STIX™ and TAXII™: Google Documents

The list of current STIX and TAXII documents in Google Docs.

In Progress

General

1. Project Plans
    a. Post-2.1 Project Plan
    b. Completed STIX 2.1 Project Plan
2. CTI FAQ
3. CTI Work Product Process (Proposal)
4. CTI Extension Process Policy (Operational)
    a. Working Document for Updates
        i. Matrix
    b. (Deprecated) CTI Extension Process (Proposal)
5. Historical Working Call Meeting Notes
6. STIX 2 Issue Tracker
7. TAXII 2 Issue Tracker
8. STIX 2.1 Change Log

STIX Working Documents

1. STIX 2.1 Errata
2. Best Practices Guide
    a. Committee Note
3. Incident Extension Object - proposed for 2.2
4. JSON Signing - evaluate forward progress on this one, follow-up agenda item
5. Using STIX 2 Opinion Objects - check if key concepts made it to best practices (TODO)
6. COA Playbook Object - standards track extension
7. Course of Action Extension - follow-up 2/28 - external reference to 6
8. Course of Action Taken Extension - follow-up
9. Cyber Analytic Extension - w/patterning follow-up, example with Incident and CACAO, review on 2/28
10. Filtering for Defensive Measures and Best Practices - incorporate parts into Best Practices
11. Malware Sample Artifact Extension - to go into common-objects

Approved / Ratified / Final

STIX 2.1 OS

1. Editable source (Authoritative): https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.docx
2. HTML: https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html
3. PDF: https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.pdf

STIX 2.1 Specification - WD 12 - (CS 03)

1. Official publication site WD12
2. Official publication site CS03
3. Google Doc: N/A

STIX 2.1 Specification - WD 11 - (CS 02)

4. Official publication site
5. Google Doc: STIX 2.1 Specification

STIX 2.1 Specification - WD08 - (CS 01)

1. Official publication site
2. Google Doc: STIX 2.1 Specification

TAXII 2.1 Specification - WD10 - (CS 01)

1. Official publication site
2. Google Doc: TAXII 2.1 Specification

TAXII 2.0 Specification - WD02 - (CS 01)

1. TAXII 2.0 Specification

STIX 2.0 Specification - WD03 - (CS 01)

1. Part 1: STIX Core Concepts
2. Part 2: STIX Objects

12. Security Event Extension Object - follow-up, compare with OCSF
13. STIX 2.x Semantic Equivalence - proposed for committee note
14. STIX 2.x Sightings: Practical Applications and Usage - some concepts incorporated into Best Practices
15. Historical
    a. STIX 2.1 - Working Draft for CS02
    b. STIX 2.1 Future Ideas and Concepts
    c. STIX Playground
    d. Cyber Observables Playground
    e. STIX Archived Content
    f. Cyber Observables Working Concepts
    g. Hypothesis Proposal

TAXII Working Documents

1. TAXII Playground

Interoperability

1. STIX 2.1 Interoperability Test Document Part 1 V0.1
2. STIX/TAXII 2.1 Interoperability Test Document Part 2 V0.1

Feature Sponsor SDO POCs: Working Documents

Tracking Document - STIX 2.1 SDO Sponsors
CTI-TC - Sponsors Working Document 1.0 Attestation Template - WD01
Attestation walkthrough

1. CTI Confidence Property - Sponsors Working Document 1.0 - WD01 [Completed]
2. CTI Opinion SDO - Sponsors Working Document 1.0 - WD01 [Completed]
3. CTI Note SDO - Sponsors Working Document 1.0 - WD01 [Completed]
4. CTI i18n - Sponsors Working Document 1.0 - WD01 [Completed]

3. Part 3: Cyber Observables Core Concepts
4. Part 4: Cyber Observable Objects
5. Part 5: STIX Patterning

Interoperability

1. STIX 2.1 Interoperability Test Document Version 1.0 Committee Specification Draft 01 DOCX HTML PDF
2. STIX 2.0 Interoperability Test Document Part 1
3. STIX 2.0 Interoperability Test Document Part 1 v1.1
4. STIX 2.0 Interoperability Test Document Part 2
5. STIXPreferred Operating Rules

5. CTI Location SDO - Sponsors Working Document 1.0 - WD01 [Completed] 6. CTI COA SDO - Sponsors Working Document 1.0 - WD01 7. CTI Grouping SDO - Sponsors Working Document 1.0 - WD01 8. CTI Infrastructure SDO - Sponsors Working Document 1.0 - WD01 9. CTI Malware SDO - Sponsors Working Document 1.0 - WD01 [Completed] 10. CTI Malware Analysis SDO - Sponsors Working Document 1.0 - WD01 11. CTI SCOs As Top-Level Objects - Sponsors Working Document 1.0 - WD01 12. CTI SCO Relationships - Sponsors Working Document 1.0 - WD01 13. CTI Deterministic IDs - Sponsors Working Document 1.0 - WD01	

Feature Status and Roadmap

The following table includes current roadmap items, their status, and their proposed release target. The definition for each status is listed below

1. Concept: The TC has been made aware that a mini-group or group of sponsors for this topic has been formed and is working on a concept to bring to the TC as a formal proposal to be accepted as an official work product item.
2. Accepted: In order for a feature or concept to be accepted by the TC, it must have at least 2 sponsors that are willing to work on the topic and drive it to completion. The topic has been accepted by the TC as an official work product item. However, it has not yet been officially picked up by the TC to be worked on. The topic may have some concepts or proposals, but it is not yet under active development.
3. Paused: Official work by the TC has started and has since stopped or been placed on hold.
4. Development: The development work for this topic is underway and work is being done during working calls, email, and slack.
5. Review: The development work is done and the topic needs to be reviewed and submitted to the Full TC for acceptance in to a specific release. Before the feature or concept can be proposed to the Full TC all specification text must be completed.
6. Draft: The feature or concept has been accepted into a specific release and is waiting for the CSD ballot.
7. CSD Approved: The feature has been approved as a CSD and is waiting for the Interop tests and Implementations to be completed.
8. Finished: The feature or concept is done and ready for acceptance into a CS release.

Feature	Sponsors (2+ required, more is better)	Implementations (2+ required, more is better)	Interoperability Tests	Initial CSD	Status	Exp Date
Confidence	DHS, Individual	DHS, Individual	DHS, Individual	CSD01	DONE	April 2, 2019
Opinion	DHS, JP Morgan, CTIN, Perch	DHS, JP Morgan, CTIN, Perch	DHS, JP Morgan, CTIN, Perch	CSD01	DONE	April 2, 2019
Note	DHS, JP Morgan, CTIN	DHS, JP Morgan, CTIN	DHS, JP Morgan, CTIN	CSD01	DONE	April 2, 2019
i18n	Fujitsu, New Context	Fujitsu, New Context	Fujitsu, New Context	CSD01	DONE	April 2, 2019
Malware	DC3	DC3		**CSD02**	DONE	
Location	DHS, Darklight	DHS, Darklight	DHS, Darklight	CSD01	DONE	April 2, 2019

TC Roadmap

.

Proposed for STIX 2.1.1

Issues labeled Target: STIX 2.1.1 in GitHub

Item	Reference	Consensus Achieved
Incident extension	https://github.com/oasis-open/cti-stix-common-objects/tree/main/extension-definition-specifications/incident-core	Do not include in an errata wholesale, consider by reference (as below)
Pointer to endorsed extensions - Incident, Identity Context, Malware Sample Artifact		Pending - needs proposed text
Pointer to external extensions - TLP 2.0		Pending - needs proposed text
309	https://github.com/oasis-tcs/cti-stix2/issues/309	Yes
307	https://github.com/oasis-tcs/cti-stix2/issues/307	Yes
301	https://github.com/oasis-tcs/cti-stix2/issues/301	Yes
299	https://github.com/oasis-tcs/cti-stix2/issues/299	Yes
297	https://github.com/oasis-tcs/cti-stix2/issues/297	Pending - The bulk of the issue will be addressed in 2.2 with a full review of SCO relationships. For 2.1.1, the relationships were added to Appendix B.
294	https://github.com/oasis-tcs/cti-stix2/issues/294	Pending approval of text that Sean proposed
~~293~~	~~https://github.com/oasis-tcs/cti-stix2/issues/29~~	~~Move to 2.2~~

	~~3~~	
Issue 292 Errata in Table 6.6.1	https://github.com/oasis-tcs/cti-stix2/issues/292	Yes
291	https://github.com/oasis-tcs/cti-stix2/issues/291	Yes, request for objections
290	https://github.com/oasis-tcs/cti-stix2/issues/290	Yes, request for objections
289	https://github.com/oasis-tcs/cti-stix2/issues/289	Yes
281	https://github.com/oasis-tcs/cti-stix2/issues/281	Yes
278	https://github.com/oasis-tcs/cti-stix2/issues/278	Yes
277	https://github.com/oasis-tcs/cti-stix2/issues/277	Pending
275	https://github.com/oasis-tcs/cti-stix2/issues/275	Yes
274	https://github.com/oasis-tcs/cti-stix2/issues/274	Yes
270	https://github.com/oasis-tcs/cti-stix2/issues/270	Yes

Proposed for STIX 2.2

Item/Topic	Reference	Status
Incident extension - standards track, full inclusion in the specification		Accepted in common objects repo

JSON Signing		TBD
Malware Sample Artifact		Accepted in common objects repo
Security Event Extension		TBD
293	https://github.com/oasis-tcs/cti-stix2/issues/293	Pending
297	https://github.com/oasis-tcs/cti-stix2/issues/297	Pending
308	https://github.com/oasis-tcs/cti-stix2/issues/308	Pending

Roadmap leading up to STIX 2.1 / TAXII 2.1

STIX 2.1: Development complete June 2021
TAXII 2.0: Development complete April, 2017

Topic	Status	Release	Contacts	LOE
Location	Complete	STIX 2.1		2
Event (Grouping)	Development	STIX 2.1		4
IEP	Mini-Group	STIX 2.1	POC: Terry MacDonald Slack: #stix Comments	4
DNS Request / Response	Development	STIX 2.1		3
Device	Development	STIX 2.1+		4
Firmware Extension	Development	STIX 2.1+		4

Operating System Extension	Development	STIX 2.1+		4
Network Share Extension	Development	STIX 2.1+		4
Digital Signatures	Mini-Group	STIX 2.2+	POC: John-Mark Gurney Slack: #signatures Google Doc	5
Echo Detection	Mini-Group	STIX 2.2+	POC: Rich Struse Slack: #stix	4
Classifications / Risk Scores	Development	STIX 2.2+	POC: Jason Keirstead	6
Passive DNS	Paused	STIX 2.2+ or never		4
Actions (potential dependency of: malware)	Paused	STIX 2.2+		4
Patterning: • External Lists • Basic Operations • Variables & Back References	Mini-Group	STIX 2.2	POC: John-Mark Gurney, Jason Keirstead Slack: #patterning	3-4
Patterning: • Data Source Specification	Mini-Group	STIX 2.2+	POC: John-Mark Gurney, Jason Keirstead Slack: #patterning	4
Patterning: • Actions • STIX-based Patterning	Paused	STIX 2.3+	Slack: #patterning	5
TAXII Channels	Paused	TAXII 2.2	Slack: #taxii	4

TC Process

Work on the core specifications (STIX and TAXII) follows the following rough process:

1. A mini-group is formed to work on an issue and come up with a rough proposal
2. The mini-group presents their work on a working call for a sanity check and to get it accepted into a release. When the work is accepted into a release, it is prioritized and added to the roadmap as a planned item.
3. Roadmap items are addressed in priority order via discussions on working calls, Slack, and e-mail.
4. When a roadmap item is completed it is presented at a TC call for acceptance into a draft.
5. The editors move the item into the draft.

Mini-Groups

If you have a project, proposal, or change that you would like to see added into STIX/TAXII, you should take the initiative and start a mini-group on that topic. Mini-groups are formed to make rapid progress and come up with a proposal for the broader community. They do their work publicly on Slack and in calls, but not on TC-wide working calls.

The mini-group process is:

1. Contact a co-chair to give them notice that work on a topic is proceeding. They will add the item to the roadmap tagged as Mini-Group, indicating that a mini-group is formed and providing contact information.
2. Post to the e-mail list and Slack that the mini-group is forming. Gather interested parties and schedule meetings to work on the topic.
3. Mini-groups are responsible for producing the following material. Note that it does **NOT** need to be fully polished and complete...it just needs to be enough that the TC can decide that it makes sense for the release and that they can pick it up and finish it.
    a. Scope: what does the proposal solve? What does it not solve?
    b. Summary of Changes: what would the proposal require changing, at a high level
    c. Open issues: what still needs to be decided or was contentious in the mini-group?
    d. Proposal: normative text, property tables, and any content that needs to go into the specification
4. When the mini-group feels they have enough of the above to bring the work to the broader TC, contact a co-chair to schedule 15 minutes during the working call to present the topic.
5. The mini-group presents their work to the TC for acceptance as a work item. The TC can decide to accept it, defer it to a later release, or to reject it. If the TC decides to accept it for the current release, it will be prioritized in the roadmap as Planned and, when the items ahead of it are finished, discussed on a working call.
6. The mini-group can continue to iterate on the topic while it is in the backlog. In particular, the more work the mini-group does on the proposal to get it finalized the quicker it can be accepted by the TC and completed.

Note: All mini-group work should be open to the TC. Please post meeting information to the e-mail list or Kavi with as much notice as possible and have discussions in public Slack channels.

Working Call Process

When a mini-group finishes a proposal, it's accepted onto the roadmap, and it comes time to discuss it the proposal will be scheduled on the regular working calls and marked as Development. Working calls are typically led by either the co-chairs or by a mini-group leader (depending on what makes the most sense for that topic).

The working call process is simply to finalize the proposal such that it is complete, polished, and ready to move into the draft release. That state can be achieved by consensus (most people agree) or by ballot. At that point, the status in the roadmap is changed to Review.

Once the proposal is completed on the working calls, it is brought up on a monthly TC call. On that call, the SC co-chairs present the topic to the TC and ask for unanimous consent or a ballot to move it into the drafts. If the ballot passes or unanimous consent is achieved, the editors move the material into the drafts and mark the item as Draft in the roadmap.

Note: The co-chairs and editors are ultimately responsible for the quality of work in the releases. As such, editors may ask that the TC continue to refine a proposal or may ask for an editorial call to refine it with the group.

Design Goals

Note: Clarity and Modularity were agreed upon at the F2F, Pragmatism and Analysis are under discussion

1. Clarity
    a. Easy to implement and understand
    b. One way to perform a use case where possible
    c. Simple things should be simple, simple is better than complex
    d. Avoid excessive nesting
    e. Well understood definitions
    f. Consistent structures and names
    g. Explicit is better than implicit
2. Modularity
    a. Provide building blocks that can be reused elsewhere
    b. Ensure tight cohesion, and low coupling of those building blocks
    c. Support customization in a consistent way
    d. Use semantic versioning
3. Pragmatism
    a. Concentrate on current problems not theoretical ones
    b. Focus on the common problems not the edge cases (the 80/20 rule)
    c. Work on improving the edge cases in subsequent releases
4. Analysis
    a. Enable sharing of higher order analysis
    b. Make it easy to graph relationships
    c. Make it easy to track changes over time

Upcoming Events

Below is a list of upcoming events that may impact future CTI meetings and F2F sessions. A list of other InfoSec conferences can be found here: https://infosec-conferences.com/

2023	Event

Events that we need to be generally mindful of
RSA
FS-ISAC
ENISA
Blackhat
Defcon
BruCON

Document Archive

Below is a list of older documents that were approved by the CTI TC

TAXII Documents

TAXII 2.0 Specification - WD01 (CSD)

Approved as a Committee Specification Draft on Wednesday, 3 May 2017 @ 11:59 pm EDT, CSD01-PR01-Public Comment Resolution Log

1. TAXII 2.0 Specification

STIX Documents

STIX 2.0 Specification - WD02 (CSD)

Approved as a Committee Specification Draft on Wednesday, 3 May 2017 @ 11:59 pm EDT, CSD02-PR01-Public Comment Resolution Log

1. Part 1: STIX Core Concepts
2. Part 2: STIX Objects
3. Part 3: Cyber Observables Core Concepts
4. Part 4: Cyber Observable Objects
5. Part 5: STIX Patterning

STIX 2.0 Specification - WD01 (CSD)

Approved as a Committee Specification Draft on Friday, 3 February 2016 @ 8:00 pm EST, CSD01-PR01-Public Comment Resolution Log

1. Part 1: STIX Core Concepts
2. Part 2: STIX Objects
3. Part 3: Cyber Observables Core Concepts
4. Part 4: Cyber Observable Objects
5. Part 5: STIX Patterning

STIX 2.0 Specification - RC2 (CSD)

Approved as a Committee Specification Draft on
Friday, 2 September 2016 @ 11:59 pm EDT

1. STIX 2.0 Specification RC2