No.36
April 23rd, 2020

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/UNSPONSORED**

New STIX & TAXII Releases Approved

- The new open standard STIX and TAXII 2.1 releases are designed to enable SOC analysts to organize and share threat intelligence a lot more easily with trusted peers in other organizations to reduce time to detection and time to mitigation.
- The richness of the new 2.1 releases, and the launch of a new 'STIX/TAXII Preferred' certification program overseen by OASIS, should help accelerate market adoption.

Threat intelligence sharing is one of the aspects of cyber security that most needs improving. Enabling defenders to have access to available intelligence, describe it, enrich it, and proactively share it with others faster, more widely, and more securely, is a key component of hardening organizations against cyber attacks.

The lifting of the political, commercial and human barriers to cyber threat sharing is happening more slowly than we'd all like but at least there's progress on the technical front with the approval of the TAXII 2.1 and STIX 2.1 standards in recent weeks.

Threat intelligence sharing is one of the aspects of cyber security that most needs improving.

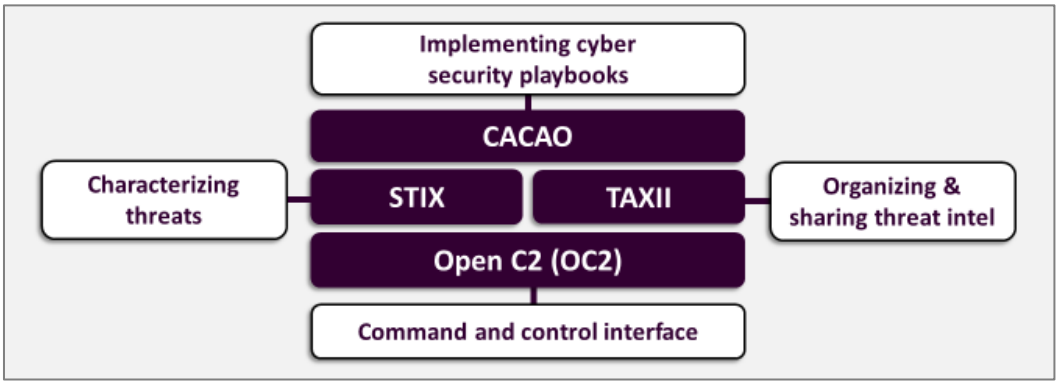
Arising from the work of OASIS

Trusted Automated Exchange of Indicator Information (TAXII) and Structured Threat Information Expression (STIX) are key cyber threat intelligence sharing standards. They are being developed by The Organization for the Advancement of Structured Information Standards (OASIS) Cyber Threat Intelligence (CTI) Technical Committee (TC).

- **STIX** is a language and serialization format for characterizing specific threats including a threat actor's motivations, capabilities and modus operandi.
- **TAXII** is an application layer protocol that allows threat intelligence – expressed in the STIX language – to be exchanged according to a range of different requirements. TAXII is designed to augment - and ultimately replace – email, instant messaging platforms, and blog posts as the preferred means of sharing threat intel. It provides an automated way of securely organizing and sharing threat intelligence, even by trust group, much faster and with a high level of security and rich feature set.

As shown in **Figure 1**, STIX and TAXII are two of the four OASIS cyber security standards. The other two are OpenC2 (OC2), which is a suite of open command and

Figure 1: OASIS Standards for Cyber Security



Source: HardenStance

control specifications, and the newest of the four, Collaborative Cybersecurity Course of Action Operations (CACAO). This provides open specifications for implementing cyber security playbooks.

The 2.0 releases of STIX and TAXII were approved in July 2017. They broke with the closed and inflexible constraints of the original 1.0 releases imposed by using protocols like XML. The 2.0 releases aligned the two standards with the Web 2.0 zeitgeist. For example, STIX adopted JSON while TAXII moved to HTTPS and a RESTful API design.

The hugely popular MITRE ATT&CK Framework uses STIX and TAXII. When the UK and US published a report on COVID-19 exploitation in early April, they made a list of COVID-19 Indicators of Compromise (IOCs) available as both CSV and STIX files. In the Cyber Threat Alliance, the association comprising 26 of the world's largest cyber security vendors, members use the STIX format with MITRE's ATT&CK framework to share indicators with enough context to enable action at machine speed.

At the level of individual vendors implementing these standards in their own product lines, adoption of the 2.0 releases has been limited.

At the level of individual vendors implementing these two standards in their own product lines, however, adoption of the 2.0 releases has been limited. Up until now adoption has been confined to a small subset of leading vendors in each of three security product spaces where security efficacy is most closely tied to effective exploitation of threat intelligence. These are the following:

- Those that generate raw threat intelligence such as Next Generation Firewall (NGFW) and Endpoint Detection and Response (EDR) products;
- Investigative tools that use threat intelligence such as a Threat Intelligence Platform (TIP) or Security Incident and Event Management (SIEM) product;
- Those that act on threat intelligence such as a Security Orchestration Automation and Response (SOAR) platform.

Even in the case of these three most relevant product categories, many vendor products don't support STIX or TAXII yet. The subset of pioneering vendors that have implemented the 2.0 releases, and have customers using them, provided the core of the feedback to the OASIS Technical Committees (TCs). This feedback has gone into the new 2.1 releases, which are now intended for widespread commercial adoption.

STIX 2.1 Substantially Expands the Data Model

The new features of STIX 2.1 fix some issues with original concepts and substantially expand the data model. Specifically, the following have been added:

- Analyst notes, opinions and feedback.
- Malware and malware analysis objects.
- Greater granularity regarding malware infrastructure so that, for example, information can be shared regarding how a specific threat type exploits the infrastructure as part of malware command and control.
- Cyber observables like IP addresses, URLs and domain names have now been made top level objects rather than being encapsulated in an observed data object. This provides better insight, allowing cyber observables to be used directly in STIX graphs. This also allows SOC teams to take better account of observables like domain names changing over time.

In the case of TAXII, the most importance fixes in the 2.1 release improve performance and pagination as well as making it easier to implement some of the resources in the RESTful API. The item based pagination specified in 2.0 has been completely removed from 2.1, for example. This arose from feedback from 2.0 users that the approach became unpredictable, hence unusable, for rapidly changing datasets.

Self-certification of STIX and TAXII compliance will be based on the Wi-Fi Alliance 'Wi-Fi-Certified' certification model, with an accompanying logo.

The goal with the 2.1 changes in TAXII is to enable SOC teams to leverage it not just to receive and ingest new threat data but also to write rules on the fly to query devices in their infrastructure for tell-tale evidence of new threats as new intelligence is received. Removing the friction associated with traditional ways of consulting blogs and emails before querying via proprietary protocols should accelerate multi-vendor automation of mitigation and remediation actions. Hence it should enable SOC teams to reduce time to detection and time to mitigation.

An important development accompanying the new releases is that vendors will now be able to self-certify that their products support STIX and TAXII according to a test-plan that is being designed and overseen by the relevant OASIS committees. The model will be based on the Wi-Fi Alliance's 'Wi-Fi-CERTIFIED' certification model with accompanying 'STIX Preferred' or 'STIX and TAXII Preferred' logos.

Certification will guarantee interoperability so users can be assured that certified vendors will describe, consume and share threat intelligence with other vendors' products as prescribed by the standards. First vendor certifications are expected from the middle of this year. Vendors that pass will be listed on the OASIS website.

More Information

- HardenStance received no payment - direct or in-kind - for publishing this Briefing.
- HardenStance Briefing: "A Window into an OpenC2 World" (August 2019).
- HardenStance White Paper: "Next Steps in Playbook-Driven Cyber Security" sponsored by Cyber Threat Alliance, IBM Security, KPN & Nokia (September 2019).
- OASIS: Cyber Threat Intelligence documentation
- TAXII SC Chair and STIX SC Co-Chair: bret.jordan@broadcom.com
- Principal Analyst: patrick.donegan@hardenstance.com www.hardenstance.com
- Register for free email notifications whenever HardenStance publishes new content.

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, OASIS, ETSI and TM Forum.

HardenStance Disclaimer