

Lab 3

Finding MITRE ATT&CK™

TTPs

Launch Kibana from Cloud

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

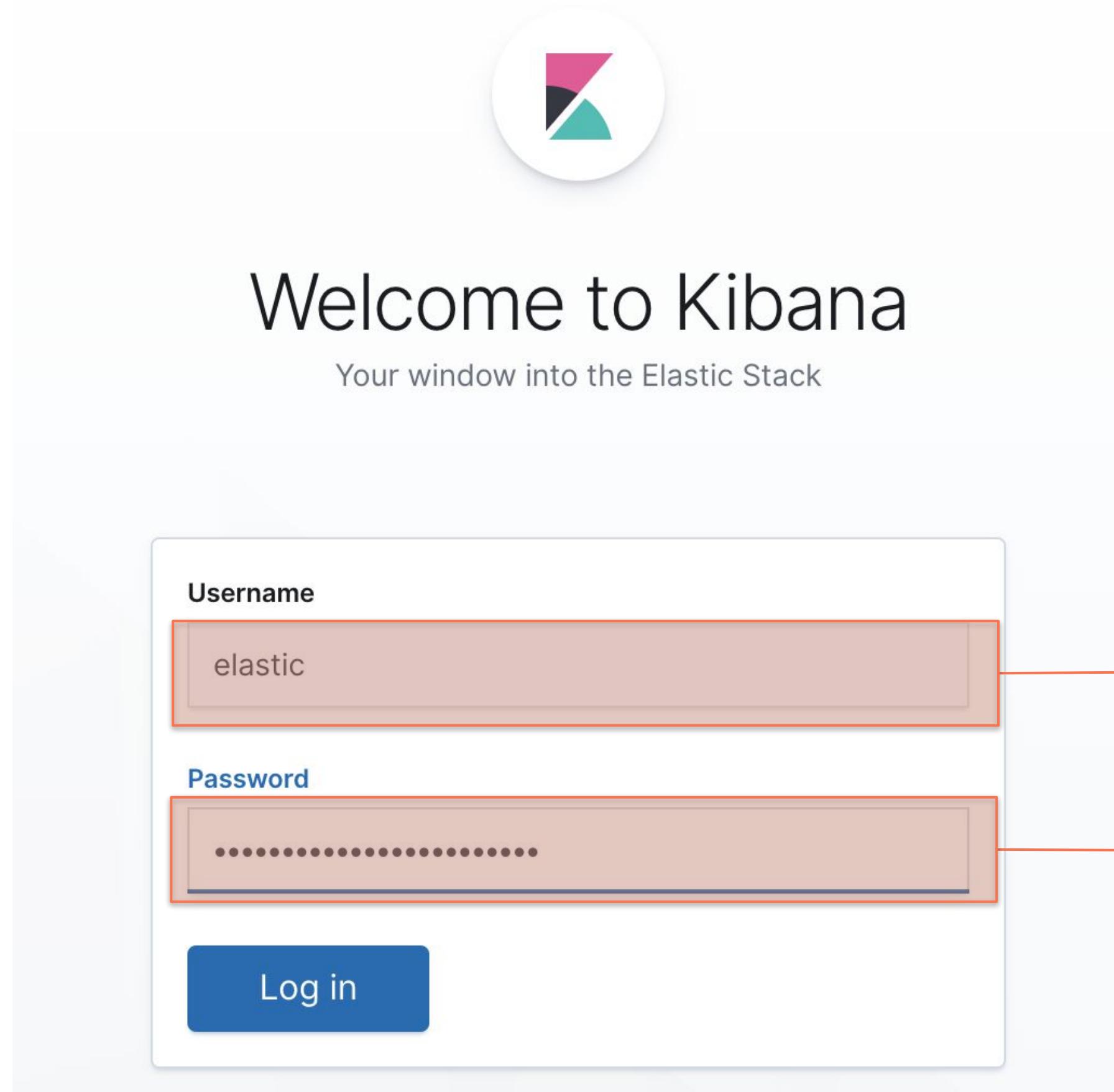
The screenshot shows the Elasticsearch Cloud interface. On the left, a sidebar lists 'Deployments', 'Custom plugins', 'Account', and 'Help'. Under 'Deployments', a 'workshop' deployment is listed with options: 'Edit', 'Elasticsearch' (with 'Logs', 'Snapshots', 'API Console'), 'Kibana' (which is highlighted with a red box), 'APM', 'Activity', 'Security', and 'Performance'. The main content area shows the 'workshop' deployment details. It includes a 'Kibana' section with the Kibana logo and the text: 'Great work! Your deployment has been created. What would like to do next?'. It offers two paths: 'Ingest and visualize data' (with a 'Launch Kibana' button) and 'Migrate existing data' (with a 'Reindex or Restore' button). At the bottom of the deployment card, there is a 'Kibana' section with a 'Launch' button and a 'Copy Endpoint URL' button, both highlighted with a red box.

1 Select Kibana under the newly created deployment.

2 Select Launch in the Kibana details.

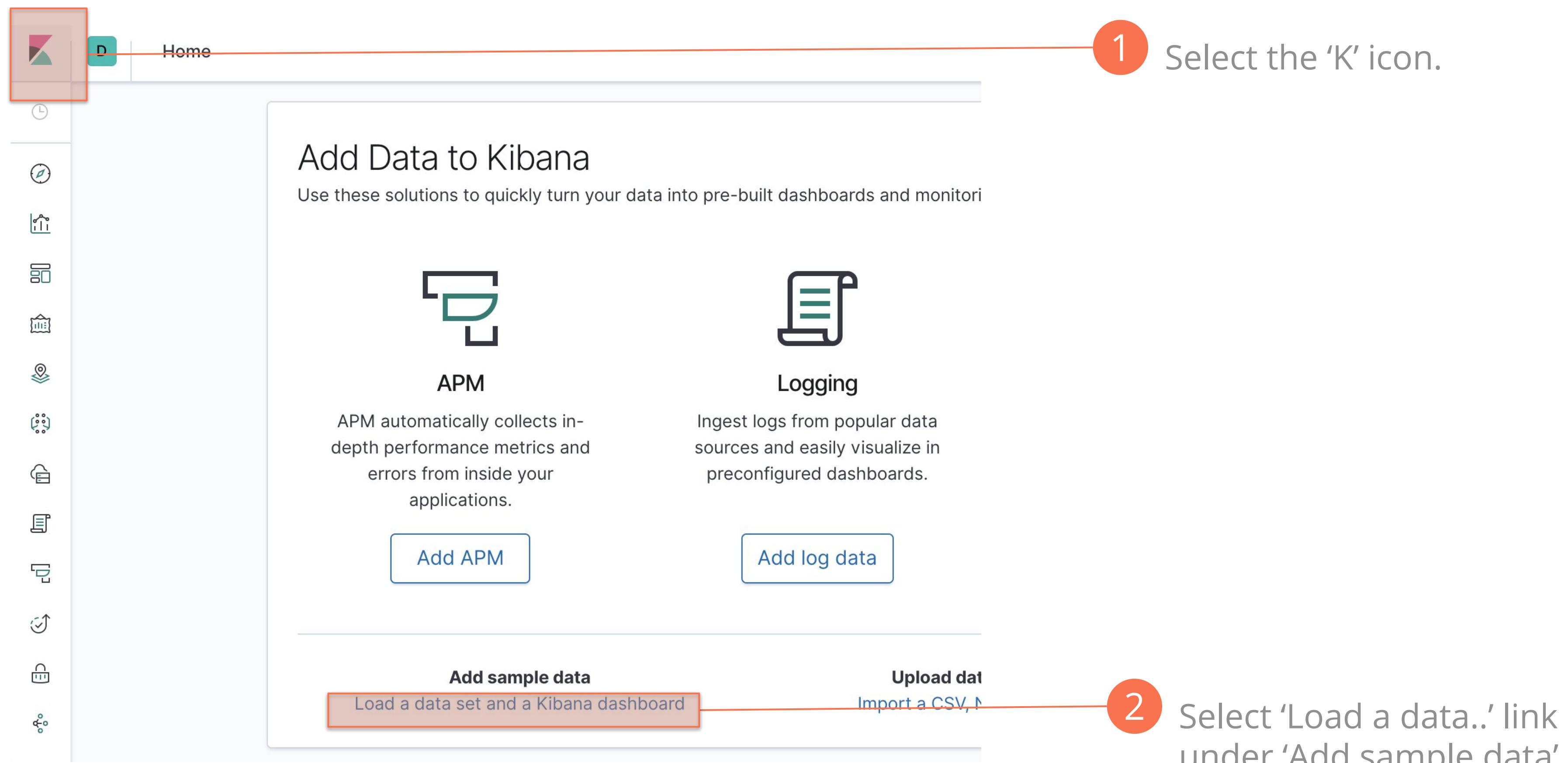
Log into Kibana

Setting Time Ranges



Load Sample Data in Kibana

Kibana load data page



Loading sample data into the Elastic Stack

Load all three data sets

Add Data to Kibana

All Logging Metrics SIEM **Sample data**

Sample eCommerce orders
Sample data, visualizations, and dashboards for tracking eCommerce orders.

Add data

Sample flight data
Sample data, visualizations, and dashboards for monitoring flight routes.

Add data

Sample web logs
Sample data, visualizations, and dashboards for monitoring web logs.

Add data

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

Navigate to Stack Monitoring

Second icon (heart) from the bottom left Navigation menu

The screenshot shows the Kibana interface for adding data. At the top, there are icons for Home and Add data. Below the navigation bar, the title "Add Data to Kibana" is displayed. A horizontal menu bar includes "All", "Logging", "Metrics", "SIEM", and "Sample data", with "Sample data" being the active tab. On the left, a sidebar lists various monitoring categories with corresponding icons. The main area contains three sections, each labeled "INSTALLED":

- Sample eCommerce orders:** Includes a summary card with a gauge (139 Trans / day), a donut chart (average spend \$75.23 per order), and a donut chart (average sold quantity 2.163 per order). Below it is a line chart showing total revenue (\$77,638.33) over time.
- Sample flight data:** Includes a summary card with a gauge (68 Total Delays), a donut chart (origin cities), and a line chart (Flight Count and Average Total Price).
- Sample web logs:** Includes a summary card with a gauge (801 Unique Visitors), a donut chart (Article Type), and a line chart (Response Codes over Time + Annotations).

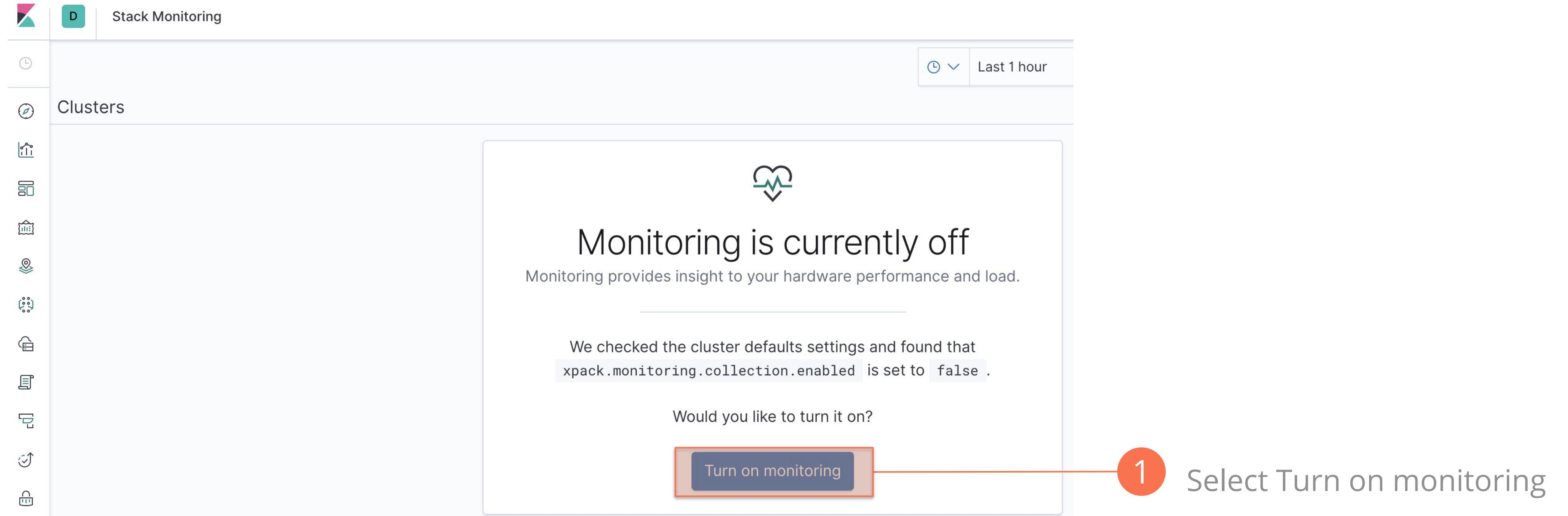
At the bottom of the screen, a navigation bar features several icons: a gear, a wrench, a heart (highlighted with a red box), a magnifying glass, a gear, and a gear. The "Stack Monitoring" icon is specifically highlighted with a red circle and a callout line pointing to the right.

1

Select Stack Monitoring

Enable Stack Monitoring

Stack monitoring lets you understand Elastic Cloud cluster performance



Ensure your Beats agents are online

After a few minutes, you should see 6 beats enabled

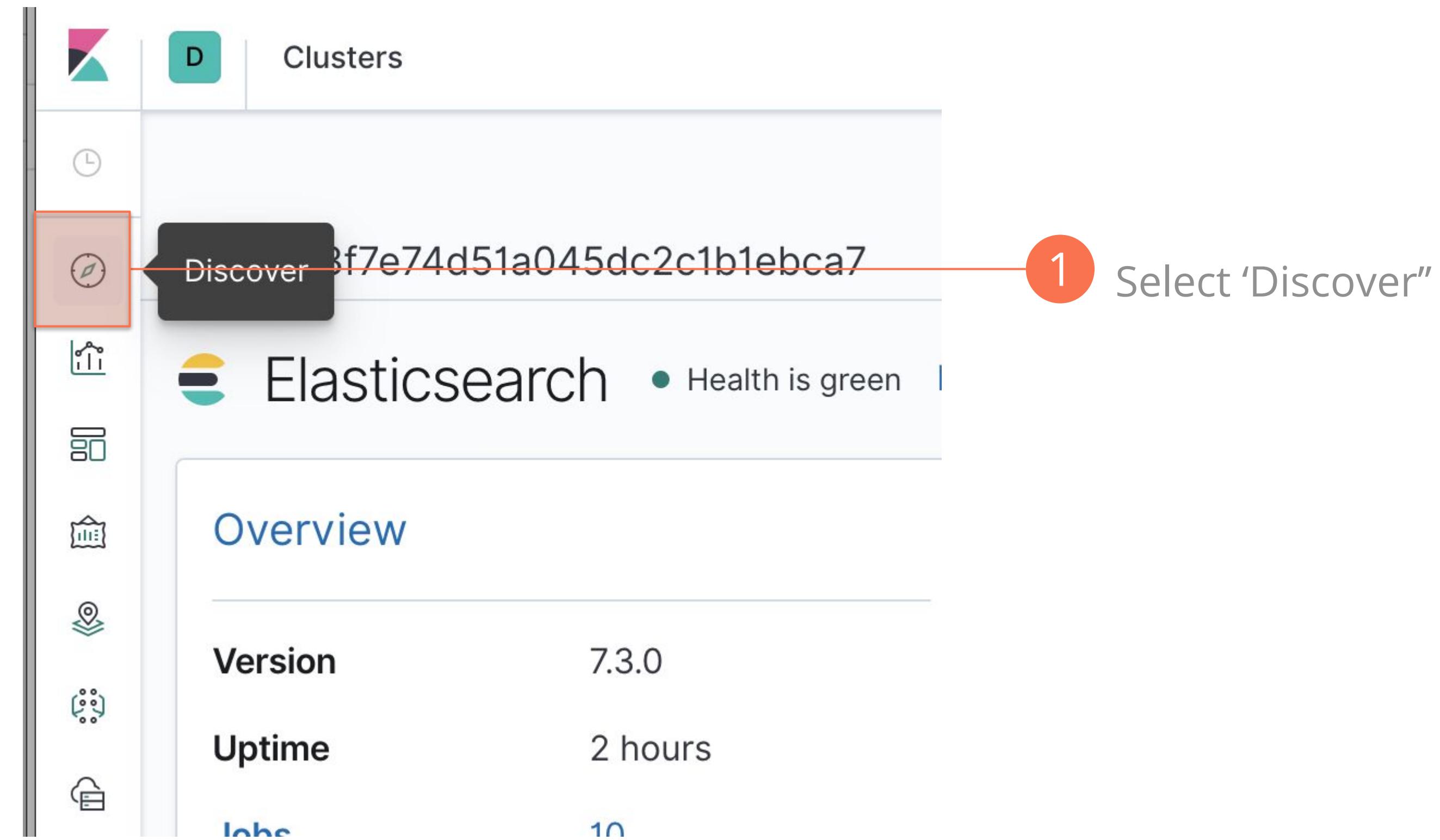
The screenshot shows the Elasticsearch dashboard with the following sections:

- Clusters**: Shows a single cluster with a green health status. Overview details: Version 7.3.0, Uptime 2 hours, Jobs 10. Node statistics: Disk Available 99.78% (243.5 GB / 244.0 GB), JVM Heap 31.47% (1.6 GB / 4.9 GB).
- Kibana**: Shows a green health status. Overview details: Requests 4, Max. Response Time 3 ms. Instance statistics: Connections 16, Memory Usage 37.10% (313.9 MB / 846.0 MB).
- Beats**: Shows a green health status. Overview details: Total Events 23.9k, Bytes Sent 49.5 MB. Beat instance statistics:
 - Beats: 6 (highlighted with a red box)
 - Metricbeat: 2
 - Filebeat: 1
 - Auditbeat: 1
 - Packetbeat: 1
 - Winlogbeat: 1
- APM**: Shows a green health status. Overview details: Processed Events 0, Last Event 1 seconds ago. APM Server statistics: APM Servers: 1, Memory Usage.

1 Six Beats should be enabled

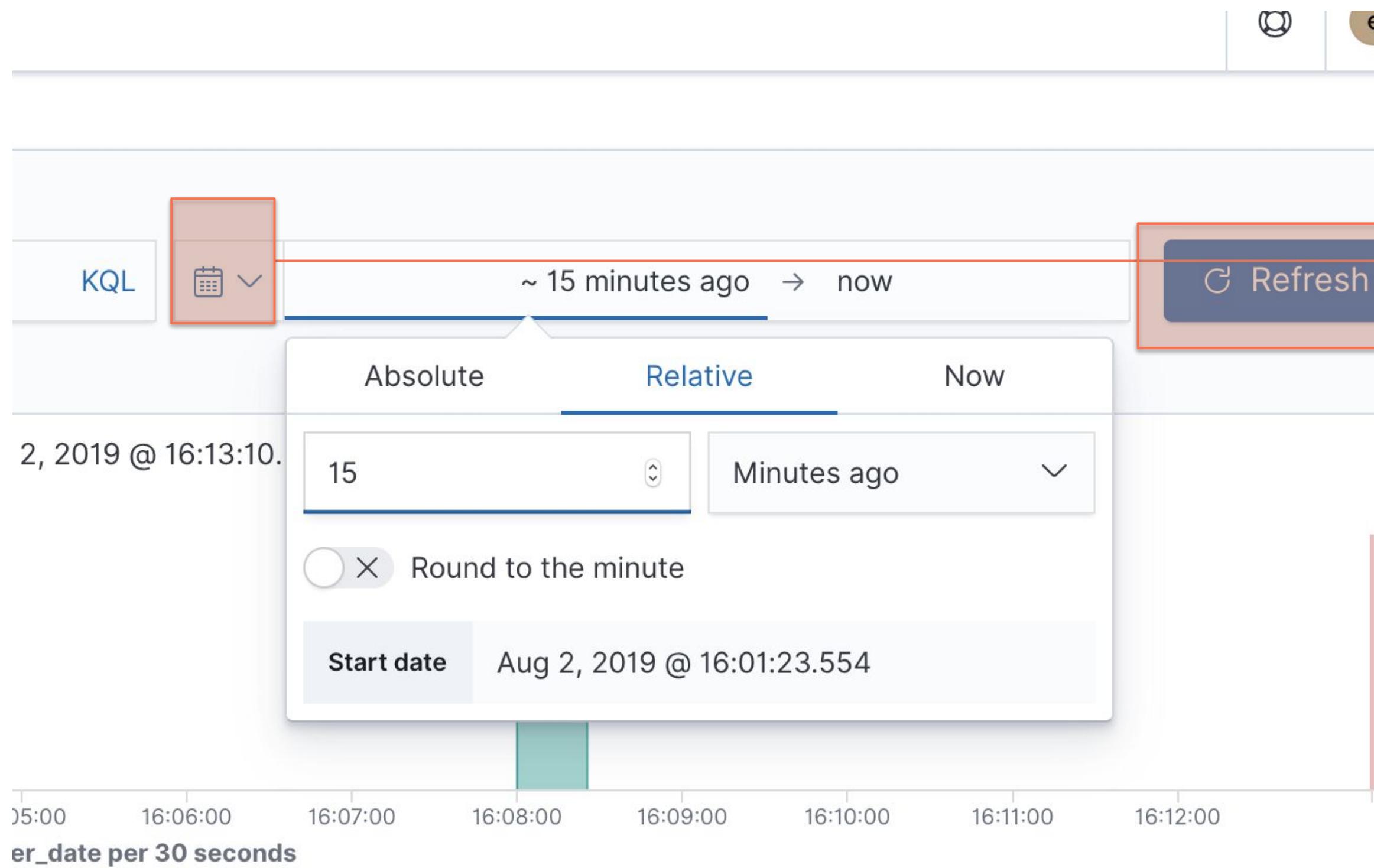
Move to the Discover app

Discovering what is in the data



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

The screenshot shows the Kibana Discover App interface. On the left, there's a sidebar with icons for location, chart, file, and cloud. The main area shows two search results:

- Discover**: Shows 2 hits. The index dropdown menu is open, with the 'Selected fields' section highlighted by a red box. A red circle labeled 1 points to the 'Selected fields' section.
- Discover**: Shows 8 hits. The 'Selected fields' section is also highlighted by a red box. A red circle labeled 1 points to the 'Selected fields' section here as well.

In the bottom right, there's a histogram with a teal bar and a count of 4.

Selected fields (highlighted by red box):

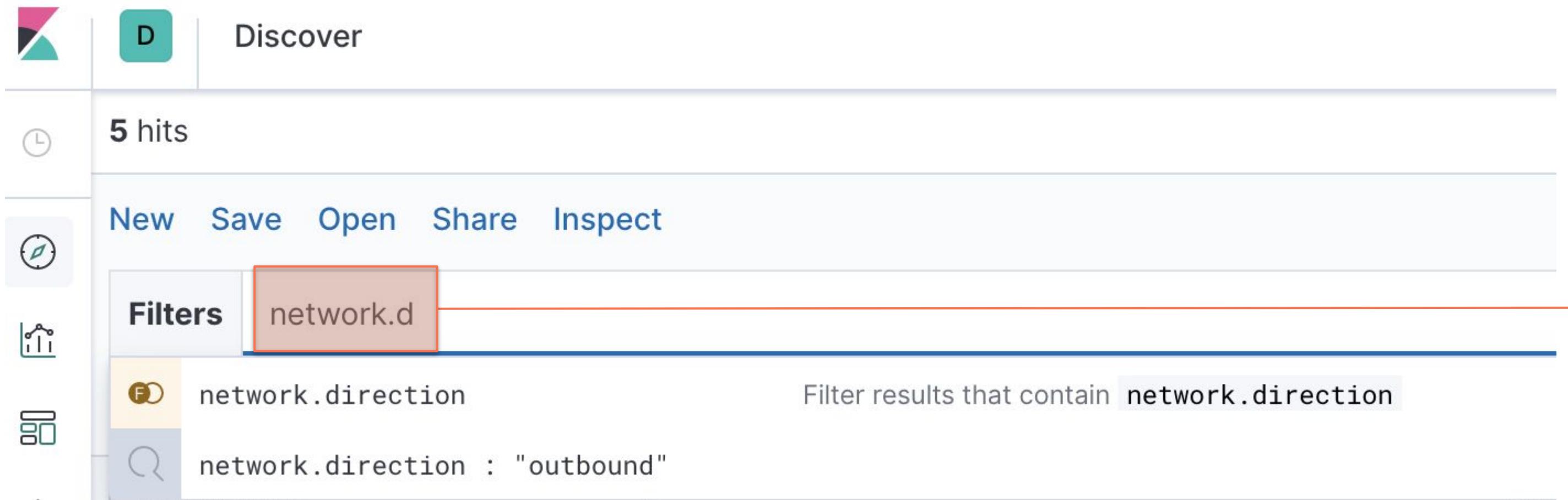
- ? _source
- auditbeat-*** (highlighted by red box)
- filebeat-*
- kibana_sample_data_ecommerce
- kibana_sample_data_flights

1 Select the Index drop down menu under 'Filter' in the Discovery App

2 Select 'auditbeat'

Search with KQL in Kibana

The default way to search



This screenshot shows the Kibana Discover interface. At the top, there's a navigation bar with a Kibana icon, a teal 'Discover' button, and a blue 'D' button. Below the navigation is a header with a clock icon and the text '5 hits'. Underneath is a toolbar with 'New', 'Save', 'Open', 'Share', and 'Inspect' buttons. On the far left, there's a sidebar with icons for 'Discover', 'Dashboard', 'Visualize', and 'Logs'. The main area is titled 'Filters' and contains a dropdown menu with 'network.d' selected. A tooltip below the dropdown says 'Filter results that contain network.direction'. Below the dropdown are two other filter options: 'network.direction' and 'network.direction : "outbound"'. The entire 'Filters' section is highlighted with a red box.

- 1 Type 'network.d' and select network.direction from the drop down menu



This screenshot shows the Kibana Discover interface again. The top navigation bar and sidebar are identical to the first screenshot. The main area is titled 'Filters' and contains a dropdown menu with 'network.direction' selected. Below the dropdown is a field with a colon ':'. A tooltip above the colon says 'equals some value'. The entire 'Filters' section is highlighted with a red box.

- 2 Select 'equals some value'

Search with KQL in Kibana

search with autocomplete

The screenshot shows two stacked Kibana Discover interfaces. The top interface has 0 hits and a search bar with 'network.direction :'. Below it, a sidebar lists filters: 'outbound', 'inbound' (which is selected and highlighted in red), and 'listening'. A callout '1 Select 'inbound'' points to the selected filter. The bottom interface has 5 hits and a search bar with 'network.direction : "inbound"'. A callout '2 Results are filtered for inbound' points to the search bar. Other interface elements include a date range selector, a 'Discover' button, and sections for 'Selected fields' and 'Available fields'.

Discover

0 hits

New Save Open Share Inspect

Filters network.direction :

- "outbound"
- "inbound"**
- "listening"

1 Select 'inbound'

Discover

5 hits

New Save Open Share Inspect

Filters network.direction : "inbound"

+ Add filter

auditbeat-*

Selected fields

? _source

Available fields

@_timestamp

Count

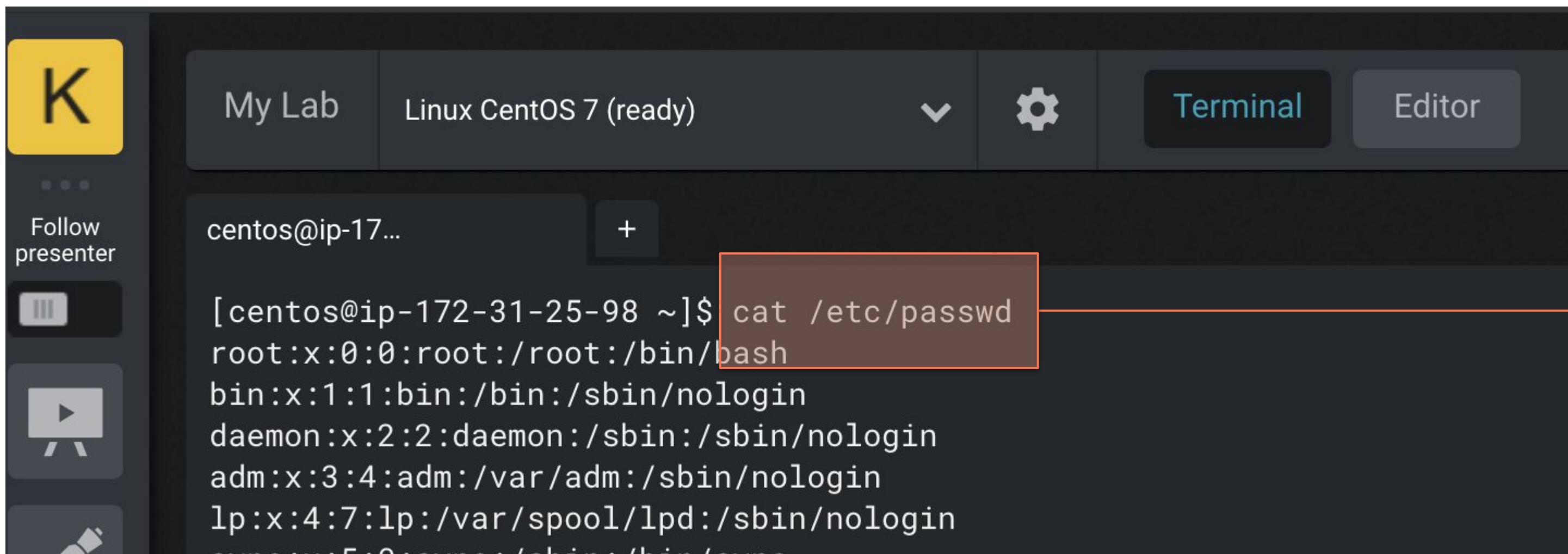
Aug 3, 2019 @ 06:20:20.903 - Aug

2 Results are filtered for inbound

elastic

ATT&CK Technique T1078 Valid Accounts

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



The screenshot shows a terminal window titled "My Lab" with the subtitle "Linux CentOS 7 (ready)". The terminal interface includes a sidebar with icons for "Follow presenter", "Screenshot", "Video", and "Note". The main terminal area displays the command "cat /etc/passwd" being run by a user named "centos". The output of the command is shown in a red box:

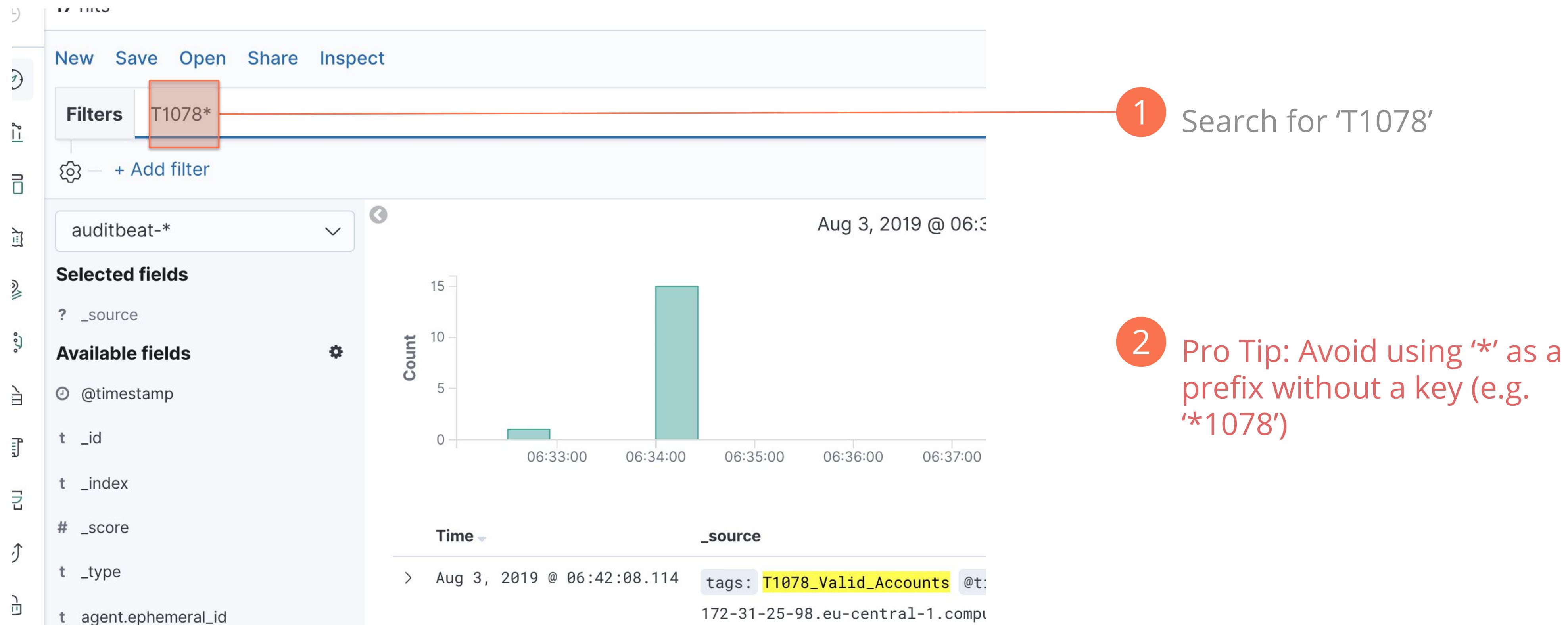
```
[centos@ip-172-31-25-98 ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin

```

- 1 Type 'cat /etc/passwd' in the terminal

Find T1078 events

Search using wildcards



Inspect an event

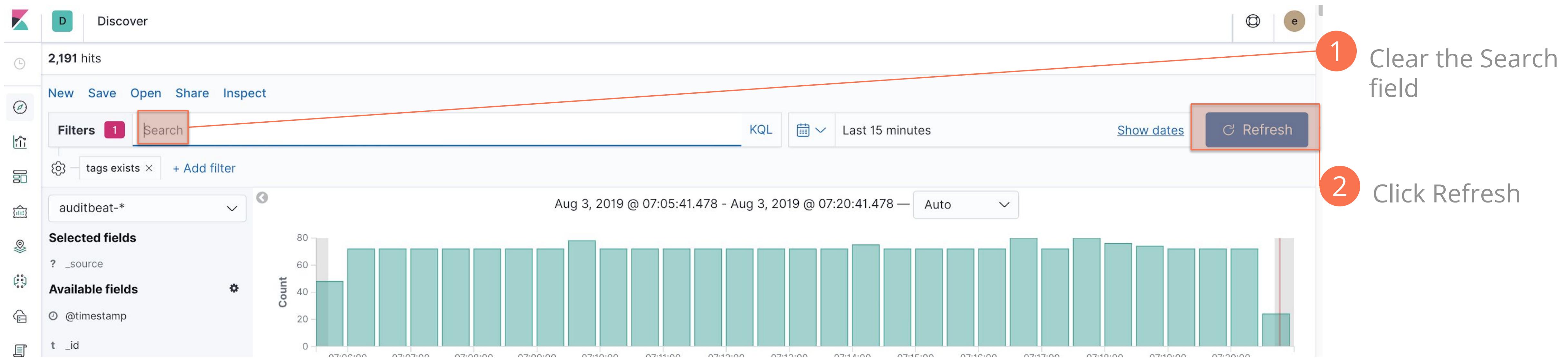
review the fields in an event, filter on 'contains tag'

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

- Select the star icon to filter for events events that contain the 'tags' field

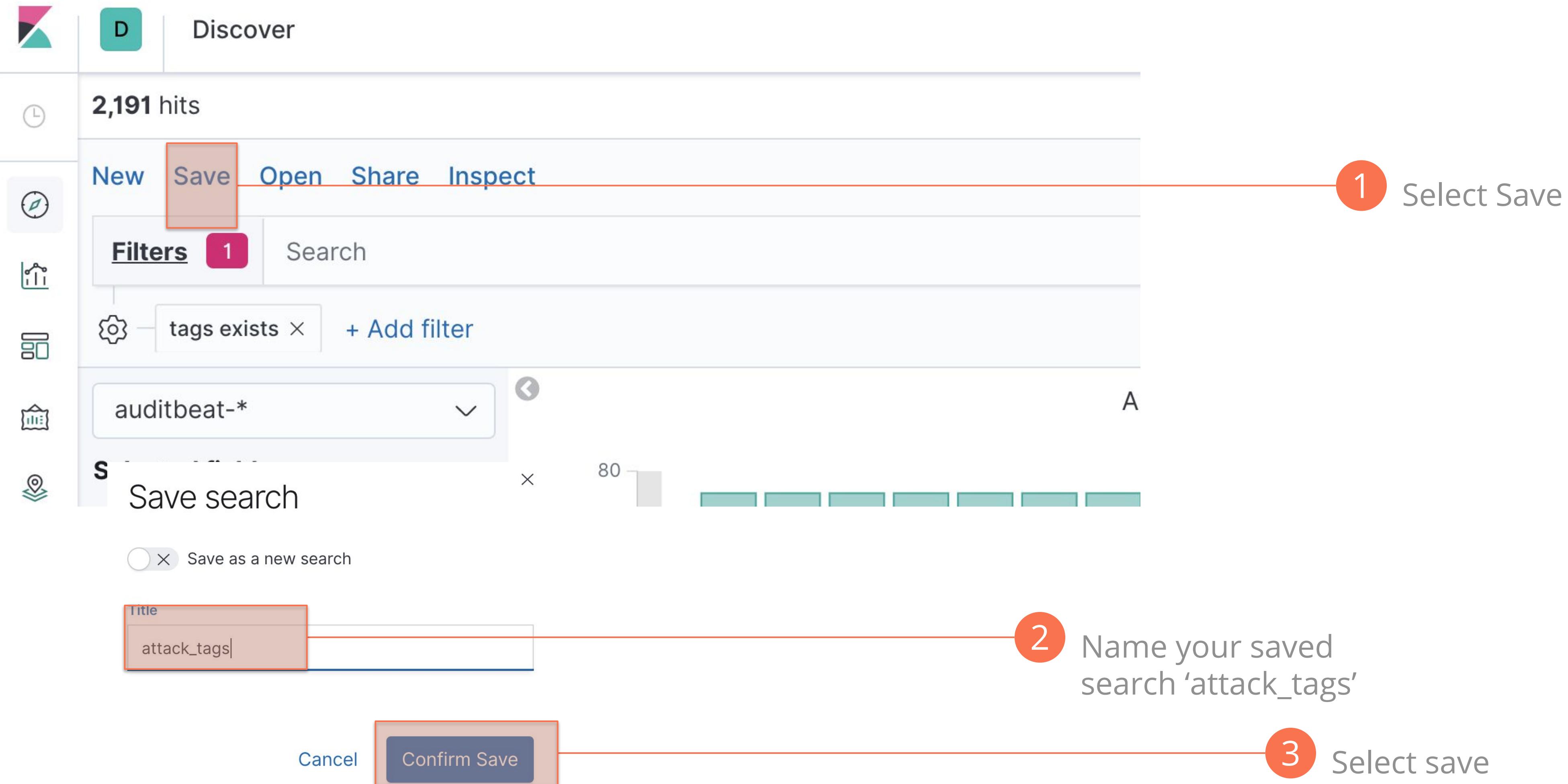
Apply tag exists filter

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



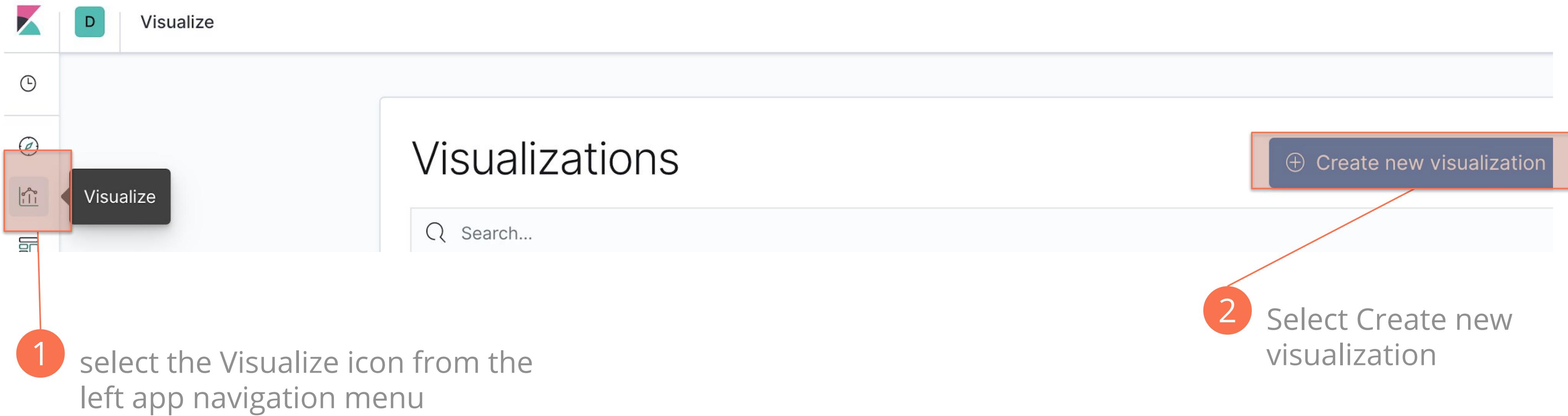
Create a saved search

save your tags filter for reuse



Start creating a new visualization

create a new visualization in the Visualize Kibana app



Create a new data table visualization

reuse your 'attack_tags' saved search

New Visualization

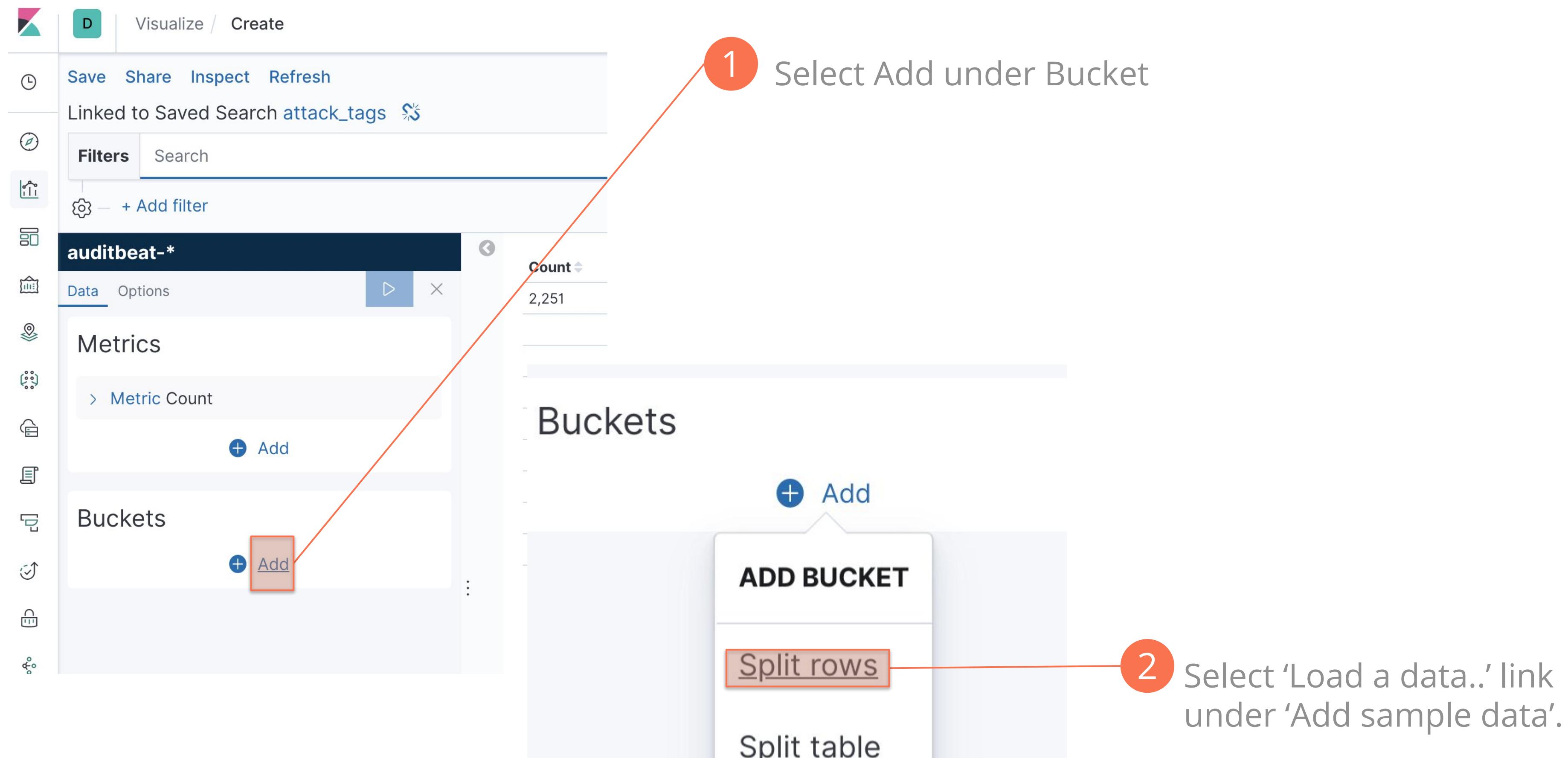
The screenshot shows the Kibana interface for creating a new visualization. At the top left is a filter bar with a magnifying glass icon and the word "Filter". Below it is a row of visualization icons: Area, Controls (with an 'E' icon), Coordinate Map, Data Table (which is highlighted with a red box and has a red arrow pointing to it from step 1), Gauge, Goal, Heat Map, and Horizontal Bar. To the right of these is a description of the Data Table visualization: "Display values in a table". A second red arrow points from step 2 to the "attack_tags" option in a dropdown menu titled "New Data Table / Choose a source". The dropdown also includes a search bar with "attac" typed in, a "Sort" button, and a "Types" button set to "2".

1 Select the Data Table icon

2 Type 'attac' and select 'attack_tags'

Editing Data Table

split rows



Editing Data Table

use terms

The screenshot shows the 'Buckets' section of the Elasticsearch interface. Under 'Aggregation', a dropdown menu is open with the placeholder 'Select an aggregation'. Below the dropdown, a list of aggregation types is shown: Geohash, Geotile, Histogram, IPv4 Range, Range, Significant Terms, and Terms. The 'Terms' option is highlighted with a red box and has a red line pointing to it from the number 1.

1 Select the Terms Aggregation

This screenshot shows the 'Field' selection step. A search bar at the top contains the text 'tag'. Below the search bar, a list of fields is displayed: string, container.image.tag, and tags. The 'tags' option is highlighted with a red box and has a red line pointing to it from the number 2.

2 Type 'tags' and select it for Aggregation Field

This screenshot shows the 'Size' configuration step. It includes an 'Order' section with 'Descending' selected and a 'Size' input field set to '10'. The 'Size' input field is highlighted with a red box and has a red line pointing to it from the number 3.

3 Set the display Size to 10

See your updated data table visualization

apply you changes

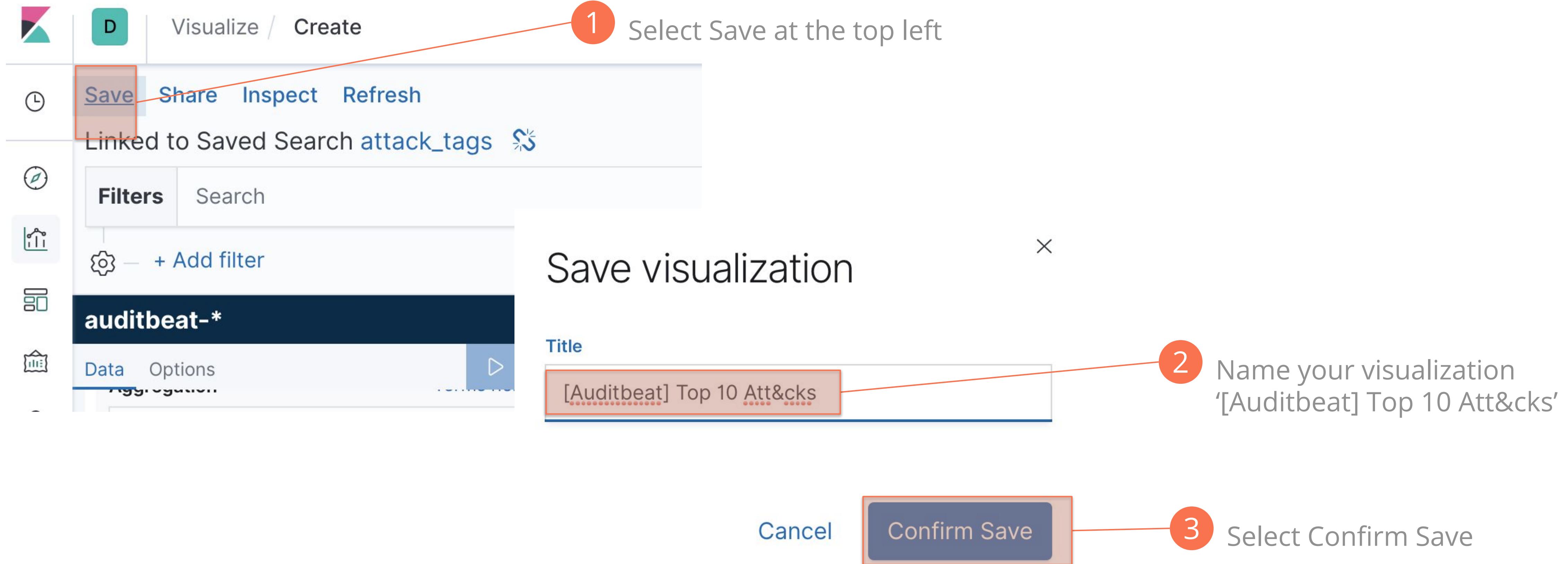
The screenshot shows the Kibana interface with a search bar at the top containing the query "auditbeat-*". Below the search bar are two tabs: "Data" (selected) and "Options". Under the "Data" tab, there are sections for "Terms", "Field", and "tags". The "tags" section has a dropdown menu with an "Apply changes" button highlighted by a red box and circled with a red arrow labeled "1". To the right of this is a data table titled "tags: Descending". The table has a header row with "Count" and a descending arrow. The data rows are:

	Count
T1156_bash_profile_and_bashrc	1,434
T1043_Commonly_Used_Port	564
T1081_Credentials_In_Files	179
T1078_Valid_Accounts	33
T1016_System_Network_Configuration_Discovery	8
T1166_Seuuid_and_Setgid	7

A red arrow labeled "2" points from the "Count" column header to the first data row.

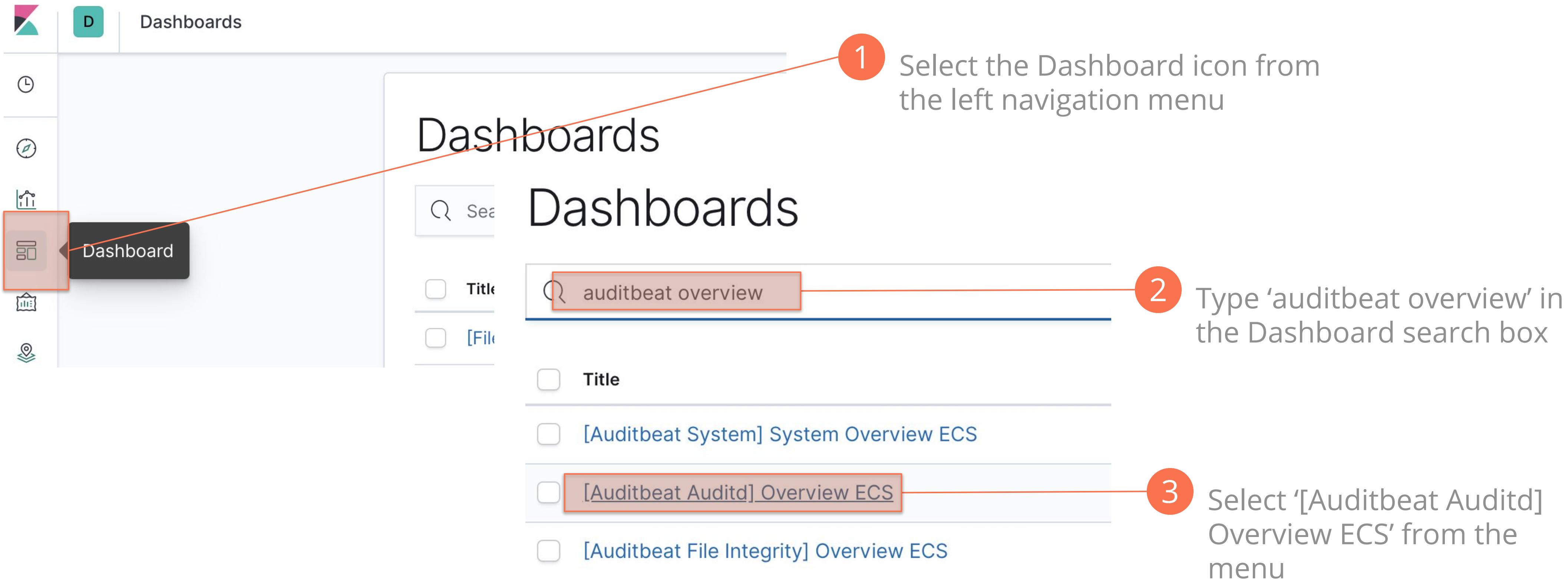
Save your visualization

Save your visualization for reuse



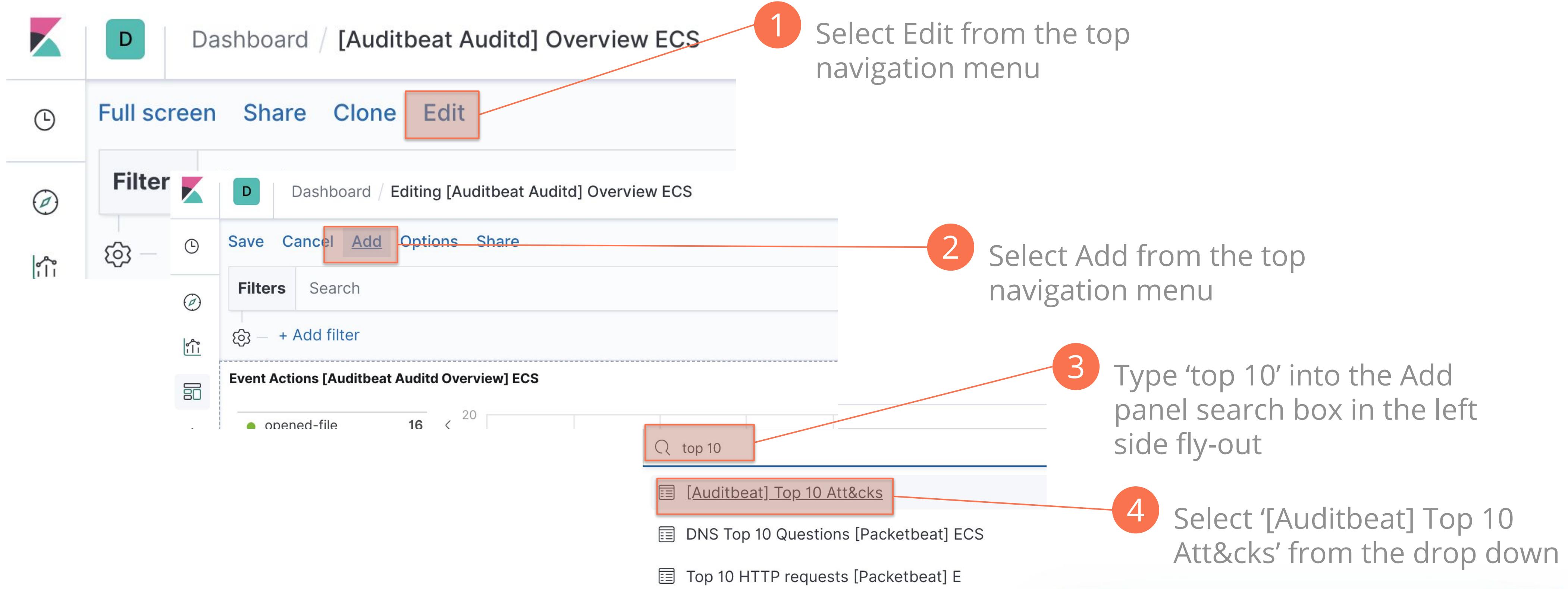
Add visualization to Auditbeat Overview

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



Add visualization to Auditbeat Overview dashboard

finish adding visualization



1 Select Edit from the top navigation menu

2 Select Add from the top navigation menu

3 Type 'top 10' into the Add panel search box in the left side fly-out

4 Select '[Auditbeat] Top 10 Att&cks' from the drop down

✓ [Auditbeat] Top 10 Att&cks (Data Table) was added to your dashboard

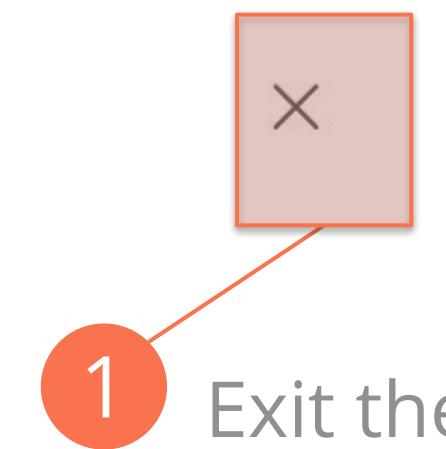
Load Sample Data in Kibana

Kibana load data page

Add panels

The screenshot shows the Kibana Load Data page. On the left, there is a sidebar with various icons for file operations like upload, download, and search. The main area displays a table of audit log entries. The first three rows show log entries from Aug 3, 2019, at 08:40:14.364, 08:40:14.363, and 08:40:14.363 respectively. The fourth row is highlighted with a red border and contains the title "[Auditbeat] Top 10 Att&cks". This row is part of a fly-out panel that includes a title bar with a close button and a table showing the top 10 attack types with their counts. The table data is as follows:

tags: Descending	Count
T1156_bash_profile_and_bashrc	1,442
T1043_Commonly_Used_Port	554
T1081_Credentials_In_Files	180
T1078_Valid_Accounts	15
T1099_Timestamp	3
T1166_Setuid_and_Setgid	1



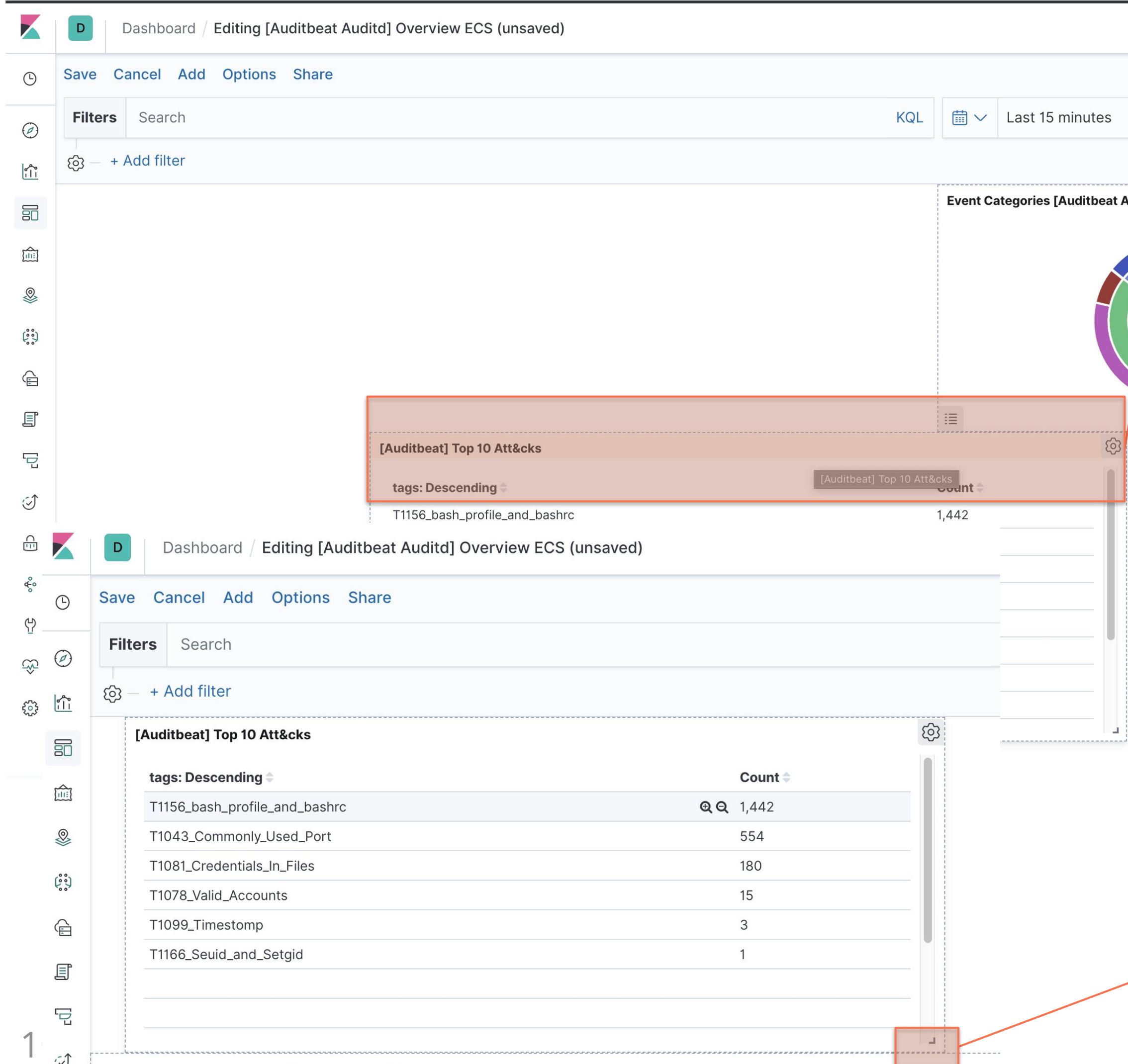
1 Exit the Add Panel fly-out



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

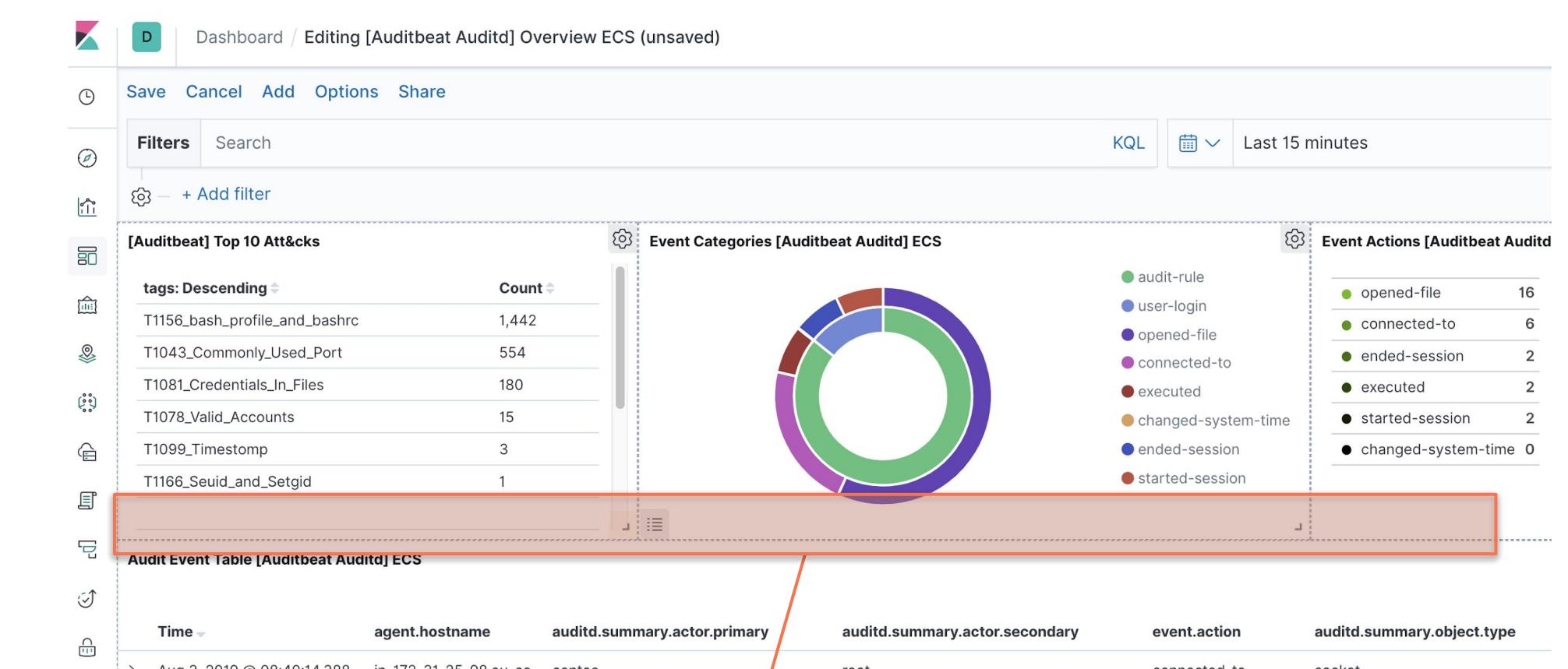
Reshaping the dashboard

changing the layout of a dashboard



1

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



3

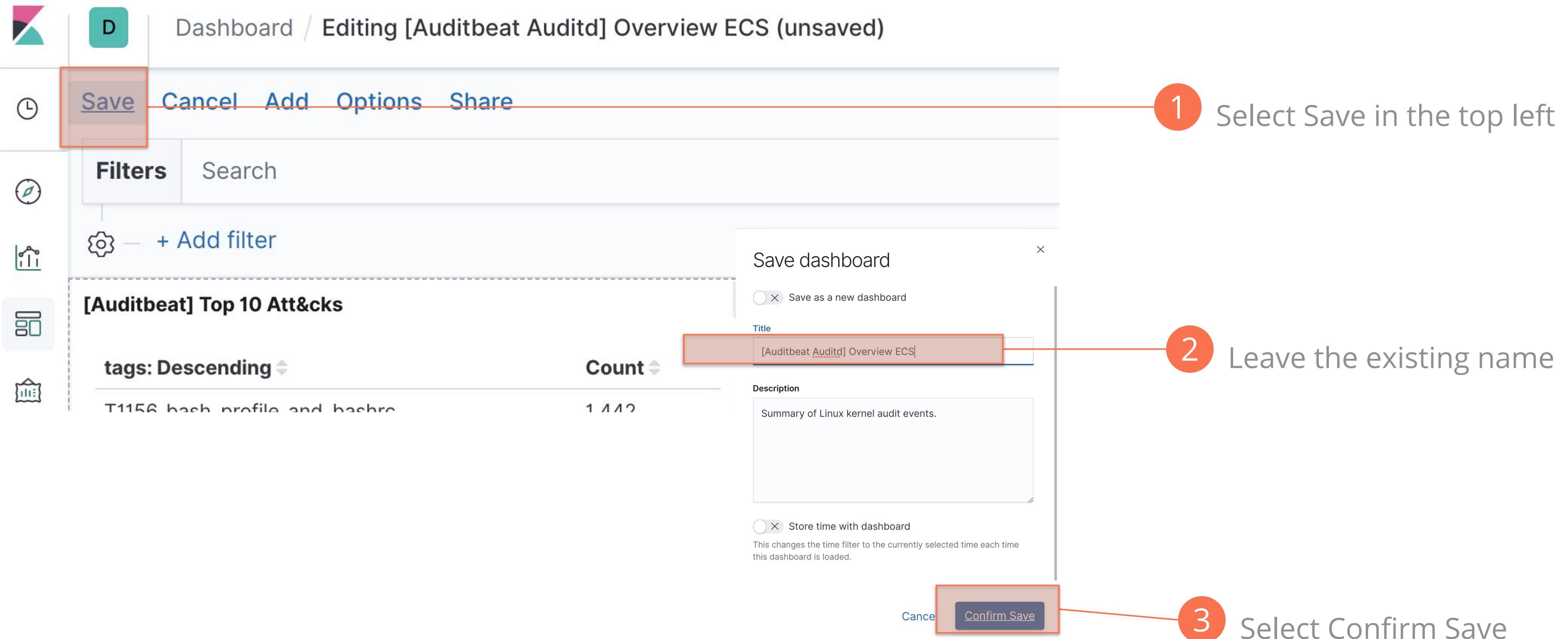
Resize other visualizations to better fit the screen

2

Resize the panel using the lower right resize arrow

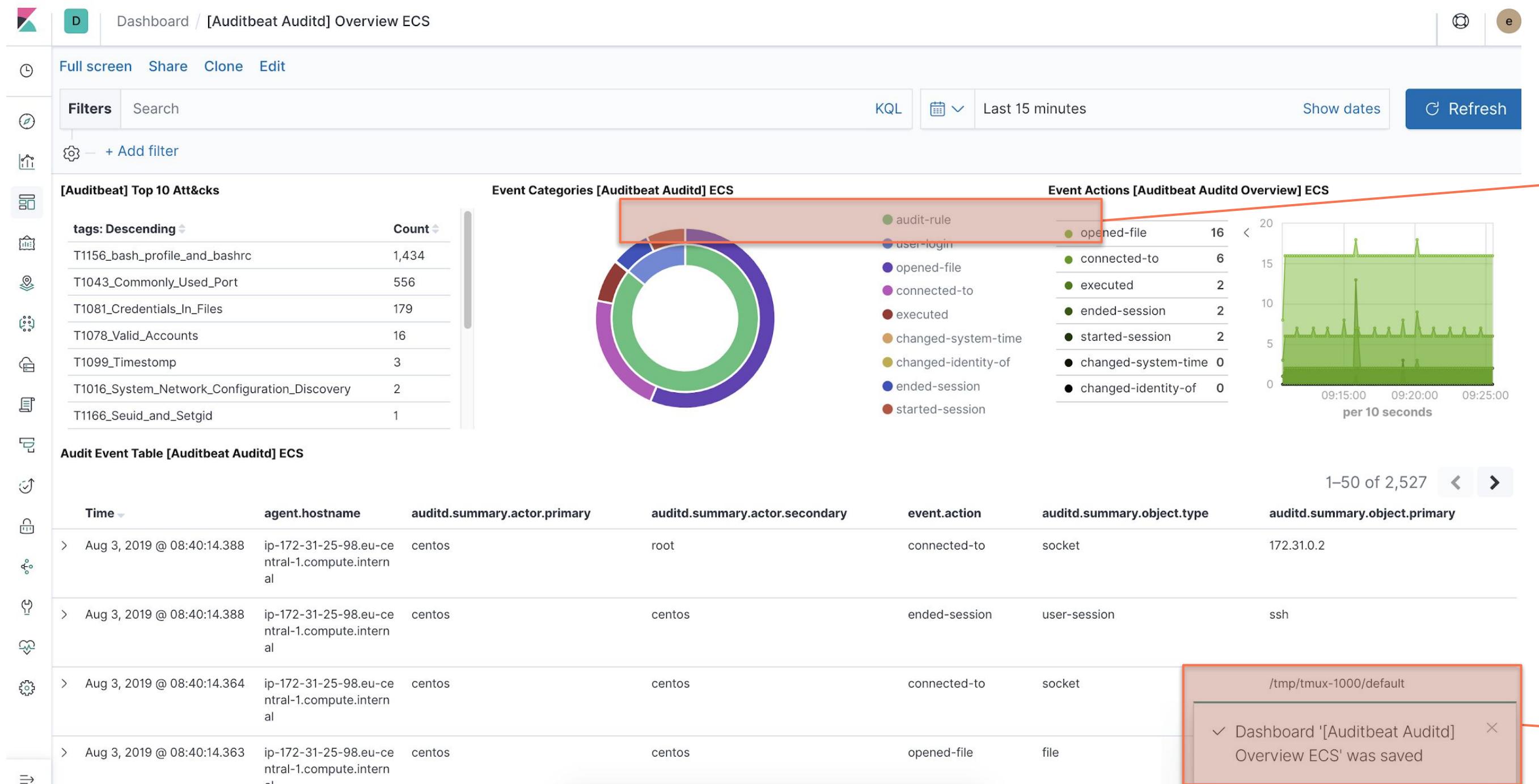
Save your updated dashboard

Top 10 attacks added to Auditbeat Overview



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

