Architectural Reference Working Group

Meeting Minutes

15 October 2020

Attendees: Adam Montville, David Lemire, Mitch Thomas, Russ Warren, Forrest Hare, Adam Montville, Jason Keirstead, Bill Munyan, Duncan Sparrell

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

Summary of Discussion: We will meet bi-weekly to complete a 'version 1' of the architecture. We will cover Open C2, IACD, Open DXL Ontology and STIX-Shifter.

The creation of a reference architecture for cybersecurity operations that brings together standards efforts would raise the awareness of OCA; showing a vendor neutral architecture that shows how to run cybersecurity operations that ties together key components (like threat management, incident response, data security, endpoint monitoring. Etc.). Showing the value of each of these 'peace parts' can interact together and provide value together. This would also establish a basis of how individual components could/should work together.

Today's silo'd approach is too complex and too expensive. The market has shown the need for an approach that would simplify how security systems should work together.

Our audience is OCA membership (show where they contribute and provide value-add). Our audience also is groups with other architectures and show how OCA can provide value to their efforts.

We could pick some example workflows and show how it would play out in an enterprise, given the OCA reference architecture. Start with SCAP V2 architecture (policy, vulnerabilities), tie that to threat detection (IECD) workflow and incident response(automation), with OpenDXL Ontology (OCA) used as the transport. Defined diagrams and workflows are the deliverables we should strive for. We should focus on a couple of workflows, as examples. Adam has offered to share the workflows (CIS 7.1 controls) as a starting example. We could use this to show how the architecture supports the value of the architecture. We can also evolve the diagram in parallel.

It was suggested we look at the C4 Model (c4model.com) as a way to document(visualize) the architecture diagram. This would provide levels of details/layers of audience diagrams as artifacts. The context is the larger system with projects (ex. mitigating risk) and containers would represent the projects (STIX-Shifter, SCAP V2, OpenDXL Ontology). Adam likes this approach and is interested in trying this approach out.

We will create a new folder on Github to contain our work. We have our current diagram posted there. It needs to be updated for SACM/SCAP content. Names were taken from IACD architecture (red boxes). These represent functions (not unique software). SOAR is decision makes, SIEM is sense making system in IACD terms. SIEM should probably be removed from the box. Function perspective is one view we need. Another view should show a solution view(implementation). Make this diagram a functional architecture (eliminate products) and update to the latest SCAP level were identified as good next step for our diagram. JK has

volunteered to do these updates. We will also need to create a terminology/reference document. JK will also create a working version of a glossary.

We will set up bi-weekly calls and have agreed to have these calls at a fixed time. Russ will set up these calls for the next 2 months. This will reserve calendars and make it easier for people to attend. We discussed Github and extending it to use workflows and projects.

We should circulate the updated diagram to the other workgroups to communicate across the OCA teams. We should also share our work outside of OCA (other open groups).