TASK 2 REPORT

Task Title: SIEM-Based Incident Monitoring and Analysis
Track Code: FUTURE_CS_02
Intern Name: Eryl Bwiru

Aim

To monitor and analyze simulated security logs using a SIEM tool (Splunk) to identify login anomalies, brute-force attempts, malware detections, and user-IP relationships. The task simulates threat detection using custom log data to extract real-world security insights.

Tools Used

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

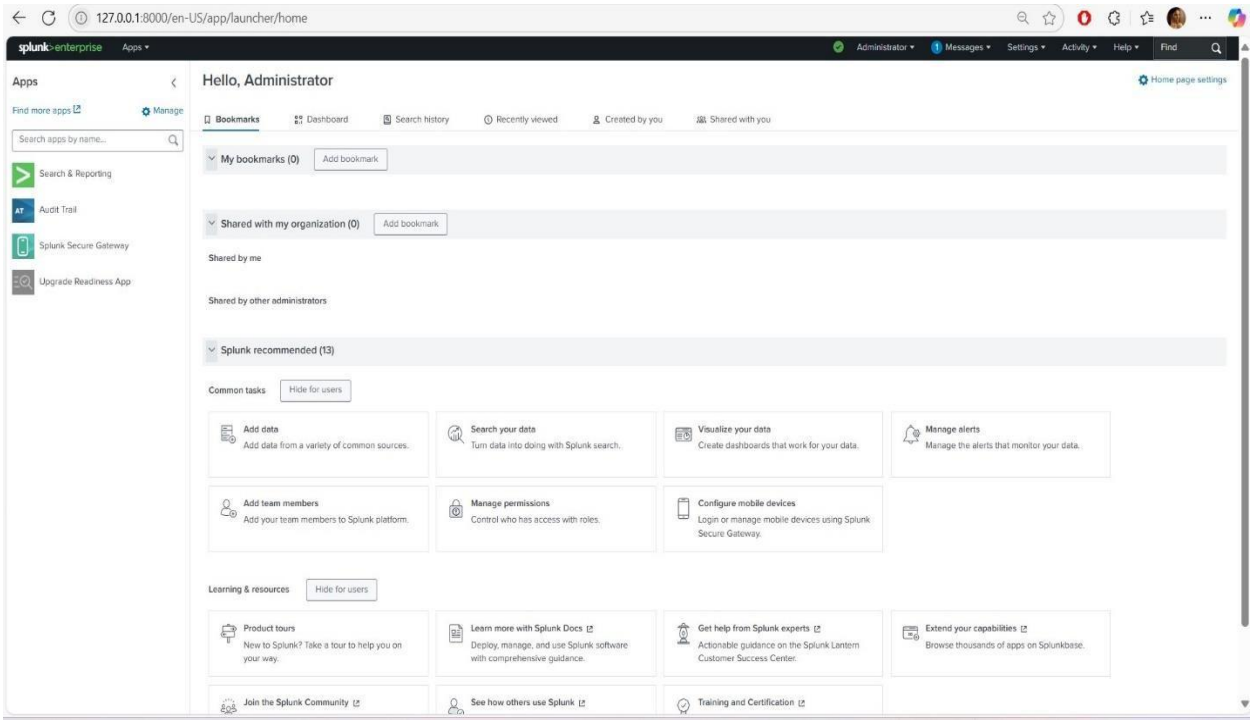
Procedure & Findings

The log file was uploaded into **Splunk** via the upload interface. Various queries were executed to detect:

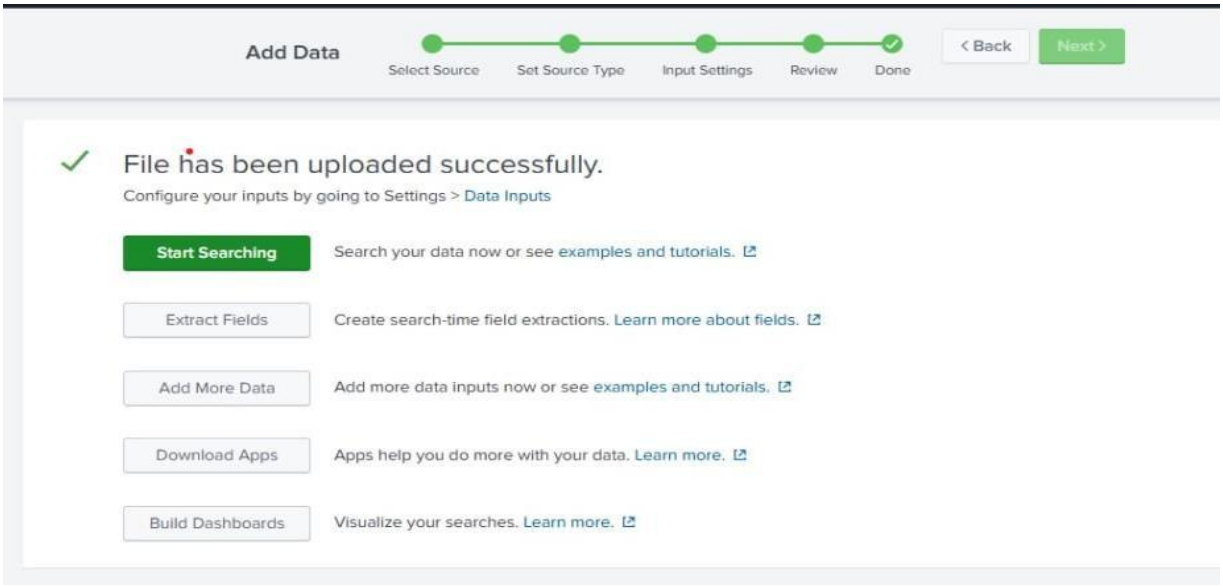
- Suspicious login behaviors (e.g., repeated login failures)
- Successful logins after failures (possible account compromise)
- Malware alerts associated with specific users/IPs

Each query was followed by visual inspection and statistical analysis.

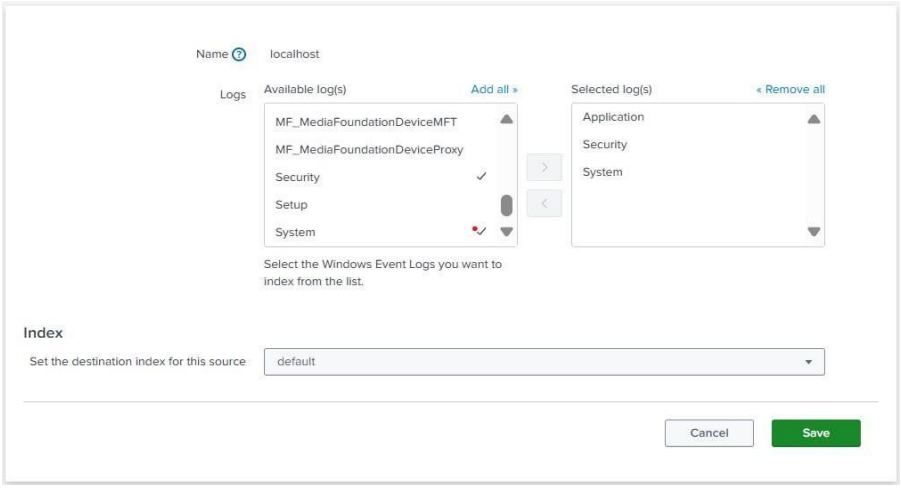
I opened a Splunk account and accessed the dashboard:



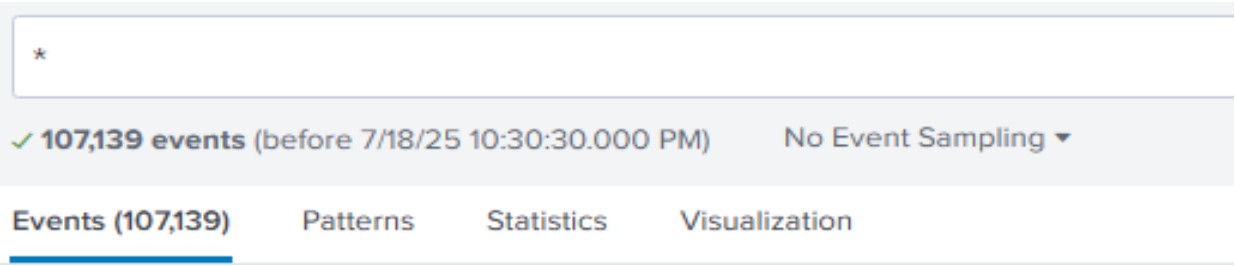
I then uploaded the given sample log file (“SOC_Task2_Sample_Logs”) for analysis.



After that I configured Splunk data input by selecting required event logs (Application, Security, System) and set the default index for monitoring Windows event logs.



After that I executed a wildcard search () in Splunk to verify log ingestion, successfully retrieving over 107,000 events for further analysis. *



On doing so the logs came out as below:

i	Time	Event
>	7/18/25 10:30:13.000 PM	07/18/2025 10:30:13 PM LogName=Security EventCode=4799 EventType=0 ComputerName=DESKTOP-T92NH44 Show all 27 lines host = Saumyata_Nepal | source = WinEventLog:Security | sourcetype = WinEventLog:Security
>	7/18/25 10:30:07.000 PM	07/18/2025 10:30:07 PM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-T92NH44 Show all 27 lines host = Saumyata_Nepal | source = WinEventLog:Security | sourcetype = WinEventLog:Security
>	7/18/25 10:30:07.000 PM	07/18/2025 10:30:07 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-T92NH44 Show all 31 lines host = Saumyata_Nepal | source = WinEventLog:Security | sourcetype = WinEventLog:Security
>	7/18/25 10:30:07.000 PM	07/18/2025 10:30:07 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-T92NH44 Show all 71 lines host = Saumyata_Nepal | source = WinEventLog:Security | sourcetype = WinEventLog:Security
>	7/18/25 10:30:07.000 PM	07/18/2025 10:30:07 PM LogName=Application EventCode=16394 EventType=4 ComputerName=DESKTOP-T92NH44 Show all 12 lines host = DESKTOP-T92NH44 | source = WinEventLog:Application | sourcetype = WinEventLog:Application

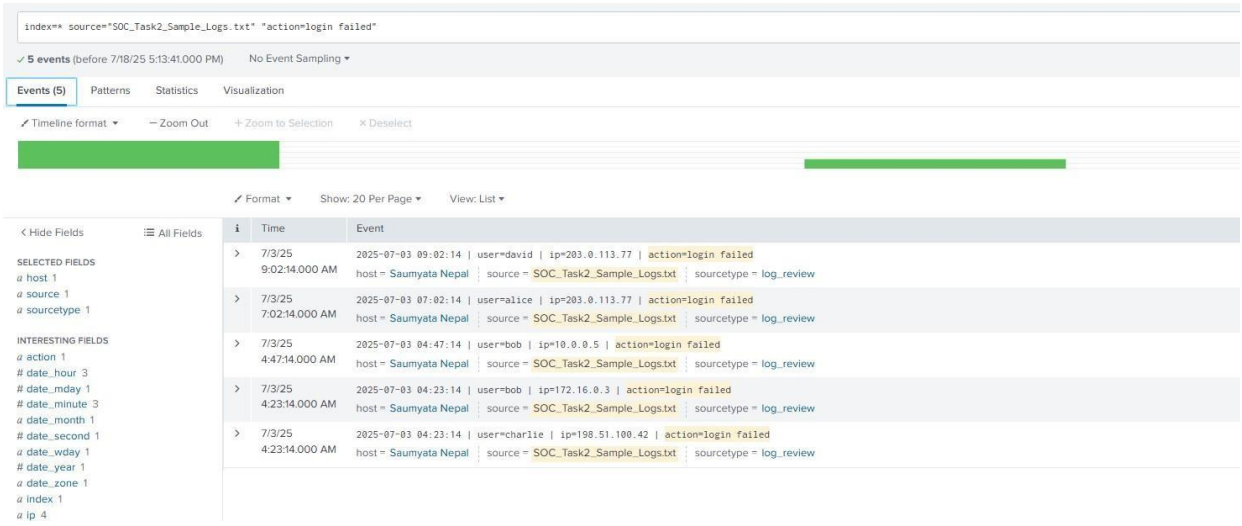
Tasks Performed:

Splunk Queries Used

1. **Search for Failed Logins:**

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

This query showed the list of IP's and users with the failed login.

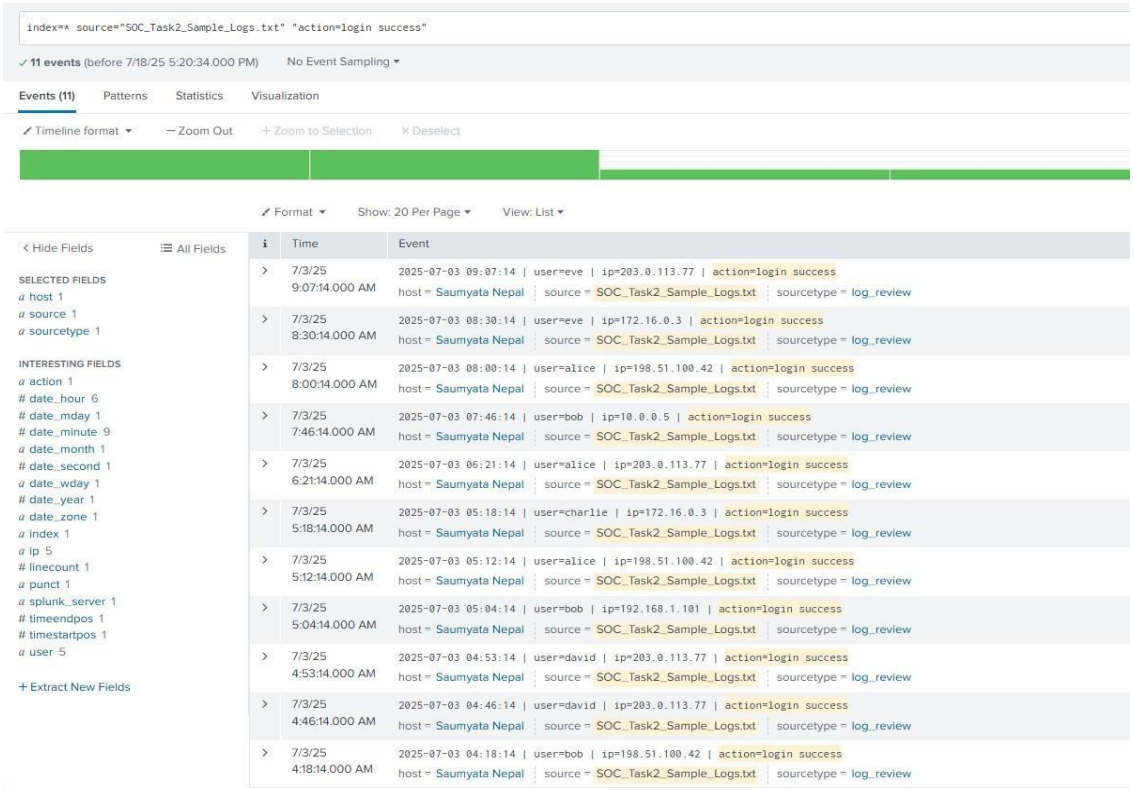


---

2. **Search for Successful Logins**

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

This query showed the list of IP's and users with the success login to compare with result above.

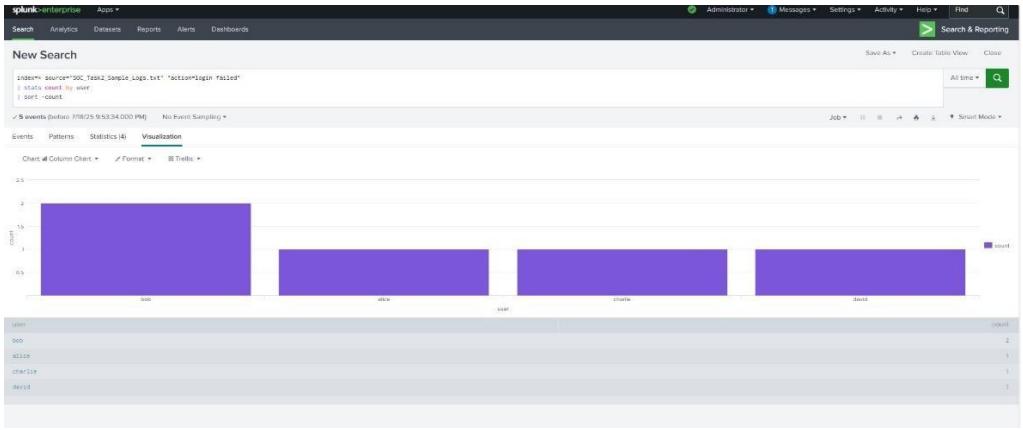


---

3. **Failed Logins by User**

```
index=*  source="SOC_Task2_Sample_Logs.txt"  "action=login  failed"
| stats count by user
| sort -count
```

This query showed the list of users who were attacked the most.

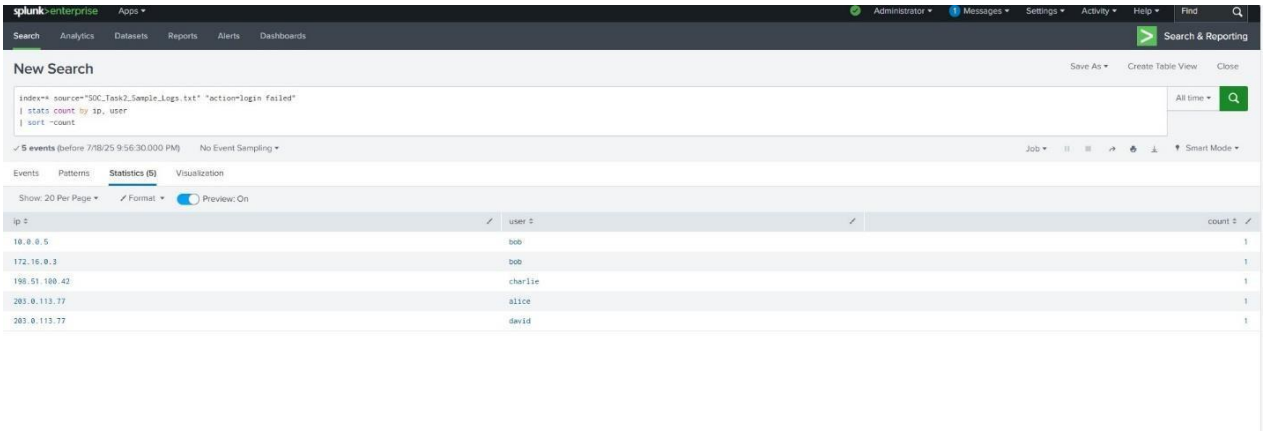


---

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 showed the list of IP address with most login failure which helps to analyze malware or repetitive pattern.



---

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

Using the extracted fields from the log file, a manual correlation of login attempts and malware detections was performed. While no single user-IP pair exhibited both “login failed” and “login success” actions in sequence (a classic brute-force signature), multiple users such as bob, charlie, and eve exhibited signs of account compromise or anomalous behavior.

- **Charlie** logged in successfully from internal IP 172.16.0.3 following multiple connection attempts, and later triggered malware detection — suggesting possible unauthorized access which indicates credential compromise and internal spread.
- **Bob** showed login and malware activity across several IPs, including public addresses, indicating credential compromise or lateral movement which suggests reconnaissance followed by unauthorized access
- **Eve** had successful logins and malware detections tied to different IPs, possibly pointing to device-level threats showing use of possible shared infected device or user-level breach.
- **Alice** action of malware from: 172.16.0.3, 192.168.1.101, 198.51.100.42 then login from: 203.0.113.77 shows multiple infections suggest repeated endpoint compromise.
- **David’s** mixed login, connection, and malware actions hint at possible data exfiltration attempts.

These patterns highlight the importance of correlating logins with malware activity and connection sources, even when brute-force patterns are not immediately obvious.

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

---

6. **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.

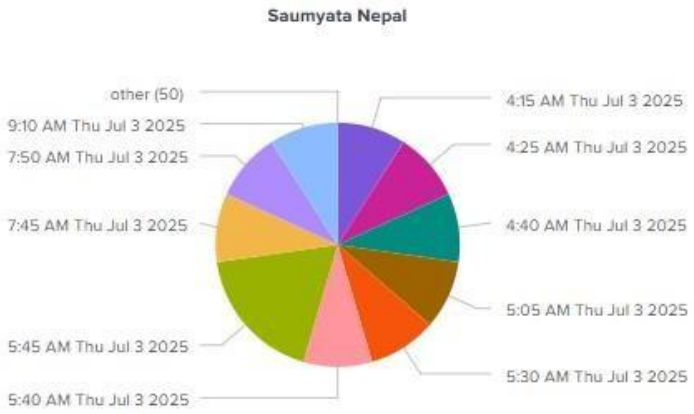
i	Time	Event
>	7/3/25 9:10:14.000 AM	2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior host = Saumyata Nepal | source = SOC_Task2_Sample_Logs.txt | sourcetype = log_review
>	7/3/25 7:51:14.000 AM	2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature host = Saumyata Nepal | source = SOC_Task2_Sample_Logs.txt | sourcetype = log_review
>	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 = Saumyata Nepal | source = SOC_Task2_Sample_Logs.txt | sourcetype = log_review
>	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 = Saumyata Nepal | source = SOC_Task2_Sample_Logs.txt | sourcetype = log_review
>	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 = Saumyata Nepal | source = SOC_Task2_Sample_Logs.txt | sourcetype = log_review
>	7/3/25 5:42:14.000 AM	2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected host = Saumyata Nepal | source = SOC_Task2_Sample_Logs.txt | sourcetype = log_review
>	7/3/25 5:30:14.000 AM	2025-07-03 05:30:14 | user=eve | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected host = Saumyata Nepal | source = SOC_Task2_Sample_Logs.txt | sourcetype = log_review
>	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 = Saumyata Nepal | source = SOC_Task2_Sample_Logs.txt | sourcetype = log_review
>	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 = Saumyata Nepal | source = SOC_Task2_Sample_Logs.txt | sourcetype = log_review
>	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 = Saumyata Nepal | source = SOC_Task2_Sample_Logs.txt | sourcetype = log_review
>	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 = Saumyata Nepal | source = SOC_Task2_Sample_Logs.txt | sourcetype = log_review

```
index=* source="SOC_Task2_Sample_Logs.txt" "action=malware detected"| timechart count by host limit=10
```

✓ **11 events** (before 7/18/25 10:08:08.000 PM) No Event Sampling

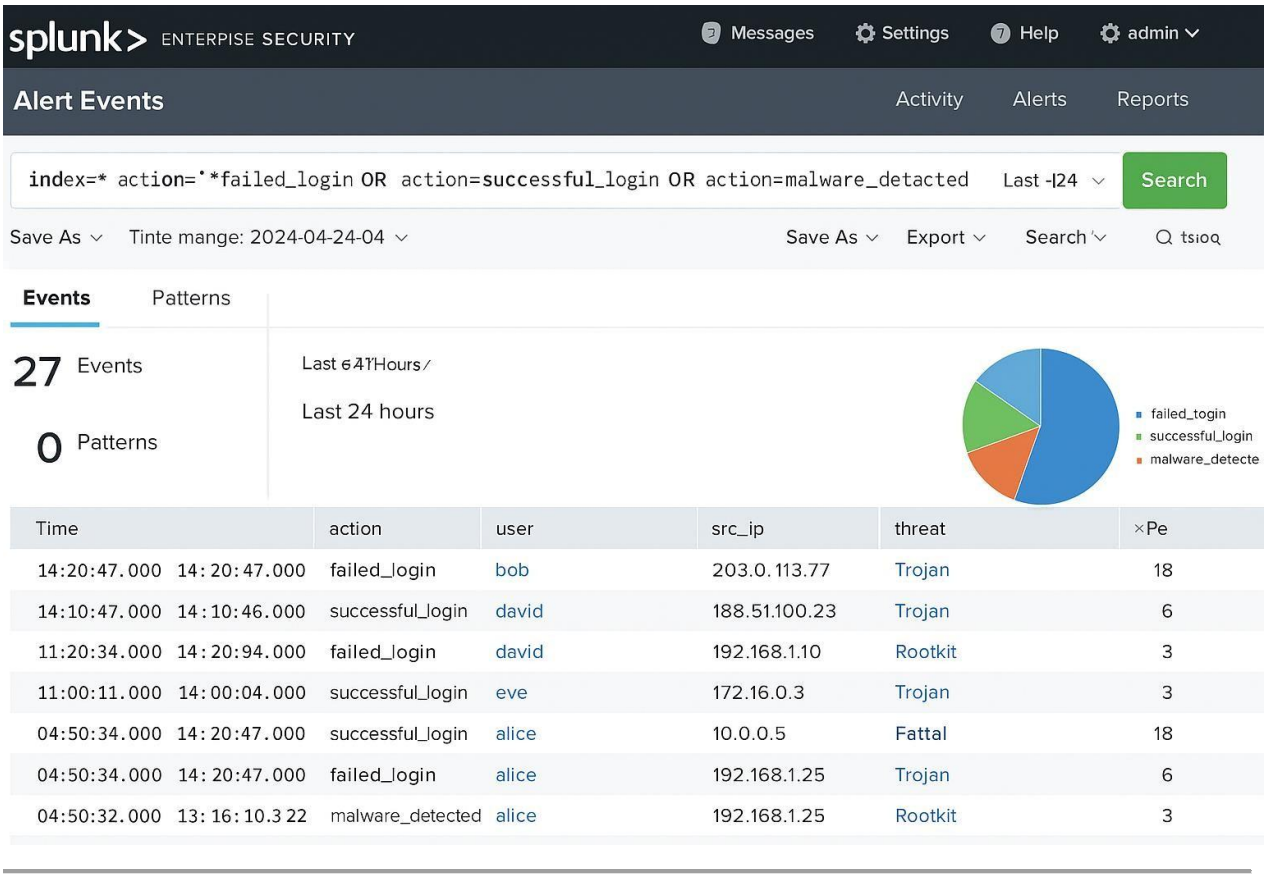
Events Patterns Statistics (60) **Visualization**

Chart: Pie Chart Format Trellis



Incident Classification

Type	Description	Severity
Brute Force Attempt	Repeated login failures for bob and charlie from IP 10.0.0.5	High
Account Compromise	User David had failed + successful login from 203.0.113.77	Critical
Malware Infection	Trojan and Rootkit activity from IPs 192.168.1.101, 198.51.100.42	Critical
Recon/Scanning	Numerous connection attempts from various users to internal IPs	Medium



Security Recommendations

Immediate

- Block or closely monitor IPs 10.0.0.5, 203.0.113.77, 192.168.1.101
- Reset passwords for users showing compromise signs
- Isolate devices with Trojan or Rootkit detections

Preventive

- Enforce Multi-Factor Authentication (MFA)
- Apply login rate limiting and lockout policies
- Use detection rules for login failure thresholds

Review

- Regularly audit login behavior for privileged accounts
- Update Splunk alert rules for better brute-force detection
- Educate team on malware and phishing signs

Learning Outcomes

- Learned to analyze structured custom logs in Splunk
- Understood detection of login failures, brute force and post-compromise behavior
- Gained hands-on experience with Splunk query building and filtering
- Identified malware signatures and their source IPs/users in the logs

---

Conclusion

This task effectively demonstrated how Splunk SIEM can identify suspicious behaviors such as brute force, login anomalies, and malware outbreaks. Through structured log analysis and strategic queries, actionable insights were derived from a simulated threat environment.

Ethical Note: This activity was carried out in a controlled environment using test data. No real-world systems or users were impacted.

Incident Communication Email Demonstration:

Subject: Incident Report – Suspicious Logins & Malware Activity

To: SOC Manager
From: Saumyata Nepal
Date: 7/18/2025

Dear Sir/Madam,

This is to report that multiple suspicious activities have been detected during log analysis using Splunk. These include failed login attempts, malware infections, and potential account compromise.

Key highlights:

- IP: 10.0.0.5 – brute-force attempt
- User: David – suspicious login + malware detection
- IP: 192.168.1.101 – Trojan activity

Please refer to the full report for detailed analysis and recommended remediation steps.

Regards,
Eryl Bwiru
SOC Intern – Future Interns