STIX 2.0 Specification - Pre-Draft

Cover Page - Version 0.1

Document Table of Contents

STIX 2.0 Documents

The STIX 2.0 pre-draft specification has been broken up into the following Google documents to make it easier to work on.

1. STIX Core Concepts
   a. Definitions
   b. STIX Concepts
   c. Core Types
   d. Common Properties
   e. Common Relationships
   f. Common Types
2. Top-Level Objects
   a. Non-cyber-concepts
      i. Report
      ii. Package
      iii. Relationship
      iv. Marking-Definition
   b. TTPs
   c. Exploit Targets
   d. Standard TLOs
3. Vocabularies
4. Playground

Overview

<add description>

Document Conventions

Font Colors and Style

The following color, font and font style conventions are used in this document:

- The `Consolas` font is used for all type names, property names and literals.
  - type names are in red with a light red background - `package`
  - property names are in bold style - **`created_at`**
  - literals are in green with a green background - `IP Watchlist`
  - as kinds of relationship are string literals, they will also appear in green with a green background - `related-to`
- In property tables if the property is being redefined from an inherited value in some way, then the background is dark grey.

All type names, property names and literals are in lower-case. Words in property names are separated with an underscore (_), while words in type names and string enumerations are separated with a dash (-).

Examples are included, using the JSON MTI serialization. They are in `Consolas` 9 pt font, with black text and a light blue background. JSON examples have a 2 character space indentation.

Development Status

Each physical documents contains a table that defines 4 levels of development for each TLO and CTI concept. The first level is called Concept. Content coming in to one of the documents starts as a Concept. Once the community starts to work on it it will move to Development. During this phase, the group will flesh out the design and come up with normative text. As the group comes to general consensus the TLO will move to a Review phase. During this phase the community can comment and offer suggestions on the normative text and design. After a period of time of no comments or feedback, the TLO will move to its final stage of Draft.

Contributors (alphabetical)

Sean Barnum
Aharon Chernin
Trey Darley
Mark Davidson
Jane Ginn
Ivan Kirillov
John-Mark Gurney
Bret Jordan
Terry MacDonald
Richard Piazza
Marlon Taylor
Allan Thomson
John Wunder

Feature Roadmap

Green = Consensus is MVP
Red = Consensus is not MVP
White = TBD

Capability	2.0	2.x	Never
Relationships			
Standardized Relationships Relationships pre-defined in STIX	13		
User-Defined Relationships Ability to use relationships that were not pre-defined in STIX	9	2	
Indicator Use Cases			
Indicators Basic indicator object	15		
CybOX Indicator Patterns Use of "native" CybOX patterning for indicator patterns	10	2	
Third-Party Indicator Patterns	7	4	2+1

Use of Snort, Yara, OpenIOC, and other signature formats as patterns			
Sightings Ability to create and share sightings of indicators, however it's done	11	2	
Incident Use Cases			
Incident Basics Just the basics needed to track incidents	12		
Asset Stub A stub of an asset model, abstracted out of Incident, likely a pointer	3+6	3	1+1
Complete Asset Model A more complete asset model that defines many fields		2+7	5
Advanced Incident Impacts, detailed analytics, etc.	2	8	
"Investigation" (pre-incident) Something to track "events", "investigations", and other activity that may not be an incident yet.	2+1	7	2
Analysis Objects			
Attack Patterns See STIX 1.2 AttackPatternType	8	4	
Exploits See STIX 1.2 ExploitType (note: NOT ExploitTargetType)	3+2	7	
Kill Chains See STIX 1.2 KillChainType and KillChainPhaseType	8	4	
Malicious Infrastructure See STIX 1.2 InfrastructureType	10	3	
Malicious Tool See STIX 1.2 ToolType	10	3	
Malware See STIX 1.2 MalwareType	10	3	?
Persona See STIX 1.2 PersonasType (was just an identity)	8	5	
Victim Targeting See STIX 1.2 VictimTargetingType	9	1	2

Configuration/Misconfiguration See STIX 1.2 ConfigurationType	6	7	
Vulnerability See STIX 1.2 VulnerabilityType	10	2	
Weakness See STIX 1.2 WeaknessType	6	6	
Attribution & Tracking			
Threat Actor See STIX 1.2 ThreatActorType	13		
Campaign See STIX 1.2 CampaignType	10	2	
Intrusion Set Representation of intrusion sets, separate from actors and campaigns	1	2+4	
Response Actions			
Course of Action See STIX 1.2 CourseOfActionType	11	1	
Automated Course of Action Structured representation for automating courses of action	1	5+6	1
Data Markings			
Object-Level Markings Markings applied to a complete top-level object (Level 1 Markings)	13	1	
Field-Level Markings Markings applied to individual fields within objects (Level 2 Markings)	3	7	2
TLP Marking Definition Representation of a TLP marking	12	1	
Copyright/TOU Marking Definition Representation of Copyright/TOU markings	12	1	1
Consensus "STIX Default" Marking Definition Representation of a more complete, consensus, "better than TLP" marking	1	6	2 + 4
Cross-Cutting Capabilities			
Packaging around TLOs (Package object)	12	1	

STIX "package" object, whatever that turns into			
Reports Report object	12		
Internationalization Support for STIX content in multiple languages/localizations	5	9	
Basic Identity Small set of critical properties	12	1	
Full Identity Extensive identity representation, similar to CIQ	3	8	2
References/Sources References to non-STIX content and information sources	11		1
Defensive Tools Representation of information about tools used for defense or to create content.	6	4	2
Rich Text HTML, Markdown, or some other rich text format for descriptions	4	7	2
Versioning Ability to version and revoke content	9	4	1
Vendor-Defined Fields Definition and conformance for how vendors can extend STIX	11	3	
Representing Confidence Representation of confidence in the accuracy of information	11	2	
Representing Impact / Potential Impact Representations of actual or potential impact of threats (e.g. for malware)	5	7	1
Custom Vocabularies Ability to use custom (non-standard) vocabularies in places we have standard vocabularies defined	10	3	1
Opinion/Assert Object Ability to represent opinions / assertions about STIX content created by others	4	9	1
STIX Request/Response Ability to create asynchronous STIX requests and responses for information beyond a single TAXII server	1	9	4

Generic Tagging Ability to tag STIX top-level objects with generic text	4	7	2
Granular Capabilities			
Each Controlled Vocabulary For each controlled vocabulary, we need to decide if coming up with vocab values is MVP			
Defined relationships for each object For each object, we need to come up with a set of defined relationships that are MVP.			
Each extension point For each defined extension point (not vendor-defined fields, but things like STIX 1.2 extensions) we need to decide if that extension point is MVP and which extensions for it are MVP.			

Gap Analysis

Document conventions are the same, except a term in `Courier` font indicates a STIX 1.2 concept.

General

- Removing short description
- Relationships/references instead of inline
- `Information_Source` is partially covered by **`created_by_ref`**
- `Statement` - Is it related to Opinion?
- `Confidence` - needs definition
- How does CIQ fit in?
- `Related_Packages` has already been deprecated
- Are self-referential relationships still needed (used for Versioning in STIX 1.2)?

STIX Package

- Profiles not in MVP 2.0
- Leaving off embedding packages in other packages

Attack Pattern

no gaps

Assets

- Missing properties: `Business_Function_Or_Role, Ownership_Class, Management_Class, Location, Nature_Of_Security_Effect`
- `Nature_Of_Security_Effect` is used to capture information related to CIA (Confidentiality, Integrity, Availablity, etc.)
- `Structured_Description` becomes **`technical_characteristics`**
- `Type` becomes **`kind_of_asset`**
- Added properties: **`compromised, owner_aware, technical_characteristics`**

Campaign

- Missing properties: `Names, Intended_Effect, Confidence, Activity`
- How does `Intended_Effect` related to **`impact`**
- `Related_TTPs` replaced by `indicates` `relationship`
- All other `Related_*` properties replaced by `related-to` `relationship`
- `Attribution` replaced by `attributed-to` `relationship`

Configuration

- `Potential_COA` could be a `relationship`
- Will CCE ids be used?

Course of Action

- Missing properties: `Efficacy`, `Objective`
- All `Related_*` properties replaced by `related-to` `relationship`
- `Type` becomes **`kind_of_coa`**
- `Parameter_Observables` could be a `relationship`. It seems different than `evidenced-by` `relationship`

Exploit

no gaps

Incidents

- Undefined in 2.0

InformationSource

Covered by `identity` and `external-reference`

- Missing properties :`Role, Contributing_Sources, Time`

Identity

- Missing properties : `Name`
- Properties used in STIX from CIQ: Accounts, Addresses, BirthInfo, ContactNumbers, CountriesOfResidence, Documents, ElectronicAddressIdentifiers, Events, Favourites, FreeTextLines, Habits, Hobbies, Identifiers, Languages, Memberships, Nationalities,

Occupations, OrganisationInfo, PartyName, PartyType, PersonInfo, PhysicalInfo, Preferences, Qualifications, Relationships, Revenues, Stocks, Vehicles, Visas

Indicator

- Third party test mechanisms not currently supported: Snort, YARA, IOC
- Is `Producer` covered by **`created_by_ref`**?
- `Alternative_ID` handled via `external-reference`
- `Valid_Time_Position` replaced by **`start_time`** and **`end_time`**
- Missing properties: `Observable`, `Likely_Impact`, `Sightings`
- `Type` becomes **`kind_of_coa`**
- `Composite_Indicator_Expression`, `negate` replaced by **`pattern`**?
- `Indicated_TTPs` replaced by `indicates` `relationship`
- `Kill_Chain_Phases` replaced by `indicates` `relationship`
- `Suggested_COAs` replaced by `suggested-coa-of` `relationship`
- All `Related_*` properties replaced by `related-to` `relationship`

Infrastructure

Changed name to `malicious-infrastructure`

- `Type` becomes **`kinds_of_malicious_infrastructure`**
- `Observable_Characterization` replaced by `evidenced-by` `relationship`?

Kill Chains

- Missing properties: `name`, `number_of_phases`
- `Kill_Chain_Phase` is replaced by the `has-kill-chain-phase` `relationship`
- `reference` handled via `external-reference`
- Is `definer` covered by **`created_by_ref`**?

Kill Chain Phases

- Missing properties: `name`
- `phase_id` replaced by **`id`**
- Ordinality - it should be a property of the “in-kill-chain” relationship. Do we support that?

Malware

- How does MAEC fit in?
- Missing properties: `Name`
- `Type` becomes `kind_of_malware`

Observable

Changed name to `observation`

- Missing properties: `Keywords`, `Observable_Source`, `Event`, `Observable_Composition`, `Pattern_Fidelity`, `sightings_count`, `negate`
- `Object` may be replace by **`cybox`**

- Added Properties: **start, end**

Persona

Persona is a wrapper for `IdentityType` in STIX 1.2. It is a stub in STIX 2.0.

Report

- All TLOs included via reference only using **report_contains_refs**

Sightings

- **count** was previously associated with `Observable`
- Missing properties: `Description, Reference`
- `Related_Observables` replaced by **observation_refs**
- **first_seen** and **last_seen** replace `timestamp` and `timestamp_precision`
- Is `Source` covered by **created_by_ref**?
- Added properties: **sighting_of_refs** (usually but not restricted to `indicator` refs)

Threat Actor

- `Identity` replaced by a `relationship` `identity-of` to `identity`
- `Observed_TTPs` replaced by a `relationship` `uses` to `ttp`
- `Associated_Campaigns` replaced by a `relationship`(s) `administers, operates, plans` to `campaign`
- `Type` becomes **kind_of_threat_actor**
- Missing properties: `Intended_Effect, Confidence`

Tool

Introduce `malicious-tool`, contains property **tool_information** (or maybe inherits from `tool`)

- `Type` becomes `kinds_of_malicious_tools`
- Missing properties: `Name`
- Should **compensation_model** be moved to `tool`
- Right now `tool` is a stub - so the whole STIX 1.2/CybOX 2.1 `Tool` type is a gap.

Victim Targeting

In STIX 1.2, this is defined as four properties: `Identity, Target_Systems, Target_Information and Targeted_Technical_Details`. In STIX 2.0 (twigs), this was defined using an array property named **targets**. There were three types of targets suggested: `identity-target`, `system-target`, and `information-target`, but their properties were not defined. This corresponds to the first three STIX 1.2 properties.

Vulnerability

- Missing properties: `is_known`, `is_publicly_acknowledged`, `OSVDB_ID`, `Source`, `CVSS_Score`, `Discovered_DateTime`, `Published_DateTime`, `Affected_Software`, `Title`, `Description`
- Should it inherit from `descriptive-properties` to include missing properties `Title`, `Description`?
- `Potential_COA` could be a `relationship`

Weakness

- Missing properties: `Title`, `Description`
- Should it inherit from `descriptive-properties` to include missing properties `Title`, `Description`?
- `Potential_COA` could be a `relationship`