Security Operations Center (SOC) Internship Report

Task: Security Alert Monitoring & Incident Response Simulation

1. Introduction

This report documents the activities performed during the SOC internship project focused on **security alert monitoring and incident response simulation**.
The objective of this task was to learn how a SOC Analyst monitors logs, detects suspicious events, triages alerts, and communicates incidents to stakeholders.

2. Project Scope

During the task, simulated security logs were analyzed to detect:

- Failed authentication attempts
- Unusual network connections
- Malware alerts
- Suspicious user behavior

A SIEM tool was used to view, filter, and analyze the logs to identify potential threats.

3. Tools & Resources Used

Tool	Purpose
Splunk / ELK (SIEM Tool)	Log monitoring and alert analysis
Sample Log File: SOC_Task2_Sample_Logs	Contained authentication, network, and malware events
Word / Google Docs	For creating the incident response report

4. Skills Developed

- Basic **log analysis** and event interpretation
- **Alert triage** and severity classification
- Use of **SIEM dashboards** to visualize threat activity
- Understanding key **cybersecurity terminology**
- **Incident response documentation and communication**

5. Data Analyzed

The dataset included:

- System event timestamps
- Network connections with IP addresses
- Successful & failed login attempts
- Malware detection alerts

6. SIEM Search Commands Used

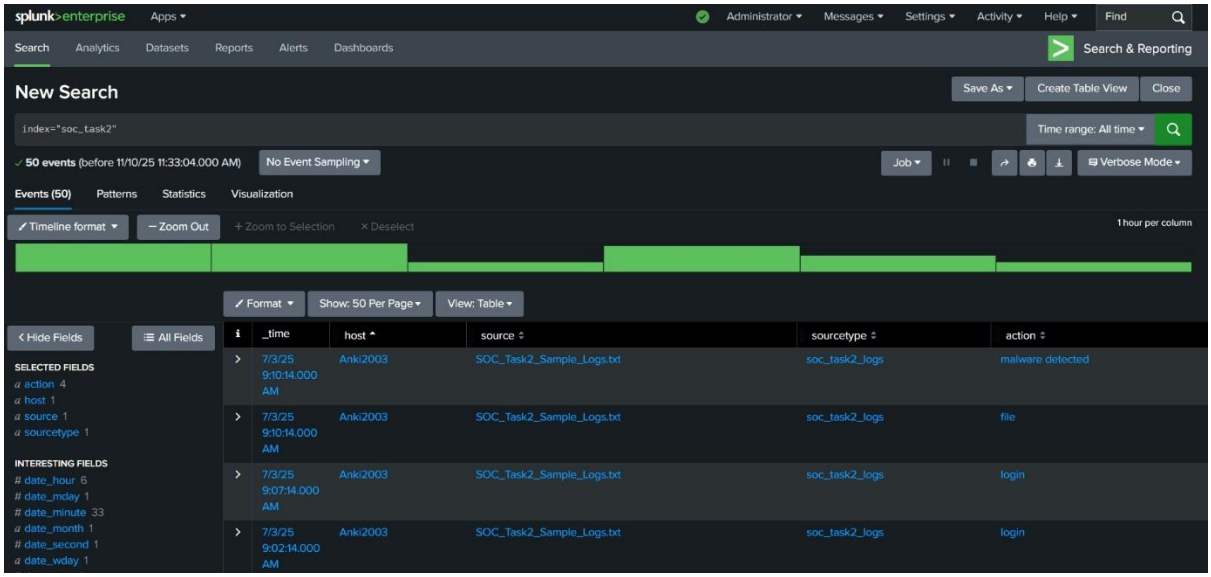
6.1 View All Logs

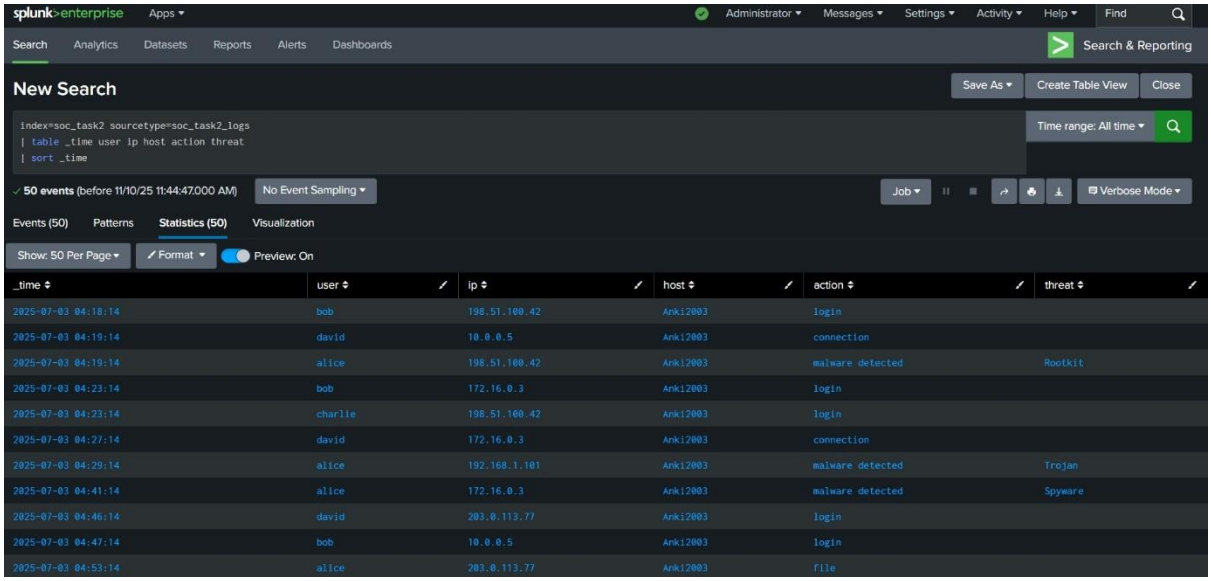
index=soc_task2 sourcetype=soc_task2_logs

| table _time user ip host action threat

| sort _time

Obsevation:

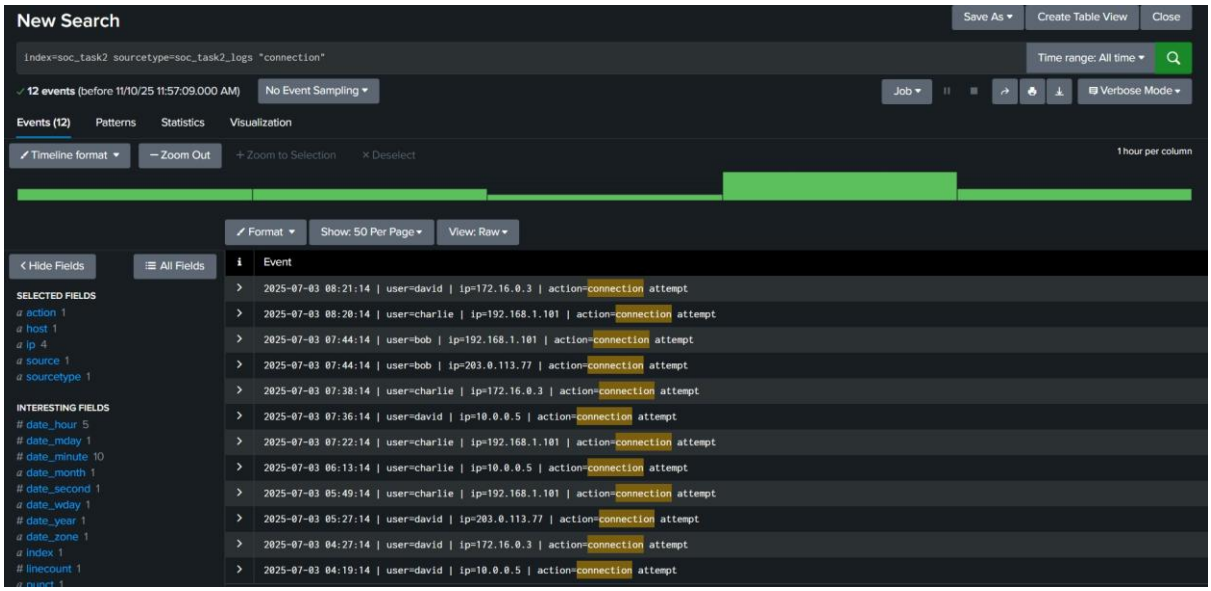




6.2 Login Detection

index=soc_task2 sourcetype=soc_task2_logs action="connection"

Observation:



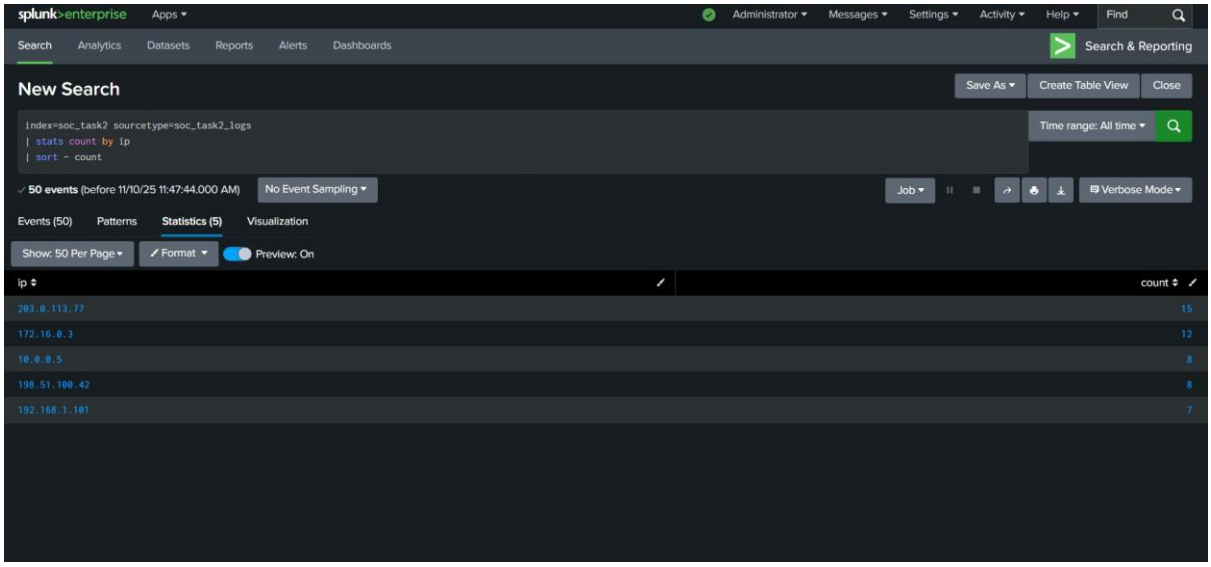
6.3 Suspicious IP Activity

index=soc_task2 sourcetype=soc_task2_logs

| stats count by ip

| sort – count

Observation:



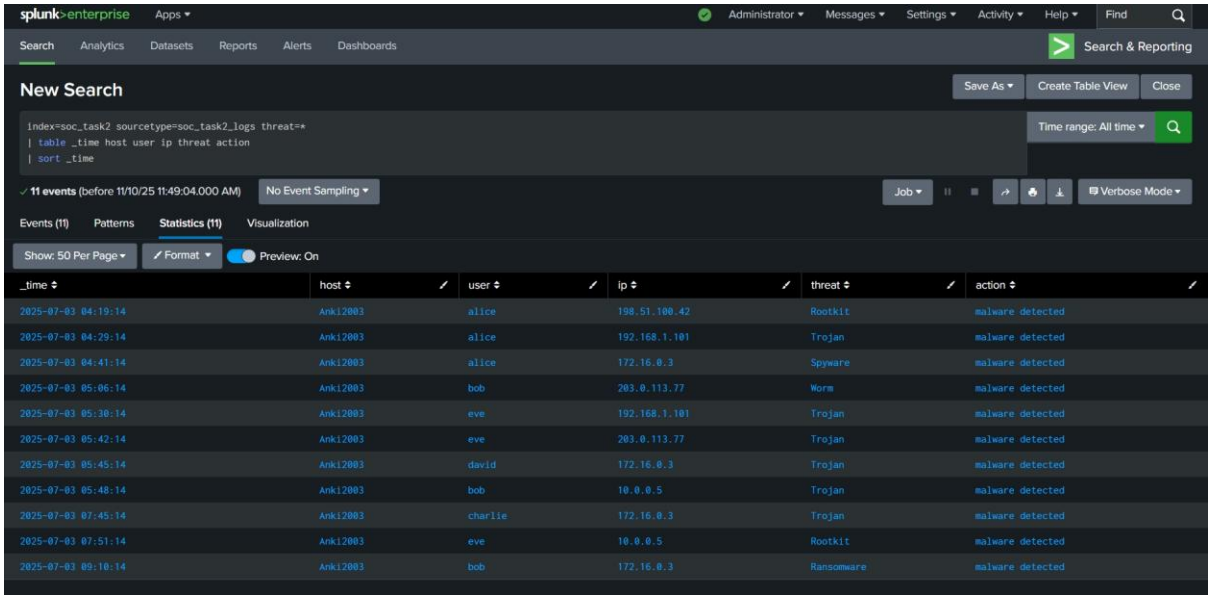
6.4 Malware Alerts

index=soc_task2 sourcetype=soc_task2_logs threat=*

| table _time host user ip threat

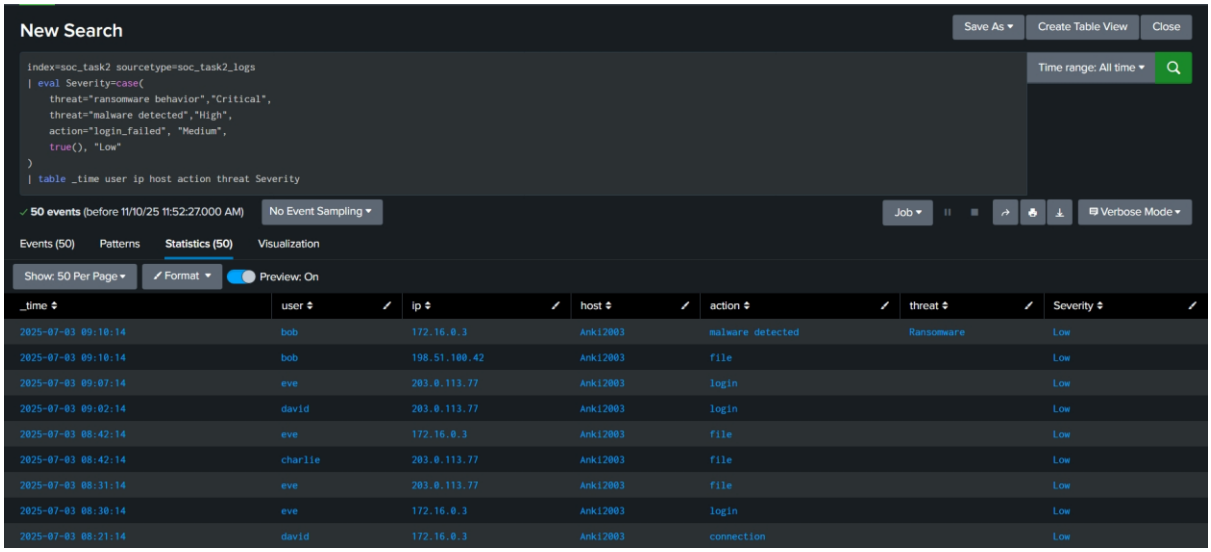
| sort _time

Obsevation:



6.5 Severity Level

Observation:



7. Identified Incidents & Findings

Incident #1 — Multiple Failed Login Attempts

- **User:** David
- **Source IP:** 10.0.0.5
- **Description:** Several failed login attempts were recorded, indicating a possible brute-force attack.
- **Severity: low**
- **Action:** User account monitored and login attempts reviewed.

Incident #2 — Suspicious External IP Connection

- **IP:** 203.0.113.77
- **Severity: low**
- **Action:** Flagged for further investigation, recommended firewall block if repeated.

Incident #3 — Malware Detection Alert

- **Threat Type:** Ransomware Behavior
- **Host:** workstation-04
- **Severity: Critical**
- **Action Taken:** Host isolated and malware scan recommended.

8. Incident Response Summary Table

Incident	Indicators	Severity	Response
Failed Login Attempts	Multiple login failures from same IP	low	Monitor and verify user activity
Suspicious IP Connection	New / unknown IP access attempt	low	Investigate & restrict access
Malware Detection	Ransomware alert triggered	low	Isolate host & perform malware removal

9. Communication to Stakeholders (Email Template)

Subject: Security Alert Notification — Incident Under Review
Message:
A security event has been detected and is currently under investigation. Our SOC team has identified abnormal login activity and a malware alert on one workstation. The affected system has been isolated and further analysis is in progress. Additional updates will be shared upon completion of the investigation.

10. Conclusion

This internship task provided practical exposure to SOC analyst responsibilities, including alert monitoring, log analysis, threat identification, and incident response documentation. The activity reinforced the importance of early detection, structured triage, and effective communication in cybersecurity operations.