TAC-TC Working Meeting

Meeting Date: March 5, 2021
Time: 11:00 AM US EST
Purpose: TAC TC March Working Meeting #1

Attendees:

<table>
<thead>
<tr>
<th>Name</th>
<th>Company</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aufderheide, Jeff</td>
<td>AT&amp;T</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Keith, Robert</td>
<td>Accenture</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Maroney, Patrick</td>
<td>AT&amp;T</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>Glasgow, Colton</td>
<td>DarkLight, Inc.</td>
<td>Member</td>
</tr>
<tr>
<td>Patrick, Paul</td>
<td>DarkLight, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Mavroeidis, Vasileios</td>
<td>University of Oslo</td>
<td>Chair</td>
</tr>
</tbody>
</table>

Agenda:
- Develop a Roadmap for TC Deliverables
- Rough draft from this meeting
- Identify some “shovelers”

Meeting Notes:

Potential Milestones along the Roadmap

- Charter Deliverables (as milestones)
- Usage Validation and Metrics
  - Membership Metrics
  - Contributor Metrics
  - Adoptions Metrics
- Publication & Presentation Goals
  - Papers/Journal Articles
  - Conference Presentations
  - Adopter Demos

Charter Milestones

- A formal ontological language representation that embraces the STIX 2.1 Standard
Additional types, vocabularies, taxonomies, and ontologies that extend the STIX 2.1 standard, such as:
- Threat Actor subtypes
- Motivation & Motive
- Industry Sectors
- Temporality

Committee Note on data store Design Specifications for Open Repositories

Instructions for Participation in TAC Open Repositories
- As Contributors
- As Consumers

Committee Note: Data Store Design Specifications for Open Repositories

- Hosting 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.

Three types of repositories are defined:
- Ontology Specification Repository
  - Formal Ontology Implementation
    - OWL Representation of the STIX 2.1 Specification
    - STIX Semantic Expression Ontology Documentation
  - OWL Representation of the TAC Ontology
    - TAC Ontology Documentation
  - Specification Documentation
    - TAC Ontology Specification Document
    - STIX Semantic Expression Ontology Document
- Research & Development Resource Library
  - Literature collections
  - Collaboration documents in progress
- Shared Cyber Threat Intelligence Repository
  - Potentially supported by a TAXII Server
  - Proof of concept SPARQL Endpoint
  - Open to Non-OASIS member contribution and access
Timeline 2021 - 2022

<table>
<thead>
<tr>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Ryan)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.a. (Ryan) [Draft]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>7.c. (Vas + Ryan + Paul) [Draft]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.a. (All)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Charter Review
2. Usage Validation and Metrics
   a. Membership Metrics
   b. Contributor Metrics
   c. Adoptions Metrics
3. Publication & Presentation Goals
   a. Papers/Journal Articles
   b. Conference Presentations
   c. Adopter Demos
4. STIX 2.1 Semantic Specification
   a. documentation
5. STIX 2.1 Semantic Extension
   a. documentation
6. Threat Actor Context Extension to STIX 2.1 Semantic Extension
   a. Documentation
7. Additional Extensions
   a. Threat Actor Subtypes
   b. Motivation & Motive
   c. Industry Sectors
   d. Temporality
8. Committee Note: Open Repository Specification
   a. Shared Cyber Threat Intelligence Repository
9. Open Repository Instructions
   a. For Contributors
   b. For Consumers

Meeting Adjourned
*******************************************************************************