TAC-TC Monthly Meeting

Meeting Date: February 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>Casey, Timothy</td>
<td>DarkLight, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Hohimer, Ryan</td>
<td>DarkLight, Inc.</td>
<td>Chair</td>
</tr>
<tr>
<td>Mavroeidis, Vasileos</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-Ontology Status
- GitHub Open Repository Status
- TAC-TC Projects
  - Threat Scenario (Mateusz)
  - Incident Extension (Ryan)
  - Knowledgebase (Ryan)

Meeting Notes:
Ryan Hohimer
Welcome everyone
Reviewed Agenda
Went over the revised Namespaces @ https://github.com/oasis-open/tac-ontology
- Stix
- Stix-semex
- Tac
Made it much more streamlined

Mat
We are developing the Threat Scenario Definition
Appendix D – NIST SP 800-61 Using for modeling exercise
We also have a new branch in the TAC Ontology

Ryan
Gave update of the work on the Knowledgebase – Using APT1 as an example
Knowledgebase Demonstration

- “Scooby Snack”
- Conversion
  - STIX JSON
  - STIX JSON-LD
  - (OWL) RDF/XML
- Linked Data
  - STIX Threat Intel

We want to create a dataset to demonstrate how this process works
We want a SPARQL endpoint so that we can demonstrate Queries

Ryan
Discussion of collaboration with CTI TC on the Incident SDO object.
Because it has started to solidify – we can now make the Semantic Extension of Incident

Recording of Meeting:
https://transcripts.gotomeeting.com/#/s/cf7e8cea209b1f54af8f2297d5d3ba8fc65690ec358e79a5c0974fd5f3937fe7

Meeting adjourned