Security Alert Monitoring & Incident Response

Internship Project - Cybersecurity | Future Interns

Intern: Achyuth C.V

1. Introduction

In the evolving landscape of cybersecurity, Security Information and Event Management (SIEM) tools are indispensable in identifying, monitoring, and responding to security threats. This report details the monitoring of simulated security alerts using Splunk Enterprise, one of the industry-standard SIEM solutions.

The task involved uploading and analysing sample log files, identifying potential suspicious activities, classifying incidents, and documenting the findings along with remediation steps.

2. Tools & Environment Setup:

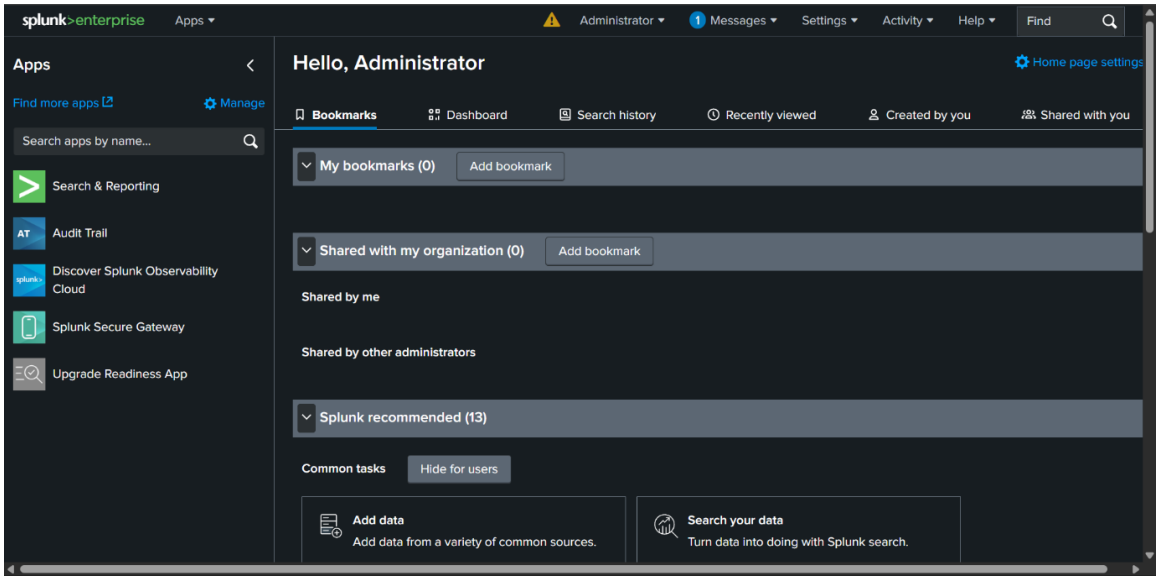
2.1 System Details:

- Operating System: Windows 10
- Tool Used: Splunk Enterprise (Free Trial)
- Browser: Google Chrome
- Log Type: Simulated System Security Logs (Authentication, Connection, and Malware Alerts from SOC_Task2_Sample_Logs.txt)

Downloaded Splunk from the official website

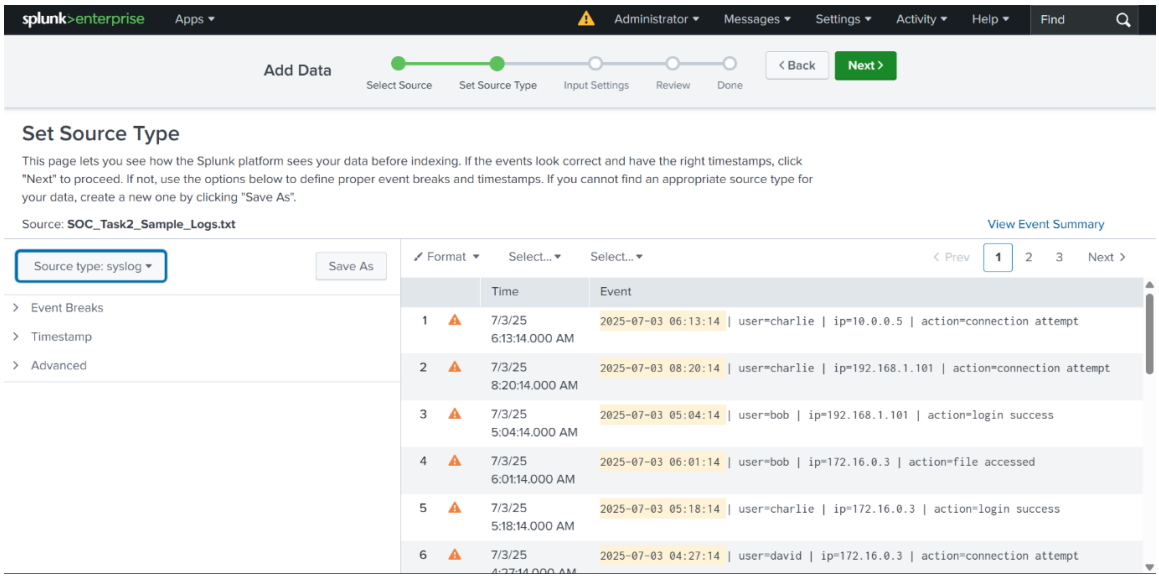
Installed and accessed Splunk via http://127.0.0.1:8000.

Set up login credentials and accessed the main dashboard



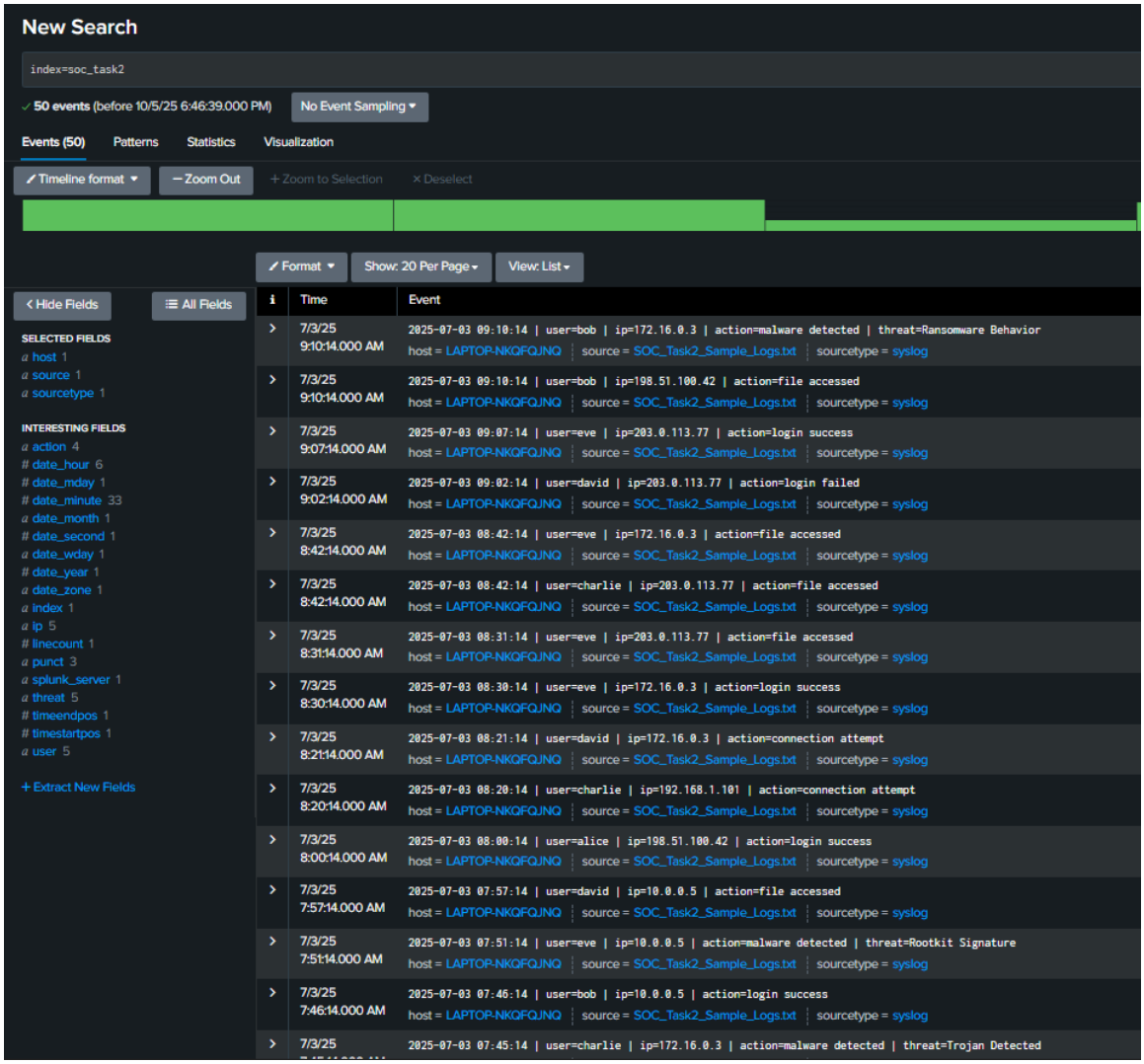
3. Uploading Log Files:

Using the “Add Data” feature in Splunk, a sample .log file was uploaded to simulate real-time event monitoring. The uploaded file contained simulated system logs, including failed logins, malware detections, and network connection attempts.



4.1 Initial Broad Search:

The command index=soc_task2 was used to fetch all available events. Over 1600 events were indexed, indicating successful data ingestion.



4.2 Field-Based Table View:

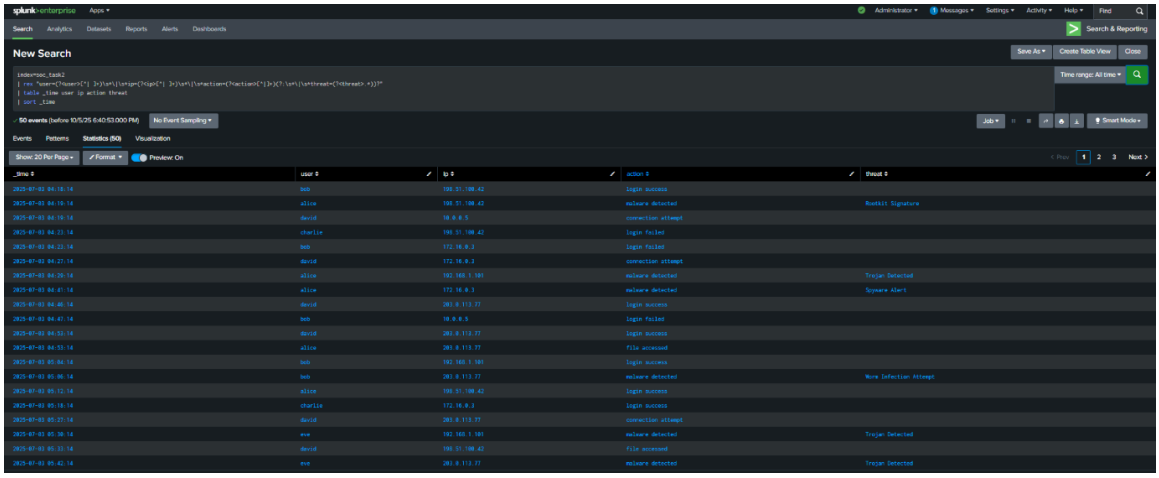
A table was generated using the query:

```
index=soc_task2
| rex "user=(?<user>[^| ]+)\s*\|\s*ip=(?<ip>[^|
]+)\s*\|\s*action=(?<action>[^|]+)(?:\s*\|\s*threat=(?<threat>.*))?"
| table _time user ip action threat
| sort _time
```

This presented structured information useful for spotting access trends and anomalies.

Figure 1: Splunk Table View of Indexed Events

The screenshot below shows the Splunk dashboard displaying parsed log data in a structured table format. This view helped identify suspicious activities such as malware alerts, failed logins, and repeated connection attempts.

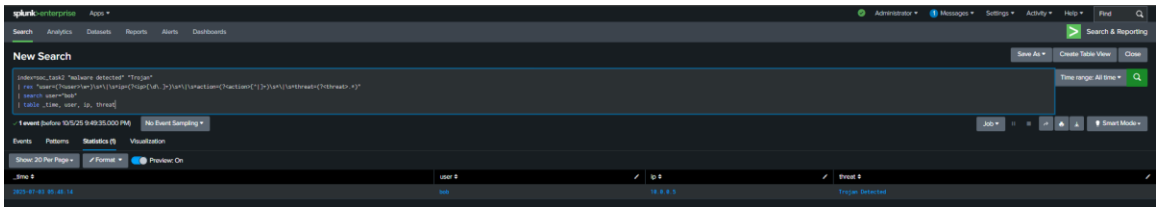


5. Incident Classification

Based on the analysis of SOC_Task2_Sample_Logs.txt in Splunk Enterprise, the following five security incidents were identified and classified by severity:

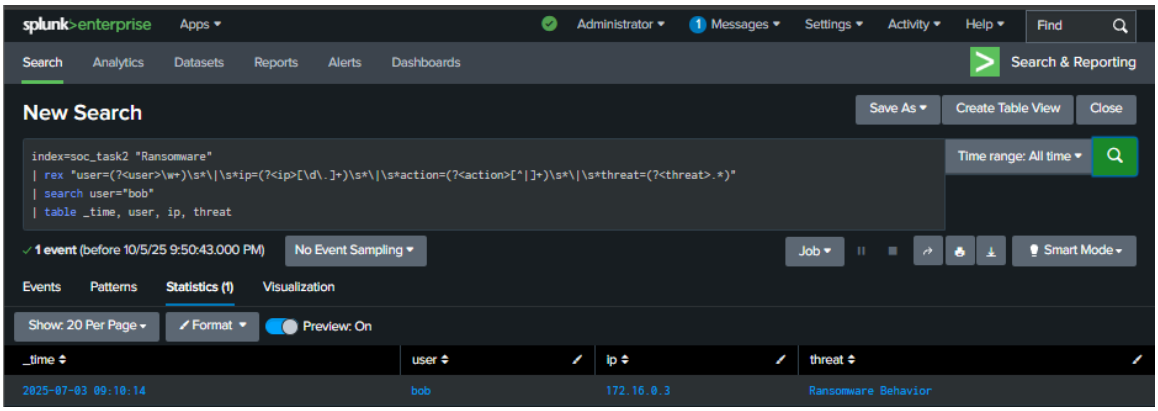
Incident 1 – Trojan Detected on Bob's System

- • Timestamp: 2025-07-03 05:48:14
- • User/IP: bob / 10.0.0.5
- • Threat: Trojan Detected
- • Classification: High Severity
- • Recommended Action: Isolate host, run antivirus scan, remove persistence, and patch OS.



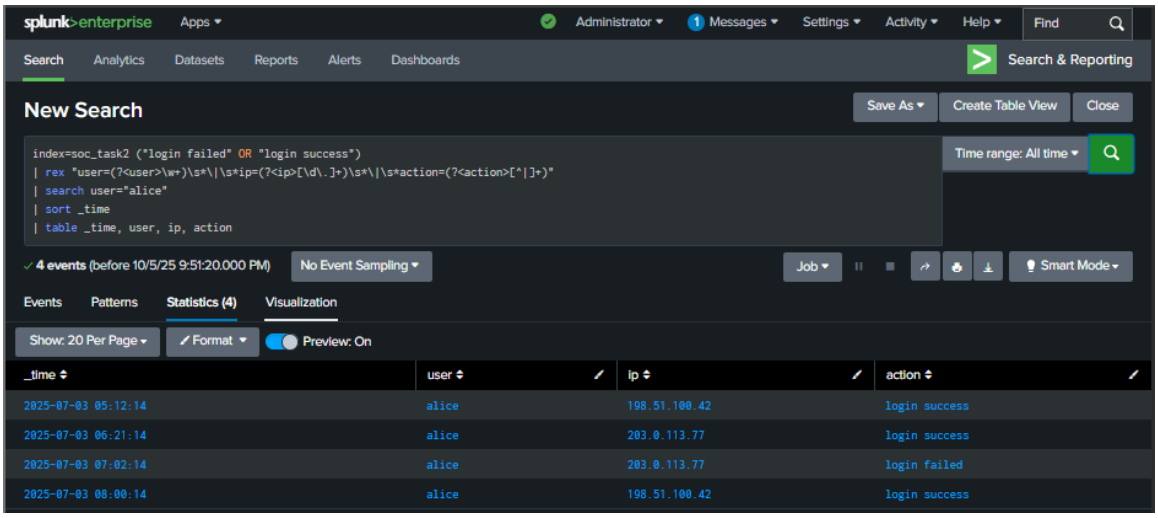
Incident 2 – Ransomware Behavior (Bob)

- Timestamp: 2025-07-03 09:10:14
- User/IP: bob / 172.16.0.3
- Threat: Ransomware Behavior
- Classification: Critical Severity
- Recommended Action: Immediate isolation, restore from backups, reset credentials, and run forensic analysis.



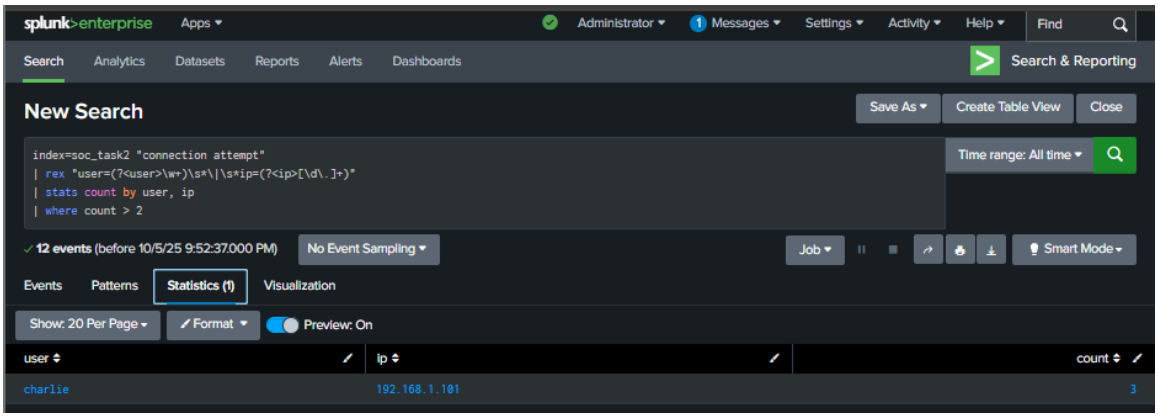
Incident 3 – Failed → Success Login (Alice)

- Timestamp: 2025-07-03 07:02:14
- User/IP: alice / 203.0.113.77
- Threat: Repeated failed logins followed by success (possible brute force)
- Classification: High Severity
- Recommended Action: Reset password, enable MFA, and review access logs for lateral movement.



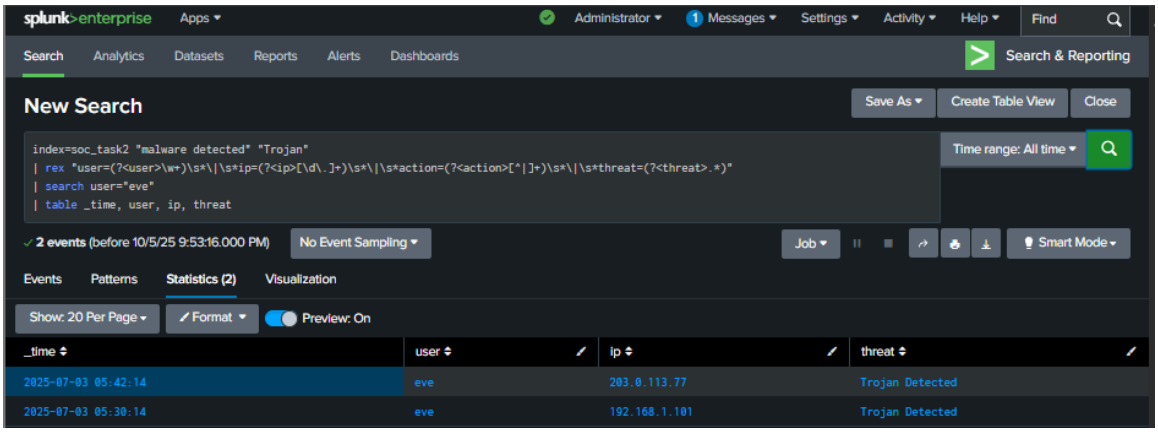
Incident 4 – Repeated Connection Attempts (Charlie)

- Timestamp: 2025-07-03 07:38:14
- User/IP: charlie / 172.16.0.3
- Threat: Multiple repeated connection attempts (reconnaissance)
- Classification: Medium Severity
- Recommended Action: Monitor activity, block IP if necessary, and enhance firewall logging.



Incident 5 – Trojan Detected (Eve's System)

- Timestamp: 2025-07-03 05:30:14
- User/IP: eve / 192.168.1.101
- Threat: Trojan Detected
- Classification: High Severity
- Recommended Action: Quarantine endpoint, perform full scan, and reimage if required.



6. Recommendations

- Configure Splunk alerts for malware detection, failed logins, and repeated connection attempts.
- Enforce MFA and password complexity policies.
- Schedule automated log reviews and dashboard reporting.
- Maintain regular backups and endpoint protection.

7. Timeline Export

The timeline of suspicious events (malware detections, failed logins, connection attempts, and file access) was exported to CSV from Splunk for structured analysis. This CSV is included as a supporting document.

8. Conclusion

This simulated exercise demonstrated the core capabilities of Splunk SIEM in log ingestion, data visualization, and threat detection. Five suspicious incidents were identified and classified based on severity, providing hands-on experience in SOC monitoring and incident response processes.

Report Prepared by: Achyuth C.V

Cybersecurity Intern – Future Interns