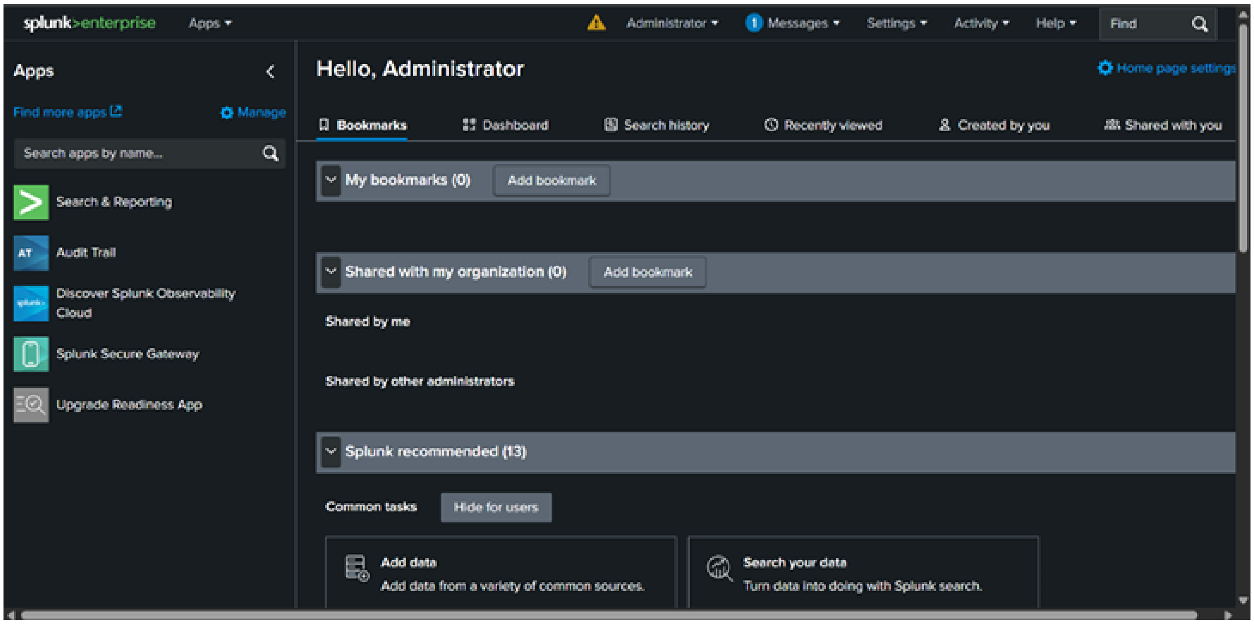
System Details:



Hello, Administrator

My bookmarks (0)

Shared with my organization (0)

Shared by me

Shared by other administrators

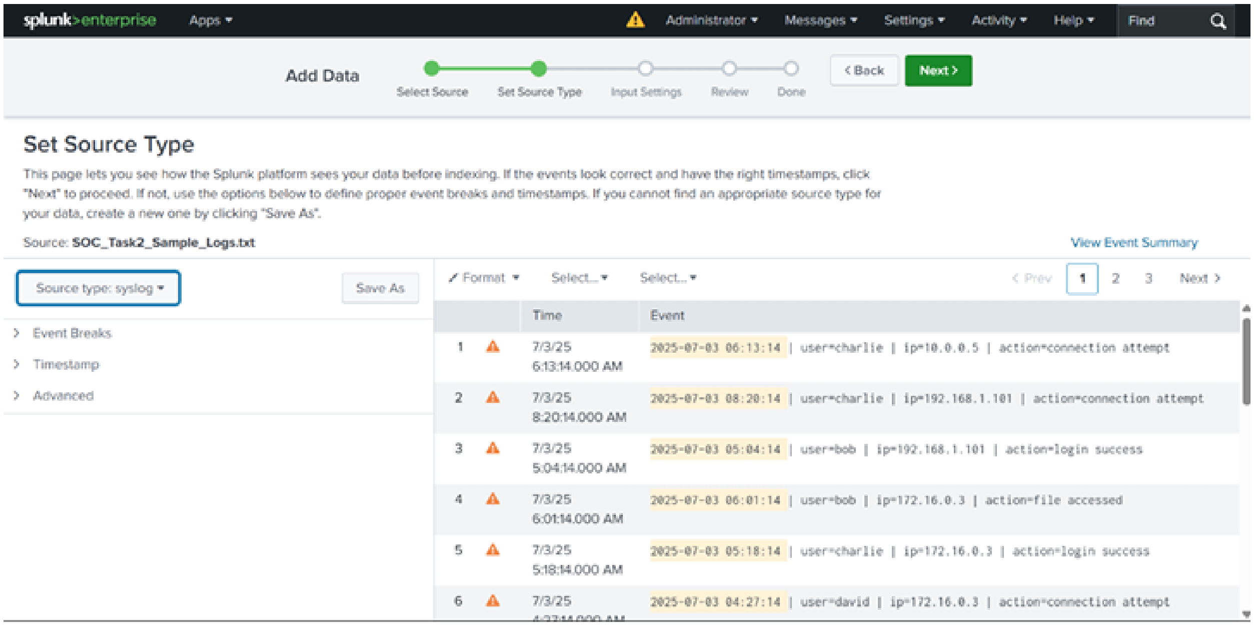
Splunk recommended (13)

Common tasks

Add data
Add data from a variety of common sources.

Search your data
Turn data into doing with Splunk search.

Uploading Log Files:



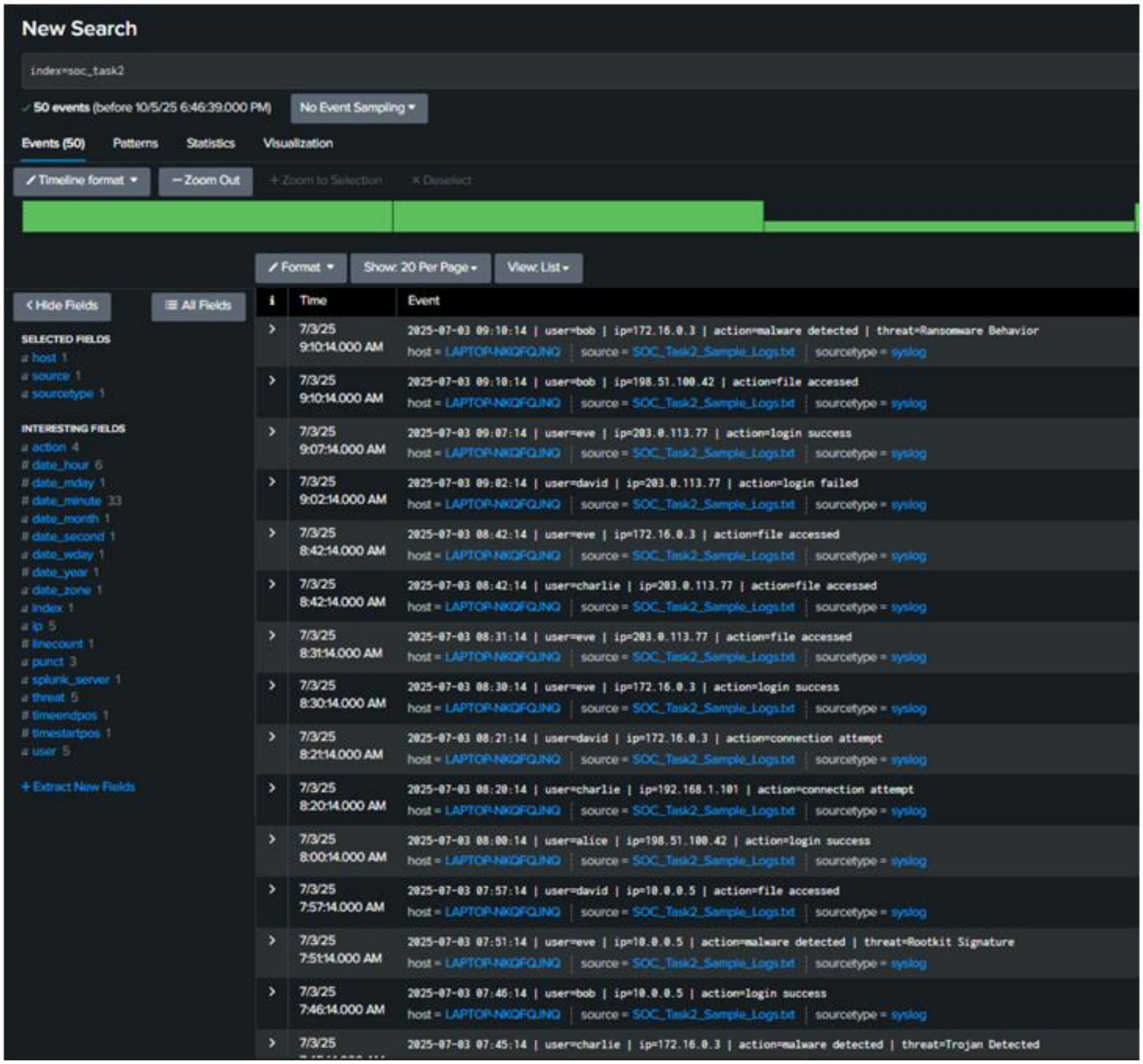
Set Source Type

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**

		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
2	⚠	7/3/25 8:20:14.000 AM	2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
3	⚠	7/3/25 5:04:14.000 AM	2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success
4	⚠	7/3/25 6:01:14.000 AM	2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed
5	⚠	7/3/25 5:18:14.000 AM	2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success
6	⚠	7/3/25 4:27:14.000 AM	2025-07-03 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt

Initial Broad Search:



```
index=soc_task2
```

✓ 50 events (before 10/5/25 6:46:39.000 PM)

SELECTED FIELDS

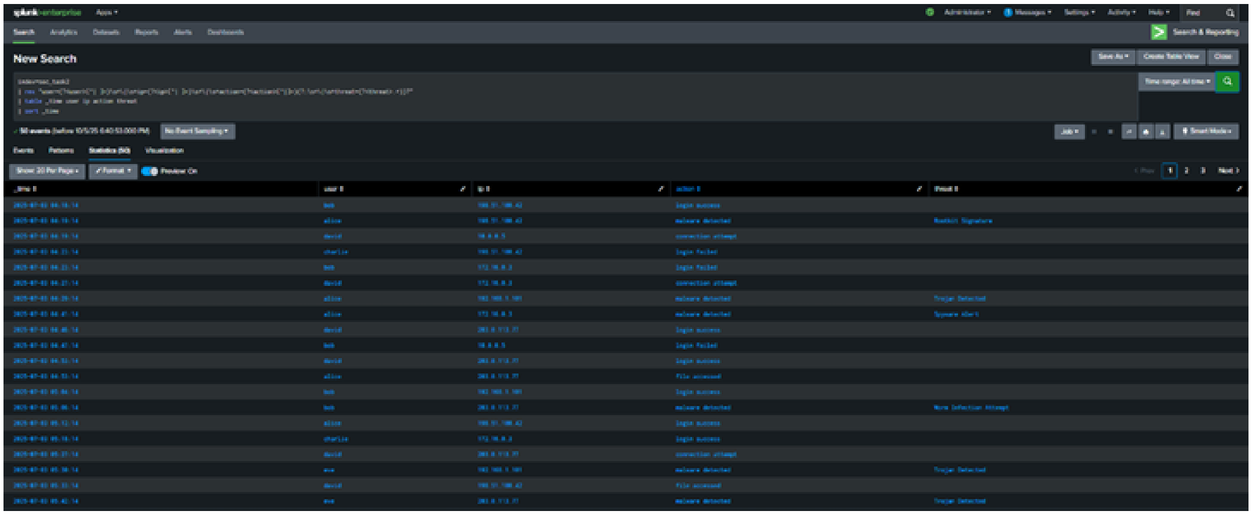
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a action 4
- # date_hour 6
- # date_mday 1
- # date_minute 33
- a date_month 1
- # date_second 1
- a date_wday 1
- # date_year 1
- a date_zone 1
- a index 1
- a ip 5
- # linecount 1
- a punct 3
- a splunk_server 1
- a threat 5
- # timeendpos 1
- # timestartpos 1
- a user 5

```
i  Time                Event
>  7/3/25              2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
   9:10:14.000 AM      host = LAPTOP-NKQFQJNQ | source = SOC_Task2_Sample_Logs.txt | sourcetype = syslog
>  7/3/25              2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
   9:10:14.000 AM      host = LAPTOP-NKQFQJNQ | source = SOC_Task2_Sample_Logs.txt | sourcetype = syslog
>  7/3/25              2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success
   9:07:14.000 AM      host = LAPTOP-NKQFQJNQ | source = SOC_Task2_Sample_Logs.txt | sourcetype = syslog
>  7/3/25              2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
   9:02:14.000 AM      host = LAPTOP-NKQFQJNQ | source = SOC_Task2_Sample_Logs.txt | sourcetype = syslog
>  7/3/25              2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed
   8:42:14.000 AM      host = LAPTOP-NKQFQJNQ | source = SOC_Task2_Sample_Logs.txt | sourcetype = syslog
>  7/3/25              2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed
   8:42:14.000 AM      host = LAPTOP-NKQFQJNQ | source = SOC_Task2_Sample_Logs.txt | sourcetype = syslog
>  7/3/25              2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed
   8:31:14.000 AM      host = LAPTOP-NKQFQJNQ | source = SOC_Task2_Sample_Logs.txt | sourcetype = syslog
>  7/3/25              2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success
   8:30:14.000 AM      host = LAPTOP-NKQFQJNQ | source = SOC_Task2_Sample_Logs.txt | sourcetype = syslog
>  7/3/25              2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt
   8:21:14.000 AM      host = LAPTOP-NKQFQJNQ | source = SOC_Task2_Sample_Logs.txt | sourcetype = syslog
>  7/3/25              2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
   8:20:14.000 AM      host = LAPTOP-NKQFQJNQ | source = SOC_Task2_Sample_Logs.txt | sourcetype = syslog
>  7/3/25              2025-07-03 08:00:14 | user=alice | ip=198.51.100.42 | action=login success
   8:00:14.000 AM      host = LAPTOP-NKQFQJNQ | source = SOC_Task2_Sample_Logs.txt | sourcetype = syslog
>  7/3/25              2025-07-03 07:57:14 | user=david | ip=10.0.0.5 | action=file accessed
   7:57:14.000 AM      host = LAPTOP-NKQFQJNQ | source = SOC_Task2_Sample_Logs.txt | sourcetype = syslog
>  7/3/25              2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature
   7:51:14.000 AM      host = LAPTOP-NKQFQJNQ | source = SOC_Task2_Sample_Logs.txt | sourcetype = syslog
>  7/3/25              2025-07-03 07:46:14 | user=bob | ip=10.0.0.5 | action=login success
   7:46:14.000 AM      host = LAPTOP-NKQFQJNQ | source = SOC_Task2_Sample_Logs.txt | sourcetype = syslog
>  7/3/25              2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
```

Field-Based Table View:



New Search

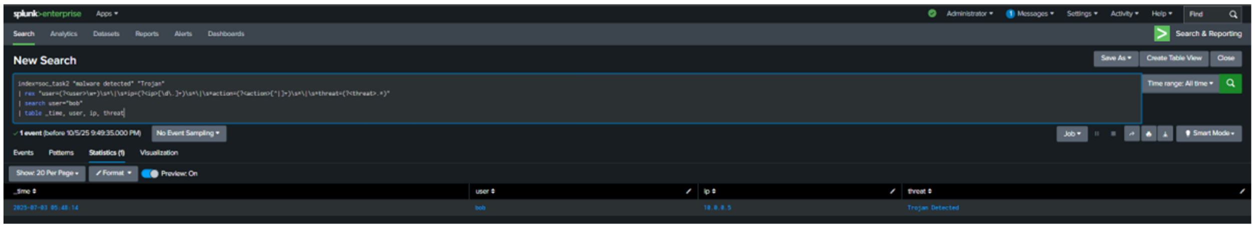
```
index=soc_task2
| rex "user=(?<user>[^|]+)\s*\|\s*ip=(?<ip>[^|]+)\s*\|\s*action=(?<action>[^|]+)\s*(?:\|\s*threat=(?<threat>.+))?"
| table _time user ip action threat
| sort _time
```

✓ 50 events (before 10/5/25 8:40:53.000 PM) No Event Sampling

_time	user	ip	action	threat
2025-07-03 04:10:14	bob	198.51.100.42	login success	
2025-07-03 04:15:14	alice	198.51.100.42	malware detected	Rootkit Signature
2025-07-03 04:19:14	david	10.0.0.5	connection attempt	
2025-07-03 04:23:14	charlie	198.51.100.42	login failed	
2025-07-03 04:23:14	bob	172.16.0.2	login failed	
2025-07-03 04:27:14	david	172.16.0.2	connection attempt	
2025-07-03 04:29:14	alice	192.168.1.101	malware detected	Trojan Detected
2025-07-03 04:41:14	alice	172.16.0.3	malware detected	Spyware Alert
2025-07-03 04:46:14	david	203.0.113.77	login success	
2025-07-03 04:47:14	bob	10.0.0.5	login failed	
2025-07-03 04:52:14	david	203.0.113.77	login success	
2025-07-03 04:53:14	alice	203.0.113.77	file accessed	
2025-07-03 05:04:14	bob	192.168.1.101	login success	
2025-07-03 05:06:14	bob	203.0.113.77	malware detected	Worm Infection Attempt
2025-07-03 05:12:14	alice	198.51.100.42	login success	
2025-07-03 05:16:14	charlie	172.16.0.3	login success	
2025-07-03 05:27:14	david	203.0.113.77	connection attempt	
2025-07-03 05:30:14	eve	192.168.1.101	malware detected	Trojan Detected
2025-07-03 05:33:14	david	198.51.100.42	file accessed	
2025-07-03 05:42:14	eve	203.0.113.77	malware detected	Trojan Detected

Incident Classification:

Incident 1 – Trojan Detected on Bob's System:



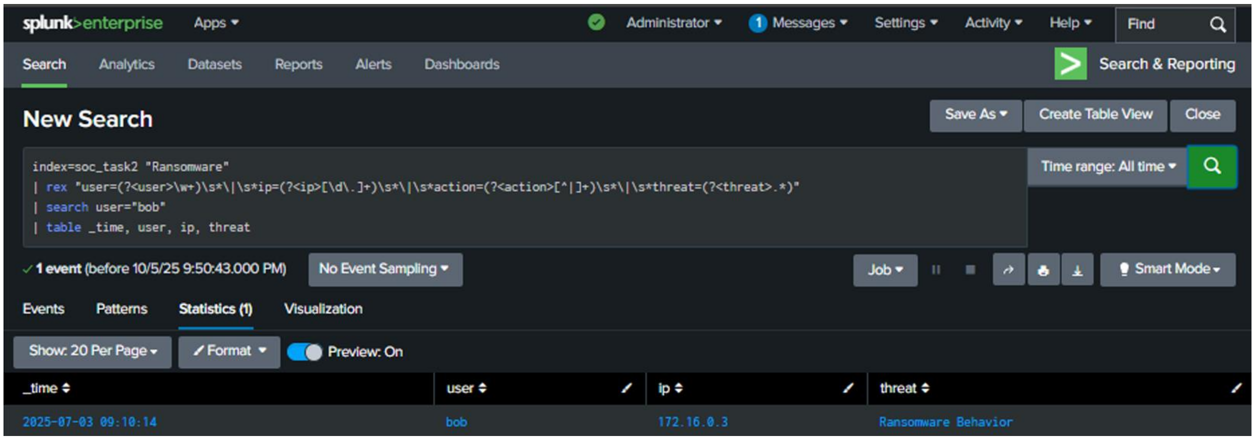
New Search

```
index=soc_task2 "malware detected" "Trojan"
| rex "user=(?<user>\w+)\s*\|\s*ip=(?<ip>[\d\.]+)\s*\|\s*action=(?<action>[^|]+)\s*\|\s*threat=(?<threat>.*)"
| search user="bob"
| table _time, user, ip, threat
```

✓ 1 event (before 10/5/25 9:49:35.000 PM) No Event Sampling

_time	user	ip	threat
2025-07-03 05:48:14	bob	10.0.0.5	Trojan Detected

Incident 2 – Ransomware Behavior (Bob):



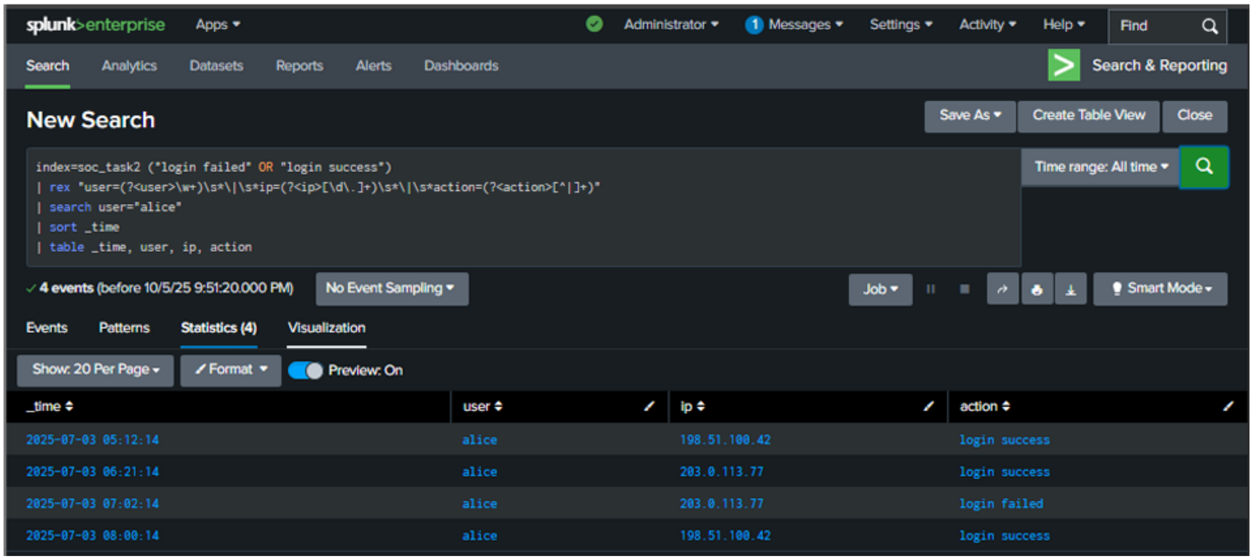
New Search

```
index=soc_task2 "Ransomware"
| rex "user=(?<user>\w+)\s*\|\s*ip=(?<ip>[\d\.]+)\s*\|\s*action=(?<action>[^|]+)\s*\|\s*threat=(?<threat>.*)"
| search user="bob"
| table _time, user, ip, threat
```

✓ 1 event (before 10/5/25 9:50:43.000 PM) No Event Sampling

_time	user	ip	threat
2025-07-03 09:10:14	bob	172.16.0.3	Ransomware Behavior

Incident 3 – Failed → Success Login (Alice):



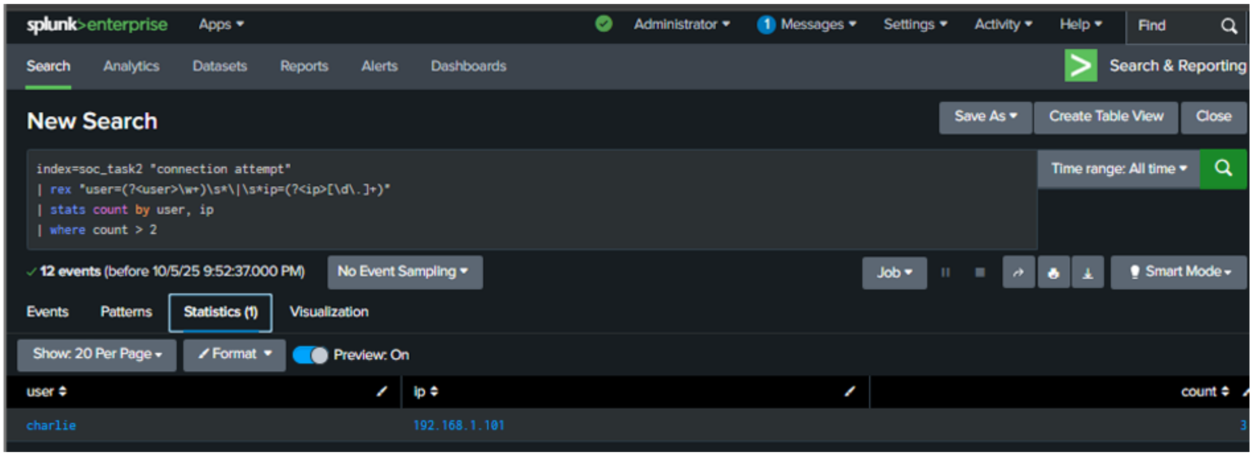
New Search

```
index=soc_task2 ("login failed" OR "login success")
| rex "user=(?<user>\w+)\s*\|\s*ip=(?<ip>[\d\.]+)\s*\|\s*action=(?<action>[^|]+)"
| search user="alice"
| sort _time
| table _time, user, ip, action
```

✓ 4 events (before 10/5/25 9:51:20.000 PM)

_time	user	ip	action
2025-07-03 05:12:14	alice	198.51.100.42	login success
2025-07-03 06:21:14	alice	203.0.113.77	login success
2025-07-03 07:02:14	alice	203.0.113.77	login failed
2025-07-03 08:00:14	alice	198.51.100.42	login success

Incident 4 – Repeated Connection Attempts (Charlie):



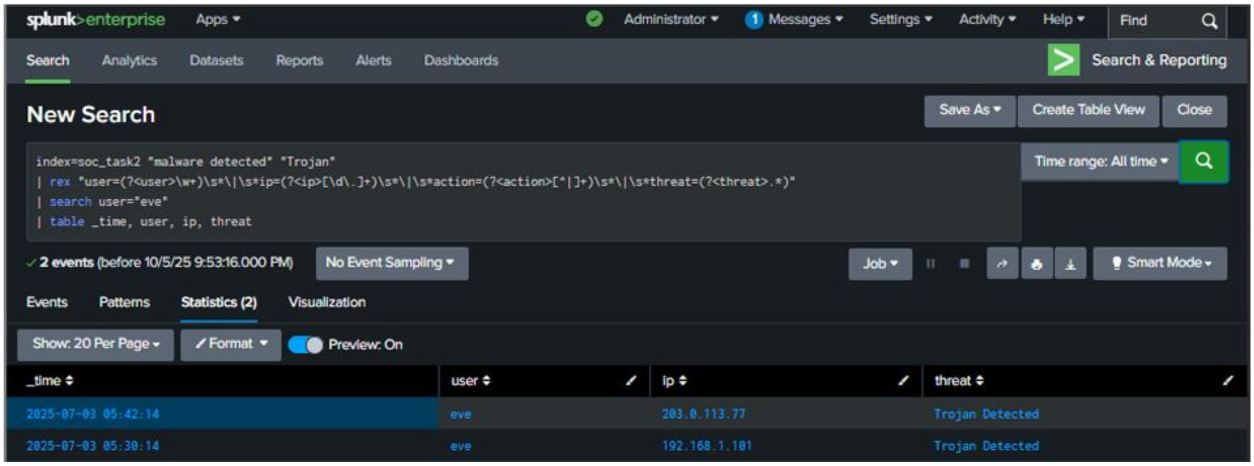
New Search

```
index=soc_task2 "connection attempt"
| rex "user=(?<user>\w+)\s*\|\s*ip=(?<ip>[\d\.]+)"
| stats count by user, ip
| where count > 2
```

✓ 12 events (before 10/5/25 9:52:37.000 PM)

user	ip	count
charlie	192.168.1.101	3

Incident 5 – Trojan Detected (Eve's System):



New Search

```
index=soc_task2 "malware detected" "Trojan"
| rex "user=(?<user>\w+)\s*\|\s*ip=(?<ip>[\d\.]+)\s*\|\s*action=(?<action>[^|]+)\s*\|\s*threat=(?<threat>.*)"
| search user="eve"
| table _time, user, ip, threat
```

✓ 2 events (before 10/5/25 9:53:16.000 PM)

_time	user	ip	threat
2025-07-03 05:42:14	eve	203.0.113.77	Trojan Detected
2025-07-03 05:30:14	eve	192.168.1.101	Trojan Detected