CTI-TC Working Session

Meeting Date:	**January 22, 2019**
Time:	**3:00 p.m. EST**
Purpose:	**Weekly Working Session**

Attendees:

Allan Thomson
David Girard
Drew Varner
Emily Ratliff
Richard Struse
Bret Jordan
Emmanuelle Vargas-Gonzalez
John-Mark Gurney
Nicholas Hayden
Jeff Mates
Jane Ginn – Recorder
Russell Matbouli
Sarah Kelley
Trey Darley

Agenda:

- **Resolve Last Four Issues – After Public Review**
- **Cyber Observables – How handle moving forward**

Meeting Notes:

Bret Jordan
I wanted to try to resolve the last four items after the Public Review
[*Discussed Integer Definition Text – to resolve final comment*]
Allan Thomson
I was thinking of what I'd do if writing code
John-Mark Gurney
[*Explained the compatibility issue*]
Allan Thomson
I knew we were making this change to be compatible with the RFC – so I compared to
The rest of the text – the only place we use is on 'counts'
If you could check that it is consistent – I'm fine if you resolve this comment
Bret Jordan
Next topic – Match property – [*Gave marking definition as example*] –
Modified Timestamp vs. Created Timestamp
Allan Thomson
I was reviewing this for the Cyber Observables Mini-Group
I wrote an update [*went over new suggested text*] Use 'Date Added'
John-Mark
I would still prefer if we have Created & Modified rather than Date Added
I think it should be general and not specific for Marking Definition
Emmanuelle
I would be happy with Allan's suggestion and, I agree with John-Mark
That we should be more agnostic
Allan Thomson
If we could craft some text in accordance with what John-Mark suggests

Bret Jordan

OK, I'll work with Emmanuelle on this and get some text into the draft

Next Topic

Asked about where highlighted text is really need (see below).

We are not sure it is needed.

version (required)	`string`	The version of this object. For objects in STIX format, the STIX **modified** property is the version. The value of this property **MUST** never be later than the date that the object was added.

John-Mark

I am concerned about the time synchronization issue

Allan Thomson

[*Gave an example of how TAXII servers might be generating at different times*]

John-Mark Gurney

I am now confused about that this text means

[*Some discussion on this property*]

I'm pretty sure the TAXII server Timestamp should continue

[Consensus was that it would be OK to remove that sentence.]

Bret Jordan

[*Emmanuelle made a suggestion on deleting an object – default parameter*]

Emmanuelle

Bret and I talked and now I see that my suggestion is not needed – Remove comment

Bret Jordan

[*Some discussion on 'pending_count' as a property*]

Sarah Kelley

That would be a breaking change to change it to 'processing'

[*Consensus to keep it as is*]

Bret Jordan

Jason had an issue – Github Issue 32 – Clarify response the POST was processed

Synchronously –

[*Discussed how status endpoint is processed and status messages*]

Allan Thomson

[*Gave an example where it would be programmed incorrectly*]

We should have a different message

Drew Varner

That would require that we keep a log for 48 hours.

Allan Thomson

What do you want the Client to do? [*Discussed how it should do from the client side*]

John-Mark Gurney

The additional text is correct, as described. With a different error message, it would make

It clearer if the Client is misbehaving

Bret Jordan

[*Gave some suggested text*]

Allan Thomson

Defensive programming is always a good thing – It would be better if we also describe

What we want the Client to do

Bret Jordan

Allan – can you help me come up with some text to try to address this?

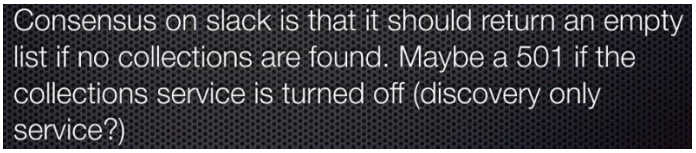
Allan Thomson

Sure

Bret Jordan

My last issue – Github issue 83

Gave a Use Case on Collections – From EcelecticIQ



John-Mark Gurney

A 400 is a Client error – and a 500 is a Server error

Bret Jordan

[*Described the Discovery service from API Root*]

OK, I will add some text about the Empty List – to make sure that is clear

Hearing no more Comments – I think we are done

I did get some comments after the Public Comment period was closed

It had to do with how the Conformance language was structured

I'll address with Drew – Put in Working Draft 6 and get that out –

We'll do a motion for a CSD03 and a 2nd Public Review

Allan Thomson

The Mini-Group has been working on a number of issues – John-Mark can cover one

I'll point out some of the changes on the Malware Definition

[*Showed screen and working version*]

Key Point is that from the Malware object, you can point to specific Cyber Observables

The Malware Analysis Object is also new – No change from previous one

Then, there was Section 7 of Part 1

There were a lot of Vocabulary definitions –

Section 7.8 Malware Analysis Environment

These were the changes from the Mini-Group on the Malware object

We'll go over these in more detail at the F2F

The other thing I wanted to point out – What properties contribute to

A **Deterministic ID** for a Cyber Observable – Showed updates to the 2.1 text

These are Optional – Need to have the same hash

We also went through all of the Extensions – and I updated text

Trey Darley

Can you go back to the hashes? [*Suggested that we stipulate a preferred one?*]

Allan Thomson

That is why we have the ordered list.

John-Mark Gurney

The text is a little confusing.

Allan Thomson

Please go into the text and help us make the text more clear

I'd like to get some of this figured out before we get to the F2F

[*Went over the Status Matrix*]

A	B	C	D	E
Task	**Details**	**Who**	**By**	**Status**
SCO - Id Hash Algorithm Writeup	Writeup Hash Algorithm Proposal Based on Digital Signature Proposal in Section 3	Bret	1st Draft 1/11/19	Sent
Fact Property Changes	Define for each SCO the set of properties that contribute to the hash for each object	Allan	1st Draft 1/11/19	Sent
Relationship Changes for SCO changes	Verify and update as necessary sections related to how SDO and SCO are connected	Bret	1/18/19	
SCO Id Property Review and Comment Changes	Verify and review/update with changes	Sean (but all should do thisA)	1/18/19	
SCO Common Changes	Verify and update any other changes to introducing SCO term and definition	Allan	1/18/19	Reviewed parts 1 - 4 and updated slightly
Fact-list changes	Verify and update use of fact-list SDO (containing SCO)	tbd	tbd	
TAXII changes	Update text on how taxii needs to be updated (preferrably not)	Bret/Allan	1/18/19	
Explanation & Examples Documentation	Add section to spec somewhere on background, examples and how-to	tbd	tbd	
Update malware spec to highlight use of SCO	Verify and update malware SDO spec section to highlight SCO use	Allan	1/22/19	
Add malware analysis spec update	Add malware analysis section to SDO spec	Allan	1/22/19	
Add explicitly named SDO to SCO relationships that we feel are important	Nice to have if we have cycles	tbd		Done for malware
Hash algorithm proposals		John-Mark	1/22/19	

John-Mark is going to develop a draft slide to show the Pros & Cons of the hash algorithm

[*Went through the draft text to show how Objects are added with type ID*]

Sarah Kelley

I just want to thank you for all of your hard work on this

Trey Darley

I second that

Richard Struse

I want to put in a plug for the F2F – We encourage remote participation

Meeting Terminated

****