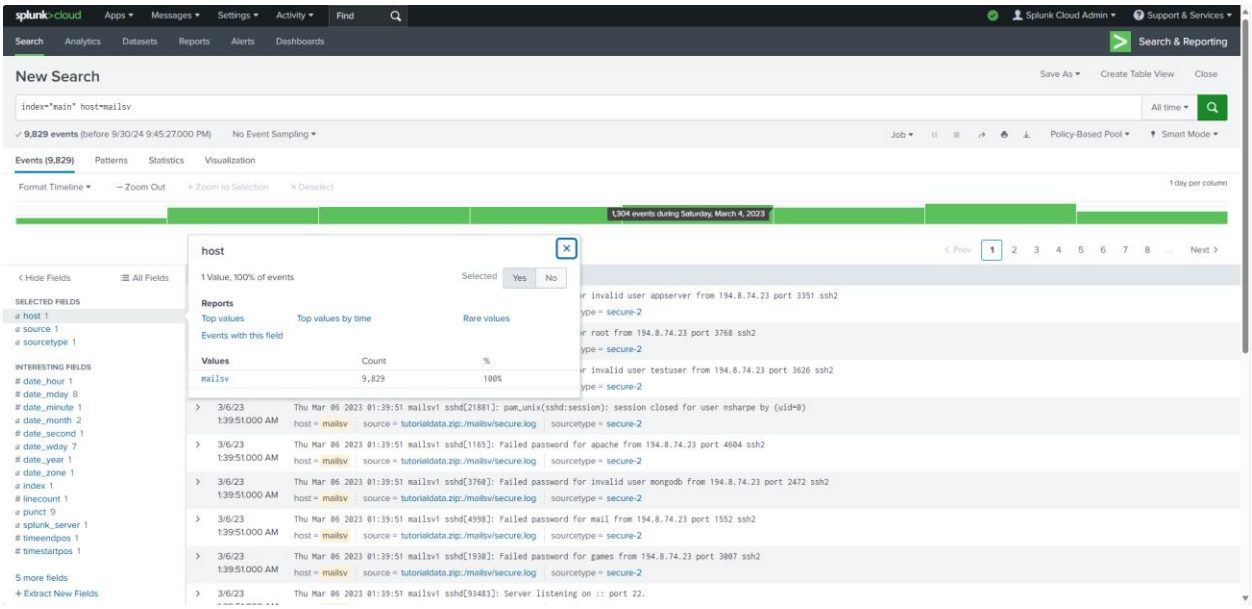
Splunk File Analysis

Scenario:

I am a security analyst working at a fictitious e-commerce store. I have been tasked with identifying whether there are any possible security issues with the mail server. To do so, I must explore any failed SSH logins for the root account.

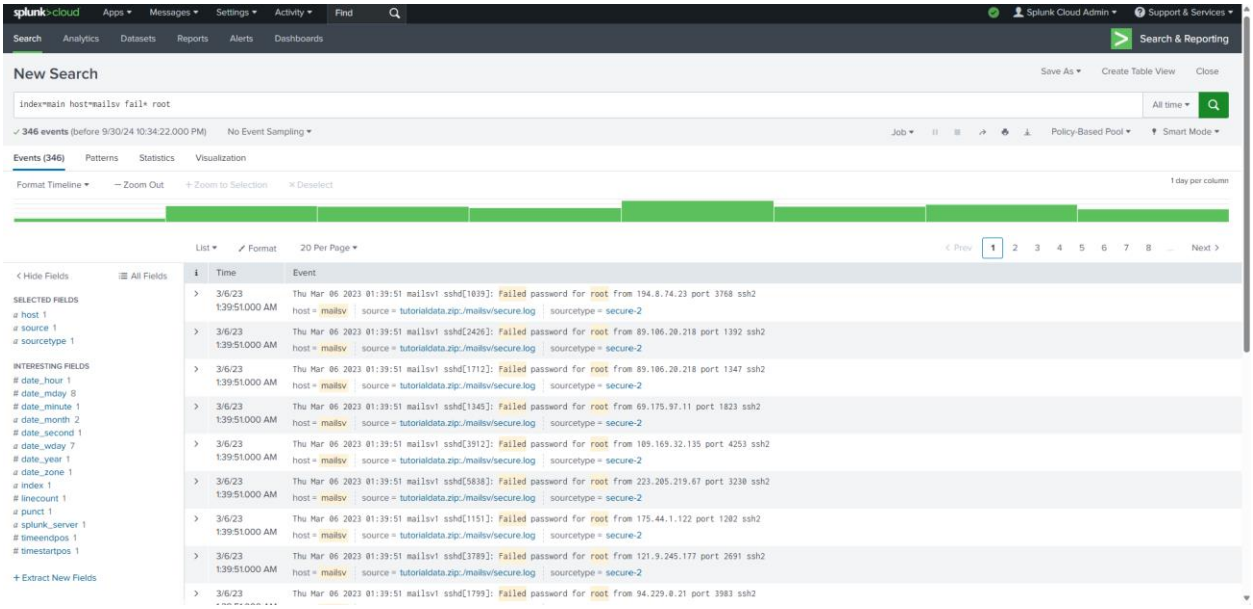
Narrow search to the mail server

Because I have been tasked with exploring any failed SSH logins for the root account on the mail server, I will need to narrow the search results for events from the mail server. I accomplished this by locating the SELECTED FIELDS tab, selecting host, and then selecting mailsv to narrow my search to the appropriate area.



Search for a failed login for root

After successfully narrowing the search results to events generated by the mail server, I continued to narrow the search to locate any failed SSH logins for the root account. I accomplished this by entering 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 i.e., asterisk symbol, 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.



Conclusion

Using Splunk, I have identified all relevant instances of failed SSH logins for the root account and can investigate these individual events further if necessary.