CTI-TC Monthly Meeting: Session #1

Meeting Date: January 17, 2019
Time: Session #1 – 11:00 AM US EDT
Purpose: Monthly CTI TC Meeting

Attendees:

Name	Company	Role
Coderre, Robert	Accenture	Member
Hayden, Nicholas	Anomali	Voting Member
Matbouli, Russell	Anomali	Member
Ginn, Jane	CTIN	Secretary
Hohimer, Ryan	DarkLight, Inc.	Member
Maroney, Patrick	DarkLight, Inc.	Member
Riley, Shawn	DarkLight, Inc.	Member
Roberts, Ian	DarkLight, Inc.	Member
Urbanski, Will	Dell	Voting Member
Fox, Steven	Supporting DHS	Guest
Huey, Caitlin	EclecticIQ	Voting Member
O'Brien, Christopher	EclecticIQ	Voting Member
van Belkum, Aukjan	EclecticIQ	Voting Member
Vaughan, Tom	EclecticIQ	Voting Member
Woodruff, Joseph (Jesus)	EclecticIQ	Member
Ricard, Chris	FS-ISAC	Voting Member
Barnum, Sean	FireEye, Inc.	Voting Member
Katz, Gary	FireEye, Inc.	Voting Member
Meck, James	FireEye, Inc.	Voting Member
Pandya, Shyamal	FireEye, Inc.	Voting Member
Patrick, Paul	FireEye, Inc.	Voting Member
Bishop, Adrian	Huntsman Security	Voting Member
Keirstead, Jason	IBM	Voting Member
Morris, John	IBM	Voting Member
Parekh, Devesh	IBM	Voting Member
Ratliff, Emily	IBM	Member
Williams, Ron	IBM	Voting Member
Darley, Trey	Individual	Chair
Casey, Tim	Intel Corporation	Voting Member
Pumo, Beth	Kaiser Permanente	Voting Member
Hostetler, Dennis	LookingGlass	Voting Member
Pladna, Matt	LookingGlass	Voting Member
Thomson, Allan	LookingGlass	Voting Member
Kelley, Sarah	Mitre Corporation	Voting Member
Kirillov, Ivan	Mitre Corporation	Voting Member
Lenk, Chris	Mitre Corporation	Voting Member
Piazza, Richard	Mitre Corporation	Voting Member

Struse, Richard	Mitre Corporation	Chair
Vargas-Gonzalez, Emmanuelle	Mitre Corporation	Voting Member
Butt, Michael	NC4	Voting Member
Davidson, Mark	NC4	Voting Member
Suarez, Natalie	NC4	Voting Member
Kakumaru, Taka	NEC	Voting Member
Varner, Drew	NineFX, Inc.	Voting Member
Hare, Forrest	SAIC	Member
Jordan, Bret	Symantec Corp.	Voting Member
Keith, Robert	Symantec Corp.	Voting Member
Kostrosky, Curtis	Symantec Corp.	Voting Member
Mauch, Michael	Symantec Corp.	Voting Member
Merchant, Aubrey	Symantec Corp.	Voting Member
Girard, David	Trend Micro	Member

Agenda:

- Introduction & Welcome
- STIXPreferred Update
  - Action on Operating Rules
  - Test example with set of logs
- Update on Cyber Observables Mini-Group
- JSON Canonicalization
- Sub-Committee Updates
  - TAXII
  - STIX
    - Example: Sponsor Document (Opinion)
- F2F Update - Sunnyvale
  - Call for topics

Meeting Notes:

Trey Darley

Welcome everyone! We have a full Agenda…. Let's get started

I'll turn it over to Allan.

Allan Thomson

[*Gave an update on the STIXpreferred activities & Pre-Launch Activities*]

https://docs.google.com/document/d/1oHgP1moU3yMYiDEoUALEiv5wjA9LNZlfYGED-LHfqkU/edit#heading=h.ri09gds88ev4

Richard Struse

[*Gave an update on why the Trademark is being used for the STIXpreferred program*]

Allan Struse

We want to reach out to the activities that plan to do a Certification for

One or more personas – we will add your company to the launch materials

We'll send an email to the TC – Please reply to the email – Ask questions

We would like to have as many people as part of the launch

New Topic

[*Went over the proposed Operating Rules*]

https://docs.google.com/document/d/11hAS1mkMPtyUqSAs94ExT_9Nu7ZrA385_VhtaF1mgwM/edit#heading=h.xf56p6m9z11l

[*Called for a Vote to approve the Operating Rules by Unanimous Consent*]

Bret Jordan seconded the motion

Richard moderated the action – **APPROVED BY UNANIMOUS CONSENT**

Moving forward to STIX 2.1

Req: Must have at least 1 STIXPreferred certified product by launch date

Future versions of STIXPreferred will be discussed at F2F

Topics include: TAXII2.1; STIX2.1; Untested 2.0 features

New Topic

[*Update on Mini-Group for Cyber Observables – Extended to Other Use Cases*]

https://docs.google.com/spreadsheets/d/1f61ZfWXRCLHpdFhixJqpH0fR-Q7qWgLeOW-Js3AssNQ/edit#gid=0

Please review this if you have an interest

We are trying to work through to resolve the various issues for F2F

Richard Struse

Our goal for this F2F is to resolve these issues

Trey Darley

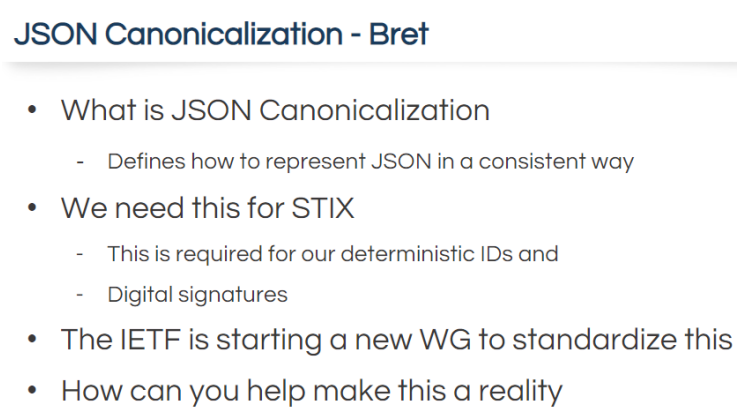
Thanks to the participants of the Mini-Group for their hard work on this.

Richard Struse

OK… moving on

Bret Jordan

Update on JSON IETF activity



New Topic

CSD 02 was approved on Dec 15th (based on WD05)

1st 30-day public review period ends this Monday

TC Last Call for comments and suggestions for WD06

Any concerns with accepting existing comments?

If no, all existing comments and suggestions will be merged early next week for WD06

Are there any additional features that need to go into TAXII 2.1?

Asked for acceptance by Unanimous Consent

[*Some discussion on why accept now*]

Richard Struse

Are there any objections to accepting this by Unanimous Consent? [None] **So moved.**

APPROVED BY UNANIMOUS CONSENT

[*Question in Chat panel about the IETF & JSON standard – Response & Discussion*]

Bret Jordan

Continuing on TAXII Status

Basic editorial changes

Ensure all endpoints that need pagination have it

Fixed typo in the name of the new spec versions filter

Added the following text to the spec versions filter

"If no spec_version parameter is provided, the server MUST return only the latest specification version that it can provide for each object matching the remainder of the request."

Changed new TAXII Envelope to mimic STIX Bundle

Changed a normative statement on the Status resource from MAY to a MUST.

Added text to allow the server to designate that it has not processed any of the objects yet.

Change the definition of Integer to be a 54-bit number [-(2**53)+1, (2**53)-1] to be compliant with RFC 7493.

Need to add some clarifying text on how to delete a version of an object

(request from Emmanuelle Vargas-Gonzalez)

Went over the schedule for TAXII 2.1

Release WD06

Friday January 25th

Open 2 Week Ballot

To approve WD06 as CSD03 and

Open 2nd public review

To run from Jan 28 to Feb 8

2nd Public Review

15 days

Address suggestions from 2nd public review

Open 2 Week Special Majority Ballot

To approve TAXII 2.1 CSD03 as TAXII 2.1 CS 01

Ship TAXII 2.1 - By end of March

Asked for Unanimous Consent action on schedule to avoid a Ballot

Allan Thomson

Asked about the value of voting on a schedule –

There may be some changes after the Cyber Observables Mini-Group concludes

Richard Struse

Let's ask it as a question – [*No objections*]

Moving on to Updates on STIX Subcommittee

Sarah Kelley

Mostly on hold pending the observed data discussion

Potential next topics:

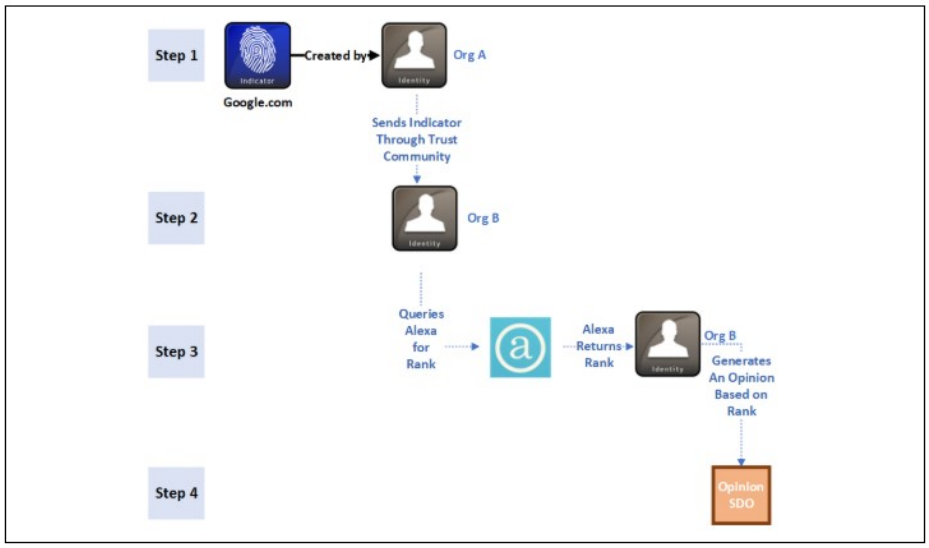
- Malware object rework
  - Which may include new Malware Analysis SDO
- Infrastructure SDO - Continue

STIX Subcommittee Updates

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

Gave update on one example = Opinion SDO

https://bit.ly/2TPxIsb



Richard Struse

Gave update on the spirit of "proving" how the code works – Not necessary to publish code -

Sarah Kelley

Is it not necessary to use the same format [as a Committee Note]

Richard Struse

We really need some Sponsors for Location –

Location needs a friend

Moved to the Community Development Corner slide –

Invited others to share in the future

An opportunity to show what you are doing and contributing to the broader community

New Topic

Let's talk about the F2F

January 29-30 2019 at Fujitsu

GCDP North Café

H Building - Fujitsu

Sunnyvale Campus

1250 E. Arques Avenue

Sunnyvale, CA 94085-5401

Go to Front Desk of H Building to be escorted to the Meeting Room

Fujitsu Sunnyvale Campus Map

Please sign-up here – Whether in-person or remotely

https://www.eventbrite.com/e/oasis-cyber-threat-intelligence-f2f-tc-meeting-january-2019-registration-53540053742

We will really focus on the Cyber Observables issues – We will engage at a deep technical level

We will also be working on the STIX Enhancement Process [*Explained why important for evolving STIX*]

We will want to formalize how a group of vendors will add custom properties and still be interoperable

Send your additional topics to us

Allan Thomson

We will also discuss the STIXpreferred topics..

Richard Struse

Any other suggestions?

We had up to 53 people on the call today – It is great to see so many people joining us

This is your TC – The way to have impact is to join us

There are opportunities to get involved

Jane Ginn

Updates on Voting Rights – please review list and let us know if not right

Also, reach out to any of the Co-Chairs if you are not yet on Slack – we can onboard you

Richard Struse

We will do this again this evening at 9:00 pm EST – Thanks everyone

Meeting Terminated

****

Appendix: List of Voting Members as of January 16, 2019*

**Please review the following list for accuracy – Contact Jane Ginn (jg@ctin.us) if you see an error.*

First Name	Last Name	Company
Kai	Li	360 Enterprise Security Group
Kyle	Maxwell	Accenture
Nicholas	Hayden	Anomali
Dean	Thompson	Australia and New Zealand Banking Group (ANZ Bank)
Jane	Ginn	CTIN
Will	Urbanski	Dell
Marlon	Taylor	DHS Office of Cybersecurity and Communications
Preston	Werntz	DHS Office of Cybersecurity and Communications
Caitlin	Huey	EclecticIQ
Christopher	O'Brien	EclecticIQ
Aukjan	van Belkum	EclecticIQ
Tom	Vaughan	EclecticIQ
Chris	Ricard	FS-ISAC
Sean	Barnum	FireEye, Inc.
Gary	Katz	FireEye, Inc.
Anuj	Kumar	FireEye, Inc.
James	Meck	FireEye, Inc.
Shyamal	Pandya	FireEye, Inc.
Paul	Patrick	FireEye, Inc.
Ryusuke	Masuoka	Fujitsu Limited
Toshitaka	Satomi	Fujitsu Limited
Koji	Yamada	Fujitsu Limited
Kunihiko	Yoshimura	Fujitsu Limited
Masato	Terada	Hitachi, Ltd.
Adrian	Bishop	Huntsman Security
Jason	Keirstead	IBM
John	Morris	IBM
Devesh	Parekh	IBM
Ron	Williams	IBM
Trey	Darley	Individual
Elysa	Jones	Individual
Terry	MacDonald	Individual
Tim	Casey	Intel Corporation
Beth	Pumo	Kaiser Permanente
Dennis	Hostetler	LookingGlass
Matt	Pladna	LookingGlass
Vlad	Serban	LookingGlass
Allan	Thomson	LookingGlass
Jonathan	Baker	Mitre Corporation
Sarah	Kelley	Mitre Corporation

Ivan	Kirillov	Mitre Corporation
Chris	Lenk	Mitre Corporation
Richard	Piazza	Mitre Corporation
Richard	Struse	Mitre Corporation
Emmanuelle	Vargas-Gonzalez	Mitre Corporation
John	Wunder	Mitre Corporation
Michael	Butt	NC4
Mark	Davidson	NC4
Daniel	Dye	NC4
Natalie	Suarez	NC4
Takahiro	Kakumaru	NEC Corporation
John-Mark	Gurney	New Context Services, Inc.
Christian	Hunt	New Context Services, Inc.
Daniel	Riedel	New Context Services, Inc.
Andrew	Storms	New Context Services, Inc.
Drew	Varner	NineFX, Inc.
Bret	Jordan	Symantec Corp.
Robert	Keith	Symantec Corp.
Curtis	Kostrosky	Symantec Corp.
Michael	Mauch	Symantec Corp.
Aubrey	Merchant	Symantec Corp.
Richard	Shok	U.S. Bank
Jeffrey	Mates	US Department of Defense (DoD)