SOUTH FLORIDA Tech Hub
SOUTHFLORIDATECHHUB.ORG

· SOFLO DEVCON 2024

Miami JVM Group

Software Composition Analysis

EUGENIO ALVAREZ

A South Florida software engineering professional. Experienced in organizational design, software design, construction, and deployment. Extensive knowledge of Java. Proponent of Unit testing. An advocate for Agile Software Engineering methods using Kanban and Scrum.

www.linkedin.com/in/ealvarez

INTRODUCTION

- Market forces are driving companies to accelerate the development of secure software to gain a competitive advantage and avoid costly security breaches.
- The software development community has found that Software Component Analysis tooling can improve the competitive need for increased security and speed.
- Software Composition Analysis tooling provides an efficient way to reduce security threats from open-source software components.

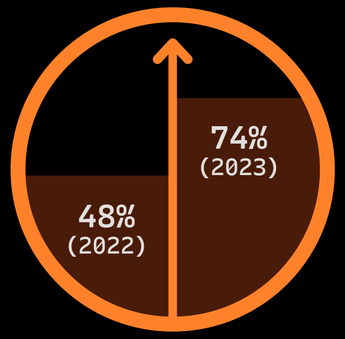
WE WILL DISCUSS

- The need for SCA to manage open source.
- How do CVEs and SBOMs relate to SCA?
- SCA tooling as part of a secure coding practice.
- The Cybersecurity landscape that is requiring SCA.
- The need for software license management with SCA.
- Third-party risk management (TPRM) and SCA.

OPEN SOURCE EXPOSURE

96%

of the total codebases **contained** open source



54% increase in codebases containing **high-risk vulnerabilities** in the past year

84%

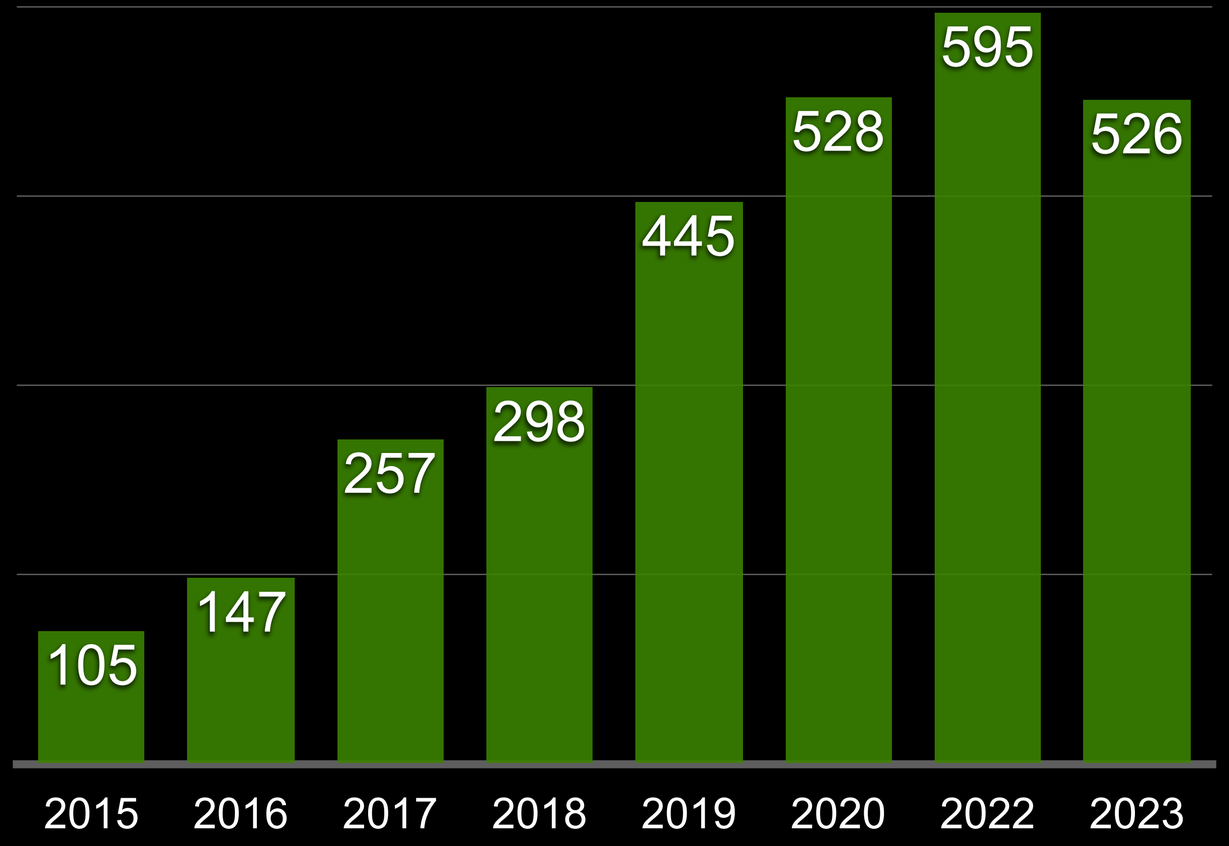
of codebases assessed for risk contained vulnerabilities

74%

of codebases assessed for risk contained high-risk vulnerabilities

Source: Synopsys Open Source Security and Risk Report 2024

OPEN SOURCE COMPONENTS
PER APPLICATION (2016-2024)



Source: Meta-analysis from Synopsys BlackDuck Open Source Security and Risk Reports 2016-2024

WHY SO MANY OPEN SOURCE COMPONENTS

AVERAGE OF 526

Source: Synopsys BlackDuck Open Source Security and Risk Reports 2024

AVERAGE OF 148
FOR JAVA APPLICATIONS

(EST. 90% OF THAT IS OPEN SOURCE)

Source: Sonatype 9th Annual State of the Software Supply Chain Report, Nov 2023

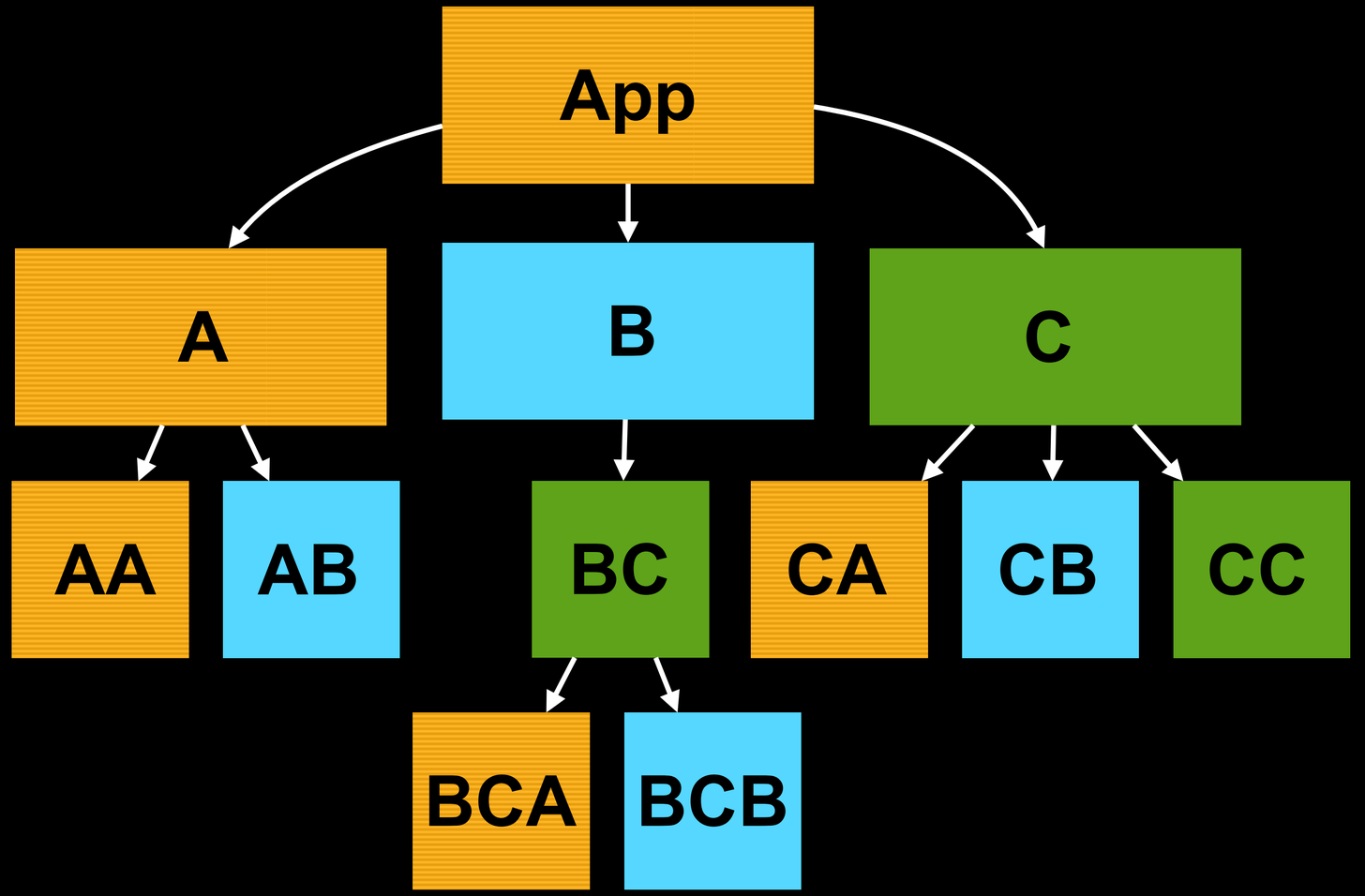
MEDIAN OF 683
FOR JAVASCRIPT APPLICATIONS

(FROM A MEDIAN OF 10 DIRECT)

Source: GitHub Octoverse Report, Dec 2020

TRANSITIVE DEPENDENCIES

“Do you realize how many dependencies?”



“INVINCIBILITY LIES IN THE DEFENCE”

TZU, SUN. *THE ART OF WAR*

“THUS, WHAT IS OF SUPREME IMPORTANCE IN WAR IS TO ATTACK THE ENEMY’S STRATEGY.”

TZU, SUN. *THE ART OF WAR*

孫子

SECURE CODING DOJO

- SAST: Static Application Security Testing
- DAST: Dynamic Application Security Testing
- SCA: Software Composition Analysis

SCA TOOLS IN ACTION

- Identify open-source components
- Identify security issues in open-source components
- Identify license issues in open-source components
- Notify and mitigate open-source issues
- Manage open-source quality

SOFTWARE COMPOSITION ANALYSIS COMBINED WITH STATIC APPLICATION SCAN

- Some SCA tools use SAST to confirm that code is vulnerable
- Be careful with false negatives
- Dynamic code can only be detected with runtime analysis

JUST A SIMPLE UPDATE?

- H2 database
- JUnit4 vs JUnit5
- Spring Framework
- Angular JS
- Apache Struts

MAYBE OR MAYBE NOT

CVE
(COMMON VULNERABILITIES AND EXPOSURES)

- Publicly released list of known cybersecurity vulnerabilities
  - Issued by vendors and researchers
  - Each CVE has an identification number “identifier”
  - A CVE does not include technical data
  - Databases of public disclosed CVEs (multiple)
    - NVD (National Vulnerabilities Database) USA

Source: https://www.cve.org/

SBOM FORMATS (SOFTWARE BILL OF MATERIALS)

CycloneDX

Open source machine-readable by OWASP

SPDX® (Software Package Data Exchange)

Open standard ISO/IEC 5692:2021 by Linux Foundation

Source: https://cyclonedx.org/
Source: https://spdx.dev/

EXAMPLE SBOM?

SPDX Example of an SBOM

```
SPDXVersion: SPDX-2.1
DataLicense: CC0-1.0
DocumentNamespace: http://www.spdx.org/spdxdocs/8f141b09-1138-4fc5-aecb-
fc10d9ac1eed
DocumentName: SpdxDoc for GNU Time
SPDXID: SPDXRef-DOCUMENT

## Creation Information
Creator: Person: Gary O'Neall
Creator: Tool: Source Auditor Open Source Scanner
Created: 2018-08-17T11:29:46Z
## Relationships
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-1

## Package Information
PackageName: GNU Time
PackageVersion: 1.9
PackageSupplier: Organization: GNU
PackageOriginator: Organization: GNU
PackageDownloadLocation: https://ftp.gnu.org/gnu/time/t
PackageChecksum: SHA1: 75868c26abbed3ad3980685bae21d7202d288317
PackageHomePage: https://www.gnu.org/software/time/
PackageLicenseConcluded: (GFDL-1.3 AND GPL-3.0-or-later AND LicenseRef-1)
## License information from files
PackageLicenseInfoFromFiles: X11
PackageLicenseInfoFromFiles: GPL-2.0-or-later WITH Libtool-exception
PackageLicenseInfoFromFiles: GPL-3.0-or-later
PackageLicenseInfoFromFiles: LicenseRef-1
PackageLicenseInfoFromFiles: GFDL-1.3
PackageLicenseDeclared: GPL-3.0-or-later
PackageLicenseComments: <text>Several files contained a GPL 2.0 or later
license.  Since they were linked to a GPL 3.0
text>
PackageCopyrightText: <text>Copyright (C) 19
Inc.</text>
PackageSummary: <text>The 'time' command runs another program, then displays
information about the resources used by that program.</text>
PackageDescription: <text>The 'time' command runs another program, then
displays information about the resources used by that program.</text>

## File Information
FileName: ./tests/help-version.sh
SPDXID: SPDXRef-164
FileType: SOURCE
FileChecksum: SHA1: 30b3973b22ddbcd9e8982a06c5a2440fcb315013
LicenseConcluded: GPL-3.0-or-later
LicenseInfoInFile: GPL-3.0
LicenseComments: Seen licenses generated by Source Auditor Scanner.  Results
should be manually verified.
FileCopyrightText: <text>Copyright Free Software Foundation, Inc</text>
FileNotice: <text>NOASSERTION</text>
```

SBOM Data Author

Timestamp Info

Depend. Relationship

Component Name

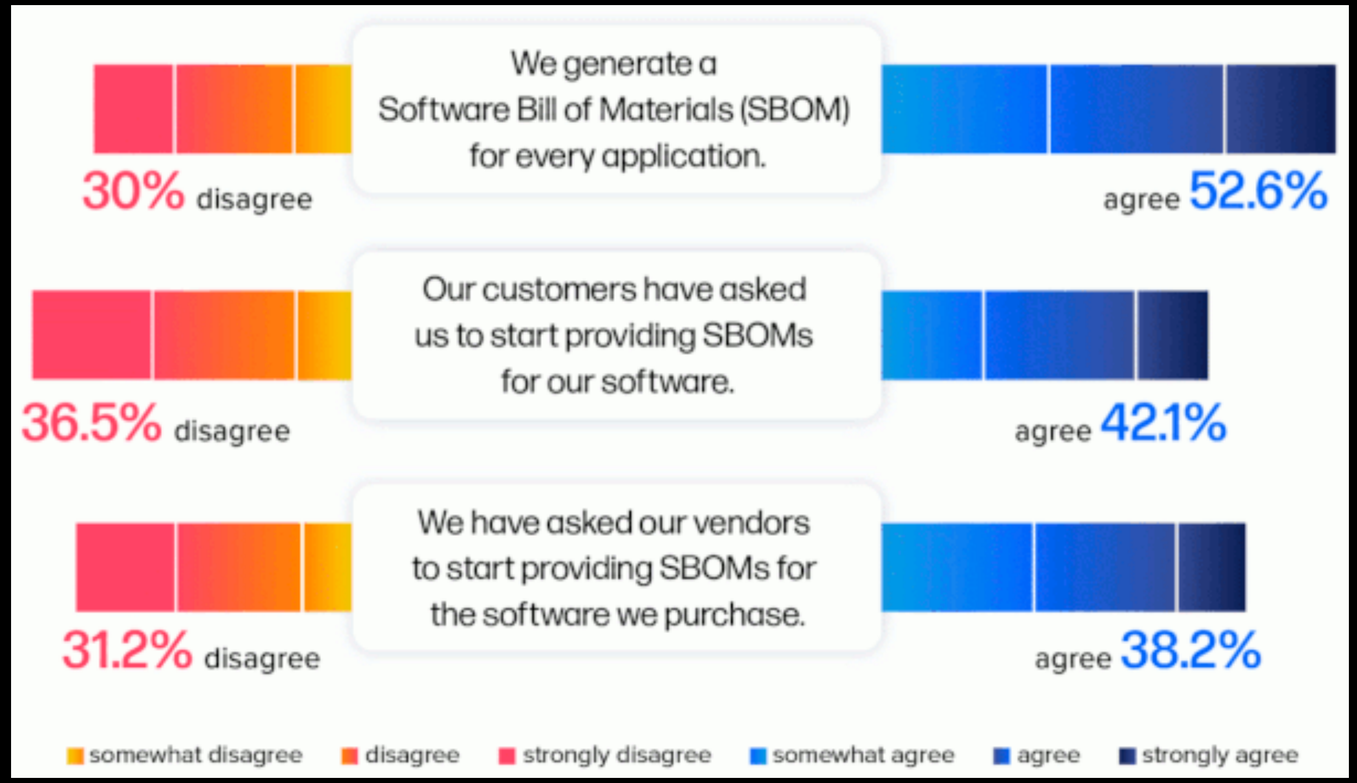
Component Version

Component Supplier

Unique Identifying Information

Source: https://www.thesslstore.com/blog/sbom-an-up-close-look-at-a-software-bill-of-materials/

SBOM USAGE SURVEY SAYS



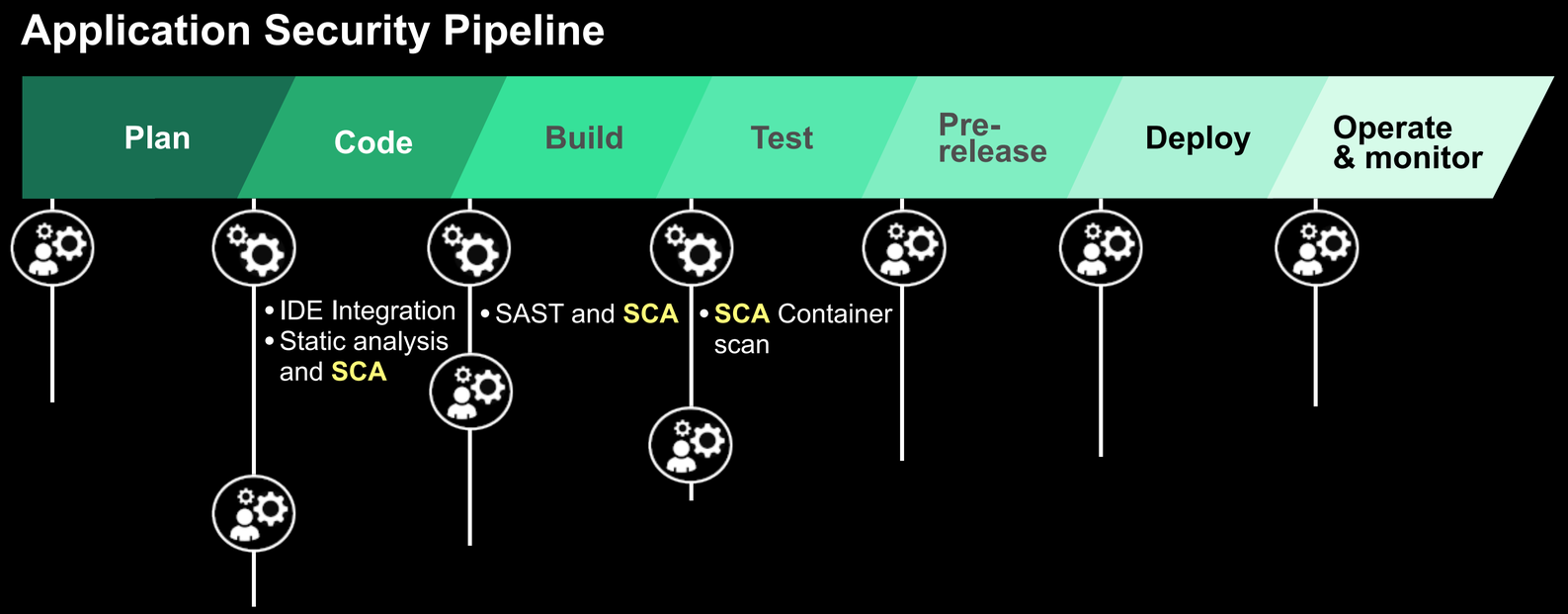
Source: Sonatype 9th Annual State of the Software Supply Chain Report, Nov 2023

SBOM ADOPTION DRIVERS

- Presidential Executive order 14028 (Cybersecurity)
  - An SBOM as part of Secure Development
- Regulatory Compliance
- Risk management via CI/CD supply chain monitoring
- Customer Assurance

Source: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

WHERE IS SCA IN BUILD PIPELINE



Source: https://vulcan.io/blog/ci-cd-security-5-best-practices/

OPEN SOURCE LICENSE IDENTIFICATION AND MANAGEMENT

- MIT License
- Apache License 2.0
- BSD License variants
- Mozilla Public License 2.0
- Public Domain
- GNU Lesser (As long as the code is unmodified)

- GNU GPL (License conflict)

Source: https://www.gnu.org/licenses/gpl-3.0.en.html

WHY GPL CAUSES A CONFLICT

- Copyleft Requirement: Any derivative work created from a GPL licensed code must be distributed under the GPL which includes the source code of the entire derivative work.
- Examples:
  - Linksys/Cisco WRT54G
  - Samsung Smart TVs

Source: https://www.fsf.org/news/2008-12-cisco-suit

OPEN SOURCE VERSION MANAGEMENT

of the codebases assessed for risk contained components that were
10 versions or more behind the most current version of the component

Source: Synopsys Open Source Security and Risk Report, Feb 2024

of the component downloads with known vulnerabilities could be avoided as a better, fixed version is already available

Source: Sonatype 9th Annual State of the Software Supply Chain Report, Nov 2023

- SCA Tools recommend the latest version

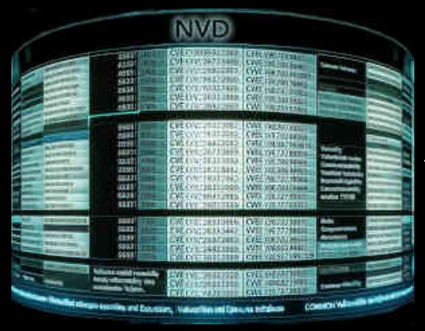
OPEN SOURCE QUALITY MANAGEMENT

“The fact that 18.6% of [open source] projects stopped being maintained in the last year highlights the need to not only choose good dependencies, but monitor those dependencies for changes in their quality.” *

Source: Sonatype 9th Annual State of the Software Supply Chain Report, Nov 2023

* maintained as defined by the OpenSSF (Open Source Security Foundation) scorecard

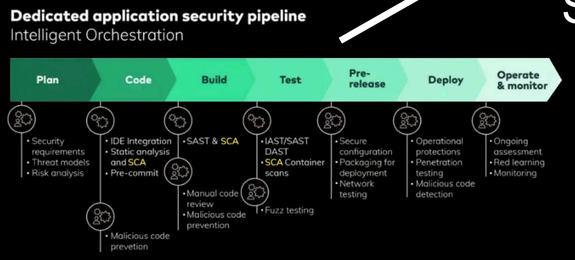
CONTINUOUS MONITORING AND NOTIFICATION



NVD et al.

24/7 Monitoring

SBOM



Pipeline

Email

Text

Microsoft Teams

SCA SCAN FOR VENDOR SOFTWARE

Source: DALL·E

SBOM FOR VENDOR SOFTWARE RECOMMENDED

THIRD-PARTY RISK MANAGEMENT (TPRM)

“98% of organizations have a relationship with a third party that has been breached.”

Source: SecurityScoreCard Global Third-Party Cybersecurity Breaches Report, Feb 2024

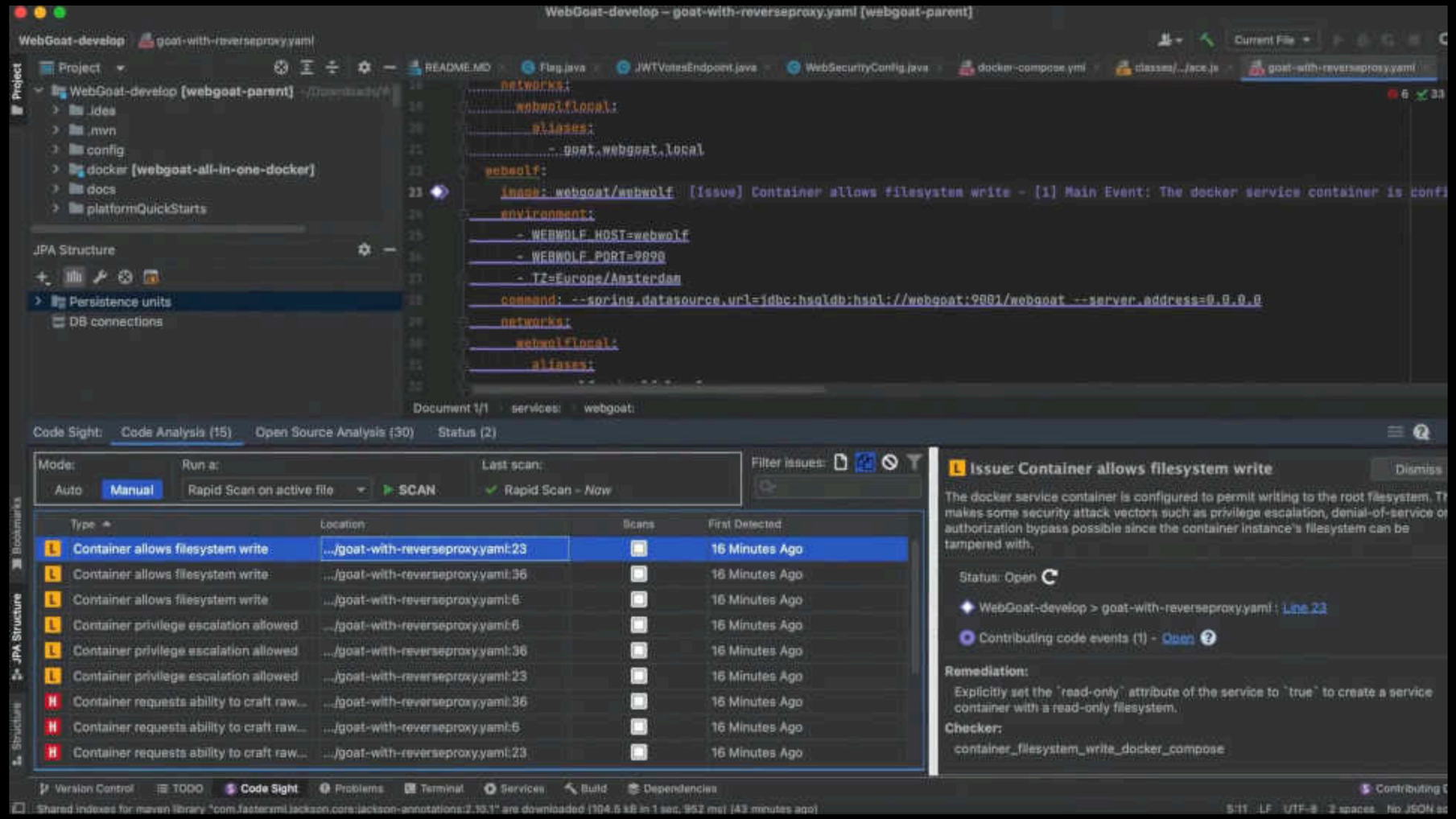
Third-party breaches by industry:
43% Technology & Telecommunications
30% Financial Services
29% Overall cross-industry rate

Source: SecurityScoreCard Global Third-Party Cybersecurity Breaches Report, Feb 2024

- Stop depending on a questionnaires for TPRM
- Vendor SBOMs can be monitored 24/7 by SCA Tooling

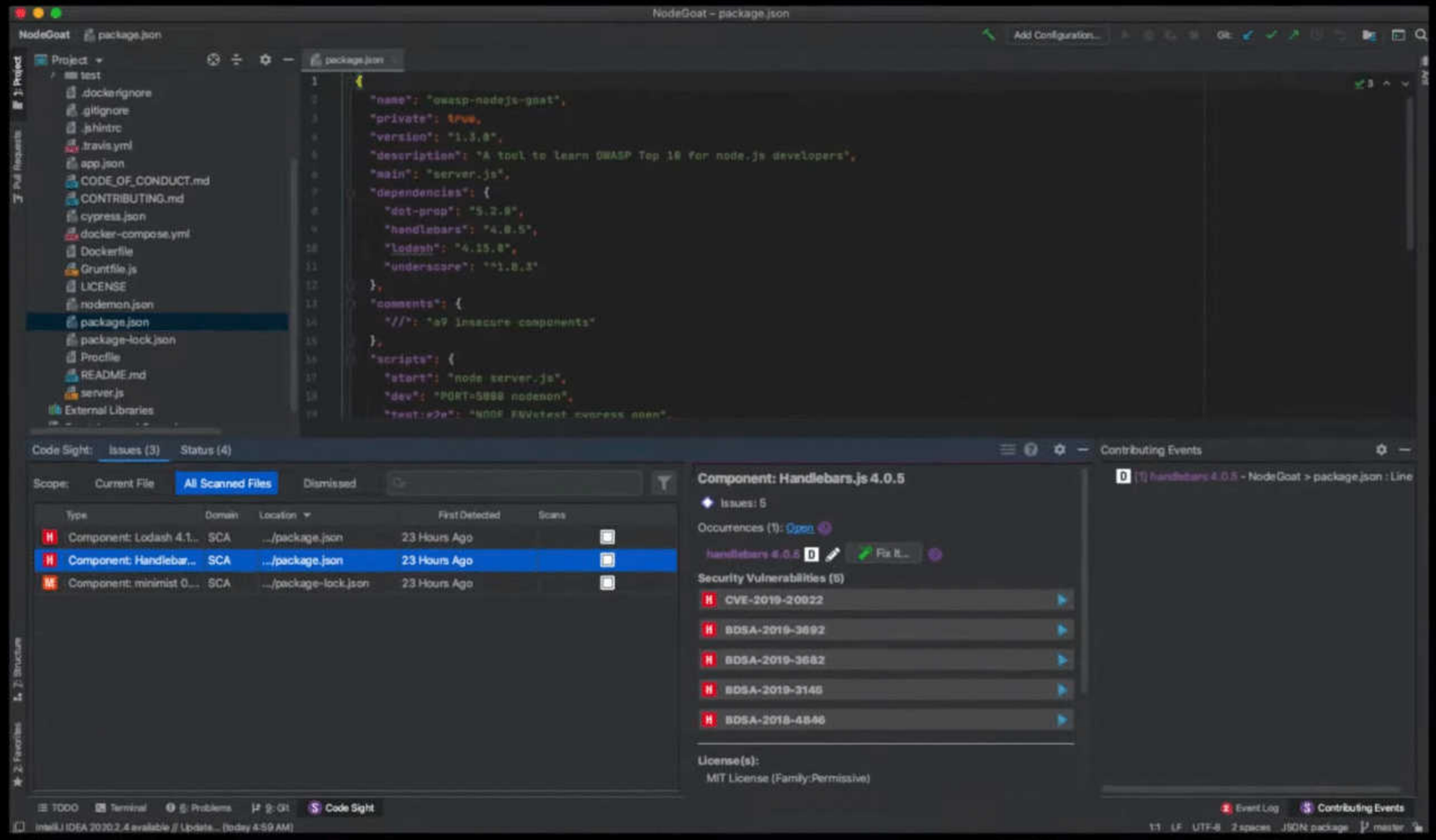
SCA TOOLS

SCA IDE PLUGINS



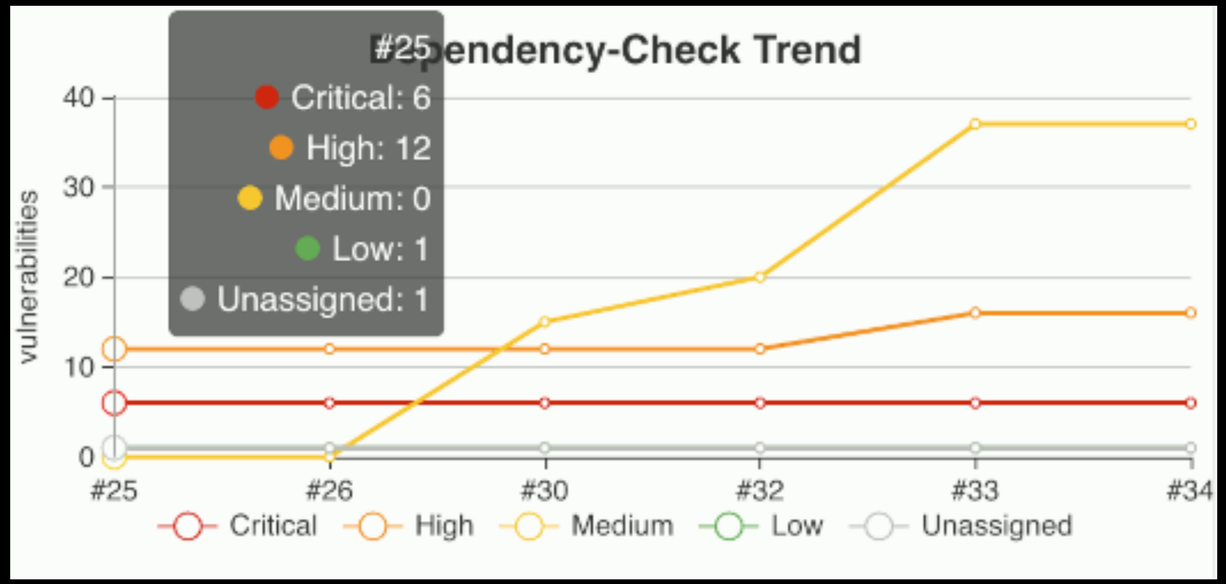
Source: https://youtu.be/6cxi96CJB14

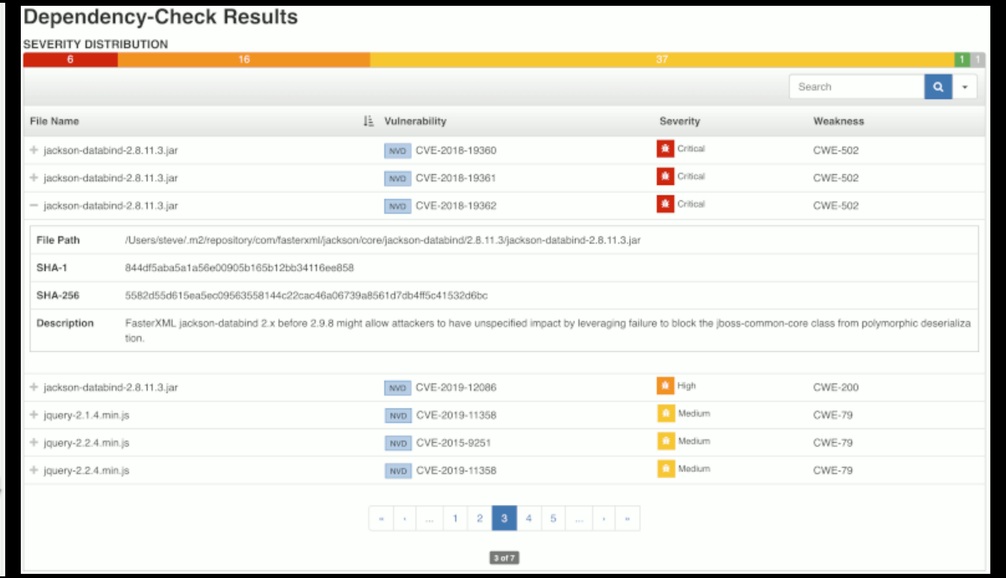
SCA IDE PLUGINS



Source: https://youtu.be/W9BHyXYw3vQ

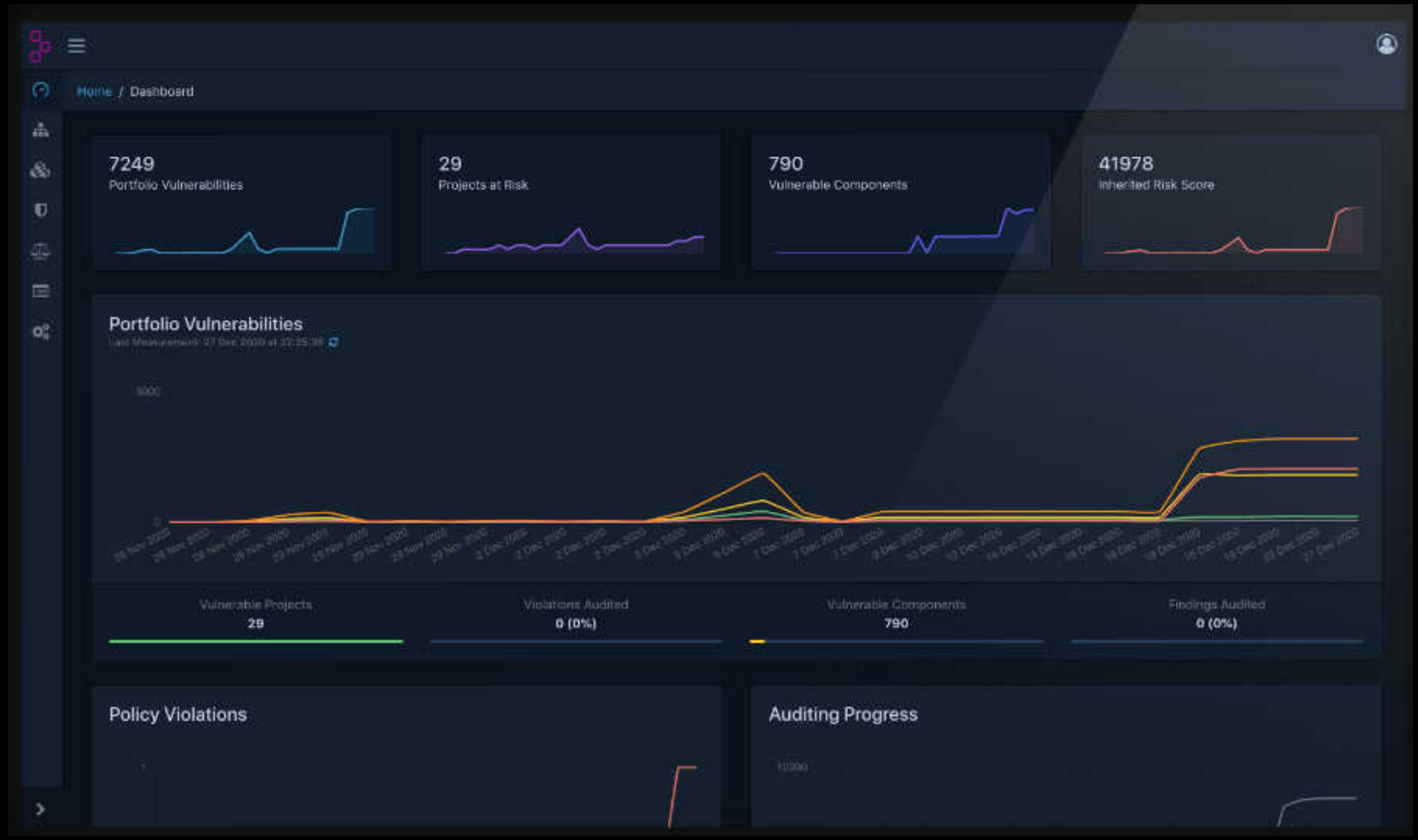
DEPENDENCY CHECK





Source: https://plugins.jenkins.io/dependency-check-jenkins-plugin/

DEPENDENCY TRACK



Source: https://www.dependencytrack.org/

Eugenio Alvarez

Thank You

www.linkedin.com/in/ealvarez

REFERENCES

- Synopsys 2024 Open Source Security and Risk Analysis Report (OSSRA)
- https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/rep-ossra-2024.pdf

- Sonatype 2023 9th Annual State of the Software Supply Chain Report
- https://www.sonatype.com/hubfs/2023 Sonatype- 9th Annual State of the Software Supply Chain- Update.pdf

- GitHub Octoverse Report 2020
- https://octoverse.github.com/2020/

- The Art of War: Sun Tzu
- https://www.amazon.com/Art-War-Sun-Tzu/dp/1599869772

- CVE (Common Vulnerabilities and Exposures)
- https://www.cve.org

- OWASP CycloneDX Software Bill of Materials (SBOM) Standard
- https://cyclonedx.org/

REFERENCES

- System Package Data Exchange (SPDX®) (SBOM) Standard
- https://spdx.dev/

- SBOM: An Up-Close Look at a Software Bill of Materials
- https://www.thesslstore.com/blog/sbom-an-up-close-look-at-a-software-bill-of-materials/

- Executive order 14028 (Cybersecurity)
- https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

- CI/CD security - 5 best practices
- https://vulcan.io/blog/ci-cd-security-5-best-practices/

- GNU General Public License
- https://www.gnu.org/licenses/gpl-3.0.en.html

- GPL Violation law suit
- https://www.fsf.org/news/2008-12-cisco-suit

REFERENCES

- SecurityScoreCard Global Third-Party Cybersecurity Breaches Report, Feb 2024
- https://securityscorecard.com/wp-content/uploads/2024/02/Global-Third-Party-Cybersecurity-Breaches-Final-1.pdf

- Code Sight IDE Plugin for Application Security Testing | Synopsys
- https://youtu.be/6cxi96CJB14

- Secure and manage open source risks in applications and contains with Black Duck SCA
- https://youtu.be/W9BHyXYw3vQ

- OWASP Dependency Check
- https://owasp.org/www-project-dependency-check/
- https://plugins.jenkins.io/dependency-check-jenkins-plugin/

- OWASP Dependency Track
- https://owasp.org/www-project-dependency-track/
- https://www.dependencytrack.org/