CTI-TC Monthly Meeting: Session #1

Meeting Date: **February 21, 2019**
Time: **Session #1 – 11:00 AM US EST**
Purpose: **Monthly CTI TC Meeting**
Attendees:

Name	Company	Role
Kyle Maxwell	Accenture	Voting Member
Nicholas Hayden	Anomali	Voting Member
Russell Matbouli	Anomali	Voting Member
Trey Darley	CCB/CERT.be	Co-Chair
Jane Ginn	Cyber Threat Intelligence Network, Inc.	Secretary
Ian Roberts	DarkLight, Inc.	Member
Jaeden Hampton	DarkLight, Inc.	Member
Patrick Maroney	DarkLight, Inc.	Member
Ryan Hohimer	DarkLight, Inc.	Member
Shawn Riley	DarkLight, Inc.	Member
Will Urbanski	Dell	Voting Member
Marlon Taylor	DHS	Voting Member
Aukjan van Belkum	EclecticIQ	Voting Member
Caitlin Huey	EclecticIQ	Voting Member
Christopher O'Brien	EclecticIQ	Voting Member
Tom Vaughn	EclecticIQ	Voting Member
Gary Katz	FireEye, Inc.	Voting Member
Paul Patrick	FireEye, Inc.	Voting Member
Sean Barnum	FireEye, Inc.	Voting Member
Shyamal Pandya	FireEye, Inc.	Voting Member
Devesh Parekh	IBM	Voting Member
John Morris	IBM	Voting Member
Beth Pumo	Kaiser Permanente	Voting Member
Allan Thomson	LookingGlass	Voting Member
Dennis Hostetler	LookingGlass	Voting Member
Matt Pladna	LookingGlass	Voting Member
Vlad Serban	LookingGlass	Voting Member
Richard Struse	MITRE	Co-Chair
Daniel Dye	NC4	Voting Member
Mark Davidson	NC4	Voting Member
Michael Butt	NC4	Voting Member
Takahiro Kakumaru	NEC Corporation	Voting Member
Christian Hunt	New Context Services, Inc.	Voting Member
Daniel Riedel	New Context Services, Inc.	Member
Aubrey Merchant	Symantec Corp.	Voting Member
Bret Jordan	Symantec Corp.	Voting Member
Michael Mauch	Symantec Corp.	Voting Member
Robert Keith	Symantec Corp.	Voting Member

David Girard	Trend Micro	Member
Jeffrey Mates	US Department of Defense (DoD)	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

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.

Allan Thomson

Made a comment about the ordering of the Roadmap items as a practical approach

Only 1 person from each organization (typically) working

Richard Struse

Made clarification on the 'pause' for TAXII 2.1

Reviewed definition of "doneness" for an SDO => Six-month time-window

Allan Thomson

Please speak-up if you do not agree with the Roadmap

Trey Darley

Let's focus our limited cycles on this Roadmap

Richard Struse

It is important to make decisions and choices

Hearing no objection, we intend to use this to drive the Agenda in coming weeks

Patrick Maroney

It looks like we have not achieved quorum in this meeting

Trey Darley

That is true, but we have not made a motion

Richard Struse

We had hoped to have STIX 2.1 done sooner – But, we have the finish line in sight

Reviewed the entire process for public review

Marlon Taylor

Update on the DHS contract discussions with MITRE

It is hoped that it would be done within the next 2 days

It would be for 1 year – Contract renewal through this time next year

Allan Thomson

We not going to do another version of STIXPreferred until we finish STIX2.1

We will update the test specifications

However, the Portal is live:

https://oasis-stixpreferred.org/

[*Went through the review & approval process*]

We will work on STIX 2.1 once it has been updated

Bret Jordan

Working Draft 07 is ready to go – we have incorporated all of the edits

We have received 2 different query & search proposals

Then the TC will need to make a decision to ship as-is

Or incorporate one of the Query proposals

Richard Struse

We'll be in a much better place to make a decision on this in 30 days

When we will tackle that as a TC

We had planned on having a demo on our Community Corner – that has been postponed

Please do reach out if you want to demo something you are doing

So, now, we started a discussion of the 'Launch' for STIX 2.1

Consensus was: we should put our focus on Launch

What should we do? PlugFest, F2F, Trainings?

There is still a lot of community awareness to be done

Feel free to reach out to Trey and I and Jane, or any of the Co-Chairs

We will run this meeting again tonight at 9:00 pm US EST

Meeting Terminated

****