CTI-TC Monthly Meeting:  
Session #2

Meeting Date:  
September 15, 2022

Time:  
Session #2 Notes + Attendance

Purpose:  
Monthly CTI TC Meeting

Recordings:  
Meeting Recordings Link

Attendees:

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hunt, Christian</td>
<td>Cyber Threat Intelligence Network, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Lumi, Qem</td>
<td>Peraton</td>
<td>Observer</td>
</tr>
<tr>
<td>Relitz, Stephen</td>
<td>Peraton</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Rosa, Michael</td>
<td>National Security Agency</td>
<td>Observer</td>
</tr>
</tbody>
</table>

Agenda:
- Welcome
- ITU Cross Standardization Update
- TC Updates
  - STIX SC
  - TAXII SC
- Q&A

Meeting Notes:
Marlon Taylor
- Welcome & Record your attendance

ITU Cross Standardization
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
- 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... Preliminary package delivered to ITU on 1 September.

What is happening now?

- The ITU has responded to OASIS on 2 September 2022
  - ITU-T SG17 will take up discussion of accepting STIX/TAXII as ITU standards as STIE and TAEII
  - There are concerns with the trademarks associated with STIX and TAXII
- What does this mean?
  - History: Bringing STIX/TAXII into OASIS back in 2015, OASIS and US DHS were unable to come to agreement on transferring the intellectual property rights (trademarks) to OASIS, leading to a potentially “encumbered IPR” scenario
  - To solve this issue, DHS granted a licence to use the STIX/TAXII terms (while retaining ownership) and OASIS Board of Directors accepted this license grant (see https://www.oasis-open.org/committees/cti/ipr.php)
  - Every time we issue a revision of the standards, the OASIS BoD needs to explicitly waive OASIS IPR rules and allow the special license grant.
What Are Our Options?

- TC leadership is working with OASIS and our ITU liaison (Duncan Sparrell) to identify next steps

- As of now, these are:
  - A: Negotiate with the original contributors (US DHS/CISA) about removal of the trademark license and restrictions, so that no third party trademark claim obstacle remains to the Study Group’s hesitancy to proceed.
  - B: Negotiate some kind of paring back of the same license, short of complete removal. We're not yet sure if that approach would address ITU-T’s concerns.
  - C: Accept the Study Group’s implied suggestion that the name of the works be modified slightly so that there no longer is any question of infringement of the trademarked names.
  - D: Withdraw the submission.

Timelines

- ITU-T SG17 has indicated they will take up STIX and TAEII at their next work session in March 2023.
  - Duncan Sparrell and Michael Rosa are the designated editors

- HOWEVER, we cannot stay idle until then.

- We need to find a solution to the IPR issue prior to the end of 2022
  - Ideally, we will have a solution (one of the aforementioned options) finalized by late October / early November.

- PLEASE GET INVOLVED!

Marlon Taylor
Mike, do you know about any other similar standards being considered by the ITU?

Mike Rosa
Yes, heard of the same standard was discussed this morning. ITU seems to have been waiting for STIX/TAXII for a while so that may have opened the door for other options.

Marlon Taylor
Benefits of the ITU would be the infrastructure and reach they have. They will provide translation services which will help with adoption and expansion.

Kelly Cullinane

Motion from this morning session:

- **MOTION:** Sean Carroll moved in the am session that a tiger team be set up to present a letter/proposal in 2 weeks time to a special session of the TC. In turn, the TC will either adopt, reject, amend this letter/proposal. In the interim the tiger team is empowered to, and can set up electronic ways to poll membership about the 4 presented choices to ensure the letter is in line with the TC’s feelings as a whole. This work product, once approved by the TC at a special session, is geared to OASIS to inform them of the TC's desires.
- **MOTION SECONDED by Jeff Mates**

Voting was conducted by raising hands in zoom

Quorum achieved: No - 7% of voting members were present at this session. 2 eligible voters were present at the time of the vote.

- Yes/In Favor: 2
- Abstain: 0
- No/Against: 0

Cumulative Voting Results:

Quorum Achieved: Yes - 71% of voting members present between the two sessions. 20 eligible voters were present between the two sessions.

- Yes/In Favor: 16
- Abstain: 4
- No: 0

The motion passes

Marlon Taylor

Please reach out to the Co-Chairs if you want to be on the tiger team
- Michael Rosa volunteered to be on the tiger team

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
All info is on the slide. Main order of business is to hold a voice vote to publish the best practices document as a committee note.

Voting was conducted by raising hands in zoom
Quorum achieved: No - 7% of voting members were present at this session. 2 eligible voters present.
Yes/In Favor: 2
Abstain: 0

Cumulative Voting Results:
Quorum Achieved: Yes - 71% of voting members present between the two sessions. 21 eligible voters were present between the two sessions at the time of voting.
  - Yes/In Favor: 20
  - Abstain: 1
  - No: 0
The motion passes.

FAQs are done. Please let the WG know if you have any additions.
OpenSSF Scorecard results - ran this against open repos.

Marlong Taylor
Any findings that we should know about?

Emily Ratliff
No major findings, did a couple of small updates. For example - branch protection on the main branch of the repos with Chet’s assistance. Enabled CodeQL scanning, very few results. Shows that the repos have been well maintained. We can serve as a best practices leader in this area.

Marlon Taylor
Is there a way to know what the scoring criteria is before we do a commit? This will help us keep this status.
OASIS CTI-TC Monthly TC Call

Emily Ratliff

CodeQL has this feature. This feature is enabled. The score gets recomputed weekly. Can click on our badge and see how the score was achieved.

TAXII SC Update

Marlon Taylor

PlugFest Part 1 - Recap

- 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

PlugFest Part 2 - TAXII Filtering Recap

- Occurred 30 August
- Tested TAXII 2.1 Filtering
  - Basic Filtering
  - Relationship Match
  - Calculation Match
- Virtual with Fujitsu, MITRE, and Peraton
  - TXCs from MITRE & Fujitsu
  - TXSs from Fujitsu & Peraton
- Groundwork to enable more efficient testing:
  - Common set of STIX Objects to filter against
  - Common set of TXC requests
  - Expected results
PlugFest 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
- Some TXC (e.g., Python-based) cannot support full Filtering capabilities

Interoperability Standards
- Identified few potential areas for improving clarity
  - e.g., the trailing URL slash ‘/’
- General errata
- Clarifications regarding implications of: Versioning for certain properties;
  Tiered Filtering with common property names, on implementations

Looking Forward

- Host more PlugFests
- More participating organizations
- Create more-automated test suite(s) for use:
  - During PlugFests
  - Potentially make available a fully-contained test suite for orgs to use
    for individual testing outside of PlugFests
- Revision(s) to the Interoperability Test Documents
- OASIS socialization of PlugFests