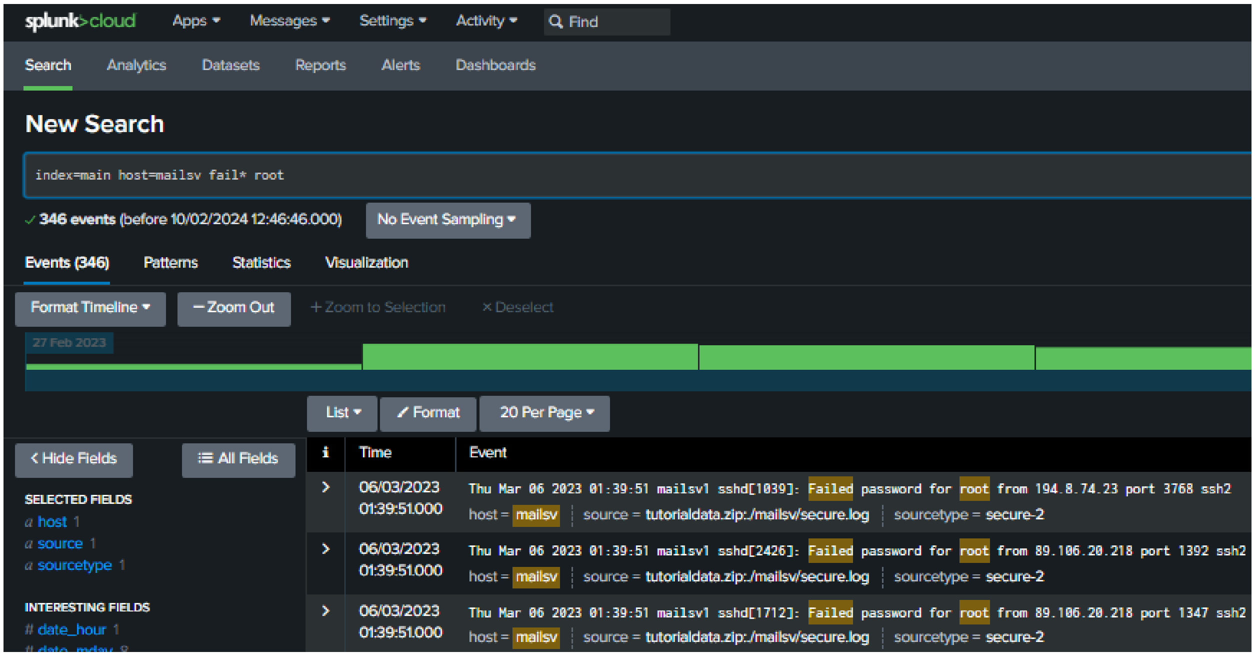
Splunk - Failed SSH logins

Problem: identify whether there are any possible security issues with the mail server.

Goal: Explore any failed SSH logins for the root account.

Process:

- Upload data into Splunk
- Navigate to Search and Reporting tab, enter index=main host=mailsv fail* root
- Results:



```
index=main host=mailsv fail* root
```

✓ 346 events (before 10/02/2024 12:46:46.000)

```
i  Time                     Event
>  06/03/2023 01:39:51.000  Thu Mar 06 2023 01:39:51 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2
                            host = mailsv | source = tutorialdata.zip:./mailsv/secure.log | sourcetype = secure-2
>  06/03/2023 01:39:51.000  Thu Mar 06 2023 01:39:51 mailsv1 sshd[2426]: Failed password for root from 89.106.20.218 port 1392 ssh2
                            host = mailsv | source = tutorialdata.zip:./mailsv/secure.log | sourcetype = secure-2
>  06/03/2023 01:39:51.000  Thu Mar 06 2023 01:39:51 mailsv1 sshd[1712]: Failed password for root from 89.106.20.218 port 1347 ssh2
                            host = mailsv | source = tutorialdata.zip:./mailsv/secure.log | sourcetype = secure-2
```