Task 1 Guide: Building a Dashboard using Splunk

Download Splunk Enterprise

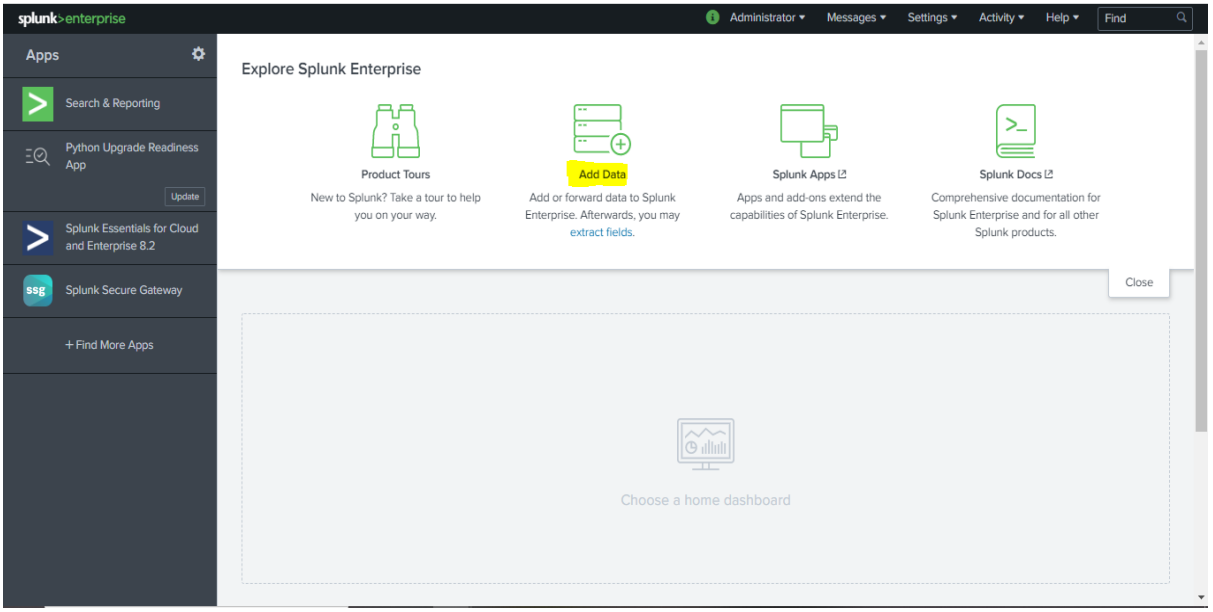
https://www.splunk.com/en_us/download/splunk-enterprise.html

Installing Splunk on Windows

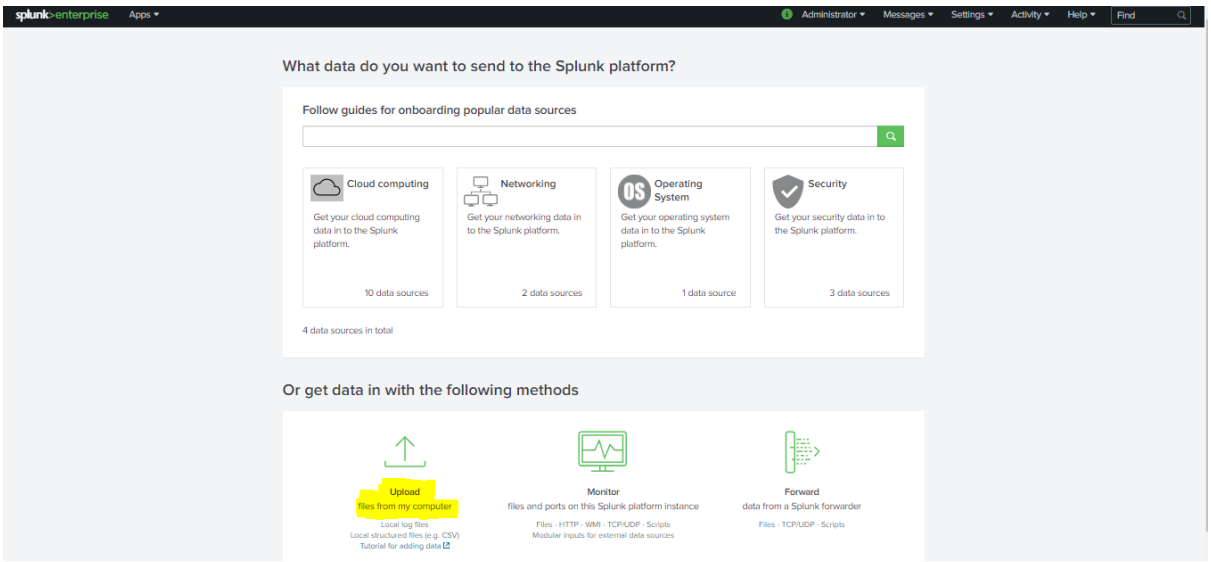
https://www.splunk.com/en_us/resources/videos/installing-splunk-enterprise-on-windows.html

Import data into Splunk

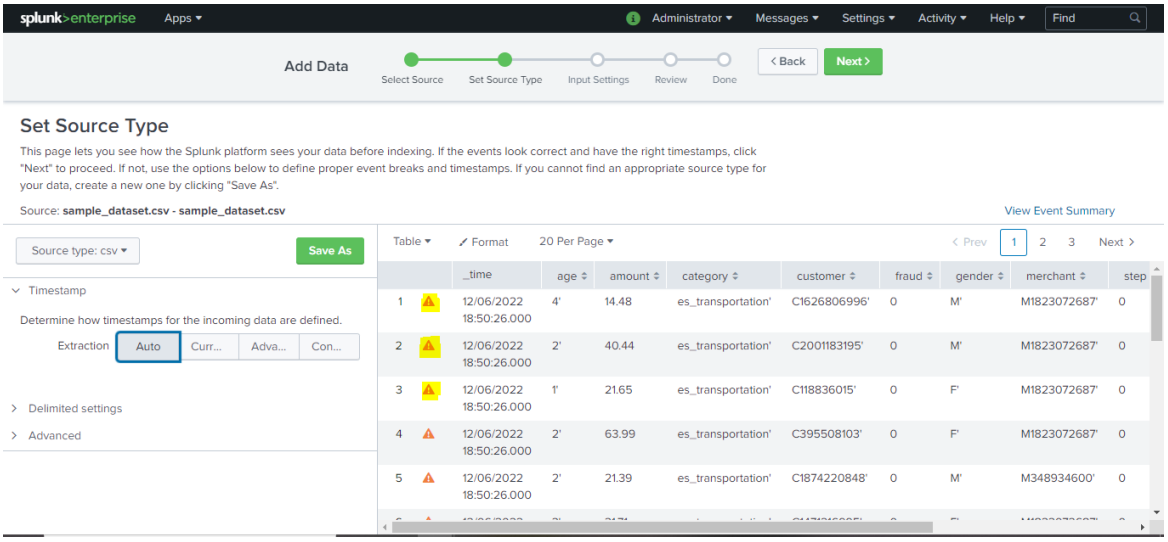
After installing Splunk Enterprise and creating an account, import “prepared_data.csv” by selecting “Add Data”.



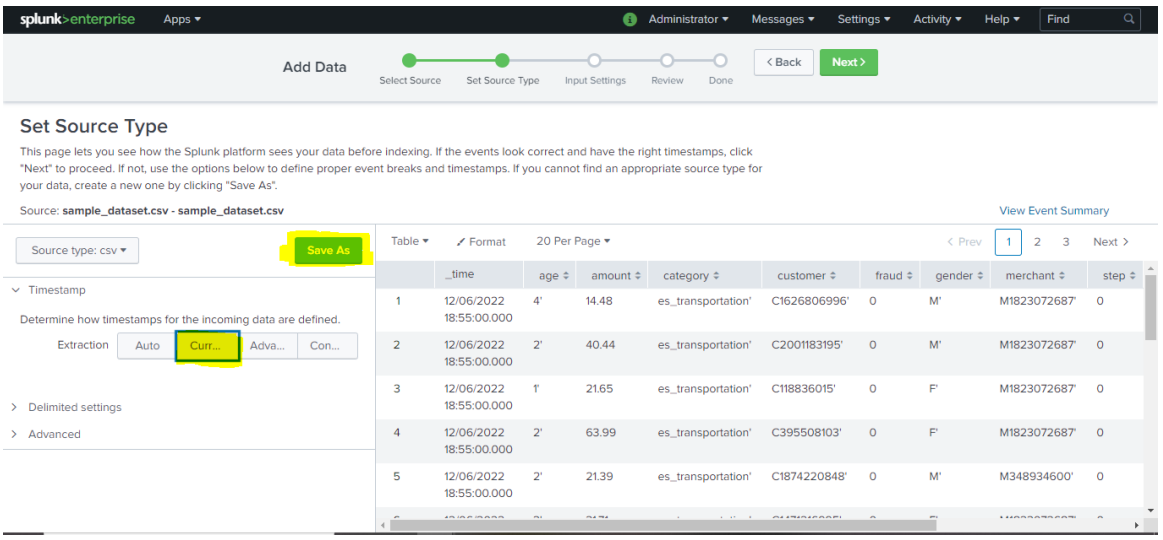
Then, click on “Upload files from my computer”. This means that the “prepared_data.csv” file should already be saved on your computer.



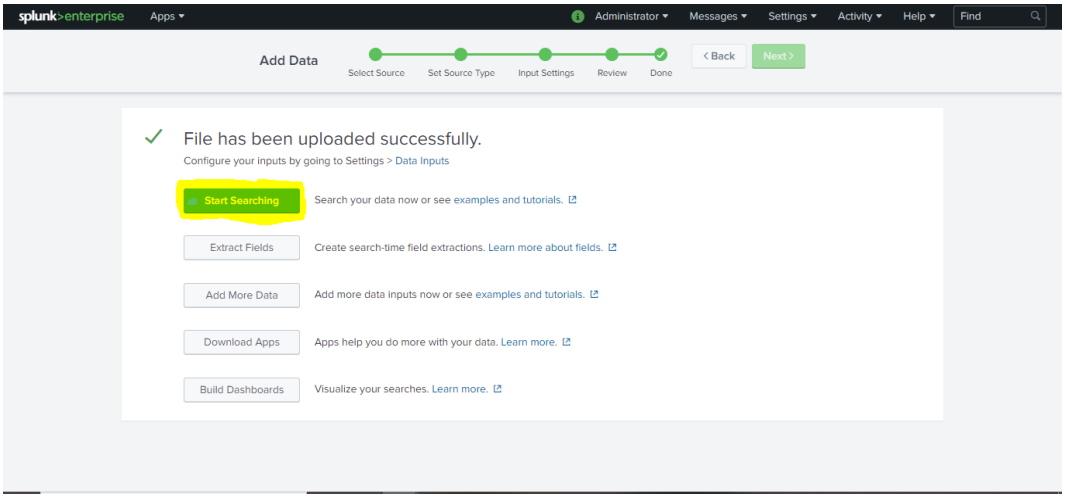
Select the file from your computer, then click on next. In the “Set Source Type” section, you may see a caution sign error, as shown below.



Go to Timestamp on the left and change from “Auto” to “Current time”, then click on “Save As”. You can name this “fraud_dectection.csv” and save.

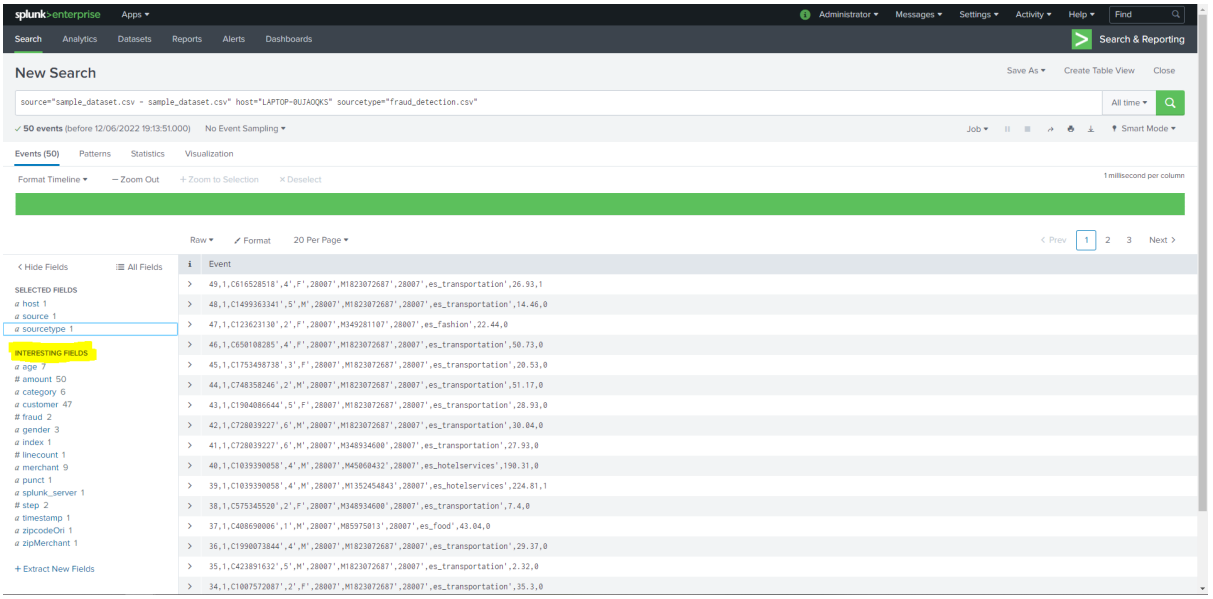


Click on “Next” until you get the result below.



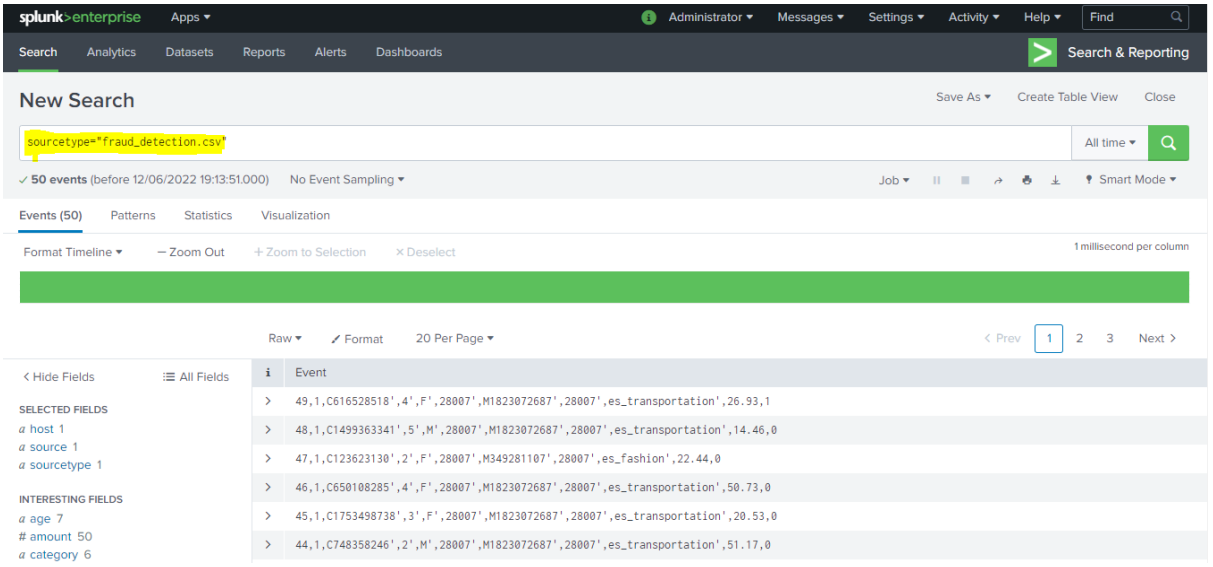
Analysing the Data

Click on “Start Searching” to start analysing. On the left, you can find the “Interesting Fields” section.

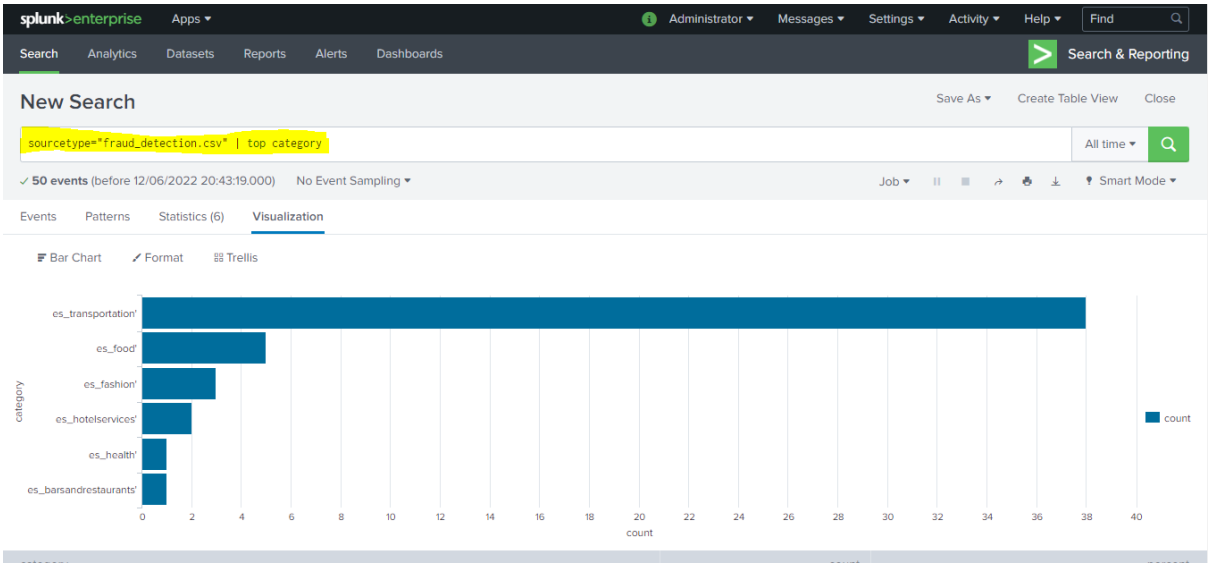


Creating the Dashboard

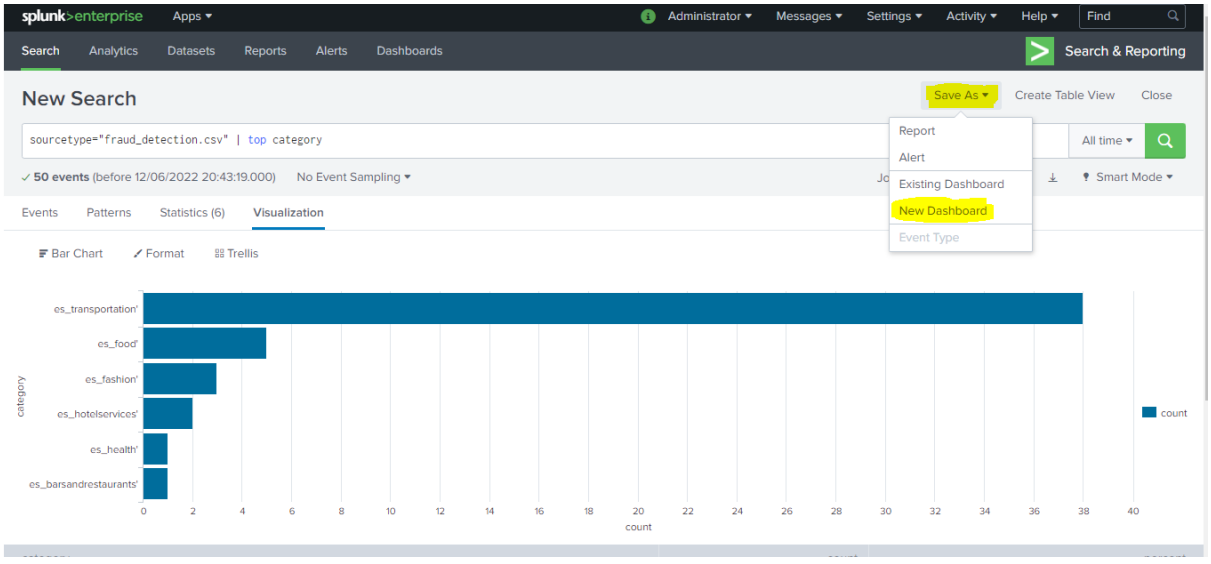
One of the ways to create a dashboard in Splunk is via search.



For example, to add “Count by category” to your dashboard, type out ***sourcetype="fraud_detection.csv"*** **|** ***top category*** in the search field. This action counts the number in each category, and you should get something like the example below:



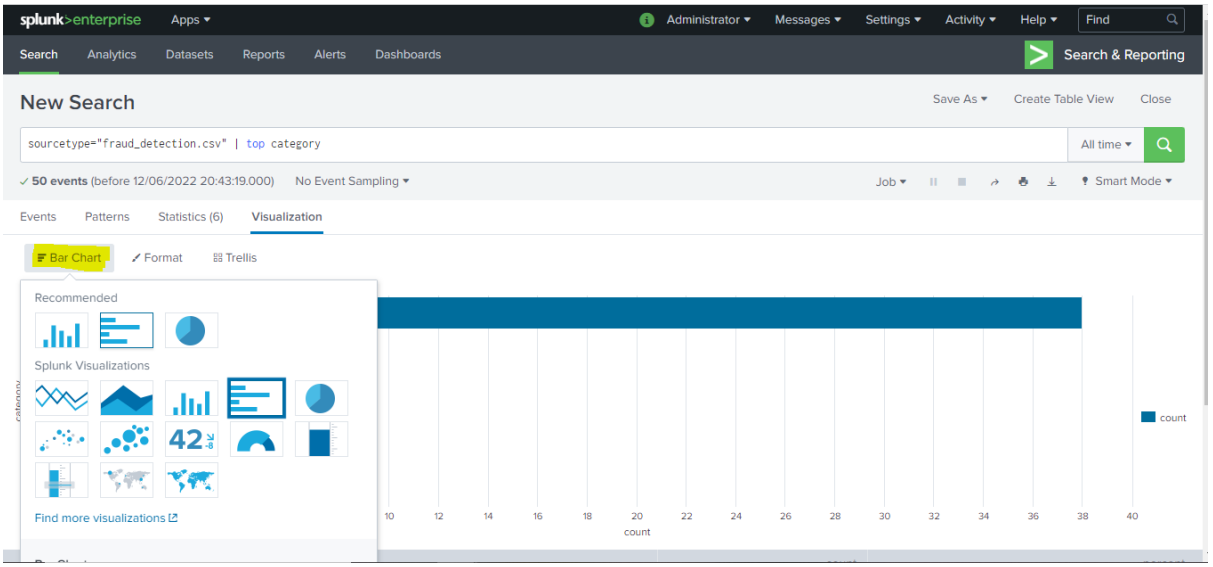
To add this chart to your dashboard, go to “Save As > New Dashboard > Dashboard Title = “Fraud Detection Dashboard” > Classic Dashboards > Save to Dashboard. This creates your dashboard.



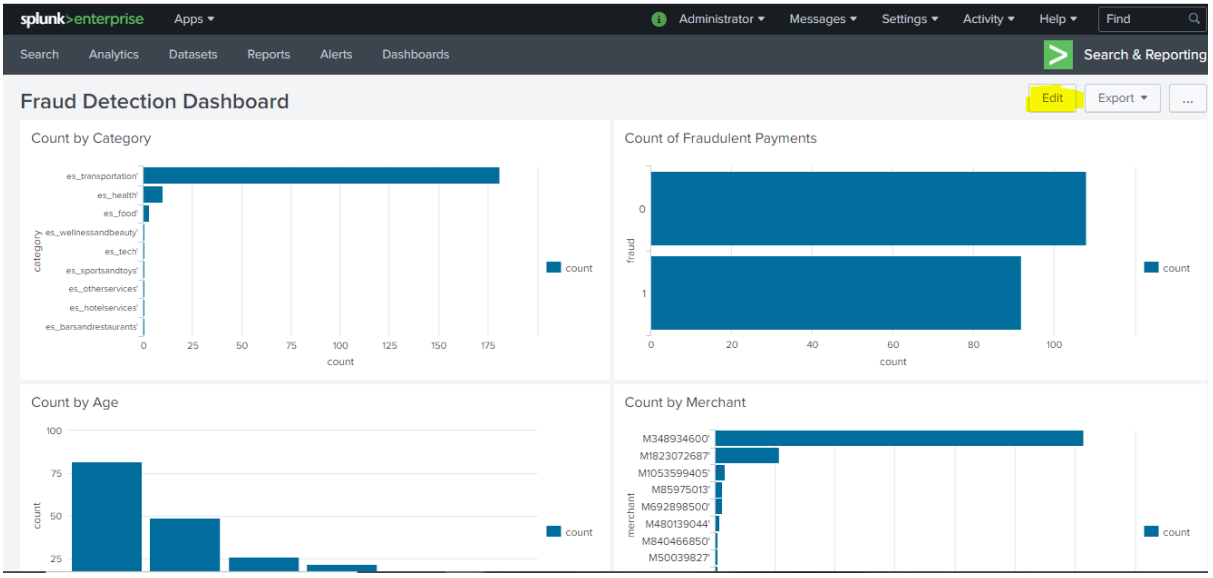
To get “Fraud detected by category”, type ***sourcetype="practicesplunk.csv" fraud="1" | stats count values(fraud) by category*** in the search field. This counts the number of fraudulent activities recorded for each category.

To get “Gender with the most fraudulent activity by category”, type ***sourcetype="practicesplunk.csv" fraud="1" gender="F'" | stats count values(fraud) by category.***

To add more charts, you need to add to “Existing Dashboard” and select the one you’ve created. Also, for more chart options (e.g., histograms, line charts), see below:



You can rearrange your dashboard to suit your liking by clicking the “Edit” button.



To export the dashboard, click the “Export PDF” button.

Troubleshooting Splunk

- If you encounter any problems while running Splunk, follow the link below to access the troubleshooting documentation:
    - https://docs.splunk.com/Documentation/Splunk/9.0.3/Troubleshooting/IntrototroubleshootingSplunk