Architectural Reference Working Group

Meeting Minutes

22 April 2021

Attendees: Mitch Thomas, Russ Warren, Stephen Wood, Adam Montville, Forrest Hare, Dee Shur, David Kemp, Mark Mastrangeli, Andrew Beard

Agenda:

Here is the agenda for our call Thursday.
(a) discuss/review data flow for SIEM
(b) focus on the SOAR and Threat Intelligence components and their data flows- need some help on these!
(c) restart 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 (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
SIEM Data Flow -->
https://github.com/opencybersecurityalliance/documentation/blob/master/Architecture%20Documents/SIEMDataFlows.svg
SIEM Actions -->
https://github.com/opencybersecurityalliance/documentation/blob/master/Architecture%20Documents/SIEM%20Use%20Case%201.pdf

Our current architecture document draft -->
PDF -->
https://github.com/opencybersecurityalliance/documentation/blob/master/The%20Open%20Cybersecurity%20Alliance%20Document.pdf

Source document --> https://drive.google.com/file/d/18dr4-8N7VWGdaf2mA-F4rTq0OLZu9XEB/view?usp=sharing

Topic 1 – Review and discuss the current diagrams

We reviewed the data flow diagrams for SIEM. We need to start SOAR and threat intelligence (Andrew has volunteered to help on these). We also reviewed the architecture paper (revision 3) that is out for review. We discussed the term IT Infrastructure, and we may want to call it the cyber-environment or network infrastructure (to differentiate with the IT operations domain). Vulnerability intelligence (coming in from the outside, list of vulnerabilities discovered from CTI, like CVE reports) and assessment (reports) are two key areas of SCAP. Add a vulnerabilities assessment box (CVEs). Automation has assessment and remediation parts (SOAR). SCAP overlaps those two areas.

For SOAR and threat intelligence, we need to identify data flows and create malware detection pictures with actions and systems they interact with. We also need to capture the actions that take with the email and endpoint scanners as well as the other security applications (SIEM, SOAR, threat). We want to get the most common things captured; we can iterate on as we evolve the architecture and ontology.

We moved to the architecture document draft. The use case section has been added. This will demonstrate the OCA architecture via the use case to show what is different from today's approach. The document will need to highlight key points (perhaps using a Note or visual box) to make it easier for the reader to spot the value of OCA. We need to focus on cohesive that work efficiently together are value propositions we point out in the front of the document. We also have loosely coupled and event driven characteristics in our architecture. Third bullet on page 19 can be enhanced to cover these characteristics (ex. common commands/formats give you loosely coupled systems).

We need to capture the value of SCAP in our pictures and diagrams. David has offered to help on this topic. SCAP focused on CVE, XCCDFs data formats. SCAP V2 is a system for continuous monitoring, that would use those data formats plus a set of interactions to do the assessments. Device assessment collection is the focus of SCAP; SOAR is focused on the remediation. SCAP is not a separate category or box in our pictures).

We need to add a picture on OPENC2 and the ontology to show how they relate. David can help on this topic.

Topic 2 – Technical Steering Committee discussion

Mark shared his current activities on the ontology. He has pulled together a draft presentation on the ontology and is defining how to approach defining the ontology. Mark is looking at a See, Know, Do model to approach the ontology work. The demo on April 29 will be a great help on how we can approach the ontology. This is an implementation of a graph-based ontology, which could be based on the OCA ontology. We need to have a good common model to achieve automation and better interoperability.

Mark will work on the document and will upload it for review.