SOFTWARE SUPPLY CHAIN RISK MANAGEMENT

Son Nguyen
Email: SonNV@mi2.com.vn
Mobile: +84977585651

AGENDA

- SOFTWARE SUPPLY CHAIN RISKS
- SBOM TO RESOLVE SOFTWARE SUPPLY CHAIN RISKS
- SSC RISK MANAGEMENT WITH BLACKDUCK
- DISCUSSION

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

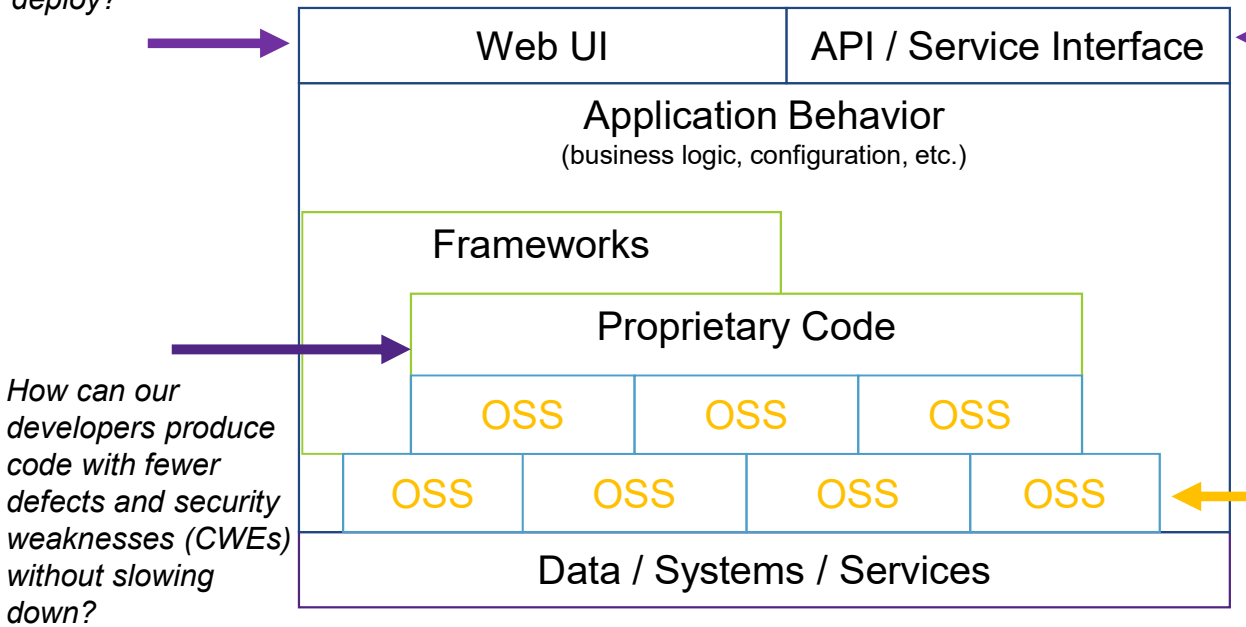
Why Are So Many People Talking About Software Supply Chain Security?

Presentation content source: Synopsys

APPLICATIONS & SECURITY ISSUES

How do we know we've addressed runtime vulnerabilities and data protection issues before we deploy?

How do we ensure the protocols & APIs our software exposes aren't vulnerable to common hacks?



How can our developers produce code with fewer defects and security weaknesses (CWEs) without slowing down?

How do we track and manage open source use and the security and license compliance risks that come with it?

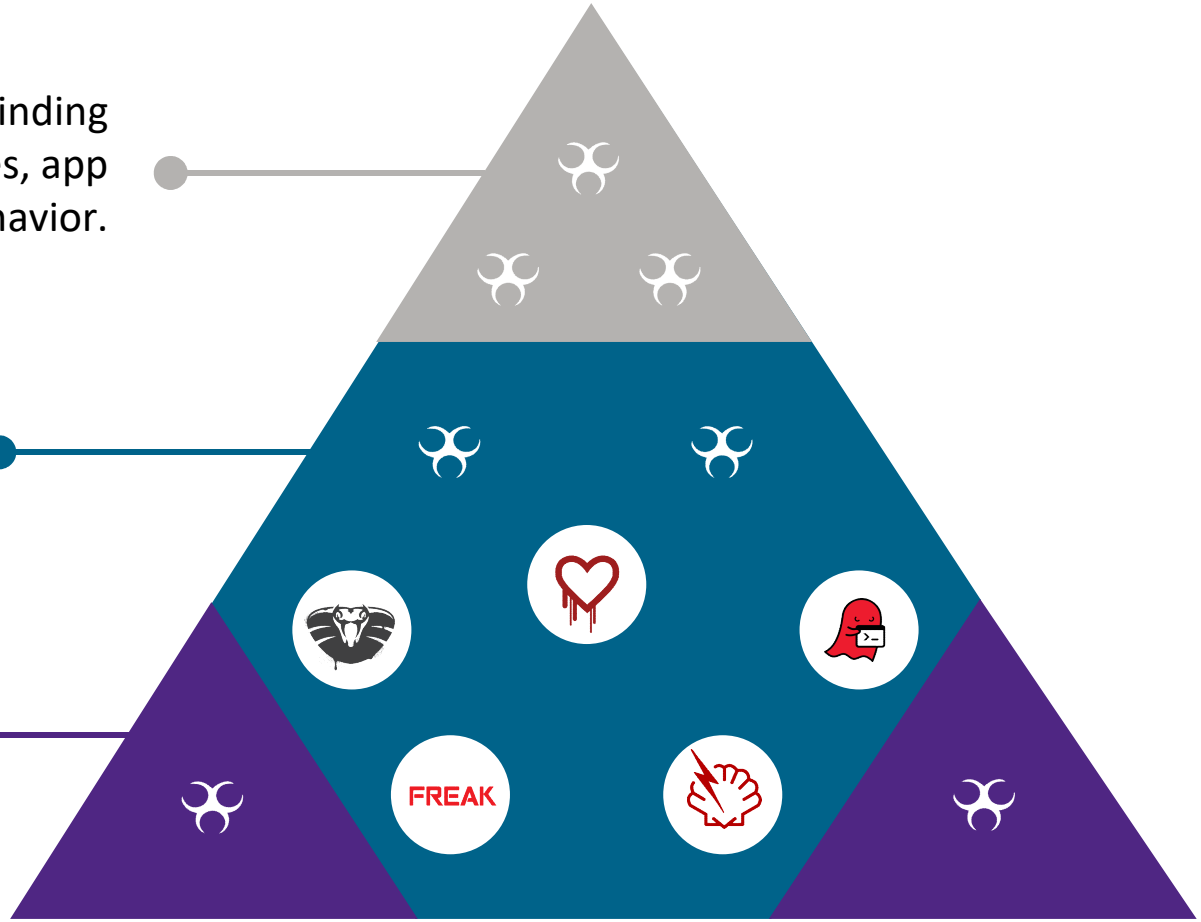
Presentation content source: Synopsys

APPLICATIONS & SECURITY ISSUES

SAST and DAST tools are good at finding security weaknesses in coding practices, app configuration, and behavior.

But most open-source vulnerabilities are too complex and too deep in the code to be found by SAST or DAST alone.

Library dependencies are often opaque to developers and open doors to vulnerabilities not in custom code.

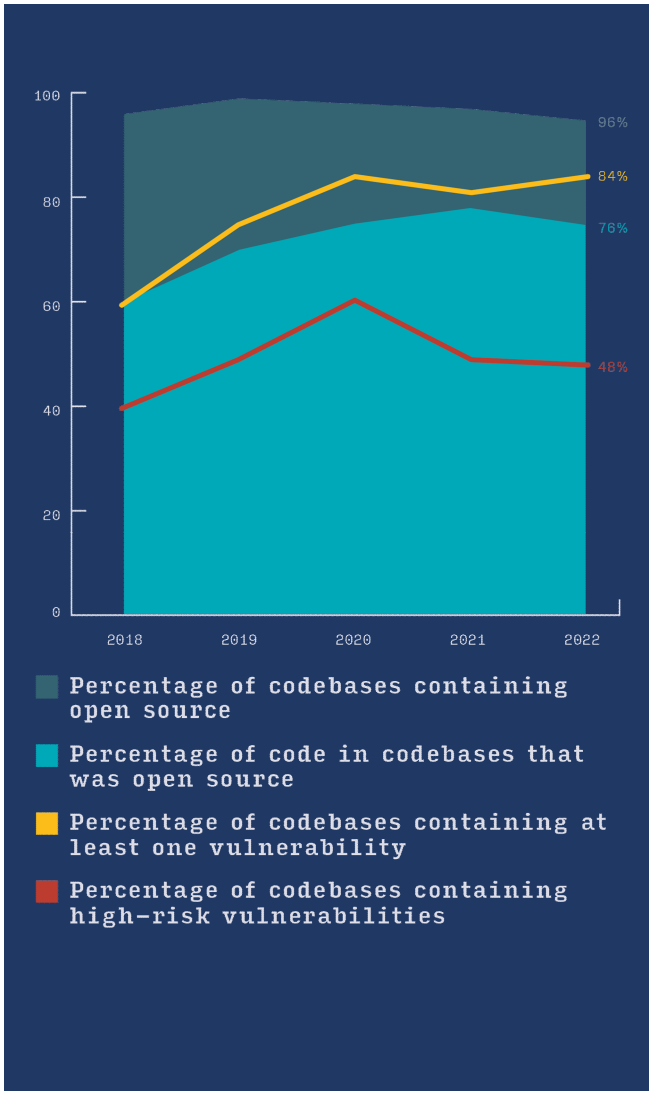


Presentation content source: Synopsys

SYNOPSYS OPEN SOURCE SECURITY AND RISK ANALYSIS REPORT 2023

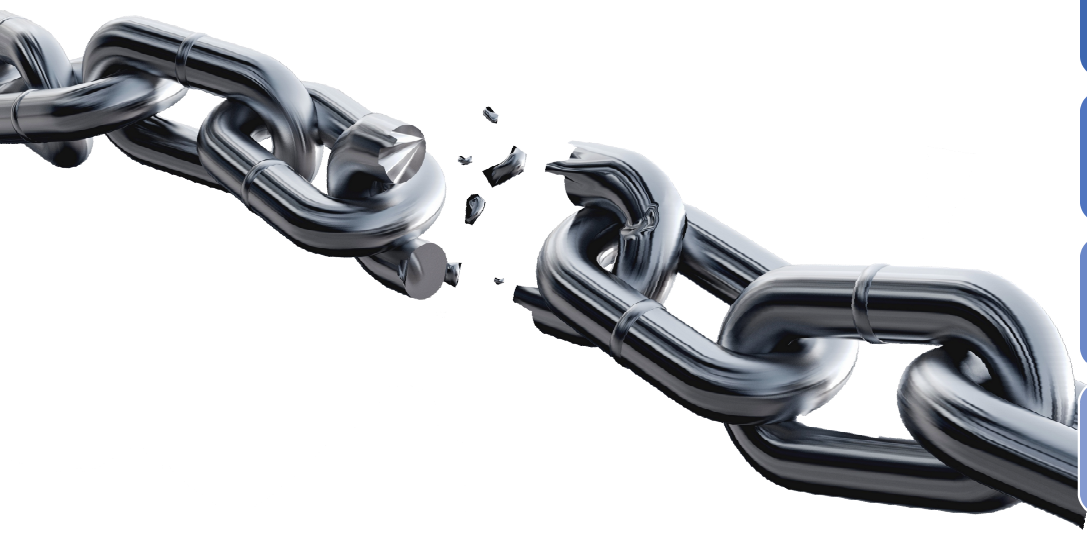
> 1703 Applications Assessed

- Almost All Codebases Contain OSS (96%)
  - Most Applications are Mostly OSS (76%)
- Most Codebases Were Vulnerable (84%)
  - High-Risk Vulnerabilities (48%)



Presentation content source: Synopsys

OPENSOURCE & SOFTWARE SUPPLY CHAIN RISKS



- Zero-Day Exploits
- Public Vulnerabilities
- License Risk
- Malware
- Information Leakage

Presentation content source: Synopsys

LEGAL RISK

All Software Should Be Licensed

- Liability
- Trademarks
- Patents
- Ownership

MIT License

Copyright 2020, Synopsys Ltd.

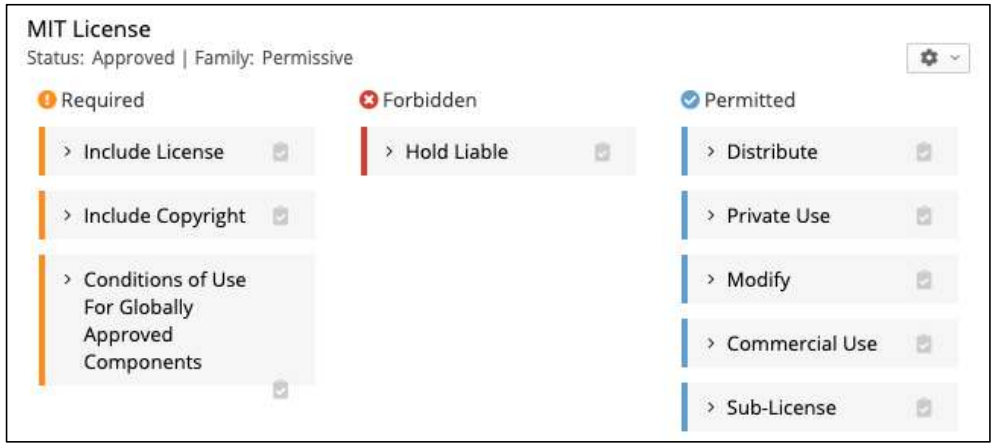
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

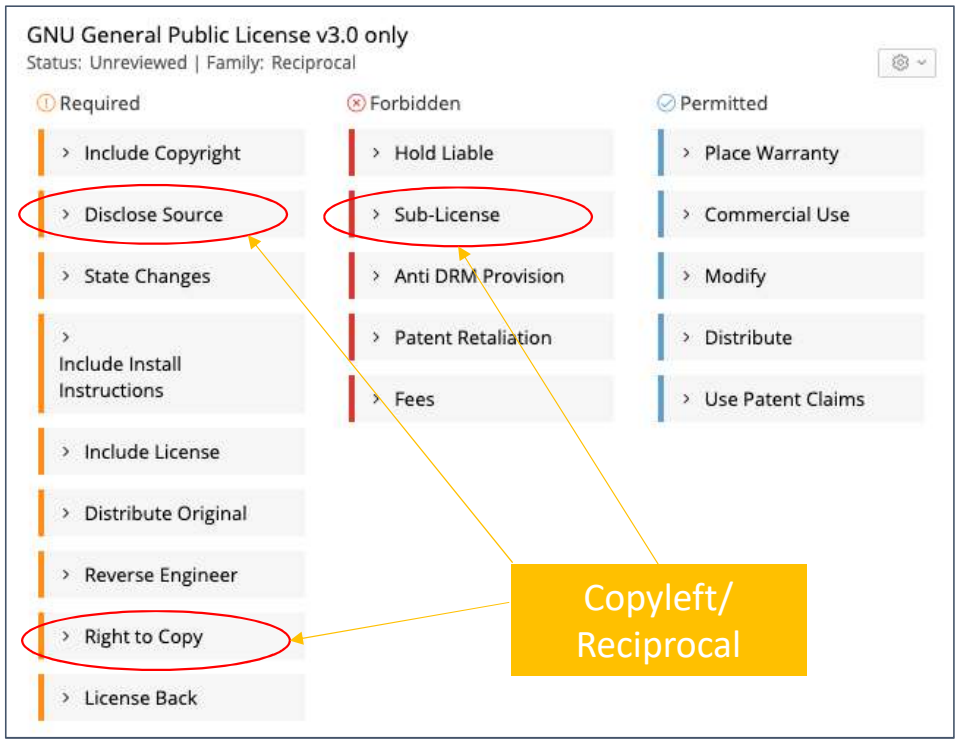
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Gnu GPL v3

OSS LICENSE OBLIGATIONS





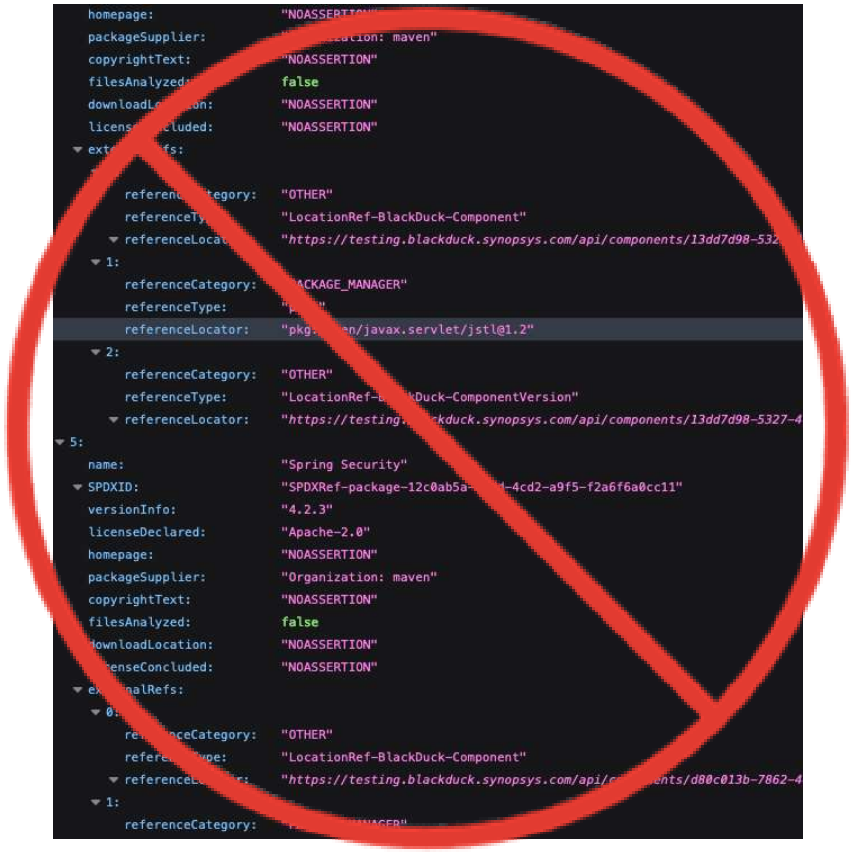
Permissive → Less Permissive

Presentation content source: Synopsys

SBOM TO SOLVE SUPPLY CHAIN RISK

WHAT IS SBOM ALL ABOUT *REALLY*?

A **software Bill of Materials (SBOM)** is a list of all the **open source** and **third-party components** present in a codebase.
An SBOM also **lists the licenses** that govern those components, **the versions** of the components used in the codebase, and **their patch status**, which allows security teams to quickly identify any associated security or license risks

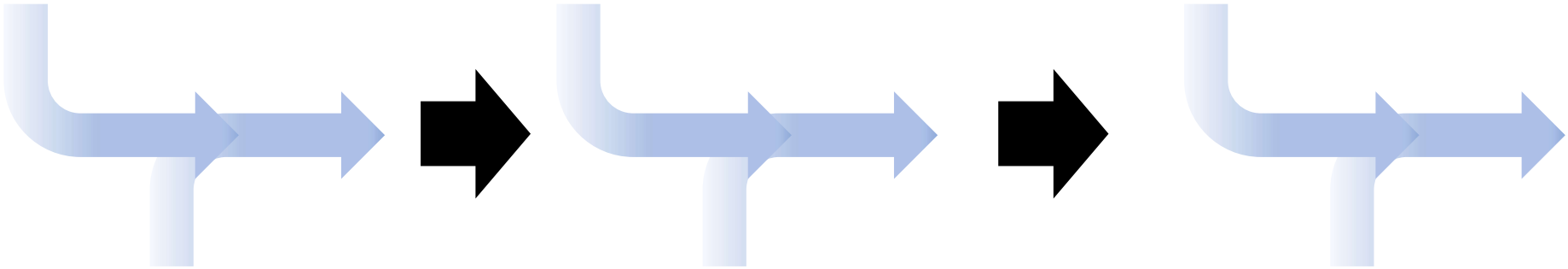


LIFE CYCLE-CENTRIC VIEW

First-Party Code

Compiled Binaries

Complete Firmware



Third-Party Dependencies

Supporting Packages

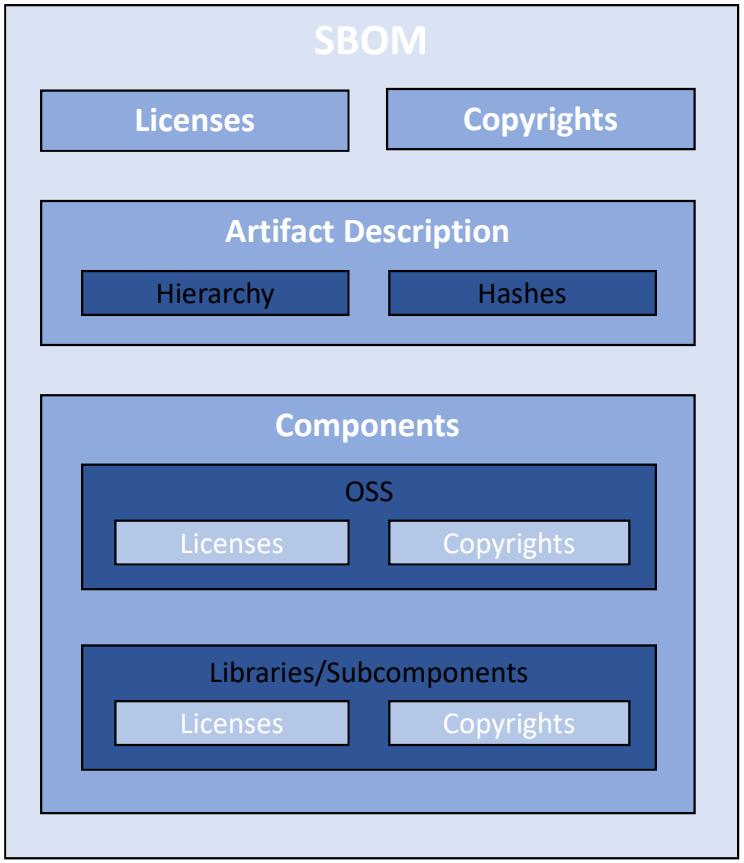
Runtime Environment

Source

Binary

Presentation content source: Synopsys

SBOM STRUCTURE

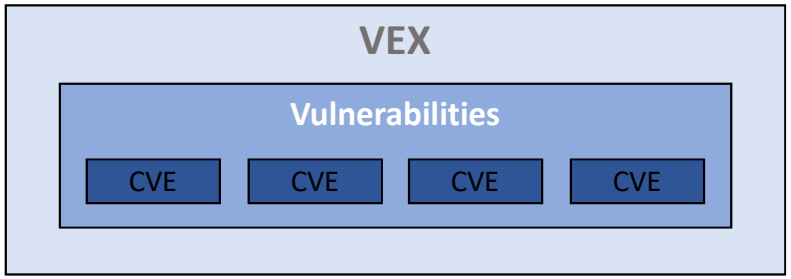


Standards

- SPDX
- CycloneDX
- ~~SWID~~

Formats

- JSON
- RDF
- Tag Value
- XML

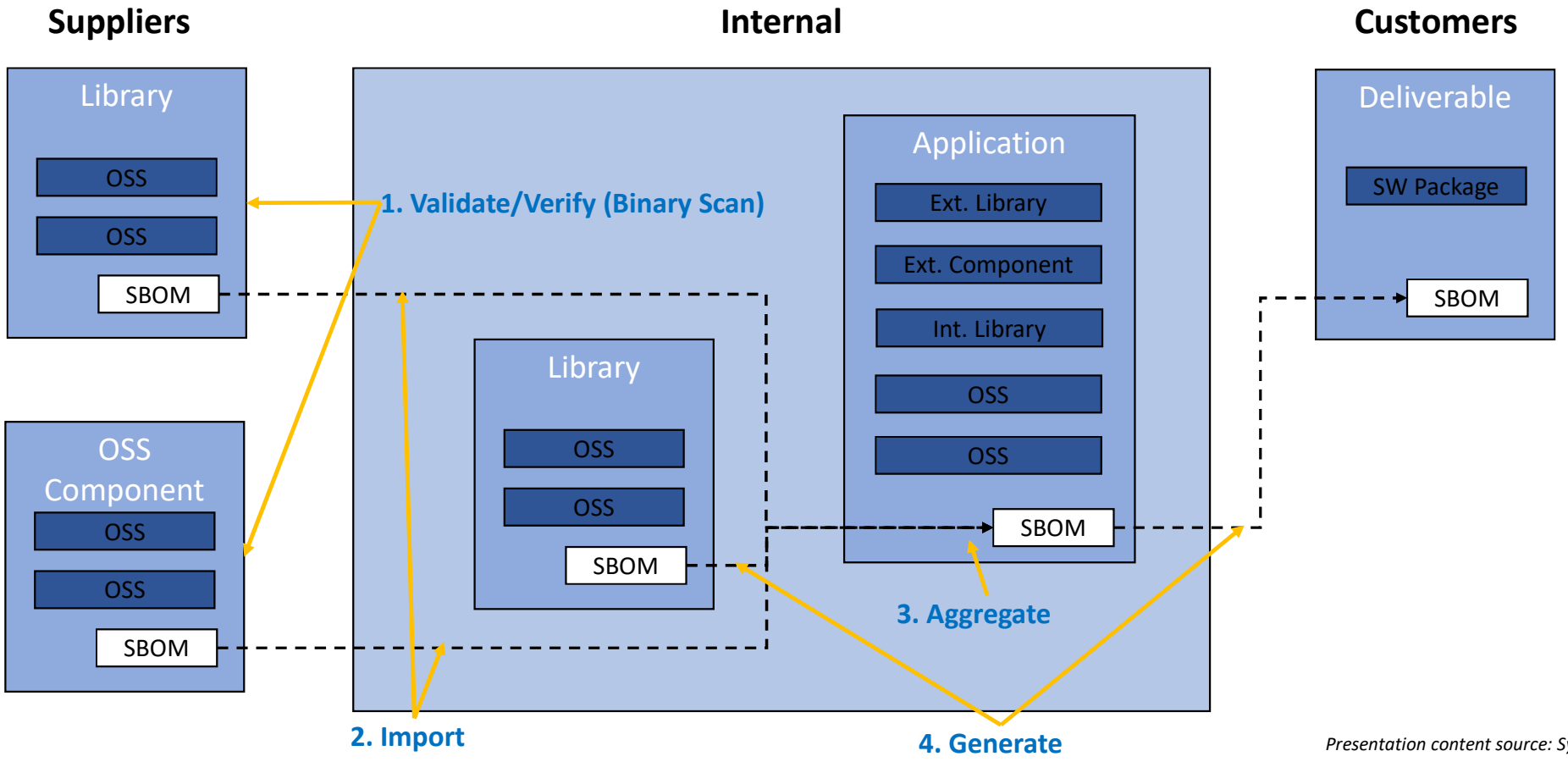


Vulnerability Exchange (VEX)

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

Presentation content source: Synopsys

SBOM WORKFLOW



Presentation content source: Synopsys

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

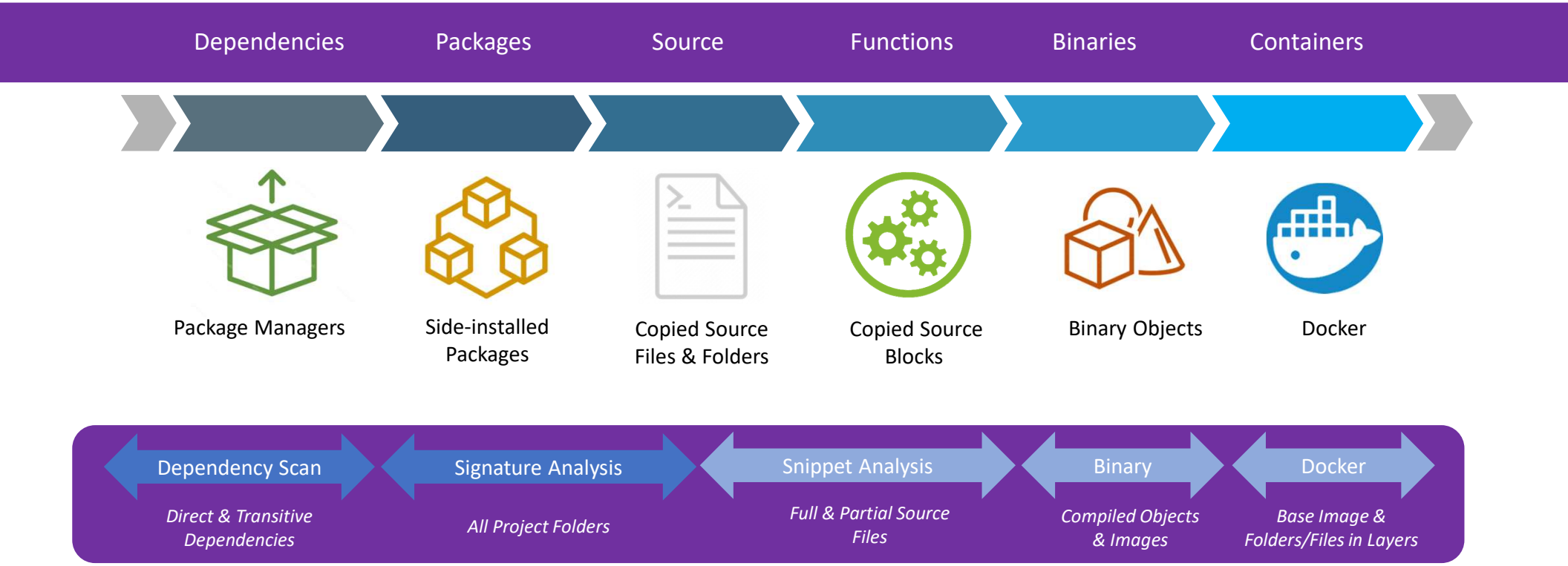
CPE *Wildcards*

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

PURL *Origin Specific - Inconsistent*

- `gem:jruby-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`

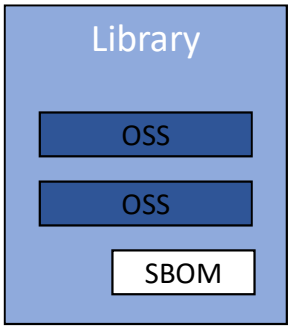
IDENTIFYING OSS AND THIRD-PARTY SOFTWARE



Presentation content source: Synopsys

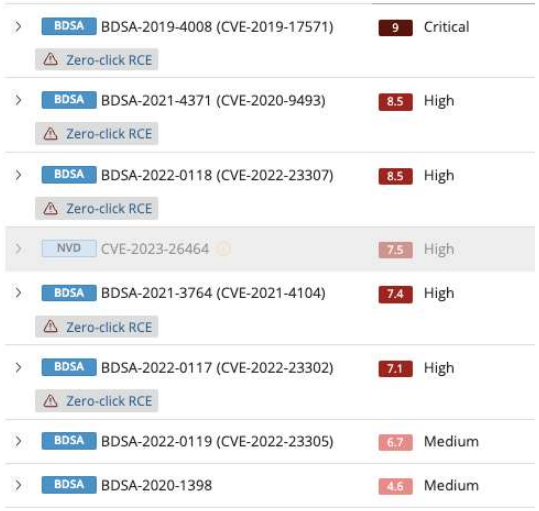
VALIDATION

Suppliers



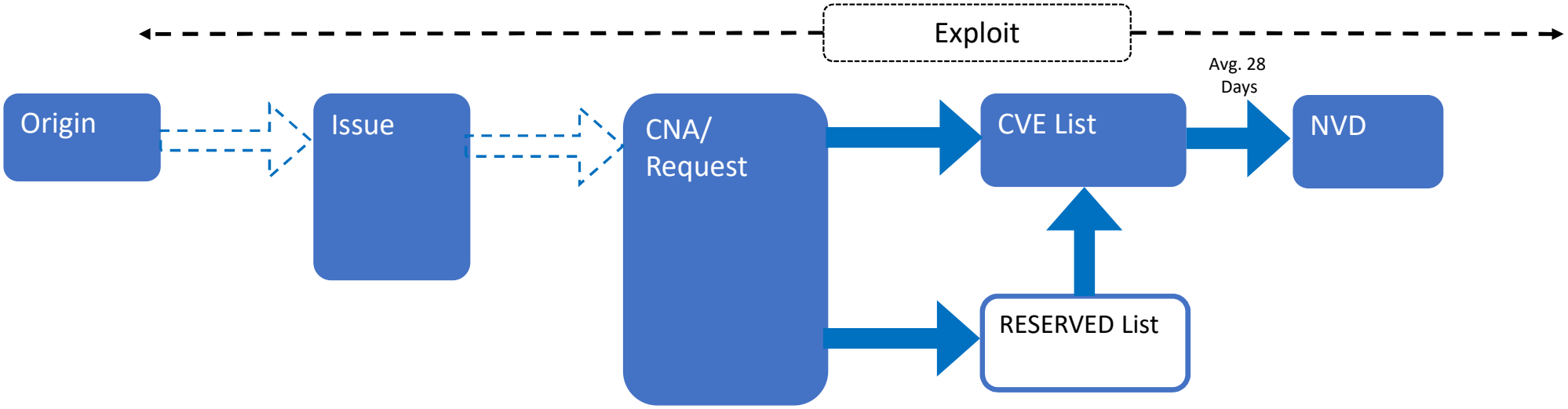
SBOM
Apache Commons Lang 3.6
Apache Commons Logging 1.2
Apache HttpClient 4.4.1
Apache HttpComponents Core 4.4.5
Apache Neethi 3.0.3
Apache POI 3.16

Binary Scan
Apache Commons Lang 3.6
Apache Commons Logging 1.2
Apache HttpClient 4.4.1
Apache HttpComponents Core 4.4.5
Apache Log4j 1.2.15
Apache Log4J API 2.9.1
Apache Neethi 3.0.3
Apache POI 3.16



Presentation content source: Synopsys

PUBLIC SECURITY WORKFLOW



Presentation content source: Synopsys

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

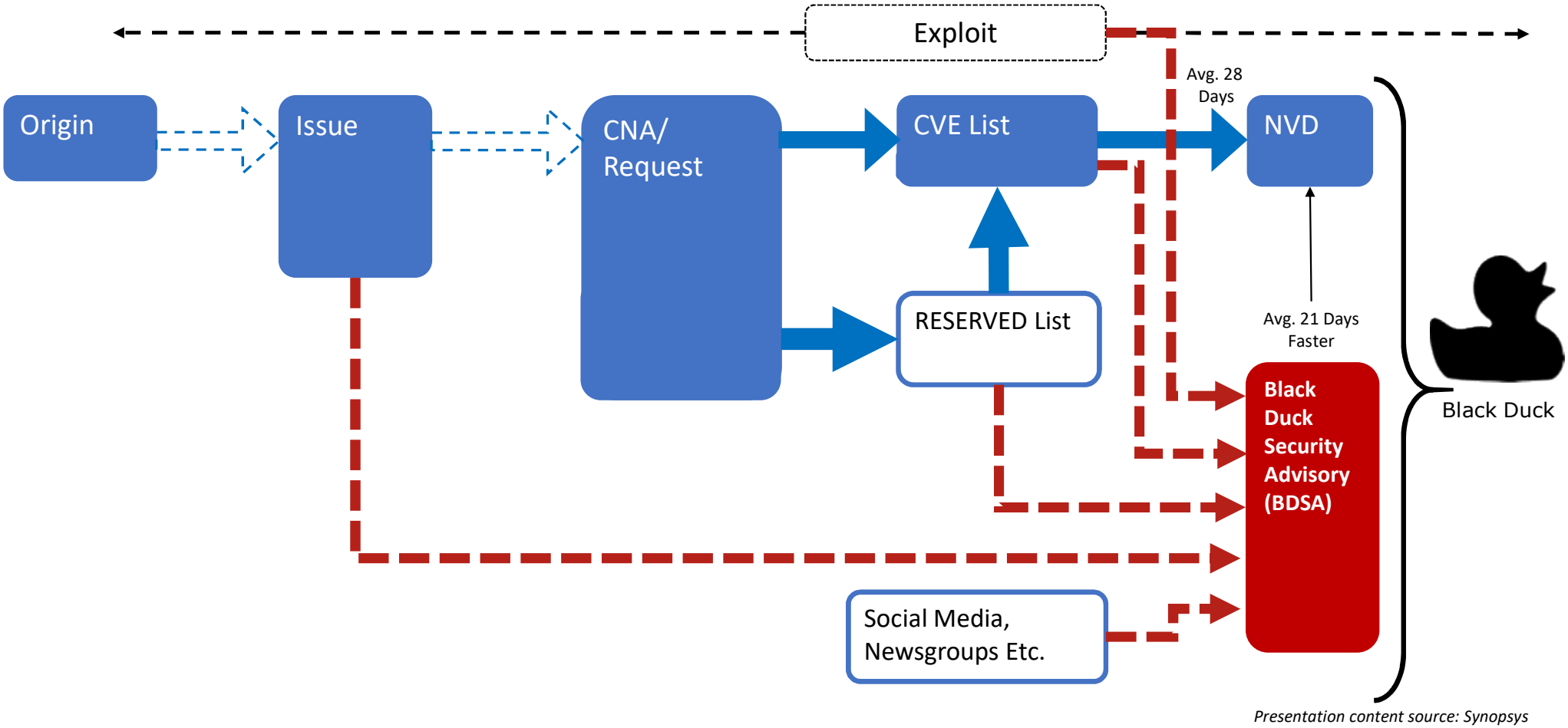
CVE-2019-0232 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

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/).

Presentation content source: Synopsys

ENHANCED SECURITY WORKFLOW WITH BLACKDUCK



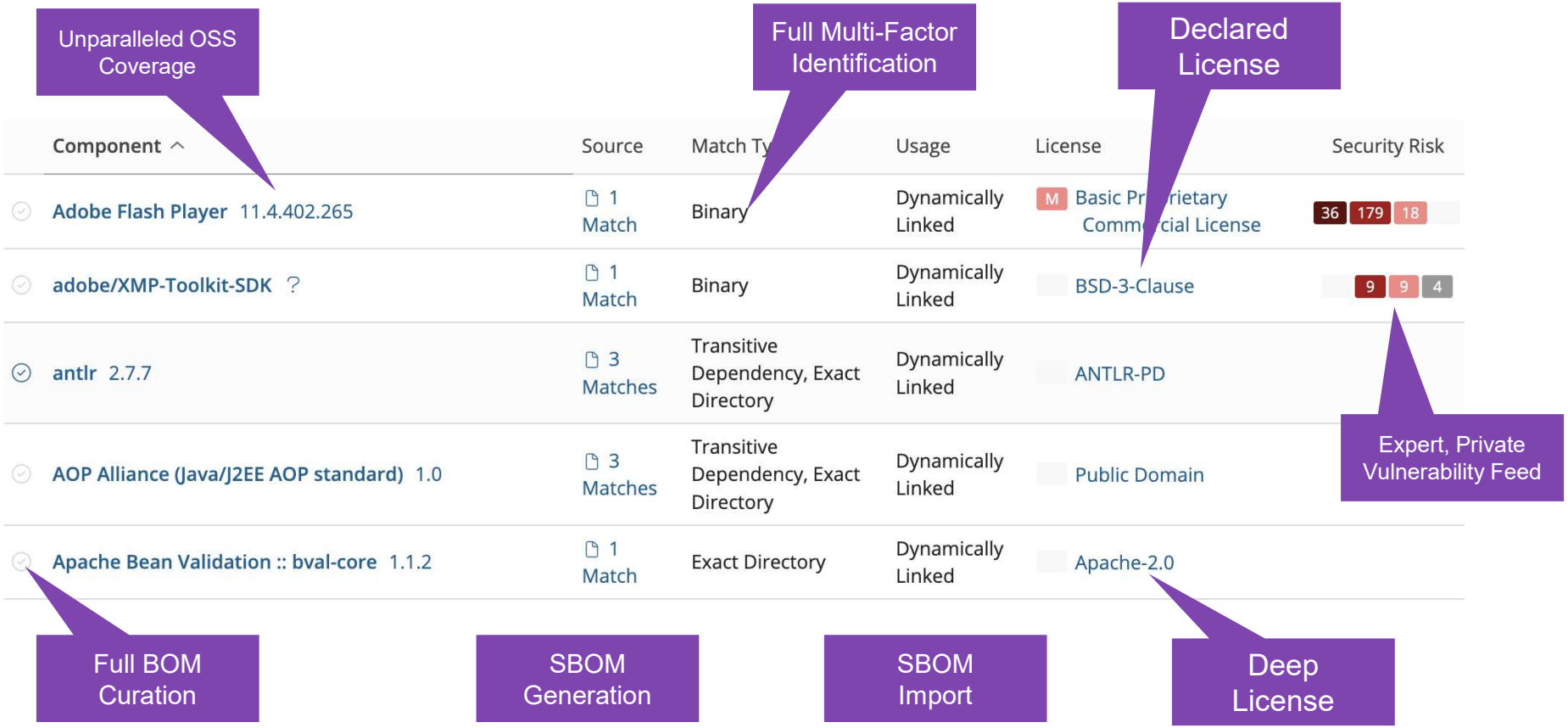
Presentation content source: Synopsys

SCA & SBOM – SUMMARY

Multi-Factor Scanning	Source, Dependencies, Binaries, Snippets etc.
Advanced Vulnerability Data	Public Data Not Reliable
Scalable, Mature SCA Capabilities	Reduce Rework
SBOM	Does not Replace Full AppSec Process Developing Standard Trust but Verify

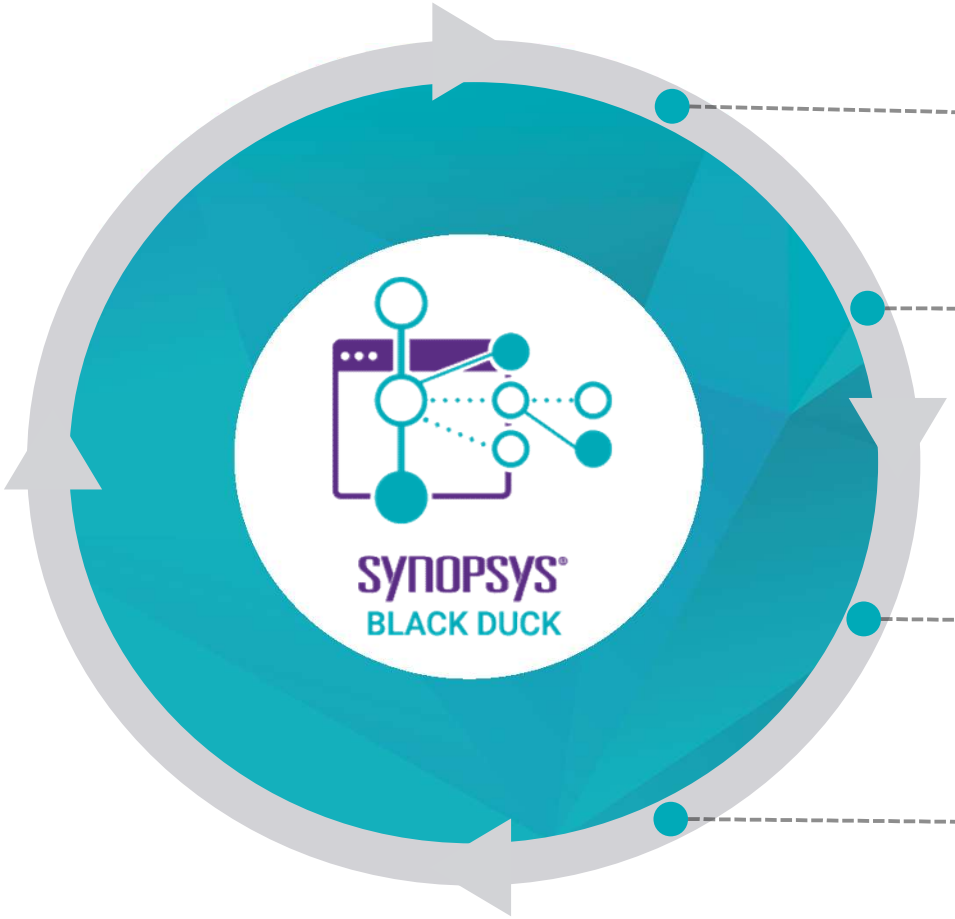
Presentation content source: Synopsys

BLACK DUCK BY SYNOPSYS



Presentation content source: Synopsys

BLACK DUCK BY SYNOPSYS



Detect
Identify and track all open source in apps and containers

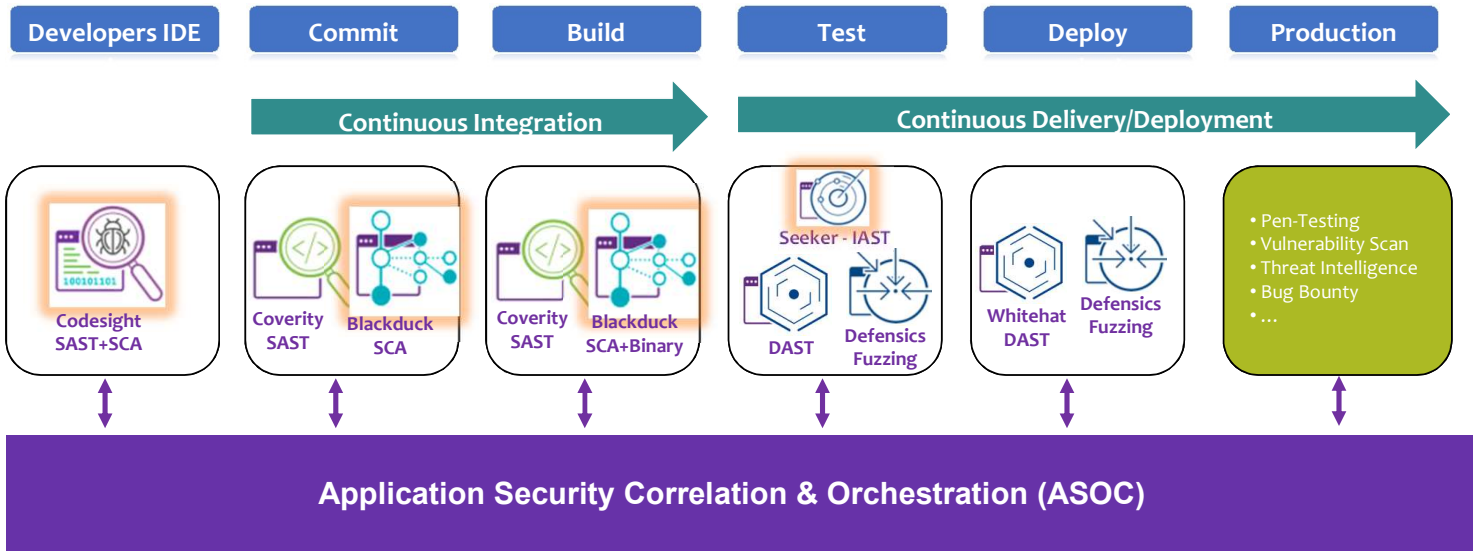
Protect
Find and fix known open-source vulnerabilities in development and production

Comply
Verify and comply with open-source license terms and conditions

Manage
Integrate and automate open source risk policy enforcement end-to-end

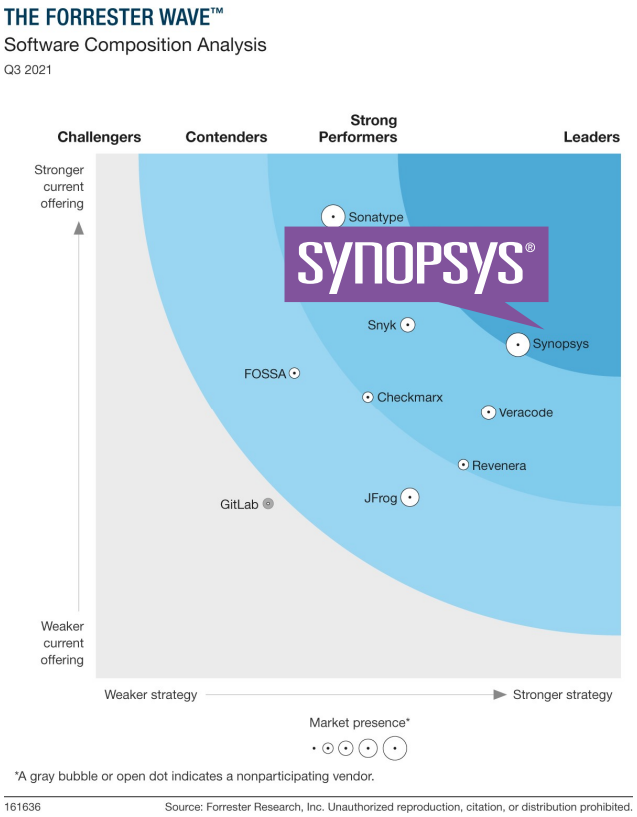
Presentation content source: Synopsys

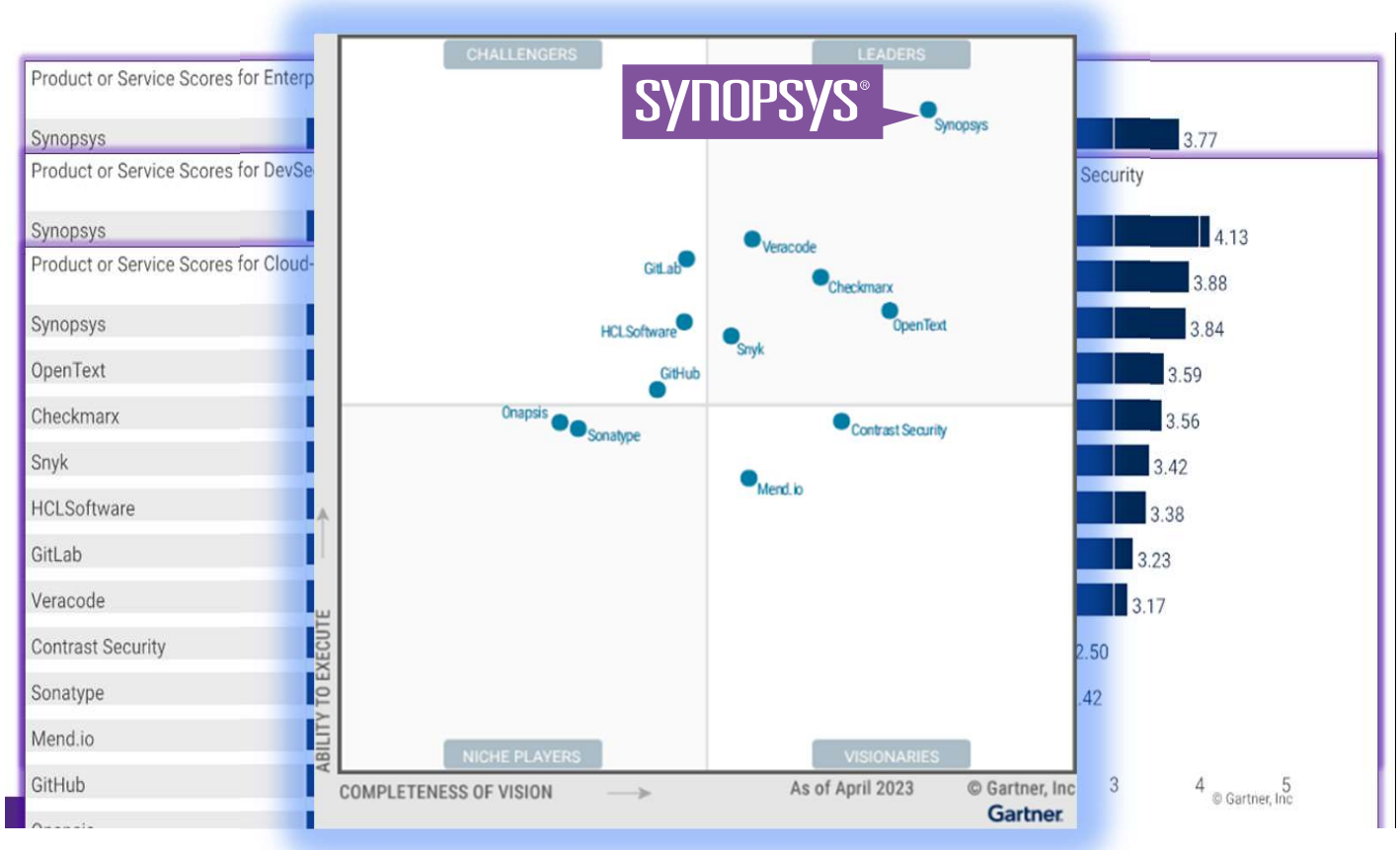
BLACK DUCK IN DEVSECOPS PIPELINE



Presentation content source: Synopsys

BLACK DUCK BY SYNOPSYS





Presentation content source: Synopsys

WITH SYNOPSYS, YOU CAN...

Build a holistic AppSec program

- Align people, processes, and technology
- Understand your AppSec gaps, risks, and objectives
- Ensure you have the skills and resources to succeed

Secure your software supply chain

- Secure and manage OSS dependencies
- Comprehensively test any type of software
- Identify weaknesses in DevOps infrastructure

Build security into DevOps

- Enable developers to build better software
- Maintain velocity while ensuring security
- Focus teams on the issues that matter most

Presentation content source: Synopsys

Thank you

mi2jsc@mi2.com.vn www.mi2.com.vn