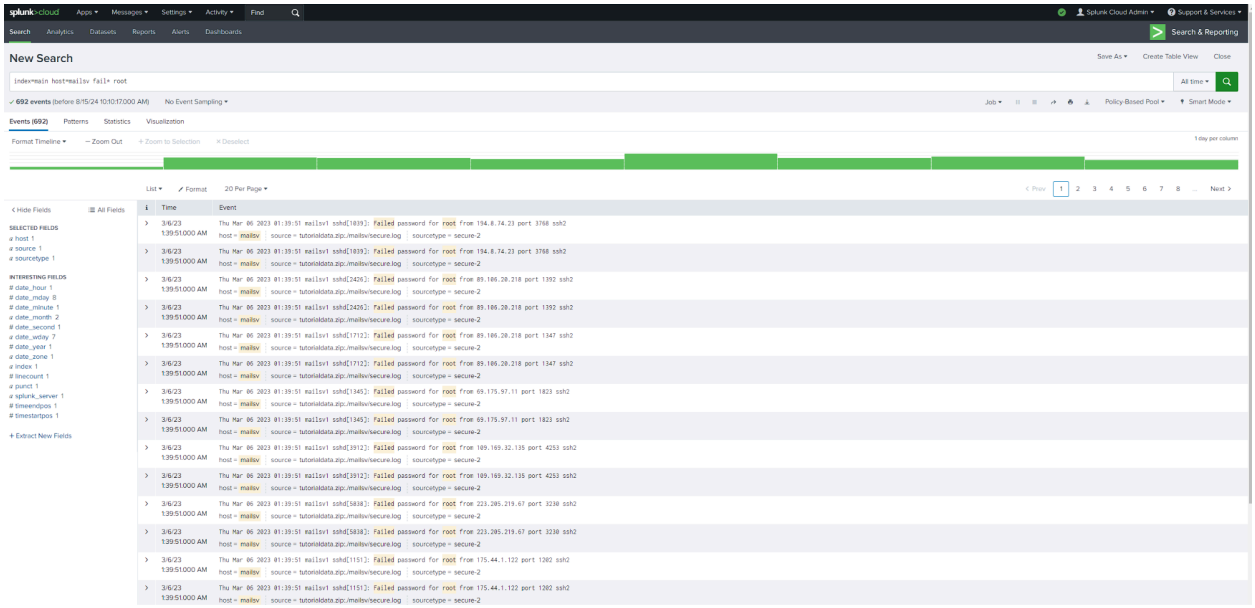
Pretext: You are a security analyst working at the e-commerce store Buttercup Games. You've been tasked with identifying whether there are any possible security issues with the mail server. To do so, you must explore any failed SSH logins for the root account.



Search query of sample data provided was:
index = main host = mailsv fail* root

- **Index** is a repository for data and in this instance, the index is a single dataset containing events from an index named main
- **Host** field specifies the name of the network host from which the event originated. In this instance, we are investigating the events generated by “**mailsv**”
- Source field indicates the file name from which the event originates, in this instance /mailsv/secure.log
- Sourcetype determined how the data is formatted, such as secure-2, in this instance
- We are interested in failed login, so we specify **fail* root**, where **fail*** is a keyword with a wildcard that expands the search term to find other terms that contain the word “fail” such as “failure” or “failed.” The keyword root searches for any event that contains the term “**root**”

In conclusion, using Splunk, we uploaded sample log data, searching through the indexed data, and evaluated the search results by identifying different data sources and locating the failed SSH logins for the root account.