**Introduction**

Effective and timely communication of Cyber Threat Intelligence (CTI) is critical to protecting national security, critical infrastructure, and private industry. Without the sharing of CTI, the cyber community becomes silos of critical information in the identification and mitigation of cyber-attacks. The current Structured Threat Information Expression (STIX) standard and Trusted Automated Exchange of Intelligence Information (TAXII) protocol are the products of over a decade of cooperation among experts in CTI and security operations (Barnum, 2014). The STIX standard aims to solve the interoperability problem between different government organizations, industries, and cybersecurity software tools by standardizing CTI into relational graph objects. STIX allows for CTI to be communicated and acted upon at machine speed while remaining human-readable.

In theory, the STIX standard should be the perfect vehicle for machine-to-machine threat intelligence sharing, but there is still much to be desired in practice. For example, with each new version of the STIX standard released, the industry must adapt current cybersecurity solutions to ingest the new schema. During these transition periods, companies are left to figure out what to do with unconsumable STIX bundles, leaving an opportunity for vital CTI to be lost with no warning to the analyst.

Furthermore, some industry leaders still decide to stick with their own proprietary CTI structures. For example, Trend Micro cybersecurity solutions convert all types of CTI into what they call User Defined Suspicious Objects, and their Apex One solution still does not ingest the newest STIX standard. This conversion drops everything within a STIX bundle except for the Indicators of Compromise (SHA-1 hashes, IP addresses, domains, etc) (“Adding STIX Objects to the User-Defined Suspicious Object List | Trend Micro Service Central”). This technique removes much of the context associated with the CTI. Even MITRE and their MITRE ATT&CK framework created extensions to the current STIX 2.1 standard to better accommodate their needs (Miller, 2023).

Identifying cyber threats has become increasingly difficult. As network architectures and technologies become increasingly complex, threat actors continue to advance the methods they use to obfuscate attacks. Though the current STIX 2.1 is designed to balance flexibility and a strict standard structure, it seems to not have the framework to adapt fast enough to meet industry needs. Furthermore, with each new STIX version comes a delayed adoption from industry tools that can produce and consume the new STIX version.

**Problem Statement**

The current threat landscape calls for more advanced and adaptable methods of threat information sharing while still maintaining the ability to share intelligence at machine speeds. More formally, how does the cyber intelligence community improve the mechanisms used to share CTI at machine speeds that do not break existing tools when standards change and allow for enhanced or extensions of the standard between industry partners? I propose a middleware tool that can be added to the STIX and TAXII server framework that can mitigate the following:

1. Improve the consumption of enhanced STIX objects by allowing CTI producers to publish their schemas so that subscribers can ingest their enhanced STIX objects as a part of a federated system, utilizing this middleware tool.
2. Improve predictable schema conversions by ingesting CTI schemas that either describe exactly what information a specific cybersecurity tool can ingest or describe what enhancements to the STIX standard the publisher will produce in their CTI feeds.
3. Prevent CTI data loss by verifying that the structure of the data meets the standard a specific tool downstream is expecting. If it does not meet the standard it gives a warning of what information will be lost in a visual way (i.e. visual graph). It then conducts a conversion to meet the standard the tool is expecting.
4. Finally, because the tool can visualize any enhanced STIX standard version based on a given schema, it allows analysts to continue to analyze CTI while industry tools catch up to adapting to the STIX objects being produced.

My proposed enhanced TAXII framework is centered around a single tool meant to be middleware between TAXII servers and TAXII clients and looks to be a standardized method for federated CTI sharing. New versions of STIX standards or enhanced standards will no longer break existing tools before they are ready to ingest new objects, while still allowing an analyst to observe all portions of a CTI report. Figures 1 and 2 depict how the middleware tool would fit into both a channel and collections TAXII framework. Along with CTI objects, threat intelligence producers would be expected to publish their schemas that fall outside the STIX standard so that threat intelligence consumers can ingest them before subscribing to the producer's threat feed. If a consumer requires a specific format other than what the producer is using, the schema tool allows an analyst to define a conversion within the tool before it reaches cybersecurity products looking to ingest the CTI downstream, avoiding unexpected behavior. If an ingested CTI does not meet any specific standard and a conversion schema is not defined, then a warning is thrown with a visual representation of the problem CTI object. This allows for centralized predictable behavior when both sharing and ingesting CTI at the machine level.

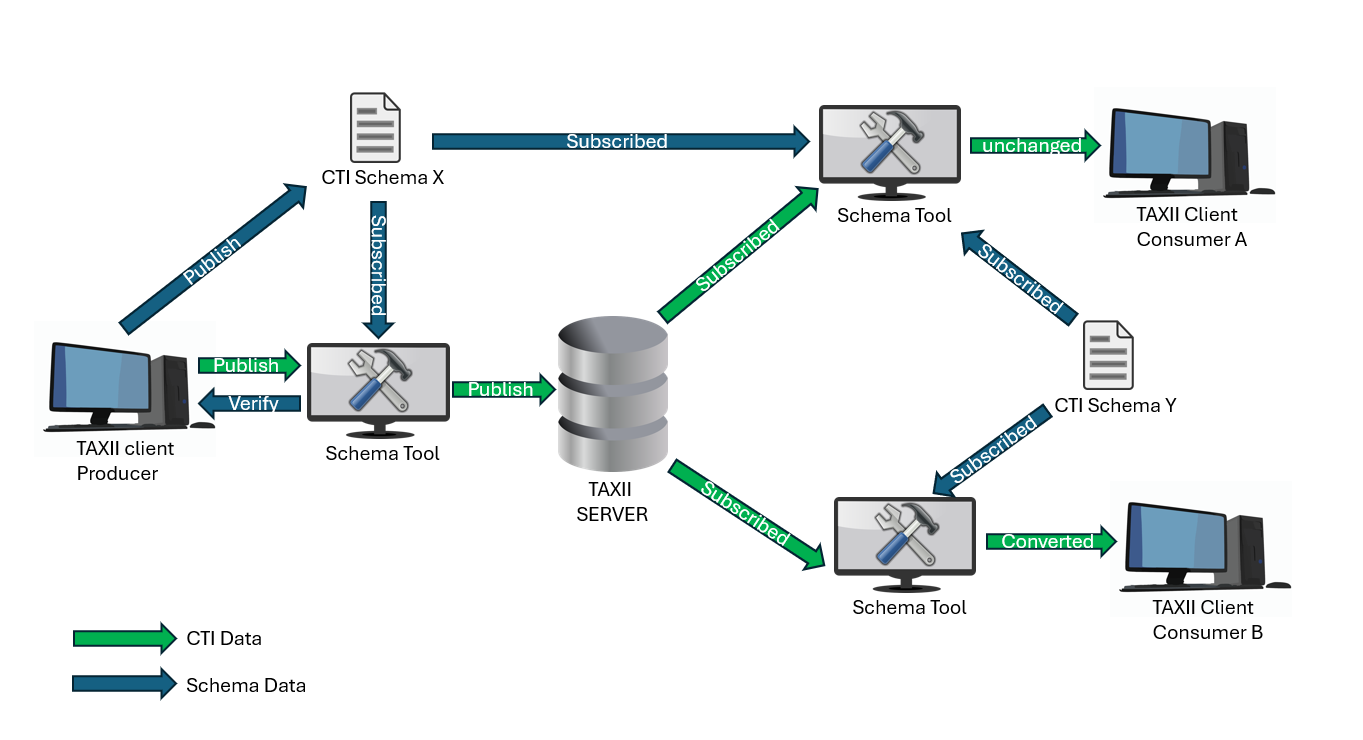


Figure 1. Enhanced TAXII Server Channel Framework

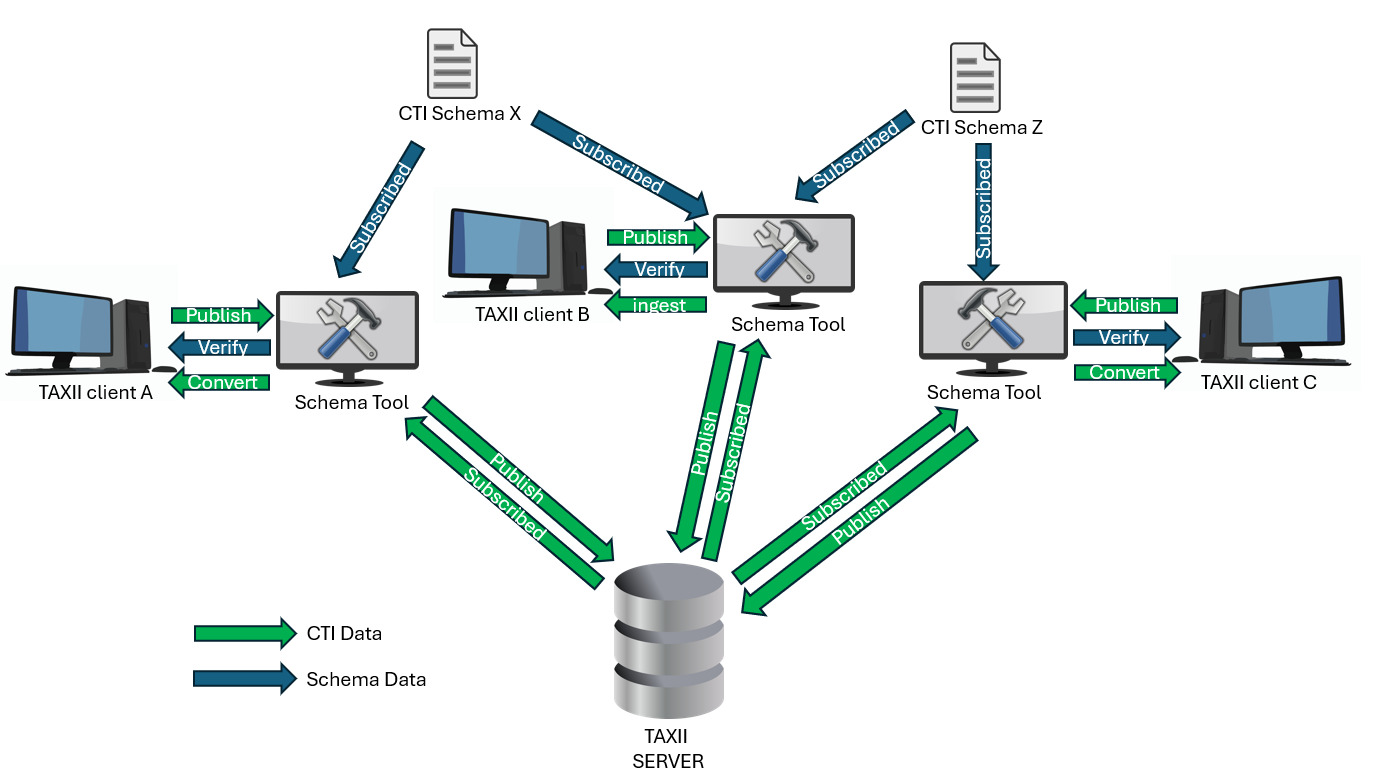


Figure 2. Enhanced TAXII Server Collections Framework

**Motivations**

Many of the early trailblazers of the internet envisioned a virtual utopia where information flowed freely and safely among willing participants, but the reality is something else (Cowles, 2009). Politics, competition, and threat actors have changed the landscape of the internet and ultimately what is openly shared. Cyber Threat Intelligence by some organizations is viewed as proprietary information. Threat intelligence sharing becomes even more complicated amongst nation-states. However, the ability to share and act on CTI is fundamental to ensuring the security of the internet, industries, and personal data. CTI allows large critical sectors of industry and government to mitigate cyber threats as a multi-organizational effort. It allows organizations to establish protections inside networks before an exploit targets their system based on the indicators and behaviors previously observed within another network. It allows these organizations to stay ahead of malicious actors or at the very least avoid an attack affecting multiple organizations. However, as threats become more advanced, so must our ability to communicate actionable intelligence. The cyber security community must continue to find means to work together effectively to mitigate attacks. I believe this research would be a step toward improving those communication techniques.

**Expected Deliverables**

This research will consist of the development and documentation of the schema tool. I will also set up a proof of concept network of TAXII Clients, Servers, and Schema tools within a docker container for both testing and demonstrating the technology. Documentation will consist of a user guide for integrating the tool into their CTI framework and a developer's guide to allow future developers to create enhanced functionality. I plan for the tool to be able to handle STIX 2.0, STIX 2.1, and MITRE ATT&CK STIX by default. I will prepare other custom forms of enhanced STIX objects for demonstration and testing purposes.

**References**

*Adding STIX Objects to the User-Defined Suspicious Object List | Trend Micro Service*

*Central*. (n.d.). Docs.trendmicro.com. Retrieved January 21, 2024, from

[https://docs.trendmicro.com/en-us/documentation/article/trend-micro-apex-centra](https://docs.trendmicro.com/en-us/documentation/article/trend-micro-apex-central-patch)

[l-patch-6-adding-stix-files](https://docs.trendmicro.com/en-us/documentation/article/trend-micro-apex-central-patch)

Barnum, Sean. (2014). *Standardizing Cyber Threat Intelligence Information with the Structured*

*Threat Information eXpression (STIXTM)*. 22.

Cowles, J. (2009). The Internet as Utopia: Reality, Virtuality, and Politics. *Oshkosh Scholar*, *IV*,

81–89.

Miller, C. (2023, October 30). *cti/USAGE.md at master · mitre/cti*. GitHub.

<https://github.com/mitre/cti/blob/master/USAGE.md#access-from-the-attck-taxii-server>