New Search

Save As ▾ Create Table View Close

```
index="main" sourcetype="soc_task2" | sort -count | stats count by user_
```

Time range: All time ▾

✓ **50 events** (before 8/10/25 11:50:38.000 PM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events Patterns **Statistics (5)** Visualization

Show: 100 Per Page ▾ Format ▾ Preview: On

user	count
alice	8
bob	14
charlie	9
david	12
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

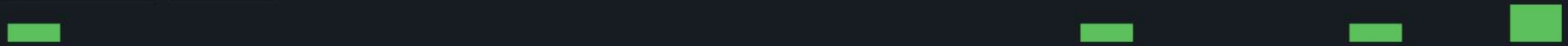
```
index="main" sourcetype="soc_task2" ip="*" | head 5 | sort - count
```

Time range: All time ▾

✓ **5 events** (before 8/11/25 12:16:40.000 AM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events (5) Patterns Statistics Visualization

Timeline format ▾ − Zoom Out + Zoom to Selection × Deselect 1 minute per column



> Show Fields Format ▾ Show: 20 Per Page ▾ View: List ▾

i	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 = soc_task2 | ip = 172.16.0.3 | source = SOC_Task2_Sample_Logs.txt | sourcetype = soc_task2
>	7/3/25 9:10:14.000 AM	2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed host = soc_task2 | ip = 198.51.100.42 | source = SOC_Task2_Sample_Logs.txt | sourcetype = soc_task2
>	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 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 8:42:14.000 AM	2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed host = soc_task2 | ip = 172.16.0.3 | 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" "failed" ip="*" | head 5 | sort - count
```

Time range: All time ▾

✓ **5 events** (before 8/11/25 12:17:53.000 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 ▾

i	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