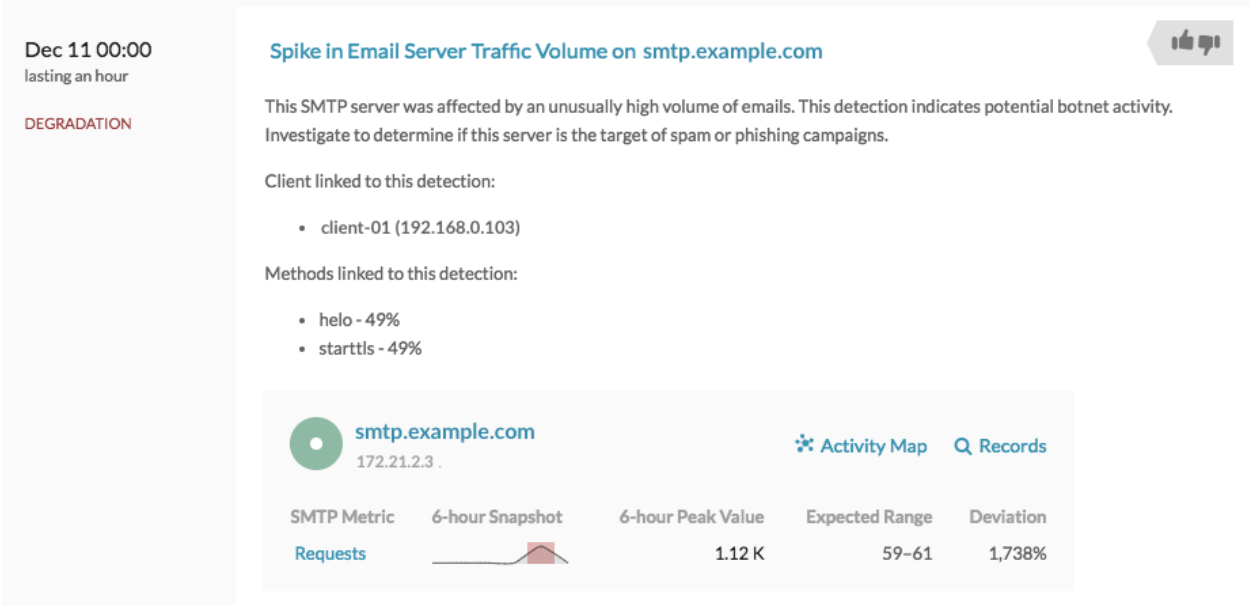
Investigate detections

Published: 2019-02-11

A detection uncovers unusual behavior on your network. After finding a detection, you might wonder how this behavior is directly affecting the devices and resources on your network. To find answers to your question, you can launch an investigation directly from a detection.

All detections include a general description of what contributed to the unusual behavior. For example, the following figure shows which client and methods are linked to the spike in server traffic volume.



To collect more specific information about a detection, you can continue your investigation by completing the following steps.

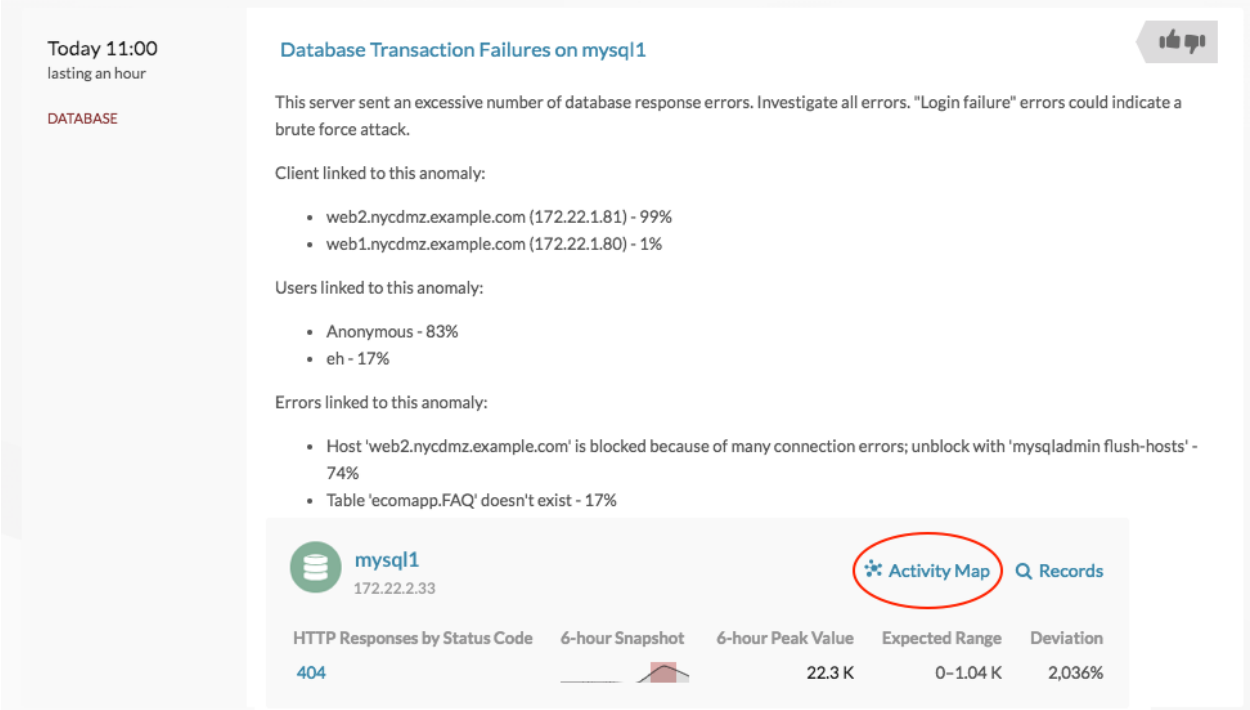
- For detections associated with L7 protocol metrics, click **Activity map** to see the peer device connections to the client or server associated with the detection.
- Click the device or application name to navigate to the protocol page.
- If you have a connected Explore appliance and detections associated with metrics, click **Records** to view transaction-level information filtered to the detection source.

> **Note:** To view records, you must have stored records for the protocol associated with the detection. For more information, see Collecting and storing built-in records.

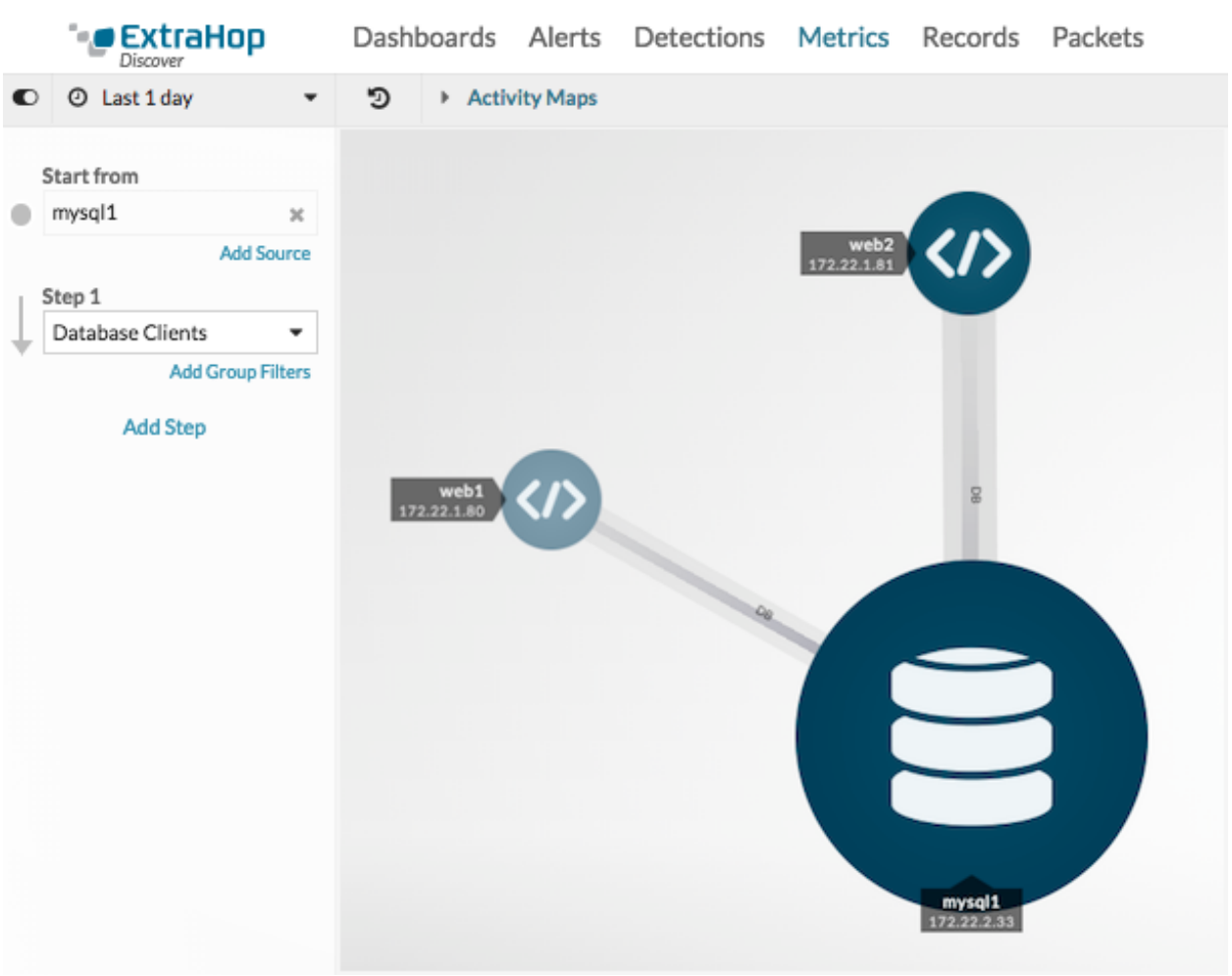
Open an activity map from a detection

When a single client or server is associated with unusual L7 protocol activity, such as a high number of HTTP errors or DNS request timeouts, an activity map link appears.

1. Log into the Web UI on a Discover or Command appliance, and then click **Detections** at the top of the page.
2. Find the detection that you want to investigate. The following figure shows an example of the **Activity Map** link for a database server that sent an unusual number of errors.

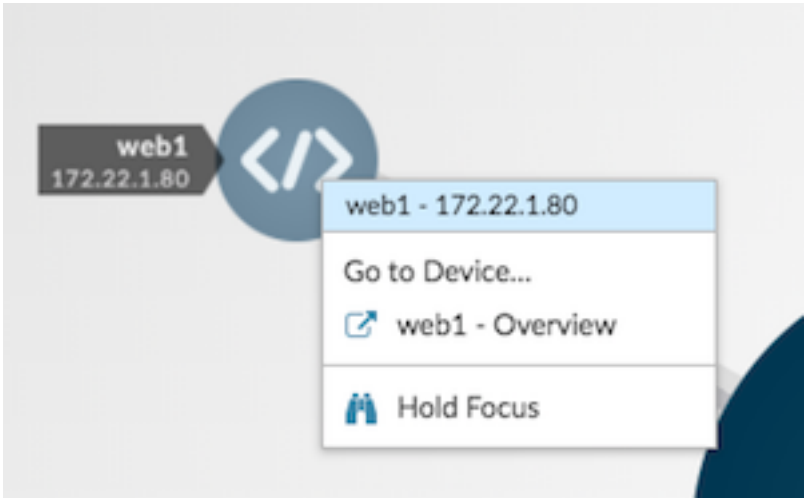


3. Click **Activity Map**.
   An activity map appears for the database server. The activity map in the following figure shows the two database clients that were connected to the server during the detection time frame.

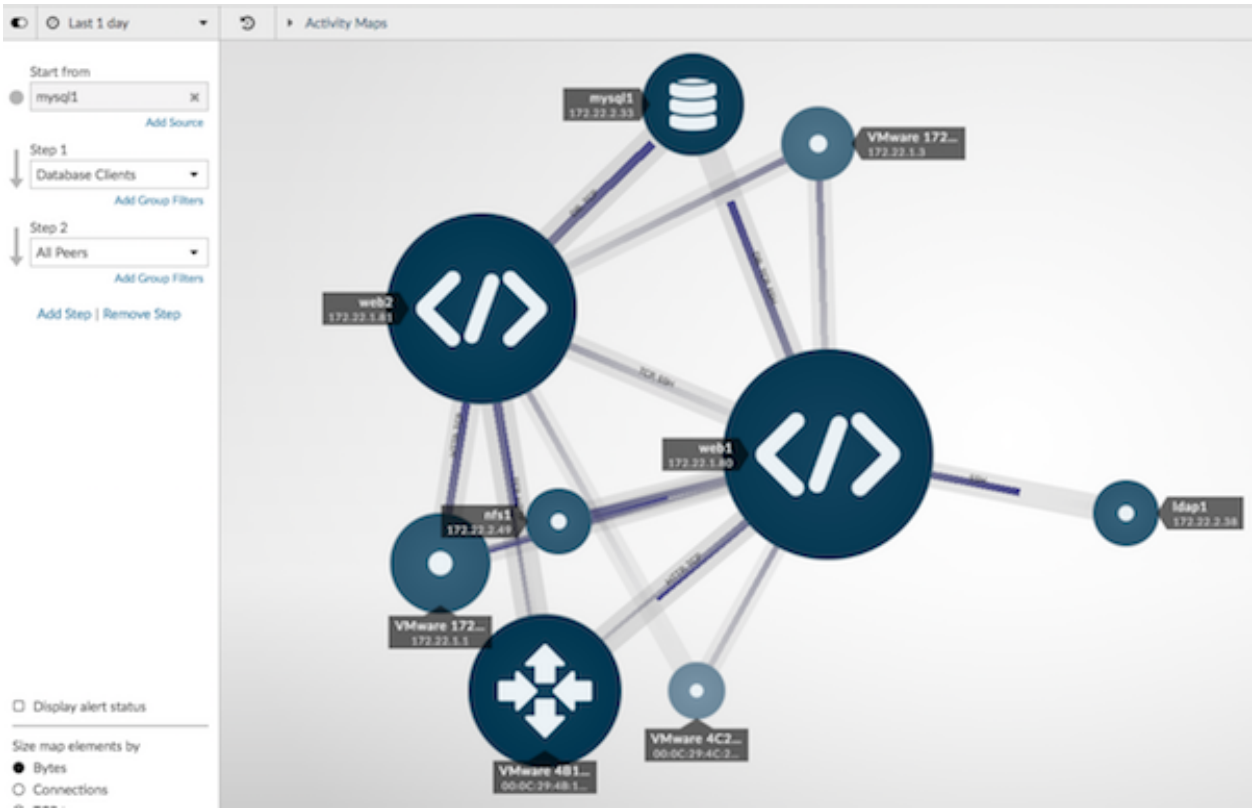


You can now interact with the activity map to learn more about the effect of the database errors across the network:

- Click any client in the map to access a menu that contains a Go to Device... link. Click the link to open a protocol page with client metrics, such as requests and responses.



- In the left pane below Step 1, click **Add Step** and then click **All Peers** in the drop-down list. The map updates to show you which downstream devices are connected to the database clients, as shown in the following figure.



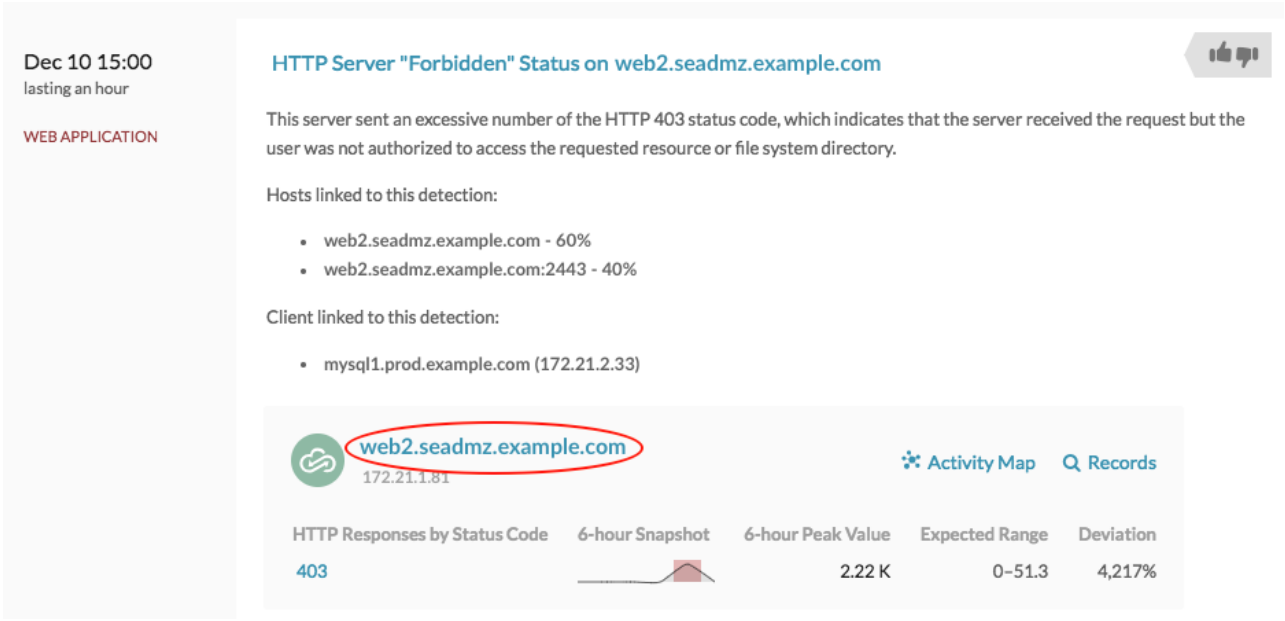
- Save and then share your activity map with other ExtraHop users.

For more information about activity maps, see Activity maps.

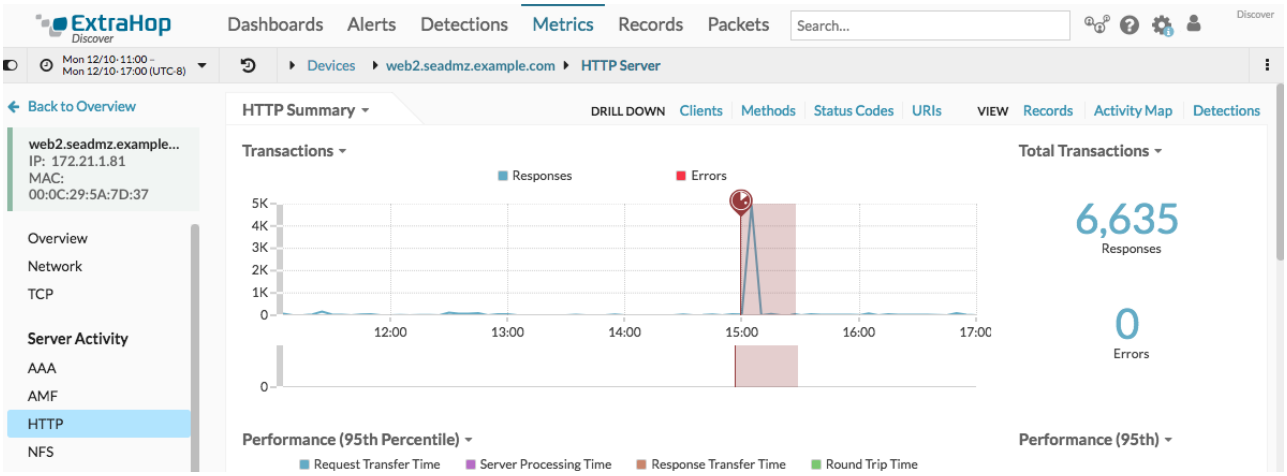
Navigate to a protocol page

If you want to further investigate anomalous metrics, you can navigate to a protocol page where you have access to additional charts, metrics, and tools.

1. Log into the Web UI on a Discover or Command appliance, and then click **Detections** at the top of the page.
2. Find the detection that you want to investigate.
3. Click the source name, as shown in the following figure.



The anomalous protocol page for the device or application appears, which displays all of metric data associated with that specific device or application during the detection time interval, as shown in the figure below.



Next steps

From a protocol page, you can then choose one of the following options to further investigate metric data:

- Create an activity map
- Drill down on metrics

Best practices for investigating detections

The Machine Learning Service provides you with high-quality, actionable data about detections—but does not replace decision-making or expertise about your network. The following best practices explain how to determine which detections are worth further investigation and when to take action.

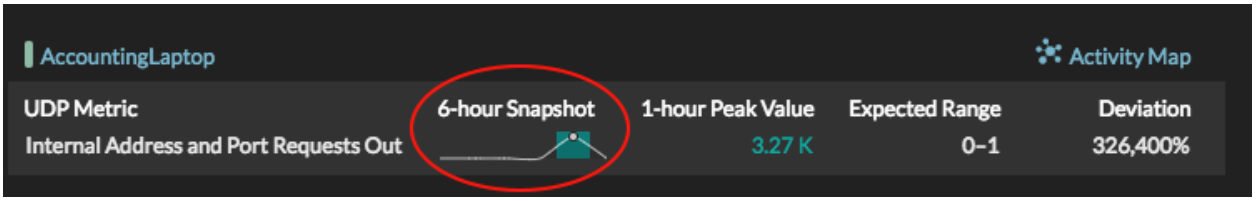
Change the time interval to see when detections occurred

Learn if detections occurred before, after, or during a reported problem. For example, does the time frame of the detection coincide with a reported issue, such as slow load times or login times? You can also compare detections from the past month to the current date, which gives you a sense of whether the occurrence or severity of detections is changing over time.

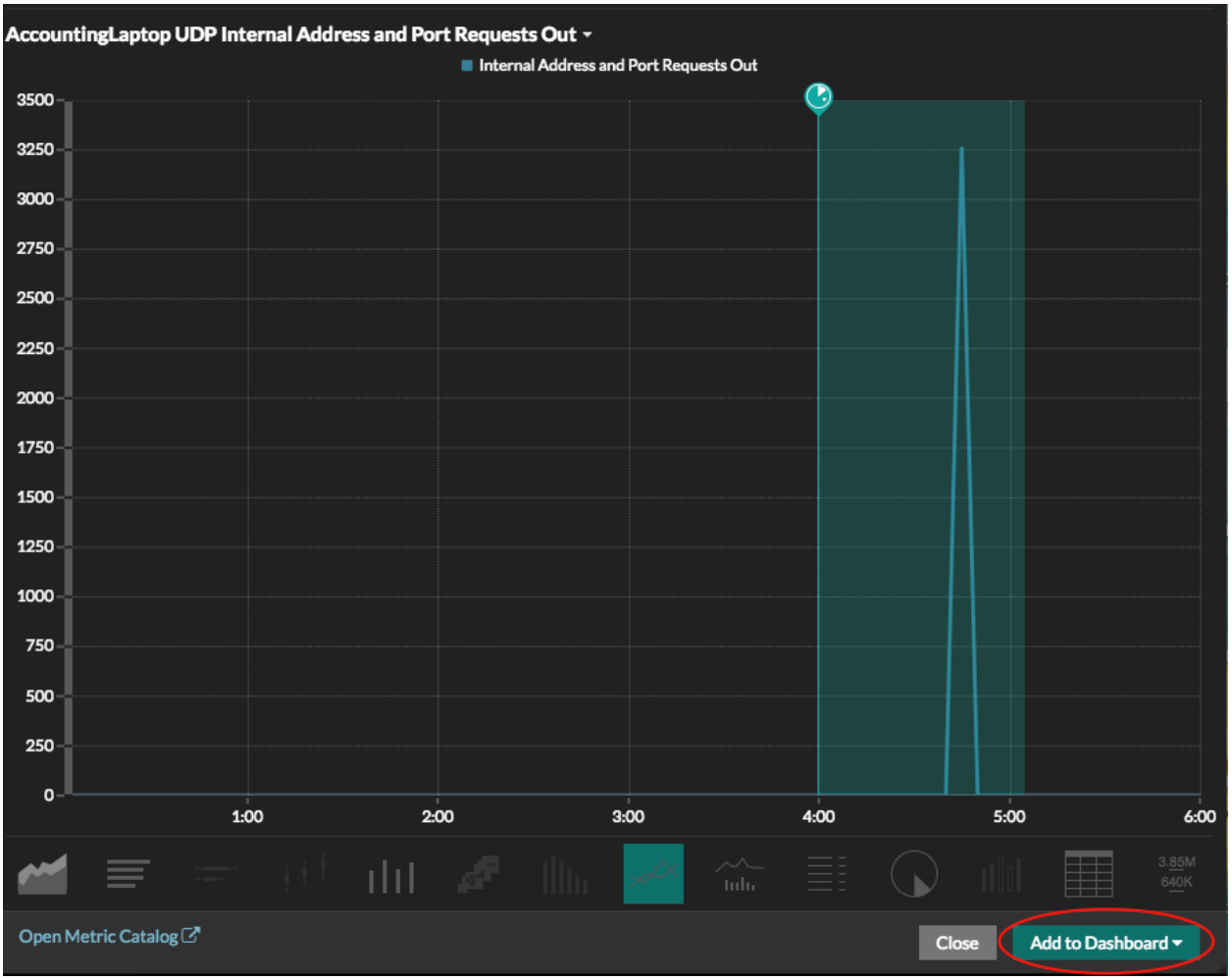
For more information, see Filter the detections list.

Monitor detection-related metrics in a dashboard chart

You can create and edit a dashboard chart from a detection. Click the sparkline, as shown in the following figure.



The detection source, metric, time interval, and drill-down details are preserved in the Metric Explorer so that you can quickly create a dashboard chart to monitor additional changes.



Create a detection alert

You can configure an alert to receive email notifications when a detection occurs. Detection alerts also help you quickly find detections for a specific device or application on the Alerts page page.

For more information, see Configure detection alert settings.