SOC LOG ANALYSIS PROJECT

Splunk-Based Security Event Monitoring

Name: Sunidhi

Role Focus: SOC Analyst

Tool Used: Splunk Cloud

1. Objective of the Project

The objective of this project is to simulate a real-time SOC investigation by analyzing Linux SSH authentication logs using Splunk.

The goal was to identify suspicious login attempts, analyze brute-force attack patterns, and determine threat sources targeting the system.

2. Environment Setup

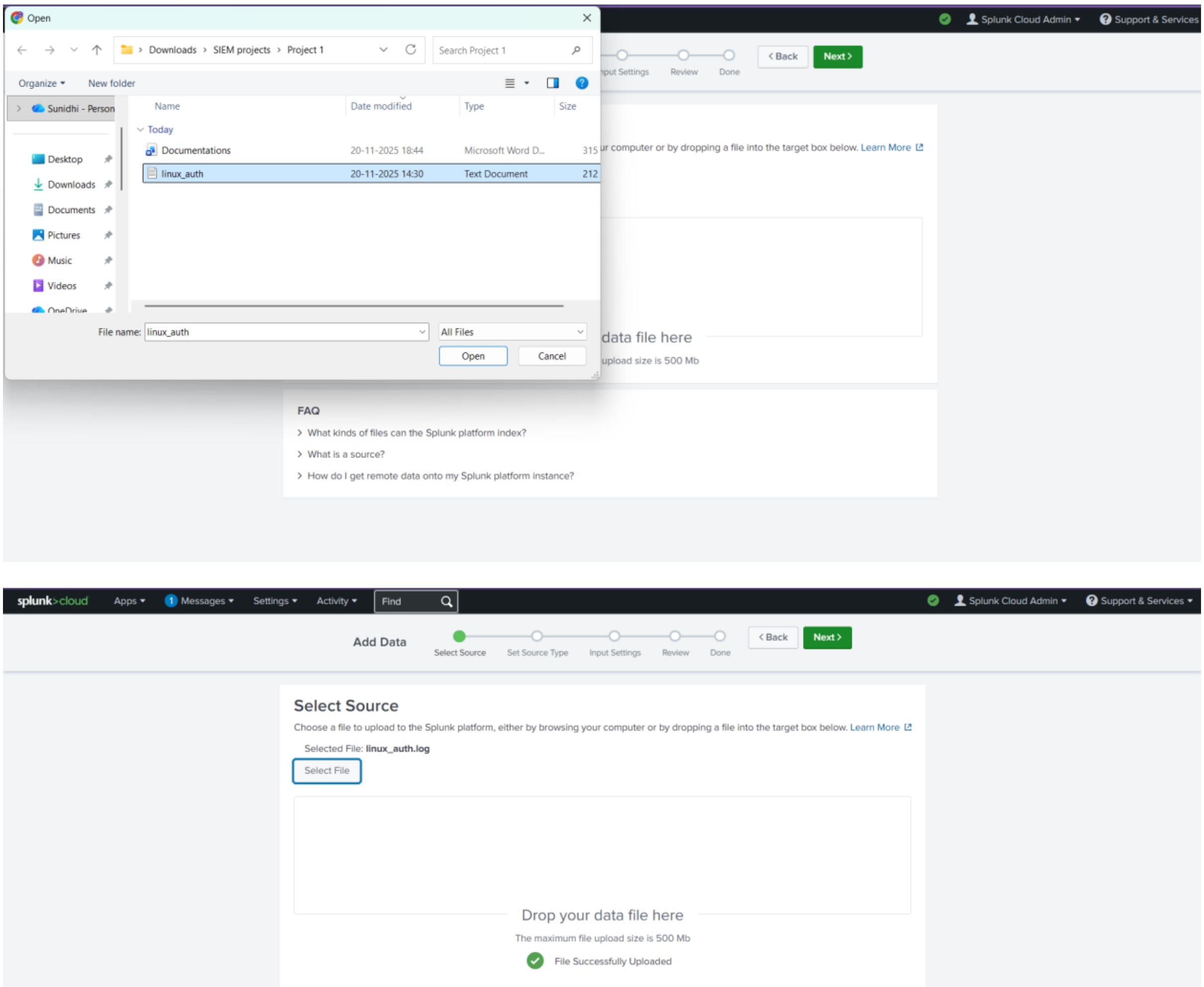
SIEM Tool: Splunk Cloud Platform

Data Type: Linux Authentication Logs

Host: linux_server01

Source Type: linux_secure

The logs were manually uploaded and analyzed using Splunk's Search Processing Language (SPL).



Name	Date modified	Type	Size
Documentations	20-11-2025 18:44	Microsoft Word D...	315
linux_auth	20-11-2025 14:30	Text Document	212

File name: linux_auth

All Files

...ur computer or by dropping a file into the target box below. Learn More

...data file here

...upload size is 500 Mb

› What kinds of files can the Splunk platform index?

› What is a source?

› How do I get remote data onto my Splunk platform instance?

Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More

Selected File: **linux_auth.log**

Drop your data file here

The maximum file upload size is 500 Mb

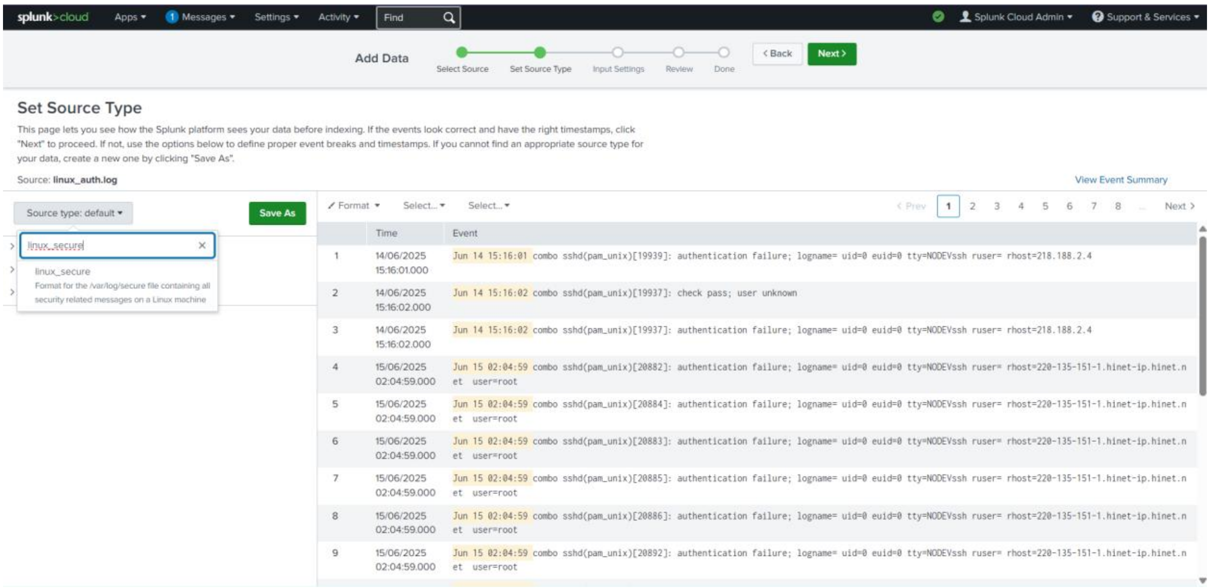
File Successfully Uploaded

Screenshot: Splunk dashboard / Data upload confirmation

3. Log Ingestion Process

The Linux authentication logs were uploaded into Splunk using the "Add Data" feature.

The source type was set to linux_secure and host was configured as linux_server01 for accurate parsing.

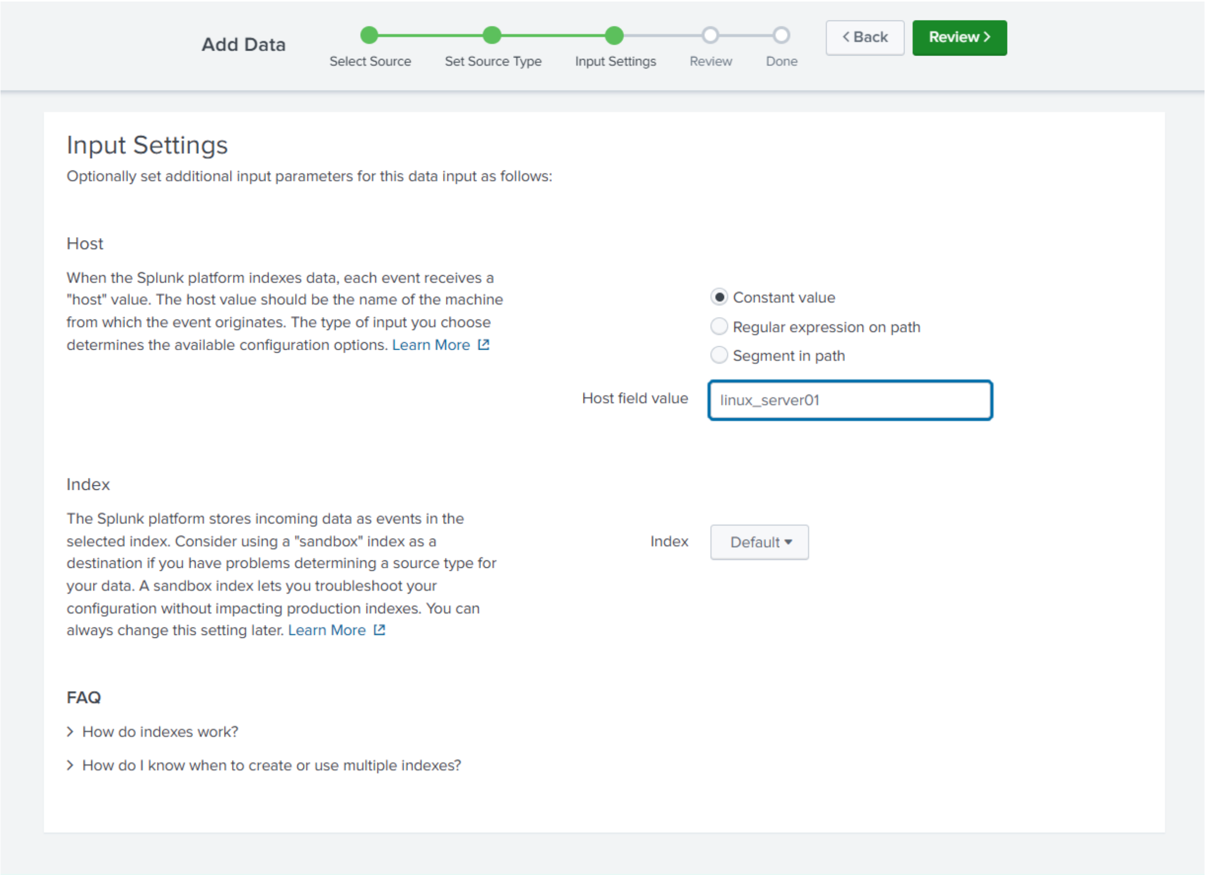


Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **linux_auth.log**

	Time	Event
1	14/06/2025 15:16:01.000	`Jun 14 15:16:01 combo sshd(pam_unix)[19939]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=218.188.2.4`
2	14/06/2025 15:16:02.000	`Jun 14 15:16:02 combo sshd(pam_unix)[19937]: check pass; user unknown`
3	14/06/2025 15:16:02.000	`Jun 14 15:16:02 combo sshd(pam_unix)[19937]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=218.188.2.4`
4	15/06/2025 02:04:59.000	`Jun 15 02:04:59 combo sshd(pam_unix)[20882]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hinet.net  user=root`
5	15/06/2025 02:04:59.000	`Jun 15 02:04:59 combo sshd(pam_unix)[20884]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hinet.net  user=root`
6	15/06/2025 02:04:59.000	`Jun 15 02:04:59 combo sshd(pam_unix)[20883]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hinet.net  user=root`
7	15/06/2025 02:04:59.000	`Jun 15 02:04:59 combo sshd(pam_unix)[20885]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hinet.net  user=root`
8	15/06/2025 02:04:59.000	`Jun 15 02:04:59 combo sshd(pam_unix)[20886]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hinet.net  user=root`
9	15/06/2025 02:04:59.000	`Jun 15 02:04:59 combo sshd(pam_unix)[20892]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hinet.net  user=root`



Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

● Constant value
○ Regular expression on path
○ Segment in path

Host field value: linux_server01

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

Index: Default ▾

FAQ

› How do indexes work?

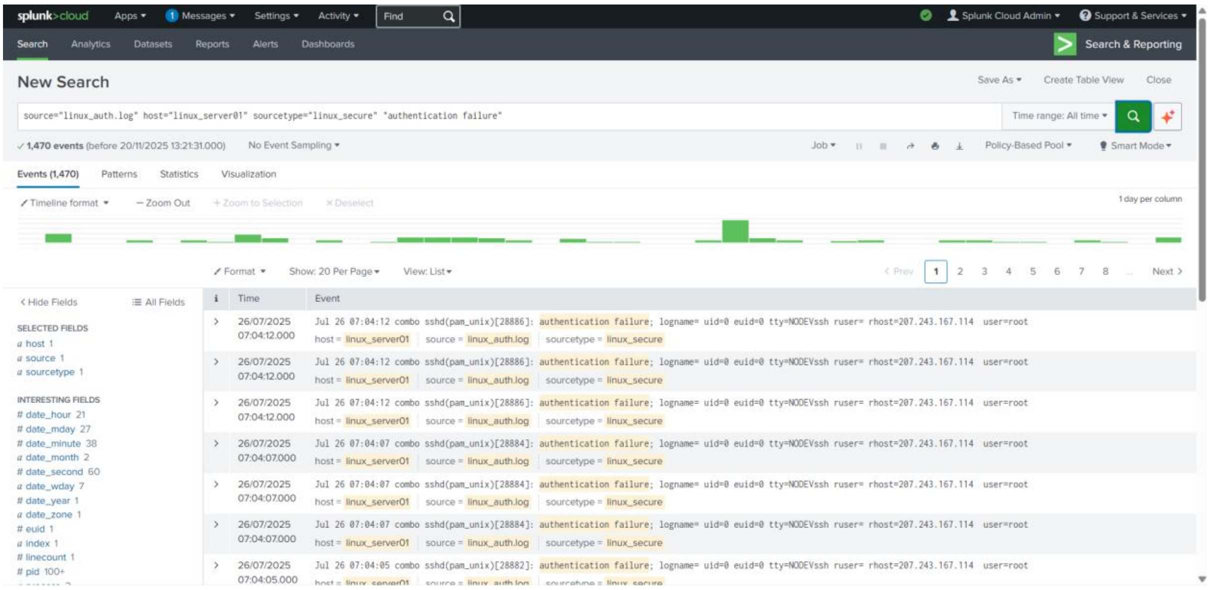
› How do I know when to create or use multiple indexes?

4. Detection Queries and Findings

4.1 Authentication Failure Detection

Query: source="linux_auth.log" host="linux_server01" sourcetype="linux_secure" "authentication failure"

This query filters all authentication failure events from the SSH logs.



New Search

```
source="linux_auth.log" host="linux_server01" sourcetype="linux_secure" "authentication failure"
```

✓ 1,470 events (before 20/11/2025 13:21:31.000) No Event Sampling

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

INTERESTING FIELDS
- # date_hour 21
- # date_mday 27
- # date_minute 38
- a date_month 2
- # date_second 60
- a date_wday 7
- # date_year 1
- a date_zone 1
- # euid 1
- a index 1
- # linecount 1
- # pid 100+

```
26/07/2025 07:04:12.000  Jul 26 07:04:12 combo sshd(pam_unix)[28886]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=207.243.167.114  user=root
                         host = linux_server01 | source = linux_auth.log | sourcetype = linux_secure
26/07/2025 07:04:12.000  Jul 26 07:04:12 combo sshd(pam_unix)[28886]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=207.243.167.114  user=root
                         host = linux_server01 | source = linux_auth.log | sourcetype = linux_secure
26/07/2025 07:04:12.000  Jul 26 07:04:12 combo sshd(pam_unix)[28886]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=207.243.167.114  user=root
                         host = linux_server01 | source = linux_auth.log | sourcetype = linux_secure
26/07/2025 07:04:07.000  Jul 26 07:04:07 combo sshd(pam_unix)[28884]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=207.243.167.114  user=root
                         host = linux_server01 | source = linux_auth.log | sourcetype = linux_secure
26/07/2025 07:04:07.000  Jul 26 07:04:07 combo sshd(pam_unix)[28884]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=207.243.167.114  user=root
                         host = linux_server01 | source = linux_auth.log | sourcetype = linux_secure
26/07/2025 07:04:07.000  Jul 26 07:04:07 combo sshd(pam_unix)[28884]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=207.243.167.114  user=root
                         host = linux_server01 | source = linux_auth.log | sourcetype = linux_secure
26/07/2025 07:04:05.000  Jul 26 07:04:05 combo sshd(pam_unix)[28882]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=207.243.167.114  user=root
                         host = linux_server01 | source = linux_auth.log | sourcetype = linux_secure
```

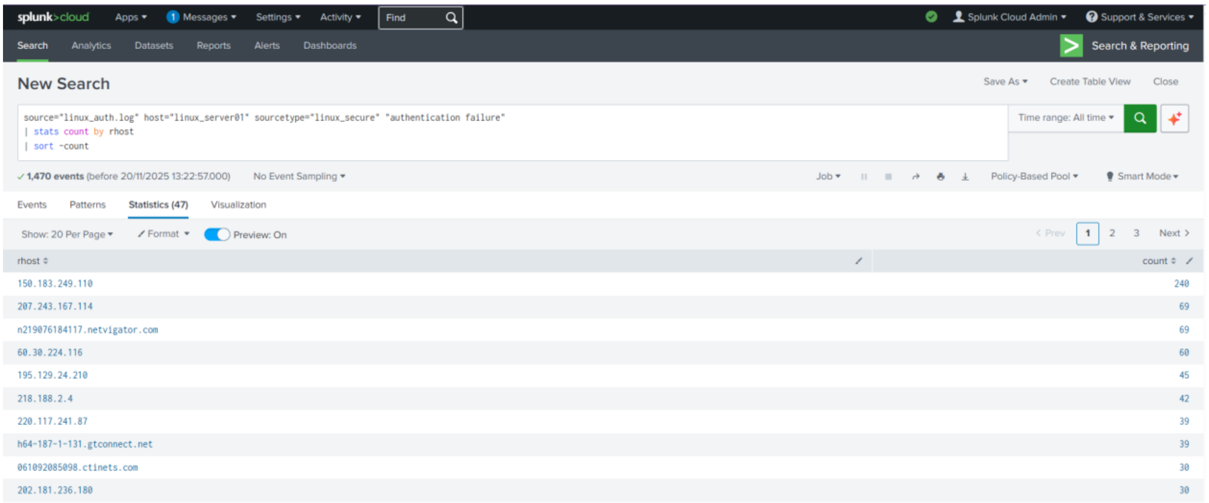
Screenshot 3: SSH Authentication Failure Events

4.2 Top Attacking Ips

Query: | stats count by rhost

| sort -count

The top attacking IP address was 150.183.249.110 with 240 failed attempts, indicating a brute-force login attack pattern. This query helped identify the most aggressive attacker by counting the number of failed login attempts per IP address.



New Search

```
source="linux_auth.log" host="linux_server01" sourcetype="linux_secure" "authentication failure"
| stats count by rhost
| sort -count
```

✓ 1,470 events (before 20/11/2025 13:22:57.000) No Event Sampling

rhost	count
150.183.249.110	240
207.243.167.114	69
n219076184117.netvigator.com	69
60.30.224.116	60
195.129.24.210	45
218.188.2.4	42
220.117.241.87	39
h64-187-1-131.gtconnect.net	39
061092085098.ctinets.com	30
202.181.236.180	30

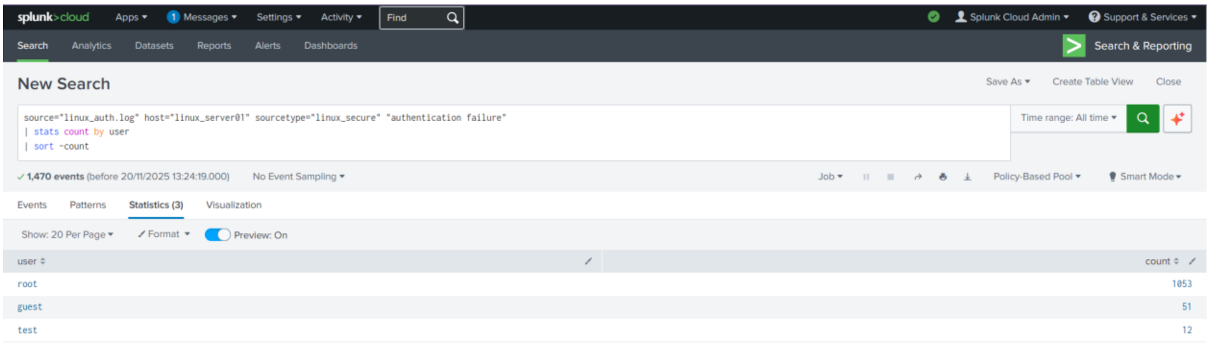
Screenshot: Top Attacking IP Addresses

4.3 Targeted User Accounts

Query: | stats count by user

| sort -count

The account "root" was targeted most frequently with 1053 failed login attempts, showing attackers were attempting privilege escalation.



```
source="linux_auth.log" host="linux_server01" sourcetype="linux_secure" "authentication failure"
| stats count by user
| sort -count
```

✓ 1,470 events (before 20/11/2025 13:24:19.000) No Event Sampling ▾

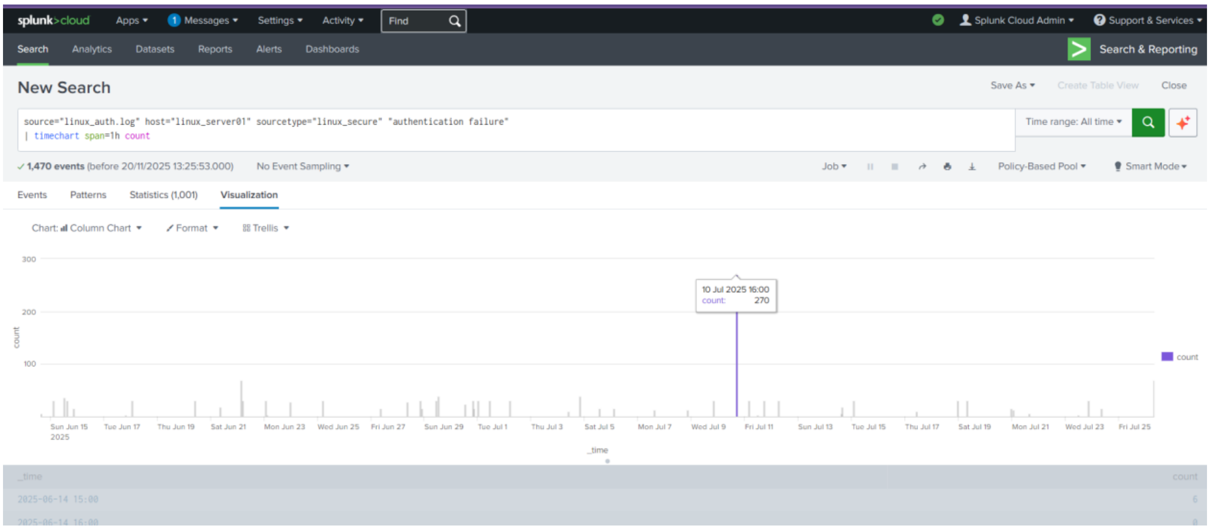
user	count
root	1053
guest	51
test	12

Screenshot: Targeted User Accounts

4.4 Attack Timeline

Query: | timechart span=1h count

A major spike occurred on July 10 around 16:00, suggesting a burst brute-force attack attempt.



```
source="linux_auth.log" host="linux_server01" sourcetype="linux_secure" "authentication failure"
| timechart span=1h count
```

✓ 1,470 events (before 20/11/2025 13:25:53.000) No Event Sampling ▾

_time	count
2025-06-14 15:00	6
2025-06-14 16:00	0

Screenshot: Attack timeline graph

5. Incident Analysis

The analysis shows repeated brute-force login attempts targeting privileged accounts from multiple external IP addresses.

These attacks indicate unauthorized access attempts and possible reconnaissance activity.

6. Conclusion

This project demonstrates how SIEM tools like Splunk can detect real-world cyber-attack patterns through log analysis.

It highlights the importance of continuous monitoring in SOC environments.

7. Recommendations

1. Implement account lockout after multiple failed attempts

2. Use key-based SSH authentication instead of passwords

3. Block malicious IP addresses using firewall rules

4. Monitor privileged account activity continuously