



DrupalCon

LILLE2023
17-20 OCTOBER

WHAT IS THE
SECURE SOFTWARE SUPPLY CHAIN
AND THE CURRENT STATE OF THE
PHP ECOSYSTEM



Paolo Mainardi

- Co-founder and CTO @[Sparkfabrik](#)
- [Drupal.org profile](#) - [Webprofiler module](#) ([lussoluca](#))
- [Linux Foundation Europe Advisory Member](#)
- Blog: [paolomainardi.com](#)
- [linkedin.com/in/paolomainardi](#)
- [continuousdelivery.social/@paolomainardi](#)
- [paolo.mainardi@sparkfabrik.com](#)



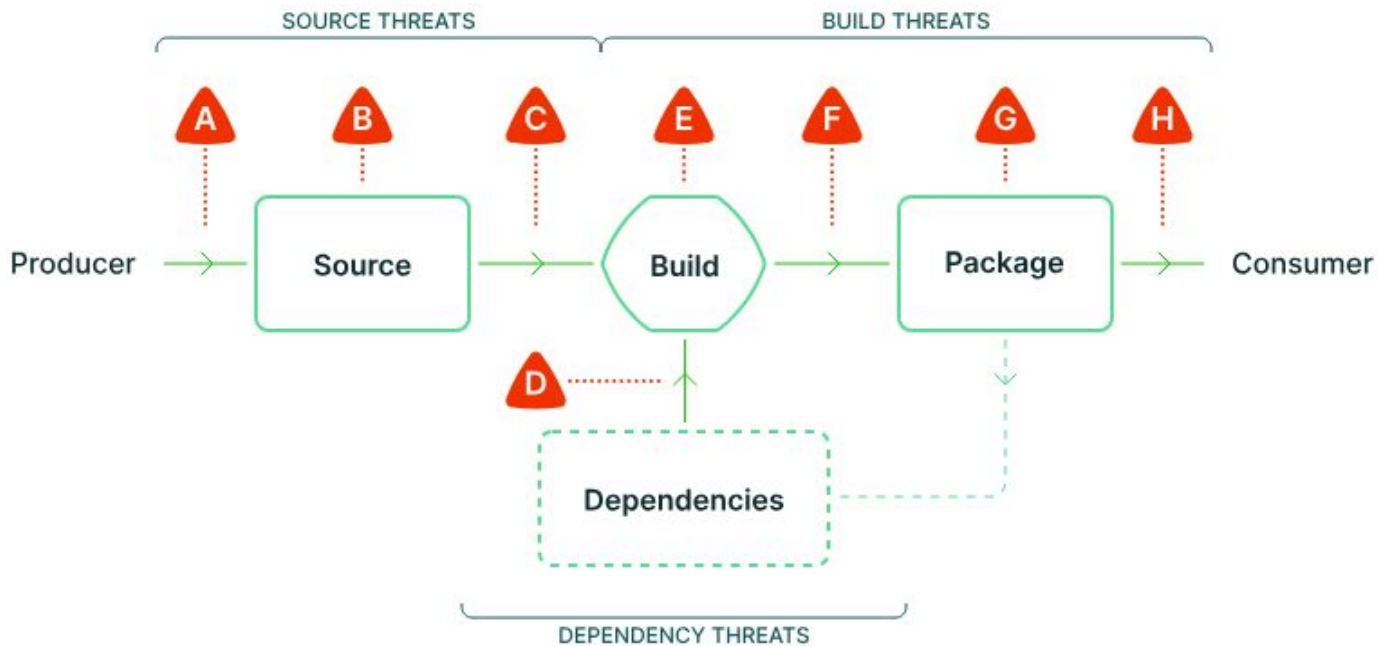
THE SESSION

- What is a **Software Supply Chain**
- State of the **PHP** ecosystem
- Threats and mitigations with **digital signatures, attestations** and **SBOM**
- DEMO



“A supply chain is a network of individuals and companies who are involved in creating a product and delivering it to the consumer”





SOURCE THREATS

- A** Submit unauthorized change
- B** Compromise source repo
- C** Build from modified source

DEPENDENCY THREATS

- D** Use compromised dependency

BUILD THREATS

- E** Compromise build process
- F** Upload modified package
- G** Compromise package repo
- H** Use compromised package



A MODERN DRUPAL APPLICATION

Application



A MODERN DRUPAL APPLICATION

Application



Dependencies



A MODERN DRUPAL APPLICATION

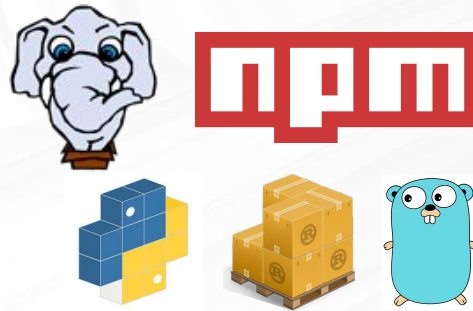
Operating system



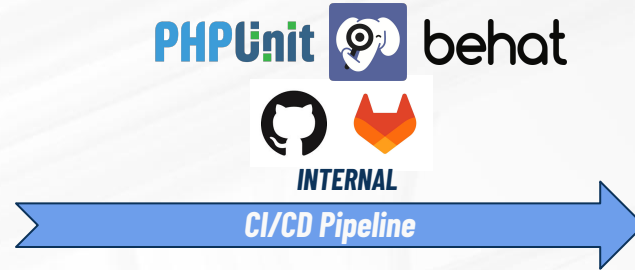
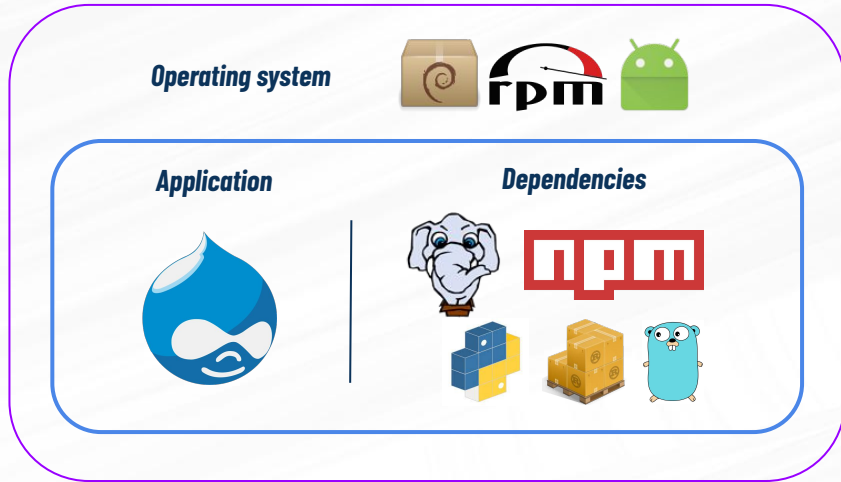
Application



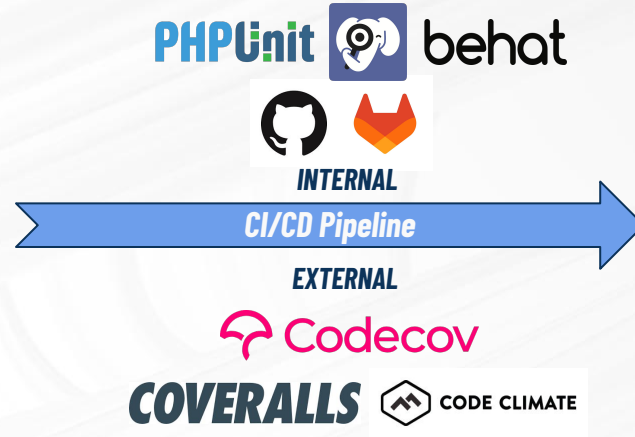
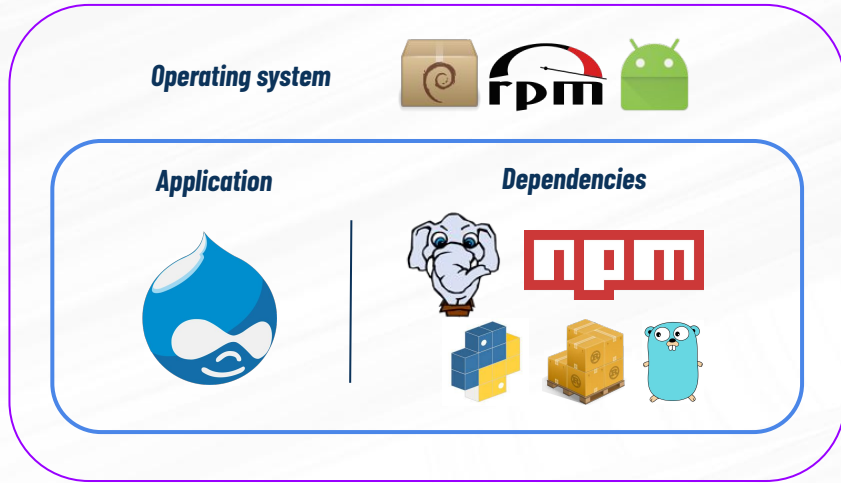
Dependencies



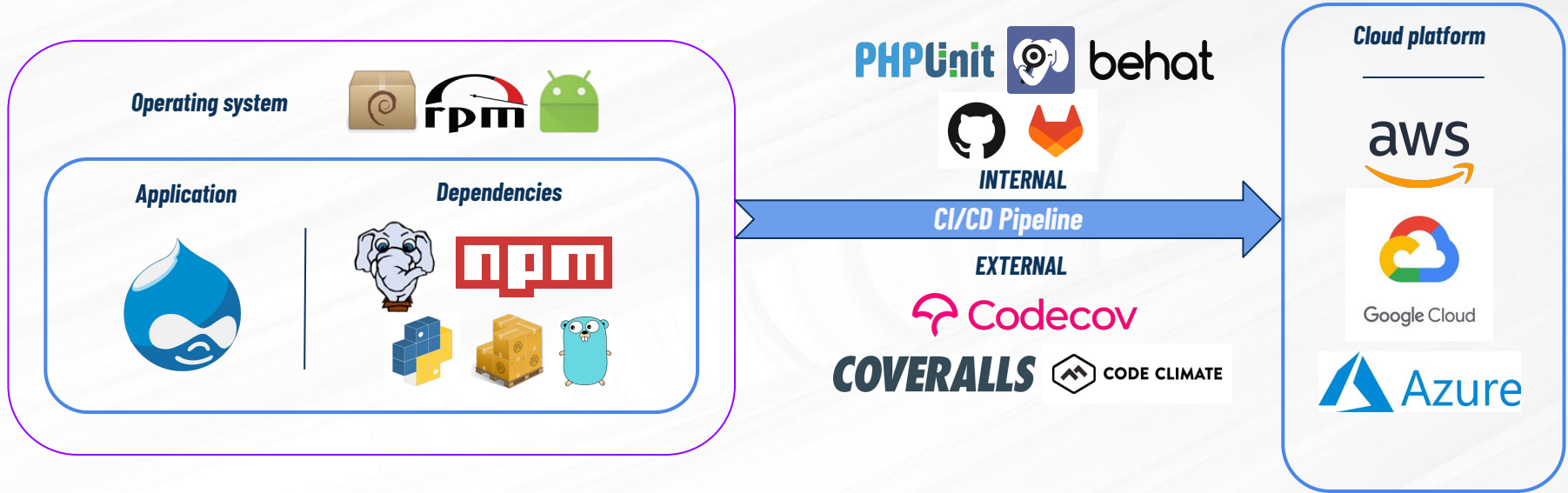
A MODERN DRUPAL APPLICATION



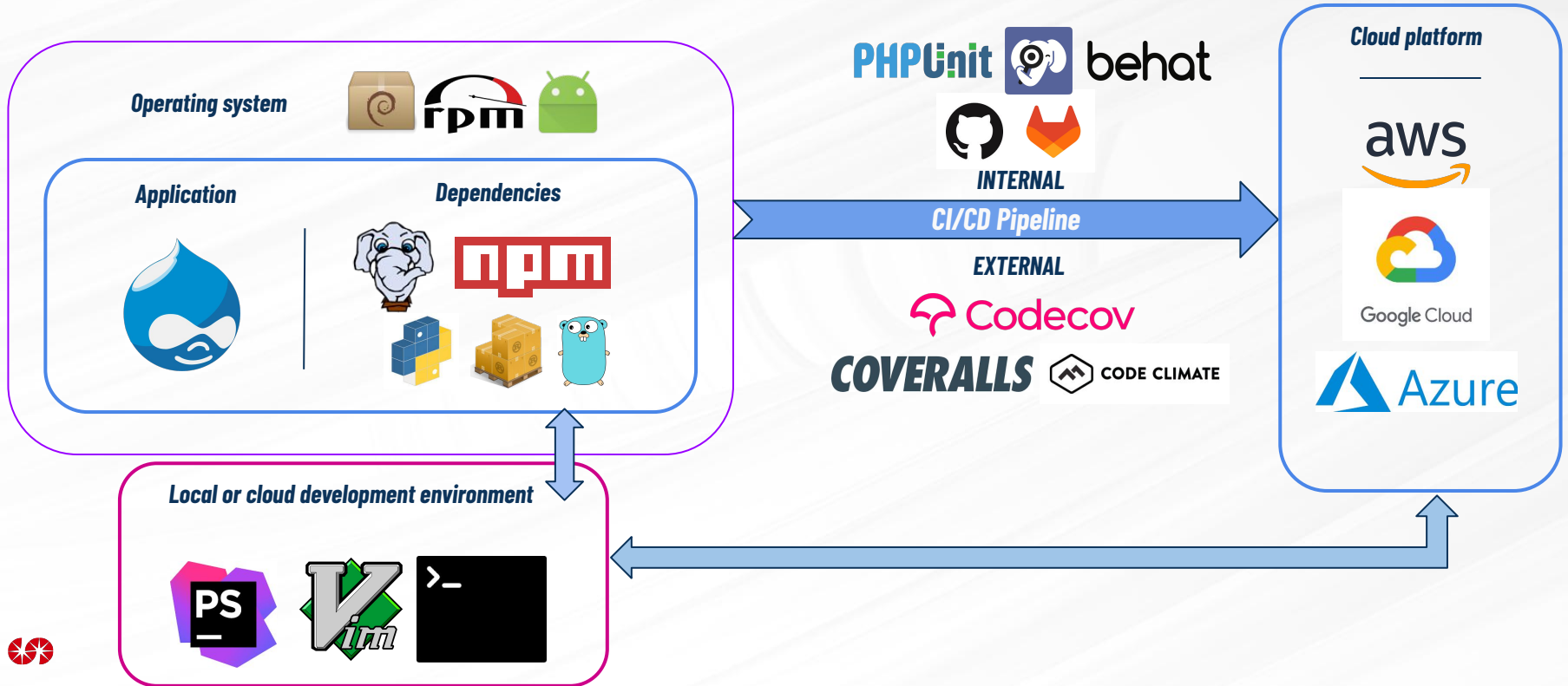
A MODERN DRUPAL APPLICATION



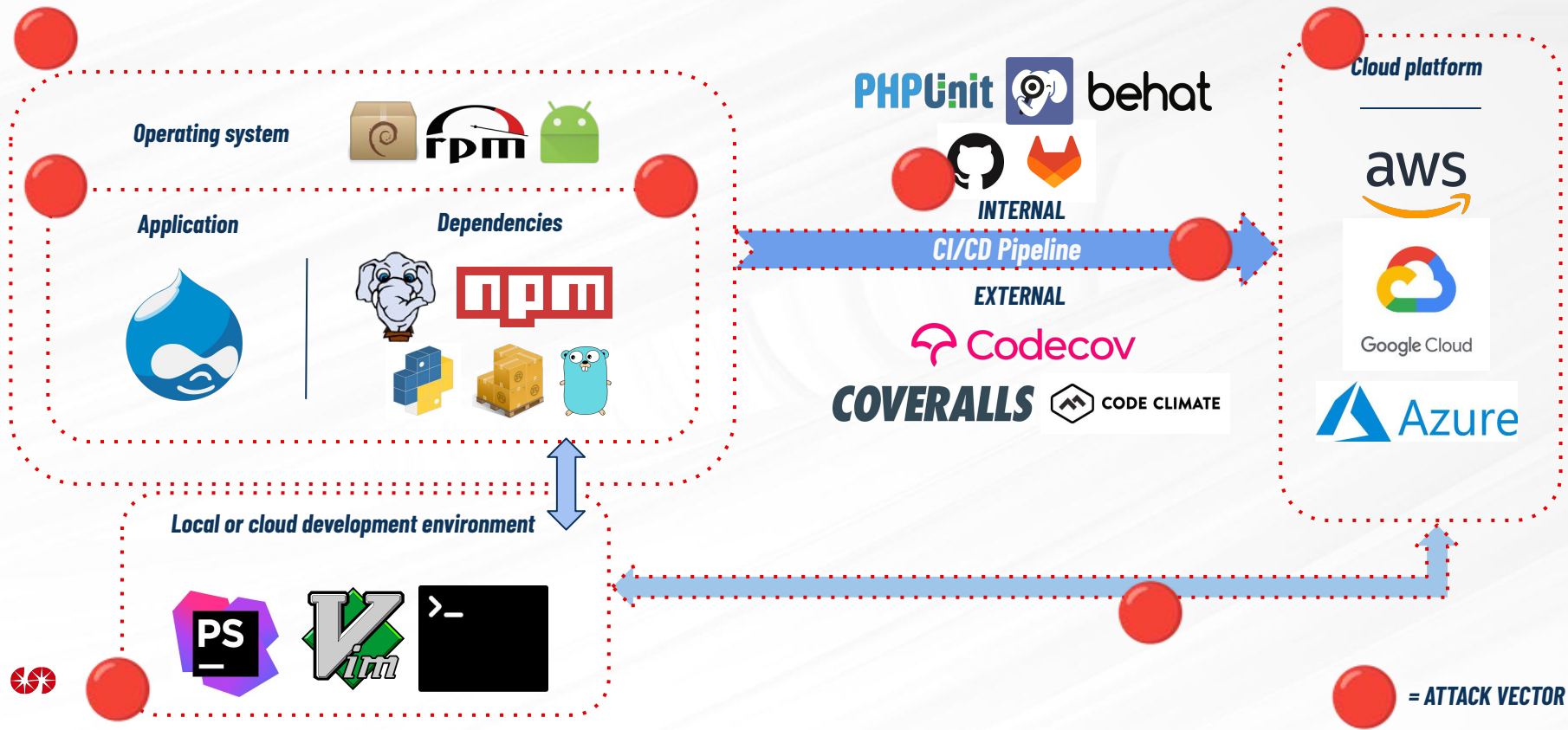
A MODERN DRUPAL APPLICATION



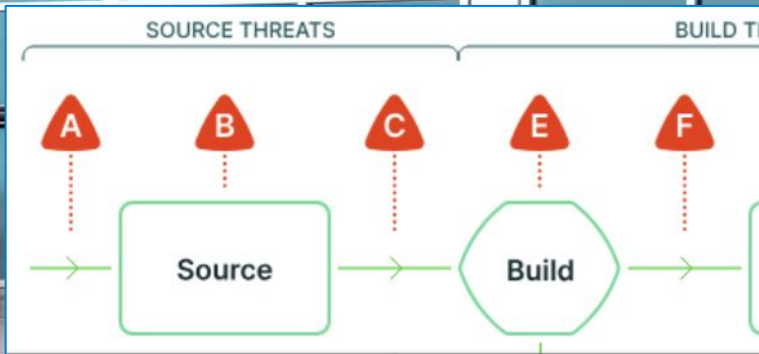
A MODERN DRUPAL APPLICATION



THREATS IN THE SUPPLY CHAIN



= ATTACK VECTOR

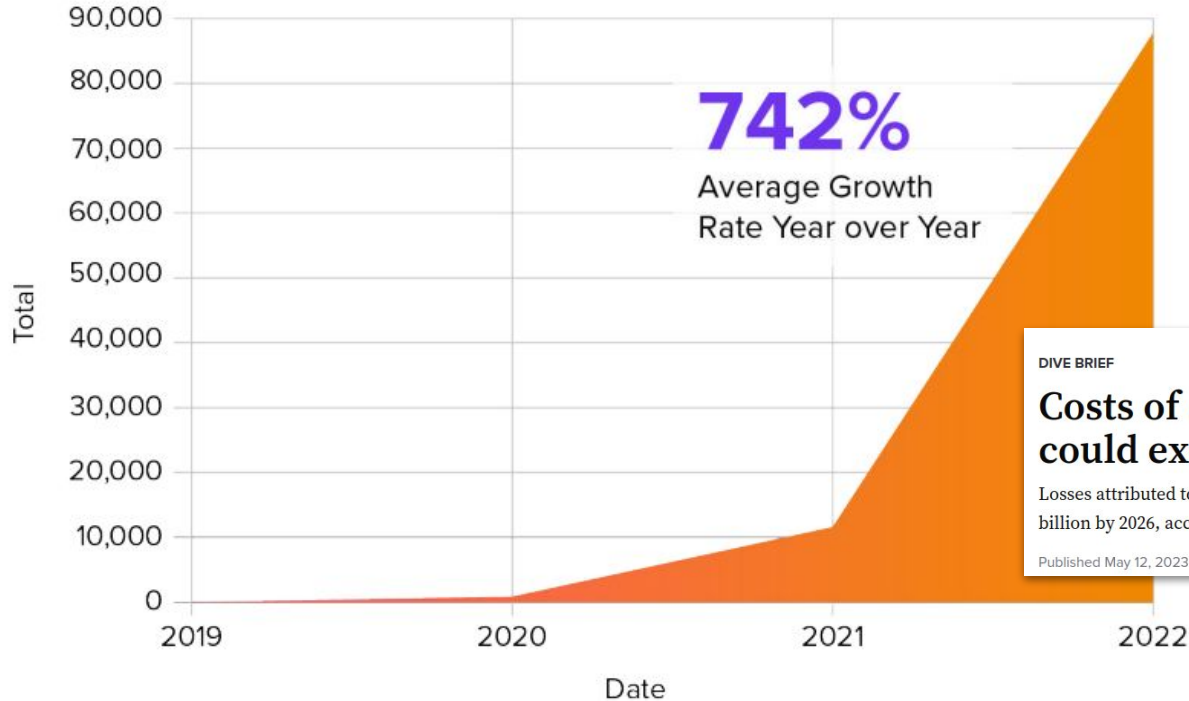


solarwinds

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 Security etc.

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>



NATIONAL CYBERSECURITY STRATEGY

MARCH 2023



EUROPEAN
COMMISSION

Brussels, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

**on horizontal cybersecurity requirements for products with digital elements and
amending Regulation (EU) 2019/1020**

CE



CALL TO ACTION FOR THE LINUX FOUNDATION EUROPE OPEN SOURCE COMMUNITY

Cyber Resilience Act: it's time to act!

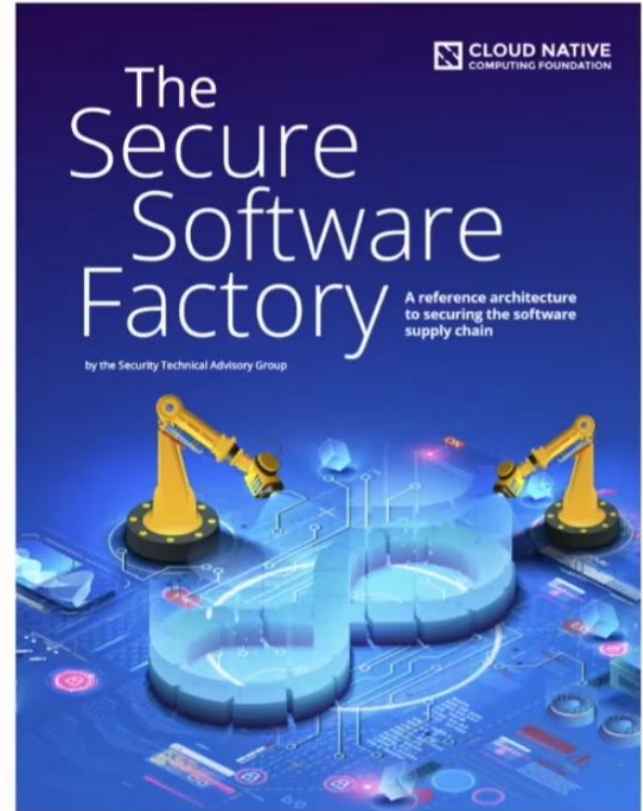
The [European Union's Cyber Resilience Act](#) (CRA) legislation is making its way through the legislative process, currently being discussed within the European Parliament (Rapporteur is [Nicola Danti](#)) and the [European Council](#). Several key milestones in the coming weeks and the potential to be approved within the year, so time is of the essence.

While the Linux Foundation vehemently shares the goal to bolster security of the software supply chain, with the [Open Source Security Foundation](#) being the most concrete example of our commitment, **there's broad consensus that the way the Act is currently drafted inadvertently risks imposing a major burden on open source contributors and non-profit foundations**. If you are not familiar with this, please take a look at this comprehensive list of reactions compiled by the [Open Source Initiative](#).



<https://linuxfoundation.eu/cyber-resilience-act>





@lumijb

[Keynote: The Next Steps in Software Supply Chain Security - Brandon Lum, Software Engineer, Google](#)



STATE OF THE PHP ECOSYSTEM



PHP PACKAGE MANAGEMENT HISTORY

PEAR - PHP Extension and Application Repository

Created by **Stig Bakken**, with the goal to *"provide reusable components, lead innovation in PHP, provide best practices for PHP development and educate developers."*

Included in the PHP runtime.



1999



2004



2008

PHP 5.3 and PHP-FIG group

Namespaces and PSR-0 autoloading standard

2009

2010



2012

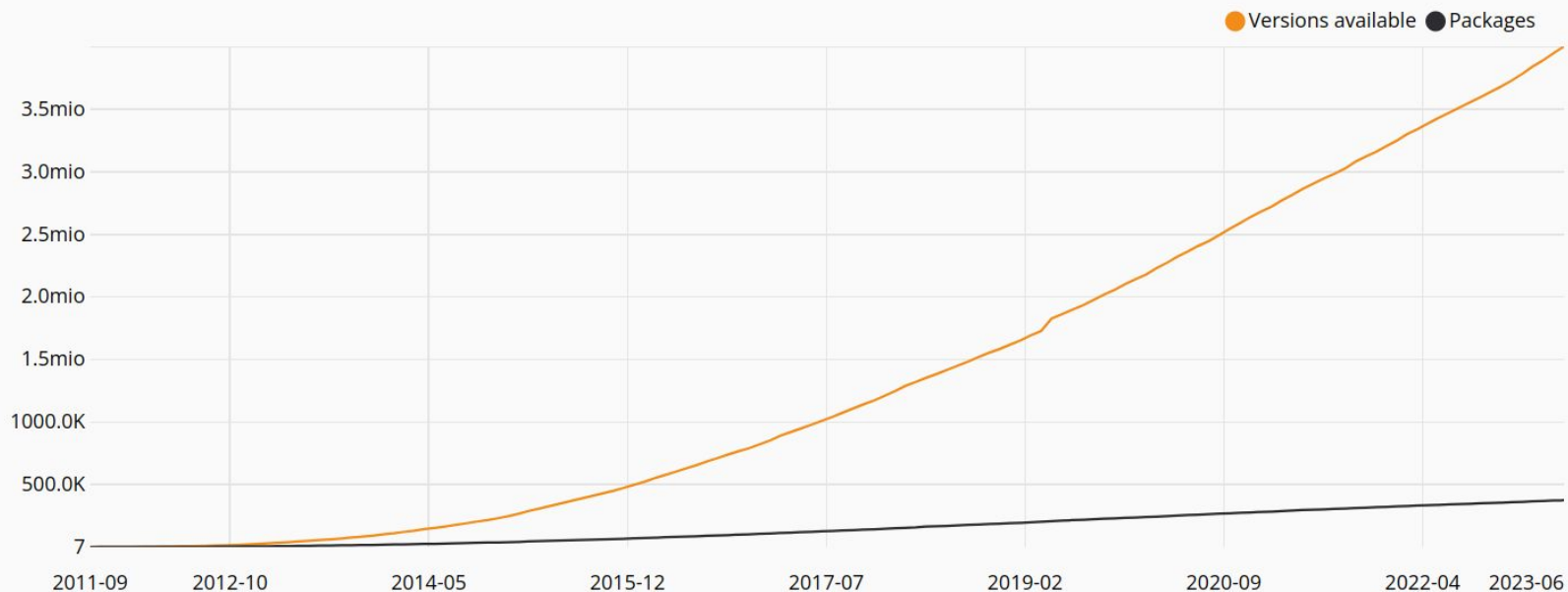
Composer

A modern and easy to use package manager, based on top of recent language improvements and ecosystem evolutions.



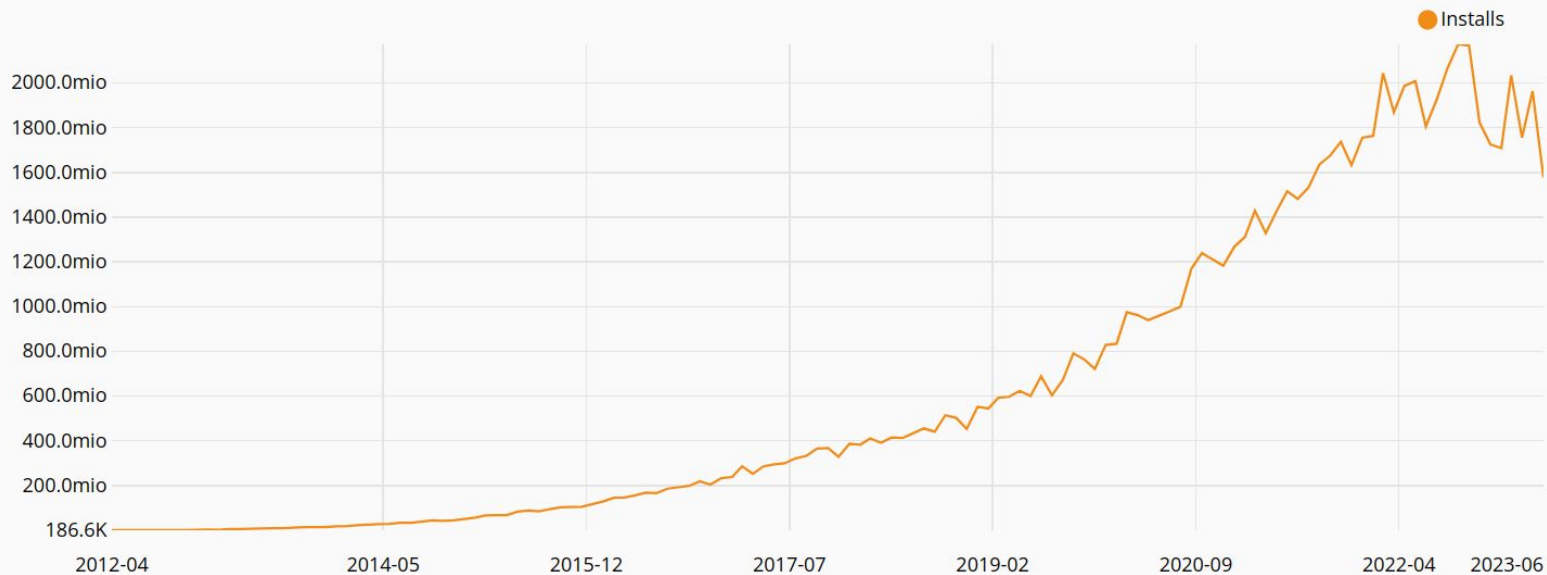
COMPOSER STATS: >300K PACKAGES AND +3.5M VERSIONS

Packages/versions over time



COMPOSER STATS: >2B INSTALLED PACKAGES PER MONTH

Packages installed per month



COMPOSER BUILT-IN SECURITY PROTECTIONS

composer require drupal / core-recommended : 10.1.0

Namespace Library name Version

Only vendor-namespaced packages allowed
(eg: NPM allows root packages)

2

Public
packagist.org



Code is always hosted on a git repository, only metadata goes on packagist.org
(eg: NPM hosts the code)

1

Custom
repositories
packages.drupal.org



Composer Repositories are Canonical by default.
(no dependency confusion)

<https://blog.packagist.com/preventing-dependency-hijacking>



THE LATEST SUPPLY CHAIN ATTACKS ON PHP

April 29, 2021

[PHP Supply Chain Attack on Composer](#)

“A critical vulnerability in the source code of Composer which is used by Packagist. It allowed us to execute arbitrary system commands on the Packagist.org server”

October 4, 2022

[Securing Developer Tools: A New Supply Chain Attack on PHP](#)

“A new critical vulnerability in similar components. It allowed taking control of the server distributing information about existing PHP software packages, and ultimately compromising every organization that uses them”

March 29, 2022

[PHP Supply Chain Attack on PEAR](#)

“In this article we present two bugs, both exploitable for more than 15 years. An attacker exploiting the first one could take over any developer account and publish malicious releases, while the second bug would allow the attacker to gain persistent access to the central PEAR server.”

May 3, 2023

[Packagist.org maintainer account takeover](#)

“An attacker accessed an inactive account on Packagist.org for a period of time but still had access to a total of 14 packages. The attacker forked each of the packages and replaced the package description in composer.json with their own message but did not otherwise make any malicious changes”

And counting

<https://www.sonatype.com/resources/vulnerability-timeline>



SO WHAT ? WHERE SHOULD WE START ?



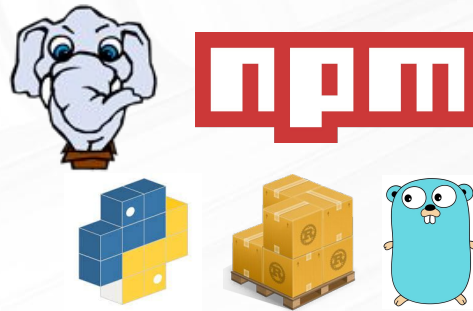
Operating system

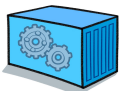


Application



Dependencies





OCI Image - <https://opencontainers.org>

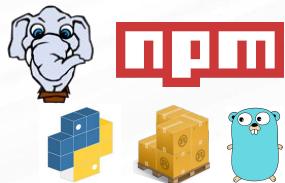
Operating system



Application



Dependencies



Dev environments

- A way to define **application and system dependencies** in a reproducible way with
- Dockerfile
- A **standard and agnostic artifact** to deploy on Kubernetes, Lambda, Cloud Run etc...
- **Cloud native tooling** (SBOM, Signatures etc..)



OCI IMAGES DEEP-DIVE



OCI stands for **Open Container Initiative**.

OCI defines the specifications and standards
for container technologies
(***Runtime, Image*** and ***Distribution*** spec).

Container registries can be also used to store
other kind of artifacts (like Helm charts)
or just ***any arbitrary files***.



What is the **trusting model** behind a Container Image,
or in general, a **digital artifact**?

How can i be sure that **what I'm running**
is coming from a **trusted source**?



Reflections on Trusting Trust

To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.

MORAL

The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code. 1

KEN THOMPSON

SECURE SOFTWARE SUPPLY CHAIN CHECKLIST

- ✓ Who built it, when and how
(Signatures and Provenance Attestations)
- ✓ The list of things who made the artifact
(SBOM - Software Bill of Material)



DIGITAL SIGNATURES 101

Integrity

Ensure the data signed was not altered.

Authenticity

Attest that the data was sent by the signer.

Non-repudiation

Ensure that the signer cannot deny the authenticity of the signature.



*Managing keys is **hard***

Distribution, Storage, Compromise



DIGITAL SIGNATURES - SIGSTORE

Sigstore is an OSS project under the umbrella of [OpenSSF](#) foundation.

Fast growing community and mainstream adopted

Used in **Kubernetes** and many other big vendors
(Github, Rubygems, Arch Linux etc..)



In collaboration with



DIGITAL SIGNATURES - SIGSTORE

Keyless signing of any software artifact

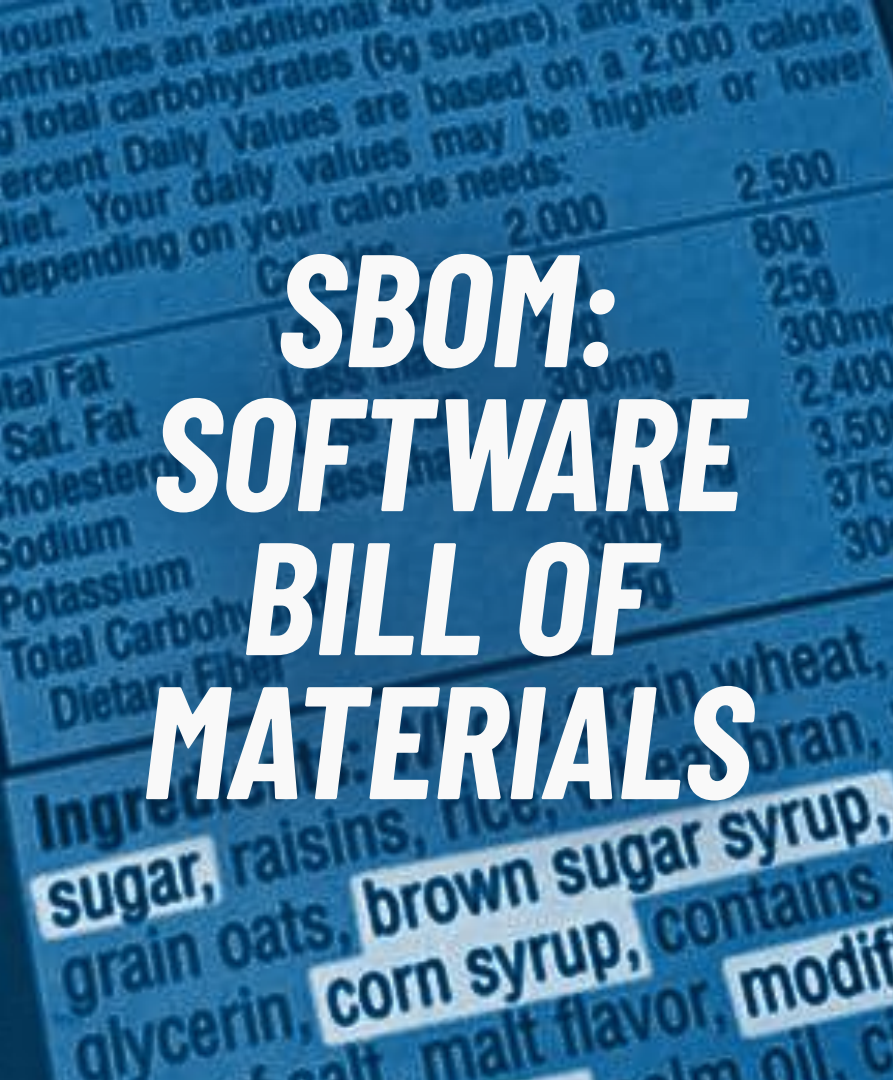
Signatures metadata are stored in a [public tamper-resistant log](#)

Signatures are stored alongside images in **OCI registry**



In collaboration with





SBOM: SOFTWARE BILL OF MATERIALS

***A list of “ingredients”
for a software artifact***

Can be used for:

- Vulnerability scanning
- Software transparency
- License policy
- Find abandoned dependencies

SBOM FOR CONTAINERS

Creating a SBOM for an artifact is a complex problem

Dependencies live at different levels:

- Operating system (Windows, Debian, Alpine etc...)
- Operating system dependencies (RPM, DEB, APK, PKG...)
- Application dependencies (Composer, NPM, Rubygems, Pypi, etc...)
- Static binaries and their dependencies (Go, Rust etc...)



SBOM - Tools



syft



aqua
trivy



\$ docker sbom



DEMO



DruBOM - Drupal Bill of Materials



<https://www.drupal.org/project/drubom>

DruBom is an Drupal module for generating a **Software Bill of Materials (SBOM)** from a **Drupal** installation.

It is still a work in progress, **any contribution is welcome:**
Syft integration, better scanning and data reporting, more SBOM formats, CI, tests, \$you name it



Join us for contribution opportunities

17-20 October, 2023
Room 4.1 & 4.2

Mentored Contribution

20 October : 09:00 – 18:00
Room 4.2

First Time Contributor Workshop

17 October: 17:15 - 18:00
Room 2.4
18 October : 10:30 - 11:15
Room 2.4
20 October : 09:00 - 12:30
Room 4.2

General Contribution

17 - 20 October: 9:00 - 18:00
Room 4.1

#DrupalContributions

Takeaways

- OCI Containers as a single unit of deployment
- Digital Signatures with Sigstore and SBOM
- DruBOM module - Drupal Bill of Materials
- * Automate your dependencies management with Github Dependabot or RenovateBot for all other platforms.
- * Add [Drupal Security Advisories for Composer](#) to your composer.json



What did you think?

Please fill in this session survey directly from the Mobile App.



Thank you!