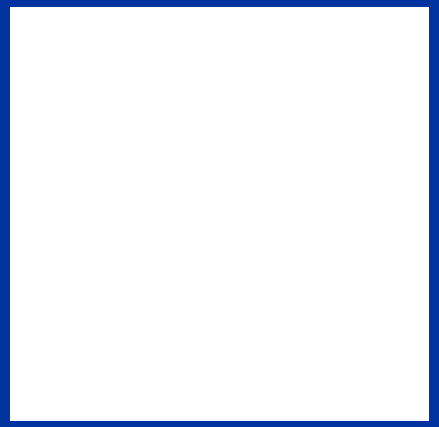


Supply chain attacks and you

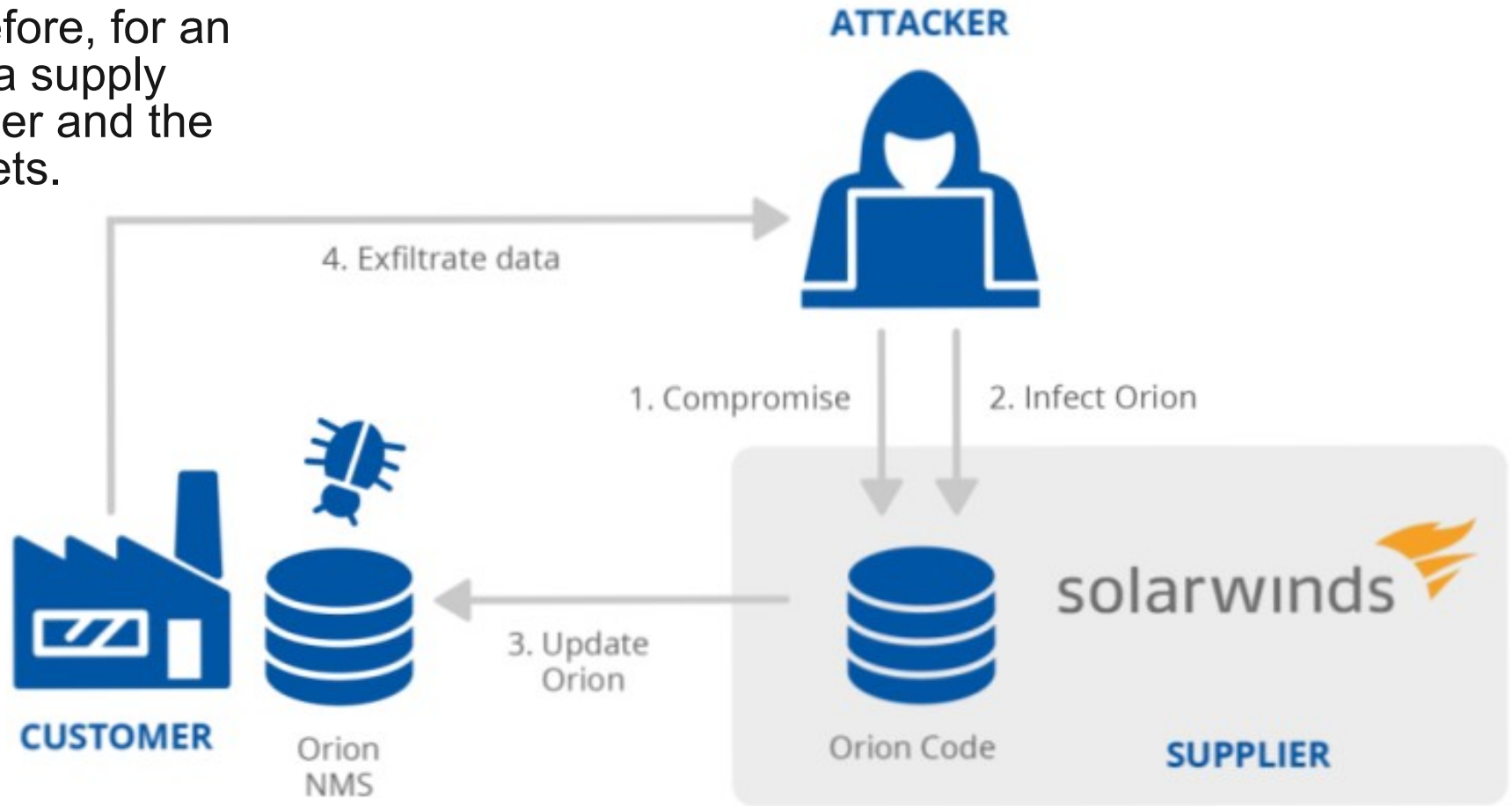
Brice Copy

Thematic CERN School of Computing on Security – 21 June 2022

Supply Chain What ?

As Defined by the European Union Agency for Cybersecurity :

- A **supply chain attack** is a combination of at least **two attacks**. The **first attack** is on a supplier that is **then used to attack the target** to gain access to its assets. The target can be the final customer or another supplier. Therefore, for an attack to be classified as a supply chain one, both the supplier and the customer have to be targets.
- **December 2020 :**
  - Solarwinds attack

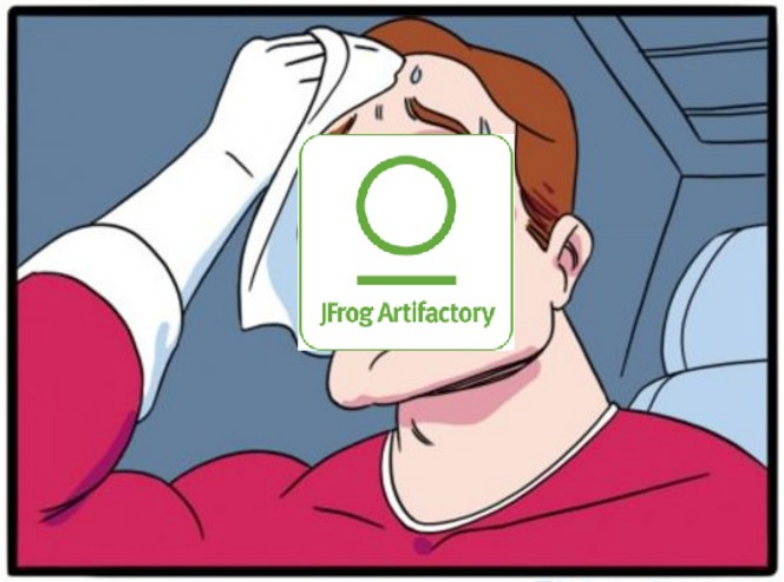


What's new ?

Increasing reliance on open-source software makes it easy and profitable to attack an organization and its customers from the inside.

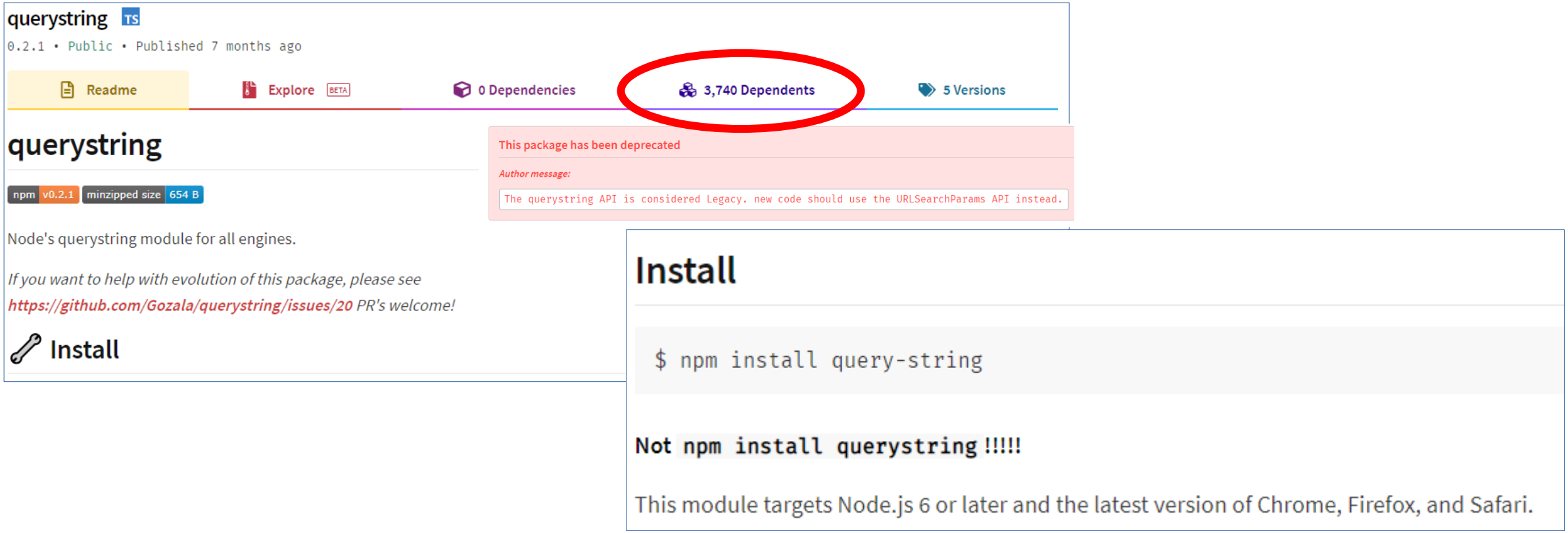
Open-source relies on large number of contributors, with varying levels of vetting or trust in the process :

- Sonatype Catches New PyPI Cryptomining Malware (June 2021)
- Remote Code Execution vulnerability in a 3 million downloads/week NPM package
  (Aug 2021)



How does it work ?

- querystring vs query-string



A few statistics about software reuse

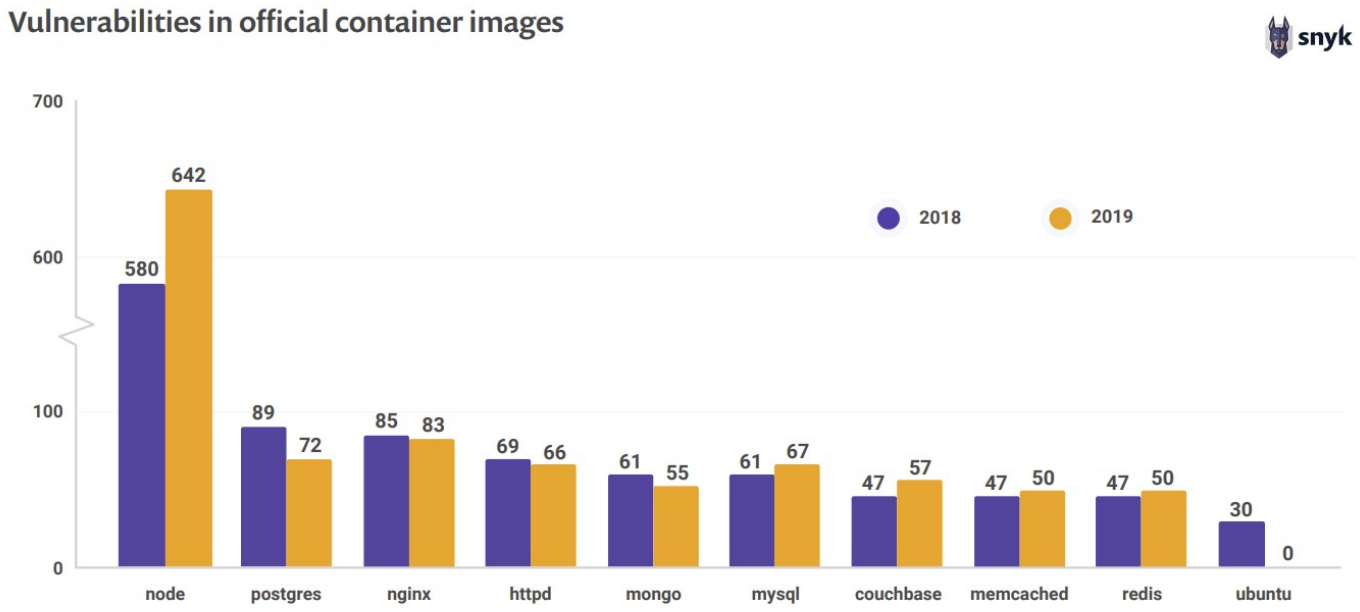
- Open source vulnerabilities **doubled** in the last 2 years
- Supply chain attacks are forecast to **quadruple** in 2021
- **78%** of vulnerabilities are found in transitive dependencies
- 80 lines of code and 7 direct dependencies in a typical Java / Spring Boot application results in :
  - 59 transitive dependencies
  - 713 348 effective lines of code
  - 0 vulnerabilities… until when ? Maybe if you configure properly and keep up to date.
- **More than 75% of global org will be running containerized apps by 2022**
  - The top 10 most popular images are > 30 vulnerabitilies
  - 76% of the top 1000 Docker Hub container images have severe known vulnerabilities

SOURCE : Gartner, Snyk State of Open Source Security Report 2019

A few reminders of current statistics (continued)

- **Node official image (14.3-buster)**
  - 17 high sev. vulnerabilities
  - 139 medium sev. vulnerabilities
- **Slimmer images carry less risk**
- **Rebuilding images / updating**
- **Automating the upstream sourcing process is essential**

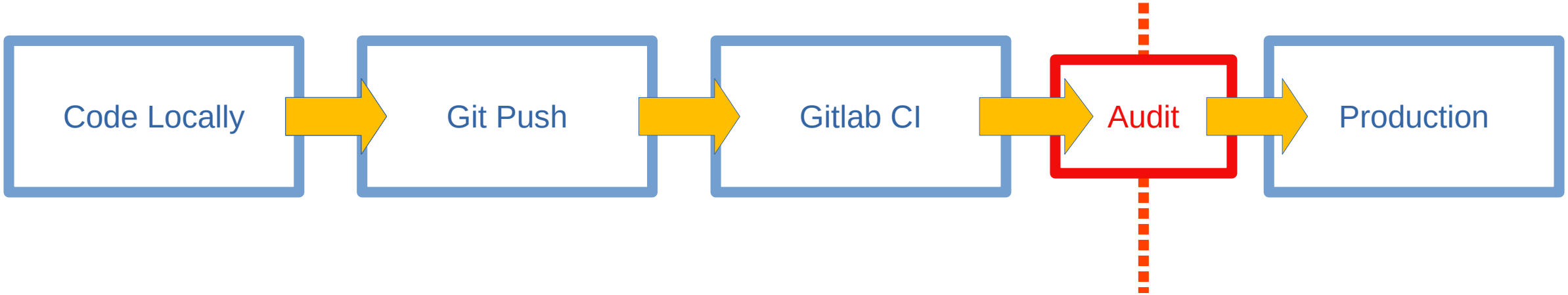
SOURCE : Snyk State of Open Source Security Report 2020




```
Project name:       docker-image|node
Docker image:       node:latest
Base image:         node:latest
Licenses:           enabled

Tested 412 dependencies for known issues, found 642 issues.

Base Image    Vulnerabilities     Severity
node:latest   642                 17 high, 139 medium, 486 low

Recommendations for base image upgrade:

Alternative image types
Base Image                Vulnerabilities     Severity
node:14.3.0-buster-slim   47                  0 high, 4 medium, 43 low
node:14-buster            291                 2 high, 60 medium, 229 low
node:14-slim              68                  6 high, 7 medium, 55 low
```

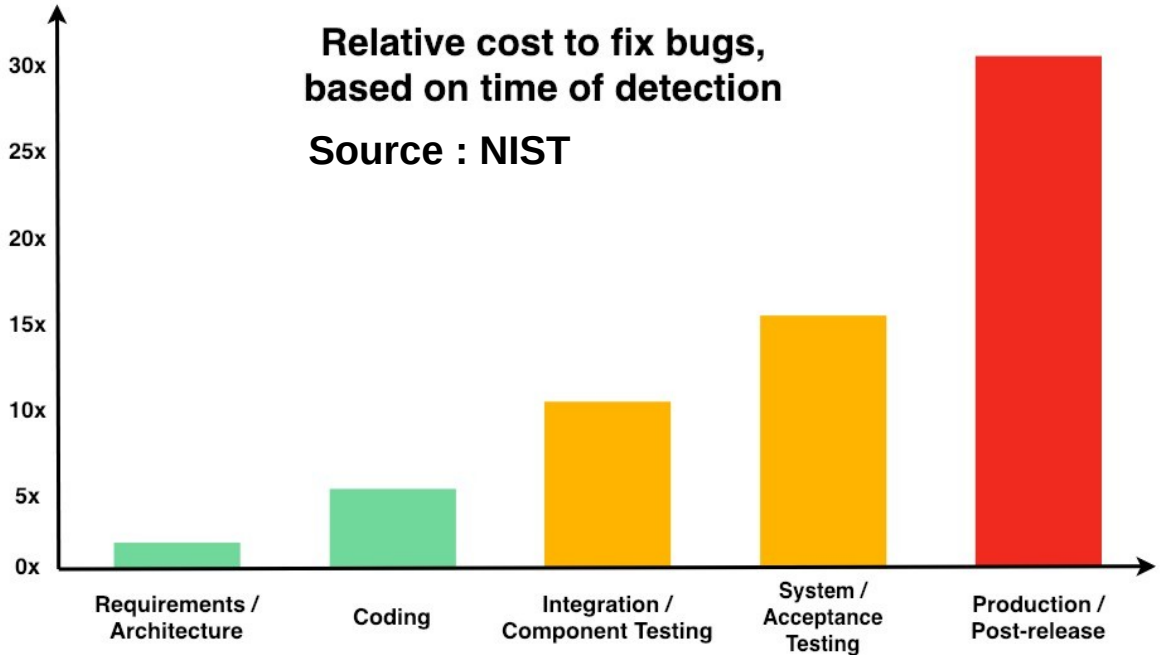
From DevOps to DevSecops

- **81% of respondents believe developers should actually own security**
  (SOURCE : Snyk DevSecops insights survey 2019)
- **33% of respondents believe that security is a major constraint on the ability to deliver software quickly**
  (SOURCE : Snyk DevSecops insights survey 2019)
- **So we agree : how do we shift the onus of secure code upstream ?**

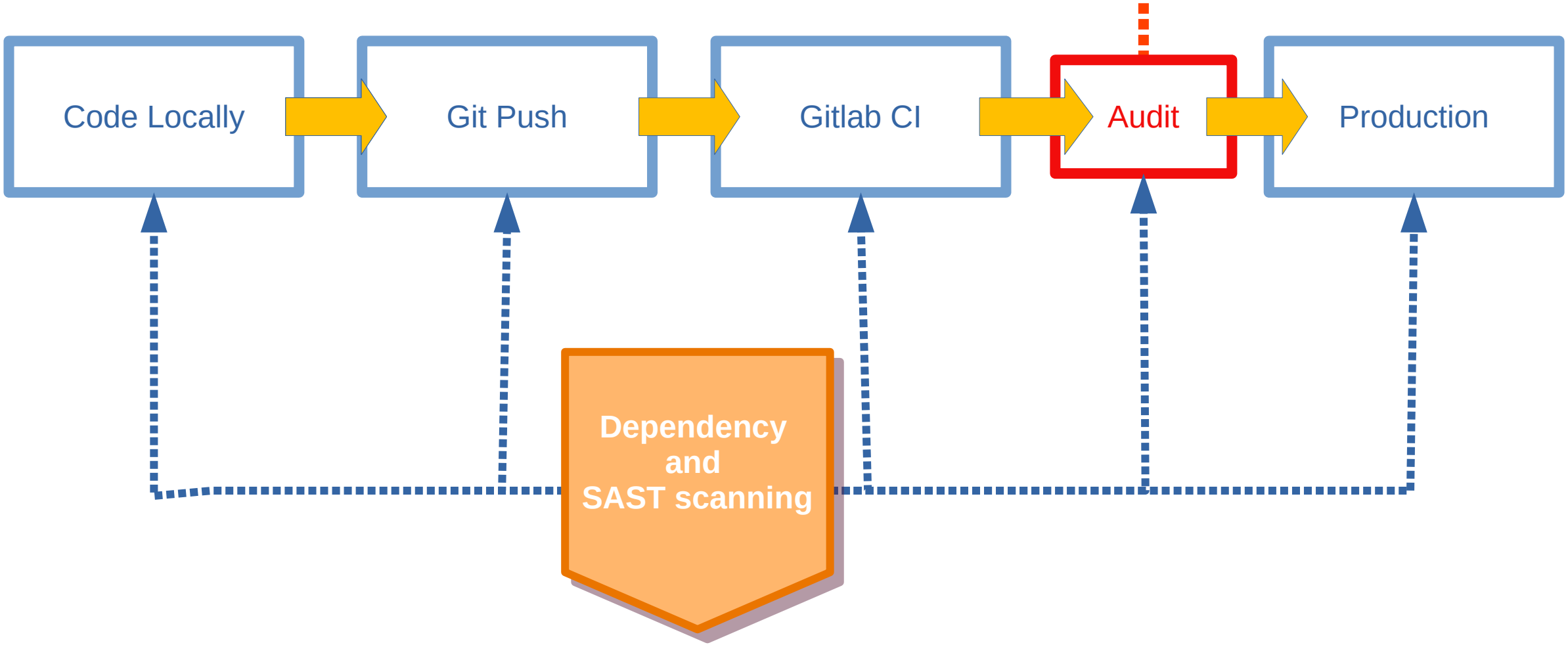


The cost of defects

- **Most defects end up costing more than it would have cost to prevent them. Defects are expensive when they occur, both the direct costs of fixing the defects and the indirect costs because of damaged relationships, lost business, and lost development time. — Kent Beck, Extreme Programming Explained**



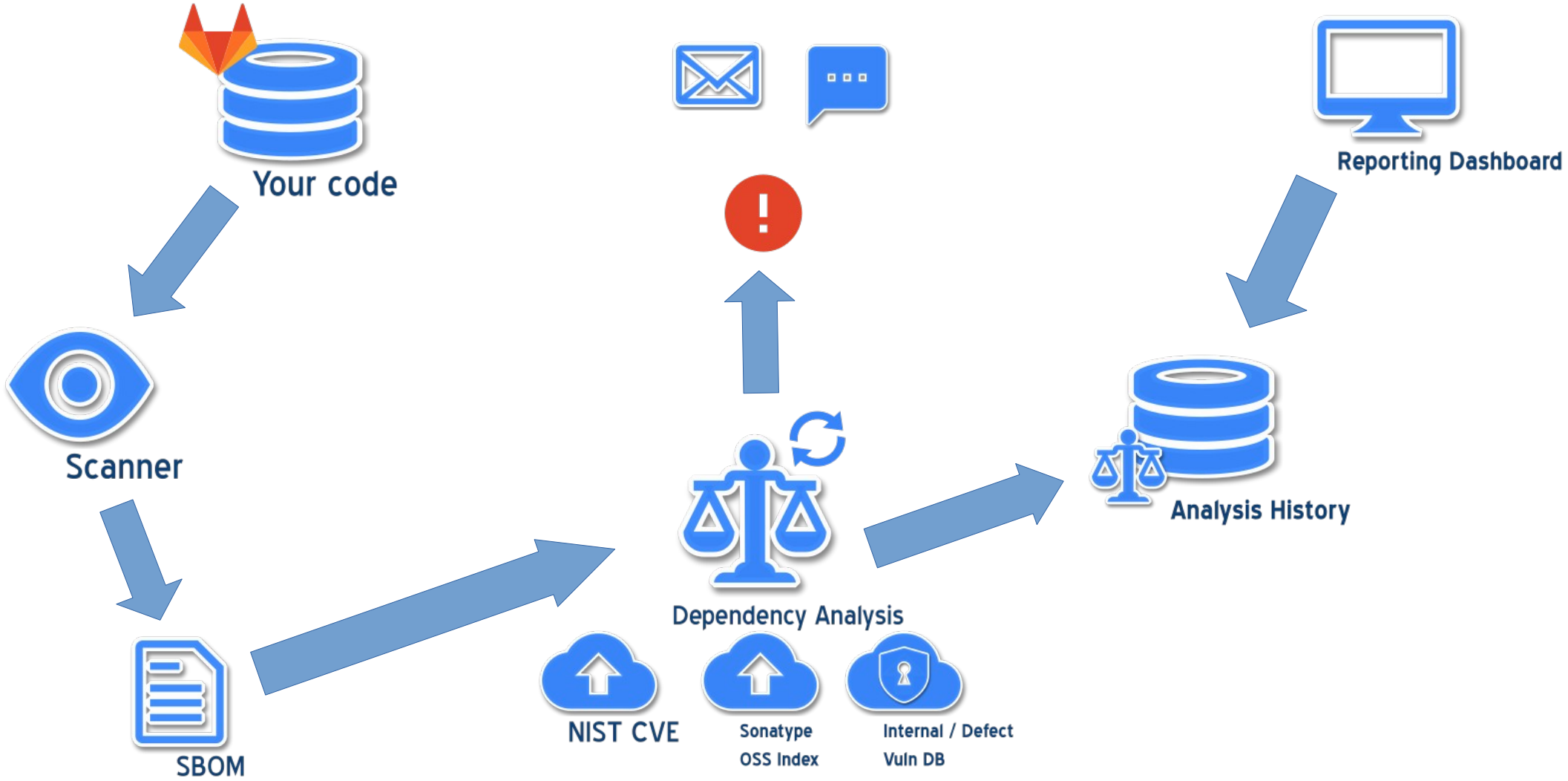
From DevOps to DevSecops



OWASP Software Bill Of Materials

- What is it ? What is it made of ?
- What do you do with it ?
- White House executive order :
  - As of May 2021, A Software Bill of Materials is mandated for all suppliers of software and service providers to US government.

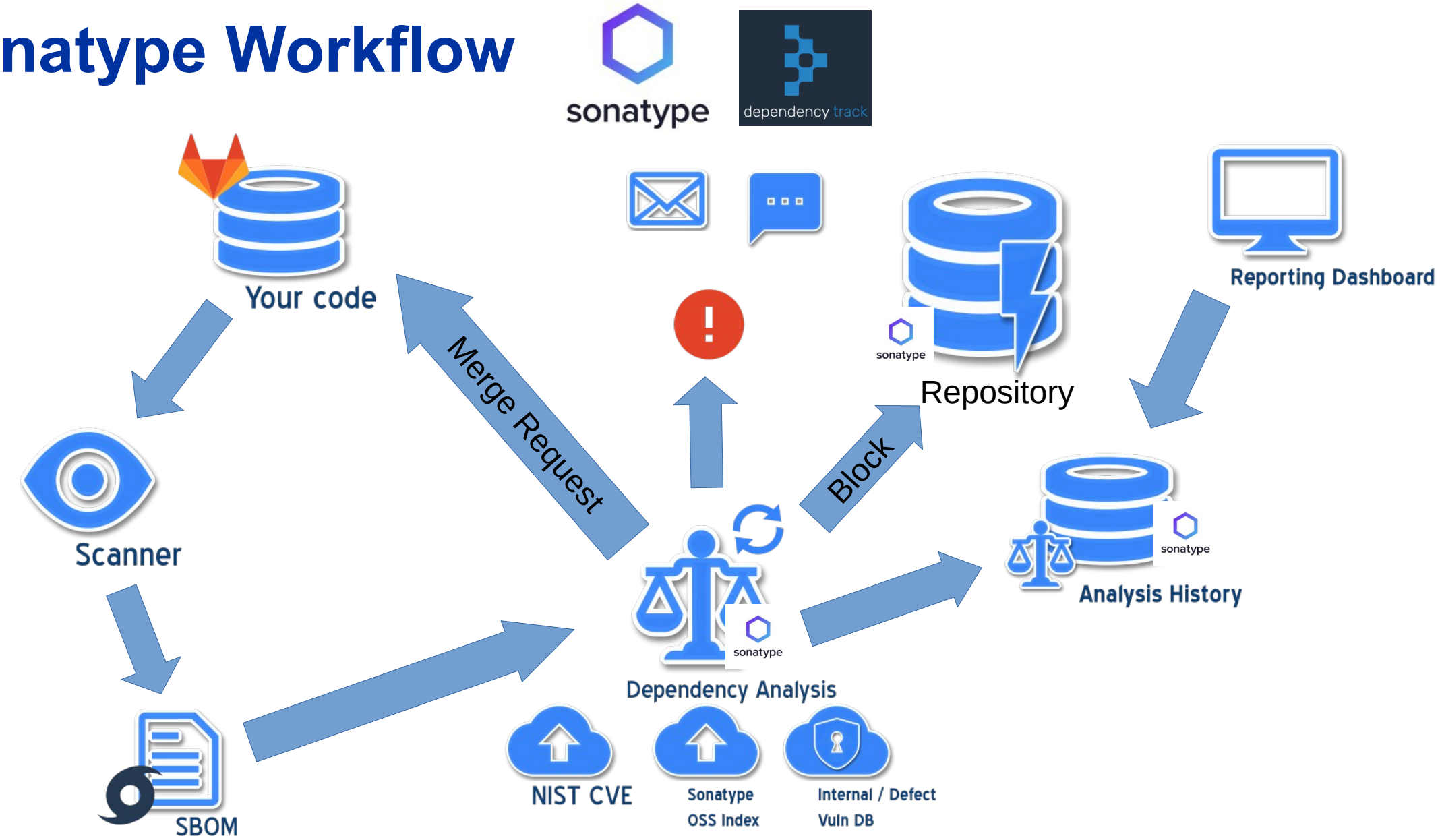
SBOM Certification and Workflow



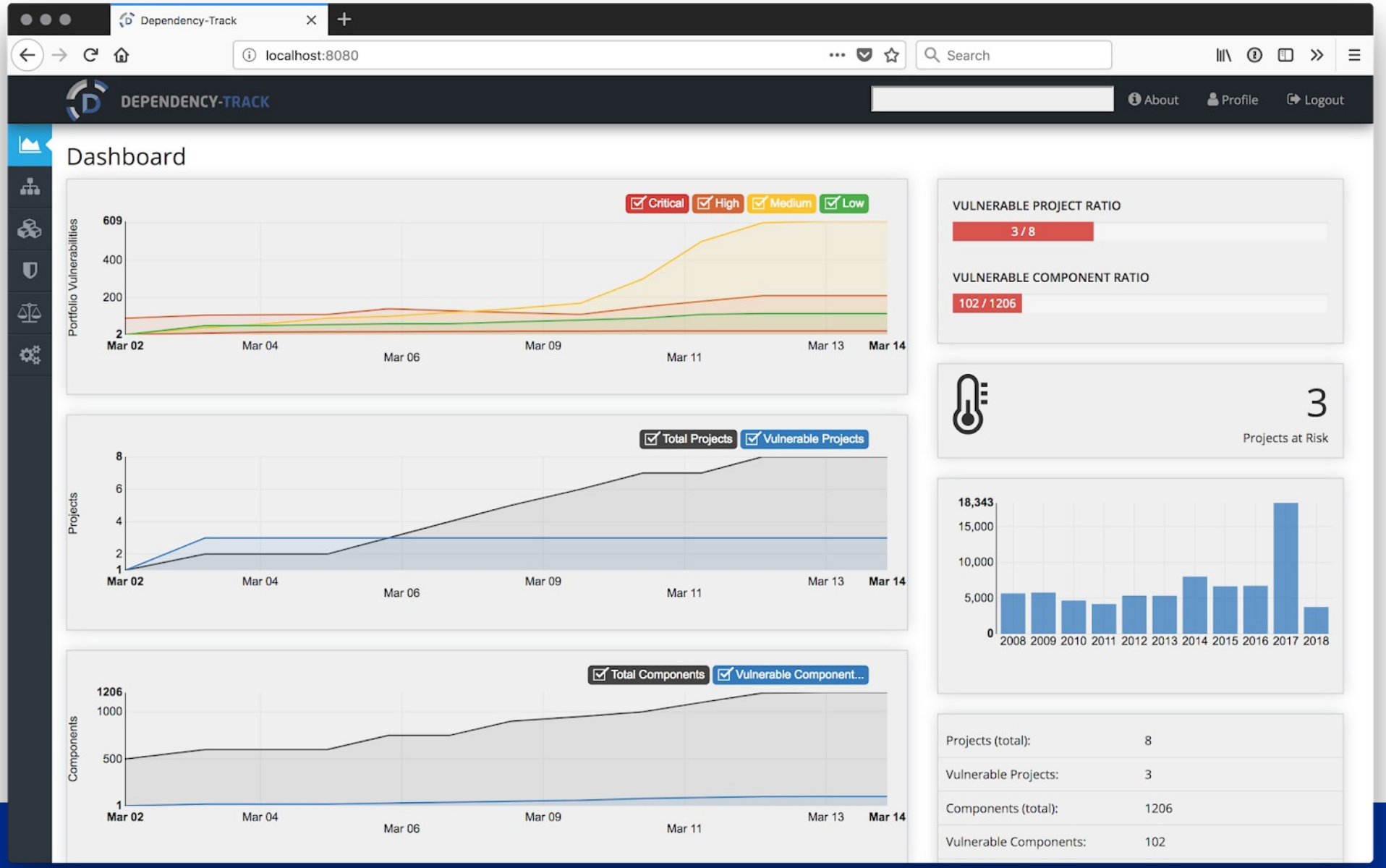
CycloneDX and Dependency Track

- OWASP (Open Web Application Security Project) foundation sponsors :
  - CycloneDX – A specification and scanning tool implementation for collecting SBOM data
  - Dependency Track – A Web API and UI to analyse and distribute SBOM data and vulnerability reports

Sonatype Workflow



Dependency Track Web Interface



Take away

- Supply chain attacks are now part of our development landscape and here to stay.
- Software Bills of Material allow to keep track of our applications' dependency and can be used to manage our security posture.
- Simple continuous integration solutions can be added for most technologies to ensure our deployments are free from malware and vulnerabilities.
- **Standards :**
  - **OWASP CycloneDX SBOM**
  - **OASIS CSAF, VEX**

Links and references

- ENISA 2021 Report on Supply chain attacks threat landscape
  https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
- Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks
  https://link.springer.com/chapter/10.1007/978-3-030-52683-2_2
- Proxies are complicated – RCE vulnerability in a 3 million downloads/week NPM package
  https://httptoolkit.tech/blog/npm-pac-proxy-agent-vulnerability/
- Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies
  https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610

home.cern