SOC Task 2 – Incident Investigation Report

Internship Project | Splunk Log Analysis

prepared by: Vishu Raj

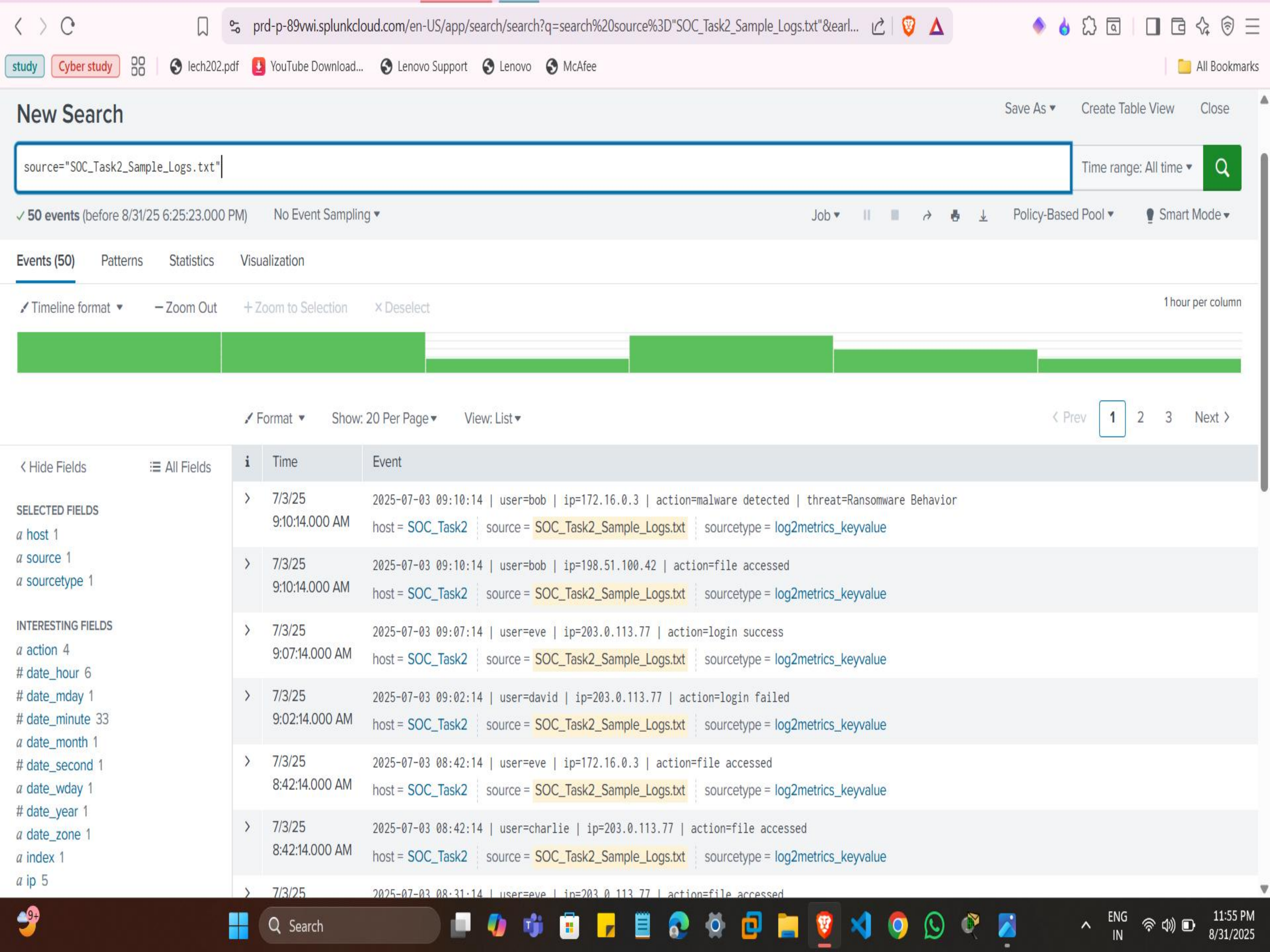
Objective

- 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**:
- All log events ingested successfully. Includes login, file access, connection attempts, and malware detections.


prd-p-89vwi.splunkcloud.com/en-US/app/search/search?q=search%20source%3D"SOC_Task2_Sample_Logs.txt"&earl...
study
Cyber study
lech202.pdf
YouTube Download...
Lenovo Support
Lenovo
McAfee
All Bookmarks

New Search

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

✓ 50 events (before 8/31/25 6:25:23.000 PM) No Event Sampling ▾

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

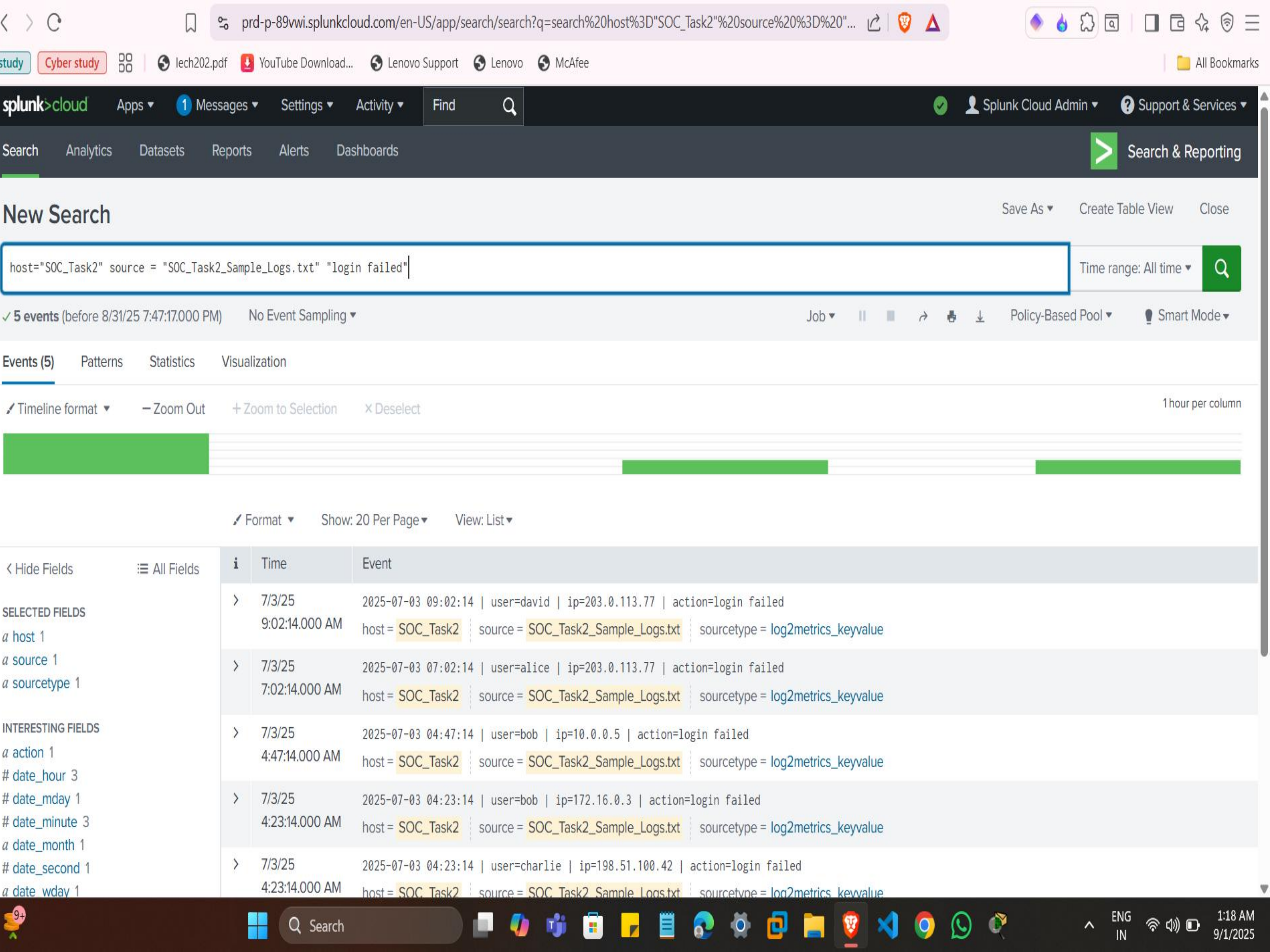
- a action 4
- # date_hour 6
- # date_mday 1
- # date_minute 33
- a date_month 1
- # date_second 1
- a date_wday 1
- # date_year 1
- a date_zone 1
- a index 1
- a ip 5

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 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
›	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 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
›	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 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
›	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 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
›	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 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
›	7/3/25 8:42:14.000 AM	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
›	7/3/25	2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed

Failed Login Attempts

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

- **Observation**:
- Several failed login attempts recorded → Possible brute force or credential-stuffing activity.



```
host="SOC_Task2" source = "SOC_Task2_Sample_Logs.txt" "login failed"
```

✓ 5 events (before 8/31/25 7:47:17.000 PM)

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

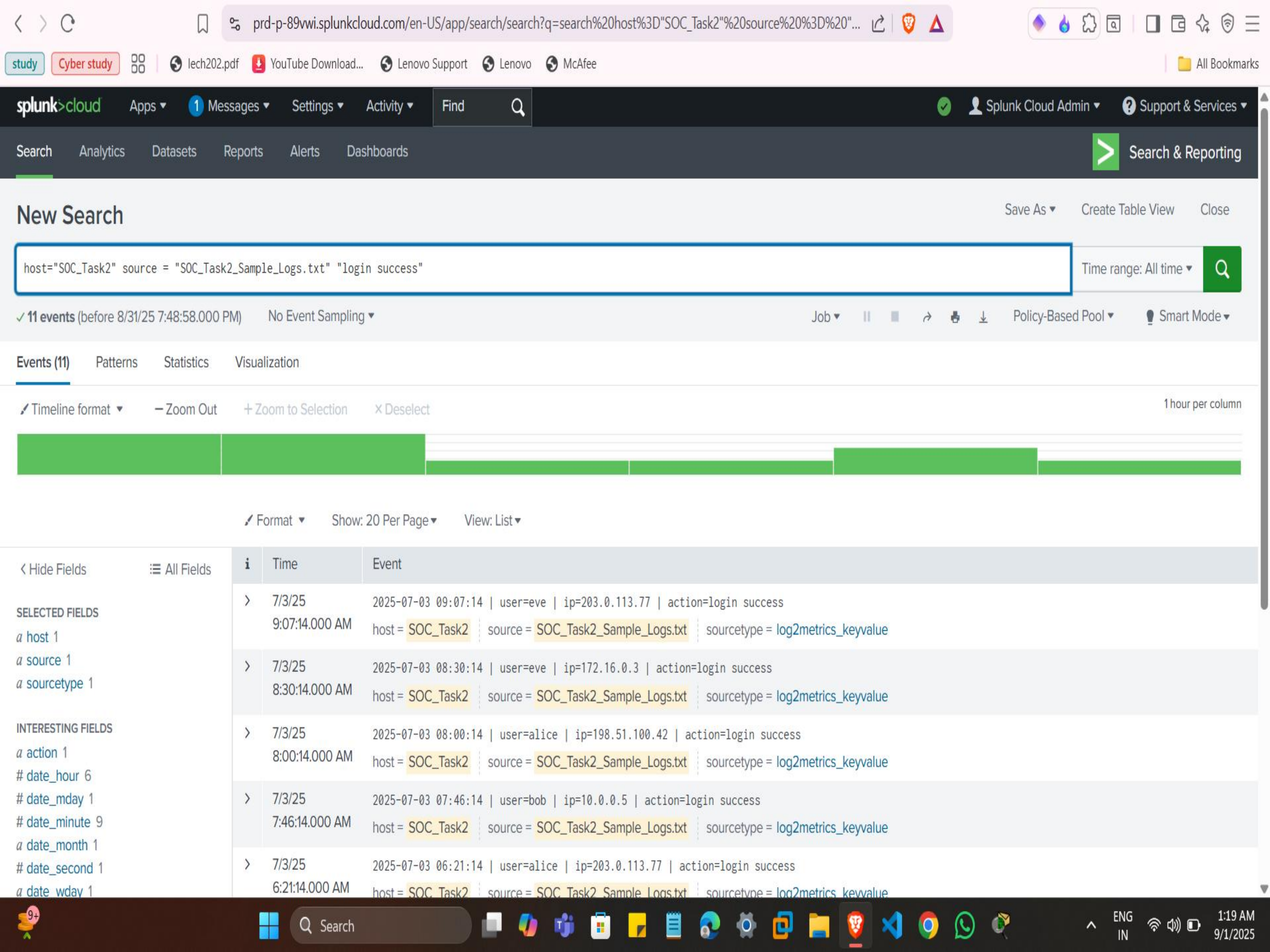
INTERESTING FIELDS
- a action 1
- # date_hour 3
- # date_mday 1
- # date_minute 3
- a date_month 1
- # date_second 1
- a date_wday 1

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 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	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 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	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 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	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 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	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 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue

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.



```
host="SOC_Task2" source = "SOC_Task2_Sample_Logs.txt" "login success"
```

✓ 11 events (before 8/31/25 7:48:58.000 PM)

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

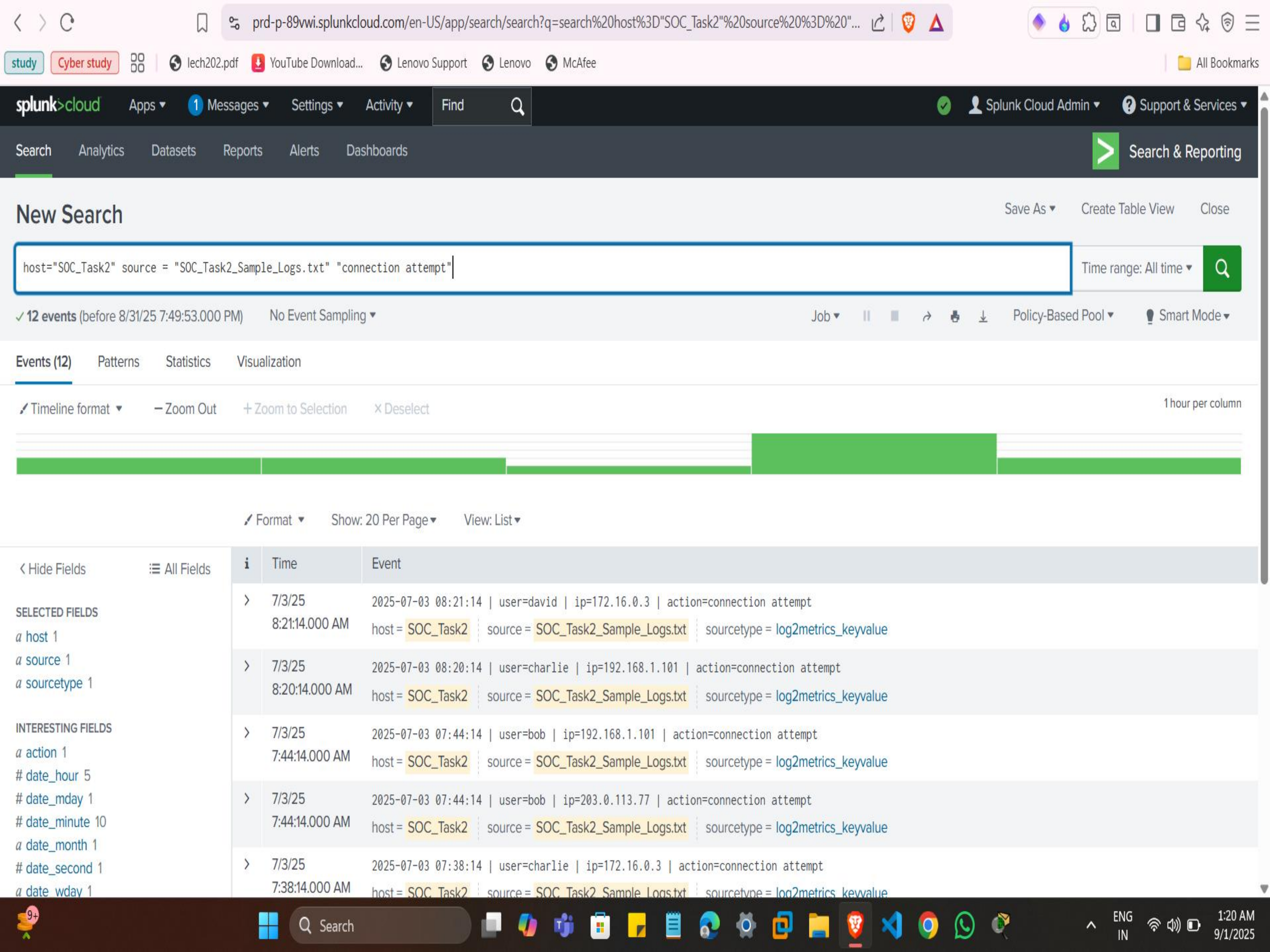
INTERESTING FIELDS
- a action 1
- # date_hour 6
- # date_mday 1
- # date_minute 9
- a date_month 1
- # date_second 1
- a date_wday 1

i	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 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
›	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 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
›	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 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
›	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 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
›	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 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue

Connection Attempts

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

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



New Search

```
host="SOC_Task2" source = "SOC_Task2_Sample_Logs.txt" "connection attempt"
```

Time range: All time

✓ 12 events (before 8/31/25 7:49:53.000 PM) No Event Sampling

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

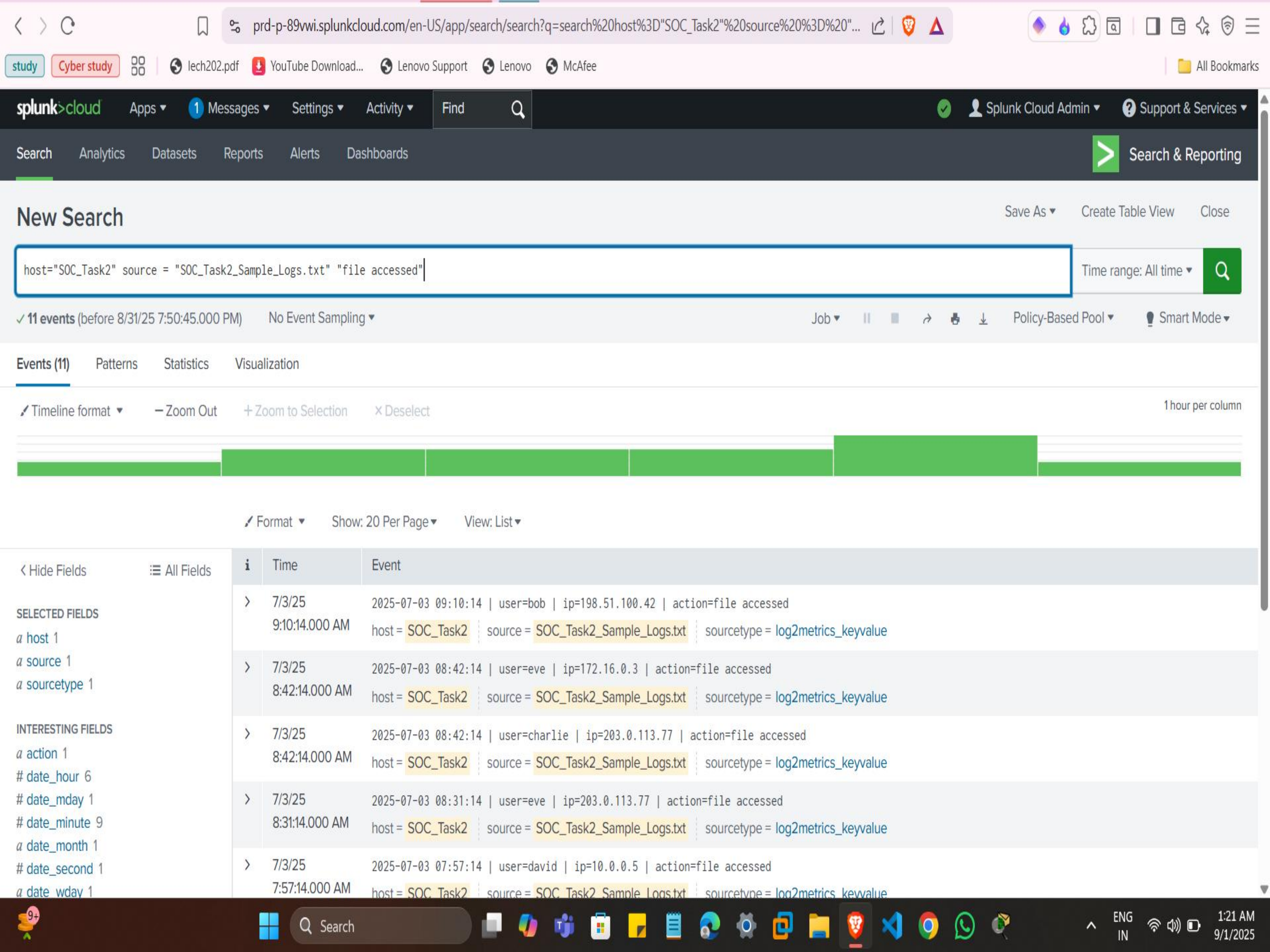
INTERESTING FIELDS
- a action 1
- # date_hour 5
- # date_mday 1
- # date_minute 10
- a date_month 1
- # date_second 1
- a date_wday 1

i	Time	Event
>	7/3/25 8:21:14.000 AM	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
>	7/3/25 8:20:14.000 AM	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
>	7/3/25 7:44:14.000 AM	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
>	7/3/25 7:44:14.000 AM	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
>	7/3/25 7:38:14.000 AM	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

File Accessed Events

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

- **Observation**:
- Files accessed by multiple users. Needs correlation with login attempts for insider activity.



New Search

```
host="SOC_Task2" source = "SOC_Task2_Sample_Logs.txt" "file accessed"
```

Time range: All time

✓ 11 events (before 8/31/25 7:50:45.000 PM) No Event Sampling

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

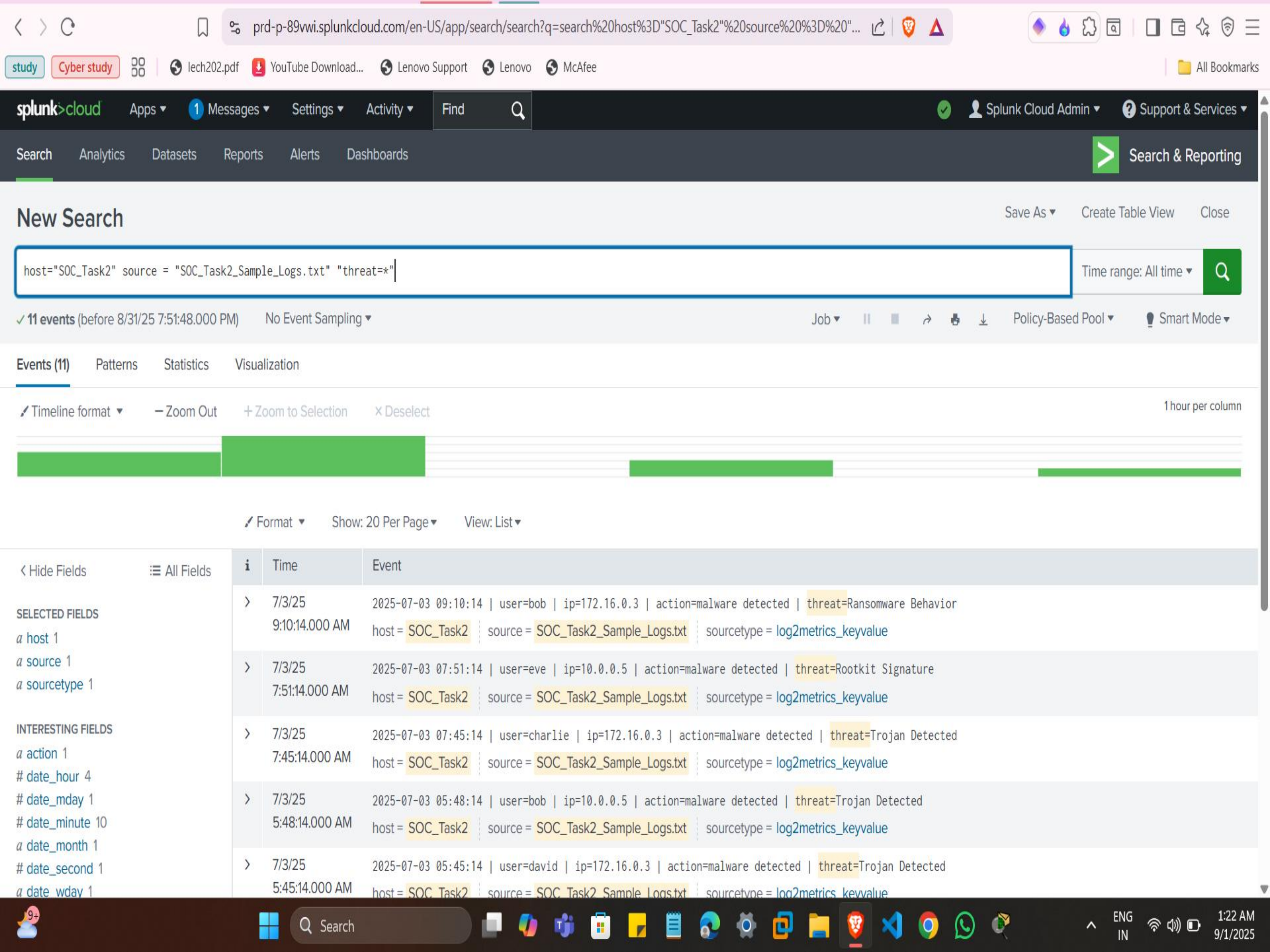
INTERESTING FIELDS
- a action 1
- # date_hour 6
- # date_mday 1
- # date_minute 9
- a date_month 1
- # date_second 1
- a date_wday 1

i	Time	Event
>	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 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	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 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	7/3/25 8:42:14.000 AM	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
>	7/3/25 8:31:14.000 AM	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
>	7/3/25 7:57:14.000 AM	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

Malware / Threat Detection

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

- **Observation**:
- Malware events detected. High severity → Requires immediate SOC response.



New Search

```
host="SOC_Task2" source = "SOC_Task2_Sample_Logs.txt" "threat=*"
```

✓ 11 events (before 8/31/25 7:51:48.000 PM) No Event Sampling

Events (11)

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

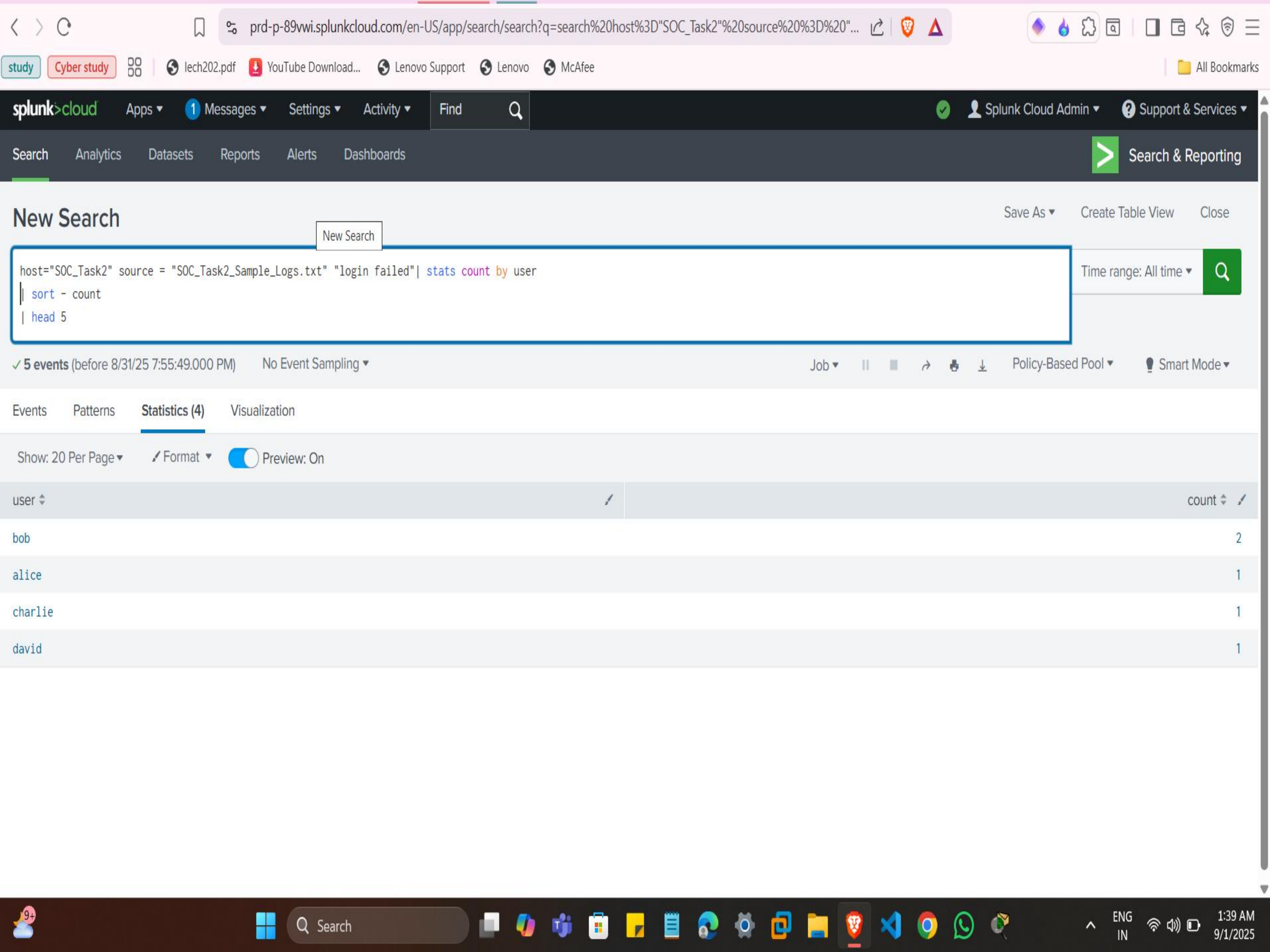
INTERESTING FIELDS
- a action 1
- # date_hour 4
- # date_mday 1
- # date_minute 10
- a date_month 1
- # date_second 1
- a date_wday 1

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 source = SOC_Task2_Sample_Logs.txt sourcetype = log2metrics_keyvalue
>	7/3/25 7:51:14.000 AM	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
>	7/3/25 7:45:14.000 AM	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
>	7/3/25 5:48:14.000 AM	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
>	7/3/25 5:45:14.000 AM	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

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**:
- Identified top 5 users with excessive failed logins.



New Search

```
host="SOC_Task2" source = "SOC_Task2_Sample_Logs.txt" "login failed"| stats count by user
| sort - count
| head 5
```

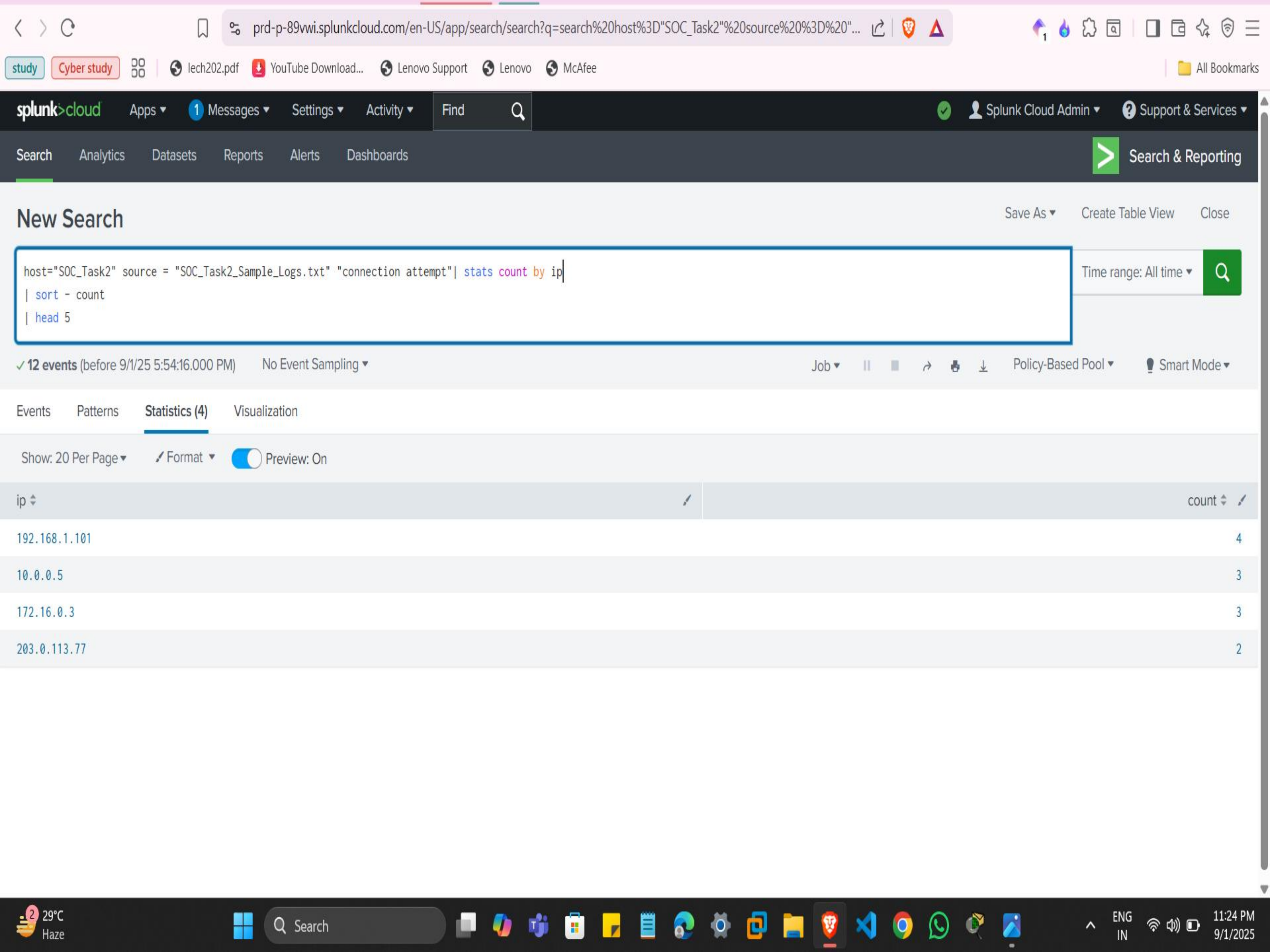
✓ 5 events (before 8/31/25 7:55:49.000 PM)   No Event Sampling

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**:
- Certain IPs show suspicious connection attempts.



New Search

```
host="SOC_Task2" source = "SOC_Task2_Sample_Logs.txt" "connection attempt"| stats count by ip
| sort - count
| head 5
```

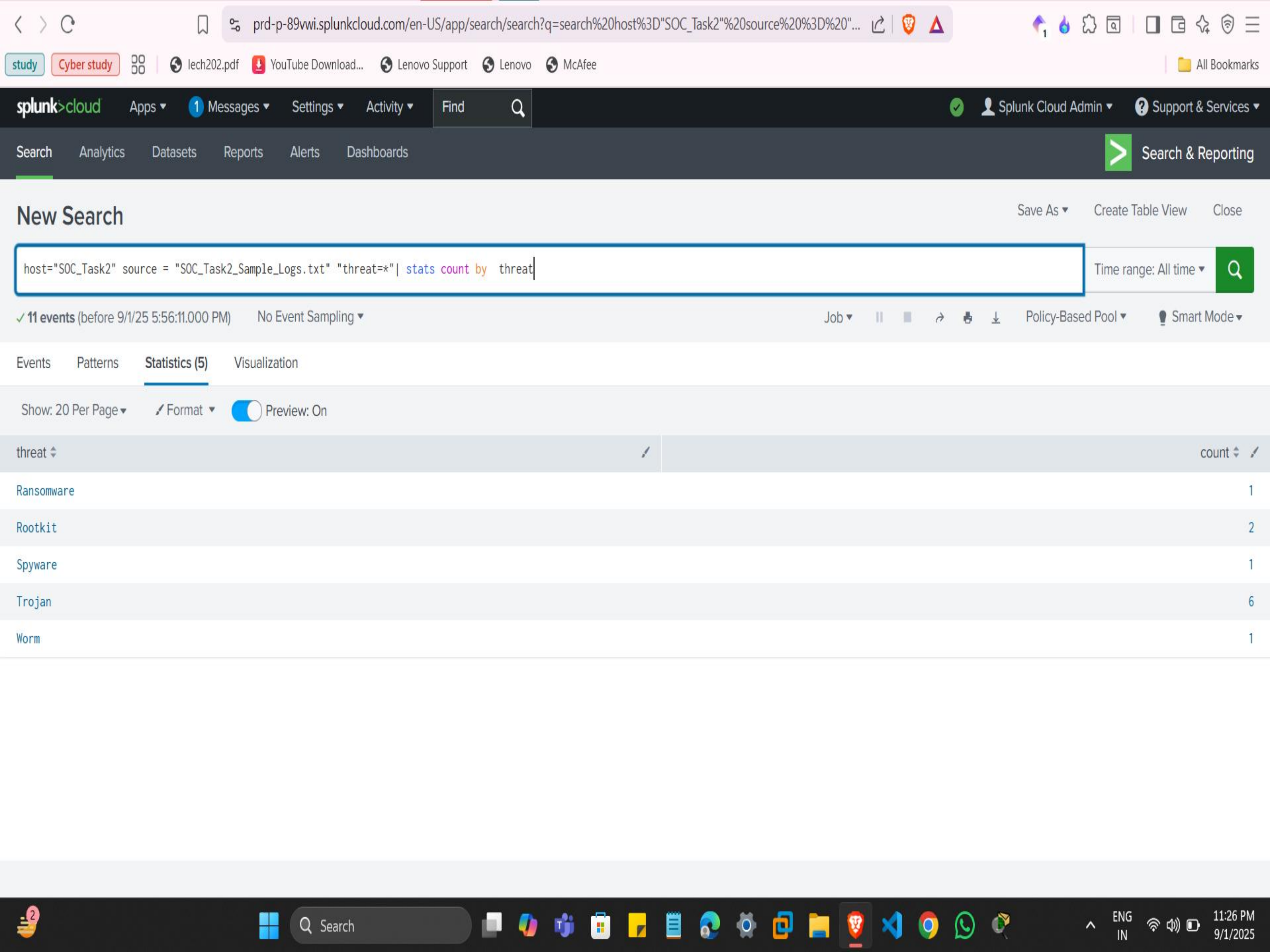
✓ 12 events (before 9/1/25 5:54:16.000 PM)

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.



New Search

```
host="SOC_Task2" source = "SOC_Task2_Sample_Logs.txt" "threat=*"| stats count by  threat
```

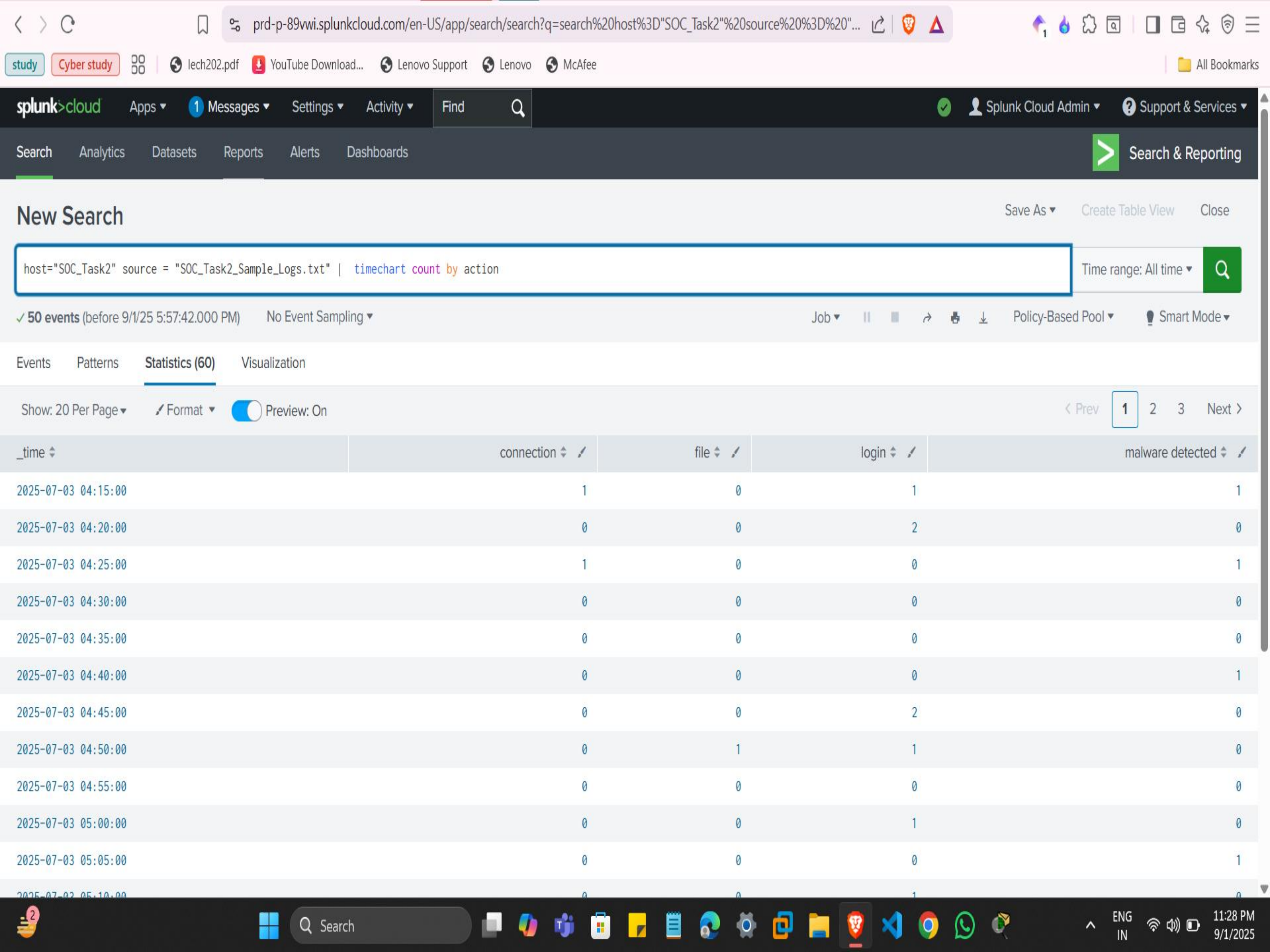
✓ 11 events (before 9/1/25 5:56:11.000 PM) No Event Sampling

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

```
host="SOC_Task2" source = "SOC_Task2_Sample_Logs.txt" |  timechart count by action
```

Time range: All time

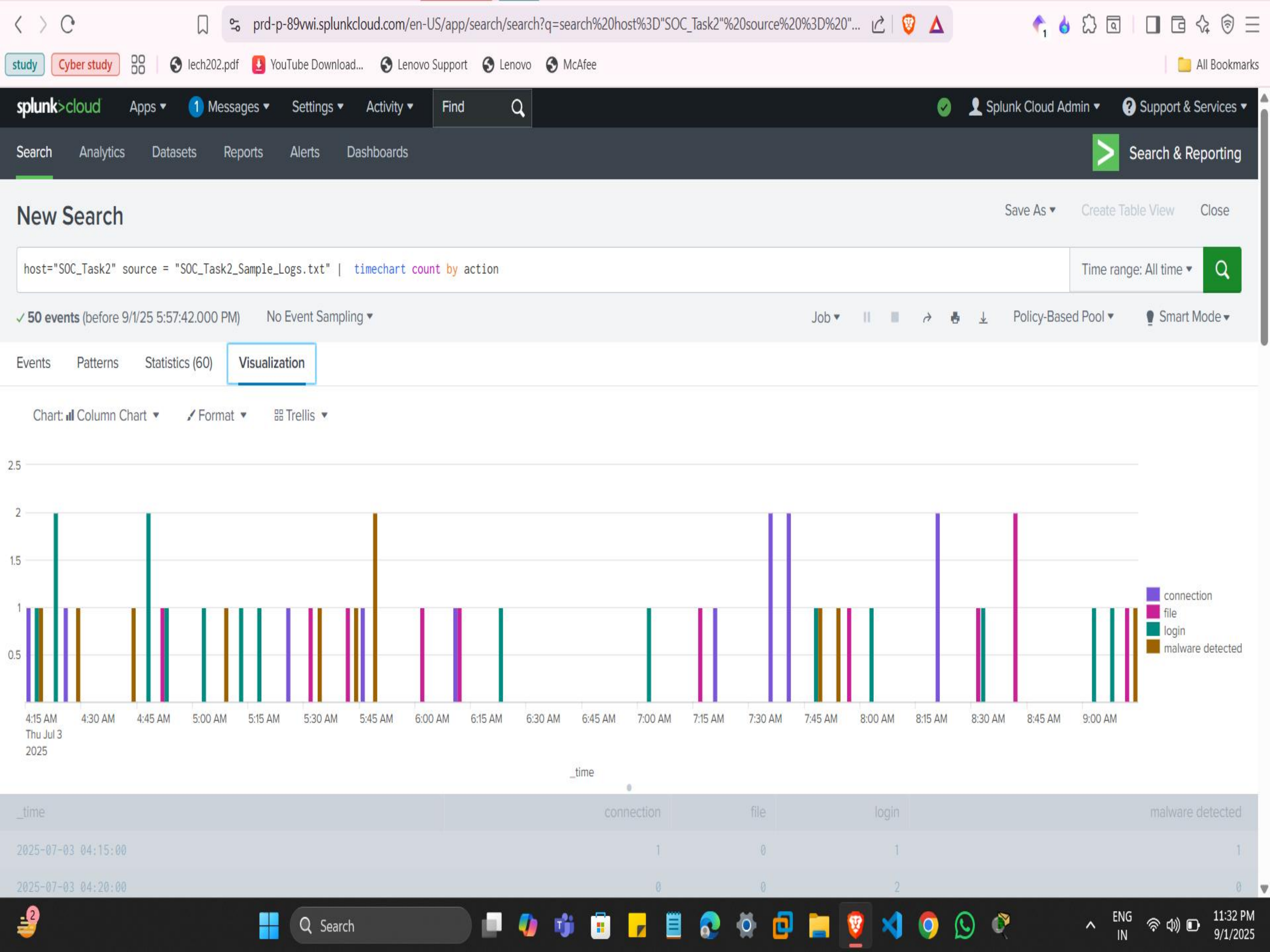
✓ 50 events (before 9/1/25 5:57:42.000 PM)   No Event Sampling

Show: 20 Per Page   Preview: On

_time	connection	file	login	malware detected
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

📊 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

```
host="SOC_Task2" source = "SOC_Task2_Sample_Logs.txt" |  timechart count by action
```

✓ **50 events** (before 9/1/25 5:57:42.000 PM)

_time	connection	file	login	malware detected
2025-07-03 04:15:00	1	0	1	1
2025-07-03 04:20:00	0	0	2	0

Conclusion & Recommendations

- **Findings**:
- - Multiple failed logins & suspicious connection attempts.
- - Top targeted users & IPs identified.
- - Malware detection confirms active threat.

- **Recommendations**:
- 1. Block IPs with excessive failed attempts.
- 2. Enforce account lockout policies.
- 3. Conduct malware remediation & isolate systems.
- 4. Add Splunk alerts for failed logins > threshold.
- 5. Forensic review of file access activity.