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

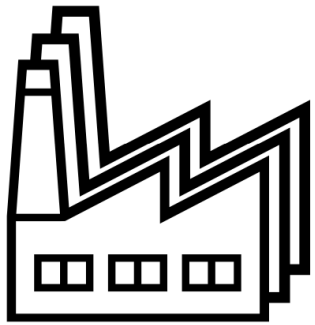
SBOM Community
2018

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

NTIAGov
1.68K subscribers
Subscribe
1
Share
Save

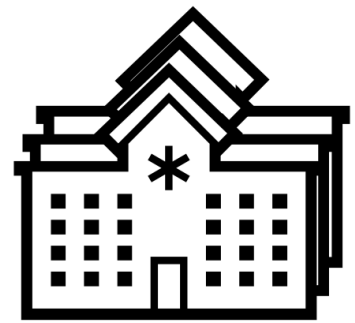
A Healthcare SBOM
Proof of Concept is Born

Healthcare SBOM Proof of Concept (Proof of Value) 2019



Manufacturers
SBOM producers

SBOMs



Hospitals
SBOM consumers

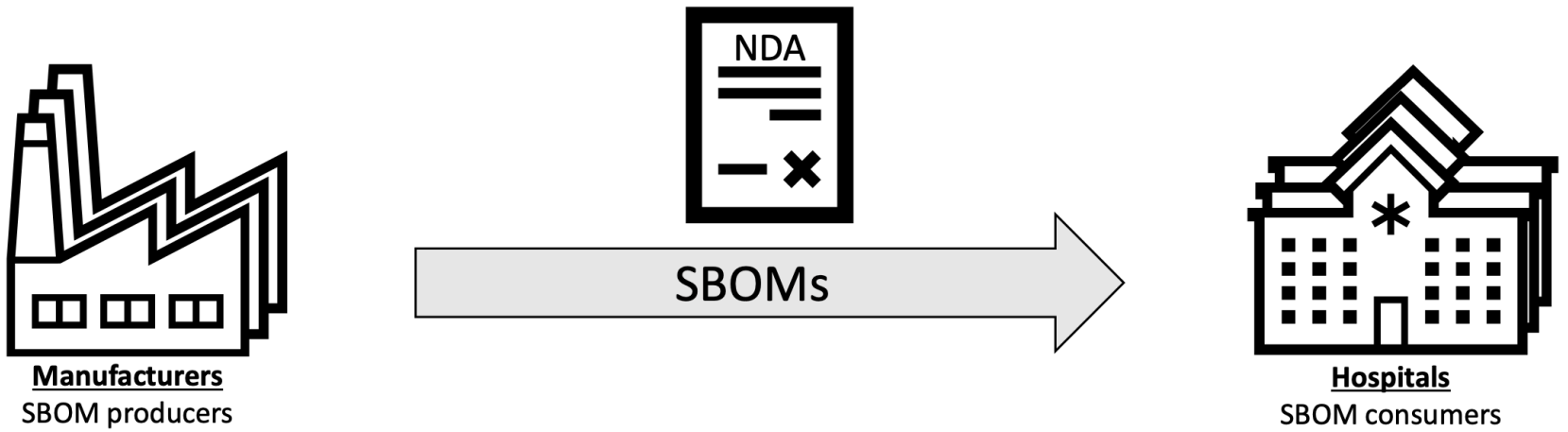
share

share

share

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

Healthcare SBOM
Proof of Concept
(Proof of Value)
2019



Manufacturers
SBOM producers

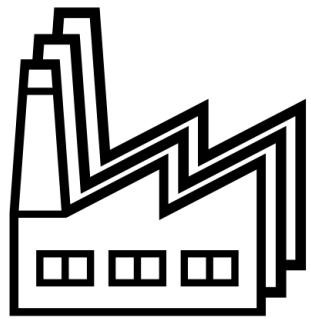
Hospitals
SBOM consumers

Value to Prove

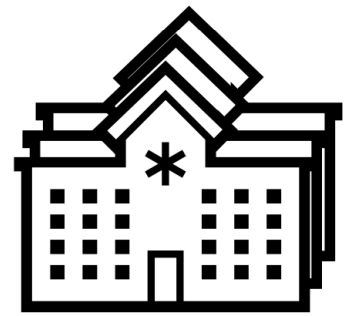
- Use cases in risk management
- Information on components never previously available

- Procurement
- Asset management
- Vulnerability management

Healthcare SBOM
Proof of Concept
(Proof of Value)
2019



Manufacturers
SBOM producers



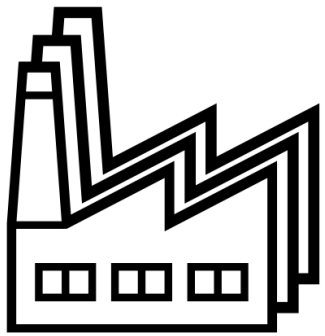
Hospitals
SBOM consumers

Proven Value

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

https://tinyurl.com/HealthcareSBOMPOC

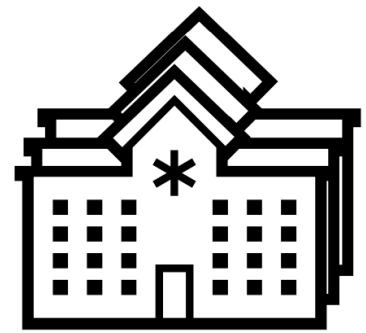
Healthcare SBOM
Proof of Concept



Manufacturers
SBOM producers

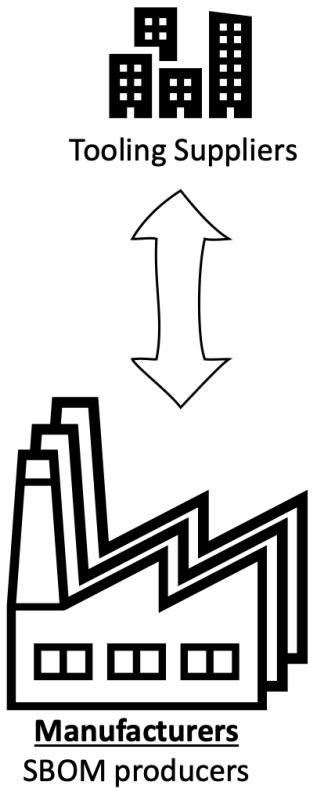
Takeaways

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

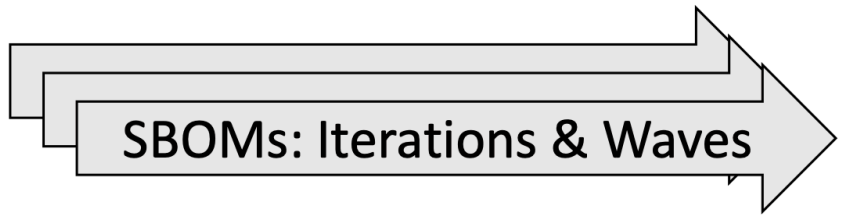


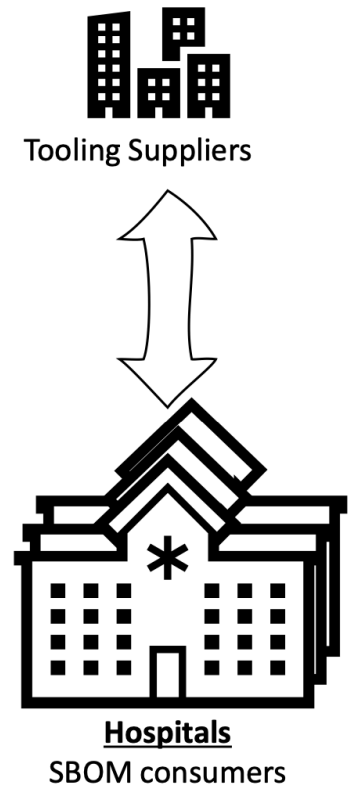
Hospitals
SBOM consumers

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



Greater Agility & Structure



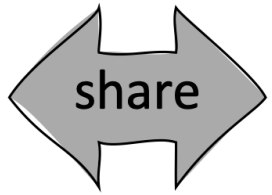


Agile

- Iterations
  - incremental sophistication
- Waves
  - incremental release of new SBOMs

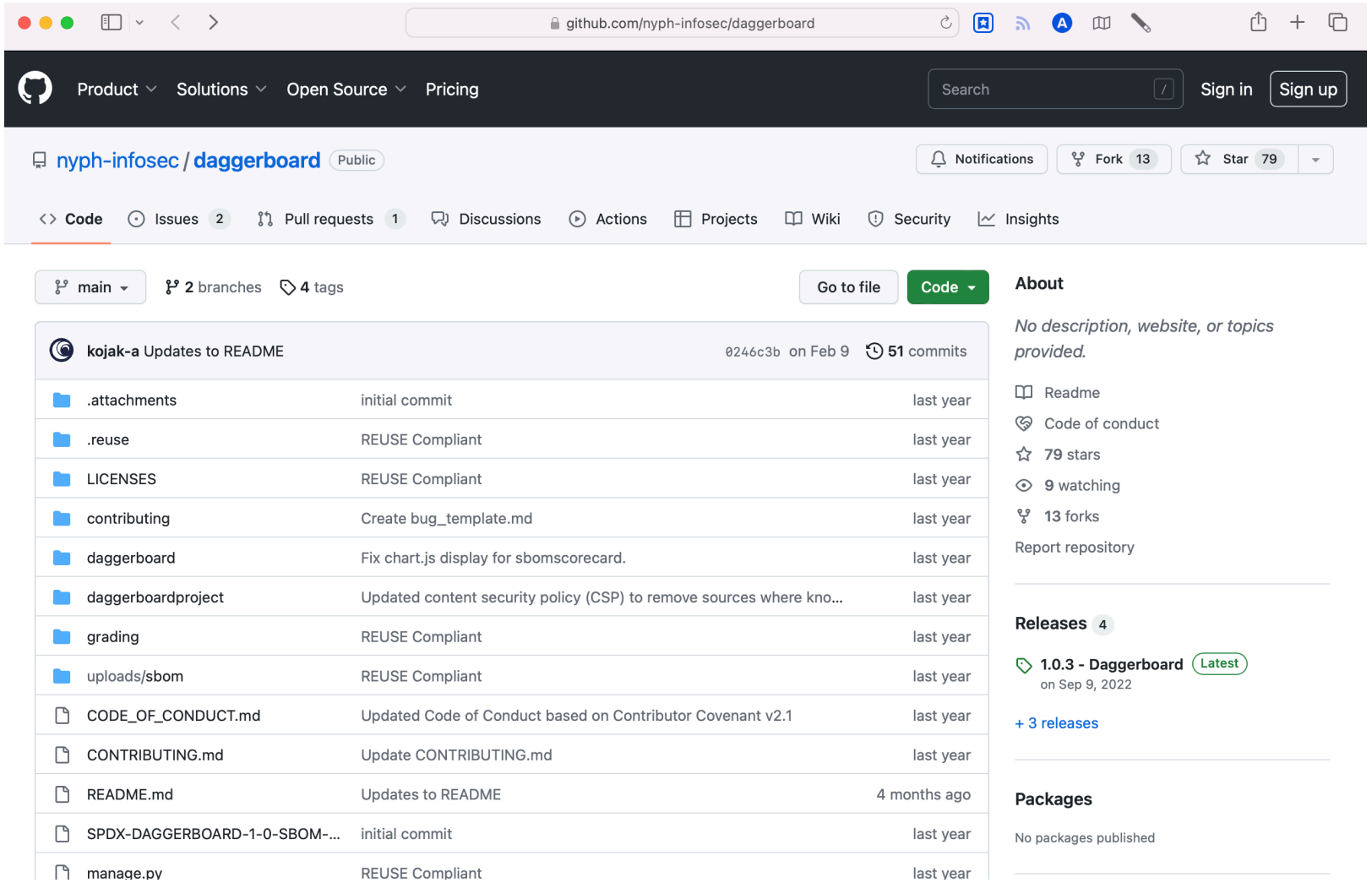
Methods and Capabilities

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



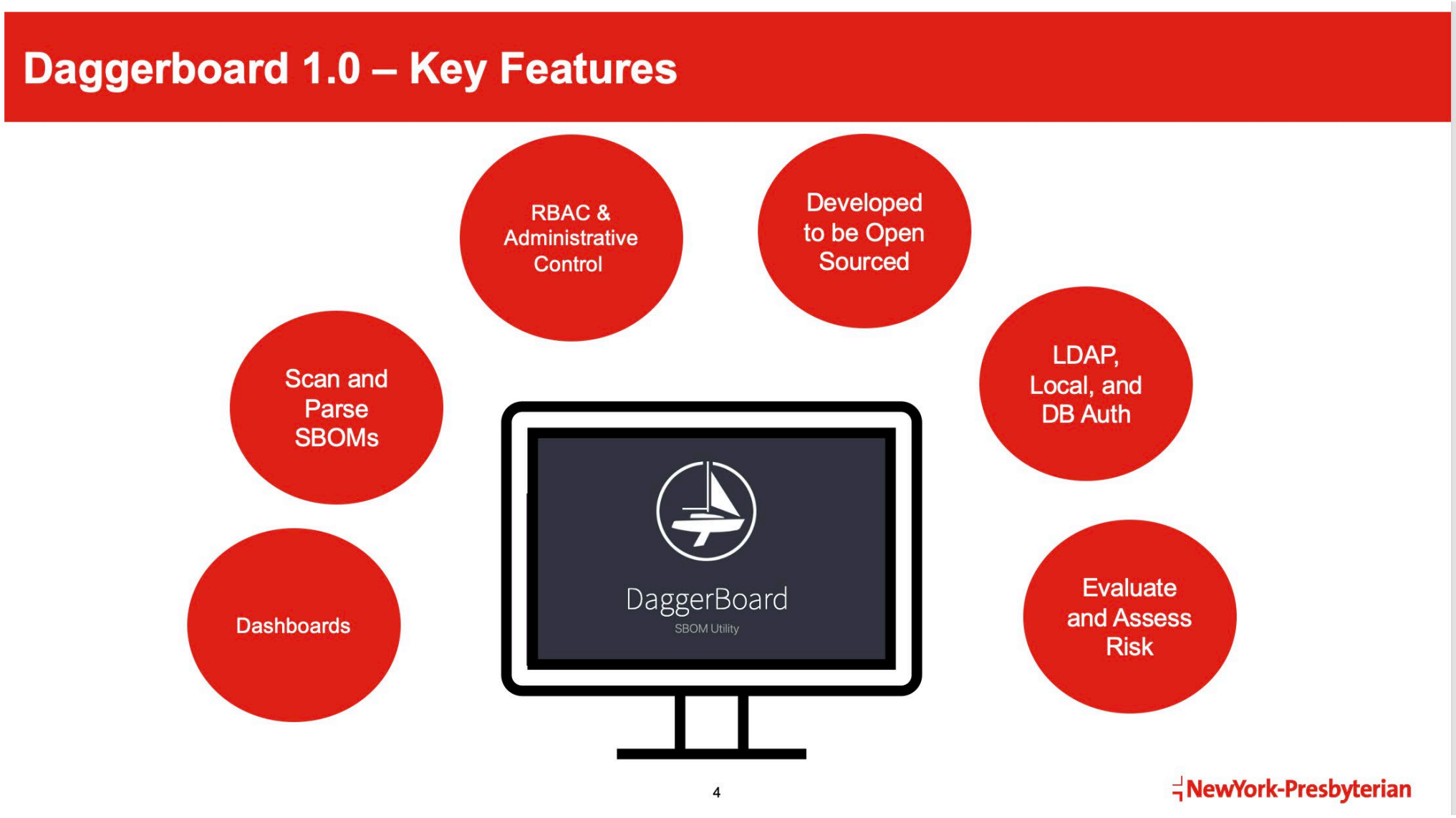
Broader Community
Leveraging better defined and more sophisticated resources

Daggerboard



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

Daggerboard



NewYork-Presbyterian

Daggerboard

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

NewYork-Presbyterian

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