

Threats:

spunk:enterpriseApps

SearchAnalyticsDatasetsReportsAlertsDashboards

Create Table View

source="SOC_Task2_Sample_Logs.txt" host="Najaf" index="test" sourcetype="logmetrics_keyvalue" threat

Filter existing fields

all fields

Q_time

time

action

date_hour

date_mday

date_minute

date_month

date_second

date_wday

date_year

date_zone

host

index

ip

linecount

punct

source

splunk_server

threat

timeendpos

timestamppos

user

Previewing 11 events (7/3/25 4:18:14.000 AM to 8/11/25 8:30:19.000 AM) Sample: Latest

#	Q_time	host	source	sourcetype	> _raw
1	2025-07-03T07:00:00+05:30	Najaf	SOC_Task2_Sample_Logs.txt	logmetrics_keyvalue	2025-07-03 09:10:14 user=Bob ip=172.16.0.3 action=malware detected threat=ransomware Behavior
2	2025-07-03T07:01:14+05:30	Najaf	SOC_Task2_Sample_Logs.txt	logmetrics_keyvalue	2025-07-03 07:51:14 user=ve ip=10.0.0.5 action=malware detected threat=Rootkit Signature
3	2025-07-03T07:45:14+05:30	Najaf	SOC_Task2_Sample_Logs.txt	logmetrics_keyvalue	2025-07-03 07:45:14 user=charlie ip=172.16.0.3 action=malware detected threat=Trojan Detected
4	2025-07-03T08:48:14+05:30	Najaf	SOC_Task2_Sample_Logs.txt	logmetrics_keyvalue	2025-07-03 05:48:14 user=Bob ip=10.0.0.5 action=malware detected threat=Trojan Detected
5	2025-07-03T09:45:14+05:30	Najaf	SOC_Task2_Sample_Logs.txt	logmetrics_keyvalue	2025-07-03 05:45:14 user=David ip=172.16.0.3 action=malware detected threat=Trojan Detected
6	2025-07-03T09:42:14+05:30	Najaf	SOC_Task2_Sample_Logs.txt	logmetrics_keyvalue	2025-07-03 05:42:14 user=ve ip=203.8.113.77 action=malware detected threat=Trojan Detected
7	2025-07-03T09:30:14+05:30	Najaf	SOC_Task2_Sample_Logs.txt	logmetrics_keyvalue	2025-07-03 05:30:14 user=ve ip=192.168.1.101 action=malware detected threat=Trojan Detected
8	2025-07-03T09:06:14+05:30	Najaf	SOC_Task2_Sample_Logs.txt	logmetrics_keyvalue	2025-07-03 05:06:14 user=Bob ip=203.8.113.77 action=malware detected threat=Worm Infection Attempt
9	2025-07-03T04:41:14+05:30	Najaf	SOC_Task2_Sample_Logs.txt	logmetrics_keyvalue	2025-07-03 04:41:14 user=alice ip=172.16.0.3 action=malware detected threat=Spware Alert
10	2025-07-03T04:29:14+05:30	Najaf	SOC_Task2_Sample_Logs.txt	logmetrics_keyvalue	2025-07-03 04:29:14 user=alice ip=192.168.1.101 action=malware detected threat=Trojan Detected
11	2025-07-03T04:19:14+05:30	Najaf	SOC_Task2_Sample_Logs.txt	logmetrics_keyvalue	2025-07-03 04:19:14 user=alice ip=198.51.100.42 action=malware detected threat=Rootkit Signature

Spyware:

spunk:enterpriseApps

SearchAnalyticsDatasetsReportsAlertsDashboards

New Search

source="SOC_Task2_Sample_Logs.txt" host="Najaf" index="test" sourcetype="Future_CS_02" threat="spyware"

Time range: All time

1 event (before 8/12/25 9:52:56.000 PM) No Event Sampling

Job

Events (1)

Timeline format

Zoom Out

Zoom to Selection

Deselect

1 millisecond per column

Hide Fields

All Fields

Time

Event

7/3/25 4:41:14.000 AM

2025-07-03 04:41:14 | user=alice | ip=172.16.0.3 | action=malware detected | threat=Spware Alert

host = Najaf

source = SOC_Task2_Sample_Logs.txt

sourcetype = Future_CS_02

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

timestamppos 1

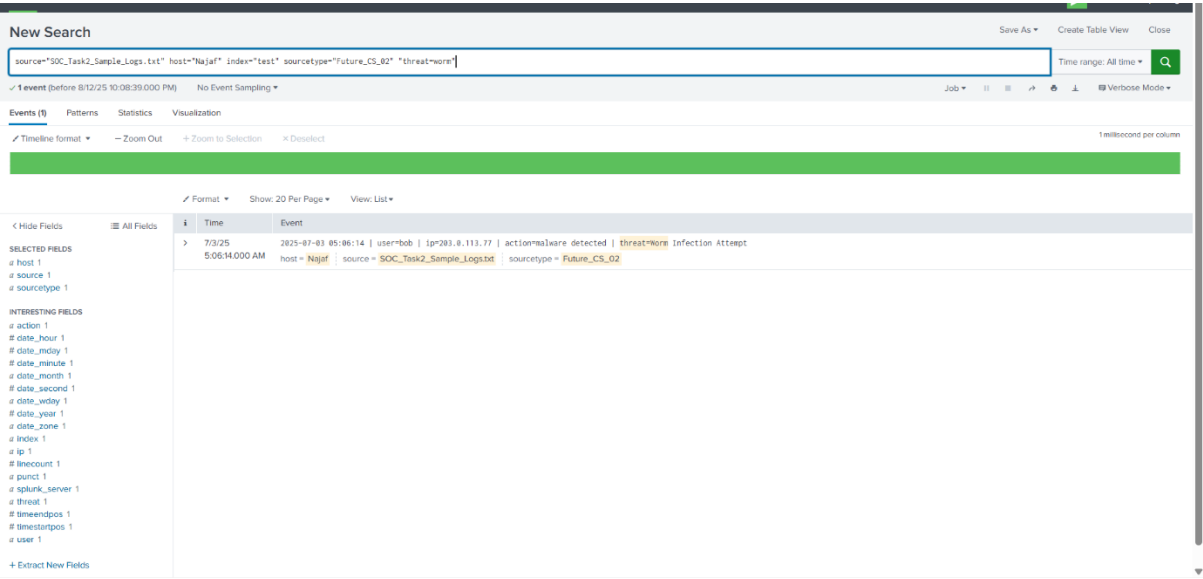
user 1

Format

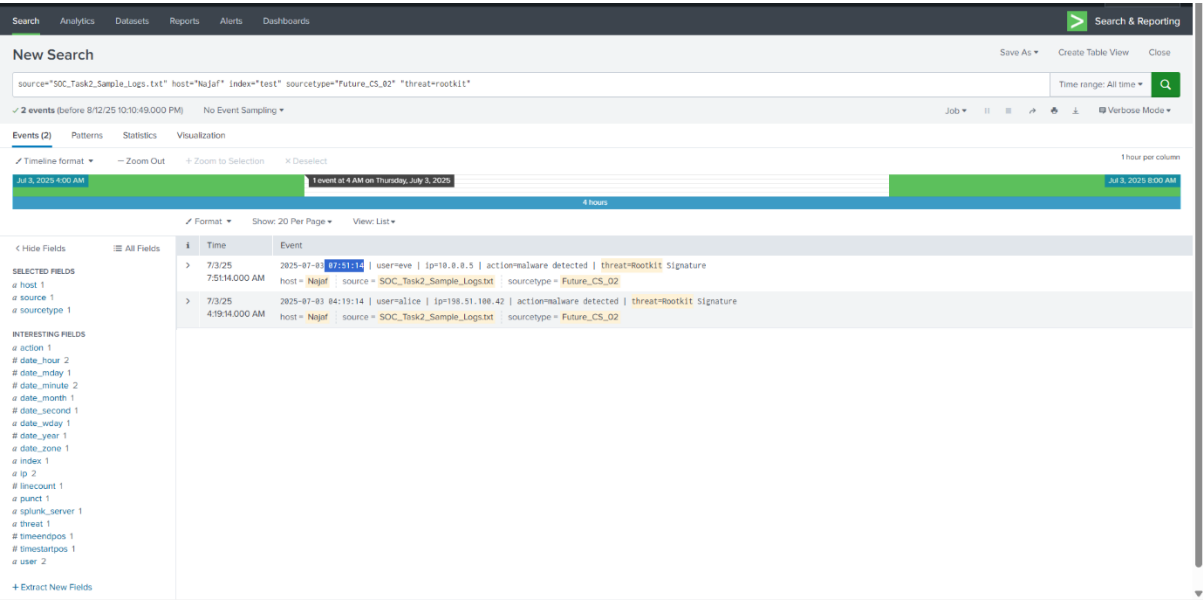
Show: 20 Per Page

View: List

Worm:



Rootkit:



Splunk Enterprise Apps Administrator Messages Settings Activity Help Find 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 Views Actions Verbose Mode

Events Patterns Statistics Visualization

✓ Timeline format Zoom Out Zoom to Selection Deselect 1 millisecond per column

Format Show 20 Per Page View List

	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

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