Week-2 Task

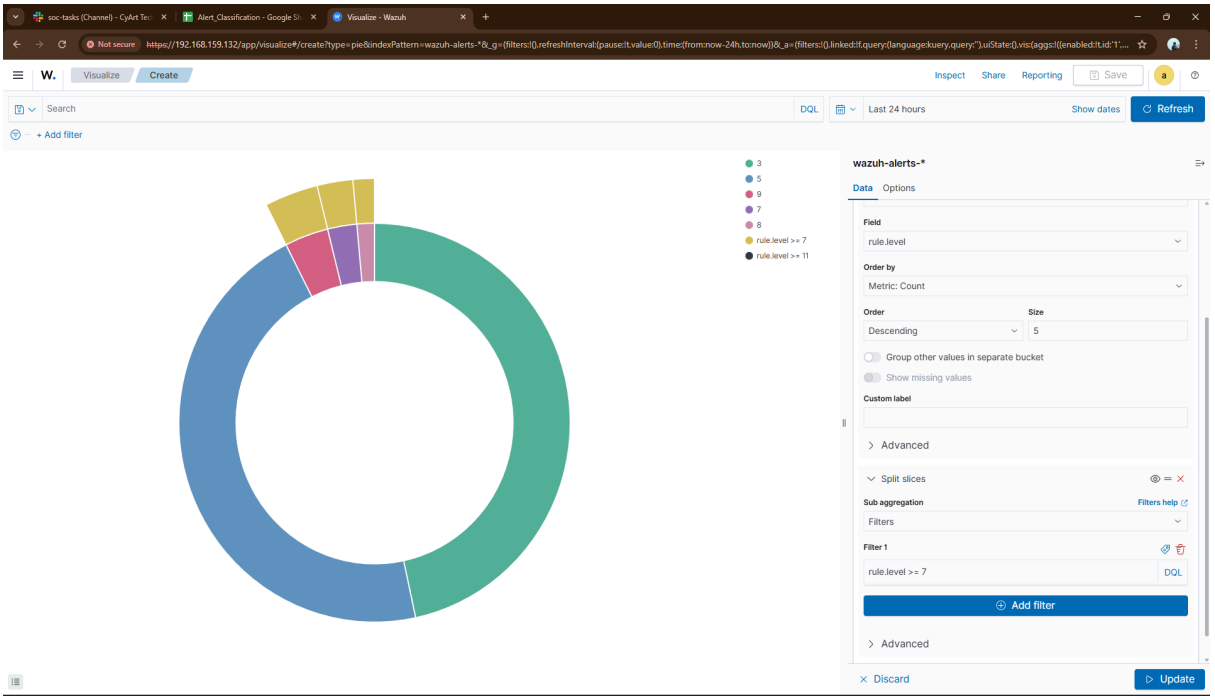
1. Alert Management Practice

Task Breakdown

- Create a Google Sheets table to map alerts to MITRE ATT&CK techniques
- Simulate alerts and score using CVSS in Google Sheets.
- Draft a ticket in TheHive
- Draft a 100-word email to escalate a Critical alert to Tier 2, summarizing the incident and IOCs.

Result

- Google Sheets id created to prioritize alerts
- created a dashboard to visualize alert priorities in pie chart for Critical vs. High alerts.



- Email Draft

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

Hello Tier 2 SOC Team,

A Critical ransomware alert has been detected on Server-X and requires immediate escalation. Initial investigation indicates the presence of a suspicious executable, **crypto_locker.exe**, which is commonly associated with ransomware activity. The affected system also established a connection with the IP address **192.168.1.50**, suspected to be malicious.

Due to the potential risk of data encryption and lateral movement, the alert has been classified as Critical. The affected host should be isolated, and further forensic analysis is recommended to confirm the scope of impact and identify any additional indicators of compromise.
Please advise on next response actions.

Regards,

Niranjan K Rajagopalan
SOC Analyst

2. Response Documentation

Incident Response Report – Phishing Incident

Summary

On 18 August 2025, the SOC identified a phishing email targeting an internal user, impersonating a Microsoft 365 security alert. The user clicked a malicious link and entered credentials on a fake login page. The incident was detected through abnormal login behavior. The affected endpoint was isolated, credentials were reset, and no data exfiltration was observed.

Incident Timeline

Timestamp	Action
2025-08-18 14:00:00	Isolated endpoint
2025-08-18 14:30:00	Memory dump collected for analysis
2025-08-18 15:00:00	User credentials reset
2025-08-18 15:30:00	Phishing domain blocked
2025-08-18 16:00:00	Incident closed

Impact Analysis

- **Affected Users:** 1
- **Affected Systems:** 1 endpoint (Windows workstation)
- **Data Compromise:** None identified
- **Business Impact:** Low
- **Threat Type:** Credential phishing
- **MITRE ATT&CK Technique:** 1566.002 – Phishing: Link

Phishing Investigation Checklist

- ☑ Confirm email headers
- ☑ Validate sender domain
- ☑ Check URL reputation using VirusTotal
- ☑ Identify affected users
- ☑ Review authentication logs
- ☑ Reset compromised credentials
- ☑ Block malicious indicators

Lessons Learned

The incident exposed delays in user reporting and alert triage. Improving phishing awareness training, enforcing organization-wide MFA, enhancing email filtering rules, and standardizing SOC response playbooks will reduce detection time and limit the impact of future phishing-related security incidents.

3. Alert Triage Practice

Objective of the Task

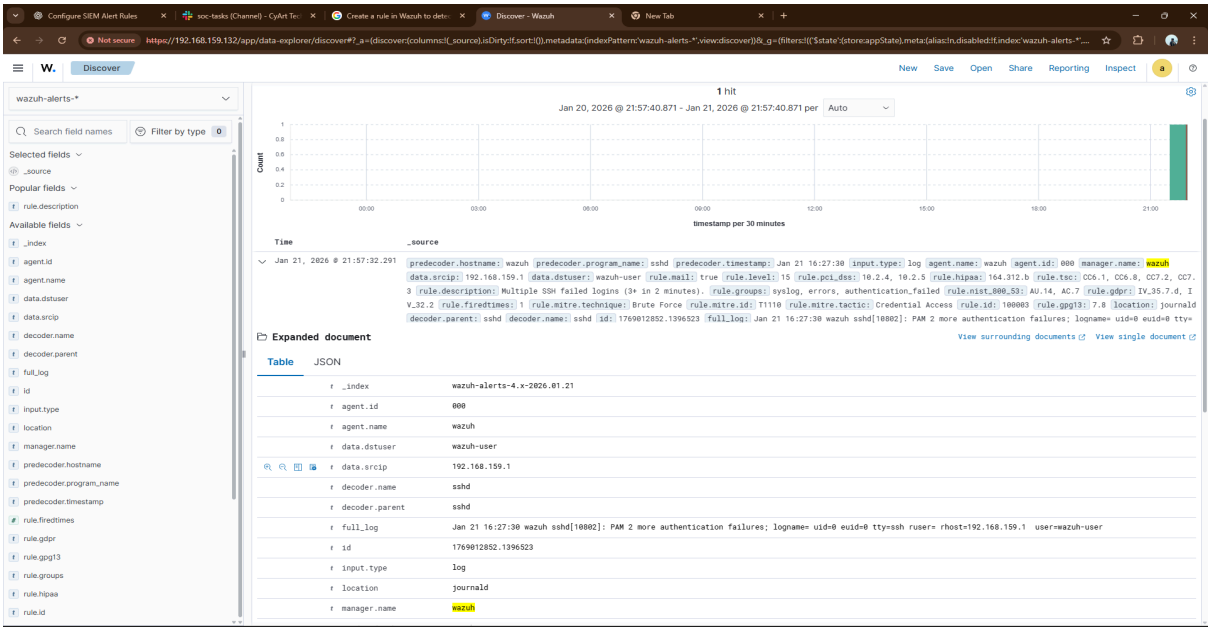
The objective of this task is to practice security operations center (SOC) alert triage and documentation by analyzing a detected SSH brute-force alert in Wazuh. This includes validating alert details, assessing severity and priority, preserving relevant evidence, and performing threat intelligence enrichment using external sources such as VirusTotal and AlienVault OTX to determine the legitimacy and impact of the alert.

Methodology

- Generated alerts in Wazuh by attempting failed logins and user account changes on the Windows host.
- Extracted IOC (source IP 192.168.159.1) from Wazuh logs.
- Queried the IOC against:
    - VirusTotal for multi-vendor security reputation.
    - AlienVault OTX for community-driven threat intelligence.
- Analyzed results to assess whether the IOC is malicious or benign.

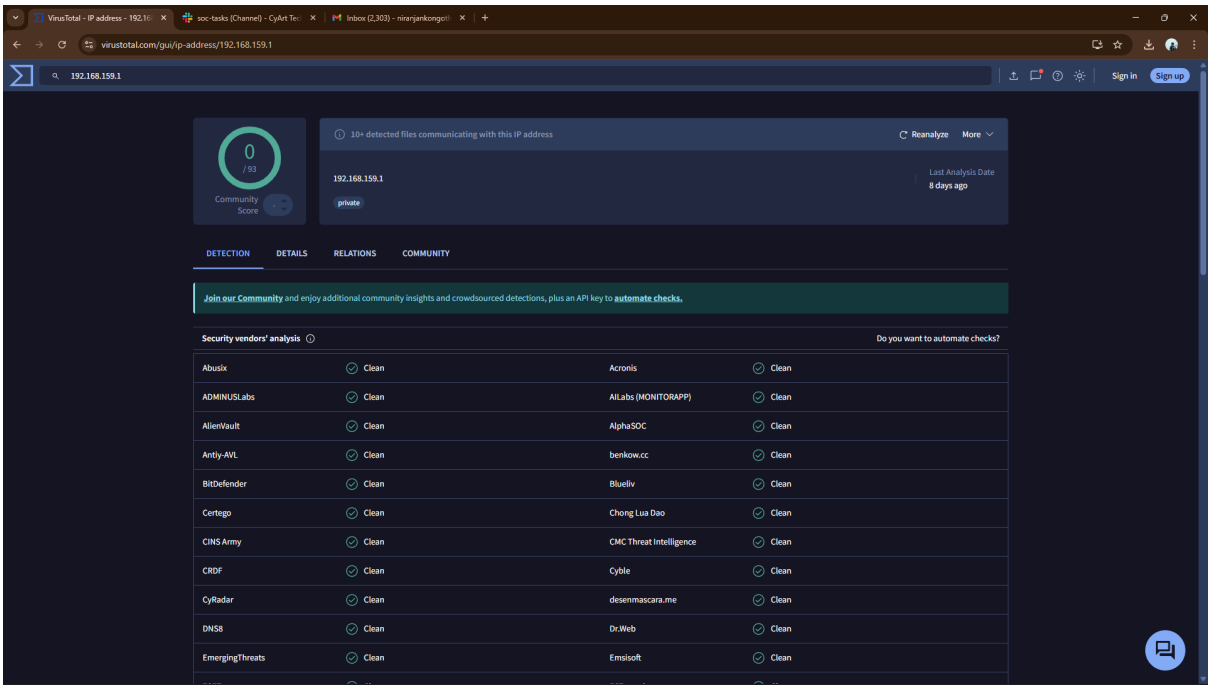
Result

- Identified alert on wazuh dashboard
- source IP identified:192.168.159.1

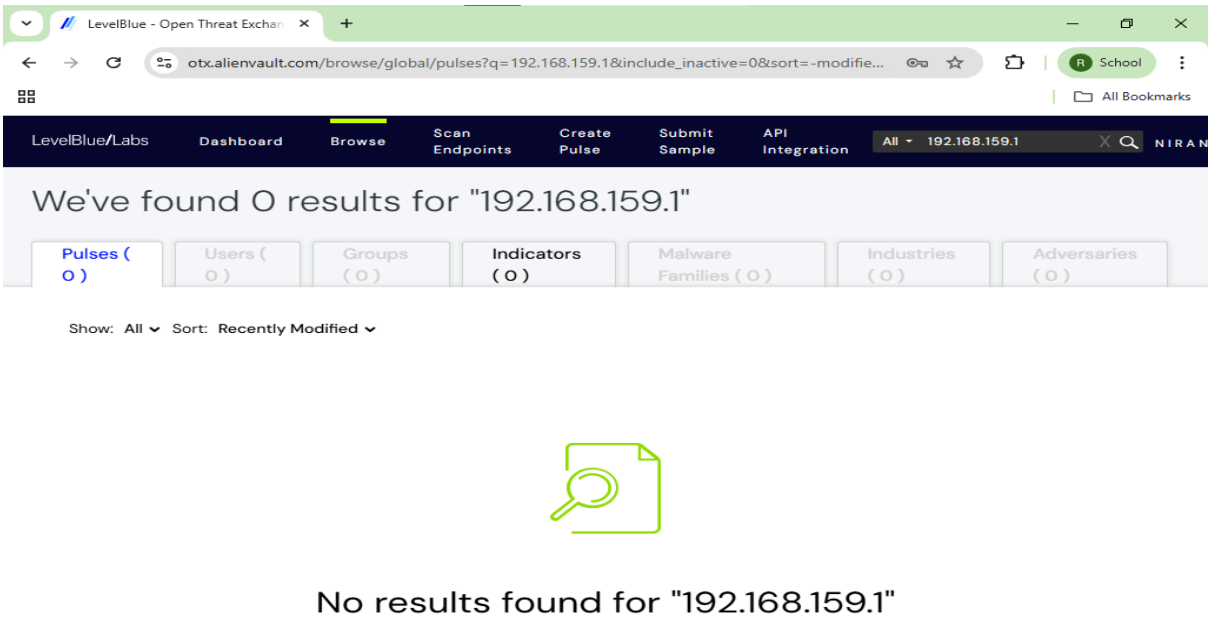


VirusTotal Analysis

- **IP Address:**192.168.159.1
- **Detection Ratio:**0
- **IP Classification: Private IP**



AlienVault OTX Analysis



Conclusion

The IP address 192.168.159.1 is a private (RFC 1918) internal IP, meaning it is used only within a local network and is not routable on the internet. Threat intelligence checks using VirusTotal and AlienVault OTX returned no detections, pulses, or indicators of compromise, confirming that the IP has no known malicious reputation.

Based on these findings, the observed activity is considered normal internal network behavior and is classified as a false positive. No containment or remediation actions are required at this time. Continued baseline monitoring is recommended to detect any future anomalies.

4. Evidence Preservation

Introduction

Evidence preservation is a critical phase of the digital forensics and incident response (DFIR) process. Its objective is to collect, handle, and store digital evidence in a forensically sound manner so that it remains accurate, complete, and legally defensible. During an incident, volatile data such as network connections and system memory can be lost if not captured promptly. Tools like Velociraptor and FTK Imager enable investigators to safely acquire this data while maintaining integrity and chain of custody.

This task focuses on collecting volatile artifacts from a Windows virtual machine, verifying their integrity using cryptographic hashing (SHA-256), and documenting the evidence for future analysis or legal review.

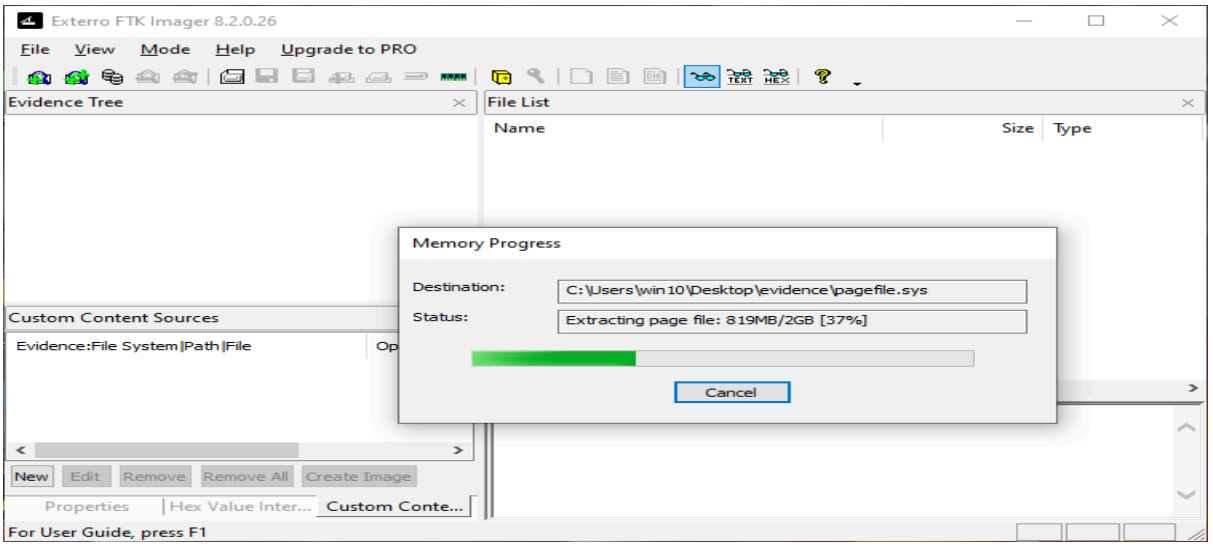
Methodology

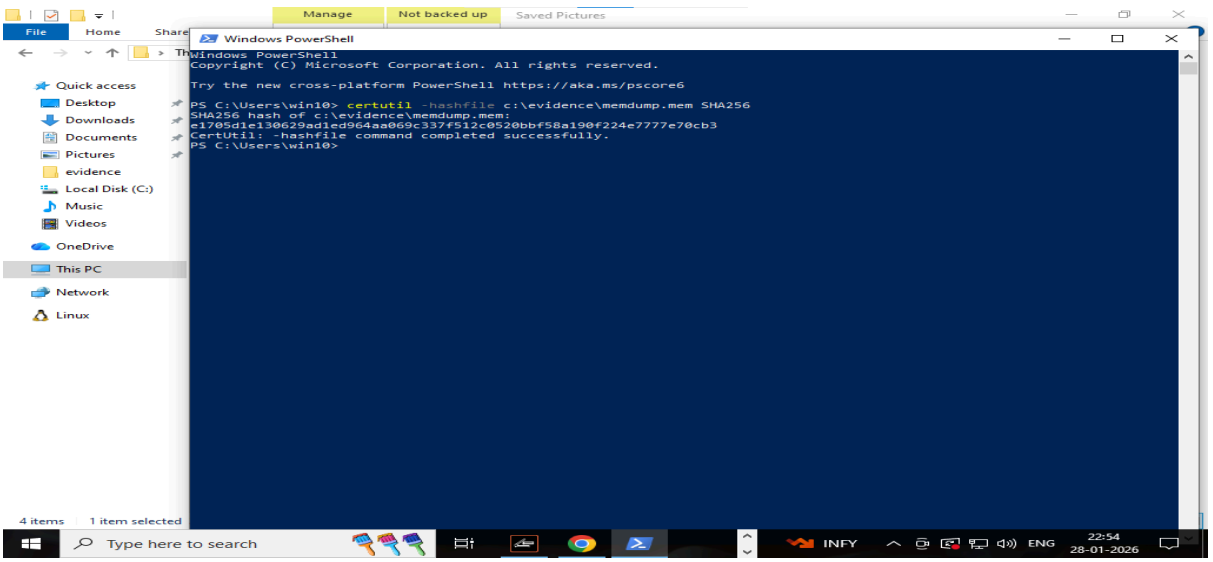
- Volatile Data Collection (Network Connections)
  - Open the **Velociraptor Web UI**.
  - Select the target **Windows client**.
  - Run the following VQL query:SELECT * FROM netstat
  - Export the results as **CSV**.
- Memory Acquisition
  - Memory Acquisition Using FTK Imager
  - Launch FTK Imager as Administrator
  - Configure Memory Capture Settings
  - Preserve the Evidence
  - Verify Integrity :A SHA-256 hash was generated for the memory dump to ensure integrity

Result

- **collected artifacts**
  - memdumb.mem:- raw memory image of system
  - netstat.csv:-snapshort of active network connection

Item	Description	Collected By	Date	Hash value
Memory Dump	Windows full Ram dump	SOC Analyst	2026-01-29	e1705d1e130629ad1ed964aa069c337f512c0520bbf58a190f224e7777e70cb3
Netstat output	Active network connection	SOC Analyst	2026-01-29	3f2825adaf875cacdabbad70dfb0d0e119ac13babbb7a625ba1f3b88d4812131





Conclusion

The evidence preservation task was successfully completed by collecting volatile network data and acquiring a full memory image from the Windows system using Velociraptor and FTK Imager. The collected evidence was securely stored and verified using SHA-256 hashing to ensure integrity and maintain chain of custody. This process followed digital forensics best practices and prepared the evidence for reliable forensic analysis or future legal review.

5. Capstone Project

Introduction

This capstone project demonstrates a complete Alert-to-Response cycle used in real-world Security Operations Centers (SOCs). The project focuses on simulating a cyberattack, detecting it through security monitoring tools, analyzing alerts, executing a response, and producing formal incident documentation. Industry-standard tools such as Metasploit, Wazuh, CrowdSec, and Google Docs are used to replicate practical SOC workflows and incident handling procedures.

A controlled attack is launched against a vulnerable Metasploitable2 virtual machine using Metasploit, exploiting the *vsftpd 2.3.4 backdoor vulnerability*. The attack is detected by Wazuh, mapped to the MITRE ATT&CK framework (T1190), and documented during triage. Incident response actions include isolating the compromised system and blocking the attacker's IP using CrowdSec, followed by verification. The project concludes with a SANS-based incident report and a non-technical stakeholder briefing, highlighting both technical and communication skills essential for SOC operations.

Methodology

1. Attack Simulation
    a. A controlled attack was performed using **Metasploit** against a deliberately vulnerable **Metasploitable2** virtual machine.
    b. The *vsftpd 2.3.4 backdoor vulnerability* was exploited to simulate an external attacker targeting a public-facing service.
2. Ingestion & Alerting
    a. Wazuh ingested and parsed the collected logs, correlating them with predefined detection rules.

   b. A security alert was generated indicating a potential exploitation of a public-facing service.
3. Triage
   a. The generated alert was reviewed to validate the attack and rule accuracy.
   b. The incident was mapped to **MITRE ATT&CK technique T1190 (Exploit Public-Facing Application)** for standardized tracking.
4. Containment & Response
   a. As a response action, the attacker's IP address was blocked using **CrowdSec**.
   b. The compromised virtual machine was isolated by disabling its network adapter to prevent further impact.
5. Evidence Collection
   a. Relevant Wazuh alerts and logs were preserved for investigation.
   b. All artifacts were retained to support reporting and incident documentation.

Findings

- Successful detection:

  Wazuh successfully detected the simulated exploitation attempt against the Metasploitable2 system. The generated alert accurately identified suspicious FTP-related activity associated with the *vsftpd 2.3.4 backdoor*.

- Accurate alert correlation:

  The alert contained relevant contextual information, including timestamp, source IP address, and severity, enabling efficient triage and validation of the incident.

Lessons Learned

- Early detection is critical-Timely alert generation by Wazuh significantly reduced the potential impact of the attack, highlighting the importance of properly tuned detection rules for public-facing services.

- Framework mapping adds value:Mapping incidents to the **MITRE ATT&CK framework** improved incident classification, reporting consistency, and threat tracking across the response lifecycle.

- Isolation limits damage:Quickly isolating the compromised virtual machine prevented lateral movement and further exploitation within the lab environment.

Conclusion

This capstone project successfully demonstrated a complete alert-to-response security operations workflow within a controlled lab environment. By simulating a real-world exploitation scenario using Metasploit against a vulnerable Metasploitable2 system, the project validated the effectiveness of Wazuh in detecting malicious activity and generating actionable security alerts aligned with the MITRE ATT&CK framework.

The incident response process, including alert triage, system isolation, and IP blocking through CrowdSec, proved effective in containing the attack and preventing further impact. Comprehensive evidence collection and structured documentation further reinforced best practices in incident handling and reporting. Overall, this project highlights the importance of integrated security tools, automation, and standardized frameworks in modern SOC operations, while providing practical experience in detection, response, and incident documentation.