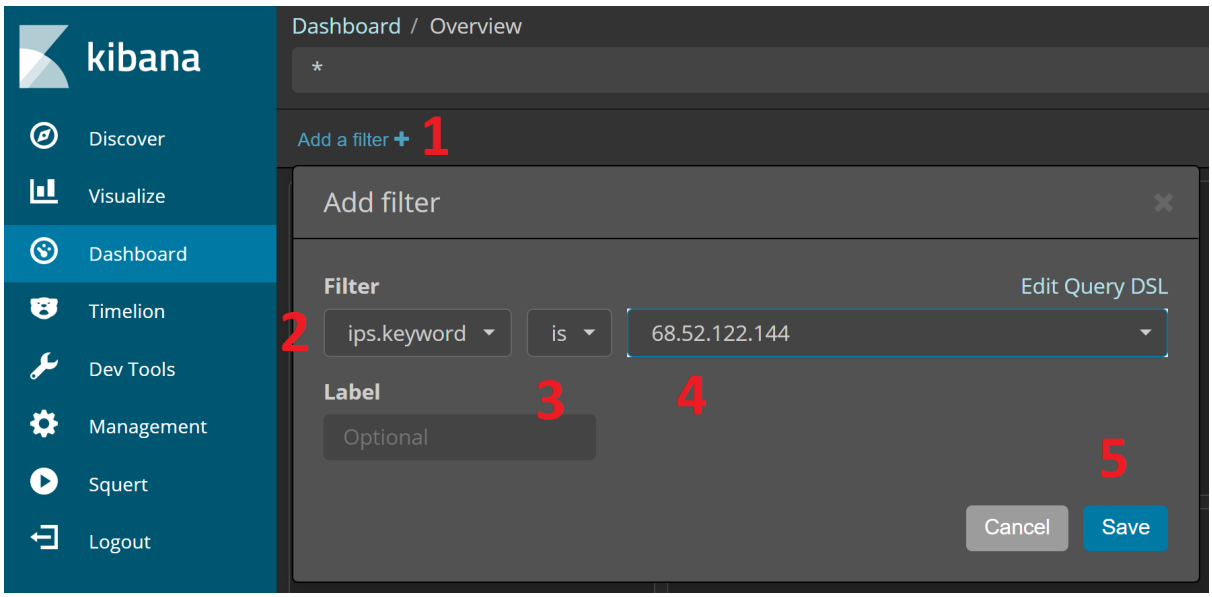
KIBANA

KIBANA Field filter keywords

Search by generic IP: **ips.keyword**
Search by source IP: **source_ips.keyword**
Search by destination IP: **destination_ips.keyword**

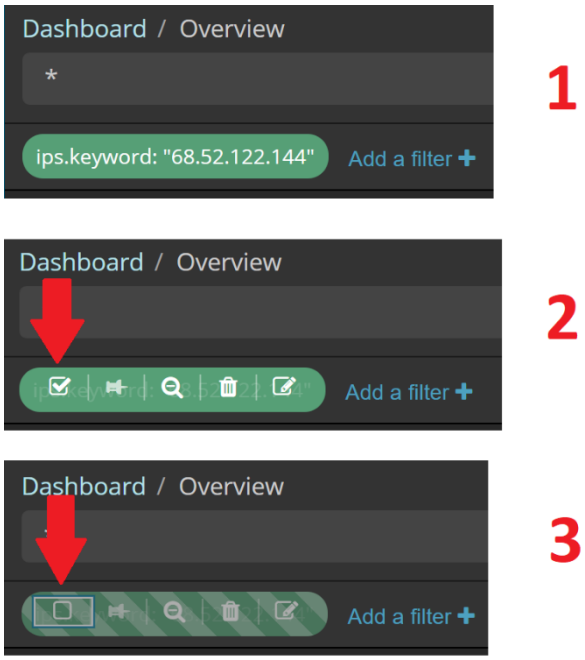
Add a filter

1. On top left, click on "*Add a filter* +". A menu will open;
2. In the textbox "*Fields…"* write the kind of resource you're looking for (examples provided below)
3. In "*Operators..."* write **is** or **is not;**
4. In "*Values"* the IP or port you're looking for;
5. Click on save.



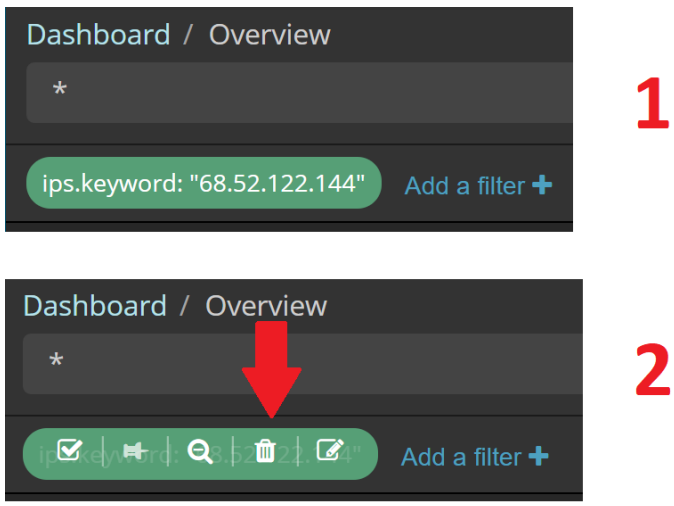
Temporarily disable filter

1. Move the mouse over the filter you want to disable;
2. Click on the checkbox icon (first icon to left);
3. Click it again to re-enable the filter.



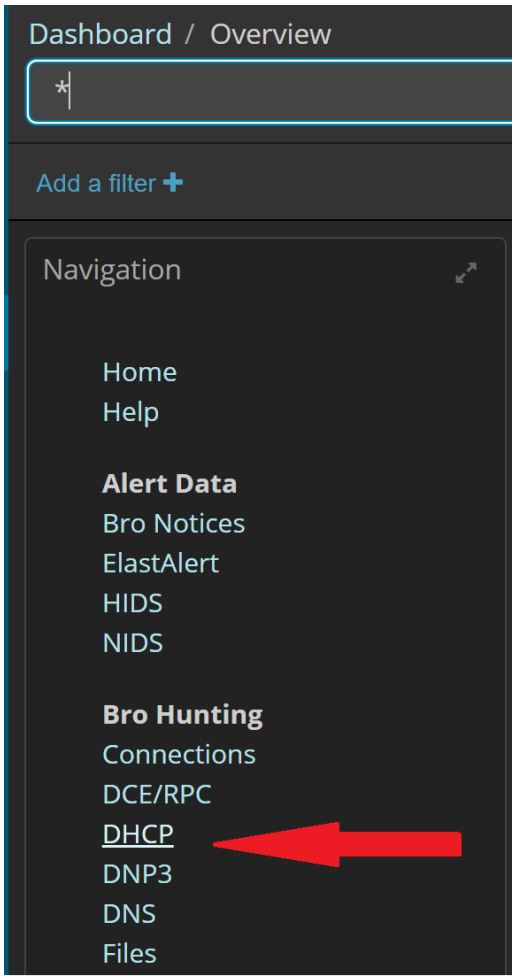
Delete filter

1. Move the mouse over the filter you want to delete;
2. Click on the trash bin icon (second from the right).

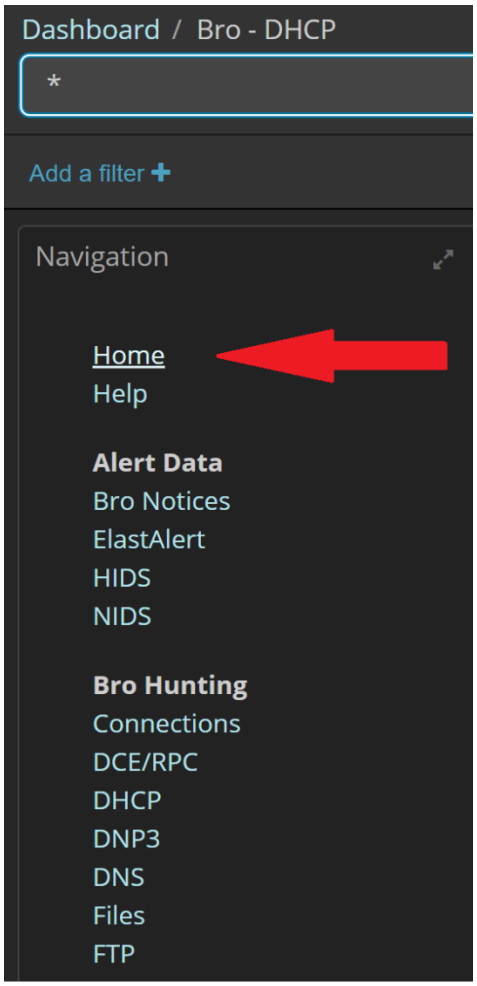


Filter by service/protocol

1. On the left, click on the required service/protocol;
2. To disable this filter, click on "*Home*" on top of the same list.



1

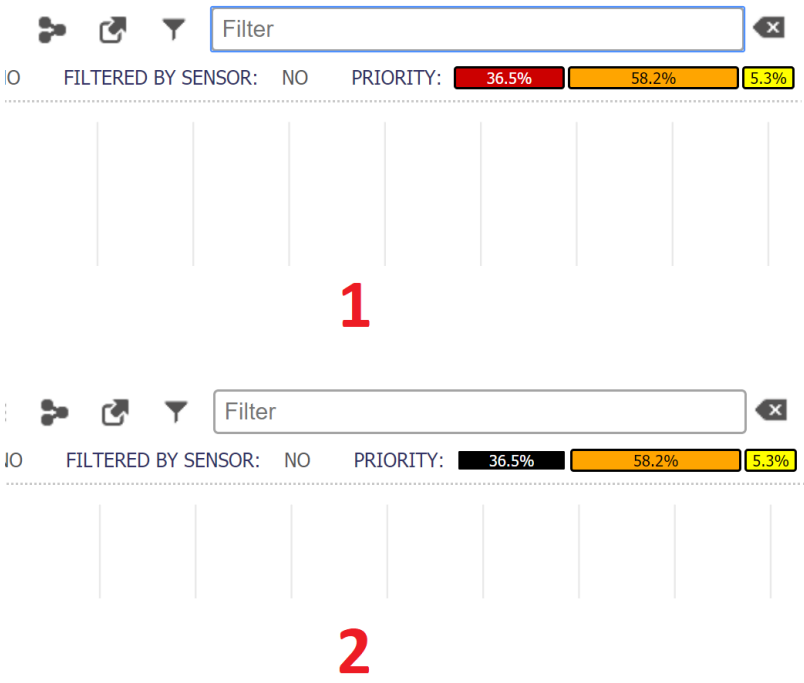


2

SQUERT

Filter by alert priority

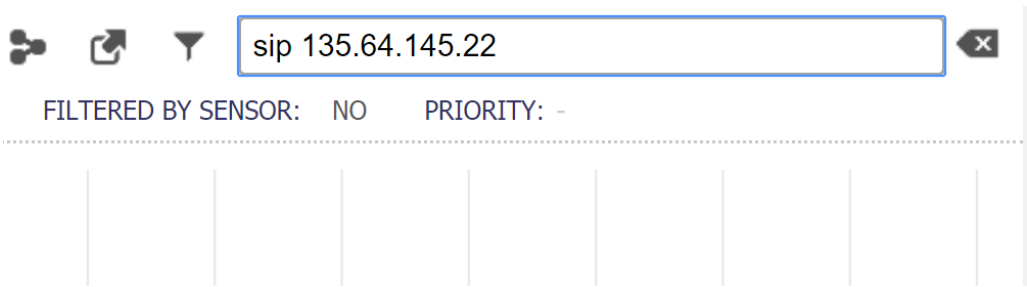
1. On top right, under “Filter”, there can be three bars. Red for high, orange for medium, yellow for low priority;
2. Click on a priority to filter the alerts accordingly;
3. Clicking again on the same priority, will disable the filter.



SQUERT Field filter keywords

Search by generic IP: **ip**
Search by source IP: **sip**
Search by destination IP: **dip**

Set a filter



1. On top right, write in the “Filter” textbox filter followed by the IP address.
2. Press enter.

Unwrap alerts and explore

1. On the list of alerts, click one of interest clicking on the number of events;
2. From here, a list will expand with the events grouped by source-destination. Click on the number of alerts to expand;
3. Now you have the single events involving those two parts. Click on RT to expand;
4. From here, you get the details about the single event, such as content and signature.