# CTI-TC Working Session

| | |
|---|---|
| **Meeting Date:** | **February 19, 2019** |
| **Time:** | **3:00 p.m. EST** |
| **Purpose:** | **Weekly Working Session** |

**Attendees:**

| | | |
|---|---|---|
| Richard Struse | Bret Jordan | Jane Ginn – Recorder |
| Trey Darley | Sean Barnum | Jason Keirstead |
| Shawn Riley | John-Mark Gurney | Marlon Taylor |
| Caitlin Huey | Jeff Mates | Gary Katz |

**Agenda:**

- **Discuss Roadmap for STIX 2.1 Release**

**Meeting Notes:**

Richard Struse

We made a lot of progress at F2F – We have developed a Roadmap for getting STIX 2.1 out

We will hold off on STIXPreferred until it is out

Discussed when "done" is done – Believes within 2 to 3 months – a Feature Complete draft

We'll be finalizing through the review process

Trey Darley

You should have all received the mail with the notional WorkPlan [*Inserted Below*].

**********

Proposed CTI TC Roadmap for STIX 2.1 Completion

---

1) Complete the ongoing SCO Integration into Main STIX 2.1 Documents:
 * SCO Integration
 * Grouping Object
 * Malware + Malware Analysis Objects
2) Publicize the revised draft specifications and ask for review by the TC.
3) Merge in revised Infrastructure SDO to STIX 2.1 (as discussed during the January F2F).
4) Drive to consensus on the discussion thread about whether to permit UUIDv5 (in addition to UUIDv4) for all STIX Objects.
5) Resolve any remaining inconsistencies in the STIX 2.1 specifications.
6) Issue a STIX 2.1 CSD02 for TC review.
7) The additions to CSD02 (SCO changes, Grouping, Malware, etc.) are validated to have interoperability tests defined and two or more sponsors attest to interoperable implementations, as per the process we're using to validate Internationalization, Location, etc.
8) Review feedback from Sponsors based on their POC implementations.
9) In parallel with the sponsor vetting of STIX 2.1 CSD02, complete TAXII 2.1.
10) Update the interoperability test specs for STIX/TAXII 2.1 STIX Preferred.
**********

Jason Keirstead

I noticed that the SEP process is not included in that list

I'd feel a lot more comfortable if we had that in STIX 2.1

Trey Darley

We devoted a lot of time during the face-to-face – but, we found that with

The other changes, the window of opportunity might close

Those at the face-to-face came to the conclusion that

We needed to get STIX 2.1 out the door

Marlon Taylor

Asked 2 questions:

1. Can we move forward with CSD 01 to a CS?
2. Can we have the SEP process as a Committee Note, rather than a part of the CSD?

I don't know if the SEP needs to be rolled into a CS

Richard Struse

I am reporting what some of the others suggested earlier on.

On 1. STIX is missing some features that need to be added – we put time in at F2F

On2. We do have Custom Objects in the current version

Working on SEP in parallel, but out of cycle with STIX 2.1, would be a viable option

Sean Barnum

To address Marlon's question – I don't think we can move forward on a CS for STIX 2.1

On the SEP thing – we find it valuable – at F2F – we all agreed –

But, it needs lots of work – That does not mean we don't start working on SEP

Trey Darley

STIX 2.0 was an MVP – We signaled to the community that we would be closing the gap

For feature parity in STIX 2.1

[*Discussed some of the new additions*]

We have been communicating "This is the tranche of work for STIX 2.1"

We don't want to undermine the trust of the community and issue a CS

On Marlon's 2nd question, we have too many open questions to finalize the SEP

The whole purpose of a Roadmap – is to focus on our main objectives

Bret Jordan

I think the reason we have the Roadmap is to focus around 1 thing

So, doing SEPs in parallel – would be counter to what we are trying to do

Richard Struse

A fair point – as a TC, for what we will cover – if a couple of people that want to go

And develop SEPs

Trey Darley

I'd like to call out Bret Jordan for all of the work he has done to merge the documents

My understanding is that this material will be available in the next few days

Bret Jordan

Just to give you an update on this… most of the substantive comments have been merged

There is something we still need to do about the Cyber Container concept

Al of the fundamental changes are in there.

Trey Darley

To that point, we'll need the next few working calls to finish out some of these items

Bret Jordan

There are some inconsistencies – these need to be addressed

Trey Darley

Reflecting back on the work so far – we are very close

Jane Ginn

Infrastructure? I don't see on the #1

Sean Barnum

It is item #3 on the list from Trey's email

Jane Ginn

OK, I see it now

Trey Darley

We wanted to address the SCO tranche first so we moved it to #3

Yes, that is a very important SDO

Would anyone have any objections if we present this to the rest of the TC?

Hearing none, we will proceed ahead.

Thanks all!

Meeting Terminated

**********