Activity Overview

In this activity, you'll be introduced to the Splunk platform. Then, you'll use Splunk Cloud to upload data, perform basic searches on the data, and answer a series of questions. Follow the instructions in the Follow-along guide for Splunk sign-up to complete the following before you begin using Splunk:

- Create a Splunk account
- Activate a free trial of Splunk Cloud
- Upload data into Splunk Cloud

Please note that this activity is optional and will not affect your completion of the course. So far, you've learned that SIEM tools, such as Splunk, are an important part of a security analyst's toolbox because they provide a platform for storing, analyzing, and reporting on data from different sources. You also explored some basic searches using Splunk's querying language, called Search Processing Language (SPL), which included the use of pipes and wildcards.
Creating effective searches is an important skill because it enables you to quickly and accurately find the information you are looking for within a large amount of data. Quick and accurate searching is especially useful during incident response, because you might need to swiftly identify and address a security incident. Effective search techniques also help you efficiently identify patterns, trends, and anomalies within data.

Scenario

Review the following scenario. Then complete the step-by-step instructions.
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.

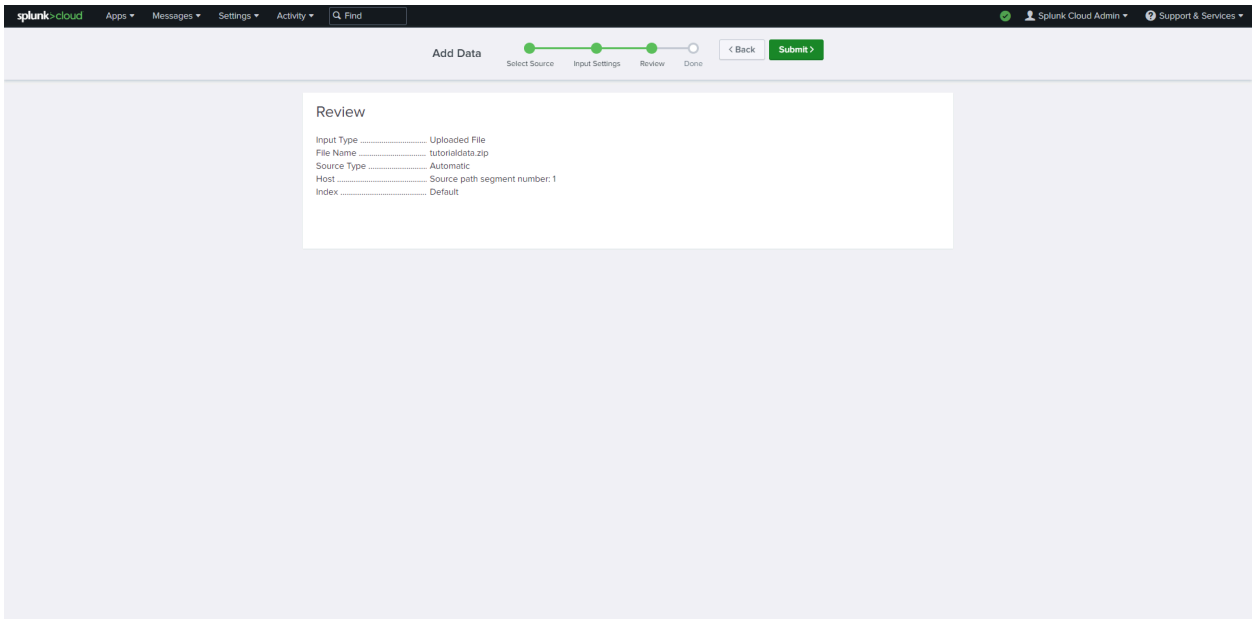
The following are the details of the data in a zipped file which you will upload it into Splunk:

- `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.

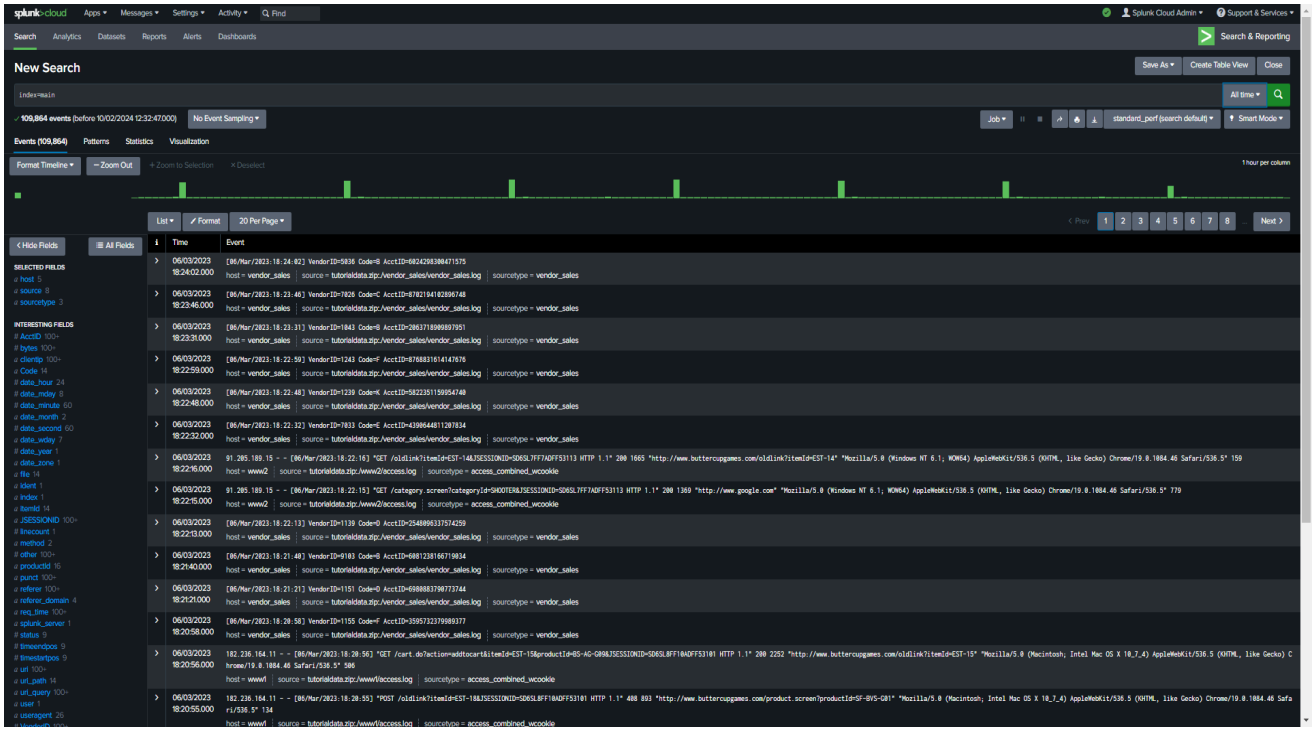
vendor_sales - Information about Buttercup Games' retail sales.

Step by Step

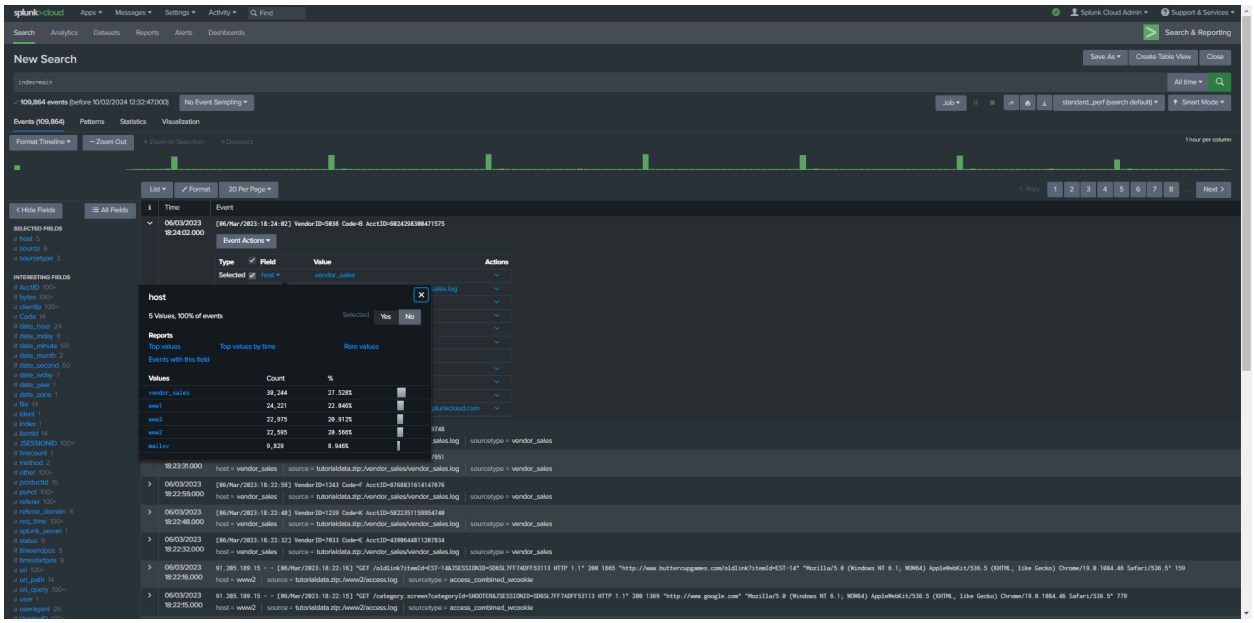
1. Login/signup to Splunk.
2. Add Data on the Splunk bar.
3. Upload data into Splunk.
4. Select file and upload `tutorialdata.zip`



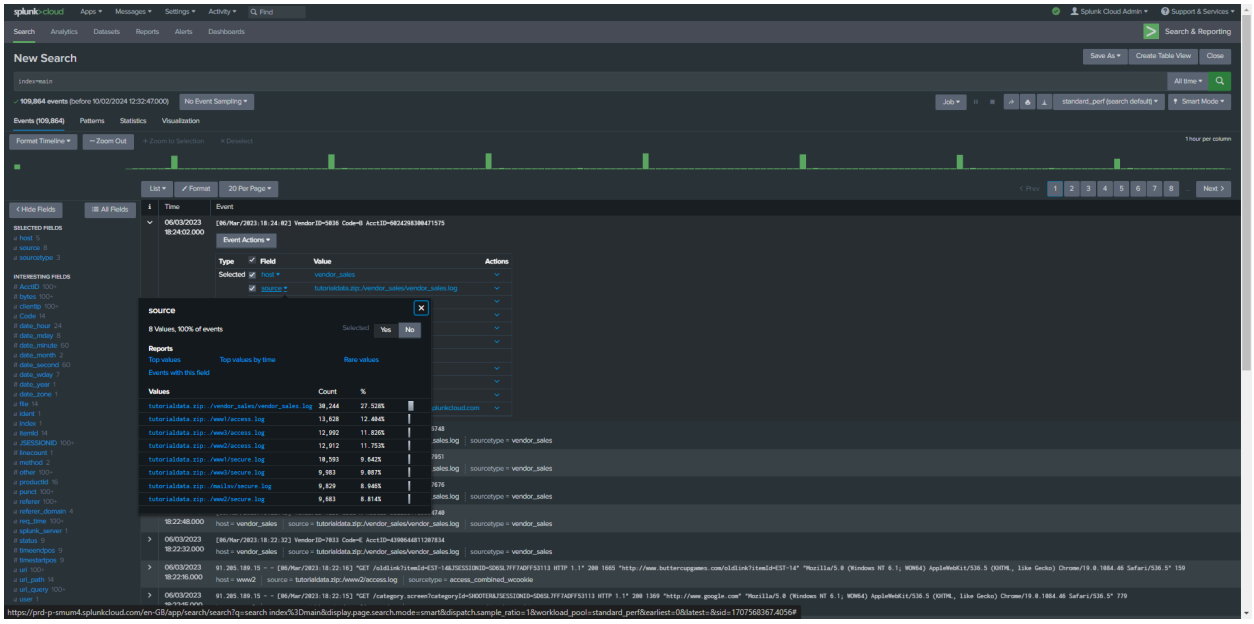
5. Navigate to Search and Reporting tab, type on the search bar `index=main` to view repository for data and select `All time` to view all the events across all time.



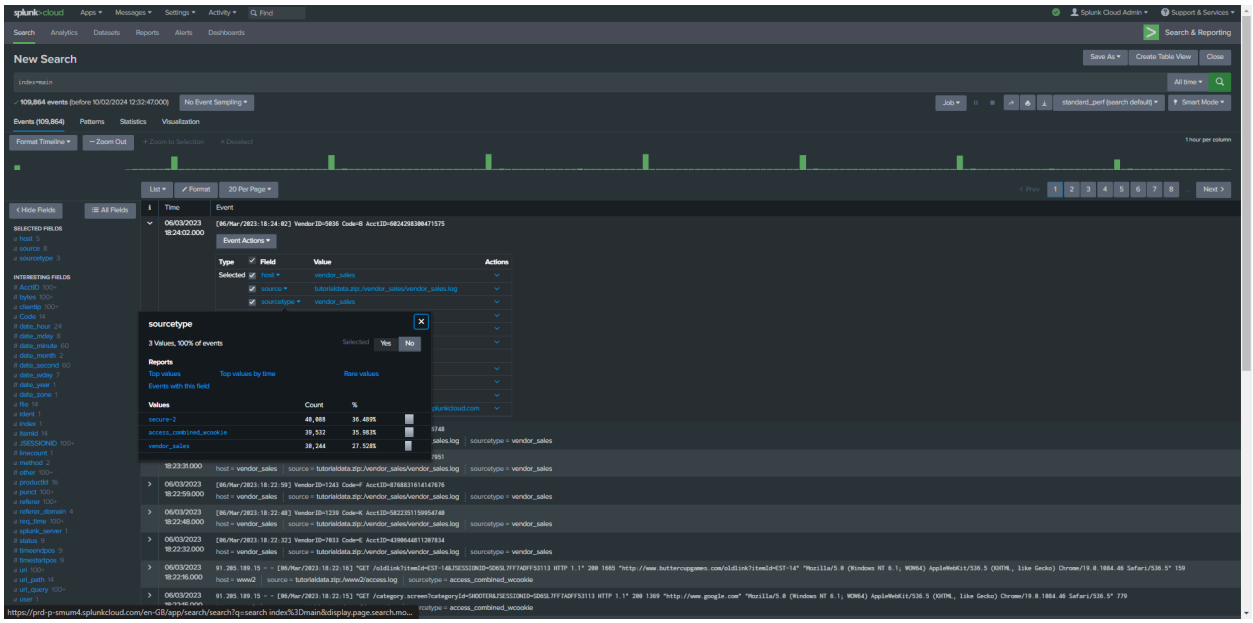
6. Let's have a look at three common components: `host`, `source`, `sourcetype`.
    - Host: Specifies the device or system that generated the event.



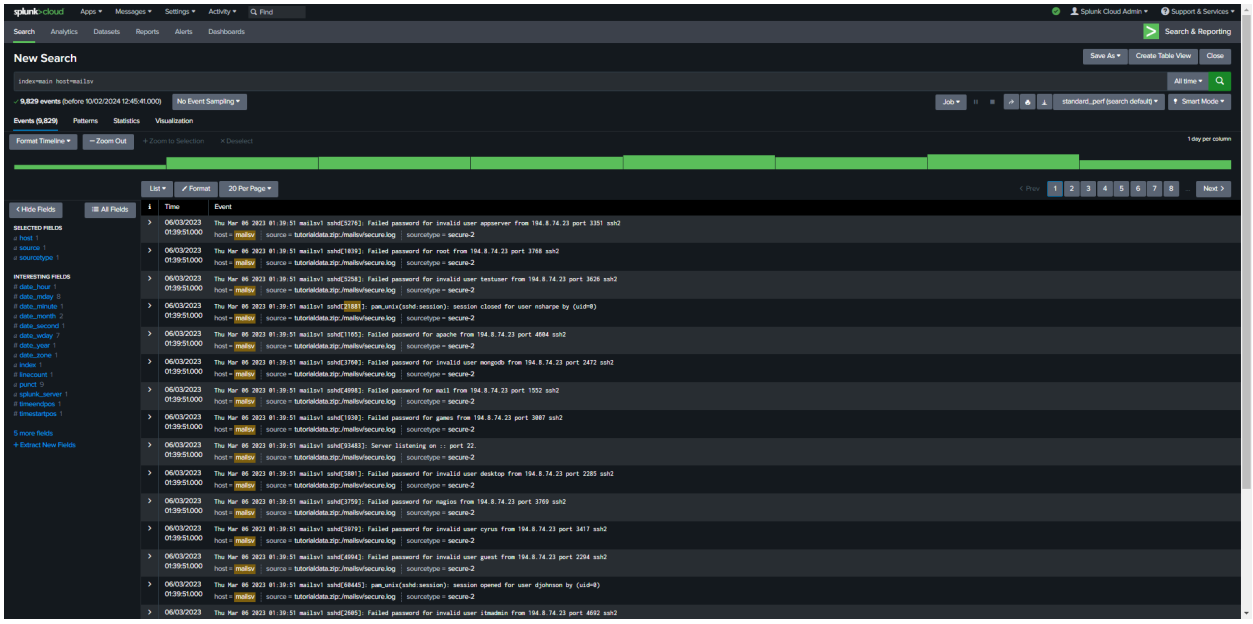
- Source: Indicates the original location of the event data within a specific device or system.



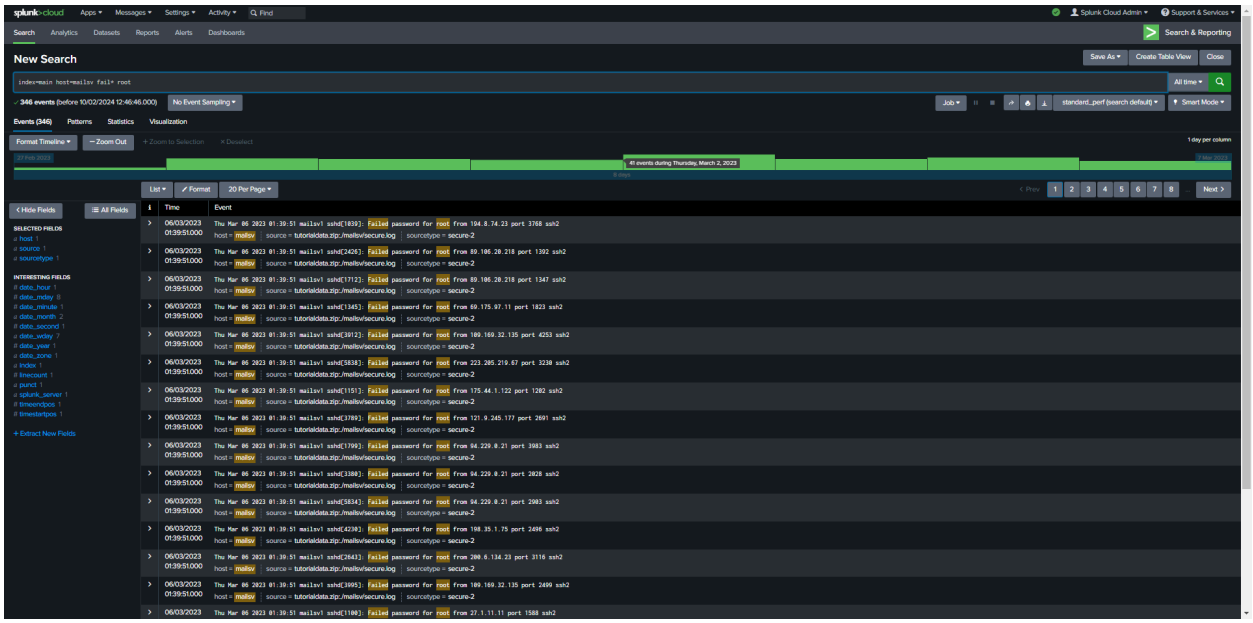
- Sourcetype: Defines the format and structure of the event data. It tells Splunk how to parse and interpret the information.



7. On the mail server, we have to explore any failed SSH logins for the root account. To do this, I wrote on the search bar: `index=main host=mailsv' to list over 9000 events that are generated by the mail server.



8. Finally, let's Search for a failed login for root. On the search bar, enter `index=main host=mailsv fail* root`. This tells Splunk to expand the search term to find other terms that contain the word `fail` such as `failure`, `failed`, etc. In addition, the keyword `root` searches for any event that contains the term `root`.



9. Investigation:
    - There are over 100,000 events that are contained in the main index across `all time`.
    - The `host` field specifies the name of a host, such as a network device or other system, from which an event originates.
    - From the scenario, The `vendor_sales` host provides information about Buttercup Games' retail sales, such as the number of products sold.
    - As of February 11th, 2024, there have been 346 failed SSH logins for the root account on the mail server.