TAC-TC Kick-off Meeting

Meeting Date: November 22, 2019
Time: 1:00 PM US EDT
Purpose: Kick-off TC Meeting

Attendees:

<table>
<thead>
<tr>
<th>Name</th>
<th>Company</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radhakrishnan, Ashwin</td>
<td>Anomali</td>
<td>Member</td>
</tr>
<tr>
<td>Maroney, Patrick</td>
<td>AT&amp;T</td>
<td>Member</td>
</tr>
<tr>
<td>Arnold, Rob</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>Hohimer, Ryan</td>
<td>DarkLight, Inc.</td>
<td>TC Convener</td>
</tr>
<tr>
<td>Riley, Shawn</td>
<td>DarkLight, Inc.</td>
<td>Member</td>
</tr>
<tr>
<td>Abraham, Jörg</td>
<td>EclecticIQ</td>
<td>Member</td>
</tr>
<tr>
<td>Huey, Caitlin</td>
<td>EclecticIQ</td>
<td>Member</td>
</tr>
<tr>
<td>O'Brien, Christopher</td>
<td>EclecticIQ</td>
<td>Member</td>
</tr>
<tr>
<td>Patrick, Paul</td>
<td>FireEye, Inc.</td>
<td>Member</td>
</tr>
<tr>
<td>Applegate, Alex</td>
<td>LookingGlass</td>
<td>Member</td>
</tr>
<tr>
<td>Garcia Robles, Javier</td>
<td>LookingGlass</td>
<td>Member</td>
</tr>
<tr>
<td>Stewart, Justin</td>
<td>LookingGlass</td>
<td>Member</td>
</tr>
<tr>
<td>Thomson, Allan</td>
<td>LookingGlass</td>
<td>Member</td>
</tr>
<tr>
<td>Ensign, Chet</td>
<td>OASIS</td>
<td>OASIS Staff Contact</td>
</tr>
<tr>
<td>Jordan, Bret</td>
<td>Symantec Corp.</td>
<td>Member</td>
</tr>
<tr>
<td>Keith, Robert</td>
<td>Symantec Corp.</td>
<td>Member</td>
</tr>
<tr>
<td>Girard, David</td>
<td>Trend Micro</td>
<td>Member</td>
</tr>
<tr>
<td>Mavroeidis, Vasileios</td>
<td>University of Oslo</td>
<td>Member</td>
</tr>
</tbody>
</table>

Agenda:
1. Call to Order and Welcome
2. Volunteer for Note Taking
3. Roll Call
4. Nominations for Chair/Co-Chairs
5. Election of Chair or Co-Chairs
6. Welcome from OASIS Staff
7. Review of the TC Charter
8. Discussion of Contributed Work
9. Adoption of Standing Rules
10. Assignment of Other Responsibilities
11. Creation of Subcommittees
12. Confirmation of Ongoing Meeting Schedule
13. Any other business
Meeting Notes:
Chet Ensign

[Performed Role Call] Quorum Met

Meeting Statistics

<table>
<thead>
<tr>
<th>Quorum rule</th>
<th>51% of voting members</th>
</tr>
</thead>
<tbody>
<tr>
<td>Achieved quorum</td>
<td>yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Individual Attendance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observing Members: 2 of 3 (66%)</td>
</tr>
<tr>
<td>Contributing Members: 19 of 29 (65%)</td>
</tr>
<tr>
<td>Voting Members: 17 of 17 (100%) (used for quorum calculation)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Company Attendance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observing Companies: 2 of 2 (100%)</td>
</tr>
<tr>
<td>Contributing Companies: 11 of 14 (78%)</td>
</tr>
<tr>
<td>Voting Companies: 10 of 10 (100%)</td>
</tr>
</tbody>
</table>

[Noted that there had been 2 Nominations for TC Chair – Ryan Hohimer]
[Asked for other Nominations – Hearing None – Ryan Hohimer elected]

Ryan Hohimer

[Went through Agenda]

Purpose:
Our purpose is to resolve ambiguity by establishing a common knowledge framework that enables semantic interoperability of threat actor contextual information. We believe this will involve enhancements that run across the strategic, operational, and tactical intelligence levels.

Benefits:
Semantic interoperability is the ability of computer systems to exchange data unambiguously. This enables machine computable logic, inferencing, knowledge discovery, and data federation between information systems. We are defining terms about Threat Actors to provide semantic interoperability between the variety of systems. We’ll be enhancing the STIX 2.x capability to define and describe in more granular detail what we know about Threat Actors.

Noted Final Charter:
https://www.oasis-open.org/committees/tac/charter.php

Note Comment Resolution Log:
https://docs.google.com/spreadsheets/d/1UpeIqfFdTJTPdUnpXguQVI9W1FT6-mdkwBbdm8rX4/edit#gid=558300134

[Noted that we got several good comments on the Draft Charter and revisions made]

Alex Applegate

[Posed question about Tasks of Charter]
Are we going to be dealing with Centralized Repositories?
Are we going to be dealing with Conflicting Information?

Ryan Hohimer
By trying to establish a basis for expressivity I believe this it is within scope.
What do you all think?

Allan Thomson
I support your answer – STIX 2.1 tried to establish the parameters – if you have 2 different Vendors that interpret an SDO differently, this would be where we can resolve
Alex Applegate
[Noted that multiple different Vendors use different naming conventions]
We need to define the process for resolving the different naming conventions

Ryan Hohimer
[Confirmed that we need to allow different contributors that add to the full picture]

Rob Arnold
I’ll offer up the concept of Multiplicity of Truths – We tend to not do a good job
Of resolving that – How can we allow that to be captured?
There is not always not one single framework

Patrick Maroney
Can we add Dr. Sample’s work to References?
On attribution – I’ll put it in the Chat – I will put in the Documents Folder for TC
From Chat:
The application of Dr. Sample’s work on use of Cultural Markers to perform Adversary
Attribution, Motives, and objectives: https://www.marmaladebox.com/podcast/culture-and-
cybersecurity-char-sample/

Ryan Hohimer
Turned to slide on the various references contributed – Noted that we want to add to Wiki


Thanked Bret Jordan for guidance on how to proceed.

Chet Ensign – OASIS Community Steward
[Began to review to OASIS process]
TC Process rules created & maintained by OASIS BoD

Role of Community Steward
• Support activities of OASIS members
• Communicate procedures & best practices to members
• Represent interests of members to staff and BoD
• Improve tools & support for community
• Recommend improvements to the process itself
• TC Process is at https://www.oasis-open.org/policies-guidelines/tc-process
Standards Track work progress:

- Working draft
- Committee Specification Draft
- Committee Specification Public Review Draft
- Candidate OASIS Standard
- OASIS Standard
- Approved Errata

Non-Standards Track work progress:

- Working draft
- Optional Committee Note / Public Review Draft
- Committee Note

*Non-Standards Track Work Products are non-normative*

- White papers, adoption collateral, etc.
- Administrative documents (meeting minutes, etc.)
Meeting minutes must be sent to TC mailing list & must track attendance and motions approved/rejected
Content must be maintained on OASIS-provided systems

**Open Repository Overview**
- Optional program to support work of the TC
- Marries strengths of open source development with stable governance of standards development
  - Runs on GitHub
  - Independent of TC standards work
  - Operates under open source license chosen by TC
  - Non-OASIS/non-TC members can contribute; Maintainers can be selected from broad community
  - Each contributor must sign a CLA
- Open Repository Guidelines & Procedures is at [https://www.oasis-open.org/policies-guidelines/open-repositories](https://www.oasis-open.org/policies-guidelines/open-repositories)

**Resources Provided by OASIS**

**Chet Ensign**

**At TC Request**

- TC wiki
  - Publicly visible but only TC members may edit
- TC version control via Github or SVN
  - OASIS Open Repository via Github
- Open source project(s) hosted by TC
- Issues management via JIRA or Github
  - Where TC feels need for capability not provided by OASIS, contact TC Admin to discuss alternatives

**About Contributions:**
- TC members may contribute existing or new material to the TC for consideration in its work
- TC is under no obligation to do anything with it
- Contribution only gives OASIS non-exclusive right to use and republish.
  - Full rights remain with the contributor
Contributions covered by terms of TC’s chosen IPR mode
Process is simple:
  Load contribution to TC’s document repository
  Can’t contribute via links
  Send email to the TC mailing list announcing the contribution and including
      link to the uploaded file
  Generally done automatically when uploaded

| TC’s run by the rules of the OASIS Committee Process and TC Process |
| Members have full participation rights and can gain voting rights. |
| Observers only ‘observe’ |
| To gain voting rights, attend two consecutive TC meetings |
| If you don’t care about voting or affecting quorum, you can request to be made a Permanent Non-Voting Member |

Ryan Hohimer
  Brought up idea of a Doodle Poll for running our regular meetings
Jane Ginn
  Suggested that we set out time to accommodate members from Europe and US
      Middle of the Week and Early in the Day US EST Time
Patrick Maroney
  +1 on doing a Doodle Poll for setting up meetings
Ryan Hohimer
  We’ll send out to get your input on the cadence of regular meetings
Jane Ginn
  Do we want to have all meetings count towards Voting Rights? What frequency
Bret Jordan
  I think all meeting should count towards Voting Rights
      [More discussion – suggested more frequent meetings at the beginning]
Ryan Hohimer
  Maybe I can facilitate a meeting among those that want to participate to discuss and frame
      Discussions in December
Jane Ginn
  Maybe our Doodle Poll should be aimed at getting feedback from all beginning in 2020
Patrick Maroney
  Jane, where should I put the Reference?
Jane Ginn
  Until we get a Wiki set-up, I’ve been putting documents in the Documents/Admin folder
Ryan Hohimer
  Thanks all for coming!

Meeting Terminated
***************************************************************************
Postscript: Sent from Chet Ensign after termination of the meeting

Congratulations on getting the TC off to a successful start. Here are some pointers to resources that may be useful to you as you move your work forward.

- TC-specific resources

1) Your Charter
Your charter is the document that governs the work of your TC. In particular, it spells out what is in and out of scope and the essential objectives that you have set out to address.
https://www.oasis-open.org/committees/tac/charter.php

2) Your public and internal TC Home Page - the public page is the web page visitors to www.oasis-open.org see. The internal page is where you can manage your roster, start electronic ballots, store working documents, etc.
Public page: https://www.oasis-open.org/committees/tac/
Internal web page: https://www.oasis-open.org/apps/org/workgroup/tac/

3) Your TC email list and comment lists - the comment list is the only allowed channel for non-OASIS member comments to the TC. You must subscribe to the comment list explicitly by sending a blank email to tac-comment-subscribe@lists.oasis-open.org. We recommend that the Chair assign a member of the TC to explicitly be responsible for monitoring the comment list.
https://lists.oasis-open.org/archives/tac/
https://lists.oasis-open.org/archives/tac-comment/

4) TC chat room - you can use this chat room to support the running of your meetings.
http://webconf.soaphub.org/conf/room/tac

5) TC Document Repository - this is where you can store your meeting minutes, working drafts, etc.

Other facilities you can request include:

6) OASIS Open Repositories, providing the ability to launch one or more TC-affiliated open source projects. See https://www.oasis-open.org/resources/open-repositories

7) GitHub Repositories for TC's work, providing the ability to perform version control with GitHub for the TC. See https://www.oasis-open.org/resources/tcadmin/github-repositories-for-oasis-tc-members-chartered-work

General OASIS policies and guidelines

1) The OASIS TC Administration How-to Guide provides specifics on how the TC Process policies are put into practice. You can access it at https://www.oasis-open.org/resources/tcadmin/tc-process-how-to-guide-introduction

2) The OASIS Naming Directives document - This document spells out the rules governing filenames and URIs for Technical Committee Work Products.
https://docs.oasis-open.org/specGuidelines/ndr/namingDirectives.html

3) The OASIS Liaison Policy - this is the policy that governs relationships between OASIS and other
organizations and may be of interest if TC is considering submitting work to other organizations in the future.
https://www.oasis-open.org/policies-guidelines/liaison

4) Other OASIS policies and guidelines - the full list of OASIS policy and guidelines documents can be found at
https://www.oasis-open.org/policies-guidelines

See in particular the OASIS Technical Committee Process and Intellectual Property Rights policy documents - these are two of the primary documents that govern work at OASIS. The IPR documentation may be relevant if a TC member intends to contribute a particular work to the TC.
https://www.oasis-open.org/policies-guidelines/tc-process
https://www.oasis-open.org/policies-guidelines/ipr

Best practices and guidance from the OASIS Technical Advisory Board (TAB)

The OASIS TAB is a group of elected representatives from the membership preparing best practices documents to help TCs produce high-quality work under the OASIS procedures, including:

3) "OASIS Keyword Guidelines" - https://www.oasis-open.org/policies-guidelines/keyword-guidelines

Other sources of helpful information

1) Help with Kavi - on the main page of your internal TC web page you will find a link to the Kavi Group help manual. This link will take you directly to that page.

2) TC Admin support request forms - These are the tickets you use to request working draft templates, ballots, public reviews, etc. These forms formally create the tickets used by TC Admin to manage its work. TC Admin will not take requests for support for these routine activities by email. The forms can also be found under the Resources tab on the OASIS home page
https://www.oasis-open.org/resources/tc-admin-requests

3) The OASIS Library -- this is where approved Work Products (Committee Specification Drafts, etc.) of your TC will be published. The top level directory will be created when your first approved work product is ready.
https://docs.oasis-open.org/tac/

In addition to these, you can be set up to use the OASIS wiki, JIRA issues tracking tool, SVN version-control tool and web conferencing chat room. Let me know if and when you are interested in using any of these tools.