Detections FAQ

Published: 2018-07-12

Here are some answers to frequently asked questions about detections.

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

How are detections identified?

After you connect to the ExtraHop Machine Learning Service, the ExtraHop system begins to apply machine learning technology to your wire data automatically. Your appliance evaluates 4-weeks of data to calculate a range of expected network and user behavior that spans hundreds of metrics and several protocols. Normal values are determined through a proprietary algorithm that combines time series decomposition, unsupervised learning, heuristics, and domain expertise to evaluate data. Detections identify deviations from the expected data range of metric values and makes updates as your network traffic pattens change.

You can view and interpret detections on the Detections page in the ExtraHop Web UI.

For more information, see How ExtraHop detections work.

How do I add a new or updated license for detections to my ExtraHop system?

If you purchased a new ExtraHop system that includes a license for detections, 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 detections, your updated license is automatically added to your ExtraHop system, but must still be applied. Follow the instructions to apply an updated license.

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.

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.

What type of detections are identified?

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

What types of security detections are identified?

Security detections identify the following types of risks:

- Command and control activity
- Brute force attacks
- Reconnaissance activity
- Remote login attempts
- Lateral movement activity
- Data exfiltration
- Rogue DHCP servers

What types of performance detections are identified?

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

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.

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.

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.

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

Why don't I see a risk score? (ExtraHop Reveal(x) only)

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.

Can I get an email alert for detected anomalies?

Yes. First, you must configure a detection alert from the Alert page in the ExtraHop system. A detection alert lets you specify which device name, application name, security detections category, performance detection category, or metric you want to receive an email for. You can also assign a severity level to the alert. Then, configure email notification settings for your detection alert.

Can detections help me identify chronic network issues?

The Machine Learning Service focuses on identifying detections for abnormal deviations from four weeks of historical behavior.

To help you determine whether a detection is a chronic issue instead of an occasional deviation, we recommend that you continuously monitor your environment for trends in network behavior. The ExtraHop Atlas report service is another good way to identify chronic issues, such as constant DNS lookup failures or a high number of errors, and receive a recommended remediation an issue.

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.

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

Yes, previous detections remain available in your ExtraHop system.

Can I provide feedback about a detection?

Yes, click the feedback icon in the top right corner of the detection to let us know if the detection was helpful. 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.