CTI-TC Monthly Meeting: Session #2

Meeting Date: **April 21, 2022**

Time: **Session #2 Notes + Attendance**

Purpose: **Monthly CTI TC Meeting**

Attendees:

Name	Company	Role
Thompson, Dean	Australia and New Zealand Banking Group	Voting Member
Gurney, John-Mark	Copado	Voting Member
Taylor, Marlon	DHS Office of Cybersecurity and Communicat...	Voting Member
Yamada, Koji	Fujitsu Limited	Member
Ratliff, Emily	IBM	Voting Member
Varner, Drew	NineFX, Inc.	Member
Lumi, Qem	Peraton	Observer
Relitz, Stephan	Peraton	Voting Member
Girard, David	Trend Micro	Voting Member

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/UCyAHGwFg1Up5PxF7RcC_L3A

STIX SC Update

Emily Ratliff

- STIX Extensions Policy Document is now in effect
  - https://docs.google.com/document/d/1bjcYUWb9uFoqYrdSP-_bqtmxVyxONB-RF7SLVR9dZC8/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 of STIX 2.1
  - This is a draft doc and is no way complete. Please send your additions.

Rob Coderre

This doc fills in the gap between the spec and interop and is a great resource. And the doc will become more important overtime.

Interop SC Update

Marlon Taylor

- 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
- **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.**

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

Steve Relitz
Applaud the efforts to try and be more inclusive.

Rob Coderre

- For now we will keep the monthly cadence for now
- The ability to communicate on a more frequent basis is important right now as we are at a critical time to decide where this TC is going
- No plans yet, but would like to keep an open mind on hosting in person meetings

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!

David Girard
Language barrier, some team members are shy to get into committees because they feel their English is not perfect. Having regional committees, that would likely encourage more participation from Tokyo/Taipei/APAC. There is also a large potential for native French speakers in this space.

Meeting Terminated