

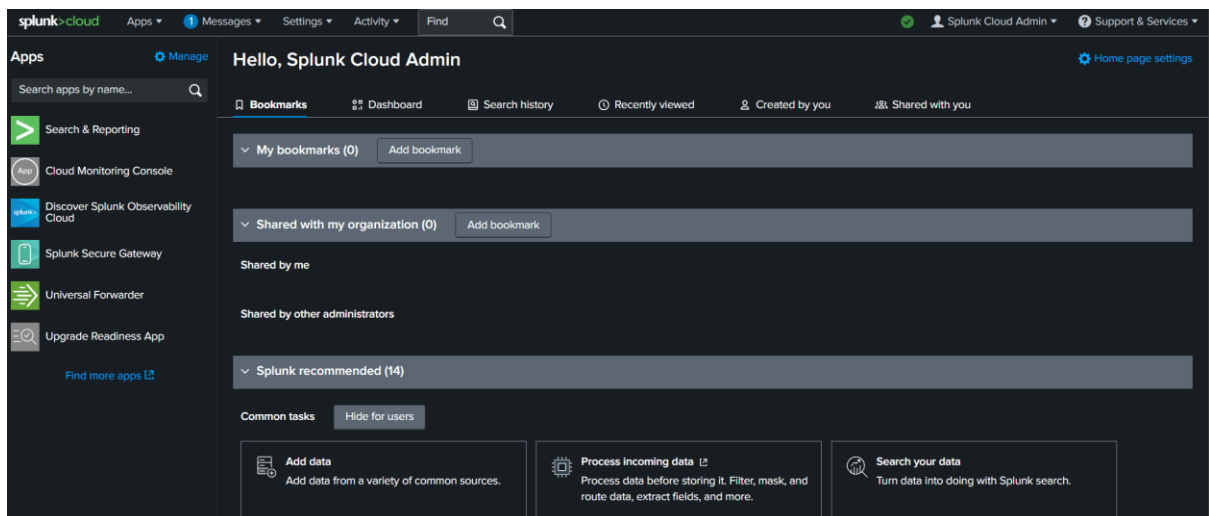
# Performing Queries in Splunk

## Project description

This simulation project puts the performer, **Maheswar Reddy Avula**, into the position of a security analyst for the e-commerce store Buttercup Games. Responsibilities include identifying whether there are any possible security issues with the mail server by exploring any failed SSH logins for the root account.

For the purpose of this project, the following prerequisites are first met:

1. A Splunk cloud accounts is created
2. A free Splunk cloud trial is activated
3. The project data is uploaded into Splunk
4. The Splunk Cloud interface is examined:

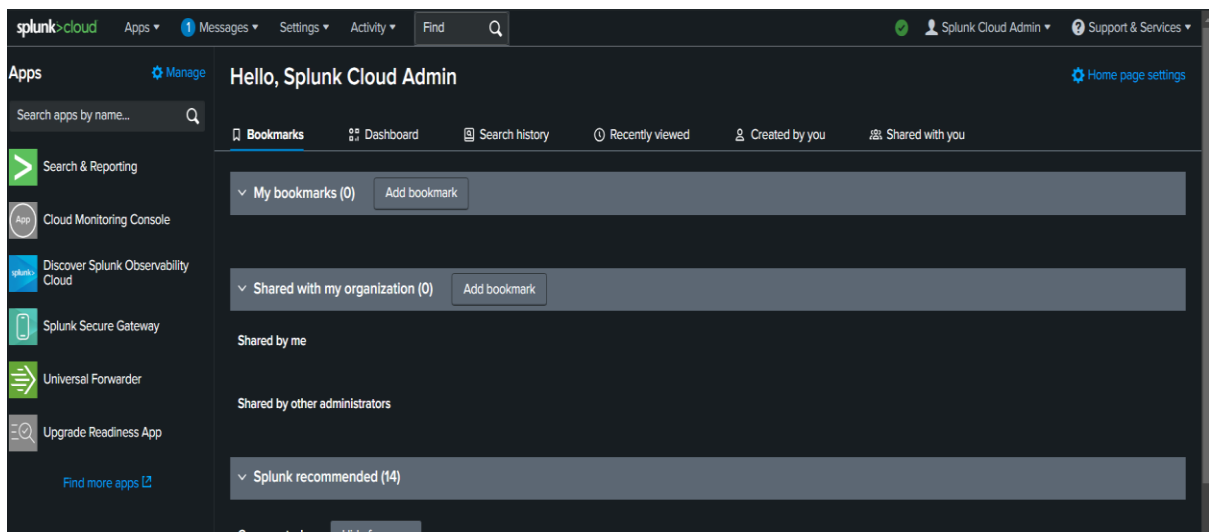


## Performing a basic search

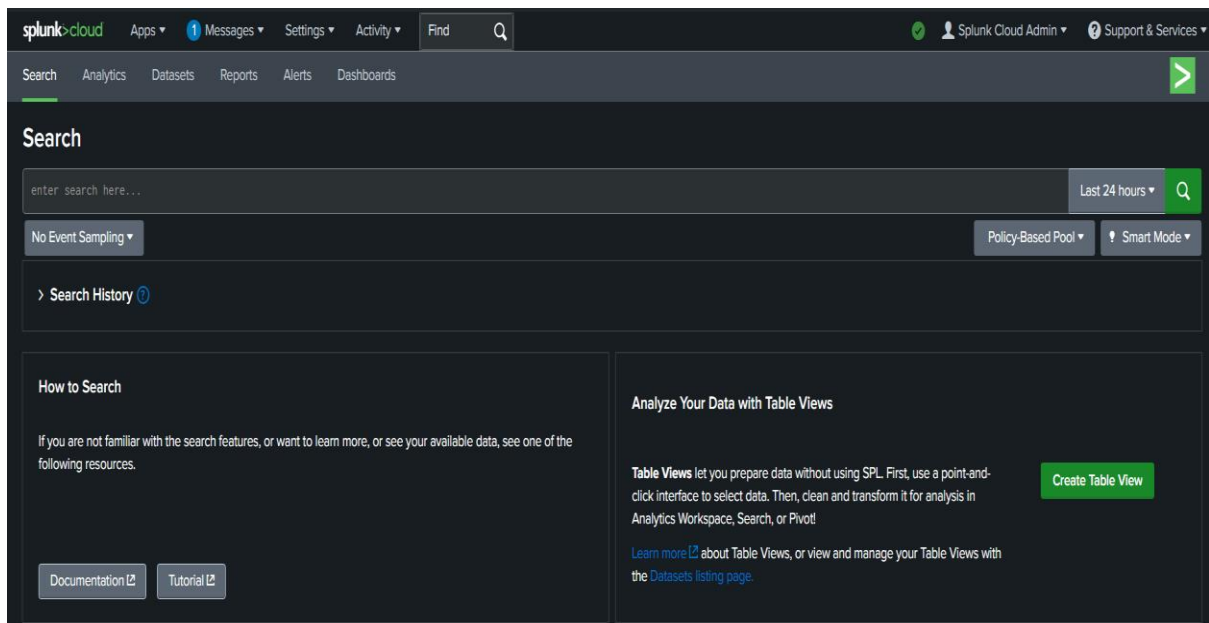
**Direction:** The analyst must perform a query to confirm that the data has been ingested, indexed, and is searchable.

The following steps are taken:

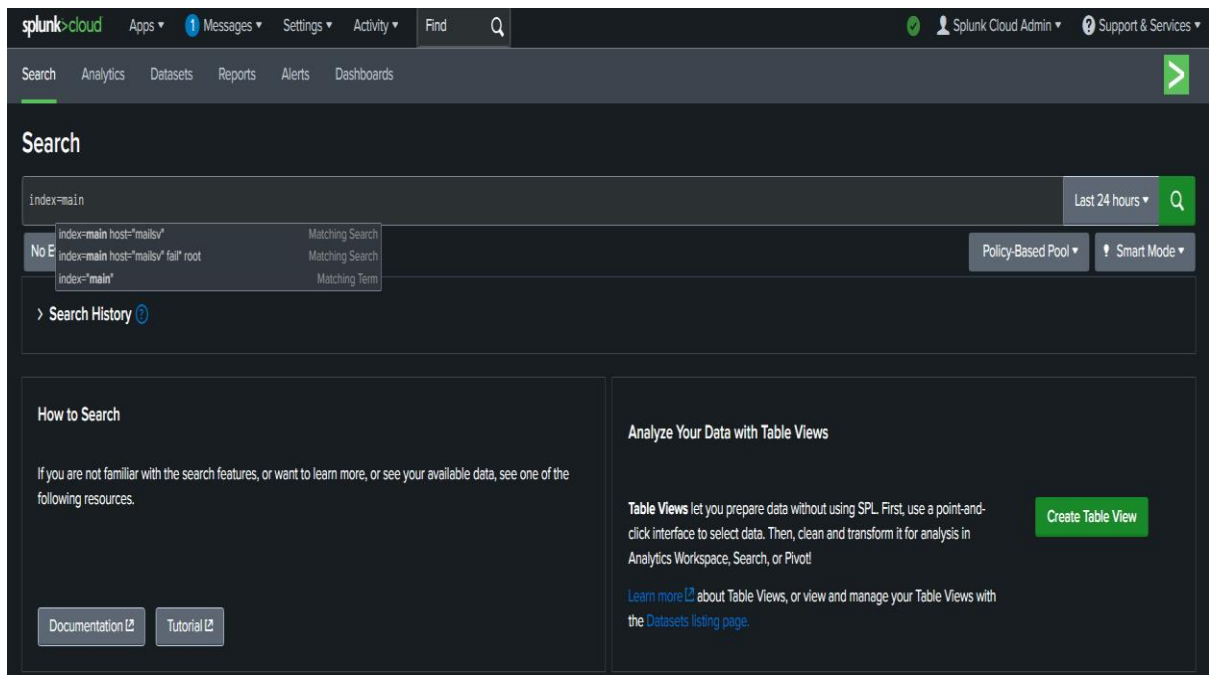
## 1. Navigate to Splunk Home, and open the **Search & Reporting** App.



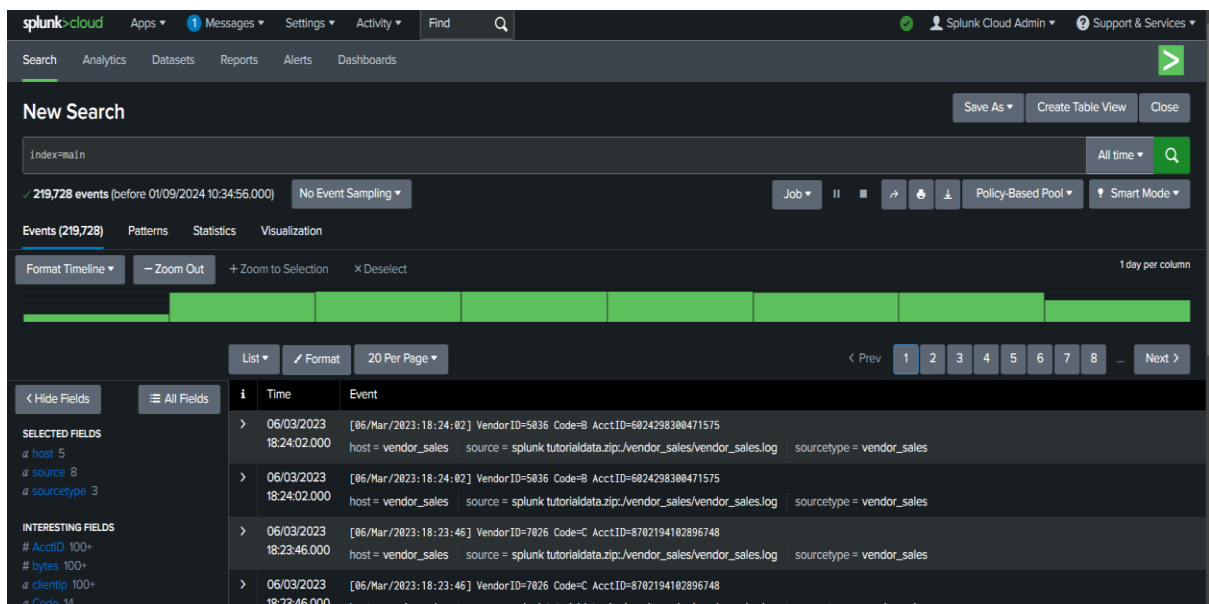
The search app opens as follows:



## 2. In the search bar, a search is performed as index=main as follows



It is observed that no results are shown. To overcome this, the search time period is defined as **All time** instead of **Last 24 hours**. The following results are shown:

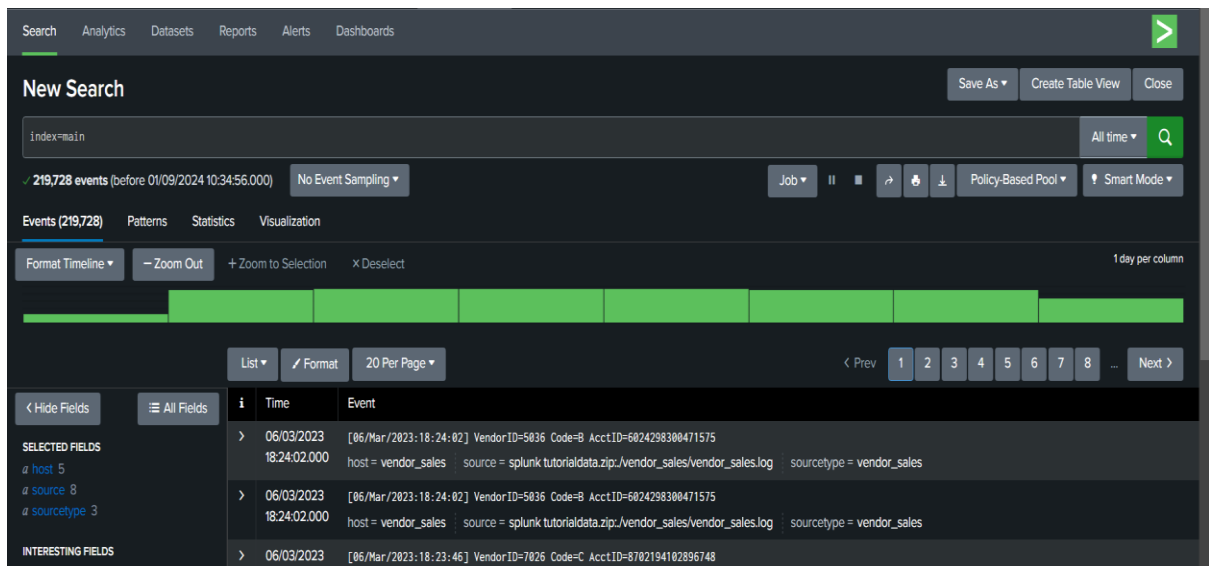


It is noted that there are 219,728 events for the index main.

## Evaluating the fields

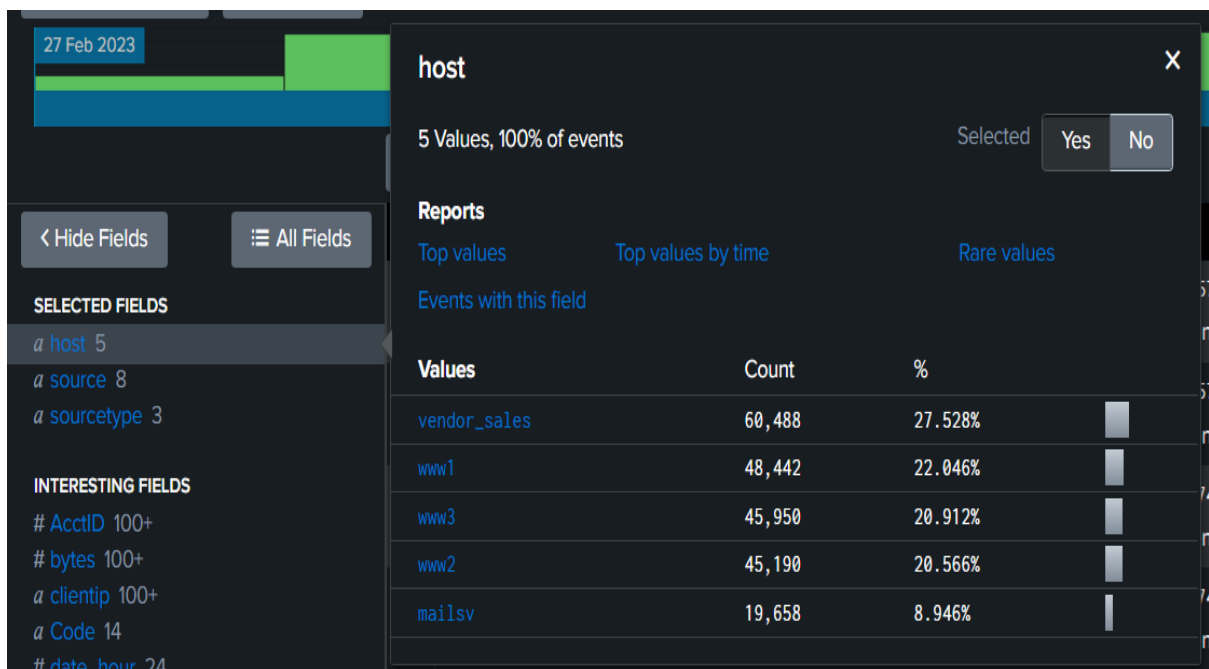
**Direction:** The analyst must examine the search results.

An overview of the results is seen as follows:



The following fields are examined:

- **host:** This field specifies the name of the network host from which the event originated. In this search, there are 5 hosts:



- **mailsv:** Buttercup Games' mail server.
- **ww1, ww2, ww3:** Buttercup Games' web applications.
- **vendor\_sales:** Information about Buttercup Games' retail sales.

**source:** This field indicates the file name from which the event originates. There are 8 sources.

**source**

8 Values, 100% of events

Selected

**Reports**

Top values      Top values by time      Rare values

Events with this field

Values	Count	%
splunk tutorialdata.zip:./vendor_sales/vendor_sales.log	60,488	27.528%
splunk tutorialdata.zip:./www1/access.log	27,256	12.404%
splunk tutorialdata.zip:./www3/access.log	25,984	11.826%
splunk tutorialdata.zip:./www2/access.log	25,824	11.753%
splunk tutorialdata.zip:./www1/secure.log	21,186	9.642%
splunk tutorialdata.zip:./www3/secure.log	19,966	9.087%
splunk tutorialdata.zip:./mailsv/secure.log	19,658	8.946%
splunk tutorialdata.zip:./www2/secure.log	19,366	8.814%

- **vendor\_sales.log:** contains information regarding Buttercup Games' retail sales.
- **access.log:** These contain information about access to the web applications ww1, ww2 and ww3.
- **secure.log:** These contain information regarding authentication and authorization attempts to the web applications ww1, ww2, ww3 and the mail server mailsv.

**sourcetype:** This determines how the data is formatted. 3 source types are examined:

**sourcetype**

3 Values, 100% of events

Selected

**Reports**

Top values      Top values by time      Rare values

Events with this field

Values	Count	%
secure-2	80,176	36.489%
access_combined_wcookie	79,064	35.983%
vendor_sales	60,488	27.528%

- secure2
- access\_combined\_wcookie
- vendor\_sales

## Narrowing the search

**Direction:** The analyst must narrow down the search to find failed SSH login events for the mail server.

To narrow down the search results, under **SELECTED FIELDS**, **host** -> **mailsv** is selected as follows:

The screenshot shows the Splunk Cloud interface. The search bar contains 'index=main'. Below the search bar, it indicates '219,728 events (before 01/09/2024 10:38:01.000)'. A modal window titled 'host' is open, showing a table of values for the 'host' field. The table has columns for 'Values', 'Count', and '%'. The values listed are 'vendor\_sales', 'www1', 'www3', 'www2', and 'mailsv'. The 'mailsv' value is highlighted, indicating it is selected. The modal also shows a 'Selected' column with 'Yes' and 'No' options.

Values	Count	%
vendor_sales	60,488	27.528%
www1	48,442	22.046%
www3	45,950	20.912%
www2	45,190	20.566%
mailsv	19,658	8.946%

Results are narrowed down as follows:

The screenshot shows the Splunk Cloud interface with the search query 'index=main host=mailsv'. It indicates '19,658 events (before 01/09/2024 10:38:28.000)'. The search results are displayed in a list view. The results show failed SSH login attempts for the 'mailsv' host. The results are as follows:

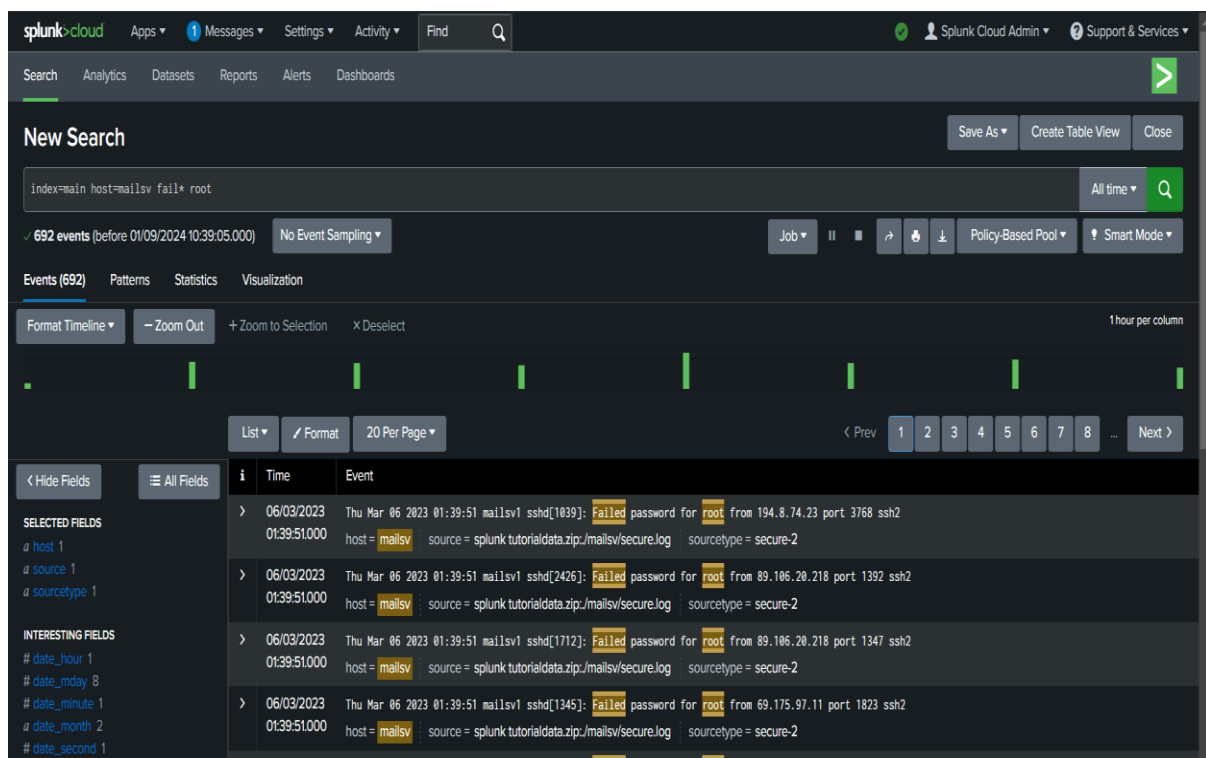
Time	Event
06/03/2023 01:39:51.000	Thu Mar 06 2023 01:39:51 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2
06/03/2023 01:39:51.000	Thu Mar 06 2023 01:39:51 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2
06/03/2023 01:39:51.000	Thu Mar 06 2023 01:39:51 mailsv1 sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2
06/03/2023 01:39:51.000	Thu Mar 06 2023 01:39:51 mailsv1 sshd[21881]: pam_unix(sshd:session): session closed for user nsharpe by (uid=0)

It is observed that the search results have been narrowed down from 219,864 to 19,658.

## Searching for a failed login for root

**Direction:** The analyst must further narrow the search down to find failed SSH login events.

To accomplish this, the keyword **fail\*** (the **\*** **wildcard** searches for all possible text strings starting with the word fail such as failed, failure etc.) and **root**. The following results are returned:



The screenshot displays the Splunk Cloud interface with a search query `index=main host=mailsv fail* root` executed. The results show 692 events. The interface includes a search bar, navigation tabs (Search, Analytics, Datasets, Reports, Alerts, Dashboards), and a results table. The table lists events with timestamps, hostnames, and details of failed SSH login attempts for the root user.

Time	Event
06/03/2023 01:39:51	Thu Mar 06 2023 01:39:51 mailsv1 sshd[1839]: Failed password for root from 194.8.74.23 port 3768 ssh2
06/03/2023 01:39:51	Thu Mar 06 2023 01:39:51 mailsv1 sshd[2426]: Failed password for root from 89.106.20.218 port 1392 ssh2
06/03/2023 01:39:51	Thu Mar 06 2023 01:39:51 mailsv1 sshd[1712]: Failed password for root from 89.106.20.218 port 1347 ssh2
06/03/2023 01:39:51	Thu Mar 06 2023 01:39:51 mailsv1 sshd[1345]: Failed password for root from 69.175.97.11 port 1823 ssh2

The events tally has been reduced from 19,829 to 692. The events are then examined and reported to the Buttercup Games Security team.

## Summary

Failed SSH login events are successfully searched in the indexed data using appropriate SPLunk queries and findings are reported to the Buttercup Games security team. All tasks were successfully completed in accordance with the directions given by the organization.