Introduction to Structured Threat Information Expression (STIX)

What is STIX?

Structured Threat Information Expression (STIX) is a standard language for describing cyber threat intelligence in a way that both humans and machines can understand and act upon. STIX is for anyone involved in cyber defense, including cyber threat analysts, malware analysts, security tool vendors, security researchers and threat sharing communities.

STIX describes cyber threats using an extensive set of properties, which include signs of malicious activity (e.g., suspect file hashes, domains, etc.) in addition to contextual information (e.g., adversary tactics, techniques, and procedures). STIX provides the means to comprehensively document cyber adversary activities, capabilities, and motivations in a standardized format to enable more effective analysis and exchange of cyber threat intelligence.

STIX is independent of any specific exchange format. However, STIX-conformant tools must support a serialized, JSON format, and may optionally include support for other serializations. In addition, STIX is transport-agnostic and does not assume a specific transport mechanism. But a specific protocol, Trusted Automated Exchange of Intelligence Information (TAXII), has been designed specifically to transport STIX.

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

STIX Benefits

- **Removes barriers to sharing cyber-threat intelligence** by providing a standard language for describing cyber-threats so this information can easily be shared between organizations and communities.

- **Enables analysts to develop reusable cyber-threat intelligence** that people can understand, and automated systems can leverage. STIX content is both meaningful to humans, and machine processable.

---

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

- **Augments cyber professionals' efforts** so they can do their jobs more effectively and in less time**.** STIX provides the means to leverage information about known cyber-threats so that cyber experts can spend their valuable time identifying and analyzing new threats.

- **Provides interoperability** between cyber-threat tools and information sources. STIX is well-defined and can be produced and consumed without the need to translate formats.

- **Supports automated defenses** that can be deployed more quickly when needed (seconds versus hours or days). STIX is machine readable and can drive automated systems to address routine cyber-threats.

How STIX Works

STIX consists of three main components:

- **STIX Domain Objects (SDOs)** describe core concepts of cyber threat intelligence (campaign, indicator, course of action, etc.).

- **STIX Cyber-observable Objects (SCOs)** describe facts about a network or host as part of a cyber-attack (e.g., files, IP addresses, registry keys, etc.).

- **STIX Relationship Objects (SROs)** tie together SDOs and SCOs to form a cyber threat intelligence product.

A STIX cyber threat intelligence product can be visualized as a graph (see Figure 1), using SDOs and SCOs as nodes and SROs as links. The STIX example below depicts a campaign (Bravo Bank Attacks) *attributed-to* a threat actor (Adversary Bravo) who *uses* malware (Malware #5). This malware *communicates-with* a C2 server at a domain (Bad Domain) and *uses* an attack technique (ATT&CK T1547.001: Registry Run Keys/Startup Folder). An indicator (Registry Keys) *indicates* the malware.

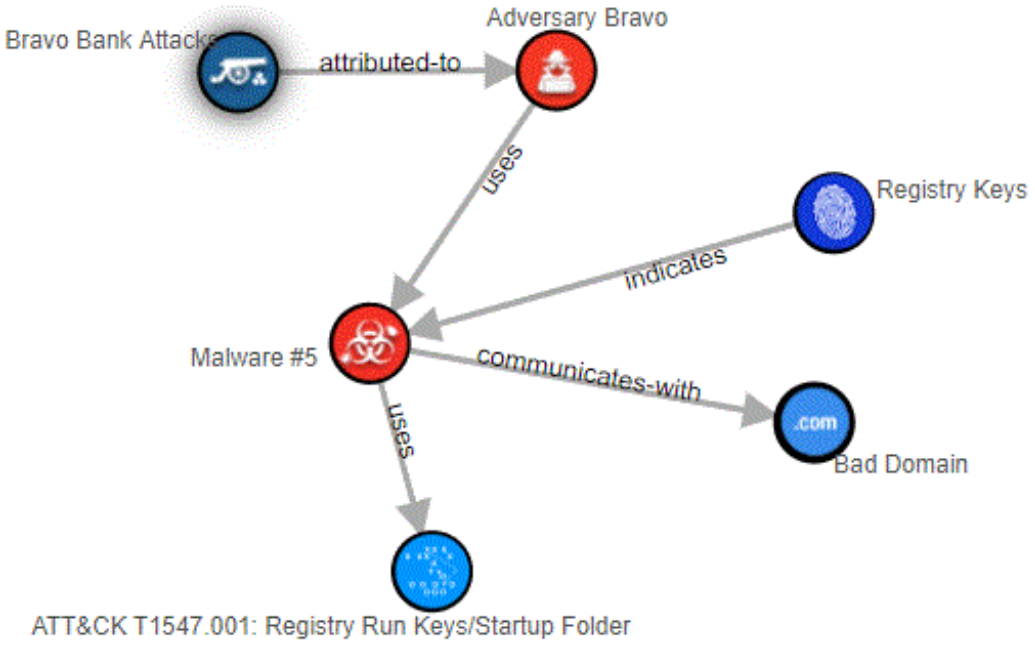

Figure 1. Graph of Cyber Threat Intelligence

See the STIX/TAXII website for other examples and detailed information about STIX version 2.1.[4]

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