PORSCHE INFORMATIK

SECURE DEVOPS ENVIRONMENT

CHRISTIAN KÖBERL, CNCF LINZ, 2022-11

SECURE YOUR ENVIRONMENT

In four simple steps

PORSCHE INFORMATIK

01

Security Testing

02

Dependency Management

03

Supply Chain Security

04

Deployment Security

SECURE YOUR ENVIRONMENT

In four simple steps

PORSCHE INFORMATIK

01

Security Testing

02

Dependency Management

03

Supply Chain Security

04

Deployment Security

SECURITY TESTING

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Interactive Application Security Testing (IAST)
- Runtime Application Self-Protection (RASP)
- Dependency Scanners - Software Composition Analysis (SCA)

SECURE YOUR ENVIRONMENT

In four simple steps

PORSCHE
INFORMATIK

01
Security Testing

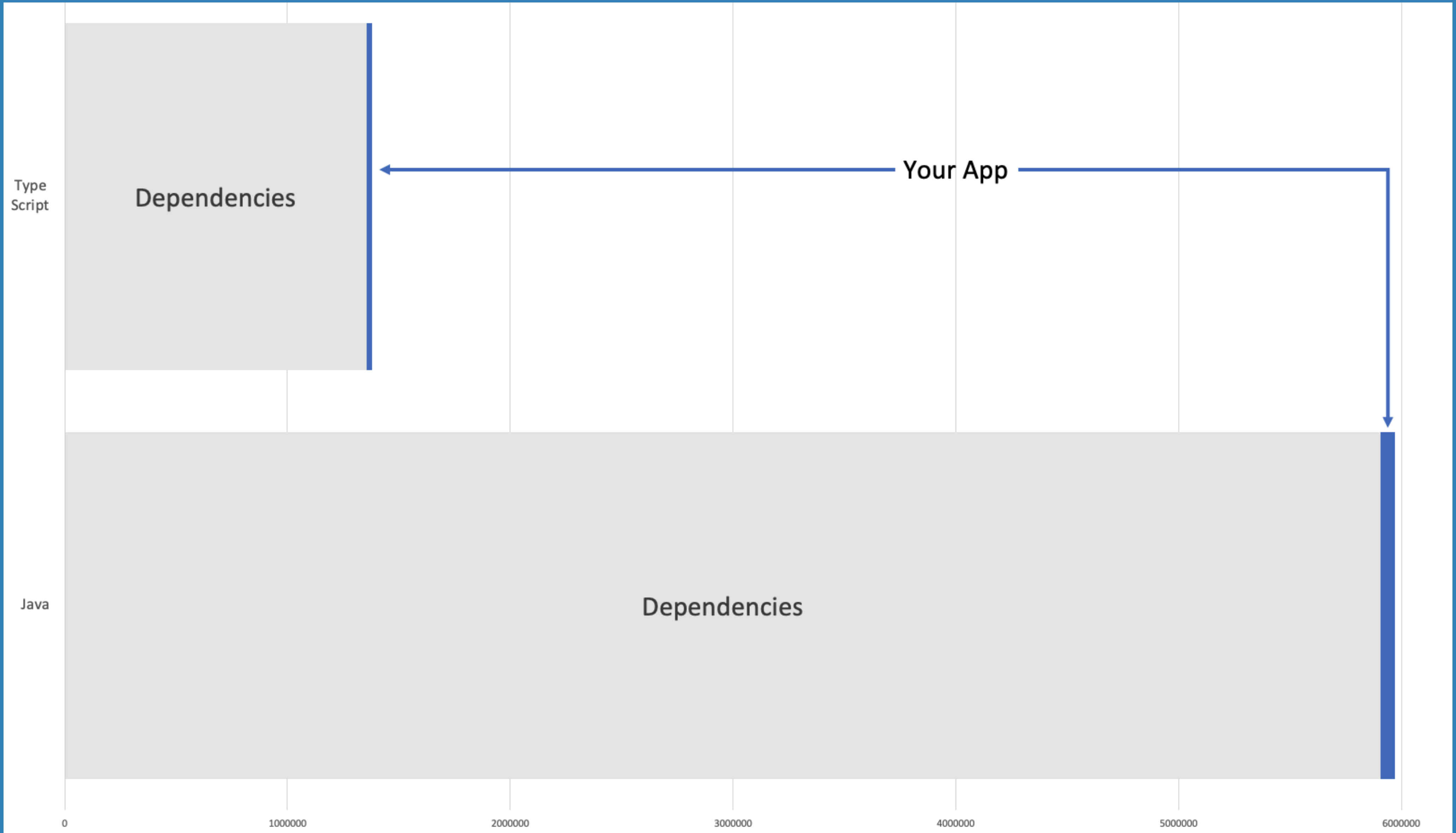
02
Dependency Management

03
Supply Chain Security

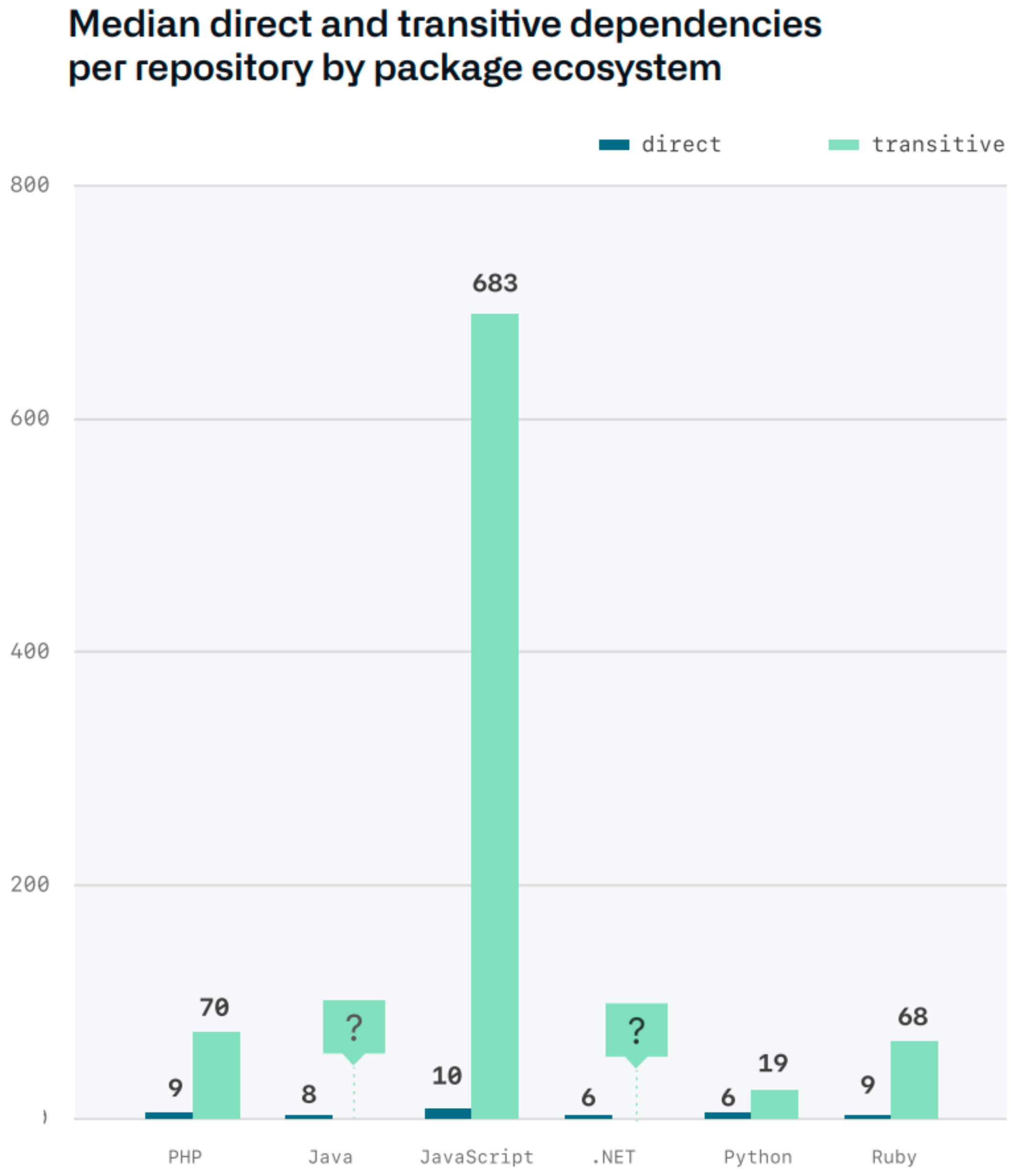
04
Deployment Security

Your next task is to figure out which applications in your org use log4j

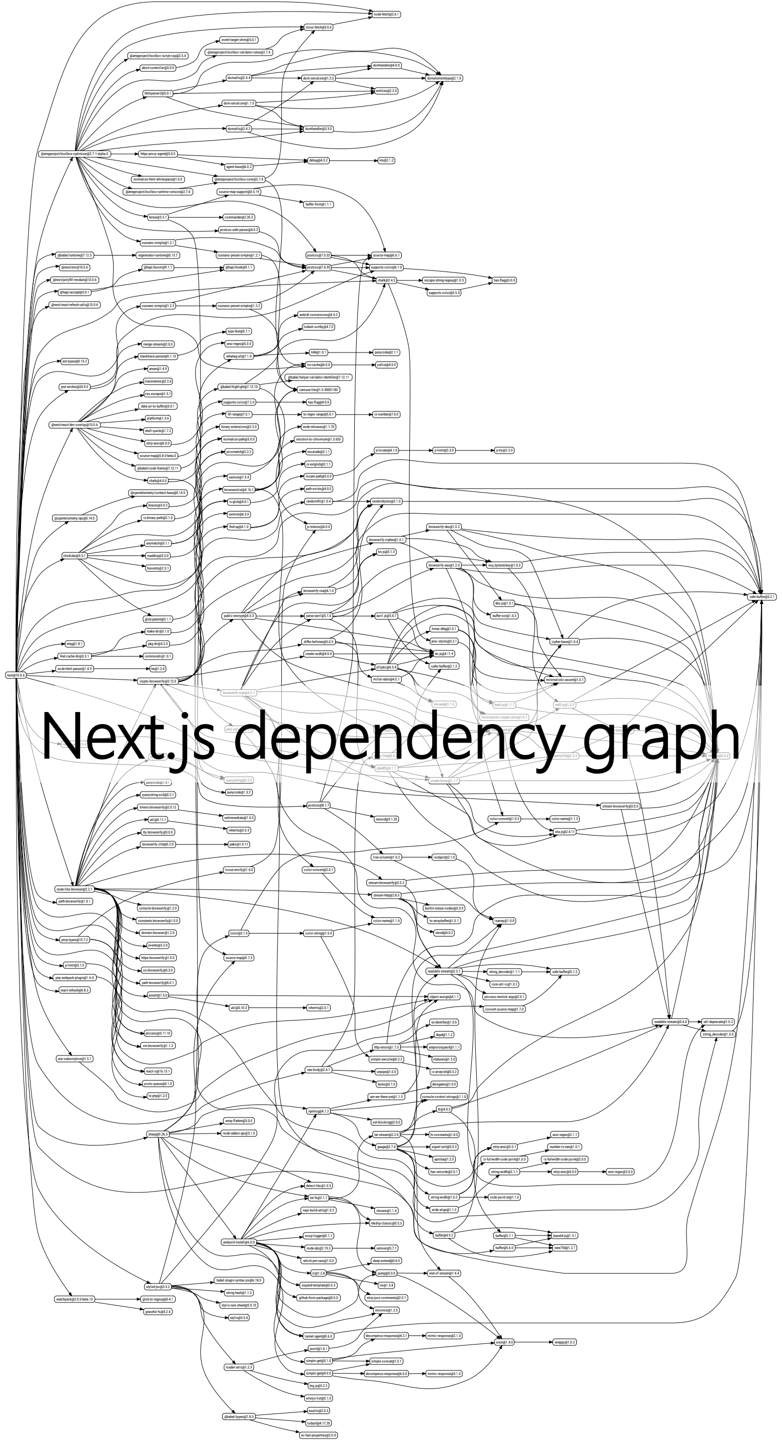
YOUR APP VS DEPENDENCIES



DEPENDENCY COUNT

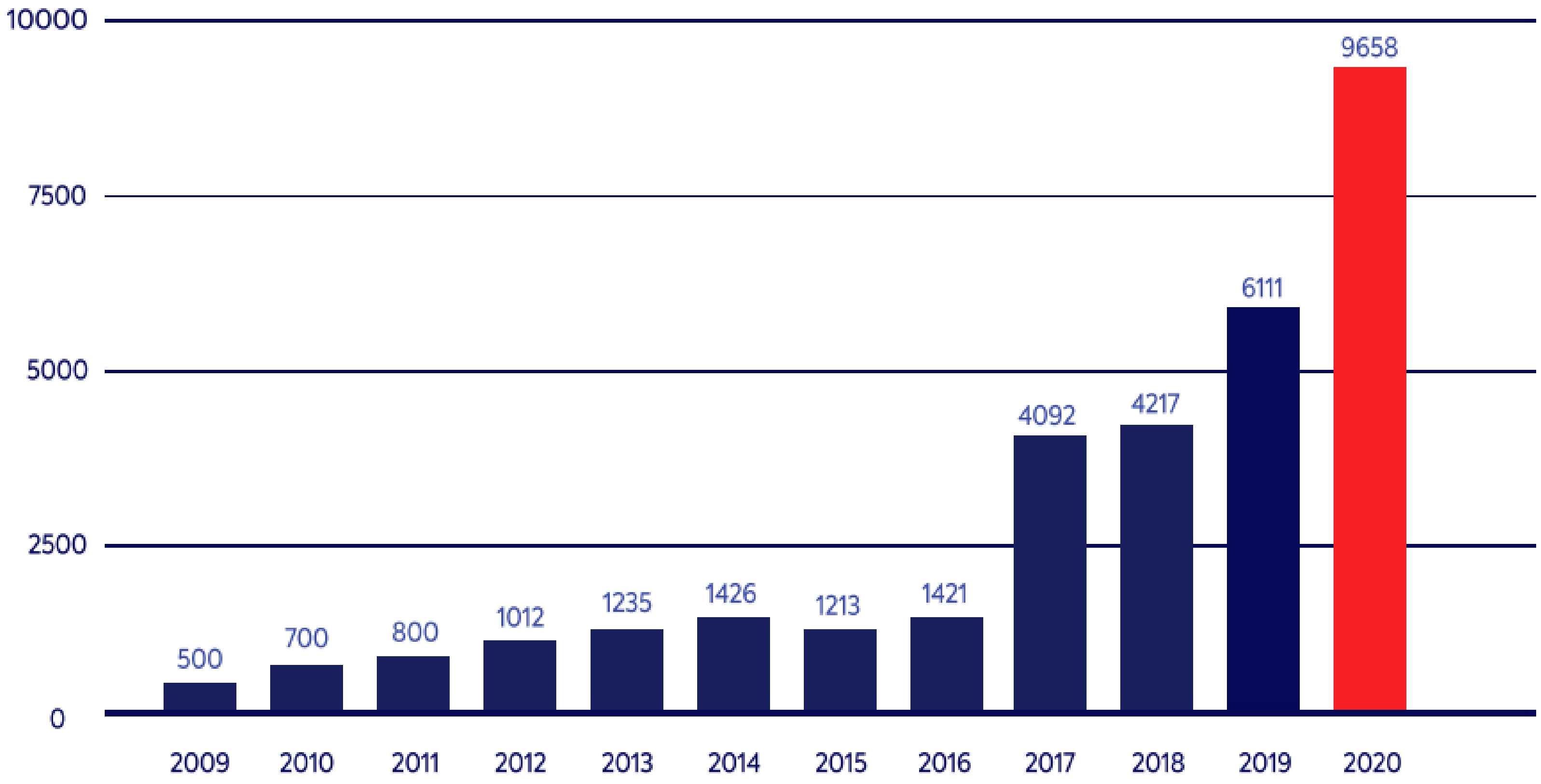


COMPLEXITY



Next.js dependency graph

VULNERABILITIES



DEVOPS TOOLS

The New Kids On the Block

Ansible
Terraform
Kubernetes
Helm
… and lots more

CONTINUOUS UPDATES

One of the solutions

Dependabot

Renovate

DEMO

Renovate

https://github.com/derkoe/renovate-demo-cncf-linz-2022-11

SECURE YOUR ENVIRONMENT

In four simple steps

01

Security Testing

02

Dependency Management

03

Supply Chain Security

04

Deployment Security

SOFTWARE BILL OF MATERIALS (SBOM)

What is this?

- List of all software components (aka dependencies)
- Including versions
- Including all transitive dependencies
- Usually also including the license

SBOM STANDARDS

The Software Package Data Exchange® (SPDX®)

An open standard for communicating software bill of material information, including components, licenses, copyrights, and security references.

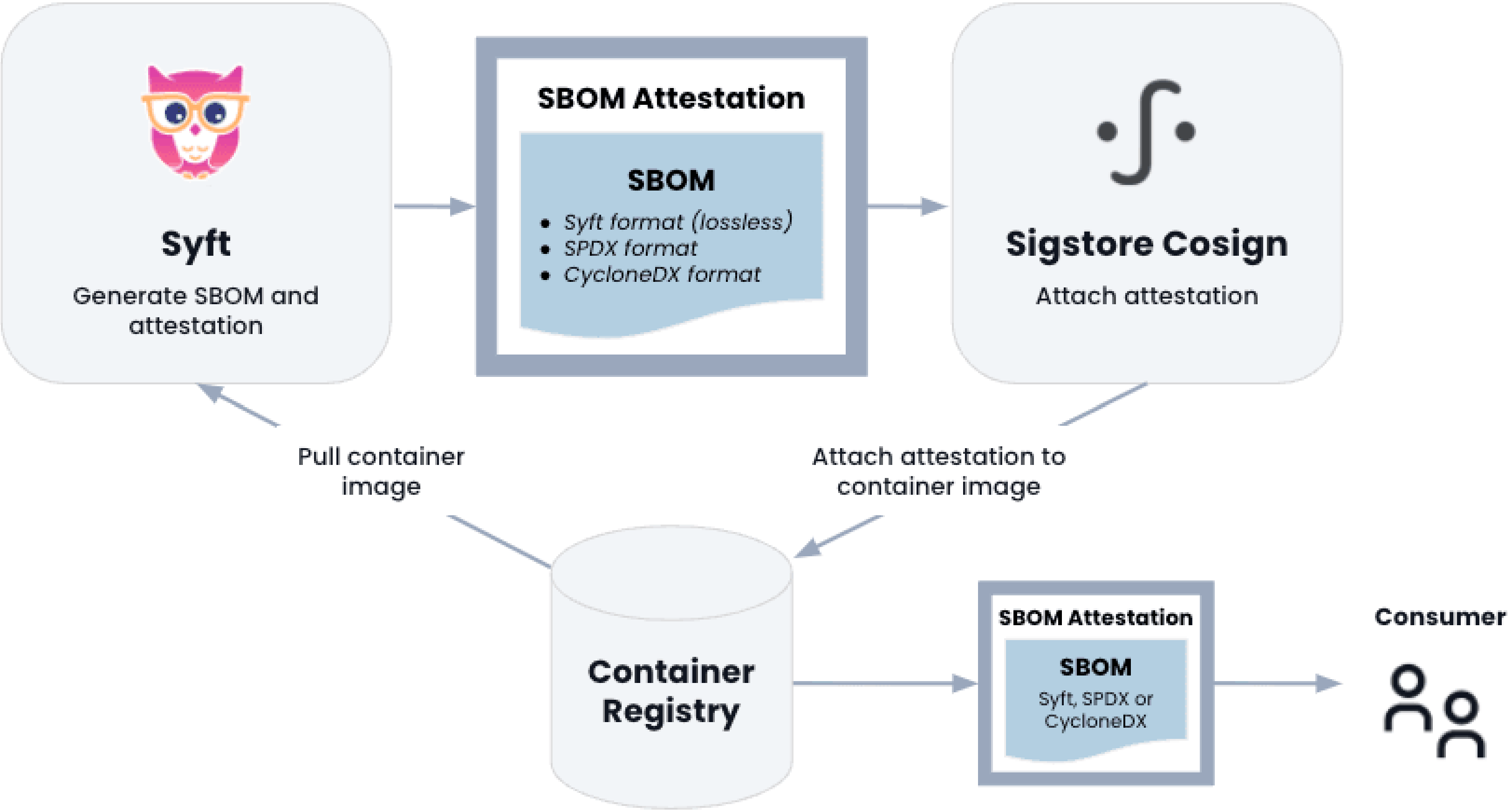
CycloneDX

OWASP CycloneDX is a lightweight Software Bill of Materials (SBOM) standard designed for use in application security contexts and supply chain component analysis.

DEMO

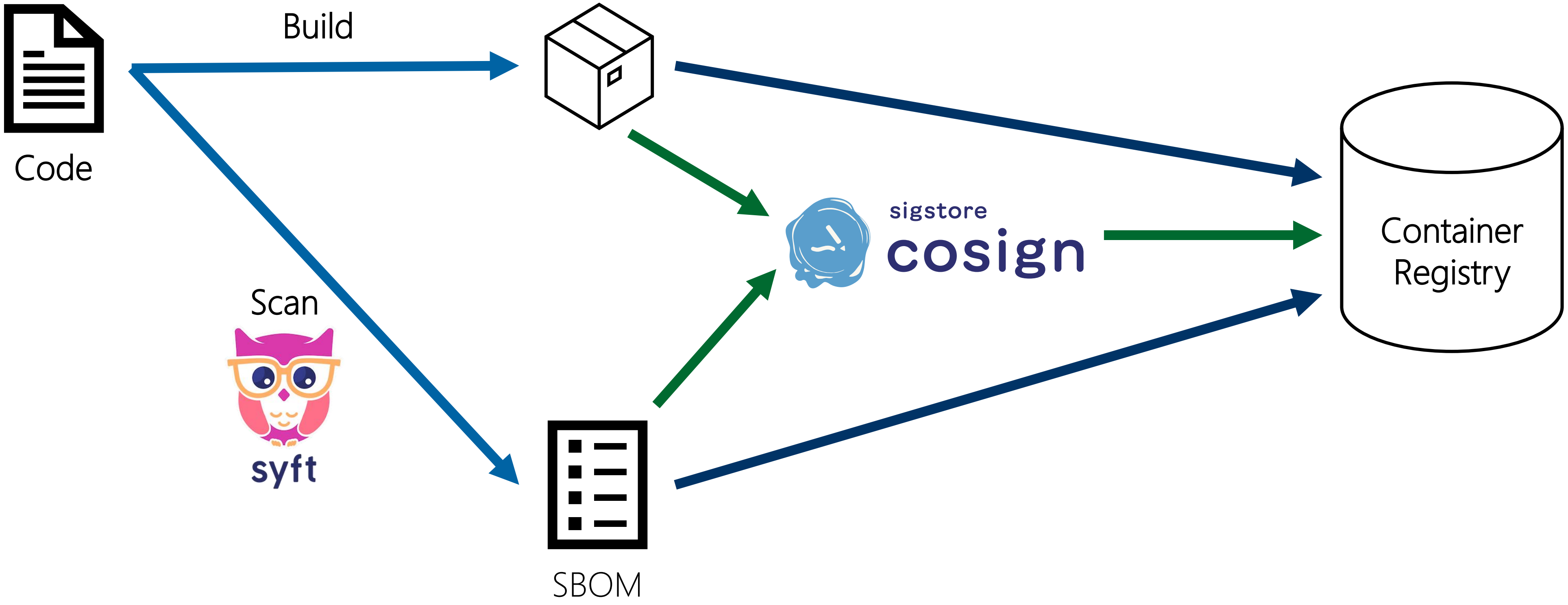
SBOM IN CONTAINER REGISTRY

Post-Build Attestation



BEST PRACTICES

For Building Software Artifacts



SBOM OPERATOR

by Christian Kotzbauer - https://github.com/ckotzbauer/sbom-operator

- `sbom-operator` scans alle Kubernetes images in a cluster with syft
- Sends data to
  - Git
  - ConfigMap
  - to an OCI Registry
  - Dependency Track

- Christian also provides a `vulnerability-operator`
  - Scans all images in a cluster with grype
  - Provides data via a JSON-file, Prometheus or a CRD (PolicyReport)

DEMO

syft

dependency track

https://github.com/derkoe/sbom-operator-demo-cncf-linz-2022-11

SECURE YOUR ENVIRONMENT

In four simple steps

PORSCHE INFORMATIK

01

Security Testing

02

Dependency Management

03

Supply Chain Security

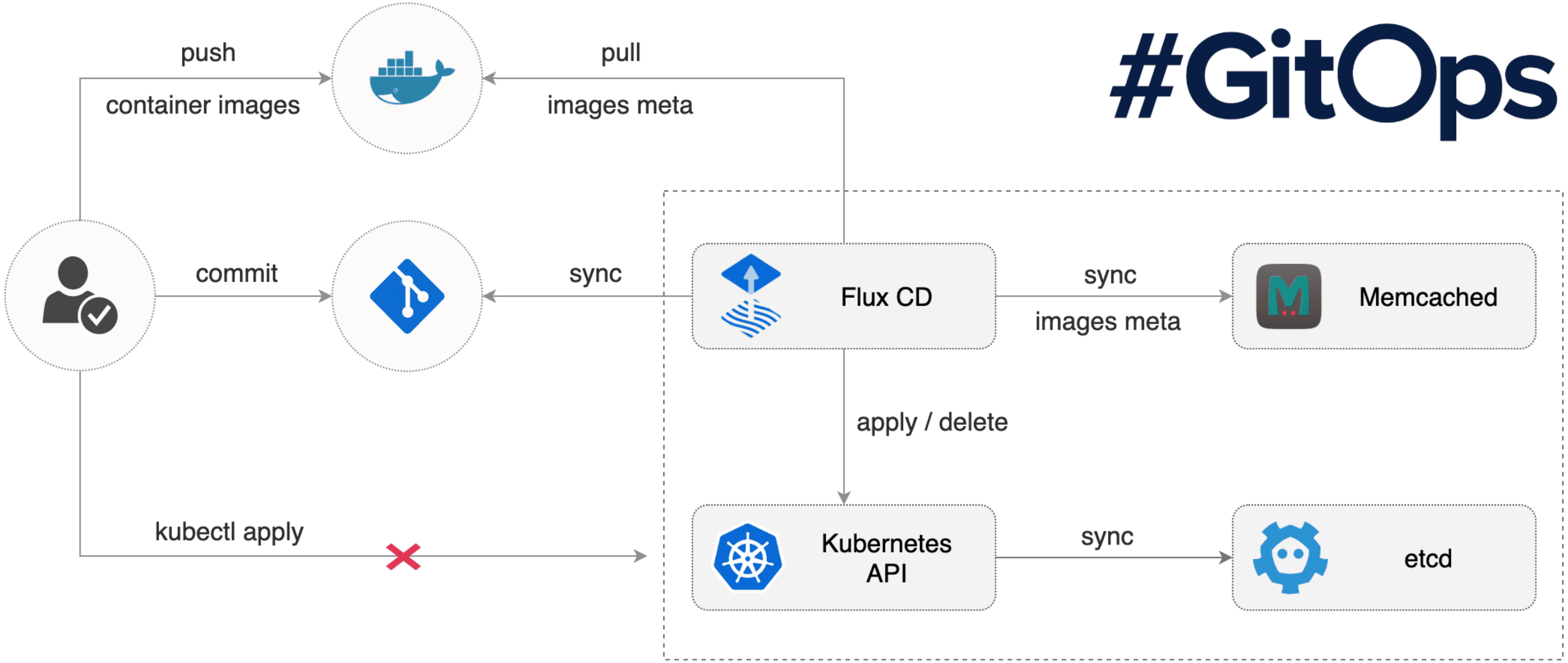
04

Deployment Security

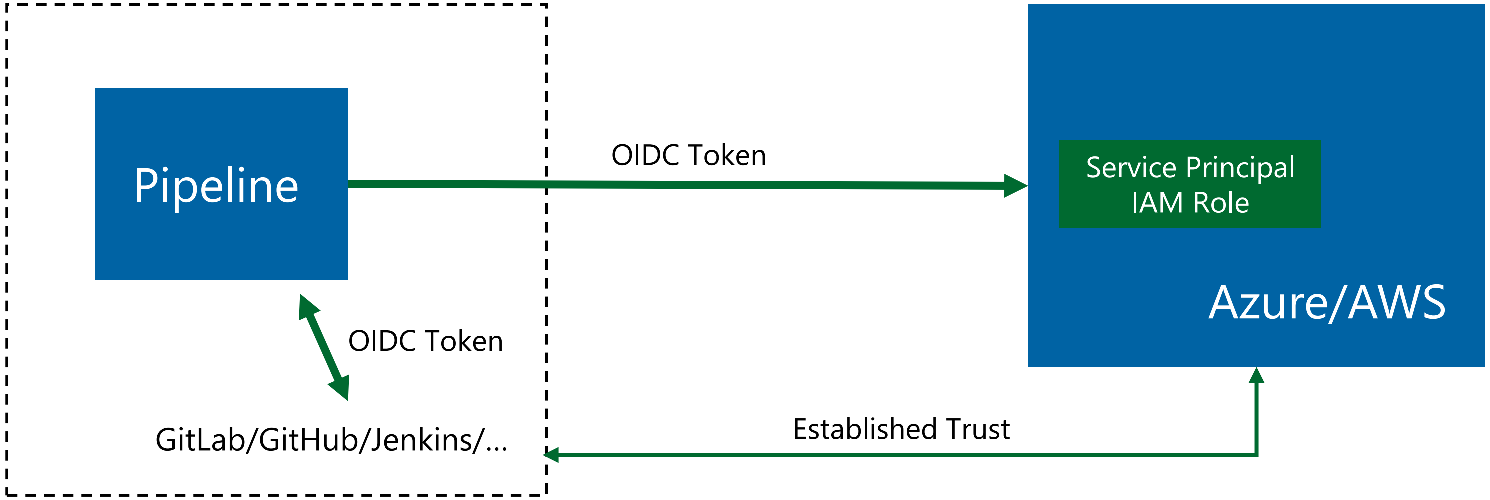
Your Deployment Pipeline

PULL-BASED DEPLOYMENTS

aka GitOps



PASSWORD-LESS DEPLOYMENT



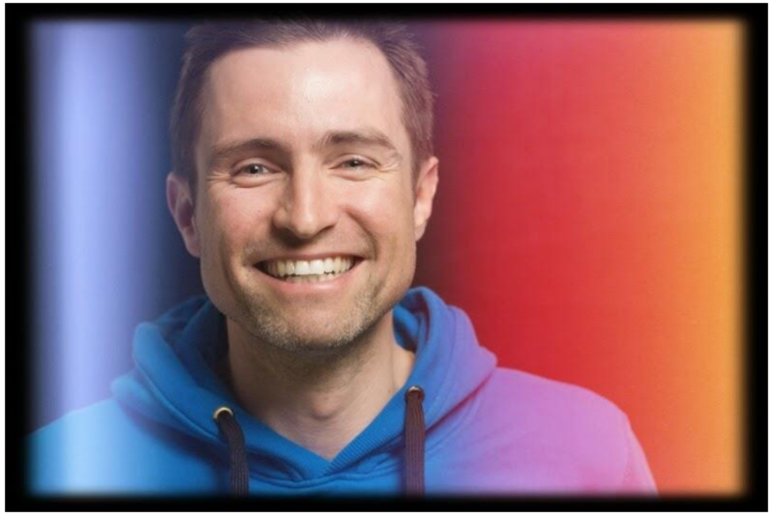
- Docs:
  - Configure OpenID Connect in AWS to retrieve temporary credentials | GitLab
  - Configure OpenID Connect in Azure to retrieve temporary credentials | GitLab
  - Configuring OpenID Connect in Azure - GitHub Docs
  - Configuring OpenID Connect in Amazon Web Services - GitHub Docs
- Example Repo with Terraform in GitLab: https://gitlab.com/derkoe/azure-terraform-oidc

SUMMARY

- Security Testing
    - Runs source code checks, tests and dependency checks
- Dependency Management
    - Use platform dependency manager
    - Automatically update dependencies (Renovate, Dependabot)
- Supply Chain Security
    - Provide SBOMs for your applications
    - Sign your application packages
    - Create an inventory of stuff running
- Deployment Security
    - Use pull-based or password-less deployments if possible

PORSCHE
INFORMATIK

THANK YOU VERY MUCH!



Christian Köberl

@derkoe

derkoe.dev

www.porscheinformatik.com

SOFTWARE / TOOLS

- Renovate
  https://docs.renovatebot.com/ | https://www.whitesourcesoftware.com/free-developer-tools/renovate/on-premises/
- syft – CLI tool and library for generating a Software Bill of Materials
  https://github.com/anchore/syft
- grype – A vulnerability scanner for container images and filesystems
  https://github.com/anchore/syft
- OWASP Dependency Track
  https://dependencytrack.org/
- SBOM Operator
  https://github.com/ckotzbauer/sbom-operator
- Cosign
  https://docs.sigstore.dev/cosign/overview
- Socket
  https://socket.dev/
- Open Source Insights
  https://deps.dev/
- Snyk Advisor
  https://snyk.io/advisor/

SOURCES

- Snyk: The State of Open Source Security 2020
  https://snyk.io/open-source-security/
- Whitesource: The State of Open Source Security Vulnerabilites 2021
  https://www.whitesourcesoftware.com/wp-content/media/2021/04/the-state-of-open-source-vulnerabilities-2021.pdf
- The 2020 State of the Octoverse
  https://octoverse.github.com/static/github-octoverse-2020-security-report.pdf#page=10
- Mike McGarr (Netflix): Dependency Hell, Monorepos and beyond https://www.youtube.com/watch?v=VNqmHJtItCs
- NPM Graph
  https://npm.broofa.com/
- Microsoft: Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers
  https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/
- SLSA (Supply-chain Levels for Software Artifacts)
  https://slsa.dev/
- Sigstore
  https://www.sigstore.dev/
- Best practices for a secure software supply chain (Microsoft Docs)
  https://docs.microsoft.com/en-us/nuget/concepts/security-best-practices