Architectural Reference Working Group

Meeting Minutes

6 May 2021

Attendees: Russ Warren, Adam Montville, Forrest Hare, Dee Shur, David Kemp, Mark Mastrangeli, Andrew Beard, Bill Munyan, Chris Murphy, David Lemire

Agenda:

Here is the agenda for our call Thursday.
(1) Discuss Rev 3 architecture paper - adding our use case as a demonstration of the OCA architecture in action

Topics:
- Review Diagrams - Discuss new input/comments; review the new diagrams
- Next steps - SOAR and Threat Intelligence - need diagrams and data flows identified for use case 1
- Need OCA overview architecture diagram updates
- Open discussion/ other items

Topic 1 – Review current document (Rev 3) – Call for review and feedback

Top level pictures have been added (we still need to update the overview diagrams that is over a year old and posted in Github). Please review and comment on this document so we can wrap up this version (for a 'Release 1' of the OCA architecture). The intention is then to share this out and make it visible so OCA members and non-OCA members can get an update of OCA. It would also be great to build a prototype to show the OCA architecture in action.

Andrew is looking at the Threat Intelligence Platform (TIP) side. He sees it as a repository and responding to queries. SOAR will listen to things and take actions. SOAR will drive orchestration to remediate. Andrew is looking to input/outputs to the TIP. For example, sandbox sends malware information to the TIP for the malware use case. OpenC2 actions could be Query or Report, targets could be a hash or file. What about threat actors? Perhaps STIX could be used here. How do we describe what we want to query? OpenC2 has some ways to represent the data flows but more will be needed (for deeper queries). Some type of command structure will be needed. STIXShifter could help. The connector maps from native API to STIX2 formats (and in the reverse direction).

Forrest shared some slides on ontology. He discussed the process template (slides have been posted in our Github). You can model response options or attacks (ex. IOBs). The ontology can define these processes (generic process) versus an instance.

David discussed OpenC2 intention (define a few nouns); majority of content is in actuator profiles that define the specific content. Not much richness is in the base of Openc2; details are meant to be in the profiles.

We have OpenC2 and the STIX format, over the common message bus. David shared some slides that parse out the OpenC2 data format and how the OpenC2 commands and actuators are related. The diagram has been posted to our Github. David went through the data format of an OpenC2 content. Message can fit in OpenDXL protocol or MQTT format. Protocol and payload comprise an OpenC2 content. The ontology covers verbs and nouns. The TIP services can be defined via the ontology.   We can create adapters for the ontology.

We discuss SOAR and SCAP/posture assessment. SCAP could be one of the triggers for SOAR to take action on. SCAP V1 has the content model and serialization. The posture assessment may result in requirements for remediation actions. The SOAR could be a target for this. There could be workflows to support posture assessments from SCAP. SCAP V2 provides continuous monitoring. IETF and the SCAP endpoint data collection identify orchestration as a needed technology to drive enterprise policy. Specific actions are identified to obtain findings to be assessed. This will then drive assessment of the posture and identify any remediations that may be required.

For our next meetings, please **send me your input by Monday Noon EST** on topics and content for the following Thursday's call. We want to finish out this document and will start to work more on the ontology during these meetings.

Topic 2 – Technical Steering Committee discussion

Mark has been working on the document. That document has been posted here.

Mark has also pulled together a draft presentation deck. This has been posted to our Github.