CTI-TC Monthly Meeting: Session #1

Meeting Date: **September 19, 2019**
Time: **Session #1 – 11:00 AM US EDT**
Purpose: **Monthly CTI TC Meeting**

Attendees:

Name	Company	Role
Maxwell, Kyle	Accenture	Voting Member
Ginn, Jane	Cyber Threat Intelligence Network, Inc.	Secretary
Russett, Stephen	Cyber Threat Intelligence Network, Inc.	Member
Joyce, Ryan	DarkLight, Inc.	Voting Member
Riley, Shawn	DarkLight, Inc.	Voting Member
Roberts, Ian	DarkLight, Inc.	Voting Member
Park, Jackie Eun	DHS Office-Cybersecurity and Communications	Voting Member
Huey, Caitlin	EclecticIQ	Voting Member
O'Brien, Christopher	EclecticIQ	Voting Member
van Belkum, Aukjan	EclecticIQ	Voting Member
Ricard, Chris	FS-ISAC	Voting Member
Patrick, Paul	FireEye, Inc.	Voting Member
Noguchi, Kazuo	Hitachi, Ltd.	Member
Lee, Chenta	IBM	Member
Morris, John	IBM	Voting Member
Ratliff, Emily	IBM	Voting Member
Williams, Ron	IBM	Voting Member
Casey, Tim	Intel Corporation	Voting Member
Marr, Karin	Johns Hopkins University Applied Physics Lab	Observer
Pumo, Beth	Kaiser Permanente	Voting Member
Hostetler, Dennis	LookingGlass	Voting Member
Pladna, Matt	LookingGlass	Voting Member
Serban, Vlad	LookingGlass	Voting Member
Stewart, Justin	LookingGlass	Member
Kirillov, Ivan	Mitre Corporation	Voting Member
Lenk, Chris	Mitre Corporation	Voting Member
Piazza, Richard	Mitre Corporation	Voting Member
Vargas-Gonzalez, Emmanuelle	Mitre Corporation	Voting Member
Butt, Michael	NC4	Voting Member
Davidson, Mark	NC4	Voting Member
Dye, Daniel	NC4	Voting Member
Gurney, John-Mark	New Context Services, Inc.	Voting Member
Riedel, Daniel	New Context Services, Inc.	Voting Member
Storms, Andrew	New Context Services, Inc.	Voting Member
Varner, Drew	NineFX, Inc.	Voting Member
Caselli, Marco	Siemens AG	Member

Name	Company	Role
Jordan, Bret	Symantec Corp.	Voting Member
Keith, Robert	Symantec Corp.	Voting Member
David Girard	TrendMicro	Voting Member
Mates, Jeffrey	US Department of Defense (DoD)	Voting Member

Agenda:

- Introduction & Welcome
- Sub-Committee Updates
  - STIX
  - TAXII
- Call for Community Development Corner (CDC) demos
- Discuss future Face-to-Face Meetings

Meeting Notes:

Richard Struse

Welcome to all. Reviewed OASIS rules about meetings open to Members only.

Administrative Updates

Welcome to Emily and Stephen Russett

Jason Kierstead will be stepping down – We will be issuing a call for nominations

Welcome to Ed Cabrera – Discussion on need for people to step up and help

Bret Jordan

Public Review Closed Sept. 12th

Resolved nearly all comments – Some discussion on how resolved

Vulnerability SDO updates –

Discussion on Patterning SCOs – No consensus on the call – Follow-up

Proposed Text for Vulnerability SDO

Old Text

A Vulnerability is "a mistake in software that can be directly used by a hacker to gain access to a system or network."

New Proposed Text

A Vulnerability is a weakness or mistake in the requirements, designs, or implementations of the computational logic (e.g., code) found in software and some hardware components (e.g., firmware) that can be directly exploited to negatively impact the confidentiality, integrity, or availability of that system.

Does this constitute a material change? Meaning, does this change have a functional impact on existing implementations such that they'd have to change to remain conformant?

Richard Struse

Asked if there was anyone who believes this is a Non-Material change – No CSD added

Tim Casey

I don't know how solid this definition is. Suggested changing the work "mistake" to "defect"

Bret Jordan

Asked for objections – None

Richard Struse

Hearing no objections – adopted

Bret Jordan

Need Sponsors for each of these

- Course of Action (COA)
- Grouping
- Infrastructure
- Malware
- Malware Analysis
- Other
  - SCOs as top-level objects
  - SCO relationships
  - Deterministic IDs

Richard Struse

This is a happy place for us to be – Great work from a MVP w/ 2.0 to now w/ 2.1

There are many of you that have asked for different features

Now at point where we have successfully gotten them into the Spec.

We need the code or the Attestation

Bret Jordan

There is a Template that Jane has developed

Jane Ginn

Clarified that the COA SDO is the current Template – Sanitized and updated

Make a copy and link to the Cover Page

Bret Jordan

Mitre has done a great job with the Deterministic IDs

Richard Struse

Do you have a message about it being "feature complete"

Bret Jordan

At this stage – from what we've heard, we are not hearing that there are gaps

The main structure of STIX 2.1 is feature complete

You can feel confident that this is complete

Daniel Riedel

How can we accelerate that?

Bret Jordan

Went back to the list of Sponsors

Daniel Riedel

New Context is volunteering to help complete that

Trey Darley

For Sponsorships – Where it is an Attestation – should there be a Co-Attestation

For Interopability

If an organization Attests that there are issues that show need for material changes

We should discuss on a working call

Bret Jordan

TAXII 2.1 New Features Implemented By

- Pagination was refactored (FreeTAXII)
- Delete Endpoint added (FreeTAXII, MITRE)
- Versions Endpoint added (FreeTAXII, MITRE)
- Added limit URL parameter (FreeTAXII)

Is there anything else that needs to be done for TAXII 2.1?
Can we move this forward as a CS and ship TAXII 2.1?

I have implemented a TAXII server and it is available as open source – w/ pagination
Has anyone implemented a TAXII server with pagination? No response
We do need at least one more group to implement –
We can address other items in TAXII 2.2

Richard Struse
As soon as we get one more implementation we'll ask OASIS to start the process
We will approve by Unanimous Consent after we get a 2nd implementation
Report on Interoperability

Stephen Russett
I will be working with the new Co-Chair to develop the Interop Docs for 2.1
I will also be doing a Java implementation

Paul Patrick
[Walked through his side-by-side comparison of changes from STIX 2.0 to STIX 2.1]
Available at:
https://www.oasis-open.org/apps/org/workgroup/cti/download.php/65918/STIX%202%20Changes.pdf

Richard Struse
Discussion on the need to start planning for Face-to-Face meetings and Plugfests
For 2020

Trey Darley
I can see the following for the Agenda for 2020: Codify SEP & Incident SDO

Bret Jordan
[*Clarified point about need to let the market drive adoption of STIX 2.1*]
And TAXII 2.1 – Continue to work privately on TAXII 2.2
But, let market adoption move forward

Richard Struse
Watch for the call for nominations for Co-Chair for the Interop SC
Thanks everyone – we'll have another session this evening at 9:00 pm EDT

Meeting Terminated
****