

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:

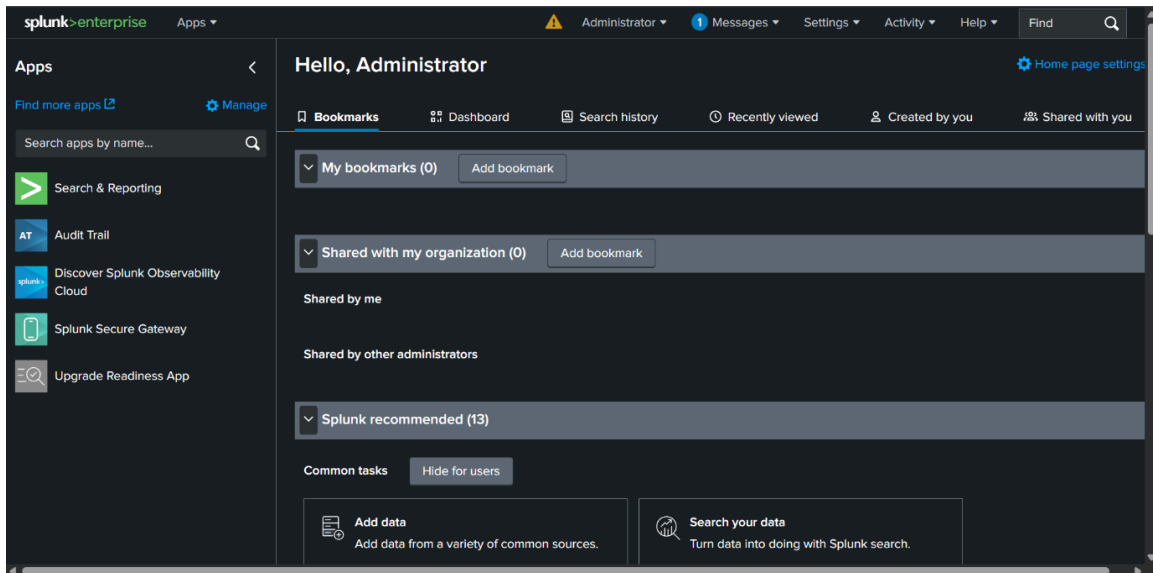
2.1 System Details:

- 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

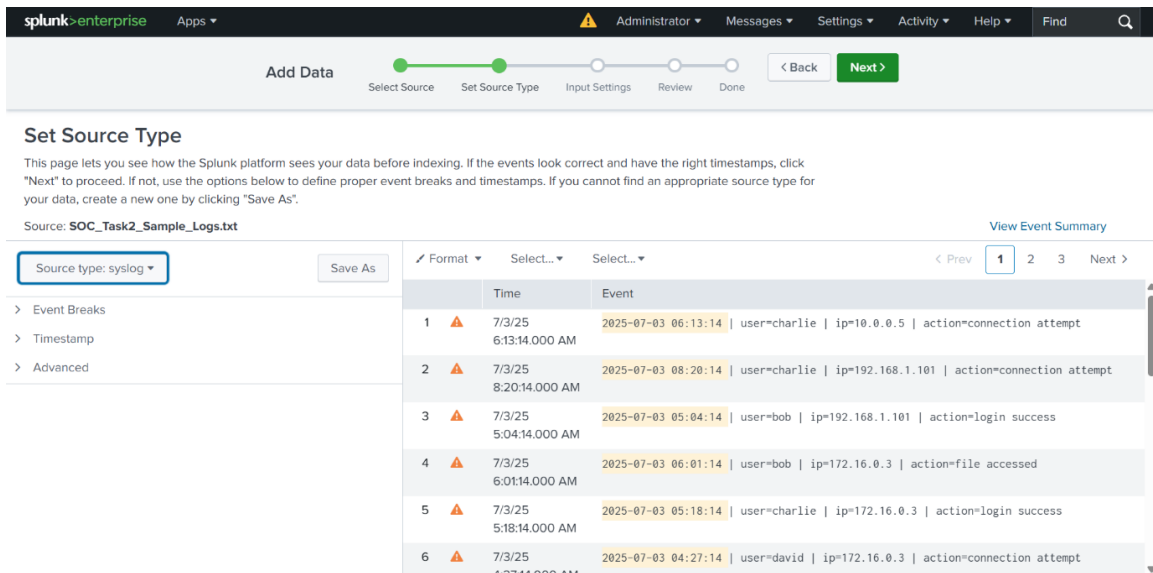
Installed and accessed Splunk via <http://127.0.0.1:8000>.

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.

New Search

index=soc_task2

✓ 50 events (before 10/5/25 6:46:39.000 PM) No Event Sampling ▼

Events (50) Patterns Statistics Visualization

Timeline format ▼ Zoom Out + Zoom to Selection × Deselect

Format ▼ Show: 20 Per Page ▼ View: List ▼

< Hide Fields	≡ All Fields	i	Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1		>	7/3/25 9:10:14.000 AM	2025-07-03 09:10:14 user=bob ip=172.16.0.3 action=malware detected threat=Ransomware Behavior host = LAPTOP-NKQFQJNQ source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
		>	7/3/25 9:10:14.000 AM	2025-07-03 09:10:14 user=bob ip=198.51.100.42 action=file accessed host = LAPTOP-NKQFQJNQ source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
INTERESTING FIELDS a action 4 # date_hour 6 # date_mday 1 # date_minute 33 # date_month 1 # date_second 1 # date_wday 1 # date_year 1 a date_zone 1 a index 1 a ip 5 # linecount 1 a punct 3 a splunk_server 1 a threat 5 # timeendpos 1 # timestartpos 1 a user 5		>	7/3/25 9:07:14.000 AM	2025-07-03 09:07:14 user=eve ip=203.0.113.77 action=login success host = LAPTOP-NKQFQJNQ source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
		>	7/3/25 9:02:14.000 AM	2025-07-03 09:02:14 user=david ip=203.0.113.77 action=login failed host = LAPTOP-NKQFQJNQ source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
		>	7/3/25 8:42:14.000 AM	2025-07-03 08:42:14 user=eve ip=172.16.0.3 action=file accessed host = LAPTOP-NKQFQJNQ source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
		>	7/3/25 8:42:14.000 AM	2025-07-03 08:42:14 user=charlie ip=203.0.113.77 action=file accessed host = LAPTOP-NKQFQJNQ source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
		>	7/3/25 8:31:14.000 AM	2025-07-03 08:31:14 user=eve ip=203.0.113.77 action=file accessed host = LAPTOP-NKQFQJNQ source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
		>	7/3/25 8:30:14.000 AM	2025-07-03 08:30:14 user=eve ip=172.16.0.3 action=login success host = LAPTOP-NKQFQJNQ source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
		>	7/3/25 8:21:14.000 AM	2025-07-03 08:21:14 user=david ip=172.16.0.3 action=connection attempt host = LAPTOP-NKQFQJNQ source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
		>	7/3/25 8:20:14.000 AM	2025-07-03 08:20:14 user=charlie ip=192.168.1.101 action=connection attempt host = LAPTOP-NKQFQJNQ source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
		>	7/3/25 8:00:14.000 AM	2025-07-03 08:00:14 user=alice ip=198.51.100.42 action=login success host = LAPTOP-NKQFQJNQ source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
		>	7/3/25 7:57:14.000 AM	2025-07-03 07:57:14 user=david ip=10.0.0.5 action=file accessed host = LAPTOP-NKQFQJNQ source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
		>	7/3/25 7:51:14.000 AM	2025-07-03 07:51:14 user=eve ip=10.0.0.5 action=malware detected threat=Rootkit Signature host = LAPTOP-NKQFQJNQ source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
		>	7/3/25 7:46:14.000 AM	2025-07-03 07:46:14 user=bob ip=10.0.0.5 action=login success host = LAPTOP-NKQFQJNQ source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
		>	7/3/25 7:45:14.000 AM	2025-07-03 07:45:14 user=charlie ip=172.16.0.3 action=malware detected threat=Trojan Detected host = LAPTOP-NKQFQJNQ source = SOC_Task2_Sample_Logs.txt sourcetype = syslog

+ Extract New Fields

4.2 Field-Based Table View:

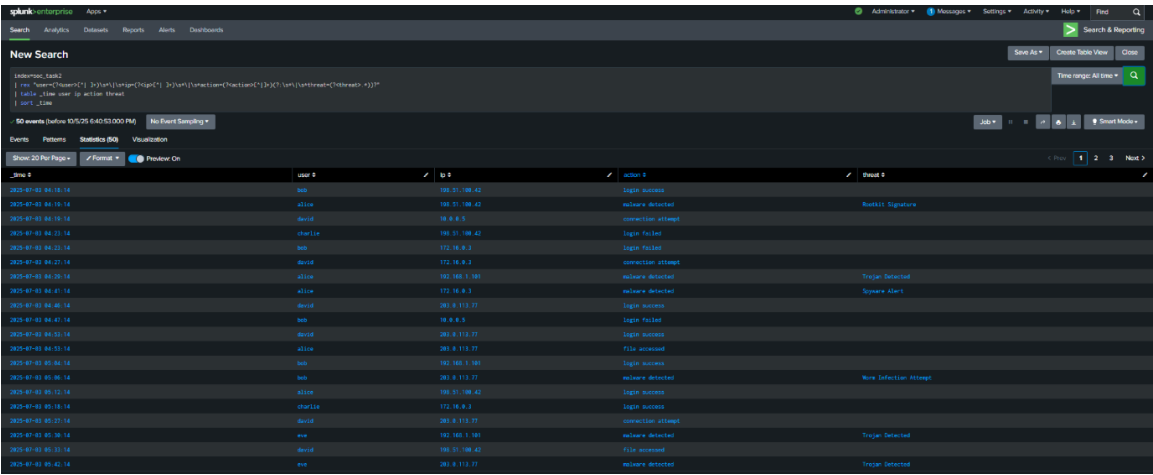
A table was generated using the query:

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



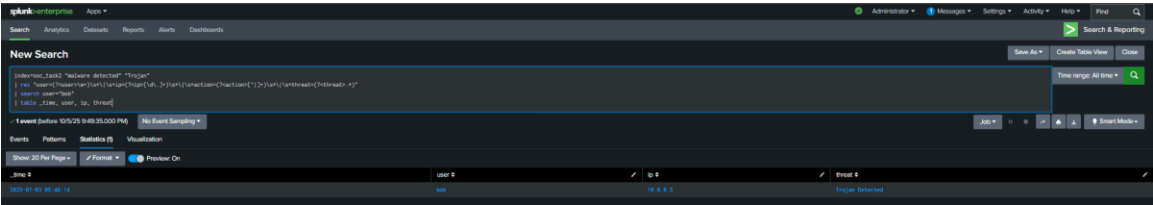
_time	user	ip	action	threat
2025-07-03 05:18:14	bob	192.07.198.42	login success	
2025-07-03 05:18:14	alice	192.07.198.42	malware detected	Rootkit, Signature
2025-07-03 05:18:14	bob	192.07.198.42	connection attempt	
2025-07-03 05:18:14	charlie	192.07.198.42	login failed	
2025-07-03 05:18:14	bob	172.16.8.3	login failed	
2025-07-03 05:22:14	alice	172.16.8.3	connection attempt	
2025-07-03 05:25:14	alice	192.168.1.181	malware detected	Trojan Detected
2025-07-03 05:45:14	alice	172.16.8.3	malware detected	Spware Alert
2025-07-03 05:46:14	bob	261.8.112.77	login success	
2025-07-03 05:46:14	bob	192.07.198.42	login failed	
2025-07-03 05:50:14	bob	261.8.112.77	login success	
2025-07-03 05:50:14	alice	261.8.112.77	file accessed	
2025-07-03 05:50:14	bob	192.168.1.181	login success	
2025-07-03 05:50:14	bob	261.8.112.77	malware detected	Worm Infection Storage
2025-07-03 05:52:14	alice	192.07.198.42	login success	
2025-07-03 05:58:14	charlie	172.16.8.3	login success	
2025-07-03 06:02:14	alice	261.8.112.77	connection attempt	
2025-07-03 06:10:14	eve	192.168.1.181	malware detected	Trojan Detected
2025-07-03 06:33:14	bob	192.07.198.42	file accessed	
2025-07-03 06:42:14	eve	261.8.112.77	malware detected	Trojan Detected

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.



_time	user	ip	threat
2025-07-03 05:48:14	bob	192.07.198.42	Trojan Detected

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.

The screenshot shows the Splunk Enterprise Search interface. The search bar contains the following query:

```
index=soc_task2 "Ransomware"
| rex "user=(?<user>\w+)\s*\s*ip=(?<ip>[\d\.]+)\s*\s*action=(?<action>[^\s]+)\s*\s*threat=(?<threat>.*)"
| search user="bob"
| table _time, user, ip, threat
```

The search results show 1 event (before 10/5/25 9:50:43.000 PM). The event details are as follows:

_time	user	ip	threat
2025-07-03 09:10:14	bob	172.16.0.3	Ransomware Behavior

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.

The screenshot shows the Splunk Enterprise Search interface. The search bar contains the following query:

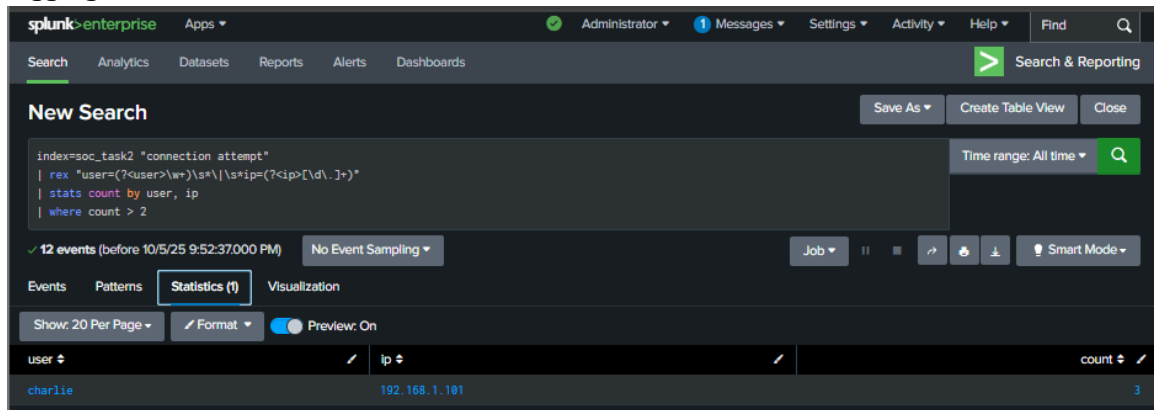
```
index=soc_task2 ("login failed" OR "login success")
| rex "user=(?<user>\w+)\s*\s*ip=(?<ip>[\d\.]+)\s*\s*action=(?<action>[^\s]+)"
| search user="alice"
| sort _time
| table _time, user, ip, action
```

The search results show 4 events (before 10/5/25 9:51:20.000 PM). The event details are as follows:

_time	user	ip	action
2025-07-03 05:12:14	alice	198.51.100.42	login success
2025-07-03 06:21:14	alice	203.0.113.77	login success
2025-07-03 07:02:14	alice	203.0.113.77	login failed
2025-07-03 08:00:14	alice	198.51.100.42	login success

Incident 4 – Repeated Connection Attempts (Charlie)

- Timestamp: 2025-07-03 07:38:14
- User/IP: charlie / 192.168.0.3
- Threat: Multiple repeated connection attempts (reconnaissance)
- Classification: Medium Severity
- Recommended Action: Monitor activity, block IP if necessary, and enhance firewall logging.

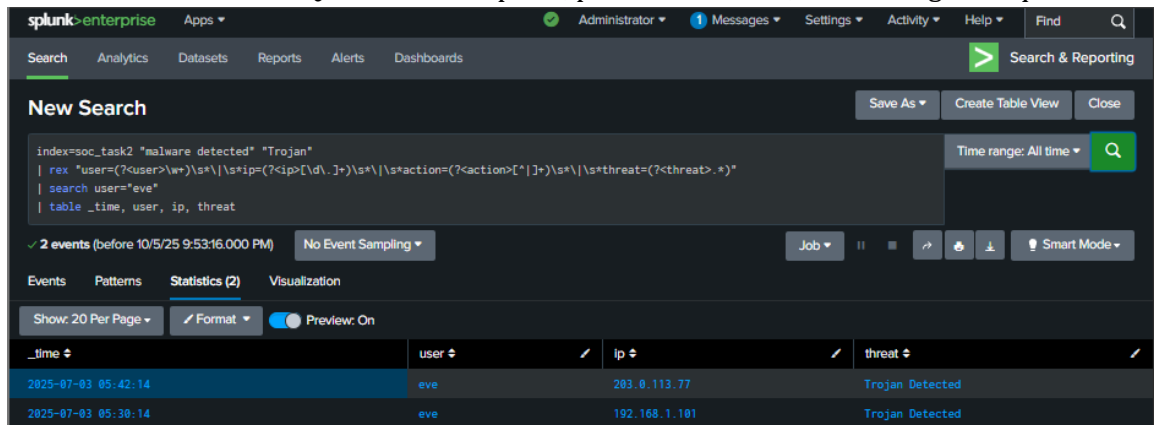


The screenshot shows the Splunk Enterprise interface with a search query: `index=soc_task2 "connection attempt"`. The results show 12 events, with the first event being a connection attempt from user 'charlie' at IP '192.168.1.101'.

user	ip	count
charlie	192.168.1.101	3

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.



The screenshot shows the Splunk Enterprise interface with a search query: `index=soc_task2 "malware detected" "Trojan"`. The results show 2 events, with the first event being a Trojan detected on user 'eve' at IP '203.0.113.77'.

_time	user	ip	threat
2025-07-03 05:42:14	eve	203.0.113.77	Trojan Detected
2025-07-03 05:30:14	eve	192.168.1.101	Trojan Detected

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