Architectural Reference Working Group

Meeting Minutes

25 March 2021

Attendees: Russ Warren, Doug Austin, Bill Munyan, Adam Montvile, Roseann Guttierrez, Forrest Hare, Dee Shur, David Kemp, Andrew Beard, Christian Hunt, Jason Keirstead, Mark Mastrangeli, Doug Austin

Agenda:

- Opening Comments
  - OCA technical meetings going forward
  - The OCA Community Forum
  - Review the objectives of our workgroup
- We will continue our review and discuss use case 1 (malware discovery).
  I have updated the diagrams for use case 1 based on our last session. 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
  -

Topic 1 – Opening Comments

We will only have one technical meeting going forward. This architecture group will meld in with the Technical Steering Committee that Mark is leading. Jason has also launched a new forum to discuss topics of interest to OCA members. This forum is called the OCA Community Forum (using the OCA mailing list). The first topic is scheduled for April 12, covering Indicators of Behaviors. Anybody can nominate a topic and/or attend the calls (they are NOT restricted to OCA members). More awareness of OCA and what we are doing is one of the objectives of these calls. Next one will have OT Security as a topic.

Our workgroup has identified needs for the ontology, and we will be discussing how we will work on defining this ontology. We will need to work the C4 high level and lower-level diagrams. We also have a document, currently drafted, that will be updated.

Adam mentioned the need to work with the SCAP endpoint data collection group. This group desires that we work with their group and join them in their meetings on occasion. We would want to create a proposal to this group (SCAP to inform the ontology) so we can work together and stay in sync. We should default to the vocabulary of an existing group (ex OPENC2, SCAP) to better ensure consistency and initial alignment. Russ will schedule a call with Dave Kemp, the OCA maintainer of the SCAP V2 prototype to discuss how we work and communicate with the SCAP endpoint data collection group.

Topic 2 – Review the use case diagrams for Use Case 1

Andrew discussed his comment and feedback on our current diagrams. Andrew's background is in controls development and incident response as well as threat research as an analyst. He mapped the use case, C4 diagrams and ontology to ensure they were aligned. He pointed out there are some places, specifically block actions (blocking a file vs blocking the device) that were not clear and aligned. We will need to update the use case for this. Ontology and actions are light and need more refinement. Quarantine based on network setups affects the ontology.

Updating on the Github is done by creating your branch, do the updates and create a PULL request to submit it back. We will review proposed changes in our bi-weekly calls. Please make proposed updates in our Github and create an Issue for any comments you have on the current material.

We need to discuss how the SCAP posture collection system communicates with the other systems in our diagrams. Dave mentioned NIST was also discussing this topic.

The yellow boxes were created from the existing ontology. These will need work to further define. We also need to identify other actions that are taken between the systems.

Forrest has offered to host a call to cover ontology overview and how to build them. This will be very helpful prior to our starting the ontology work. Russ will follow up with Forrest to get this scheduled.

Andrew asked about the posture collection system (PCS) (not mentioned in use case nor ontology). Mark mentioned work he planned to do on the ontology to bring in the SCAP work. Several members posted some reference web sites. I have capture them below and will pos to our GIthub.

Dave discussed SCAP and how it relates to SOAR, threat intelligence systems and SIEM. Capabilities of the PCS is underway at this time. ITS management, for assets, are involved with the PCS. Adam mentioned an example of how the systems could be ties together. Mark suggested the event modeling approach (a given, when, then) for the ontology work. This would be a loose-coupling distributed architecture. SCAP architecture is predicated on some IETF work (support decoupled systems).

SACM architecture updates are being worked on by Bill and Adam; expected to be completed in a few weeks. They will let us know when it is available. Our current diagrams on SACM, born out of posture assessment, need to be updated. SIEM, SOAR and EDR , beyond the current posture assessment, are in scope for SACM.

We discussed our overview document and the need for updates.

- Add text to the lines
- Indicate where there are multiple instances (ex. telemetry ingestion box, EDR)
- Make clearer the scope of the Sense making analytics framework (higher level across all data)
- Data Fabric is a thing to call
- Allow arrows should be in the ontology (all data flows)
- Update to latest OpenC2 and align with SCAP work

Next steps is to decompose the SIEM component. Mark discussed the need for data acquisition and connecting to a data source is a part of the integration service. Some capabilities in a SIEM should be segment out to better leverage these services in other systems. SIEMs collect many different types of data. Defining a looser coupling of data that a specific system has that is needed by others. Andrew suggested we think of these questions: What can you do? What can you provide? What can you export?

Doug raised a question about our scope. We want to ensure it is achievable. We are focused on interoperation. Jason suggested we name all arrows and map it to IACD, SCAP, … to relate to existing work to show what exists today.

Refences:

- https://eventmodeling.org
- SCAP v2 Data Collection Architecture https://docs.google.com/document/d/1ne53W3iVAUUi7d56zLviHEpZh1usZ4Wc/edit
- SACM Architecture https://datatracker.ietf.org/doc/draft-ietf-sacm-arch/?include_text=1
- Data Collection Architecture Sub-Group https://docs.google.com/presentation/d/1k1upJM0Afob0C7EdOD9Z6XDs7uZlTSLkXUI7KLcFa7Y/edit#slide=id.p1