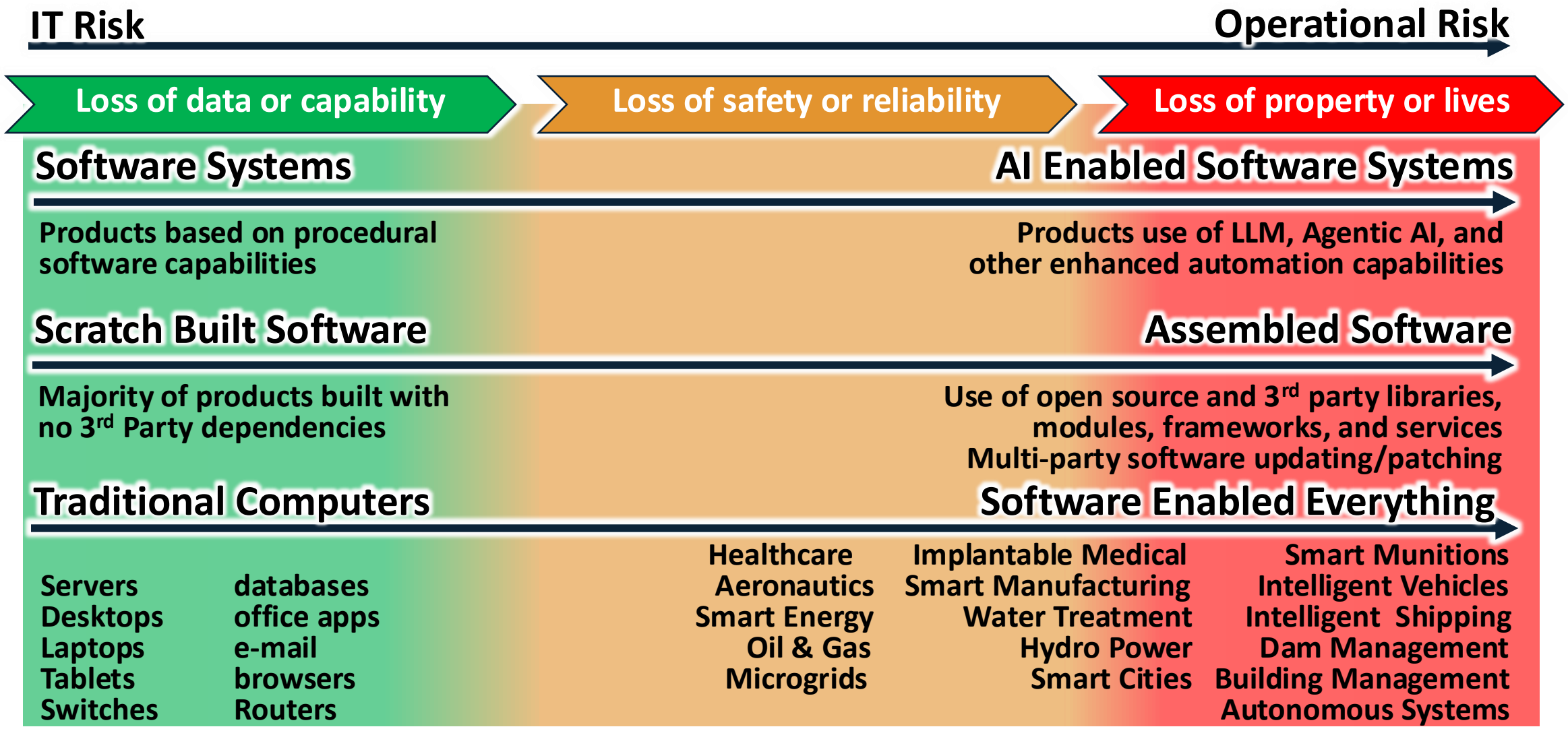
Transparency and Security of Your Software and Systems Supply Chains

Robert Martin
Senior Software and Supply Chain Assurance Principal Engineer
Cyber Solutions Innovation Center
MITRE Labs

Presented 26 August 2025

MITRE

Software is Pervasive, Assembled, and “Smart”



Enterprise Software Examples Making use of AI

Customer relationship management

Project management

HR & Recruitment

Communication

Cloud services

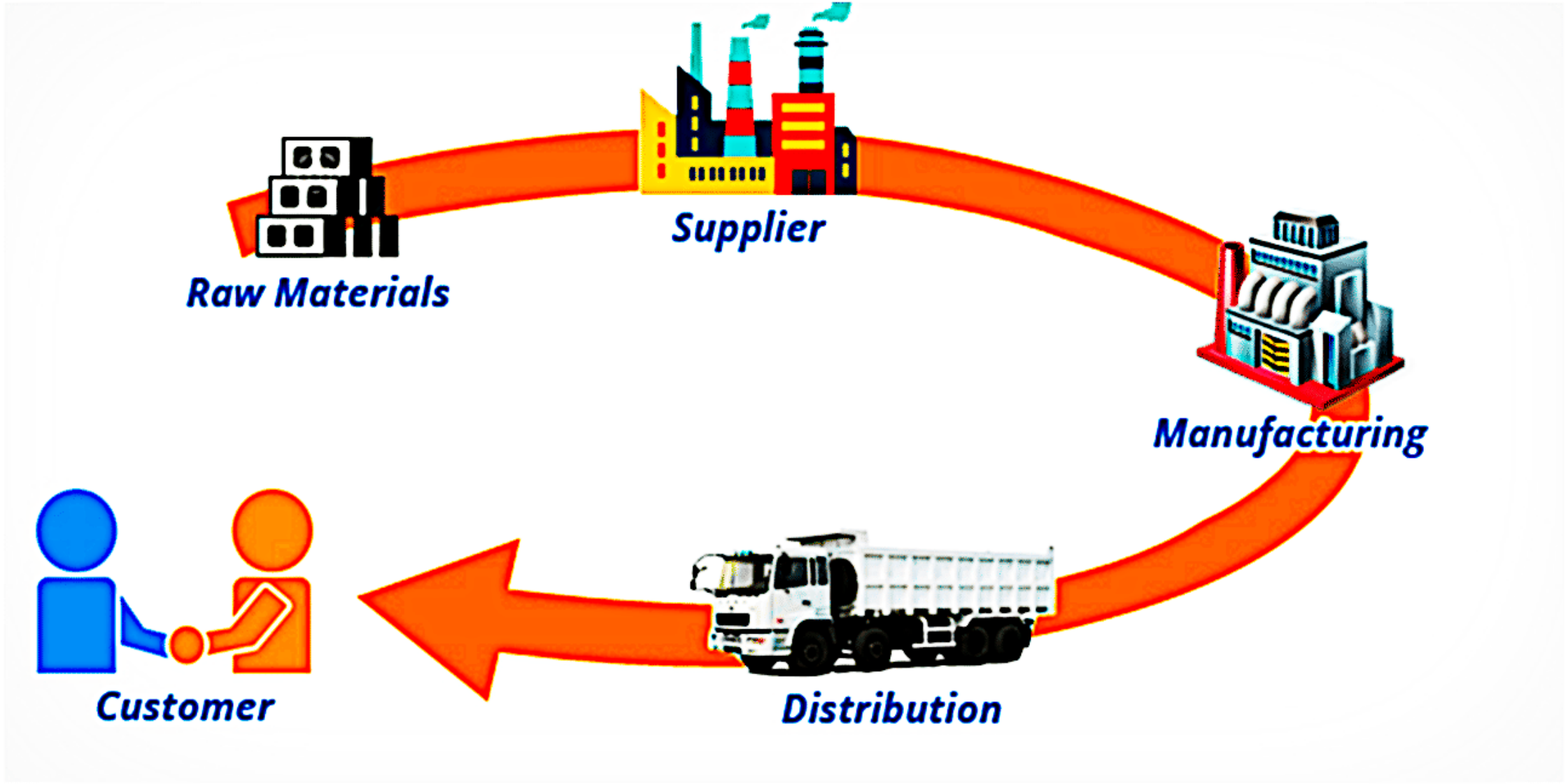
ERP software

Software repository

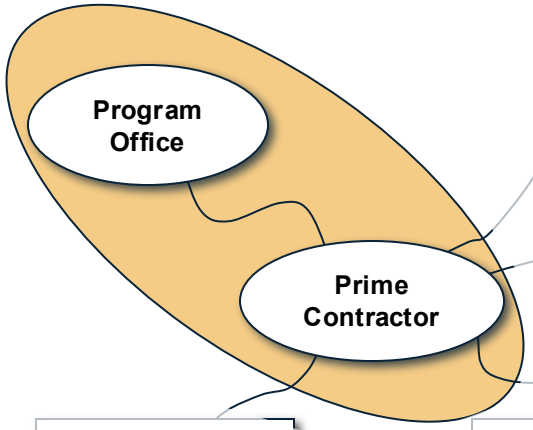
Accounting software

Productivity software

Characterizing Supply Chains



Software Supply Chains Are Opaque – Transparency is needed

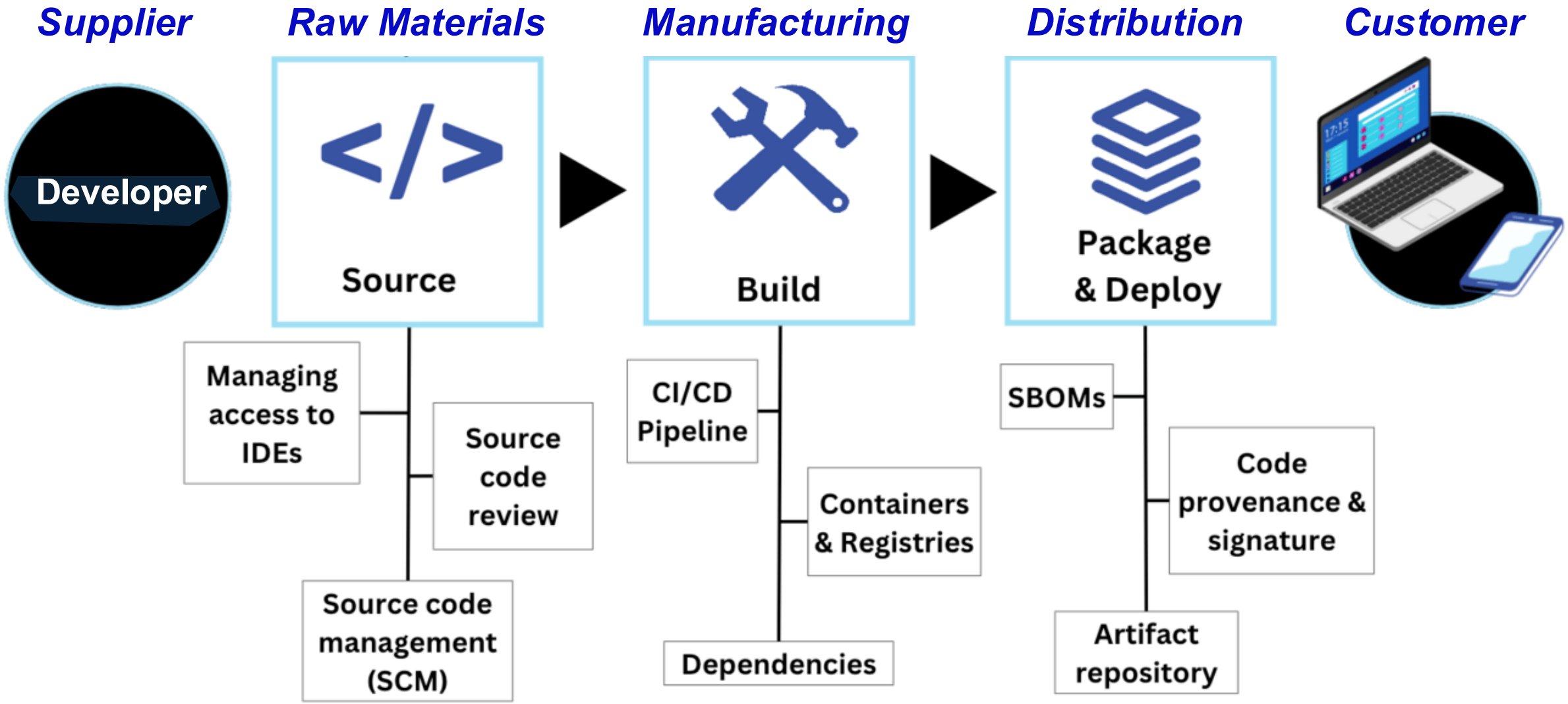


Reuse
Outsource
Acquire
Develop In-house
Supplier
COTS
Software
US
Off-shore
Foreign Location
Foreign Developers
Legacy Software
Other Programs
Contractor
Supplier
US
Global
Foreign
Contractor
Supplier
Reuse
Acquire
Develop In-house
Outsource

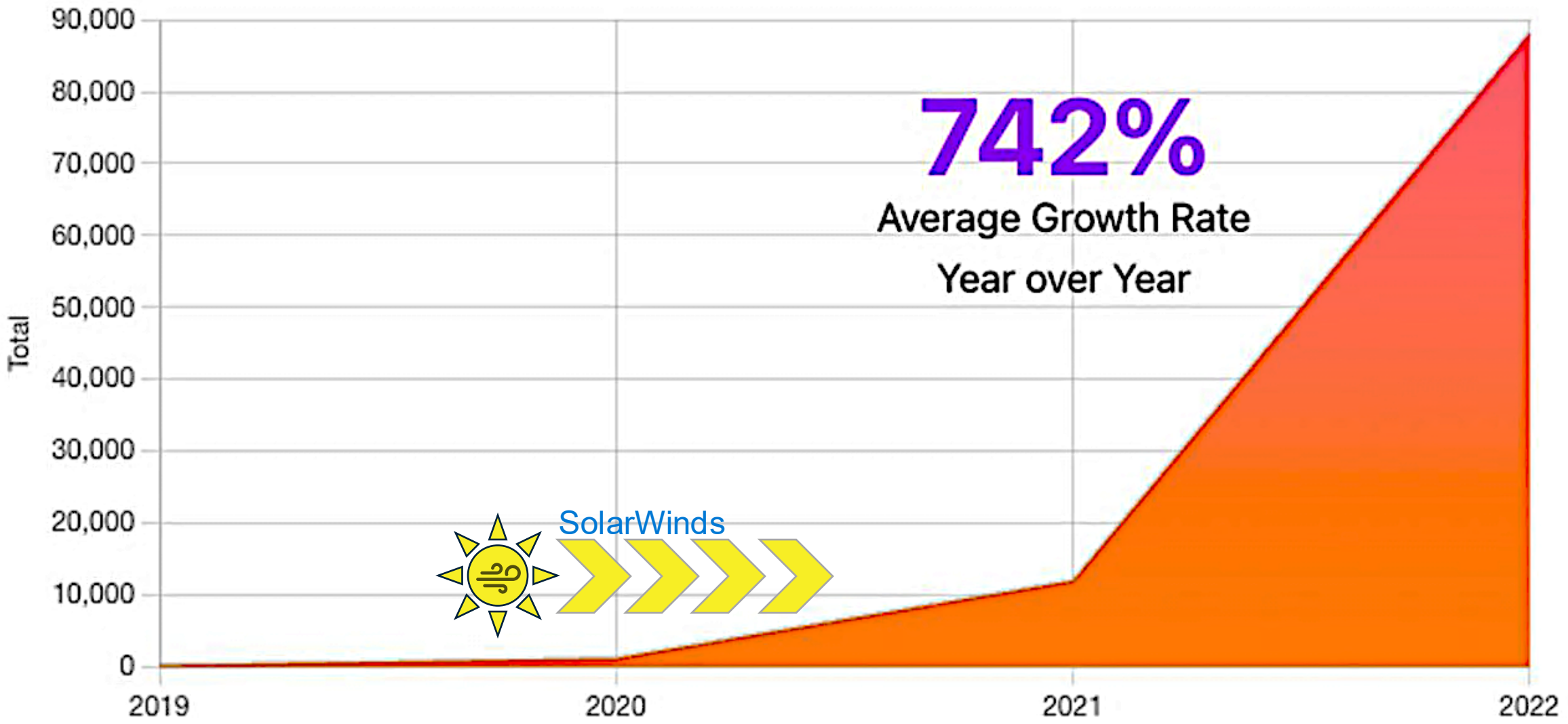
Provenance for software components (code AND models AND datasets)

- **Origin – Chain of Custody?**
- **Tool Chains Used?**
- **Languages and versions?**
- **Licenses?**

Software Supply Chain Attack Points



10th Annual State of the Software Supply Chain – Sonatype

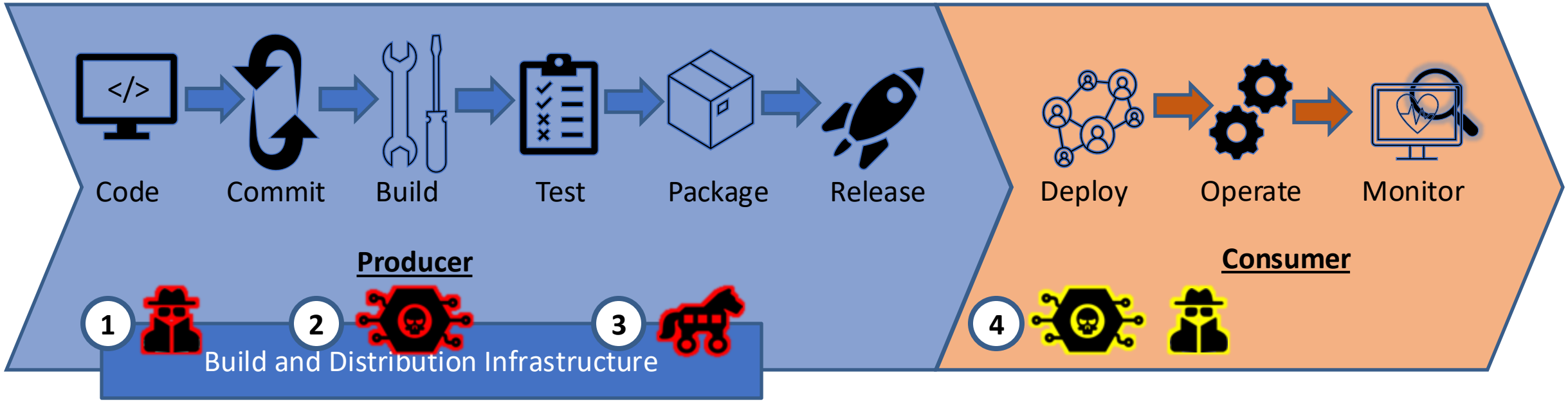


https://www.sonatype.com/state-of-the-software-supply-chain/introduction#open-source-security

MITRE

Real-World Software Supply Chain Attack (a.k.a SolarWinds)

1. Preparatory compromises at SolarWinds date back to **October 2019**. (Refs 11 & 12)
2. At some point there was a compromise of the build environment itself.
3. Malicious code sent in SolarWinds updates released between March and at least **June 2020**. (Refs 32 & 33)
4. Approximately 18,000 organizations receive the tainted updates and may have been targeted and impacted.

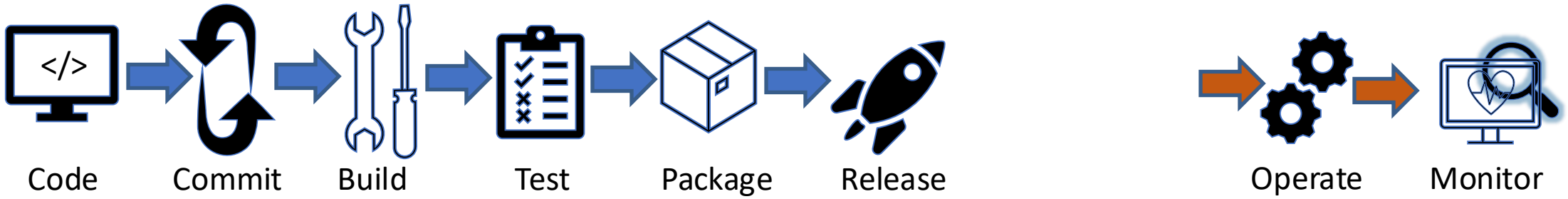


Software S & Integrity

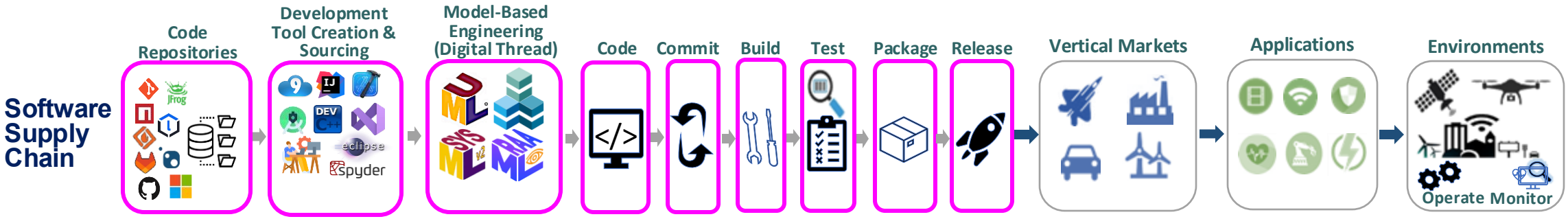
Jan 2021

https://www.mitre.org/sites/default/files/publications/pr-21-0278-deliver-uncompromised-securing-critical-software-supply-chains.pdf

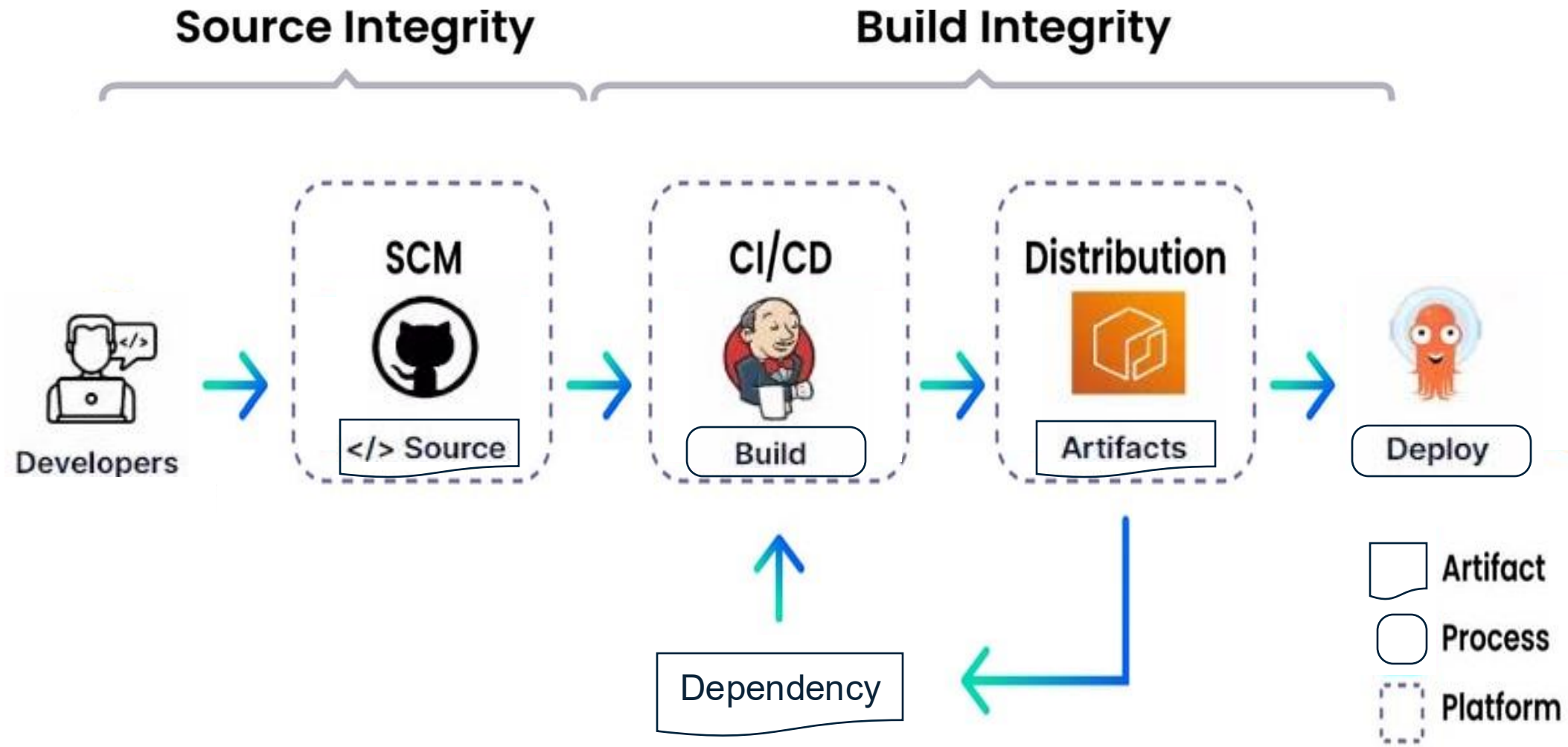
Software Supply Chain Integrity



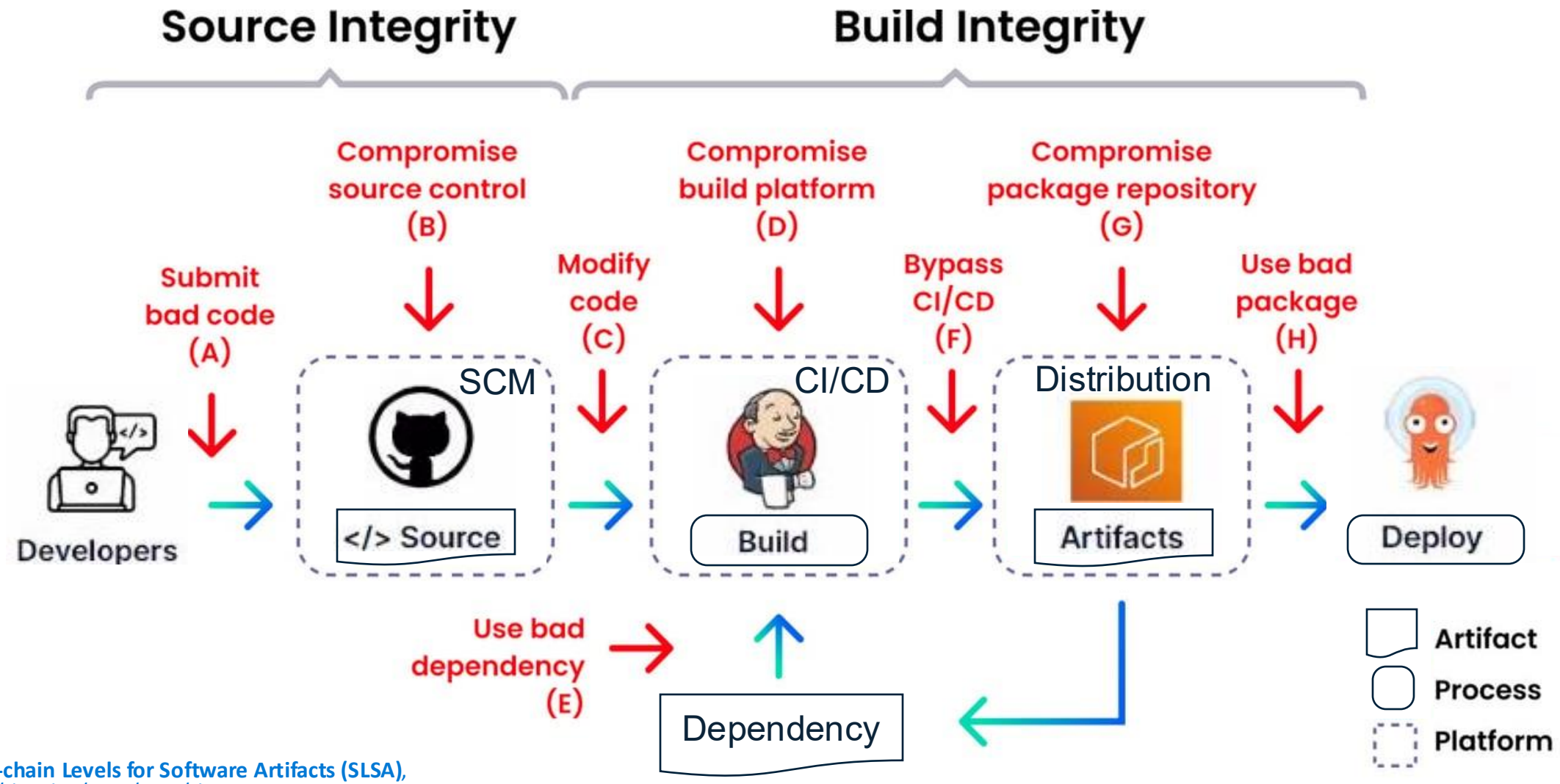
Software Supply Chain Integrity



The Software Supply Chain



Software Supply Chain Risks



Supply-chain Levels for Software Artifacts (SLSA), https://slsa.dev/spec/v1.0/threats-overview

Software Supply Chain Real-world Risk Examples

Risks to SW	Category	Example
(A) Inject bade code	Source threat	Linux hypocrite commits: Researcher intentionally introduces vulnerabilities into Linux kernel via patches
(B) Compromise source control	Source threat	PHP: Attacker compromised PHP's self-hosted git server and submits two malicious commits
(C) Build from modified source	Build threat	Webmin: Attacker modifies build infra to use source files not matching source control
(D) Compromise build process	Build threat	SolarWinds: Attacker compromised build platform
(E) Vulnerable dependency	Source threat Build threat	Event-stream: Attacker added innocuous dependency then turned dependency malicious
(F) Bypass CI/CD + inject bad artifact	Build threat	CodeCov: Leaked credentials used to upload malicious artifact to GCS bucket
(G) Compromise package repo/signing	Build threat	Attacks on Package Mirrors: Mirrors run on popular package repos
(H) Compromise deploy process	Deployment + runtime threat	Browserify typosquatting: Similar name to original used

MITRE

Supply Chains as sources of risks and vulnerabilities

March 2014

"Before Target, They Phished the Heating Guy"

Updated – 1/15

Software

INCIDENT:
A nationwide heist of financial data took place in Target stores from November –December, 2013, affecting over 110 million customers. The breach was initiated with an attack against a HVAC contractor with remote access to Target's network.

Hackers used an email phishing scheme to steal the contractor's login credentials and infiltrate Target's network. Once inside, hackers installed point-of-sale malware to steal data at nearly 2,000 Target store. The stolen information included names, mailing addresses, encrypted personal identification numbers, and phone numbers.

IMPACT:
The incident compromised customer data and stole 40 million credit and debit card accounts from payment terminals.

Following the breach, Target reported a 46% net drop in sales, $61 million in costs related to the breach, and facing numerous lawsuits. Financial institutions have spent over $200 million in costs related to reissuing cards.

Courts recently held Target negligent in its cybersecurity posture, opening the door for a class action lawsuit.

MITIGATION:
Target began an overhaul of its security operations and practices and offered free credit monitoring services to affected customers for a year. Financial institutions reissued credit and debit cards to customers.

According to the HVAC contractor, their IT system and security measures are in full compliance with industry practices. They are fully cooperating with the Secret Service and Target to identify the possible cause of the breach and to help create proactive initiatives that will further enhance the security of client/vendor connections making them less vulnerable to future breaches.

- http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
- http://www.nextgov.com/cybersecurity/2014/02/target-data-hack-cost-banks-more-200-million/78965/
- https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/
- http://www.computerweekly.com/news/2240234281/Home-Depot-traces-credit-card-data-hack-to-supplier-compromise
- http://www.bankinfosecurity.com/target-home-depot-breaches-lessons-a-7544/op-1
- http://krebsonsecurity.com/tag/target-data-breach/

Jan 2014

"Outsiders Access Japanese Nuclear Reactor Control Room Data"

Software

INCIDENT:
In January 2014, it was determined that hackers may have stolen private information from one of the eight computers in the reactor control room at the Monju fast-breeder reactor offices. For 5 days starting on December 26, 2013, the computer, which stores more than 42,000 e-mails and staff training reports, had been accessed more than 30 times with the requests coming from a website based in South Korea. A server administrator discovered that the malware infected the computer after an employee updated free software that was installed on the computer.

IMPACT:
Since the computer is only used by workers to file paperwork, the damage that the malware could have caused is limited. However, after finding traces of out-bound transmissions, investigators concluded that the cybercriminals controlling the malware could have stolen sensitive documents, including emails, training records and employee data sheets.

MITIGATION:
The Japan Atomic Energy Agency (JAEA) currently is investigating how the infection occurred and identifying the data on the computer that could have been accessed. In November 2013, the agency had been warned by the country's nuclear regulator that its anti-terrorism measures were not up to snuff. "The regulatory agency rebuked the JAEA for violating security guidelines meant to protect nuclear materials from terrorism and other malicious attacks," Enformable reported.

- http://www.nextgov.com/cybersecurity/threatwatch/2014/01/breach/689/
- http://enformable.com/2014/01/computer-control-room-monju-fast-breeder-reactor-infected-virus/

January 2015

" Home Depot Hack Linked to Compromised Supplier, Login Credentials, and Malware"

Software

INCIDENT:
In November 2014, Home Depot announced that criminals used a third-party vendor's username and password to enter the perimeter of its network in September 2014. From there, hackers acquired "elevated rights" that allowed them to navigate portions of Home Depot's network and to deploy custom-built malware on the retailer's self-checkout systems in the U.S. and Canada, compromising millions of customer data.

The malware used in the attack was designed to evade detection by anti-virus software, according to Home Depot. Although Home Depot has not identified the supplier linked to the breach, the revelation highlighted the importance of information security throughout the supply chain.

IMPACT:
Home Depot revealed that some 53 million customer e-mail addresses were stolen in the attack, in addition to the compromise of 56 million payment cards.

Those customers who have had their e-mail addresses compromised should be on heightened alert for phishing attacks, says Shirley Inscoe, analyst at Aite Group.

Home Depot estimates it will spend $62 million in fiscal 2014 for breach-related costs, including investigating the incident, providing credit monitoring services to its customers, increasing call center staffing, and paying legal and professional services. The company expects its insurance to cover about $26 million of that expense.

MITIGATION:
The company is notifying affected customers in the U.S. and Canada. Home Depot is warning customers to be on guard against phishing scams.

The company also has completed a major payment security project that provides enhanced encryption of payment data at the point of sale. The project required writing tens of thousands of lines of new software code and deploying nearly 85,000 new PIN pads to stores. Rollout of enhanced encryption to 180 Canadian stores will be completed by early 2015. U.S. stores will have EMV in place by the end of this year.

All individuals affected by the breach will receive free identity theft protection services, including credit monitoring, for one year, Home Depot says.

- http://www.computerweekly.com/news/2240234281/Home-Depot-traces-credit-card-data-hack-to-supplier-compromise
- http://www.bankinfosecurity.com/target-home-depot-breaches-lessons-a-7544/op-1
- http://www.databreachtoday.com/home-depot-53-million-e-mails-stolen-a-7537?webSyncID=1612ec2c-3c8b-85ba-87a0-33b952bb87ca&sessionGUID=478e7423-6501-0104-a32a-86d53cbd0ace

January 2015

"Counterfeit Versions of Windows with Preinstalled Malware Sold in China"

Software

INCIDENT:
As part of an investigation into the sale of counterfeit software, Microsoft's digital crimes unit purchased brand new computers from different cities in China. The investigators discovered that of the computers were running forged versions of Windows and that 20% of the computers were pre-infected with viruses including the aggressive botnet virus Nitol.

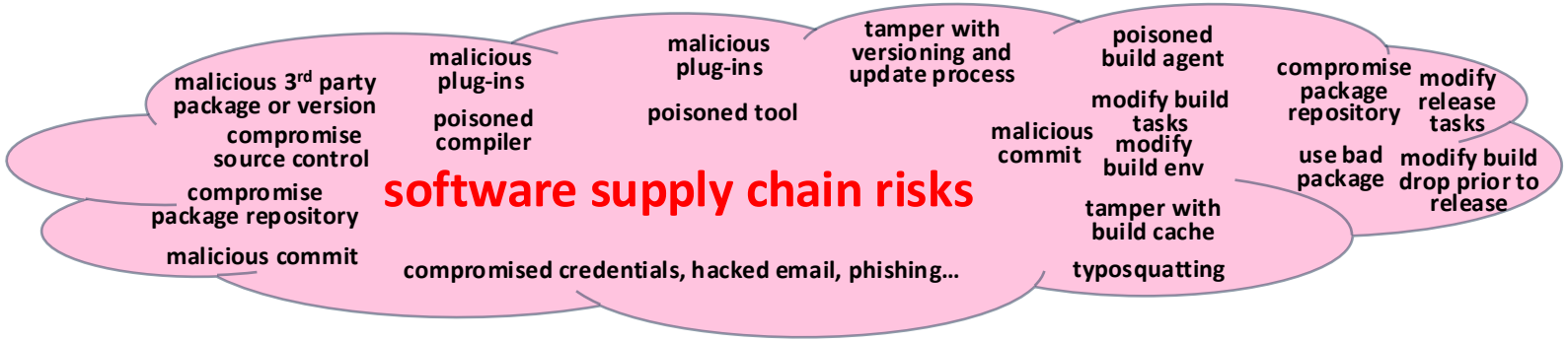
IMPACT:
Microsoft detected nearly 4,000 Nitol infections, which likely represents only a subset of the number of infected computers. The Nitol virus is capable of performing DDOS attacks, spreading through removable and network devices, and acting as a backdoor by allowing an attacker to run additional malware.

Although Microsoft did not explicitly address this in its filing, experts say 3322.org has long been associated with malware used in highly targeted attacks aimed at stealing corporate and government secrets from U.S. and other Western firms.

MITIGATION:
Microsoft received permission from a United States court to take down the network of Nitol-infected computers and successfully sinkholed the virus' command and control domain, 3322.org, and any other subdomains linked to malware. The takedown was part of a legal campaign called Project MARS (Microsoft Active Response for Security), which takes the lead in combating digital crime by obtaining court orders to seize web domains and computers without notifying the owners of the property.

- http://www.bbc.co.uk/news/technology-19585433
- http://krebsonsecurity.com/2012/09/microsoft-disrupts-nitol-botnet-in-piracy-sweep/
- http://www.theguardian.com/technology/2012/sep/14/malware-installed-computers-factories-microsoft
- http://www.theregister.co.uk/2012/09/13/botnet_takedown/

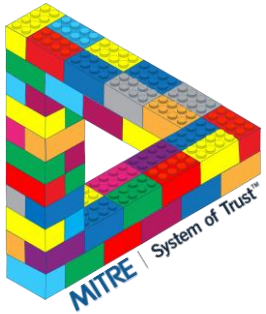
Software Supply Chain Risks

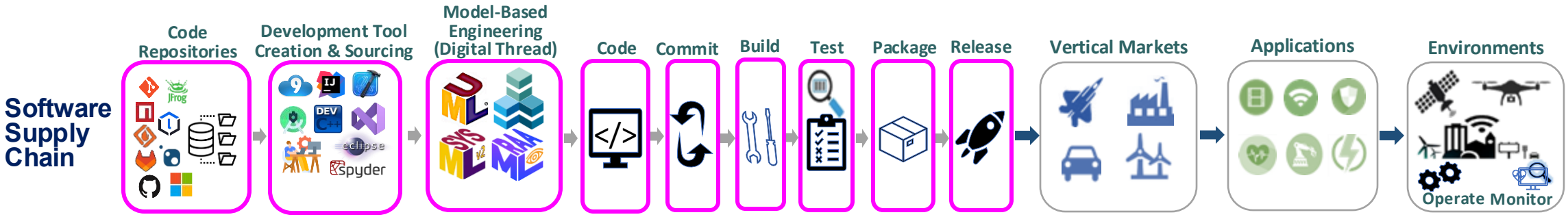


System of Trust™

Catalog of the different potential supply chain risks

SoT.MITRE.ORG

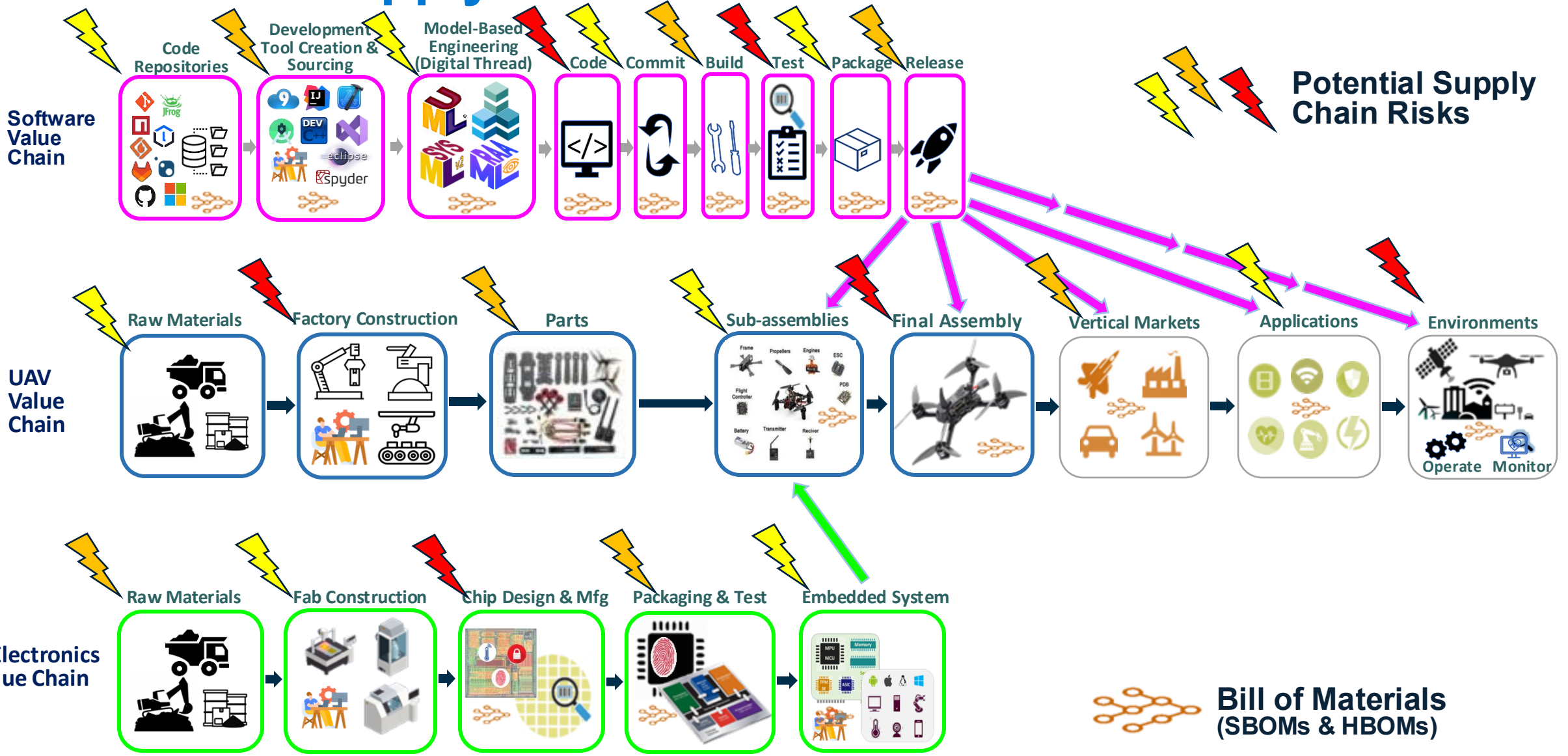




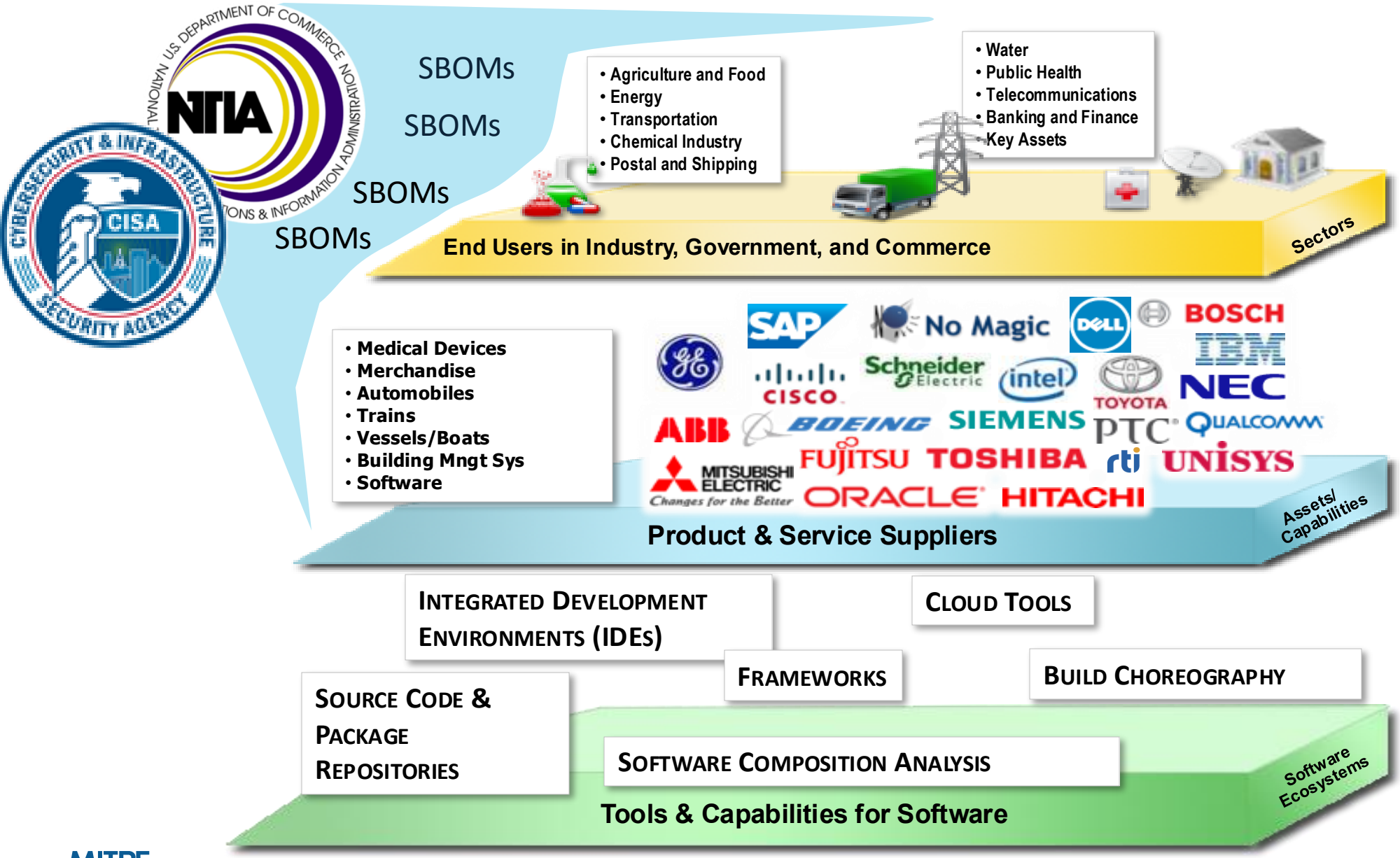
Threat List Sources:

- **Supply-chain Levels for Software Artifacts (SLSA)**, https://slsa.dev/spec/v1.0/threats-overview
- **Taxonomy of Attacks on Open-Source Software Supply Chains (SoK)**, 2023 IEEE Symposium on Security and Privacy - DOI: 10.1109/SP46215.2023.10179304
- **Uncovering Software Supply Chains Vulnerability: A Review of Attack Vectors, Stakeholders, and Regulatory Frameworks**, DOI: 10.1109/COMPSAC57700.2023.00281

Software Supply Chain



Enabling Adoption of SBOMs



System Package Data Exchange (SPDX) 3.0 SBOM Standard effort targeted here

SPDX®

THE LINUX FOUNDATION OMG Standards Development Organization

MITRE

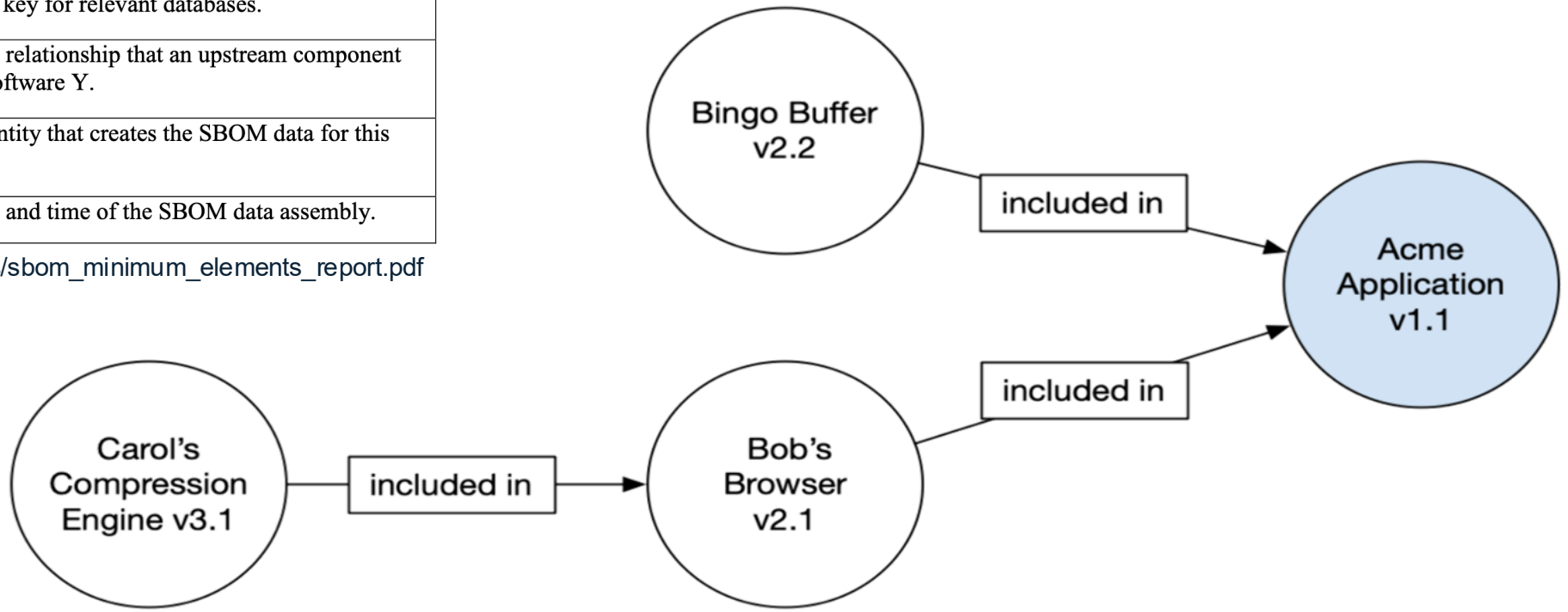
SBOM Definition

Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.

https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

Minimum Elements	
Data Fields	Document baseline information about each component that should be tracked: Supplier, Component Name, Version of the Component, Other Unique Identifiers, Dependency Relationship, Author of SBOM Data, and Timestamp.
Automation Support	Support automation, including via automatic generation and machine-readability to allow for scaling across the software ecosystem. Data formats used to generate and consume SBOMs include SPDX, CycloneDX, and SWID tags.
Practices and Processes	Define the operations of SBOM requests, generation and use including: Frequency, Depth, Known Unknowns, Distribution and Delivery, Access Control, and Accommodation of Mistakes.

https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

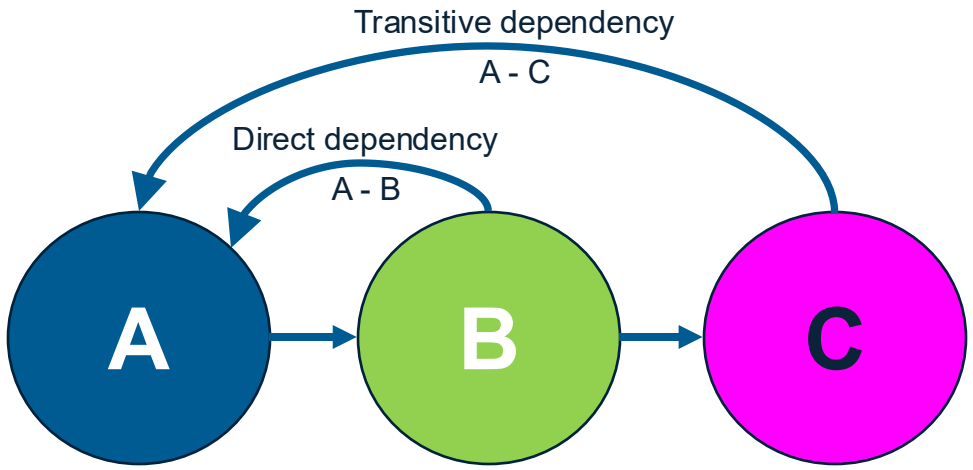


Source: https://www.ntia.gov/files/ntia/publications/ntia_sbom_framing_2nd_edition_20211021.pdf

ISO/IEC 5962:2021 (SPDX 2.1), OMG/LF SPDX 3.0, and ECMA-424 (CycloneDX 1.6)

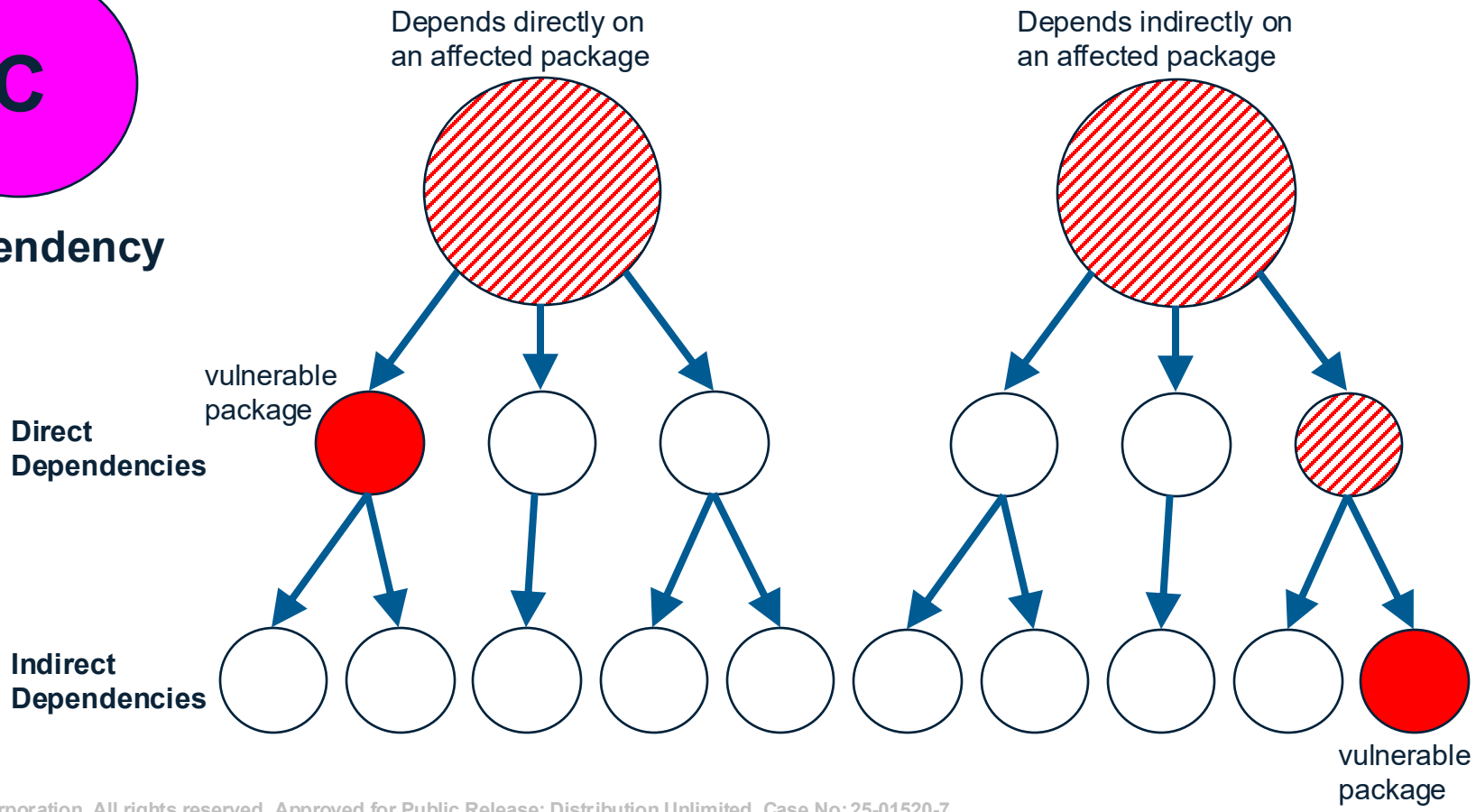
MITRE

Direct and Transitive Dependencies



Direct dependency vs Transitive dependency

Direct vulnerabilities vs Indirect (transitive) vulnerabilities



SBOMs – EO 14028, NIST SSDF, NSM, DoD & OMB memos

EO 14028 - May 2021

MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

NSM-8 - Jan 2022

JANUARY 19, 2022

Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems

NIST SP800-218 - Feb 2022

NIST Special Publication 800-218

Secure Software Development Framework (SSDF) Version 1.1:

Recommendations for Mitigating the Risk of Software Vulnerabilities

Murugiah Souppaya
Karen Scarfone
Donna Dodson

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-218

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Department of the Air Force Cyber Cake

OMB M-22-18 - Sep 2022

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

OMB M-23-16 - Jun 2023

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

Common Self Attestation Form - Mar 2024

Department of Homeland Security

DoD CIO Golden Dome memo - Jul 2025

OFFICE OF THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

GOLDEN DOME FOR AMERICA

JUL 24 2025

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Golden Dome for America (GDA) Cybersecurity Requirements

On May 20, 2025, the Secretary of Defense announced support for the Golden Dome for America (GDA), a next-generation missile defense shield formalized in Executive Order (EO) 14186. As stated in the EO, the Golden Dome will include space-based interceptors and sensors, all seamlessly integrated with U.S. systems and technology already in service, such as air and missile defense.

GDA's success will rely upon bold vision, innovation, and cutting-edge technology provided by the Defense Industrial Base (DIB). DIB companies, both large and small, are the targets of malicious cyber actors' intent on theft of intellectual property, disruption of operations, or espionage. GDA is a system of systems, reliant on numerous technologies integrated into a holistic system. To that end, the Department of Defense (DoD) must ensure the security of the GDA program through the application of supply chain requirements for the entirety of the GDA DIB ecosystem.

The GDA program office will ensure that all vendors who handle Controlled Unclassified Information (CUI) must comply with the prescribed level of information handling. This includes but are not limited to, Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, DFARS 252.204-7018, DFARS 252.204-7019, DFARS 252.204-7020 and, when published, and effective, the revised DFARS clause 252.204-7021. The revised DFARS clause 252.204-7021 will require contractors to verify compliance with the security requirements outlined in 32 Code of Federal Regulations (CFR) Parts 170 and 2002 for CUI, i.e. National Institute of Standards and Technology (NIST) SP 800-171 requirements and in DoD policy for breakthrough technologies and critical programs (including selected but not limited to requirements inside NIST SP 800-172).

Contractors participating in the GDA program with enhanced protections will be required to implement and verify compliance with selected requirements from NIST SP 800-172, as outlined in the revised DFARS clause 252.204-7021. Along with these requirements GDA vendors shall also meet the following requirements:

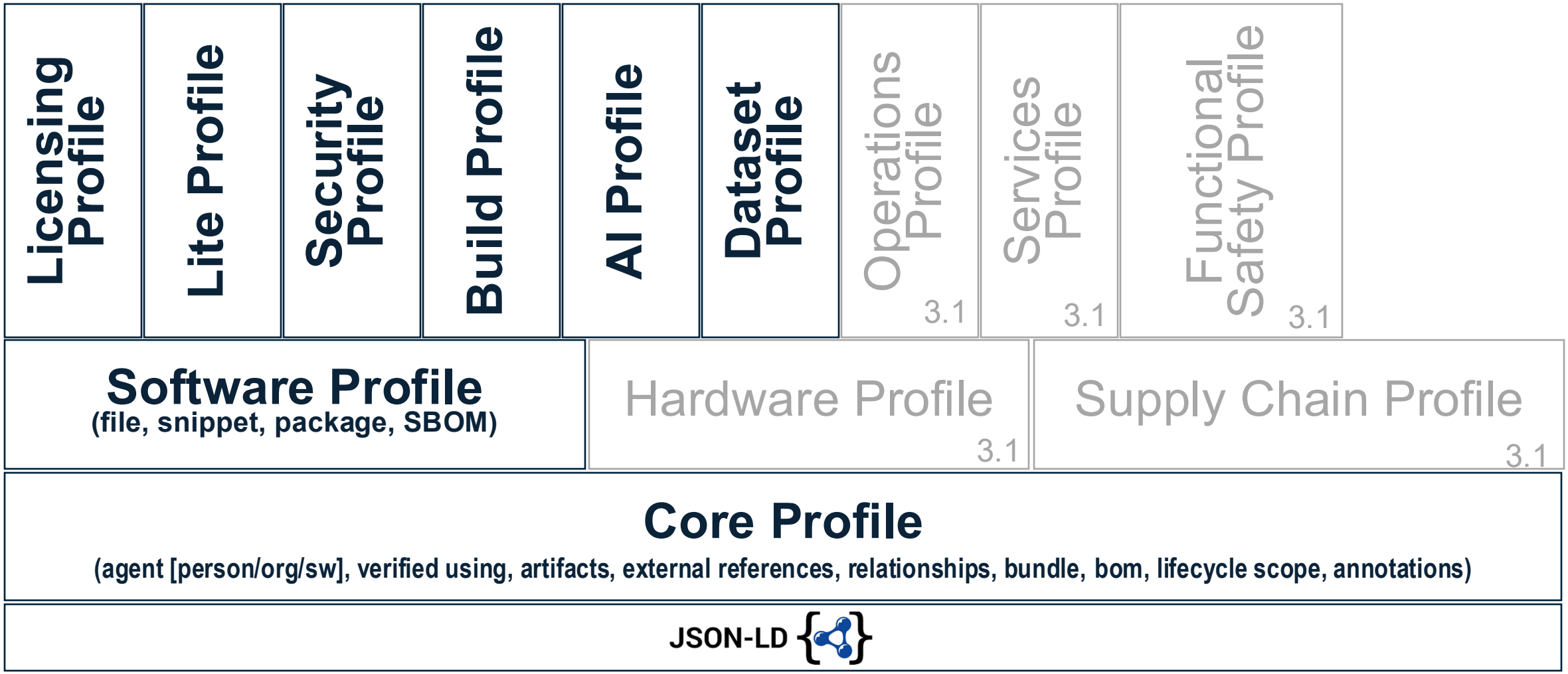
1. Each vendor in the supply chain must subscribe to the National Security Agency (NSA) Cybersecurity Collaboration Center's (CCC) threat intelligence sharing. In addition, vendors will be expected to conduct vulnerability monitoring and scanning. The NSA CCC offers additional services that may augment a vendor's responsibility to demonstrate this capability. For more information, contact DIB_DEFENSE@cyber.nsa.gov.

MITRE

Other SBOM Market Forces

- **U.S. regulations**
  - FDA requires SBOMs for medical devices at the premarket stage, including lifecycle and vulnerability data,
  - U.S. Army Directive mandates SBOMs for most software contracts starting in February 2025.
  - PCI DSS v4.0 introduced controls that will require organizations to maintain living, searchable SBOMs by 2025.
- **Global regulations**
  - EU Cyber Resilience Act and Germany's BSI TR 03183 are setting SBOM requirements for digitally connected products
  - Japan, the UK, and Australia are also advancing SBOM initiatives or offering strong guidance for adoption

SPDX 3.0 Scalable Modularity



SPDX Core Profile Relationships to Clarify Dependencies

DESCRIBES	DEPENDENCY_OF	PREREQUISITE_FOR	GENERATES	VARIANT_OF
DESCRIBED_BY	RUNTIME_DEPENDENCY_OF	HAS_PREREQUISITE	TEST_OF	FILE_ADDED
CONTAINS	BUILD_DEPENDENCY_OF	ANCESTOR_OF	TEST_TOOL_OF	FILE_DELETED
CONTAINED_BY	DEV_DEPENDENCY_OF	DESCENDENT_OF	TEST_CASE_OF	FILE_MODIFIED
DYNAMIC_LINK	OPTIONAL_DEPENDENCY_OF	DOCUMENTATION_OF	EXAMPLE_OF	PATCH_FOR
STATIC_LINK	PROVIDED_DEPENDENCY_OF	BUILD_TOOL_OF	METAFILE_OF	PATCH_APPLIED
AMENDS	TEST_DEPENDENCY_OF	EXPANDED_FROM_ARCHIVE	PACKAGE_OF	REQUIREMENT_FOR
COPY_OF	OPTIONAL_COMPONENT_OF	DISTRIBUTION_ARTIFACT	DATA_FILE_OF	SPECIFICATION_FOR
DEPENDS_ON	DEPENDENCY_MANIFEST_OF	GENERATED_FROM	DEV_TOOL_OF	OTHER

For more details see: https://spdx.github.io/spdx-spec/v2.3/relationships-between-SPDX-elements/

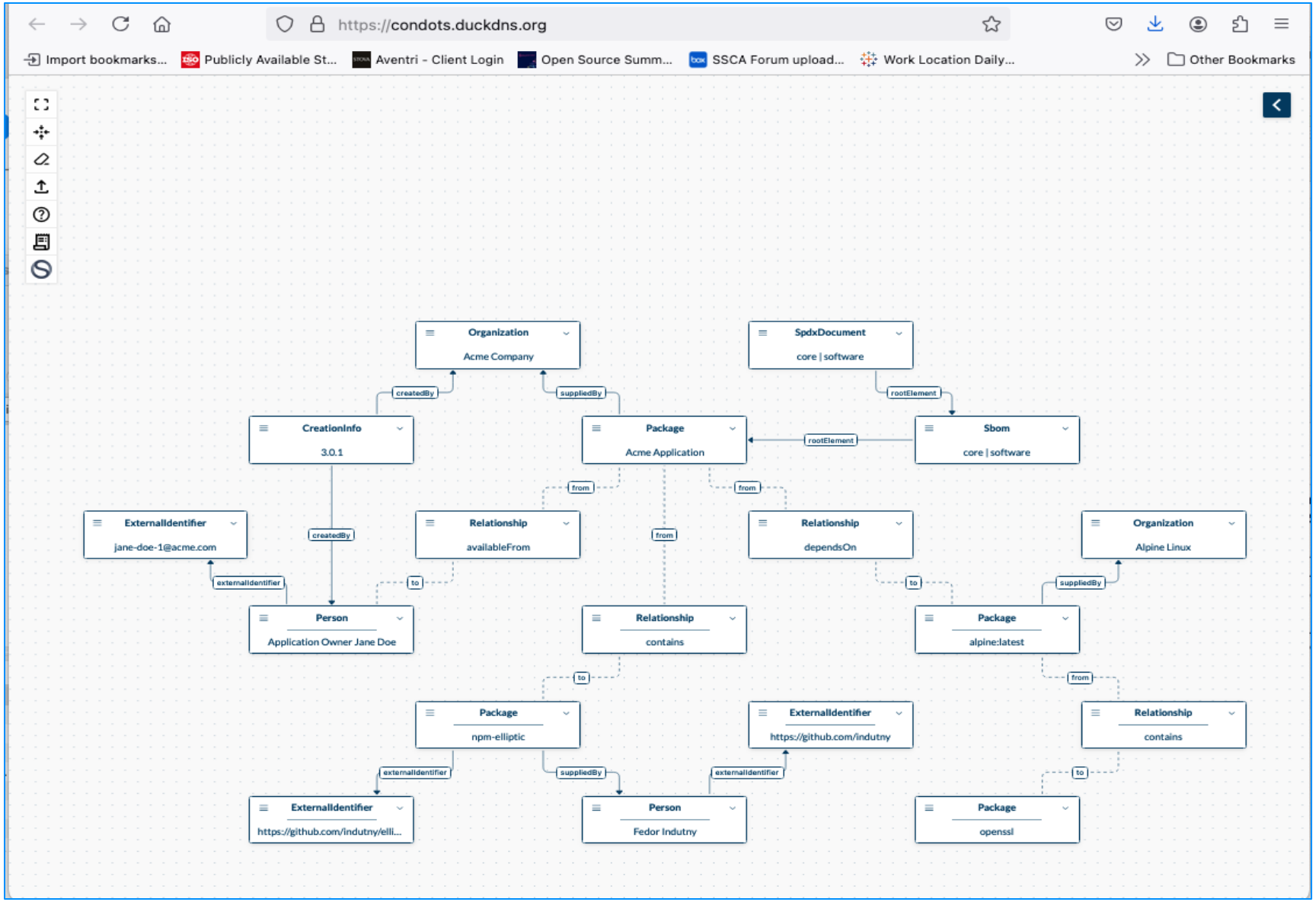
MITRE

Introduction to SPDX 3.0 tutorial

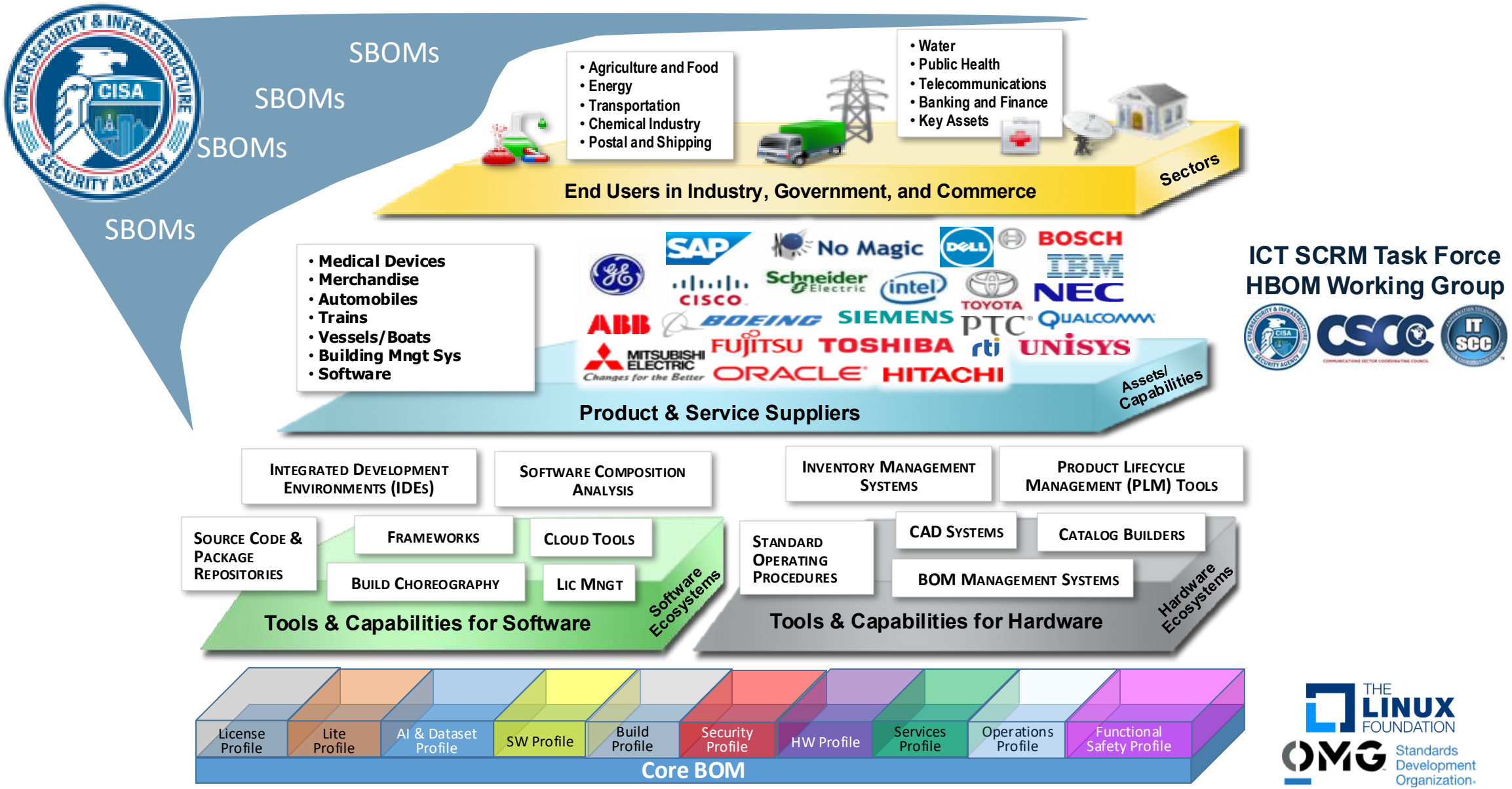
https://www.youtube.com/watch?v=J4hbb4PeLIU

DOTS graph tool for visualizing SPDX 3.0 materials

https://condots.duckdns.org/



Lowering Adoption Hurdles for SBOMs and more



ICT SCRM Task Force
HBOM Working Group

SPDX 3.0 → SPDX 3.1

Revised

SPDX SECURITY	Security information - vulnerability details related to software
SPDX BUILD	Build related information - provenance and reproducible builds
SPDX AI	AI model information - ethical, security, and model data
SPDX DATASETS	Dataset information - AI and other data use cases
SPDX LICENSING	Information about copyrights and licenses - supports compliance
SPDX SOFTWARE	Software information
SPDX CORE	Information used across all profiles

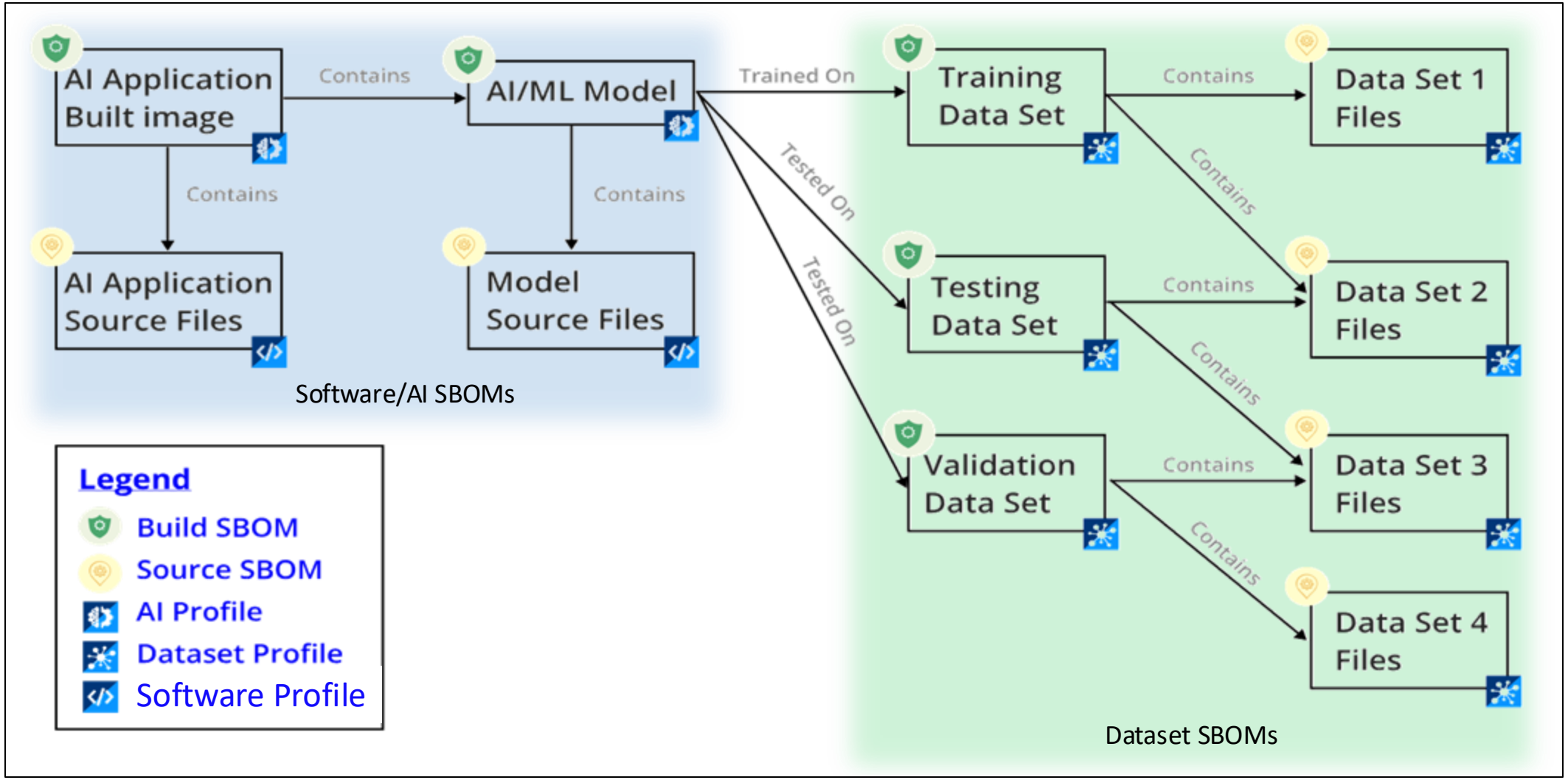
New

SPDX HARDWARE	Information specific to physical things (chips, boards, FPGAs,…)
SPDX SERVICES	Software service information
SPDX SAFETY	Functional safety information - requirements and test case mapping
SPDX OPERATIONS	Information about business operations (export control, cryptography,…)
SPDX SUPPLY CHAIN	Information about product supply chains

MITRE

27

Transparency with the AI, SW, & Dataset Profiles



https://www.linuxfoundation.org/hubfs/LF%20Research/lfr_spdx_aibom_102524a.pdf

MITRE

The Cautionary Tale of LAION-5B and Stable Diffusion

- One of the world's most popular text-to-image models, Stable Diffusion, used LAION-5B and its 5 billion images as a training source
- Standford researchers discovered over 1600 child pornography images in LAION-5B (Dec 2023)
- Virtually nobody had an inventory of AI dependencies to alert them to the issue, or to determine where LAION-5B was deployed.

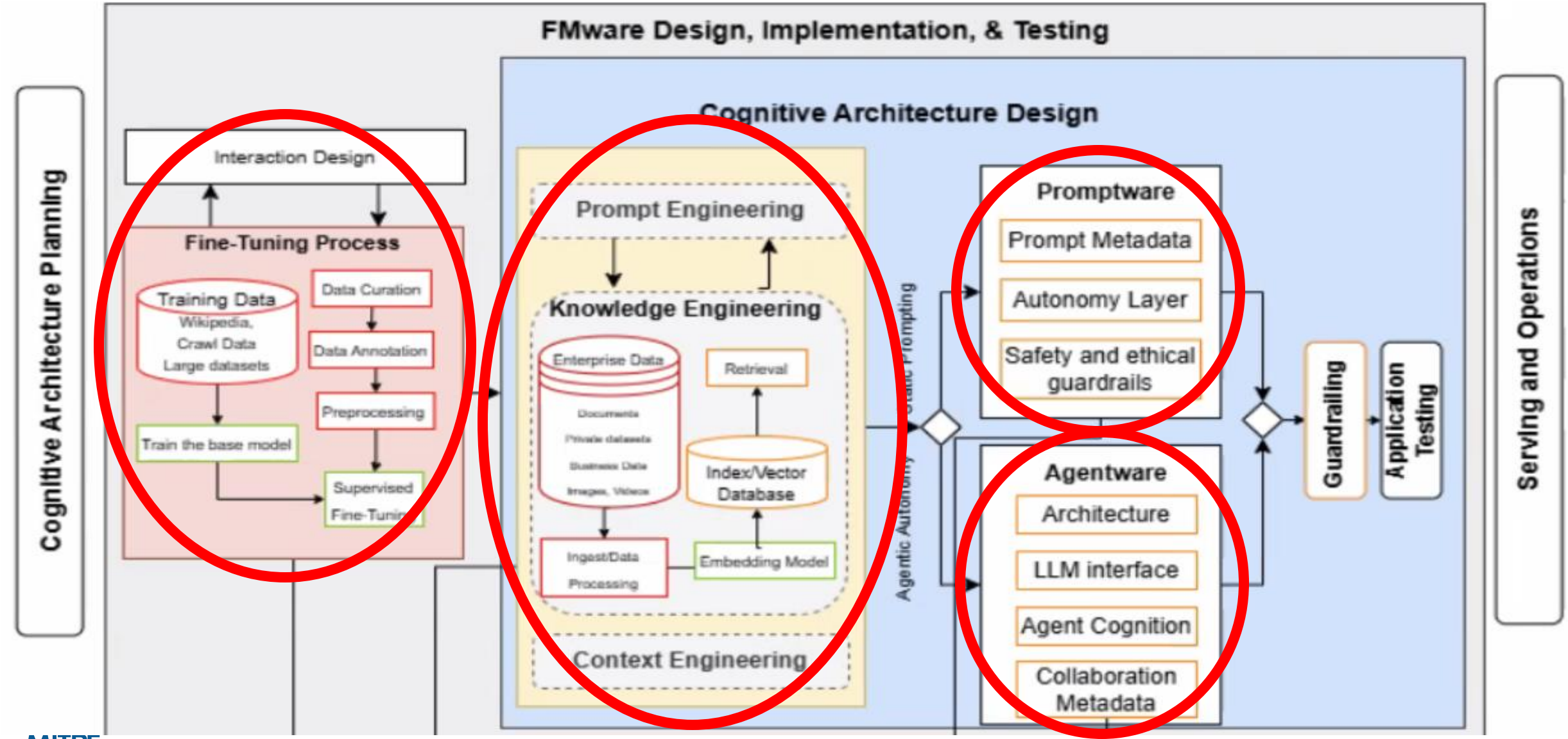
Dec 20, 2023

Courtesy of Daniel Bardenstein, Manifest

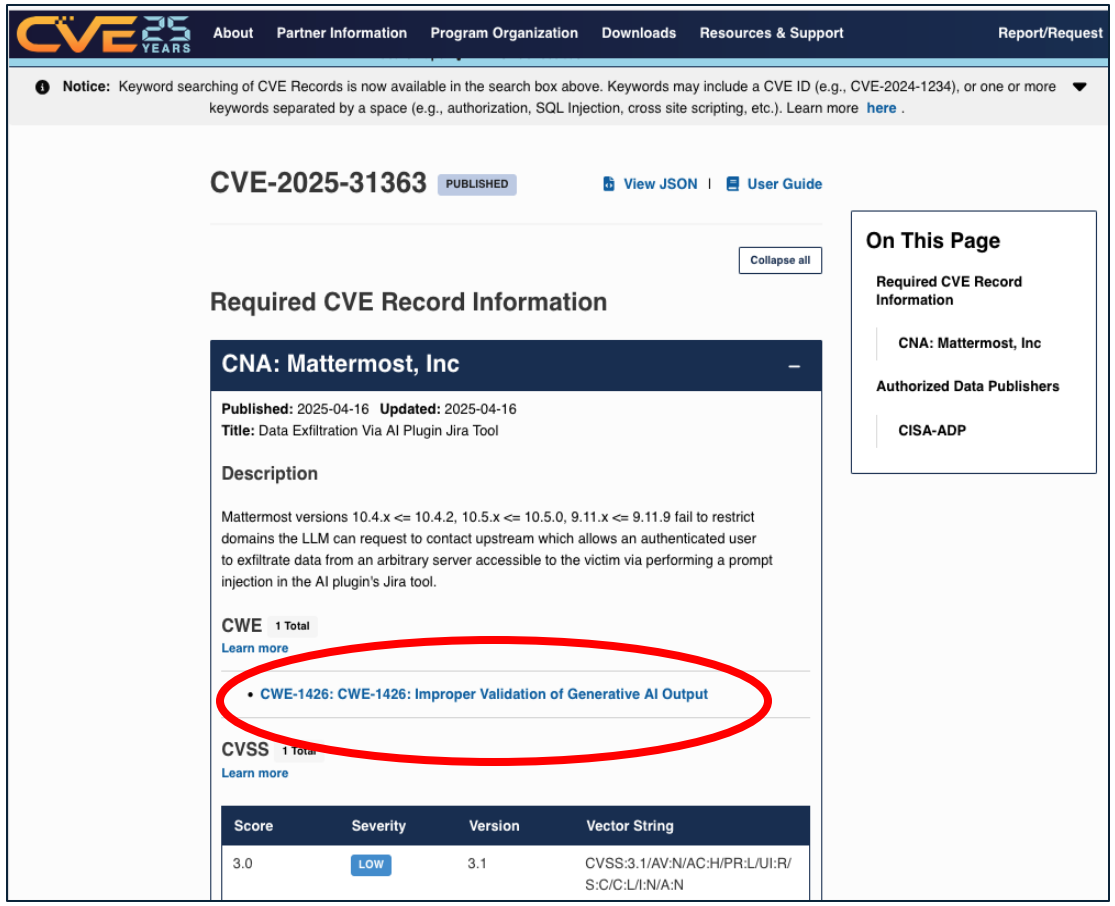
LAION-5B Response Questions

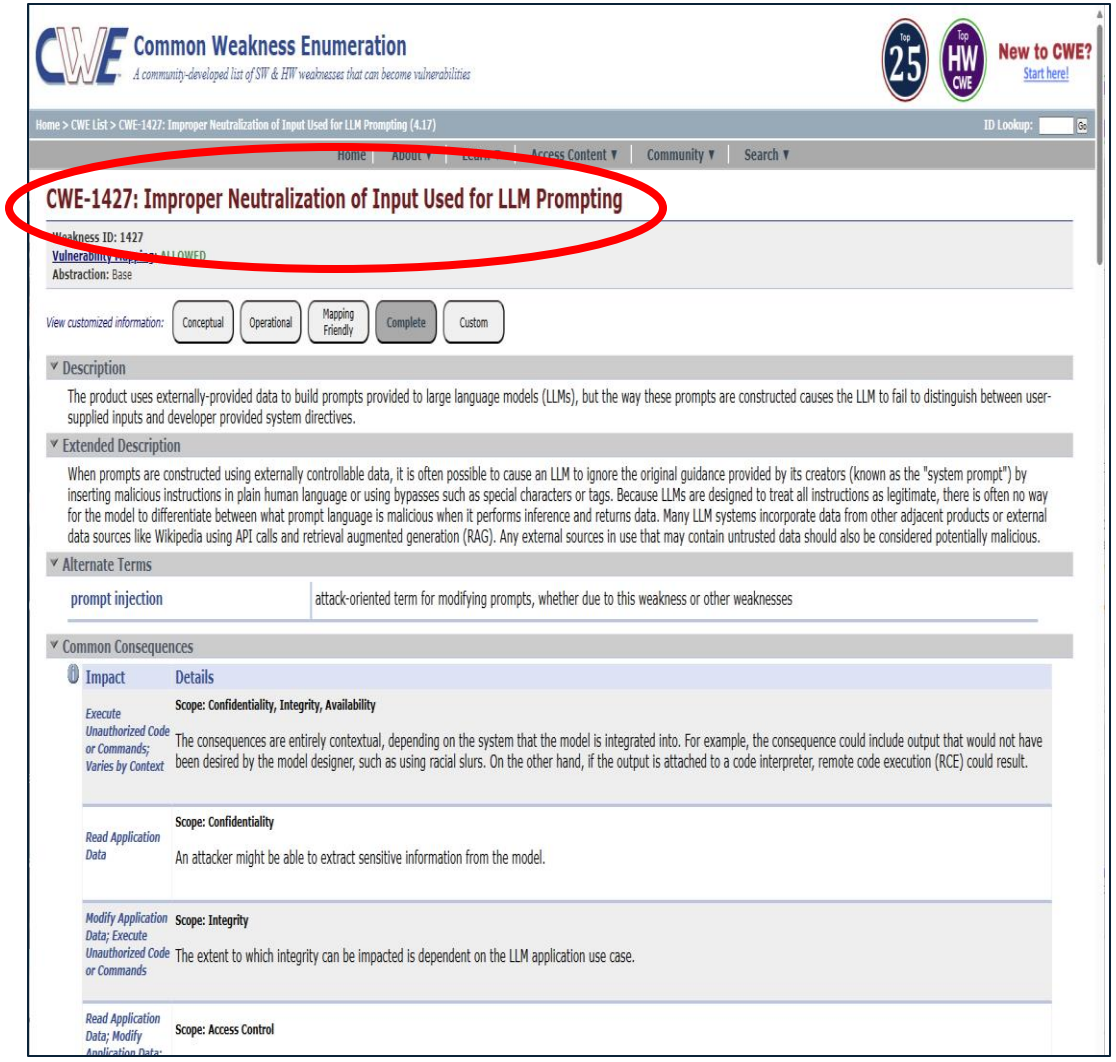
- Have we trained any of our models on this dataset?
- Have we used Stable Diffusion (or a specific AI model)?
- Have we derived any of our custom models from Stable Diffusion?

Enhancing the SPDX AI and Dataset Profiles



CVE and CWE are covering AI issues, but…



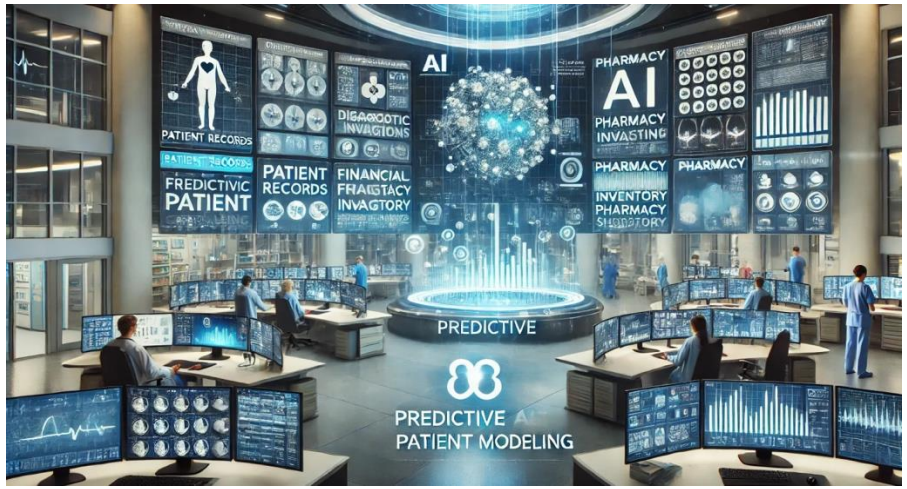


Most CVEs for AI systems are about traditional weaknesses – not weaknesses unique to AI

What Cyber Physical Capabilities are Powered by AI?

Is AI providing advice to humans or taking control?

Medical



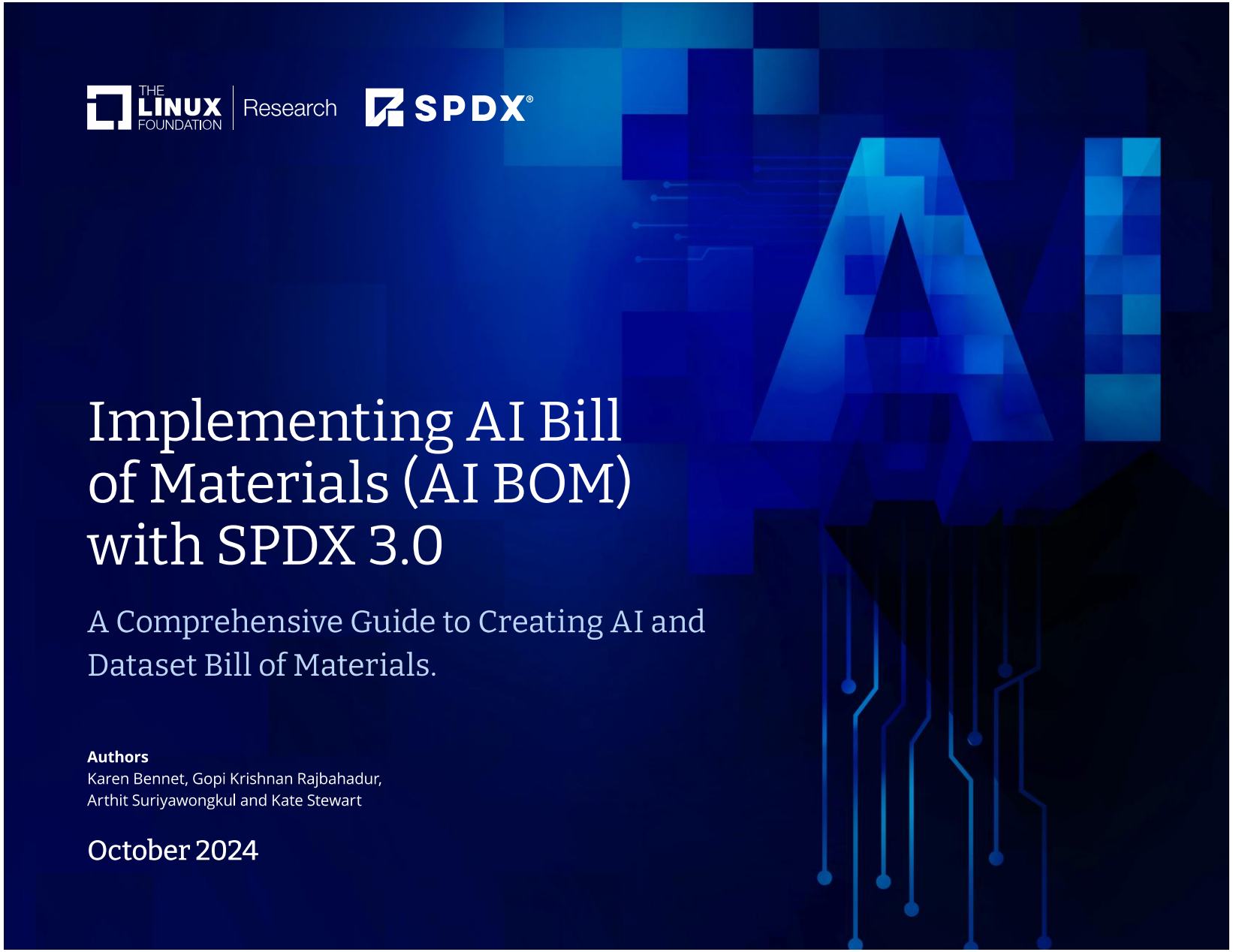
Buildings

Manufacturing

Pharma

Vehicles

Oil and Gas



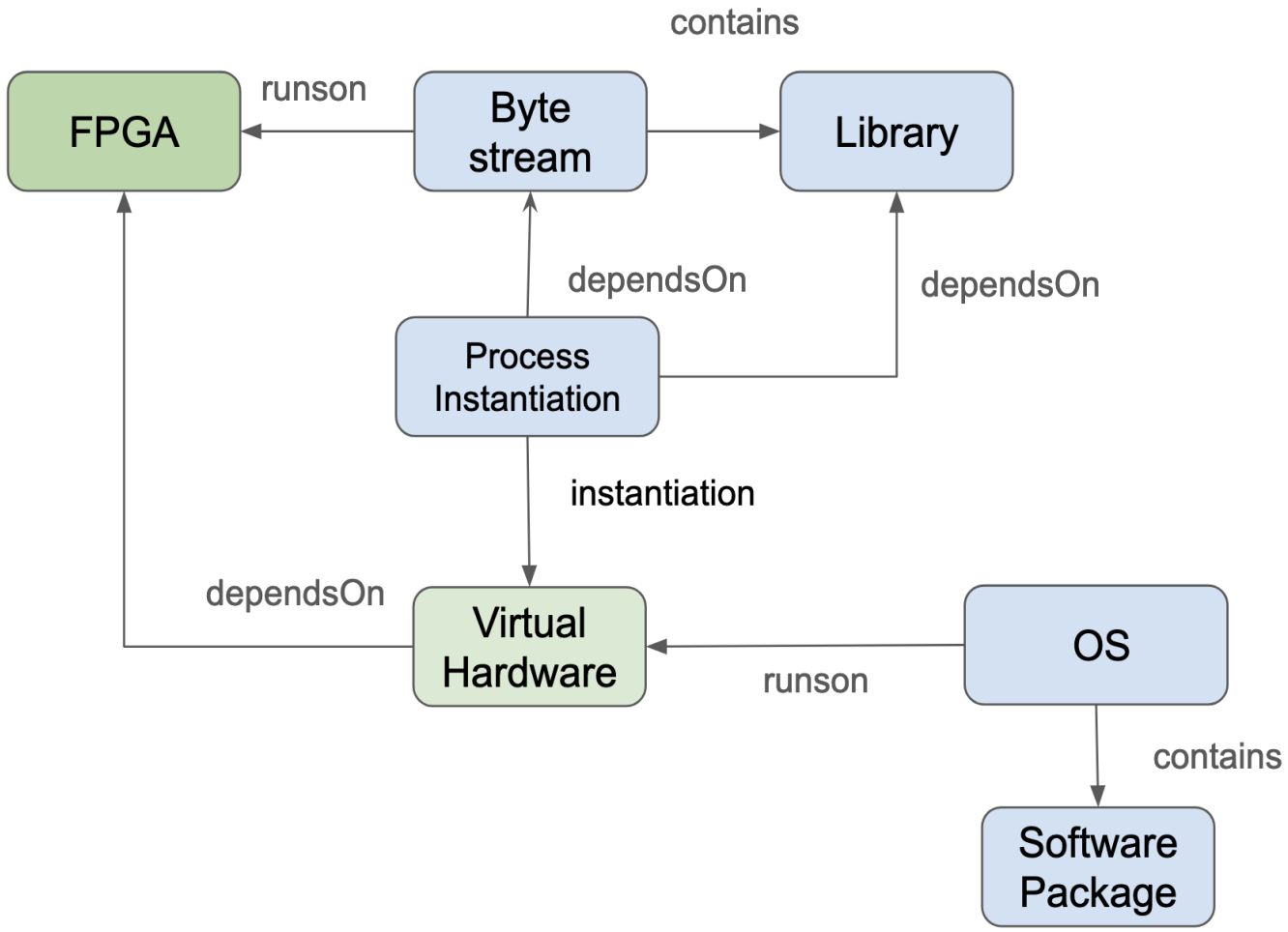
https://www.linuxfoundation.org/hubfs/LF%20Research/lfr_spdx_aibom_102524a.pdf

Hardware Profile for SPDX 3.1

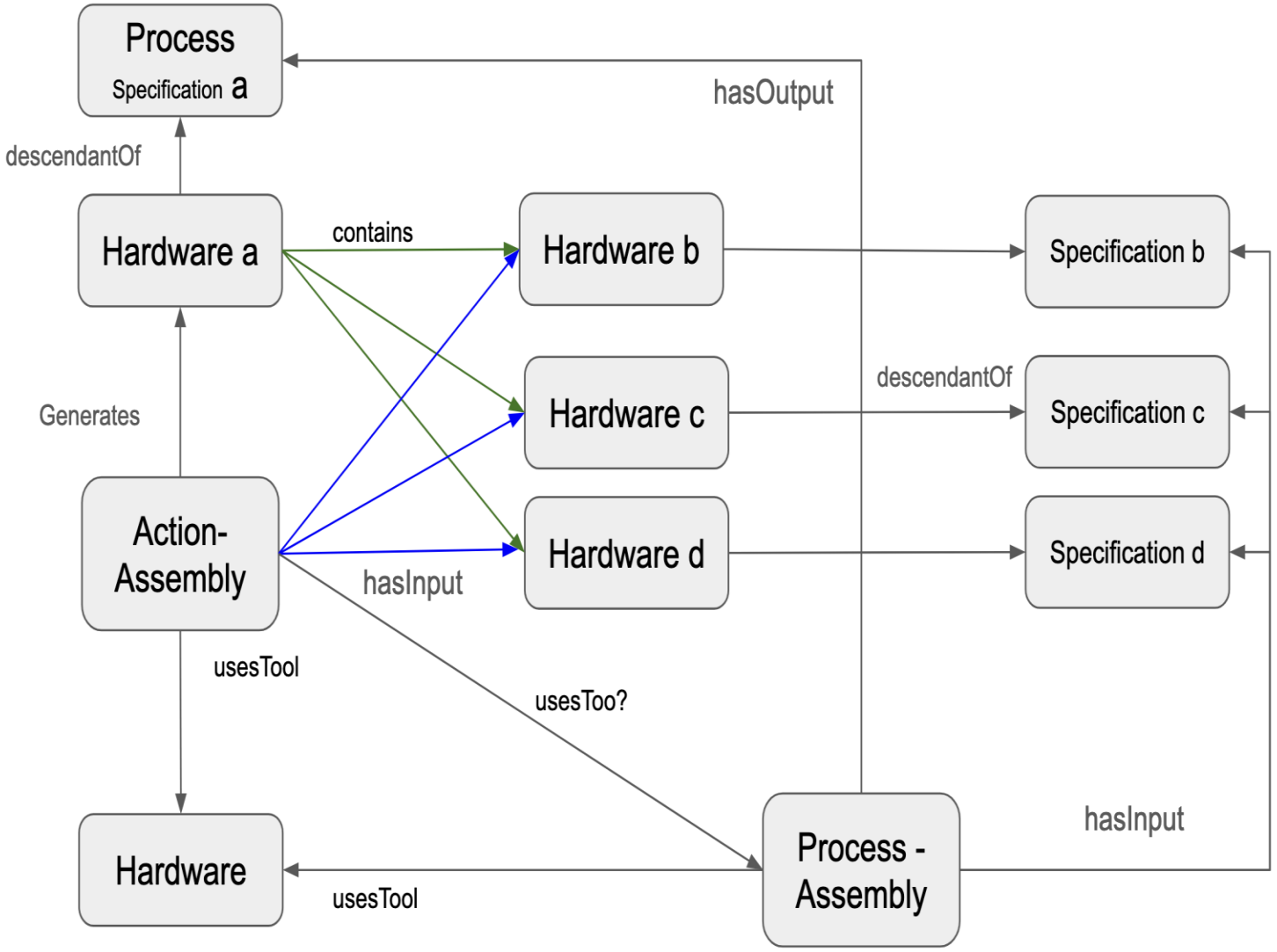
- Defining “Hardware”
  - Hardware is any product, real or virtual. A product is tangible, immutable and is the result of labor, or of a natural or artificial process.
    Any software product installed on a piece of hardware where the unit is made immutable, should be considered to be hardware.

Hardware Profile for SPDX 3.1

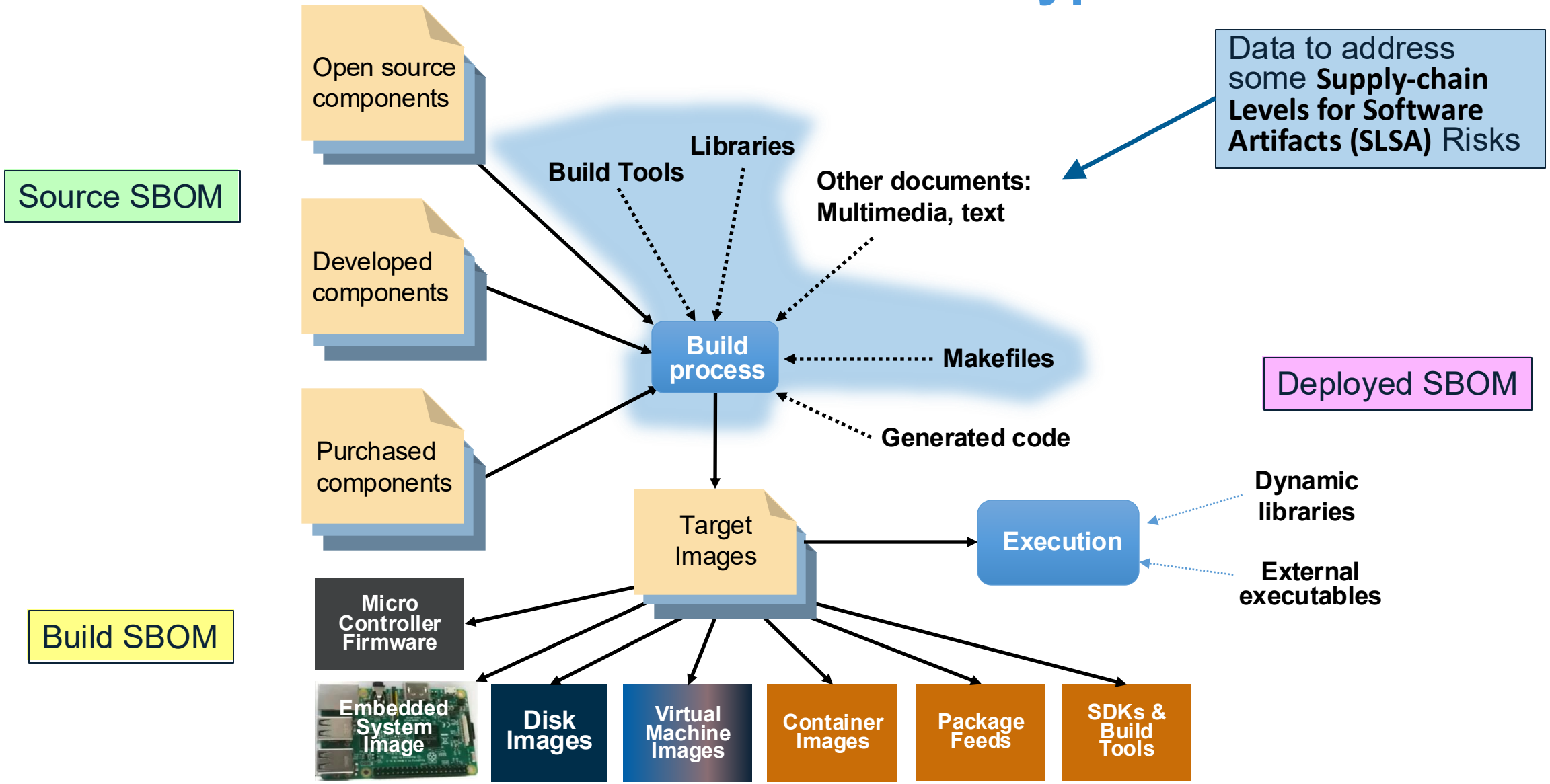
Defining Containers, VMs and Digital Twinning



Hardware Profile for SPDX 3.1



Software Bill of Materials Types



From the CISA Community-led Working Group on SBOM Tooling and Implementation, [cisa.gov/sbom]

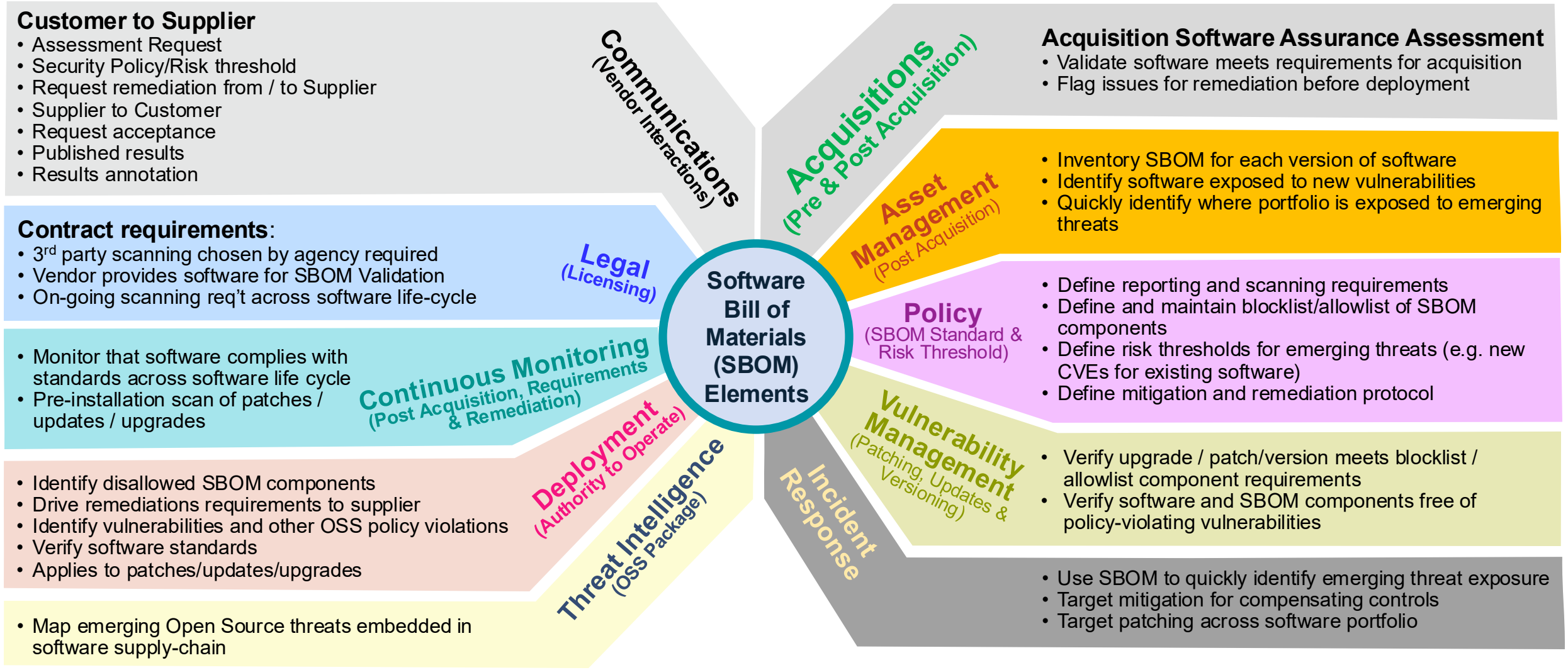
Table 1: SBOM Type Definition and Composition

SBOM Type	Definition	Data Description
Design	SBOM of intended design of included components (some of which may not exist) for a new software artifact.	Typically derived from a design specification, RFP, or initial concept.
Source	SBOM created directly from the development environment, source files, and included dependencies used to build an product artifact.	Typically generated from software composition analysis (SCA) tooling, with manual clarifications.
Build	SBOM generated as part of the process of building the software to create a releasable artifact (e.g., executable or package) from data such as source files, dependencies, built components, build process ephemeral data, and other SBOMs.	Typically generated as part of a build process. May consist of integrated intermediate Build and Source SBOMs for a final release artifact SBOM.
Analyzed	SBOM generated through analysis of artifacts (e.g., executables, packages, containers, and virtual machine images) after its build. Such analysis generally requires a variety of heuristics. In some contexts, this may also be referred to as a "3rd party" SBOM.	Typically generated through analysis of artifacts by 3rd party tooling.
Deployed	SBOM provides an inventory of software that is present on a system. This may be an assembly of other SBOMs that combines analysis of configuration options, and examination of execution behavior in a (potentially simulated) deployment environment.	Typically generated by recording the SBOMs and configuration information of artifacts that have been installed on systems.
Runtime	SBOM generated through instrumenting the system running the software, to capture only what is loaded and executing in memory, as well as external call-outs or dynamically loaded components. In some contexts, this may also be referred to as an "Instrumented" or "Dynamic" SBOM.	Typically generated from tooling interacting with a system to record the artifacts present in a running environment and/or that have been executed.

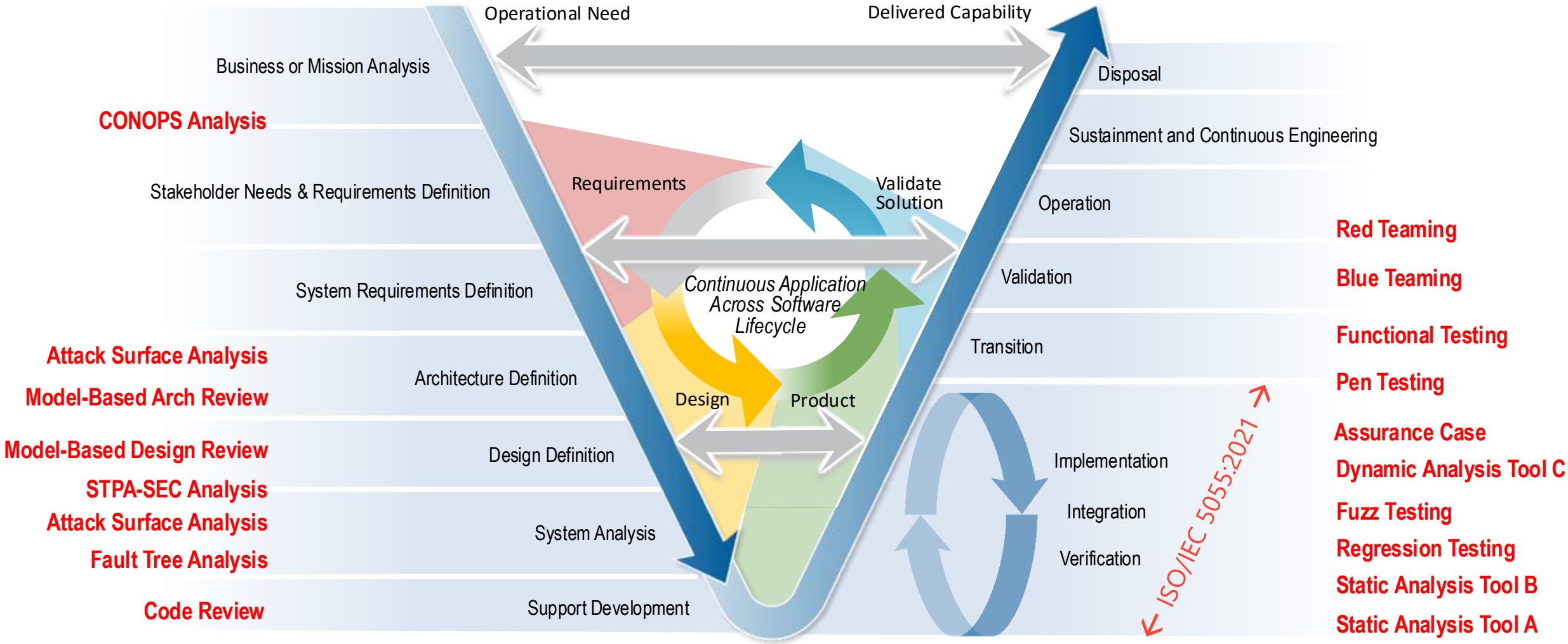
MITRE

SBOM Communications Channels and Use Cases

- ❑ Design
- ❑ Source
- ❑ Build
- ❑ Analyzed
- ❑ Deployed
- ❑ Runtime



Software Development and Assurance Evidence Sources



NOTE: *Lifecycle processes typically occur simultaneously, **not** in sequence; see ISO/IEC 15288 & 12207*

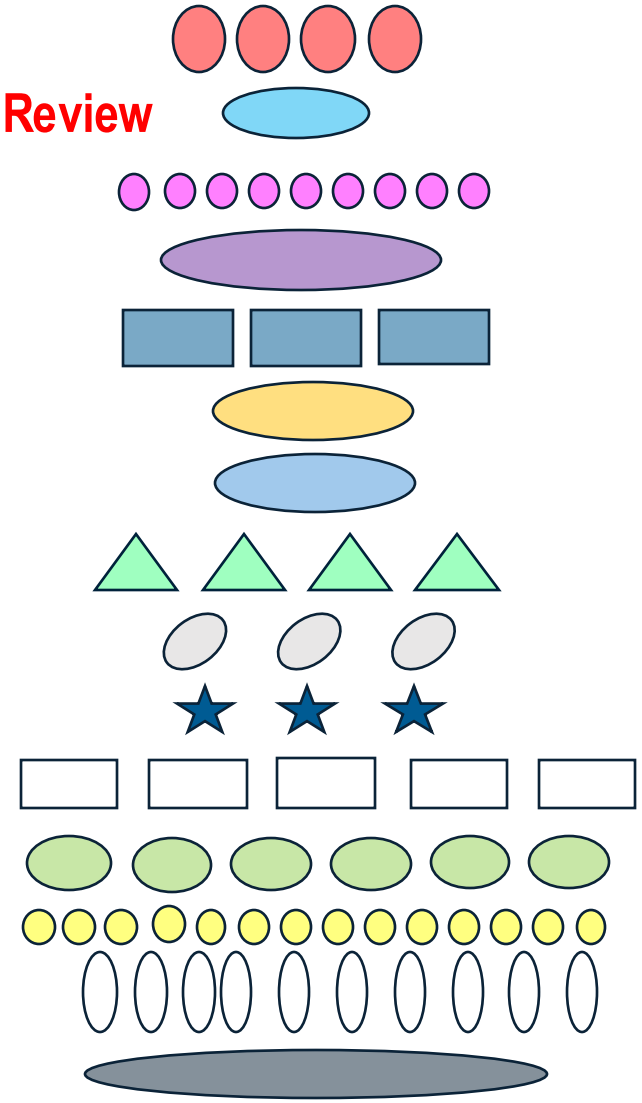
NOTE: *Implementation, Integration & Verification are often performed continuously & simultaneously with the aid of Integrated Development Environments (IDEs) & other tools.*

Figure 3-2 from "Software Trustworthiness Best Practices," 2020, https://www.iiconsortium.org/pdf/Software_Trustworthiness_Best_Practices_Whitepaper_2020_03_23.pdf

Utilizing Appropriate Detection Methods to Collect Evidence to Gain Assurance…

Artifacts	Detection Methods
CONOPS	CONOPS Evaluation
Requirements	Model-Based Arch/Design Review
Architecture	STP-SEC Analysis
Design	Functional Testing
System Model	Code Review
Process	Attack Surface Analysis
Code	Fault Tree Analysis
Binary	Static Analysis Tool A
Running Binary	Static Analysis Tool B
Environment of System	Regression Testing
Live System	Dynamic Analysis Tool C
	Fuzz Testing
	Pen Testing
	Blue Teaming
	Red Teaming

Coverage



CVE, reqts, CWE, functions, CAPEC, …

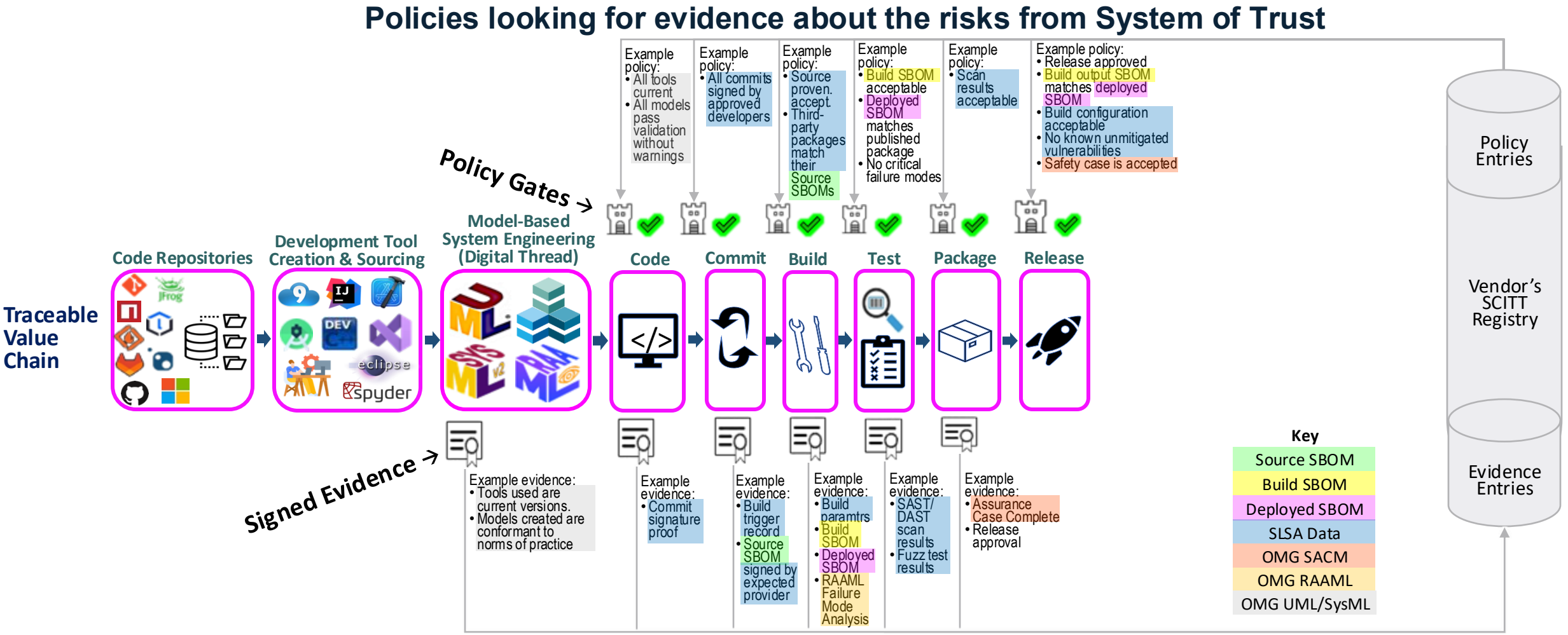
Most Important Quality & Functional Issues

MITRE

Multiple Sources of Assurance Evidence from Throughout the Lifecycle of the item(s) needing Assurance.

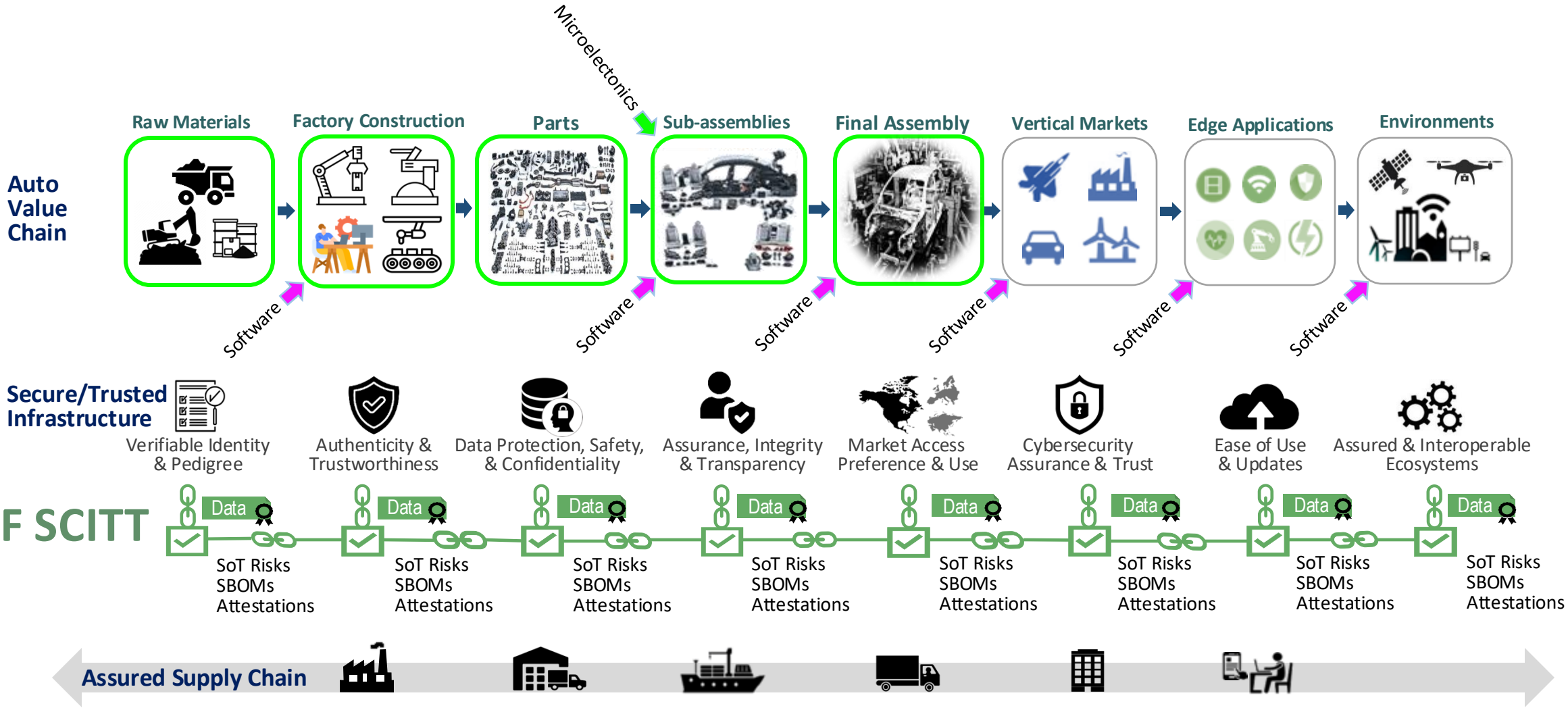
But how can we get this hightly proprietary data from our suppliers?

Example of IETF's Supply Chain Integrity, Transparency, and Trust (SCITT) standards in Software Supply Chain Security



Example of the IETF SCITT in SW Development

Example of IETF's Supply Chain Integrity, Transparency, and Trust (SCITT) standards in System Supply Chain Security



IETF SCITT

- **SCITT IETF Working Group** - focused on **specification development**. Charter and Meeting schedule outlined by the IETF: https://datatracker.ietf.org/wg/scitt/about/
  - IETF-SCITT Mailing List https://www.ietf.org/mailman/listinfo/scitt
  - IETF 124 (Montreal) SCITT Session is planned for Tuesday 4 Nov from 9:30-11:30am

- **SCITT Community** - focused on IETF **specification adoption** https://github.com/ietf-wg-scitt/ including advocacy, outreach, testing, ensuring interoperability of implementations, rapid prototyping, and open source libraries, tooling and examples, like the SCITT API Emulator https://github.com/microsoft/scitt-api-emulator, and View COSE tool https://v.gluecose.org/.
  - The **SCITT Community** is open to the public and new members are invited to join!

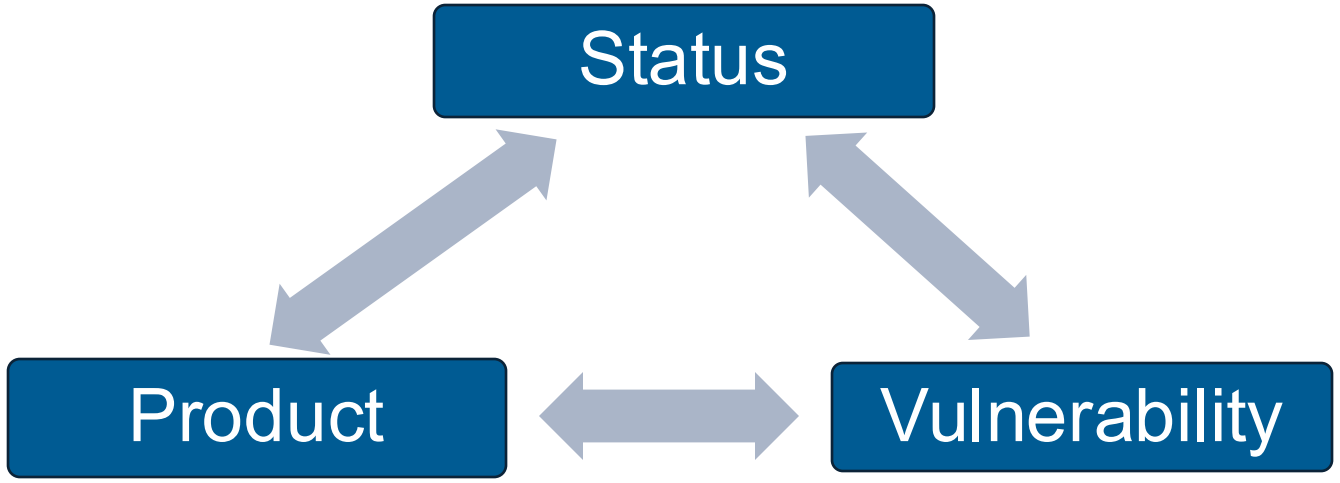
One More Thing…

Vulnerability Exploitability (VEX): Problems to solve

- Number of security advisories is rising
- SBOM adds to load } Scalability
- Not every vulnerability can be exploited } Exploitability

"VEXed by vulnerabilities that don't affect your product? Try this!" – July 2022
Allan Friedman (CISA, USA)
Thomas Schmidt (BSI, Germany)

Needed fields for VEX



"VEXed by vulnerabilities that don't affect your product? Try this!" – July 2022
Allan Friedman (CISA, USA)
Thomas Schmidt (BSI, Germany)

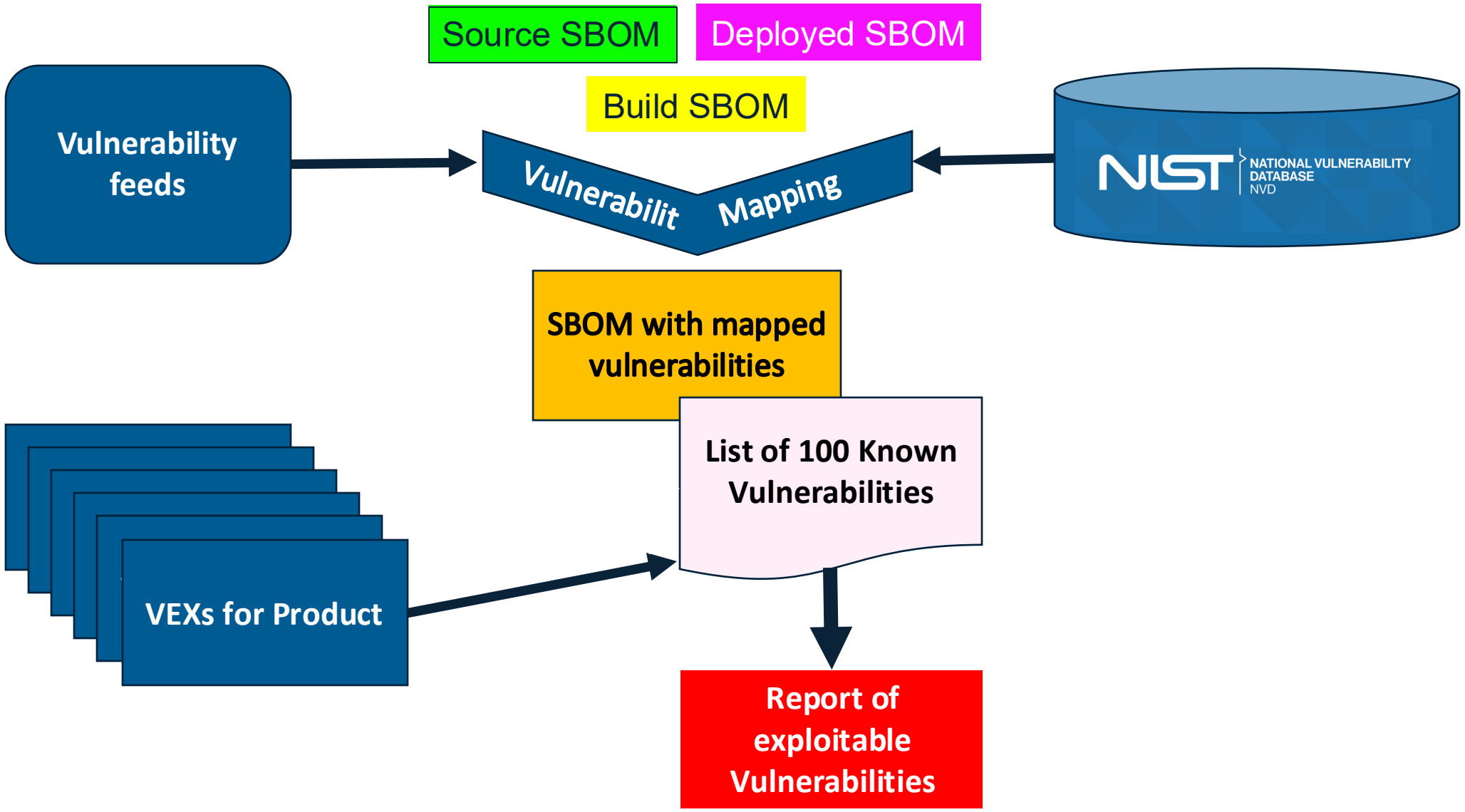
Required fields for a VEX

Metadata (author, id, timestamp)	
Product id	Product id
Vulnerability ID Vuln details Product Status Action statement / Impact statement	Vulnerability ID Vuln details Product Status Action statement / Impact statement

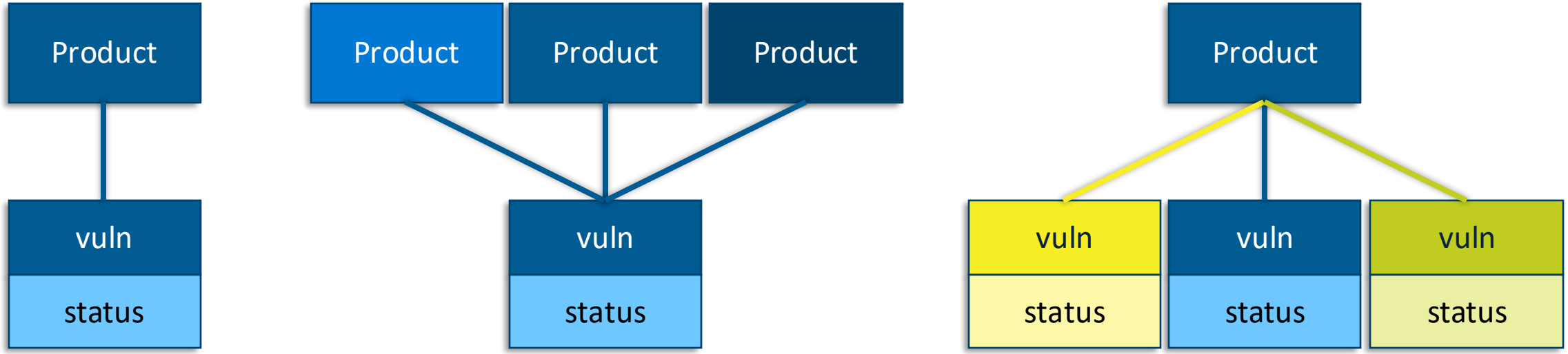
"VEXed by vulnerabilities that don't affect your product? Try this!" – July 2022
Allan Friedman (CISA, USA)
Thomas Schmidt (BSI, Germany)

MITRE

VEX and SBOM in a workflow…



“Modality” of VEX – Use Cases



“VEXed by vulnerabilities that don’t affect your product? Try this!” – July 2022
Allan Friedman (CISA, USA)
Thomas Schmidt (BSI, Germany)

MITRE

SBOM papers - three from MITRE, one from the Atlantic Council, and one from the Linux Foundation


Standardizing SBOM within the SW Development Tooling Ecosystem

Many end-user organizations across the world are facing operational and supply chain related questions about whether the software they are using to do their day-to-day work and support their ongoing business areas is authentic and unaltered, contains known vulnerabilities, or whether their use is proper and legal given the licensing terms placed on the constituent parts of that software by its developers. The fact that software is being used to run more and more of the critical aspects of each of our organization's business, embedded, and cyber-physical systems makes it these pressing and unavoidable questions for almost everyone.

Much attention has focused on identifying the needs for Software Bill of Materials (SBOM) information in end-user organizations, which extends to understanding the software content of their operational systems, the supplier communities of that software, whether that equipment has software embedded or they are directly supplying software. At the same time the software development tools ecosystem organizations, those who will be key in supplying the tools that are foundational to supplying automated SBOM information, need to be engaged and the SBOM standardization needs to support and help the integration of the different development, assessment, and analysis tools into the emerging DevSecOps abilities being explored across the market.

Minimal Common Information Needs

The following discussion explores several different ways an SBOM can be used to help understand and address software supply chain and operations risks in end-user organizations and identifies the minimal information needed in a SBOM to support those uses[1]. Following that is a discussion on the role that this same data could have in tool-to-tool exchanges within the software tools ecosystem and ideas about how that data could be captured as a specific tool-to-tool information exchange standard.

To be useful to end-user organizations an SBOM needs to include the basic information that enables correlating and connecting related information about the software as it moves through the supply chain and into operations. It is also critical that the SBOM be as small and concise as possible to help ease the integration and adoption and keep management of SBOM data as simple as possible. A key idea in driving that minimalization is to aim at having the data in the SBOM static and fixed. Any information that will change and evolve over time should be separately managed so it can be correlated and linked to the SBOM, but it should not be included in the SBOM. That does not mean that an SBOM is static. Better information or more refined information about a specific version of software may be created, discovered, or recovered and an updated SBOM authored with the new/revised information could be provided.

For example, information about what components contain components is something key to understanding the nature of the software linked to an SBOM. Once the component is created this information does not change and provides the organizational context for understanding what other software components were included by the developers of the components and having it in the SBOM seems essential to the functionality of SBOMs in an enterprise.

However, information about vulnerabilities in the software should be separate from the SBOM since new ones are being discovered all the time and the knowledge about what to do about the vulnerability, how to mitigate it and address it also changes. To be operationally useful any organization planning to utilize SBOMs for security of their systems will need to have activities that can connect the information in the SBOMs to their vulnerability management activities, but that mapping is a separate activity, one enabled and enhanced by future pervasive existence of SBOMs for all of the software in the enterprise.

On the other hand, an example of one type of information that could be considered for inclusion in the SBOM is the licensing terms for the software when it is created. Organizations can change licensing terms whenever they like but for a specific version of the software that licensing is fixed at the point of release/creation and can safely be included in the SBOM. If the licensing terms of software are of concern the organization would need an organizational ability to understand and map the terms of licensing of the specific SBOMs for the different versions of software they will have in their enterprise and use they will

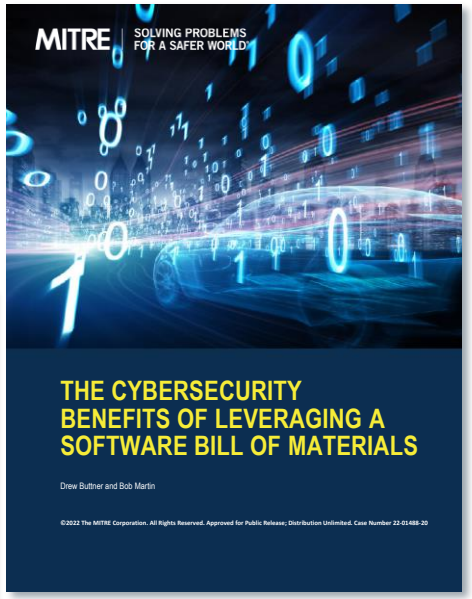
[1] Based primarily on the National Telecommunications and Information Agency's (NTIA's) Software Transparency efforts <www.ntia.doc.gov/SoftwareTransparency>

1

© 2019 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case No: PR_19-01876-16

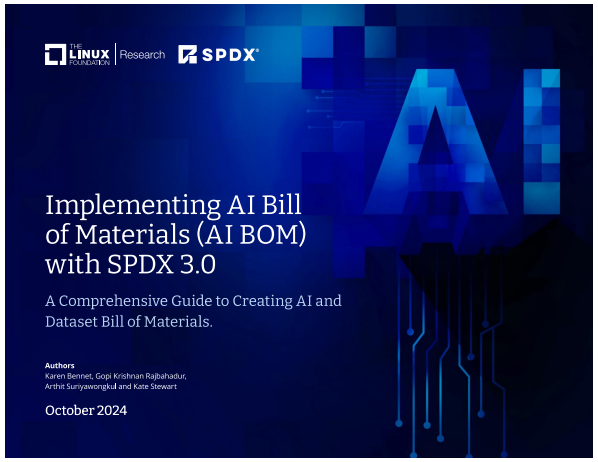
https://www.mitre.org/sites/default/files/2021-10/pr-19-01876-16-standardizing-sbom-within-the-sw-development-tooling-ecosystem.pdf

https://www.mitre.org/sites/default/files/publications/pr-21-0278-deliver-uncompromised-securing-critical-software-supply-chains.pdf



https://www.mitre.org/sites/default/files/2022-10/cybersecurity_benefits_of_sbom_september_2022.pdf

https://www.atlanticouncil.org/wp-content/uploads/2022/11/AC_SBOM_IB_v2-002.pdf



https://www.linuxfoundation.org/hubfs/LF%20Research/lfr_spdx_aibom_102524a.pdf

Questions?

ramartin@mitre.org

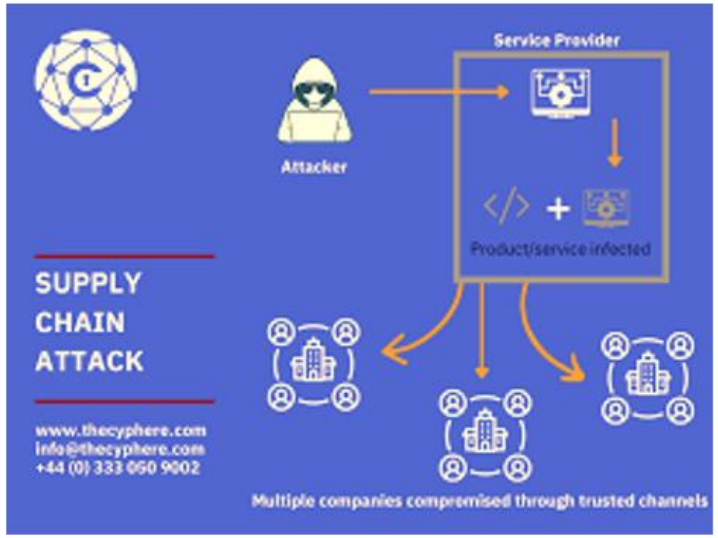
MITRE

Final Thoughts…

UNCLASSIFIED

Adversary | ICT Supply Chain Relationship

When the adversary **exploits** your supply chain



e.g. Solar Winds

When the adversary **becomes** your supply chain

Bad Actor

Commercial software
OEM Products

Job requisitions for US company

Senior Software Engineer - XXX Technologies
St Petersburg, Russia

Front-End Developer (Angular) – VXXX Inc
St Petersburg, Russia

What's in your code?

UNCLASSIFIED

MITRE