SOC Analyst Training & Practical Application Portfolio

This repository documents the successful completion of a comprehensive Security Operations Center (SOC) analyst training program. It showcases the theoretical knowledge and practical skills acquired in alert triage, incident response, evidence preservation, and security reporting.

Table of Contents

---

1. Theoretical Knowledge Foundation

This project is built upon a solid theoretical understanding of core SOC concepts, including:

* **Alert Priority Levels:** Understanding and applying severity levels (Critical, High, Medium, Low) using frameworks like CVSS and considering factors like asset criticality and business impact.
* **Incident Classification:** Categorizing incidents using standard taxonomies like the MITRE ATT&CK® framework, VERIS, and ENISA to streamline investigations.
* **Basic Incident Response:** Mastering the six phases of the incident response lifecycle: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned, as defined by NIST and SANS.

---

2. Practical Application: Task Reports

The following sections detail the hands-on tasks completed to demonstrate practical SOC skills.

Task 1: Alert Management Practice

Objective: To establish and practice core alert management workflows, including classification, prioritization, ticketing, and escalation.

Tools Used: Google Sheets, Wazuh, TheHive (simulated).

Alert Classification System

Mapped alerts to the MITRE ATT&CK® framework to provide immediate context.

| Alert ID | Alert Type | Priority | MITRE Tactic | MITRE Technique |

| :--- | :--- | :--- | :--- | :--- |

| **001** | Phishing Email: Suspicious Link | **High** | Initial Access | T1566: Phishing |

| **002** | Multiple Failed Logins | **Medium** | Credential Access | T1110: Brute Force |

| **003** | Port Scan Detected | **Low** | Reconnaissance | T1046: Network Service Scanning |

| **004** | Log4Shell Exploit Detected | **Critical** | Initial Access | T1190: Exploit Public-Facing Application |

Incident Ticket in TheHive

Drafted a formal incident ticket for a critical ransomware event.

> **Title:** `[Critical] Ransomware Detected on Server-X`
>
> **Description:** EDR agent on **Server-X (192.168.1.50)** triggered a high-severity alert for ransomware-like behavior. Indicators: [File: `crypto_locker.exe`], [IP: `192.168.1.50`].
>
> **Priority:** `Critical`
> **Assignee:** `SOC Analyst`

Escalation Email

Drafted a concise escalation email to Tier 2.

> **Subject:** URGENT: Escalation of Critical Ransomware Incident - IOCs Included

>

> Tier 2 Team,

>

> This is a formal escalation of a critical ransomware incident. At 14:30 UTC, EDR detected active ransomware on **Server-X (192.168.1.50)**. We have placed the host in network quarantine. Please take ownership of this incident for immediate eradication. The full ticket is available in TheHive (Case #2025-058).

Task 2: Response Documentation

Objective: To create clear, actionable, and repeatable documentation for incident response and analysis.

Tools Used: Google Docs, Draw.io (simulated).

Investigation Steps Log

Created a chronological log of actions for a mock incident.

| Timestamp (UTC) | Action | Notes |

| :--- | :--- | :--- |

| 2025-10-06 10:10:15 | Acknowledged EDR Alert and started investigation. | Alert for "Suspicious PowerShell Activity." |

| 2025-10-06 10:15:30 | **Isolated endpoint** `WKSTN-108` via EDR console. | Containment action to prevent lateral movement. |

| 2025-10-06 10:30:00 | Blocked malicious domain and IP on firewall. | Proactive remediation step. |

| 2025-10-06 11:30:00 | **Collected memory dump** from the isolated endpoint. | Evidence preservation. |

Phishing Analysis Checklist

Developed a standard checklist for analyzing suspicious emails.

- [x] Confirm email headers (`Return-Path`, `SPF`).
- [x] Check link reputation (VirusTotal).
- [x] Check attachment hash reputation (VirusTotal).
- [x] Identify all affected users via email gateway search.
- [x] Block malicious indicators (domain, hash, sender).

Post-Mortem Summary

Summarized key findings from a simulated breach.

> The simulated breach revealed a critical gap in our alert notification process. **Improvement:** We will implement a redundant alerting system that automatically escalates to the secondary analyst and SOC manager if a critical alert is not acknowledged within 15 minutes.

Task 3: Alert Triage Practice

Objective: To practice the initial analysis of alerts and validate IOCs using threat intelligence.

Tools Used: Wazuh, VirusTotal, AlienVault OTX.

Triage Simulation

Documented a brute-force SSH alert from Wazuh.

Alert ID	Rule ID	Description	Source IP	Priority	Status
002	5712	SSHD brute force trying to get access to the system.	185.222.58.64	**Medium**	**Open**

Threat Intelligence Validation

Cross-referenced the source IP in AlienVault OTX.

> The IP address `185.222.58.64` was cross-referenced in AlienVault OTX. The IP is associated with multiple recent threat pulses related to SSH scanning and brute-force attacks. Community reports confirm it is a known bad actor. This validates the alert as a true positive, representing a real threat.

Task 4: Evidence Preservation

Objective: To demonstrate forensically sound collection of volatile and non-volatile data.

Tools Used: Velociraptor, FTK Imager (simulated), `sha256sum`.

Volatile Data Collection

Used Velociraptor to collect active network connections from a live host.

* **VQL Query:** `SELECT * FROM netstat`
* **Output:** Saved to `network_connections_20251007.csv` for analysis.

Evidence Collection & Chain of Custody

Collected a memory dump and documented the chain of custody to ensure its integrity.

Item	Description	Collected By	Date	Hash (SHA256)
Memory Dump	Full memory dump from Server-X following a critical EDR alert.	SOC Analyst	2025-10-07	`a34b9e7c5b2a8f8d9b9e1c2a3b4c5d6e7f8a9b0c1d2e3f4a5b6c7d8e9f0a1b2c`

Task 5: Capstone Project - Full Alert-to-Response Cycle

Objective: To demonstrate the end-to-end incident response process by simulating an attack and executing the full detection, triage, response, and reporting cycle.

Tools Used: Metasploit, Wazuh, CrowdSec, Google Docs.

1. Attack Simulation

Successfully exploited the `vsftpd_234_backdoor` vulnerability on a Metasploitable2 VM from an attacker machine (`192.168.1.100`) to gain a remote shell.

2. Detection and Triage

The attack was immediately detected by Wazuh.

| Timestamp (UTC) | Source IP | Alert Description | MITRE Technique |

| :--- | :--- | :--- | :--- |

| 2025-10-07 11:00:15 | 192.168.1.100 | VSFTPD backdoor exploit detected. | T1190 |

3. Response

* **Containment:** The compromised VM was immediately isolated from the network at the hypervisor level.

* **Blocking:** The attacker's IP (`192.168.1.100`) was banned using CrowdSec.

* **Verification:** A ping test from the attacker machine failed, confirming successful containment.

4. Reporting & Stakeholder Briefing

A final report was drafted summarizing the incident and providing recommendations. A non-technical briefing was prepared for management.

> **Manager Briefing Summary:**

> Today, our security team ran a successful test to validate our defense systems. We simulated an attack on a lab server, which was immediately detected. Our response plan worked exactly as designed: we instantly isolated the server and blocked the attacker. There was zero risk to business operations, and the test confirms our security procedures are effective.