Architectural Reference Working Group

Meeting Minutes

10 December 2020

Attendees: Mitch Thomas, Russ Warren, Stephen Wood, Doug Austin, Mark Mastrangeli, Bill Munyan, Adam Montvile

Agenda: Completing a 'version 1' of our architecture by the end of this year.

(1) Review and discuss the current diagrams
(2) Review and discuss the first draft of the architecture document
(3) Identify next steps

Mitch took us through the diagrams (forked initial-c4-diagrams). We discuss the Github pull requests. Mitch took us through the Pull requests, and we agreed with the content, so the Pull will be merged after our meeting. Component diagrams from the SCAP architecture are almost complete; one more iteration and review next meeting should give us a good picture for SCAP. Adam mentioned we should review these diagrams with the SCAP team to ensure alignment as a follow-on action.

Russ agreed to act as a focal point for any Pull requests that are done between meetings, so as to enable Pull requests to be done without a meeting for us to review them. We intend to use our bi-weekly meeting to review, discuss and approve the Pull requests as our main vehicle.

We discussed next steps, including a higher-level view to tie in the rest of the OCA components (including users). We also discussed use cases and Doug Austin has offered to help by drafting them. We discussed a possible synergy with the threat management component, as we are investigating its proposed ontology. A work item for us to follow up on is to look at the SACM ontology and define next steps to bring some of this work into the OpenDXL ontology project. Mark discussed the desire to change the OPENDXL ontology name (perhaps call it the OCA Ontology) so as to better align with OCA.

Adam created a glossary and started populating it with the SCAP work underway. This glossary will be an evolving document that we should add to as we progress.

We discuss the initial draft of the architecture document. It has been posted as a google doc for review, comments and input at https://drive.google.com/drive/folders/1L2yHqeSoLquVYCxaRc9N5VLGOk_HeSwi?usp=sharing.

Next step will be for all to review this document and mark it up in Google Documents. We will review and discuss the comments in our next call (mid-January). Follow on work items include defining the relationships and communications among the OCA projects (OpenDXL Ontology, STIX-Shifter, SCAP V2). The C4 diagrams activity can continue to iterate and we can add these projects and their components, eventually building our the OCA architecture (and replacing our current diagrams).