2.0

Healthcare SBOM Proof of Concept

UPDATE 2020-04-15

Summary / Status

2.0

Goals

Prove viability of Framing document's definition

Expansion beyond initial PoC
- Expanded use cases
- Expanded participant list
- 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 finalized
- Cedars-Sinai
- Christiana Care
- Mayo Clinic
- New York Presbyterian
- Sutter Heath

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

Tooling Suppliers
- Not finalized

Tooling

2.0

The PoC welcomes additional tooling suppliers / vendors capable of speaking SBOM*

Usage

- Creation of SBOMs: integration into code analysis and build processes
- Consumption of SBOMs: integration into asset management and risk management
- Also possible: comparing (Diffing) documents, translating between formats

Vendors are encouraged to participate

- If not already in the PoC, contact Allan Friedman (AFriedman@ntia.gov) to sign up
- Participation may require execution of existing NDA, depending upon level of involvement

*At this point, we are targeting SPDX and SWID

Use Cases (Overviews)

2.0

Procurement: Cross-team exercise to explore how the SBOM impacts the purchasing decision, including the development of contract language.

Asset Management: Demonstrate the inventorying of application components using both manual processes and CMDB/CMMS technologies.

Risk Management: Leverage manual processes and automated eGRC technologies to identify new vulnerabilities and risks over time and implement risk mitigation techniques.

Vulnerability Management: Identify ways to supplement and integrate SBOM data into vulnerability identification and security scanning activities.

Use Cases (Activities)

2.0

- Transmit the SBOM over the Internet and identify lifecycle management processes
- Develop contract language to coincide with procurement activities
- Identify vulnerable, end-of-life, and/or custom software components, as well as potential system conflicts and measure vulnerability vs exploitability
- Suggest compensatory or alternative controls to reduce the risk of vulnerable components
- Measure potential reduction of assessment artifacts (i.e. vendor questionnaires)
- Determine licensing agreements around support and patching and which anti-malware software type and version are able to be installed
- Determine if another product should be considered with less inherent problems due to the software lifecycle
- Identify roadmaps to improve MDM vulnerabilities

Procurement | Asset Management | Risk Management | Vulnerability Management

Use Cases (Activities)

2.0

- Adopt a standard naming convention
- Establish workflows to support the intake and management of assets into the CMDB/CMMS
- Correlate vulnerability information (i.e. NVD) to perform initial and ongoing risk assessments
- Leverage SBOM data to provide insight into end of life identification and planning; determine if custom software can also be reasonably identified and inventoried
- Initiate invasive scanning and penetration testing (when the device is not in use) to measure and compare known vulnerabilities with SBOM information and potential clinical exposure
- Implement and document mitigation strategies and measure changes in risk
- Monitor vulnerability announcements, track patching activities, and assess device risk over time
- Measure and analyze SBOM inventory across a fleet of products and systems

Procurement | **Asset Management** | Risk Management | Vulnerability Management

Use Cases (Activities)

2.0

- Utilize common database (i.e. NVD), data analytics tooling and CMDB/CMSS to identify vulnerabilities
- Explore eGRC processes and technologies to support automated, periodic risk analysis and reporting; potential utilization of an automation tool to build ISO 9001 standard rules to do risk assessment
- Develop mitigation strategies within the HDOs and in collaboration with the MDMs
- Supplement machine-readable MDS2 with SBOM software component information as part of a comprehensive risk assessment
- Leverage SBOM data to support risk mitigation and management across the fleet using type, make/model, etc.
- The POC will also explore utilizing vulnerability vs exploitability (VEX) information if available to facilitate risk management activities. Note: this is *not a requirement* for the minimally viable SBOM.

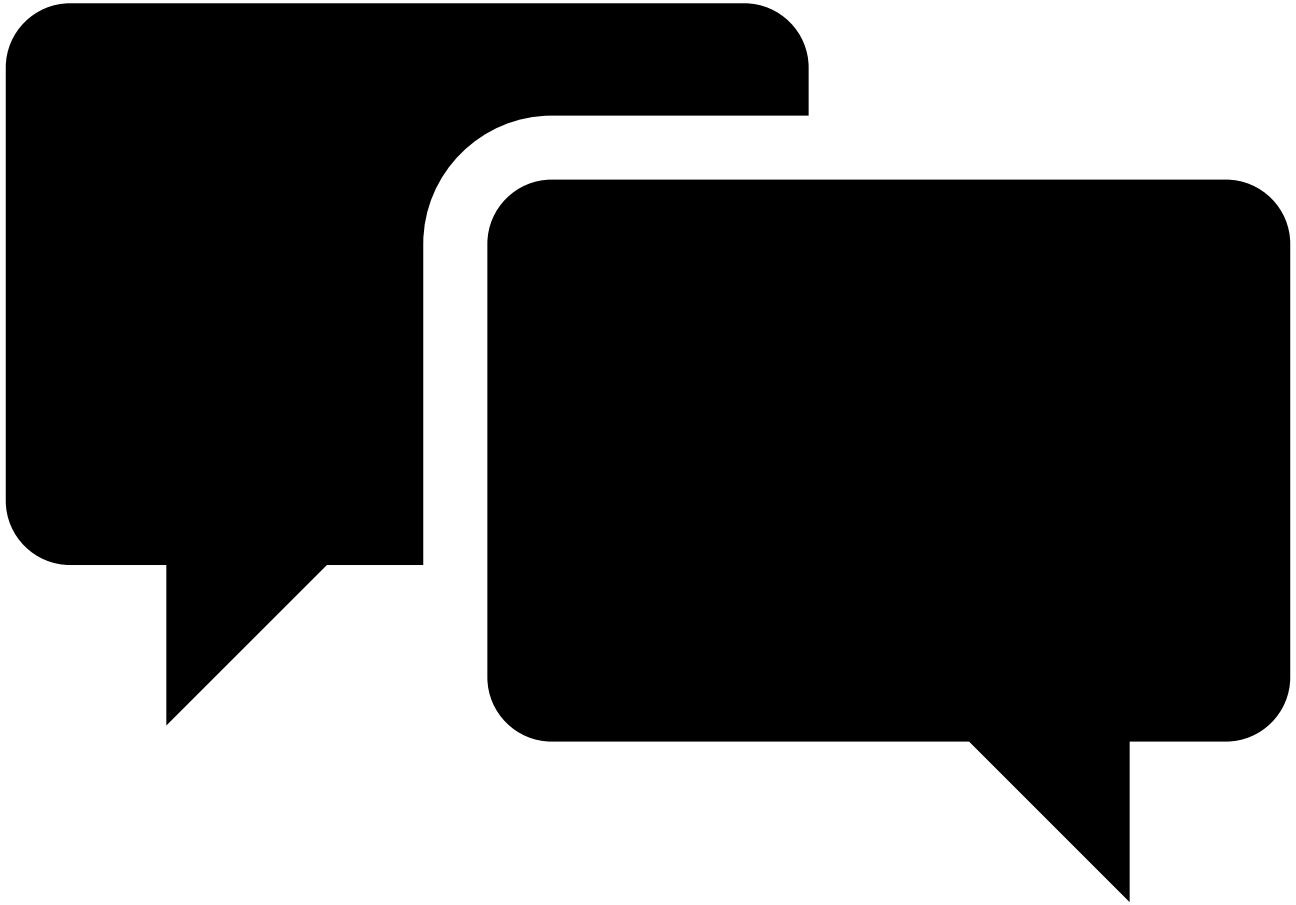
Procurement | Asset Management | **Risk Management** | Vulnerability Management

Use Cases (Activities)

2.0

- Identify integration points with the SBOM and existing security scanning tools
- Determine appropriate scan configurations for BioMed and IoT devices to prevent crashes or denial of service
- Automate vulnerability management activities with SBOM information that me be imported into a CMDB/CMSS and capture this activity as a playbook deliverable
- Locate vulnerabilities that cannot be easily mitigation or patched and explore network controls to reduce the risk to an acceptable level. *Determine what other strategies are successful, from whitelisting and MDM initiated BIOS changes, to what can be written to the partition, to micro segmentation of a network and port blocking*
- Establish a repeatable workflow with MDMs to mitigate vulnerabilities identified at the different software layers of SBOMs

Procurement | Asset Management | Risk Management | **Vulnerability Management**



Discussion

Questions? Comments? Suggestions? Volunteers?