CTI-TC Monthly Meeting: Session #1

Meeting Date: January 16, 2020
Time: Session #1 – 11:00 AM US EST
Purpose: Monthly CTI TC Meeting

Attendees:

<table>
<thead>
<tr>
<th>Name</th>
<th>Company</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applegate, Alex</td>
<td>LookingGlass</td>
<td>Member</td>
</tr>
<tr>
<td>Aviles, Jorge</td>
<td>Johns Hopkins University Applied Physics Lab</td>
<td>Observer</td>
</tr>
<tr>
<td>Butt, Michael</td>
<td>NC4</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Caselli, Marco</td>
<td>Siemens AG</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Casey, Tim</td>
<td>Intel Corporation</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Davidson, Mark</td>
<td>NC4</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Garcia Robles, Javier</td>
<td>LookingGlass</td>
<td>Member</td>
</tr>
<tr>
<td>Ginn, Jane</td>
<td>Cyber Threat Intelligence Network, Inc.</td>
<td>Secretary</td>
</tr>
<tr>
<td>Girard, David</td>
<td>Trend Micro</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Hayden, Nicholas</td>
<td>Anomali</td>
<td>Member</td>
</tr>
<tr>
<td>Hohimer, Ryan</td>
<td>DarkLight, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Huey, Caitlin</td>
<td>Cisco Systems</td>
<td>Member</td>
</tr>
<tr>
<td>Jones, Elysa</td>
<td>Individual</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Jordan, Bret</td>
<td>Broadcom</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Joyce, Ryan</td>
<td>DarkLight, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Katz, Gary</td>
<td>FireEye, Inc.</td>
<td>Member</td>
</tr>
<tr>
<td>Keirstead, Jason</td>
<td>IBM</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Keith, Robert</td>
<td>Symantec Corp.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Kirillov, Ivan</td>
<td>Mitre Corporation</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Kostrosky, Curtis</td>
<td>Symantec Corp.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Lee, Chenta</td>
<td>IBM</td>
<td>Member</td>
</tr>
<tr>
<td>Lenk, Chris</td>
<td>Mitre Corporation</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Maroney, Patrick</td>
<td>AT&amp;T</td>
<td>Member</td>
</tr>
<tr>
<td>Mates, Jeffrey</td>
<td>US Department of Defense (DoD)</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Maxwell, Kyle</td>
<td>Accenture</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Merchant, Aubrey</td>
<td>Broadcom</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Morris, John</td>
<td>IBM</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Noguchi, Kazuo</td>
<td>Hitachi, Ltd.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>O'Brien, Christopher</td>
<td>EclecticIQ</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Parekh, Devesh</td>
<td>IBM</td>
<td>Member</td>
</tr>
<tr>
<td>Patrick, Paul</td>
<td>FireEye, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Pumo, Beth</td>
<td>Kaiser Permanente</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Radhakrishnan, Ashwin</td>
<td>Anomali</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Ratliff, Emily</td>
<td>IBM</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Reaume, Greg</td>
<td>TELUS</td>
<td>Member</td>
</tr>
<tr>
<td>Ricard, Chris</td>
<td>FS-ISAC</td>
<td>Voting Member</td>
</tr>
</tbody>
</table>
OASIS CTI-TC Monthly TC Call

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Riedel, Daniel</td>
<td>New Context Services, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Riley, Shawn</td>
<td>DarkLight, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Serban, Vlad</td>
<td>LookingGlass</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Stewart, Justin</td>
<td>LookingGlass</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Storms, Andrew</td>
<td>New Context Services, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Taddei, Arnaud</td>
<td>Broadcom</td>
<td>Member</td>
</tr>
<tr>
<td>Taylor, Marlon</td>
<td>DHS Office of Cybersecurity and Communications</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Thomson, Allan</td>
<td>LookingGlass</td>
<td>Voting Member</td>
</tr>
<tr>
<td>van Belkum, Aukjan</td>
<td>EclecticIQ</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Vargas-Gonzalez, Emmanuelle</td>
<td>Mitre Corporation</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Williams, Ron</td>
<td>IBM</td>
<td>Voting Member</td>
</tr>
</tbody>
</table>

**Agenda:**

- Introduction & Welcome
- Sub-Committee Updates

**Meeting Notes:**

**Trey Darley**

Let’s kick this off – We hold these two times a month to accommodate global time zones
Be sure to record your attendance.

We are close to the finish line
Important for us to make decisions & maintain Voting Rights
Have colleagues join the second call

**Emily Ratliff**

Sponsorship updates

**Gary Katz**

Update on Malware – Will not be able to do Infrastructure

**Trey Darley**

If we don’t have another Sponsor for Infrastructure, we’ll have to pull it out and
Do another release

**Richard Struss**

Asked for another Sponsor to step forward for Infrastructure – it will be dropped

**Andrew Storms**

Please – we are the biggest TC rather than OASIS – We’ll help you get up to speed
There needs to be another Sponsor

**Bret Jordan**

If you’ve already completed your work – please let us know so we can update status
MITRE has completed Deterministic IDs
You can complete the Attestation Template

**Chris Lenk**

MITRE, on behalf of DHS Grouping, Malware, Malware Analysis & Deterministic IDs

**Looking Glass**

We completed SOCs as First Level Objects

**Gary Katz**

We submitted the Malware object from FireEye
SCOs and SCO relationships has already been submitted by DC3 and FireEye

**Greg Reaume**

Is there an open-source project we could have staff developers contribute to
as a form of sponsorship?

Clarified that he was asking so he could support on the Infrastructure SDO

Bret Jordan
My GO project [gave update on status]

Emily Ratcliff
I had submitted some STIX pull requests

Allan Thomson
[Gave clarification on why the Sponsorships were added to the process]

Emily Ratcliff
[Gave a summary on the Sponsorships]

Jeffrey Mates
I hope to get Malware Analysis done next week

Richard Struse
Reiterated Allan’s point about how important to have another Infrastructure Sponsor
We are serious about following these rules – we will drop it with no Sponsor

Allan Thomson
If people are not seeing the use of Infrastructure in their products,
they are doing it another way ~ Suggested people are doing it another way

Greg Resume
[On Chat: Is there a list of currently maintained open-source projects somewhere?
I am happy to take an action to do some legwork and contribute that. However, I’ve been
away from the community a while and not sure if this is already done somewhere and where
I should contribute that if I take it up.]

Andrew Storms
I’ll have John-Mark Gurney reach out to you on this

From Chris Lenk to Everyone [On Chat]: 09:22 AM
Not necessarily a complete list, but there is: https://wiki.oasis-open.org/cti/#Open-
Source_APIs_and_Tools_.28in_order_of_contribution.29

Bret Jordan
[Gave an update on Chat]
Course of Action

Grouping
MITRE/DHS : DONE
EclecticIQ : DONE

Infrastructure
New Context : in progress

Malware
MITRE/DHS : DONE
FireEye : will be done

Malware Analysis
MITRE / DHS : DONE
DC3 : should be done next week
SCOs as TLOs
Looking Glass : DONE
FireEye ; DONE

SCO Relationships
FireEye : DONE
Looking Glass : will be done

Deterministic IDs
MITRE / DHS : DONE
Looking Glass : will be done

Bret Jordan
Clarified about what we would do if the Sponsorships yield evidence that the code
Needs to change

Jason Kiersted
Asked for clarification on what constitutes a Material Change

Bret Jordan
We can bring up with Chet and get clarification

Allan Thomson
Made a point on a Deprecated Relationship – Wanted to get clarification on
Need for Product support – Definition of Deprecated – is going to go away
In the Future (Whether an Optional or Mandatory relationship)

Bret Jordan
These were Required properties ~ they were embedded

Allan Thomson
Highlighted a point about Required properties vs. Deprecation

Jason Kiersted
In the GitHub issue, you seemed to agree, and now?

Allan Thomson
No, it will be a lot more work to handle in the Patterning Grammar – so we should fix

Bret Jordan
Gave an update on non-Material changes – Mainly editorial
We could accept this recommendation and remove references to Deprecated
Asked for additional comments from the floor

From Marlon to Everyone [On Chat]: 09:32 AM
"Material Change" is any change to the content of a Work Product that that would require a
compliant application or implementation to be modified or rewritten in order to remain
compliant or which adds new features or otherwise expands the scope of the work product.
I would agree with Jason. Non required (conformance) changes shouldn't be material
changes.

Richard Struse
Can you pose that question in the slide? So we can also cover this for Session #2

Bret Jordan
Asked for objected to remove references to deprecated [no objections]
Rich Piazza and I will schedule an Editors call and make that change

Bret Jordan
Gave an update on TAXII Timeline
Developed a visual to clarify the actions to date:
Gave update on moving forward on the motion ~ Chet will move forward with opening Ballot

It looks like it will pass –

In regards to the query issue — Gary Katz and I submitted a proposal — Trey

Has produced a proposal — DHS has produced a proposal

We have not reached resolution

Richard Struse

This is our opportunity as a TC to discuss — the Ballot is passing at the moment

Vote tally as of now: Yes: 67.857%. No: 32.142%

As Bret has laid out — there is not clear consensus

We need to deliver STIX & TAXII 2.1 to the Community, then get STIXPreferred implemented

Then, we should get the parties together on the TAXII Query issue

This is something that needs a lot of thought

What I am advocating – We continue to get 2.1 Spec out

We also have the STIX Enhancement proposal – We should make a STIX/TAXII effort

Marlon Taylor

I posted a question on the Chat — When will TC address the Proposal – Filtering

Bret Jordan

[Gave some background on when the Filtering topic was covered — Salt Lake F2F]

Jason & Terry produced a counter-proposal

There has not been a groundswell to resolve now — We can take this up as the first item

I’ve not heard consensus on the TC to add this

Marlon Taylor

Does TC plan on incorporating guidance into the specification?

Bret Jordan

Talked about how to fast track — Then could make its way into Interop Testing

Richard Struse

STIXPreferred is based on final Spec’s

Delaying STIX/TAXII 2.1 would have a spillover effect into the STIXPreferred

We could start working on a follow-on proposal

Marlon Taylor

The proposal submitted in Dec. would be a non-Material change, it would not effect Timeline

Bret Jordan

When we talked about that before, there was significant pushback in the community

Mark Davidson

[Gave some input on his POV on getting the Specs out ASAP]

Chris Ricard

We can incorporate additional functionality in the future – we need to get 2.1 out

Trey Darley
OASIS CTI-TC Monthly TC Call

Marlon, I feel your pain – There is consensus that this is something that we need
But, we have an opportunity in the global marketplace of ideas – to ship 2.1
But, we are feeling pressure to get these shipped as CSs ASAP
Is that something you can live with.

Marlon Taylor
We are definitely supporters of getting that shipped. I just want to emphasize that
My proposal is a change to a Table – a non-material change
The proposal would not impact the release of 2.1

Richard Struse
I don’t think we have time to answer that issue – we have one minute left

Justin Stewart
We have a roadmap of what we hope to accomplish in 2020
Mark Davidson and Solarium can host a PlugFest in May – Let’s look forward to this

Mark Davidson
I have a room blocked off for 3 days – May 13th to May 15th
Agenda to be determined

Trey Darley
Thank you all for joining us – Let’s look forward to getting STIX & TAXII 2.1 Shipped
Then we can celebrate that!

Thanks to all!

Meeting Terminated

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

Appendix: Summary of TAXII Query Proposals

<table>
<thead>
<tr>
<th>Author</th>
<th>Title</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trey Darley</td>
<td>Possible TAXII 2.0 REST-based Query API</td>
<td><a href="https://docs.google.com/document/d/11wKWQaJB_8Mun_u4PakSK2XziT0RaNvmvmU8wuaFaQ/edit#heading=h.slj1uv7eu18b">https://docs.google.com/document/d/11wKWQaJB_8Mun_u4PakSK2XziT0RaNvmvmU8wuaFaQ/edit#heading=h.slj1uv7eu18b</a></td>
</tr>
<tr>
<td>Jason Keirstead &amp;</td>
<td>TAXII Information Request and Response</td>
<td><a href="https://docs.google.com/document/d/1Cy_9BhSkXEkDH5g2iv5c3AwiqVr7ygbbKXWOv4-uxbs/edit#heading=h.1jcqb6vc5y7z">https://docs.google.com/document/d/1Cy_9BhSkXEkDH5g2iv5c3AwiqVr7ygbbKXWOv4-uxbs/edit#heading=h.1jcqb6vc5y7z</a></td>
</tr>
<tr>
<td>Terry McDonald</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bret Jordan &amp; Gary Katz</td>
<td>A TAXII Search / Pivoting Proposal</td>
<td><a href="https://docs.google.com/document/d/1fquYYI-6d2eN-2MHoql_V88qNcq9TozVyyg4XFeY7as/edit#heading=h.xlss9yvcjfoy">https://docs.google.com/document/d/1fquYYI-6d2eN-2MHoql_V88qNcq9TozVyyg4XFeY7as/edit#heading=h.xlss9yvcjfoy</a></td>
</tr>
<tr>
<td>DHS / MITRE</td>
<td>Tiered Filtering Proposal (this idea has evolved over time)</td>
<td><a href="https://www.oasis-open.org/committees/document.php?document_id=66520&amp;wg_abbrev=cti">https://www.oasis-open.org/committees/document.php?document_id=66520&amp;wg_abbrev=cti</a></td>
</tr>
</tbody>
</table>