CTI-TC Working Group Meeting

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

Attendees:
Bret Jordan
Caitlin Huey
Chris Lenk
Christian Hunt
David Girard
Drew Varner
Emily Ratliff
Gary Katz
Jason Keirstead
John-Mark Gurney
Marco Caselli
Robert Keith
Rich Piazza
Sarah Kelley
Trey Darley

Action Items:

- [Chairs] Revisit Github issue 70 during next meeting
- [Chairs] Revisit Github issue 164 during next meeting
- [All participants] Prepare to discuss resolution of these issues at next meeting
- [John-Mark, Jason, Drew, cvoid, Marco] Work on consensus proposal for issue 70

Meeting Notes:
[Bret Jordan]
Kicked off the meeting. STIX 2.1 CSD ballot closed Friday, July 26. Approximately 80% of eligible voters voted and everyone voted yes. There was 1 ballot comment. We filed the request in JIRA over the weekend to publish CSD02 for 1st public review. Desire is for everyone in the working group to have a clear understanding of the roadmap. Monday, July 29 starts the 6 month timer for implementations of each new substantial change in the spec. 2 sponsors are needed for each new feature [see meeting slides for list of features requiring sponsor]. Proof of concepts are ok, but the implementations have to do more than just serialize/deserialize the object. They should show that it works.

Rough timeframe, August will be dedicated to the public review period. We have until roughly mid-September to address comments from the public review. If changes are deemed to be substantive, then a new CSD will be required. Every public review after the first is 15 days.

[Sarah]
Each subsequent public review after the first, reviews only the changes made after the previous review, correct?

[Bret]
That is a great point. That is correct. The goal is to start winding down the changes. The end of January is the deadline for sponsorship work. Note that the CTI TC historically has shut down between the end of November and January.

[Trey]
What happens if we get substantive comments during public review?

[Bret]
We may need a new CSD to address them.

(During previous rounds) Jane led a group that did a lot of work on sponsorship. Allen found issues. Sponsorship is part of the process to make sure that we get things right.

It is possible to do multiple CS's. It has not been traditionally done by this TC, but it is part of the OASIS process. Please be patient with the number of ballots that this process entails and please vote early and diligently.

[Emily]
What do sponsors have to do to show that they did the work?

[Bret]
Come back and show what you have done and talk about it. Mention any issues that you faced during development. The TC does not require source code, merely assertion and a list of issues. Jane's previous work is the ultimate high bar. If after 6 months, there are not two implementations, then the feature will get dropped.

[Emily]
What if it is a fundamental feature like SCOs as a top-level object?

[Bret]
Hopefully that won't happen. If it does, we will have to come together as a TC and decide what to do.

There were 3 comments from John-Mark, Jason, and Chris Lenk. John-Mark's was a ballot comment that things would have to change otherwise will result in a no vote on CS.

[John-Mark]
Github issue 70 is the big one. Changes were made without proper understanding and my objections were not listened to.

[Bret]
Issue was discussed on a couple of working calls which led to the consensus for what is included in the document.

[Jason]
My concerns were around the conformance requirements for cyber observables as top-level objects. The conformance requirements should be strengthened.

[Bret]
Please enter your comment as a public comment within the next 30 days.

[Chris]
Hashes is an open vocabulary but there are several places in the document [see meeting slides for full list] where there is a MUST requirement for the hash to be listed in the open vocabulary. This is like saying that something MUST come from any type.

There are 3 possible ways to solve this: 1) change the open vocab to an enum, or 2) change the MUST to a SHOULD, or 3) make it a defacto enum, an open vocab that can't be added to.

[John-Mark]
Need clean-up around open vocabulary

[Bret]
Could list the allowed hashes explicitly rather than using the open vocab.

[Jason]
There was a reason it was an open vocab to allow for additional hashes. It should be a should

[John-Mark]
But for some uses, we want a fixed list of hashes.

[Jason]
Yes, it is a problem. We didn't consider uses cases when we created the open vocab.

[Rich]
Artifact lists 4 of the 6 hashes. It is confusing.

[Bret]
How best do we fix this?

[John-Mark]
We should promote the use of safe hashes.

[Bret]
Options 1) clarify text, 2) use an enum, 3) create 2 has vocabs, 1 enum and 1 open vocab.
Let's come back to this one on the next call. We can make a decision at the end of the public review.

[See slides for full list of Chris Lenk's editorial suggestions] Does anyone have additional editorial suggestions?

Now on Github Issue 70

[Drew]
Observations can be combined in nonsensical ways in patterns. Proposal to limit to 1 each of WITHIN, startstop, REPEAT. John-Mark wants more complex patterns. Patterns should parse to actionable AST. Proposed changes to ANTLR grammar but didn't meet one of John-Mark's requirements.

[John-Mark]
The restriction to just one is to strict and omits valid patterns. This is a compiler optimization problem. The proposals are overly restrictive.

[Jason]
My perspective is aligned with Drew's perspective. Even if it makes sense logically, there is no use case for multiples. Feedback that we have received from customers is that it is confusing to have multiples and no one knows what ti means. Who will write expressions like this in reality?

[John-Mark]
Even with this restriction, if you want to provide backwards compatibility to STIX 2.0 you will have to parse multiples. I have given a valid use case for wanting multiple WITHINs.

[Bret]
Let's have a straw poll. Who supports the more strict view as in the current document – 2
Who supports the broader view – 4
Some people didn't vote but generally support the concept of a strict and correct grammar. No consensus.

[Sarah]
If no consensus for making a change, then we default to not making the change

[Bret]

Please work together to see if you can come to a consensus and produce a proposal before the next meeting.
[Trey]
Would like for John-Mark to have the opportunity to produce a proposal

[Bret]
Agreed. Would like to see a proposal before the next meeting.

Github issue 164
[John-Mark]
If a property matches the default, it can be omitted. This leads to different behavior for EXISTS when the property is present and matches the default and when the property has been omitted because it matches the default. Proposal is for EXISTS to to return false of the property exists and matches the default.

[Drew]
No comment

[Jason]
Need to evaluate. Undefined behavior is not desirable for this very common scenario

[Bret]
Do you support the proposal?

[Jason]
Not sure. Need to evaluate what part of pattern this is for.

[Bret]
We will pick up issue 164 on the next call.

Next meeting is currently scheduled for August 20.

**End of Meeting