

The Healthcare SBOM Proof of Concept – the History and the Future

SBOM Community 2018



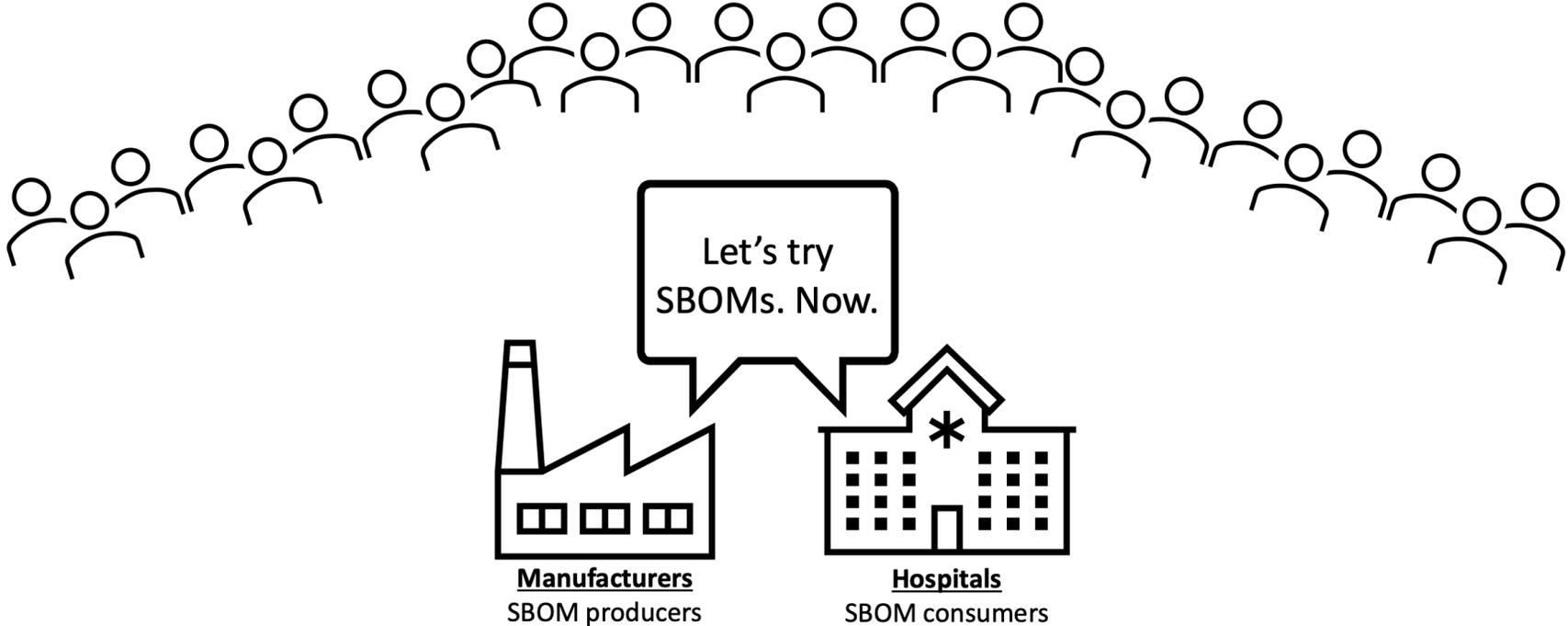
11/06/2018 Software Component Transparency Meeting - Healthcare Proof of Concept

 NTIAGov
1.68K subscribers

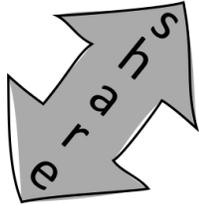
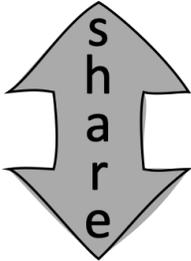
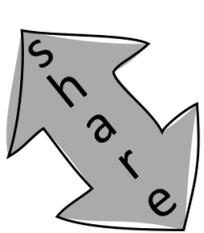
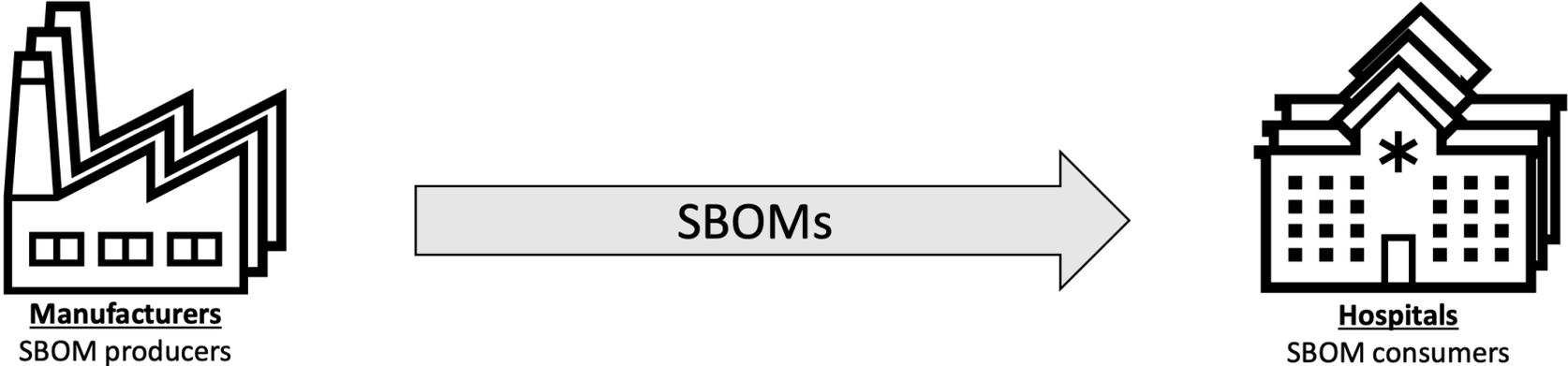
Subscribe

1 Like Comment Share Save ...

**A Healthcare SBOM
Proof of Concept is Born**

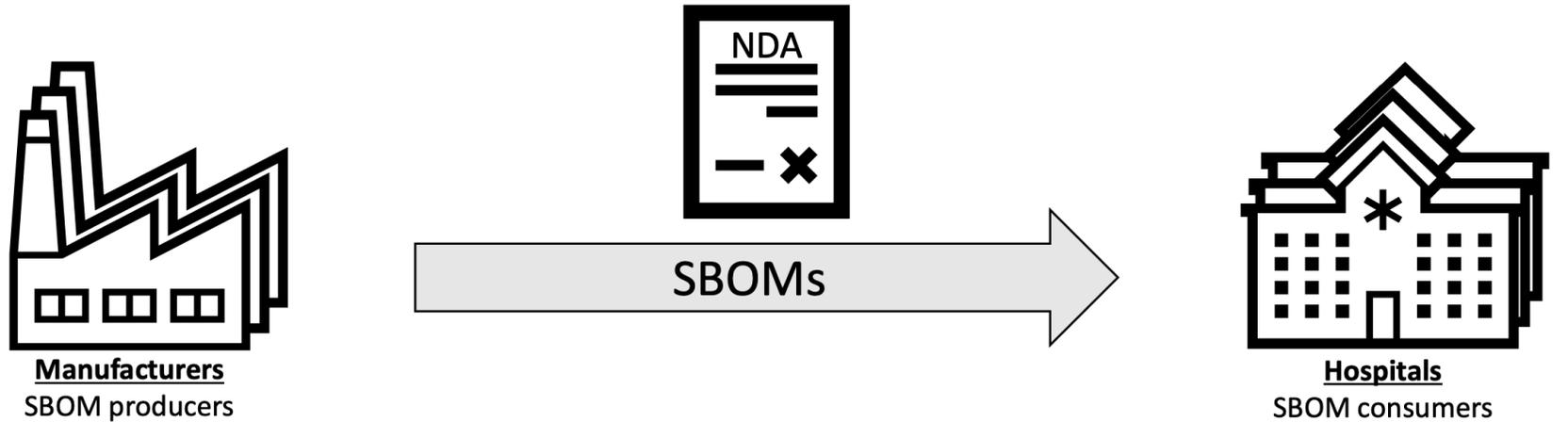


**Healthcare SBOM
Proof of Concept
(Proof of Value)
2019**



Broader Community
- Design and implementation input to PoC participants
- Insights and findings from participants

Healthcare SBOM Proof of Concept (Proof of Value) 2019

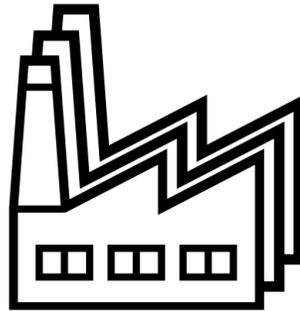


Value to Prove

- Use cases in risk management
- Information on components never previously available

- Procurement
- Asset management
- Vulnerability management

Healthcare SBOM Proof of Concept (Proof of Value) 2019



Manufacturers
SBOM producers



Hospitals
SBOM consumers

Proven Value

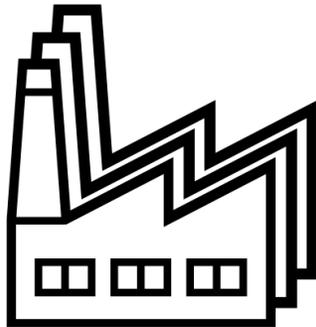
- ✓ Use cases in risk management
- ✓ Transparency information not previously available
- ✓ ***Not specific to healthcare***

<https://tinyurl.com/HealthcareSBOMPOC>

Healthcare SBOM Proof of Concept

Takeaways

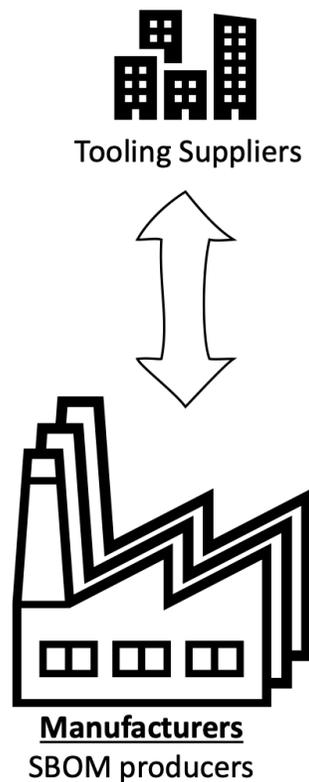
- Build trust:
 - collaboration mindset
 - transparency
- Incremental sophistication
 - crawl, walk, run
- Working with 3rd party vendors
 - grow the ecosystem
- Playbooks for others
- No industry specificity
-  



Manufacturers
SBOM producers

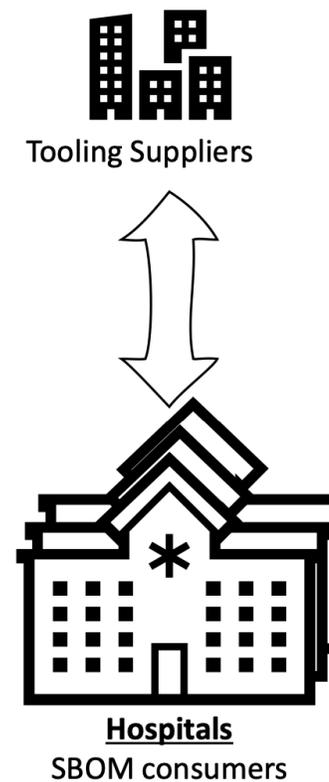
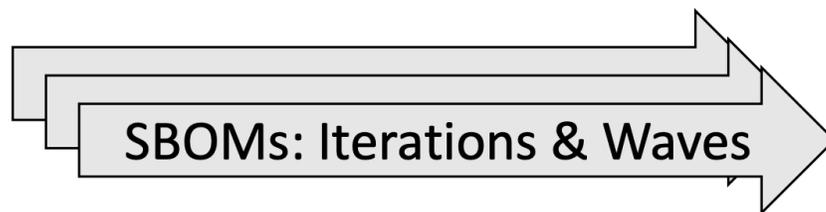


Hospitals
SBOM consumers



Healthcare SBOM
Proof of Concept 2
(Proof of Methods & Capabilities)
2020+

Greater Agility & Structure

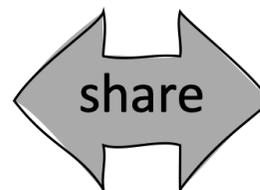


Agile

- Iterations
 incremental sophistication
- Waves
 incremental release of new SBOMs

Methods and Capabilities

- Formats
- Tooling & automation
- Increasing depth
- Contextual information



Broader Community
 Leveraging better defined
 and more sophisticated
 resources

Daggerboard

github.com/nyph-infosec/daggerboard

Product Solutions Open Source Pricing

Search Sign in Sign up

nyph-infosec / daggerboard Public

Notifications Fork 13 Star 79

Code Issues 2 Pull requests 1 Discussions Actions Projects Wiki Security Insights

main 2 branches 4 tags

Go to file Code

About

No description, website, or topics provided.

Readme Code of conduct 79 stars 9 watching 13 forks Report repository

Releases 4

1.0.3 - Daggerboard Latest on Sep 9, 2022

+ 3 releases

Packages

No packages published

File/Folder	Description	Last Commit
kojak-a	Updates to README	0246c3b on Feb 9 51 commits
.attachments	initial commit	last year
.reuse	REUSE Compliant	last year
LICENSES	REUSE Compliant	last year
contributing	Create bug_template.md	last year
daggerboard	Fix chart.js display for sbomscorecard.	last year
daggerboardproject	Updated content security policy (CSP) to remove sources where kno...	last year
grading	REUSE Compliant	last year
uploads/sbom	REUSE Compliant	last year
CODE_OF_CONDUCT.md	Updated Code of Conduct based on Contributor Covenant v2.1	last year
CONTRIBUTING.md	Update CONTRIBUTING.md	last year
README.md	Updates to README	4 months ago
SPDX-DAGGERBOARD-1-0-SBOM-...	initial commit	last year
manage.py	REUSE Compliant	last year

<https://github.com/nyph-infosec/daggerboard> (with a special thanks to Kate and our friends at the Linux foundation)

Daggerboard

Daggerboard 1.0 – Key Features



Daggerboard

An HDO's Perspective: How does the process work?



Select Product

1

Org interested in product and wants to assess security stance



Obtain SBOM

2

Software bill of materials (SBOM) is generated for widely available software, product, etc



Upload to Daggerboard

3

Org uploads SBOM to Daggerboard for analysis



Review Findings

4

Daggerboard outputs list of embedded packages and associated vulnerabilities

Healthcare SBOM Proof of Concept

Phase 3, Iteration 1 (the future)

SBOM

- Additional SBOM content has been uploaded
 - There are now 24 SBOMs available in SPDX or CDX format

VEX

- The team is creating guidance on “When to Publish a VEX Statement”
 - The guidance will build upon the guidance document under development by the CISA VEX Working Group
 - It will be added to the VEX presentation covering the scope of this iteration
- The team is collaborating with the NYP team to determine how to use Daggerboard for this iteration
- The VEX content generation will begin once the plans for using Daggerboard are finalized