CTI-TC F2F Meeting: Day #2

Meeting Date: **January 30, 2019**
Time: **Day #2 – 8:30 AM US PST to 4:30 PM PST**

Agenda:

Wednesday 30 January 2019

Time	Title	Moderator(s)
08:30 - 08:40 (PST)	Welcome	Richard Struse
08:40 - 10:10 (PST)	Finish Remaining Observed Data Text Proposal Review & Discussion – Malware & Grouping	Allan Thomson
10:10 - 10:40 (PST)	STIXPreferred 2.1 Requirements	Allan Thomson
11:00 - 12:00 (PST)	STIXPreferred 2.1 Details	Allan Thomson
13:00 - 14:15 (PST)	SEPs [Modified in real time]	Trey Darley
14:30 - 15:30 (PST)	SEPs [Modified in real time]	Trey Darley
15:30 - 16:30 (PST)	Wrap-up	Richard Struse

Attendees:

First Name	Last Name	Company
Participating On-Ground		
Bret	Jordan	Symantec
Drew	Varner	NineFX
Ryusuke	Masuoka	Fujitsu System Integration Laboratories
Richard	Struse	MITRE
Jane	Ginn	Cyber Threat Intelligence Network, Inc.
David	Girard	Trend Micro
Allan	Thomson	LookingGlass
Gary	Katz	FireEye
Andrew	Storms	New Context
Trey	Darley	CERT.be
John-Mark	Gurney	New Context
Toshitaka	Satomi	Fujitsu System Integration Laboratories
Sean	Barnum	FireEye
Jyoti	Verma	Cisco Systems
Daniel	Riedel	New Context
Remotely Participating		
Marlon	Taylor	DHS
Preston	Werntz	DHS

Sarah	Kelley	MITRE
Chris	Ricard	FS-ISAC
Christian	Hunt	New Context Services
Richard	Piazza	The MITRE Corporation
Emily	Ratliff	IBM
Forrest	Hare	SAIC
Russell	Matbouli	Anomali
Michael	Rosa	DHS CS&C
Matthew	Pladna	Looking Glass
Ron	Williams	IBM
Chris	Ricard	FS-ISAC
Chris	Lenk	MITRE
Patrick	Maroney	DarklLight
Emmanuelle	Vargas-Gonzalez	MITRE
Jyoti	Verma	Cisco
Matt	Pladna	LookingGlass Cyber Solutions

Meeting Notes:

Richard Struse

We made good progress yesterday – Let's keep working towards agreement

Preston Wertz

Gave the TC a warning that if there is another government shutdown, it may impact MITRE's staff

Allan Thomson

What is our plan for addressing this?

Richard Struse

[*Talked through some of the issues – Don't want to lose the forward momentum*]

Gary Katz

Let's get through today with some Action Items – then, have a back-up for the MITRE people

Later today – let's address this

Richard Struse

Good idea – Let's get agreement on Cos & SEPs, Malware and maybe Infrastructure

Fundamental point of SEPS is to empower TC members of the broader community

To add features – the point is to devolve a lot of this to the TC members to define solutions

Post 2.1 – this will be our operating model – This changes the fundamental nature of the TC

I think SEPs are the vehicle to help us to do that.

Gary Katz

If we don't get far enough along on SEPs today? [*A question to all]*

Trey Darley

I don't think there is that much heavy lifting to do to get a SEP done. [*Talked through issues.*]

Bret Jordan

My concern is the mechanics – This TC does not like breaking changes.

Allan Thomson

[*Opened discussion on the acronym to use for the updated Cyber Observables objects.*

After debate – decision to leave it as is]

Allan Thomson

[*Raised the issue of Malware Object – People needed to refresh their "mental stack" on this*

So, we moved to after lunch – then went on to discuss 'Grouping' object]

Sean Barnum

[*Gave the historical perspective on the Grouping object*]

Allan Thomson

Having browsed through – We should integrate it into the STIX 2.1 document – then Tweak it there.

Forrest Hare

[*Posted question in the Chat Panel*]

What things would be grouped together in this object aggregate item that doesn't fall under an existing concept like a "campaign"?

Or intrusion set?

Allan Thomson

[*Gave background on when to use Grouping object*]

Forrest Hare

If it is not well defined – It might be sitting there.

[*Discussion on when the Grouping object would be used*]

Gary Katz

This was raised in the context of the MISP Galaxy:

https://github.com/MISP/misp-galaxy/tree/master/clusters

Sarah Kelley

Grouping object came out of the Incident and Event discussion

Bret Jordan

Where we left off, editorially, was the need to address the final comments

There were 2 action items – We need to go back to MISP – there are other uses too.

Concern that it was becoming more like the Report object.

If 3 or more values we make an open vocabulary (-ov)

Marlon Taylor

One of the other key Use Cases for Grouping object would give Producers an ability to aggregate

Sightings objects – you would look inside text to get a sense of the number

Trey Darley

Made a motion to move into the main document

John-Mark Gurley

I second the motion

Gary Katz

Question to Bret on TAXII – Do we also need to deal with Relationships? De-referencing is an issue.

Bret Jordan

Gave a discussion on how TAXII would handle.

Made notes on the Editorial issues – wants to resolve before moving. If we could resolve most I can do that right now.

Ryu

Quick procedure question – When Grouping is going into STIX 2.1 – then we need a Sponsor

Clarification given by Richard Struse – Sponsors would have up to 6 months – if done earlier – it would not hold up publication of STIX 2.1

Bret Jordan

[*Drove discussion on resolution of comments*]

[*Asked Allan to contribute some text to the Description field to make a Certain Use Case clear*]

Sarah Kelley

When we move the Grouping object over to the Draft document

We need to identify Sponsors to develop POC code

COFFEE BREAK

Allan Thomson

Presented the STIXpreferred Options for moving forward.

Option	Notes	Impact
A) Do Nothing & Hope	- Launch STIXPreferred without vendor inclusion; no examples for download - No further updates to STIXPreferred until STIX/TAXII v2.1 completed and it appears vendors are implementing them	- Likely minimal on market or vendors - Eventually the market may adopt and recognize the value
B) Carrot: Sharing with AIS	- Discuss with DHS AIS sharing program and encourage *required* certification for any vendor pulling or pushing data connected to AIS - Depends on STIX2.1 being released	- Longer term due to AIS adoption and lead-time given to vendors to update - Will force (encourage ☺) vendors to certify products
C) Carrot: Industry Outreach	- Meet with several leading organizations that publish RFPs and get agreement to include STIXPreferred certification as requirement - Likely requires STIX2.1 being released but not mandatory	- Longer term due to RFP adoption and response cycle - Will force (encourage ☺) vendors to recognize the need to certify products
D) Ignoring Current Reality: Refresh for STIX/TAXII v2.1 Features	- Combine with Option A) path - Update STIXPreferred Tests for v2.1 features	- Ignores lack of impact STIXPreferred launch may or may not have - Focus on v2.1 based certification needs - Possibly complete waste of time if STIXPreferred never becomes relevant
E) Others?		

[*Discussion of OASIS level of support for moving forward*.]

Carol Geyer

OASIS is fully committed to supporting this launch

[*Discussion of when to step in and be more proactive*]

Allan Thomson

[*Discussion of STIXpreferred adoption – Drew analogy with WiFi Alliance*]

Richard Struse

[*Outlined plans to set-up meetings with Industry Analysts*]

Marlon Taylor

Our plan is to go forward with AIS 2.0 and that will leverage STIX 2.1

[*Noted that with Sponsorship period – Timing is baked in – Sponsorships help*]

[*Discussed release of an Interoperability Committee Note with additional tests*]

Gary Katz

There are some vendors that don't want to implement STIX – [*Gave reasons why*]

Bret Jordan

We are in good shape on TAXII 2.1 – The big problem is that we don't have the ability

To Pivot on Relationships (Query) – Terry McDonald & Jason Keirstead have

Provided a proposal – if we could get that added, it would help the community

Sarah Kelley

In line with doing a Soft Launch – Launch as is, without big giant push – to get some adoption

Carol Geyer

When I think of 'launch' it is announcing to consumers and press – Are you guys

Suggesting that we need to do that now?

Allan Thomson

My idea – Portal out – sign-up some vendors – we don't broadcast in Tweets until we

Have some vendors out

Richard Struse

Is it just for commercial products?

Allan Thomson

No. There is nothing in the text documents that point to that.

Richard Struse

With MITRE, we've created this TAXII2 Server, if we were to go… would that be a good idea

Can we prime the pump with some capability?

Allan Thomson

I think there is value in that.

Bret Jordan
My FreeTAXII server will pass all of the tests – as soon as we issue a 2.1 version, I will submit.
Allan Thomson
[*Discussed timing with STIX 2.1 launch*]
There are competitive advantages to doing it early.
Marlon Taylor
We'll go for our implementation of STIXpreferred will be against STIX 2.1.
Trey Darley
What if we had a 'Countdown' to STIX 2.1 Blog – Periodically post updates
Have a STIXpreferred 'Wait List'
Have an announcement that STIX 2.0 was an MVP – Add your name
RFPs issuers would have a place to go
Allan Thomson
Let's clean-up the website to remove the fake data – we should all talk to vendors
"Loosy goosy soft launch" Until we are ready for release of STIX 2.1 –
There is not much use to talk to Analysts.
Bret Jordan
What else in TAXII 2.1 needs to be done? No updates to Cyber Observables that need to be done
After the text we added yesterday. Does the TC need the pivoting?
Drew Varner
On TAXII 2.1 – we've got time on our side to implement it.
Allan Thomson
Other people will need to be working on it too – I think we should finishing STIX 2.1 done
Bret Jordan
TAXII 2.1 is almost done – Realistically, STIX is 9 months out. With TAXII I could have my internal
Development people working on it.
John-Mark Gurney
STIX 2.1 is at least 9 months out until we have a standard.
Richard Struse
If we made appropriate scoping decisions – Then it would not have to be that long.
Cyber Observables + Groupings, SEPs, Malware. Punt on Infrastructure.
If we have the discipline to scope it properly.
Trey Darley
And Sarah brings up the point in Chat that it would be six months
Richard Struse
A huge signal to the TC and the Community would be to get STIX 2.1 out.
Bret Jordan
I know that I've pushed for Infrastructure for a long time, I would be OK to draw the line.
If we could cut a CSD in 30 days. You could build a marketing campaign around that.
Then, tackle Infrastructure in STIX 2.2
Allan Thomson
We have morphed the discussion – since OASIS is on the call… we need to come back to
The STIXpreferred topic – Asked if anyone disagreed that? [*None*]
We are going to focus our attention on starting to adopt STIX 2.1
In our individual meetings – we mention STIXpreferred… and note STIX 2.1 soon out.
Carol Geyer
I really like the idea of a high-level Roadmap.
Allan Thomson
Our ability to commit to a Roadmap is 10%
Richard Struse

That is the past – I would like to go back to Bret's suggestion – we should scope
A Roadmap for STIX 2.1 – Lay out the processes to make it a formal standard.
I could start working on that now with Carol.

John-Mark Gurney

I think we should get all of the MITRE utilities tested on STIX 2.1 to support launch.

Sarah Kelley

We also put Course of Action in 2.1.

Bret Jordan

As one of the initial Sponsors of Course of Action I would no longer support that.

Marlon Taylor

I want to understand the consensus.
We would not go through more CSDs… we would go to CS with Rev. 2

Carol Geyer Summary in Chat:

1) Clean up portal to remove fake test results.
2) Add a statement/link to portal, 'subscribe to a mailing list to be notified about 2.1'
3) Work with Rich on high-level roadmap to 2.1, perhaps as a webinar primarily for vendors, 1-2 page doc, or a slide deck
4) See if Trey and/or others are willing to provide 'Countdown to 2.1' blog series
5) Plan on public launch, major hoopla when STIXPreferred 2.1 is ready

LUNCH BREAK

Allan Thomson

Picking up on the updated Malware Proposal with the changes to accommodate the Cyber Observables changes
[*Discussion of properties & which should be Required and which should be Optional*]
[*Discussion of comments on the Compromise Draft*]
https://docs.google.com/document/d/12I2vOdPU48VoyNMiE9HOp3AzDZJA8cOnnuomEvbjZbQ/edit#heading=h.s5l7katgbp09

John-Mark Gurney

[*Pointed out the problem of fanged vs. de-fanged data*]

Allan Thomson

[*Suggested developing a 'Test' case to demonstrate how to do it*.]

Richard Struse

Suggested developing an "Implementors Guide"… to take pressure off of the Spec
[*Comments and suggestions were recorded on the Malware Compromise Working Document*]
[*They will be merged into the STIX 2.1 CSD02 by the Editors*]

COFFEE BREAK

Allan Thomson

[Advocated finishing this for showing progress]
Moving to the Parking Lot Topics:
Comment from Marlon: How do we handle new properties?
[*Discussion on how Cyber Observables update will change path forward*]

Marlon Taylor

Concerned about how properties will be dealt with for Malware that has a hash
How do consumers know without the 'Modified' property?

Trey Darley

I believe the question is: How do you update an SCO if something changes?

John-Mark Gurney

Just to iterate the point, versioning in Derterministic IDs is impossible.
If any of the properties change, it will change the Deterministic ID

Gary Katz

That is true if you use a subset of the properties on the SCO.

Trey Darley

[*Gave an example Use Case with a typo mistake*]

[*Gave an example using all properties for generating a Deterministic ID*]

[*Noted that some of these issues are implementation specific*]

[*Suggested using derived_from plus a Timestamp*]

Forrest Hare

Talked about how important it is to make Objects very clear and complex

For generating Trust in the system – Does that make sense?

We need to reduce the proliferation of Objects.

Allan Thomson

That makes sense to me. [*Discussed the topic of Semantic Equivalence*]

Machines should be doing most of this, especially, with Deterministic IDs

John-Mark Gurney

One of the issues that comes up with using Deterministic IDs is that there may

Be multiple versions

Bret Jordan

The data is going to change… so, you need some way of identifying which version

You are pointing to. I'm guessing AIS is going to need Data Markings on Cos

We decided yesterday we are going to use UUIDv.5 – and we need a Name Space.

Sean Barnum

We need to define a Default Name Space for generating these UUIDs.

[*Gave description of a File CO and an evolution of analysis, step-by-step*]

[*Noted that as it moves towards a 'Malware' object- Properties will change]*

[*Used another example of Data Markings*]

Bret Jordan

The file object is a classic example here – [Relating one Graph to another Graph]

The amount of SROs and tools would be a mess

I'm not advocating as full TLOs… but, we may need a subset for operations

Richard Struse

The hard things are not at the extremes. Given the SCO definitions we talked about

Yesterday – What is the minimal set of things for the Deterministic ID

Bret Jordan

I think there are three:

Marking Definitions, Object Definitions Refs, Granular Markings, Spec Version

Then, how do you identify that this is a Versioned object.

Richard Struse

I'm trying to get to an agreement, so we can ship. The addition of a Version.

Allan Thomson

If they are required, I would object. For the other Use Cases for Attribution

I am going to object. If you are going to add as Optional – Go ahead

Sean Barnum

We are fine the way it is; and we are going to add as Custom.

Bret Jordan

List of properties on an SCO for generating a Deterministic ID

Created (Optional)

Modified_time (Optional)

Marking_refs (Optional)

Granular_markings (Optional)

Spec_verion (Optional)

Trey Darley

Suggested a compromise for those items that will not change

Richard Struse

It is part of an insurance policy

[*Some discussion on including Spec Version on the generation of Deterministic IDs*]

Gary Katz

Gave a summary of the use of the above 5 properties – All Optional

Marlon Taylor

Can we add Revoked as an Optional Property? [*Some discussion on why needed*]

Bret Jordan

Adding Revoked is a bad idea – [*Explained why*]

To deal with some of the file storage issues – we might modify Time as a String

John-Mark Gurney

Gave a solution for space saving and transport

Allan Thomson

Not practical for analysis in real time [*More discussion*]

Richard Struse

Summarized on the key points of consensus made through the course of the past 2 days.

Discussion and resolution on balancing concerns

Agreement on Cyber Observables & Malware and Malware Analysis

And STIXpreferred

To make this really a victory is to have that Scoping Decision on STIX 2.1

Let's put a bow on STIX 2.1 and get it out the door

If we could draw a line in the sand and finish STIX 2.1 and get it out the door

Then, from operational experience, we can refine moving forward

If we don't do that; all of the work we've done, will go 'poof'!

Do we snatch Victory from the jaws of Victory – we can drive to

A definition of 2.1 and get it out the door – the TC will be amazed!

We have been getting a fair number of new members – it would send a great

Message to the rest of the TC then, we get it out the door

Let's drive to a definition of STIX 2.1 that is focused – let's get it done

Bret Jordan

What is going in the STIX 2.1? [Discussion on what is in and out]

1. The Cyber Observables Compromise
2. Malware and Malware Analysis
3. Grouping
4. Location (Darklight and maybe LG? sponsors with DHS)
5. Infrastructure [Needs to be finished]

Richard Struse

What else do we need to do before the next monthly meeting to get this done

If you have an issue – reach out to myself and Trey – we'll get it back on course

When we get it out the door, then vendors will ask about Roadmap

We are well on the way on a CS – when we stop iterating on CSDs on STIX 2.1

That sends a clear message to the community to move to development

Bret Jordan

Parting comment on TAXII – Think about what you else you may need – I have a proposal

For the next working call – for next 15 minutes.

Trey Darley

I cannot do the A/V for the next F2F – Can we reach out the broader TC to find someone

Richard Struse

We will be reaching out to find someone to help Jane as Co-Secretary – It is a lot of work

She needs help. ……..Thanks all for a productive F2F!