SIEM Visualization Example 2: Failed Logon Attempts (Disabled Users)

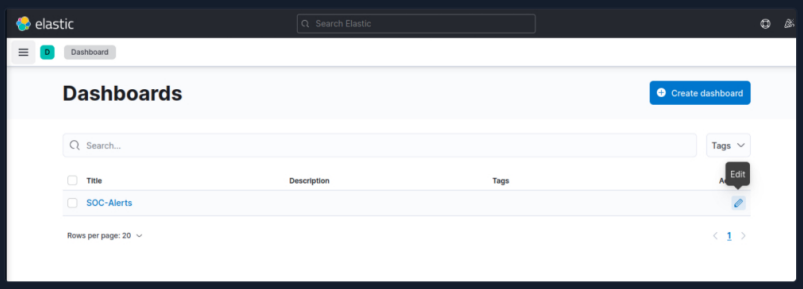
In this SIEM visualization example we want to create visualization to monitor failed login attempts against disabled users.

We mention "failed" because it is not possible to log in with a disabled user, so it will never be successful even if the correct credentials are provided. In a scenario where the correct credentials are provided, the Windows logs will contain an additional SubStatus value of 0xC0000072, that indicates the reason of the failure.

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

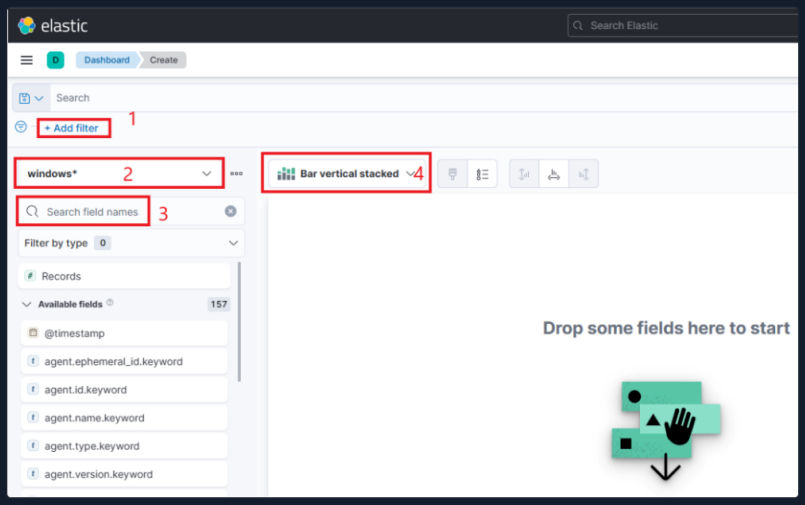
Navigate to `http://[Target IP]:5601`, click on the side navigation toggle, and click on "Dashboard".

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



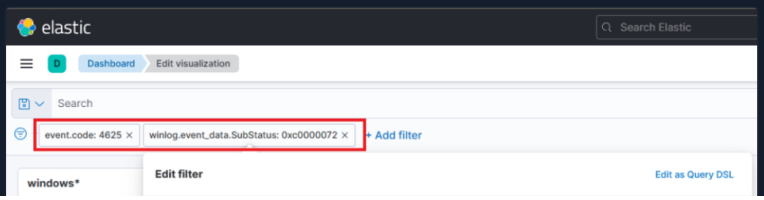
Now, to initiate the creation of our first visualization, we simply have to click on the "Create visualization" button.

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



There are four 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 failed logon attempts against disabled users only. We can use a filter to only consider event IDs that match `4625 - Failed logon attempt on a Windows system`, like we did in the previous visualization example. In this case though, we should also take into account the SubStatus (`winlog.event_data.SubStatus` field) that indicates, when set to 0xC0000072, that the failure is due to a logon with disabled user. The following image demonstrates how we can specify such a filter.



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

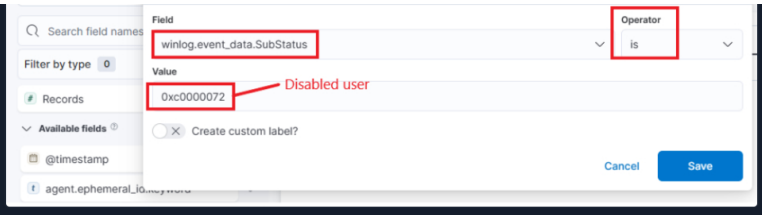
Skills Assessment
- Skills Assessment

My Workstation

OFFLINE

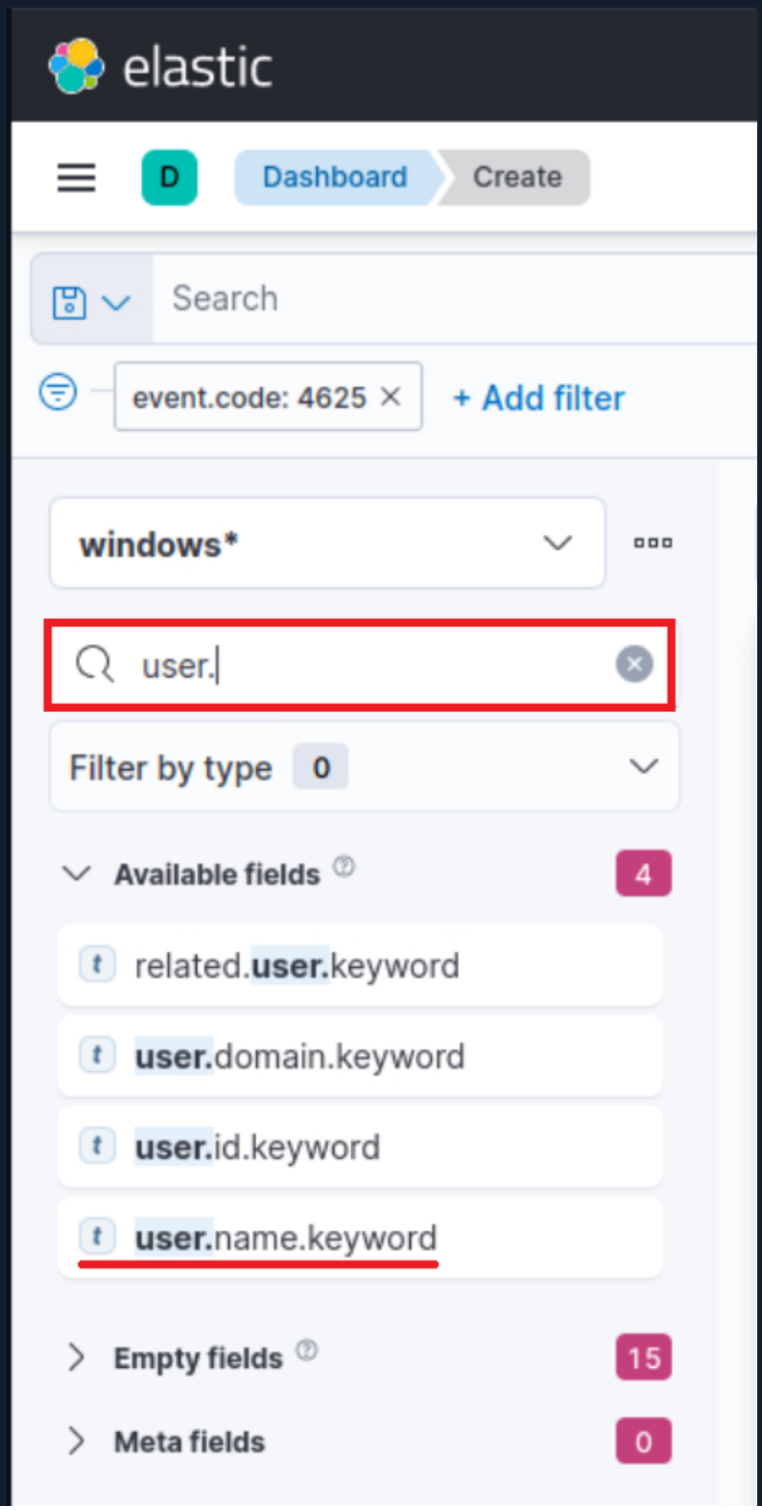
Start Instance

∞ / 1 spawns left

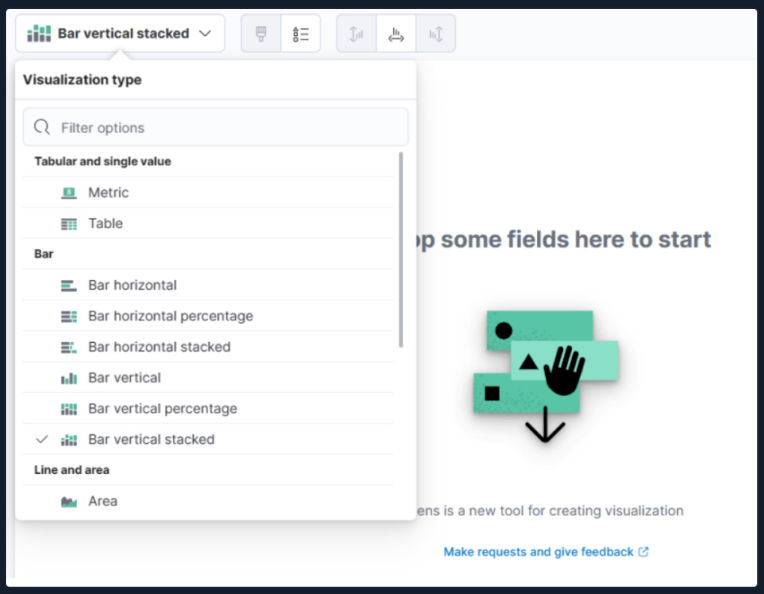


2. This field indicates the data set (index) that we are going to use. It is common for data from various infrastructure sources to be separated into different indices, such as network, Windows, Linux, etc. In this particular example, we will specify `windows*` in the "Index pattern".

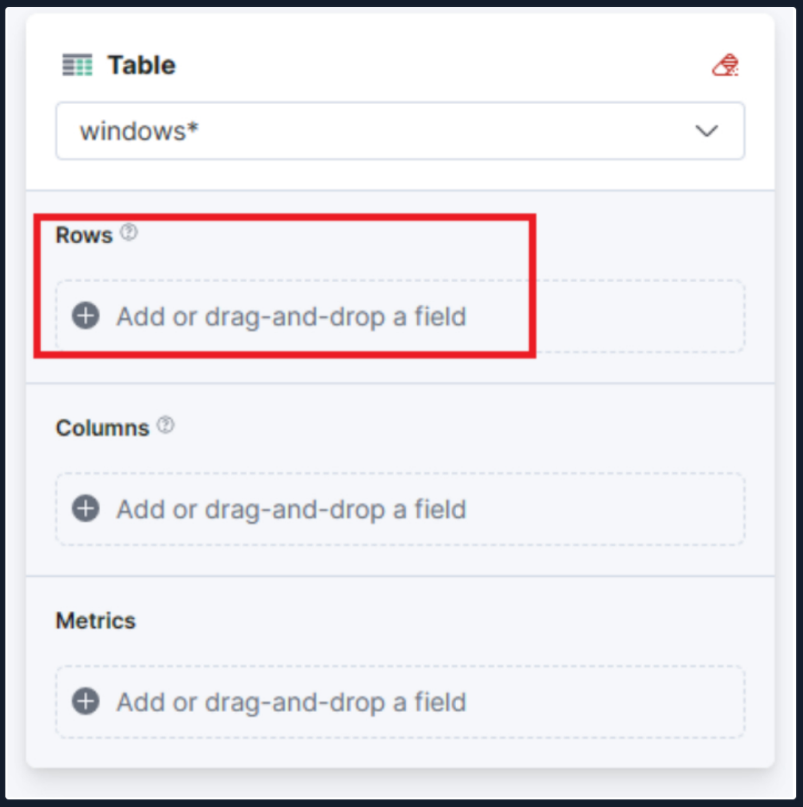
3. This search bar provides us with the ability to double-check the existence of a specific field within our data set, serving as another way to ensure that we are looking at the correct data. Like in the previous visualization, we are interested in the `user.name.keyword` field. We can use the search 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.



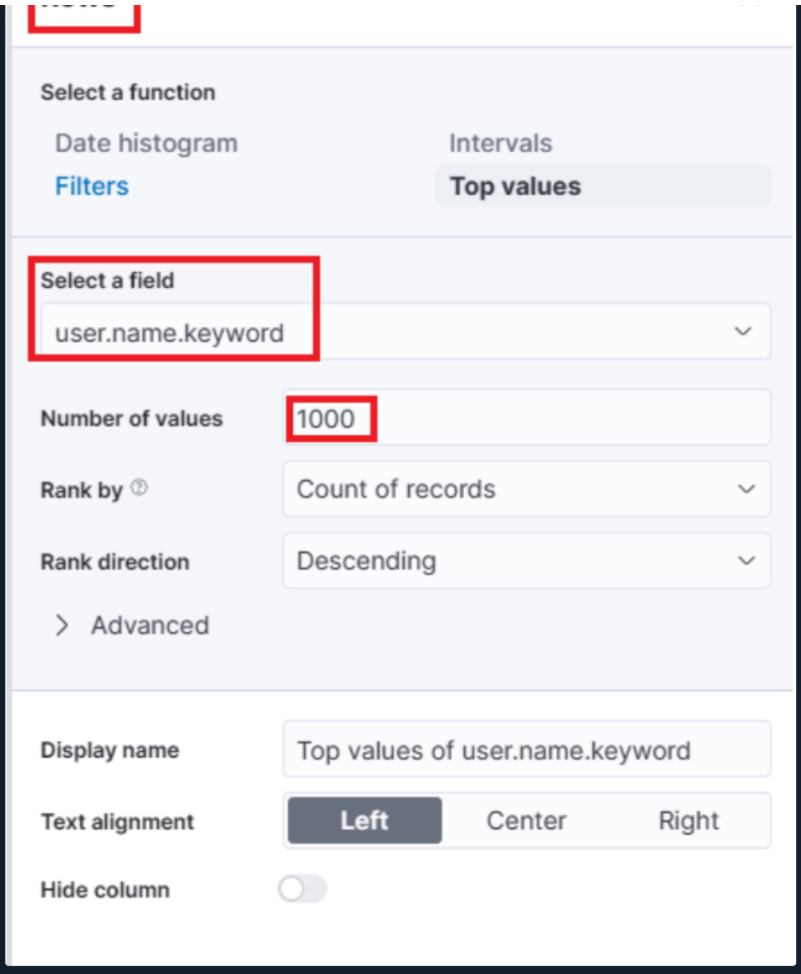
4. Lastly, this drop-down menu enables us to select the type of visualization we want to create. The default option displayed in the earlier image is "Bar vertical stacked". If we click on that button, it will reveal additional available options (image redacted as not all options fit on the screen).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



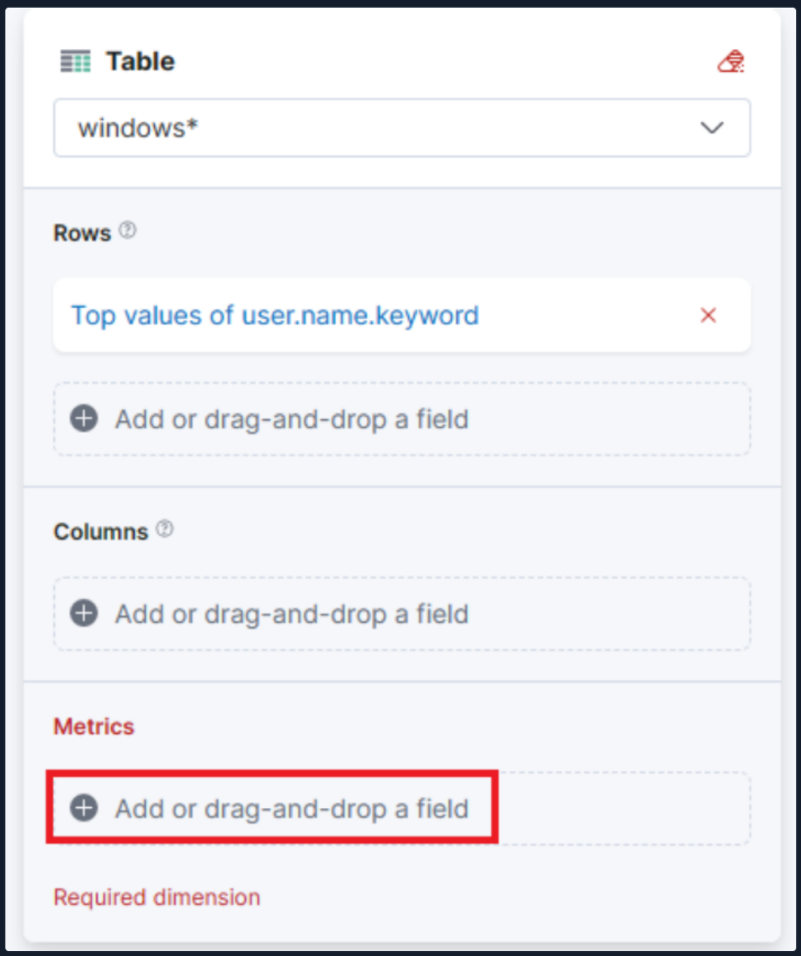
For this visualization, let's select the "Table" option. After selecting the "Table", we can proceed to click on the "Rows" option. This will allow us to choose the specific data elements that we want to include in the table view.



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

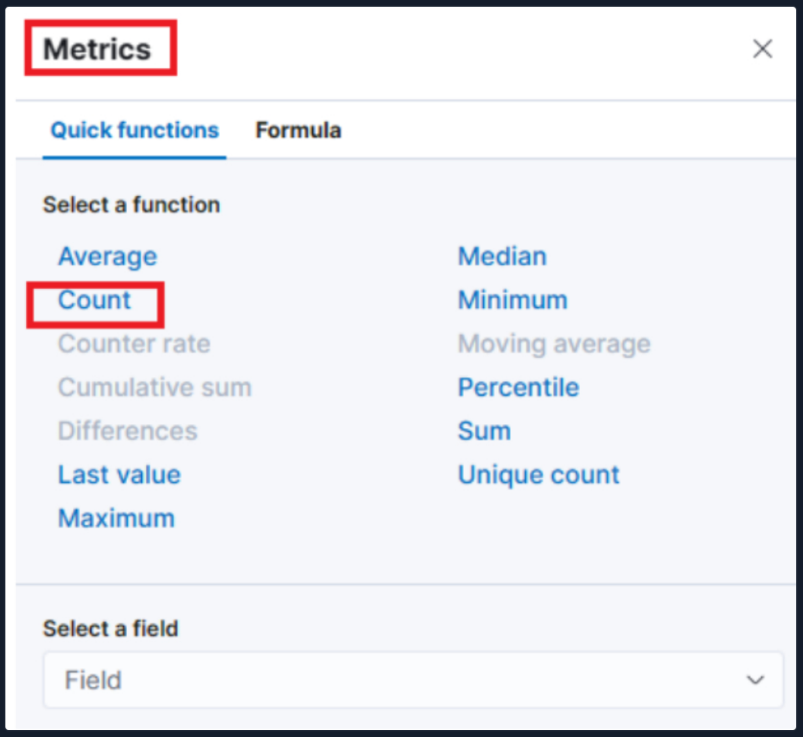


Moving forward, let's close the "Rows" window and proceed to enter the "Metrics" configuration.

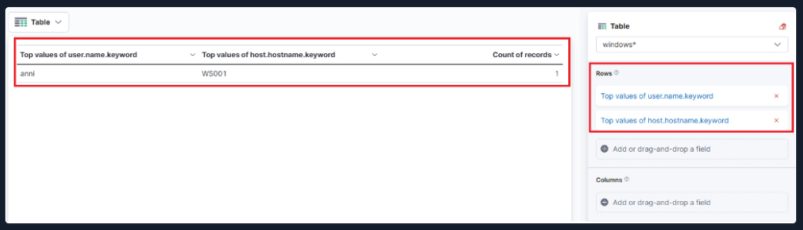


In the "Metrics" window, let's select "count" as the desired metric.

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



One final addition to the table is to include another "Rows" setting to show the machine where the failed logon attempt occurred. To do this, we will select the `host.hostname.keyword` field, which represents the computer reporting the failed logon attempt. This will allow us to display the hostname or machine name alongside the count of failed logon attempts, as shown in the image.

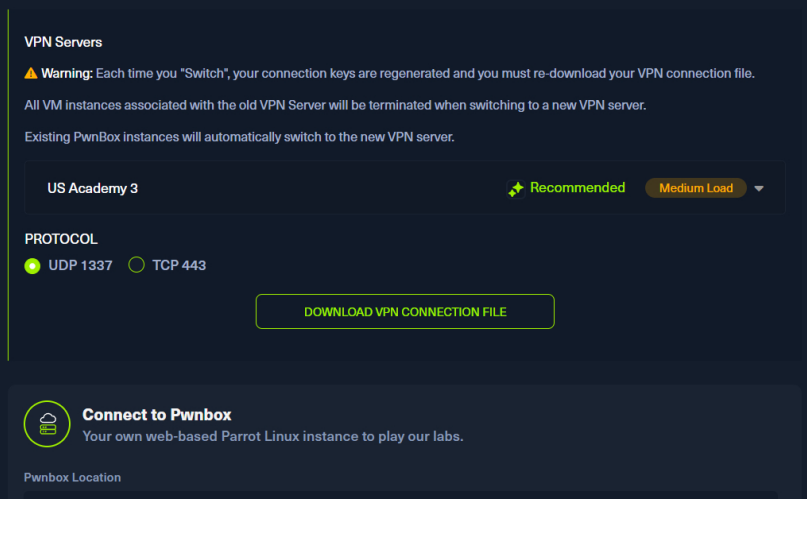


Now we can see three columns in the table, which contain the following information:

1. The disabled user whose credentials generated the failed logon attempt event.
2. The machine on which the logon attempt occurred.
3. 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.



UK 161ms

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". Either create a new visualization or edit the "Failed logon attempts [Disabled user]" visualization, if it is available, so that it includes failed logon attempt data related to disabled users including the logon type. What is the logon type in the returned document?

Interactive

Submit

+ 1 Navigate to http://[Target IP]:5601, click on the side navigation toggle, and click on "Dashboard". Either create a new visualization or edit the "Failed logon attempts [Admin users only]" visualization, if it is available, so that it includes failed logon attempt data where the username field contains the keyword "admin" anywhere within it. What should you specify after user.name: in the KQL query?

admin

Submit

Previous Next

Mark Complete & Next