Architectural Reference Working Group

Meeting Minutes

15 July 2021

Attendees: **Russ Warren, Adam Montville, David Kemp, David Lemire, Mark Mastrangeli, Forrest Hare, Mike Rosa, Andrew Beard**

Agenda:

Here is the agenda for our call Thursday.

(1) Forrest to discuss **New DoD Zero Trust Architecture Plan**
(2) Andrew to review the Threat Intelligence Analyst use case for discussion and feedback
(3) Bill/Adam to discuss SCAP/SACM project
(4) Dave/Russ to discuss OPENC2 and OCA ontology
(5) Forrest to continue work on ontology
The start of our work has been posted here --->
https://drive.google.com/drive/folders/1Smvo0gpR-wPM-Ma2Xo-avWD9gYWuqdSI

Topic 1- DoD Zero Trust Architecture Document

Forrest provided an overview of the DOD Zero Trust Reference Architecture, issued by the US Dept of Defense and the US National Security Agency (2/21). Forrest provided this as a reference for the group. We can also leverage some of the defined terms and models for our OCA ontology work. We discussed that we should ensure OCA projects and architecuture should be able to operate within a Zero Trust architecture. A good high-level picture of this architecture is on Page 12 (OV-1).

Topic 2 – Review the Threat Intelligence Analyst use case

Andrew reviewed our updated use case where he added threat intelligence. Andrew has added a glossary up front, as requested in our last call. Andrew will submit the Pull request so we Can merge in his updates. We can now update the use case to align with the personas identified. SOAR is the final input we need and is next to be added (personas and products).

Topic 3 – SACM/SCAP project

Adam took us through the approach being taken around SCAP/SACM. As the SCAP V2 effort has wound down (NIST has prioritized payloads as top priority), the endpoint data collection effort has been working with the IETF SACM workgroup. CIS and Mike Rosa’s team want to proceed with the effort. Bill and Adam have defined a new project called Posture Attribute Collection and Evaluation (PACE). The team is working on defining the scope and owner for this work and have started to define an OCA Github project to contain this work. This project will carry forward the efforts on the endpoint data collection.

David Kemp has added the OpenC2 terminology to the spreadsheet. We need to add the SCAP terminology as well.

Topic 4 – OpenC2 and OpenDXL Ontology

Russ and David Kemp reviewed the discussion on focusing the OCA efforts to define messages, data content and responses rather than use the OCA OpenDXL ontology project as there seemed to be overlap between these projects. We discuss 2 issues previously identified in the OpenDXL Ontology project regarding the usage of OpenC2. David Lemire provided some updates to address those issues:

- "*Supporting one action to many responses requires that OpenDXL Ontology actions be more generic than their OpenC2 counterparts.*" I'd assert that OpenC2 supports this. An OpenC2 request that doesn't internally specify an actuator type ("profile") could be received and acted on by OpenC2 Consumers hosting a variety of actuator profiles that support the action / target pair specified in the request. So I think the desired generality is available.
- "*The OpenDXL Ontology also supports the concept of "notification" messages. ... OpenC2 does not currently have an equivalent concept.*"There actually is a notification concept in OpenC2, but it hasn't been further specified due to a dearth of use cases. While it doesn't show up in the currently published specification, it is captured in the in-development content for the next version of the specification (follow this link, and scroll down to the table labeled "**Type: OpenC2-Content (Choice)**". We'd been holding back on defining the notification message type because there was concern over lapping over into the security alerting space, but given some clear use cases this should be a pretty easy add to the current spec.

David Lemire took us though his assessment of the SACM and OpenC2 projects and how SACM could leverage OpenC2 (over OpenDXL) for its commands and data flows. A Posture Collection Actuator would need to be defined and an Actuator profile added in OpenC2. All this work seems feasible and fits well within OpenC2. The group felt this assessment was valuable and could serve as a basis for the SACM prototype effort (replace the SCAP V2 Mitre based approach).

Topic 5 - Ontology

Forrest clarified the scope of this effort and will follow an iterative process; based on our use case and architecture. This effort will enable OCA to enhance the value of the data customers already have by providing common semantic meaning across disparate data.