Perform a Query with Splunk

Scenario

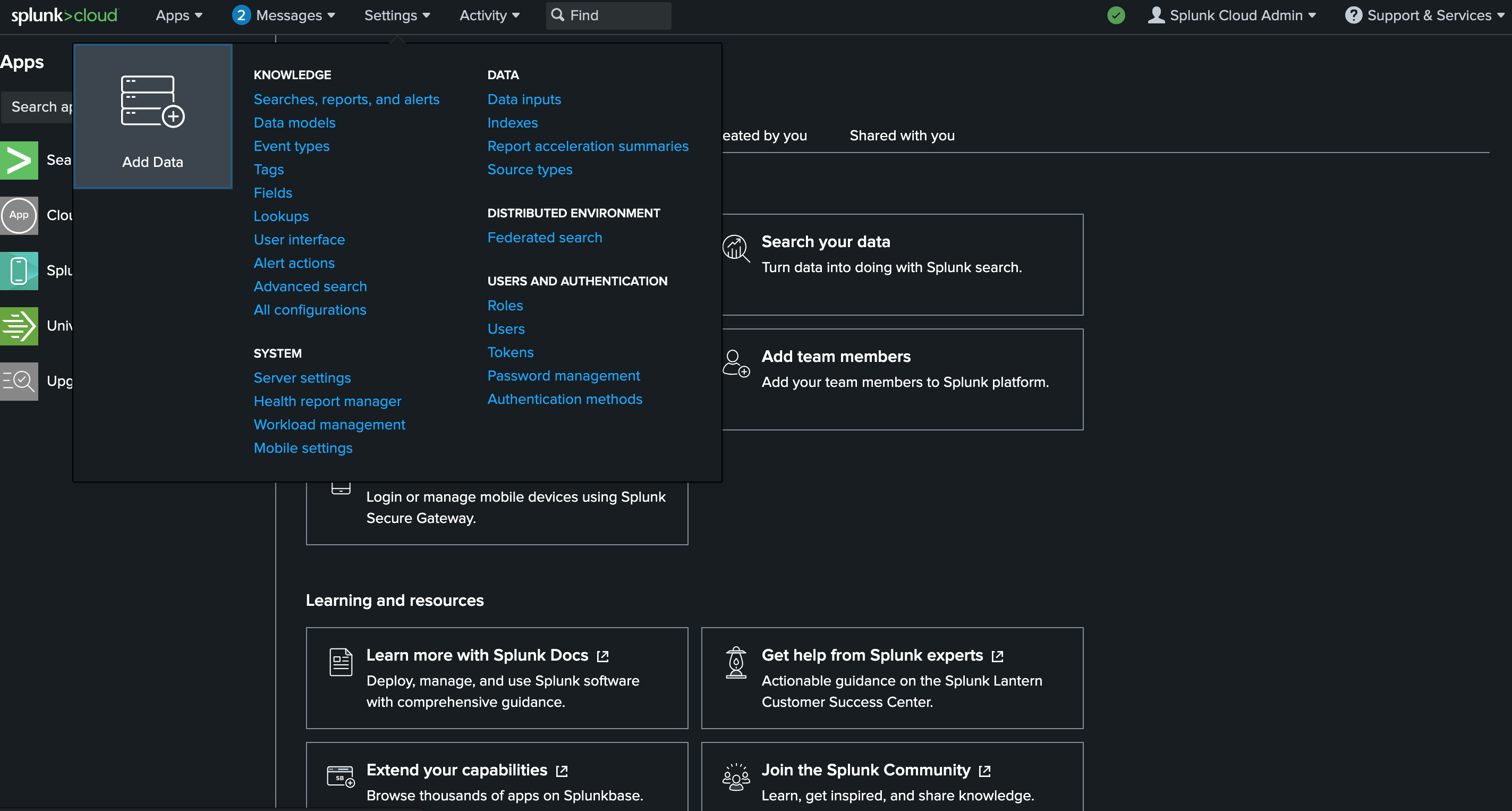
You are a security analyst working at the e-commerce store Buttercup Games. You've been tasked with identifying whether there are any possible security issues with the mail server. To do so, you must explore any failed SSH logins for the root account.

Project Description

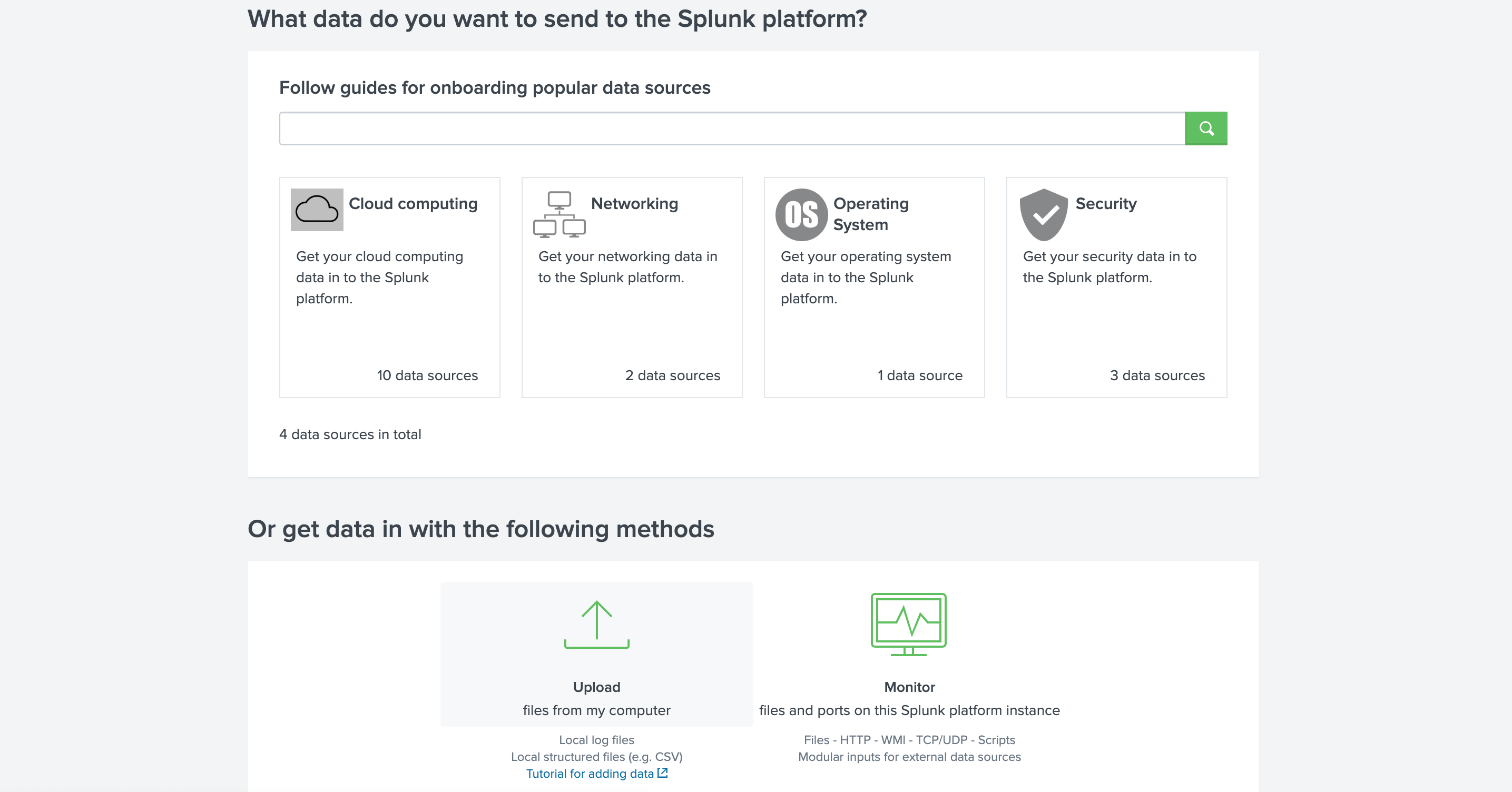
Creating effective searches is an important skill because it enables you to quickly and accurately find the information you are looking for within a large amount of data. Quick and accurate searching is especially useful during incident response, because you might need to swiftly identify and address a security incident. Effective search techniques also help you efficiently identify patterns, trends, and anomalies within data.

Upload Data to Splunk:

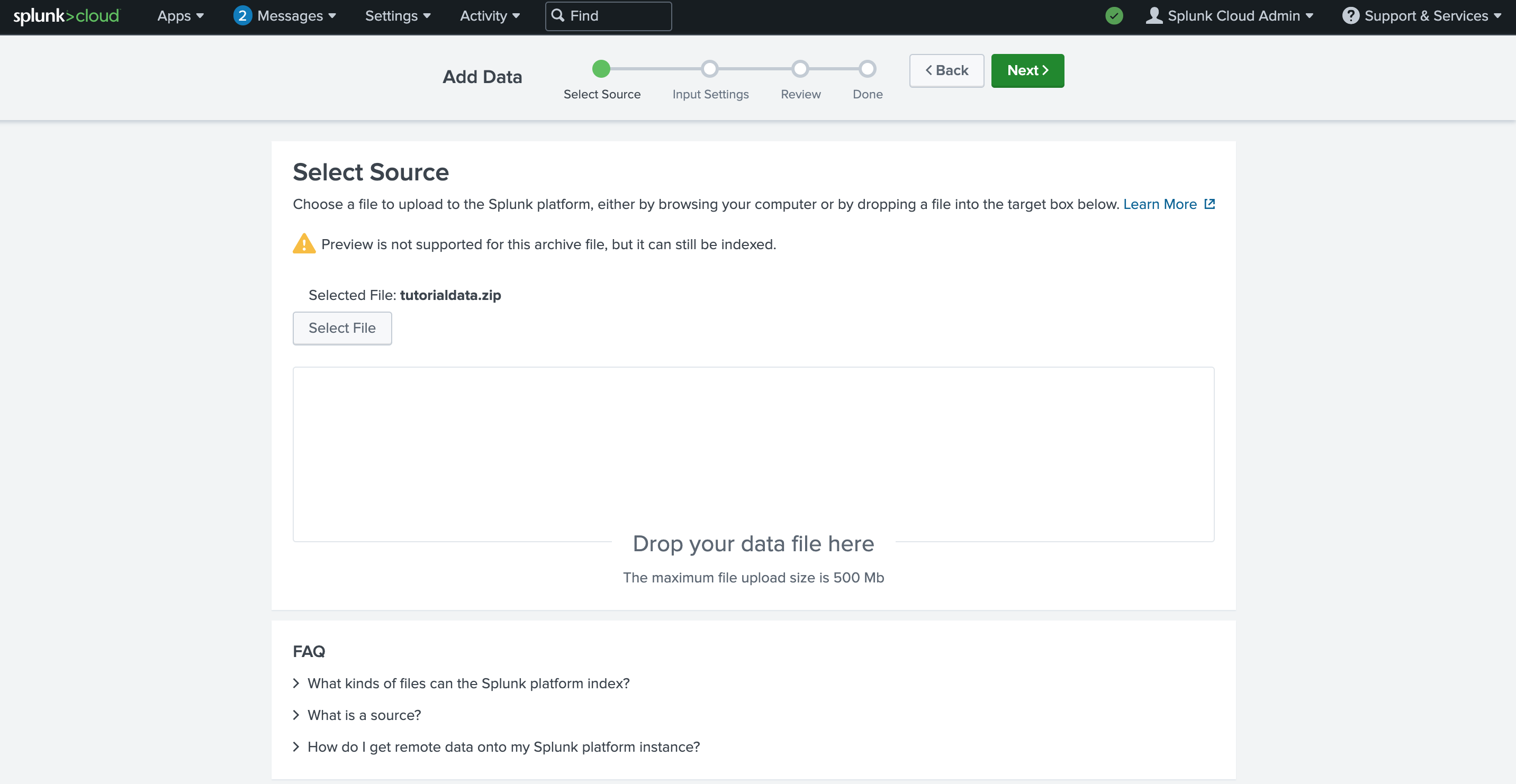
* Navigate to Splunk Home from your Splunk Cloud free trial instance. You might need to log in again using your credentials from Step 3.
* On the Splunk bar, click Settings. Then click the Add Data icon.



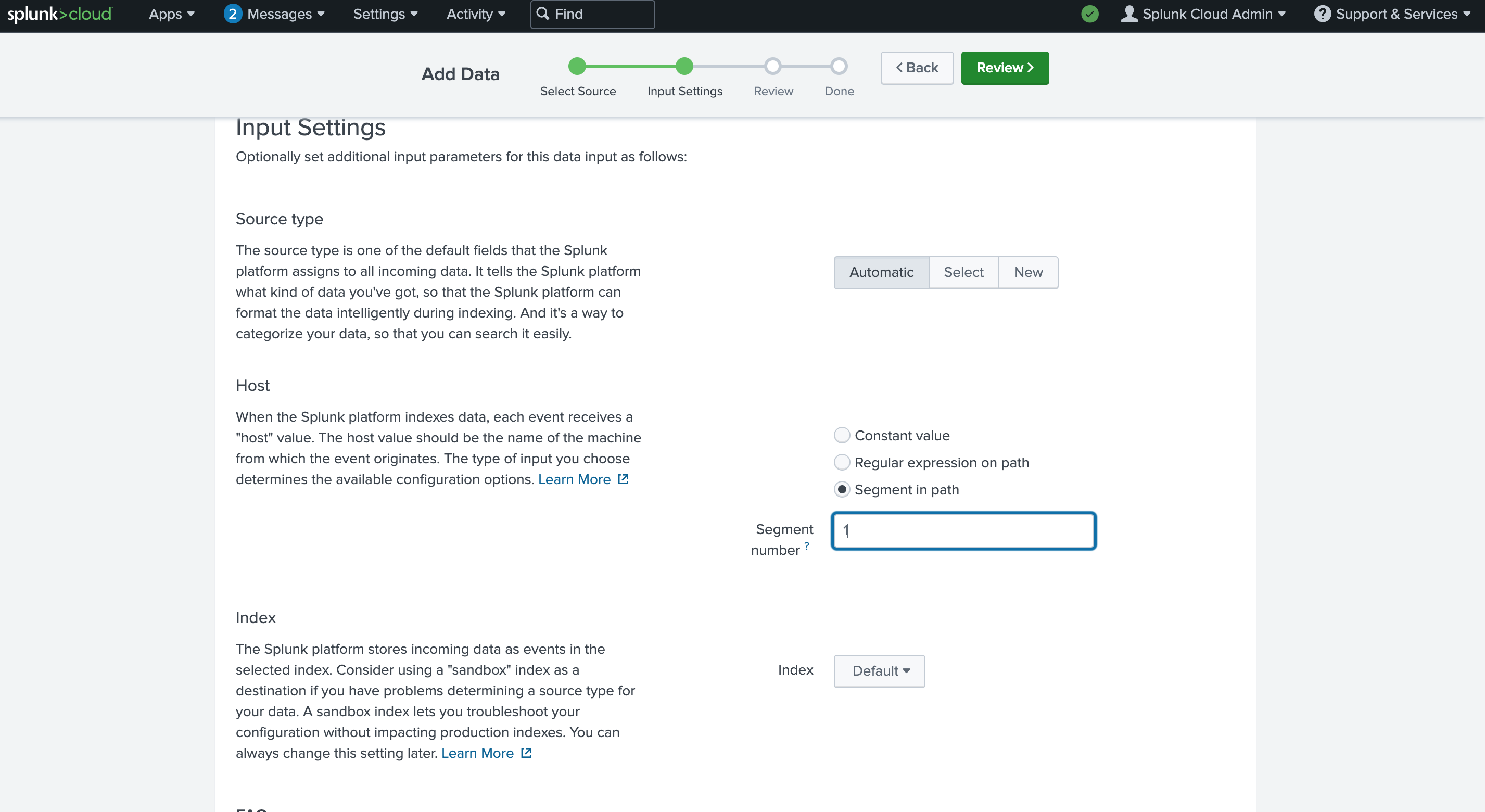
* Click Upload.



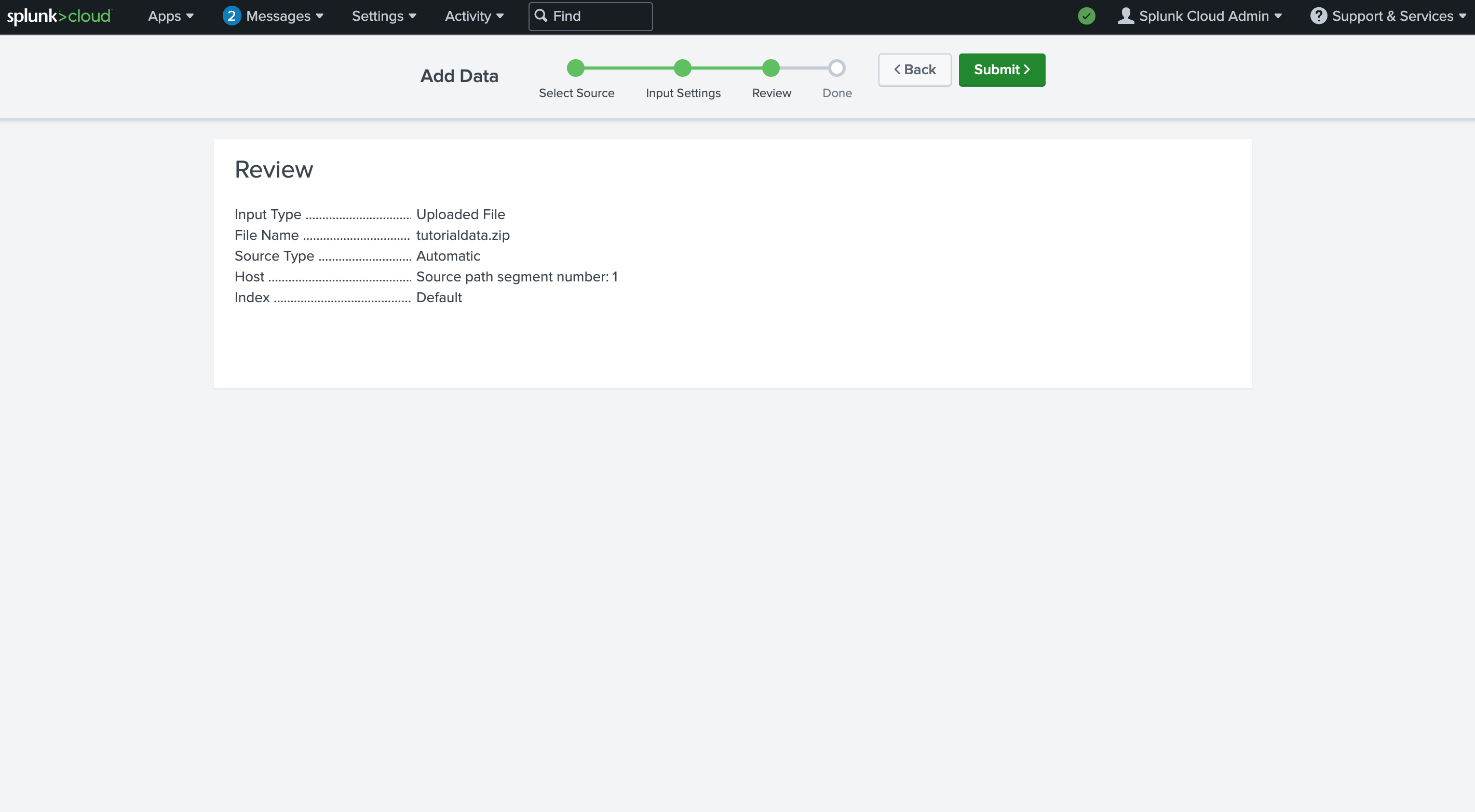
* Click the Select File button.
* Upload the tutorialdata.zip file, and click Open.



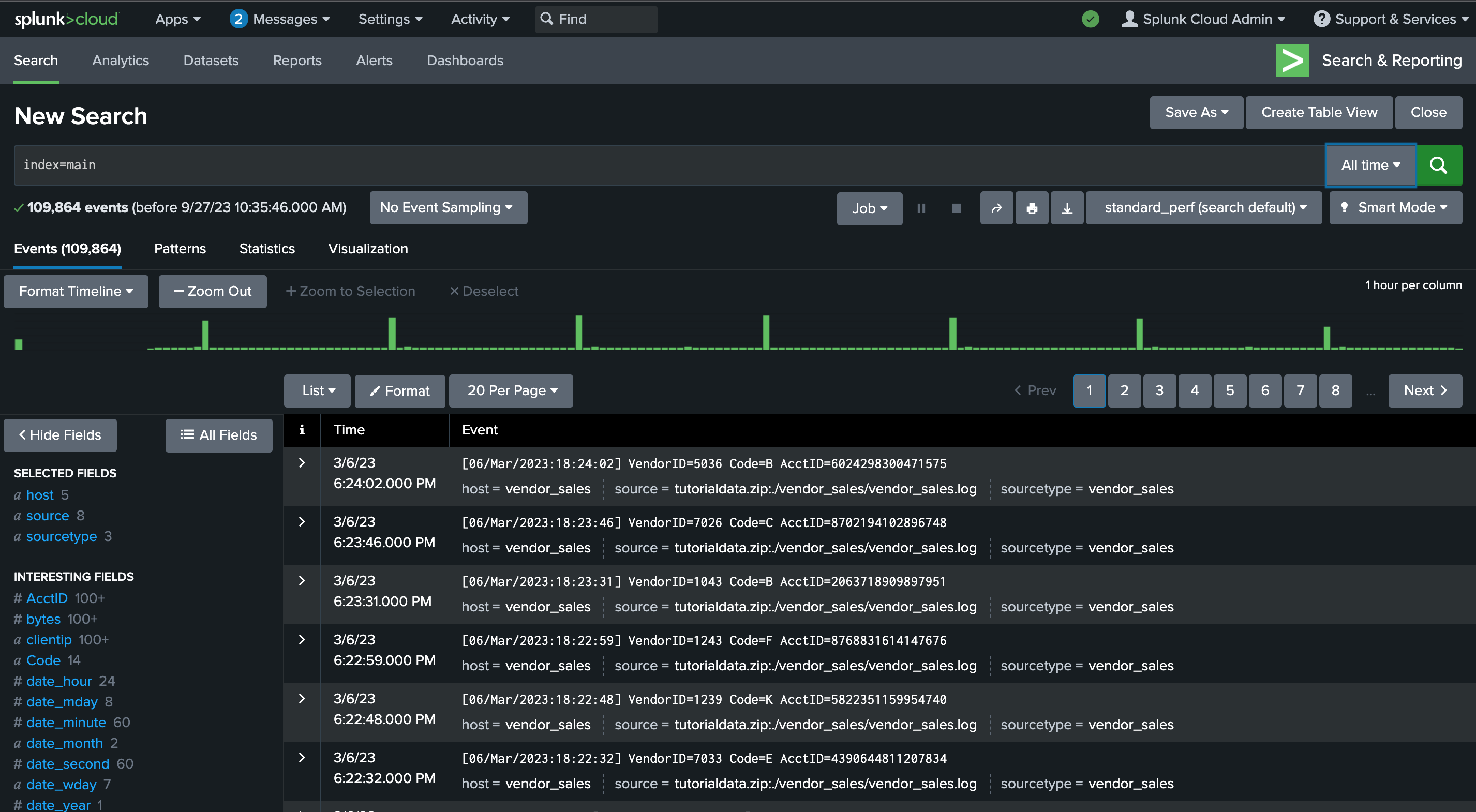
* Click the Next button to continue to Input Settings.
* By the Host section, select Segment in path and enter 1 as the segment number.



* 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 Index: Default.

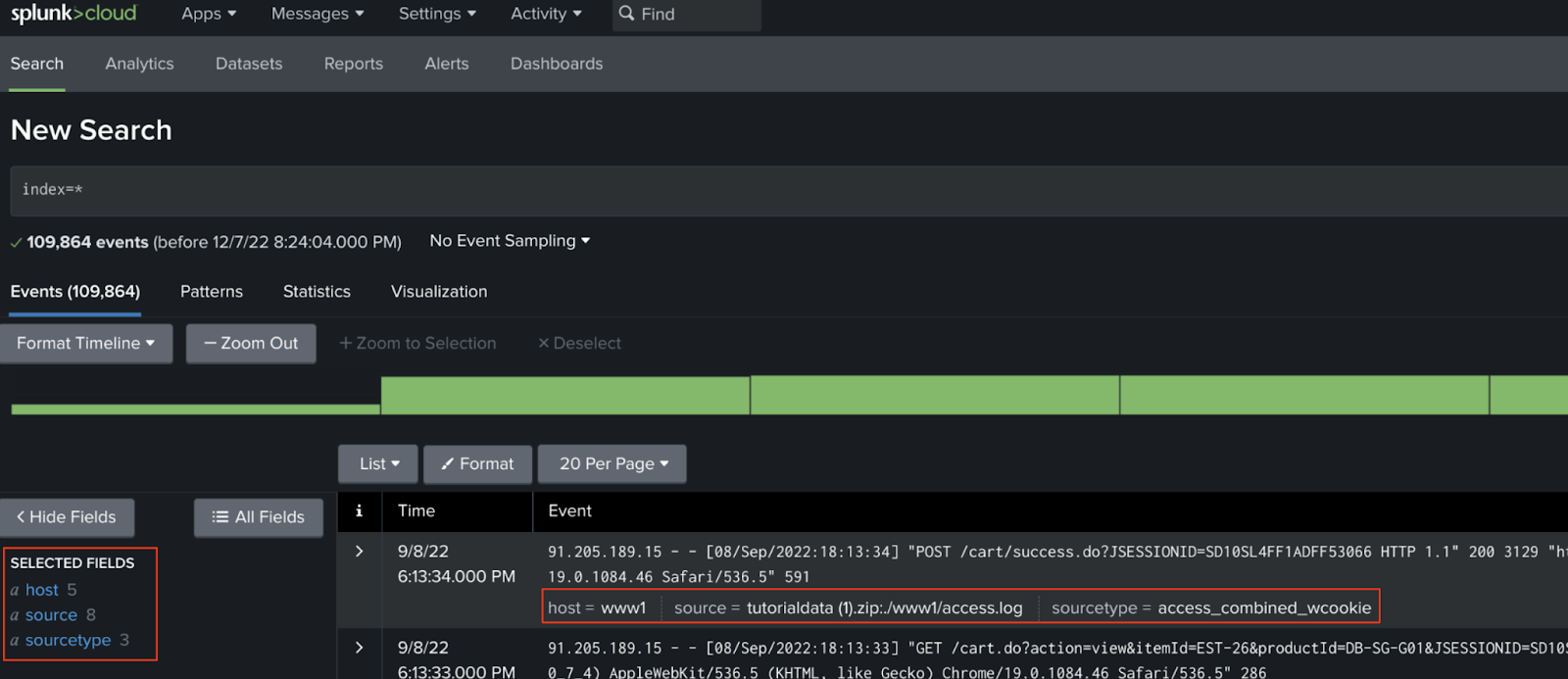


* Click Submit. Once Splunk has ingested the data, you will receive confirmation that the file was successfully uploaded.
* Navigate to Splunk Home. (To return to Splunk Home, click the Splunk Cloud logo on the Splunk Cloud page.)
* Click Search & Reporting. You may close any pop ups that appear.
* In 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.
* Select All Time from the time range dropdown to search for all the events across all time.
* Click the search button. Note that the search button is represented by the magnifying glass icon. Your search should retrieve thousands of events.



When Splunk indexes data, it attaches fields to each event. These fields become part of the searchable index event data. This helps security analysts easily search for and find the specific data they need. Now that you've run your first query, examine the search results and the fields.

For each event the fields are host, source, and sourcetype. Under SELECTED FIELDS, examine the same fields.



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.

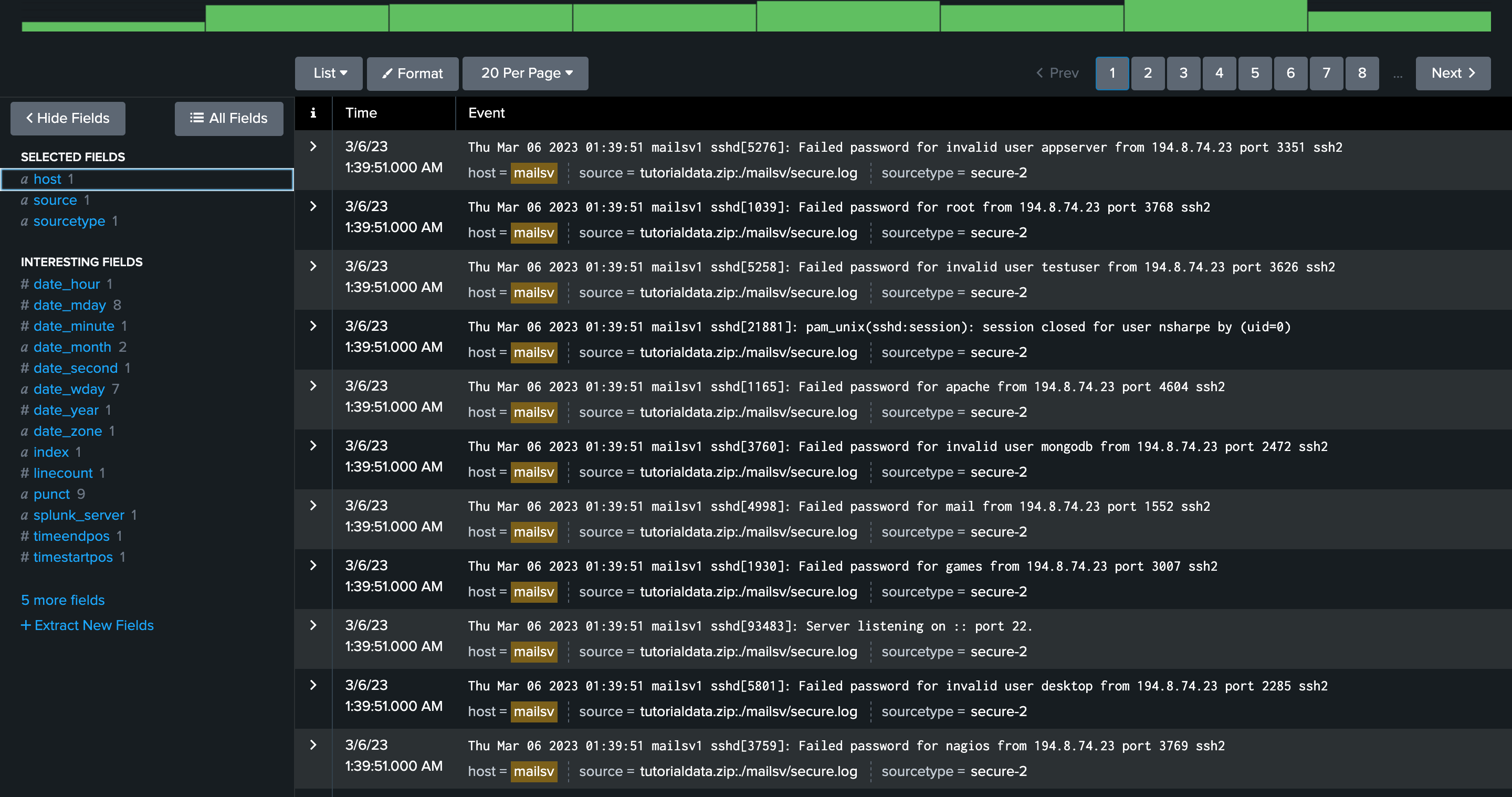
www3 - This is one of Buttercup Games' web applications.

vendor\_sales - Information about Buttercup Games' retail sales.

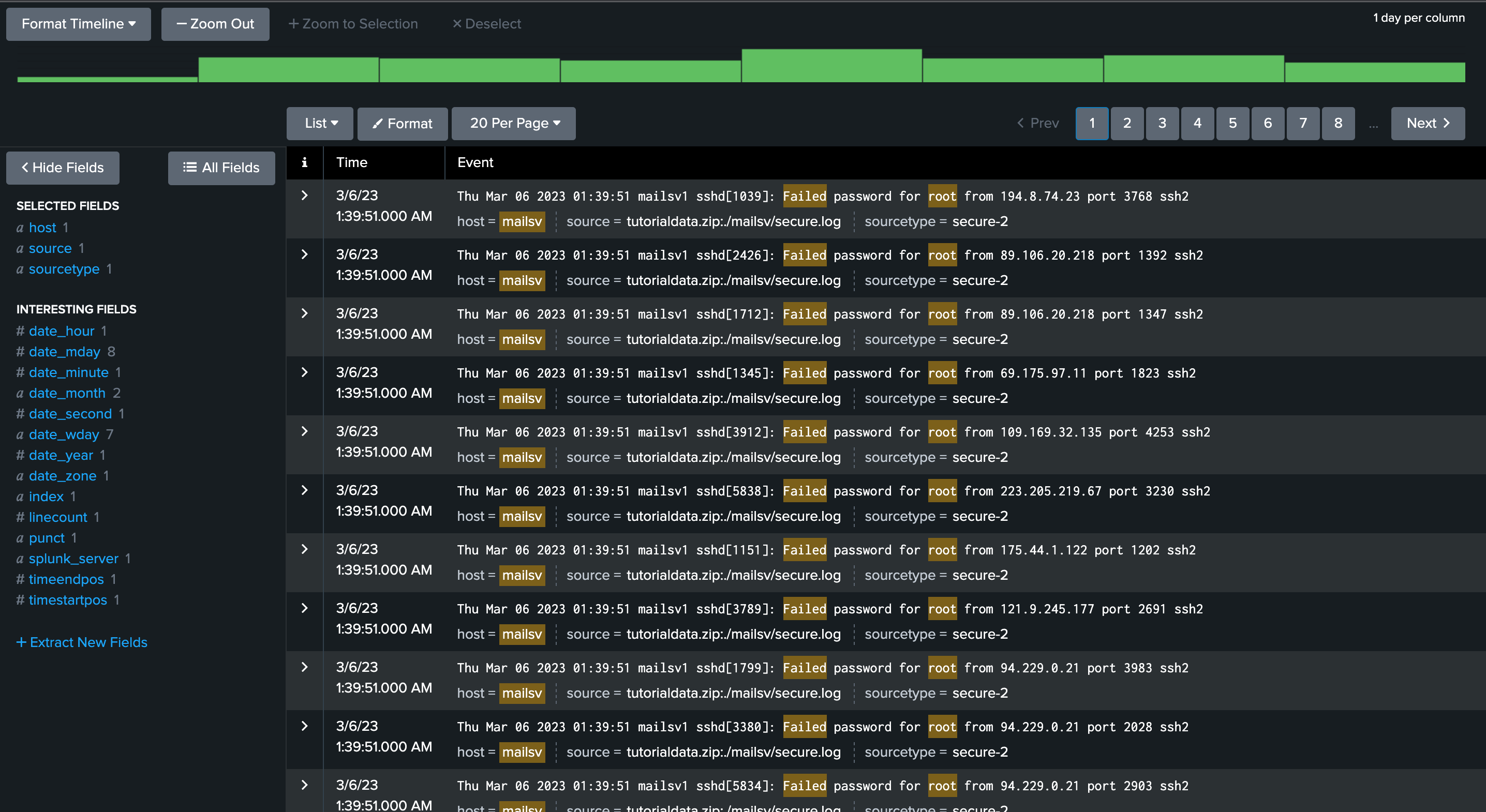
source: The source field indicates the file name from which the event originates. You should identify eight sources. Notice /mailsv/secure.log, which is a log file that contains information related to authentication and authorization attempts on the mail server.

sourcetype: The sourcetype determines how data is formatted.

* Under SELECTED FIELDS, click host and click mailsv.



* Enter index=main host=mailsv fail\* root into the search bar.



This search expands on the search from the previous task and searches for the keyword fail\*. The wildcard tells Splunk to expand the search term to find other terms that contain the word fail such as failure, failed, etc. Lastly, the keyword root searches for any event that contains the term root.