Investigate security detections

Published: 2020-02-23

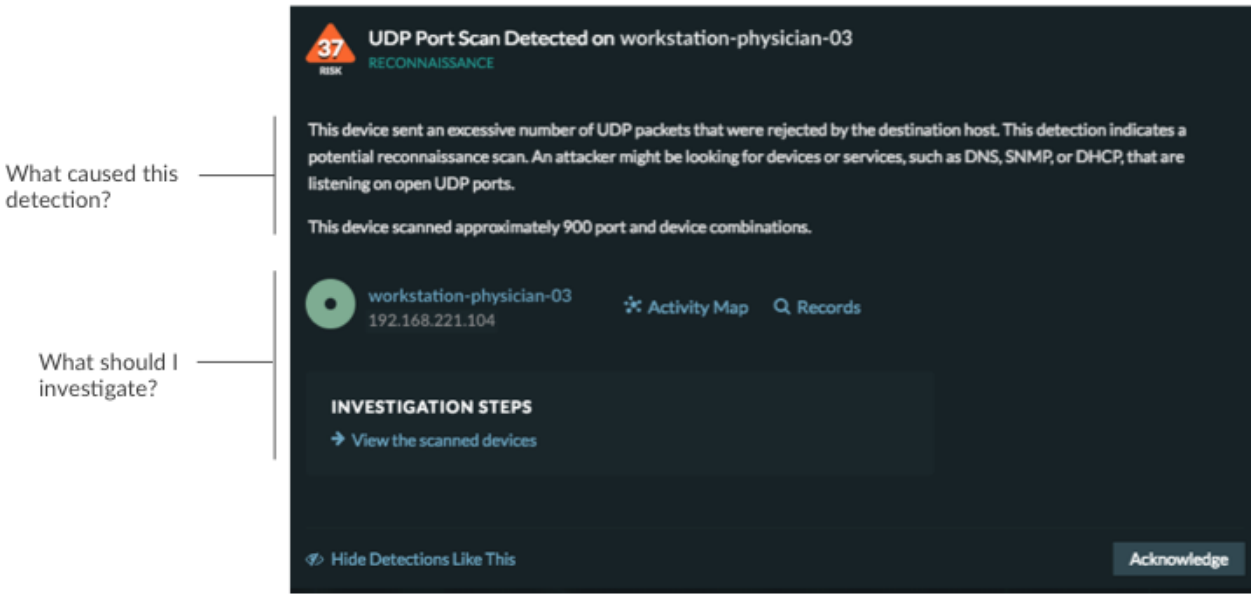
When an interesting detection appears, you should investigate whether the detected behavior points to a low-priority issue or a potential security risk. You can start your investigation directly from the detection card, which provides links to data across the ExtraHop system.

There are a number of tools that can help you filter your view to see the detections that you want to prioritize for investigation. Look for the following trends to get started:

- Did any detections occur at unusual or unexpected times, such as user-activity on weekends or after hours?
- Are any detections appearing in large clusters on the timeline?
- Are there detections appearing for critical assets or high-value endpoints?
- Are there detections that have high risk scores?

Start your investigation

Review the detection title and summary to learn what caused the detection.



Refine your investigation

A detection card includes several links to data within the ExtraHop system. The availability of these links depends on which devices and metrics are associated with the detection. Each link is described in the sections below.

Investigation Steps

Click a link in the Investigation Steps section to quickly view metrics, records, or packets that help answer the following types of questions:

- Which devices were scanned?

- Which server was targeted by the brute force attack?
- What type of data is being exfiltrated?

Each Investigation Step link is designed to answer a specific question. After clicking a link, you will navigate to either a detail metric page, Records page, or Packets page that contains relevant data. For example, if you get a DNS tunnel detection, you can learn about the content of each suspicious DNS host query that was exchanged with a potential command and control server.

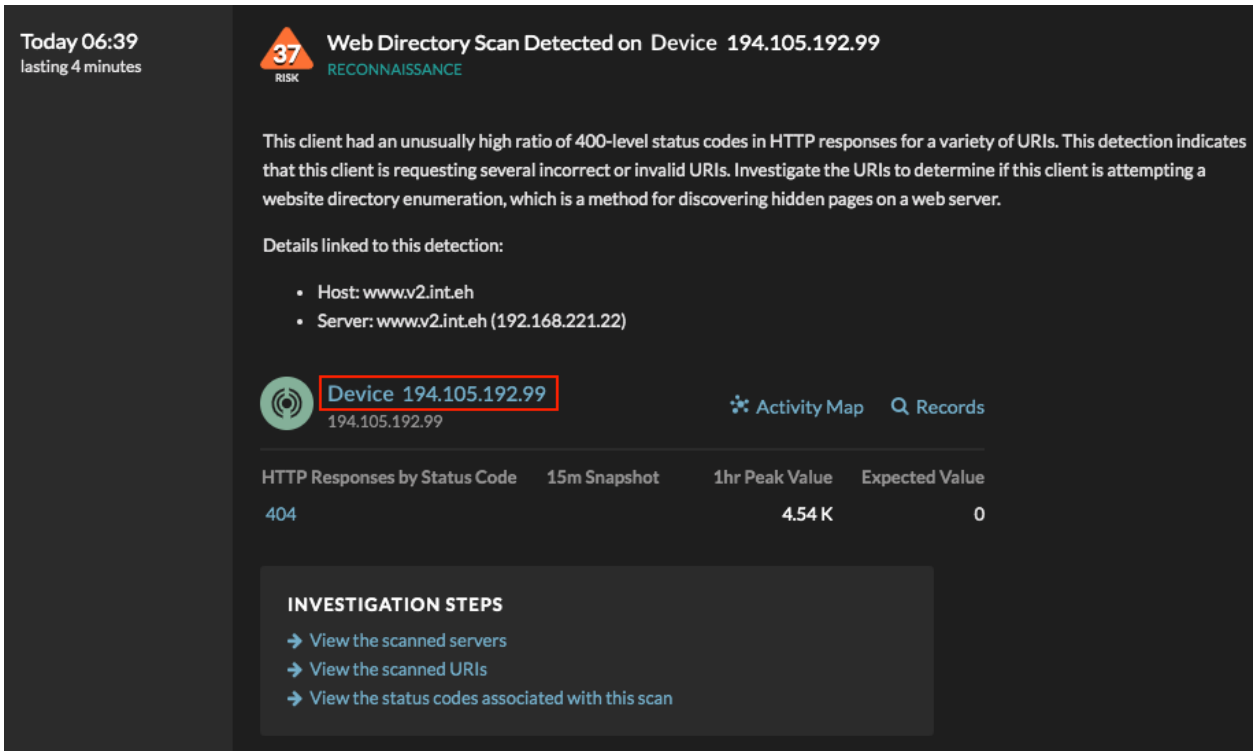
Availability

Because Investigation Step links are tailored to each detection, the number and type of these links vary in availability. In addition, links to records or packets are only available when you have a connected Explore or Trace appliance.

Device name

Click a device name to navigate to a protocol page, which contains all of the protocol metrics associated with the device. A protocol page gives you a complete picture of what the device was doing at the time of the detection. Click **Overview** in the left pane to see the role, users, and tags associated with the device.

For example, if you get a reconnaissance scan detection, you can learn if the device associated with the scan is assigned the Vulnerability Scanner role.

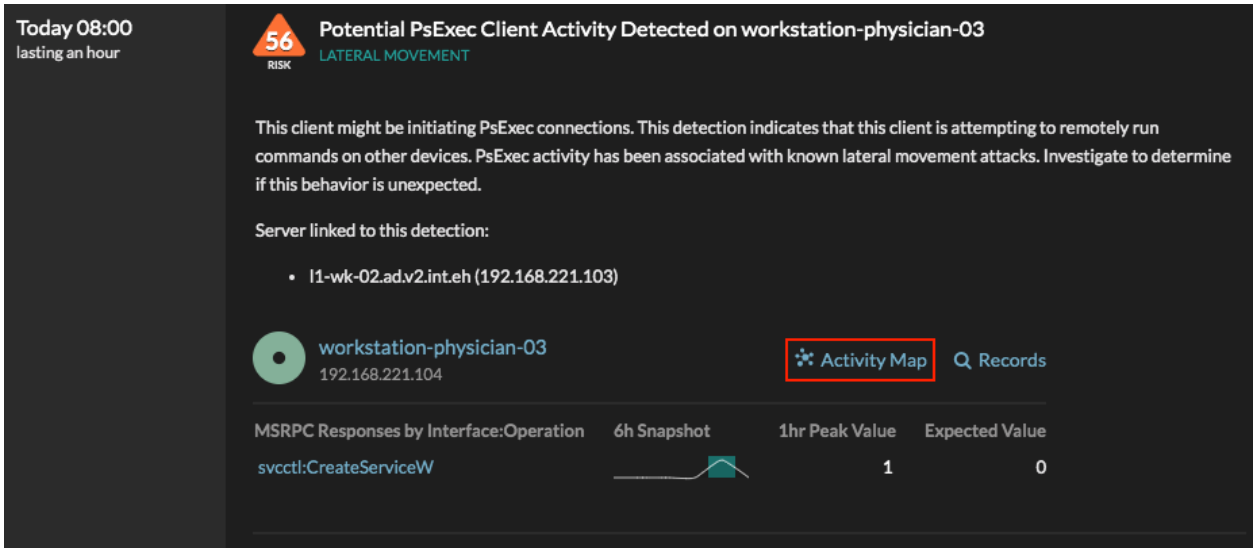


Availability

Device name links are only available for devices that have been automatically discovered by the ExtraHop system. Remote devices that are located outside of your network are represented by their IP addresses.

Activity map

Click **Activity Map** to see device connections by protocol during the time of the detection. For example, if you get a lateral movement detection, you can learn if the suspicious device established connections over a remote control protocol with other clients, IT servers, or domain controllers on your network.

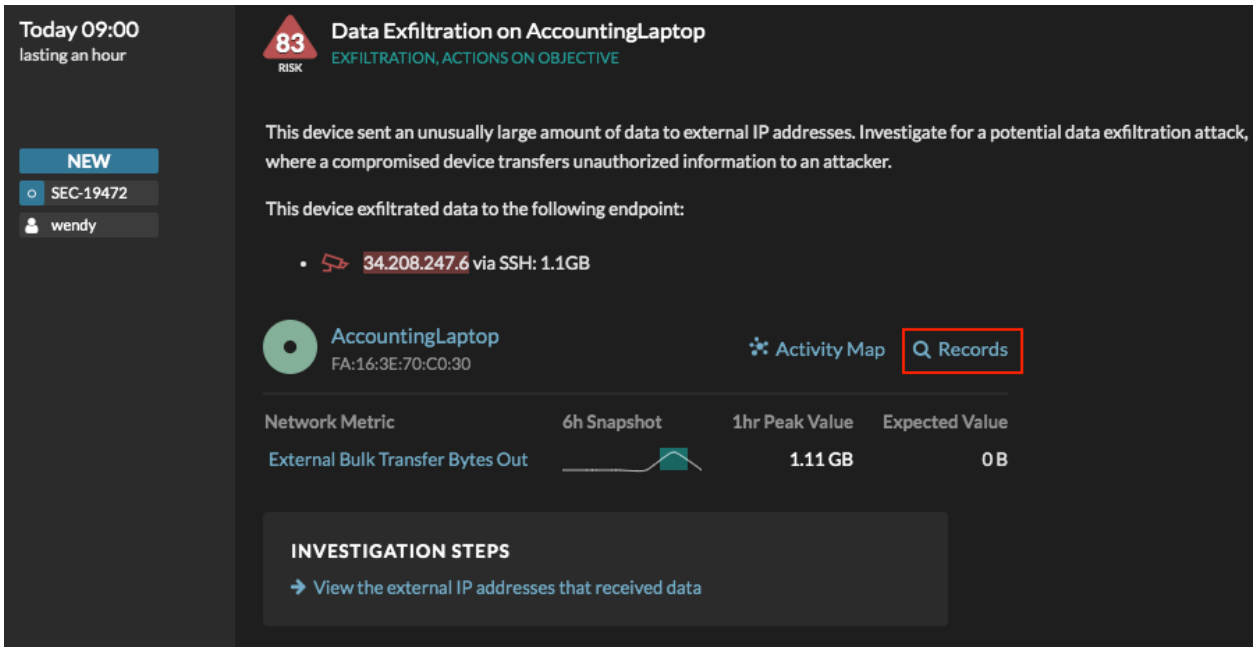


Availability

An activity map is available 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.

Records

Click **Records** to navigate to a Records page, which includes structured information about client-server transactions within customizable fields. For example, if you get a data exfiltration detection, you can learn about the type of data that was transferred to an external endpoint during the detection.

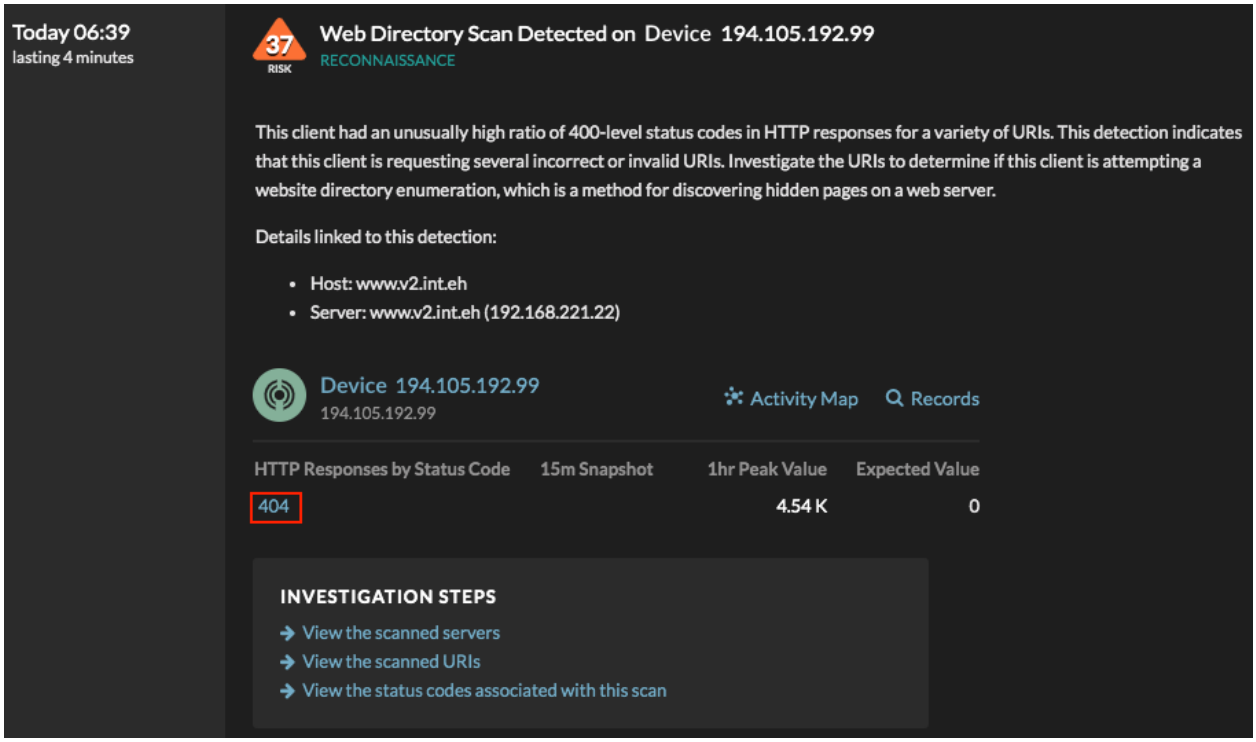


Availability

Records are available when you have a connected Explore appliance.

Detail metric drill down

Click a detail metric link to drill down on a metric value. A detail metric page appears, which lists metric values by a key, such as client IP address, server IP address, method, or error. For example, if you get a reconnaissance scan detection, drill down to learn which client IP addresses were associated with the unusually high number of 404 status codes during the detection.

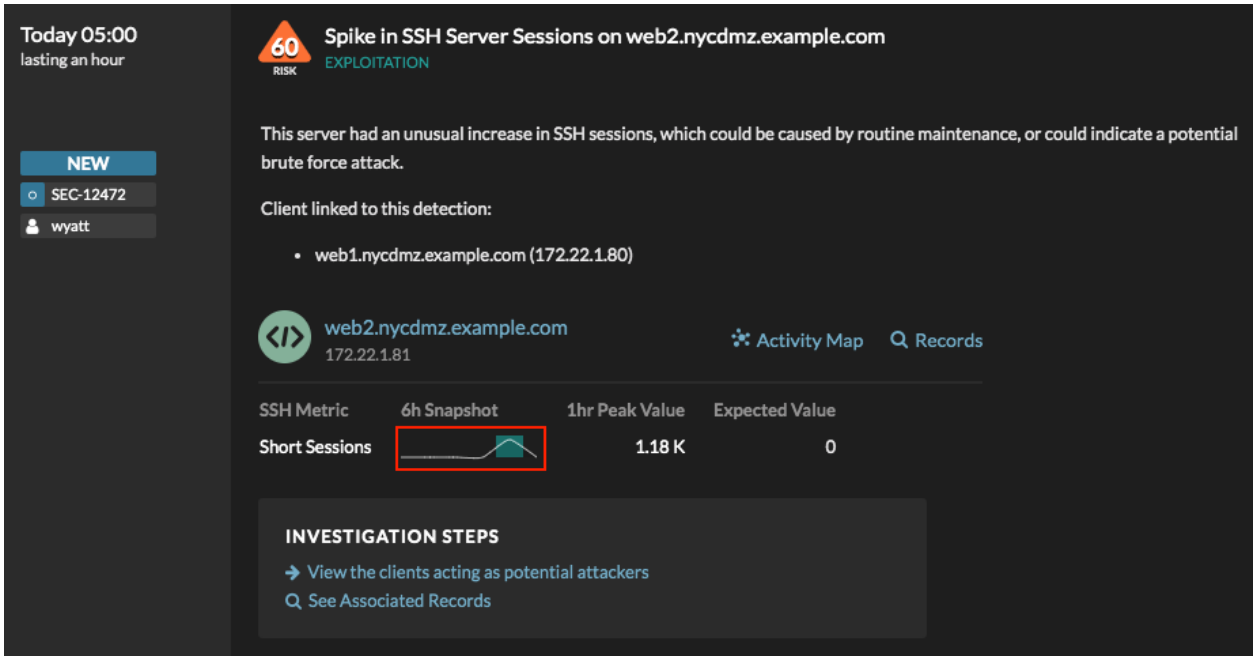


Availability

The drill-down option is available for detections associated with topnset detail metrics.

Sparkline

Click the sparkline to create a chart that includes the source, time interval, and drill-down details from the detection, which you can then add to a dashboard for monitoring. For example, if you get a detection about an unusual number of remote sessions, create a chart with SSH sessions for that server and then add that chart to a dashboard about session management.



Availability

The sparkline option is available for detections that were associated with metrics and had a duration over one-hour. For 1-second metrics, a sparkline is available when the duration was over 30-seconds.