Architectural Reference Working Group

Meeting Minutes

8 March 2021

Attendees: Mitch Thomas, Russ Warren, Stephen Wood, Bill Munyan, Adam Montville, Roseann Guttierrez, Forrest Hare, Dee Shur, David Kemp, Mark Mastrangeli, Andrew Beard, Chris Murphy

Agenda:

- Here is the agenda for our call Thursday. Please send me your comments/or post issues to the current C4 diagrams. I want to wrap this section up this week so we can
  - (a) kickoff the ontology work to define the actions/data
  - (b) focus on the SOAR and Threat Intelligence components and their data flows
- Topics:
  - Review Diagrams - Discuss new input/comments; review the new diagrams (expecting an update for the overview diagram; see below for the SIEM diagram we discussed on the last call
  - Next steps - SOAR and Threat Intelligence - need diagrams and data flows identified for use case 1
  - Open discussion/ other items

- Here are our use case 1 diagram. PLEASE review and comment (open an issue); we will discuss these on our next call Thursday.
- Overview Diagram --> https://github.com/opencybersecurityalliance/documentation/blob/master/Architecture%20Documents/SystemLandscapeMalwareOCA-031921.svg
- SIEM Diagram --> https://github.com/opencybersecurityalliance/documentation/blob/master/Architecture%20Documents/SIEMComponentUseCase1-031921.svg
- I have added the SIEM data flow diagram ---> https://github.com/opencybersecurityalliance/documentation/blob/master/Architecture%20Documents/UseCase1SIEM.svg

Topic 1 – Review and discuss the current diagrams

We discussed the SIEM diagram that shows the data flows into the SIEM. Need to add standard flows (ex. Syslog, PCAP) and indicate some example solutions for the sources of this data to make it clearer. Security data and network flows seem to relate, may have overlap, so we need to flatten out the information (perhaps a BUS diagram?). Threat intelligence should flow into the SIEM (part of the network information). Some log information can indicate threat intelligence information. Security data can be provided by any of the IT infrastructure components. Analytics can have a similar role as a SIEM and can also be provided by the IT infrastructure. Perhaps we can define the role for each of the boxes?

Ontology will probably be role based (common criteria?). Perhaps we can use higher level boxes (ex 1 network box versus two). Perhaps we can use STIX2 as a standard format for data flows to standardize.

We reviewed the list of actions provided by integrated endpoint solutions as well as the integrated email security solutions. This is a starting list, and we need input on other actions that can be taken on an endpoint and email security solution.

We discussed ontology and STIX and how we can map to a knowledge model. Forrest has discussed this with the STIX TC a few years ago. At that time, STIX did not prioritize this work. Objects and relationships between them do exist in STIX; but not mapped into a logical construct. We could work with STIX as it is now.

Topic 2 – Technical Steering Committee discussion

Mark discussed the next steps for the TC. He is working on a draft to merge OPENC2 with the ontology. He is also working on new topics and use case (ex. file submission to a sandbox) examples. Mark will schedule a date to review this work. Mark is also setting up a call with Forrest to continue the discussion on ontology to prepare to start the OCA ontology. Forrest is contacting Precisely to show an example of using the knowledge model approach. Forrest has offered to present this presentation for the Borderless cyber webinar (Dee will work with Forrest on this).

Mark shared the document he is working on and he will post it out into the Github for review. He will also change the name of the ontology (from OpenDXL ontology). Mark is looking to align with Gartner on terminology (ex SIEM, SOAR,..). He wants to start with the topic level and work down into more detail. Forrest suggested Mark put the definitions with the terms as you evolve the document.