CTI-TC Monthly Meeting: Session #1

Meeting Date: June 23, 2022

Time: Session #1 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>Beck, Desiree</td>
<td>Mitre Corporation</td>
<td>Member</td>
</tr>
<tr>
<td>Carroll, Sean</td>
<td>National Security Agency</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Caselli, Marco</td>
<td>Siemens AG</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Casey, Timothy</td>
<td>DarkLight, Inc.</td>
<td>Member</td>
</tr>
<tr>
<td>Coderre, Robert</td>
<td>Accenture</td>
<td>Chair</td>
</tr>
<tr>
<td>Cullinane, Kelly</td>
<td>Copado</td>
<td>Secretary</td>
</tr>
<tr>
<td>Darley, Trey</td>
<td>Accenture</td>
<td>Chair</td>
</tr>
<tr>
<td>Desai, Kartikey</td>
<td>Mitre Corporation</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Ginn, Jane</td>
<td>Cyber Threat Intelligence Network, Inc. (C...</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Girard, David</td>
<td>Trend Micro</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Haynes, Danny</td>
<td>Mitre Corporation</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Jones, Elysa</td>
<td>Individual</td>
<td>Member</td>
</tr>
<tr>
<td>Keirstead, Jason</td>
<td>IBM</td>
<td>Member</td>
</tr>
<tr>
<td>Keith, Robert</td>
<td>Accenture</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Lee, Chenta</td>
<td>IBM</td>
<td>Member</td>
</tr>
<tr>
<td>Lenk, Chris</td>
<td>Mitre Corporation</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Lumi, Qem</td>
<td>Peraton</td>
<td>Observer</td>
</tr>
<tr>
<td>Maroney, Patrick</td>
<td>AT&amp;T</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Mates, Jeffrey</td>
<td>US Department of Defense (DoD)</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Noguchi, Kazuo</td>
<td>Hitachi, Ltd.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Patrick, Paul</td>
<td>DarkLight, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Piazza, Richard</td>
<td>Mitre Corporation</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Quittelier, Margaux</td>
<td>Sopra Steria Group</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Relitz, Stephan</td>
<td>Peraton</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Ricard, Chris</td>
<td>Financial Services Information Sharing and...</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Robertson, Scott</td>
<td>Kaiser Permanente</td>
<td>Observer</td>
</tr>
<tr>
<td>Ron, Aviv</td>
<td>IBM</td>
<td>Member</td>
</tr>
<tr>
<td>Rosa, Michael</td>
<td>National Security Agency</td>
<td>Observer</td>
</tr>
<tr>
<td>Sparrell, Duncan</td>
<td>sFractal Consulting LLC</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Studer, Christian</td>
<td>CIRCL</td>
<td>Voting Member</td>
</tr>
</tbody>
</table>
OASIS CTI-TC Monthly TC Call

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

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 ‘/’

Trey Darley
Any bits of advice for next time? Would you do it again?
Kartikey Desai
Yes, we do it again when we have significant updates to the interop standard. Advice - developing a common set of objects and automation as much as possible would be helpful. Good note taking is also important.

Steve Relitz
Other lessons learned - we made changes in rapid succession to work with other producers and consumers. One suggestion for the next one would be working with other TCs within OASIS that are using STIX (TAC, etc) data.

Jason Kierstead
For the bugs discovered, is this in the tool, in the testing suites, or testing tools?

Kartikey Desai
The bugs were in the tools brought by participants. We found a few areas where clarity on the standard could be useful – specifically URL slashes.

Jason Kierstead
Sounds like there are a few things the TC needs to improve upon.

Kartikey Desai
The testing suite was not automated. Individual orgs went down a manual checklist to see if sending and receiving matched. Suggest going automated for the next time.

Trey Darley
I'm still holding onto test suite domains for the TC if/when we want to use them.

Pat Maroney
As former interop SC, we worked with the Univ of New Hampshire and spent a lot of time doing automated test suite research with them. We got pretty far in terms of execution and delivery, some production and maintenance costs to be handled. I volunteer to engage with the SC and discuss moving forward.

Kartikey Desai
We would be interested in taking this conversation to the SC. We could possibly hold another plugfest to prove this out and get more participation.

STIX SC Update
Christian Sutder

- Best Practices Doc contributed by Rich Piazza
  - Many things were punt as a best practice during development of STIX 2.1
  - This is a draft doc and is no way complete. Please send your additions.

Rich Piazza
Please add you comments
Thanks to Jeff Mates for adding to the incidents and objects. There are new additions, please check it out again.
Future of the TC
Rob Coderre
● We have not dedicated much time to the recharter exploratory committee yet.
● We are hoping as we enter summer we can make progress on this to give it the attention it deserves.

Cyber Automation Workshop
Duncan Sparrel
● Thanks to all who participated
● This was an interop effort and STIX shifter was in play at the workshop
● Please look at the results section on the website, please add your results if you participated
● We had good discussions on seeing bigger picture
● We had a focus on PACE related use cases

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
  - 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...
OASIS CTI-TC Monthly TC Call

Duncan Sparrel
Lesson learned - We need to keep OASIS in the loop on the plans for administrative purposes. It would be great if we don't add any delays so it makes it into the ITU August cycle.

Rob Coderre
I am in contact with Chet on this and working to make sure there are limited delays.

Trey Darley
We will meet in July, and skip August
Please send us any agenda items that you want dealt with before we resume in the fall.

Rob Coderre
Thank you for joining and see you next month.

Meeting Terminated