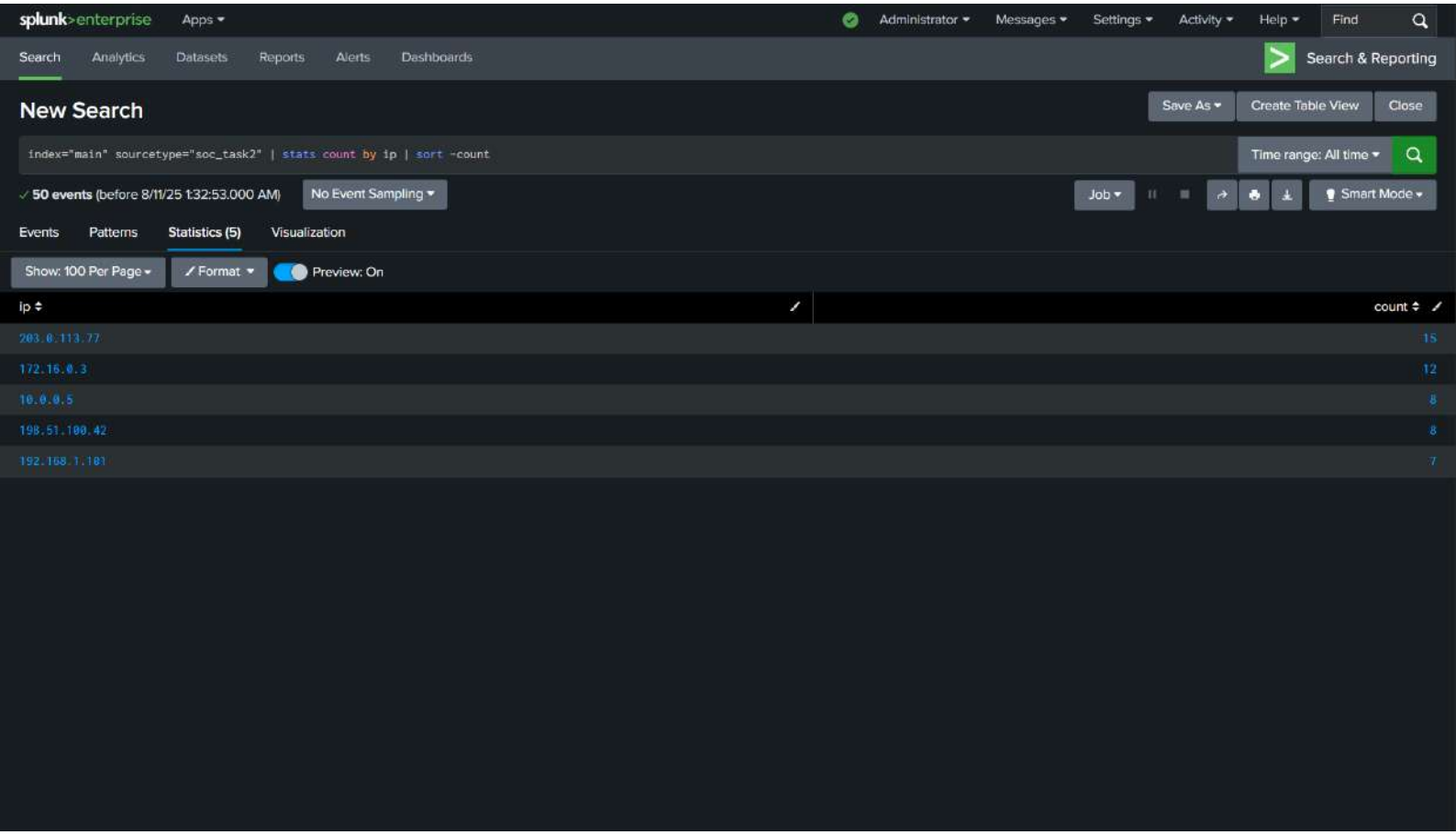
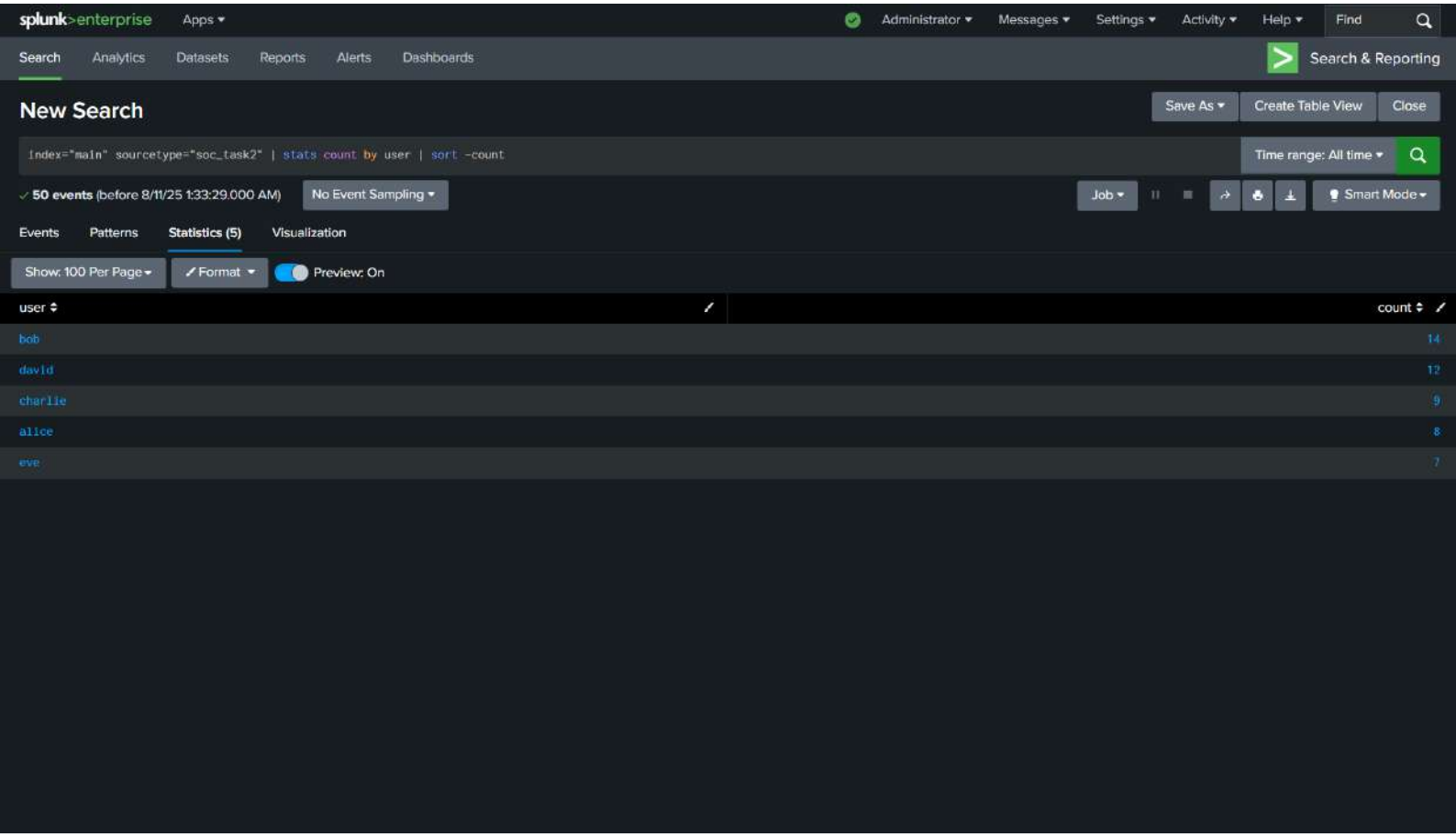
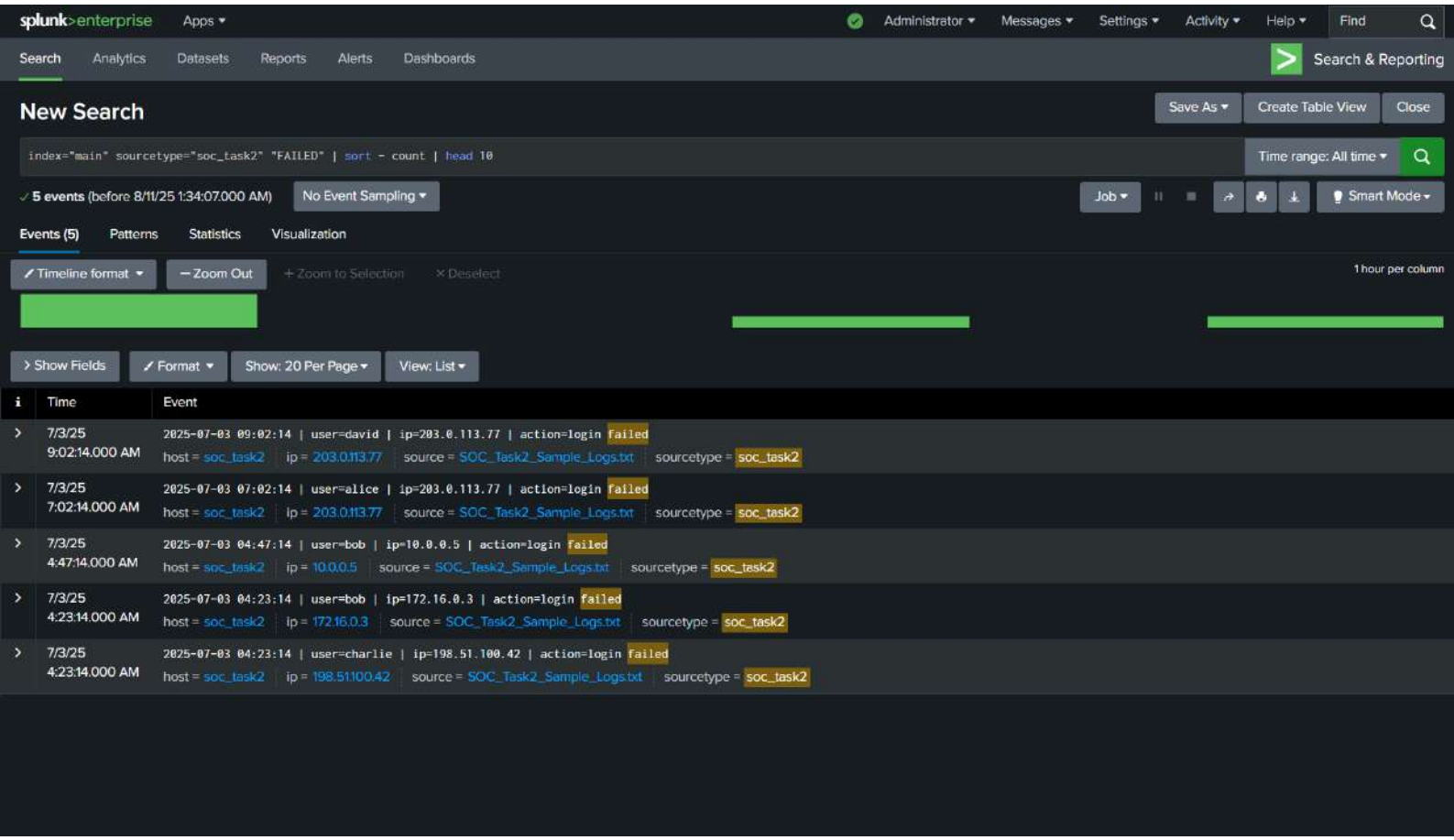
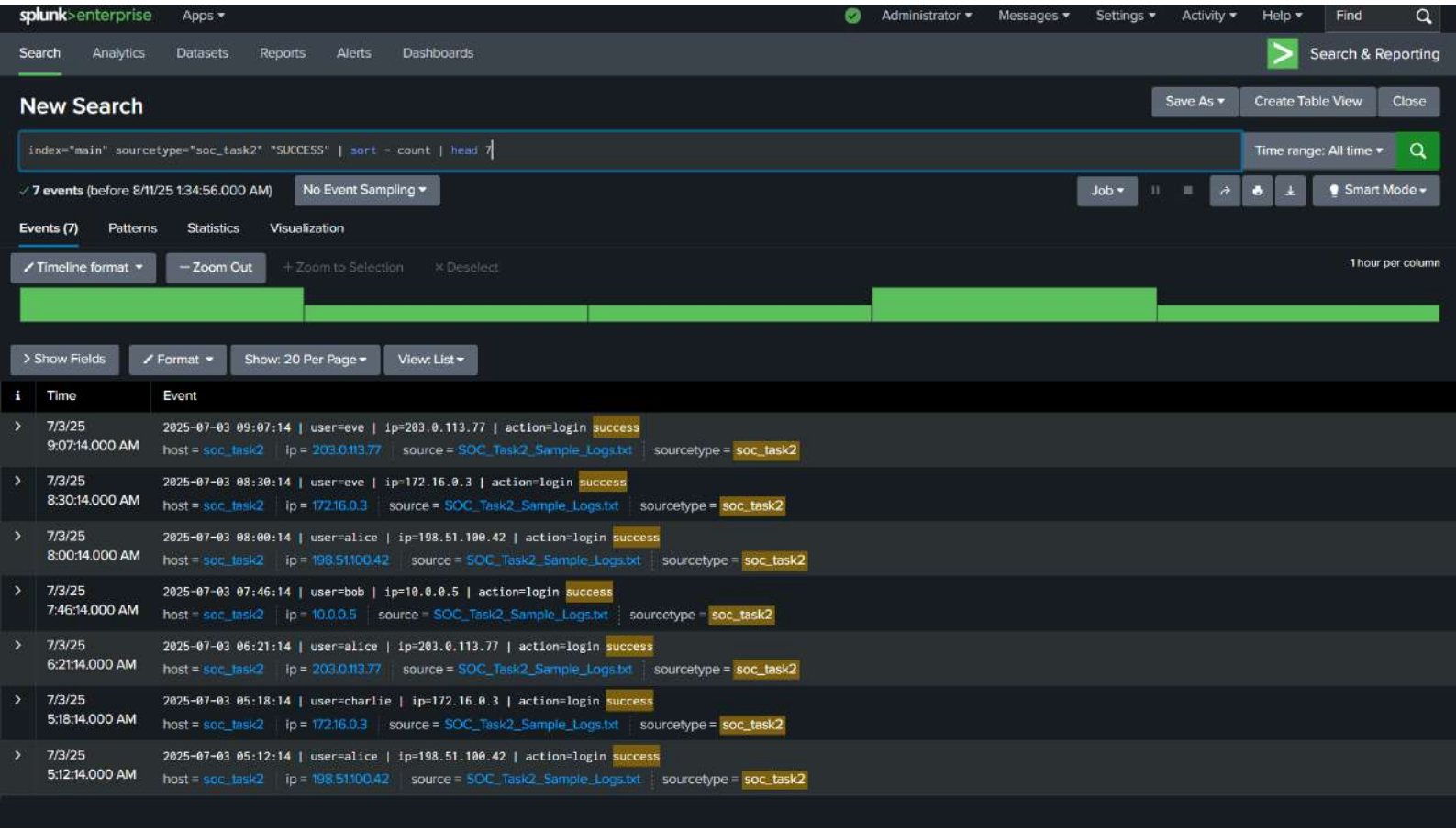
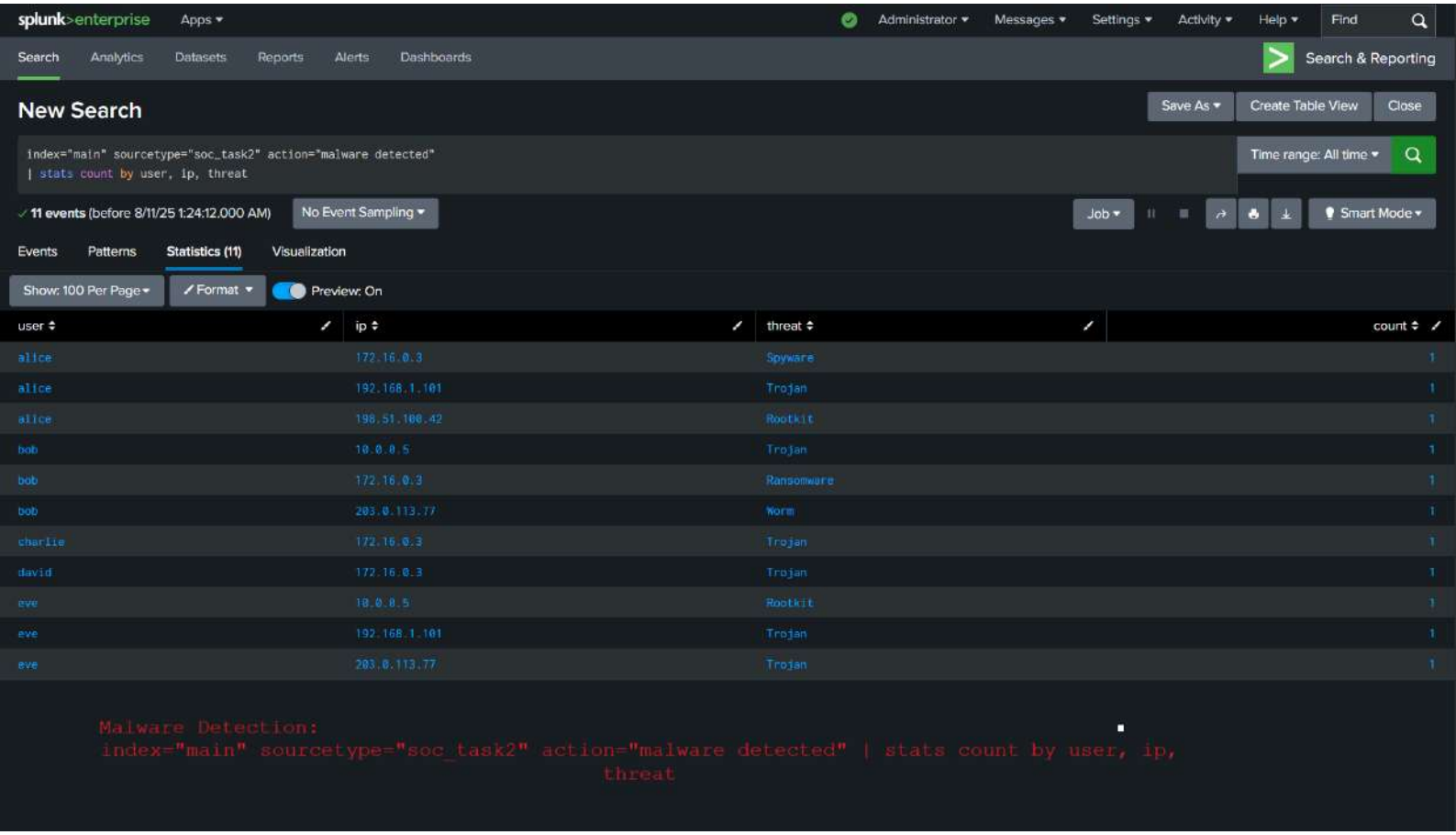

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index="main" sourcetype="soc_task2" | stats count by ip | sort -count
Time range: All time
50 events (before 8/11/25 1:32:53.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (5)
Visualization
Show: 100 Per Page
Format
Preview: On
ip
count
203.0.113.77 15
172.16.0.3 12
10.0.0.5 8
198.51.100.42 8
192.168.1.101 7


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="main" sourcetype="soc_task2" | stats count by user | sort -count
Time range: All time
50 events (before 8/11/25 1:33:29.000 AM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (5)
Visualization
Show: 100 Per Page
Format
Preview: On
user
count
bob 14
david 12
charlie 9
alice 8
eve 7


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="main" sourcetype="soc_task2" "FAILED" | sort - count | head 10
Time range: All time
5 events (before 8/11/25 1:34:07.000 AM)
No Event Sampling
Job
Smart Mode
Events (5)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Show Fields
Format
Show: 20 Per Page
View: List
Time
Event
7/3/25 9:02:14.000 AM
2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
host = soc_task2 | ip = 203.0.113.77 | source = SOC_Task2_Sample_Logs.txt | sourcetype = soc_task2
7/3/25 7:02:14.000 AM
2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed
host = soc_task2 | ip = 203.0.113.77 | source = SOC_Task2_Sample_Logs.txt | sourcetype = soc_task2
7/3/25 4:47:14.000 AM
2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed
host = soc_task2 | ip = 10.0.0.5 | source = SOC_Task2_Sample_Logs.txt | sourcetype = soc_task2
7/3/25 4:23:14.000 AM
2025-07-03 04:23:14 | user=bob | ip=172.16.0.3 | action=login failed
host = soc_task2 | ip = 172.16.0.3 | source = SOC_Task2_Sample_Logs.txt | sourcetype = soc_task2
7/3/25 4:23:14.000 AM
2025-07-03 04:23:14 | user=charlie | ip=198.51.100.42 | action=login failed
host = soc_task2 | ip = 198.51.100.42 | source = SOC_Task2_Sample_Logs.txt | sourcetype = soc_task2


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="main" sourcetype="soc_task2" "SUCCESS" | sort - count | head 7
Time range: All time
7 events (before 8/11/25 1:34:56.000 AM)
No Event Sampling
Job
Smart Mode
Events (7)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Show Fields
Format
Show: 20 Per Page
View: List
Time
Event
7/3/25 9:07:14.000 AM
2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success
host = soc_task2 | ip = 203.0.113.77 | source = SOC_Task2_Sample_Logs.txt | sourcetype = soc_task2
7/3/25 8:30:14.000 AM
2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success
host = soc_task2 | ip = 172.16.0.3 | source = SOC_Task2_Sample_Logs.txt | sourcetype = soc_task2
7/3/25 8:00:14.000 AM
2025-07-03 08:00:14 | user=alice | ip=198.51.100.42 | action=login success
host = soc_task2 | ip = 198.51.100.42 | source = SOC_Task2_Sample_Logs.txt | sourcetype = soc_task2
7/3/25 7:46:14.000 AM
2025-07-03 07:46:14 | user=bob | ip=10.0.0.5 | action=login success
host = soc_task2 | ip = 10.0.0.5 | source = SOC_Task2_Sample_Logs.txt | sourcetype = soc_task2
7/3/25 6:21:14.000 AM
2025-07-03 06:21:14 | user=alice | ip=203.0.113.77 | action=login success
host = soc_task2 | ip = 203.0.113.77 | source = SOC_Task2_Sample_Logs.txt | sourcetype = soc_task2
7/3/25 5:18:14.000 AM
2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success
host = soc_task2 | ip = 172.16.0.3 | source = SOC_Task2_Sample_Logs.txt | sourcetype = soc_task2
7/3/25 5:12:14.000 AM
2025-07-03 05:12:14 | user=alice | ip=198.51.100.42 | action=login success
host = soc_task2 | ip = 198.51.100.42 | source = SOC_Task2_Sample_Logs.txt | sourcetype = soc_task2



Malware Detection:

```
index="main" sourcetype="soc_task2" action="malware detected" | stats count by user, ip,
threat
```