Trusted Automated eXchange of Indicator Information — TAXII™
Enabling Cyber Threat Information Exchange

TAXII defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries. TAXII, through its member specifications, defines concepts, protocols, and message exchanges to exchange cyber threat information for the detection, prevention, and mitigation of cyber threats. TAXII is not a specific information sharing initiative or application and does not attempt to define trust agreements, governance, or other non-technical aspects of cyber threat information sharing. Instead, TAXII empowers organizations to achieve improved situational awareness about emerging threats, and enables organizations to easily share the information they choose with the partners they choose.

TAXII use cases include:

- **Public Alerts or Warnings**
- **Private Alerts and Reports**
- **Push and Pull Content Dissemination**
- **Set-up and Management of Data Sharing Between Parties**

TAXII and STIX

TAXII is the preferred method of exchanging information represented using the Structured Threat Information Expression (STIX™) language, enabling organizations to share structured cyber threat information in a secure and automated manner.

Challenge

The gathering and use of detailed cyber intelligence is the best defense against today's determined cyber adversaries. "Cyber intelligence" — or the collecting, analyzing, and countering of cyber security threat information — starts with gathering information about attacks, such as spear-phishing email header and content, urls to malicious links, and malware analysis-derived artifacts like Command and Control (C2) domain names and IP addresses. With a corpus of threat data, skilled cyber analysts can group patterns of similar activity, attribute activity to certain threat actors, quickly identify and implement mitigation strategies, and anticipate the launch of similar attacks in the future.

To fully realize the benefits of cyber intelligence, organizations need to share cyber threat data, if not defensive strategies and more, with trusted partners. Current cyber threat information sharing, however, is often either a time-consuming, manual process or a limited-scope automation effort tied to particular cyber threat information sharing community or technology.

Solution

TAXII fills this void. The TAXII services and message exchanges are designed to enhance interoperability of different cyber security solutions and vendors are encouraged to incorporate support for TAXII within their cyber security products and services. By supporting TAXII, vendors enhance the value of their solutions by allowing their customers to leverage actionable intelligence from multiple sources.

TAXII's goal is to help add automation to the processes of existing cyber threat information sharing communities and to help establish new communities of sharing by simplifying the technical aspects of cyber threat information exchange. It is recognized that sharing communities are highly diverse and cannot be reduced to a single sharing model. For this reason, TAXII uses a modular design that can accommodate a wide array of sharing models. Individual services in TAXII are optional for any given implementation, allowing enterprises to include only the services desired for their particular sharing model.

TAXII™

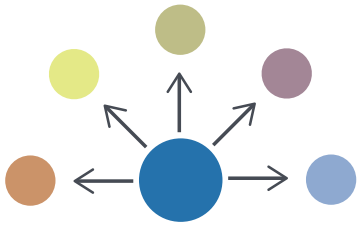
taxii.mitre.org

TAXII is a U.S. Department of Homeland Security–led effort of the office of Cybersecurity and Communications. MITRE, operating as DHS's FFRDC, manages the TAXII website, community engagement, and discussion lists to enable open and public collaboration with all stakeholders.

Sharing models supported by TAXII include (but are not limited to):

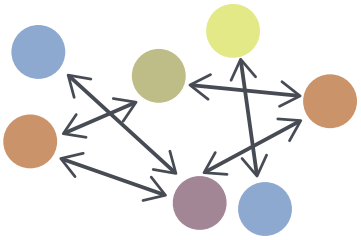
Source-Subscriber

A single entity publishes information out to a group of consumers. This is a common model in commercial environments, where the data source is a vendor and the subscribers purchase access to the vendor's information. This is also a common model for free alerts from some authoritative source.



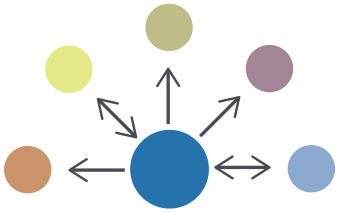
Peer-to-Peer

A group of data producers and data consumers establish direct relationships with each other. The group may have a single governing policy, but all sharing exchanges are between individuals.



Hub-and-Spoke

A group of data producers and consumers share information with each other, but instead of sending directly, the information is sent to a central hub, which then handles dissemination to all the other spokes as appropriate. This model can be viewed as being similar to e-mail distribution lists, where a sender provides a message to a mailing-list service, which then forwards the message on to all the members of the list.



Push or Pull Sharing

TAXII supports both push and pull messaging in all models, allowing sharing scenarios where data consumers are automatically provided with new data, or where the consumer can request updates at times of their choosing. Data producers in a TAXII architecture can choose whether data consumers can pull data from the producer, whether data is pushed from the producer, or whether a mixture of the two methods is supported.

Lightweight, Non-Disruptive Design

Existing sharing communities often have established an infrastructure for storing and managing threat information. TAXII is designed to enable the exchange of this information without impacting existing data management infrastructure. TAXII defines network-level messages and services, but does not impose significant requirements on behavior below the network layer. As such, TAXII is intended to be layered on top of existing data management schemes with minimal disruption. For similar reasons, enterprises without existing infrastructure are free to use their own favored data management schemes, confident that such schemes can integrate with TAXII services and messages.

Cyber threat information is frequently sensitive and organizations may be highly selective as to what information is shared with specific parties. The information that factors in to such decisions can vary from organization to organization. Rather than attempting to standardize such behavior, TAXII focuses on ensuring secure transport of the information over the wire and leaves decisions as to what is shared with whom to the back-end infrastructure of the enterprise. TAXII imposes no requirements or limits on sharing decisions and allows organizations to decide what information is visible to individual requesters using their native decision processes.

TAXII leverages existing protocols and specifications wherever possible. The TAXII core services are designed in a fashion that is neutral with regard to network protocols and data formats. TAXII defines bindings to specific network protocols and data formats separately from the core services. Implementers can select the bindings they wish to use or even define their own. Because all bindings share the same understanding of the TAXII services and messages a party that can only support a very constrained set of protocols or formats can still make use of the services and messages of TAXII, and thus would have a window for receiving threat information from a significantly larger set of sources.

Feedback Requested

TAXII Community members can make contributions to TAXII development and manage issue tracking for the TAXII specifications, schemas, and supporting information by joining the TAXII Community at https://taxii.mitre.org/community/. Members of the cyber security community are invited to participate in this growing community effort.