CTI-TC Monthly Meeting: Session #1

Meeting Date: March 17, 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>Kostrosky, Curtis</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>Darley, Trey</td>
<td>CCB/CERT.be</td>
<td>Chair</td>
</tr>
<tr>
<td>Chan, Kevin</td>
<td>Copado</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Cullinane, Kelly</td>
<td>Copado</td>
<td>Secretary</td>
</tr>
<tr>
<td>Ginn, Jane</td>
<td>Cyber Threat Intelligence Network, Inc.</td>
<td>Secretary</td>
</tr>
<tr>
<td>Hohimer, Ryan</td>
<td>DarkLight, Inc.</td>
<td>Member</td>
</tr>
<tr>
<td>Patrick, Paul</td>
<td>DarkLight, Inc.</td>
<td>Member</td>
</tr>
<tr>
<td>Ailshire, David</td>
<td>DHS Office of Cybersecurity and Communications</td>
<td>Member</td>
</tr>
<tr>
<td>Park, Jackie Eun</td>
<td>DHS Office of Cybersecurity and Communications</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>van Belkum, Aukjan</td>
<td>EclecticIQ</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Ricard, Chris</td>
<td>FS-ISAC</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Satomi, Toshitaka</td>
<td>Fujitsu Limited</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Noguchi, Kazuo</td>
<td>Hitachi, Ltd.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Keirstead, Jason</td>
<td>IBM</td>
<td>Member</td>
</tr>
<tr>
<td>Lee, Chenta</td>
<td>IBM</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Ratliff, Emily</td>
<td>IBM</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Beck, Desiree</td>
<td>Mitre Corporation</td>
<td>Member</td>
</tr>
<tr>
<td>Desai, Kartikey</td>
<td>Mitre Corporation</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Haynes, Danny</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>Struse, Richard</td>
<td>Mitre Corporation</td>
<td>Member</td>
</tr>
<tr>
<td>Relitz, Stephan</td>
<td>Peraton</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Sparrell, Duncan</td>
<td>sFractal Consulting LLC</td>
<td>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>Member</td>
</tr>
<tr>
<td>Girard, David</td>
<td>Trend Micro</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
  - Progress on Open Repo Maintainers
  - STIX SC
  - Interop SC
- Community Development Corner
- Q&A

Meeting Notes:
Rob Coderre
Call for nominations for open TC leadership roles
- Jane Ginn will be stepping down as Co-Secretary as of 1 May 2022
  - Thank you, Jane for your many years of service to the TC.
  - We appreciate everything you did for all of us.
Richard Struse
Many thanks for the countless hours, Jane. You are a true public servant. This community is better for your service.

Rob Coderre
- 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

Repo Maintainers
- Thank you to Emily Ratliff and Duncan Sparrell for volunteering their time to help maintain our Open Repositories!
  - We do need a few more volunteers to help out!
- The following repos are still in search of a second maintainer:
  - cti-stix-elevator
  - cti-stix-slider
  - cti-taxii-client
  - cti-taxii-server
- Please reach out to Chris Lenk (clenk@mitre.org) if interested

STIX SC Update
Emily Ratliff
- CTI TC Cover Sheet:
  - [https://docs.google.com/document/d/1yvqWaPPnPw-2NiVCLqzRszcx91ffMowFT5MmE9Nsy_w/edit#heading=h.8bbhgdisbmt](https://docs.google.com/document/d/1yvqWaPPnPw-2NiVCLqzRszcx91ffMowFT5MmE9Nsy_w/edit#heading=h.8bbhgdisbmt)
- Please review Extensions Policy Document!
  - [https://docs.google.com/document/d/1bjcYUWb9uFoqYrdSP_bqtmxVyxONB-RF7SLVR9dZC8/edit?usp=sharing](https://docs.google.com/document/d/1bjcYUWb9uFoqYrdSP_bqtmxVyxONB-RF7SLVR9dZC8/edit?usp=sharing)
  - One week left to review!
  - Received comments and would like to execute on making the policy operational
MITRE participated in WG this past week and shared extension proposals
  ▪ The WG will start bringing extensions in with the policy

- Ongoing work on JSON Signing
  o The write up is out, pls review and add comments

- Incident Extension Object
  o Jeff continuing to add updates
  o Will be discussing next week during WG meeting

Interop SC Update
Kartikey Desai
- The STIX 2.1 Interoperability Test Document Version 1.0 was published as a Committee Specification Draft.
  o [https://docs.oasis-open.org/cti/stix-2.1-interop/v1.0/csd01/stix-2.1-interop-v1.0-csd01.docx](https://docs.oasis-open.org/cti/stix-2.1-interop/v1.0/csd01/stix-2.1-interop-v1.0-csd01.docx)
  o [https://docs.oasis-open.org/cti/stix-2.1-interop/v1.0/csd01/stix-2.1-interop-v1.0-csd01.html](https://docs.oasis-open.org/cti/stix-2.1-interop/v1.0/csd01/stix-2.1-interop-v1.0-csd01.html)
  o [https://docs.oasis-open.org/cti/stix-2.1-interop/v1.0/csd01/stix-2.1-interop-v1.0-csd01.pdf](https://docs.oasis-open.org/cti/stix-2.1-interop/v1.0/csd01/stix-2.1-interop-v1.0-csd01.pdf)

Rob Coderre
Any doc that has normative text (ex – ‘must’, ‘shall’, ‘should’) needs to be published as a CSD. This doesn’t change how we will operate. The only difference is that if we want to publish updates, we will need to run a vote and publish a CSD 2.0.

OPEN BALLOT
Kartikey Desai
**TAXII™ 2.1 Interoperability Committee Specification Version 1.0**

Ballot Link: [TAXII™ 2.1 Interoperability Committee Specification Version 1.0](https://docs.oasis-open.org/cti/stix-2.1-interop/v1.0/csd01/stix-2.1-interop-v1.0-csd01.pdf)

Closes Date: **2022-03-25**

This is the Interoperability test document to supplement the Trusted Automated Exchange of Intelligence Information (TAXII) 2.1 OASIS Standard developed by the Cyber Threat Intelligence Technical Committee (CTI TC) of the Organization for the Advancement of Structured Information Systems (OASIS).

Marlon Taylor
We have enough people on the call to pass it now if everyone goes and votes. Please vote now.

Plugfest Update
- Meetings:
  ▪ Last meeting: March 10
- Participation:
  ▪ 12 Organizations on rooster
- Plugfest:
  • STIX Personas identified so far (MAS, SIEM, SXP*, SXC*, TIP) all at Level 2
18+ Interop use-cases TDB (out of 21 use-cases)
- TAXII Personas identified (TXS, TXC)
- Tentative Date June 2022 (2nd/3rd week)
- Sponsorship with virtual and in-person USA-DC – Peraton is the sponsor
- Please let Marlon know if you are interested in participating

Duncan Sparrell:
Event Happening Around same time:
http://www.cybersecurityautomationworkshop.org/

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.

Steve Relitz
Need a headcount as soon as possible for location planning

Marlon Taylor
Let’s use current participant list as the headcount

**STIX Semantic Equivalence**
Chris Lenk
See meeting recording
Discussion of a white paper to detect content with possible similar meaning in STX

**Community Development Corner**
  - STIX Knowledge Graphs with Ryan Hohimer
    See meeting recording
    Presenting on work happening in the TAC working group

**Closing Comments**
Jeff Mates
Please look at the Incident Document, especially the method for reporting of time fidelity.
Please look at the proposal and respond if you have concerns on this issue.

Meeting Terminated