PROJECT

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

Dashboards – visualization of data from tools

Linked to work package KPB2
Dashboards – analysis of security events

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

Kibana – Dashboard....4
Discover....5
Dasboards....13
Alerts....16
Investigating a security alert....18

List of figures

Figure 1.... 4
Figure 2.... 5
Figure 3.... 6
Figure 4.... 6
Figure 5.... 7
Figure 6.... 7
Figure 7.... 8
Figure 8.... 8
Figure 9.... 8
Figure 10.... 9
Figure 11....10
Figure 12....10
Figure 13....11
Figure 14....11
Figure 15....12
Figure 16....12
Figure 17....13
Figure 18....15
Figure 19....16
Figure 20....16
Figure 21....17
Figure 22....17
Figure 23....18

Kibana – Dashboard

In Kibana, it is possible to create so-called spaces. These spaces serve to separate data logically.

Accounts in Kibana are created according to a specific role, which allows access only to the required space.

The three most important sections in our deployment are currently the *Discover*, *Dashboards* and *Alerts* ***(Security section)*** sections. The Discover section serves to display the collected data in text form. The Dasboards section serves to display the created visualizations of the collected data. The Alerts section serves to display security alerts.

We access the individual sections using the “hamburger” button in the upper left corner of the screen.

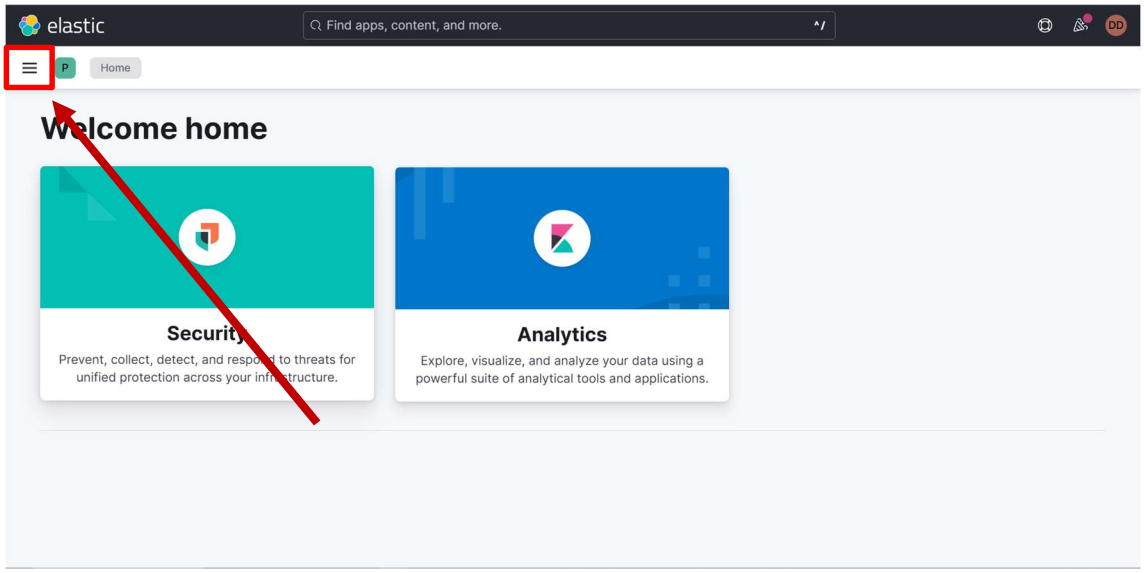


Figure 1

After clicking, a menu expands containing the individual sections.

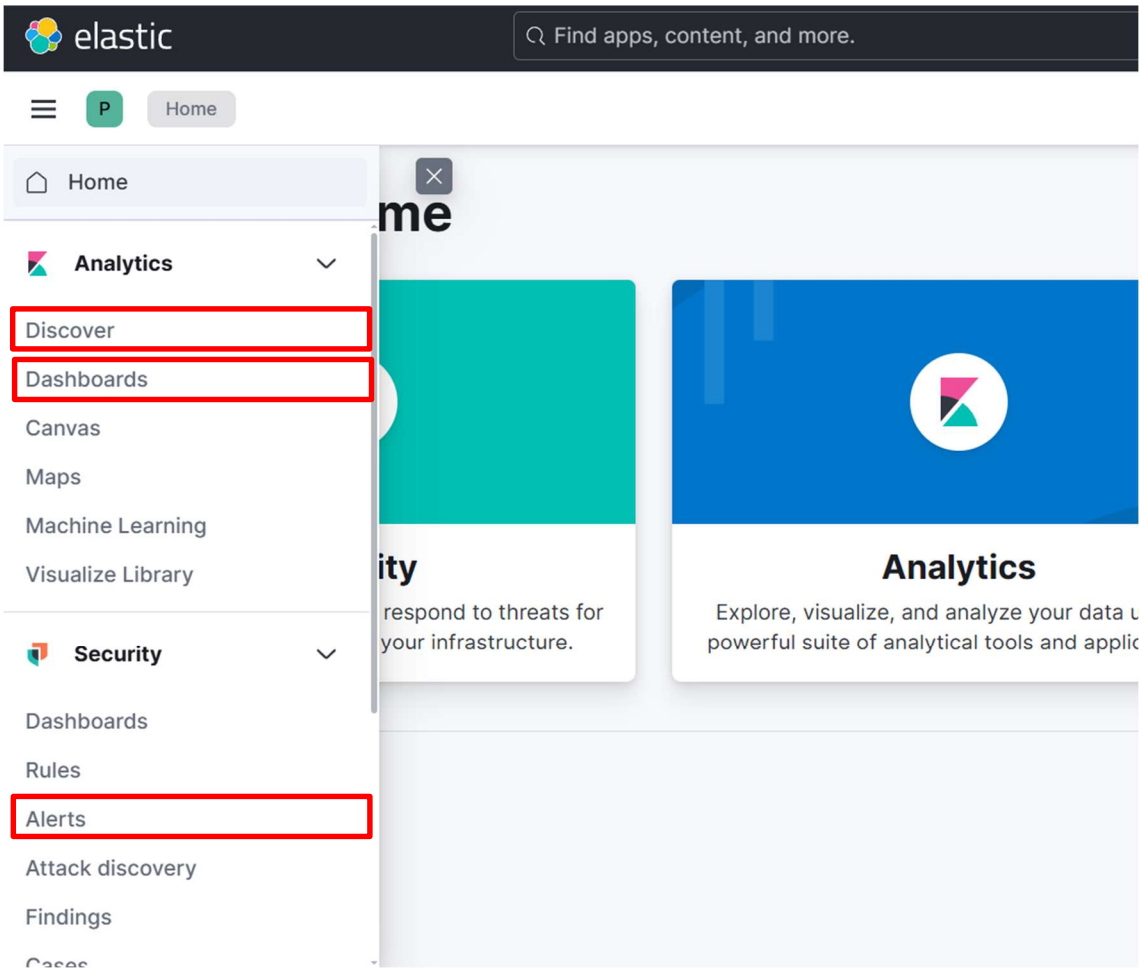


Figure 2

Discover

The Discover section looks as follows.

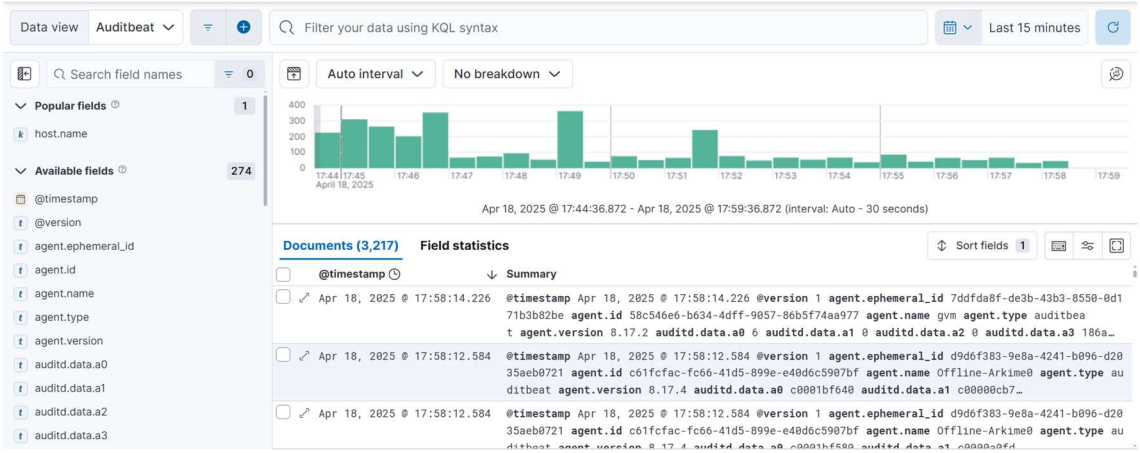


Figure 3

As can be seen in the figure, the individual pieces of received data are stored as records, i.e. documents. The documents are sorted by time, i.e. by the *timestamp* field. Records can be sorted in ascending or descending order.

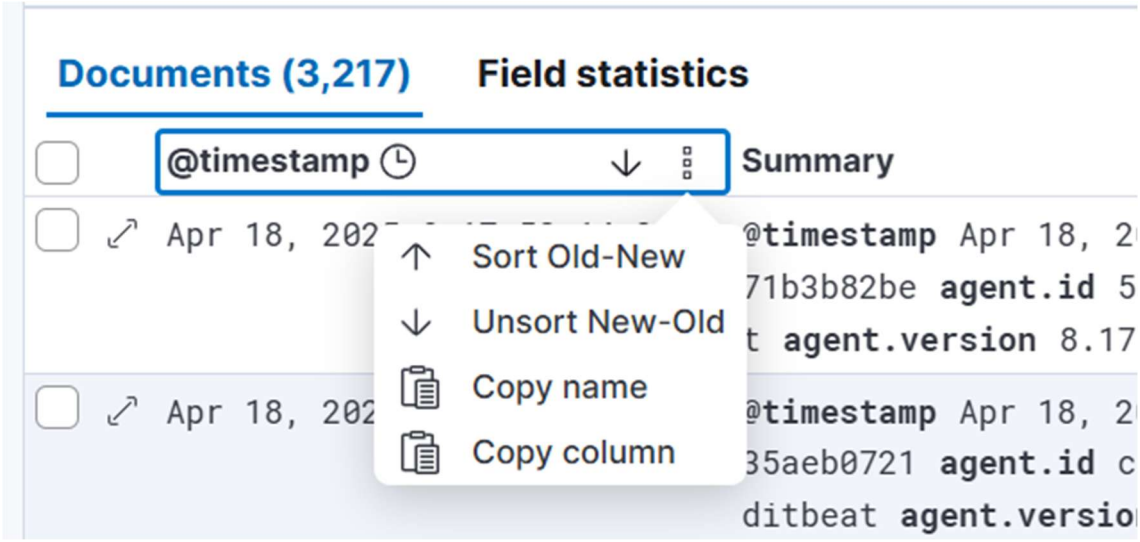


Figure 4

Time is very important for correct analysis; therefore, the first step is to set the correct time range, i.e. the time window. The setting for the time range can be found in the upper right corner.

Funded by the European Union
NextGenerationEU
RECOVERY AND RESILIENCE PLAN
GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

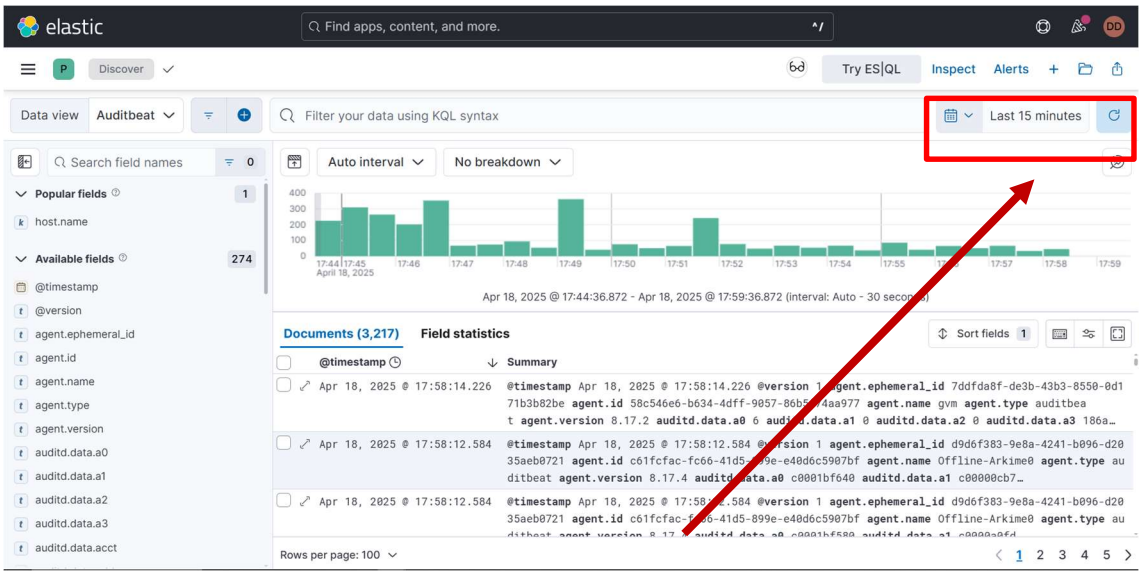


Figure 5

If we click on the calendar icon, we can choose from several options for selecting the time window. These options are predefined and extend from some point in the past to the current moment.

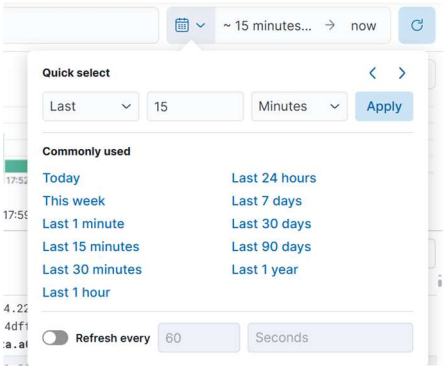


Figure 6

The figure shows that we can also set an automatic refresh of the data; this is suitable for dashboards or alerts, but we do not recommend it for Discover. If we click on the part just after the calendar icon, we select the “Start date”.

Funded by the European Union
NextGenerationEU
RECOVERY AND RESILIENCE PLAN
GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

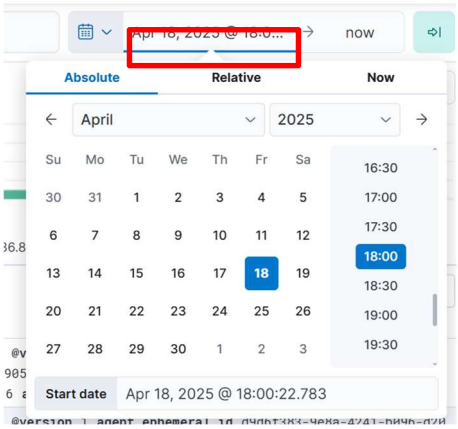


Figure 7

We can choose from the options *Absolute*, *Relative* and *Now*. The *Relative* option serves to select predefined values. The *Absolute* option serves to select a specific point in time. Similarly, if we click on the rear part after the calendar symbol, we select the “End date”.

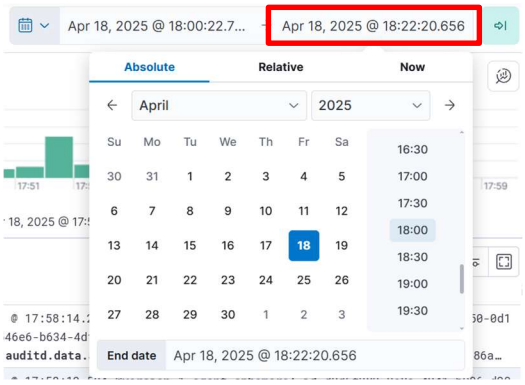


Figure 8

The selection of the time window must, of course, be confirmed.

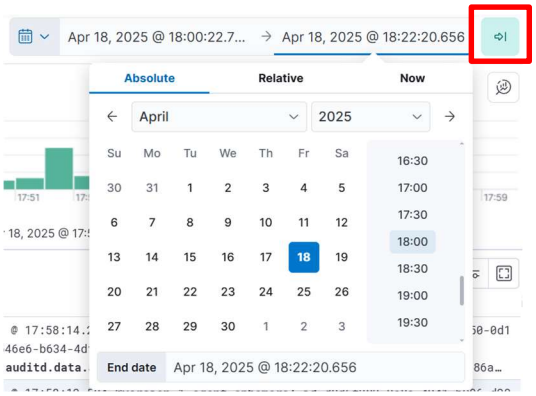


Figure 9

Funded by the European Union
NextGenerationEU
RECOVERY AND RESILIENCE PLAN
GOVERNMENT OFFICE OF THE SLOVAK REPUBLIC

Even more important than selecting the correct time window is selecting the correct data source. Data sources are represented by means of a *Data view*. The data view is selected in the left corner of the screen.

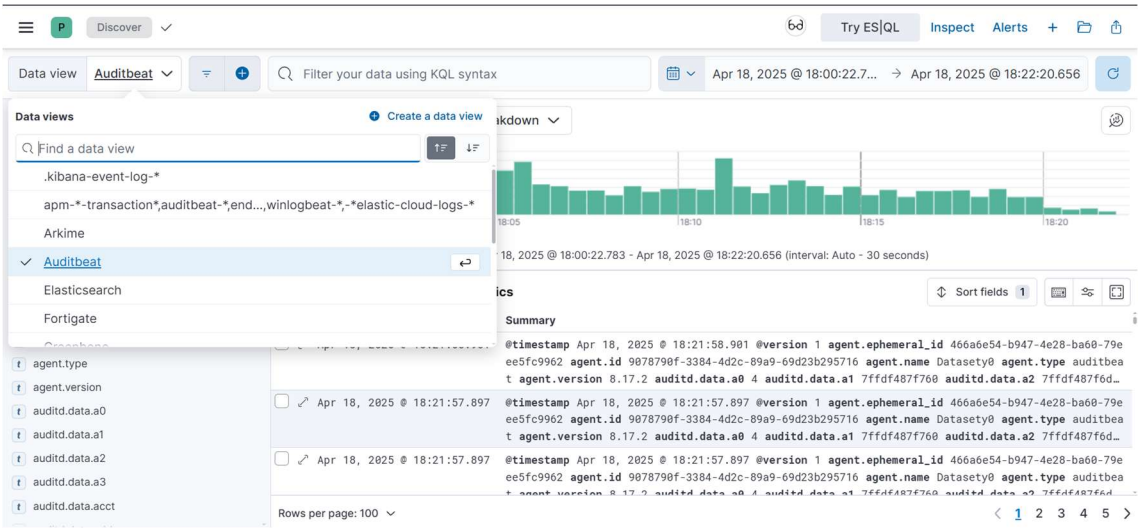


Figure 10

We can choose from several data views that we have created.

- **Auditbeat** – data from Linux devices
- **Arkime** – data from the Arkime tool
- **Elasticsearch** – extended logging of the Elasticsearch tool
- **Fortigate** – data from the firewall device
- **Monitoring** – data from Metricbeat, for the purposes of dashboards
- **Suricata** – data from both Suricata IDSs
- **Threatintel** – collection of CTI information
- **WAF** – collection of data from the WAF device

For efficient searching of data in the Discover section, it is necessary to work with filters. We can filter using KQL (Kibana Query Language), using individual fields in documents or by creating graphical filters. For quick filtering, we recommend using KQL or filtering based on document fields. KQL queries are written in the search field at the top of the page.

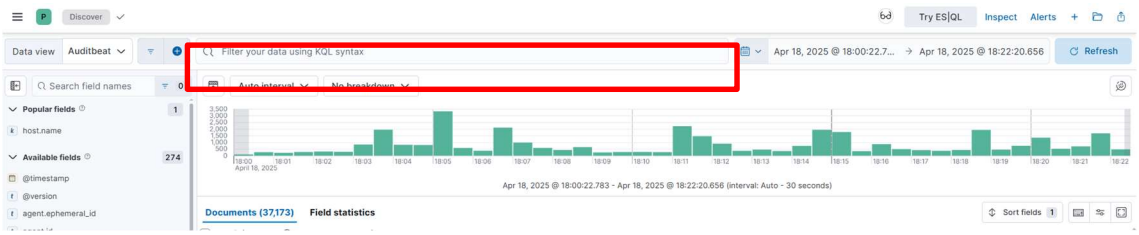


Figure 11

In this field, it is also possible to use so-called full-text search. If we want to search for a piece of text, we enclose this text in quotation marks, “text”. Most often, we create a filter in which we specify a field and its value. In the values, we can use so-called wildcards, i.e. *, which stand for any number of arbitrary characters. The symbol = means that the value is equal. In filters, we can also use the logical operators *and*, *or* and *NOT*. We can also extend the logic of filters using parentheses () .

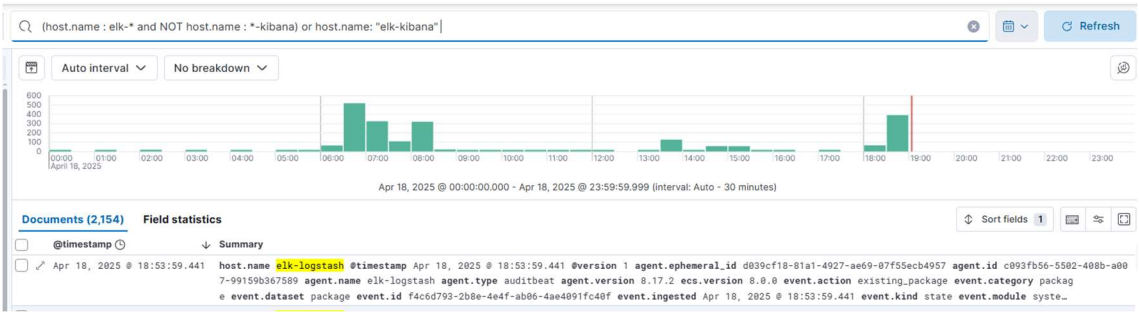


Figure 12

The figure above shows the use of a more complex filter in KQL. We display all data about a given record, i.e. document, using the double-headed arrow at the beginning of the record. More detailed information about the given record is displayed in the right-hand part.

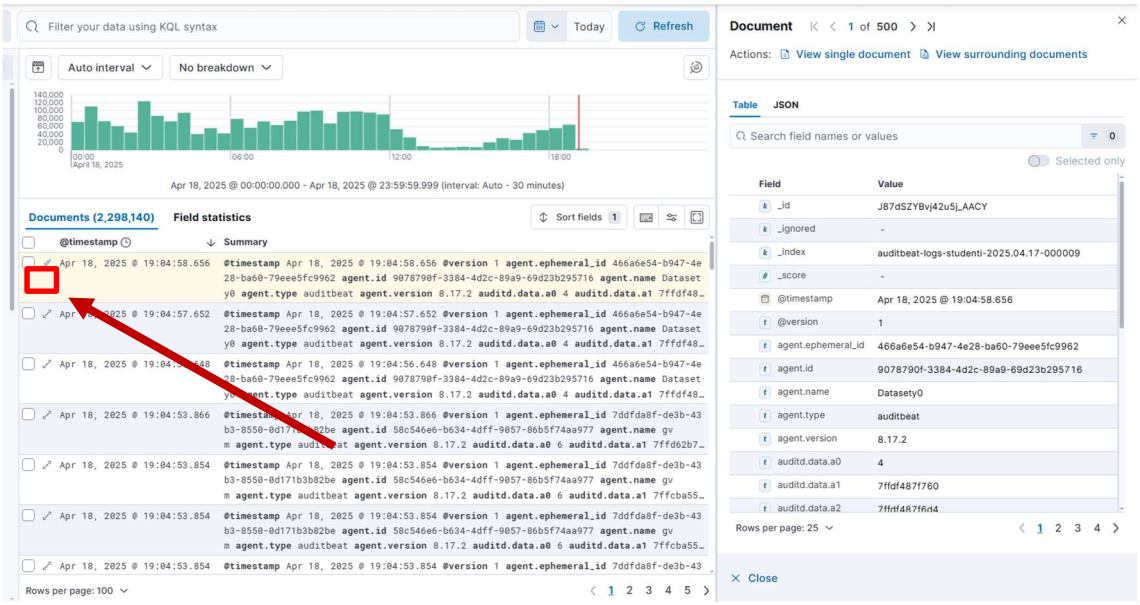


Figure 13

The right-hand part, which contains information about the given record, offers the option of filtering using a search field. We can improve the clarity of documents by displaying relevant information directly in the document preview. The left-hand part contains a list of the individual document fields. If we click on the plus symbol next to a field, only the fields selected in this way are displayed in the main preview.

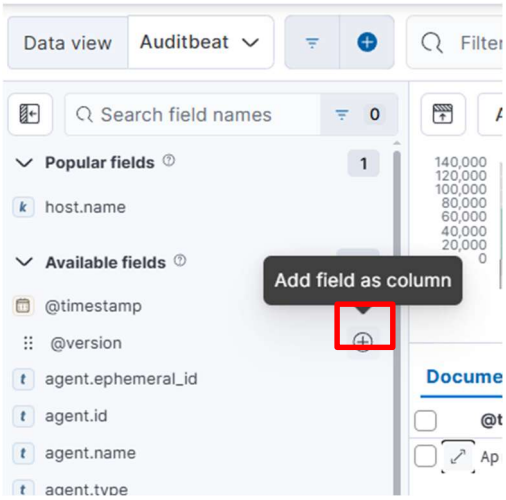


Figure 14

A customized main preview may, for example, look as follows.

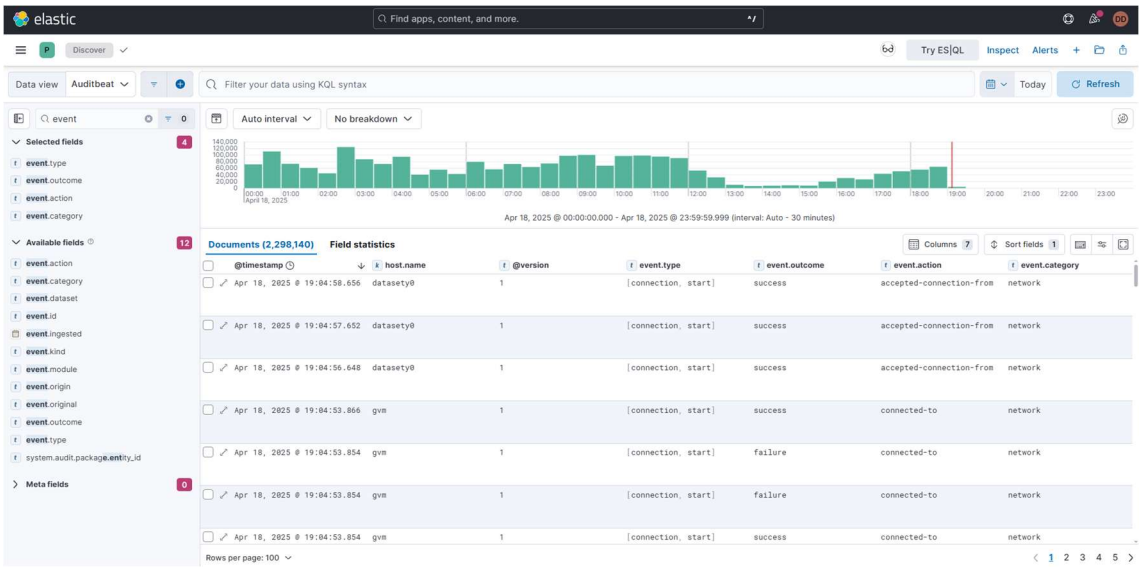


Figure 15

If we want to filter using a field of a given document, we can do so in the main view or in the view where the details of the given document are displayed. We go to the given field in the document and, with the plus symbol, display only records with this value, or, with the minus symbol, display records that do not contain this value.



Figure 16

Dasboards

The solution involves creating dashboards that display, for example, network statistics and successful/failed logins.

Procedure for creating a new dashboard:

1. Open the Dashboards page in Kibana.
2. Select the Create dashboard option and start with an empty dashboard.
3. After the dashboard is created, you are automatically taken to edit mode and can make changes to the dashboard.
4. Add content to the dashboard. You have several options, which are described in more detail in the Visualizations section:

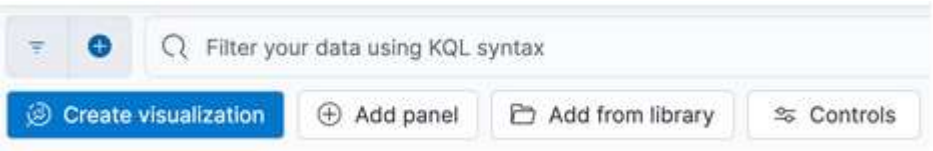


Figure 17

Create visualization. This option is a shortcut for creating a chart using Lens, the default visualization editor in Kibana.

Add panel. Select one of the available panels to add and configure content on the dashboard.

Add from library. Select existing content that has already been configured and saved to the Visualize library.

Controls. Add controls that help you filter the dashboard content.

5. Options for adding content to the dashboard
6. Organize the dashboard by arranging the various panels.
7. Define the main dashboard settings from the **Settings** menu, which is located in the toolbar.
8. A meaningful title, description and tags allow you to quickly find the dashboard later when browsing the list of dashboards or using the Kibana search bar.

   Additional display options allow you to unify the look and feel of the panels on the dashboard:

   Store time with dashboard – Saves the specified time filter.

Use margins between panels – Adds a margin between the individual panels.

Show panel titles – Displays the titles in the panel headers.

Sync colour palettes across panels – Applies the same colour palette to all panels on the dashboard.

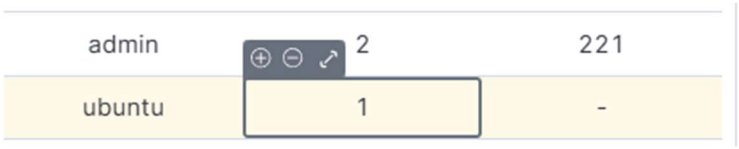
Sync cursor across panels – When you hover the mouse cursor over a time series chart or a heat map, the cursor is automatically displayed on all other related charts of the dashboard.

Sync tooltips across panels – When you hover the mouse cursor over a Lens chart, tooltips are automatically displayed on all other related charts of the dashboard.

9. Click Apply.

Example: **Login Activity Monitoring** – display of information about successful or failed user logins to the individual monitored servers

In dashboards, as in Discover, the principles of filtering and setting the time window apply.



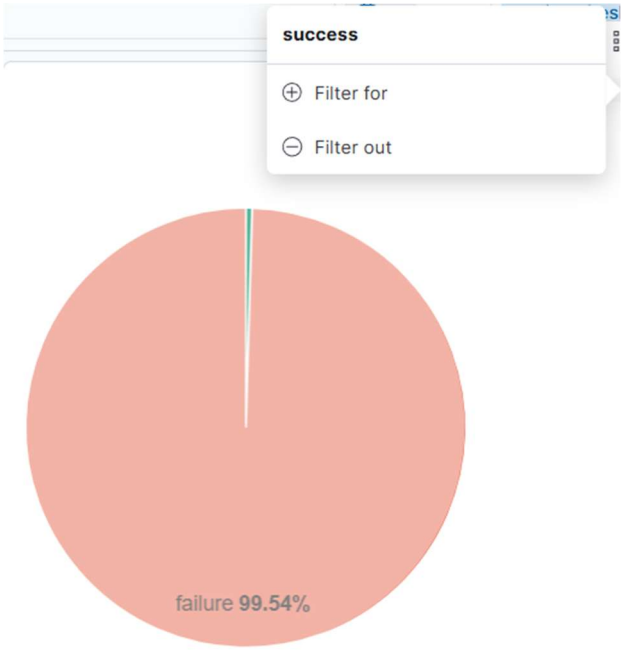


Figure 18

Alerts

Alerts display security alerts that were generated on the basis of predefined detection rules. The rules may be default (Elasticsearch) or custom. As part of the custom rules, we have created rules for detecting brute-force attacks, transformation rules, and rules that compare the received data with CTI data.

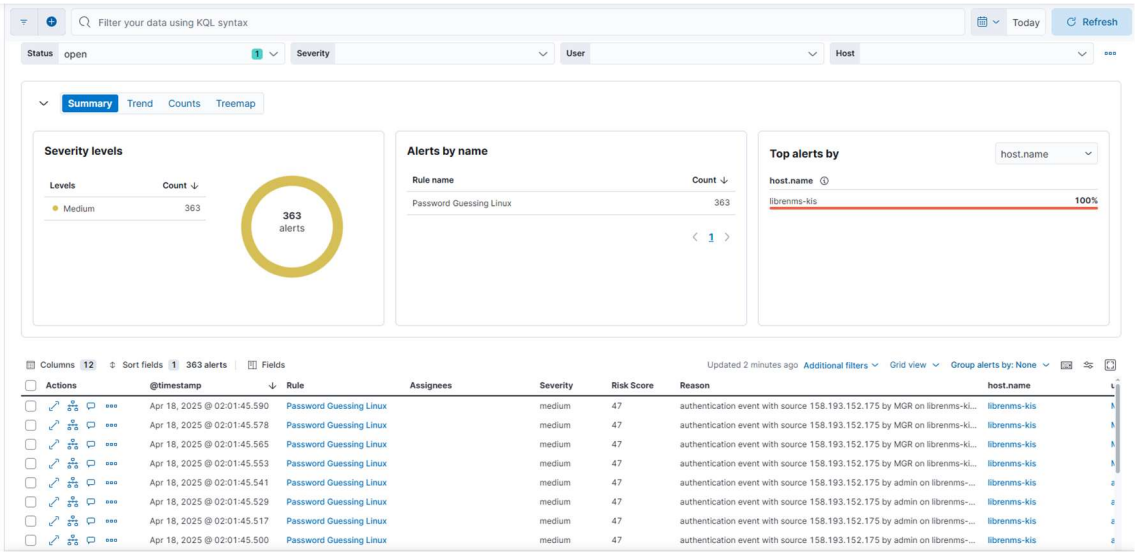


Figure 19

In the Alerts section too, filtering and setting the time window are used in the same way as in the Discover and Dashboards sections. A single security alert may be triggered by one or more records. We verify this by opening the so-called timeline.



Figure 20

After clicking, one or more records, i.e. documents, are displayed.

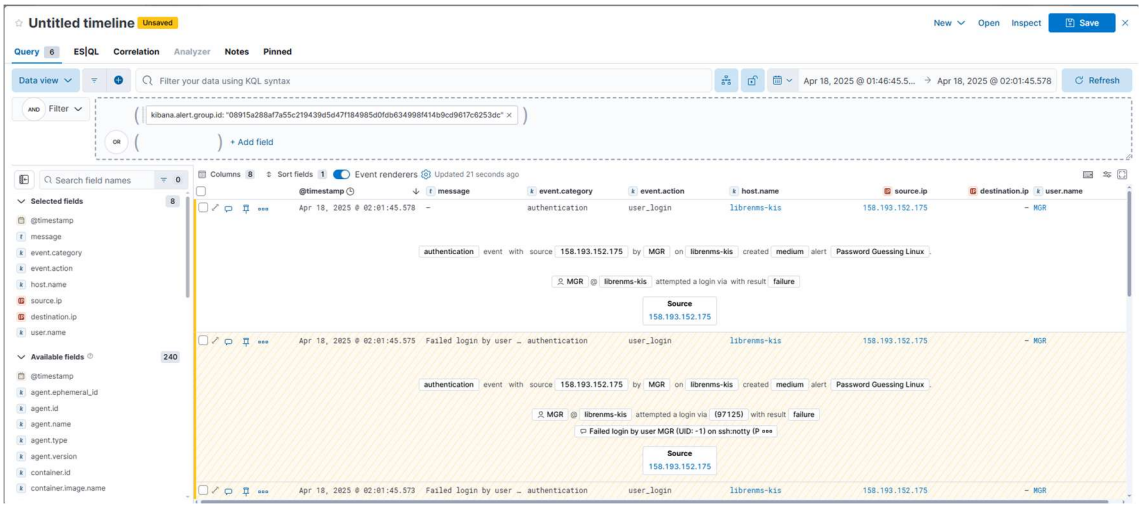


Figure 21

More detailed information about a security alert is displayed in the same way as information about a document in Discover. For a better understanding of the rule, it is possible to display the details of this rule and focus on its logic.

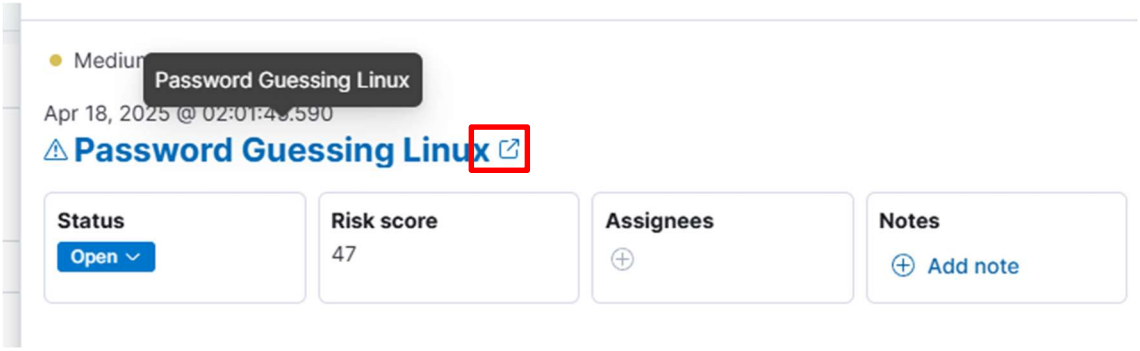


Figure 22

However, this does not apply to the transformation rules we have created.

For better clarity, it is possible to set which fields are to be displayed for the individual security alerts and in what order.

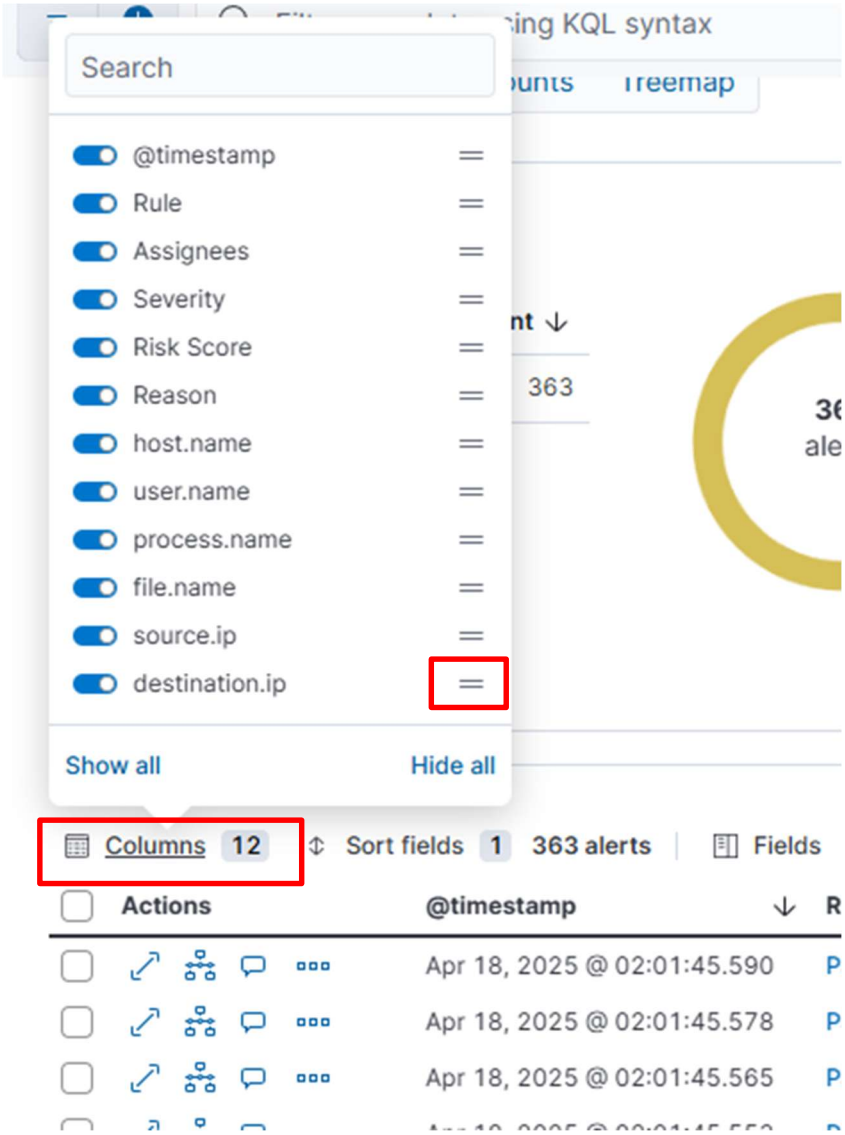


Figure 23

Investigating a security alert

First of all, it must be said that the user cannot know all the detection rules. For this reason, it is necessary first to understand why the given security alert was triggered. Displaying information about the given rule can help with this. Language models can also be very helpful. It is very important to verify the information. When handling a security incident, not all information from the machine to which the security alert relates is monitored; it is advisable to communicate with the owner of the system to which the given security alert relates. During the investigation, we recommend working in the Discover

section. The analysis requires perceiving the system as a whole. Focusing on the single activity for which the alert was triggered is incorrect. If it were an attack, more steps would be needed to carry it out. We recommend looking at the *Cyber Kill Chain* and *MITRE ATT&CK*. It is also advisable to use online tools:

- www.virustotal.com – checking IP addresses and files
- www.abuseipdb.com – checking IP addresses
- www.any.run - sandbox
- www.tria.ge – sandbox
- www.urlscan.io – checking websites