Detections FAQ

Published: 2020-02-23

Here are some answers to frequently asked questions about detections.

Note: This topic applies to all ExtraHop systems, including ExtraHop Reveal(x).

Note: Detections require a connection to the cloud-based ExtraHop Machine Learning Service.

How are detections identified?

After you connect to the ExtraHop Machine Learning Service, the ExtraHop system automatically applies machine learning technology to your wire data. The historical data stored on the appliance is analyzed to calculate a range of expected network and user behavior that spans hundreds of metrics and several protocols.

Normal values for both security and performance detections are determined through a suite of proprietary algorithms and models that combine time series decomposition, unsupervised learning, heuristics, and domain expertise to evaluate data. As deviations are identified from the expected data range of metric values over time, the algorithm becomes more sensitive to changing network traffic patterns and detections become increasingly accurate.

In addition to machine-learning detections, detections can be identified through triggers. Triggers for rules-based detections are authored by ExtraHop, but you can write a trigger to create a custom detection that identifies specific environment variables.

How quickly can a detection be identified?

The Machine Learning Service analyzes data for detections every 30 seconds or every hour, depending on the metric. Identified detections are sent from the cloud-based service to the ExtraHop system within minutes.

After connecting to the Machine Learning Service, the amount of historical data required to identify detections depends on the type of detection and the behavior identified.

Some security detections can be identified with one hour of historical data. For example, your appliance can immediately search for potentially risky behavior on your network, such as a new SSH connection to an external endpoint or communication with an external endpoint on a non-standard HTTP port. The service intelligently determines whether there is enough historical data to accurately analyze each security detection, and continues to identify more security detections as data is collected each week.

Performance detections require two weeks of historical data to calculate a range of expected network and user behavior that spans hundreds of metrics and several protocols.

What type of detections are identified?

Detections are unusual deviations from normal network behavior or notable activity in your environment. Depending on your ExtraHop subscription, detections surface either security risks or performance issues.

Security detections identify the following types of risks:

- Command and control activity
- Brute force attacks
- Reconnaissance activity
- Ransomware activity
- Botnet activity
- Cryptocurrency mining
- Suspicious remote login attempts
- Lateral movement activity
- Data exfiltration
- Rogue DHCP servers

Performance (IT operations) detections identify the following types of network infrastructure and performance issues:

- Failed login or authorization attempts
- Database errors and performance issues
- Poor user experience associated with Citrix sessions
- Infrastructure performance issues, such as DHCP configuration or network congestion
- Email service degradation
- File storage access issues
- Web application errors

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	Detections
How are they generated?	By conditions you define through Alert settings. You can configure trend, threshold, or detection 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 Web UI.	Click **Detections** from the top menu of the Web UI.
How do I set up email notifications?	After an email server is configured in the Admin UI, you can set up email notification settings for any alert.	After an email server is configured in the Admin UI, you can configure a detection alert and then set up email notifications.
What are the benefits?	You decide which business critical 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

	Alerts	Detections
		algorithm better understand your network.
What are the challenges?	As your network changes, your configuration might become outdated or require continual maintenance of alert configurations.	Several security detections can be identified immediately after you connect to the ExtraHop Machine Learning Service; however, traffic must be stored on the Discover appliance for two weeks before the algorithm understands typical patterns of behavior for your network traffic and can identify performance detections.

What is a risk score? (ExtraHop Reveal(x) 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

Risk scores were added to detections in Reveal(x) Summer 2018. If a detection was identified in a previous version, the risk score is unavailable for that detection.

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

How do I see ongoing detections?

Change the time interval to the **Last 30 minutes** and then visit the Detections page in the ExtraHop Web UI. Ongoing detections are listed at the top of the page.

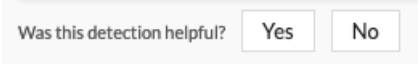
Why can't I view source device details for a detection?

If the source of a detection is a device that hasn't been discovered by the ExtraHop system, there is no device information to share; the detection only shows the IP address of the device and there is no device link.

Similarly, when detections are grouped by source on the Security Overview page or Detections page, an IP address is displayed in place of a device name to indicate that an undiscovered device is the source of the detection.

Can I provide feedback about a detection?

Yes, the following feedback buttons are available at the bottom of the detection details:



Your feedback is valuable and helps us improve our detection process. All feedback is anonymous and will not have an immediate effect on your detections. You can submit feedback for an detection more than once.

Are detections available on the ExtraHop Command appliance?

If you are managing multiple ExtraHop Discover appliances through a Command appliance, you can access detections for any connected Discover appliances that are enabled for detections.

After connecting to the Machine Learning Service, how far back are detections found?

After you first connect to the Machine Learning Service, you can look for detections starting one week back. 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?

In ExtraHop 7.0 and later, 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 Troubleshoot your connection to ExtraHop Cloud Services.

What data is sent from the ExtraHop system to the cloud-based 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. Sensitive data remains on-premise and under your control. The ExtraHop Machine Learning Service has received the SOC 2, Type 1 compliance certification.

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 that must added to your appliance. 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.

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

Yes, previous detections remain available in your ExtraHop system.