

TASK 2 REPORT

Task Title: SIEM-Based Incident Monitoring and Analysis

Track Code: FUTURE_CS_02

Intern Name: Sarita Sharma

Aim:

The objective is to use a SIEM tool (Splunk) to track and analyze simulated security logs, aiming to detect potential threats such as unusual login behavior, brute-force attacks, malware activity and patterns between users and IP addresses. This task replicates real-world threat detection scenarios using custom log data to derive meaningful security insights.

Tools Used:

- **SIEM Tool:** Splunk (Free Trial)
- **Environment:** Custom formatted log file
- **Log File Analyzed:** SOC_Task2_Sample_Logs.txt

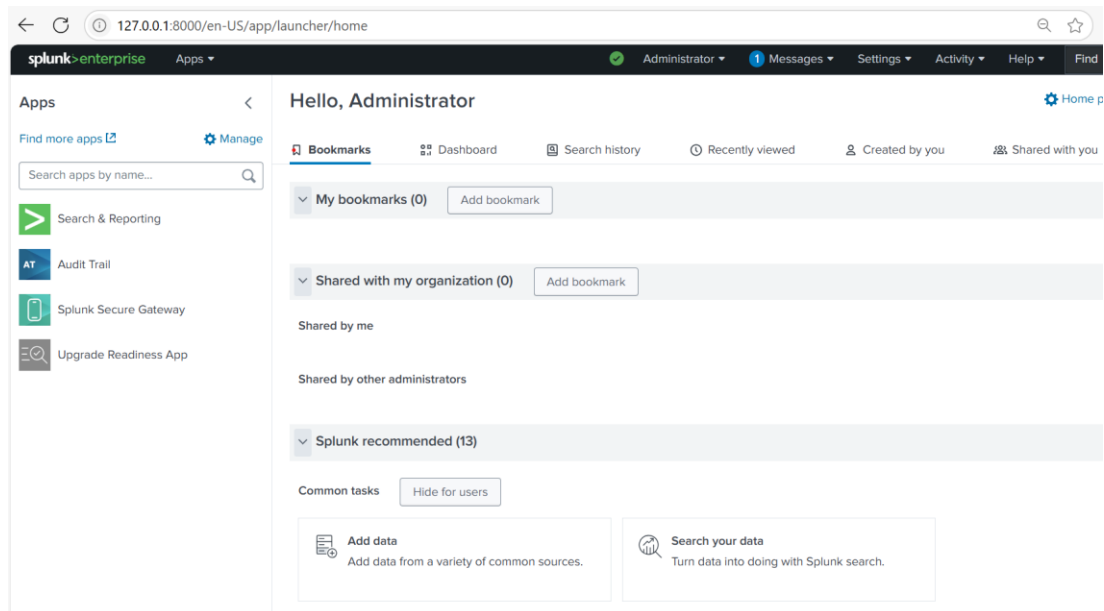
Procedure & Findings:

The log file was imported into Splunk using the upload feature. Several searches were performed uncover:

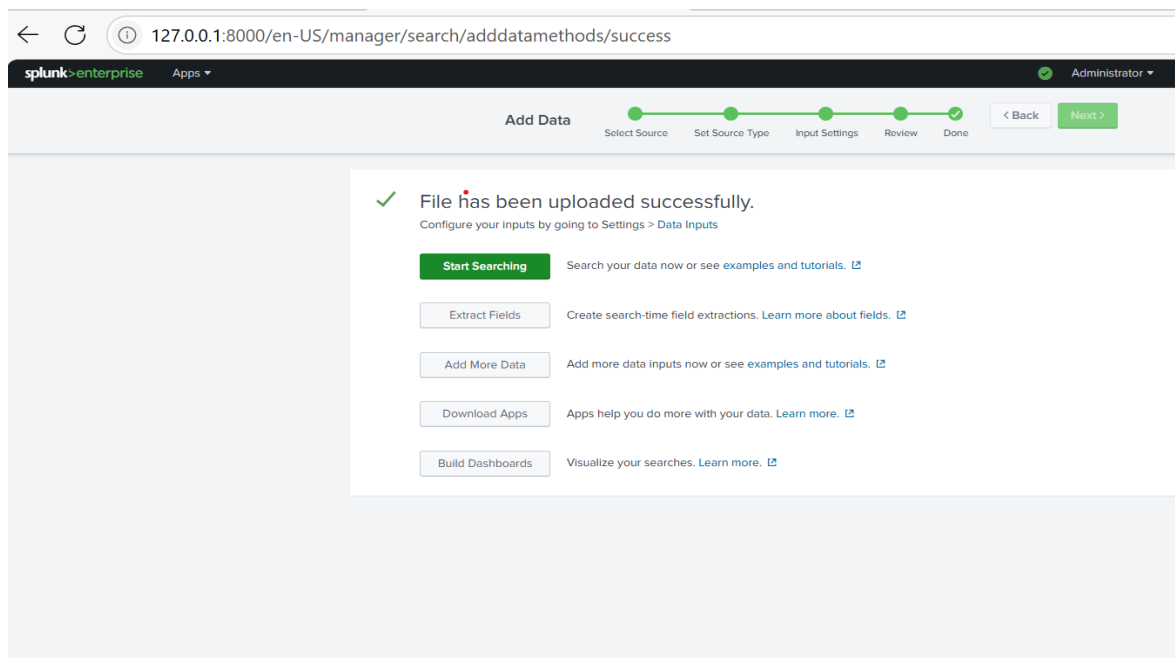
- Unusual login patterns, such as multiple failed attempts
- Successful logins following repeated failures, indicating possible account compromise
- Malware detections linked to specific users or IP addresses

Each search result was examined visually and analyzed using statistical tools to gain deeper insights.

I created a Splunk account and navigated to the dashboard interface.



After that, I uploaded the provided sample log file (“SOC_Task2_Sample_Logs”) to begin the analysis.



Next, I set up the Splunk data input by choosing the necessary event log types: Application, Security, and System—and assigned a default index to monitor Windows event logs.

The screenshot shows the 'Name' field set to 'localhost'. Under the 'Logs' section, there are two lists: 'Available log(s)' and 'Selected log(s)'. The 'Available log(s)' list contains 'MF_MediaFoundationDeviceMFT', 'MF_MediaFoundationDeviceProxy', 'Security' (checked), 'Setup', and 'System'. The 'Selected log(s)' list contains 'Application', 'Security', and 'System'. Below these lists is a note: 'Select the Windows Event Logs you want to index from the list.' At the bottom, the 'Index' field is set to 'default'. There are 'Cancel' and 'Save' buttons at the bottom right.

Name	Value
Name	localhost

Logs

Available log(s)

MF_MediaFoundationDeviceMFT

MF_MediaFoundationDeviceProxy

Security ✓

Setup

System

Add all >

Selected log(s)

Application

Security

System

< Remove all

Select the Windows Event Logs you want to index from the list.

Index

Set the destination index for this source

default

Cancel

Save

I then ran a wildcard search (*) in Splunk to confirm that the logs were ingested correctly, which returned over 117,838 events for detailed analysis.

The screenshot shows the Splunk search results page. The top navigation bar includes 'splunk>enterprise' and 'Apps'. The main navigation bar includes 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'Search' tab is selected. The page title is 'New Search'. The search query is '*'. The results show '✓ 117,838 events (before 7/19/25 4:50:49.000 PM)' and 'No Event Sampling'. Below the results, there are tabs for 'Events (117,838)', 'Patterns', 'Statistics', and 'Visualization'. The 'Events (117,838)' tab is selected.

splunk>enterprise

Apps

Search

Analytics

Datasets

Reports

Alerts

Dashboards

New Search

*

✓ 117,838 events (before 7/19/25 4:50:49.000 PM)

No Event Sampling

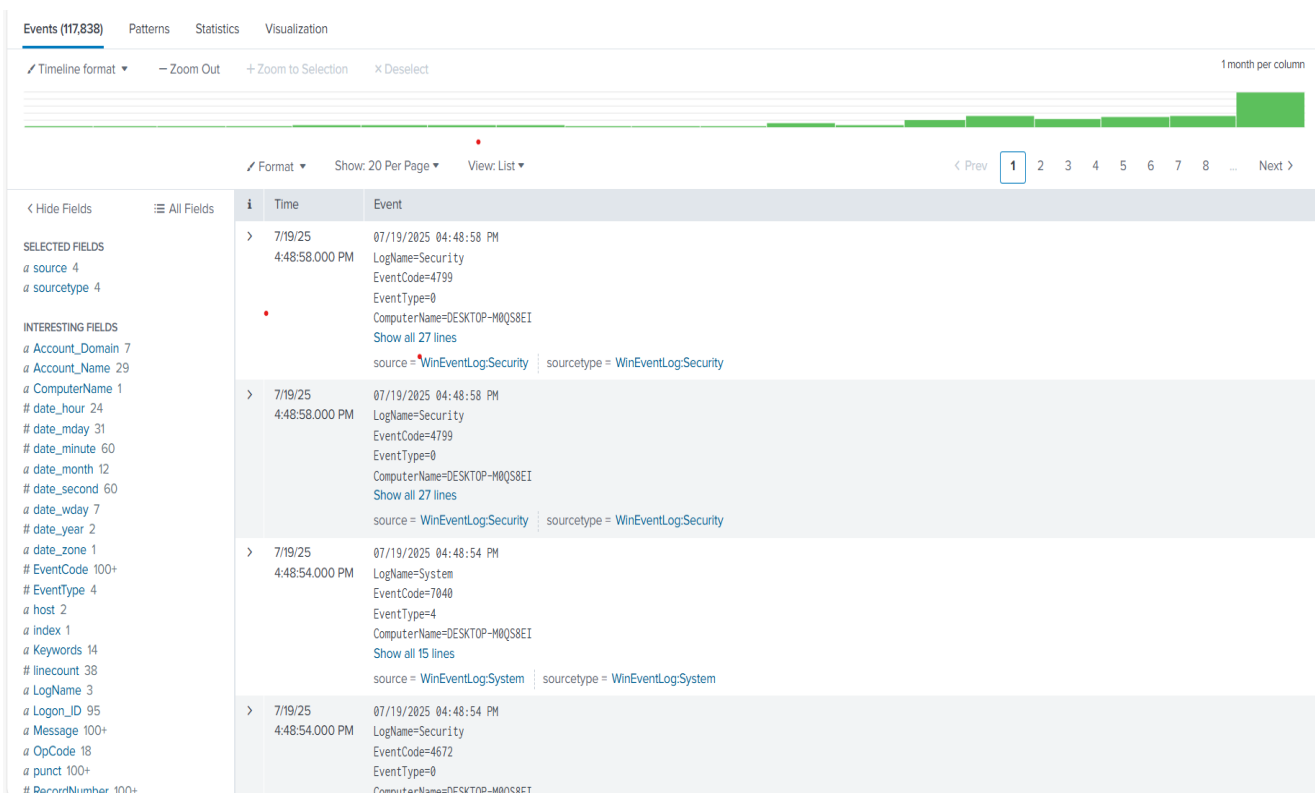
Events (117,838)

Patterns

Statistics

Visualization

After doing that, the logs appeared as follows:



Tasks Performed:

Splunk Queries Used

1. Search for Failed Logins:

```
Index =* source="SOC_Task2_Sample_Logs.txt" "action=login failed"
```

It retrieved a list of users and their corresponding IPs involved in failed login events.

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `index=* source="SOC_Task2_Sample_Logs.txt" "action=login failed"`. The results show 5 events. The table below summarizes the data:

i	Time	Event
>	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 = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	7/3/25 7:02:14.000 AM	2025-07-03 07:02:14 user=alice ip=203.0.113.77 action=login failed host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	7/3/25 4:47:14.000 AM	2025-07-03 04:47:14 user=bob ip=10.0.0.5 action=login failed host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	7/3/25 4:23:14.000 AM	2025-07-03 04:23:14 user=bob ip=172.16.0.3 action=login failed host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	7/3/25 4:23:14.000 AM	2025-07-03 04:23:14 user=charlie ip=198.51.100.42 action=login failed host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file

2. Search for Successful Logins:

```
Index =* source="SOC_Task2_Sample_Logs.txt" "action=login success"
```

This query returned a list of IP addresses and users with successful logins for comparison with the above results.

New Search

index=* source="SOC_Task2_Sample_Logs.txt" "action=login success"

✓ 11 events (before 7/18/25 10:58:22.000 PM) No Event Sampling ▼

Events (11) Patterns Statistics Visualization

✓ Timeline format ▾ — Zoom Out + Zoom to Selection × Deselect

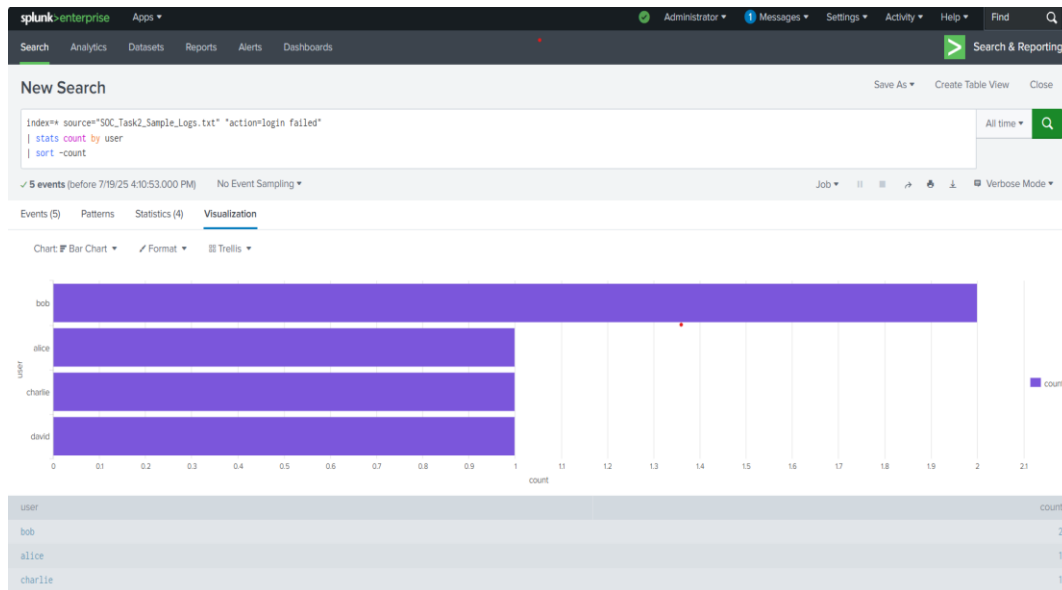
i	Time	Event
>	7/3/25 9:07:14.000 AM	2025-07-03 09:07:14 user=eve ip=203.0.113.77 action=login success host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	7/3/25 8:30:14.000 AM	2025-07-03 08:30:14 user=eve ip=172.16.0.3 action=login success host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	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 = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	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 = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	7/3/25 6:21:14.000 AM	2025-07-03 06:21:14 user=alice ip=203.0.113.77 action=login success host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	7/3/25 5:18:14.000 AM	2025-07-03 05:18:14 user=charlie ip=172.16.0.3 action=login success host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	7/3/25 5:12:14.000 AM	2025-07-03 05:12:14 user=alice ip=198.51.100.42 action=login success host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	7/3/25 5:04:14.000 AM	2025-07-03 05:04:14 user=bob ip=192.168.1.101 action=login success host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file

3. Failed Logins by User

stats count by user

| sort -count

It returned a list of users most frequently targeted by attacks.



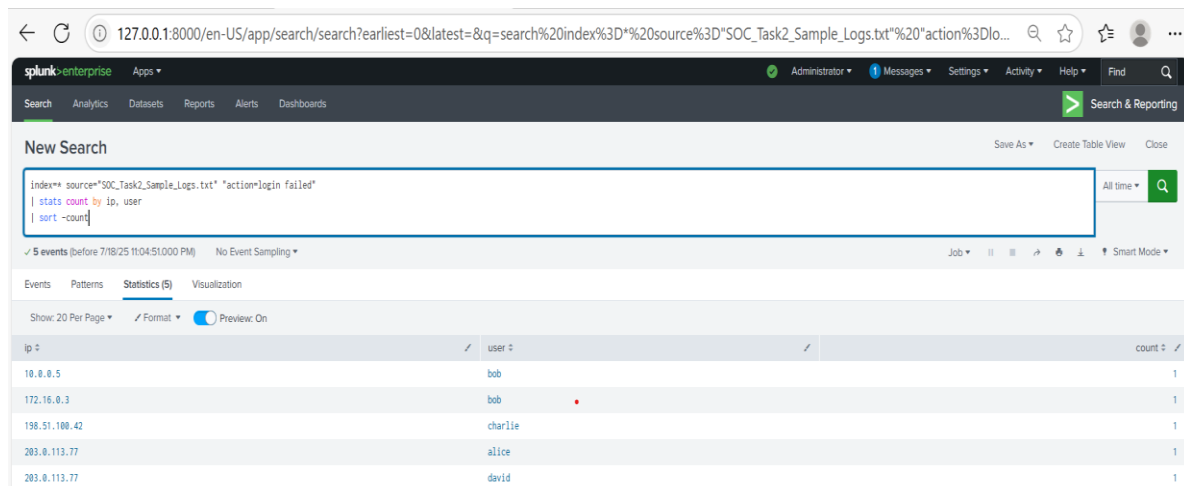
4. Frequent Login Failures from IPs

Index =* source="SOC_Task2_Sample_Logs.txt" "action=login failed"

| stats count by ip, user

| sort -count

This query returned a list of IP addresses with the highest number of login failures, aiding in the analysis of potential malware activity or recurring attack patterns.



ip	user	count
10.0.0.5	bob	1
172.16.0.3	bob	1
192.168.1.101	charlie	1
203.0.113.77	alice	1
203.0.113.77	david	1

5. Accounts with Both Failures and Success (Brute-force Indication)

Index =* source="SOC_Task2_Sample_Logs.txt" ("action=login failed" OR "action=login success")

| stats values(action) as actions by user, ip

| where mvcount(actions)=2 AND "login failed" IN actions AND "login success" IN actions

6. Brute Force / Compromise Analysis

Manual correlation of login, connection, and malware events uncovered suspicious patterns across several users, even without traditional brute-force sequences. The following user-IP combinations suggest possible account compromise or lateral movement:

Bob:

10.0.0.5: login + malware

172.16.0.3: login + malware

192.168.1.101: login + connection

→ Indicates credential compromise and internal spread.

Charlie:

172.16.0.3: login + malware + connection

10.0.0.5 & 192.168.1.101: multiple connection attempts

→ Suggests reconnaissance followed by unauthorized access.

Alice:

Malware from: 172.16.0.3, 192.168.1.101, 198.51.100.42

Login from: 203.0.113.77

→ Multiple infections suggest repeated endpoint compromise.

Eve:

Login: 172.16.0.3

Malware: 10.0.0.5

→ Possible shared infected device or user-level breach.

David:

Login: 203.0.113.77

Malware: 172.16.0.3

→ Actions point to potential data exfiltration or compromised endpoint.

These findings show how correlating user actions with IP-based indicators (login, malware, connection) can reveal threats not visible through brute-force patterns alone.

Show: 20 Per Page ▾ Format ▾ Preview: On		
user ▾	ip ▾	actions ▾
alice	198.51.100.42	login malware
alice	203.0.113.77	file login
bob	10.0.0.5	login malware
bob	172.16.0.3	file login malware
bob	192.168.1.101	connection login
bob	198.51.100.42	file login
bob	203.0.113.77	connection file malware
charlie	10.0.0.5	connection
charlie	172.16.0.3	connection login malware
charlie	192.168.1.101	connection
charlie	198.51.100.42	login
charlie	203.0.113.77	file
david	10.0.0.5	connection file
david	172.16.0.3	connection malware
david	198.51.100.42	file
david	203.0.113.77	connection file login
eve	10.0.0.5	malware
eve	172.16.0.3	file login

7. Detected Malware Activity

```
index=* source="SOC_Task2_Sample_Logs.txt" "action=malware detected"
```

This query showed rows or charts indicating of malware, action, users and threats.

127.0.0.1:8000/en-US/app/search/search?earliest=0&latest=&q=search%20index%3D*%20source%3D"SOC_Task2_Sample_Logs.txt"%20"action%3Dm...

Search & Reporting

Splunk Enterprise

Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

New Search

Save As Create Table View Close

index=* source="SOC_Task2_Sample_Logs.txt" "action=malware detected"

All time

11 events (before 7/18/25 11:06:09.000 PM) No Event Sampling

Job

Smart Mode

Events (11) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

1 hour per column

Format Show: 20 Per Page View: List

< Hide Fields

All Fields

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

date_month 1

date_second 1

date_wday 1

date_year 1

a index 1

a ip 5

linecount 1

a punct 2

a splunk_server 1

a threat 5

timeendpos 1

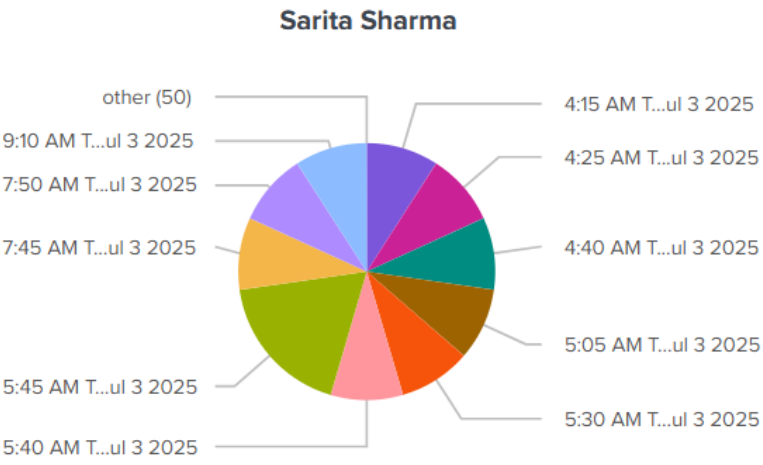
i	Time	Event
>	7/3/25 9:10:14.000 AM	2025-07-03 09:10:14 user=bob ip=172.16.0.3 action=malware detected threat=Ransomware Behavior host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	7/3/25 7:51:14.000 AM	2025-07-03 07:51:14 user=reve ip=10.0.0.5 action=malware detected threat=Rootkit Signature host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	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 = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	7/3/25 5:48:14.000 AM	2025-07-03 05:48:14 user=bob ip=10.0.0.5 action=malware detected threat=Trojan Detected host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	7/3/25 5:45:14.000 AM	2025-07-03 05:45:14 user=david ip=172.16.0.3 action=malware detected threat=Trojan Detected host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	7/3/25 5:42:14.000 AM	2025-07-03 05:42:14 user=reve ip=203.0.113.77 action=malware detected threat=Trojan Detected host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	7/3/25 5:30:14.000 AM	2025-07-03 05:30:14 user=reve ip=192.168.1.101 action=malware detected threat=Trojan Detected host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	7/3/25 5:06:14.000 AM	2025-07-03 05:06:14 user=bob ip=203.0.113.77 action=malware detected threat=Worm Infection Attempt host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	7/3/25 4:41:14.000 AM	2025-07-03 04:41:14 user=alice ip=172.16.0.3 action=malware detected threat=Spyware Alert host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	7/3/25 4:29:14.000 AM	2025-07-03 04:29:14 user=alice ip=192.168.1.101 action=malware detected threat=Trojan Detected host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file
>	7/3/25 4:19:14.000 AM	2025-07-03 04:19:14 user=alice ip=198.51.100.42 action=malware detected threat=Rootkit Signature host = Sarita Sharma source = SOC_Task2_Sample_Logs.txt sourcetype = log_file

Incident Classification

Type	Description	Severity
Brute Force Attempt	Repeated failed logins for Bob and Charlie from IP 10.0.0.5	High
Account Compromise	David showed both failed and successful logins from 203.0.113.77	Critical
Malware Infection	Trojan/Rootkit activity from IPs 192.168.1.101, 198.51.100.42	Critical
Recon/Scanning	Multiple connection attempts to internal IPs	Medium

Events Patterns Statistics (60) **Visualization**

Chart:  Pie Chart  Format  Trellis



Security Response Summary

Urgent Actions

- **Block/Watch IPs:** 10.0.0.5, 203.0.113.77, 192.168.1.101 flagged for suspicious activity
- **Password Resets:** Immediate reset for users showing signs of compromise
- **Quarantine Devices:** Isolate any endpoints linked to Trojan or Rootkit detections

Preventive Steps

- Activate Multi-Factor Authentication (MFA) across all accounts
- Apply rate limiting and account lockout after multiple login failures
- Create alerts for abnormal login failure volumes

Ongoing Checks

- Regularly review privileged account logins
- Strengthen Splunk detection logic to catch brute-force attempts
- Conduct staff training on spotting phishing and suspicious behaviors

Learning Outcomes:

- Used Splunk to analyze custom log formats effectively
- Identified login failures, brute-force behavior, and post-attack traces
- Practiced building and refining SPL queries for real-time insights
- Tracked malware sources using IP and user activity correlation

Conclusion

This hands-on lab demonstrated how Splunk can uncover threats like unauthorized access and malware activity. Targeted queries enabled quick detection and response to simulated attacks.

Ethical Note: All analysis was conducted in a safe lab using demo data—no real systems were impacted.

Incident Communication Email Demonstration:

Subject: Incident Report – Unusual Login Activity & Malware Detection

To: SOC Manager

From: Sarita Sharma

Date: 07/18/2025

Dear Sir/Madam,

This is to inform you that several suspicious activities were identified during log analysis conducted in Splunk. The findings point to multiple failed login attempts, signs of malware infections, and possible account compromise.

Summary of key findings:

IP 10.0.0.5 – Detected brute-force login attempt

User: David – Unusual login behavior and malware presence

IP 192.168.1.101 – Indications of Trojan activity

For detailed insights and recommended actions, please refer to the full report.

Best regards,
Sarita Sharma
SOC Intern – Future Interns