CTI-TC
Interoperability Subcommittee

Meeting Date: Wednesday, April 13, 2016
Time: 18:00 UTC - 02:00pm to 03:00pm EDT
Purpose: Monthly Meeting

Attendees:

<table>
<thead>
<tr>
<th>Name</th>
<th>Company</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allan Thomson</td>
<td>Looking Glass</td>
<td>Co-chair</td>
</tr>
<tr>
<td>Jason Keirstead</td>
<td>IBM</td>
<td>Co-Chair</td>
</tr>
<tr>
<td>Nicole Gong</td>
<td>MITRE</td>
<td>InterOpp Secretary</td>
</tr>
<tr>
<td>Jane Ginn</td>
<td>CTIN</td>
<td>Secretary</td>
</tr>
<tr>
<td>Brad Jordan</td>
<td>Symantec Corp.</td>
<td>Voting member</td>
</tr>
<tr>
<td>Ivan Kirillov</td>
<td>MITRE</td>
<td>Voting member</td>
</tr>
<tr>
<td>Joseph Frazier</td>
<td>U.S. Bank</td>
<td>Voting member</td>
</tr>
<tr>
<td>Mark Davison</td>
<td>NC4</td>
<td>Voting member</td>
</tr>
<tr>
<td>Jyoti Verman</td>
<td>Cisco</td>
<td>member</td>
</tr>
<tr>
<td>Marlon Taylor</td>
<td>DHS Office of Cybersecurity and Communications</td>
<td>Voting member</td>
</tr>
<tr>
<td>Masato Terada</td>
<td>Hitachi, Ltd.</td>
<td>Voting member</td>
</tr>
</tbody>
</table>

Agenda:
I. Update on interoperability use case document
II. Review three sections Allan has been working on.

Meeting Notes:

Moderator: Allan Thomson
Co-Chair: Jason Keirstead
Recorder: Nicole Gong

Google use case document URL:
https://docs.google.com/document/d/1l54RhjxwuXrZUQ19zIHUiZ7_c6otbLbVfluKJogU7s/edit?ts=5890ba79

Allan Thomason
- So everyone is familiar with what we are doing on this use cases document, except for maybe Joseph who is new, and welcome

Joseph Frazier
- From U.S. Bank, and just learning STIX 2.0, using the current version of STIX at the bank.
Welcome Joseph and please signup Slack for interoperability channel

Just want to give everyone an update on what I have been working on – the interoperability use case document. Thanks to Bred, who recently refreshed the document to the OASIS standard template, so now it is more conforming to the OASIS format, thank you Bred, much appreciated.

The document I have spent some cycles on and signed up for, mainly focused on three sections: in section 1.4.3 Indicator sharing, Sighting sharing, and Visioning

I started to going through it and realized that may be it is easier and better to describe the general work flow of indicator sharing, rather than going through each one of the indicators and doing repeated tasks. Then rather things unique to the specific tasks or for some specific indicators, we can call out. So we don’t under up with 500 pages of document.

Any opinion on that change? Do you agree on this?

I think that’s a great idea, I always find graphics really help, graphics lays out the workflow, I can help with the graphics at high-level, if you need help with graphics.

So Gus is not on the call, I did have some feedbacks for him to his diagrams. I do want to see him to put the draft fair version. I agree with you on showing the high-level exchange of data in the graphics and what’s being exchanged, It’s definitely helpful. Any other comments?

So, just call out what I did: we have IPv4, IPv4 CIDR, we got some feedbacks on to have 2 indicators combined to show the “OR” statement, so I did that to show the combination of the logic

I have:
- Indicator IPv4 Address
- Indicator IPv4 Address CIDR
- I added two Indicators with IPv4 Address CIDR
- Indicator with IPv6 Address
- Indicator with IPv6 Address CIDR
- Also added an example for IPV6 Multiple Indicators within the same bundle
- Added FQDN
- added URL, and I do have Indicator FQDN or URL
- And a combination example of URL and Domain

I do have a question for STIX expert, one of things I want to do is sighting section, to do sightings. I added test for domain. Let’s say for example if I want to do Google domain.com, where I want to second level domain from google...

do I define that as URL or do I define domain with pattern /*?

I would say probably a URL, or URL with pattern, I think it is URL makes more sense

You can also use this match syntax, kind like SQL match syntax, I think URL makes more sense

I kind agree with that, just want to confirm that. Any other opinions on that?
Call-User-3 – Jason?
- Well, what are we asking? If it’s possible to do or Are we asking just specific interoperability example? Or are we asking something else? I don’t think we are trying to cover every possible scenario here for the use cases.

Allan
- I know, we are not. You asked if it is specifically for the interoperability examples. Yes, it is. Because what I was doing for the sightings, I wanted to show an example of match google domain /* then I want to show at sighting’s cascade is observer data matching one of these subdomains in the overserve data and how to able to report that.
- May be I skip to the end here.
  Here is an example I added, it’s a sighting with URL. If I am looking at google.com, So that the indicator is: try to find all URLs matches this .com/* so that would be the test.
- So I just want to confirm that, because there a couple options of that. Use domain or URLs.
- Here is an example I added, see section 2.2.5.5 Sighting + Indicator with URL
- Are there any other tests/indicators do we want to specifically call out?
- Just want to cover the core ones:
  We have IP address, Domains and URL, are there any other test cases?
- IPV 6 is optional
- Are there other things people want to add it?

Ivan?
- Is this purely network specific cases? Domain, I would say

Ivan
- I would say Just Domain, File hash I think, pretty topical host based indicator

Jason
- I agree, if anything missing is File hash, we can add File hash

Jane
- MD5 and Sha 256

Allan
- Ok, I will Add: file hash test (md5/sha256)
- I will also add sighting observable example, so we can say the test data is sufficient for this round. Let’s make sure this persona behavior is adequate. This is the next step
- 2.12.1 producer test case data

Allan
- Any other suggestion? These diagrams definite needs to be updated a bit.
- Giving Gus is not on the call, I can take action on that, to see where Gus is. Updating off line
- Are there any other feedbacks on the diagram that we can pass to Gus?
- Please comment on it, if no one is commenting on it, then that’s fine.

Jyoti
- Hi Allan, this is Jyoti, I join it for the first time, how do I access the document.

Allan
OASIS CTI-TC Interoperability Subcommittee

- Jason and myself can add you, if you send Jason and I an email or through slack channel, we can add you are google account. But you should be able to see it as read only, if you just click on the link I just sent in web-ex chat. Do you want to just review it or do you want to contribute to it?

Jyoti
- I will just read first, and I will reach out to you

Allan
- Any opinions on Sighting
- I will come back for that, if you like volunteer please just add your name and put “in progress” next to the topic.
- I will update the examples and updating the sighting section. 2.2.5.5 Sighting + Indicator with URL

**Next Section on versioning**

- So this section on versioning, basically handles the STIX project versioning, producer or consumer must support versioning.
- 2.3.2.1 Description
  The producer persona has identified an STIX object that they wish to share to consumers.
- 2.3.2.2 Required Producer Persona Support
  - The producer persona must be able to create a STIX bundle with one or more objects with the appropriate date representing when the object was created for sharing.
  - I think this section is pretty complete, other than we have filling out persona, for TDS, and stuff like that, this case is pretty complete.
  - Anybody would like to see any other test? Any opinions? No?
  - Ok, I will continue to refine that. Those are the three things I am working ok. I will come back to that list things we said we want to flush out:
  - We have threat actor sharing, report sharing, campaigning sharing, ..., and data marking
  - No bodying is working on that right now, if you like volunteer please just add your name and put “in progress” next to the topic. Anybody else? If not, then I will continue work on these three things and then come back on that.
  - so Any opinions on Sighting? I will come back for that, if you have cycle, to work on these section please considered to contribute.

Jason
- I started to looked persons this morning, and talk to Bret, we thought we should start to do something simpler, may be two of three of that. Wonder if anybody else has an opinion on that? Because I am not sure on that.

Allan
- My company does this; it matches the product my company produces – it pairs how my company produces.

Jason
- There is a gap in “persona”
- I will try to take a stab on this
- Find the list of personas, we need to get the persona nailed, then I will come back help you
Allan
- Top two or three Personas, those are pretty common in STIX data:
  - Data feed providers
  - Tip providers
  - SIEM
- Those three personas are pretty obvious, the last a few are pretty advanced.
- Are all included
- The other personas are not as important they may not talk STIX native format
- 1.4.2 Personas, as for STIX 2.0 version we made choice on minimum things need done, now I come around, and agreed on that

Bret
- My concern is that make it simple, get it done first. We made this choice to get minimum viable things done, to release quickly. Getting something out door is far valuable.

Allan
- I will review other gaps, that’s good idea, I will review the list, I like Jason’s idea to review the persona list.

Jason
- May be we could send an email to the whole TC list, this is a very simple action. We can ask people to take look at the persona list, and see where their company’s product fit in this list. This is the area we need help: we need people to reach out and review the personas. This is very important; these personas’ will drive the interoperability’s use cases.

Allan
- I will craft an email to the STIX community, the entire group so we get a big/broader audience, request for review, let’s make sure we get everything covered. I think we have done that before,
- But it does not hurt to do that again. I added some Annotations on what MVPs are too
- Should I add or remove anything? What I just classified as MVP?

Jason
- What are we saying when we say “MVP”? are we trying.
- Define “MVP” personas

Allan
- I’d like to do is focus our effort for this version to define MVP definitions and same excises across different sharing for this version of the document. The strategy is based on my personal products, my company products. So that’s are most products do right now.
- We need define what means interoperability. Also focus on persona and I will write up the MVP definitions. Do they need all be defined?
- Sighting is MVP
- Indicator is MVP
- Versioning is MVP, all other elements are sharing

Jason
- Yeah, I look at ... this is should be MVP not personas
There are multiple dimensions

For example, vulnerability sharing, if we don’t cover in this version. Then vulnerability management products won’t be covered, because that’s their bread.

People work on the MVP stuff first, like myself, so I am focus on MVP first. But, people need to speak up, if you feel strongly that other object should be or is MVP. Anyone? Please speak up. If anything on this list if you feel should be MVP, then? Other than the three I marked?

Data Marking? How about Data Marking?

Maybe “report”?
If people feel strongly, then “yes”

If you feel strongly, then we can mark it.

Indicator is the golden child, that is MVP MVP

We should have started there. Any other MVP stuff? So Marlon, let me repeat, We do need add at least data market test. So if nothing else, I would like
Please record that we reviewed the list and agreed the following four should be MVP:
1. Indicator sharing - MVP
2. Sighting sharing
3. Visioning
4. Data Marking, we need at least basic data marking test
I would like to capture course of action: should be MVP
All you have to do is validate

No, how far down we are in the rabbit hole on this?

No? the test case called out are IPV4, IPV 6 two IP CIDR
  Indicator IPv4 Address
  Indicator IPv4 Address CIDR
  I added two Indicators with IPv4 Address CIDR
  Indicator with IPv6 Address
  Indicator with IPv6 Address CIDR
  Also added an example for IPV6 Multiple Indicators within the same bundle
  Added FQDN
  added URL, and I do have Indicator FQDN or URL
  And a combination example of URL and Domain

We added file hashes, domain, you were not on the call yet.
Two IPVs are in the same bundle, you are able to ingest data in your products, you have to understand the case correctly
Whether SIEM is capable of doing is beyond what we want to do here
Marlon
- Ok, I understood, may be course of action?

Allan
- This is based on STIX 2.0 right now,
  Marlon
- I don’t think we incorporated the OpenC2 stuff yet

Allan
- That’s correct

Bret
- then we get into the rabbit hole, I don’t think we should do that yet, let’s just get something done first. Let’s just get done. It’s more important we get something done than to cover everything.

Jason
- If no one in the vendors are doing the course of action right now, then?

Mark
- Speaking for Soltra per sa
  - Marking TLP specifically we use, something we will use in STIX 2.0
  - Indicator for the consumer portion it does not cover anything

Jason
- We need figure out, how we want to do intop TLP itself? what TLP test case is for?

Allan
- Here

Bret
- If I ask for amber red, should get every red. If everything below, then
  - That is really a function of TAXII

Mark
- I agree with Jason, not sure how people to with TLP

Bret
- TLP is important but that is really a function of TAXII, if you really want this, then you need to write proposal for TAXII to be done.

Allan
- I can imagine a couple cases we can craft. If data says TLP red, then
  - We can say data markings
  - We should provide data marking, then here is bare minimum you support
  - You should provide this as standard format

Bret
- If producer doesn’t want to do data marking, then we can’t force that.

Allan
- If you say you support data marking, then you need provided the basics
  - If you say you support TLP, then you have to do this XYZ…I think.
  - So please some body try to craft that out.

Bret
- Question for Allan:

Allan
I was thinking more semantic checking, the data block, these field must be same for example. They should be filling in these field with time stamps.

Bret
- What happens when you revoke?

Jason
- May be, we can look at create test scripts after this documents are done. We can do the same thing for indicator sharing.

Allan
- Let’s get these things flush out first, then we can look at automation stuff. We ran out time.
- Action items: Jason will review the persona list, Jane will help
- Jyoti: will get access to the document first, then may be contribute later.
- Course of Action -- Marlon like to contribute to it.
- Thanks everyone

Meeting Terminated