

Incident Management

Incident management is a set of defined processes to identify, analyze, prioritize, and resolve security incidents to restore the system to normal service operations as soon as possible, and prevent recurrence of the incident. It involves not only responding to incidents but also triggering alerts to prevent potential risks and threats. A security administrator must identify software that is open to attacks before someone takes advantage of the vulnerabilities.

Incident management includes the following:

- Vulnerability analysis
- Artifact analysis
- Security awareness training
- Intrusion detection
- Public or technology monitoring

The incident management process is designed to:

- Improve service quality
- Resolve problems proactively
- Reduce the impact of incidents on an organization or its business
- Meet service availability requirements
- Increase staff efficiency and productivity
- Improve user and customer satisfaction
- Assist in handling future incidents

Conducting training sessions to spread awareness among users is an important part of incident management. Such sessions help end-users to recognize suspicious events or incidents easily and report an attacker's behavior to the appropriate authority.

The following people perform incident management activities:

- Human resources personnel take steps to fire employees suspected of harmful computer activities.
- The legal counsel sets the rules and regulations in an organization. These rules can influence the internal security policies and practices of the organization in case an insider or an attacker uses the organization's system for harmful or malicious activities.
- The firewall manager keeps filters in place. These filters are frequently where denial-of-service attacks are made.
- An outsourced service provider repairs systems infected by viruses and malware.

Incident response is one of the functions performed in incident handling. In turn, incident handling is one of the services provided as part of incident management. The following diagram illustrates the relationship between incident response, incident handling, and incident management.

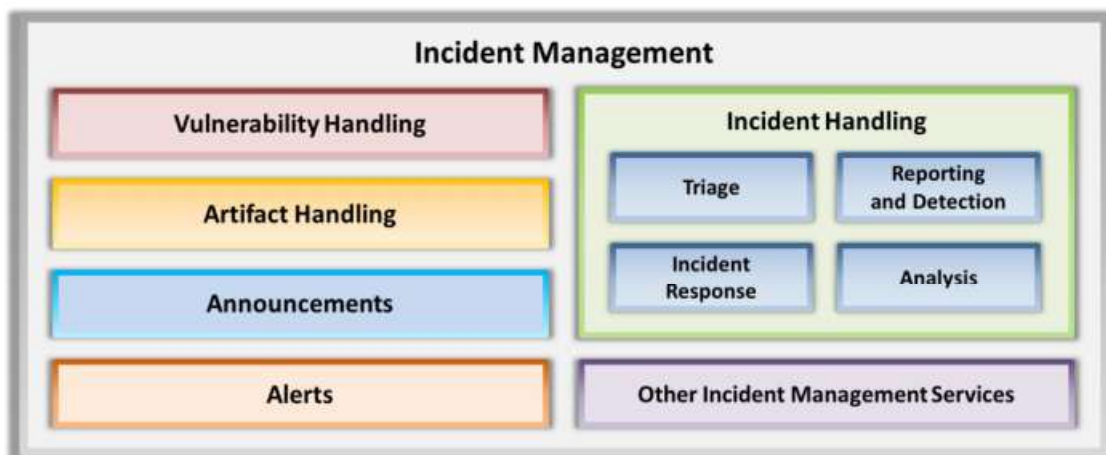



Figure 1.4: Block Diagram of Incident Management

Incident Handling and Response



■ Incident handling and response (IH&R) is the **process of taking organized and careful steps** when reacting to a security incident or cyberattack

Steps involved in the IH&R process:

| | |
|---|--|
| 1 Preparation | 7 Eradication |
| 2 Incident Recording and Assignment | 8 Recovery |
| 3 Incident Triage | 9 Post-Incident Activities <ul style="list-style-type: none">• Incident Documentation• Incident Impact Assessment• Review and Revise Policies• Close the Investigation• Incident Disclosure |
| 4 Notification | |
| 5 Containment | |
| 6 Evidence Gathering and Forensic Analysis | |

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

Incident Handling and Response

Incident handling and response (IH&R) is the process of taking organized and careful steps when reacting to a security incident or cyberattack. It is a set of procedures, actions, and measures taken against an unexpected event occurrence. It involves logging, recording, and resolving incidents that take place in the organization. It notes the incident, when it occurred, its impact, and its cause. It is the practice of managing the incident response processes, such as preparation, detection, containment, eradication, and recovery, to overcome the impact of an incident quickly and efficiently. IH&R processes are important to provide a focused approach for restoring normal business operations as quickly as possible after an incident and with a minimal impact on the business.

The IH&R process involves defining user policies, developing protocols, building incident response teams, auditing organizational assets, planning incident response procedures, obtaining management approval, incident reporting, prioritization, and managing response. It also includes establishing proper communication between the individuals responding to an incident and guiding them to detect, analyze, contain, recover, and prevent incidents.

Discussed below are the steps involved in the IH&R process:

- **Step 1: Preparation**

The preparation phase includes performing an audit of resources and assets to determine the purpose of security and define the rules, policies, and procedures that drive the IH&R process. It also includes building and training an incident response team, defining incident readiness procedures, and gathering required tools as well as training the employees to secure their systems and accounts.

- **Step 2: Incident Recording and Assignment**

In this phase, the initial reporting and recording of the incident take place. This phase handles identifying an incident and defining proper incident communication plans for the employees and also includes communication methods that involve informing IT support personnel or submitting an appropriate ticket.

- **Step 3: Incident Triage**

In this phase, the identified security incidents are analyzed, validated, categorized, and prioritized. The IH&R team further analyzes the compromised device to find incident details such as the type of attack, its severity, target, impact, and method of propagation, and any vulnerabilities it exploited.

- **Step 4: Notification**

In the notification phase, the IH&R team informs various stakeholders, including management, third-party vendors, and clients, about the identified incident.

- **Step 5: Containment**

This phase helps to prevent the spread of infection to other organizational assets, preventing additional damage.

- **Step 6: Evidence Gathering and Forensic Analysis**

In this phase, the IH&R team accumulates all possible evidence related to the incident and submits it to the forensic department for investigation. Forensic analysis of an incident reveals details such as the method of attack, vulnerabilities exploited, security mechanisms averted, network devices infected, and applications compromised.

- **Step 7: Eradication**

In the eradication phase, the IH&R team removes or eliminates the root cause of the incident and closes all the attack vectors to prevent similar incidents in the future.

- **Step 8: Recovery**

After eliminating the causes for the incidents, the IH&R team restores the affected systems, services, resources, and data through recovery. It is the responsibility of the incident response team to ensure that the incident causes no disruption to the services or business of the organization.

- **Step 9: Post-Incident Activities**

Once the process is complete, the security incident requires additional review and analysis before closing the matter. Conducting a final review is an important step in the IH&R process that includes:

- Incident documentation
- Incident impact assessment
- Reviewing and revising policies
- Closing the investigation
- Incident disclosure