Incident Responses

Lecture – Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment - please engage accordingly.
- No question is daft or silly - **ask them!**
- There are Q/A sessions midway and at the end of the session, should you wish to ask any follow-up questions.
- You can also submit questions here: hyperiondev.com/sbc4-cs-questions
- For all non-academic questions, please submit a query: www.hyperiondev.com/support
- Report a safeguarding incident: hyperiondev.com/safeguardreporting
- We would love your feedback on lectures: https://hyperionde.wufoo.com/forms/zsgv4m40ui4i0g/

Previously:

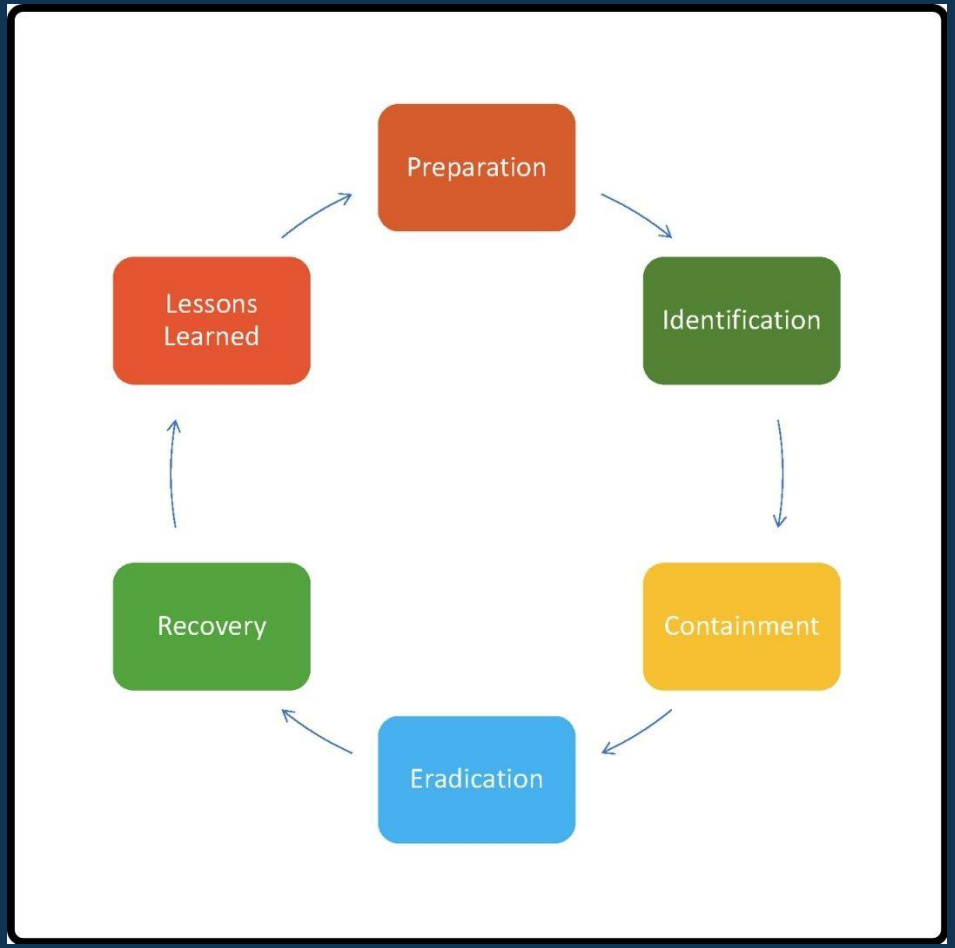
- What Governance + Compliance is
- Principles for Security Governance
- Compliance Frameworks
- Benefits/Considerations

Objectives

- Understand the process of incident response.

Incident Response Overview

According to IBM Incident response (sometimes called cybersecurity incident response) refers to an organization's processes and technologies for detecting and responding to cyberthreats, security breaches or cyberattacks. The goal of incident response is to prevent cyber attacks before they happen, and to minimize the cost and business disruption resulting from any cyber attacks that occur.



https://external-content.duckduckgo.com/iu/?u=https%3A%2F%2Fisea.utoronto.ca%2Fwp-content%2Fuploads%2F2021%2F05%2FIncident-Response-Graphic.jpg&f=1&nofb=1&ipt=083605c369c8773665efb44bca0918eeed3aef4bf5b4687582c68fb577aad96e&ipo=images

Incident Response Process (I)

1 - Preparation: This first stage of incident response is ongoing to ensure that the CSIRT always has the best policies and resources available to respond to incidents as quickly as possible with the least amount of business disruption.

- The CSIRT regularly assesses risks to identify network vulnerabilities, categorizes the different security incidents that could endanger the network, and assigns a priority to each type based on the likelihood that it will have an adverse effect on the organization. The CSIRT may update current incident response plans or create new ones in light of this risk assessment.

2 - Detection and Analysis: Members of the security team keep an eye on the network during this stage for any unusual activity or potential threats. They examine information, notifications, and alerts obtained from device logs and from various security tools (firewalls, antivirus software), which are installed on the network. They remove false positives and rank the actual alerts according to their seriousness.

Incident Response Process (II)

3 - Containment: The incident response team acts to prevent the breach from causing additional harm to the network. Activities for containment can be divided into two groups:

- Short-term containment: Aims to stop the current threat from spreading by isolating the affected systems, i.e taking infected devices offline.

- Long-term containment strategies concentrate on defending unaffected systems by enclosing them in tighter security perimeters, like separating network segments for sensitive databases from the rest of the system

In order to prevent further data loss and to gather forensic evidence of the incident for later investigation, the CSIRT may also at this point create backups of both affected and unaffected systems.

Incident Response Process (III)

- To assist security teams in monitoring and analyzing security events in real time and automating incident detection and response procedures, the majority of organizations use one or more security solutions today, such as SIEM (security information and event management) and EDR (endpoint detection and response).

- During this phase, the communication plan is also used. Before moving on to the next phase of the incident response process, the CSIRT will notify the appropriate personnel once they have identified the type of threat or breach they are dealing with.

4 - Eradication: The team then moves on to complete remediation and removal of the threat from the system once it has been contained. In order to do this, the threat must be actively eliminated (e.g., by destroying malware or kicking an unauthorized or rogue user off the network). Affected and unaffected systems must also be examined to make sure no evidence of the breach is still present.

Incident Response Process (IV)

5 - Recovery: The CSIRT gathers evidence of the breach and records the steps it takes to contain and eliminate the threat during each stage of the incident response process. The CSIRT now examines this data to comprehend the incident more fully. In order to prevent similar incidents from happening in the future, the CSIRT aims to identify the attack's primary cause, pinpoint how it successfully breached the network, and fix any vulnerabilities.

6 - Post-incident review: The CSIRT gathers proof of the breach during each stage of the incident response process and records the actions it takes to eliminate the threat. At this point, the CSIRT examines this data to gain a better understanding of the incident. The CSIRT works to identify the attack's underlying causes, show how it successfully broke into the network, and fix any vulnerabilities to prevent similar incidents from happening in the future.

Incident Response Process (V)

The CSIRT also reviews what went well and looks for opportunities to improve systems, tools, and processes to strengthen incident response initiatives against future attacks. Depending on the circumstances of the breach, law enforcement may also be involved in the post-incident investigation

Questions and Answers

https://cdn.ttgtmedia.com/rms/onlineImages/disaster_recovery-incident_response_planning.jpg

Careers

Incident responders and handlers: Identify, assess, and respond to security incidents. To reduce risks and the effects of incidents, they look into and contain security breaches, create incident response plans, and work with various stakeholders.

Threat Intelligence Analysts: These professionals gather and examine data on potential threats, weaknesses, and new developments in the field of cyber security. They give incident response teams useful information that enables them to proactively identify and address potential risks.

Security Operations Center (SOC) Analyst: SOC analysts keep an eye out for security-related incidents on networks, systems, and applications. They investigate security alerts, analyze the information, and take the appropriate steps to deal with incidents. Analysis of digital evidence pertaining to security incidents and the identification and remediation of security breaches in rea are crucial tasks performed by SOC analysts.

Wrapping Up

We covered the essential elements of effectively managing and mitigating security incidents in this lecture on incident response.

We looked at the incident response lifecycle, which entails planning, identification and analysis, elimination and containment, recovery and restoration, and learning from mistakes.

Organizations can lessen the impact of security incidents, safeguard crucial assets, and resume normal operations by putting in place a strong incident response plan.

To ensure effective incident management, it is crucial to constantly stay up to date on incident response frameworks, methodologies, and best practices.

Next up

- Recap Lecture

Questions and Answers

Hyperiondev

Thank you for joining us

1. Take regular breaks
2. Stay hydrated
3. Avoid prolonged screen time
4. Practice good posture
5. Get regular exercise

"With great power comes great responsibility"