2.0

Healthcare SBOM Proof of Concept

UPDATE 2020-07-09

Topics

Overview / Status	Jim Jacobson
SBOM Generation Summary The Medical Device Manufacturer (MDM) perspective from Iteration 1	Ed Heierman
SBOM Consumption Update The Healthcare Delivery Organization (HDO) experience from Iteration 1 – interim	Michael Dittamo
Vendor Participation Framework	Jennings Aske

Overview / Status

2.0

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
- Johns Hopkins
- Mayo Clinic
- New York Presbyterian
- Partners/Mass. General
- Sutter Health

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

Vendors
- Medigate
- Censinet
- Nuvolo

SBOM Generation Summary

ED HEIERMAN, ABBOTT

POC Phase II, Iteration 1 Participants

Medical Device Manufacturers

- Abbott
- Medtronic
- Philips
- Siemens
- Thermo Fisher

Healthcare Delivery Organizations

- Cedars Sinai
- Christiana Care
- Mayo Clinic
- New York Presbyterian
- Sutter Health

Objectives

2.0

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 next iteration

Confirm Baseline Elements

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

Execution

2.0

NDA put in place to protect MDM proprietary data

HDOs provided inventory of deployed MDM devices

Best-effort approach for Software Identity

Created SPDX example and guidance document

MDMs created SBOMs manually and with generator tooling

- Iterative deliveries over a six week period
- Total of 17 SBOMs created, versus 7 in POC 1

Distributed SBOMs using Box

- Provides controlled access
- Simulates delivery through customer portals often used by MDMs for other device documentation

Challenges

2.0

Collecting SBOM Data

Inconsistent identification of the same Included Component occurred across MDMs

- Inconsistent Supplier and Component Names
- Inconsistent Version Strings

HDOs were not always aware of SBOM updates

Incomplete SPDX support for purl Unique Identifier

- Included as a package comment
- Addressed in SPDX-2.2

Limited Tooling

Collaboration With Framing Group

2.0

Provided list of Suppliers

- Identities established by participating MDMs
- Framing can use for further analysis of Supplier Identity challenges and provide input for Iteration 2

Provided list of Included Components

- Software Identities established by MDMs
- Some components used by multiple MDMs
- COTS and Open-Source
- Framing can use for further analysis of Component Identification challenges and provide input for Iteration 2

Holding discussions to establish Iteration 2 objectives

- SBOM for Medical Devices (IoTs)
  - Medical Device as a Primary Component
  - Medical Device as a System of Systems
- Distribution/Discovery/Access
- Component Hash
- Exposure to Vulnerabilities
- SBOM Versions
- SBOM Formats
  - SWID
  - CycloneDx

Summary Reports Created for Iteration 1

SBOM Generation Summary

- Provides guidance on generating an SBOM in the SPDX format
- Highlights the Use Cases and SPDX example

Tool Summary

- Discusses various tools used, explored, or under consideration for Iteration 2
- Provides some guidance on tool usage

Crawl, Walk, Run Maturity Evaluation

- Experiences with major SBOM elements and topics
- High-level assessment of maturity with creating an SBOM

SBOM Consumption Update

MICHAEL DITTAMO, NEW YORK PRESBYTERIAN

HDO Use Cases (Update)

2.0

The following Use Case updates represent three of the participating HDOs

- Procurement
  - All three of the responding HDOs were able to successfully ingest the SPDX SBOM into their respective SIEM solutions, immediately making the data searchable for manual identification of security vulnerabilities across a fleet of products. This data can also be converted into a human—readable, tabular format.
  - Multiple HDOs are collaborating with vendor partners to explore direct ingestion into medical device asset/risk management solutions as part of device procurement.
  - Cedars Sinai is collaborating with one of their vendor partners to explore direct ingestion into a healthcare Vendor Risk Management (VRM) solution.
  - NYP has developed a ”How-To Guide” focusing on how to properly parse out the Packages fields using regular expressions (regex). The recommended regex also takes into consideration some of the slight differences in SBOM SPDX schemas.
  - Cursory analysis shows that Software Component Naming still appears to present an issue when correlating the parsed information to external resources.
  - HDO’s continue to explore automated correlation to authoritative vulnerability data upon procurement.
- Asset Management
  - Two of the responding HDOs have begun configuring their respective CMDB platforms to allow for software component assets as children under the parent asset entries. This use case not only explores initial entry, but management of the device over time using methods such as API import/update using the parsed data from the SIEM ingestion.
  - Multiple HDOs are collaborating with vendor partners to manage devices into medical device asset/risk management solutions through the life of the device, by allowing for periodic update and an audit trail.

Procurement | Asset Management | Risk Management | Vulnerability Management | Legal

HDO Use Cases (Update)

2.0

The following Use Case updates represent three of the participating HDOs

- Risk Management
  - All of the responding HDOs are exploring vulnerability identification upon procurement (i.e. SIEM) and on an on-going basis (i.e. SIEM, CMDB/CMMS, VRM).
  - It is the intention of the participating HDOs that tabletop mitigation plan / compensating control exercises will be performed to identify vulnerable components, measure exploitability, implement risk reduction techniques, and document this data alongside the SBOM.

- Vulnerability Management
  - Cedars Sinai is working with their Biomed team to manually perform vulnerability management processes on information extracted from SBOM data. Cedars will only leverage scanning tools for Cedars owned workstation that are connected medical devices to discover additional information.
  - NYP is working with their Vulnerability Management team to evaluate correlated SBOM data to credentialed/non-credentialed scans of the same device; this may also prove useful in an information audit use case.
  - Sutter Health is currently working with their Vulnerability Management team on leveraging the SBOM data to supplement regular scanning results.

- Legal
  - Participating HDOs have been developing SBOM product security language to add cybersecurity safeguards to the contract documentation.

Procurement | Asset Management | Risk Management | Vulnerability Management | Legal

Vendor Participation Framework

JENNINGS ASKE, NEW YORK PRESBYTERIAN

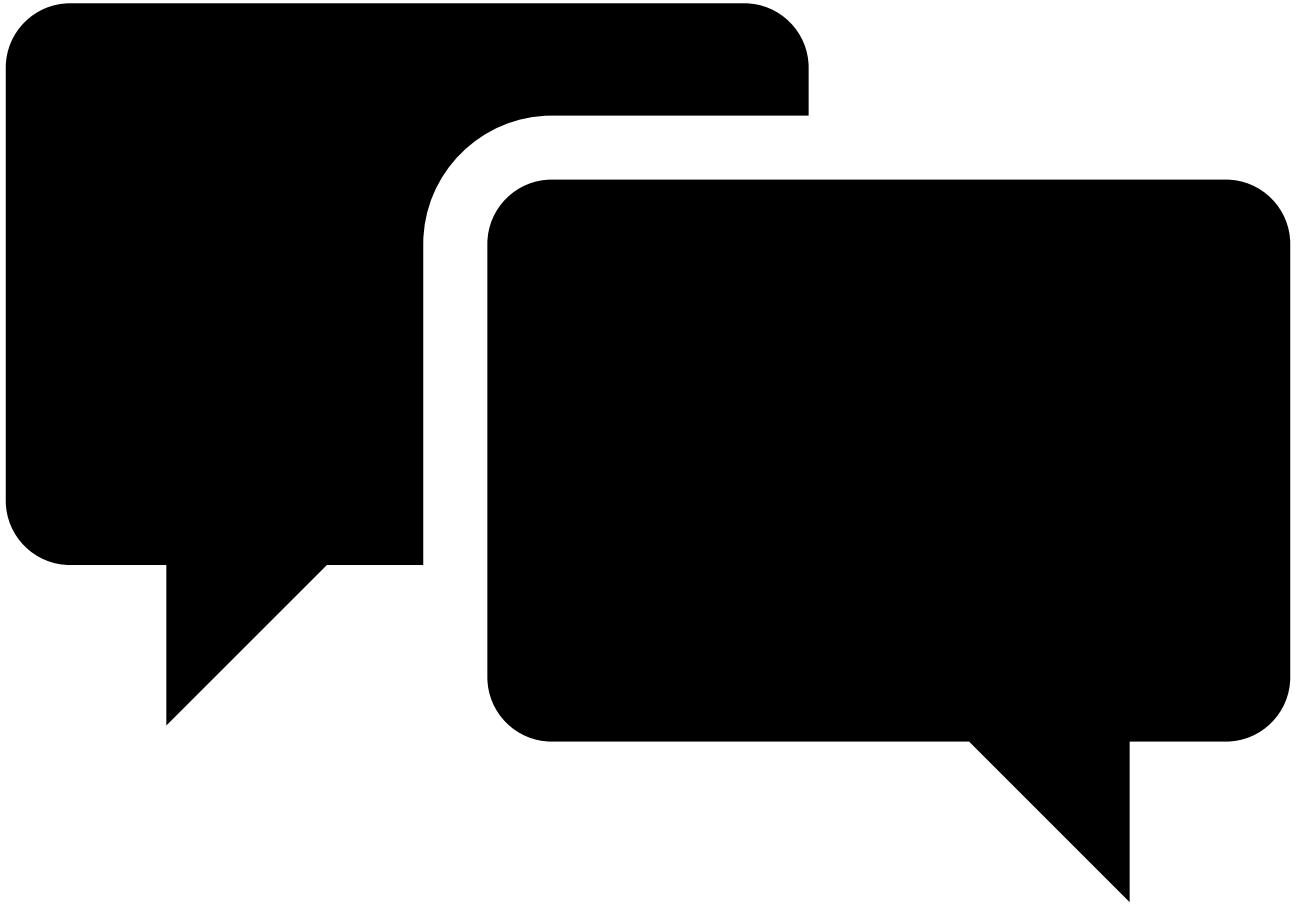
Vendor Participation Framework

The Healthcare SBOM PoC working group provides an opportunity for solution/tooling suppliers or vendors to participate in executing use cases around SBOM production and consumption.

Participation is open to any vendor which meets the requirements which include:

- Applicability
- Enrollment with the Tooling working group
- Recognition that SBOMs used are not official documents of the parties involved and information contained is not to be used outside of the proof of concept
- Execution of a non-disclosure agreement (NDA)

More details on the framework will be described in an update to this section, and reviewed during the meeting.



Discussion

Questions? Comments? Suggestions? Volunteers?