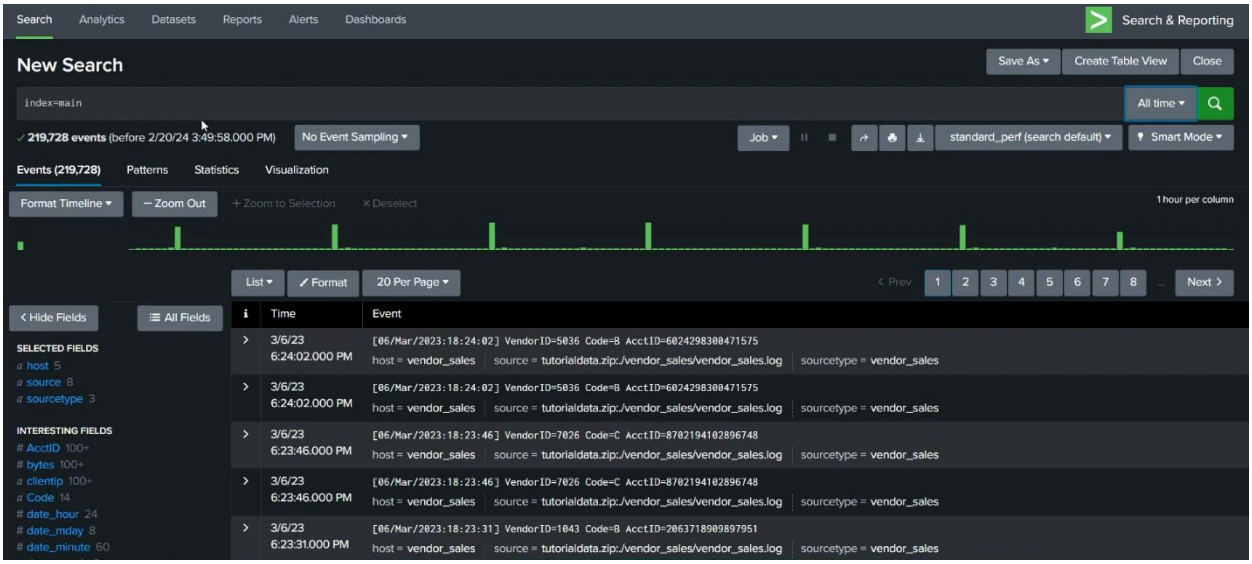
Performing Queries with Splunk

In this project I explore some basic searches using Splunk's querying language, called Search Processing Language (SPL). In this scenario, I have been tasked with identifying whether there are any possible security issues with a company's mail server. I do this by querying for failed SSH logins for the root account.

Performing a basic search using Splunk Cloud

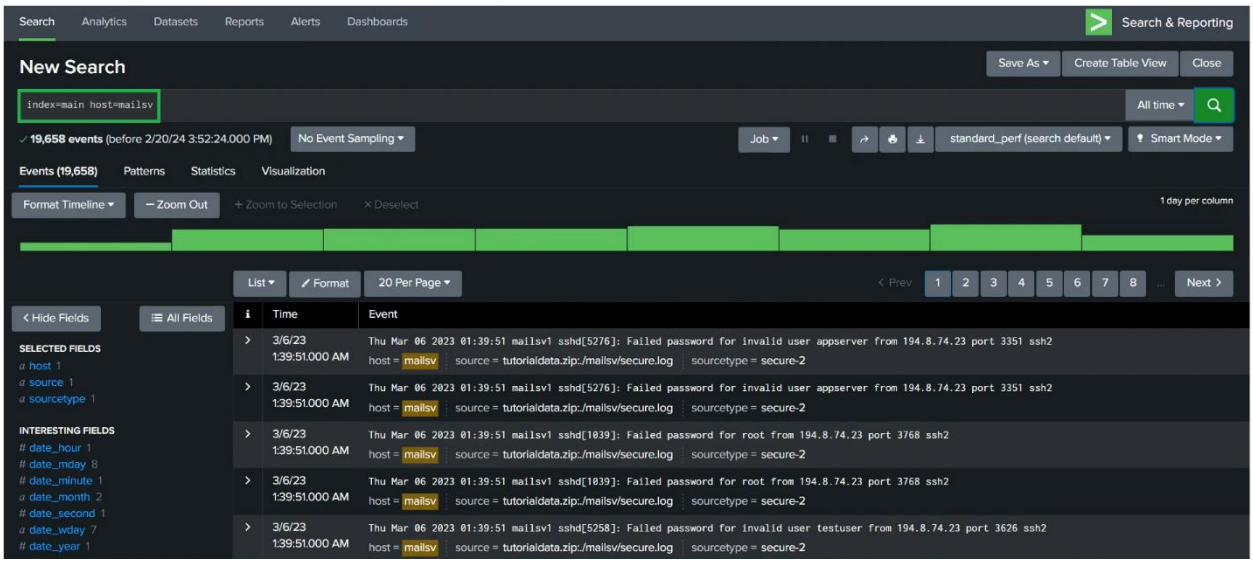
To begin, we click on **Apps>Search & Reporting** and type *index=main* into the search bar. This is an old dataset, so we click on the drop-down menu next to the magnifying glass on the right and select **All Time**. Now all of the data is available for queries. In this case we have over 200,000 results. In a real-word setting, however, selecting the shortest possible time-range related to an incident would be the best practice, so that any security breaches are identified and contained as soon as possible. That way results are returned faster and fewer resources are used.



Evaluating the fields and narrowing the search

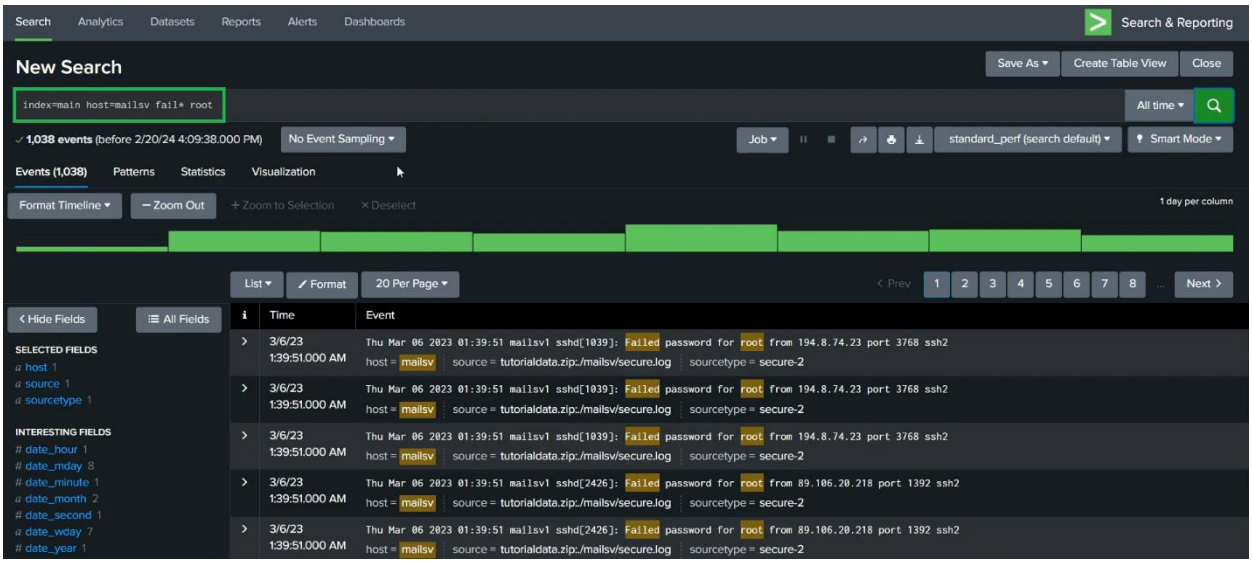
Because the task is to explore any failed SSH logins for the root account on the mail server, we'll need to narrow the search results for events from the mail server. When Splunk indexes data, it attaches fields to each event. For each event the fields here are *host*, *source*, and *sourcetype*. The host field specifies the name of the network host from which the event originated. In this search there are five hosts. The source field indicates the file name from which the event originates. We identify eight sources in this project. We also notice */mailsv/secure.log*, which is a log file that contains information related to authentication and authorization attempts on the mail server. The sourcetype determines how data is formatted. Here we observe three sourcetypes.

In this case, the we find the mail server called *mailsv* in the host field. We could either input *index=main host=mailsv* into the search bar or under **SELECTED FIELDS**, click **host** and click **mailsv**.



Searching for a failed login for root

To further narrow down our search and query for failed login attempts for the root account, we should add *fail* root* into our existing query. This search expands on the previous query 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., while the keyword *root* searches for any event that contains the term root. We have now narrowed down the results from over 200,000 to a little over 1000.



Based on these results, actions should be taken to harden the mail server in order to protect it from brute force attacks.