Expanded Threat Intelligence FAQ

Published: 2024-05-15

What is expanded threat intelligence?

Expanded threat intelligence enables users to share select data with ExtraHop for review against a larger collection of CrowdStrike threat intelligence indicators, benign endpoints, and other network traffic information. Reviewing data against an expanded library of intelligence results in enhanced identification of malicious endpoints, improved accuracy of detections, and contextual enrichment of detection information to support quick and informed evaluations of detections.

RevealX Enterprise users must activate this service by enabling ExtraHop Cloud Services and opting in to expanded threat intelligence in the Administration settings. Once enabled, the system can send IP addresses, domain names, hostnames, file hashes, and URLs observed on your system for real-time review against a larger collection of threat intelligence. This setting is enabled in RevealX360 by default and can not be disabled. For a full list of data types sent to ExtraHop Cloud Services, and to see how the data is applied to improve threat detection, see the Machine Learning section of the .

How secure is my data?

When you opt-in to to expanded threat intelligence, the ExtraHop sensor sends this metadata to ExtraHop Cloud Services through TLS 1.2 or TLS 1.3 connections and perfect forward secrecy (PFS). IP addresses, domain names, hostnames, file hashes, and URLs sent to Cloud Services for expanded threat intelligence are reviewed immediately then discarded.

You can learn more about how ExtraHop secures your data in the ExtraHop Security, Privacy and Trust Overview.

Why should I opt-in?

Here are the ways that you benefit from expanded threat intelligence.

The power of cloud-processing

ExtraHop cloud-based machine learning offers processing capabilities that extend far beyond the capacity of individual sensors. Opting in to expanded threat intelligence opens up a massive library of threat indicators that could not be applied efficiently at the sensor level, but can be processed in real-time with the computing power of ExtraHop cloud resources.

Additional CrowdStrike coverage

The ExtraHop system offers quality threat collections from CrowdStrike as a standard component of built-in threat intelligence. Due to processing constraints, there is a large remainder of CrowdStrike intelligence that cannot be included on sensors. Opting in to expanded threat intelligence embraces the additional processing power provided by ExtraHop Cloud Services and enables a much larger collection of CrowdStrike indicators to review against your network traffic.

More information now, less investigation later

Threat intelligence is not just about identifying suspicious IP addresses or malicious file hashes. It is also about quickly identifying traffic that is not suspicious. ExtraHop leverages network data to classify benign network activity and remove the noise of harmless activity from investigation workflows. Opting in to expanded threat intelligence enables ExtraHop to filter what analysts are going to see through the largest possible collection of threat indicators and benign behavior patterns and present only quality, actionable information.

What is the difference between expanded threat intelligence and collective threat analysis?

Data sent to collective threat analysis is added to an anonymized pool of data and studied to enhance machine-learning detections, identify new attack types, generate detections for malicious file hashes, and

improve the accuracy of existing detections. Data shared with expanded threat intelligence is immediately reviewed against an extended collection of threat intelligence, then is discarded.

Both services are enabled automatically in RevealX 360, but RevealX Enterprise administrators must opt-in from the Administration settings.

Can I opt out?

This service is enabled in RevealX360 by default and can not be disabled. RevealX Enterprise systems are opted out of expanded threat intelligence by default and can opt in to the service in Administration settings.

The following settings are available:

- I agree to send IP addresses, domain names, hostnames, file hashes, and URLs to ExtraHop Cloud Services.
- I do not want to send IP addresses, domain names, hostnames, file hashes, and URLs to ExtraHop Cloud Services and understand my data will not be reviewed against the full collection of threat intelligence.

Will opting out stop all detections based on threat intelligence?

No. Opting out of expanded threat intelligence will only keep your data from being reviewed against a full collection of threat intelligence. Network data will still be reviewed against threat intelligence from local sources including built-in threat collections, uploaded STIX files, and TAXII feeds. For example, you will still see detections based on built-in CrowdStrike threat collections.