



Software Supply Chain Risk: What Is It and Why Should You Care?

Covering New EU and U.S. SBOM Regulation

Matthew Brady
Senior Manager, Sales Engineering, Synopsys



CONFIDENTIAL INFORMATION

The information contained in this presentation is the confidential and proprietary information of Synopsys. You are not permitted to disseminate or use any of the information provided to you in this presentation outside of Synopsys without prior written authorization.

IMPORTANT NOTICE

In the event information in this presentation reflects Synopsys' future plans, such plans are as of the date of this presentation and are subject to change. Synopsys is not obligated to update this presentation or develop the products with the features and functionality discussed in this presentation. Additionally, Synopsys' services and products may only be offered and purchased pursuant to an authorized quote and purchase order or a mutually agreed upon written contract with Synopsys.

By attending this presentation your data will be shared by the organisers of the event and Synopsys may contact you about products and services you may be interested in. You can unsubscribe at anytime.

Agenda

- Legislation
- Software Supply Chain Risks
- Scope of the Problem
- SBOM to Solve Software Supply Chain Risks
- SBOM Challenges
- Summary

Legislation

Why are so
many people talking
about software supply
chain security?

EQUIFAX

solarwinds

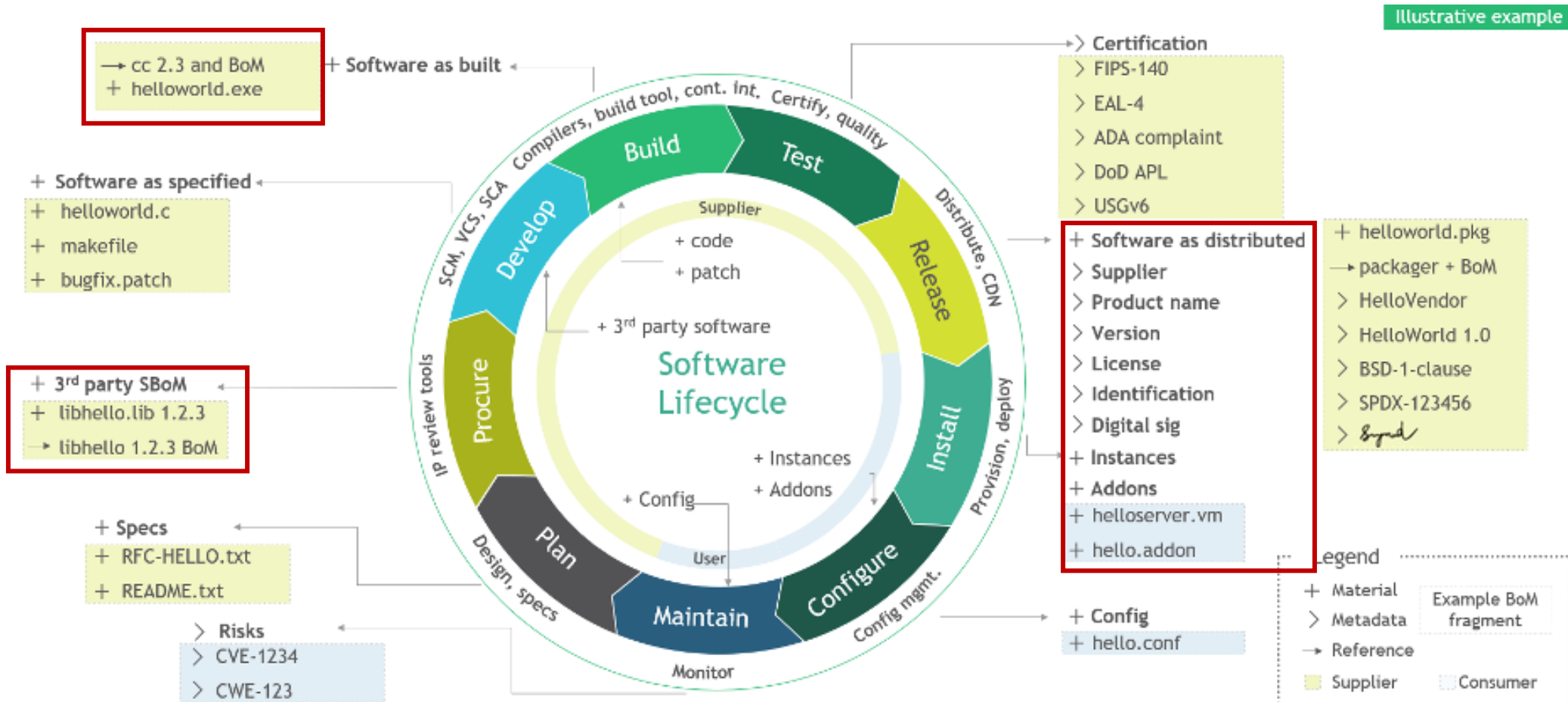


Executive Order on Improving the Nation's
Cybersecurity (14028)

May 12, 2021 Presidential Actions

Executive Order 14028

Improving the Nation's Cybersecurity

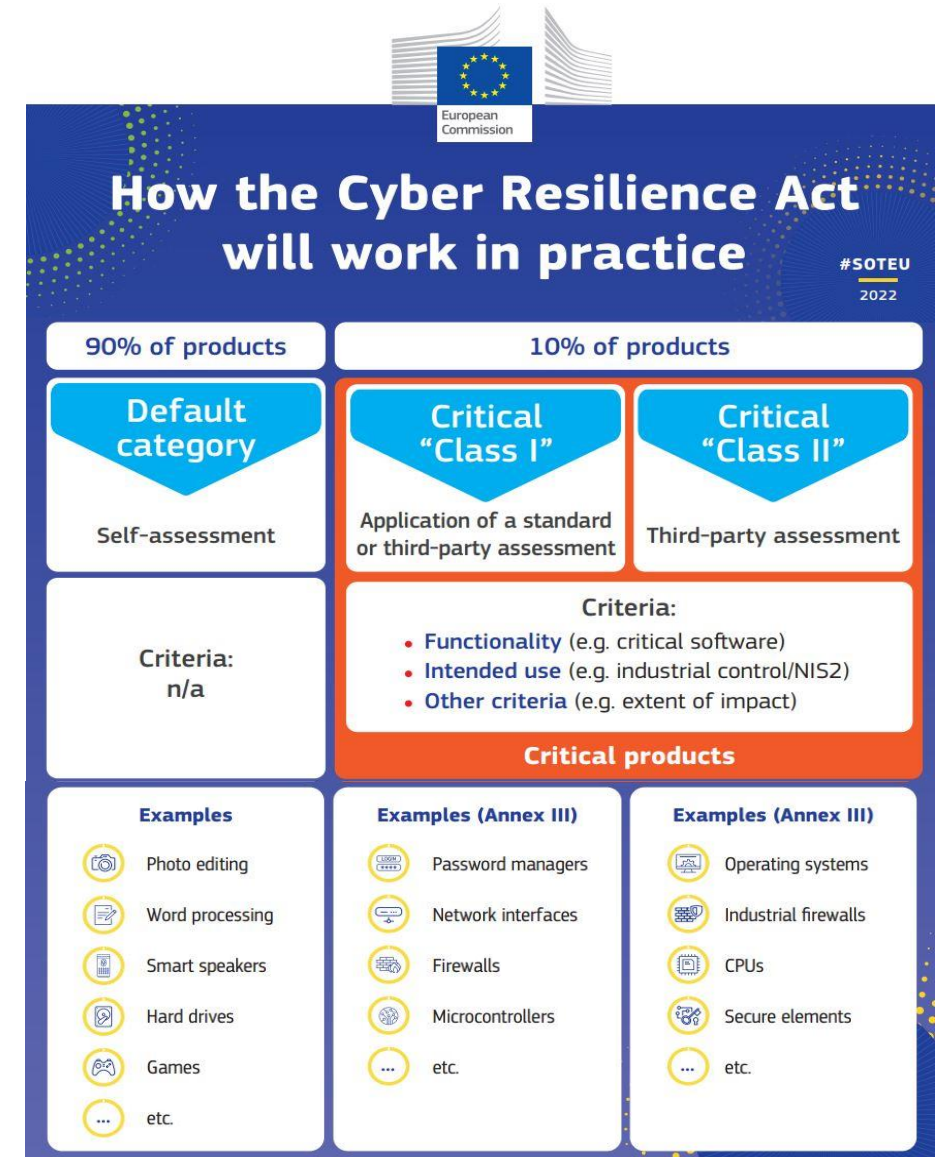


Cybersecurity - EU Regulations

- NIS Directive (2018)
 - Essential services and operators
- Cybersecurity Act (2021)
- NIS Directive II (Jan 2023)
 - NIS + Digital comms, Water, Pharma, Food, Space, Delivery Services, Public Administration
- Cyber Resilience Act (Proposal)

SBOM Mandated

*"Manufacturers of the products with digital elements shall:
(1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format..."*



Cybersecurity – UK Legislation

- U.K. PSTI: Product Security and Telecommunications Infrastructure Act (2022)
 - Covers IoT Devices
 - Secondary Legislation Expected 2023; Will Formalize SBOM
- U.K. Policy Paper: Feedback Process
 - Ended May 1, 2023
 - Includes SBOM

Software Supply Chain Risks



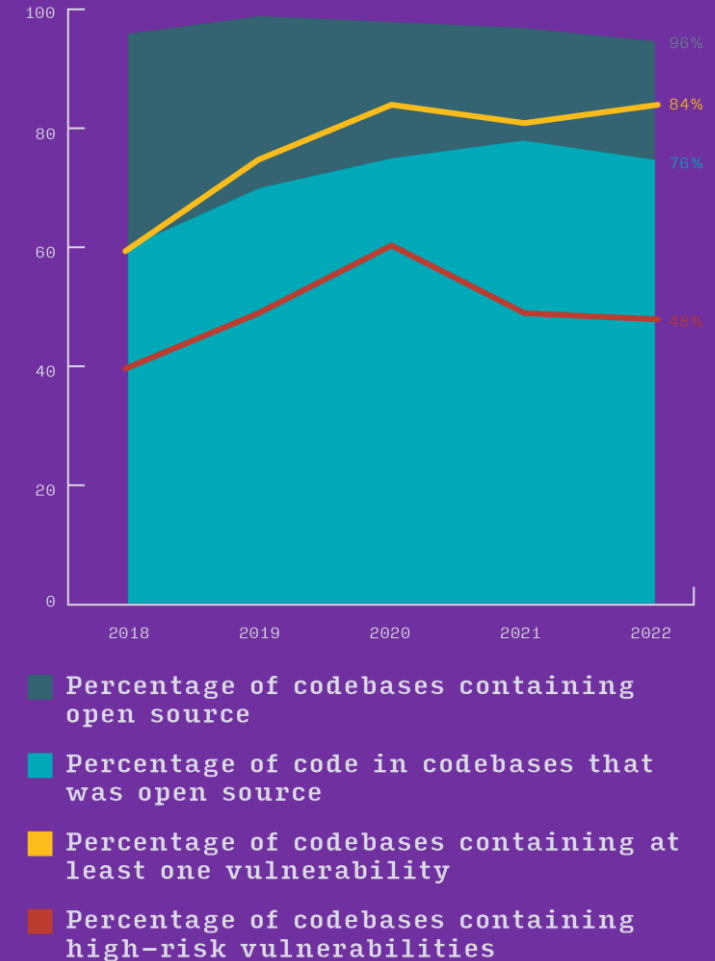
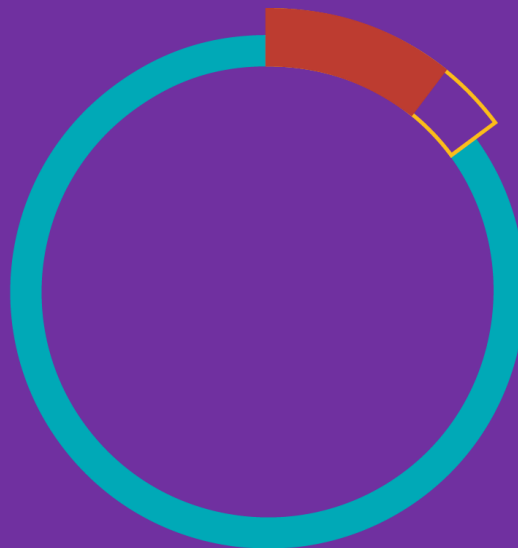
Software Supply Chain Risks

- 1 Zero-day exploits
- 2 Public vulnerabilities
- 3 License risk
- 4 Malware
- 5 Information leakage
...and many more

Synopsys “Open Source Security and Risk Analysis” Report 2023

- 1,703 applications assessed
- Almost all codebases contain OSS (96%)
 - Most applications are **mostly** OSS (76%)
- Most codebases were vulnerable (84%)
 - Almost half had high-risk vulnerabilities (48%)

568 Java codebases were scanned.
11% contained a vulnerable Log4J component, down from **15%** last year.



Scope of the Problem

Simple NodeJS App Demonstrating the Scope

Build an App to Integrate Slack & Instagram

```
"dependencies": {  
  "@slack/bolt": "^3.2.0",  
  "axios": "^0.21.1",  
  "dotenv": "^8.2.0",  
  "get-pixels": "^3.3.2",  
  "image-size": "^0.9.3",  
  "instagram-private-api": "^1.43.3",  
  "sharp": "^0.27.1",  
  "snoowrap": "^1.22.0"  
}
```

8 Declared Suppliers
(Dependencies)



@slack/bolt TS

3.4.0 • Public • Published 8 days ago



Readme



Explore

BETA



15 Dependencies

Bolt for JavaScript



codecov 66%

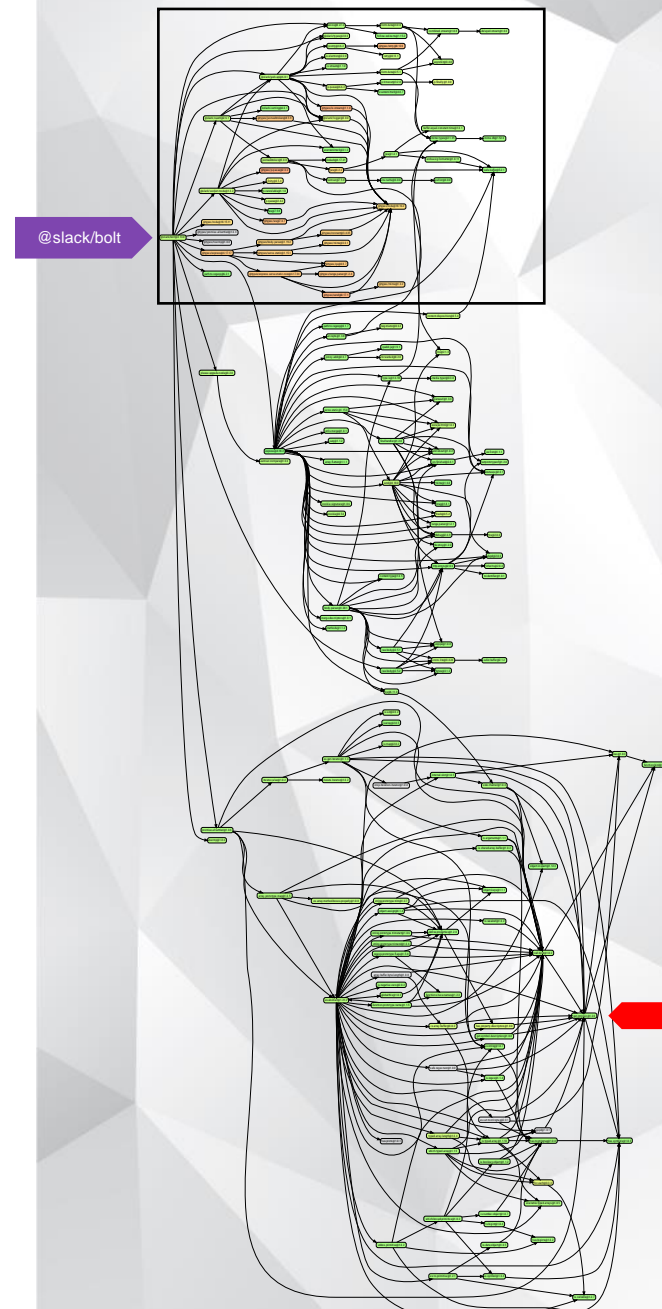
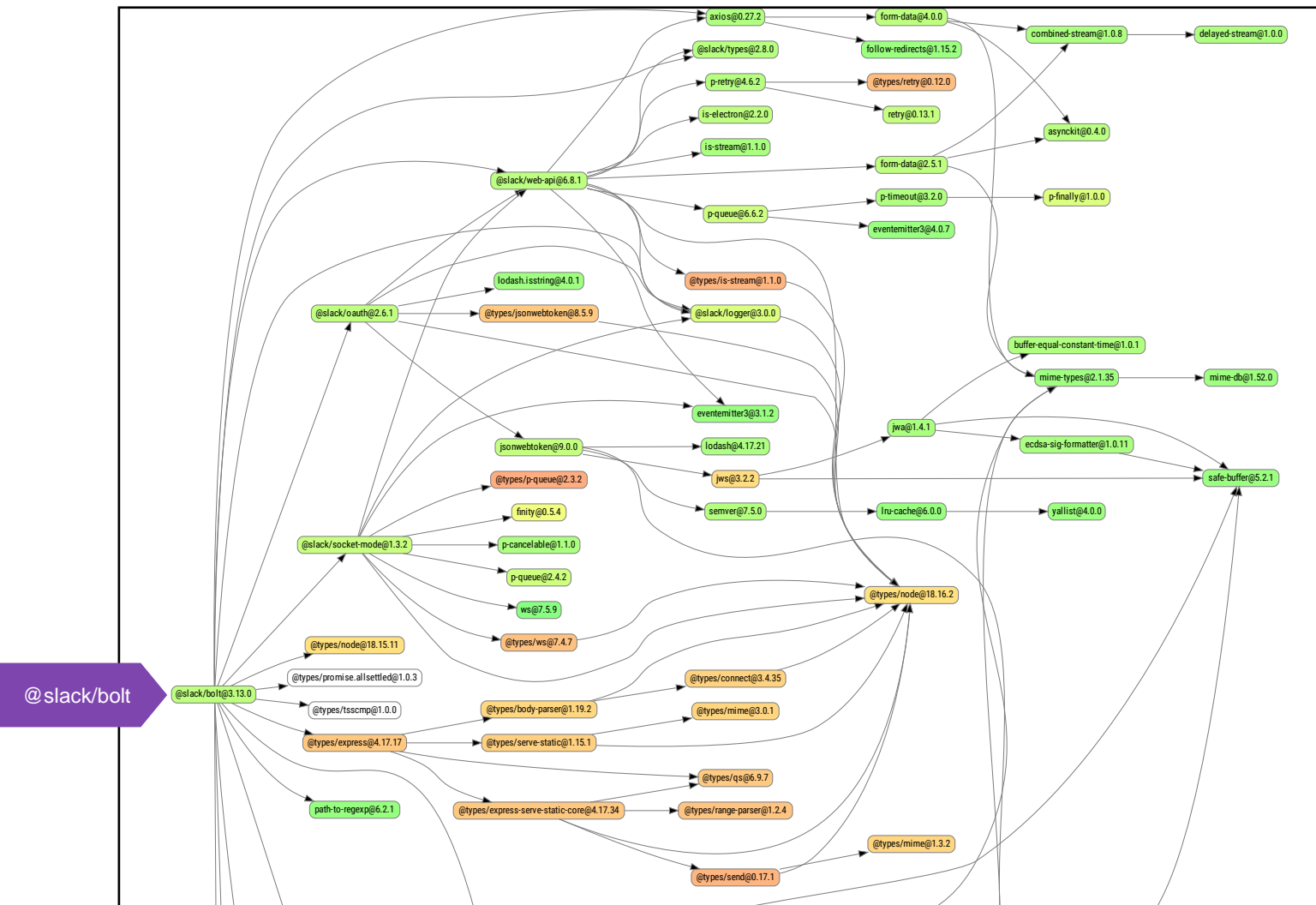


Node.js CI passing


A JavaScript framework to build Slack apps in a flash with the latest platform features.

Read the [getting started guide](#) to set-up and run your first Bolt app.

Dependency Tree: @slack/bolt



Handling Component End-of-Life Can Be Challenging

request 

2.88.2 • Public • Published a year ago



Readme



Explore

BETA



20 Dependencies

Deprecated!

As of Feb 11th 2020, request is fully deprecated. No new changes are expected land. In fact, none have landed for some time.

For more information about why request is deprecated and possible alternatives refer to [this issue](#).

Open

Request's Past, Present and Future #3142

mikeal opened this issue on Mar 30, 2019 · 394 comments

Maintenance Mode

Here's the plan.

- request will stop accepting new features.
- request will stop considering breaking changes.
- The committers that are still active will try to merge fixes in a timely fashion, no promises though.
- Releases will be fully automated, any merge into master will be published. I've already built this for [some other projects using GitHub Actions](#).
 - We're going to have to remove inactive collaborators and enforce 2fa, because commit rights will effectively become npm publish rights.



2413



178



80



131



245



656



204



233

What About Vulnerabilities?

🚫 CVE-2020-28282 Detail

Description

Prototype pollution vulnerability in 'getobject' version 0.1.0 allows an attacker to cause a denial of service and may lead to remote code execution.

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

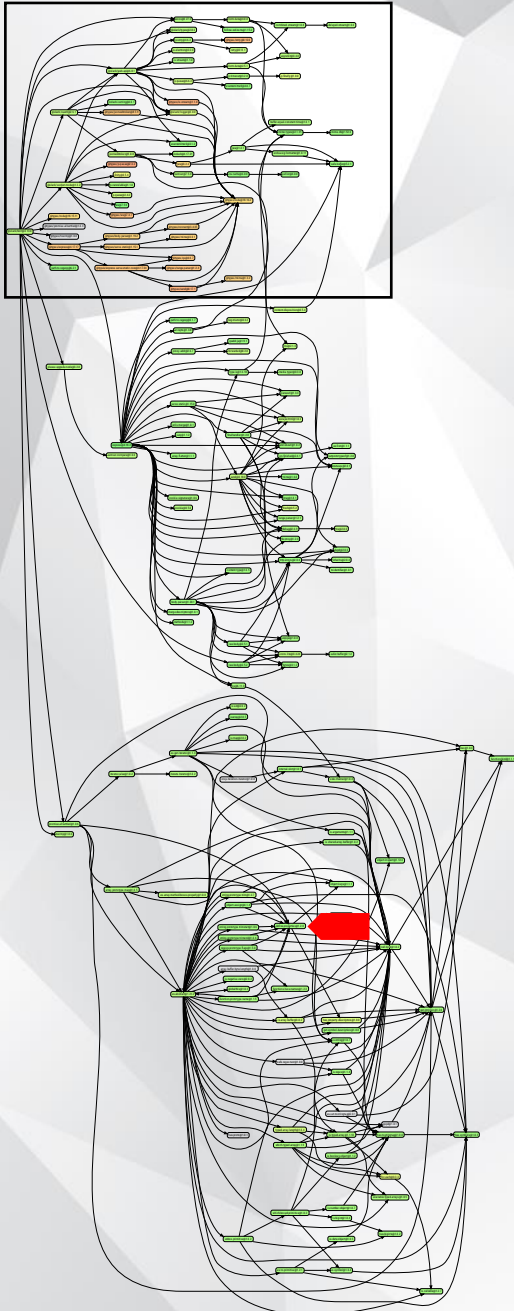
Base Score: 9.8 CRITICAL

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

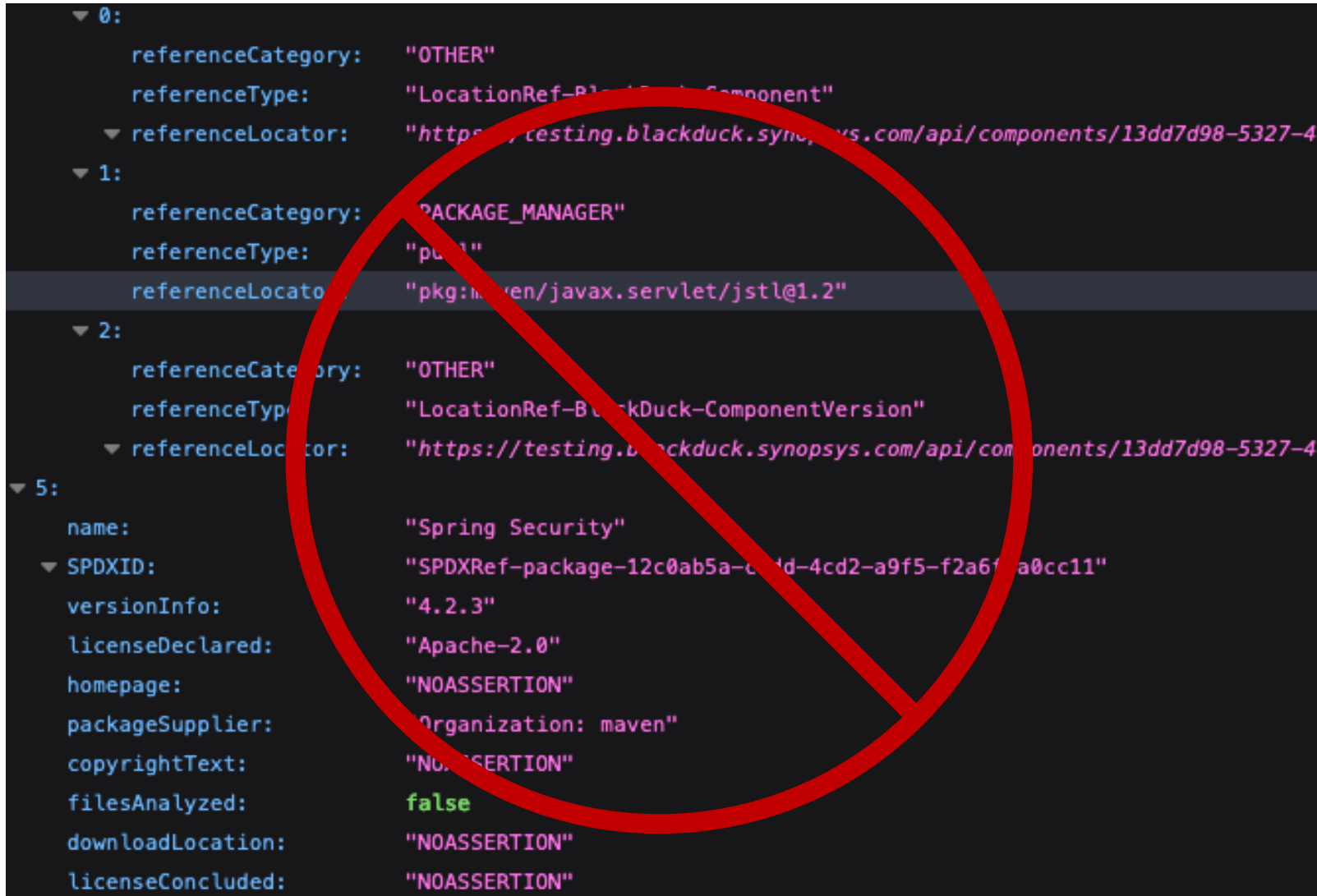
Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

@slack/bolt



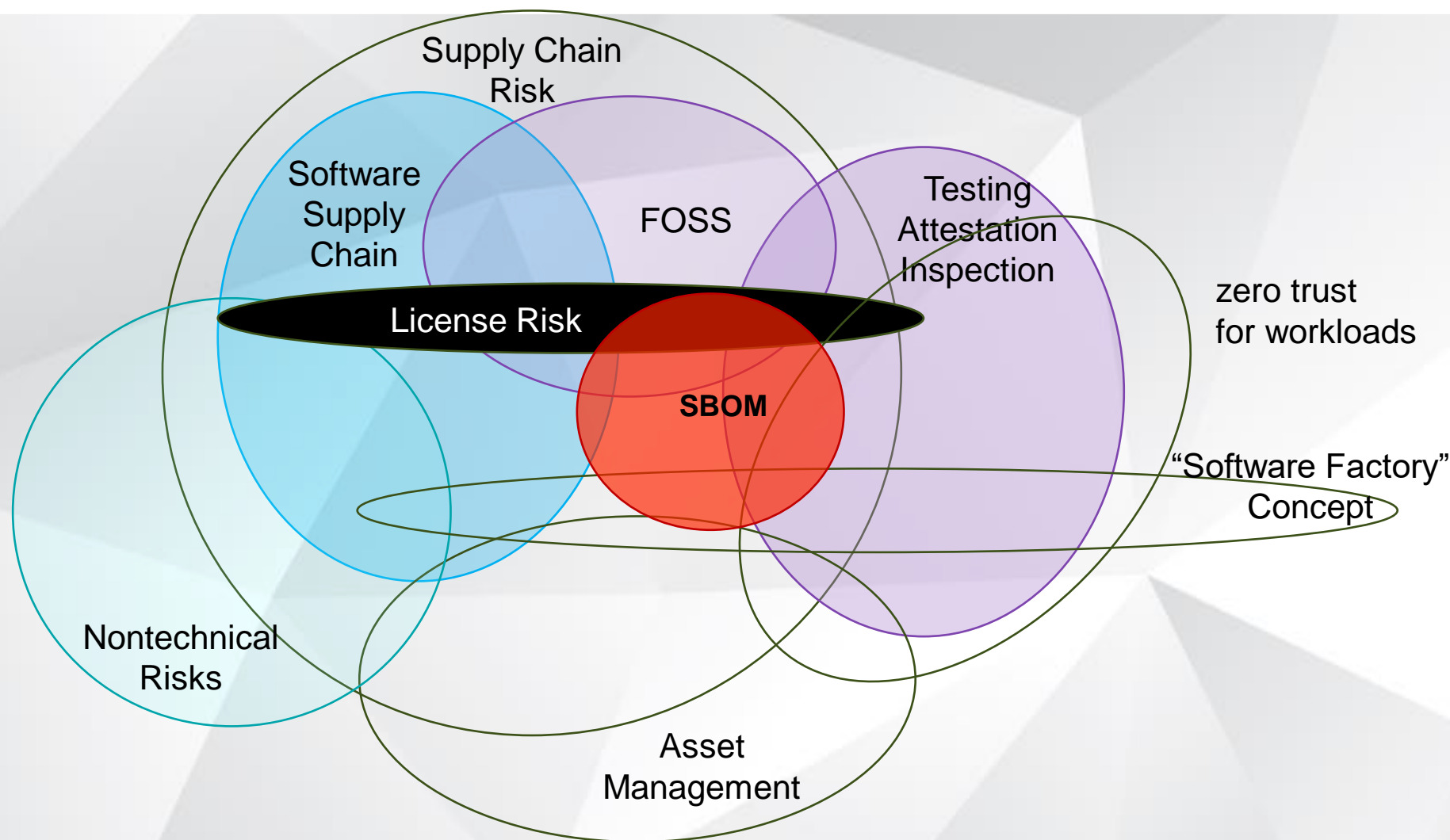
SBOM to Solve Software Supply Chain Risks?

What Is SBOM All About *Really*?

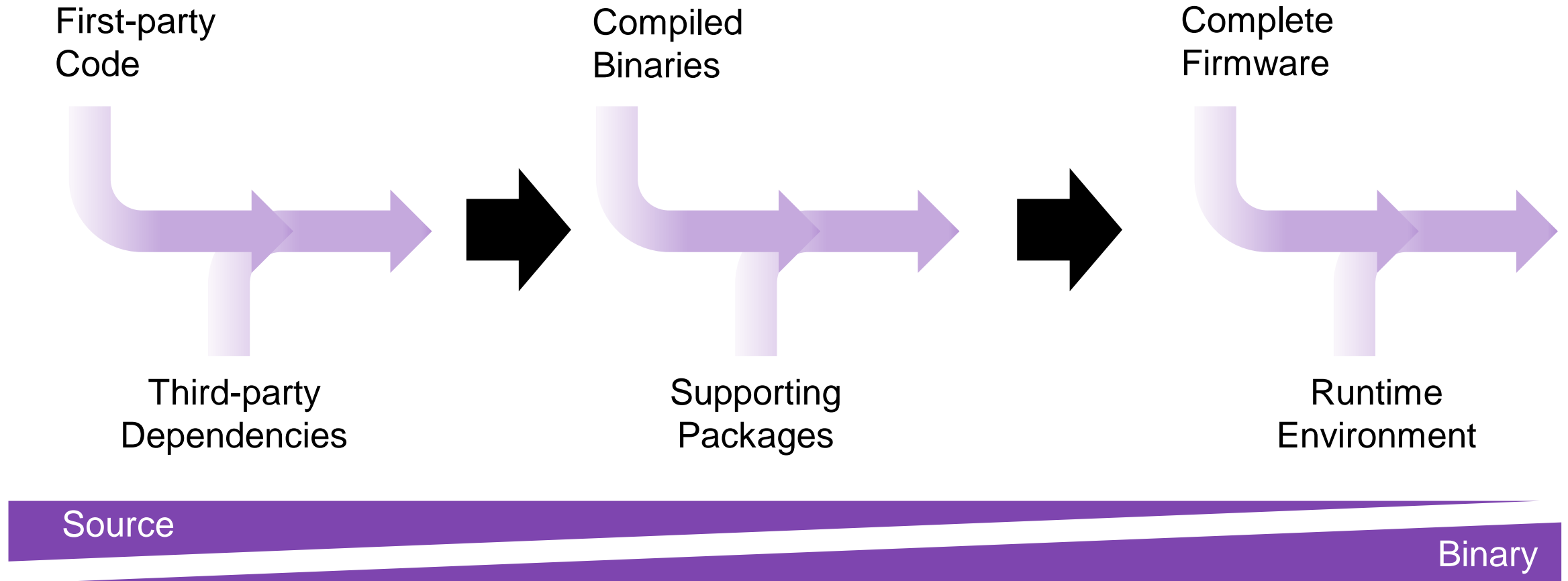


Software Supply Chain

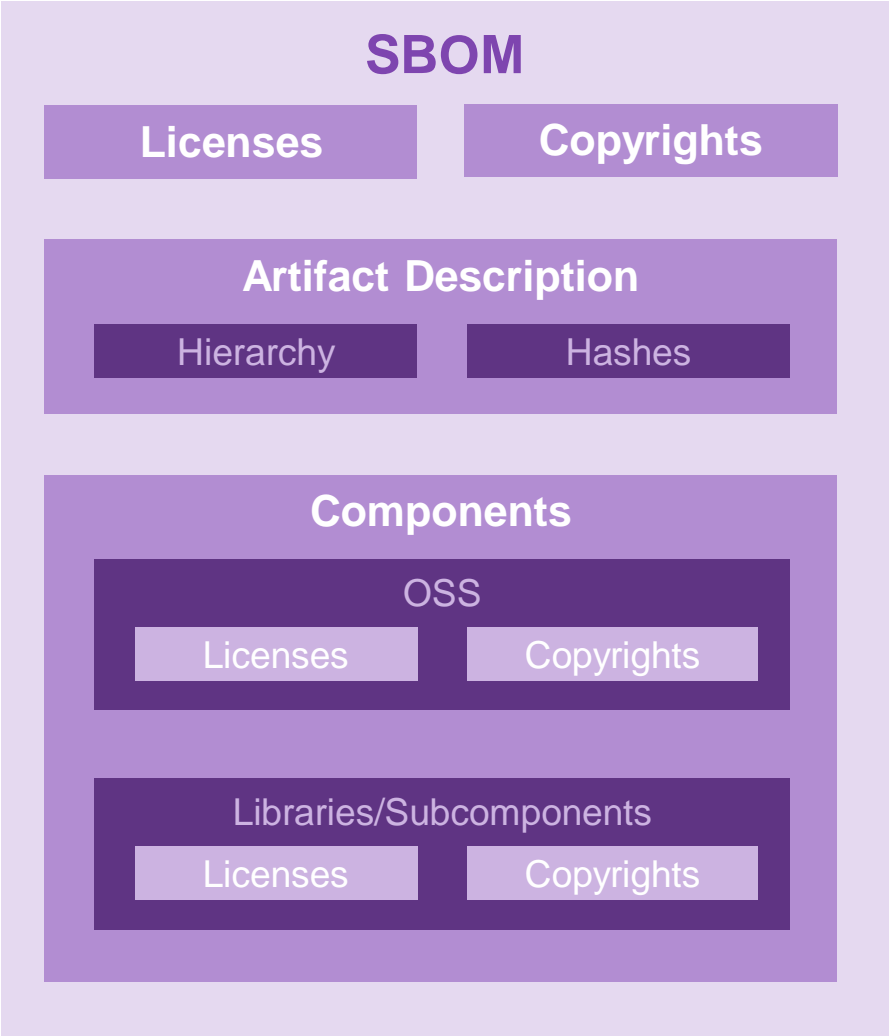
SBOMs Do Not Exist in Isolation



Life-Cycle Centric View



SBOM Structure



Standards

- SPDX
- CycloneDX

Formats

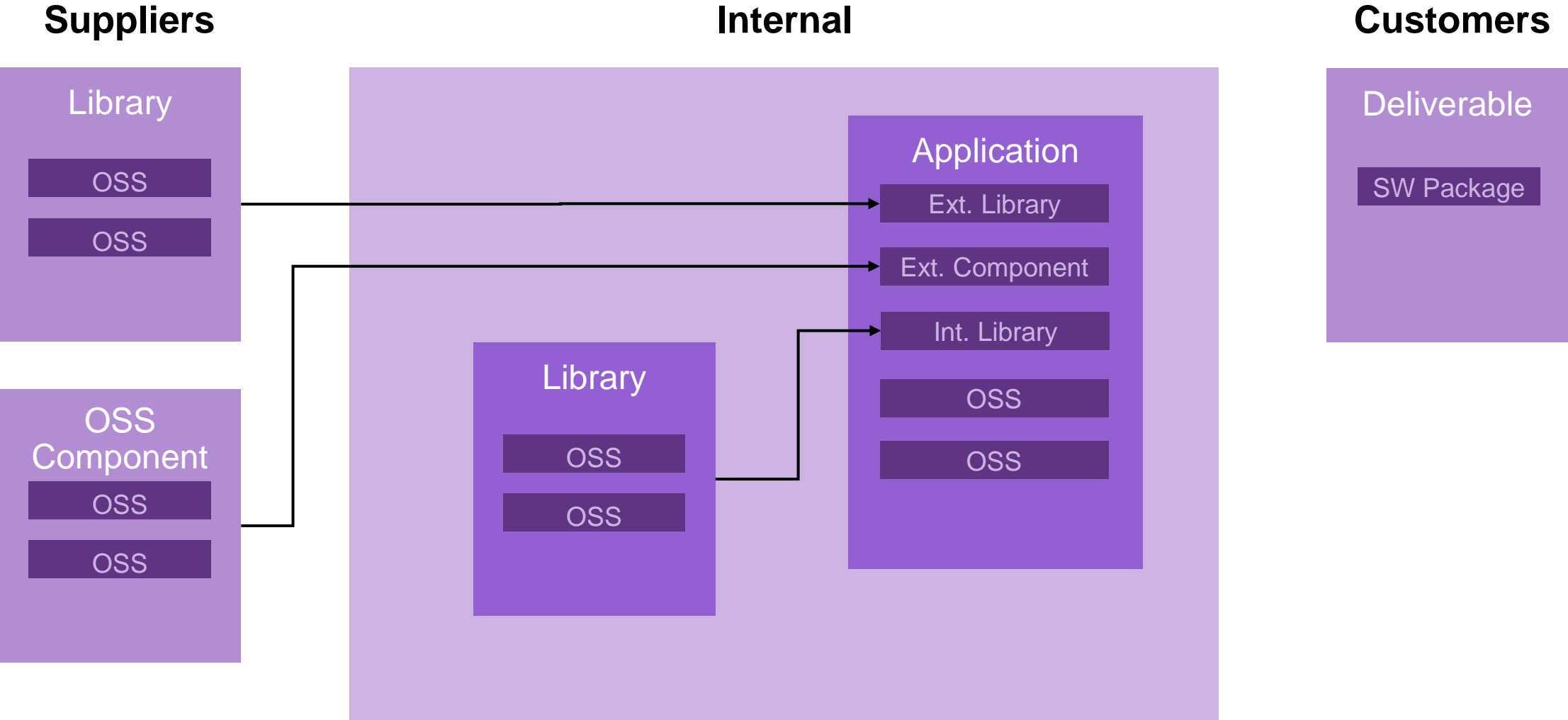
- JSON
- RDF
- Tag Value
- XML



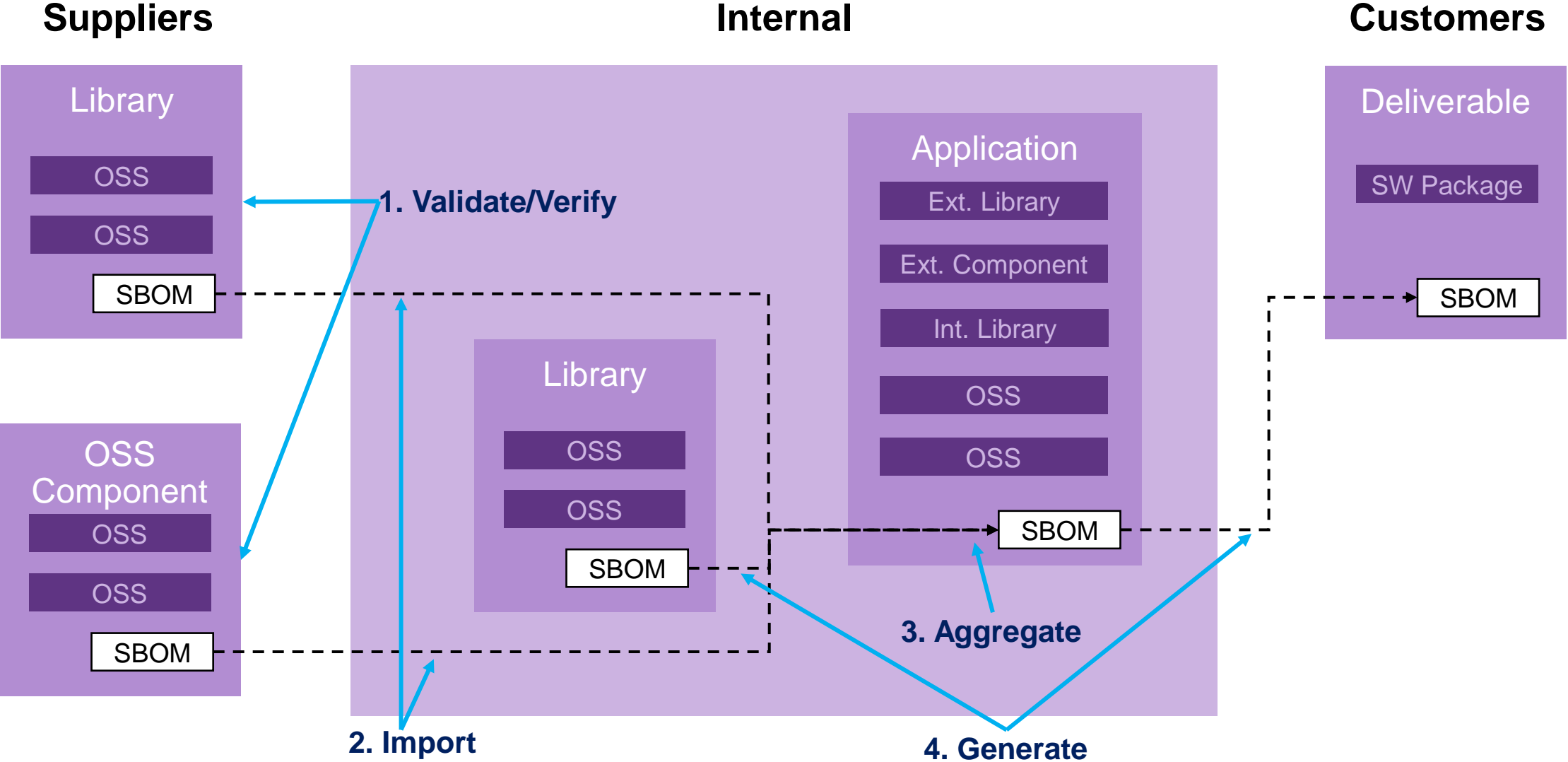
Vulnerability Exchange (VEX)

- Supported in CycloneDX 1.4
—(Not compliant with NTIA?)
- Not Yet Supported in SPDX

SBOM Workflow



SBOM Workflow



SBOM Gaps

- Developing standard: stream of new requirements
- Multiple standards
 - CycloneDX, SPDX, SWID
- Inconsistent aggregation
 - Package
 - Component
 - Subcomponent
 - File
 - Artifact
- Inconsistent package identification
 - CPE: common platform enumeration
 - PURL: package URL

CPE

Wildcards

```
cpe:<cpe_version>:<part>:<vendor>:<product>:<version>:  
<update>:<edition>:<language>:<sw_edition>:<target_sw>:  
<target_hw>:<other>
```

PURL

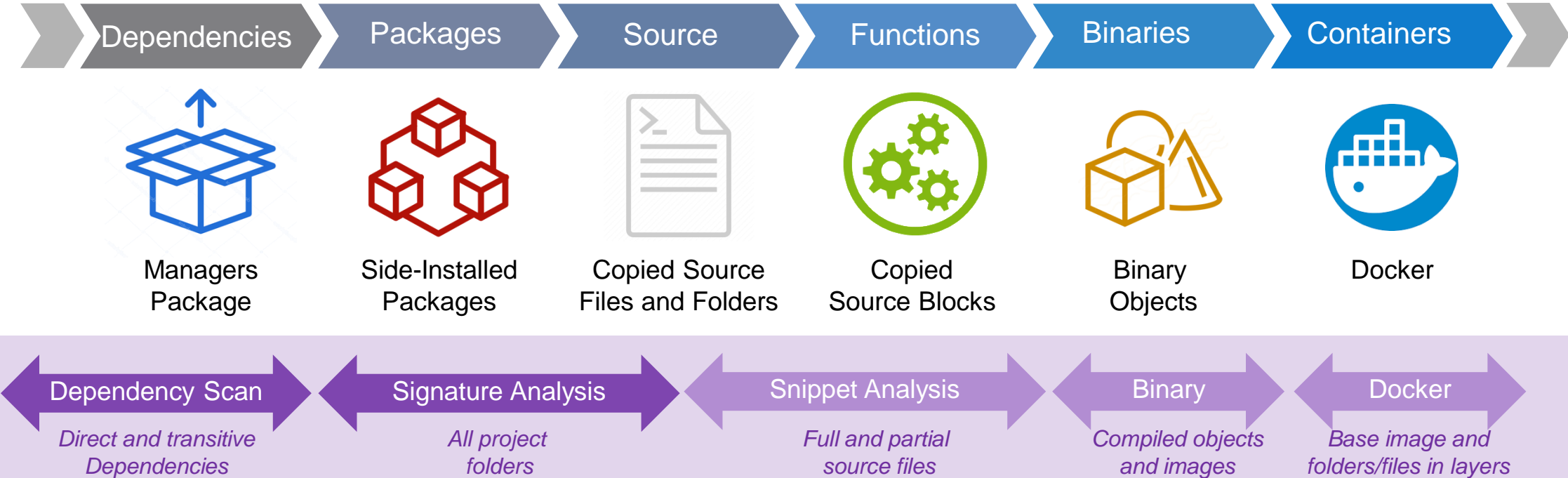
Origin Specific - Inconsistent

```
• gem:ruby-launcher@1.1.2?platform=java  
• github:package-url/purl-spec@244fd47e07d1004f0aed9c  
• golang:google.golang.org/genproto#googleapis/api/annotations  
• maven:org.apache.xmlgraphics/batik-  
  anim@1.9.1?repository_url=repo.spring.io
```

SBOM Challenges

Accurate Identification and Validation

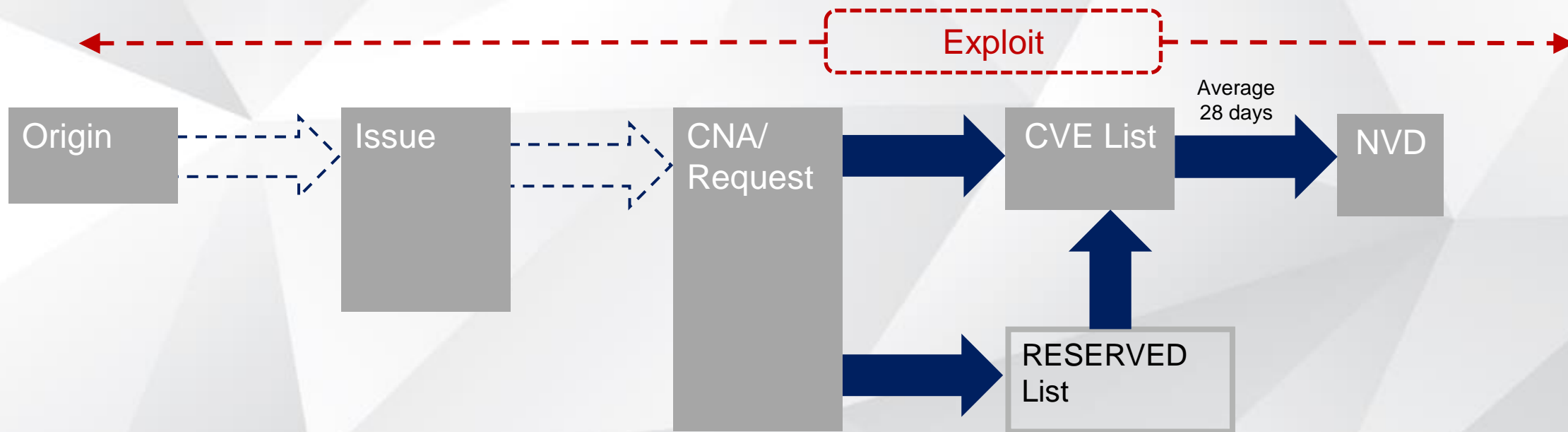
Identifying OSS and Third-Party Software



SBOM Challenges

Precise Vulnerability Guidance

Public Security Workflow

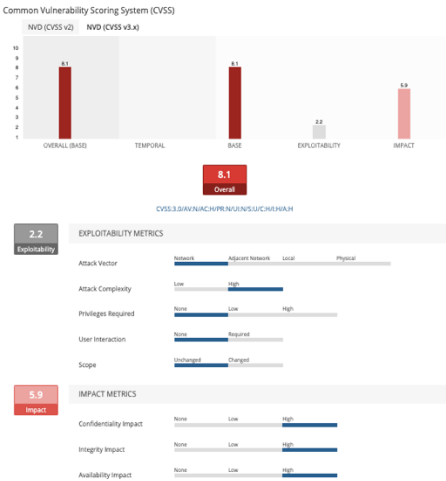


Public Security Workflow

4 YEARS
Vulnerabilities go undetected before being identified

4.4 WEEKS
For the community to code and release a fix after a vulnerability is identified

10 WEEKS
To alert the community on the availability of a security update



SLOW!

INCOMPLETE

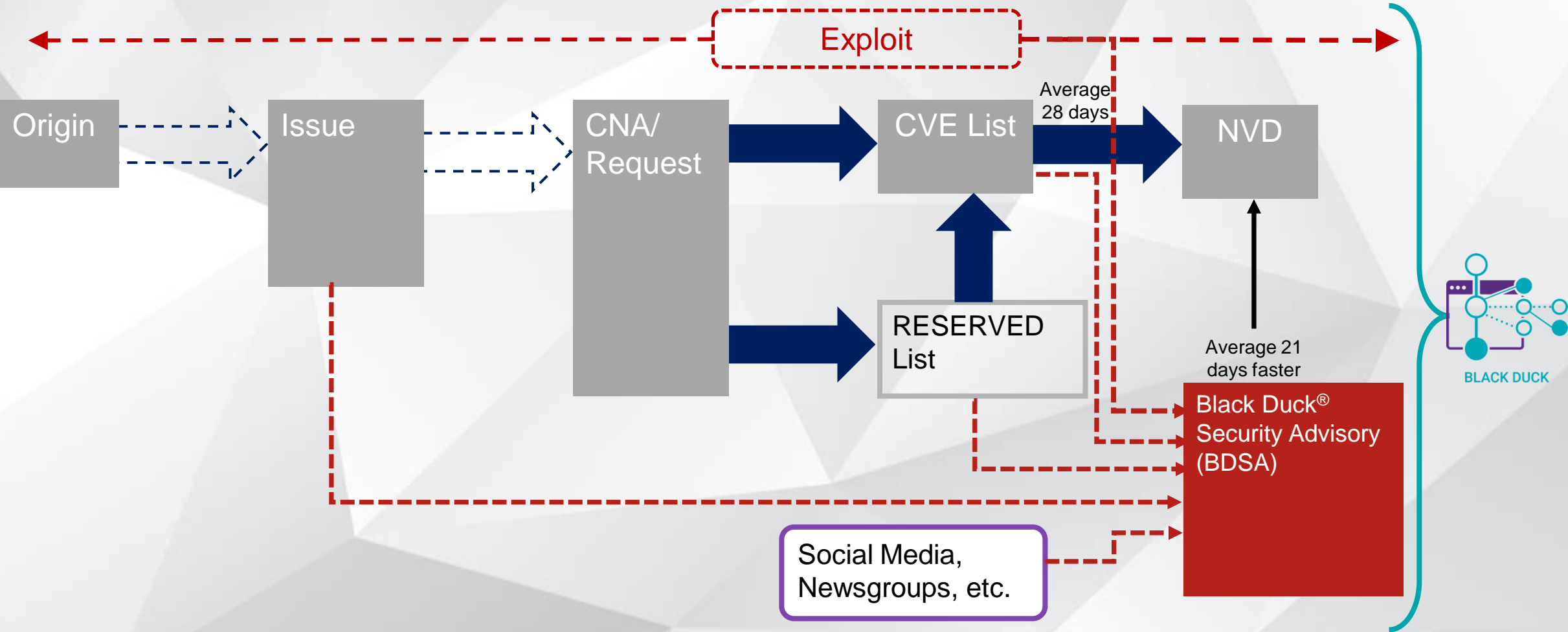
POOR REVIEW

NO GUIDANCE

CVE-ID	
CVE-2019-0232	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default. The CGI option enableCmdLineArguments is disable by default in Tomcat 9.0.x (and will be disabled by default in all versions in response to this vulnerability). For a detailed explanation of the JRE behaviour, see Markus Wulftange's blog (https://codewhitesec.blogspot.com/2016/02/java-and-command-line-injections-in-windows.html) and this archived MSDN blog (https://web.archive.org/web/20161228144344/https://blogs.msdn.microsoft.com/twistylittlepassagesallalike/2011/04/23/everyone-quotes-command-line-arguments-the-wrong-way/).	

<https://www.esecurityplanet.com/applications/open-source-security-a-big-problem/>
<https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis>

Enhanced Security Workflow



SCA and SBOM Summary



Multifactor Scanning

source, dependencies, binaries, snippets, artefacts etc.



Advanced Vulnerability Data

public data not reliable



Shift Everywhere

automation, compliance, validation



SBOM

does not replace full appsec process;
developing standard; trust but verify

Black Duck by Synopsys

Unparalleled OSS Coverage

Full Multi-Factor Identification

Declared License

Component ^	Source	Match Type	Usage	License	Security Risk
✓ Adobe Flash Player 11.4.402.265	1 Match	Binary	Dynamically Linked	M Basic Proprietary Commercial License	36 179 18
✓ adobe/XMP-Toolkit-SDK ?	1 Match	Binary	Dynamically Linked	BSD-3-Clause	9 9 4
✓ antlr 2.7.7	3 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	ANTLR-PD	
✓ AOP Alliance (Java/J2EE AOP standard) 1.0	3 Matches	Transitive Dependency, Exact Directory	Dynamically Linked	Public Domain	
✓ Apache Bean Validation :: bval-core 1.1.2	1 Match	Exact Directory	Dynamically Linked	Apache-2.0	

Expert, Private Vulnerability Feed

Full BOM Curation

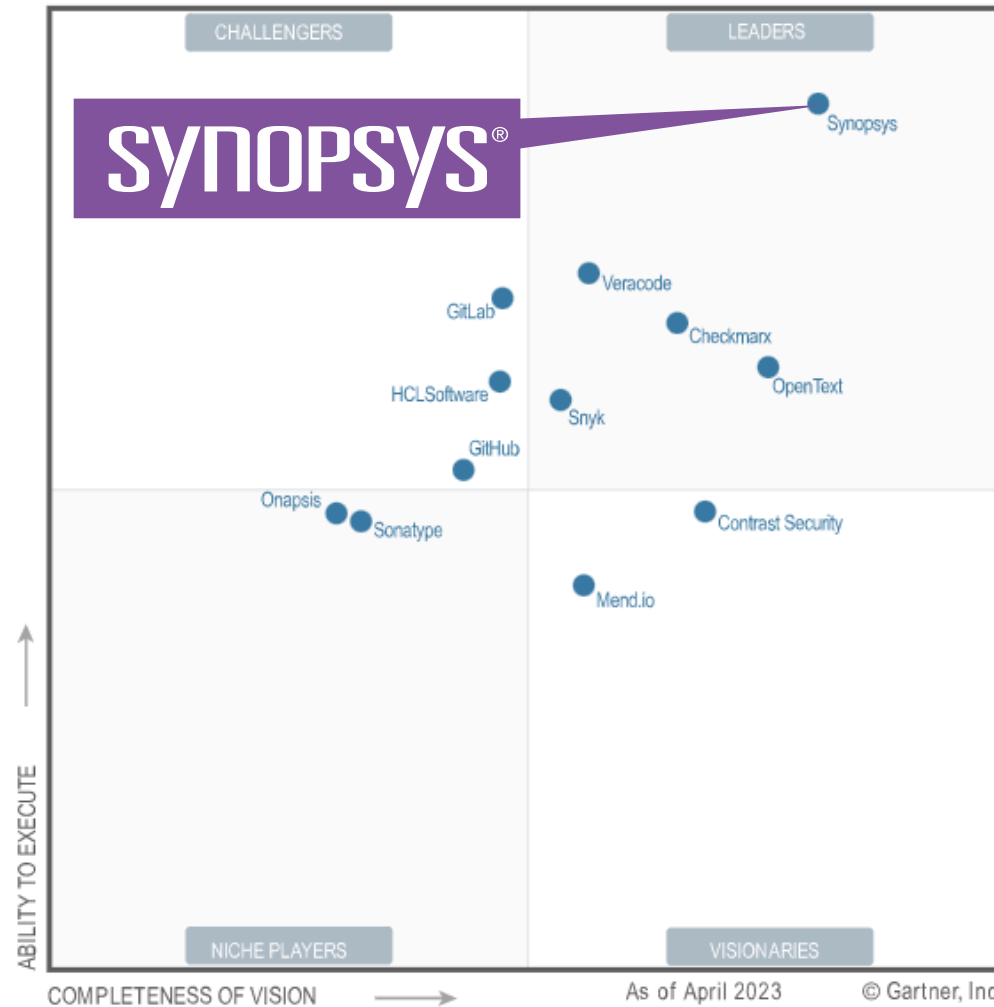
SBOM Generation

SBOM Import

Deep License

Gartner® 2023 Magic Quadrant™ for Application Security Testing

Synopsys: The Recognized Leader in Application Security





Come & Talk to us - Stand U20