Collective Threat Analysis FAQ

Published: 2024-04-08

What is collective threat analysis?

Collective threat analysis enables users to share select data with ExtraHop to improve the accuracy of detections, such as Command-and-Control (C&C) Beaconing, and generate new detections, such as the identification of malicious file hashes.

By default, any data sent to the ExtraHop Cloud Service that might uniquely identify a network participant (such as an IP address or username) is encrypted with a key that is stored on the sensor and to which ExtraHop has no access.

Reveal(x) Enterprise users can send data to the Machine Learning Service by enabling ExtraHop Cloud Services and opting in to collective threat analysis in the Administration settings. For example, the system can send domain names, hostnames, file hashes, and external IP addresses. This setting is enabled in Reveal(x)360 by default and can not be disabled. For a full list of data types sent to the ExtraHop Machine Learning Service, and to see how the data is applied to improve threat detection, see the Machine Learning section of the ExtraHop Security, Privacy and Trust Overview.

By opting in to share this plaintext data, you contribute to a large community dataset that can be analyzed for everyone's benefit—especially your own. This dataset includes both plaintext data and de-identified metadata associated with threats detected by ExtraHop.

How secure is my data?

When you opt-in to collective threat analysis the ExtraHop sensor sends this metadata to the Machine Learning Service through TLS 1.2 or TLS 1.3 connections and perfect forward secrecy (PFS). Both data in transit and data at rest is stored securely in an encrypted highly-protected datastore.

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 contributing to collective research and analysis.

Improve context about your detections

ExtraHop cloud-based machine learning can take advantage of plaintext data when analyzing suspicious behavior. Rich data surfaces detections with higher confidence.

For example, take the website of a local coffee shop that has poorly configured web analytics. This website frequently reaches out to an external analytics server with performance statistics. The website traffic might be detected on your network for 30-second rapid beaconing—a behavior that is also commonly observed in malicious command-and-control (C&C) beacons. However, with access to the external plaintext hostname and IP address of the analytics server associated with the detection, the ExtraHop system can better determine whether the rapid beaconing is tied to a known malicious source. Improved context helps ExtraHop tell you when traffic is malicious and reduces false positives.

Help stop novel attacks on your network

ExtraHop performs big-data analytics to hunt for stealthy and advanced attacks that individual organizations might overlook. The entire customer base is automatically and immediately protected from each newly identified threat.

For example, ExtraHop might observe that devices across multiple networks are establishing reverse SSH tunnels to a suspicious IP address. Upon further analysis, the suspicious IP address appears to be hosting a C&C server that is exhibiting behaviors previously associated with a known threat

group. ExtraHop immediately updates all deployed sensors with detections to protect all cloud-connected deployments from the newly identified threat.

Improve machine-learning models in your detections

ExtraHop leverages community-sourced data when training machine-learning algorithms and developing new machine-learning models, which are designed to find attacks on user networks. We also refine our understanding of benign behavior patterns by monitoring how behaviors manifest across the networks of different industries, sizes, and geographic locations.

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 Reveal(x) 360, but Reveal(x) Enterprise administrators must opt-in from the Administration settings.

Can I opt out?

In Reveal(x) Enterprise sensors, you can opt out of the default setting that enables collective threat analysis.

Detectors that support collective threat analysis show all users a reminder notification in the Group by Detection Type view and Detection Detail view. Administrators can opt to hide the in-product reminders.

The following settings are available:

- Contribute domain names, hostnames, file hashes, and external IP addresses for collective threat analysis
- Do not contribute to collective threat analysis
- Do not contribute to collective threat analysis and do not display in-product reminders