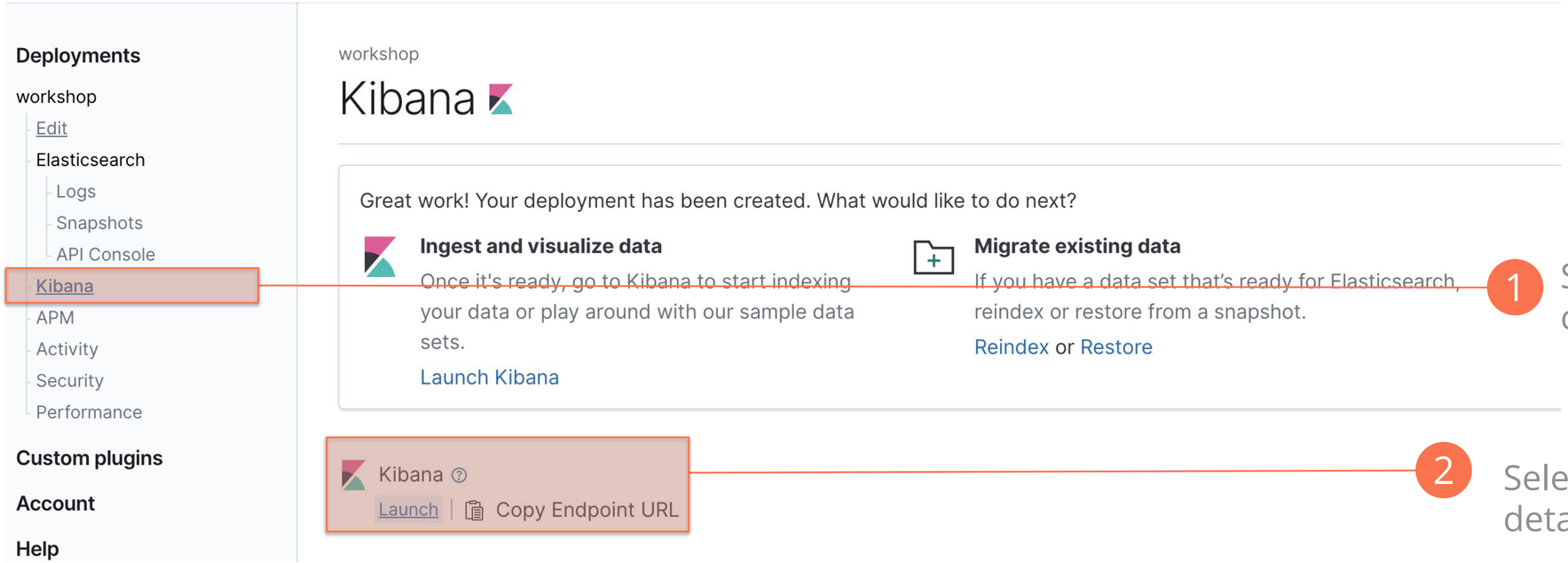
Lab 3

Finding MITRE ATT&CK™ TTPs

elastic

Launch Kibana from Cloud

Login to cloud.elastic.co account created in lab #1



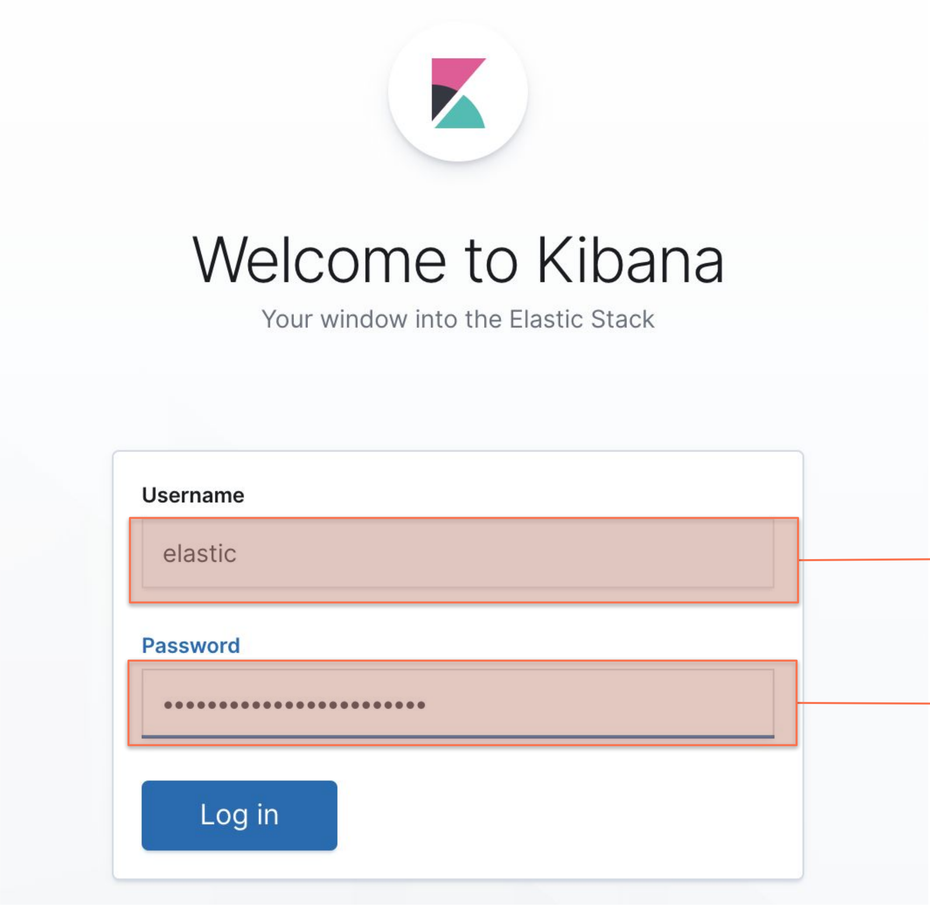
1 Select Kibana under the newly created deployment.

2 Select Launch in the Kibana details.

elastic

Log into Kibana

Setting Time Ranges

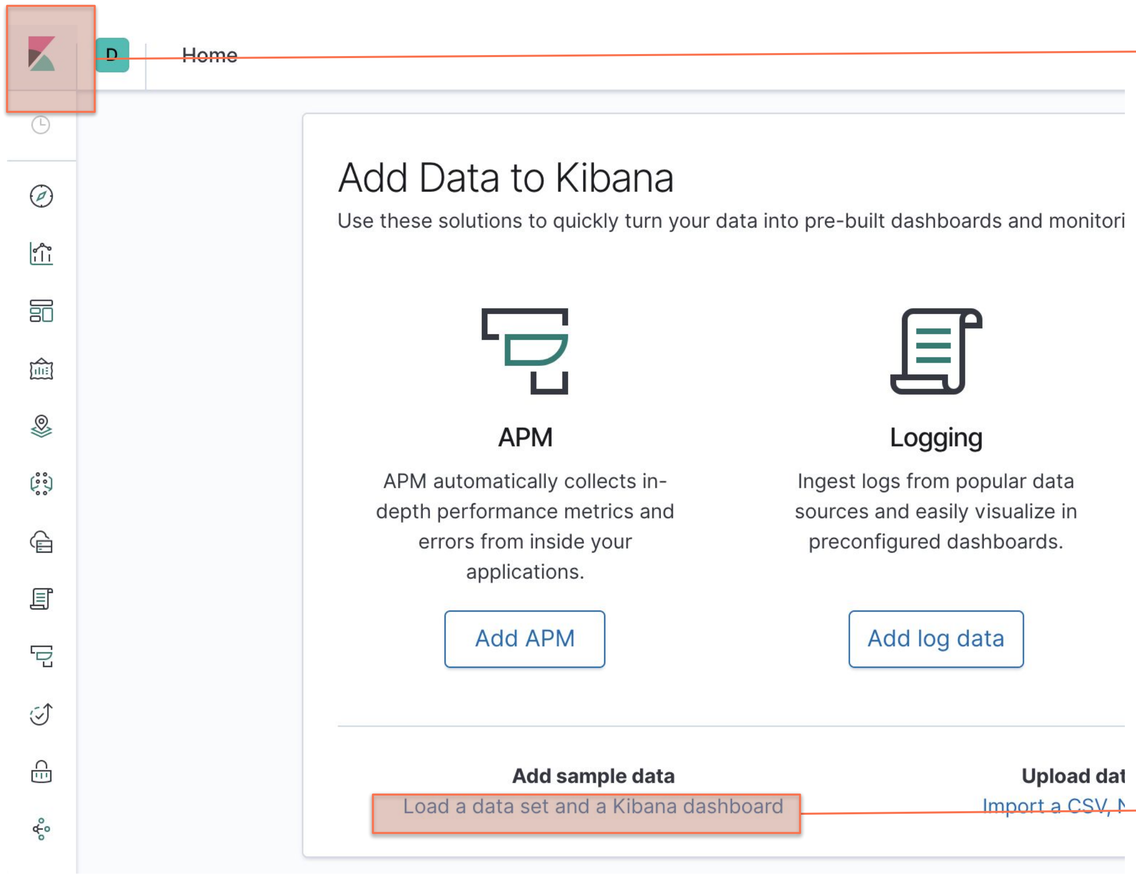


1. Username is: elastic
2. Copy-n-Paste the Cloud elastic user password saved in Lab #1.

elastic

Load Sample Data in Kibana

Kibana load data page



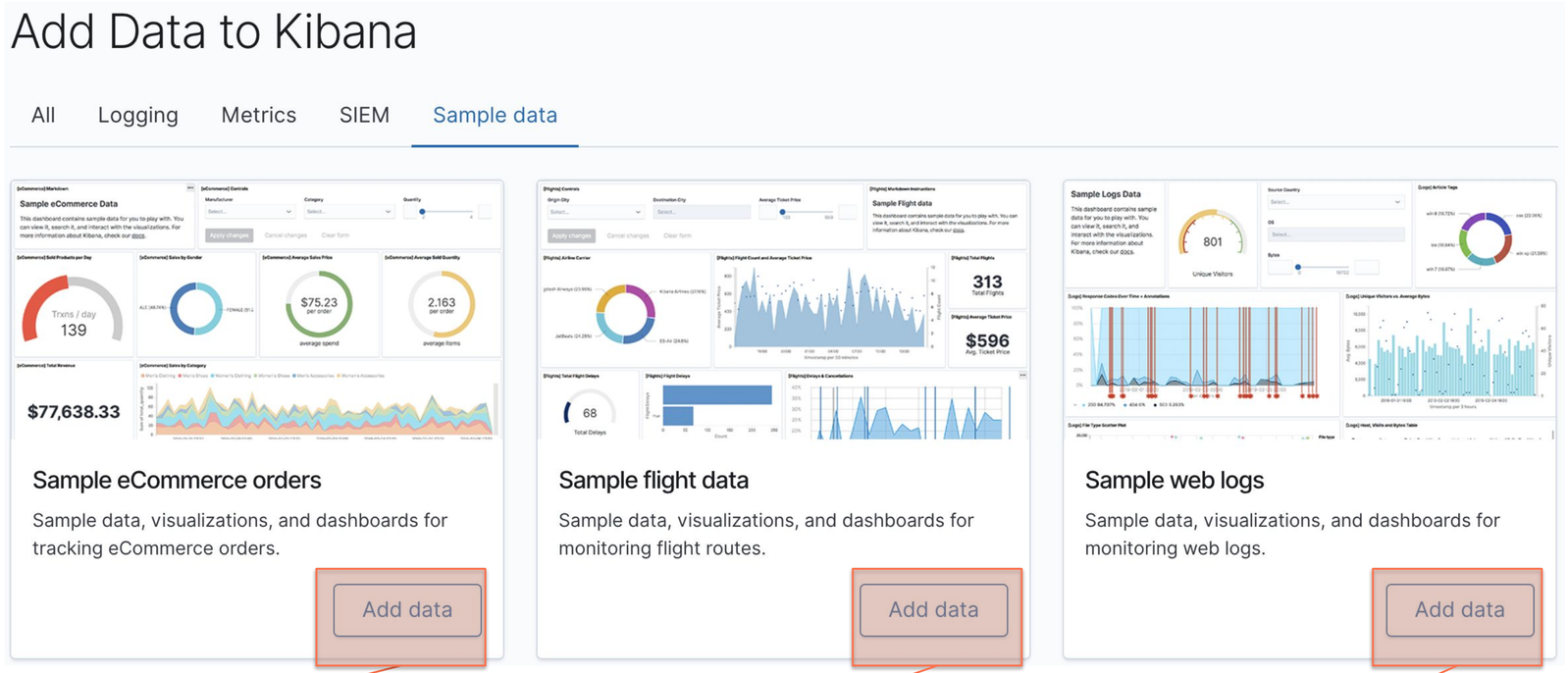
1 Select the ‘K’ icon.

2 Select ‘Load a data..’ link under ‘Add sample data’.

elastic

Loading sample data into the Elastic Stack

Load all three data sets

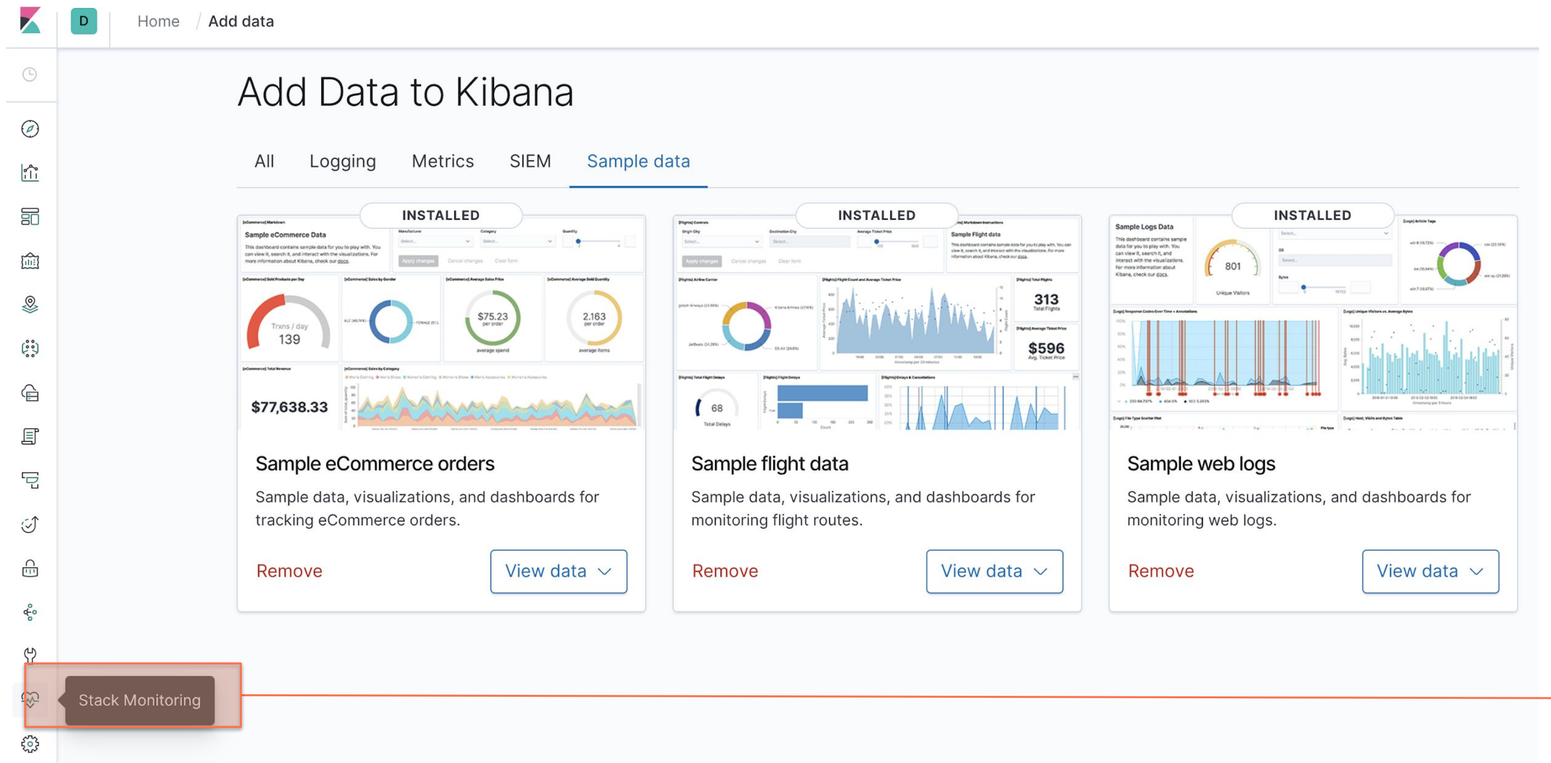


1. Add Sample eCommerce orders
2. Add Sample flight data
3. Add Sample web logs

elastic

Navigate to Stack Monitoring

Second icon (heart) from the bottom left Navigation menu

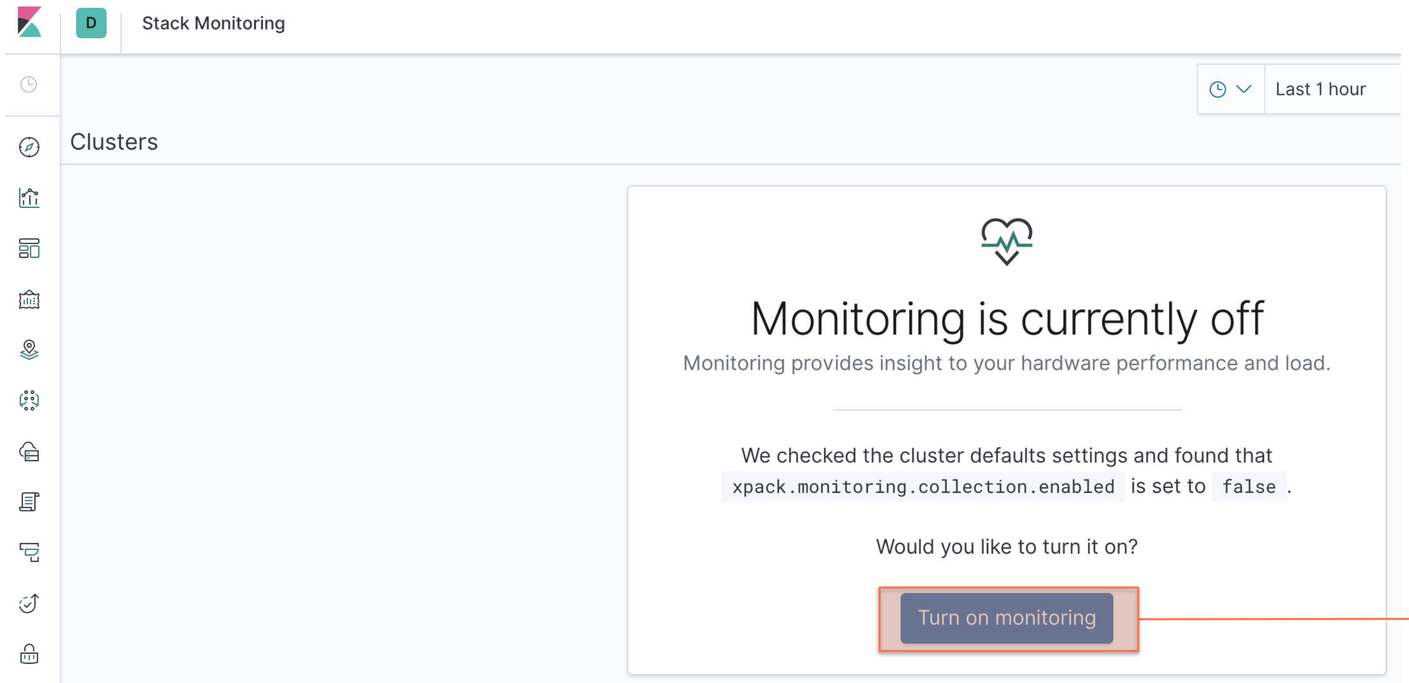


1 Select Stack Monitoring

elastic

Enable Stack Monitoring

Stack monitoring lets you understand Elastic Cloud cluster perfomance

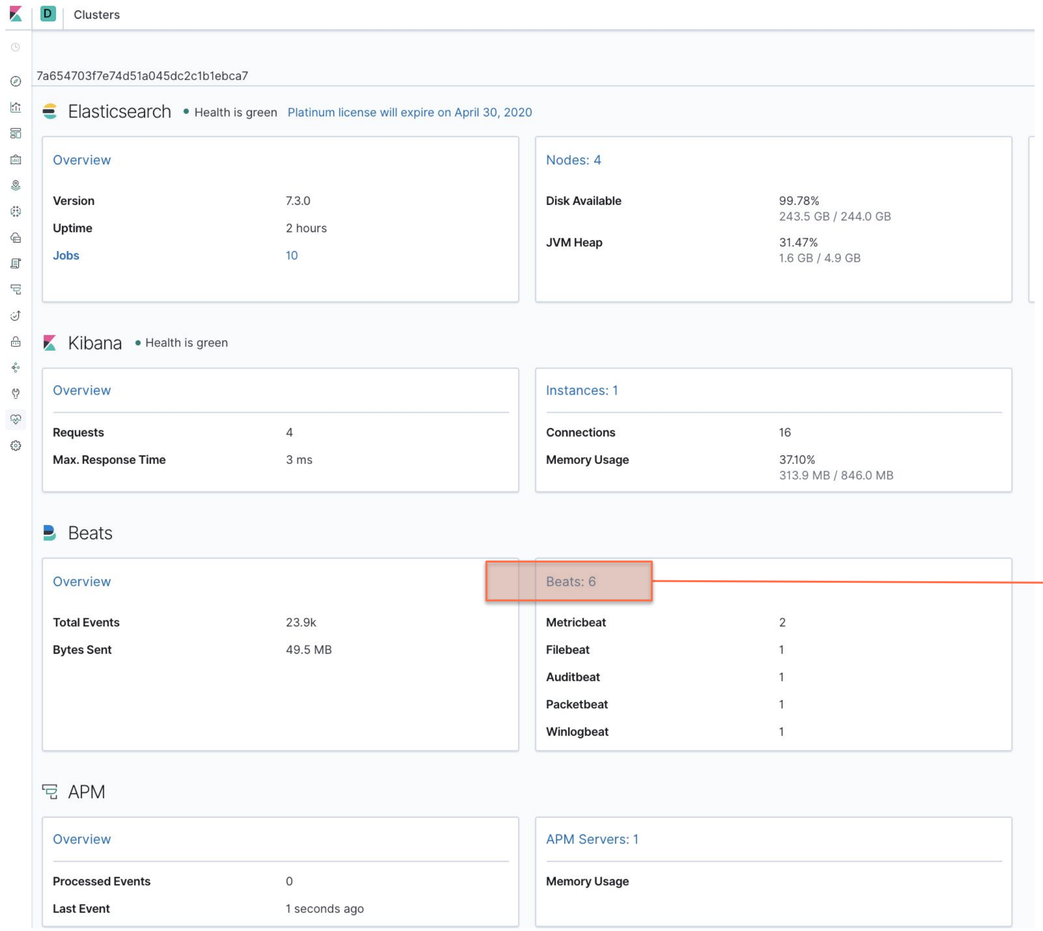


1 Select Turn on monitoring

elastic

Ensure your Beats agents are online

After a few minutes, you should see 6 beats enabled

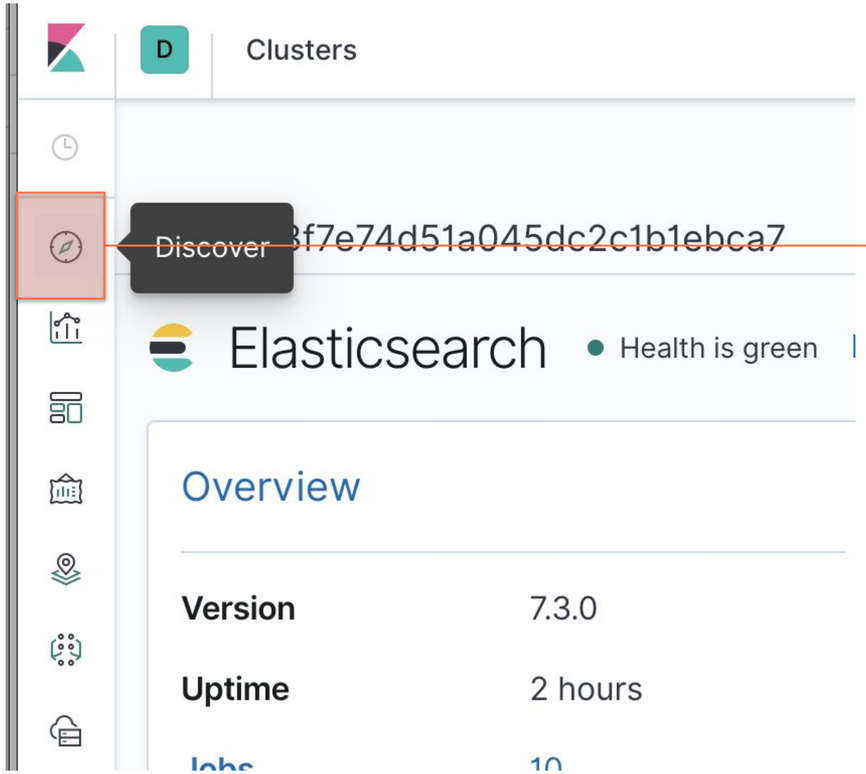


1 Six Beats should be enabled

elastic

Move to the Discover app

Discovering what is in the data

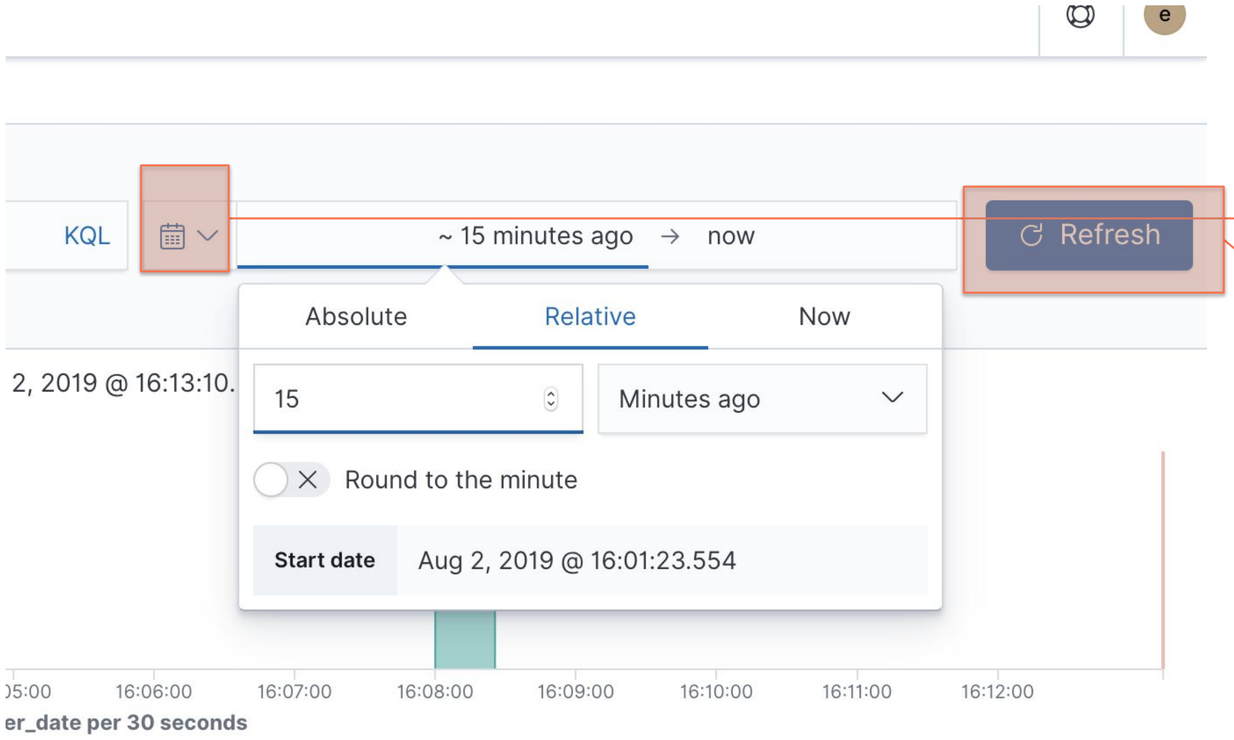


1 Select ‘Discover”

elastic

Setting the time range

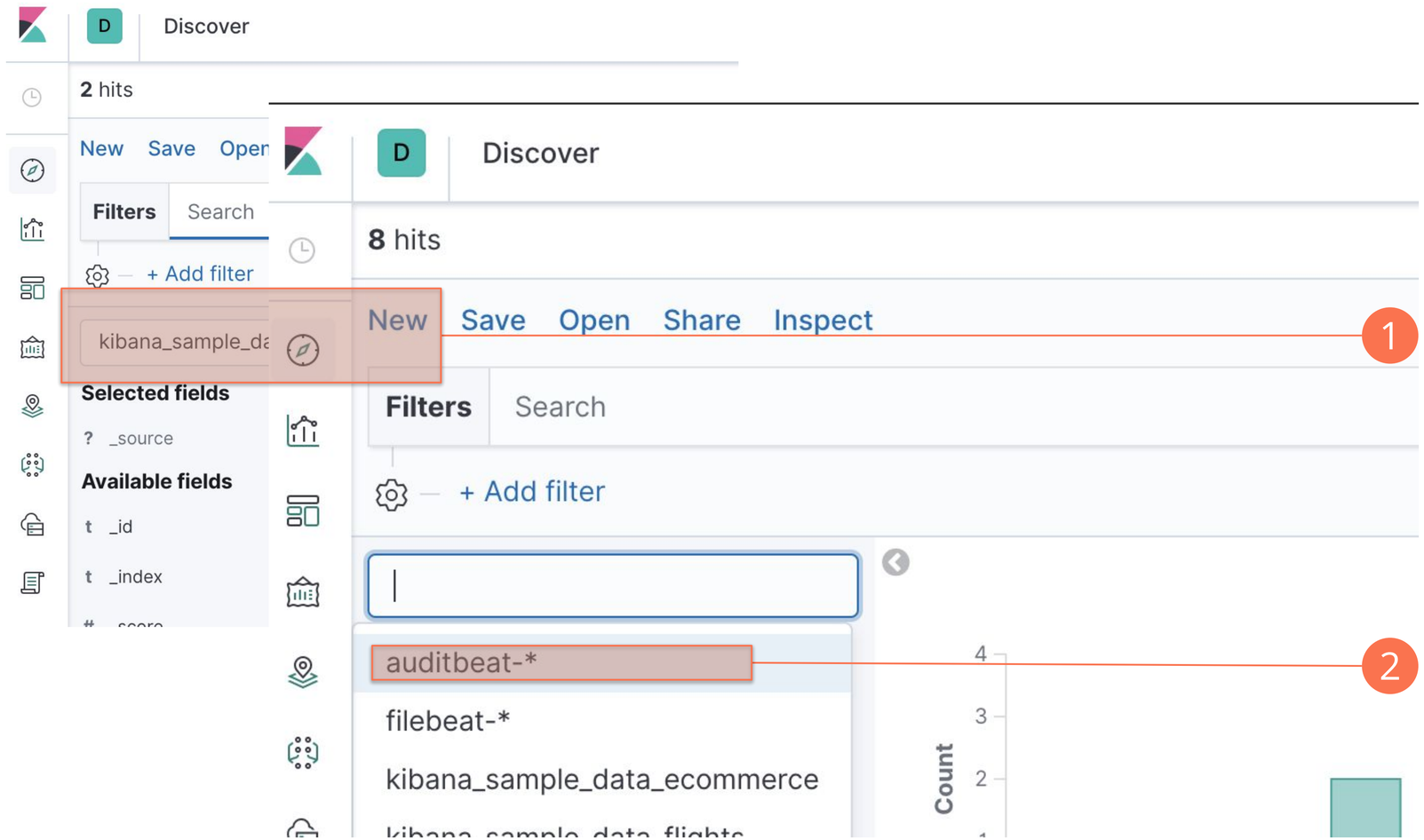
Ensure kibana is set to the last 15 minutes



1. Select the calendar icon, Then set the last 15 minutes
2. Select Refresh

Select the index

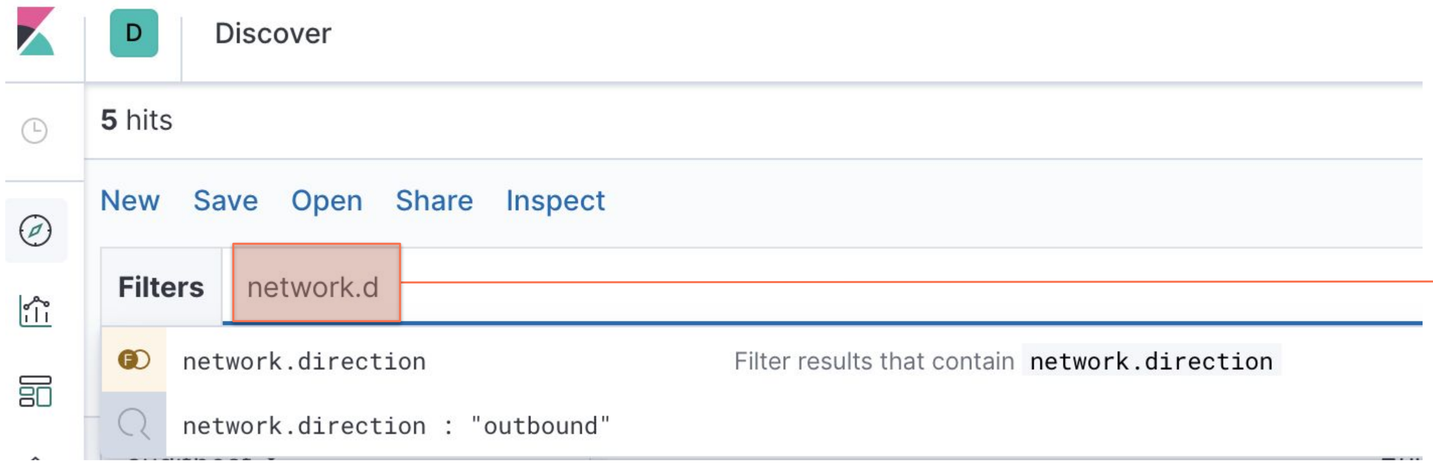
Kibana has multiple indices, select auditbeat



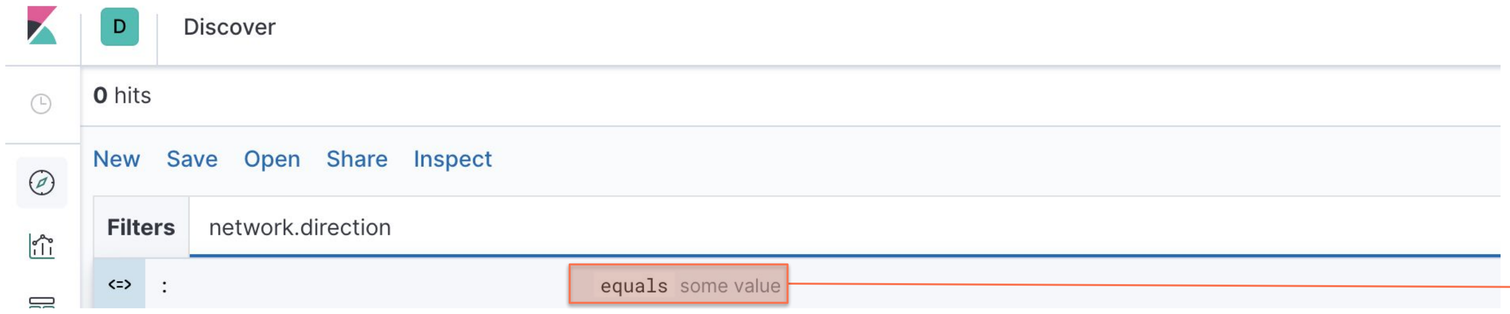
elastic

Search with KQL in Kibana

The default way to search



1 Type ‘network.d’ and select network.direction from the drop down menu

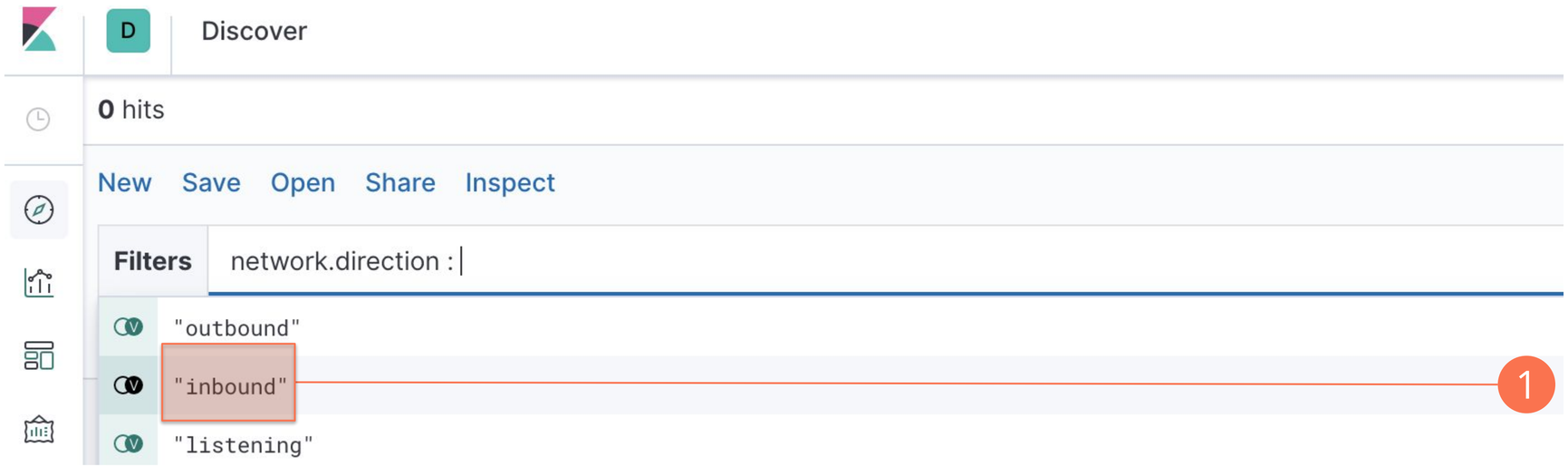


2 Select ‘equals some value’

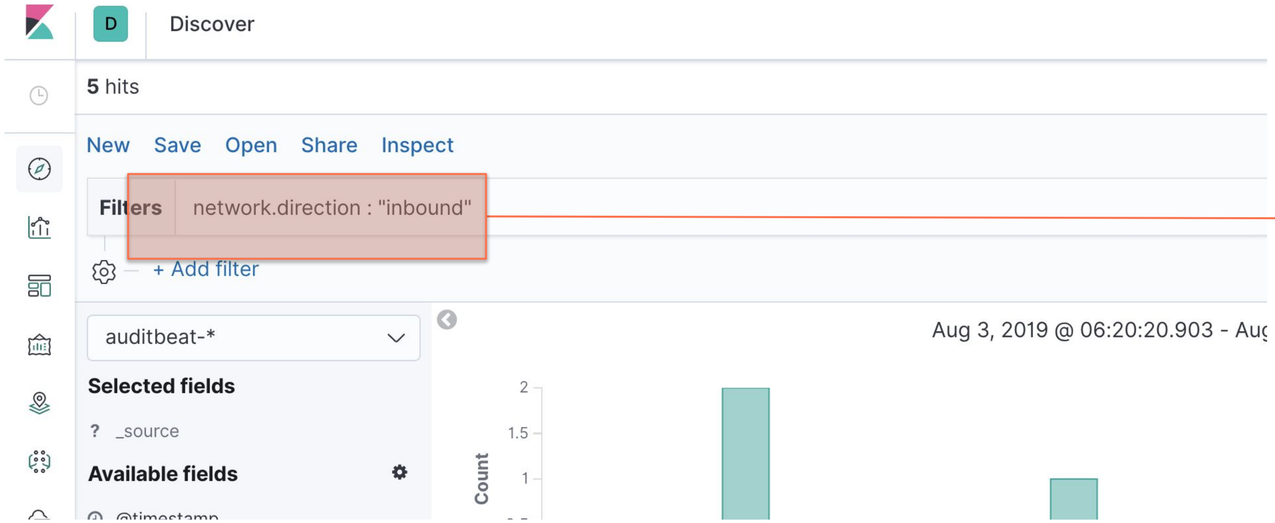
elastic

Search with KQL in Kibana

search with autocomplete



1 Select ‘ inbound’

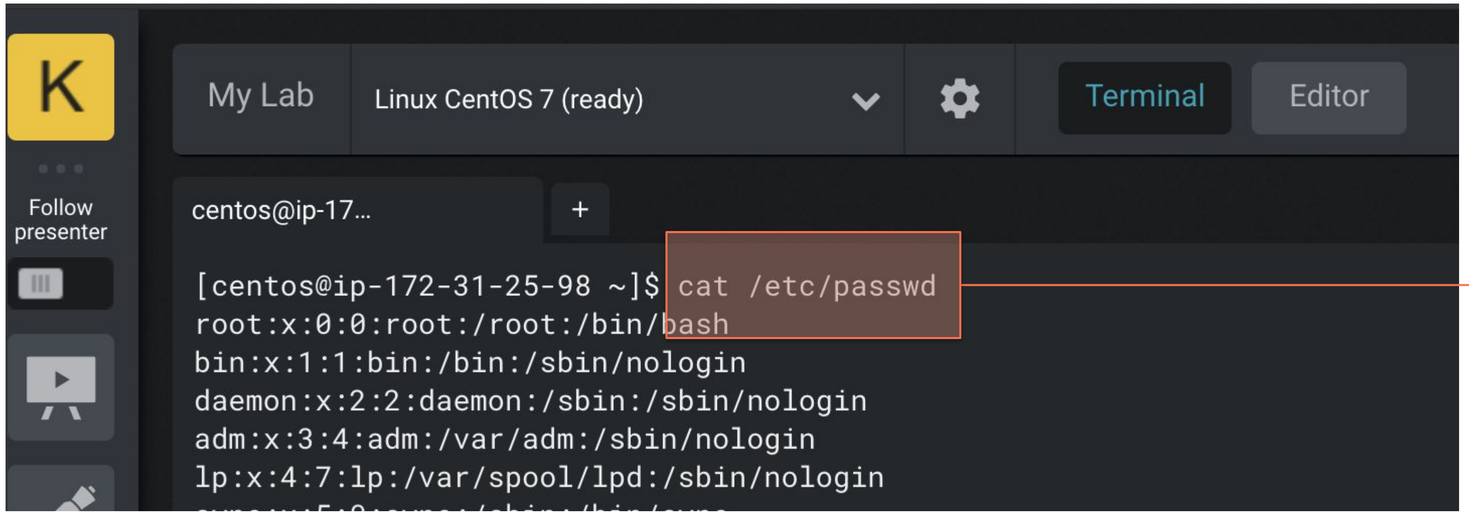


2 Results are filtered for inbound

elastic

ATT&CK Technique T1078 Valid Accounts

in strigo’s Linux lab terminal: cat /etc/passwd

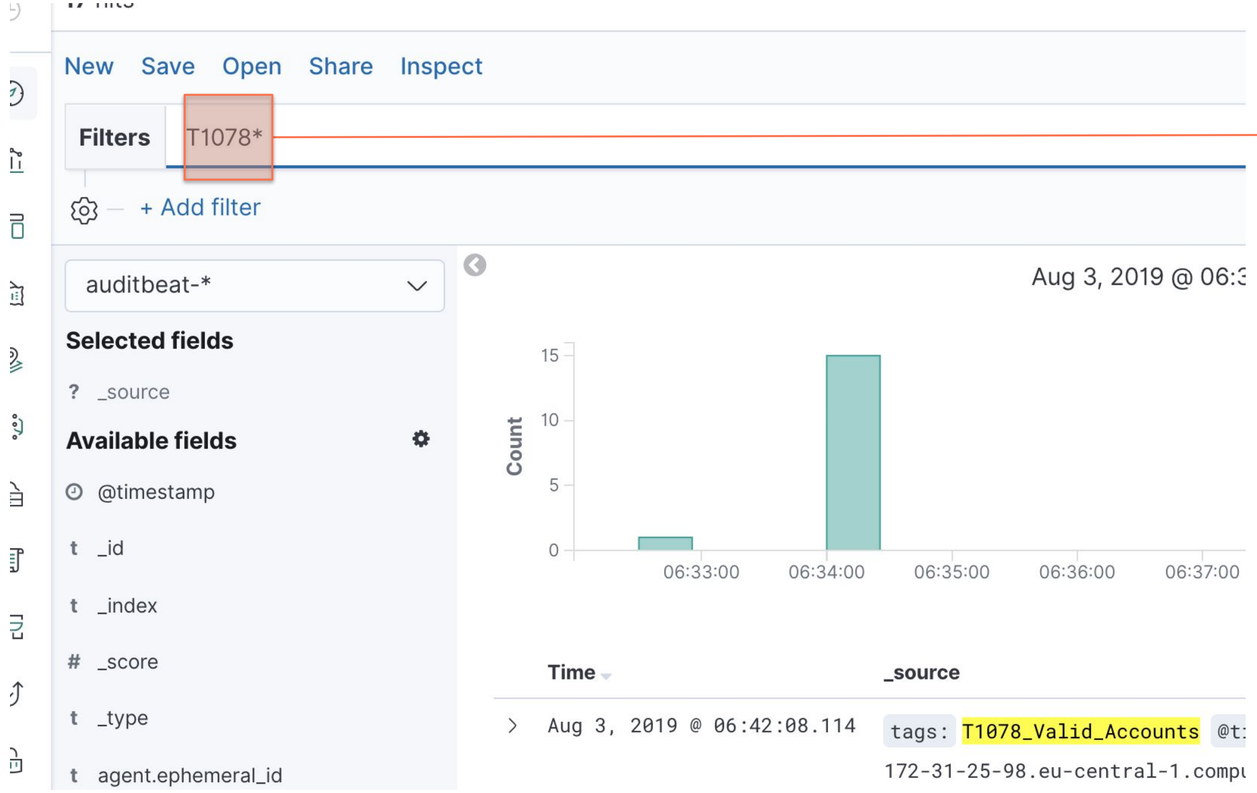


1 Type ‘cat /etc/passwd’ in the terminal

elastic

Find T1078 events

Search using wildcards



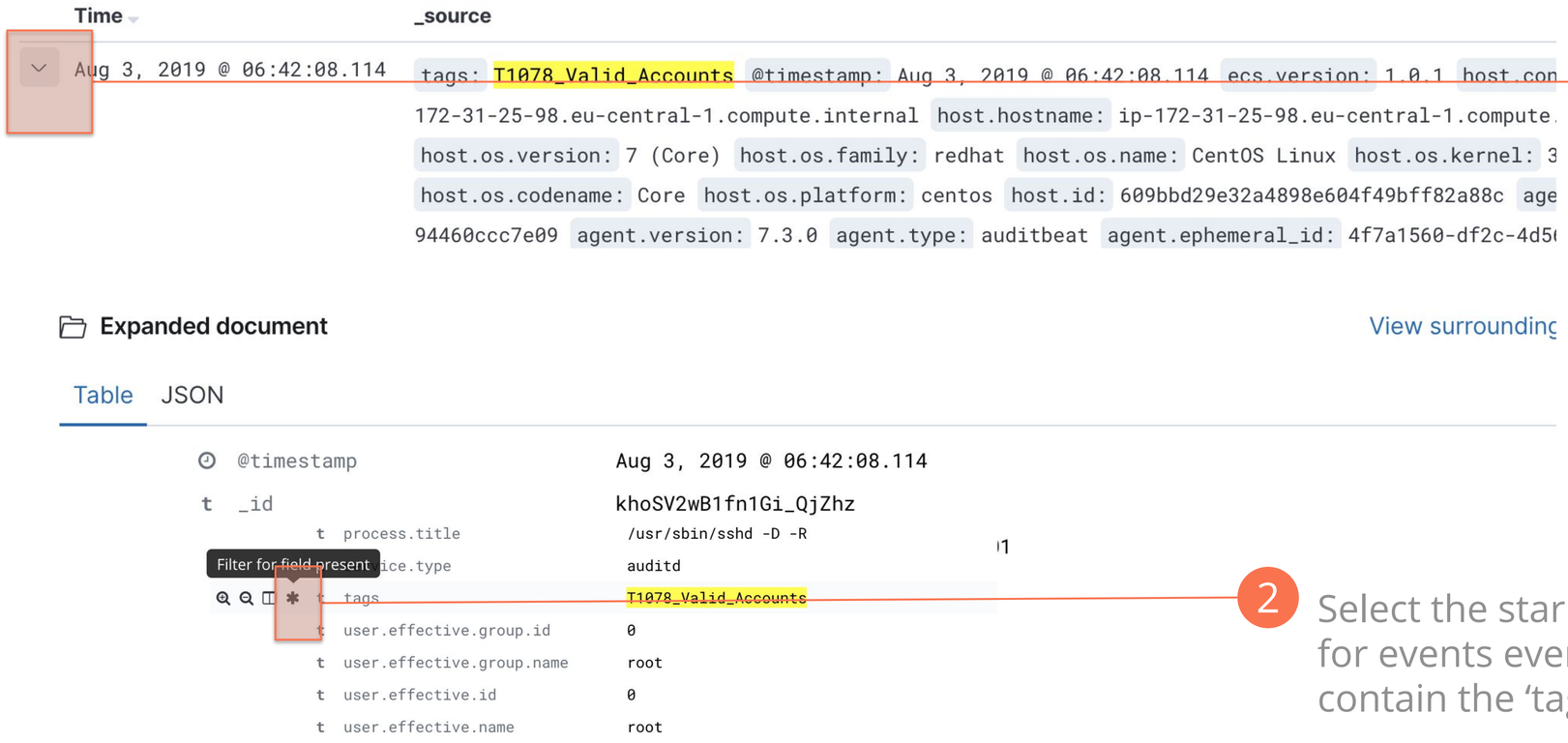
1 Search for ‘T1078’

2 Pro Tip: Avoid using ‘*’ as a prefix without a key (e.g. ‘*1078’)

elastic

Inspect an event

review the fields in an event, filter on ‘contains tag’



1 Select the drop down arrow icon next to a matching event.

2 Select the star icon to filter for events events that contain the ‘tags’ field

elastic

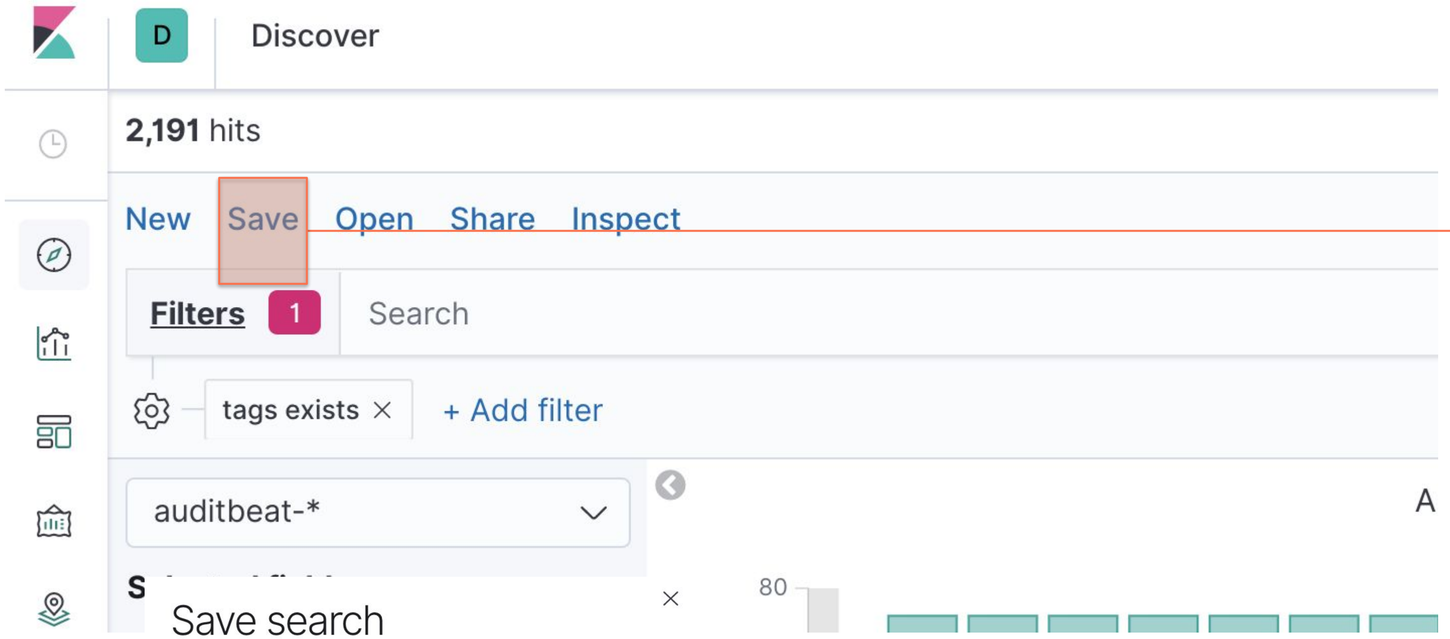
Apply tag exists filter

clear the search box and refresh to see only results that contain ‘tag’

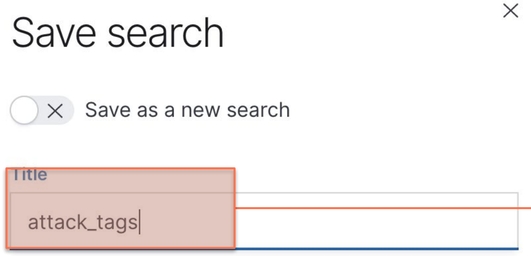
elastic

Create a saved search

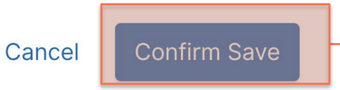
save your tags filter for reuse



1 Select Save



2 Name your saved search ‘attack_tags’

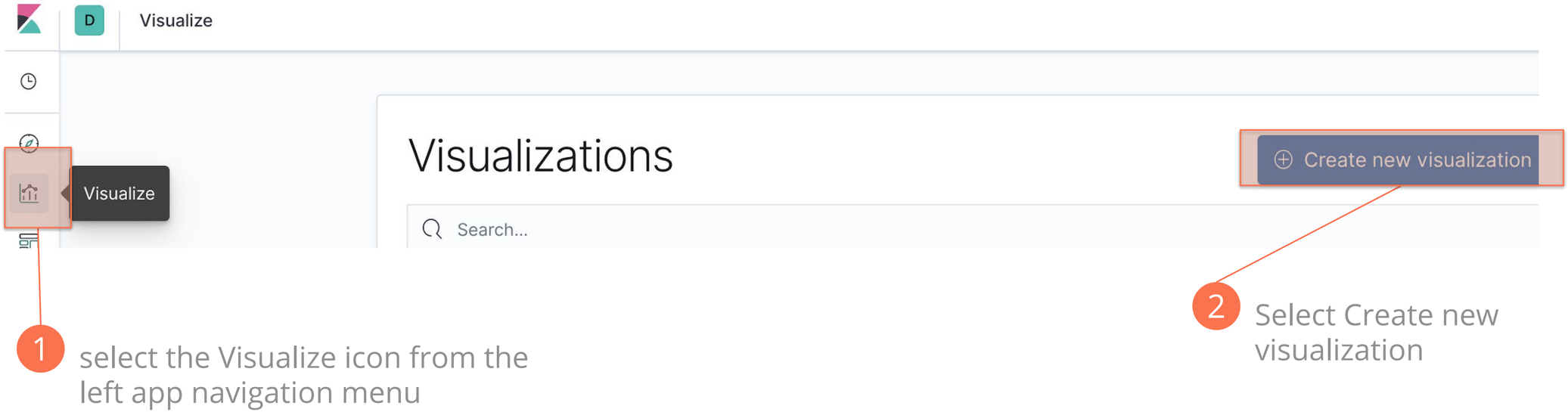


3 Select save

elastic

Start creating a new visualization

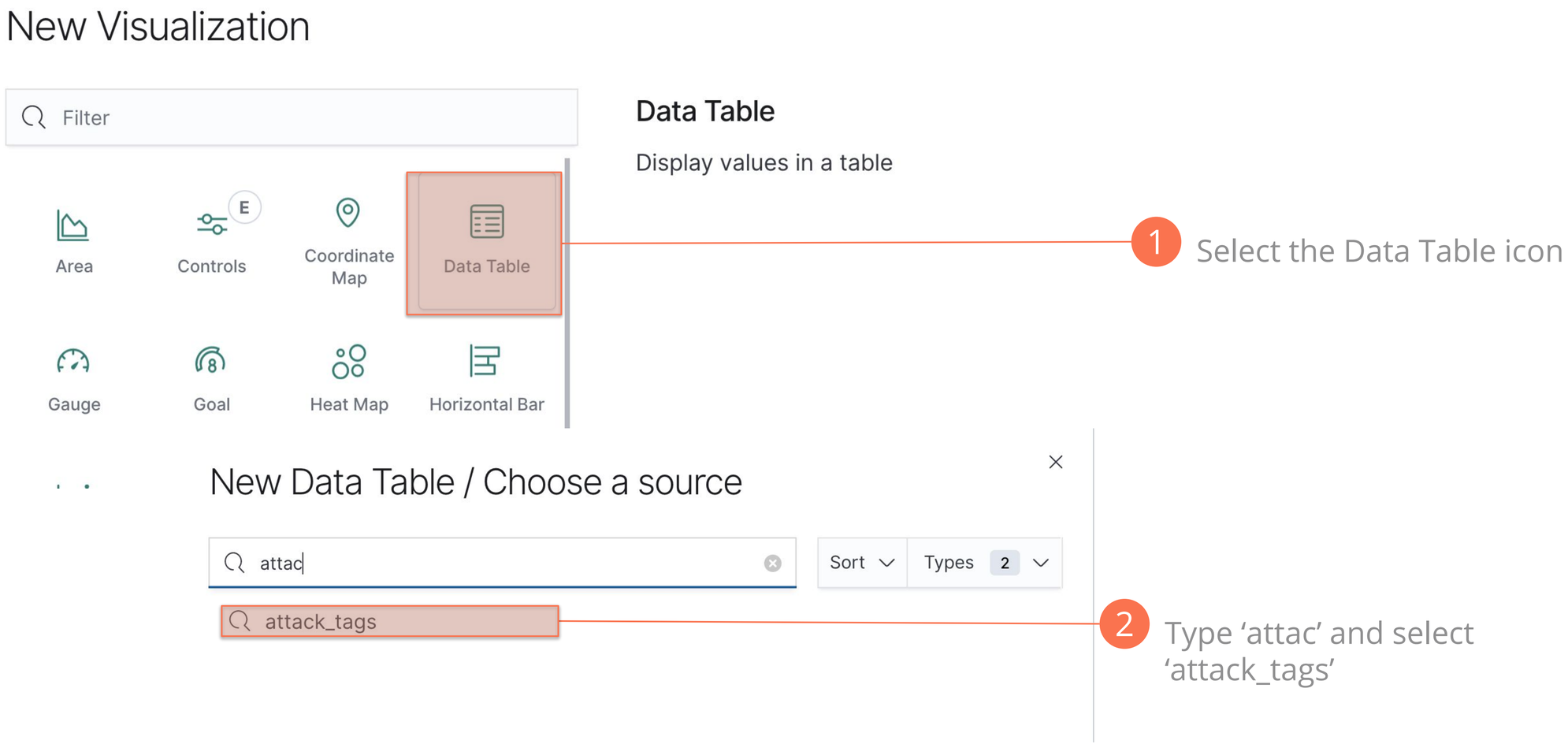
create a new visualization in the Visualize Kibana app



elastic

Create a new data table visualization

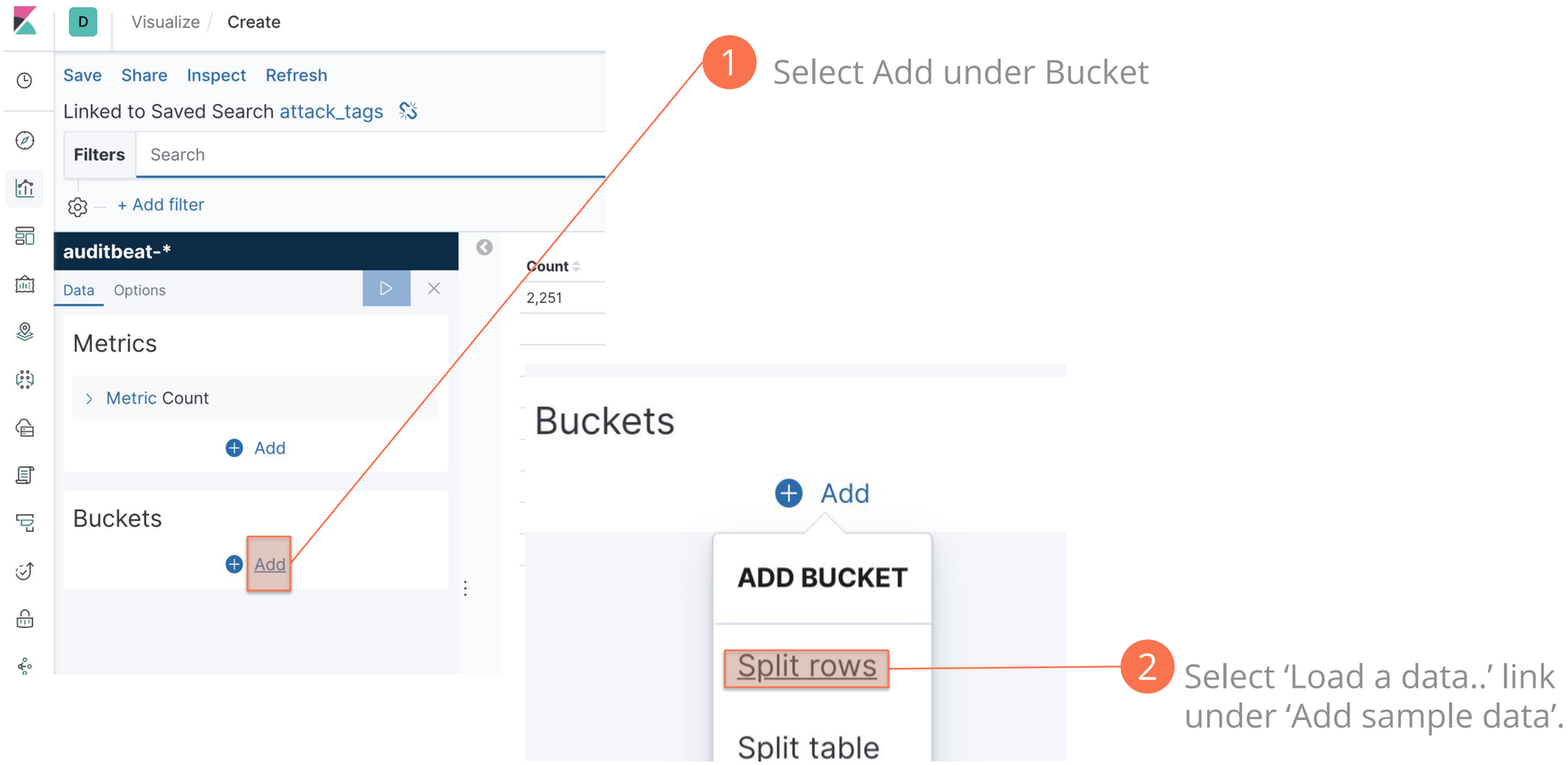
reuse your ‘attack_tags’ saved search



elastic

Editing Data Table

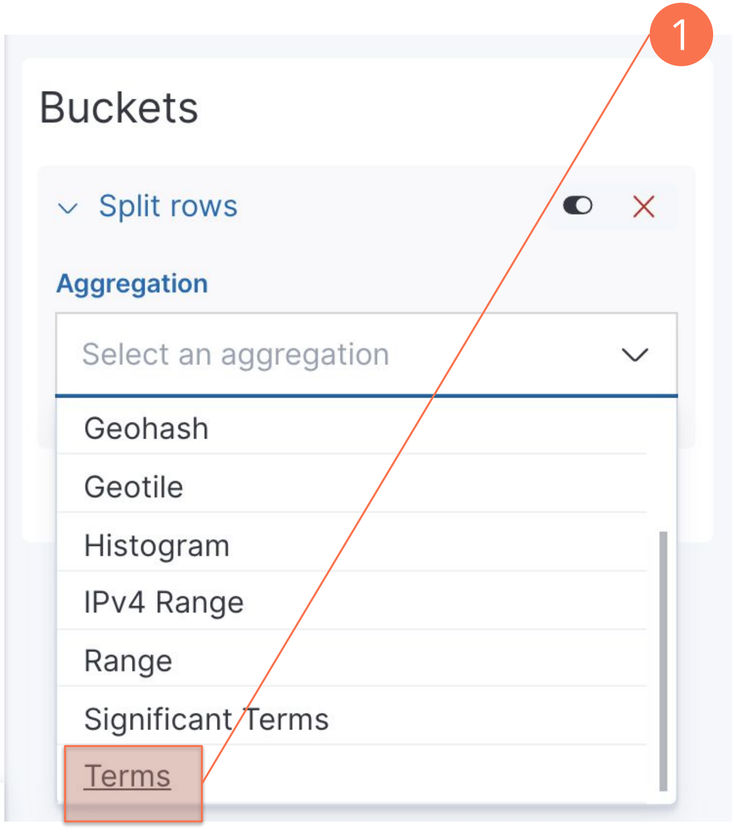
split rows



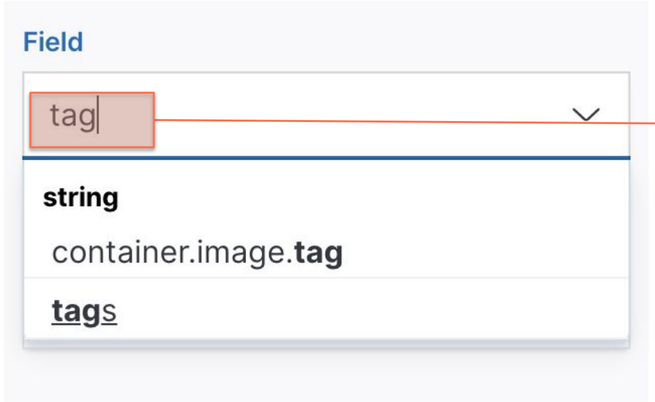
elastic

Editing Data Table

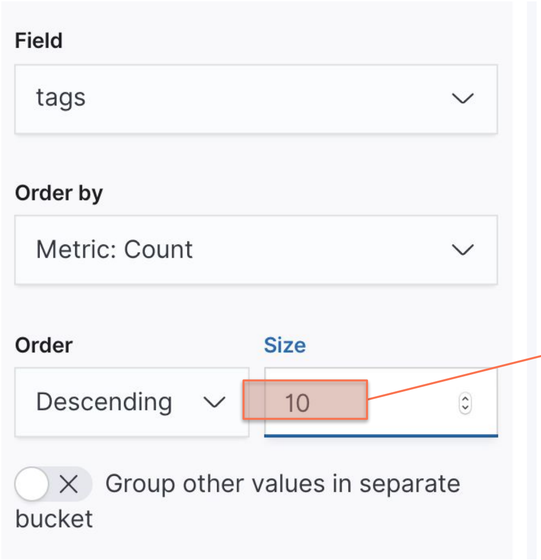
use terms



1 Select the Terms Aggregation



2 Type ‘tags’ and select it for Aggregation Field

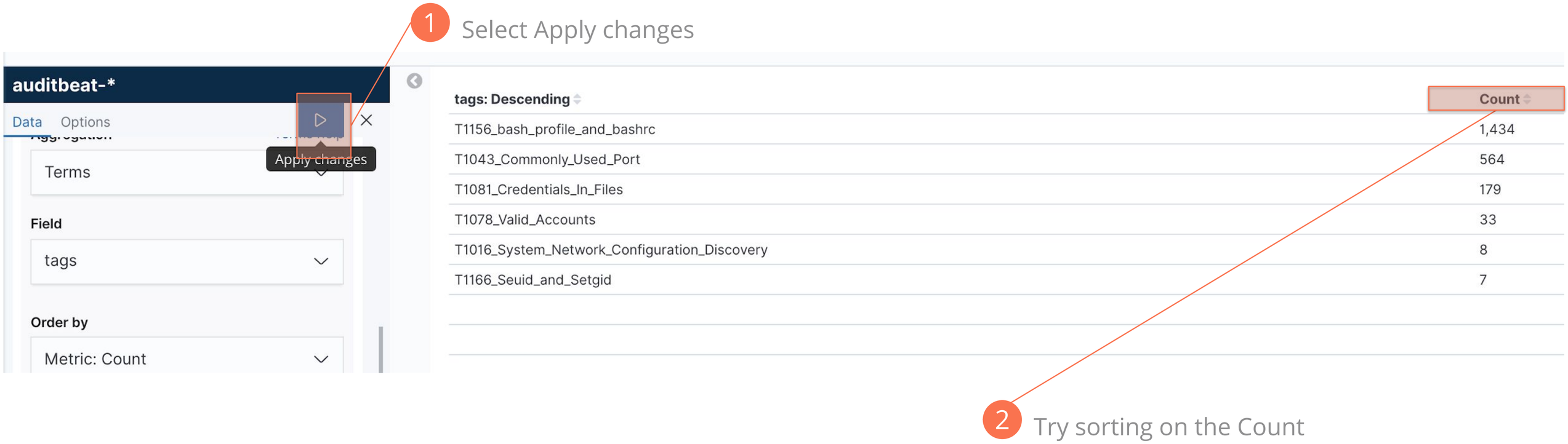


3 Set the display Size to 10

elastic

See your updated data table visualization

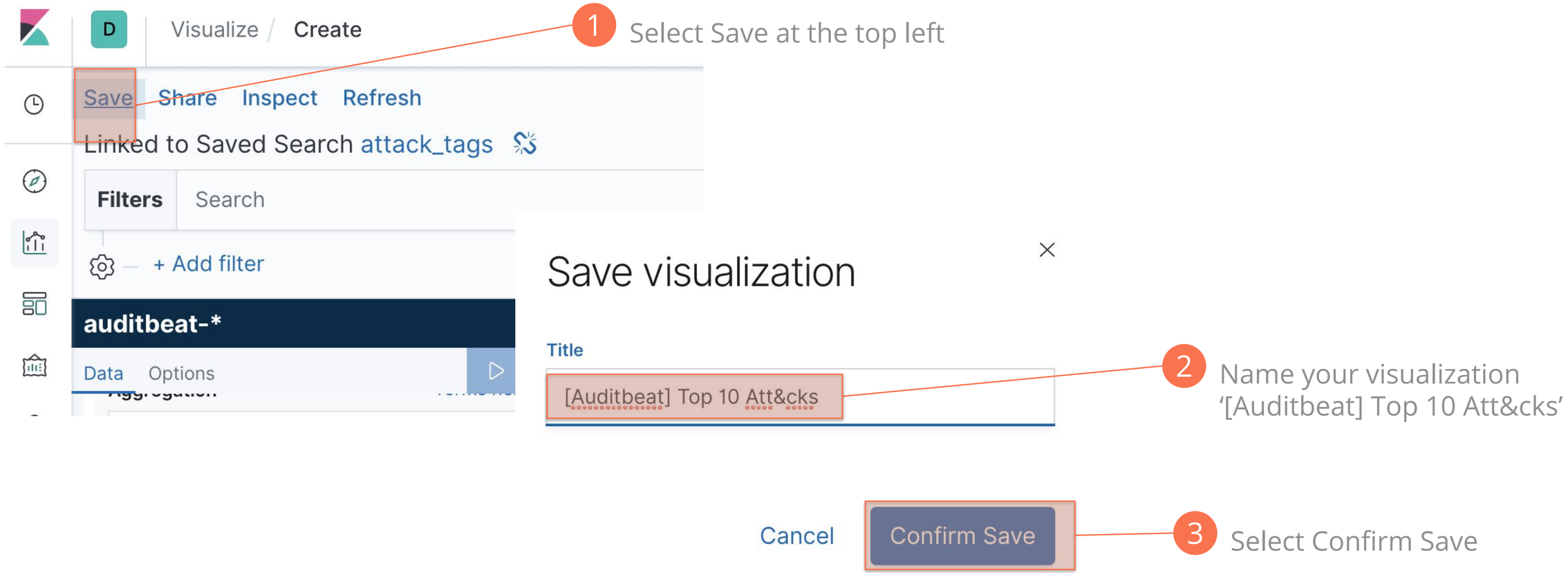
apply you changes



elastic

Save your visualization

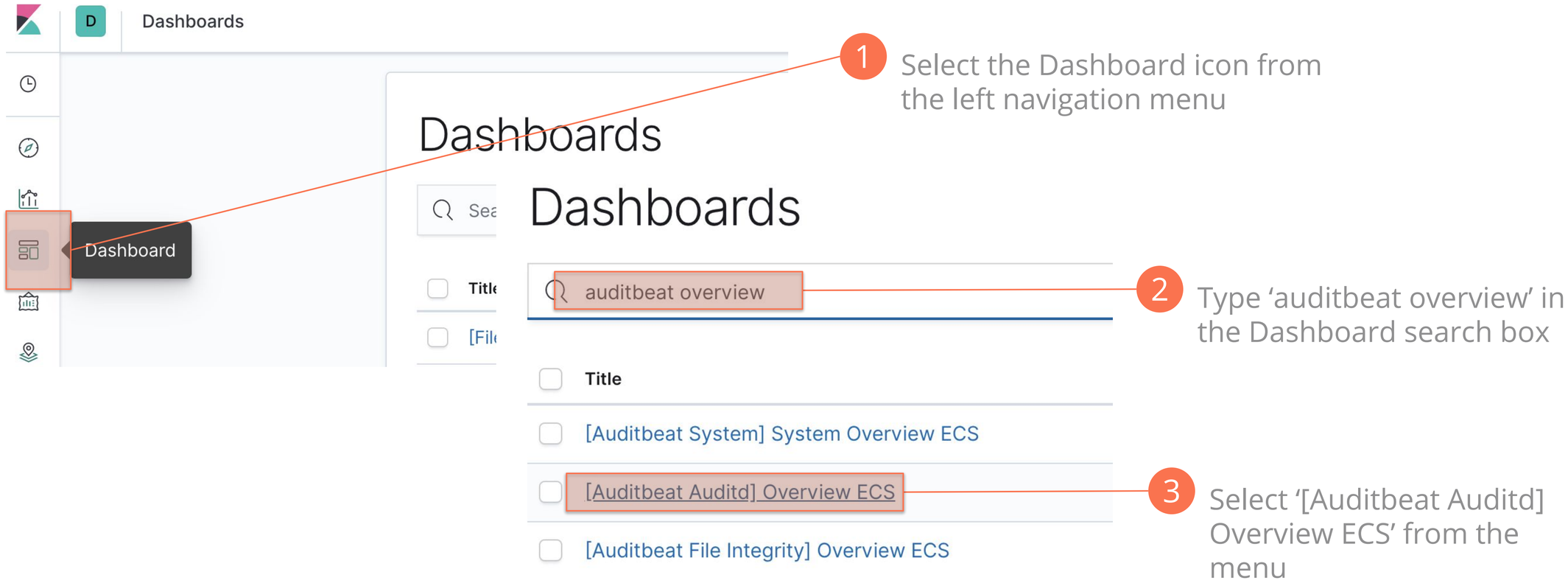
Save your visualization for reuse



elastic

Add visualization to Auditbeat Overview

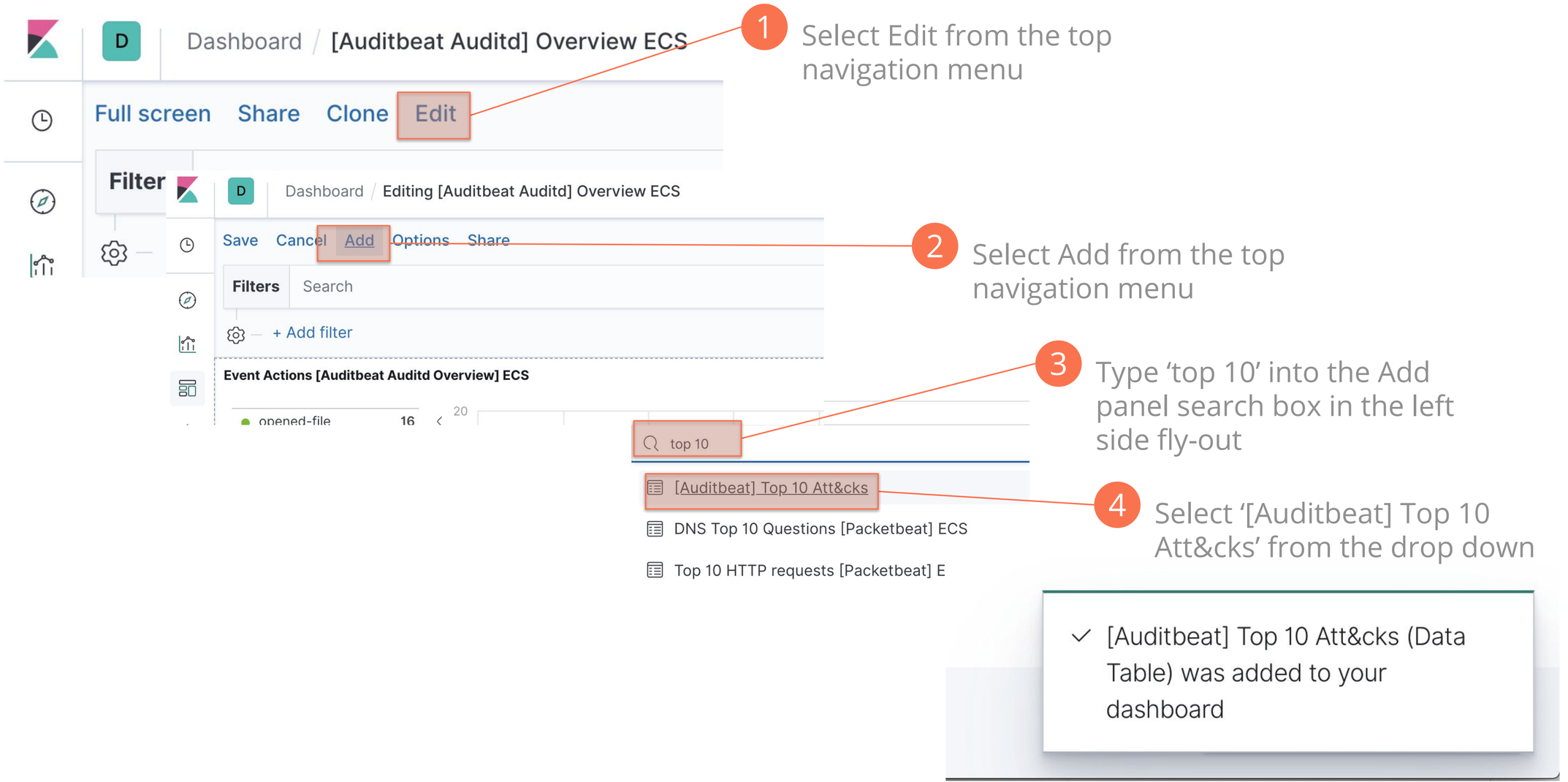
navigate to the '[Auditbeat Auditd] Overview ECS' dashboard



elastic

Add visualization to Auditbeat Overview dashboard

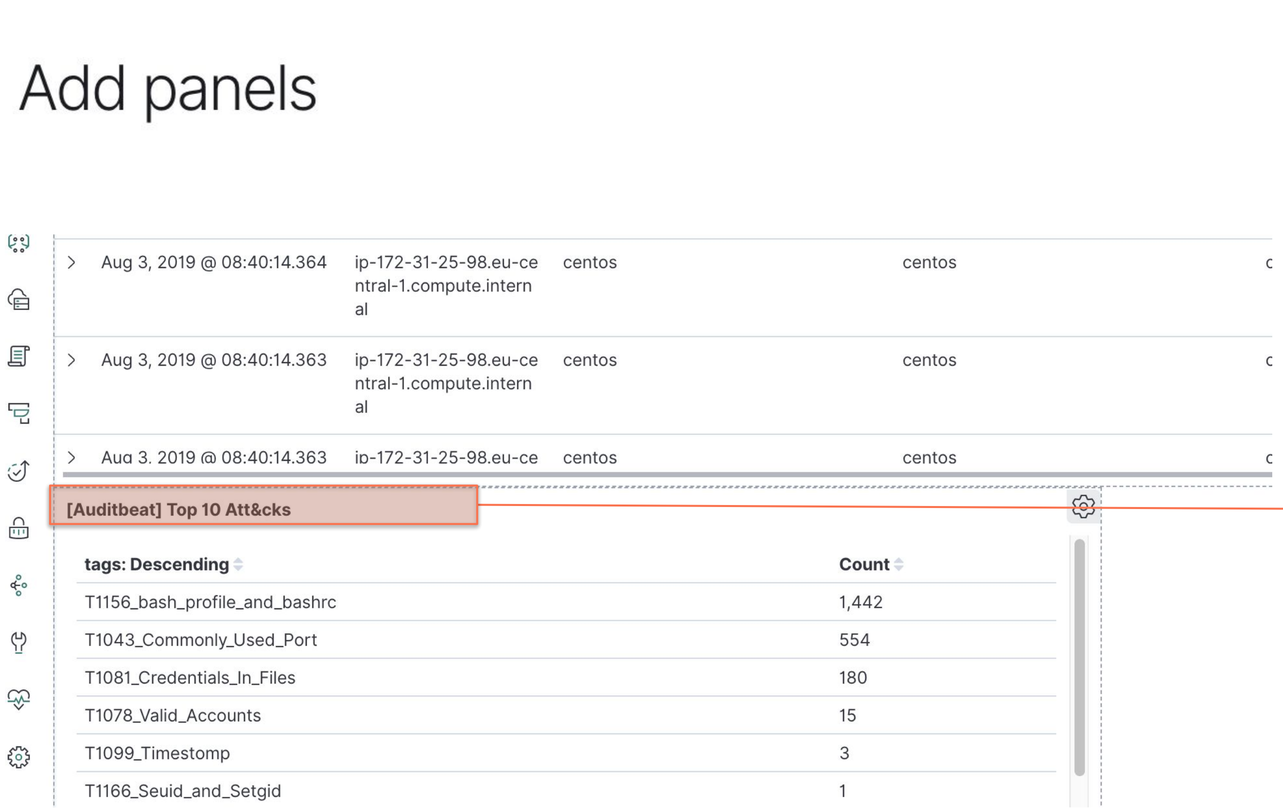
finish adding visualization



elastic

Load Sample Data in Kibana

Kibana load data page



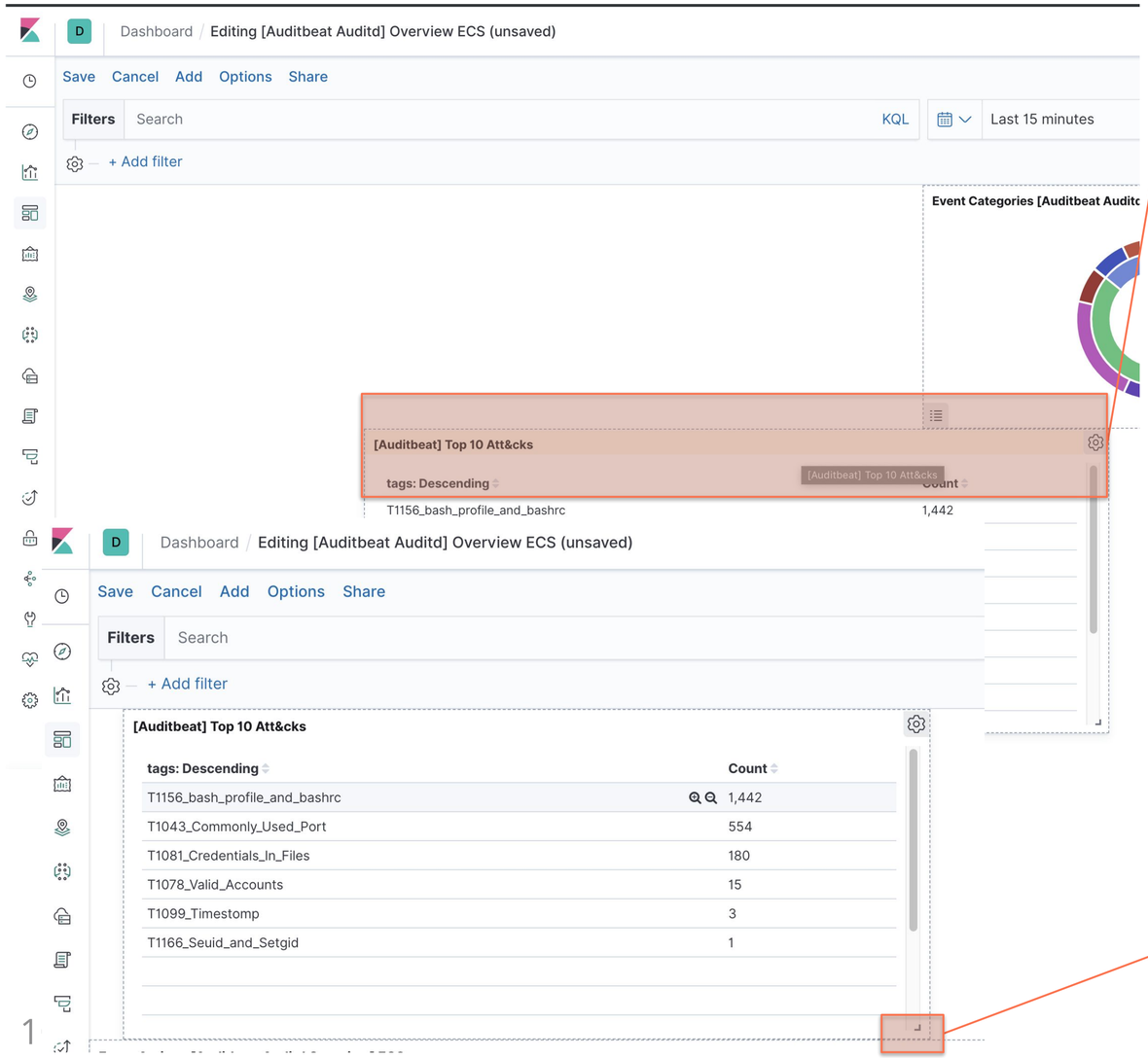
1 Exit the Add Panel fly-out

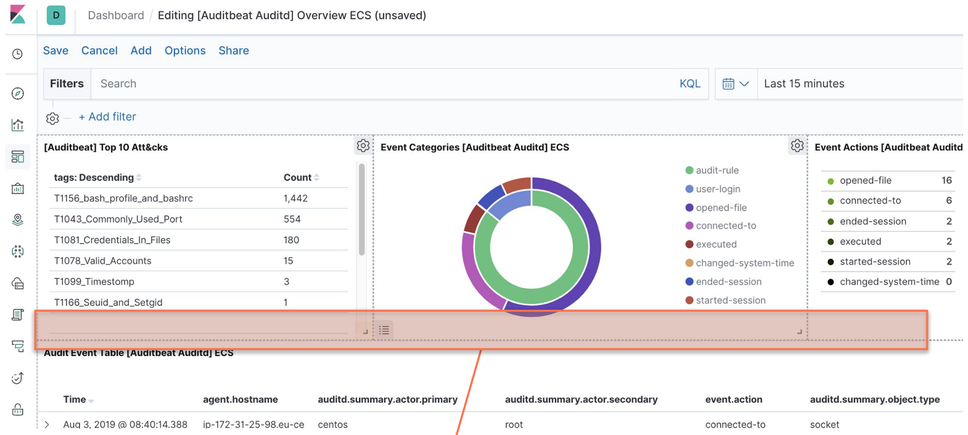
2 Scroll down to the very bottom of the dashboard to find your visualization

Reshaping the dashboard

changing the layout of a dashboard

1 Drag the visualization to the top by dragging while holding the left click button down.



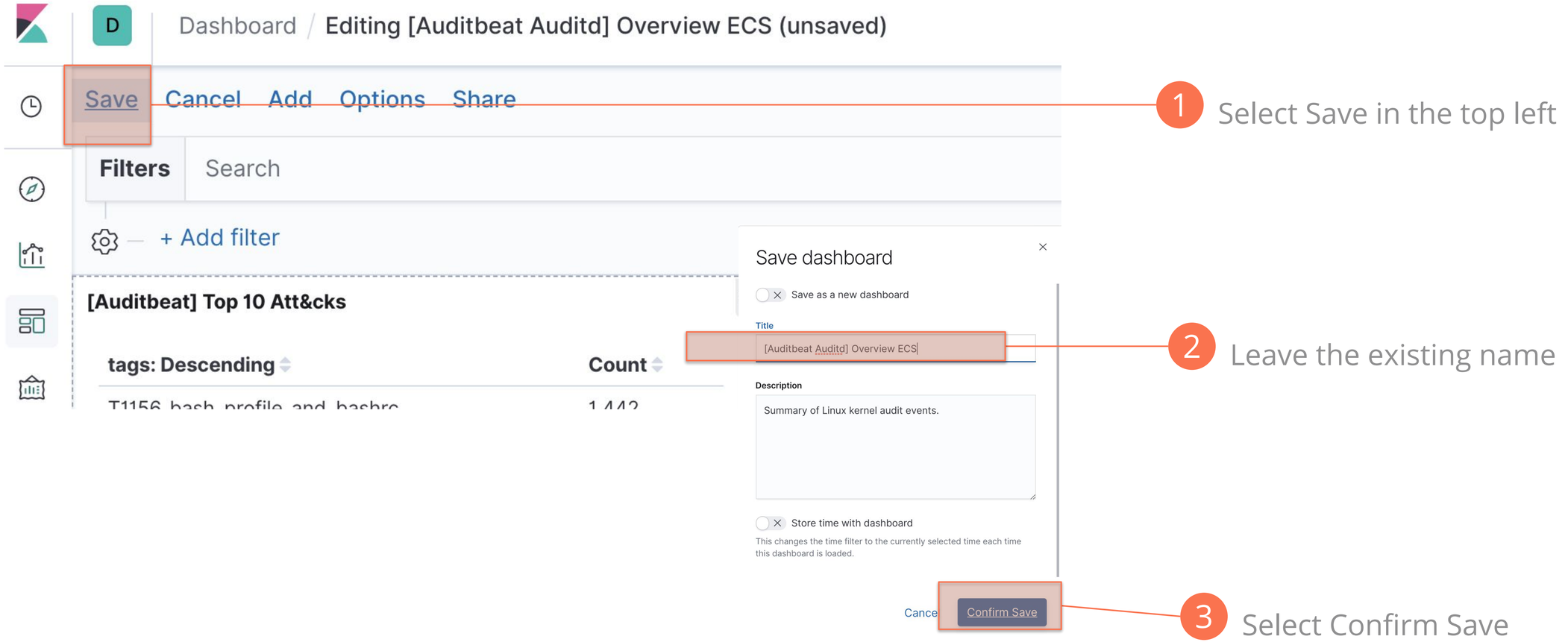


3 Resize other visualizations to better fit the screen

2 Resize the panel using the lower right resize arrow

Save your updated dashboard

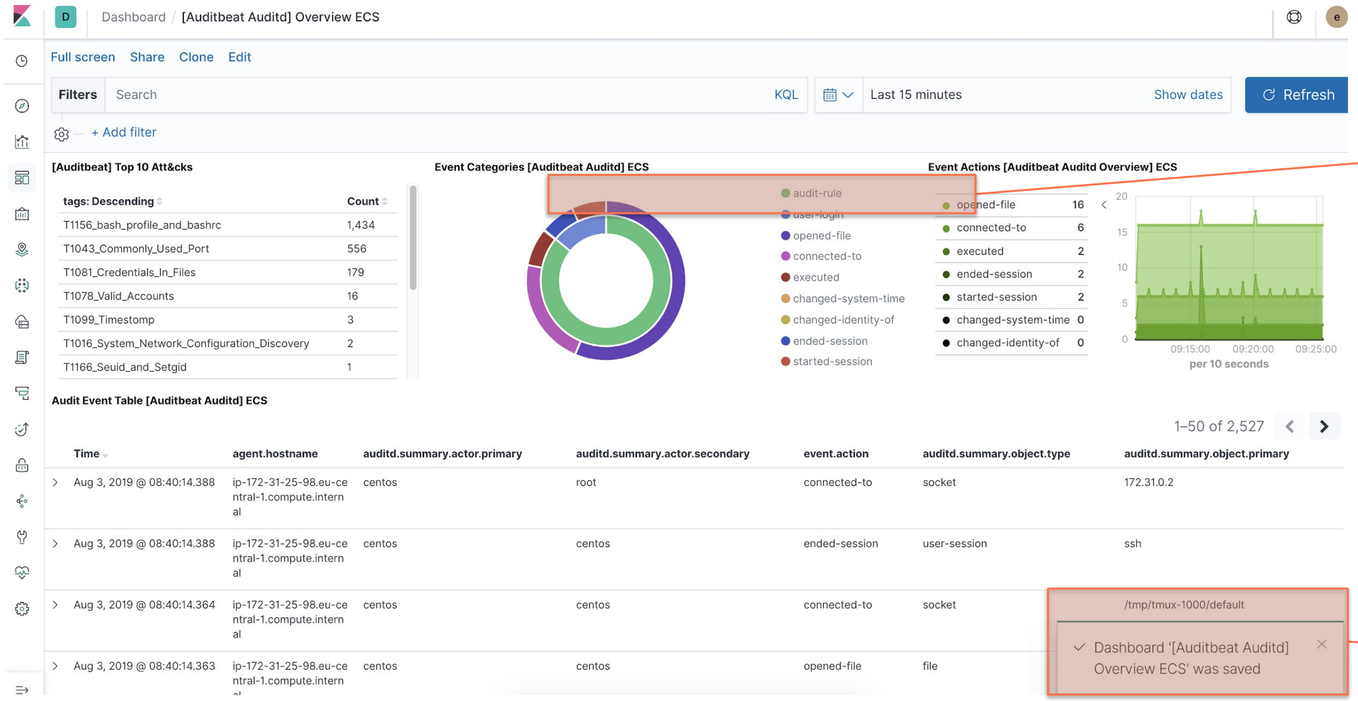
Top 10 attacks added to Auditbeat Overview



elastic

Play time

click around with ‘+’ to filter data instantly

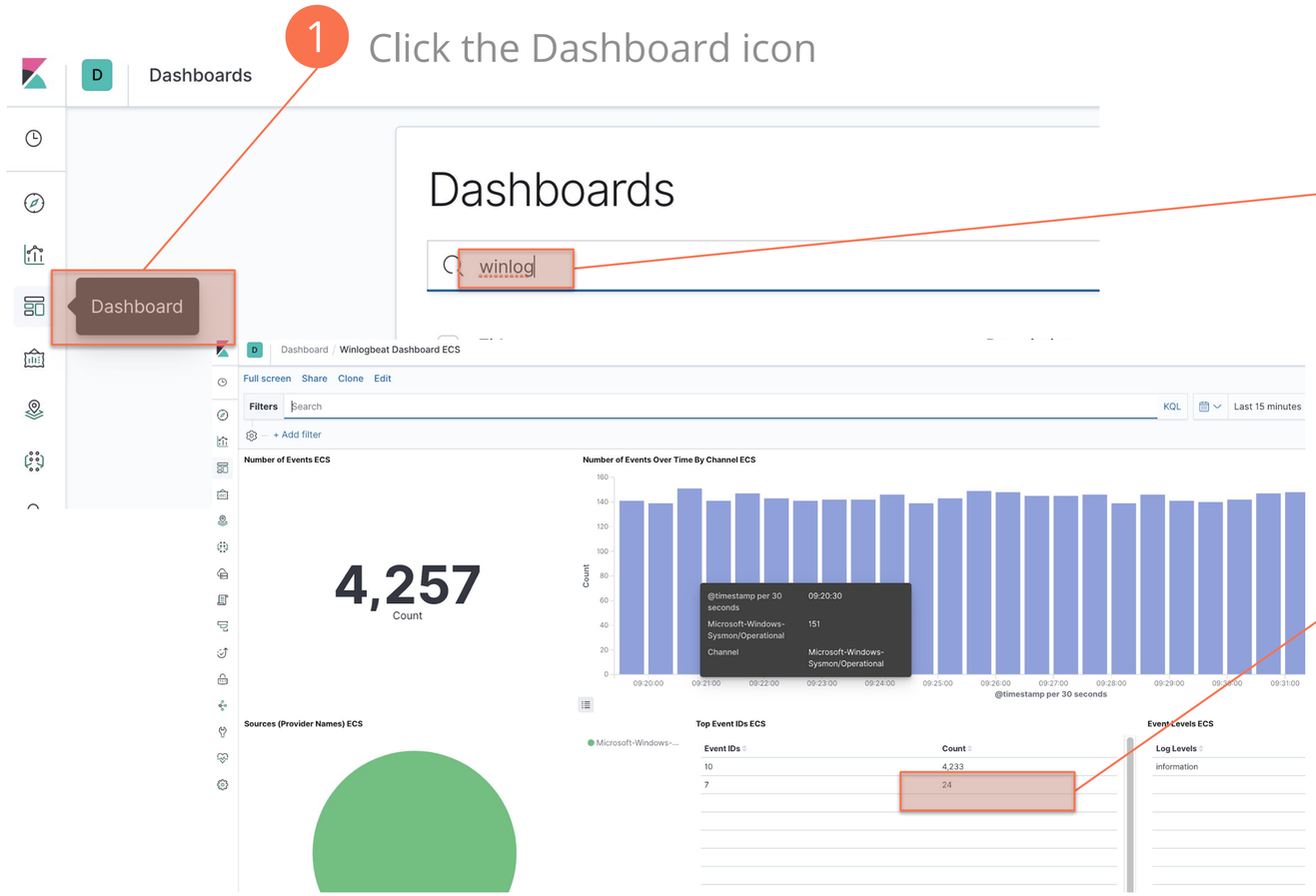


2 Select the ‘+’ icon to create filters automatically

1 A saved tool tip should appear

Other Dashboards

click around with ‘+’ to filter data instantly



elastic