Detections FAQ

Published: 2025-01-29

Here are some answers to frequently asked questions about detections.

- How are detections different from alerts?
- What is a risk score?
- Why can't I view source device details for a detection?
- How far back are detections found?
- Can I connect to the Machine Learning Service through a proxy?
- What data is sent from the ExtraHop system to the Machine Learning Service?
- How secure are detections?
- How do I add a new or updated license for the Machine Learning Service to my ExtraHop system?
- Why am I not receiving certain machine learning detections?
- After my Machine Learning Service license expires, can I still view my previous detections?

How are detections different from alerts?

Alerts ⧉ and detections are similar in that they both provide information about conditions on your network. The following table describes how they differ. Alerts provide Configured alert conditions determine when an alert is generated.

	Alerts	Detections
How are they generated?	By conditions you define through Alert settings. You can configure trend or threshold alerts.	Automatically observed from your network data by the ExtraHop Machine Learning Service.
How do I view them?	Click **Alerts** from the top menu of the ExtraHop system.	Click **Detections** from the top menu of the ExtraHop system.
How do I set up email notifications?	You can add a notification to an alert configuration ⧉ to send emails when alert conditions are met.	You can create a notification rule ⧉ to send emails about detections that match specific criteria.
What are the benefits?	You decide which high-priority devices and services to monitor and determine the level of change that generates notification.	Notable changes to your network behavior are automatically surfaced. By providing feedback for detections, you help the Machine Learning Service algorithm better understand your network.

What is a risk score? (ExtraHop RevealX only)

A risk score ⧉ indicates the severity of a detection and is calculated based on the likelihood of an attack, the difficulty of exploiting the detection, and the level of impact to your operations.

Risk scores are grouped into one of the following color-coded severity levels:

- Red = 80-99
- Orange = 31-79
- Yellow = 1-30

No risk score is displayed for an individual detection if a score has not been evaluated and defined for that detection.

Why can't I view source device details for a detection?

If the source of a detection is a device that hasn't been discovered by the ExtraHop system, the detection only shows the IP address and hostname of the device, if available. You can hover over the undiscovered device to see the geolocation of the IP address and a link to the ARIN Whois website.

Why don't I see user information for a detection participant?

Detections can only display the username associated with a participant if the detection is associated with a protocol that contains a username. The ExtraHop system can observe usernames in the following protocols: FTP, Kerberos, LDAP, NTLM, RDP, RPC, and SMB.

How far back are detections found?

Machine-learning detections are identified one week back from the time the service is connected. The service then identifies all new detections moving forward.

Note that the Machine Learning Service requires four weeks (28 days) of data to calculate an expected range of metric values. The expected range represents normal network behavior. Data processing is typically completed within a few hours.

Can I connect to the Machine Learning Service through a proxy?

The Machine Learning Service supports implicit and explicit proxies. The proxy requires that DNS resolve all *.extrahop.com domains, and the outbound 443 port is open to all IP addresses on the internet. These settings are implemented on the firewall for the proxy's source IP address.

For more information on configuring an explicit proxy, see Connect to ExtraHop Cloud Services through a proxy ⤤.

What data is sent from the ExtraHop system to the Machine Learning Service?

The Machine Learning Service takes advantage of the unique processing capabilities of the ExtraHop system to "pre-process" wire data for hundreds of metrics on-premise. The ExtraHop system encrypts metric values and IP addresses that are sent to the Machine Learning Service. The ExtraHop system does not send custom metrics or sensitive data such as file names, strings, or payloads.

How secure are detections?

Detections are designed to be secure from end-to-end. Unlike a typical SaaS solution, detections do not ingest payloads, file names, strings, or other data categories that might contain sensitive information. ExtraHop has obtained SOC 2 Type 2 and SOC 3 compliance certification for all online services, and these certifications are performed yearly.

How do I add a new or updated license for the Machine Learning Service to my ExtraHop system?

If you purchased a new ExtraHop system that includes a license for the Machine Learning Service, you will receive an email with a new product key. Follow the instructions to register your appliance ⤤.

If you have added a license for the Machine Learning Service, your updated license is automatically added to your ExtraHop system, but must still be applied. Follow the instructions to apply an updated license ⤤.

Why am I not receiving certain machine learning detections?

The Machine Learning Service supports versions of the ExtraHop firmware for approximately 15 months after the firmware is released. If you do not upgrade your ExtraHop firmware for over 15 months, you might not receive the latest updated and new detections from the Machine Learning Service. Contact ExtraHop Support for assistance with a firmware upgrade by creating a case on the Customer Portal ⤤ (requires login).

After my Machine Learning Service license expires, can I still view my previous detections?

Yes, previous detections remain available in your ExtraHop system.