SIEM Visualization Example 4: Users Added Or Removed From A Local Group (Within A Specific Timeframe)

In this SIEM visualization example, we aim to create a visualization to monitor user additions or removals from the local "Administrators" group from March 5th 2023 to date.

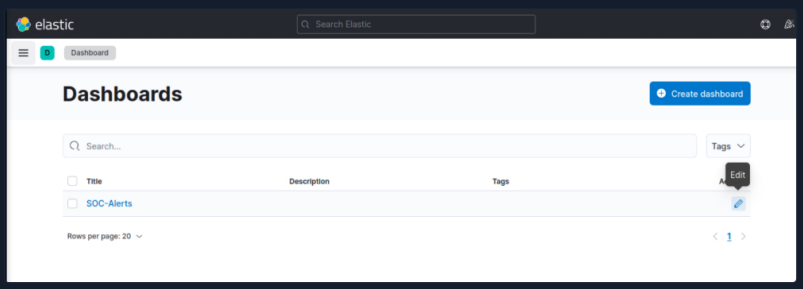
Our visualization will be based on the following Windows event logs.

- `4732: A member was added to a security-enabled local group`
- `4733: A member was removed from a security-enabled local group`

Navigate to the bottom of this section and click on `Click here to spawn the target system!`.

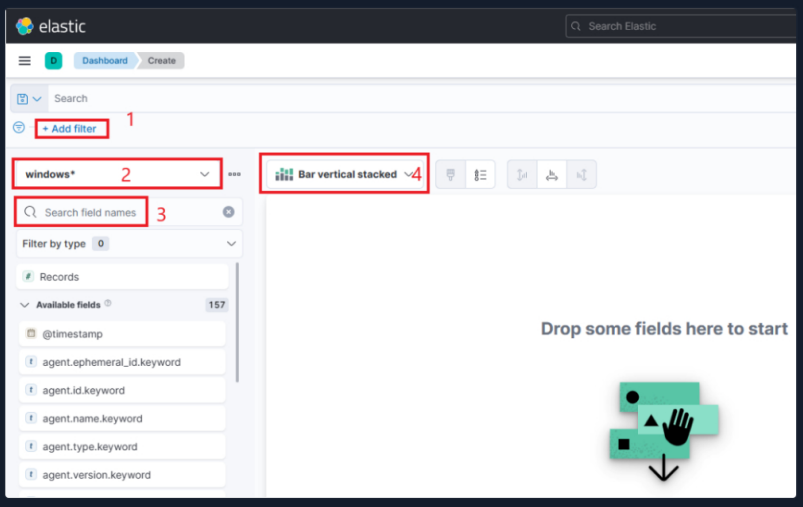
Navigate to `http://[Target IP]:5601`, click on the side navigation toggle, and click on "Dashboard".

A prebaked dashboard should be visible. Let's click on the "pencil"/edit icon.



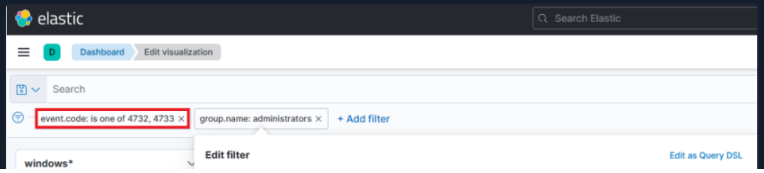
Now, to initiate the creation of our first visualization, we simply have to click on the "Create visualization" button.

Upon initiating the creation of our first visualization, the following new window will appear with various options and settings.



There are five things for us to notice on this window:

1. A filter option that allows us to filter the data before creating a graph. In this case our goal is to display user additions or removals from the local "Administrators" group. We can use a filter to only consider event IDs that match `4732 - A member was added to a security-enabled local group` and `4733 - A member was removed from a security-enabled local group`. We can also use a filter to only consider 4732 and 4733 events where the local group is the "Administrators" one.

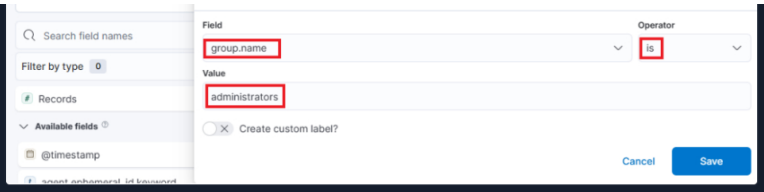


My Workstation

OFFLINE

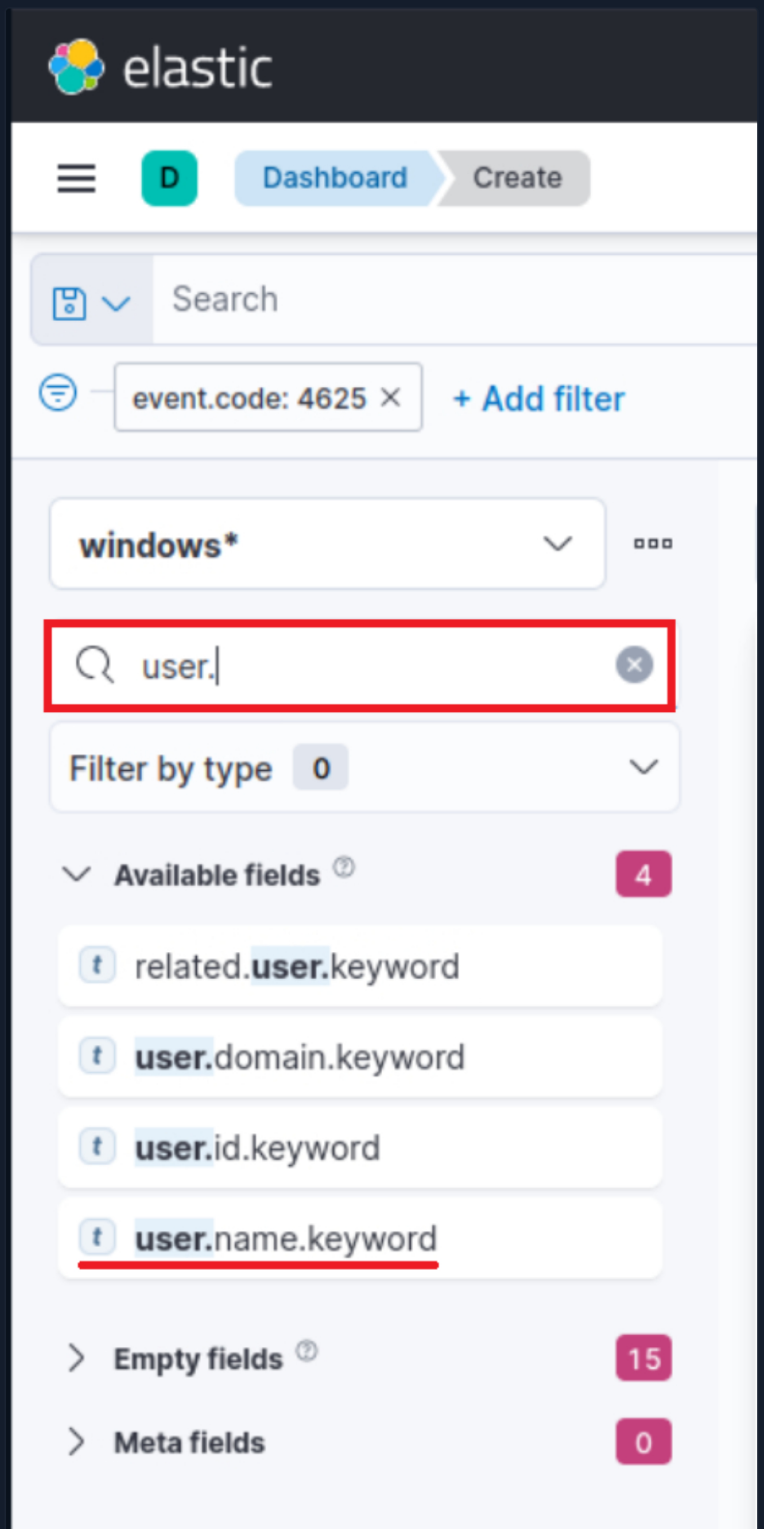
Start Instance

∞ / 1 spawns left

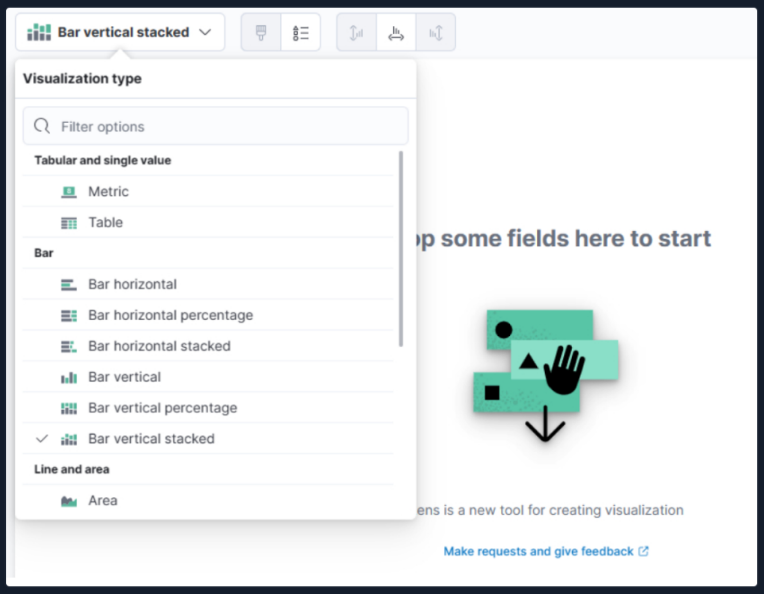


2. This field indicates the data set (index) that we are going to use. It is common for data from various infrastructure sources to be separated into different indices, such as network, Windows, Linux, etc. In this particular example, we will specify `windows*` in the "Index pattern".

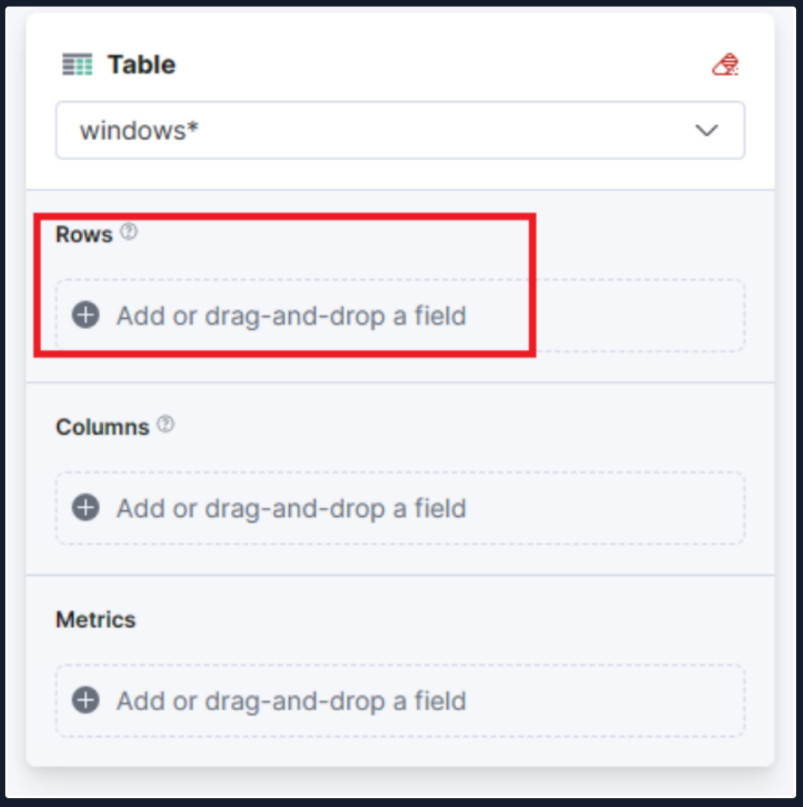
3. This search bar provides us with the ability to double-check the existence of a specific field within our data set, serving as another way to ensure that we are looking at the correct data. We are interested in the `user.name.keyword` field. We can use the search bar to quickly perform a search and verify if this field is present and discovered within our selected data set. This allows us to confirm that we are accessing the desired field and working with accurate data.



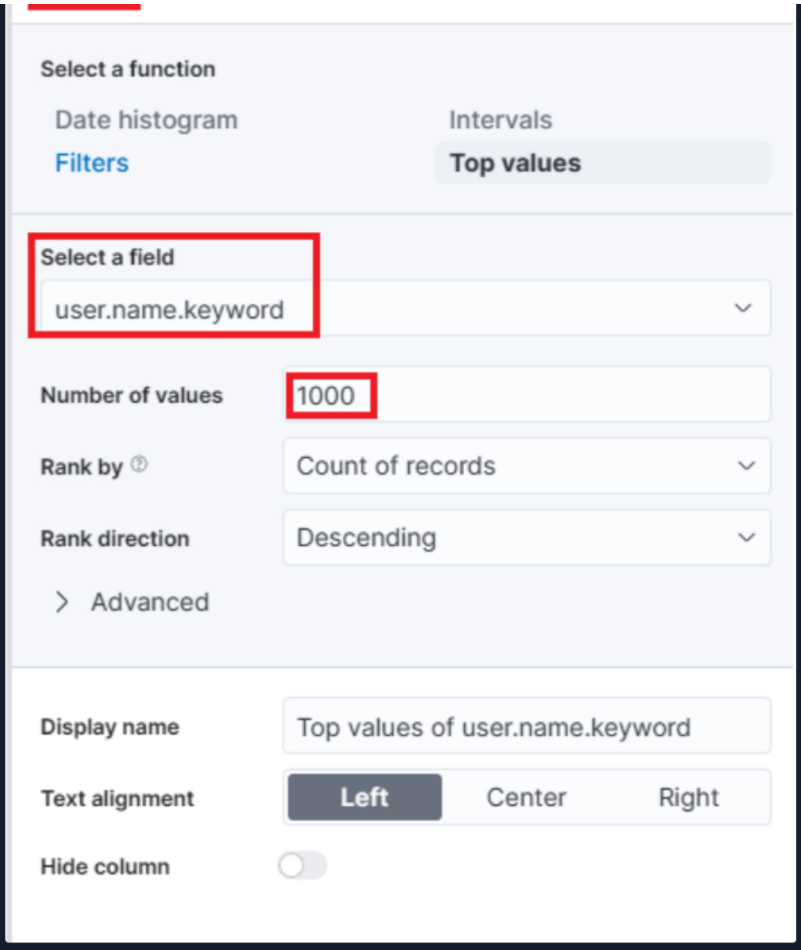
4. Lastly, this drop-down menu enables us to select the type of visualization we want to create. The default option displayed in the earlier image is "Bar vertical stacked". If we click on that button, it will reveal additional available options (image redacted as not all options fit on the screen). From this expanded list, we can choose the desired visualization type that best suits our requirements and data presentation needs.



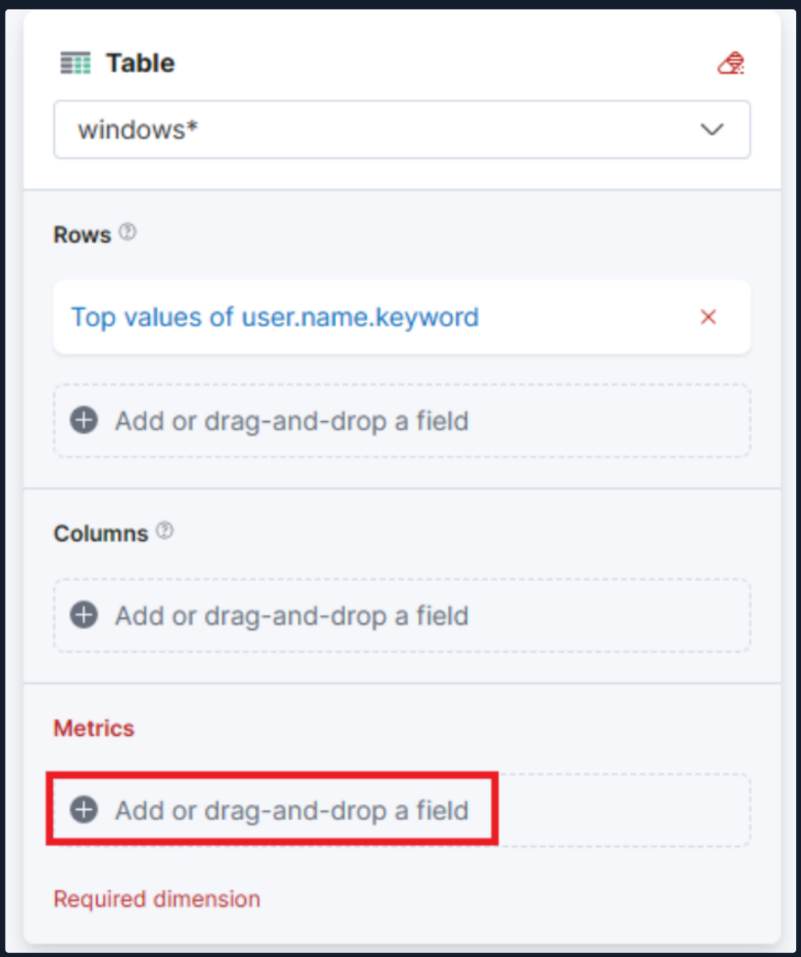
For this visualization, let's select the "Table" option. After selecting the "Table", we can proceed to click on the "Rows" option. This will allow us to choose the specific data elements that we want to include in the table view.



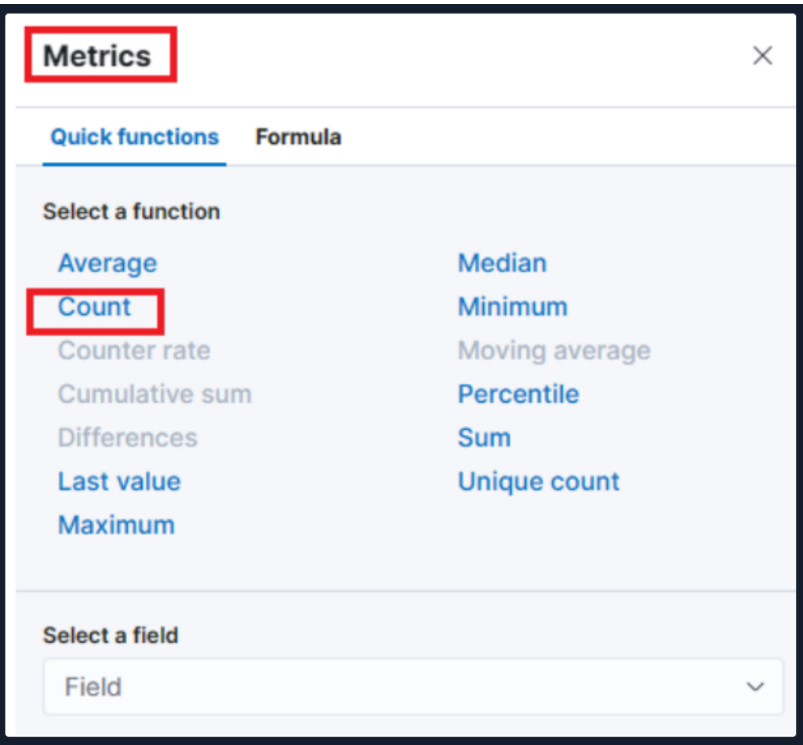
Let's configure the "Rows" settings as follows.



Moving forward, let's close the "Rows" window and proceed to enter the "Metrics" configuration.

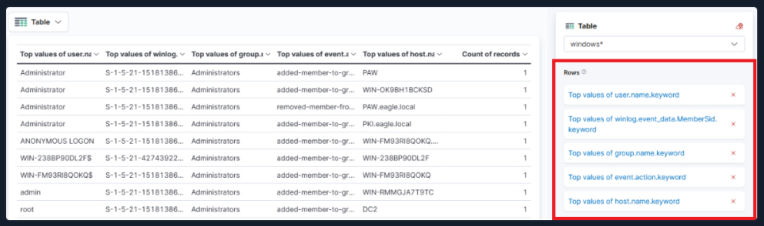


In the "Metrics" window, let's select "count" as the desired metric.



One final addition to the table is to include some more "Rows" settings to enhance our understanding.

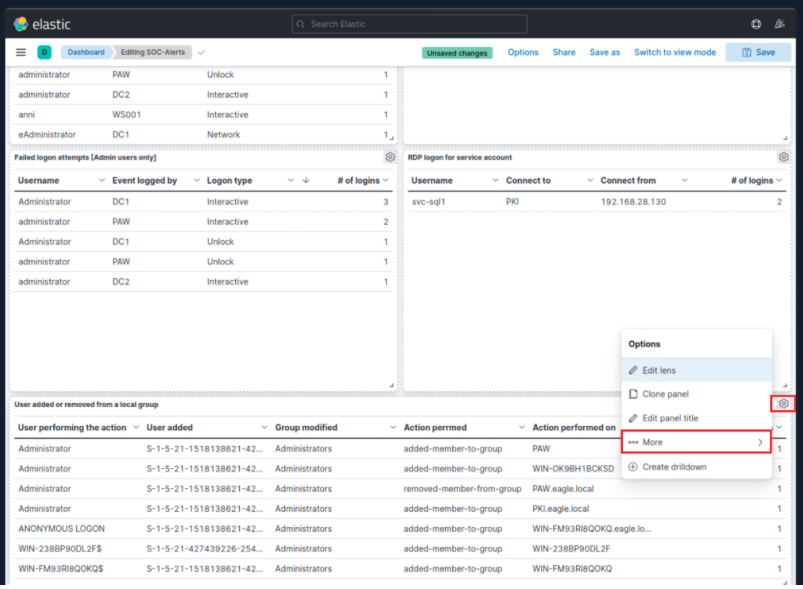
- Which user was added to or removed from the group? (`winlog.event_data.MemberSid.keyword` field)
- To which group was the addition or the removal performed? (double-checking that it is the "Administrators" one) (`group.name.keyword` field)
- Was the user added to or removed from the group? (`event.action.keyword` field)
- On which machine did the action occur? (`host.name.keyword` field)

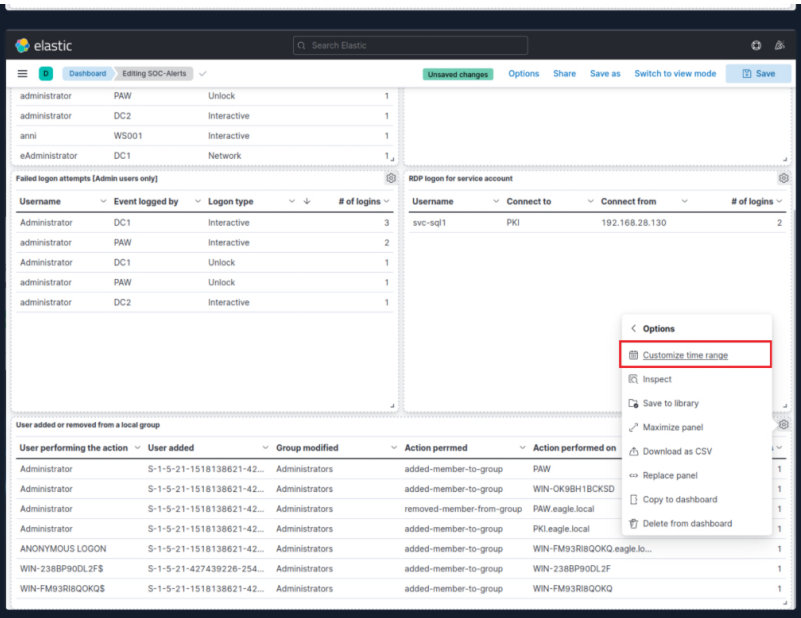


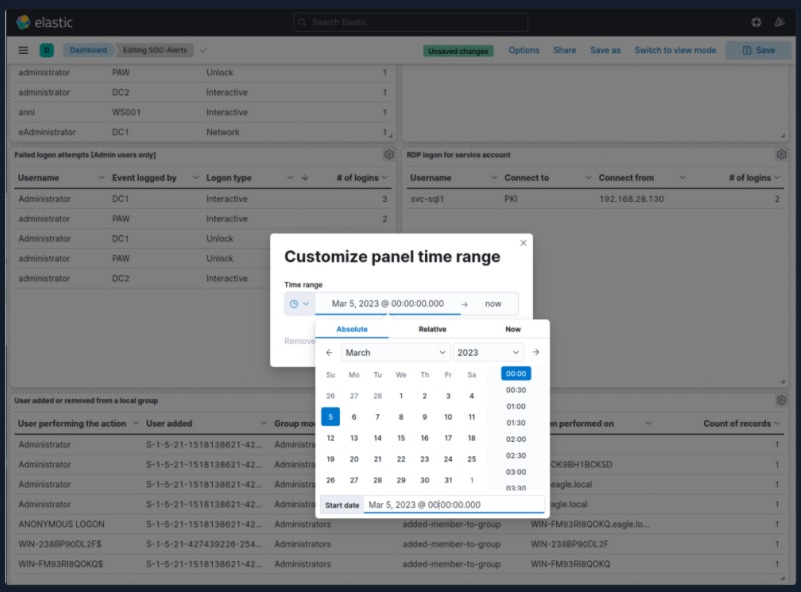
Click on "Save and return", and you will observe that the new visualization is added to the dashboard.

As discussed, we want to monitor user additions or removals from the local "Administrators" group *within a specific timeframe (March 5th 2023 to date)*.

We can narrow the scope of our visualization as follows.







Finally, let's click on the "Save" button so that all our edits persist.

Please allow 3-5 minutes for Kibana to become available after spawning the target of the questions below.

`Note`: As Elasticsearch uses `buckets` to aggregate data (time ranges, etc.) in groups, we must use an `absolute` time range for every occasion when creating the visualization. If we don't consider this, the bucket will showcase a weekly interval instead of a daily one.

VPN Servers

⚠ **Warning:** Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3 — Recommended — Medium Load

PROTOCOL

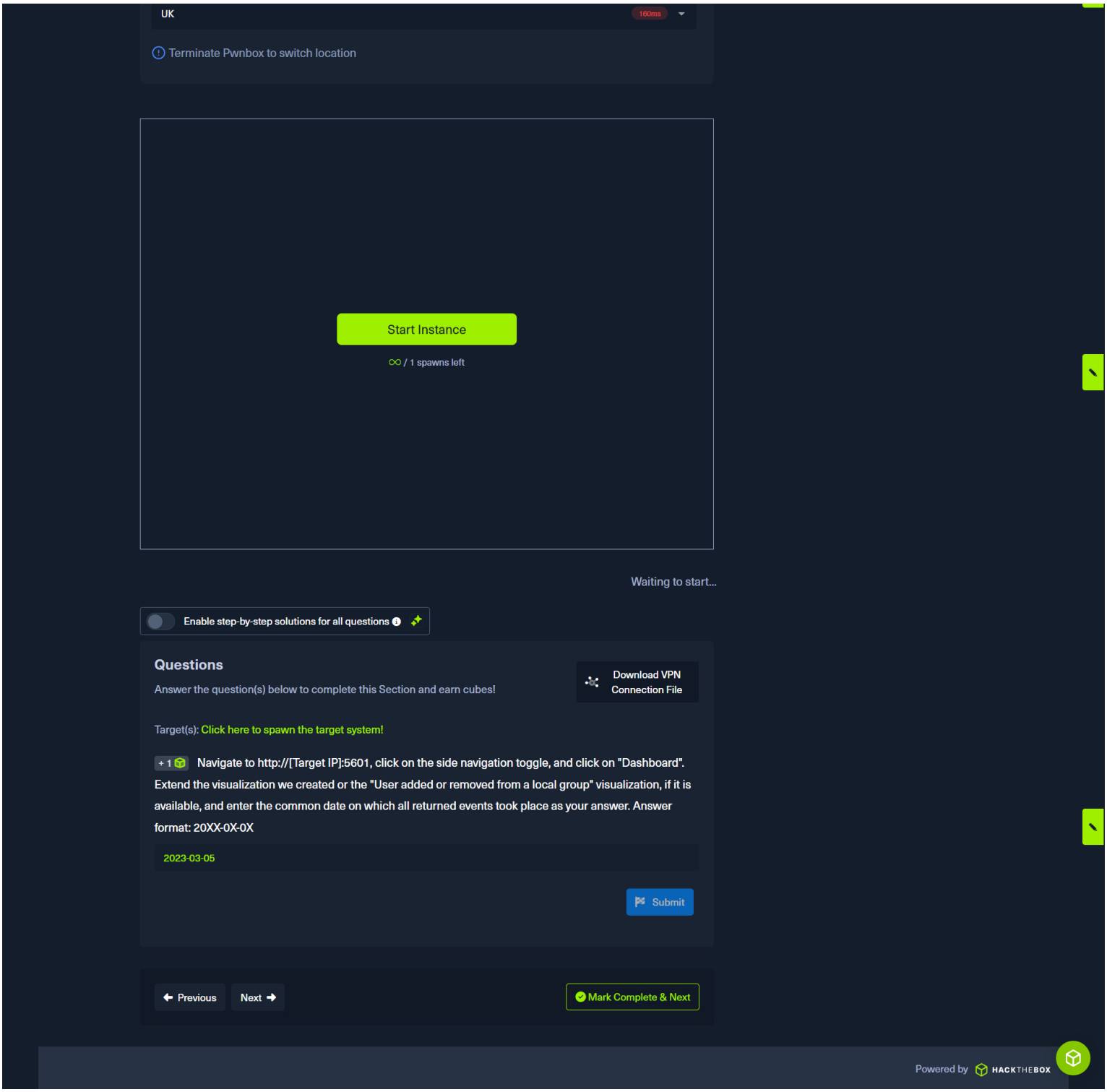
UDP 1337 TCP 443

DOWNLOAD VPN CONNECTION FILE

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location


UK
160ms
Terminate Pwnbox to switch location
Start Instance
∞ / 1 spawns left
Waiting to start...
Enable step-by-step solutions for all questions
Questions
Answer the question(s) below to complete this Section and earn cubes!
Download VPN Connection File
Target(s): Click here to spawn the target system!
+ 1
Navigate to http://[Target IP]:5601, click on the side navigation toggle, and click on "Dashboard". Extend the visualization we created or the "User added or removed from a local group" visualization, if it is available, and enter the common date on which all returned events took place as your answer. Answer format: 20XX-0X-0X
2023-03-05
Submit
Previous
Next
Mark Complete & Next
Powered by HACKTHEBOX