

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

[? Go to Questions](#)

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](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.

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

[Start Instance](#)

∞ / 1 spawns left

The screenshot shows the Kibana interface with a search bar at the top containing "event.code: 4624 X + Add filter". Below the search bar is a modal titled "Edit filter" with the following fields:

- Field: event.code
- Operator: is
- Value: 4624

At the bottom of the modal are "Cancel" and "Save" buttons.

The screenshot shows the Kibana interface with a search bar at the top containing "user.name: svc-* KQL Dec 31, 2021 @ 23:00:00.000 now Refresh". Below the search bar is a modal titled "Edit filter" with the following fields:

- Field: winlog.logon.type
- Operator: is
- Value: RemoteInteractive

At the bottom of the modal are "Cancel" and "Save" buttons.

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.

The screenshot shows the Kibana Dashboard interface with a search bar at the top containing "Search event.code: 4625 X + Add filter". Below the search bar is a modal titled "Edit filter" with the following fields:

- Field: windows*

Below the modal is a search bar containing "user.name.keyword" with a red border around it. At the bottom of the interface are sections for "Filter by type" (0) and "Available fields" (4).

t related.user.keyword

t user.domain.keyword

t user.id.keyword

t **user.name.keyword**

> Empty fields ② 15

> Meta fields 0

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.

Bar vertical stacked

Visualization type

Filter options

Tabular and single value

- Metric
- Table

Bar

- Bar horizontal
- Bar horizontal percentage
- Bar horizontal stacked
- Bar vertical
- Bar vertical percentage
- Bar vertical stacked

Line and area

- Area

Drop some fields here to start

Make requests and give feedback

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.

Table

windows*

Rows ②

Add or drag-and-drop a field

The screenshot shows two sections of a configuration interface. The top section is labeled 'Columns' and contains a button '+ Add or drag-and-drop a field'. The bottom section is labeled 'Metrics' and also contains a similar button '+ Add or drag-and-drop a field'. Both sections have a dashed border around them.

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

The screenshot shows the 'Rows' configuration window. At the top, there is a title 'Rows' and a close button 'X'. Below the title, there is a section 'Select a function' with two options: 'Date histogram' and 'Intervals'. Underneath these are two tabs: 'Filters' (blue) and 'Top values' (grayed out). A red box highlights the 'Select a field' dropdown below. The dropdown contains the value 'user.name.keyword'. Another red box highlights the 'Number of values' input field, which contains the value '1000'. Below these are three dropdowns: 'Rank by' (Count of records), 'Rank direction' (Descending), and 'Advanced' (with a right-pointing arrow). In the bottom half of the window, there are three sections: 'Display name' (Top values of user.name.keyword), 'Text alignment' (Left, Center, Right, with Left selected), and 'Hide column' (with a toggle switch). A red box highlights the 'Text alignment' section.

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

The screenshot shows the 'Table' configuration window. At the top, there is a title 'Table' with a grid icon and a cloud icon. Below the title is a search bar containing the text 'windows*'. Underneath the search bar is a section labeled 'Rows' with a blue link 'Top values of user.name.keyword'. A red 'X' button is located to the right of this link. The rest of the window is mostly blank.

The screenshot shows a user interface for defining metrics. At the top, there's a placeholder box with a plus icon and the text "Add or drag-and-drop a field". Below it, under "Metrics", is another such placeholder box. A red box highlights the second placeholder box. At the bottom, the text "Required dimension" is displayed.

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

The screenshot shows the "Metrics" window with the "Quick functions" tab selected. A red box highlights the "Count" option in the list. Other options include Average, Median, Minimum, Counter rate, Moving average, Cumulative sum, Percentile, Differences, Sum, Last value, Unique count, and Maximum. Below this, there's a "Select a field" section with a dropdown menu set to "Field".

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 successful RDP logon attempt. This will allow us to display the involved machines alongside the count of successful logon attempts, as shown in the image.

The screenshot shows the "Rows" window with the "Select a function" section. A red box highlights the "Top values" option. Other options include Date histogram and Intervals. Below this, there's a "Filters" section.

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

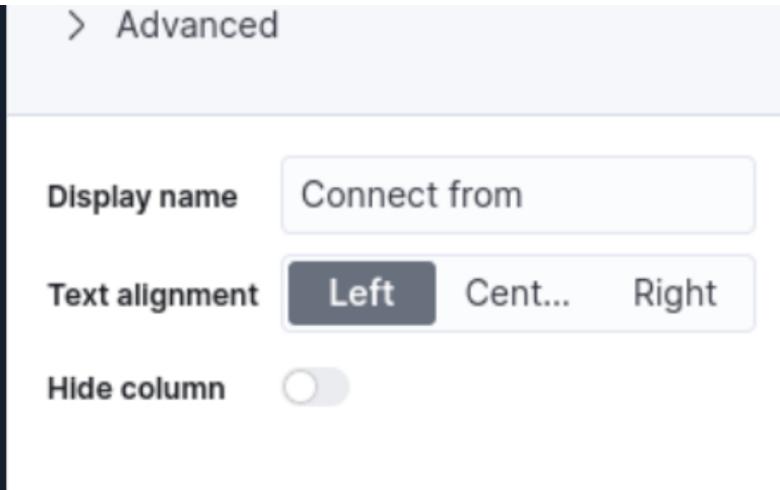
Rank by ⓘ

of logins

Rank direction

Descending

> Advanced



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

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

The screenshot shows the Elastic Stack interface with the following details:

- Header:** Search bar with "Search Elastic".
- Top Bar:** Dashboard, Edit visualization, Inspect, Download as CSV, Cancel, Save to library, Save and return.
- Search Bar:** Contains filters: "user.name: svc-*" and "event.code: is one of 4624, 4825" (with a dropdown for "winlog.logon.type: RemoteInteractive"). Buttons include "KQL", "Add filter", "Dec 31, 2021 @ 23:00:00.000" (dropdown), "now", and "Refresh".
- Left Panel:** A sidebar with sections:
 - Available fields: @timestamp, agent.ephemeral._id.keyword, agent.id.keyword, agent.name.keyword, agent.type.keyword, agent.version.keyword, ecs.version.keyword, event.action.keyword, event.category.keyword, event.code.keyword, event.created.
 - Records: A table with columns: Username (svc-sq1), Connect to (PKI), Connect from (redacted), # of logins (2).
- Right Panel:** A sidebar with sections:
 - Table: A table with columns: Username (svc-sq1), Connect to (PKI), Connect from (redacted).
 - Rows: Fields for Username, Connect to, and Connect from.
 - Columns: A placeholder for adding a field.
 - Metrics: A placeholder for adding a metric.

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.

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.

IIS 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

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](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

