## CTI-TC Monthly Meeting: Session #1

**Meeting Date:** April 21, 2022  
**Time:** Session #1 Notes + Attendance  
**Purpose:** Monthly CTI TC Meeting  

### Attendees:

<table>
<thead>
<tr>
<th>Name</th>
<th>Company</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coderre, Robert</td>
<td>Accenture</td>
<td>Chair</td>
</tr>
<tr>
<td>Keith, Robert</td>
<td>Accenture</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Maroney, Patrick</td>
<td>AT&amp;T</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Studer, Christian</td>
<td>CIRCL</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Cullinane, Kelly</td>
<td>Copado</td>
<td>Secretary</td>
</tr>
<tr>
<td>Hohimer, Ryan</td>
<td>DarkLight, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Patrick, Paul</td>
<td>DarkLight, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Taylor, Marlon</td>
<td>DHS Office of Cybersecurity and Communications</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Masuoka, Ryusuke</td>
<td>Fujitsu Limited</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Satomi, Toshitaka</td>
<td>Fujitsu Limited</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Ratliff, Emily</td>
<td>IBM</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Jones, Elysa</td>
<td>Individual</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Robertson, Scott</td>
<td>Kaiser Permanente</td>
<td>Observer</td>
</tr>
<tr>
<td>Desai, Kartikey</td>
<td>Mitre Corporation</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Lenk, Chris</td>
<td>Mitre Corporation</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Piazza, Richard</td>
<td>Mitre Corporation</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Carroll, Sean</td>
<td>National Security Agency</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>Caselli, Marco</td>
<td>Siemens AG</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Quittelier, Margaux</td>
<td>Sopra Steria Group</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Mates, Jeffrey</td>
<td>US Department of Defense (DoD)</td>
<td>Voting Member</td>
</tr>
</tbody>
</table>
OASIS CTI-TC Monthly TC Call

Agenda:
- TC Updates
  - Call for co-secretary
  - Welcome to YouTube!
  - STIX SC
    - Interop SC
- Future of the TC
- Q&A

Meeting Notes:
Rob Coderre
- Welcome! Please record your attendance
- Many thanks to Jane Ginn! We appreciate her years of service to the TC!
- 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

Welcome to YouTube!
- Recorded meetings will now be posted on YouTube! Please Subscribe!
- [https://www.youtube.com/channel/UCyAHGwFg1Up5Px7RcC_L3A](https://www.youtube.com/channel/UCyAHGwFg1Up5Px7RcC_L3A)

STIX SC Update
Emily Ratliff
- STIX Extensions Policy Document is now in effect
  - [https://docs.google.com/document/d/1bjcYUWb9uFoqYrdSP_bqtmxVyxBONB-RF7SLMR9dZC8/edit?usp=sharing](https://docs.google.com/document/d/1bjcYUWb9uFoqYrdSP_bqtmxVyxBONB-RF7SLMR9dZC8/edit?usp=sharing)
  - All future proposed extensions will go through this process
- Currently working the Best Practices Doc contributed by Rich Piazza
  - Many things were punted as a best practice during development phases

Rich Piazza
The Best Practices Doc has ideas from MITRE and our DHS sponsor. It is no way complete or perfect, and likely missing some valid ideas. Please review and add any comments or ideas.

Duncan Sparrel
Is the plan to eventually store it Git to handle change control?

Emily Ratliff
No current plan. Google doc has some revision history capabilities.

Interop SC Update
Kartikey Desai
- Interop ballot passed!
  - Ballot Link: [TAXII™ 2.1 Interoperability Committee Specification Version 1.0](#)
  - Ballot Status: Passed
PlugFest Update

- Meetings: Last meeting: April 14
- Participation: 3 Participating Organizations (MITRE, Peraton, Fujitsu)
- Plugfest:
  - STIX Personas identified so far (MAS, SIEM, SXP*, SXC*, TIP) all at Level 2
    - 18+ Interop use-cases TBD (out of 21 use-cases)
  - TAXII Personas identified (TXS, TXC)
  - Date 15-17 June 2022
  - Sponsored by Peraton with virtual and in-person USA-DC
  - Please reach out if you are interested in participating
  - Next Session: April 28 @9pm ET

Remaining STIX Personas Not Covered by Current Plugfest Members

- **Adversary Infrastructure Mapping (AIM)**
  - Software or system, that consumes and produces STIX content, that is used to map out adversarial networks.
- **Local Infrastructure Mapping (LIM)**
  - Software that scans local networks and provides STIX representations of these finds.
- **Threat Detection System (TDS)**
  - Software instance of any network product that monitors, detects and alerts such as Intrusion Detection Software (IDS), Endpoint Detection and Response (EDR) software, web proxy, etc. This is applicable for both Producers and Consumers.
- **Threat Mitigation System (TMS)**
  - Software instance that acts on Course of Action and data from other threat mitigations such as a firewall, IPS, Endpoint Detection and Response (EDR) software, etc. This is applicable for both Producers and Consumers.

Future State of the TC

- In mid-2021, we did a minor update to the charter of the CTI TC in order to comply with new OASIS rules for TCs. At that time the TC decided to defer big picture discussions regarding the future of the CTI TC (which might require a total restructuring of the CTI TC) until after STIX 2.1 and TAXII 2.1 had reached full OASIS standard status.
- Based on the original TC charter, we’ve largely accomplished our goals! The question before us now is “What’s next?”
- Based on informal feedback and input from the community, our next major goals are around interop and accessibility. These are not in our current charter.
- There is also a backlog of work to continue as well, including build-out of cyber observables (could be extensions or new SDOs), patterning, SBOMs
- We have seen a significant drop-off in attendance and participation in monthly meetings and working sessions, primarily due to a few reasons:
  - The STIX/TAXII specs are largely complete and full global OASIS standards
  - We all have day jobs; most of us aren't compensated directly for working on this stuff!
- How do we recognize our updated purpose and get more people involved in the TC and work efforts?
- Diversity of thoughts and opinions are crucial to the long-term success of the threat intelligence community
OASIS CTI-TC Monthly TC Call

- **Proposal:** Creation of an exploratory committee to define a vision statement and new charter for the TC. Seeking volunteers to work on this effort and bring results back to the TC in 90 days.

Trey Darley
There is no reason why we couldn't have more than one proposal.

In Chat
Duncan Sparrel volunteered to work on the new charter

Duncan Sparrel
Not necessarily bad that our meetings are small. We should be open to the idea that we don’t need to recharter at all – just reorganization.

Trey Darley
Recharter is necessary because Interop is not in our original charter. Adding this, per OASIS rules, requires a recharter. Not suggesting that we split into several groups, just that we might have several competing ideas on ways forward.

Rob Coderre
To recap: looking to see what our options are. Don’t want to create unnecessary recharter work if we don’t need it. Really looking for a revised mission statement first. Then we can work with OASIS to see what the boundaries are, and even look at rule changes in OASIS.

Notional New TC Org Structure

- **Proposal:** Move towards a more global focus and take the emphasis away from a North American-centric viewpoint
  - Three regions, Europe, Asia-Pacific and North America, each led by a regional chair (equivalent to current co-chair)
  - A “community manager” to help the regional chair organize meetings and activities in more local time zones

In Chat
Margaux Quittelier, located in France, would like to participate with approval of leadership.

Duncan Sparrel
We can increase participation by creating a liaison for submitting to the ITU. This will increase international participation.

Trey Darley
We are holding off until Interop is more built out. Move that we hold off on this conversation and get back to the agenda. Move to bring this up next month.

Rob Coderre
Considerations
- How do we continue forward momentum of STIX/TAXII standards without breaking things?
- OASIS approval rules can be a challenge
- What about a more regular cadence of standard releases?
  - Like more modern software, consider 6-month release cycle
Minor releases that only add functionality and not introduce any breaking changes

- We need your inputs on this!

Pat Maroney
There are TC members that are willing to dig deep on specific topics, like ontology, STIX implementation, if we decide to go that way.

Trey Darley
We’ve historically held off on ontology because of the time it requires. We are only now starting to get to a place to handle this. If a committee wanted to start exploring this, I would support it.

Rich Piazza
MITRE is doing work on CIRCL on compatibility on MISP and STIX - just wanted to mention this.

Ryan Hohimer
Threat Actor Context (TAC) TC - is gaining momentum. Might be an implementation that is extending STIX. Would be happy to be in discussions on how ontologies and knowledge bases that incorporate STIX could unfold.

Trey Darley
What about quarterly or semi annual releases - maybe it’s just errata or extensions? This would establish a cadence and keep people engaged. Would this change our collaborative development environment? Can we iterate on 2.1 with point releases as long as possible?

Jeff Mates
As long as we can push extensions, that works well.

Rob Coderre
This would require that we don't do any major changes. We don't need to solve this today, but these are the topics that we need to be working on.

Rich Piazza
Extension write up doc mentioned earlier - if we want to have several releases a year, this will require management and a formalized plan. Some of this is in the doc, and can be built upon.

Pat Maroney
We previously discussed going to quarterly meetings, are we going to still meet monthly?

Rob Coderre
Yes, sticking with monthly for now.

Meeting Terminated

----------------------------------------------------------------------------------