Title: SOC Training Report

Topic: Alert Prioritization, Incident Classification, and Response Practice

Date: 2025-08-28

1. Theoretical Knowledge

1.1 Alert Priority Levels

Core Concepts: Learned about alert severity definitions (Critical, High, Medium, Low), based on impact and urgency. Example: Ransomware = Critical, Unauthorized Admin Access = High.

Assignment Criteria: Prioritization depends on asset criticality, exploit likelihood, and business impact.

Scoring Systems: Explored CVSS (Common Vulnerability Scoring System) and SOC risk scoring in tools like Splunk.

Key Learning Resources: FIRST CVSS Guide, NIST SP 800-61, and real-world mapping via Log4Shell (CVE-2021-44228, CVSS 9.8 = Critical).

1.2 Incident Classification

Core Concepts: Categorized incidents (malware, phishing, DDoS, insider threat, data exfiltration).

Taxonomy: Used MITRE ATT&CK (e.g., T1566 - Phishing), ENISA Incident Taxonomy, and VERIS.

Contextual Metadata: Incorporated IOCs (IPs, hashes, timestamps, affected systems) for incident enrichment.

Key Learning Resources: MITRE ATT&CK, ENISA, SANS case studies.

1.3 Basic Incident Response

Incident Lifecycle: Mastered six phases — Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

Procedures: Learned system isolation, evidence preservation, and communication protocols.

Tools & Automation: SOAR tools like Splunk Phantom for orchestration.

Key Learning Resources: NIST SP 800-61, SANS Incident Handler’s Handbook, Let’s Defend (practical simulations).

2. Practical Application

2.1 Alert Management Practice

Built a classification table in Google Sheets (alerts mapped to MITRE ATT&CK).

Prioritized alerts with CVSS scoring: Log4Shell exploit (CVSS 9.8) marked Critical.

Created a Wazuh dashboard to visualize alerts by priority.

Drafted an incident ticket in TheHive:

Title: [Critical] Ransomware Detected on Server-X

Indicators: crypto_locker.exe, IP 192.168.1.50

2.2 Response Documentation

Used a SANS incident template in Google Docs: Executive Summary, Timeline, Impact, Remediation, Lessons Learned.

Recorded investigation steps in table format (e.g., endpoint isolation, memory dump).

Built a phishing checklist (headers, VirusTotal link check, affected users).

Conducted a mock post-mortem highlighting need for faster email filtering and user awareness.

2.3 Alert Triage Practice

Simulated a Brute-force SSH alert in Wazuh, documented status in a triage table.

Used AlienVault OTX & VirusTotal to validate IOCs and eliminate false positives.

2.4 Evidence Preservation

Practiced volatile data collection with Velociraptor (netstat output saved to CSV).Captured a memory dump, hashed with SHA256, and logged chain-of-custody in a table.

2.5 Capstone Project: Full Alert-to-Response Cycle

Attack Simulation: Exploited VSFTPD backdoor in Metasploitable2 with Metasploit.

Detection & Triage: Wazuh flagged the exploit attempt, mapped to MITRE Technique T1190.

Response: Isolated target VM and blocked attacker IP via CrowdSec.

Reporting: Wrote a structured 200-word incident report including Executive Summary, Timeline, and Recommendations.

Stakeholder Briefing: Delivered a concise 100-word summary for non-technical management.

3. Key Takeaways

Developed risk-based prioritization skills using CVSS and business impact. Learned to classify and enrich incidents with standard taxonomies (MITRE, ENISA, VERIS)Gained hands-on practice in incident lifecycle management — from detection to recovery. Strengthened documentation and communication skills via tickets, templates, post-mortems, and escalation briefs. Successfully executed a full SOC workflow (alert-to-response cycle) in a controlled environment.