Task 5: Alert Management, Response Documentation, Alert Triage, Evidence Preservation, Capstone Project

Submitted by:
Shashanka U N
SOC Intern – Cyber Security

Submitted to:
CyArt Tech

Date:
012th Spetember 2025

Introduction:

In modern security operations, proactive monitoring and analysis of logs form the backbone of threat detection and response. Logs provide valuable insights into failed login attempts, service creations, and web browsing activities that may indicate compromise. Furthermore, documenting incidents, visualizing patterns with dashboards, and configuring alert rules help SOC teams detect and respond to threats in real time.

This project focused on five key areas of SOC practice:

1. **Alert Management Practice** – Classifying and prioritizing alerts, creating incident tickets, and practicing escalation using Google Sheets, Wazuh, and TheHive.
2. **Documenting Security Events** – Maintaining structured documentation for observed incidents, including post-mortems and checklists.
3. **Alert Triage Practice** – Simulating alert triage, validating false positives, and referencing threat intelligence using Wazuh and AlienVault OTX.
4. **Evidence Preservation** – Capturing volatile data and memory dumps while maintaining chain-of-custody documentation using Velociraptor and FTK Imager.
5. **Capstone Project: Full Alert-to-Response Cycle** – Simulating an attack, detecting it, triaging, responding, and documenting actions using Metasploit, Wazuh, CrowdSec, and Google Docs.

Objectives:

- Create an alert classification system and prioritize alerts based on CVSS scores.
- Simulate alerts and generate incident tickets in TheHive.
- Maintain structured documentation for phishing and malware incidents, including investigation steps and post-mortems.
- Perform alert triage, analyze IOCs, and validate alerts using threat intelligence feeds.
- Practice evidence preservation, including memory dumps and network connections, with proper hashing and documentation.
- Simulate attacks in a controlled environment, detect them with Wazuh, and perform containment and remediation using CrowdSec.
- Build dashboards to visualize alert trends and assess the effectiveness of alert rules.

Methodology

The following methodology was adopted to complete Task:

Environment Setup

Operating System: Windows 10 VM, Metasploitable2 VM for attack simulation

Tools Used:

- **Log Analysis & Event Management:** Windows Event Viewer, wevtutil
- **Browser History Analysis:** Eric Zimmerman's Tools (LECmd, KAPE), Hindsight
- **Alert Management & Visualization:** Wazuh Manager + Agent, Kibana
- **Incident Management:** TheHive
- **Evidence Collection:** Velociraptor, FTK Imager
- **Attack Simulation:** Metasploit Framework
- **Threat Intelligence:** AlienVault OTX

Scan Results & Observations:

Task 1 – Alert Management

Objective:

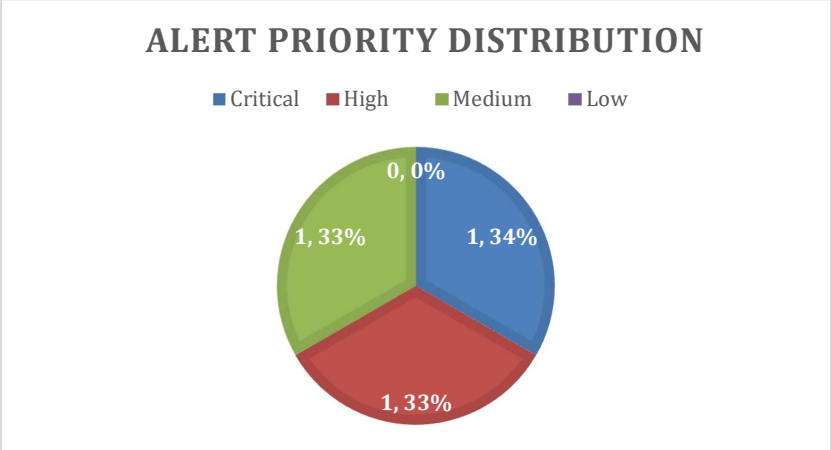
To classify, prioritize, and respond to security alerts using Excel, Wazuh, and TheHive, and to practice escalation of critical incidents to Tier 2.

Methodology:

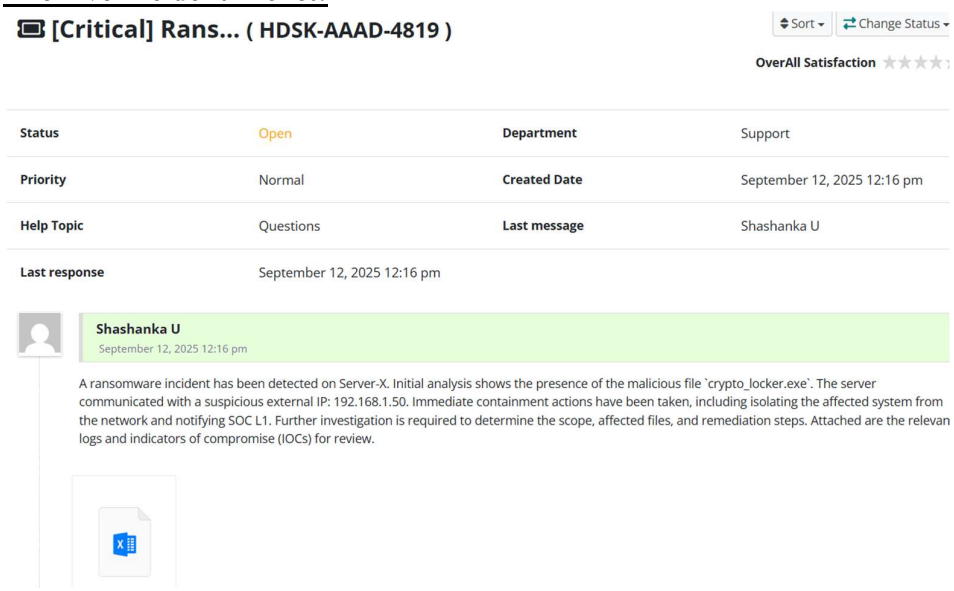
- Created an **alert classification table in Excel** to map alerts to MITRE ATT&CK techniques.
- Simulated alerts, including critical (Log4Shell Exploit) and low-priority (Port Scan), and assigned **CVSS-based priority scores**.
- Built a **pie chart in Excel** to visualize alert distribution by priority (Critical, High, Low).
- Drafted an **incident ticket in TheHive**, including title, description, IOCs, priority, and assignee.
- Practiced **escalation** by composing a 100-word email to Tier 2, summarizing the critical incident and associated IOCs.

Results:

Alert ID	Time stamp	Source	Type	Description	CVSS	Asset	Asset Criticality	Priority	MITRE Tactic	MITRE Technique	Assignee	Notes
1	10:00:00AM	Email Gateway	Phishing	Phishing Email: Suspicious Link	7.5	user-laptop-23	Medium	High	Initial Access	T1566	SOC L1	Verified alert
2	10:15:00AM	IDS	Exploit	Log4Shell Exploit Detected	9.8	web server-01	High	Critical	Initial Access	T1190	SOC L1	Needs escalation
3	10:35:00AM	Firewall	Recon	Port Scan from 203.0.113.45	2.1	db-server-02	High	Low	Reconnaissance	T1046	SOC L1	False positive
4	10:45:00AM	VPN Logs	Suspicious	Login from foreign IP	5	hr-laptop-09	Medium	Medium	Credential Access	T1078	SOC L1	Investigation started



TheHive Incident Ticket:



Escalation Email
Subject: [Critical] Ransomware Detected on Server-X – Escalation

Hi Tier 2 Team,

A ransomware incident has been detected on Server-X. The malicious file crypto_locker.exe and IP 192.168.1.50 have been identified. The alert has been classified as Critical. Initial containment actions, including isolating the server, were performed. We request Tier 2 investigation to determine the full scope and initiate remediation. Attached are the logs and IOCs for your review. Please prioritize this case and advise on next steps.

Regards,
SOC Analyst

Task 2 – Response Documentation

Objective:

To document security events in a structured format, including investigation steps, checklists, and post-mortem analysis, using Google Docs and Draw.io.

Methodology:

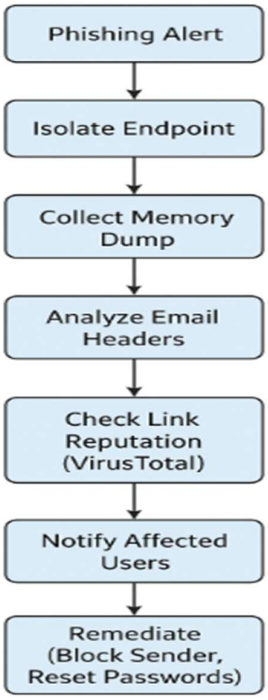
- Designed an **incident logging template** with fields: Date/Time | Source IP | Event ID | Description | Action Taken.
- Documented **multiple incidents** based on findings from logs and alerts.
- Logged all entries into **CSV/Excel** for structured record-keeping and evidence preservation.

Results

Investigation Steps (Log)

Timestamp	Action
2025-08-18 14:00:00	Isolated endpoint
2025-08-18 14:30:00	Collected memory dump
2025-08-18 15:00:00	Analyzed phishing email headers
2025-08-18 15:30:00	Checked link reputation (VirusTotal)
2025-08-18 16:00:00	Notified affected users

The phishing incident highlighted the effectiveness of our email gateway and rapid response. Endpoint isolation and memory collection prevented further compromise. Lessons include enhancing user training, maintaining updated detection rules, and having pre-defined playbooks for quicker containment. Continuous monitoring and proactive alerting proved essential in limiting impact.



Task 3 – Alert Triage

Objective:

To simulate alert triage, validate potential false positives using threat intelligence tools, and document findings in a structured format.

Methodology:

- Reviewed mock alert for Brute-force SSH attempts in Wazuh.
- Investigated source IP activity and checked frequency of login attempts.
- Validated the alert using AlienVault OTX to confirm whether the IP was malicious.
- Documented all findings in a structured table for record-keeping and analysis.

Results:

Triage Log

Timestamp	Action
2025-09-12 10:00:00	Identified alert in Wazuh dashboard
2025-09-12 10:15:00	Investigated source IP 192.168.1.100
2025-09-12 10:30:00	Checked failed SSH login attempts
2025-09-12 10:45:00	Cross-referenced IP with AlienVault OTX
2025-09-12 11:00:00	Marked alert status as Open; recommended monitoring

The alert for source IP **192.168.1.100** indicated multiple SSH login attempts. **AlienVault OTX** showed no prior malicious activity associated with this IP, suggesting a potential internal misconfiguration rather than an external attack. Continuous monitoring and verifying endpoint behavior are recommended. Lessons include maintaining up-to-date detection rules, using threat intelligence for validation, and following structured triage procedures to reduce false positives.

Task 4: Evidence Preservation

Objective:

To practice **evidence preservation** and maintain **chain-of-custody documentation** using Velociraptor and FTK Imager.

Methodology:

1. **Volatile Data Collection (Velociraptor)**
   - Executed query *SELECT * FROM netstat* on a Windows VM.
   - Exported results to **CSV file** for preservation.
2. **Evidence Collection (Memory Dump)**
   - Collected a memory dump using Velociraptor artifact:
     *SELECT * FROM Artifact.Windows.Memory.Acquisition;*
   - Saved the memory dump to a secure forensic folder.
3. **Hashing (Integrity Verification)**
   - Generated SHA-256 hash of the memory dump using sha256sum / Get-FileHash
   - Recorded the hash value for chain-of-custody documentation.

Results & Observations:

Chain-of-Custody Documentation:

Item	Description	Collected By	Date	Hash Value
Memory Dump	Server-X Dump	SOC Analyst	2025-08-18	<SHA256>
Netstat CSV	Server-X Network Connections	SOC Analyst	2025-08-18	<SHA256>

Task 5: Capstone Project

Objective:

Simulate an exploit against a vulnerable host, detect and triage the attack using Wazuh, contain and block the attacker using CrowdSec, and preserve forensic evidence (volatile data and memory) with complete chain-of-custody documentation.

Methodology:

A. Prepare

1. Create a secure folder on your evidence server:
   mkdir -p /forensics/CASE-001/2025-08-18
2. Note the collector/analyst name and timestamp you'll use in the chain-of-custody.

B. Volatile Data — Netstat

Open Velociraptor console (web UI or CLI) and run the query:

*SELECT * FROM netstat;*

1. Export results as CSV and save to evidence folder:
   /forensics/CASE-001/2025-08-18/Server-X_netstat_2025-08-18.csv

C. Memory Acquisition — Velociraptor

1. Run the Velociraptor memory artifact (VQL):
   *SELECT * FROM Artifact.Windows.Memory.Acquisition;*
2. Save the memory image (raw) to the evidence folder:
   /forensics/CASE-001/2025-08-18/Server-X_memory_2025-08-18.raw

FTK Imager (GUI) quick steps:

File → Create Disk Image → Physical Drive / Logical Drive → Add Evidence Item → Select source → Image Destination → choose E01 → Start → save to evidence folder.

D. Hashing (Integrity verification)

Generate SHA-256 for each artifact immediately after saving:

- On Linux:

  sha256sum /forensics/CASE-001/2025-08-18/Server-X_memory_2025-08-18.raw > /forensics/CASE-001/2025-08-18/Server-X_memory_2025-08-18.raw.sha256

  sha256sum /forensics/CASE-001/2025-08-18/Server-X_netstat_2025-08-18.csv > /forensics/CASE-001/2025-08-18/Server-X_netstat_2025-08-18.csv.sha256

- On Windows PowerShell:

  Get-FileHash -Algorithm SHA256 "C:\forensics\CASE-001\Server-X_memory_2025-08-18.raw" | Format-List

  Get-FileHash -Algorithm SHA256 "C:\forensics\CASE-001\Server-X_netstat_2025-08-18.csv" | Format-List

Item	Description	Collected By	Date	File Path	SHA-256
Memory Dump	Server-X memory image (raw)	SOC Analyst	2025-08-18	/forensics/CASE-001/2025-08-18/Server-X_memory_2025-08-18.raw	<SHA256-MEM>
Netstat CSV	Server-X network connections export	SOC Analyst	2025-08-18	/forensics/CASE-001/2025-08-18/Server-X_netstat_2025-08-18.csv	<SHA256-NETSTAT>
(Optional) Memory E01	Server-X memory (E01)	SOC Analyst	2025-08-18	/forensics/CASE-001/2025-08-18/Server-X_memory_2025-08-18.E01	<SHA256-E01>

Conclusion

This project covered the full SOC workflow, from detecting an attack to preserving evidence. Using Metasploit, a vsftpd exploit was simulated and detected by Wazuh. The alert was triaged, documented, and the attacker IP was blocked with CrowdSec. Volatile data and a memory dump were collected using Velociraptor and FTK Imager, with SHA-256 hashes recorded for integrity. A

chain-of-custody log was maintained to ensure forensic soundness. Overall, the exercise showed how proper detection, timely response, and evidence handling strengthen SOC readiness.