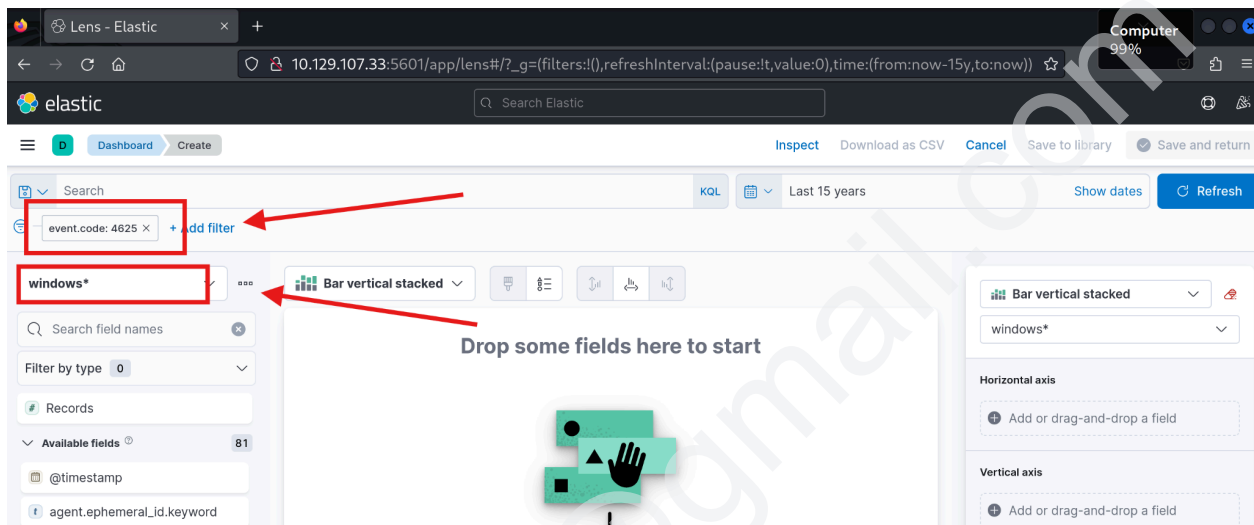


# Elastic Stack As a SIEM Solution

## 1.Failed Logon Attempts (All Users)

### 1. Developing a New Dashboard & Visualization

1.1 Create a filter to display only failed login attempts (Event ID 4625 – failed logins on Windows systems | **event.code 4625**) from Windows-related logs (matching **windows\***).



### 1.2 Select the Visualization type as “Table”

And Create Table Rows,

Row 1 - **user.name.keyword** renamed as **Username**

Row 2 - **host.name.keyword** renamed as **Event logged by**

Row 3 - **winlog.logon.type.keyword** renamed as **logon type**

Row 4 - **Metrics** renamed as **No.logins**

It shows **which user** logged in, **which host** generated the event, the **type of logon** (like interactive or remote), and the **number of times** each type of login occurred.

The top screenshot shows the Elastic Lens interface with a search filter 'event.code: 4625'. The visualization type is set to 'Table'. The configuration panel on the right shows the 'Rows' section with 'user.name.keyword' selected, 'Number of values' set to 1000, 'Rank by' set to 'Alphabetical', and 'Rank direction' set to 'Descending'. The 'Display name' is set to 'Username'.

The bottom screenshot shows the resulting table of data. The columns are 'Username', 'Event logged by', 'logon type', and 'No.logins'. The data rows are as follows:

Username	Event logged by	logon type	No.logins
DC1\$	DC1	Network	10
DC1\$	DC2	Network	2
EAGLE.LOCAL/ESCAC...	PKI	Network	12
Administrator	DC1	Interactive	3
Administrator	DC1	Unlock	1
DESKTOP-DPOESND	DC1	Network	4
PAW	DC2	Network	4
WIN-OK9BH1BCKSD	DC1	Network	4
WIN-RMMGJA7T9TC	DC1	Network	4
administrator	PAW	Interactive	2

The configuration panel on the right shows the 'Rows' section with 'Username' selected, 'Event logged by' selected, and 'logon type' selected. The 'Columns' section shows 'No.logins' selected.

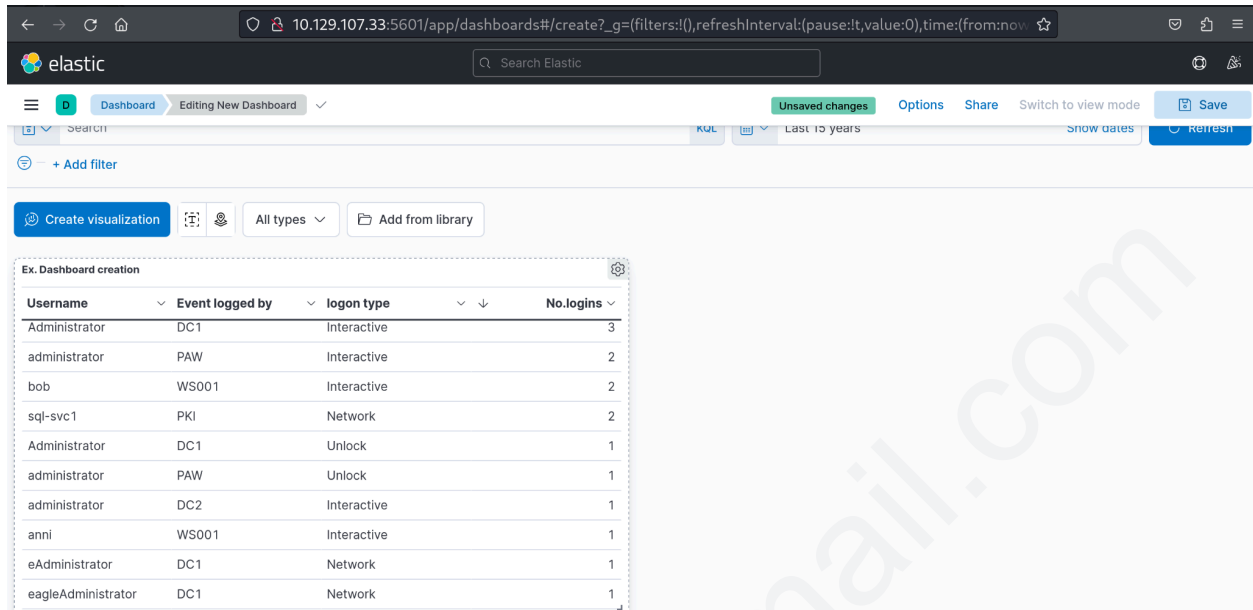
1.3 Add a filter to exclude username DESKTOP-DPOESND.(WIN-OK9BH1BCKSD, and WIN-RMMGJA7T9TC also excluded later)

1.4 This filter excludes events without a username and ensures only security-related logon events are shown, making the data more relevant and focused.

NOT user.name: \*\$ AND winlog.channel.keyword: Security

Username	Event logged by	logon type	No.logins
PAW	DC2	Network	4
Administrator	DC1	Interactive	3
administrator	PAW	Interactive	2
bob	WS001	Interactive	2
sql-svc1	PKI	Network	2
Administrator	DC1	Unlock	1
administrator	PAW	Unlock	1
administrator	DC2	Interactive	1
anni	WS001	Interactive	1
eAdministrator	DC1	Network	1

1.5 Finally, This dashboard displays filtered Windows security logon events to highlight valid user login attempts, showing who logged in, from where, how, and how often—helping detect unusual or failed login patterns.



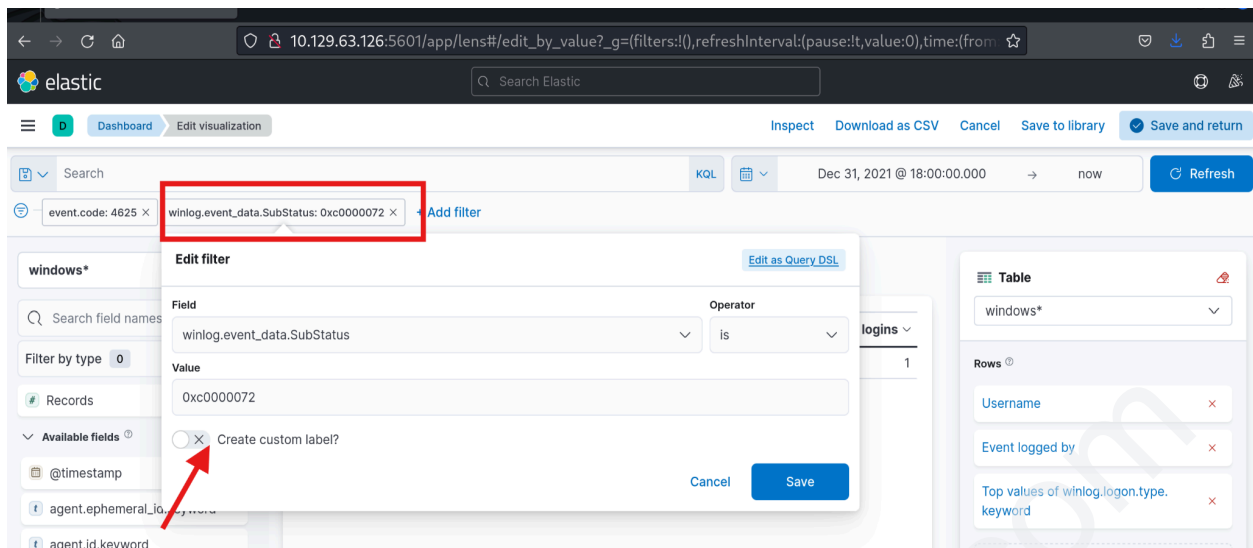
The screenshot shows the Elastic dashboard interface. At the top, there's a search bar and navigation tabs. Below the dashboard title, there's a table titled "Ex. Dashboard creation" with the following data:

Username	Event logged by	logon type	No.logins
Administrator	DC1	Interactive	3
administrator	PAW	Interactive	2
bob	WS001	Interactive	2
sql-svc1	PKI	Network	2
Administrator	DC1	Unlock	1
administrator	PAW	Unlock	1
administrator	DC2	Interactive	1
anni	WS001	Interactive	1
eAdministrator	DC1	Network	1
eagleAdministrator	DC1	Network	1

## 2. Failed Logon Attempts (Disabled Users)

2.1. Modify the dashboard to visualize Failed logon attempts on Disabled Users .

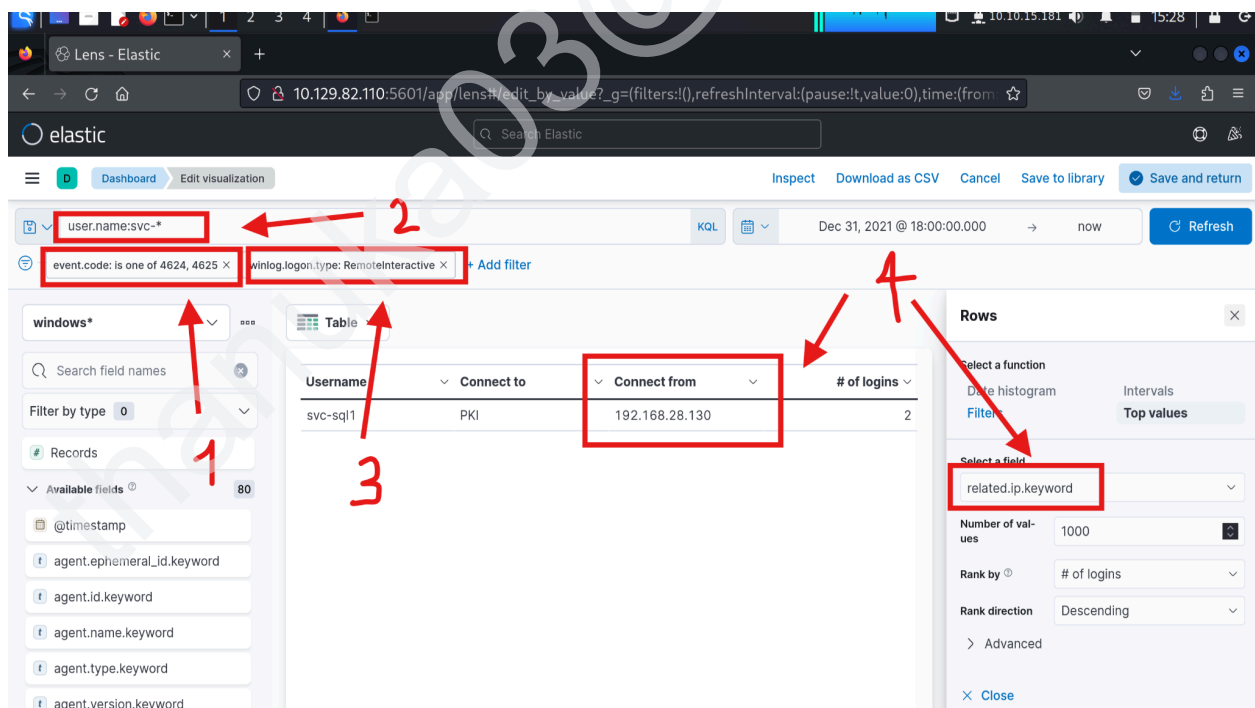
\*\* when set to 0xC0000072, that the failure is due to a logon with disabled user.



### 3. Successful RDP logon related to the Service Accounts

3.1. Creating a visualization to monitor successful **RDP logons** specifically related to **service accounts** (Service accounts are start with svc- )

- 1) **event.code: 4624** - Account was successfully logon
- 2) **user.name:svc-** - To filter service account logons only
- 3) **winlog.logon.type:RemoteInteractive** - To filter only Remote logons
- 4) **related.ip.keyword** - IP address of the service account



### 4. User Added or Removed from a Local group (Within a specific Timeframe)

#### 4.1 Creating a visualization to monitor user addition or removal from the local “Administrator” group from 5th 2023

The screenshot shows the Elastic Lens interface with a search query: `event.code: is one of 4732, 4733` and `group.name: administrators`. The table visualization displays the following data:

User perform	User added	Group modified	Action performed	Action performed on	Count of records
Administrator	S-1-5-21-15...	Administrators	added-memb...	PAW	1
Administrator	S-1-5-21-15...	Administrators	added-memb...	WIN-OK9BH1...	1
Administrator	S-1-5-21-15...	Administrators	removed-memb...	PAW.eagle.local	1
Administrator	S-1-5-21-15...	Administrators	added-memb...	PKI.eagle.local	1
ANONYMOUS	S-1-5-21-15...	Administrators	added-memb...	WIN-FM93RI...	1
WIN-238BP9...	S-1-5-21-42...	Administrators	added-memb...	WIN-238BP9...	1
WIN-FM93RI...	S-1-5-21-15...	Administrators	added-memb...	WIN-FM93RI...	1
admin	S-1-5-21-15...	Administrators	added-memb...	WIN-RMMGJ...	1
root	S-1-5-21-15...	Administrators	added-memb...	DC2	1

- 7) **4732** - member is added to a security enabled local group  
**4733** - member is removed from a security enabled local group
- 6) **group.name:administrators** - display user additions or removal from the local “Administrator” group
- 1) **user.name.keyword** - who did
- 2) **winlog.event\_data.MemberSid.keyword** - which user was added to or removed
- 3) **group.name.keyword** - in which group does this happens ?
- 4) **event.action.keyword** - was the user added to or removed from the group
- 5) **host.name.keyword** - which machine did the action occur?

#### 4.2 Customizing the Timeframe from 5th March 2023 to Now

The screenshot shows the Elastic Lens interface with a search query: `event.code: is one of 4732, 4733` and `group.name: administrators`. The table visualization displays the same data as in the previous screenshot. The timeframe is set to **Mar 5, 2023 @ 18:00:00.000** to **now**.