Healthcare SBOM Proof of Concept – Phase II Summary (2021-10-14)

Introduction

The value of providing SBOM information, proven in Phase I, was reconfirmed in Phase II. The second phase of the Healthcare SBOM Proof of Concept extended beyond Phase I by:

- Proving the viability of the baseline elements defined in the Phase I framing document
- Expanding the use cases considered
- Expanding the participants in generating (7)* and consuming(8)** SBOMs
- Development of a How-to Guide for creating SBOMs (52 documents created)
- Exploring the use of VEX (Vulnerability Exploitability eXchange)

The execution of this phase (Phase II) PoC was divided into three iterations.

Iteration 1 Goals and Accomplishments

- Naming-focused use cases: created by supplier & created by other SBOM stakeholder
- Confirmation of SPDX compatibility for SBOMs
- Confirmation of baseline elements: Author Name, Supplier Name, Component Name, Version String, Unique Identifier, Relationship, Primary and Included Components

Iteration 2 Goals and Accomplishments

- SBOM document version
- SBOM component completeness
- Unique identification using purl
- Software identity: list of common components, conventions to establish software identity, alignment on common components across suppliers' SBOMs
- SBOM component content provided by 1) direct inclusion, and 2) external SBOM reference
- SBOMs for system of systems devices with 1) single endpoint, and 2) multiple endpoints
- Use of a PoC-specific SBOM registry

Iteration 3 Goals and Accomplishments

- Exploration of VEX use cases using CSAF format
- Multiple unique identifiers: purl and CPE (or CPE format)
- Establishment of file naming conventions to identify the corresponding device
- Publication of a How-to Guide for SBOM producers
- Unrealized goals: component hash, CycloneDX format, use case for manufacturer as final goods assembler (supplier ingestion of component SBOMs)

Next Steps

A Phase III of the Healthcare SBOM Proof of Concept is anticipated to focus on:

- Driving adoption of SBOMs in the healthcare sector
- Expanded participation, especially to other business profiles (e.g., smaller organizations)
- Automating SBOM sharing (delivery/retrieval)
- Further work in VEX
- Communicating End of Life / End of Support
- Exploration of topics in unrealized goals from Phase II

*Device Manufacturers: Abbott, Becton Dickenson, Medtronic, Philips, Roche, Siemens Healthineers, Thermo Fisher Scientific
**Healthcare Providers: Cedars-Sinai, Christiana Care, Cleveland Clinic, Intermountain Healthcare, Mayo Clinic, New York Presbyterian, Sutter Health, Univ. of Virginia