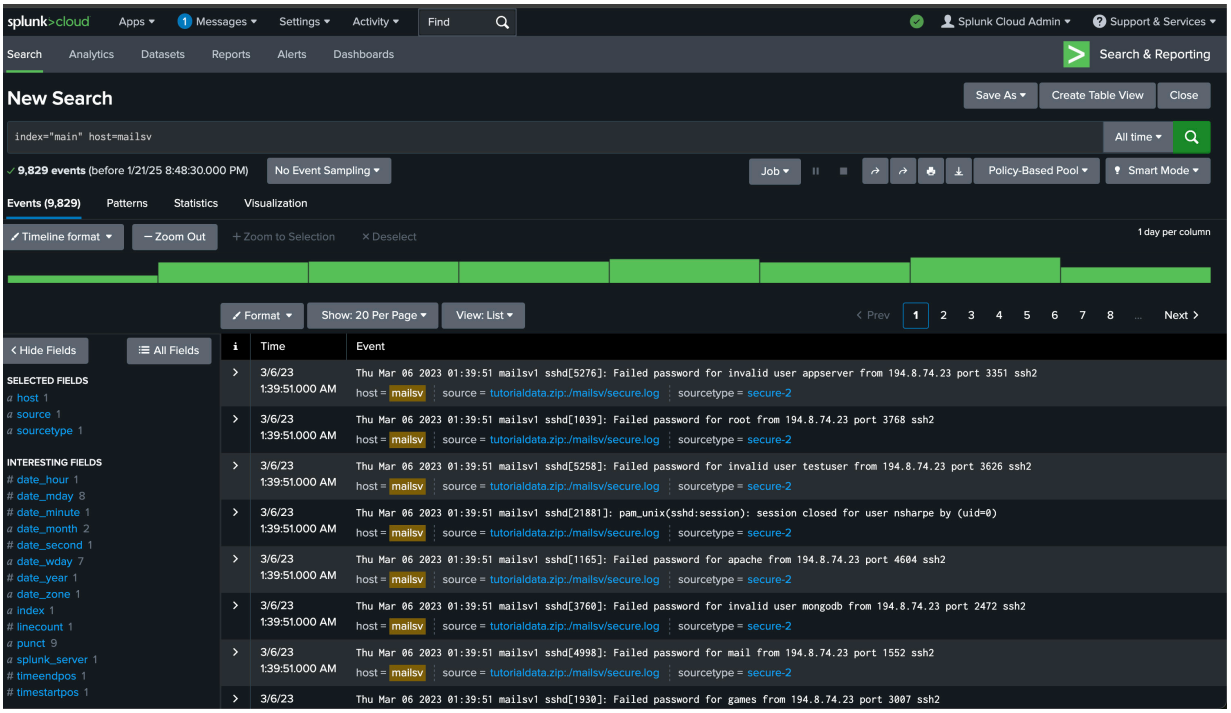
As part of my investigation into failed SSH login attempts for the root account on the mail server, I narrowed the search results by using the code `index=main host=mailsv` in Splunk. This allowed me to focus on relevant data related to unsuccessful login attempts. By honing in on this information, I can effectively analyze potential security issues associated with the root account.



I used the code `index=main host=mailsv fail*` to narrow the search results to events generated by the mail server. Next, I continued to refine the search to specifically locate any failed SSH login attempts for the root account. This focused approach allows me to effectively identify potential security issues related to unauthorized access attempts.