TAC-TC Monthly Meeting

Meeting Date: October 26, 2021
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>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:

- Gantt Chart (Roadmap Review)
- TAC-Ontology Status
  - Threat-Incident-extension Branch
- GitHub Open Repository Status
  - http://github.com/oasis-tcs/tac-ontology
  - tac-common-semantic-individuals
- TAC-TC Projects
  - Incident Extension
  - Threat Scenario
  - Resource Organization
  - Papers

Meeting Notes:

Ryan Hohimer
Revise Agenda
Reviewed schedule – Gantt Chart updates
  Asked for Jane to help with developing standard to supplement ontology
  Gave status on migration of existing TC-only GitHub content to the Open Repo
  Plan to have migration done by next week
Some discussion on how the TAC use of term ‘Extension’ differs from STIX use of term

**STIX Extension Definition and Semantic Extension Differ**

The TAC Ontology uses a formal ontological language (OWL) to represent concepts such as classes and properties. OWL has the syntax to create a subclass and sub-property. It is an inherent capability in the OWL language. Because of this capability it is straight forward (easy) to create extensions.

The Extension Definition provided in the STIX specification is not expressive enough to create these subsumptive relationships. It does allow the writer to add properties to existing objects (or create new objects) but the mechanism does not assert any relationships between the new class/property and the old.

New Semantic Extensions should be given their own namespaces during development. The new extensions will be in their own ontology files. These ontology files can be imported into the stix-semex ontology (stix-semex.owl).

- Some discussion of using Read the Docs tool that is integrated with GitHub
  For documentation on how to use the various Knowledge Bases
Vasileios Mavroeidis
OCA is using this to document their tools

Ryan Hohimer
Outlined some other projects he is working on

Publications and White Papers

- **Papers:**
  - On the Integration of Course of Action Playbooks into Shareable Cyber Threat Intelligence
  - Semantic Definition of Threat
- **White Papers:**
  - Reporting versus Modeling
- **Social Media Posts:**
  - STIX Extension Definition and OWL subclassOf

Ryan Hohimer
Discussed areas where we need support

---

**Meeting Adjourned**

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