Task 5: Advanced Log Analysis, Threat Intelligence Integration, Incident Escalation, Alert Triage, Evidence Preservation

Submitted by:
Shashanka U N
SOC Intern – Cyber Security

Submitted to:
CyArt Tech

Date:
18th Spetember 2025

Introduction:

In today's evolving threat landscape, Security Operations Centers (SOCs) play a critical role in detecting, analyzing, and responding to cyber threats in real-time. Effective monitoring, correlation of events, and proactive threat intelligence integration are essential to identify suspicious activity, mitigate risks, and protect organizational assets. This report demonstrates practical SOC exercises encompassing log analysis, anomaly detection, threat intelligence integration, incident escalation, alert triage, and a capstone simulation of a real-world attack scenario. Each exercise focuses on applying industry-standard tools such as Elastic Security, Wazuh, TheHive, and CrowdSec to develop and refine hands-on skills in monitoring, detection, response, and evidence preservation.

Objectives:

1. **Advanced Log Analysis:**
   - Correlate failed login events with outbound traffic to identify suspicious patterns.
   - Detect anomalies such as high-volume data transfers.
   - Enrich log data with geolocation metadata for improved investigative insights.
2. **Threat Intelligence Integration:**
   - Incorporate external threat feeds from platforms like AlienVault OTX into Wazuh.
   - Enrich alerts with reputation data and indicators of compromise (IOCs).
   - Conduct proactive threat hunting aligned with MITRE ATT&CK techniques.
3. **Incident Escalation Practice:**
   - Create structured incident cases and Situation Reports (SITREPs).
   - Automate escalation workflows to ensure timely Tier 2 intervention.
   - Document investigation steps and mitigation actions effectively.
4. **Alert Triage with Threat Intelligence:**
   - Validate alerts against external sources such as VirusTotal and OTX.
   - Determine the priority and status of alerts based on corroborated intelligence.
   - Reduce false positives and improve SOC decision-making.
5. **Capstone Project – Real-World Attack Simulation:**
   - Simulate cyberattacks to test detection, triage, and response capabilities.
   - Implement containment strategies and escalate incidents appropriately.
   - Preserve evidence and document findings for forensic and compliance purposes.

Scan Results & Observations:

Task 1 – Advanced Log Analysis

Objective:

To correlate failed login events with outbound traffic, detect anomalies such as high-volume data transfers, and enrich log data with geolocation information using Elastic Security and Security Onion.

Methodology:

- Ingested sample logs from the **Boss of the SOC dataset** into Elastic Security.
- Queried Windows Security Event **4625 (Failed Logon)** and matched events with outbound traffic from the same source IP within a short time window.
- Documented findings in a structured table.
- Created an anomaly detection rule in Elastic Security to identify high outbound traffic (network.bytes_out > 1MB within 1 minute).
- Tested the rule using a mock file transfer to simulate large data exfiltration.
- Applied the **GeoIP enrichment processor** in Elastic ingest pipelines to add geolocation details to source IPs.

Results:

Timestamp	Event ID	Source IP	Destination IP	Notes
2025-08-18 12:00:00	4625	192.168.1.100	8.8.8.8	Suspicious DNS request

- **Detection Rule:** Successfully triggered when outbound traffic exceeded 1MB/min.
- **GeoIP Enrichment**: Source IP 192.168.1.100 enriched with geolocation metadata, identifying foreign connections.

Summary:

Log correlation identified failed logins followed by outbound DNS traffic from the same host, suggesting possible brute-force attempts with external communication. An anomaly detection rule flagged high-volume transfers, simulating data exfiltration. GeoIP enrichment added geographic context, revealing connections to unexpected regions and improving investigative insights for threat detection.

Task 2 – Threat Intelligence Integration

Objective:

To integrate threat intelligence feeds with Wazuh, enrich alerts with external reputation data, and perform proactive threat hunting using AlienVault OTX and TheHive.

Methodology:

- Imported AlienVault OTX threat feeds into Wazuh to automatically match indicators of compromise (IOCs) such as malicious IPs.
- Tested feed integration with a mock IOC (192.168.1.100).
- Enriched Wazuh alerts with OTX IP reputation details.
- Documented findings in a structured table.
- Conducted a threat hunt for MITRE ATT&CK technique **T1078 – Valid Accounts** using Wazuh queries (user.name != "system").

Results

Alert ID	IP	Reputation	Notes
003	192.168.1.100	Malicious (OTX)	Linked to C2 server

Summary:

OTX integration enhanced Wazuh detection by matching IOCs with external feeds. A mock malicious IP was successfully enriched with OTX reputation data, confirming its role in command-and-control activity. Threat hunting for T1078 revealed anomalous logins by non-system accounts, highlighting the value of continuous IOC validation and proactive monitoring.

Task 3 – Incident Escalation Practice

Objective:

To practice structured incident escalation, draft Situation Reports (SITREPs), and design automated escalation workflows using TheHive and Google Docs.

Methodology:

- Created a **High-priority case** in TheHive for unauthorized access.
- Drafted a **100-word escalation summary** for Tier 2 analysts.

- Prepared a SITREP in Google Docs documenting the incident timeline and actions.
- Designed a simple Splunk Phantom playbook to auto-assign high-priority alerts to Tier 2.

Results:

A high-priority alert was triggered for unauthorized access on Server-Y at 2025-08-18 13:00. The source IP 192.168.1.200 was identified, correlating with MITRE ATT&CK technique **T1078 – Valid Accounts**. Immediate actions included isolating the server from the network and containing potential lateral movement. Evidence logs were preserved, and Tier 2 escalation was initiated for deeper investigation. TheHive case management facilitated structured documentation, ensuring all IOCs, remediation steps, and incident details were tracked. Automation with Phantom improved efficiency by assigning critical alerts directly to Tier 2 analysts.

SITREP:

- **Title:** Unauthorized Access on Server-Y
- **Summary:** Detected at 2025-08-18 13:00, IP: 192.168.1.200, MITRE T1078
- **Actions:** Isolated server, escalated to Tier 2

Task 4: Alert Triage with Threat Intelligence

Objective:

To simulate alert triage in Wazuh, validate IOCs using VirusTotal and AlienVault OTX, and update alert status based on intelligence findings.

Methodology:

- Reviewed a mock alert for “Suspicious PowerShell Execution.”
- Investigated alert details including source IP and priority.
- Cross-referenced the IP and file hash against VirusTotal and OTX databases.
- Documented triage status in a structured table.

Results & Observations:

Alert ID	Description	Source IP	Priority	Status
004	PowerShell Execution	192.168.1.101	High	Open

The triage of a suspicious PowerShell execution alert revealed the source IP 192.168.1.101 was flagged as malicious in both VirusTotal and OTX. Given its high priority and confirmed IOC status,

the alert remained open for further investigation. This reinforced the importance of external validation during SOC triage workflows.

Task 5: Capstone Project

Objective:

To simulate a real-world attack scenario, detect and triage the event, respond with containment, escalate appropriately, and document findings in a final report.

Methodology:

- Simulated a Samba exploit on Metasploitable2 using Metasploit (exploit/multi/samba/usermap_script).
- Configured Wazuh to generate alerts on exploitation attempts.
- Triaged alerts and correlated with MITRE ATT&CK techniques.
- Contained attacker by isolating VM and blocking malicious IP with CrowdSec.
- Escalated incident to Tier 2 via TheHive with a structured case summary.
- Drafted SITREP and final incident report using SANS template.

Timestamp	Source IP	Alert Description	MITRE Technique
2025-08-18 14:00:00	192.168.1.101	Samba exploit	T1210

On August 18, 2025, a simulated Samba exploit was executed against Metasploitable2 using Metasploit. The attack was promptly detected by Wazuh, which generated a high-severity alert mapped to MITRE Technique T1210 (Exploitation of Remote Services). The SOC team triaged the alert, confirming exploitation activity sourced from IP 192.168.1.101. Immediate containment was performed by isolating the target VM and blocking the malicious IP with CrowdSec, ensuring no further lateral movement. Evidence preservation included volatile data (netstat) and memory acquisition, hashed to confirm integrity. Escalation to Tier 2 analysts was performed via TheHive with all indicators and logs attached. The incident timeline documented detection, response, and escalation steps. Recommendations include strengthening Samba patch management, enabling stricter firewall rules, and continuous monitoring of remote services. The exercise validated SOC capabilities in detecting, responding, and preserving evidence during cyber incidents.

Conclusion

This report highlighted key SOC practices, including log correlation, anomaly detection, and GeoIP enrichment to identify suspicious activity. Threat intelligence integration with OTX improved alert enrichment and proactive hunting. Incident escalation through TheHive ensured structured response and workflow automation. Alert triage with VirusTotal reduced false positives and improved IOC validation. Evidence preservation using Velociraptor and FTK Imager maintained forensic integrity with proper chain-of-custody. The capstone project integrated all tasks, simulating a real-world attack and demonstrating effective detection, containment, escalation, and reporting. Together, these exercises strengthened SOC readiness and enhanced practical cybersecurity skills.