



CTI-TC Monthly Meeting: Session #2

Meeting Date: June 23, 2022
Time: Session #2 Notes + Attendance
Purpose: Monthly CTI TC Meeting
Recordings: [Meeting Recordings Link](#)
Attendees:

Company	Name	Role
Copado	Hunt, Christian	Voting Member
Australia and New Zealand Banking Group (A...	Thompson, Dean	Voting Member
Fujitsu Limited	Yamada, Koji	Voting Member

Agenda:

- TC Updates
 - STIX SC
 - Interop SC
- ITU Cross Standardization
- Q&A

Meeting Notes:

Rob Coderre

- Welcome! Please record your attendance.
- Seeking members in the following roles:
 - Co-Secretary
 - TAXII SC Chair/Co-Chair
- Please reach out to the co-chairs or listserv for more information

STIX SC Update

Rob Coderre

- [Best Practices Doc](#) contributed by Rich Piazza
 - Many things were punted as a best practice during development of STIX 2.1

- This is a draft doc and is no way complete. Please send your additions.

Dean Thompson

What is the intended use of the Best Practices document? Is it similar to work done in the STIX 1 days?

Rob Coderre

The doc is meant to provide additional guidance and act as a companion to the specs and describe how to use the data fields and relations, with an eye towards helping implementers put together usable and descriptive STIX content.

Interop SC Update

Kartikey Desai

Plugfest

- Occurred 15-17 June
- Tested the interoperability of STIX and TAXII tools, per the STIX 2.1 and TAXII 2.1 Interoperability standards
- Sponsored and hosted in-person by Peraton, with MITRE, Peraton, and Fujitsu participating!
- Personas tested:
 - Fujitsu | TIP2, SIEM2
 - Peraton | TIP2, MAS2, SXP
 - MITRE | SXC, SXP
 - All orgs had a TXC and TXS
- 169 total STIX sessions/connections between the various systems
 - With additional sessions specifically for testing TAXII 2.1 Interoperability
- Continuation of PlugFest, focused on TAXII 2.1 Filtering, will be scheduled soon

Lessons Learned

- Testing
 - Have pre-defined common set of STIX 2.1 objects and TAXII 2.1 requests
 - Try for automated test suite to enable rapid results verification
 - Need to ensure connectivity issues resolved prior to PlugFest

Tools

- Various bugs discovered
- Potential ideas sharing about UI and other features
- Realized some opportunities for increased efficiencies

Interoperability Standards

- Identified few potential areas for improving clarity
 - e.g., the trailing URL slash '/'

Dean Thompson

Is there a library of predefined STIX objects for use by the participants? Or did participants bring their own data?

Kartikey Desai

There was not a specific repository of STIX object data for use by all participants, but that is definitely a recommendation for the next PlugFest. The InterOp documents do have test data, but that data is not

OASIS CTI-TC Monthly TC Call

easily consumable as code at this time, and that is a project someone should take up to make that available via the GitHub repositories.

Dean Thompson

Did the PlugFest use cases test out object deletion and revocation?

Kartikey Desai

While the focus was primarily on higher order operations, there are specific use cases defined in the InterOp specification for testing object modify / delete / revocation scenarios. PlugFest specifically focused on the ability to send / ingest data between implementations, and did not dictate how an individual implementation internally consumed the information.

Koji Yamada

Will OASIS publicize the PlugFest results via social media or press release as was done for the STIX 1.1 PlugFest?

Rob Coderre

We can ask OASIS if that is something they want to pursue. We welcome any write ups from the participants in the PlugFest.

ITU-T Cross-Standardization

Rob Coderre

Where are we in the process?

- TC Motion to proceed - passed on 19 May
- TC to submit official request to OASIS staff - completed on 25 May
- OASIS will conduct a Special Majority Vote to approve the submission of request to the OASIS President
 - Ballot opened on 16 Jun
(<https://www.oasis-open.org/apps/org/workgroup/cti/ballot.php?id=3706>)
 - Ballot closes on 23 June at 11:59pm UTC (Currently 23 votes in favor, needed 20)

What is next?

- Upon Special Majority Vote passage, OASIS will open a 15-day staff review period
- Next, a public 30-day call for comment to OASIS membership occurs
- Post this comment period, if there are no issues, the President has up to 15 days to approve/reject the submission.
- If approved, 15 days to submit to ITU, then the ITU review and approval process takes over...

Dean Thompson

What does the ITU-T approval process look like? And how involved is it?

Rob Coderre

Great question and I don't know the answer. I will reach out to Jamie Clark and Duncan Sparrell for more info and reply back to the listserv.

Rob Coderre

Thank you for joining and see you next month.

Meeting Terminated

.....