



CTI-TC Monthly Meeting: Session #2

Meeting Date: February 21, 2019
Time: Session #2 – 9:00 PM US EST
Purpose: Monthly CTI TC Meeting
Attendees:

Name	Company	Role
Kai Li	360 Enterprise Security Group	Member
Robert Coderre	Accenture	Voting Member
Dean Thompson	Australia and New Zealand Banking Group	Voting Member
Jane Ginn	Cyber Threat Intelligence Network, Inc.	Secretary
Ryan Joyce	DarkLight, Inc.	Member
Jackie Eun Park	DHS C&C	Member
Preston Wertz	DHS C&C	Voting Member
Chris Ricard	FS-ISAC	Voting Member
Ryusuke Masuoka	Fujitsu Limited	Voting Member
Toshitaka Satomi	Fujitsu Limited	Voting Member
Koji Yamada	Fujitsu Limited	Voting Member
Kunihiko Yoshimura	Fujitsu Limited	Voting Member
Kazuo Noguchi	Hitachi, Ltd.	Member
Jason Keirstead	IBM	Voting Member
Richard Struse	Mitre Corporation	Chair
John-Mark Gurney	New Context Services, Inc.	Voting Member
Curtis Kostrosky	Symantec Corp.	Voting Member

Agenda:

- Introduction & Welcome (Trey & Rich)
- Roadmap for STIX 2.1 & TAXII 2.1
- Subcommittee Updates
- STIXPreferred Update
- Community Development Center
- Open Discussion on 2.1 Launch

Meeting Notes:

Richard Struse

Kicked-off meeting – Went over Agenda – Discussed the F2F & outcomes

Preston Wertz

Delay in the contract for MITRE support – government shutdown affects schedule

Circumstances of shut-down – Hope to have MITRE contract back

In one week or earlier

Richard Struse

A full and important Agenda:

Discussed the recommended Roadmap

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.

Talked about priorities, and how to focus the Working Calls and discussions on the list

[Mentioned importance of Malware + Malware Analysis + Infrastructure = 2.1]

[Noted that STIXPreferred will not get any traction until STIX 2.1 is finished]

Ryu Masuoka

[Asked a question about the time schedule]

Richard Struse

[Walked through the committee timeline & OASIS review process]

Ryu Masuoka

Number 8?

Richard Struse

Yes, we are watching the input from the Sponsors – and incorporating findings

Ryu Masuka

Asked about the time-span of Roadmap

Richard Struse

It could be 60 days – it depends on the TC

[Discussed the importance of focusing on the Roadmap in the Working Calls]

Ryu Masuka

STIXPreferred is CSD 02?

Jason Keirstead

We are putting a hold on updating STIX 2.x until the STIX 2.1 is finalized.

Richard Struse

Noted the schedule for the Sponsor documents

Jane Ginn

Confidence is a Property – Different from the rest of the SDOs

Jason Keirstead

[Gave update on STIXPreferred Program]

But Site is up: <https://oasis-stixpreferred.org/>

Richard Struse

[Gave update on status – Noted the outstanding Query & Pivoting function]

[Gave update on Community Development Center]

[Gave update on Launch for STIX 2.1]

Thanks to all – Connect at RSA Conference.

Meeting Terminated
