CSA SINGAPORE | SG Passion Made Possible

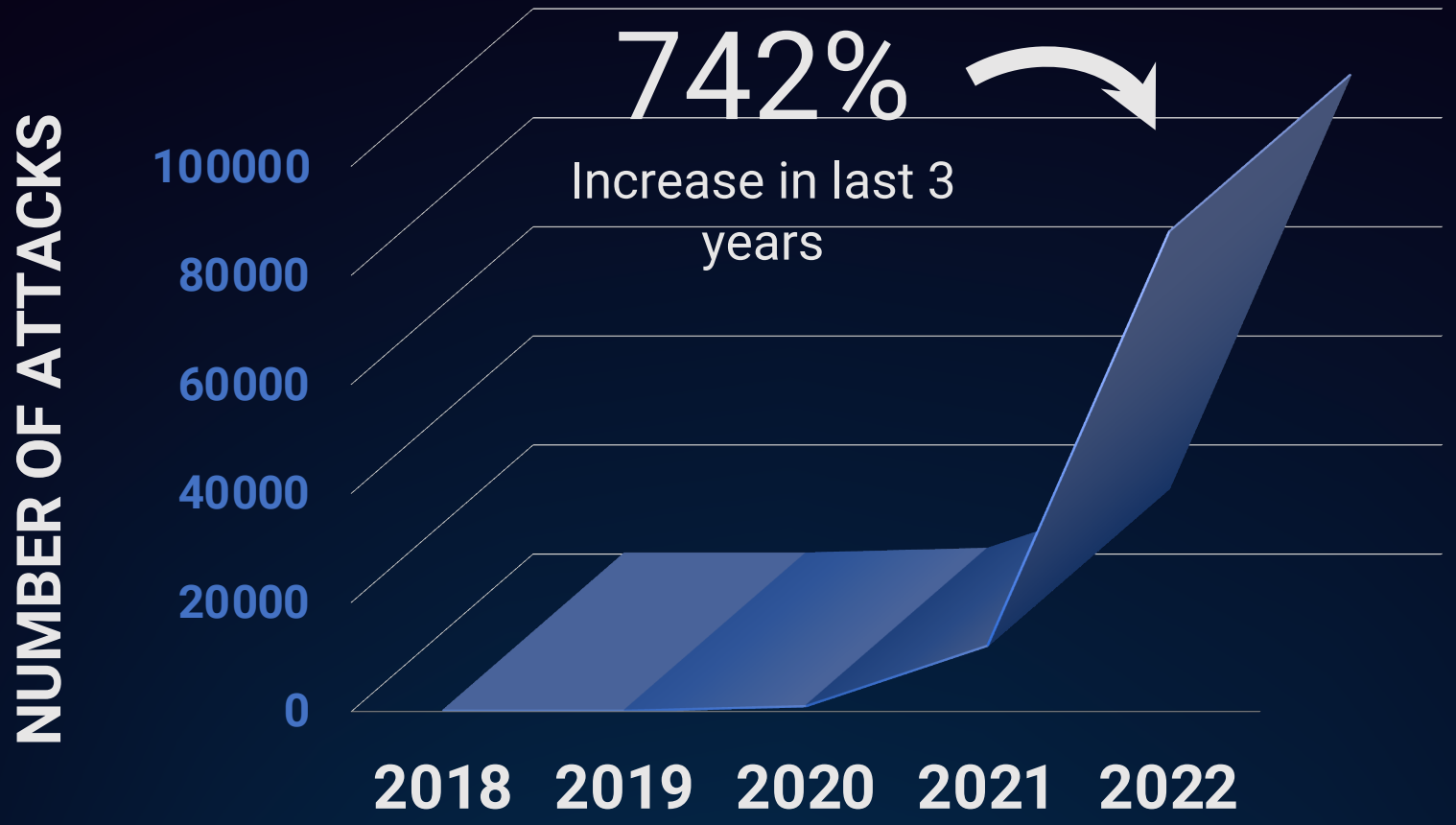
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

22 – 23 AUGUST 2023

Evolving Threats and Emerging Regulations in OT Software Supply Chain Security

Section 1: Untangling the Software Supply Chain Attack

Software Supply Chain Attacks Are Increasing Exponentially



State of the Software Supply Chain, Sonatype, 2022

Confusion About What Is Considered a Supply Chain Incident

What Is a Software Supply Chain Attack? (one common definition)

> ***A software supply chain attack occurs when a cyber threat actor infiltrates a software vendor's network and employs malicious code to compromise the software before the vendor sends it to their customers. The compromised software then compromises the customer's data or system.***

Cybersecurity and Infrastructure Security Agency

US Federal Government

What Is a Software Supply Chain Attack? (another definition)

> ***Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.***

Committee on National Security Systems (CNSS) Glossary

NIST Computer Security Resources Center

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

What Is a Software Supply Chain Attack? (a broader definition)

> ***Attacks that exploit the inherent trust between the participants in the software supply chain to target and exploit one or more end users of a product***

What Makes Software Supply Chain Attack Special?

> ***An organization could be vulnerable to a supply chain attack even when its own defences are quite good***

> ***More than 50% of the supply chain attacks were attributed to APT groups or well-known attackers***

ENISA Threat Landscape For Supply Chain Attacks
European Union Agency for Cybersecurity

Section 2: A Barrage of Regulations

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

A Rapidly Maturing Regulatory Environment in the United States

Executive Order 14028
Improving the Nation's Cybersecurity

May 2021

- Software Bill of Materials (SBOMs)
- Tools to check for and remediate vulnerabilities
- Accurate, up-to-date provenance of software

DHS/TSA Security Directives
for Critical Pipeline Owners & Operators

Jul 2021

- Report confirmed & potential cybersecurity incidents
- Report gaps and remediation measures to address cyber risks

National Security Memorandum
Improving Cybersecurity for Critical Infrastructure Control Systems

Oct 2021

- Performance goals
- Threat visibility, indicators, detections, and warning

Software Supply Chain Risk Mgmt Act

Dec 2021

- SBOMs required for all critical software used in federal systems
- Certification that each item in SBOM is free from security vulnerabilities

OMB Memorandum M-22-18

Sep 2022

Agencies required to obtain:

- self-attestation for 3rd-party software
- SBOMs for critical software

National Cybersecurity Strategy

Mar 2023

- Encourage coordinated vulnerability disclosure across all technology types and sectors; promote the further development of SBOMs
- Build on implementation of EO 14028, including the Software Bills of Material (SBOM)

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

International Regulation and Guidance on Supply Chain Security

IT Security Act 2.0
Increasing the Security of IT Systems

2021

Requirements:
- Manufacturers must provide a declaration of guarantee
- The declaration covers the manufacturer's entire supply chain

ENISA:
Threat Landscape for Supply Chain Attacks

2021

Recommendations:
- Define quality objectives: number of externally identified vulnerabilities
- Maintain accurate, current data on origins of software code or components
- Risk analysis via a vulnerability scoring system
- Patch verification and testing

EU Cyber Resilience Act

2022

Requirements:
- Commission to specify format/elements of SBOMs
- Manufacturers to document vulnerabilities and components, and create SBOMs

CII Supply Chain Programme 2022

2022

Initiatives:
- Real time transparency in cyber supply chain risks

Call for Views on Software Resilience and Security

Feb 2023

Survey on security controls and processes:
- Produce a component inventory or SBOM and share with customers
- Share a vulnerability exploitability alert (e.g., VEX)

A Guide to Implementing the Software Bill of Materials (SBOM) for Software Management

July 2023

Guidance on:
- Benefits of introducing SBOMs
- SBOM creation and sharing
- SBOM operation and management

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Industry-Specific Mandates

Medical Devices

FDA — Ensuring Cybersecurity of Medical Devices – S. 524B (Takes effect Oct 1, 2023)

Requirements for manufacturers:

- Create a plan to monitor, identify, and address, as appropriate, in a reasonable time, post-market cybersecurity vulnerabilities
- Provide a software bill of materials, including commercial, open-source, and off-the-shelf software components

Bulk Electrical Systems

NERC CIP-013 Cyber Security — Supply Chain Risk Management (Enforced July 2020)

Requirements for manufacturers:

- Develop one or more documented supply chain cybersecurity risk management plan(s)
- Disclose known vulnerabilities
- Verify software integrity and authenticity of all software and patches provided by the vendor

Automotive

NHTSA — Cybersecurity Best Practices for the Safety of Modern Vehicles (Draft 2022)

Requirement for suppliers and vehicle manufacturers:

- Maintain a database of their operational hardware and software components (aka SBOM)
- Track sufficient details related to software components, so when a new vulnerability is identified manufacturers can quickly identify what ECUs and specific vehicles would be affected

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Company-Specific Direction and Research

EEI Model Procurement Contract Language
(Published October 2022)

Terms now getting included in utility procurement contracts:

- Provide a software bill of materials for procured (including licensed) products consisting of a list of components and associated metadata
- Use reasonable efforts to investigate whether computer viruses or malware are present in any software or patches before providing such software or patches…
- To the extent Contractor is supplying third-party software or patches, Contractor will use reasonable efforts to ensure the third-party will not insert any code…
- When install files, scripts, firmware, or other […] solutions are flagged as malicious, infected, or suspicious by an anti-virus vendor, Contractor must provide technical justification as to why the “false positive” hit has taken place

Industry Response Research

Government intervention, the rise of the SBOM and the evolution of software supply chain security — Sonatype
(Survey Conducted May 2023)

Findings:

- 76% of enterprises globally have adopted an SBOM in the past two years
- 60% of respondents mandating that the businesses they work with maintain an SBOM
- 41% of security decision-makers see cyber regulation as the factor having the greatest positive impact on software security

Section 3: Trust, but Verify

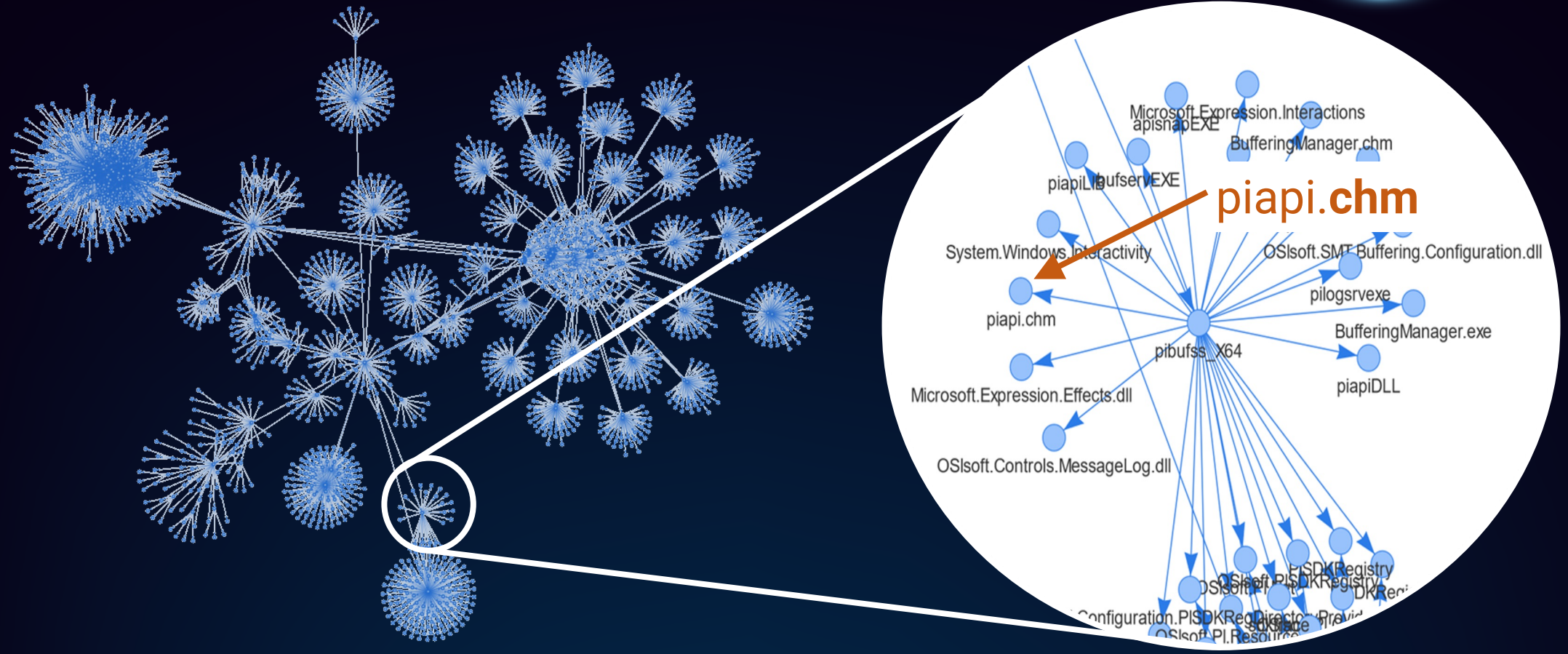
What Is a Software Bill of Materials (SBOM)?

> ***Software Bill of Materials (SBOM):***
> ***A formal record containing the details and supply chain relationships of various components used in building software.***

The Minimum Elements For a
Software Bill of Materials (SBOM)
The United States Department of Commerce

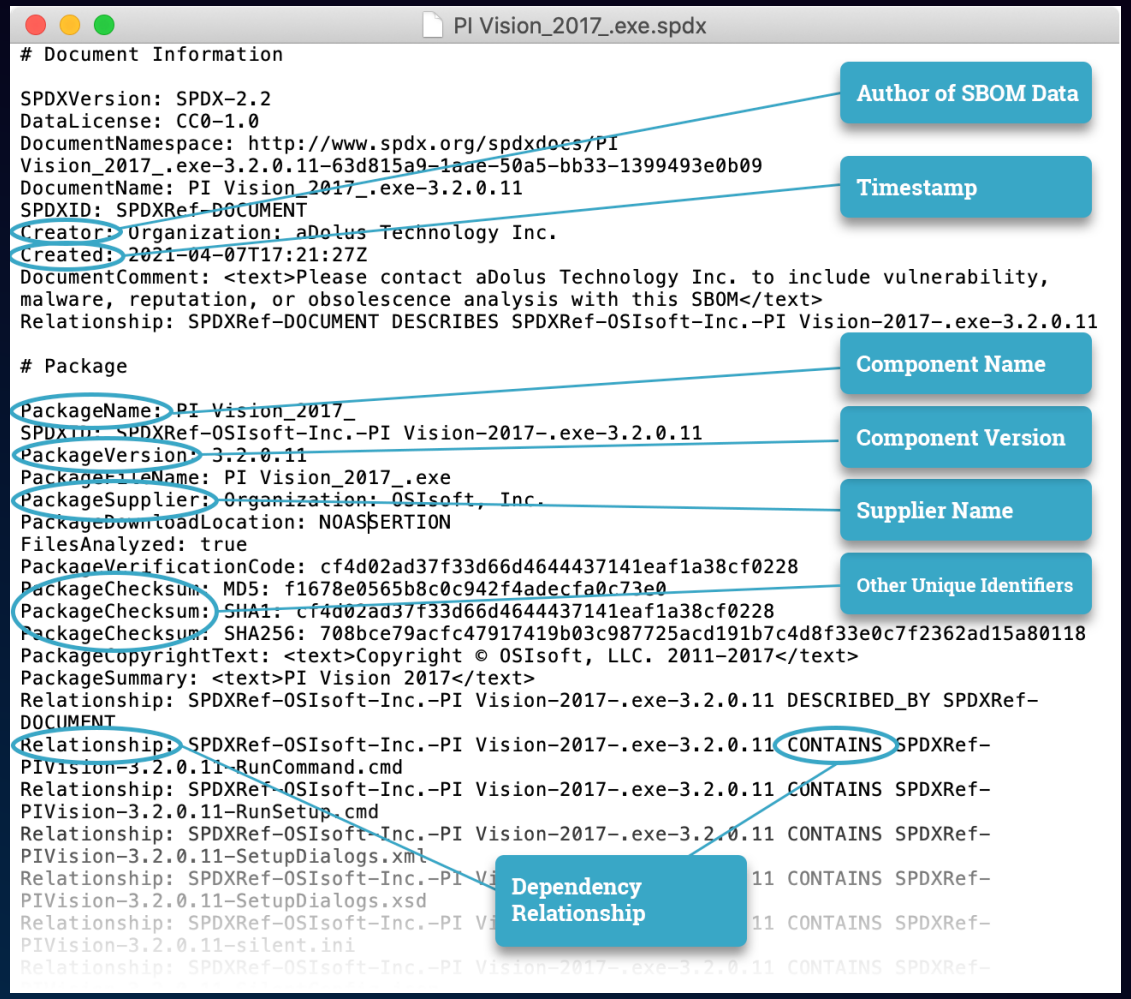
SBOMs Provide Transparency, Not Risk Analysis

Just the Ingredients, Not the Risk Report



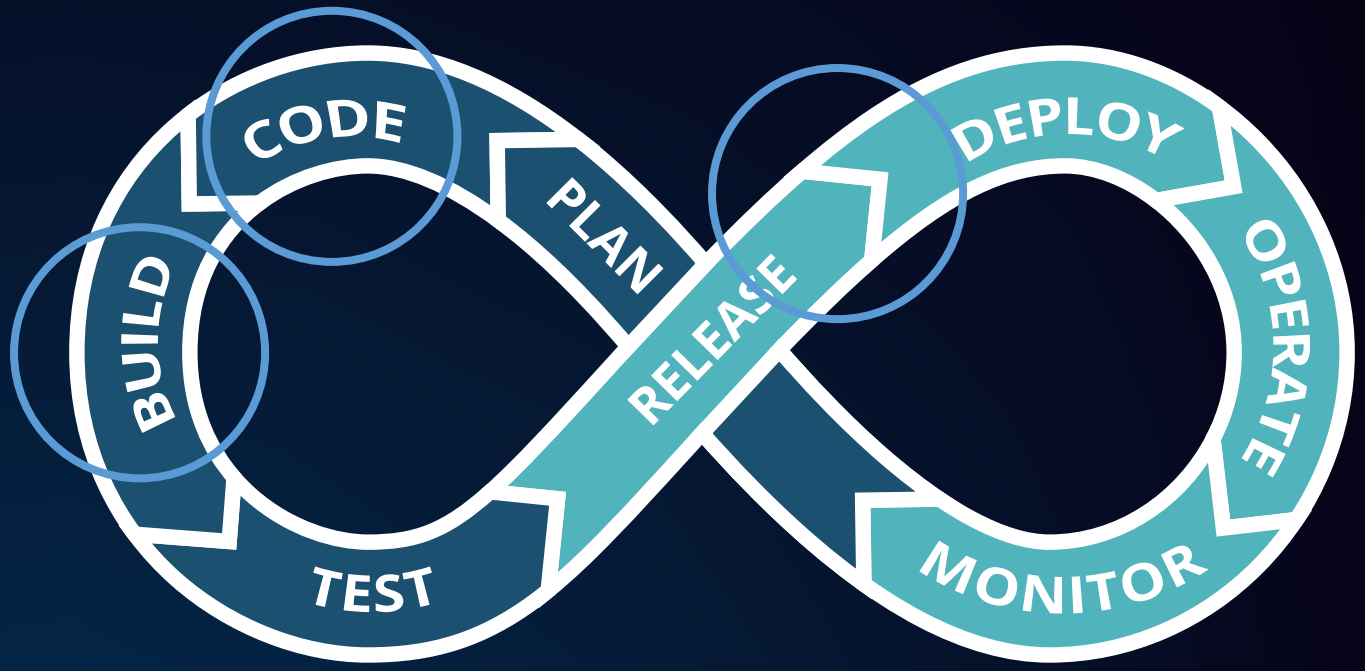
Minimum Components of an SBOM

- **NTIA defined the requirements for an SBOM**
- **Three approved formats:**
  1. SWID
  2. SPDX
  3. CycloneDX



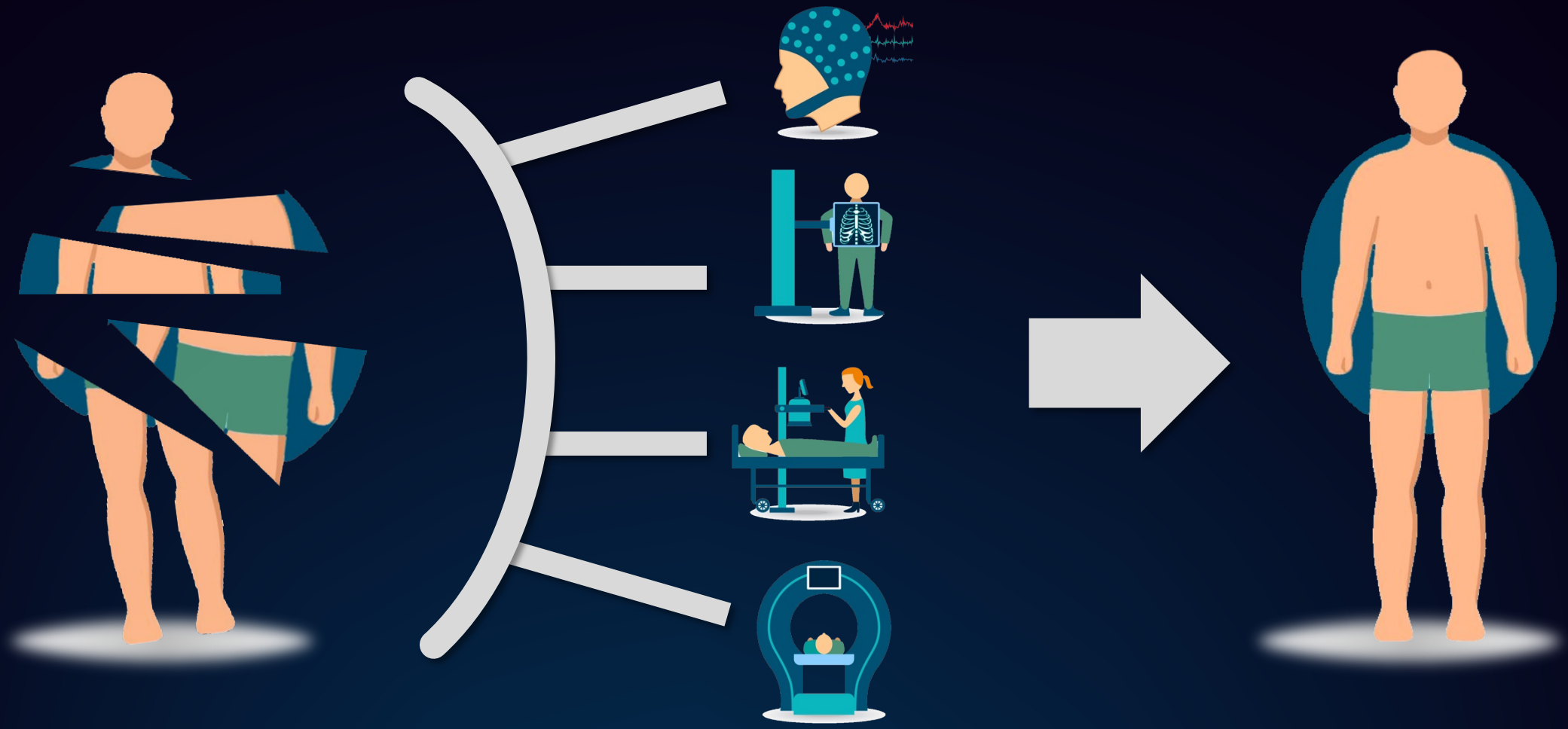
When to Generate an SBOM

- **NTIA requirements state SBOMs may be generated:**
    1. From a source repository (Source SBOMs)
    2. At software build time (Build SBOMs)
    3. From static analysis of already-built software (Binary SBOMs)



OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

The Sum Is Greater Than The Parts



Section 4: What to Do with all those SBOMs

Responding to the Log4j Incident the Old Way

> ***My team was forced to manually call almost 200 of our software suppliers to determine if the software they had sold us contained Log4j. It took over two weeks to complete.***

Chief Information Security Officer
Major US Defense Contractor

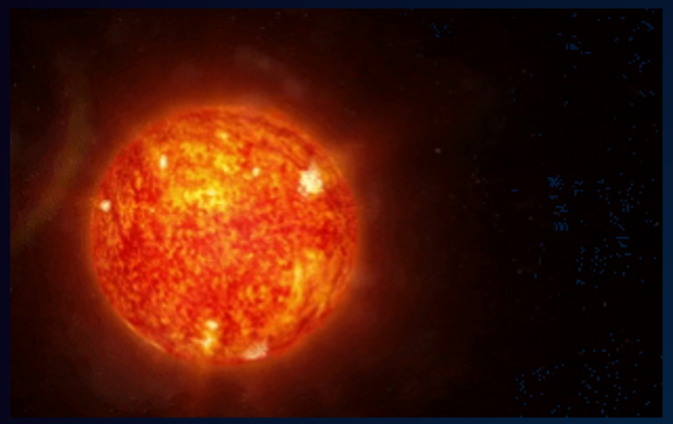
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

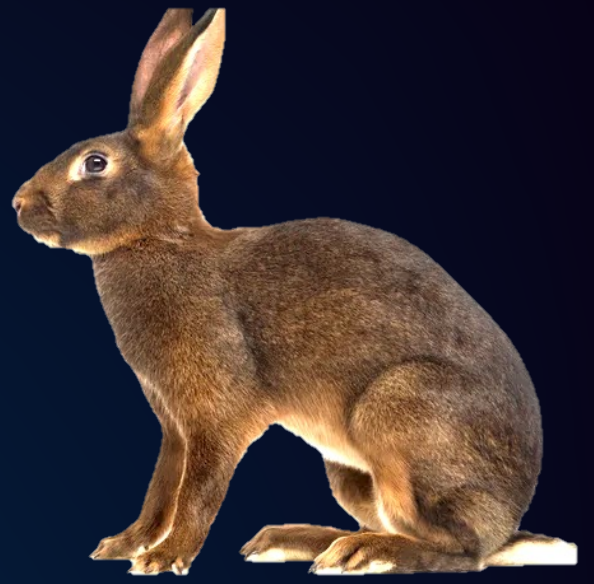
Responding to the SolarWinds Incident with SBOMs

> ***[My company] was able to investigate all of our approximately 1,200 on-premise products in about two hours to determine they were not vulnerable to the SolarWinds attack. Most of that two hours was determining the names of the affected components.***

Product Cybersecurity Strategist

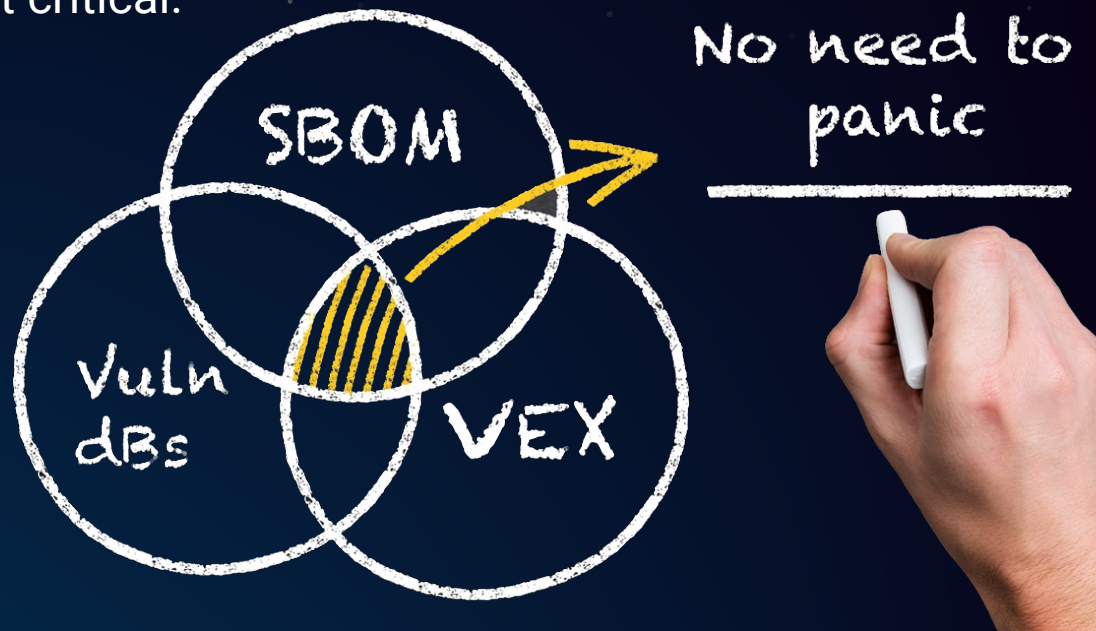
Top 5 IT Software Company





SBOM Companion Reports – VDR and VEX

- **Vulnerability Disclosure Report (VDR): A** document that lists all the vulnerabilities discovered in an SBOM for a single product.
- **Vulnerability Exploitability eXchange (VEX)**: A document that summarizes the vulnerability intelligence found within a product or a product family to help end users quickly focus on the vulnerabilities that are most critical.



OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Some Key Takeaways

Organizations with good defences can be vulnerable to supply chain attacks

Supply chain security foundations are built on transparency

Both government and industry are demanding visibility into the supply chain

SBOMs make risk analysis possible; they do not replace it