Security Operations Center (SOC) Week2 – Theory

Alert Priority Levels

- **Priority Definitions**:
    - **Critical** → Severe impact, needs immediate response.
      Example: Active ransomware encrypting production servers.
    - **High** → Serious, but slightly less urgent.
      Example: Unauthorized admin access detected.
    - **Medium** → Noticeable, but can be scheduled.
      Example: Suspicious login attempts on a test system.
    - **Low** → Minimal impact, monitor only.
      Example: Single failed login attempt.

5. **Asset Criticality** → Production servers > Test VMs.
6. **Exploit Likelihood** → Public exploit available = higher priority.
7. **Business Impact** → Downtime or financial loss raises severity.

- **Scoring Systems**:
    - **CVSS (Common Vulnerability Scoring System)** → Standard for scoring vulnerabilities (0–10 scale).
      Example: Log4Shell (CVE-2021-44228) scored **9.8 (Critical)**.
    - **SOC Tools** (Splunk, SIEMs) → Provide risk-based alert scoring.

2. Incident Classification

- **Incident Categories**:
    - Malware → Ransomware infection
    - Phishing → Credential theft attempt
    - DDoS → Service disruption
    - Insider Threat → Employee exfiltrating data
    - Data Exfiltration → Large outbound data transfer
- **Taxonomy Standards**:
    - **MITRE ATT&CK** → Tactics & techniques (e.g., T1566 – Phishing).
    - **ENISA Incident Taxonomy** → EU standard categories.

- **VERIS Framework** → Vocabulary for consistent incident sharing.

- **Contextual Metadata**:
  - Enrich incidents with details:
    - Affected systems
    - Timestamps
    - Source/destination IPs
    - IOCs (hashes, domains, malware signatures)

3. Basic Incident Response

◆ **Core Concepts**

- **Incident Lifecycle (NIST SP 800-61)**:
  1. **Preparation** → Playbooks, IR team, tools ready.
  2. **Identification** → Triage alerts, confirm incident.
  3. **Containment** → Isolate infected systems.
  4. **Eradication** → Remove malware, disable accounts.
  5. **Recovery** → Restore services, monitor for reinfection.
  6. **Lessons Learned** → Post-incident review, improve defenses.

- **Procedures**:
  - **System Isolation** → Disconnect from network.
  - **Evidence Preservation** → Memory dump, file hashing.
  - **Communication** → Escalation matrix, legal/PR if needed.
  - **SOAR Tools** → Automate workflows (Splunk Phantom, Cortex XSOAR).