Security Alert Monitoring & Incident Report Task-2

Intern name : Mithileshwaran

Internship domain : Cyber Security

Task tittle : Security Alert Monitoring & Incident Response

Date : August 2025

Tool used : Splunk Cloud Free Trail

1.Objective :

The objective of this task was to simulate real-world Security Operations Center (SOC) activities using Splunk. I uploaded and analyzed a simulated log file (`SOC_Task2_Sample_Logs.txt`) containing various system events such as login attempts, malware alerts, IP connections, and host activity.

The goal was to identify security threats by running custom queries, classify alerts based on severity, and document findings through screenshots. This included detecting malware presence, high-volume host logs, failed login attempts, and possible port scanning behavior — mimicking how SOC teams monitor and respond to potential cyber incidents.

2. Log Source:

- **Log File Name:** `SOC_Task2_Sample_Logs.txt`
- **Description:** Simulated system logs containing authentication attempts, usernames, IP addresses, malware alerts, and network activity.
- **Upload Platform:** Splunk Cloud (Free Trial)

3. Summary of Alerts:

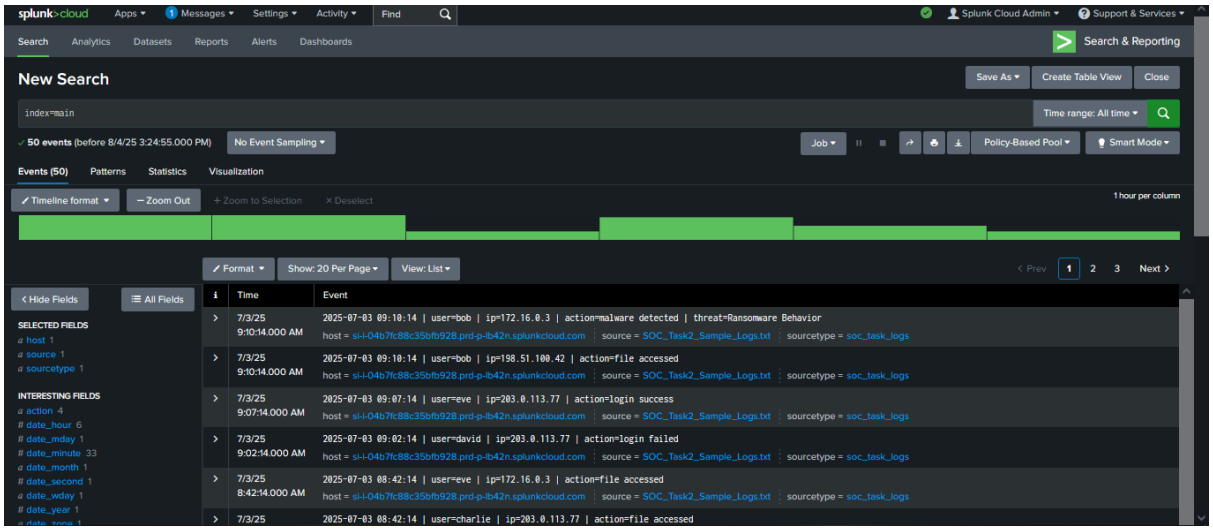
Alert ID	Type	Description	Severity
A01	Full Log View	Index-wide search to observe full logs (`index=main`)	Low
A02	Malware Detection	Trojan found in logs from Splunk	High
A03	High Host Activity	Host logged 50+ events — possible automation or misuse	Medium
A04	Failed Login Attempts	Multiple failed authentication attempts observed	High
A05	Port Scanning Detected	Repeated connections/port activity logged	Medium

4. Detailed Incident Analysis

A01 – Full Log Overview:

Query Used: `index=main`

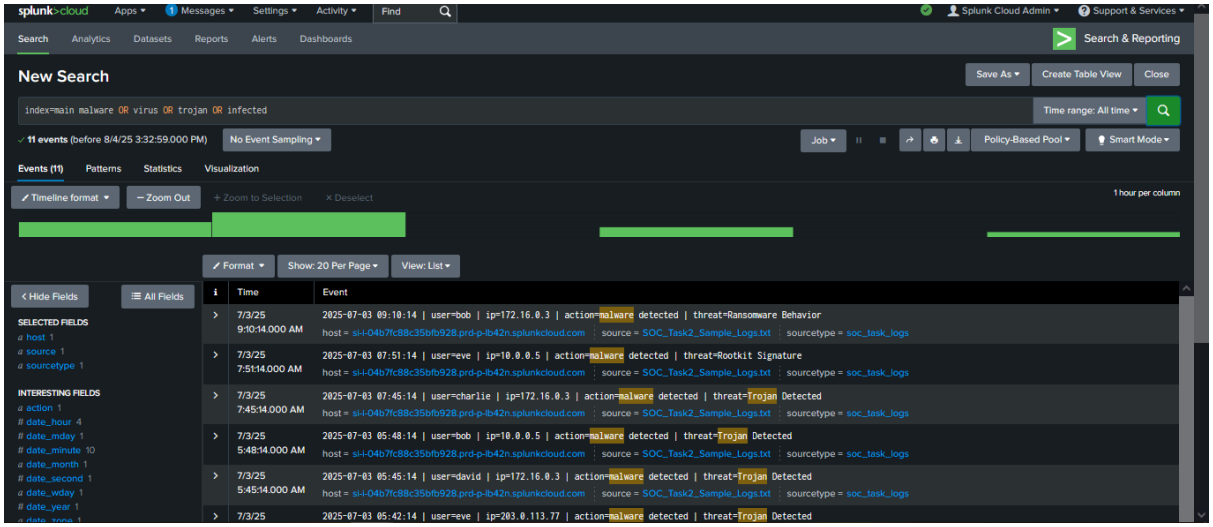
A general log overview was performed to validate that log ingestion into Splunk was successful. This gave context for further threat hunting.



A02 – Malware Detection:

Query Used: `index=main malware OR trojan OR virus`

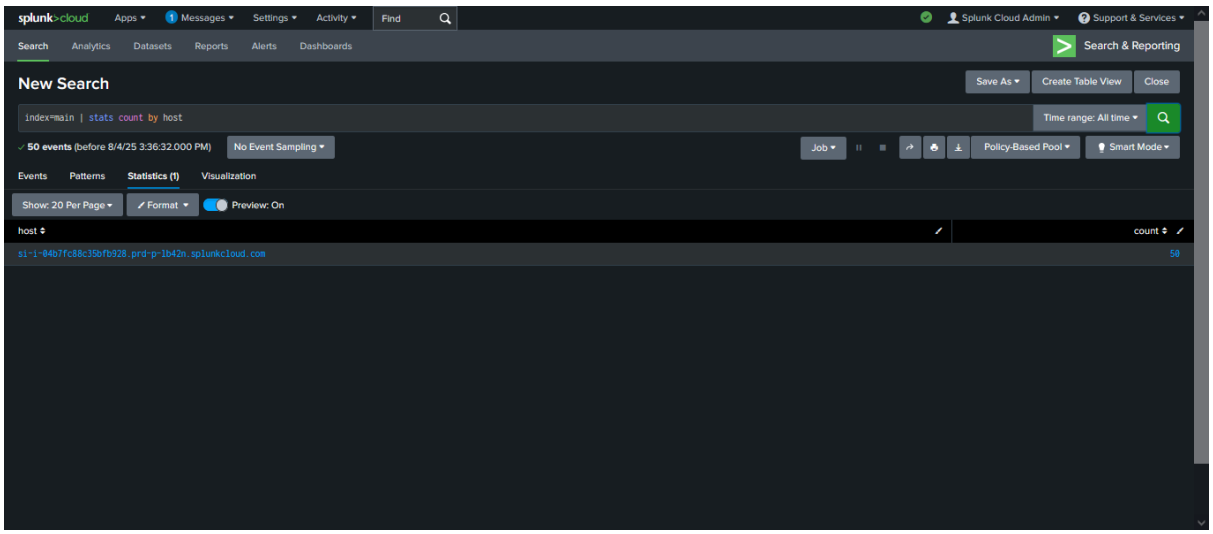
A Trojan was detected in the logs, suggesting possible system compromise. Malware should be isolated and removed immediately.



A03 – High Host Activity:

Query Used: `index=main | stats count by host`

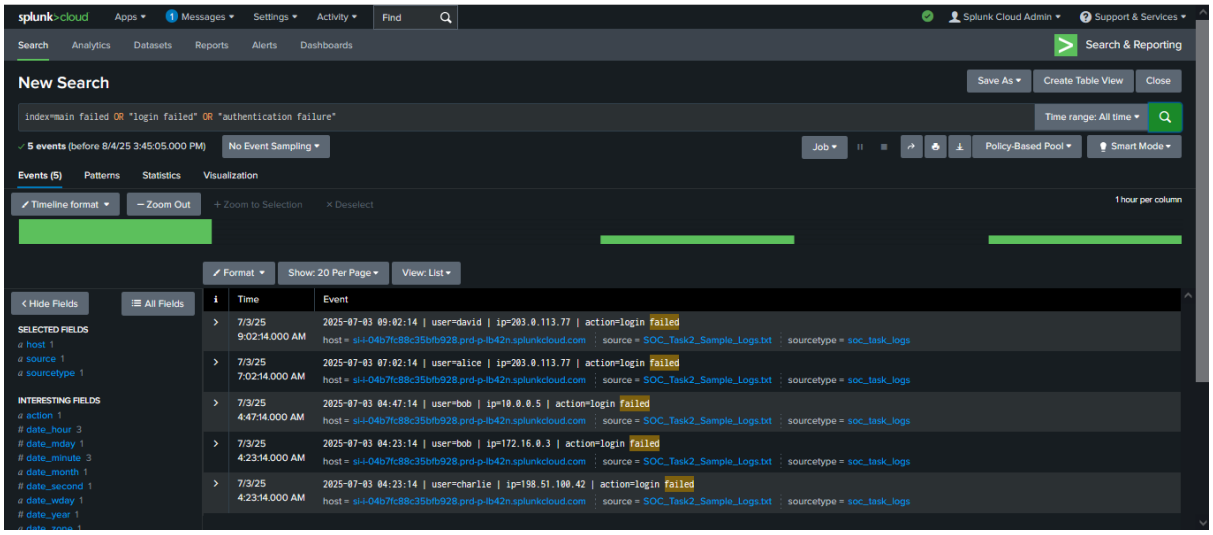
One host (`si-i-04b7fc88...`) generated over 50 logs, indicating abnormal or automated behavior. Monitoring of this host is advised.



A04 – Failed Login Attempts:

Query Used: `index=main failed OR "login failed"`

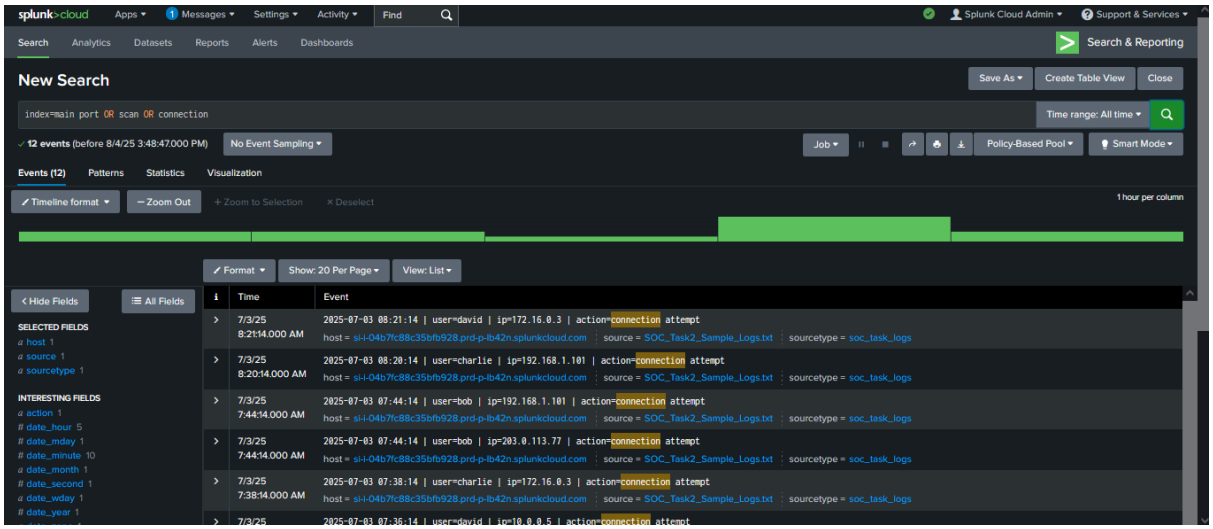
Multiple failed authentication attempts may indicate a brute-force attack. Lockouts or alerting mechanisms should be considered.



A05 –Port Scan or Network Probe:

Query Used: `index=main port OR scan OR connection`

Logs revealed several port-related or connection attempts — common indicators of port scanning or reconnaissance by threat actors.



5. Incident Report Summary:

Incident Type	IP Address	Severity	Notes
Malware Detection	172.16.0.3	High	Ransomware / Trojan detected
	10.0.0.5	High	Rootkit Signature
	172.16.0.3	High	Trojan Detected
	10.0.0.5	High	Trojan Detected
	203.0.113.77	High	Trojan Detected
Failed Login Attempts	203.0.113.77	Medium	Multiple login failures
	10.0.0.5	Medium	Brute-force suspected
	172.16.0.3	Medium	Failed login by user “bob”
	198.51.100.42	Medium	Unauthorized login attempt
High Host Activity	si-04b7fc88c35bfb928...	High	50+ log events from single host
Port Scan Activity	172.16.0.3	High	Multiple connection attempts
	192.168.1.101	High	Connection attempt – possible scan
	203.0.113.77	High	Scan behaviour
	10.0.0.5	High	Repeated scan signs

6. Conclusion:

- Used a **SIEM tool (Splunk)** for log analysis
- Wrote **basic SPL queries** to search and filter security events
- Detected **brute-force attacks** and **suspicious activities**
- Documented incidents in a **structured incident response report**

This forms the foundation of what real-world **Security Operations Center (SOC)** teams do for live incident monitoring and response.