RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **GPS1-F02V**

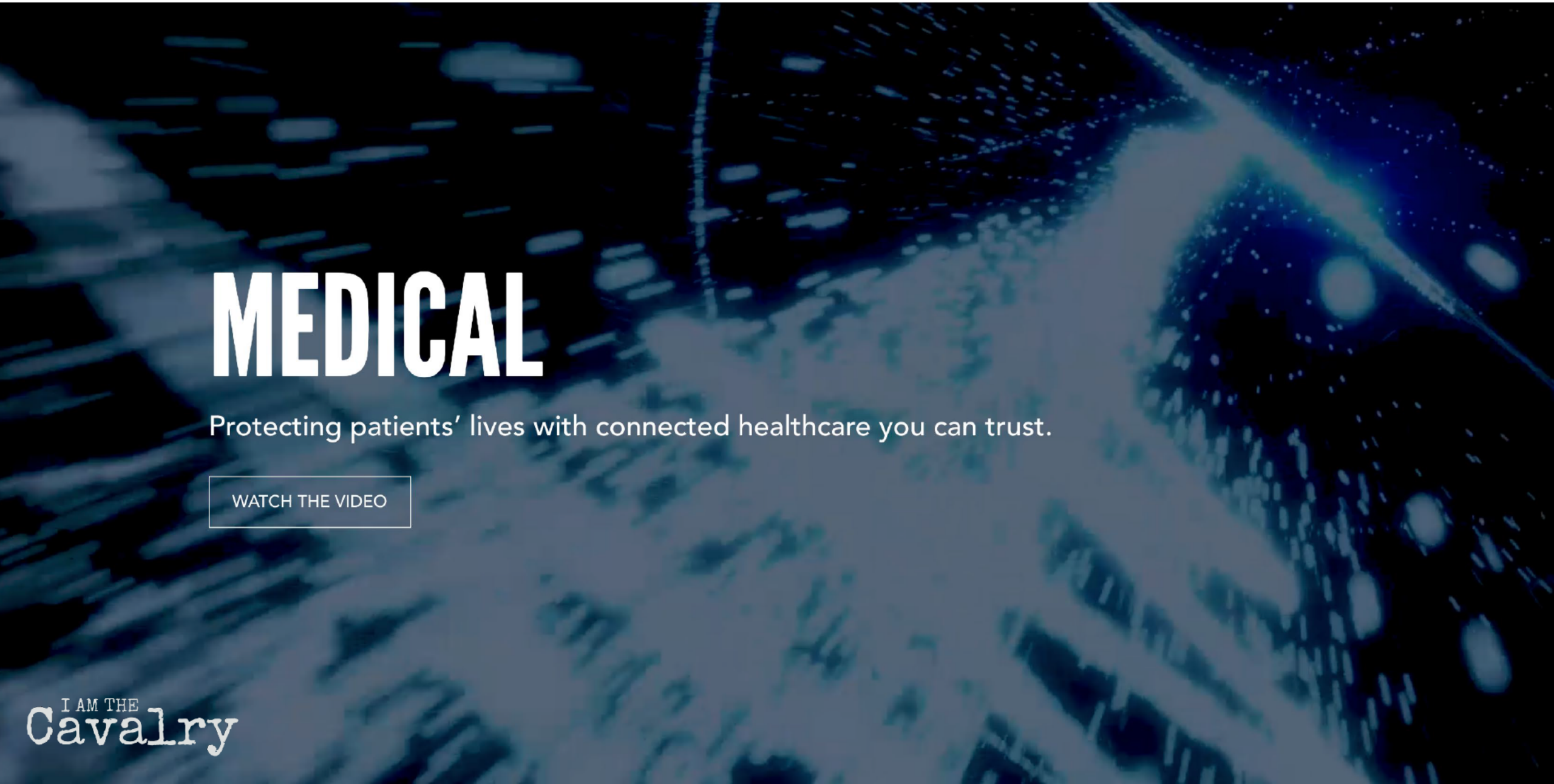
Taking Control of Cyber Supply Chain Security

Beau Woods

Cyber Safety Advocate
I Am The Cavalry
@beauwoods

Allan Friedman, PhD

Director of Cybersecurity Initiatives
NTIA / U.S. Department of Commerce
@allanfriedman
afriedman@ntia.gov


MEDICAL
Protecting patients' lives with connected healthcare you can trust.
WATCH THE VIDEO
I AM THE
Cavalry


WIND
WHEN IT MATTERS, IT RUNS ON WIND RIVER.
Contact Us
Search
Menu
VxWorks
WATCH THE VIDEO

URGENT/11

Green Hills Platform for Avionics

- The proven provider
- Absolute reliability
- Proven in safety-critical systems
- In-house certification expertise
- Proven pedigree
- Complete safety-critical line

Green Hills Software products are the leading choice for the avionics industry. The company's full line of safety and security critical products are being used in almost every current and next-generation aircraft, including: the Airbus A380, Boeing 777, Boeing 787, Lockheed Martin F-35 Joint Strike Fighter, F/A-22, Eurofighter Typhoon, Lockheed Martin F-16, Bell Helicopter UH-1Y and AH-1Z helicopters (on the Northrop Grumman mission computers), the Textron RQ-7B Shadow UAS (on the Rockwell-Collins mission computer), and more.

The proven provider of safety & security solutions

Green Hills Platform for Avionics combines the INTEGRITY-178 RTOS with support for aviation industry standard ARINC 653-1 application software interface, and the documentation required for FAA safety certification. INTEGRITY-178 has proven iteself many times by being certified to this top safety-critical level in multiple applications. It is now the leading RTOS choice for the avionics industry for current and next generation aircraft.

The list of avionics suppliers that have selected Green Hills Software solutions is the who's who for this industry and includes: BAE Systems, Boeing, CMC Electronics, EADS, General Electric, Honeywell, Lockheed Martin, Northrop

URGENT/11


interpeak
secure networking software

interpeak

secure networking software

- > INTEGRITY
- > ITRON
- > Linux/MontaVista
- > MQX
- > Nucleus
- > OSE, OSEck
- > ThreadX
- > velOSity
- > VxWorks

Software Supply Chains and the Need for Transparency

- Supply chain risks are growing
- Supply chains are long and opaque
- A “software bill of materials” offers actionable intelligence
- SBOMs are coming, and you can help shape that future

RSAConference2020 APJ

A Virtual Learning Experience

“supply chain”

You keep using that word..

Suppliers to the new BMW 5 Series

Image source: BMW AG

ROOF MODULE WITH GESTURE RECOGNITION SYSTEM
DELPHI

HARMAN KARDON SOUND SYSTEM
HARMAN/BECKER

PYROTECHNICAL SAFETY SWITCH
AUTOLIV

NEXT GEN CARBON CANISTER
KAUTEX TEXTRON

COMPRESSOR WITH CLUTCH
DENSO

CYLINDER HEAD GASKET
DANA

CLASSICAL SUNROOF
WEBASTO

OIL FILTER MODULE
UFI FILTERS

SMART OPENER
BROSE

MECHANICAL PUMP
SALERI

TRANSMISSION OIL COOLER
MAHLE

SOUND DEADENER PACKAGE
FAIST CHEMTEC

THERMO MANAGEMENT MODULES
SCHAEFFLER

CO-EXTRUDED ARMREST SEAL [TIER 2]
COBA PLASTICS

FRONT ARMREST DAMPERS
CULTRARO AUTOMAZIONE ENGINEERING

DAMPER FORKS
HIRSCHVOGEL UMFORMTECHNIK

PNEUMATIC LUMBAR SUPPORT
KONGSBERG AUTOMOTIVE

SEALING SIDE PANEL
RÖCHLING AUTOMOTIVE

FRONT & REAR WIPER SYSTEM
VALEO

LASER WELDED BLANK
VOESTALPINE

TRUNK LIGHT STRIP
GRUPO ANTOLIN

ROOF MOULDINGS
SMIA

EXHAUST TRIM
TAJCO A/S

BACKLITE
CARLEX

DOUBLE NUT
AMTEK TEKFOR

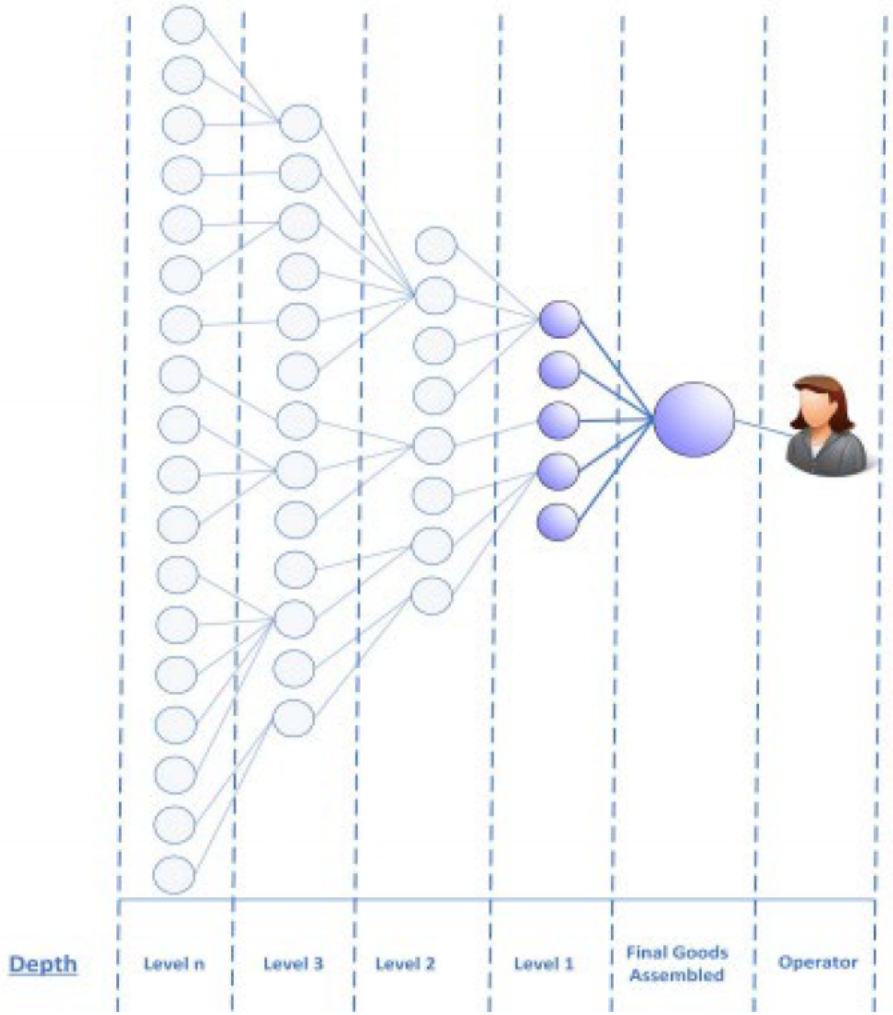
VALVE COTTERS
FEDERAL-MOGUL

FRONT & REAR SEATBELTS
AUTOLIV

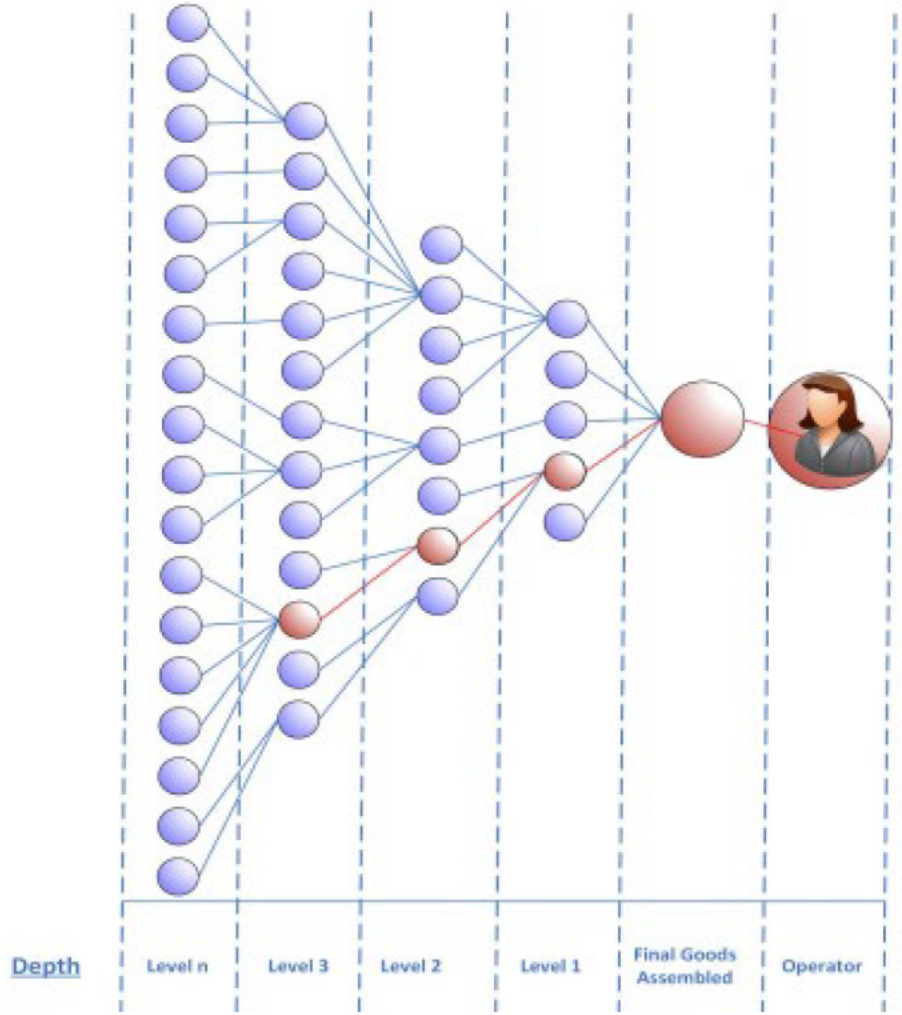
TRAILER COUPLING SWITCH
MARQUARDT

STORAGE COMPARTMENT
MEGATECH INDUSTRIES

FORGING WHEELS
SUPERALLOY INDUSTRIAL CO. LTD

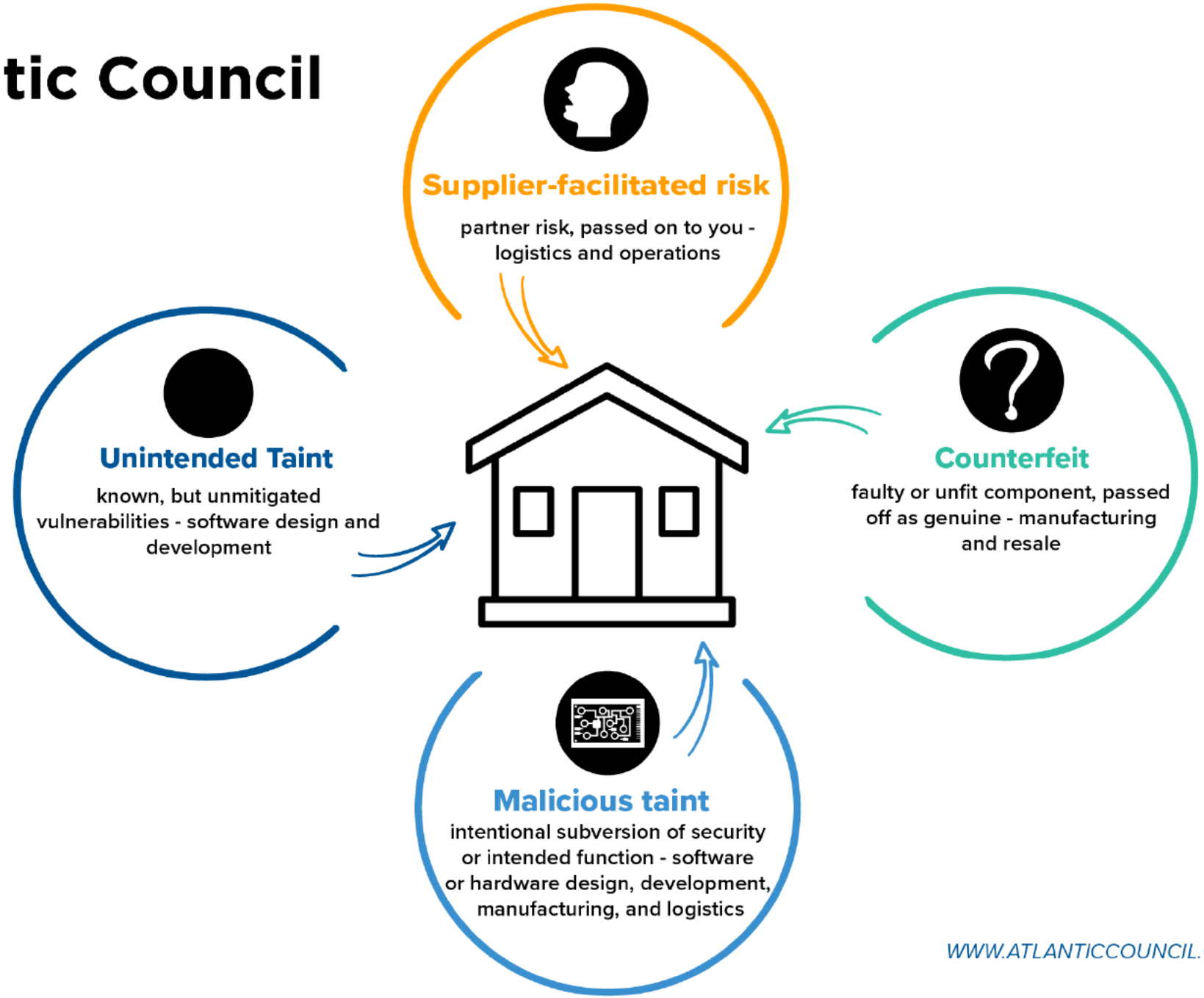


Limited visibility enables less awareness of risk



More complete visibility enables more complete awareness of risk

Atlantic Council



What can we do about it?

Three perspectives across the supply chain

Produce Software

Choose Software

Operate Software

Use Cases: Producing software

- Monitor for vulnerabilities in components
- Better manage code base & minimize bloat
- Execute allowed or excluded software practices
- Prepare and respond to end-of-life contingencies
- Know and comply with l
- Provide an SBOM for cu

I AM THE Cavalry

NTIA

Use Cases: Choosing software

- Identify known vulnerabilities
- More targeted security analysis
- Compliance
- EOL awareness
- Verify sourcing & supplier claims
- Understand software integration
- Market signal of secure development process.

I AM THE Cavalry

NTIA

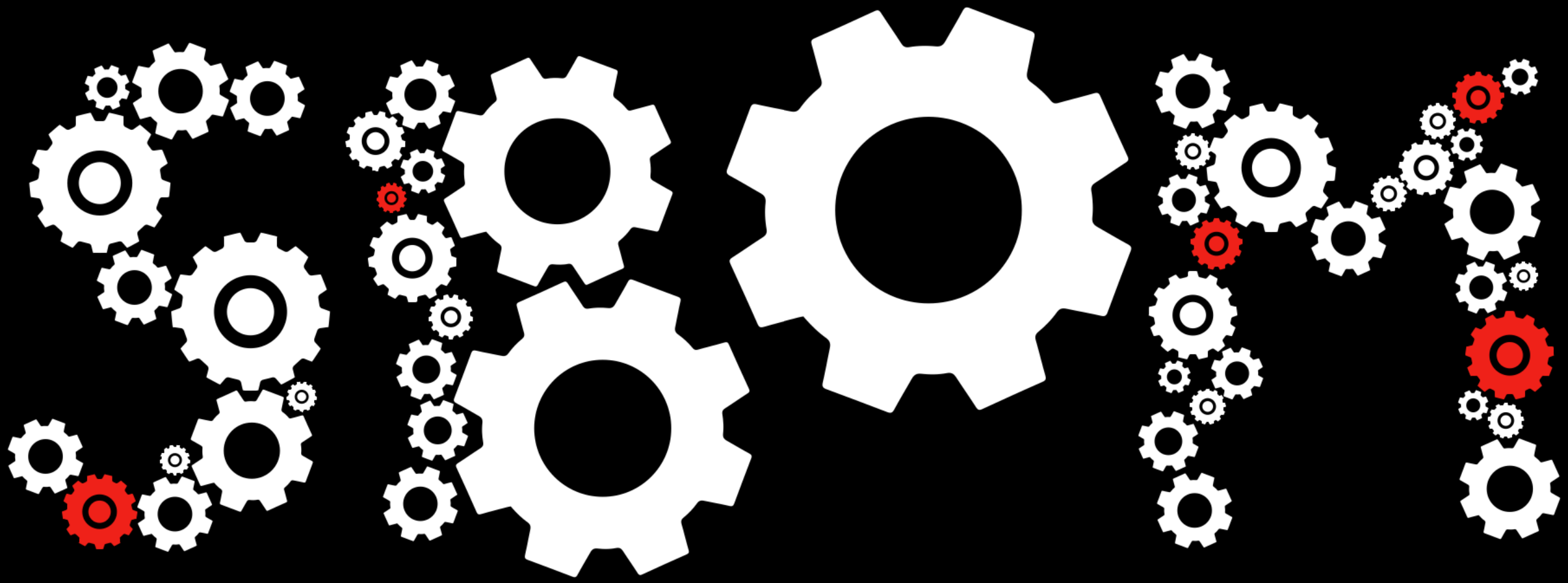
Use Cases: Operating Software

- Vulnerability management
- Better understanding of operational risks
- Real time data on components in assets
- Improved understanding of potential exploit
- Enable potential non-SW mitigations

I AM THE Cavalry

NTIA

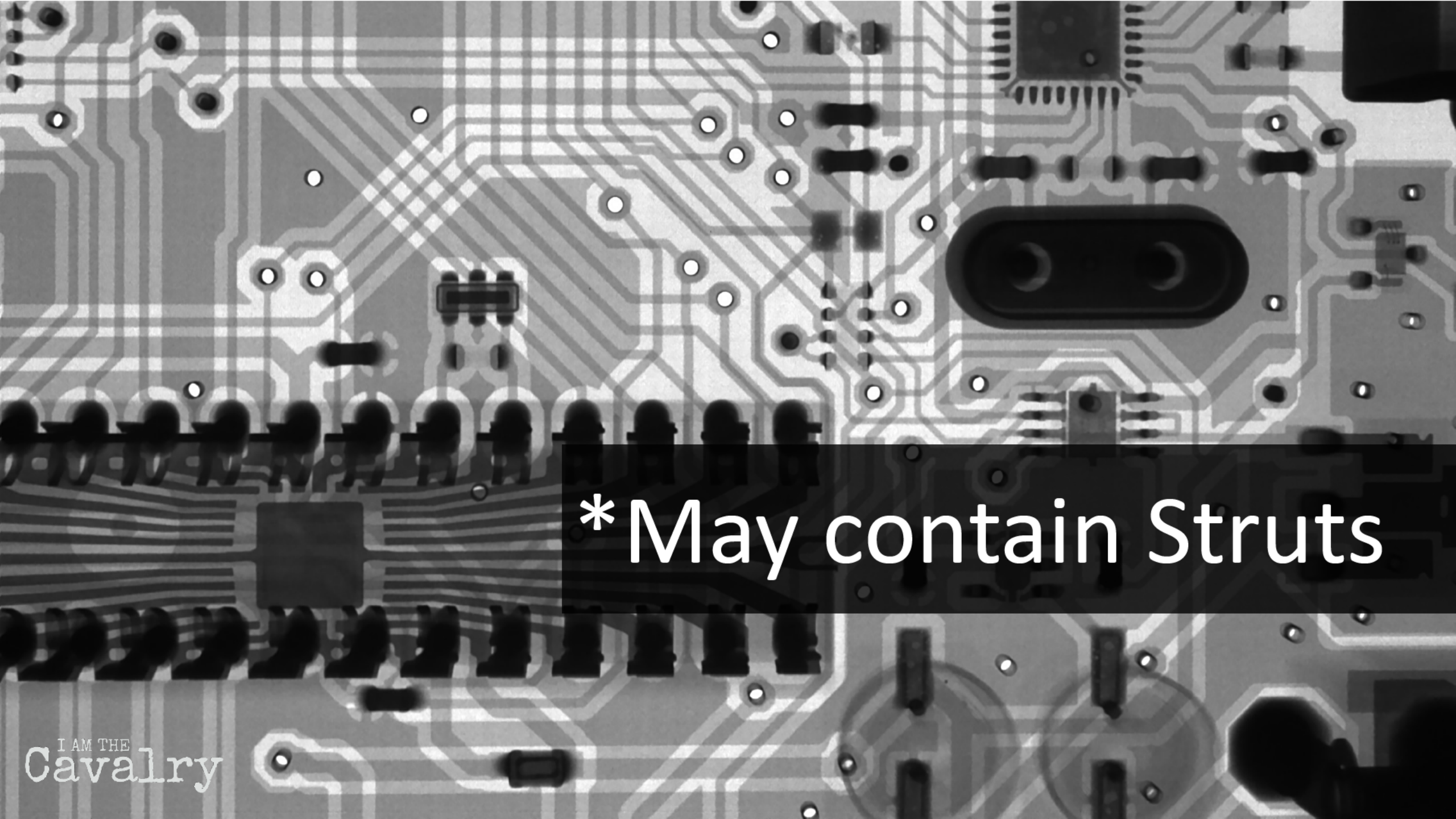
Transparency



Software Bill of Materials

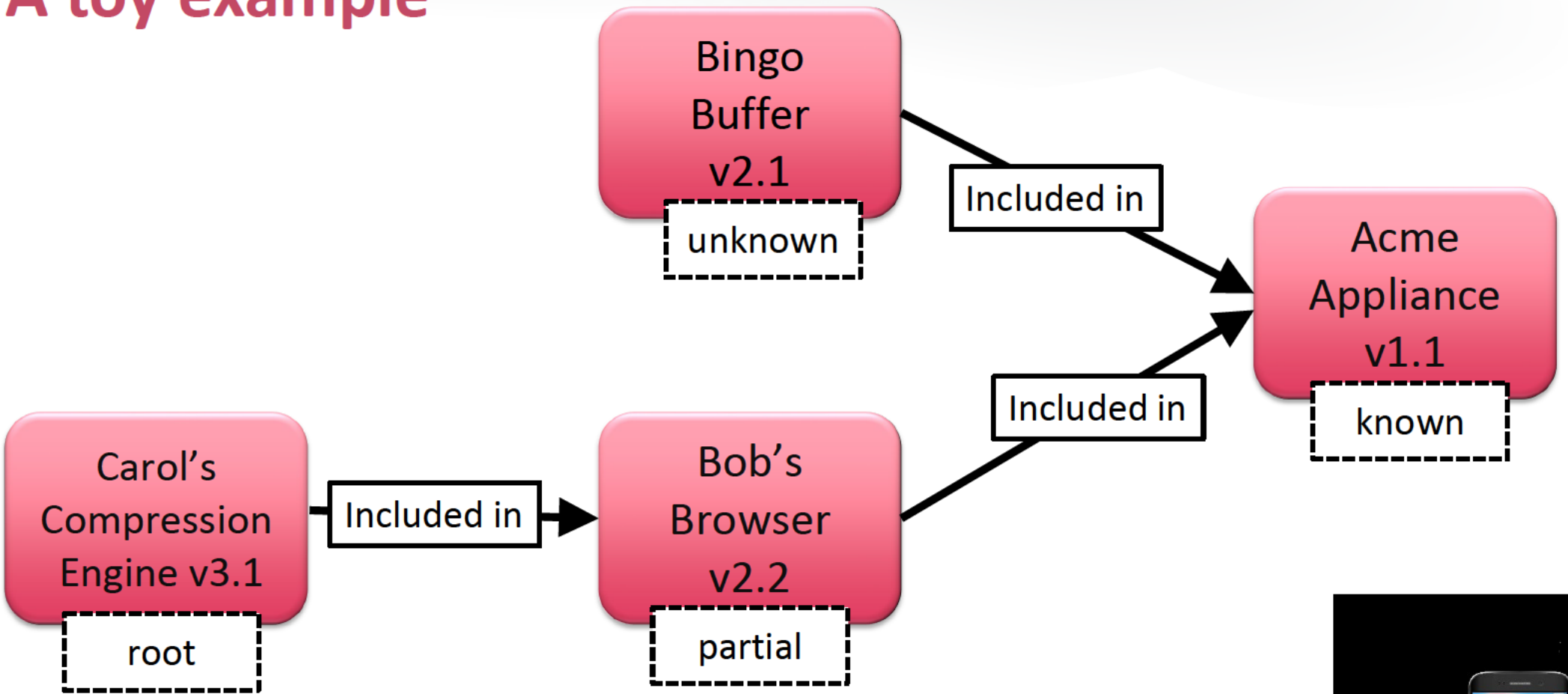
I AM THE Cavalry


*May contain nuts
I AM THE
Cavalry

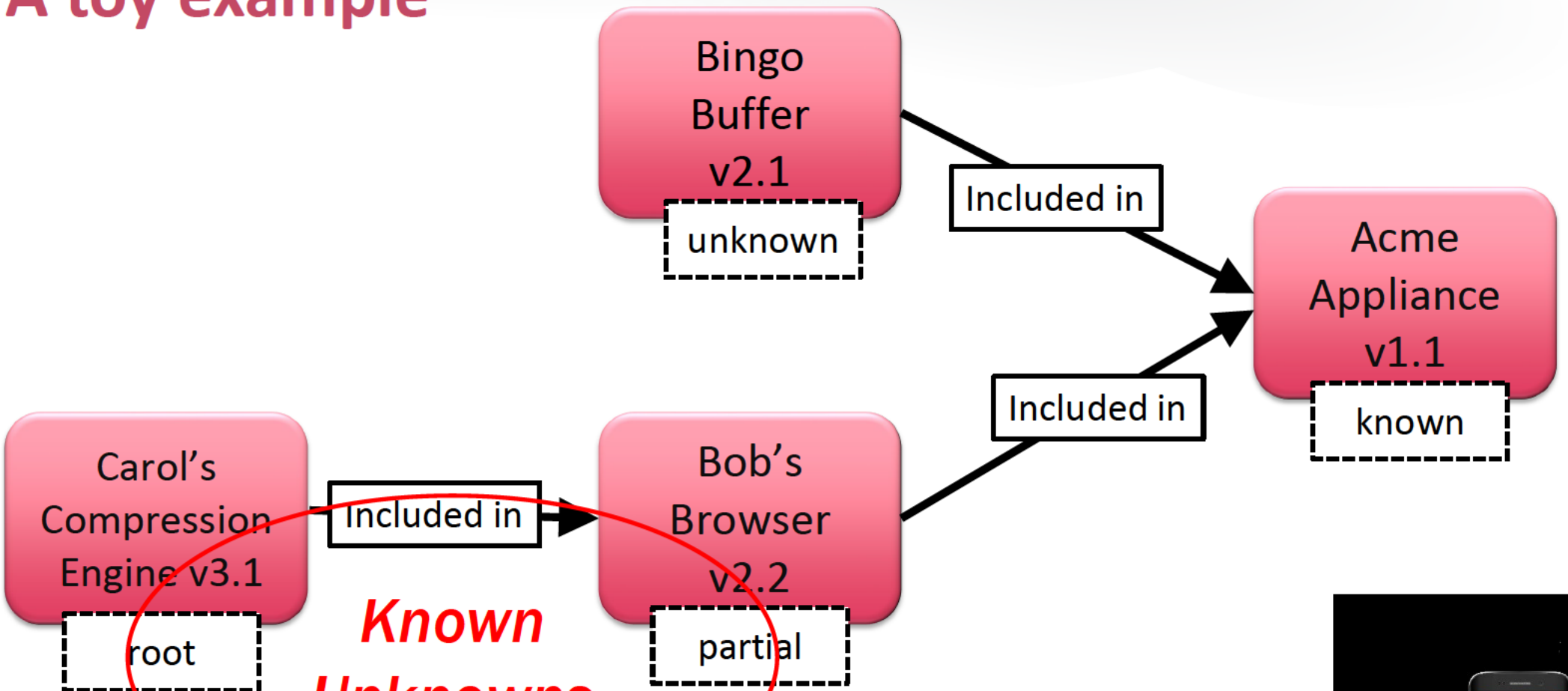

*May contain Struts
I AM THE
Cavalry

Wait… what exactly is an SBOM?

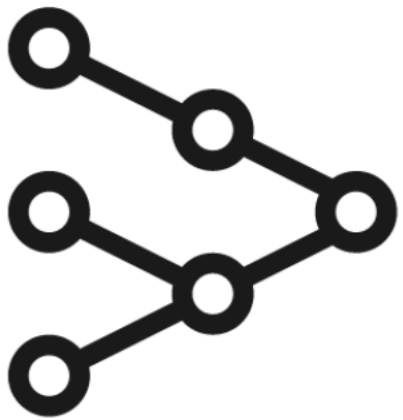
A toy example



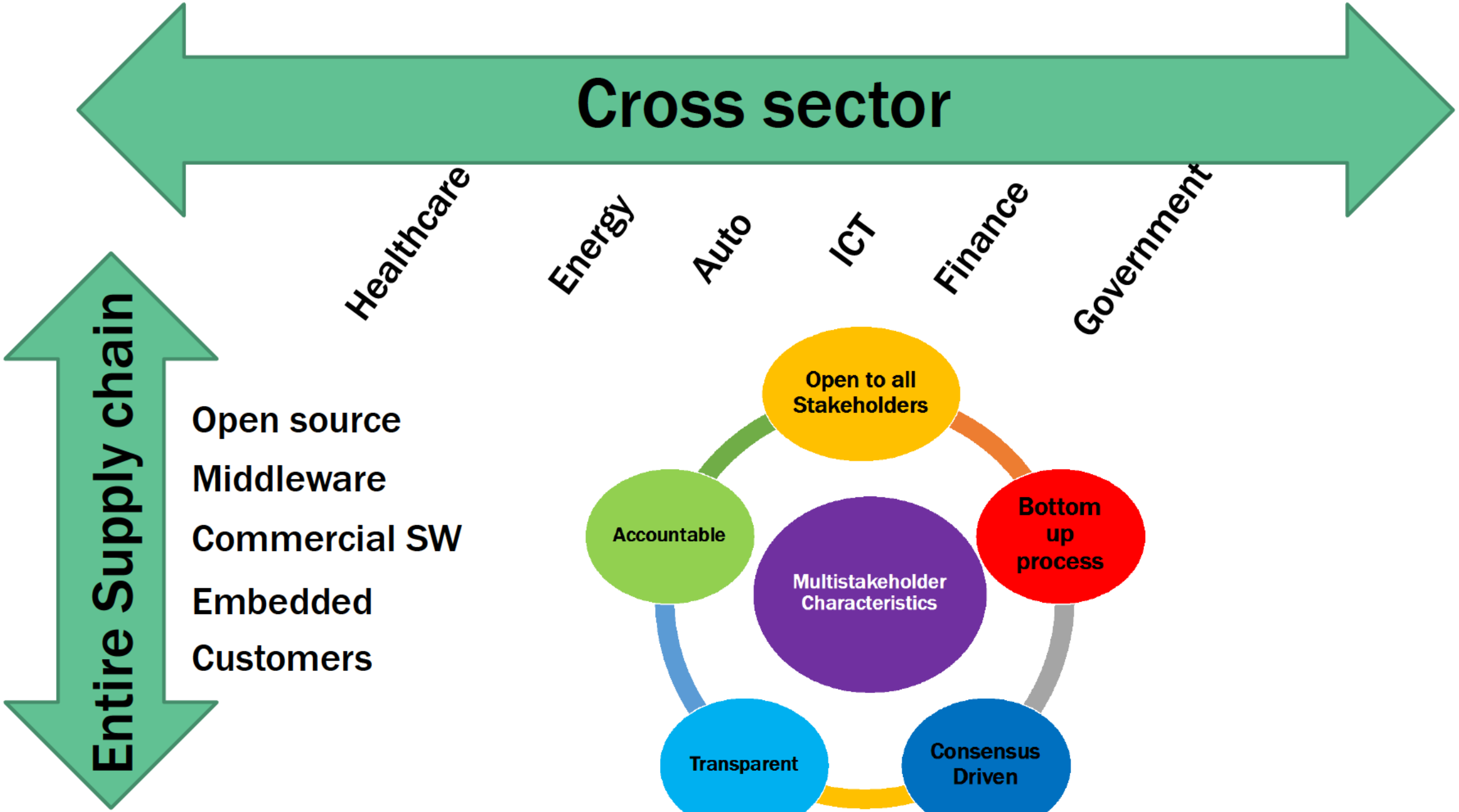
A toy example



How many levels deep?



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

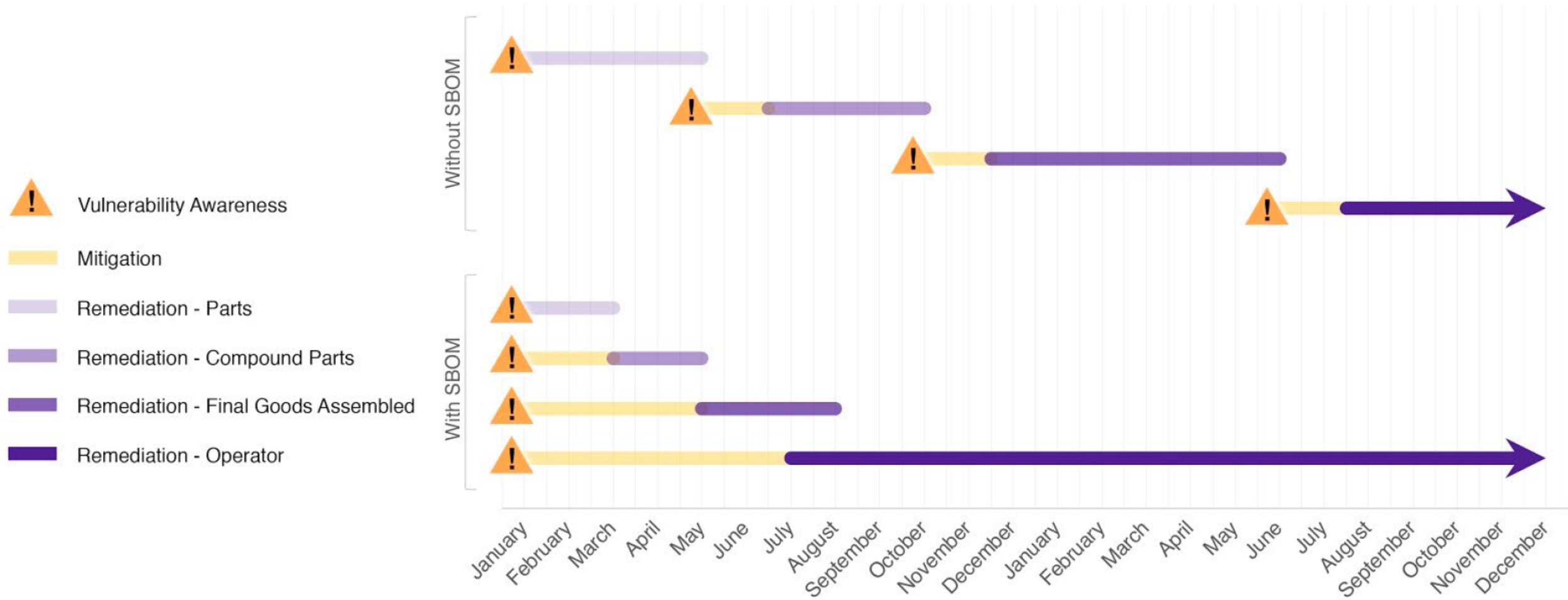

Cross sector
Healthcare
Energy
Auto
ICT
Finance
Government
Entire Supply chain
Open source
Middleware
Commercial SW
Embedded
Customers
Open to all Stakeholders
Bottom up process
Consensus Driven
Transparent
Accountable
Multistakeholder Characteristics

RSAConference2020 APJ
A Virtual Learning Experience

Why should we SBOM?

Time to Remediation Case Studies

Without and With SBOM



https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf

Natural selection in the software ecosystem

SBOMs make simple financial sense

"Having visibility into all our product families through an SBOM could easily save us **100,000 man hours** in time and effort to identify where potentially risky components are, and efficiently manage them across our development teams and customers."

-- Product Security Director, Fortune Global 500 company

RSAConference2020 APJ
A Virtual Learning Experience

How do we SBOM?

Two 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—all committed to creating a standard for software package data exchange formats.

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.

I AM THE Cavalry

NTIA

Translation between formats

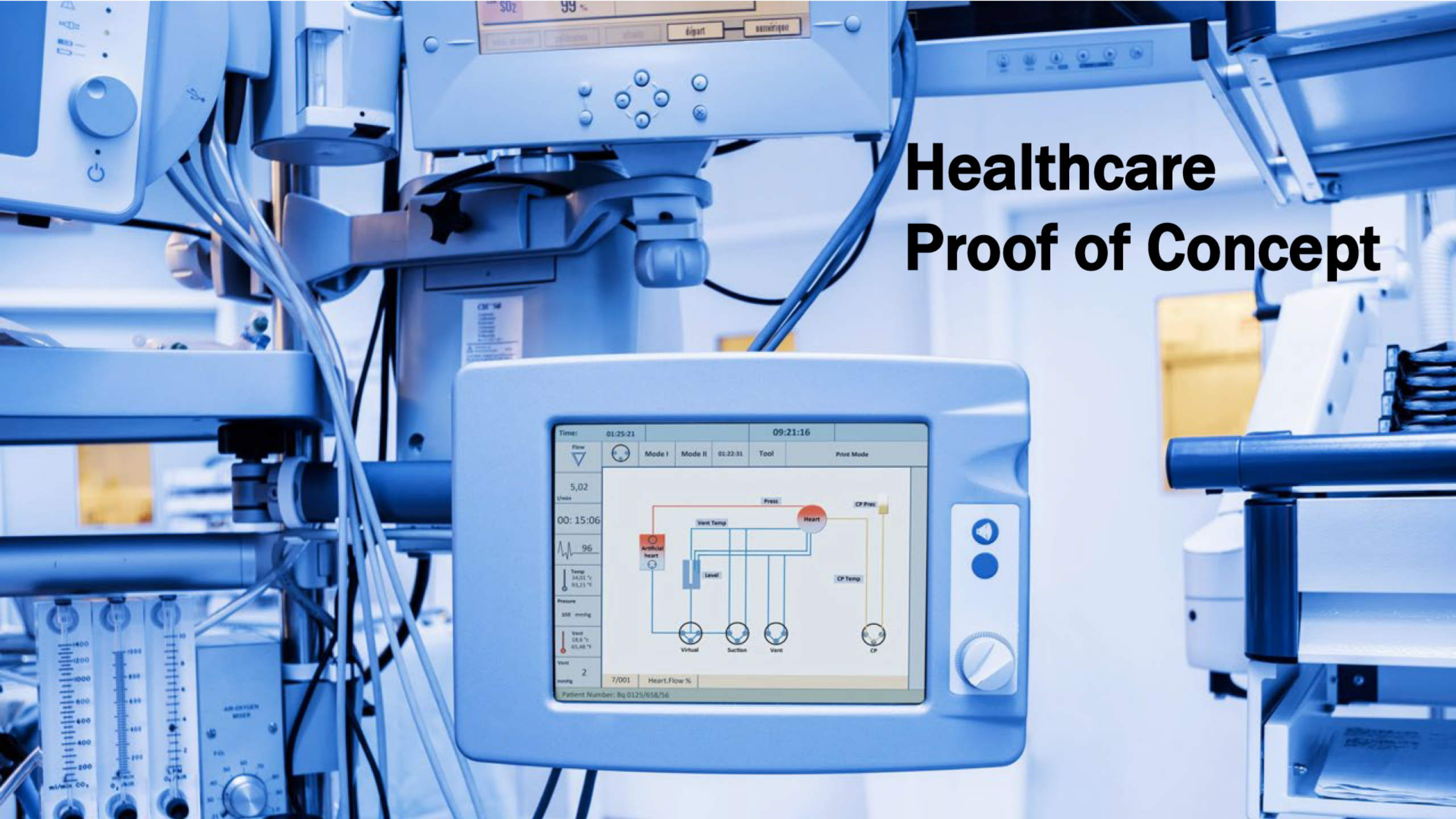
- We have identified the common elements.
- A ‘multilingual’ ecosystem does not offer too many challenges
- Rather than pick a winner, we will build out guidance to support all formats with effective interoperability.

Implementing core SBOM fields

Baseline	SPDX	SWID
Supplier Name	(3.5) PackageSupplier:	<Entity> @role (softwareCreator/publisher), @name
Component Name	(3.1) PackageName:	<softwareIdentity> @name
Unique Identifier	(3.2) SPDXID:	<softwareIdentity> @tagID
Version String	(3.3) PackageVersion:	<softwareIdentity> @version
Component Hash	(3.10) PackageChecksum:	<Payload>/../<File> @[hash-algorithm]:hash
Relationship	(7.1) Relationship: CONTAINS	<Link> @rel, @href
Author Name	(2.8) Creator:	<Entity> @role (tagCreator), @name

https://www.ntia.gov/files/ntia/publications/ntia_sbom_formats_and_standards_whitepaper_-_version_20191025.pdf

Healthcare Proof of Concept



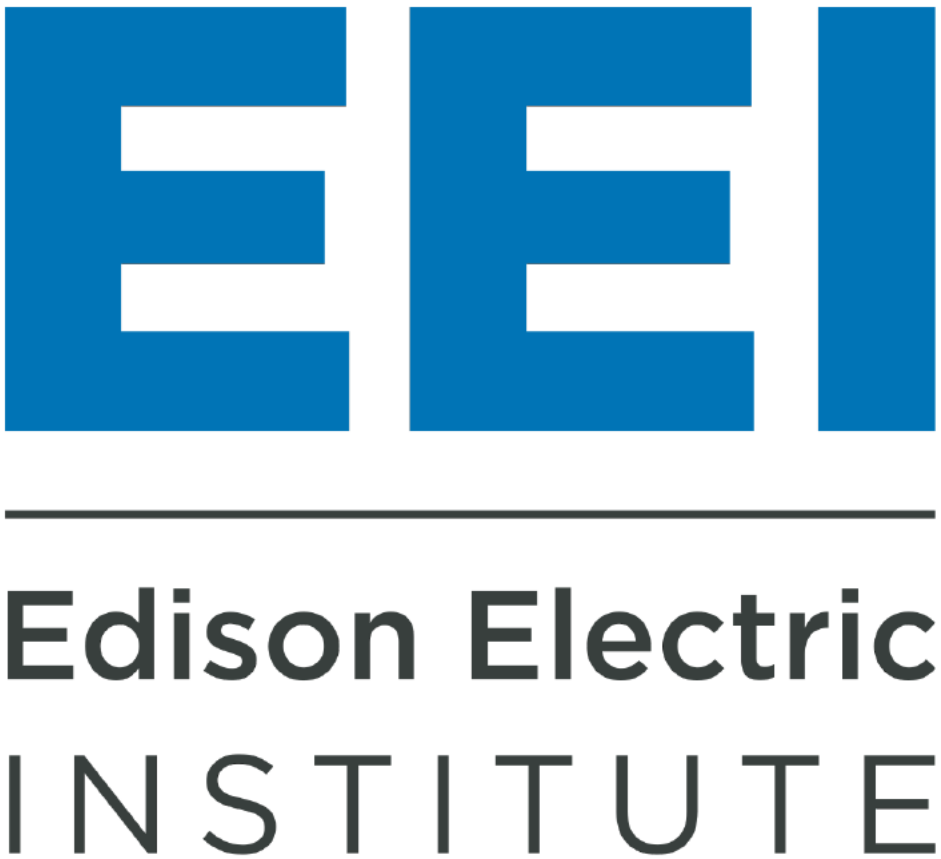
Next steps

- Refining and extending the model
  - Software namespace
  - Mechanism for sharing SBOM data
  - 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

What else can be done?

Enabled by SBOM

Model Procurement Language



I AM THE Cavalry

Monitor software for vulnerabilities


New Liability Models
I AM THE
Cavalry

What to do next

- Talk to your procurement officer
  - What do they need to make it easy to get you what you need?
- Ask sellers if they provide SBOMs
  - If they can't tell you what is in their product, your costs to protect your environment go up.
- Consider accountability and responsibility
  - Who does what when, and what happens if they don't?
- Brainstorm how you will respond to new vulnerabilities

Cross sector

Healthcare

Energy

Auto

ICT

Finance

Government

Entire Supply chain

Open source

Middleware

Commercial SW

Embedded

Customers

Join one of the open forums where these discussions are taking place, alongside diverse stakeholders to catalyze real progress across the ecosystem.

ntia.gov/SoftwareTransparency

Resources

- Supply Chain in the Software Era (Issue Brief)
  - https://atlanticcouncil.org/in-depth-research-reports/issue-brief/supply-chain-in-the-software-era/
- NTIA SBOM Project
  - https://ntia.gov/sbom
  - Join the open, international, industry-led process: afriedman@ntia.gov
- Supply Chain Sandbox materials
  - https://supplychainsandbox.org

RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **GPS1-F02V**

Taking Control of Cyber Supply Chain Security

Beau Woods

Cyber Safety Advocate
I Am The Cavalry
@beauwoods

Allan Friedman, PhD

Director of Cybersecurity Initiatives
NTIA / U.S. Department of Commerce
@allanfriedman
afriedman@ntia.gov