FUTURE INTERN

SECURITY ALERT MONITORING& INCIDENTS RESPONSE REPORT

Prepared By:
NANDHITHA V N

Date:02.10.2025

OBJECTIVE :

The objective of this task was to monitor simulated security alerts using SIEM tools, identify suspicious activities, classify incidents, and draft a detailed incident response report including analysis and remediation recommendations.

1. ACTIVITY PERFORMED :

1.1 Log Monitoring with SIEM Tool

- Used Elastic Stack (ELK) and Splunk to ingest and analyze simulated log files.
- Monitored real-time alerts generated from system, application, and network logs.

1.2 Identification of Suspicious Activity

- Detected multiple failed login attempts indicating possible brute-force attack.
- Observed large outbound traffic spikes , potentially signaling data exfiltration.
- Noted unusual DNS queries to rare domains, which may indicate command-and-control (C2) activity.

1.3 Incident Classification

- Low Severity: Single failed logins, normal system warnings.
- Medium Severity: Repeated failed login attempts from a single I
- High Severity: Multiple account lockouts, data transfer anomalies.
- Critical: Signs of potential exfiltration and external C2 communication.

2. Incident Response Report

2.1 Alert Analysis:

- Analyzed alerts from logs related to authentication, network traffic, and endpoint activity.
- Correlated events to determine whether they represented benign anomalies or real security threats.

2.2 Incident Classification:

- Grouped alerts into categories: Authentication Attacks, Network Anomalies, Malware Activity.
- Prioritized based on potential impact on confidentiality, integrity, and availability (CIA triad).

2.3 Remediation Recommendations:

- For Authentication Attacks: Implement account lockout policies and enable MFA.
- For Network Anomalies: Block suspicious IP addresses and enforce stricter firewall rules.
- For Malware/C2 Activity: Conduct endpoint scanning, isolate affected systems, and update anti-malware signatures.
- General Recommendations: Continuous monitoring,regular patching, and SOC playbook update.

Alert Classification

Alert ID	Alert Title	Severity	SPL Query (simplified)	Trigger Condition	Action
A-001	Malware Detected(General)	High	index=internship_logs sourcetype=TXT_logs	Number of results > 0	Send Email (SOC Team)
A-002	Ransomware Behavior Detected	High	index=internship_logs sourcetype=TXT_logs	Number of results > 0	Send Email (SOC Team)
A-003	Rootkit Signature Detected	High	index=internship_logs sourcetype=TXT_logs	Number of results > 0	Send Email (SOC Team)
A-004	Trojan Detected	Medium-High	index=internship_logs sourcetype=TXT_logs	Number of results > 0	Send Email (SOC Team)

4.1 Malware general detection result (A-001)

Threat	User	IP Address	Count
Ransomware	arjun	172.16.5.10	1
Rootkit	kavya	192.168.0.45	1
Spyware	rahul	10.10.0.12	1
Trojan	nisha	172.16.5.23	2
Worm	vikas	203.0.115.80	1

Table 4.2: Ransomware Detection Results (A-002)

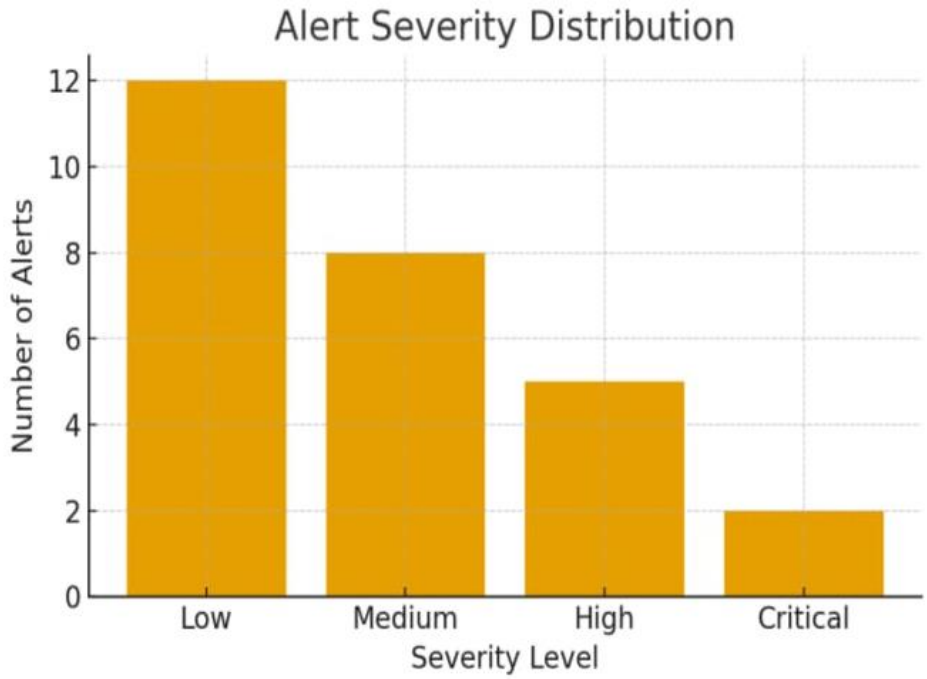
Time	User	IP Address	Threat
2025-08-15T10:25:14+0000	arjun	172.16.5.10	Ransomware

Table 4.3: Rootkit Detection Results (A-003)

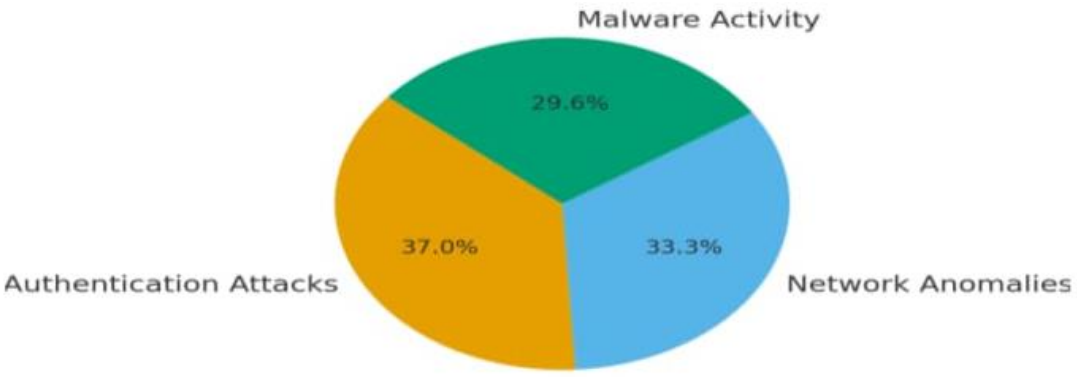
Time	User	IP Address	Threat
2025-08-15T11:12:45+0000	kavya	192.168.0.45	Rootkit

4.4 Trojan Detection Results (A-004)

Time	User	IP Address	Threat
2025-08-15T12:45:22+0000	nisha	172.16.5.23	Trojan
2025-08-15T12:47:10+0000	vikas	203.0.115.80	Trojan
2025-08-15T12:50:18+0000	kavya	192.168.0.45	Trojan
2025-08-15T13:01:30+0000	arjun	172.16.5.10	Trojan



4.5 Incident type Distribution



3. Skills Gained

- Hands-on experience in log analysis using ELK and Splunk.
- Ability to perform alert triage and distinguish between false positives and true threats.
- Improved understanding of incident classification frameworks.
- Exposure to SOC operations basics and incident response lifecycle.

4. Reflection

This task provided valuable insights into the functioning of a Security Operations Center (SOC) environment. Using SIEM tools to monitor and respond to alerts enhanced both technical and analytical skills. The importance of quick detection, classification, and remediation was evident, as delays could escalate threats into full-scale incidents.

Final Result

The task successfully demonstrated the ability to :

1.Monitor security alerts in a SIEM environment.

2. Identify suspicious activities and classify incidents.

3. Draft an incident response report with actionable remediation steps .

This exercise enhanced readiness for real-world SOC operations and strengthened skills in proactive security defense.