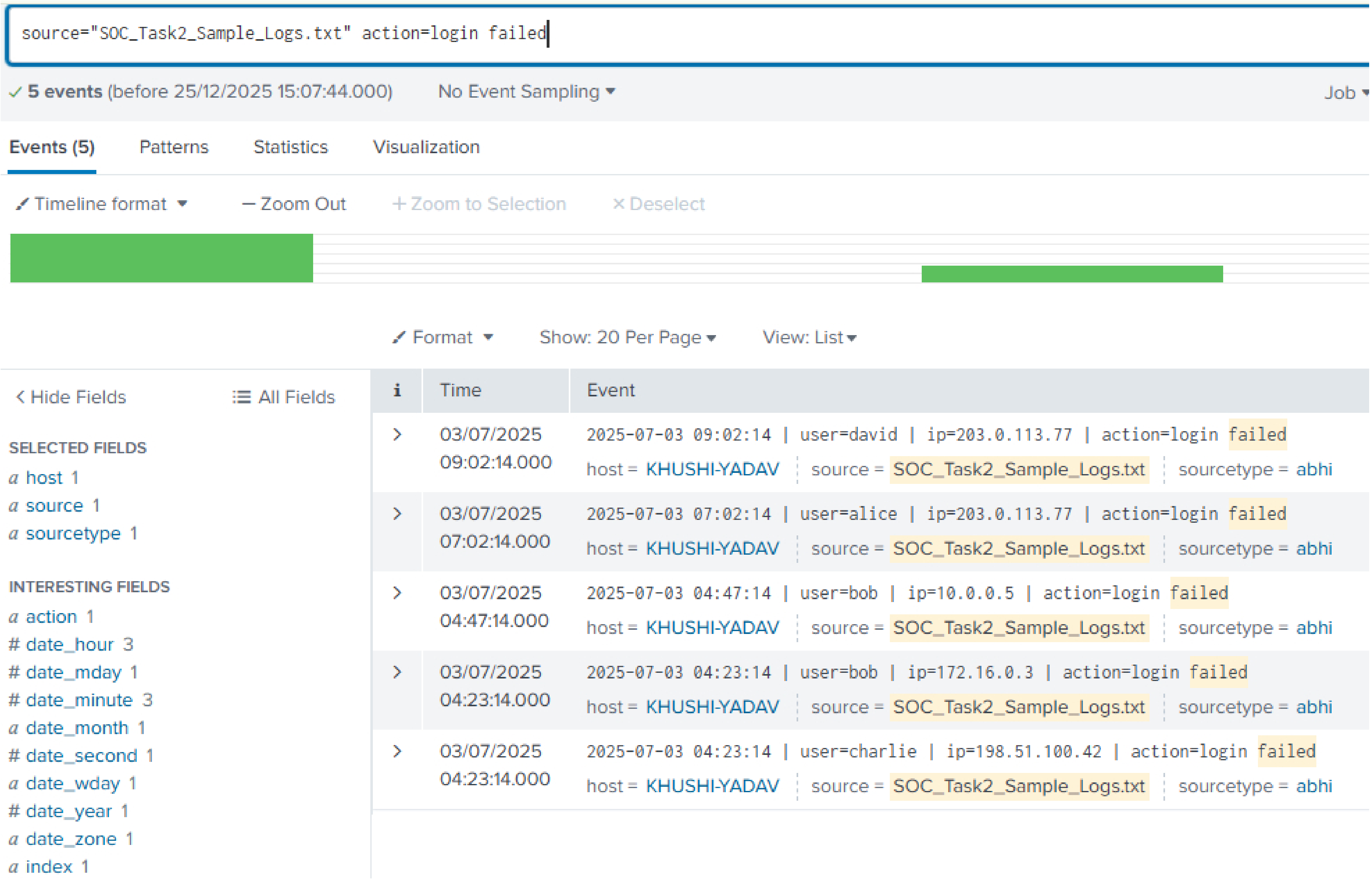


```
source="SOC_Task2_Sample_Logs.txt" action=login failed
```

✓ **5 events** (before 25/12/2025 15:07:44.000) No Event Sampling ▾ Job ▾

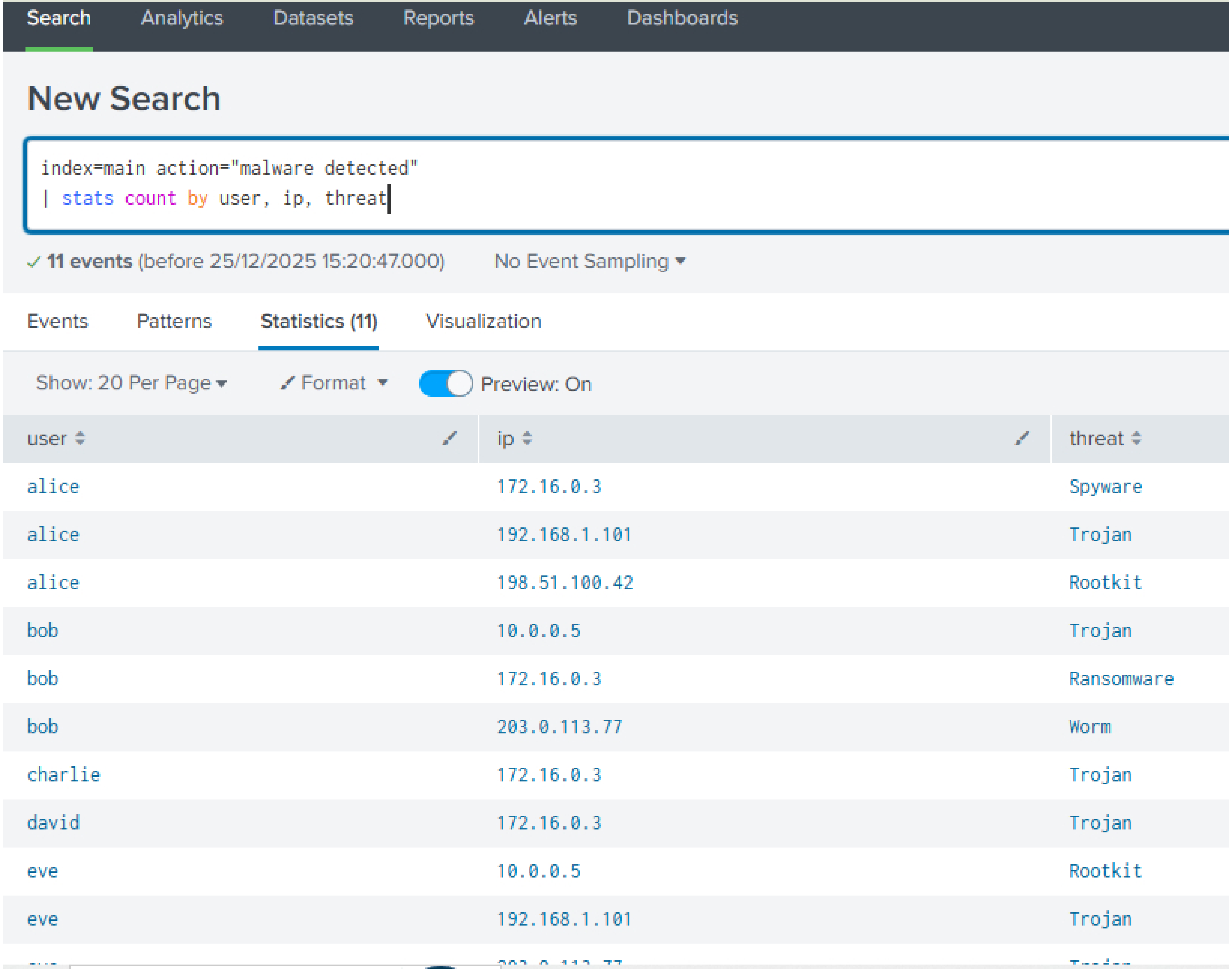
SELECTED FIELDS

a	host	1
a	source	1
a	sourcetype	1

INTERESTING FIELDS

a	action	1
#	date_hour	3
#	date_mday	1
#	date_minute	3
a	date_month	1
#	date_second	1
a	date_wday	1
#	date_year	1
a	date_zone	1
a	index	1

i	Time	Event
›	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

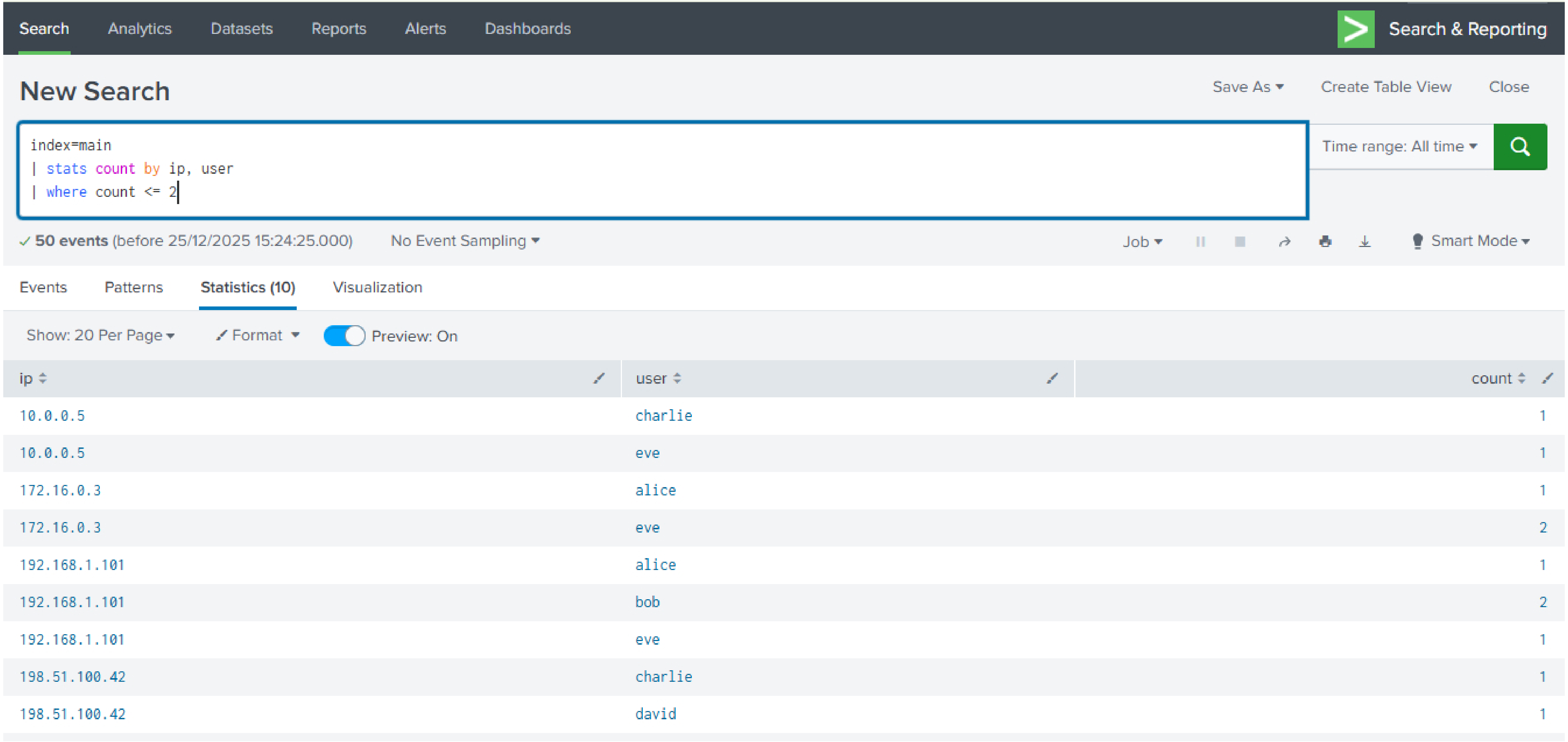


New Search

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

✓ **11 events** (before 25/12/2025 15:20:47.000) No Event Sampling ▾

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
eve	203.0.113.77	Trojan



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

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

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