Software Bill of Materials (SBOM)

November 18, 2019

Healthcare Proof of Concept

Unrestricted © Siemens Healthcare GmbH, 2019

Accomplishments

- **Objective:** This is a collaborative effort between healthcare delivery organizations (HDOs) and medical device manufacturers (MDMs) to employ a provisional SBOM format and exercise use cases for SBOM production and consumption. The goal is to demonstrate successful use of SBOMs and relate to the overall cross-sector effort to establish standardized formats and processes.

- **Publication:** The report details scope and use cases, as well as information on SBOM creation by the MDMs, consumption by the HDOs, and the exercising of the Procurement, Asset Management, Risk Management, and Vulnerability Management use cases; https://ntia.gov/sbom

- **Results:** The group demonstrated that the SBOM is an effective tool for MDMs to transfer hitherto unavailable security-related information to HDOs, allowing them to exercise risk management use cases that can be generalized to other verticals. The Proof of Concept identified technical issues that must be addressed in order to become an automated process—a requirement for widespread adoption.

- **Challenges:** Challenges and areas for improvement were identified and documented around an absence of naming standards, partial version information, vulnerability vs exploitation qualification, configuration vulnerabilities, no authoritative end of life database, and lack of patching level data.

Overview of PoC 1.0 Use Cases

Procurement

- Vulnerable/EOL components, system conflicts, and custom software
- Reduction in questionnaires

Risk Management

- Risk assessment
- Compensating control usage

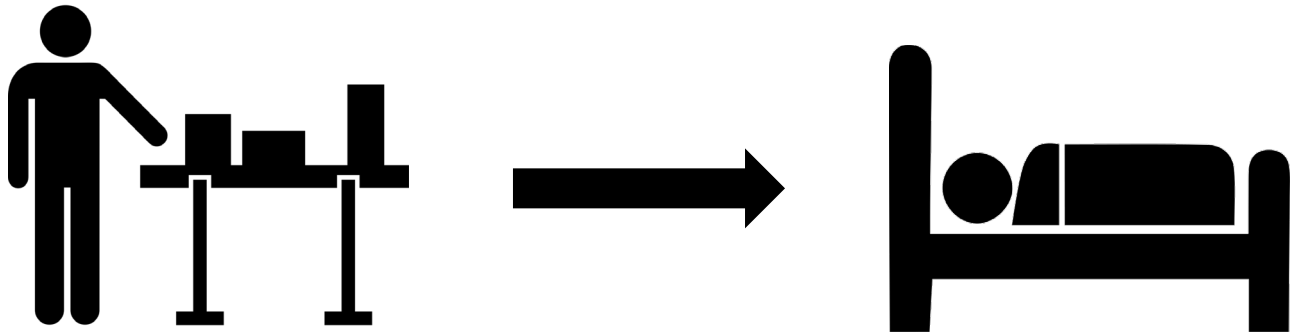
Vulnerability Management

- Ongoing vulnerability identification
- Batch asset querying
- Quantitative analysis

Asset Management (General)

- Lifecycle Management
- Asset Inventory

Bring the Proof of Concept from "Bench to Bedside*"

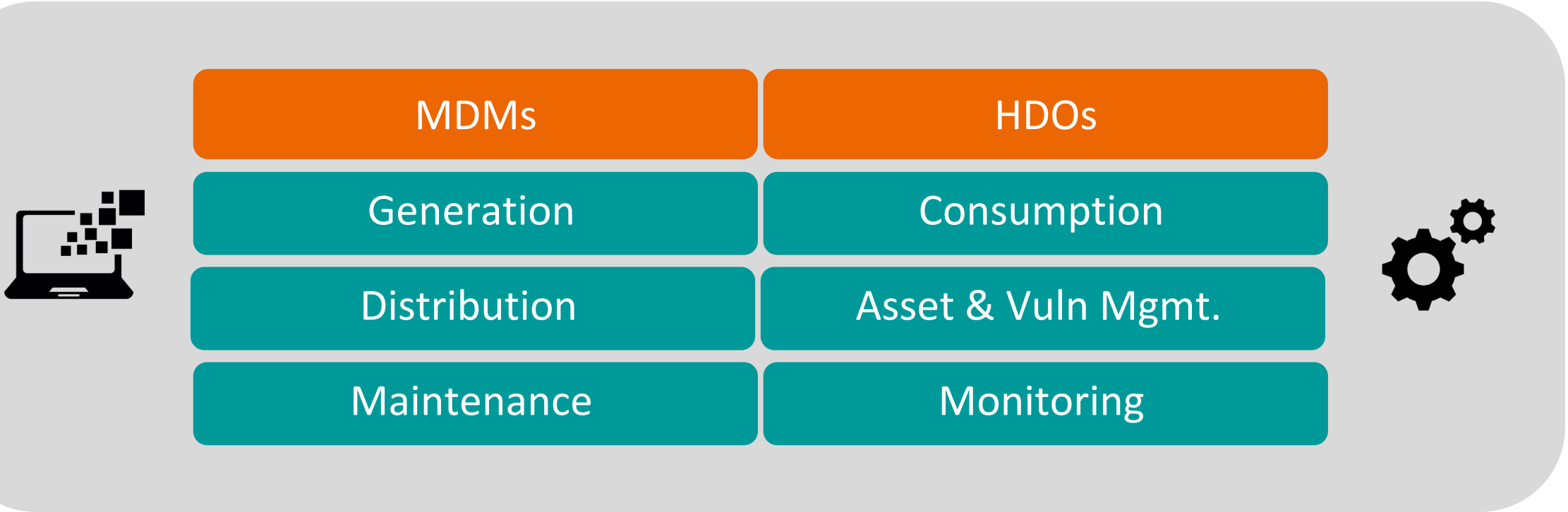


*A term used to describe the process by which the results of research done in the laboratory are directly used to develop new ways to treat patients.

Introduction to PoC 2.0

Organizational Reference Model

1. Identify processes, activities, tasks and other business operations critical for adoption, performance, and management
2. Explore both industry agnostic and industry specific applications
3. Define ecosystem/taxonomy (technology & processes)



Areas for Collaboration

Leverage identified areas for improvement and issues as catalysts for periodic collaboration across working groups:

- Lack of standard naming conventions
- Tooling improvements needed around SBOM generation, Internet delivery, and consumption
- Identification of second, third, fourth, etc. level components within the SBOM (components of components; how many hops)
- Patch level; full versioning
- Proving a method to describe the context of components (allowing HDOs to distinguish between exploitability and vulnerability)

Next Steps

- Solidify and come to a consensus on 2.0 objectives and scope (in/out)
- Identify other industry vertical PoC's for periodic information sharing, feedback, and potential collaboration
- Seeking additional participants from the MDM, HDO, and third party supplier communities (any volunteers?)
- Work towards a start date of **February 5th, 2020** with a formal project kickoff at the remote NTIA meeting in January/February

Open Discussion & Questions