CTI-TC Weekly Working Sessions

Meeting Date:	**May 24, 2016**
Time:	**12:00:00 UTC**
Purpose:	**Weekly CTI-TC Joint Working Session**

Attendees:

Gary Katz
Bret Jordan
Trey Darley
Iain Brown
Greg Reaume
Ryusuke Masuoka
Kyle Maxwell
Richard Piazza
Paul Patrick
Mark Davidson
Greg Back
John Wunder - Moderator
John-Mark Gurney
Julie Modlin
Allan Thomson
Sreejith Padmajadevi
Jason Keirstead
Jane Ginn – Recorder
Other Guests

Agenda:

Status Updates
- Resolve issues from Aharon's email last week
- F2F in Brussels

Discussions

Meeting Notes:

Bret
- Please take the time to review the items on the email from Aharon
- Will be a F2F in Brussels at Borderless Cyber Event
- I'll set up a Slack Channel

John
- Discussion in Google Docs
  - Controlled Vocabularies – Mark Davidson made some comments
  - I'll go over them
    - Find in STIX 2.1-1 doc
  - Open Vocab
    - Using Indicator-Type – Have open string with suggested values (SHOULD & MAY)
    - Seemed to be good consensus on that

Allan
- I would support it, yes.

Kyle
- Hugely in favor of Open Vocabs

John
- Feel free to go through and make comments

Allan
- I submitted text to Bret

Bret
- I've merged your comments and Jason's – then we broke up into two docs…

has gone through several reviews

Mark

I have one comment to bring up – Closed Vocabs

John

One I really wanted to talk through was Closed Vocab

Lock down the field with a defined set of values – Strict set in a base set

Also has a companion field for you to define – with extension Vocab

We formulated this approach because we wanted to standardize as much as possible

Each default Vocab would have an 'Other' Item

Encourage standardization and interoperability

We have written up and have not discussed in a Working Call

Mark

The purpose of an Open Vocab – Have a defined set

Controlled Vocab – Have Defined and 'Other' – Kind of like the same thing.

Implemented two different ways

Allan

Repeated what he said

Mark

Clarified his approach

Allan

I agree – I had recommended that to Bret

Kyle

I would recommend that the closed ARE NOT extensible

Let's make sure that any Closed Vocabs are really Closed

Allan

I agree – Most fields will be defined as Open and a few as Closed

Since this is the first version of this Spec – More will be defined going forward

Kyle

Only reason is to use to Validate a field

Allan, you are spot on – Small set for a closed set

Mark

Does anyone oppose?

Rich

Let's discuss to make sure that we don't leave out a Use Case

Asked a question about how it will work

Once you say they are controlled… then there are no other options

Mark

Described how to use extension

Rich

If they look at options A, B & C and they use a D

Bret

I can get on board – If we don't understand it well enough… it should not be a Controlled Vocab

We discussed in Tampa

We don't make anything a Controlled or Closed Vocab unless we understand it really well

Mark

A concrete example is what we did in TAXII with the Status Message

The Spec defines Success, Failure – Consumer knows how to treat it

Greg Back

Looking back to version 1 – Were useful if you wanted to use your own

It sounds like what we are talking about are Enumerations

John

Every field is one on the list – that is how we define Enumerations
Now proposed – gives the extensibility

Allan

Bottom line is that vendors will add additional attributes – will create their own list
The intent would be to have an extension Vocab on an existing list

Mark

So long as those that don't use the extension, can't receive

John

For Closed Vocab – We'll remove the 'Other' extension
The only one we have now is the 'Relationship' field on the Relationship object
I can't think of a good example of a Closed Vocab right now

Rich

One more point – In some Controlled Vocabs, there are values like 'Undefined'
What do we do with those?

Allan

We can't make a general rule… it depends on the attribute

Mark

If it means Other… then OK

John

Ok, we'll make the updates to the text – We'll try to get ready for this week
TTP discussion

Gary

Yes, I'm on the line
Allan and I talked through and had some side conversations
We were trying to come to agreement about Attack_Pattern only
Getting a good TTP Object didn't seem to be achievable in the initial release
In STIX 1.2 there are a lot of things defined… but very few things being used
We need to define so that it can be used for Analytics
I think that we can push back the development of the TTP object – see how really being used
Let's create a TTP Object that will work for machine analytics
We are not saying don't have a way to represent malware
Some people were saying Attack_Pattern and refer to CAPEC

Allan

I agree with everything you said
I originally suggested that we have a TTP with Top Level Objects
Now I am fine with Gary's suggestion
The question is whether to have the named grouping
I can go either way – I fine with either choice
I think there will be multiple revisions of STIX and, I agree

Greg Reaume

I do want to ask about references to CAPEC

Allan

If a vendor wants to refer, can add a Custom field to a TLO

Greg Reaume

From my perspective – My organization uses CAPEC
Is there a way to preserve that

John

Wouldn't the CAPEC ID just be inside the Attack_Pattern object

Gary

In some ways, I'm a little hesitant… but, I realize that some organizations need it – we can

Greg

The way we envision it – there are multiple campaigns – Not a custom model
We like to have some representation that links to CAPEC

Bret

Last night John and I put some JSON to this – I'll paste in the chat bar
I'd like to something that we can write normative text for
Let's move the discussion down from the abstract level
https://docs.google.com/document/d/1ei7poJMigVasVkoKeEhe0sBa-BS59WU0xJwtBDwpmv0/edit#heading=h.ezp7bzdjessy

John

I can talk through what I did
The way you talked about it – Some want Attack Pattern & Malware & Malicious Tools
Things like Exploit and Infrastructure – Let's make that Not MVP

Gary

Pointed out that there are two different issues under discussion
Malicious Infrastructure definition – Anything that is sitting outside of your own infrastructure
Most basic one would be C2 – but can have others – Fake website

Allan

What if they are inside your network? Lateral movement

Gary

I guess you could say that is malicious because they have now taken over the server

Allan

I'm raising the question because it is anything that is used to attack
I don't think you can restrict from inside or outside a network

Gary

May be true – it is really how the Analyst's use

Allan

We need to define very closely
In STIX 1.x there are lots of objects without good definitions – Vendors used differently
We want to STIX 2.0 to succeed

Gary

I agree in principal – That is why we have taken that approach in Campaign
But, for certain defined User Groups – we need some flexibility so that Analysts can use it

Allan

Basically what you are saying is that we need to make sure that the
people that are using the standard will fit their Use Cases

Gary

We do need to make sure we have good definitions… but, let's get back to TTP
So let's look at some of the other things without the TTP layer of abstraction

Bret

Let's focus on the things we can do and understand – Attack_Pattern is one we can do
Malware is another – maybe Malicious Tool
I'd like to see us start whittling away and get some things done

Gary

We should look at all separately

Paul

I've yet to see the value in a separate TTP object
I took a look at John's code
We need coverage of everything

John

One thing that is not covered is Exploit – We should look at

I'll put together one for Infrastructure so people can look at it
A couple of other points
Use External IDs – Don't know if we can standardize on CAPEC
Some people are using AA&CK
Please look through the proposal
Other one is Kill Chains –
We still need to talk about that – Let's put that on the Agenda for next week
Think about that as you are reviewing

John

Noted where the Proposal document is
There are two other things I wanted to point out
Arrays
IDs
Other thoughts on TTPs? Hearing none
I didn't have any

Sharma

I'm from CISCO Systems
We recently presented a proposal XMPP Grid – proposal – Can we consider

Bret

We can set up a TAXII working call to look at that

Sharma

Thank you

John

Internationalization Mini group is having a working call tomorrow – Ryu is organizing that
They need some more inputs

Bret

OK, if there are no other topics, we can give you back 7 minutes of your day

********** ******

Meeting Terminated