CTI-TC Monthly Meeting: Session #1

Meeting Date: October 18, 2018
Time: Session #1 – 11:00 AM US EDT
Purpose: Monthly CTI TC Meeting
Attendees:

Name	Company	Role
Jane Ginn	Cyber Threat Intelligence Network	Secretary
Sean Barnum	FireEye, Inc.	Voting Member
Gary Katz	FireEye, Inc.	Voting Member
Anuj Kumar	FireEye, Inc.	Member
James Meck	FireEye, Inc.	Member
Shyamal Pandya	FireEye, Inc.	Member
Paul Patrick	FireEye, Inc.	Voting Member
Masato Terada	Hitachi, Ltd.	Member
Jason Keirstead	IBM	Voting Member
John Morris	IBM	Voting Member
Beth Pumo	Kaiser Permanente	Voting Member
Jamison Day	LookingGlass	Voting Member
Dennis Hostetler	LookingGlass	Voting Member
Matt Pladna	LookingGlass	Member
Vlad Serban	LookingGlass	Member
Allan Thomson	LookingGlass	Voting Member
Jonathan Baker	Mitre Corporation	Member
Sarah Kelley	Mitre Corporation	Voting Member
Ivan Kirillov	Mitre Corporation	Voting Member
Chris Lenk	Mitre Corporation	Voting Member
Richard Piazza	Mitre Corporation	Voting Member
Richard Struse	Mitre Corporation	Co-Chair
Emmanuelle Vargas-Gonzalez	Mitre Corporation	Member
John Wunder	Mitre Corporation	Voting Member
John Anderson	NC4	Member
Michael Butt	NC4	Voting Member
Daniel Dye	NC4	Voting Member
Natalie Suarez	NC4	Voting Member
Trey Darley	New Context Services, Inc.	Co-Chair
John-Mark Gurney	New Context Services, Inc.	Voting Member
Drew Varner	NineFX, Inc.	Voting Member
Bret Jordan	Symantec Corp.	Voting Member
Robert Keith	Symantec Corp.	Voting Member
Michael Mauch	Symantec Corp.	Member
Aubrey Merchant	Symantec Corp.	Voting Member
Richard Shok	U.S. Bank	Voting Member
Jeffrey Mates	US Department of Defense (DoD)	Voting Member

Agenda:

- TC structural change update
- STIXPreferred update
- Community Development Corner
- Subcommittee updates
- NYC F2F recap
- Q&A

Meeting Notes:

Richard Struse

Welcome to all – Record your attendance – There will be another session later tonight
[*Went through the organizational changes*]
Welcome to my new Co-Chair, Trey Darley

- We added a TC co-chair.
  - During the September CTI TC calls this was approved by unanimous consent.
  - Following a call for nominations (during which Jason Keirstead and Trey Darley were nominated), a ballot was opened to elect the new CTI TC co-chair.
  - Trey Darley was elected by the CTI TC. Trey has already stepped down as Cyber Observables SC co-chair
- We are folding responsibility for Cyber Observables into the STIX subcommittee, eliminating Cyber Observables as a subcommittee.
  - During the September CTI TC calls this was approved by unanimous consent. Rich and Trey are working with OASIS staff to update Kavi to reflect this change.
  - John Wunder has stepped down as STIX co-chair, leaving Sarah Kelley and Ivan Kirillov as STIX SC co-chairs.
- Mark Davidson has stepped down as TAXII SC co-chair, leaving Bret Jordan as the sole chair of the TAXII SC for the moment.
- The TC can decide whether to backfill this role but in the judgement of the TC leadership, based on the current development velocity of TAXII2, a single SC chair is probably sufficient for now.

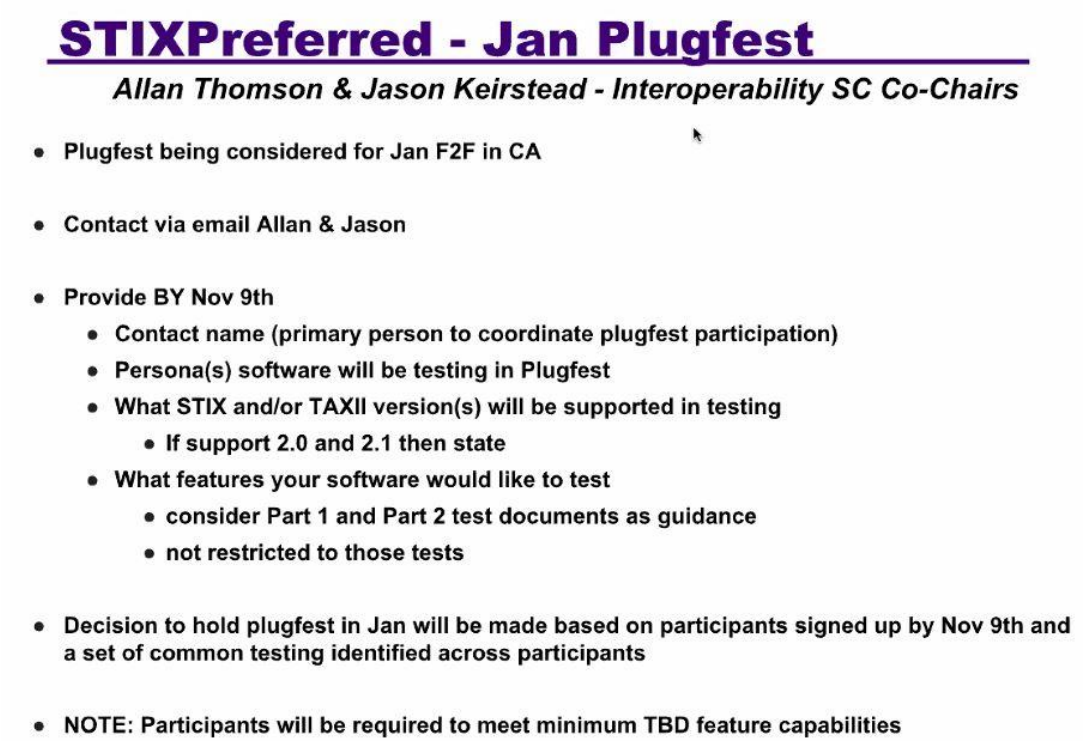
Trey Darley

Thanks to all – I'm honored – Updates should be made on Kavi
Let us know if you see anything else that needs to be updated

Allan Thomson

Part 2 is available for review:
https://docs.google.com/document/d/1VY-uz3qnWpF8LMCWLgB_tY3uVLmw_lVcuXSwgdGEFHc/edit#heading=h.gjdgxs
[*Richard Struse emphasized importance of reviewing the document*]
Went over the STIX Preferred Program
[*Gave Demo of the Portal*]
https://docs.google.com/document/d/1MCnrLR4m1CnkqZcLM0FcIzgJrvId3on3GTkqcwtdH1I/edit#
[*Emphasized importance of using the review document on making comments*]

https://docs.google.com/document/d/1MCnrLR4m1CnkqZcLM0FcIzgJrvId3on3GTkqcwtdH1I/edit#heading=h.i3o6gvkwteti



Marlon Taylor

Asked whether remote participation would be possible

Allan Thomson

[Pointed out that it is difficult, but can be done under special circumstances]

Ivan Kirillov

Presented Sightings Paper

https://docs.google.com/document/d/1QWgCi2HkVXFje5T3p8hxxVij8zb2eKEcciKZmeIQXjg/edit#

Comment period is still open [*Went over some of the key topics they covered and feedback*]

- Semantic Equivalence
  - https://docs.google.com/document/d/1zPqKX9LY8wB9Prj_aua0iD505ti6k7jY5PWLwEd731U/edit#
- Close of comments: Oct. 31st
- Plan is to submit both as an OASIS non-standard track work product once their content is finalized

Sarah Kelley

- STIX 2.1 CSD01
  - The ballot was approved, the countdown clock has begun.
  - April 2, 2019 is the deadline for “DONE”
- Continuing work on:
  - STIX Enhancements Proposals (SEPs) and supporting TC processes
  - Observables
  - Infrastructure (and how it uses observables)
  - Malware (and how it uses observables)
  - ACH Proposal (SEP?)

Name	Sponsors (2 needed)	Due Date
Confidence	IBM (tentative), DHS, New Context (tentative)	April 2, 2019
i18n	Fujitsu, New Context	April 2, 2019
Location	DHS	April 2, 2019
Note	DHS, JP Morgan, CTIN	April 2, 2019
Opinion	DHS, JP Morgan, CTIN, Perch, New Context (tentative)	April 2, 2019

Need additional sponsors!

Bret Jordan

- TAXII 2.1 CSD01 was approved
- Current Work Items
  - TAXII Wrapper
  - Some URL Parameters (limit, stix versions)
  - Query
  - Wordsmithing and document cleanup
- Submit Working Draft 04 to the TC for review
  - Plans for CSD02 and 2.1 CS

Sarah Kelley & Trey Darley

SEPs

- https://github.com/oasis-open/cti-sep-repository

Observables / Malware / Infrastructure

- Modeling two possible solutions using the same use cases (https://docs.google.com/document/d/1puPuKVWNSelrWH05yu9It99OuqQGdYo_Et0nmZKAZz8/edit)

1 Prime – Headed up by Sean Barnum

Option 7 – Expanding Observed Data Object – John Wunder and Ivan Kirillov

[*Bret Jordan made a point about how Relationships will be handled*]

Discussion of breaking Malware SDO into two parts

The working call next week will be on that topic

TAXII

- Adding a "limit" parameter
- Adding a TAXII envelope/bundle
- Adding an alias to Collection resource
- Mandatory properties on Manifests

Minor Issue Triage

- Check GitHub for latest changes
- (https://github.com/oasis-tcs/cti-stix2/issues)

Richard Struse

[*Talked about the next Face to Face meeting*]

Save the Date!

January 29-31 2019 at Fujitsu in Sunnyvale, CA USA

GCDP North Café
Fujitsu Sunnyvale Campus
1250 E. Arques Avenue
Sunnyvale, CA 94085-5401

Fujitsu Sunnyvale Campus Map

OASIS

[*Emphasized points about dates and need to finalize plans for PlugFest*]
If you are interested in hosting a PlugFest reach out to me and Trey and Jane Ginn
If you are willing to help with the planning for the PlugFest, reach out to Allan and Jason

We do this again at 9:00 pm Eastern Time!

Thank you all for joining!

Meeting Terminated
****