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.

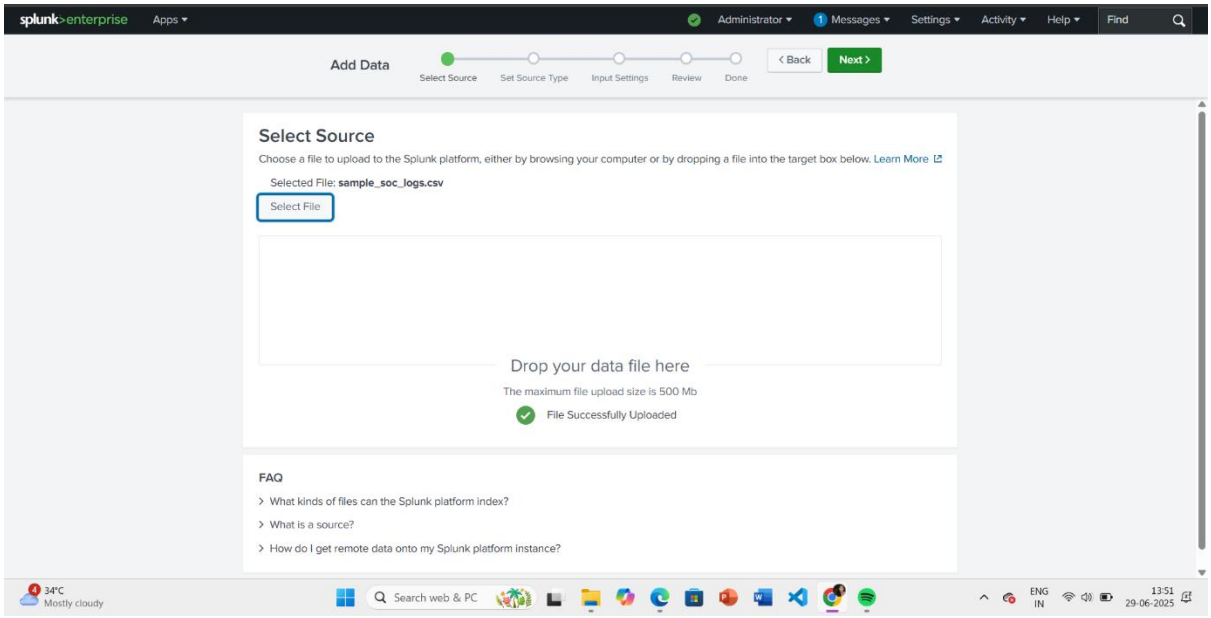
Tools & Techniques Applied

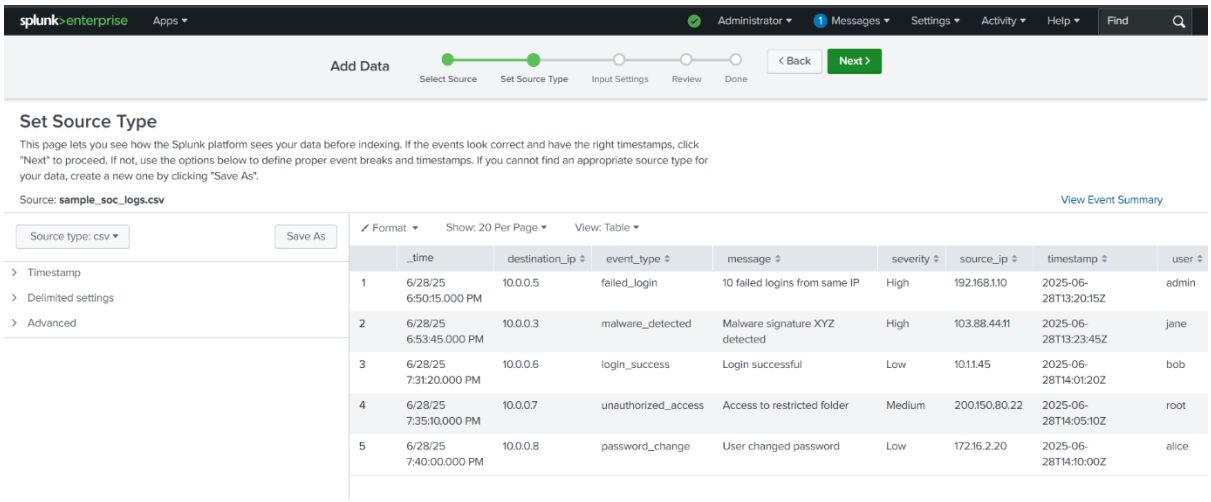
- Log ingestion using Splunk's upload function
- Filtering and searching using SPL
- Pattern detection using stats, top, and event filtering
- Severity-based event triage

Open splunk and Login using your admin username and password

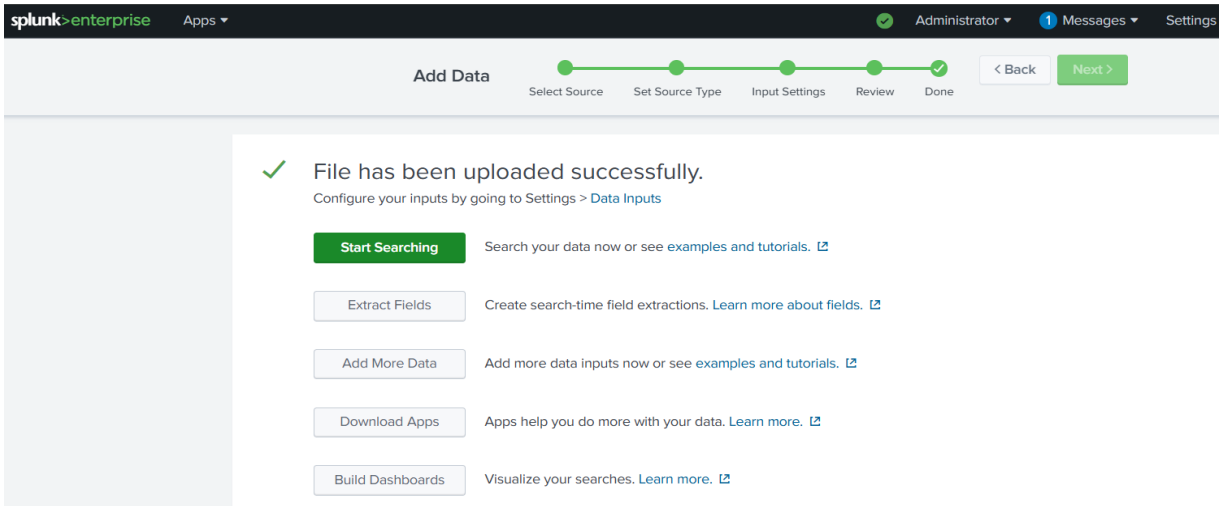
Log Ingestion and Index Creation

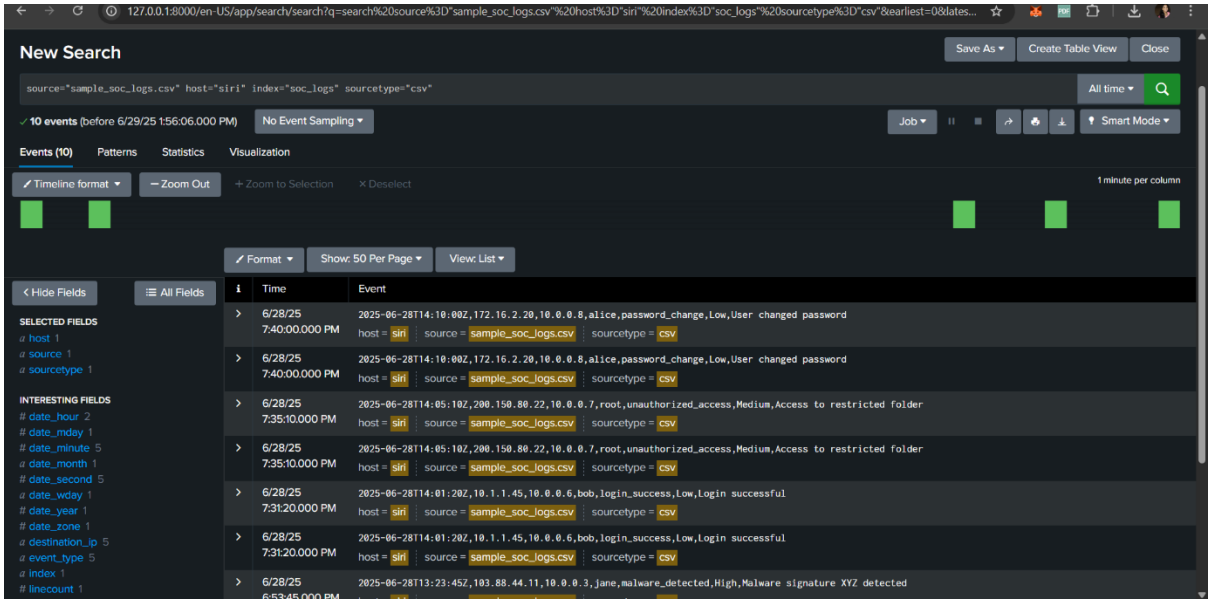
1. Go to "Add Data" → Choose "Upload"
2. Select File: Upload sample_soc_logs.csv
3. Source Type: Select "CSV"
4. Create Index: Name it soc_logs
5. Click Next → Review → Submit

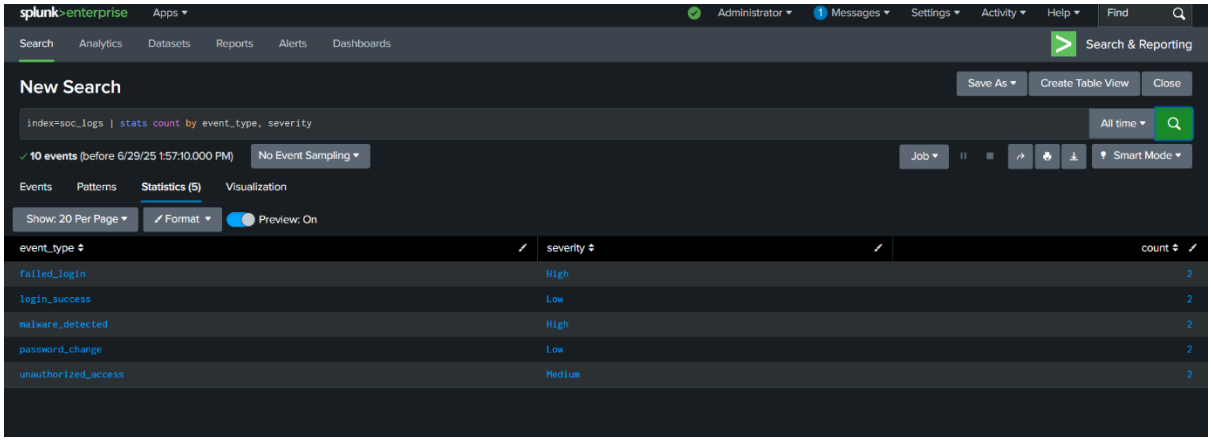


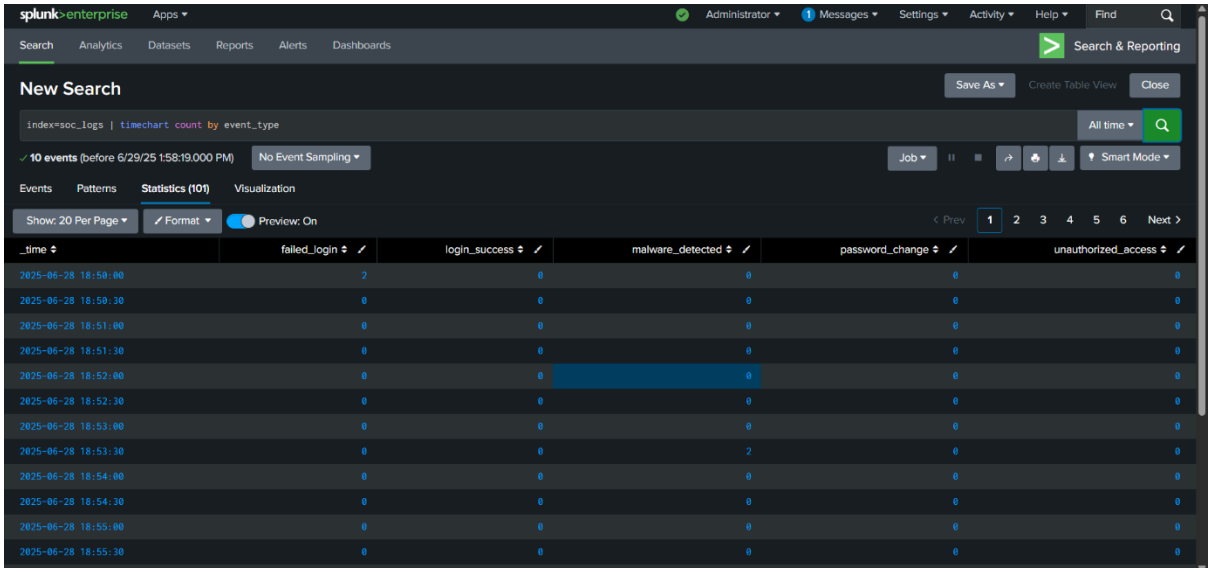


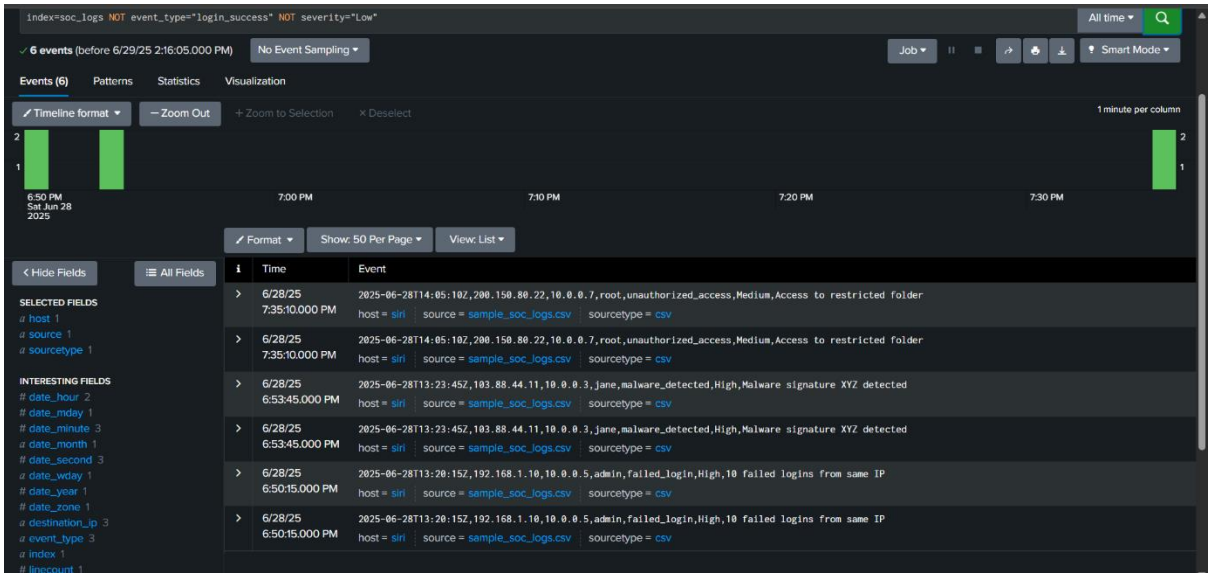
	_time	destination_ip	event_type	message	severity	source_ip	timestamp	user
1	6/28/25 6:50:15.000 PM	10.0.0.5	failed_login	10 failed logins from same IP	High	192.168.1.10	2025-06-28T13:20:15Z	admin
2	6/28/25 6:53:45.000 PM	10.0.0.3	malware_detected	Malware signature XYZ detected	High	103.88.44.11	2025-06-28T13:23:45Z	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




New Search
Save As
Create Table View
Close
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
Job
Smart Mode
Events (10)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 minute per column
Format
Show: 50 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
date_hour 2
date_mday 1
date_minute 5
date_month 1
date_second 5
date_wday 1
date_year 1
date_zone 1
destination_ip 5
event_type 5
index 1
linecount 1
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,200.150.80.22,10.0.0.7,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,200.150.80.22,10.0.0.7,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
2025-06-28T13:23:45Z,103.88.44.11,10.0.0.3,jane,malware_detected,High,Malware signature XYZ detected


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
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
Job
Smart Mode
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
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=soc_logs | timechart count by event_type
All time
10 events (before 6/29/25 1:58:19.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (101)
Visualization
Show: 20 Per Page
Format
Preview: On
Prev
1
2
3
4
5
6
Next
_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.