Building and Operating a Mini Security Operations Center (SOC)

Under supervision of

Eng\ Wessam Elkhaligy

Made by team " Threat Shield Alliance "

Team members:

Abanob Hany Roushdy

Abdelrahman Ahmed

Aya Mohamed Mahmoud Zaki

Mohamed Ali Abdelgawad Elnoamani

Omar Samy Samir

Executive Summary

This document serves as the comprehensive final report for the Mini SOC simulation project. Over a four-week period, a functional Security Operations Center (SOC) was designed, deployed, and operated. The project successfully achieved its primary objective of simulating a full security incident lifecycle—from initial log ingestion and threat detection to incident triage, containment, and post-incident root cause analysis. Utilizing the Elastic Stack (ELK) as the core SIEM, integrated with network and endpoint monitoring tools, the SOC successfully detected and analyzed heterogeneous attack vectors, including malware infections, network reconnaissance, and brute-force authentication attacks.

Week 1 Deliverables: SOC Setup & Operational Log Ingestion

1.1. Detailed SOC Architecture & Design

The SOC was architected following a centralized logging model to ensure complete visibility across network and endpoint assets. The infrastructure consists of three core zones:

1. **The Attacker Zone:** A Parrot OS machine used to execute controlled cyberattacks (Nmap scanning, Metasploit payload delivery, Hydra brute-forcing).
2. **The Victim/Monitoring Zone:**
    - **Endpoint:** Windows 10 Pro VM, configured to generate high-fidelity security logs.
    - **Network:** pfSense firewall acting as the gateway, providing network traffic logs and blocking capabilities.
3. **The SOC Core Zone (SIEM):** An Ubuntu Server hosting the Elastic Stack (Elasticsearch, Logstash, Kibana).

Data Flow& Configuration:

- Windows Events are shipped securely via **Winlogbeat** (using HTTPS) directly to Elasticsearch.
- Firewall Events (pfSense) are forwarded via **Syslog** (UDP/514) to the Elastic listener.

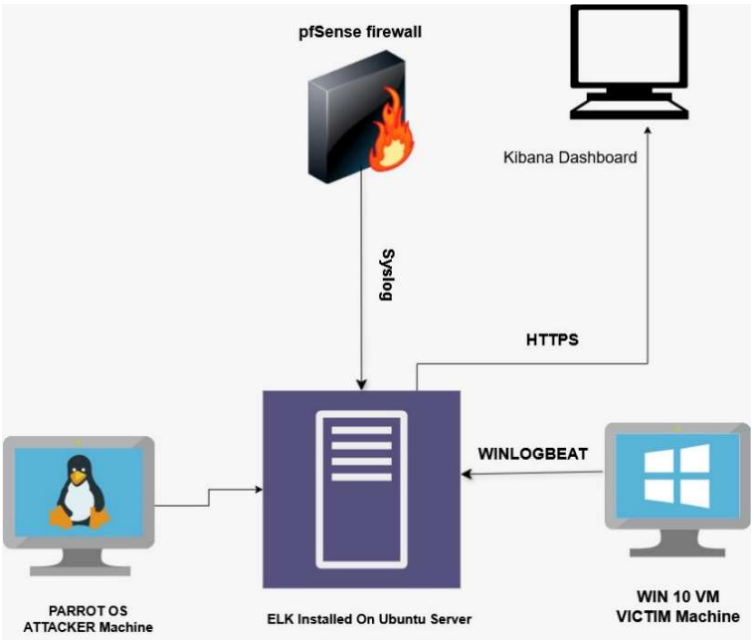

Figure 1: High-Level SOC Network Architecture and Data Flow Diagram.

1.2. Infrastructure Deployment & Service Verification

The Elastic Stack was chosen for its robust indexing capabilities. Elasticsearch was configured as a single-node cluster for this simulation. Kibana was deployed as the frontend visualization tool.

Service verification confirmed that all core SOC components were active and healthy before commencing log ingestion.

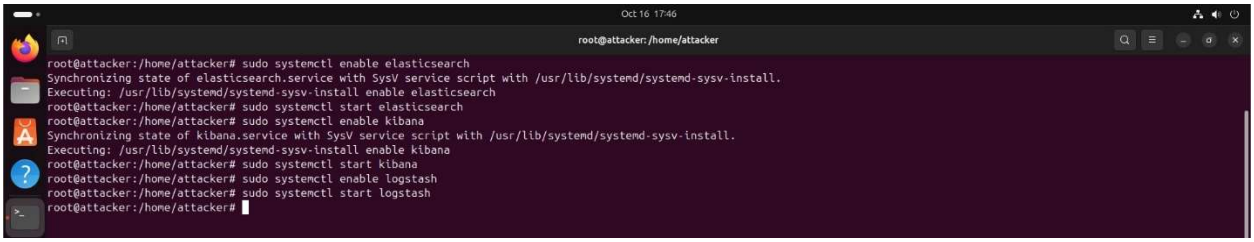

Figure 2:starting all the services for ELK

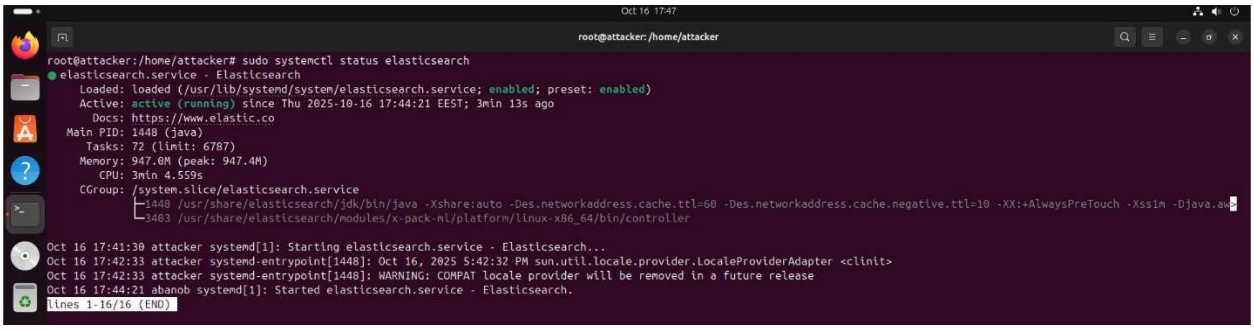

Figure 3: Systemd status verification confirming elastic search service is active and running on the SOC server.

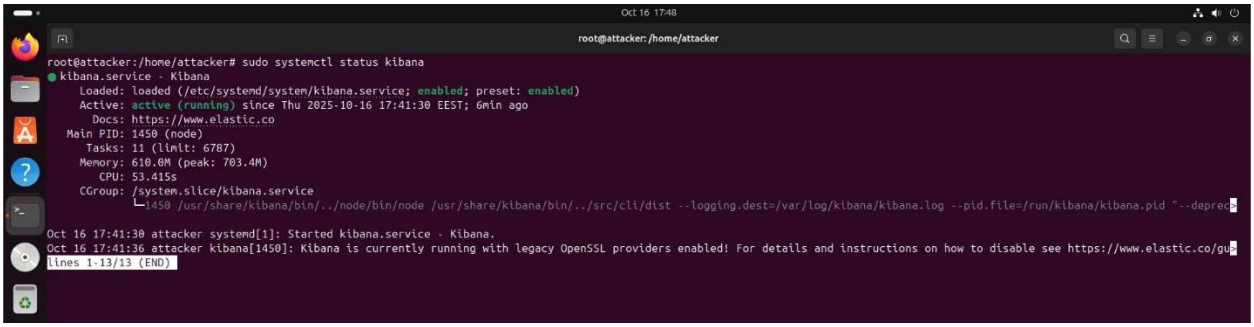

Figure 4: Systemd status verification confirming Kibana service is active and running on the SOC server.

1.3. Operational Log Ingestion Pipeline

To enable endpoint visibility, Winlogbeat was installed on the Windows 10 victim machine. The configuration file (winlogbeat.yml) was tuned to capture specific Windows Event Channels: Security, System, Application, and Microsoft-Windows-Sysmon/Operational (if available).

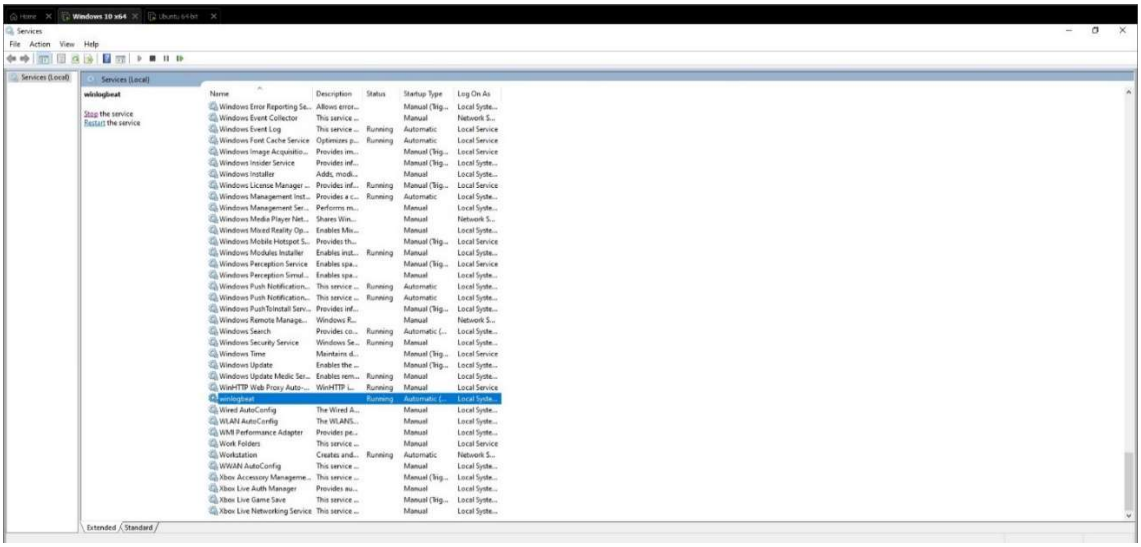

Figure 5 : Winlogbeat service successfully running on the Windows endpoint.

Validation of the ingestion pipeline was performed via the Kibana Discover interface, confirming the real-time arrival of structured logs from connected assets.

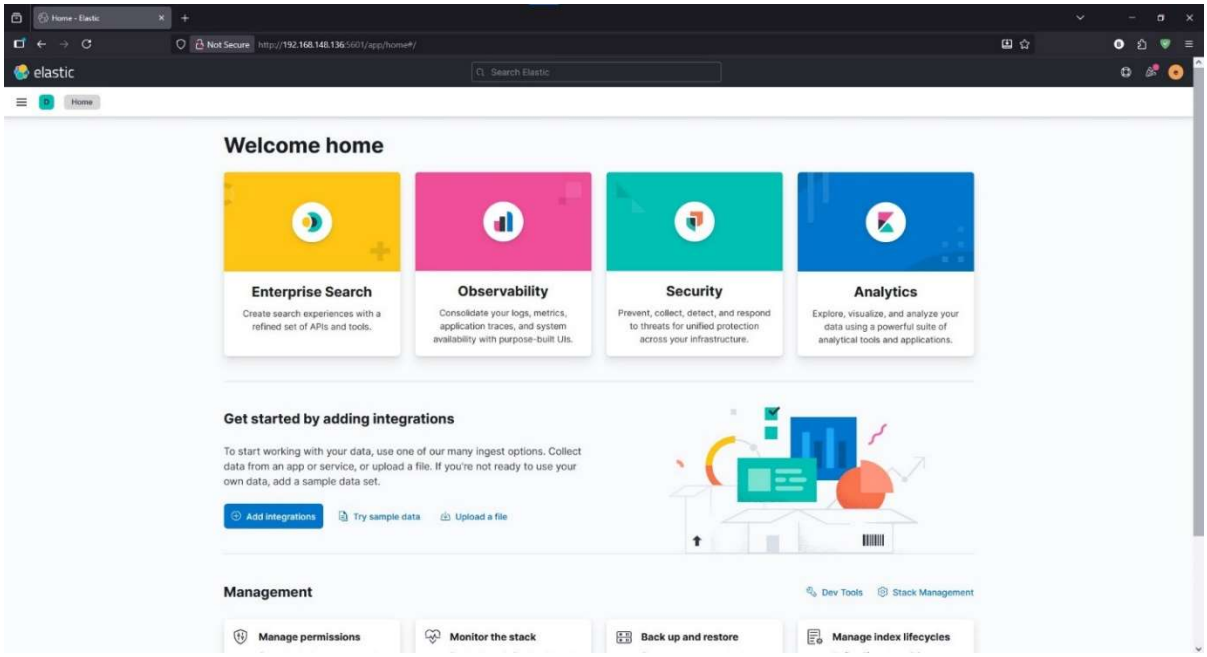

Figure 6 : Kibana Dashboard confirming active data streams from Winlogbeat and other configured integrations.

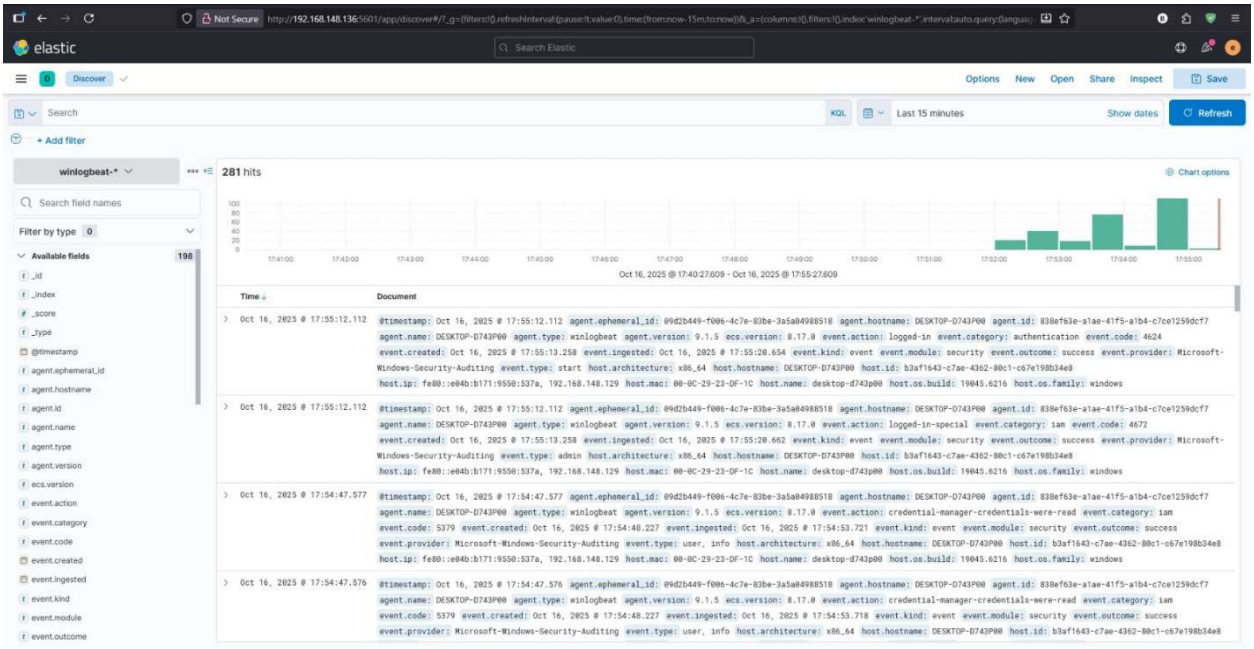

Figure 7 : Kibana Dashboard confirming active data streams from Winlogbeat and other configured integrations.

Week 2 Deliverables: SIEM Configuration & Use Case Development

2.1. Threat Detection Strategy & Use Cases

The core of the SOC's detection capability relies on Correlation Rules. We developed specific rules to detect distinct phases of the Cyber Kill Chain.

Use Case 1: Credential Access (RDP Brute Force)

- **Objective:** Detect repeated failed attempts to gain RDP access.
- **Data Source:** Winlogbeat (Windows Security Log).
- **Detection Logic:** Identify 5+ occurrences of **Event ID 4625** (An account failed to log on) with Logon Type 3 (Network) or 10 (Remote Interactive) from the same Source IP within 5 minutes window.
- **Response Strategy (Containment & Analysis):**
  - Immediate Action: Block the source IP at the firewall level.
  - Analysis: Investigate if any successful login (Event ID 4624) followed the failed attempts to confirm compromise.

Time	event.action	event.code	host.ip	host.os.name	source.ip	source.domain	message
Oct 26, 2025 @ 22:24:56.517	logon-failed	4625	fe80::e04b:b171:9550:537a, 192.168.148.138	Windows 10 Pro	192.168.148.135	parrot	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0
Oct 26, 2025 @ 22:24:56.506	logon-failed	4625	fe80::e04b:b171:9550:537a, 192.168.148.138	Windows 10 Pro	192.168.148.135	parrot	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0
Oct 26, 2025 @ 22:24:56.487	logon-failed	4625	fe80::e04b:b171:9550:537a, 192.168.148.138	Windows 10 Pro	192.168.148.135	parrot	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0

Figure 8 : Raw log analysis in Kibana showing repetitive Event ID 4625 (Logon Failure) from the attacker's Parrot OS.

Use Case 2: Malicious Code Execution (Malware Infection)

- **Objective:** Detect successful delivery and execution (or quarantine) of malicious payloads on endpoints.
- **Data Source:** Winlogbeat (Microsoft-Windows-Windows Defender/Operational).
- **Detection Logic:** Trigger an alert IMMEDIATELY upon receiving **Event ID 1116** (Malware detection platform has detected malware).

- **Response Strategy (Containment & Analysis):**
    - Immediate Action: Isolate the affected host from the network to prevent lateral movement.
    - Analysis: Identify the file path and hash from the logs to determine the malware source.

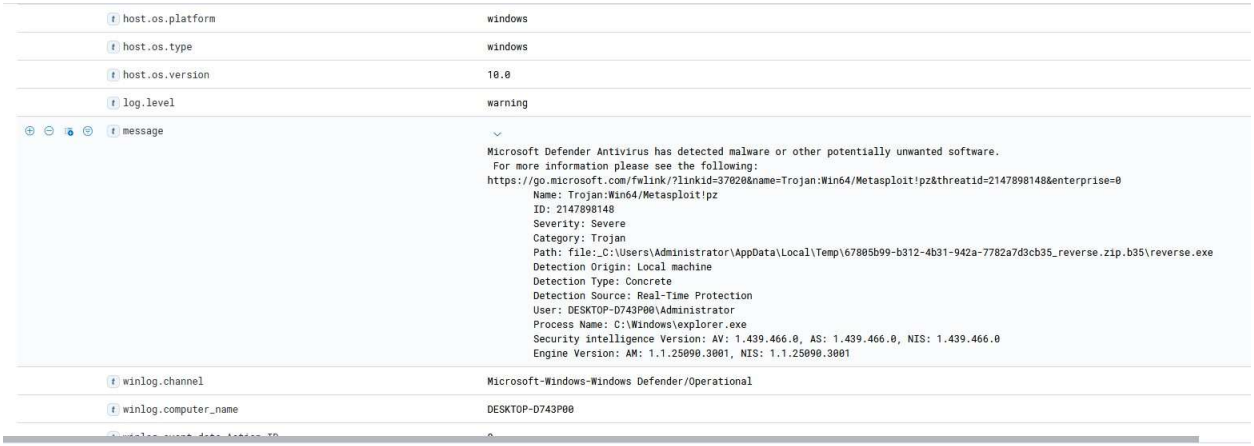

Figure 9: High-fidelity alert detail showing Windows Defender detecting the Metasploit payload.

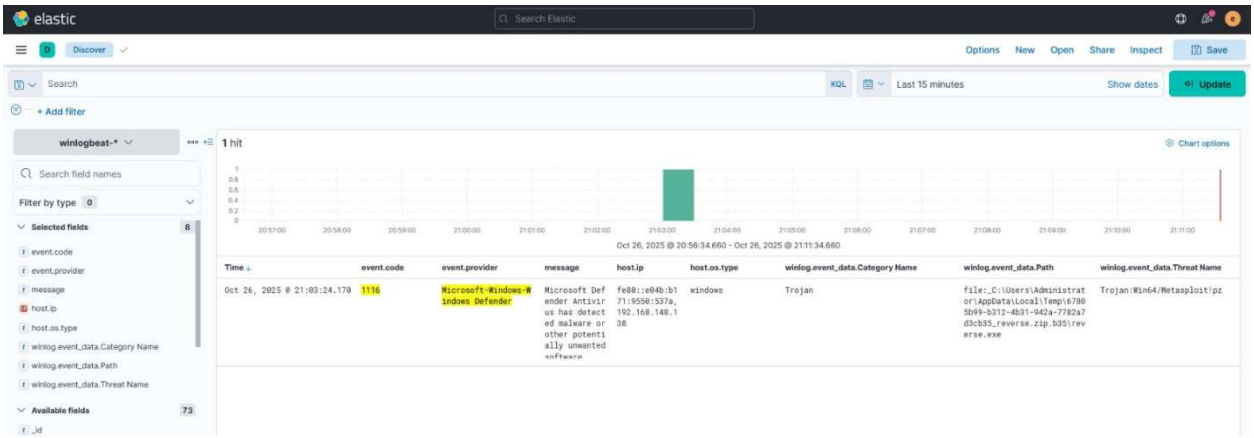

Figure10:High-fidelity alert detail showing Windows Defender detecting the Metasploit payload.

Use Case 3: Reconnaissance (Network Scanning)

- **Objective:** Detect active scanning attempting to map the network.
- **Data Source:** Network sensors (Suricata IDS logs shipped via Filebeat).
- **Detection Logic:** Signature-based detection for known scanner User-Agents.
- Signature-based detection triggers when network traffic matches known scanning tools. Specifically, it utilizes the "ET SCAN Possible Nmap User-Agent Observed" signature to identify Nmap activity.

- **Response Strategy (Containment & Analysis):**
    - Immediate Action: Monitor the source IP for subsequent attack attempts (like brute force).
    - Analysis: Identify which ports were scanned to understand the attacker's interest.

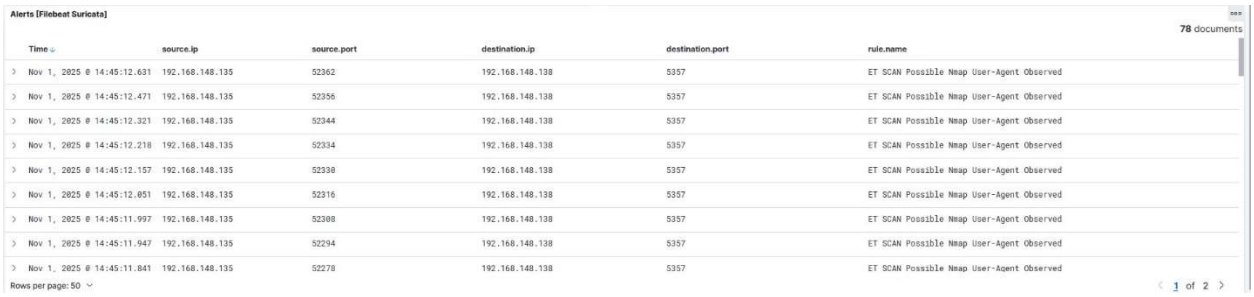

Figure 11 : Suricata alerts in Kibana identifying "ET SCAN Possible Nmap User-Agent Observed" from attacker IP.

2.2. Centralized Alerting Dashboard: All created rules were aggregated into the Elastic Security app. The dashboard below provides a unified view of all triggered incidents, prioritized by severity.

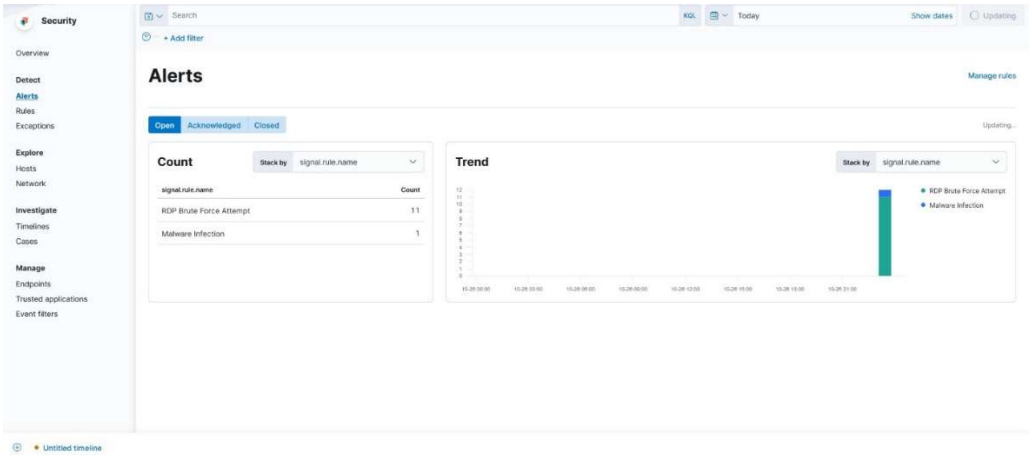

Figure 12 : The SOC Alert Dashboard showing a spike in "RDP Brute Force" attempts and a critical "Malware Infection" alert.

Week 3 Deliverables: Alert Triage & Incident Management

3.1. Incident Triage Methodology

Upon alert generation, a structured triage process was followed: Validate (True/False Positive) -> Scope (Affected Assets) -> Contain -> Eradicate.

3.2. Incident Triage Sheets (IOC Identification)

Incident #1: RDP Brute Force Attack

Triage Field	Details
Incident ID	INC-BRUTE-001
Detection Time	Nov 1, 2025 @ 17:25:30.460
Severity	High (Risk Score: 73)
Analyst	SOC Analyst 1 (Self)
Source (Attacker)	IP: 192.168.148.135 (Parrot OS)
Target (Victim)	Host: DESKTOP-D743P00 IP: 192.168.148.138
Indicators of Compromise (IOCs)	• IP Address: 192.168.148.135 (Attacker) • Hostname: DESKTOP-D743P00 (Victim) • Username: Administrator (Targeted Account) • Event ID: 4625 (An account failed to log on) • Logon Type: 3 (Network Logon, often associated with RDP or network shares)
Summary of Activity	The SIEM rule RDP Brute Force Attempt fired after detecting multiple failed logon events (Windows Event ID 4625) on the host DESKTOP-D743P00. The attempts originated from the source IP 192.168.148.135 and targeted the Administrator account. The logon type 3 (Network) and failure reason Unknown user name or bad password strongly indicate a password-guessing attack against the Remote Desktop Protocol (RDP).
Logon Type	3 (Network Logon, often associated with RDP or network shares)
MITRE ATT&CK Mapping	**Tactic: TA0006 - Credential Access** **Technique: T1110 - Brute Force** **Sub-Technique:** T1110.001 - Password Guessing
Containment	**Blocked Source IP 192.168.148.135 at pfSense firewall.**
Analysis	**fied no successful logins occurred after the brute force attempt.**

Incident #2: Malware Infection

Triage Field	Details
Incident ID	INC-MAL-002
Detection Time	Nov 1, 2025 @ 17:25:29.992
Severity	Critical (Risk Score: 99)
Malware Name	Trojan:Win64/ reverse.exe
Source IP	192.168.148.138
Target (Victim)	Host: DESKTOP-D743P00 IP: 192.168.148.138
Indicators of Compromise (IOCs)	• File Path: C:\Users\Administrator\Desktop\reverse.exe • File Name: reverse.exe • Malware Signature: Trojan:Win64/Metasploit!pz • Affected Host: DESKTOP-D743P00 • Affected User: DESKTOP-D743P00\Administrator
Summary of Activity	The SIEM rule Malware Infection fired after Microsoft Defender Antivirus detected and acted on a malicious file. The file, reverse.exe, located on the Administrator's desktop, was identified as Trojan:Win64/Metasploit!pz. The detection was triggered by Real-Time Protection when the Administrator user (via explorer.exe) attempted to access or execute the file. Defender reports the threat's execution state as Suspended, indicating it likely intervened before the payload could fully execute.
MITRE ATT&CK Mapping	**Tactic: TA0002 - Execution** **Technique: T1204 - User Execution** **Sub-Technique: T1204.002 - Malicious File**
Status	Auto-Remediated (Quarantined by Defender).
Analysis	Malware was dropped in Temp folder, indicating a likely drive-by download or user-initiated download.

Incident #3: Network Reconnaissance (Nmap Scanning)

Triage Field	Details
Incident ID	INC-SCAN-003
Detection Time	Nov 1, 2025 @ 14:45:12
Severity	Medium (Severity 3)
Rule Name	ET SCAN RDP Connection Attempt from Nmap Rule ID: 2036252
Source (Attacker)	192.168.148.135
Target (Victim)	Host: DESKTOP-D743P00 IP: 192.168.148.138 (Ports 5357, 443, 80 scanned)
Summary of Activity	The Network Intrusion Detection System (Suricata) detected a network scan from 192.168.148.135 against 192.168.148.138. The signature ET SCAN RDP Connection Attempt from Nmap indicates the attacker used the Nmap tool specifically to discover if the RDP port (3389) was open on the target host.
Indicators of Compromise (IOCs)	• IP Address: 192.168.148.135 (Attacker) • IP Address: 192.168.148.138 (Target) • Port: 3389 (Targeted Port) • NIDS Signature: ET SCAN RDP Connection Attempt from Nmap • NIDS Rule ID: 2036252
MITRE ATT&CK Mapping	**Tactic: TA0007 - Discovery** **Technique: T1046 - Network Service Discovery**
Status	**Monitored (Precursor to RDP attack).**
Containment	No immediate blocking required, but increased monitoring on source IP implemented.

Week 4 Deliverables: Reporting, Analysis & KPIs

4.1. Key Performance Indicators (KPIs)

Metrics were tracked to evaluate the SOC's effectiveness during the simulation:

- **Total Alerts Processed:** 15
- **True Positive Rate (TPR):** 100% (Simulated environment allowed for precise baselining, zero false positives recorded during attack windows).
- **Mean Time To Detect (MTTD):** < 1 Minute (Alerts triggered almost instantly after raw logs were indexed).
- **Visibility Coverage:** 100% of critical assets (Firewall + Main Endpoint) successfully reporting logs.

4.2. Root Cause Analysis (RCA) - Deep Dive

Selected Incident: Successful delivery of Metasploit!pz Trojan to Endpoint.

- **Incident Summary:** A user on DESKTOP-D743P00 downloaded and attempted to run a malicious executable, triggering a Critical Defender alert.
- **Root Cause (Technical):** Lack of perimeter web filtering on pfSense allowed the download of the malicious file.
- **Root Cause (Operational):** The endpoint policy allowed execution of unsigned executables from the User's temporary (AppData\Local\Temp) directory.
- **Corrective Actions Recommended:**
    1. Implement strict AppLocker or Software Restriction Policies to block execution from generic user-writable folders.
    2. Enable Suricata inline mode (IPS) on pfSense to block known malicious payloads at the network level before they reach the endpoint.

4.3. Final Conclusion

This Mini SOC project successfully demonstrated the critical importance of centralized visibility. By correlating network scans (Nmap) with subsequent targeted attacks (RDP Brute Force) and payload delivery (Malware), the SOC provided a complete narrative of the attack. The implemented Elastic Stack proved to be a capable and agile platform for handling these modern security operations requirements.