TAC-TC Monthly Meeting

Meeting Date: May 25, 2021
Time: 10:00 AM US EDT
Purpose: TAC TC May Full TC Meeting

Attendees:

<table>
<thead>
<tr>
<th>Name</th>
<th>Company</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<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>Thompson, Dean</td>
<td>Australia and New Zealand Banking Group</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Campbell, Stephen</td>
<td>Cyber Threat Intelligence Network, Inc.</td>
<td>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>Glasgow, Colton</td>
<td>DarkLight, Inc.</td>
<td>Member</td>
</tr>
<tr>
<td>Hohimer, Ryan</td>
<td>DarkLight, Inc.</td>
<td>Chair</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>
<tr>
<td>Zych, Mateusz</td>
<td>University of Oslo</td>
<td>Member</td>
</tr>
</tbody>
</table>

Agenda:
- Review Schedule
- Discuss results of Working Session #1
- Discuss results of Working Session #2
- New Business

Meeting Notes:
Ryan Hohimer
Review of schedule
STIX Specification – will slip to end of May
Migration from STIX to a semantic graph – That will slip
We will give a new estimation of dates for these

Review of results of Working Session #1
Covered how what we worked on – Brainstormed outline for the Specification
Outline given below
[Invited members to comment on outline]

Table of Contents

Introduction 5
  IPR Policy 5
  Terminology 5
  Normative References 5
  Non-Normative References 5

Objectives 6
  Semantic Representations of Threat Intelligence 6
    The Reasoning Behind Semantic Representations 6
    Representing Known Threat Intelligence Facts 7
    Inferring New Facts from Known Facts 7
  Embracing STIX 7
    Representing STIX Specification as a Property Graph 7
    Representing STIX Property Graph as a Semantic Graph 7
  Development of a Threat Actor Context Ontology 7
    TAC as a STIX Semantic Graph Extension 7

STIX Specification Representation 7
  Common Datatype Representation 7

STIX Semantic Extension 8
  STIX Relationship Object (SRO) 8

Threat Actor Context Extension 8
  Defining Attributes 8

Ryan Hohimer
Went over what we covered in Working Session #2
Noted the previous work that needs to be done
Community has done a lot in this area (Vulnerability)
CSAF Common Vulnerability Reporting Framework (CVRF) Version 1.2
Committee Specification 01
13 September 2017

Specification URLs
This version:
http://docs.oasis-open.org/csaef/csaef-cvrf/v1.2/c01/csaef-cvrf-v1.2-c01.pdf (Authoritative)
http://docs.oasis-open.org/csaef/csaef-cvrf/v1.2/c01/csaef-cvrf-v1.2-c01.html
http://docs.oasis-open.org/csaef/csaef-cvrf/v1.2/c01/csaef-cvrf-v1.2-c01.docx

Previous version:
http://docs.oasis-open.org/csaef/csaef-cvrf/v1.2/cspv01/csaef-cvrf-v1.2-cspv01.pdf (Authoritative)
http://docs.oasis-open.org/csaef/csaef-cvrf/v1.2/cspv01/csaef-cvrf-v1.2-cspv01.html
http://docs.oasis-open.org/csaef/csaef-cvrf/v1.2/cspv01/csaef-cvrf-v1.2-cspv01.docx

Latest version:
http://docs.oasis-open.org/csaef/csaef-cvrf/v1.2/csaef-cvrf-v1.2.pdf (Authoritative)
http://docs.oasis-open.org/csaef/csaef-cvrf/v1.2/csaef-cvrf-v1.2.html
http://docs.oasis-open.org/csaef/csaef-cvrf/v1.2/csaef-cvrf-v1.2.docx

Jane Ginn
Noted that during Working Session #2 Vas had outlined the problem of using STIX 2.1 embedded references using external_ref property
Also noted that during that session Ryan had outlined the approach he has taken
[Further discussion on other ontologies to embed in the data object]

Ryan Hohimer
Presented how we use the tools ~ That gets to the Charter of this TC

Jane Ginn
I think we need to make sure we cover this work on Vulnerability in the Spec
Let’s flush that out during a Working Session.

Stephen Campbell
Are we handling the issue of misconfiguration of cloud instances? How?
Are we incorporating the CCEs?
[Some discussion on status]
Does anyone know the people within MITRE that are working on this?
Is it being kept up to date?

Paul Patrick
It is being updated, but within government it becomes a compliance issue under STIGS ~ as opposed to a configuration issue

Ryan Hohimer
That is a good thing to discuss in the next Working Session, too ~ let’s flush it out.
[No more new business]
Thanks everyone!

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