TAC-TC Monthly Meeting

Meeting Date: September 23, 2022
Time: 10:00 AM US EDT
Purpose: TAC TC Full TC Meeting

Attendees:

<table>
<thead>
<tr>
<th>Name</th>
<th>Company</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thompson, Dean</td>
<td>Australia and New Zealand Banking Group</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Ginn, Jane</td>
<td>Cyber Threat Intelligence Network, Inc.</td>
<td>Secretary</td>
</tr>
<tr>
<td>Schifilliti, Francesco</td>
<td>Cyber Threat Intelligence Network, Inc.</td>
<td>Member</td>
</tr>
<tr>
<td>Casey, Tim</td>
<td>DarkLight, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Hohimer, Ryan</td>
<td>Darklight, Inc.</td>
<td>Co-Chair</td>
</tr>
<tr>
<td>Masuoka, Ryusuke</td>
<td>Fujitsu Limited</td>
<td>Observer</td>
</tr>
<tr>
<td>O’Brien, Chris</td>
<td>Google Inc.</td>
<td>Member</td>
</tr>
<tr>
<td>Mavroeidis, Vasileios</td>
<td>University of Oslo</td>
<td>Co-Chair</td>
</tr>
<tr>
<td>Zych, Mateusz</td>
<td>University of Oslo</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Mates, Jeffrey</td>
<td>US Department of Defense (DoD)</td>
<td>Observer</td>
</tr>
<tr>
<td>Ates, Keven</td>
<td>US Federal Bureau of Investigation</td>
<td>Member</td>
</tr>
</tbody>
</table>

Agenda:
- Review Work Ongoing
- Discussion of Updates to Ontology
- Review of TAL Refactoring
- Update on OCA – Indicators of Behavior Working Group Presentation

Meeting Notes:

Vasileios Mavroeidis

[Explained the reasons for the refactoring the TAC TC-Ontology]

At: https://github.com/oasis-open/tac-ontology

We need to normalize the namespaces to remove duplicates

The STIX2.1 SCOs and SCOs are formally subsumed in the TAC Ontology

We also need to update the documentation for the Ontology.

[Editors Note: Here are the links to the Starter Docs for the TAC TC Documentation – Request Links if needed]

TAC Ontology Architecture Specification:
https://docs.google.com/document/d/1ejdrBLzVrP-NgrZmHI9bN62EgishRlLlq2f90_h5d3s/edit#heading=h.105543clms0k

TAC Technical Specification
https://docs.google.com/document/d/1ky1CAUDKpn3RdzbCvYGudctwL5LGi2SMs_fTKdpQ8w/edit#heading=h.gidgxs

Jane Ginn
How will we handle Extensions in the TAC Ontology?
Vasileios Mavroeidis

The Extension Definition allows you to make changes, but schema needs to be Immutable –
When you are going to apply an ontology – Extension definition makes the Concept changeable – and that destroys the concept of a formal Definition
CTI TC has developed a formal framework for levels of adoption of Extensions
1. Ad Hoc
2. Maintainers look at Pull Request & Conformance
3. Candidate for inclusion

Jane Ginn

[Asked about where Incident Extension SDO was in this framework]

Jeffrey Mates

[Gave an update on where Incident SDO Extension is relative to this formal process]

Incident is at Level 3 and is cited in the CTI TC Proposed Best Practices

Vasileios Mavroeidis

[Also gave an update on another set of activities related to Course of Action SDO]
We sent an official Pull request to the CTI TC Common Objects Repository https://docs.google.com/document/d/1hSf8K5JGu7nuQ9eex6OB4FkIMsVcBVOi/edit#heading=h.gjd

COA is a Stub in STIX – We have created an extension for sharing Security Playbooks (e.g., for CACAO)
And we have a set of meta-data to use
We also want to have a mechanism for fuzzy hashing
We need an ability to check nearness to other playbooks

Jeffrey Mates

I do have some concerns about this – [Gave observations use of Deterministic IDs]

Vasileios Mavroeidis

The property incorporates the Playbook
We need to consider the CACOA – It has a mechanism for multiple ‘Signatures’
Please review the proposal when it comes out

Vasileios Mavroeidis

In Summary: To update the TAC Ontology, we normalize the namespaces
We hope to have in the next two weeks.
Documentation is being written too
We are developing a Style Guide
We need to develop the Threat Scenario concept to help implementors
Understand how to use the TAC Ontology
We want people to have a Toolkit for a reference architecture
We want a Knowledge Management System that is based on STIX as extended
We need to check all of the relationships – integrate 3 or 4 as examples Based on Web Standards
Tim Casey

[Gave an update on the refactoring of the Threat Agent Library]

Reverse look-up for the Threat Agents based on a set of characteristics
The inference engine uses the heuristics to correlate to the set of Characteristics
Process can be integrated into different tools
There are a lot of possibilities for implementations
We have to complete the mapping for the reverse look-up

Vasileios Mavroeidis

I’ll do my best to have the STIX 2.1 mapping updated within two weeks

***New Topic***

Gave an update on the work of the Open Cybersecurity Alliance (OCA)
It is focused on open-source tools for automation
Especially for threat intelligence and automation
Gave an update on the activities of Indicators of Behavior (IOB) group
We are trying to interconnect CACAO Security Playbooks
IOB asked Vasileios to present the TAC Ontology to them
They have published a STIX Extension for creating
Indicators of Behavior
Attack Patterns and Indicators that are seen (Sigma Rules)

On October 11 Vasileios will explain the TAC Ontology
Benefits of having STIX2.1 encoded into Web Standards
I hope to be able to have a Slide Deck & Documentation

Note: To Join the OCA Slack channel, please send an email to
Jane Ginn (jg@ctin.us) for an invitation. Once in that Slack channel
Join the #iob-wp Subchannel.
Chair of the Subchannel is: Charles Frick of JPL

Video of TAC TC Call:

Unlisted video. Only people with the link can view.

https://vimeo.com/sedonacyberlink/tac-sept2022

Meeting adjourned