Prepared by: Sahil Danecha
Organization: CyArt
Title: SOC Analysis **Week-3**
Date: 21 Nov 2025

INTRODUCTION

This final SOC master report consolidates all Week-3 activities into a structured, point-wise, professional-grade document aligned with CyArt SOC reporting standards. Each task details objectives, tools used, steps performed, observations, screenshots-ready placeholders, and final conclusions. Tasks 1–6 collectively simulate a full SOC workflow including detection, triage, incident handling, escalation, threat intelligence enrichment, evidence preservation, and a capstone attack-response lifecycle.

1. ADVANCED LOG ANALYSIS

❖ **Objective:**

- Analyze authentication failures and correlate network behavior.
- Detect anomalies in outbound traffic.
- Enhance logs with GeoIP enrichment.

❖ **Tools Used:**

- ElasticSearch & Kibana
- Windows Event Viewer
- Python HTTP Server for file transfer

❖ **Steps Performed:**

1. Generated multiple failed login attempts on Windows (Event ID 4625).
2. Correlated failed logons with outbound DNS/ICMP traffic using Elastic Query DSL.
3. Implemented anomaly detection rule for >1MB outbound traffic per minute.
4. Performed GeoIP enrichment using MaxMind database via Elastic pipelines.

❖ **Key Findings:**

- Login failures linked to abnormal DNS traffic.
- GeoIP enrichment identified foreign IP access origins.
- High-volume data transfer successfully triggered anomaly alert.

Timestamp	Event ID	Source IP	Destination IP	Notes
2025-11-27	4625	192.168.1.100	8.8.8.8	Suspicious DNS

10:15 Request

Summary

This task successfully demonstrated log correlation, anomaly detection, and enrichment using Elastic Security. Failed logins were correlated with outbound connections, high-volume transfers were detected, and GeoIP data enhanced visibility.

---

2. THREAT INTELLIGENCE INTEGRATION

❖ **Objective**:
- Integrate external threat feeds.
- Enrich alerts with hashing, IP reputation, and IOC context.
- Conduct threat hunting (T1078 - Valid Accounts).

❖ **Tools Used:**
- Wazuh Manager
- OTX (AlienVault)
- TheHive (optional correlation)

❖ **Steps Performed:**
1. Added custom OTX pulse including mock malicious IP 192.168.1.100.
2. Configured Wazuh integrator to fetch OTX indicators.
3. Validated alerts enriched with OTX reputation.
4. Performed T1078 threat hunting via Wazuh search queries.

❖ **Findings:**
- IOC successfully matched in Wazuh.
- Pulse data enriched alerts with threat classification.
- Non-system account access attempts identified during hunt.

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

Summary

This task demonstrated effective integration of threat intelligence feeds with Wazuh. AlienVault OTX feeds were successfully imported, alerts were enriched with IOC metadata, and threat hunting for MITRE T1078 revealed multiple non-system login

attempts. The procedure strengthened situational awareness and enhanced detection capability.

3. INCIDENT ESCALATION PRACTICE

❖ **Objective:**

- Escalate an incident using TheHive.
- Draft SITREP and simulate Tier-2 escalation.
- Implement automation using Phantom.

❖ **Steps Performed:**

1. Created incident case: 'Unauthorized Access on Server-Y'.
2. Added observables: Source IP, timestamp, MITRE mapping.
3. Drafted a detailed SITREP including Impact & Next Steps.
4. Built auto-escalation Phantom playbook for high-priority events.

❖ **Key Findings:**

- Incident classification aligned with T1078.
- SITREP properly documented with executive clarity.
- Playbook automation reduces analyst workload.

Conc.

At 22:00, an alert was generated indicating unauthorized access on Server. The source IP 192.168.1.90 performed login attempts that match MITRE ATT&CK T1078 (Valid Accounts). This behavior strongly indicates credential misuse and unauthorized activity.

Impact:

Potential lateral movement attempt and unauthorized credential use within internal systems.

Actions Taken:

- Server isolated
- Incident escalated to Tier 2
- Investigation initiated through TheHive

Next Steps:

- Verify possible credential compromise
- Perform malware scan
- Reset access credentials
- Continue monitoring SIEM for anomalies

Summary

This task successfully demonstrated key SOC incident escalation workflows. A high-priority alert was created and escalated using TheHive, a SITREP was drafted to summarize the incident, and an automation playbook was developed in Splunk Phantom to streamline high-priority alert handling. These activities strengthen SOC readiness and operational efficiency.

4. ALERT TRIAGE WITH THREAT INTELLIGENCE

❖ **Objective:**

- Validate PowerShell-based malicious activity.
- Cross-reference IOC hash/IP with VirusTotal & OTX.

❖ **Steps Performed:**

1. Ingested PowerShell execution logs into Wazuh.
2. Extracted script hash and submitted to VirusTotal.
3. Queried OTX for matching threat pulses.
4. Categorized alert severity and recommended containment.

❖ **Findings:**

- VT flagged script as malicious (AMSI bypass + C2 activity).
- OTX confirmed IP in multiple malware pulses.
- Alert triaged as HIGH requiring immediate response.

Alert ID	Description	Source IP	Priority	Status
004	Suspicious PowerShell Execution	192.168.1.90	High	Open

Summarize findings

IOC validation showed that the PowerShell execution originated from IP 192.168.1.90, which appears in multiple OTX threat pulses. VirusTotal confirmed malicious indicators linked to the script. The alert was triaged as high priority, requiring immediate containment and deeper investigation due to potential credential misuse and execution of malicious commands.

Recommended Response Actions

- Immediately isolate the affected system from the network.
- Perform memory and disk forensics using Volatility and KAPE.
- Reset all local and domain credentials.
- Check for persistence mechanisms such as scheduled tasks or registry autostart entries.
- Monitor for repeated PowerShell execution from the same host.
- Implement PowerShell logging level ‘Verbose’ for improved traceability.

---

5. EVIDENCE PRESERVATION & ANALYSIS

❖ **Objective:**

- Preserve forensic integrity of volatile and non-volatile evidence.
- Maintain chain-of-custody.

❖ **Steps Performed:**

1. Collected volatile network data using Velociraptor netstat artifact.
2. Acquired full memory dump using FTK Imager.
3. Verified dump integrity through SHA-256 hashing.
4. Documented evidence storage, handler, and timestamps.

❖ Key Findings:

- Volatile capture identified active remote sessions.
- Memory dump preserved without corruption.
- Hashing confirmed no tampering during analysis.

Item	Description	Collected By	Date	Hash Value
Memory Dump	Server RAM Dump	SOC Analyst	2025-11-27	<SHA256-VALUE>

Summary

This task successfully demonstrated proper forensic acquisition techniques, including volatile data collection and memory dump preservation. Velociraptor captured active network connections for immediate analysis, while FTK Imager generated a complete memory snapshot. The SHA-256 hash ensured evidence integrity, supporting reliable future investigation and legal admissibility.

---

6. FULL SOC WORKFLOW SIMULATION (CAPSTONE)

❖ **Objective:**
- Simulate full attack-detection-response-escalation workflow.

❖ Steps Performed:
1. Launched Metasploit Samba exploit (usermap_script).
2. Wazuh detected remote command execution attempt.
3. CrowdSec blocked attacker IP for containment.
4. Tier-2 escalation initiated in TheHive.
5. Drafted SANS-style report + executive briefing.

❖ Findings:
- Exploit successful, confirming vulnerability.
- SOC tools responded in correct order (Detect → Triage → Contain → Escalate).
- Final reporting captured business-level impact narrative.

Timestamp	Source IP	Alert Description	MITRE Technique
2025-11-27 22:00:00	192.168.1.90	Samba Exploit	T1210

Detection and Triage (Wazuh)

Wazuh successfully detected the exploitation attempt and generated high-severity alerts. The alert indicated suspicious remote command execution originating from 192.168.1.101. During triage, the analyst verified event correlation, reviewed logs, and identified the exploit pattern. The alert status was marked 'Open' and assigned to Tier-1 SOC for initial investigation.

Response and Containment (CrowdSec)

CrowdSec was used to block the attacker's IP address (192.168.1.90) to prevent further exploitation attempts. A four-hour decision ban was applied, and the block was verified using a ping test. The targeted server (Metasploitable2) was isolated for further forensic analysis and evidence preservation.

Escalation to Tier-2

A case titled 'Samba Exploit – Unauthorized Root Access' was created in TheHive. The incident included system-level compromise indicators, privilege escalation, and post-

exploitation activity. Due to the high impact and potential for lateral movement, the case was escalated to Tier-2 for deeper analysis.

Tier-2 Escalation Summary (100 Words)

During SOC monitoring, a high-severity alert was detected by Wazuh indicating exploitation against the Samba service on Server (192.168.1.90). After analysis, it was confirmed that the Metasploit usermap_script exploit successfully executed, providing unauthorized system-level access. The attacker, operating from 192.168.1.90, gained a reverse shell. CrowdSec immediately blocked the attacker's IP and the compromised server was isolated to prevent further activity. Considering the critical nature of remote service exploitation and potential lateral movement, the case has been escalated to Tier-2 for advanced investigation and remediation.

SANS-Style Incident Report (200 Words)

Executive Summary:
On August 18, 2025, the SOC detected an exploitation attempt targeting the Samba service on Server (192.168.1.90). The attack originated from 192.168.1.90 and used a known Samba usermap_script vulnerability to gain system-level access. Wazuh generated multiple alerts which prompted immediate investigation.

Incident Timeline:
22:00 – Wazuh detected suspicious Samba exploitation traffic.
22:03 – Reverse shell established by attacker.
22:05 – CrowdSec blocked attacker IP.
22:10 – Incident escalated to Tier-2.
22:15 – Forensic acquisition initiated.

Recommendations:
- Patch Samba to the latest secure version.
- Enable strict firewall rules and network segmentation.
- Enforce strong authentication and credential rotation.
- Deploy ongoing vulnerability scanning.
- Improve alert correlation within Wazuh to detect similar exploits earlier.

FINAL SUMMARY

This detailed report reflects a full-scale SOC workflow covering log analysis, threat intelligence, triage, response automation, evidence preservation, exploitation simulation, and incident briefing. Each task builds toward operational readiness, demonstrating capability across analyst responsibilities including detection engineering, threat hunting, incident handling, and forensic evidence management.