ANOMALI

What are STIX/TAXII?

The old adage of "sharing is caring" is paramount within the cyber threat intelligence community. Quick and in-depth transfer of knowledge between individuals, organizations, products, and platforms can lead to improved prevention and mitigation of cyber-attacks. There are many sources of information possible for acquiring such knowledge, but sharing opens many questions:

- How best to share this information and what should the information look like?
- What structure will ensure that it is quickly and efficiently parsed?
- How can you guarantee that the information you share is detailed and accurate?

Cyber threat sharing protocols called Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Intelligence Information (TAXII) have been developed in response to these questions. The establishment of STIX/TAXII is an open, community-driven effort that provides free specifications to aid in the automated expression of cyber threat information.

STIX and TAXII — One standard to rule them all

Technically speaking, STIX and TAXII are not sharing programs, tools, or software, but rather components and standards that support them. STIX states the *what* of threat intelligence, while TAXII defines *how* that information is relayed. Unlike previous methods of sharing, STIX and TAXII are machine-readable and therefore easily automated. Both possess an active community of developers and analysts.

STIX/TAXII aims to improve security measures in a few ways:

- Extend the capabilities of current threat intelligence sharing,
- Turn focus of security outward rather than inward,
- Balance response with proactive detection,
- Encourage a holistic approach to threat intelligence.

STIX

STIX, short for Structured Threat Information eXpression, is a standardized language developed by MITRE and the OASIS Cyber Threat Intelligence (CTI) Technical Committee for describing cyber threat information. It has been adopted as an international standard by various intelligence sharing communities and organizations. It is designed to be shared via TAXII, but can be shared by other means. STIX is structured in such a fashion that users can describe threat:

- Motivations
- Abilities
- Capabilities
- Response

STIX is made up of several constructs:

1. Observable — dynamic event or stateful property (previously represented in CybOX).
2. Indicator — an observable with context. Can contain a time range, information source, intrusion detection system, etc.
3. Incident — a set of activities associated with the same adversary.
4. TTP — tactics, techniques, and procedures.
5. Exploit target — the targeted group or individual.
6. Campaign — instances of threat actors pursuing an intent.
7. Threat actor — individual with malicious intent.
8. Course of action — steps to remediate an identified problem.

CybOX

CybOX (Cyber Observable eXpression) is a standardized language for expressing information about cyber observances, which are events that occur in the operational cyber domain. Through its schematic system users would be able to automate sharing, mapping, detection, and analysis of these cyber observables. CybOX was designed as a system for describing base level objects that tie into higher level languages such as STIX. CybOX has since been integrated into STIX as STIX 2.0 is developed.

TAXII

TAXII, short for Trusted Automated eXchange of Intelligence Information, defines how cyber threat information can be shared via services and message exchanges. TAXII is becoming an international standard. It is designed specifically to support STIX information, which it does by defining an API that aligns with common sharing models. The three principal models for TAXII include:

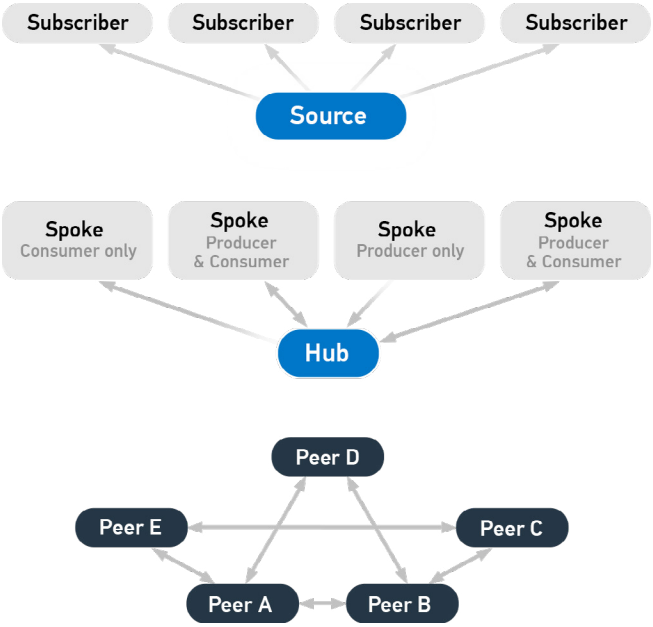
1. Hub and spoke — one repository of information,
2. Source/subscriber — one single source of information,
3. Peer-to-peer — multiple groups share information.

TAXII defines four services. Users can select and implement as many as they require, and combine them for different sharing models.

1. Discovery — a way to learn what services an entity supports and how to interact with them,
2. Collection Management — a way to learn about and request subscriptions to data collections,
3. Inbox — a way to receive pushed content (push messaging),
4. Poll — a way to request content (pull messaging).

Flexible Sharing Models

Most sharing models are variants of these three basic models. TAXII can support participation in any of these models or multiple models simultaneously.



History

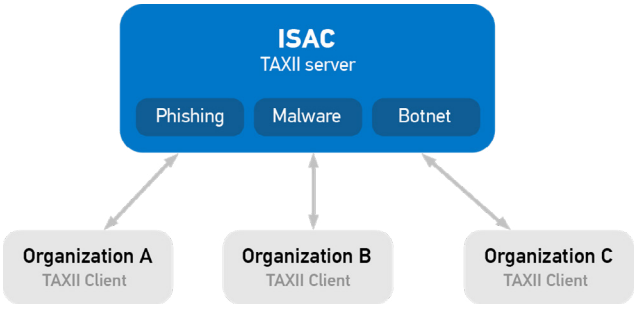
STIX and TAXII were developed by the MITRE Corporation and the Department of Homeland Security (DHS). From the project's inception, the DHS maintained that STIX and TAXII would be transitioned to a standards development organization once it reached a sufficient level of maturity. As of 2015, both STIX and TAXII were transitioned to OASIS in the newly formed Cyber Threat Intelligence Committee, which is recognized internationally as a non-profit consortium that drives the development, convergence, and adoption of open source standards for the Internet. Anomali is a member organization, and CEO Hugh Njemanze represented Anomali (then ThreatStream) on the

original Technical Committee Call for Participation. This transition to an open-source entity was planned to ensure that this set of standards would be freely available to anyone around the world and allow for greater transparency and participation within the cyber security community. The DHS continues to play an active role within the development of STIX/TAXII, but concentrates its efforts on promoting worldwide adoption of these standards.

More information can be found in the Technical Committee Charter.

Use Cases

STIX/TAXII supports a variety of use cases regarding cyber threat management, including analyzing cyber threats, specifying indicator patterns, and managing and sharing cyber threat information. Wide adoption of STIX/TAXII has been seen by governments and Information Sharing and Analysis Centers (ISACs), which range in focus from industry to geolocation.

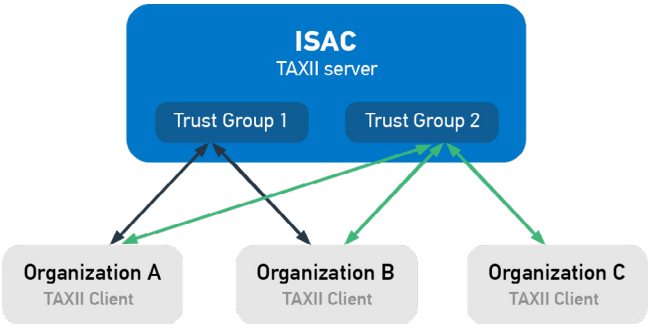


Sharing categorized information

Organizations can push and pull information into categories. For example, if one industry experiences a targeted phishing attack, they can share that information within the phishing category of the ISAC. Other organizations can automatically ingest that intelligence and bolster their own defenses.

Sharing with Groups

Organizations with a TAXII client can push and pull information into the TAXII servers of trusted sharing groups. Some organizations may have access to private groups within these ISACs that provide more detailed information.



Coming Soon: STIX 2.0

The OASIS CTI TC has developed STIX 2.0 in an effort to ameliorate sharing of threat intelligence. Some of the more significant changes include enabling

Summary of changes between STIX 1.x/CybOX 2.x and STIX 2.0.

	STIX 1.x	STIX 2.0
Language	XML	JSON
Consolidation into STIX	CybOX	STIX Cyber Observables
Organization	Embedded objects	STIX Domain Objects (SDO) – all top level
Model	Wide variety of properties, none required	Fewer properties, some required
New Features	x	STIX Relationship Objects (SROs) [new]
Data Markings	No serialization specific language (e.g. XPath)	Object marking/granular marking
Specifications	Generic TTP & Exploit Target types	Separate top level objects (malware, tool, attack pattern, vulnerability)

relationships to be defined between objects, consolidating standards, and requiring more information from users by default.

STIX 2.0 describes a set of STIX Domain Objects (SDOs) to represent a minimally viable product (MVP) to fulfill 12 basic requirements for sharing:

1. Attack pattern — a type of TTP that describes ways threat actors attempt to compromise targets.
2. Campaign — a group of adversarial behaviors that describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets.
3. Course of action — an action taken to prevent an attack or respond to an attack.
4. Identity — individuals, organizations, or groups, as well as classes of individuals, orgs, or groups.
5. Indicator — contains a pattern that can be used to detect suspicious or malicious activity.
6. Intrusion Set — a set of adversarial behaviors and resources with common properties believed to be orchestrated by a single threat actor.
7. Malware — a type of TTP (also known as malicious code and malicious software) used to compromise the confidentiality, integrity, or availability of a victim's data or system.
8. Observed Data — conveys info observed on a system or network (e.g. an address).
9. Report — collections of threat intelligence focused on one or more topics, such as descriptions of a threat actor, malware, or attack technique.
10. Threat Actor — individuals, groups, or organizations believed to be operating with malicious intent.
11. Tool — software that can be used by threat actors to perform attacks.
12. Vulnerability — a mistake in software that can be directly used by a hacker to gain access to a system or network.

STIX 2.0 is currently in public review and is predicted to be released in early Summer of this year. Work is currently underway on the development of STIX 2.1, which will likely be released at the end of this year.

Online Resources

There are many ways to get involved with STIX/TAXII. If you'd like to engage with the community and contribute to creation efforts, you can join a committee within the OASIS TC. If you'd like to learn more about STIX/TAXII, here are some additional resources:

STIX/TAXII Overviews

- GitHub
- OASIS CTI TC Wiki

STIX

- Detailed description of STIX 2.0 (Google Doc)
- Information on the differences between STIX 1.x/CybOX 2.x and STIX 2.0 (GitHub)

TAXII

- TAXII Discussion and Announcement mailing lists
- Python library for managing TAXII messages and services (GitHub)
- Proof of concept TAXII server Yeti (GitHub)
- Access open source feeds via Hailataxii

Conclusion

In an industry where the adversaries always have an edge, collaborating on effective solutions is critical. One such solution is to standardize the way in which cyber threat intelligence is shared, thus ensuring it can be utilized quickly and effectively. Intelligent and automatic sharing of threat intelligence enables faster detection and prevention of breaches, ultimately protecting businesses and strengthening the cyber threat intelligence community.