

TASK-02

Intern Name: Pulugu Sirivarshini

Project Title: Security Log Monitoring & Threat Analysis using Splunk

Tool Used: Splunk Free Trial

Log Source: sample_soc_logs.csv (Simulated Security Event Logs)

Objective

To simulate the activities of a SOC analyst by monitoring logs, identifying threats, analyzing patterns, and generating insights using SIEM (Splunk). The goal was to detect suspicious events such as failed login attempts, unauthorized access, or malware alerts, and respond effectively.

Tools & Techniques Applied

- Log ingestion using Splunk's upload function
- Filtering and searching using SPL
- Pattern detection using stats, top, and event filtering
- Severity-based event triage

Open splunk and Login using your admin username and password

Log Ingestion and Index Creation

1. Go to "Add Data" → Choose "Upload"
2. Select File: Upload sample_soc_logs.csv
3. Source Type: Select "CSV"
4. Create Index: Name it soc_logs
5. Click Next → Review → Submit

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

Add Data

Select SourceSet Source TypeInput SettingsReviewDone

< BackNext >

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: **sample_soc_logs.csv**

Select File

Drop your data file here

The maximum file upload size is 500 Mb

File Successfully Uploaded

FAQ

- > What kinds of files can the Splunk platform index?
- > What is a source?
- > How do I get remote data onto my Splunk platform instance?

34°C Mostly cloudy

Search web & PC

ENG IN

13:51 29-06-2025

splunk>enterpriseApps

AdministratorMessagesSettingsActivityHelpFind

Add Data

Select SourceSet Source TypeInput SettingsReviewDone

< BackNext >

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: **sample_soc_logs.csv** [View Event Summary](#)

Source type: csvSave As

> Timestamp

> Delimited settings

> Advanced

	_time	destination_ip	event_type	message	severity	source_ip	timestamp	user
1	6/28/25 6:50:15.000 PM	10.0.0.5	failed_login	10 failed logins from same IP	High	192.168.1.10	2025-06-28T13:20:15Z	admin
2	6/28/25 6:53:45.000 PM	10.0.0.3	malware_detected	Malware signature XYZ detected	High	103.88.44.11	2025-06-28T13:23:45Z	jane
3	6/28/25 7:31:20.000 PM	10.0.0.6	login_success	Login successful	Low	10.1.1.45	2025-06-28T14:01:20Z	bob
4	6/28/25 7:35:10.000 PM	10.0.0.7	unauthorized_access	Access to restricted folder	Medium	200.150.80.22	2025-06-28T14:05:10Z	root
5	6/28/25 7:40:00.000 PM	10.0.0.8	password_change	User changed password	Low	172.16.2.20	2025-06-28T14:10:00Z	alice

splunk>enterpriseApps

AdministratorMessagesSettings

Add Data

Select SourceSet Source TypeInput SettingsReviewDone

< BackNext >

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](#).

127.0.0.1:8000/en-US/app/search/search?q=search%20source%3D%20sample_soc_logs.csv%20host%3D%20siri%20index%3D%20soc_logs%20sourcetype%3D%20csv%20earliest=0&latest=0

New Search

source="sample_soc_logs.csv" host="siri" index="soc_logs" sourcetype="csv" All time

✓ 10 events (before 6/29/25 1:56:06.000 PM) No Event Sampling

Events (10) Patterns Statistics Visualization

Timeline format Zoom Out + Zoom to Selection X Deselect 1 minute per column

Format Show: 50 Per Page View List

Time	Event
6/28/25 7:40:00.000 PM	2025-06-28T14:10:00Z,172.16.2.20,10.0.0.8,alice,password_change,Low,User changed password host = siri source = sample_soc_logs.csv sourcetype = csv
6/28/25 7:40:00.000 PM	2025-06-28T14:10:00Z,172.16.2.20,10.0.0.8,alice,password_change,Low,User changed password host = siri source = sample_soc_logs.csv sourcetype = csv
6/28/25 7:35:10.000 PM	2025-06-28T14:05:10Z,200.158.86.22,10.0.0.7,root,unauthorized_access,Medium,Access to restricted folder host = siri source = sample_soc_logs.csv sourcetype = csv
6/28/25 7:35:10.000 PM	2025-06-28T14:05:10Z,200.158.86.22,10.0.0.7,root,unauthorized_access,Medium,Access to restricted folder host = siri source = sample_soc_logs.csv sourcetype = csv
6/28/25 7:31:20.000 PM	2025-06-28T14:01:20Z,10.1.1.45,10.0.0.6,bob,login_success,Low,Login successful host = siri source = sample_soc_logs.csv sourcetype = csv
6/28/25 7:31:20.000 PM	2025-06-28T14:01:20Z,10.1.1.45,10.0.0.6,bob,login_success,Low,Login successful host = siri source = sample_soc_logs.csv sourcetype = csv
6/28/25 6:53:45.000 PM	2025-06-28T13:23:45Z,103.88.44.11,10.0.0.3,jane,malware_detected,High,Malware signature XYZ detected

splunk enterprise Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

index=soc_logs | stats count by event_type, severity All time

✓ 10 events (before 6/29/25 1:57:10.000 PM) No Event Sampling

Events Patterns Statistics (5) Visualization

Show: 20 Per Page Format Preview: On

event_type	severity	count
failed_login	High	2
login_success	Low	2
malware_detected	High	2
password_change	Low	2
unauthorized_access	Medium	2

splunk enterprise Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search

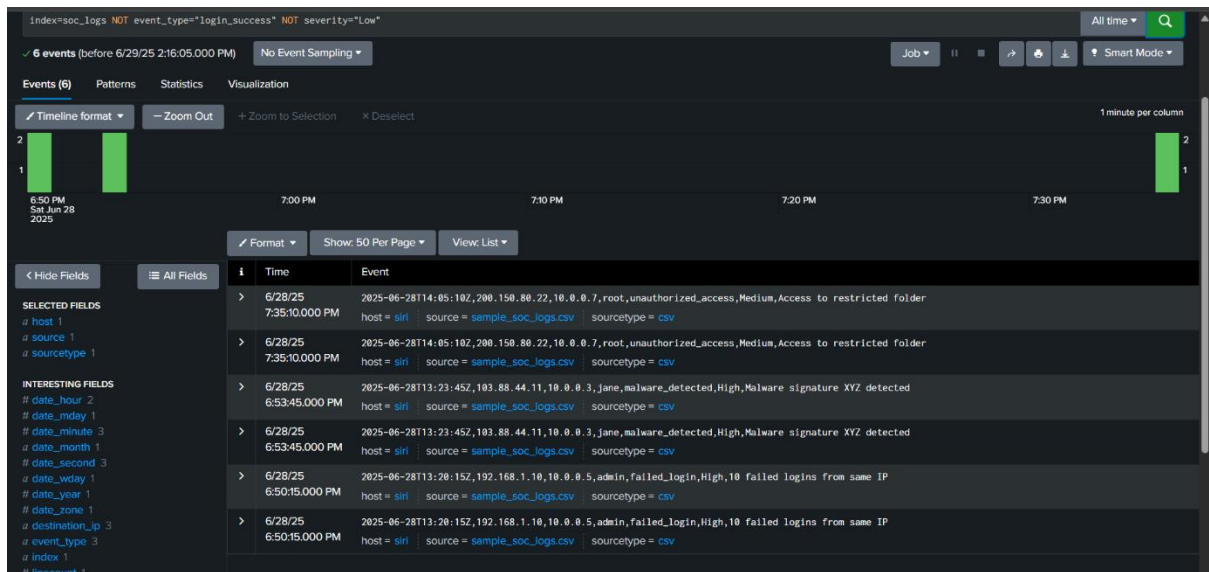
index=soc_logs | timechart count by event_type All time

✓ 10 events (before 6/29/25 1:58:19.000 PM) No Event Sampling

Events Patterns Statistics (10) Visualization

Show: 20 Per Page Format Preview: On

_time	failed_login	login_success	malware_detected	password_change	unauthorized_access
2025-06-28 18:50:00	2	0	0	0	0
2025-06-28 18:50:30	0	0	0	0	0
2025-06-28 18:51:00	0	0	0	0	0
2025-06-28 18:51:30	0	0	0	0	0
2025-06-28 18:52:00	0	0	0	0	0
2025-06-28 18:52:30	0	0	0	0	0
2025-06-28 18:53:00	0	0	0	0	0
2025-06-28 18:53:30	0	0	2	0	0
2025-06-28 18:54:00	0	0	0	0	0
2025-06-28 18:54:30	0	0	0	0	0
2025-06-28 18:55:00	0	0	0	0	0
2025-06-28 18:55:30	0	0	0	0	0



Conclusion:

In conclusion, by uploading and analyzing the simulated log file (sample_soc_logs.csv) in Splunk, I was able to apply key SOC analyst skills such as threat detection, event classification, and incident reporting. Using a custom index (soc_logs) and relevant SPL queries, I successfully identified critical security events including repeated failed login attempts, malware detections, and unauthorized access incidents.