SOC Task 2 – Incident Investigation Report

Internship Project | Splunk Log Analysis

Prepared by: Rishav Raj

CIN ID: FIT/AUG25/CS3104

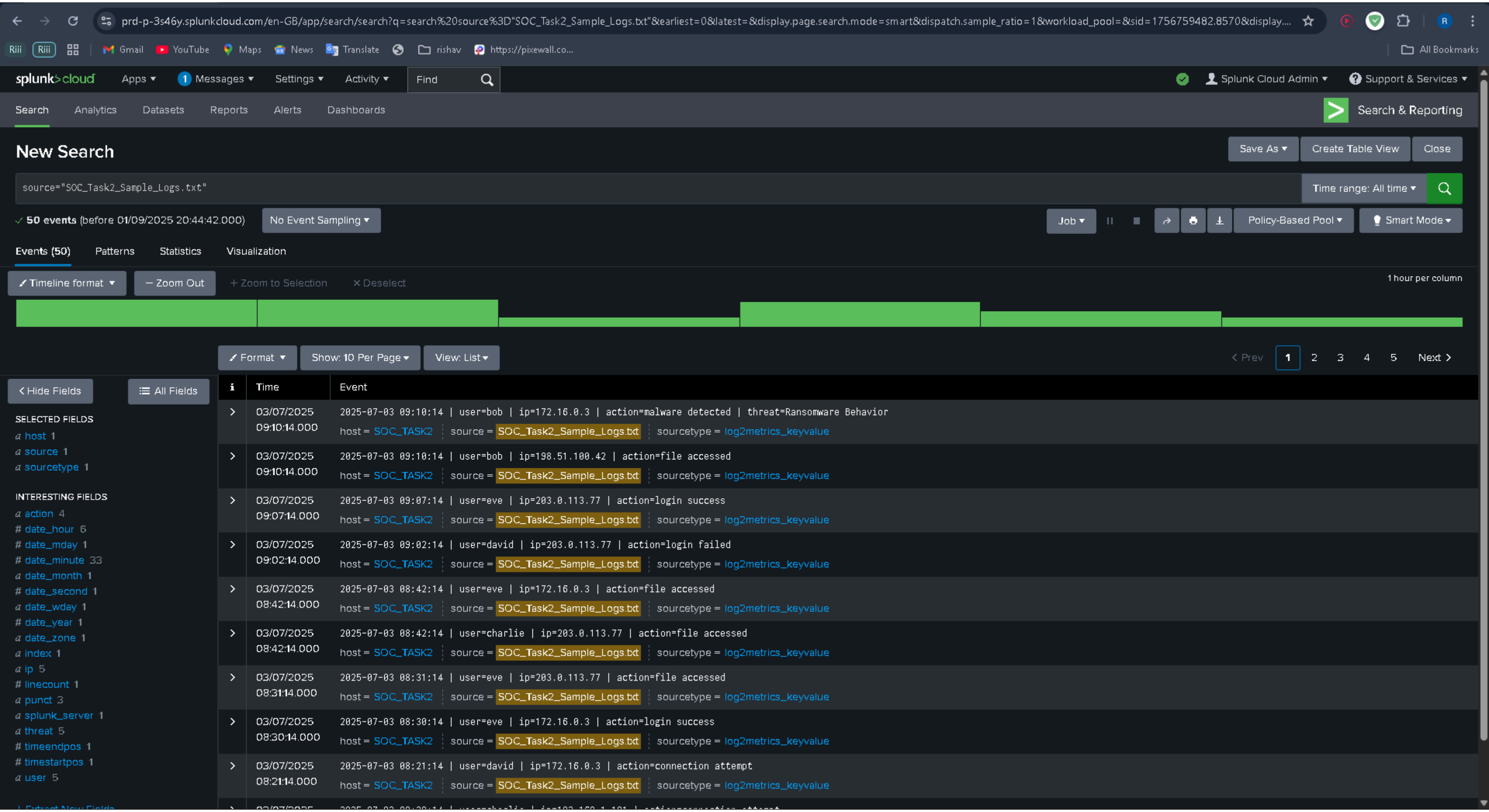
Objective

- The purpose of this task is to analyze the provided log file `**SOC_Task2_Sample_Logs.txt**` using Splunk, identify suspicious activities, and visualize them through dashboards.

All Events (Baseline Check)

- **Query:**
- **source**="**SOC_Task2_Sample_Logs.txt**"

- **Observation**:
- Alllogeventsingested successfully. Includes login, file access, connection attempts, and malware detections.



```
source="SOC_Task2_Sample_Logs.txt"
```

✓ 50 events (before 01/09/2025 20:44:42.000)

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

+ Extract New Fields

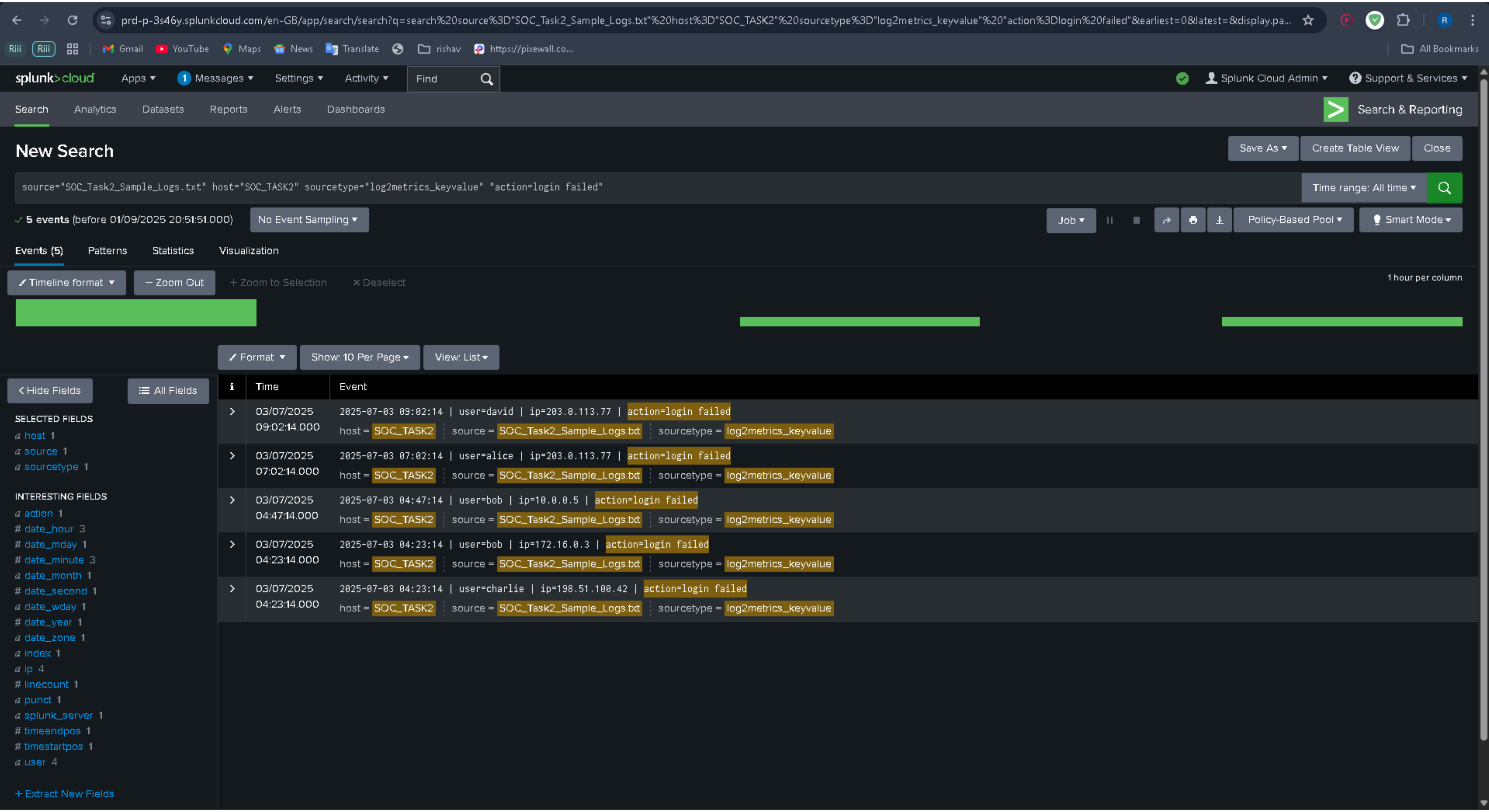
i	Time	Event
>	03/07/2025 09:10:14.000	2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior host = SOC_TASK2 ¦ source = SOC_Task2_Sample_Logs.txt ¦ sourcetype = log2metrics_keyvalue
>	03/07/2025 09:10:14.000	2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed host = SOC_TASK2 ¦ source = SOC_Task2_Sample_Logs.txt ¦ sourcetype = log2metrics_keyvalue
>	03/07/2025 09:07:14.000	2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success host = SOC_TASK2 ¦ source = SOC_Task2_Sample_Logs.txt ¦ sourcetype = log2metrics_keyvalue
>	03/07/2025 09:02:14.000	2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed host = SOC_TASK2 ¦ source = SOC_Task2_Sample_Logs.txt ¦ sourcetype = log2metrics_keyvalue
>	03/07/2025 08:42:14.000	2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed host = SOC_TASK2 ¦ source = SOC_Task2_Sample_Logs.txt ¦ sourcetype = log2metrics_keyvalue
>	03/07/2025 08:42:14.000	2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed host = SOC_TASK2 ¦ source = SOC_Task2_Sample_Logs.txt ¦ sourcetype = log2metrics_keyvalue
>	03/07/2025 08:31:14.000	2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed host = SOC_TASK2 ¦ source = SOC_Task2_Sample_Logs.txt ¦ sourcetype = log2metrics_keyvalue
>	03/07/2025 08:30:14.000	2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success host = SOC_TASK2 ¦ source = SOC_Task2_Sample_Logs.txt ¦ sourcetype = log2metrics_keyvalue
>	03/07/2025 08:21:14.000	2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt host = SOC_TASK2 ¦ source = SOC_Task2_Sample_Logs.txt ¦ sourcetype = log2metrics_keyvalue
>	03/07/2025	2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt

Failed Login Attempts

- **Query:**
- **source="SOC_Task2_Sample_Logs.txt" action="login failed"**

- **Observation**:

- Severalfailedloginattempts recorded → Possible brute force or credential-stuffing activity.



New Search

```
source="SOC_Task2_Sample_Logs.txt" host="SOC_TASK2" sourcetype="log2metrics_keyvalue" "action=login failed"
```

Time range: All time

✓ 5 events (before 01/09/2025 20:51:51.000) No Event Sampling

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 = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 07:02:14.000	2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 04:47:14.000	2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 04:23:14.000	2025-07-03 04:23:14 | user=bob | ip=172.16.0.3 | action=login failed host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 04:23:14.000	2025-07-03 04:23:14 | user=charlie | ip=198.51.100.42 | action=login failed host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue

SELECTED FIELDS

a	host	1
a	source	1
a	sourcetype	1

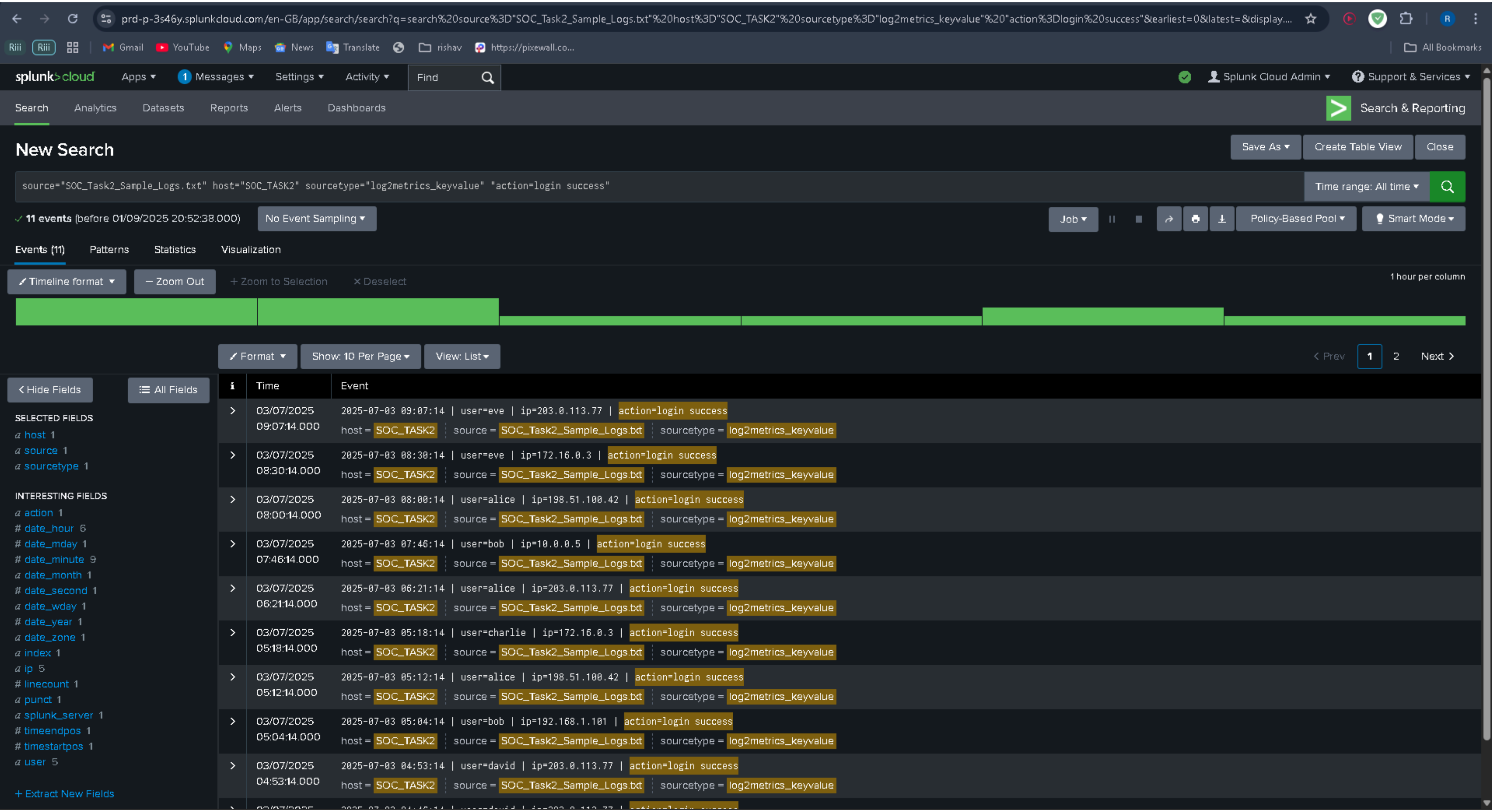
INTERESTING FIELDS

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
a	ip	4
#	linecount	1
a	punct	1
a	splunk_server	1
#	timeendpos	1
#	timestartpos	1
a	user	4

Successful Login Attempts

- **Query:**
- **source="SOC_Task2_Sample_Logs.txt" action="login success"**

- **Observation**:
- Legitimate successful login events recorded. Baseline for comparison with failed attempts.



prd-p-3s46y.splunkcloud.com/en-GB/app/search/search?q=search%20source%3D"SOC_Task2_Sample_Logs.txt"%20host%3D"SOC_TASK2"%20sourcetype%3D"log2metrics_keyvalue"%20"action%3Dlogin%20success"&earliest=0&latest=&display....

New Search

```
source="SOC_Task2_Sample_Logs.txt" host="SOC_TASK2" sourcetype="log2metrics_keyvalue" "action=login success"
```

Time range: All time ▾

✓ 11 events (before 01/09/2025 20:52:38.000)

No Event Sampling ▾

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a action 1
- # date_hour 6
- # date_mday 1
- # date_minute 9
- 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 1
- a splunk_server 1
- # timeendpos 1
- # timestartpos 1
- a user 5

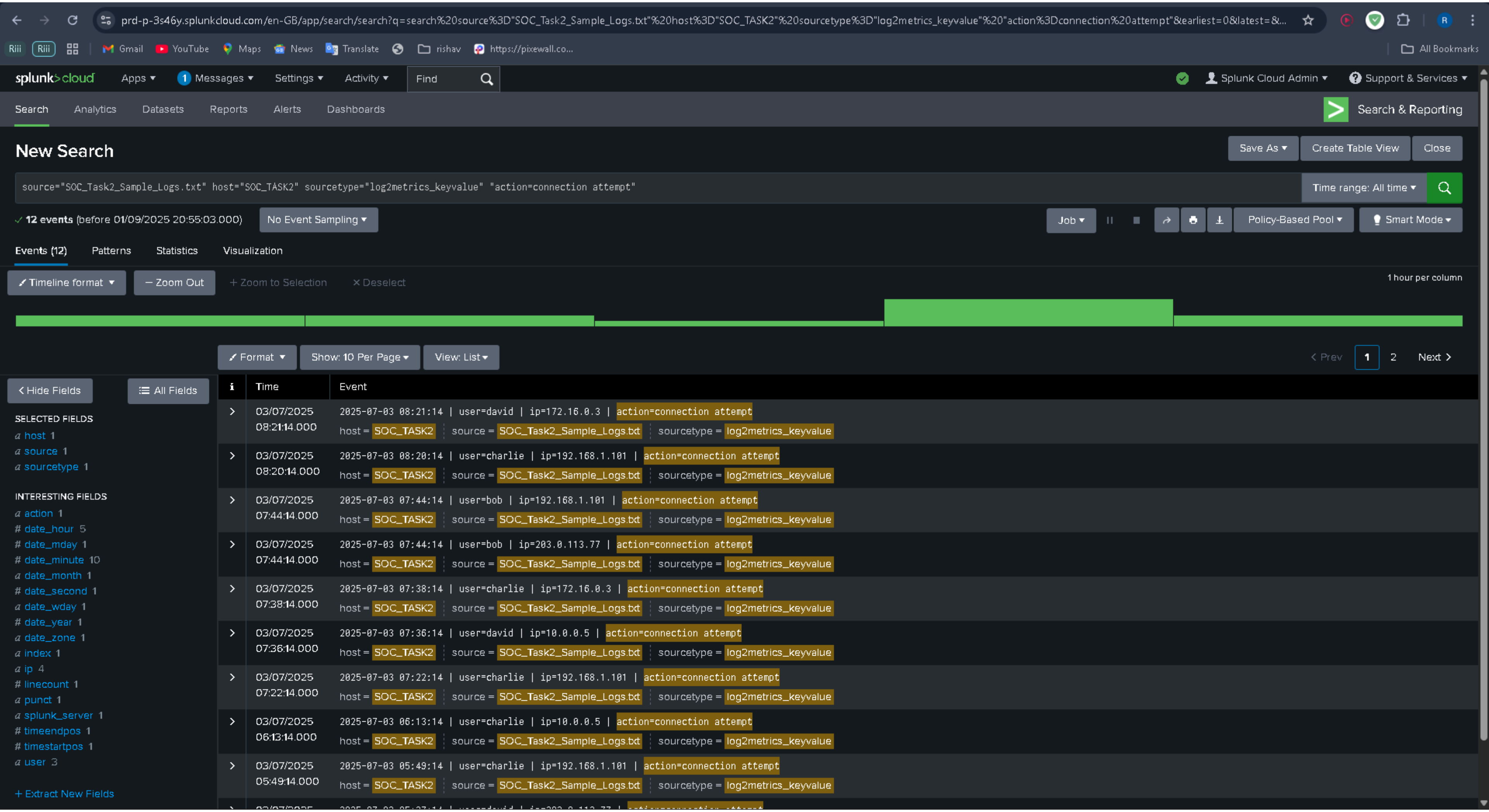
+ Extract New Fields

i	Time	Event
>	03/07/2025 09:07:14.000	2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 08:30:14.000	2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 08:00:14.000	2025-07-03 08:00:14 | user=alice | ip=198.51.100.42 | action=login success host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 07:46:14.000	2025-07-03 07:46:14 | user=bob | ip=10.0.0.5 | action=login success host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 06:21:14.000	2025-07-03 06:21:14 | user=alice | ip=203.0.113.77 | action=login success host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 05:18:14.000	2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 05:12:14.000	2025-07-03 05:12:14 | user=alice | ip=198.51.100.42 | action=login success host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 05:04:14.000	2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 04:53:14.000	2025-07-03 04:53:14 | user=david | ip=203.0.113.77 | action=login success host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue

Connection Attempts

- **Query:**
- **source=**"**SOC_Task2_Sample_Logs.txt**" **action=**"**connection attempt**"

- **Observation**:
- High number ofconnection attempts observed → Possible brute force or scanning attempts.



```
prd-p-3s46y.splunkcloud.com/en-GB/app/search/search?q=search%20source%3D"SOC_Task2_Sample_Logs.txt"%20host%3D"SOC_TASK2"%20sourcetype%3D"log2metrics_keyvalue"%20"action%3Dconnection%20attempt"&earliest=0&latest=&...
```

New Search

```
source="SOC_Task2_Sample_Logs.txt" host="SOC_TASK2" sourcetype="log2metrics_keyvalue" "action=connection attempt"
```

Time range: All time

✓ 12 events (before 01/09/2025 20:55:03.000)   No Event Sampling

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a action 1
- # date_hour 5
- # date_mday 1
- # date_minute 10
- a date_month 1
- # date_second 1
- a date_wday 1
- # date_year 1
- a date_zone 1
- a index 1
- a ip 4
- # linecount 1
- a punct 1
- a splunk_server 1
- # timeendpos 1
- # timestartpos 1
- a user 3

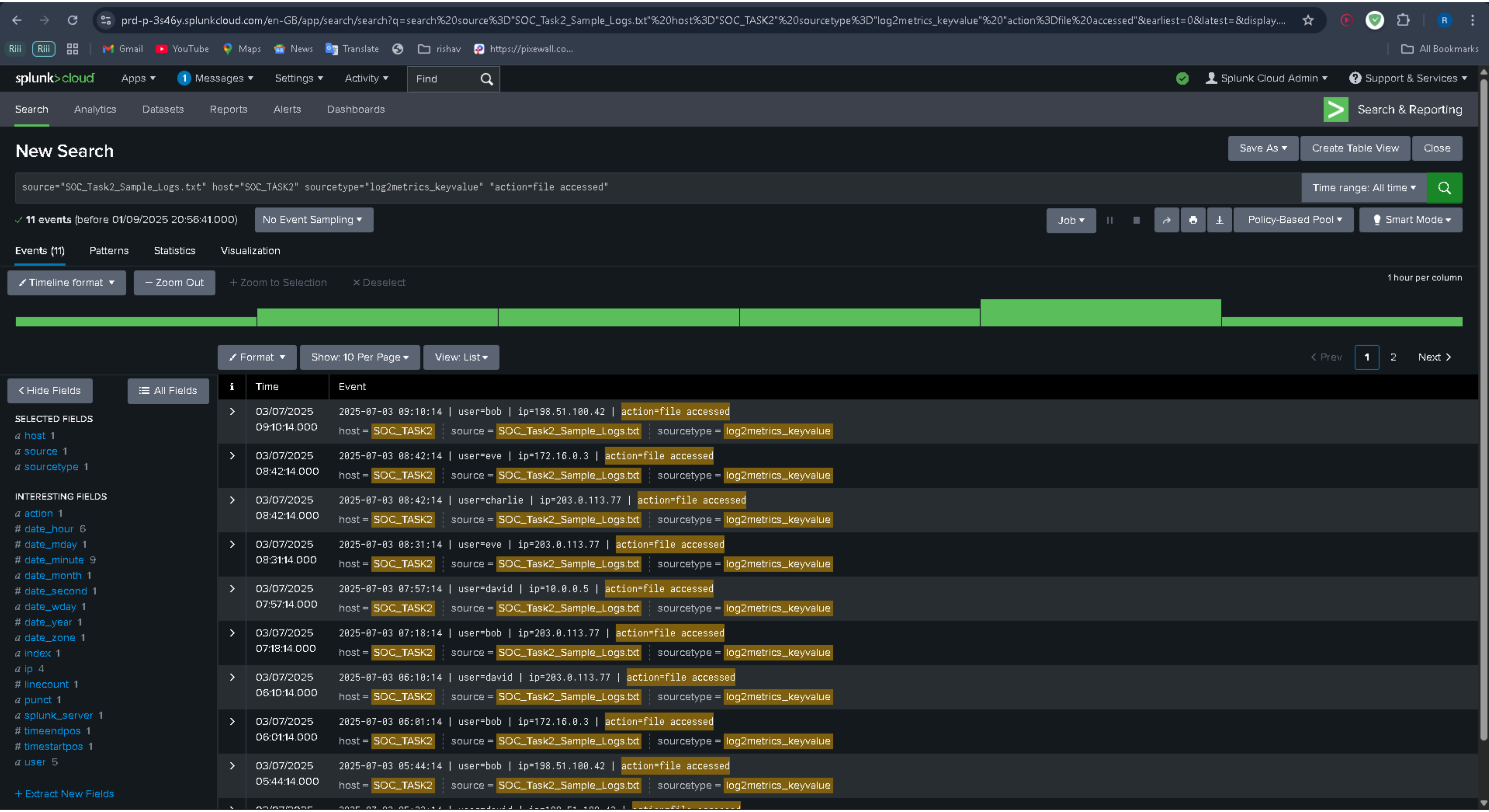
i	Time	Event
>	03/07/2025 08:21:14.000	2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt host = SOC_TASK2 ¦ source = SOC_Task2_Sample_Logs.txt ¦ sourcetype = log2metrics_keyvalue
>	03/07/2025 08:20:14.000	2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt host = SOC_TASK2 ¦ source = SOC_Task2_Sample_Logs.txt ¦ sourcetype = log2metrics_keyvalue
>	03/07/2025 07:44:14.000	2025-07-03 07:44:14 | user=bob | ip=192.168.1.101 | action=connection attempt host = SOC_TASK2 ¦ source = SOC_Task2_Sample_Logs.txt ¦ sourcetype = log2metrics_keyvalue
>	03/07/2025 07:44:14.000	2025-07-03 07:44:14 | user=bob | ip=203.0.113.77 | action=connection attempt host = SOC_TASK2 ¦ source = SOC_Task2_Sample_Logs.txt ¦ sourcetype = log2metrics_keyvalue
>	03/07/2025 07:38:14.000	2025-07-03 07:38:14 | user=charlie | ip=172.16.0.3 | action=connection attempt host = SOC_TASK2 ¦ source = SOC_Task2_Sample_Logs.txt ¦ sourcetype = log2metrics_keyvalue
>	03/07/2025 07:36:14.000	2025-07-03 07:36:14 | user=david | ip=10.0.0.5 | action=connection attempt host = SOC_TASK2 ¦ source = SOC_Task2_Sample_Logs.txt ¦ sourcetype = log2metrics_keyvalue
>	03/07/2025 07:22:14.000	2025-07-03 07:22:14 | user=charlie | ip=192.168.1.101 | action=connection attempt host = SOC_TASK2 ¦ source = SOC_Task2_Sample_Logs.txt ¦ sourcetype = log2metrics_keyvalue
>	03/07/2025 06:13:14.000	2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt host = SOC_TASK2 ¦ source = SOC_Task2_Sample_Logs.txt ¦ sourcetype = log2metrics_keyvalue
>	03/07/2025 05:49:14.000	2025-07-03 05:49:14 | user=charlie | ip=192.168.1.101 | action=connection attempt host = SOC_TASK2 ¦ source = SOC_Task2_Sample_Logs.txt ¦ sourcetype = log2metrics_keyvalue
>	03/07/2025	2025-07-03 05:37:14 | user=david | ip=203.0.113.77 | action=connection attempt

File Accessed Events

- **Query:**
- **source=**"**SOC_Task2_Sample_Logs.txt**" **action=**"**file accessed**"

- **Observation**:

- Filesaccessedbymultiple users. Needs correlation with login attempts for insider activity.



New Search

```
source="SOC_Task2_Sample_Logs.txt" host="SOC_TASK2" sourcetype="log2metrics_keyvalue" "action=file accessed"
```

Time range: All time

✓ 11 events (before 01/09/2025 20:56:41.000) No Event Sampling

SELECTED FIELDS

a host	1
a source	1
a sourcetype	1

INTERESTING FIELDS

a action	1
# date_hour	6
# date_mday	1
# date_minute	9
a date_month	1
# date_second	1
a date_wday	1
# date_year	1
a date_zone	1
a index	1
a ip	4
# linecount	1
a punct	1
a splunk_server	1
# timeendpos	1
# timestartpos	1
a user	5

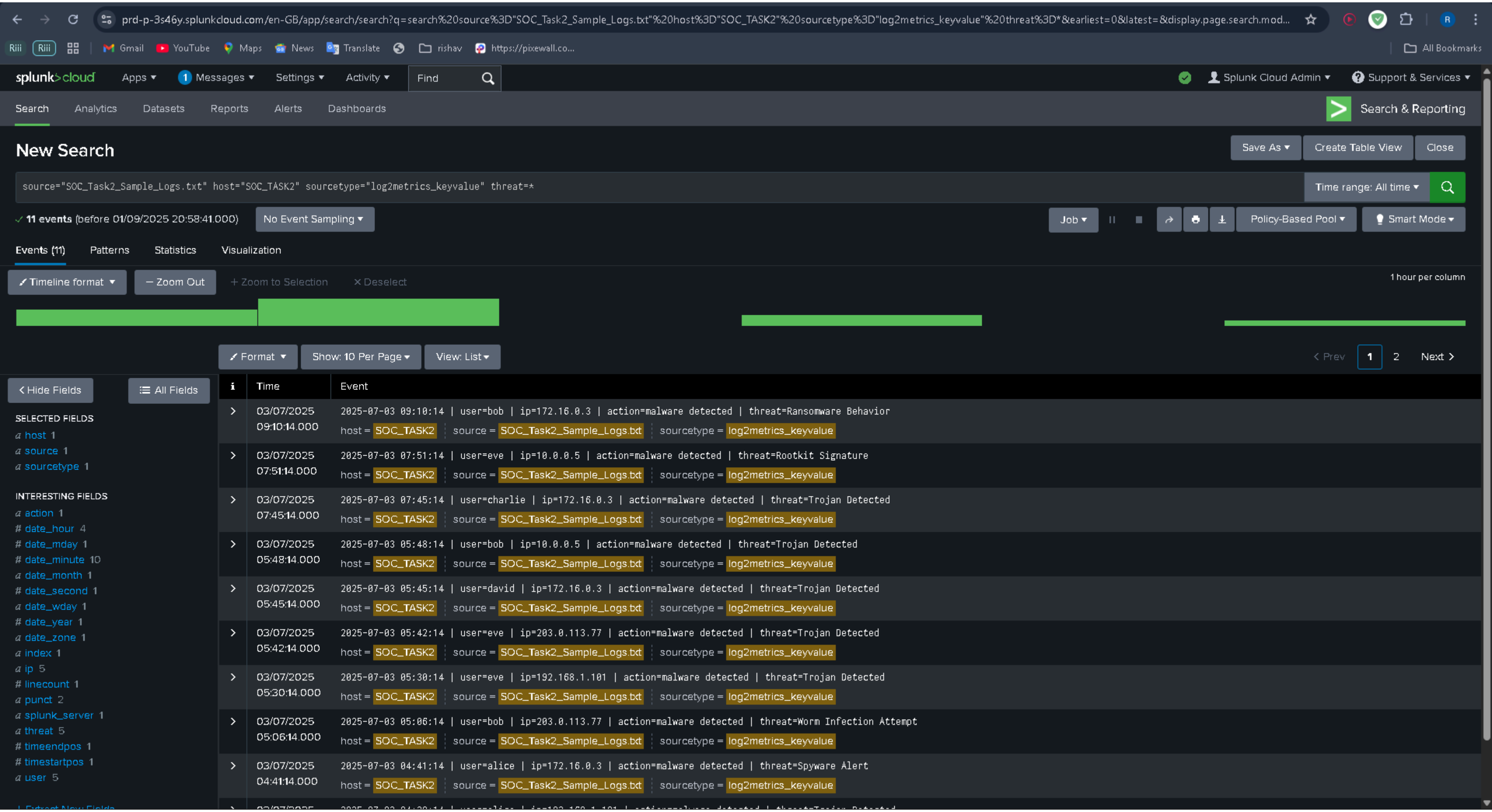
i	Time	Event
>	03/07/2025 09:10:14.000	2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 08:42:14.000	2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 08:42:14.000	2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 08:31:14.000	2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 07:57:14.000	2025-07-03 07:57:14 | user=david | ip=10.0.0.5 | action=file accessed host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 07:18:14.000	2025-07-03 07:18:14 | user=bob | ip=203.0.113.77 | action=file accessed host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 06:10:14.000	2025-07-03 06:10:14 | user=david | ip=203.0.113.77 | action=file accessed host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 06:01:14.000	2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	03/07/2025 05:44:14.000	2025-07-03 05:44:14 | user=bob | ip=198.51.100.42 | action=file accessed host = SOC_TASK2 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue

Malware / Threat Detection

- **Query:**
- **source=**"**SOC_Task2_Sample_Logs.txt**" **threat=***

- **Observation**:

- Malwareevents detected. High severity → Requires immediate SOC response.



```
source="SOC_Task2_Sample_Logs.txt" host="SOC_TASK2" sourcetype="log2metrics_keyvalue" threat=*
```

✓ 11 events (before 01/09/2025 20:58:41.000)

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a action 1
- # date_hour 4
- # date_mday 1
- # date_minute 10
- 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 2
- a splunk_server 1
- a threat 5
- # timeendpos 1
- # timestartpos 1
- a user 5

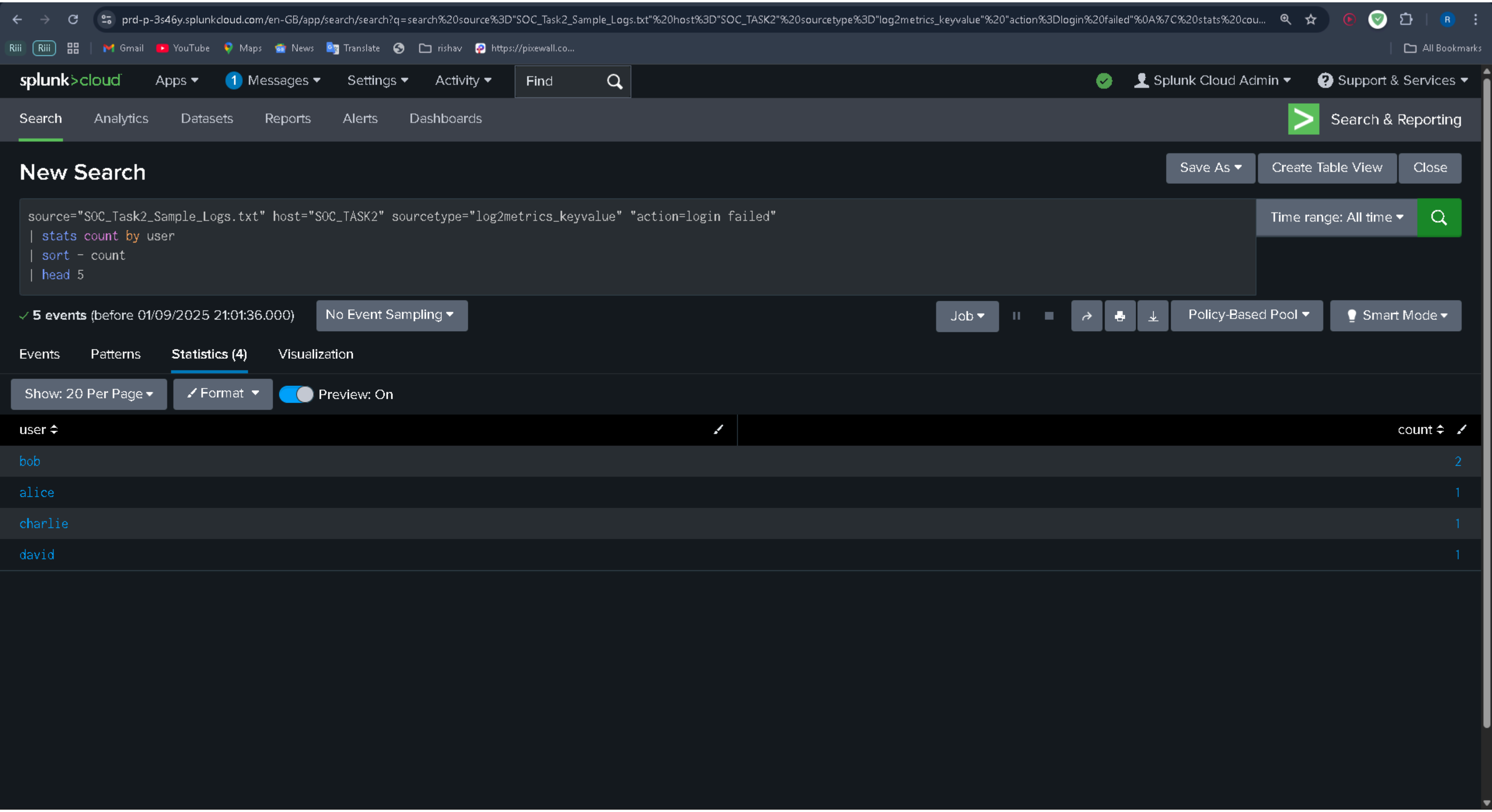
+ Extract New Fields

```
i  Time                     Event
>  03/07/2025 09:10:14.000  2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
                            host = SOC_TASK2 | source = SOC_Task2_Sample_Logs.txt | sourcetype = log2metrics_keyvalue
>  03/07/2025 07:51:14.000  2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature
                            host = SOC_TASK2 | source = SOC_Task2_Sample_Logs.txt | sourcetype = log2metrics_keyvalue
>  03/07/2025 07:45:14.000  2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
                            host = SOC_TASK2 | source = SOC_Task2_Sample_Logs.txt | sourcetype = log2metrics_keyvalue
>  03/07/2025 05:48:14.000  2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected
                            host = SOC_TASK2 | source = SOC_Task2_Sample_Logs.txt | sourcetype = log2metrics_keyvalue
>  03/07/2025 05:45:14.000  2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
                            host = SOC_TASK2 | source = SOC_Task2_Sample_Logs.txt | sourcetype = log2metrics_keyvalue
>  03/07/2025 05:42:14.000  2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected
                            host = SOC_TASK2 | source = SOC_Task2_Sample_Logs.txt | sourcetype = log2metrics_keyvalue
>  03/07/2025 05:30:14.000  2025-07-03 05:30:14 | user=eve | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
                            host = SOC_TASK2 | source = SOC_Task2_Sample_Logs.txt | sourcetype = log2metrics_keyvalue
>  03/07/2025 05:06:14.000  2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt
                            host = SOC_TASK2 | source = SOC_Task2_Sample_Logs.txt | sourcetype = log2metrics_keyvalue
>  03/07/2025 04:41:14.000  2025-07-03 04:41:14 | user=alice | ip=172.16.0.3 | action=malware detected | threat=Spyware Alert
                            host = SOC_TASK2 | source = SOC_Task2_Sample_Logs.txt | sourcetype = log2metrics_keyvalue
>  03/07/2025               2025-07-03 04:30:14 | user=alice | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
```

Top 5 Users with Most Failed Logins

- **Query:**
- **source="SOC_Task2_Sample_Logs.txt" action="login failed" | stats count by user | sort - count | head 5**

- **Observation**:
- Identifiedtop5users with excessive failed logins.



```
source="SOC_Task2_Sample_Logs.txt" host="SOC_TASK2" sourcetype="log2metrics_keyvalue" "action=login failed"
| stats count by user
| sort - count
| head 5
```

✓ 5 events (before 01/09/2025 21:01:36.000)

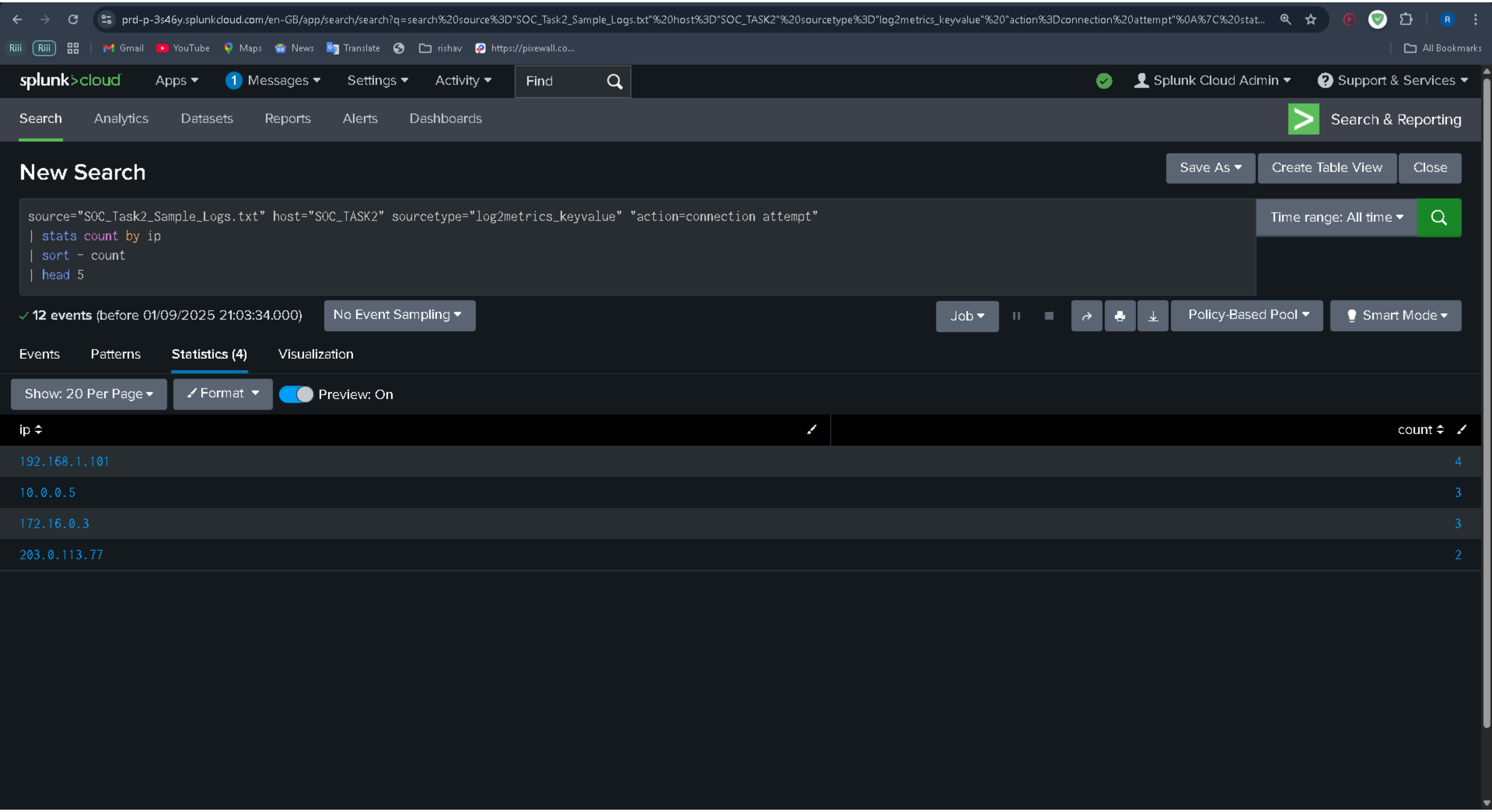
Statistics (4)

user	count
bob	2
alice	1
charlie	1
david	1

Top 5 IPs with Most Connection Attempts

- **Query:**
- **source="SOC_Task2_Sample_Logs.txt" action="connection attempt" | stats count by ip | sort - count | head 5**

- **Observation**:
- CertainIPsshowsuspicious connection attempts.



New Search

```
source="SOC_Task2_Sample_Logs.txt" host="SOC_TASK2" sourcetype="log2metrics_keyvalue" "action=connection attempt"
| stats count by ip
| sort - count
| head 5
```

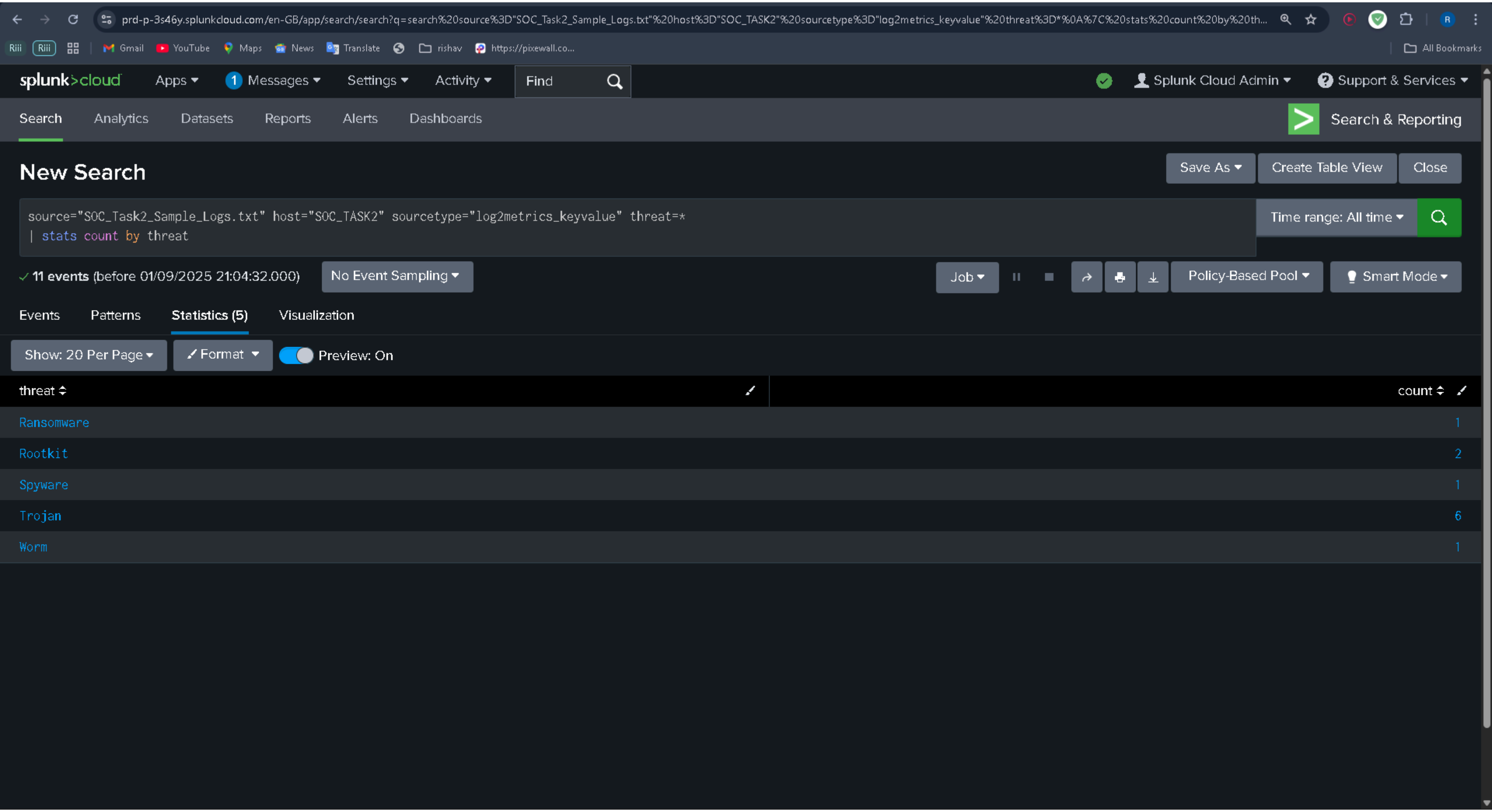
✓ 12 events (before 01/09/2025 21:03:34.000)

ip	count
192.168.1.101	4
10.0.0.5	3
172.16.0.3	3
203.0.113.77	2

Malware Type Count

- **Query**:
- **source**="**SOC_Task2_Sample_Logs.txt**" **threat=* | stats count by threat**

- **Observation**:
- Different malware types detected → Classification of threats possible.



prd-p-3s46y.splunkcloud.com/en-GB/app/search/search?q=search%20source%3D"SOC_Task2_Sample_Logs.txt"%20host%3D"SOC_TASK2"%20sourcetype%3D"log2metrics_keyvalue"%20threat%3D*%0A%7C%20stats%20count%20by%20th...

New Search

```
source="SOC_Task2_Sample_Logs.txt" host="SOC_TASK2" sourcetype="log2metrics_keyvalue" threat=*
| stats count by threat
```

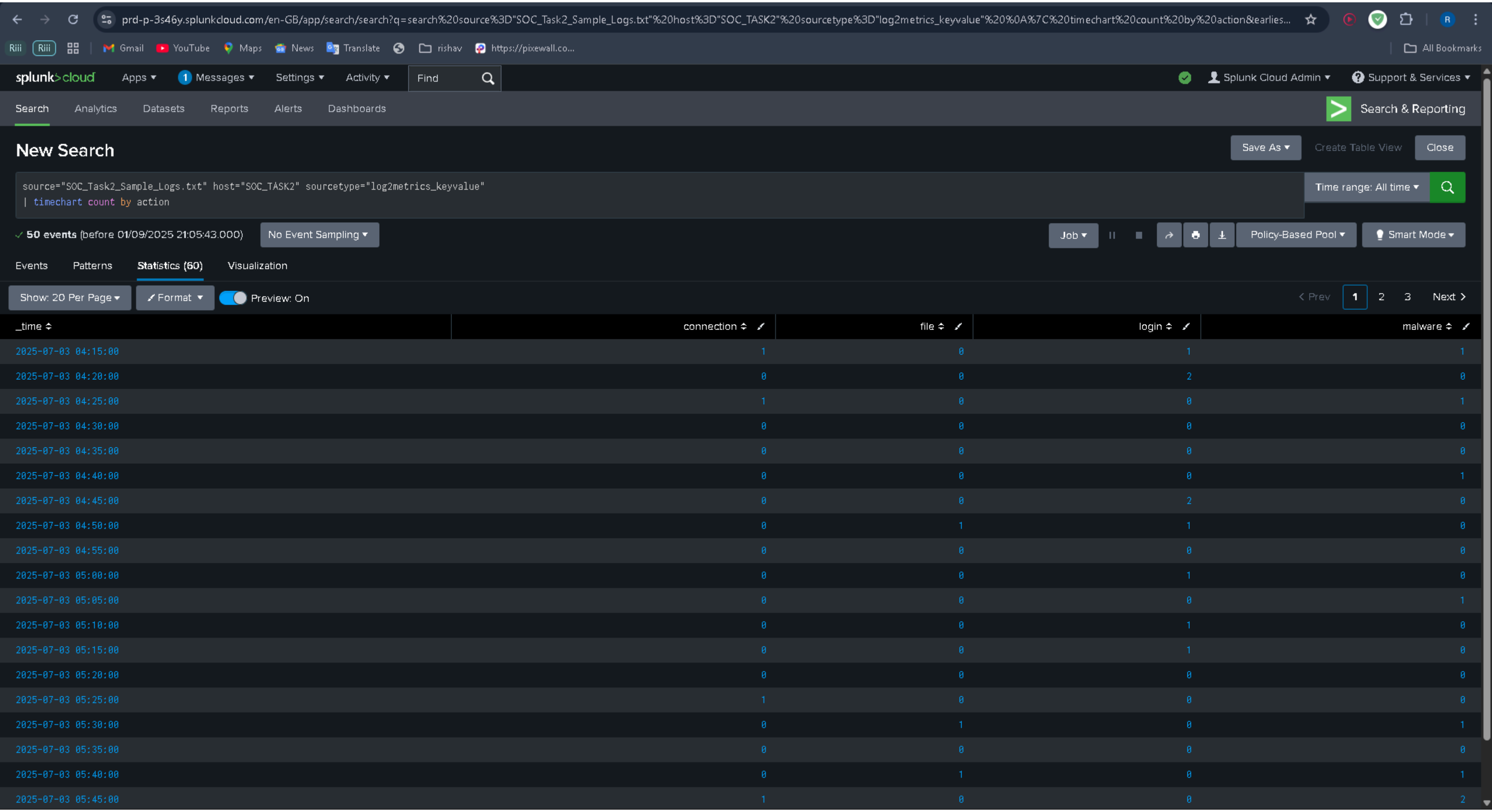
✓ **11 events** (before 01/09/2025 21:04:32.000)

threat	count
Ransomware	1
Rootkit	2
Spyware	1
Trojan	6
Worm	1

Timeline of Events

- **Query:**
- **source="SOC_Task2_Sample_Logs.txt" | timechart count by action**

- **Observation**:
- Timeline shows peaks in failed logins and malware detections (attack windows).



New Search

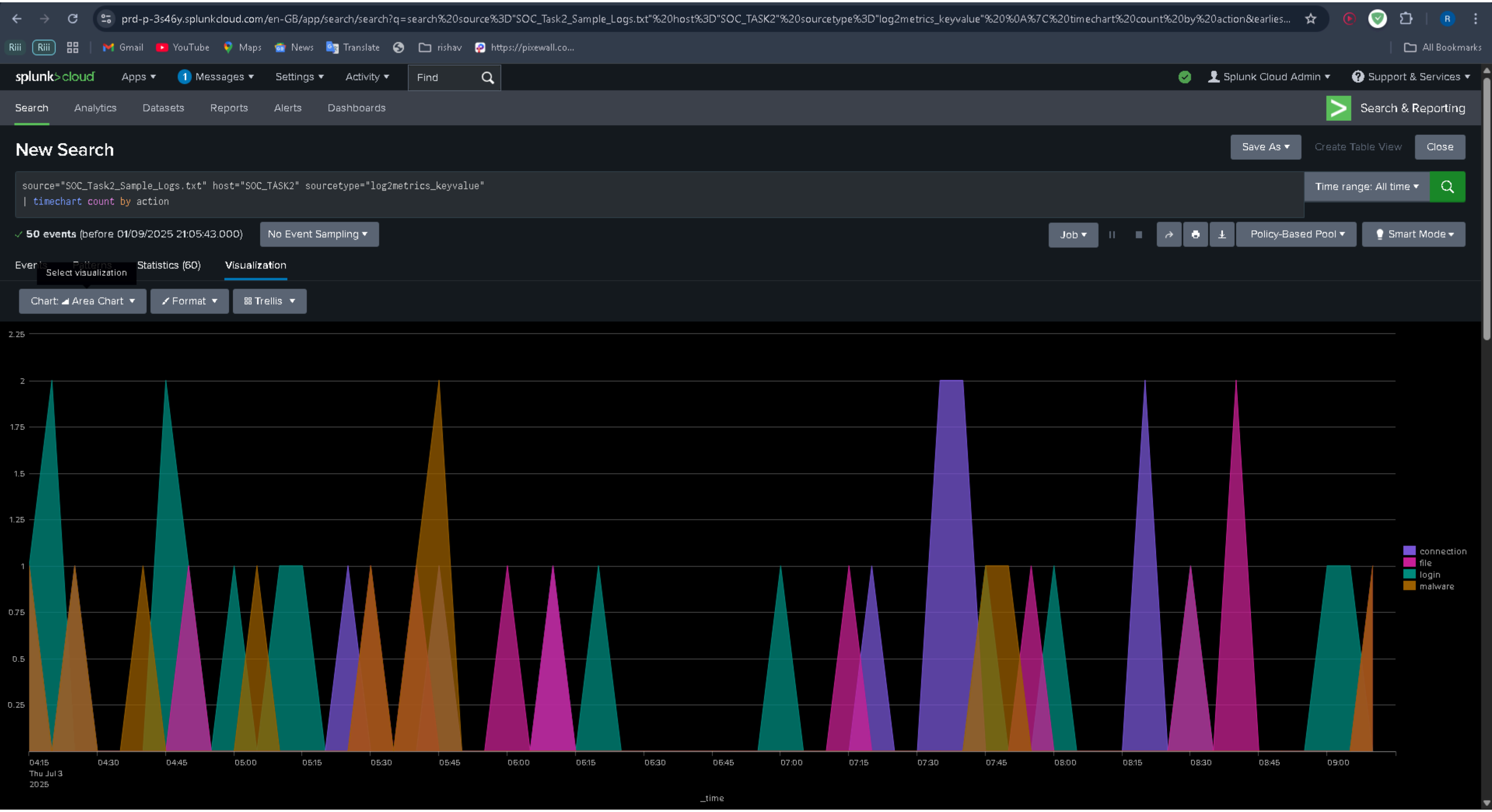
```
source="SOC_Task2_Sample_Logs.txt" host="SOC_TASK2" sourcetype="log2metrics_keyvalue"
| timechart count by action
```

✓ 50 events (before 01/09/2025 21:05:43.000)

_time	connection	file	login	malware
2025-07-03 04:15:00	1	0	1	1
2025-07-03 04:20:00	0	0	2	0
2025-07-03 04:25:00	1	0	0	1
2025-07-03 04:30:00	0	0	0	0
2025-07-03 04:35:00	0	0	0	0
2025-07-03 04:40:00	0	0	0	1
2025-07-03 04:45:00	0	0	2	0
2025-07-03 04:50:00	0	1	1	0
2025-07-03 04:55:00	0	0	0	0
2025-07-03 05:00:00	0	0	1	0
2025-07-03 05:05:00	0	0	0	1
2025-07-03 05:10:00	0	0	1	0
2025-07-03 05:15:00	0	0	1	0
2025-07-03 05:20:00	0	0	0	0
2025-07-03 05:25:00	1	0	0	0
2025-07-03 05:30:00	0	1	0	1
2025-07-03 05:35:00	0	0	0	0
2025-07-03 05:40:00	0	1	0	1
2025-07-03 05:45:00	1	0	0	2

� Combined Log Activity Chart

- “This chart provides a consolidated visualization of all security events recorded during the monitoring period, including login attempts connection activities, file access events, and malware detections. The timeline trend highlights peaks of unusual activity, helping SOC analysts quickly spot anomalies such as brute-force login attempts abnormal file access, and malware outbreaks. Such an aggregated view enables faster incident triage, prioritization of high-risk alerts and improved situational awareness for proactive threat response.”



New Search

```
source="SOC_Task2_Sample_Logs.txt" host="SOC_TASK2" sourcetype="log2metrics_keyvalue"
| timechart count by action
```

✓ **50 events** (before 01/09/2025 21:05:43.000)

Conclusion & Recommendations

The internship tasks provided practical exposure to SOC operations, focusing on log monitoring, alert classification, and incident response reporting. By simulating real-world alerts such as malware infections, brute-force login attempts, and suspicious file access, the analysis reinforced critical skills in threat detection and response. **Key Takeaways:** - Strengthened ability to identify and prioritize security alerts using SIEM queries. - Improved knowledge of incident timelines, impact assessment, and remediation planning. - Developed professional SOC reporting practices with structured evidence and documentation. **Recommendations:** 1. Implement Multi-Factor Authentication (MFA) across all critical accounts to reduce login compromise risk. 2. Automate detection of brute-force attempts and integrate with alert escalation workflows. 3. Regularly patch and update endpoint systems to mitigate malware infections. 4. Enhance monitoring of insider threats with User and Entity Behavior Analytics (UEBA). 5. Establish routine SOC drills to improve incident response readiness. This report highlights how SOC monitoring and incident response simulations contribute to building a strong cybersecurity foundation and prepare interns for real-world security operations.