

SIEM Visualization Example 1: Failed Logon Attempts (All Users)

[? Go to Questions](#)

Dashboards in SIEM solutions serve as containers for multiple visualizations, allowing us to organize and display data in a meaningful way.

In this and the following sections, we will create a dashboard and some visualizations from scratch.

Developing Our First Dashboard & Visualization

Navigate to the bottom of this section and click on [Click here to spawn the target system!](#)

Now, navigate to [http://\[Target IP\]:5601](http://[Target IP]:5601), click on the side navigation toggle, and click on "Dashboard".

Delete the existing "SOC-Alerts" dashboard as follows.

Title	Description	Tags	Actions
SOC-Alerts			

Rows per page: 20

When visiting the Dashboard page again we will be presented with a message indicating that no dashboards currently exist. Additionally, there will be an option available to create a new Dashboard and its first visualization. To initiate the creation of our first dashboard, we simply have to click on the "Create new dashboard" button.

Create your first dashboard

You can combine data views from any Kibana app into one dashboard and see everything in one place.

New to Kibana? [Install some sample data](#) to take a test drive.

[Create new dashboard](#)

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

[Create visualization](#)

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

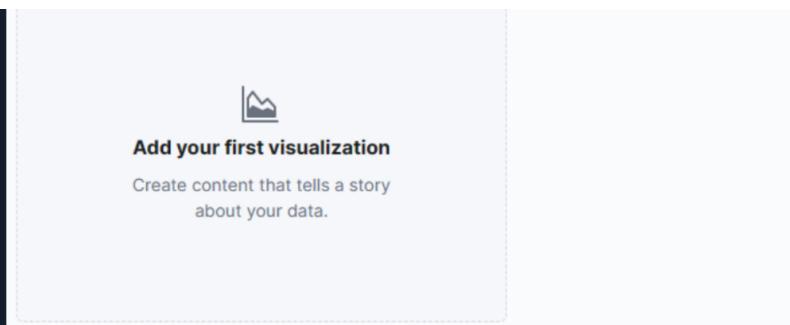
- [Skills Assessment](#)

My Workstation

OFFLINE

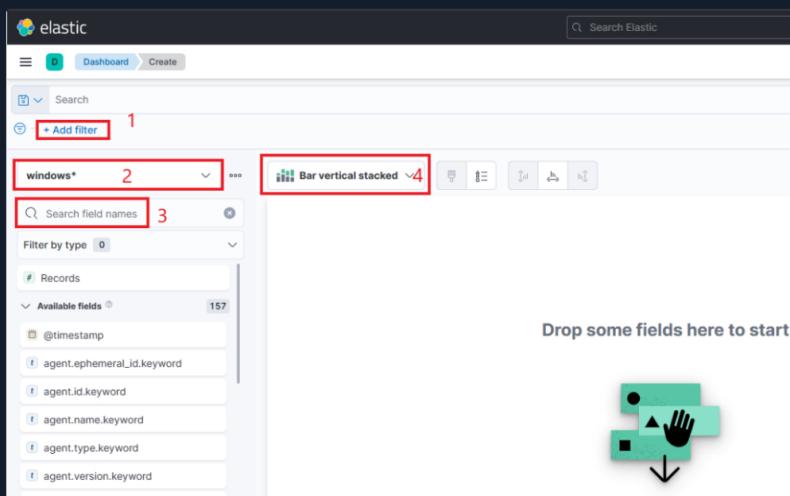
Start Instance

∞ / 1 spawns left



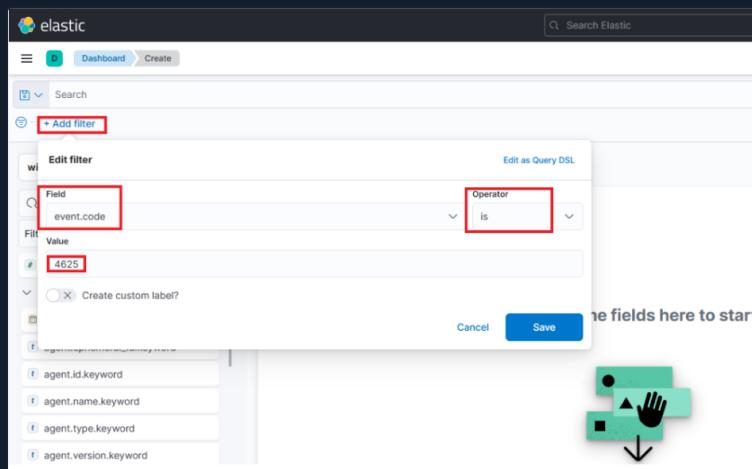
Upon initiating the creation of our first visualization, the following new window will appear with various options and settings.

Before proceeding with any configuration, it is important for us to first click on the calendar icon to open the time picker. Then, we need to specify the date range as "last 15 years". Finally, we can click on the "Apply" button to apply the specified date range to the data.



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. For example, if our goal is to display failed logon attempts, we can use a filter to only consider event IDs that match **4625 - Failed logon attempt on a Windows system**. The following image demonstrates how we can specify such a filter.

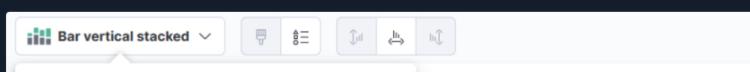


2. This field indicates the data set (index) that we are going to use. It is common for data from various infrastructure sources to be separated into different indices, such as network, Windows, Linux, etc. In this particular example, we will specify **windows*** in the "Index pattern".
3. This search 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. For example, let's say 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 Elastic Stack interface, specifically the search bar area. At the top, there is a search bar with a blue 'Search' button and a dropdown arrow. Below it is a filter bar with a magnifying glass icon and the text 'event.code: 4625 X'. To the right of the filter bar is a '+ Add filter' button. The main search input field contains the text 'user.' with a magnifying glass icon to its left. This entire search input field is highlighted with a red rectangular border. Below the search input, there is a 'Filter by type' section with a dropdown arrow showing '0' filters. Underneath this, there is a section titled 'Available fields' with a dropdown arrow showing '4' fields. The listed fields are: 'related.user.keyword', 'user.domain.keyword', 'user.id.keyword', and 'user.name.keyword'. The 'user.name.keyword' field is underlined with a red line, matching the color of the search input's border. At the bottom, there are two more sections: 'Empty fields' with a count of '15' and 'Meta fields' with a count of '0'.

"Why `user.name.keyword` and not `user.name`?," you may ask. We should use the `.keyword` field when it comes to aggregations. Please refer to this [stackoverflow question](#) for a more elaborate answer.

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.



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 ⓘ

+ Add or drag-and-drop a field

Columns ⓘ

+ Add or drag-and-drop a field

Metrics

+ Add or drag-and-drop a field

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

Rows

Select a function

Date histogram

Filters

Intervals

Top values

Select a field

user.name.keyword

Number of values

1000

Rank by <small>②</small>	Count of records	▼
Rank direction	Descending	▼
> Advanced		
Display name	Top values of user.name.keyword	
Text alignment	Left	Center
Hide column	<input type="checkbox"/>	

Note: You will notice **Rank by Alphabetical** and not **Rank by Count of records** like in the screenshot above.

This is OK. By the time you perform the next configuration below, **Count of records** will become available.

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

Table	
windows*	
Rows <small>②</small>	
Top values of user.name.keyword ×	
+ Add or drag-and-drop a field	
Columns <small>②</small>	
+ Add or drag-and-drop a field	
Metrics	
+ Add or drag-and-drop a field	
Required dimension	

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

Metrics	×
Quick functions	Formula
Select a function	
Average	Median
Count	Minimum
Counter rate	Moving average

The screenshot shows the Kibana Metrics panel. On the left, there's a sidebar with metrics like 'Cumulative sum', 'Differences', 'Last value', and 'Maximum'. The main area is titled 'Select a field' with a dropdown menu labeled 'Field'. A modal window titled 'Metrics' is open, showing various functions: Average, Count (which is highlighted with a red box), Counter rate, Cumulative sum, Differences, Last value, Maximum, Median, Minimum, Moving average, Percentile, Sum, and Unique count. Below this, there's a 'Select a field' dropdown set to 'Records', a 'Display name' input field containing 'Count of records', and other settings like 'Value format' (Default), 'Text alignment' (Right), and 'Color by value' (None). At the bottom right of the modal is a 'Close' button.

As soon as we select "Count" as the metric, we will observe that the table gets populated with data (assuming that there are events present in the selected data set)

The screenshot shows a Kibana Table visualization titled 'Top values of user.name.keyword'. The table has three columns: 'Top values of user.name.keyword' (containing values like DC1\$, EAGLE.LOCAL\ESCAACCS, Administrator, DESKTOP-DPOE3ND, PAW, WIN-OK9BH1BCKSD, etc.), 'Top values of host.hostname.keyword' (containing values like DC1, DC2, PK1, DC1, DC1, DC2, DC1, DC1, DC2, etc.), and 'Count of records' (containing values like 10, 2, 12, 4, 4, 4, 4, 4, 2, 1, 1). Below the table, there's a 'Suggestions' section with icons for 'Current visualization', a donut chart, a bar chart, and a summary of 84. The overall interface is dark-themed.

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.

The screenshot shows the same Kibana Table visualization as before, but now it includes a 'Rows' section at the bottom. The 'Rows' section contains a table with two columns: 'Top values of user.name.keyword' (DC1\$, DC1\$, EAGLE.LOCAL\ESCAACCS, etc.) and 'Top values of host.hostname.keyword' (DC1, DC2, PK1, DC1, DC1, DC2, etc.). The 'Count of records' column from the main table is still present in the rows table. The overall interface is dark-themed.

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

1. The username of the individuals logging in (Note: It currently displays both users and computers. Ideally, a filter should be implemented to exclude computer devices and only display users).
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, appearing as shown in the following image.

The screenshot shows the Kibana dashboard interface. At the top, there's a header with the Elastic logo, a search bar, and navigation links for 'Dashboard', 'Editing New Dashboard', 'Unsaved changes', 'Options', 'Share', and 'Save'. Below the header are filters for 'Search', 'KQL', 'Last 1 year', 'Show dates', and 'Refresh'. There are also buttons for 'Create visualization', 'Add filter', 'All types', and 'Add from library'. The main area shows a table visualization titled '[No Title]' with three columns: 'Top values of user.name.keyword', 'Top values of host.hostname.keyword', and 'Count of records'. The data in the table matches the structure described in the previous steps. The overall interface is dark-themed.

EAGLE.LOCAL/ES...	PKI	12
Administrator	DC1	4
DESKTOP-DPOES...	DC1	4
PAW	DC2	4
WIN-OK9BH1BCK...	DC1	4
WIN-RMMGJA7T...	DC1	4
administrator	PAW	3
administrator	DC2	1

Let's not forget to save the dashboard as well. We can do so by simply clicking on the "Save" button.

The screenshot shows the Elasticsearch interface with a 'Save dashboard' dialog box overlaid. The dialog contains fields for 'Title' (set to 'SOC-Alerts'), 'Description' (containing a note about the dashboard being for HTB Academy's SOC Analyst Job-Role Path.), and 'Tags'. A checkbox labeled 'Store time with dashboard' is checked. At the bottom of the dialog are 'Cancel' and 'Save' buttons, with the 'Save' button highlighted by a red box.

Refining The Visualization

Suppose the SOC Manager suggested the following refinements:

- Clearer column names should be specified in the visualization
- The Logon Type should be included in the visualization
- The results in the visualization should be sorted
- The DESKTOP-DPOESND, WIN-OK9BH1BCKSD, and WIN-RMMGJA7T9TC usernames should not be monitored
- Computer accounts should not be monitored (not a good practice)

Let's refine the visualization we created, so that it fulfills the suggestions above.

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

The dashboard we previously created should be visible. Let's click on the "pencil"/edit icon.

The screenshot shows the 'Dashboards' page in the Elasticsearch interface. It lists a single dashboard titled 'SOC-Alerts'. To the right of the dashboard title is an 'Edit' icon, which is highlighted by a red box.

Let's now click on the "gear" button at the upper-right corner of our visualization, and then click on "Edit lens".

The screenshot shows the 'Editing SOC-Alerts' dashboard. In the bottom-left corner of the visualization area, there is a small gear icon. A red box highlights the 'Edit lens' option in the dropdown menu that appears when this icon is clicked.

"Top values of user.name.keyword" should be changed as follows.

Table

windows*

Rows 

[Top values of user.name.keyword](#) 

[Top values of host.hostname.keyword](#) 

 Add or drag-and-drop a field

Columns 

 Add or drag-and-drop a field

Metrics

[Count of records](#) 

 Add or drag-and-drop a field

Rows 

Select a function

Date histogram  Intervals

[Filters](#) [Top values](#)

Select a field

user.name.keyword

Number of values

1000

Rank by ?

Alphabetical

Rank direction

Ascending

> Advanced

Display name

Username

Text alignment

Left

Center

Right

Hide column



"Top values of host.hostname.keyword" should be changed as follows.

Rows



Select a function

Date histogram

Intervals

Filters

Top values

Select a field

host.hostname.keyword

Number of values

1000

Rank by ?

Count of records

Rank direction

Descending

> Advanced

Display name

Event logged by

Text alignment

Left

Center

Right

Hide column



The "Logon Type" can be added as follows (we will use the `winLog.Logon.type.keyword` field).

Table

windows*



Rows ?

Top values of user.name.
keyword



Event logged by



+ Add or drag-and-drop a field

Columns ?

+ Add or drag-and-drop a field

Metrics

Count of records



+ Add or drag-and-drop a field

Rows

X

Select a function

Date histogram

Intervals

Filters

Top values

Select a field

winlog.logon.type.keyword

Number of values

1000

Rank by ?

Count of records

Rank direction

Descending

> Advanced

Display name

Logon Type

Text alignment

Left

Cent...

Right

Hide column



"Count of records" should be changed as follows.

Metrics

X

Quick functions

Formula

Select a function

Average

Median

Count

Minimum

Counter rate

Moving average

Cumulative sum

Percentile

Differences

Sum

Last value Unique count

Maximum

Select a field

Records ▼

Add advanced options ▼

Display name # of logins

Value format Default ▼

Text alignment Left Cent... Right

Hide column

Summary Row None ▼

Color by value None Cell Text

We can introduce result sorting as follows.

Username	Event logged by	Logon Type	# of logins
DC1\$	DC1	Network	88
DC1\$	DC2	Network	26
DC1\$	PAW	Network	19,913
DC1\$	WS001	Network	2,983
DC2\$	DC1	Network	10
DC2\$	PKI	Network	4
SYSTEM	DC1	Service	2,138
SYSTEM	WS001	Service	1,651
SYSTEM	PAW	Service	859
SYSTEM	PKI	Service	874
SYSTEM	DC2	Service	1,079
WS001\$	WS001	Network	209
WS001\$	PAW	Network	1,079

All we have to do now is click on "Save and return".

The DESKTOP-DPOESND, WIN-OK9BH1BCKSD, and WIN-RMMGJA7T9TC usernames can be excluded by specifying additional filters as follows.

The screenshot shows the Kibana interface with a search bar at the top containing 'event.code: 4625 x + Add filter'. Below the search bar is a 'Create visualization' button and an 'Edit filter' dialog. The 'Edit filter' dialog has a 'Field' dropdown set to 'user.name.keyword', an 'Operator' dropdown set to 'is not', and a 'Value' dropdown set to 'DESKTOP-DPOESND'. There is also a 'Create custom label?' checkbox. At the bottom of the dialog are 'Cancel' and 'Save' buttons. Below the dialog is a table visualization showing logon attempts with columns: Username, Event logged by, Logon Type, and # of logins. The table includes rows for various users like DC1\$, PAW, and Administrator.

Computer accounts can be excluded by specifying the following the KQL query and clicking on the "Update" button.

The screenshot shows a visualization titled 'SIEM Visualization Example 1: Failed Logon Attempts (All Users)'. The query is 'NOT user.name: *\$ AND winlog.channel.keyword: Security'. At the top right of the visualization area is a 'Update' button, which is highlighted with a red box.

The **AND winlog.channel.keyword: Security** part is to ensure that no unrelated logs are accounted for.

The screenshot shows the 'Edit filter' dialog with several filters applied: 'NOT user.name: *\$ AND winlog.channel.keyword: Security', 'event.code: 4625', 'NOT user.name.keyword: DESKTOP-DPOESND', 'NOT user.name.keyword: WIN-OK9BH1BCKSD', and 'NOT user.name.keyword: WIN-RMMGJAJ7T9TC'. At the top right of the dialog is a 'Update' button, which is highlighted with a red box.

This is our visualization after all the refinements we performed.

The screenshot shows the refined visualization. The table now only shows logon attempts for PAW, Administrator, and bob. The columns are: Username, Event logged by, Logon Type, and # of logins. The table includes rows for PAW (DC2, Network, 4), Administrator (DC1, Interactive, 3), administrator (PAW, Interactive, 2), bob (WS001, Interactive, 2), sql-svc1 (PKI, Network, 1), Administrator (DC1, Unlock, 1), administrator (PAW, Unlock, 1), administrator (DC2, Interactive, 1), anni (WS001, Interactive, 1), administrator (DC1, Network, 1), and eagleAdministrator (DC1, Network, 1).

Finally, let's give our visualization a title by clicking on "No Title".

The screenshot shows the 'Customize panel' dialog open over the visualization. The dialog has a 'Title' input field containing '(No Title)'. The visualization below it shows the same refined data as the previous screenshot.

		Network
sql-svc1	PK1	Network
Administrator	DC1	Unlock
administrator	PAM	Unlock
administrator	DC2	Interactive
anni	WS001	Interactive
eAdministrator	DC1	Network
eagleAdministrator	DC1	Network

Show panel title

Panel title

Reset

Cancel Save

Don't forget to click on the "Save" button (the one on the upper-right hand side of the window).

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.

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

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](http://[Target IP]:5601), click on the side navigation toggle, and click on "Dashboard".

Browse the refined visualization we created or the "Failed logon attempts [All users]" visualization, if it is available, and enter the number of logins for the sql-svc1 account as your answer.

 Submit

◀ Previous

Next ▶

 Mark Complete & Next

Powered by 

