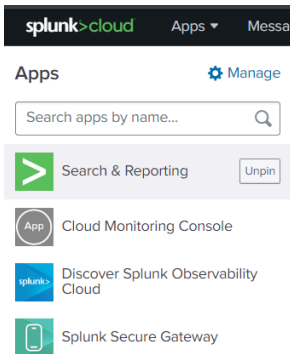
Performing a query with Splunk

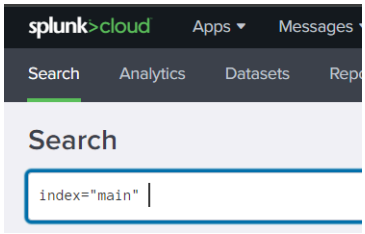
In this project I was able to ingest data provided by the Google Cybersecurity Certificate programme into Splunk to analyse.

Searching for data

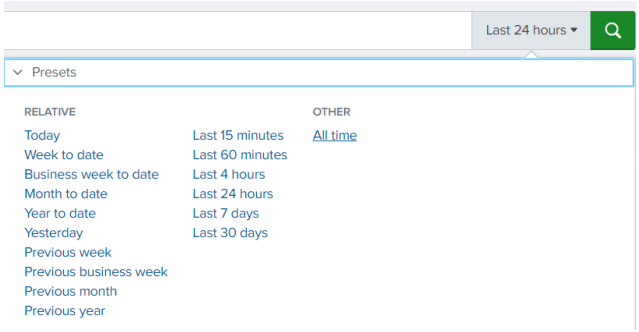
First, I needed to query Splunk to display all the data that I had ingested earlier, before analysing this data.



To do this, I first clicked on “Search & Reporting” as shown in the screenshot above.

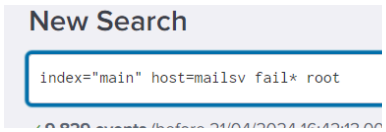


I then used the search bar which appeared after the previous step, to search for the data using the search query “index=”main”” as displayed above.

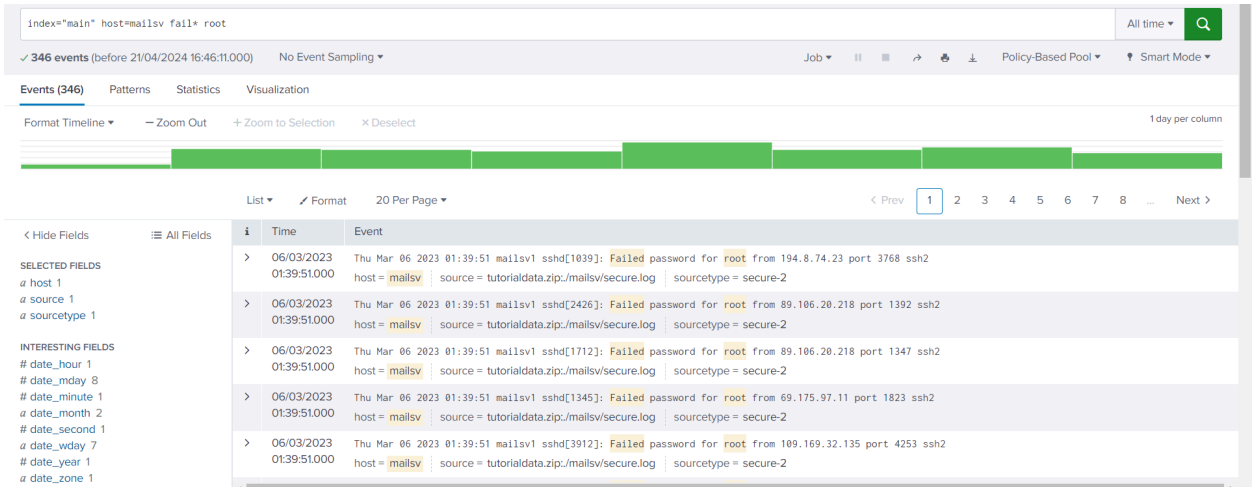


After that, I needed to set the filter to display data from all time instead of the last 24 hours. To do this, I clicked on the time range drop down button before selecting “All time”. I then clicked on the magnifying glass button to begin the search as displayed in the screenshot above.

After the search results were presented, I then needed to click on “host” under “SELECTED FIELDS” as shown in the first screenshot above, to filter the results for the host “mailsv” as shown in the second screenshot above.



The previous filter has resulted in removing any hosts that weren’t called “mailsv”. I now needed to further query Splunk to display data that has the word “fail” and “root” in it. To do this, I added “fail* root” to the search query as shown in the screenshot above. This means that any data with the keyword “root” will be displayed while any data including the string “fail” will be displayed even if there are more letters that follow it such as “failure” or “failed”.



The screenshot displayed above shows the end result where we can see the query has successfully generated the specific information I had requested. I am now able to view all the failed login attempts that occurred.

Summary

Completing this project has given me a good insight into using a popular cyber security tool. It has enabled me to experience the ease such software provides security professionals when dealing with incoming threats as the navigation was simplistic and the organisation of information was tidy. I was able to successfully query Splunk to be presented with all of the failed login attempts from the initial data, which in the world of cyber security can be a red flag.