CTI-TC Monthly Meeting: Session #2

Meeting Date: February 17, 2022
Time: Session #2 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>Thompson, Dean</td>
<td>Australia and New Zealand Banking Group</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Hunt, Christian</td>
<td>Copado</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Ginn, Jane</td>
<td>Cyber Threat Intelligence Network, Inc.</td>
<td>Secretary</td>
</tr>
<tr>
<td>Patrick, Paul</td>
<td>DarkLight, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Taylor, Marlon</td>
<td>DHS</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>Casey, Tim</td>
<td>Intel</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Relitz, Stephan</td>
<td>Peraton</td>
<td>Member</td>
</tr>
<tr>
<td>Girard, David</td>
<td>Trend Micro</td>
<td>Voting Member</td>
</tr>
</tbody>
</table>

Agenda:

- TC Updates
  - STIX SC Update
  - Interop SC Updates
- Community Development Corner

Meeting Notes:

Rob Coderre
Welcome to all – thank for you recording your attendance
This meeting will be recorded
We really need additional maintainers – MITRE Supports ends this year: May 6th, 2022
We need to keep the key Repos up to date.

Emily Ratliff
Last month Rich Piazza did a good extension update – Watch Video
Last month – video – Jeff Mates leading WG
Ongoing work right now is on JSON Signing
We really need reviews of the documents – please provide your input
https://docs.google.com/document/d/1bjcYUWb9uFogYrdSP-_bqtmxVyxONB-RF7SLVR9dZC8/edit?usp=sharing

Rob Coderre
Brought up some details about the work in Interop

Rob Coderre
Welcome a new Co-Chair for Interop – Kartikey Desai
Reviewed his resume
Welcome our new co-chair: Kartikey Desai

- Organization: Senior Cybersecurity Engineer at The MITRE Corporation
- Education: BS in Computer Science and is currently working on MS in Computer Science
- OASIS CTI-TC:
  - Interop: Lead editor for TAXII Interoperability and STIX Interoperability documents
  - Development: Developer/maintainer for several OASIS OPEN repositories including python-stix2 and cti-stix-visualization.
- Other Efforts: Implement a Zero Trust Architecture, and International Cyber Capacity building.

Interop Calls at 2:00 pm EST

PlugFest Update

Meetings:
- Last meeting: Jan 27

Participation:
- 12 Organizations on rooster - follow up with the all 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

Rob Coderre

Discussed the updates to the Interop Part II

Optional Interop TAXII Filtering

- Based on 3.4 Filtering from TAXII Version 2.1 and extends 3.4.1 Supported Fields for Match
- Provides additional support for filtering (snippet below):
  - Confidence
    - `match[confidence]=00,01,02,03,04,05,06,07,08,09,100`
  - Vocabs
    - `match[sectors]=financial-services,manufacturing`
  - Hashes
    - `match[SHA-256]=97e7e313e78a6b975127b3930b9be9669686f9a82374f6133d31d2b7108f`
  - Object Relationships (e.g. Reports, Sightings, Groupings)
    - `match[object_mref=jindicator=34496a1b-f7fa-4e8a-bcc9-4eab0c3e7fbb,cighting=34496a1b-f7fa-4e8a-bcc9-4eab0c3e7fbb]`
  - Valid Indicators
    - `match[valid_until]=2022-01-31T00:00:00Z`

Rob Coderre

Noted that we do not have a leader for the TAXII Subcommittee
We are looking for the next steps with real world implementations
TAXII Update

- Looking for volunteers to lead TAXII SC. Please consider!
- What additional features does TAXII need to have?
  - For example:
    - OpenCTI using Message BUS
    - Use MQTT?
    - Expanded language around authentication and modern API usage? (versus minimum basic auth)
- Please share your thoughts with the TC!

Rob Coderre

Along with Noaa Kless and others he began working on STIX Shifter

“Our open source project is a friendly UI for creating or editing stix shifter modules which can be used online.”

Can be found here: https://github.com/IBM/map-my-shifter

The map-my-shifter (MMS) project provides a visual editor for building mappings for STIX-Shifter modules.

A typical (module) connector requires two types of field mappings:

- **From STIX** pattern mapping - When building the data source query from a STIX query, the STIX fields, for example file:name, is mapped to the target data source's field. Read more...
- **To STIX** object mapping - When a results object is back from the data source, this object gets translated in the final result as a STIX object. For example {"filename": "xxxxx"} should be translated to a STIX object of type file. Read more...

*From STIX mappings:*

You can do your own mapping – or import [used CarbonBlack mapping]

You can also add custom fields

[Gave demo]

*To STIX mappings:*

[Gave demo of how to use it from a browser]

map-my-shifter is licensed under the Apache License, Version 2.0. See LICENSE for the full license text.

Ryusuke Masuoka

Asked question about AIS 2.0 – has anyone worked with it?

Marlon Taylor

Clarified that it is a test version

Rob Coderre

Thanks all! See you next month or in Working Group sessions.

Meeting Terminated