CTI-TC Monthly Meeting: Session #2

Meeting Date: May 20, 2021
Time: Session #2
Purpose: Monthly CTI TC Meeting

Attendees:

<table>
<thead>
<tr>
<th>Name</th>
<th>Company</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kostrosky, Curtis</td>
<td>Accenture</td>
<td>Member</td>
</tr>
<tr>
<td>Thompson, Dean</td>
<td>Australia and New Zealand Banking Group</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Ginn, Jane</td>
<td>Cyber Threat Intelligence Network, Inc.</td>
<td>Secretary</td>
</tr>
<tr>
<td>Jordan, Bret</td>
<td>Cyber Threat Intelligence Network, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Masuoka, Ryusuke</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>Thomson, Allan</td>
<td>Individual</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Gurney, John-Mark</td>
<td>New Context Services, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Hunt, Christian</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
- STIX and TAXII SC Updates
- Interop SC Updates

Meeting Notes:
Bret Jordan
Went over agenda.
Reviewed the types of comments that came in during Public Comment period.

Now Working Draft 12 is open as a Ballot – Moving that to Call for Consent.
Call for those Voting Members to vote on both items (Approve & Call).
TAXII is in a holding pattern for this Ballot to close.
TC Membership will not be voting – Primary Rep. votes – 14 days.
Estimated that, given timing, mid-June for final.

Allan Thomson
Asked for same name for both SOUs – On call for consent. Chet handle.

Bret Jordan

We have many SOUs – Thank you

Statements of Use for STIX 2.1 CS02
1. Accenture
2. Fujitsu
3. New Context
4. SEKOIA
5. DHS
6. EclecticIQ
7. Trend Micro
8. Darklight
9. Avast
10. Anomali
11. IBM

Statements of Use for TAXII 2.1 CS01
1. Fujitsu
2. Celerium
3. LookingGlass
4. CyWare
5. FreeTAXII
6. SEKOIA
7. DHS
8. EclecticIQ
9. Trend Micro
10. Avast Software

*If your organization submitted one or more SOUs and you don't see your organization's name listed here, please speak up on the call or email ping.Trey or行政执法.*
Went over Marlon’s proposal for testing – Then in future version of STIX to address
  • Issues 262/263 conformance issues were discussed
    - Optional fields not required per conformance
    - Use of “parsing” not defined
  • To address in the spec would be a material change
    - Pro: Remove conformance ambiguity loopholes
    - Con: Release Timeline for STIX 2.1
  • During public review working call, no objection to address this to a future release of the spec

Reviewed Marlon’s comparison table.
  • During the public review call, we discussed Interop options to resolve these issues in the interim
  • Trying to address via Interop
    - Pro: No impact to STIX 2.1 release timeline
    - Con: Not a complete solution - only applies to Interop and not STIX conformance
  • Based on Interop working call, Interop would support:

<table>
<thead>
<tr>
<th>Rank</th>
<th>Input: Keep Original</th>
<th>Process: Translate to Internal Data Model</th>
<th>Export Original</th>
<th>Export Processed</th>
<th>Disposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>18</td>
<td>Yes</td>
<td>Some</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>25</td>
<td>Yes</td>
<td>All</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Discussion on next items on Agenda

What are the next steps?

Dean Thompson
Need for Advocacy – We need to work on this.

Jane Ginn
Dee reached out to ask about Marketing – Allan could you give us your input?

Allan Thomson
We need to finish Interop Committee Notes – and STIXPreferred first.

Dean Thompson
I agree, we need to look at what the vendors are doing.
[Described experience in working with vendors that claimed conformance]

Allan Thomson
[Described how vendors need to point to test results]
A better investment of marketing.

Bret Jordan
The precursor of that is getting the Interop Documents out.

Drew Varner
What would TAXII look like next round? Channels?

Bret Jordan
[Discussed how to do that – Issue as stand-alone update]
Ryu Masuoka
   Support Interop, PlugFest – we also need to map out the landscape.
   Integration with ATT&CK, MISP, etc... and entire ecosystem.

Bret Jordan
   We also have the Playbook work.
   Reminder to Vote on Ballot.
   Thanks everyone – see you next month.

Meeting Terminated
***************************************************************************