Case Study:

Perform a Query with Splunk

Skills Acquired:

By using Splunk Cloud to perform a search and investigation, I was able to:

- Upload sample log data
- Search through indexed data
- Evaluate search results
- Identify different data sources
- Locate failed SSH login(s) for the root account

Scenario:

You are a security analyst working at the e-commerce store Buttercup Games. You've been tasked with identifying whether there are any possible security issues with the mail server. To do so, you must explore any failed SSH logins for the root account.

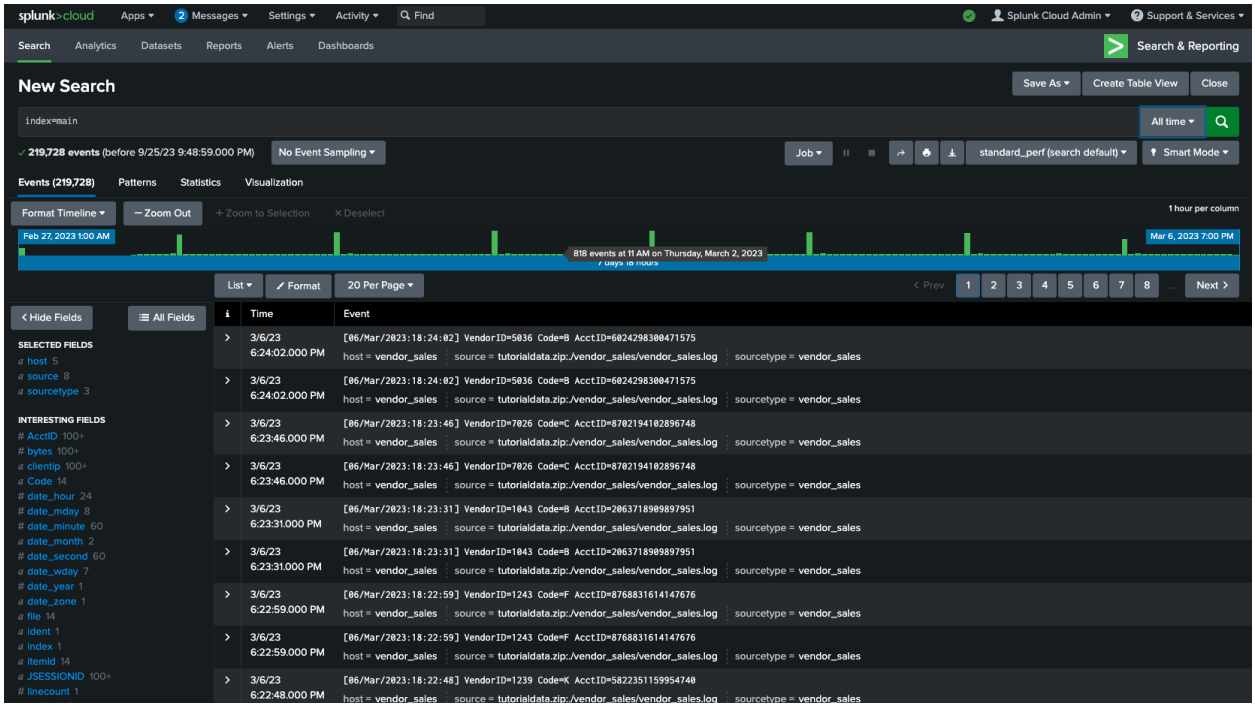
Task 1 Upload Data into Splunk

Download tutorialdata.zip file and upload it to Splunk.

Task 2 Perform a Basic Search

Now that you've uploaded the data into Splunk, perform your first query to confirm that the data has been ingested, indexed, and is searchable. Follow these steps to perform a query:

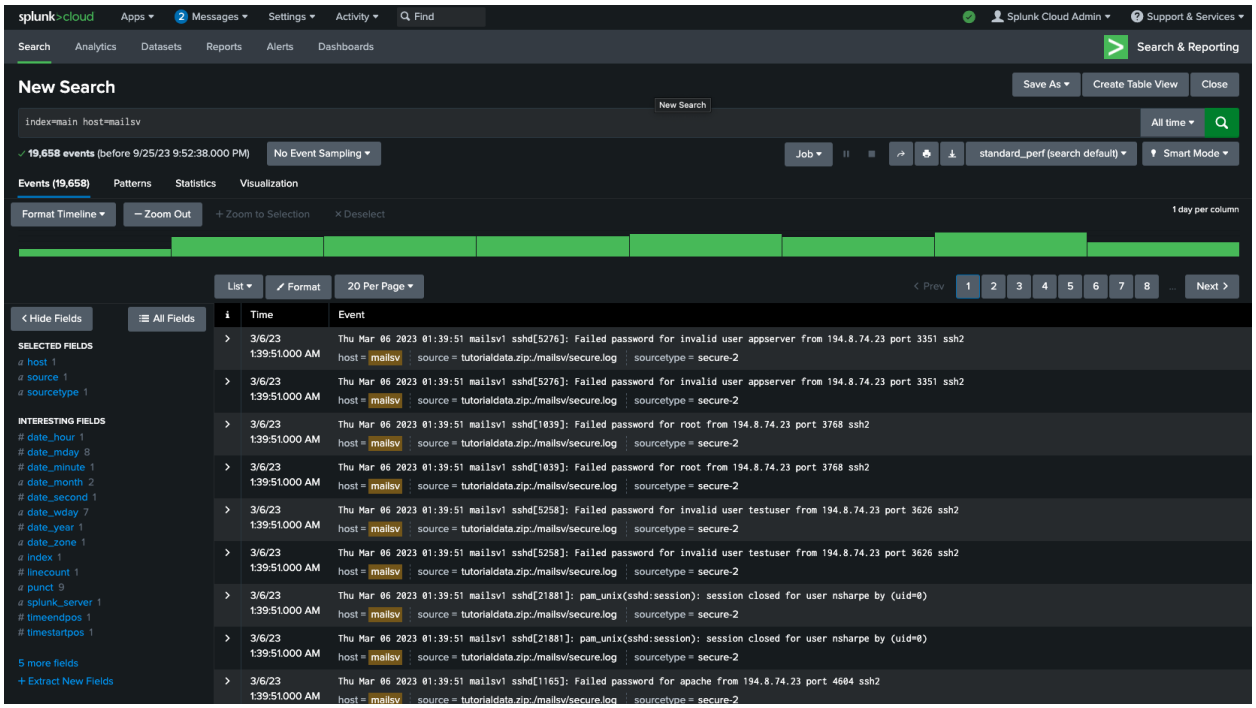
1. Navigate to Splunk Home. (To return to Splunk Home, click the Splunk Cloud logo on the Splunk Cloud page.)
2. Click Search & Reporting. You may close any pop ups that appear.
3. In the search bar, enter your search query: **index=main** This search term specifies the index. An index is a repository for data. Here, the index is a single dataset containing events from an index named main.
4. Select All Time from the time range dropdown to search for all the events across all time.
5. Click the search button. Note that the search button is represented by the magnifying glass icon. Your search should retrieve thousands of events.



Task 3 Narrow Your Search

Because you've been tasked with exploring any failed SSH logins for the root account on the mail server, you'll need to narrow the search results for events from the mail server.

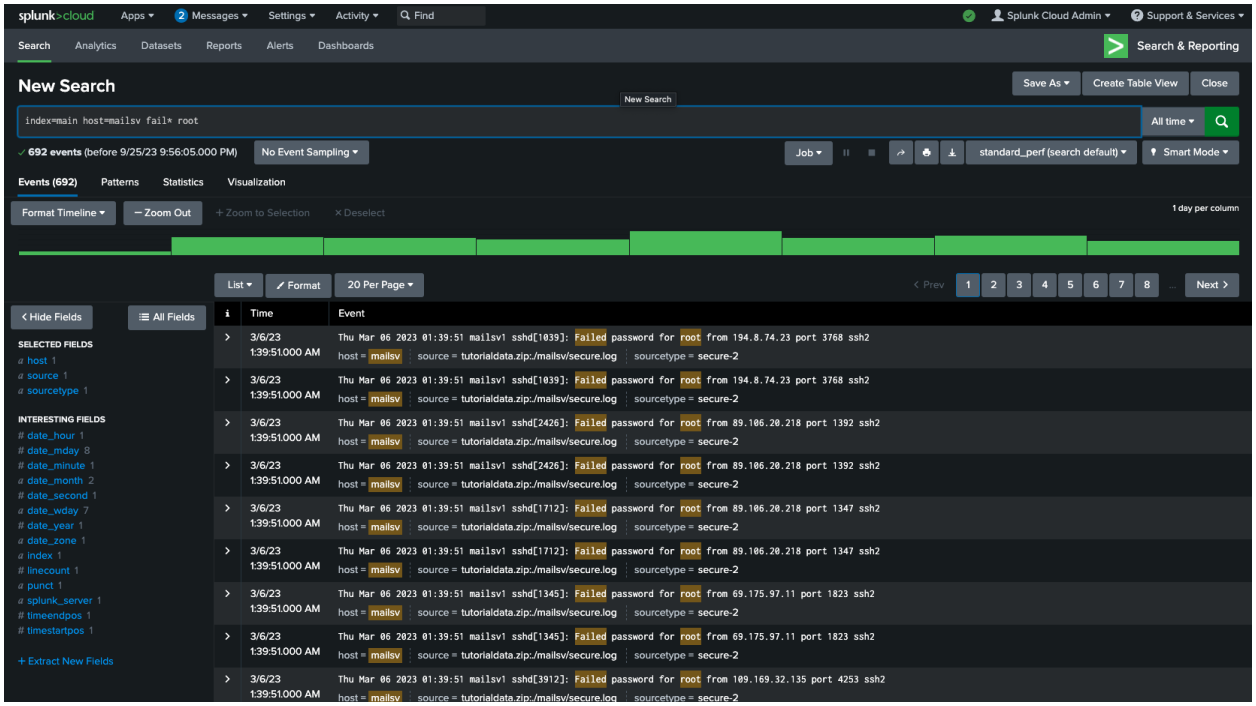
Under SELECTED FIELDS, click host and click mailsv.



Task 4 Search for a Failed Login for Root

Now that you've narrowed your search results to events generated by the mail server, continue to narrow the search to locate any failed SSH logins for the root account.

1. Clear the search bar.
2. Enter **index=main host=mailsv fail* root** into the search bar.
3. Click search.



Questions

1. How many events are contained in the main index across all time?

   Over 100,000

2. Which field identifies the name of a network device or system from which an event originates?

   Host

3. Which hosts used by Buttercup Games contain log information relevant to financial transactions?

   Vendor_sales

4. How many failed SSH logins are there for the root account on the mail server?

   More than 100