

Find and filter detections

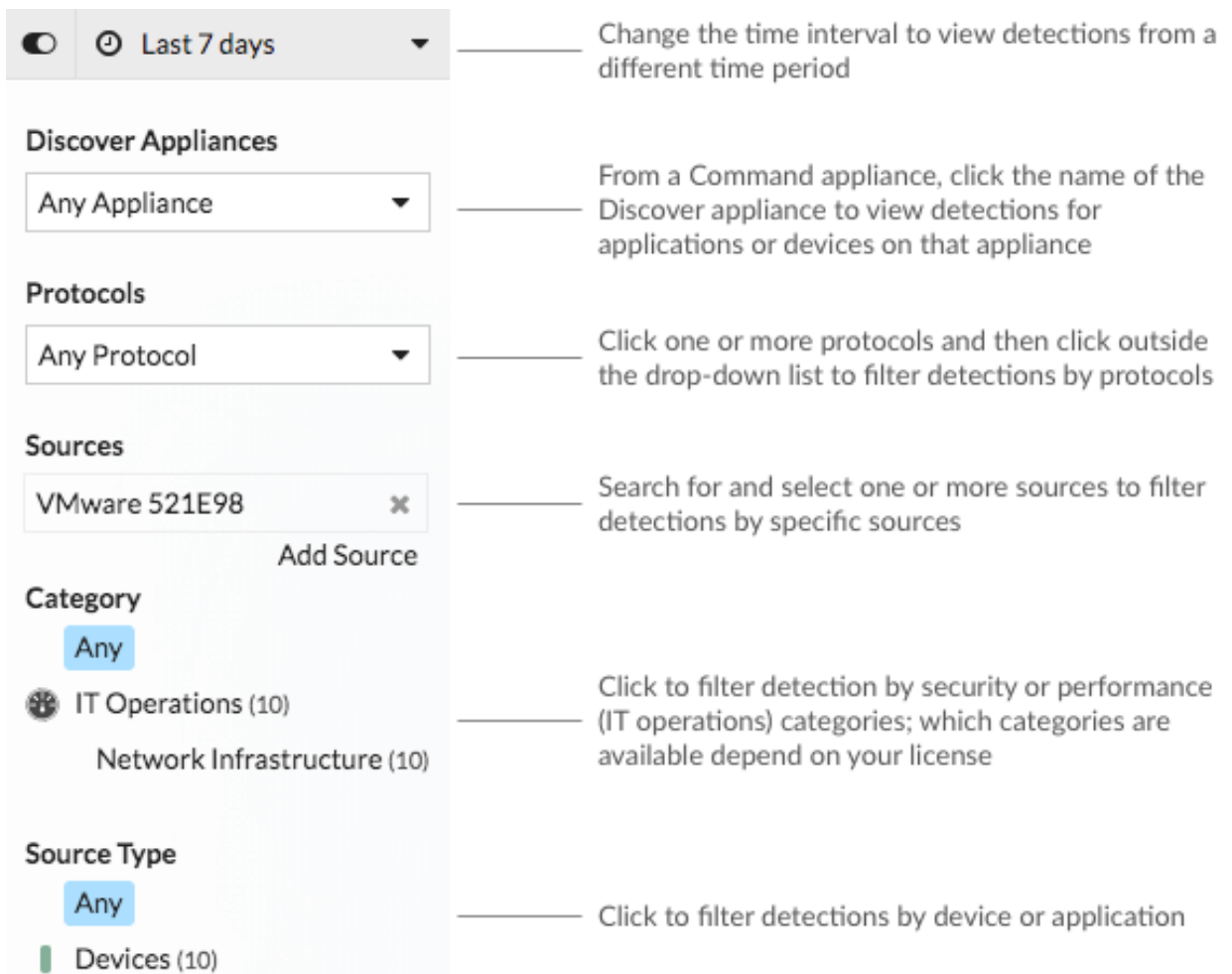
Published: 2018-07-07

You can filter detections by time interval, protocol, category, applications, or devices. Detections are sorted by their start time and the most recent detection is listed first.

Before you begin

You must be [connected to the ExtraHop Machine Learning Service](#).

1. Log into the Web UI on a Discover or Command appliance, and then click **Detections** at the top of the page.
A list of detections for the current time interval appears. If the list is empty, the Machine Learning Service has not identified detections for the selected time interval.
2. In the left pane, filter detections by selecting the options as shown in the following figure:



The screenshot shows a sidebar with the following filters and their corresponding callouts:

- Time Interval:** A dropdown menu set to "Last 7 days". Callout: "Change the time interval to view detections from a different time period".
- Discover Appliances:** A dropdown menu set to "Any Appliance". Callout: "From a Command appliance, click the name of the Discover appliance to view detections for applications or devices on that appliance".
- Protocols:** A dropdown menu set to "Any Protocol". Callout: "Click one or more protocols and then click outside the drop-down list to filter detections by protocols".
- Sources:** A search box containing "VMware 521E98" with an "Add Source" button. Callout: "Search for and select one or more sources to filter detections by specific sources".
- Category:** A list of categories: "Any" (selected), "IT Operations (10)", and "Network Infrastructure (10)". Callout: "Click to filter detection by security or performance (IT operations) categories; which categories are available depend on your license".
- Source Type:** A list of source types: "Any" (selected) and "Devices (10)". Callout: "Click to filter detections by device or application".

Next steps

- [Investigate detections](#)
- [Configure detection alert settings](#) to see an alert when a specific detection is identified
- [Add a notification to an alert configuration](#) to receive emails when a detection alert is generated
- Monitor detection alerts from the [Alert History](#) page