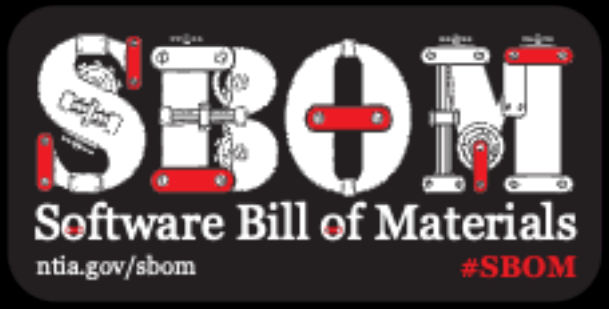
How We Learned to Stop Worrying and love the SBOM

Allan Friedman, PhD
National Telecommunications & Information Administration
US Department of Commerce
afriedman@ntia.doc.gov @allanfriedman
https://ntia.gov/SBOM



Dr. Friedman

Or: How We Learned to Stop Worrying and Love the SBOM

afriedman@ntia.doc.gov https://ntia.gov/SBOM @allanfriedman

How many organizations can answer:

Am I potentially affected by $vulnerabilty

URGENT/11

Should I pay attention or look at literally anything else on the Internet?

- Transparency helps markets across the supply chain
  - Some motivating examples
- Progress towards SBOM and transparency
  - The what, the why, and the how
  - Current, ongoing work
- How you can get involved
  - The need to integrate SBOM data into existing security flows
  - Join this international, cross-sector community
  - SBOM – ask for it by name!

INGREDIENTS: ENRICHED BLEACHED WHEAT FLOUR [FLOUR, REDUCED IRON, "B" VITAMINS (NIACIN, THIAMINE MONONITRATE (B1), RIBOFLAVIN (B2), FOLIC ACID)], WATER, SUGAR, CORN SYRUP, HIGH FRUCTOSE CORN SYRUP, PARTIALLY HYDROGENATED VEGETABLE AND/OR ANIMAL SHORTENING (SOYBEAN, COTTONSEED AND/OR CANOLA OIL, BEEF FAT), WHOLE EGGS, DEXTROSE. CONTAINS 2% OR LESS OF: SOY LECITHIN, LEAVENINGS (SODIUM ACID PYROPHOSPHATE, BAKING SODA, CORNSTARCH, AND MONOCALCIUM PHOSPHATE) WHEY, MODIFIED CORN STARCH, GLUCOSE, SOY FLOUR, SALT, MONO AND DIGLYCERIDES, CELLULOSE GUM, CORNSTARCH, SODIUM STEAROYL LACTYLATE, NATURAL AND ARTIFICIAL FLAVOR, SORBIC ACID (TO RETAIN FRESHNESS), POLYSORBATE 60, SOY PROTEIN ISOLATE, CALCIUM AND SODIUM CASEINATE, YELLOW 5, RED 40. 518701

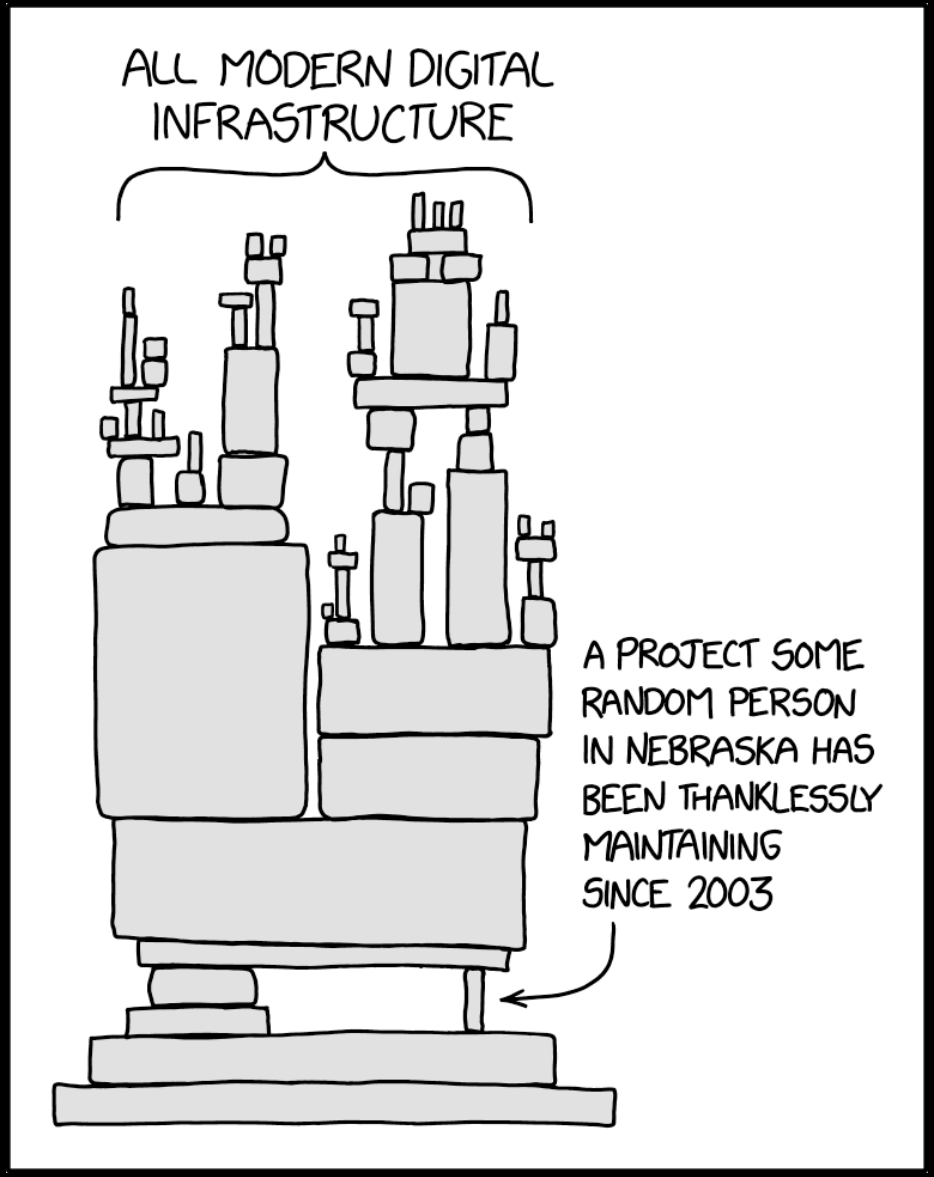
CONTAINS WHEAT, EGG, MILK AND SOY

212016_MP

OUR [FLOUR, REDUCED IRON, "B"
1), RIBOFLAVIN (B2), FOLIC ACID)],
TOSE CORN SYRUP, PARTIALLY
MAL SHORTENING (SOYBEAN,
AT), WHOLE EGGS, DEXTROSE.
N, LEAVENINGS (SODIUM ACID
STARCH, AND MONOCALCIUM
H, GLUCOSE, SOY FLOUR, SALT,
CORNSTARCH, SODIUM STEAROYL
VOR, SORBIC ACID (TO RETAIN
FRESHNESS), POLYSORBATE 60, SOY PROTEIN ISOLATE, CALCIUM AND SODIUM
CASEINATE, YELLOW 5, RED 40.
CONTAINS WHEAT, EGG, MILK AND SOY
212016_MP

518701

INGREDIENTS: ENRICHED BLEACHED WHEAT FLOUR [FLOUR, REDUCED IRON, "B" VITAMINS (NIACIN, THIAMINE MONONITRATE (B1), RIBOFLAVIN (B2), FOLIC ACID)], WATER, SUGAR, CORN SYRUP, HIGH FRUCTOSE CORN SYRUP, PARTIALLY HYDROGENATED VEGETABLE AND/OR ANIMAL SHORTENING (SOYBEAN, COTTONSEED AND/OR CANOLA OIL, BEEF FAT), WHOLE EGGS, DEXTROSE. CONTAINS 2% OR LESS OF: SOY LECITHIN, LEAVENINGS (SODIUM ACID PYROPHOSPHATE, BAKING SODA, CORNSTARCH, AND MONOCALCIUM PHOSPHATE) WHEY, MODIFIED CORN STARCH, GLUCOSE, SOY FLOUR, SALT, MONO AND DIGLYCERIDES, CELLULOSE GUM, CORNSTARCH, SODIUM STEAROYL LACTYLATE, NATURAL AND ARTIFICIAL FLAVOR, SORBIC ACID (TO RETAIN FRESHNESS), POLYSORBATE 60, SOY PROTEIN ISOLATE, CALCIUM AND SODIUM CASEINATE, YELLOW 5, RED 40. 518701
CONTAINS WHEAT, EGG, MILK AND SOY
212016_MP



https://xkcd.com/2347/

Agenda

- Ripple20
- CVE-2020-11901
- Exploiting CVE-2020-11901

DEF CON SAFE MODE TALKS

Ripple20

ANDY GREENBERG SECURITY 06.16.2020 09:00 AM

A Legion of Bugs Puts Hundreds of Millions of IoT Devices at Risk

The so-called Ripple20 vulnerabilities affect equipment found in data centers, power grids, and more.

ILLUSTRATION: WIRED STAFF

SECURITY EXPERTS HAVE warned for years that the drive to connect every device imaginable to the internet would offer a bonanza for hackers. Now researchers have found that one chunk of software designed to enable those internet connections is itself riddled with hackable vulnerabilities. As a result, security flaws have ended up in hundreds of


Load: 0%
Batt: 99%
APC
Smart-UPS
750

8:40
◂ Safari

Background

[redacted] Inc.
11 yrs 11 mos

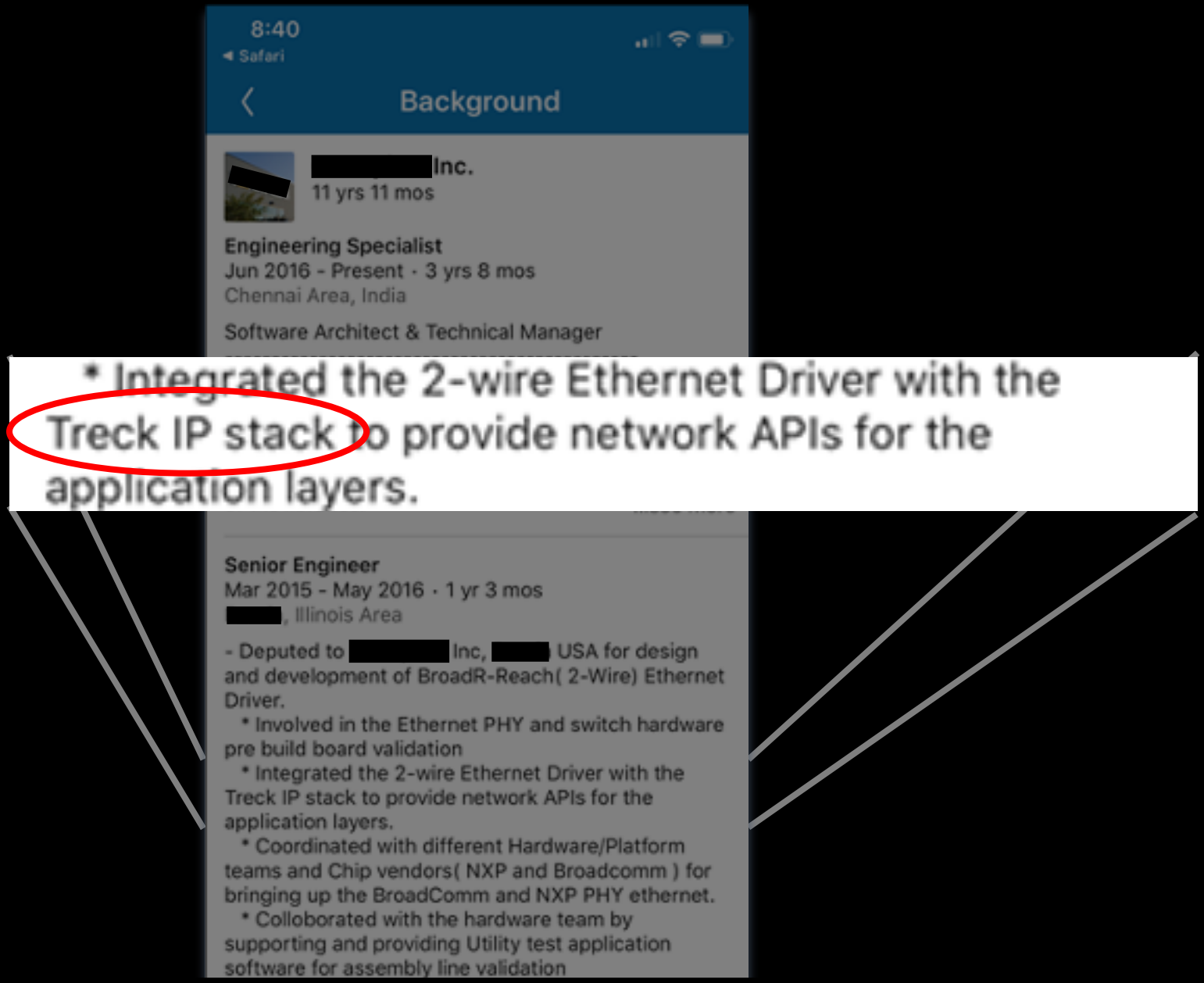
Engineering Specialist
Jun 2016 - Present · 3 yrs 8 mos
Chennai Area, India

Software Architect & Technical Manager

- Primary Datalink Software Architect for the System Common Layer J1939, CDL based datalink libraries and BroadR-Reach Ethernet Drivers.
Accountable and primary contact point, in terms of the quality, Change request and feature enhancement of the libraries. ...see more

Senior Engineer
Mar 2015 - May 2016 · 1 yr 3 mos
[redacted], Illinois Area

- Deputed to [redacted] Inc, [redacted] USA for design and development of BroadR-Reach(2-Wire) Ethernet Driver.
* Involved in the Ethernet PHY and switch hardware pre build board validation
* Integrated the 2-wire Ethernet Driver with the Treck IP stack to provide network APIs for the application layers.
* Coordinated with different Hardware/Platform teams and Chip vendors(NXP and Broadcomm) for bringing up the BroadComm and NXP PHY ethernet.
* Colloborated with the hardware team by supporting and providing Utility test application software for assembly line validation


8:40
Safari
Background
[redacted] Inc.
11 yrs 11 mos
Engineering Specialist
Jun 2016 - Present · 3 yrs 8 mos
Chennai Area, India
Software Architect & Technical Manager
* Integrated the 2-wire Ethernet Driver with the Treck IP stack to provide network APIs for the application layers.
Senior Engineer
Mar 2015 - May 2016 · 1 yr 3 mos
[redacted], Illinois Area
- Deputed to [redacted] Inc, [redacted] USA for design and development of BroadR-Reach(2-Wire) Ethernet Driver.
* Involved in the Ethernet PHY and switch hardware pre build board validation
* Integrated the 2-wire Ethernet Driver with the Treck IP stack to provide network APIs for the application layers.
* Coordinated with different Hardware/Platform teams and Chip vendors(NXP and Broadcomm) for bringing up the BroadComm and NXP PHY ethernet.
* Colloborated with the hardware team by supporting and providing Utility test application software for assembly line validation

Vendor / Brand

3TR6XIR

Vendor / Brand

Orange Sources

Model

unknown

Vendor / Brand

iLLumiShield

Model

unknown

Vendor / Brand

TVT-EA

Model

Unknown

Vendor / Brand

TVT-EA

Model

Unknown

Vendor / Brand

HIKVISON

Model

DS-2CD3332-I

Vendor / Brand

n

Vendor / Brand

Security Camera King

Model

IPOD-PR2

Vendor / Brand

KT&C

Model

KNC-P3TR3XIR

Vendor / Brand

CMPLE

Vendor / Brand

HIKVISON

Vendor / Brand

Hikvison

Model

unknown

[See Asuka Nakajima's OEM Finder](http://oemfinder.ilab.ntt.co.jp/oem)

http://oemfinder.ilab.ntt.co.jp/oem

Vendor / Brand

n

Vendor / Brand

PWS Security

Model

unknown

Vendor / Brand

TSL

Model

Unknown

Vendor / Brand

Eziview

Model

unknown

Vendor / Brand

Security Camera King

Model

TVIOD-PRM2EXIR

Vendor / Brand

Generic

Model

NIU-D4042

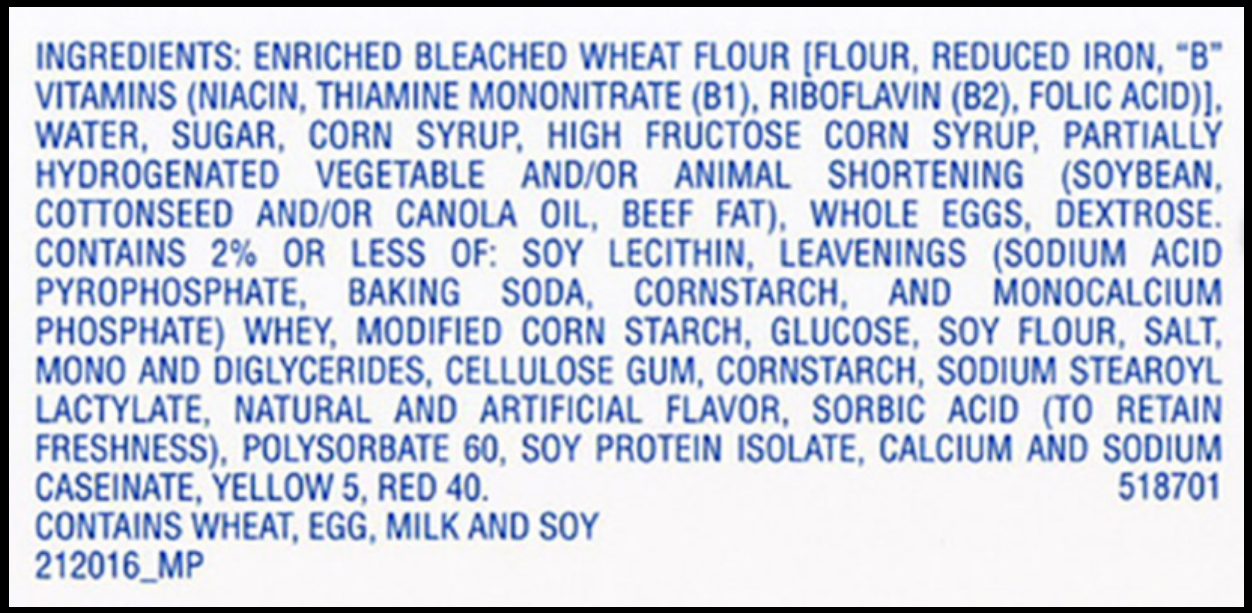
URGENT/11

selected a real time operating system to be provided by Green Hills Software to develop an upgraded em

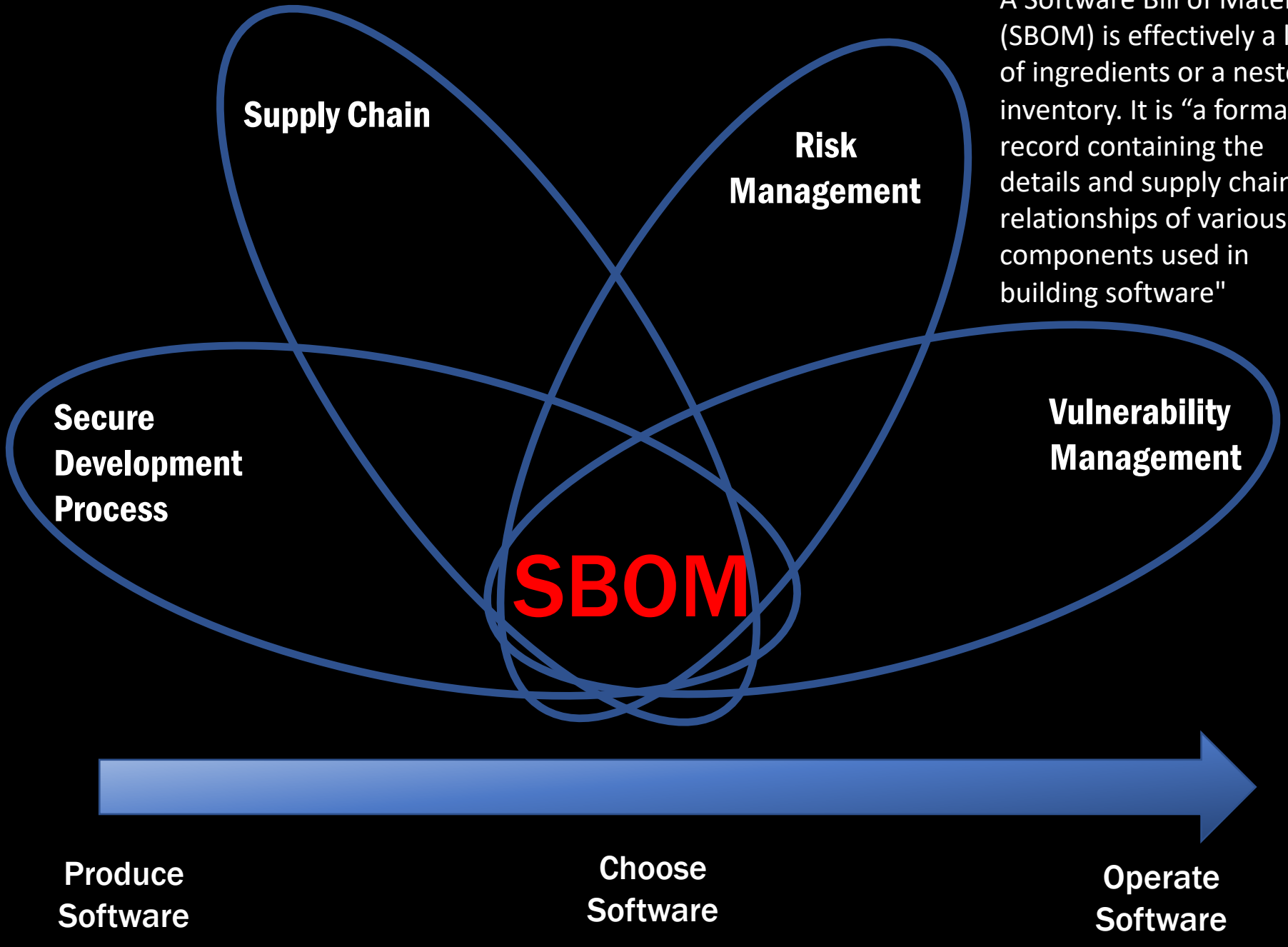
for E-2D Hawkeye and F-22 Raptor aircraft. Photo: U.S. Air Force.

Northrop Grumman selected a real time operating system to be provided by Green Hills Software to develop an upgraded embedded GPS system for E-2D Hawkeye and F-22 Raptor aircraft. Photo: U.S. Air Force.

What is the software equivalent?



INGREDIENTS: ENRICHED BLEACHED WHEAT FLOUR [FLOUR, REDUCED IRON, "B" VITAMINS (NIACIN, THIAMINE MONONITRATE (B1), RIBOFLAVIN (B2), FOLIC ACID)], WATER, SUGAR, CORN SYRUP, HIGH FRUCTOSE CORN SYRUP, PARTIALLY HYDROGENATED VEGETABLE AND/OR ANIMAL SHORTENING (SOYBEAN, COTTONSEED AND/OR CANOLA OIL, BEEF FAT), WHOLE EGGS, DEXTROSE. CONTAINS 2% OR LESS OF: SOY LECITHIN, LEAVENINGS (SODIUM ACID PYROPHOSPHATE, BAKING SODA, CORNSTARCH, AND MONOCALCIUM PHOSPHATE) WHEY, MODIFIED CORN STARCH, GLUCOSE, SOY FLOUR, SALT, MONO AND DIGLYCERIDES, CELLULOSE GUM, CORNSTARCH, SODIUM STEAROYL LACTYLATE, NATURAL AND ARTIFICIAL FLAVOR, SORBIC ACID (TO RETAIN FRESHNESS), POLYSORBATE 60, SOY PROTEIN ISOLATE, CALCIUM AND SODIUM CASEINATE, YELLOW 5, RED 40. 518701
CONTAINS WHEAT, EGG, MILK AND SOY
212016_MP



A Software Bill of Materials (SBOM) is effectively a list of ingredients or a nested inventory. It is “a formal record containing the details and supply chain relationships of various components used in building software"

NTIA's Process on Software Component Transparency

Cross sector

Healthcare

Energy

Auto

ICT

Finance

Government

Entire Supply chain

Open source

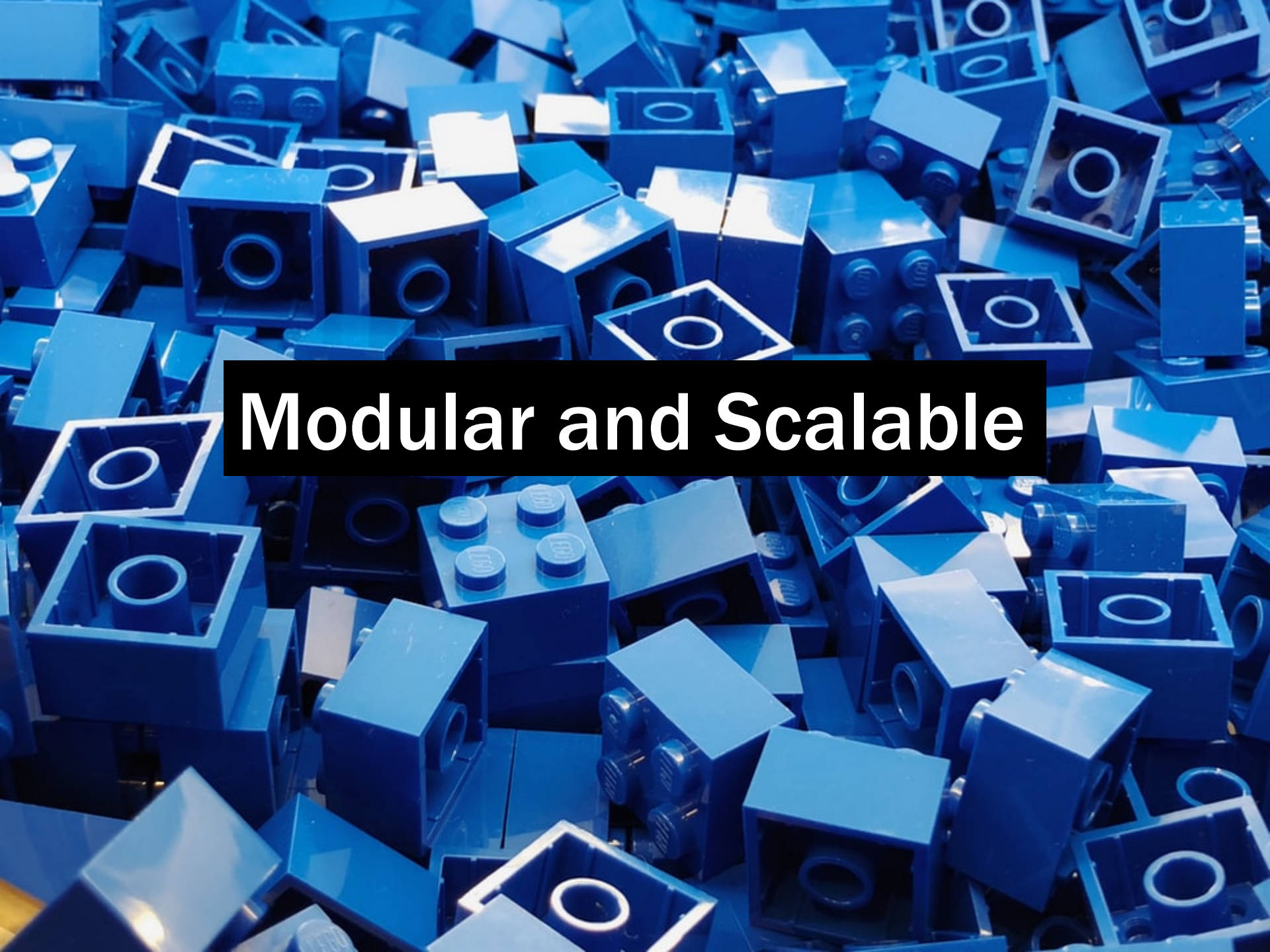
Middleware

Commercial SW

Embedded

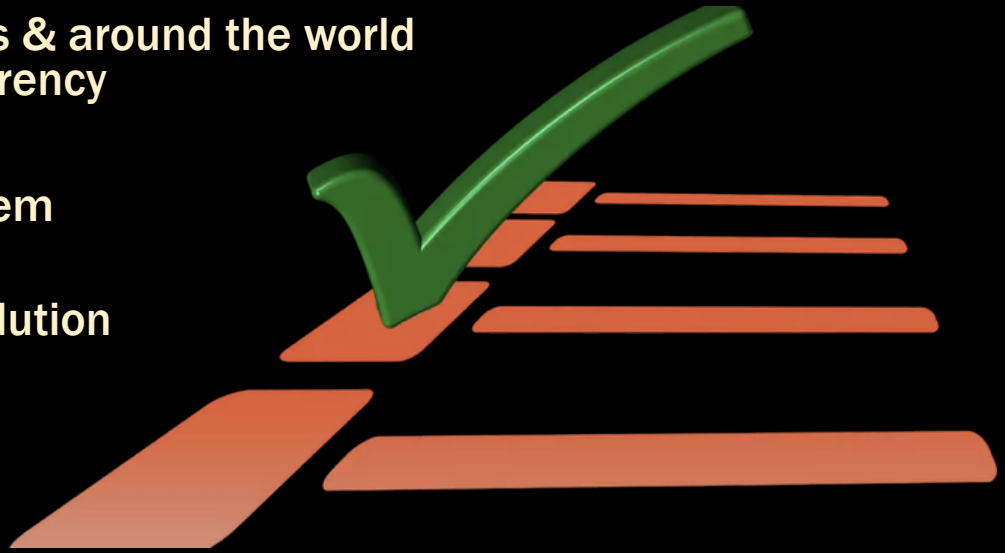
Customers

NTIA's open, transparent, consensus-based processes bring together diverse stakeholders can catalyze real progress across the ecosystem.


Modular and Scalable

Making progress

- Clear appreciation across sectors & around the world on the potential value of transparency
- Consensus on
  - The broad scope of the problem
  - Focus on a baseline SBOM
  - Machine-readability of the solution
  - Modularity and Scalability
- Resources: ntia.gov/SBOM



✓ What is an SBOM

✓ Why should we SBOM

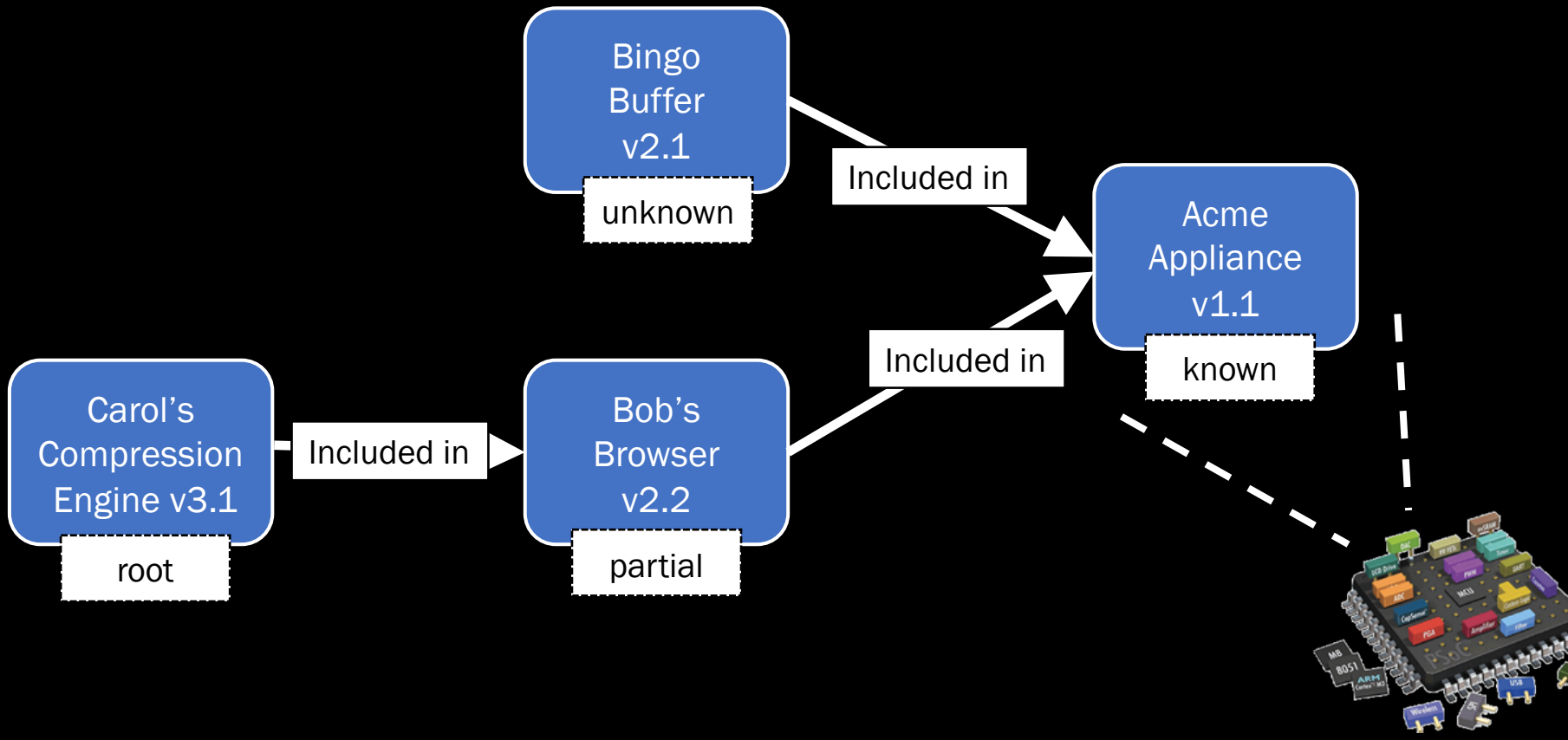
✓ How do we SBOM

✓ Can we SBOM today?

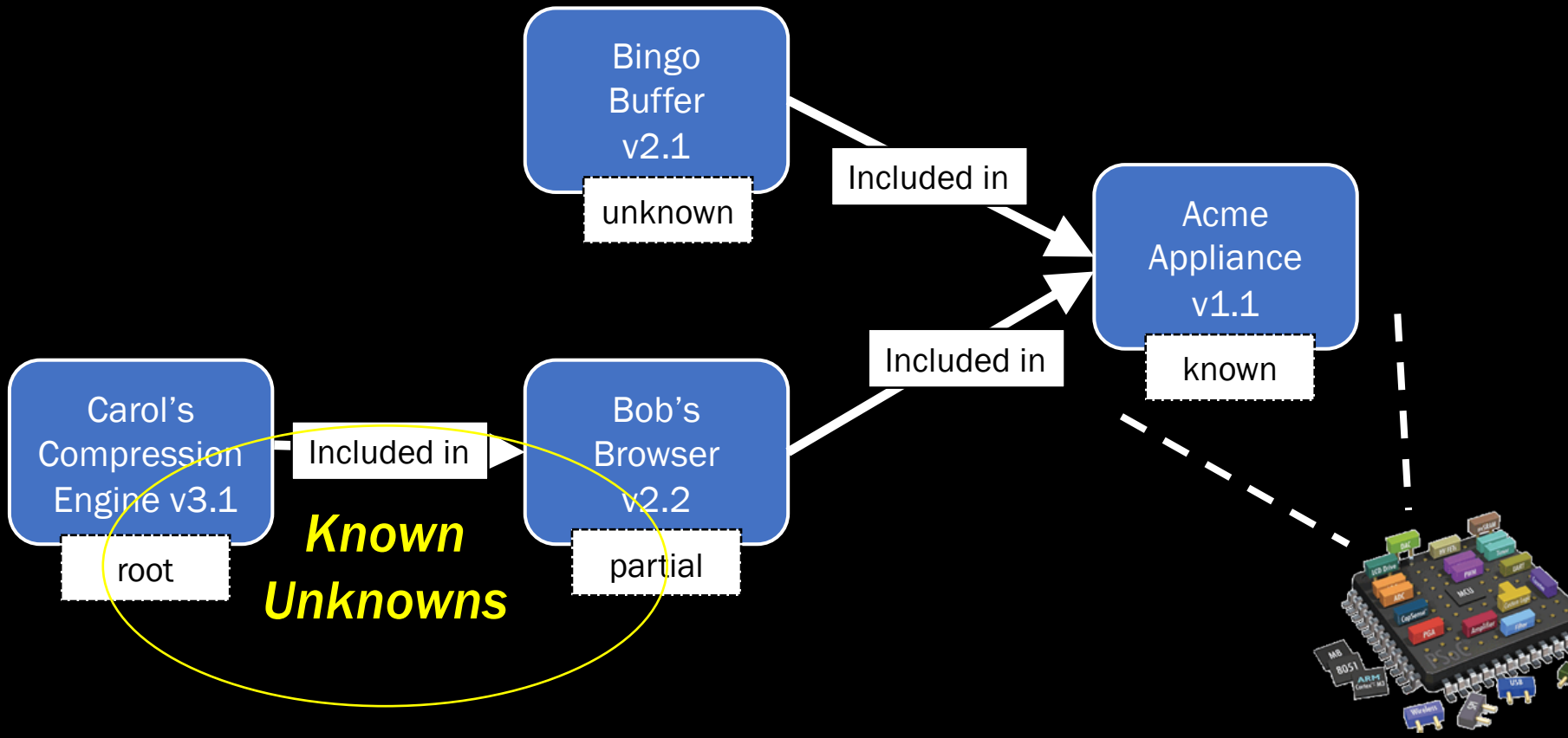
Current work: focus on deployment and SBOMs in the real world

What is an SBoM?

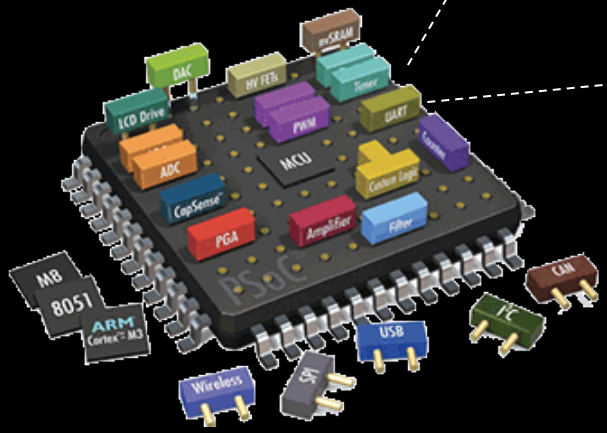
A toy example

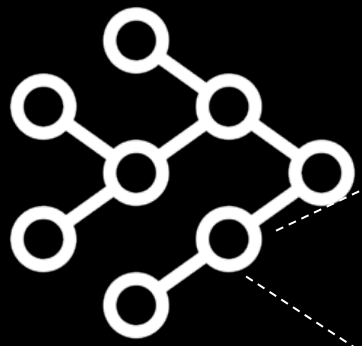


A toy example



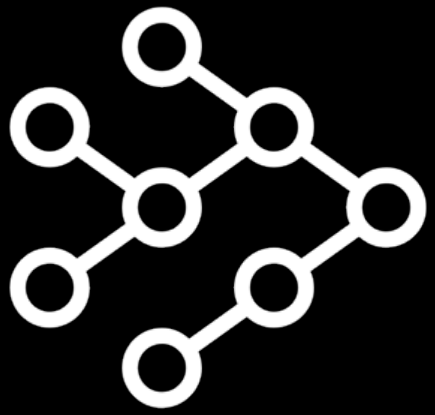
Software Components





Supplier
Component
Version
Hash

How many levels deep?



<u>Must</u> include all top-level includes.
<u>Should</u> ask for includes' SBOMs.
<u>Ideally</u> makes a best-effort for all known components.

Why should we SBoM?

SBOM Roles and Benefits

Produce Software

Understand component and code dependencies

Monitoring/reviewing for vulnerabilities

Awareness of component EOL, orphan, etc.

Enable allow- and deny-lists

Less unplanned maintenance work

Transparency for customers

Choose Software

Identify vulnerable components

Compliance with policies

Awareness of component EOL, orphan, etc.

Show best practices by supplier

Know and comply with licensing

Operate Software

Easily ID vulnerabilities

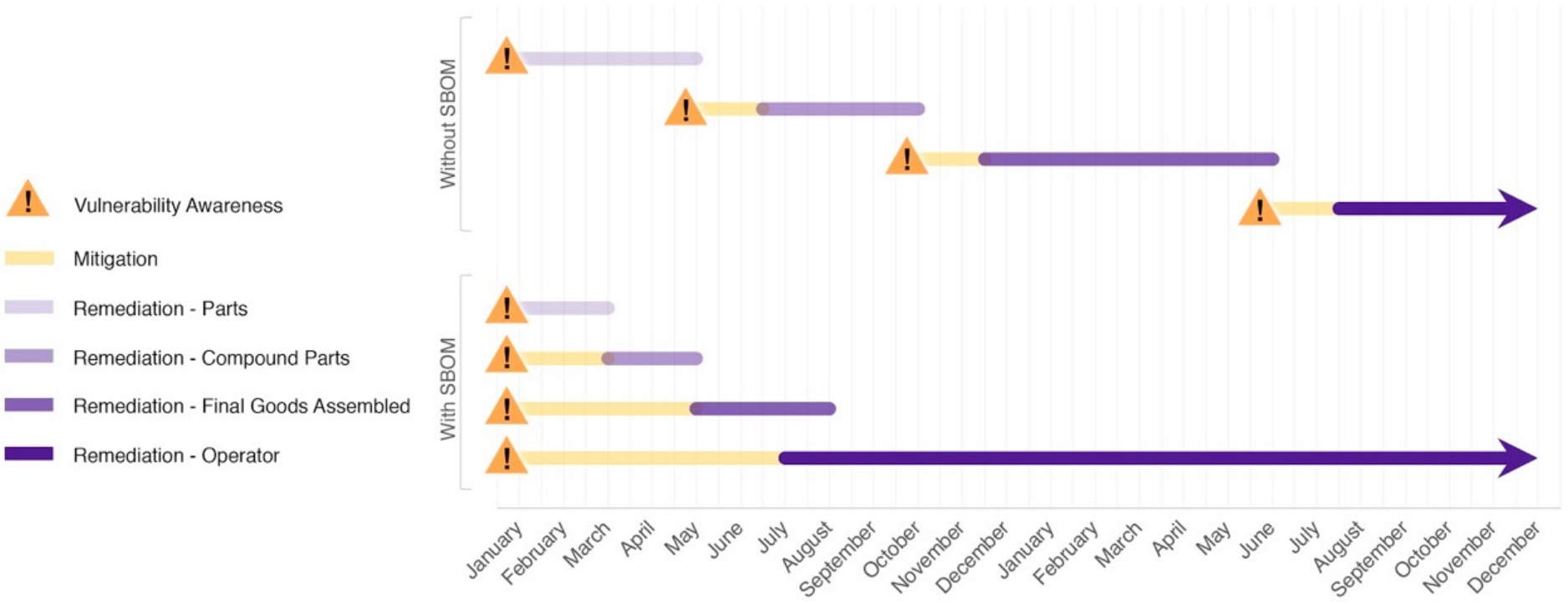
Better risk analysis - “Roadmap for the defender”

Streamline administration

Drive independent mitigations

Time to Remediation Case Studies

Without and With SBOM



Natural Selection
in the SW ecosystem

How do we SBoM?

Three formats to implement SBOM

SPDX is an open standard for communicating software bill of material information (including components, licenses, copyrights, and security references). The SPDX specification is developed by the SPDX workgroup, which is hosted by The Linux Foundation. The grass-roots effort includes representatives from more than 20 organizations—software, systems and tool vendors, foundations and systems integrators.

SWID tags record unique information about an installed software application, including its name, edition, version, whether it is part of a bundle and more. SWID tags support software inventory and asset management initiatives. The structure of SWID tags is specified in international standard ISO/IEC 19770-2:2015.

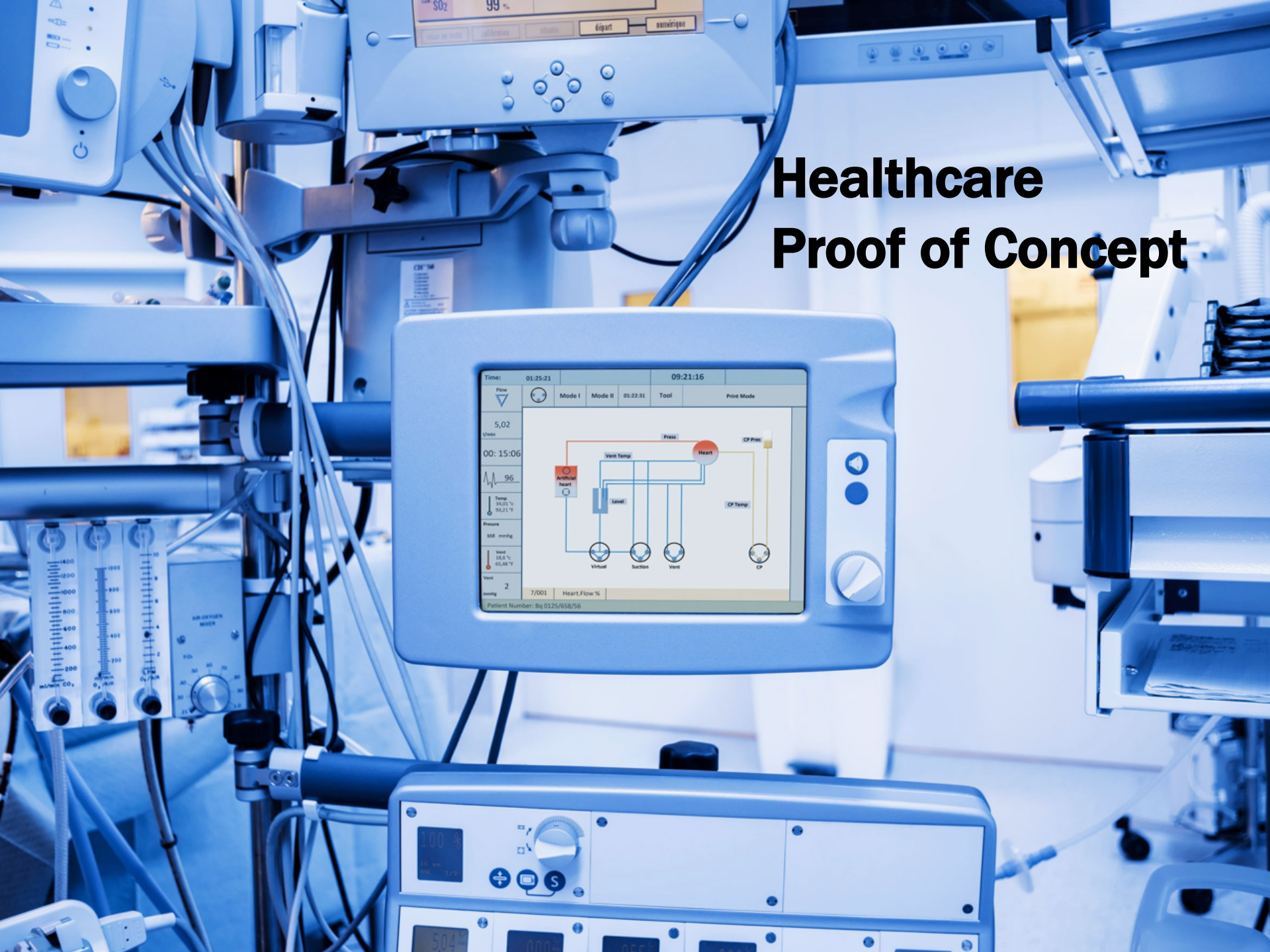
CycloneDX is a lightweight software bill of materials (SBOM) specification originally concieved for use with the OWASP Dependency-Track platform. It is designed for use in application security contexts and supply chain component analysis.

Translation between formats

- We have identified the common elements.
- A ‘multilingual’ ecosystem does not offer too many challenges
- Rather than pick a winner, we will build out guidance to support both formats with effective interoperability.

Implementing core SBOM fields

Field	SPDX	SWID	CycloneDX
Supplier	(3.5) PackageSupplier:	<Entity> @role (softwareCreator/ publisher), @name	publisher
Component	(3.1) PackageName:	<softwareIdentity> @name	name
Unique Identifier	(3.2) SPDXID:	<softwareIdentity> @tagID	bom/serialNumber and component/bom-ref
Version	(3.3) PackageVersion:	<softwareIdentity> @version	version
Component Hash	(3.10) PackageChecksum:	<Payload>/../<File> @[hash-algorithm]:hash	hash
Relationship	(7.1) Relationship: CONTAINS	<Link>@rel, @href	(Nested assembly/subassembly and/or dependency graphs)
SBOM Author	(2.8) Creator:	<Entity> @role (tagCreator), @name	bom-descriptor: metadata/manufacture/ contact


Healthcare
Proof of Concept

Next steps: What we're working on now!

- Refining and extending the model
  - Software namespace
  - Mechanism for sharing SBOM data
  - Vulnerability vs Exploitability
  - High assurance: integrity, pedigree, provenance
  - Cloud & containers
  - Dock with other efforts around supply chain
- Tooling for automation
  - What tools exist today?
  - What tools do we need?
- Awareness and adoption
  - Get the message to the community
  - Draft contract language
  - Further demonstrations in different sectors
- Playbooks and how-to guides

Integrating SBOM Data

Challenge: Software Naming

Challenge: Sharing SBOM data

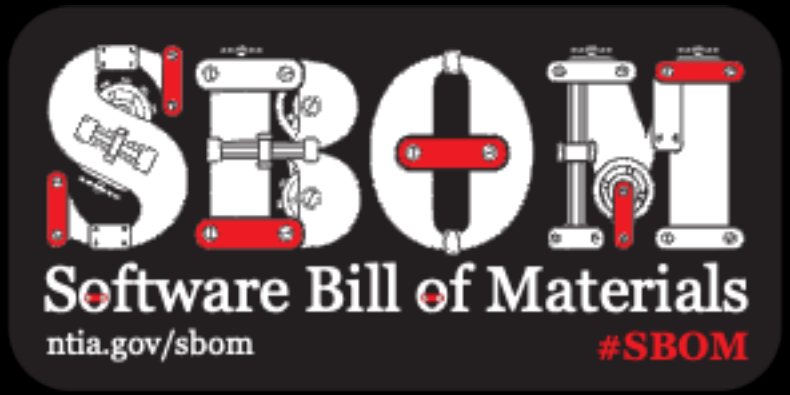
Challenge:

Vulnerability vs. Exploitability


Transparency

To recap...

- Tracking third party components can help understand and address a wide range of risks across the entire ecosystem
- Cross-sector supply-chain driven approach
  - What a Software Bill of Materials is
  - Why it can help across the supply chain
  - How we can implement it
- Sectors and orgs can shape their own future through Proof-of-Concept exercises
- Ongoing work needs your help to build and use SBOM data



Get involved in the NTIA process!

Contact: afriedman@ntia.gov

Read: ntia.gov/SBOM

Join the conversation

@allanfriedman #SBOM