Security Alert Monitoring & Incident Response Report

Future Interns – Cyber Security Internship (Task 2)

Name of Candidate: Shruti Mate
Internship Provider: Future Interns
Domain: Cyber Security (SOC Operations)
Date of Execution: December 2025
Tool Used: Splunk Enterprise

---

1. Introduction

A Security Operations Center (SOC) is responsible for continuously monitoring organizational systems to detect, analyze, and respond to cybersecurity threats. SOC analysts review security alerts and log data to identify malicious activities and minimize potential risks.

This task simulates real-world SOC operations by using a SIEM platform to analyze system and network logs. The objective was to identify suspicious activities, classify incidents based on severity, and recommend appropriate response actions, similar to the responsibilities of a SOC analyst in a real organization.

---

2. Objective

The primary objectives of this task were:

- To gain hands-on experience with a SIEM tool
- To monitor and analyze security logs
- To identify and classify security incidents
- To understand incident response procedures
- To document findings in a professional SOC report

---

3. Tool Used

Splunk Enterprise

Splunk Enterprise is a widely used SIEM solution that enables real-time log ingestion, searching, and analysis of machine-generated data. In this task, Splunk was used to ingest simulated security logs and perform keyword-based searches to detect potential security incidents.

---

4. Log Source Description

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

- Successful and failed authentication attempts
- Network connection and access events
- File access activities
- Malware detection alerts

The logs were ingested as **unstructured data (misc_text)**, requiring keyword-based searches and manual analysis to identify security incidents.

---

5. Incident Detection Methodology

The following approach was followed during the analysis:

- Upload the provided logs into Splunk
- Identify relevant keywords related to security events
- Analyze patterns such as repeated login failures and malware alerts
- Correlate events to identify suspicious behaviour
- Classify incidents based on severity
- Document impact and recommended response actions

---

6. Stakeholder Notification Draft

Subject: Security Incident Alert : Malware Activity Identified

Dear Management Team,

During routine security monitoring using the SIEM platform, multiple malware-related alerts were identified in system logs. These events have been classified as **High Severity** due to the detection of malicious indicators such as Trojan and Rootkit signatures.

Immediate actions have been recommended, including system isolation, enhanced monitoring, and malware remediation to prevent further impact. A detailed incident response report has been prepared outlining the findings and suggested corrective measures.

Please let us know if further clarification or action is required.

Regards,
Shruti Mate
SOC Analyst Intern
Future Interns

---

7. Identified Security Incidents

Incident 1: Malware Infection Detected

Search Query Used:
index=main "malware detected"

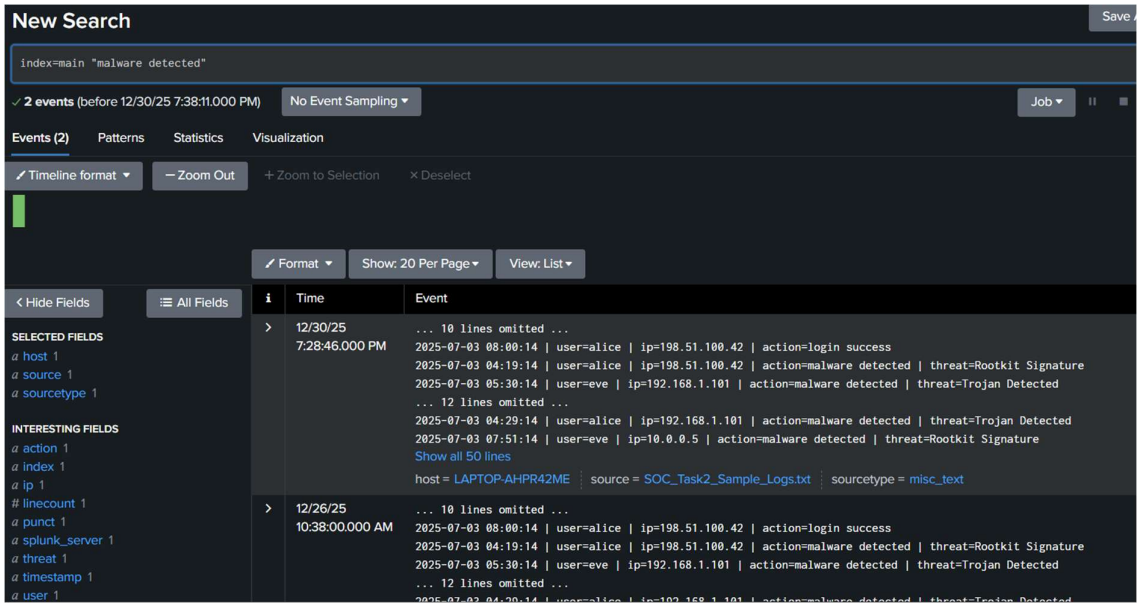
Description:
Multiple malware alerts were identified in the logs, including threats such as Trojan Detected, Rootkit Signature, and Worm Infection Attempt. These events indicate potential compromise of affected systems.

Severity: High

Impact:
Malware infections can result in data theft, system instability, and unauthorized access.

Recommended Response:

- Isolate affected systems
- Perform full malware scans
- Remove malicious files
- Apply security patches



Incident 2: Multiple Failed Login Attempts

Search Query Used:
index=main "login failed"

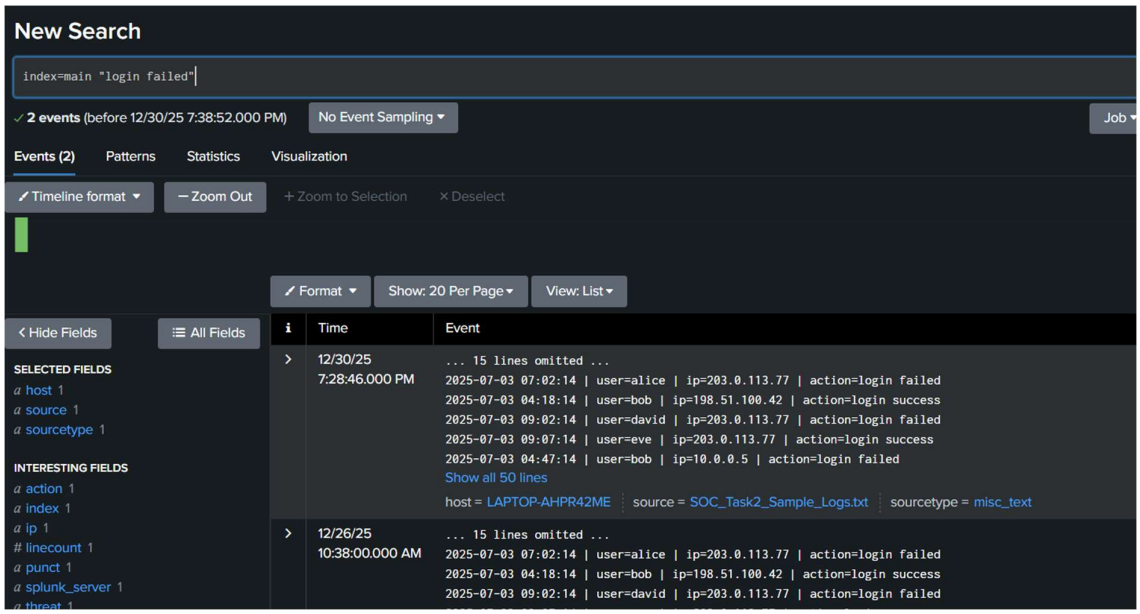
Description:
Repeated failed login attempts were observed from specific IP addresses, suggesting possible brute-force or credential-guessing attacks.

Severity: Medium

Impact:
May lead to account compromise if attacks succeed.

Recommended Response:

- Enable account lockout mechanisms
- Enforce strong password policies
- Monitor and block suspicious IP addresses



Incident 3: Suspicious IP Address Activity

Search Query Used:
index=main "203.0.113.77"

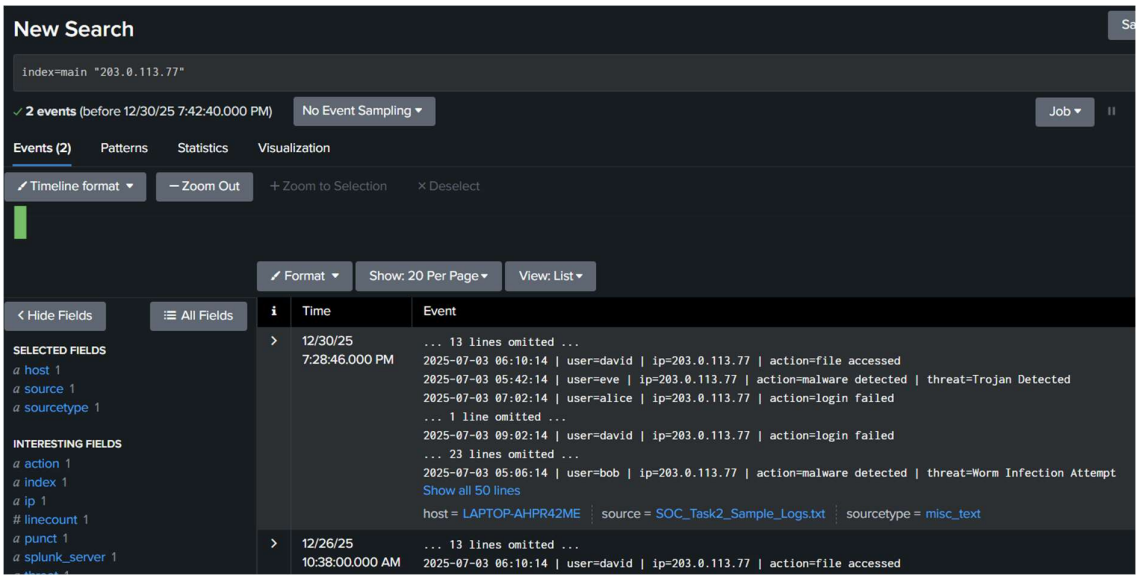
Description:
The same external IP address was involved in multiple activities such as login failures, malware detection, and file access, indicating coordinated malicious behavior.

Severity: Medium

Impact:
Suggests reconnaissance or multi-stage attack attempts.

Recommended Response:

- Block or restrict the suspicious IP
- Monitor network traffic
- Apply firewall and IDS/IPS rules



Incident 4: Unusual File Access Activity

Search Query Used:
index=main "file accessed"

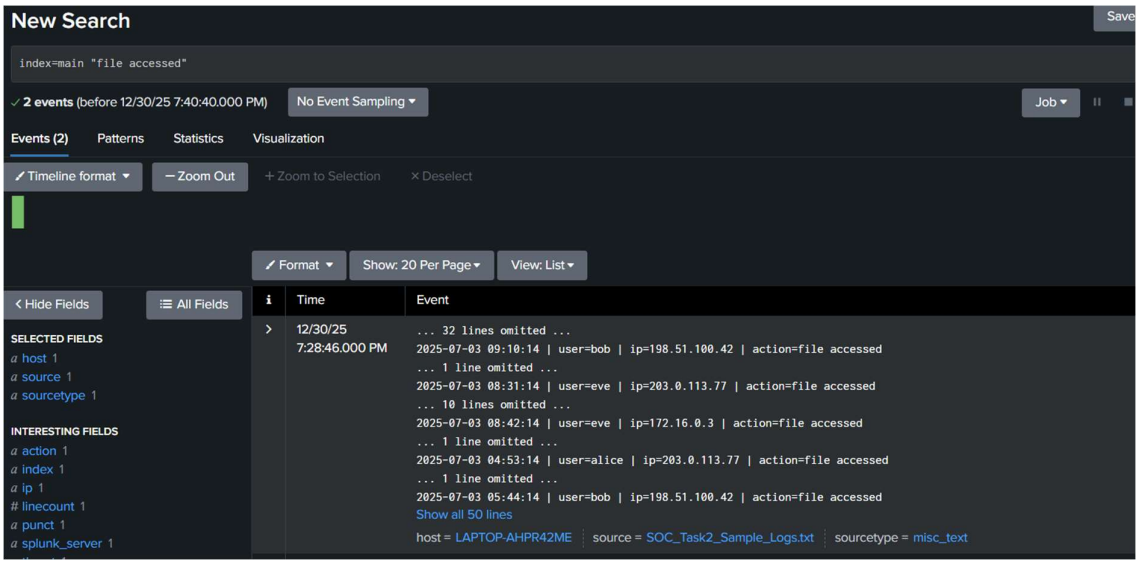
Description:
Unusual file access events were detected that may indicate unauthorized or abnormal access to system resources.

Severity: Low

Impact:
Potential data exposure or misuse of sensitive files.

Recommended Response:

- Review user access permissions
- Implement strict access control policies
- Enable file activity monitoring



8. Incident Severity Classification Summary

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

---

9. Challenges Faced

- Understanding SIEM workflows in Splunk
- Working with unstructured log data
- Correlating multiple events to identify attack patterns

---

10. Learning Outcomes

Through this task, the following skills were developed:

- Understanding SOC operations and alert monitoring
- Practical experience with Splunk SIEM
- Incident classification and severity assessment
- Importance of timely incident response
- Professional documentation of security incidents

---

11. Conclusion

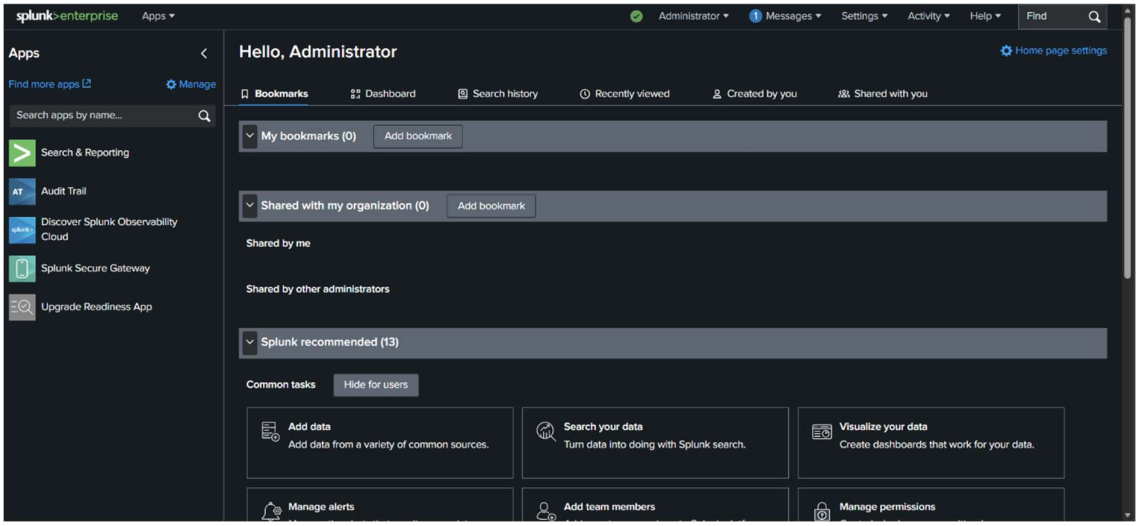
This task provided hands-on exposure to SOC alert monitoring and incident response activities. By analyzing security logs using Splunk, multiple security incidents were successfully identified and classified. The exercise demonstrated the importance of continuous monitoring, effective analysis, and timely response in maintaining a secure environment.

---

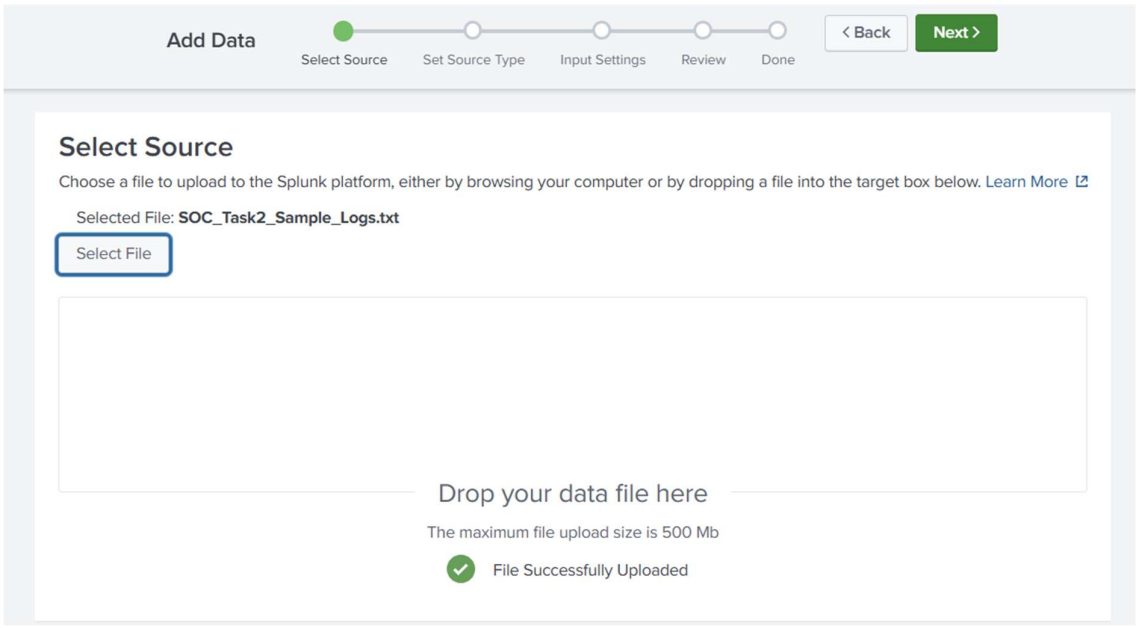
12. Screenshots & Evidence

Relevant screenshots were captured during Splunk analysis to support the findings. These include evidence of malware detection, failed login attempts, suspicious IP activity, and file access events.

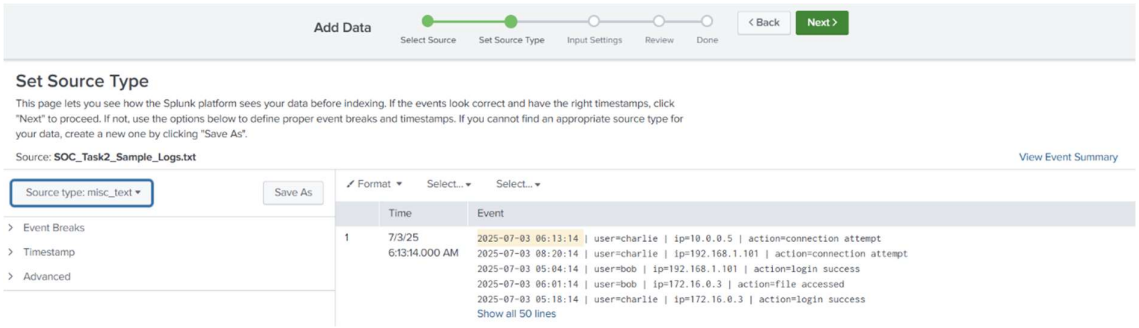
1.


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Apps
Find more apps
Manage
Search apps by name...
Search & Reporting
Audit Trail
Discover Splunk Observability Cloud
Splunk Secure Gateway
Upgrade Readiness App
Hello, Administrator
Home page settings
Bookmarks
Dashboard
Search history
Recently viewed
Created by you
Shared with you
My bookmarks (0)
Add bookmark
Shared with my organization (0)
Add bookmark
Shared by me
Shared by other administrators
Splunk recommended (13)
Common tasks
Hide for users
Add data
Add data from a variety of common sources.
Search your data
Turn data into doing with Splunk search.
Visualize your data
Create dashboards that work for your data.
Manage alerts
Add team members
Manage permissions

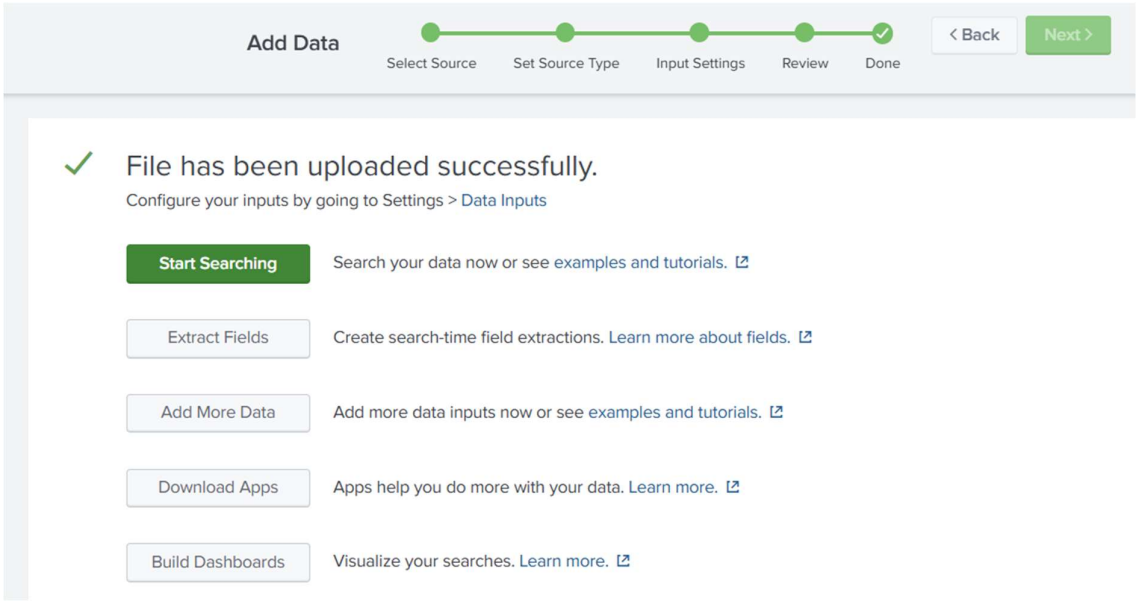
2.


Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Next
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

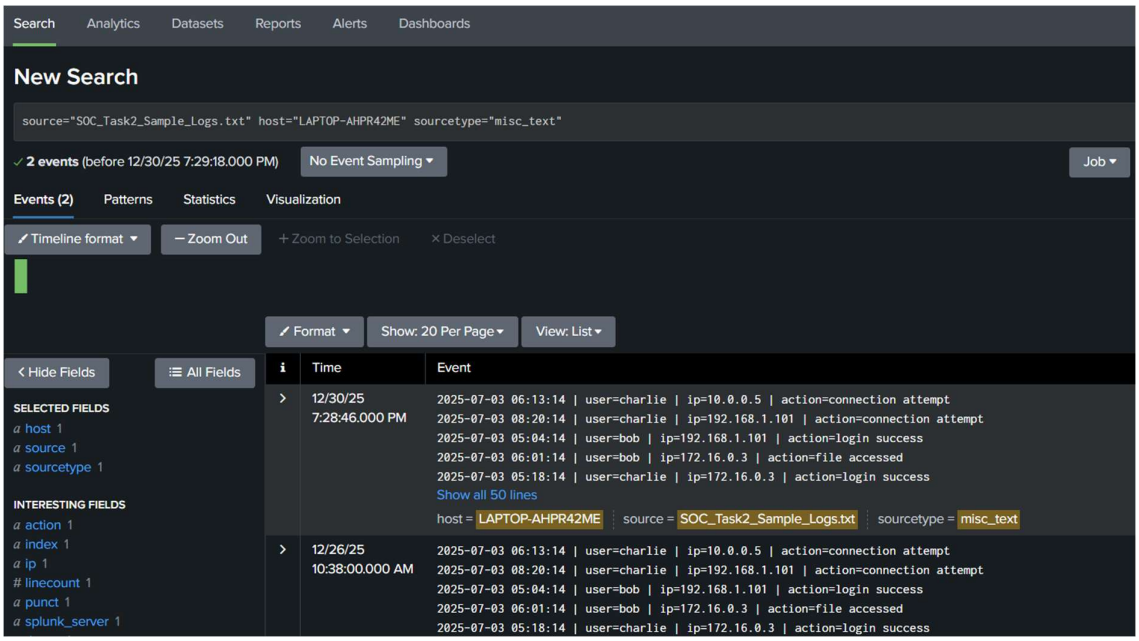
3.


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: misc_text
Save As
Event Breaks
Timestamp
Advanced
Format
Select...
Select...
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
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

4.


Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Next
File has been uploaded successfully.
Configure your inputs by going to Settings > Data Inputs
Start Searching
Search your data now or see examples and tutorials.
Extract Fields
Create search-time field extractions. Learn more about fields.
Add More Data
Add more data inputs now or see examples and tutorials.
Download Apps
Apps help you do more with your data. Learn more.
Build Dashboards
Visualize your searches. Learn more.

5.


Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
source="SOC_Task2_Sample_Logs.txt" host="LAPTOP-AHPR42ME" sourcetype="misc_text"
2 events (before 12/30/25 7:29:18.000 PM)
No Event Sampling
Job
Events (2)
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
12/30/25
7:28:46.000 PM
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
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