Architectural Reference Working Group

Meeting Minutes

17 June 2020

Attendees: Adam Montville, David Lemire, Michael Stair, Russ Warren, Forrest Hare, Stephen Wood, Jason Keirstead, Michael Herring, Jory Burson, Joe Brule, Duncan Sparrell, David Camp

Agenda: Discuss the current architecture drawing from Jason and Adam (covers SCAP mapped to OCA); Discuss OpenC2 and OpenDXL ontology and current status on alignment
Summary of Discussion:

Topic 1: Architecture drawing discussion

Adam reviewed the SACM (IETF) model and how SCAP 2,0 aligned with it. The drawing reflects collecting state from resources, evaluating them against a known good or expected result. SCAP focuses on providing a posture evaluation/assessment from the information collected. OCA has a larger focus (taking actions) so SCAP would be a part of the overall OCA architecture.

Jason discuss his overlay of the OCA projects on top of Adams diagram. The SD Fabric represents the federation of security data (query/response). The Integration service represents the Open DXL ontology. Discussion on how these two services should be a single component with these two interfaces. Jason will follow up with an updated diagram to re-represent these services. Jason added the Positive Attribute Repository to capture asset information. Discuss also covered the boxes (some services, some products) and the arrows and identified the inconsistency and need for similar entities be represented vs mixed.

Discuss on our goals for the architecture were to interoperate with SACM and IACD so the architecture picture for OCA should align with theirs. Jason was going to overlap the IACD architecture on our current drawing so as to capture this goal. There is a desire for our drawing to reflect, via the arrows, all the interfaces between components and this would define our work efforts for Open DXL ontology, STIX, and SCAP and OpenC2. The desire is to cover all the arrows with current existing work as well as define new work items to cover the rest.

Topic 2: Open C2 and Open DXL ontology

David Lemire prepared a set of charts to cover the scope of Open C2 and take a look at how Open DXL currently positions with it. Open c2 has 3 focus areas: a language, an accentuator profile and implementations. Open C2 is focused on acting/response. This is positioned as the acting phase of IEC (OODA loop). Open C2 used JSON for its definitions. Open DCL ontology is a messaging fabric containing actions and notifications. Open DXL ontology expects to support other open standards and there has been an Open C2 messaging over Open DXL prototype built.

The discussion was that Open C2 and Open DXL ontology overlap and we should request and effort from our TSC to

- Ensure that our objective is to align Open DXL ontology with Open C2 (to clearly state this as a goal and ensure we have actions in place to keep the alignment current)
- Examine the action defined by Open DXL ontology and Open C2, identify the overlaps or gaps (David pointed out two actions that seem to be the same that could be aligned: Deny vs Block/Blacklist and Contain vs Quarantine).
- Ensure the schema being used for Open DXL ontology and Open C2 are current. Discussion surfaced 2 needs
    - Open C2 currently does not have an approved schema; this is being worked on
    - Open DXL ontology has an older version of the schema.

Our actions identified:

- Meet next week to discuss and review the modified architecture drawing. JK took the action to modify the drawing and make available by Wednesday this week.
- An action was identified to ask the TSC to look into the Open C2/ Open DXL ontology areas identified above and come back with recommendations