finding an active attacker.

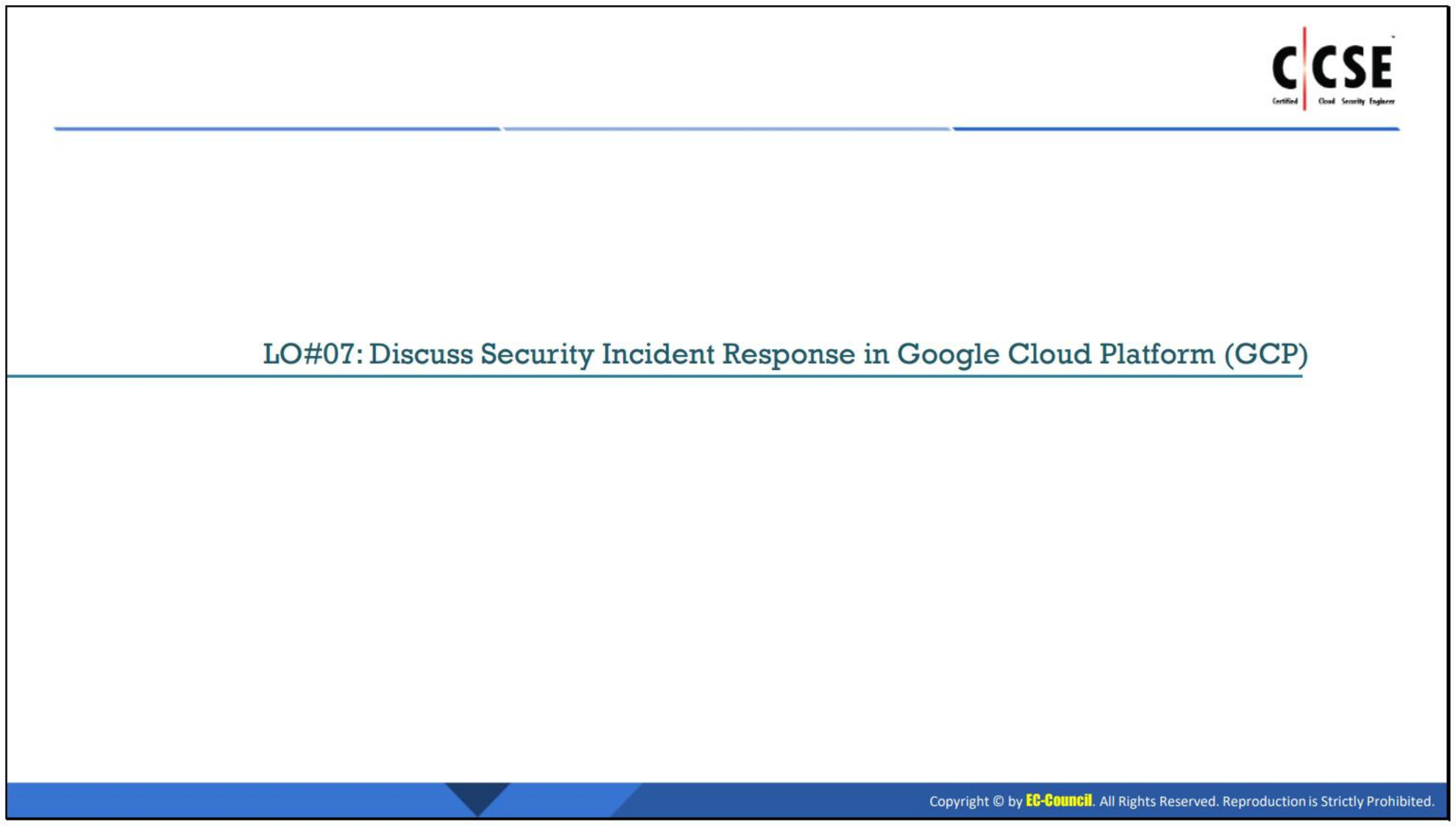
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Process and Playbook:** Adjust the current threat hunting, investigation, and remediation processes according to the differences in the operation of various cloud platforms (different tools, identity protocols, data sources, etc.).
- **Education:** Educate security analysts on cloud transformation, updated or new processes, and technical details of a platform for them to understand the differences and fulfill their requirements.

- The focus areas of education and planning efforts include
  - **Shared Responsibility Model and Cloud Architectures:** Security analysts may find Azure as a software-defined datacenter that provides multiple services, including those similar to on-premises services (e.g., VMs) and those which are different (e.g., Azure SQL functions). In the cloud, the best data is stored in service logs or threat detection services. Security analysts need to understand what data to expect, how to get it, and its format while working in a cloud environment.
  - **Endpoint Data Sources**: Use cloud-native detection tools such as EDR systems and ASC to get insights and data for malware and attacks on servers hosted on the cloud.
  - **Network and Identity Data Sources**: Security analysts should develop a deep understanding of cloud identity protocols to get visibility into attacker activity to support incident response and investigation. Identity protocols and directories on the cloud are different from those on-premises. They are commonly based on OAuth, SAML, etc.
  - **Practice Exercises**: Conduct exercises involving simulated attacks and responses because they help verify the organizational readiness to handle incidents.

hide01.ir

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

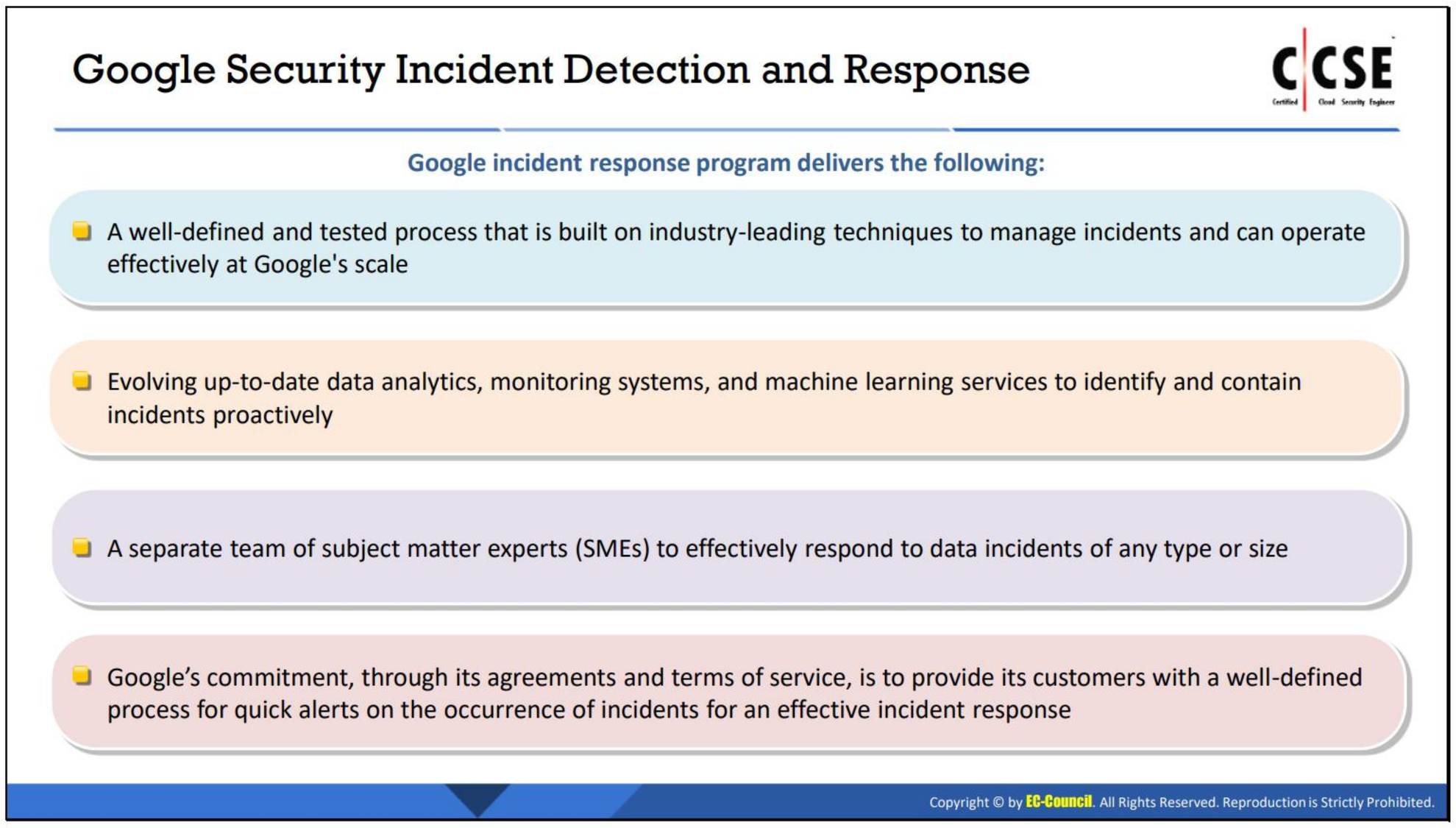


LO#07: Discuss Security Incident Response in Google Cloud Platform (GCP)

The objective of this section is to explain the process of security incident detection and response in Google cloud platform (GCP) such as identification, coordination, resolution, closure, and continuous improvement. It also describes the responsibilities of an incident response team and shows how to implement various tools for detecting and responding to incidents in GCP.

hid01.ir

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



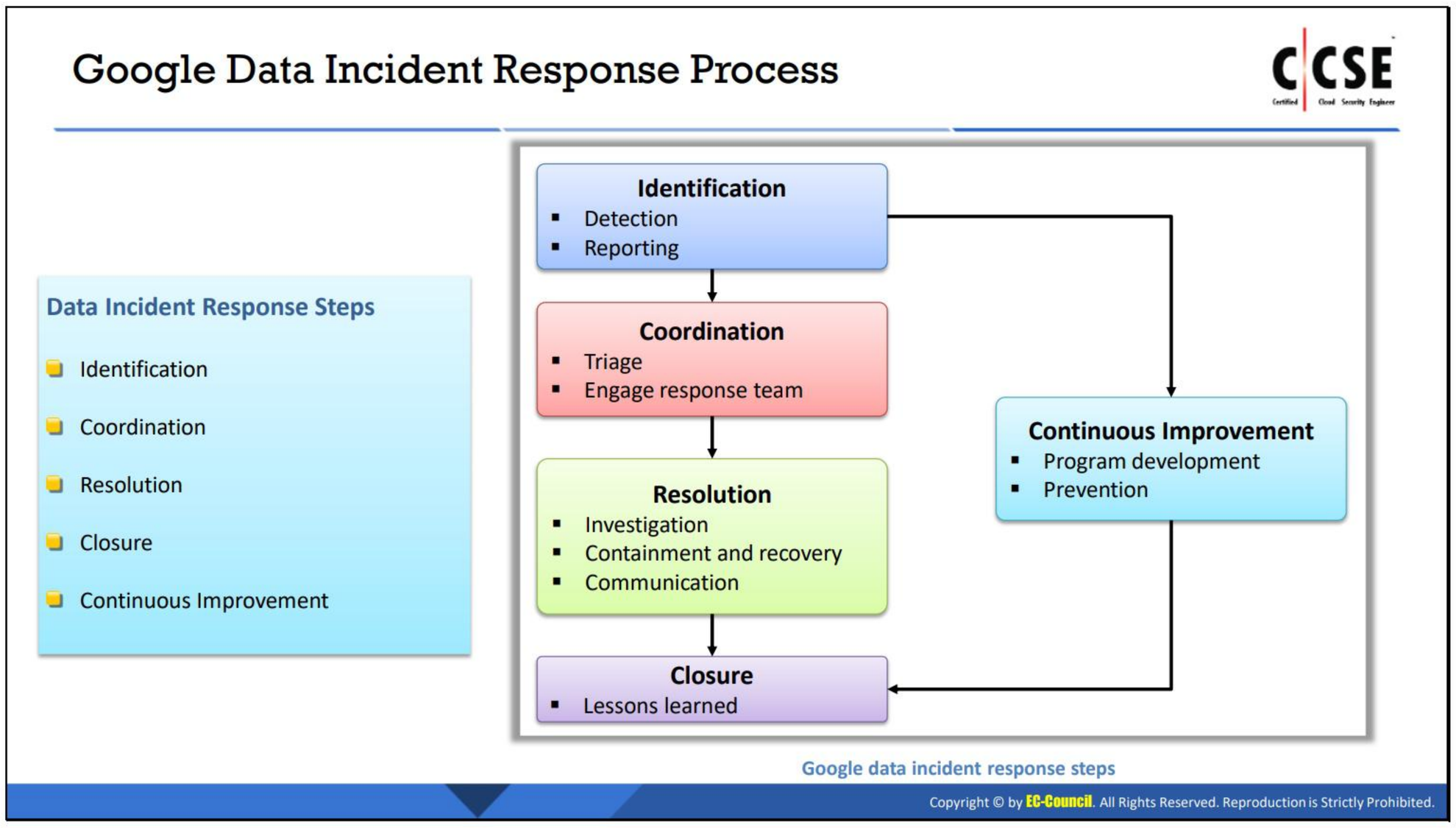
Google Security Incident Detection and Response

Google incident response (IR) program includes actions, escalations, mitigations, resolutions, and notifications of incidents to ensure confidentiality, integrity, and availability. Google incident response has the following features:

hide01.ir

- Google IR program offers the latest techniques to resolve incidents efficiently.
- It detects and mitigates incidents by deploying monitoring systems, data analytics services, and machine learning techniques.
- It includes subject matter experts (SMEs) who can be deployed for responding to any type or size of data incident.
- Google IR program notifies the affected customers in accordance with the service terms and agreements.

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



Google Data Incident Response Process

Incident response in GCP includes five steps:

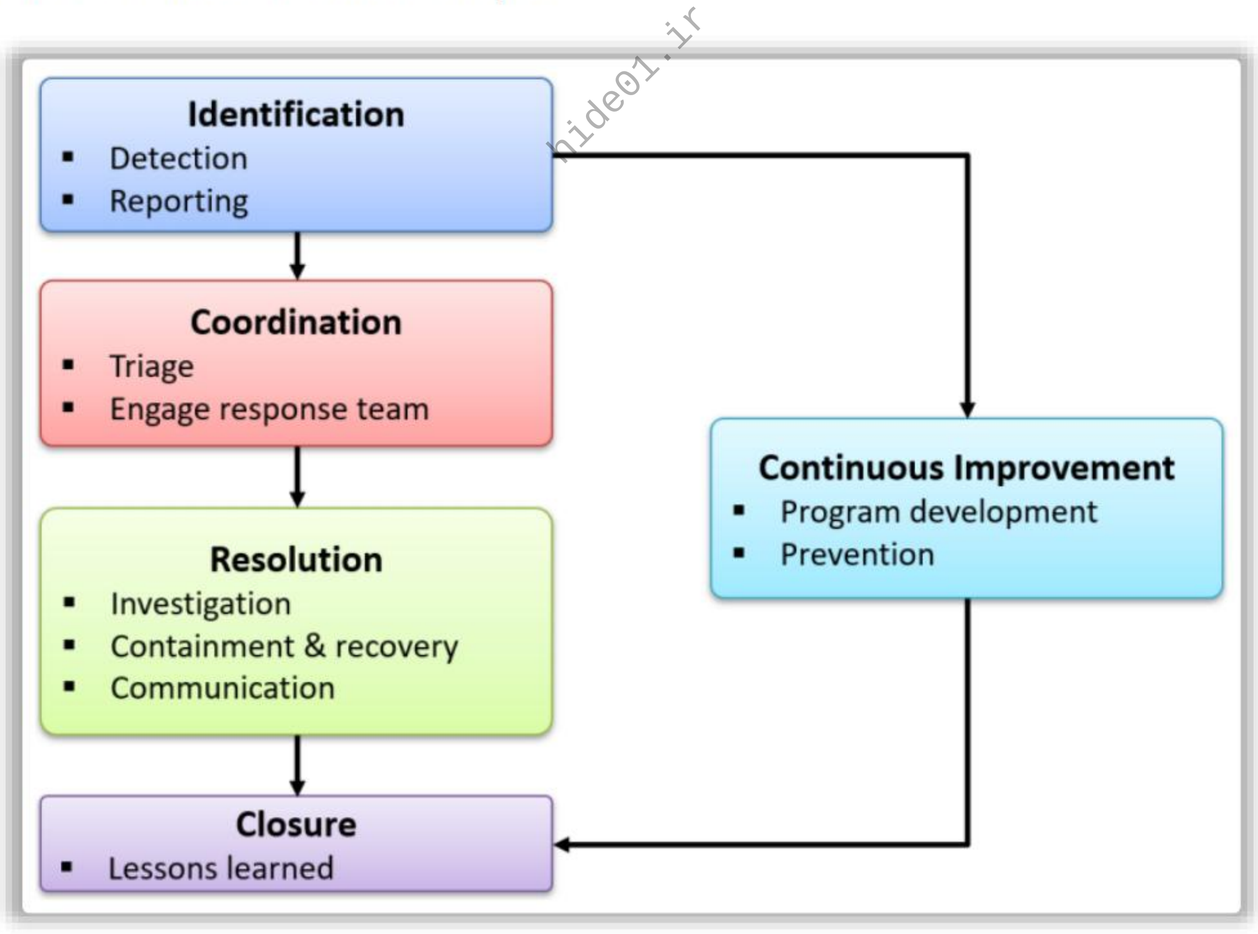


Figure 7.72: Google Data Incident Response Steps

- **Identification**

  The best approach to protect GCP data from incidents is the early detection of an incident. GCP provides tools, signals, and alert mechanisms for an early incident detection. The methods deployed by Google for the early identification of an incident are

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

- **Automated Logs Analysis**: Google employs automated network traffic analysis to monitor any type of suspicious activities.
- **Testing**: The security team of Google performs penetration tests, intrusion detection tests, and quality assurance checks on the infrastructure.
- **Internal Code Reviews**: Verification of the source code helps detect any hidden vulnerabilities and design flaws.
- **Product Specific Tools**: Product-level incidents can be detected by domain-specific automated tools.
- **Anomaly Detection**: To differentiate between legitimate and malicious activities, machine learning systems are deployed at different layers.
- **Vulnerability Rewards Programs**: Google offers vulnerability rewards programs where security researchers can report any vulnerabilities in GCP infrastructure and will be eligible for rewards if they are valid.

- **Coordination**

  The Google incident response process starts only after an on-call responder reviews the incident type to check whether it is a data incident. The incident is then forwarded to an incident commander, and the team coordination starts here. This is followed by triage assessment, severity assessment, and informing the incident response team to analyze the areas that require an investigation. The incident response processes are decided by the product lead and legal lead. The severity assessment is based on the nature of an incident, the type of affected data, impact, and the incident status.

- **Resolution**

  The real cause of an incident, its mitigation, and the necessary security fixes can be done in this phase. To determine the reason behind an incident or the type of its impact on the data, a forensic analysis is performed. To notify the customers if the incidents affects their data, the communications lead develops a communication plan in consultation with the product and legal leads. They inform the customers about the data incident.

- **Closure**

  Critical incidents are closed with a post-mortem analysis to identify the underlying reasons and the measures to be adopted to prevent such incidents in the future. Project managers are assigned with incident follow-up tasks if required. The incident is closed after completing the remediation process.

- **Continuous Improvement**

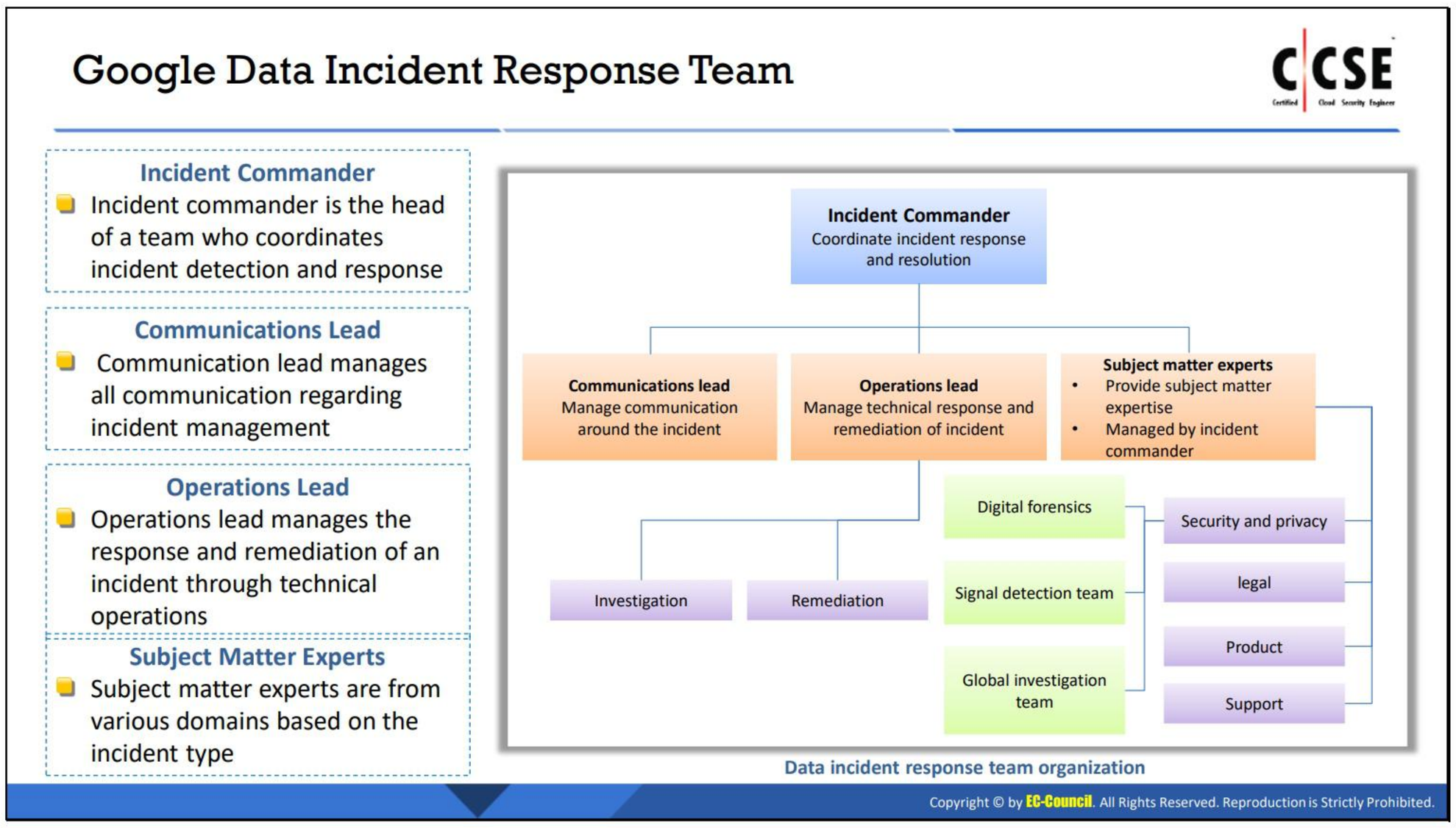
  Google improves the overall security posture by analyzing previous incidents and deploying measures to prevent future incidents. Machine learning methods are employed for analyzing malicious activities, responding to threats, and conducting security audits. Project Zero team of Google reports bugs to software providers, which

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

helps prevent attacks. Google conducts security awareness campaigns, and incident response procedures are tested on systems that store sensitive information.

hide01.ir

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



Google Data Incident Response Team

The team organization of the incident response team includes an incident commander as the head. The different responsibilities of other team members are assigned by the incident commander based on the different aspects of an incident. The incident response team organization includes the following:

- **Incident Commander:** The head of a team who coordinates the incident response and resolution plans.
- **Communications Lead:** A communication lead manages the communications related to an incident.
- **Operations Lead:** The operations lead manages the response and remediation of an incident through technical operations.
- **Subject Matter Experts:** The subject matter expert team includes experts from different fields based on the incident type. They are involved in different domains such as security and privacy, legal, product, support, digital forensics, signals detection, and global investigations.

hide01.ir

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

The hierarchy of the incident response team is shown below.

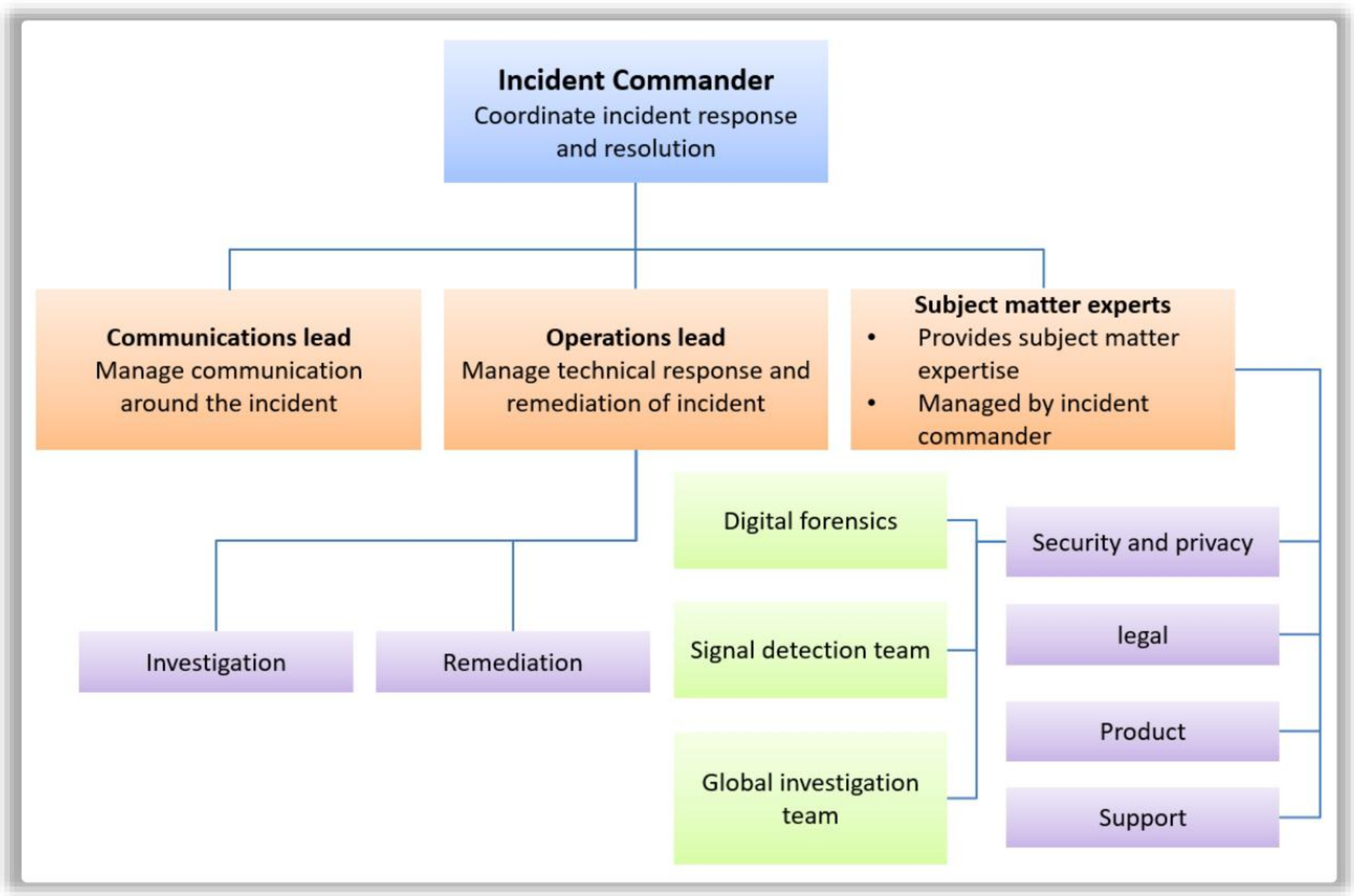
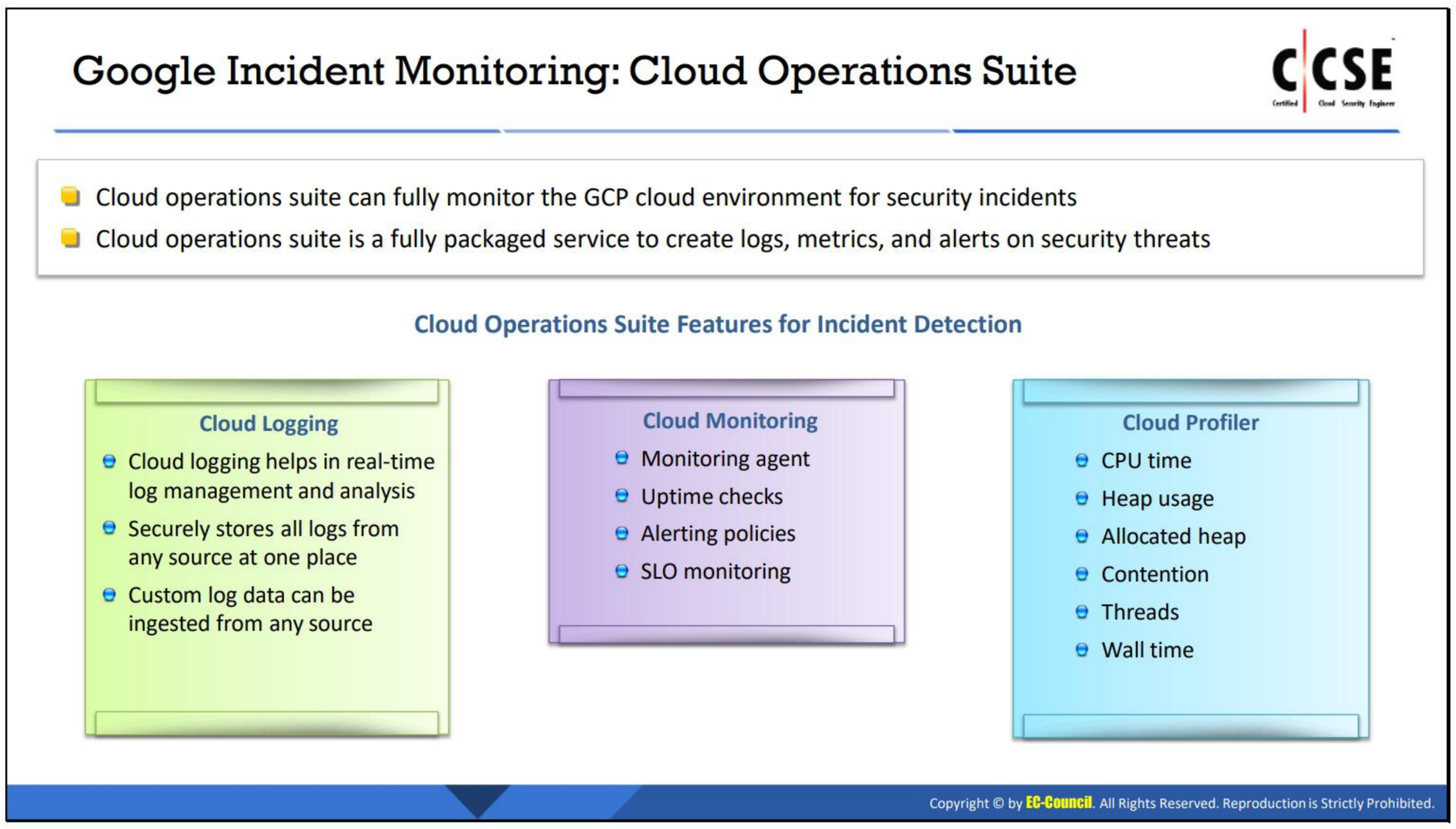


Figure 7.73: Data Incident Response Team Organization

hide01.ir

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



Google Incident Monitoring: Cloud Operations Suite

The GCP cloud environment can be monitored by GCP operations suite, a fully packaged service that creates logs, metrics, and alerts on security incidents. Filters can be applied to the logs and alerts to investigate a particular incident. Security Command Center is another platform in GCP for real-time monitoring of the infrastructure. It consists of Security Health Analytics, Web Security Scanner, and Event Threat Detection, and helps collect log data to take necessary actions on threats.

Google Cloud Operations Suite

Google Cloud operations suite specifically detects incidents on applications deployed in GCP. It includes

- **Cloud Logging**: Cloud Logging helps in the management of logs.

  It consists of a user interface called Logs Explorer, a storage for logs, and an API to manage the logs. The different features of Cloud Logging that help in incident detection are

  - **Logging Agent:** Logs are collected from third-party applications and system software by logging an agent's default configuration. It can also be configured to collect additional logs.
  - **Log Entries**: The log entries, considered the basic logging units, provide information on specific types of events in a system and then inform users that everything is working as expected or information about any failures. A log entry consists of a timestamp, deployed resources, payload/messages, and a corresponding log name.

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

- **Logs**: Named set of log entries.
- **Log Types in Cloud Logging:** Cloud Logging receives and stores the log entries from various sources, and supports the following types of logs:
  - **Google Cloud Platform Logs**: These logs are service-specific and depend on the resources used by the customer in the GCP project.
  - **User Logs**: The logs generated by user software, services, or applications.
  - **Agent Logs**: These logs are collected by a logging agent and then sent to Cloud Logging.
  - **Admin Activity Audit Logs**: The admin activity logs include information about administrative action API calls that create or modify the infrastructure's resources.
  - **Data Access Audit Logs**: Data access audit logs contain information about API calls that read, create, or modify data.
  - **System Event Audit Logs**: System event audit logs contain information regarding GCP actions that modify resources.
  - **Policy Denied Audit Logs**: Policy denied audit logs contain information about a GCP service that is denied access to an account because of security policy violations.
  - **Access Transparency Logs**: Access transparency logs provide the measures adopted by Google when a user is accessing the content. It also helps in ensuring the security compliance of the organization.
  - **Hybrid-cloud and Multi-Cloud Logs:** Logs that are collected from other CSPs (e.g., AWS and Azure) and ingested by GCP are known as multi-cloud logs. The logs from on-premises infrastructure and applications are called hybrid-cloud logs.
  - **Structured Logs**: Structured logs are a type of logs in Cloud Logging with a jsonpayload field to add a structure to the payloads.
  - **VPC Flow Logs**: VPC Flow logs contain information regarding the network traffic sent and received from VM instances.
  - **Firewall Rules Logging**: This feature helps verify the working of firewall rules to ensure they are functioning as intended.
  - **Retention Period**: The time for which the logs will be available in Cloud Logging before being deleted is called retention period. The retention period can be configured for some logs.
- **Monitored Resources**: The log entry also includes the name of the monitored resource.

hide01.ir

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

- **Queries**: Queries are expressions in logging query language to select log entries based on specific parameters.
- **Logs Router**: The Cloud Logging APIs pass the logs through the Logs Router, which verifies them and then stores, exports, or discards them.
- **Sinks**: The logs can be exported using log sinks. The sink includes a destination and a filter which selects the log entries to be exported.
- **Logs-based Metrics**: The value of these metrics is the number of log entries matching a specified query.

- **Cloud Monitoring:** Cloud Monitoring helps analyze whether the services hosted in GCP are healthy, whether a service loads, and whether they are performing well. The different types of Cloud Monitoring are
  - **Black Box Monitoring:** In black box monitoring, the monitoring procedure is similar to what a normal user does to avail a service. This type of monitoring does not reveal any information regarding the internals.
  - **White Box Monitoring:** White box monitoring can be performed to monitor only specific services.
  - **Gray Box Monitoring:** Information regarding the present state of the service environment can be collected by gray box monitoring.
  - **Logs-based Metrics:** Metrics collected from the content of the logs in Cloud Logging are called logs-based metrics.

The different capabilities of Cloud Monitoring are

- **Workspaces**: Workspaces can be used for monitoring the resources of multiple GCP projects. A single workspace can monitor exactly a single GCP project or AWS account. Thus, every workspace has a host project, which is the GCP project used to create the workspace.

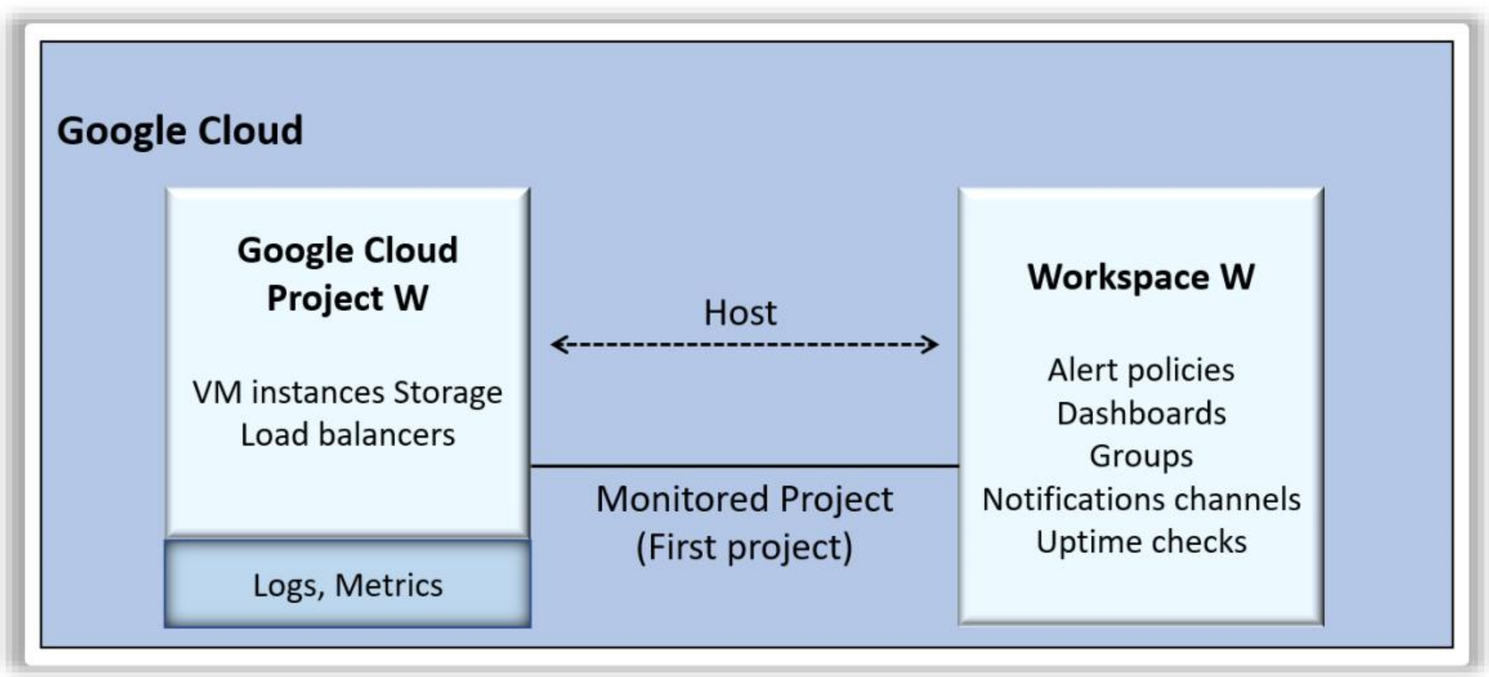


Figure 7.74: Workspace

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

- **Monitoring Agent:** The system and application metrics are collected from VM instances and then sent to monitoring by the Cloud Monitoring agent. The disk, CPU, network, and process metrics are collected by default.
- **Uptime Checks:** Uptime checks are performed to check the availability of a resource. It is performed by sending a request to the resource and verifying whether it responds.
- **Alerting Policies:** An alerting policy can be created based on the conditions under which and how an alert is generated. The alerting policies specify
  - **Conditions**: The conditions identify whether the resources are in a state that requires an action.
  - **Notifications**: To inform the support team that the conditions are met. The notification channels include emails, Cloud Console Mobile App, PagerDuty, SMS, and Slack.
  - **Documentation**: Documentation can be done for some notifications to resolve an issue.
  - **Metrics Explorer:** Charts can be built by Metrics Explorer for the metrics collected by the project. The charts can be shared and saved, and the configurations can be viewed in a JSON format.
  - **Dashboards and Charts:** Predefined dashboards for services are provided by GCP. Custom dashboards can also be created with Cloud Monitoring.
  - **Custom Metrics**: Custom metrics can be created within the GCP projects and they begin with custom.googleapis.com. Time-series data can be added to custom metrics.
  - **Monitoring Query Language (MQL)**: MQL contains a set of operations and functions to manipulate time-series data and view it in a text-based interface.
  - **SLO Monitoring**: SLO monitoring includes three concepts: SLI, SLO, and error budget.
    - **Service Level Indicator (SLI)**: A performance measurement
    - **Service Level Objective (SLO)**: A statement of the desired performance
    - **Error Budget**: A measurement of the difference between real performance and desired performance.

  SLO monitoring provides tools to create alerting policies based on SLOs, and thus helps in monitoring the health of GCP services.
- **Resource Groups**: A set of resources can be defined as a group and alerting policies, charts, and dashboards can be configured to monitor it. A dashboard will

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

be created by Cloud Monitoring if a group is created. Group dashboards provide the functionalities for editing or deleting a group, managing the alerting policies, viewing incidents and events, etc.

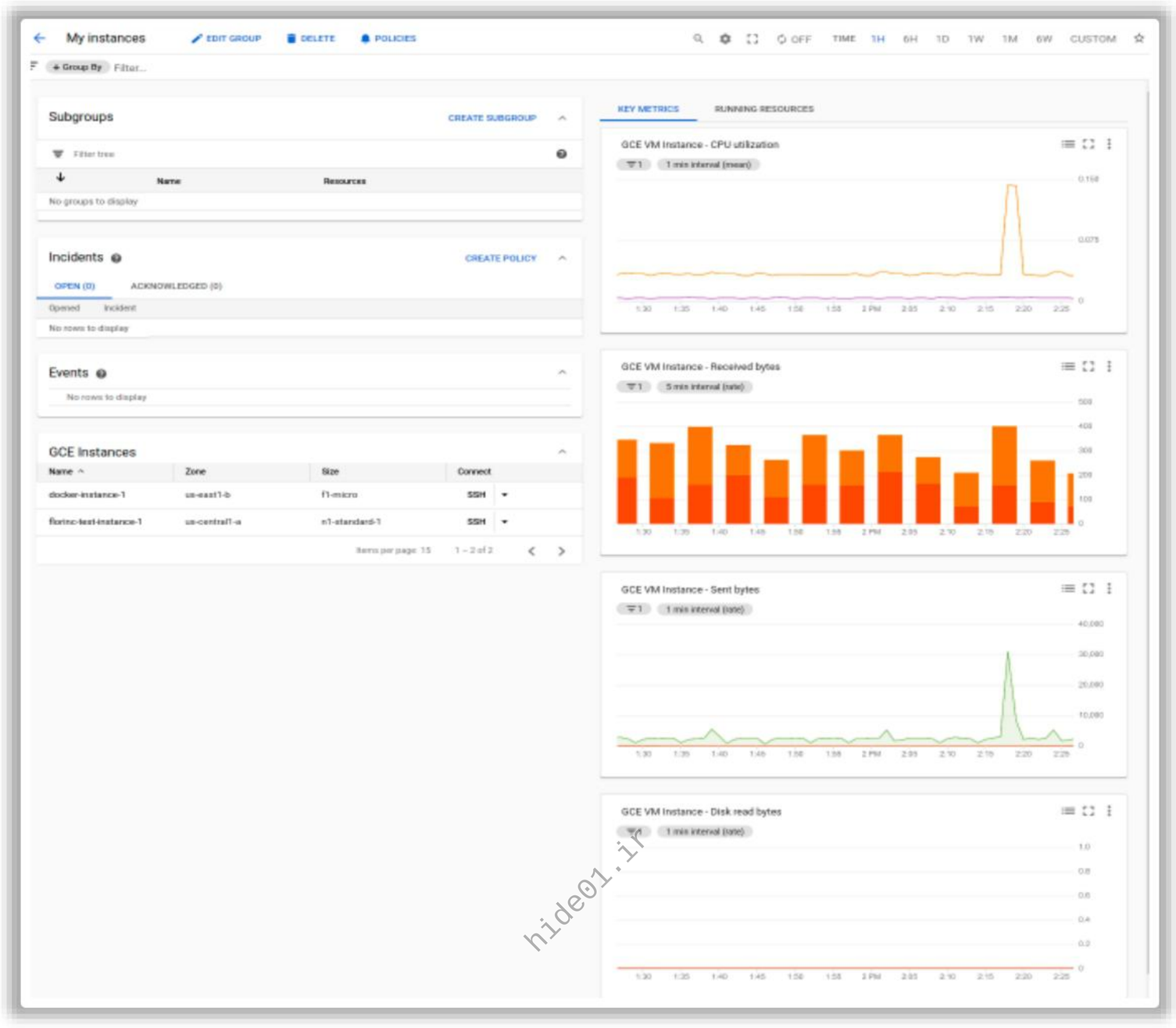


Figure 7.75: Group Dashboard

- **Cloud Profiler**

  Cloud Profiler can collect the information regarding the CPU usage and memory allocation of applications deployed in GCP. Thus, the application performance can be monitored in real-time. The profiling agent collects the data, and the console interface helps view it.

  Types of Profiling in Cloud Profiler

  - **CPU Time**: CPU time is the time consumed by a CPU to execute a block of code.
  - **Heap (**heap usage/ memory usage) is defined as the amount of memory that is assigned in the program's memory at a single point of time when the profile was collected.
  - **Allocated Heap**: The total memory allocated from the program's memory when the profile was collected.
  - **Contention**: In multiple threading programs, knowing the time spent in accessing a shared resource can help design a code and tune the performance accordingly.

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

- **Threads**: Applications that are suffering from blocked threads.
- **Wall Time**: The time consumed in running a block of code.
- **Flame Graphs**: Cloud Profiler displays the monitoring data using flame graphs. An advantage of flame graphs is that they contain a lot of information in a small readable format. The frames in a flame graph depict a function in a particular service. The width of the frame represents the analyzed metric's consumption.

- **Cloud Profiler Interface**

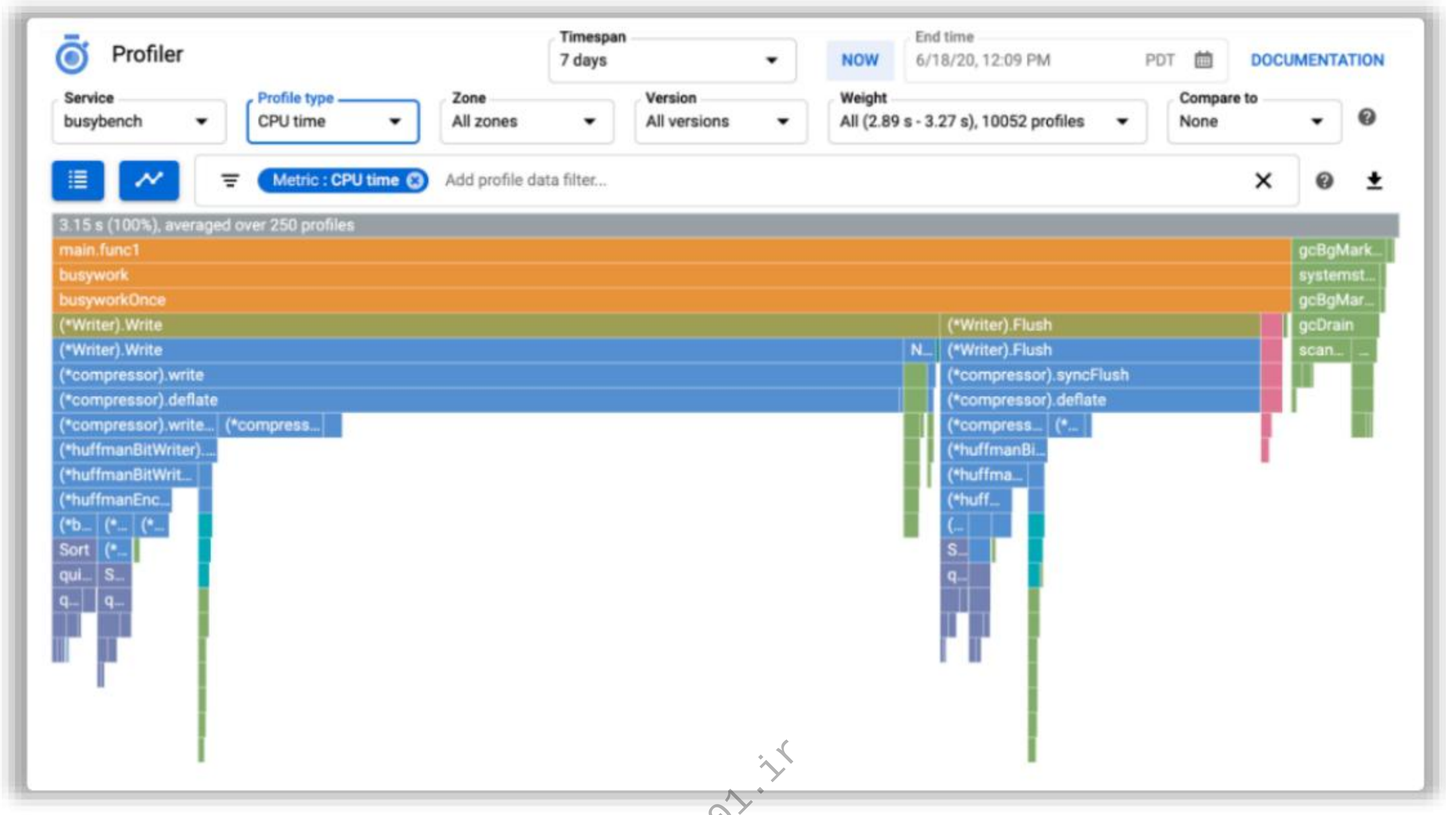


Figure 7.76: Cloud Profile Interface

- **Viewing the Selected Profiles**
  - **List**: To view the list of functions and metric consumption.

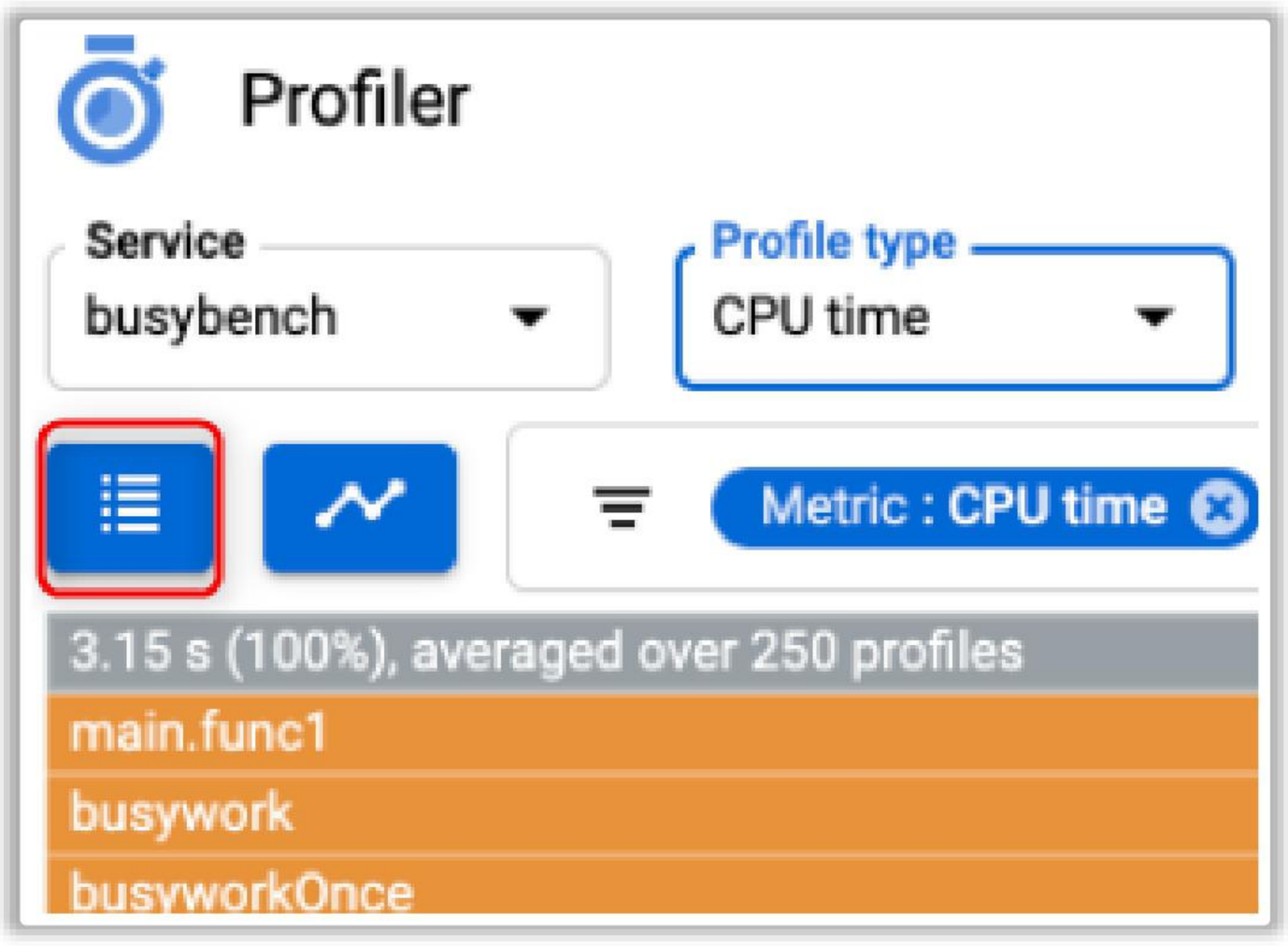


Figure 7.77: CPU Time

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

- **History**: The **History** button displays the average resource usage over the past 30 days.

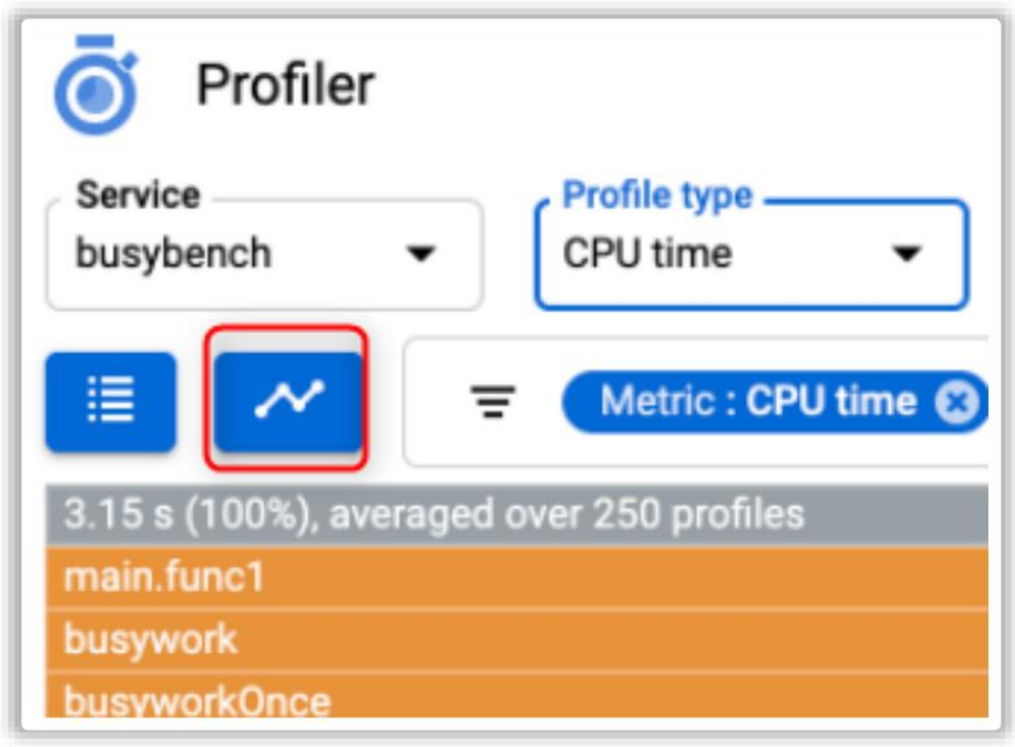


Figure 7.78: History

- **Filter:** The view of the selected profiles can be adjusted by applying filters.

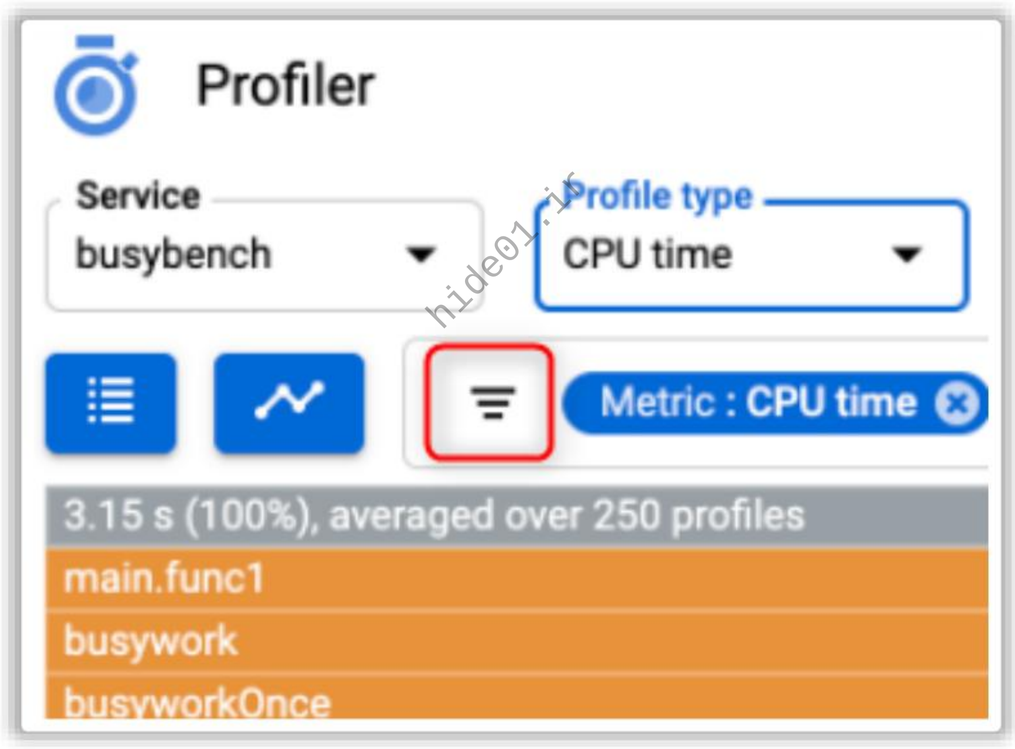


Figure 7.79: Filter

- **Download:** To download the currently viewed profile to a local system

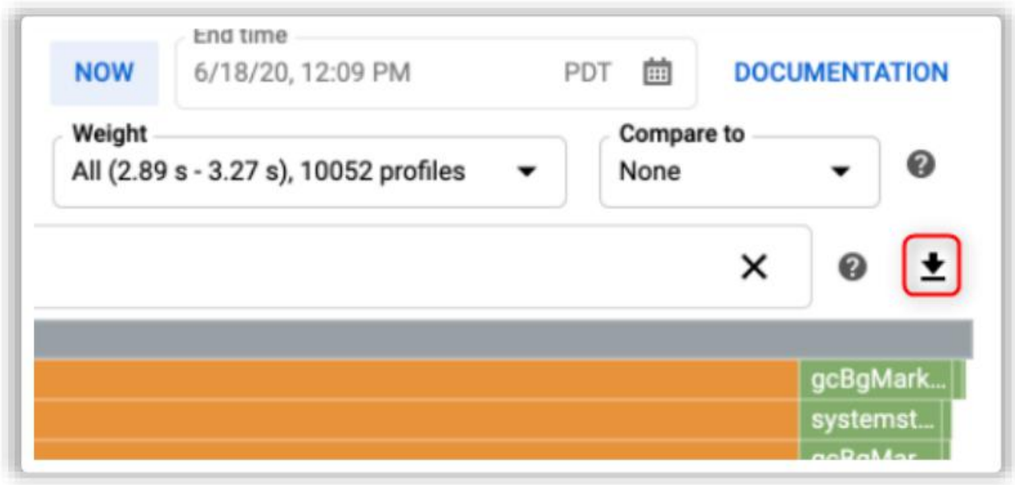


Figure 7.80: Download Profile

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



Incident Detection and Response: Security Command Center

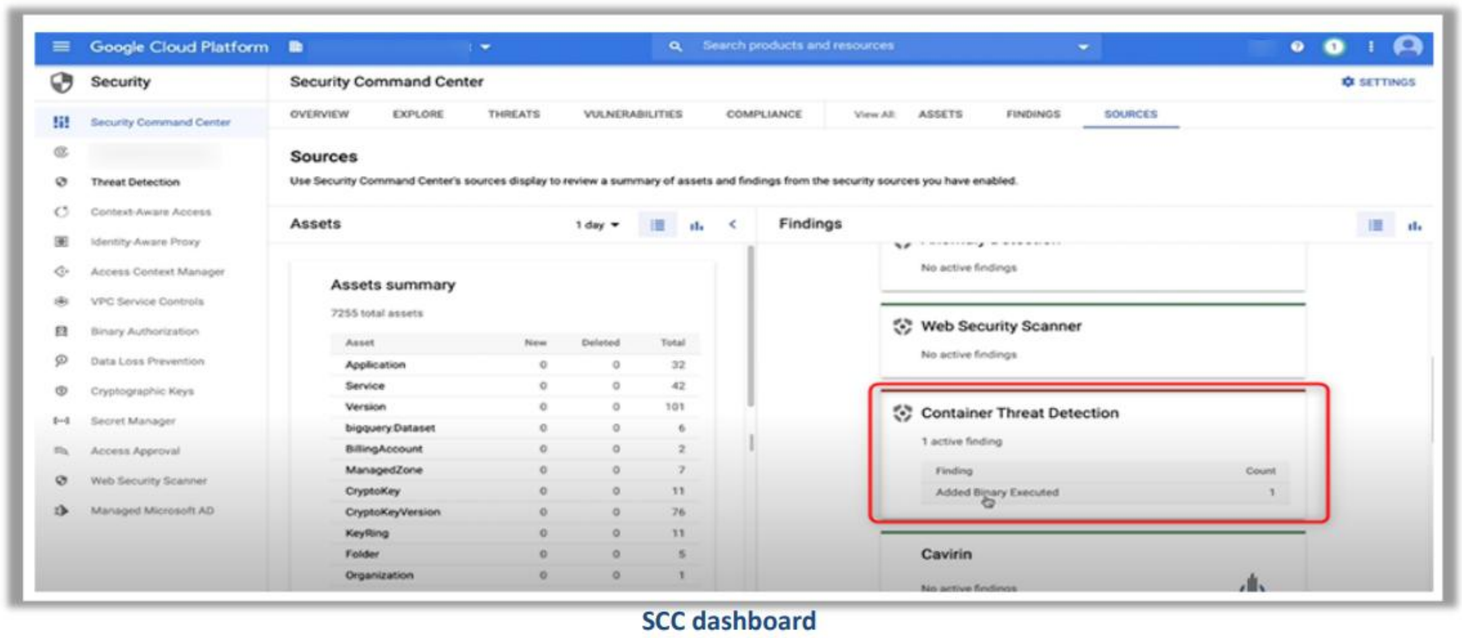
Security command center (SCC) is a security and risk management platform that provides dashboard-based analytics for detecting and responding to security risks in GCP. In GCP SCC, assets are a systematic view of the threats and attacks to the GCP infrastructure. Findings are the possible security vulnerabilities in the infrastructure collected by the security detection services. The IR features of SCC are

- **Asset Review**: SCC executes asset discovery scans to detect new, modified, or removed assets.
- **Identification of Sensitive Data**: SCC identifies sensitive data and prevents it from any unauthorized access or exposure.
- **Detection of Application Vulnerabilities**: The Web Security Scanner in SCC helps in detecting application vulnerabilities such as cross-site scripting.
- **Monitoring Access Control**: SCC monitors access controls across the GCP infrastructure and sends alerts for deviations.
- **Anomaly Detection**: The anomaly detection capabilities of SCC help in identifying threats, such as abnormal network traffic and bot attacks.
- **Real-time Alerts**: SCC provides real-time alerts through emails and SMS.
- **Security Marks**: Findings or assets can be annotated using security marks. These marks can be used to perform searches, filter, add access levels, group the findings for applying policies, and prioritize findings.
    - **Tags**: Tags are user-level annotations for defining security groups, network segmentation, and firewall rules.

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

Security Command Center: Container Threat Detection

- Container Images are monitored in real time to detect run-time attacks and alerts
- The low-level behavior in a guest kernel is collected and events are detected
- Types of detectors: added binary executed detector, added library loaded detector, and reverse shell detector



SCC dashboard

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

Security Command Center: Container Threat Detection

The container images are monitored by Container Threat Detection, a built-in service to detect run-time attacks and their related alerts. The low-level behavior in a guest kernel is collected to detect events. Added binary executed, added library loaded, and reverse shell are the detector types.

hidden01.ir

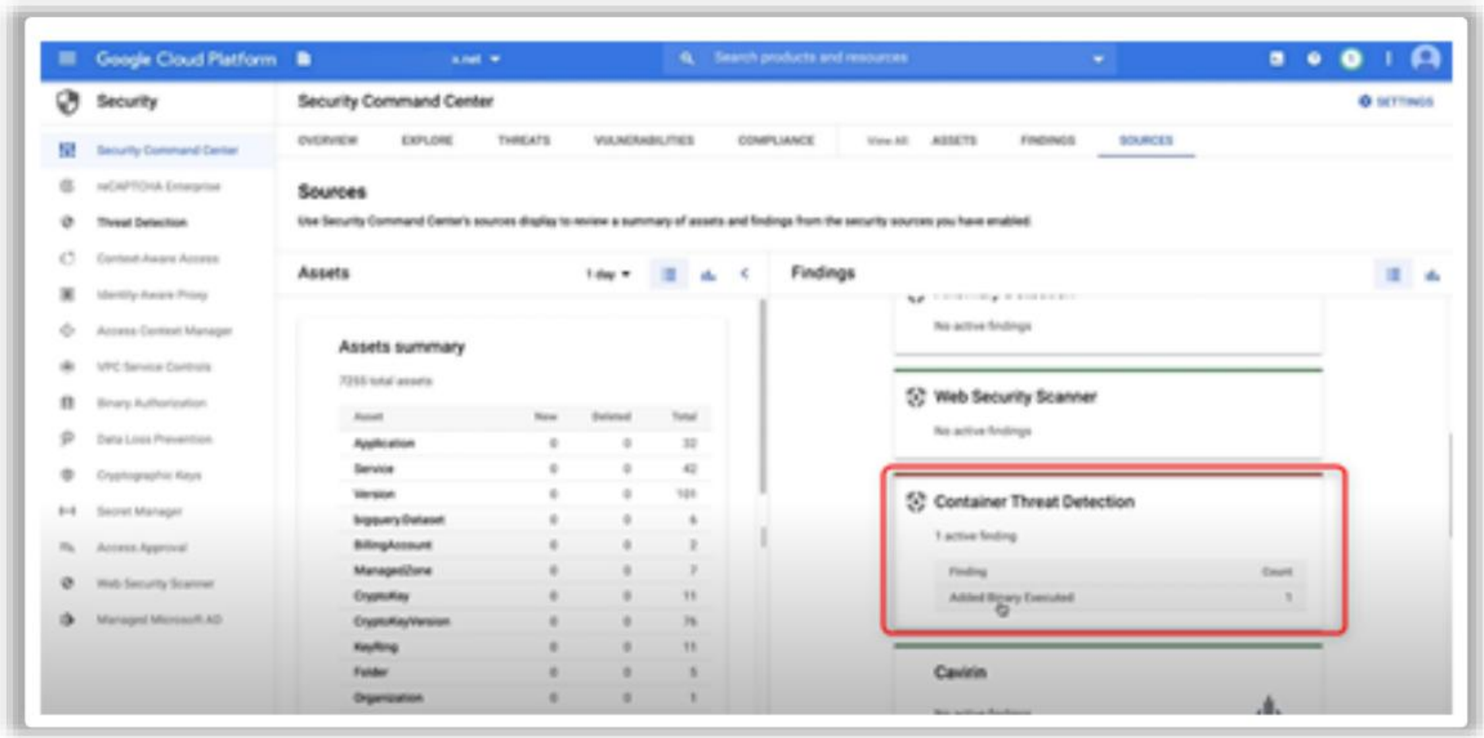
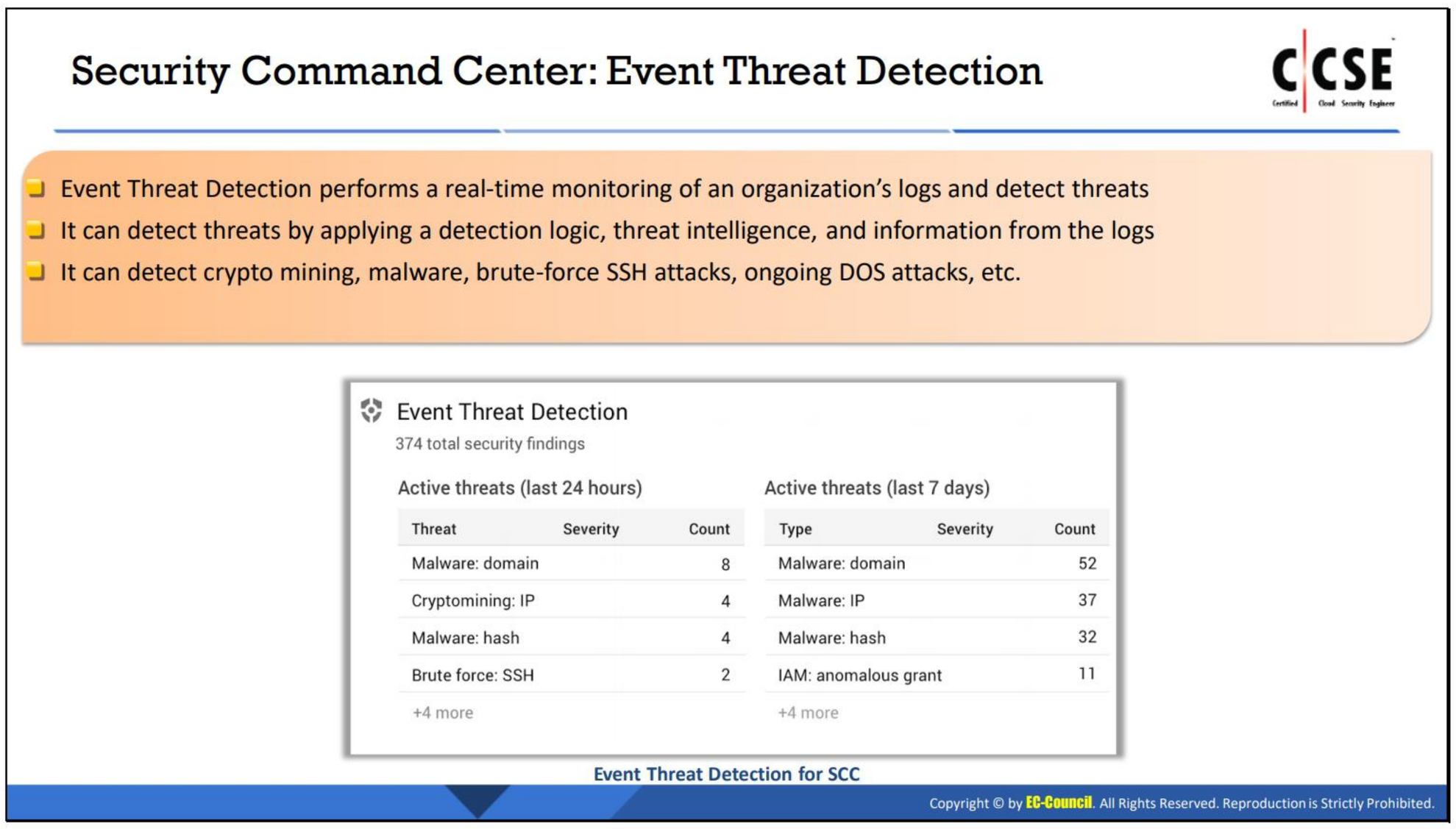


Figure 7.81: Container Threat Detection

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



Security Command Center: Event Threat Detection

Event threat Detection performs a real-time monitoring of an organization's Cloud Logging logs and detect threats by applying a detection logic, threat intelligence, and information from the logs. It can detect crypto mining, malware, brute-force SSH attacks, ongoing DoS attacks, etc.

hid001.ir

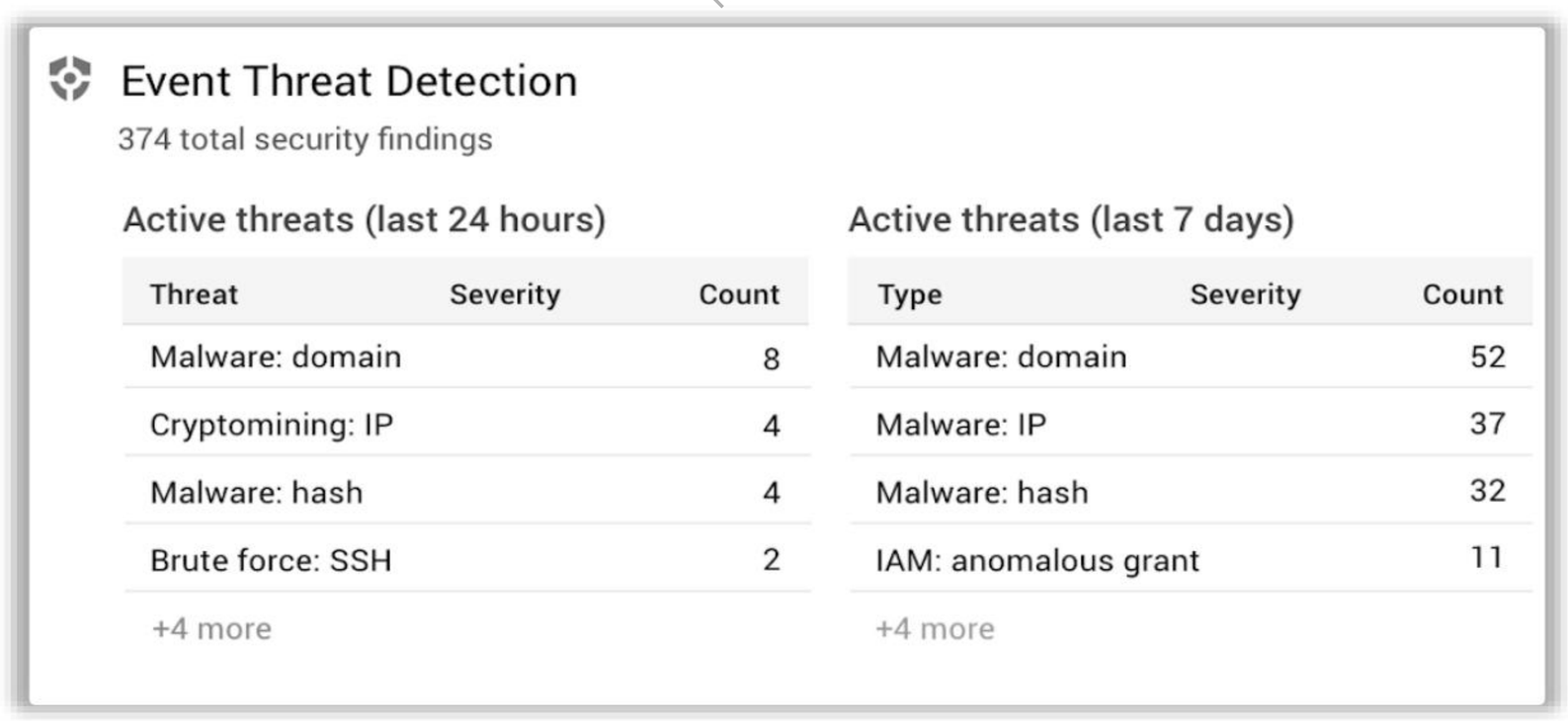
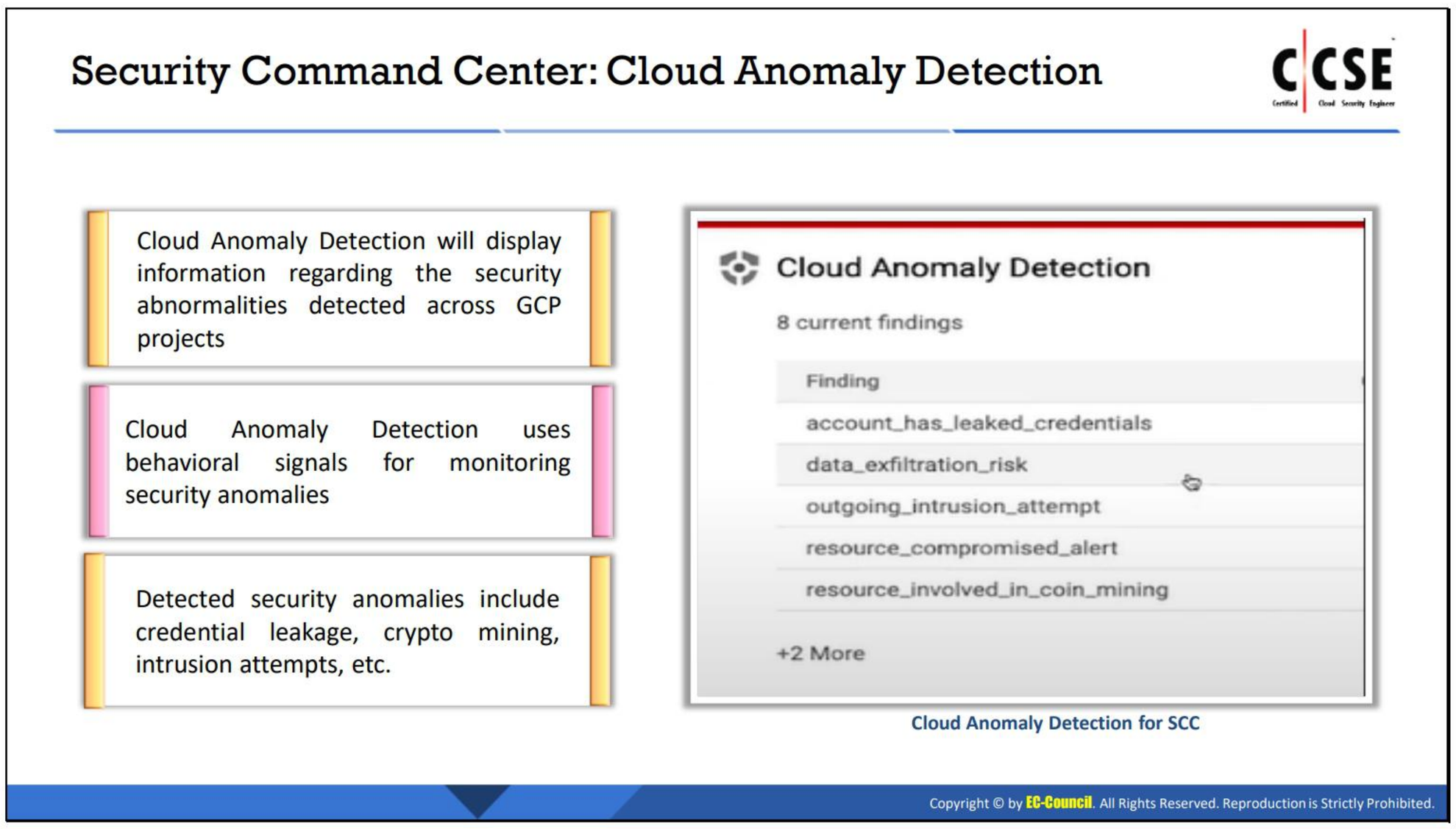


Figure 7.82: Event Threat Detection

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



Security Command Center: Cloud Anomaly Detection

Cloud Anomaly Detection, a built-in service in SCC, displays the information on security abnormalities detected across GCP projects. Security anomalies include credential leakage, crypto mining, intrusion attempts, etc.

hide01.ir

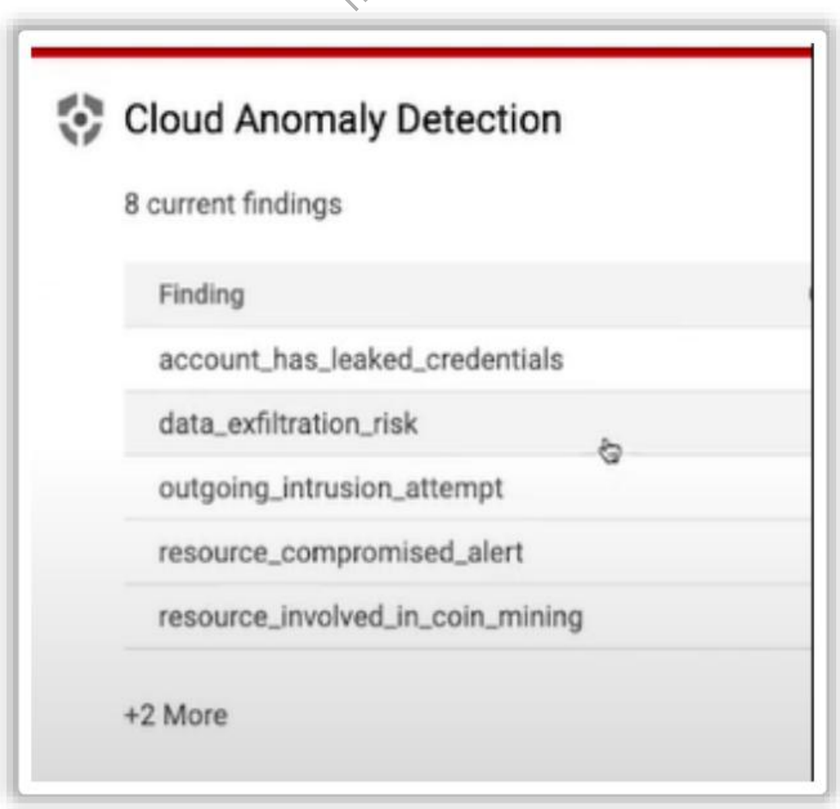
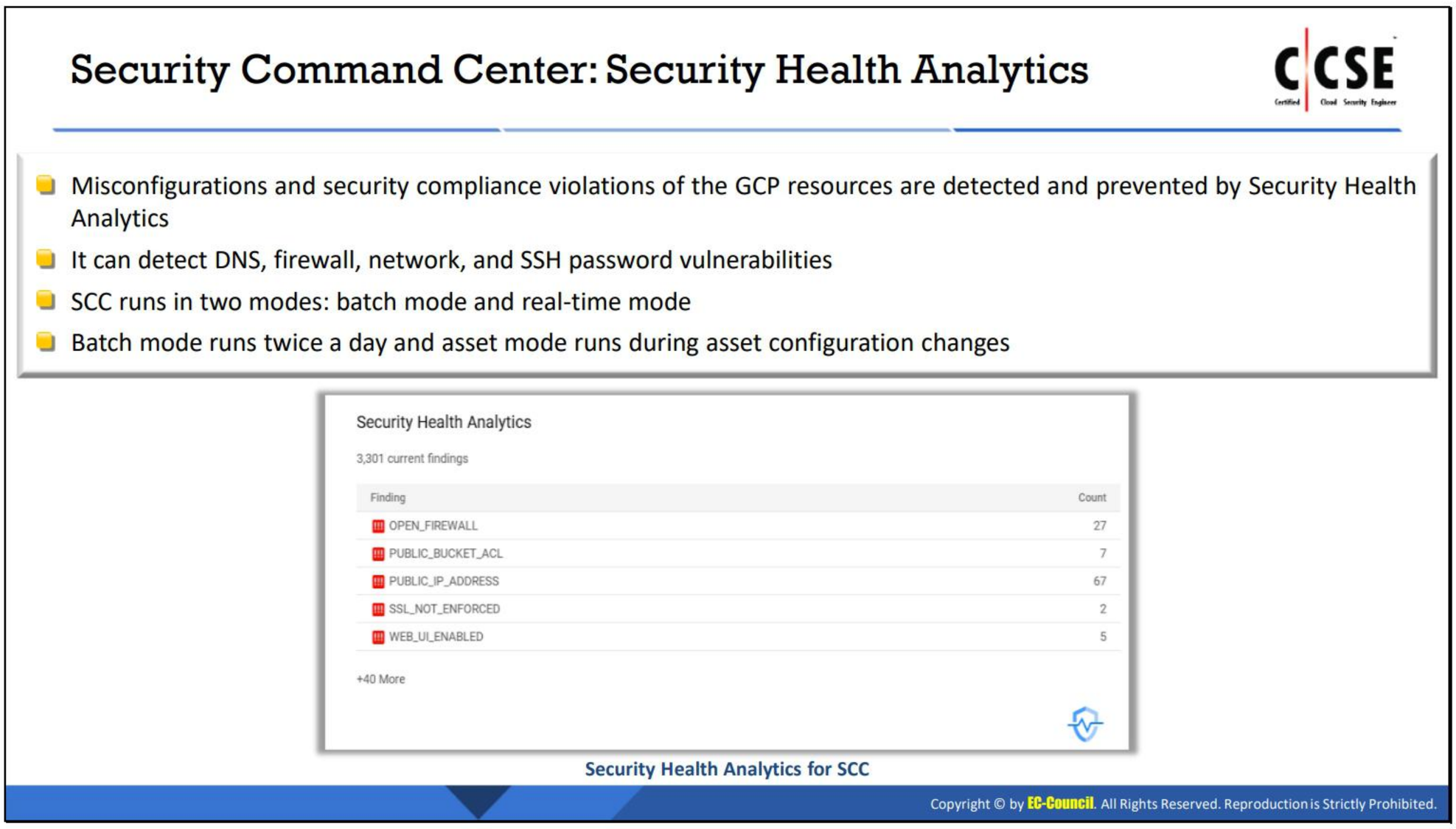


Figure 7.83: Cloud Anomaly Detection

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



Security Command Center: Security Health Analytics

Security Health Analytics in SCC uses Cloud audit logs for monitoring the infrastructure for specific security events. It can detect the following threats:

- User accounts without multi-factor authentication
- Container vulnerabilities
- DNS vulnerabilities
- Firewall vulnerabilities
- Network vulnerabilities
- SSH password vulnerabilities

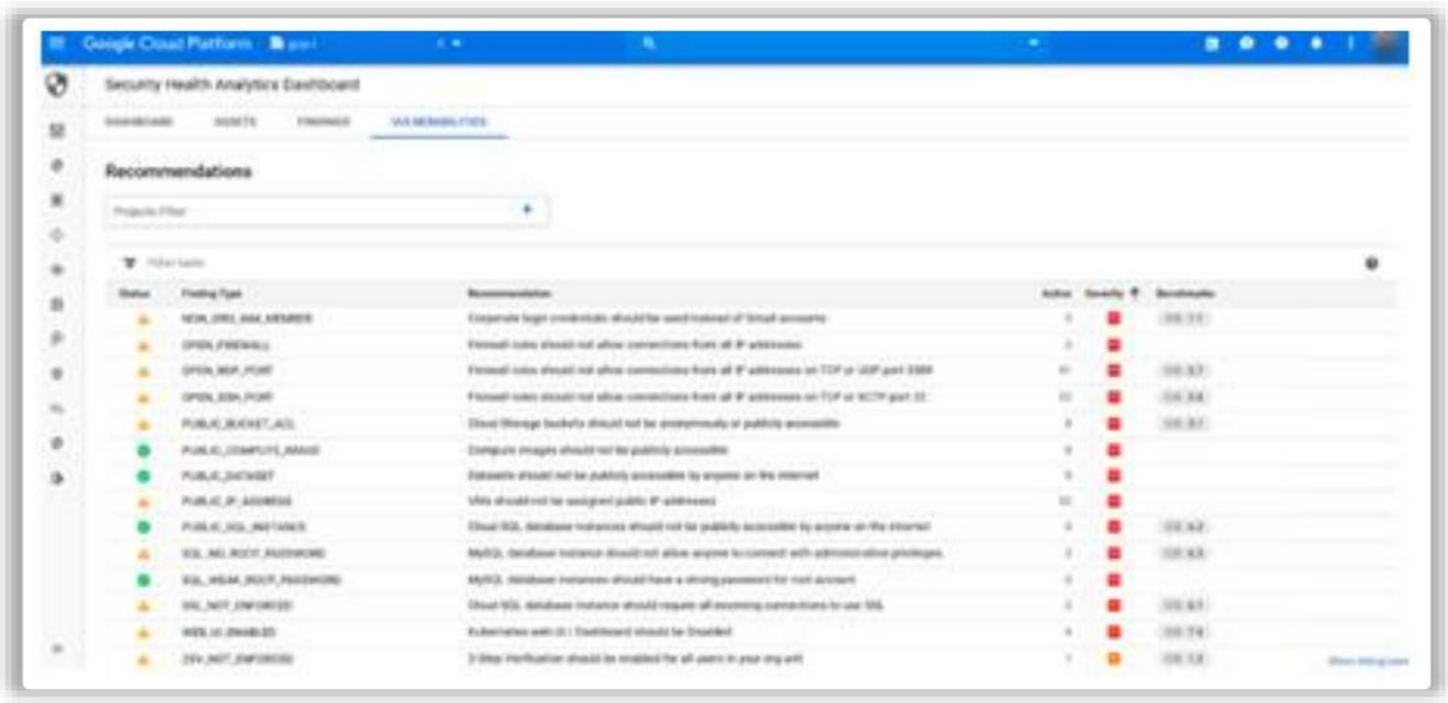


Figure 7.84: Security Threat Analytics

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

Security Command Center: Web Security Scanner

- Web Security Scanner can detect security vulnerabilities in the web applications hosted in GCP
- It eliminates false positives, and therefore, does not display low-confidence alerts
- It includes managed scans and custom scans
- Managed scans centrally manage vulnerability detection and custom scans can detect application vulnerabilities



Web Security Scanner for SCC

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

Security Command Center: Web Security Scanner

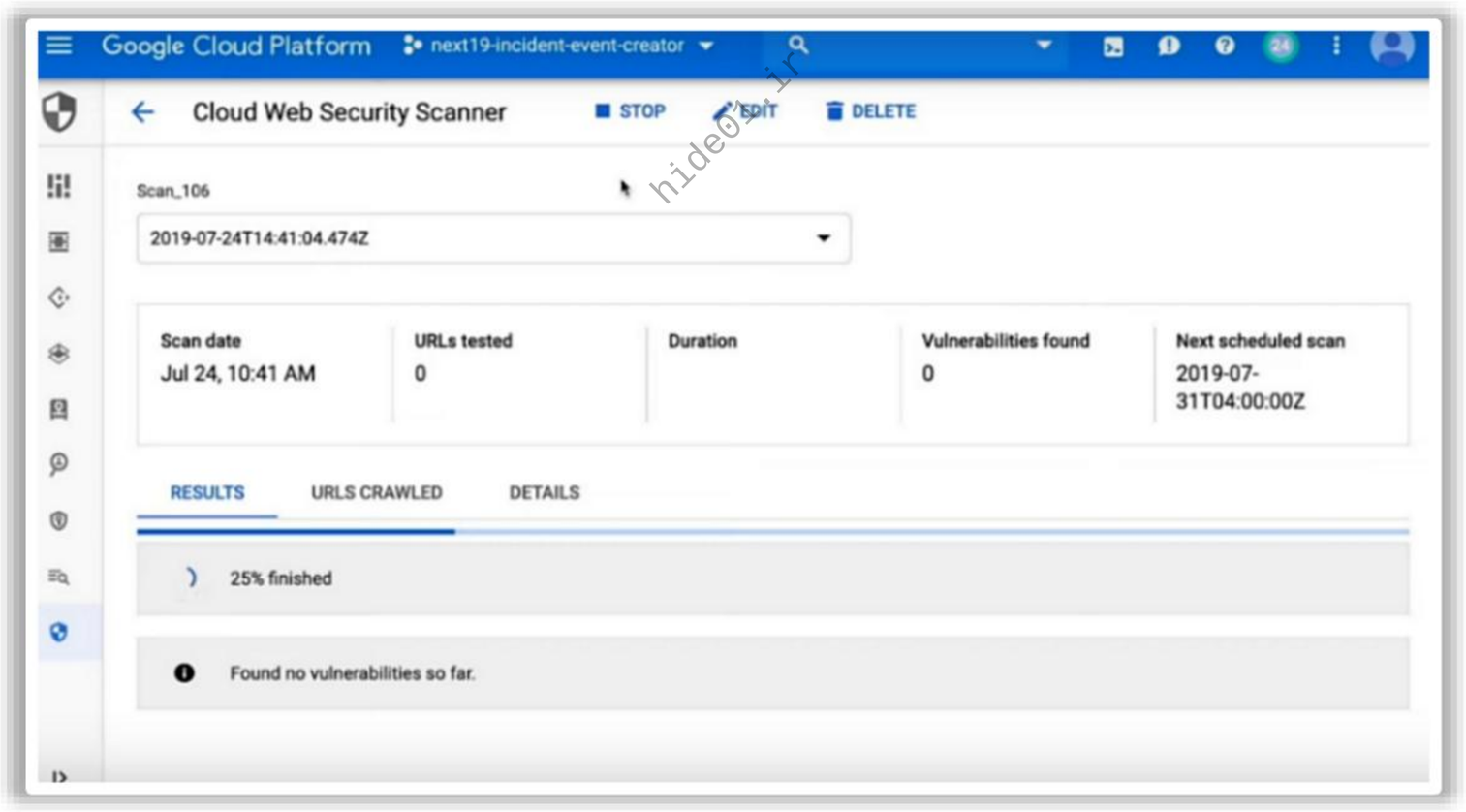


Figure 7.85: Web Security Scanner

Web Security Scanner can detect security vulnerabilities in the web applications hosted on various GCP platforms. It is quite efficient in threat detection as it does not display low-confidence alerts, which eliminates false positives. It includes managed scans and custom scans. Managed scans can centrally manage vulnerability detection in applications and custom scans can detect vulnerabilities such as XSS, outdated libraries, etc.

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

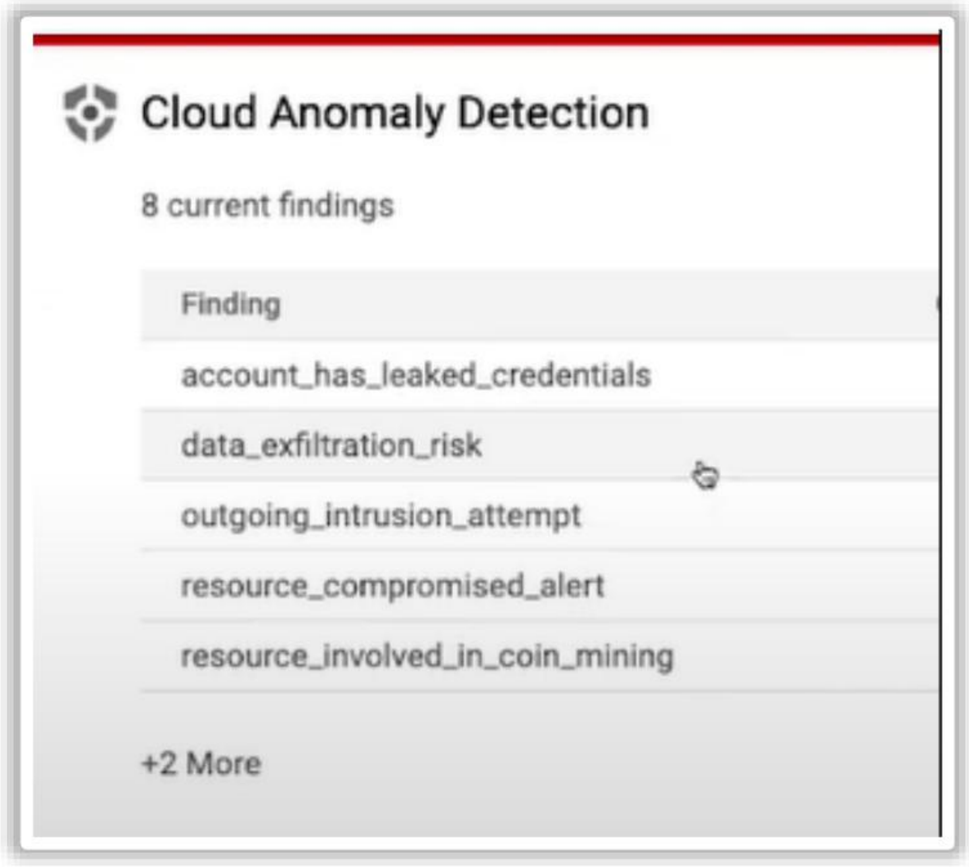


Figure 7.86: Cloud Anomaly Detection

- **Integration with Cloud Functions**

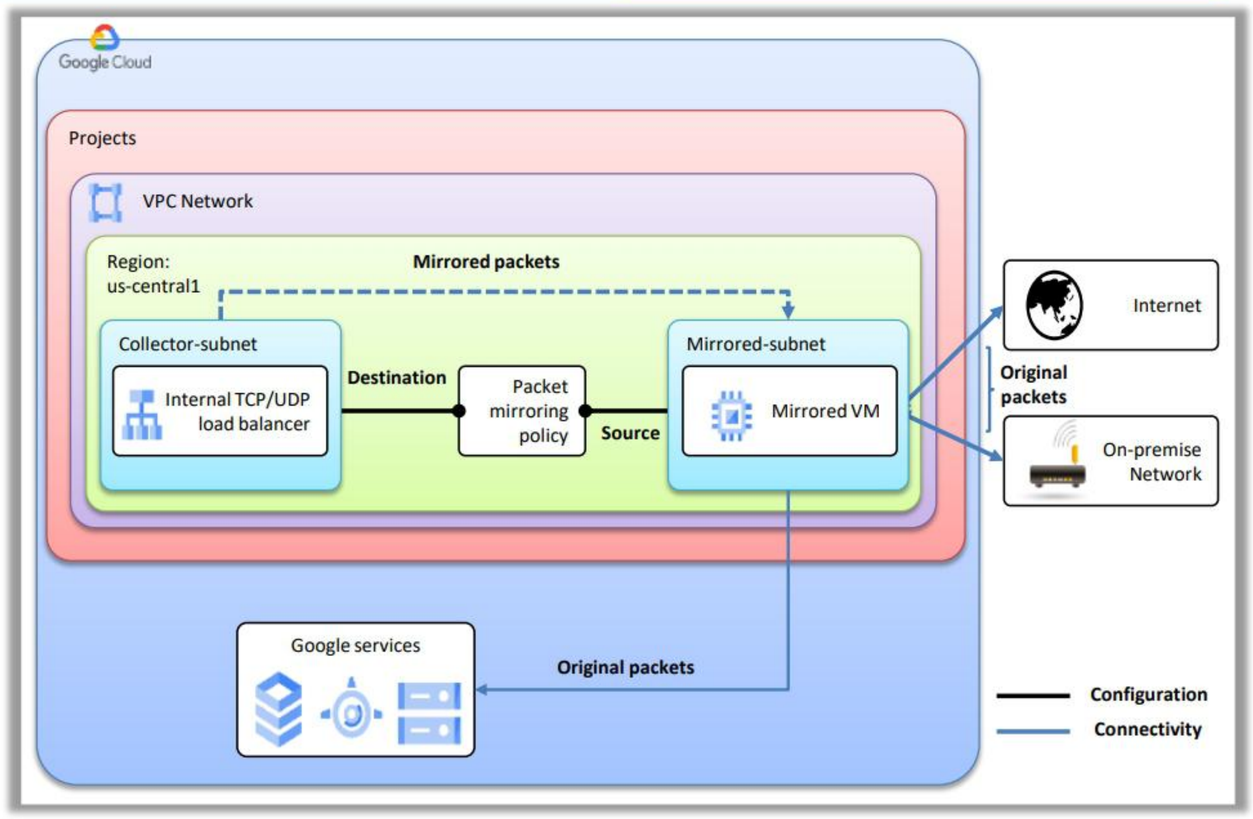
These are serverless functions that can be used for automated responses to the findings. The Cloud functions contain codes that helps in responding to pub/sub notifications provided by Event Threat Detection and Security Health in SCC. For automated actions against SCC findings, Google provides security response automation (SRA). The SRA actions for an automated response to SCC findings are as follows:

- For performing a forensic analysis, disk snapshots are created.
- IAM grants that violate the configured policies are revoked, and non-organization members are removed.
- All public IPs are removed from the network interface.
- SQL instances are updated to ensure SSL connections.

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

Packet Mirroring

- Packet Mirroring captures the network traffic packets so that they can be used for examining vulnerabilities
- Packet capture can be configured for both inbound and outbound network traffic
- The two main components of the packet mirroring policy are collector destinations and mirrored sources
- Mirrored sources are the compute engine VM instances and collector destinations are the instance groups behind an internal load balancer



Packet Mirroring workflow

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

Packet Mirroring

Packet Mirroring captures the network traffic packets so that they can be used for examining vulnerabilities. Packet capture can be configured for both inbound and outbound network traffic.

The traffic from the mirrored sources is copied to the collector destination by the Packet Mirroring service. A packet mirroring policy must be created to configure Packet Mirroring. The created policy should specify a source and destination. For an internal load balancer, a forwarding rule must be created for Packet Mirroring. The non-mirrored traffic sent to the internal load balancer is dropped. The mirrored traffic can be used to detect any vulnerabilities or security threats in an application.

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

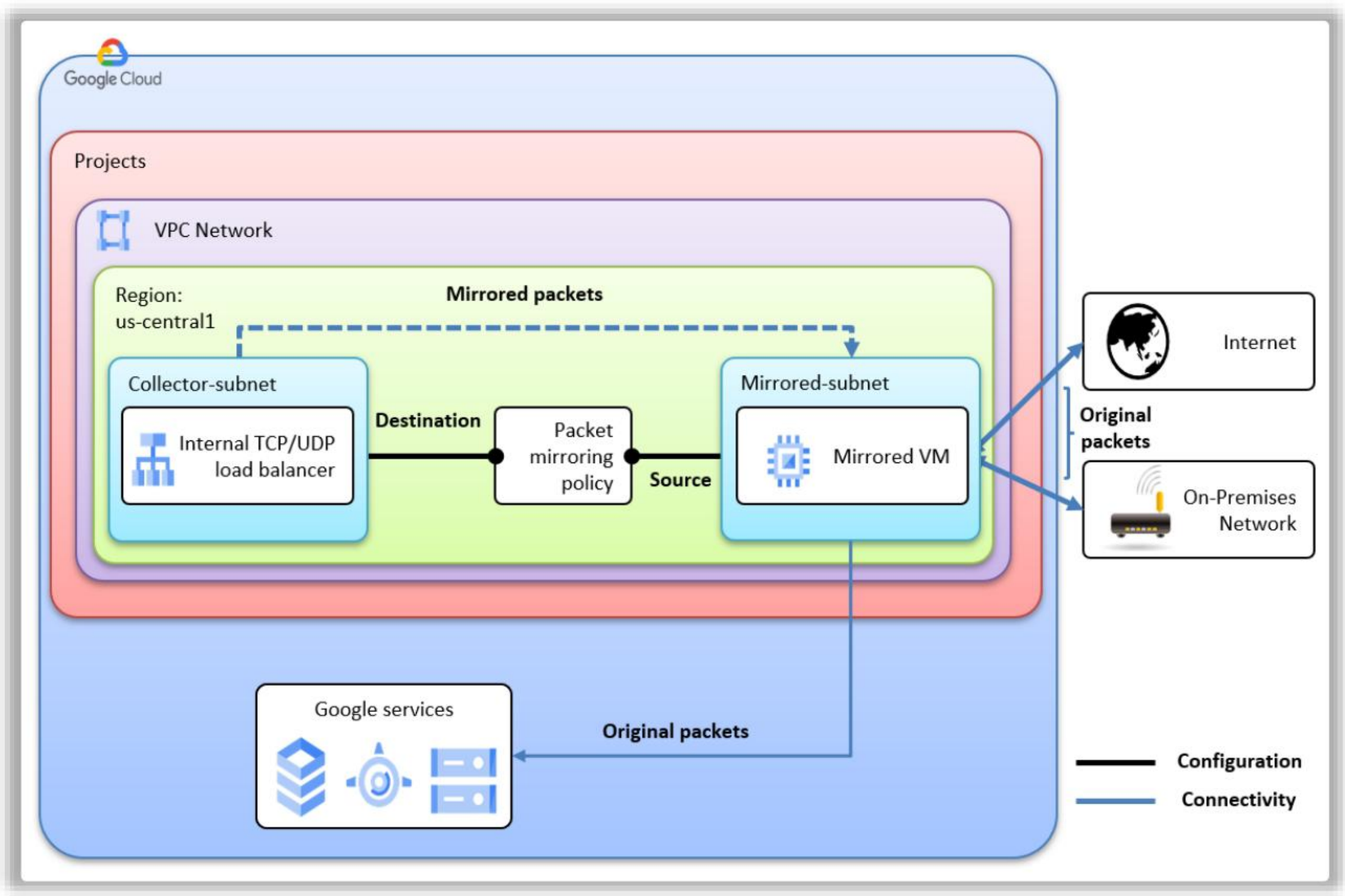


Figure 7.87: Packet Mirroring Workflow

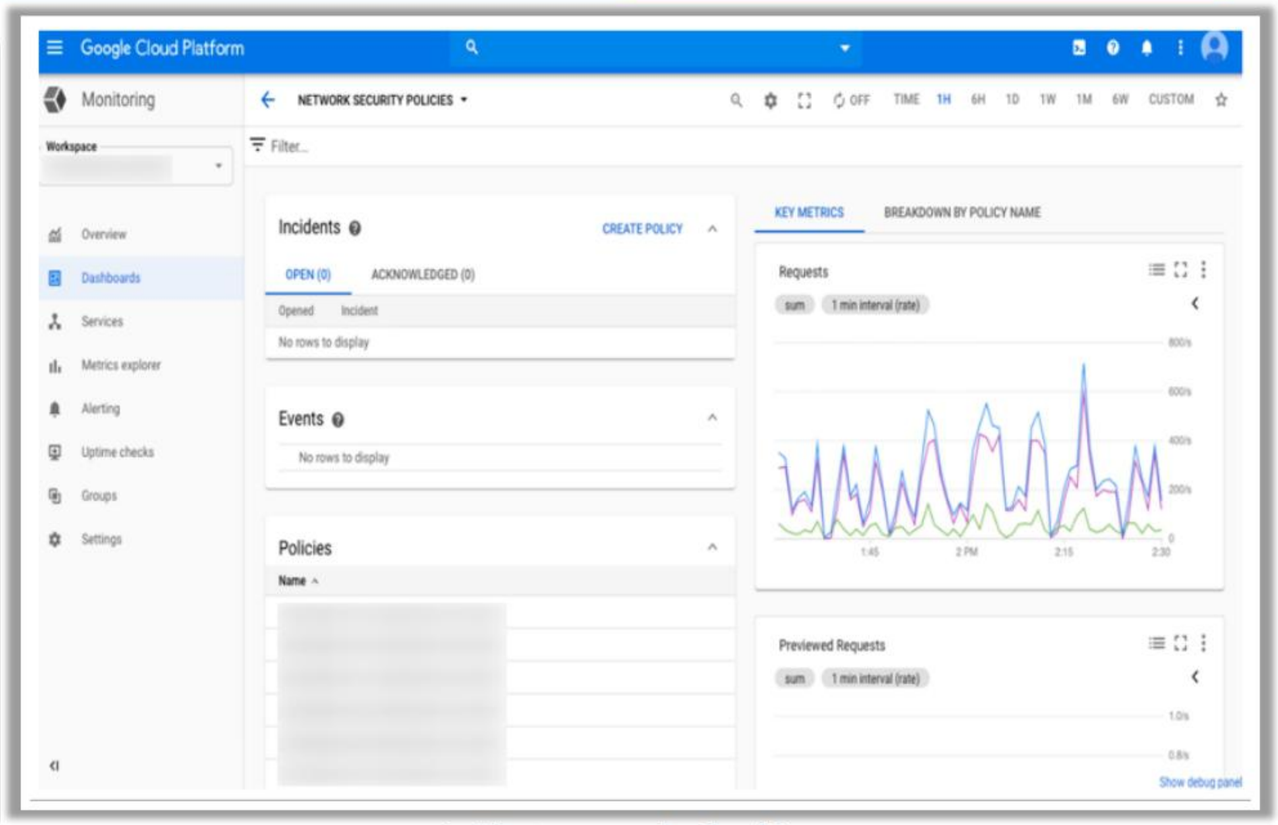
Packet mirroring policy has mirrored sources and collector destinations. Mirrored sources are compute engine VM instances, and collector destinations are instance groups behind the internal load balancer.

hide01.ir

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

Automated Application Incident Response by Cloud Armor

- Cloud Armor has automated features for detecting and preventing DDOS attacks and other OWASP vulnerabilities
- The incoming web requests are filtered by Cloud Armor based on their IP or location
- In Cloud Armor, security policies can be configured to filter the incoming traffic based on IP address, IP range, etc.
- Cloud Armor findings of allowed traffic spike and increasing deny ratio are exported to the SCC



Incident response by Cloud Armor

Source: https://cloud.google.com

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

Automated Application Incident Response by Cloud Armor

Google Cloud Armor is equipped with automated features and manual configurations to detect and prevent DDoS attacks and other Top-10 OWASP risks on the application.

hide01.ir

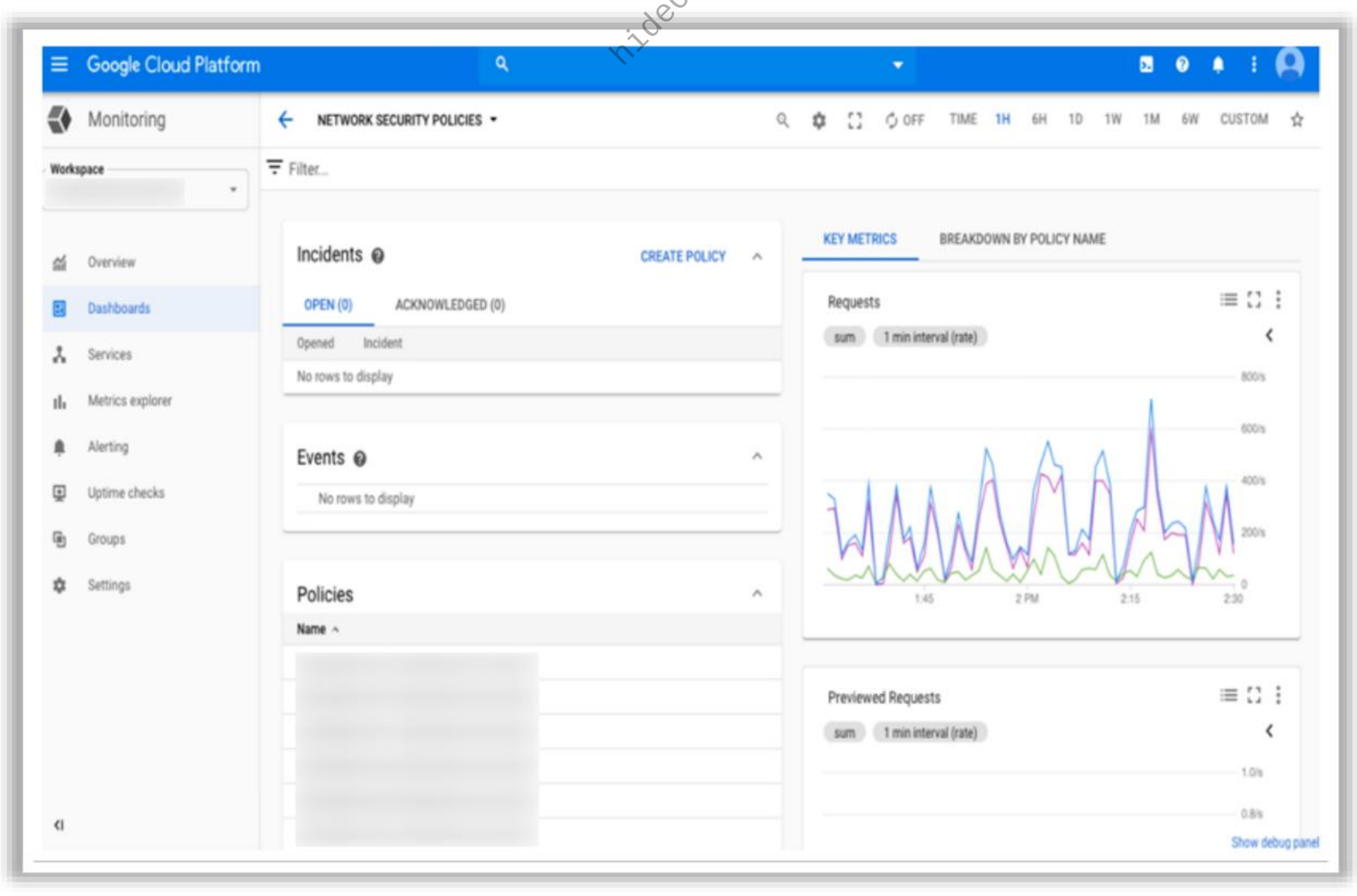


Figure 7.88: Incident Response by Cloud Armor

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

Some features of Cloud Armor that help in threat detection are

- **Access Control Based on IP Address and Geographic Location:** The incoming requests can be filtered, and then access can be granted based on IPv4 and IPv6 address or classless inter-domain routings (CIDRs) and the geographic location.
- **Named IP Lists:** The incoming network traffic can be allowed or denied based on a group of IP addresses under different names.
- **Security Policies:** The applications deployed in GCP can be protected from DDoS attacks by configuring security policies. The security policies contain a group of rules to filter the incoming traffic based on IP address, IP range, or request header. The rules contain a match condition and a corresponding action when the condition is met. An incoming request is then allowed or denied based on the rule.
    - **Rule Evaluation Order**: Rule priority is considered as the benchmark for determining the rule evaluation order. The rule with highest logical priorities has numerically low values and is evaluated first.
    - **Default Rule**: The Google Cloud Armor default rule is matched if there are no defined rules or none of the defined rules match.
    - Type of rules:
        - **IP Address Allow List and Deny List Rules**: The IP address allow list and deny list rules can be specified within a security policy, such as allowing/denying access to external load balancers based on a source IP address.
        - **Preconfigured Rules for Mitigating Certain Attacks**: Preconfigured rules can be used to mitigate XSS, SQL injection, local file inclusion (LFI), remote file inclusion (RFI), and remote code execution (RCE) attacks.
- **Preconfigured WAF Rules:** The predefined web application firewall rules of Cloud Armor contain signatures of known attacks and the incoming requests are evaluated with the preconfigured rules. An incoming request matches a preconfigured rule if any signature in the preconfigured rule matches the incoming request.
- **Integration with SCC:** Google Cloud Armor is integrated with SCC. The allowed traffic spike and increasing deny ratio findings are exported to SCC.
- **Allowed Traffic Spike:** Allowed traffic is the configured requests reaching the backend after configuring a security policy. When there is a sudden increase in the number of requests per second (RPS) in comparison to a normal traffic, an RPS finding is generated. An allowed traffic spike identifies the backend at which the spike occurred and why Cloud Armor detected it as a traffic spike. These traffic spikes can detect DDoS attacks and suggest preventive measures to mitigate them.

hidoi.ir

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

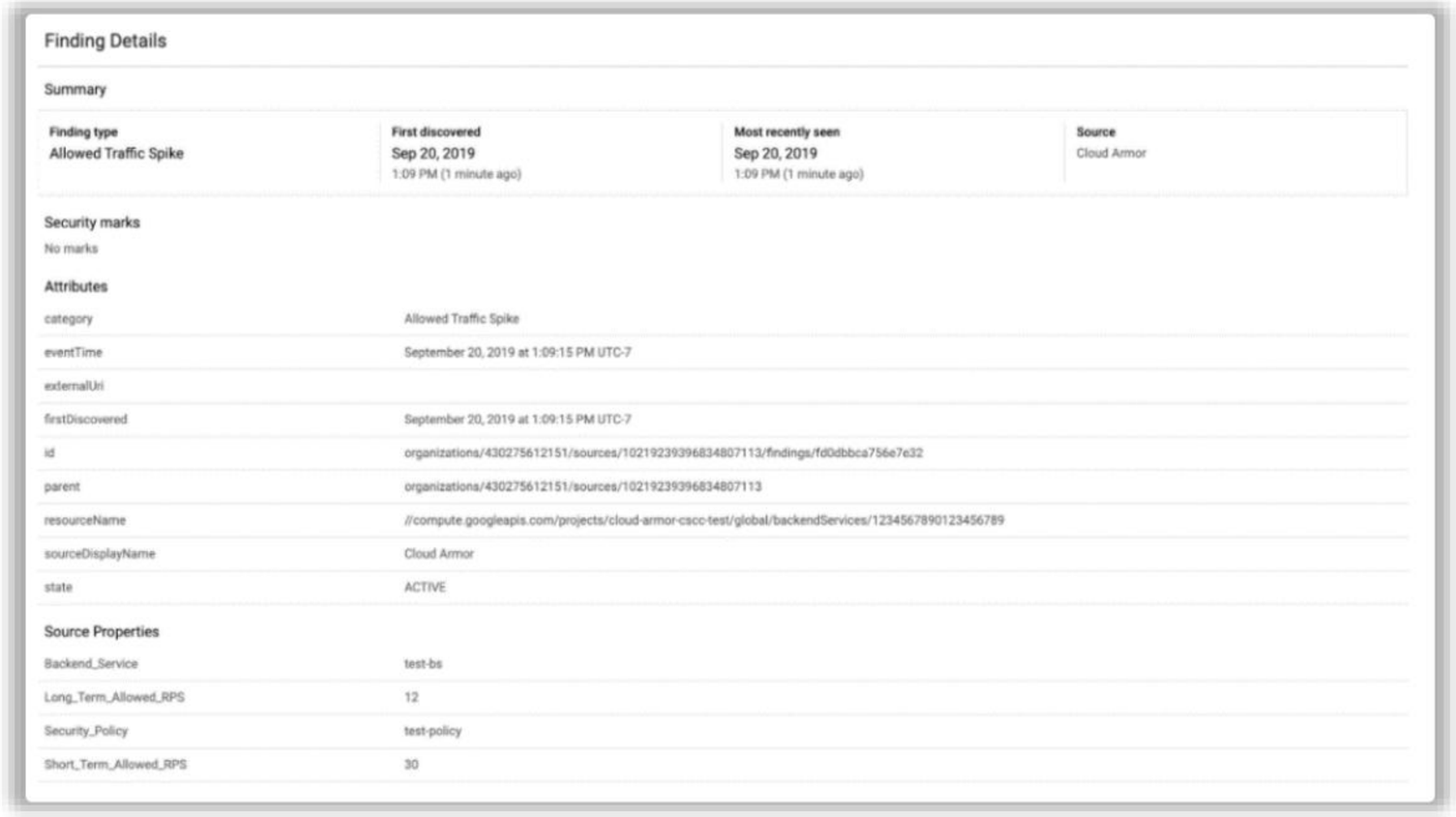
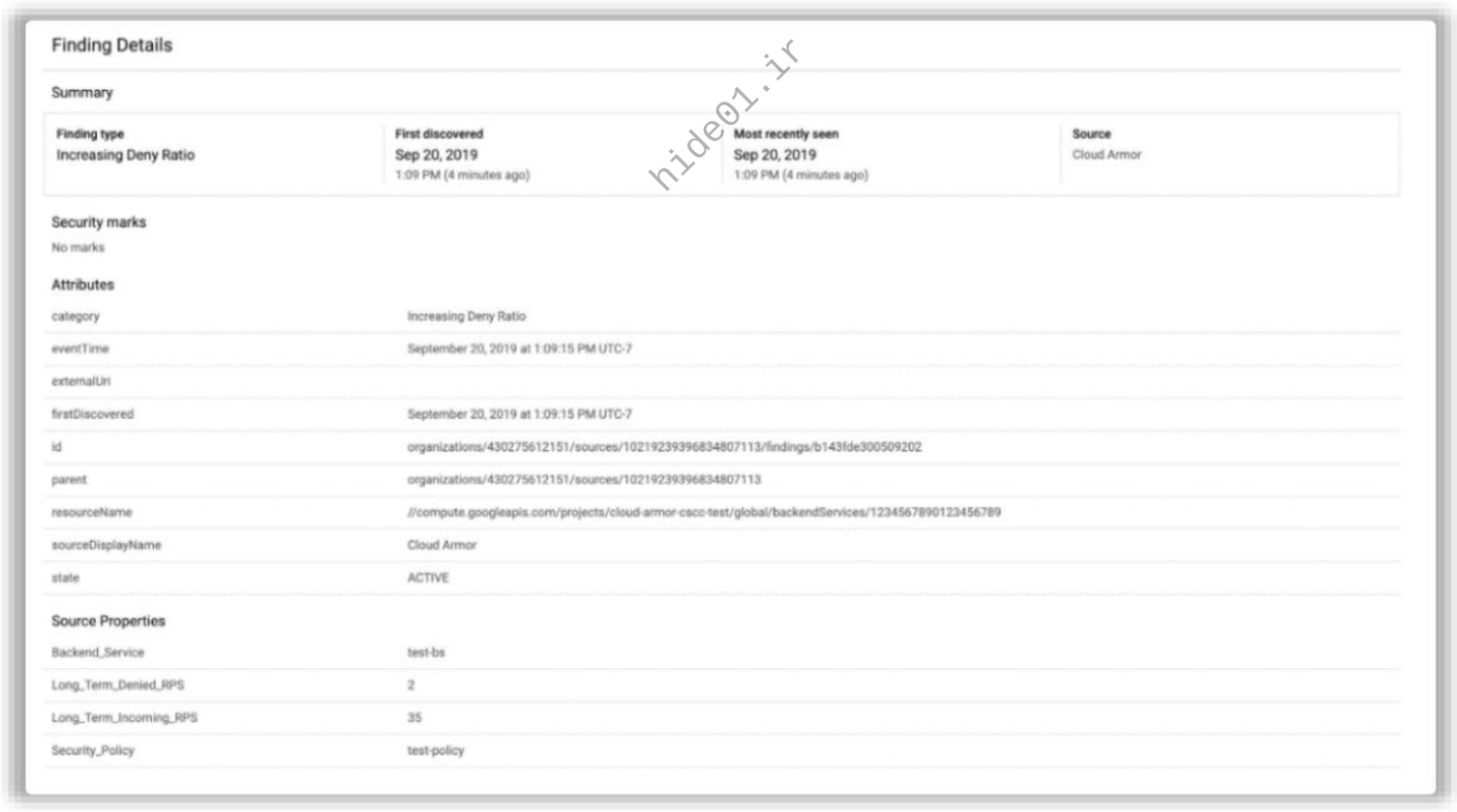


Figure 7.89: Finding Details

- **Increasing Deny Ratio:** The increasing deny ratio will notify the traffic ratio that gets blocked because of a user-configured rule in the security policy. This finding can be used to detect abnormal traffic. The request per second (RPS) and the incoming traffic are also included with the finding.



hide01.ir

Figure 7.90: Increasing Deny Ratio

Steps to Set Up Cloud Armor

- **Step 1: Set up Google Cloud Armor**
  - Open **Google Cloud Console**, go to **Network Security,** and click on **Cloud Armor.**

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

- Click **Create Policy.**

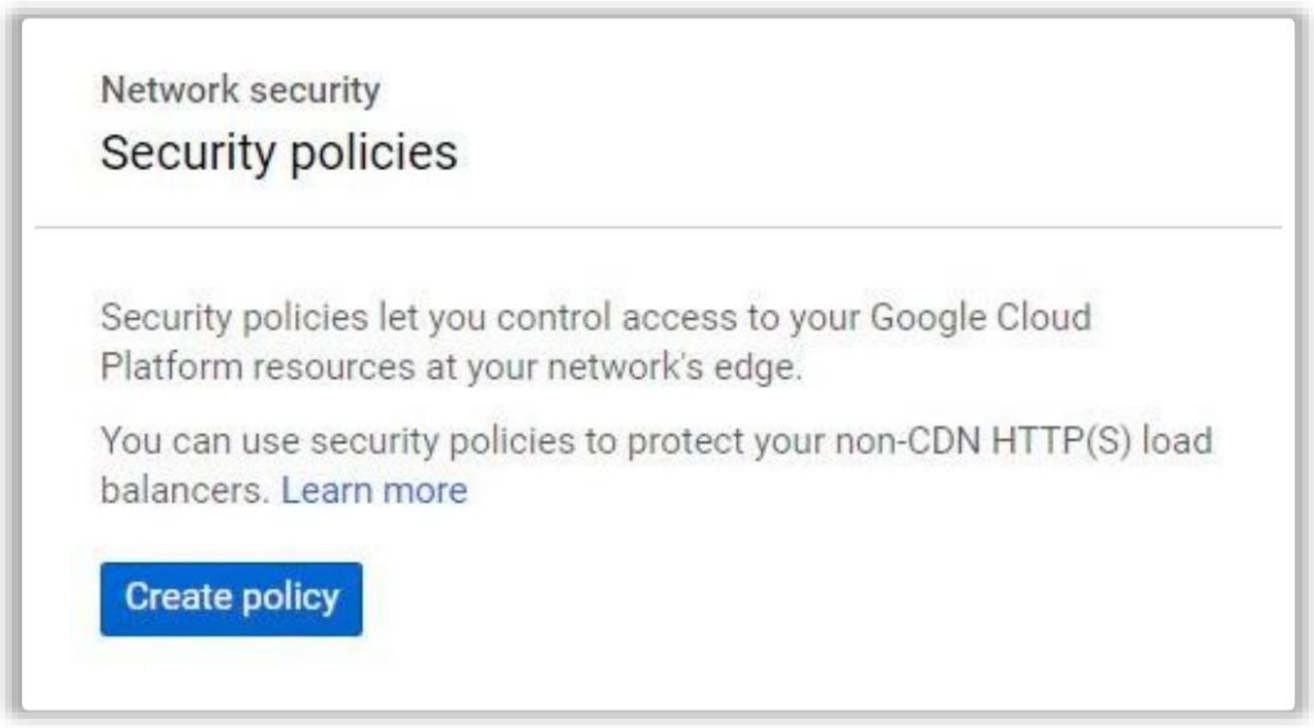


Figure 7.91: Creating a Policy

- **Step 2: Create Cloud Armor Security Policy**
  - In the name field, type the name of the policy.
  - Type a description of the policy.
  - Select **Allow** or **Deny** for the **Default Rule Action.**

  (Note: If a deny rule is being created, choose Deny)
  - Click **Next Step.**

hide01.ir

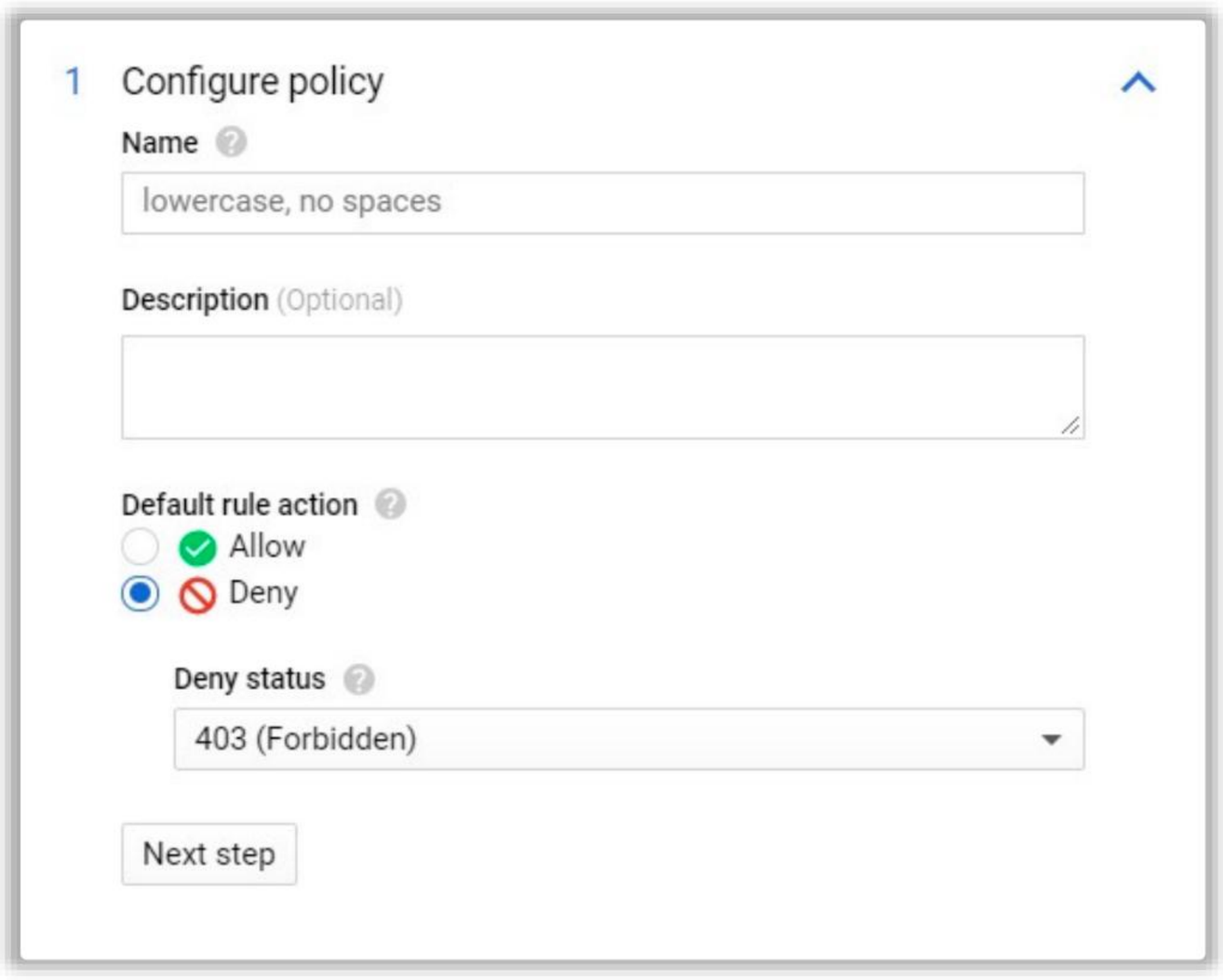


Figure 7.92: Filling Details of a Policy

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

- **Adding More Rules**
  - Type a description of the rule.
  - In the **Match** field, type 1–5 IP address ranges to match the rule.
  - Depending on the rule, choose **Allow** or **Deny.**
  - To enable the rule, click the **Enable** checkbox.
  - Give priority to the rule in the **Priority** field.
  - Click **Done.**
  - If more rules are to be added, Click **Add Rule.**
  - Click **Next Step.**

- **Step 3: Apply Policy to Targets**

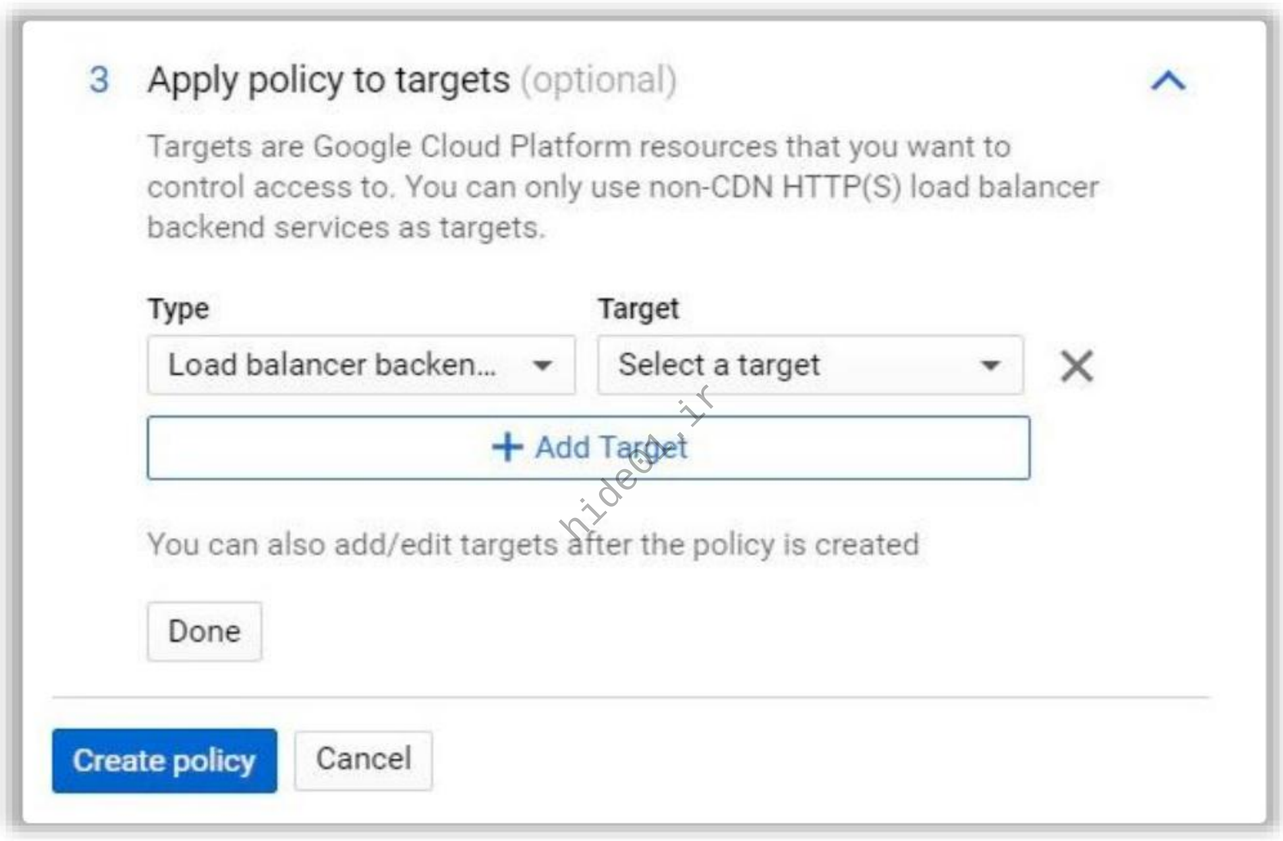
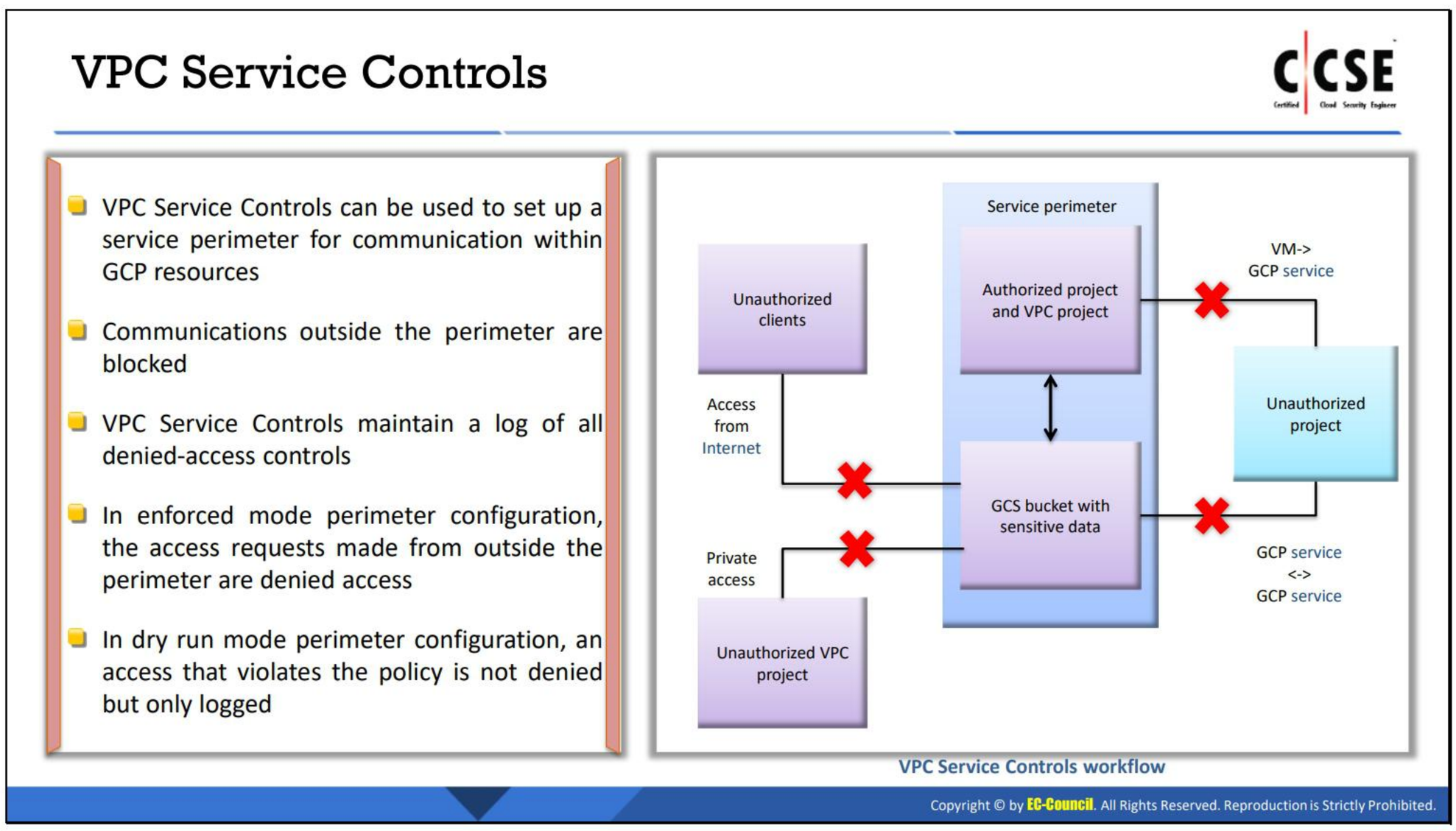


Figure 7.93: Applying Policy

- Click on **Add Target**
- From the drop-down, select a target.
- Click **Add Target** if more targets need to be added.
- Click **Done,** and then click **Create Policy.**

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



VPC Service Controls

VPC Service Controls can be used to set up a service perimeter for communications within GCP resources. The communications outside this perimeter are blocked. These controls help prevent data exfiltration from GC services such as BigQuery and Cloud Storage. They offer an additional layer of defense that is not dependent on IAM. VPC Service Controls maintains a log of all denied access controls. In the enforced mode perimeter configuration, the access requests made from outside the perimeter are denied. In the dry run mode perimeter configuration, an access that violates the policy is not denied but only logged. It is recommended to use both IAM and VPC Service Controls for a better security.

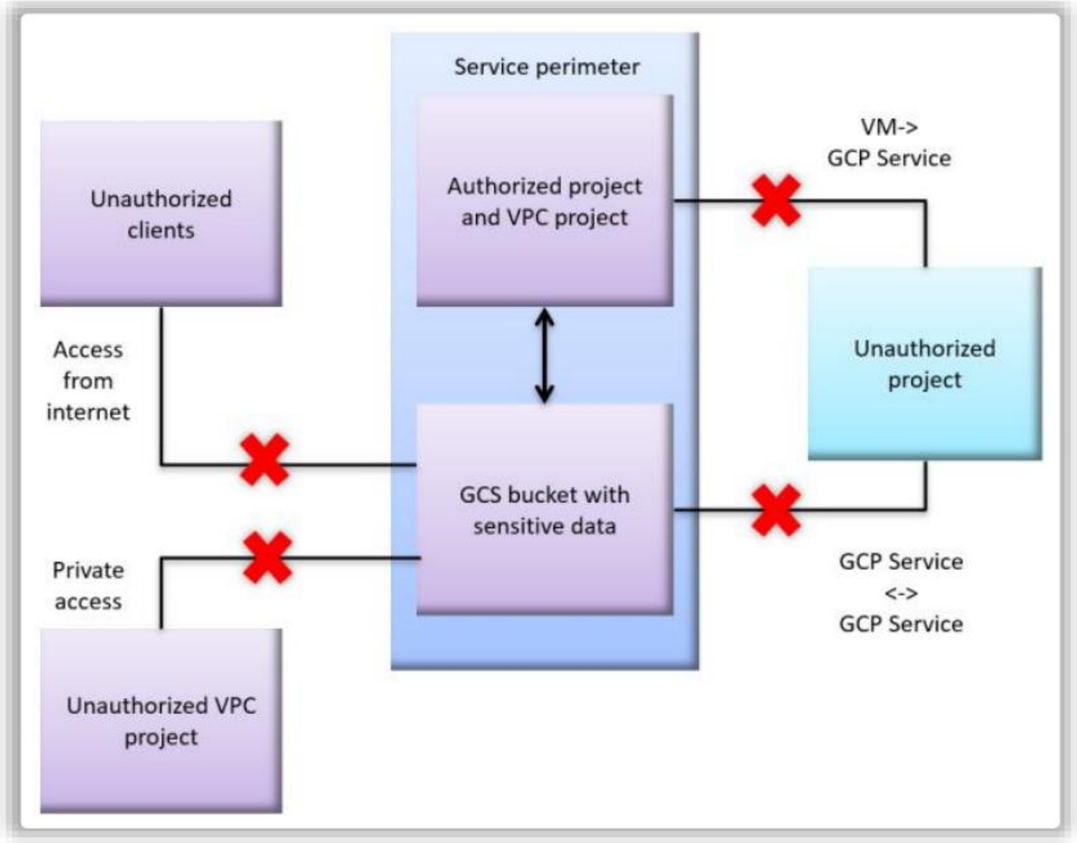
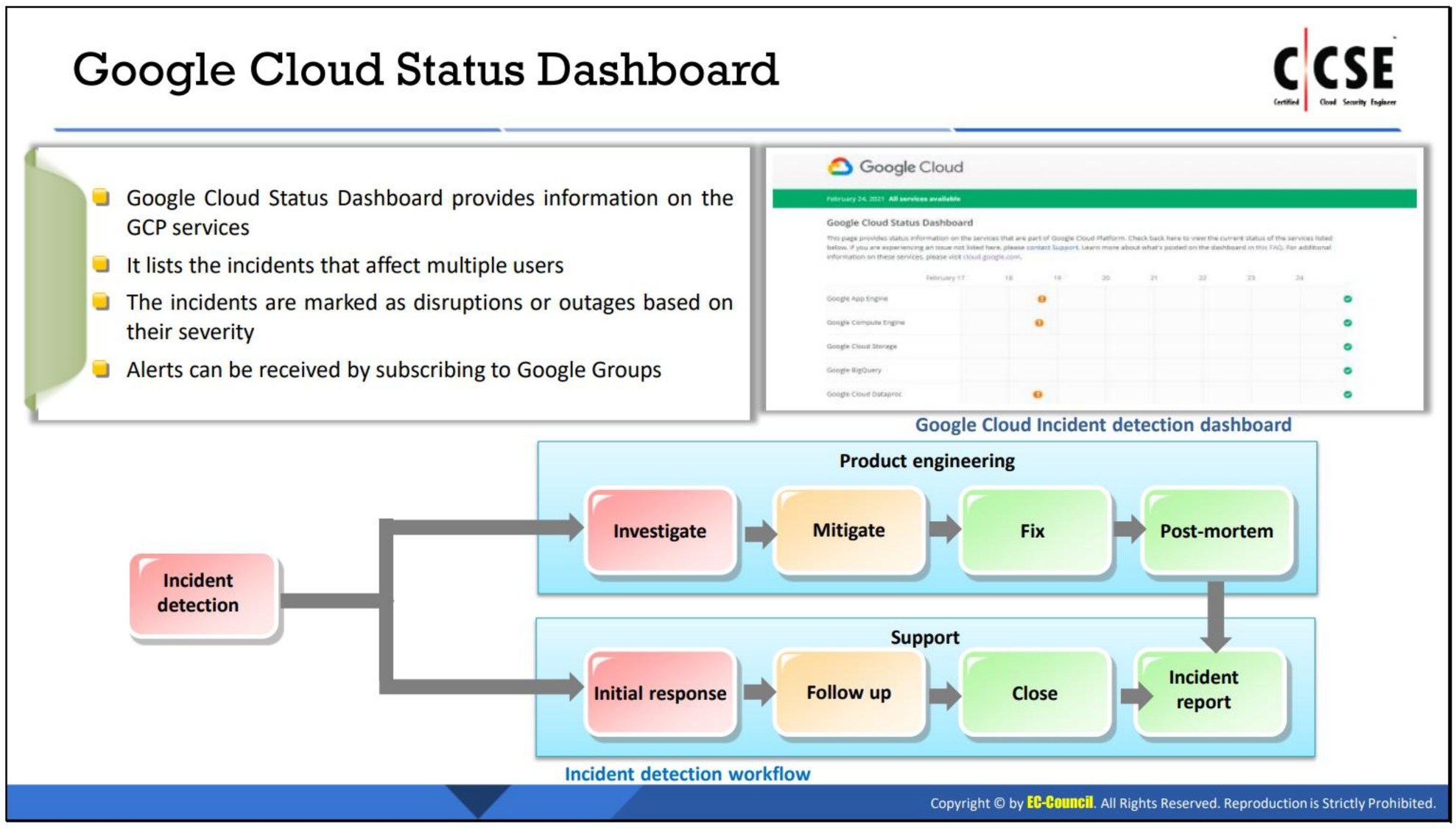


Figure 7.94: VPC Service Controls Workflow

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



Google Cloud Status Dashboard

- **Google Cloud Status Dashboard**

  Information on the GCP services is included in the Cloud Status Dashboard. In the case of any service availability issues, the administrators must check the Cloud Status Dashboard. The dashboard lists incidents that affect multiple users. The incidents are marked as a disruption or an outage based on their severity. The alerts on the Google Cloud Status Dashboard incidents can be received by subscribing to the Google Groups associated with certain services.

- **Life Cycle of an Incident**

  - **Incident Detection**

    Google uses internal detection and black box monitoring of external behavior to detect incidents.

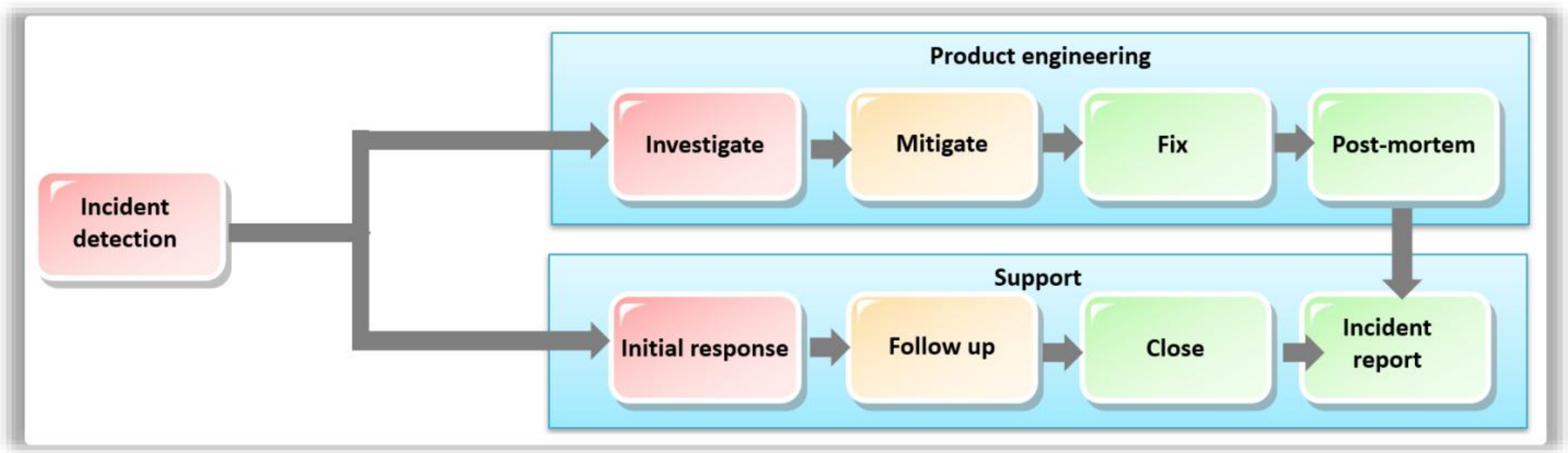


Figure 7.95: Incident Detection Workflow

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

- **Initial Response**

  The Google customer care team communicates with the customer if an incident is detected.

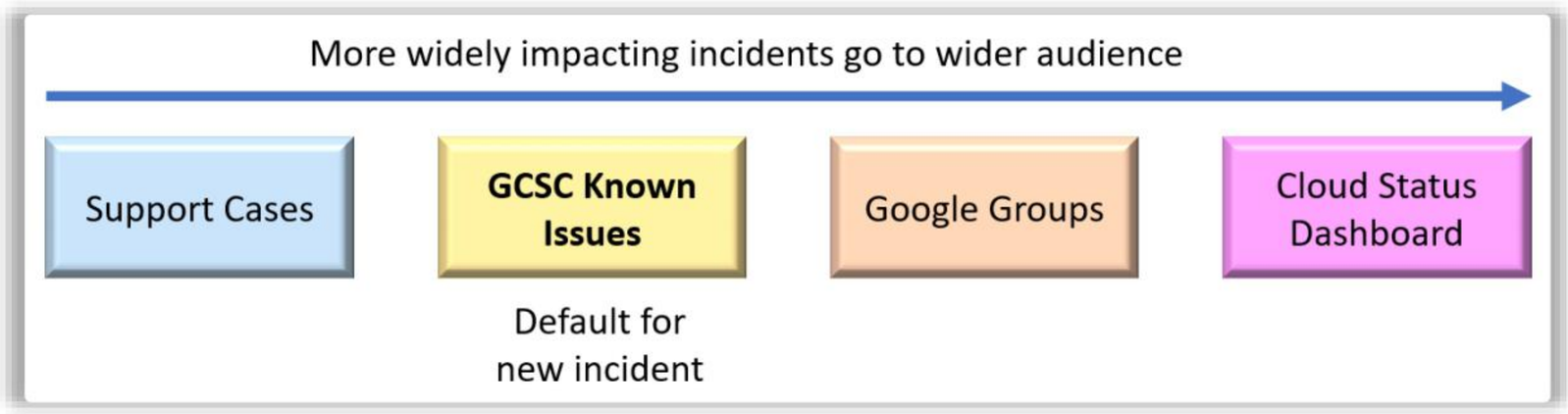


Figure 7.96: Initial Response

When an incident is detected, the user must use the Cloud Status Dashboard to check whether it affects several users. They may be marked as outages or disruptions based on their severity. The Google Cloud Support Center and the Cloud Console Support page display only the information about issues that may not be a major incident or affect only a few, otherwise classified as known issues.

- **Investigation**

  Site reliability engineers will perform the incident management and the actual cause of an incident will be investigated by the product engineering teams.

- **Mitigation/Fix**

  An incident is fixed if its impact ends after a particular time or duration and its mitigation reduces the impact of any potential incident. If a mitigation is not possible, the Google team communicates workarounds, which are the procedures a user can adapt to meet the underlying needs.

- **Follow Up**

  The customer care team provides continuous updates for the ongoing incidents. These updates include

  - Other details of the incident, such as the impact and the affected regions
  - Workarounds
  - The status of an incident

- **Post-mortem**

  A post-mortem or forensic analysis can be done on the incidents to study the possible improvements for preventing such an issue in the future.

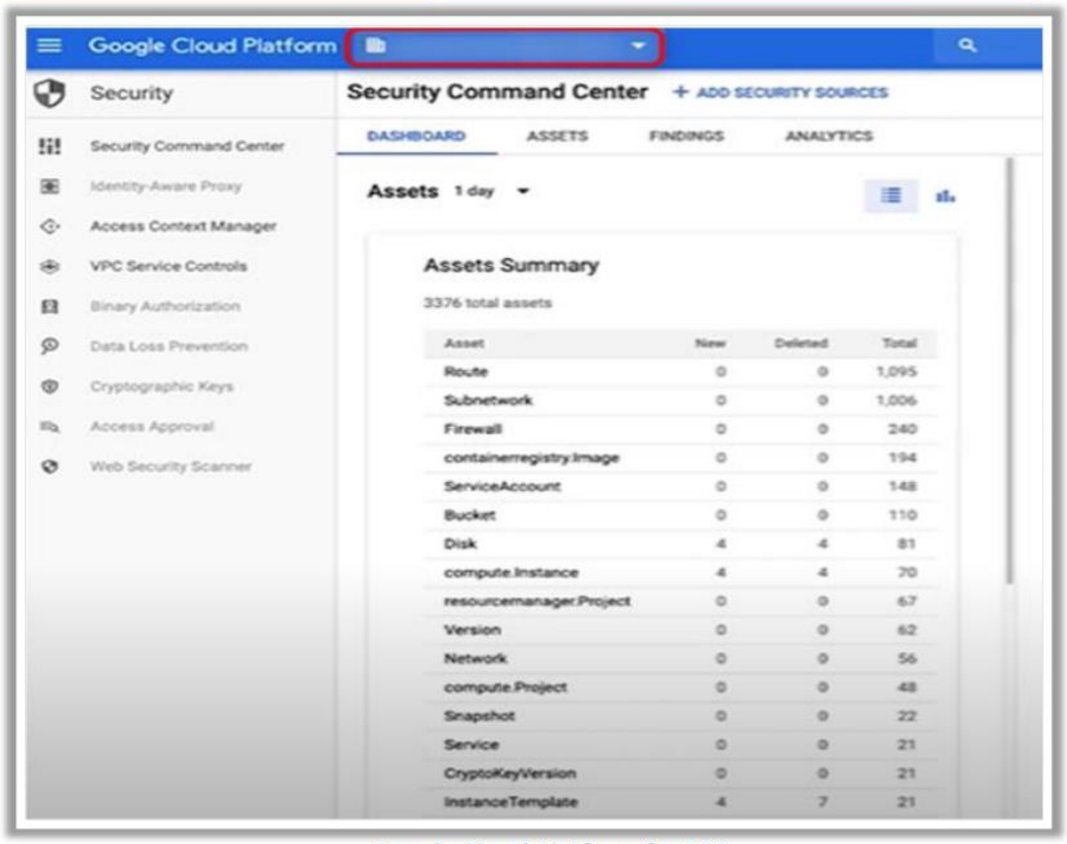
- **Incident Report**

  Google provides incident reports, which explains the reason, remediation, and prevention of such major incidents.

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

Prevent, Detect, and Respond to Threats with Security Command Center Dashboard

- Cloud Security Command Center (SCC) provides an analytic dashboard summarizing resources that helps prevent, identify, and respond to threats in a Google Cloud environment
- SCC provides real-time alerts for vulnerabilities and threats along with remediation measures
- Cloud SCC can be used only by a user with a security center IAM role
- The security state of the organization can be monitored for a specified time, along with the assets that have changed over time



Google Cloud Platform for SCC

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

Prevent, Detect, and Respond to Threats with Security Command Center Dashboard

Security Command Center (SCC) is a security and risk management platform that provides dashboard-based analytics for detecting and responding to security risks in GCP. In GCP SCC, assets are a systematic view of the threats and attacks to the GCP infrastructure. Findings are the possible security vulnerabilities in the infrastructure collected by the security detection services. SCC provides a unified dashboard to prevent, identify, and respond to threats in a Google Cloud environment. It provides real-time alerts for vulnerabilities and threats along with their remediation measures. It can be used only by a user with a security center IAM role. It helps in monitoring the organization's security state for a specified time and the assets that have changed over time.

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

Steps to Prevent, Detect, and Respond to Threats with SCC Dashboard

- **Step 1: Configure Cloud IAM permissions**
  - Navigate to **IAM & Admin** and select **IAM** in the console.

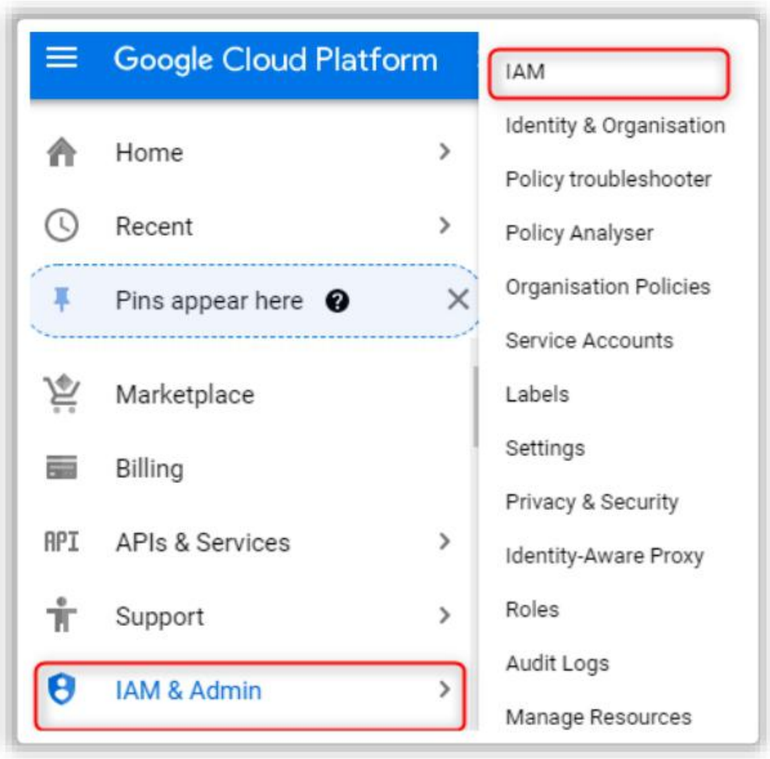


Figure 7.97: Navigating to IAM and Admin

  - Click on **Add** in the **IAM** page.

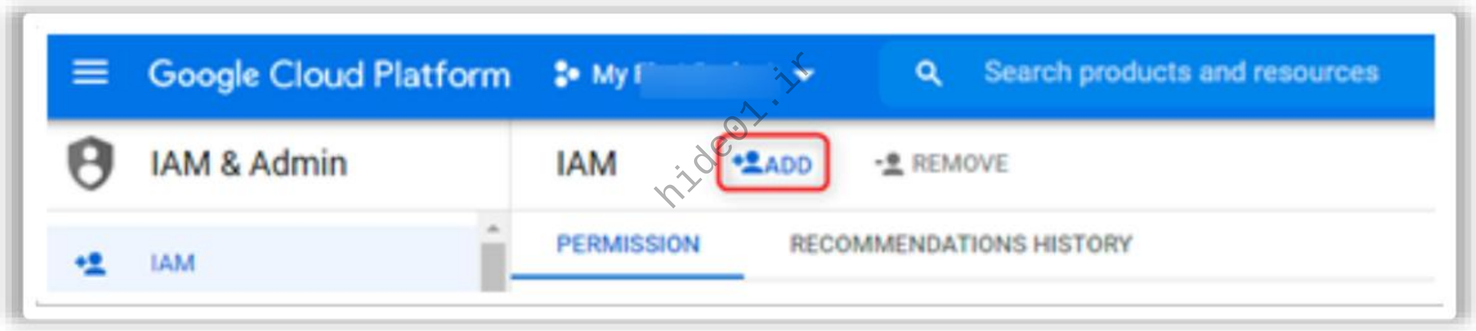


Figure 7.98: Adding Permissions

  - In the **Role** field for access to administer all resources belonging to the organization, select **Organization Administrator.**

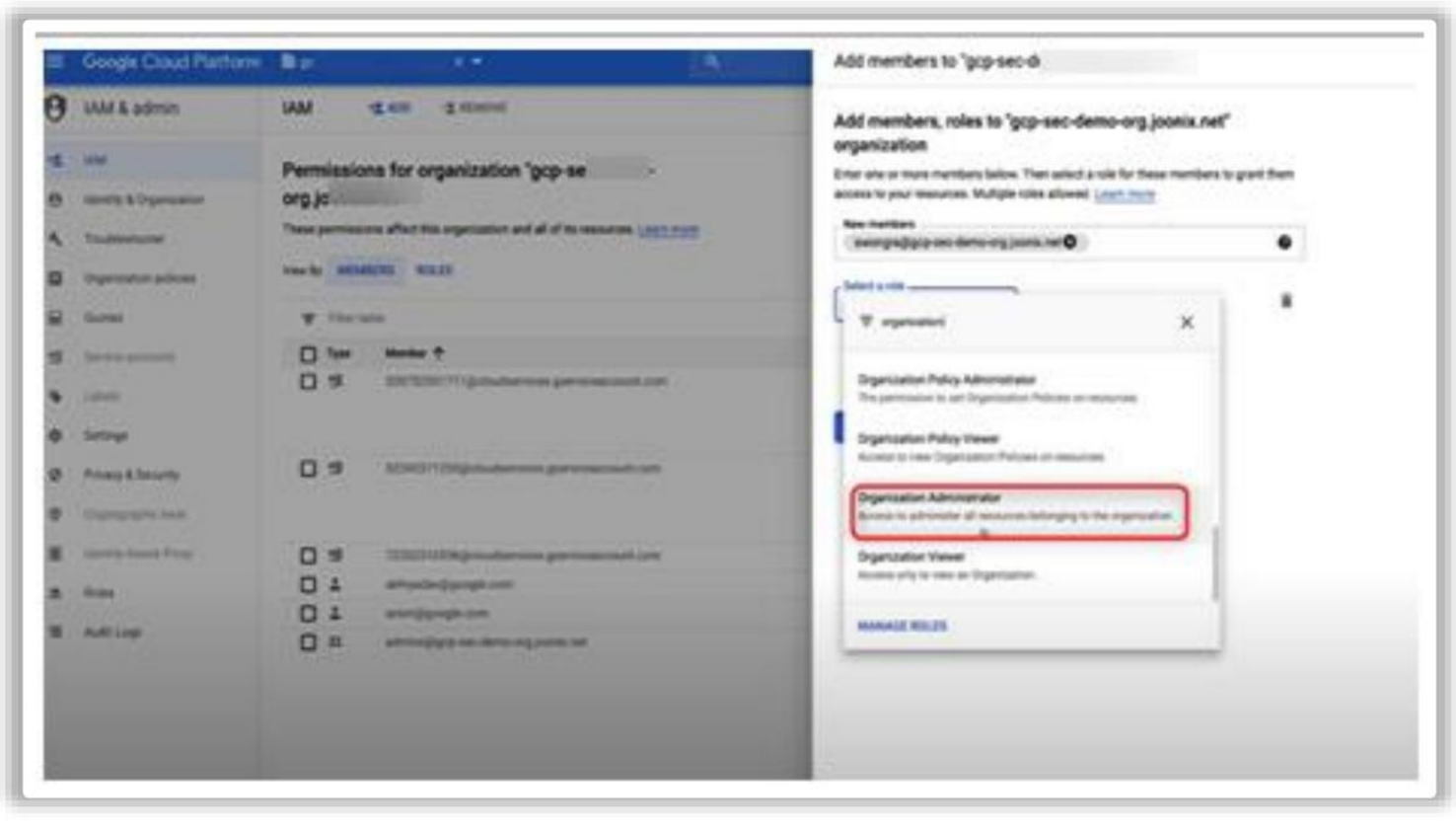


Figure 7.99: Selecting Organization Administrator

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

- Click on **Add Another Role** to assign **SCC IAM Role** to other users**.**
- In the **Role** field for Admin access to the security center, select **Security Center Admin.**
- Click on **Save.**

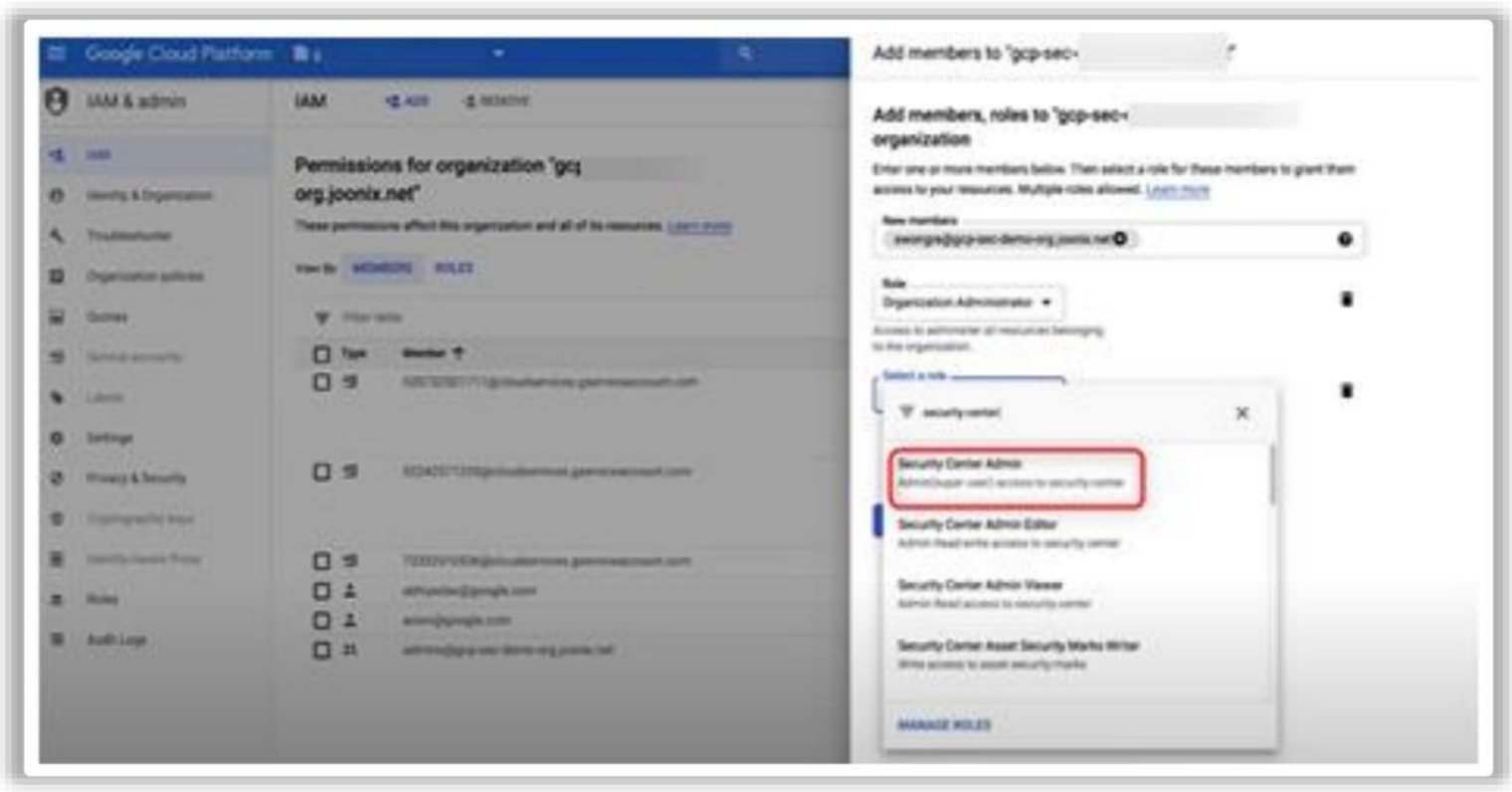


Figure 7.100: Saving IAM Permissions

- **Step 2: Enable Cloud SCC**
  - Navigate to **Security** in the console and click on **Security Command Center.**

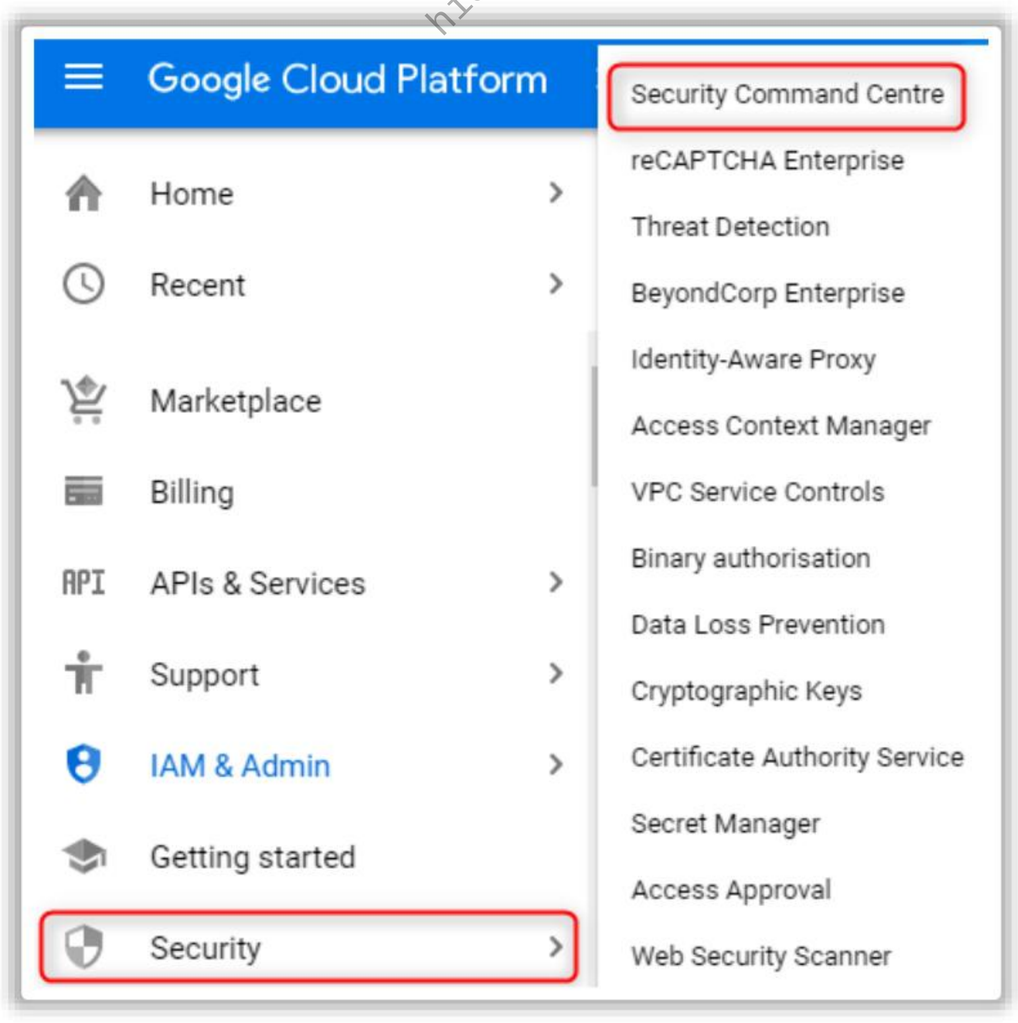


Figure 7.101: Navigating to Security

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

- Go to the **Organization drop-down** list and choose the organization on which SCC is to be enabled.

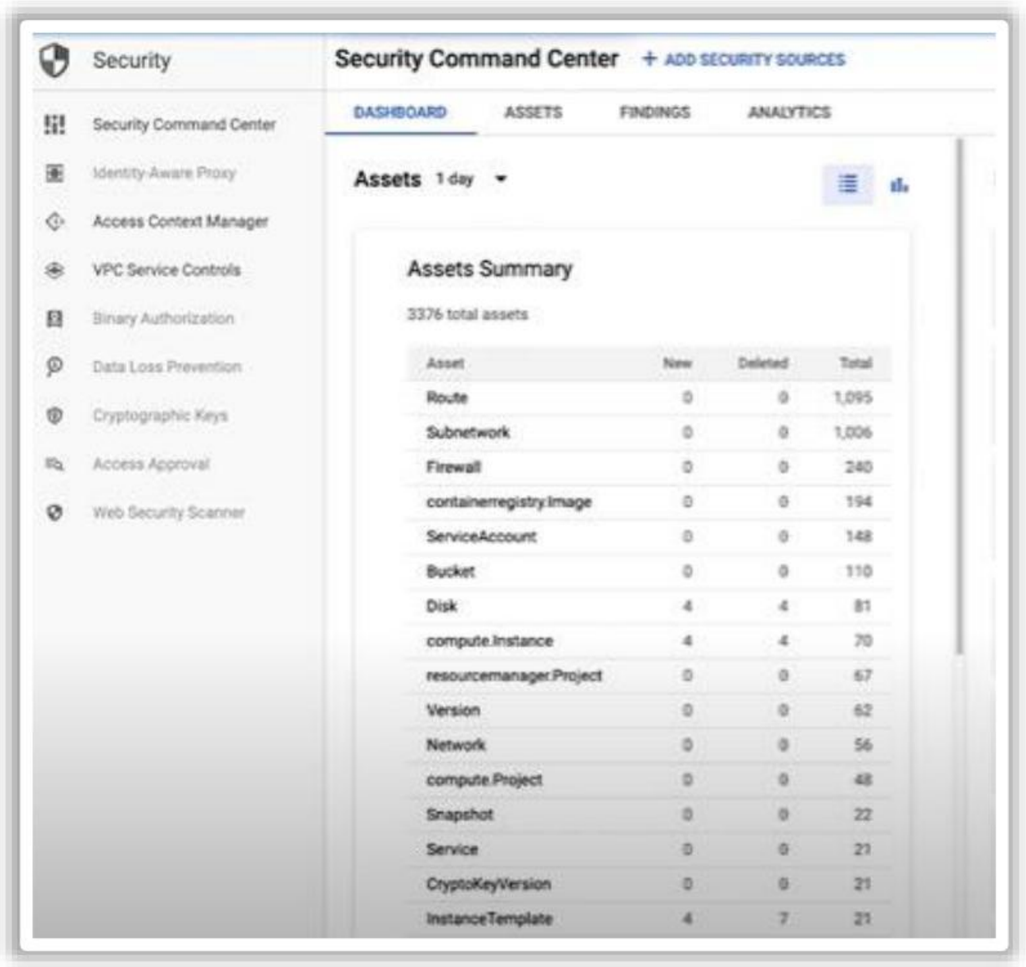


Figure 7.102: Choosing the Organization to Enable SCC

- Select the Organization for which SCC is to be enabled.

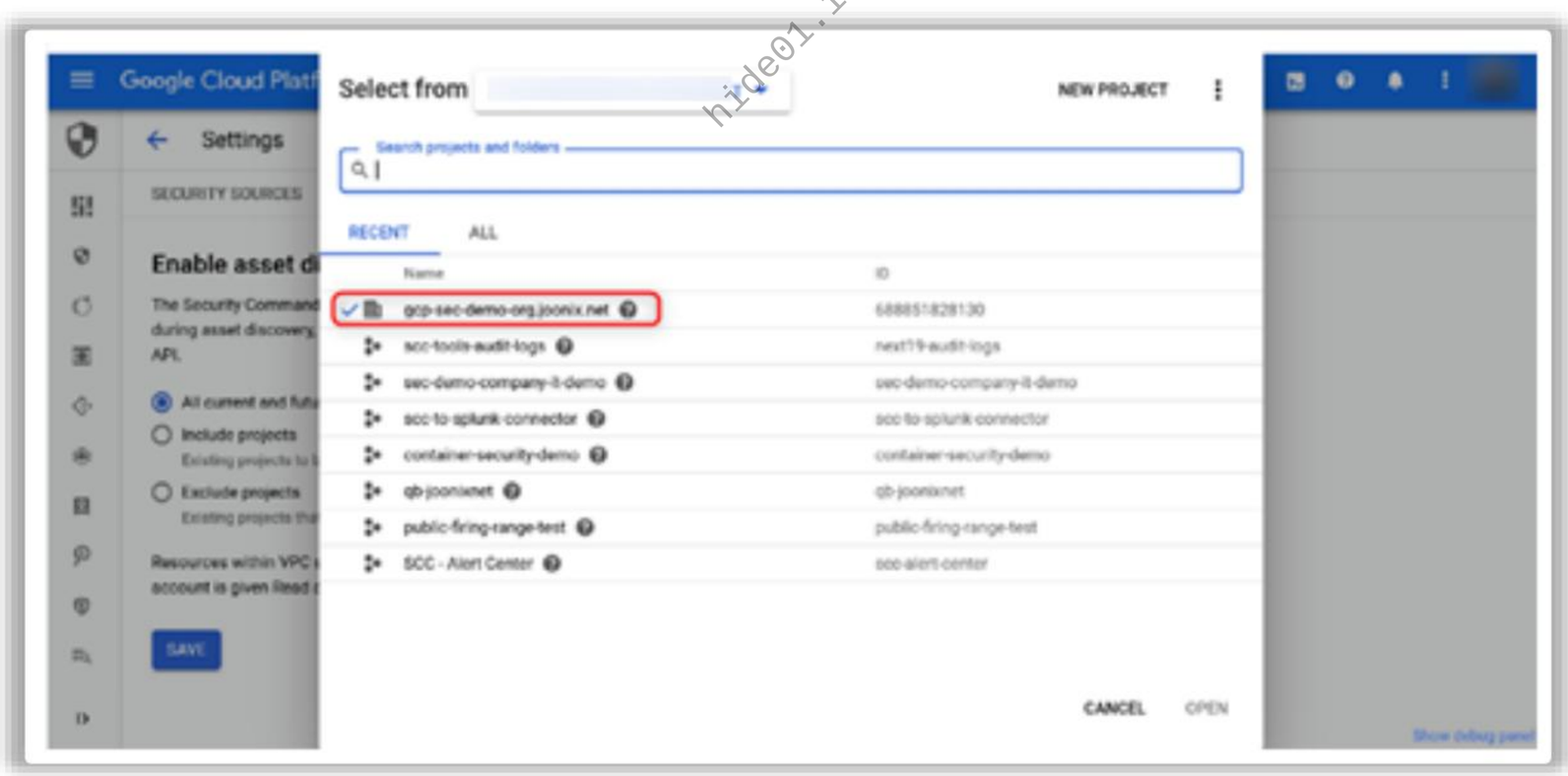


Figure 7.103: Selecting Organization

- Go to settings and select **Asset Monitoring.**

hide01.ir

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

- Click on the checkbox **All Current and Future Projects** to enable asset discovery and click on **Save.**

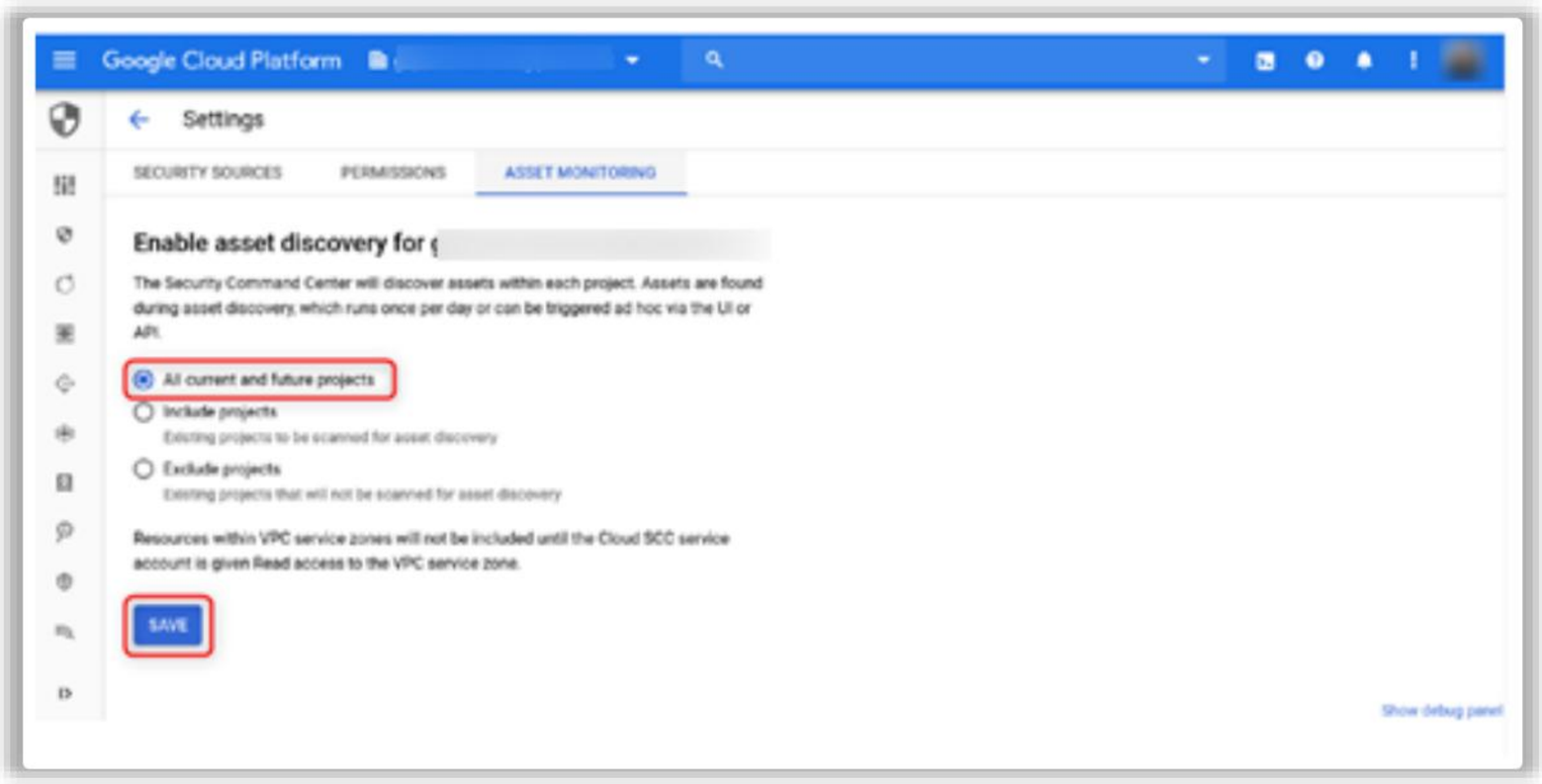


Figure 7.104: Enabling Asset Discovery

- **Step 3: Turn on All Built-In Security Sources to Monitor Vulnerabilities and Threats**
  - Under the Settings toolbar, select **Security Sources.**
  - Turn on all built-in security capabilities for an insight into the vulnerabilities, threats, and misconfigurations.

hide01.ir

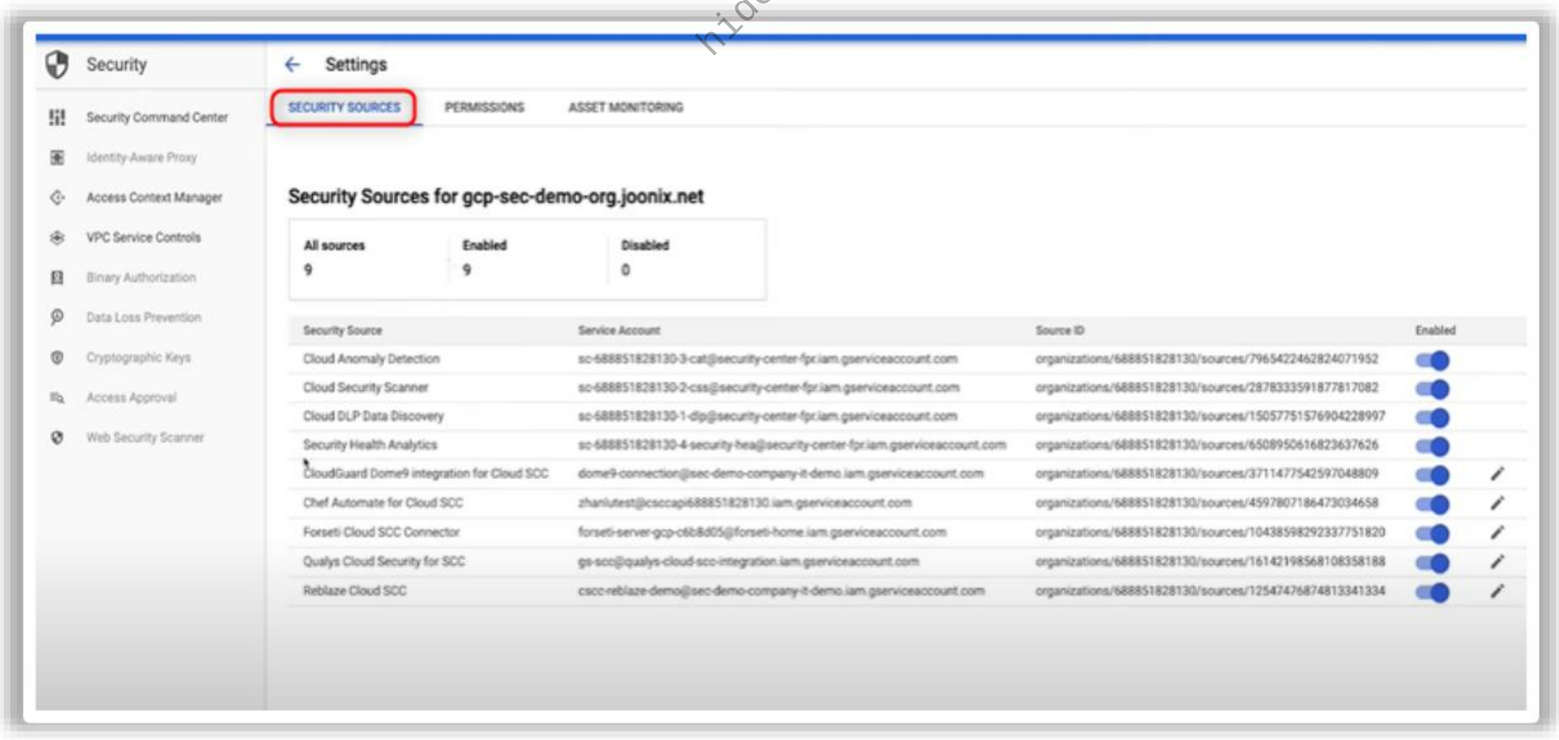


Figure 7.105: Turn On Built-In Security Capabilities

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

- **Step 4: View the Security Status by Asset Type**
  - In the **Security Command Center** dashboard, click on **Assets.**

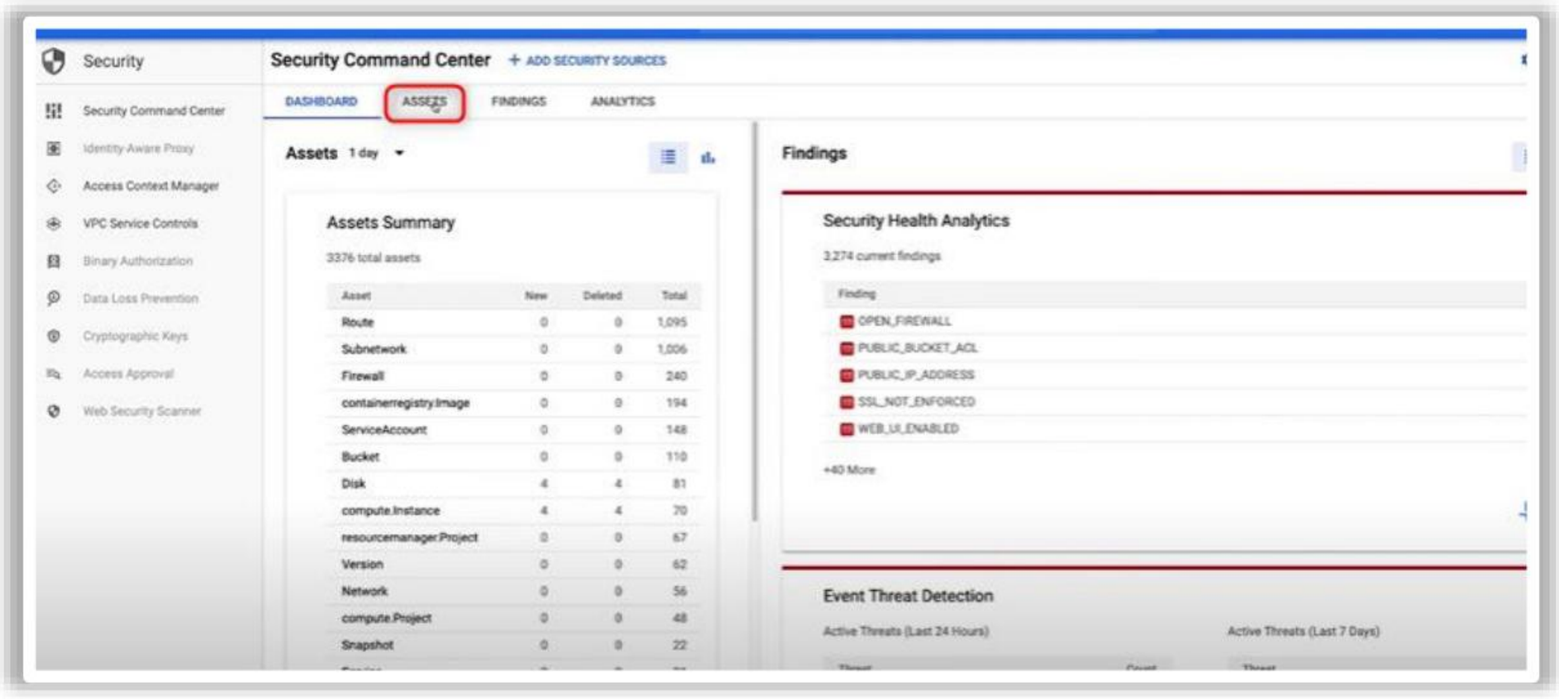
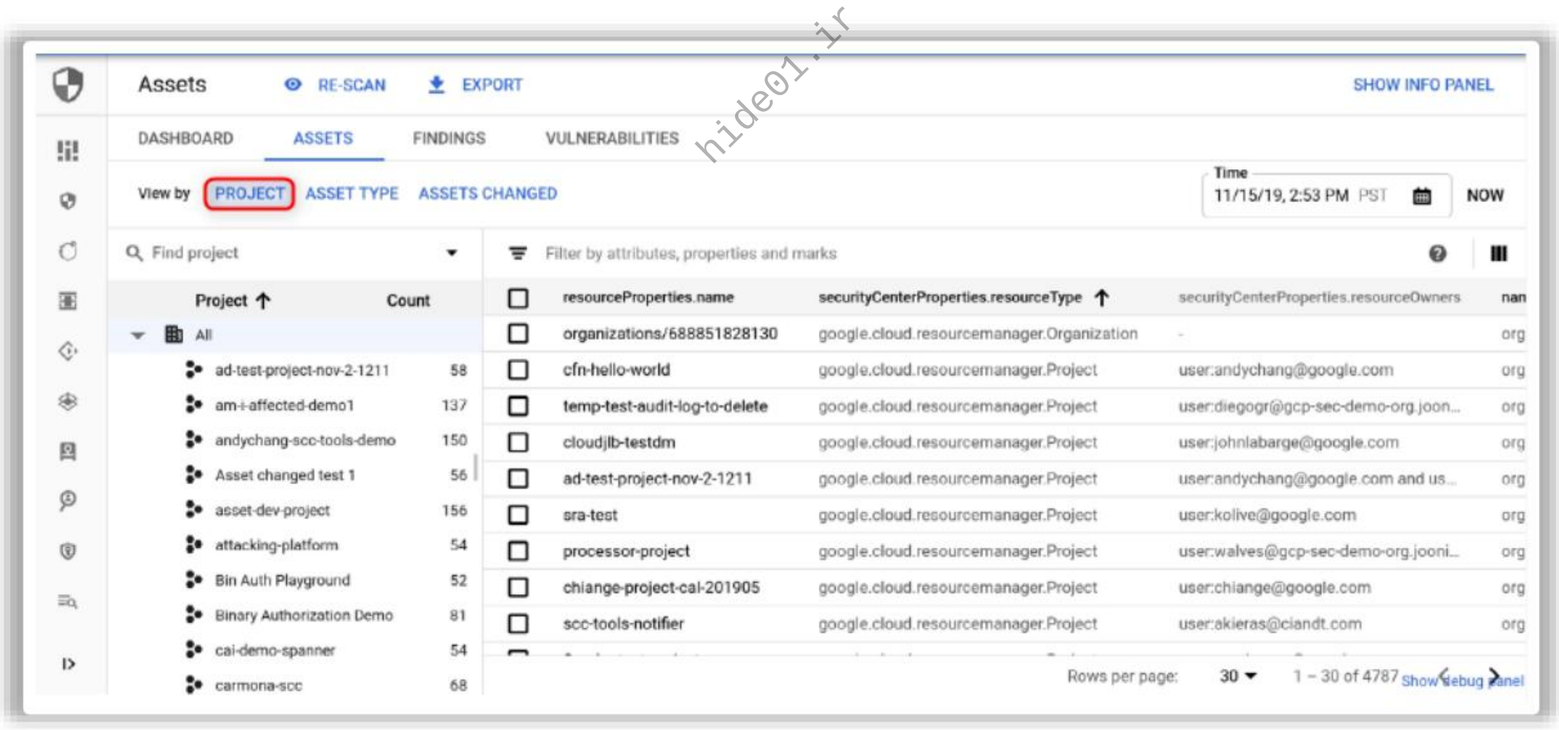


Figure 7.106: Assets

- The security status based on the project can be viewed by clicking on **View by Project.**
- The security status at a particular time can be viewed by clicking on the **Time** field.



hide01.ir

Figure 7.107: Time Field

- Based on **Asset Type,** click on view by **Asset Type**

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

- The security status at a particular time can be viewed by clicking on the **Time** field.

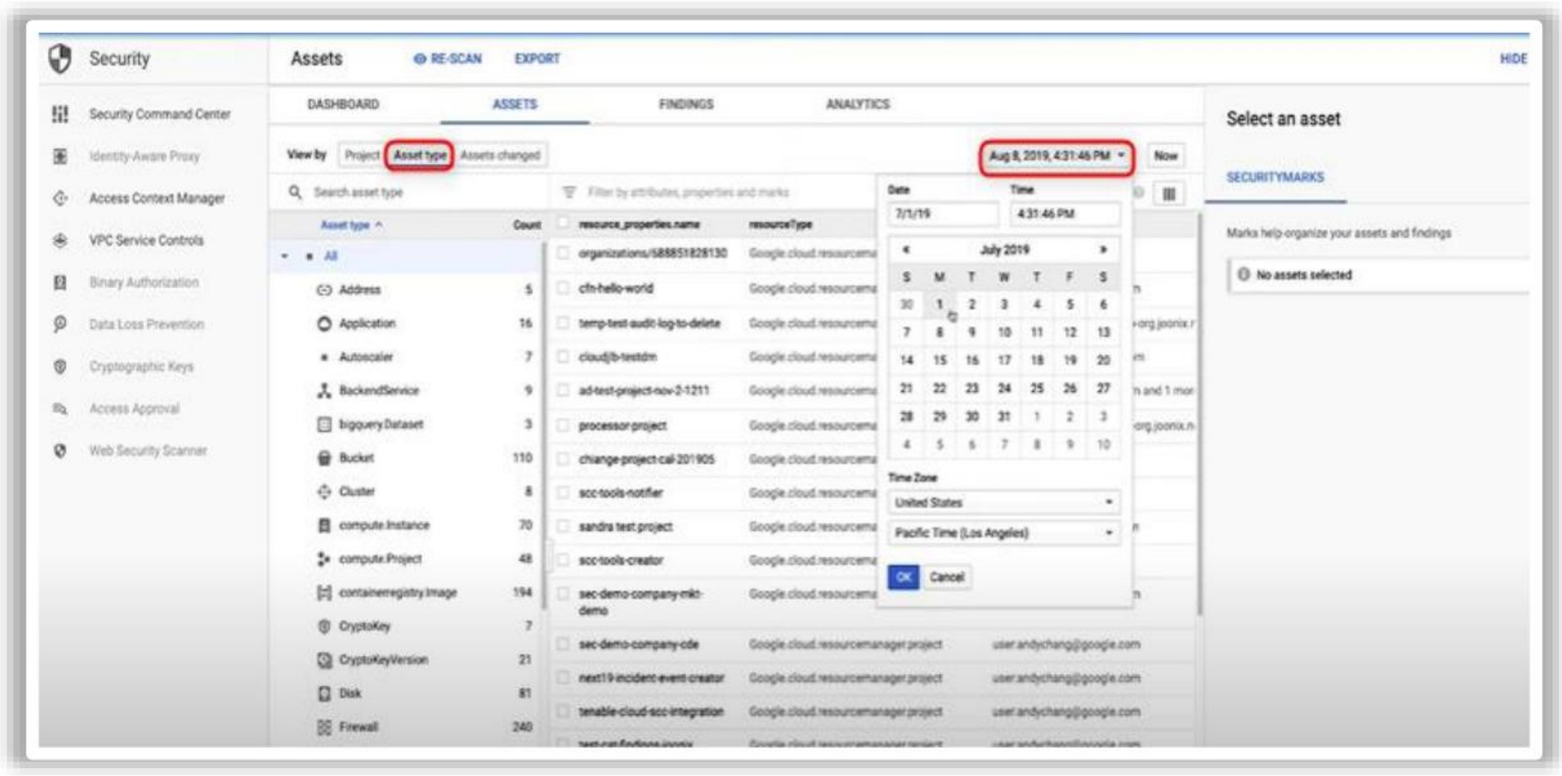


Figure 7.108: Time Field

- **Step 5: View the Cloud SCC Findings on the Assets**
  - Click on **Findings.** Click on **Source Type** to view the service that discovered the issue.
  - The security issue at a particular time can be viewed by selecting the **Time** field and setting the date and time.

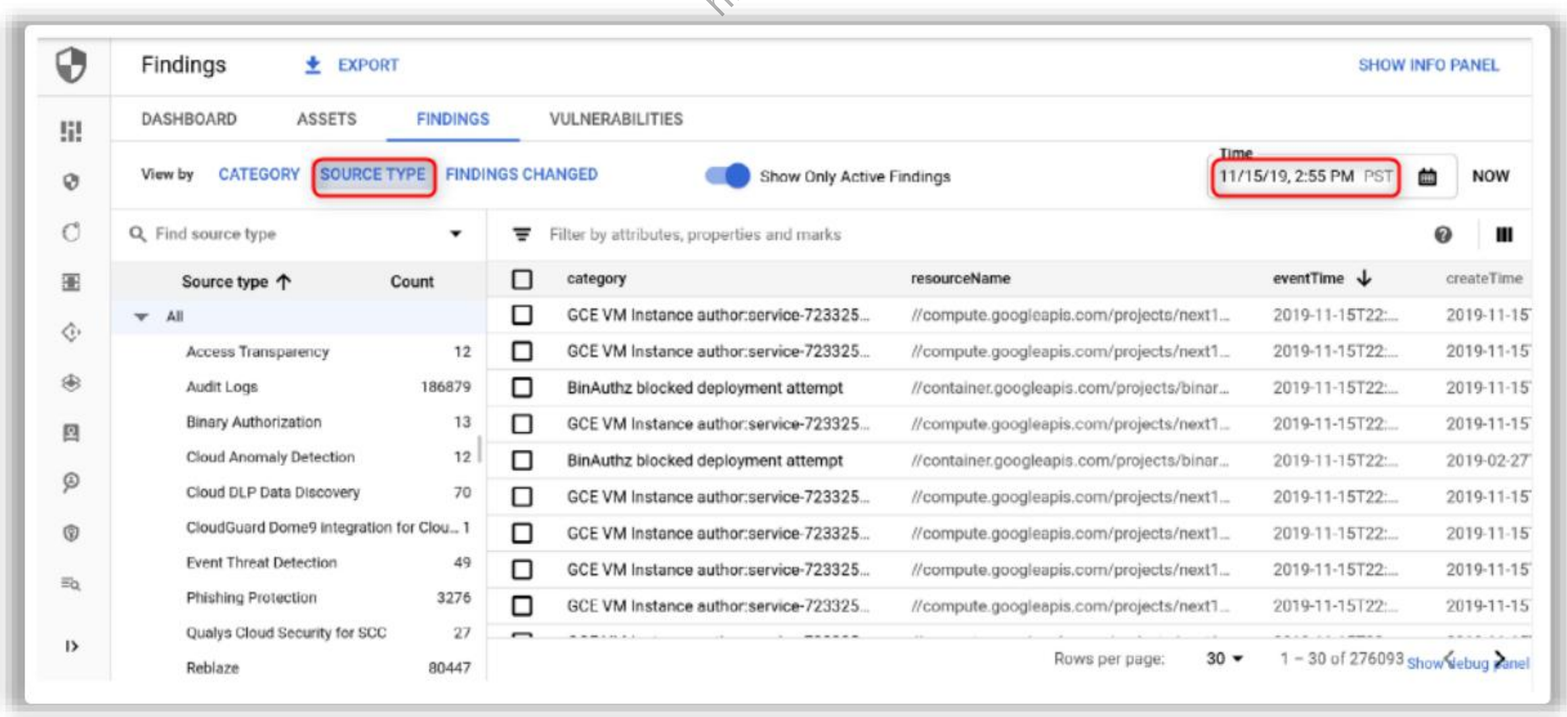


Figure 7.109: Time of a Security Issue

- The findings can be filtered based on security marks by clicking on the checkbox next to the resource for focusing on specific security resources.

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

- Enter a key name under the **Key** field and value under the **Value** field, and then click **Save.**

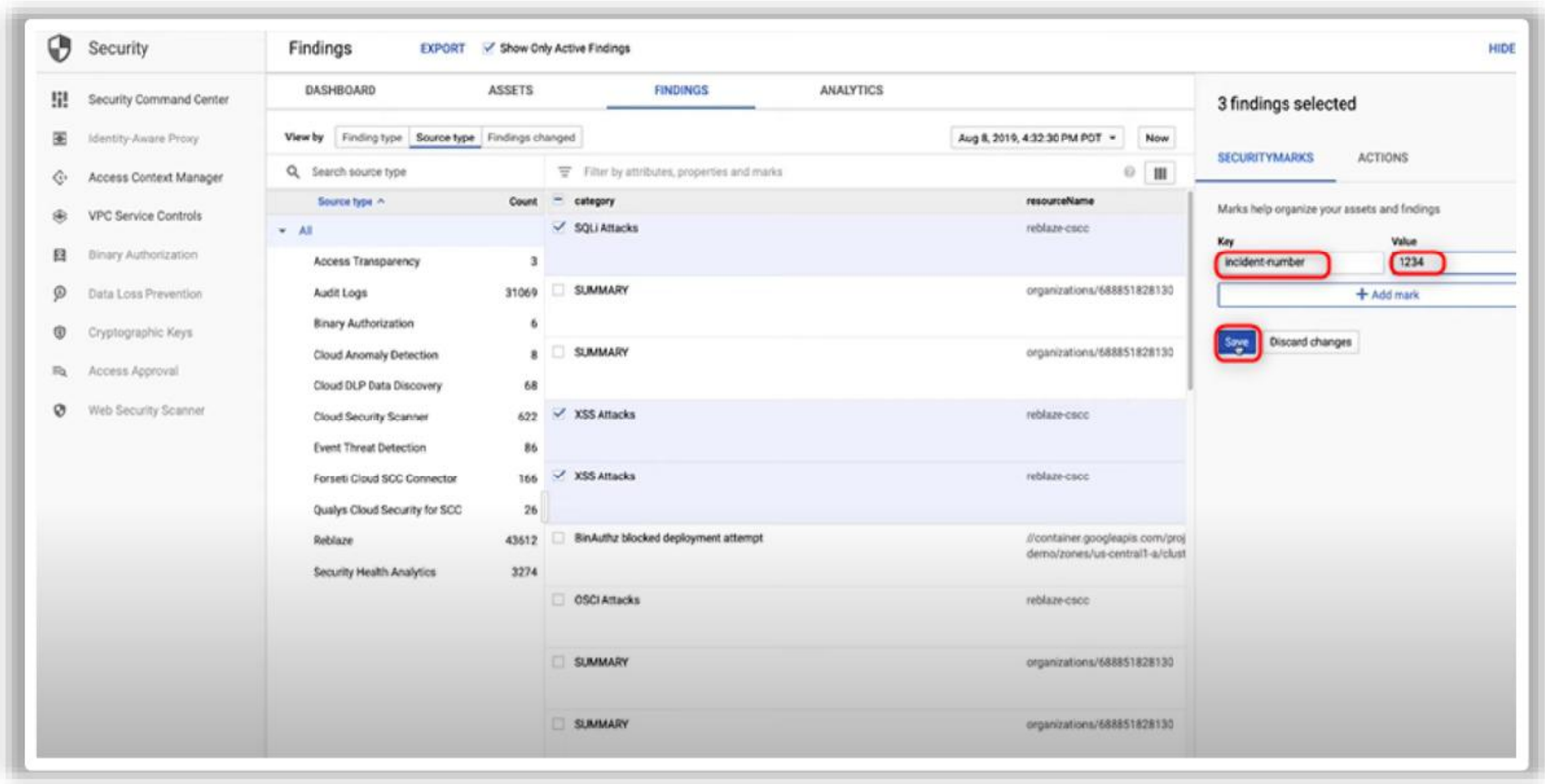


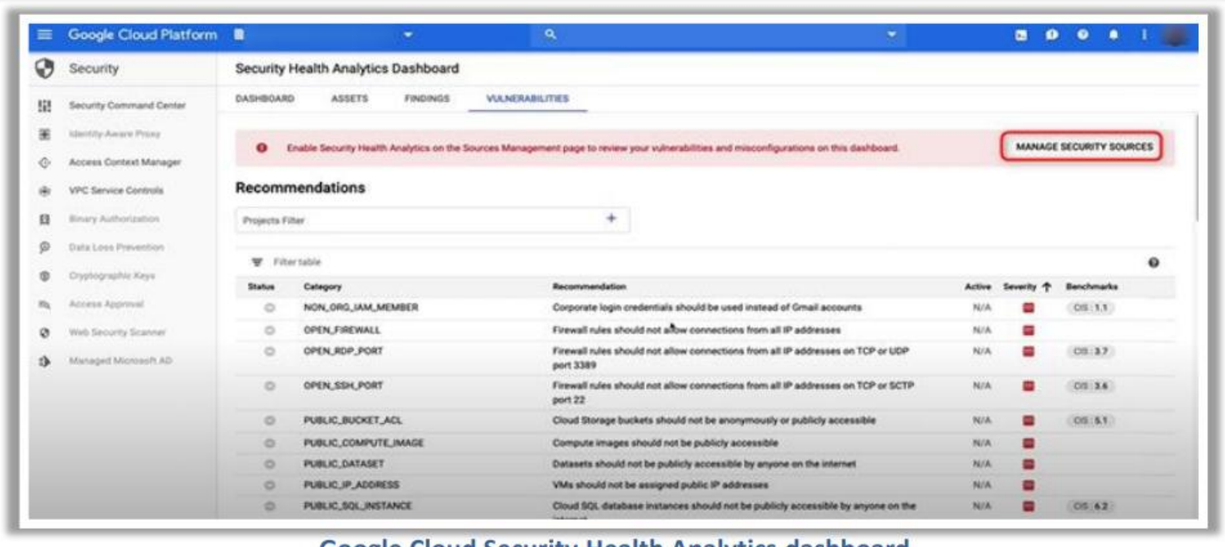
Figure 7.110: Entering Key and Value

hide01.ir

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

Responding to Misconfigurations with Security Health Analytics

- The misconfigurations and security compliance violations in GCP resources can be detected and prevented using Security Health Analytics (SHA)
- An SHA user must have either organization administrator cloud IAM role or security center IAM role
- The vulnerabilities detected by SHA include publicly accessible firewall rules, cloud storage buckets, instances that do not enforce SSL, etc.
- The SHA findings provides a description of how to remediate an issue



Google Cloud Security Health Analytics dashboard

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

Responding to Misconfigurations with Security Health Analytics

The misconfigurations and security compliance violations in GCP resources can be detected and prevented using Security Health Analytics (SHA). The misconfigurations are based on some recommendations and are sorted based on their severity level. The active column shows the currently active findings. The status column shows the status of the detector that presented the finding. The benchmark column shows the benchmark associated with a misconfiguration. After the SCC is enabled, it runs in two modes: batch mode and real-time mode. The batch mode automatically runs twice a day in 12 hours. The real-time mode runs scans during asset configuration changes. An SHA user must have either an organization administrator IAM role or a SCC IAM role. The vulnerabilities detected by SHA include publicly accessible firewall rules, Cloud Storage buckets, instances that have not enforced SSL, etc. The SHA findings describe how to remediate an issue.

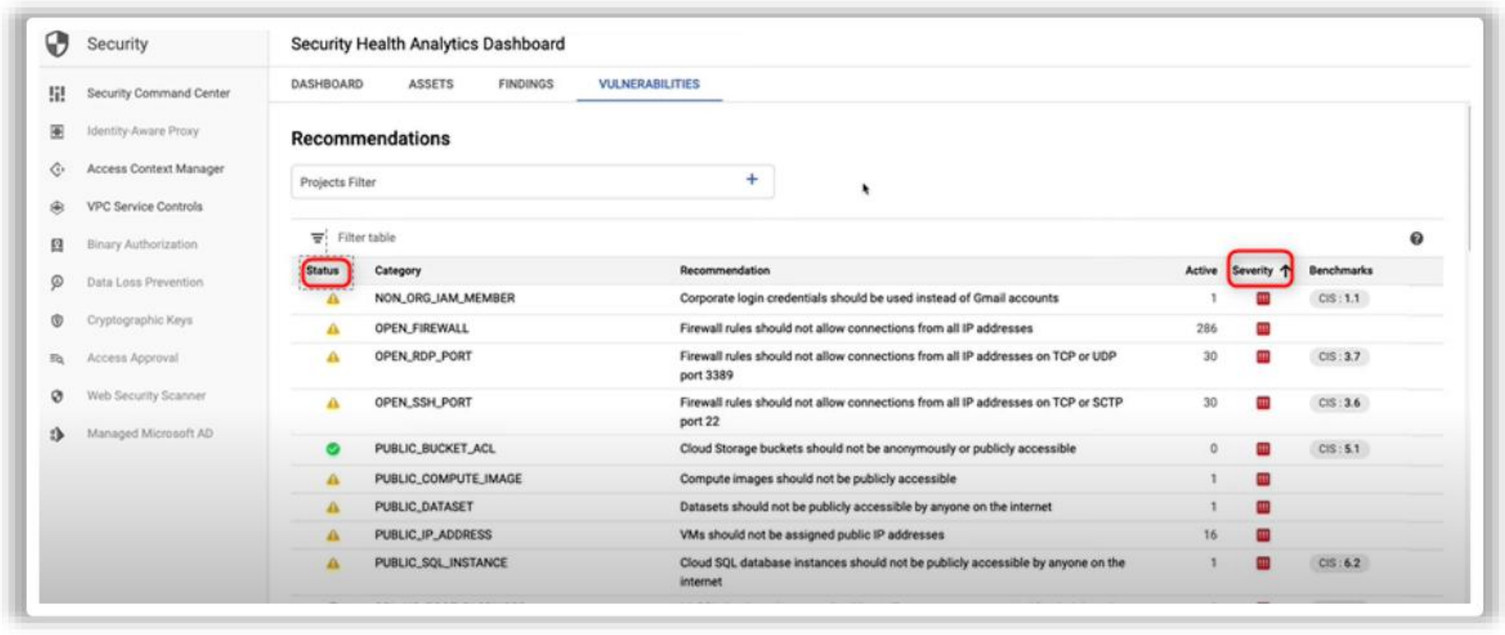


Figure 7.111: Google Cloud Security Health Analytics Dashboard

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

Steps to Detect and Respond to Misconfigurations With Security Health Analytics

- **Step 1: Enable Security Health Analytics**
  - Navigate to **IAM & Admin** in the console and select **IAM.**
  - Click **Add.**

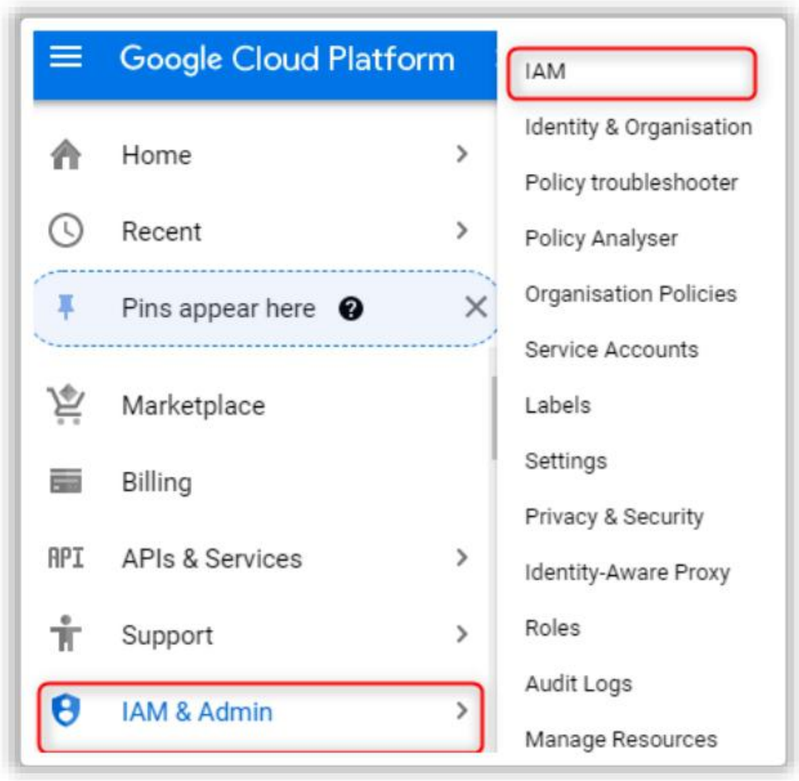


Figure 7.112: Navigating to IAM

- Click on **Add** in the **IAM** page

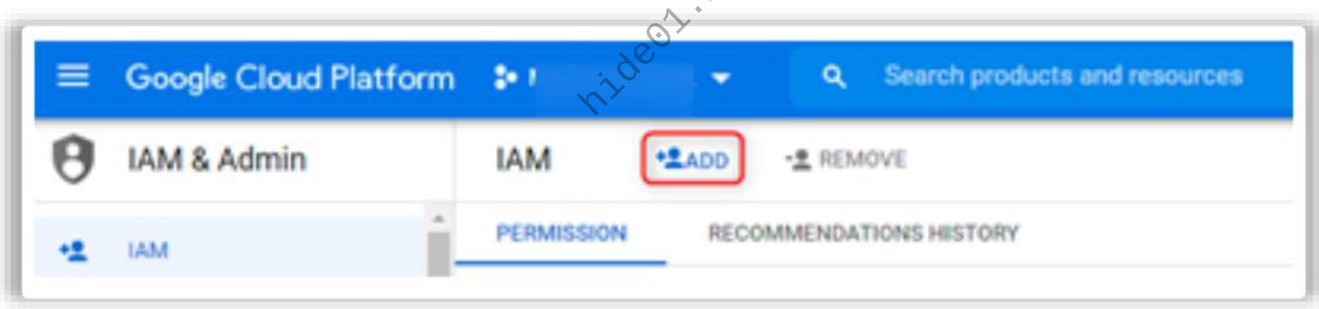


Figure 7.113: Adding Permissions

- In the **Role** field for access to administer all resources belonging to the organization, select **Organization Administrator.**

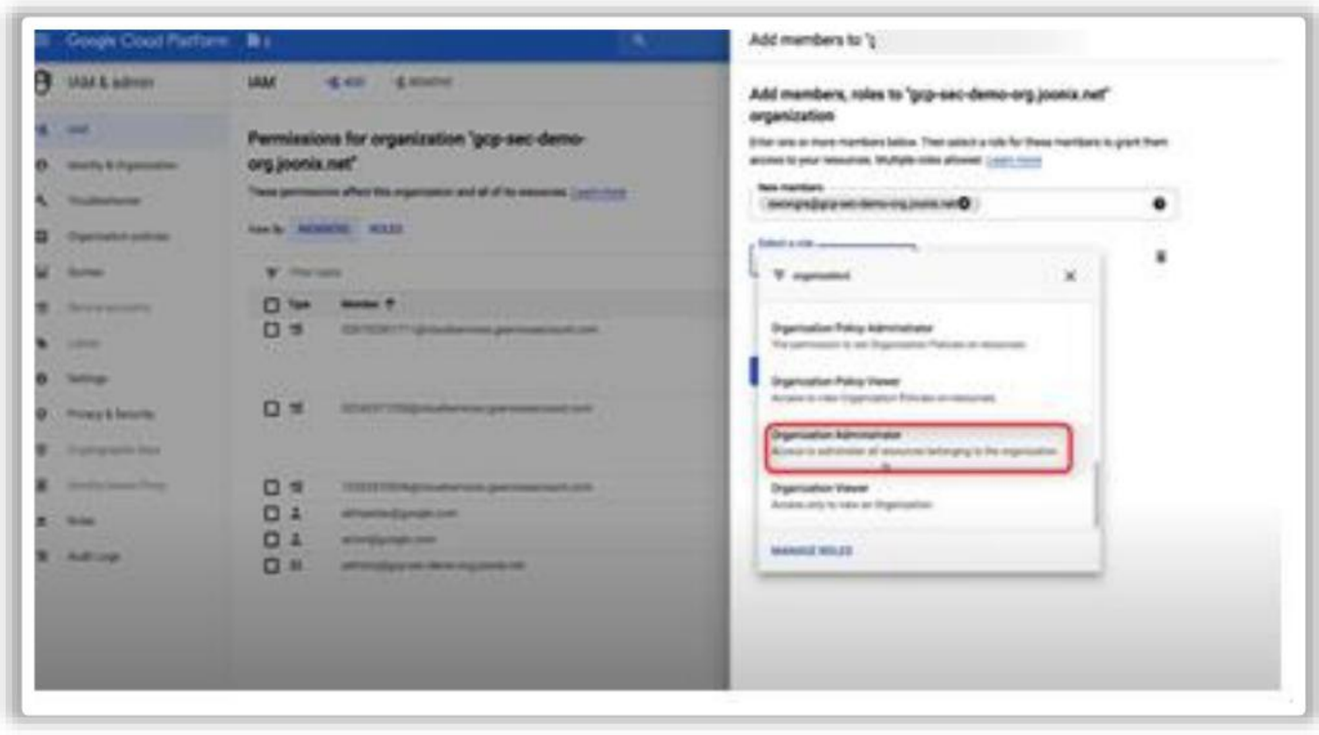


Figure 7.114: Selecting Organization Administrator

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

- Click on **Add Another Role** to assign **SCC IAM Role** to other users
- In the **Role** field for Admin access to security center, select **Security Center Admin.**
- Click on **Save.**

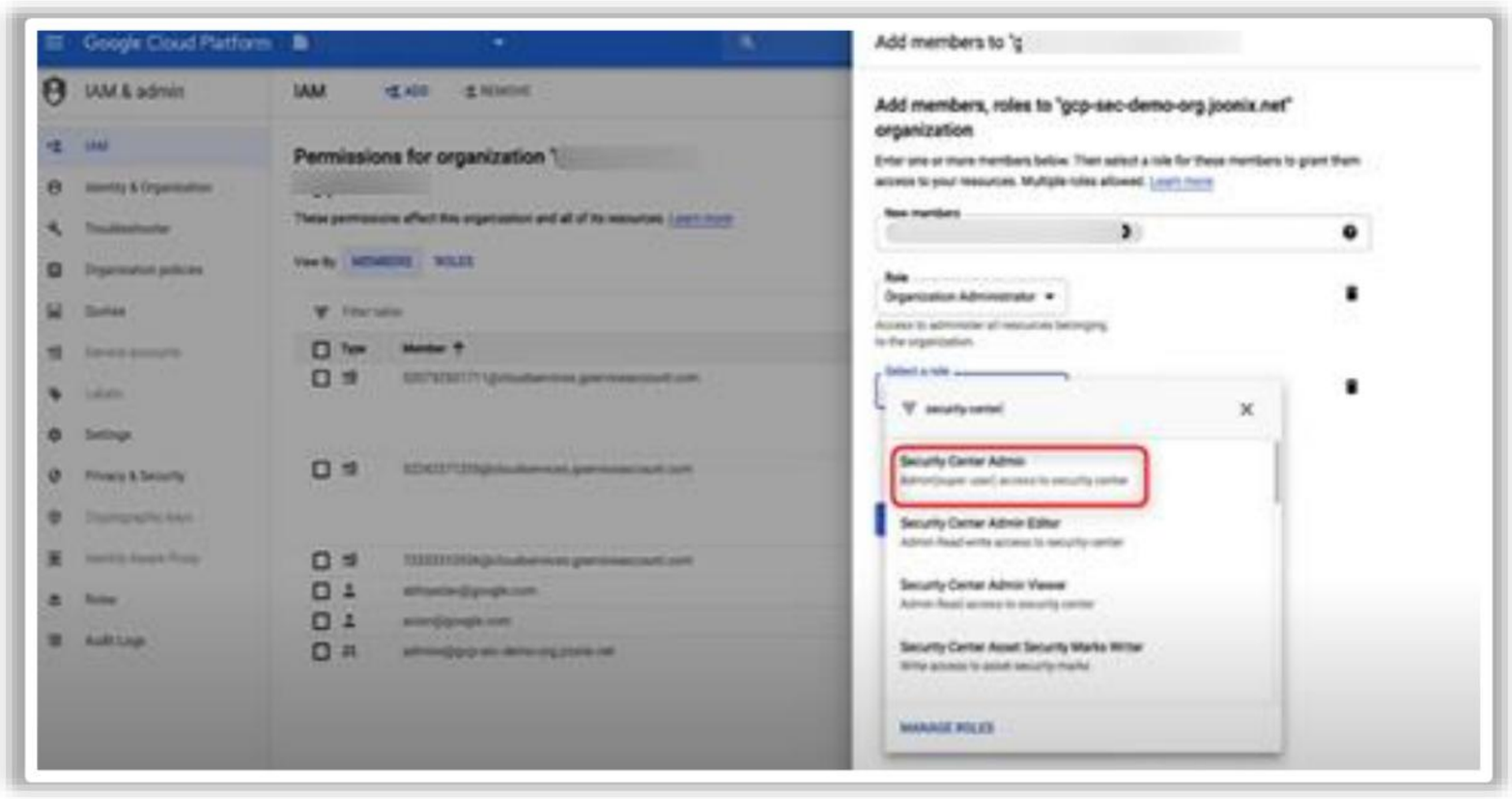


Figure 7.115: Selecting Security Center Admin

- **Step 2: View the Misconfigurations**
  - Navigate to **Security** in the console and click on **Security Command Center.**

hi0101.ir

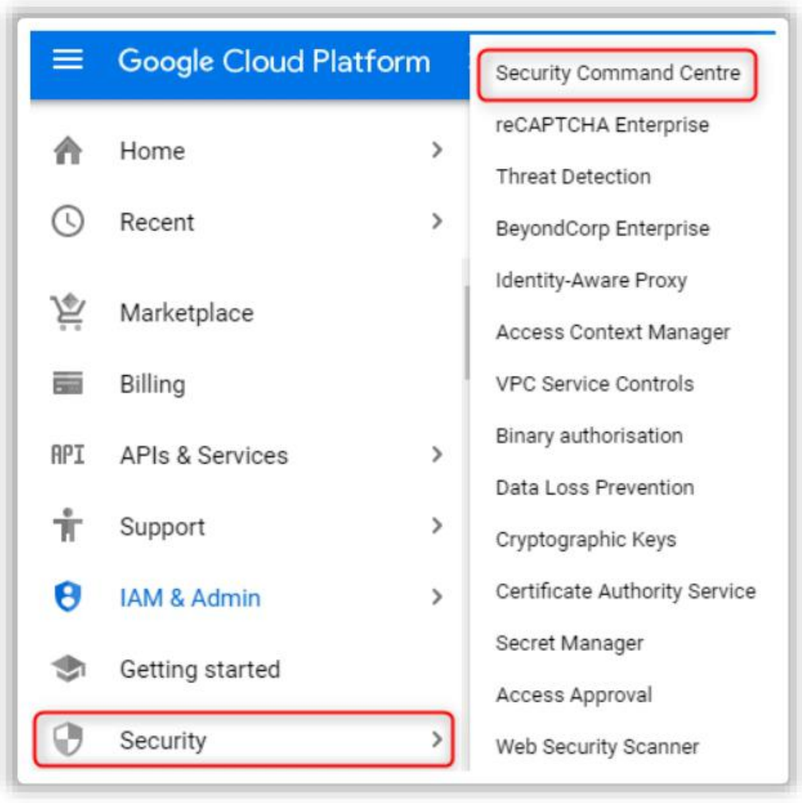


Figure 7.116: Navigating to Security Command Center

- Click on the **Vulnerabilities** tab in the **Security Health Center** dashboard. If Security Health Center is not enabled, a message will appear to enable **Security Health Analytics.**

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

- Click on **Manage Security Sources.**

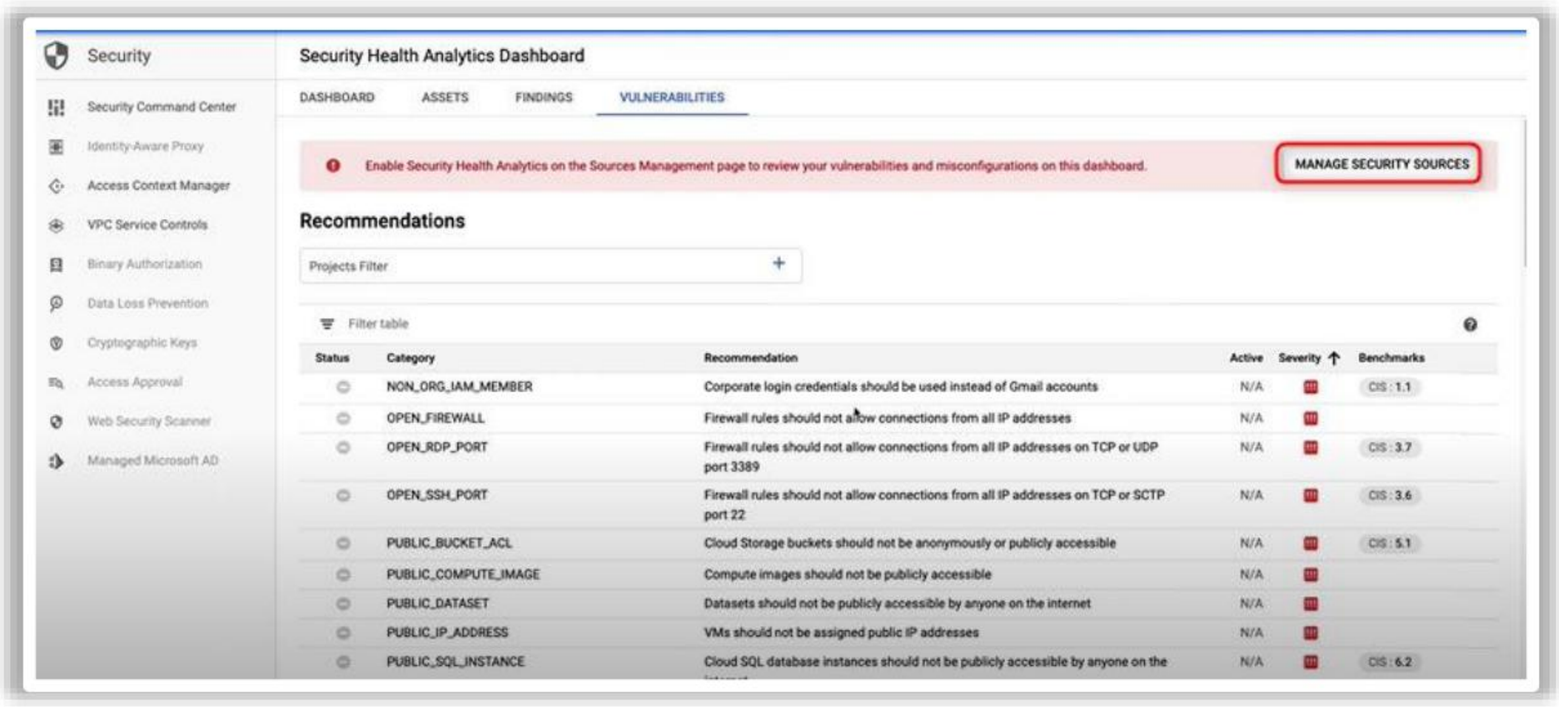


Figure 7.117: Manager Security Sources

- Turn on **Security Health Analytics** to enable it.

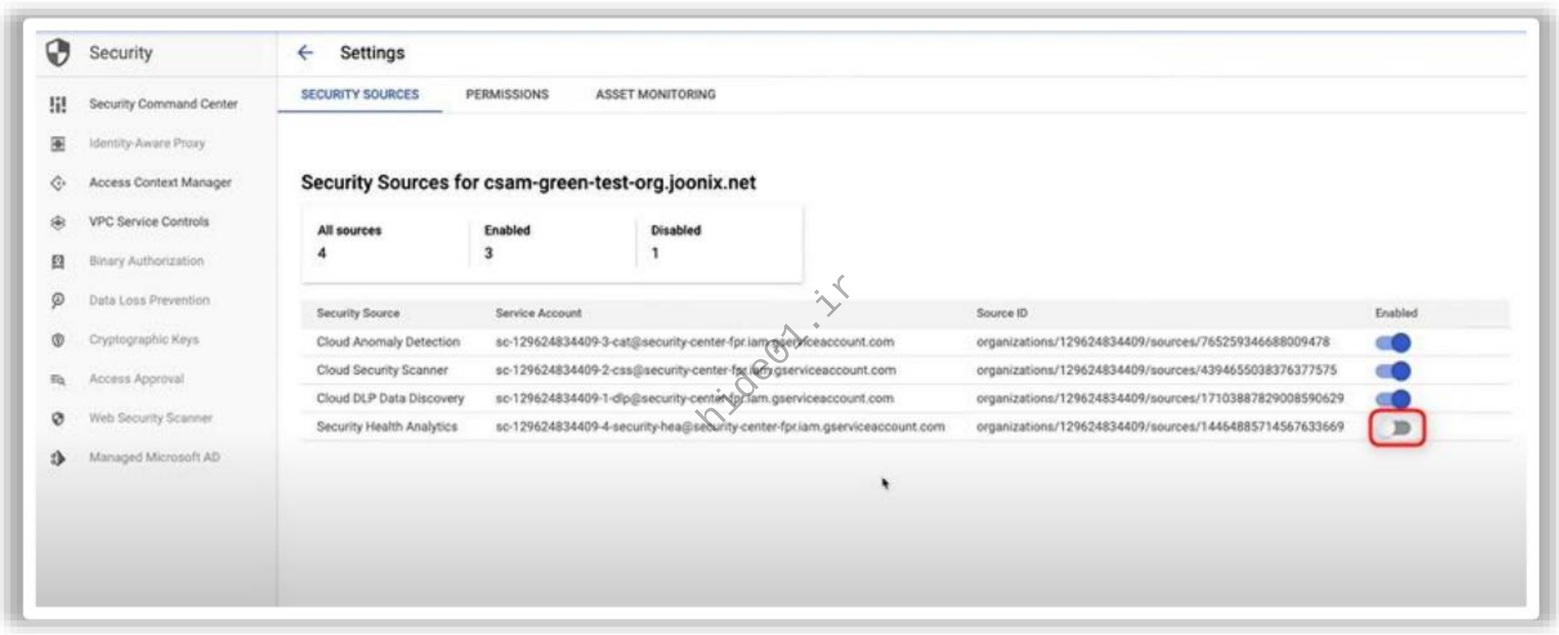


Figure 7.118: Turning On Security Health Analytics

- Click on the **Vulnerabilities** tab to view the detected misconfigurations.

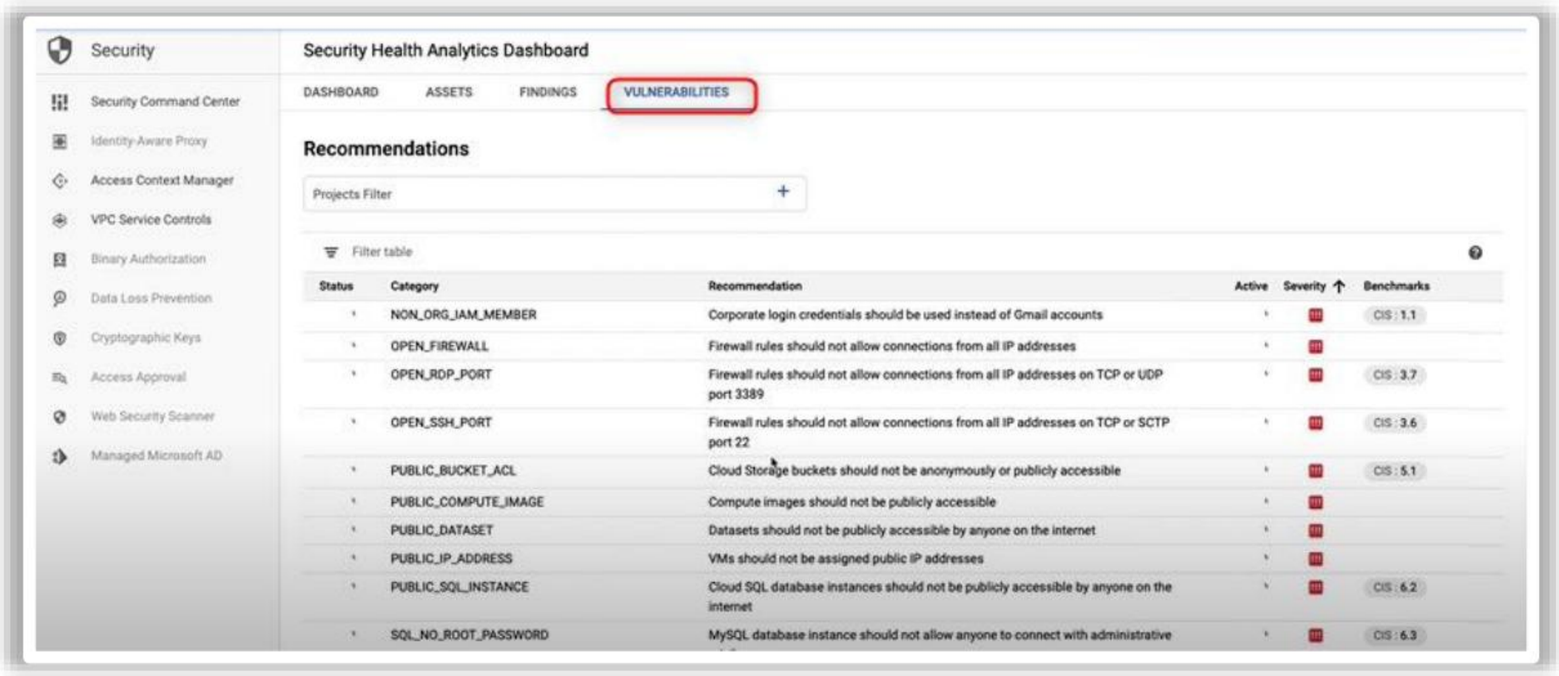


Figure 7.119: Vulnerabilities

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

- Click on the **+ icon** in the **Projects Filter** to sort the vulnerabilities based on the project.

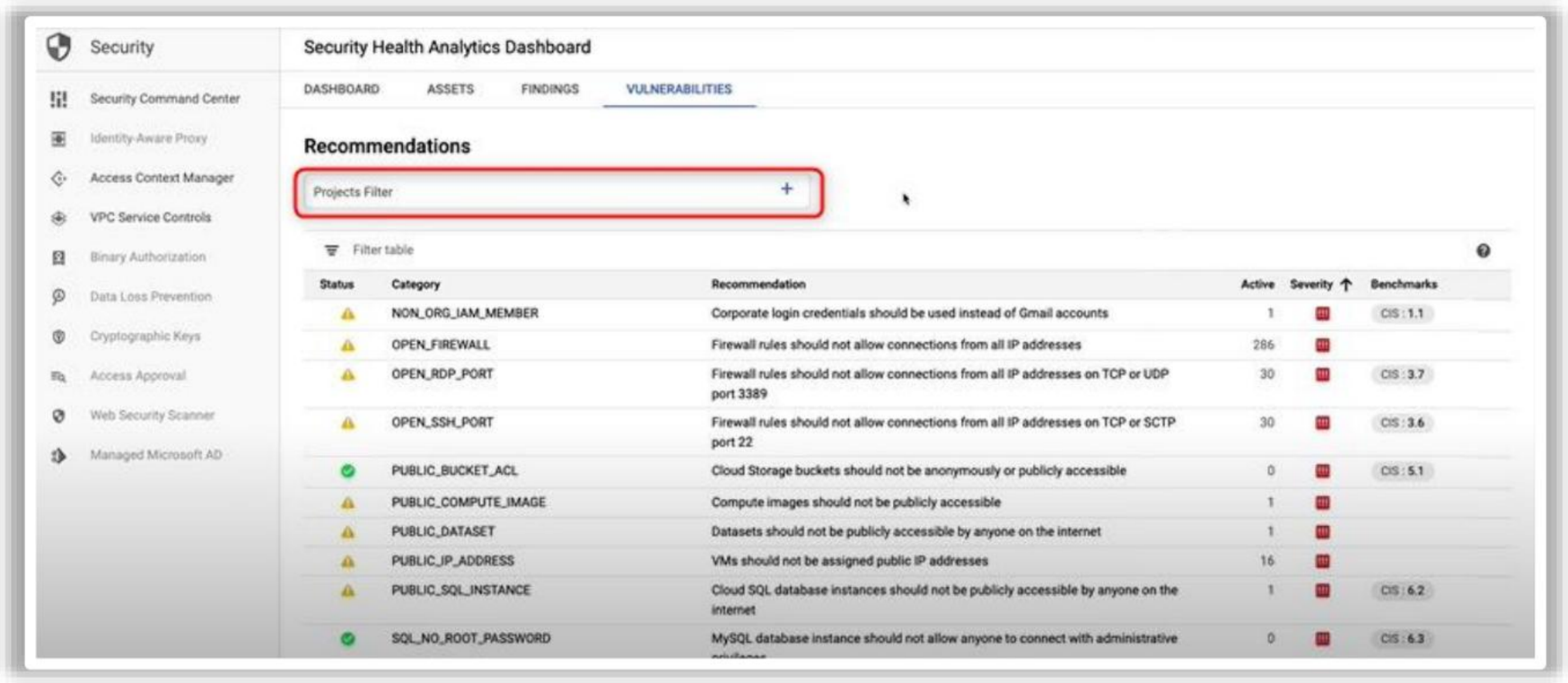


Figure 7.120: Using Project Filter

- **Step 3: Remediation of a Security Vulnerability**
  - Click on a misconfiguration.

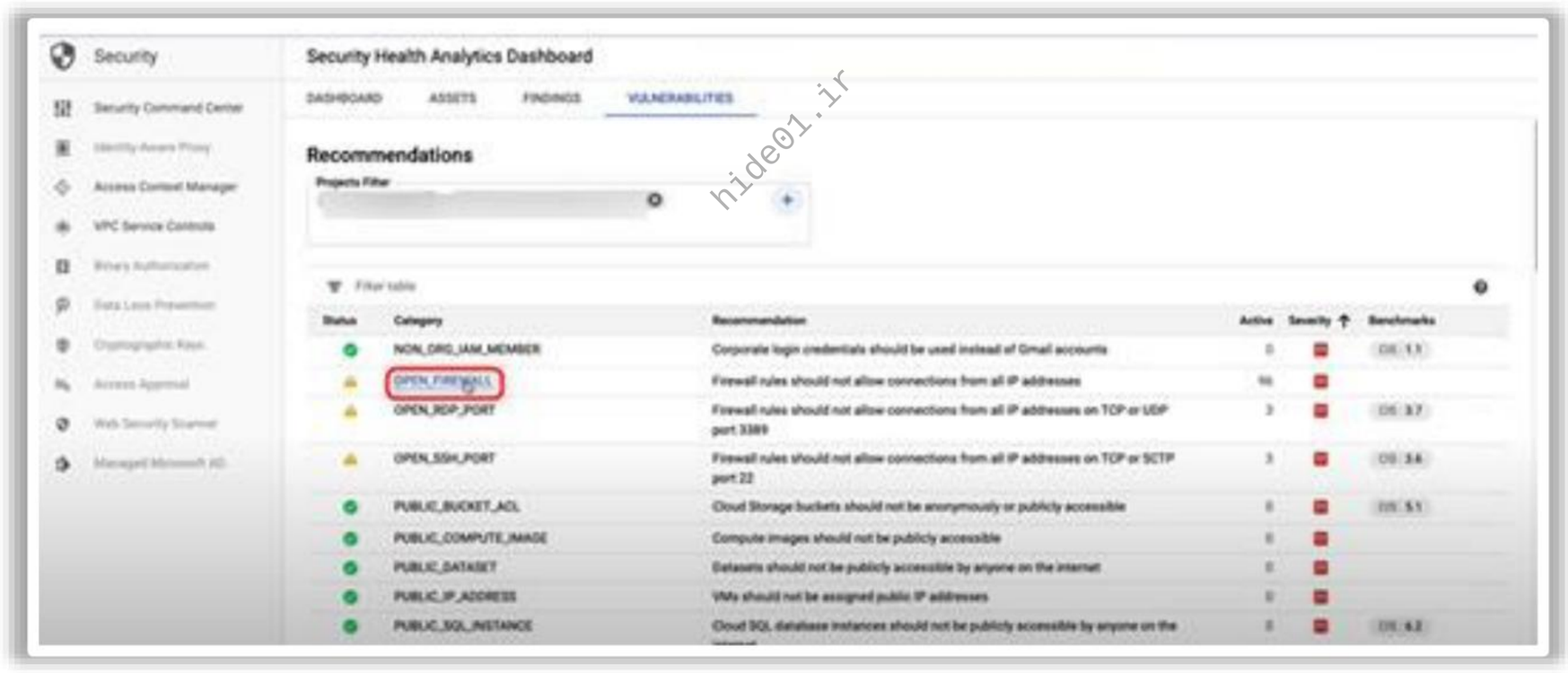
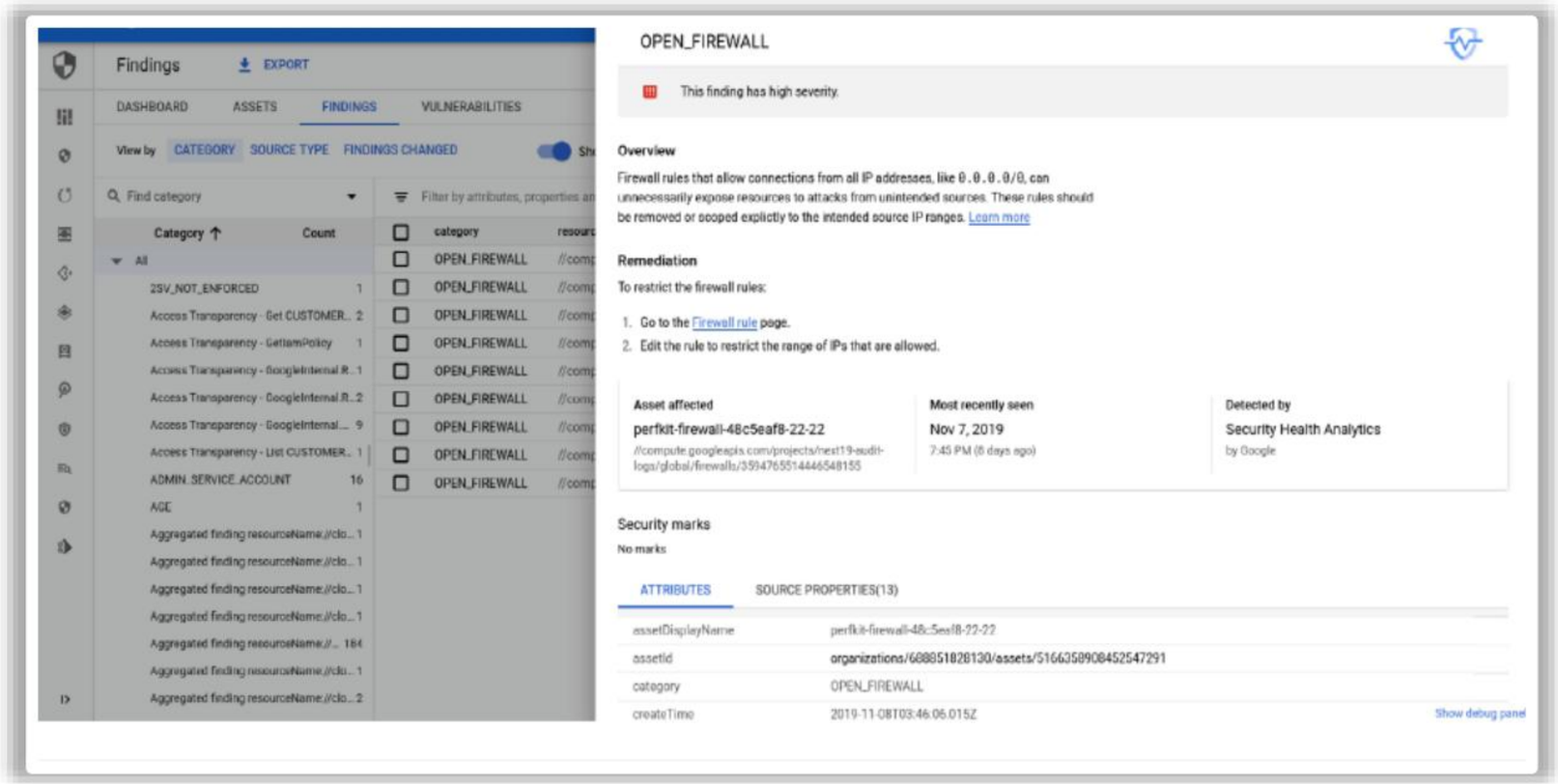


Figure 7.121: Misconfiguration Issue

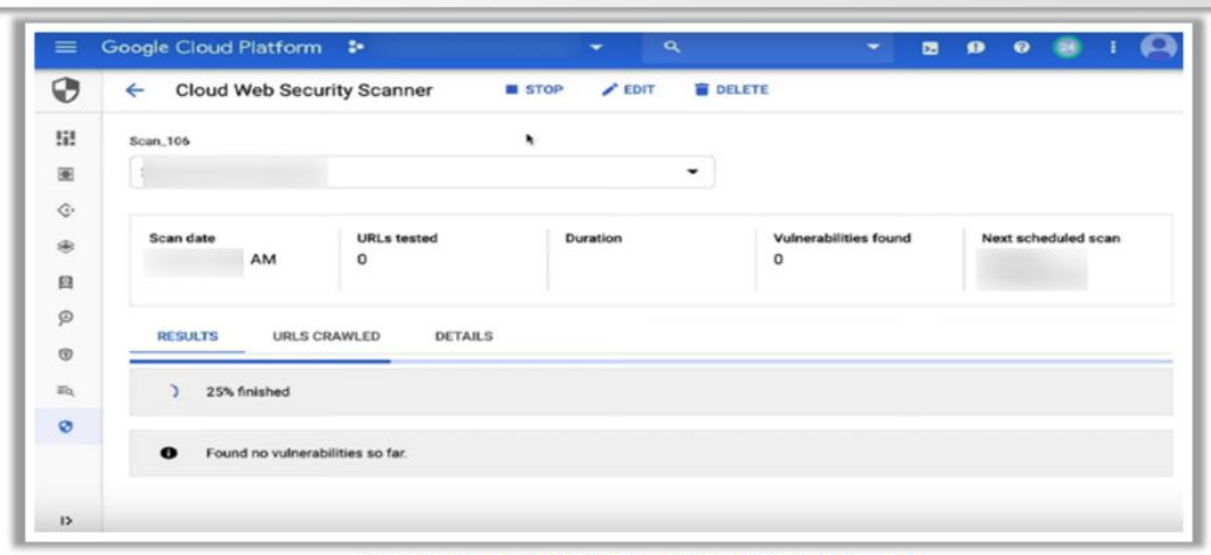
Certified Cloud Security Engineer Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The pop-up page will show the misconfiguration details and remediation steps to solve the issue. Follow the remediation steps on the page to solve the issue.


Findings
EXPORT
DASHBOARD
ASSETS
FINDINGS
VULNERABILITIES
View by
CATEGORY
SOURCE TYPE
FINDINGS CHANGED
Find category
Filter by attributes, properties an
Category
Count
All
2SV_NOT_ENFORCED 1
Access Transparency - Get CUSTOMER... 2
Access Transparency - GetIamPolicy 1
Access Transparency - GoogleInternal.R... 1
Access Transparency - GoogleInternal.R... 2
Access Transparency - GoogleInternal.... 9
Access Transparency - List CUSTOMER... 1
ADMIN_SERVICE_ACCOUNT 16
AGE 1
Aggregated finding resourceName://clo... 1
Aggregated finding resourceName://clo... 1
Aggregated finding resourceName://clo... 1
Aggregated finding resourceName://clo... 1
Aggregated finding resourceName://... 184
Aggregated finding resourceName://clo... 1
Aggregated finding resourceName://clo... 2
category
OPEN_FIREWALL
OPEN_FIREWALL
OPEN_FIREWALL

Detecting Web Application Vulnerabilities with Cloud Web Security Scanner

- Web Security Scanner can detect vulnerabilities in applications before they are deployed into production
- It eliminates false positives, and therefore, does not display low confidence alerts
- It includes managed scans and custom scans
- The managed scans identify vulnerabilities such as mixed content, clear-text passwords, and outdated libraries



Google Cloud Web Security Scanner dashboard

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

Detecting Web Application Vulnerabilities with Cloud Web Security Scanner

Web Security Scanner can detect security vulnerabilities in the web applications hosted on App Engine, Compute Engine, and Google Kubernetes Engine in GCP before they are deployed into production. It is very efficient in threat detection as it does not display low-confidence alerts, thereby eliminating false positives. It crawls the application automatically. Web Security Scanner includes managed scans and custom scans. Managed scans are enabled by default. It centrally manages vulnerability detection in the applications and custom scans can be performed to detect vulnerabilities such as XSS, outdated libraries, mixed content, etc.

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

Steps to Detect Web Application Vulnerabilities with Cloud Web Security Scanner

- **Step 1: Enable Cloud Web Security Scanner**

  Enable Managed Scans

  - Navigate to **IAM & Admin** and select **IAM** in the console.

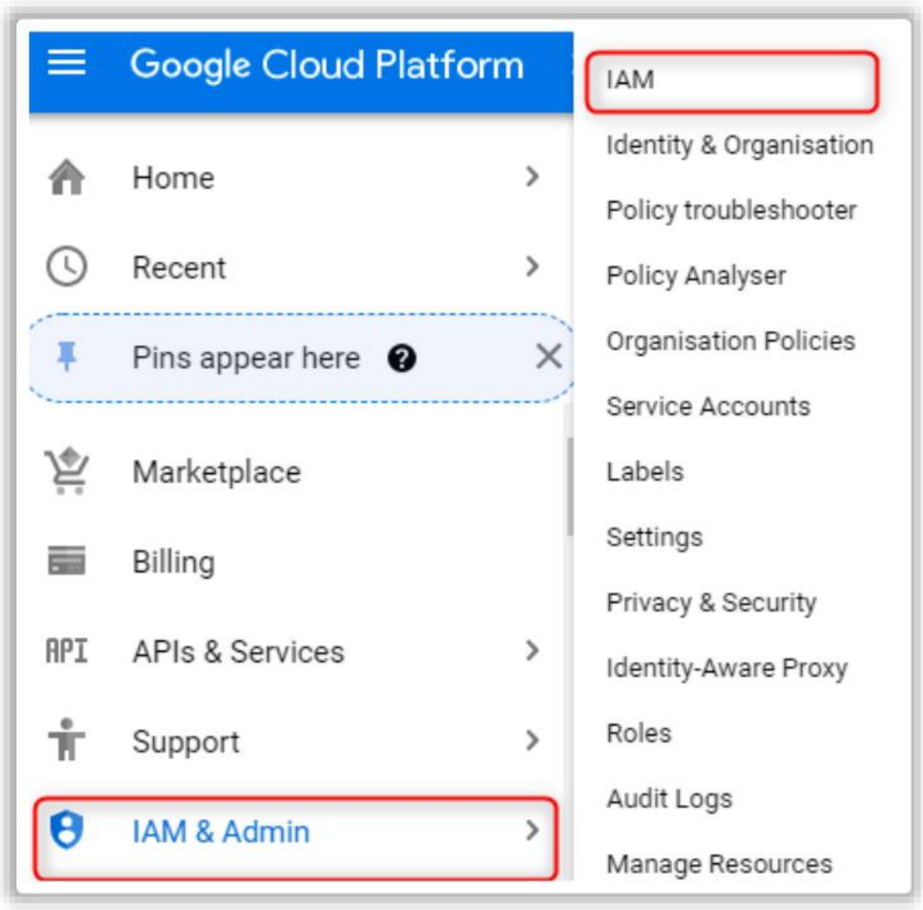


Figure 7.123: Navigating to IAM

hide01.ir

  - Click on **Add** in the **IAM** page.

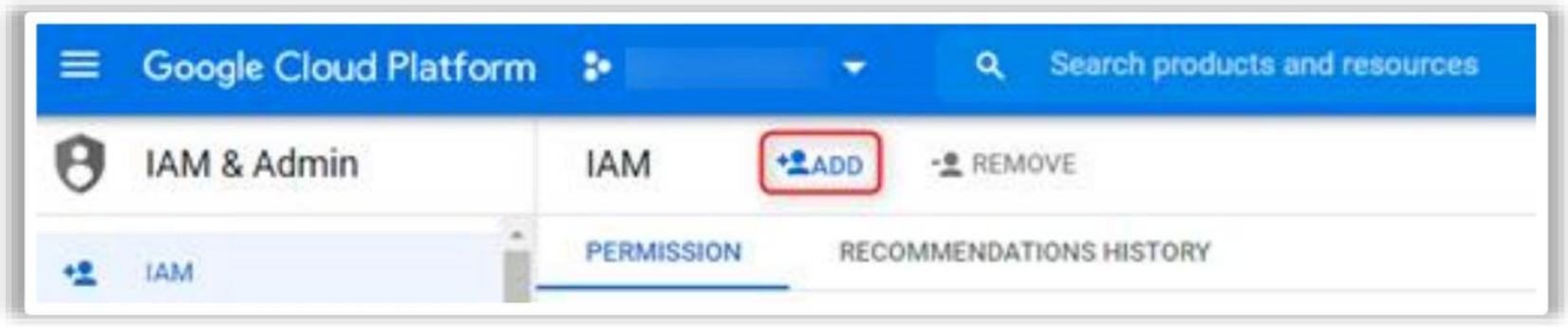


Figure 7.124: Adding Permissions

  - In the **Role** field for access to administer all resources belonging to the organization, select **Security Center Admin.**
  - Click on **Add Another Role** to assign **SCC IAM Role** to other users.
  - In the **Role** field for **Admin access** to security center, select **Security Center Sources Admin.**

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

- Click on **Save.**

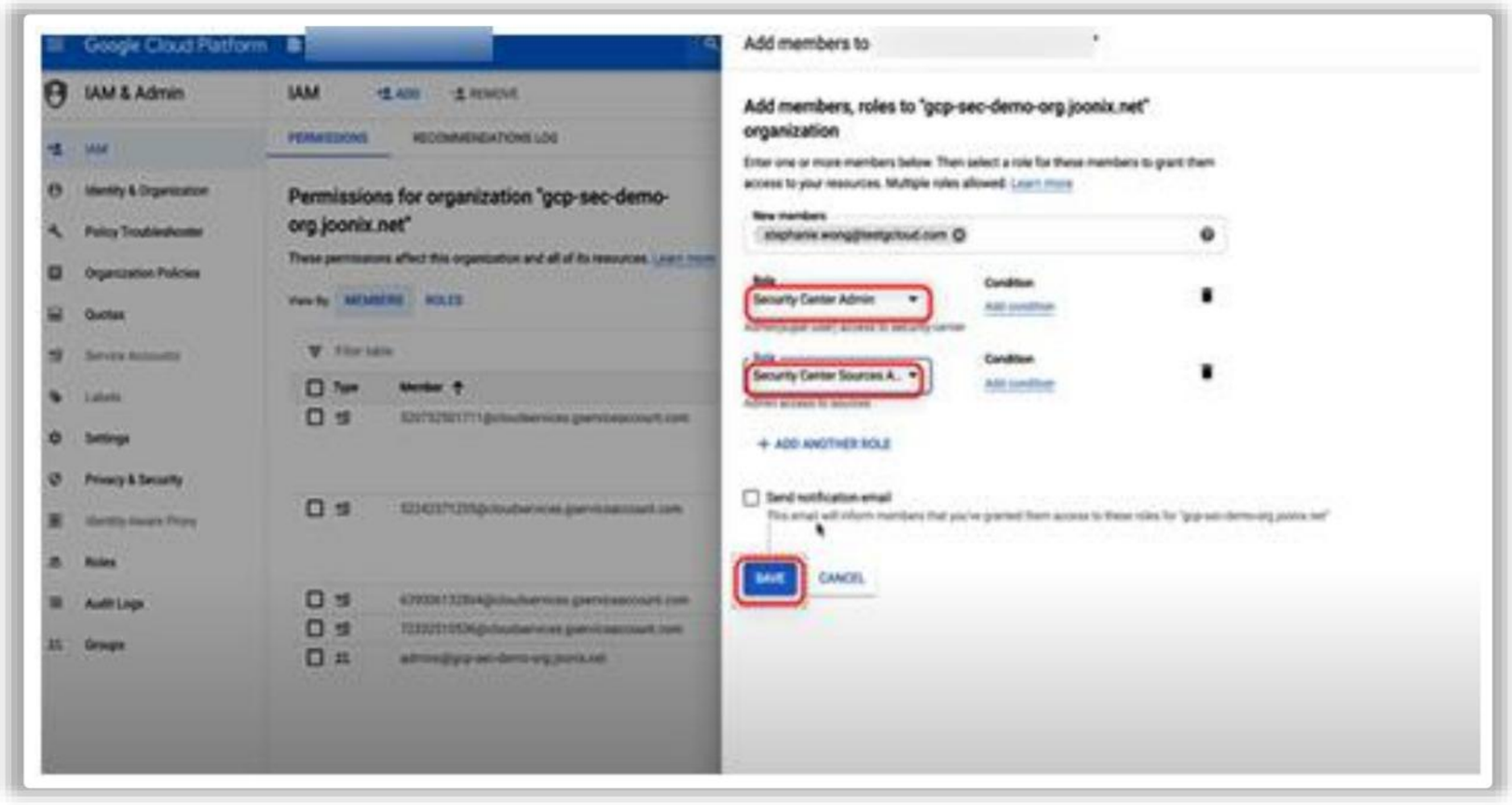


Figure 7.125: Adding Roles

- Navigate to **Security Command Center** in the dashboard and click on **Settings** to enable managed scans.

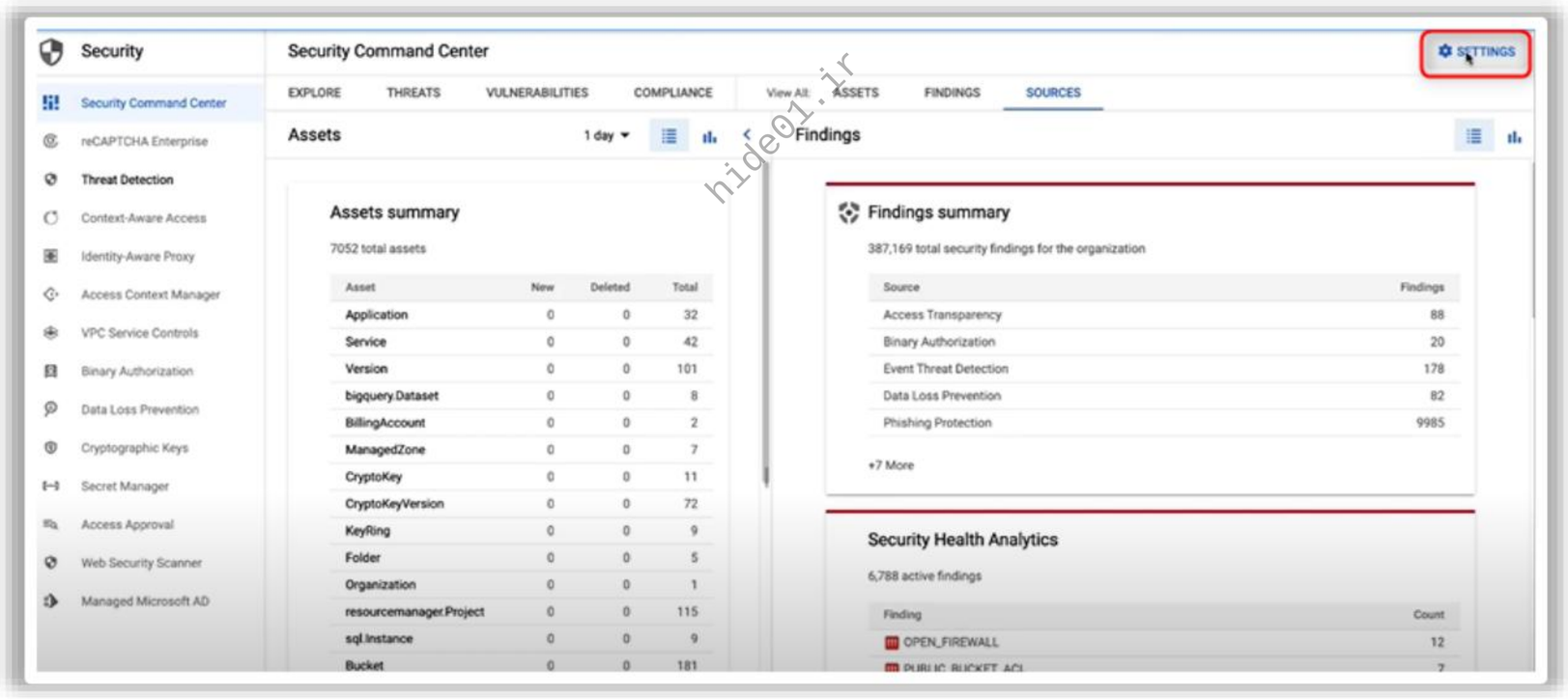


Figure 7.126: Navigating to Settings

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

- Turn on **Web Security Scanner** and click **Save.**

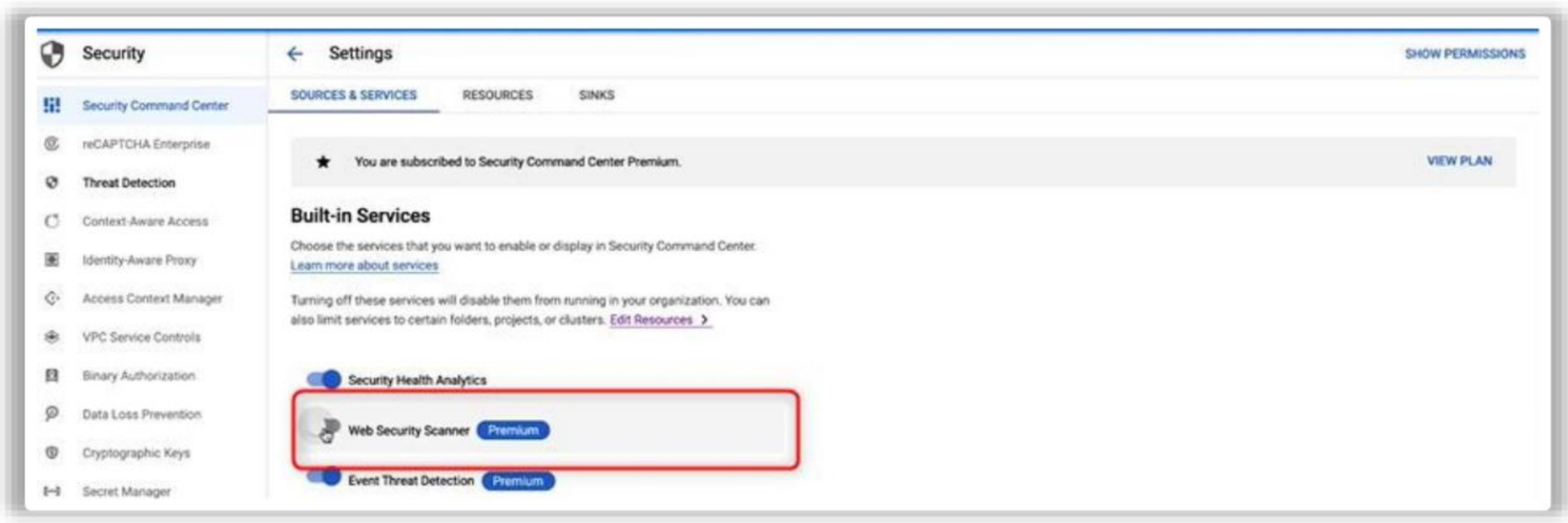


Figure 7.127: Turning On Web Security Scanner

Enable Custom Scans

- Navigate to **IAM & Admin** in the **Console** and select **IAM**.
- In the **Role** field for **Edit access** to all resources, select **Editor.**
- In the **Role** field for **Admin access** to security center, select **Security center Admin.**
- In the **Role** field for **Admin access** to sources, select **Security Center Sources Admin.**

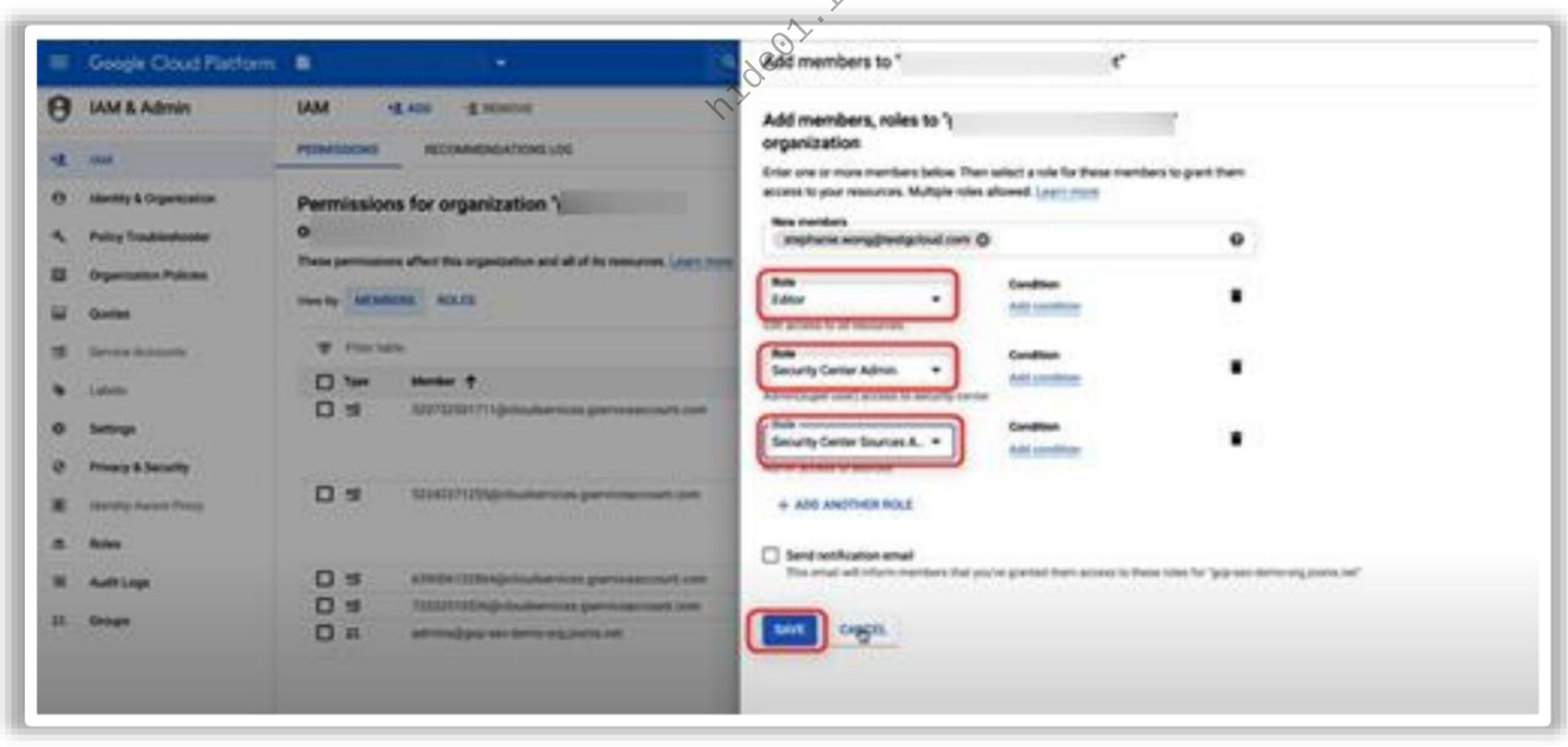


Figure 7.128: Enabling Custom Scans

- Make sure Web Security Scanner is enabled and the application to be tested is running on the public URL and IP.

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

- Navigate to **Web Security Scanner** in the console and select one of the projects.

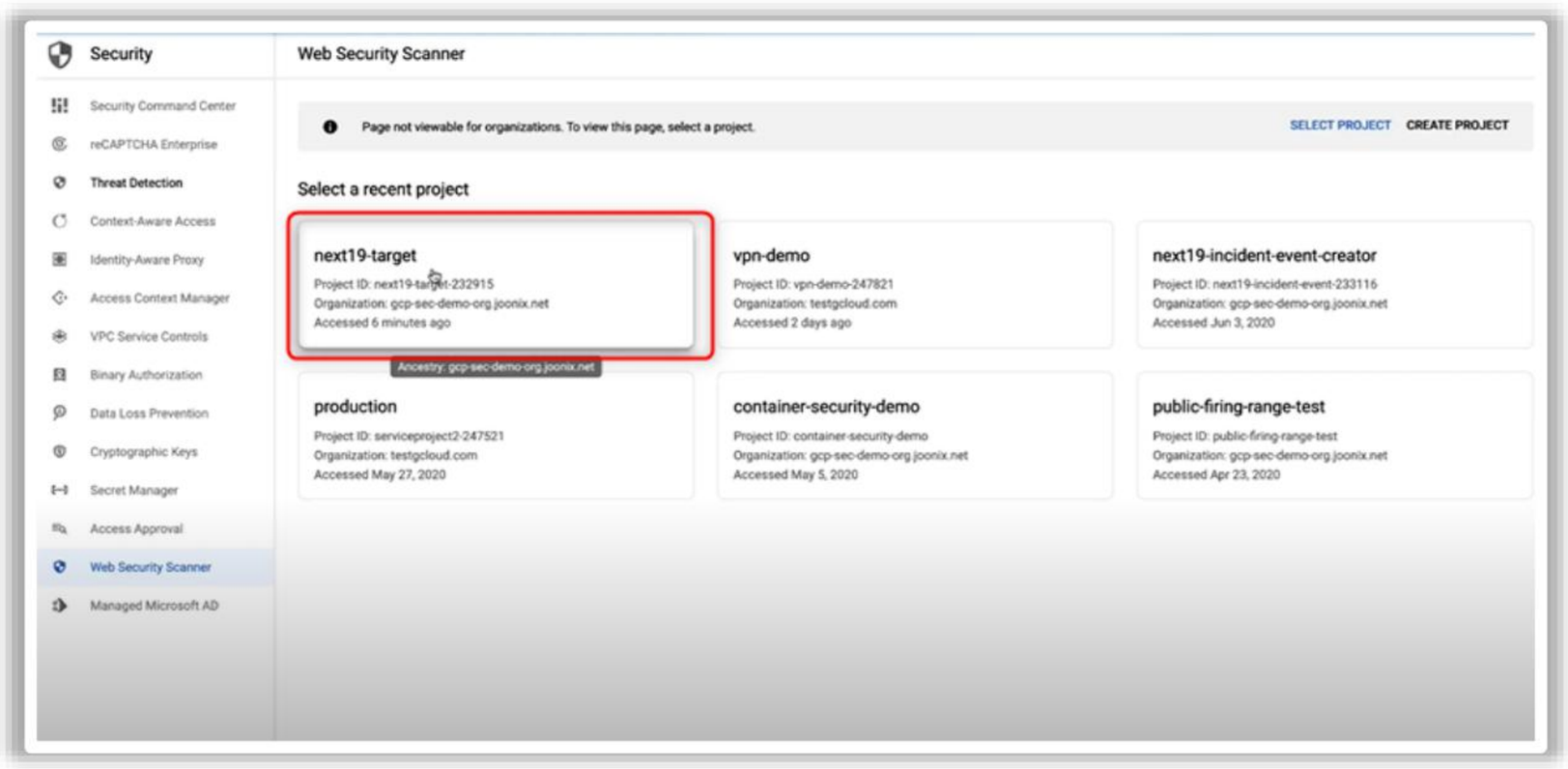


Figure 7.129: Navigating to Web Security Scanner

- **Step 2: Create, Save, and Run Scans**
  - Click on **New Scan.**

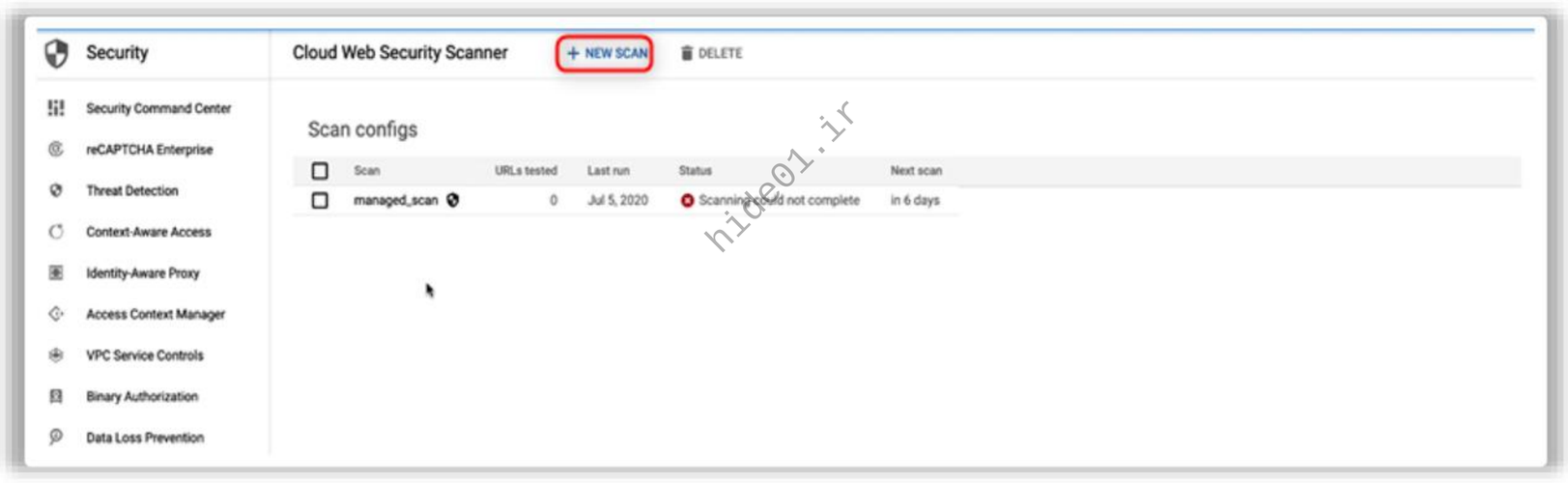


Figure 7.130: Selecting New Scan

  - Copy the URL of the application that needs to be tested under **Starting URLs.**
  - Select the **Authentication Method** as **Google Account** or **Cloud IAP**.
  - Select the **Schedule** of the scan.

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

- Click on **Save.**

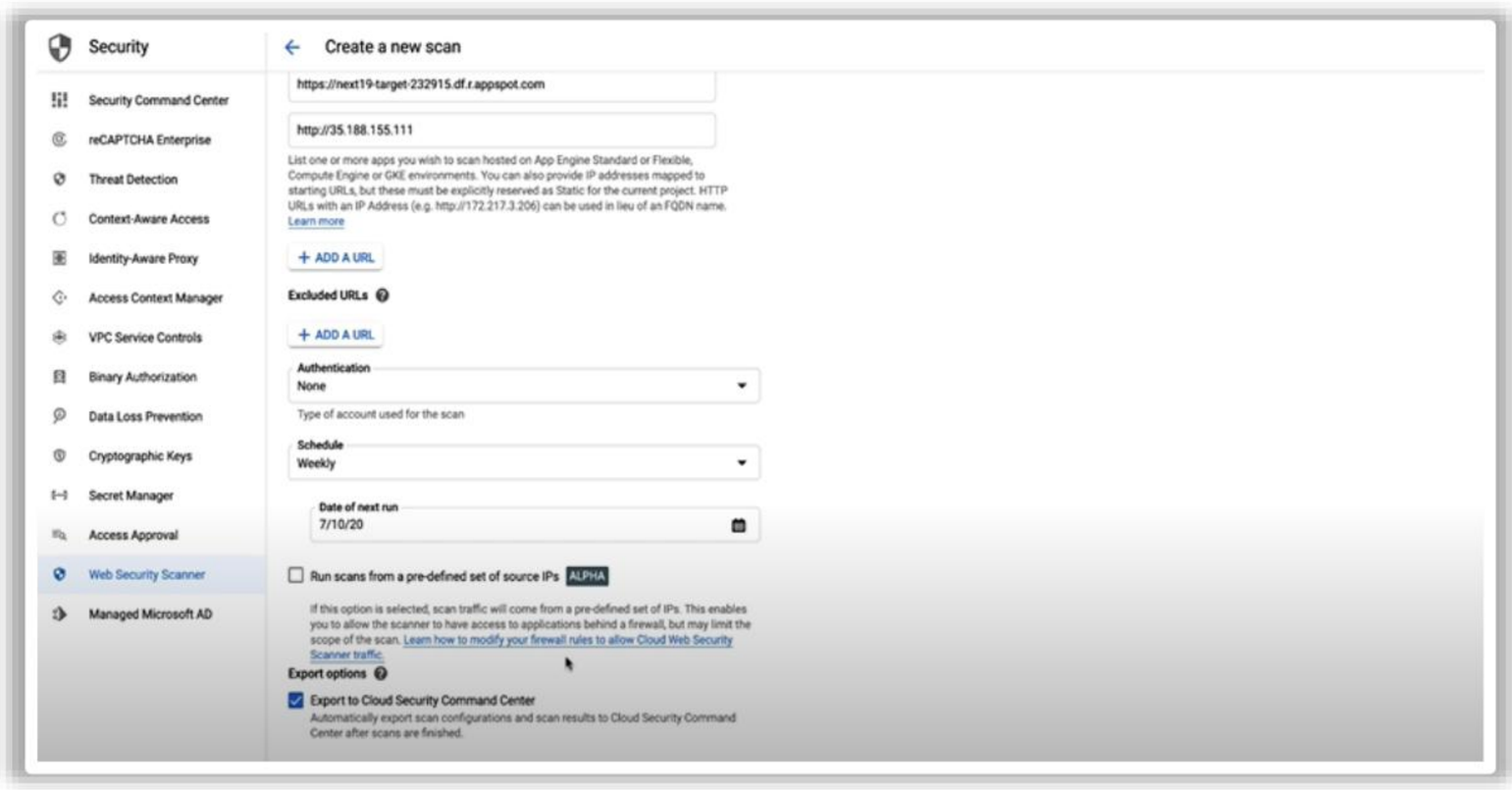


Figure 7.131: Creating a New Scan

- Click on **Run Scan.**

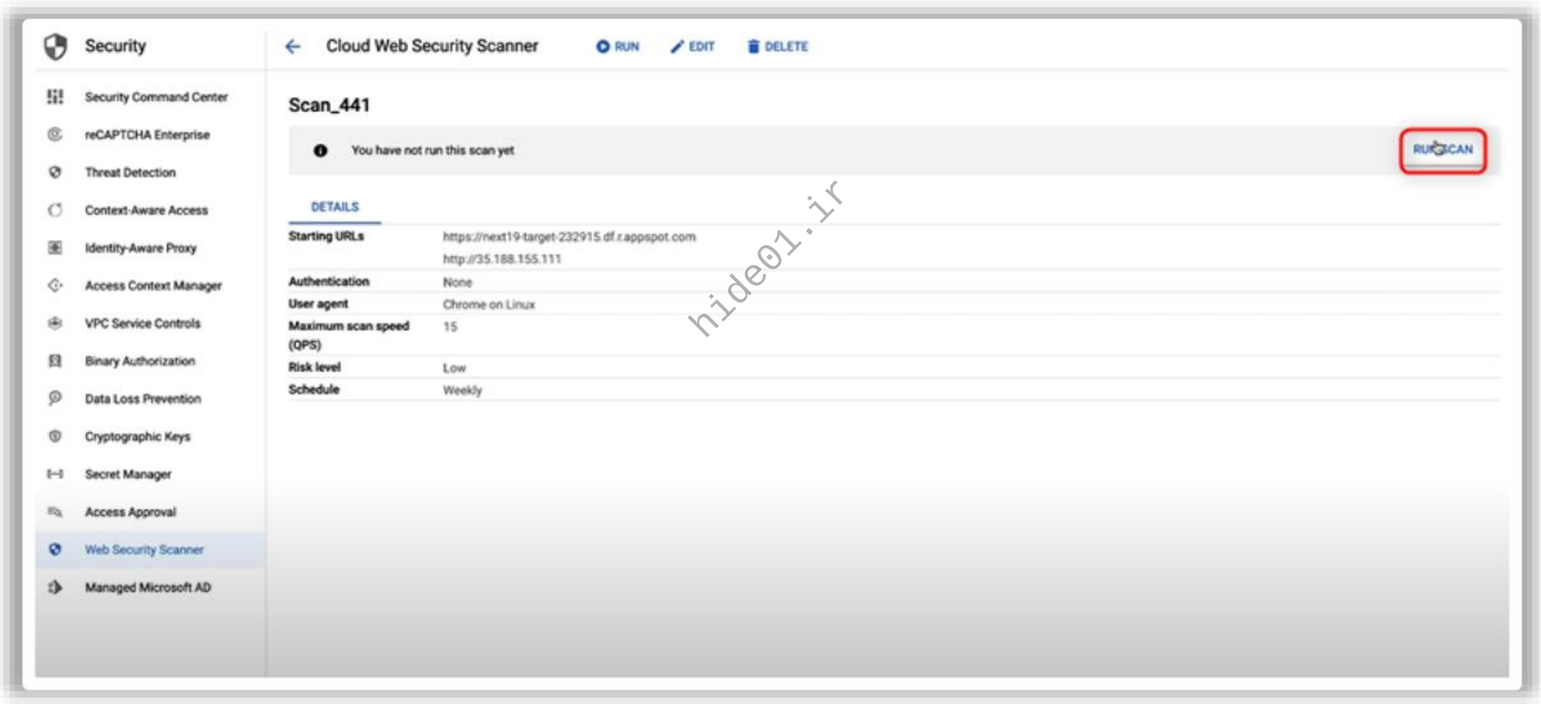


Figure 7.132: Running Scan

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

- After the scan is completed, the **scan** page displays the results.

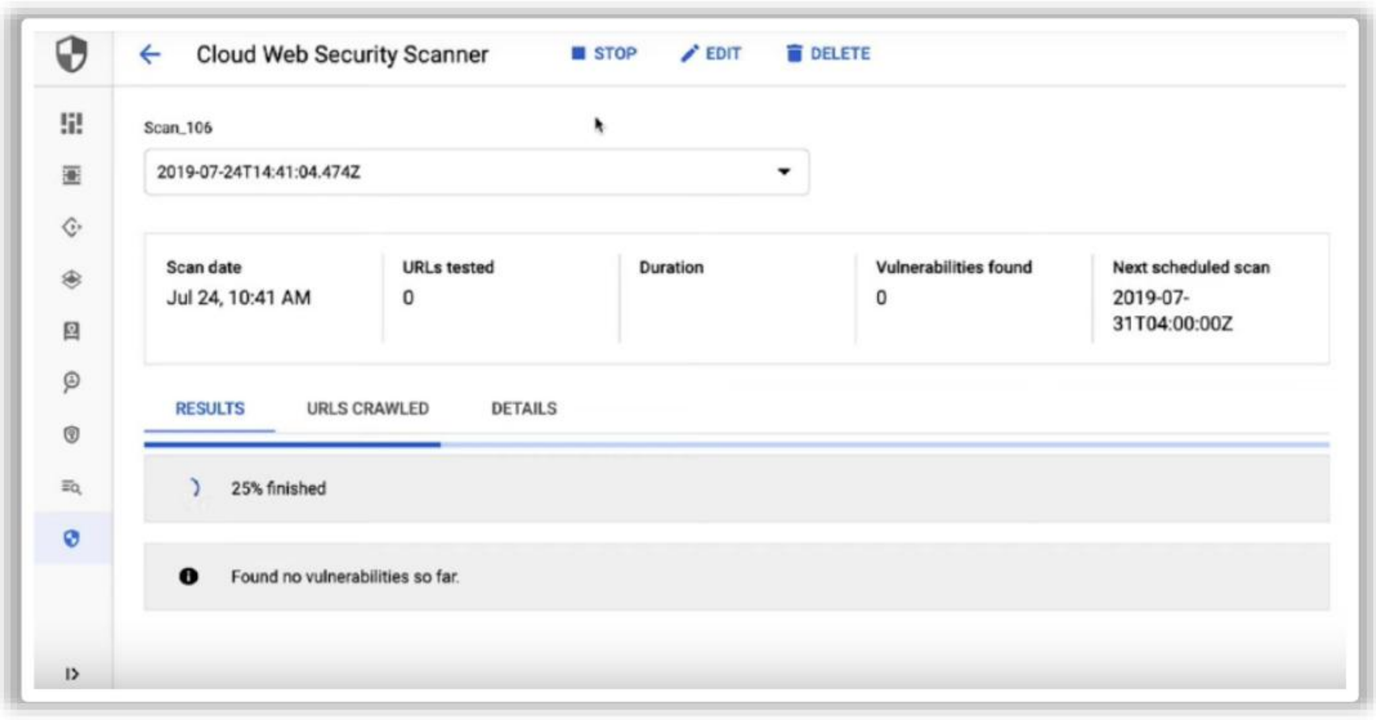


Figure 7.133: Scan Results

Step 3: Fix Vulnerabilities

- Navigate to the **Vulnerabilities** tab in the dashboard.

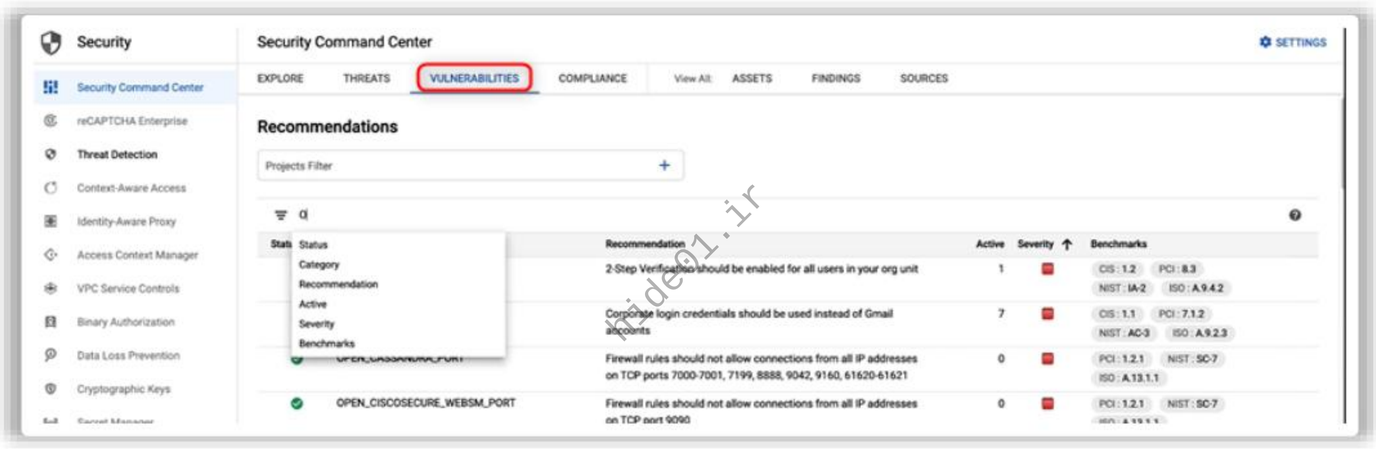


Figure 7.134: Navigating to Vulnerabilities

- Filter by the type of vulnerability in the **Projects Filter** field.

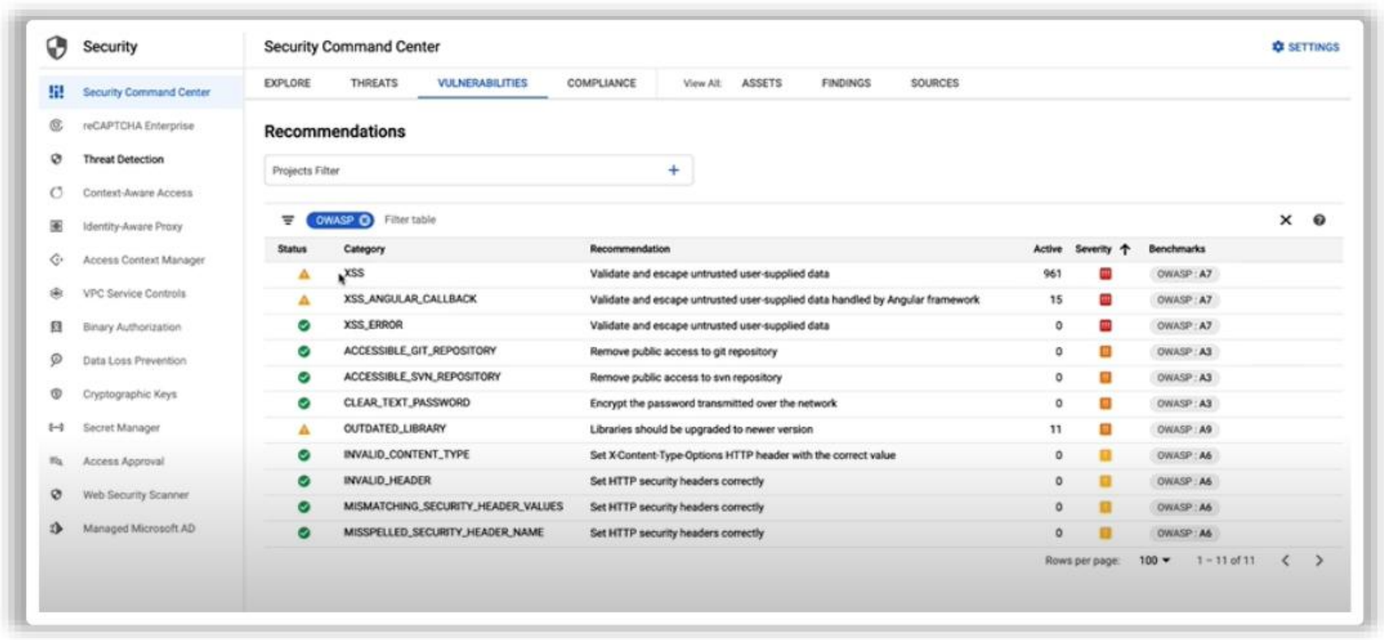


Figure 7.135: Using Project Filter

- A pop-up will display all details and remediation steps after clicking on a particular vulnerability.

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

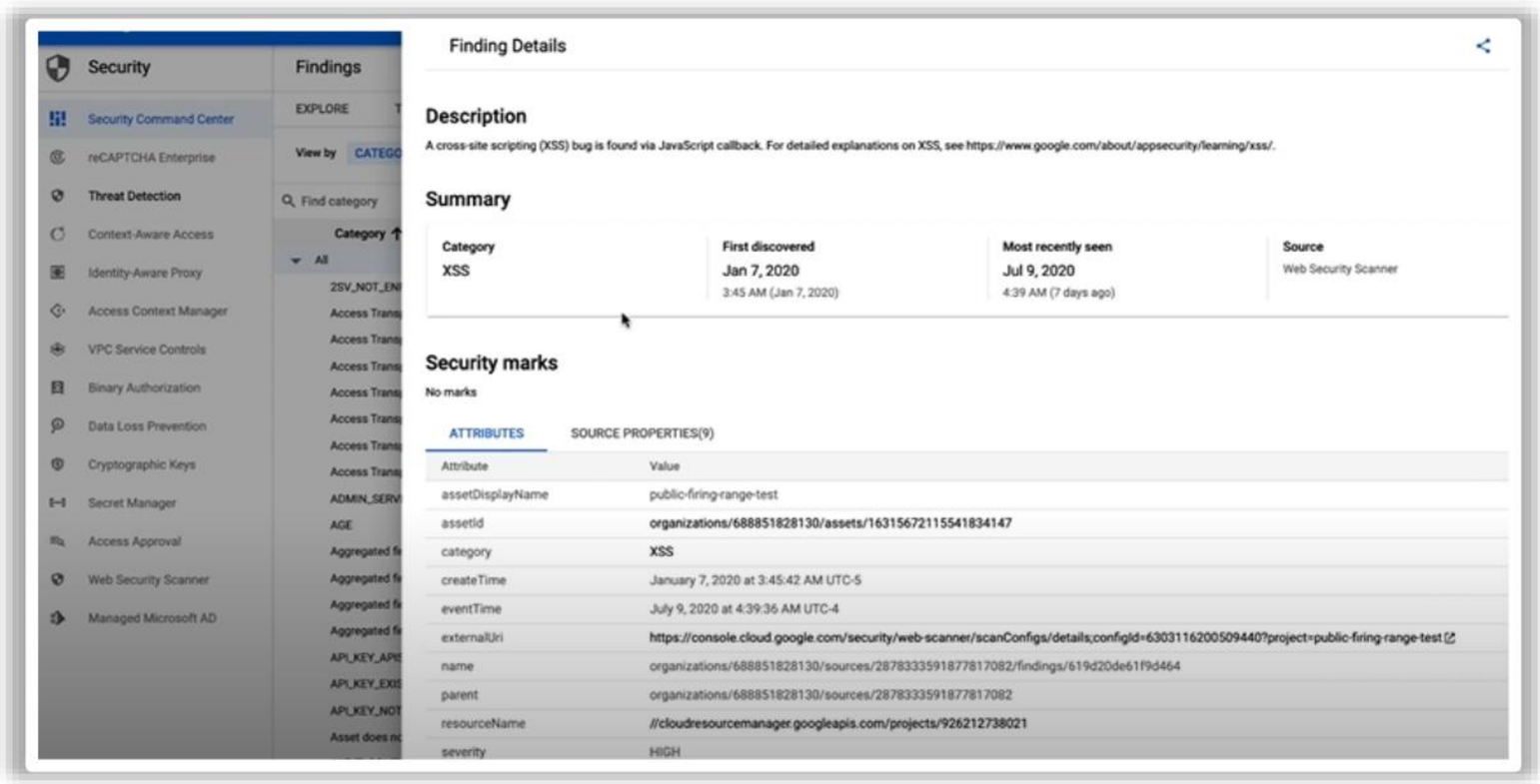


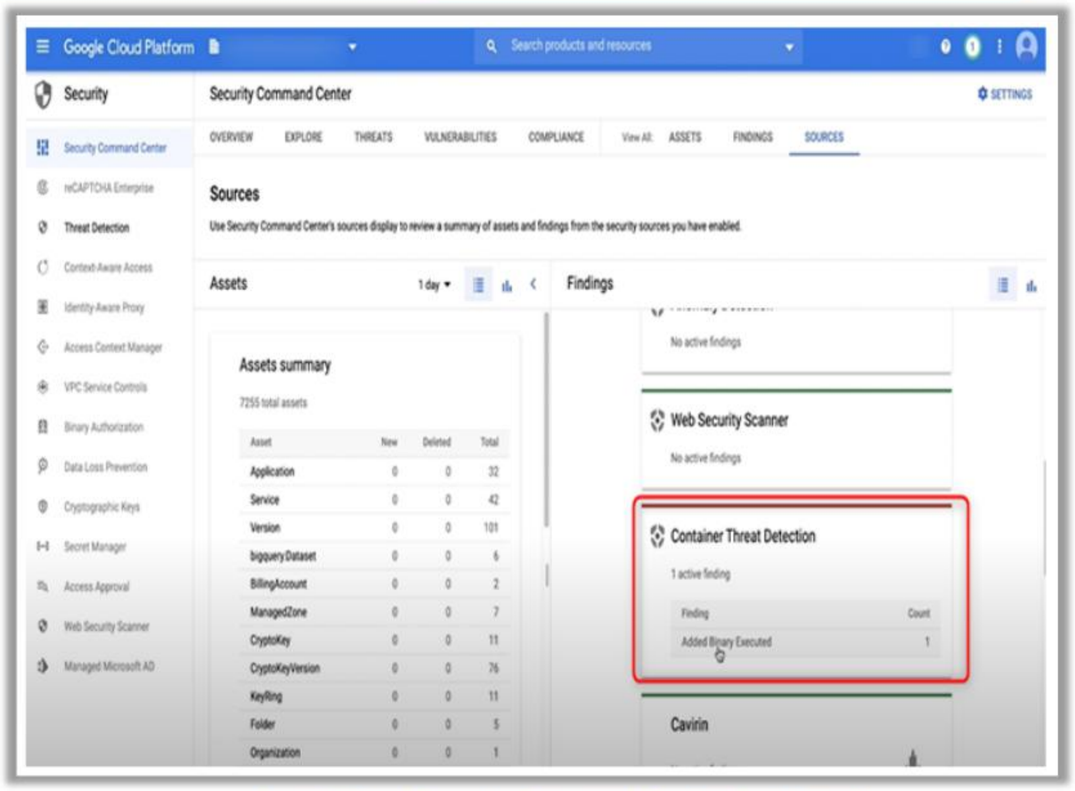
Figure 7.136: Details and Remediation Steps of a Vulnerability

hide01.ir

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

Setting Up Container Threat Detection in Security Command Center

- Container Threat Detection monitors the container images in real time to detect attacks and send alerts
- In Container Threat Detection, the low-level behavior in a guest kernel is collected to detect events
- Added Binary Executed Detector searches for an executed binary that was not included in the original container image
- Added Library Loaded Detector searches for a binary that is being executed but was not included in the original container image
- Reverse Shell detector searches for a stream redirection to a remote-controlled socket



Google Cloud Security Command Center dashboard

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

Setting Up Container Threat Detection in Cloud Security Command Center

Container images are monitored in real-time by the built-in Container Threat Detection service to detect run-time attacks and their related alerts. The low-level behavior in a guest kernel is collected to detect events. The event information is passed to a detector service, which determines whether it indicates an incident. A confirmed event (an incident) is posted as a finding in SCC. The types of container threat detectors are

- **Added Binary Executed:** The added binary executed detector searches for an executed binary that was not included in the original container image.
- **Added Library Loaded:** The added library loaded detector searches for a binary that is being executed but was not included in the original container image.
- **Reverse Shell:** The reverse shell detector searches for stream redirections to a remote-controlled socket.

Steps to Set Up Container Threat Detection in Cloud SCC

- **Step 1: Enable Container Threat Detection**
  - Navigate to **IAM & Admin** in the console and click on **Add.**
  - Add **Admin access** to security center **Role** as **Security Center Admin.**
  - Click on **Add Another Role** and add **Security Center Sources Admin** as the **Role.**

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

- Click **Save.**

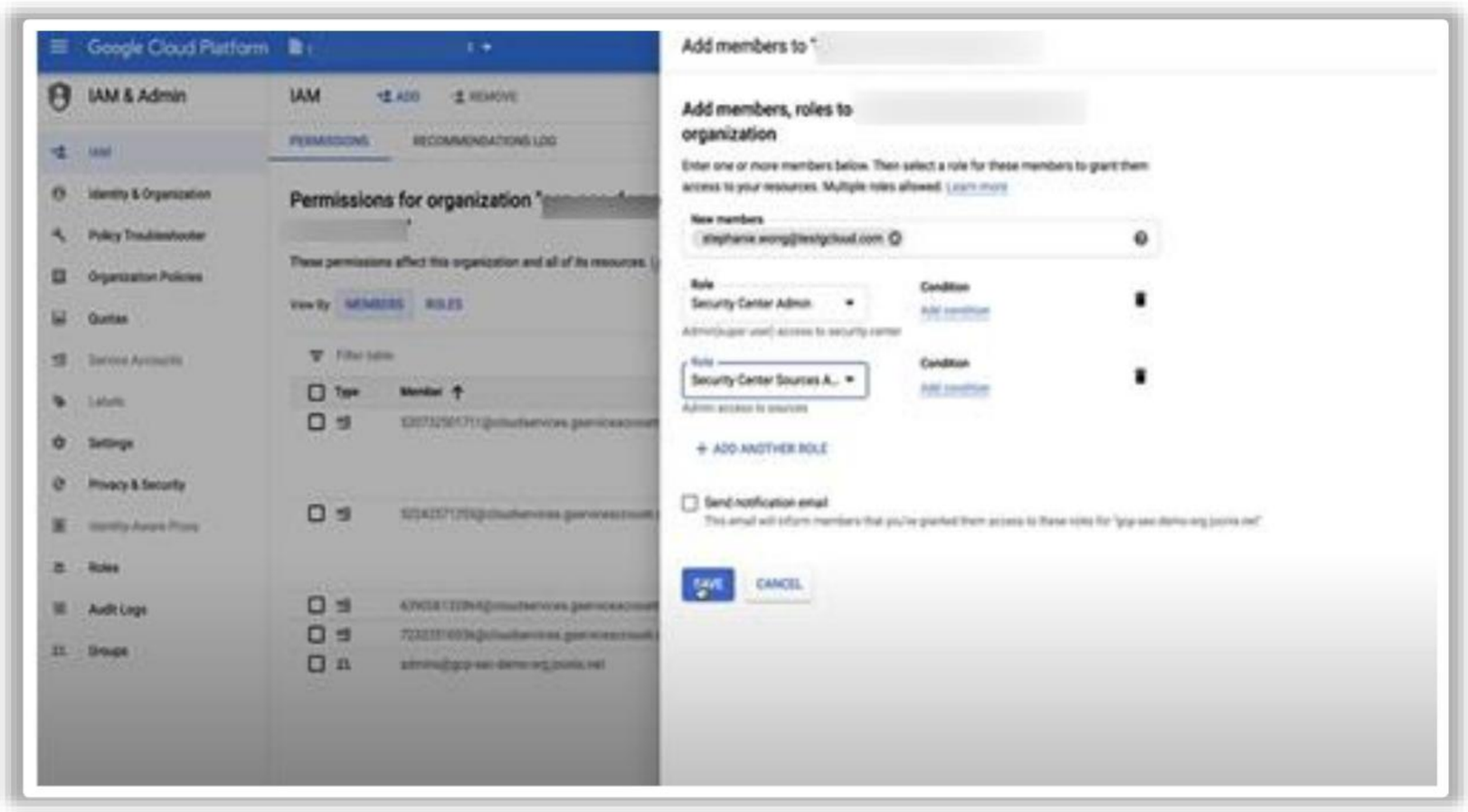


Figure 7.137: Adding Roles and Members

- Navigate to **Security Command Center** in the console and click on **Settings.**
- Click on **Sources & Services** and turn on **Container Threat Detection.**

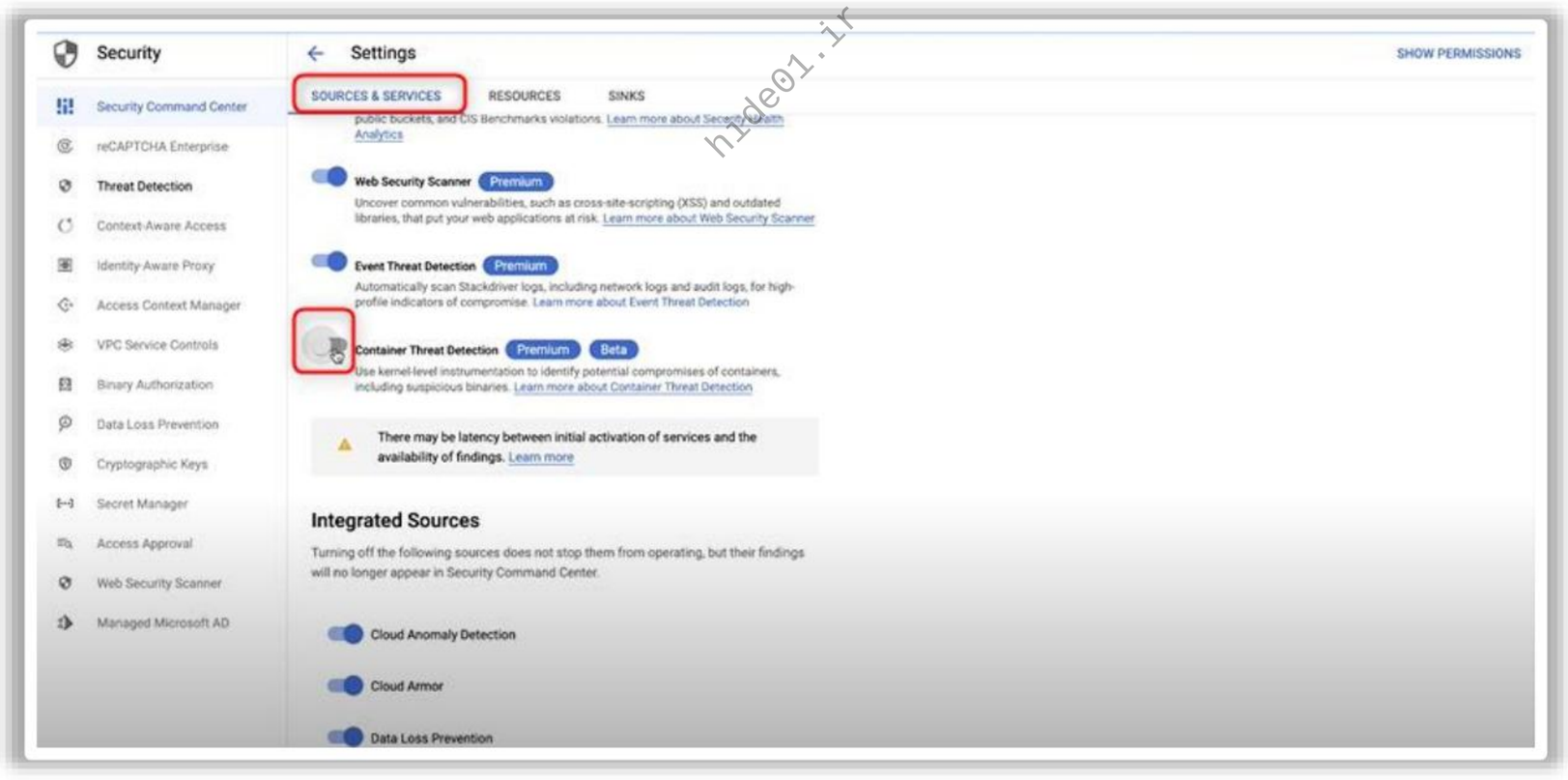


Figure 7.138: Container Threat Detection

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

- Once **Container Threat Detection** is enabled, the findings will be displayed in **SCC Dashboard**.

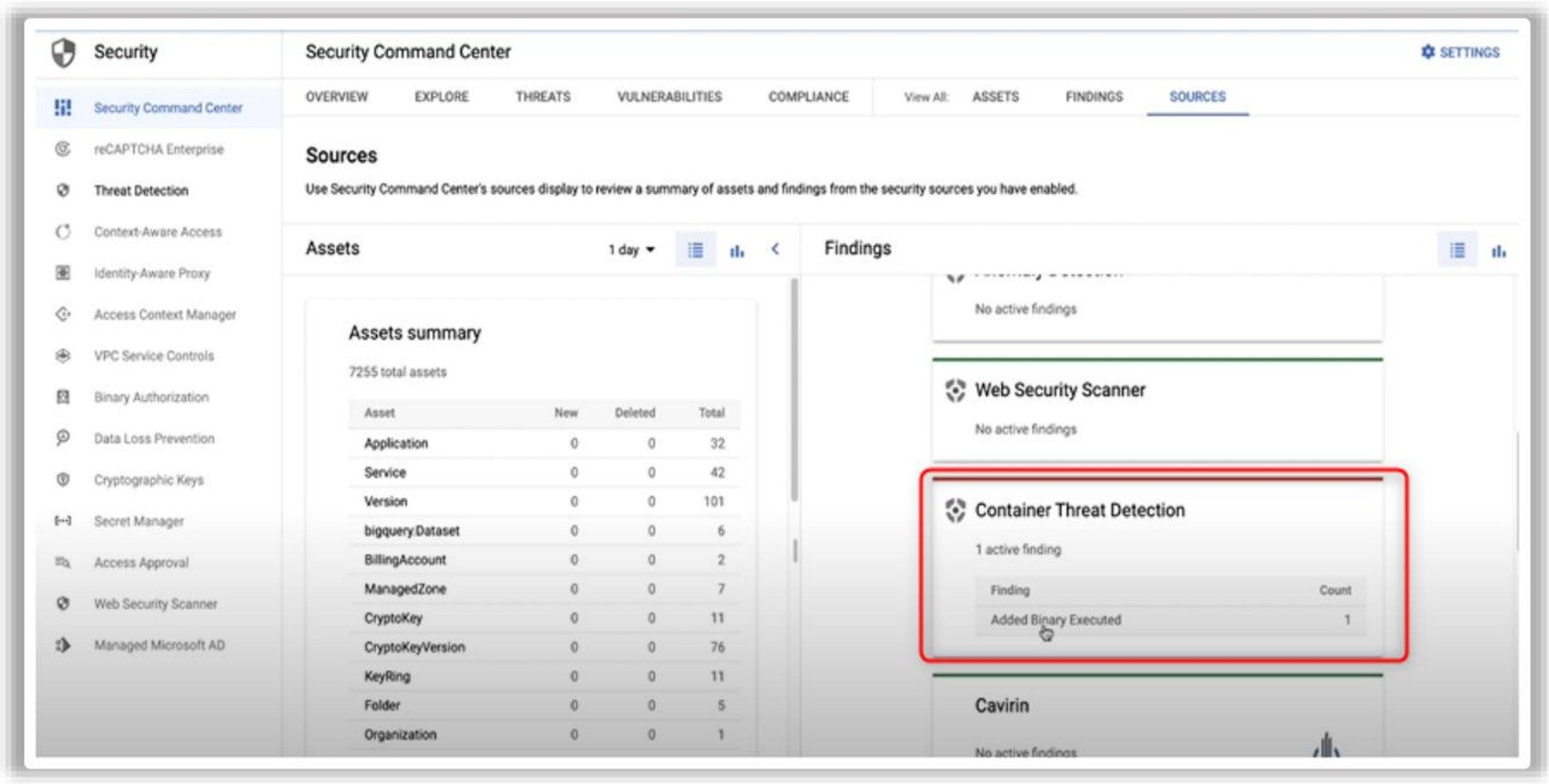
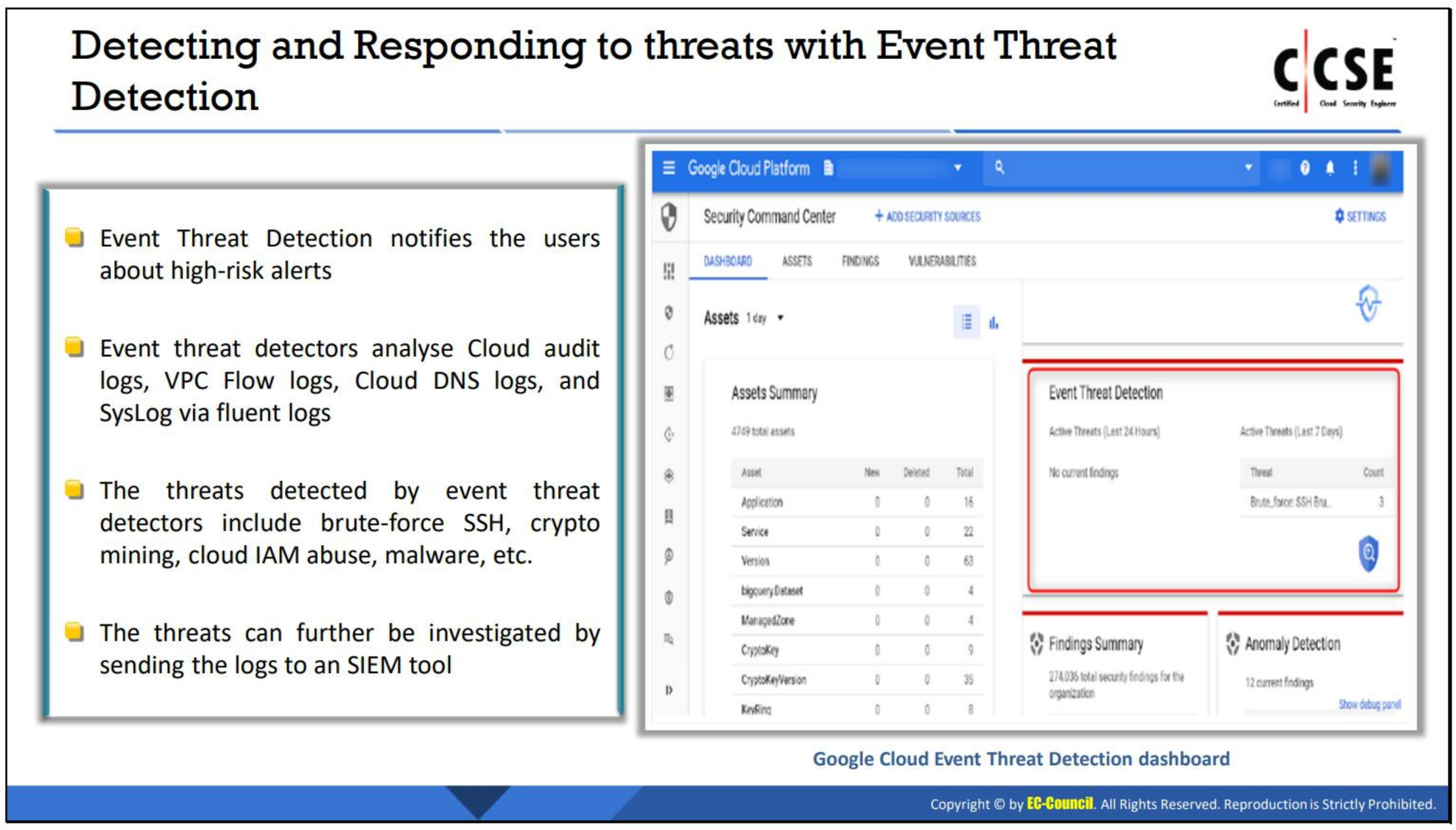


Figure 7.139: SCC Dashboard Showing Findings

hide01.ir

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



Detecting and Responding to Threats with Event Threat Detection

Event threat Detection performs the real-time monitoring of an organization's Cloud Audit logs, VPC Flow Logs, Cloud DNS and Syslog via Fluentd logs, and detects threats by applying a detection logic, threat intelligence, and the information from these logs. Event Threat Detection logs are automatically available in the console. It notifies users about high-risk alerts. The following types of threats can be detected:

- **Brute-force SSH:** Event Threat Detection examines Linux auth logs for failures and detects any brute-force SSH attempts.
- **Crypto Mining:** Event Threat Detection examines VPC logs, and thus, can detect coin mining malware.
- **Cloud IAM Abuse:** The addition of accounts from outside the organization's domain are detected by Event Threat Detection.
- **Malware:** Event Threat Detection examines VPC Flow logs and Cloud DNS logs for connections to bad domains to detect malware.
- **Phishing:** Event Threat Detection can detect phishing attempts by examining VPC Flow logs for a connection to known phishing domains.
- **Outgoing DDoS Attacks:** Outgoing DDoS attacks are detected by Event Threat Detection by examining the size, type, and number of VPC Flow logs.

These threats can be further investigated by sending the logs to an SIEM tool.

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

Steps To Detect and Respond to Threats Using Event Threat Detection With Cloud SCC

- **Step 1: Monitor Event Threat Detection logs**
  - Navigate to the **Security Command Center** dashboard.

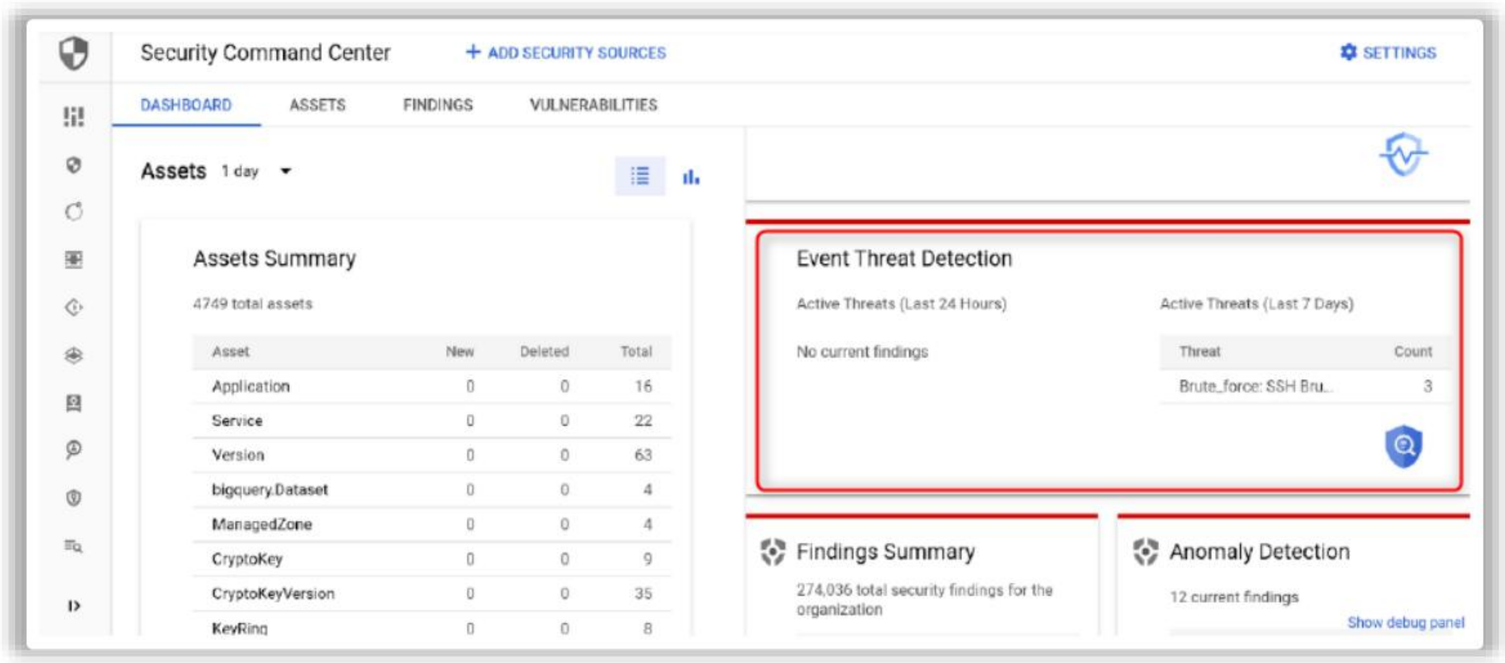


Figure 7.140: Navigating to Security Command Center

  - Click on a threat to get more details regarding the findings.
  - Click on **Event Threat Detection** to get the recent logs.

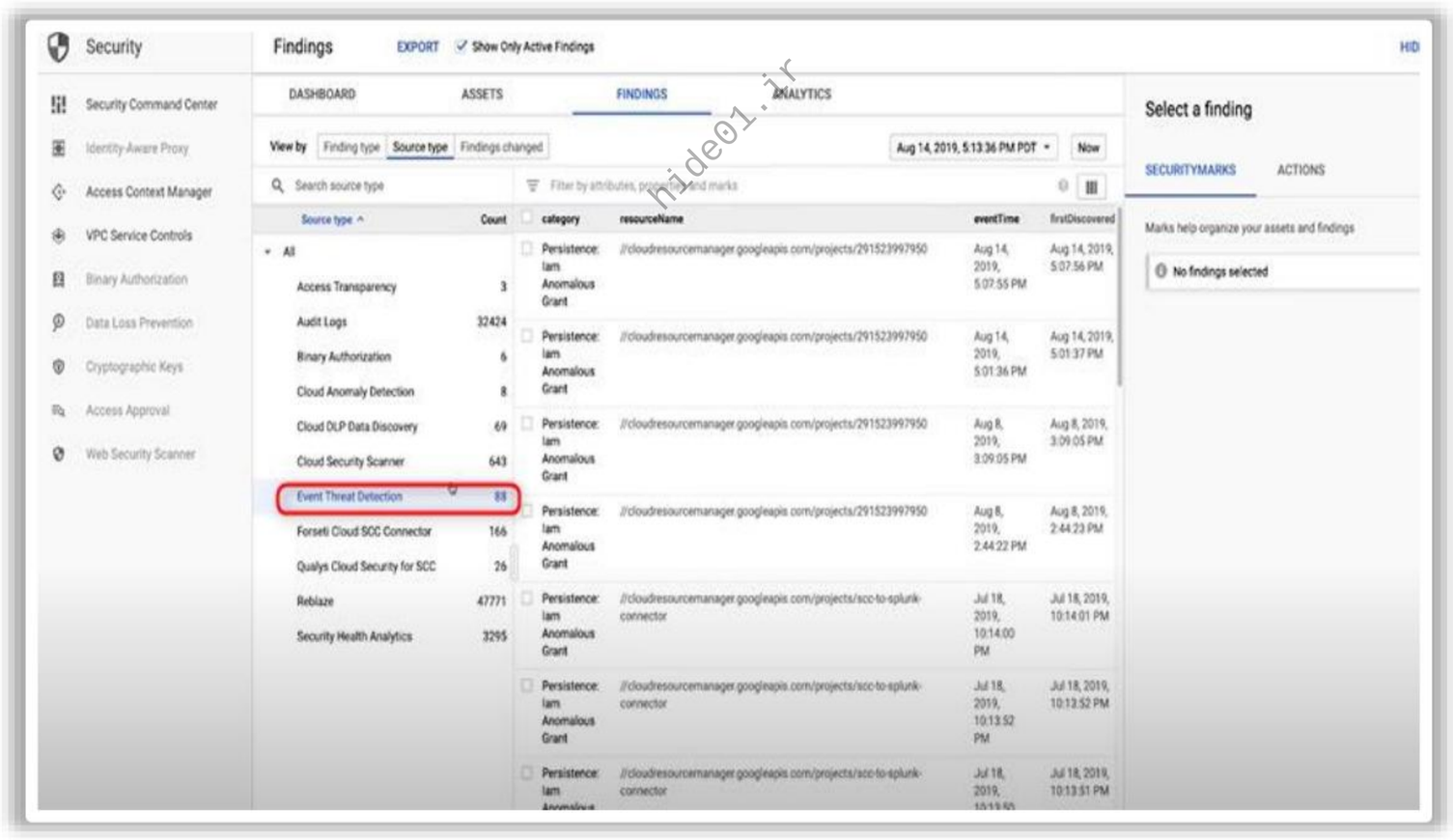


Figure 7.141: Event Threat Detection

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

- **Step 2: Remediate Threats**
  - Click on one of the findings under **category.**

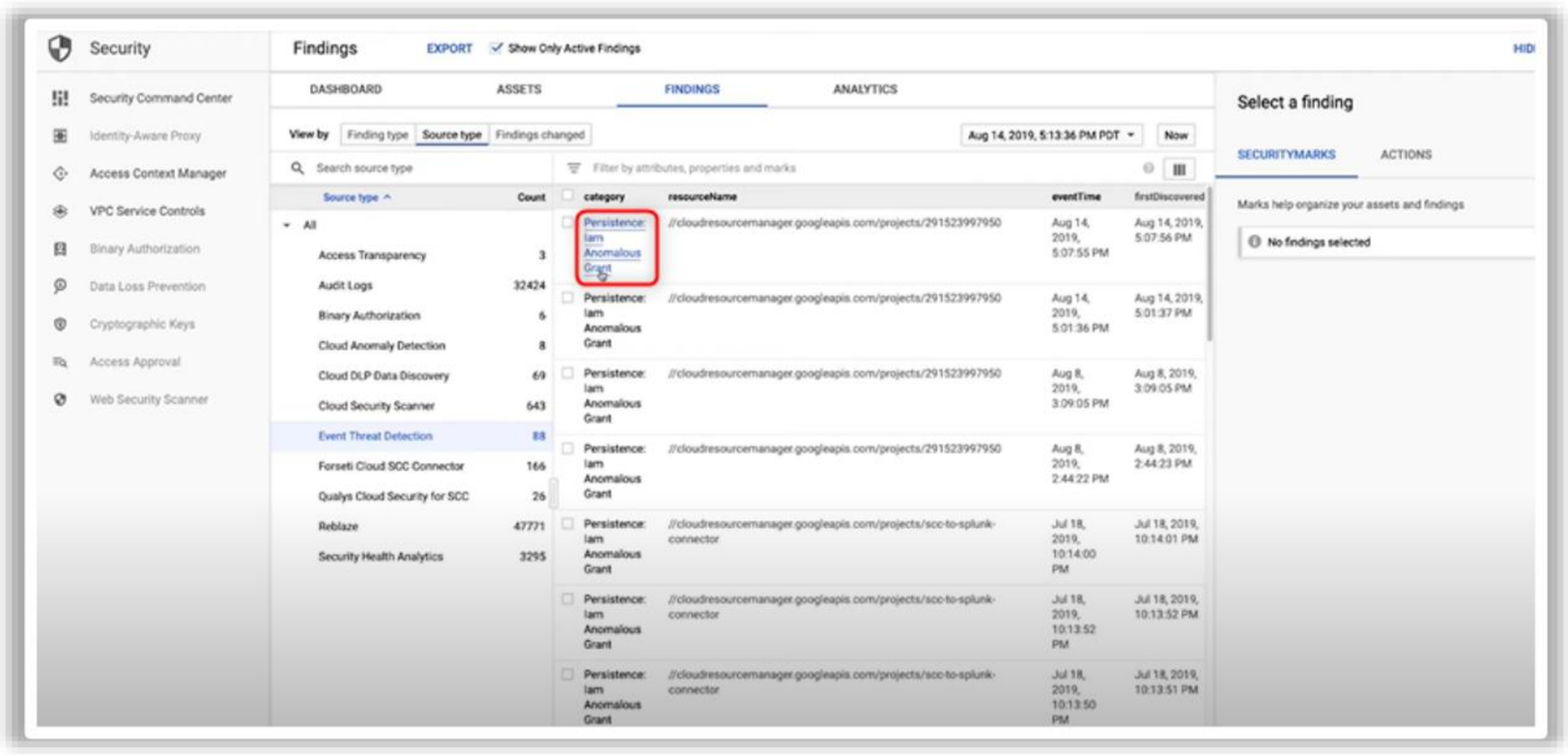


Figure 7.142: Navigating to Findings

- A pop-up will display the details of a threat, such the event time, source, priority, and actions taken.

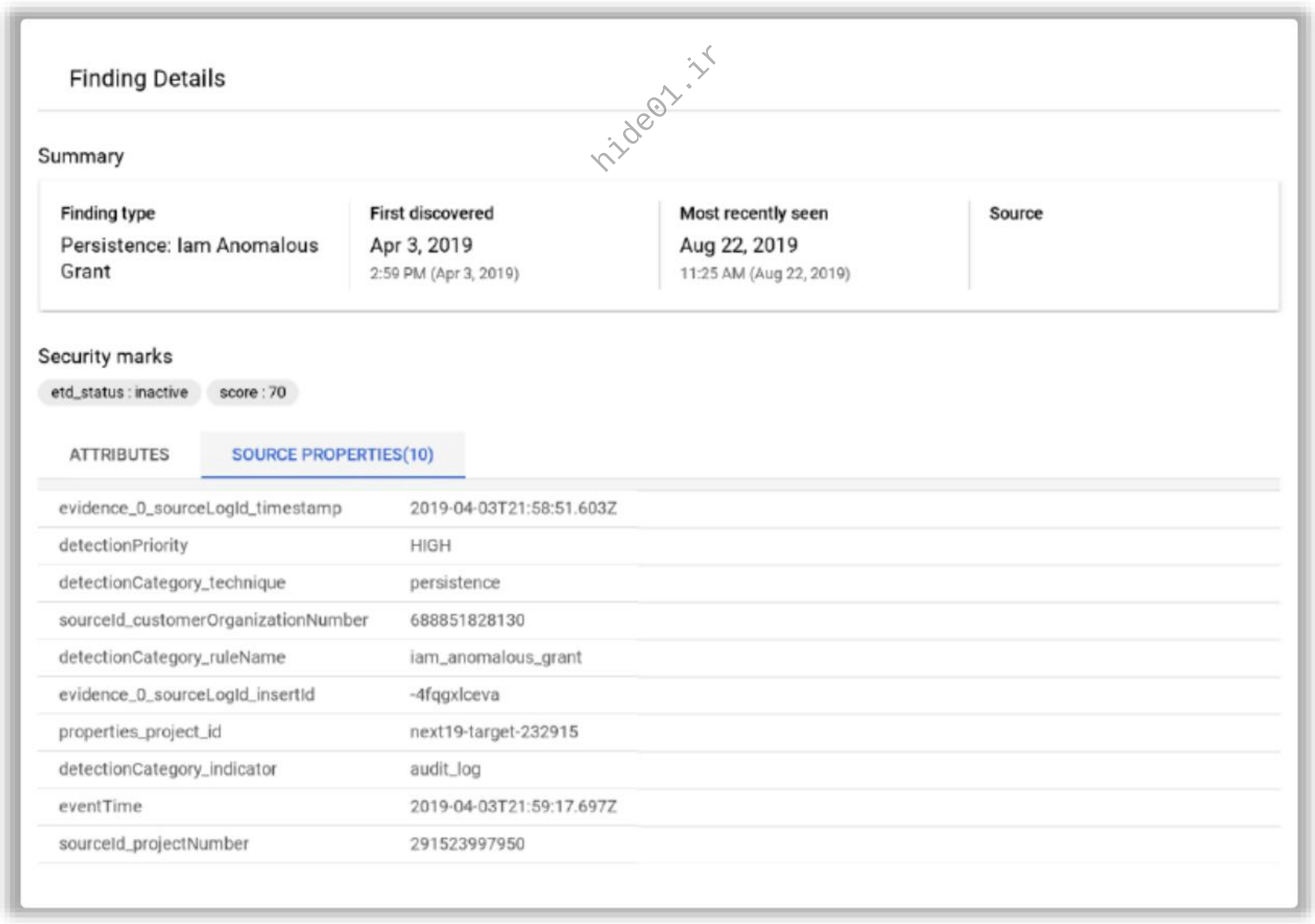
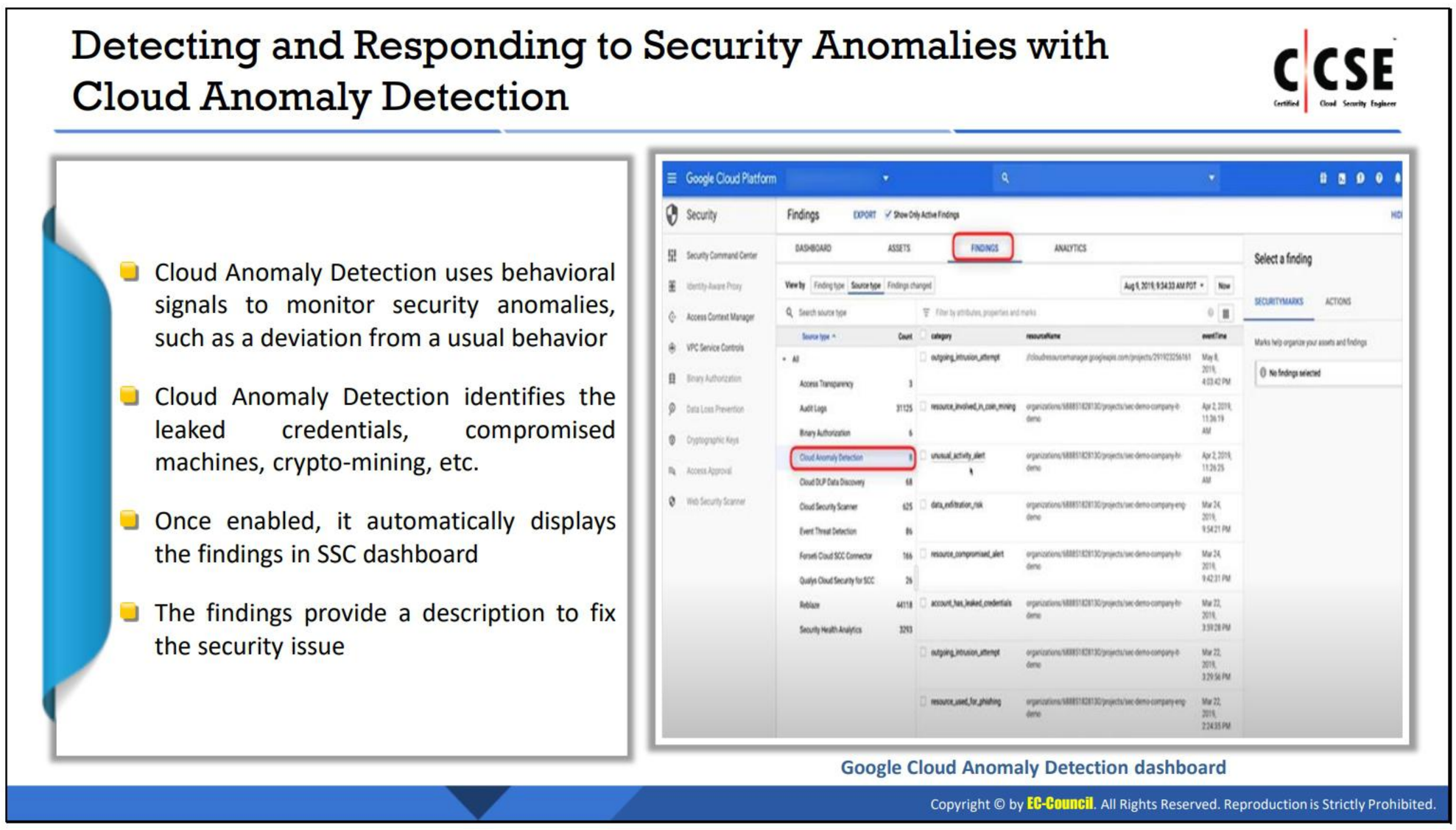


Figure 7.143: Details of a Threat

The threat can further be investigated by sending the logs to an SIEM tool. The logs can be exported using a Splunk connector.

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



Detecting and Responding to Security Anomalies with Cloud Anomaly Detection

Cloud Anomaly Detection uses behavioral signals to monitor security anomalies, such as a deviation from a usual behavior. Once Cloud Anomaly Detection is enabled, the findings will be automatically displayed in the SCC dashboard. These findings provide a description for fixing the security issue. The anomalous security findings detected by Cloud Anomaly Detection are

- **Leaked Account Credentials:** Cloud Anomaly Detection detects unintentionally leaked GCP service account credentials.
- **Resources Utilized for Outbound Intrusions:** Various resources that are used for intrusions, such as brute-force SSH, port scan, and brute-force FTP
- **Compromised Machine:** The compromise of a resource in the organization
- **Crypto Mining:** The behavioral signals in a VM indicate illegal crypto mining activities.
- **Unusual Activities:** A deviation from the normal activity in an organization
- **Resource Used for Phishing:** The resources in an organization that could be used for phishing activities

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

Steps to Detect and Respond to Security Anomalies with Cloud Anomaly Detection

- **Step 1: Enable Cloud Anomaly Detection**
  - Navigate to **IAM & Admin** and select **IAM** in the console.

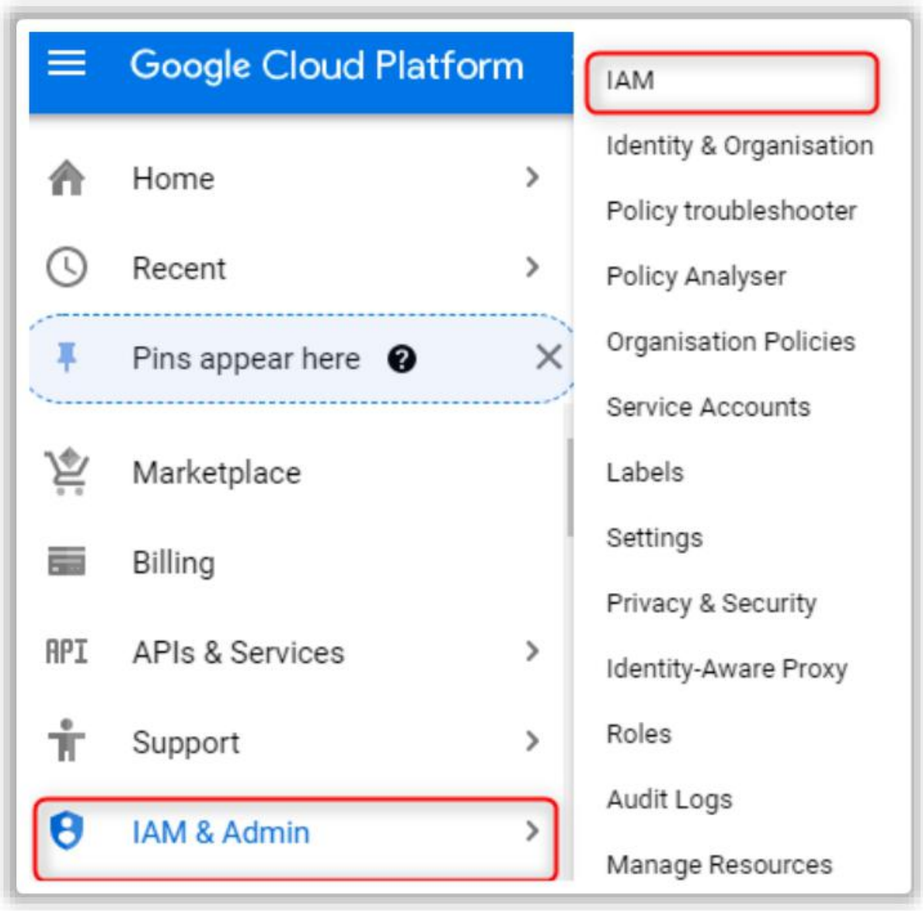


Figure 7.144: Navigating to IAM

  - Click on **Add** in the **IAM** page.

hide01.ir

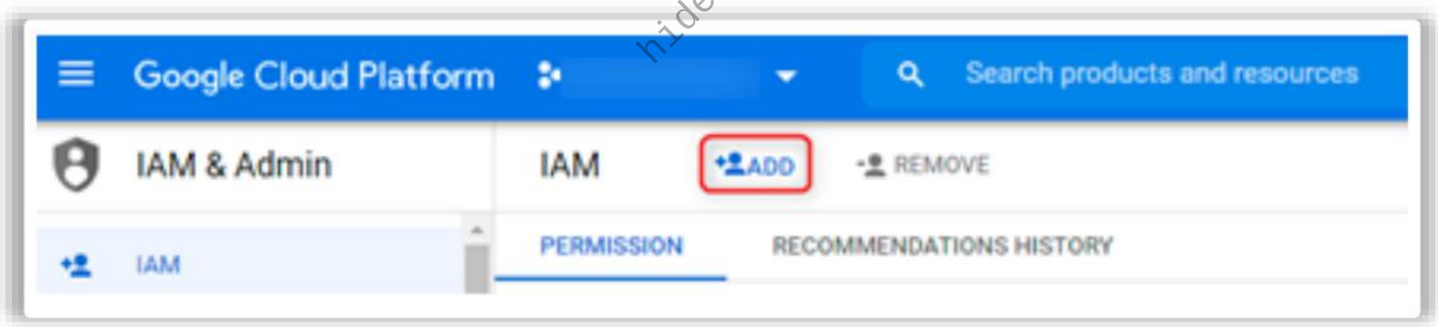


Figure 7.145: Adding Permissions

  - In the **Role** field for Access to administer all resources belonging to organization, select **Organization Administrator** and click on **save**.

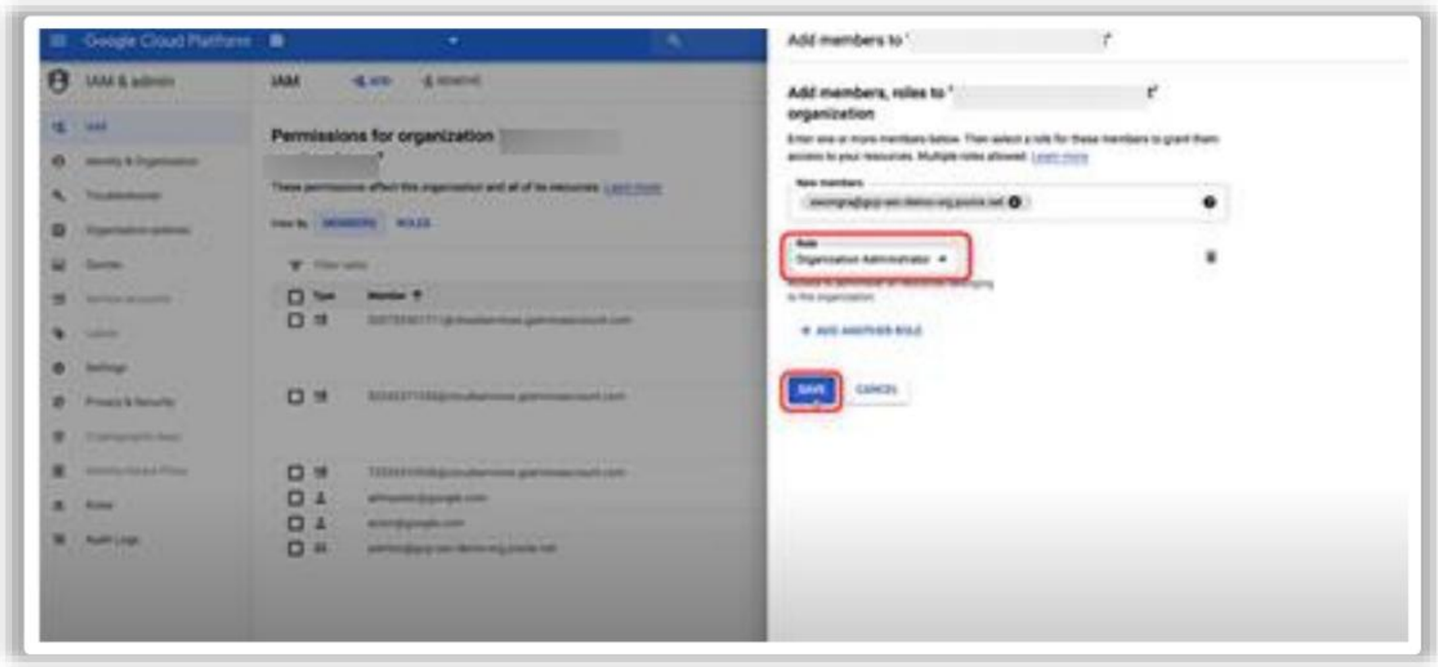


Figure 7.146: Choosing Organization Administrator

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

- Navigate to **Security Command Center** in the console and click on **settings** to enable Cloud Anomaly Detection.

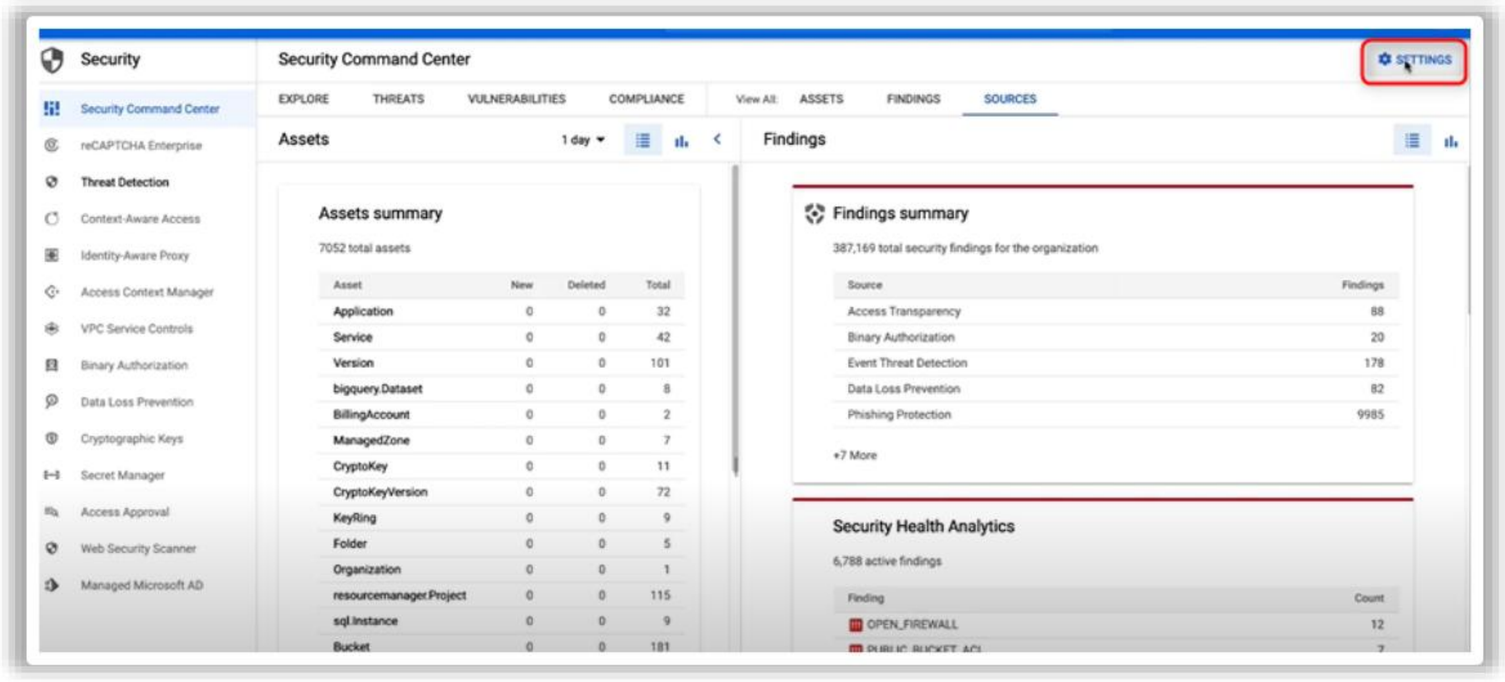


Figure 7.147: Navigating to Settings

- Click on **Security Sources** and turn on **Cloud Anomaly Detection** to enable it.

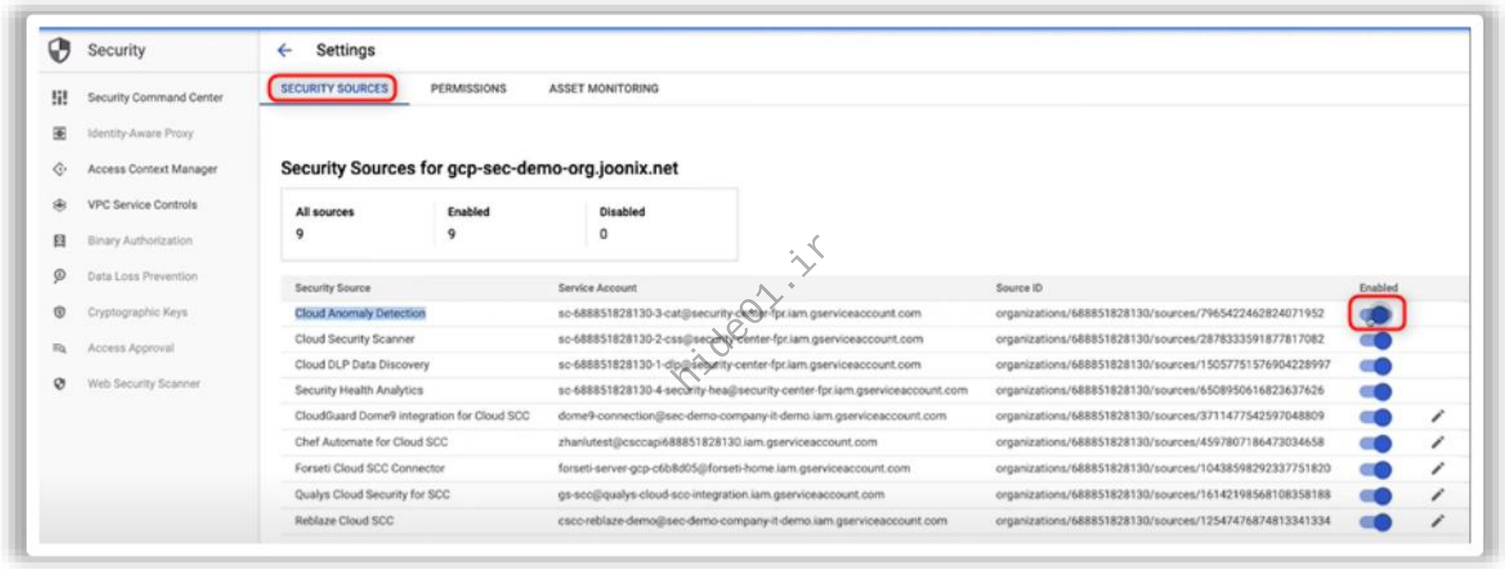


Figure 7.148: Turning on Cloud Anomaly Detection

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

- Click on the **Findings** tab in Security Command Center; for **Cloud Anomaly Detection,** it will display all anomalies.

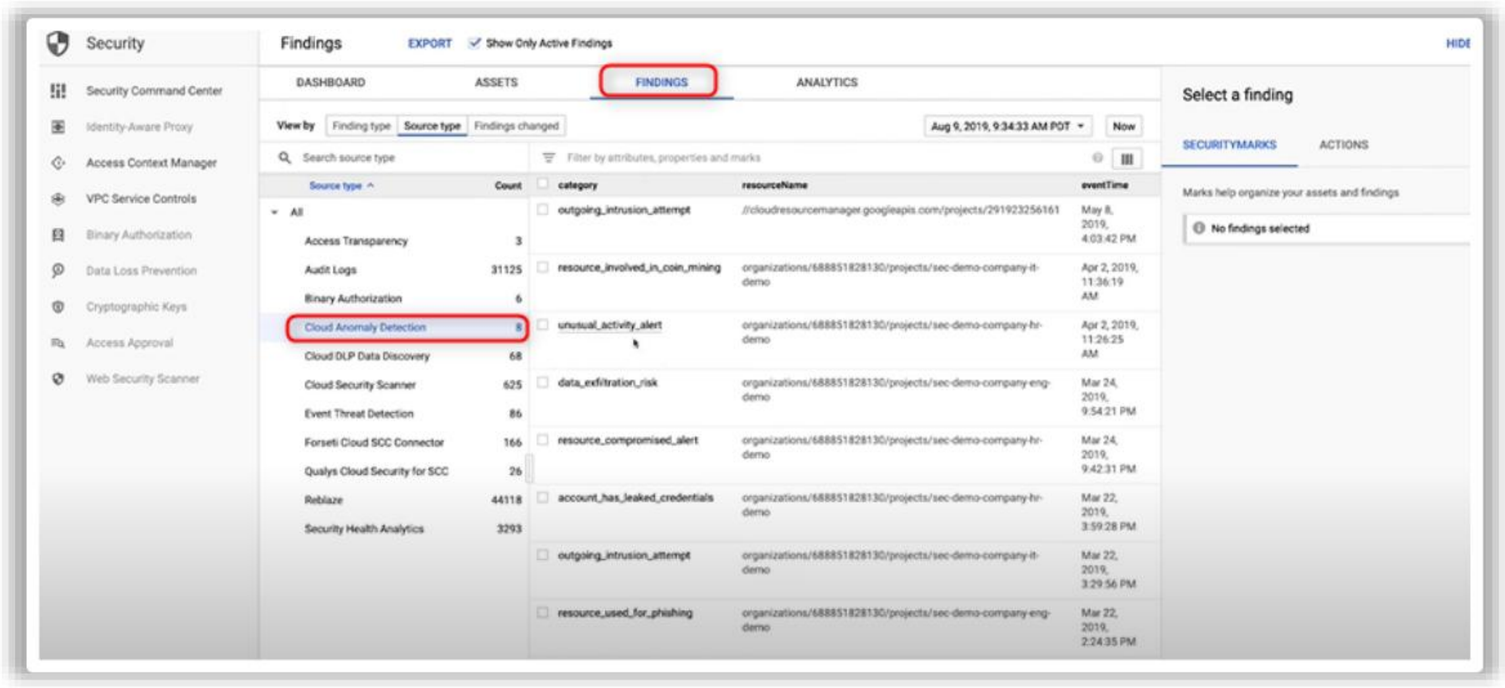


Figure 7.149: Navigating to Findings

- **Step 2: Remediate the Anomalies Detected by Cloud Anomaly Detection**
  - Click on an anomaly to get more details, such as the attributes and source properties.



Figure 7.150: Details of Findings

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

- To remediate an anomaly, click on the date on which it was detected and click on Audit Logs.

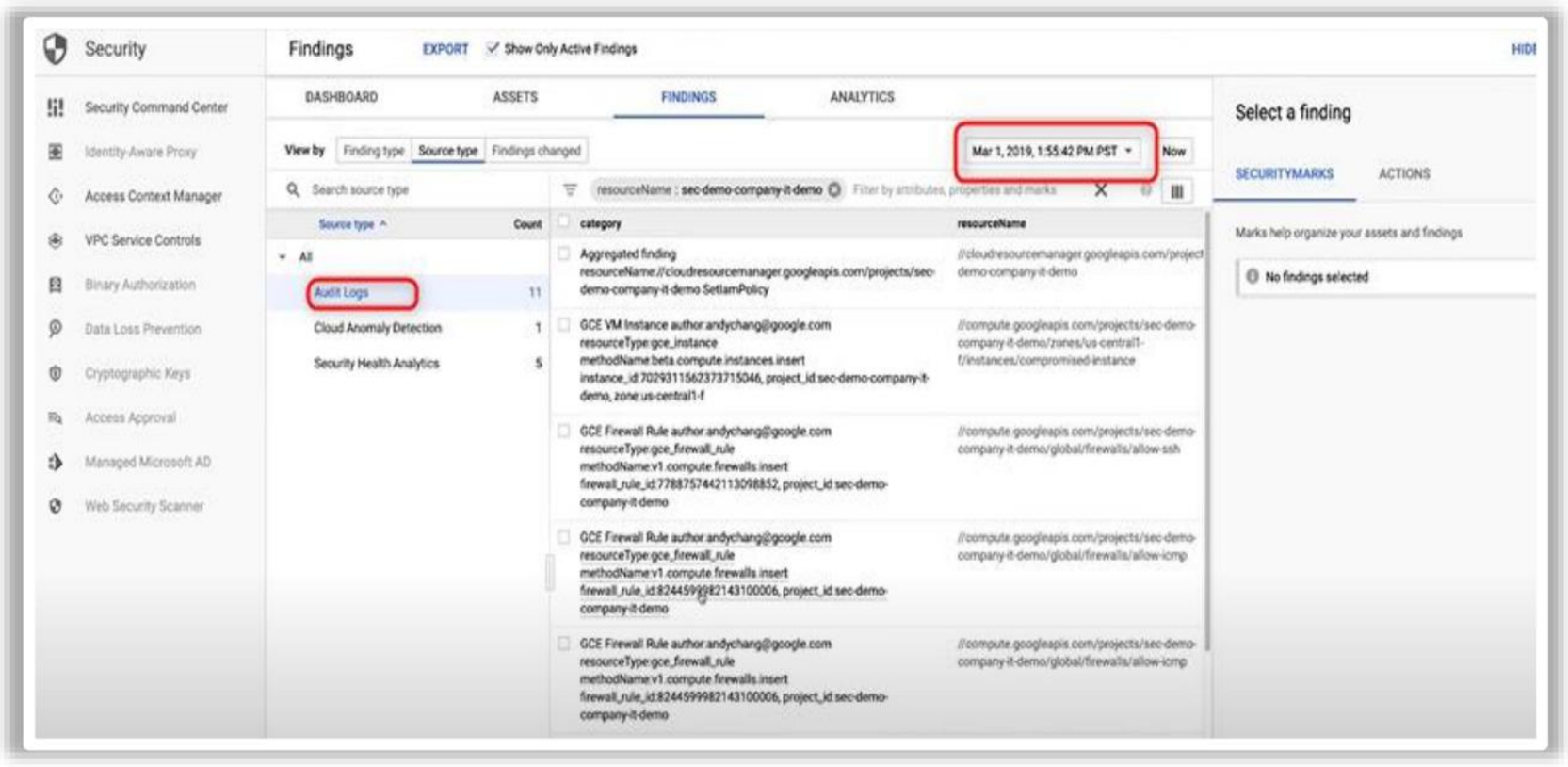
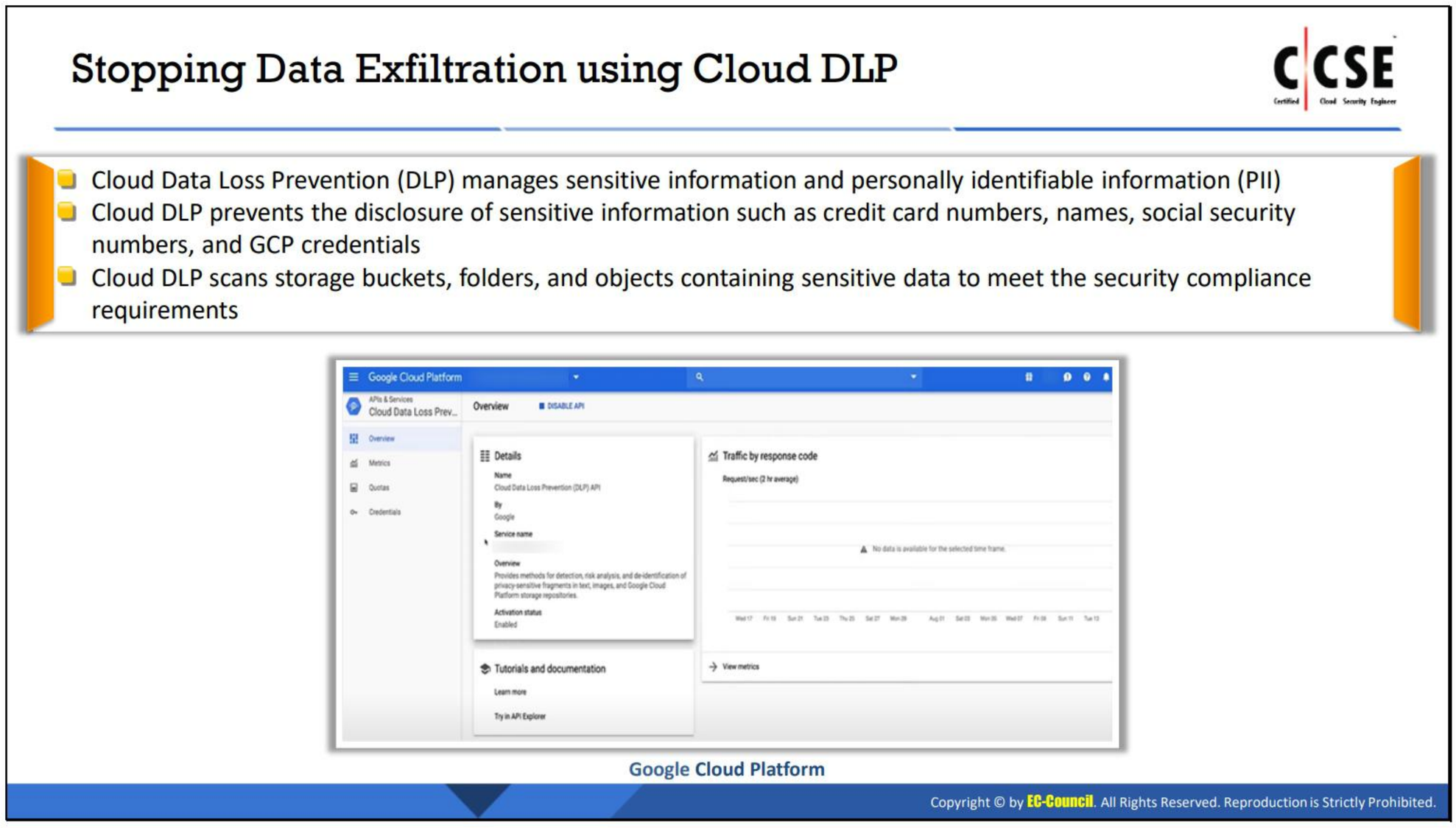


Figure 7.151: Moving to Audit Logs

- Based on the information available in the audit logs, the issue can be remediated.

hide01.ir

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



Stopping Data Exfiltration using Cloud DLP

Cloud Data Loss Prevention (DLP) helps meet your specific compliance requirements by allowing you to understand and manage critical data. Cloud DLP manages sensitive information and personally identifiable information (PII).

hide01.ir

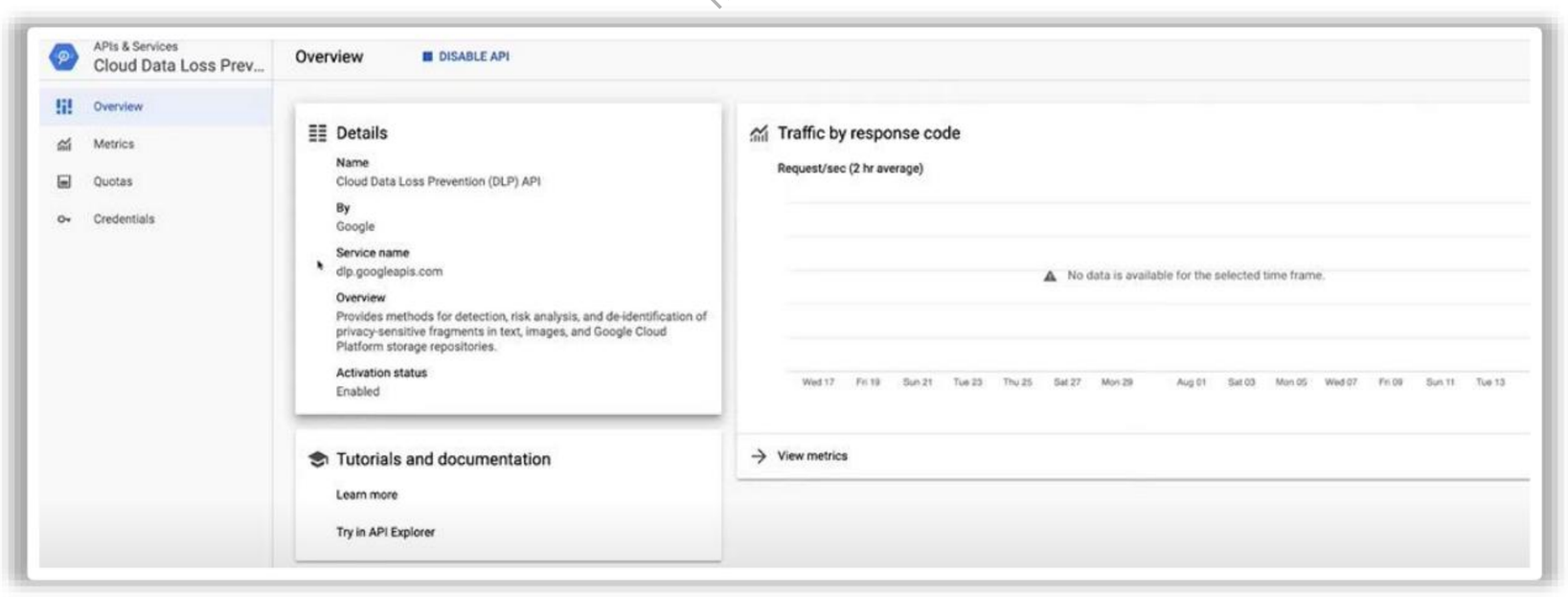


Figure 7.152: Cloud DLP

Cloud DLP prevents the disclosure of sensitive information, such as credit card numbers, names, social security numbers and GCP credentials, by offering scalability and fast information classification and redaction. Cloud DLP scans storage buckets, folders, and objects containing sensitive data to meet the security compliance requirements.

Steps to Use Cloud DLP to Protect Sensitive Data

- **Step 1: Choose Storage Repositories**
  - Select the storage repository that needs to be scanned by DLP.

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

- Open the project where the repository is present if you want to scan an existing storage bucket, Cloud Datastore, or BigQuery table.

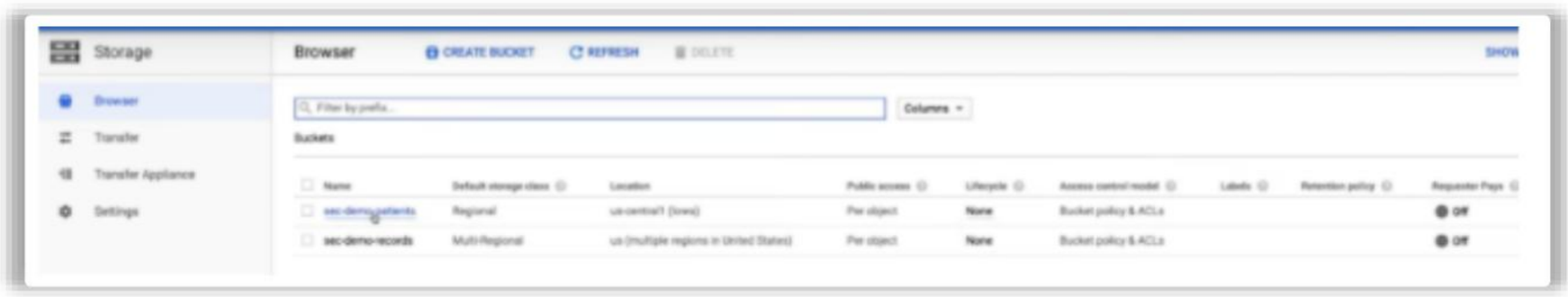


Figure 7.153: Opening the Project

- **Step 2: Enable DLP**
  - Navigate to **APIs and Services** from the menu and then go to **Library**. Ensure the project to be scanned is in the same organization where SCC is enabled and has a storage to be scanned (bucket, BigQuery table, etc.)
  - Now, search for and select **Cloud DLP API** to enable it.

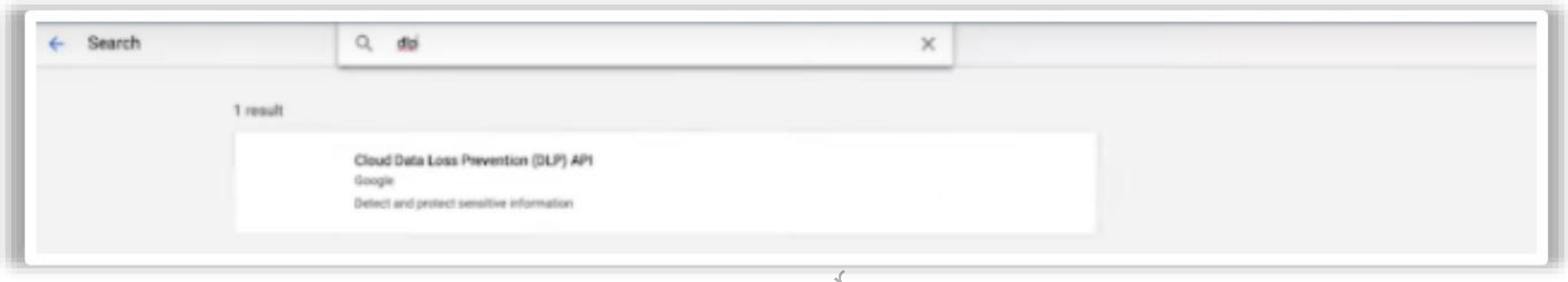


Figure 7.154: Enabling Cloud DLP API

- **Step 3: Select the Org Admin IAM Role**
  - Ensure you have the Org Admin IAM role for using Cloud DLP and sending its results to SCC.

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

- If you do not have one, choose the organization for which SCC should be enabled from the **Organization** drop-down list. Under the **Member** column, locate the username or simply add a new user. Then, assign **DLP job** and **Security Center Admin** roles to the user.

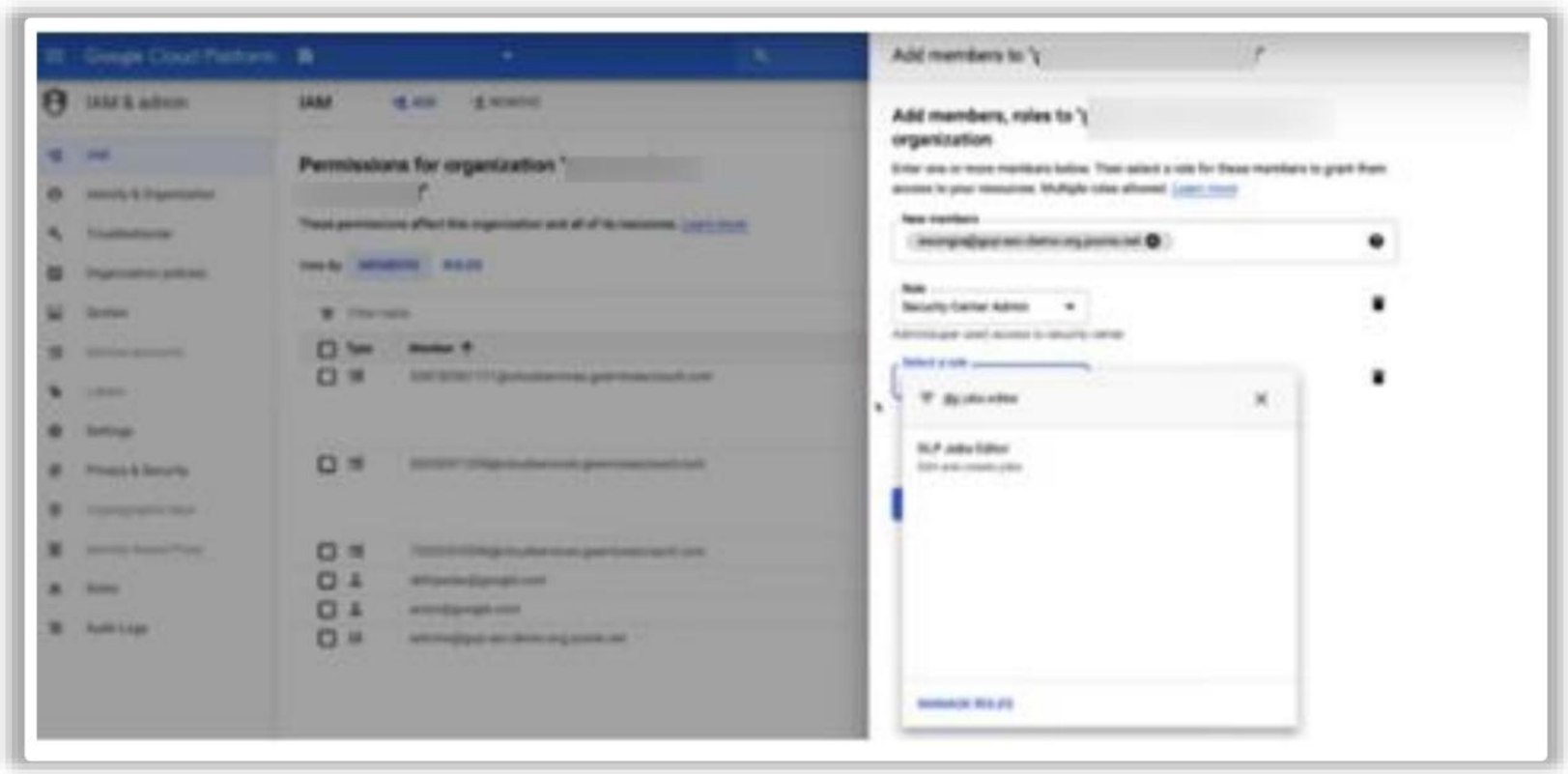


Figure 7.155: Selecting Organization Admin IAM Role

- **Step 4: Enable DLP as a Security Source**
  - On the **SCC homepage**, navigate to **Security Sources** and choose **Cloud DLP**.
  - The SCC dashboard will display findings for DLP via the **Findings cards**.

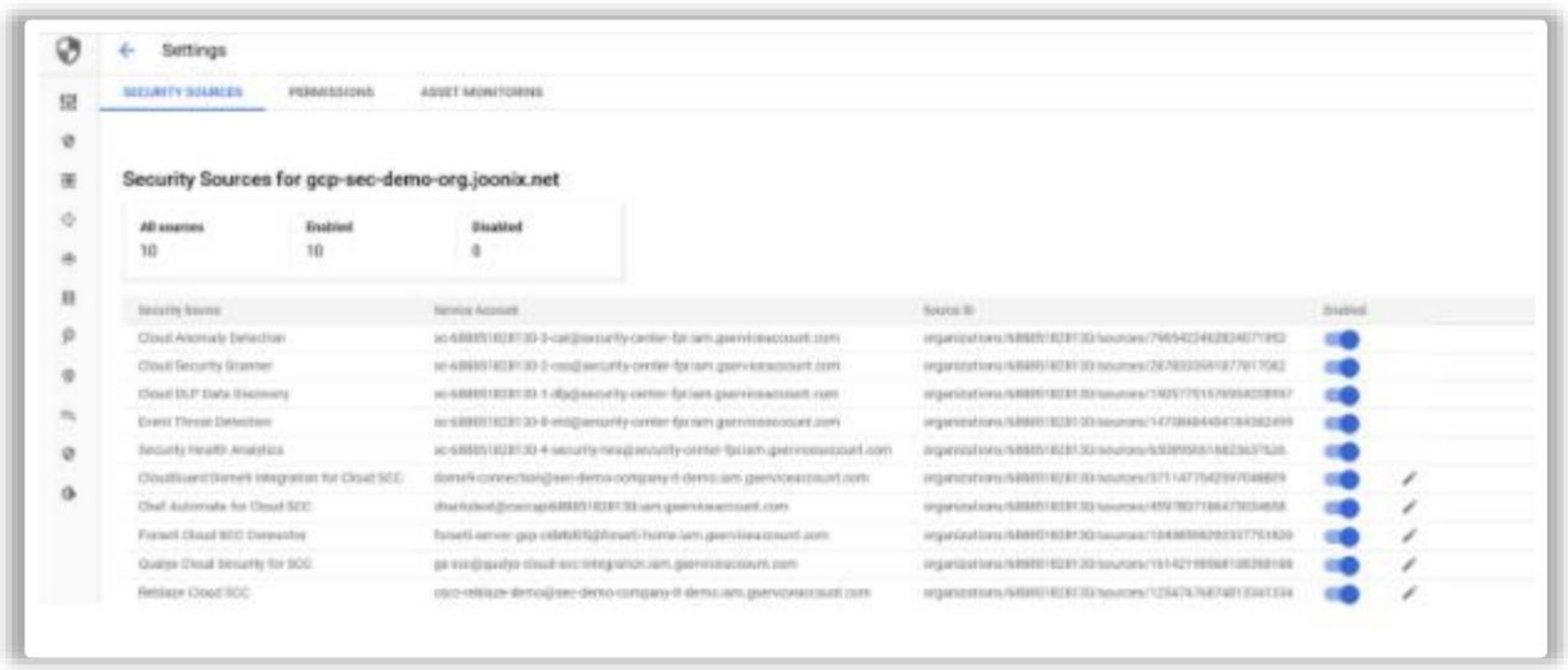
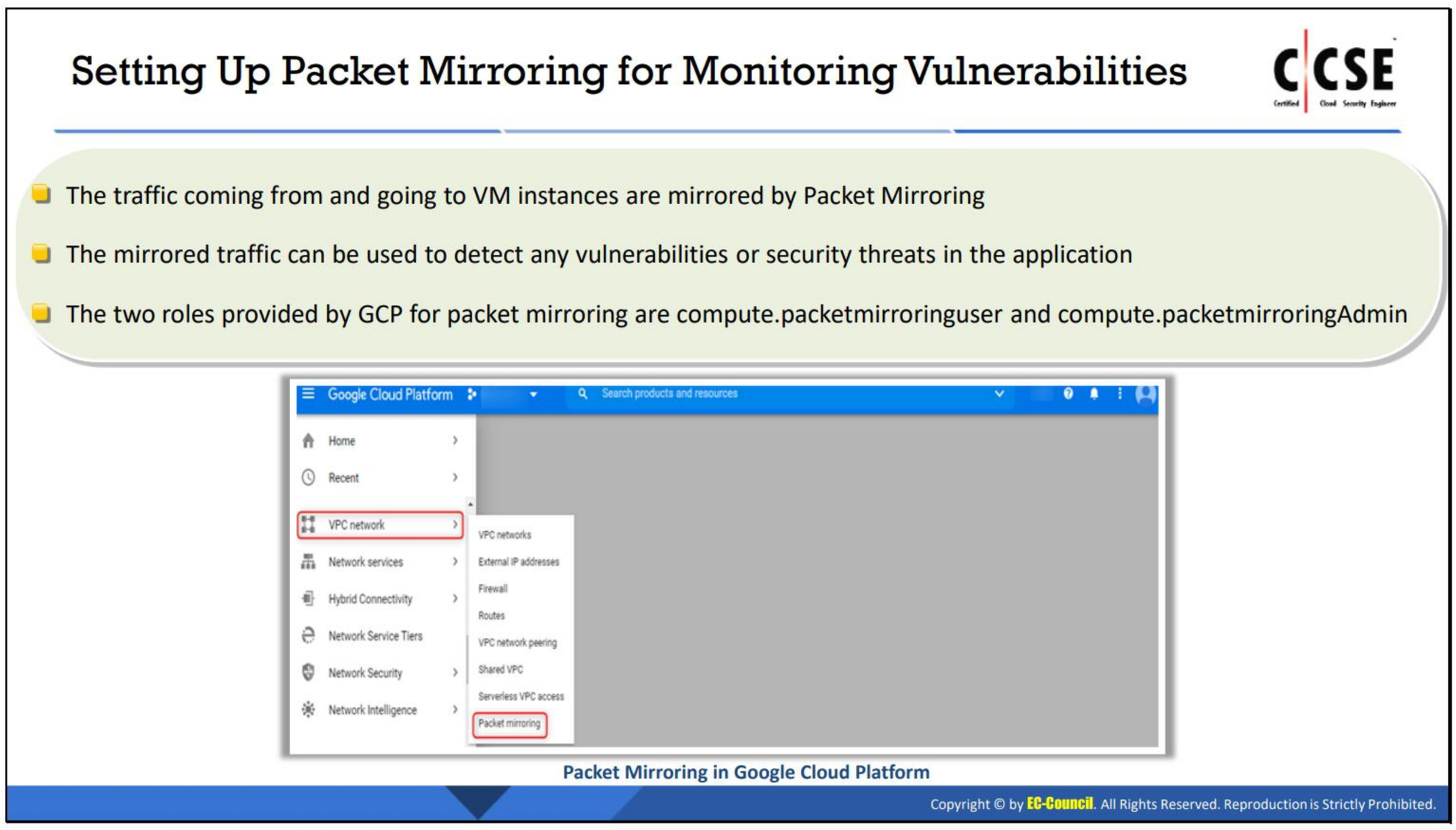


Figure 7.156: Enabling DLP as a Security Source

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



Setting Up Packet Mirroring for Monitoring Vulnerabilities

The Packet Mirroring service in GCP offers a full packet capture of the network traffic for detecting any abnormalities. Packet capture can be configured for both inbound and outbound network traffic. Since the packet mirroring happens on VM instances, it consumes excess bandwidth on VMs.

hidden1.ir

- **Mirrored Sources**: Mirrored sources are compute engine VM instances. They can be selected by specifying subnets. If done so, all traffic in that subnet is mirrored.
- **Collector Destination**: Instance groups behind an internal load balancer constitute a collector destination.

The traffic from the mirrored sources is copied to a collector destination by the Packet Mirroring service. A policy must be created to configure Packet Mirroring. The created policy should specify a source and destination. For an internal load balancer, a forwarding rule must be created for packet mirroring. The non-mirrored traffic sent to the internal load balancer will be dropped. The mirrored traffic can be used to detect any vulnerabilities or security threats in the application.

Packet Mirroring mirrors the traffic coming from and going to VM instances. This traffic can be used to detect any vulnerabilities or security threats in the application. GCP provides two roles for packet mirroring:

- compute.packetMirroringUser: grants user permissions to create, update, and delete packet mirroring policies.
- compute.packetMirroringAdmin: grants user permissions to mirror particular resources.

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

An internal TCP/UDP load balancer with a forwarding rule is configured as a packet mirroring collector. A firewall rule with an outbound rule to send traffic to an internal TCP/UDP load balancer and an inbound rule to receive traffic from mirrored instances are also essential.

Steps to Set Up Packet Mirroring for Detecting Threats

- **Step 1: Create a Packet Mirroring Policy**
  - Navigate to **VPC Network** in the console**.**
  - Click on **Packet Mirroring.**



Figure 7.157: Navigating to Packet Mirroring

  - Click on Create Policy.
  - Enter the name and region, and then select Enabled.
  - Click Continue.
  - Select the VPC Networks which contain the mirrored source and collector destination and click Continue.
  - If the source and destination are in the same network, select Mirrored Source and Destination in same VPC Network. Otherwise, select Mirrored Source and Destination are in separate, peered VPC Networks.
  - Select Mirrored source and click Continue.
  - Select the Subnets, Network tags, and Instance Name.
  - Select the internal TCP/UDP load balancer configured for packet mirroring.
  - Click Continue.
  - To mirror only specific traffic, select Mirror Filtered Traffic.
  - Click Submit.
- **Step 2: Enable Packet Mirroring**
  - Navigate to Packet Mirroring page in the console.
  - Select the packet mirroring policies to be enabled.
  - Click Enable.

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

- Confirm by clicking Enable again.

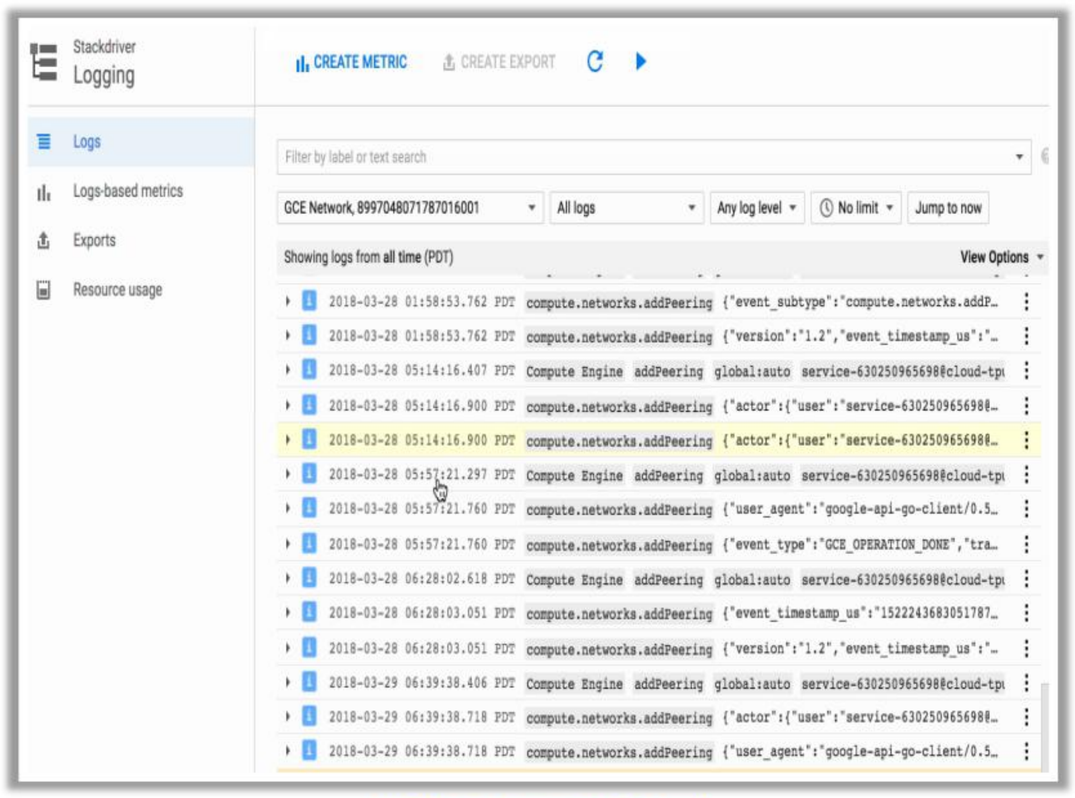
- **Step 3: View Packet Mirroring in Compute Engine Console**
  - Navigate to VM Instances page in the console.
  - Select the project which contains a mirrored instance.
  - Click on the name of the instance.
  - Click on Monitoring.
  - The Mirrored Network Bytes and Mirrored Network Packets charts show the mirrored bytes and packets.

hide01.ir

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

VPC Flow Logging for Monitoring Network Packets

- VPC Flow Logging provides information on the packets going in and out of a network to identify threats
- VPC Flow logs help in real-time monitoring of the network traffic and performance analytics
- Network forensics can be performed on the VPC Flow logs to examine any malicious IP addresses
- It helps in real-time monitoring through APIs and integrates with SIEM tools to generate alerts on security incidents



VPC Flow Logging dashboard

Source: https://cloud.google.com

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

VPC Flow Logging for Monitoring Network Packets

VPC Flow Logging provides information on the packets going in and out of a network to identify threats. VPC Flow logs collect a sample of network flow sent or received by VM instances for network monitoring, real-time security analysis, forensics, etc.

hidoo1.ir

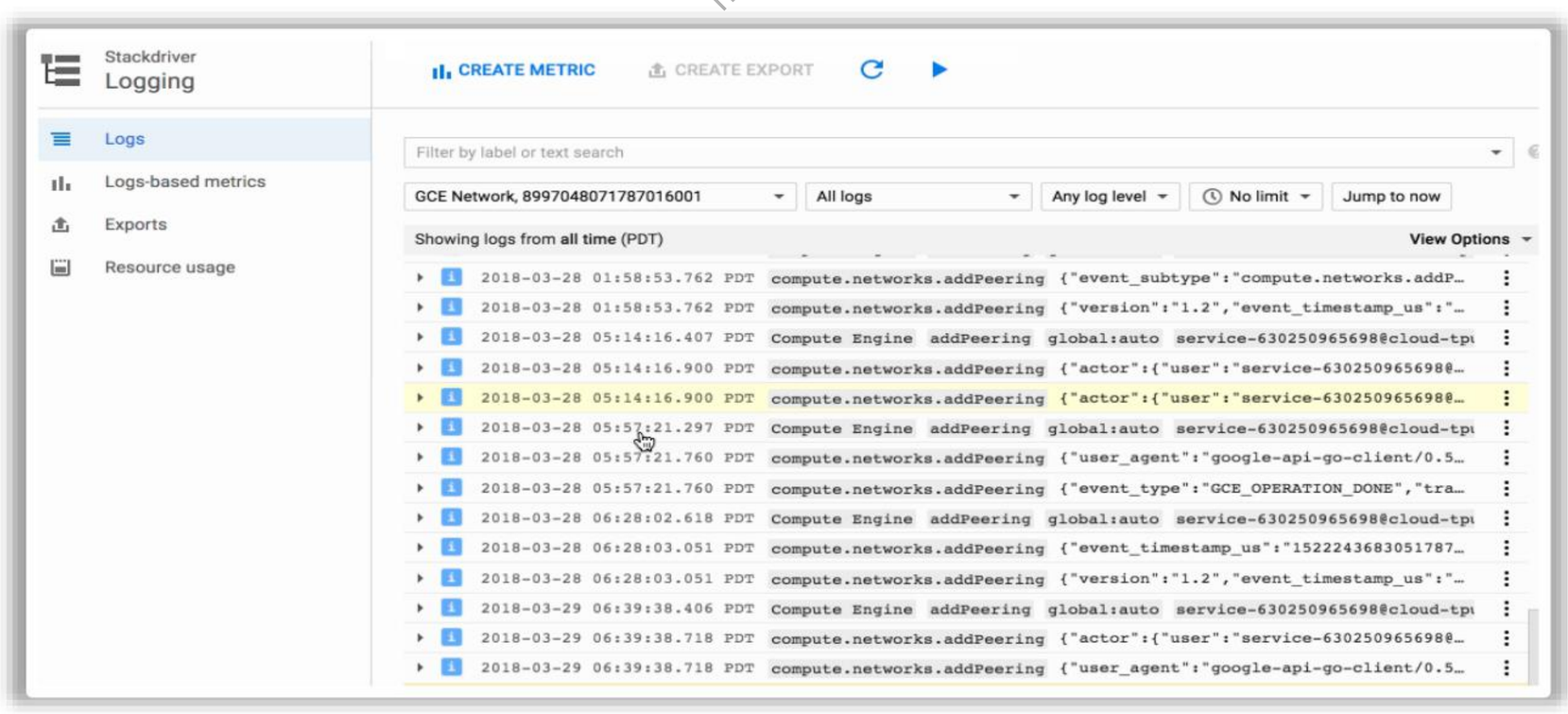


Figure 7.158: Logs

VPC Flow logs help in real-time monitoring of network traffic and performance analytics. A network forensics can be performed on the VPC Flow logs to examine any malicious IP addresses. It helps in real-time monitoring through APIs and can be integrated with SIEM tools to generate alerts on security incidents. The cloud admin can use VPC Flow logs to identify suspicious traffic and access patterns that may indicate security or operational risks.

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

Steps to Use VPC Flow Logging

Enable VPC Flow Logging for a New Subnet

- On the GC console, go to the **VPC networks** page.

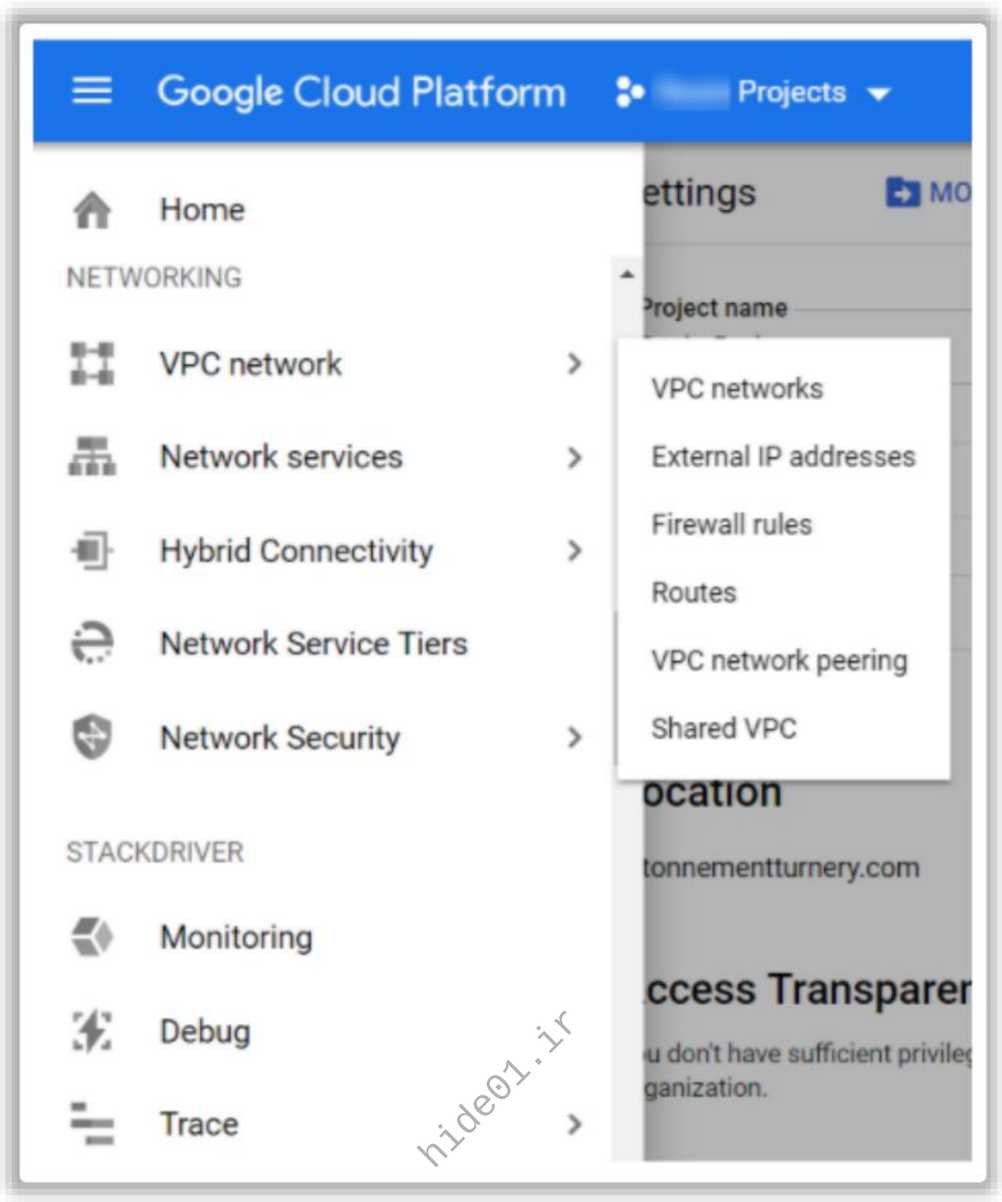


Figure 7.159: Navigating to VPC Networks

- Click on the network where the subnet is to be added.
- Click on **Add subnet** and choose **On** under **Flow logs**.



Figure 7.160: Turning On Flow Logs

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

- For adjusting log sampling and aggregation, choose **Configure logs** and then adjust
  - **Aggregation Interval**
  - Include **metadata** or not
  - **Sample rate**. Keep it at 100% to include all entries.

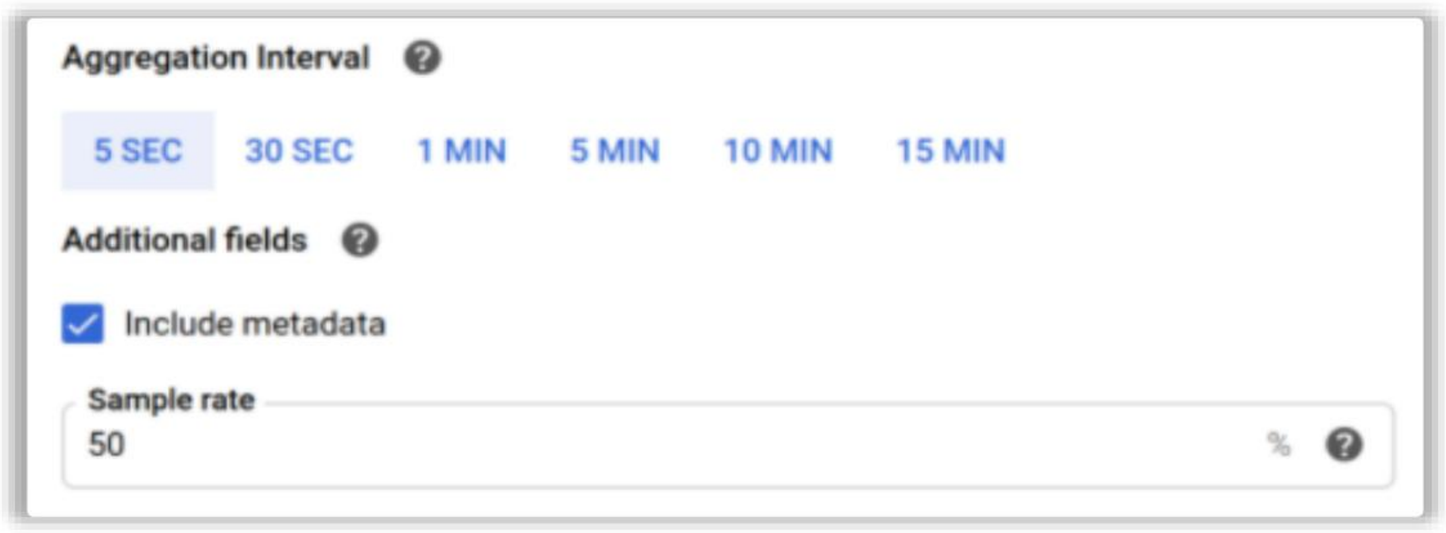


Figure 7.161: Aggregation Interval

- Fill other relevant fields as appropriate and click **Add**.

Turn on VPC Flow Logging for an Available Subnet

- On the GC console, go to the **VPC networks** page.
- Choose the subnet that is to be updated and click Edit.
- Choose **On** under **Flow logs**.

hide01.ir

Figure 7.162: Turning On Flow Logs

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

- For adjusting log sampling and aggregation, choose **Configure logs** and then adjust
  - **Aggregation interval**
  - Include **metadata** or not
  - **Sample Rate**. Keep it at 100% to include all entries.

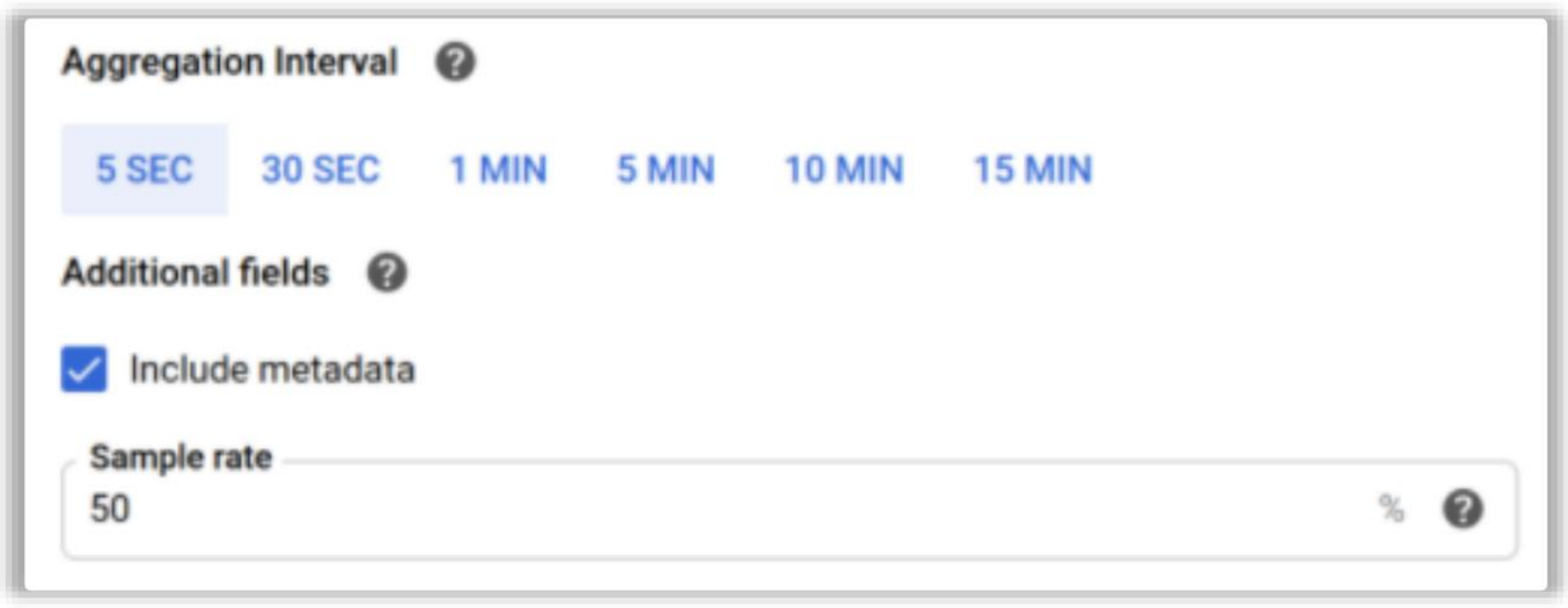


Figure 7.163: Aggregation Interval

- Click **Add.**

Access all VPC Flow Logs

- On the GC console, go to the **Logs** page.
- From the first pull-down menu, choose **Subnetwork**.
- From the second pull-down menu, choose **compute.googleapis.com/vpc_flows**
- Click on **OK.**

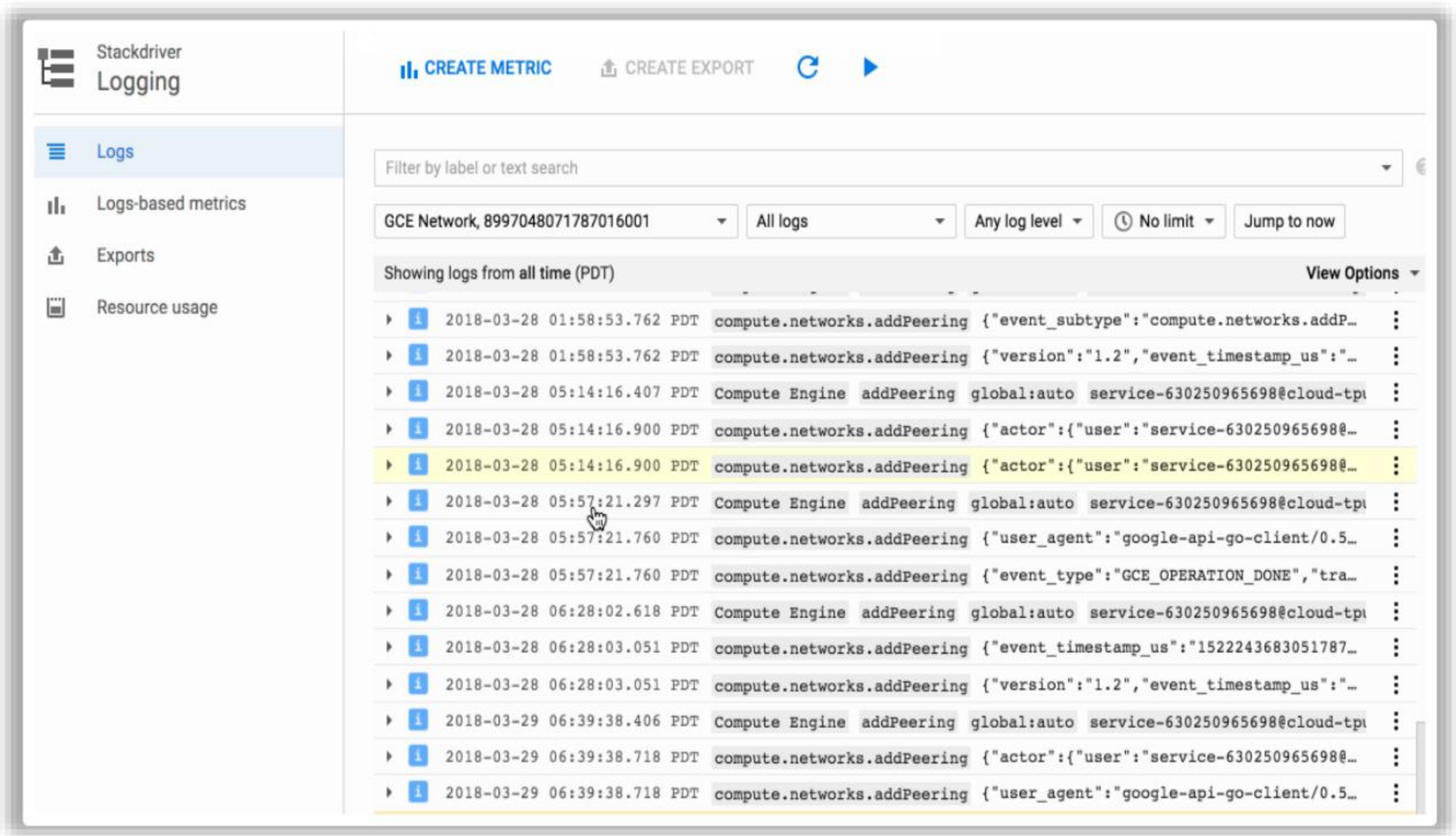
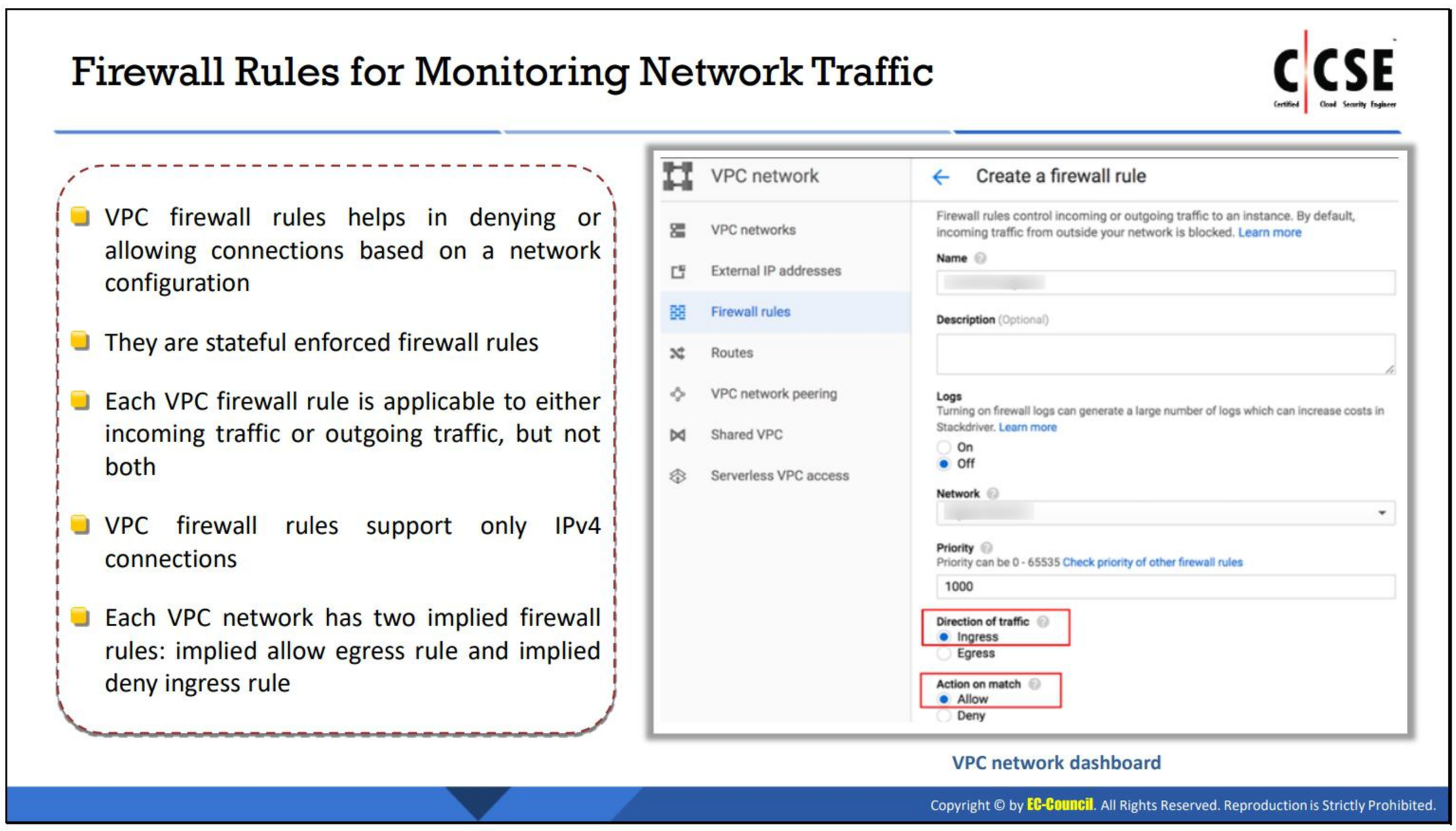


Figure 7.164: Accessing VPC Flow Logs

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



Firewall Rules for Monitoring Network Traffic

VPC firewall rules help in denying or allowing connections based on a network configuration. They are stateful enforced firewall rules. These rules control the network traffic and strengthen the security of your cloud environment. Each VPC firewall rule is applicable to either incoming traffic or outgoing traffic, but not both. These rules support only IPv4 connections. Use firewall rules to monitor network packets for any malicious content. Each VPC network has two implied firewall rules: implied allow egress rule and implied deny ingress rule. Cloud admins can use default firewall rules or create their own rules.

Steps for Creating a VPC Firewall Rule (Ingress)

- Go to VPC network from the GC console and select **Firewall rules**.

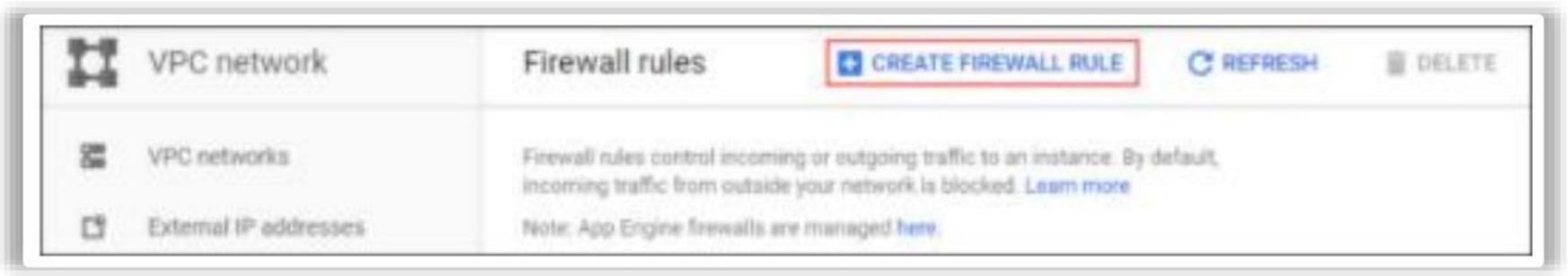


Figure 7.165: Creating Firewall Rules

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

- Choose **Create Firewall Rule** and provide the requested details. Keep the **Direction of traffic** as **Ingress** and choose **Allow for Action on match**.

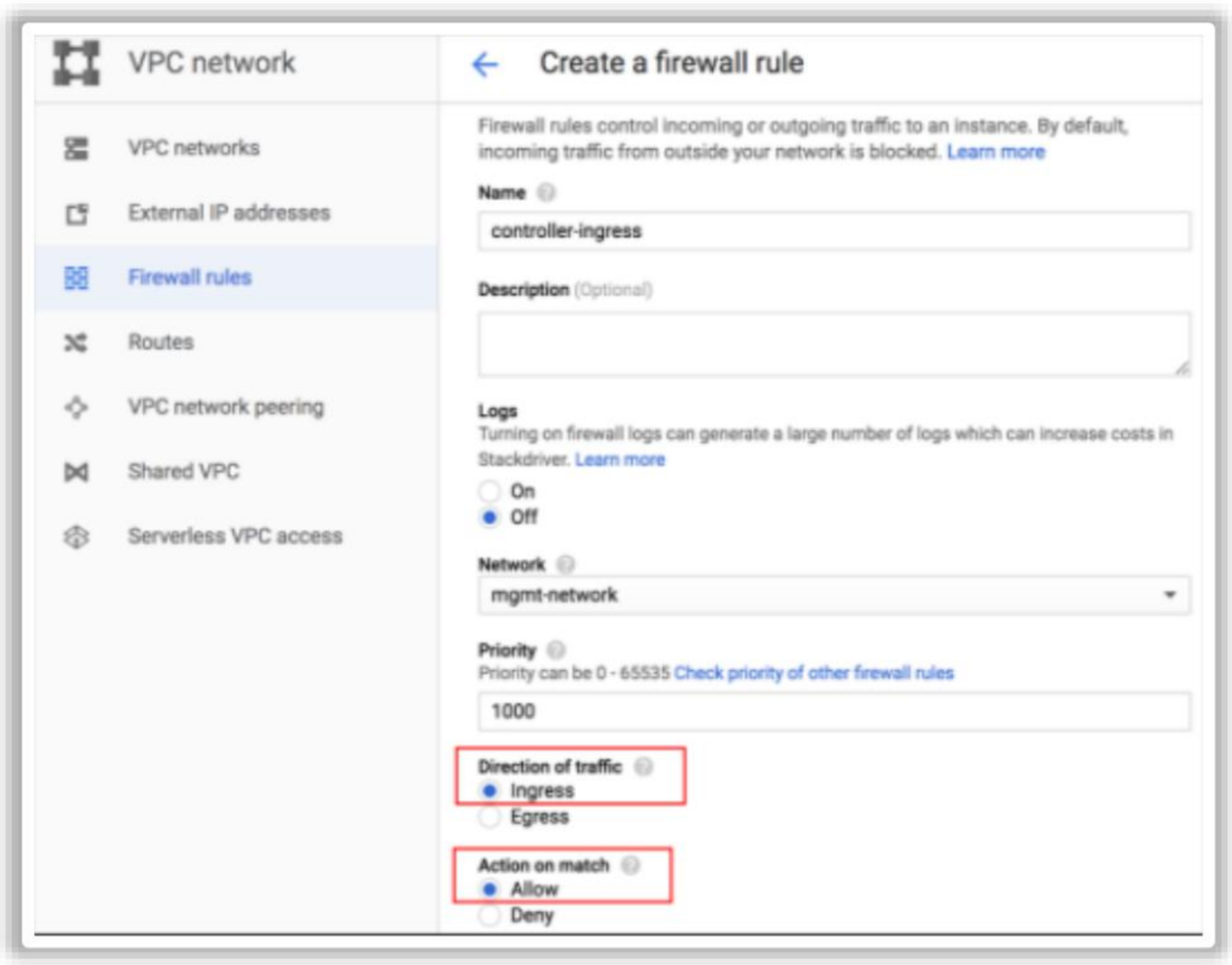


Figure 7.166: Filling Details for Creating a Firewall Rule

- Choose **Specified target tags** so that firewall rules are applied to the selected instances only inside the VPC.
- Provide the **Target tags** and choose **Specified protocol and ports**. Choose **tcp** or **udp** ports to which these rules must apply.

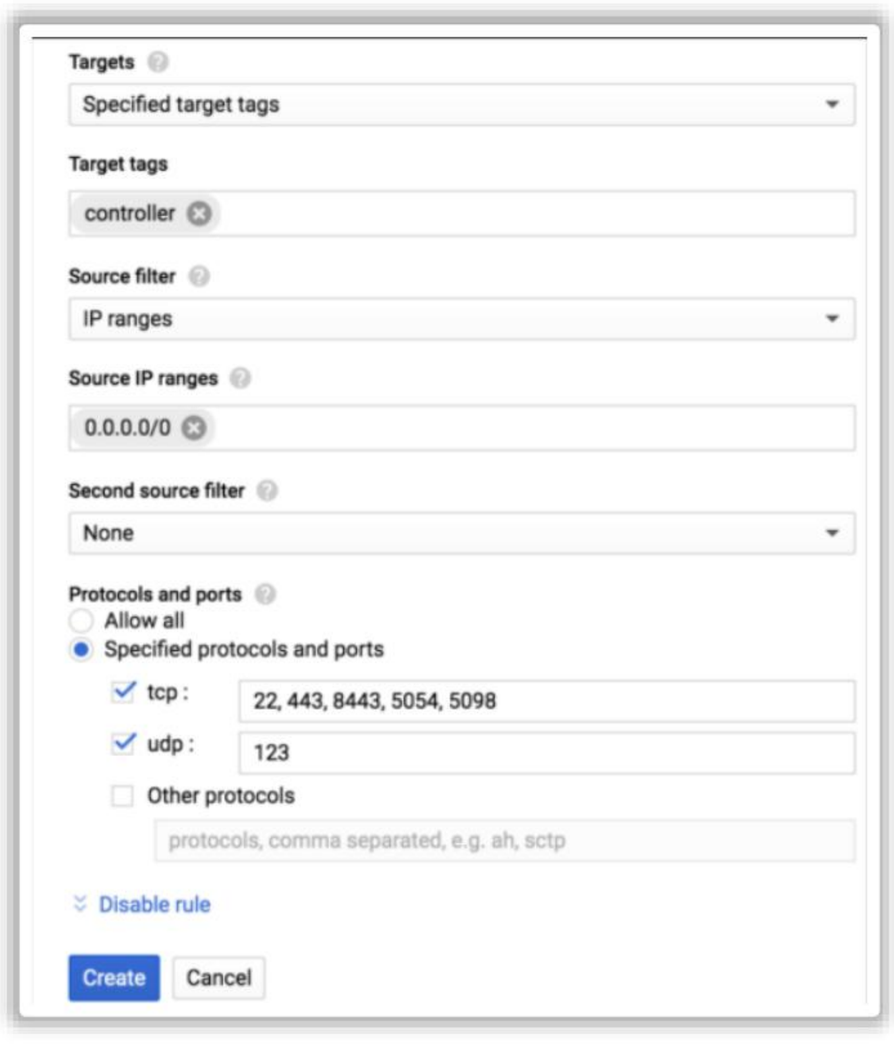


Figure 7.167: Selecting Ports

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

- Choose **Create.**

Steps for Creating a VPC Firewall Rule (Egress)

- Choose **Create Firewall Rule** and provide the requested details. Keep the **Direction of traffic** as **Egress** and choose **Allow for Action on match**.

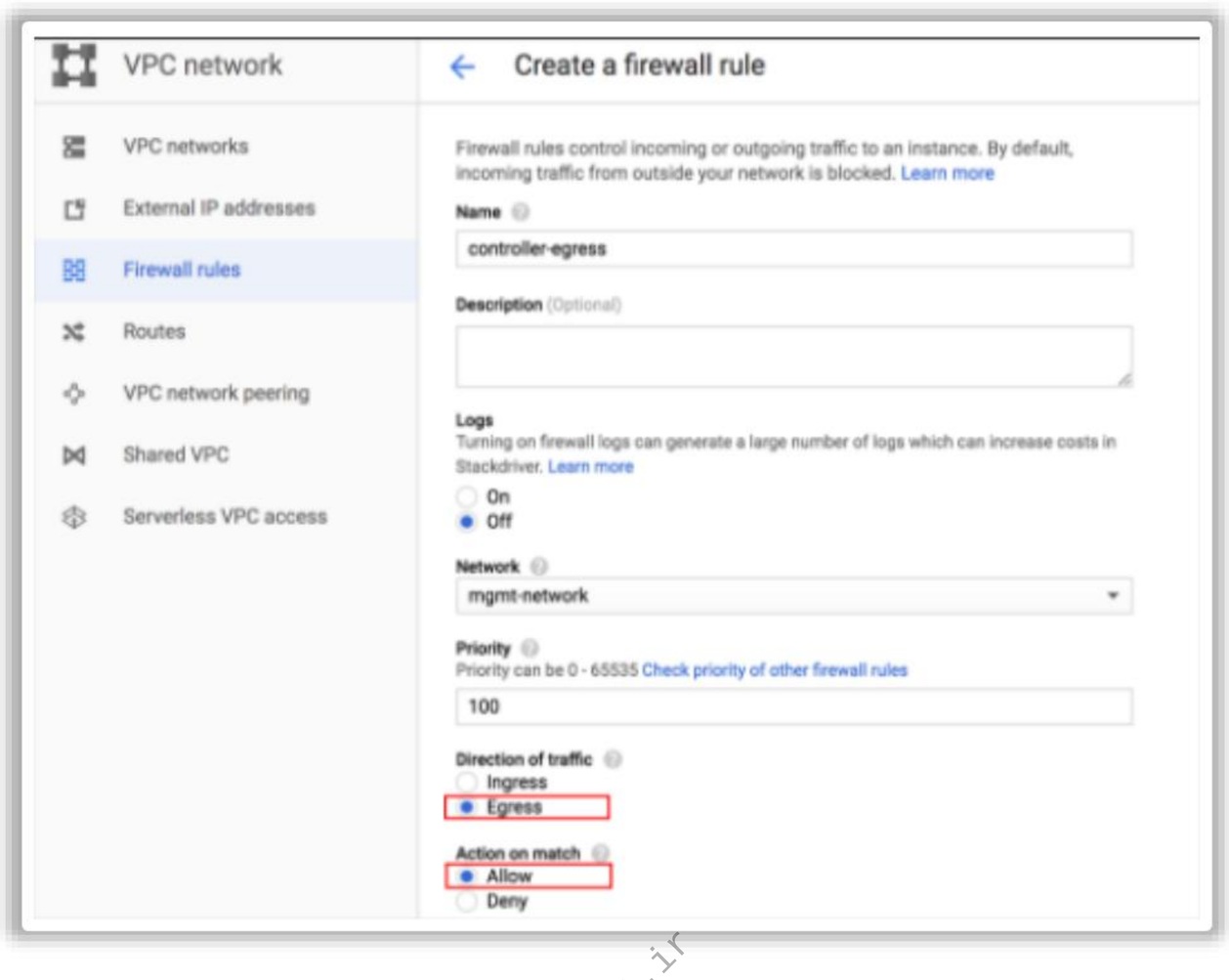


Figure 7.168: Setting Direction of Traffic

- Provide the **Target tags** and choose **Specified protocols and ports**.
- Add the port numbers under **Specified protocols and ports** and choose **Create**.

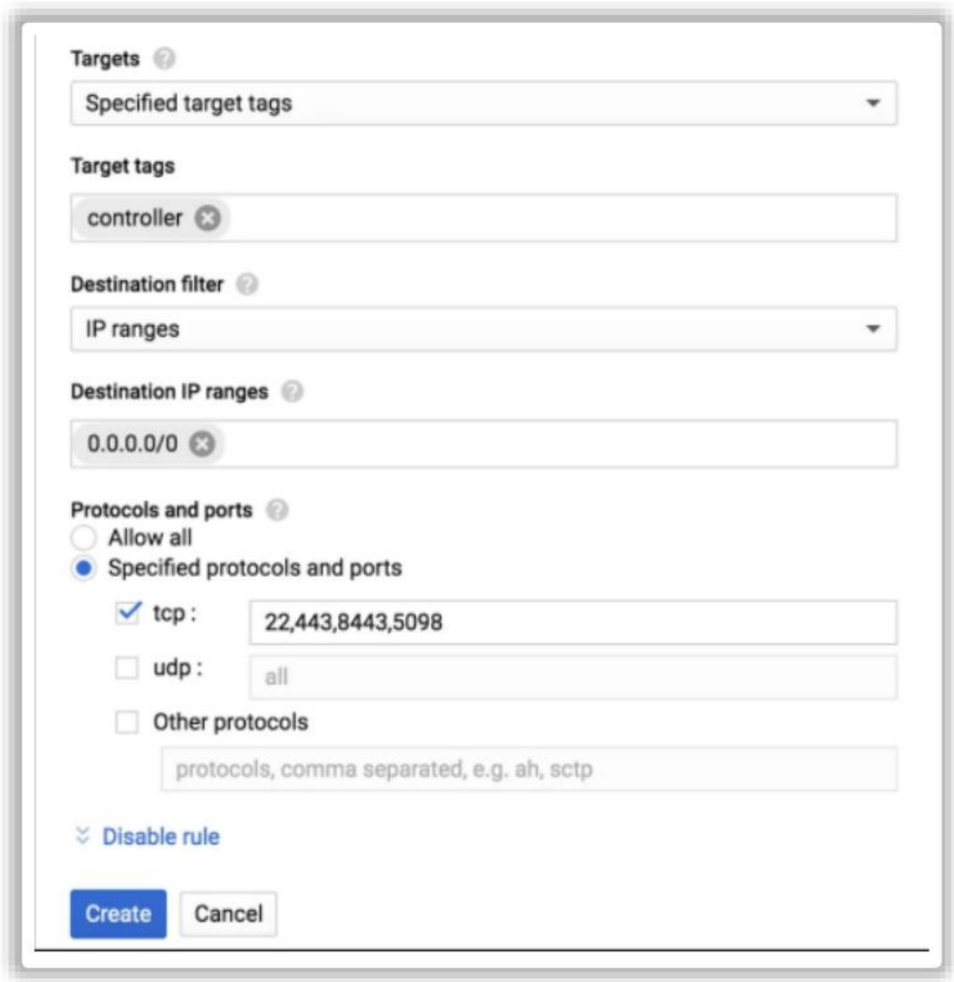
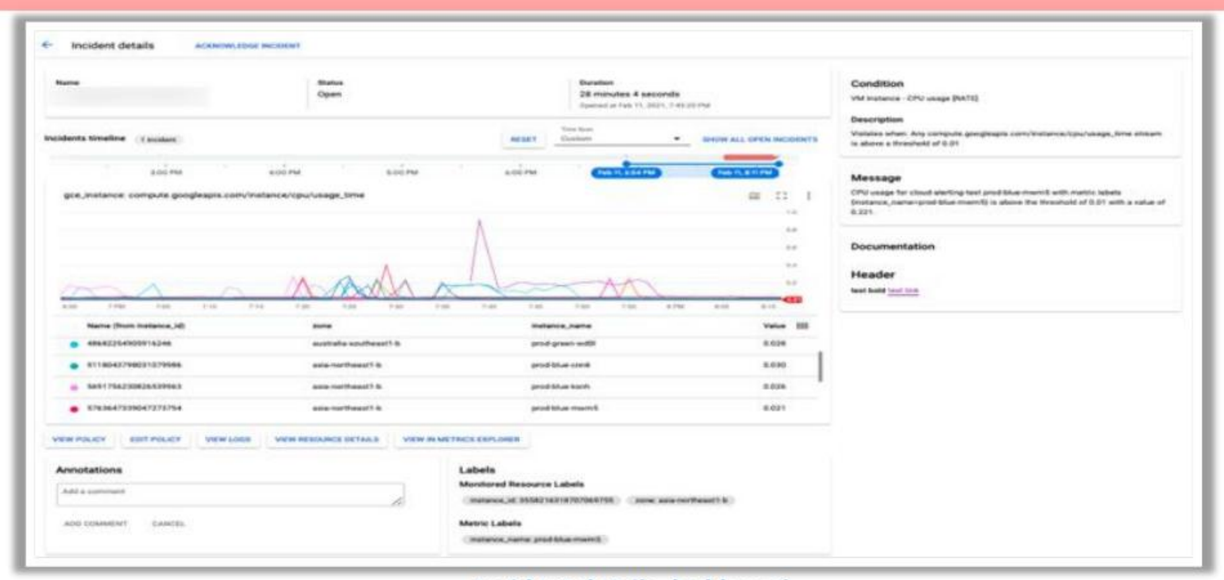


Figure 7.169: Adding Port Numbers

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

Detecting and Responding to Incidents via Cloud Monitoring

- Google Cloud Monitoring alerts inform a user about the security issues in GCP applications
- The alerting policies specify the conditions, notifications, and documentation to trigger alerts
- An incident is a record of the alerting policy trigger
- The incidents can be in three states: open, acknowledged, and closed



Incident details dashboard

Source: https://Cloud.google.com

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

Detecting and Responding to Incidents via Cloud Monitoring

Google Cloud Monitoring alerts inform a user about the security issues in GCP applications. Alerting policies can be defined for the circumstances under which an alert is to be generated. The alerting policies specify the following:

hide01.ir

- **Conditions**: The conditions identify whether the resources are in a state which requires an action.
- **Notifications**: They inform the support team that the conditions are met. The notification channels include email, Cloud Mobile App, PagerDuty, SMS, and Slack.
- **Documentation**: Documentation can be done for some notifications to resolve an issue.

An incident is a record of the alerting policy trigger. When the conditions of an alerting policy are satisfied, an incident is recorded by Cloud Monitoring. The incidents can be in three states:

- **Open:** Open status indicates the alerting policy conditions are satisfied or there is no data to indicate the conditions are not satisfied.
- **Acknowledged:** Acknowledged indicates that an incident is open and under investigation.
- **Closed:** Closed status indicates the policy condition has been terminated.

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

Steps to Detect and Respond to Incidents by Cloud Monitoring

- **Step 1: Find Incidents**
  - Navigate to **Monitoring** and click on **Alerting** in the GCP console.

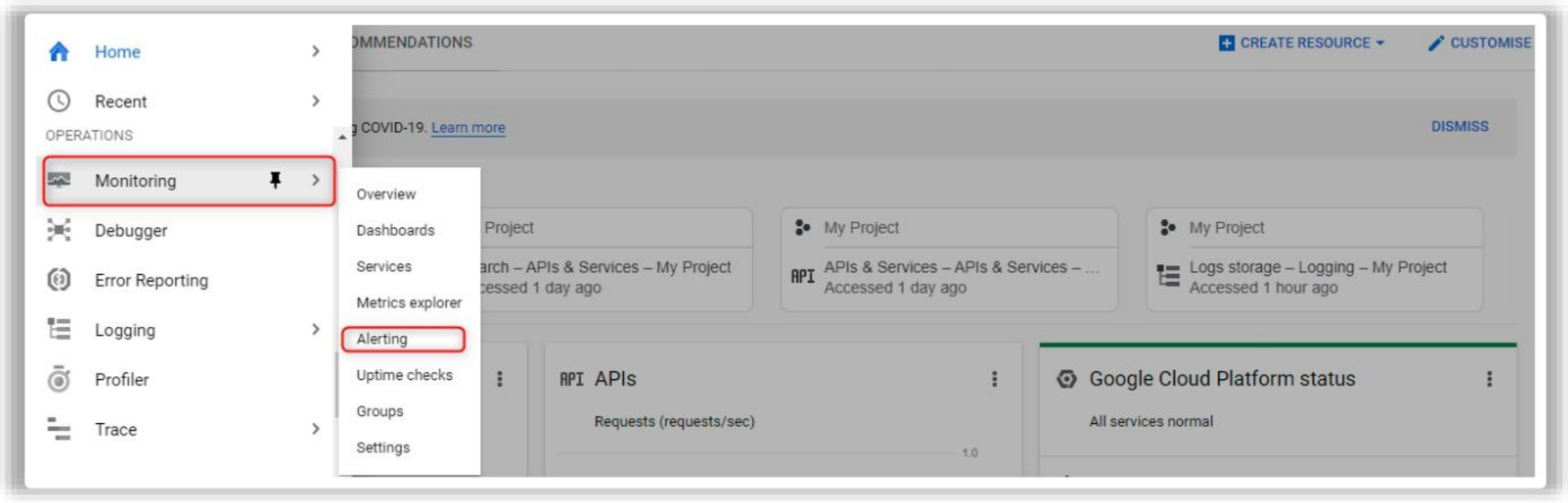


Figure 7.170: Navigating to Alerting Section

  - The open incidents are listed by the Summary tab.
  - The Incidents pane displays recent incidents.
  - Click on Show Closed Incidents to view the closed incidents.

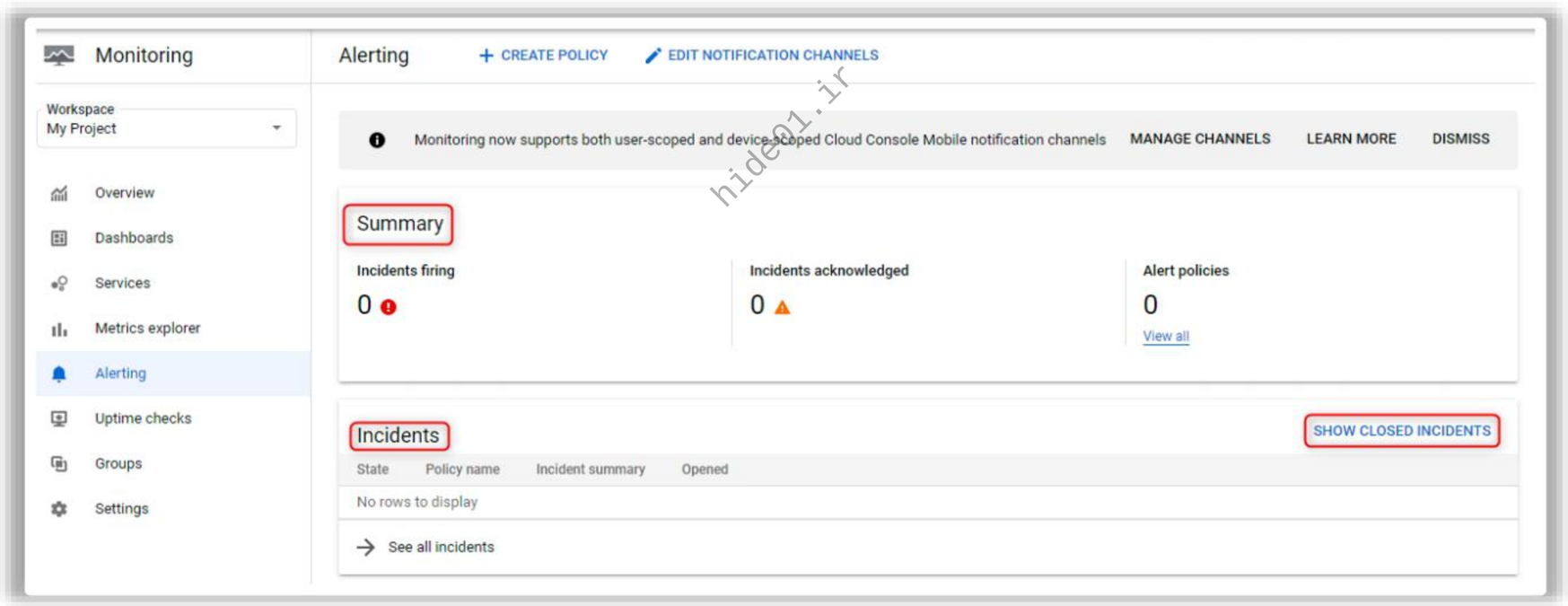


Figure 7.171: Closed Incidents

  - To filter incidents, click on see all incidents under Incidents.

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

- Click on the Filter icon to filter incidents based on their properties.

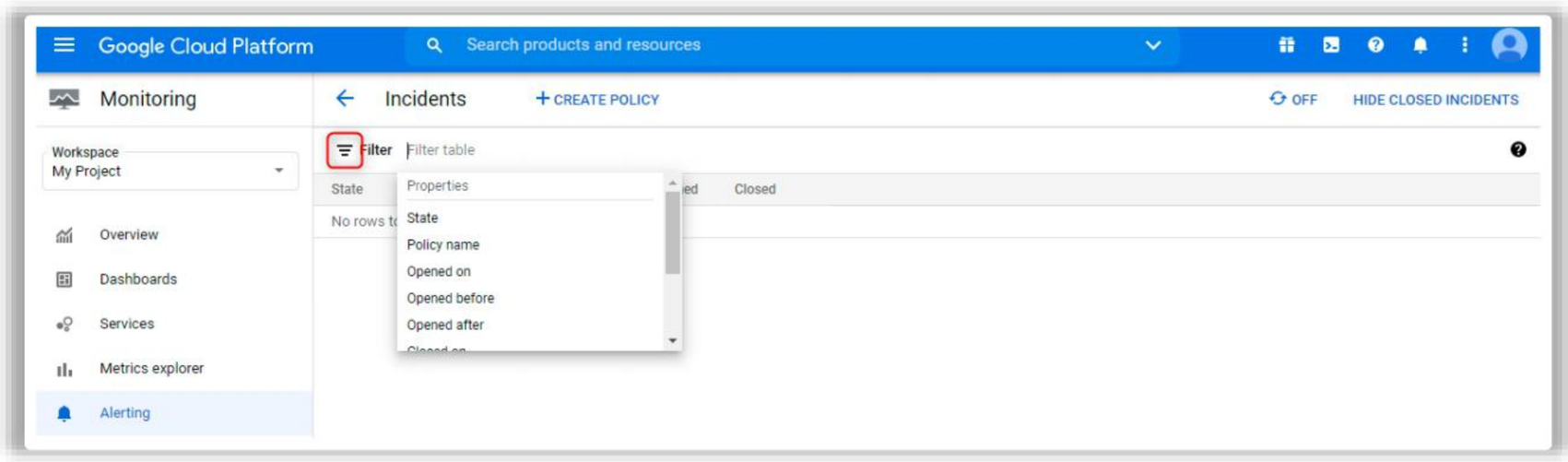


Figure 7.172: Filtering Incidents

▪ Step 2: Investigate the Incident

- To investigate an incident, navigate to the Incident Details page.
- Click on Incident Summary to get the details.

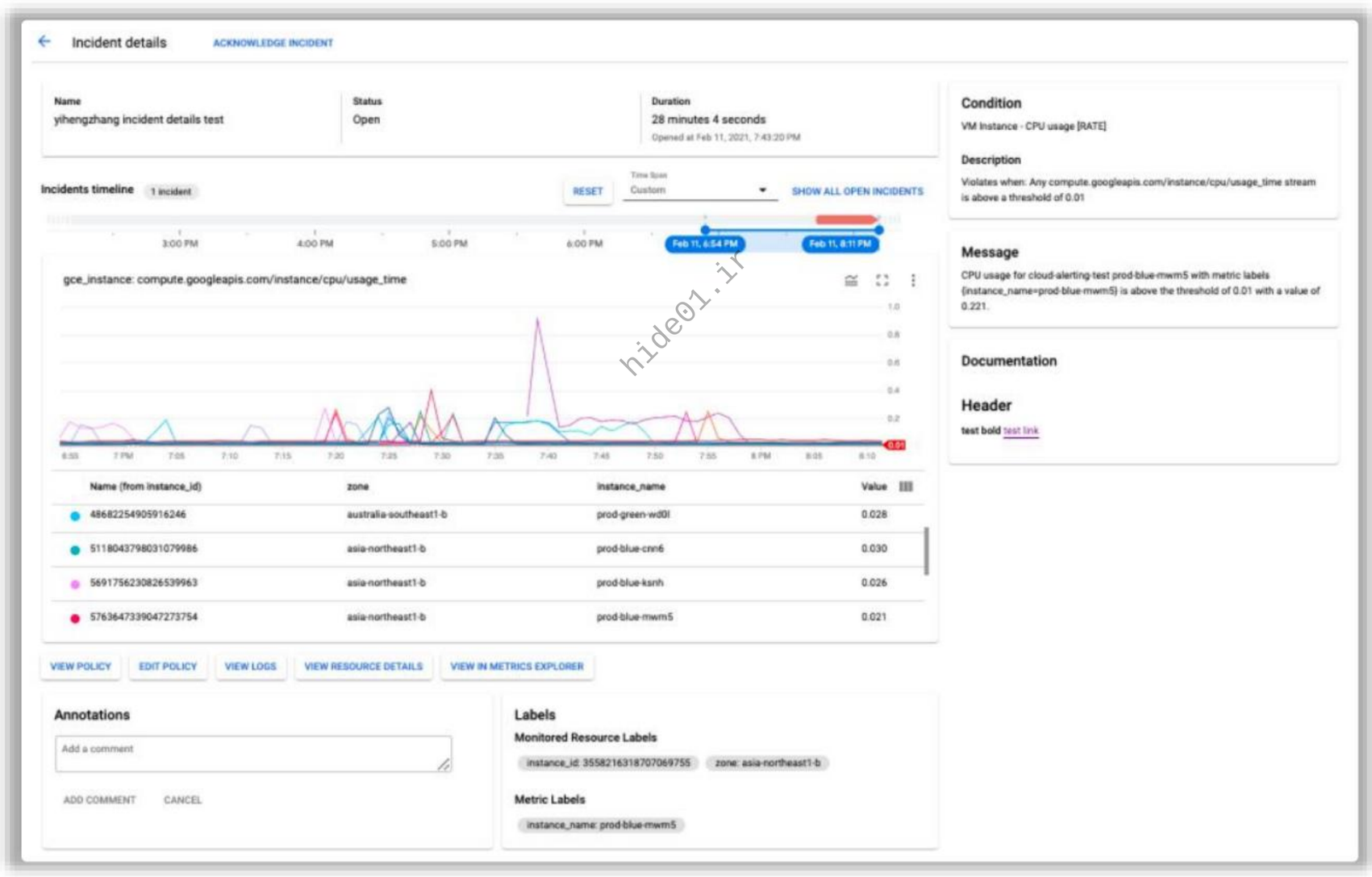
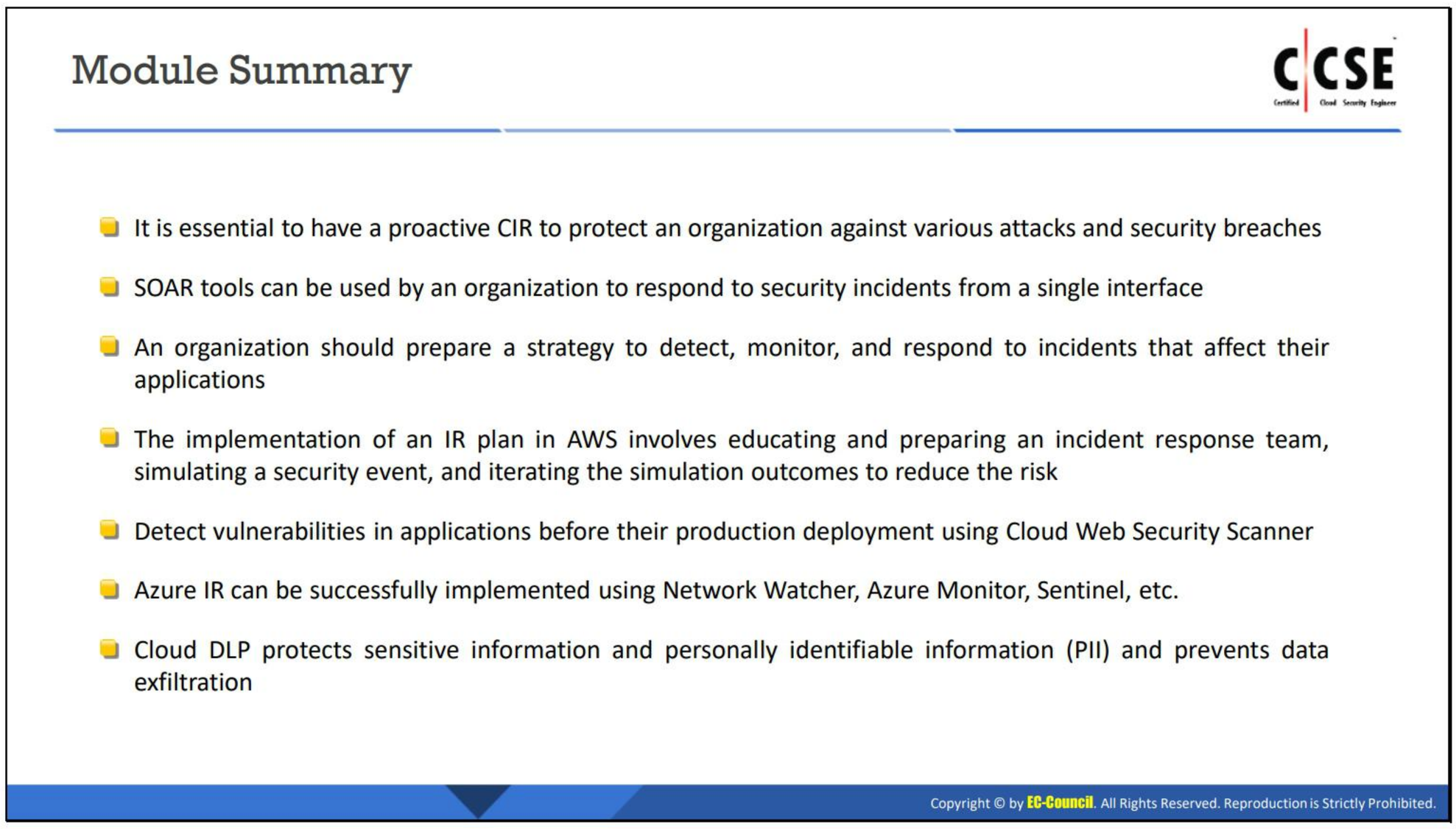


Figure 7.173: Incident Summary

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



Module Summary

This module explains the various technical aspects of handling incident detection and response in the cloud.

hide01.ir

The module highlights are as follows:

- It is essential to have a proactive CIR to protect an organization against various attacks and security breaches.
- SOAR tools can be used by an organization to respond to security incidents from a single interface.
- An organization should prepare a strategy to detect, monitor, and respond to incidents that affect their applications.
- The implementation of an IR plan in AWS involves educating and preparing an incident response team, simulating the security event, and iterating the simulation outcomes to reduce the risk.
- Azure IR can be successfully implemented using Network Watcher, Azure Monitor, Sentinel, etc.
- A Google incident response process should be built on industry-leading techniques for resolving incidents and refined to operate efficiently at Google's scale.

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