USE SPLUNK CLOUD TO PERFORM A SEARCH AND INVESTIGATE LOG DATA

Pedro Osorio Lopez.

1. High-Level Project Description:

*In this activity, we'll upload sample log data, and use Splunk Cloud to perform a search and investigate this data.

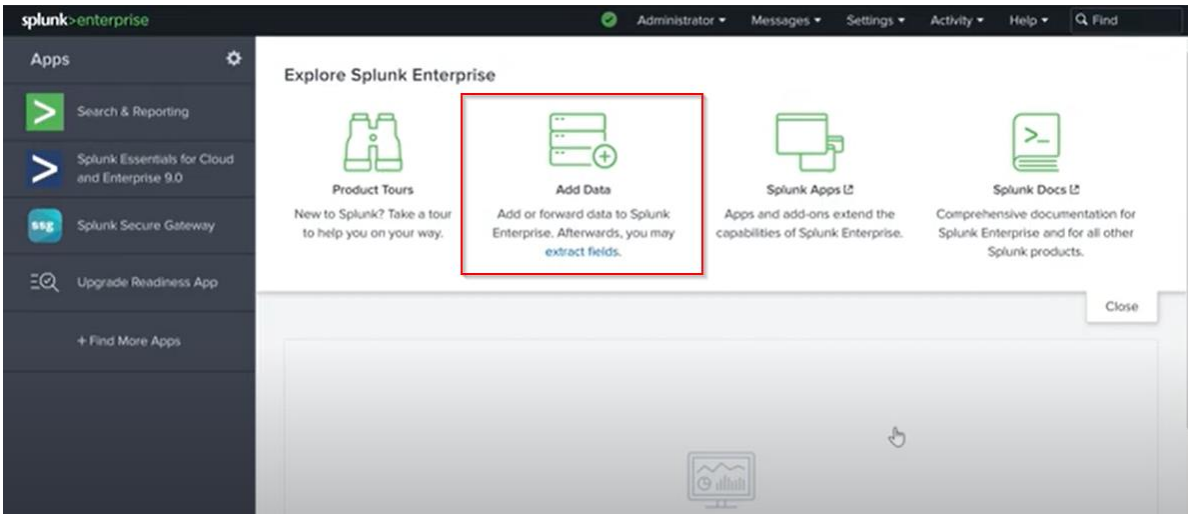
2. Project Setup and Required Tools:

*All we need to complete this activity is a Splunk account, so we can use this extremely popular SIEM tool on any device.

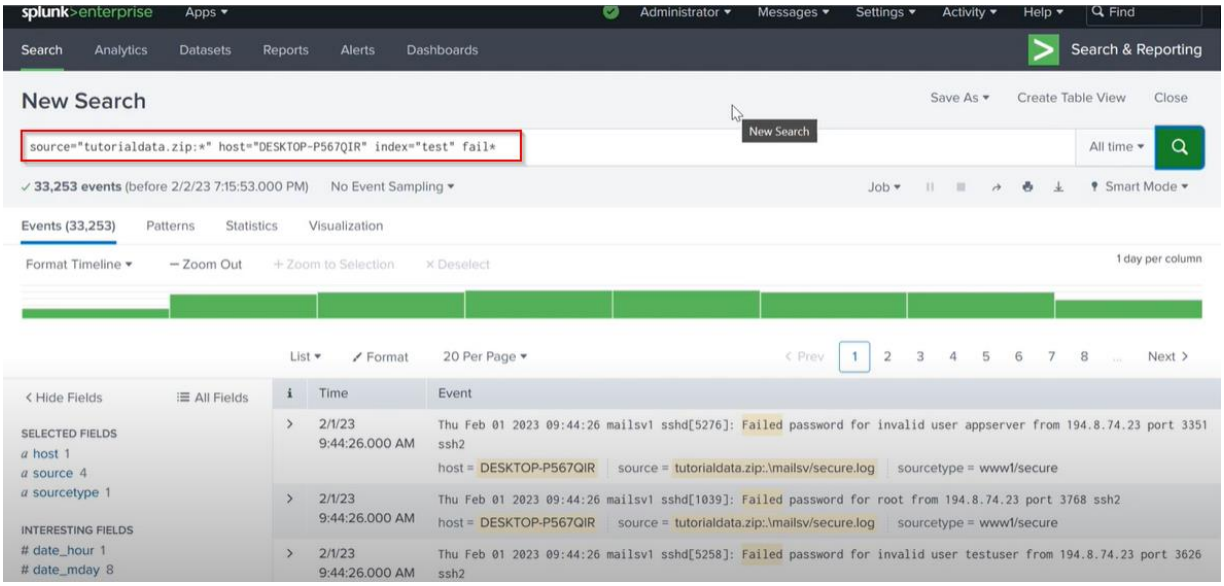
3. Step by Step Project Walkthrough

*In this lab, we will: Upload sample log data, search through indexed data, evaluate search results, identify different data sources, and locate failed SSH login(s) for the root account.

*The first step is pretty straightforward, since one logged in into Splunk, in the main interface we just need to click "Add Data" and proceed to upload it and fill out the necessary information. Note that Splunk can ingest zip data; Google already provided sample files to us, but these can be downloaded from Splunk as well if necessary.

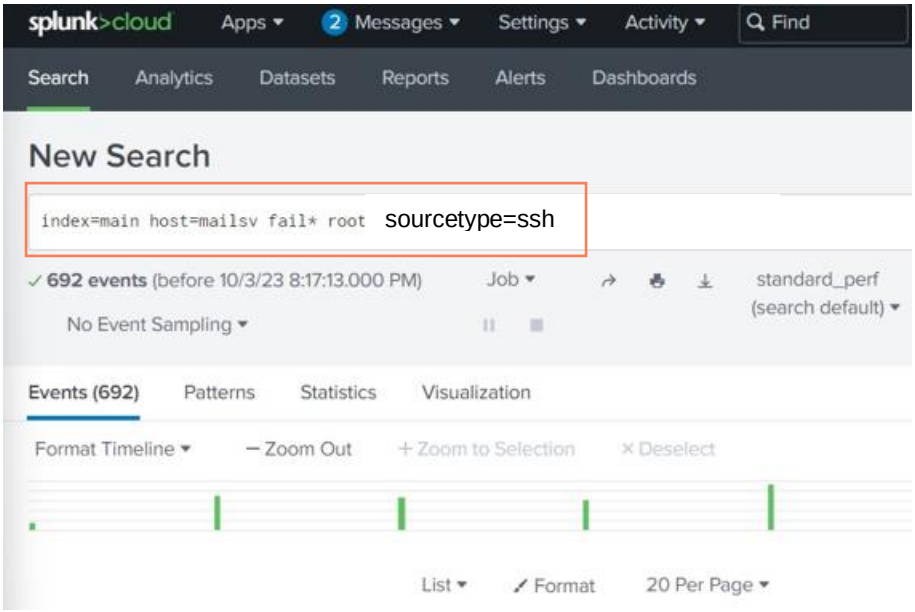


*Once successfully uploaded, we can proceed to search through all the indexed data included in the imported file. For example:



In this query, we are using a source (the uploaded zip file), a host, and an index to get a series of results. In we add the keyword “fail), we will be checking for all the entries that contain words which start with fail (including fail, failed failure, etc), to check for anomalies such as failed login attempts.

*Lastly, if we want to locate failed SSH login(s) for the root account, we can do so with the following search query:



4. Summary and/or Recommendations:

*In this activity, we learned how to use Splunk, a SIEM tool of extreme popularity used by many major companies to safeguard and monitor their data.