CTI-TC Weekly Working Call

Meeting Date: August 29, 2017
Time: 3:00 pm EDT
Purpose: Weekly CTI TC / STIX SC

Attendees:
Ivan Kirillov        Bret Jordan        John Wunder – Moderator
Sarah Kelley        Trey Darley        Andras Iklody
Allan Thomson       Nicholas Hayden    K. Schneider
Mark Davidson       Christian Hunt    Richard Struse
John-Mark Gurney    Bill Chu          Jane Ginn - Recorder
Paul Patrick        Sean Barnum

Agenda:
• Report SDO – incorporate MISP comments
• Investigation/Event SDO
  o LookingGlass Proposal
  o FireEye Proposal
• MISP Approach – Report vs. Collection SDO

Meeting Notes:
John Wunder
  Opened discussion with a comparison of the Incident/Event with proposals
  Asked from input from MISP
Andras
  We could use the Report SDO, as long as it is not finished
Allan
  The concept of having a Report that is not finished – My concern is that it is not a binary flag
Andras
  We have something different for that – We only use binary if we want to automate
Bret
  Can we handle that with ‘labels’? Would that work for you?
Andras
  Not necessarily – Labels have to be known by the partner you are sharing with.
  The advantage of a boolean, is it could be in the standard
Allan
  It is not enforceable
Andras
  That could be true with other fields as well
Allan
  Just to be clear, the STIX standard is about the exchange format… there is a separate
  Test document for that
John
  Explained the semantic meaning – We can make it an -ov, then give a state of the report
  Then people could use work flows
Sean
  If you have a use case where things are related some way – Where is the decision made
  About when to create a separate object – How Report gets used, or other objects –
  It goes back to the semantic issue – Right now, Report is like is was in the past
  Now, if a Report is going out – It could have labels – Then when a Collection
Trey
  Let’s use raised hands to cue
So that makes sense what Sean says.

I think we are coming to consensus here

Just as a naming thing, the Intel community uses ‘Collection’ as a term of art

It is confusing to other communities, too. I don’t think we should have two separate objects

If we do end up going with two objects – We’ll need some volunteers

I don’t care if we have 1 or 2 – But the naming thing will be a challenge

If we are clear about the specifications – it is incumbent on us to help

Users to know what to put what where

Ran a Straw Poll to gauge the preferences of the attendees about 1 or 2 separate objects

If an object has a publication date – people will think about it as being published

We also need to be careful about marking definitions

I think using an -ov is OK… we need to be careful about the Labels

I am against renaming it… Keep it called ‘Report’… use Labels

And make ‘publish date’ optional

As long as it is clearly described – That will work for us

Yes, we have to be clear about the Object and the Labels

Is it possible for us to go to a consensus vote on what to do?

What changes to we need to make to the Report object to accommodate the MISP use case

I would like to put some thought into what goes into the -ov

I was wondering if there was a general consensus

I applaud and agree that making a decision is good… but, unless we have something to review

Good question – We can work through the details

Switching gears – Let’s talk about this Investigation or Event SDO

I can share my screen – I took the version that was in Google Docs

My intention was to update the SDO so that our company could use it for an Event

I will try to describe it here… [Walked through his mark-up]

I’m trying to wrap my head around the Blacklist, versus the Indicator

I was going to make the same comment – I think ‘E’ overlaps with Infrastructure

If Infrastructure becomes a First-Class Citizen – We’ll have to revisit

[Explained how indicators could be rolled into a CIDR range] If that is too confusing,

We can use Indicator SDO

I don’t think there is a problem with using Observed Data here vs. Indicator

[ gave example of seeing internal IPs]

On to my other comment – I generally agree with what Allan has outlined here – I do

Have a concern about the timing of the COA – this proposal does not address it

I agree – it does not fully address that – It is not a full description – error states, other changes
If that is something that we do want to address by the community, we can do that.

John Wunder
First on the Indicator overlap – it is not inherently a problem – not a perfect use case for OD. That is more semantically an Indicator [If it is something that other people should look for]
On second item – We should think of a descriptive way to document COA

John-Mark
I think it should be a COA rather than an Indicator – I am leaning more for Indicator

Sean
I have numerous concerns – Let’s stay with the high-level ones
On the first definition – it sounds like a Bundle to me
[Asked a number of questions about how to interpret it]
This is a very broad topic, with lots of wiggle room
Also, it has a lot more detail than what we may want to tackle now
I don’t think we, as a community, know what to do with it
We don’t know where the stake would go

Allan
What would you change?

Sean
I would go back to what we proposed [Gave examples]

Allan
It would be a good thing to come to agreement

Sean
[Explained how he is interpreting the mark-up]
[Debate between Sean and Allan about the mark-up versus the FireEye proposal]

Allan
I think we are closer to each other than it may seem – Automated data vs. manual data
We can do a lot of refinement with MRTI
The question is: when does an Event become an Investigation?

Sean
Look at my Proposal – Triggers and Triage

Trey
The conversation has devolved to a conversation between two people –
One of the major topics is Timeline for delivery for 2.1 – Minimum amount for various SDOs
So, people in the 80/20 can get it done

Allan
The original description in Google doc – didn’t work for me either – Merge edits or no edits?

John
It seems to me that we’ve been iterating on this for a while – What FireEye proposed is close
Let’s tighten it down – And take what we can to the others

Bret
Let’s figure out where to go – Our marching orders – What is the scope?
We need to figure out where we agree and where we disagree – so we don’t talk in circles

Allan
That’s why I wanted to review it and mark-up the Google doc

Trey
Trying to reconcile that with three distinct documents – I suggest an editorial-type call
To reconcile

John
We need to iterate on this – Let’s do a Straw Poll
[Went through some of the comments]

Sean
We are trying to tackle things that we don’t really understand – like COA
If this is going to be used as an Investigation, not Event – we need to be clear on that.

John
We’ll pick this up in a Mini-Group later

Meeting Terminated
*******************************************************************************