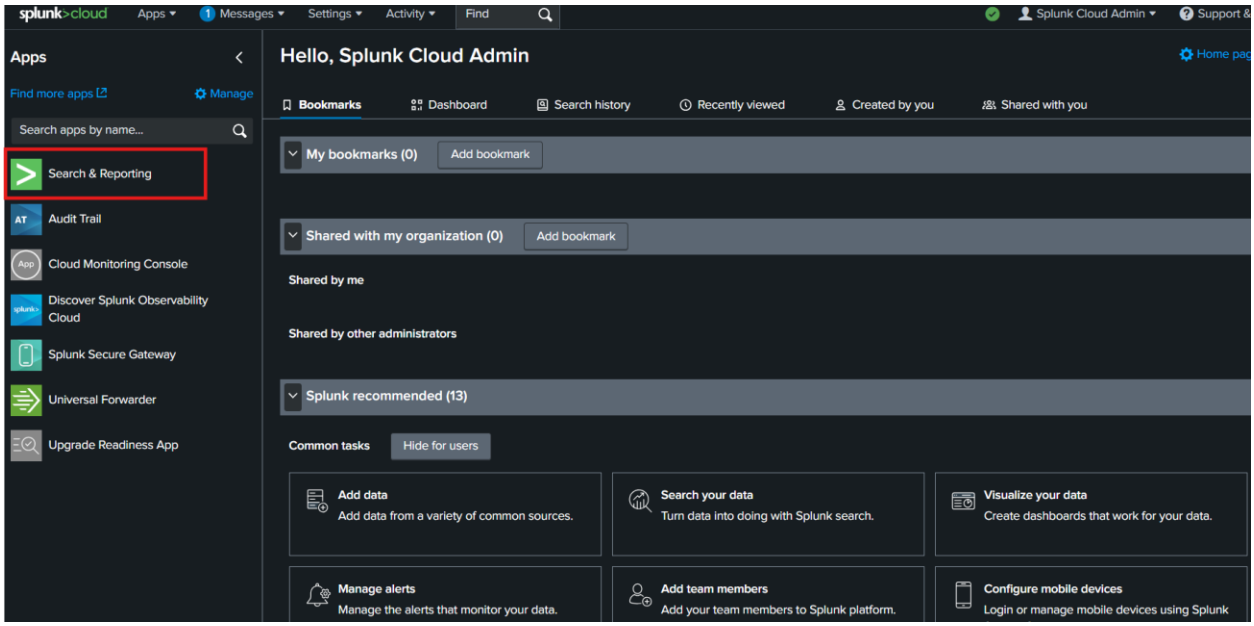
Querying in Splunk SIEM Tool

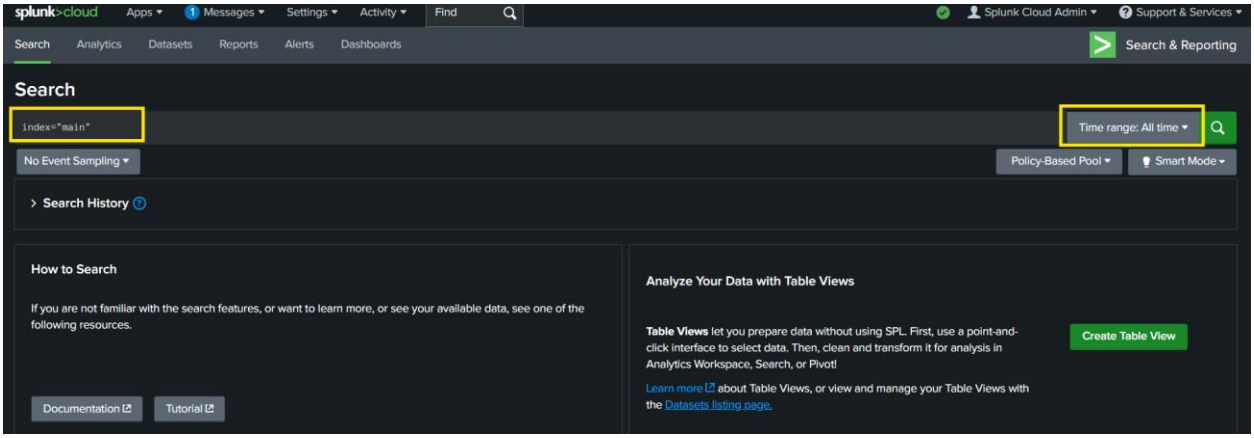
Project:

In this project I want to identify whether there are any possible security issues with the company's mail server. To do that, I'll need to check for any failed SSH logins for the root acct.

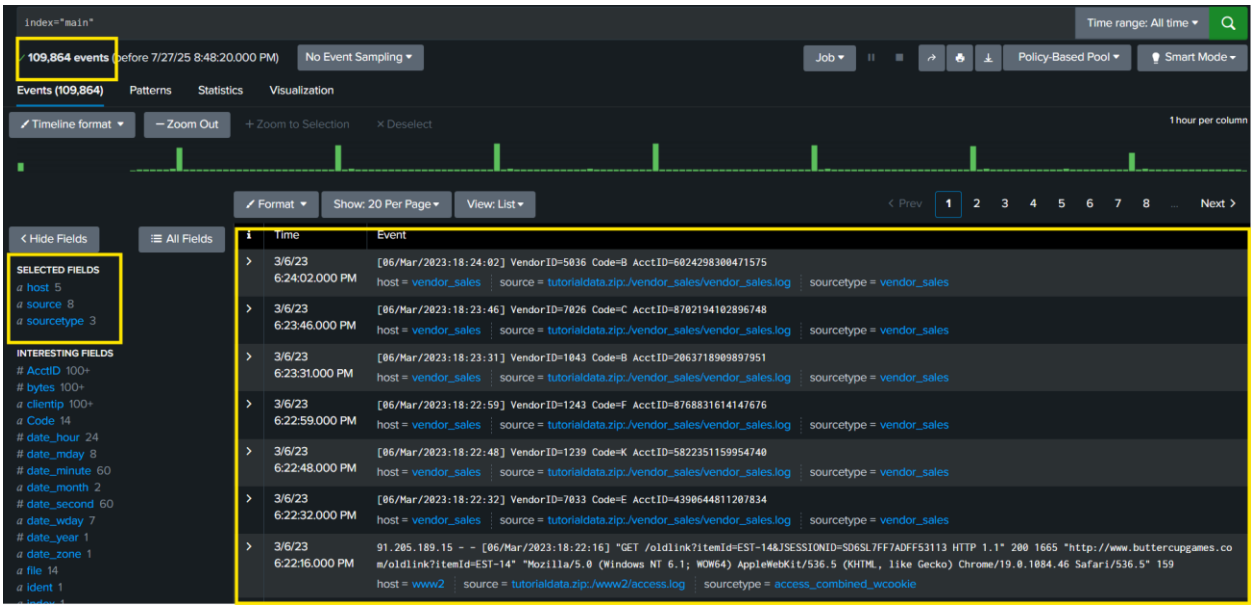
First, by navigating to "Search & Reporting" from the app panel:



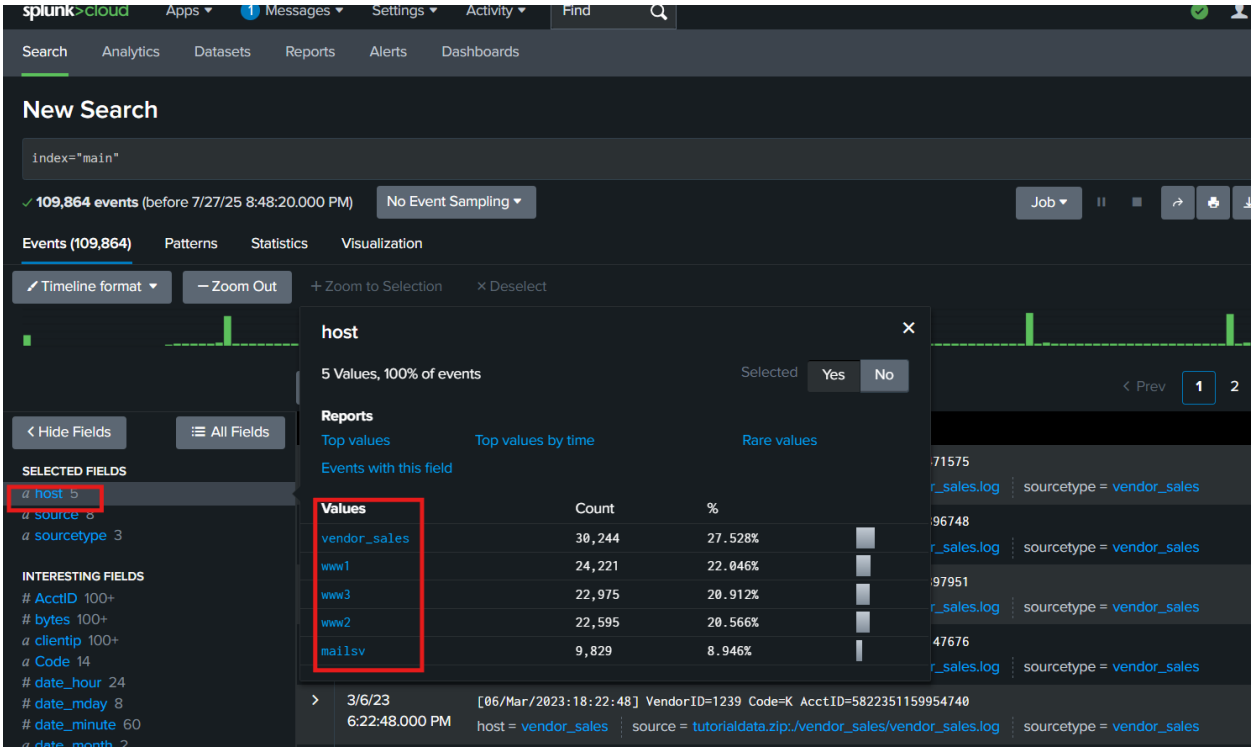
I'll enter a query to index the "main" data storage and filter to check for 'all time' to look at **everything** ever captured:



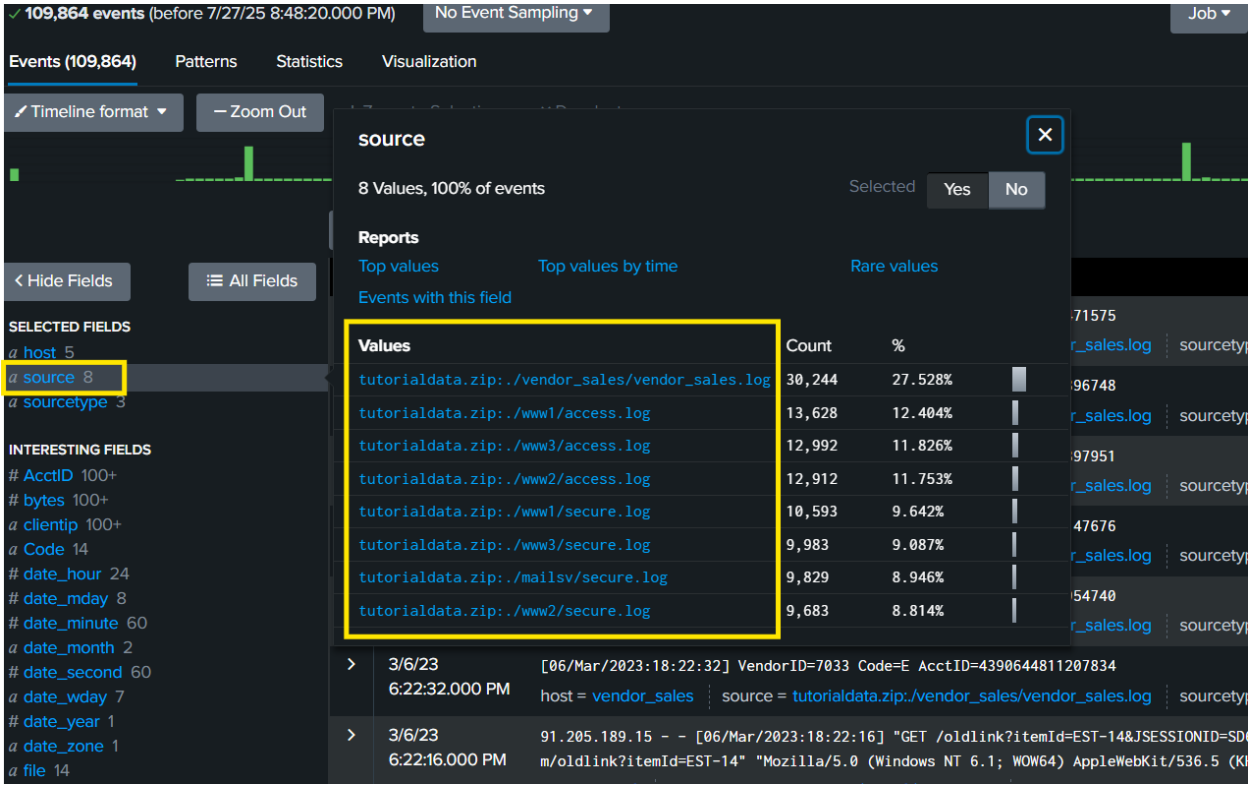
After querying, it returns raw logs or events, which are like time-stamped notes. I'm also able to explore the "Selected Fields" which tells me the number of hosts, sources, & source types:



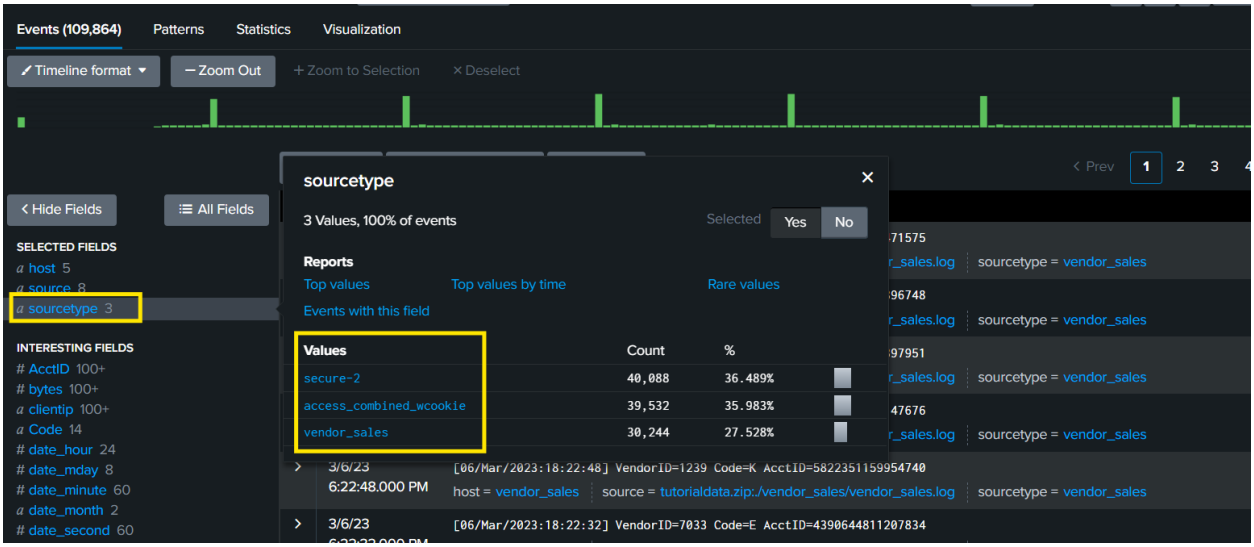
Selecting the *host* field, all 5 network host are shown (1 sales data, 3 web apps, & 1 mail server)



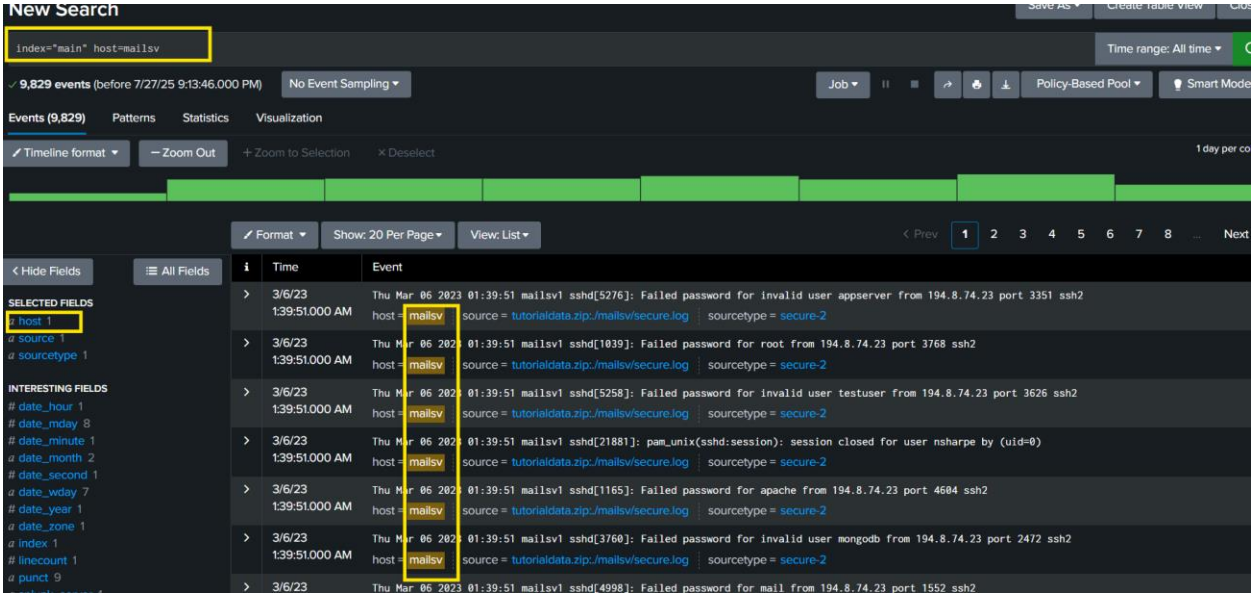
Alternately, selecting the *source* field, it indicates the file name from which the event originates:



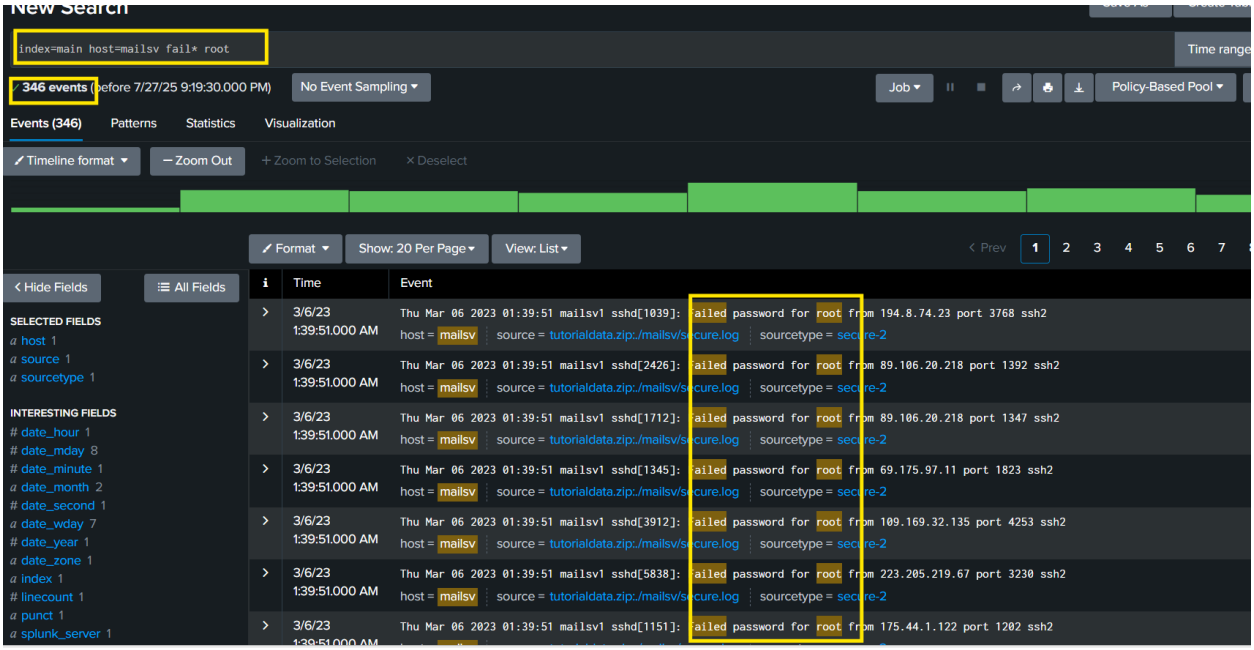
Same goes for *sourcetype*, which determines how data is formatted:



But for this project, I'm focusing on exploring failed SSH login for the mail server, so I'll populate the *mailsv* host and notice that a new term has been added to the search bar and the number of events have significantly decreased to just over 9k:



Now to query for failed logins from the host *mailsv* that's attached to word *root*, which returns less than 350 events, and shows all failed attempts:



After reviewing all 18 pages, I have concluded that there were over 300 failed SSH logins for the root account