CYART SOC Internship – Week 3

Advanced Security Operations & Incident Response Documentation

Prepared by: Kalash Mahajan

Date: 2026-02-19

Executive Summary

Week 3 focused on advanced SOC capabilities including log correlation, anomaly detection, threat intelligence integration, structured escalation workflows, alert triage validation, forensic evidence preservation, and full attack-to-response simulation. Activities were performed within a controlled virtual lab to strengthen analytical depth, automation readiness, and structured documentation aligned with SOC best practices.

1. Advanced Log Analysis

Elastic Security ingested Windows authentication logs for behavioral analysis. Correlation logic was implemented to detect brute-force patterns using Event ID 4625.

Correlation Logic Implemented:

- Event ID 4625 (Failed Logon)
- Same Source IP
- ≥5 attempts within 2 minutes

GeoIP enrichment was configured using an Elasticsearch ingest pipeline to append country, city, and geolocation metadata to IP fields, improving investigative context.

Workflow Summary:

1. Ingested Windows Security logs into Elasticsearch.
2. Created threshold-based correlation rule.
3. Validated repeated authentication failures.
4. Implemented GeoIP enrichment pipeline.
5. Verified enriched fields in indexed documents.

2. Threat Intelligence Integration

AlienVault OTX was integrated with Wazuh for IOC enrichment. Authentication alerts were cross-referenced against external threat intelligence feeds.

Threat Hunting:

- Technique: MITRE ATT&CK T1078 – Valid Accounts
- Reviewed NTLM authentication failures (Event ID 4625).

Workflow Summary:

1. Configured OTX API integration in Wazuh.
2. Generated authentication alert for validation.
3. Verified IP reputation using threat feeds.

4. Conducted targeted threat hunt for credential misuse.

3. Incident Escalation Practice

A high-severity unauthorized access scenario was simulated and documented in TheHive. The incident was mapped to MITRE T1078 and escalated to Tier 2 for forensic review.

SOAR Automation:

- Playbook: Auto_Assign_High_Severity_To_Tier2
- Trigger: New High-Severity Alert
- Action: Assign to Tier2_Queue and mark as Open

Workflow Summary:

1. Created High-severity case in TheHive.
2. Drafted SITREP documentation.
3. Configured Splunk SOAR automation logic.
4. Validated automated escalation behavior.

4. Alert Triage with Threat Intelligence

A PowerShell execution alert (Event ID 4104) was analyzed and mapped to MITRE techniques T1082 and T1083. Script block logging confirmed local discovery commands. Threat intelligence validation using VirusTotal and OTX identified no malicious external indicators. The alert was classified as controlled lab activity.

Workflow Summary:

1. Reviewed Wazuh alert metadata.
2. Analyzed PowerShell script block logs.
3. Cross-referenced potential IOCs.
4. Classified activity as monitored behavior.

5. Evidence Preservation and Analysis

Volatile data was collected using Velociraptor (Windows.Network.Netstat). A full memory acquisition was performed and preserved.

SHA256 Hash of Memory Dump:
cfc6a21704f1752c41b3c80eca36db10e7e3858f9fb49f6460a253f0626e4ef6

Workflow Summary:

1. Collected live network connections.
2. Acquired RAM image from Windows VM.
3. Generated SHA256 hash for integrity validation.
4. Documented evidence in chain-of-custody log.

6. Capstone Project – Full SOC Workflow Simulation

A controlled Samba exploitation (MITRE T1210) was performed using Metasploit. Wazuh detected correlated suspicious activity aligned with the attack timeframe.

Timeline:
• 10:22 – Exploit initiated
• 10:23 – Shell session confirmed
• 10:24 – Wazuh alert review
• 10:35 – Containment via CrowdSec
• 10:40 – Escalation to Tier 2

An incident report and executive briefing were prepared outlining detection, response actions, containment measures, and remediation recommendations.

7. Key Skills Developed

• Advanced authentication log correlation
• IOC enrichment using external threat intelligence
• Tier-based escalation and structured SITREP reporting
• Forensic memory acquisition and integrity validation
• End-to-end SOC detection-to-containment workflow simulation