TAC-TC Monthly Meeting

Meeting Date: February 18, 2020
Time: 10:00 AM US EST
Purpose: Monthly CTI 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>Jordan, Bret</td>
<td>Broadcom</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Keith, Robert</td>
<td>Broadcom</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Ginn, Jane</td>
<td>Cyber Threat Intelligence Network</td>
<td>Secretary</td>
</tr>
<tr>
<td>Hohimer, Ryan</td>
<td>DarkLight, Inc.</td>
<td>Chair</td>
</tr>
<tr>
<td>Riley, Shawn</td>
<td>DarkLight, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Patrick, Paul</td>
<td>FireEye, Inc.</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Casey, Tim</td>
<td>Intel Corporation</td>
<td>Observer</td>
</tr>
<tr>
<td>Girard, David</td>
<td>Trend Micro</td>
<td>Voting Member</td>
</tr>
<tr>
<td>Jøsang, Audun</td>
<td>University of Oslo</td>
<td>Member</td>
</tr>
<tr>
<td>Mavroeidis, Vasileios</td>
<td>University of Oslo</td>
<td>Chair</td>
</tr>
<tr>
<td>Palmstrøm, Ulrik</td>
<td>University of Oslo</td>
<td>Member</td>
</tr>
</tbody>
</table>

Agenda:

Ryan Hohimer
- Welcome
- Review Agenda
  - Welcome - call to order
  - Contextual Requirements Discussion
  - Call for Use Cases
  - Thai Cert Discussion
  - MITRE ATT&CK Discussion
  - STIX Grouping Discussion
  - New Business
Bret Jordan

Noted that the types of Threat Actor properties & labels that were used in CTI TC
Were too granular – Gave example of the need within Secret Service to have a less granular definition

- Criminals
- Hacktivists
- Spies

Ryan Hohimer

Possible to tie the elements together

Bret Jordan

The key point I was trying to make was about the ‘typing’

Shawn Riley

Noted that there are different hierarchies that are used in different contexts –
Cited https://slack-files.com/files-pri-safe/TN47CS0G3-FSJ70UTSS/2740_vollede_tekst_tcm28-273243.pdf?c=1582044711-906c4c702d2e0b2a5d26c1d568b4a3f97c305e6c

Audun Jøsang

With very broad categories, it may not work – Different groups track for different reasons
And, it depends on who the ‘attack’ comes from and who is the victim

Patrick Maroney

I posted the article that Shawn is referring to [Note: Shawn uploaded to Slack]

Ryan Hohimer

Let’s all share some Use Cases, then extract the representations, then we can find
The important things that we need to cover in this TC
Vasileios will cover the slides with his thoughts on the Thai CERT report

[NOTE: To be covered during the March Working Meeting]
ThaiCert Discussion

Considering these reports as a concrete example (Use Case), what can we glean from them?

We need to be able to map these different frameworks together
We need to be able tie together using a semantically interoperable framework
Noted the difference between prose and MRTI

Jane Ginn
Identity SDO helps us to link social media cyber observables

Patrick Maroney
That is why we included the CIQ in the original STIX framework
We do need to identify ways to map these data

Ryan Hohimer
Organization ontology is what Shawn Riley and I have used
That is an overlapping topic with what we need
https://www.w3.org/TR/vocab-org/

Patrick Maroney
We are mapping to MISP – in the most recent release, there is a mapping to ATT&CK
But, we still need the glue that this semantic framework can bring

Bret Jordan
If there is something we need to do within the CTI TC for STIX 2.2 – then we can put through
If we can show good Use Cases and a good design, we can petition STIX community
To adopt

Ryan Hohimer
Examine the sources that we are currently using – get the sources and some Use Cases
Let’s get it on the table so we can discuss
What are the requirements to express content?
Let’s address in the next working call

Bret Jordan
Let’s also figure out how to make some of these concepts go mainstream

Patrick Maroney
We will ultimately need to go to JSON LD – What is the appetite within the community

Bret Jordan
There has never been a good explanation as to why something is needed
Gave an example of some of his own ideas that he has pushed

Patrick Maroney
I’m not trying to re-litigate this discussion from 5 years ago... I just thought we could
Bring up

Ryan Hohimer
Shawn Riley and I have found that the STIX 2.1 Grouping object looks very
Promising to me – I can create links to materials – even those not in STIX 2.1
As expressed now in the Grouping object – Open Vocab

Bret Jordan
It was a request from MISP – but, they didn’t help design it
It is a great SDO for us to consider for that purpose

Ryan Hohimer
Grouping – a collection of facts that have

Jane Ginn
Use Grouping object with ACH methodology

Patrick Maroney
Look at that paper on my LinkedIn page... I cover that time-based
‘grouping’ challenge
Point-of-order – Leave of absence request

Jane Ginn
I will handle with update of Voting Rights

Ryan Hohimer
Call for new business

Jane Ginn
Reminder to log in to Kavi and register attendance

Ryan Hohimer
We’ll look forward to seeing you all 1st Thursday of the month
On the working call

Meeting Terminated
***************************************************************************