CTI-TC Monthly Meeting: Session #1

Meeting Date: May 20, 2021
Time: Session #1 Notes + Attendance
Purpose: Monthly CTI TC Meeting
Attendees:

Name	Company	Role
Coderre, Robert	Accenture	Voting Member
Keith, Robert	Accenture	Voting Member
Maxwell, Kyle	Accenture	Voting Member
Fischer, Greg	Anomali	Voting Member
Maroney, Patrick	AT&T	Voting Member
Thompson, Dean	Australia and New Zealand Banking Group	Voting Member
Darley, Trey	CCB/CERT.be	Chair
Ginn, Jane	Cyber Threat Intelligence Network, Inc.	Secretary
Jordan, Bret	Cyber Threat Intelligence Network, Inc.	Voting Member
Casey, Timothy	DarkLight, Inc.	Voting Member
Hohimer, Ryan	DarkLight, Inc.	Member
Patrick, Paul	DarkLight, Inc.	Voting Member
Park, Jackie Eun	DHS Office of Cybersecurity and Communications	Voting Member
Taylor, Marlon	DHS Office of Cybersecurity and Communications	Voting Member
van Belkum, Aukjan	EclecticIQ	Voting Member
Ricard, Chris	FS-ISAC	Voting Member
Noguchi, Kazuo	Hitachi, Ltd.	Voting Member
Guttierrez, Roseann	IBM	Voting Member
Keirstead, Jason	IBM	Voting Member
Lee, Chenta	IBM	Voting Member
Ratliff, Emily	IBM	Voting Member
Desai, Kartikey	Mitre Corporation	Voting Member
Haynes, Danny	Mitre Corporation	Voting Member
Piazza, Richard	Mitre Corporation	Voting Member
Cullinane, Kelly	New Context Services, Inc.	Secretary
Hunt, Chris	New Context Services, Inc.	Voting Member
Caselli, Marco	Siemens AG	Voting Member
Girard, David	Trend Micro	Voting Member
Mates, Jeffrey	US Department of Defense (DoD)	Voting Member

Agenda:

- Introduction & Welcome
- General Announcements
- YAB (Yet Another Ballot)
- STIX and TAXII SC Updates
- Interop SC Updates
- An interesting twist

Meeting Notes:

Trey Darley

Welcome to all - Please record your attendance!

Open Ballot

Trey Darley

- Ballot Issue: Do you approve working draft 12 of STIX v2.1 as CS03 and submitting this CS to the OASIS membership for consideration for OASIS Standard?
- Ballot closes Friday 21 May 23h59 UTC
- This is a super-majority ballot. It is currently passing by one vote, but we can do much better than that!

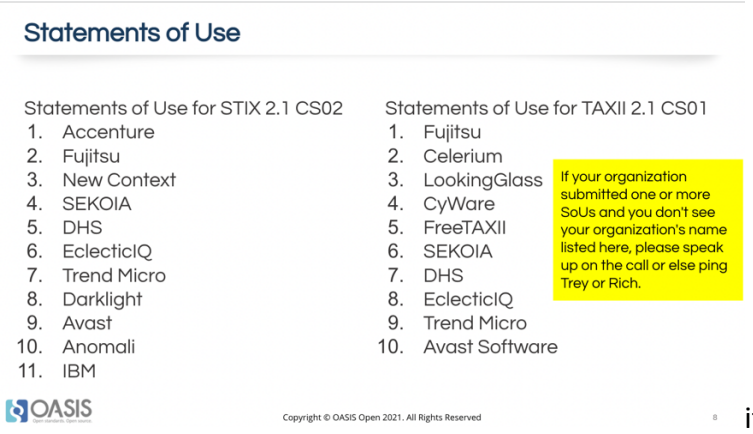
Bret Jordan

- Full OASIS Standards:
  - STIX 21. SC03 Ballot
  - TAXII 2.1
- Verified with Chet what constituted material and non-material in regard to bugs
- Since there were non-material changes, a new ballot was required
- Statements of use do not need to be updated
- No comments for TAXII 2.1 – does not need a ballot
  - This will go out for a call for consent with STIX2.1
- CS03 will be published to website next week by Chet and sent to full OASIS membership to be ratified as full OASIS standard
  - This process usually takes about 2 weeks
  - Mid-end of June they are likely to be fully ratified as full OASIS standards
- 6 standards released in 5 years – this is an amazing feat!

Statements of Use

Bret Jordan

- Statements can still be submitted
  - Need statements within the next week
  - They will be included in Chet's notices to the full OASIS body
- Statements must reference the approved specification and need to be approved by your organization's primary representative to OASIS
- Needs to reference approved spec



ification

Statement of Use Example

<ACME Cyber> has successfully implemented STIX Version 2.1 Committee Specification 02, approved 25 January 2021 and TAXII Version 2.1 Committee Specification 01, approved 27 January 2020, in accordance with the conformance clauses defined in Section 12 and Section 8, respectively. This implementation <did | did not> include the interoperation of multiple independent implementations.

Interop Subcommittee Update
Marlon Taylor

- Issues 262/263 conformance issues were discussed
  - Optional fields not required per conformance
  - Use of "parsing" not defined
- To address in the spec would be a material change
  - Pro: Remove conformance ambiguity loopholes
  - Con: Release Timeline for STIX 2.1
- During public review working call, no objection to address this to a future release of the spec
  - During public review call, we discussed Interop options to relive issues in the interim
    - Pro: No impact to STIX 2.1 release time
    - Con: Not a complete solution
    - Interop currently supports:

Row	Ingest: Keep Original	Process: Translate to internal Data Model	Export Original	Export Processed	Disposition
15	Yes	None	Yes	No	Yes
19	Yes	Some	Yes	No	Yes
20	Yes	Some	Yes	Yes	Yes
23	Yes	All	Yes	No	Yes
24	Yes	All	Yes	Yes	Yes

- Question: Are there any objection to trying to address these via Interop in the interim of future release of STIX specification?
  - No objections on this call to this question
- Regular Interop will resume working calls on May 25th
  - Work has been happening in the background during the open comment period
- STIX 2.1 Interoperability Test Document Part 1
  - Currently updating from extensive comments
    - https://docs.google.com/document/d/1SabxIhjxfg1RAaBj6grsktBzX_UHFI4C8VYStybi-c0/edit
- STIX/TAXII 2.1 Interoperability Test Document Part 2
  - On roadmap - Be sure to review & comment
    - https://docs.google.com/document/d/1_y8pstc26Q511No7Z9Ny-PzEZ0aum_lpAEuq6PvEY0M/edit
- STIXPreferred Website
  - Update Website & Develop Workflows

Trey Darley

- Where do we go from here?
  - Do we change to quarterly meetings? Do we start new work – 2.2? Do we recharter the TC? Do we close the TC?

Marlon Taylor

- Suggested the TC put focus on Interop SC. Possibly work towards a plugfest.

Jason Keirstead

- Agrees with Marlon. Interop needs to become a focus now that implementing is more important. No need to recharter at this point as there is still a lot of work to be done on things like patterning.

Trey Darley

- The charter does not mention the Interop. Is it worth revisiting this issue?

Bret Jordan

- Interop is going to need 4-6 months to finish their current work, including ballot.
- Community events should be considered once the work is complete.
  Open issues are mostly regarding patterning and some objects. This could be a focus moving forward.

Trey Darley

- Thank you everyone for joining. Meeting adjourned.

Meeting Terminated