LECTURE 7: SECURITY INCIDENT RESPONSE

INTRODUCTION

- **An event** is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.

- **A security incident** refers to any adverse event or series of events that can compromise the confidentiality, integrity, or availability of an organization's information or information systems. Security incidents can vary widely in scope and impact. Examples of security incidents are:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

SECURITY INCIDENT RESPONSE TEAM

SECURITY INCIDENT RESPONSE TEAM

Possible structures for security incident response team include the following:

- **Central Incident Response Team**. A single incident response team handles incidents throughout the organization. This model is effective for small organizations and for organizations with minimal geographic diversity in terms of computing resources.
- **Distributed Incident Response Teams.** The organization has multiple incident response teams, each responsible for a particular logical or physical segment of the organization. This model is effective for large organizations (e.g., one team per division) and for organizations with major computing resources at distant locations (e.g., one team per geographic region, one team per major facility).

However, the teams should be part of a single coordinated entity so that the incident response process is consistent across the organization and information is shared among teams. This is particularly important because multiple teams may see components of the same incident or may handle similar incidents.

SECURITY INCIDENT RESPONSE TEAM

Security incident response teams can also use any of three staffing models:

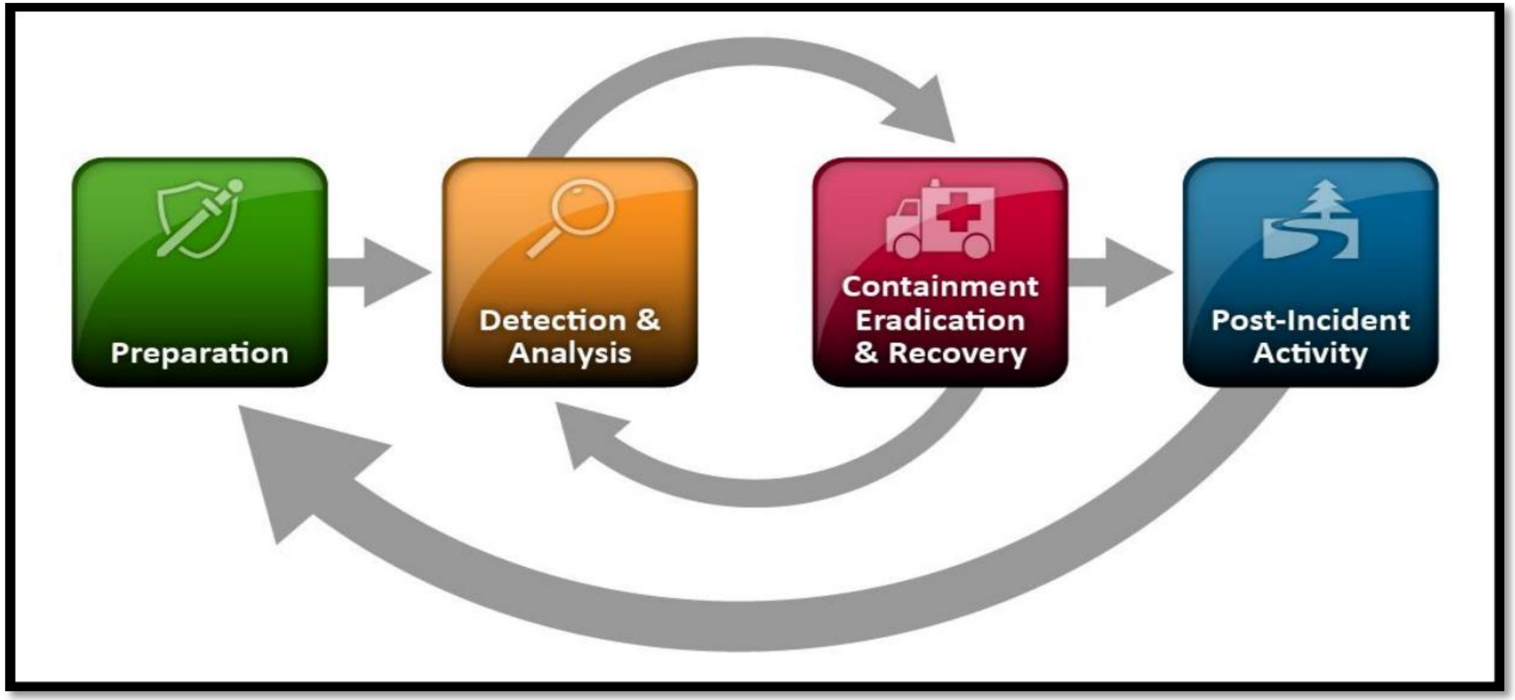
- **Employees**: The organization performs all of its incident response work, with limited technical and administrative support from contractors.
- **Partially Outsourced**: The organization outsources portions of its incident response work.
- **Fully Outsourced**: The organization completely outsources its incident response work, typically to an onsite contractor. This model is most likely to be used when the organization needs a full-time, onsite incident response team but does not have enough available, qualified employees. It is assumed that the organization will have employees supervising and overseeing the outsourcer’s work.

HANDLING SECURITY INCIDENT

Within cybersecurity, incident response (IR) is the process of handling and mitigating cyber attacks or security breaches. Above all, it involves identifying, analyzing, and responding to incidents to prevent future threats and minimize damage.

The incident response process has several phases.

- Preparation
- Detection and Analysis
- Containment Eradication and Recovery
- Post-incident activity.



security incident response life cycle

HANDLING SECURITY INCIDENT : PREPARATION

In this phase, the organization creates an incident management plan that can detect an incident in the organization’s environment. The preparation step involves, for example, identifying different malware attacks and determining what their impact on systems would be. It also involves ensuring that an organization has the tools to respond to an incident and the appropriate security measures in place to stop an incident from happening in the first place.

HANDLING SECURITY INCIDENT : DETECTION AND ANALYSIS

In this phase the incident response team should work quickly to identify, investigate, and assess suspicious activity or incidents within an organization's network or systems. When the team believes that an incident has occurred, the team should rapidly perform an initial analysis to determine the incident’s scope, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited).

The initial analysis should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident.

HANDLING SECURITY INCIDENT : CONTAINMENT ERADICATION AND RECOVERY

This phase encompasses three steps:

- **Containment:** In this step, all possible methods are used to prevent the spread of malware or viruses. Actions might include disconnecting systems from networks, quarantining infected systems , or blocking traffic to and from known malicious IP addresses.
- **Eradication:** After containing the security issue in question, the malicious code or software needs to be eradicated from the environment. This might involve using antivirus tools or manual removal techniques. It will also include ensuring that all security software is up to date in order to prevent any future incidents.
- **Recovery:** After eliminating the malware, restoring all systems to their pre-incident state is essential. This might involve restoring data from backups, rebuilding infected systems, and re-enabling disabled accounts.

HANDLING SECURITY INCIDENT : POST-INCIDENT ACTIVITY

The goal of this phase, also known as a “Lessons Learned”, is to understand precisely what occurred, why it happened, and how to prevent it from happening again. This review goes beyond technical aspects; it may also involve changes to policies or infrastructure.

The purpose of this phase is not to assign blame (though this can sometimes occur) but rather to reduce the likelihood of future incidents, where It's common for attackers to target the same system again or use similar methods to compromise other resources within the organization. Another goal is to scope the damage; a comprehensive review helps assess the entire response process, minimizing the impact and ensuring more effective recovery. These reviews aim to strengthen cybersecurity defenses, close gaps, and ultimately mature the organization's security posture to handle future incidents better

HANDLING SECURITY INCIDENT : POST-INCIDENT ACTIVITY

A central part of the incident response methodology is learning from previous incidents to improve the process.

we should ask, investigate and document the answers to the following questions:

- What happened, and at what times?
- How well did the incident response team deal with the incident? Were processes followed, and were they sufficient?
- What information was needed sooner?
- Were any wrong actions taken that caused damage or inhibited recovery?
- What could staff do differently next time if the same incident occurred?
- Could staff have shared information better with other organizations or other departments?
- Have we learned ways to prevent similar incidents in the future?
- Have we discovered new precursors or indicators of similar incidents to watch for in the future?
- What additional tools or resources are needed to help prevent or mitigate similar incidents?

we use our findings to improve the process, adjust your incident response policy, plan, and procedures, and feed the new data into the preparation stage of your incident response process.