Session #1: 11:00 AM EDT
September 22, 2016*

Session #2: 9:00 PM EDT
September 22, 2016*

CTI TC

Monthly Meeting

UPDATES

* Attendance at **either** Session #1 or Session #2 Counts Towards Voter Eligibility

CTI-TC September Meeting: Agenda

Kick-off Session – Richard Struse, Chair

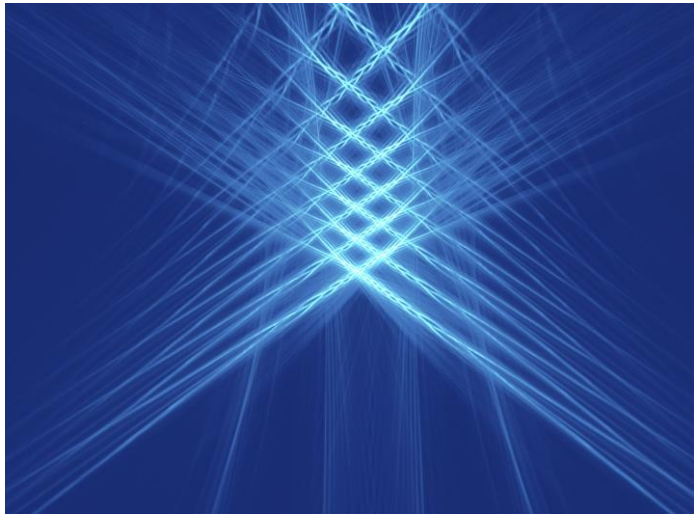
- Updates on STIX 2.0 CSD & Brussels Face-to-Face

CybOX Update – Ivan Kirillov & Trey Darley

STIX Update – John Wunder & Aharon Chernin

Borderless Cyber Tokyo + Meet-up – Rich Struse

Other Items?



Current Status

STIX 2.0 RC2 Committee Specification Draft*

STIX 2.0 RC2 approved as Committee Specification Draft (equivalent)

Brussels Face to Face – Update

- Strong consensus in the room that 2.0 should be a Committee Specification
  - Get public review and comment early
- Discussion of some technical topics
  - Internationalization
  - Location
  - Analyst notes
  - Infrastructure
  - Malware
  - Confidence
  - MISP Taxonomies

Are two standards better than one?

First things first…

- CybOX 3.0 draft is nearly complete!

- Thanks again to all of the feedback, discussions, and participation in our myriad working calls

Now, to the issues at hand

- STIX and CybOX share a common goal of sharing CTI information across both humans and machines
- Historically, CybOX was around before STIX, but is now a core part of it
  - Observed Data
  - Indicators
- There are problems with this current approach:
  - Explaining STIX/CybOX to implementers, marketers, customers, etc. is difficult
    - Most people do not understand what CybOX is, what relationship it has to STIX, and why there are two things mentioned
  - The current dependency between STIX and CybOX means that STIX must be updated each time CybOX is updated in order to incorporate the new version

Proposal

- **Broadly**: CybOX is subsumed by STIX
- CybOX is merged into the STIX 2.0 specification
  - STIX 2.0 RC3
- CybOX goes away as a separate OASIS work product and deliverable
- The CybOX name is deprecated and replaced with “STIX Cyber Observables” (SCO)

- Are there other impacts beyond the merger?
  - STIX Cyber Observables still retains its own sub-committee and leadership
  - New Objects can still be added to the STIX Cyber Observables layer as needed
  - STIX Cyber Observables can be referenced from other specifications (e.g., MAEC) without having to reference STIX as a whole

Benefits

- **Ease of use in implementation**: allows implementers to consider a complete spec of what they have to support as related/consistent content.
- **Simplified testing and interoperability**: all testing is done by STIX version, rather than by a STIX/CybOX matrix
- **Enables better marketing and promotion of the CTI standards**: there will be only a single thing to discuss, i.e. ”STIX 2.0.” No ambiguity or distraction associated with details of what CybOX provides when communicating products that support “STIX”.
- **Streamlines the standards process**: removes some red tape and allows focus on STIX specification as a whole during review, ballots, and processing.

Straw Poll/Discussion

What do **YOU** think?

Path Forward

- We will open a ballot on this issue - expect to see it within a few days
  - Co-chairs/editors will be working closely together to collect community feedback and work through open questions
- If ballot passes:
  - Document editors will be collaborating on the merger of the specifications. There will likely be open questions and “unknown unknowns” to deal with.
  - CybOX SC will be renamed to STIX Cyber Observable SC
  - CybOX SC charter will be tweaked slightly

STIX

PATH FORWARD

Decision Points

1. What is the release philosophy for 2.0?

Running consensus (confirmed at recent working call) is that we should continue the time-based release philosophy and therefore release 2.0 ASAP.

- Fix any bugs
- Remove items we aren't sure are correct
- Add conformance section and references

2. Do we take 2.0 to Committee Specification?

Consensus at the F2F and working call is **yes**, 2.0 should go through public review and be taken to a full committee specification.

- Convert to OASIS templates
- Approve a new CSD with fixes
- Vote to send to public review

Objections to continuing on this path?

Roadmap

Through Mid-October

Update the document:

- Discuss and resolve open issues for 2.0
- Remove features that we can't get right in time (e.g. location attributes)
- Address editorial issues (broken examples, other minor comments)
- Add conformance section
- Implement CybOX merge (to be discussed)

Late October

Convert documents to OASIS templates

Early November

Open ballot to approve CSD

(assumes previous points are confirmed)

Tokyo Meet-up

PROPOSED FOR OCTOBER 31