

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](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.

[? 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

[Start Instance](#)

∞ / 1 spawns left

Search field names

Filter by type 0

Records

Available fields @timestamp

group.name administrators

Create custom label?

Cancel Save

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.

elastic

Dashboard Create

Search

event.code: 4625 + Add filter

windows*

user.

Filter by type 0

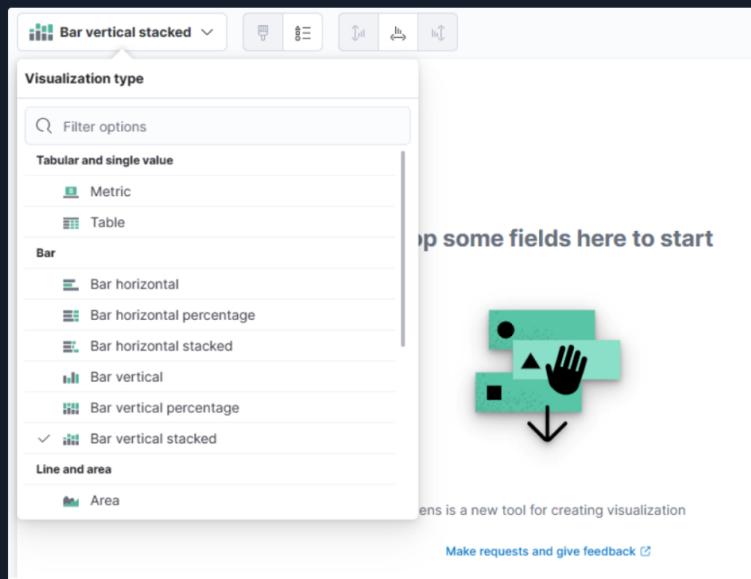
Available fields 4

- related.user.keyword
- user.domain.keyword
- user.id.keyword
- user.name.keyword

Empty fields 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.



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.

Rows

Select a function

Date histogram Intervals
Filters Top values

Select a field user.name.keyword

Number of values 1000

Rank by Count of records

Rank direction Descending

Advanced

Display name Top values of user.name.keyword

Text alignment Left Center Right

Hide column

This screenshot shows the 'Top values' configuration window. It includes fields for selecting a field ('user.name.keyword'), specifying the number of values (set to 1000), ranking by count of records, and displaying the results in descending order. The display name is set to 'Top values of user.name.keyword'. The 'Text alignment' section shows 'Left' selected. A 'Hide column' checkbox is also present.

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

Table

windows*

Rows ②

Top values of user.name.keyword X

+ Add or drag-and-drop a field

Columns ②

+ Add or drag-and-drop a field

Metrics

+ Add or drag-and-drop a field

Required dimension

This screenshot shows the 'Table' configuration window. It displays a single row named 'windows*'. Under the 'Rows' section, there is a list item 'Top values of user.name.keyword'. Below this, there is a placeholder for adding more fields. The 'Metrics' section is currently empty, indicated by a red-bordered placeholder 'Add or drag-and-drop a field'. The 'Required dimension' section is also empty.

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

Metrics

Quick functions **Formula**

Select a function

- Average
- Count**
- Counter rate
- Cumulative sum
- Differences
- Last value
- Maximum
- Median
- Minimum
- Moving average
- Percentile
- Sum
- Unique count

Select a field

Field

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)

Row	Value
1	Top values of user.name.keyword
2	Top values of winlog.event_data.MemberSid.keyword
3	Top values of group.name.keyword
4	Top values of event.action.keyword
5	Top values of host.name.keyword

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.

The screenshot shows the Elastic Stack interface with several visualizations:

- A table visualization titled "Failed logon attempts [Admin users only]" showing logins for administrator, amni, eAdministrator, and DC1.
- A table visualization titled "RDP login for service account" showing a single entry for SVC-sql1 connecting from 192.168.28.130.
- A table visualization titled "User added or removed from a local group" showing additions and removals for various users across different groups.

A context menu is open over the "User added or removed from a local group" visualization, with the "Edit panel title" option highlighted with a red box.

Failed logon attempts [Admin users only]

Username	Event logged by	Logon type	# of logins
Administrator	DC1	Interactive	3
administrator	PAW	Interactive	2
Administrator	DC1	Unlock	1
administrator	PAW	Unlock	1
administrator	DC2	Interactive	1

RDP login for service account

Username	Connect to	Connect from	# of logins
svc-sql1	PKI	192.168.28.130	2

< Options

- Customize time range
- Inspect
- Save to library
- Maximize panel
- Download as CSV
- Replace panel
- Copy to dashboard
- Delete from dashboard

Customize panel time range

Time range

Absolute Relative Now

Mar 5, 2023 @ 00:00:00.000 → now

Remove

Absolute Relative Now

← March ↓ 2023 →

Su	Mo	Tu	We	Th	Fr	Sa	00:00
26	27	28	1	2	3	4	00:00
5	6	7	8	9	10	11	01:00
12	13	14	15	16	17	18	02:00
19	20	21	22	23	24	25	03:00
26	27	28	29	30	31	1	04:00

Start date: Mar 5, 2023 @ 00:00:00.000

Action performed on Count of records

Action performed on	Count of records
WIN-FM93RIBQOKQ.eagle.lo...	1
OK9BH1BCKSD	1
eagle.local	1
WIN-FM93RIBQOKQ\$	1
WIN-238BP90DL2F\$	1
WIN-FM93RIBQOKQ\$	1

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](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

