

source="SOC\_Task2\_Sample\_Logs.txt" action=login failed

✓ 5 events (before 25/12/2025 15:07:44.000)No Event SamplingJob

Events (5)PatternsStatisticsVisualization

Timeline formatZoom OutZoom to SelectionDeselect

FormatShow: 20 Per PageView: List

<div>&lt; Hide Fields</div> <div>≡ All Fields</div> <div>SELECTED FIELDS</div> <div>a host 1</div> <div>a source 1</div> <div>a sourcetype 1</div> <div>INTERESTING FIELDS</div> <div>a action 1</div> <div># date_hour 3</div> <div># date_mday 1</div> <div># date_minute 3</div> <div>a date_month 1</div> <div># date_second 1</div> <div>a date_wday 1</div> <div># date_year 1</div> <div>a date_zone 1</div> <div>a index 1</div>	< Hide Fields		≡ All Fields		
	>	03/07/2025 09:02:14.000	2025-07-03 09:02:14	user=david   ip=203.0.113.77   action=login failed	
			host = KHUSHI-YADAV	source = SOC_Task2_Sample_Logs.txt	sourcetype = abhi
	>	03/07/2025 07:02:14.000	2025-07-03 07:02:14	user=alice   ip=203.0.113.77   action=login failed	
			host = KHUSHI-YADAV	source = SOC_Task2_Sample_Logs.txt	sourcetype = abhi
	>	03/07/2025 04:47:14.000	2025-07-03 04:47:14	user=bob   ip=10.0.0.5   action=login failed	
			host = KHUSHI-YADAV	source = SOC_Task2_Sample_Logs.txt	sourcetype = abhi
	>	03/07/2025 04:23:14.000	2025-07-03 04:23:14	user=bob   ip=172.16.0.3   action=login failed	
			host = KHUSHI-YADAV	source = SOC_Task2_Sample_Logs.txt	sourcetype = abhi
	>	03/07/2025 04:23:14.000	2025-07-03 04:23:14	user=charlie   ip=198.51.100.42   action=login failed	
			host = KHUSHI-YADAV	source = SOC_Task2_Sample_Logs.txt	sourcetype = abhi

# New Search

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

✓ 11 events (before 25/12/2025 15:20:47.000)

No Event Sampling ▾

Events

Patterns

Statistics (11)

Visualization

Show: 20 Per Page ▾

 Format ▾

 Preview: On

user ↕	ip ↕	threat ↕
alice	172.16.0.3	Spyware
alice	192.168.1.101	Trojan
alice	198.51.100.42	Rootkit
bob	10.0.0.5	Trojan
bob	172.16.0.3	Ransomware
bob	203.0.113.77	Worm
charlie	172.16.0.3	Trojan
david	172.16.0.3	Trojan
eve	10.0.0.5	Rootkit
eve	192.168.1.101	Trojan
...	203.0.113.77	Trojan

## New Search

Save As ▼ Create Table View Close

```
index=main
| stats count by ip, user
| where count <= 2
```

Time range: All time ▼





✓ 50 events (before 25/12/2025 15:24:25.000) No Event Sampling ▼

Job ▼       Smart Mode ▼

Events Patterns **Statistics (10)** Visualization

Show: 20 Per Page ▼  Format ▼  Preview: On

ip 	user 	count 
10.0.0.5	charlie	1
10.0.0.5	eve	1
172.16.0.3	alice	1
172.16.0.3	eve	2
192.168.1.101	alice	1
192.168.1.101	bob	2
192.168.1.101	eve	1
198.51.100.42	charlie	1
198.51.100.42	david	1