CTI-TC Working Group Meeting

Meeting Date: July 16, 2019
Time: 20:00 UTC
Purpose: Working group meeting on TAXII

Attendees:
Allan Thomson
Bret Jordan
Chris O'Brien
Chris Lenk (cvoid)
David Girard
Drew Varner
Emanuelle Vargas-Gonzalez
Emily Ratliff
Ivan Kirillov
Marco Caselli
Paul Patrick
Robert Keith
Rich Piazza
Richard Struse
Sean Barnum
Trey Darley

[Bret Jordan]
Kicked off the meeting. STIX 2.1 CSD ballot is open until Friday (July 26). If it passes, STIX 2.1 will go for public review.

[Trey]
How do we report issues?

[Bret]
Copy the text and include it in an email to the working group.

TAXII 2.1 WD07 is almost ready for release. There have been substantive enough changes that it will require a 15 day public review.

One open update on version. The text leaves the action up to the server implementation what to use if version is not included in the object. Consensus was that the update was fine and it was accepted.

The issue of basic querying functionality came back up, specifically about pivoting and a decision about what to do must be made before TAXII 2.1 can proceed. There are 3 alternatives. Option 1: full TAXII query capability. Option 2: lightweight TAXII endpoint to allow pivoting on relationship. Option 3: tiered solution

[Emanuelle Vargas-Gonzalez]
Presented slides on option 3. [Slides were sent to the mailing list after the meeting on July 16, 2019; Subject: [cti] CTI TC Working Call: Slides on Tiered Proposal]

[Allan Thomson]
Have you implemented it?

[Emanuelle]
Not yet, but if there is interest then we will look into implementing it.

[Allan Thomson]
Proving that it works for real use cases will be difficult but necessary.

[Bret Jordan]
It would be possible to combine options 2 & 3.

[Trey]
Option 1 was pulled from TAXII 2.1 because it was tightly coupled with STIX 2.1 which wasn't ready at the time.

[Bret Jordan]
The key need is pivoting on relationships. Risks are delay to 2.1, lack of adoption of 2.1 due to missing features, pressure to release 2.2 early

Bret has implemented Option 2.

There are 5 options:
A: We do option 1 and delay TAXII 2.1
B: We only do option 1 but do it in TAXII 2.2+
C: We do option 2 [updated to include 3 during meeting] now for TAXII 2.1 and look at option 1 later
D: We do nothing now, ship TAXII 2.1, and address all of this at a later time
E: Try to find a merged solution

[Emanualle]
Votes for C

[Allan Thomson]
Option F: Implement the proposals and decide later based on fully implemented proposals

[Bret]
Calls for a straw poll showing of hands.
9 vote for D
3 vote for C

Solid consensus to do nothing now and address the topic in the future.

[Somebody, perhaps Paul or David asked]
Question about SEP. Is there something between 2.2 and 2.1 where features can be added?

[Bret]
Nothing formal but the TC wants people to implement new features and prove them out

[Trey]
While the SEP process has not been formalized there is an adequate playground to test out new feature – establish a MiniGroup to gain consensus

[Bret]
Volunteers to donate his time on a separate document on TAXII querying as well as on writing code to test the concepts.

Consensus ship 2.1. Bret and Trey will open ballot.

No call for next week. Bret will work with Jane to get calls scheduled every other week going forward.

**End of Meeting