Architectural Reference Working Group

Meeting Minutes

21 June 2021

Attendees: Russ Warren, Adam Montville, David Kemp, David Lemire, Bill Munyan, Mudit Tyagi, Mark Mastrangeli, Mitch Thomas, Forrest Hare

Agenda:

Here is the agenda for our call Thursday.

1- SCAP diagram updates to tie to the existing use case review
2- Review TIP use case
3- Mark and Forrest to discuss the ontology and how to start the workgroup

Topic 1 – SCAP diagram

We discussed the linkage of the scanners (email and file scanners) with the SCAP PCS system (Posture Connection System). Perform Posture Collection and Publish Posture Attribute Collection are 2 actions identified that need to be part of the OCA ontology.

We also discussed the connections between the SOAR, SIEM and Threat Intelligence systems with the SCAP Posture Assessment systems. SOAR will be an orchestrator and will send Orchestrate Posture Collection and Orchestrate Posture Assessment action that will be needed in our OCA ontology. The SIEM system could query the PCS and PAS systems to get context on the posture of system(s) and we will need a Collect Posture Attribute Action and Assess Endpoint Posture Action actions in our OCA ontology.

The SCAP system goes provide events that can be obtained from other systems (like a SIEM).
A status topic is defined in SCAP to subscribe to system events.

We noted that there are ambiguities in what a SIEM, SOAR and endpoint product provide in terms of capabilities. We may want to note that in our diagrams to be clearer on the interactions between security components. One possibility is to focus on the user (ex SOC Analyst).

Topic 2 – Ontology Workgroup

We need to get this workgroup started! We have a base use case and diagrams to show the interactions between them. We want to also align OpenC2 and the OCA ontology. Forrest took us through an approach. Ontology will create a formal representation of our diagram in a machine-readable format. We have a use case (malware detection) and a user (Bob) that we can use to define the instance level data model. We would start simple with the OCA ontology, leverage other relevant ontologies, and evolve it.

Mark wants to define the upfront design rules for the ontology. A general representation, versus use case based, can be defined. The use case based shows the ontology in action. Use case models will have real data behind it. We would also use the use case description written up and posted in our Github.

We can start up the discussion in July at this work group. Forrest set up a call for Monday 3-5 EST 6/28 to start this discussion (Monday 3-5 EST 6/28) with interested parties.

Ontology would define the Actions, OpenC2 would implement as structures. We will define the terms during the oncology work and tie it to other efforts (ex OpenC2). We discussed the OpenC2 data structure (posted in our Github). Open C2 has a list of verbs/actions. Allow and Deny are two such actions. Mapping current OCA ontology to Open C2: Quarantine is Contain, Block is Deny. We need to align the current OpenC2 with Ontology. Mark is working to find a developer to do this work (not extending it, just aligning it).

We will come up with new actions, we will need to rev the OpenC2 specification along with the OCA ontology. SCAP would be an example of what we will need to add, (Query Assessment). Profiles will need to be written to define the Query command. The IETF specification would be used by the SCAP project.

We will need to define topics for our ontology. This would define the queues to post and listen to.