Domain 11: Incident Response & Resilience

Introduction

Incident response (IR) is a critical aspect of any information security program. A cloud service customer (CSC) will likely experience a security breach at some point, regardless of how strong its security posture is. While many CSCs have an incident response plan for investigating attacks, cloud adaptation introduces distinct variations in processes, technologies, and governance, adding complexity to responding to incidents.

This domain seeks to identify and explain best practices for cloud incident response and resilience that security professionals may use as a reference when developing their own incident plans and processes. This domain is organized according to the commonly accepted Incident Response Lifecycle described in the CSA Cloud Incident Response (CIR) Framework[47] and NIST Computer Security Incident Handling Guide (NIST SP 800-61 Rev. 2)[48]. Other resources include the CSA incident response research hub[49] and other international standard frameworks for incident response, such as ISO/IEC 27035 and the ENISA Strategies for incident response and cyber crisis cooperation.

Organizational resilience to cyber-attacks and other risk scenarios critically depends on adequate incident response, which is rooted in proper architecture.

Learning Objectives

The learning objectives for this domain aim to provide readers with knowledge on:

- Distinguish between events, incidents, and breaches and use a response process to react.
- Prepare and respond to incidents.
- Detect and analyze relevant data.
- Contain, eradicate, and recover.
- Perform resilience planning for failure.

[47] CSA. (2021) Cloud Incident Response Framework.
[48] NIST. (2012) Computer Security Incident Handling Guide. Comment period for potential revisions closed mid-2024.
[49] CSA. (2024) CSA Research landing page.

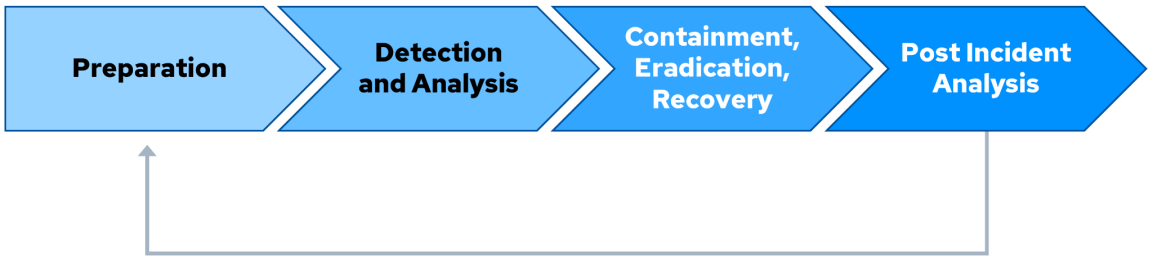
11.1 Incident Response

Cloud IR is about detecting, identifying, and responding to events that could affect a cloud platform, applications, and data. This necessitates a clear differentiation between events, incidents, and breaches. Each represents a distinct level of threat and requires tailored response strategies.

An 'event' is any observable issue on a cloud platform that may indicate an underlying security or availability issue.[50] An event can escalate to an 'incident' when it is determined to violate security policies, unauthorized use or access, or any condition that could threaten operations or the cloud environment. Incidents require immediate attention to contain and mitigate their effects, preventing escalation. The apex of this characterization is 'breaches,' which signify a successful penetration or circumvention of security measures, leading to unauthorized access or extraction of data.

11.1.1 Incident Response Lifecycle

The Incident Response Lifecycle described by NIST includes four phases and major activities: Preparation, Detection and Analysis, Containment Eradication and Recovery, and Post-Incident Activity.[51]



Based on NIST 800-61rev2 (Post Incident Analysis replaces Post Mortem) [52]

Figure 29: Phases of IR Life Cycle in Cloud Security

Preparation: Establish an incident response capability to respond to incidents. This entails the following:

- Establish an incident response process
- Build a team and assign roles and responsibilities
- Train the team and run exercises
- Establish a communication plan and facilities
- Responder access to environments
- Responder access to tools: incident analysis services, hardware, and software
- Internal documentation (e.g., port lists, asset lists, network traffic baseline)
- Evaluate infrastructure: proactive scanning and monitoring, vulnerability and risk assessments
- Subscribe to third-party threat intelligence services

[50] Additional material on events is provided in Domain 6: *Security Monitoring*.
[51] The Incident Response Life Cycle is described in the CSA Cloud Incident Response Framework and NIST 800-61rev2. This content focuses on incident response for the cloud environment, however, while cloud IR is primarily separate, it often overlaps with traditional IR. Responders focused on both environments should work closely together using this consistent response process.
[52] NIST. (2012) Computer Security Incident Handling Guide, Figure 3-1. Incident Response Life Cycle, Page 21.

- Evaluate CSPs and their capabilities to aid in incident response regarding the services/resources consumed
    - Audit logs, snapshots, forensics capabilities, and e-discovery features
- Conduct backup restoration testing regularly and disaster recovery (DR) tests at least once per year to ensure that incident response plans are up-to-date and effective

Detection & Analysis: Identify security incidents and analyze their impact. This entails the following:

- Detection engineering
- Alerts:[53] This includes Cloud Security Posture Management (CSPM), security information and event management (SIEM), workload protection, and network security monitoring.
- Validate alerts (reduce false positives), with escalation.
- Estimate the scope of the incident.
- Assign an Incident Manager to coordinate actions.
- Build a timeline of the attack.
- Determine the extent of the potential data loss or impact.
- Notify and coordinate activities.
- Communicate the incident containment and recovery status to senior management.

Containment, Eradication, & Recovery: Isolate the incident to prevent further damage and remove the root cause; recovery: restore affected systems.

- Containment: Isolate identities and workloads, taking systems or services offline, and consider the tradeoffs between data loss versus service availability.
- Eradication & Recovery: Clean up compromised assets and restore systems and services to normal operation. Deploy controls to prevent similar incidents.
- Document the incident and gather forensic evidence (e.g., chain of custody).

Post-Incident Analysis[54]: Learn from the incident, document, and improve future responses.

- Lessons learned: Which detections worked, and which alerts fired properly? What detections and protections need to be created based on the event? What improvements does the incident response process need to make? What Indicators of Compromise (IOC) were discovered and were they shared with the community?

Many incidents may span cloud and traditional infrastructure and devices, requiring incident responders to ensure they do not develop tunnel vision and only look at one facet of an incident.

11.2 Preparation

The Preparation phase can be broken into four major categories which will be covered in detail in the following sections:

[53] Additional material on alerts is provided in Domain 6: *Security Monitoring*.
[54] Note that some incident response framework versions have a "Post-Mortem" phase. The industry now refers to the "Post-Mortem" phase as "Post-Incident Analysis" since this better reflects the activity. CSA, NIST, and other industry authoritative bodies follow this change in nomenclature.

- Changes due to the relationship with the cloud provider
- Changes in responder training
- Changes needed to support the CIR process
- Changes required to support CIR technologies

11.2.1 Incident Response Preparation & Cloud Service Providers

Cloud incidents are shared incidents, even when the customer owns all of the affected resources. Any incident involving a public cloud requires an understanding of the contractual agreement, including the specific service level agreements (SLAs), and what resources the CSP offers to CSCs. Depending on the relationship with the provider, there might not be direct points of contact and might be limited to whatever is offered through standard support channels. Many providers have different support levels, and CSCs should consider subscribing to the level of support that is appropriate to the business criticality of the service (e.g., direct contacts and faster support for any business-critical deployments or deployments with highly sensitive or regulated data).

In addition to paid support, some CSPs extend some level of incident response assistance to customers at no additional cost. For each CSP worked with, it is important to have a list of the incident support options (paid and free) and contact information for each. This information should be recorded in a cloud deployment registry.

At this stage, it is also important to plan for incidents that affect the CSP and are out of the CSC's control. For example, there are documented cases of public vulnerabilities and denial-of-service attacks that impact a CSP. A CSC is not necessarily helpless, and there may be response activities it can perform itself, depending on the nature of the incident. The incident response team should understand this risk and game out some possible scenarios and mitigating actions. This usually requires coordination with business continuity activities.

11.2.2 Training for Cloud Incident Responders

Although cloud incident response shares many characteristics and processes with traditional incident response, it is important for responders to understand the process and technology differences.

For specific details on specific cloud IR training, refer to the CCSK Security Guidance documentation, and papers published by CSA IRWG.

11.2.2.1 Enable Responder Access

Some key adjustments are needed by other teams and the organization to support cloud incident response: The cloud incident response team should have persistent read access to all deployments. It is nearly impossible to investigate a cloud incident without being able to review the resources and configurations involved. All use of these privileges should be logged and reviewed. Two levels should be supported, depending on the capabilities of the cloud provider:

- Read access to metadata and configurations, sometimes called "security audit," should be persistent, and the default level of access for responders.
- Full-read access, which allows review of the data, not just the metadata, can and in many cases should require multiple approvals to use and follow a "break glass" process.

The incident response team should have access to the cloud deployment registry, and that registry should have current information to contact the business owner and technical leads. Incident responders may need access to CI/CD pipelines, code repositories, and other locations that manage and modify cloud configurations. Response processes for Containment, Eradication, and Recovery will likely need to use these resources and services. This is a case where the IR team and the deployment or application owners must be prepared to work together.

11.3 Detection & Analysis

The fundamentals of incident detection and analysis do not necessarily change at a high level with the introduction of the cloud, but the details do change significantly.

Key cloud differences include:

- The new telemetry for detection and analysis that cloud introduces
- The additional attack surface of the management plane, which has to be the primary focus during any response
- The higher rate of activities in the cloud, which include the speed of attackers (who are highly automated) and the speed of change of cloud environments themselves
- The lack of a traditional network perimeter and the addition of an IAM blast radius
- The API-driven nature of the cloud and the ephemeral nature of resources
- The decentralized management of infrastructure by cloud and development teams
- The impact of automation, infrastructure as code (IaC), serverless, and other cloud-native technologies

These differences sometimes improve our ability to detect and analyze incidents, while others create new challenges. The guidance in this section highlights these major differences and how to adjust detection and response activities.

11.3.1 Cloud Impact on Incident Response Analysis

The focal point of incident analysis in cloud settings is often the management plane, which offers a comprehensive view of cloud activities through its logs. These logs are invaluable for identifying unauthorized access, misconfigurations, and other anomalies that could indicate a security incident.[55]

The dynamic nature of cloud environments, where resources can be rapidly provisioned and decommissioned, demands that incident response teams adapt their methodologies. This includes

[55] Additional material on incidents is provided in Domain 6: *Security Monitoring*.

leveraging automation and machine learning to keep pace with the speed of cloud operations and configuration changes.

For environments managed using CI/CD, the analysis should include the pipeline and its supply chain, since they can be a major target for attackers and a powerful vector to compromise cloud applications and infrastructure.

Finally, the shared nature of cloud services makes it more relevant to include external threat intelligence services.

There are multiple places to perform detection as seen in the figure below:[56]

- CDR
- SIEM
- CSPM/Cloud Native Application Protection Platform (CNAPP)
- CSP/Identity Provider (IdP)

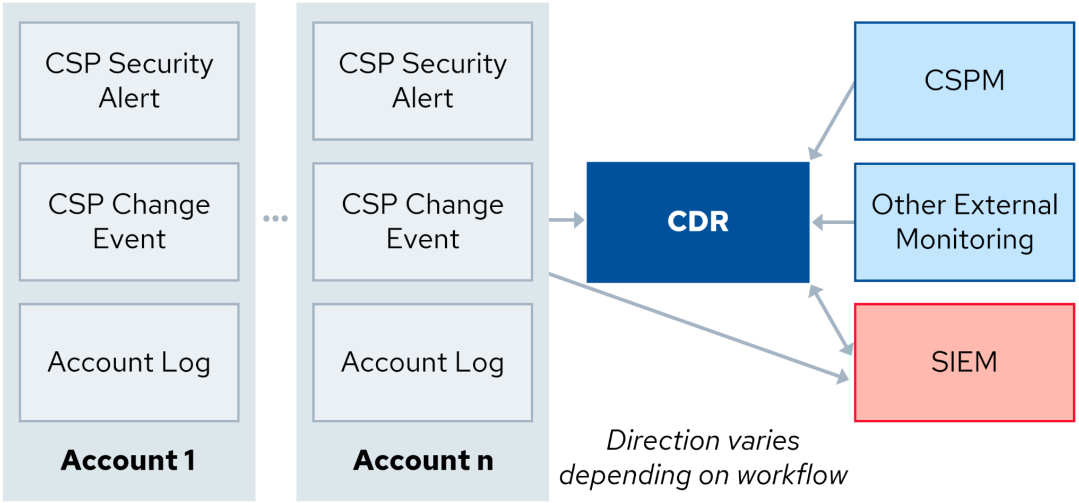


Figure 30: Figure 30: Example of an IR Analysis Workflow

11.3.2 Cloud System Forensics

Cloud forensics falls into two major categories: analysis of management plane, service, and other logs, and system forensics for virtual machines (VMs) and containers. Traditional digital (systems) forensics methodologies often rely on physical access to hardware and local data storage, which is not possible in the cloud. Instead, cloud forensics requires incident response teams to work within the constraints and capabilities provided by CSPs.

[56] This topic is covered in more detail in *Domain 6: Security Monitoring*.

Key aspects of cloud forensics include:

- **Snapshots:** Nearly all CSPs and container management systems support snapshots which can be used for forensics analysis. A CSC should grasp how and why to take snapshots of storage volumes immediately when an incident is detected to preserve the state of the VM for analysis.
- **Volatile memory acquisition:** Without the ability to instrument hardware, if memory forensics is required, the responders will need to install software tools which will also affect the system.
- **Log analysis:** Management plane logs, along with system, application, and user activity logs, can also be used to present a fuller picture of incidents even when the focus is on VMs/containers. They can, for example, help identify an attacker who obtained system credentials and pivoted to the management plane.
- **Evidence preservation:** Preserving digital evidence in cloud environments requires a thorough understanding of the backup and data retention policies of both the CSP and the CSC and the chain of custody of snapshots.

11.3.2.1 Cloud Forensics: Container & Serverless Considerations

The rise of containerization and serverless computing introduces additional layers of complexity to cloud forensics.

The following are key container and serverless considerations:

- **Containers:** Containers are naturally ephemeral, often existing for only short periods. This transience poses significant challenges for forensic data collection and analysis. Forensic strategies must include capturing container logs and snapshots of container states to provide insights into the activities and data a container processes. Because of that, it is highly recommended to redirect container logs, VM logs, and service logs to external log storage.
- **Serverless computing:** Serverless architectures further abstract the execution environment from the user, with CSPs managing the underlying infrastructure. Forensic analysis in serverless environments relies heavily on the logs generated by serverless functions, including execution logs, access logs, and application logs. Understanding the invocation and execution patterns of serverless functions is crucial for reconstructing events during an incident.

The following is an example of using a forensics acquisition and analysis environment and collecting storage volume snapshots from a compromised workload in a separate deployment.

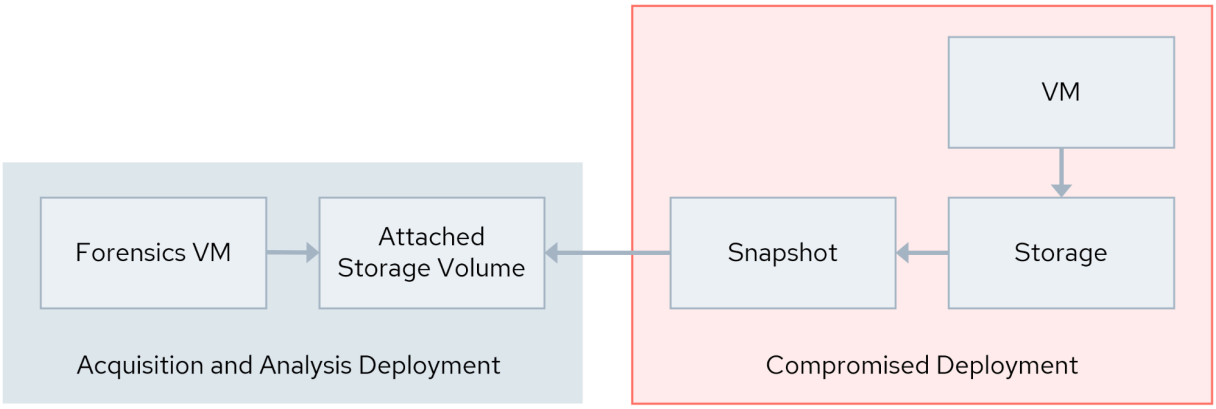


Figure 31: Cloud Forensics: Snapshot Acquisition and Analysis Process

11.4 Containment, Eradication, & Recovery

Of all the incident response activities, those in the Containment, Eradication, and Recovery phases are most deeply affected by the specific technical and architectural models used in cloud deployments. Immutable IaC, autoscaling, microservices, identity federation, and the underlying technologies profoundly impact the processes and techniques available for these activities. In many cases bringing significant advantages compared to responses in traditional datacenters.

11.4.1 Containment

It is important to engage the cloud and application owner, when possible, to assist in determining the proper containment plan. They may also be the best to implement the plan since they know their deployment environment better than any central incident response team does. IAM and management plane containment should be the top priorities in any security incident. Proper IAM containment can be very difficult. Cloud typically relies on federated identity, where authentication and authorization are separated and often performed on different platforms. Containment may require different actions on both the identity provider and within the relying party, where the relying party will need to alter entitlements (such as using a deny policy) or add conditions (such as only accepting tokens issued after a particular time).

A second complication is when service account credentials are compromised and abused. IAM containment also requires a good understanding of whether the attacker was able to use their access to escalate or pivot into different identities, just as we track attackers pivoting around a network. This may require tight coordination between an analyst and a responder if those are separate roles.

Network containment is often easier in cloud networks since it relies on Software Defined Networking. Rules can be changed very quickly and easily using API calls and web consoles.

Containment activities should also prioritize resources that have been made public or were shared with an unknown destination (e.g., an unknown cloud account/subscription/project in the same CSP). For critical data, containment may need to risk breaking application functionality temporarily, and incident responders should have a timely escalation path to the authority and capability to make this decision and take action in highly critical situations.

11.4.2 Eradication

The primary focus of eradication should be to permanently remove the attacker from the management plane. This could be through credential rotation, adding additional policy conditions, adding MFA or digital certificates, and similar techniques. This is only possible when the origin of the incident is determined so the source IAM/access can be locked down. An analysis needs to be performed during and after an incident, not just on detection, to identify if the attacker was able to pivot within the management plane or IAM system.

Eradication often requires deleting old versions of images, serverless code, and IaC. Attackers may use these to re-compromise a deployment, especially if an employee accidentally re-deploys an old version in whole or in part.

11.4.3 Recovery

IaC, autoscaling, and other automation are incredibly powerful for incident recovery. They can rapidly deploy hardened versions of applications and infrastructure or even deploy a clean version into an entirely new environment. All images, resources, and templates used in recovery should be analyzed to ensure that the root cause was eliminated and that the attacker did not leave any lingering backdoors.

11.5 Post Incident Analysis

One of the most important, yet often overlooked, stages of incident response is determining the lessons learned and then taking active steps to reduce the likelihood or impact of future, similar events. This is done in the post-incident analysis phase. In this phase the responders determine the root cause of the incident, analyze the response process, and try to identify areas of improvement. This is less about assigning blame, and more about trying to identify structural issues that can be modified to prevent, or limit, future events.

The fundamentals of the Post Incident Analysis phase are not different for the cloud, but there are a few best practices to highlight.

- Since many cloud incidents involve working with the team that managed the cloud deployment, they should be included in any post-incident analysis.
- Responders should be required to create a new runbook/playbook for new incident types they encounter.

- Many cloud security incidents are the result of misconfigurations. Rather than assigning blame, CSA recommends following a Just Culture[57] approach, which focuses on the identification of systemic failures before blaming individuals, while still holding individuals accountable for their actions. For example, if over-privileged IAM was the source of the breach, the CSC may consider utilizing scanners to identify potential IAM issues. Security may provide common baselines and work with teams to review permissions. Alternatively, the organization can move from static credentials to Just-in-Time entitlements combined with strong authentication, using frictionless tooling that doesn't slow down developers.

[57] Just Culture is a concept that is related to systems thinking. The concept emphasizes that mistakes are typically a fault of the organizational culture rather than a fault of a person. The idea is to shift from "who did it" to "what went wrong".