CTI-TC Working Group Meeting

Meeting Date: September 30, 2019
Time: 19:00 UTC
Purpose: Working group meeting on STIX/TAXII

Attendees:
Allan Thomson
Bret Jordan
Chris Lenk
Chris O'Brien
David Girard
Drew Varner
Emmanuelle Vargas-Gonzalez
Emily Ratliff
Gary Katz
Ivan K.
Jeff Mates
John-Mark Gurney
Justin Stewart
Marco Caselli
Marlon Taylor
Trey Darley
+1 unidentified phone attendee

Action Items:

- [Chairs] Send links to previous sponsorship documentation

Meeting Notes:
[Bret Jordan]
TAXII 2.1 public review ended August 28. Received editorial comments – many broken links were fixed. Paul Patrick requested that the example text about pagination be restored.
STIX 2.1 public review ends on September 12. If you have comments, send them to the cti-comments list. We currently have received comments on hashing, broken links, other editorial issues, and a request to add the TLSH fuzzy hash to the hashing open vocabulary.

[David] TLSH is a fuzzy hash, open source.

[Allan] This seems like a no-brainer, why would we not do this?

[John-Mark] We removed about half the hashed from the list about a year ago, why add a niche hash now?

[David] TLSH is currently used by MISP and Trend Micro.

[Trey] It is an open vocab, this isn't an efficient use of our time.

[Bret] We have to adjudicate every comment received.

[Trey] The T in TLSH stands for a company name and no company names should appear in the specification.

[Bret] Show of hands for who is in favor of adding it.

<6 hands raised>

[Bret] Who is opposed to adding it?

<No hands raised>

[Bret] Working call consensus to add w/Trey's caveat.

TAXII Pagination Issue <See slides for proposed text>
[Bret] The TAXII pagination example text is non-normative so with working group consensus it can be added without incurring another public review.

[] There is an issue with the example algorithm, if the pagination is based on the date, then more than the requested number of objects might be returned if more than that number came in on the date in question, or if the pagination cuts off some of the objects on that date, then some objects may be omitted from the results.

[Bret] This text will be emailed to the mailing list for commentary and updates.

Deterministic ID Fallback
[Bret] In implementing deterministic IDs, MITRE noticed that there are some SCOs where ID contributing properties are optional and some examples in the specification where the optional properties are omitted, so there are no properties for the deterministic ID to use. The spec does not contain guidance for what to do in most cases, but in one case recommends falling back to UUIDv4 which seems like the right thing to do. MITRE has requested that the spec be updated with this guidance.

[Allan] It would be a normative change but not a substantive change. It would be better to change the examples to contain properties.

[Chris] Examples are a separate issue. Examples can be changed without a spec rev.

[Trey] Does an open vocab addition require a spec rev?

[Bret] In the past, the TC has allowed open vocab changes without revving the spec. It is a TC decision.

[] Interoperability changes are handled by the Interop subcommittee, so it seems like it would be a great place to handle the deterministic ID fallback case. Fix the examples in the spec. Flag this issue – we won't make the changes if this is the only normative change, but if we have to rev the spec, then we will fix this at that time.

Sponsorship
[Bret]
We have 8 items needing sponsorship. Who will sponsor these items?

<silence>

The sooner we get sponsors for these items, the sooner we can publish as a standard. Trey and Rich will bring this up on the full TC call.

[Gary] What is required for sponsorship? We implemented deterministic IDs but for internal objects which are not STIX objects.

[Allen] Examples of prior sponsorship documents can be sent to the list.

[Marlon] Examples are available on page 2 of the TC cover page

[Bret] The chair will mail links to the examples to the mailing list.

TAXII Query
[Bret]
We had a call to merge the design ideas for TAXII query. If work progresses, then TAXII query will be released as a stand-alone document in 3-5 months. We won't hold up TAXII 2.1 for this feature, but will release query as standalone and then fold it into 2.2 when there is a need for another revision.

[Trey] Has there been any discussion about sponsorship for TAXII 2.1? Bret fully implemented. Open repos are in process of being updated.

[Marlon] Is it still possible to get query into 2.1 if TAXII 2.1 is held up waiting for STIX?

[Bret] TAXII 2.1 has been ready to go since December, and query will take several months to get right, so let's not hold up TAXII 2.1 for it.

[Allan] Concerns about query scalability.

[Allan] Has the call for nominations for Interop Co-chair closed?

[Trey] The call for nominations closes at 17:00 Eastern today.

**End of Meeting