Perform a query with Splunk

Overview

SIEM, such as Splunk, is an important part of a security analyst's toolbox because it provides a platform for storing, analyzing, and reporting on data from different sources. The Splunk's querying language, called Search Processing Language (SPL), includes the use of pipes and wildcards. In addition, effective search helps us efficiently identify patterns, trends, and anomalies within data.

Scenario

As a security analyst working at the e-commerce store Buttercup Games. I was tasked with identifying any possible security issues with the mail server. To do so, I had to explore any failed SSH logins for the root account.

First Steps

1. Login to Splunk.
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.
    a. Click the Review button and review the details of the upload before you submit. The details should be as follows:
        i. Input Type: Uploaded File
        ii. File Name: tutorialdata.zip

iii. Source Type: Automatic

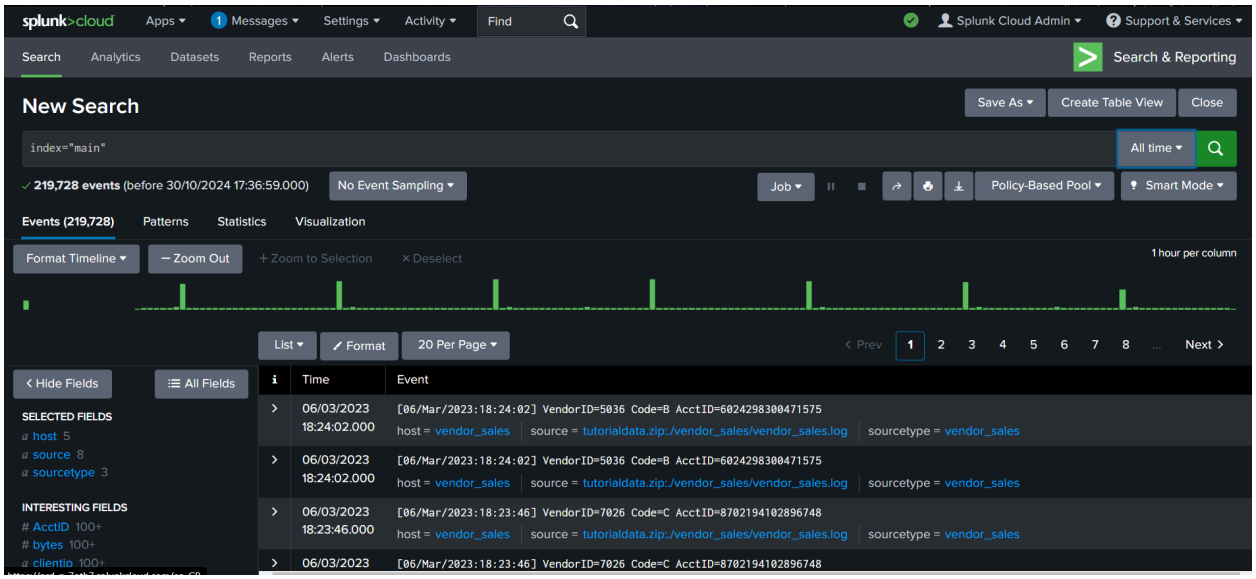
iv. Host: Source path segment number: 1

v. Index: Default

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

Task 1. View all the events across all time.

1. I navigated to Splunk Home.
2. Clicked Search & Reporting.
3. In the search bar, I entered my search query: index="main".
4. Then select "All Time" from the time range dropdown to search for all the events across all time.



Task 2. Evaluate the fields.

When Splunk indexes data, it attaches fields to each event. These fields become part of the searchable index event data.

I examined the field values by clicking on the field under SELECTED FIELDS. I observed the following labels in the result of the search:

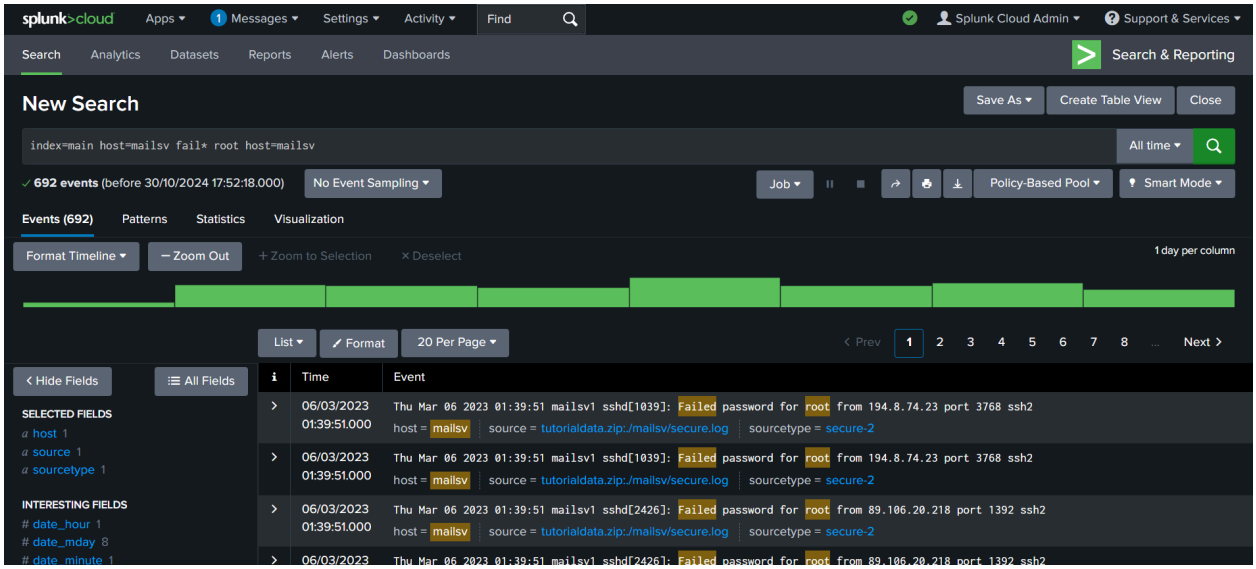
- **host**: The host field specifies the name of the network host from which the event originated. In this search there are five hosts:

    - `mailsv` - Buttercup Games' mail server. Examine events generated from this host.
    - `www1` - This is one of Buttercup Games' web applications.
    - `www2` - This is one of Buttercup Games' web applications.
    - `www3` - This is one of Buttercup Games' web applications.
    - `vendor_sales` - Information about Buttercup Games' retail sales.
- **source**: The source field indicates the file name from which the event originates. You should identify eight sources. Notice `/mailsv/secure.log`, which is a log file that contains information related to authentication and authorization attempts on the mail server.
- **sourcetype**: The sourcetype determines how data is formatted.

Task 3. Search for failed login for root.

Next I clicked on "host" under SELECTED FIELDS, then clicked on "`mailsv`."

I entered "`index=main host=mailsv fail* root`" into the search bar. This search expanded on the previous search by searching for the keyword "fail*" using a wildcard to find terms like "failure" and "failed." Additionally, I searched for any event containing the term "root."



As of October 30th, 2024, there have been 692 failed SSH logins for the root account on the mail server.

Summary

In this activity, I used Splunk Cloud to perform a search and investigation. Using Splunk Cloud, I was able to:

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