TAC-TC Monthly Meeting

Meeting Date: June 3, 2022 (May Meeting Make-up)
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, Tim</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, 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:
- Review Roadmap
- Read-out of Automation Workshop

Meeting Notes:
Ryan Hohimer
- Roadmap – Accomplished several things in support of inputs to Automation Workshop
  - Ran into problem with Protégé Reasoners – failed with custom data types
  - Solution: remove the vocab.owl file from imported ontologies
  - Need to refactor the TAL Ontology – Will work with Tim on that
  - TAL needs to be translated into class equivalency expressions

Vasileios Mavroeidis
- You may be able to use the representation we prepared last year – It is here

Vasileios Mavroeidis
- Gave read-out of Automation Workshop
  - Revolved around the IACD Framework –
  - Our breakout session focused on sense making
  - Different presentations on OpenC2, CACAO, TAC.

Threat Actor Context Ontology

The University of Oslo presented the Threat Actor Context Ontology of the OASIS Threat Actor Context Technical Committee (TAC TC) in support of cybersecurity automation and, in particular, the sense-making and decision-making functions of cyberspace defense as they are described in the IACD framework.

The core model of the TAC ontology is based on the STIX 2.1 standard and further augments it with other representations that describe components from the domain of Cyber Threat Intelligence (CTI). For example, we presented the Threat Agent Library (developed by Tim Casey and Intel Corporation in 2007) that describes a threat actor type typology. We extended the ontology by encoding the TAL typology in Web Ontology Language (OWL). We demonstrated the reasoning capability of the ontology by automatically inferring the
types of a set of adversaries and their activities in near real-time (e.g., cybercriminals or nation-state-sponsored).

The following video provides an introduction to the TAC ontology and how it consumes STIX data to provide us with searchable, shareable, and interoperable knowledge graphs of CTI as linked open data.

TAC Ontology Video on Youtube: [https://www.youtube.com/watch?v=p5cF6ZmNaNI](https://www.youtube.com/watch?v=p5cF6ZmNaNI).

We further discussed how the TAC ontology could integrate with other open-source solutions (STIX shifter and Kestrel threat hunting language) and utilize open standards (OpenC2, CACAO, SBOM, VEX, CSAF) to address different cybersecurity automation use cases.

**CACAO Security Playbooks**

As an ad-hoc contribution, we briefed about the CACAO security playbooks "standard" and presented use cases on how CACAO can orchestrate and automate cyberspace defense, also by utilizing STIX and TAXII, OpenC2, Kestrel, and the TAC ontology. An emphasis was given in demonstrating how CACAO can utilize OpenC2 for command and control of cyber defense systems and components. Finally, we discussed and demonstrated how we can share (and couple with CTI) CACAO security playbooks using STIX 2.1. To achieve that we designed a STIX 2.1 property extension for the Course of Action object type. The STIX 2.1 "Extension" we demonstrated is available on GitHub. We provided for further reading a technical report that explains the STIX 2.1 extension we presented.

**Use Cases and Take Aways**

The participants showed high interest in the inference capabilities of the Threat Actor Context ontology to derive new understandings pertinent to CTI and support human intelligence analysis and decision making.

Another well-received aspect is the availability of a plethora of open source and closed source software that can consume the ontology and be used as knowledge management solutions.

Two tools from the Open Cybersecurity Alliance (OCA) were also demonstrated. These are summarized below.

**Kestrel**

*Presentation by Dr. Xiaokui Shu of IBM and Founder of the Kestrel Program*

Kestrel is a language for efficient cyber threat hunting. Kestrel provides a layer of abstraction to stop the repetition involved in cyberthreat hunting. It is an efficient cyberthreat hunting symbiosis between humans and machines to ask and answer different types of hunting questions: What to hunt, and How to hunt.
It uses building reusable, composable, and shareable huntflows across different data sources and threat intel. To quickly develop new interfaces for data sources and analytics, Kestrel abstracts the connection to data source and analytics with two layers: Kestrel runtime communicates with interfaces and the interfaces communicate with the data sources or analytics. Both data source and analytics interfaces can be quickly developed by creating a new Python package following the rules in Kestrel Data Source Interface and Kestrel Analytics Interface.

Resource links:
https://www.youtube.com/watch?v=pbJXGkb_BoY
https://www.youtube.com/watch?v=9llUoGpXvYo
STIX-Shifter

Presentation by Danny Elliot of IBM, one of the Maintainers of the STIX-Shifter tools.

- Based on STIX2.1
- JSON structure to exchange threat intelligence
- Open-source project – part of Open Cybersecurity Alliance (OCA)
- Python library that allows software to connect to and query data repositories
- Includes connectors for several security products.

Resource link:
https://www.youtube.com/watch?v=XC1c8nKiXgE
https://www.youtube.com/watch?v=aUiiZkmqVczQ&list=PLaYKtNo_BitYDj-uHhGNFiK2VAnU-4WHP&index=28

Common Security Advisory Framework (CSAF)

There was no representative in the breakout room; however, the earlier Forum discussion did cover CSAF topics. In addition, the mid-day Keynote speaker, Allan Friedman, outlined the purpose of VEX and its relationship to CSAF. Resource links given below.

The purpose of CSAF is to Standardize automated disclosure of cybersecurity vulnerability issues.

Resource Links:
http://www.cybersecurityautomationworkshop.org/Results/
https://www.youtube.com/watch?v=GiZ5VHrwM0A&list=PLaYKtNo_BitYDj-uHhGNFiK2VAnU-4WHP

Link to Video Recording of TAC TC Monthly Meeting: https://vimeo.com/716942585
PW: 2022

Meeting adjourned