CYBER KILL CHAIN

VAISHALI SHISHODIA

The cyber kill chain is a model that breaks down a cyberattack into distinct stages, from initial reconnaissance to achieving the attacker's objectives, helping security teams understand and defend against sophisticated attacks. It is developed by Lockheed Martin that outlines the different stages of a cyberattack. It helps cybersecurity professionals detect, analyze, and mitigate threats. The framework consists of **seven stages**, and I'll explain each with examples.

1. Reconnaissance (Information Gathering)

- The attacker gathers information about the target (organization, individual, or system).
- They look for vulnerabilities, employee details, email addresses, open ports, and technologies in use.
- This step helps attackers plan the next phase of the attack.

2. Weaponization (Preparing the Attack)

- The attacker creates a malicious payload, such as a virus, trojan, or ransomware.
- They develop a **zero-day exploit** or customize existing malware.
- The payload is designed to exploit the target's vulnerabilities.

3. Delivery (Sending the Payload)

- The attacker delivers the malicious file, link, or exploit to the target.
- Common methods include:
    - **Phishing emails**
    - **Malicious websites**
    - **Drive-by downloads**
    - **USB drops**

4. Exploitation (Executing the Attack)

- The attacker exploits a vulnerability in the system or tricks the user into executing the malicious payload.
- If successful, this stage allows attackers to install malware, steal credentials, or escalate privileges.

5. Installation (Establishing Foothold)

- The attacker installs malware or a backdoor on the victim's system.
- This allows **persistent access** to the network.

6. Command & Control (C2)

- The compromised system connects to the attacker's **Command & Control (C2) server**.
- The attacker can now send remote commands, steal data, or deploy additional malware.

7. Actions on Objectives (Final Attack)

- The attacker **achieves their goal**, which may include:
    - **Data theft** (stealing intellectual property, customer data).
    - **System disruption** (DDoS attacks, shutting down servers).
    - **Ransomware deployment** (demanding payment in exchange for decryption).
    - **Espionage or sabotage** (modifying or deleting critical files).

How to Defend Against the Cyber Kill Chain?

Organizations can break the kill chain at multiple stages:
Reconnaissance → Use threat intelligence and limit OSINT exposure.
Weaponization & Delivery → Train employees on phishing, use email filters, and sandbox attachments.
Exploitation → Keep software updated, apply patches, and enforce strong access controls.
Installation & C2 → Use endpoint detection, block known malicious domains, and monitor network traffic.
Actions on Objectives → Implement data loss prevention (DLP) and regularly back up critical data.

Let's walk through a realistic cyberattack scenario using the Cyber Kill Chain framework and then discuss how a SOC can detect, investigate, and respond to each stage.

Scenario: A Ransomware Attack on a Financial Institution

A **threat actor group** targets a **bank** with the goal of encrypting sensitive customer data and demanding ransom.

Step 1: Reconnaissance (Information Gathering)

Attacker's Actions

- The attackers perform **Google Dorking** to find exposed employee email addresses.
- They use **LinkedIn** to identify bank IT staff and **social engineer** them.
- They scan the bank's network for **open ports and vulnerable services** using tools like **Shodan, Nmap**.

SOC Detection & Response

Detect:

- Monitor **unusual scanning activity** on firewalls and IDS (Intrusion Detection Systems).
- Check for **repeated access to login pages** from unknown locations.

Respond:

- **Harden OSINT exposure** by limiting employee details online.
- Implement **Geo-blocking** and strict firewall rules.
- Conduct **security awareness training** to prevent social engineering.

Step 2: Weaponization (Preparing the Attack)

Attacker's Actions

- The attacker crafts a **malicious Excel file** with an embedded **macro** to deploy ransomware.
- The file is designed to exploit a known **Microsoft Office vulnerability (CVE-2023-23397)**.

SOC Detection & Response

Detect:

- Use **Threat Intelligence Feeds** to identify malware payloads.
- Implement **sandboxing** to analyze unknown files before reaching users.

Respond:

- Ensure **endpoint protection solutions** block macro execution.
- Apply **patch management** to fix vulnerabilities.

Step 3: Delivery (Sending the Payload)

Attacker's Actions

- The attacker sends **spear-phishing emails** to finance department employees, pretending to be from the **CEO**, instructing them to open the attached Excel file.

SOC Detection & Response

Detect:

- Use **email security solutions** to scan for malicious attachments and URLs.
- Deploy **User Behavior Analytics (UBA)** to detect **suspicious email activities**.

Respond:

- Implement **email filtering** to block malicious attachments.
- Train employees on **phishing awareness**.

Step 4: Exploitation (Executing the Attack)

Attacker's Actions

- When the victim opens the **Excel file**, the macro executes and downloads a **ransomware payload** onto the system.

SOC Detection & Response

Detect:

- EDR (Endpoint Detection & Response) detects suspicious macro execution.
- Monitor **PowerShell commands** often used in **fileless attacks**.

Respond:

- **Isolate infected endpoints** to prevent lateral movement.
- **Alert the security team** to investigate the source.

Step 5: Installation (Establishing Foothold)

Attacker's Actions

- The ransomware **establishes persistence** by modifying registry keys and **creating scheduled tasks**.
- A **Trojan backdoor** is installed for remote access.

SOC Detection & Response

Detect:

- SIEM alerts on **unauthorized registry modifications**.
- Monitor **new services/processes** created on endpoints.

Respond:

- Use **HIDS (Host Intrusion Detection System)** to block unauthorized persistence mechanisms.
- Deploy **Network Segmentation** to limit lateral movement.

Step 6: Command & Control (C2)

Attacker's Actions

- The infected system communicates with the **attacker's C2 server**, awaiting further instructions.
- Data **exfiltration begins**, and credentials are stolen.

SOC Detection & Response

Detect:

- SIEM triggers an alert for **outbound traffic to known malicious IPs**.
- Monitor **unusual DNS queries** or traffic spikes.

Respond:

- **Block C2 server IPs** at the firewall.
- Enable **Network Intrusion Prevention System (NIPS)** to disrupt attacker communication.

Step 7: Actions on Objectives (Final Attack Execution)

Attacker's Actions

- The ransomware **encrypts files** and drops a ransom note.
- The attacker demands **Bitcoin payment** to restore data.

SOC Detection & Response

Detect:

- SIEM detects **mass file encryption** events.
- **Backup access logs** are monitored for unusual activity.

Respond:

- **Immediately disconnect infected machines** to prevent further spread.
- Restore from **offline backups**.
- Conduct **Forensic Investigation** to determine root cause and patch vulnerabilities.

Final Thoughts: How SOC Uses the Cyber Kill Chain?

- **Prevention (Reconnaissance & Weaponization)**
  - OSINT monitoring
  - Email security
  - Threat intelligence
- **Detection (Delivery, Exploitation, Installation, C2)**
  - SIEM, EDR alerts
  - IDS/IPS monitoring
  - UBA for anomalous behavior

- **Response (Actions on Objectives)**
  - Incident containment
  - Data recovery & forensics
  - Strengthening security post-attack
