Architectural Reference Working Group

Meeting Minutes

26 August 2021

Attendees: **Russ Warren, Mark Mastrangeli, David Kemp, David Lemire, Ian Featherstone, Dee Schur, Andrew Beard, Adam Montville, Dennie Moreau**
Agenda:

Here is the agenda for our call Thursday.
Topic 1 - Discuss the level set email I sent out last week:

(1) Level set our architecture based on: (a) Change of SCAP project - new PACE project (b) Leverage OpenC2 versus developing the OpenDXL ontology project (suggest we sunset this project)
(2) Define a reference architecture prototype which we can build towards to demonstrate and show the OCA reference architecture in action
(a) Using our Malware detection and response use case to scope the effort, and the new SCAP/PACE project as a basis (I think this new project will use OpenC2, we need to add in STIXSHifter),
identify and define the needed flows, data formats, commands and events via OpenC2.
(b) define the OCA formal ontology (Ian/Forrest leading)
(c) identify technology that can implement parts of the OCA reference architecture (ie. endpoint, email, SOAR, SIEM, threat intelligence) and develop plans for a prototype to support the OCA reference architecture prototype project
(d) identify other items that need to be addressed in order to achieve a prototype of t he OCA architecture (ex. define communications architecture and protocols)
(3) Refresh the architecture paper to (a) align with the new SCAP and OpenC2 focus and (b) factor in the New DoD Zero Trust Architecture Plan
(4) Define the OCA reference architecture prototype project (scope, timelines, etc)

Topic 2- The OCA ontology work - Ian Featherstone will be leading. The start of our work has been posted here ---> https://drive.google.com/drive/folders/1Smvo0gpR-wPM-Ma2Xo-avWD9gYWuqdSI

IAN will drive the OCA ontology work . He will look at the use cases, diagrams, and terms we have defined so far. He will review this material, load up some ontologies we can use and start leading our group in defining the OCA ontology.

Topic 1 Discussion

Dennis Moreau from VMware joined us for the first time. He introduced himself to the group.

We discussed where we are in the architecture group thus far. We discuss the email that lays out next steps and what we want to accomplish next. We discussed the new PACE project which replaces the SCAP V2 prototype project (as the NIST funding has ended). PACE is looking to leverage OpenC2. We are at a point to start defining common commands/actions and events, so

we discussed looking at OpenC2 versus going down the OpenDXL ontology project path (to eliminate redundancy and focus on projects that have traction and activities).

We discussed the documentation of the architecture. We discussed DODF / TOGAF (formal architecture definition). We have been using C4diagram tool to define the architecture. Concepts to capture are activities, interfaces (info exchange requirements between nodes). Set of nodes, set of activities each node performs and interchanges between nodes are common things to document. We need to determine if our approach using C4 is adequate or if we need to adopt another tool for the architecture documentation. I will work with Dave Kemp and Dave Lemire to determine what is needed here (or perhaps we need to work our current diagram some more (ex SOAR needs to be broken down ex Orchestrator).

We must have an implementable architecture and can be implemented into a product for our architecture to be considered a success.

We discussed the new PACE project. Dave (PACE) posture attribute collection and evaluation named by Bill and Adam. Dave Lemire reviewed the SACM architecture for ad hoc collection diagram to show the data flow. Dave added a diagram that shows the flows between components and mapped them to OpenC2. Notification message formats have not yet been developed in OpenC2 but are placeholders. NSA has an OIF orchestrator (open source) and It is mapped to the SACM components (manager and orchestrator). Posture collection is an OpenC2 actuator. Profile would need to be defined (may be one or several actuators). Dave presentation defined next steps and actions to map SACM to the OpenC2 actions and targets. We would like to do a similar exercise with our current OCA architecture. Russ will work with Dave to see if we can create a similar set of charts for our OCA material. This would map what we need to do to enrich OpenC2 to achieve our malware detection and response use case.

One of the goals of our efforts is to arrive at the ability to implement the OCA architecture. We will need product groups help to identify products and how they fit into the OCA architecture. We would want to products to use the OCA projects (STIXShifter, OpenC2 and PACE), where it makes sense. We may need mappers (to go from today's APIs and data formats) to enable the connection of current technologies to the OCA reference architecture.

We will discuss the US government DOD Zero Trust Framework paper and determine how it affects the OCA projects and OCE reference architecture. We need to identify any technology requirements from this paper and align our projects with these requirements.

Topic 2- The OCA ontology work

Ian Featherstone will be leading this effort going forward. Ian has reviewed our current documentation and model that Forrest started. We want to expand this work and make progress on the malware detection and response use case. Ian will set up a bi-weekly meeting to focus on the ontology work. We will need SMEs to help with the progress of this work. Ian will poll the group to identify folks that will continue to work on this.