Architectural Reference Working Group

Meeting Minutes

1 July 2021

Attendees: **Russ Warren, Adam Montville, David Kemp, David Lemire, Bill Munyan, Mark Mastrangeli, Mitch Thomas, Forrest Hare, Mike Rosa**
Agenda:

Here is the agenda for our call Thursday.

(1) Andrew to review the Threat Intelligence Analyst use case for discussion and feedback

(2) Forrest to review work from our first ontology call Monday to level set those that did not make it; discuss any updates since then and continue the discussion on developing the ontology.

The start of our work has been posted here ---> https://drive.google.com/drive/folders/1Smvo0gpR-wPM-Ma2Xo-avWD9gYWuqdSI

Topic 1 – Review the Threat Intelligence Analyst use case

Andrew reviewed our updated use case where he added threat intelligence. Andrew has added Threat intelligence personas and their actions as well as identified threat intelligence solutions and how they are used in this use case. Andrew created a PULL request with this updated use case and asked for input from the group. Mitch suggested adding a 'glossary' up front, introducing the 4 personas and the products involved in the use case.

SOAR is the final input we need and is next to be added (personas and products).

Topic 2 – Ontology Workgroup

Forrest took the group though the first workgroup meeting spreadsheet. We discussed the current sets of terms, the approach we will be using to create the OCA ontology, a basic formal ontology, common core ontology and a tool we can use to look at the existing definitions (Protégé). He discussed OWL and RDF formats.

David Kemp has added the OpenC2 terminology to the spreadsheet. We need to add the SCAP terminology as well.

Our next Ontology workgroup call is scheduled for Weds, July 7. With the defined approach Forrest presented, the tools and existing ontology that we can leverage, and our use case and diagrams, we have a basis to start working on the OCA ontology.

We need to continue to evolve the current OCA ontology; rename to OCA ontology, align with OpenC2 and start tracking the needs to extend this ontology based on our use case.