Module 08

Handling and Responding to Cloud Security Incidents

This page is intentionally left blank.

Module Objectives

Cloud computing is an emerging technology to deliver computing services such as online business applications, online data storage, and webmail over the internet. A cloud implementation allows to distribute workforce, reduces organization expenses, provides data security, among other benefits. As many enterprises are adopting the cloud, it is target of attackers that exploit vulnerabilities to gain unauthorized access to its valuable data. Therefore, organizations must give utmost importance to cloud security and build skillful incident handling and response teams. They should prepare appropriate plans beforehand for efficiently handling security incidents occurring in the cloud. Incident responders should understand the various security threats and challenges in cloud security.

This module begins with an overview of cloud computing concepts. It presents an introduction on handling cloud security incidents as well as the responsibilities and challenges involved. It also explains various cloud security threats and attacks. Then, it describes various preparation steps to handle cloud security incidents and presents a discussion on the detection and analysis of cloud security incidents. Moreover, it explains steps for containing and eradicating cloud security incidents and discusses how to recover from various of these incidents. It finally explains various best practices against cloud security incidents and tools that help to monitor and detect such incidents.

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

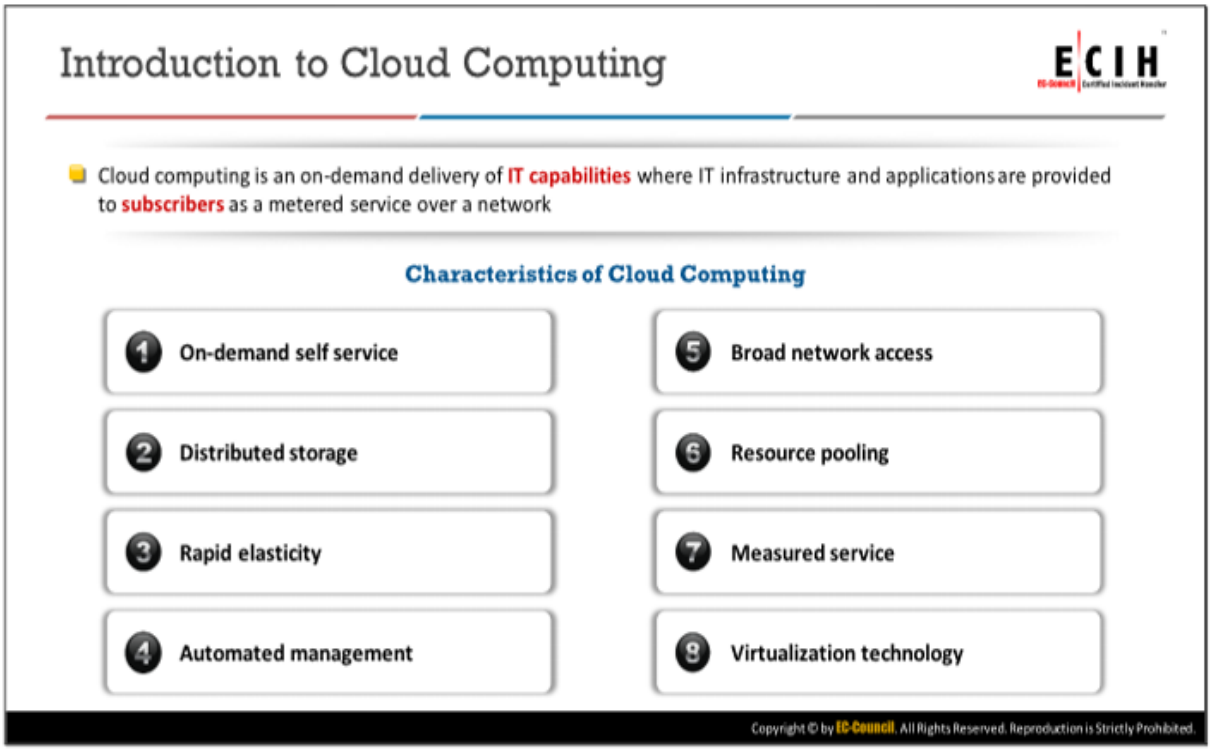
- Understand essential cloud computing concepts
- Explain responsibilities and challenges in handling cloud security incidents
- Explain cloud security threats and attacks

- Discuss the preparation steps required to handle cloud security incidents
- Understand detection and analysis of various cloud security incidents
- Explain containment steps for cloud security incidents
- Explain the eradication and recovery from cloud security incidents
- Describe best practices for cloud security

Cloud Computing Concepts

Cloud computing delivers various types of services and applications over the internet. These services enable users to use software and hardware managed by third parties at remote locations. Available cloud service providers (CSPs) include Google, Amazon, and Microsoft. Due to the increasing usage of cloud services by various organizations, cloud computing resources and services are vulnerable to various security incidents. To handle such incidents, the incident response team should first understand the basic concepts of cloud computing.

This section provides an overview of cloud computing, types of cloud computing services, separation of responsibilities in the cloud, cloud deployment models, and the NIST cloud deployment reference architecture.



Introduction to Cloud Computing

Cloud computing is an on-demand delivery of IT (information technology) capabilities that provides access to both IT infrastructure and applications to subscribers as metered services over communication networks. It enables the sharing of resources, such as networks, servers, storage, virtual machines (VMs), applications, and services. Examples of cloud solutions include Gmail, Facebook, Dropbox, and Salesforce.com.

Below, we discuss the characteristics of cloud computing that attract many businesses today to adopt cloud-based technologies:

- **On-demand self-service**

  Cloud computing allows users to expand resources such as computing power, storage, and networking whenever required through simple requests or by enabling options in their existing accounts. This minimizes human interaction with service providers and the physical management of computing resources.

- **Distributed storage**

  Distributed storage in the cloud improves scalability, availability, and reliability of data. However, cloud distributed storage presents security and compliance concerns.

- **Rapid elasticity**

  The cloud offers instant provisioning of capabilities to rapidly scale up or down services according to the demand. To the cloud customers (CCs), the resources available for provisioning seem to be unlimited, and they can generally purchase them in any quantity at any time.

- **Automated management**

  By minimizing user involvement, cloud automation speeds up processes, reduces labor costs, and reduces the possibility of human errors.

- **Broad network access**

  Cloud resources are available over the network and accessed through standard procedures via a wide variety of platforms including laptops, smartphones, and tablets.

- **Resource pooling**

  The CSP pools all the resources together to serve multiple CCs in a multi-tenant environment, with physical and virtual resources being dynamically assigned and reassigned on demand by the cloud users.

- **Measured service**

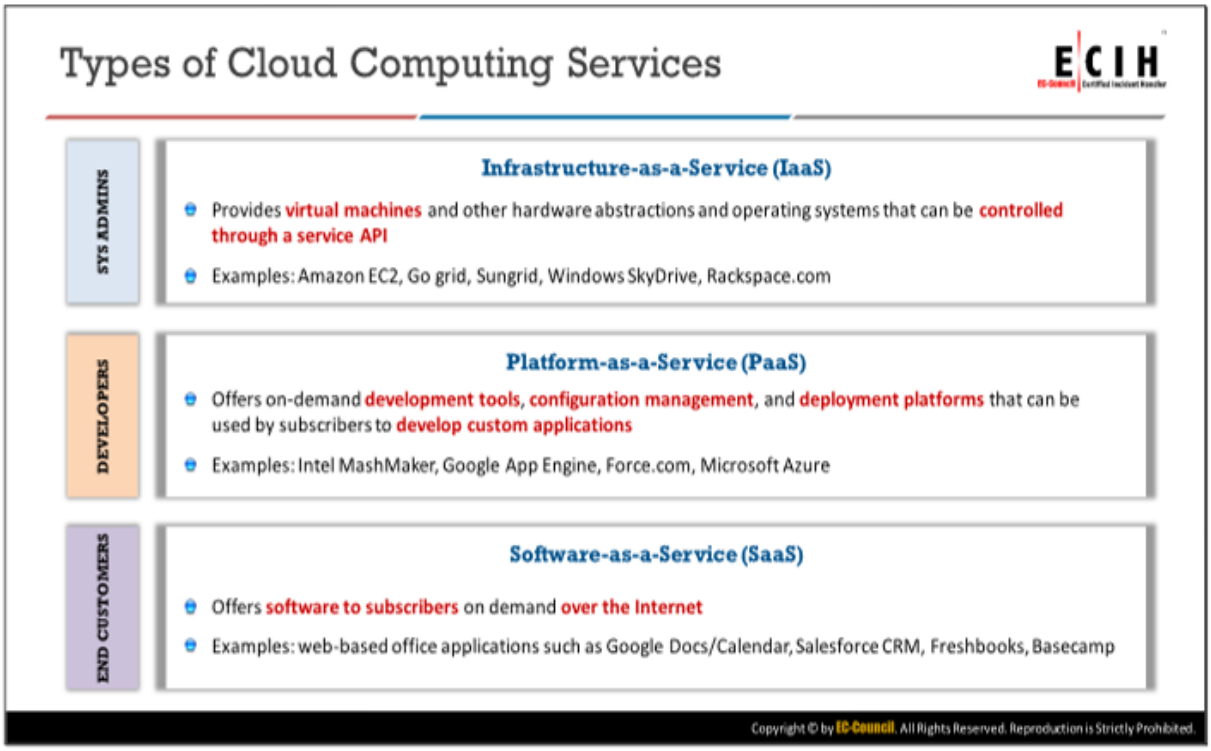
  Cloud systems employ a pay-per-use metering method. Subscribers pay for cloud services by monthly subscription or according to usage of resources such as storage, processing power, and bandwidth. CSPs monitor, control, report, and charge the consumption of resources by customers with complete transparency.

- **Virtualization technology**

  Virtualization replaces hardware or an operating system (OS) by its virtual or digital version. This reduces the amount of investment, maintenance, and management required for physical devices. Virtualization technology in the cloud enables rapid scaling of resources in a way that traditional IT environments cannot achieve.

Limitations of cloud computing:

- Limited control and flexibility by organizations regarding the services
- Service vulnerability to outages and other technical issues
- Security, privacy, and compliance issues
- Contracts and lock-ins
- Dependence on network connection



Types of Cloud Computing Services

Cloud services are divided broadly into three categories:

- **Infrastructure as a service (IaaS)**

  IaaS enables subscribers to use fundamental IT resources such as computing power, virtualization, data storage, and network on demand. This service provides VMs and abstracts hardware and OSs for control through a service API (application programming interface). As CSPs are responsible for managing the underlying cloud infrastructure, subscribers avoid the costs of human capital, hardware, and others. IaaS examples include Amazon Elastic Compute Cloud (EC2), Go grid, SunGrid, Microsoft OneDrive, and Rackspace.com.

  Advantages:

  - Dynamic infrastructure scaling
  - Guaranteed uptime
  - Automation of administrative tasks
  - Elastic load balancing
  - Policy-based services
  - Global accessibility

  Disadvantages:

  - Software security at high risk (third-party providers are more prone to attacks)
  - Performance issues and slow connection speeds compromising the service

- **Platform as a service (PaaS)**

  PaaS offers a framework for developing applications and services. Subscribers do not require to buy and manage the underlying software and infrastructure but have authority over the deployed applications and occasionally over application hosting environment configurations. Hence, PaaS offers development tools, configuration management, and deployment platforms on demand for use by subscribers to develop custom applications. PaaS examples include Google App Engine, Salesforce.com, and Microsoft Azure. Advantages of writing applications in the PaaS model include dynamic scalability, automated backups, and other platform services while omitting explicit coding.

  Advantages:

  - Simplified deployment
  - Prebuilt business functionality
  - Low security risk
  - Instant community
  - Pay-per-use model
  - Scalability

  Disadvantages:

  - Vendor lock-in
  - Data privacy risks
  - Difficult integration with other system applications

- **Software as a service (SaaS)**

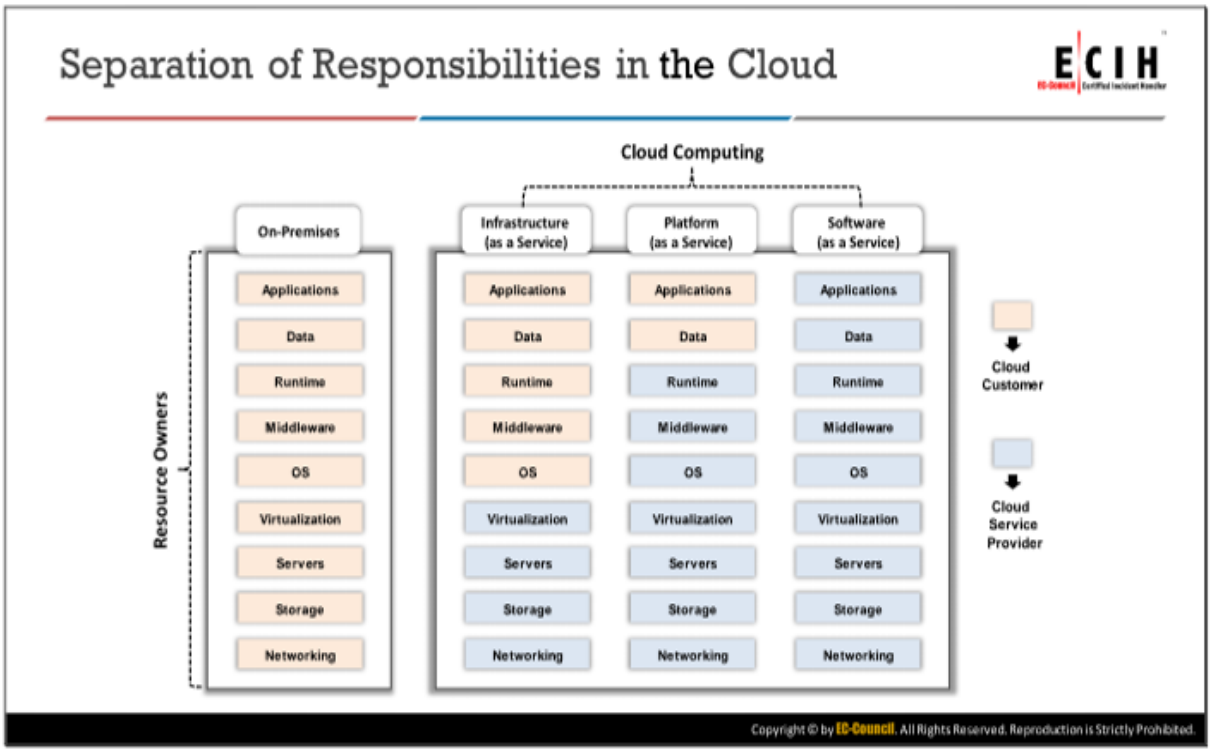
  SaaS offers application software to subscribers on demand over the internet. The provider charges for it on a pay-per-use basis, by subscription, by advertising, or by sharing among multiple users. SaaS examples include web-based office applications like Google Docs and Calendar, Salesforce CRM (customer relationship management), FreshBooks, and Basecamp.

  Advantages:

  - Low cost
  - Easy administration
  - Global accessibility
  - Compatibility (no specialized hardware or software is required)

  Disadvantages:

  - Security and latency issues
  - Complete dependency on the internet
  - Difficult migration between SaaS vendors



Separation of Responsibilities in the Cloud

In cloud computing, the separation of responsibilities between the CC and CSP depends on the service model. Separation of duties prevents conflicts of interest, illegal acts, fraud, abuse, and errors, and helps identifying security control failures including information theft, security breaches, and evasion of security controls. It also restricts the amount of influence held by any individual and ensures that there are no conflicting responsibilities.

The three types of cloud services, namely, IaaS, PaaS, and SaaS have specific limitations regarding the service delivery model during access. The diagram shown on the above slide illustrates the separation of cloud responsibilities specific to the service delivery model.

- **IaaS**

  In IaaS, the CSP provides the required infrastructure including data centers, servers, CPUs, memory, and storage. Therefore, the CSP is responsible for incident response related to the networks, storage, servers, and virtualization.

  The CSP is responsible for providing logs related to server, storage, and database incidents, and can perform related processes. The CSP also gathers evidence related to network traffic and media.

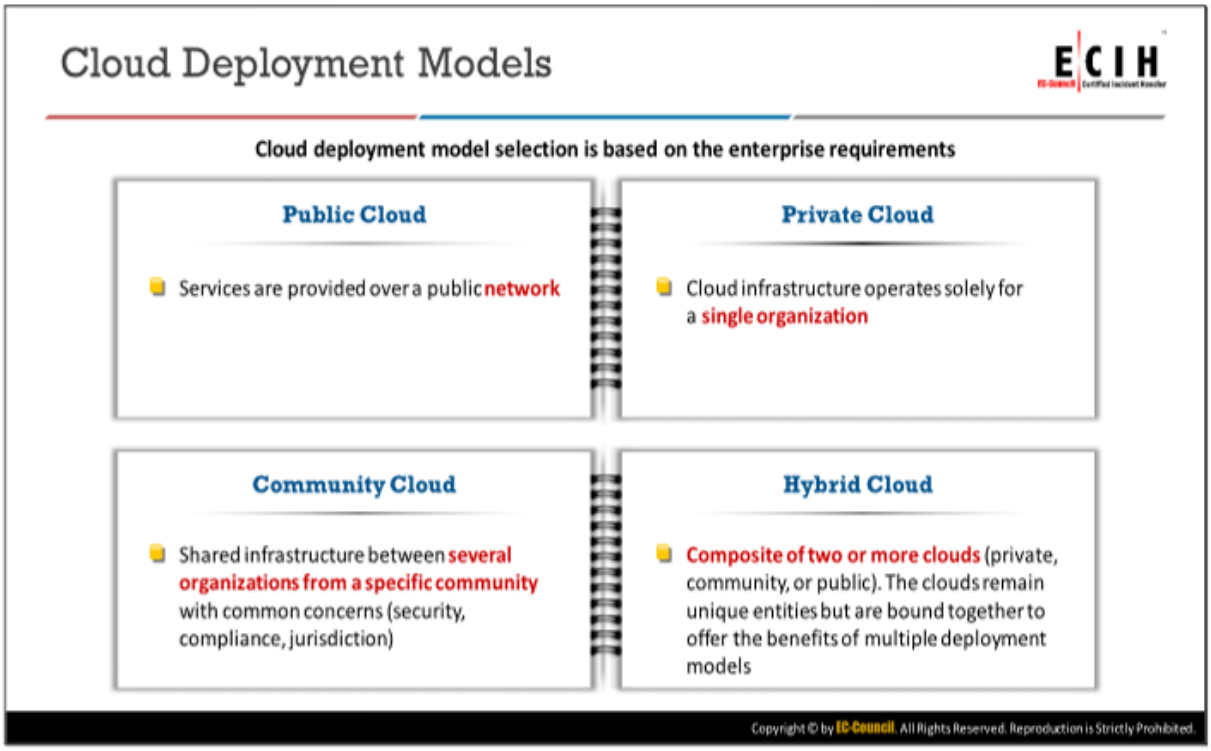
  The CC is responsible for installing the OS, build virtual middleware, data, applications, and access control of the cloud. The CC is responsible for all the incident response processes on the functions and assets it creates and maintains. Therefore, the CC should generate access logs, perform data duplication, and maintain backups of the data stored in the cloud.

- **PaaS**

  In PaaS, the CSP is responsible for providing a platform where the customers can install and run their applications, store data, and create accounts for different users. Therefore, the CC is only responsible for incident response regarding the data, applications, and access control data, whereas the CSP is responsible of all the cloud functions.

- **SaaS**

  In SaaS, the CSP offers all the required software, storage, applications, and data, while the CC creates accounts required to access the cloud services. In this case, the CSP is completely responsible for incident response, whereas the CC is liable to produce access control logs for incident responders.



Cloud Deployment Models

The selection of a cloud deployment model is based on the enterprise requirements. Cloud services can be deployed in different ways, according to the following factors:

- Host of cloud computing services
- Security requirements
- Sharing of cloud services
- Ability to manage some or all the cloud services
- Customization

Based on the type of ownership, size, and access, the four cloud deployment models are:

- **Public cloud**

  In this model, the provider makes services such as applications, servers, and data storage available to the public over the internet. The CSP is liable for creating and constantly maintaining the public cloud and its IT resources. Public cloud services may be free or adopt a pay-per-usage model and examples include Amazon Elastic Compute Cloud, IBM Cloud, Google App Engine, and Microsoft Azure cloud computing and services.

  - **Advantages:**
    - Simplicity and efficiency
    - Low cost
    - Reduced time (when server crashes, needs restarting or reconfiguring cloud)

- No maintenance (public cloud service is hosted off-site)
- No contracts (no long-term commitments)

- **Disadvantages:**
  - Lack of security
  - Lack of control (third-party providers are in charge)
  - Slow speed (relies on internet connections, limited data transfer rate)

- **Private cloud**

  A private cloud, also known as internal or corporate cloud, is a cloud infrastructure exclusively operated by a single organization. The organization can implement the private cloud within a corporate firewall. Organizations deploy private cloud infrastructures to retain full control over corporate data.

  - **Advantages:**
    - Enhanced security (cloud services are dedicated to a single organization)
    - Control over resources (organization is in charge)
    - High performance (deployed within the firewall, improving data transfer rates)
    - Customizable hardware, network, and storage performances (as the organization owns private cloud)
    - Easy to comply with relevant laws and standards (e.g., Sarbanes–Oxley Act, Payment Card Industry Data Security Standard—PCI DSS, and Health Insurance Portability and Accountability Act—HIPAA)
  - **Disadvantages:**
    - Expensive
    - On-site maintenance required

- **Community cloud**

  This model establishes a multi-tenant infrastructure shared among organizations from a specific community with common computing concerns such as security, regulatory compliance, performance requirements, and jurisdiction. The community cloud can be either on-premises or off-premises and governed by the participating organizations or by a third-party managed service provider.

  - **Advantages:**
    - Less expensive than private cloud
    - Flexibility to meet community needs
    - Compliance with legal regulations
    - High scalability

- Organizations can share a pool of resources from anywhere via internet

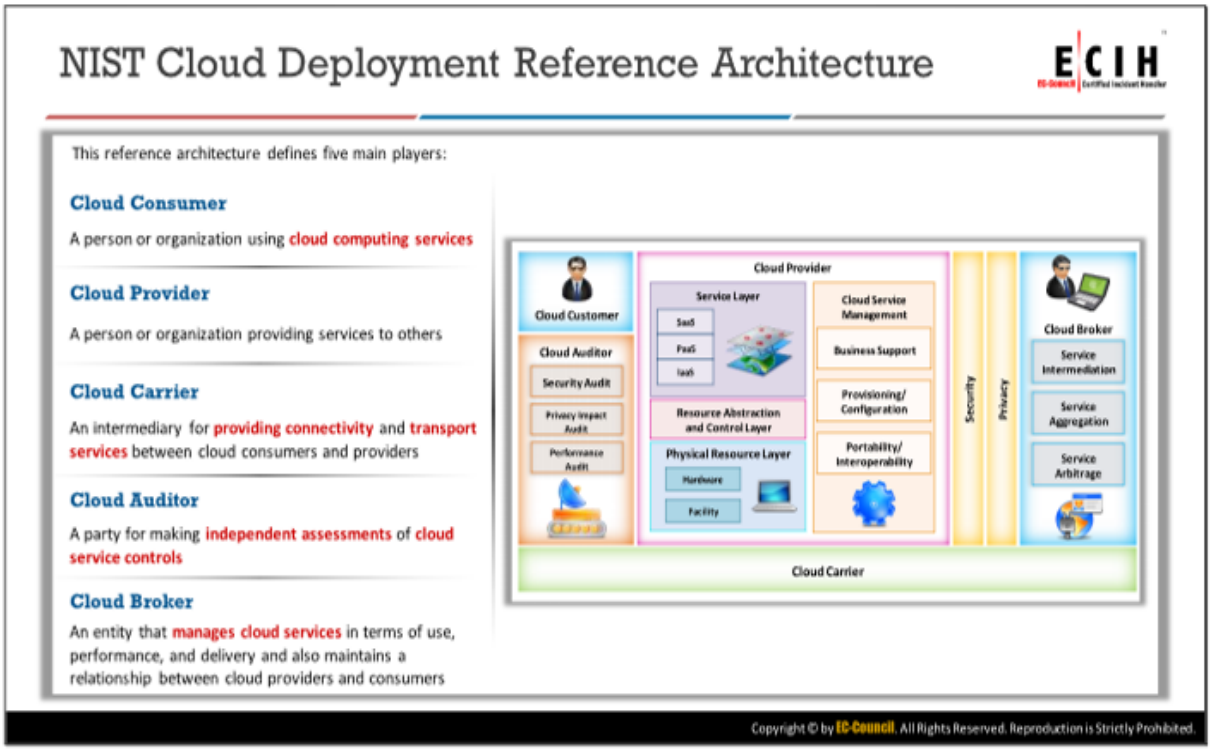
- **Disadvantages:**
  - Competition between customers in usage of resources
  - No accurate prediction of required resources
  - Difficulty to handle legal issues
  - Moderate security as other tenants can also access data
  - Trust and security concerns between tenants

- **Hybrid cloud**

  This cloud environment comprises two or more clouds (private, public, or community cloud) that remain unique entities but bound together for offering the benefits of multiple deployment models. In this model, the organization makes available the services, manages some resources in-house, and provides other resources externally.

  Example: An organization performs its critical activities on a private cloud (e.g., operational customer data) and non-critical activities on a public cloud.

  - **Advantages:**
    - More scalable as it can include public, private, and/or community clouds
    - Offers both secure resources and scalable public resources
    - High level of security (from a private cloud)
    - Allows to reduce and manage costs according to requirements
  - **Disadvantages:**
    - Communication at network level may conflict when implementing public and private clouds
    - Difficult to achieve data compliance
    - Organization should rely on internal IT infrastructure for support to handle any outages (requiring redundancy across data centers)
    - Complex service-level agreements (SLAs)



NIST Cloud Deployment Reference Architecture

The NIST cloud computing reference architecture helps to understand the major actors regarding computing, their activities, and functions in the cloud. The diagram on the above slide shows a generic high-level architecture to illustrate the uses, requirements, characteristics, and standards of cloud computing.

The five significant actors are:

- **Cloud consumer (CC)**

  A CC is a person or organization that maintains a business relationship with a CSP and uses cloud computing services. The CC browses the CSP service catalog requests for acquiring the desired services, sets up service contracts with the CSP (either directly or via a cloud broker), and uses the service. The CSP bills the CC according to the services provided. The CSP should fulfill an SLA in which the CC specifies technical performance requirements such as quality of service, security, and remedies for performance failures. The CSP may also define limitations and obligations, if any, that the CC must accept.

  The following services are available to a CC within IaaS, PaaS, and SaaS:

  - **IaaS**—storage, service management, CDN (content delivery network), platform hosting, backup and recovery, and computing
  - **PaaS**—database, business intelligence, application deployment, development and testing, and integration
  - **SaaS**—human resources, ERP (enterprise resource planning), sales, CRM, collaboration, document management, email and office productivity, content management, financials, and social networks

- **Cloud service provider (CSP)**

  A CSP, also known as cloud provider, is a person or organization that makes services available to the CCs. This entity acquires and manages the computing infrastructure intended for providing services (directly or via a cloud broker) to interested parties via network access. The CSP is responsible for managing the IT infrastructure, networks, services, and business applications required for the cloud services.

- **Cloud carrier**

  A cloud carrier acts as an intermediary that provides connectivity and transport services between CCs and CSPs. The cloud carrier provides access to consumers via network, telecommunication solutions, and access devices.

- **Cloud auditor**

  A cloud auditor performs independent examinations of cloud service controls to express an opinion thereon. Audits verify adherence to standards by reviewing objective evidence. A cloud auditor can evaluate the services provided by a CSP in terms of security controls (e.g., management, operational, and technical safeguards intended to protect confidentiality, integrity, and availability of the system and its information), privacy impact (e.g., compliance with applicable privacy laws and regulations governing individual's privacy), performance, among others.

- **Cloud broker**

  The integration of cloud services is becoming highly complex for CCs to manage. Thus, a CC may request cloud services from a cloud broker rather than directly contacting a CSP. The cloud broker is an entity that manages cloud services in terms of use, performance, and delivery, and supports the relationship between CCs and CSPs.

  Cloud brokers provide services in three categories:

  - **Service intermediation**

    Improves a given function by adding specific capabilities to provide value-added services to CCs

  - **Service aggregation**

    Combines and integrates multiple services into one or more new services

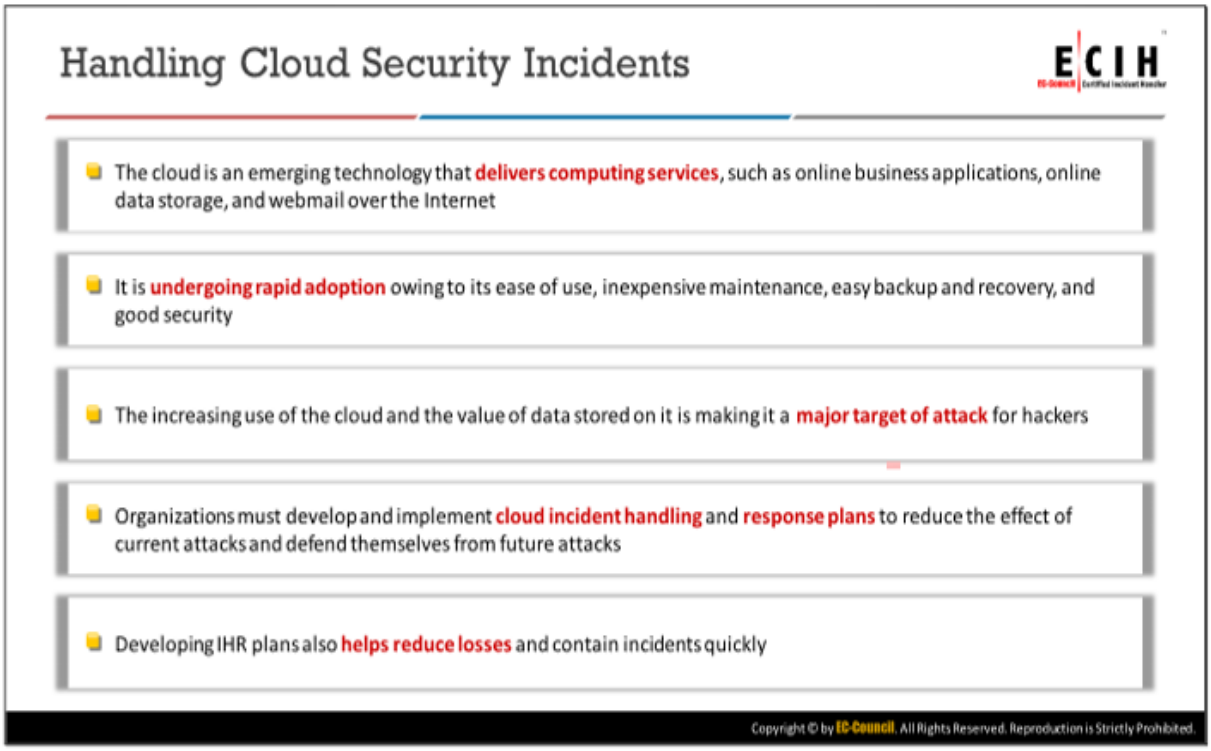
  - **Service arbitrage**

    Similar to service aggregation, but the aggregated services are not fixed (e.g., the cloud broker flexibly chooses services from different CSPs)

Overview of Handling Cloud Security Incidents

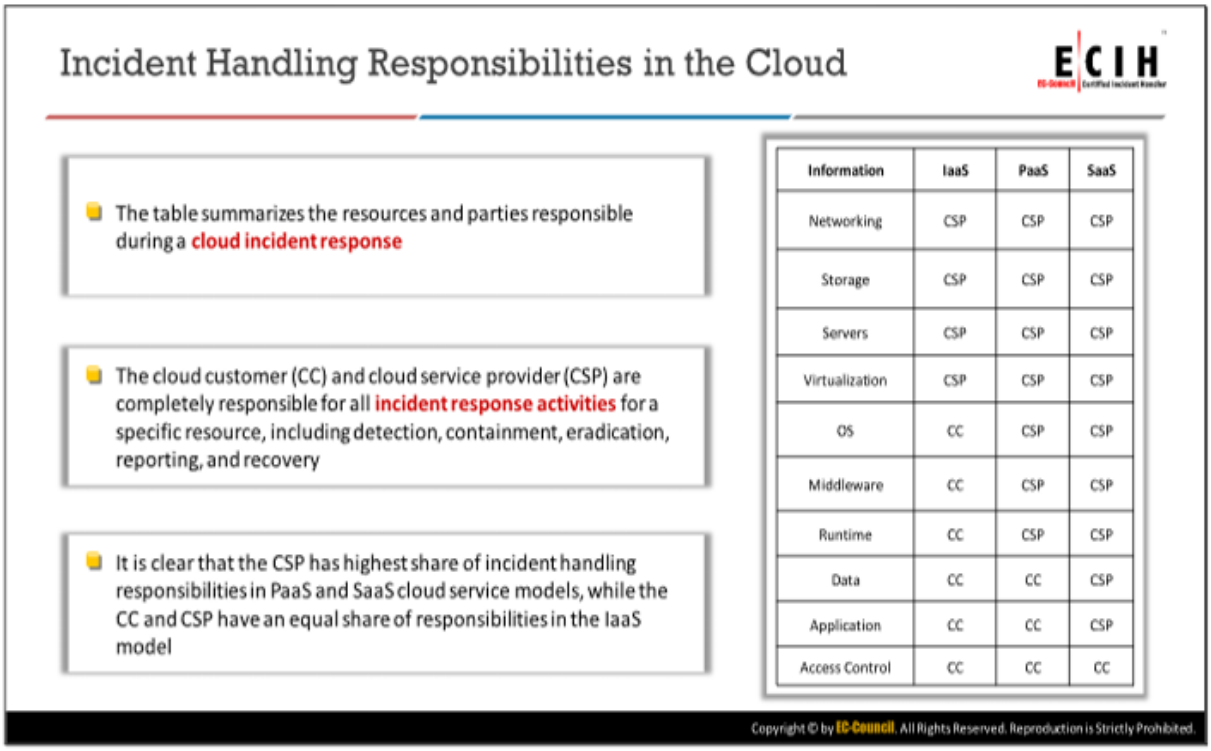
The enormous benefits that the cloud offers have increased the dependency of organizations and society on its services. In this scenario, securing the cloud resources, services, and stored data against various cybersecurity incidents is a major challenge. Incident handlers must understand how to handle various cloud security incidents.

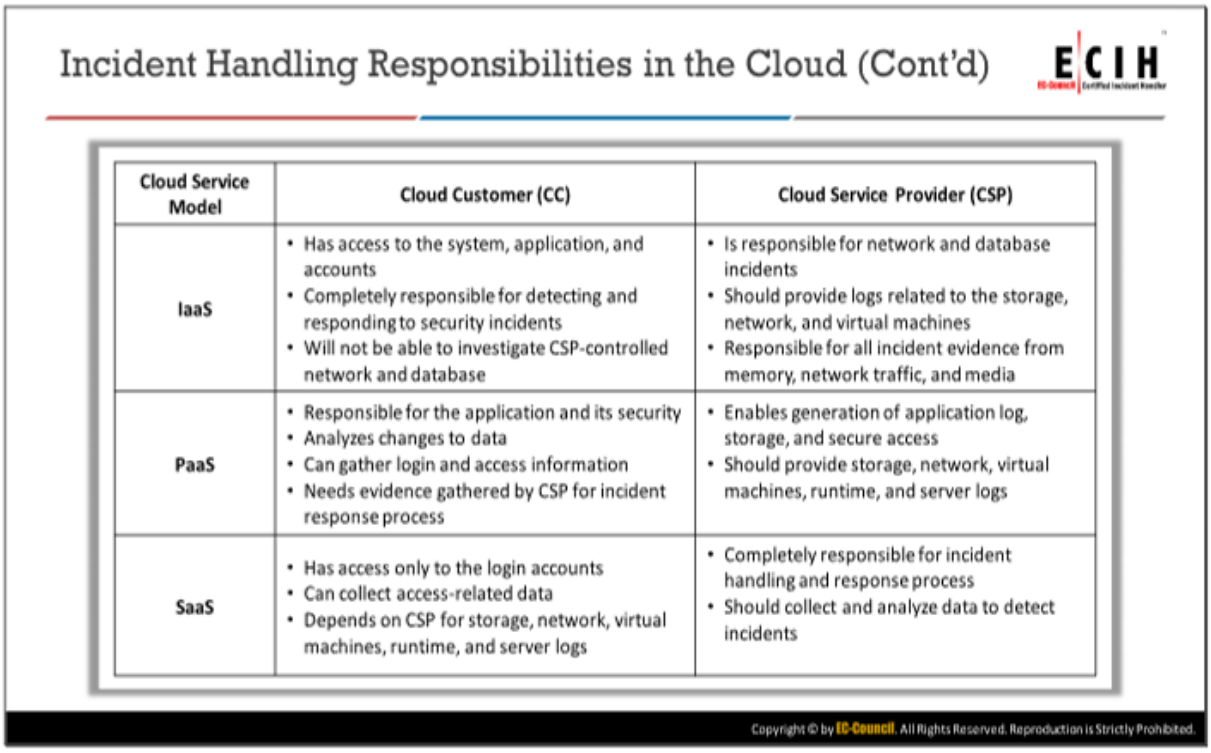
This section provides an introduction on handling cloud security incidents, discusses various incident handling responsibilities in the cloud and various challenges regarding cloud security incident handling and response.



Handling Cloud Security Incidents

The cloud is an emerging technology that delivers computing services such as online business applications, online data storage, and webmail over the internet. It is being increasingly adopted given the myriad of benefits including ease of use, inexpensive maintenance, ease in backup and recovery, and security. The cloud also enables organizations to implement a distributed workforce, reduce expenses, among other advantages. However, with the increased adoption and value of stored data, the cloud has become a major target of attackers. Therefore, organizations must develop and implement cloud security incident handling and response plans to reduce the impact of existing attacks and defend themselves from future attacks. In addition, developing this plan helps to reduce losses and contain incidents within the shortest time possible.





Incident Handling Responsibilities in the Cloud

The table shown on the slide lists the resources required for a cloud service and the party responsible for collection of evidence from each resource in the cloud service models. The CSP clearly has the highest share of incident handling responsibilities in the PaaS and SaaS models, while both the CC and CSP share responsibilities in the IaaS model. Moreover, the CC and CSP should handle their corresponding processes of incident response, including detection, analysis, containment, eradication, and recovery.

The table given on the slide describes the responsibilities of CCs and CSPs in handling cloud security incidents according to the cloud service model.

Challenges in Cloud Security Incident Handling and Response

Architecture and Identification

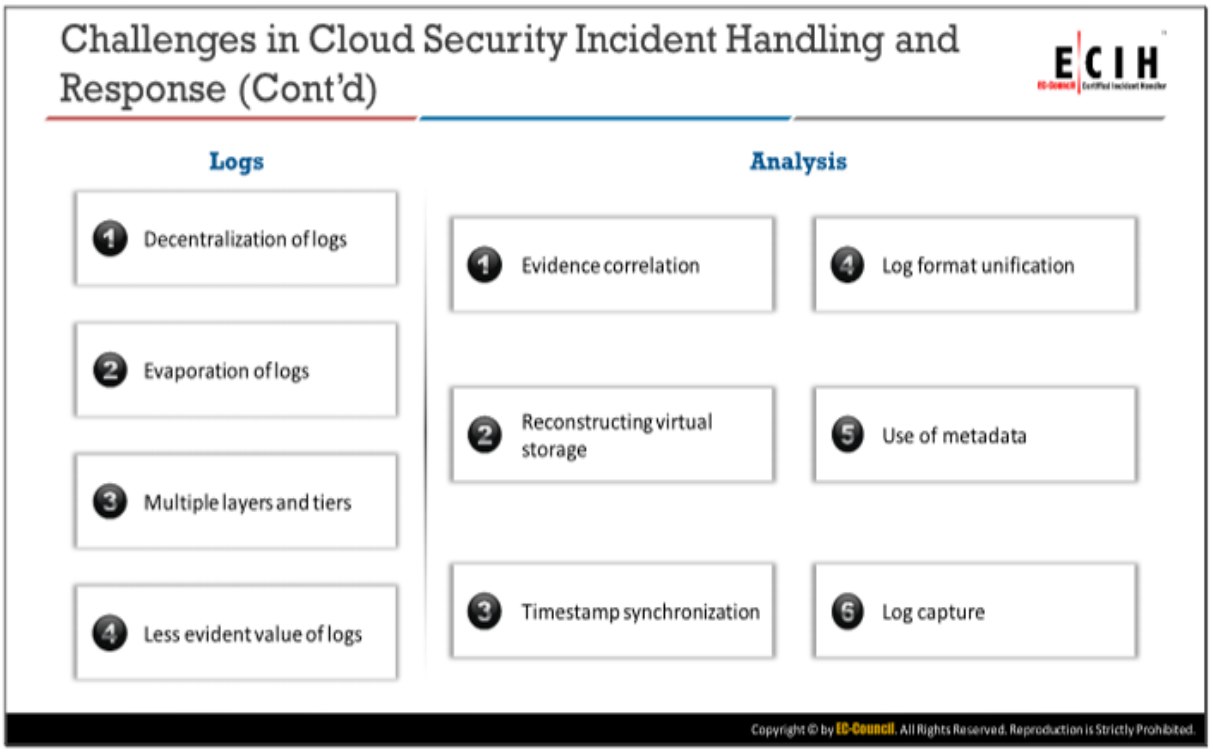
1 Deletion in the cloud	7 Criminals access to low-cost computing power	13 Cloud confiscation and resource seizure
2 Recovering overwritten data	8 Real-time investigation intelligence processes not possible	14 Errors in cloud-management portal configurations
3 Interoperability issues among CSPs	9 Malicious code may circumvent VM isolation methods	15 Potential evidence segregation
4 Single points of failure	10 Multiple venues and geo-locations	16 Boundaries
5 No single point of failure for criminals	11 Lack of transparency	17 Secure provenance
6 Detection of the malicious act	12 Locating criminal activity in the cloud	18 Data chain of custody

Source: NIST Cloud Computing Forensic Science Challenges (*http://csrc.nist.gov*)

Challenges in Cloud Security Incident Handling and Response (Cont'd)

Data Collection

1 Decreased access and data control	7 Locating storage media	13 Additional collection is often not possible	19 Root of trust
2 Chain of dependencies	8 Evidence identification	14 Imaging the cloud	
3 Locating evidence	9 Dynamic storage	15 Selective data acquisition	
4 Data location	10 Live forensics	16 Cryptographic key management	
5 Imaging and isolating data	11 Resource abstraction	17 Ambiguous trust boundaries	
6 Data available for a limited time	12 Application details are not available	18 Data integrity and evidence preservation	



Challenges in Cloud Security Incident Handling and Response

Source: NIST Cloud Computing Forensic Science Challenges (*http://csrc.nist.gov*)

Given the variety of services and huge amount of stored data, the cloud is rapidly becoming a main target of cybercriminals. The increasing ratio of attacks to the cloud poses many challenges for handling and responding to the various types of cloud security incidents. We describe below these challenges:

- **Architecture and identification**
  - **Deletion in the cloud**
    - The total volume of data and users operating regularly in a cloud environment confines the amount of backups retained by the CSP.
    - CSPs may not implement necessary methods to retrieve information from deleted data in the IaaS or PaaS model.
  - **Recovering overwritten data**
    - It is very difficult to recover data marked as deleted, as they may be overwritten by data of another user sharing the cloud.
    - A snapshot (e.g., backup) might not be taken timely for preserving a data duplicate before overwriting.
  - **Interoperability issues among CSPs**
    - Collection and preservation of forensic evidence is challenging given the lack of both interoperability among CSPs and control from the CC end of the proprietary architecture and/or technology being used.
  - **Single points of failure**
    - The cloud ecosystem has single points of failure, which may adversely affect evidence acquisition.
  - **No single point of failure for criminals**
    - Collection and analysis of evidentiary data from distributed and disparate sources is highly difficult, as criminals may choose one CSP to store data, another CSP to obtain computing services, and a third CSP to route their communications.
  - **Detection of malicious act**
    - It is difficult for an incident handler to detect a malicious act by identifying the series of small changes made across many systems and applications conforming the attack launched by a perpetrator to access the cloud.
  - **Criminals access to low-cost computing power**
    - Cloud computing provides computing power that would otherwise be not available to criminals at a low cost, thus enabling unpredictable attacks that would be unfeasible outside a cloud environment.
  - **Real-time investigation intelligence processes not possible**
    - Investigating real-time incidents in the cloud is very difficult as it requires intelligence processes, which are often not possible while working along with the CSPs or other actors. A special legal means should be applied in many cases to collect data.

- **Malicious code may circumvent VM isolation**
  - Vulnerabilities in server virtualization allow malicious code to evade VM isolation and interfere with either other guest VMs or the hypervisor itself.
- **Multiple venues and geolocations**
  - Managing the scope of data collection is challenging, as distributed data collection and chain of custody from multiple venues or geolocation unknowns can lead to jurisdictional issues.
- **Lack of transparency**
  - Cloud operational details are not clear enough to incident handlers, resulting in lack of trust and hindering auditing.
- **Criminals can hide in the cloud**
  - The distributed nature of cloud computing allows criminal organizations to maintain isolated cells of operation and preserve anonymity among cells, thus hindering identification and correlation of cells by incident handlers.
- **Cloud confiscation and resource seizure**
  - Cloud confiscation and resource seizure may often affect the business continuity of other tenants.
- **Errors in cloud management portal configurations**
  - Configuration errors in cloud management portals may allow an attacker to gain control, reconfigure, or delete CC resources or applications.
  - It is hard to find the source of such unauthorized change, because the cloud management portal is being used by multiple tenants simultaneously.
- **Potential evidence segregation**
  - Segregation of potential evidence pertaining to one tenant in a multi-tenant cloud system is challenging because it cannot be achieved without breaching the confidentiality of other tenants.
- **Boundaries**
  - Protecting system boundaries is challenging, as it is difficult to define system interfaces.
- **Secure provenance**
  - It is a challenge for incident handlers to maintain proper chain of custody and security of data, metadata, and possibly hardware, as determining the ownership, custody, or exact resource location may be difficult.

- **Data chain of custody**
  - It is almost impossible to identify and validate a data chain of custody given the multilayered and distributed nature of cloud computing.

- **Data collection**
  - **Decreased access and data control**
    - In every combination of cloud service model and deployment model, the incident handler has limited access and control of forensic data.
    - CSPs hide data locations purposefully to ease data movement and replication.
  - **Chain of dependencies**
    - Often, CSPs and most cloud apps rely on other CSP(s), and the dependencies in a chain of CSPs/CCs can be highly dynamic.
    - In such conditions, handling cloud security incidents may rely on investigation of each link in the chain and level of complexity of dependencies.
  - **Locating evidence**
    - Locating and collecting evidence is challenging because data in the cloud may be quickly altered or lost and given the lack of knowledge on where and how data are stored in the cloud.
  - **Data location**
    - Collecting data of a target is challenging by the CSP flexibility to migrate data between data centers and geographic locations.
  - **Imaging and isolating data**
    - Data imaging and isolating, a migrating data target, is challenging in the cloud ecosystem due to its key characteristics: elasticity, automatic provisioning/deprovisioning of resources, redundancy, and multi-tenancy.
  - **Data available for limited time**
    - Data collection and preservation of VM instances are challenging due to the lack of standard practices and tools.
  - **Locating storage media**
    - Locating storage media with certainty in the cloud ecosystem is difficult as it requires in-depth understanding of the cloud architecture and implementation.
  - **Evidence identification**
    - Evidence identification is challenging because the sources/traces of evidence are either not accessible or created/stored differently than in non-cloud environments.

- **Dynamic storage**
  - Often, CSPs dynamically allocate storage based on the CC requirements, thus hindering data collection, and systems search storage after an item is deleted.
- **Live forensics**
  - Validating the integrity of collected data is challenging because data within the cloud are volatile and frequently changing. In addition, live forensics tools may make modifications to the suspect system.
- **Resource abstraction**
  - Identifying and collecting evidentiary data are challenging tasks because resources are abstracted and information about the cloud architecture, hardware, hypervisor, and file system is not available to exactly understand the cloud environment.
- **Unavailable application details**
  - Obtaining details of cloud-based software/applications used to create records is challenging because such details are usually unavailable to the incident handler.
- **Unfeasibility of additional collection in the cloud**
  - Collecting additional evidence is often unfeasible in the cloud, as specific data locations are not known, the system size may be prohibitive, and non-standard protocols and mechanisms may have been used to exchange data with poorly or inexistent documentation.
- **Imaging the cloud**
  - Imaging the cloud is challenging because it is unfeasible as a whole, while partial imaging may have legal consequences during presentation to a court.
- **Selective data acquisition**
  - Selective data acquisition in the cloud is challenging because it requires gaining prior knowledge about the relevant data sources, which is very difficult.
- **Cryptographic key management**
  - Decryption of data is challenging because ineffective cryptographic key management contributes to lose the ability to decrypt forensic data stored in the cloud.
- **Ambiguous trust boundaries**
  - In a multi-tenant cloud environment, using cloud services may increase the risk to data integrity both at rest and during processing.
  - Not all CSPs implement vertical isolation for tenants' data, leading to questionable data integrity.

- **Data integrity and evidence preservation**
  - For stakeholders, maintaining evidence quality, evidence admissibility, data integrity, and evidence preservation is challenging because faults and failures in data integrity are shared among multiple parties, and the chance for such faults and failures is high in a cloud environment due to shared data/responsibilities.
- **Root of trust**
  - Determining the reliability and integrity of cloud forensics data is challenging given the dependence on collective integrity of multiple layers of abstraction throughout the cloud ecosystem.

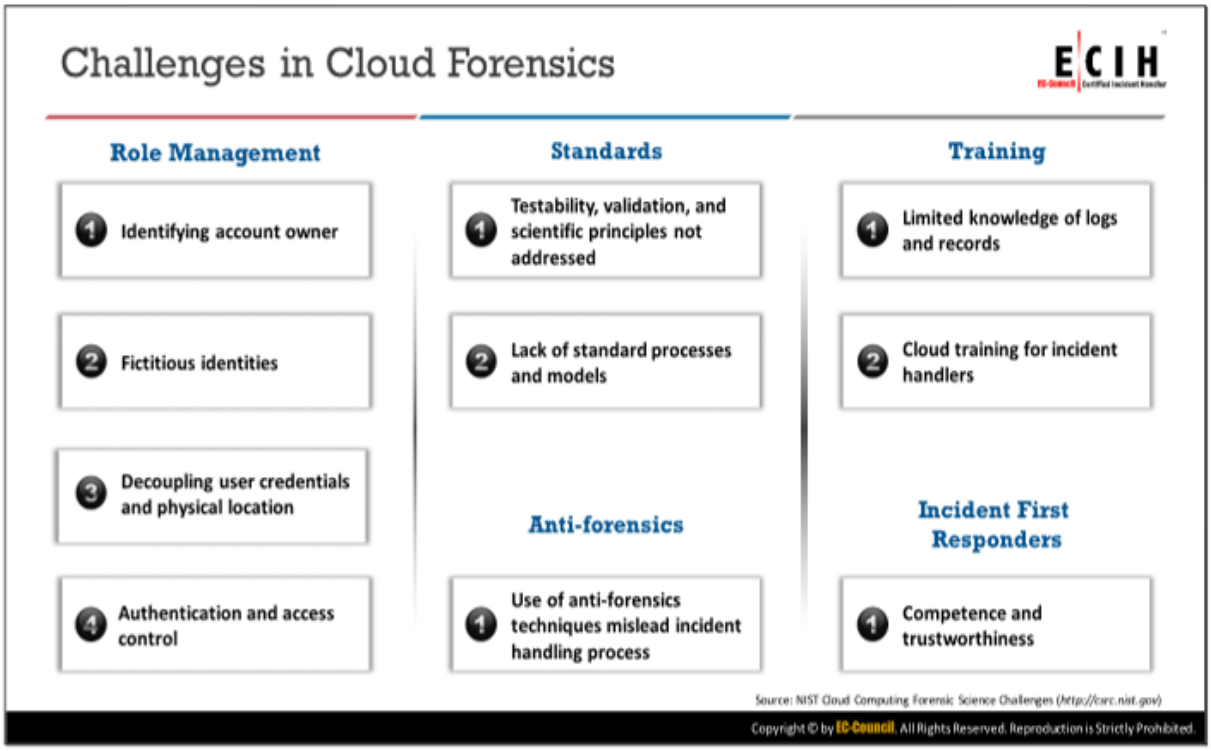
- **Logs**
  - **Decentralization of logs**
    - Log information is not stored at a centralized log server in the cloud but distributed across different servers.
  - **Evaporation of logs**
    - Some logs in the cloud environment are stored in volatile memory, such as in VMs. Once the VM instance is switched off, the logs vanish.
  - **Multiple layers and tiers**
    - There are many layers and tiers in the cloud architecture, and logs are generated in each tier. These logs are valuable to the incident handler but the collection from different places (e.g., application, network, OS, and database) is challenging.
  - **Less-evidently value of logs**
    - Different CSPs and different layers of cloud architecture provide logs in different (heterogeneous) formats, and not all logs provide relevant information (e.g., who, when, where, and why some incident was executed) for detection and analysis of cloud security incidents.

- **Analysis**
  - **Evidence correlation**
    - Correlation of an activity across multiple CSPs is challenging due to the lack of interoperability.
  - **Reconstructing virtual storage**
    - Virtual storage media duplication in some cloud ecosystems may cause damage to the actual media, thereby increasing the risk of being prosecuted.
    - Reconstruction algorithms should be developed and validated.

- **Timestamp synchronization**
  - Correlating activities observed with accurate time synchronization is challenging because timestamps may be inconsistent between different sources.
- **Log format unification**
  - Unifying log formats or converting them into each other is very difficult given the enormous number of resources available in the cloud. Conversion may also result in lack and/or exclusion of critical data.
  - On the other hand, uncommon or proprietary log formats of one party can become a major hurdle when combining information.
- **Use of metadata**
  - Using metadata as authentication method may be at risk, because common fields (e.g., creation date, last accessed date, last modified date) may change when data are moved into and within the cloud and during data gathering.
  - Considering the impact of cloud on metadata, it should be checked whether the CSP preserves metadata and are readily accessible for e-discovery purposes.
- **Log capture**
  - Timeline analysis of logs for DHCP (Dynamic Host Configuration Protocol) log data is challenging due to inconsistencies across CSPs regarding log data collection.

- **Legal**
  - **Missing terms in contract or SLA**
    - Lack of forensic related terms in cloud contracts may prevent the generation and collection of existing relevant data and generation of potentially relevant data.
  - **Limited investigative power**
    - In civil cases, incident handlers are often provided with limited investigative power to properly obtain data under the corresponding jurisdictions.
  - **Reliance on cloud providers**
    - Acquiring forensic data from the cloud requires CSP cooperation, which may be limited by the number of employees and other resources in the provider end.
  - **Physical data location**
    - Specifying the physical location(s) of data on a subpoena is challenging because the requestor often does not know where the data are physically stored.
  - **Port protection**
    - Scanning ports is challenging because CSPs do not provide access to the physical infrastructure of their networks.

- **Transfer protocol**
  - Dumping of TCP/IP (Transmission Control Protocol/Internet Protocol) network traffic is challenging because CSPs do not provide access to the physical infrastructure of their networks.
- **E-Discovery**
  - The response time for e-discovery can be compromised by the ambiguity of data location and uncertainty about whether all relevant data were discovered.
- **Lack of international agreements and laws**
  - Gaining access and exchanging data are challenging tasks due to the lack of international collaboration and legislative mechanisms across nations.
- **International cloud services**
  - Real-time live access to data on international cloud services is challenging by the lack of definition regarding the scope of data acquisition on non-national cloud services and agreements dealing with authority to access data.
- **Jurisdiction**
  - Gaining legal access to data is challenging because questions of international jurisdictions may have not been addressed.
- **International communication**
  - Achieving effective, timely, and efficient international communication when dealing with an incident in a multijurisdictional cloud is challenging because existing mechanisms and networks for such communication are often slow and inefficient.
- **Confidentiality and personally identifiable information**
  - Preserving privacy of personal, business, and governmental information in the cloud is challenging due to the lack of legislation governing the conditions under which such data can be accessed by incident handlers.
- **Reputation fate sharing**
  - For CSPs and co-tenants, recovering the reputation affected by illegal activity of a CC is challenging because a spammer using the CSP IP range may lead to blacklisting of these IP addresses.
  - The compromised cloud can disrupt the service for legitimate CCs if they are later assigned the blacklisted IP addresses.



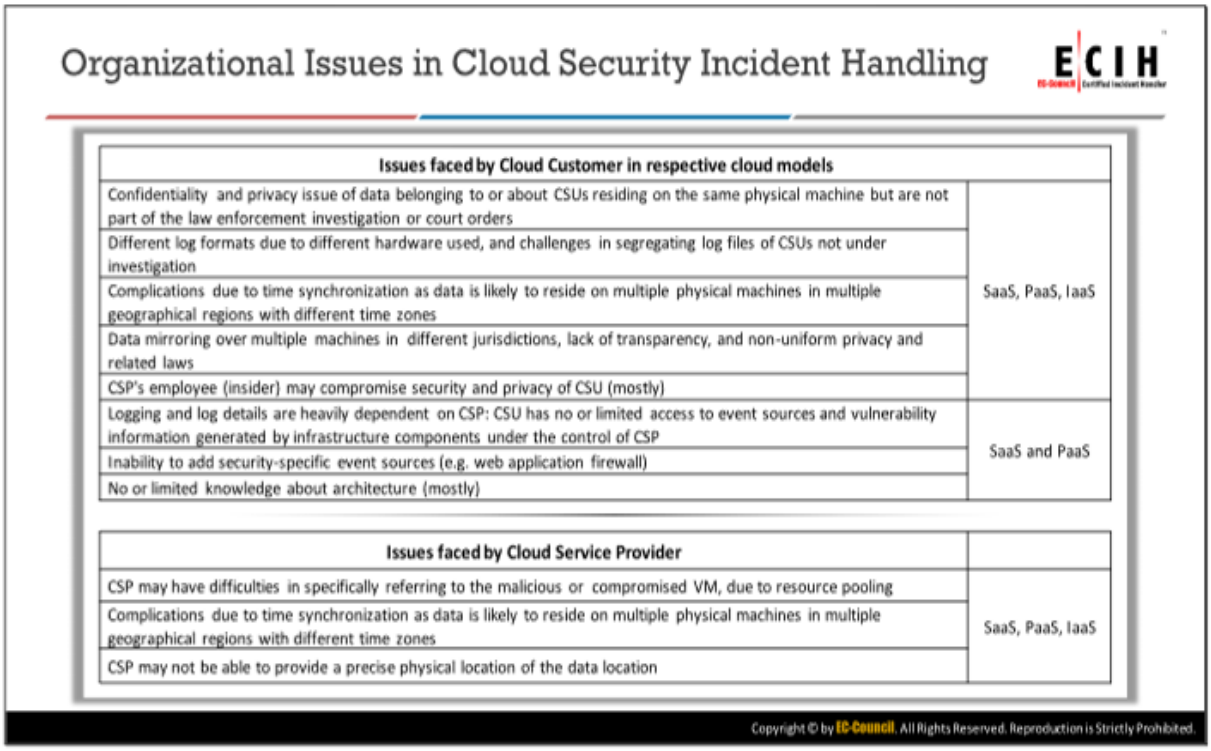
Challenges in Cloud Forensics

Source: NIST Cloud Computing Forensic Science Challenges (*http://csrc.nist.gov*)

Below, we discuss various challenges related to cloud forensics:

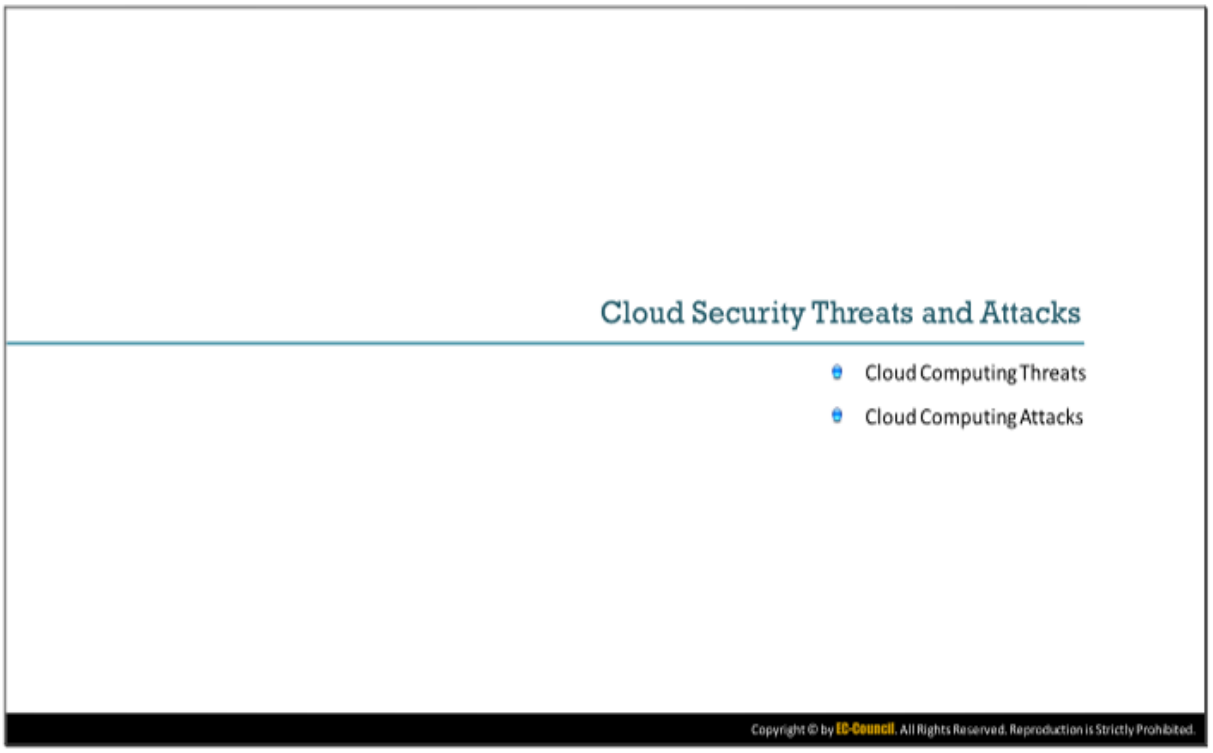
- **Role management**
  - **Identifying account owner**
    - Identifying the owner of an account is challenging because the technology or policy usually does not allow sufficient identification.
  - **Fictitious identities**
    - Determining the identity of a cloud user as being legitimate or illegitimate is challenging because criminals can often create accounts with fake identities.
  - **Decoupling user credentials and physical location**
    - Positively attributing a cloud user's credentials to a physical user is challenging because no mandatory non-repudiation methods are implemented in the cloud, and sophisticated encryption and network proxy services may question the validity of network-type metadata.
  - **Authentication and access control**
    - Positively identifying the entities that accessed data without being authorized is challenging because the authentication and access control to users' cloud accounts may not adhere to data protection regulations.

- **Standards**
  - **Testability, validation, and scientific principles not addressed**
    - Using and/or collecting results from tested and validated tools and techniques is challenging given the scarcity of test beds, test processes, validated techniques, and trained test engineers specialized in cloud environments.
  - **Lack of standard processes and models**
    - Establishing standard procedures and best practices for handling incidents in the cloud is challenging because such standards and procedures and those for response are much less mature than in traditional incident handling and far from being widely adopted.
- **Training**
  - **Limited knowledge of logs and records**
    - Trusting records/logs kept in cloud environments is challenging because custodians and individuals responsible for these operations might have only limited knowledge and may not be qualified for evidence preservation.
  - **Cloud training for incident handlers**
    - Training in cloud computing technology and incident handling and response operations in cloud environments may be inadequate because most training materials are outdated and do not address cloud environments.
- **Anti-forensics**
  - Using anti-forensics techniques (e.g., obfuscation, data hiding, malware) prevents or misleads incident handling and may affect data collection, preservation, and identification during forensic investigation.
  - For example, malware may circumvent VM isolation.
- **Incident first responders**
  - **Competence and trustworthiness**
    - For stakeholders, confidence, competence, and trustworthiness of CSPs acting as first responders are challenged as the objectives and priorities of CSPs may differ from those of the incident handlers.
    - For example, when an incident occurs in the CSP end, its main concern is to restore the service rather than preserving evidence.



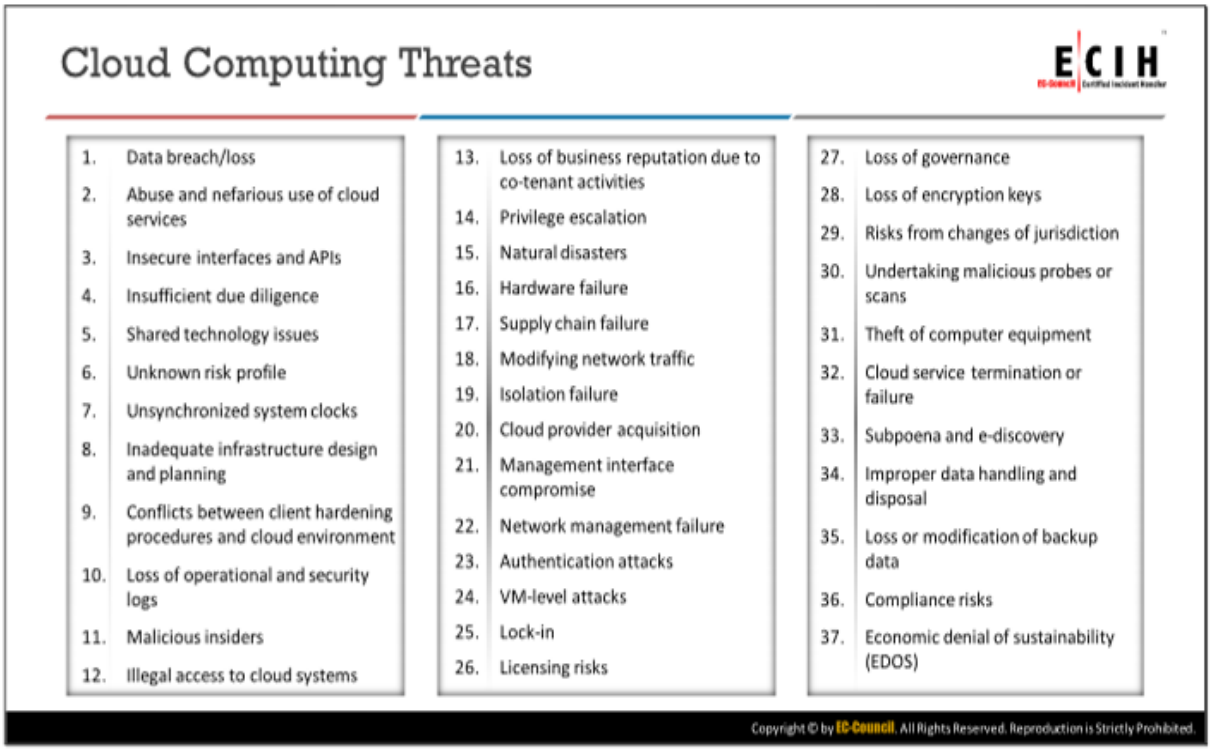
Organizational Issues in Cloud Security Incident Handling

The table given on the slide describes various organizational issues while handling and responding to cloud security incidents.



Cloud Security Threats and Attacks

Most organizations adopt cloud technologies to reduce costs via optimized and efficient computing and obtain other advantages provided by the cloud. Robust cloud technology offers different types of services to end users. However, users are concerned about critical cloud security risks and threats that can be exploited by attackers to compromise data security, gain illegal access to the network, among other harmful activities. This section describes various cloud security threats and attacks.



Cloud Computing Threats

Below, we discuss various threats to cloud computing:

- **Data breach/loss**

  An improperly designed cloud computing environment with multiple clients is at high risk of data breach as a flaw in one client's application may allow attackers to access other clients' data. Data loss or leakage is highly dependent on the cloud architecture and its operation.

  Data loss issues include:

  - Data are erased, modified, or decoupled (lost)
  - Encryption keys are lost, misplaced, or stolen
  - Illegal access to data in the cloud occurring due to improper authentication, authorization, and access controls
  - Data are misused by CSP

- **Abuse and nefarious use of cloud services**

  Weak registration systems in the cloud environment give rise to this threat. Attackers create anonymous accesses to cloud services and perpetrate various attacks such as password cracking, building rainbow tables and CAPTCHA farms, launching dynamic attack points, hosting exploits on cloud platforms, hosting malicious data, botnet command or control, and DDoS (distributed denial of service).

- **Insecure interfaces and APIs**

  Interfaces or APIs allow CCs to manage and interact with cloud services. Nevertheless, cloud service models must be security integrated, and users must be aware of security risks during use, implementation, and monitoring of such services. Some interface and API risks are listed below:

  - Circumvent user-defined policies
  - Lack of credential leak proof
  - Breach in logging and monitoring facilities
  - Unknown API dependencies
  - Reusable passwords/tokens
  - Insufficient input data validation

- **Insufficient due diligence**

  Ignorance of the CSP cloud environment poses risks to operational responsibilities such as security, encryption, incident response, and related problems including contractual issues as well as design and architectural issues.

- **Shared technology issues**

  IaaS vendors share infrastructure to deliver services in a scalable way. Most underlying components that constitute this infrastructure (e.g., GPU, CPU caches) do not offer substantial isolation properties in a multi-tenant environment, enabling attackers to attack other machines if they can exploit vulnerabilities in clients' applications. To address this gap, virtualization hypervisors mediate access between guest OSs and the physical resources possibly containing loopholes that allow hackers to gain unauthorized control over the underlying platforms. Issues include Rutkowska's Red and Blue Pill exploits and Kortchinsky's Cloudburst presentations.

- **Unknown risk profile**

  Software updates, threat analysis, intrusion detection, security practices, and various other components determine the security posture of an organization. Client organizations are unable to clearly analyze internal security procedures, security compliance, configuration hardening, patching, auditing, and logging, because they are less involved with the hardware and software ownership and maintenance in the cloud. However, organizations must be aware of issues such as internal security procedures, security compliance, configuration hardening, patching, and auditing and logging.

- **Unsynchronized system clocks**

  This threat arises due to the failure of synchronizing clocks at end systems. Unsynchronized clocks can affect the operation of automated tasks. For example, if cloud computing devices do not have synchronized or matched times, the divergence of timestamps may render the network administrator unable to accurately analyze log files for any malicious activity. Unsynchronized clocks can cause various other problems. For

example, in case of money transactions or database backups, mismatched timestamps may result in significant problems or discrepancies.

- **Inadequate infrastructure design and planning**

  An agreement between the CC and CSP establishes the quality of service that the CSP offers regarding aspects such as downtime, physical- and network-based redundancies, standard data backup, restore processes, and availability periods.

  At times, CSPs may not satisfy the rapid rise in demand due to a shortage of computing resources and/or poor network design (e.g., traffic flows through a single point despite the necessary hardware being available), leading to unacceptable network latency or inability to meet the agreed service levels.

- **Conflicts between client hardening procedures and cloud environment**

  Certain client hardening procedures may conflict with a CSP environment, impeding their implementation by the CC. In fact, as a cloud is a multi-tenant environment, the colocation of many CCs causes conflict for CSPs, whose CCs' communication security requirements are likely to diverge from one another.

- **Loss of operational and security logs**

  The loss of operational logs hinders the evaluation of operational variables, and the options for solving issues are limited when no data are available for analysis. The loss of security logs threatens the implementation of an information security management program. Loss of security logs may occur if storage is under-provisioned.

- **Malicious insiders**

  Malicious insiders are disgruntled current/former employees, contractors, or other business partners who have/had authorized access to cloud resources, intentionally exceeding or misusing that access to compromise the confidentiality, integrity, or availability of the organization's information. Malicious insiders who have authorized access to cloud resources can also abuse their position to compromise the information available in the cloud. Threats include loss of reputation, productivity, and financial theft.

- **Illegal access to the cloud**

  Weak authentication and authorization controls can lead to unlawful access, thereby compromising confidential and critical data stored in the cloud.

- **Loss of business reputation due to co-tenant activities**

  This threat arises by inappropriate resource isolation, lack of reputational isolation, vulnerabilities in the hypervisors, among other causes. As resources are shared in the cloud, malicious activity of one co-tenant might affect the reputation of others, resulting in poor service delivery, data loss, and other consequences that undermine the organization's reputation.

- **Privilege escalation**

  A mistake in the access allocation system, such as coding errors and design flaws, can result in a customer, third party, or employee obtaining more access rights than intended. This threat arises by AAA (authentication, authorization, and accountability) vulnerabilities, user provisioning and deprovisioning vulnerabilities, hypervisor vulnerabilities, unclear roles and responsibilities, misconfiguration, among other factors.

- **Natural disasters**

  Depending on the geographic location and climate, data centers may be exposed to natural disasters such as floods, lightning, and earthquakes that can affect cloud services.

- **Hardware failure**

  Hardware failure in devices such as switches, servers, routers, access points, hard disks, network cards, and processors in data centers can render cloud data inaccessible. Most hardware failures occur by hard disk problems, whose identification, tracking, and solving are time consuming given low-level complexities. Hardware failures can lead to poor performance experienced by end users and harm business activities.

- **Supply chain failure**

  This threat arises by aspects such as incomplete and non-transparent terms of use, hidden dependencies created by cross-cloud applications, inappropriate CSP selection, and lack of supplier redundancy. As CSPs outsource certain tasks to third parties, the security of the cloud is directly proportional to that of each link and the extent of dependency on third parties. A disruption in the chain may lead to loss of data privacy and integrity, service unavailability, SLA violations, economic and reputational losses when failing to meet the CC demand, and cascading failures.

- **Modification of network traffic**

  The network traffic in the cloud may be altered by flaws during provisioning or deprovisioning and vulnerabilities in communication encryption. Modification of network traffic may cause loss, alteration, or theft of confidential data and communications. This threat arises by vulnerabilities in user provisioning and deprovisioning, communication encryption, among other causes.

- **Isolation failure**

  Multi-tenancy and shared resources characterize cloud computing. Strong isolation or compartmentalization of storage, memory, routing, and reputation among different tenants may be lacking. By exploiting isolation failures, attackers may be able to control operations of other CCs and gain illegal access to data.

- **CSP acquisition**

  CSP acquisition may increase the probability of tactical shift and affect non-binding agreements at risk. This could hinder compliance with security requirements.

- **Management interface compromise**

  The customer management interfaces of CSPs are accessible via the internet and facilitate access to several resources. This access increases risks, especially when combined with remote access and web browser vulnerabilities. This threat arises by improper configuration, system and application vulnerabilities, remote access to the management interface, and so on.

- **Network management failure**

  Poor network management leads to network congestion, misconnection, misconfiguration, lack of resource isolation, and other inconveniences, affecting both services and security.

- **Authentication attacks**

  Weak authentication mechanisms (e.g., weak passwords, reuse of passwords) and inherent limitations of one-factor authentication may allow attackers to gain unauthorized access to cloud computing systems.

- **VM-level attacks**

  Cloud computing extensively uses virtualization technologies offered by several vendors including VMware, Xen, VirtualBox, and vSphere. Threats to these technologies arise by vulnerabilities in the hypervisors.

- **Lock-in**

  Lock-in refers to the inability of CCs to migrate from one CSP to either another CSP or in-house systems by the lack of tools, procedures, or standard formats for data, applications, and service portability. This threat arises by inappropriate selection of CSP, incomplete and non-transparent terms of use, lack of standardization, among other factors.

- **Licensing risks**

  The CC may incur in substantial licensing fees if the CSP charges the software deployed in the cloud on a per-instance basis. Therefore, the CC should always retain ownership over its software assets located in the CSP environment. Risks to licensing occur by incomplete and non-transparent terms of use.

- **Loss of governance**

  When using cloud infrastructures, CCs grant control to CSPs regarding issues that can affect security. In addition, SLAs may not offer a commitment on the part of the CSP to provide such services, thus leaving a gap in security defenses. This threat results from unclearness of roles and responsibilities, lack of a vulnerability assessment process, conflicting promises in SLAs, no certification schemes, lack of jurisdiction, unavailability of audits, among other factors.

Loss of governance results in consequences such as noncompliance with security requirements, lack of confidentiality, integrity, and availability of data, poor performance and quality of service.

- **Loss of encryption keys**

  The loss of encryption keys required for secure communication or system access may allow a potential attacker to get unauthorized assets. This threat arises due to poor management of keys and key generation techniques.

- **Risks from changes of jurisdiction**

  Clouds may store CC data in multiple jurisdictions, of which some may represent high risks. Local authorities in high-risk countries (e.g., those without the rule of law, with an unpredictable legal framework and enforcement, with autocratic police states) may raid data centers, and data or information systems may be subject to enforced disclosure or seizure. Change in jurisdiction of data leads to this risk, in which data or information systems are blocked or impounded by the government or other organization. CCs should consider jurisdictional ambiguities before adopting cloud technologies, as local laws of some countries for data storage could provide government access to private data.

- **Undertaking malicious probes or scans**

  Malicious probes or scans allow an attacker to collect sensitive information that may lead to loss of confidentiality, integrity, and availability of services and data.

- **Theft of computer equipment**

  Theft of equipment may occur due to inadequate controls on physical parameters such as smart card access at facility entries, which may lead to loss of physical equipment and compromise sensitive data.

- **Cloud service termination or failure**

  Termination of a cloud service by non-profitability or disputes might lead to data loss unless the end users obtain legal protection. Many factors, such as competitive pressure, lack of financial support, and an inadequate business strategy, can lead to the termination or failure of a cloud service.

  This threat results in poor service delivery, loss of investment, and low quality of service. Furthermore, failures in services outsourced to the CSP may affect the CC ability to meet its duties and commitments with its clients.

- **Subpoena and e-discovery**

  Customer data and services are subject to cease requests from authorities or third parties. This threat occurs due to improper resource isolation, data storage in multiple jurisdictions, and lack of details about jurisdiction conditions.

- **Improper data handling and disposal**

  It is difficult to ascertain data handling and disposal procedures followed by CSPs by the limited access to cloud infrastructure. When CCs request data deletion, data may not be truly eliminated because:

  - Multiple copies of data may be stored but not available
  - The disk to be destroyed might also contain data of other clients
  - Multi-tenancy and reuse of hardware resources in cloud keeps clients' data at risk

- **Loss/modification of backup data**

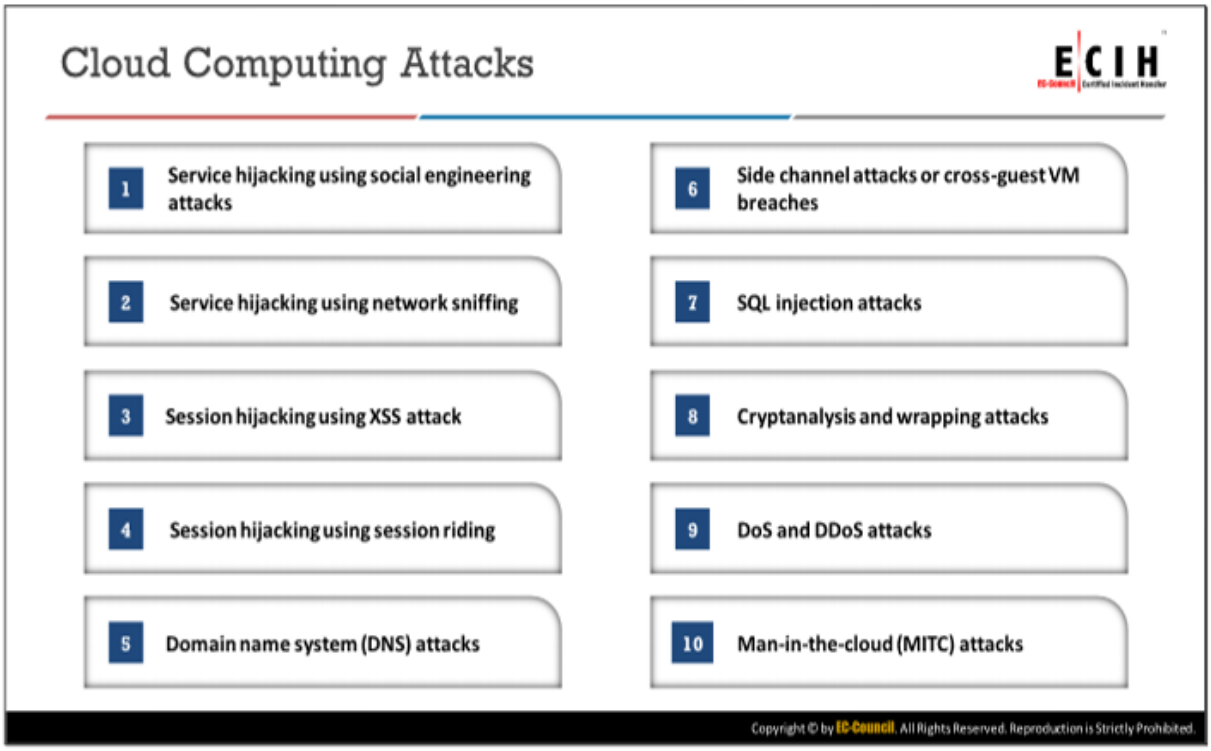
  Attackers might exploit vulnerabilities such as SQL (Structured Query Language) injection and insecure user behavior (e.g., storing or reusing passwords) to gain illegal access to data backups in the cloud. After gaining access, attackers might delete or modify data stored in databases. Lack of data restoration procedures in case of backup data loss keeps the service levels at risk.

- **Compliance risks**

  Organizations that seek to obtain compliance to standards and laws may be at risk if the CSP fails to provide evidence of the required compliance, outsource cloud management to third parties, and/or impede audits by the CC. This threat occurs by lack of governance over audits and industry standard assessments. Consequently, CCs may not be aware of the processes, procedures, and practices of CSPs in the areas of access, identity management, and segregation of duties.

- **Economic denial of sustainability (EDoS)**

  The payment method in a cloud system may be 'no use, no bill': the CSP charges the CC according to the recorded data involved when the CC makes requests, the duration of requests, the amount of data transfer in the network, and the number of CPU cycles consumed. Economic denial of sustainability destroys financial resources, and in the worst case, it can lead to CC bankruptcy or other serious economic impacts. If an attacker engages the cloud with a malicious service or executes malicious code that intensely consumes computational power and storage from the cloud server, the legitimate account holder is charged for the employed resources until the primary cause of CPU usage is detected.



Cloud Computing Attacks

Below, we discuss various attacks that can be perpetrated in cloud computing environments:

- **Service hijacking using social engineering attacks**

  In account or service hijacking, an attacker steals the CSP or CC credentials by methods such as phishing, pharming, social engineering, and exploitation of software vulnerabilities. Using the stolen credentials, attackers can gain access to the cloud computing services and compromise data confidentiality, integrity, and availability.

  Attackers might target CSPs to reset passwords or IT staff to access their cloud services to reveal passwords. Other ways to obtain passwords include password guessing, keylogging malware, implementing password-cracking techniques, and sending phishing emails. Social engineering attacks result in exposed customer data, credit card data, personal information, business plans, staff data, identity theft, and other information.

- **Service hijacking using network sniffing**

  Network sniffing involves the interception and monitoring of network traffic sent between two cloud nodes. Unencrypted sensitive data (e.g., login credentials) during transmission across a network are at higher risk.

  Attackers use packet sniffers (e.g., Wireshark, Cain and Abel) to capture sensitive data such as passwords, session cookies, and other web-service-related security configurations including UDDI (Universal Description, Discovery, and Integration), SOAP (Simple Object Access Protocol), and WSDL (Web Services Description Language) files.

- **Session hijacking using cross-site scripting (XSS) attack**

  Attackers implement cross-site scripting to steal cookies from the cloud user authentication process by injecting a malicious code into a website. Using the stolen cookies, attackers exploit active computer sessions, thereby gaining unauthorized access to data.

  Note: An attacker can also predict or sniff session IDs.

  The attackers host web pages with malicious scripts on to the cloud servers. When the users view these pages, the HTML (Hypertext Markup Language) codes containing malicious scripts run on the browser. The malicious script may collect browser cookies, redirect the users to the attacker's server, and send requests with the collected cookies.

- **Session hijacking using session riding**

  Attackers exploit websites by engaging in cross-site request forgery (XSRF) to transmit unauthorized commands. In session riding, attackers access an active computer session by sending an email or tricking users to visit a malicious webpage directed to the actual target site for login. When the user clicks the malicious link, the website executes the request as an authenticated user to perform activities such as modifying or deleting user data, executing online transactions, and resetting passwords.

- **DNS (Domain Name System) attacks**

  Attackers can perform DNS cache poisoning by directing users to a fake website that collects authentication credentials. The user sends a request for DNS information to the internal DNS server, which forwards it to the respective cloud server. Attackers block the DNS response from the cloud server and send a manipulated DNS response with the IP address of a fake website to the internal DNS server. Thus, the internal DNS server cache updates itself with the IP address of the fake website and automatically directs the user to it.

  Types of DNS attacks

  - **DNS poisoning:** Involves diverting users to a spoofed website by poisoning the DNS server or the DNS cache on the user's system
  - **Cybersquatting:** Involves conducting phishing scams by registering a domain name that is similar to that of a CSP
  - **Domain hijacking:** Involves stealing a CSP domain name
  - **Domain sniping:** Involves registering a domain name right after expiration

- **Side-channel attacks or cross-guest VM breaches**

  Attackers compromise the cloud by placing VMs near a target cloud server and running them on the same physical host of the user's VM. Then, they can take advantage of shared physical resources (e.g., processor cache) to launch side-channel attacks (e.g., timing attack to extract cryptographic keys/plain text secrets to steal the user's credentials). The attackers may use the stolen credentials to impersonate the user.

- **SQL injection attacks**

  SQL is intended for use in database management systems. In an SQL injection attack, attackers insert malicious code generated using special characters into a standard SQL query to gain unauthorized access to a database and ultimately to confidential information.

  Attackers target SQL servers running vulnerable database applications. It generally occurs when an application uses an input to construct dynamic SQL statements. Attackers may be able to manipulate the database contents, retrieve sensitive data, remotely execute system commands, or even take control of the web server for further criminal activities.

- **Cryptanalysis attacks**

  Insecure or obsolete encryption renders cloud services susceptible to cryptanalysis. The cloud stores encrypted data to prevent disclosure to malicious parties. However, critical flaws in cryptographic algorithm implementations (e.g., weak random number generation) might weaken or break encryption. Moreover, novel methods are constantly developed to break cryptography.

  Attackers can obtain partial information from encrypted data by monitoring clients' query access patterns and analyzing accessed positions.

- **Wrapping attack**

  When users send requests through a browser, the requests first reach a web server, which generates a SOAP message containing structural information required for exchange with the browser during message passing. Before passing occurs, the browser should sign and authorize the XML (Extensible Markup Language) document. In addition, it should append the signature values to the document. Finally, the SOAP header contains all the necessary information for the destination after computation.

  In a wrapping attack, the attacker does its deception during translation of the SOAP message in the TLS (Transport Layer Security) protocol. The attacker duplicates the body of the message and sends it to the server as a legitimate user. The server checks authentication by the signature value (also duplicated) and its integrity. As a result, the attacker can intrude into the cloud and run malicious code to interrupt the operation of cloud servers.

- **DoS (denial of service) and DDoS (distributed denial of service) attacks**

  Performing DoS attacks on CSPs may leave tenants without access to their accounts. In the cloud infrastructure, multiple tenants share CPU, memory, disk space, bandwidth, and other resources. Thus, if attackers gain access to the cloud, they can generate fake data requests or code that can run applications of legitimate users.

  Such malware requests utilize the CSP CPU, memory, and all other resources, and once the server reaches its threshold limit, it starts offloading its jobs to another server. The same happens to other inline servers for the attackers to finally engage the whole cloud

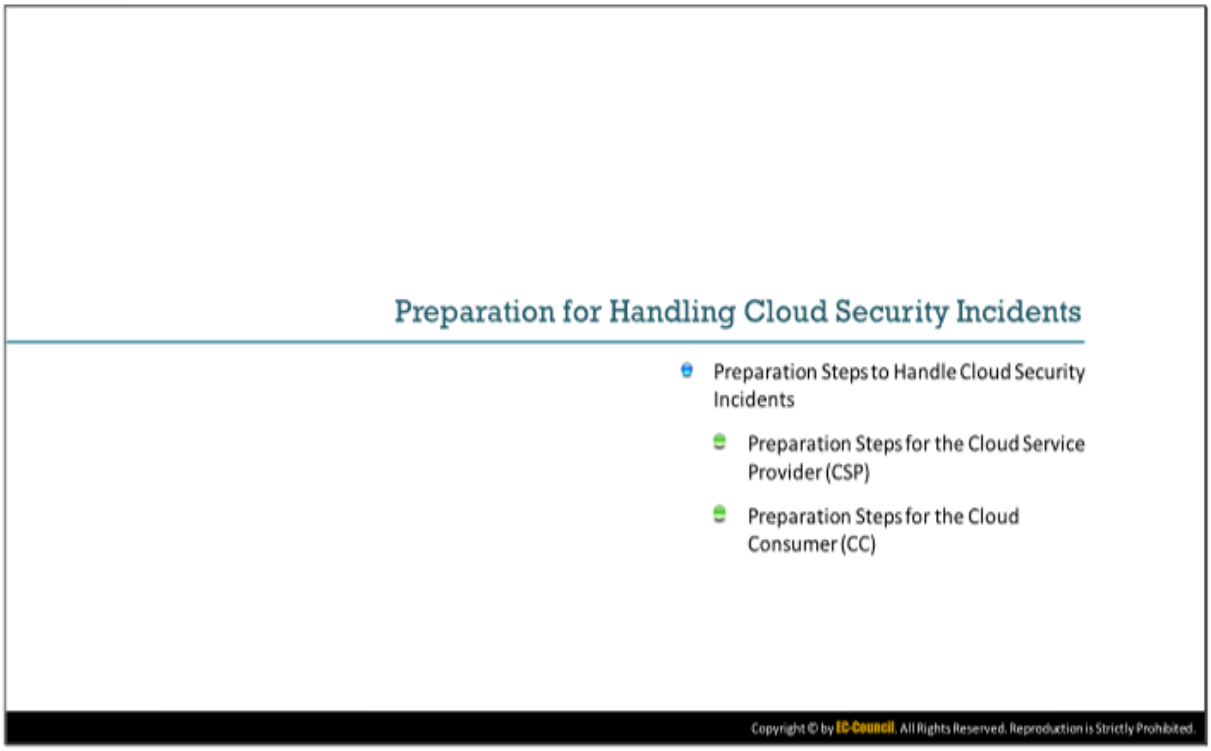
system just by interfering the usual processing of one server. This attack impedes legitimate users of the cloud to access their services.

If the attacker performs a DoS attack by using a botnet (i.e., a network of compromised machines), then the attack becomes distributed. A DDoS attack involves several compromised systems attacking a single target system, thereby causing DoS for users of the target system.

- **Man-in-the-cloud (MITC) attack**

  An MITC attack is an advanced version of the man-in-the-middle (MITM) attack, in which an attacker uses an exploit that intercepts and manipulates the communication between two parties. Likewise, MITC attacks are carried out by abusing cloud file synchronization services such as Google Drive or DropBox for data compromising, command and control, data exfiltration, and remote access. Synchronization tokens are used for application authentication in the cloud, which cannot distinguish malicious from normal traffic. The attacker then abuses this weakness in cloud accounts to perform MITC attacks.

  The attacker tricks a user to install malicious code that plants the attacker's synchronization token in the user's drive. Then, the attacker steals the user's synchronization token and employs it to gain access to user's files. Next, the attacker restores the malicious token with the original synchronized token of the user, returning the drive application to its original state and remaining undetected.



Preparation for Handling Cloud Security Incidents

Due to the increasing number of cloud platform attacks, both the CCs and CSPs may face adverse consequences. Therefore, it is essential for both parties to be prepared by following guidelines and procedures to handle cloud security incidents and stop them from damaging critical assets.

This section provides various preparation steps and responsibilities of CCs and CSPs when handling cloud security incidents.

Preparation Steps to Handle Cloud Security Incidents

- The CSP and CC share **responsibility for handling cloud incidents** based on the type of service, SLA, and attack
- Common preparation steps for both CSP and CC include:

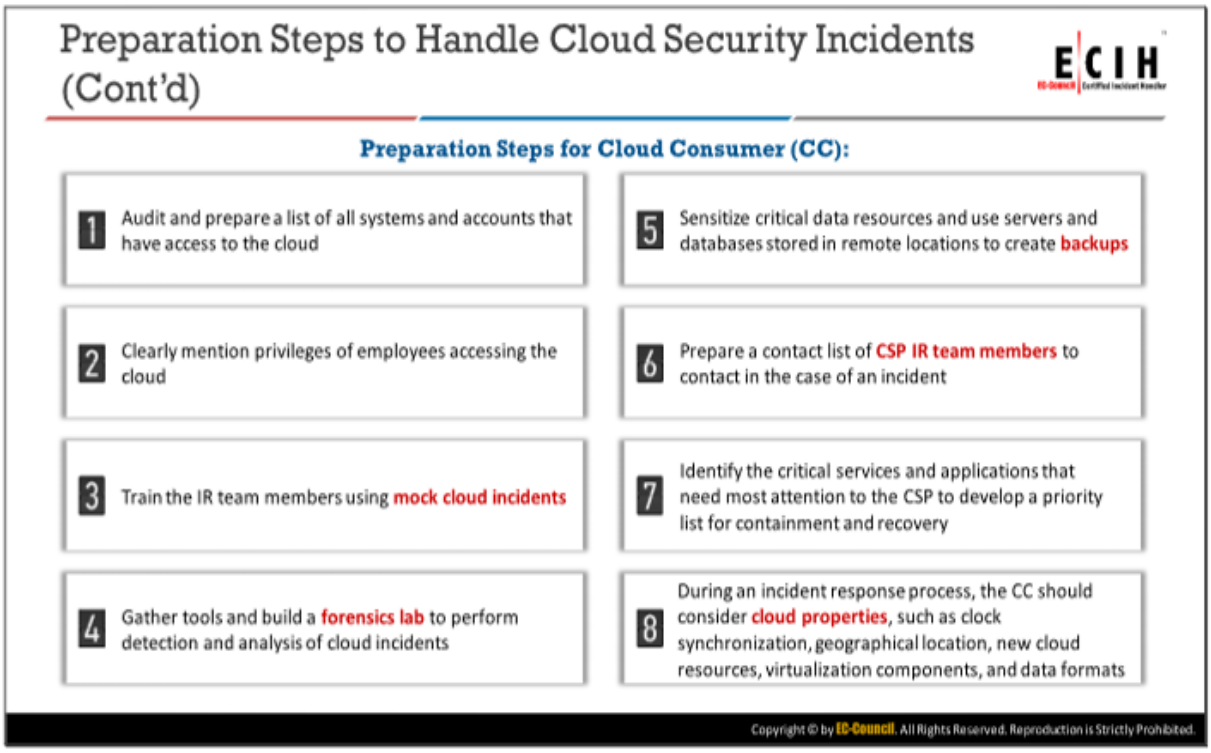
- Write a SLA with clear division of incident handling responsibilities based on the **type of service** and **type of attack**
- Ensure SLA includes provisions for gathering or obtaining the data required to contain and remove threats
- Devise incident response plans and policies according to the SLAs
- Include team members with experience in handling cloud environments
- Train the team to handle cloud incidents using mock drills
- Train employees regarding safe usage practices and proper incident reporting procedures
- The IR team must have knowledge of various cloud file formats and the different tools for converting and analyzing virtual memory files

- Gather tools and resources required to handle **cloud-based incidents**
- IR teams from both the CC and CSP should work closely together for better incident response
- Both parties need to create **regular backups** of critical data; in SaaS and PaaS the responsibility lies mainly with CSP
- Define the communication channels with a contact list of IR team members
- The CC and CSP should agree to **exchange incident data** or **artifacts** and decide the format and means of exchange
- Exchange details of changes, security measures, IR testing, and other activities that could impact the cloud

Preparation Steps to Handle Cloud Security Incidents (Cont'd)

Preparation Steps for Cloud Service Provider (CSP):

1. Assign separate IR teams with incident **handling equipment** at different geographical locations
2. Install various physical security monitoring devices
3. Enable logging on all devices, servers, databases, and software applications
4. Employ Syslog servers to collect the logs and SIEM tools for correlation
5. Install database activity monitoring (DAM), data leak prevention (DLP), log analysis, and SIEM tools to simplify incident detection
6. Do not disclose the **location of databases** to the public or clients unless necessary
7. Maintain lists of customers that need to be contacted in the case of an incident on a cloud environment
8. Prepare the internal team to help and join forces with the **CC incident response team**



Preparation Steps to Handle Cloud Security Incidents

In a cloud environment, the CC and CSP share responsibilities when handling incidents according to the type of service, SLA, and attack. In addition, they should prepare separately for handling cloud security incidents.

Common preparation steps for CCs and CSPs for handling cloud security incidents include:

- Craft an SLA with clear division of incident handling responsibilities based on the type of service and attack
- Ensure the SLA includes provisions for gathering or obtaining the required data to contain and eradicate incidents
- Clearly mention the responsibilities of the CC and CSP in the SLA during and after an incident according to the type of service
- Devise incident response plans and policies according to the SLA

  The SLA should include provisions for the following:

  - Points of contact, communication channels, and availability of incident response teams for each party
  - Standard notification process between parties and to external sources
  - Incident data exchange and storage
  - Details of roles/responsibilities during a security incident
  - Sharing of incident data/artifacts during a security incident including the sharing format and method of exchange

  - Detailed explanation of sanitization methods performed on acquired data
  - Clear specifications of incident response tests performed by each party
  - Sharing of incident response test results
  - Definition of process for performing postmortem analysis and validation, including final incident reports
  - Proper containment and eradication methods for controlling security incidents
- Build a team with members having experience in handling cloud environments
- Define the roles and responsibilities of team members during security incident response
- Train members in handling cloud security incidents using mock drills
- Train employees regarding safe usage practices and proper reporting of security incidents
- Maintain a knowledge base for the incident response team on various cloud file formats and ability to use different tools to convert and analyze virtual memory files
- Gather tools and resources required to handle cloud security incidents
- Build proper incident response teams for CCs and CSPs. Teams may work closely for improved incident response
- Create regular backups of critical data on the CC and CSP sides, including databases, applications, and logs. In the PaaS and SaaS models, this responsibility lies mainly on the CSP
- Define communication channels with a contact list of incident response team members
- Agree to exchange incident data or artifacts between CCs and CSPs and decide the format and means of exchange
- Exchange details of changes, security measures, incident response testing, and other activities that may impact the cloud
- Provide training and proper practice to members and equip them with tools required to handle cloud security incidents
- Create a forensics lab for analysis and validation of security incidents. Ensure that it has the updated tools and equipment required to extract, analyze, and validate the forensics data. The lab should also include large storage media to store evidentiary data
- Ensure that incident response teams properly document the incident response process, maintain the chain of custody for evidentiary data, and create detailed reports

Both CC and CSP share responsibilities to maintain adequate security in their systems. Different cloud service models (IaaS, PaaS, and SaaS) require varying level of control between CCs and CSPs.

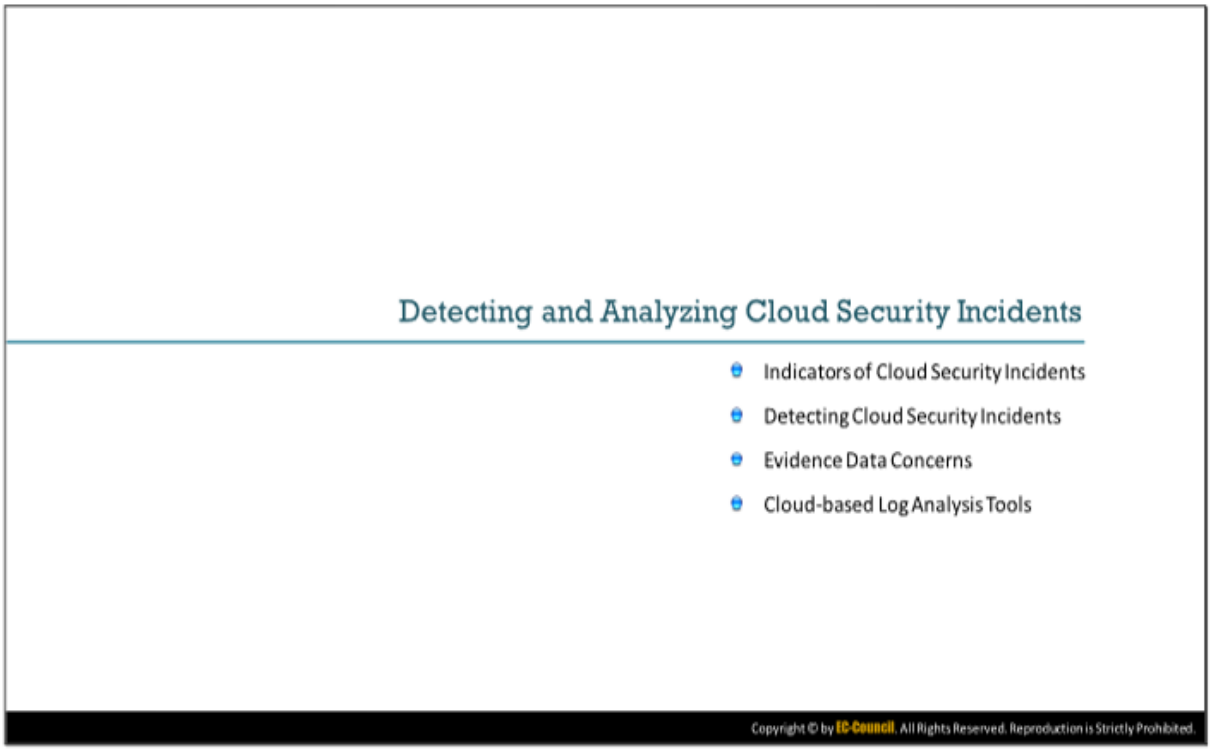
Below, we discuss the preparation steps for CC and CSP against cloud security incidents:

- **Preparation steps for CSP**
  - Use distributed storage for cloud and place all the databases at different geographical locations
  - Prepare multiple databases that store copies of the data and use proper backup and recovery systems
  - Assign separate incident response teams at different geographical locations with the required tools and equipment
  - Provide teams with proper communication channels among them, including teams in distant locations
  - Implement physical security monitoring and authentication systems to ensure authorized entries in every facility
  - Recruit security personnel and frame strict policies regarding physical access to the cloud infrastructure
  - Install alarms in case of physical security breach, disasters, and other physical threats
  - Enable logging on all the devices, servers, networks, databases, OSs, and applications
  - Employ syslog servers to collect logs at a centralized location
  - Install SIEM (security information and event management) tools to perform event correlation and alert the incident response teams in the event of an attack
  - Install DAM (database activity monitoring), DLP (data leak prevention), log analysis, and SIEM tools to simplify detection of incidents
  - Not disclose the location of databases to public or clients unless necessary to prevent physical attacks or physical access events
  - Create backups of cloud data on various distant servers
  - Maintain lists of customers, brokers, and other parties related to a cloud premise along with the details of the service provided and deployment models. The incident response team should be able to access these details in case of emergency
  - Obtain detailed reports from recent audits and highlight concerns with the auditor if any. Audit reports should include important data such as status of application, OSs, servers, databases, and networks in the cloud
  - Coordinate the CC and CSP incident response teams to jointly detect, contain, and eradicate incidents

- Ensure sharing of incident response process data along with updates, changes in configuration, monitoring procedures, containment, eradication steps, and evidentiary data between the CC and CSP incident response teams
- Provide security solutions and share chain of custody data with clients
- Ensure that services comply with relevant international standards and laws in regions where the CSP stores data and clients operate. The CSP must comply with the laws when data are distributed across several jurisdictions with conflicting laws. The CSP should also mention whether the client can access data from different locations and whether it notifies or asks permission to move data to other locations
- Make provisions for clients and legal/government agencies to perform forensic imaging of compromised systems and services in case of attack

- **Preparation steps for CC**
  - List and regularly audit all services, accounts, virtual systems, applications, and other elements of the clouds it governs. The list should include details such as versions, update schedules, account privileges, employees having the access, and security features enabled for all the components
  - Clearly mention privileges of employees accessing the cloud
  - Train the incident response team and perform mock cloud security incidents for practice
  - Gather tools and build a forensics lab to perform detection and analysis of cloud security incidents
  - Sensitize critical data resources and use servers and databases stored in distant locations to create backups
  - Prepare a contact list of the CSP incident response team members for contact and report in case of an incident
  - Communicate with the CSP incident response team to discuss their response methodology and create an incident response strategy accordingly
  - Identify critical assets, data, services, applications, and other aspects required for running the business. Communicate the priority list to the CSP. This will help in prioritizing the recovery of resources for business continuity
  - Consider aspects of the cloud such as clock synchronization, geographical location, new cloud resources, virtualization components, and data formats during incident response
  - Determine the importance of data and their requirement during selection of cloud services and deployment model. Ensure that the CSPs provide regulatory compliant services and abide by the jurisdictional standards in the operation regions

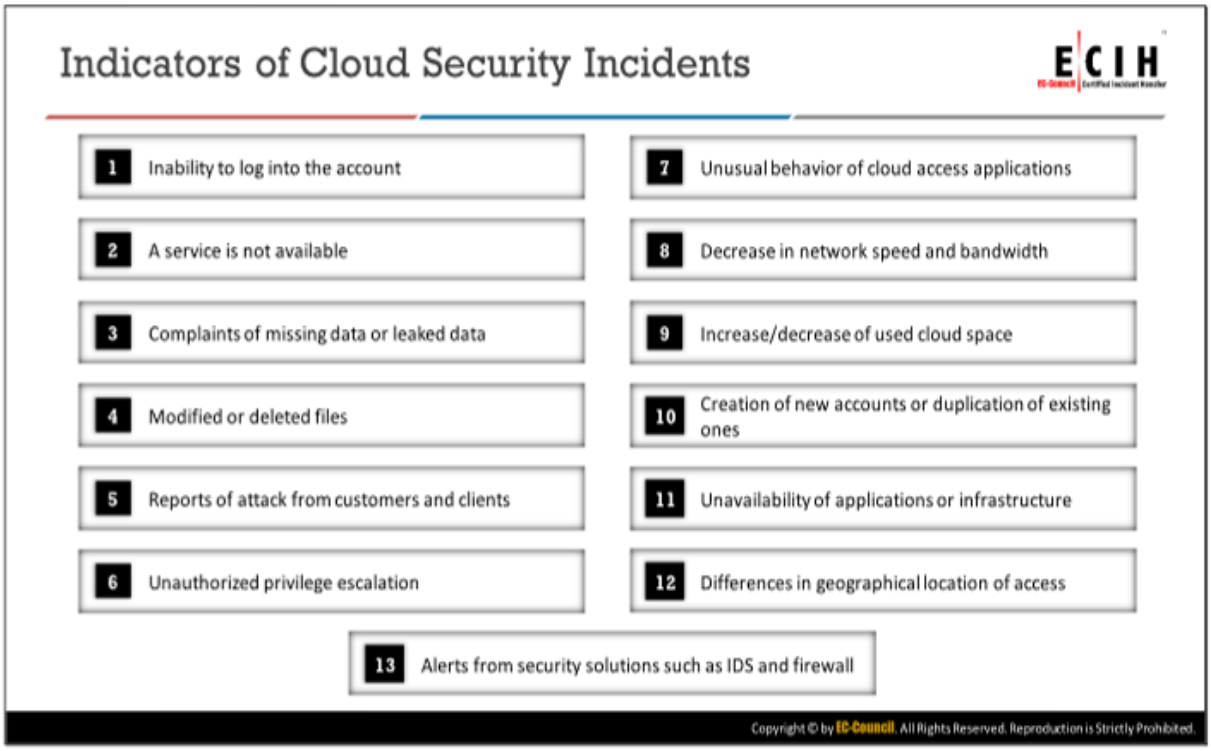
- Ensure that the service offers proper backup and recovery options along with damage protection and forensics support. The CSP should have a detailed incident response plan and an incident response team
- Consider the incident response and handling according to the type of service. The client is completely responsible for incident response in the IaaS model and partially responsible in the PaaS and SaaS models
- Frame policies for access, authentication, and use of cloud services, and implement them across the organization
- Enable logs to record access time and duration, location of user, IP and MAC (media access control) addresses of systems used for access, network protocols, and other relevant information
- Maintain backup of all the cloud components in the IaaS model and have a backup for data stored in the cloud in the PaaS and SaaS models
- Build an incident response team with members having experience in handling cloud security incidents
- Create regular backups of critical data, systems, and applications
- Enable logging on the systems and devices used to access the cloud services. The CC must manage accounts, audit and report applications and services, create and implement policies for fair usage, configuration management, contingency planning, and authentication. The CC should also ensure proper incident response policy and procedures



Detecting and Analyzing Cloud Security Incidents

On-time detection and analysis of cloud security incidents can enable the incident response team to take proper measures for preserving the organizational assets against various cloud attacks. The detection and analysis process includes monitoring the system for potential attack vectors, signs of an incident, and prioritization of incidents based on their severity.

This section describes various indicators of cloud security, detection of cloud security incidents at different levels such as network, storage, servers, virtualization, and applications, data concerns related to evidence, and cloud-based log analysis tools.



Indicators of Cloud Security Incidents

Compromised cloud networks and applications exhibit various indicators that can represent attacks or malfunctioning in networks, servers, systems, and applications.

Indicators of a compromised cloud environment include the following:

- Inability to log in to an account can indicate DoS or compromised account
- Unavailability of service may indicate attacks to the network, account, application, or servers related to the cloud
- Information or complaints about leaked data from the cloud may be the result of attack or compromised security
- Modified or deleted files in a cloud indicate unauthorized access and modification of data
- Reports of attack from customers and clients
- Unauthorized privilege escalation indicates that attackers are trying to increase privileges to perform advanced attacks
- Unusual behavior of cloud access applications may indicate attacks on application or database hosting them
- Reduced network speed may result from consumed bandwidth and other network resources by unauthorized users or attackers
- Attacks in the cloud can result in increase/decrease of used space, because attackers can delete data, install malware or malicious code, or modify crucial data for inflicting harm

- After compromising clouds, attackers may also try to create new accounts or duplicate existing ones
- Unavailability of applications or infrastructure
- Compromised cloud logs can show differences in geographical location when perpetrators try to access them
- Cloud security solutions such as intrusion detection systems and firewalls generate alerts when attackers try to gain unauthorized access

Detecting Cloud Security Incidents

- Incident responders on both the CC and CSP side must collaborate to handle the cloud incidents
- On receiving an incident report, the responders must **inform their peers** in the other organization and provide all known details
- They must discuss all **incident response methodologies** they intend to apply to analyze, contain, and eradicate the incident
- Based on the type of attack, they must perform detection and containment processes concurrently

To detect incidents at the CSP side, the incident responders should perform the following activities:

Network-related incidents

- The CSP is mainly responsible for providing proper **network services** and **handling network-related incidents** in all the cloud service models
- In the case of an incident, the CSP incident response team can **collect logs** recorded from various networking devices including servers, routers, firewalls, honeypots, and IDS and assess them for suspicious entries
- Network detection and analysis is the most important process to locate attacks on a cloud as the CSP does not have any other means of access
- The process will help identify suspicious IP addresses, MAC addresses, user accounts, systems, applications, services, and other attack vectors

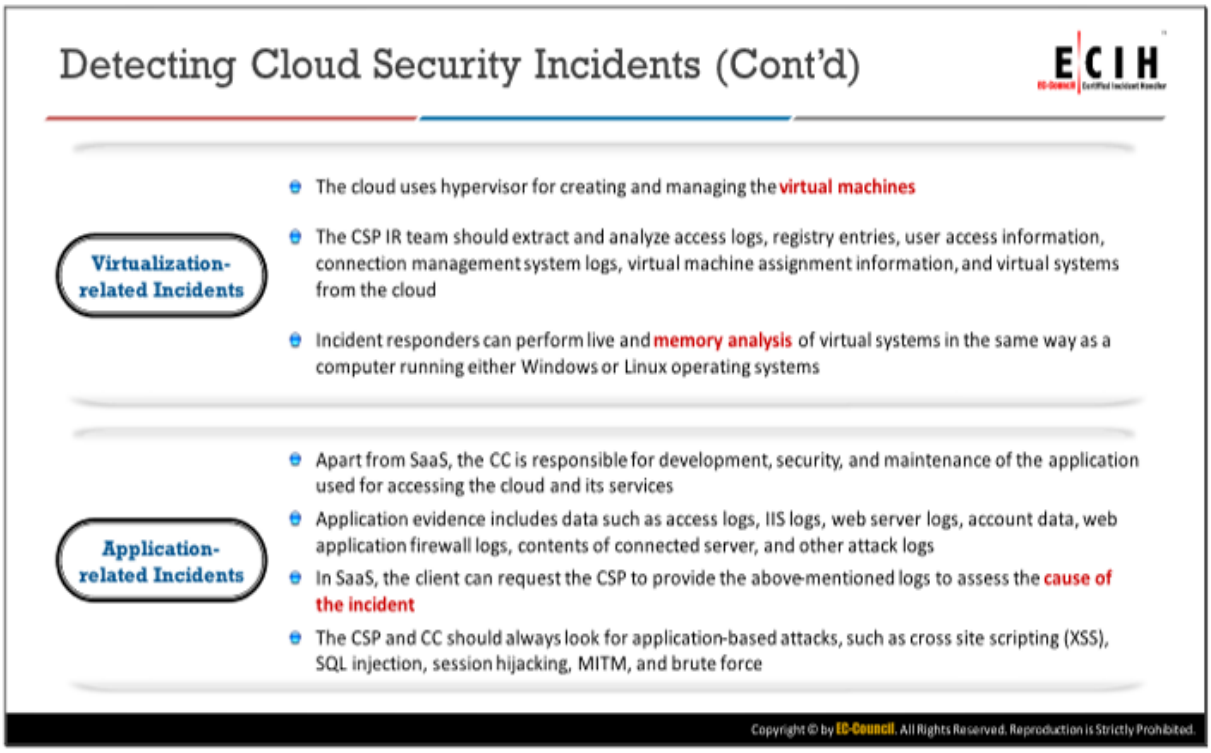
Detecting Cloud Security Incidents (Cont'd)

Storage-related Incidents

- In a cloud, storage refers to databases holding the data, virtual machines, operating systems etc.
- Only the CSP has access to databases and is responsible for acquiring snapshots of the database, access and application logs, and analyzing them to **find suspicious entries**
- Incident responders should analyze the file systems, slack spaces, and metadata of the **storage units** to find hidden malware and evidence of attacks

Server-related Incidents

- The CSP is responsible for **managing servers** and **handling response activities** related to servers
- The IR team must **collect server logs** and other evidence files, such as: transaction logs, database plan caches, error logs, trace files, and user account data
- Incident responders must analyze these files to **detect suspicious entries** and malicious actions



Detecting Cloud Security Incidents

Customers or client's personnel can be the first to experience indicators of a compromised cloud environment and may report the incident to the client organization and CSP. The CSP is responsible for determining whether the incident is impacting a specific CC or the complete cloud. This helps to determine the attack vectors, such as applications, accounts, networks, servers, and databases.

Reports from multiple clients residing on the same cloud can indicate an attack on the CSP-controlled assets. Both CC and CSP can assess the type of attack from network, application, server, and system alerts. Incident responders on the CC and CSP sides must collaborate to handle cloud security incidents. Both parties should simultaneously start the incident response process immediately after finding signs of an event. Upon reception of an incident report, the responders must inform their peers on the other side and provide all the known details. They must discuss the incident response methodologies to adopt for analyzing, containing, and eradicating the incident. Based on the type of attack, they must perform detection and containment processes concurrently.

Incident response in a cloud is a layer-based approach, in which the incident responder must collect evidence from various layers and correlate them to recreate the event and determine its impact to the cloud and customers.

A cloud is similar to a traditional network, comprising virtualized forms of the corresponding hardware and software. Therefore, incident responders can leverage methods from traditional incident response to detect cloud security incidents.

To detect an incident on the CSP side, the incident responders should perform the following activities:

- **Network-related incidents**

  Networks are the only media to access cloud data, services, and applications. Therefore, incident responders should gather and analyze network information on the CC and CSP sides. The CSP is responsible for providing proper network services and handling incidents related to the networks that enable connectivity between servers, databases, and other external networks.

  The CSP incident response team must collect logs from various networking devices including servers, routers, firewalls, honeypots, and intrusion detection systems (IDSs) to identify suspicious entries or IP addresses that have tried to access the cloud components. The network detection and analysis process is considered as the most important to find attacks performed on a cloud, as attackers do not have any other means of access.

  The CC can collect logs from internal and remote networks used to access the cloud, applications, and data to identify the perpetrator by determining suspicious IP and MAC addresses, user accounts, systems, applications, services, and other details of potential attackers trying to access the cloud on the client side.

  After gathering network logs, organizations can use log viewers to determine suspicious traffic and adopt SIEM along with log correlation tools to recreate the event or create a timeline of the attack. This also helps detecting compromised servers, applications, accounts, databases, and data.

- **Storage-related Incidents**

  In a cloud, storage refers to media devices and databases that contain data, VMs, OSs, virtual networks, and security solutions. The CSP is the only responsible for performing incident response and forensics on the databases and storage media, as the CC team does not have access to them. The incident response team should not analyze the files directly but either create copies or acquire an image and work on these duplicate data.

  Databases record events such as creation, modification, deletion, encryption, and decryption of data in the form of logs. The logs store details of events including time, duration, user account, type of access, protocols, and type of networks used for access. Only the CSP has access to databases and is responsible to acquire snapshots of the database, user access, and application logs.

  Incident responders should analyze the evidentiary data available in the file systems, slack spaces, and metadata of the storage units to find hidden malware and evidence of malice. In addition, they must extract and analyze the database logs to find suspicious entries.

- **Server-related incidents**

  Servers refer to the hardware devices on the CSP side that help users to connect with their respective clouds and access data. The CSP is responsible for managing servers and

handling incident response related to them, because CCs do not have access to these physical devices. Servers store access logs containing details of the accounts, systems, applications, and locations of users trying to access data and services.

The incident response team must collect server logs and other evidentiary data such as transaction logs, database plan cache, error logs, trace files, and user account data. It should then analyze these data to detect suspicious entries and malicious actions. The cloud can require various servers that use different technologies and ways of storing the data to serve a wide client requirement. Thus, the incident response team should be competent to analyze data from different server technologies.

- **Virtualization-related incidents**

  Virtualization refers to the platform in a cloud that allows clients to install the VMs, systems, and servers required to run applications. CSPs use different virtualization platforms for different clouds depending on their services and cloud deployment model. The format of VMs and systems changes according to the type of virtualization.

  Most clouds use hypervisors for creating and managing VMs. The CSP incident response team should extract and analyze the access logs, registry entries, user access information, connection management system logs, VM assignment information, and virtual systems from the cloud.

  Virtualization makes the data available in the cloud more volatile and susceptible to loss, because these systems eliminate volatile information when the user logs out or switches off the system. Incident responders can perform live and memory analysis of a virtual system in the same way as of a computer running on different OSs.

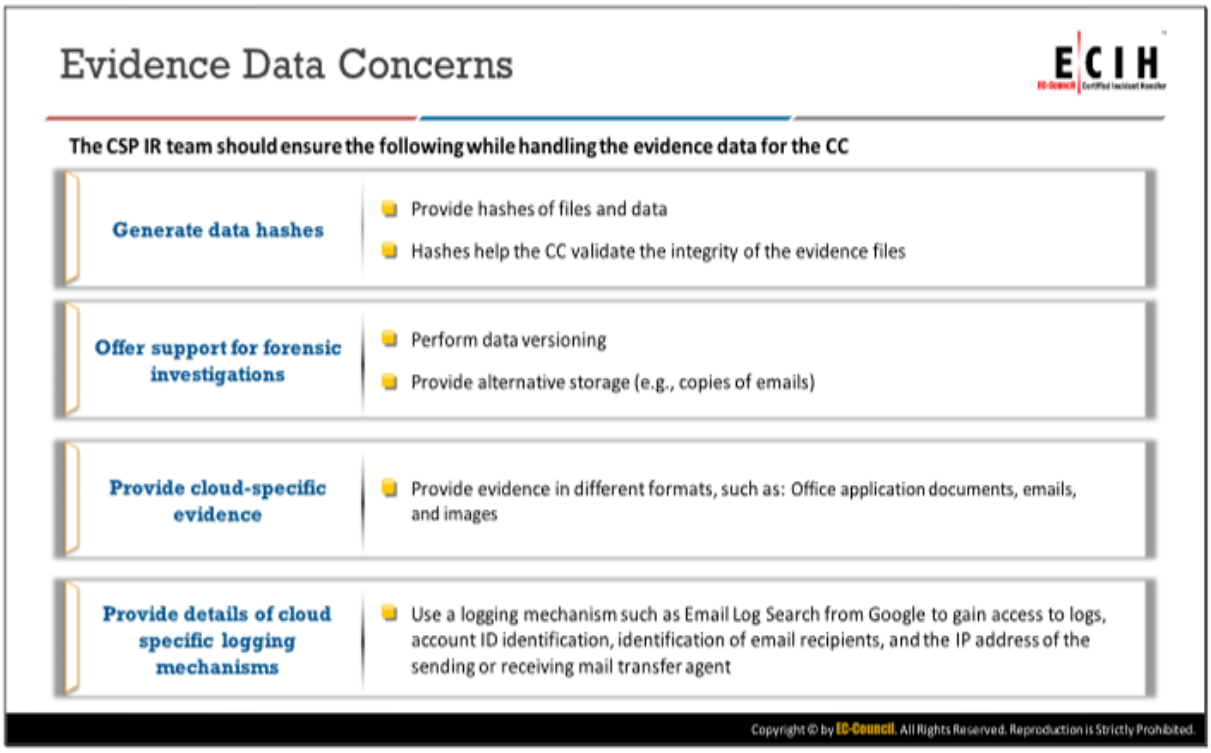
  In the IaaS model, the client installs a virtualization platform on the infrastructure provided by the CSP and is responsible for the related incident response functions. In the PaaS and SaaS models, the CSP is responsible to acquire data from the virtual platforms and provide these data to the CC for further analysis.

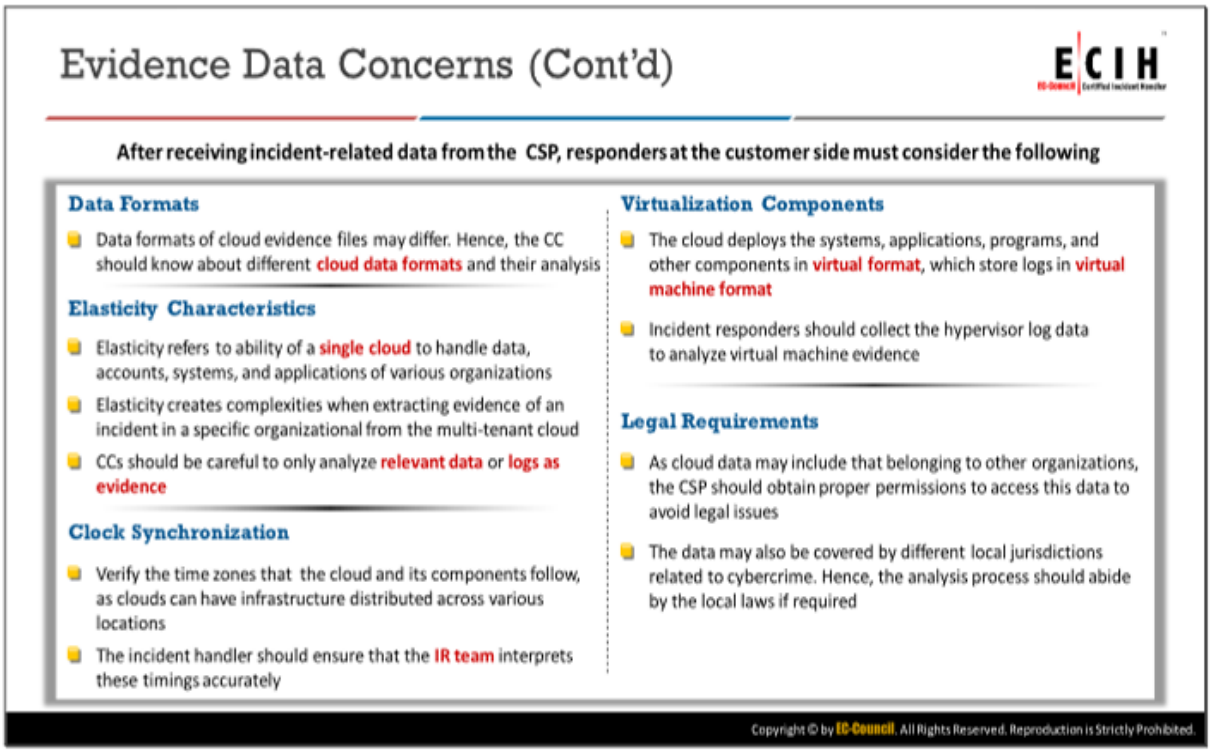
- **Application-related incidents**

  Applications are user interfaces that allow clients to access the cloud, store and manage data, manage accounts, and perform other activities in the cloud. Except for the SaaS model, the CC is responsible in the IaaS and PaaS models for the development, security, and maintenance of the applications for accessing the cloud and its services. Applications also allow the users to manage account logins and data, escalate service requirements, and modify the cloud usage properties.

  Incident responders can acquire application evidence such as access logs, IIS (Internet Information Service) logs, web server logs, account data, web application firewall logs, contents of connected servers, and other logs for identifying the source and path of an attack to the cloud.

  In the SaaS model, the client incident handling team must request the CSP the logs to assess the cause of a security incident. CCs and CSPs should always look for application-based attacks, such as cross-site scripting, SQL injection, session hijacking, man-in-the-middle, and brute force attacks.





Evidence Data Concerns

A defensible response toward a cloud security incident depends on the reliability of evidentiary data. Therefore, it is critical to handle evidence with precision and care to maintain its quality and integrity as well as preserve it from overwriting, destruction, and corruption.

The incident response team on the CSP side should ensure the following while handling evidentiary data to a CC:

- **Generate data hashes**

  CSPs should save hashes (digital fingerprints) along with each data record for eventual use in forensic analysis. CCs and CSPs must remember to establish such procedures in advance in the SLA along with the related technical documentation to ensure data credibility. The CSP should provide hashes of evidence to help the CC to validate the integrity of evidence files.

- **Offer support for forensic investigations**

  CSPs could add extra services to their existing cloud services as proactive support for forensic investigations. These service packets may offer data versioning, alternative storage of forensic data (e.g., email copies), automatic hashes, relevant data interfaces, and analysis tools.

- **Provide cloud-specific evidence**

  An investigator should have expertise in handling both cloud-specific evidence and formats of evidence found during investigation in a traditional environment. Some formats of cloud evidence include Office application documents, emails and images, as well as several new forms of evidence, particularly pertaining to user's activity logs.

- **Provide details of cloud-specific logging mechanisms**

  Some cloud-specific logging mechanisms include Email Log Search, a service from Google that enables investigators to gain access to logs regarding aspects such as emails sent on a specific date, account identification for a specific email, identification of specific email recipients, and the IP address of the sending or receiving MTA (Mail Transfer Agent) and Amazon Simple Storage Service (S3) Logging that provides logging details for 'buckets' including the type of request and time/date it raised.

After receiving incident data from a CSP, the incident responders on the CC side must consider the following key areas while analyzing data:

- **Data formats**

  Data formats of cloud evidence files may differ, and the CC should gain knowledge about the different cloud data formats and their analysis.

- **Elasticity characteristics**

  Elasticity refers to the ability of a single cloud to handle data, accounts, systems, and applications of various organizations. It increases the complexity while extracting evidence of a specific organizational incident from a multi-tenant cloud. CCs should be careful while analyzing evidence and consider only relevant data or logs.

- **Clock synchronization**

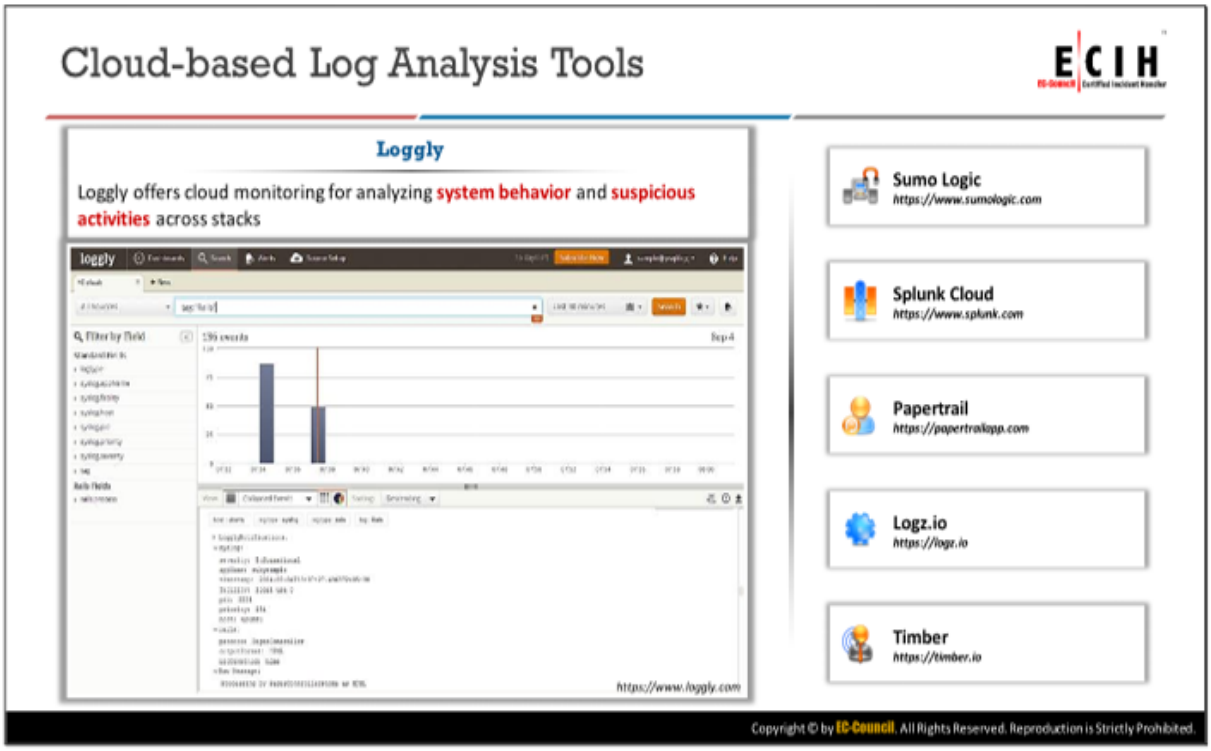
  Verify the time zones that the cloud and its components follow, because the cloud may have its infrastructure distributed over various locations across the globe. The incident handler should ensure that the incident response team accurately interprets timing.

- **Virtualization components**

  The cloud deploys the systems, applications, programs, and other components in virtual formats and stores logs in a VM format. Incident responders should collect the hypervisor log data to analyze VM evidence.

- **Legal requirements**

  Cloud data may include those belonging to different organizations. Therefore, the CC incident handler should ensure that the CSP has obtained proper permissions to prevent legal issues. Data may also be distributed across geographical locations with different jurisdictions related to cybercrime, and the handler should ensure that the analysis process abides by local laws if required.



Cloud-based Log Analysis Tools

Cloud-based log analysis tools help incident handlers to collect and analyze various logs and detect cloud security incidents in real time at an early stage to reduce their impact.

Below, we discuss some important cloud-based log analysis tools:

- **Loggly**

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

  Loggly automatically recognizes common log formats and gives a structured summary of all the parsed logs. It provides real-time log monitoring, system behavior, and unusual activity detection. It brings logs from the depths of an organization's infrastructure to track activity and analyze trends. Moreover, it shows how components interact and identifies correlations. Logs can be captured in real time either on syslog or HTTP (Hypertext Transfer Protocol) formats.

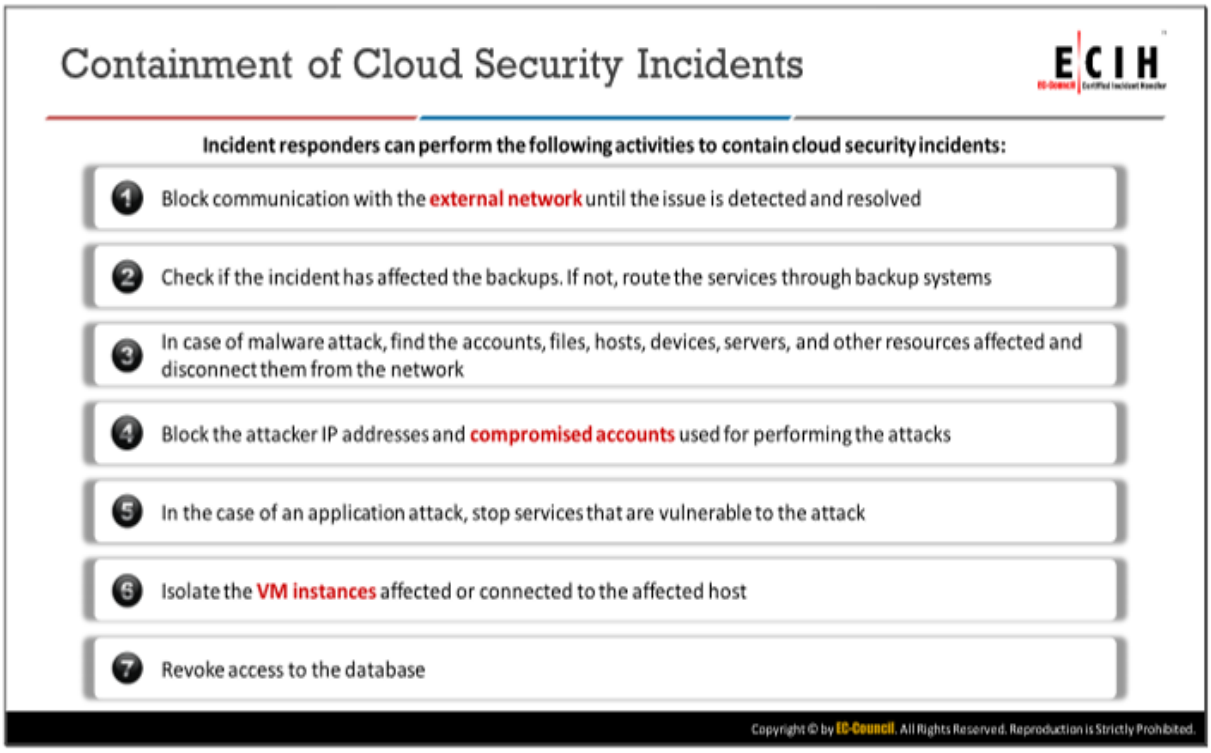
  Features:

  - Monitors cloud for analyzing system behavior and suspicious activity across the stack
  - Tracks SLA compliance and identifies anomalies and suspicious events
  - Secures log data transmission
  - Generates a real-time, bird's-eye view of logs

Some additional cloud-based log analysis tools are listed below:

- Sumo Logic (*https://www.sumologic.com*)
- Splunk Cloud (*https://www.splunk.com*)

- Papertrail (*https://papertrailapp.com*)
- Logz.io (*https://logz.io*)
- Timber (*https://timber.io*)
- Logentries (*https://logentries.com*)
- Sematext Cloud (*https://sematext.com*)



Containment of Cloud Security Incidents

Containment is a crucial step to prevent additional damage to cloud resources and services. During containment, the incident response team plans various strategies to avoid further losses from taking place while ensuring that no forensic evidence related to the cloud security incident is destroyed or tampered.

This section provides various steps for the incident responder to contain cloud security incidents.

Containment of an incident in the cloud may impact the business services of all the clients. It is the responsibility of the CCs and CSPs to immediately report incidents and work together to contain and eradicate them. CSPs should inform other CCs in the compromised cloud about the incident and obtain permissions to perform containment activities, even if the attack is targeted to a specific CC. For instance, the data of uncompromised CCs should be routed to other databases while disconnecting the compromised client data to contain the attack.

Incident responders can perform the following activities for containing cloud security incidents:

- Block communication with the external network until the incident is detected and resolved
- Check if the incident has affected backups and route the services through backup systems
- In case of a malware attack, find the accounts, files, hosts, devices, servers, and other affected resources for disconnection from the network
- Block the attacker IP addresses and compromised accounts used to perform the attack
- In case of an application attack, stop the services that are vulnerable to the attack
- Isolate the VM instances affected or connected to the affected host
- Revoke access to databases

Containment Tool for Cloud Security Incidents

In the cloud environment, the incident responders do not have physical access to hardware and other resources, thus hindering containment and forensics in the cloud. Incident responders need to deploy containment tools to effectively contain a potential cloud security incident and gather the required forensic evidence. Below, we describe a containment tool that can be used during cloud security incidents.

- **CloudPassage Quarantine**

  Source: *https://github.com*

  CloudPassage Quarantine is a containerized application that monitors the /v1/events endpoint in the Halo API looking for specific events. If a targeted event is matched, the tool moves the workload into the configured quarantine group.

  How it works

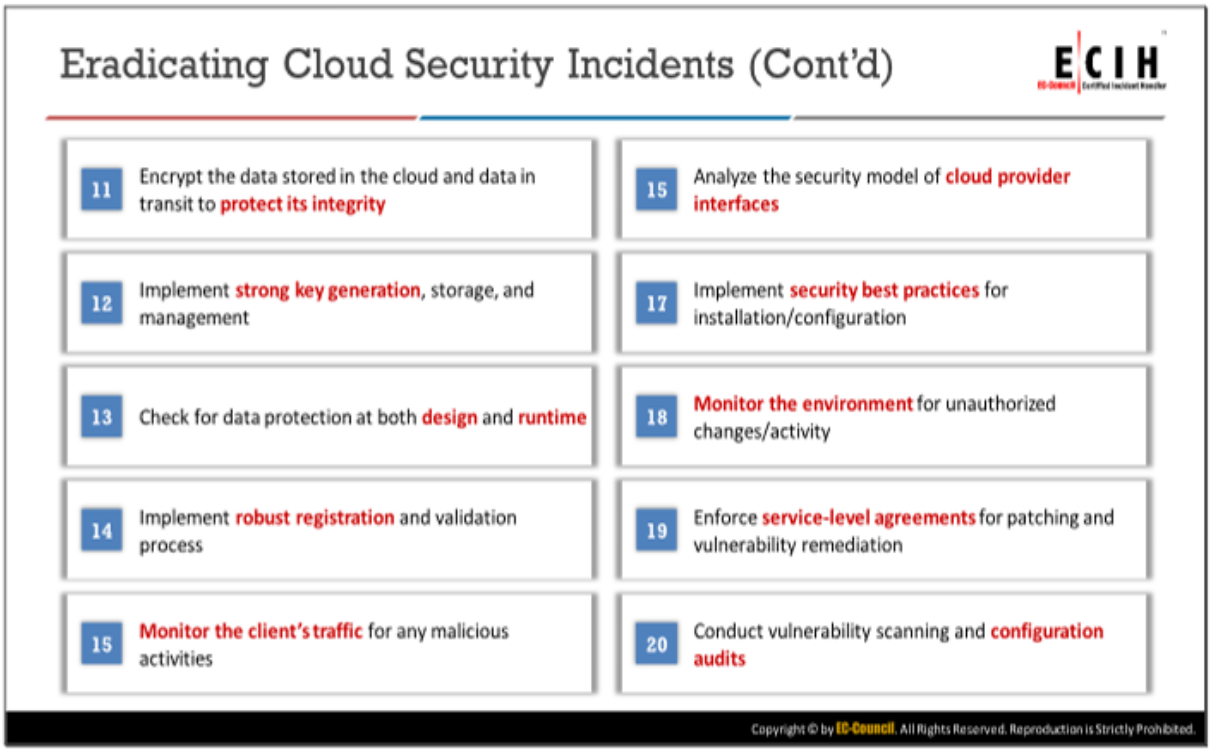
  The targeted events are listed, one per line, in `/conf/target-events`. The tool either alters the file and rebuilds the container or mounts it in the config file from a persistent volume. When the end of the events stream is reached, the tool continues to query until more events arrive. If the incident handler does not set the `HALO_EVENTS_START` environment variable, the tool starts at the beginning of the current day.

  The quarantine group is defined with the `$QUARANTINE_GROUP_NAME` environment variable. If the handler does not define this environment variable, it is assumed to be Quarantine. The group should be configured in the Halo account of the incident handler before execution of the tool. We recommend applying a firewall policy to the group that restricts all outbound traffic and only allows inbound traffic from Ghostports users.

Eradication of Cloud Security Incidents

The eradication of security incidents is a major step in handling and responding to cloud security incidents. It allows to clean every attack footprint from the cloud resources such as network, servers, and applications. This further helps incident handlers to protect the cloud from evolving threats.

This section presents various steps involved in eradicating cloud security incidents and detecting an MITC attack using the Tripwire tool.



Eradicating Cloud Security Incidents

Eradication is the process of getting rid of compromised cloud networks and applications that can represent attacks or malfunctioning in networks, servers, systems, applications, and other resources related to the cloud. The first step of eradication is cleaning up infected software (e.g., removing malwares or viruses) and rebuilding or reconstructing the compromised networks or applications back to their normal operation. The second step is notifying the relevant officials about the incident.

Incident responders can eradicate cloud security incidents by performing the following activities:

- Remove malware files and traces from the affected components
- Update security solutions such as firewall, intrusion detection systems, and antiviruses with the malware signature
- Revoke access to compromised accounts, inform the users regarding this via email, and assign new accounts
- Warn users when trying to log in to their accounts from different systems or locations
- Update all the VMs and OSs to remove vulnerabilities
- Contact the developers about security flaws in applications and patch them as early as possible
- Implement secure authentication and access controls
- Enable security options such as two-factor authentication and CAPTCHA
- Patch database vulnerabilities and improve isolation mechanisms for a compromised account not to affect others
- CCs must train all the employees to use the cloud securely
- Enable scanning for the files that users will store in the cloud
- Encrypt data stored in the cloud and data in transit to protect their integrity
- Implement strong key generation, storage, and management
- Check for data protection during design and runtime
- Implement robust registration and validation processes
- Monitor the client's traffic for any malicious activity
- Analyze the security model of the CSP interfaces
- Implement security best practices for installation and configuration
- Monitor the cloud environment for unauthorized changes or activity
- Enforce SLAs for patching and vulnerability remediation
- Conduct vulnerability scanning and configuration audits
- Disclose applicable logs and data to CCs
- Use clock synchronization solutions such as NTP (Network Time Protocol)
- Install a time server within an organization's firewall to minimize external threats and maximize time accuracy on the network
- The Network Time System can also be used to synchronize clocks with an enterprise network server

- Set clear segregation of responsibilities expressing the minimum actions consumers must undertake
- Implement effective policies and procedures such as information security policies.
- Clients should be permitted to audit/review CSPs information security policies and procedures.
- Monitor operational and security logs on a regular basis
- Enforce strict supply chain management and conduct a comprehensive supplier assessment
- Specify human resource requirements as part of legal contracts
- Require transparency in the overall information security and management practices, as well as compliance reporting
- Employ an adequate privilege separation scheme
- Update software on a regular basis to fix newly discovered privilege escalation vulnerabilities, if any
- Maintain data backups at different geographical locations
- Prepare an effective business continuity and disaster recovery plan
- Develop a containment plan to restrict the damage caused by a party that is trusted to fail
- Create visibility mechanisms to determine when elements of a supply chain are compromised
- Perform network traffic analysis using tools to find abnormalities
- It is essential to keep memory, storage, and network access isolated
- Practice persistent and careful efforts for execution of SLAs
- Use strong algorithms such as AES and RSA encryption to generate keys.

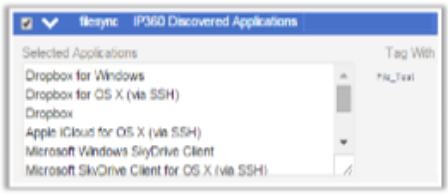
MITC Attack Detection Tool: Tripwire

Tripwire tools can be used to monitor user and network activities, and changes in files and registry entries

Step 1

Scanning the network for cloud-based file synchronization applications

- Tripwire IP360 tool can be used to scan the network for file synchronization applications such as OneDrive, Google Drive, and Dropbox
- Tripwire Enterprise tool is used to tag the critical organizational assets where these file synchronization applications are present
- Responders can achieve this by asset tagging integration between Tripwire IP360 and Tripwire Enterprise
- For example, the incident responders can set a tag called "File_Test", as shown below:



https://www.tripwire.com

MITC Attack Detection Tool: Tripwire (Cont'd)

Step 2

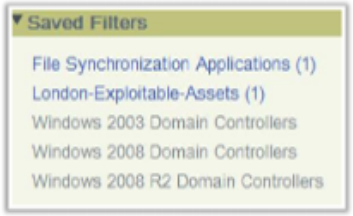
Applying rules for file changes/registry keys

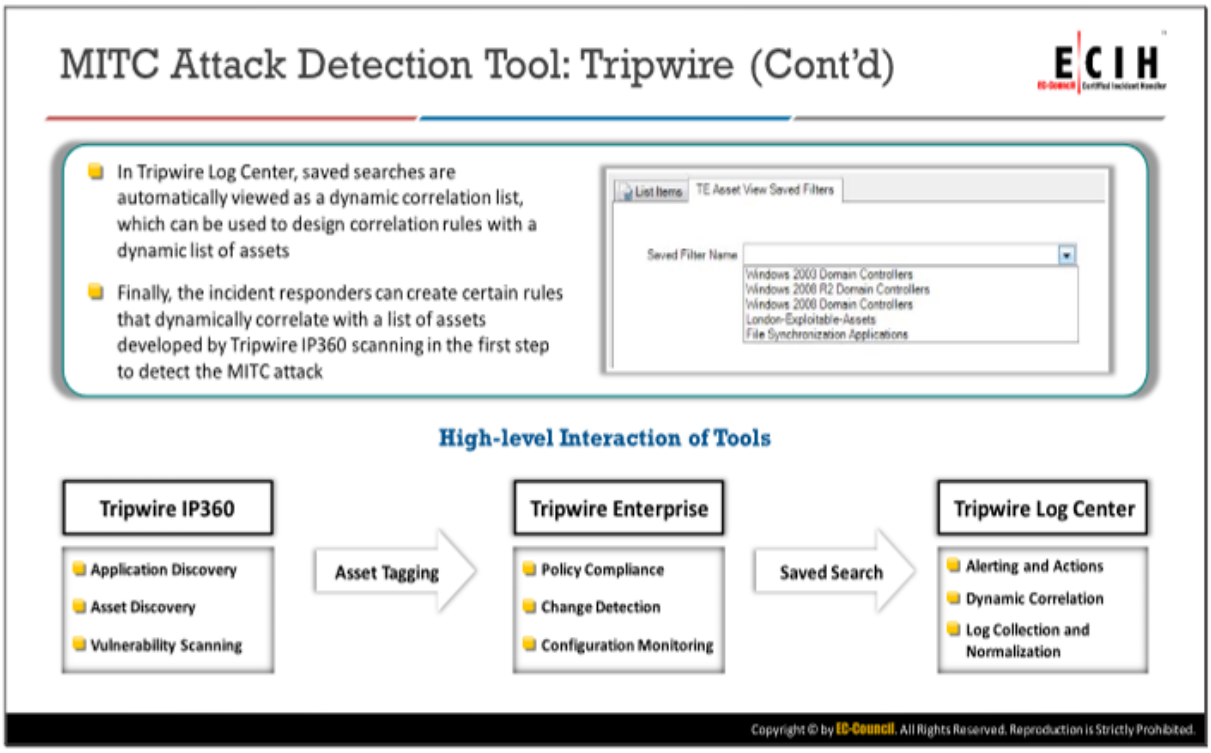
- The incident responders must create Tripwire Enterprise rules for monitoring changes in system files and registry keys
- Tripwire Enterprise offers real-time monitoring, which allows responders to view the files that are created, modified, or deleted in the network
- It can be used to detect malware responsible for MITC attack by monitoring synchronization application folders

Step 3

Generating alerts on security incidents

- An alert is generated if an attacker uses exploit to target a user on file synchronization application
- The responders can send this data change captured by Tripwire Enterprise to Tripwire Log Center to perform correlation using Dynamic Correlation Lists
- The responders can further use Tripwire Enterprise to create a saved search for assets with the "File_Test" tag, as shown in the screenshot





MITC Attack Detection Tool: Tripwire

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

The Tripwire tool can be used for monitoring user and network activities, changes in files, registry entries, and other events. This type of real-time monitoring of the network can assist incident responders in the detection of attacks such as MITC.

Attack detection can be accomplished by performing the following steps:

- **Scanning the network for cloud-based file synchronization applications**

  Incident responders can use the Tripwire IP360 tool to scan the network for file synchronization applications such as OneDrive, Google Drive, and Dropbox. After a complete scan of network, the scan report can be filtered to view only these applications.

  Similarly, the Tripwire Enterprise tool allows to tag critical organizational assets where these file synchronization applications are present. Responders can accomplish this through asset tagging integration between Tripwire IP360 and Tripwire Enterprise. For instance, the incident responders can set tag "File_Test" as shown in the screenshot given on the slide.

  Using this tagging rule, all the file synchronization applications in Tripwire Enterprise with string "File_Test" are automatically tagged by Tripwire IP360.

- **Applying rules for file changes/registry keys**

  The next step incident responders should take is the creation of Tripwire Enterprise rules for monitoring changes in system files and registry keys.

Tripwire Enterprise offers a real-time monitoring for the responders to view the files that are created, modified, or deleted in the network. It can also assist in detecting covering tracks or clearing file activities performed by attackers in the network. Similarly, Tripwire Enterprise allows to detect malware responsible for MITC attacks by monitoring synchronization application folders.

The tool can also collect SHA-1 (Secure Hash Algorithm 1) or other bits of data that can used as indicator of compromise (IoC) for further integration with an internal or an external threat database. When a change in the system or network is detected, the data are searched against the indicator of compromise database to evaluate a match to any known potential threats. If a match is found, an alert is generated.

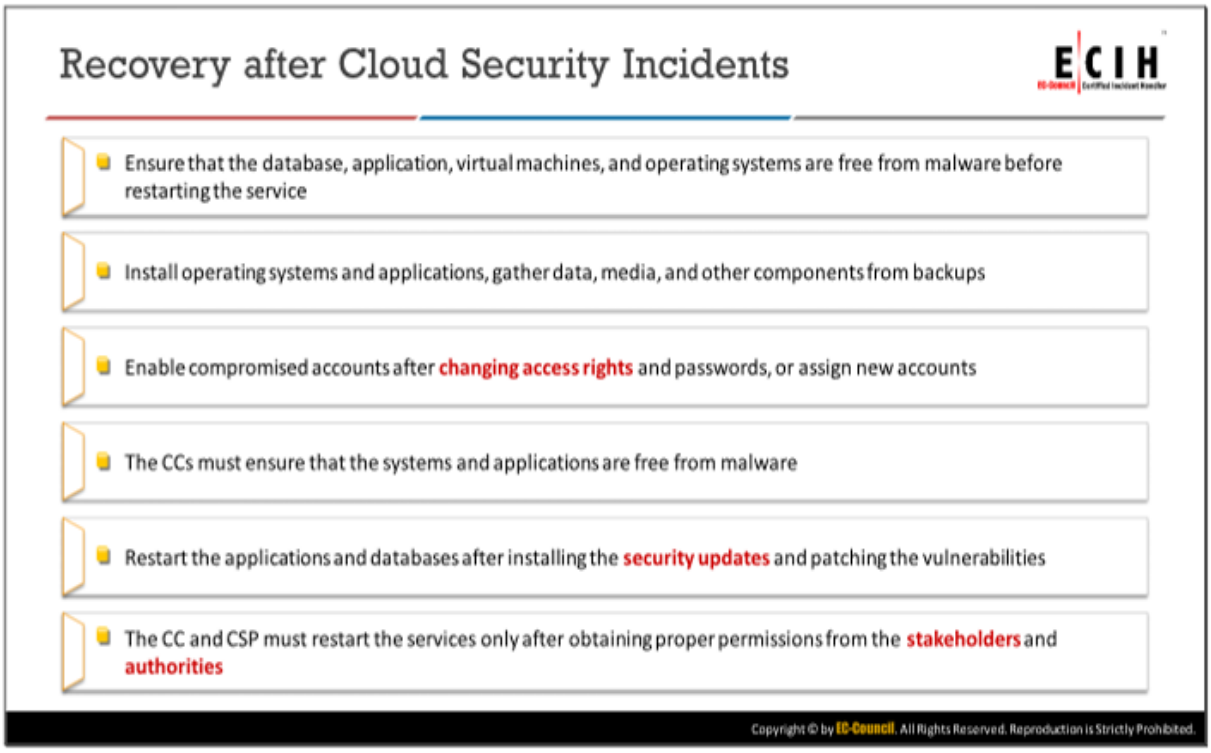
- **Generating alerts on security incidents**

  The Tripwire Log Center tool allows to detect any suspicious activity through the correlation of events and data. An alert is generated if an attacker uses a exploit to target a user in the file synchronization application. Incident responders can send these modification data captured by Tripwire Enterprise to Tripwire Log Center to perform correlation using dynamic correlation lists.

  The responders can further use Tripwire Enterprise to save searches for assets with the "File_Test" tag, as shown in the screenshot given on the slide.

  In Tripwire Log Center, the saved searches are automatically viewed as dynamic correlation lists, which can be used to design correlation rules that use the dynamic list of assets. Ultimately, incident responders can create rules that dynamically correlate on the list of assets developed by Tripwire IP360 scanning, created in the first step, to detect an MITC attack.

By performing the above mentioned steps, incident responders can dynamically monitor the cloud environment by correlating the collected data, finally alerting when an attack, such as MITC, is detected.



Recovery after Cloud Security Incidents

A compromised cloud platform can lead to severe consequences such as losing critical data, unavailability of network resources, and user credential theft. While prevention is key to limit the impact caused by an incident, the recovery procedure is also mandatory after an incident. Therefore, incident responders must follow various steps to control the damage incurred by an incident and follow a recovery process to restore the system operation and files.

This section provides various steps that must be taken by incident responders to recover from cloud security incidents.

Once incident responders detect security incidents in the cloud, they should contain the incident and then perform a recovery process to retrieve stolen files, restore individual assets that were compromised, and collect evidentiary data for further investigation. First, the incident responders must remove all the traces of malware and recover the data from backups in case the attacker has damaged any data or inserted malware in the cloud data. The responders must also ensure that administrators perform regular backups and test them for integrity and availability. The backup media must be kept secured from alteration, theft, or destruction.

Below, we list various steps that must be performed by incident handlers for recovery from cloud security incidents:

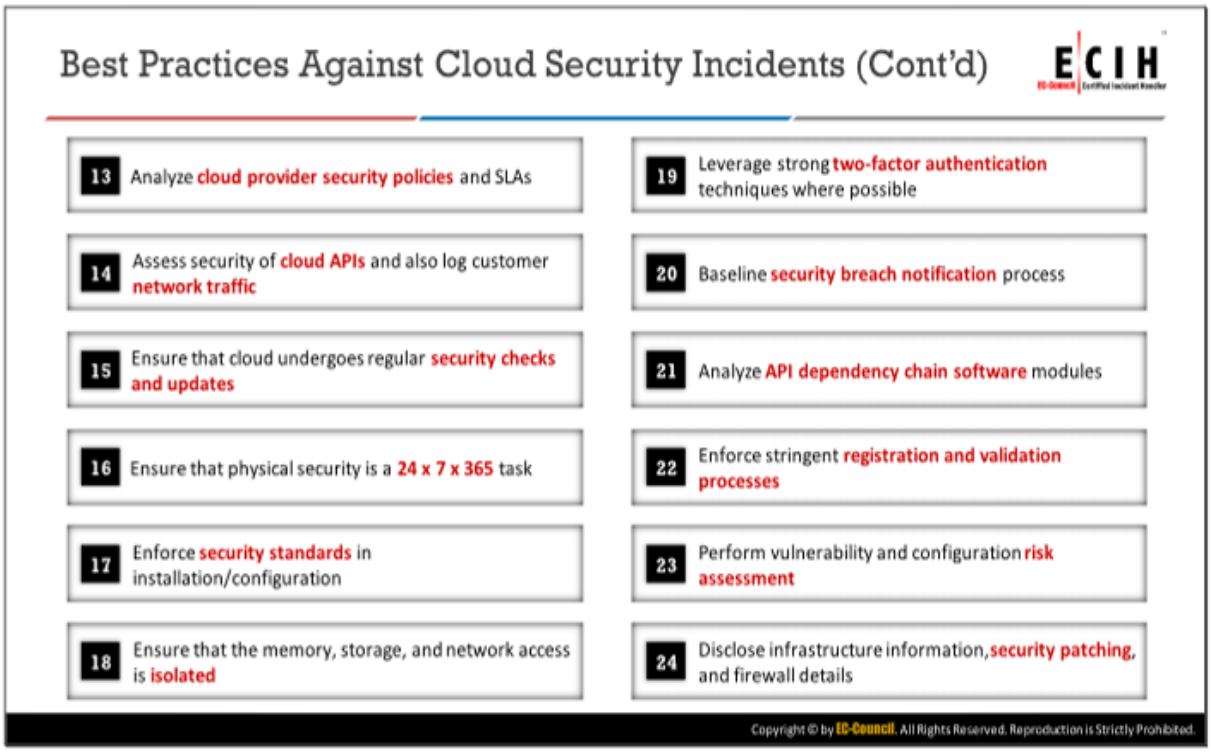
- Ensure that the databases, applications, VMs, and OSs are free from malware before restarting the services
- Install OSs and applications, gather data, media, and other components from backups
- Enable compromised accounts after changing access rights and passwords or assign new accounts
- Ensure that the systems and applications of the CCs are free from malware
- Restart the applications and databases after installing security updates and patching vulnerabilities
- Restart the services on the CC and CSP sides only after obtaining proper permissions from stakeholders and authorities

Best Practices Against Cloud Security Incidents

- Best Practices Against Cloud Security Incidents
- Cloud Security is the Responsibility of both Cloud Provider and Consumer
- Cloud Security Tools

Best Practices Against Cloud Security Incidents

1 Enforce **data protection**, **backup**, and **retention** mechanisms	7 Implement strong **authentication**, **authorization**, and **auditing** mechanisms
2 Enforce **SLAs** for patching and vulnerability remediation	8 Check for **data protection** at both design and runtime
3 Vendors should regularly undergo **AICPA SAS 70 Type II audits**	9 Implement **strong key generation**, storage and management, and destruction practices
4 Verify one's own cloud in **public domain blacklists**	10 Monitor the **client's traffic** for any malicious activities
5 Enforce **legal contracts** in employee behavior policy	11 Prevent unauthorized server access using **security checkpoints**
6 Prohibit **user credential sharing** among users, applications, and services	12 Disclose applicable **logs** and **data** to customers



Best Practices Against Cloud Security Incidents

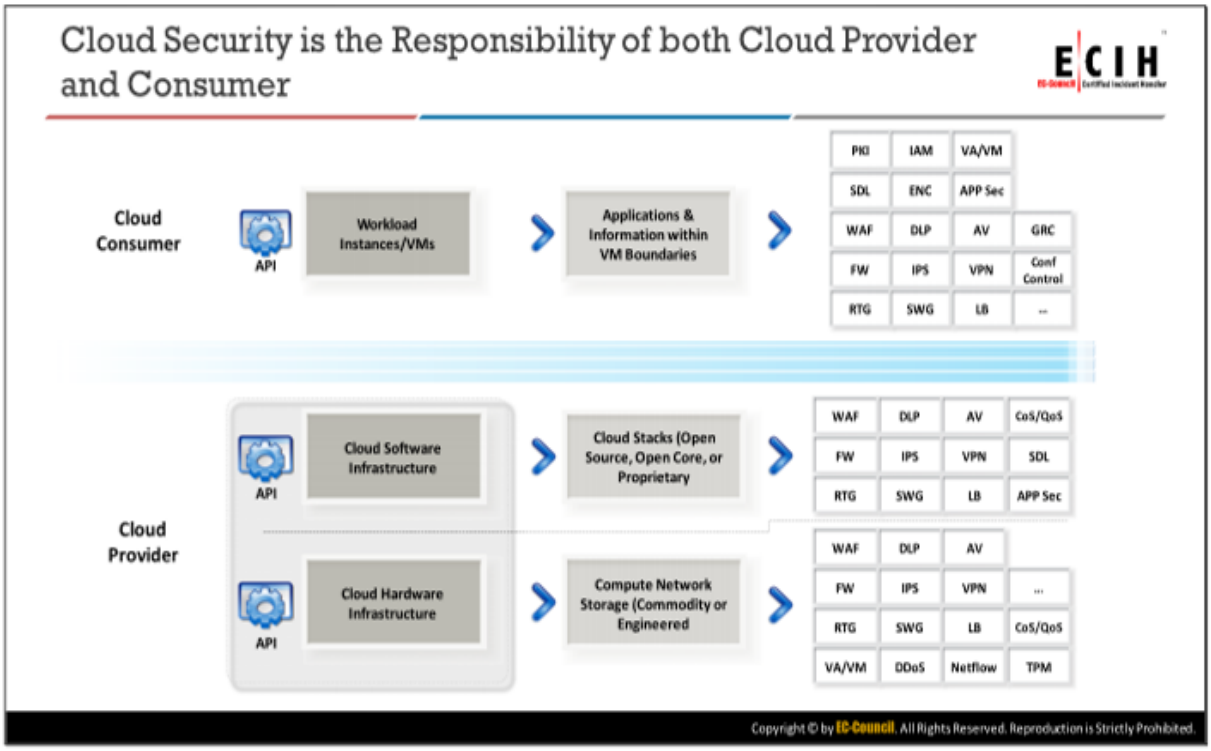
Various risks and threats are associated with cloud service adoption and migration of business-critical data to third-party systems. Nevertheless, the following security guidelines and best practices strengthen the business case for cloud adoption.

This section provides various best practices against cloud security incidents and various cloud security tools.

Below, we list best practices for securing the cloud:

- Enforce data protection, backup, and retention mechanisms
- Enforce SLAs for patching and vulnerability remediation
- Vendors should regularly undergo AICPA (American Institute of Certified Public Accountants) SAS (Statements on Auditing Standards) 70 Type II audits
- Verify the cloud in public domain blacklists
- Enforce legal contracts in employee behavior policy
- Prohibit user credentials sharing among users, applications, and services
- Implement secure authentication, authorization, and auditing mechanisms
- Check for data protection during design and runtime
- Implement strong key generation, storage and management, and destruction practices
- Monitor client's traffic for any malicious activity
- Prevent unauthorized server access using security checkpoints

- Disclose applicable logs and data to CCs
- Analyze CSP security policies and SLAs
- Assess security of cloud APIs and log customer network traffic
- Ensure that the cloud undergoes regular security checks and updates
- Ensure that physical security is available 24 × 7 × 365
- Enforce security standards during installation/configuration
- Ensure that memory, storage, and network access is isolated
- Leverage strong two-factor authentication techniques where possible
- Implement baseline security breach notification process
- Analyze API dependency chain software modules
- Enforce stringent registration and validation processes
- Perform vulnerability and configuration risk assessments
- Disclose infrastructure information, security patching, and firewall details to CCs
- Enforce stringent cloud security compliance, SCM (Software Configuration Management), and management practice transparency
- Employ security devices such as intrusion detection systems, intrusion prevention systems (IPSs), and firewalls to guard and stop unauthorized access to data stored in the cloud
- Enforce strict supply chain management and conduct comprehensive supplier assessments
- Enforce stringent security policies and procedures like access control policy, information security management policy, and contract policy
- Ensure infrastructure security through proper management and monitoring, availability, secure VM separation, and service assurance
- Use VPNs (virtual private networks) to secure clients' data and ensure that data are completely deleted from primary servers along with their replicas when requested for data disposal
- Ensure use of SSL (Secure Sockets Layer) for sensitive and confidential data transmission
- Analyze security model of CSP interfaces
- Understand terms and conditions in SLA, such as minimum level of uptime and penalties in case of failure to satisfy the agreed level
- Enforce basic information security practices, namely, strong password policy, physical security, device security, encryption, data security, and network security



Cloud Security is the Responsibility of both Cloud Provider and Consumer

Security is a shared responsibility in cloud systems, in which both CCs and CSPs have varying levels of control over the available computing resources. Compared to traditional IT systems, in which a single organization has authority over the complete stack of computing resources and the entire lifecycle of systems, CCs and CSPs should work together to design, build, deploy, and operate cloud systems. Therefore, both parties share responsibilities to maintain adequate security in these systems. The different cloud service models (i.e., IaaS, PaaS, and SaaS) imply varying levels of control between CCs and CSPs.

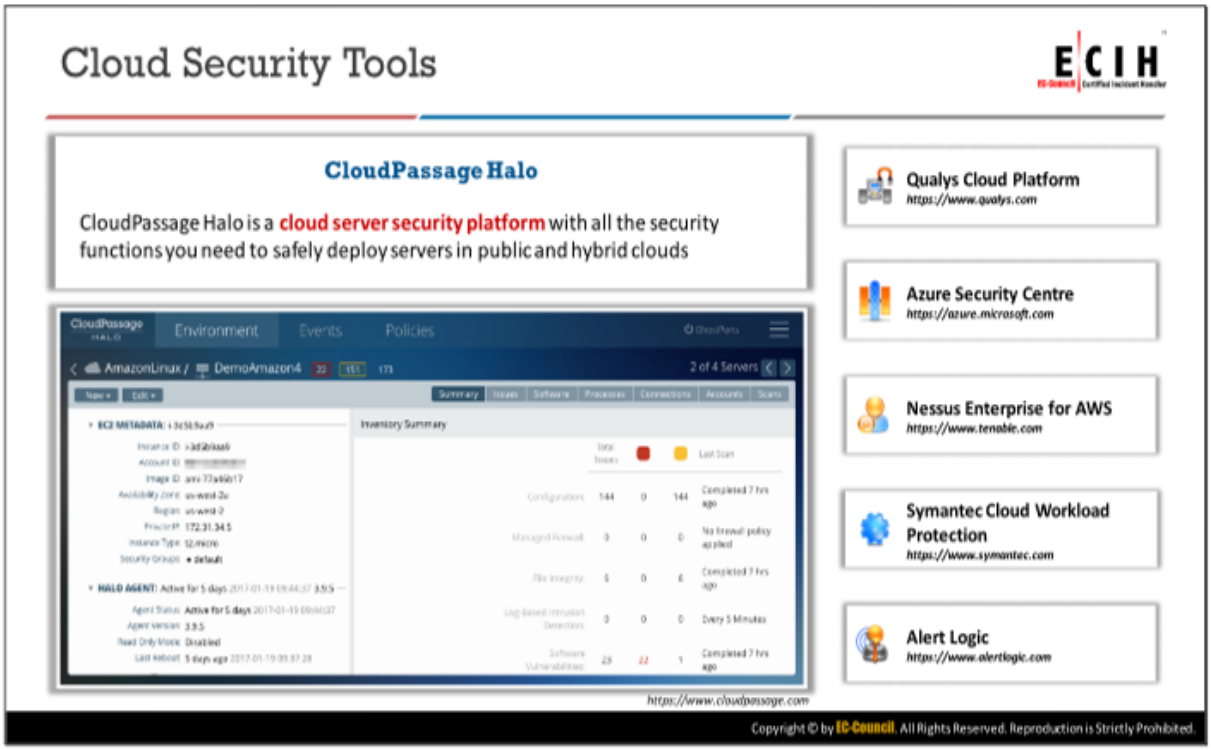
Example:

In the IaaS model, the CSP usually performs account management control for the initial system privileged users, whereas a CC controls user account management for applications deployed in the IaaS but not for those in the CSP.

Various cloud security controls are listed below:

- **PKI**: Public key infrastructure
- **SDL**: Security Development Lifecycle
- **WAF**: Web application firewall
- **FW**: Firewall
- **RTG**: Real Traffic Grabber
- **IAM**: Identity and access management
- **ENC**: Encryption
- **DLP**: Data loss prevention

- **IPS**: Intrusion prevention system
- **SWG**: Secure Web gateway
- **VA/VM**: Virtual application/virtual machine
- **App Sec**: Application security
- **AV**: Antivirus
- **VPN**: Virtual private network
- **LB**: Load balancer
- **GRC**: Governance, risk management, and compliance
- **Config Control**: Configuration control
- **CoS/QoS**: Class of service/quality of service
- **DDoS**: Distributed denial of service
- **TPM**: Trusted Platform Module
- **Netflow**: Network protocol by Cisco



Cloud Security Tools

Although migrating to the cloud can provide enormous benefits, security issues are the primary concern for enterprise cloud adoption. Nevertheless, many security services and tools are available for securing cloud resources and services to ensure confidentiality, integrity, and security of the data hosted in the cloud.

Below, we list some important cloud security tools:

- **CloudPassage Halo**

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

  The CloudPassage Halo software-defined security (SDSec) platform was built to protect private clouds, public IaaS, and hybrid/multi-cloud infrastructures. It provides security and compliance automation from development to deployment across clouds, data centers, servers, and containers—at DevOps speed and cloud scale. In addition, it automates and orchestrates layered access control, vulnerability management, compromise prevention, compliance monitoring, and security intelligence collection.

  Features:

  - **Workload firewall management:** Deploy and manage dynamic firewall policies across public, private, and hybrid cloud environments
  - **Multifactor network authentication:** Enables secure remote network access using two-factor authentication via SMS (short message service) to a mobile phone or using a YubiKey without requiring additional software or infrastructure
  - **Configuration security monitoring:** Automatically monitors the OS and application configurations, processes, network services, privileges, and so on

- **Software vulnerability assessment:** Scans for vulnerabilities in packaged software rapidly and automatically across all the cloud environments
- **File integrity monitoring:** Protects the integrity of cloud servers by continually monitoring for unauthorized or malicious changes to essential system binaries and configuration files
- **Server account management:** Evaluates who has accounts in which cloud servers, what privileges they operate under, and the usage of accounts
- **Event logging and alerting:** Detects a broad range of events and system states, alerting on their occurrence
- **Halo REST (representational state transfer) API:** Provides full automation of cloud deployment and integrates security platforms with other systems

Various additional cloud security tools include:

- Qualys Cloud Platform (*https:/www.qualys.com*)
- Azure Security Centre (*https://azure.microsoft.com*)
- Nessus Enterprise for AWS (Amazon Web Services) (*https://www.tenable.com*)
- Symantec Cloud Workload Protection (*https://www.symantec.com*)
- Alert Logic (*https://www.alertlogic.com*)
- Deep Security (*https://www.trendmicro.com*)
- SecludIT (*https://secludit.com*)
- Panda Cloud Office Protection (*https://www.pandasecurity.com*)
- Data Security Cloud (*https://www.informatica.com*)
- Cloud Application Control (*https://www.zscaler.com*)
- Intuit Data Protection Services (*https://security.intuit.com*)

Module Summary

In this module, we have discussed fundamental concepts of cloud computing and provided an overview of handling cloud security incidents. In addition, the responsibilities and challenges involved in handling and responding to cloud security incidents and various cloud security threats and attacks have been described. We have also discussed general preparation steps to handle cloud security incidents and detailed various methods to detect and analyze cloud security incidents.

Then, we have discussed the containment of cloud security incidents and containment tools. We have also detailed the eradication of cloud security incidents and recovery from the incidents. Finally, we provided various best practices to prevent against cloud security incidents.

In the next module, we detail the handling and response to insider threats.

This page is intentionally left blank.