**Security Operations Center**

**Alert Priority Levels:**

 Critical: A ransomware encryption attempt on a production database server.

 High: Unauthorized admin login attempts on a web server.

 Medium: A suspicious PowerShell script running on a test machine.

 Low: A routine vulnerability scan generating benign traffic.

**Basic Decision-Making Workflow for Alert Triage:**

**Critical alerts →** Immediate escalation and response.

**High alerts →** Quick investigation with containment readiness.

**Medium alerts →** Scheduled investigation.

**Low alerts →** Monitor and document.

**Incident Classification**

Categorizing incidents based on type, source, and context. The main categories include

**Malware:** Ransomware sample scenario.

**Phishing:** A crafted email attempting credential theft (MITRE ATT&CK T1566).

**DDoS:** Simulated high-volume traffic from multiple IPs.

**Insider Threat:** An employee copying sensitive files to a USB drive.

**Frameworks:**

**MITRE ATT&CK:** Used for mapping techniques (e.g., T1566 – Phishing, T1059 – Command Line Execution).

**ENISA Incident Taxonomy:** For broad classification such as availability, integrity, confidentiality.

**VERIS:** To document metadata such as action, actor, and asset.

Basic Incident Response

**Incident Response Lifecycle based on NIST SP 800-61 and SANS guidelines.**

**Preparation:** Incident playbooks and communication protocols.

**Identification**: Review alerts in a mock SIEM dashboard to detect anomalies.

**Containment**: Simulate isolating a compromised endpoint from the network.

**Eradication**: Removing malicious files and registry entries from an infected host.

**Recovery**: Restore systems from clean backups and applied patches.

**Lessons** **Learned**: Documented a post-incident report with timeline and recommendations.

**Documented Security Events**

| **Date/Time (UTC)** |  | **Event ID** | **Event Description** |  | **Priority** |
| --- | --- | --- | --- | --- | --- |
| 2025-08-22 14:32 |  | EVT-001 | Phishing email with malicious attachment targeting HR |  | High |
| 2025-08-22 15:10 |  | EVT-002 | Multiple failed SSH login attempts (brute force) |  | Medium |
| 2025-08-22 15:45 |  | EVT-003 | Unusual outbound traffic (possible data exfiltration) |  | Critical |
| 2025-08-22 16:20 |  | EVT-004 | Suspicious PowerShell execution on test VM |  | Low |

**Incident Classification**

| **Incident ID** | **Category** |  |  |
| --- | --- | --- | --- |
| INC-001 | Phishing |  |  |
| INC-002 | Brute Force |  |  |
| INC-003 | Data Exfiltration |  |  |
| INC-004 | Insider Threat |  |  |

**Final Reflection**

By working through alert prioritization, incident classification, and incident response, I developed a clear understanding of how SOC teams manage security events efficiently. This exercise highlighted the importance of:

Quick and accurate alert triage.

Consistent classification with shared frameworks.

A disciplined response lifecycle with evidence handling.