CTI-TC Monthly Meeting - Notes

Meeting Date:	**January 18, 2018**
Time:	**Session #1 - 11:00 AM US EDT**
Purpose:	**Monthly Full TC Meeting**

Attendees:

Name	Company	Role
Anderson, John	NC4	Voting Member
Baker, Jonathan	MITRE Corporation	Voting Member
Barnum, Sean	FireEye, Inc.	Voting Member
Butt, Michael	NC4	Voting Member
Casey, Tim	Intel Corporation	Voting Member
Coderre, Robert	Accenture	Voting Member
Darley, Trey	New Context Services, Inc.	Voting Member
Davidson, Mark	NC4	Voting Member
Dye, Daniel	NC4	Voting Member
Gong, Nicole	MITRE Corporation	Member
Hagen, Stefan	Individual	Voting Member
Hayden, Nicholas	Anomali	Voting Member
Hostetler, Dennis	Lookingglass	Voting Member
Jones, Elysa	Individual	Member
Jordan, Bret	Symantec Corp.	Voting Member
Kakumaru, Takahiro	NEC Corporation	Voting Member
Keith, Robert	Symantec Corp.	Voting Member
Kelley, Sarah	CIS	Voting Member
Kostrosky, Curtis	Symantec Corp.	Voting Member
Mates, Jeffrey	US Department of Defense (DoD)	Voting Member
Mauch, Michael	Symantec Corp.	Voting Member
Maxwell, Kyle	Accenture	Voting Member
Morris, John	IBM	Voting Member
Pepin, Michael	NC4	Member
Pumo, Beth	Kaiser Permanente	Voting Member
Ricard, Chris	Financial Services Information Sharing and	Voting Member
Riedel, Daniel	New Context Services, Inc.	Voting Member
Royer, Philip	Phantom	Voting Member
Shok, Richard	U.S. Bank	Voting Member
Sparrell, Duncan	sFractal Consulting LLC	Member
Storms, Andrew	New Context Services, Inc.	Voting Member
Struse, Richard	MITRE Corporation	Chair
Suarez, Natalie	NC4	Voting Member
Taddei, Arnaud	Symantec Corp.	Member

Taylor, Marlon	DHS Office of Cybersecurity and Communication...	Voting Member
Van Dyk, Robert	Northrop Grumman	Voting Member
Varner, Drew	NineFX, Inc.	Member
Werntz, Preston	US Department of Homeland Security	Voting Member
Witten, Brian	Symantec Corp.	Member

Agenda:

======

1. Report from Prague workshop and hackathon
2. Live demo!
3. EU STIX/TAXII decision
4. STIX update
5. Observables update
6. Ongoing discussions + Patterning
7. TAXII update
8. Discussions on Version 2.1
9. Interop update
10. Plans for Upcoming Plugfest
11. Update on Salt Lake City F2F

Meeting Notes:

Moderating: Richard Struse - Chair, CTI TC

Richard kicks off the meeting, reminded everyone to record the attendance because the monthly meeting counts toward your voting rights. It is important to do so to maintain or regain the voting rights. First, Rich wish everyone happy new year! And on behave of the CTI TC, thank everyone for the work you did in the past year (the year of 2017). We have a lot of content to discuss today, so I want to get straight into it.

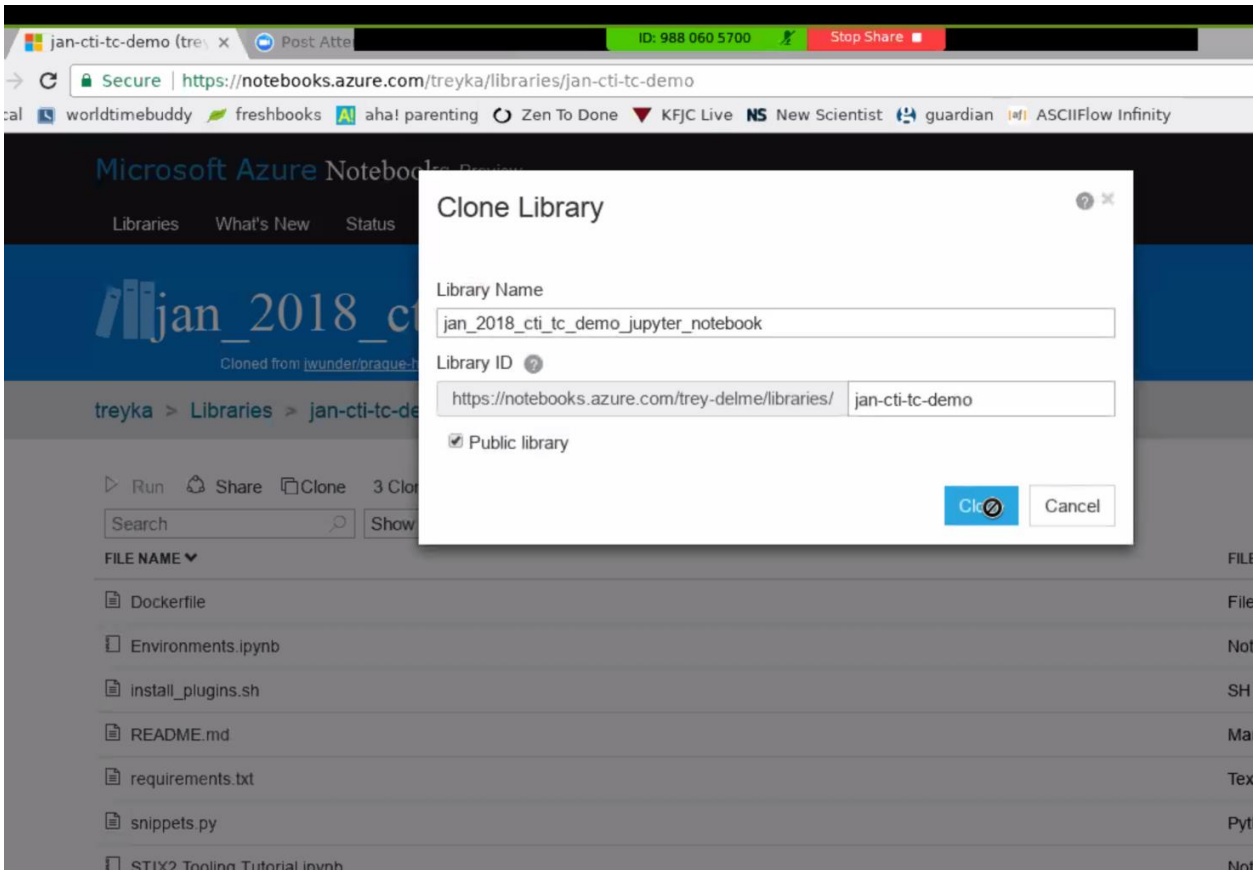
1. **Report from Prague workshop and hackathon - Rich**

Back in December, in conjunction with the joint OASIS and first technical symposium, we had two events on Prague; On Friday after the event, we hosted two things, one was the morning STIX 2.0 and TAXII 2.0 workshops and then the hackathon. The workshop goal was to help people understand what's new in STIX 2 and TAXII 2. Walking through some threat report. People enjoyed the session and got a lot of it. MITRE contributed the slides deck/training material that we developed for the training workshop and to the open repository in the next week. It intended to be the OASIS resource (not MITRE resource) for people to continue to use in their own organization, extend it, modify and improve them. We really hope it becomes true open source that everyone extends it improves it and then share back to the community. So that was the morning. In the afternoon, we had the hackathon, John Wunder, Trey Darley and I ran it. I really must thank John Wunder and Trey for the tremendous amount of work they did to make the hackathon success. Our goal was to take and provide, make it easy by providing the corpus of STIX2 data and a set of suggested challenges/problems to solve. We had STIX data from a variety of sources. We got throughout the room by the end of the day. We have people stayed all day working on stuff. I think it was SUCCESSFUL; I hope we do it again this year. At this point, I'd like to turn this to Trey to take us through a quick demo of what we did in Progue, and why it is important.

2. **Live demo! - Trey Darley**
   https://notebooks.azure.com/treyka/libraries/jan-cti-tc-demo

I set a live demo same as the Hackathon, John and I set up the Hackathon, we initially thought we were going to do the ants, but the hotel network was not great, we ran out of the time. John discovered that the Microsoft Azure has this "lovely" environment for hosting Jupyter notebook.
The Microsoft Jupyter notebook is kind an interactive python coding environment where you can have mixed text and graphics. As you can see, I have this throwaway account; you can go to notebooks.azure.com, I am just going to sign in here, and as you can see, I have no libraries; I am going to quickly clone the Library that we used in Progue. It is the same one that was used in the Hackathon but it's been slightly updated earlier today. The library link is provided (as above). You can login to the notebook.azure.com yourself with your Microsoft account, the same credentials we used for Skype, and it should just work. So I am cloning this into my throwaway environment. It should just take a moment, and It will run in the sandbox. Can you see it?

"no," it is black. Sorry about this, why don't we move on with the agenda, and let me figure it out what's wrong with this environment, then we can come back to this, okay?



3. **EU STIX/TAXII decision – Rich**
   So, there are some email traffic discussions about the EU decision; it is tremendous. What that is, is that

EU has made a formal Decision to recognize the use of STIX 1.2 and TAXII 1.1 for use in public procurement.

- Commission Implementing Decision (EU) 2017/2288 of 11 December 2017: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1515520575463&uri=CELEX:32017D2288
- This Decision covers all 28 EU countries and is also applied by the 4 EFTA countries. *
    - EU: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom;
    - EFTA: Iceland, Liechtenstein, Norway, and Switzerland.

*This means those 32 countries support STIX and TAXII to be used in the public procurement document. So, in their procurement, they can say the product implements STIX and TAXII, this is a big deal because for many years people think the STIX and TAXII specifications are the U.S. Government controlled things and EU organizations cannot really reference them. It really means U.S Cert has transitioned STIX and TAXII to OASIS. Last week, people asked what it means to previous versions and subsequent versions. The interpretation OASIS council has given us is that the EU will consider the updates to STIX and TAXII, for example, STIX 2.x as covered by this decision. Bottom line, this is a big deal, STIX and TAXII are ready for prime time. STIX and TAXII are proper to be referenced in the procurement documents.
This will help the ecosystems, especially the commercial ecosystems around STIX 1.x / TAXII 1.x and beyond. Just want to see if people have any questions and comments? Rich is particularly interested in hearing Vendors comments and feedbacks as the results of the EU decision.
Positive/negative/questions/interpretations, anything? Hopefully, this is viewed as an acceleration of the adoption of the STIX and TAXII in Europe primary, but maybe it will influence another part of the world, people may see it as a good idea, and they would adopt it as well, again, happy to answer the questions. We should be happy and proud of it. The work has been done, thank you all!

Alright, Trey – do you want to give another shot?

Trey: let's try it. If I get a black screen, I will immediately give back to Sarah.

*** Black screen again ****

Back to Sarah.

Rich: thanks to Trey, these things do happen. Thank your efforts to do this, Trey.
Bottom line John and Trey did a lot of work in the hackathon; this Jupiter environment is cool. Within a few minutes, you are writing python code using STIX2 APIs. Because of the data sets, organization contributed. we can have code to run STIX via several TAXII servers. Jordan provided the TAXII servers. Trey stood up the TAXII servers. It's easy to manipulate the STIX data.

I want to thank the organizations provided the STIX data (made data available for the Hackathon), and whoever agreed that data could be continue accessed, and to be there for people to use. That includes the open source feeds Brad has mapped, the folks from Anomali, and with Lemo (?), IBM contributed extra source in STIX2, folks at Perche(?) who contributed the dataset includes Opinion object and Sighting Object, which is kinda cool, not just Indicators, the Department of Homeland Security contributed data from AIS.

Trey: There are also all the IntOps validation datasets for different personas have been added. So, if you are implementing and you want to test against IntOps different Persona data, the dataset is there. If you look at Jupiter, all of that is there. The demo failure was not a Jupiter failure, it was a zoom on LINUX failure, if you are interested, you can reach out to me privately. Then I can walk you through that.

Rich: I think what we can do is to do this on another TC meeting or working call because this is valuable. With that, I would like to turn to DHS Preston Werntz (?) for a couple of minutes.

Preston – Just want to jump in for a few minutes to inform people that DHS maintains work order with MITRE, the current task order has expired, and there is a DHS contract issue, DHS has not gotten the new task order in time to covers people like John Wunder, Greg, Iven, this is because of the DHS contracting issue, it has nothing to do with MITRE. Just want to make people aware of that, DHS is working as harder as they can, to get a new task order issued. Pretty soon you will see folks back in and support the TC activities.
You will see much more activities from them.

Rich explained that his role and participation is directly supported by the MITRE Corporation, it is not under any contract. Therefore Rich's role will never be impacted by a specific contract; it will never be expired.
So that is the differences. Rich thanks to Preston for taking the time to explain this. If anyone has questions, can reach out to Preston.

STIX update – Sarah Kelly

First thing we want to talk about is the Assertion object, back in December or may be the end of November We were talking about the Assertion object.

- **Assertion**

  This was agreed to on a working call. Last call for objections/concerns before merging it into 2.1.
  There is a link to the google docs:
  - ➢ https://docs.google.com/document/d/15qD9KBQcVcY4FlG9n_VGhqacaeiLlNcQ7zVEjc8I3b4/edit#heading=h.qxvz3vox3ksj

Basically, this was agreed to on a working call. On the working calls, we cannot do the consents, so as for the procedure purposes, we want to bring this topic up for last chance of objections.

Rich added a correction here, Sarah agreed that, and thanks Rich for correcting her or remind her, this was debated on the call back in December. it is NOT an object itself, but it is a large property, that would be on several objects including indicators, etc. It is an assertion property or field. It is a block that kind looks like SDO. An example below:

Property Name	Type	Description
valid from (optional)	timestamp	The first time at which this Assertion was considered valid. If the **valid_until** property is provided, then the value MUST be greater than or equal to the value in **valid_until** If the **valid_from** property is omitted, then there is no constraint on the first time for which the Assertion should be considered valid.

valid_until (optional)	timestamp	The time at which this Assertion should no longer be considered valid. If the valid from property is provided, then the value MUST be less than or equal to the value in valid_from If the valid_until property is omitted, then there is no constraint on the latest time for which the Assertion should be considered valid.
source (optional)	string	The source of this assertion.
threat_level (optional)	integer	The threat_level property identifies the threat level that the creator is asserting with respect to this data. It should be noted that this value SHOULD NOT assume anything about the recipient of the assertion; that is, the value should be receiver-agnostic and not consider any specifics with regard to the environment, industry, etc. If present, the value MUST be a number in the range of 0-100.
description (optional)	string	A description that provides the recipient with a human-readable description of this threat level
categories (reserved)	N/A	This is reserved

Then for the categories, we didn't have enough information and time to get it corrected in 2.1, so we decided to leave it as is, and reserve it for as a future thing to be populated.

If you want to know more or FULL details, you can look at the google doc; it does need to be cleaned up, there are some comments to be resolved, you can look at it. But for the most part, we pretty much have reached the consent, and it is good to go.

So, does anyone has any questions about the Assertion property?

Marlon – I am not sure if it is getting clarified in google docs or not. On the threat level, I didn't see the indicated number order. Does the highest number mean highest threat? or lower number means lower threat? I just want to make sure it is clear.
Sarah does not recall if that was indicated in the google doc if Marlon can add this in the google doc, that would be great.

Sean asked if comments/feedbacks were tracked in the JIRA or something, Sean explained that google docs were great for quick collaborations, however, once the comments were resolved and passed the consent, the comments or the history of it would be gone. It is not a good place for tracking, in contrast, something like JIRA may be good for keeping a record of the comments and resolutions.

Brad: as one of the editors, I can answer that. In the google docs, all the comments, edits are kept in the Google land, so you can go back look at them. For new content, some of them has been put in issue track As CSD vote, we as a TC can start doing. Unlike word document, there is no way to track them.

Sean suggested that we open a ticket for JIRA track right now, for example, to track situations as the Assertion property where we have reached a consent and are ready to move on to the next stage. Google doc is great to track the comments and feedbacks in the background, but we need

Rich thinks that is an excellent idea, to track major milestones, for situations like this where we are in a good place for transition and have a history, we should open a tracker to record the summary of what happened, comments, feedbacks and resolutions of it and conclusion. This would help us. So, if people ask why did we do this? we could go back and review the history of it. So, thanks to Sean, I think that is a great idea!

Brad agreed to take action, will issue a tracker for this after the call, Brad is the only editor right now, so, it may take little longer, Sean can look at it after Brad opens the tracker. Other people can also look at and comment it on.

Sarah gave a summary of what other pending objects are, grouping was discussed on the working call.

Grouping

We have one Open question over the values in grouping-label-of

- https://docs.google.com/document/d/15qD9KBQcVcY4FlG9n_VGhqacaeiLlNcQ7zVEjc8I3b4/edit#heading=h.t56pn7elv6u7

Infrastructure

We have not discussed much on the working call; this is likely to be a topic to be discussed at F2F. We talked about the need to do modeling exercises. Please take it as a homework exercises and bring it to the F2F, that is if you are coming. There are many other open questions we have not talked about it, that is the status. They are:

Do we need the object? How does it relate to Observed Data/Indicators? Should it have external or embedded relationships?

- https://docs.google.com/document/d/15qD9KBQcVcY4FlG9n_VGhqacaeiLlNcQ7zVEjc8I3b4/edit#heading=h.maky5z1n51ds

The last two Items are IEP and COA.

IEP

IEP, which we talk about several times. Terry brought this to us.

We seem to have consensus that we want to add it with a caveat saying we're adding it to facilitate interchange but not defining how to implement it in tools
The doc needs to be cleaned up, the caveat needs to be added, and it likely needs to go through a final round of approval.

https://docs.google.com/document/d/1wiG6RoNEFaE2lrblfgjpu3RTAJZOK2q0b5OxXCaCV14/edit#heading=h.8tzg8tq7p9du

Brad – IEP is a great piece work we did, it provides a neat way of doing some more laborious type of marking and tagging. Problem is that when you try to implement it, it is difficult to figure it out what you suppose to do or a lot of elements in IEP that are difficult to figure out what we need to do. So that is why this caveat is there so there is no enforcement, because we don't want IEP or STIX to have this black eye, we don't want people to start implementing this IEP then run into this and that wearied little caveats then saying why this is not supported. We want people to understood that we put there to facilitated interchange but solution cannot be operating on this easily, it must bubble up to human, therefore STIX or anything can define around that? There is more information in the document.

COA -- Sarah

Course of Action (COA) object is there on the agenda for the F2F, COA is there for some time, Jody has sent a proposal to the list back in September or maybe November. They want to include it in STIX 2.1, so that is why we included this in the F2F agenda.

https://docs.google.com/document/d/1VVeXcXsKHbfjjdglLo-mFQlXpjUhyGbGUBPSBFnSERY/edit#

So that is all for STIX, if anybody has question, now it would be a good time, okay, hear none.

Cyber Observables Subcommittee Update – Trey

- DNS-based Patterning looks done for 2.1
  - Please review: https://goo.gl/NsRjb9
- Reviewing Terry MacDonald's Webpage and HTTP-Response-ext proposals
- Reviewing some STIX Patterning fixes (based on implementer feedback)

Don't have so much to report from the Cyber Observables, since Ivan is out due to the contact renew issues. We did finalize the DNS-based patterning report, please review it. Talk to Terry with his webpage and the HTTP-Responses-ext proposals. Maybe this can be reviewed at F2F. Then also there is some STIX patterning fixes. That's all I have to report.

Rich wants to know if there is way to make you and your organization have some meaningful participation for F2F, please let him know. Whether is through email, phone or through the list, whatever is best for you. This reminds him about Austin F2F, he wants 2018 be more successful, broaden the participation and want people to actively review and comment on it. Help sharping the standards. We also want to do more modeling, to model each of these capabilities before we agree

that they are ready for prime time. Maybe for example, you or your organization may not thrill to commenting on some property names or do not do care about the certain properties, however you do have datasets and are willing to do some modeling, that would be a great contribution to the TC. So, again, that is a general call, there are things we can do, things I can do or things the TC can do, whether is meeting schedule, or schedule/discuss how we make this happen. whatever suggestions you have I am interested to hearing them. So, we can really help sharping or expanding the STIX and TAXII. Again, we mentioned the EU decision earlier, and let's make some capitalization on that, make STIX and TAXII to response to many organization as possible.

TAXII Subcommittee Update – Brad

We had many organizations now working on code for TAXII and working on their implementations, I put together an implementation for TAXII and it is FREE available for people to use or looking at it. There are lot of users/people outside of TC are writing clients to talk to it. I got a lot of feedbacks and request, and varies elements how they implement it. So that is really a good sign. We have people working on implementing the protocols. We got enormous things right. Maybe a few things we implemented were not right, or may be wrong, we have to fix those in 2.1. Some of those are listed here:

- Clarifying Text
- Media Types
- Return Codes
- Manifest Resource
- Pagination
- Discovery Services
- API Root Paths

Media types and Clarifying Text

we need to fix Media types. Media types were incorrect, Clarifying Text, it is not clear to implementer to know what they need to do. Media types we choose were given to us by the OASIS staff. Then we learned from post CSboo (?), the media types were incorrect.
We were not supposed to use vendor's tree(?), and we need to use standard's tree (?). So, I will not approve the documents as the current Spec, we need to make some break changes. There are couple of ideas we can do with media types. We had people struggling with various TAXII end points, with some people use STIX media type, and some of them use TAXII media type. So, I have a proposal that where we just use single media type for STIX and TAXII content. And then, people want to use other content such as PDF executable, they can still do so. But for STIX and TAXII we will all use single media type.

Return codes dealing with posting data to a TAXII server, there are some ambiguity there, content is directly consumed versus some asynchronous…we need to clean that up.

Manifest Resource

I ran into some problems with Manifest Resource, where media type is available for that object, but you can get into weird situations because media types are not bind to a specific version. Manifest Resource is STIX object with all the versions TAXII knows about. So, we need to unravel, kind go back

fix that with media types and Manifest resource, because you can get into a bad state, part of doing specification development, then you have bunch people writing code, write implementations, find problems, then you go back and fix it. That is where we are at.

Pagination

Pagination is another area that is kind problematic for performance and for actual implementation, I have a proposal there to simplify the code and make it much easier to implement also to make it much more performant. There is a big array of issues, I have not on that, not going to go through every one of them, will discuss this at F2F and the next several working calls to try to close out those items. IBM has filed a lot of these issues as well and made comments on them from their server implementations

Discovery Services

Then we had some issues with discovery services, so we are going to go look at those, try to find better solutions for those. I have been talking to people from NIST about the way their people implement the discovery services for Woolly (?) which is IETM standard which is very similar to TAXII, we are trying to borrow some ideas from there, to make discovery services work better.

API Root Paths

New features for TAXII 2.1

- **Channels**
- **Query**
- **Question and Answer**

The new features we are looking at, and additional to the fixes people have been asking for is channel support, and TAXII query, that is something we started to work on, then stopped, because there is lot of things we needed to flush out with STIX. Trey put together a document all about query, So, we will use a lot of that. Jason K. and Terry McDonald have worked on some questions and Answers. The concept can potentially go across the TAXII channel, it can potentially go across the repository connection as well, so we will be talking about that.

- **Timelines for TAXII 2.1 - Proposals**
  - **Address all breaking changes ASAP**
  - **Release a CSD-01 after the F2F**
  - **Release CSDs as features for 2.1 get finished**

Timelines for TAXII 2.1 and the notional proposals from my stand point view. I would like to see as a subcommittee TC to try to fix all the break changes as soon as possible. And release CSD for 2.1 that contains all these changes and things we know solutions for, and things need to be immediately fixed. That way people can start implementing and verifying these changes are sufficient. Then I

would propose as we work on these changes we need to release what we are working on until we get everything finished.

That is all.

Interoperability Subcommittee Updates -- Rich

Jason and Allan are not on the call, InteOpt Subcommittee has number of things on the agenda:

- F2F Interop Agenda
  - Plugfest Debrief & Lessons Learned
  - Focus on STIX2.1 & TAXII 2.1 test updates
  - OASIS STIX Preferred logo and brand in progress
- Plugfest (Jan 30, 2018)
  - TC Participants: 11 orgs/individuals
  - Planning document has been completed (except public URLs we will use)
    - Tests cover persona (TXS, DFP, TIP, TMS, TDS, TIS, SIEM)
    - Basic connectivity, sharing and collaboration

At the F2F January 31, we will first start with debriefing and lessons learned, it is going to be really interesting. I am sure we will also have learned that implementations for the specifications can be improved.

Plugfest is on the Jan30, 2018, I am looking forward to seeing what come out of this. They had planning document out there and they are covering lots personas. They did tremendous amount of work, to ensure the plugfest successful and as productive as possible. I am looking forward to seeing the outcome. Again, the idea behind the plugfast is to get individuals together in the room (both virtually or physically there in UTAH) to work through some interoperability test see if they can talk to each other. At the end of the day, we would have good sense of what worked and what didn't. and what needs to be done to improve the interoperability on the specs and specific implementations.

Allan is also going to talk about STIX2.1 & TAXII 2.1 test updates and STIX Preferred logo and brand updates. That is the program we are lunching allow organizations to self-certify. Once they are self-certified they are allowing to use this preferred logo in their marketing materials. That is all for the interoperability.

Salt Lake City CTI TC F2F

F2F is coming up in Salt Lake City, registration is closed, however, if you are interested to participate we absolutely welcome you all, and if we inspired you as result of this meeting, you decided to go and jump on the plane to get to Salt Lake City, you need to let Brat Know as soon as possible. So, Brad can get things setup and get everyone access to the facility. Thank you so much to Brad and Symantec to make this happen.

Remote access is challenge, we will everything to make virtual attendance easier, make things as smooth as possible. If you interest participates remotely, I don't think registration is necessary, but please let Brad know. So, we can get the information to you, and so you can connect and get on.

Plenty of parking spaces, Brad added.

Rich needs feedbacks from implementers, especially those who doing commercial products, we would like to hear what you are looking for and waiting for before you start to commit resources to develop the code with respect to 2.1. Whether is CSD or a committee specification? this is your chance, you have opportunities to impact what we do and sharp the standards. More concrete feedback we get, the more we can help make decisions as TC where we can make break changes.

Anything else? This is the first meeting of this year, Rich wants to reminder people about 2018, lots of great work we did for 2.1, and 2.0. for 2018 we want to get people to implement. We need help people to adopt STIX and TAXII and implement STIX and TAXII to get them in the operation environment.

Thank you all.

****

Meeting Terminated