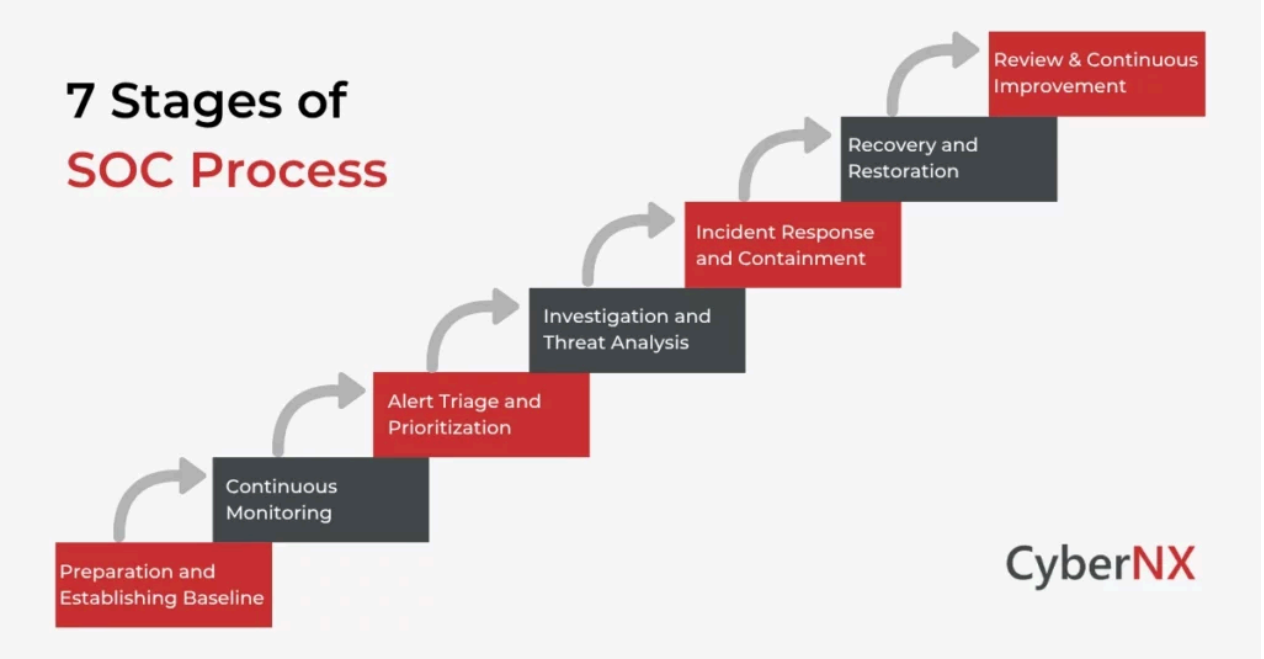
Day 1

Introduction to SOC

1. **What is SOC**?
   - SOC (Security Operations Center) is a team of security professionals that continuously monitor and analyze the security procedures of an organization while responding to incidents, isolates and mitigates security risks.
2. **SOC roles : L1, L2, L3**
   - **Level 1(L1)** :

     The L1 analyst or Tier 1 analyst is responsible for:
     - Monitoring the SIEM (Security Information and Event Management) alerts
     - Managing and configuring security monitoring tools.
     - Prioritizing and triaging alerts or issues to determine whether a real security incident is taking place.
   - **Level 2 (L2)**:
     The L2 analyst or Tier 2 analyst is responsible for:
     - Performing deep analysis of security incidents
     - Defining and executing on strategy for containment, remediation, and recovery.
     - Correlating with threat intelligence to better map out the nature of the attack and compromised systems, networks or data affected.
   - Level 3 (L3):
     The L3 analyst or Tier 3 analyst is responsible for:
     - Proactively hunting for threats that have made their way into the network.
     - Conduct advanced security assessments.
     - Day-to-day vulnerability assessment and reviewing alerts.
3. **SOC processes and workflows**:

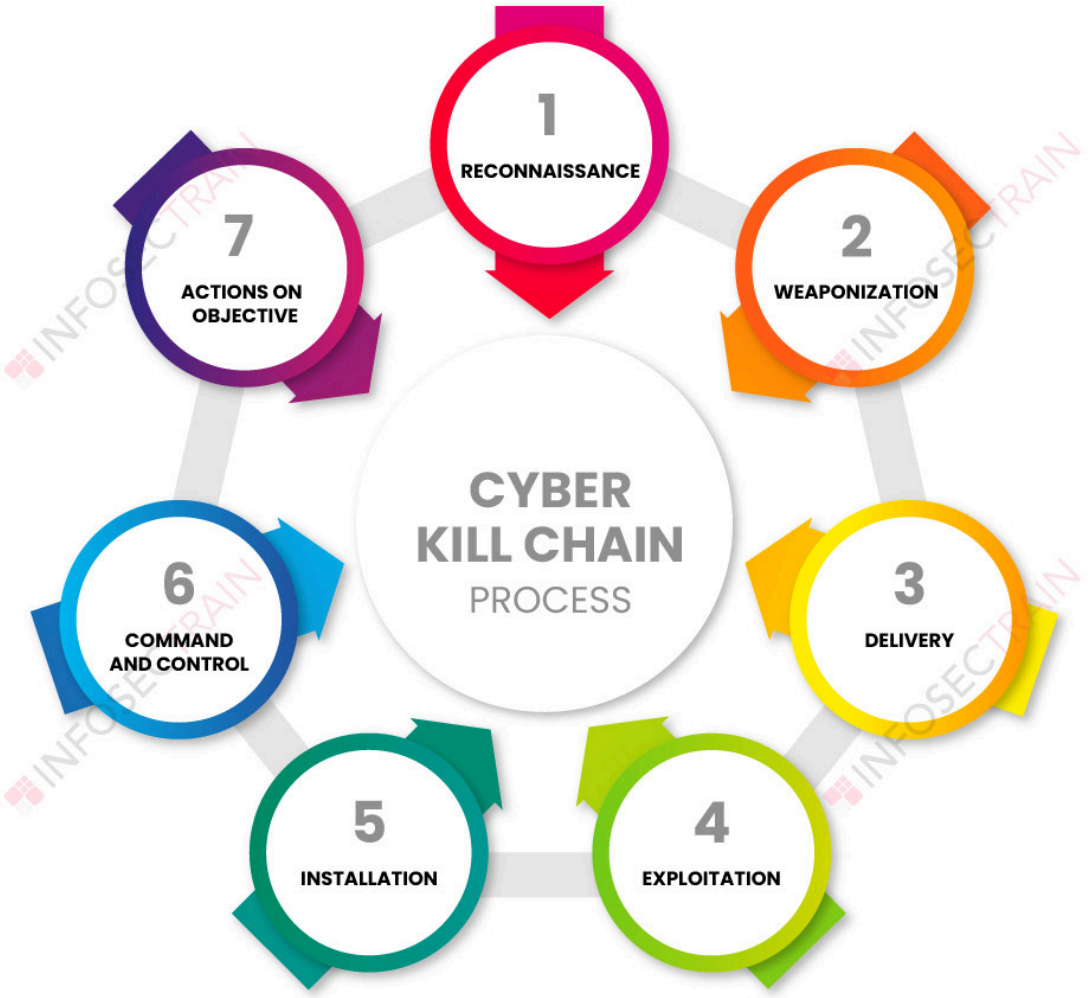


- **SOC L1 workflow**:
    1. Alert Reception
    2. Initial alert review
    3. Correlation with Historical Data
    4. Determine Validity
    5. Documentation
    6. Escalation
- SOC L2 Workflow:
    1. Receive Escalated Incident
    2. Detailed Analysis
    3. Contextual Analysis
    4. Threat Intel
    5. Additional Checks
    6. Documentation
    7. Initial Response
    8. Escalation
- SOC L3 workflow:
    1. Receive Escalated Incident
    2. Advanced Threat analysis
    3. Exploit and root cause analysis
    4. Comprehensive documentation
    5. Strategic Recommendations
    6. Coordination with the SOC Manager
    7. Post-Incident Review
- SOC Manager workflow
    1. Incident Oversight
    2. Coordination and Communication

3. Resource allocation
4. Post-Incident Review
5. Process Improvement

Cyber Kill Chain & MITRE ATT&CK

- **Attack lifecycle**:



1. **Reconnaissance:**
   Scanning the environment for potential vulnerabilities or harvesting info from social media.
2. **Weaponization**:
   Pairing malicious code with an exploit to create a weapon.
3. **Delivery:**
   Delivering the weapon/malware to the target (e.g. via email, USB, website, etc.)
4. **Exploitation**:
   The delivered malware is triggered upon user interaction. It exploits the vulnerability.
5. **Installation**:
   The weapon install malware on the system.
6. **Command and Control**:
   A command channel for remote manipulation of the victim.

7. **Action on objectives**:
   With hands-on access the attacker can achieve their objective.

- **Mapping alerts to ATT&CK:**
  1. **Initial Access (TA0001):**
     - Represents how the attacker first gains access or compromises your environment.
     - Example Alert:
       “Repeated failed authentication attempts followed by a successful login from IP 185.220.X.X”. Mapping T1078 (Valid Accounts) Attackers using compromised credentials.
  2. **Execution (TA0002)**:
     - Execution shows how adversaries run malicious code.
     - Example:
       Windows Events ID 4688 (Process creation) showing cmd.exe spawning powershell.exe with encoded commands, or scheduled tasks executed at suspicious times.
  3. **Persistence (TA0003)**:
     - Allows attackers to maintain access across reboots and credential changes.
     - Common artifacts:
       Registry Run Keys, scheduled tasks, WMI event subscriptions, service creation, or DLL sideloading configurations. Your EDR must alert to modifications to HKLM\Software\Microsoft\Windows\CurrentVersion\Run or new services installed outside maintenance windows.
  4. **Privilege Escalation (TA0004):**
     - Attackers exploit misconfigurations, vulnerable drivers, or legitimate Windows features to gain elevated access.
     - Detection Focus:
       Look for processes requesting uncommon privileges, indicators of exploitation tools (such as PsExec, Mimikatz), or unusual parent-child process relationships in which low-privilege processes spawn elevated children.
  5. **Lateral Movement (TA0008)**:
     - The attackers move deeper into the network, e.g. from one compromised system to another.
     - Investigation Pattern:
       Spot authentication logs from the same compromised account accessing multiple systems in quick succession. Often with SYSTEM or administrative processes spawning from remote procedures.

Another way to map the alerts to MITRE ATT&CK is DETT&CK:

DETT&ACK Framework

- **DETT&CK** stands for DEtect, Tactics, Techniques & Combat Threats.
- The purpose of DeTT&CT is to assist blue teams using MITRE ATT&CK to score and compare data log source quality, visibility coverage and detection coverage.
- How does it work?
    - Uses YAML file (simple text files) to keep track of our security status.

Pillar	What it tracks
Data Sources	List of all your logs (e.g., Windows Logs, Firewall, Antivirus). It scores their quality from 0 to 5.
Visibility	Shows if you have the *potential* to see an attack based on the logs you have.
Detection	Shows if you actually have an *alert* or "rule" set up to catch the bad guy.
Groups	Compares your defense against specific hacker groups (e.g., "Can we stop APT29?").

DETT&CK framework answers these 3 questions:

References:

Image source: https://www.infosectrain.com/blog/what-is-the-cyber-kill-chain-process