CTI-TC Weekly Working Sessions

Meeting Date:	**Tuesday, April 5, 2016**
Time:	**3:00 pm UTC**
Purpose:	**Weekly CTI-TC Joint Working Session**

Attendees:

Ivan Kirillov
Rich Piazza
Bret Jordan
Gary Katz
Aaron Chernin
David Eilken
Jon Baker
Sarah Kelly
Jason Keirstead
Patrick Maroney
Iain Brown
Trey Darley
Scott Shreve
Rich Piazza
Allan Thompson
Ryusuke Masuoka
Mark Davidson - Moderator
Jane Ginn - Recorder
Other Guests

Agenda:

- Update on Face-to-Face in D.C. Area
- Review the MVP Matrix – Initial Ballots

Meeting Notes:

Face-to-Face Meeting Planning update

Jason Keirstead
-Will be April 19 & 20 in D.C. area
- Space only holds 16 people – Gary Katz looking into alternate location
Gary Katz
- DC3 Conference Room – Close to BWI airport – Holds 43 people
- Can bring laptops to this room
Mark Davidson
- Any objections?
Allan Thompson
- It is the best thing to do
Iain Brown
- I'll be coming in
Jason Keirstead
- As of today, there are 3 people that are not from the U.S.

Discuss the MVP Ballot

Rick Piazza
- John Wunder put together a table and asked everyone to put their votes in
Mark Davidson
- To be clear – this was an informal vote
Allan Thompson
- Columns don't all add up
Rich Piazza
- Green means accepted
- Red, voted down
- White – means 2 or less votes
I'll go through the table – Go through list
Aaron Chernin

- I'm going to identify myself – so I am not anonymous
- See the 2.x – Do we want MVP and "Extra Stuff"
- More we get on left column the longer it will be to release

Gary Katz

- We didn't realize voting was going on – so no one in my organization voted
- Is there an ability for someone in community to work on things?

Allan Thompson

- Can the chairs state how they would define the MVP?

Aaron Chernin

- We just identify a gap – Before we identify the features
- We need a Mission Statement
- If we get agreement

Allan Thompson

- I represent a company that is building products
- MVP needs to address Use Cases

Rich Piazza

The 80/20 rule should drive – Everyone has Use Cases

Allan Thompson

-If it is 80% of Use Case – and what a vendor needs to do
- Need to be open-mined about vendor extensions

Aaron Chernin

- We create a STIX/TAXII product – but does not mean to me that meets all
- I can still do other things in STIX 1.x
- My definition is: Make STIX easy enough for consumers
- If does not support – I'll fall back to STIX 1.x

Gary Katz

- My POV – We build for large organizations w/ more than 100 members
- Also need to build to support the Analysts
- If not, does not support an MVP
- If does not allow us to restrict data in way U.S. Government need… we cannot use
- If things that need to be included – Effects overall architecture – Look at it now

Rich Piazza

- Can include in 2.x

Gary Katz

- Use example of Versioning – needs to be in 2.0
- If we rush to include it, and we get it wrong… then that is a risk

Rich Piazza

- We may require some thinking about it…

Bret Jordon

- Also important with framing of this discuss – put in a cadence of release cycle
- 2.0 could potentially be released in July
-2.1 could be in September timeframe
-What is the minimum that needs to be done so people can start writing code?
-By time finish ramp-up, 2.1 will likely go out
-I suggested we do not go to full standard until 2.1 or 2.2

Gary Katz

- Understand that… but have some concern from the architecture side
- With STIX 1.x we didn't think about some things about how would work in the larger system
- There are major components that need to be considered
- Used example of field-level data markings
- Used by U.S. government & commercial consumers

Rich Piazza

-Once we decide on 2.0 or 2.x – we need to take into consideration what all want

- Just because it is not in 2.0 – it does not mean that you don't think about it

Allan Thompson

- In previous company I was involved in the 802.11 standards – many sections that are not used
- In the end, there is a core group that is implemented
- We should focus

Trey Darley

- Confirmed that some faulty parts of 802.11 stack…

Mark Davidson

- How do we get back to this MVP discussion?

Rich Piazza

- Let's just use this first cut as a basis
- Try to take through the list
- Third-party indicators – Surprised

Aaron Chernin

- Didn't vote for it in the STIX – Don't see in his feeds
- Should be in 2.x – It needs to be here

Patrick Maroney

- Some communities have very sensitive signatures
- Reason that not sharing today – Would support for 2.x

Gary Katz

- I would support what Patrick said

Patrick Maroney

- This is the secret sauce – Lack of data markings is reason

Bret Jordon

- We do a lot of Yara rules

Rich Piazza

- Consensus on the phone – 2.x

Allan Thompson

- OK with moving to 2.x

Rich Piazza

Some of the ideas divided between basic and more advanced

- Example – Complete Asset Model
- Where along that spectrum do we want to be?

Patrick Maroney

- Not having Target as Top-level object? There was a group in the past
- Asset considerations pivot off of that decision

Rich Piazza

- Gary could you talk about Investigation
- Pre-cursor to an Incident
- Some people don't think needs to be in the MVP

Bret Jordan

- Is this a separate TLO or just a State within an Incident?

Patrick Maroney

- Those that have to report within 72 hours – Statutory Requirement
- So it could be an important issue

Gary Katz

- Whole topic – difficult to tell because of lack of definition

Patrick Maroney

- I did supply those links – I'll resend them out to the community

Mark Davidson

- Point of this list is to come to agreement about MVP in 2.0 & 2.x
- Gary – Open Question about how to define – We need to track
- We need to get this list to a point where we can get this out to a ballot

Rich Piazza

- Good point – Just because it is Red… cannot go the other way
- Pat is going to post some resources – we can reconsider
- Exploits did not get a Majority
- People did not really know what the definition is

Jason Keirstead

- Link back to CVE?

Rich Piazza

That is a good example

Trey Darley

How many people voted? 15 of 60
Can we resend it out?

Mark Davidson

Less than ¼ of voting members
Go through whole list

Rich Piazza

Proceeded on down the list – Configuration/Misconfiguration
Was a CCE – But not used that much
This was the closest vote

Aaron Chernin

CCE is important

- It is a vulnerability – one of the most used

Ivan Kirillov

- CCE has not been updated since 2013

Bret Jordan

- It seems like we are adding things… How much in 1.2?

Rich Piazza

- If easy to bring over, then we can use
- If not being used. We need to reconsider
- CWEs people were not using as much
- I want to go through all
- Intrusion Sets

Gary Katz

- I'll put out a Straw Man

Rich Piazza

- Course of Action – passed
- Automated Course of Action
    - People are not ready to go for… but may want to have an extension
- Field-level markings – Most people want to delay
- Object level marking – Accepted
- Delay other markings..to 2.x
- Internationalization – Postponed to 2.x
- Full Identity – Similar to CIQ
- Defensive Tools did not get a full majority
- Rich Text voted down
- Versioning in 2.0

- If have Vendor-defined fields… vendors can extend
- Representing Impact / Potential Impact – 2.x

Mark Davidson
- We all have the same goal
- SurveyMonkey or other Ballot
- Need to further refine… Then go back out for a vote
- Let's iterate on this

Rich Piazza
- For people that did not vote.. It would be good to get their votes in

Bret Jordan
- Co-Chairs get together with John Wunder – consider what constitutes Approved?
- Should we move all into SurveyMonkey

Rich Piazza
- Let's get more people to vote on this informal ballot
-Then go for an OASIS vote

Mark Davidson
- Anyone who objects

Gary Katz
- We are the people that are trying to define the standard
– That is different from the people that are going to use
- Have a couple of new topics
  -- Want to have something on the Agenda for presentation
  -- Back on CTI-Common issue – Vote
  -- If we move the issue to merge – Will have major implications want to reconsider

Rich Piazza
- Old ballot wording was misleading
- Would 2nd that

Trey Darley
- As author of ballot – I'll try harder next time

Gary Katz
- Can we readdress?

Rich Piazza
-Let's discuss on Slack

Gary Katz
- I cannot get on Slack

Mark Davidson
- Let's discuss on email
- OK…

Meeting Terminated