When dependabot is not enough

Protecting our software supply chain

Edoardo Dusi

Developer Relations Engineer @ SparkFabrik

edoardo.dusi@sparkfabrik.com

@edodusi

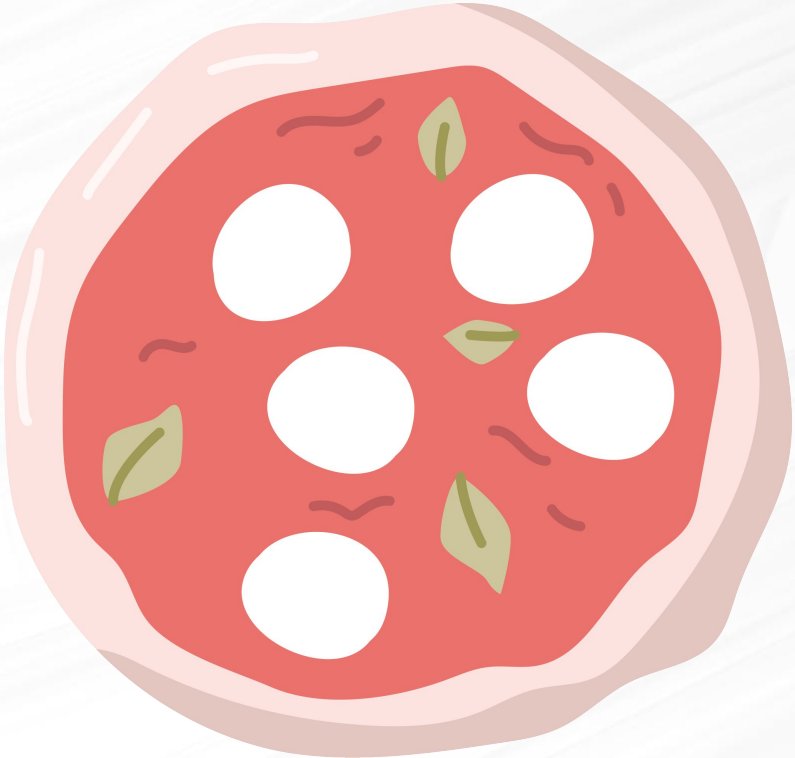
@edo@continuousdelivery.social

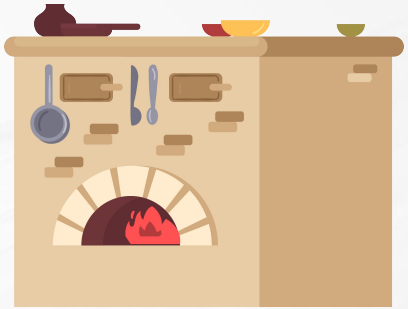
HackInBo Spring 2024 Edition
22ª EDIZIONE

What is the Software Supply Chain

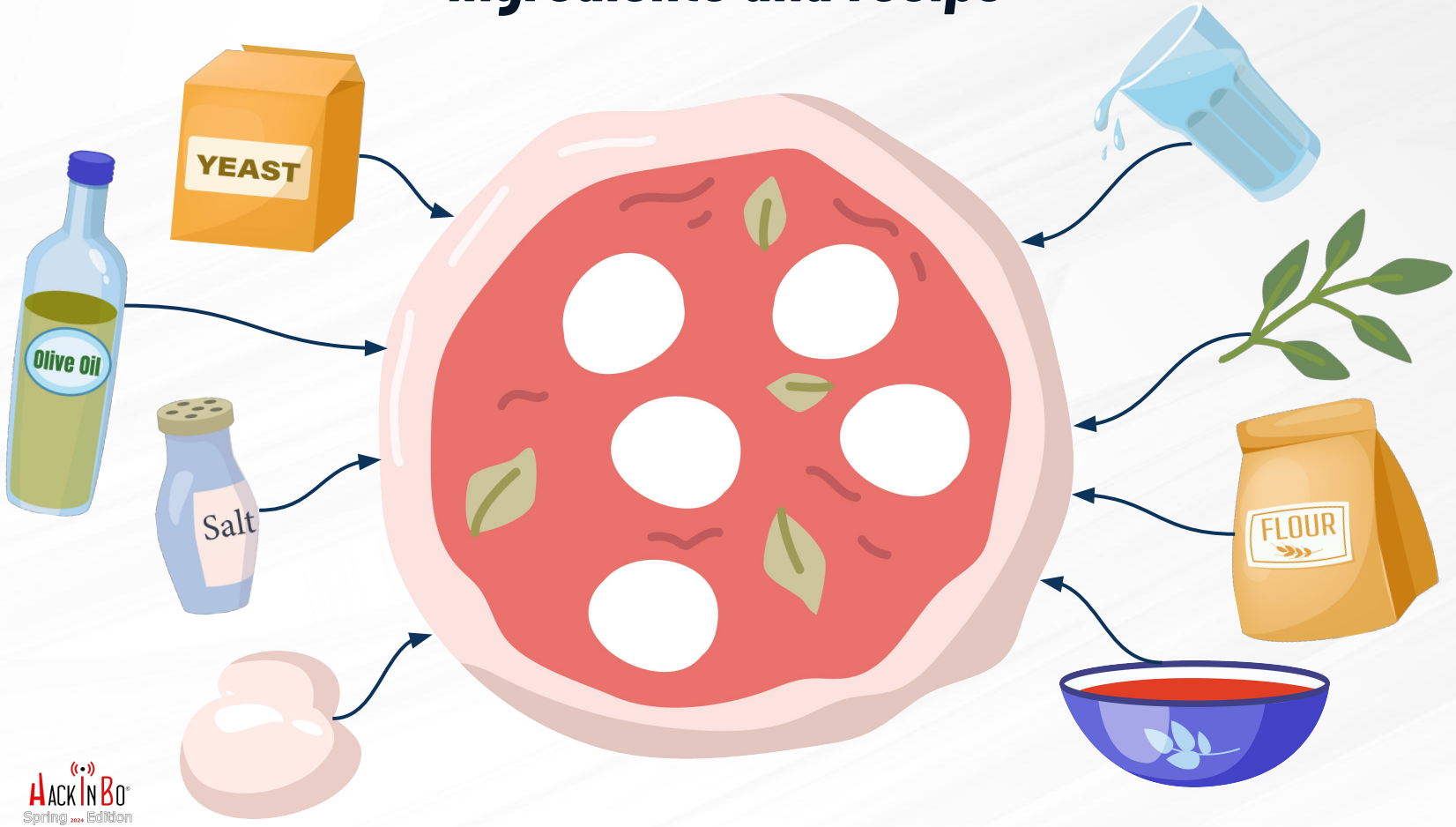
The **software supply chain** refers to the end-to-end process of creating, delivering, and maintaining software applications.

The supply chain of a pizza





Ingredients and recipe



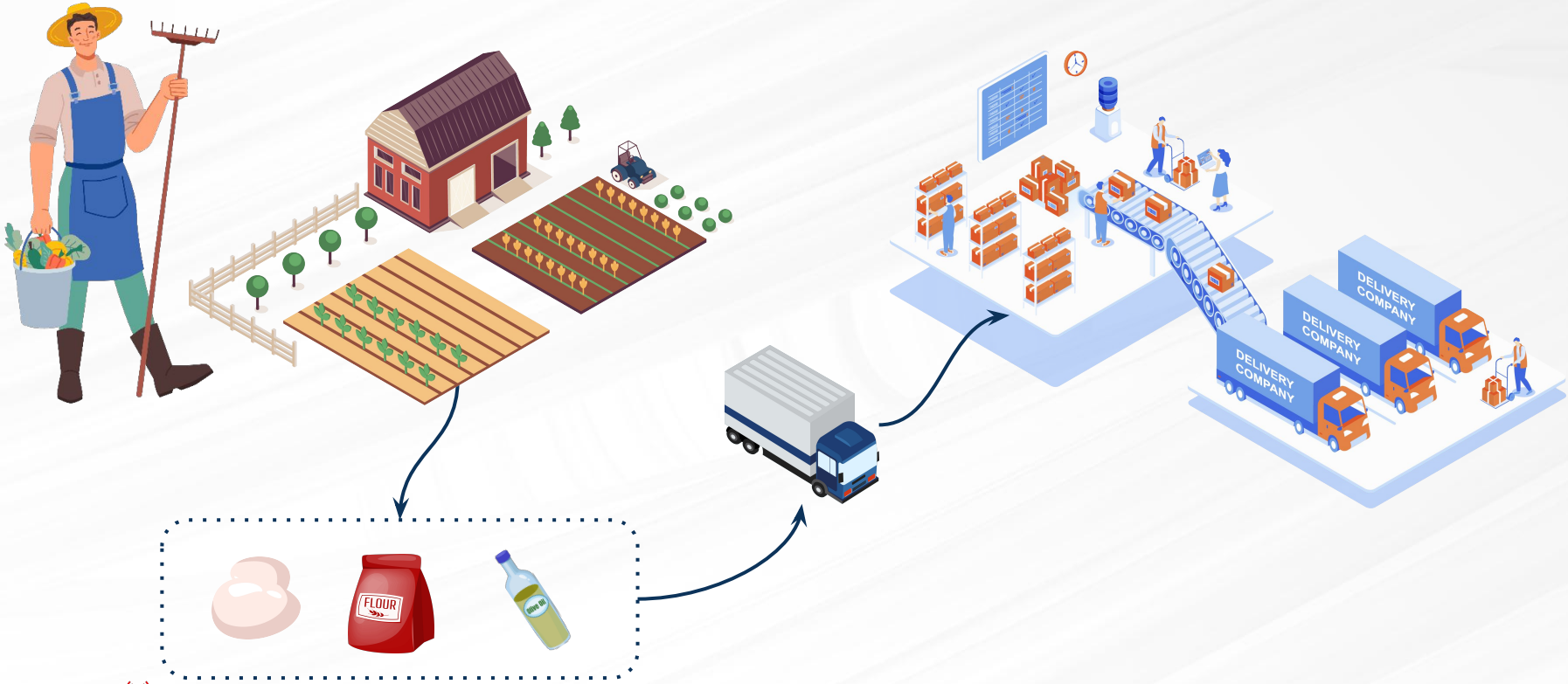
Distributors

Possible Threats

"Conformité Européenne" "China Export"

Distribution

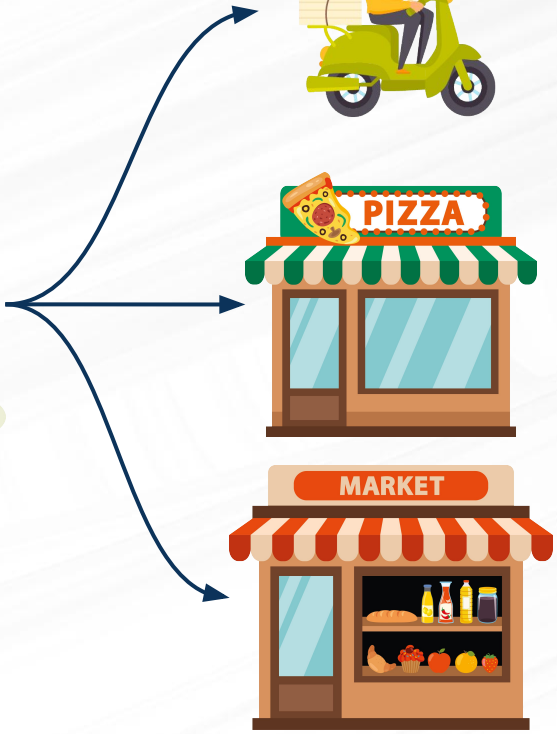
Supply Chain

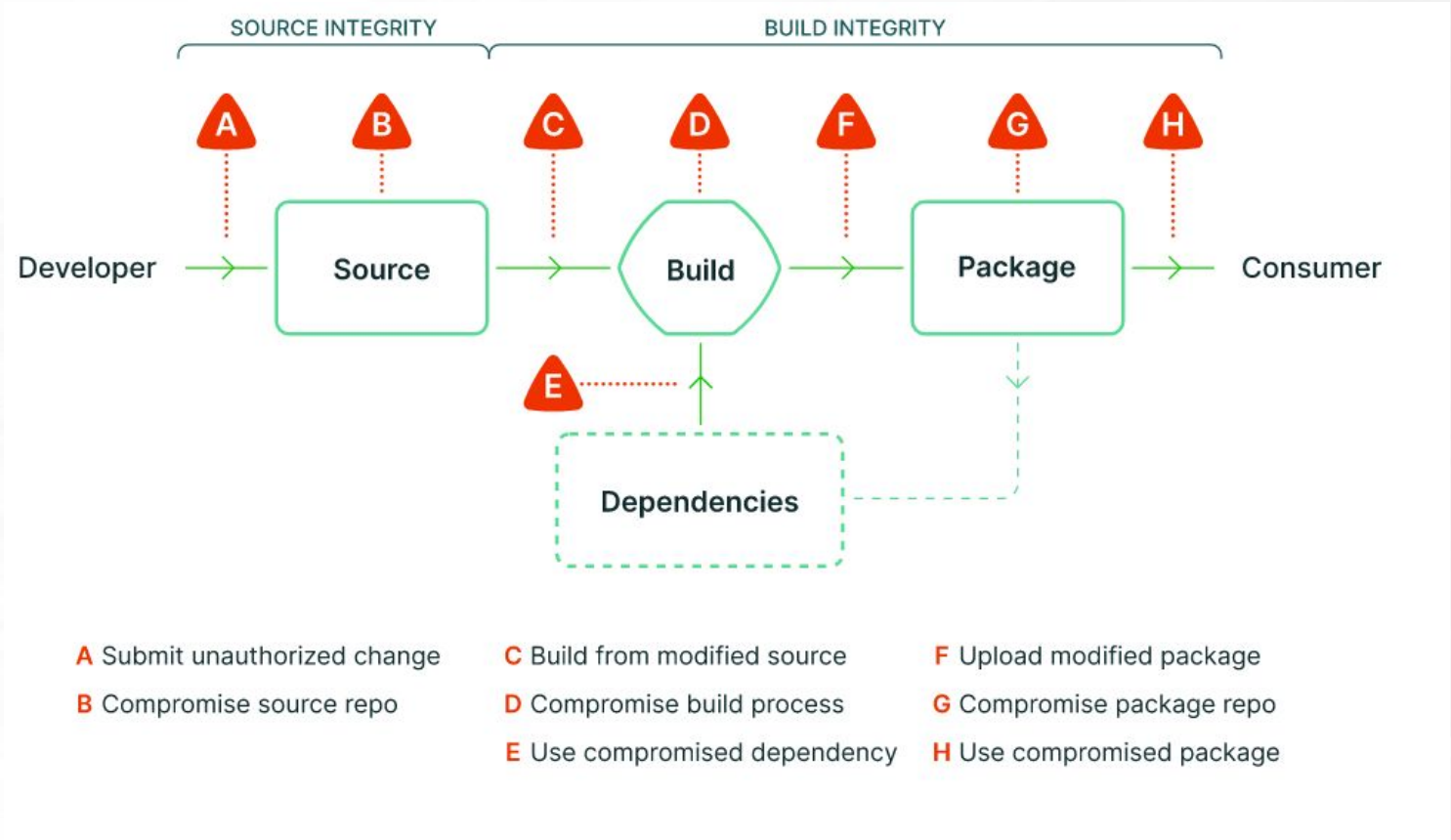


Get ingredients and check receipts

Cooking

Delivery





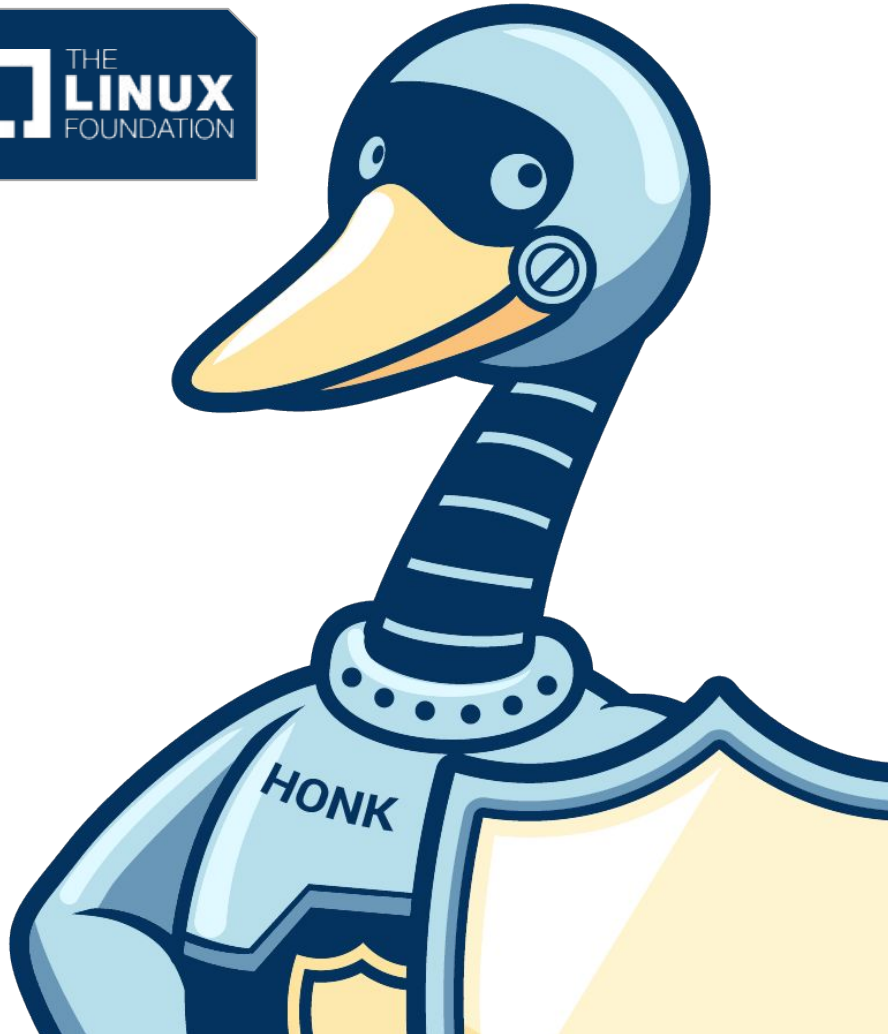
From: SLSA specification

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

We are part of THE LINUX FOUNDATION

Purpose

The OpenSSF is a cross-industry organization that brings together the industry's most important open source security initiatives and the individuals and companies that support them. The OpenSSF is committed to collaboration and working both upstream and with existing communities to advance open source security for all.



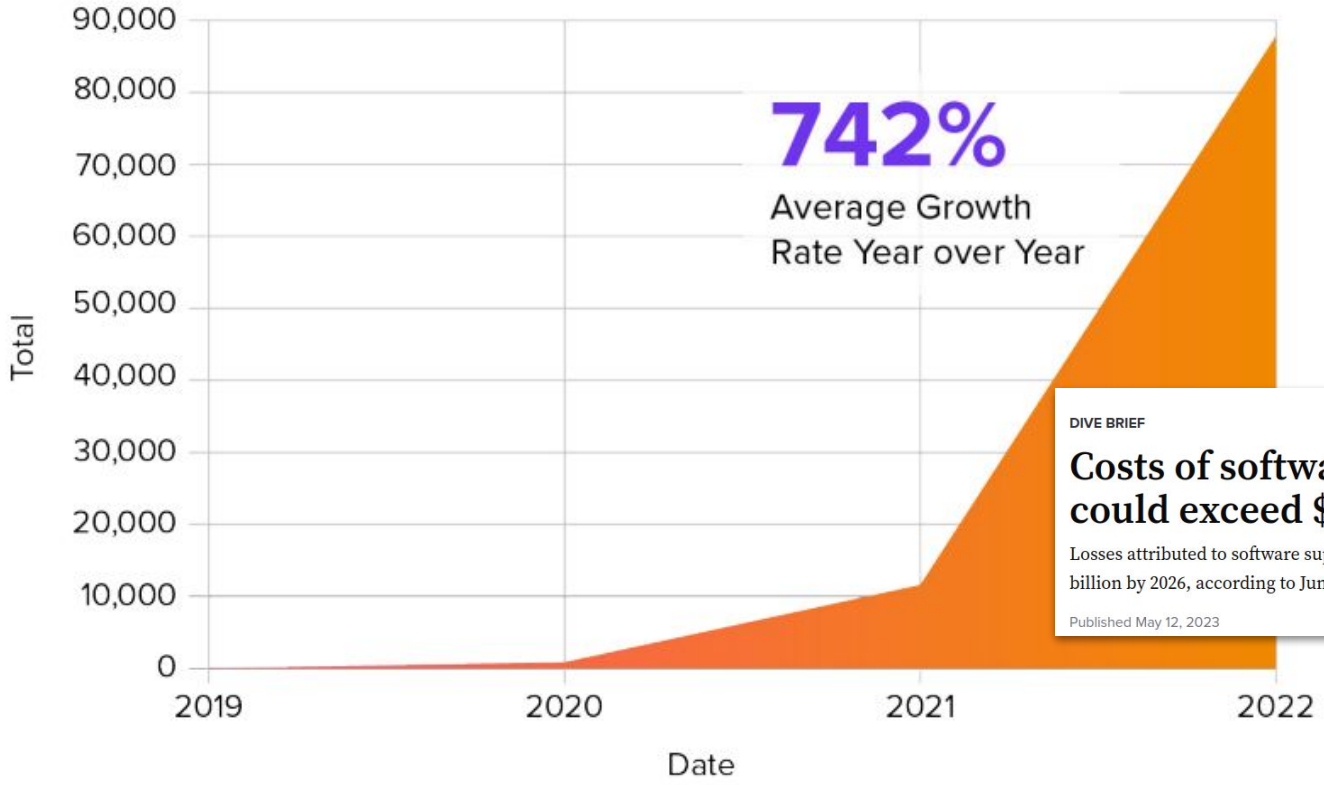
HACK IN BO
Spring 2024 Edition
22ª EDIZIONE

Key Components

- ➔ **Development**: The phase where code is written and applications are built
- ➔ **Build and Integration**: Compiling source code, integrating modules, and creating a package
- ➔ **Testing**: Unit or E2E testing to identify and fix bugs, ensuring software reliability
- ➔ **Deployment**: Deploying software to a server
- ➔ **Distribution**: Packaging and delivering software to end users, through physical media or digital channels
- ➔ **Updates and Maintenance**: Ongoing efforts to enhance, fix issues, and provide support post-deployment

Importance of Software Supply Chain Security

FIGURE 1.6 NEXT GENERATION SOFTWARE SUPPLY CHAIN ATTACKS, 2019-2022



DIVE BRIEF

Costs of software supply chain attacks could exceed $46B this year

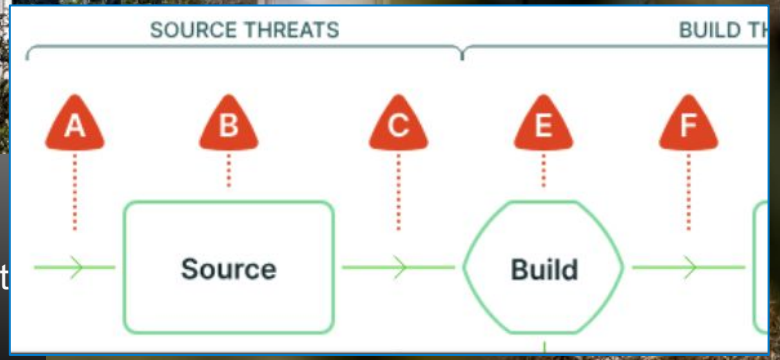
Losses attributed to software supply chain attacks will jump 76%, reaching almost $81 billion by 2026, according to Juniper Research.

Published May 12, 2023

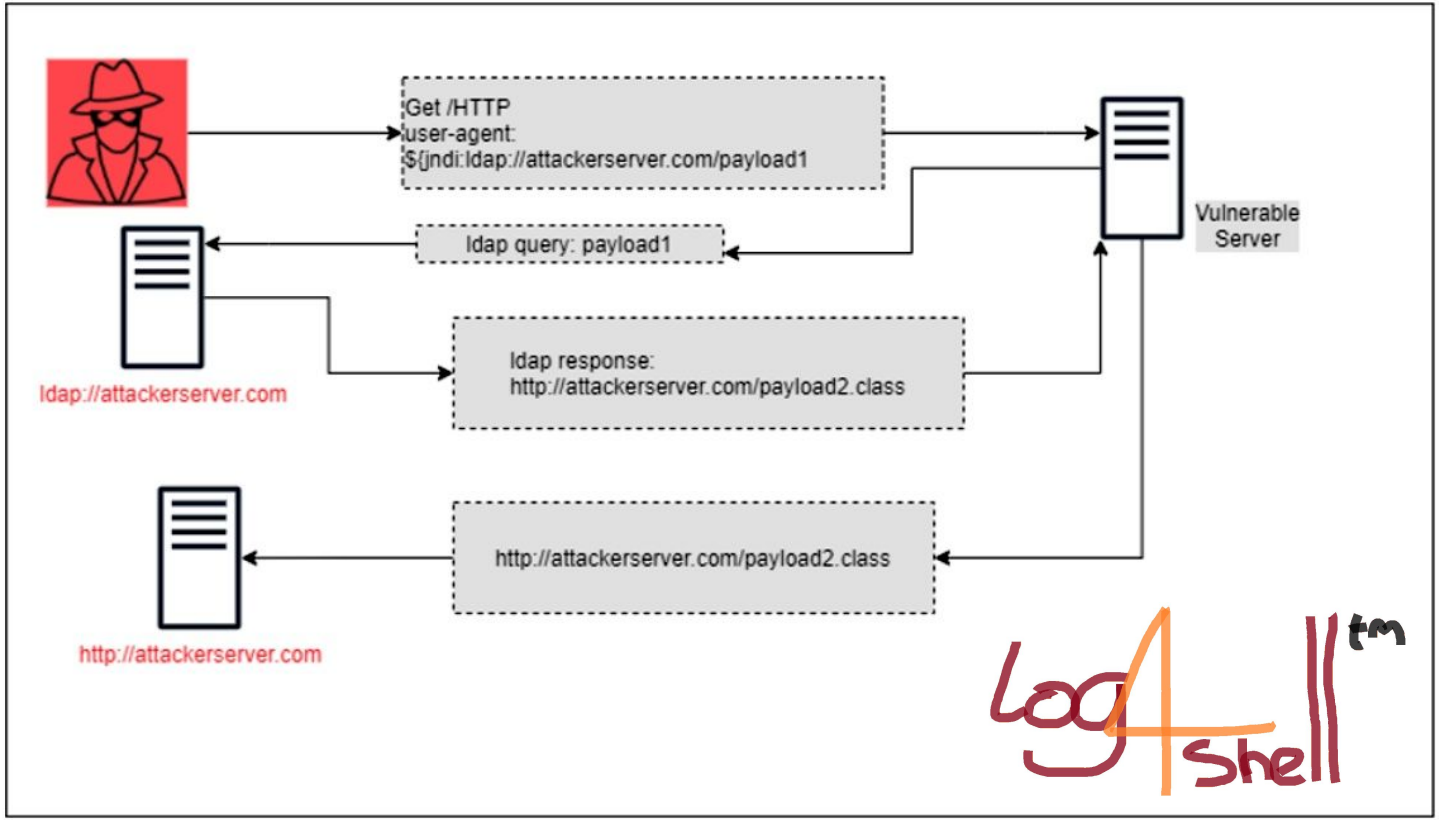
https://www.sonatype.com/state-of-the-software-supply-chain/introduction

2020

About **18,000 customers of SolarWinds** installed the infected updates, including firms like Microsoft (Cisco, Intel, Deloitte) and top government US agencies like Pentagon, Homeland security, National Nuclear Securit etc.



Description of the CVE-2021-44228 vulnerability



National Cybersecurity Strategy

MARCH 2023

European Commission

CYBER RESILIENCE ACT

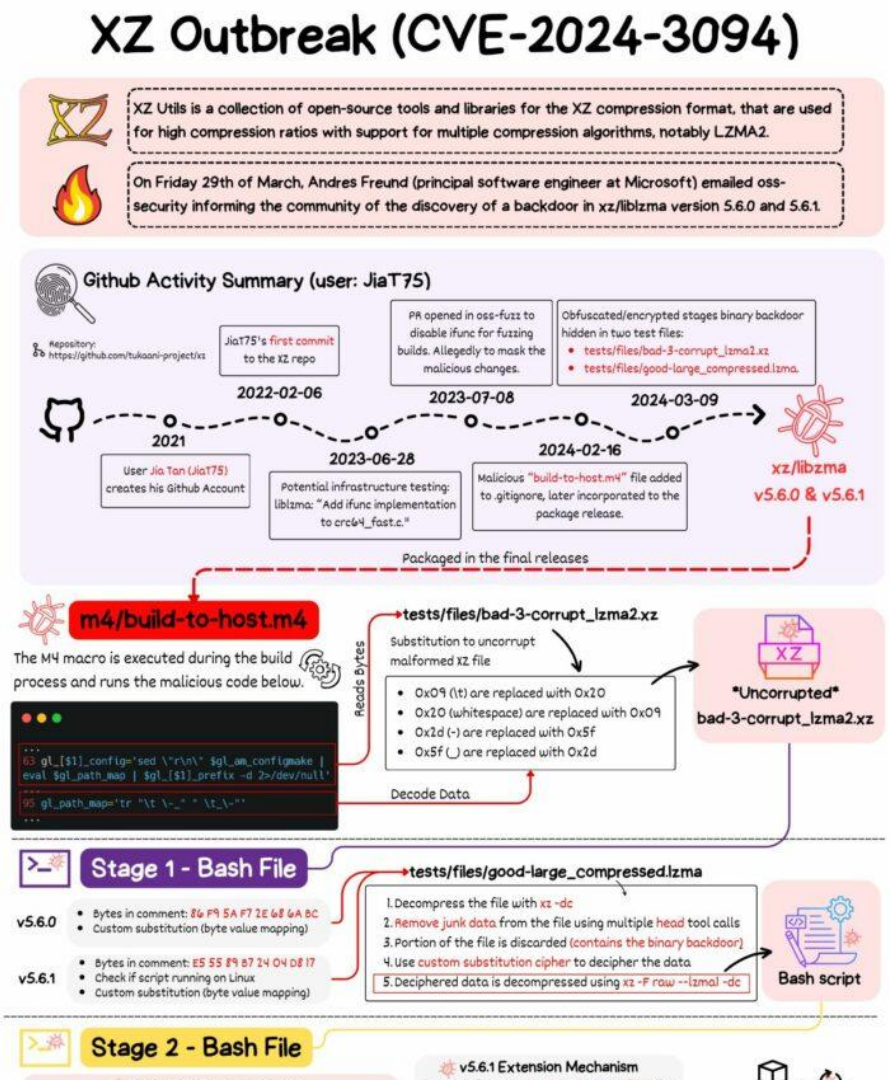
New EU cybersecurity rules ensure more secure hardware and software products

#DigitalEU #SecurityUnion #Cybersecurity

#SOTEU

SEPTEMBER 2022 – UPDATED **DECEMBER 2023**

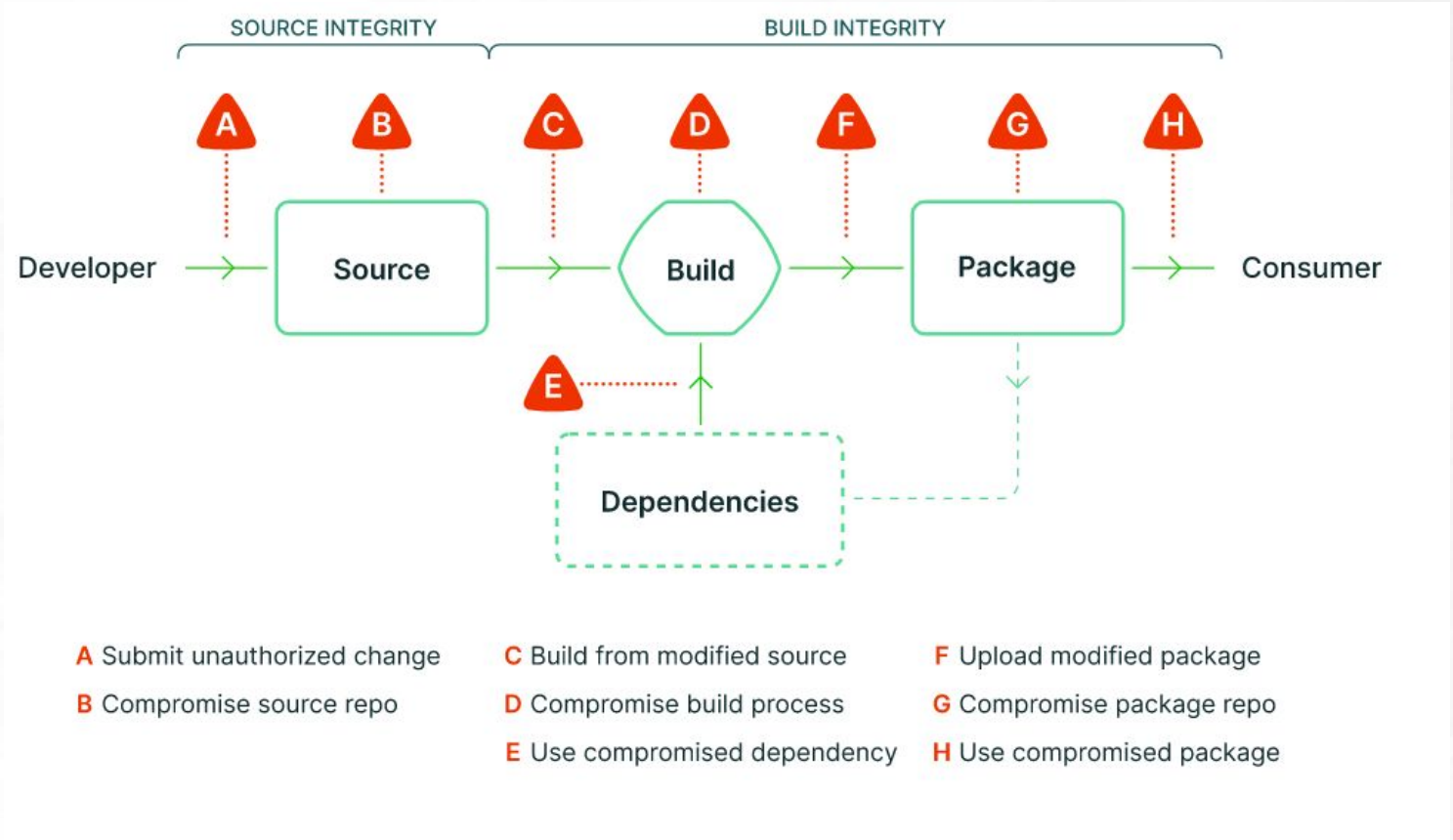
HACK IN BO Spring 2024 Edition
22ª EDIZIONE



One of the most dangerous attacks on the Linux supply chain, mitigated thanks to a lucky break.

How many **backdoors** remain undetected?

Risks in the Software Supply Chain



From: SLSA specification

Potential Threats

- ➔ Submit unauthorized change (to source repo)
- ➔ Compromise source repo
- ➔ Build from modified source
- ➔ Use compromised dependency
- ➔ Compromise build process
- ➔ Upload modified package
- ➔ Compromise package registry
- ➔ Use compromised package

- ➔ Dependency becomes unavailable

The JavaScript Supply Chain

*"Installing an **average** npm package introduces an implicit **trust** on **79 third-party packages and 39 maintainers**, creating a surprisingly large attack surface."*

https://www.researchgate.net/publication/331343484_Small_World_with_High_Risks_A_Study_of_Security_Threats_in_the_npm_Ecosystem

A massive ecosystem

npm statistics, 2023 (Sonatype)

- **2.5M** Total Projects
- **37M** Total Projects Versions
- **2.6T** 2023 Annual Request Volume
- **27%** YoY Project Growth
- **18%** YoY Download Growth
- **15** Average Versions Released per Project

The PHP Supply Chain

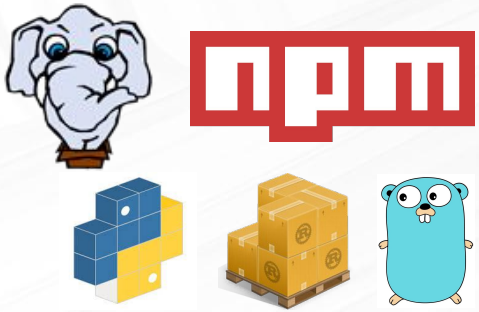
A MODERN PHP APPLICATION

Application

A MODERN PHP APPLICATION

Application

Dependencies

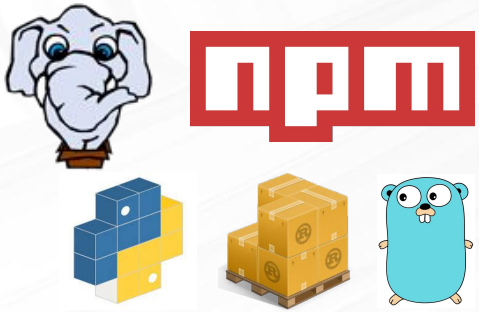


A MODERN PHP APPLICATION

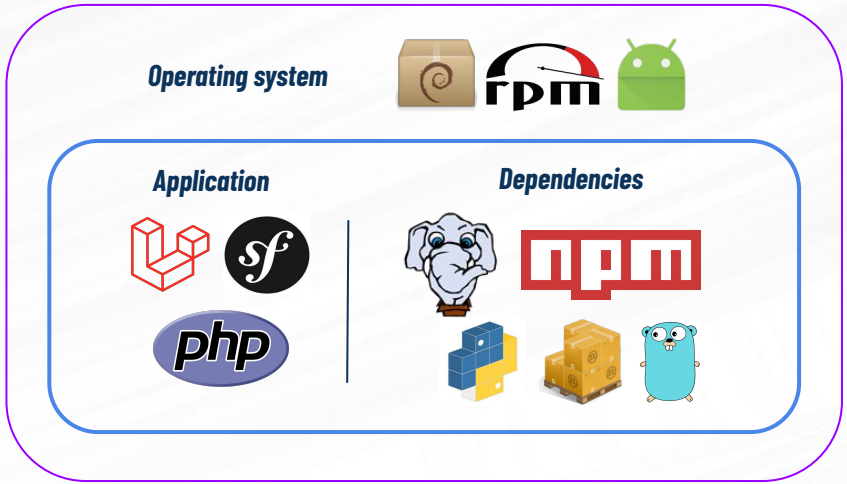
Operating system

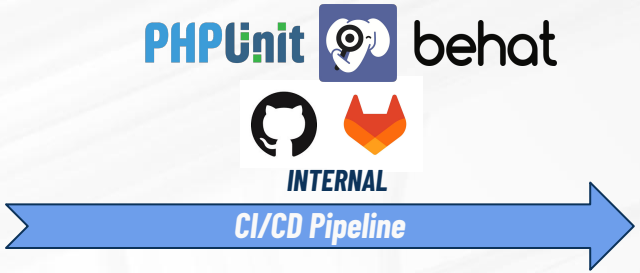
Application

Dependencies

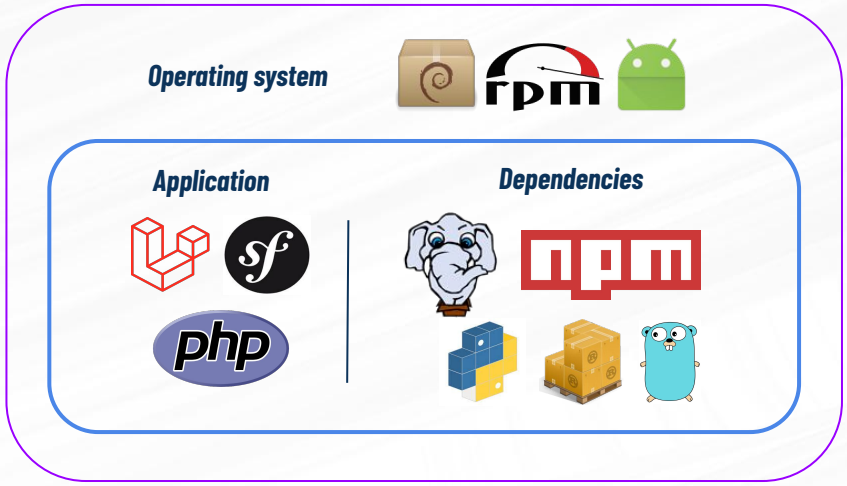


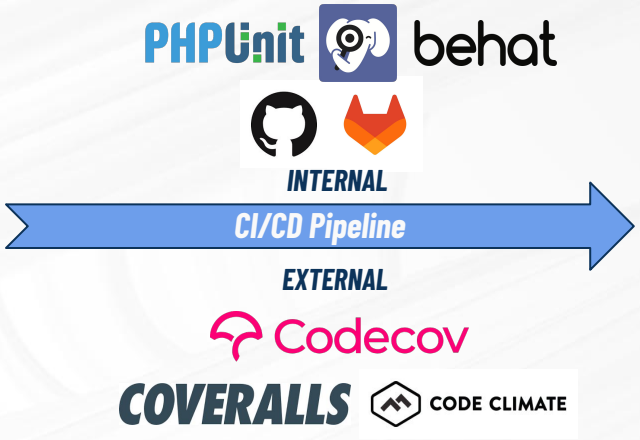
A MODERN PHP APPLICATION



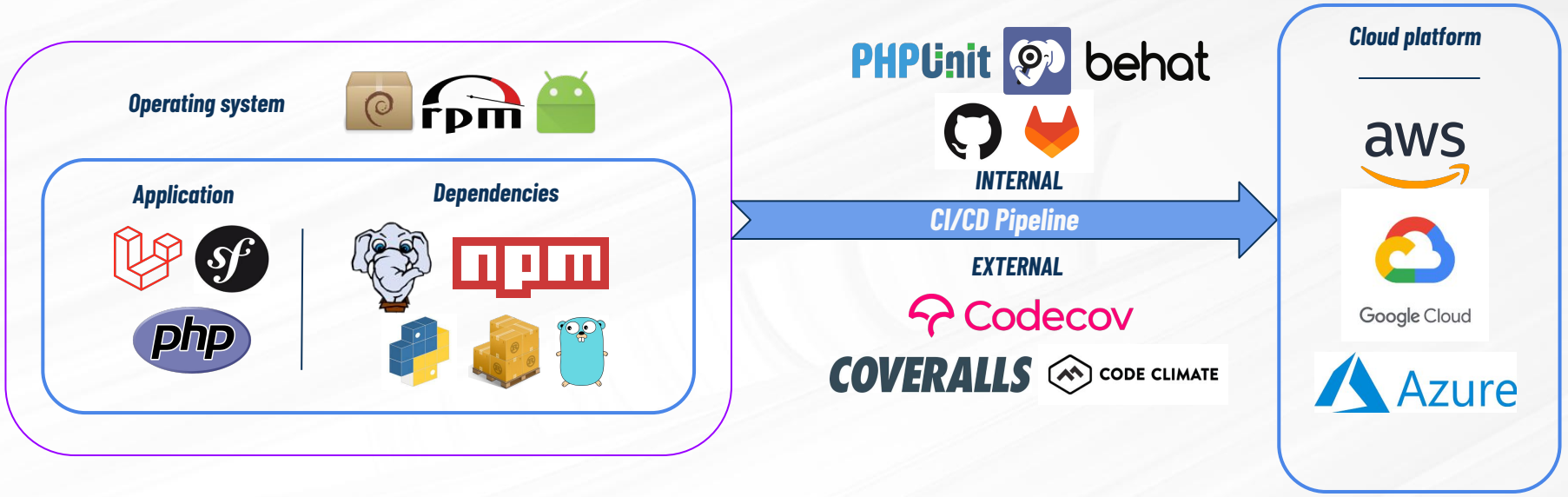


A MODERN PHP APPLICATION

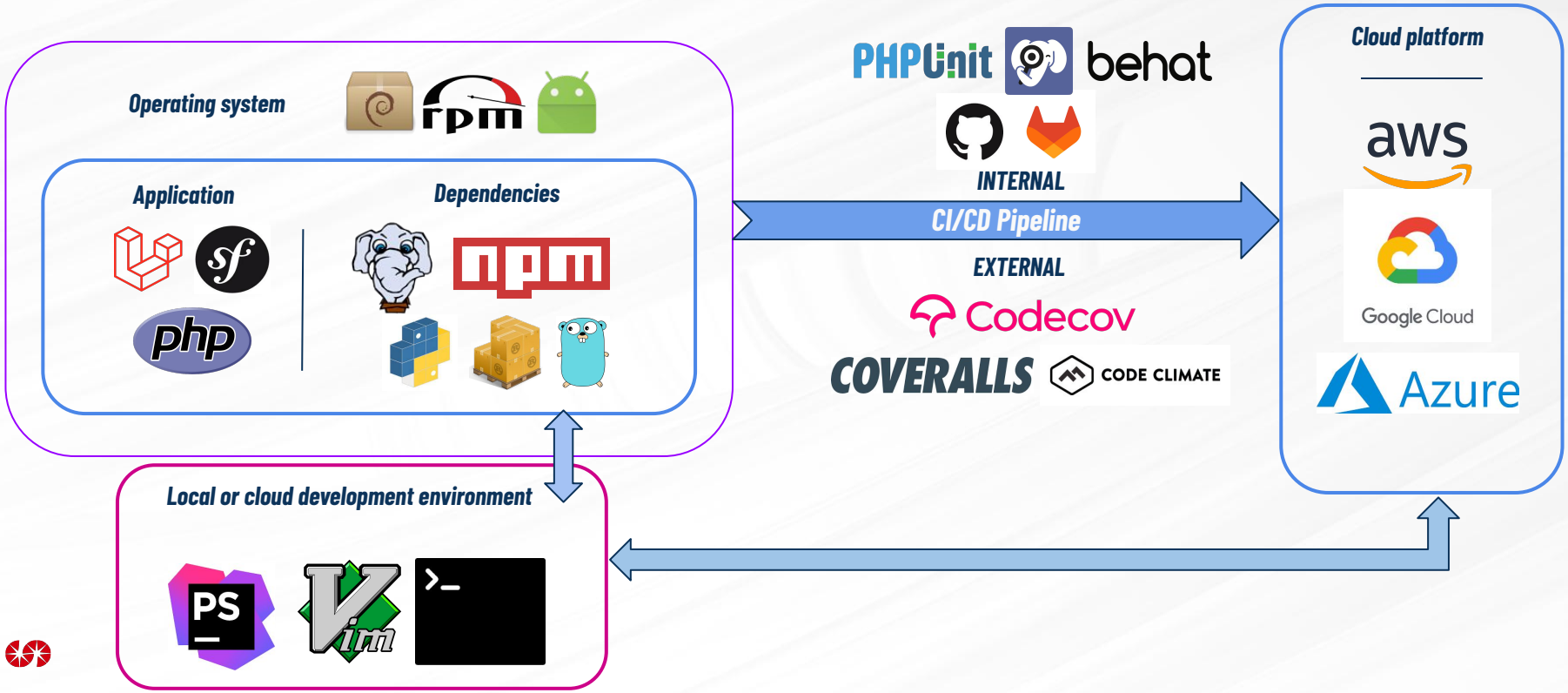




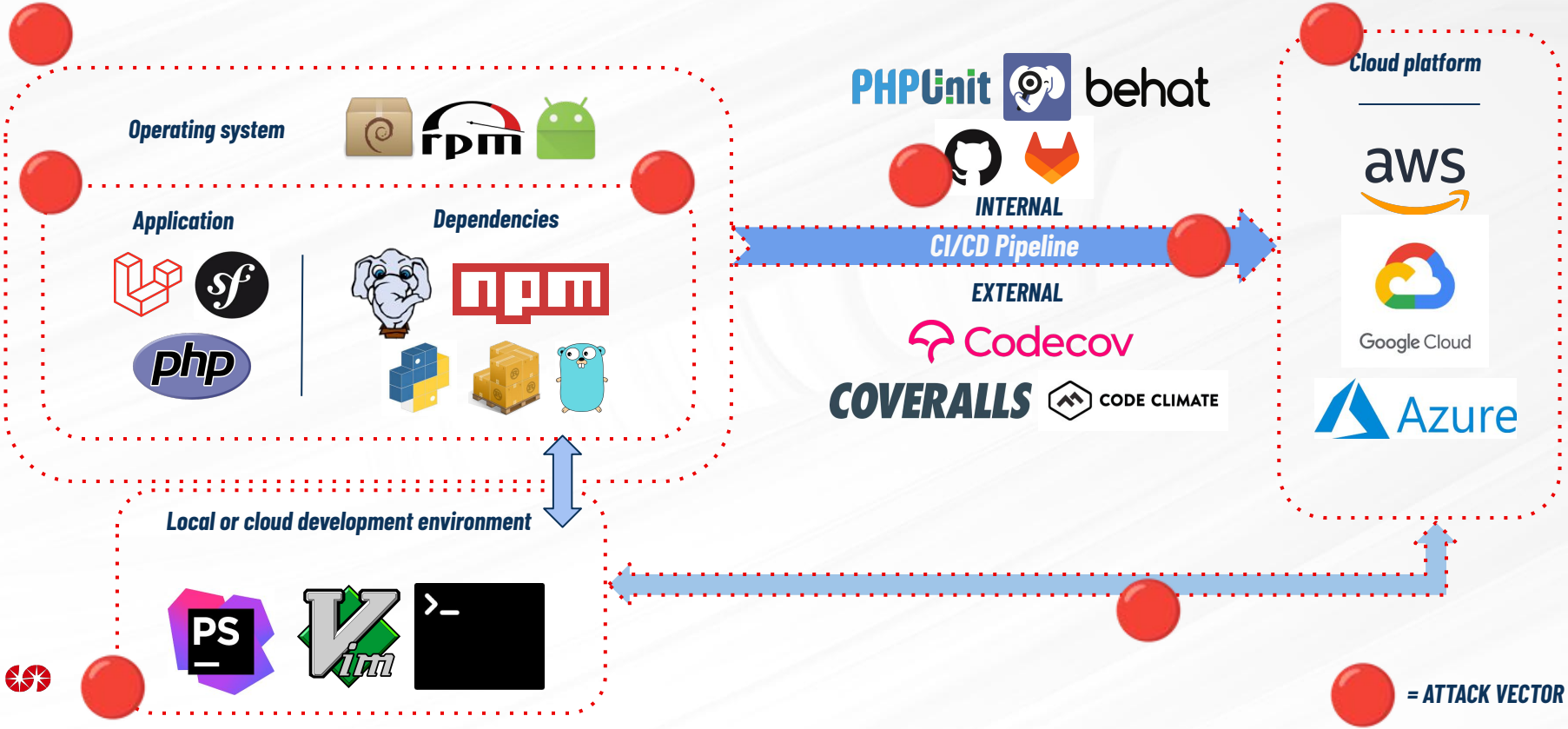
A MODERN PHP APPLICATION

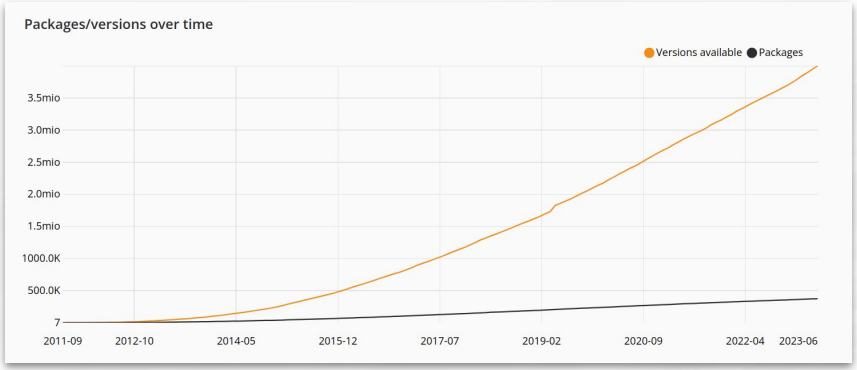


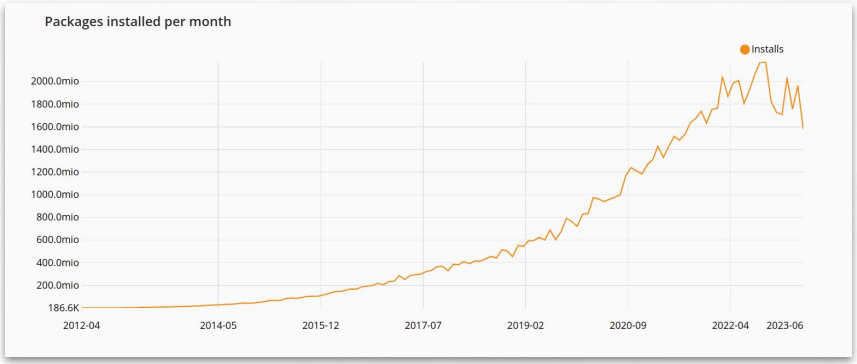
A MODERN PHP APPLICATION



A MODERN PHP APPLICATION







Composer statistics

- ➔ Created in 2012 by Nils Adermann and Jordi Boggiano
- ➔ The de facto standard for PHP package management
- ➔ packagist.org hosts over 300k packages and 2.5M revisions

What is a vulnerability

"A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability."

Common Vulnerabilities and Exposures (CVE) Program

Anything a threat actor can exploit to perform **malicious activity**

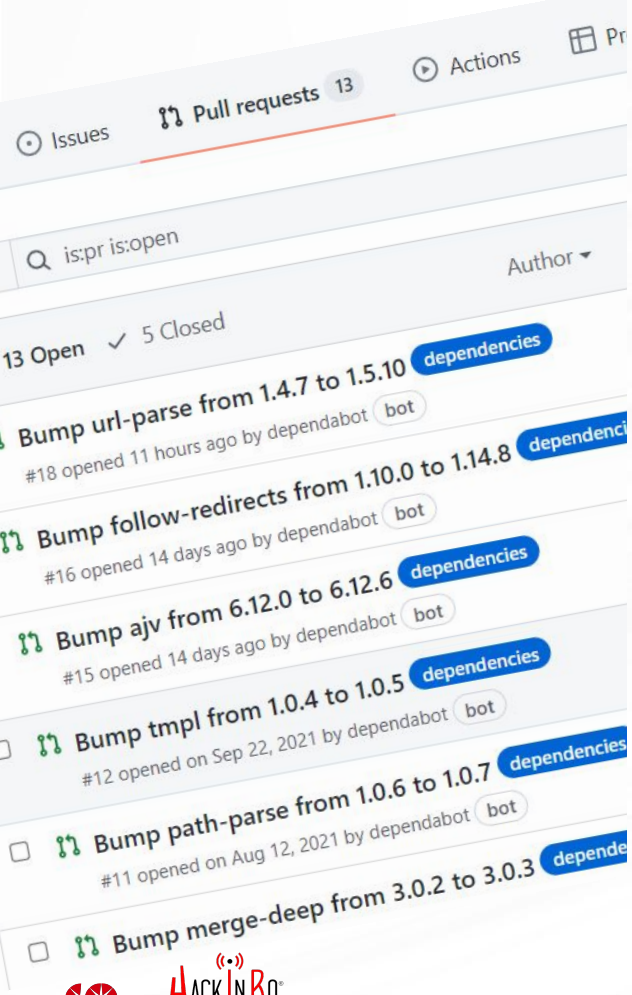
Dependencies are **crucial**

KNOW YOUR DEPENDENCIES

Dependabot

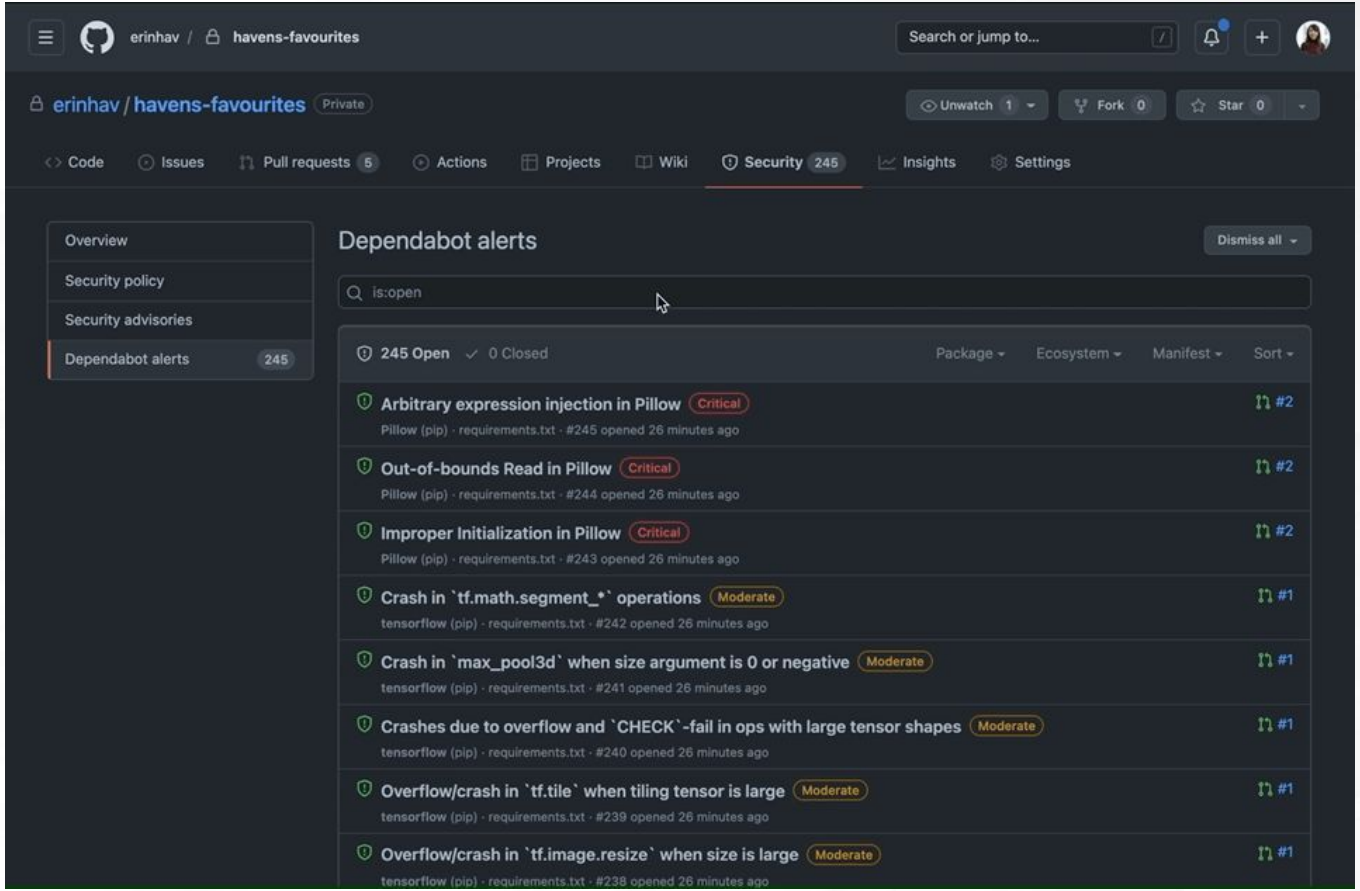
Automated dependency management

- Dependabot is a tool developed independently and then acquired by **GitHub** to **enhance security and development practices**
- It was developed to automate the process of **updating project dependencies**
- It helps developers to **keep their software up-to-date**
- It's now **fully integrated with GitHub**
- **The core is open source** with MIT License

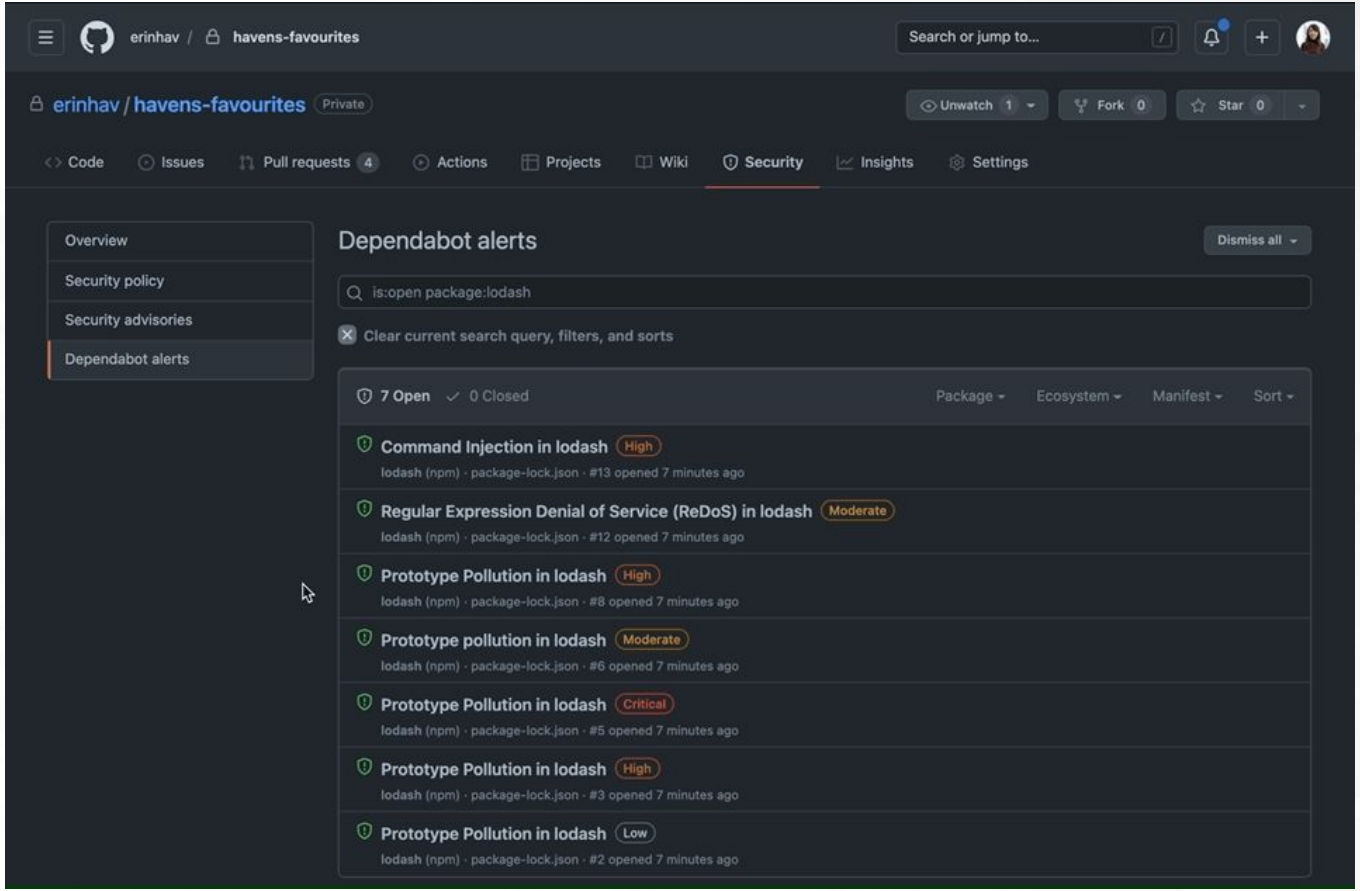


How does Dependabot work

- ➔ **Scans repositories** for outdated or insecure dependencies
- ➔ **Opens pull requests** to update dependencies to the latest version
- ➔ Can be configured to **run at specified intervals**
- ➔ **Provides alerts** for vulnerabilities found in current dependencies
- ➔ Support **private** and **public** repositories on GitHub
- ➔ Can be integrated with other SCM like **GitLab**



Demo of Dependabot alerts

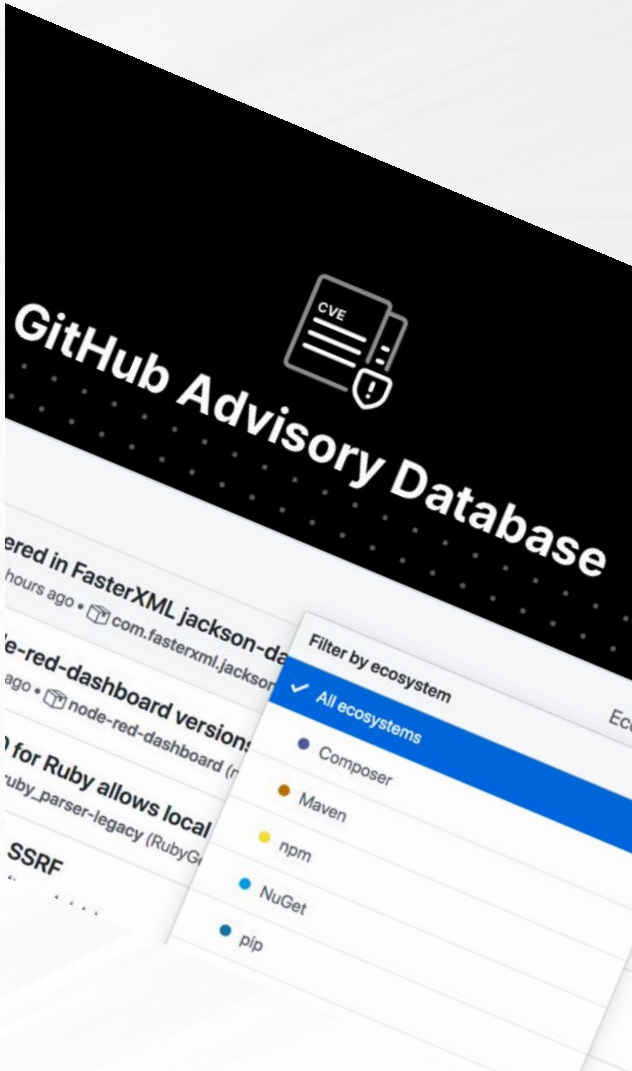


Dependabot update integration demo

Where is the **vulnerabilities information** coming from

GitHub Advisory Database

- Dependabot alerts are powered by the **GitHub Advisory Database** `https://github.com/advisories`
- This is the **largest vulnerability database** available worldwide
- It's maintained by a **dedicated team of curators** and supported by community contributions
- Security advisories are published as JSON files in the **Open Source Vulnerability (OSV)** format
- The GitHub Security Advisories monitor several sources for vulnerabilities, the most prominent of which is the **National Vulnerability Database (NVD)**



National Vulnerability Database

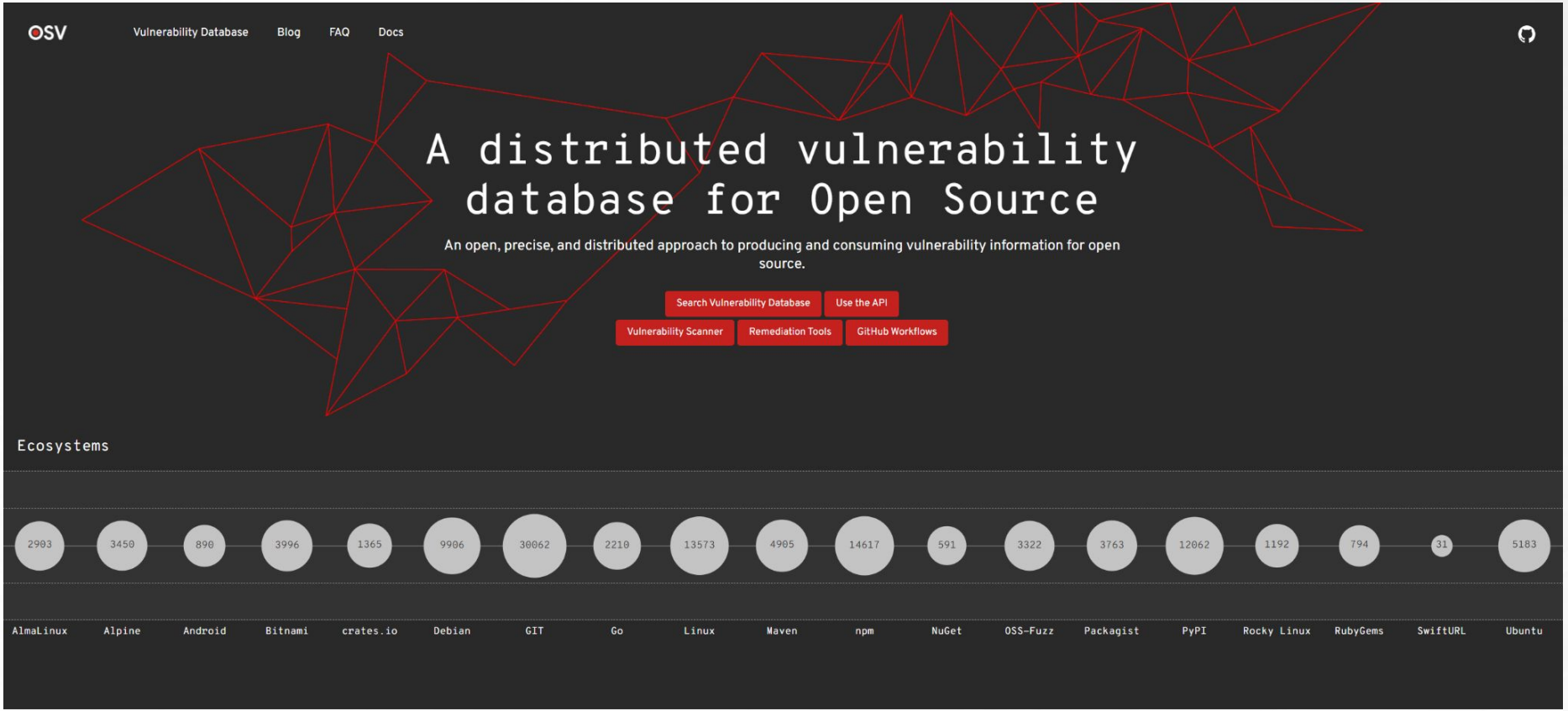
- The NVD is the **US government repository** for vulnerability management data
- It represents this data using the **Security Content Automation Protocol (SCAP)**
- It's managed by the US government agency the **National Institute of Standards and Technology**
- All vulnerabilities are assigned a **Common Vulnerabilities and Exposures (CVE)** identifier
- It scores vulnerabilities using the **Common Vulnerability Scoring System (CVSS)**

CVE identifiers

- The **CVE Program** was launched in 1999
- The primary purpose is to **uniquely identify vulnerabilities**
- A publicly disclosed security issue is assigned a **CVE ID number**
- CVE associates **specific versions** of a software or library to the vulnerability
- Using CVEs ensures **consistent referencing** and sharing of information

Common Vulnerabilities & Exposures

Are there **other** databases?

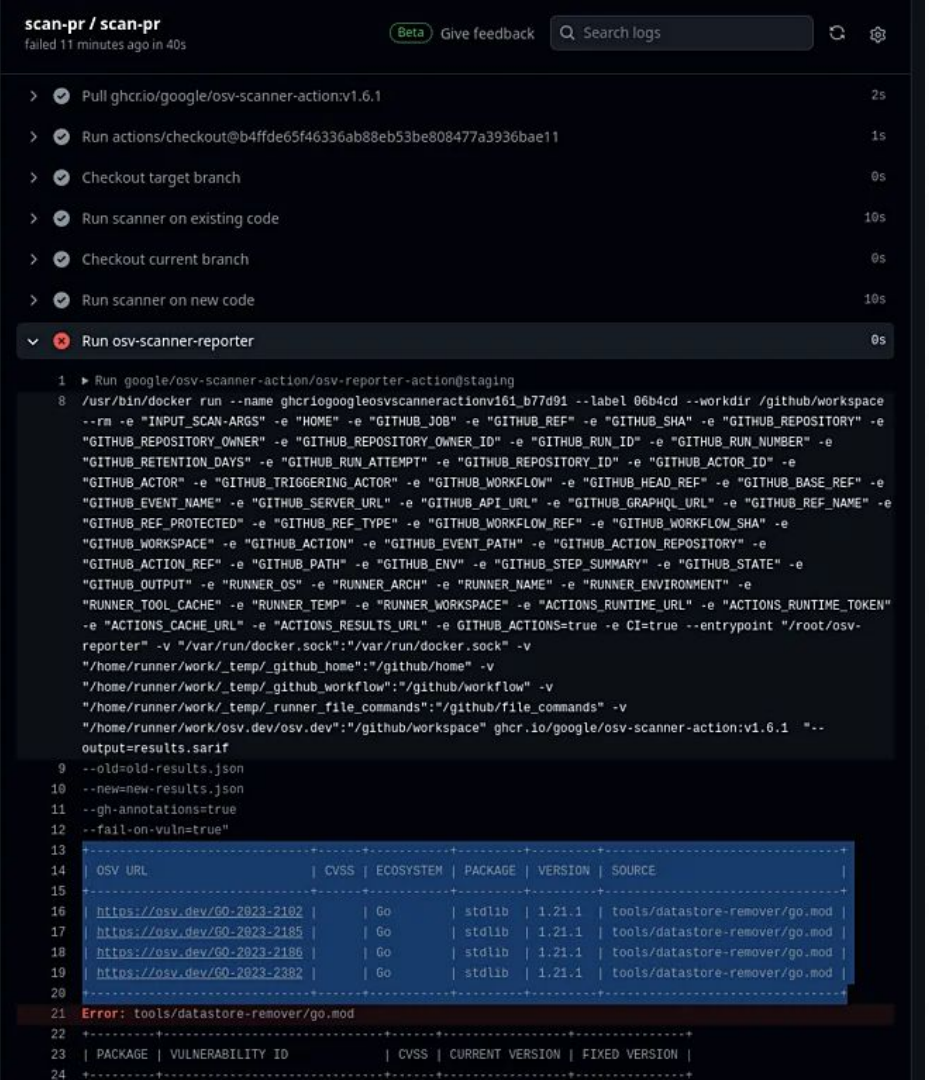


osv.dev homepage

Open Source Vulnerability DB

- ➔ OSV was **launched in 2004**
- ➔ OSV is an **open and distributed approach** to producing and consuming vulnerability information for Open Source Software
- ➔ **OSV Schema** introduced in 2021 is a **data format** to describe vulnerabilities that map to precise version
- ➔ OSV Schema **created by members of OpenSSF** and hosted by the foundation
- ➔ OSV serves as **aggregator of vulnerability db** that have adopted the schema, including GitHub Advisory, PyPA, RustSec etc...

Scanning vulnerabilities with **different tools**



OSV-Scanner

- ➔ Tool written in Go that **scans the project dependencies** to link them with known vulnerabilities
- ➔ Frontend to the **OSV database**
- ➔ **Analyses all transitive dependencies**, manifests, SBOMs and commit hashes
- ➔ OSV-Scanner is integrated into **OpenSSF Scorecard**

Renovate

- ➔ **Multi-platform** automatic dependency updates
- ➔ Dependabot **competitor**
- ➔ **Customizable** via config file
- ➔ Supports **many different SCM**
- ➔ Can be **self-hosted**
- ➔ Open Source with **AGPL**

Snyk Open Source

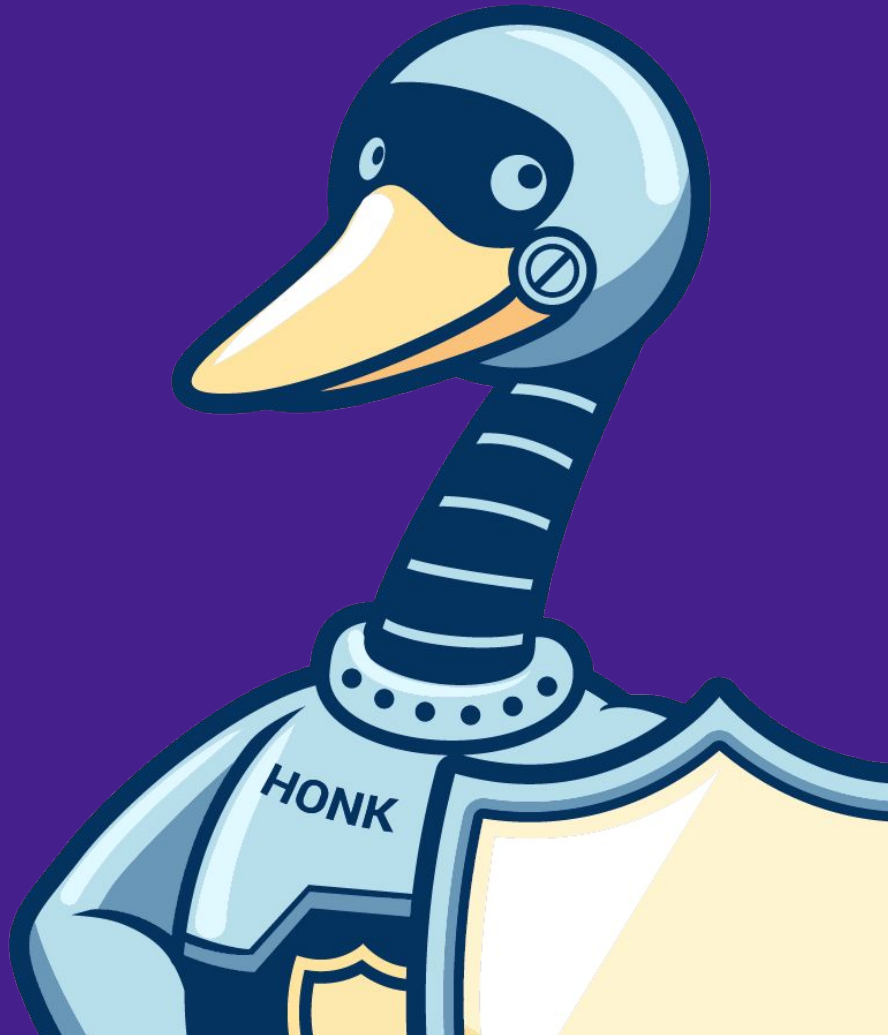
- **Snyk Open Source** is a vulnerability scanner part of the Snyk Platform
- Snyk is a **member of OpenSSF**
- It also scans for **licensing issues**
- Can be integrated in **any step of the SDLC**
- Uses the **Snyk Vulnerability Database**
- Can **automatically fix vulnerabilities** from the command-line, code editor or CI/CD pipeline

Best practices for vulnerability scanning

What to look for in an open source security tool

- **Comprehensive view** of packages and vulnerabilities affecting them
  - Are you depending on vulnerable components?
- **Automation**
  - Set policies around fixes, pull requests, patches, and upgrades
- **Integrations** with developer tools, workflows, and pipelines
  - Developers should easily see and apply fixes
- **Up-to-date and enriched database** that goes beyond known CVEs
  - Look beyond public databases for proprietary, curated databases
- **Continuous monitoring** of projects
  - Applications should monitor themselves and be equipped to defend themselves against attacks

How can you contribute?



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Ways to Participate

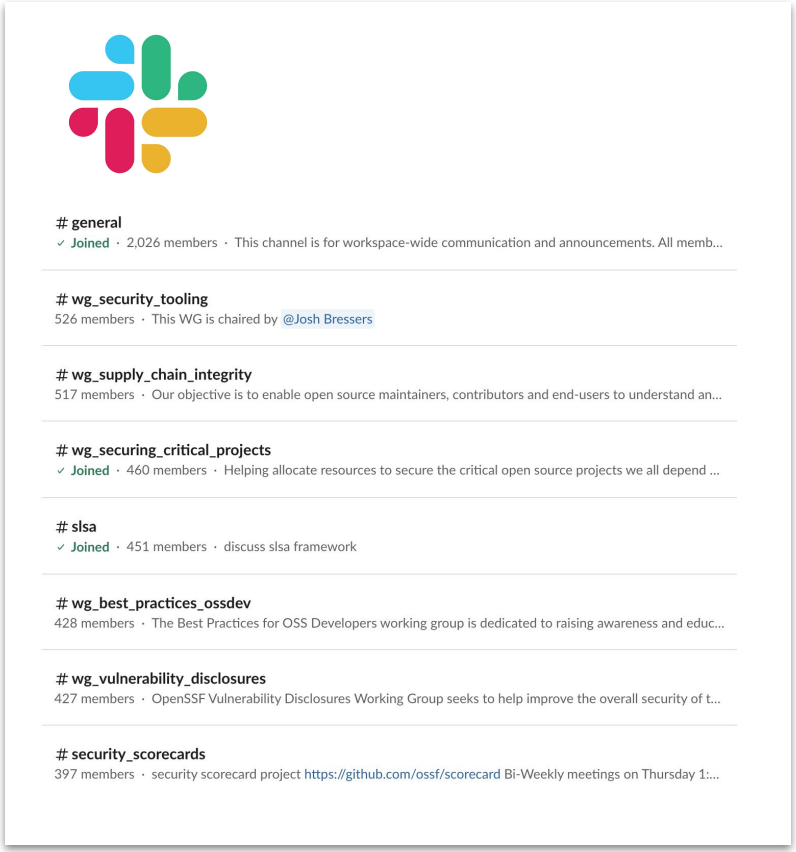
- **Join the OpenSSF Mailing List**
- Follow us on LinkedIn
- Follow us on Mastodon
- Follow us on Facebook
- Subscribe to our YouTube Channel
- Follow us on X
- Join a Working Group/Project
- **Access the Public Meetings Calendar**
- **Participate on Slack**
- Follow OpenSSF on GitHub
- Become an Organizational Member

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Attend a Public Meeting

bit.ly/ossf-calendar

OpenSSF
OPEN SOURCE SECURITY FOUNDATION



Message on Slack

slack.openssf.org

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Follow us on Social Media

X
@openssf

LinkedIn
OpenSSF

Mastodon
social.lfx.dev/
@openssf

YouTube
OpenSSF

Facebook
OpenSSF

Thank you.

Edoardo Dusi

Developer Relations Engineer @ SparkFabrik

edoardo.dusi@sparkfabrik.com

HACK IN BO®
Spring 2024 Edition
22ª EDIZIONE

@edodusi

@edo@continuousdelivery.social