TAC-TC Monthly Meeting

Meeting Date: January 21, 2020
Time: 10:00 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>Arvidson, Mark</td>
<td>AT&amp;T</td>
<td>Member</td>
</tr>
<tr>
<td>Maroney, Patrick</td>
<td>AT&amp;T</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Thompson, Dean</td>
<td>Australia and New Zealand Banking Group</td>
<td>Member</td>
</tr>
<tr>
<td>Jordan, Bret</td>
<td>Broadcom</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Ginn, Jane</td>
<td>Cyber Threat Intelligence Network, Inc.</td>
<td>Secretary</td>
</tr>
<tr>
<td>Goel, Anuj</td>
<td>Cyware Labs</td>
<td>Member</td>
</tr>
<tr>
<td>Hohimer, Ryan</td>
<td>DarkLight, Inc.</td>
<td>Chair</td>
</tr>
<tr>
<td>Riley, Shawn</td>
<td>DarkLight, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>O’Brien, Christopher</td>
<td>EclecticIQ</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Patrick, Paul</td>
<td>FireEye, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Casey, Tim</td>
<td>Intel Corporation</td>
<td>Member</td>
</tr>
<tr>
<td>Applegate, Alex</td>
<td>LookingGlass</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Garcia Robles, Javier</td>
<td>LookingGlass</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Keith, Robert</td>
<td>Symantec Corp.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Girard, David</td>
<td>Trend Micro</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Jøsang, Audun</td>
<td>University of Oslow</td>
<td>Member</td>
</tr>
<tr>
<td>Mavroeidis, Vasileios</td>
<td>University of Oslow</td>
<td>Voting Member</td>
</tr>
</tbody>
</table>

Agenda:

- Welcome
  - Introductions
- Quick Review of Purpose & Scope
  - Clarification of the TAC-TC Scope
    - Why are we thinking about Threat Actor Context?
      - The value proposition – (better resiliency decisions & faster incident response)
    - The delivered work product – (a documented knowledge framework)
  - Progressing, Not Regressing (additive)
    - Threat Actor Characteristics
    - Semantic Interoperability
- Path Forward
  - Call for Proposals?
- Ambiguity Recognition & Resolution Discussion
  - STIX 2.1 Grouping
  - Industry Ambiguous Terms Discussion
    - Threat
Mitigation

Meeting Notes:
Ryan Hohimer

Welcome everyone! [Reviewed the Agenda]

Let’s review the Charter

Let’s also discuss whether or not we need Subcommittees

I’d also like to call for nominations for a Co-Chair

Review of the Charter

Our purpose is to resolve ambiguity in the context of TA across different sources and solutions, to support organizing what is known, and to share information about Threat Actors and the STIX Domain Objects (SDOs) related to them, such as Intrusion Sets, Campaigns, and Indicators. In this context “Threat Actor” can be, but not necessarily limited to an individual, an organization, a criminal syndicate, a nation-state or other type of adversarial entity.

To resolve ambiguity, we will establish a common knowledge framework that enables semantic interoperability of threat actor contextual information. We believe this may involve enhancements that run across the strategic, operational, and tactical intelligence levels for use by public and private sector entities defending networks and endpoints. The TC will establish one or more Open Repositories under the OASIS rules, and each OASIS Member and non-Member will be eligible to contribute only after signing either an Entity Contributor License Agreement (CLA) or an Individual CLA per OASIS rules at https://www.oasis-open.org/resources/open-repositories/faq.

The purpose of this TC is to create a knowledge framework that enables semantic interoperability of threat actor contextual information. In other words, the purpose of the TAC TC is to help the community have coherent conversations in the STIX language. (This does not exclude the possibility of TAC been used standalone or integrated also into other CTI standards or solutions)

The scope of this TC’s efforts will include:

• Hosting one or multiple OASIS Open Repositories of Threat Actor information in STIX 2.x format. The intent is to facilitate schema alignment.
  
  • Facilitating disparate contributors to submit contributions of Threat Actor information that is aligned with the repository schema is within the scope of this TC.
  
  • Mechanisms to allow for data marking and other associated metadata to describe the source of the contribution are considered within scope.

• Validation, confirmation, curation, or quality control of the contributors’ assertions into the repository is not within the scope of this TC.

• Defining and documenting concepts that provide best practices and guidelines to remove ambiguity from STIX documents produced by different authors (e.g. Intrusion Set naming conventions)

• Identify appropriate extensions that are needed to operationalize STIX 2.x threat information including but not limited to:
  
  • Strategic Context
  • Operational Context
  • Tactical Context
  • Motivational Context

• Providing algorithms to align schema is an aspirational activity of this TC.

The base data model for the TAC data store would stem from the STIX 2.x Threat Actor SDO, the Campaign SDO, the Intrusion Set SDO and the Indicator SDO (including patterning) at a minimum. This will provide a uniform interface for integration of schema and content from multiple credible sources.
Patrick Maroney

[Noted that the audience was hearing Ryan and in agreement with purpose and scope]

Ryan Hohimer

I am a Knowledge Engineer – I get to work with the subject matter experts (SMEs)

[Gave example of some of the frameworks]

Bret Jordan

There are many different frameworks [Gave example of Tim Casey’s work]

What is producible vs. What is consumable? – We need to work with
What is consumable for the general applicability of the audience

There is a delicate balance – we need to keep that in mind

Shawn Riley

We are driving towards a knowledge framework that humans can understand
Then we can get to the way machines can process the information

Bret Jordan

I agree, we just need to be aware of what vendors can really code to

Ryan Hohimer

With a knowledge framework it helps the humans comprehend the masses of data

Tim Casey

I understand what the caller (Bret Jordan) is saying – We ran into that problem too
Strategic intelligence is really new
We have an opportunity here to create a new tool – Will it be fully automatable?
Probably not – We need to create the databases – we need to get there
We are in the start-up phase – we need to prime the pump –
Counter what the adversaries are doing

Ryan Hohimer

So, why do this? Why Threat Actor Context?

The Scope: Resolve ambiguity via creation of a standard for expressing Threat Actor Context that facilitates semantic interoperability and enables human and AI analysis.

• Solution providers and government agencies are expressing Threat Actor Context today.
  • A de facto standard is not readily apparent. There is no consensus among solution providers.
• There are multiple good frameworks available from OASIS, NIST, DHS, NSA, ODNI, and others.
  • Making these disparate frameworks semantically interoperable is of high value.
• Transition to practice by validating via Open Repositories.
  • Validation of the contributors’ assertions into the repositories is NOT within scope.

Mark Arvidson

[In Chat: There are a number of standard information models covering many areas outlined here, such as TM Forum SID and DMTF CIM. Suggest looking at extending these as part of this effort.]

Ryan Hohimer

A lot of progress has been made – but, there is still some ambiguity

Different groups are modelling ‘threats’ in different ways – even with STIX
[Gave some examples of ‘Intrusion Set’ and ‘Grouping’]
Within the context of Object-Oriented Programming, open vocabularies are a start.

Jane Ginn

*Brought up the point about Strategic, Operational, Tactical approaches to Grouping*
Also, can see in Producing and Consuming threat intelligence

Bret Jordan

1. We need to create some Best Practices
2. We need to further flush out the STIX data objects
3. We need to document the various databases and frameworks that are out there

How do we as an industry do things in a similar way?

Tim Casey

Are you suggesting that we populate a sample database?

Bret Jordan

Yes. Made reference to the Thai CERT report [referred to as Indian]—Convert into STIX

*Gave some background on the early discussion*

Tim Casey

If I had to do it over again, even within our own organization, there are things
We could do differently
Use the current work, then fit into the current framework
Then look at a more MACRO picture—We need to start with concrete examples
Bret Jordan
   I agree – I just want to make sure we take this on in bite-sized chunks
Ryan Hohimer
   I agree – That is what this TC is all about
Jane Ginn
   [Pointed out that the report was from the THAI CERT] – I’ll put it up on the Wiki
   You all should have edit rights
Ryan Hohimer
   [Nominated Vasileios as Co-Chair]
   Asked for commentary on when to schedule Working Calls
   Asked Secretary to do a Doodle poll to find the best time for all attendees
Jane Ginn
   Asked Vasileios if he was willing and able – to make a statement to the group
Vasileios Mavroeidis
   Yes, I am willing to serve as Co-Chair
Jane Ginn
   Then, I second the nomination
Ryan Hohimer
   [Called for objections] [hearing none] Adopted by unanimous consent
   Quorum Achieved

<table>
<thead>
<tr>
<th>Meeting Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Quorum rule</strong></td>
</tr>
<tr>
<td>51% of voting members</td>
</tr>
<tr>
<td><strong>Achieved quorum</strong></td>
</tr>
<tr>
<td>yes</td>
</tr>
<tr>
<td><strong>Individual Attendance</strong></td>
</tr>
<tr>
<td>Contributing Members: 16 of 30 (53%)</td>
</tr>
<tr>
<td>Voting Members: 12 of 16 (75%)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Company Attendance</strong></td>
</tr>
<tr>
<td>Contributing Companies: 12 of 16 (75%)</td>
</tr>
<tr>
<td>Voting Companies: 10 of 11 (90%)</td>
</tr>
</tbody>
</table>

It is so moved, Vasileios Mavroeidis will serve as Co-Chair

Thanks everyone!

---

**Meeting Terminated**

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