CTI-TC
Interoperability Subcommittee

Meeting Date:       Wednesday, August 16, 2017
Time:              12:00 pm to 1:00pm EDT
Purpose:           Monthly Meeting

Attendees:

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jason Keirstead</td>
<td>IBM</td>
<td>Moderator</td>
</tr>
<tr>
<td>Jane Ginn</td>
<td>CTIN</td>
<td></td>
</tr>
<tr>
<td>Christine Hunt</td>
<td>New Context</td>
<td></td>
</tr>
<tr>
<td>Trey Darley</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nicole Gong</td>
<td>MITRE</td>
<td>Recorder</td>
</tr>
<tr>
<td>John Anderson</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Agenda:

1) Review the Part 2 document and the Intel Collaboration test case workflows.
   a. The section currently describes Indicator sharing between 2 systems including expected test verification for creation, modification, and display of Indicator
   b. 1st use case allows modifying of existing intel without having to create new intel
   c. 2nd use case allows creation of intel that is related to other intel but respects the rules around related and versioning
2) Further feedback on outstanding questions in other sections of Part2 that require TC discussion
3) Discuss/review Ted’s comments in Slack channel for the Test Documents Part 1, see comments below:
   Have you considered a persona that is simply a sink for intel?
   For instance, an enforcement point that consumes intel but does not produce sightings. We have built a system that consumes intel (currently STIX 1.2.1...but looking to support 2.x) on behalf of several different enforcement points and makes it available to them in a very simplified form (think black lists/gray lists /white lists). Some of these consumers may not be able to send us sightings, but instead will use their built-in reporting capabilities.
4) Discuss Jason’s proposal on virtual Interoperability Plugfest

Part 2 document:  https://docs.google.com/document/d/11MocPK3s8im8O5-7rgZhtVHo72aQicJj2v-HDXQ8/edit?usp=sharing
Documents URLs:

1. Google use case document URL:
   https://docs.google.com/document/d/1I54RhxwuXrZUQ19zIHYi7_c6otbLvVfluKJogU7s/edit?ts=5890ba79
   - 1) part document has been updated for all changes agreed so far:
     https://docs.google.com/document/d/1I54RhxwuXrZUQ19zIHYi7_c6otbLvVfluKJogU7s/edit#heading=h.ehzdxcsjrzgp
   - 2) part 2 document has been updated to reflect taxii use cases to test (draft list only).
     https://docs.google.com/document/d/11MocPK3s8im8O5-7rgZhtVHoO72aQicj2v-HDx-Q8/edit#heading=h.avris7u5njsd

2. STIX™ 2.0 Interoperability Use Cases Future Ideas:
   https://docs.google.com/document/d/1xe1jSbb6324dYAXsy_zrLZxVIKeWa9FVL-uuillYjfg/edit#

3. Persona Metrix:

4. General MITRE -- ATT&CK library
   https://attack.mitre.org
   as STIX 2.0 objects and posted them to Github here:
   https://github.com/mitre/cti/tree/master/ATTACK

5. GitHub  cti - Cyber Threat Intelligence Repository of ATT&CK and CAPEC catalogs expressed in STIX 2.0
   http://mitre/cti

Summary of the discussion and outcome:
Based on Ted’s suggestion for adding a new persona on Intel Sink Persona, Allan added it, and named “Threat Intelligence Sink”, hearing no objections. Allan added. The meeting discussed if other places shall address or add sink as well, the meeting, then discussed and reviewed Ted’s comments in Slack channel, see comments below:

"Part 1. Have you considered a persona that is simply a sink for intel? For instance, an enforcement point that consumes intel but does not produce sightings. We have built a system that consumes intel (currently STIX 1.2.1...but looking to support 2.x) on behalf of several different enforcement points and makes it available to them in a very simplified form (think black lists/gray lists/white lists). Some of these consumers may not be able to send us sightings, but instead will use their built-in reporting capabilities."

However, Ted was not available to discuss or review the changes made. The committee briefly discussed the changed. Decided to defer the review to the Week of August 22 to continue the discussion.

The meeting continues with topic # 2, Jason proposed to have an interoperability virtual plugfest, all believed that was a great idea, however needs time to do some prepare, maybe coordinate with Brad to see if possible to combine it at the next F2F.

**Action Items:** Jason to discuss with Brad

- **Action:**
  -  

**Details:**

The meeting started with some discussions on Ted Bedwell’s comments on Slack Channel, background information:

Aug 4th at 10:37:31 AM, Ted Bedwell from manor.org posted a comment on the slack interoperability channel. See message below:

"Hello Interop folks. First off, thank you for all the efforts so far. Great work product in Test Document - Part 1. Have you considered a persona that is simply a sink for intel? For instance, an enforcement point that consumes intel but does not produce sightings. We have built a system that consumes intel (currently STIX 1.2.1...but looking to support 2.x) on behalf of several different enforcement points and makes it available to them in a very simplified form (think black lists/gray lists/white lists). Some of these consumers may not be able to send us sightings, but instead will use their built-in reporting capabilities."

Allan responded the following:

"hi ted - this could be a variant of a TMS or TDS system that just consumes but does not produce sightings. So, in this case the system under test would verify that they can consume the data feed of indicators but they would *not* test the sightings use cases.... if you think this is not..."
sufficient then we can consider adding an additional persona in part 2 if others agree that this is an important case.

Ted asked: “As I read the checklist, the sightings cases are mandatory from a self-certification perspective. Am I reading that incorrectly?”

“yup. for TDS and TMS they are currently.” Allan answered.

“So, we have a choice.... we could make sightings tests optional for those persona or we could add another persona where those sightings tests are optional”

Allan decided to make a new persona in part 2 (and checklist), make them optional, Ted agreed, and offered to review it. Allan then added a placeholder in the part2 persona list.

So, Allan made changes to the part 2 documents, however the google doc isn’t clear in this feature, it does not show what changes were made in between the versions. It cannot display two versions at same time and to show the DIFF.

The threat Intelligence persona was added by Allan per Ted’s suggestion. It looks like the following was added on Page 5:

- **Threat Intelligence Sink (TIS) “NEW TO PART 2”**

  - Software Instance that consumes STIX 2.0 content in order to perform translations to domain specific formats consumable by enforcement and/or detection systems that do not natively support STIX 2.0. These consumers may or may not have the capability of reporting sightings. A (TIS) that consumes STIX content will typically consume indicators.

  - **TAXII Server (txs) “NEW TO PART 2”**

    - Software instance that acts as a TAXII Server enabling sharing between producers and respondents of STIX 2 content.

For an organization to receive OASIS interoperability compliance certification, the software instances must adhere to persona behavior and prescribed bundle contents as detailed in the Required Personal/Profile Support section of each use case.

For persona checklist and test requirements per persona please refer to 3 Persona Checklist.
It looks like Allan added as a placeholder, Jason was planning to ask Ted some questions related to that. But Ted won’t be available until August 23.

Next Agenda, review other comments see if we can resolve them.

**First comment in section 2.1 (page 8):** “Verifying produces with these tests with TC...” Ted made some changes to the new persona, called Threat SINK, Jason is not clear, has some questions for Ted, the persona seems to consumes intelligence but cannot provide anything back, so just act as a repository? Jason would like to clarify it when Ted is available.

This is a basic intel collection use case. We added this new persona, how many places should we sticks this? It seems to me that we have to add a lot of these in many places. We really have to talk to Ted about this. -- Jason

We added into “Basic feed sharing”, but we don’t add to “intel collaboration” for the producer persona, not for the respondent persona. -- Jane

**Next comment in the section 2.3 General Error Handling.** “This section could be combined with common connection tests.”

Jason agrees with this comments, error handling should be combined. Jane also agreed. The question is should the error handing be it’s own section and test it, or be part of the basic connection. Trey agrees that should be part of basic connection. The problem is that other documents have error handling on it’s own section.

Jason is going to take care of this action item.

**Next comment: “update to reflect correct taxii 1.0 request + incorrect version in taxii 2 request” on page 13, 2.3.4.5 Incorrect Version Info Get Returns Not Acceptable. So, it should be “2.0”, where it says “1.0”.**

Jason will just update it and take care of that.

**Jason added a new common:** “We have to add an option C behaviour for a read-only collection.”

In the section 2.5.3 Required Producer Persona Support. In the collection options, there is one missing. We need add an option C behaviour for a read-only collection. Jane thinks we also have to add some informations to this new sink, this is where the new sink should be tested. Another comment added as: New “Sink” persona?

So, it looks like we have gone them them all, the rest of things relates to the new persona, we have to wait to next week to discuss when Ted is on the call.

No one had other comments, Jane offered to edit some editorial items.

**Topic #2:** organize an internal ad-hoc virtual plug fast, with vendors. Suggest to do something like that with STIX 2.0 and TAXII 2.0.

A plugfest is an event based on a certain standard where the vendors get together to perform some software test, to test the interoperability of their products or designs with those of other vendors.
Jason is proposing to do it virtually, to start this with a few vendors. Everybody can meet on the slack, and trying to plug their products together. For people in the cloud maybe simpler, as for those who is not in the cloud, it may be tricky to go through VPN and all. Do you think we should propose that to the TC?

Jane asked if it should be open to members only or should it open to none members as well? Jason thinks that it could be open to anybody. We can organize it, since we are not talk about anything relates to API. It could be open to anybody.

Jane, thinks that may be OK with the OASIS rules, other TCs have done that, the OASIS rule said plug fast can be open to none-members. It would probably work. Jason is wonder if OASIS have done this in a virtual format/style. Location maybe a concern.

If so, what do the logistics need to be in places, Slack? Screen sharing?

Trey thinks it is a great idea, clearly falls into interoperability sub-committee, maybe we can use zoom or google hangout? Zoom probably can share screen. What about NDA? Some vendors may have STIX 2.0 implemented but may not shipped yet, they may want a NDA in place.

Not sure how it works if gets into NDA.

Document high level behaviors, we can select some test cases, and documents the result.

John: can we allow vendors to voluntary OPT in and do some self-testing? What about use accounts?

Amazon has some features for the cloud.

Jason: we have two aspects to it.

John, yes, we can allow vendors to voluntary OPT in and do some self-testing, test some of the use cases.

Trey: in the old days, the electronic vendors, they get together and test their equipment’s for interoperability’s, that takes like 1 week. Right? I suggest we do that after the Salt Lake F2F, in person.

It makes sense to do in April 2018 for example. We can announce it during F2F. If they have facilities available, may be Jason should talk to Brad. You need at least 2 days, with a large room with powers and everything, what about to tag along with F2F?

Should we wait to April? We need test early enough; January time frame is better.
Jane suggest to survey the TC, see if who may be interested, then try to work out a few bugs.
Jason: if we get a firm day, then it gives people a date to aim for, and prepare for it, or pair up.

We need to give people enough time. Jason needs to confirm with Brad. Another problem is that skiing season, per Brad, rental car, and logistics may be harder, hotels will be all booked, Hard to get.

We may look at other locations. Survey monkey survey? But it may not reach vendors outside of TC, none members. We need to find other ways to connect with none-members, most of us have some relationships with other vendors. So, we, will discuss that with Brad, consider logistics, and a date.

Jason won’t be available on the call for August 23, he will chat with Allan. Follow up discussions for next week. That is all on the agenda.

Interoperability work is important, Trey believes. He appreciates all the works Allan and Jason have done.

Meeting Terminated