Establishing Trustworthy Software Supply Chains

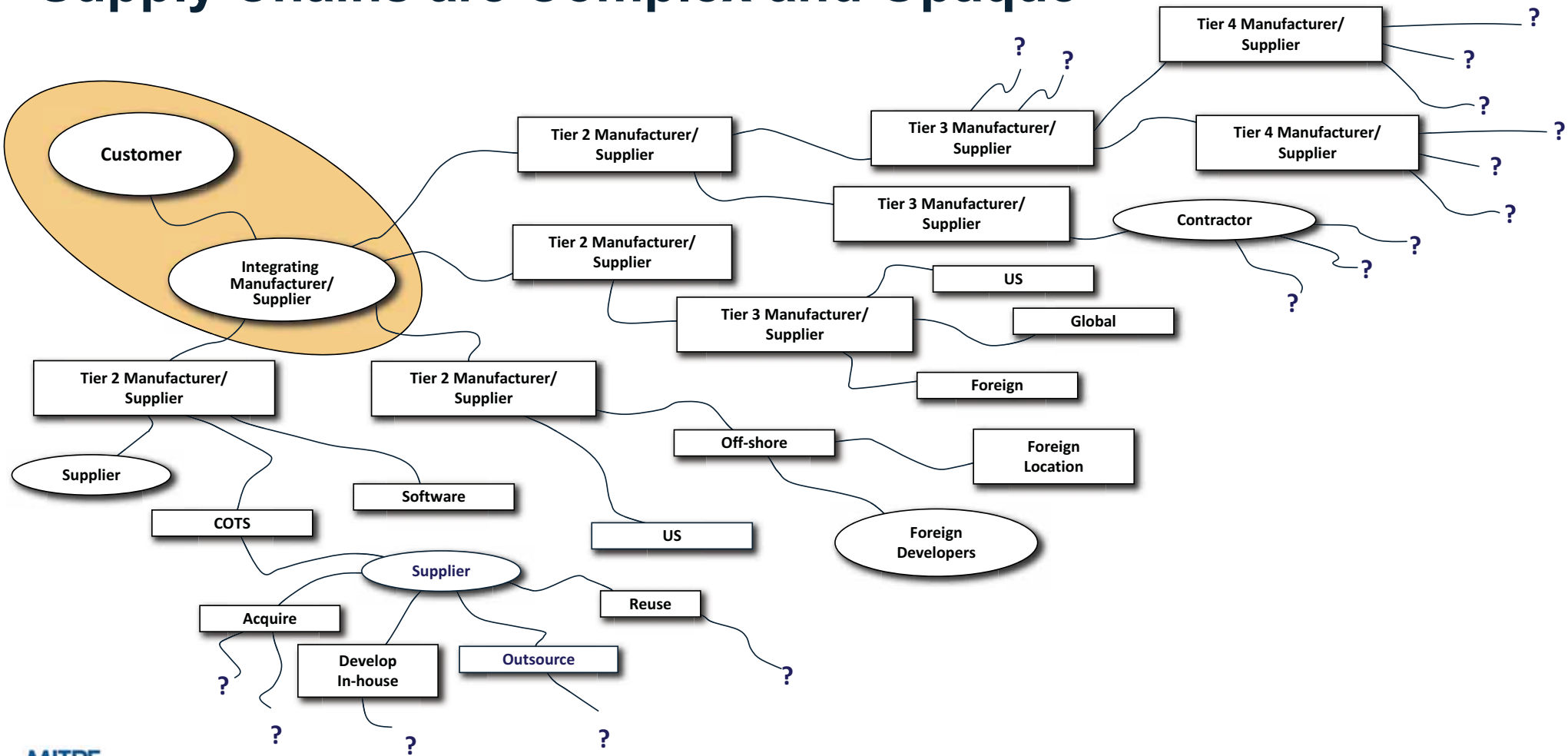
Sr. Software and Supply Chain Assurance Prin. Eng.
Cross Cutting Solutions and Innovation Dept.
Cyber Solutions Innovation Center
MITRE Labs

October 28, 2021

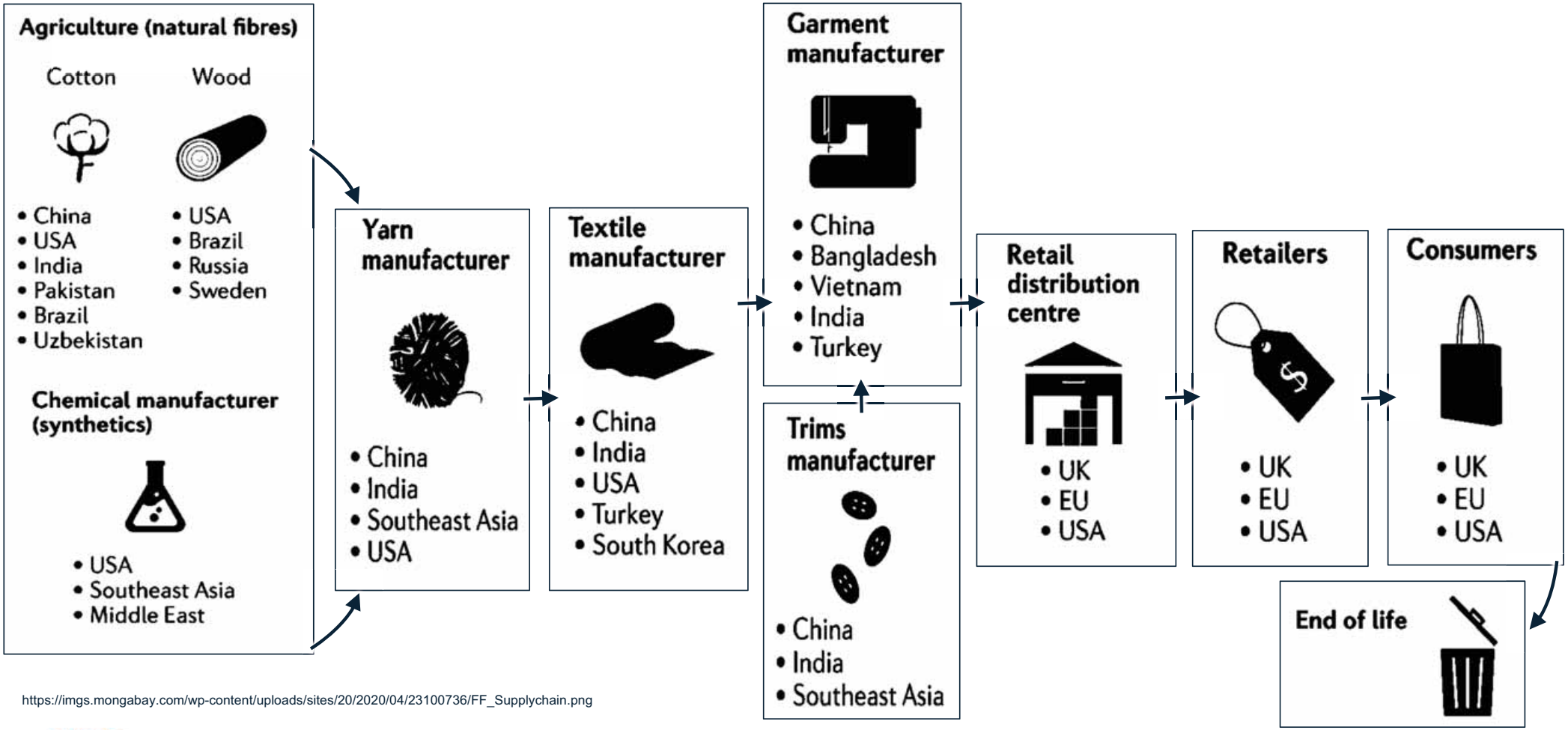
MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

Computational Cybersecurity in Compromised Environments
2021 Fall Workshop | October 27-28 | Virtual

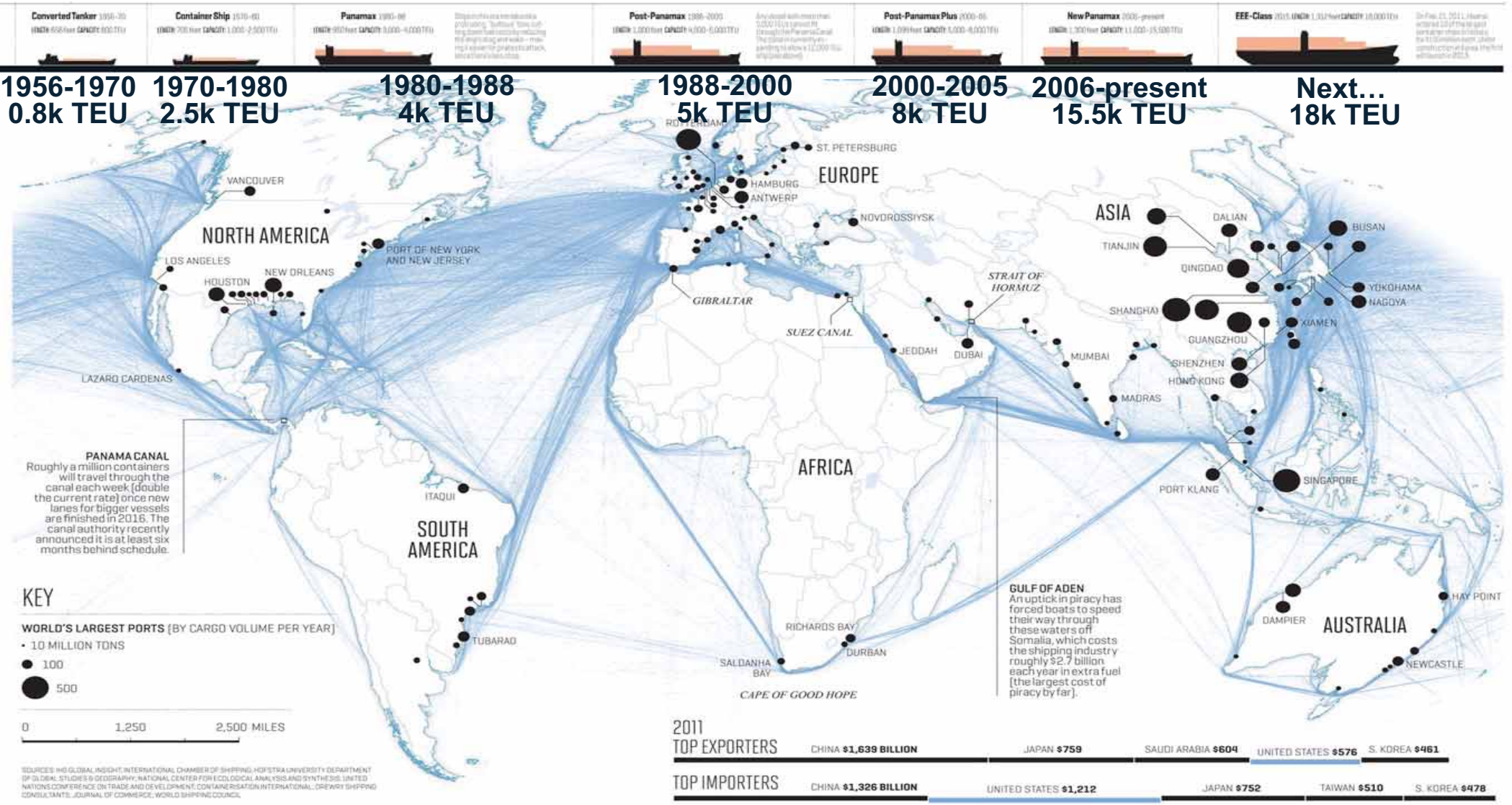
Supply Chains are Complex and Opaque



Supply Chain Example – Consumer Clothing



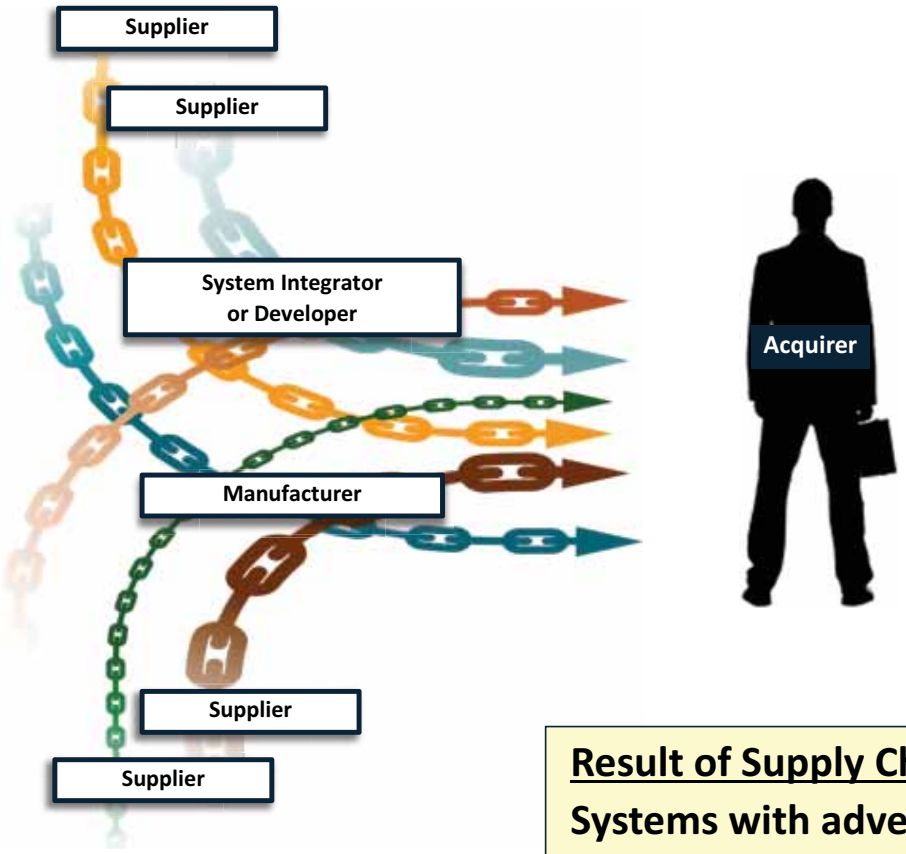
https://imgs.mongabay.com/wp-content/uploads/sites/20/2020/04/23100736/FF_Supplychain.png



SOURCES: IHS GLOBAL INSIGHT; INTERNATIONAL CHAMBER OF SHIPPING; HOFSTRA UNIVERSITY DEPARTMENT OF GLOBAL STUDIES & GEOGRAPHY; NATIONAL CENTER FOR ECOLOGICAL ANALYSIS AND SYNTHESIS; UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT; CONTAINERISATION INTERNATIONAL; DREWRY SHIPPING CONSULTANTS; JOURNAL OF COMMERCE; WORLD SHIPPING COUNCIL

MITRE

Supply Chain Trustworthiness: Intentional and Unintentional Acts



Based on SEI/CMU materials

Intentional acts

- Counterfeit products
- Disruption, hijacking, theft, civil unrest,…
- Malicious taint or insertion

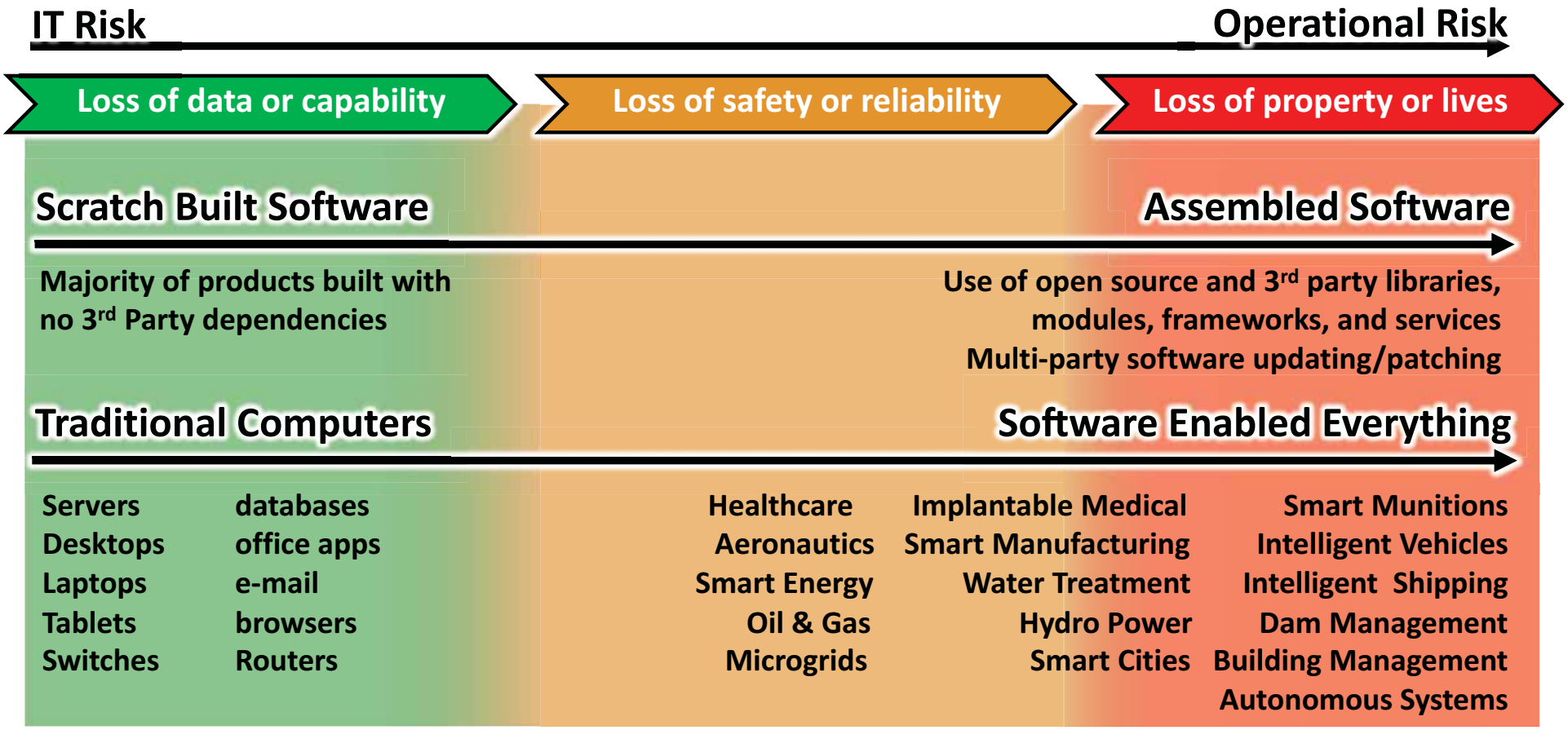
Unintentional acts

- Poor quality/tainted goods/shortages/weather disruptions
- Vulnerable software/hardware inserted unintentionally (components/modules w/CWEs and/or CVEs)

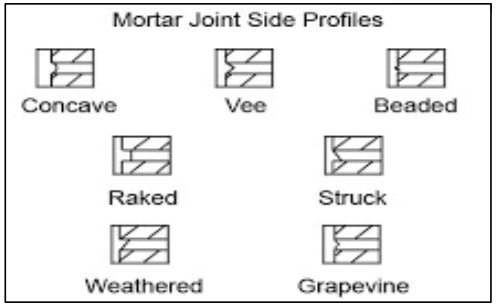
Result of Supply Chain Attacks:

Systems with adverse behaviors including functional degradation, data exfiltration, espionage, adversarial control and disruption.

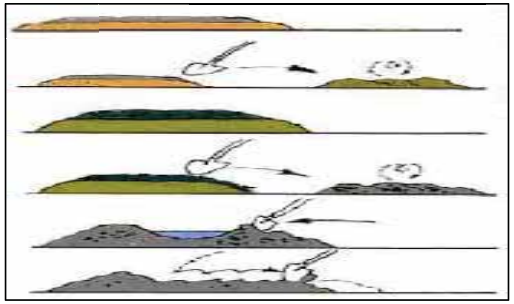
Software is Ubiquitous, Assembled, and Critical



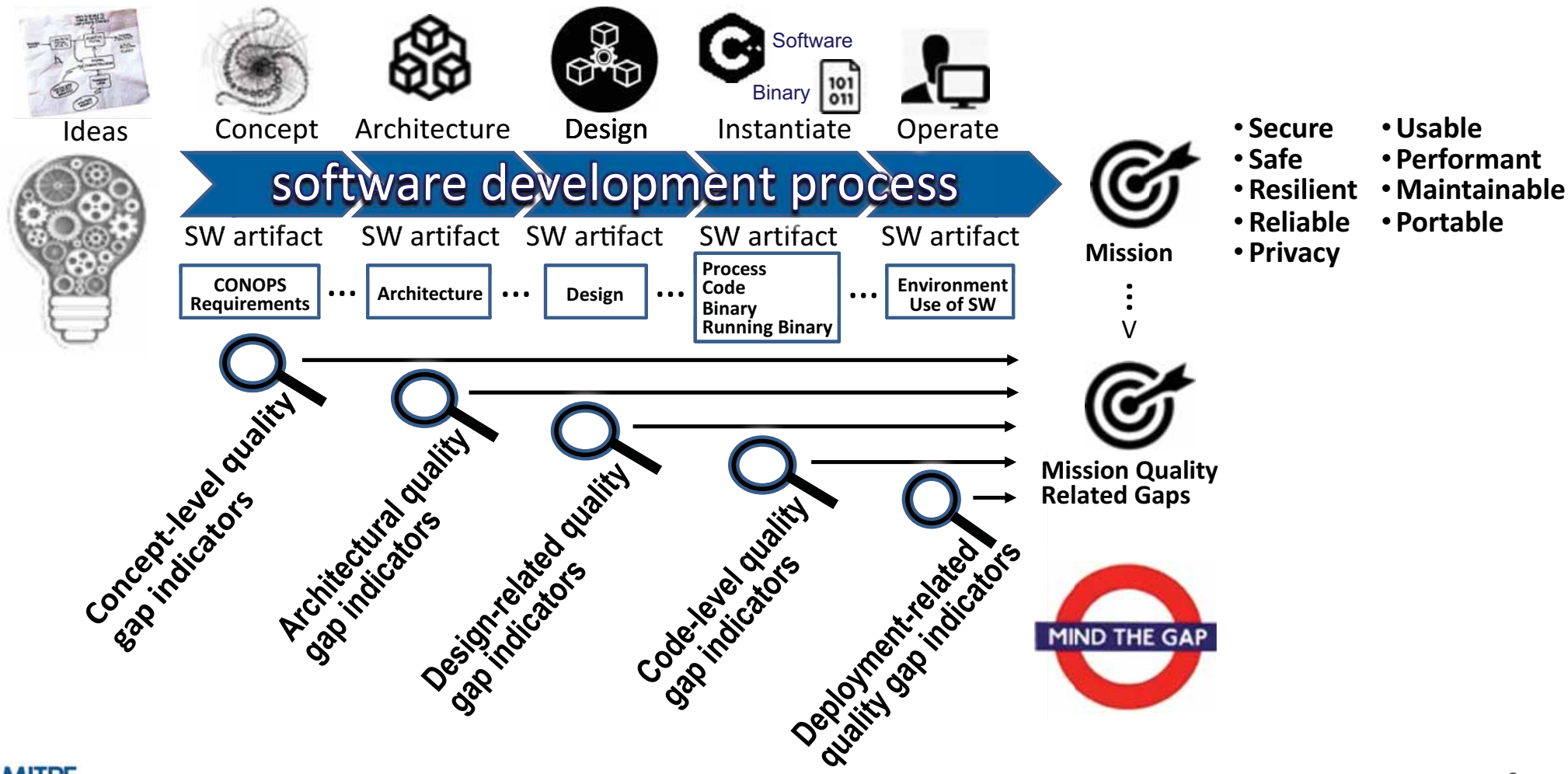
Software is a Building Material – the kind, techniques, composition, & impurities impact fit for purpose



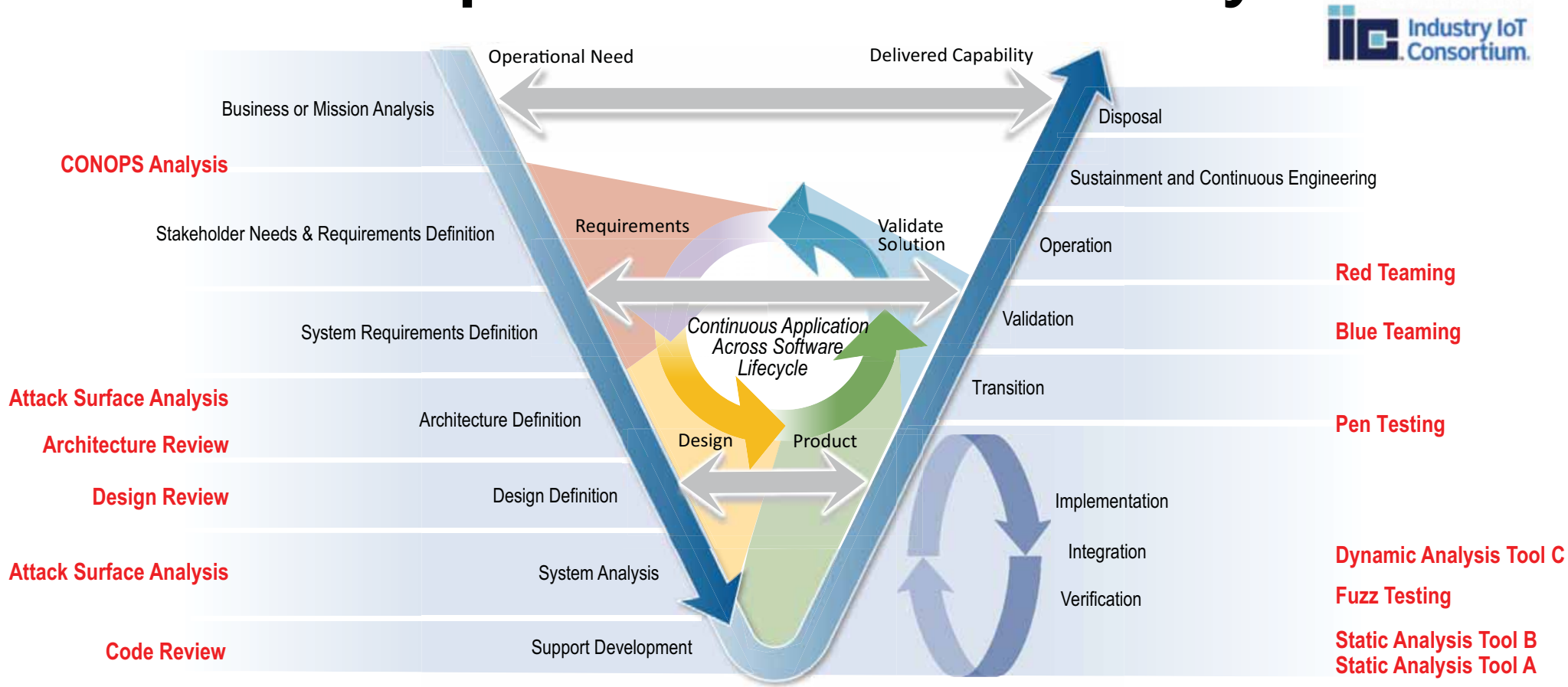
Type	Composition (parts) Cement	Lime	Sand	Compressive Strength (Mpa)
M	4	1	12-15	17.25
S	2	1	8 - 9	12.5
N	1	1	5 - 6	5.1
O	1	2	8 - 9	2.4
K	1	3	10 - 12	0.5
L	0	4	9 - 12	< 0.5



Identifying Quality Issues Through the SW Lifecycle



Software Development and Assurance Lifecycle Phases



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.*

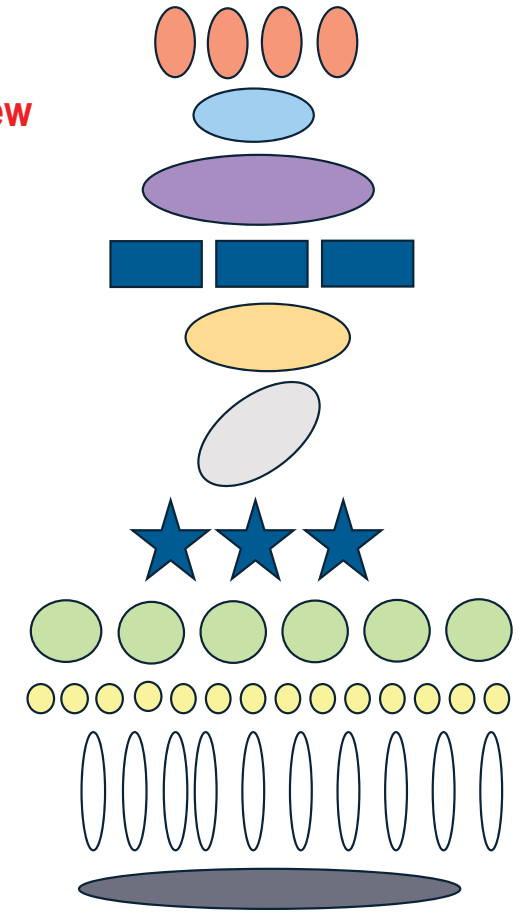
Figure 3-2 from "Software Trustworthiness Best Practices," 2020, https://www.iiconsortium.org/pdf/Software_Trustworthiness_Best_Practices_Whitepaper_2020_03_23.pdf

MITRE

Utilizing Appropriate Detection Methods to Collect Evidence to Gain Assurance…

Artifacts	Detection Methods
CONOPS	CONOPS Evaluation
Requirements	Architecture/Design Review
Architecture	Code Review
Design	Attack Surface Analysis
Process	Static Analysis Tool A
Code	Static Analysis Tool B
Binary	Dynamic Analysis Tool C
Running Binary	Fuzz Testing
Environment of System	Pen Testing
Use of Mission Software	Blue Teaming
	Red Teaming

Coverage



CVE,
CWE,
CAPEC, …

Most Important Quality Issues

MITRE

What Is ISO/IEC 5055:2021


INTERNATIONAL STANDARD

ISO/IEC 5055

First edition 2021-03

Information technology — Software measurement — Software quality measurement — Automated source code quality measures

ISO IEC

Reference number ISO/IEC 5055:2021(E)

© ISO/IEC 2021

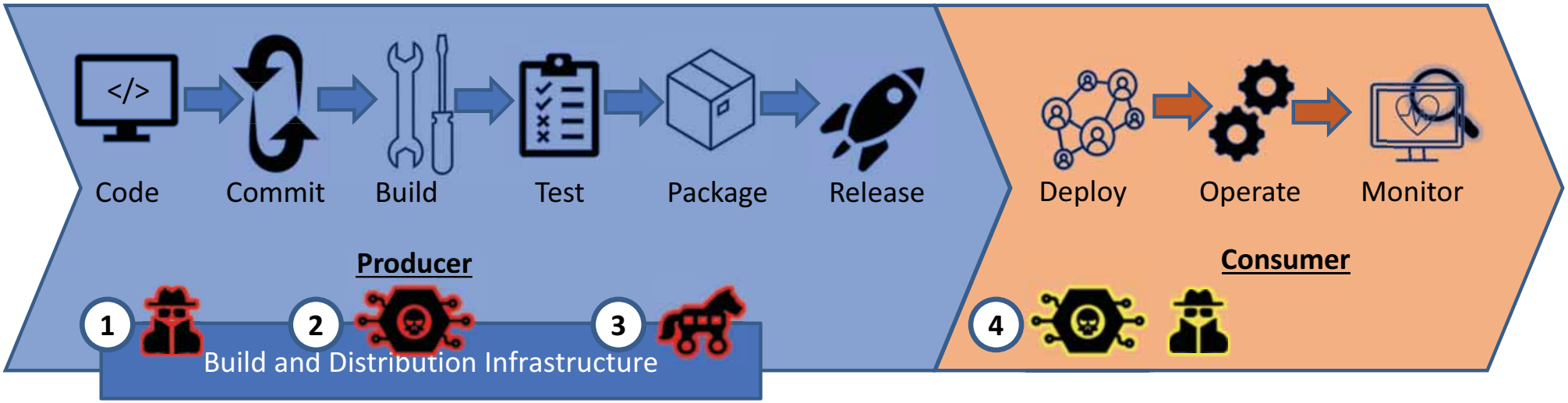
Material curtesy of Bill Curtiss and CISQ.

- **Defines measures of the internal, structural quality of software for four ISO/IEC 25010 software quality characteristics:**
  - **Reliability**
  - **Security**
  - **Performance Efficiency**
  - **Maintainability**
- **Measures are calculated from automated detection and counting of severe architectural and coding weaknesses (CWEs)**
- **'Shift-left' structural quality measurement**
- **Can be used for:**
  - **Internal product and process improvement**
  - **System acquisition contracts and acceptance criteria**
  - **Internal and external monitoring and benchmarking**
- **Fasttracked to ISO as a Publicly Available Standard by OMG (Object Management Group) and can be obtained for free at:** https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Software Supply Chain Integrity Attack (a.k.a SolarWinds)

Jan 2021

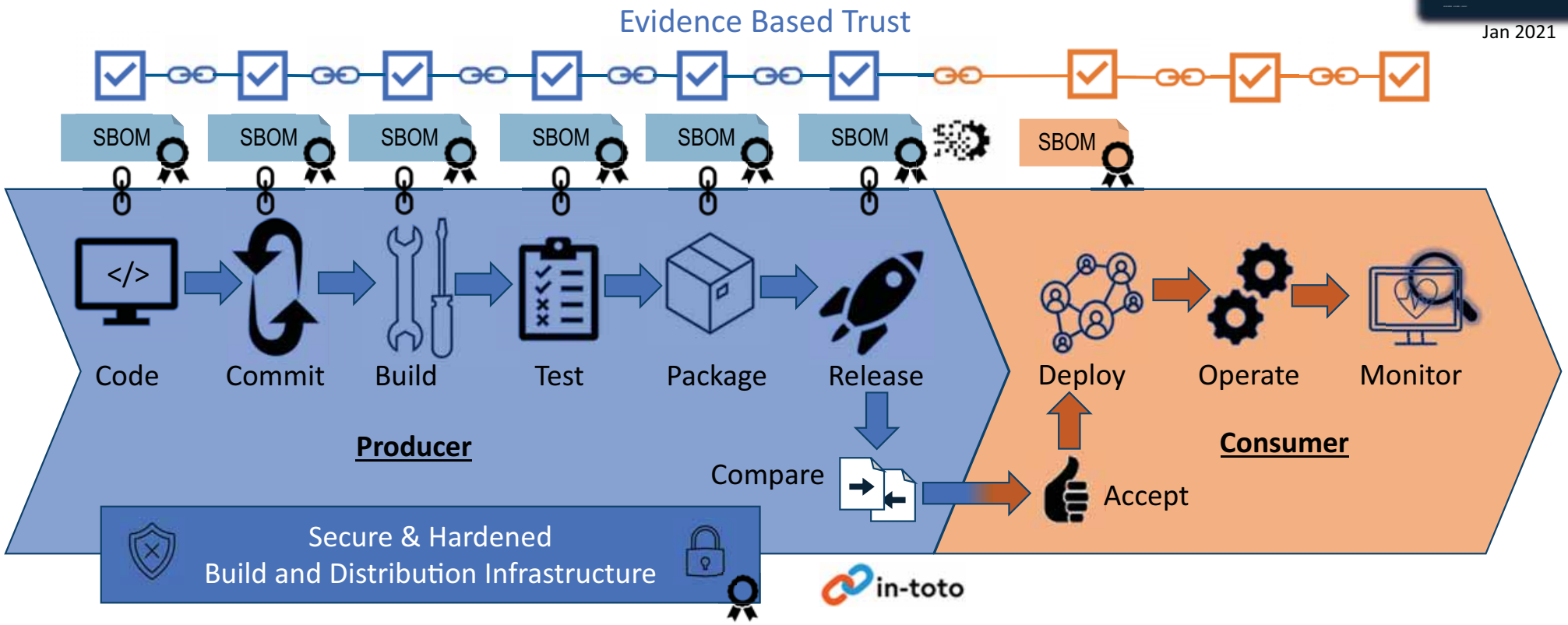
1. Preparatory compromises at SolarWinds date back to October 2019. (Refs 11 & 12)
2. At some point there was a compromise of the build environment itself.
3. Malicious code sent in SolarWinds updates released between March and at least June 2020. (Refs 32 & 33)
4. Approximately 18,000 organizations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



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

Software Supply Chain Integrity

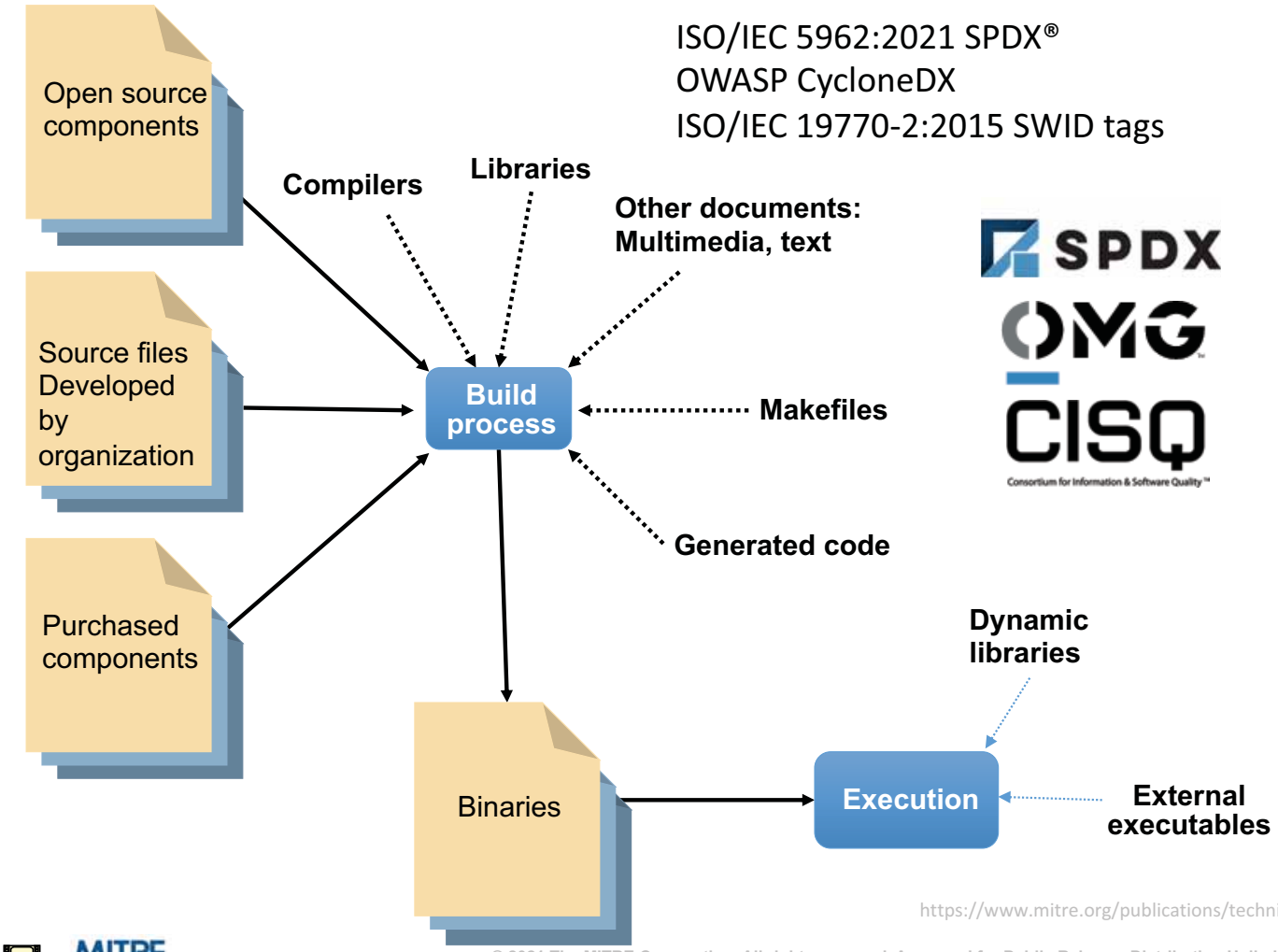
Jan 2021



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

Software Bill of Materials Standardization

ISO/IEC 5962:2021 SPDX®
OWASP CycloneDX
ISO/IEC 19770-2:2015 SWID tags

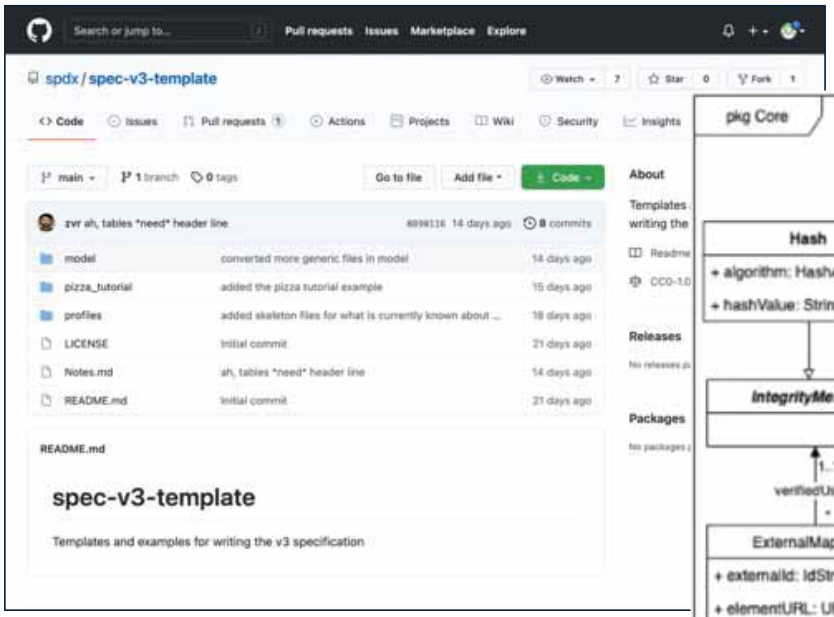


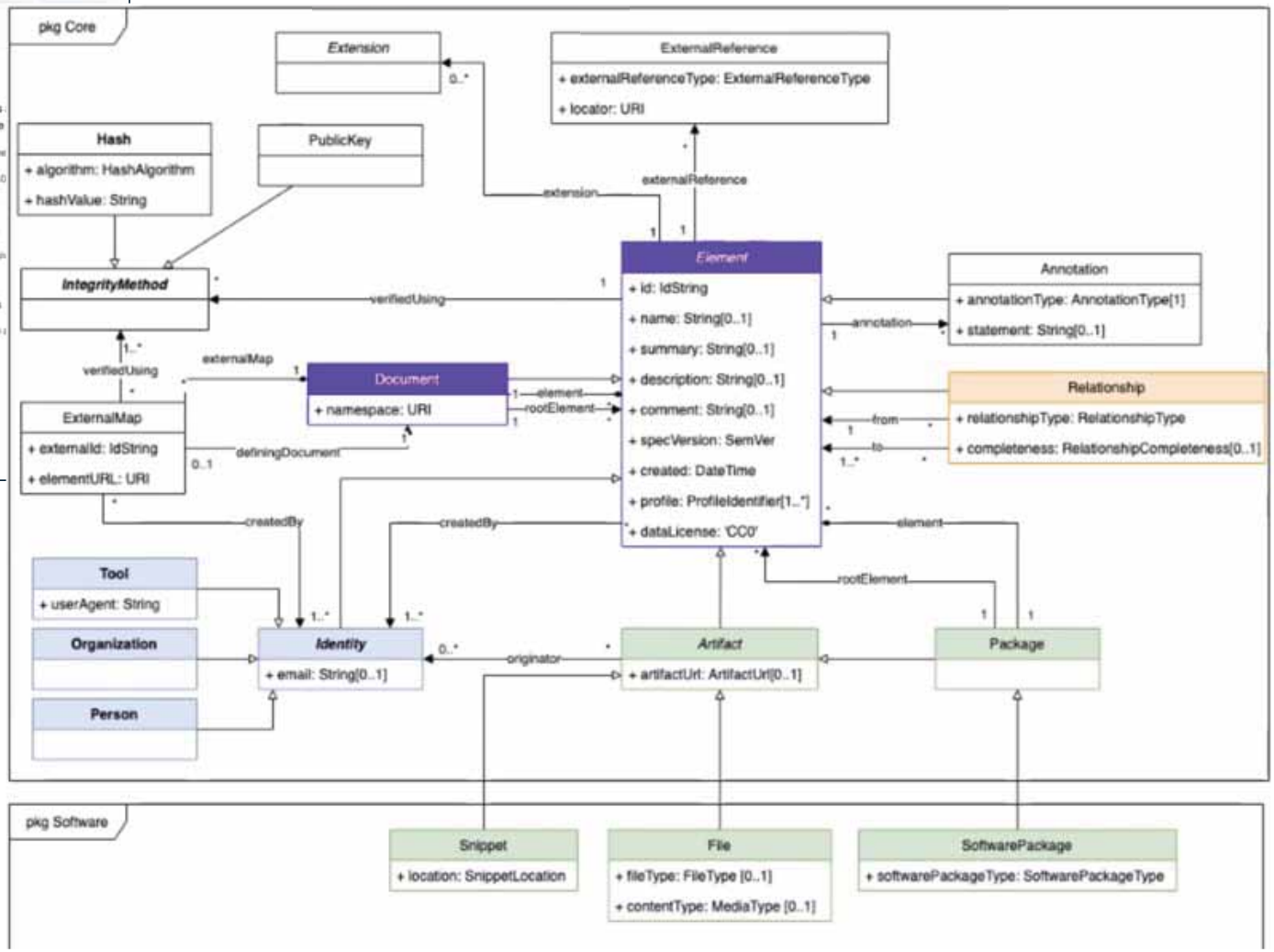
Usage Scenarios Around SBOMs

- Refer, Transfer or Purchase (definition of what it is)
- Pedigree (history of how it was produced)
- Provenance (chain of custody of it)
- Integrity (cryptographic basis of unalteredness)
- Proper and Legal (conditions about its use)
- Known Sw Vulns (known fixes are applied to it)
- Assurance (safe-secure-resilient)
- SBoM of a SW Service (SBoM of sw delivering service)
- Supply Chain Sequence Integrity

https://www.mitre.org/publications/technical-papers/standardizing-sbom-within-the-sw-development-tooling-ecosystem

SPDX 3.0 effort

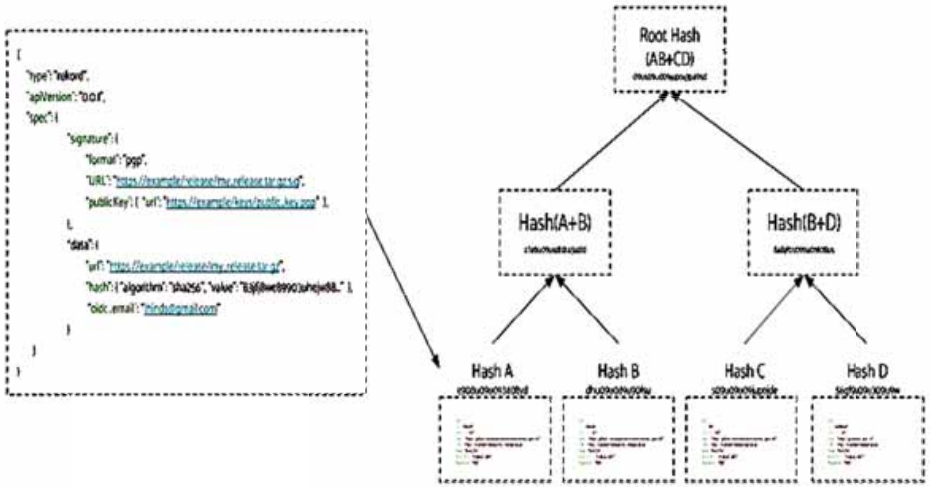




MITRE

A non-profit service to improve the open source software supply chain by easing the adoption of cryptographic software signing, backed by transparency log technologies

https://sigstore.dev/what_is_sigstore/



sigstore manifests entry into the transparency log

fulcio – free Root-CA for code signing certs

- issues certificates based on an OIDC email address.
- only signs short-lived certificates valid for under 20 minutes.

rekor – the binary transparency log project under sigstore

- client CLI (for adding an entry to a rekor transparency log)
- pluggable PKI and support present for: GPG, X.509, Minisign

cosign – Container Signing, Verification and Storage in an OCI registry.

- aims to make signatures **invisible infrastructure**.
- supports: Hardware and KMS signing, Bring-your-own PKI, OIDC PKI (Fulcio), Built-in binary transparency and timestamping service (Rekor)
- Tested/demonstrated with the following registries:
  1. AWS Elastic Container Registry
  2. GCP's Artifact Registry and Container Registry
  3. Docker Hub
  4. Azure Container Registry
  5. JFrog Artifactory Container Registry
  6. The CNCF distribution/distribution Registry
  7. Gitlab Container Registry
  8. GitHub Container Registry
  9. The CNCF Harbor Registry
  10. Digital Ocean Container Registry
  11. Sonatype Nexus Container Registry

MITRE

OCI Registry As Storage (ORAS)

https://github.com/oras-project

Tools and libraries to enable leveraging OCI registries for arbitrary artifacts

Open Container Initiative

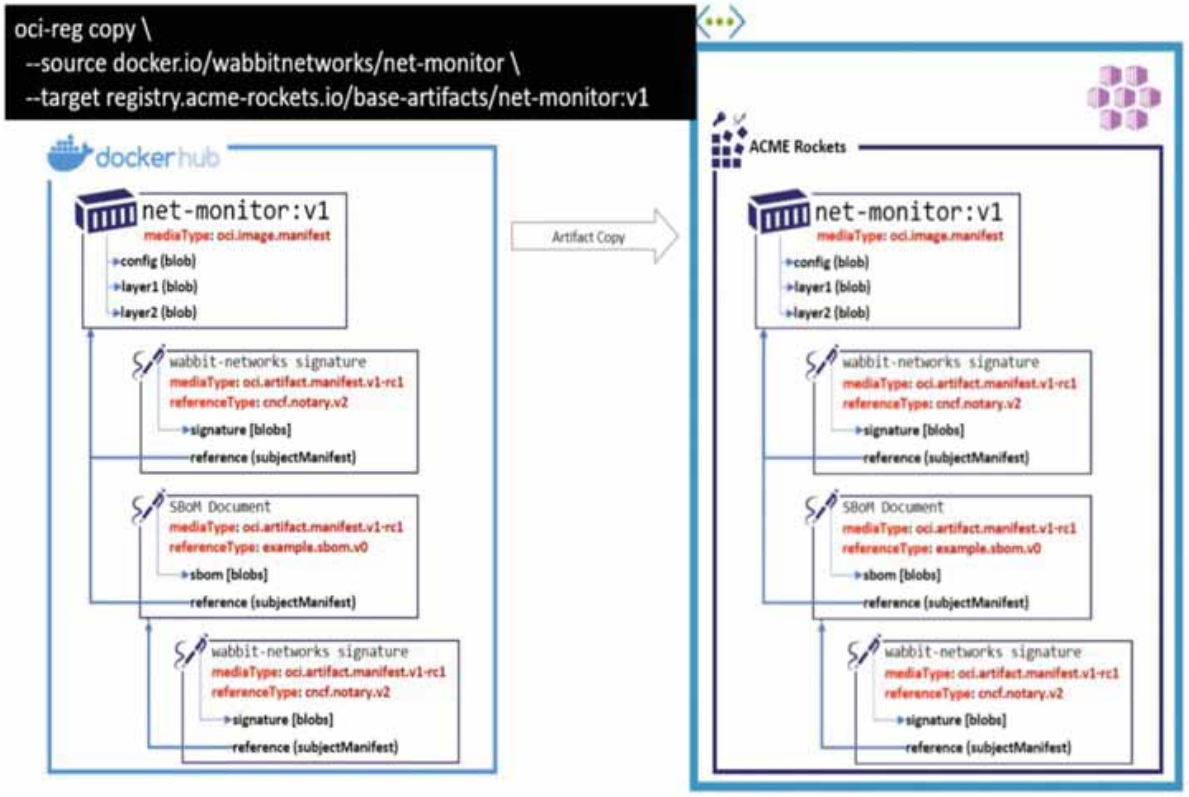
https://github.com/opencontainers/

Creating open standards around container technology

OCI artifact manifest, Phase 1-Reference Types #29

The OCI artifact manifest generalizes the use of OCI image manifest, by reducing the constraints on all artifacts, enabling specific artifact-specs to set constraints for their type. Phase 1 adds support for artifacts to reference other artifacts through a subjectManifest property enabling reference graphs, as those required for secure supply chain efforts.

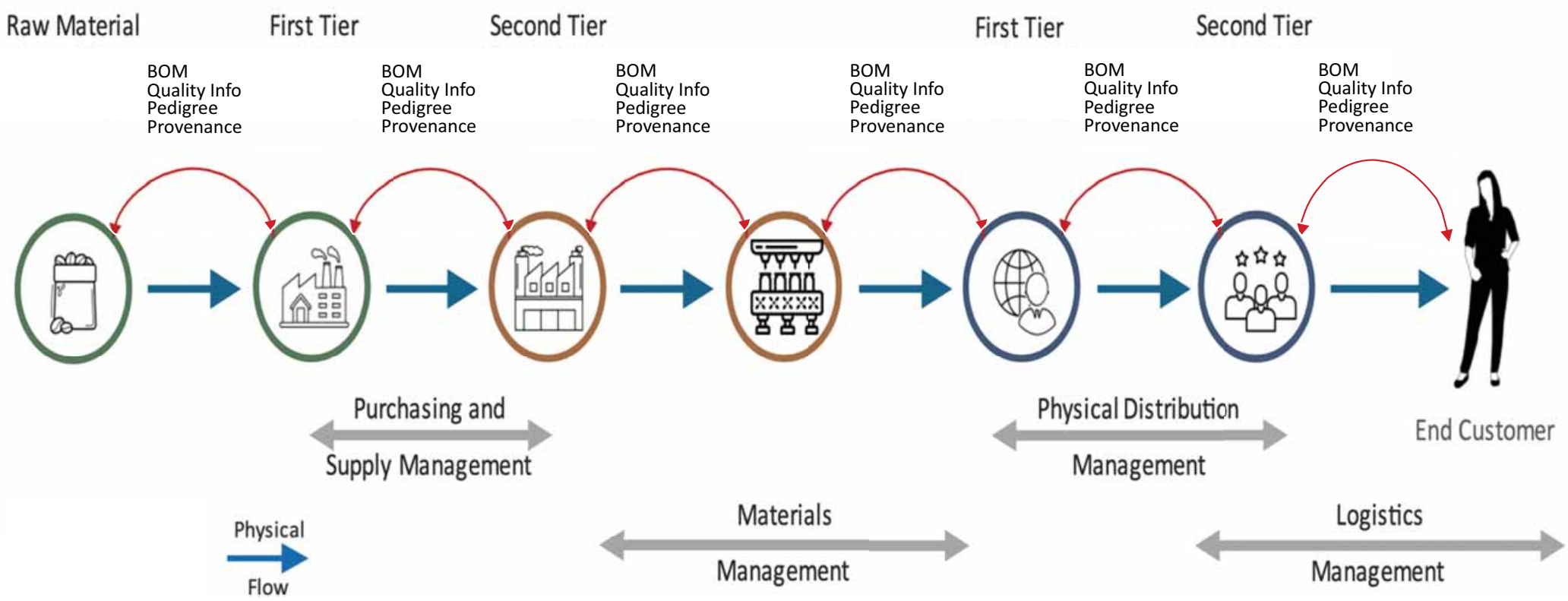
Phase 1: Reference Types
The PR focuses on Phase 1, enabling reference type support in 2021, supporting secure supply chain artifact types including signatures and SBoMs.



- OCI Artifacts Reference Types: github.com/opencontainers/artifacts/pull/29
- ORAS Reference Types: github.com/deislabs/oras/blob/reference-types/docs/artifact-manifest.md
- CNCF Distribution Reference Types: github.com/notaryproject/distribution/blob/prototype-2/docs/reference-types.md
- Notary v2: github.com/notaryproject/notaryproject

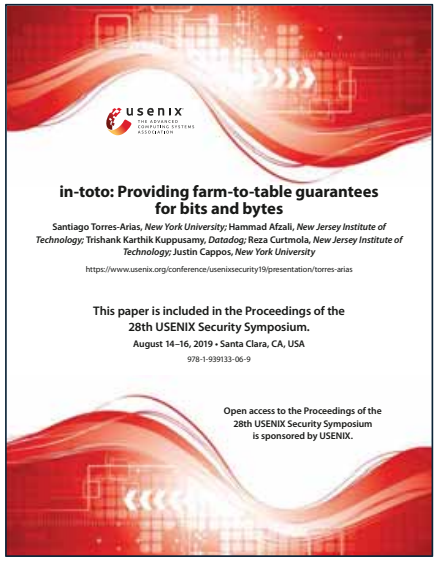
MITRE

Supply Chain Network Stakeholders



https://www.iiconsortium.org/pdf/Trustworthiness_Framework_Foundations.pdf

MITRE



Oct 2016+

in-toto

https://www.nist.gov/document/responses-enhancing-software-supply-chain-security-toto-team

THE LINUX FOUNDATION

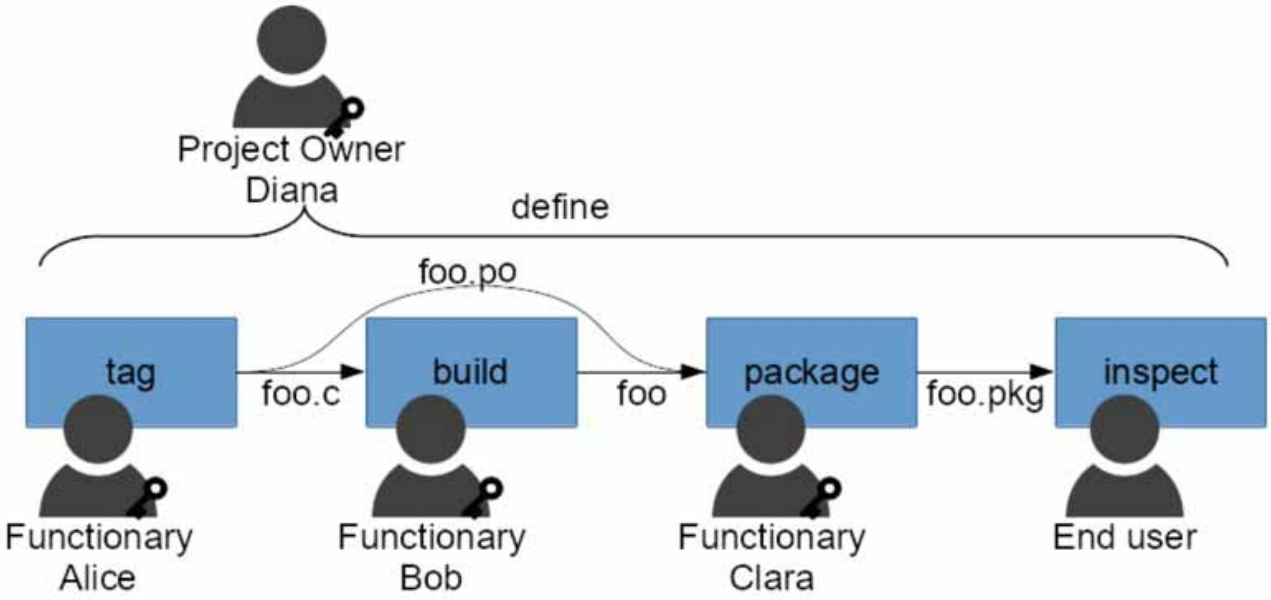
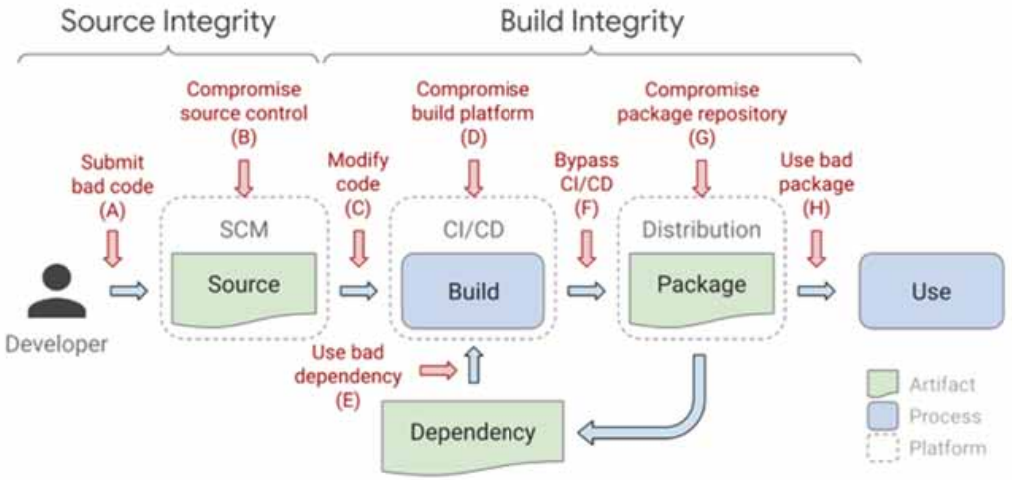


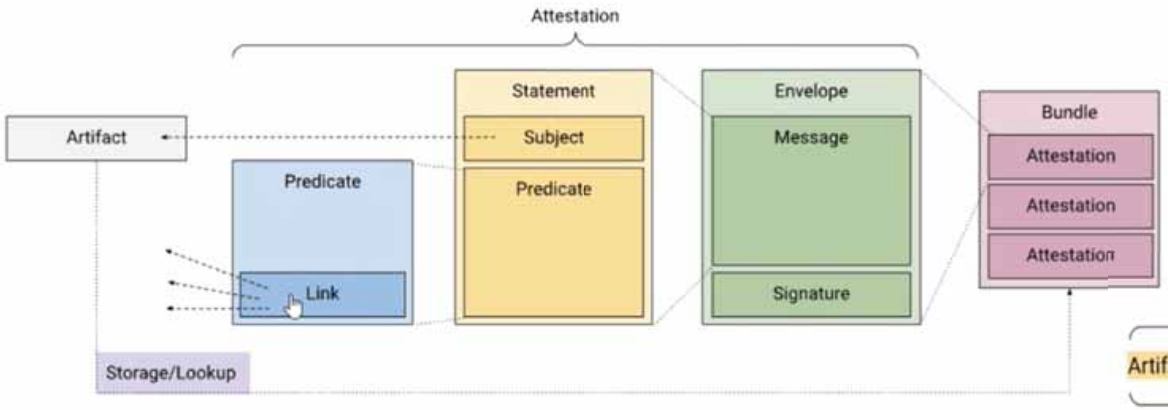
Figure 1: Graphical depiction of the software supply chain with `in-toto` elements added. The project owner creates a layout with three steps, each of which will be performed by a functionary. Notice how the tag step creates `foo.c` and a localization file `foo.po`, which are fed to different steps down the chain.

https://www.usenix.org/system/files/sec19-torres-arias.pdf

MITRE

Supply-chain Levels for Software Artifacts (SLSA)



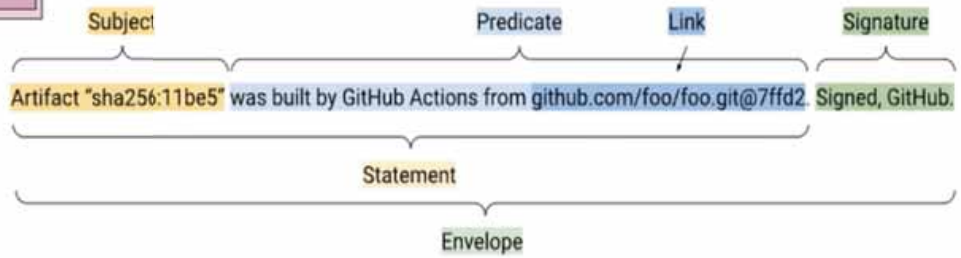


SLSA guidelines have 4 levels of incremental and actionable things that software producers can claim to do to protect against specific integrity attacks

https://github.com/slsa-framework/slsa

Requirement	SLSA 1	SLSA 2	SLSA 3	SLSA 4
Source - Version Controlled		✓	✓	✓
Source - Verified History			✓	✓
Source - Retained Indefinitely			18 mo.	✓
Source - Two-Person Reviewed				✓
Build - Scripted Build	✓	✓	✓	✓
Build - Build Service		✓	✓	✓
Build - Ephemeral Environment			✓	✓
Build - Isolated			✓	✓
Build - Parameterless				✓
Build - Hermetic				✓
Build - Reproducible				O
Provenance - Available	✓	✓	✓	✓
Provenance - Authenticated		✓	✓	✓
Provenance - Service Generated		✓	✓	✓
Provenance - Non-Falsifiable			✓	✓
Provenance - Dependencies Complete				✓
Common - Security				✓
Common - Access				✓
Common - Superusers				✓

O = required unless there is a justification



Supply Chain Integrity Model (SCIM)

Technologies leveraged:

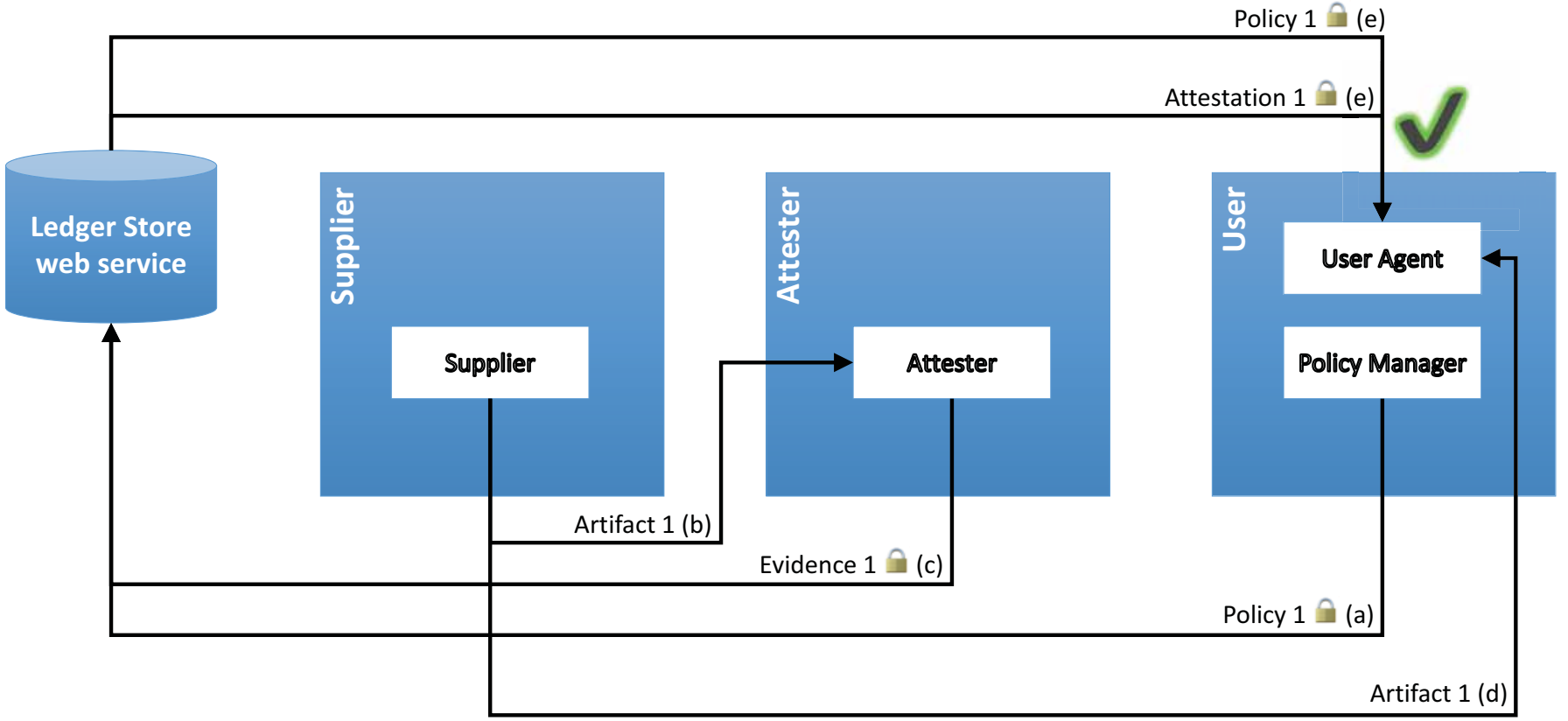
- **Attestations/Evidence, Confidential Ledgers, Hardware Roots of Trust, BOMs for SW and HW, CBOR (RFC 8949) and COSE (RFC 8152)**

SCIM:

- **defines minimum standards around the:**
  - **preparation, storage, distribution, consumption, validation and evaluation of arbitrary attestations/evidence about artifacts that are critical to maintaining the integrity of supply chains**
- **specifies an end-to-end system for validating arbitrary artifacts in terms of supply chains whose integrity has been proven.**
- **is applicable to both hardware (objects in the physical world) and software (digital) artifacts.**
- **does not define how artifacts are produced or distributed, nor the methods by which attestations/evidence about artifacts are produced prior to preparation for inclusion in SCIM.**

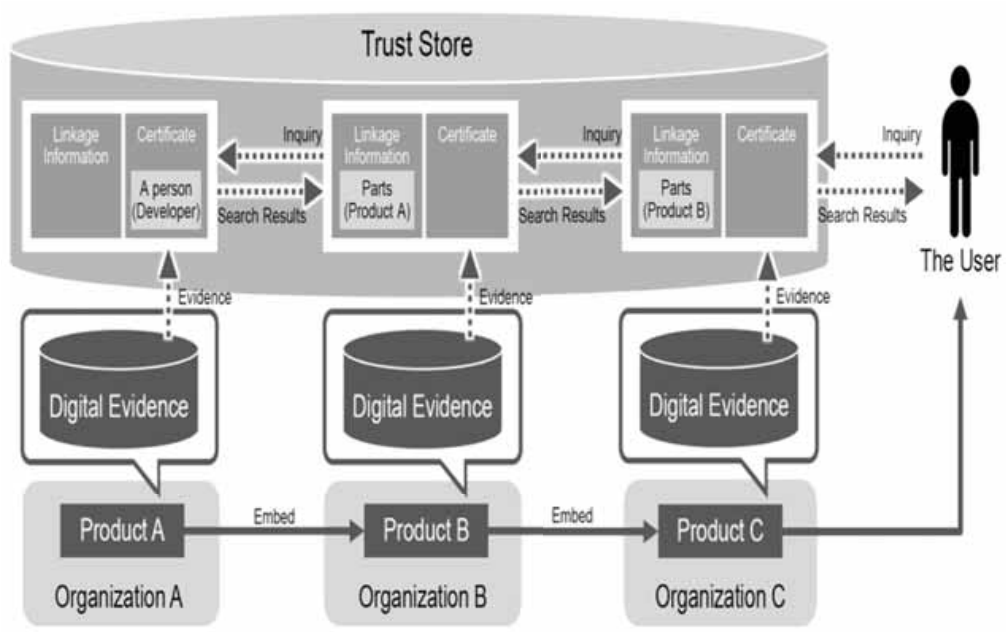
https://www.nist.gov/system/files/documents/noindex/2021/06/08/Microsoft - Executive Order - NIST workshop position paper 5- Software integrity chains Microsoft Corporation.pdf

SCIM Usage Scenario



https://www.nist.gov/system/files/documents/noindex/2021/06/08/Microsoft - Executive Order - NIST workshop position paper 5- Software integrity chains Microsoft Corporation.pdf

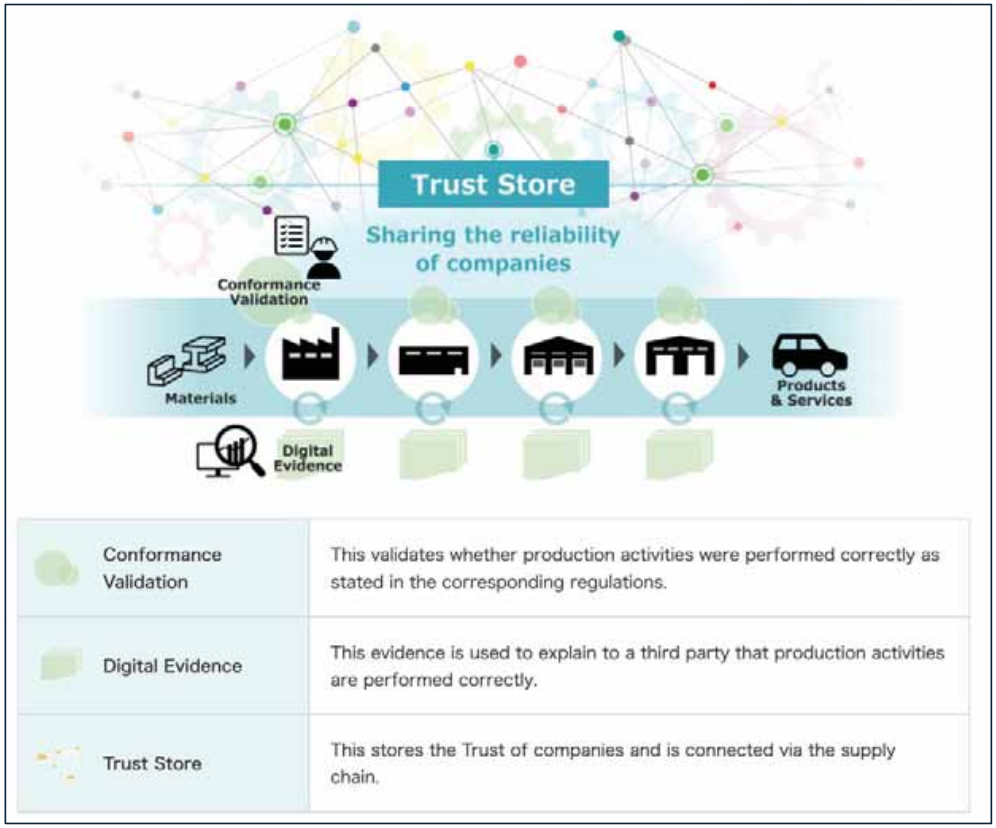
Trust Systems for a Supply Chain



https://www.iiconsortium.org/pdf/Trustworthiness_Framework_Foundations.pdf

Industry IoT Consortium

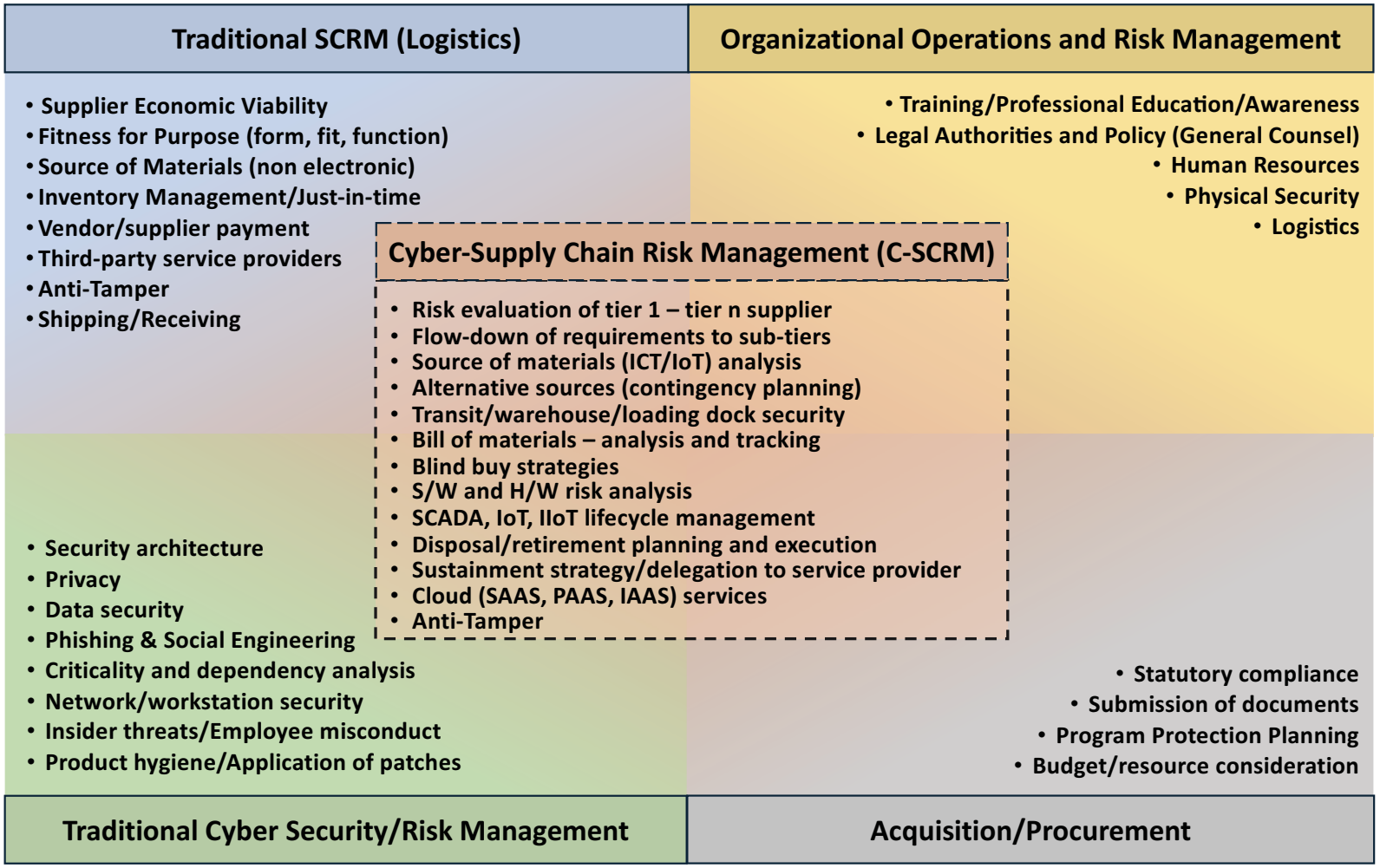
HITACHI



https://www.hitachi.co.jp/products/it/security/activities/digitaltrust/english/index.html

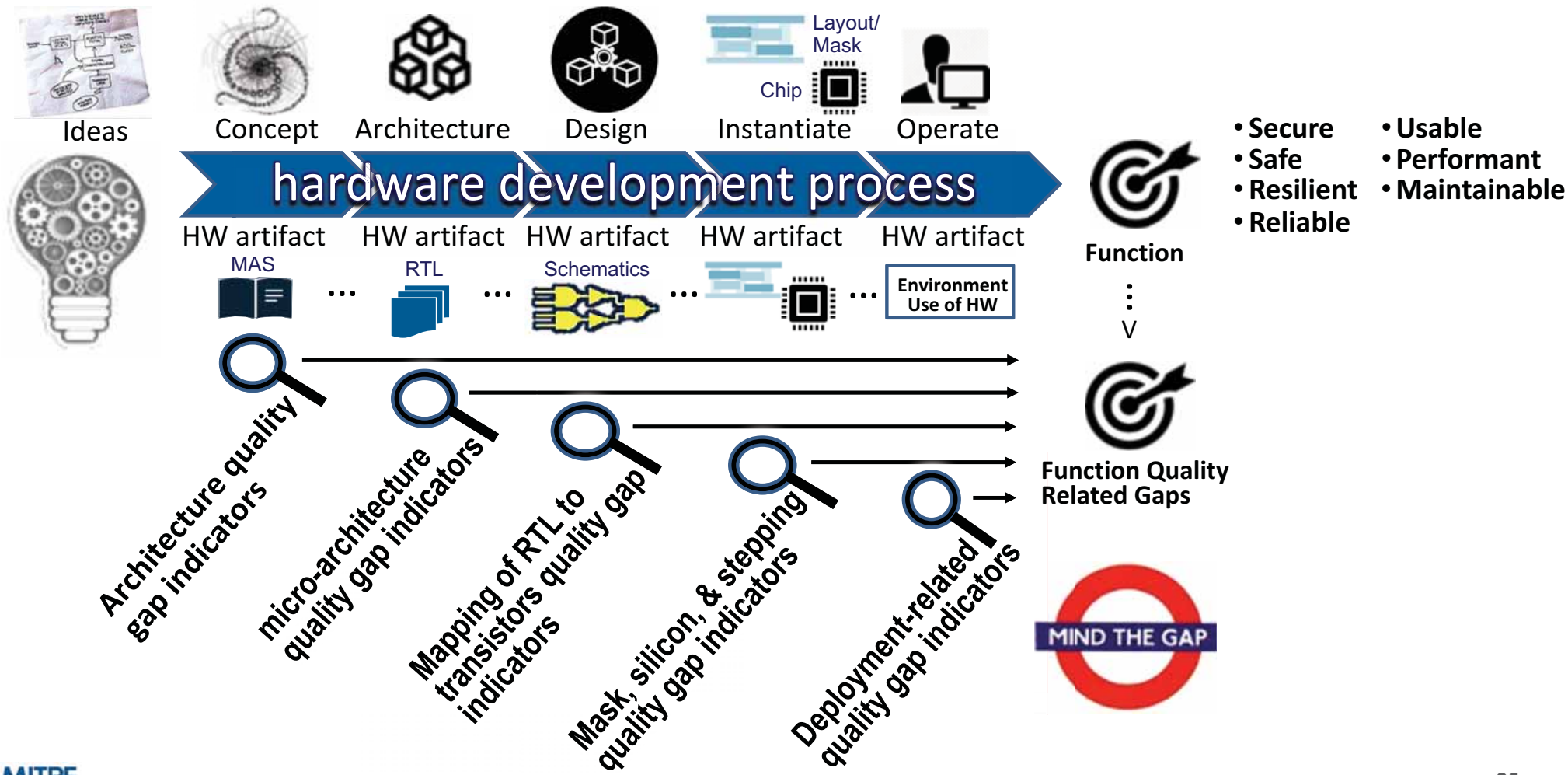
MITRE

Supply Chain Security Risk Management: Elements of Practice

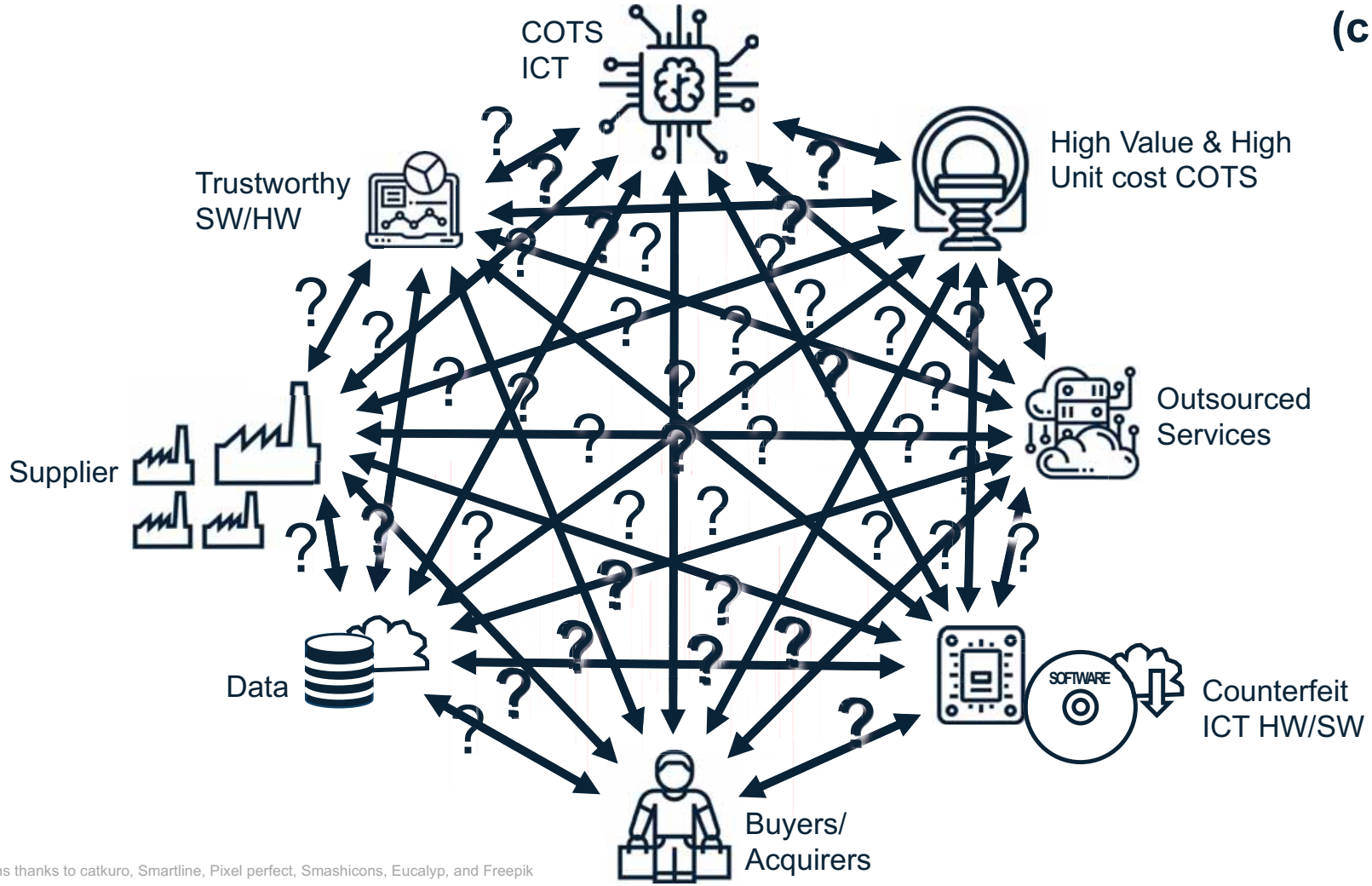


MITRE

Identifying Quality Issues Through the HW Lifecycle



Difficult Interactions for Supply Chain Participants Regarding Trust (circa 2020)



Icons thanks to catkuro, Smartline, Pixel perfect, Smashicons, Eucalyp, and Freepik

Standardized Supply Chain Trustworthiness Risks

Supply Chain Risks													
Supplier Risks							Supply Risks			Services Risks			
External Influences	Financial Stability	Organizational Stature	Susceptibility	Quality Culture	Maliciousness	Organizational Security	Hygiene	Malicious Taint	Counterfeit	Integrity of Service Delivered	Quality of Service Delivered	Reliability of Service Delivered	Security of Service Delivered
Company foreign relationships with countries of concern	Questionable debt management	Corporate ownership reputation	Customers	Company has a low CMMI rating	Foreign Intelligence Service (FIS) influence	Concerns regarding facility access	Product quality	Facilities integrity	Copycat manufacturing	Service infrastructure pedigree	Service infrastructure pedigree	Service infrastructure pedigree	Service infrastructure pedigree
Company operational locations in countries of concern	Questionable financial stewardship	Diversity and inclusion	Industry sector	Internal company QC, SCRM policy & practice	Fraud and corruption	Concerns regarding software access	Product resilience	Functional integrity	Mislabeling	Service Infrastructure provenance	Service infrastructure provenance	Service infrastructure provenance	Service infrastructure provenance
Foreign registration/incorporation	Questionable future outlook	Geographic concentration	Location	Subcontractor supply chain health / risk	Legal/law issues	Concerns regarding hardware access	Product security	Geopolitical integrity	Packaging integrity	Service specific integrity	Service specific quality	Service specific reliability	Service specific security
Geopolitical instability	Questionable profitability	Mergers & acquisitions frequency	Personnel		Sanction list status	Cyber threat activity		Logistics / transportation integrity	Technical authenticity				Susceptibility to manipulation of service infrastructure via physical access/touch
Key Management Personnel (KMP) and non-person entity relationships of concern	Vulnerability of financial stability to foreign influence	Natural disasters	Technical susceptibility			Data security status		Maintenance integrity	Unsanctioned manufacturing				Susceptibility to manipulation of service infrastructure via remote/virtual access/touch
National corruption	Vulnerability of financial stability to market factors	Operational volatility				Type/ level /frequency of security training		Manufacturing process integrity					
National governance	Vulnerability to takeover	Sustainability				Vulnerabilities		Packaging integrity					
Organization ownership and control								Reputational integrity					
Politically Exposed Persons (PEPs) in corporate leadership								Supply chain integrity					
Political vulnerability													
Transparency of organization control													

MITRE Supply Chain System of Trust™ Risk Areas

https://www.mitre.org/publications/technical-papers/trusting-our-supply-chains-a-comprehensive-data-driven-approach

MITRE

Questions?