TAC-TC Monthly Meeting

Meeting Date: August 27, 2020
Time: 10:00 AM US EDT
Purpose: Monthly CTI 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>Aufderheide, Jeff</td>
<td>AT&amp;T</td>
<td>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>Member</td>
</tr>
<tr>
<td>Ginn, Jane</td>
<td>Cyber Threat Intelligence Network, Inc.</td>
<td>Member</td>
</tr>
<tr>
<td>Hohimer, Ryan</td>
<td>DarkLight, Inc.</td>
<td>Secretary</td>
</tr>
<tr>
<td>Patrick, Paul</td>
<td>DarkLight, Inc.</td>
<td>Chair</td>
</tr>
<tr>
<td>Applegate, Alex</td>
<td>LookingGlass</td>
<td>Member</td>
</tr>
<tr>
<td>Mavroeidis, Vasileios</td>
<td>University of Oslo</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Palmstrøm, Ulrik</td>
<td>University of Oslo</td>
<td>Chair</td>
</tr>
</tbody>
</table>

Agenda:

- Update on Ontologies in the Repository
- Steps Forward for ‘Inference’ with Vocabularies

Meeting Notes:
Ryan Hohimer

OASIS GitHub TAC-ONTOLOGY Repository Update

• Three TAC-TC Ontologies in the repository
  • STIX Specification Ontology
    • An OWL representation of the STIX 2.1 Specification
  • STIX Semantic Extension Ontology
    • Imports STIX Specification Ontology and adds owl:ObjectProperties
  • TAC Ontology
    • Imports the STIX Semantic Extension Ontology
    • Imports the Threat Agent Library Ontology

- stix-schema: Corrected the namespaces of stix-schema
- stix-spec: added STIXAbstractType class to core
- tac: changing threat_action_types to threat_actor_types and adding Threat...
Two open issues on GitHub

- There are two (2) open issues
  - Issue #7
    - COTS Reasoners not able to use custom datatype definitions
  - Issue #6
    - “Context” modules can cause logical inconsistencies as defined in specification `<module>-context.owl`

Closed issues on GitHub

- There are two (2) closed issues
  - Issue #3
    - COTS reasoners do not deal with our Vocabularies, and cause logical inconsistencies
  - Issue #4
    - `object_ref` and `object_refs` are not valid IRIs and must be corrected

Applied the Ontology to Valid STIX 2.1
Jane Ginn
Ryan mentioned Intrusion Sets as central to the Ontology very early – this illustrates that

Ryan
Groupings, Bundles and Intrusion Sets are central to the application of the Ontology
Ryan

Quite a few Embedded Objects in STIX 2.1 – especially the Cyber Observables
Developed a work-around within their software for the Embedded Objects

Embedded Relationships

- Object references are not handled with stix:Relationship objects.
- An “id” owl:DataProperty was added to stix-semex.owl to allow for the construction of an IRI (range of an owl:ObjectProperty). It is transient data to enable convert the _id to an IRI.

Example Implementation of conversion:

```
SPARQL Query:
PREFIX malware: <http://docs.oasis-open.org/cti/ns/stix/malware#>
PREFIX stixCore: <http://docs.oasis-open.org/cti/ns/stix/core#>
CONSTRUCT {
  ?iri stixCore:sample_refs ?sampleRef .
  ?iri malware:operating_system_ref ?osRef .
}
WHERE {
  BIND(iri([G([0][0]])])AS ?iri).
  ?iri stixCore:sample_refs_id ?id.
  ?iri malware:operating_system_ref_id ?osId.
  BIND(iri(CONCAT("http://docs.oasis-open.org/cti/ns/stix/core#", ?osId))AS ?osRef).
  BIND(iri([CONCAT("http://docs.oasis-open.org/cti/ns/stix/core#", ?osId))AS ?osRef].
}
```

Vasileios Mavroeidis
Can we get a copy of the Mandiant report?
Ryan Hohimer
I’m trying to think how to give this to you without the software
Paul Patrick
We had to validate the report – We can get the triple set to you
Vasileios Mavroeidis
I was wondering if there is a tool that the community can use
Paul Patrick
Summarized his research on how to make something available
  Mentioned Elevator
    ■ Some of you may remember R2RML –
    ■ I’ve been playing with RML – can ingest JSON and XML
Ryan Hohimer
We’ve been in touch with Jason Minnik – he is developing some tooling
Paul Patrick
We may have a basis to have an open source authoring tool – conversion technology
Ryan Hohimer
It is going to have to deal with the propagation of these
We need to get the momentum going in the TC
Jane, I have a question for you..
  Are we booked for a presentation for the Community Development Corner for the CTI-TC?
Jane Ginn
Based on the enthusiasm I’ve experienced I would say yes.
Ryan Hohimer

Do people on the TC believe that we are in a position to present?

Vasileios Mavroeidis

I think we should put it off until October... when we have some tooling & inference

[Discussion on this – decision to do a short demo in September, then push main presentation to October]

Ryan Hohimer

Is anyone opposed to that? [No opposition]

Vasileios Mavroeidis

One of the key things we need to do is develop Inference

We mapped many threat reports to the Intel Corporation TAL

We tried to develop ‘Inference’ from the reports to the TAL categories

We need to update and merge the various vocabularies

We can start with the TAL (also used in STIX 2.1) and the Motivation vocabulary

Some of the attributes are very difficult to populate, such as ‘Resources’

Gave example of difference between Government/Organization for ‘Resources’

We need to develop a nominal scale (Low/Medium/High)

I would like to have commonly agreed definitions

Gave example of what EU CERT uses to make point that we need to have

Common vocabularies

Let’s start with one vocabulary, then move on.

Ryan Hohimer

Gave example of ODNI Threat Life Cycle versus Lockheed Martin Kill Chain

Then juxtaposed TAL and CERT-EU

Is it possible to make different vocabularies ‘pluggable’ into the TAC ontology?

Vasileios Mavroeidis

For some of them – There are no definitions – For some they are not sophisticated
Paul Patrick
You’ve hit on something really important here...

Vasileios Mavroeidis
I’ve read about 50 threat reports in the past two weeks... gave examples of some of the Terms used that don’t coincide – Term like ‘jihadism’ is not defined

Paul Patrick
Broad categories – We need to have a tiering mechanism for those that understand The most ‘abstract’... used Ideology as example, then a tier below Jihadism

Vasileios Mavroeidis
I don’t want to make this more complex – in the next TC meeting I will have A first draft presentation with TALs – and Motivations
Plus more than a dozen from national CERTs
Gave example – No category that applies to ‘Cyber Criminal’ on TAL – only Mobster
Gave another example from TAL – No ‘financial gain’ only personal gain

Paul Patrick
Gave additional examples

Vasileios Mavroeidis
We need to also be able identify polymorphism – Gave example of the Lazarus Group Then, discussed how the queries have to be developed
We need to have robust definitions – then we can achieve
More expressivity and granular
Then we can facilitate Inference
Ryan Hohimer

It is a matter of creating the Object Model first – then getting the hierarchy defined
These groups tend to morph over time – there is a time element

Jeff Aufderheide

Asked a question about certain content – risk and outcome relationships
Is there a copy of the slide deck?

Ryan Hohimer

Initially we have focused on the Ontology for STIX 2.1 –
Once we get this built out we’ll move into some of those questions

Jane Ginn

I have embedded screenshots of the images into the minutes –
and I’ll give Jeff access via Google Docs

Ryan Hohimer

We’ll be back on the regular schedule for next month & give a short brief for CTI-TC
To generate enthusiasm for a more detailed presentation in October
First Thursday – Working call
Third Tuesday – Main TC call

[Editors Note: We maintain the back-up and working documents for this TC on a restricted shared folder on Google Docs; that is, restricted only to members of the TC. If you would like access to this shared folder, please send a request to either of the chairs or to Jane Ginn at: jg@ctin.us]

Meeting Terminated

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