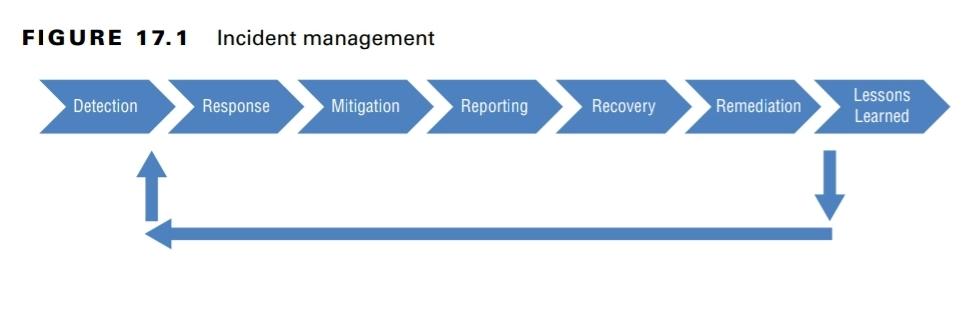
**Chapter 17: Preventing and Responding to Incidents**

In general, an incident is any event that has a negative effect on the confidentiality, integrity, or availability of an organization’s assets.

Incident management is an ongoing activity, and the results of the lessons learned stage are used to improve detection methods or help prevent a repeated incident.

Steps - (DR MR RRL)



Detection is the first step and can come from automated tools or employee observations. Personnel investigate alerts to determine if an actual incident has occurred and if so, the next step is a response. Containment of the incident is essential during the mitigation stage. It’s also important to protect any evidence during all stages of incident management. Reporting may be required based on governing laws or an organization’s security policy. In the recovery stage, the system is restored to full operation, and it’s important to ensure that it is restored to at least as secure a state as it was before the attack. The remediation stage includes a root cause analysis and will often include recommendations to prevent a re-occurrence. Last, the lessons learned stage examines the incident and the response to determine if there are any lessons to be learned.

A preventive control attempts to thwart or stop unwanted or unauthorized activity from occurring.

A detective control attempts to discover or detect unwanted or unauthorized activity. Detective controls operate after the fact and can discover the activity only after it has occurred.

The computers in a botnet are like robots (referred to as bots and sometimes zombies). Multiple bots in a network form a botnet and will do whatever attackers instruct them to do. Computers are typically joined to a botnet after being infected with some type of malicious code or malicious software.

Denial-of-service (DoS) attacks prevent a system from processing or responding to legitimate traffic or requests for resources and objects. A DoS attack comes from a single system and targets a single system.

Another form of DoS attack is a distributed denial-of-service (DDoS) attack. A DDoS attack occurs when multiple systems attack a single system at the same time.

A distributed reflective denial-of-service (DRDoS) attack is a variant of a DoS. It uses a reflected approach to an attack. In other words, it doesn’t attack the victim directly but instead manipulates traffic or a network service so that the attacks are reflected back to the victim from other sources.

In a SYN flood attack, the attackers send multiple SYN packets but never complete the connection with an ACK. An attacker will send hundreds or thousands of SYN packets to the victim. Each incomplete session consumes resources, and at some point, the victim becomes overwhelmed and is not able to respond to legitimate requests.

In TCP Reset Attack, attackers spoof the source IP address in a RST packet and disconnect active sessions between the two systems. The systems then need to reestablish the session. This is primarily a threat for systems that need persistent sessions to maintain data with other systems. When the session is reestablished, they need to re-create the data, so it’s much more involved than just sending three packets back and forth to establish the session.

A smurf attack is a type of ping flood attack, which floods the victim with Internet Control Message Protocol (ICMP) echo packets instead of with TCP SYN packets.

Fraggle attacks are similar to smurf attacks. However, instead of using ICMP, a fraggle attack uses UDP packets.

A ping flood attack floods a victim with ping requests. This can be very effective when launched by zombies within a botnet as a DDoS attack.

A zero-day exploit refers to an attack on a system exploiting a vulnerability that is unknown to others.

Employee sabotage is a criminal act of destruction or disruption committed against an organization by an employee.

An intrusion occurs when an attacker can bypass or thwart security mechanisms and access an organization’s resources.

Intrusion detection is a specific form of monitoring that monitors events (often in real time) to detect abnormal activity indicating a potential incident or intrusion.

An intrusion detection system (IDS) automates the inspection of logs and real-time system events to detect intrusion attempts and system failures.

The most common method of intrusion detection is knowledge-based detection (also called signature-based detection or pattern-matching detection). It uses a database of known attacks developed by the IDS vendor.

The second detection type is behavior-based detection (also called statistical intrusion detection, anomaly detection, and heuristics-based detection). Behavior-based detection starts by creating a baseline of normal activities and events on the system. Once it has accumulated enough baseline data to determine normal activity, it can detect abnormal activity that may indicate a malicious intrusion or event.

When the IDS detects an event, it triggers an alarm or alert. It can then respond using a passive or active method. A passive response logs the event and sends a notification. An active response changes the environment to block the activity in addition to logging and sending a notification.

An intrusion prevention system (IPS) is a special type of active IDS that attempts to detect and block attacks before they reach target systems. IPS is always placed inline to the traffic to be able to analyze and block traffic in real time before it reaches the target system. Because an IPS includes detection capabilities, you’ll often see them referred to as intrusion detection and prevention systems (IDPSs).

If an active IDS is placed inline with the traffic, it is an IPS. If it is not placed inline with the traffic, it isn’t a true IPS because it can only block the traffic once it has analyzed the logs and detected the incident. By this time the incident has either happened or is in progress.

A host based IDS (HIDS) monitors activity on a single computer.

An NIDS monitors and evaluates network activity to detect attacks or event anomalies.

Aside from IDS and IPS, administrators typically implement additional security controls to protect their networks.

* Honeypots are individual computers created as a trap or a decoy for intruders or insider threats. A honeynet is two or more networked honeypots used together to simulate a network. They look and act like legitimate systems, but they do not host data of any real value for an attacker. The goal is to grab intruders’ attention and keep them away from the legitimate network.
* Warning banners inform users and intruders about basic security policy guidelines. In most situations, the wording in banners is important from a legal standpoint because these banners can legally bind users to a permissible set of actions, behaviors, and processes.
* The most important protection against malicious code is the use of antimalware software with up-to-date signature files and heuristic capabilities.
* Administrators today use a allow list (for whitelisting) and deny list or block list (for blacklisting) for applications. Using these lists is an effective preventive measure that blocks users from running unauthorized applications.
* Firewalls are used to prevent network attacks.
* Sandboxing is used to test unknown applications. If the application displays suspicious characteristics, the sandboxing technique prevents the application from infecting other applications or the operating system.

Logging is the process of recording information about events to a log file or database. Logging captures events, changes, messages, and other data describing activities on a system.

Audit trails are records created when information about events and occurrences is stored in one or more databases or log files.

A SIEM collects data from dissimilar devices. It includes a correlation and aggregation feature converting this data into useful information. Advanced analytic tools within the SIEM can analyze the data and raise alerts and/or trigger responses based on preconfigured rules.

Sampling, or data extraction, is the process of extracting specific elements from a large

collection of data to construct a meaningful representation or summary of the whole.

Clipping is a form of nonstatistical sampling. It selects only events that exceed a clipping level, which is a predefined threshold for the event. The system ignores events until they

reach this threshold.

Log management refers to all the methods used to collect, process, and protect log entries.

Security orchestration, automation, and response (SOAR) refers to a group of technologies that allow organizations to respond to some incidents automatically.

In the context of incident response, a playbook is a document that defines how to verify an incident and what actions to be taken when the incident is identified. A runbook implements the playbook data (actions) into an automated tool.

Threat hunting is the process of actively searching for infections or attacks within a network. Threat intelligence refers to the actionable intelligence created after analyzing incoming data, such as threat feeds.