SIEM Visualization Example 3: Successful RDP Logon Related To Service Accounts

In this SIEM visualization example, we aim to create a visualization to monitor successful RDP logons specifically related to service accounts. Service account credentials are never used for RDP logons in corporate/real-world environments. We have been informed by the IT Operations department that all service accounts on the environment start with `svc-`.

The motivation for this visualization stems from the fact that service accounts often possess exceptionally high privileges. We need to keep a close eye on how service accounts are used.

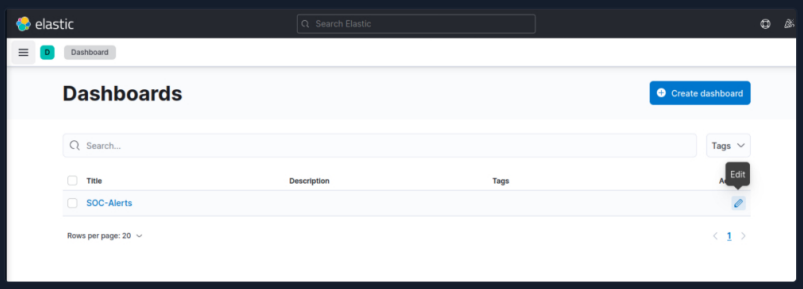
Our visualization will be based on the following Windows event log.

- `4624: An account was successfully logged on`

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

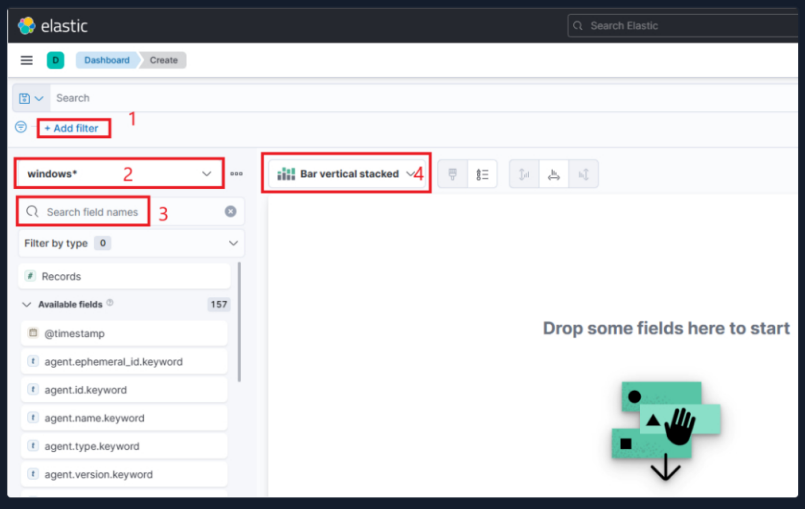
Navigate to `http://[Target IP]:5601`, click on the side navigation toggle, and click on "Dashboard".

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



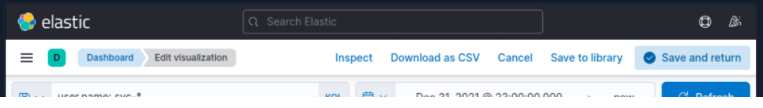
Now, to initiate the creation of our first visualization, we simply have to click on the "Create visualization" button.

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 successful RDP logons specifically related to service accounts. We can use a filter to only consider event IDs that match `4624 - An account was successfully logged on`. In this case though, we should also take into account the logon type which should be `RemoteInteractive` (`winlog.logon.type` field). The following images demonstrates how we can specify such filters.



Go to Questions

Table of Contents

SIEM & SOC Fundamentals
- SIEM Definition & Fundamentals
- Introduction To The Elastic Stack
- SOC Definition & Fundamentals
- MITRE ATT&CK & Security Operations
- SIEM Use Case Development

SIEM Visualization Development
- SIEM Visualization Example 1: Failed Logon Attempts (All Users)
- SIEM Visualization Example 2: Failed Logon Attempts (Disabled Users)
- SIEM Visualization Example 3: Successful RDP Logon Related To Service Accounts
- SIEM Visualization Example 4: Users Added Or Removed From A Local Group (Within A Specific Timeframe)

Alert Triaging
- The Triaging Process

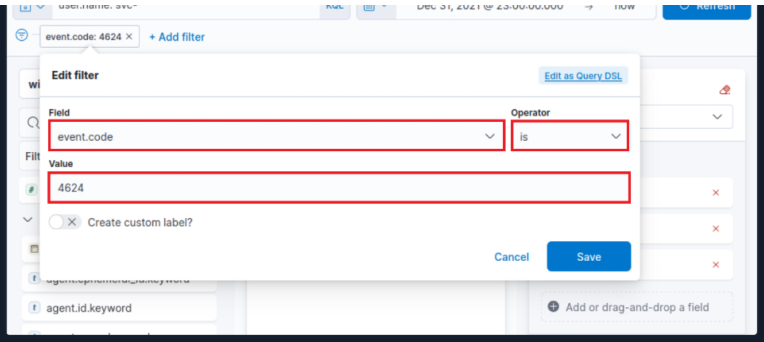
Skills Assessment
- Skills Assessment

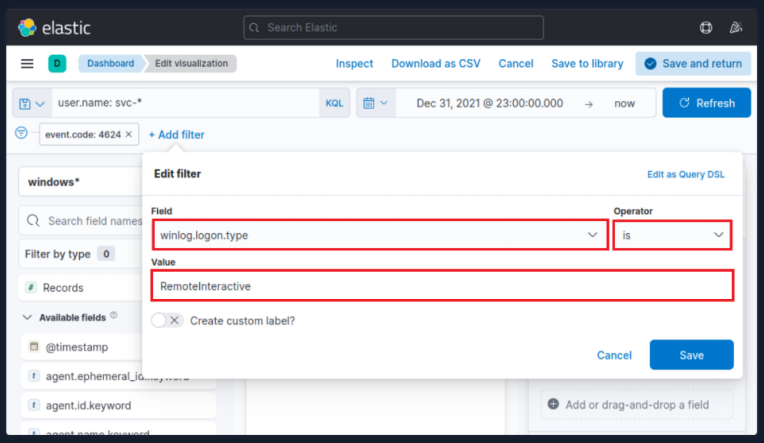
My Workstation

OFFLINE

Start Instance

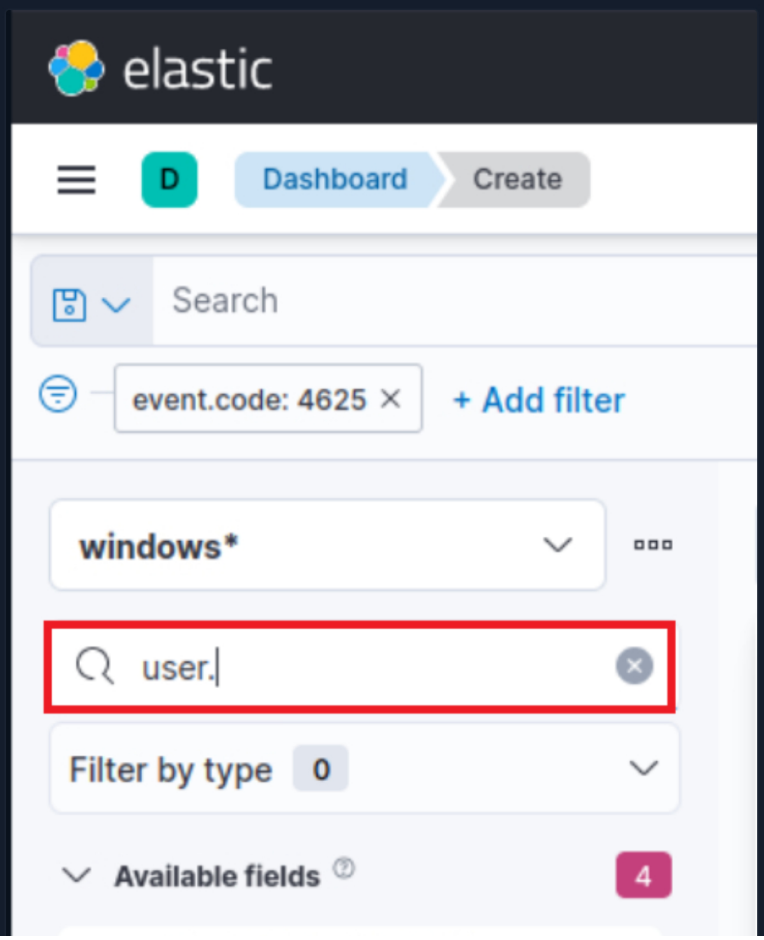
∞ / 1 spawns left

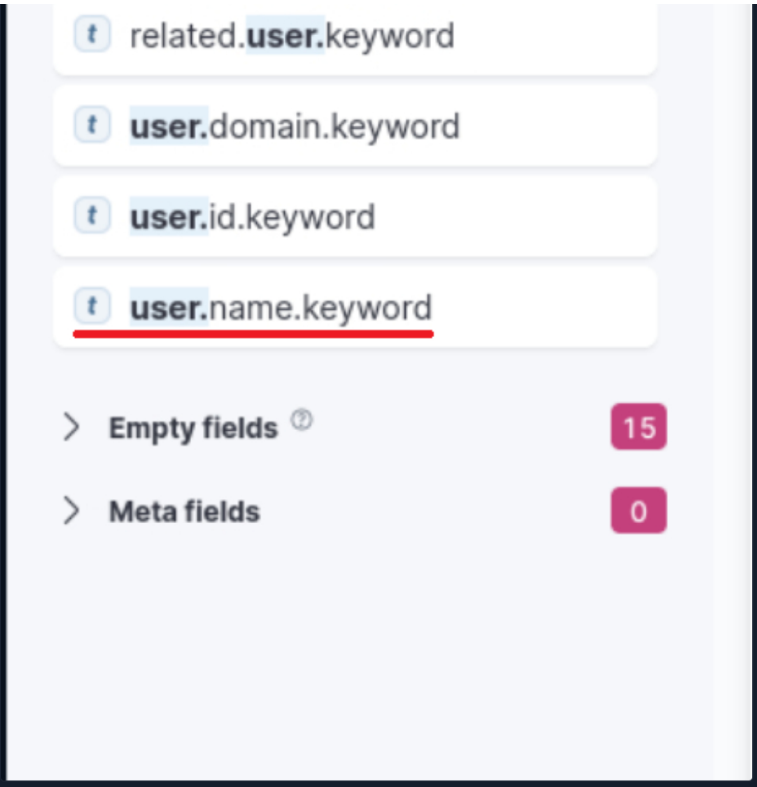




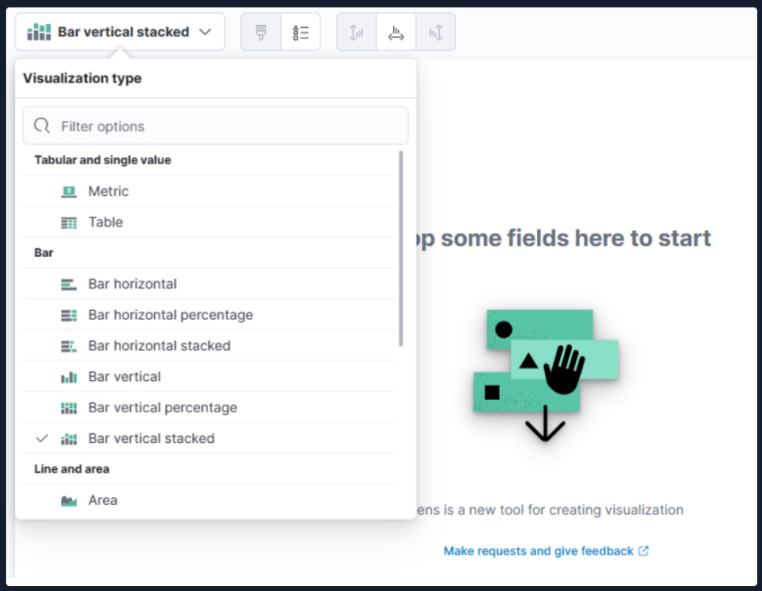
2. This field indicates the data set (index) that we are going to use. It is common for data from various infrastructure sources to be separated into different indices, such as network, Windows, Linux, etc. In this particular example, we will specify `windows*` in the "Index pattern".

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.

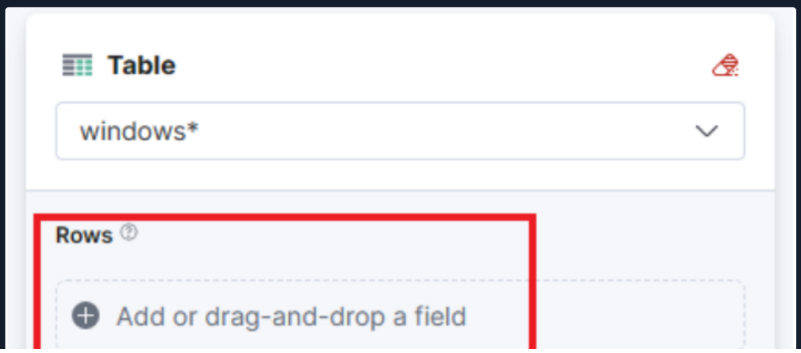


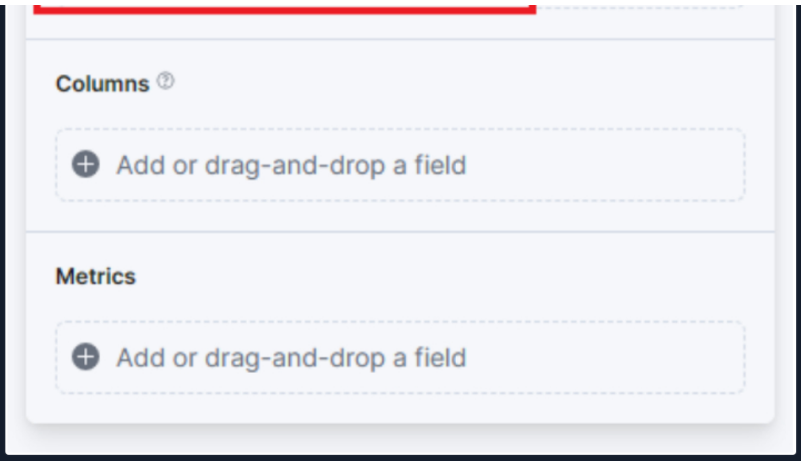


4. Lastly, this drop-down menu enables us to select the type of visualization we want to create. The default option displayed in the earlier image is "Bar vertical stacked". If we click on that button, it will reveal additional available options (image redacted as not all options fit on the screen).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

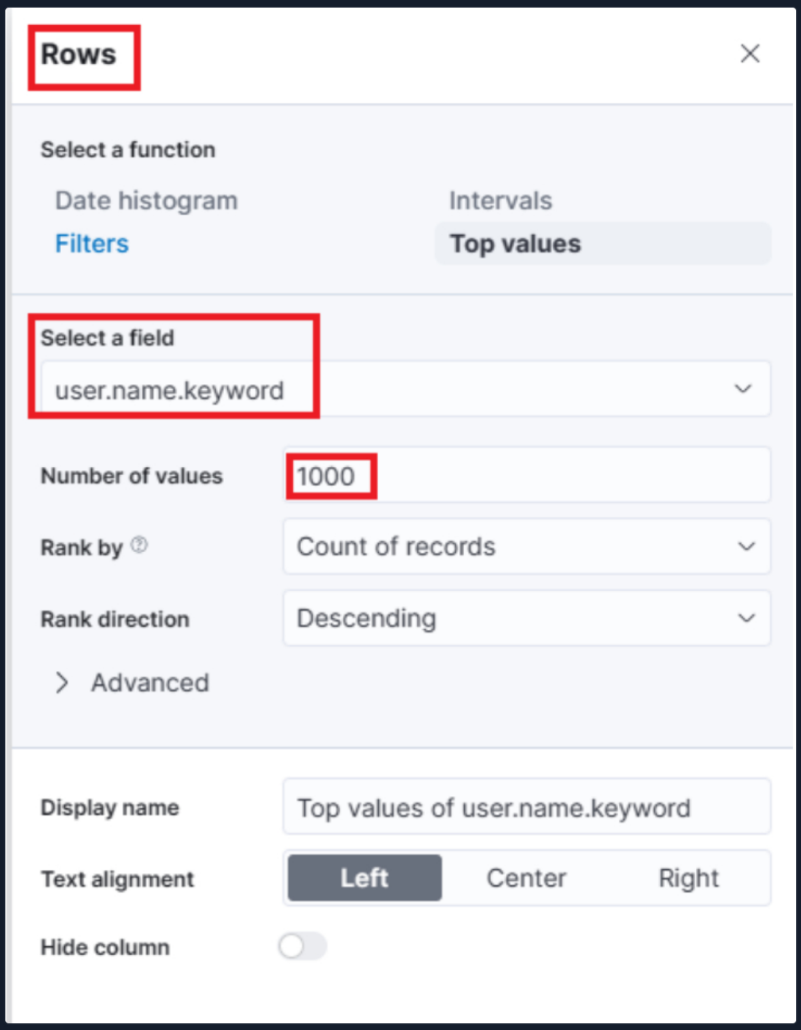


For this visualization, let's select the "Table" option. After selecting the "Table", we can proceed to click on the "Rows" option. This will allow us to choose the specific data elements that we want to include in the table view.

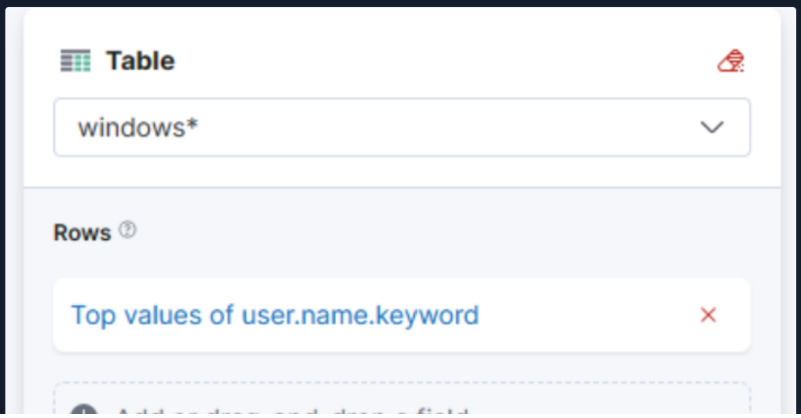


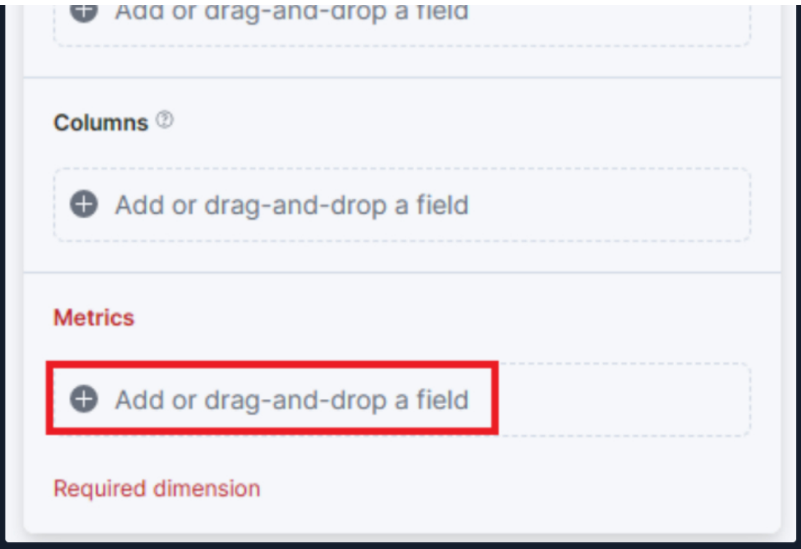


Let's configure the "Rows" settings as follows.

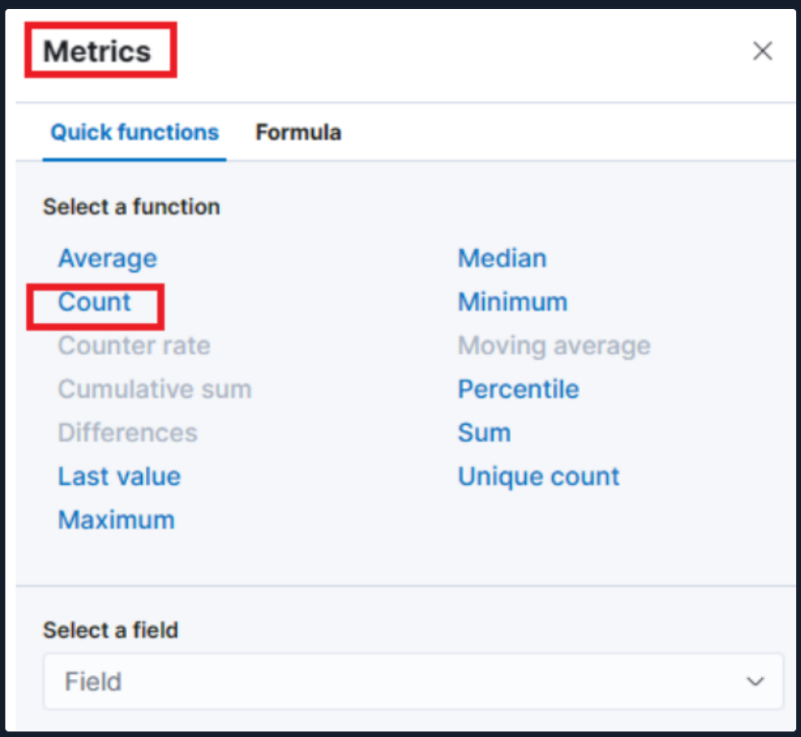


Moving forward, let's close the "Rows" window and proceed to enter the "Metrics" configuration.

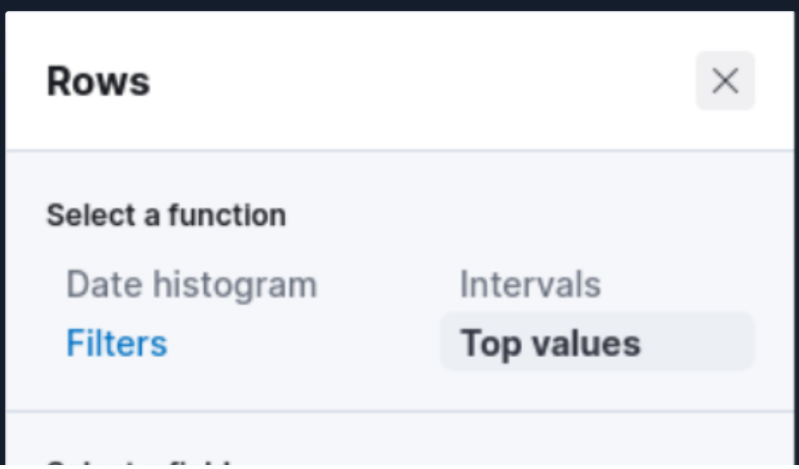




In the "Metrics" window, let's select "count" as the desired metric.



One final addition to the table is to include two more "Rows" settings to show the machine where the successful RDP logon attempt occurred and the machine that initiated the successful RDP logon attempt. To do this, we will select the `host.hostname.keyword` field that represents the computer reporting the successful RDP logon attempt and the `related.ip.keyword` field that represents the IP of the computer initiating the succsessful RDP logon attempt. This will allow us to display the involved machines alongside the count of successful logon attempts, as shown in the image.



Select a field

host.hostname.keyword

Number of values: 1000

Rank by: # of logins

Rank direction: Descending

> Advanced

Display name: Connect to

Text alignment: Left | Cent... | Right

Hide column

Rows

Select a function

Date histogram | Intervals

Filters | **Top values**

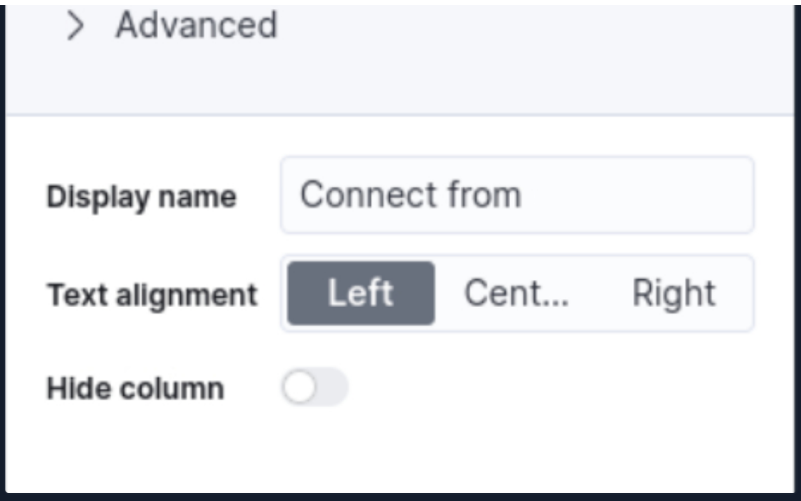
Select a field

related.ip.keyword

Number of values: 1000

Rank by: # of logins

Rank direction: Descending

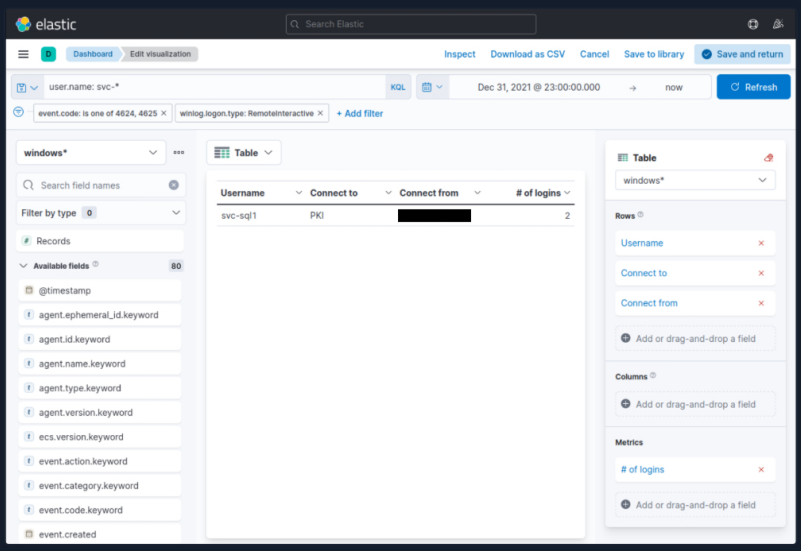


As discussed, we want to monitor successful RDP logons specifically related to service accounts, knowing for a fact that all service accounts of the environment start with `svc-`. So, to conclude our visualization we need to specify the following KQL query.

SIEM Visualization Example 3: Successful RDP Logon Related To Service Accounts

```
user.name: svc-*
```

Note: As you can see we don't use the `.keyword` field in KQL queries.

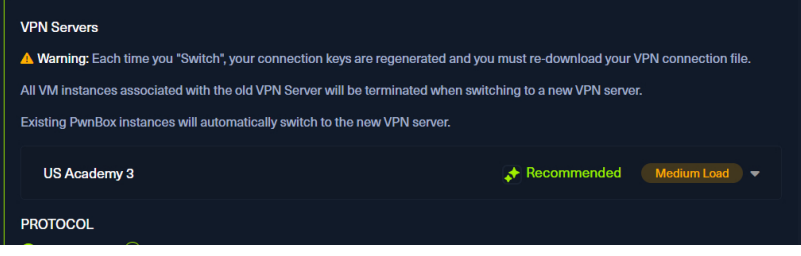


Now we can see four columns in the table, which contain the following information:

1. The service account whose credentials generated the successful RDP logon attempt event.
2. The machine on which the logon attempt occurred.
3. The IP of the machine that initiated the logon attempt.
4. The number of times the event has occurred (based on the specified time frame or the entire data set, depending on the settings).

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

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



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 159ms

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". Browse the visualization we created or the "RDP logon for service account" visualization, if it is available, and enter the IP of the machine that initiated the successful RDP logon using service account credentials as your answer.

192.168.28.130

Submit

Previous Next

Mark Complete & Next