Architectural Reference Working Group

Meeting Minutes

11 February 2021

Attendees: Mitch Thomas, Russ Warren, Stephen Wood, Doug Austin, Bill Munyan, Adam Montvile, Duncan Sparrell, Chris Murphy, Roseann Guttierrez, Forrest Hare, Dee Shur

Agenda:

(1) Review and discuss the current diagrams
(2) Review and discuss the draft of the architecture document
(3) Discuss use case approach

We welcomed Chris Murphy, from Truestar, as a new member of the OCA. Chris worked at AlienVault and has a threat intelligence background.

Topic 1 – Review and discuss the current diagrams

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. The next step is to add people to the diagrams. This update combined the multiple draw.io files and presents these views via Tabs with a single draw.io file. This makes the navigation easier. This can be exported as html. Work is being done to make the navigation work properly. Tabs can be exported as svg files. More help is needed to evolve these diagrams. Threat intelligence expertise and configuration policy management systems are two areas we would like to focus and need some expertise. Please let us know (via the email list) if you and/or your colleagues can help us on this. The posture assessment system (SCAP V2) has been the focus. Question on assessment vs collection has come up. Dotted lines represent a process. One work item identified is that collection instructions need to be defined in the Ontology work. We discussed opening a Github issue for these types of items.

Duncan brought up the need to define swim lanes for the PGB, TSC, project teams and architecture teams.

Adam mentioned he reviewed these diagrams with the SCAP endpoint data collection group to ensure alignment as a follow-on action. Adam, Bill and Mitch will work with this group, which meets bi-weekly, to identify items that need to be opened and actioned by the OCA SCAP V2 Prototype Project team. There will be synergy between this group and the OCA Ontology team. We will need to keep in sync with the SCAP teams as they plan to continue In parallel with the OCA SCAP V2 project work. NIST is trying to define the plumbing for SCAP.

We discussed the architecture terminology document and what has been populated as the diagrams are being developed. This terminology document will be an evolving document that we should add to as we progress. We discussed the need to add people to the diagrams as a next step.

Topic 2 – Review and discuss the architecture document draft

We discuss the draft of the architecture document. It has been posted as a google doc for review, comments and input at https://drive.google.com/file/d/18dr4-8N7VWGdaf2mA-F4rTq0OLZu9XEB/view?usp=sharing

The first 2 sections have been updated (objectives and our approach sections). Please review and comment.

As part of the documentation, we will need to develop a high-level diagram to cover the OCA architecture. We currently have a diagram posted in the Github repository that needs to be updated (noted issues: missing security controls/devices, people/humans, mix of products and functional boxes).

We discussed the C4 diagrams and the configuration policy management system box (which was not in our OCA diagram posted in the Github). SCAP data collection group's word document had the concept of an application using the configuration policy management system. We discussed a draft high-level diagram and how to approach building it. Mitch proposed we use the C4 System Landscape Diagram template and is going to take a pass at this, using our current diagram as a start.

We need to continue to define roles and relationships between the OCA projects. Duncan would like to see the things you buy (firewalls, IDS, sandboxes, etc) in the diagrams. The diagrams need to show real networks and identify the devices and how they interact with the security products and components. Distinguish between what people do versus what the systems do. IACD gives a functional model that could be used as a model.

Topic 3 – Discuss the use case approach

We discussed the use cases posted in Github and next steps.
(https://github.com/MitchellJThomas/documentation/blob/c4-diagrams-cuarta-parte/Architecture%20Documents/Use%20Cases%20for%20Open%20Cybersecurity%20Alliance%20v1.pdf)

We will use the use case 1 as a start and map to the diagrams and documentation underway. This will scope our effort as well as enable us to better tie the architecture together, identify missing items and actions to be taken and result in something we can use to demonstrate what OCA is doing and its value. The use cases will be converted to linkable MD files (for better collaboration). Section headings in markdown can denote the linkage to the use cases.

We discussed adding issues in Github for the current list of open issues and where we need help.