



2.0

Healthcare SBOM Proof of Concept

UPDATE 2021-04-29

Overview

Goals

Prove viability of Framing document's definition

Expansion beyond initial PoC

- Expanded use cases
- Expanded participant list: HDOs, MDMs, vendors/suppliers
- Tooling and automation

“How-to” / playbooks for HDOs and MDMs

Approach

Collaborate with other working groups on definition

SBOMs produced for a predefined set of devices

Execute proposed use cases including procurement

Iterate to increasing complexity and speculative topics with published deliverables each iteration

Participants


HDOs

- Cedars-Sinai
- Christiana Care
- Cleveland Clinic 
- Intermountain Healthcare 
- Mayo Clinic
- New York Presbyterian
- Sutter Health
- University of Virginia 

MDMs

- Abbott
- Medtronic
- Philips
- Siemens Healthineers
- Thermo Fisher Scientific

Vendors

- Medigate
- Censinet
- Nuvolo
- IONChannel 

Iteration 1 Objectives

Execute Naming-Focused Use Cases

- Use Case 1: A Supplier Creates an SBOM for a Primary Component
- Use Case 2: An SBOM Stakeholder Creates an SBOM

Confirm SPDX format supports content

- One format for this iteration
- Additional formats in following iterations

Confirm Baseline Elements

- Author Name
- Supplier Name
- Component Name
- Version String
- Unique Identifier
- Relationship
- Primary Component
- Included Components

Iteration 2 Objectives

Software Document Version

SBOM Component Completeness

Unique Identifier using **purl**

Software Identity

- List of common components
- Conventions to establish software identity
- Alignment across participant SBOMs for common components

SBOM Content for Included Components

- Include in the SBOM Document
- Reference an External SBOM Document

SBOM for Medical Device System-of-Systems

- Single Endpoint
- Multiple Endpoints

SBOM Registry

- List of POC SBOMs

Iteration 3 Objectives

Exploring “VEX”

- Use Cases
- Content
- CSAF Format

Multiple Unique Identifiers

- **purl** for Supplier
- **CPE** (or pseudo-CPE) for VEX

Component Hash

Additional SBOM Formats

- CycloneDX

SBOM File Naming

- Establish file name conventions to identification of the medical device

Exploring MDM as Final Goods Assembler

- Ingestion of Component SBOM

MDM How-To Guide for Healthcare POC SBOM (Playbook)

VEX POC Use Cases

Vulnerability in a Component That is Not Included in the Medical Device

- Allows MDM to clearly establish the vulnerability is not present because the component is not used
- Can also be discovered by consuming the SBOM

The Vulnerability in a Component is Under Investigation

- The MDM has not completed their assessment of the vulnerability, and more details will follow

Medical Device Pre-procurement

- VEX statements can be evaluated as part of the HDO pre-procurement process

Vulnerability in a Component that Does Not Impact the Medical Device

- No actions by the HDO are required to mitigate the vulnerability

Vulnerability in a Component that Does Impact the Medical Device

- The MDM is providing recommended actions the HDO can perform to mitigate the vulnerability

VEX Content

VEX Document Identity

- Document Name
- Document Version
- Document Author
- Publication Date
- Supplier Contact

Product

- Single product only for the POC
- SBOM Primary Component
- Software Identity of the Primary Component
 - Supplier Name
 - Component Name
 - Version String
 - Unique Identity (from Supplier)

VEX Content (cont.)

Vulnerability

- Included Component from SBOM
- Software Identity of the Included Component
 - Supplier Name
 - Component Name
 - Version String
 - Unique Identity (from Supplier)
- Included Component Unique Identifier (CPE)
- Identifier of the Vulnerability (CVE)

Vulnerability Statement

- Vulnerability Status
 - Impact coded value (VEX sub-group codes)
 - Known_Affected
 - Known_Not_Affected
 - Impact statement
 - Textual description
 - Additional context on the impact
- Resulting Risk Score
 - CVSS 3.0 Rubric for Medical Devices
- Consumer Action
 - Textual description
 - Recommended actions for the HDO

VEX Distribution

Separate VEX Document

Located in Box Restricted Folder

Available in Same Folder as SBOM Documents

Updated SBOM Registry with VEX Document

Use as VEX Issued at Release or Post-release

Documents and Resources

MDM How-To Guide for Healthcare POC
SBOM (in progress)

SBOM Examples

- SPDX
- SWID

SBOM Medical Device System-of-Systems
Examples

SBOM Registry

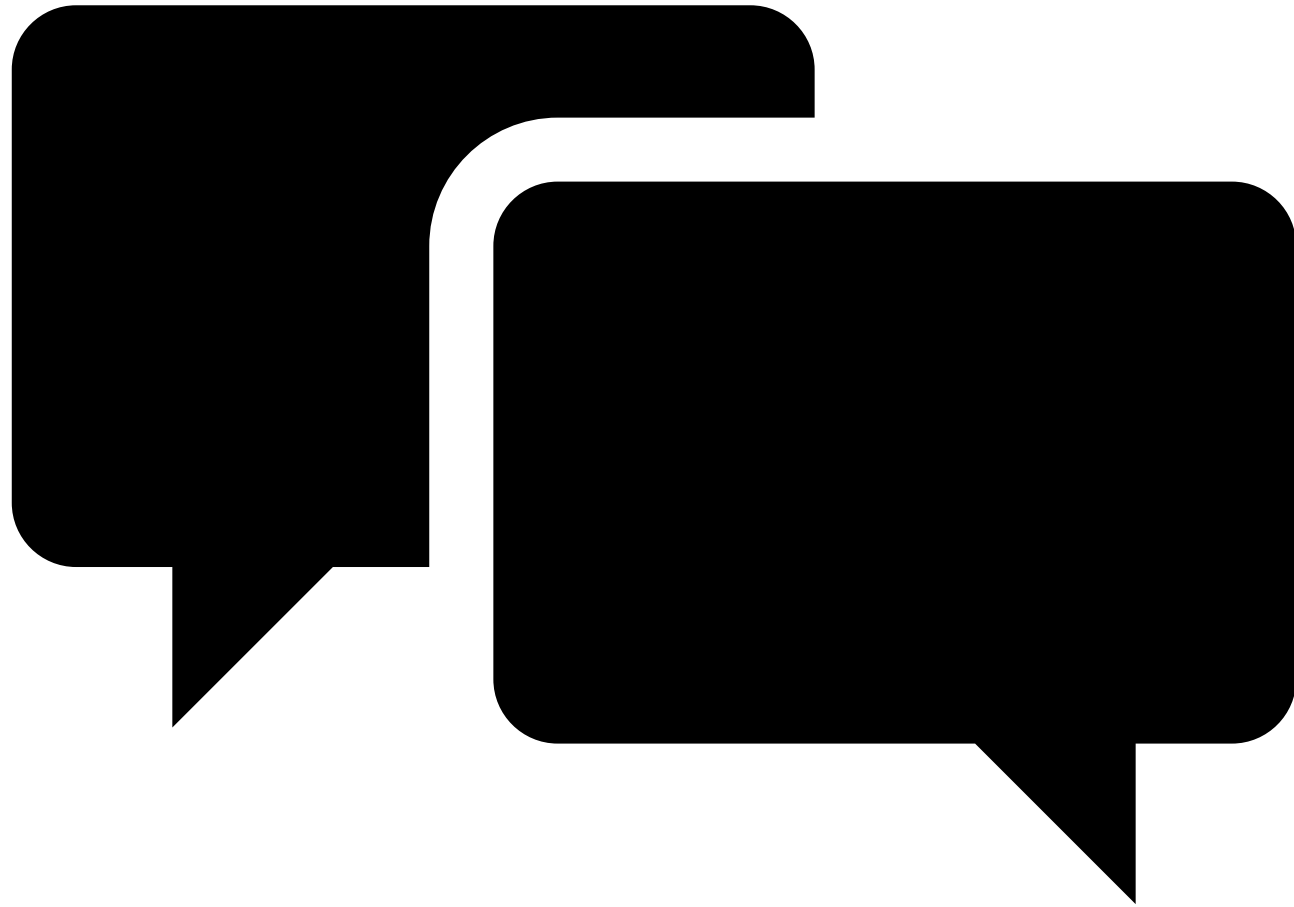
SBOM Generation Tools

- SwiftBOM
- Excel SPDX Generator

SBOM Conformance Tools

VEX Scenarios for Healthcare POC

VEX Content Example



Discussion

Questions? Comments? Suggestions? Volunteers?