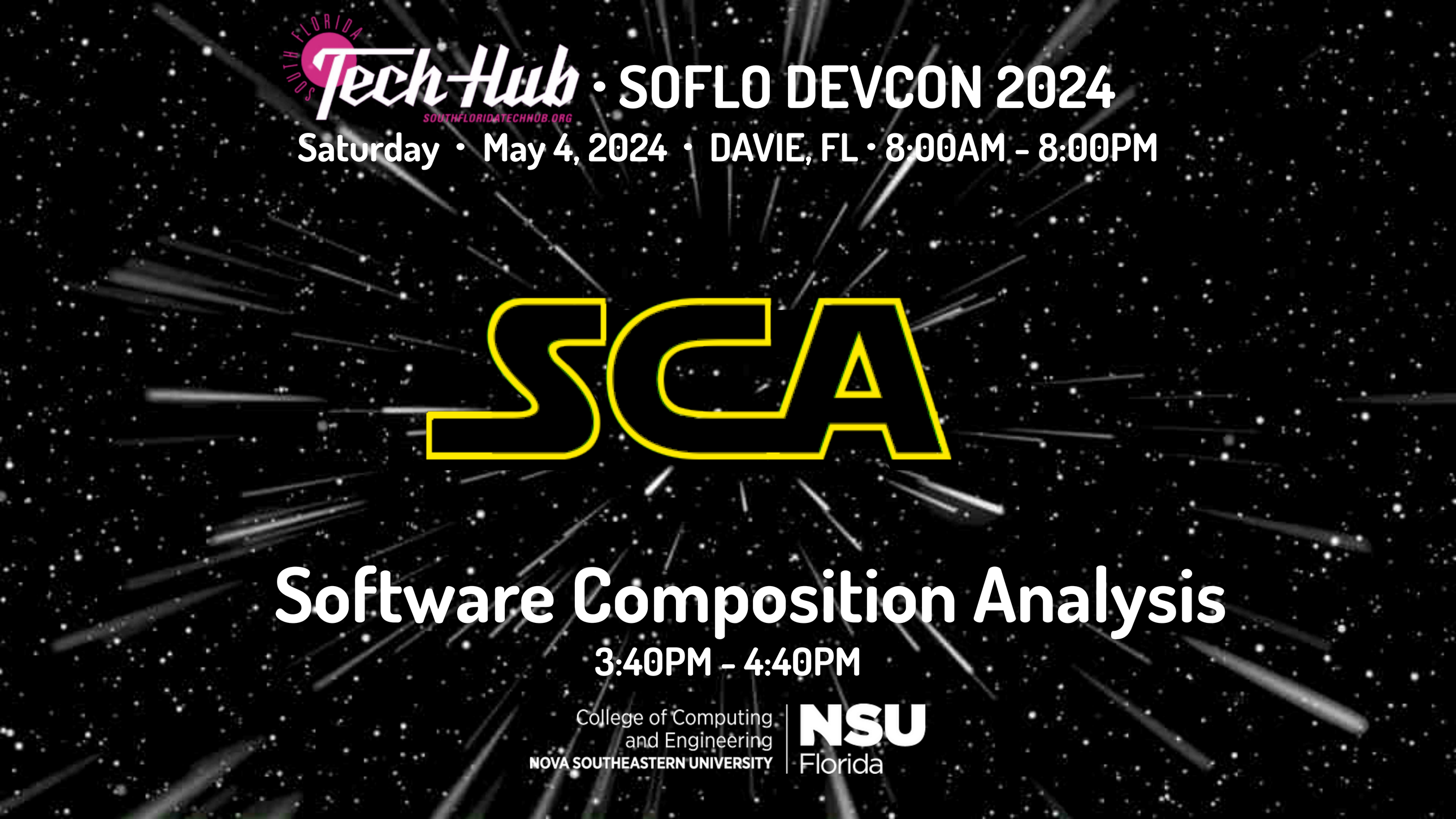

SOUTH FLORIDA
TechHub
SOUTHFLORIDATECHHUB.ORG
· SOFLO DEVCON 2024
Saturday · May 4, 2024 · DAVIE, FL · 8:00AM – 8:00PM
SCA
Software Composition Analysis
3:40PM – 4:40PM
College of Computing and Engineering
NOVA SOUTHEASTERN UNIVERSITY
NSU Florida

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

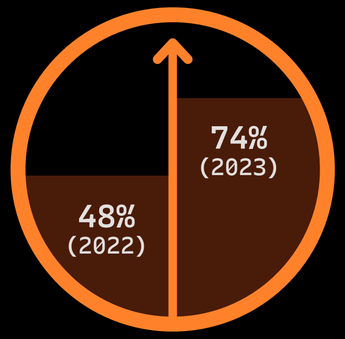
INTRODUCTION

- Market forces are driving companies to develop secure software faster to gain a competitive advantage.
- 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.

OPEN SOURCE EXPOSURE

96%

of the total codebases **contained** open source



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

84%

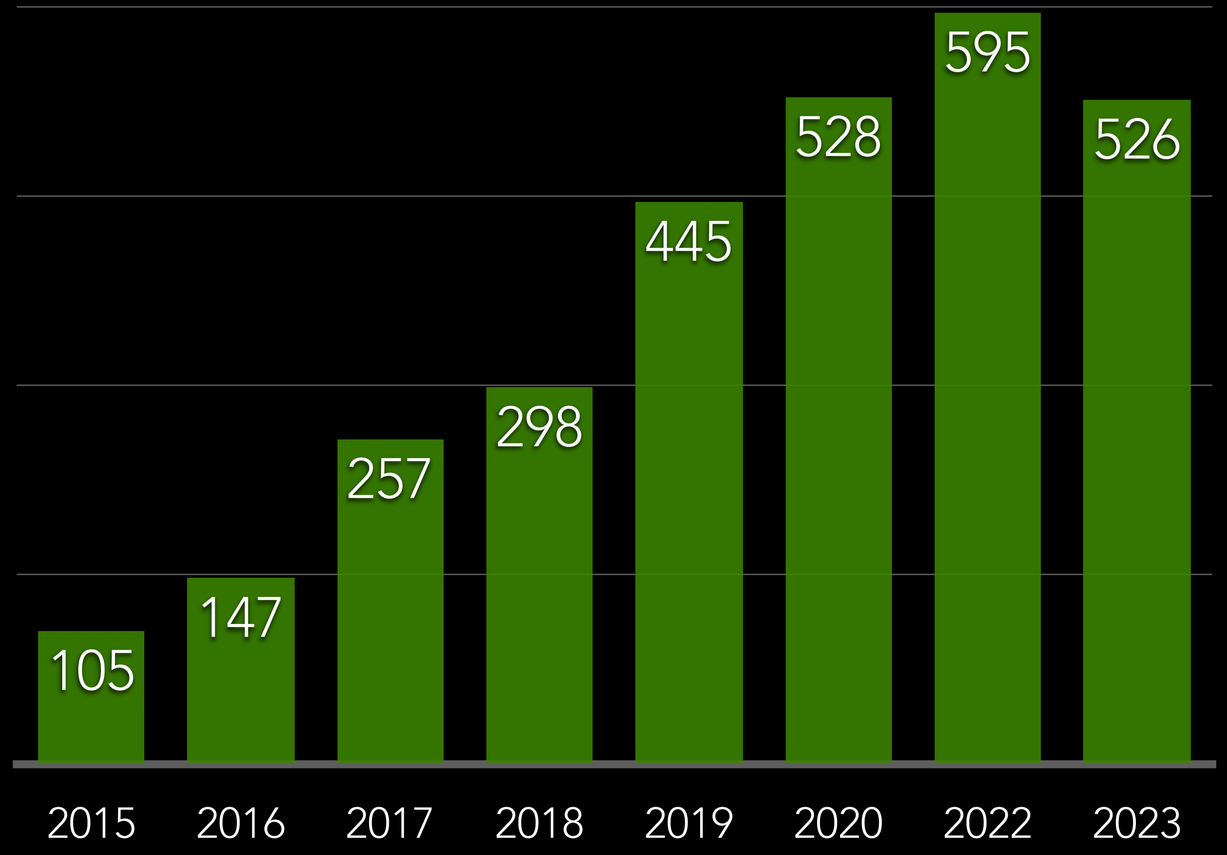
of codebases assessed for risk contained vulnerabilities

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

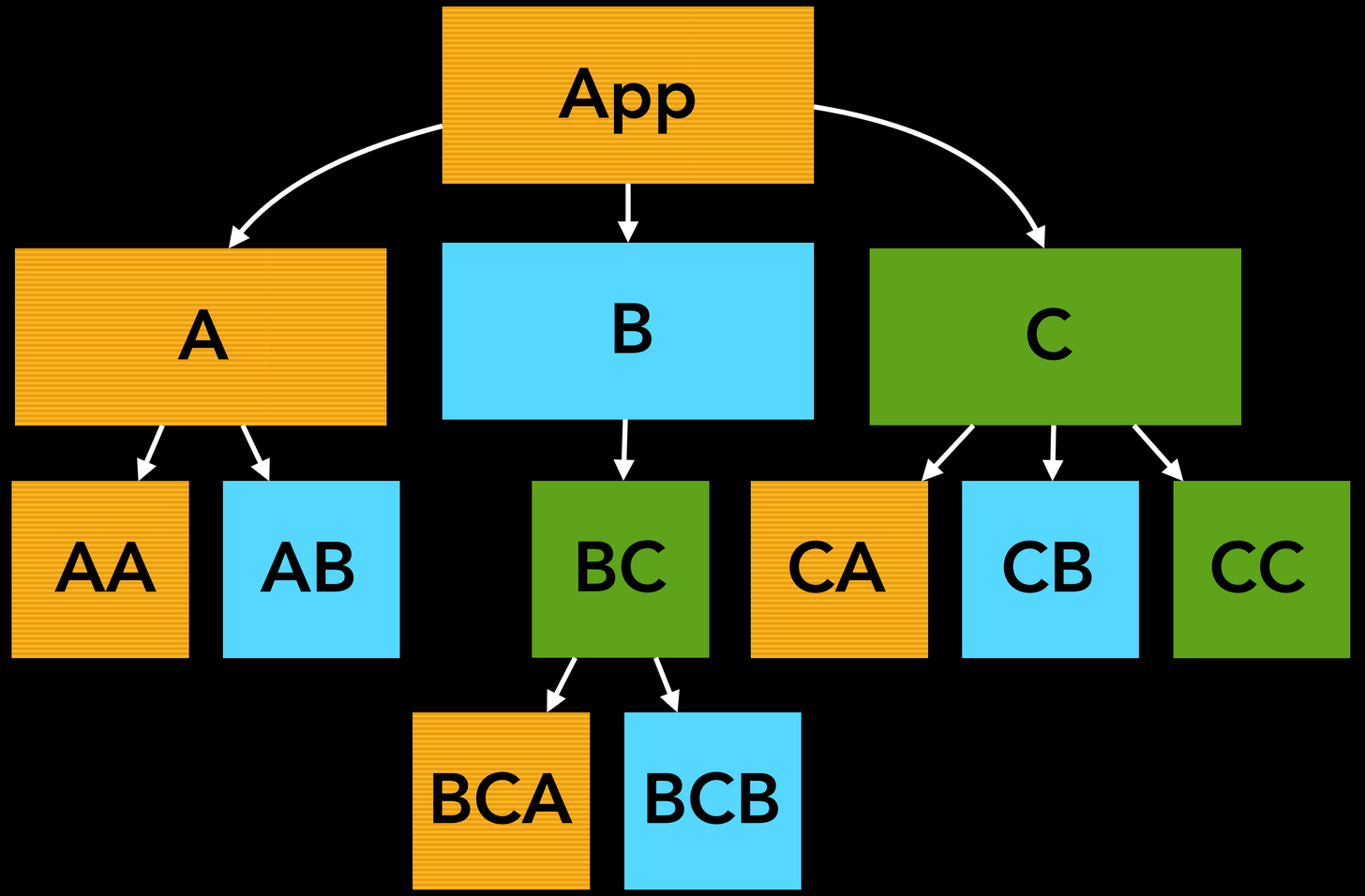
MEDIAN OF 683 FOR JAVASCRIPT APPLICATIONS

(FROM A MEDIAN OF 10 DIRECT)

Source: GitHub Octoverse Report, Dec 2020

TRANSITIVE DEPENDENCIES

"Do you realize how many dependencies?"



"A JEDI USES THE FORCE FOR KNOWLEDGE AND DEFENSE, NEVER FOR ATTACK."

Source: https://www.starwars.com/news/the-starwars-com-10-best-yoda-quotes
https://www.starwars.com/databank/the-force

SECURE CODING TOOL CHEST

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

SCA USE-CASES

- Identify open source components
- Identify security issues in open source components
- Identify license issues in open source components
- Mitigate open-source issues
- Manage open-source quality
- Audits for M&A (Mergers and Acquisitions)
- Monitor vendor software

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 confirmed 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

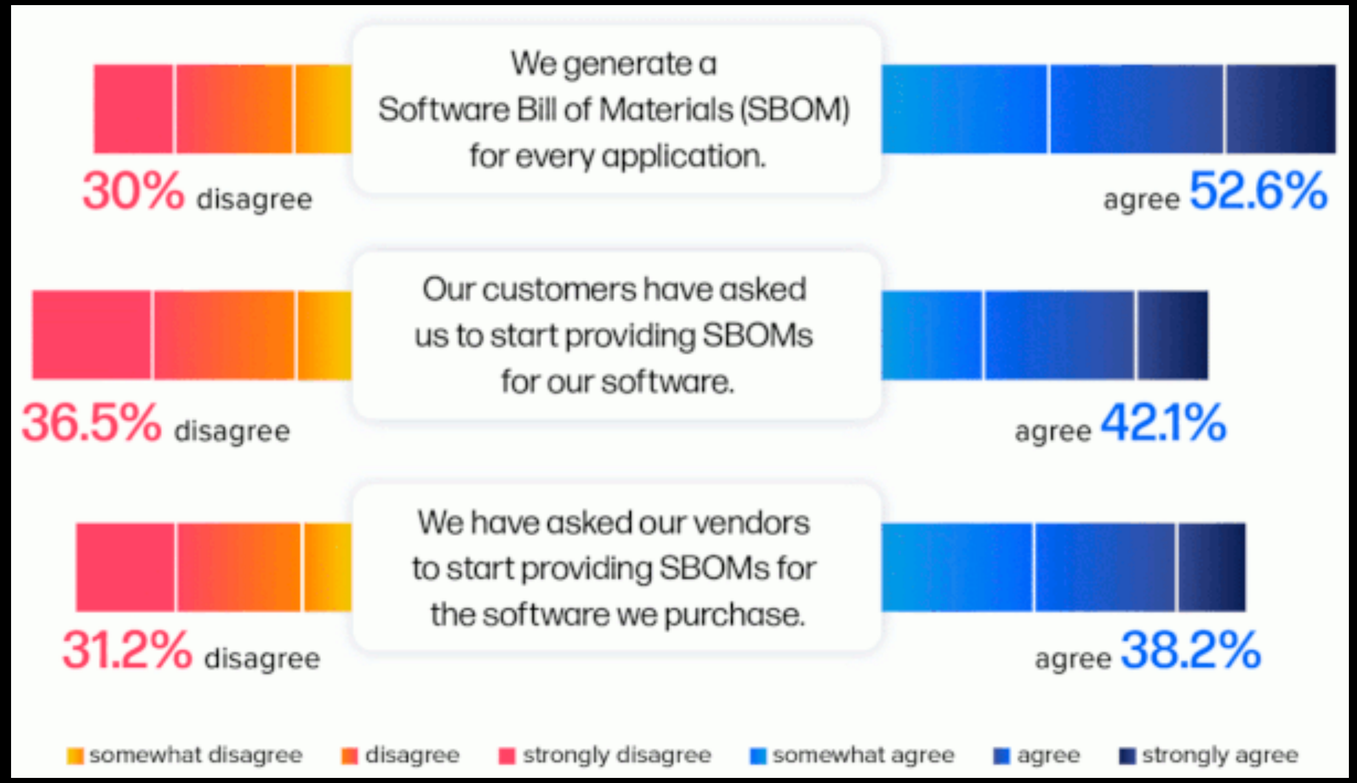
- SPDX® (Software Package Data Exchange)
  - Open standard ISO/IEC 5692:2021 by Linux Foundation

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

EXAMPLE SBOM?

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

SBOM USAGE SURVEY SAYS



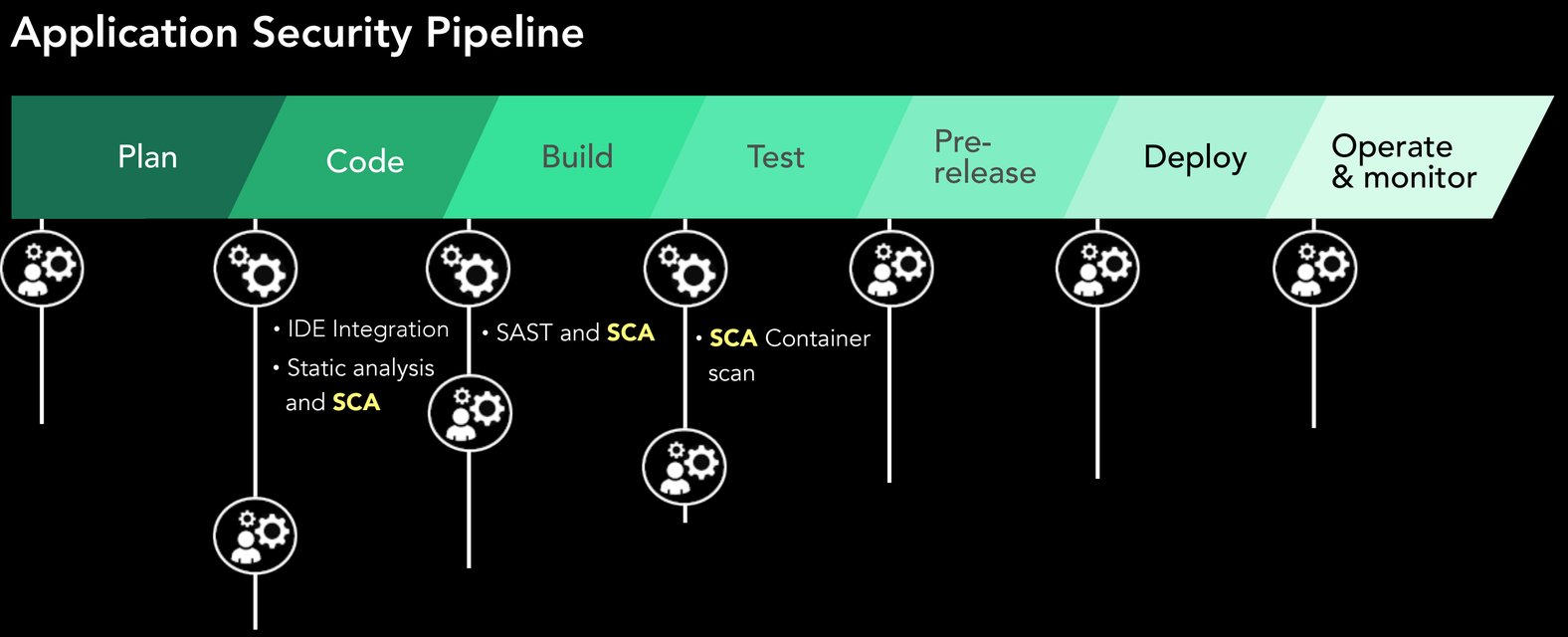
Source: Sonatype 9th Annual State of the Software Supply Chain Report, Nov 2023

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 cost 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

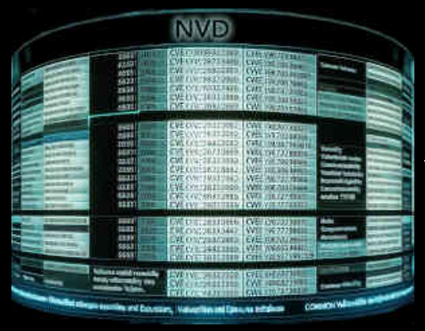
OPEN SOURCE QUALITY MANAGEMENT

"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

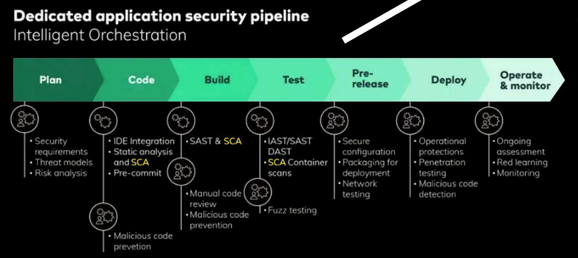


NVD et al.

24/7 Monitoring

SCA SERVICE

SBOM



Pipeline

Email

Text

Microsoft Teams

slack

Jira Software

git GitHub

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

M&A USE-CASE

- Searching for code vulnerabilities
- Searching for licensing conflicts
- Experience
  - Scan and correct before initial engagement
  - Third-party software will be used to audit
  - Do not expect to explain any risk assessment

AI HALLUCINATIONS

The Register

AI hallucinates software packages and devs download them – even if potentially poisoned with malware

Simply look out for libraries imagined by ML and make them real, with actual malicious code. No wait, don't do that

Thomas Claburn — Thu 28 Mar 2024 // 07:01 UTC

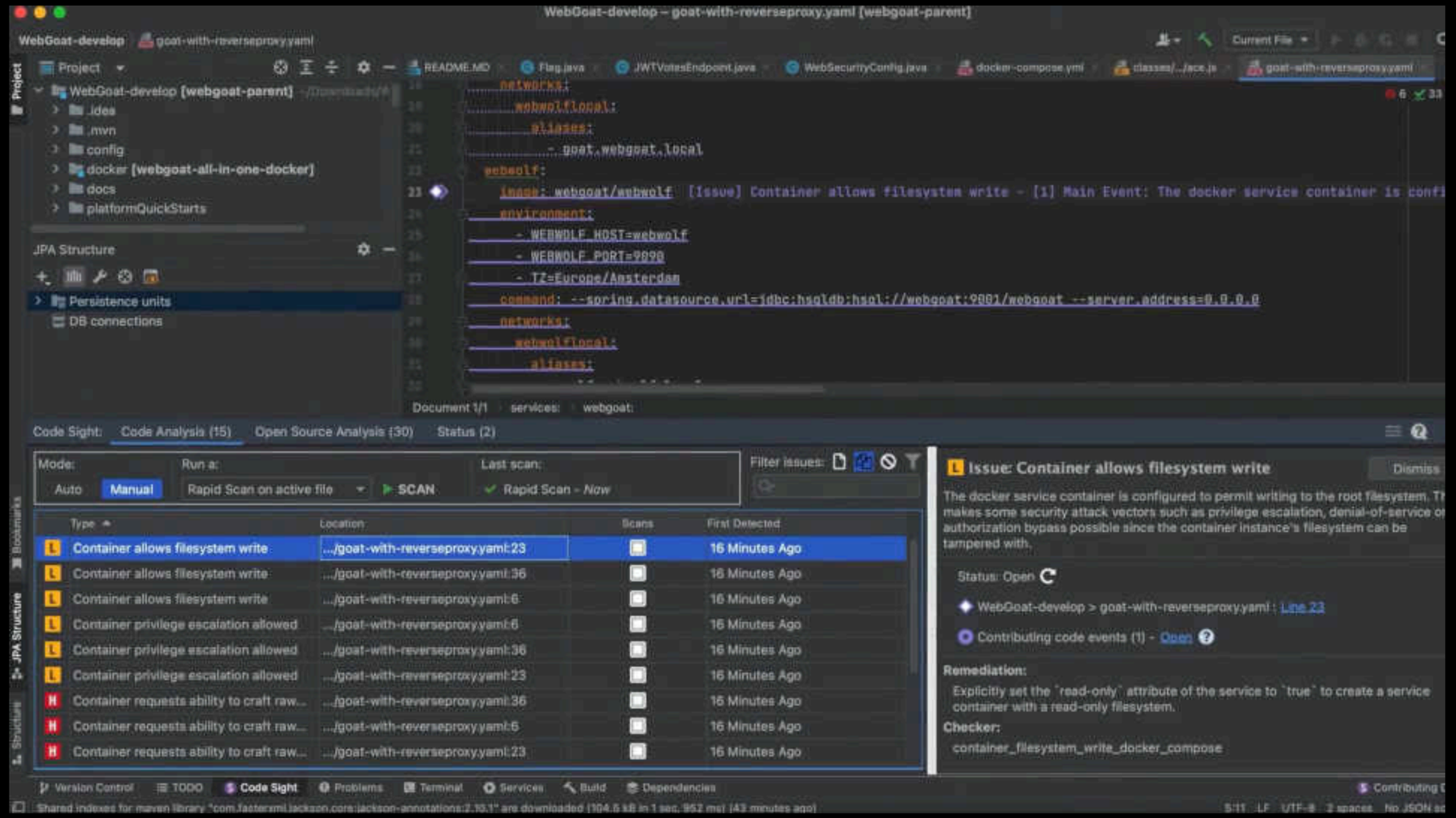
IN-DEPTH Several big businesses have published source code that incorporates a software package previously hallucinated by generative AI.

Not only that but someone, having spotted this reoccurring hallucination, had turned that made-up dependency into a real one, which was subsequently downloaded and installed thousands of times by developers as a result of the AI's bad advice, we've learned. If the package was laced with actual malware, rather than being a benign test, the results could have been disastrous.

Source: https://www.theregister.com/2024/03/28/ai_bots_hallucinate_software_packages/

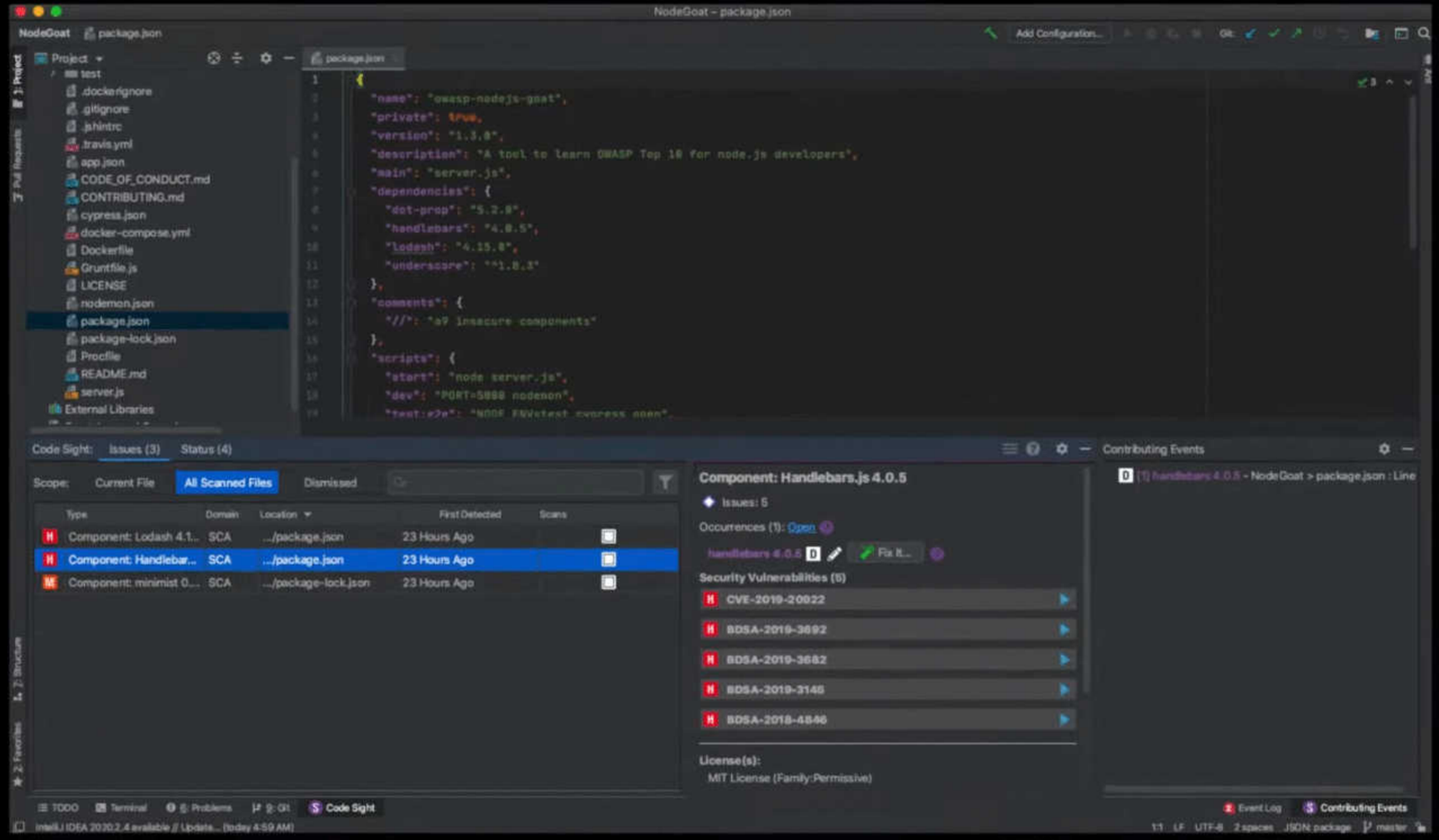
SCA TOOLS

SCA IDE PLUGINS



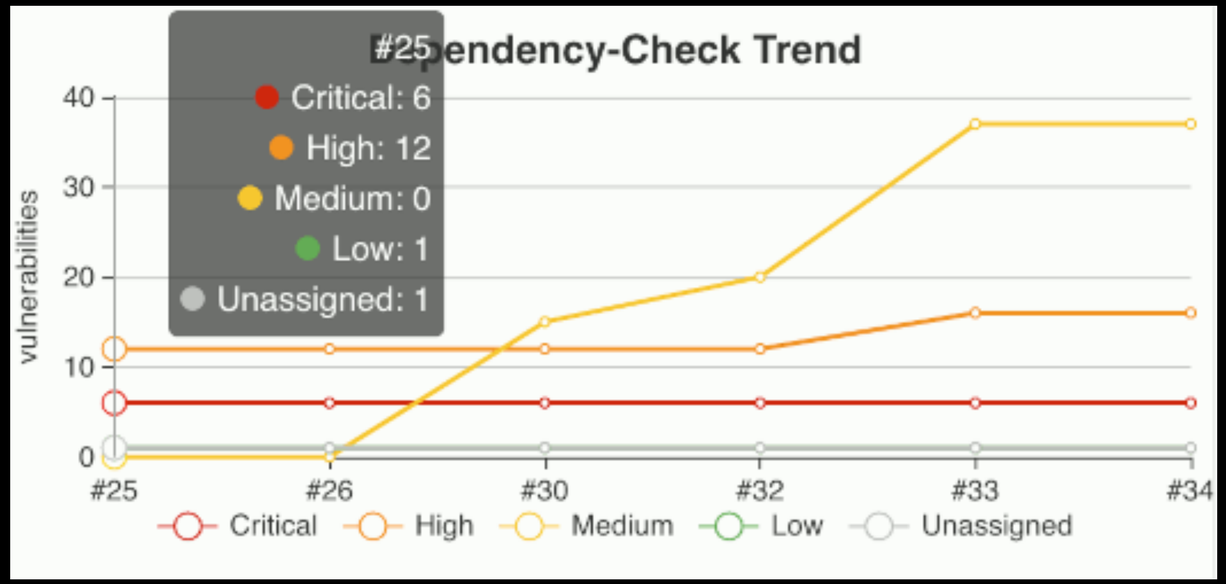
Source: https://youtu.be/6cxi96CJB14

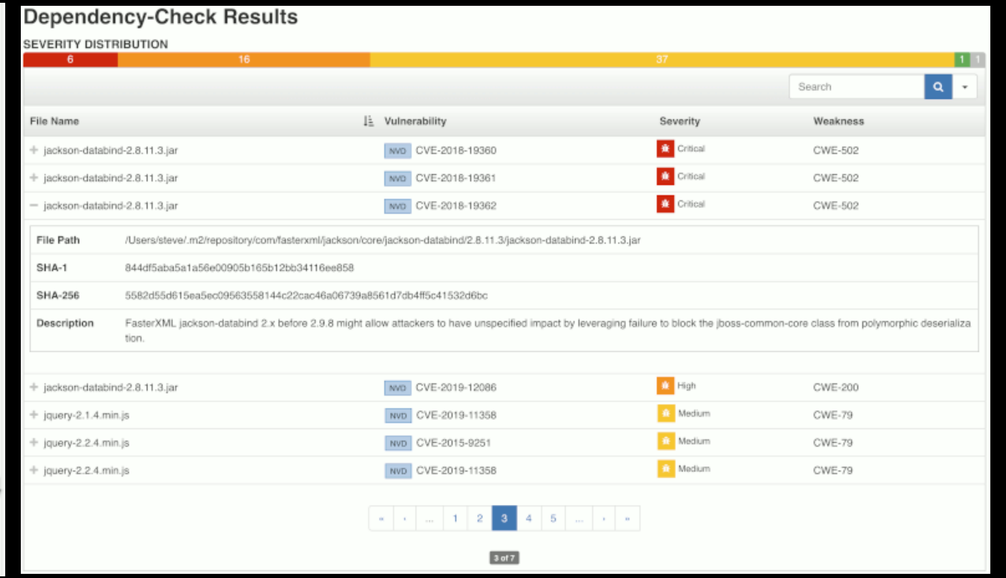
SCA IDE PLUGINS



Source: https://youtu.be/W9BHyXYw3vQ

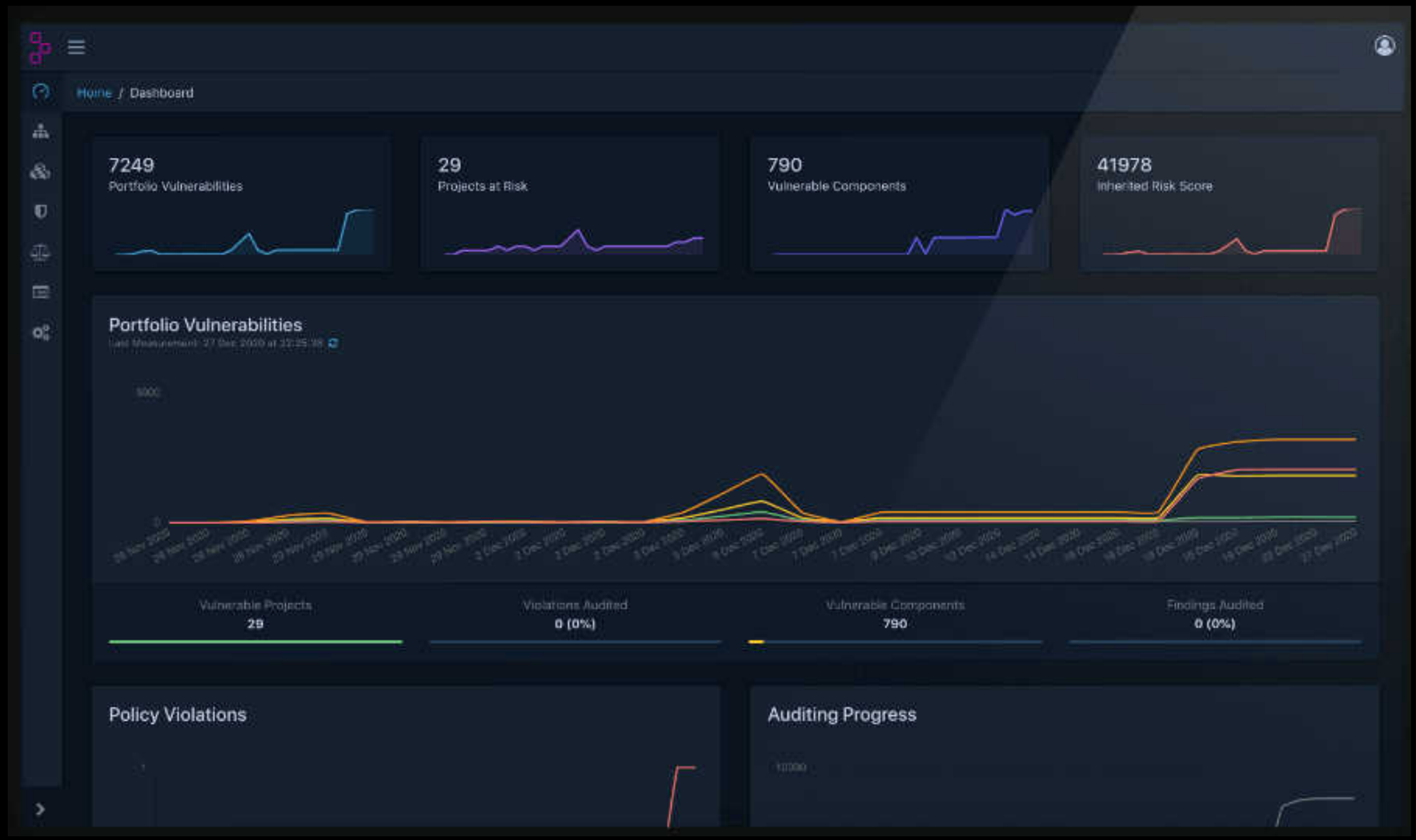
DEPENDENCY CHECK





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

DEPENDENCY TRACK



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

DEPENDENCY TRACK DEMO OVERVIEW

- Step 1: Download application code from GitHub
- Step 2: Create SBOM from project
- Step 3: Upload SBOM to Dependency Track
- Step 4: Observe project's CVEs in Dependence Track

RUNNING DEPENDENCY TRACK

- Step 1: Requirements
  - Windows/Mac/Linux with
    - Memory: Recommend 16 gigabytes
- Step 2: Download/install Docker
- Step 3: Download/install Dependency Track Docker image
  - curl -LO https://dependencytrack.org/docker-compose.yml
  - docker-compose up -d
- Step 4: Download/install git
- Step 5: Download/install npm
- Step 6: Download/install cdxgen
  - npm install -g @cyclonedx/cdxgen

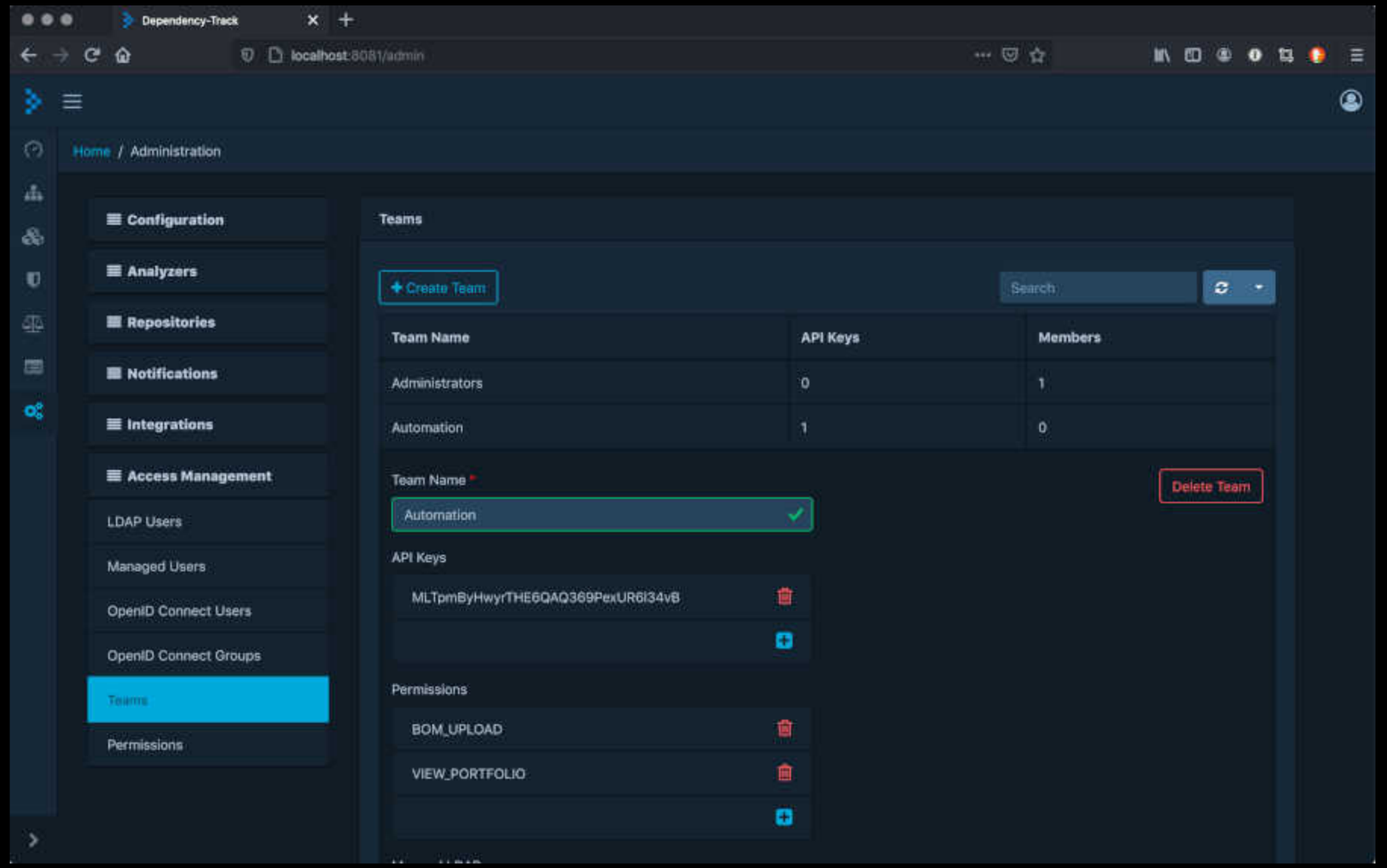
WHAT HAPPENS WHEN DEPENDENCY TRACK IS STARTED THE FIRST TIME

- Downloading the Docker compose file
  - curl -LO https://dependencytrack.org/docker-compose.yml
- Starts Docker container
  - docker-compose up -d
- An embedded H2 database is the default
  - Options: PostgreSQL or Microsoft SQL Server
- Initial startup downloads CVE database
  - Database download takes at least 30 mins.

DEPENDENCY TRACK API SETUP

- Step 1: Login with user/password: admin/admin
  - http://localhost:8080/
  - Default: admin/admin
- Step 2: Dependency Track needs time to download DB (min. 30 mins)
- Step 3: Change admin password
- Step 4: Retrieve API key
  - Home / Administration / Access Management / Teams / Automation
- Note: UI: localhost:8080 / API: localhost:8081

DEPENDENCY TRACK API RETRIEVE API KEY



- Note: Add “PROJECT_CREATION_UPLOAD” permission

CREATING THE SBOM

- Why use cdxgen?
  - Multi-language support:
    - Python, C/C++, Java, JavaScript, Go, Ruby, Rest and more..
- Command line:
  - cdxgen -o bom.json
- Maven plugin (Java maven based projects):
  - mvn cyclonedx:makeAggregateBom

- Chose random Java application
  - git clone https://github.com/neo-nico-neiman/fullstack-booking.git

SENDING SBOM VIA CURL

```
curl -X "POST" "http://localhost:8081/api/v1/bom" ^
-H "Content-Type: multipart/form-data" ^
-H "X-Api-Key: odt_mt3zaRUX48bKPt82IBlQyhzluk7YRknG" ^
-F "autoCreate=true" ^
-F "projectName=fullstack-booking-cdxgen" ^
-F "projectVersion=2.9" ^
-F "bom=@bom.json"
```

* Window batch file example

DEPENDENCY TRACK

DEMO TIME!

South Florida Developer Conference (SoFlo Dev Con)

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 StarWars.com 10: Best Yoda Quotes
- https://www.starwars.com/news/the-starwars-com-10-best-yoda-quotes

- 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

- The Register: AI hallucinates software packages
- https://www.theregister.com/2024/03/28/ai_bots_hallucinate_software_packages/

- 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/

- CycloneDX: A multi-language tool that can create SBOM (Bill of Materials) in CycloneDX format.
- https://cyclonedx.github.io/cdxgen/