Architectural Reference Working Group

Meeting Minutes

18 November 2021

Attendees: **Russ Warren, David Kemp, Andrew Beard, Mike Rosa, Forrest Hare, Dennis Moreau, Forrest Hare, Bob Besharat, Stefaan Van Daele, Michael Rosa, Ray Harris, Remko De Knikker**

Agenda:

Here is the agenda for our call Thursday.

(1) Update on our work with OpenC2 and EDR

(2) Dennis Moreau will describe his progress on extending the use case to include EDR, and possibly NDR. His first step has been to identify candidate actions, enabled by APIs for representative EDR and NDR technologies. He will also describe how EDR usage, moderated by OpenC2 style communication, might fit into typical EDR use cases/workflows.

We have started discussions with the OpenC2 EDR actuator profile authors. We submitted our mappings of what we intend to use and what additions we will need. Use case for 3 personas (threat hunter/investigator, SIEM admin and SOAR admin) were send over to demonstrate the requirement for a Query/Response capability.

Dennis went through his presentation on his initial work looking at EDR and NDR and how we can extend our current approach and use case. His material will be posted to our Github. Dennis pointed out several references (MITRE and Gartner) to define the capabilities of an EDR solution. Dennis also reviewed current EDR tools and some of their scope and capabilities. Dennis went on to describe the various way EDR solutions interact and how the semantics differed. He also covered MDR and XDR and how these areas were evolving.

We discussed possible approaches and next steps. Dennis will continue this discussion on our next call.