NAME-SAMRIDDHI DIXIT

CYBER SECURITY INTERNSHIP-TASK 2

Security Operations Center (SOC) Internship Task:

Security Alert Monitoring & Incident Response Simulation

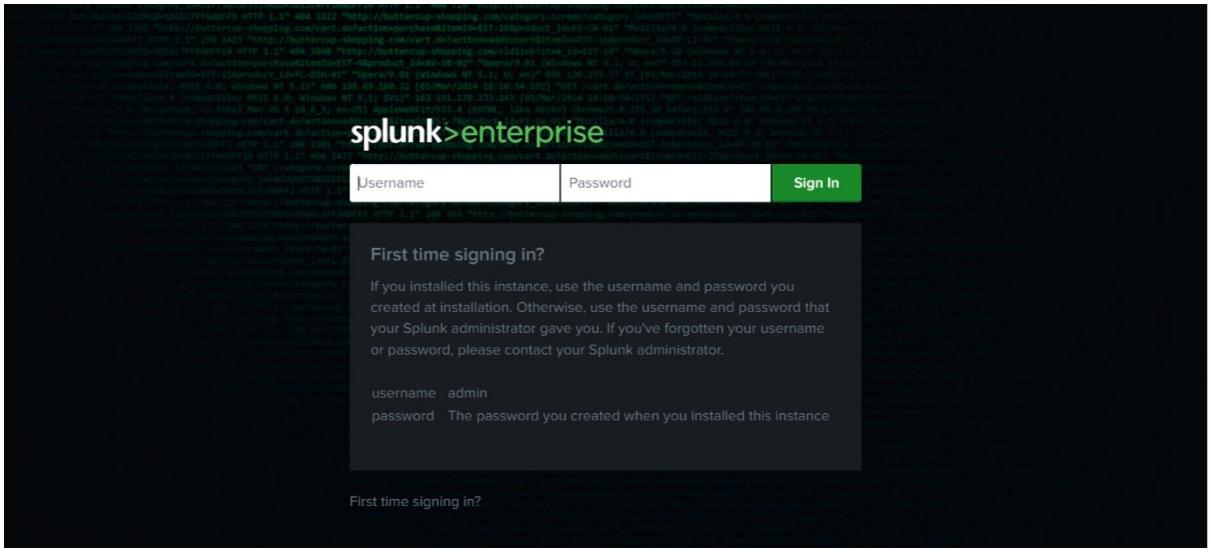
1. Executive Summary

As part of SOC Task-2, Security Alert Monitoring and Incident Response activities were performed using Splunk Enterprise SIEM. Sample security logs were ingested and analysed to identify suspicious activities such as failed login attempts, access from unusual IP addresses, and malware-related events.

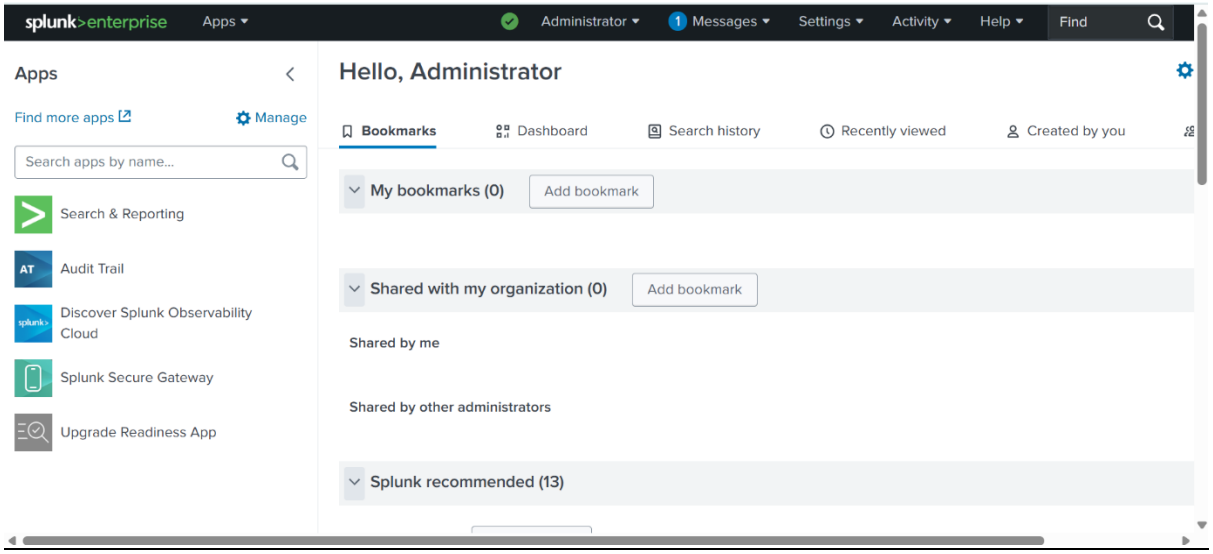
The objective of this task was to simulate real-world SOC operations including alert detection, severity classification, and incident response actions.

2. Lab Environment

- **Operating System:** Windows (Local Machine)
- **SIEM Tool:** Splunk Enterprise (Free Trial)
- **Splunk Web Interface:** http://localhost:8000
- **Log Source:** SOC_Task2_Sample_Logs



Splunk Enterprise login page



Splunk Enterprise -Home Page

3. Methodology

1. **SIEM Configuration** – Set up Splunk Enterprise to perform security monitoring and log analysis.
2. **Log Preparation** – Utilized simulated security logs as the input data source.

3. **Log Ingestion Process** – Imported and indexed log data into Splunk for analysis.
4. **Security Query Creation** – Developed SPL queries to identify suspicious activities.
5. **Dashboard Development** – Created visual dashboards to monitor security events.
6. **Alert Severity Assessment** – Analysed and categorized alerts based on risk level.
7. **Incident Documentation** – Recorded incident details, timelines, and response actions.

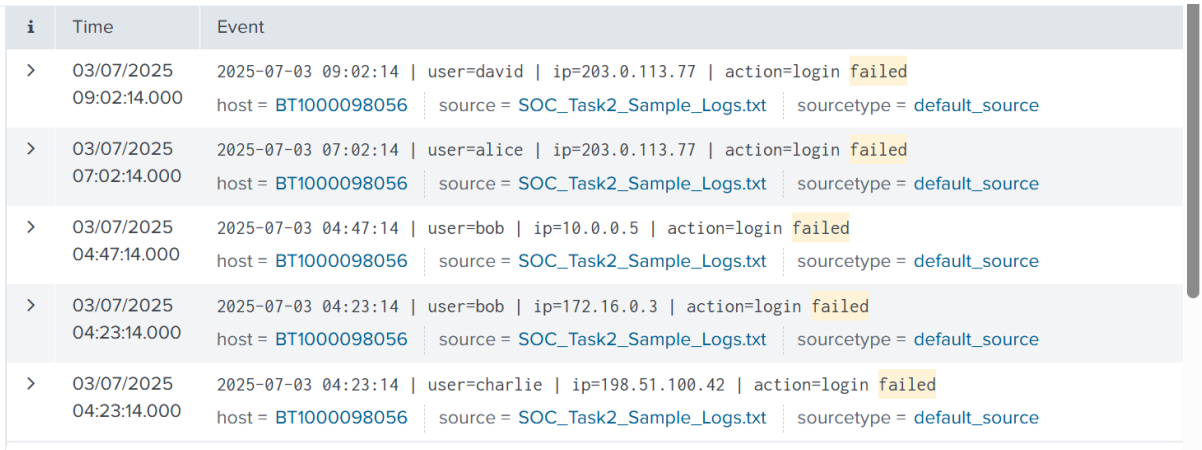
4. Security Monitoring & Alert Detection

4.1 Failed Login Attempts

Query Used: index=main failed OR failure OR "login failed"

Observation:
Multiple failed login attempts were detected from the same username and IP address.

Reason for Suspicion:
This behavior may indicate a brute-force login attempt.



i	Time	Event
>	03/07/2025 09:02:14.000	2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 07:02:14.000	2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 04:47:14.000	2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 04:23:14.000	2025-07-03 04:23:14 | user=bob | ip=172.16.0.3 | action=login failed host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 04:23:14.000	2025-07-03 04:23:14 | user=charlie | ip=198.51.100.42 | action=login failed host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source

Failed login attempts from the same user(bob)

4.2 Unusual / External IP Address Activity

Query Used: index=main src_ip

Observation:
Login attempts were observed from unknown or external IP addresses, IP's that are not private and repeated access attempts.

Reason for Suspicion:
Possible unauthorized or external access attempts.

i	Time	Event
>	03/07/2025 04:47:14.000	2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 04:46:14.000	2025-07-03 04:46:14 | user=david | ip=203.0.113.77 | action=login success host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 04:41:14.000	2025-07-03 04:41:14 | user=alice | ip=172.16.0.3 | action=malware detected | threat=Spyware Alert host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 04:29:14.000	2025-07-03 04:29:14 | user=alice | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 04:27:14.000	2025-07-03 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 04:23:14.000	2025-07-03 04:23:14 | user=bob | ip=172.16.0.3 | action=login failed host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 04:23:14.000	2025-07-03 04:23:14 | user=charlie | ip=198.51.100.42 | action=login failed host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025	2025-07-03 04:19:14 | user=david | ip=10.0.0.5 | action=connection attempt

External IP addresses (203.0.113.77,198.51.100.42)

4.3 Malware Detection

Query Used: index=main malware OR trojan OR virus

Observation:
Malware-related keywords were detected in the logs. (malware detected, trojan found, infected file, quarantined).

Reason for Suspicion:
Indicates a potential malware infection or security incident.

i	Time	Event
>	03/07/2025 09:10:14.000	2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 07:51:14.000	2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 07:45:14.000	2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 05:48:14.000	2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 05:45:14.000	2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 05:42:14.000	2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 05:30:14.000	2025-07-03 05:30:14 | user=eve | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected

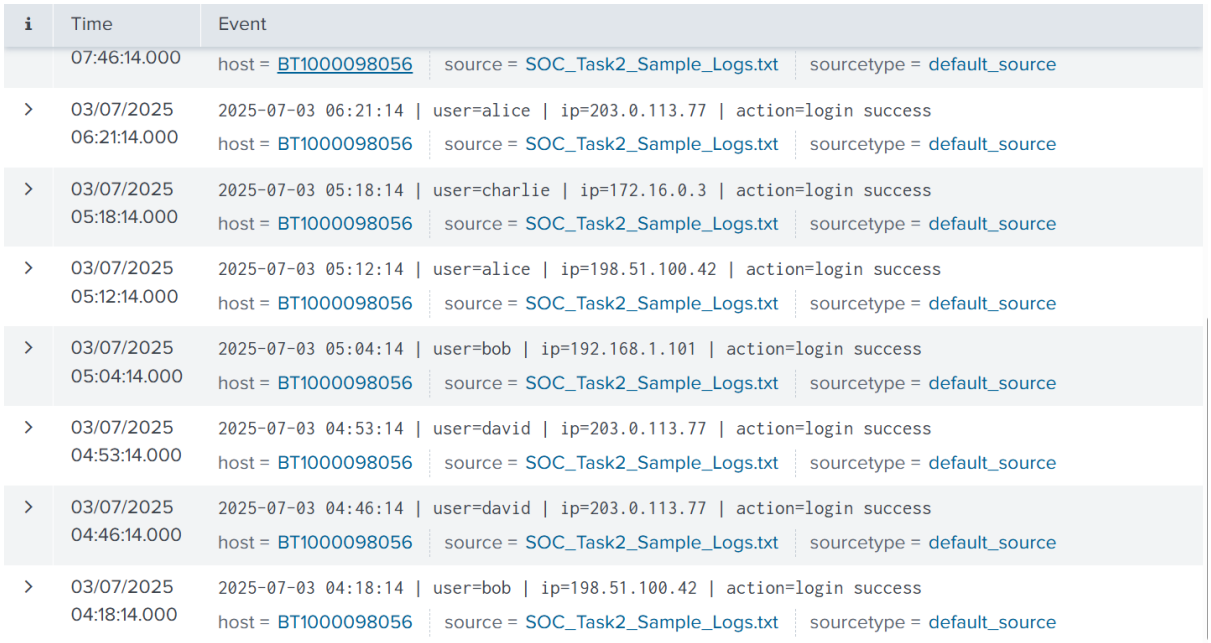
High Severity Malware Incidents

4.4 Successful Login After Failures

Search authentication logs for failed login attempts, then identify successful logins occurring shortly after.
Correlate events using the same username and IP address to track suspicious patterns.

Observation:
A successful login occurred shortly after multiple failed login attempts from the same IP.

Reason for Suspicion:
A failure followed by a success from the same source may indicate **credential compromise**.



i	Time	Event
	07:46:14.000	host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 06:21:14.000	2025-07-03 06:21:14 | user=alice | ip=203.0.113.77 | action=login success host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 05:18:14.000	2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 05:12:14.000	2025-07-03 05:12:14 | user=alice | ip=198.51.100.42 | action=login success host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 05:04:14.000	2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 04:53:14.000	2025-07-03 04:53:14 | user=david | ip=203.0.113.77 | action=login success host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 04:46:14.000	2025-07-03 04:46:14 | user=david | ip=203.0.113.77 | action=login success host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source
>	03/07/2025 04:18:14.000	2025-07-03 04:18:14 | user=bob | ip=198.51.100.42 | action=login success host = BT1000098056 source = SOC_Task2_Sample_Logs.txt sourcetype = default_source

Successful login after multiple attempts

5. Alert Classification

Alert ID	Description	Severity	Reason
A-01	Multiple failed login attempts	Medium	Possible brute-force
A-02	Malware detected	High	Active security threat
A-03	Login from unusual IP	High	Possible unauthorized access
A-04	Late-night login activity	Low	Needs verification

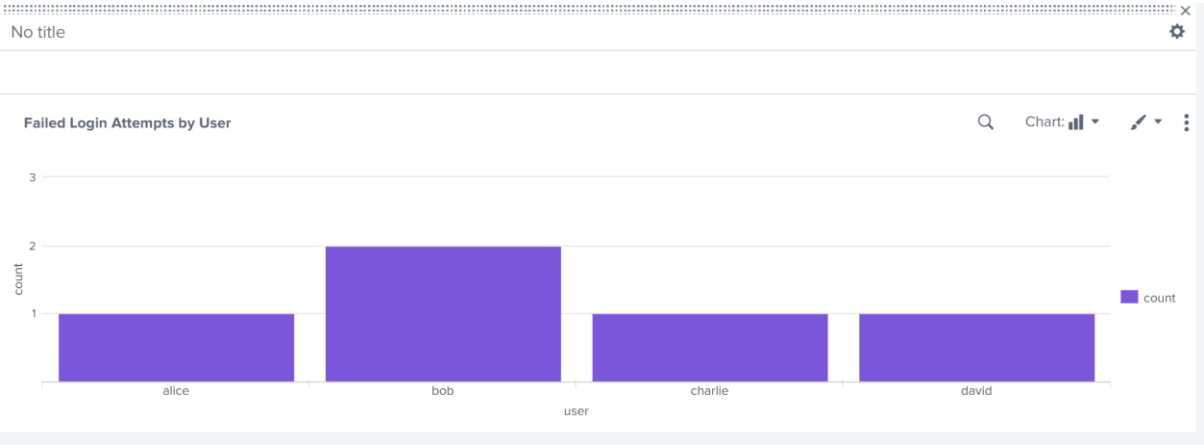
6. SOC Dashboard Creation

A SOC monitoring dashboard was developed in Splunk to provide a centralized view of critical security events. The dashboard was designed to support continuous monitoring and rapid identification of suspicious activities.

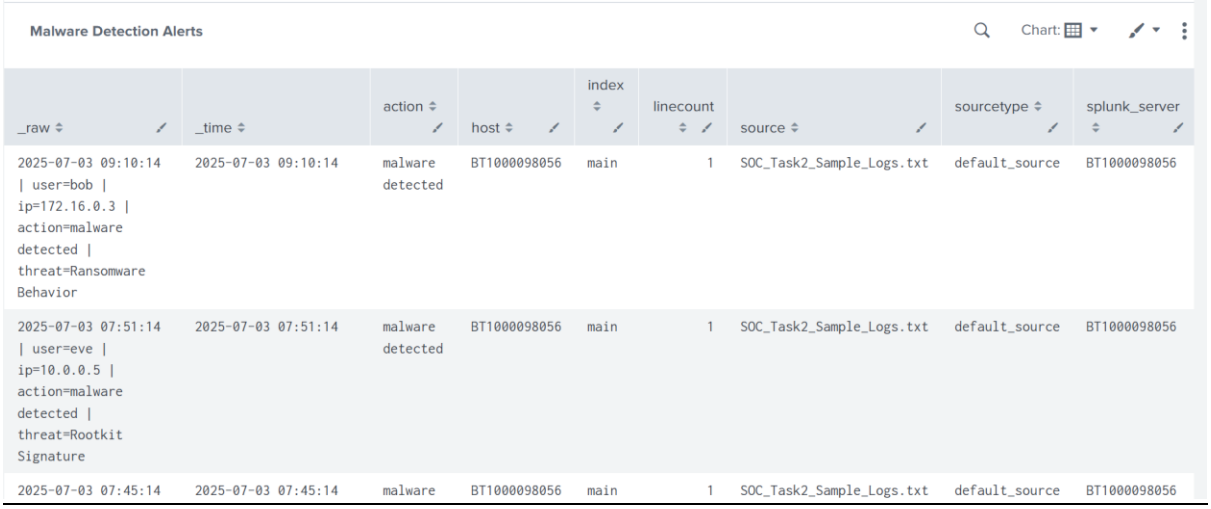
- Total count of failed login attempts

- Malware detection alert count
- Top source IP addresses generating security events

This visualization enables SOC analysts to quickly assess the security posture of the environment, identify abnormal patterns, and prioritize incidents for further investigation.

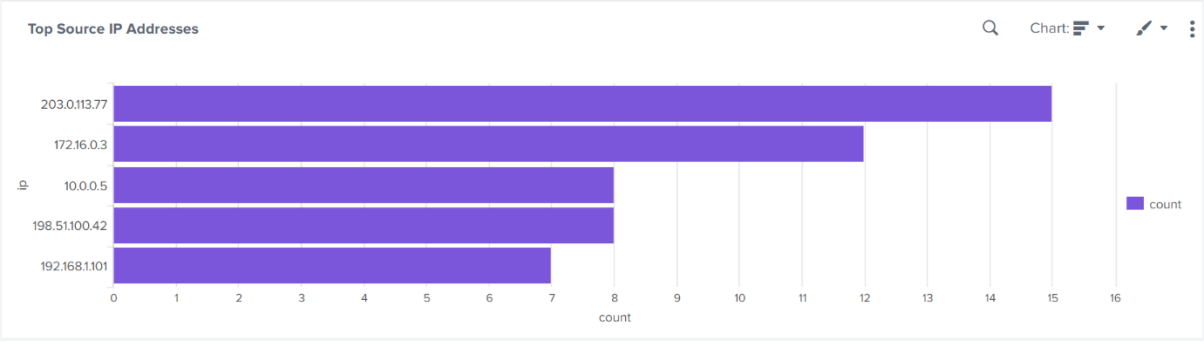


Visualisation for failed login attempts on DashBoard

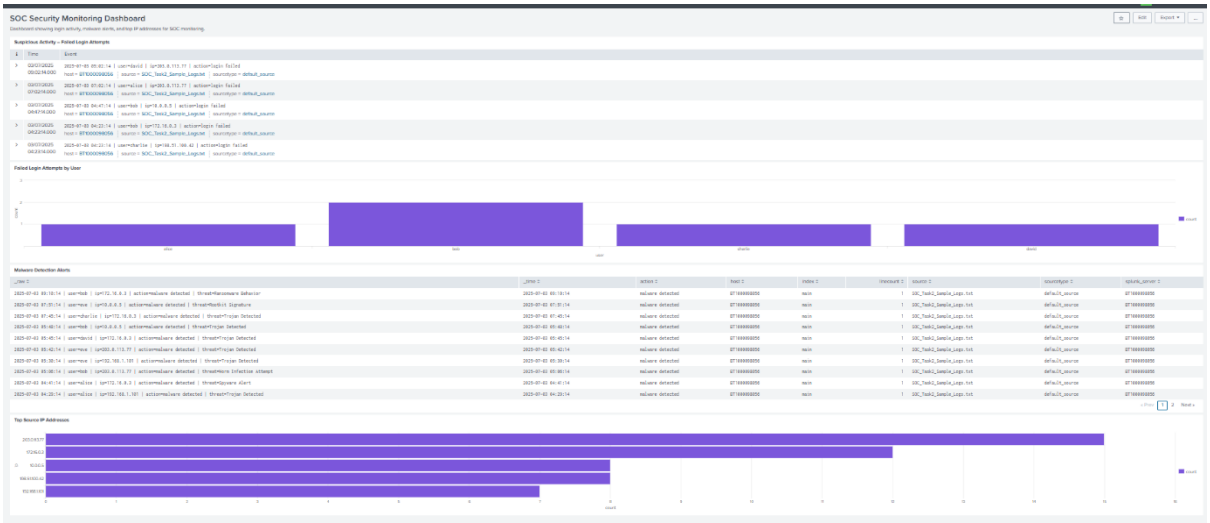


_raw	_time	action	host	index	linecount	source	sourcetype	splunk_server
2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior	2025-07-03 09:10:14	malware detected	BT1000098056	main	1	SOC_Task2_Sample_Logs.txt	default_source	BT1000098056
2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature	2025-07-03 07:51:14	malware detected	BT1000098056	main	1	SOC_Task2_Sample_Logs.txt	default_source	BT1000098056
2025-07-03 07:45:14	2025-07-03 07:45:14	malware	BT1000098056	main	1	SOC_Task2_Sample_Logs.txt	default_source	BT1000098056

Visualisation(table) for malware detection alerts



Visualisation for top IP addresses



Complete Dashboard with all Visualisations

7. Incident Response Report

7.1 Incident Overview

During routine security monitoring using Splunk SIEM, multiple suspicious security events were detected from the ingested logs. These events included repeated failed login attempts, a successful login from an external IP address, and multiple malware detection alerts. Correlation of authentication and malware events indicates a potential security incident involving unauthorized access attempts and malware activity.

- **Incident Type:** Brute Force Login Attempts and Malware Detection
- **Severity Level:** High

- **Affected Asset:** User workstation (Host: BT1000098056)
- **Detection Tool:** Splunk SIEM

7.2 Incident Timeline

Time (UTC)	Event Description
04:23	Multiple failed login attempts detected for users *bob* and *charlie* from IPs 172.16.0.3 and 198.51.100.42
04:27	Connection attempts observed from IP 172.16.0.3
04:29	Malware detected (Trojan) on user *alice* from IP 192.168.1.101
04:41	Malware detected (Spyware Alert) on user *alice* from IP 172.16.0.3
04:46	Successful login recorded for user *david* from external IP 203.0.113.77
04:47	Additional failed login attempt detected for user *bob* from IP 10.0.0.5

This sequence of events suggests repeated authentication failures followed by malware-related activity and a successful login from an external IP address.

7.3 Indicators of Compromise (IOCs)

The following indicators were identified during the investigation:

- **Usernames:** bob, alice, charlie, david
- **Suspicious IP Addresses:**
    - 198.51.100.42
    - 203.0.113.77
    - 172.16.0.3
    - 10.0.0.5
- **Detected Threats:** Trojan, Spyware

- **Event Types:** Login failure, login success, connection attempt, malware detected

---

7.4 Impact Analysis

The observed activity indicates a potential risk of unauthorized access due to repeated login failures and a successful login from an external IP address. The presence of malware alerts increases the risk of system compromise, data leakage, and lateral movement within the environment if not addressed promptly.

7.5 Response Actions

Based on the detected activity, the following response actions were documented:

- Blocked identified suspicious IP addresses at the network level
- Reset credentials for affected user accounts
- Isolated the system associated with malware detections
- Conducted malware scanning and remediation
- Continued enhanced monitoring through the SIEM
- Notified the management and security team of the incident

---

8. Security Recommendations

Based on the SIEM analysis performed during this task, the following improvements are suggested to enhance security monitoring and reduce future risks.

8.1 Access Control Enhancements

- Limit repeated login attempts to prevent brute-force activity
- Introduce multi-factor authentication for user accounts
- Apply stronger password complexity requirements

- Restrict sensitive access to trusted network locations

8.2 Monitoring Improvements

- Configure alerts for authentication failures and malware events
- Monitor login behavior for unusual IP addresses and timings
- Expand visibility by including additional log sources where possible

8.3 Incident Handling Improvements

- Define clear steps for responding to high-severity alerts
- Maintain basic documentation for detected incidents
- Improve communication flow between SOC analysts and management

---

9. Challenges and Mitigation

9.1 Log Interpretation

Challenge:
Some events required manual inspection to understand user activity and IP details.

Mitigation:
Event timestamps and available fields were correlated to identify suspicious patterns.

9.2 Alert Correlation

Challenge:
Single events did not always indicate an incident on their own.

Mitigation:
Multiple related events were reviewed together to determine potential security threats.

9.3 Dashboard Simplicity

Challenge:
Presenting security events in a clear and readable format.

Mitigation:
Simple metrics such as event counts and top IP addresses were used for visualization.

---

10. Conclusion

This SOC Task-2 activity provided practical exposure to security alert monitoring and incident response using a SIEM platform. By analyzing simulated security logs, common threat patterns such as failed login attempts, unusual access behavior, and malware-related events were identified and examined. The process demonstrated how individual log events can be correlated to recognize potential security incidents.

The creation of a SOC dashboard highlighted the importance of visualization in maintaining real-time visibility into security activity and supporting faster investigation. Classifying alerts by severity reinforced the need for effective prioritization during security operations.
