CTI-TC Working Session

Meeting Date:	**December 11, 2018**
Time:	**3:00 p.m. EST**
Purpose:	**Weekly Working Session**

Attendees:

Allan Thomson – Moderator	Bret Jordan	Jason Keirstead
Trey Darley	Sean Barnum	Chris Ricard
Sarah Kelley	Nicholas Hayden	Vivek Jain
Gary Katz	Tom Vaughn	Jackie Eun Park
John-Mark Gurney	Taneika Hill	Jane Ginn – Recorder
Richard Struse	Emmanuelle Vargas-Gonzalez	

Agenda:

- **Cyber Observables – How handle moving forward**

Meeting Notes:

Allan Thomson

Introduced the work of the Mini-Group on the Cyber Observables issue

Richard Struse

We need to reach resolution on this issue – time is important – We'll discuss in full TC

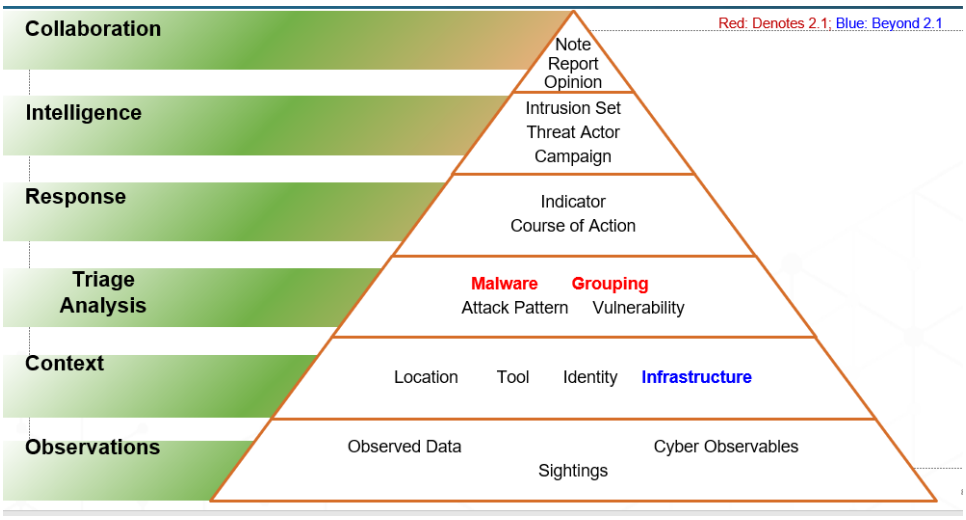
Allan Thomson

Noted that this is being discussed relative to specific Use Cases – Using Malware SDO

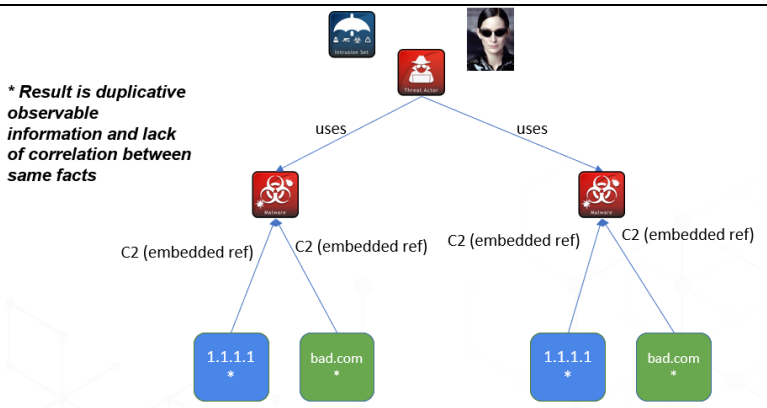
It will also affect Infrastructure SDO – But, that is not currently in STIX 2.1

If you think we need this extra Use Case, please comment on the Slide

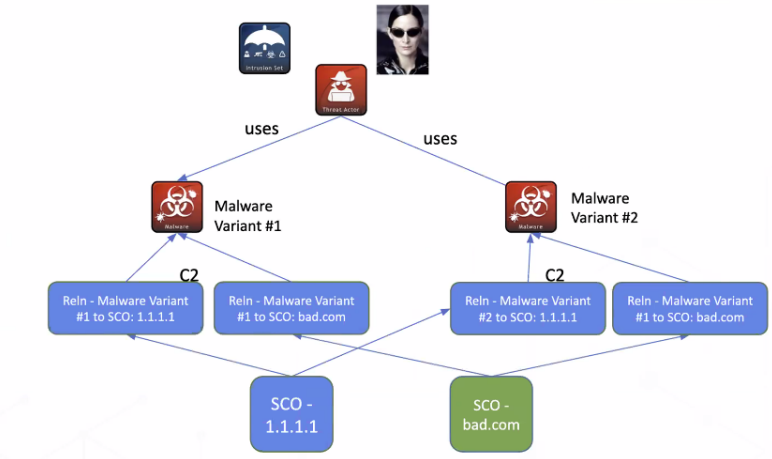
Gary put this slide in:



As it is now (Malware Example):



With the proposed solution (Malware Example):



Proposed Solution: Part 1 - Standard SCO IDs

- Introduce ID property for SCO (STIX Cyber Observable)
- Will define a subset of cyber observable properties per cyber observable that make up the ID for that cyber observable
- Will update relationships to allow references between SDO/SRO/SCO
- Introduce ID-creation-mapping property
  - Absence of property and default will be standard defined in spec
- Will define standard mapping for ID creation property
- Compliance:
  - Will add statement on orgs **SHOULD** use the defined approach for SCO ID creation
  - STIXPreferred Interoperability will be updated to include testing for specific persona

Proposed Solution: Part 2 - Org Customizable SCO IDs

- Producers MAY define their own ***separate*** method for creating an ID on a per-object basis
  - **Used instead of standard ID creation method**
- Producers **MUST** publish those ID creation definitions in a CTI OASIS defined schema if non-standard approach
- Producers and Consumers MAY BE ABLE generate an org-specific IDs
- Secondary Org MAY reference Original Producer's objects provided ID

Allan asked for comments

Chris Ricard

I think it may break some more things than it solves. I wrote up my rationale, but it didn't go out.
I'll send it to you, Allan – Can you send out?

Sarah Kelley

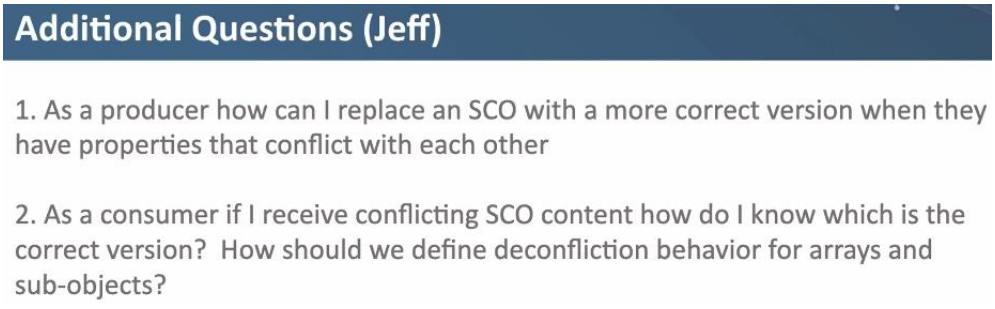
I see that this proposal combines some of the features of the two proposals. It is a nice compromise

Bret Jordan

I agree with Sarah – It will require that we write more code, but it is a compromise that appears
To solve the problem of the Use Cases we are looking at

Allan Thomson

We need to present this to the full TC, then go to a Ballot
For the Minutes – We had almost Unanimity that this approach might work – with one exception
Also, Jeffrey had raised some issues on the Slack channel
Does anyone object to going through these issues?



[*Articulated Jeff's concerns – offered an approach to resolve the solution*]

Sean Barnum

[*Gave an example of how SDOs and COs evolve through time – And how could be shared through time*.]
We feel very strongly about approach to versioning…. We want to keep all of the old data
[*Talked about the Modified version*]

John-Mark Gurney

[*Talked about core properties issue*] [*Talked about some other issues that might arise with this approach*]

Jeffrey Mates

I'll point out – One issue with a certain Timestamp – it assumes a centralized system from each Producer
[*Then gave example of sensor-generated IDs – and modifying*]
I worry about this if we are saying "latest always wins" or "more detailed version always wins"

Gary Katz

If you want to hash everything – it would be possible by this approach –
I want to go to John-Mark's point
[*Gave some examples of how issue could be handled*]
This approach is designed to address that problem

John-Mark Gurney

It was really related to versioning – if you update, you can lose your data

Gary Katz

We really need to do a good write-up on how to do versioning

Sean Barnum

[*Talked about how the various implementations will differ – Discussed what STIX needs to do*]

Allan Thomson

[*Gave some observations about how different products will respond to the data with these changes.*]
The context of consuming this data is dependent on the consumer

John-Mark Gurney

We could make it complicated and add rules – but, I agree, that we don't want to do that
One possibility is a SIM link
The other point- there is an implicit assumption that the ID is part of the Object

Chris Ricard
I want to make sure that what-ever we come up with will work with TAXII versioning
Jeffrey Mates
We do call this out with TLOs currently…. [*Explained how currently handled*]
In this case – there may be some overlapping because of these rules
John-Mark Gurney
Previously ID was globally unique – Now, we will have some overlapping
Jeffrey Mates
I agree about the globally unique issue
John-Mark Gurney
This is also tied to how TAXII deals with over-writes
Sean Barnum
I'm never assuming that our solution is right – But, we know that it does work – Others may do it too.
This is possible to solve
Allan Thomson
Some things are not solved with STIX alone
We have 3 minutes left – I want to put a wrap-up on the call
We'll use this slide deck on the full TC call later this week
If you have additional concerns – please send your concerns to the Mini-Group
We'll continue to work on this – if you want to get involved – please join the Slack Channel
Trey Darley
We are coming up to the Holiday season – we should probably do a Doodle Poll – Schedule calls
Notional deadline of January 31.
I'll propose that we find some serious time to work through issues and write text – we will need
Everyone to get together – we'll need to incorporate the Digital Signature updates.
That work will start in January – if we don't do the work, we'll revert to earlier version.

Meeting Terminated
****