**LEMUEL OKECHUKWU**

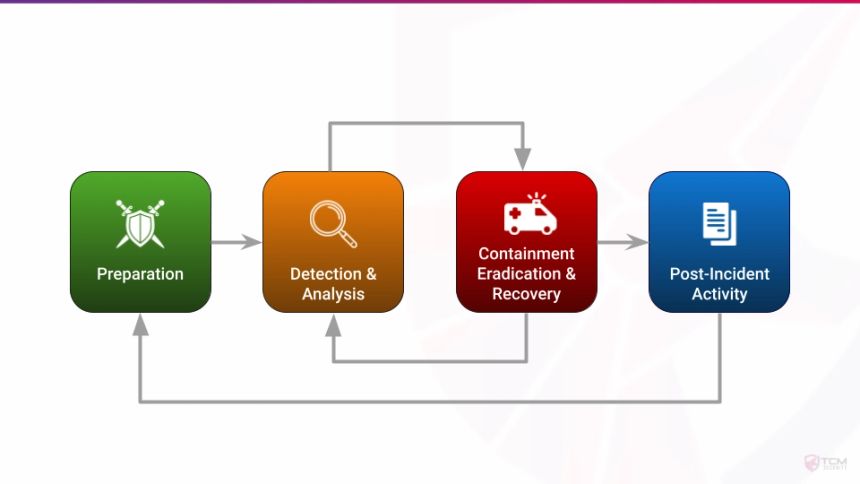
**VEPH/20B/CY082**

**TASK 35A**

**THREAT HUNTING GROUND: INCIDENT RESPONSE LIFE CYCLE**

**TASK 35A:**

* In the context of cybersecurity operations, define Incident Response (IR) and provide a detailed explanation of the standard phases within the NIST Incident Response lifecycle.
* Provide a detailed explanation of the Cyber Kill Chain framework and discuss how it models the stages of a targeted cyber-attack from reconnaissance to data exfiltration

[](https://tcm-sec.com/nist-guidelines-for-incident-response-best-practices/)

Cybersecurity incidents have become a necessary evil for businesses that want to scale faster. There were[1,767 data breaches](https://www.securitymagazine.com/articles/95793-data-breaches-in-the-first-half-of-2021-exposed-188-billion-records) reported in the first half of 2021, exposing over 18.8 billion records. This spike is a stark increase from the same period a year earlier when malicious actors accessed 4.1 billion records.

Today, hackers deploy ever-changing tactics and sophisticated technology to steal valuable data from businesses. These organizations are left struggling to fend off cyber threats. No matter what they do, hackers are always a step ahead, as substantiated by the fact that enterprises with robust security measures often deal with data breaches. The NIST (National Institute of Standards and Technology) serves as a medium to investigate, checkmate and prevent such attacks through an Incident response module.

**What Is the NIST Incident Response Life Cycle:** is a repeatable process that guides organizations in handling cybersecurity incidents efficiently and effectively. By breaking incident management into four distinct phases, the life cycle ensures a consistent, systematic approach to mitigating threats.Its purpose is to minimize damage from incidents like data breaches, ransomware attacks, or malware infections. It’s widely adopted across industries by organizations that prioritize robust cybersecurity management to protect sensitive data and critical infrastructure.

**The NIST Incident Response Life Cycle is composed of four distinct phases, each critical to effective incident management.**

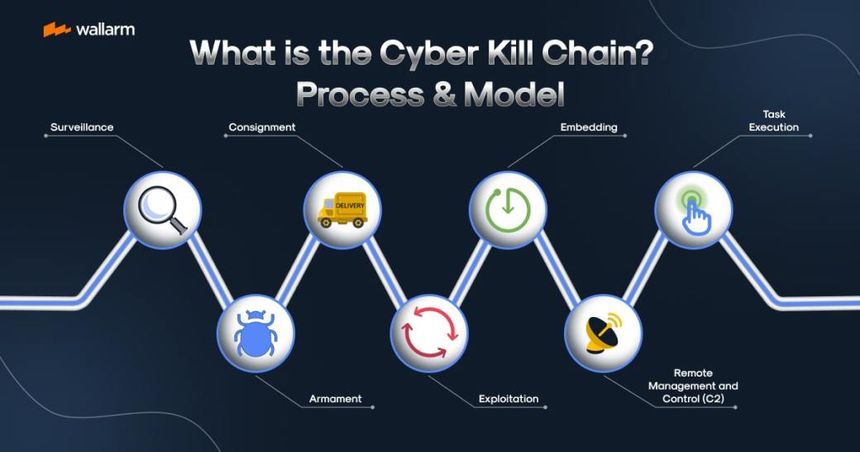
|  |  |  |
| --- | --- | --- |
| **Phase** | **Objective** | **Key Actions** |
| **Preparation** | **Establish incident response capabilities before a cybersecurity event occurs.** | **• Develop an incident response policy and incident handling procedures. • Define roles and responsibilities within the incident response team. • Conduct regular employee security training and tabletop exercises. • Deploy security tools like firewalls, endpoint protection, and SIEM solutions.** |
| **Detection and Analysis** | **Identify and evaluate potential security incidents.** | **• Monitor system logs, network traffic, and security alerts. • Use automated threat detection tools and threat intelligence platforms. • Analyze indicators of compromise (IOCs) and suspicious activity. • Classify incidents by severity level and business impact.** |
| **Containment, Eradication, and Recovery** | **Limit the spread of the incident, eliminate threats, and restore normal operations.** | **• Short-Term Containment: Isolate affected systems to prevent further damage. • Long-Term Containment: Apply patches, disable compromised accounts, and strengthen security controls. • Eradication: Remove malicious files, malware, or intruders from the system. • Recovery: Restore affected systems from backups and validate system functionality, and conduct post-recovery assessments to ensure normal operations.** |
| **Post-Incident Activity** | **Learn from the incident to improve future response efforts.** | **• Conduct root-cause analysis to identify how the incident occurred. • Review incident handling procedures and update response plans accordingly. • Generate a post-incident report with findings and recommended improvements. • Share lessons learned with the incident response team and relevant stakeholders.** |

**How the Incident Response Life Cycle Aligns with the NIST CSF**

The NIST Incident Response Life Cycle is deeply integrated with the [NIST Cybersecurity Framework (CSF)](https://cynomi.com/nist/nist-cybersecurity-framework-csf/), supporting its core functions:

* Detect (DE): Monitoring systems for anomalies and generating alerts support the Detection and Analysis phase.
* Respond (RS): Activities like containment and eradication align directly with the Respond function in NIST CSF.
* Recover (RC): Recovery efforts ensure continuity and align with the Recover function, addressing operational resilience.
* Identify (ID): The Preparation phase incorporates risk assessments and audits, aligning with the Identify function.

The NIST Incident Response Life Cycle provides organizations with a structured approach to managing cybersecurity incidents effectively.

[](https://lab.wallarm.com/what/what-is-the-cyber-kill-chain-process-model/)

**Cyber Kill Chain Stages**

The Cyber Kill Chain framework, developed by Lockheed Martin, is a security model that outlines the stages of a targeted cyber-attack from reconnaissance to data exfiltration. This framework helps security professionals understand the sequence of events during a cyber-attack and develop strategies to detect and prevent these attacks.

**The Cyber Kill Chain consists of seven stages:**

1. **Reconnaissance:** The attacker gathers information about the target to identify potential vulnerabilities. This stage involves both passive and active reconnaissance methods.
2. **Weaponization:** Once the attacker identifies a vulnerability, they create a tailored piece of malicious code, such as a virus or worm, to exploit it.
3. **Delivery:** The attacker delivers the malicious payload to the target system, often through email attachments, links, or other means.
4. **Exploitation:** The malicious code is executed, exploiting the identified vulnerability to gain unauthorized access to the target system.
5. **Installation:** After gaining access, the attacker installs additional tools or malware to maintain control over the compromised system.
6. **Command and Control (C2):** The attacker establishes a connection with the compromised system to issue commands and control the malware installed.
7. **Actions on Objectives:** Finally, the attacker achieves their goal, which could be stealing sensitive data, disrupting services, or causing other harm.

By understanding and monitoring these stages, organizations can implement defensive measures to detect and mitigate attacks at various points along the chain