Architectural Reference Working Group

Meeting Minutes

4 November 2021

Attendees: **Russ Warren, David Kemp, David Lemire, Mike Rosa, Forrest Hare, Dennis Moreau, Dee Schur**
Agenda:

Here is the agenda for our call Thursday.
(1) Continue working on the mapping the OCA architecture to OpenC2

We reviewed the updates to the mapping per comments from our last call:

- Add a row for missing targets (ex. Add Domain and URL)
- Add a column for missing actions (ex Scan)
- Color code the circles (traffic light)

We discussed the mapping of the OCA use case to the OpenC2 EDR Actuator. We changed two of the rows concerning the where the EPSW is checking for new network blocks and updated hashes. This would be configured as automatic recurring periodic actions of the EPSW rather than requiring OpenC2 commands to trigger them. This approach would be something like an OpenC2 'set' action to configure the parameters of retrieval: how often, where to pull from, rather than sending an 'update/query files' request to the EPSW when it should make such a check. It's much cleaner to configure 1,000 endpoints once each to do something routinely than to routinely send the same command to 1,000 endpoints.

We discussed linking with the OpenC2 team, including the leaders of the EDR actuator, Martin Evans and Vasileios Mavroeidis. We also discussed meeting with the OpenC2 technical committee to start our engagement. Russ will work with Dave Lemire to schedule this meeting. We will review OCA (goals/objectives), discuss our use case and mapping to the EDR actuator. We can then identify next steps.

Mike Rosa is going to look at our use cases to identify potential areas for new actuators as he is trying to build a roadmap for these in OpenC2.

Dennis suggested we add to our current use case to address malware as discovered by NDR solutions. This will also help us address XDR. Dennis suggested we want to be able to connect malware events from both an EDR and XDR solution to align the information reported to enable it to be correlated. Dennis will extend the current use case document as well as diagram.

Russ discussed the next steps and indicated we have additional use cases document from Doug Austin in the Github. We should select another use case, either from this list or suggest another one and repeat the process we did with the first use case (building the diagrams and mapping to OpenC2).