CTI-TC Monthly Meeting: Session #2

Meeting Date: January 16, 2020
Time: Session #2 – 9:00 PM US EST
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>Voting Member</td>
</tr>
<tr>
<td>Thompson, Dean</td>
<td>Australia and New Zealand Banking Group</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Jordan, Bret</td>
<td>Broadcom</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Ginn, Jane</td>
<td>Cyber Threat Intelligence Network, Inc.</td>
<td>Secretary</td>
</tr>
<tr>
<td>Park, Jackie Eun</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>Yamada, Koji</td>
<td>Fujitsu Limited</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Yoshimura, Kunihiko</td>
<td>Fujitsu Limited</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Terada, Masato</td>
<td>Hitachi, Ltd.</td>
<td>Member</td>
</tr>
<tr>
<td>Ratliff, Emily</td>
<td>IBM</td>
<td>Voting Member</td>
</tr>
<tr>
<td>MacDonald, Terry</td>
<td>Individual</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Stewart, Justin</td>
<td>LookingGlass</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>Co-Chair</td>
</tr>
<tr>
<td>Gurney, John-Mark</td>
<td>New Context Services, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Varner, Drew</td>
<td>NineFX, Inc.</td>
<td>Voting Member</td>
</tr>
</tbody>
</table>

Agenda:

- Introduction & Welcome
- Sub-Committee Updates

Meeting Notes:

Richard Struse

Welcome everyone! We have a lot to cover, including some exciting things on Interop. Be sure to record your attendance

Emily Ratcliff

[Gave update on the Sponsorships]

We had a lot of discussion during Session #1 on where the Sponsors were

Here is a table that summarizes all of the Sponsorships we currently have
Bret Jordan
  We got a lot of input earlier today
John-Mark Gurney
  We need a second Sponsor on COA – We need this
Richard Struse
  [Gave clarification on why we added the idea of Sponsorship]
  [Clarified how it can be documented]
Jane Ginn
  This morning we discussed the implications of not having a Sponsor
Bret Jordan
  [Gave some insight on what the cascading effects will be if an SDO has no Sponsor]
Richard Struse
  [Talked about Infrastructure – getting TELUS and Looking Glass involved]
On Chat:
  From Terry MacDonald to Everyone:  07:12 PM
  Can a removed object be added back in a future CSD if the work kicks off again?
  Or is it automatically kicked until the next release of STIX?
  From Bret Jordan to Everyone:  07:12 PM
  Yes, it can Terry
  From Terry MacDonald to Everyone:  07:13 PM
  ok cool. Thanks Bret
Bret Jordan
  Just let us know if you’ve worked on this – We can be really discreet
Emily Ratliff
  [Gave update on GitHub issues – Non-material changes addressed]
  GitHub Issue 202 is non-Material – no code change
  [Posed question to participants to making relationships not depreciated]
Bret Jordan
  [Gave clarification on discussion from this morning]
John-Mark Gurney
  I’ll support that change
Bret Jordan
  The Editors will have a call and address this issue – if there are no concerns
  Rich Piazza and I will have a call – we’ll make those changes
*************TAXII Update***************

Bret Jordan

All of the inputs and Sponsorships have been very helpful
I’ve put together a graphic that shows the timeline

---

TAXII has gone through a lot of review
There are a number of things that I wish were in 2.1 – but there was never really any Consensus
After the last review – we had included everything in there – Motion to CS and 2nd
An individual in PC objected
Chet opened a Ballot to get a consensus on how to move forward
About 70% say we should move forward – 30% said no
There was never TC consensus on how to handle

[Went over all of the proposals] [See Appendix]
We have about 4 to 5 proposals on TAXII query and filtering – we don’t have a consensus
We had a straw poll – Consensus was to move forward

Richard Struse

I just want to emphasize how important it is to move forward
A lot of pent-up demand in the marketplace. We need to respond to this
The Query and Filtering need to be considered carefully – it will take some time
We as a TC – we’ve done a lot of work – Thanks to Bret and all – We can work on query
For next version – Enhancement proposals + query
People have been waiting a long time – let’s deliver it

Bret Jordan

Maybe we can release a TAXII 2.1 Spec on Query – we could turn around quickly
I’ll facilitate and make it happen

Jane Ginn

I put links to all the proposals to the various proposals in the Session #1 notes

Richard Struse

Prototype the thing you are proposing

Ryusuke Masuoka

The current Ballot is: A Ballot to open a Ballot – Simple majority, right?

Bret Jordan

Yes, Overwhelmingly passing – on Monday, the Ballot can be opened
Chet will open a Special Ballot for opening a CS for TAXII

Richard Struse

I will ask Chet to open the Ballot a Ballot to make it a CS.

Emily Ratliff

[Noted the time zone difference]
Bret Jordan
We’ve come a long way – A lot of vendors have implemented 2.1
Please vote

Richard Struse
Make your voice heard – Exercise your voting rights

Justin Stewart
I’ll give an Interop SC update

- Create STIX 2.1 Interoperability Test Document (target Q1, Q2)
  - Identify significant changes (SDO, SCO, Patternning) and add test cases specific to STIX 2.1
- Create TAXII 2.1 Interoperability Test Document (target Q1, Q2)
  - Identify significant changes (Pagination, etc.) and add test cases specific to TAXII 2.1
- Update STIXPreferred for STIX/TAXII 2.1 specification
  - Update website as needed, improve marketing and response
- Sponsor Plugfests (target Q2, Q4)
  - Celerium will host a PlugFest on May 12-14 in Tysons Corner, VA

Put May 12-14 on calendar if you want to participate

Richard Struse
Thanks to Solarium and Mark Davidson in particular
We do this to achieve Interoperability
Please give this attention – This is where it gets REAL!
This is where we drive it home – Let’s take advantage of that

One of the purposes of the Sponsorship
1. Spec text
2. Attestation
3. Interop

These are the three purposes of Sponsorship

Are there any other questions or comments? [None]

Jane Ginn
Gave Invitation for presenting in Community Development Corner

Richard Struse
Our only restriction is that it be Open Source
Any other comments? Questions?
Thanks everyone!

Meeting Terminated
***************************************************************************
## Appendix: Summary of TAXII Query Proposals

<table>
<thead>
<tr>
<th>Author</th>
<th>Title</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trey Darley</td>
<td>Possible TAXII 2.0 REST-based Query API</td>
<td><a href="https://docs.google.com/document/d/11wKWQaJ6B_8MujQ_u4PakSKzXztOL0RanmvU6wuaFaQ/edit#heading=h.s4jv7ef18b">https://docs.google.com/document/d/11wKWQaJ6B_8MujQ_u4PakSKzXztOL0RanmvU6wuaFaQ/edit#heading=h.s4jv7ef18b</a></td>
</tr>
<tr>
<td>Jason Keirstead &amp; Terry McDonald</td>
<td>TAXII Information Request and Response</td>
<td><a href="https://docs.google.com/document/d/1Cy_yBhS5KExdHSz2v5c3Awrqy77Yq6KXXWQv4-uH/ps/edit#heading=h.1jcqb6vc5y7z">https://docs.google.com/document/d/1Cy_yBhS5KExdHSz2v5c3Awrqy77Yq6KXXWQv4-uH/ps/edit#heading=h.1jcqb6vc5y7z</a></td>
</tr>
<tr>
<td>Bret Jordan &amp; Gary Katz</td>
<td>A TAXII Search / Pivoting Proposal</td>
<td><a href="https://docs.google.com/document/d/1fquYyI-I6d2eN-2MHqJl_V68qNcnqTOv2vpg4XFeF7as/edit#heading=h.xlss9yc6jov">https://docs.google.com/document/d/1fquYyI-I6d2eN-2MHqJl_V68qNcnqTOv2vpg4XFeF7as/edit#heading=h.xlss9yc6jov</a></td>
</tr>
<tr>
<td>DHS / MITRE</td>
<td>Tiered Filtering Proposal (this idea has evolved over time)</td>
<td><a href="https://www.oasis-open.org/committees/document.php?document_id=66520&amp;wg_abbrev=cti">https://www.oasis-open.org/committees/document.php?document_id=66520&amp;wg_abbrev=cti</a></td>
</tr>
</tbody>
</table>