Security overview concepts

Published: 2018-07-09

The Security Overview page enables you to quickly evaluate the scope and importance of security risks and to launch investigations into any suspicious activity. To mitigate security threats, you must first be able to detect risks—preferably as early in the attack as possible. Reveal(x) analyzes wire data in real-time and provides definitive information to manage escalations and incident reports.

Note: This topic applies only to ExtraHop Reveal(x).

From the Security Overview page, you can answer the following questions:

What are the most important risks right now?

Security detections are ranked by highest risk score, so you can quickly determine the severity of a security issue.

What devices should I focus on?

At the top of the page, security detections are listed by asset, so you can immediately focus on a specific device or application for your investigation. At the bottom of the page, signal metrics highlight changes in security-related activity. Click the metric title to identify the clients and servers that are contributing to suspicious activity.

What are devices on the network doing?

Rotating activity maps provide a high-level view of device activity for a specific protocol. If the map is hidden by security detections, click anywhere on the page to show the map. Hover and click on a device in the map to learn more about its connections.

Note: To view metrics associated with threat intelligence data, click **Dashboards** at the top of the page, and then click **Security** to view the Security dashboard.

Navigate the Security Overview page

Important security information is presented as three unique types of information: detections, activity maps, and signal metrics. The Security Overview page refreshes activity map and signal metric data every minute. Detections are analyzed every 30 seconds or every hour, depending on the metric.

When there are no security detections found by Reveal(x) during the selected time interval, an activity map and signal metrics are provided, as shown in the following figure.

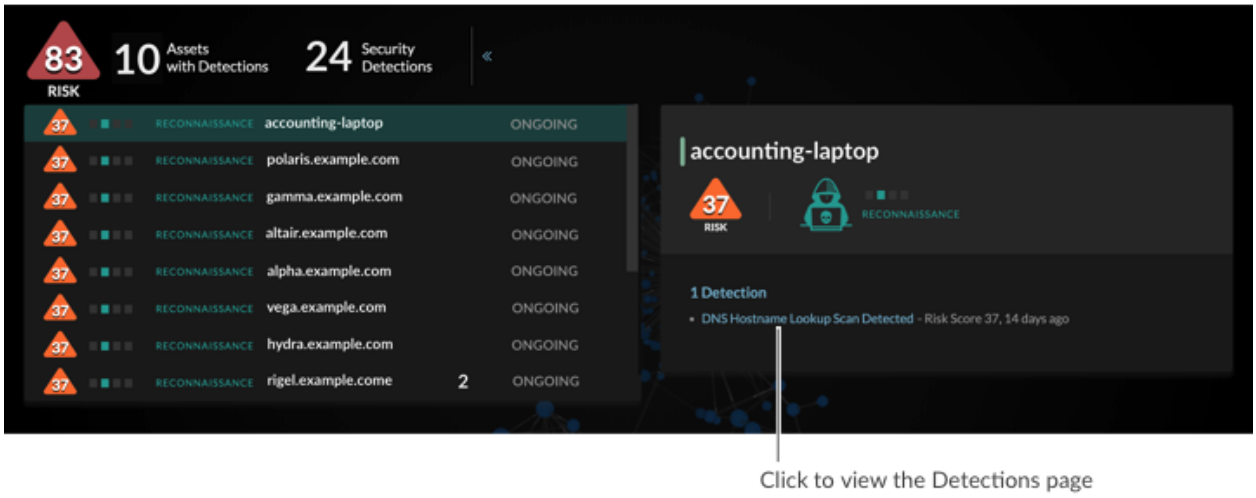
When there are security detections, information about the affected asset, attack chain, and risk score appears, as shown in the following figure.

Learn more about detections, activity maps, and signal metrics in the following sections.

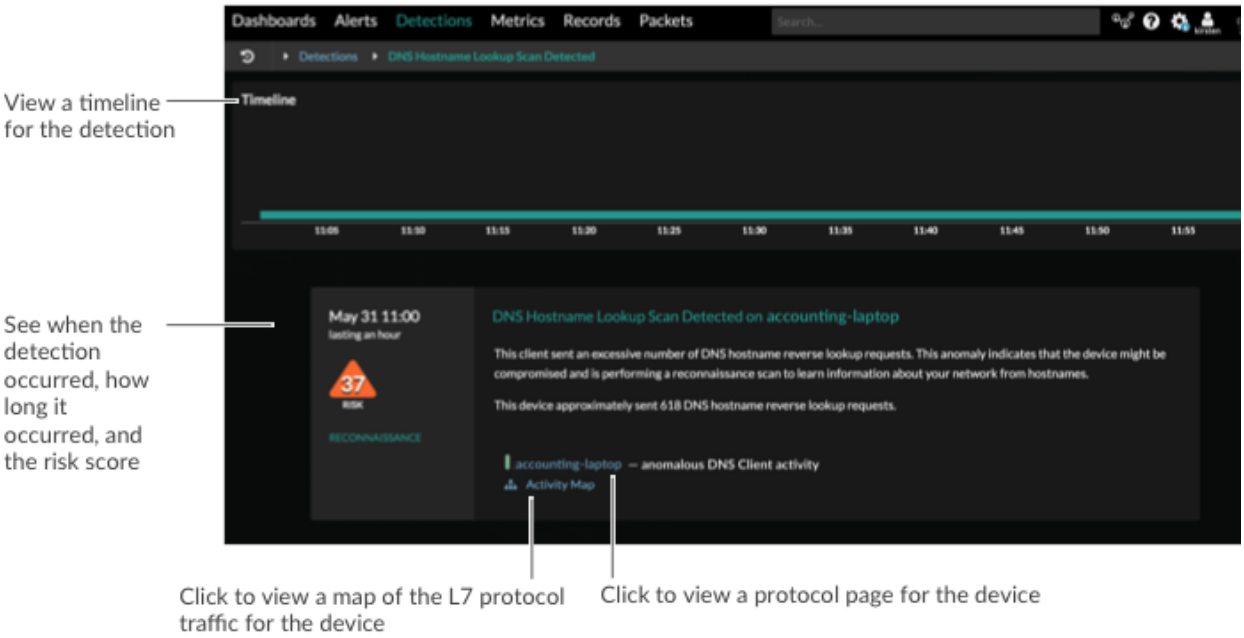
Security detections

Reveal(x) analyzes L2-L7 protocol activity from wire data and extracts every transaction on your network, including accessed files, database transactions, HTTP responses, DNS responses, and authentication requests. Reveal(x) then applies machine learning techniques to wire data to automatically detect unusual behavior associated with attack chain phases.

On the Security Overview page, each asset with a security detection is displayed on the left. Click an asset to view detection information on the right. Then click the detection title on the right, as shown in the following figure.



A Detections page appears with more information and investigation options, as shown in the following figure. You can then investigate and share detections.



Activity maps

On the Security Overview page, an activity map displays network traffic for a security-related protocol. The activity map rotates between the following protocols (if there is activity for that protocol) each minute:

- CIFS
- Database (DB)
- DNS
- FTP
- HTTP
- LDAP
- SSH
- SSL
- Telnet

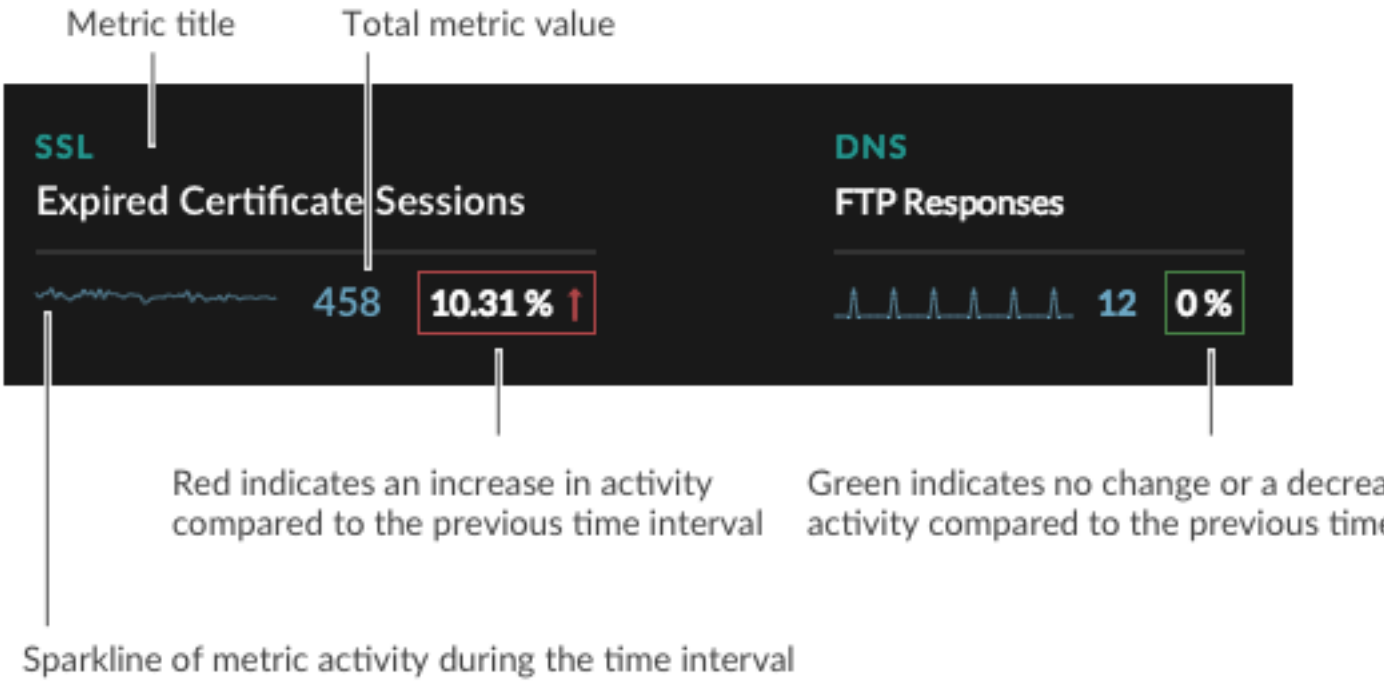
There are several ways to interact with the map to launch an investigation about a device connection.

- Click to rotate the map and scroll to zoom in.
- Hover over a circle to see device labels and highlight device connections.
- Click a circle and then click the device name to view a protocol page for the device.
- Click the protocol in the upper right corner of the page. An Activity Map page appears, where you can add steps and group filters to the map.

Signal metrics

Signal metrics provide information about changing network activity that is associated with potential attacks or vulnerabilities. For example, signal metrics can help you identify increases in vulnerable DNS queries or insecure SSL sessions.

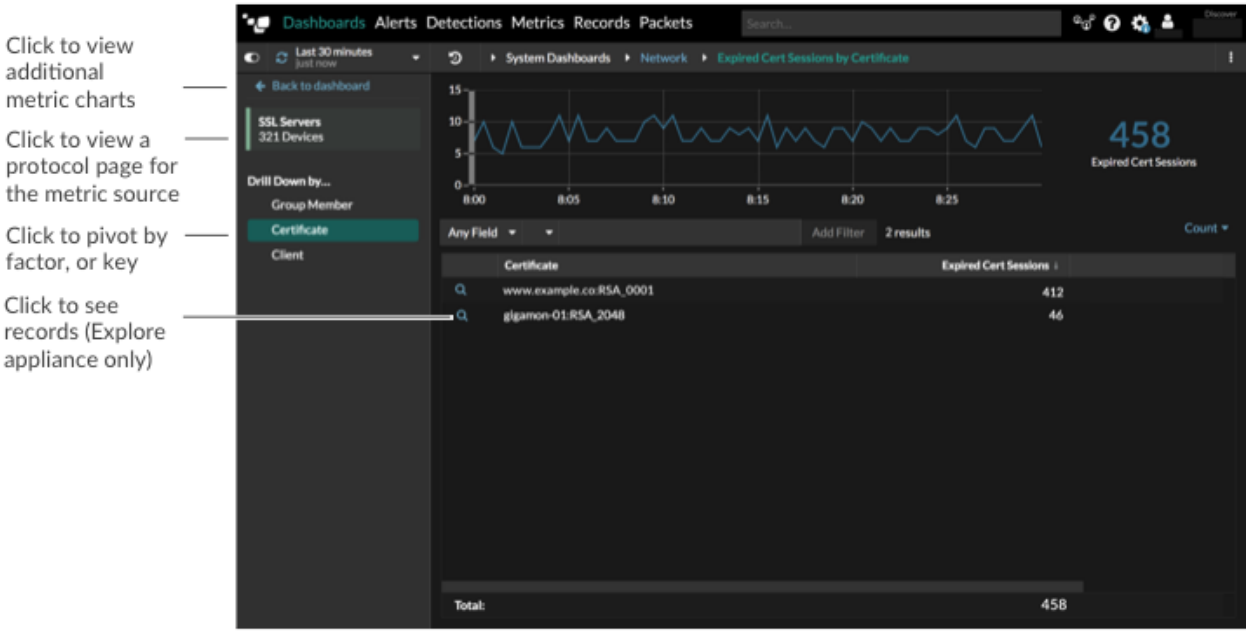
At the bottom of the Security Overview page, these metrics are dynamically displayed based on the amount of change in activity between the current and previous time interval. Metrics with the largest increase in change are displayed in descending order from left to right, as shown in the following figure.



The following list shows the set of signal metrics that can potentially appear on the Security Overview page:

- DNS - Request Timeouts
- DNS - FTP Responses
- DNS - Address Mapping Record Queries
- DNS - Text Record Queries
- HTTP - 404 Not Found Errors
- HTTP - 500 Server Errors
- SSL - Self-signed Sessions
- SSL - Weak Cipher Sessions
- SSL - Expired Certificate Sessions
- SSL - Insecure SSLv3 Protocol Sessions
- SSL - Insecure TLSv1.0 Protocol Sessions

You can launch an investigation into interesting data by clicking the metric title to drill down to a detail page that contains detail metrics. You can then investigate which factors are contributing to the activity, as shown in the following figure.



Related topics

Check out the following resources for more information about Reveal(x) security concepts.

- Threat intelligence concepts
- Security detections and Detections concepts
- Security dashboard