CTI-TC Weekly Working Call

Meeting Date:	**July 18, 2017**
Time:	**3:00 pm EDT**
Purpose:	**Weekly CTI TC STIX SC**

Attendees:

Trey Darley
Bret Jordan
Thomas Schreck
Nathan Reller
Paul Patrick
Allan Thomson
Christian Hunt
Ivan Kirillov
John Wunder
John-Mark Gurney
Mark Davidson
Rich Piazza
Sarah Kelley
Chris Ricard
Richard Struse
Crystal Hayes
Jane Ginn - Recorder

Agenda:

- Precision Field – Location SDO
- Event SDO – Relationship to Incident SDO

Meeting Notes

John

We need to keep it down to 10 minutes

John added a precision field (optional) defaults to 10 km in the Location SDO

If you don't add LAT/LONG it defaults to 10 km

Bret

I'd rather not use it at all – vendors use MaxMind

Rich

Really, all?

John

MaxMind is IP based and this would add LAT/LONG for non-IP based location

John-Mark

[*Explained why he recommended it*]

Recommend that we use it – we need beyond MaxMind

Would help pointing to another [*Described why important*]

Bret

If feels like this is the same discussion we've had on Timestamps

John-Mark

We made decision for precision on Timestamps

Trey

Conversation has been limited to Slack – there are some 3-letter agencies that need it

Allan

I think we should have it as Optional with no Default

Rich

We need to make it clear -There are a lot of Consumers that need it

Allan

We can have it for the 3-letter agencies

Trey

We need to think also about Consumers

The argument that John-Mark made – 'X' over someone's house… not the city

Nathan

Asked question about a location like 'United States'

John-Mark

I have some text for that – suggested putting in bodies of water

U.S. has a specific approach

Bret

It seems like we are trying to use LAT/LONG as a replacement for region or city

And so, by specifying some level of precision on LAT/LONG

If not, use the city/state/region

John-Mark

If you do not know the precision of the LAT/LONG – you shouldn't share

Allan

We need to work to higher quality data – this standard is not going to fix that problem
The market will decide

John

I didn't want to spend the entire call talking about this… I'd like to take it to the list
To see if we can get a consensus and if not, go to a Ballot

Trey

Recapped…. We need to decide if we address in 2.1
Objections? Hearing none…. Let's move into the Event SDO

John

There are two topics: 1) How we describe Event (labels, vocabulary)
On Labels:
[*Showed screen with the options*]
Asked about the event type field

Rich

Pointed out how used
Investigation seems like a temporal state. There are a lot of organizations that care about
The word 'Incident' so they need a different stack for tracking things
Investigation… overlap with event status
Labels, status and type need to be considered as a whole

John-Mark

I'm find with using labels – we are using it other places

Bret

Investigation does not belong in Event type – I'm mixed on status… Boolean value
What we are trying to do is get rid of everything and a Boolean on if it turns into an Incident

Allan

One of the things we see is that multiple events are turned into a 'case'
Do we have a way in Malware where you have multiple that are grouped?
Is there a similar case where we have that construct?

Trey

[*Mentioned Intrusion Set as an example construct*]

Allan

[*Further described how multiple events are investigated and how closed out*]
When you close out the case – you close out all of them

Chris

It seems like the Event type is more like a Boolean – The thinking in the industry
If you call something an Incident – you have to report it to an Agency
I see what Allan was saying – but are we trying to make this into a Case Management System

Allan

It is a reality of intel processing… individual analysts work on events… or cases
We are creating the data structures for what people commonly do with this data

Chris

Is this something that could be handled by Relationships?

Allan

It could be, but it seems to be a verbose way

Bret

I agree with you. Use Boolean… now this Event is being promoted to an Incident state

Rich

What we are successfully doing with this design… we make objects late binding
Allan's Use Case could be addressed by having a label that is a Case
If we use Labels… we are going to be boxing people in less
The less we use an approach where we are

Allan

If you want to be about to handle as a first-class object (update versioning) beyond labels

John-Mark

We already have done this with Relationship objects. Using labels with SROs… would be easier

Bret

I agree with you Allan… IR tools have been in use for a long time. Well established
You have events that are bubbled up to Incident

John

Do you mean to have a TLO as ‘Case’?

Sarah

Not to pay devil’s advocate, but can’t you do that with the event-type-ov the way it is?
event, investigation, incident? And then all you’d need was relationships from event to event

Rich

When does something go from an Event to Investigation to Case to Incident

Sarah

Explained that it is a list – Three separate things. One or the other

Paul [*on chat*]

I agree with what Sarah just stated. In our IR engagements, we tend to talk about events, investigations, and incidents.

John

I wonder how concrete these terms are?

Allan

Who are you asking?

John

To Rich’s point, if we don’t do what is in common use then it won’t be used

Thomas

We are measuring when detected, finish investigation, then establish incident

Trey

Can I ask a Devil’s advocate question?

Bret

When I did IR – Tools were completely separated from NOC and SOC
In threat intelligence, you want to have it tied back into what we are doing in STIX
We want to be able to capture enough of that data and put it in blobs so people can
So how it goes together… then tools can be built to show the data

Chris

I went back and looked at the Malware SDO – Boolean “is_family”
Suggested an “is_incident”.. if matches the organization’s definition

Thomas

I want to go back to Incident handling – We want to bring up to our database
[*Described how he has been handling*]

Rich

I encourage a late-binding view

John

Described how to achieve the late-binding approach with a vocab
As we look at this Incident, does it work?

Bret

That would work… the main thing is that we maintain fidelity

Allan

[*Walked us through his scenario – how it would work*]
There would be 3 or 4 created. There would potentially be thousands a day
If you are going to use Relationships to link these together
Original event, investigation (or case) and the SRO
Is that the most effective way to represent – if just a single

John

Are you suggesting an embedded relationship?

Sarah

Outlined the problem if it was revised

Allan

Yes, but….[*described how it could work*]

Bret

What would you do if you have to revise it

Allan

We need to think about the implications of using this because of the volume of data

John

I think we need to look into the way embedded would work… model it out

Nathan

I'm wondering about how to group Event A and Event B

John

The way we have done it in the past is a list of properties

[*Described how it would work*]

We have some design rules for when we use external references.

Bret

I need to think about the implications

John

We made some progress on the two topics for today.

People should think about these

We can iterate on this before next week – talk about next week

Bret

OK, great progress

John

Thanks everybody

Meeting Terminated

****