TAC-TC Monthly Meeting

Meeting Date: March 22, 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>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>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>Hohimer, Ryan</td>
<td>DarkLight, Inc.</td>
<td>Chair</td>
</tr>
<tr>
<td>Mavroeidis, Vasileios</td>
<td>University of Oslo</td>
<td>Chair</td>
</tr>
<tr>
<td>Zych, Mateusz</td>
<td>University of Oslo</td>
<td>Voting Member</td>
</tr>
</tbody>
</table>

Agenda:
- Updates on TAC-TC Integration with OCA Work
  - Update on Work with DC3 Ontology on Forensics
- TAC-TC Projects
  - Presentation to CTI TC
  - Threat Scenario Modeling update
  - Incident Extension Integration into TAC Ontology

Meeting Notes:

Ryan Hohimer
Welcome everyone
Reviewed Agenda
Ryan Hohimer
Reviewed integration and work with OCA – Depending on TAC TC’s Ontology
OCA also wants to integrate with DC3 Ontology – focused on forensics
  Strong support by European community
  Ryan working with OCA on integration
CUBRC – Common Core Ontology

Ryan gave a presentation to the CTI TC on March 17th
STIX provides a well-founded dictionary – TAC TC extending
  Purpose: Represent CTI as Linked Open Data
  Available for mainstream queries – Like SPRQL

Patrick Maroney
Allows us to take advantage of many different communities
  Universities, think tanks, open source communities

Ryan Hohimer
Powerful TAXII server on steroids
  [Reviewed the presentation]
OASIS TAC-TC Monthly TC Call

Graphs from STIX are Simple to make

- Add a “@context” to the STIX 2.1 JSON (makes it JSON-LD)
- Convert it with COTS software (e.g. rdf-Toolkit, Protege)
- Knowledge Graph of the STIX 2.1 Report (SPARQL Endpoint)

Ryan Hohimer
Gave an update on the integration of the proposed Incident SDO into the TAC Ontology

Mateusz Zych
Some revisions to the model – will formalize with a Template
Everything is available on the Google Drive

Vasileios Mavroeidis
We have a clear vision – on what to write for new paper
We will explain how to augment STIX data and interlink with other sources
With regard to Threat Scenario – We will develop a Template for additions
Then, issue as a Committee Note

Ryan Hohimer
Noted that this was what TAC TC did for the Incident SDO Extension
Use that process for this Template and for the Threat Scenario
Vasileios Mavroeidis

We have the same for the Security Playbook which is an Extension of Course of Action SDO

Gave update on work that Johns Hopkins is sponsoring

Presented a new STIX SDO for Indicators of Behavior (IoB Group)

Describes behaviors of TTPs

They introduced a new object rather than an Extension

Vas invited them to the TAC TC

Ryan Hohimer

Also developing an ATT&CK Knowledge Graph using MITRE data

Before ‘Extensions’ formalized in STIX 2.1 – MITRE began using an X_

Used that as a way to provide a namespace to MITRE TTPs

From the MITRE ATT&CK STIX JSON

Would be analogous to TAL as an Extension

Patrick Maroney

Also noted the MISP Galaxy work in attack frameworks

https://github.com/MISP/misp-galaxy

Also mentioned the Model Driven (Magic Draw) model

https://models.modeldriven.org/models/ThreatRisk/Threat%20Risk%20Model.html

Jane Ginn

Asked if Patrick would do a MISP overview. Patrick agreed for April 1st.

Ryan Hohimer

Any other business? None. See you April 1st for Working Call

Recording of Meeting: https://vimeo.com/691067793 [Email jg@ctin.us for password]

Meeting adjourned