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.

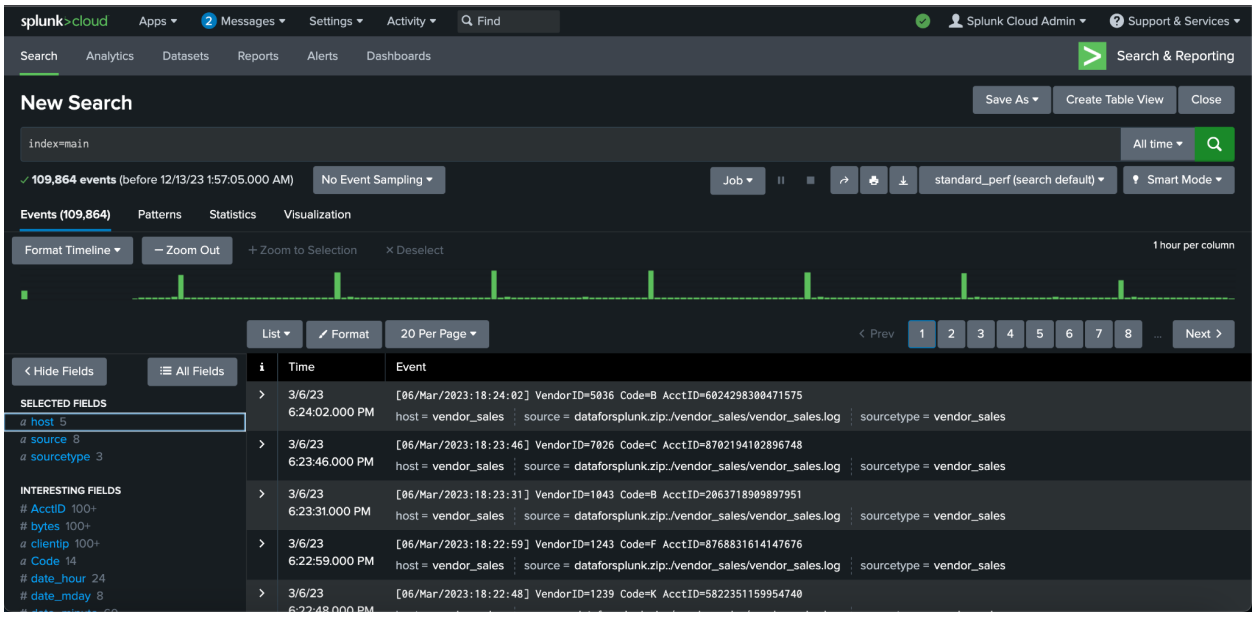
Directions:

1. If you haven't already, download the data file from Step 1: tutorialdata.zip. Click the link then click the download icon. Do not uncompress the file.
2. Navigate to Splunk Home from your Splunk Cloud free trial instance. You might need to log in again using your credentials from Step 3.
3. On the Splunk bar, click Settings. Then click the Add Data icon.
4. Click Upload.
5. Click the Select File button.
6. Upload the **tutorialdata.zip** file, and click Open.
7. Click the Next button to continue to Input Settings.
8. By the Host section, select Segment in path and enter 1 as the segment number.

Click the Review button and review the details of the upload before you submit. The details should be as follows:

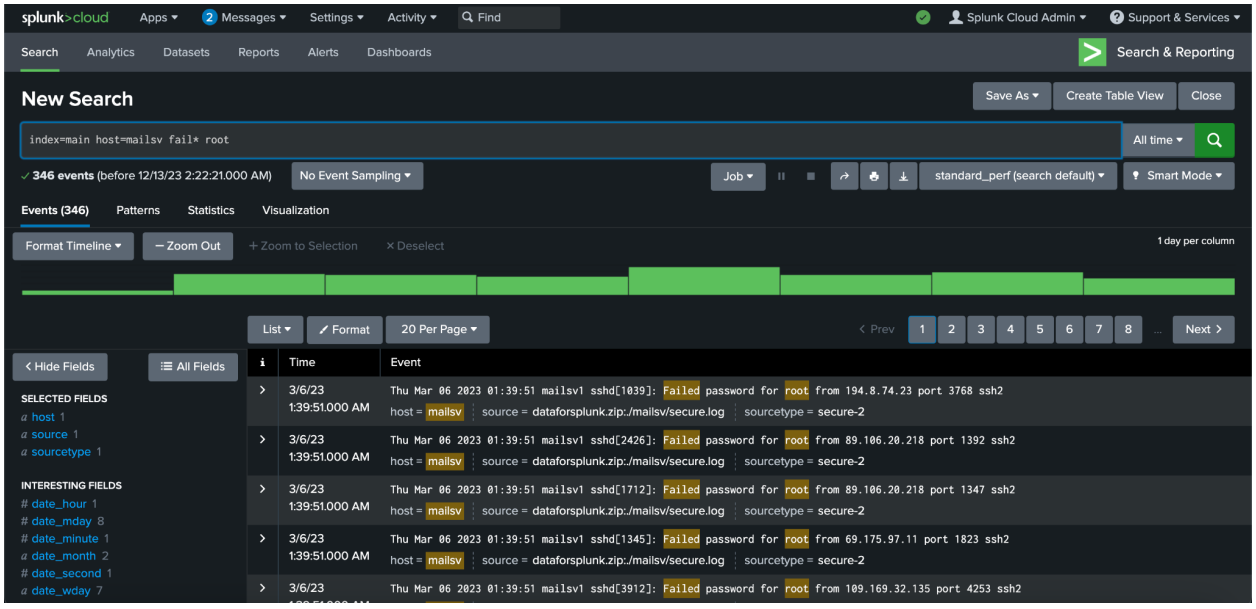
Input Type: Uploaded File
File Name: tutorialdata.zip
Source Type: Automatic
Host: Source path segment number: 1

9. Index: Default
10. Click Submit. Once Splunk has ingested the data, you will receive confirmation that the file was successfully uploaded.



*Over 100,000 events in the main index!

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.
Notice that a new term has been added to the search bar: **`index=main host=mailsv`**.
The search results have narrowed to over 9000 events that are generated by the mail server.



Key takeaways

In this activity, we used Splunk Cloud to perform a search and investigation. Using Splunk Cloud, we were 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