Architectural Reference Working Group

Meeting Minutes

24 June 2020

Attendees: Adam Montville, David Lemire, Russ Warren,
Forrest Hare, Stephen Wood, Jason Keirstead, Michael Herring, Jory Burson

Agenda: Discuss the current architecture drawing from Jason

Summary of Discussion:

Topic 1: Architecture drawing discussion

Current drawing aligns OCA with SACM and IACD. The arrows represent possible OpenDXL Ontology efforts. Adam mentioned that SACM has some of the arrows (SCAP format which defines data format and functions, using the OVAL approach). Adam will review our architecture picture with the SCAP team to get feedback. Our goal is to align with SACM and IACD, with OCA providing the interoperability layer.

Forest discussed IACD, along with Michael Herring and where it would fit. IACD is focused on the orchestration layer and it would communicate with the security message fabric layer. SOARS are doing direct communications today but many were built before a message fabric existed. There is an opportunity to align SOAR and orchestration and playback works with a message fabric. We discussed AI and how it could make use of sense and sense making functions. These calls help AI obtain more information before taking actions and could leverage the fabric. The fabric would facilitate the enrichment of the information. AI help bypass the collaboration phase. JK is going to update the drawing to include this flow. The picture also needs to add query and response arrows to the Decision Making box.

JK will distribute the picture via Email to enable feedback from these groups. Adam will share this with the SACM group; Michael and Forest to share this with the IACD group.

We discussed how the OCA, IACD and SACM related. We did not see any conflicts at this point. SACM is focused on collecting telemetry, storing and reporting this information. IACD is focused on SOAR (threat response lifecycle) and OCA is focused on the interoperability and communication between components.

We discussed the need to different representation of the reference architecture. We will need one for outward facing audiences. We discussed that use case based pictures would be very helpful. As we complete the detailed reference architecture picture and obtain the feedbacks, we will need to work on these types of diagrams as a next step.