Structured Threat Information eXpression — STIX™

A Structured Language for Cyber Threat Intelligence Information

STIX is a collaborative, community-driven effort to define and develop a structured language to represent cyber threat information. The STIX Language conveys the full range of potential cyber threat information and strives to be fully expressive, flexible, extensible, automatable, and as human-readable as possible. All interested parties are welcome to participate in evolving STIX as part of its open, collaborative community.

STIX use cases include:

- **Analyzing Cyber Threats**
- **Specifying Indicator Patterns for Cyber Threats**
- **Managing Cyber Threat Prevention and Response Activities**
- **Sharing Cyber Threat Information**

STIX and TAXII

Trusted Automated eXchange of Indicator Information (TAXII™) is the preferred method of exchanging information represented using the STIX Language, enabling organizations to share structured cyber threat information in a secure and automated manner.

Challenge

Organizations today must maintain a "cyber threat intelligence" capability as a key part of their defense against determined cyber adversaries. Examples of cyber intelligence include understanding and characterizing information such as what sort of attack actions have occurred and are likely to occur; how can these actions be detected and recognized; how can they be mitigated; who are the relevant threat actors; what are they trying to achieve; what are their capabilities, in the form of tactics, techniques, and procedures (TTP) they have leveraged over time and are likely to leverage in the future; what sort of vulnerabilities, misconfigurations, or weaknesses they are likely to target; what actions have they taken in the past; etc.

A key component of success for this capability is information sharing with partners, peers, and others they select to trust. But while cyber threat intelligence and information sharing can help focus and prioritize the use of the immense volumes of complex cyber security information organizations face today, they have a foundational need for common, structured representations of this information to make it tractable.

Solution

STIX is a community-driven solution to this, providing structured representations of cyber threat information that is expressive, flexible, extensible, automatable, and readable. STIX enables the sharing of comprehensive, rich, "high-fidelity" cyber threat information across organizational, community, and product/service boundaries. STIX extends simple indicator sharing to enable the management and exchange of significantly more expressive sets of indicators as well as other full-spectrum cyber threat information.

STIX Language

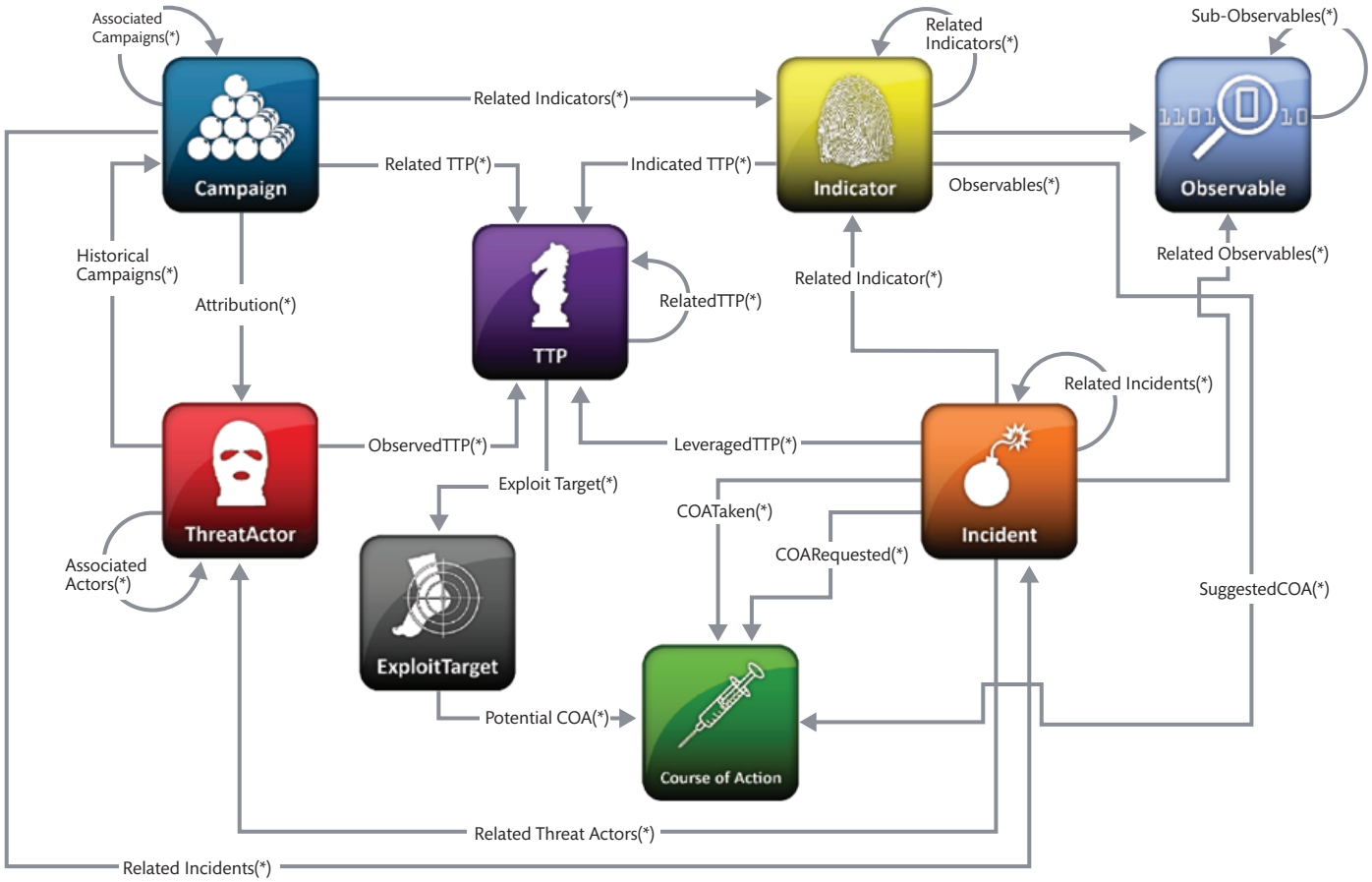
The STIX Language is a community effort being developed in collaboration with any and all interested parties for the specification, capture, characterization, and communication of standardized cyber threat information. It does this in a structured fashion to support more effective cyber threat management processes and application of automation.

STIX provides a common mechanism for addressing structured cyber threat information across and among a wide range of use cases improving consistency, efficiency, interoperability,

STIX™

stix.mitre.org

STIX 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 STIX website, community engagement, and discussion lists to enable open and public collaboration with all stakeholders.



STIX Architecture

and overall situational awareness. In addition, STIX provides a unifying architecture tying together a diverse set of cyber threat information including:

- Cyber Observables (e.g., a registry key is created, network traffic occurs to specific IP addresses, email from a specific address is observed, etc.)
- Indicators (potential observables with attached meaning and context)
- Incidents (instances of specific adversary actions)
- Adversary Tactics, Techniques, and Procedures (including attack patterns, malware, exploits, kill chains, tools, infrastructure, victim targeting, etc.)
- Exploit Targets (e.g., vulnerabilities, weaknesses or configurations)
- Courses of Action (e.g., incident response or vulnerability/weakness remedies)
- Cyber Attack Campaigns (sets of Incidents and/or TTP with a shared intent)
- Cyber Threat Actors (identification and/or characterization of the adversary)

To enable such an aggregate solution to be practical for any single use case, existing structured languages may be leveraged where appropriate such as Cyber Observable Expression (CybOX™), Malware Attribute Enumeration and Characterization (MAEC™), Common Attack Pattern Enumeration and Classification (CAPEC™), etc., and numerous flexibility mechanisms are designed into the language.

In particular, almost everything in this definitively-structured language is optional such that any single use case could leverage only the portions of STIX that are relevant for it — from a single field to the entire language or anything in between — without being overwhelmed by the rest.

Feedback Requested

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