



IAITAM ACE

May 7-9, 2024 The M Resort  Las Vegas, NV

What's in the Box?

The Importance of Software Bill of Materials

Allan Friedman, PhD

US Cybersecurity & Infrastructure Security Agency

Finding your IAITAM Oasis



What's in the Box?

The Importance of Software Bill of Materials



Allan Friedman, PhD
US Cybersecurity and
Infrastructure Security Agency

Foundational Question

Can you say that you are doing ITAM or SAM if you don't actually know what is in your software?





Key takeaways

Understanding what's in our software and how it was made is a critical part of the software process. This is called a Software Bill of Materials (SBOM).

Why would anyone buy, use, or manage software without knowing what's in it or knowing how it's made?

Transparency in all software is coming—and it can help you for your roles in managing assets and risk.



Paying attention or getting a proper coffee

- Why are ingredients important?
- Software risks – security, but so much more!
- What is an SBOM?
- Why is SBOM and why you should care
- Is someone going to make me do this?
- Summary – the slides to take pictures of



Who's this guy from the gubmint?



May 7–9, 2024 The M Resort  Las Vegas, NV

Who's this guy from the gubmint?



I'm from the
government, and
I'm here to help...



May 7-9, 2024 The M Resort  Las Vegas, NV

Who's this guy from the gubmint?

- The Cybersecurity and Infrastructure Security Agency is the national coordinator for critical infrastructure security and resilience
 - Defend today
 - Collaborate to build a more secure infrastructure for tomorrow
- Mission: We lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.
- A secure and resilient critical infrastructure for the American people.



*Finding your
ITAM Oasis*

May 7-9, 2024 The M Resort  Las Vegas, NV

An analogy



An analogy - Benefits



Transparency in food is a critical part of health, lifestyle, and management of our daily life



An analogy - Limits



This will not *by itself*

- Prevent allergens
- Keep you on a diet
- Enforce dietary rules

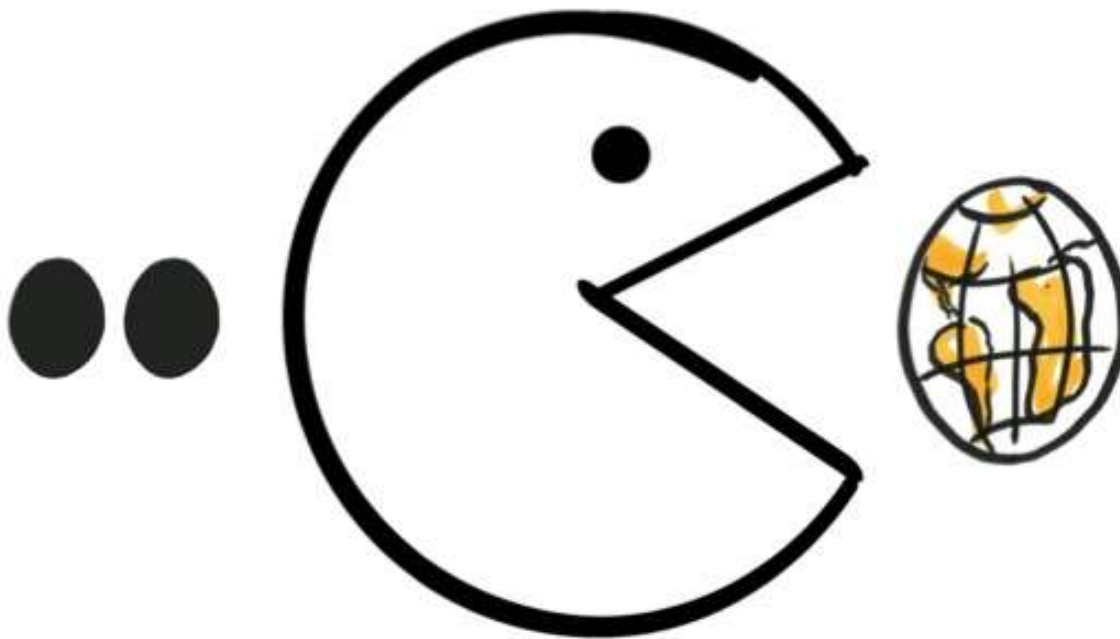
(and you need to know what words mean)



Supply Chains



Software is eating up the world*



* Marc Andreessen
in Wall Street Journal

5

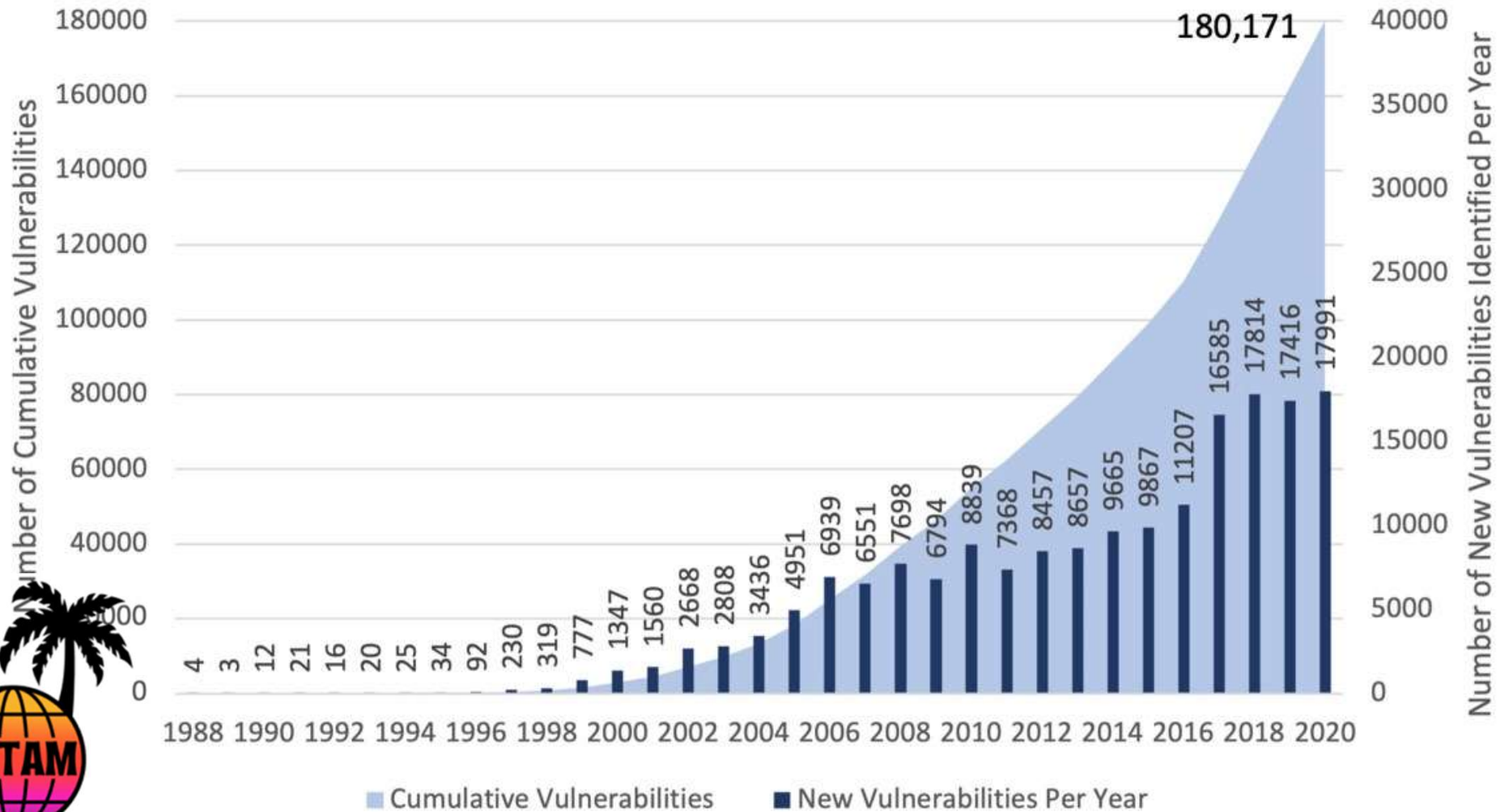




Vulnerabilities

“Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.”

New Vulnerabilities Identified Each Year, 1988-2020





Allan...
This isn't a cybersecurity
conference!



*Finding your
ITAM Oasis*

May 7-9, 2024 The M Resort  Las Vegas, NV

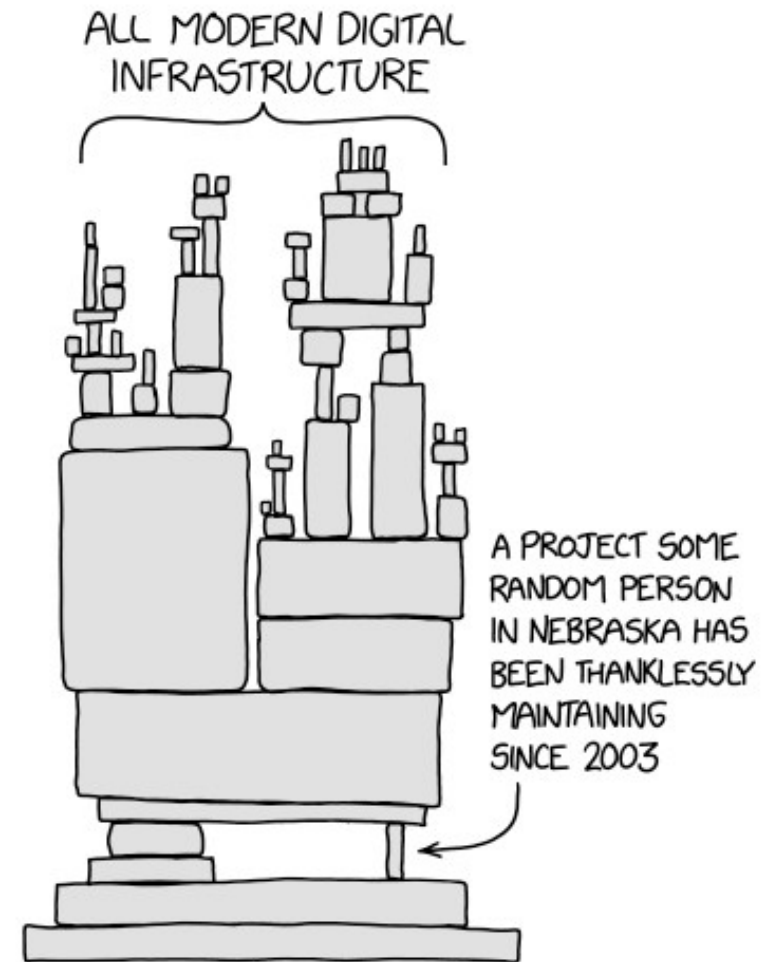


Open Source Software



OSS dependencies

- Lack of visibility
- Lack of incentives
- Lack of levers



<https://xkcd.com/2347/>

End of Life and End of Support





National Cyber
Security Centre

ABOUT NCSC

CISP

Home

Information for...

Advice & guidance

Education & skills

Products & services

NEWS

Exploitation of vulnerabilities affecting Ivanti Connect Secure and Ivanti Policy Secure



Kevin Beaumont

@GossiTheDog@cyberplace.social

Enjoying this fully patched Ivanti Pulse Connect box (yes, the kernel has dirty in it)

Linux version 2.6.32-00366-gsd3b182-dirty - December 2009

curl 7.19.7 2009-11-04 (14 years)
openssl 1.0.2n-fips 2017-12-07 (6 years)
perl 5.6.1 2001-04-09 (23 years)
psql 9.6.14 2019-06-20 (5 years)
cabextract 0.5 2001-08-20 (22 years)
ssh 5.3p1 2009-10-01 (14 years)
unzip 6.00 2009-04-29 (15 years)

Feb 09, 2024, 13:38 · 37 · 28

May 7-9, 2024



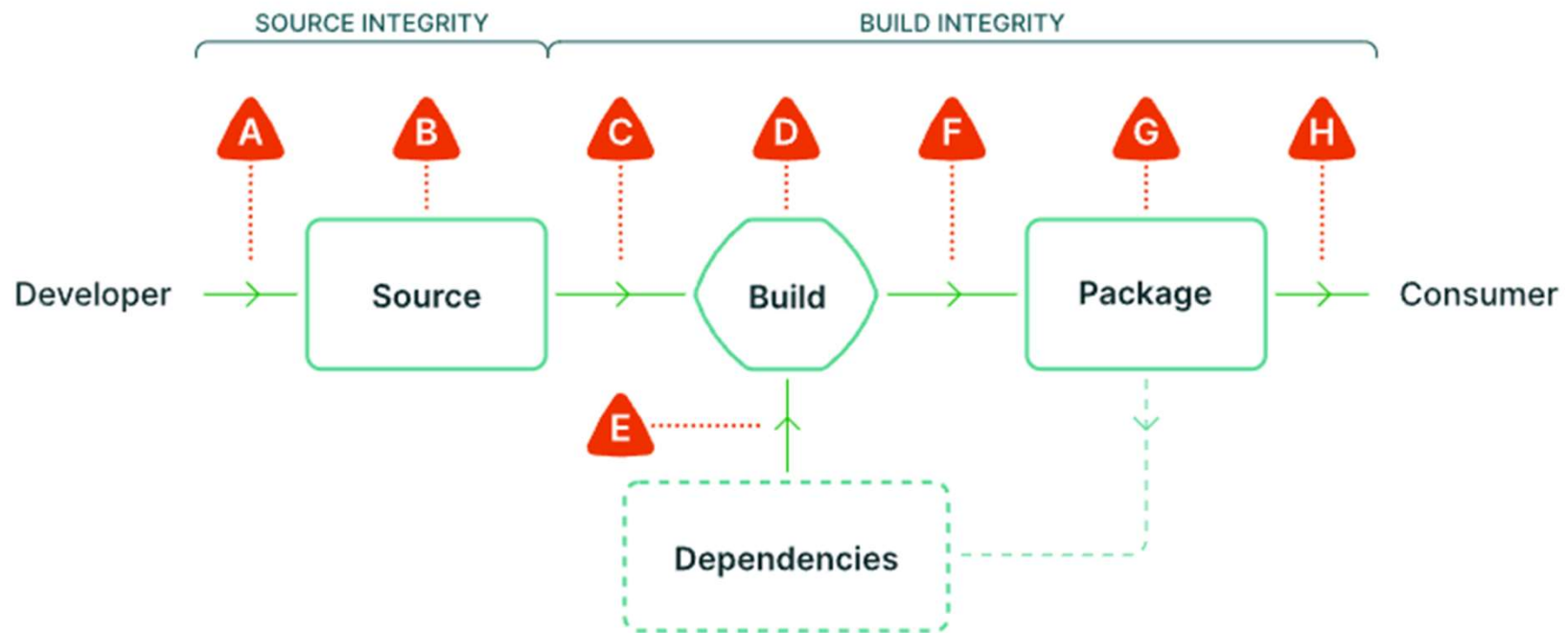
*Finding your
ITAM Oasis*

Can you guarantee that an asset is current?



Patching requirements may be more complex than just single vendors





A Submit unauthorized change
B Compromise source repo

C Build from modified source
D Compromise build process
E Use compromised dependency

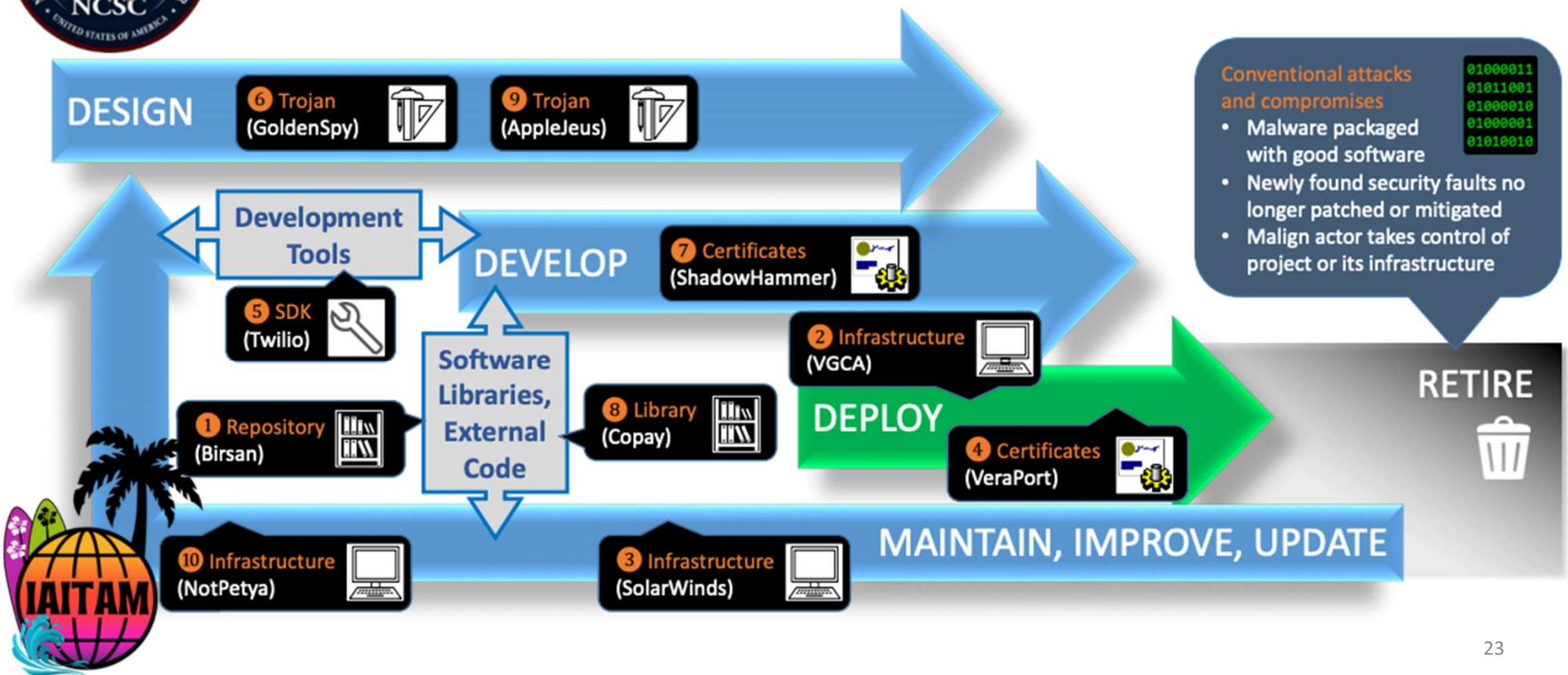
F Upload modified package
G Compromise package repo
H Use compromised package

Source: slsa.dev



Software Supply Chain Attacks

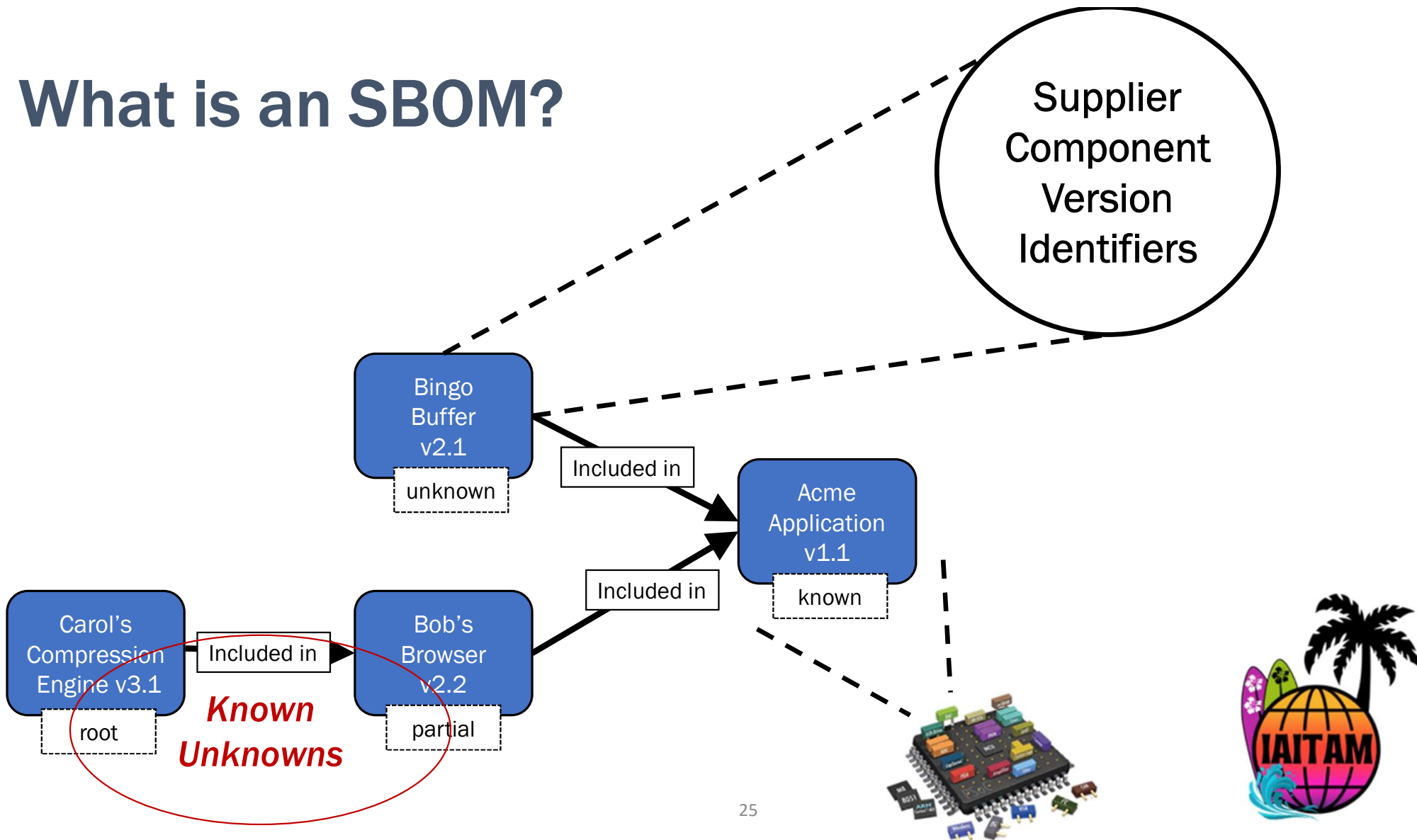
Definition: Compromising software through cyber attacks, insider threats, or other malign activities at any stage throughout its entire lifecycle.



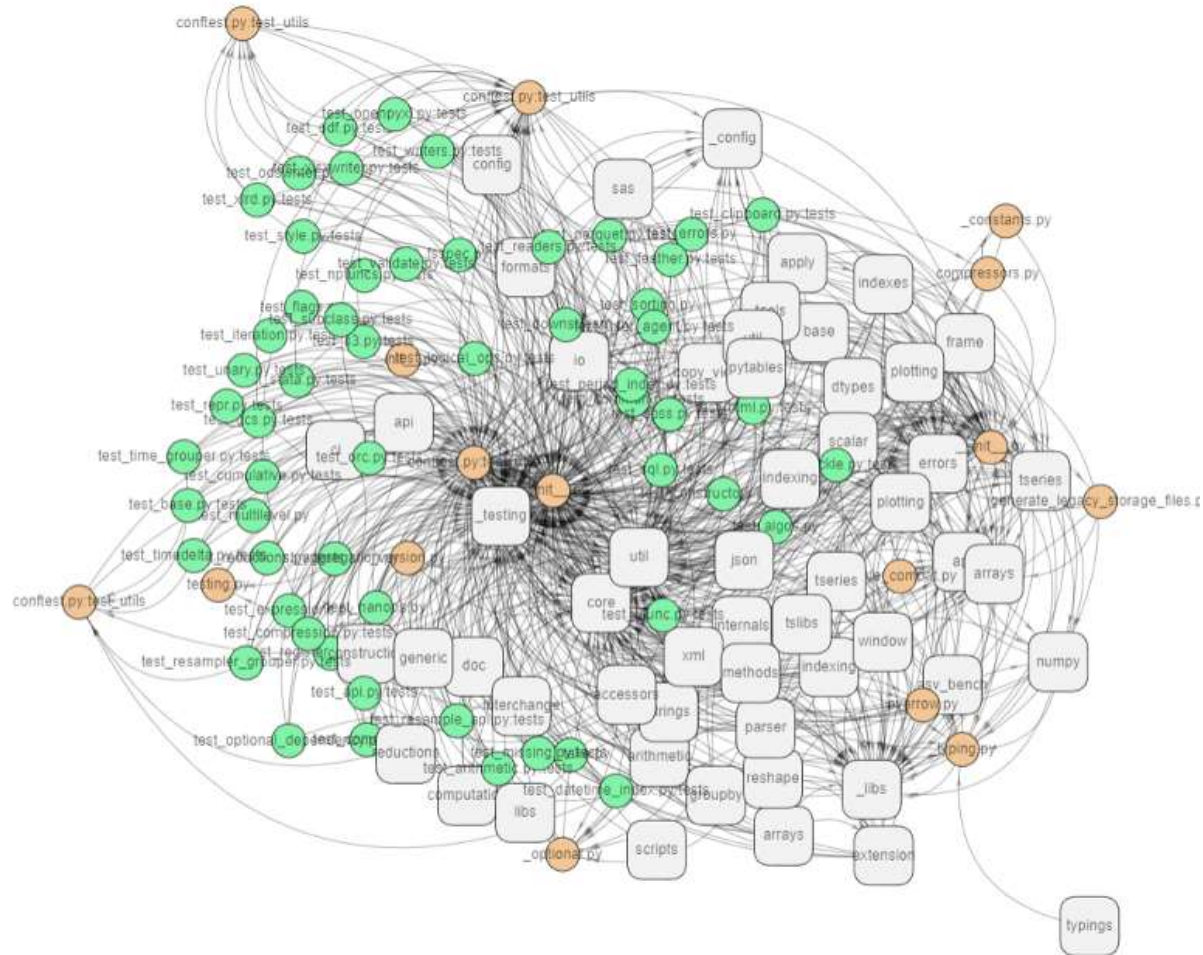
Hidden risks require transparency



What is an SBOM?



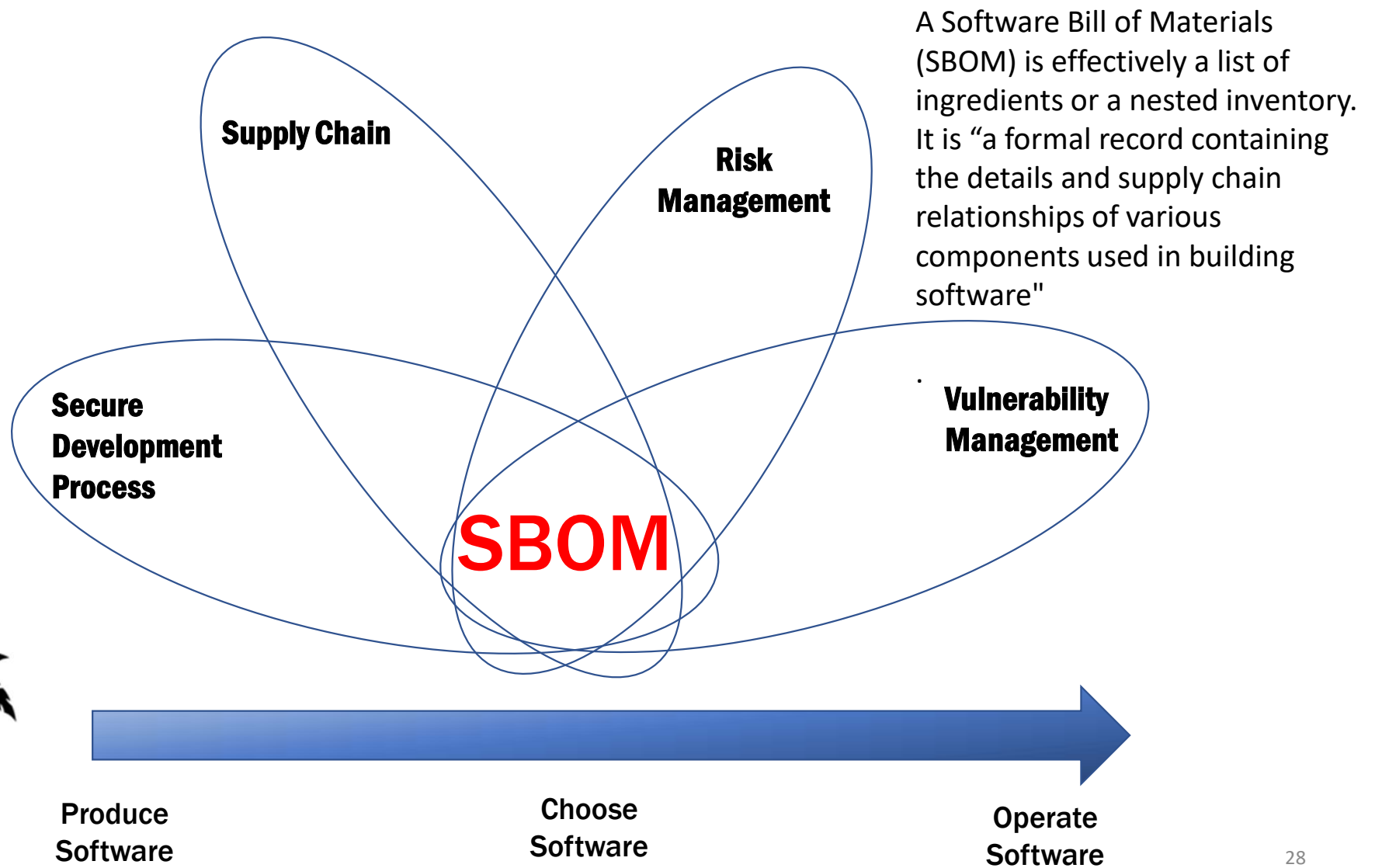
An SBOM is a “directed acyclic graph”



An SBOM is just a pile of JSON

```
3147 "SPDXID": "SPDXRef-npm-readable-stream-2.3.8",
3148 "name": "readable-stream",
3149 "versionInfo": "2.3.8",
3150 "filesAnalyzed": true,
3151 "downloadLocation": "https://registry.npmjs.org/readable-stream/-/readable-stream-2.3.8.tgz",
3152 "originator": "Organization: NPM",
3153 "supplier": "Person: calvin.metcalf@gmail.com,hello@matteocollina.com,build@iojs.org",
3154 "summary": "Node.js Streams, a user-land copy of the stream library from Node.js",
3155 "hasFiles": [
3156   "SPDXRef-npm-readable-stream-2.3.8-lib-stream-readable.js",
3157   "SPDXRef-npm-readable-stream-2.3.8-lib-stream-duplex.js",
3158   "SPDXRef-npm-readable-stream-2.3.8-lib-stream-writable.js",
3159   "SPDXRef-npm-readable-stream-2.3.8-LICENSE",
3160   "SPDXRef-npm-readable-stream-2.3.8-package.json",
3161   "SPDXRef-npm-readable-stream-2.3.8-lib-stream-transform.js",
3162   "SPDXRef-npm-readable-stream-2.3.8-lib-stream-passthrough.js"
3163 ],
3164 "licenseDeclared": "LicenseRef-MIT-24536810",
3165 "copyrightText": "Node.js contributors. All rights reserved.\n\t Joyent, Inc. and other Node contributors.\n\t Node.js contributors. All rights reserved.\n\t Joyent, Inc. and
3166 "homepage": "https://www.npmjs.com/package/readable-stream",
3167 "licenseConcluded": "NOASSERTION",
3168 "checksums": [
3169   {
3170     "algorithm": "MD5",
3171     "checksumValue": "5cf6052be99a6ac1167068508e61b654"
3172   },
3173   {
3174     "algorithm": "SHA1",
3175     "checksumValue": "08fc0ba09af404f2752fa41194635825c23f03fc"
3176   },
3177   {
3178     "algorithm": "SHA256",
```





How do we implement this?



SPDX

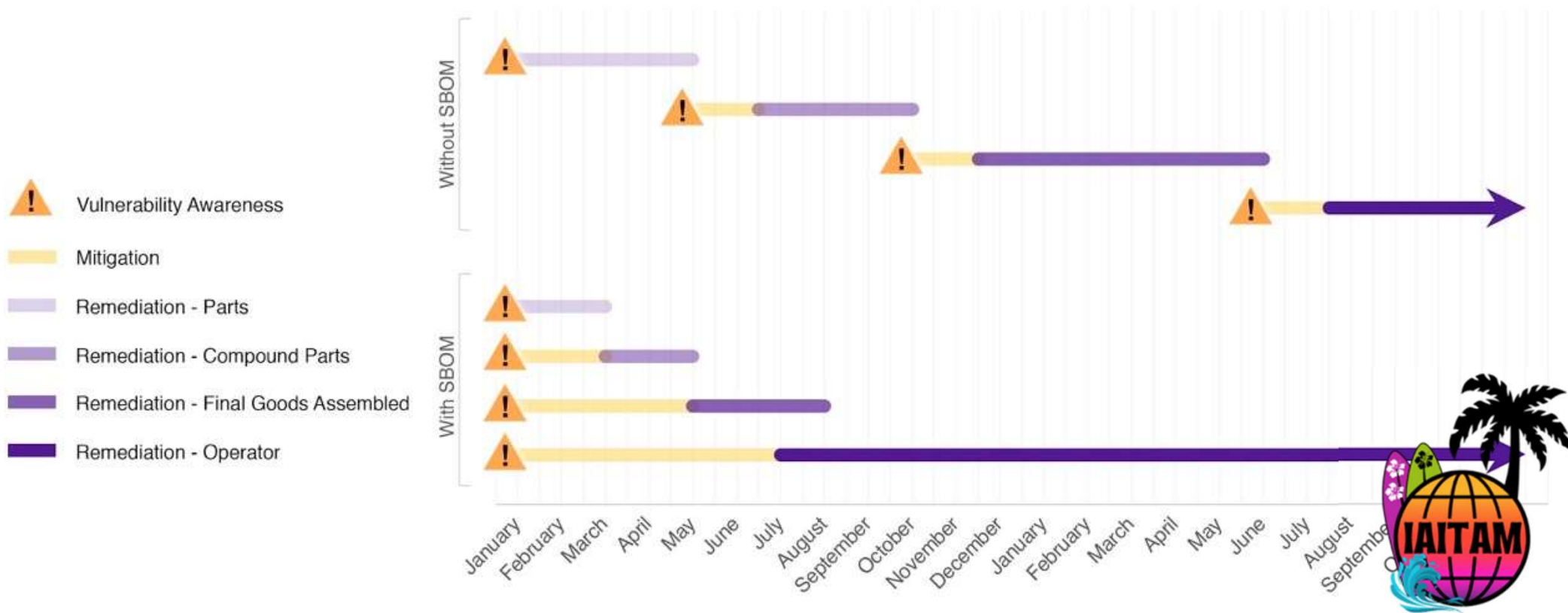


CycloneDX

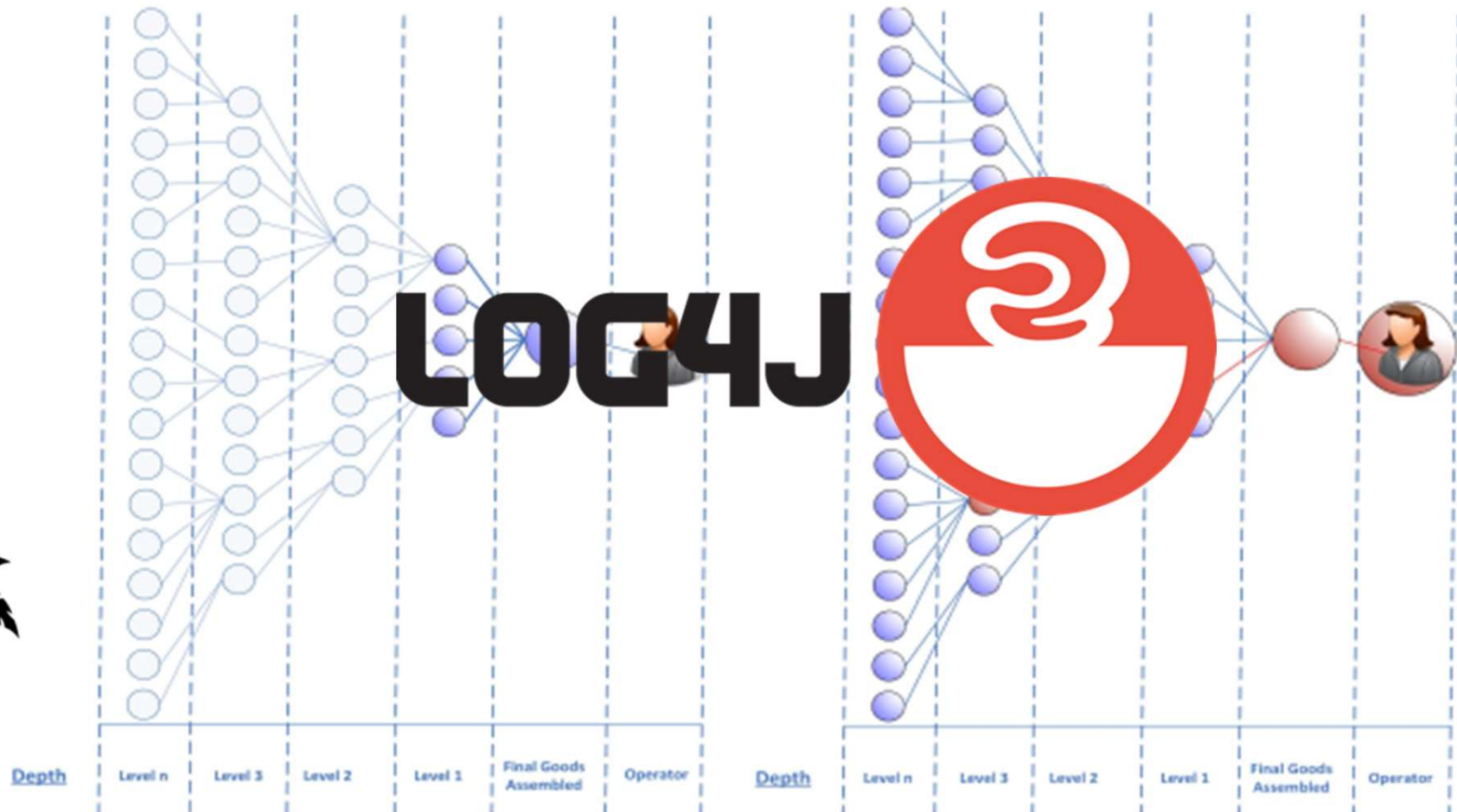



Time to Remediation Case Studies

Without and With SBOM



Depth Matters





***“If we had this today across our organization,
It would save us thousands of hours.”***





***“We like this idea...
We’ll do it when someone makes us.”***

- Product Security Lead for F100 company





The Power of the
Purse

&

Compliance



Executive Order 14028 (May 12, 2021)

“Improving the Nation’s Cybersecurity”



- "The trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is..."
- Uses government purchasing requirements as a lever
- Focus is on what is expected of software providers
- **Section 4: Enhancing Software Supply Chain Security.**
 - Separate build environments
 - MFA requirements
 - Documenting dependencies
 - Vulnerability management
 - SBOM
 - “attesting to conformity with secure software development practices”



US Government Supply Chain Policy

Executive Order 14028



The White House
May 2021

Secure Software
Development Framework



NIST
February 2022

OMB Memo 22-18



Office of Mgmt & Budget
September 2022

Self-Attestation Form
(draft)



CISA
Oct 2023

SBOM Minimum Elements



NTIA
July 2021



May 7-9, 2024 The M Resort  Las Vegas, NV

OMB Memo 22-18

- “Enhancing the Security of the Software Supply Chain through Secure Software Development Practices”
- Initial implementation based on NIST 800-218 “Secure Software Development Framework”
- Sets the model of “self-attestations”
- Target is government agencies
- Agencies *may* ask for an SBOM
- **CISA tasked to update SBOM “minimum elements” as needed.**



Self-Attestations

- Published by CISA in March 2024
 - Scope: new, proprietary software sold to the US government
 - Form that each vendor must sign for each product
 - Goes into effect Fall 2024
- Includes claims about
 - Secure development and build environments
 - Multi factor authentication
 - Continuous monitoring
 - Automated supply chain monitoring tools
 - Automated vulnerability management tools
- “The software producer maintains provenance for internal code and third-party components incorporated into the software to the greatest extent feasible”
- cisa.gov/secure-software-attestation-form



Medical Devices and FDA regulation

- Background
 - Explicitly mentioned in Congressional Healthcare Industry Cybersecurity Task Force (2017)
 - Idea raised in FDA 2018 Draft Pre-Market Guidance
 - Authorities for cybersecurity granted to FDA in FY 2023 Omnibus
 - Explicit SBOM requirements for “cyber devices”
- Submission Requirements for Devices
 - Must give FDA an SBOM if you qualify as a “cyber device”
 - Recommend an SBOM for non-Cyber Devices
 - “Refusal to Accept”
 - Is the submission complete
 - Will work with MDMs until Oct 1, and then *may* reject incomplete submissions
 - Supports the industry-recognized machine-readable formats (No PDFs)
- Status: Finalized Guidance still forthcoming
 - 2022 Draft Guidance offers details, including SBOM
- International Medical Device Regulators Forum





European Policies

Network and Information Systems Directive 2 (NIS2 2022)

Assess the risks associated with the products, services, and supply chains of third-party suppliers

Cyber Resilience Act (CRA 2024?)

Vulnerability Disclosure

SBOM requirements

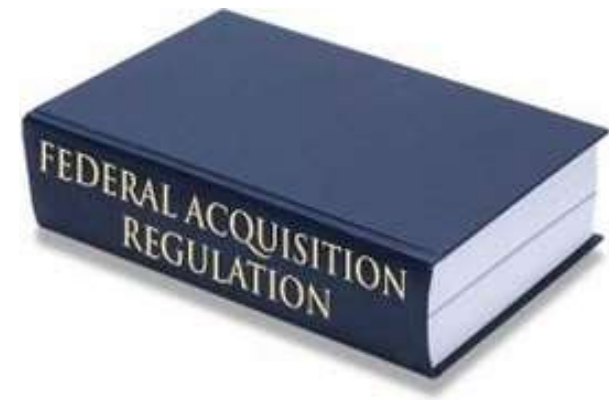
- Must have an SBOM

- Does not have to be public

- Available to the market surveillance auth

Federal Acquisition Regulation (FAR)

- New rules proposed in Oct 2023 for public comment 2021-017
- *“The Contractor shall maintain, and upon the initial use of such software in the performance of this contract, provide or provide access to the Contracting Officer a current SBOM for each piece of computer software used in performance of the contract. Each SBOM shall be produced in a machine-readable, industry-standard format and shall comply with all of the minimum elements...”*





Red-teaming SBOM Why not do this?

May 7-9, 2024 The M Resort  Las Vegas, NV



 **ITI** Promoting Innovation Worldwide

 **Cybersecurity
Coalition**




July 19, 2023

Why Do SBOM Haters Hate? Or Why Trade Associations Say the Darndest Things

by John Speed Meyers, Sara Ann Brackett,
and Trey Herr

SBOMs are an important step forward for software supply chain security, so despite pushback and opposition, industry and government should take a page out of Taylor Swift's book and just keep cruisin'—don't let SBOM haters get



- 
- “Roadmap to the attackers”
 - Intellectual Property
 - Do we actually need it?
 - It’s just not ready...



Red-teaming SBOM Why not do this?

May 7-9, 2024 The M Resort  Las Vegas, NV

Software by any other name...

46

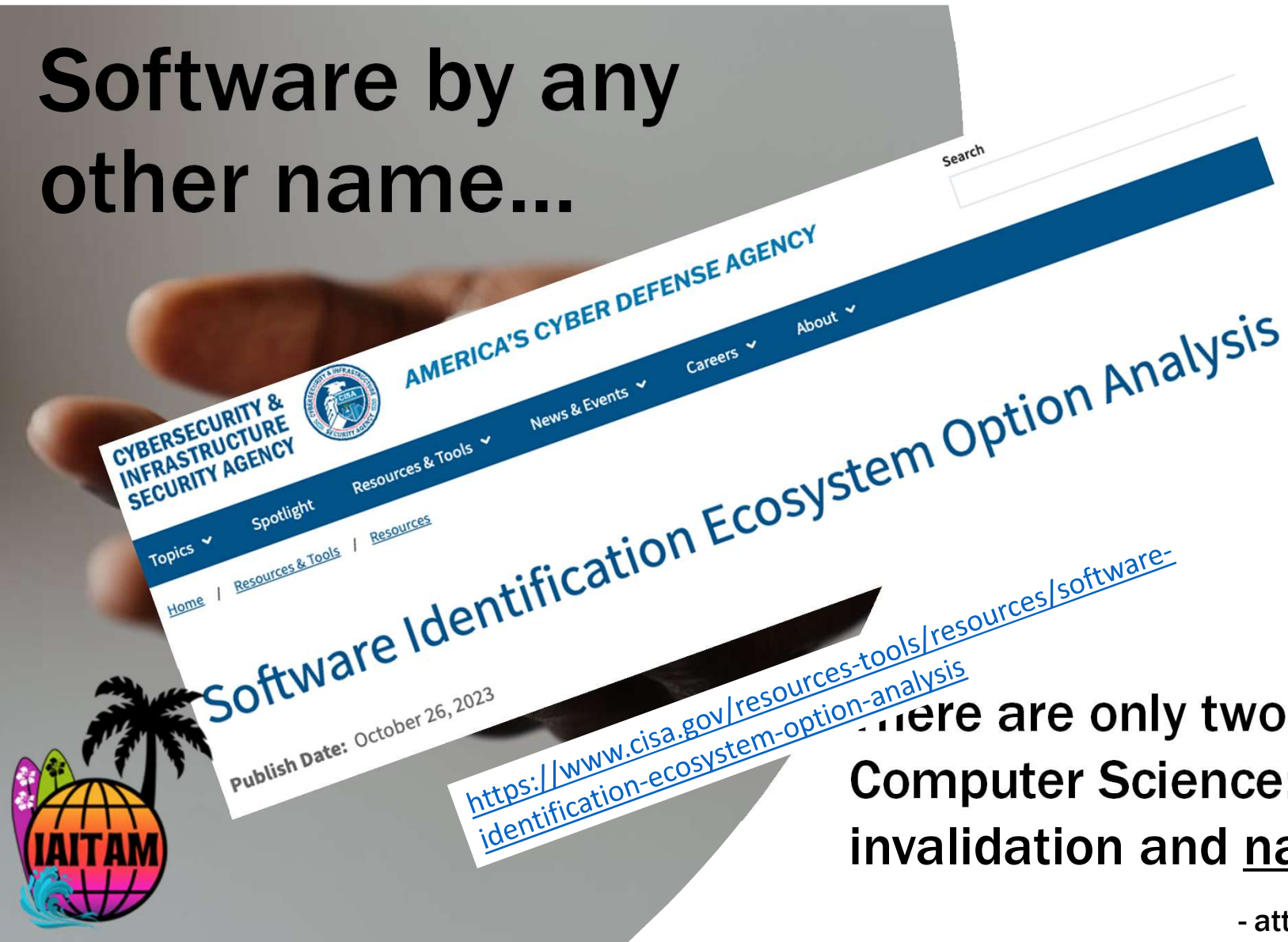


There are only two hard things in Computer Science: cache invalidation and naming things.”

- attributed to Phil Karlton

Software by any other name...

47



There are only two hard things in Computer Science: cache invalidation and naming things."

- attributed to Phil Karlton

Hardware Bill of materials



Summary: Why the ITAM Community should look *inside* the box with SBOM

- Improved visibility – what software do you actually have?
- Maintenance – plan for EOL in advance
- License compliance – direct and secondary risks
- Vulnerability management – risks in the supply chain
- Decision-making – more details about SW composition
- Cost optimization – unused or duplicate components
- Compliance – gubmints gonna gubmint





Revisiting takeaways

Understanding what's in our software and how it was made is a critical part of the software process

Why would anyone buy, use, or manage software without knowing what's in it or knowing how its made?

Transparency in all software is coming—and it can help you for your roles in managing assets and risk.



allan.friedman@cisa.dhs.gov
SBOM@cisa.dhs.gov
[@allanfriedman](#) #SBOM





IAITAM ACE

May 7-9, 2024 The M Resort 🌴 Las Vegas, NV

CISA.gov/SBOM

SBOM@cisa.dhs.gov

allan.friedman@cisa.dhs.gov

Finding your IAITAM Oasis

