CTI-TC Working Session

Meeting Date:	**November 27, 2018**
Time:	**3:00 p.m. EST**
Purpose:	**Weekly Working Session**

Attendees:

Chris Ricard
Chris Lenk
Trey Darley
Sean Barnum
Rich Piazza
Emmanuelle Vargas-Gonzalez
Taneika Hill
Jeffrey Mates
John Wunder
Allan Thomson
Nicholas Hayden
Drew Varner
Bret Jordan
Sarah Kelley
Dr. Masato Terada
Jane Ginn - Recorder
John-Mark Gurney
Gary Katz
Jackie Eun Park

Agenda:

- **TAXII 2x Updates**
  - Working Draft 04 Review
  - Query proposals
  - Client User-Agent
- **Cyber Observables Mini-Group Updates**

Meeting Notes:

Bret Jordan

WD04 Update

• The review period ends this Friday, end-of-day
• What is new in this draft
  • The TAXII Envelope all media types are now TAXII
  • Add “limit” and “spec_versions” filter parameters
  • Added clarifying text around date added timestamp needing to be millisecond precision
  • Cleanup on descriptions of error messages

TAXII Query Problem Statement

• There is no current way to find the relationships that point at a STIX Object.
• The only thing you can do is pull every relationship down and then try and filter then on the client.
• We need a way to pivot
  • I have an indicator or campaign, tell me if anything is linked against it
• There are two proposal ideas for doing this

Proposal #1

• Create a simple endpoint like: {api-root}/collections/{id}/relationships/related/{stix-id}/
• This would result in a very simple database query and URL filtering logic. Something like:
  Pseudo SQL code: **select** * **from** table-objects **where** type=relationship && (source_ref = stixid || target_ref = stixid)

We should define a URL parameter called ?deref=true

• This would tell the server to not only send the relationship object,
but also the object that it points to
• This could also be used for simple queries where you want to ask the server to automatically send the created_by_ref identity as well
• Or automatically send you all of the objects from a Report

Proposal #2 (Not Mutually Exclusive)

Create one or more search endpoints like

{api-root}/collections/{id}/search/
{api-root}/search/

• These endpoints would accept some sort of "query or information-request object"

Summary

• We talked about this on the list and there seems to be 6 people that like or prefer a simple solution that we could deploy quickly.
• 1 TC member is against proposal 1 as it does not provide all of the features and solve all of the use-cases needed for query
• We could easily do both, the simple solution now TAXII 2.1, and the more complex one in TAXII 2.2.

Chris Ricard

Let's keep it as consistent with previous versions as possible

Jeffrey Mates

I like the proposal – Proposal 1

Gary Katz

I think this is a good start – the Use Cases in the future will need to be developed

Sean Barnum

Proposal 2 has been on the table for a while – I concur with Gary that Proposal 1 would not
Paint us into a corner

Drew Varner

In terms of API, we have a 'objects' endpoint –
it seems odd to have a 'relationships' endpoint

Bret Jordan

I was trying to get something on paper, we could work on this – get out an WD05

Drew Varner

Would relationships return 'relationships'

Bret Jordan

I was trying to find a way to add a pivot functionality, in a RESTful way… and
Can get out quickly

Trey Darley

I am sympathetic to the Jason & Terry proposal – I still want to Crawl, Walk, Run
And having the simple Pivot in the short term would be good.

Allan Thomson

[*Tried to get clarification on the Use Cases each proposal would represent*]

Bret Jordan

[*Gave examples for clarification*]

Allan Thomson

I am still somewhat skeptical of this proposal – We are going to spend time adding
To the Spec… and Interop
What is driving this? I get the concept and look-ups…

Trey Darley

[*Gave example of the basic need for pivoting from his [analyst] days and other*]

It was a disincentive to implementing TAXII

Allan Thomson

They are treating TAXII as the repository of information, rather than a database

Designed for some of this stuff – you raised an example

It is a product that uses TAXII

Any products should use a database designed to do this

Trey Darley

[*Made argument that an interoperable ecosystem should pivot with query*]

Allan Thomson

If the majority think there is value is this… and they are willing to do the work

Then, I stand aside – If everyone is willing to do the work

My opinion is that it is not a well-defined Use Case

Sean Barnum

Speaking as a Threat Intel provider – this is one of the most fundamental thing – Query

[*Gave example of 'Push' model, Gave example of 'Pull-Query' model, & Gave example of 'Interactive-Pivot'*]

That is an hourly, if not minute-by-minute request from our customers

Talked about the way it is now – This is a very real-world very high priority

Gary Katz

Yes, sometimes you have a small enough volume – but, if you are a provider that

Has terabytes of data – you are not going to tell them to go pull everything.

Gave example of PassiveTotal and VirusTotal – They have APIs

Sarah Kelley

We are enforcing the concept of 'Done' on STIX2…. Should we be implementing

The same thing for TAXII2?

Bret Jordan

Is there anyone other than Allan that is against doing this?

Trey Darley

I remain supportive and I hear Sarah's concerns – and so I think we may want to POC

Bret Jordan

I do actually have one implementation on this

**********New Topic*********

Bret Jordan

[*Outlined the topic brought up by Marlon on User-Agent*]

- A TC member has asked that we add support for a TAXII Client user-agent element.
- This would more easily allow servers to diagnose problems from clients talking to the server.
- Should we add support for this?
  - If so, should this be an optional or mandatory feature?

Jeffrey Mates

Made point of how change from where we are now

John-Mark Gurney

Made point about use of automation for User Agent

John Wunder

Would it be 'Required'?

Bret Jordan

Should be a 'Should' – and would be based on HTTP

John-Mark Gurney

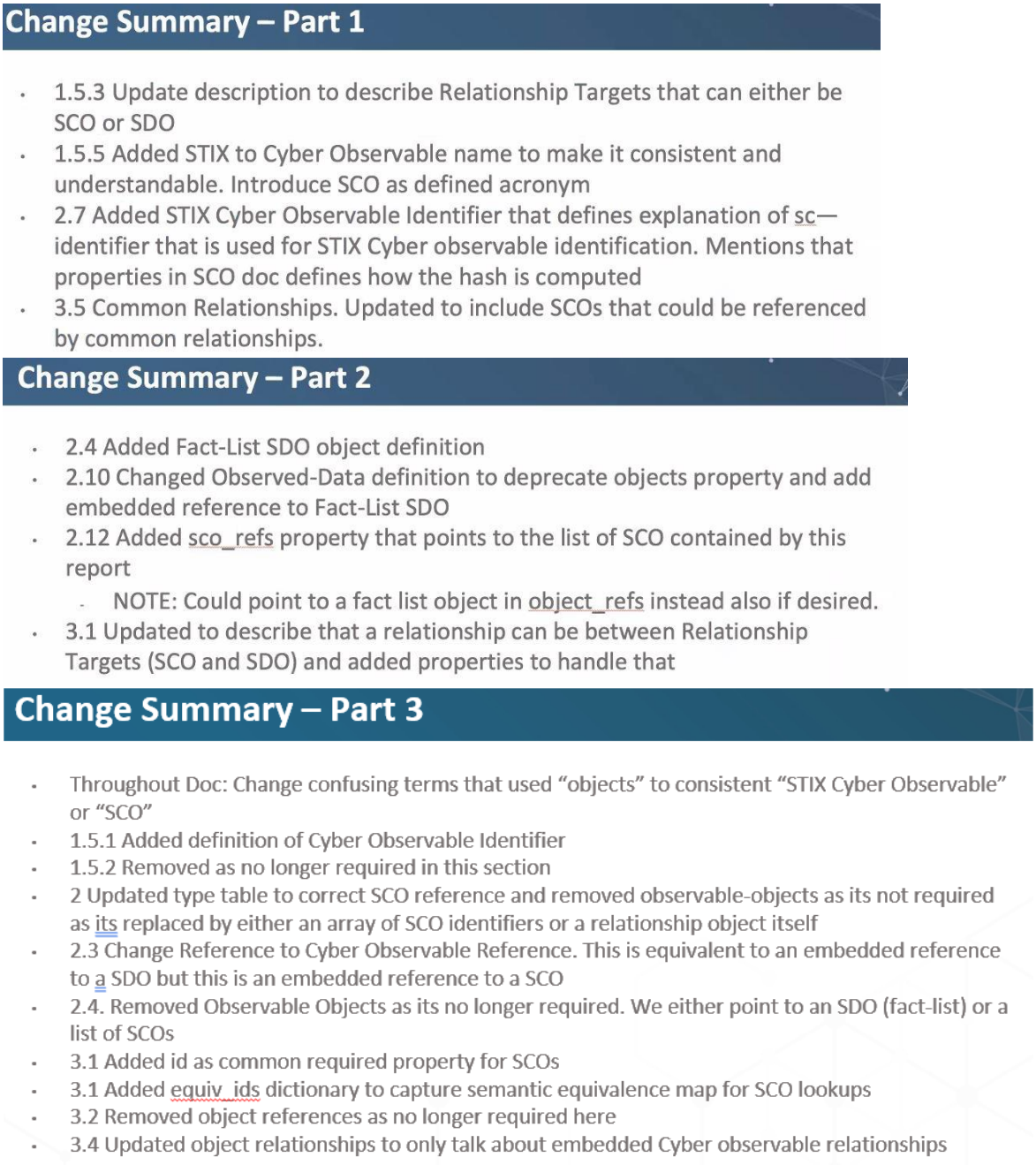
I would agree that it should be a 'Should' – A lot of HTTP Clients already are using this

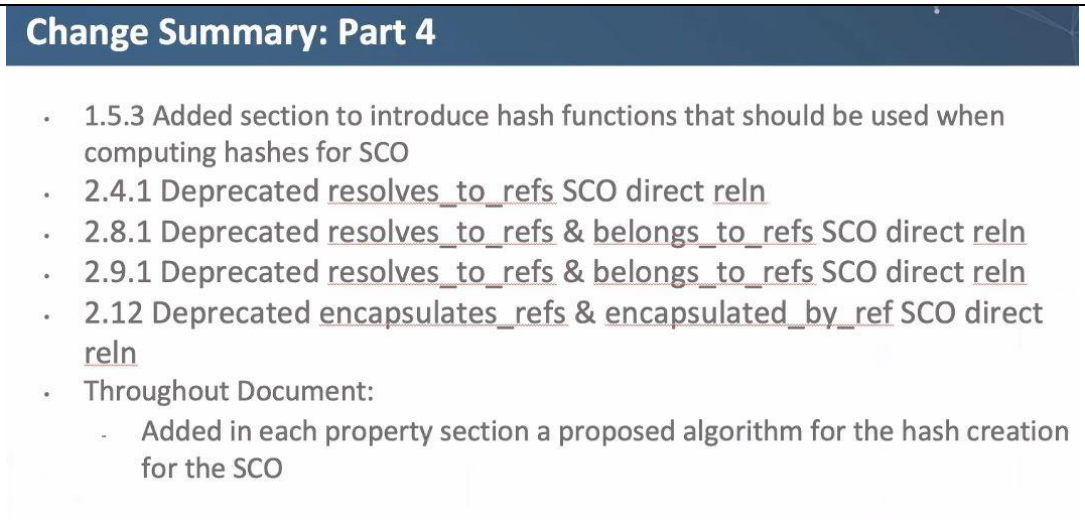
John Wunder

I should take a look at the ATT&CK logs to see if it does it – and others

Allan Thomson

[*Gave update on Observed Data Proposal*]





John-Mark Gurney

I'd like to participate in this Mini-Group

Allan Thomson

We'll make sure you get invited to the next meeting

Gary Katz

I have a presentation on this – we don't have time – I do have a point on how ID set

Allan Thomson

I agree – I thought that from the beginning

The MiniGroup has made progress – It takes everyone to come to the table

With a willingness to compromise

Trey Darley

Come with ideas… and come with the spirit of compromise

Chat Panel:

From chris ricard to Everyone: 01:24 PM

Allan - I get a sighting on an indicator, and I want to know more about it.

From Allan Thomson to Everyone: 01:24 PM

i would like to respond to trey

From sean.barnum to Everyone: 01:25 PM

This sort of pivoting is one of the most fundamental and common needs for TAXII access to threat intel providers

From Allan Thomson to Everyone: 01:26 PM

most systems today pull information in complete sets based on periodic polling and do pivoting once sync-d.

From John Wunder to Everyone: 01:33 PM

I'm not against doing it but I agree w/ Sarah that it should follow the same vetting process

From Allan Thomson to Everyone: 01:34 PM

if the vetting occurred then it would show the value of the feature and help justify.

From Emmanuelle Vargas-Gonzalez to Everyone: 01:38 PM

The OASIS TAXII client does use the User-Agent

From jordan to Everyone: 01:47 PM

I am scared silly of doing anything in TAXII that cannot be verified to work first.

Meeting Terminated

****