Security Alert Monitoring & Incident Response Report Future Interns – Cyber Security Internship (Task 2)

Name of Candidate: Aditya Gunjal
Internship Provider: Future Interns
Domain: Cyber Security (SOC Operations)
Date of Execution: 26 December 2025
Tool Used: Splunk Enterprise
Log Source: SOC_Task2_Sample_Logs.txt
Environment: Windows (Localhost)

---

1. Introduction

Security Operations Centers (SOC) play a critical role in monitoring, detecting, and responding to cybersecurity threats in real me. SOC analysts continuously analyze logs and alerts generated by systems and networks to identify suspicious activities and prevent potential security incidents.

This task simulates real-world SOC operations by analyzing system and network logs using a SIEM tool. The objective of this task was to monitor security alerts, identify potential threats, classify incidents based on severity, and propose appropriate incident response actions.

---

2. Objective

The main objectives of this task were:

- To gain hands-on experience with a SIEM tool
- To analyze security logs and identify suspicious ac vi es
- To classify incidents based on severity (High, Medium, Low)
- To document incident response actions and recommendations
- To understand the workflow of a SOC analyst

---

3. Tool Used

Splunk Enterprise

Splunk Enterprise is a powerful SIEM platform used for collecting, indexing, and analyzing machine generated data. In this task, Splunk was used to ingest simulated SOC logs and perform keyword-based searches to detect security incidents.

---

4. Log Source Description

The log file SOC_Task2_Sample_Logs.txt contained simulated security events, including:

- Authentication logs (successful and failed logins)
- Network connection attempts
- File access ac vi es
- Malware detection alerts

The logs were ingested as unstructured text (misc_text), and keyword-based searches were used for incident detection.

---

5. Incident Detection Methodology The following approach was used:

1. Upload logs into Splunk
2. Perform keyword-based searches to identify suspicious activity
3. Analyze patterns such as repeated failures, malware alerts, and unusual access
4. Classify incidents by severity
5. Document impact and response actions

---

6. Stakeholder Notification Draft

Subject: Security Incident Alert – Malware Detection Identified

Dear Management Team,

During routine security monitoring ac vi es, a security incident related to malware detection was identified through the SIEM monitoring system. The incident has been classified as High Severity due to the presence of malicious indicators such as Trojan and Rootkit signatures within the system logs.

Immediate response actions were initiated, including identification of affected systems, enhanced monitoring, and recommendations for malware removal and system isolation to prevent further impact.

Further analysis is ongoing to ensure that no additional systems are affected and to prevent recurrence of similar incidents. A detailed incident response report has been prepared and is available for review.

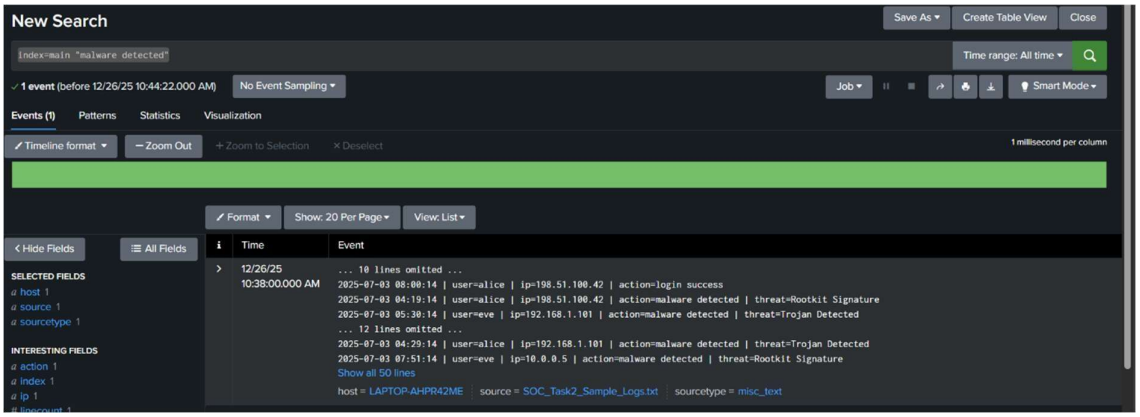
Please let us know if any additional actions or clarifications are required.

Regards,
Aditya Gunjal
Cybersecurity Intern
Future Interns

6. Identified Security Incidents Incident 1: Malware Infection Detected Search Query Used:

index=main "malware detected"

- Description:
  Multiple malware alerts were detected in the logs, including threats such as Trojan Detected and Rootkit Signature. These alerts indicate that malicious so ware was present on the system.
  Severity: High
- Impact:
  Malware infections can lead to data the, system compromise, and unauthorized access.
- Recommended Response:
  - Isolate the affected systems
  - Run full antivirus and malware scans
  - Remove infected files



Incident 2: Multiple Failed Login Attempts

- Search Query Used:

  index=main "login failed"

- Description:
  Failed login attempts were detected, indica ng possible brute-force or credential-stuffing attacks.

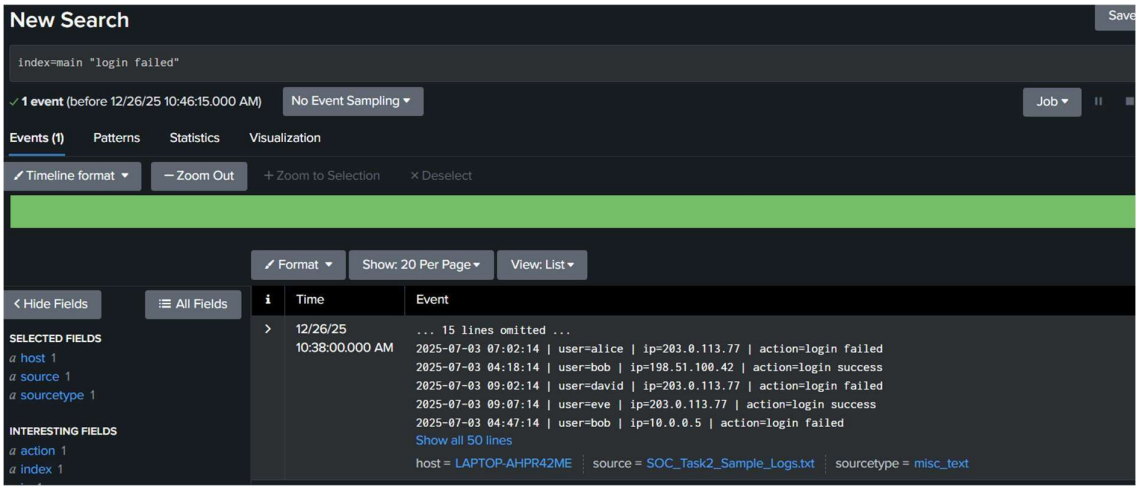
  Severity: Medium
- Impact:

Repeated failed logins may result in account compromise if successful.

- Recommended Response:
    - Enable account lockout policies
    - Enforce strong password

    requirements
    - Monitor login attempts and block

    suspicious Ips



Incident 3: Suspicious IP Address Activity

- Search Query Used:

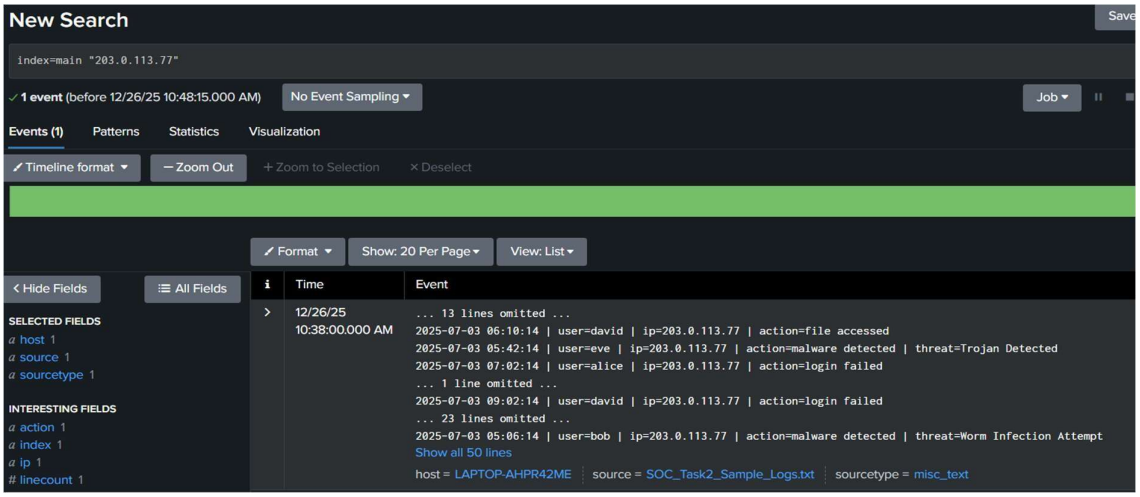
  index=main "203.0.113.77"

- Description:
  The same external IP address was involved in multiple activities, including login attempts and access events, indica ng suspicious behaviour.

  Severity: Medium

- Impact:
  Repeated access attempts from a single IP may indicate reconnaissance or attack preparation.

- Recommended Response:
    - Block or restrict the suspicious IP
    - Monitor network traffic
    - Implement firewalls and IDS/IPS



Incident 4: Unusual File Access Activity

- Search Query Used:

  index=main "file accessed"

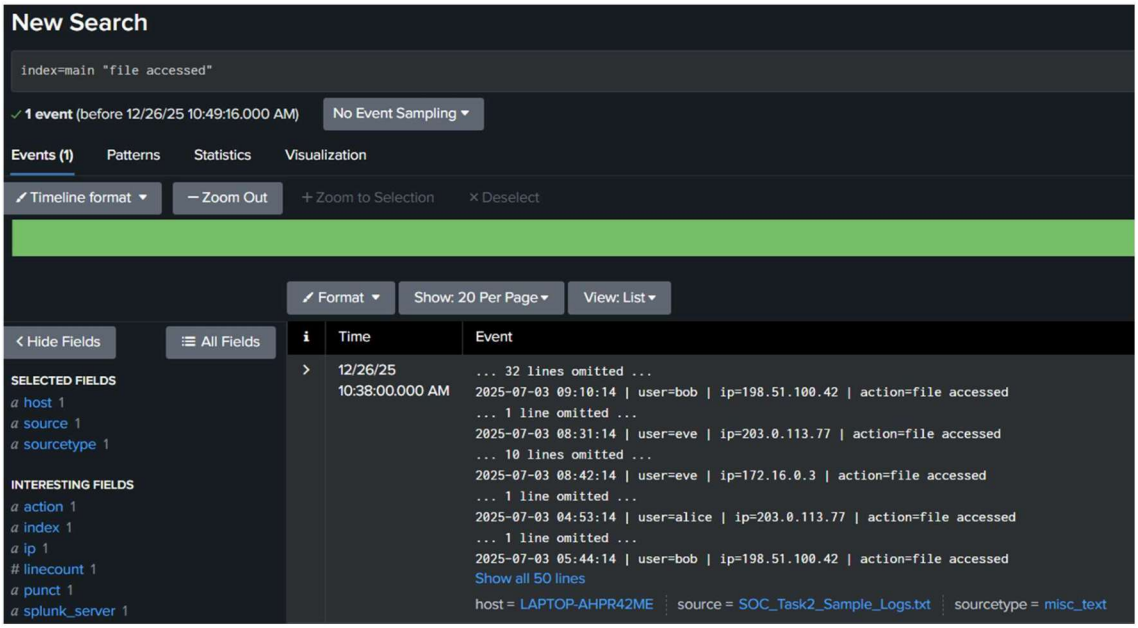
- Description:
  File access events were detected that may indicate unauthorized or unusual access to sensitive files.

  Severity: Low

- Impact:
  Could lead to data leakage if sensitive files are accessed without authorization.

- Recommended Response:
  - Review user permissions
  - Implement access control policies
  - Enable file activity monitoring

- Enable file activity monitoring



---

7. Incident Severity Classification Summary

Incident	Description	Severity
Malware Infection	Malware detected in system logs	High
Failed Login Attempts	Possible brute-force attack	Medium
Suspicious IP Activity	Repeated actions from one IP	Medium
Unusual File Access	Possible unauthorized access	Low

---

8. Challenges Faced

- Understanding SIEM workflows and navigation within Splunk
- Working with unstructured logs and performing keyword-based searches
- Correlating events to accurately identify security incidents

---

9. Learning Outcomes

Through this task, I learned:

- Basics of SOC operations and alert monitoring
- How to use a SIEM tool for log analysis

- Incident classification and severity assessment
- Importance of timely incident response
- Professional documenta on of security incidents

---

10. Conclusion

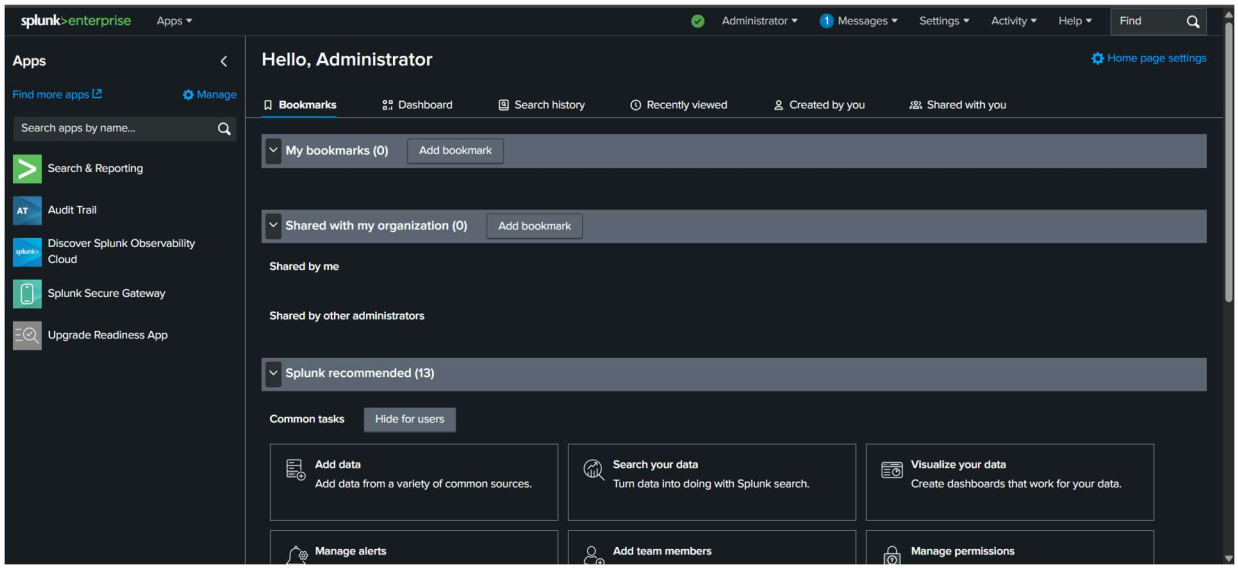
This task provided valuable hands-on experience in security alert monitoring and incident response. By analyzing logs using Splunk, multiple security incidents were successfully identified and classified. The exercise highlighted the importance of continuous monitoring, timely detection, and proper response to cybersecurity threats. Implementing the recommended security measures can significantly improve an organization's security posture.

---

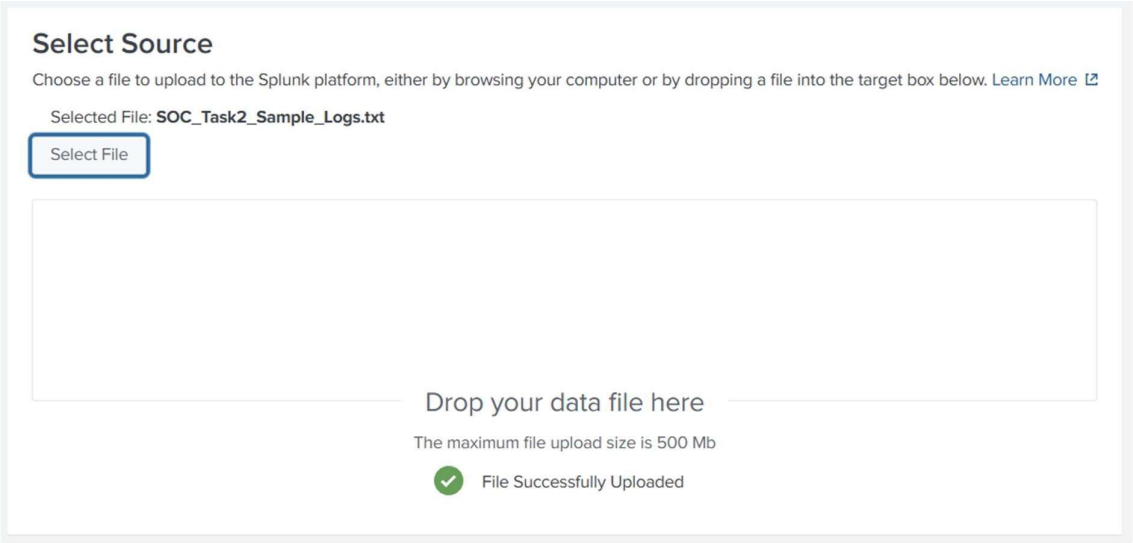
11. Screenshots & Evidence

Screenshots were captured during the log analysis process using Splunk Enterprise to support and validate the identified security incidents. The evidence includes screenshots of SIEM search queries and corresponding results highlighting suspicious ac vi es such as malware detection, failed login attempts, suspicious IP behaviour, and unusual file access events.

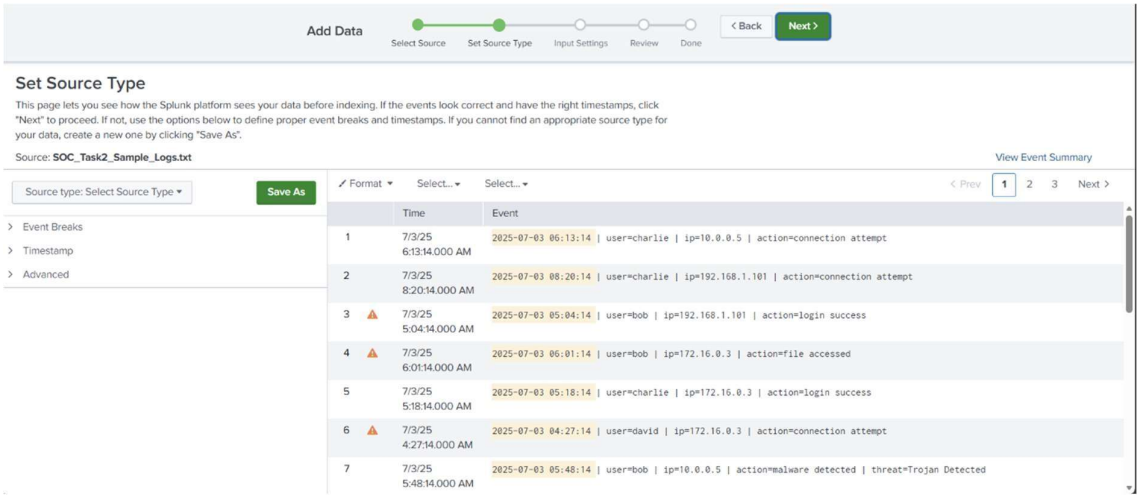
1.



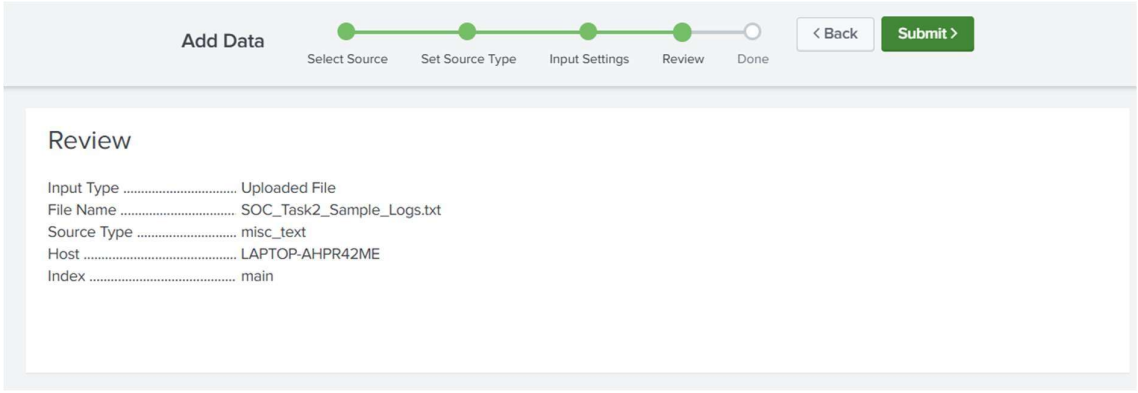
2.


Select Source
Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More
Selected File: SOC_Task2_Sample_Logs.txt
Select File
Drop your data file here
The maximum file upload size is 500 Mb
File Successfully Uploaded

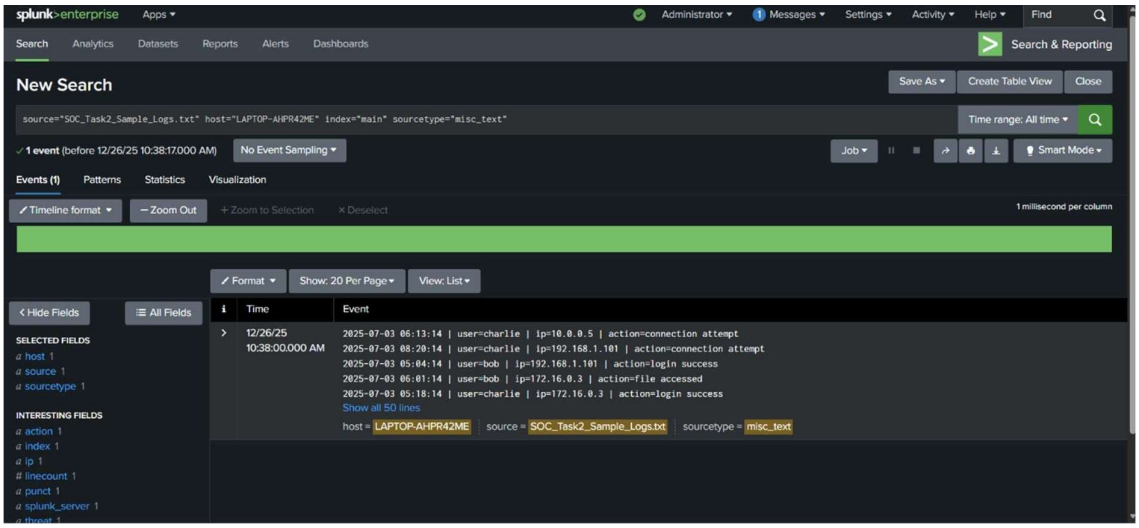
3.


Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Next
Set Source Type
This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".
Source: SOC_Task2_Sample_Logs.txt
View Event Summary
Source type: Select Source Type
Save As
Format
Select...
Select...
Prev
1
2
3
Next
Event Breaks
Timestamp
Advanced
Time
Event
1 7/3/25 6:13:14.000 AM 2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt
2 7/3/25 8:20:14.000 AM 2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
3 7/3/25 5:04:14.000 AM 2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success
4 7/3/25 6:01:14.000 AM 2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed
5 7/3/25 5:18:14.000 AM 2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success
6 7/3/25 4:27:14.000 AM 2025-07-03 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt
7 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

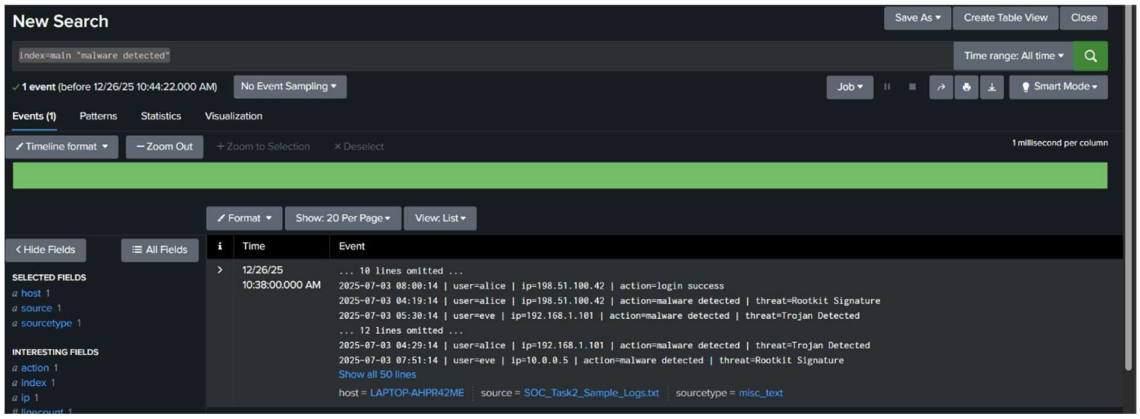
4.


Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Submit
Review
Input Type ..... Uploaded File
File Name ..... SOC_Task2_Sample_Logs.txt
Source Type ..... misc_text
Host LAPTOP-AHPR42ME
Index ..... main

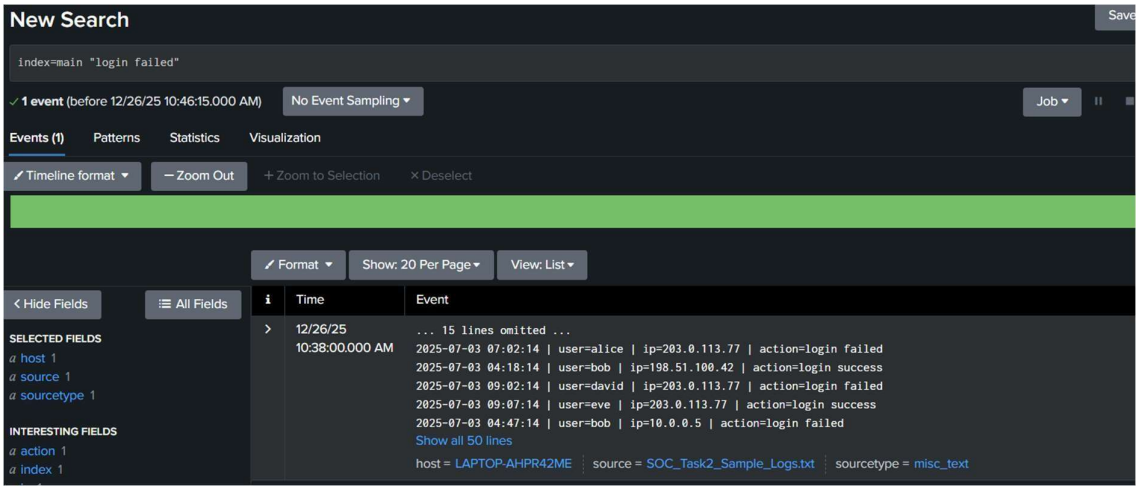
5.


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="SOC_Task2_Sample_Logs.txt" host="LAPTOP-AHPR42ME" index="main" sourcetype="misc_text"
Time range: All time
1 event (before 12/26/25 10:38:17.000 AM)
No Event Sampling
Job
Smart Mode
Events (1)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 millisecond per column
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
action 1
index 1
ip 1
linecount 1
punct 1
splunk_server 1
Time
Event
12/26/25
10:38:00.000 AM
2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt
2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success
2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed
2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success
Show all 50 lines
host = LAPTOP-AHPR42ME
source = SOC_Task2_Sample_Logs.txt
sourcetype = misc_text

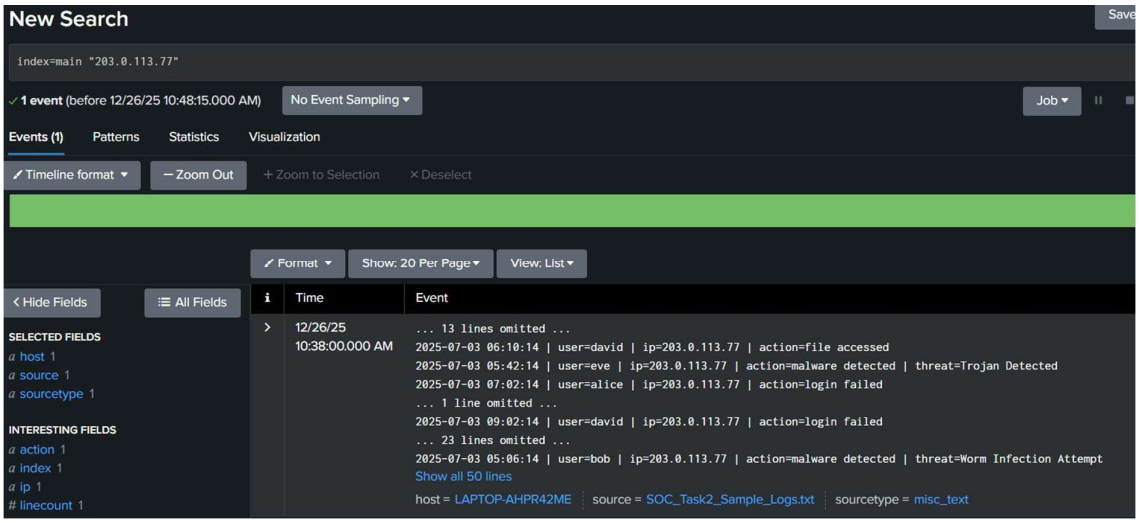
6.


New Search
Save As
Create Table View
Close
index=main "malware detected"
Time range: All time
1 event (before 12/26/25 10:44:22.000 AM)
No Event Sampling
Job
Smart Mode
Events (1)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 millisecond per column
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
action 1
index 1
ip 1
Time
Event
12/26/25
10:38:00.000 AM
... 10 lines omitted ...
2025-07-03 08:00:14 | user=alice | ip=198.51.100.42 | action=login success
2025-07-03 04:19:14 | user=alice | ip=198.51.100.42 | action=malware detected | threat=Rootkit Signature
2025-07-03 05:30:14 | user=eve | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
... 12 lines omitted ...
2025-07-03 04:29:14 | user=alice | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature
Show all 50 lines
host = LAPTOP-AHPR42ME
source = SOC_Task2_Sample_Logs.txt
sourcetype = misc_text

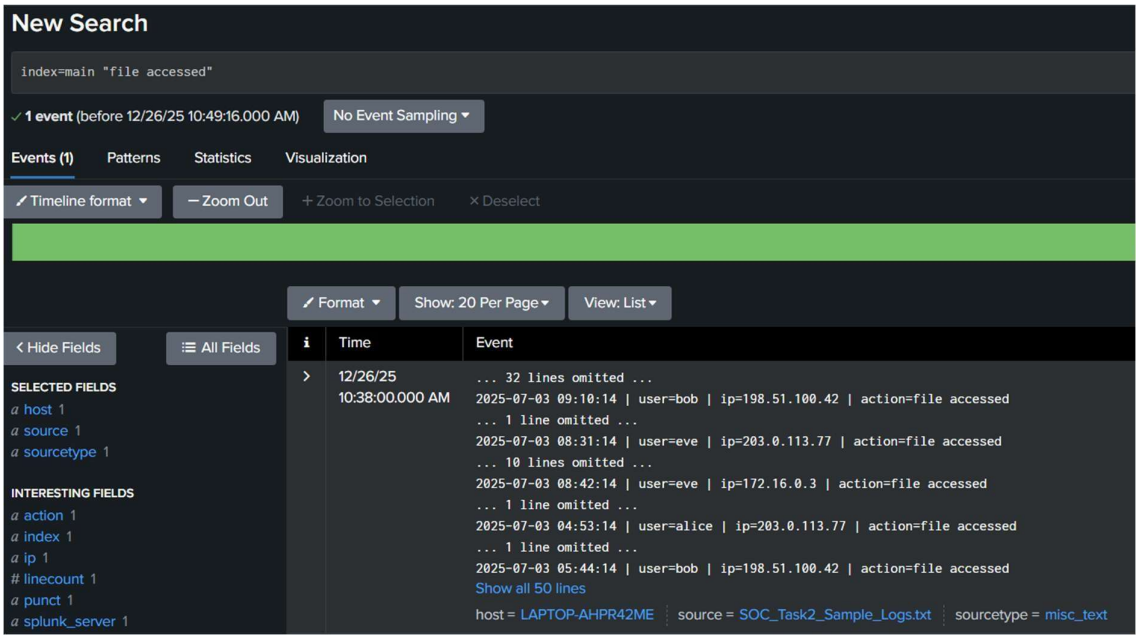
7.


New Search
Save
index=main "login failed"
1 event (before 12/26/25 10:46:15.000 AM)
No Event Sampling
Job
Events (1)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
action 1
index 1
Time
Event
12/26/25
10:38:00.000 AM
... 15 lines omitted ...
2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed
2025-07-03 04:18:14 | user=bob | ip=198.51.100.42 | action=login success
2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success
2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed
Show all 50 lines
host = LAPTOP-AHPR42ME
source = SOC_Task2_Sample_Logs.txt
sourcetype = misc_text

8.


New Search
Save
index=main "203.0.113.77"
✓ 1 event (before 12/26/25 10:48:15.000 AM)
No Event Sampling
Job
Events (1)
Patterns
Statistics
Visualization
Timeline format
– Zoom Out
+ Zoom to Selection
× Deselect
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
a index 1
a ip 1
linecount 1
Time
Event
12/26/25
10:38:00.000 AM
... 13 lines omitted ...
2025-07-03 06:10:14 | user=david | ip=203.0.113.77 | action=file accessed
2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected
2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed
... 1 line omitted ...
2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
... 23 lines omitted ...
2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt
Show all 50 lines
host = LAPTOP-AHPR42ME
source = SOC_Task2_Sample_Logs.txt
sourcetype = misc_text

9.


New Search
index=main "file accessed"
✓ 1 event (before 12/26/25 10:49:16.000 AM)
No Event Sampling
Events (1)
Patterns
Statistics
Visualization
Timeline format
– Zoom Out
+ Zoom to Selection
× Deselect
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
a index 1
a ip 1
linecount 1
a punct 1
a splunk_server 1
Time
Event
12/26/25
10:38:00.000 AM
... 32 lines omitted ...
2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
... 1 line omitted ...
2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed
... 10 lines omitted ...
2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed
... 1 line omitted ...
2025-07-03 04:53:14 | user=alice | ip=203.0.113.77 | action=file accessed
... 1 line omitted ...
2025-07-03 05:44:14 | user=bob | ip=198.51.100.42 | action=file accessed
Show all 50 lines
host = LAPTOP-AHPR42ME
source = SOC_Task2_Sample_Logs.txt
sourcetype = misc_text