Architectural Reference Working Group

Meeting Minutes

26 February 2021

Attendees: Mitch Thomas, Russ Warren, Stephen Wood, Doug Austin, Bill Munyan, Adam Montvile, Roseann Guttierrez, Forrest Hare, Dee Shur, David Kemp

Agenda:

- Adam, Bill and Mitch review of the evolving our C4 diagrams (System Landscape draft?)
- Russ to review use case 1 diagrams (malware detection)
  - Use case documented here ---> https://github.com/opencybersecurityalliance/documentation/blob/master/Architecture%20Documents/UseCases.md
  - Diagrams (2) - current state and mapped to the OCA architecture https://github.com/opencybersecurityalliance/documentation/blob/master/Architecture%20Documents/SystemLandscapeMalware-3.svg https://github.com/opencybersecurityalliance/documentation/blob/master/Architecture%20Documents/SystemLandscapeMalwareOCA.svg

Topic 1 – Review and discuss the current diagrams

Adam reported on the meeting they held last week with the SCAP V2 Endpoint Data Collection group. They discussed the C4 diagrams Adam, Bill and Mitch have created. The SCAP team got some initial education on C4 diagraming and how to use it. There was good interaction with the SCAP team and the team had some good suggestions on updating these C4 diagrams. These diagrams initiated some good discussions that will continue in the planned bi-weekly meetings. The intention of these discussions is to ensure alignment and help define the OCA SCAP V2 prototype project actions (which will involve working with the OCA ontology project team). They want to identify who talks to the posture assessment system. The SCAP team would love to understand these use cases (context level).

The C4 diagrams were not updated (so you have time to catch up!). Mitch is going to attempt to build a System Landscape diagram for the next meeting.

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

Use cases are now in markdown format. Two landscape diagrams, one for pre-OCA architecture and one with the OCA architecture have been posted to our GitHub. These diagrams show the events sent by the malware scanners (file and email) and the receivers of the events (SIEM, SOAR, Threat Intelligence).

We will need to develop use cases for the security administrators (SIEM, SOAR, Threat Intelligence)

Diagrams need to be updated:

- Include timestamps on the diagrams
- The workstation may have resident scanners to add in
- Context diagrams are 2 directional; should the brown arrows be bi-directional?
- Should draw line to the people as they initiate actions
- We will show other feeds (ex. vulnerability scanners) and more detailed processes (ex log manager for SIEM, automation, asset model) at the component level diagrams

For the OCA diagram:

- Ontology should be labeled on the diagram and not represented as a box; sub-note in boxes
    - We want ontology to be a broker between systems; (standardize meaning of data flows)
    - Represent data via the lines (labels) that should be in the ontology (what, where and when data is being passed via the ontology).
    - Relationships between each system – shows lines between them (vs relationship between each system and the ontology). We can assume the broker. Shows lines between the systems and label the ontology we need so they can communicate.
- Scans should feed into the Posture Collection System (Blue box)
- Queries come into the Posture Collection System from the SIEM, SOAR, Threat Intelligence
- Showing one block (ex SIEM) - receives events, then processes it (container level diagram) Show how the SIEM talks to the malware protection systems. Should there be two lines to the SIEM, SOAR and threat intelligence systems?
- Black line show events from the scanners; Red lines from the SIEM, SOAM, Threat Intelligence. Add a key for these lines.
- Need to add a line to the posture collection system (red line) for queries from SIEM, SOAR and Threat Intelligence systems
- Add red line to the workstation from the STIXShifter boxes; Label red lines from SIEM, SOAR and Threat Intelligence systems (data flow)
-