Introduction to Trusted Automated eXchange of Intelligence Information (TAXII)

What is TAXII?

Trusted Automated Exchange of Intelligence Information (TAXII) is an application layer protocol for communicating Cyber Threat Intelligence (CTI) in a simple and scalable manner. TAXII defines a RESTful API and requirements for client and server implementations to discover and share CTI.

TAXII enables organizations to share logical groupings of CTI and defines searchable metadata pertaining to CTI content. A TAXII client can request desired CTI from a TAXII server by specifying a set of metadata filters included in the request. A manifest of available CTI content can also be requested, in addition to information about how a CTI collection is structured and may be navigated.

TAXII was designed to transport Structured Threat Information Expression (STIX) and some of its features are intended to align with STIX. However, TAXII is payload-agnostic and does not assume any specific CTI format. TAXII and STIX are independent standards. TAXII can be used to transport non-STIX CTI and STIX does not rely on any specific transport mechanism.

Both TAXII and STIX are OASIS standards, developed and managed by the CTI Technical Committee (TC).[1] See the CTI TC document repository for the latest versions of the TAXII and STIX standards.[2,3]

TAXII Benefits

- **Provides easy integration with existing sharing agreements.** TAXII supports commonly used threat sharing models: hub-and-spoke, peer-to-peer, and source-subscriber.

- **Supports communication with automated defenses.** TAXII is machine readable and can update automated defenses quickly to address emerging, routine cyber threats.

---

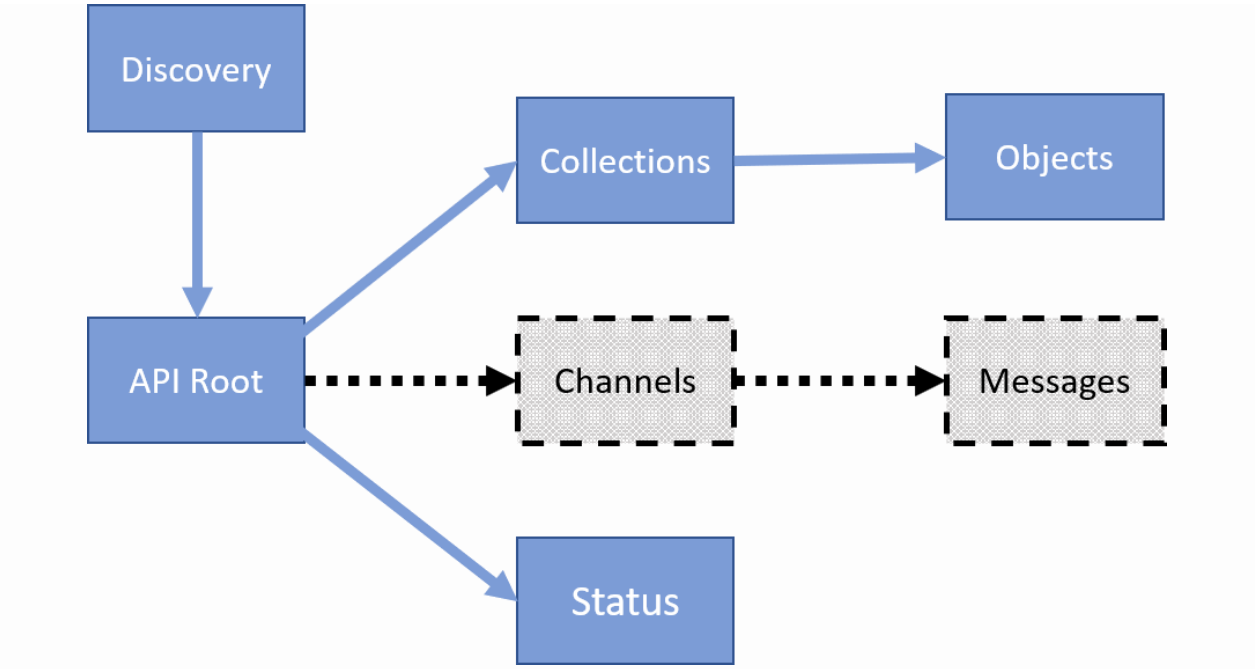
[1] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti
[2] https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.html
[3] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html

- **Minimizes operational changes needed for adoption.** TAXII is a simple, application layer protocol that can be easily applied to support custom, cyber threat sharing processes.

How TAXII Works

TAXII relies on existing protocols wherever possible. It uses HTTP for content negotiation and authentication. TAXII servers can be discovered within a network via DNS service records. TAXII uses UTF-8 encoded JSON as the serialization format for all TAXII exchanges. In addition, HTTPS provides the transport for all TAXII communications.

TAXII defines an *API Root* that organizes and provides access to CTI data. A TAXII Server can host multiple API Roots to provide for division of content and access control. The figure below depicts the logical structure of an API Root.[4]



- **Discovery** information can be used to learn about the API Roots hosted by a TAXII Server.

- **Collections** in an API Root allow TAXII Clients and Servers to exchange CTI using a request-response paradigm. Interactions with Collections include getting a manifest of CTI contained in the Collection, adding new CTI content, and retrieving CTI content. Individual items of CTI content in a Collection are referred to as **Objects**.

[4] http://docs.oasis-open.org/cti/taxii/v2.1/taxii-v2.1.html

- **Channels** will allow TAXII Clients to exchange information using a publish-subscribe paradigm, using **Messages.** Channels will be specified in a future version of TAXII.

- **Status** information pertaining to requests sent to the TAXII Server are also supported by the API Root. For example, if a TAXII Client submitted new CTI to a Collection, a Status request allows the Client to check on whether the new CTI was accepted and added to the Collection.

See the STIX/TAXII website for more information about TAXII version 2.1.[5]

[5] https://oasis-open.github.io/cti-documentation/