

Task 1 Guide: Building a Dashboard using Splunk

Download Splunk Enterprise

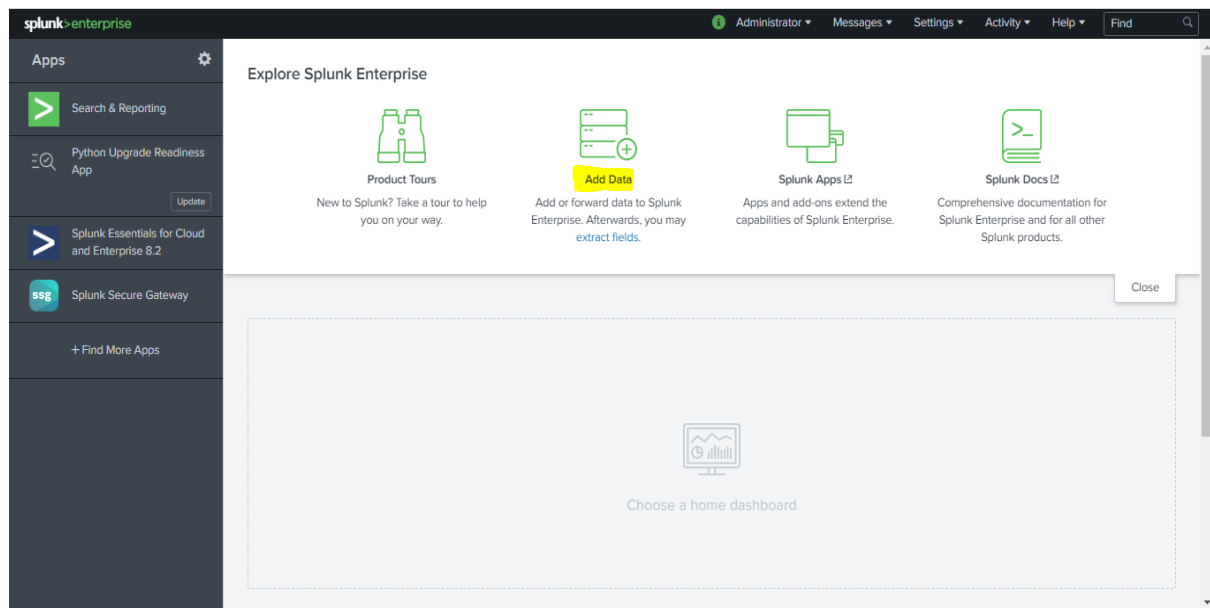
https://www.splunk.com/en_us/download/splunk-enterprise.html

Installing Splunk on Windows

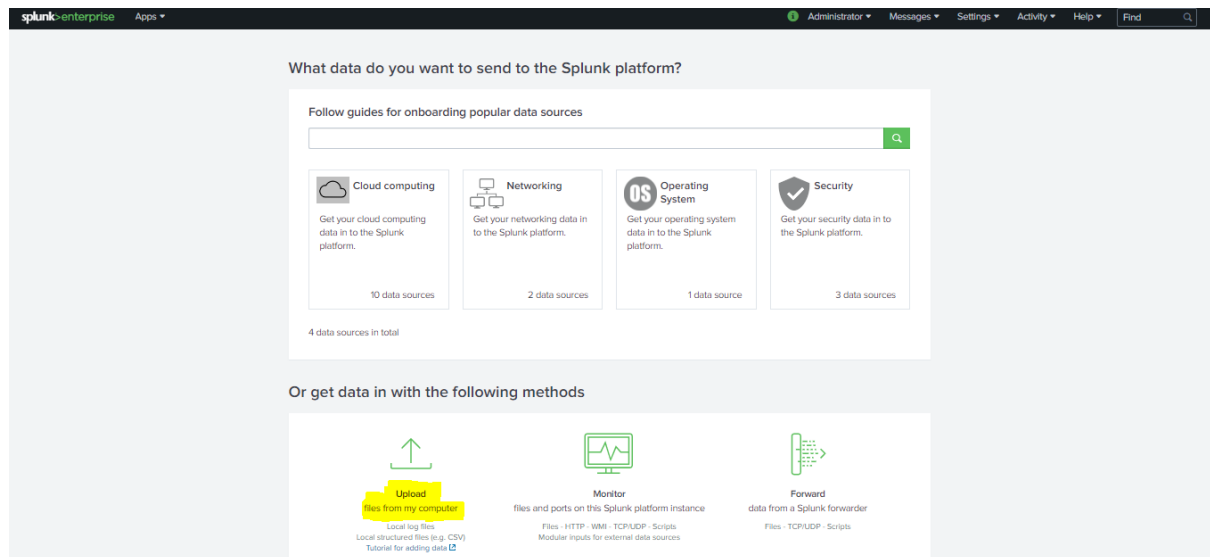
https://www.splunk.com/en_us/resources/videos/installing-splunk-enterprise-on-windows.html

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.

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: `sample_dataset.csv - sample_dataset.csv`

Source type: `csv` Save As

Timestamp

Determine how timestamps for the incoming data are defined.

Extraction Auto Curr... Adva... Con...

> Delimited settings

> Advanced

	_time	age	amount	category	customer	fraud	gender	merchant	step
1	12/06/2022 18:50:26.000	4'	14.48	es_transportation'	C1626806996'	0	M'	M1823072687'	0
2	12/06/2022 18:50:26.000	2'	40.44	es_transportation'	C2001183195'	0	M'	M1823072687'	0
3	12/06/2022 18:50:26.000	1'	21.65	es_transportation'	C118836015'	0	F'	M1823072687'	0
4	12/06/2022 18:50:26.000	2'	63.99	es_transportation'	C395508103'	0	F'	M1823072687'	0
5	12/06/2022 18:50:26.000	2'	21.39	es_transportation'	C1874220848'	0	M'	M348934600'	0

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

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

Add Data Select Source Set Source Type Input Settings Review Done < Back Next >

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **sample_dataset.csv** - sample_dataset.csv [View Event Summary](#)

Source type: csv **Save As**

Timestamp
Determine how timestamps for the incoming data are defined.
Extraction Auto **Cur...** Adv... Con...

> Delimited settings
> Advanced

	_time	age	amount	category	customer	fraud	gender	merchant	step
1	12/06/2022 18:55:00.000	4'	14.48	es_transportation'	C1626806996'	0	M'	M1823072687'	0
2	12/06/2022 18:55:00.000	2'	40.44	es_transportation'	C2001183195'	0	M'	M1823072687'	0
3	12/06/2022 18:55:00.000	1'	21.65	es_transportation'	C118836015'	0	F'	M1823072687'	0
4	12/06/2022 18:55:00.000	2'	63.99	es_transportation'	C395508103'	0	F'	M1823072687'	0
5	12/06/2022 18:55:00.000	2'	21.39	es_transportation'	C1874220848'	0	M'	M348934600'	0

Click on "Next" until you get the result below.

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

Add Data Select Source Set Source Type Input Settings Review **Done** < Back Next >

✓ **File has been uploaded successfully.**
Configure your inputs by going to [Settings > Data Inputs](#)

Start Searching Search your data now or see [examples and tutorials](#).

Extract Fields Create search-time field extractions. [Learn more about fields.](#)

Add More Data Add more data inputs now or see [examples and tutorials](#).

Download Apps Apps help you do more with your data. [Learn more.](#)

Build Dashboards Visualize your searches. [Learn more.](#)

Analysing the Data

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

New Search

source=sample_dataset.csv | sample_dataset.csv host=LAPTOP-0UJAQK5 source=sample_dataset.csv sourcetype=fraud_detection.csv

✓ 50 events (before 12/06/2022 19:13:51.000) No Event Sampling

Format Timeline Zoom Out Zoom to Selection Deselect

1 millisecond per column

Raw	Format	20 Per Page
< Hide Fields	All Fields	i Event
SELECTED FIELDS		> 49,1,C616528518',4',F',28007',M1823072687',28007',es_transportation',26.93,1
a host 1		> 48,1,C1499363341',5',M',28007',M1823072687',28007',es_transportation',14.46,0
a source 1		> 47,1,C123623130',2',F',28007',M349281107',28007',es_fashion',22.44,0
a sourcetype 1		> 46,1,C650108285',4',F',28007',M1823072687',28007',es_transportation',50.73,0
INTERESTING FIELDS		> 45,1,C1753498738',3',F',28007',M1823072687',28007',es_transportation',20.53,0
a age 7		> 44,1,C748358246',2',M',28007',M1823072687',28007',es_transportation',51.17,0
# amount 50		> 43,1,C1904086644',5',F',28007',M1823072687',28007',es_transportation',26.93,0
a category 6		> 42,1,C728039227',6',M',28007',M1823072687',28007',es_transportation',30.84,0
a customer 47		> 41,1,C728039227',6',M',28007',M34934600',28007',es_transportation',27.93,0
# fraud 2		> 40,1,C1039390058',4',M',28007',M45060432',28007',es_hotelservices',190.31,0
a gender 3		> 39,1,C1039390058',4',M',28007',M352454843',28007',es_hotelservices',224.81,1
a index 1		> 38,1,C575345520',2',F',28007',M34934600',28007',es_transportation',7.4,0
# linecount 1		> 37,1,C40869006',1',M',28007',M85975013',28007',es_food',43.04,0
a merchant 9		> 36,1,C1990073844',4',M',28007',M1823072687',28007',es_transportation',29.37,0
a punct 1		> 35,1,C423891632',5',M',28007',M1823072687',28007',es_transportation',2.32,0
a splunk_server 1		> 34,1,C1007572087',2',F',28007',M1823072687',28007',es_transportation',35.3,0
# step 2		
a timestamp 1		
a zipCodeOn 1		
a zipMerchant 1		
+ Extract New Fields		

Creating the Dashboard

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

New Search

sourcetype=fraud_detection.csv

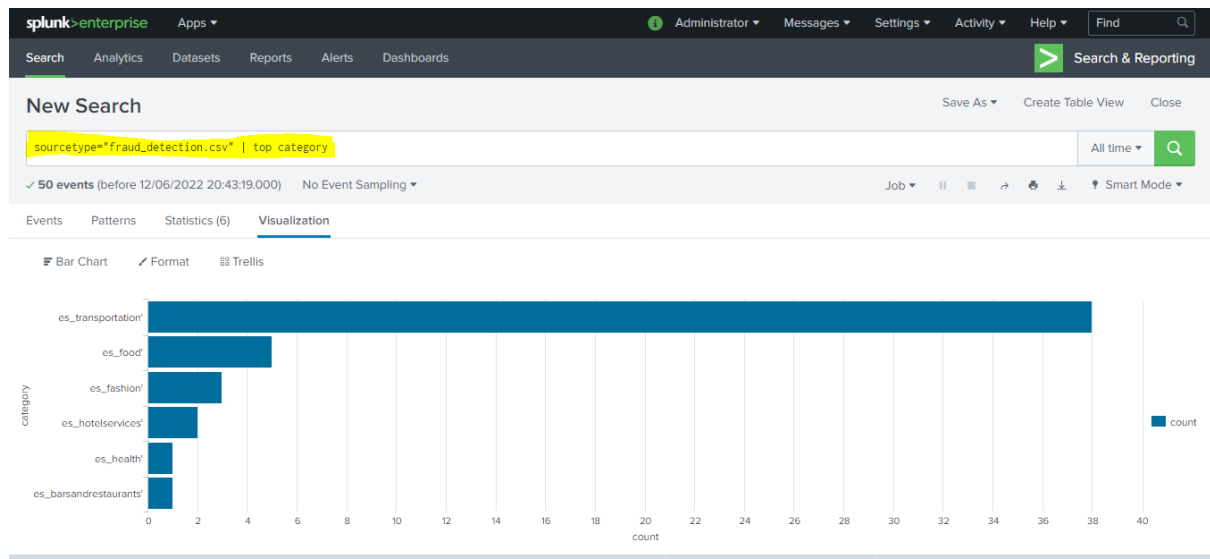
✓ 50 events (before 12/06/2022 19:13:51.000) No Event Sampling

Format Timeline Zoom Out Zoom to Selection Deselect

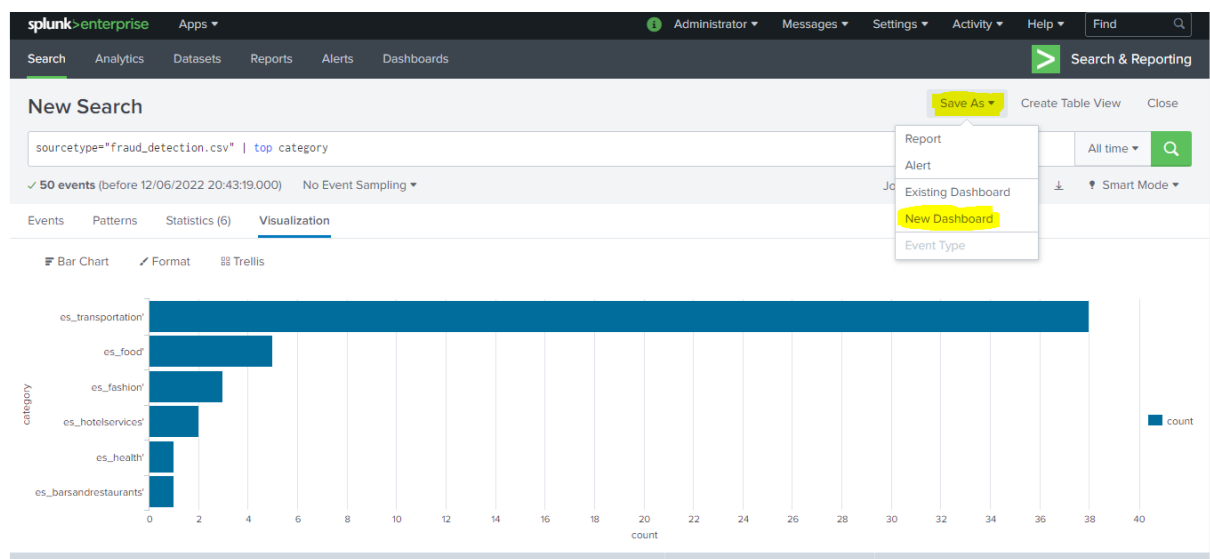
1 millisecond per column

Raw	Format	20 Per Page
< Hide Fields	All Fields	i Event
SELECTED FIELDS		> 49,1,C616528518',4',F',28007',M1823072687',28007',es_transportation',26.93,1
a host 1		> 48,1,C1499363341',5',M',28007',M1823072687',28007',es_transportation',14.46,0
a source 1		> 47,1,C123623130',2',F',28007',M349281107',28007',es_fashion',22.44,0
a sourcetype 1		> 46,1,C650108285',4',F',28007',M1823072687',28007',es_transportation',50.73,0
INTERESTING FIELDS		> 45,1,C1753498738',3',F',28007',M1823072687',28007',es_transportation',20.53,0
a age 7		> 44,1,C748358246',2',M',28007',M1823072687',28007',es_transportation',51.17,0
# amount 50		
a category 6		

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:



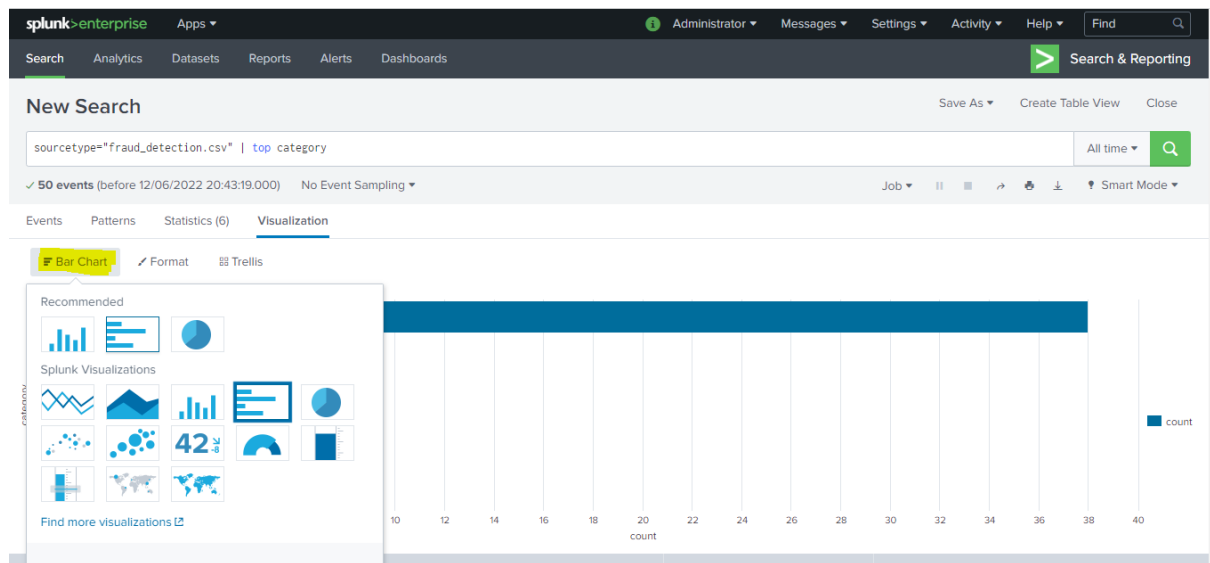
To add this chart to your dashboard, go to “Save As > New Dashboard > Dashboard Title = “Fraud Detection Dashboard” > Classic Dashboards > Save to Dashboard. This creates your dashboard.



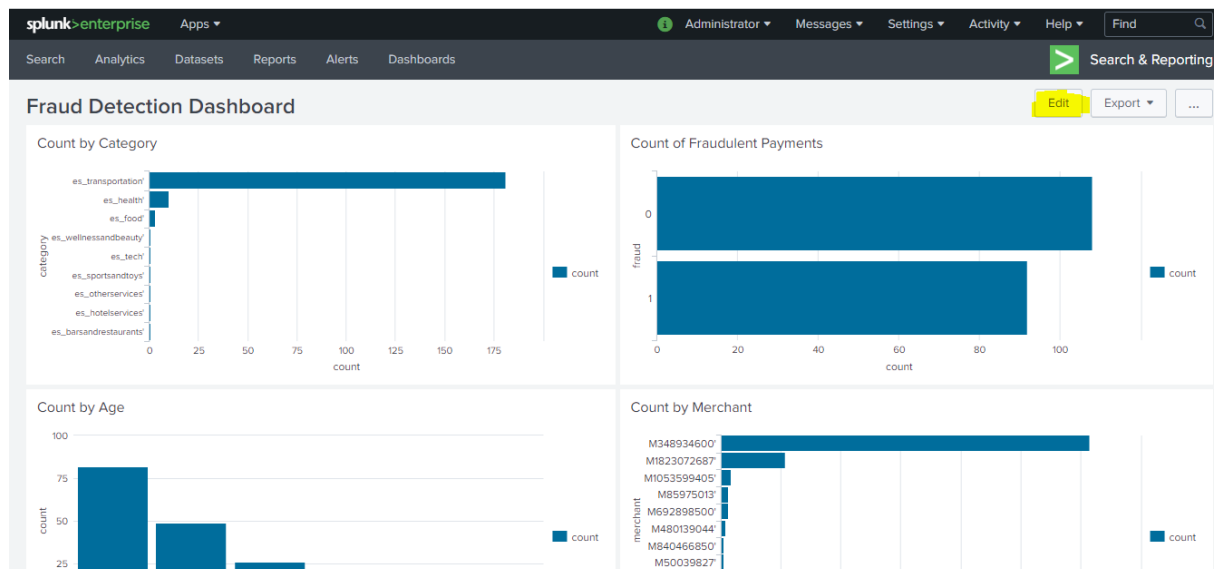
To get “Fraud detected by category”, type ***sourcetype="practicesplunk.csv" fraud="1" | stats count values(fraud) by category*** in the search field. This counts the number of fraudulent activities recorded for each category.

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>