Security Operations Center (SOC) Project Report

Intern Name: Sanskar Dahatre
Organization: Future Interns (Cybersecurity Internship)
Project: SOC Task 2 – Security Monitoring and Incident Analysis
Date: October 30, 2025

Detailed Overview

This internship project simulates the daily operations of a Security Operations Center (SOC) where analysts monitor logs and detect cybersecurity threats using Splunk Enterprise.
The purpose was to analyze simulated network and authentication logs, identify indicators of compromise (IOCs), and respond to potential incidents following SOC playbook standards.

Tools and Techniques used

Tool / Resource	Purpose
Splunk Enterprise	For ingesting, indexing, and visualizing log data
SOC_Task2_Sample_Logs.txt	Simulated network, authentication, and malware event logs
Windows 10	System used for local Splunk setup
Google Docs / Word	Documentation and formatting assistance

Process and Methodology

1. Environment Setup

- Installed Splunk Enterprise on Windows.
- Configured local indexing for text-based log ingestion.
- Verified Splunk web interface access at http://localhost:8000.

2. Log Ingestion

- Uploaded the SOC_Task2_Sample_Logs.txt file as a data source.
- Assigned a custom sourcetype: sample logs.
- Indexed under the default main index for easy query access.

3. Log Exploration (Search & Analysis)

Executed search queries in Splunk Search Head to analyze log events:

```
index="main" sourcetype="sample logs"
index="main" sourcetype="sample logs" action="login failed"
index="main" sourcetype="sample logs" action="malware detected"
```

This helped identify repeated login failures, malware infections, and connections from unusual IP addresses.

4. Visualization & Dashboard Creation

Built a custom Splunk dashboard including:

- Bar Chart: Number of login failures by user
- Pie Chart: Malware types detected
- Line Chart: Timeline of security incidents
- Table Panel: List of all suspicious IP addresses
- Single Value Panel**:** Total number of high-severity incidents

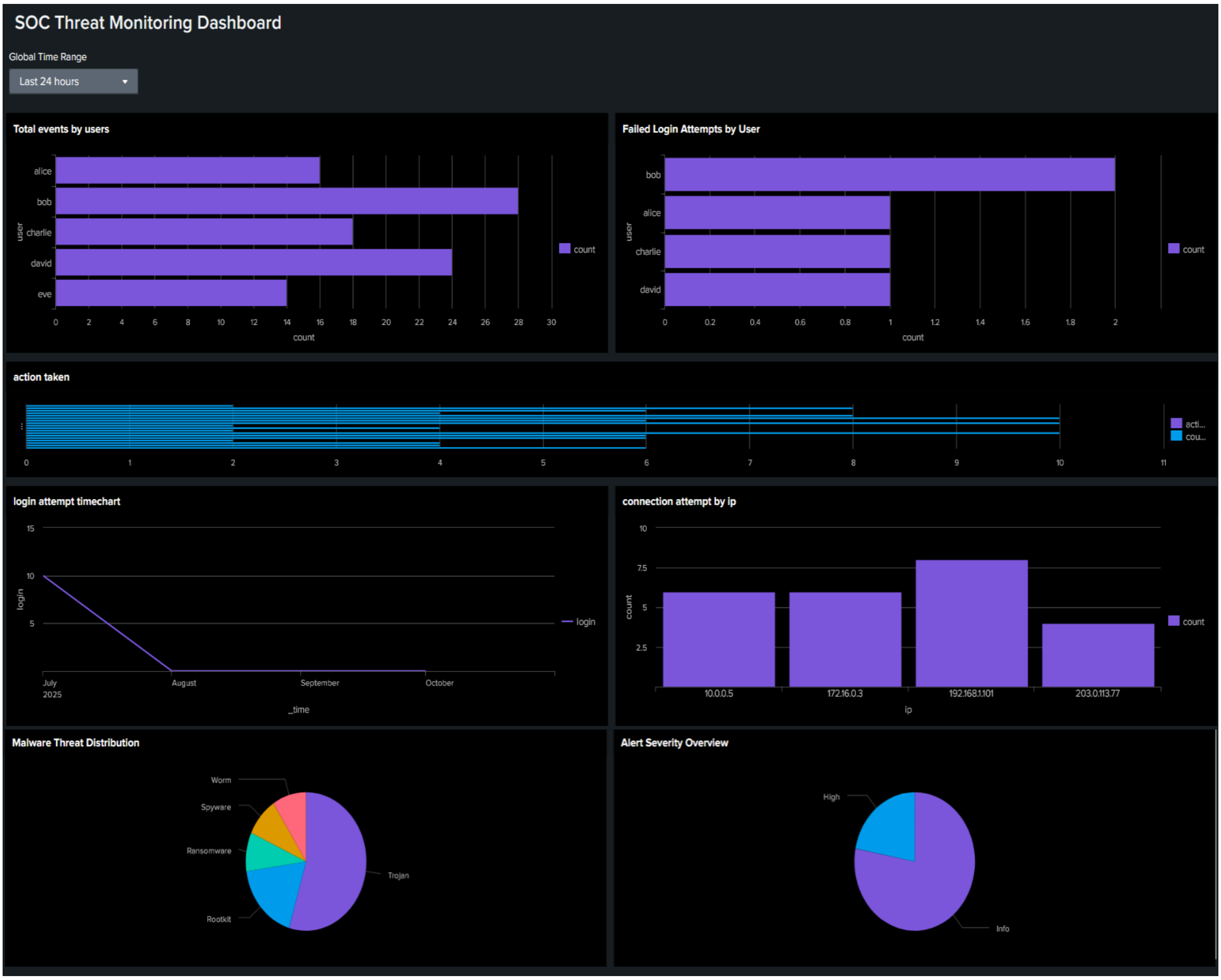
The dashboard gave a real-time SOC-style visualization of system health and threat indicators.

5. Incident Identification

From the logs and visualizations, suspicious behaviors were observed:

- Multiple failed logins from the same IP (203.0.113.77)
- Trojan, Rootkit, and Ransomware activity across different users
- Repeated connections from potentially compromised hosts (10.0.0.5, 172.16.0.3)

Dashboards



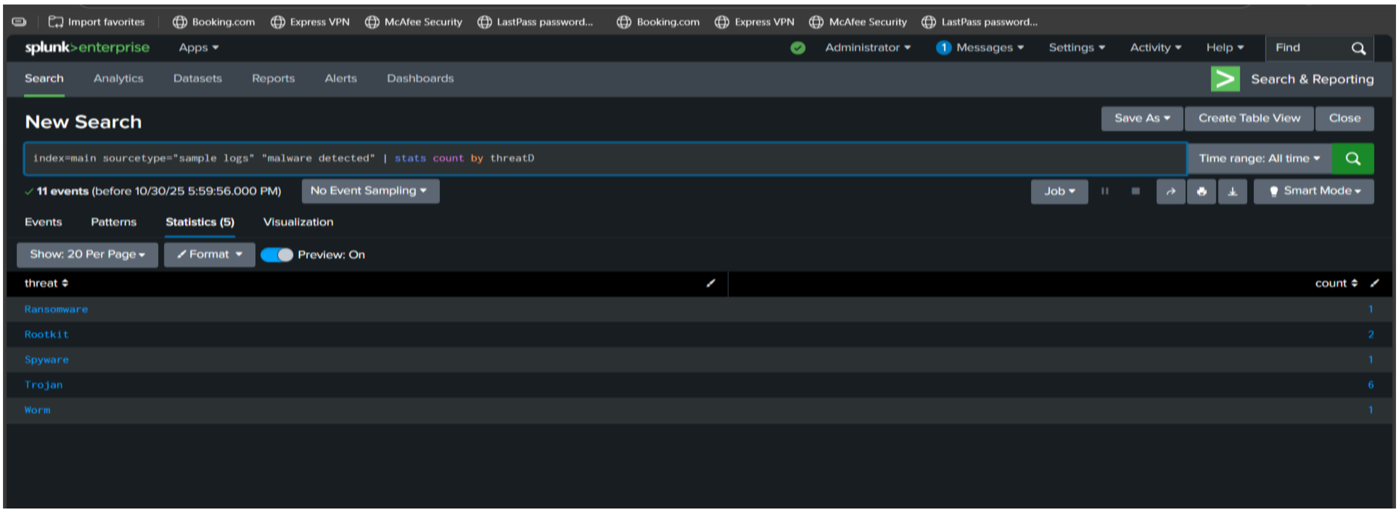
Log Summary

Data Source: SOC_Task2_Sample_Logs.txt Log Volume: 20 events (simulated)
Log Types: Authentication, Connection, File Access, and Malware Detection Events.

Suspicious Activity Identified

Timestamp	User	IP Address	Action	Threat/Details
2025-07-03 09:10:14	bob	172.16.0.3	malware detected	Ransomware Behavior
2025-07-03 07:51:14	eve	10.0.0.5	malware detected	Rootkit Signature
2025-07-03 07:45:14	charlie	172.16.0.3	malware detected	Trojan Detected
2025-07-03 09:02:14	david	203.0.113.77	login failed	Possible brute-force attempt
2025-07-03 07:44:14	bob	203.0.113.77	connection attempt	Repeated suspicious outbound connections

Screenshots of analyzed Events



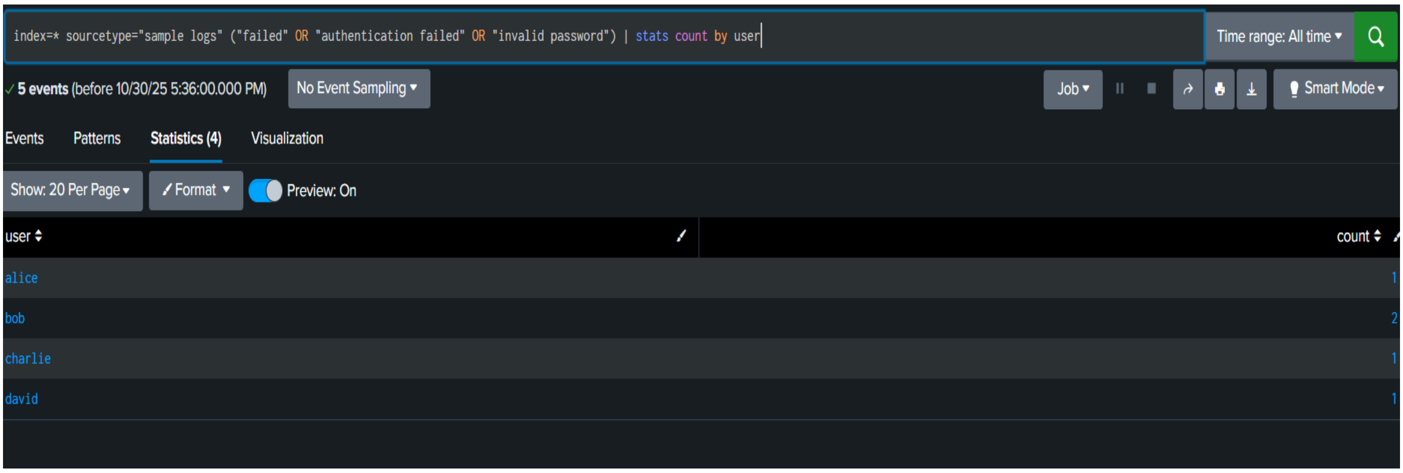
New Search

```
index=main sourcetype="sample logs" "malware detected" | stats count by threatD
```

✓ 11 events (before 10/30/25 5:59:56.000 PM) No Event Sampling

Statistics (5)

threat	count
Ransomware	1
Rootkit	2
Spyware	1
Trojan	6
Worm	1

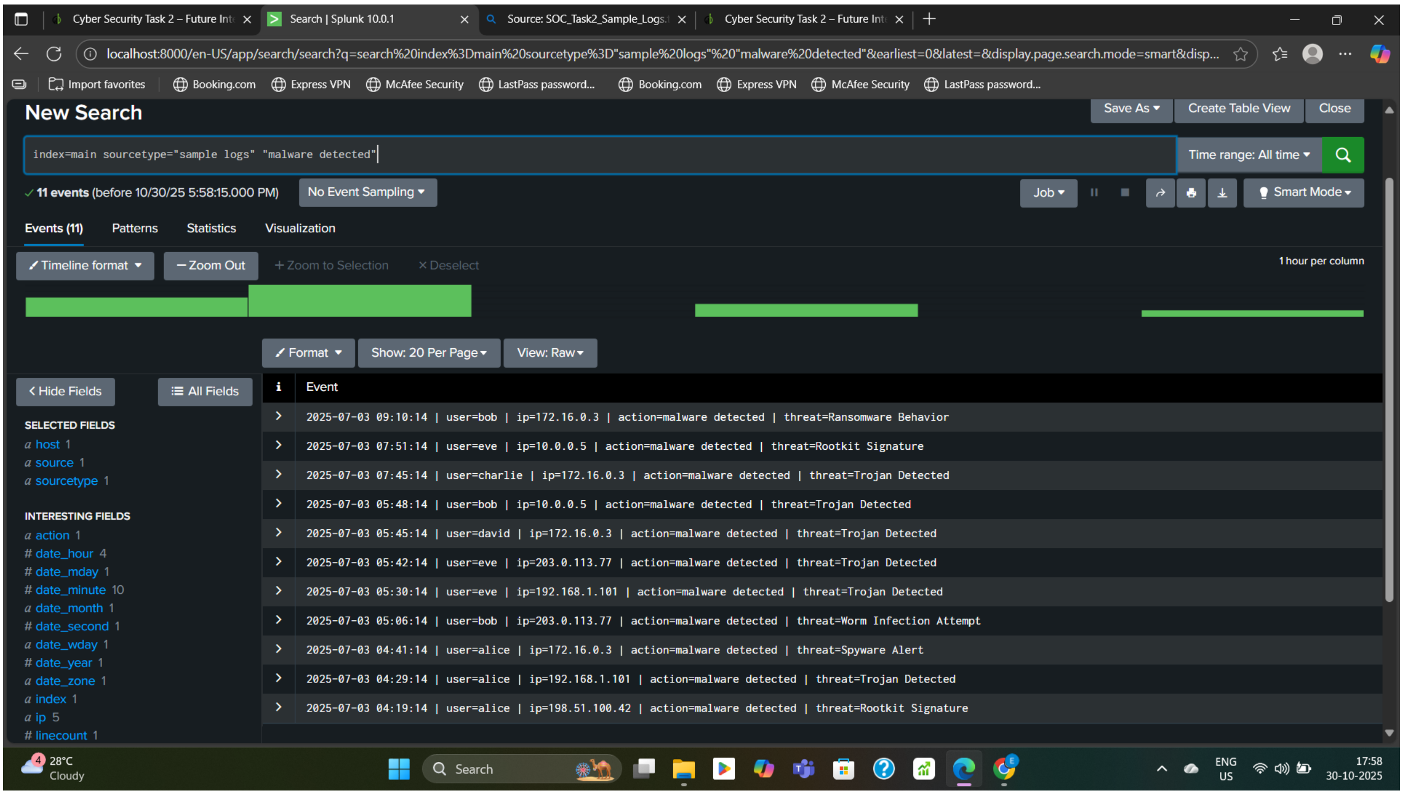


```
index=* sourcetype="sample logs" ("failed" OR "authentication failed" OR "invalid password") | stats count by user
```

✓ 5 events (before 10/30/25 5:36:00.000 PM) No Event Sampling

Statistics (4)

user	count
alice	1
bob	2
charlie	1
david	1



New Search

```
index=main sourcetype="sample logs" "malware detected"
```

✓ 11 events (before 10/30/25 5:58:15.000 PM) No Event Sampling

Events (11)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 1
# date_hour 4
# date_mday 1
# date_minute 10
a date_month 1
# date_second 1
a date_wday 1
# date_year 1
a date_zone 1
a index 1
a ip 5
# linecount 1

```
2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature
2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected
2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected
2025-07-03 05:30:14 | user=eve | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt
2025-07-03 04:41:14 | user=alice | ip=172.16.0.3 | action=malware detected | threat=Spyware Alert
2025-07-03 04:29:14 | user=alice | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
2025-07-03 04:19:14 | user=alice | ip=198.51.100.42 | action=malware detected | threat=Rootkit Signature
```

Analysis & Findings

1. Compromised Hosts: IPs 10.0.0.5 and 172.16.0.3 show consistent malware activity.
2. Credential Attack: Brute-force attempts observed on David’s account.
3. Malware Spread: Trojan and ransomware activity indicates lateral movement.
4. Insider Risk: Eve accessed multiple infected hosts, possibly compromised.

Incident Classification

Category	Description	User(s)	IPs Involved	Severity
Malware Infection	Trojan, Rootkit, Ransomware signatures detected	bob, charlie, eve	10.0.0.5, 172.16.0.3	High
Failed Login Attempts	Brute-force or unauthorized access attempts	david	203.0.113.77	Medium
Unusual File Access	Access to sensitive files from multiple accounts	eve	172.16.0.3	Medium
Suspicious Network Traffic	Repeated connection attempts from the same IPs	charlie, bob	192.168.1.101	Low

Recommended Actions

1. Contain: Isolate infected hosts, disable compromised accounts.
2. Eradicate: Run EDR/AV scans, reset credentials.
3. Recover: Restore systems from backups, monitor traffic.
4. Prevent: Enforce MFA, lockout policies, and user training.

Incident Communication (Email Template)

Subject: Security Incident Alert – Malware and Unauthorized Access Detected Dear Team

During routine Splunk log monitoring, suspicious activities were identified:
- Malware detections (Trojan, Ransomware, Rootkit) on 10.0.0.5 and 172.16.0.3
- Failed logins and unauthorized file access from users Bob, Charlie, and Eve
- External access attempts from 203.0.113.77

These incidents are classified as HIGH severity. Immediate actions: isolate systems, reset passwords, and perform scans.

Best Regards, Sanskar Dahatre
SOC Intern – FutureInterns

Learning Outcomes

- Hands-on experience with **SIEM tools** and **log analysis**.
- Understanding **incident lifecycle management** (Detection → Response → Recovery).
- Developed skills in **threat classification, visualization, and documentation**.
- Learned to simulate a **SOC analyst's workflow** for monitoring and reporting.

Conclusion

This project successfully replicated a miniature SOC environment, demonstrating the complete flow of threat detection, analysis, and response using Splunk.

By identifying real security patterns in simulated logs and documenting the response professionally, this task strengthened analytical, technical, and communication skills essential for a cybersecurity analyst role.