Architectural Reference Working Group

Meeting Minutes

28 January 2021

Attendees: Mitch Thomas, Russ Warren, Stephen Wood,, Bill Munyan, Adam Montville, Dee Schur, Jason Keistead, Lodrina Cherne, Ronald Conant, Forrest

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 and comments received
(3) Discuss next steps and focus areas for 2021

Topic 1 – Review and discuss the current diagrams

Mitch took us through the diagrams (forked initial-c4-diagrams, PART3 Branch). We discuss the Github pull requests. Mitch took us through the Pull request, and we agreed with the content, so the Pull will be merged after our meeting. This latest update added more text descriptions and started to align with OpenDXL Ontology and the current use case that is posted in our Github.

Four areas of interaction have been identified that need OCA member input and feedback.

- Provide feedback and input on the current diagrams, especially in the area of threat intelligence.
- Review the current terminology document posted in Github. Add relevant additional terms.
- Align SCAP with OpenDXL Ontology. There is not a current ontology for posture information. This is a key area for SCAP. We need to start working on OpenDXL Ontology and align with SCAP's current architecture and formats.
- Continue evolving the use case with the objective of including endpoints. Continue to evolve our current diagrams to cover the use case.

Topic 2 – Review and discuss the architecture document and initial feedback

We discussed 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.

The document is a first pass and we noted the need for the following:

- Indicate the audience for this document
- Indicate the goals of the document for the audience
- Provide more documentation on our intent and motivation for the architecture; point out what is different and why we feel this approach is better than the current approaches
- Provide more information on how our 3 projects fit into the architecture and clearly indicate their scope and role
- Document how OCA relates to other open standards/project work (SCAP, IACD, OpenC2,..)

Topic 3 – Discuss next steps and focus areas for 2021

Several actions were identified for areas we can focus on in 2021;

- Continue to evolve the C4 diagrams to encompass the larger picture (including the DXL ontology and STIXShifter scopes). The goal here would be to ensure we have an overall architecture that clearly shows how our projects will fit together and define the scope/role each project plays. We would evolve the diagrams as we go.
- Define the interactions across the components (ex threat or SIEM or SOAR); see our overall diagram here --> https://github.com/opencybersecurityalliance/documentation/blob/master/Architecture%20Documents/SACM_OCA_IACD.svg. Our objective here would be to focus on specific components and use cases to drill deeper into part of the over architecture to enable us to get to the ability to demonstrate interoperation.
- Define how the projects fit together. The goal here is to segment out part of the architecture and get into more details on how parts of the architecture fit together. We would evolve the document as we go. Here are two possible approaches to make progress in this area:

➔ Relate opendxl ontology with OpenC2 and SACM ontology and Jason Flood's findings ontology
➔ Relate STIXshifter to the SACM data collection component

We discussed a model where we can evolve via refining our diagrams, aligning and extending the use case so that we can show an end-to-end (endpoint to security apps like SIEM/SOAR) prototype to demonstrate how the OCA architecture would work. **We are looking for volunteers to help us evolve these items. If interested, please contact the architecture team via SLACK or send an email to oca-architecture-wg@lists.oasis-open-projects.org.**

Topic 4 – Discuss publishing our meeting recordings to the OCA YouTube channel

We discussed a proposal to publish our architecture meeting recording to the OCA YouTube channel. This would enable a broader distribution of the material, currently posted on our Github. We want to encourage more members to engage and will need our membership's expertise in order to be successful. Please encourage your company to get more involved in 2021 as we have a base set of assets in place that we can all work on together.