Security Events

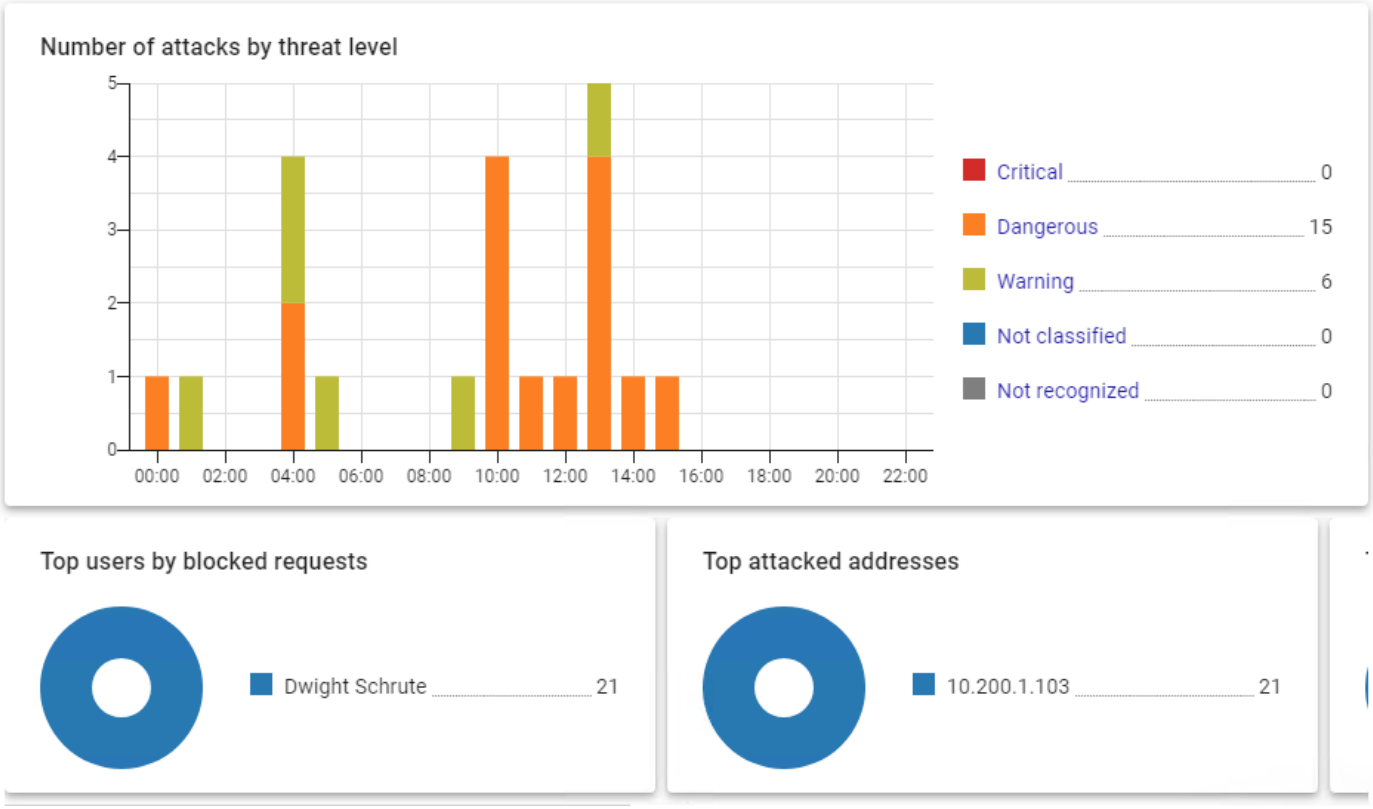
Contains information about the triggering of the rules specified in the Intrusion Prevention section.

> All widgets are generated in the server's time zone.

The section structures the information received from the **Intrusion prevention** section.

Period selection

All displayed data can be filtered by date and time. For example, set some time period (by clicking the "Choose date" button) or use one of the preset filters:



If no filter by date and time is set, then the interval is set to **Today** in the server's time zone by default.

Widgets

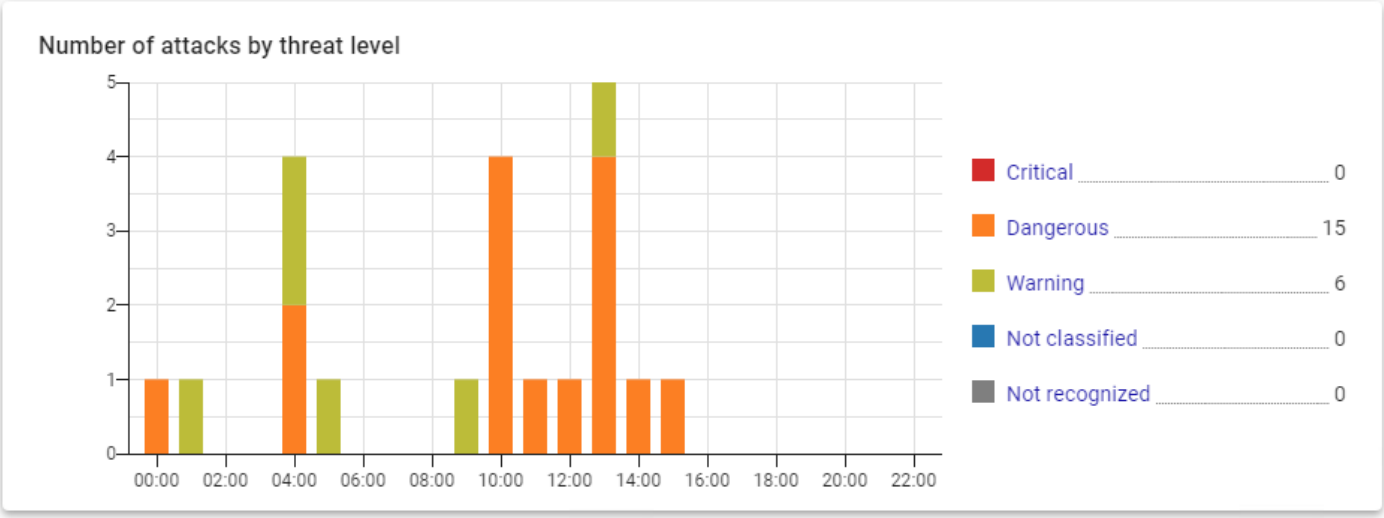
All information collected by widgets is presented in detail in the form of a table at the bottom of the section. In it, you can find the ID of the rule that worked and, if necessary, create an exception in the **Intrusion prevention** section.

Number of attacks by threat level

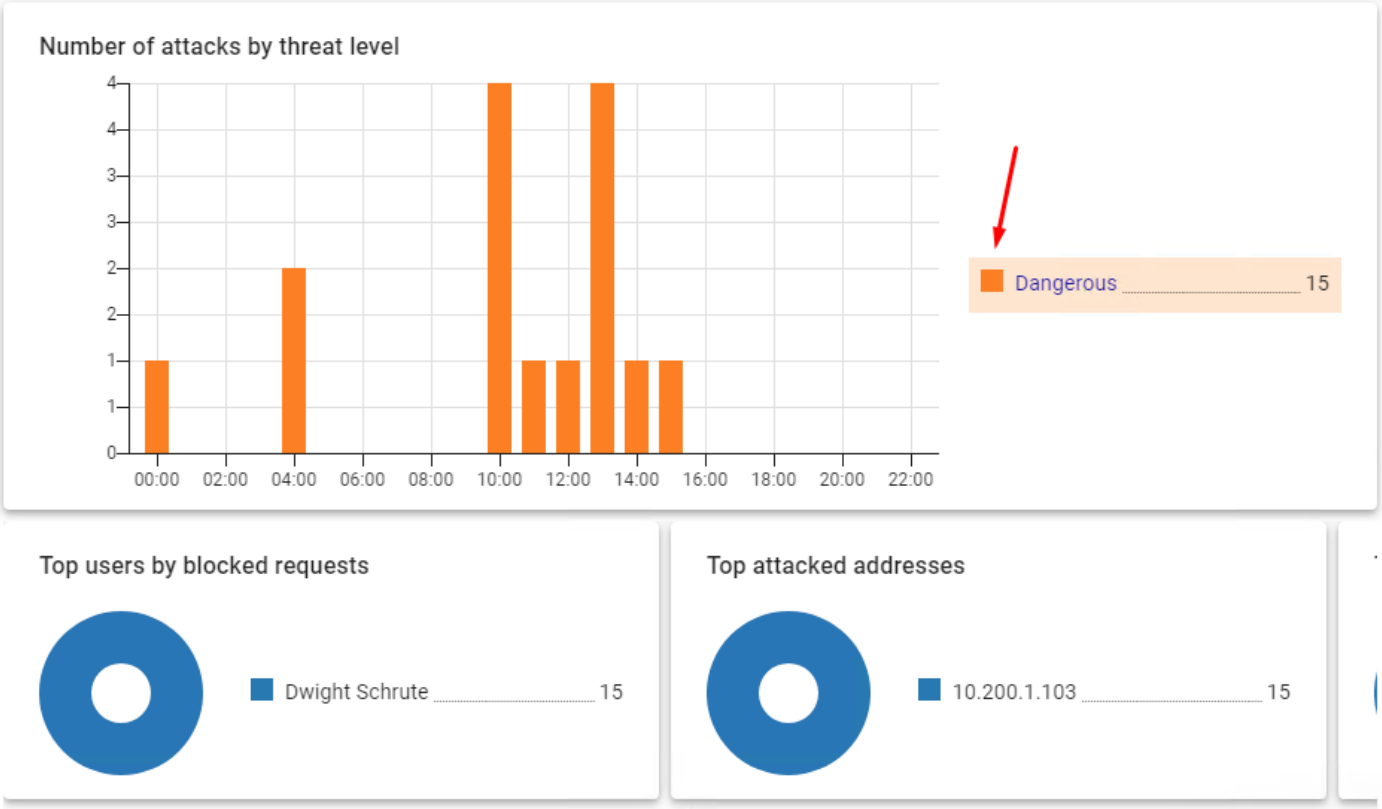
The information is provided in the form of a graph with five security threat values:

- **Critical** - threat level 1.
- **Dangerous** - threat level 2.
- **Warning** - threat level 3.
- **Not classified** - threat level 4.
- **Not recognized** - threat level 255.

Widget example Number of attacks by threat level:



When you click on a threat level, all widgets and the table filter the content for that level. To go back to the list of threat levels, click again on the selected level:



Top users by blocked requests

Only those users who were successfully authorized get to the top. Thus, unauthorized users whose requests were blocked will not get into the diagram.

Top Attacked Addresses

Both external and internal areas fall into that of the attack. One example where the attacked address is external is when a Trojan operates from inside the protected network.

Top attacking addresses

The attacking address can be either external or internal. For example, the address from which the work of the Trojan was recorded can be considered an internal attacking address.

Top Blocked Attack Types

The widget calculates the statistics of attack types (for example, attack types IP Address Blacklist or Attempts to obtain administrator privileges, combining a group of several rules) by the number of hits with this type of attack.
The type of attack is listed in the Security Event column in the table at the bottom of the section.

Top attacking countries

The top attacking countries are based on the IP addresses obtained when the rules in the Intrusion Prevention section are triggered. If an IP address is not geocoded into a country name, that address is not displayed in the widget.
For this reason, local IP addresses are not shown in the widget.

Revision #5
Created 27 August 2022 17:44:50 by Val Redman
Updated 13 October 2022 15:49:03 by Val Redman