More about incident response phases

So far, you've learned how incident management protects assets in a cloud environment and helps security operations teams effectively respond to a security threat. As a reminder, **incident management** involves the identification, analysis, and resolution of security incidents within a cloud environment.

In this reading, you'll explore more about each phase involved in incident response, along with the key roles and responsibilities of an incident response team.

Please note, the following reading should not be considered legal advice. If there is an investigation in a workplace situation, reach out to your organization's legal council.

Incident response and management

Organizations rely on incident response to mitigate the impact of a security incident and enable quick recovery. A security incident is also used as a teachable moment, helping organizations learn from what happened and work to prevent similar occurrences in the future. As a cloud security professional, you and your team will conduct incident management in five main phases:

1. **Detection**
2. **Analysis**
3. **Containment and eradication**
4. **Recovery**
5. **Lessons learned and improvement**

Detection

The early detection of potential issues is critical for any incident response plan. During this phase, security teams are notified of potential security incidents. Typically, notifications about security incidents are provided by an organization's security solution. Tools like intrusion detection systems (IDS) and security information and event management (SIEM) monitor events in a cloud environment and send alert notifications to security teams when a potential security incident is detected. Another way security teams can receive incident notifications is by users who submit reports about any suspicious activity they observe on their systems.

Analysis

If a security incident is detected, then security teams must perform a detailed analysis of the alert. The purpose of this phase is to get a better understanding of what happened, assess the potential impact, and determine the severity so that security teams can identify the next steps to take.

The importance of preserving evidence

During analysis, it's critical to ensure that evidence is properly preserved because it may be required by law enforcement, regulatory bodies, or insurance vendors. Examples of evidence preservation include:

- Taking images of affected devices to capture the state of the device at a specific point in time
- Documenting all actions that were taken using a chain of custody
- Storing the evidence in a secure location
- Protecting evidence from unauthorized access

Containment and eradication

After you analyze a security incident, you must contain it to limit additional damage. Then, you need to eradicate all artifacts the attacker created related to the security incident. This includes unauthorized applications, virtual machines, files, or storage buckets.

Containment steps

Here are some steps that a security team commonly takes to contain a security incident:

- **Identify the compromised resources**: Review your logs to identify the suspicious activity.
- **Isolate the compromised resource**: Disable the network interface card (NIC), or create a new firewall rule that blocks network traffic to the compromised resources.
- **Revoke access to the compromised resources**: Revoke the access tokens for the compromised users and service accounts.
- **Reset the passwords of compromised user accounts**: Reset passwords to prevent attackers from accessing the compromised resources again.
- **Monitor your environment for any suspicious activity**: Monitor the environment to detect any new attacks.

Eradication steps

When an attacker gains access to your network, it's important to have a plan in place to evict them as quickly as possible. This is because the longer the attacker remains on your network, the more damage they can do. An eviction plan should include these steps:

- **Identify the attacker**: To identify the attacker, review your network logs for suspicious activity to identify IP addresses, DNS accounts, and compromised systems.
- **Isolate the attacker**: Once you identify the attacker, you need to isolate them from the rest of your network. To do this, create a new firewall rule that blocks traffic from the attacker's IP address and disables the accounts or expires the OAuth token.
- **Evict the attacker**: Once you isolate the attacker, evict them from your network. To do this, reset their passwords or disable their accounts to remove persistence mechanisms.

Recovery

After the security team properly contains and eradicates the security incident, the team focuses on restoring business operations back to normal. During recovery, the team works to ensure that systems are functioning as expected and implements precautionary measures. Once the team evicts the attacker, the team needs to restore any critical services that were affected by the attack to a point in time before they were compromised.

Lessons learned and improvement

In the final phase, the security team reviews the details of the incident and response to help determine the incident's root cause and identify areas of improvement.

Best practices

This list includes best practices for incident response and management:

- **Update detection rules**: After the security team reviews an incident, they can identify gaps in security posture. Security teams might need to create new detection rules or update rules to identify suspicious activity based on what was discovered during the investigation.
- **Harden systems**: Once security gaps are filled, the security team can take steps to harden the systems against attack. This can include creating strong passwords, enabling two-factor authentication, closing firewall rules, and keeping software up to date.
- **Conduct a tabletop exercise**: A tabletop exercise is an exercise where participants are given an attack scenario and discuss how they would use the organization's incident response plan to mitigate the attack.

Note: On-premises incident response and cloud incident response differ significantly. Typically, on-premises incident response focuses on analyzing endpoints—which are any devices connected to a network—while cloud incident response typically focuses on digital identity—which are user accounts used to authenticate into environments and access cloud resources.

Roles and responsibilities

Here are some of the common roles in an incident response team:

- **Incident commander**: The incident commander is responsible for coordinating the incident response from the start to the end of the incident. The incident commander assigns experts from different teams to form the incident response team and delegates responsibilities.
- **Communications lead**: The communications lead manages communication around the incident. They can also be responsible for communicating with key stakeholders and keeping all relevant parties informed of the incident status.
- **Operations lead**: The operations lead manages technical response and remediation of the incident.
- **Subject matter expert**: The subject matter expert—also called the SME—provides subject matter expertise.

Other members may be included throughout the incident response process. This can include executive sponsors, business representatives, legal team members, corporate communications, third-party vendors, and government representatives.

Note: Many organizations will use a Responsible, Accountable, Consulted, and Informed (RACI) chart to identify roles and clarify responsibilities in a security incident response.

Key takeaways

As a cloud security professional, you'll likely assist in incident response efforts. Understanding the processes behind incident management can help prepare you to respond to security incidents in the cloud and help minimize data loss and damage to your organization's critical systems.