PROJECT

Multi-tenant cybersecurity operations centre designed
as an open cloud service with machine learning elements

Dashboards – demonstration of creating visualizations in Kibana

Linked to work package KPB2 – Design of the SOCaaS service

Linked to output
V6 – Description of dashboards, the monitoring and reporting system

Funded by the European Union
NextGenerationEU

RECOVERY AND RESILIENCE PLAN

GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

Contents

List of figures 3
Creating Kibana dashboards 4
Index pattern 4
Visualizations 4
Filters 9
Dashboard 9
Description of visualizations 10
Adding a visualization description 11
Changing the chart type 12
List of filters used 15

List of figures

Figure 1 - Kibana - index pattern 4
Figure 2 - Kibana menu - visualize 5
Figure 3 - Kibana - list of visualizations 6
Figure 4 - Kibana - choice of visualization 7
Figure 5 - Kibana - choice of chart 8
Figure 6 - Kibana - creating a bar chart 9
Figure 7 - Kibana - dashboard example 10
Figure 8 - Kibana - adding a visualization description 11
Figure 9 - Kibana - displaying the description in the dashboard 12
Figure 10 - Kibana - Changing the chart type 13
Figure 11 - Kibana - Chart after the change 14

Creating Kibana dashboards

In this part of the document, we present a demonstration of the procedure for creating the visualizations and dashboards we worked on.

Index pattern (Engl. index pattern)

First, in the section Management/Stack management/Index pattern, we needed to create a so-called index pattern from the available indices. A pattern created in this way serves to determine the indices that will be visualized. All indices that match the specified form (in this case “sessions2*”) will be included in the visualizations and dashboards being created.

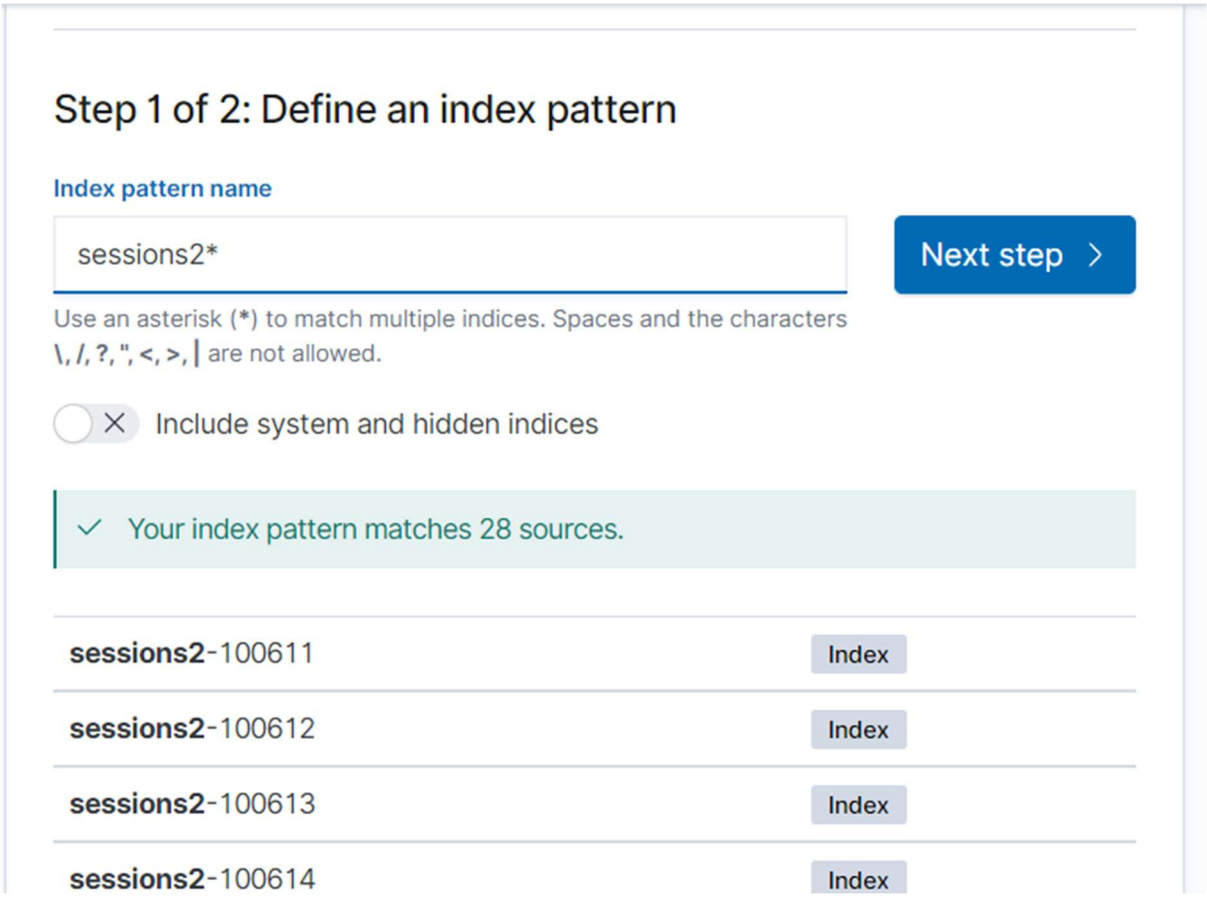


Figure 1 - Kibana - index pattern

Visualizations

Visualizations are among the main elements of dashboards. They are a graphical representation of selected data, mostly in the form of charts. They can be created in

several ways, of which we will demonstrate one in this document. In the Kibana menu, we select Visualize under the category Analytics.

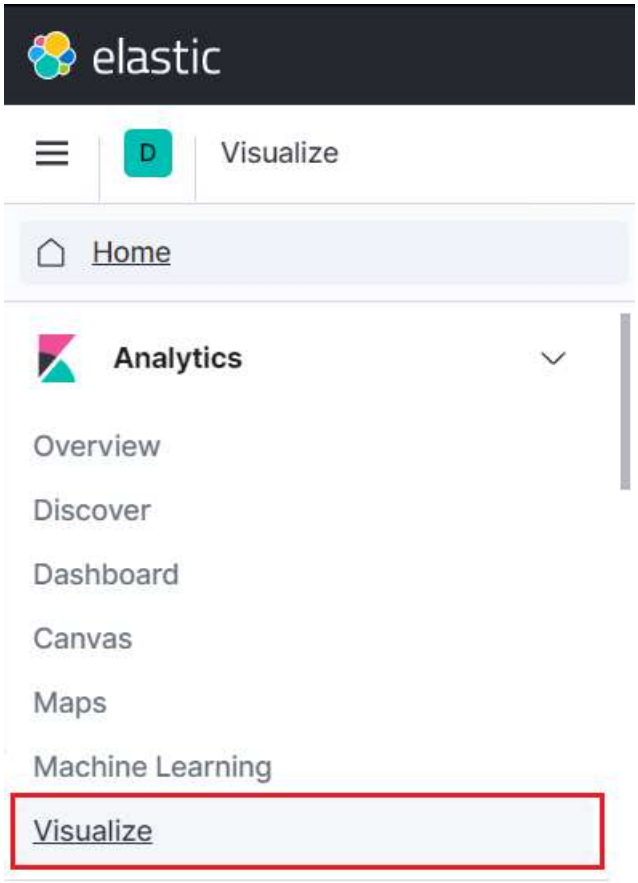


Figure 2 - Kibana menu - visualize

We get to the list of already created visualizations, where we create a new visualization by clicking the blue button.

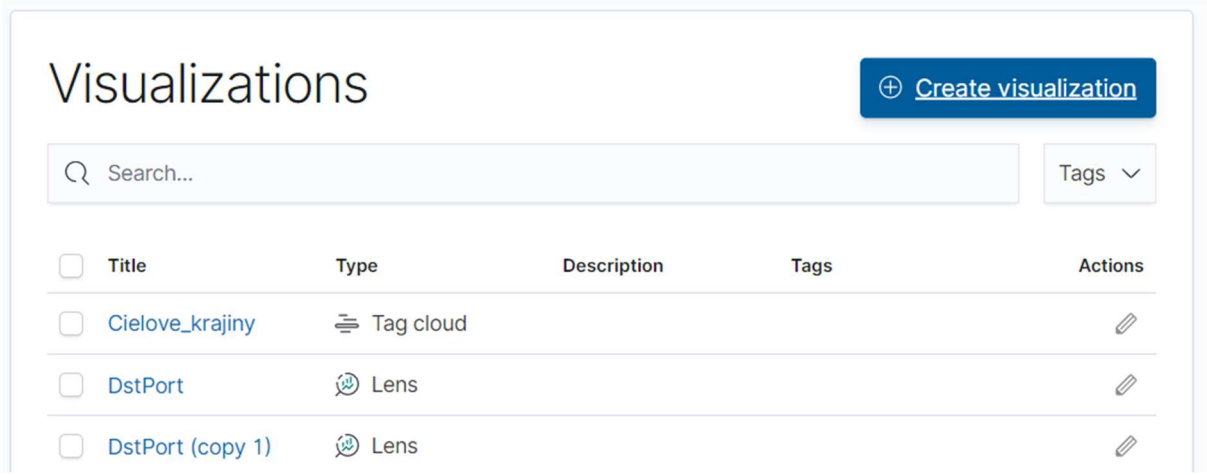


Figure 3 - Kibana - list of visualizations

Next, we choose from the options that are available to us. The most frequently used option was “Agregation based”, where we then selected the required chart type.

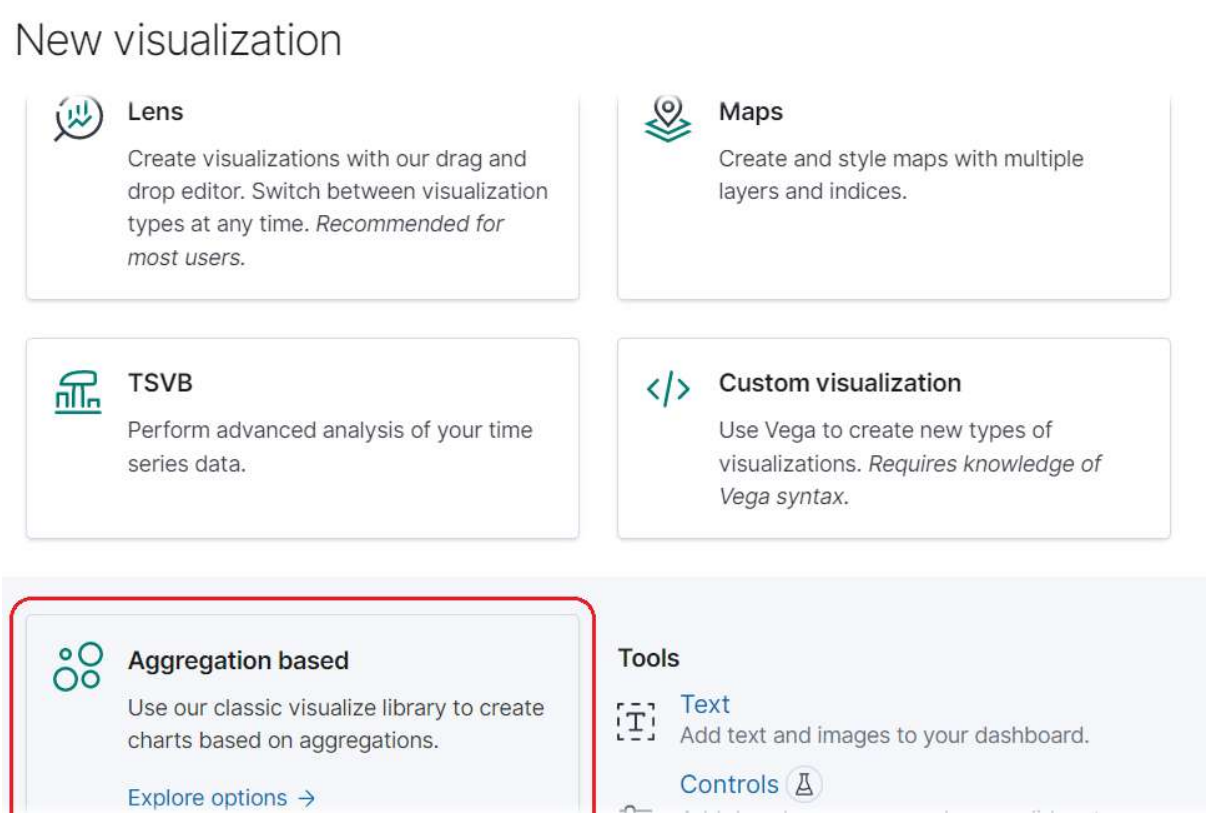


Figure 4 - Kibana - choice of visualization

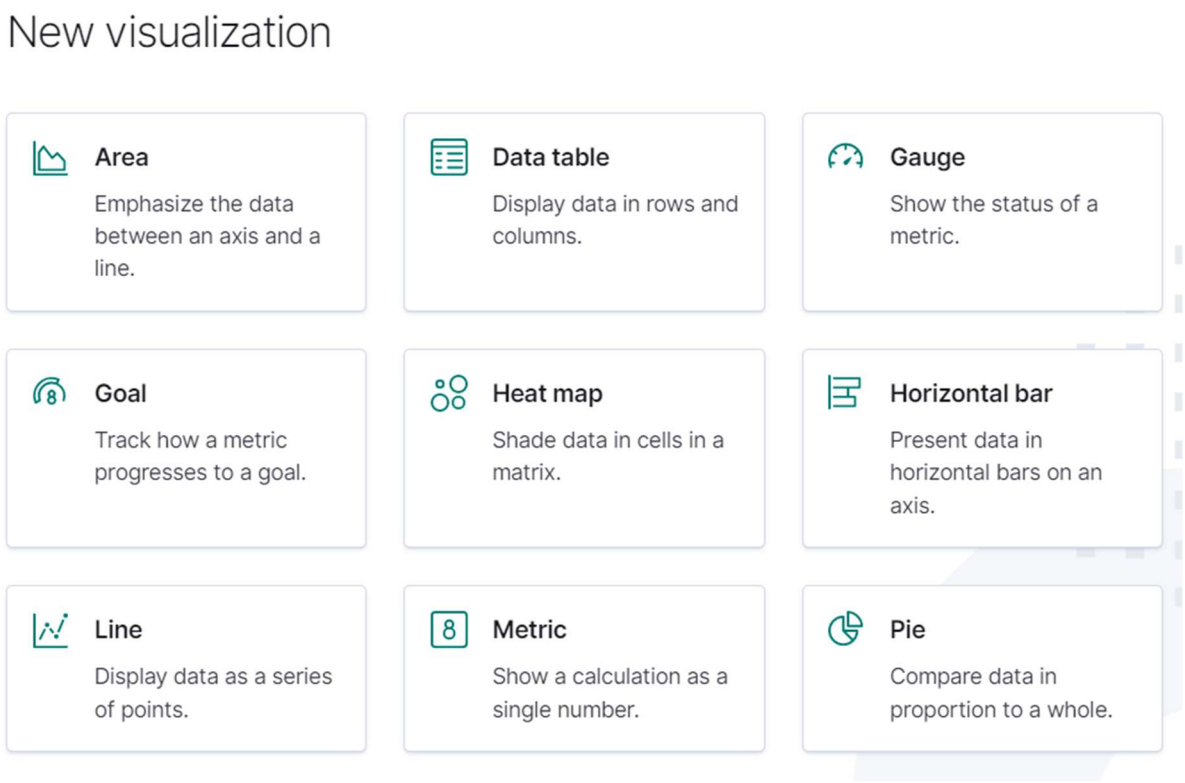


Figure 5 - Kibana - choice of chart

After these choices, we proceed to the creation of a specific chart by defining the axes, metrics or other parameters offered by the Kibana tool. It then depends on what we want to display with the given visualization. In the figure below, we can see the environment for creating a bar chart.

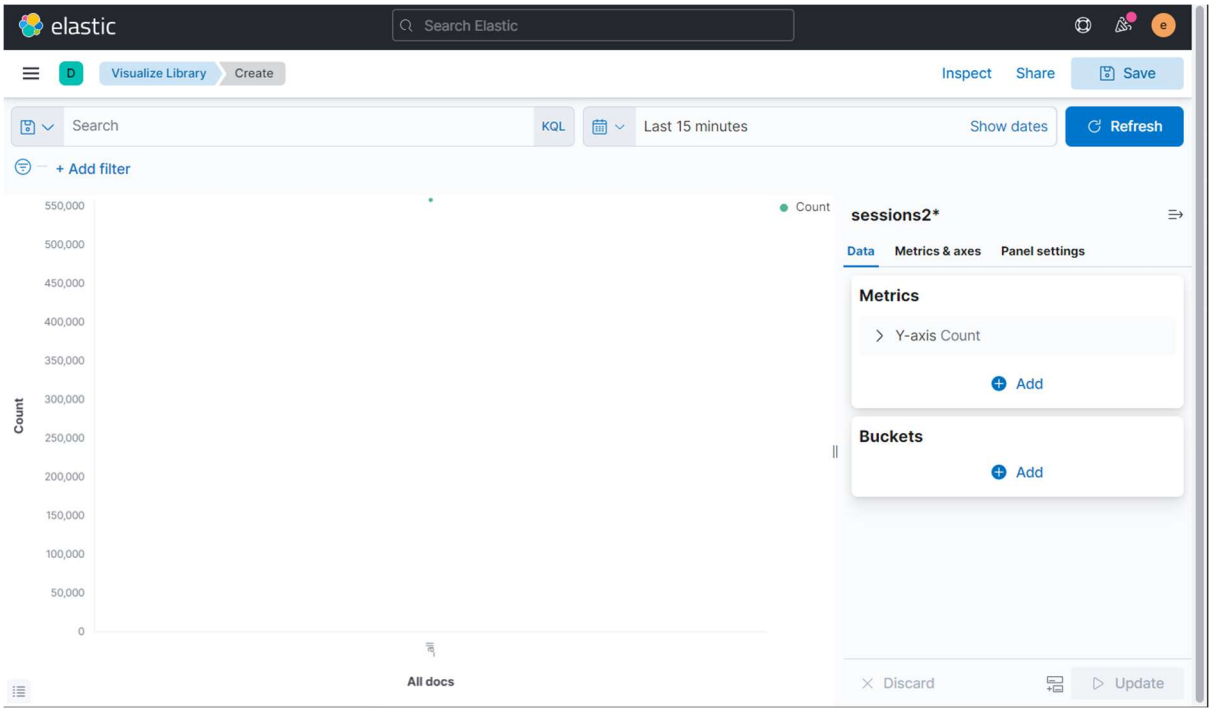


Figure 6 - Kibana - creating a bar chart

Filters

Visualizations generally use filters that specify more precisely which part of the records they should focus on. Whether it concerns specific IP addresses, ports or protocols, in our case we used the filters that are listed at the end of this document.

Example: dstIp : "<IPaddress>" or dstIp : "<IPaddress>" "

Dashboard

Creating the dashboard itself consists of inserting visualizations into a designated space. We can insert these visualizations in any order, move them or resize them exactly according to our needs. In this way, we can assemble all the necessary visualizations in one place and thus make our work easier. The final appearance of the

dashboards depends on the preferences of the analyst, or on the requirements of the centre, or rather of the organization.

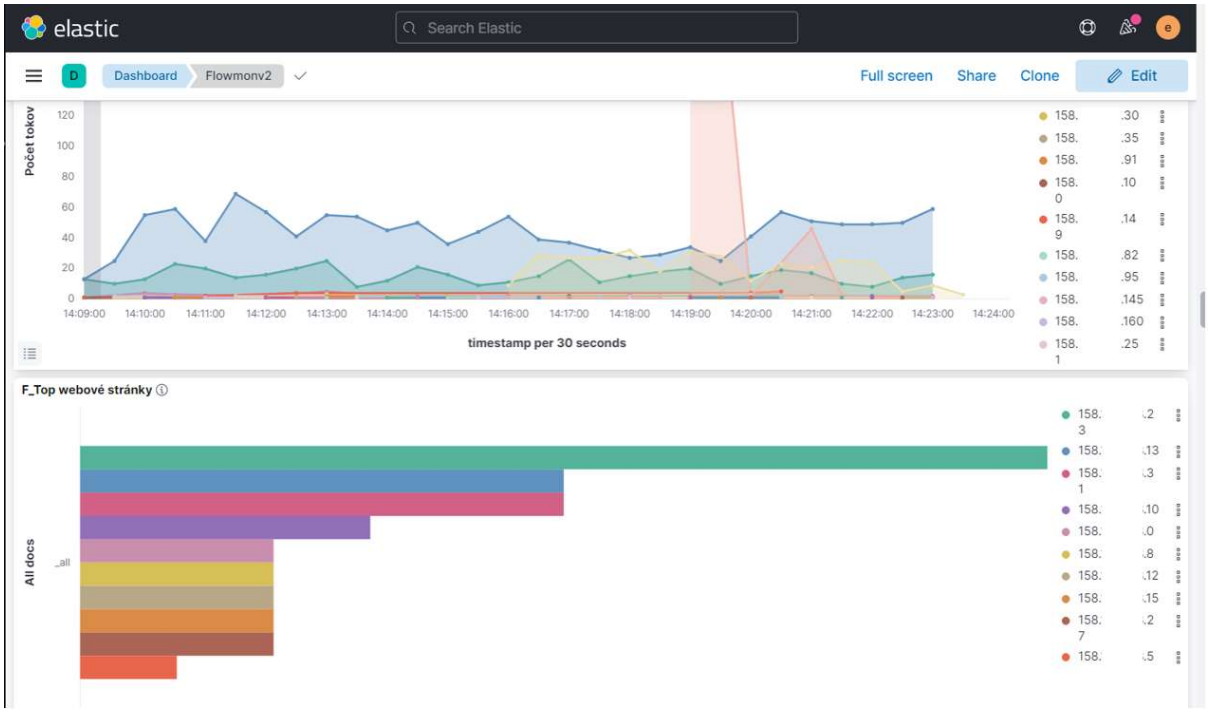


Figure 7 - Kibana - dashboard example

Description of visualizations

It serves mainly for a better understanding of a particular visualization, because sometimes it is not clear at first glance what the given visualization is trying to express. Especially when a person is looking at the dashboards for the first time. The way to add these descriptions is shown in the figure below. The description is added directly when creating the visualization, or rather when saving it. Likewise, if the visualization has already been created, after opening it we have the option to click the “Save” button even without making any changes and insert the description into the appropriate section.

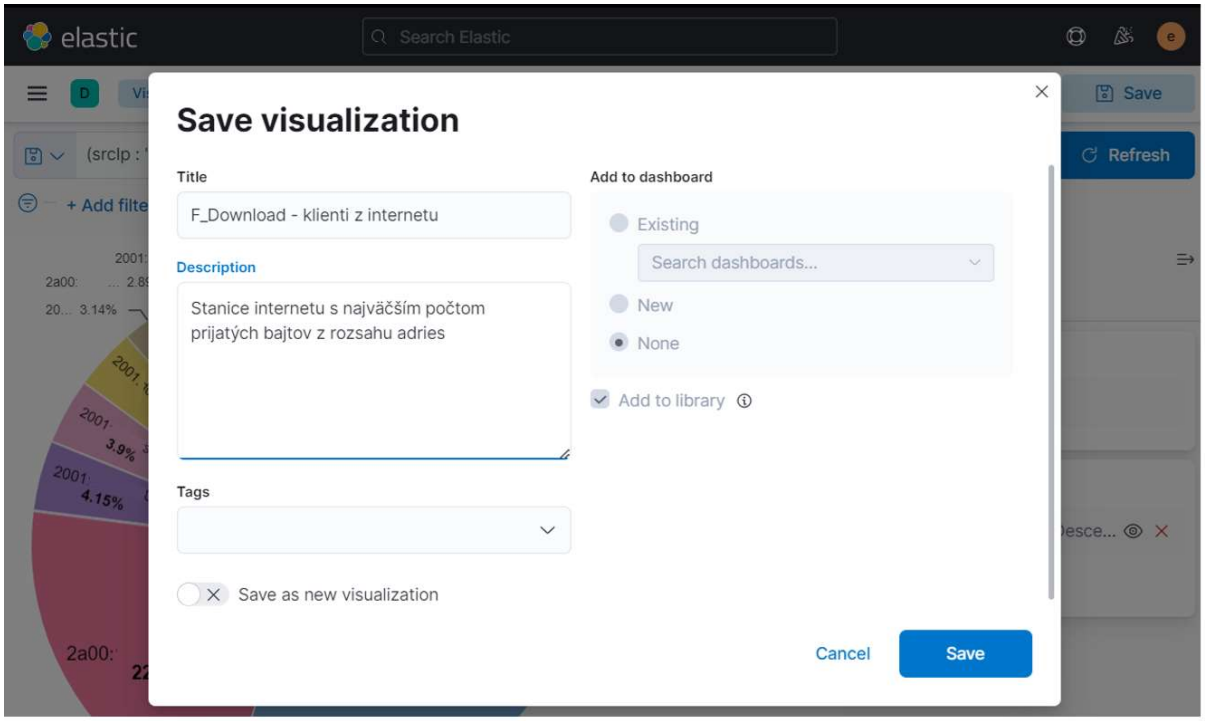


Figure 8 - Kibana - adding a visualization description

Adding a visualization description

The description is displayed directly in the list of created visualizations. However, it is equally visible directly in the dashboards, where next to the visualization name we can see a small "?" icon; when we hover over it with the mouse, the description is displayed in a pop-up bubble, which we can see in the figure below.

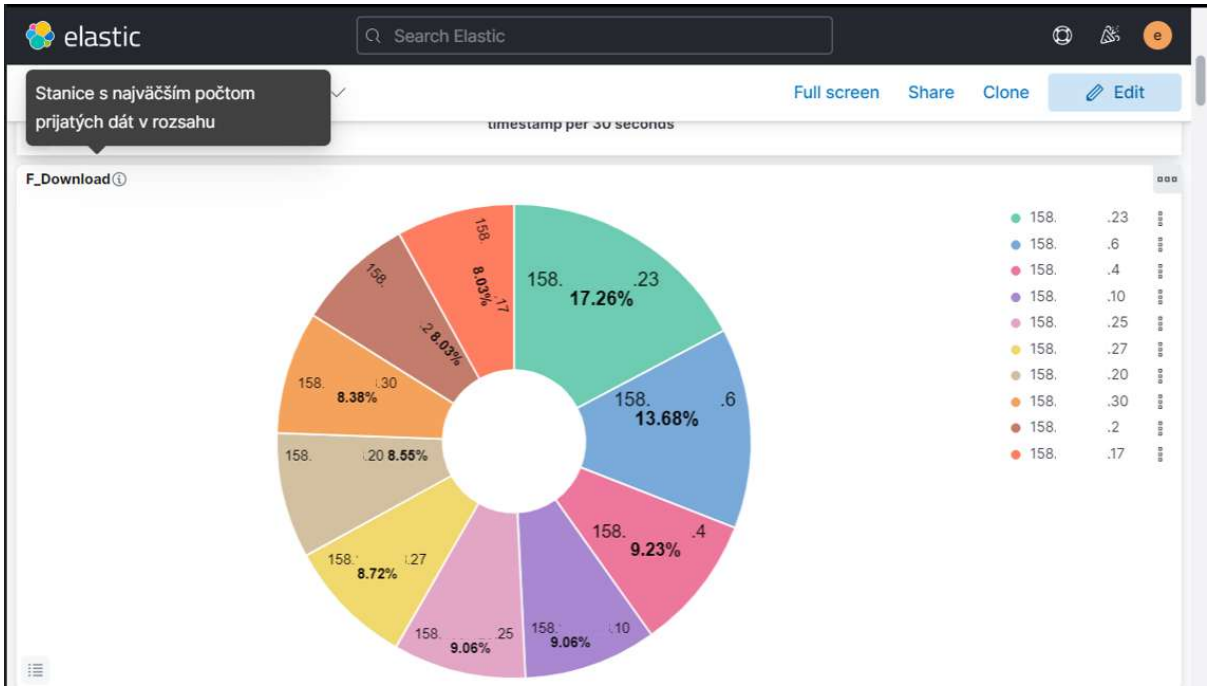


Figure 9 - Kibana - displaying the description in the dashboard

Changing the chart type

In the usual creation of a chart, as described above, a problem arises when changing the chart type. As regards changing bar charts, a change to a line or area chart is possible. We can make this change on the “Matrics & axes” tab and switch “chart type” to the required type. The course of the change and its result can be seen on the following page.

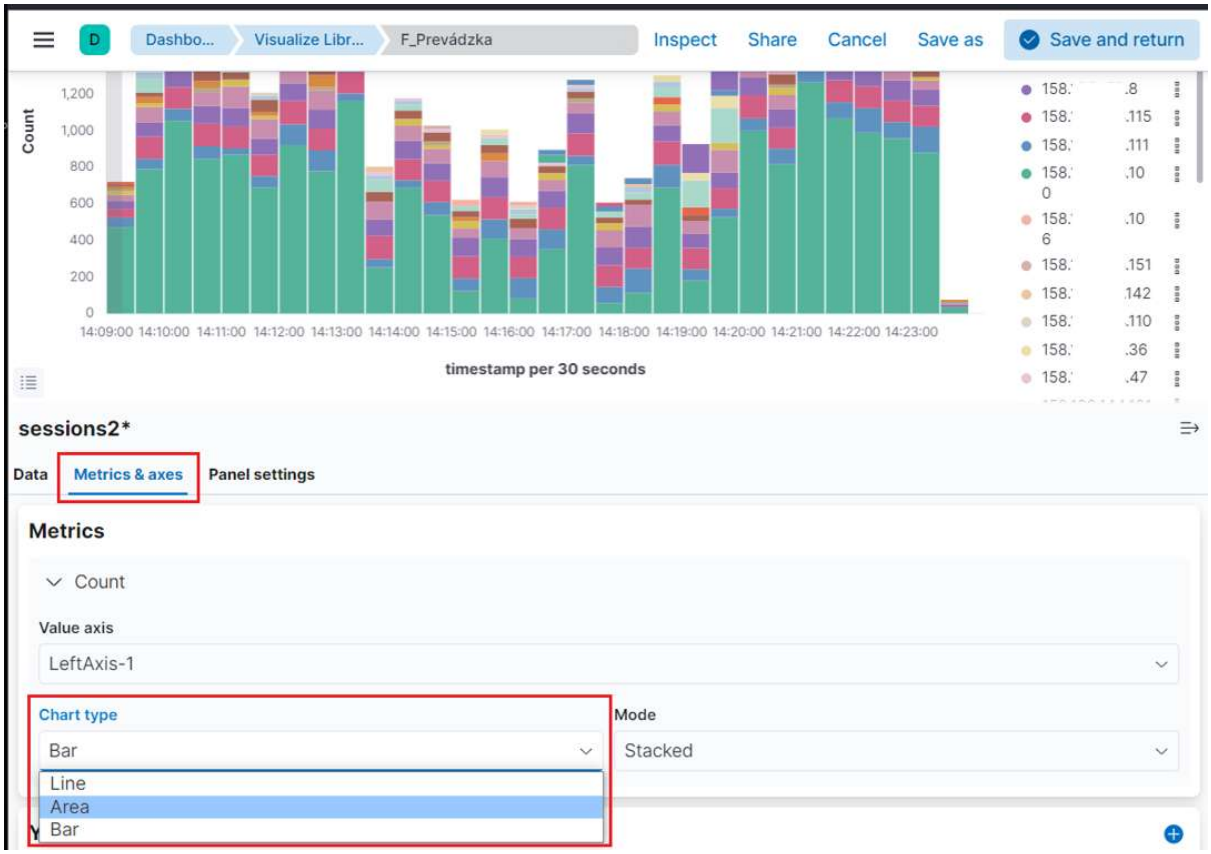


Figure 10 - Kibana - Changing the chart type

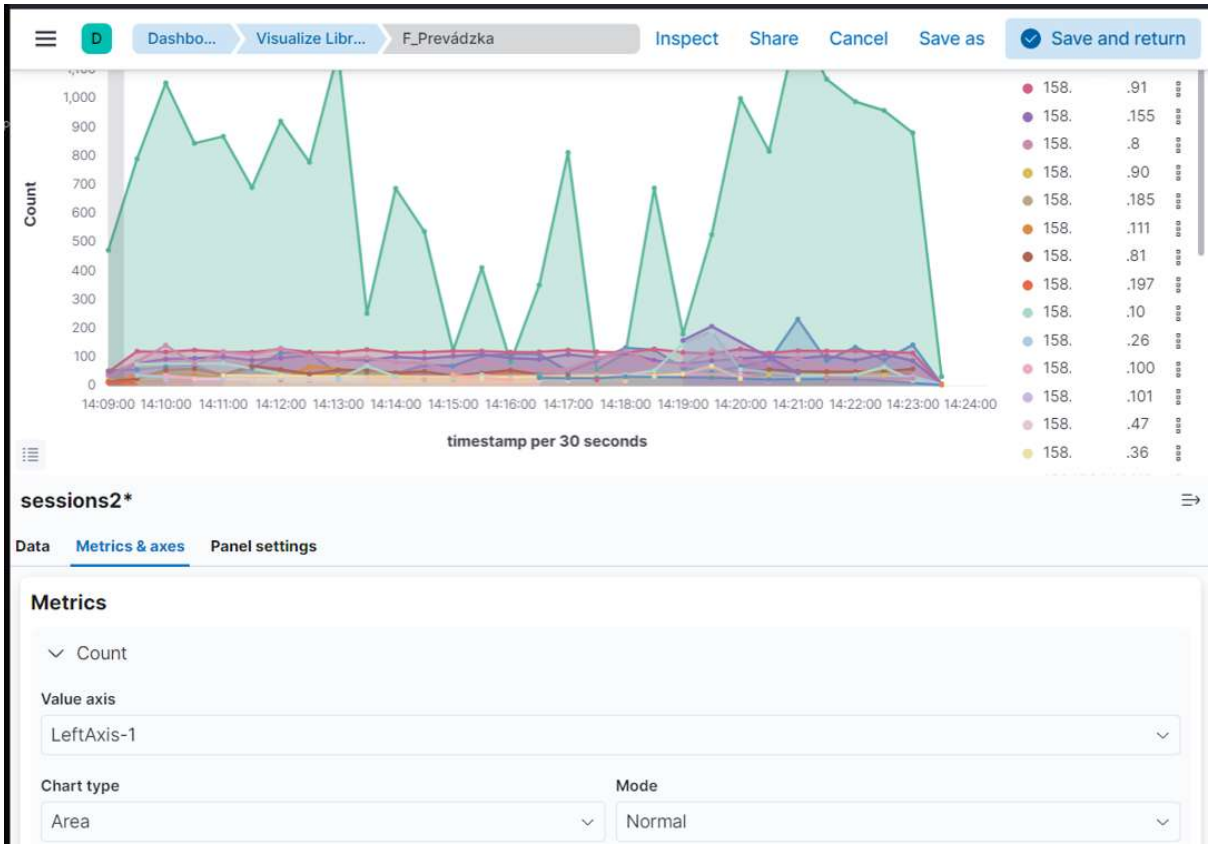


Figure 11 - Kibana - Chart after the change

List of filters used

1. F_CelkovaPrevadzka
-
2. F_Download
dstIp : "158.***.***.0/27" or dstIp : "2001:***:***::0/48"
3. F_Upload
srcIp : "158.***.***.0/27" or srcIp : "2001:***:***::0/48"
4. F_Download - clients from the Internet
(srcIp : "158.***.***.0/27" or srcIp : "2001:***:***::0/48") and (NOT dstIp : "158.***.***.0/27" or NOT dstIp : "2001:***:***::0/48")
5. F_Upload - clients from the Internet
(NOT srcIp : "158.***.***.0/27" or NOT srcIp : "2001:***:***::0/48") and (dstIp : "158.***.***.0/27" or dstIp : "2001:***:***::0/48")
6. F_Service traffic (network application services)
(protocol : "tcp" or protocol : "udp") and (
(dstPort : 161 or dstPort : 162) or
(dstPort : 25 or dstPort : 587 or dstPort : 465 or dstPort : 2525) or
(dstPort : 53) or
(dstPort : 67 or dstPort : 68) or
(dstPort : 445 or dstPort : 139) or
(dstPort : 23)
)
7. F_Routing protocols ***
protocol :"gre"
8. F_Operations
(dstIp : "158.***. ***.0/24" or dstIp : "158.***. ***.0/24" or dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24" or dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24" or dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24") or
(dstIp : "158.***. ***.0/24") or
(dstIp : "158.***.***.0/24" or dstIp : "158.***. ***.0/24")
9. F_Traffic by laboratories
(srcIp : "158.***. ***.0/24") or
(srcIp : "158.***. ***.0/24") or
(srcIp : "158.***. ***.0/24") or

(srcIp : "158.***. ***.0/24") or
(srcIp : "158.***. ***.0/24")

10. F_Top websites
(dstIp : "158.***.***.0/27" or dstIp : "2001:***:***::0/48") and (dstPort : 80 or dstPort : 443)

11. F_Top websites - Internet
(NOT dstIp : "158.***.***.0/27" or NOT dstIp : "2001:***:***::0/48") and (dstPort : 80 or dstPort : 443)

12. F_Top web servers - Intranet
(srcPort : 80 or srcPort : 443) and (protocol : "tcp") and (srcIp : "158.***.***.0/27" or srcIp : "2001:***:***::0/48")

13. F_Top web servers - Internet
(srcPort : 80 or srcPort : 443) and (protocol : "tcp") and (NOT srcIp : "158.***.***.0/27" or NOT srcIp : "2001:***:***::0/48")

14. F_TCP services
protocol : tcp and srcIp : "158.***.***.0/27" and srcPort < 49151

15. F_UDP services
protocol : "udp" and srcIp : "158.***.***.0/27" and srcPort < 49151

16. F_Mail traffic
(srcPort : 110 or srcPort : 995) or
(srcPort : 143 or srcPort : 993) or
(srcPort : 25 or srcPort : 587 or srcPort : 465 or srcPort : 2525)

17. F_Stations with the highest number of flows
srcIp : "158.***.***.0/27" or srcIp : "2001:***:***::0/48"

18. F_Stations with the highest number of flows - Internet
NOTsrcIp : "158.***.0.0/16" or NOT srcIp : "2001:***:***::0/48"

19. F_Top mail senders and SMTP servers
(protocol : "tcp" or protocol : "udp") and (srcPort : 25 or srcPort : 587 or srcPort : 465 or srcPort : 2525)

20. F_Top mail users and POP3/IMAP servers
(srcPort : 110 or srcPort : 995) or
(srcPort : 143 or srcPort : 993)

21. F_Downlad – Cloud2
dstIp : "158.***. ***.0/24" or dstIp : "2001:***:***:124::/64"

22. F_Upload – cloud2
NOT srcIp : "158.***. ***.0/24"

23. F_Upload - labs2
srcIp : "158.***. ***.0/24" or srcIp : "158.***. ***.128/25"

24. F_Download - labs2
dstIp : 158.***. ***.0/24 or srcIp : 158.***. ***.128/25