DATA SHEET

THREATQ DATA EXCHANGE

How the ThreatQ Platform and ThreatQ Data Exchange can help organizations efficiently share focused and curated threat intelligence

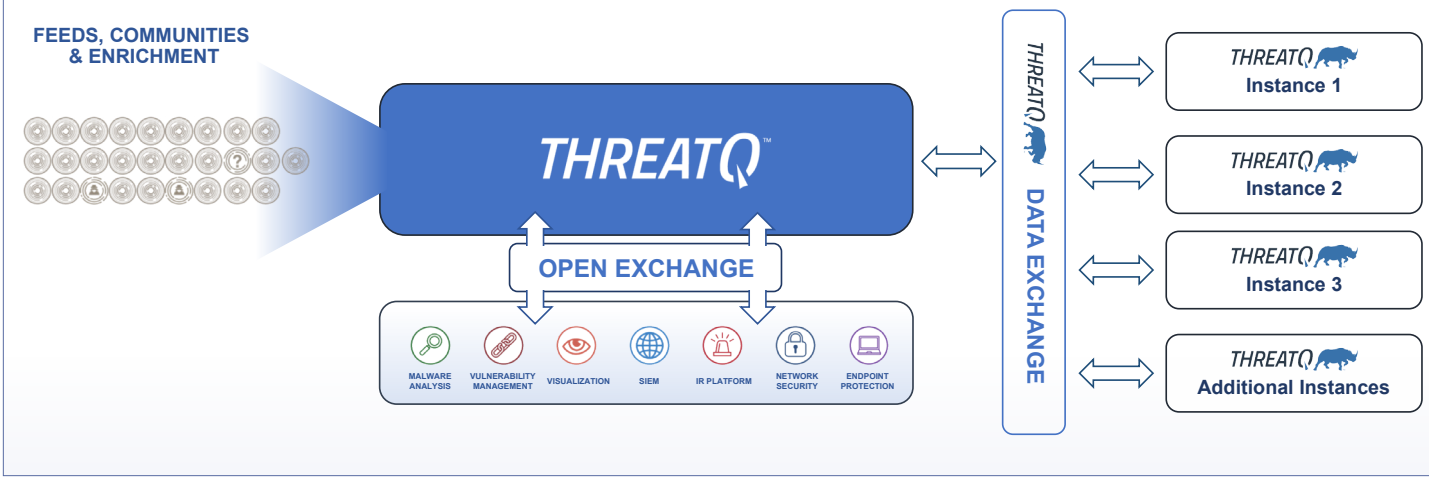
ThreatQ Data Exchange is the best way to enable and manage intel collaboration across organizations or multiple organizations of any size and complexity. ThreatQ Data Exchange makes it simple to set up bidirectional sharing of any and all of your intelligence data within the ThreatQ platform and scale sharing across many teams and organizations of all sizes.

Built on the foundation of ThreatQuotient's flexible data model and support for open intelligence sharing standards, the solution is designed for customization and collaboration. This means individual teams can operate according to their specific requirements and missions and collaborate with partners without limiting the breadth of data they want to share or leaking data they want to keep private.

Highlights

- An intuitive user interface to easily establish bidirectional or unidirectional connections with external systems.
- Interactive topology graph canvas that represents all connected systems and makes administration and monitoring simple and easily scalable.
- Easy installation workflows utilize connection configuration bundles which makes the task of adding multiple connected nodes simple and repeatable.
- A robust activity log provides the status of connections and details of exchanged data for tracking and reporting.

DATA TRANSFER USING THREATQ DATA EXCHANGE



Who benefits from ThreatQ Data Exchange?

Any multi-tiered threat intelligence sharing network where control and monitoring must be available to a global administrator will gain a faster and easier way to operationalize threat intelligence with ThreatQ Data Exchange. This includes:

- Larger government entities with distinct intel teams and missions that continuously collaborate and share relevant intel.
- MSSPs that provide multi-sector or geo coverage to end customers.
- Large or medium-sized commercial organizations with a global presence or segmented business units (multinationals, conglomerates, entities with multiple geo coverage with intel data segregation requirements).

USE CASE

An enterprise has its corporate security operations located at their headquarters. Due to the nature of their business, they have multiple subsidiaries throughout the globe and the need to share curated threat intelligence to the security teams within these subsidiaries. The cyber threat intelligence (CTI) team at headquarters is responsible for collecting, analyzing and prioritizing threat intelligence relevant to their industry. A subset of this intelligence needs to be sent to each subsidiary in order to provide consistent detection around the globe and ensure that global security risk is covered.

With ThreatQ Data Exchange, the central team is able to configure their ThreatQ platform as the primary source of threat intelligence in their environment. Enabling entities to receive data from the primary source is straightforward. They simply generate a connection bundle on the primary ThreatQ platform and export it to every single subsidiary node. Once these bundles are in place, the communication can start.

Analysts who are using the primary ThreatQ platform can curate the threat intelligence so that when the subsidiaries receive and consume the data collected, it is relevant and prioritized for their environment. The central CTI team can save the search so that each time they create a data collection and share it for local consumption, it is already curated based on parameters they have set. Data collections are not restricted to technical indicators but can include context as well as information about malware, specific campaigns and threat actor tactics, techniques and procedures (TTPs) and motivations. Turning on the data transfer streams curated threat intelligence to each subsidiary.

A two-way exchange

It is also important for the central CTI team to be able to collect feedback from subsidiaries around the globe on disseminated intelligence. ThreatQ Data Exchange provides bidirectional integration so that it is possible to configure the exact same transport layer to provide feedback from each subsidiary back to the central CTI team. This enables the central CTI team to better understand the security posture of the global organization with respect to specific threats they are tracking, highlighting trending intelligence and pinpointing areas of weakness in the coverage.

Bidirectional communication can also be used to build a centralized, global memory of threats. As each subsidiary manages security incidents, uncovers new threats or finds additional context around known threats, this data can be stored in the central repository. The transport layer can simply be configured to automatically send all incident-related information or locally-created intelligence back to the main ThreatQ platform to build a single source of truth that can be shared back out to teams around the globe.