Architectural Reference Working Group

Meeting Minutes

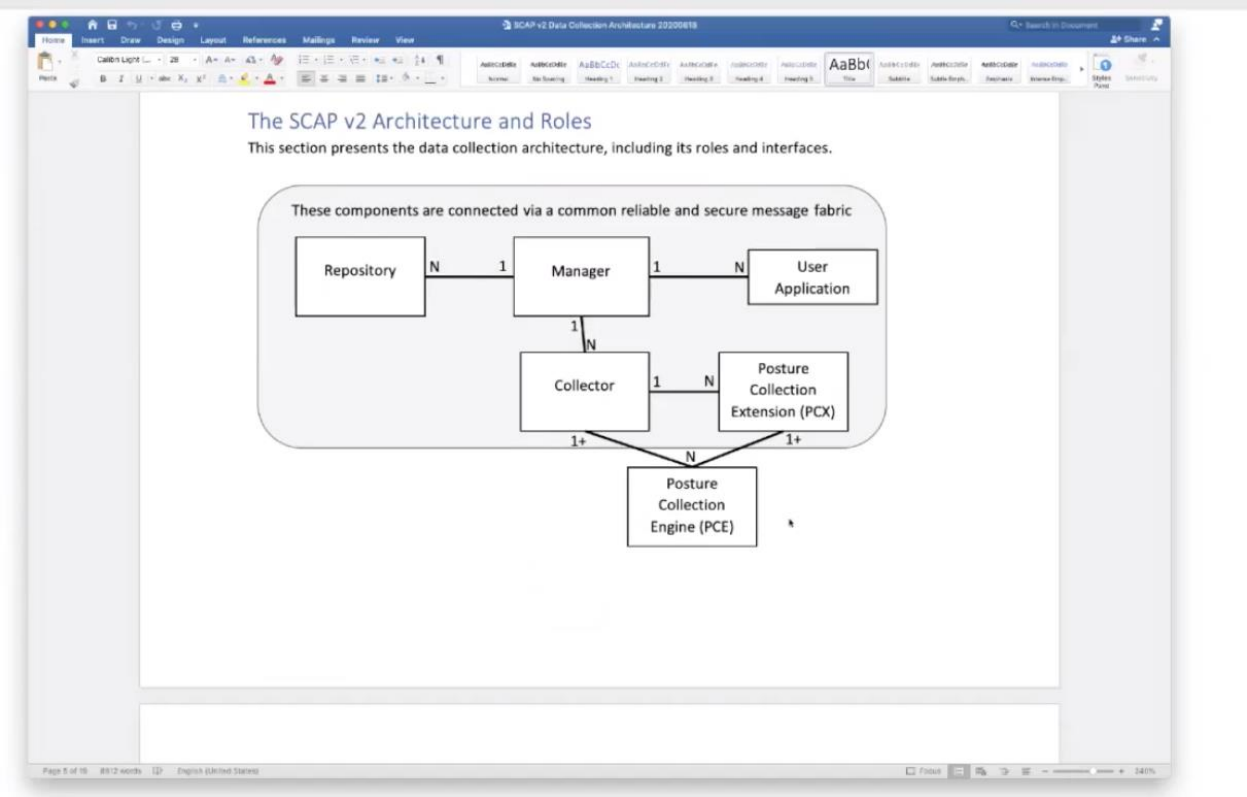
10 Sept 2020

Attendees: Adam Montville, David Lemire, Kent Landfield, Russ Warren, Mike Farmer, Stephen Wood, Jason Keirstead, Jory Burson, Duncan Sparrell, Doug Austin, Bill Munyan, RoseAnn Guttierrez

Agenda: Discuss the SCAP V2 architecture - Adam (also discussed SCAP architecture mapped to OCA's draft architectutre picture);

Summary of Discussion:

Topic 1: SCAP V2 Architecture



Adam reviewed the above diagram as well as more detailed diagrams of the SCAP V2 architecture. The objective of this architecture is to collect and assess data from targets (focus today is on endpoints). The posture of the endpoint (software loaded, vulnerabilities, configuration state,…) is assessed and stored in the repository. The repository is meant to be the source of queries from interested applications (like SIEM, SOAR). The SCAP architecture components are focused on continuous monitoring and collection of endpoint status. We also discussed the ongoing activity at IETF regarding orchestration

onboarding and ad-hoc evaluations. We referenced the software bill or materials work as a starting point for the collection of cybersecurity assets and inventory, a key feature needed to align the data source information. It was noted that asset management is not in our current architecture and discussed the need for follow on work in this area. Forrest referenced ontology work was ongoing in this area, using the OWL format to express the data. Adam mentioned he has done some work in this area, with Buill Munyan, and he sent out a draft paper to this group after our meeting.

Kent discussed the SCAP development prototype and its objectives to be the reference implementation. The prototype will be used to test out this architecture. MITRE , contracted via the NSA, is working on some development and they intend to donate source code to the OCA repository being set up. SCAP will continue to evolve the architecture and specification(s).

Noted actions included updating our architecture to reflex SCAP V2 (terminology cleanup, add missing roles). We discuss OPENDXL Ontology and its relationship to SCAP. SCAP has been using OPENDXL and there is some ontology developed already (not available in open source yet). This ontology would need to be updated to the SCAP V2 level and would be a good first step to align OPENDXL ontology with SCAP v2 prototype.