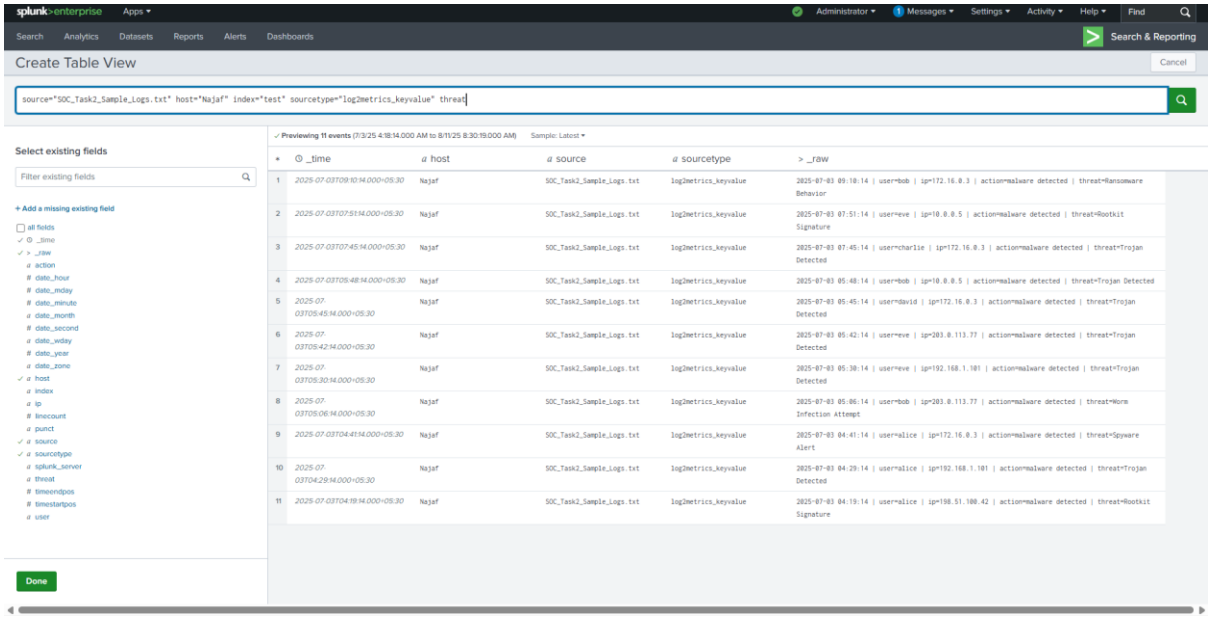
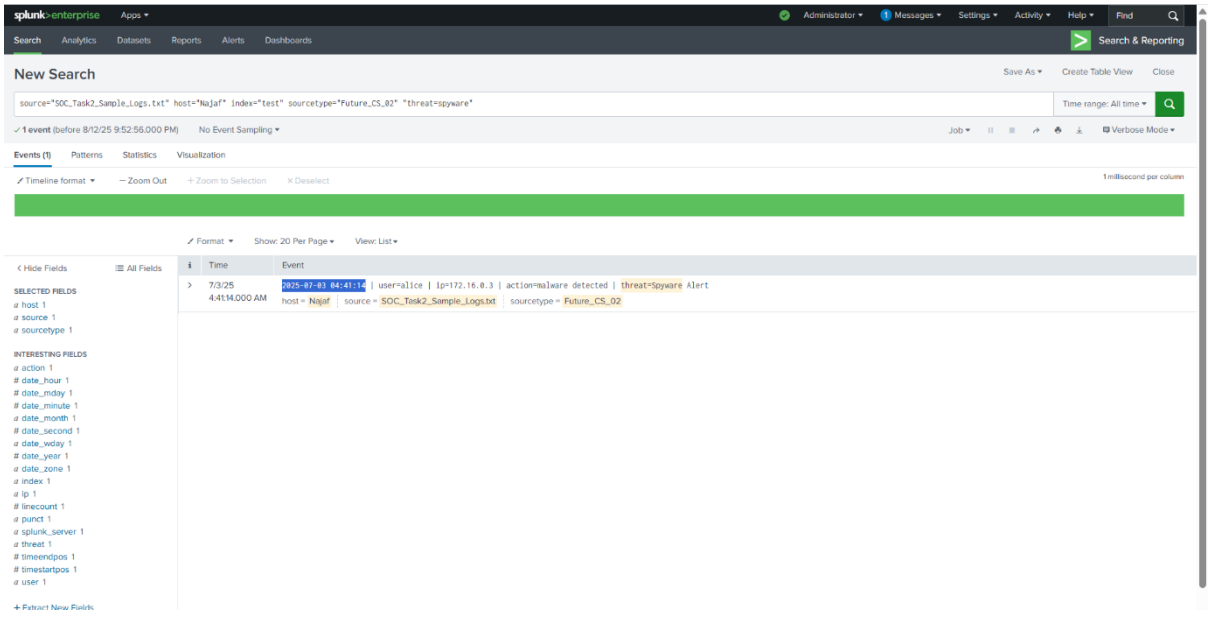
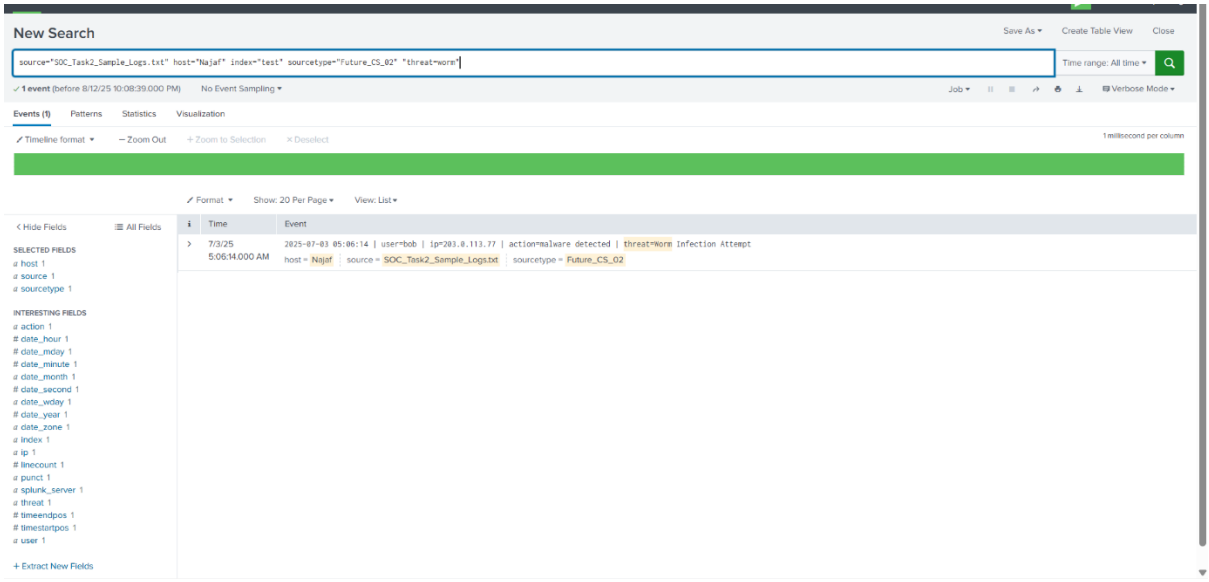
Threats:



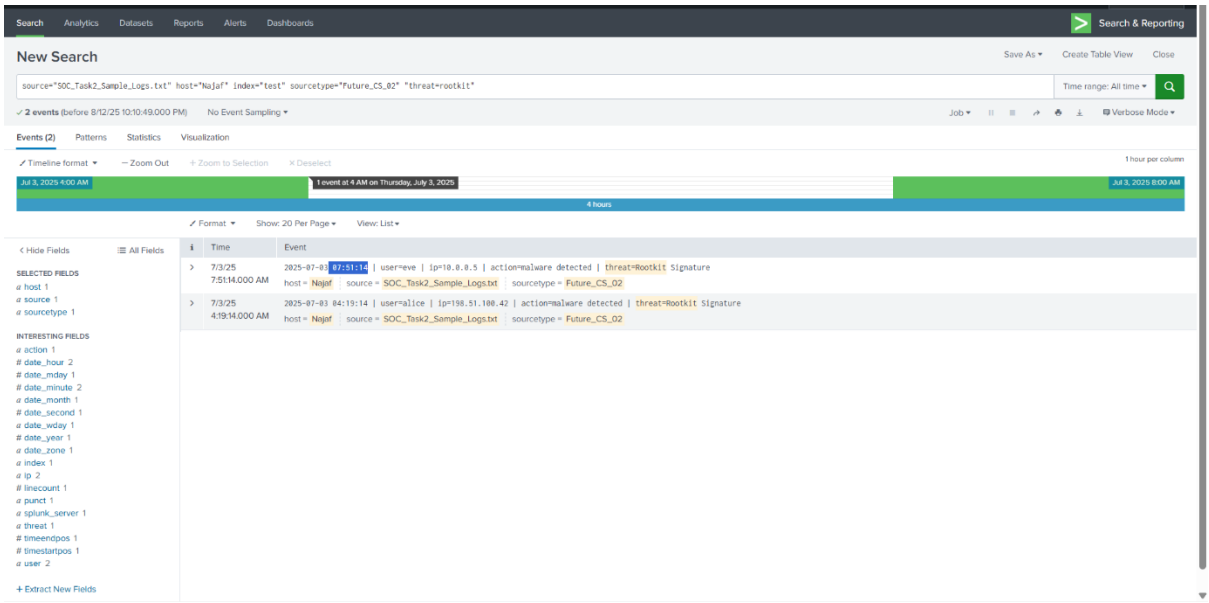
Spyware:



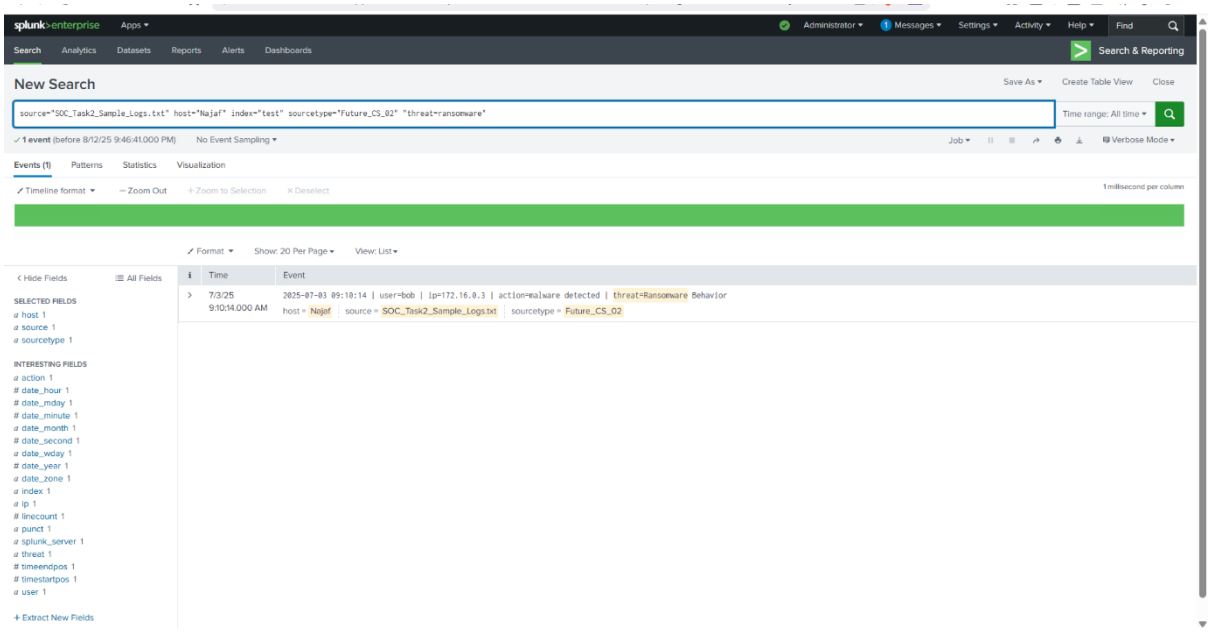
Worm:



Rootkit:



Ransomware:


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="Najaf" index="test" sourcetype="Future_CS_02" "threat=ransomware"
Time range: All time
1 event (before 8/12/25 9:46:41.000 PM)
No Event Sampling
Job
Verbose 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
date_hour 1
date_mday 1
date_minute 1
date_month 1
date_second 1
date_wday 1
date_year 1
date_zone 1
index 1
ip 1
linecount 1
punct 1
splunk_server 1
threat 1
timeendpos 1
timestartpos 1
user 1
Extract New Fields
Time
Event
7/3/25
9:10:14.000 AM
2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
host = Najaf
source = SOC_Task2_Sample_Logs.txt
sourcetype = Future_CS_02