Security Overview - Reveal(x) only

Published: 2020-02-23

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.

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.

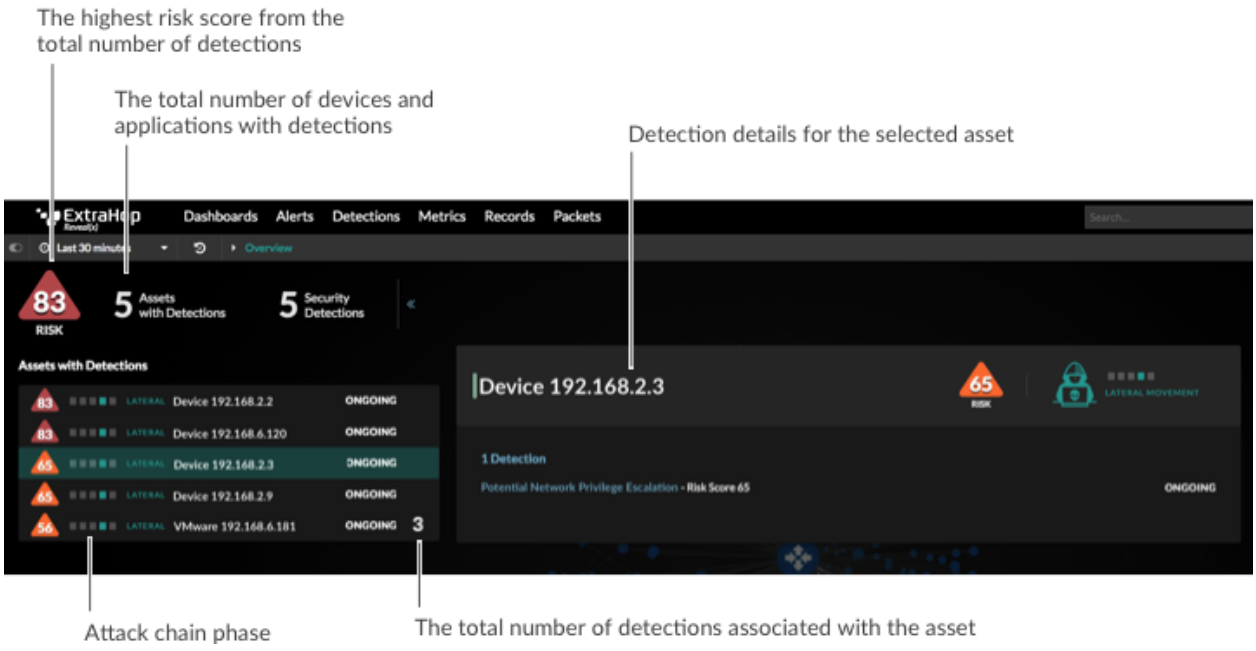
Note: To view metrics associated with threat intelligence data, click **Dashboards** at the top of the page, and then click **Security** to view the Security dashboard. (ExtraHop Reveal(x) Premium and Ultra only)

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.

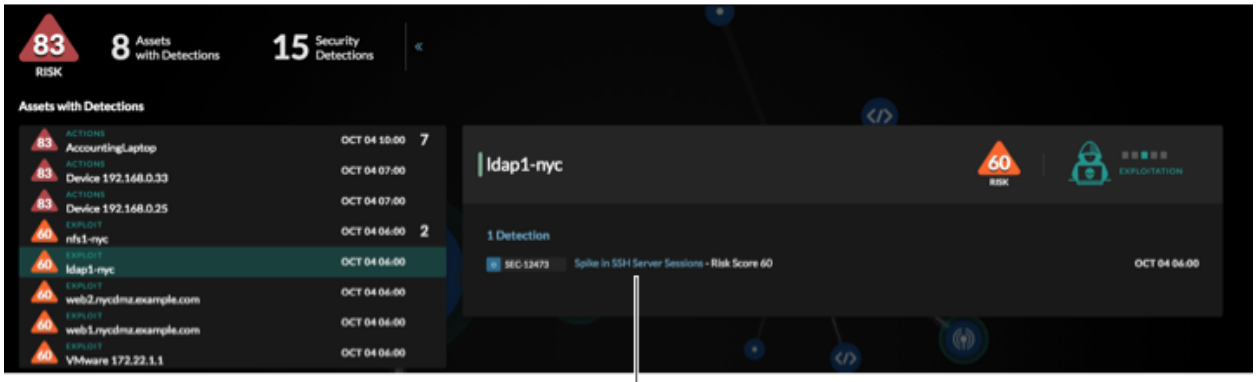


Learn more about detections, activity maps, and signal metrics in the following sections.

Security detections

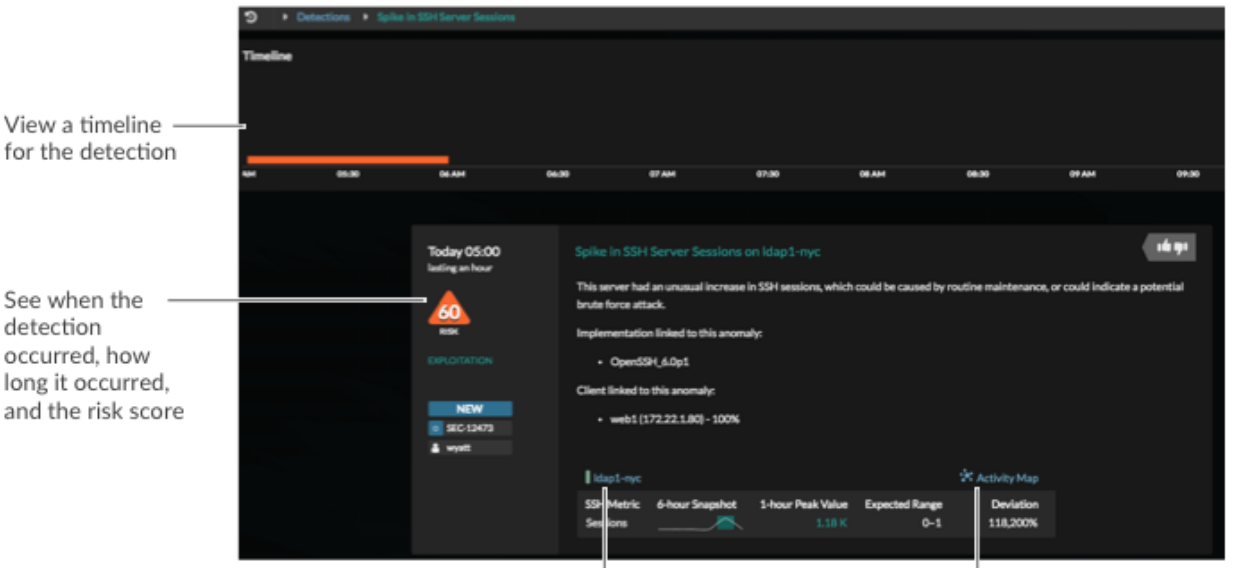
Reveal(x) analyzes L2-L7 protocol activity from wire data and extracts every transaction on your network, including accessed files, database transactions, HTTP responses, DNS responses, and authentication requests. Reveal(x) then applies machine learning techniques to wire data to automatically detect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



Click to view the Detections page

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



Click to view a protocol page for the device

Click to view a map of the L7 protocol traffic for the device

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.

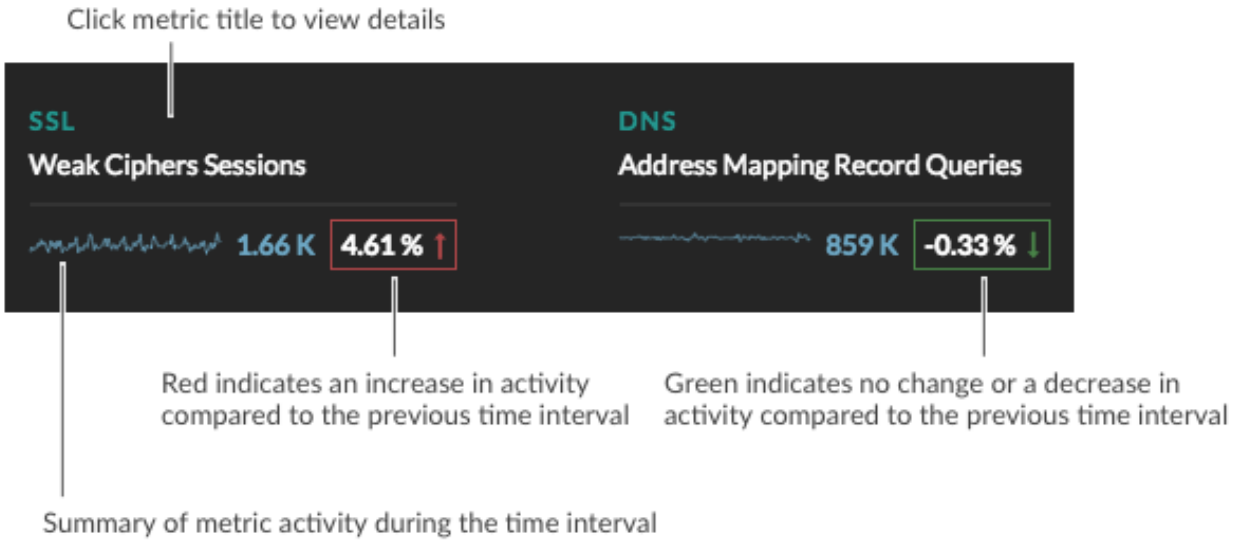
- Click to rotate the map and scroll to zoom in.
- Hover over a circle to see device labels and highlight device connections.
- Click a circle and then click the device name to view a protocol page for the device.
- Click the protocol in the upper right corner of the page. An Activity Map page appears,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

Signal metrics

Signal metrics are security-relevant metrics that indicate weaknesses in network security or potentially suspicious activity. While detections show you specific instances of unusual behavior, signal metrics show you general trends related to network security health.

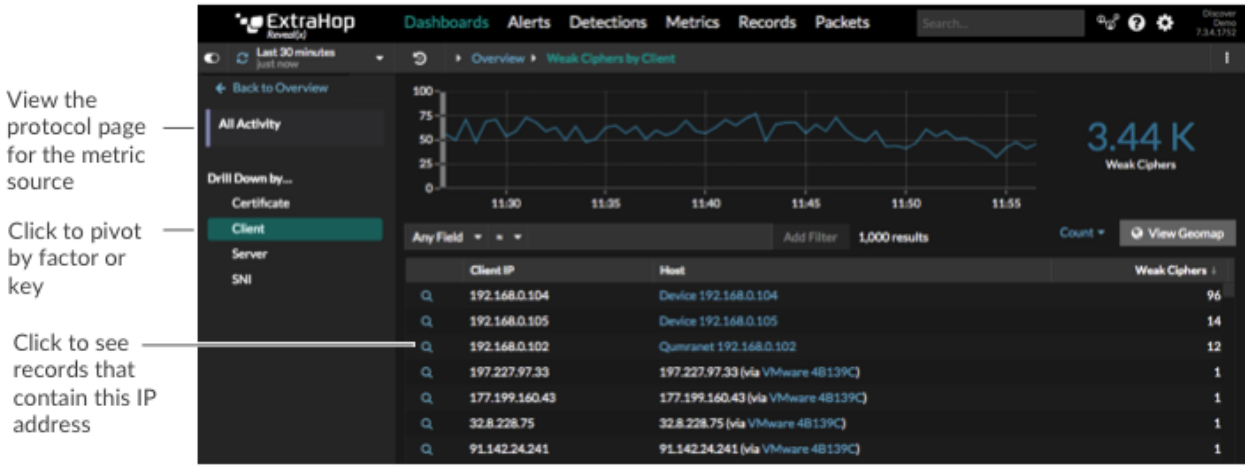
Signal metrics are dynamically displayed at the bottom of the Security Overview page. Metrics with the largest increase in change are listed in descending order from left to right, as shown in the following figure.

Next to each signal metric, you can see the percentage of change in network activity compared to a previous time interval.



Depending on the type of network activity and the amount of change, you can launch an investigation by clicking the metric title to drill down to a detail page. You can then investigate which factors are contributing to the activity.

For example, click the title, such as Weak Ciphers Sessions. A detail page appears with all the clients, servers, certificates, and SNIs that were associated with weak cipher sessions, as shown in the following figure.



The following signal metrics can appear on the Security Overview page.

DNS - Address Mapping Record Queries

This signal metric shows you the number of DNS requests received by DNS servers that included the A record type. An A record maps a domain name to the IP address (IPv4) of the domain host. Click the metric title to see which clients sent the most requests.

Why is this metric a security health indicator?

While DNS address mapping queries are normal, large or sudden increases can be an indicator of potential data exfiltration or a DNS tunnel. A DNS tunnel is a technique that encodes data into DNS queries for data exfiltration or command and control attacks. For example, sensitive data can be encoded into the hostname within the A record. You can view the A record by clicking the records icon next to a client that sent a high number of DNS requests.

DNS - FTP Responses

This signal metric shows you the number of FTP responses sent by DNS servers. Click the metric title to see which servers sent the highest number of FTP responses.

Why is this metric a security health indicator?

The primary activity for DNS servers should be to resolve hostnames instead of sending files over FTP. Attackers can exploit weaknesses in DNS servers, which often go undetected. If there is an increasing number of FTP data transfer by DNS servers, investigate this suspicious activity.

DNS - Request Timeouts

This signal metric shows you the number of timeouts that occurred after repeated unanswered DNS query requests were sent from clients. Click the metric title to see which clients were affected and which servers were not responding.

Why is this metric a security health indicator?

DNS can be a bottleneck in your network if hostname resolution cannot take place. A spike, or large increase in request timeouts, is disruptive to your network in general, and can also be an indicator of a distributed denial of service (DDoS).

DNS - Requests with Suspicious Hosts

This signal metric shows you the number of DNS requests that included a suspicious hostname, based on threat intelligence information uploaded to the ExtraHop system. Click the metric title to see which hosts are considered suspicious. Click the red camera icon to see related threat intelligence details about the hostname.

Why is this metric a security health indicator?

Threat intelligence information includes indicators of compromise from several types of known security attacks. Because threat intelligence is curated by a community of security professionals, there are many sources of information that can vary in quality or relevance to your environment. Any DNS request associated with threat intelligence information should be investigated. You can view information about the entire DNS transaction by clicking the records icon next to a suspicious host query.

DNS - Text Record Queries

This signal metric shows you the number of DNS requests received by DNS servers that included the TXT record type. A TXT record associates human-readable text with a host. Click the metric title to see which client sent the most DNS requests with the TXT record type.

Why is this metric a security health indicator?

DNS queries that include TXT records are typically uncommon, and large increases can be an indicator of a potential DNS tunnel. A DNS tunnel is a technique that encodes data into DNS queries for data exfiltration or command and control attacks. For example, malware or sensitive data can be encoded into the TXT record. You can view the TXT record by clicking the records icon next to a client that sent a high number of DNS requests.

HTTP - 404 Not Found Error

This signal metric shows you the number of HTTP responses that included the 404 (Not Found) status code. Click the metric title to see which URIs were associated with the 404 status code.

Why is this metric a security health indicator?

While a certain number of 404 errors might be considered normal, a large increase in this client-side error could indicate a potential web directory scan. Attackers rely on information about the underlying web server and associated components that are returned in the HTTP 404 status code.

HTTP - 500 Server Errors

This signal metric shows you the number of HTTP responses sent by servers that contained the 500 (Server Error) status code. Click the metric title to see which URIs were associated with the 500 status code.

Why is this metric a security health indicator?

A large or sudden increase in this server-side error could indicate a potential web directory scan. Web penetration tools deployed by attackers rely on information about the underlying web server and associated components that are returned in the HTTP 500 status code.

HTTP - Requests with Suspicious Hosts

This signal metric shows you the number of HTTP requests that included a suspicious hostname, based on threat intelligence information uploaded to the ExtraHop system. Click the metric title to see which hosts are considered suspicious. Click the red camera icon to see related threat intelligence details about the host.

Why is this metric a security health indicator?

Threat intelligence information includes indicators of compromise from several types of known security attacks. Because threat intelligence is curated by a community of security professionals, there are many sources of information that can vary in quality or relevance to your environment. Any HTTP request associated with threat intelligence information should be investigated. You can view information about the entire HTTP transaction by clicking the records icon next to a suspicious host.

HTTP - Requests with Suspicious URIs

This signal metric shows you the number of HTTP requests that included a suspicious URI, based on threat intelligence information uploaded to the ExtraHop system. Click the metric title to see which URIs are considered suspicious. Click the red camera icon to see related threat intelligence details about the URI.

Why is this metric a security health indicator?

Threat intelligence information includes indicators of compromise from several types of known security attacks. Because threat intelligence is curated by a community of security professionals, there are many sources of information that can vary in quality or relevance to your environment. Any HTTP request associated with threat intelligence information should be investigated. You can view information about the entire HTTP transaction by clicking the records icon next to a suspicious URI.

SSL - Expired Certificate Sessions

This signal metric shows you the number of TLS/SSL sessions that were established with an expired certificate. Click the metric title to see which expired certificates had the most sessions.

Why is this metric a security health indicator?

Certificate authorities add expiration dates to certificates, which are required for establishing a secure TLS or SSL session. Sessions established with expired certificates could indicate that servers have certificate verification disabled, or that users ignored browser warnings when establishing the session. This type of activity increases the vulnerability of devices to man-in-the-middle attacks. Consider configuring your web servers to remove expired certificates.

SSL - Insecure SSLv3 Protocol Sessions

This signal metric tells you the number of connections on your network that were established with SSL version 3.0. Click the metric title to see a list of servers and clients with SSLv3 sessions.

Why is this metric a security health indicator?

Known vulnerabilities, such as BEAST and POODLE, are associated with SSLv3. If you have a high number of SSLv3 sessions, consider configuring servers to support the latest version of TLS.

SSL - Insecure TLS 1.0 Protocol Sessions

This signal metric tells you the number of connections on your network that were established with TLS version 1.0. Click the metric title to see a list of servers and clients with TLS 1.0 sessions.

Why is this metric a security health indicator?

Known vulnerabilities, such as BEAST and POODLE, are associated with TLS 1.0. If you have a high number of TLS 1.0 sessions, consider configuring servers to support the latest version of TLS.

SSL - Self-signed Sessions

This signal metric shows you the number of TLS/SSL sessions that were established with self-signed certificates. Click the metric title to see which clients were associated with self-signed certificate sessions.

Why is this metric a security health indicator?

Self-signed certificates are not issued or verified by a certificate authority. The presence of self-signed certificates might indicate that software on your systems is not validating certificates, making your network vulnerable to man-in-the-middle attacks. A sudden or large increase in sessions with self-signed certificates could also indicate that an attacker is communicating with command and control servers.

SSL - Weak Cipher Sessions

This signal metric shows you the number of the number of TLS/SSL sessions that were established with weak ciphers. Click the metric title to see which clients are associated with weak ciphers.

Why is this metric a security health indicator?

A cipher suite is a set of encryption algorithms that help secure a TLS/SSL connection. Algorithms within a cipher suite that are associated with known vulnerabilities are considered weak. You can view the cipher suite by clicking the records icon next to a client. Consider configuring your web servers to remove weak ciphers.

TCP - Suspicious TCP Connections

This signal metric shows you the number of the number of outbound connections to suspicious IP addresses, based on threat intelligence information uploaded to the ExtraHop system. Click the metric title to see which IP addresses are considered suspicious. Click the red camera icon to see related threat intelligence details about the IP address.

Why is this metric a security health indicator?

Threat intelligence information includes indicators of compromise from several types of known security attacks. Because threat intelligence is curated by a community of security professionals, there are many sources of information that can vary in quality or relevance to your environment. Any device connection with a known suspicious IP address should be investigated.

Related topics

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

- Threat intelligence - Reveal(x) only
- Security detections (Reveal(x) only) and Detections
- Security dashboard - Reveal(x) only