CTI-TC
Interoperability Subcommittee

<table>
<thead>
<tr>
<th>Meeting Date:</th>
<th>Wednesday, July 13, 2016, 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time:</td>
<td>18:00 UTC - 02:00pm to 03:00pm EDT</td>
</tr>
<tr>
<td>Purpose:</td>
<td>Monthly Meeting</td>
</tr>
</tbody>
</table>

**Proposed Agenda:**

- Strategic White Paper prepared by the OASIS
- Self-Certification Process
- Testing frameworks

**Strategic White Paper prepared by the OASIS**

... For all the participants both in looking together for the documentation and technical data files required for these test suites, also the participants in terms chasing clarity, it’s not a trivial task, that’s the primary take away here. There are some similarities and primary scope here, we have some unique challenges here under the OASIS Cyber Threat Intelligence committee, essentially we have 6 different technical standards under the committee, we consider STIX, TAXII, Cybox as three different standards. The next generation standards will be evolutionally, and not going to be revolutionary. Transition from XML form to JSON and also changes will be making to the TAXII.

We discussed between with the subcommittee co-chairs, some very knowledgeable folks in other OASIS TCs, and Dr. Berger from Georgetown University. Research findings are the University of NH IOL aligns well with our requirements. The central elements are a software based tool, that CTI TC members who are doing the test can have local instantiation of it. So we all testing use the same framework, and so we will have a consistent result.

During the conversation, we discovered that the OASIS thought leaders, president of OASIS had engaged Chet, and then the advisory board put together a recommendation white paper. OASIS has identified this topic as a key strategic aspect of testing for all CTI standards, so we can have one stop cohesive test suites. We decided to put current efforts on hold to evaluate the proposed OASIS Self-Certification process. We will not go through this paper today, but encourage anybody who is interested this topic, please read this white paper.
Self-Certification Process - Executive Summery by Chet Ensign - OASIS

- Background on white paper, where does OASIS stand now?
- How Chet thinking CTI TC may want to start

Challenge:

OASIS has hand off Cybox 3.1.1 spec for publication and public review, the spec has 94 parts, challenge is that there 94 parts and everything has to be done 94 times!

If you look at any of the cover page for any other specs that been done, either committee spec draft or committee public draft or compare to STIX and TAXII, for Cybox, everything has to do 94 times. Only finished committee specification draft yesterday. Now try to plowing through the CSPIV release. (comments: happy to get some of your time here and your engagement going forward. By the way, we hope that is 95 documents, the one includes them all)

Background On Self-Certification:

The self-certification topic came up beginning of the year, when work on strategic goal for 2016. The reason this came out was that CTI TC wanted to get out a whole package, to better support the members. To provide not only in the development of the specification or standards but also in adoption, promotion, dissemination, one stop interoperable stop shop. The ideal is that; you can come to OASIS to get all the pieces needed to build a community around your work. You may see the announcement about Open source project on “GitHub”. Now TC can choose and support more Open source projects, they are truly open source projects hosted by the technical committee. TC can launch an open source project, so the community can grow resources around it. We are working on making it possible for TC to commute to get out the same way as the svn conversion control. We also working on possible for TC conversion and control. Also want to do the notion of supporting for self-certification program.

Self-Certification Vs. Thirty Party Certification

We have looked through various industry group program out there, and learned that there are two types certifications out there:

1. Self-Certification
2. Thirty Party Certification

The distinction between self-certification and thirty party certification, self-certification you test the scenarios yourself, and you submit the results, then you certified it.

The third party program on the other hand, you have to contracting through a lab where you testing at the lab and you have to pay that lab. The one we looked at they are quite expensive. It looks like they would add quite large amount of work to the companies want to certified.
Self-Certification program where importation setups, testing infrastructure and criteria what have you. Depending on how you want to work, there are several things can be done. But party speaking self-certification can run sets of test, and get the result back to OASIS, and then certified the product. We felt that this approach is far more feasible.

So that’s what we really focused on self-certification, in looking at TC have done certification. What they have done is interoperability testing.

Self-Certification can be done with a check list, you test them, and check them, get the results back to OASIS and then certify it. This looks like we can do that ourselves, develop criteria then test them. Where we are at the moment is we get the concept in place, we have not had time to get much further, I got stack of meeting Materia, several contact to talk to just start to think about practical consideration. Hoping to get together / working together, work with other OASIS staff, bring in third part contract and TC, we can build the “house”, I think this is a good group to start with.

What we see is that there are three different topics, it is easily mixed up together:

- Interoperability demonstration
- interoperability testing
- self-certification

**Interoperability demonstration**

I know that OASIS is targeting for the RSA Demo 2017, the goal is to have something in place for then. To do an interoperability demo more than anything else, we can get prove of concept, that’s a pretty challenge goal for 2017.

- First question is that should we start with version 1.x? or version 2.0? or
- Are we going to try build something in parallel with version 2.0 still work at that point?
- It may be the next generation spec by RSA 2017 possible
- Main Interoperability showcase demo probably will have focused on 1.x, vendors have some 2.0 products to show too

We originally hope to have something in the fall. One of the issues is that the group has to decided what to demonstrated. First of all, you should have a stable set of normative. Should start with a core set. For example, initial set of 30 functions everyone should pass the test.

- Agree with start to test at 1.x, baby step with 1.x standard.
- May be something in between, hope there won’t be many refactoring required when we move to 2.x.
- One suggestion is to test against other vendors, every other vendor for example, controlled self-certification. InterOp demo. Two products test against each other, then put it on the wiki page.
- Suggest the baby step is 1.2 -- Uncontrolled Self-Certification with something like two vendor references (against a specific traditional profile) and in parallel work 2.0 toward Resource/ Service based self-certification as a goal
• Even having some kind of standard of communication of self-certification would be a big step

**InterOp Demonstration**

Need a roadmap to test broader version and testing plan, 1.x self-certification plan, in parallel we can testing against other vendors. Self-controlled certified. Then we can put them out for approval.

Chet’s time commitment: 2 weeks from now, by then would have Cybox done, OASIS have annual on-site meeting at the end of July.

**What does interoperability mean in each standard?**

- Interoperability on TAXII is much simpler, we need developer different profile and use cases.
- First we need to determine what do we mean profile.
- Other things to consider - where do we have the servers? or where can we host them?

**Testing Framework**

- Topics to be prepared
- An interoperability standard maturity testing framework may be reviewed next time

**Other topic**

- Looking for volunteers for any particular skills
- If you have a particular skill, please speakup