Navigating the EU Cyber Resilience Act

A DevSecOps Approach

Who am I ?

bespinian

Cloud Native Citizens

Platform Engineer

remmen.io

AI and Digital Media Coach

letsboot.ch

swiss dev training

Trainer

Marc Herren

Agenda

- Overview of the CRA (Cyber Resilience Act)
- What organisations can expect
- A DevSecOps approach to address the CRA

Before we start...

- I'm sharing my technical understanding of these regulations
- This isn't legal advice - I'm not a lawyer!
- Every organization's situation is different
- Always consult legal experts for compliance decisions

Who remembers ?

7. April 2014

CVE-2014-0160

https://www.heartbleed.com/

24. November 2021

CVE-2021-44228

https://en.wikipedia.org/wiki/Log4Shell

Was it remediated?

4 months later
76% of Global 2000 organizations still vulnerable to Heartbleed

April 2015
74% remain unpatched

www.cyberark.com

Apache LOG4J™

2 years later
38% of applications still use vulnerable Log4j versions.

www.veracode.com

Who is responsible

for a secure digital product ?

Manufactures

- No mandatory cybersecurity requirements
- No standardized security-by-design obligations
- Limited incentive to invest in security
- No mandatory incident reporting

Consumers & Businesses

- Limited access to security information
- Responsible for secure configuration

Outside of sectors with existing regulations (medical devices, aviation, …)

Ongoing Cyber threats

From the CRA factsheet

Every 11 seconds there is a **ransomware attack**

Ransomware attacks alone are estimated to have cost the world roughly **€20 billion** in 2021

In 2021, **cybercriminals** launched around **10 million DDoS attacks** worldwide

CRA Factsheet

EU Cybersecurity Strategy

16 December 2020

EVERYONE should be able to safely live their digital lives.

The EU's Cybersecurity Strategy in the Digital Decade

Where does the CRA fit?

Existing regulations

- NIS2 (Network and Information Security Directive)
- RED (Radio Equipment Directive)
- **CRA covers all digital products with connectivity or digital elements across the entire EU market**

Overview of the CRA

Cyber Resilience Act

Factsheet

- Ensure that **products with digital elements** placed on the EU market have **fewer vulnerabilities** and that manufacturers remain **responsible for cybersecurity** throughout a product's life cycle
- **Improve transparency** on security of hardware and software products
- Business users and consumers benefit from **better protection**

In scope

Products with digital elements (PDE)

- Hardware products
- Software products

…including their remote data processing solutions!

Benjamin Bögel
The Regulators Are Coming: One Year On

Outside the scope

- Non-commercial products
- Services
- Outright exclusions
  (cars, medical devices, in vitro,
  certified aeronautical equipment, marine equipment)

Benjamin Bögel
The Regulators Are Coming: One Year On

Manufacturer’s obligation

secure by default!

Cybersecurity is taken into account in **planning**, **design**, **development**, **production**, **delivery** and **maintenance** phase

All **cybersecurity risks** are documented;

Manufacturers will have to **report actively exploited vulnerabilities and incidents**

CRA Factsheet

Manufacturer’s obligation

Once sold, manufacturers must ensure that for the **duration of the support period**, **vulnerabilities are handled effectively**

Clear and understandable instructions for the use of products with digital elements

Security updates to be made **available to users for the time the product is expected to be in use**

CRA Factsheet

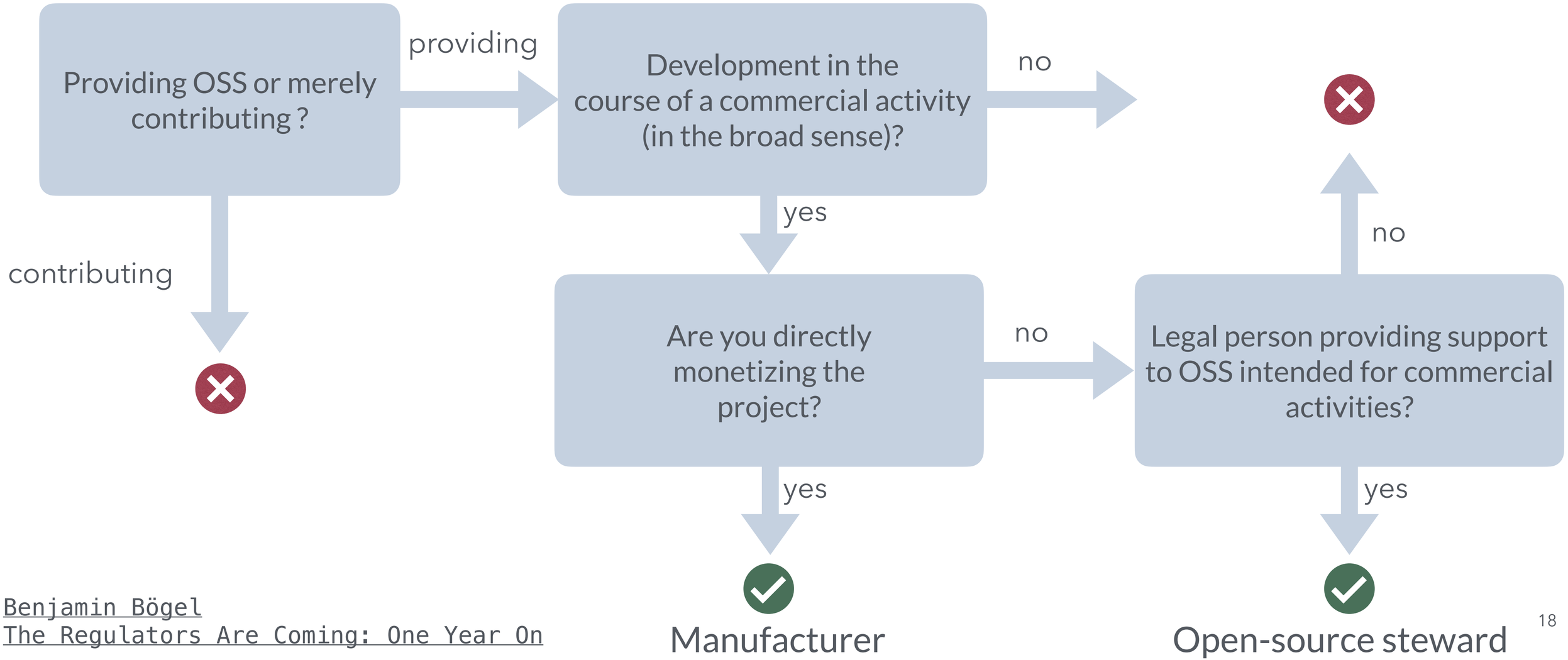
Is the CRA relevant for 🇨🇭 ?

Swiss companies exporting to EU must comply with CRA

Homburger insights – EU Cyber Resilience Act's Impact on Swiss Companies

Open-source projects

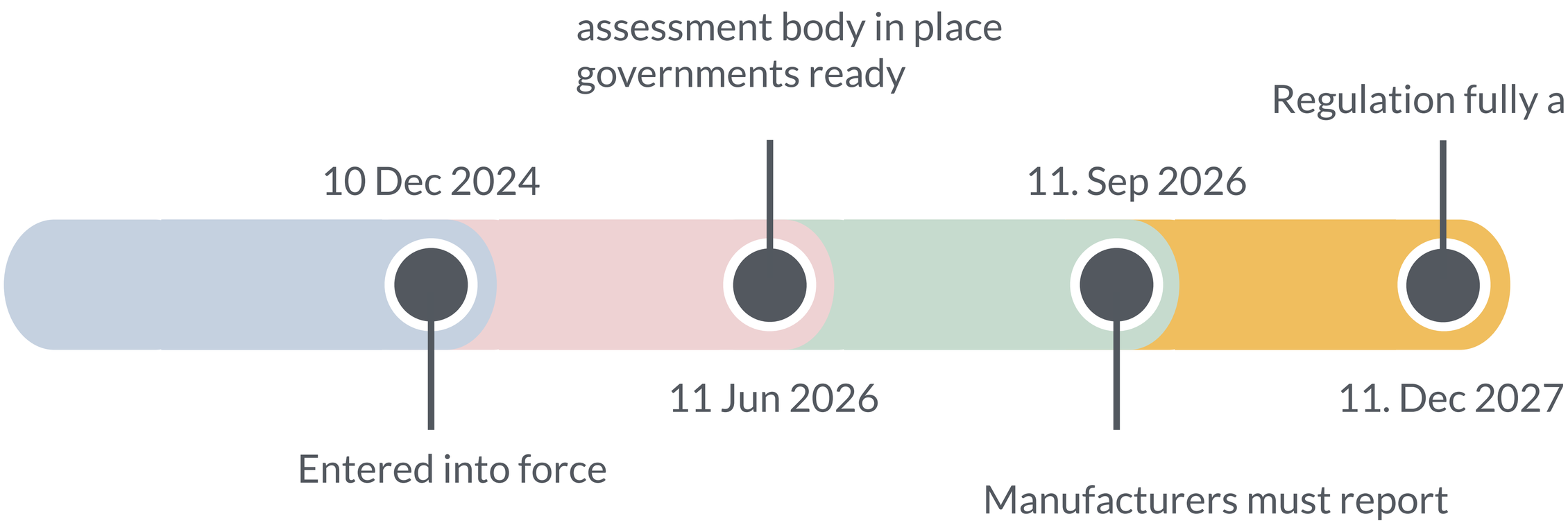
Does your open-source project fall under the CRA?



Benjamin Bögel
The Regulators Are Coming: One Year On

What organisations can expect

CRA Timeline



Reporting obligations

- Actively exploited vulnerability in PDE that it becomes aware of:
  - Early warning < 24 hours
  - General info < 72 hours
  - Final report < 14 days after correction/mitigation available
- Notify for a severe incident:
  - Early warning < 24 hours,
  - Incident notification < 72 hours,
  - Final report < 1 month

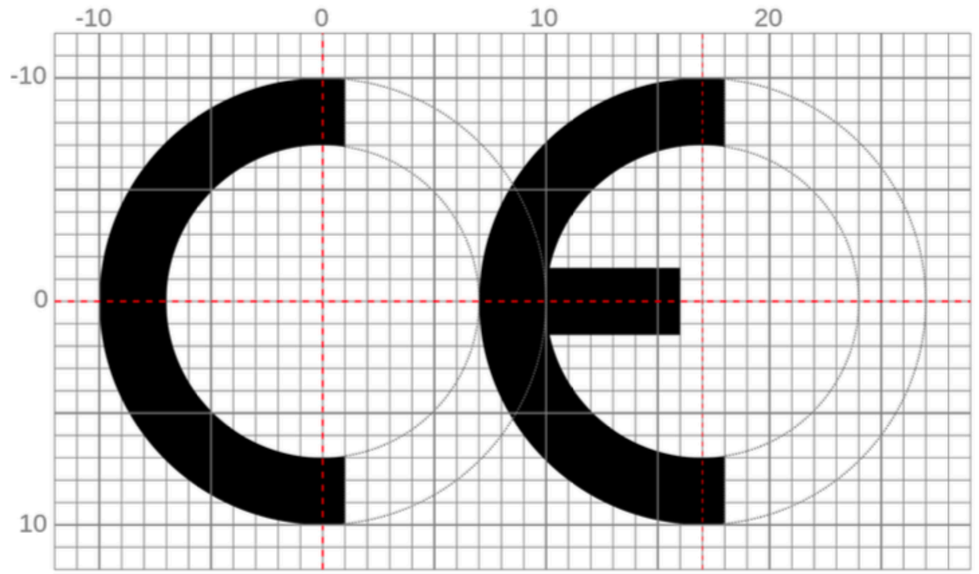
Penalties

- **Essential requirements** Up to €15M or 2.5% turnover
- **Other obligations** Up to €10M or 2% turnover
- **Misleading info** Up to €5M or 1% turnover

https://www.european-cyber-resilience-act.com/Cyber_Resilience_Act_Article_53_15.9.2022.html

CE marking

Products will bear the CE marking to indicate that they comply with the CRA requirements.



https://www.cyberresilienceact.eu/how-to-obtain-a-ce-certificate-for-the-cra/

A DevSecOps approach to address the CRA

From DevOps

you build it

you run it

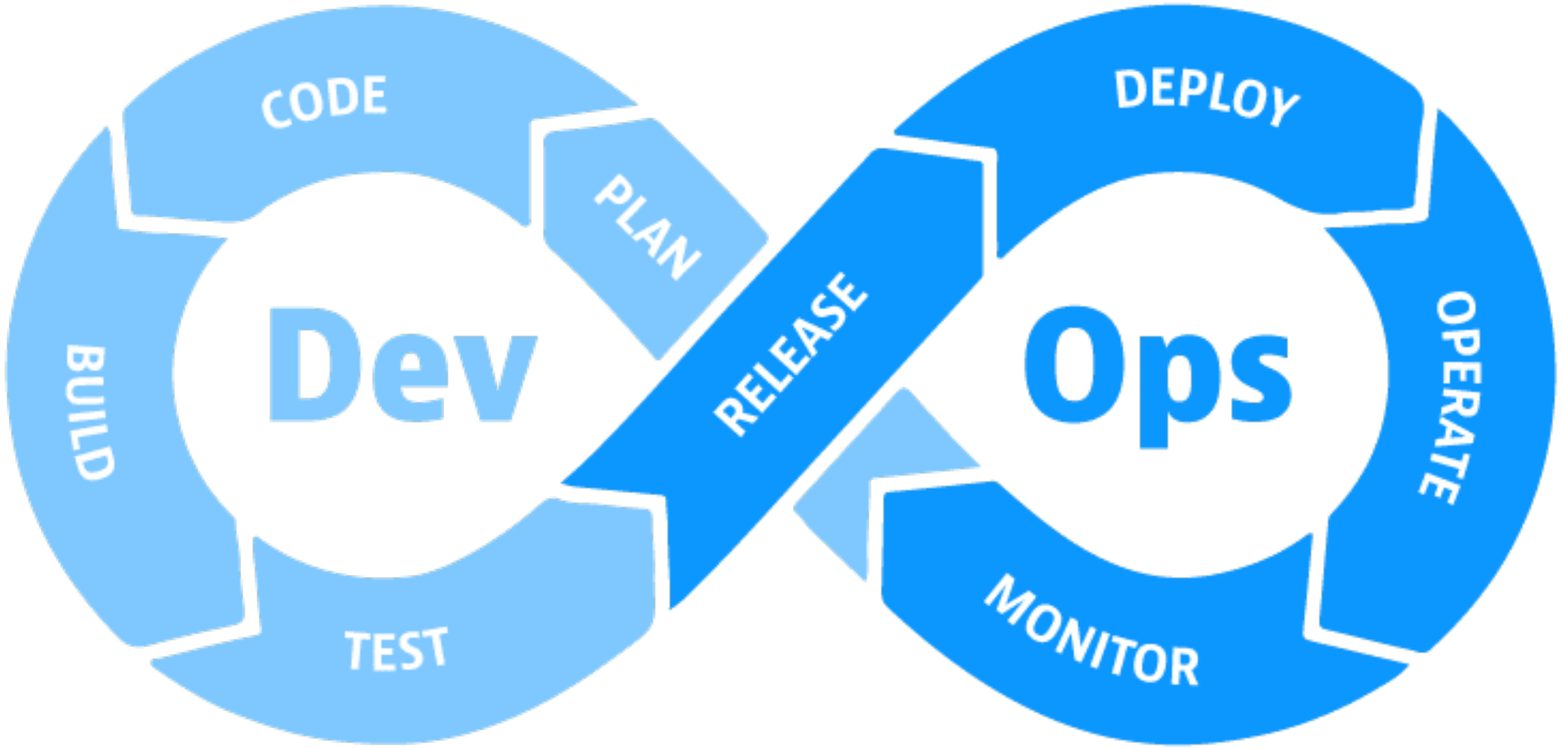
to DevSecOps

you build it

you run it

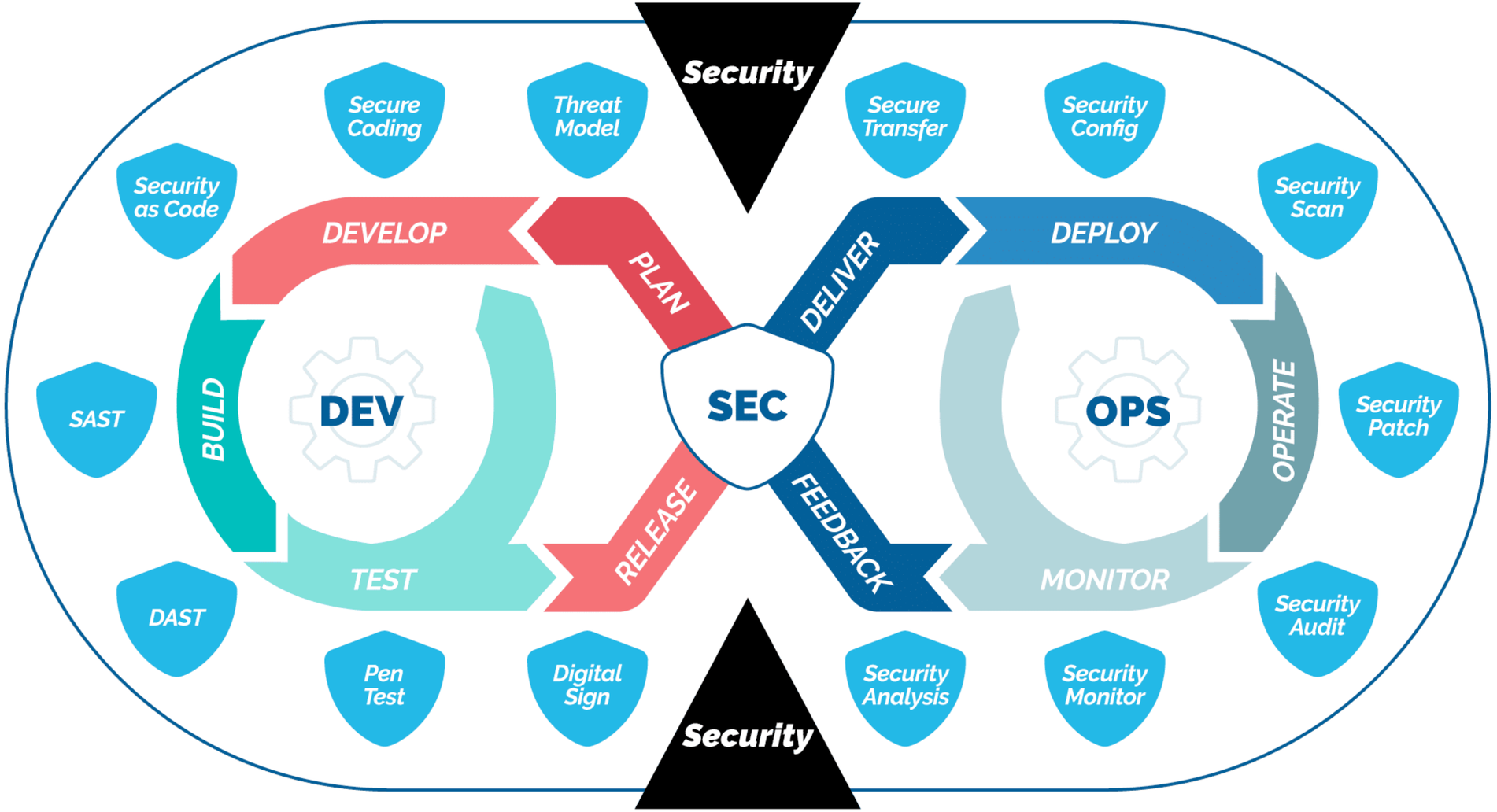
you care
you protect it
about it

From DevOps



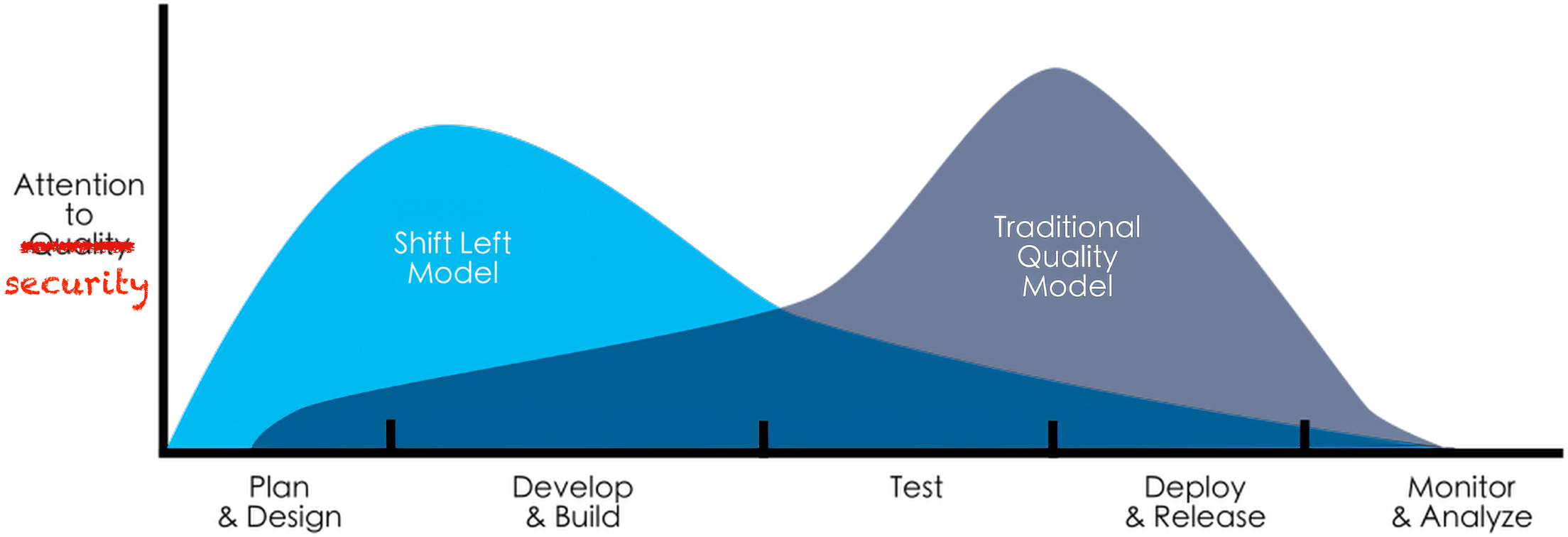
https://www.dynatrace.com/news/blog/what-is-devops/

to DevSecOps



https://www.cloudbolt.io/data-center-automation/devsecops-tools

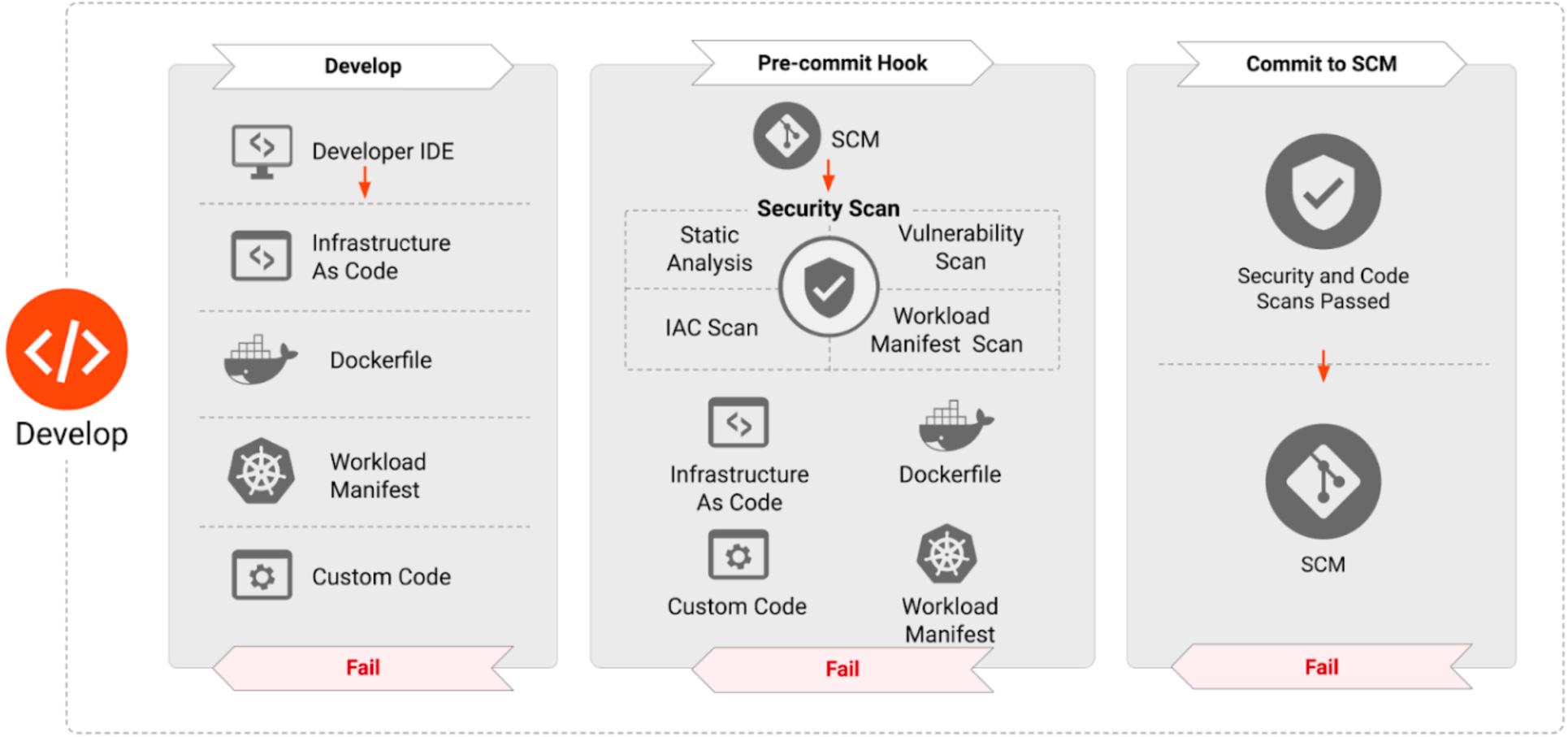
Shift Left



https://devopedia.org/shift-left

Shift Down

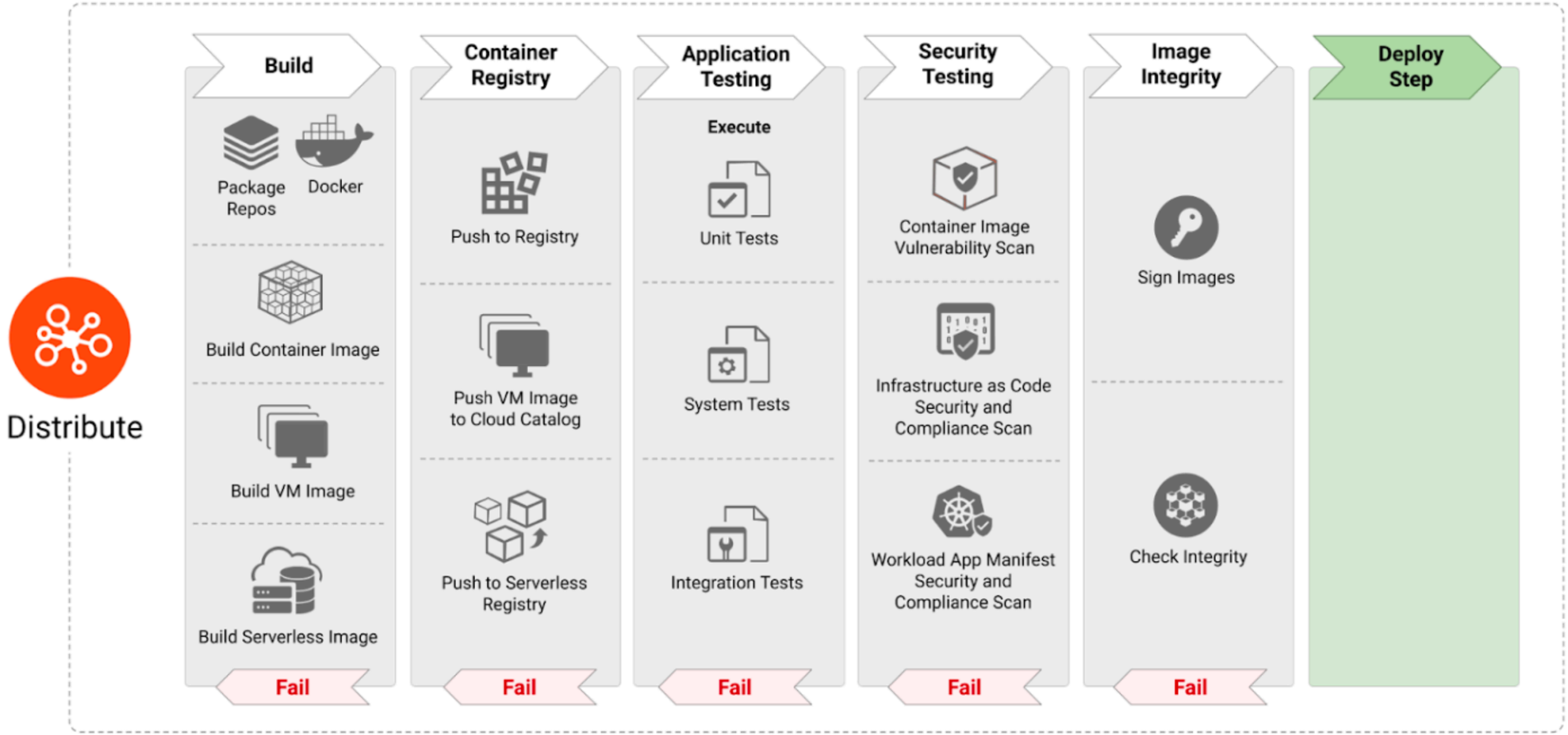
CNCF white paper on cloud native security



https://kubernetes.io/docs/concepts/security/cloud-native-security/

Shift Down

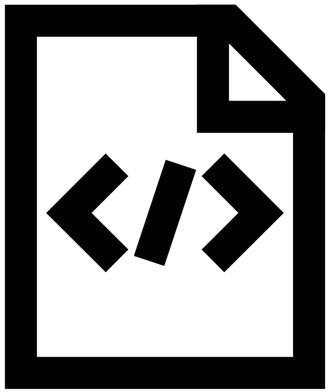
CNCF white paper on cloud native security



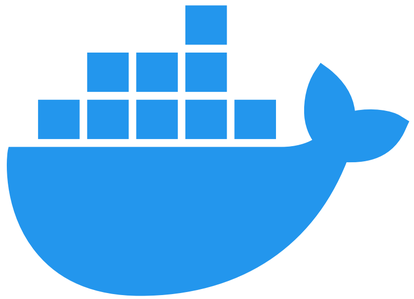
https://kubernetes.io/docs/concepts/security/cloud-native-security/

The 4C Security Model

Kubernetes security best practices

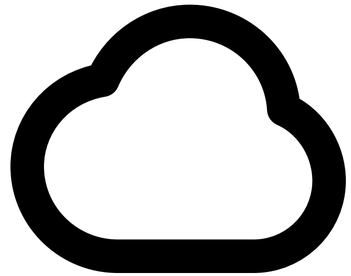


Code



Container

Cluster



Cloud

https://www.cncf.io/blog/2022/02/14/kubernetes-security-best-practices-definitive-guide/

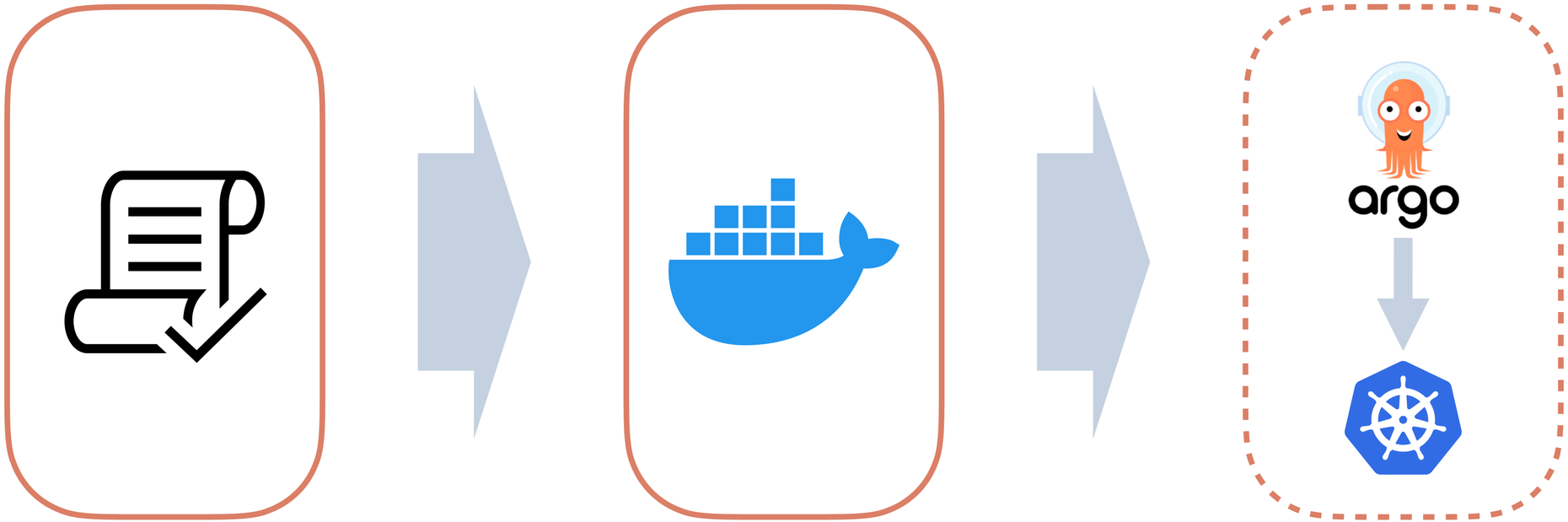
SLSA

Supply-chain Levels for Software Artifacts

SLSA

https://slsa.dev/

Basic CI/CD Pipeline



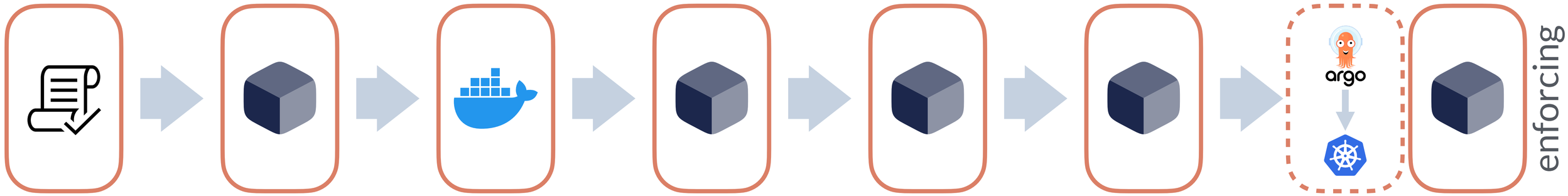
test

build

deploy

DevSecOps Pipeline

Get ready for the CRA using automation and adequate tools



test

code quality

build

vulnerability scanning

tracking

signing

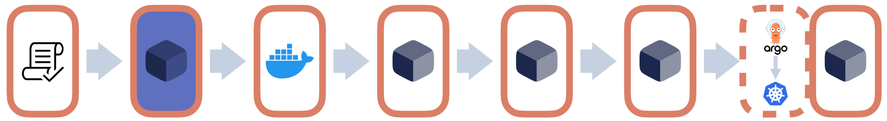
deploy

Let’s replace the black boxes

Examples based on open-source tools
- many more exist, both free and commercial

Code quality

Quality and security checks at the lowest level

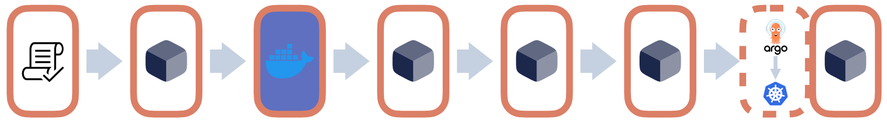


Semgrep

sonarqube

Base container

Quality and security checks at the lowest level



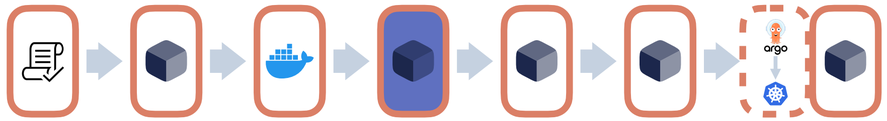
Buildpacks.io

Distroless

Chainguard

Vulnerability scanning

Create SBOMs for vulnerability assessment



syft

aqua
trivy

SBOMs

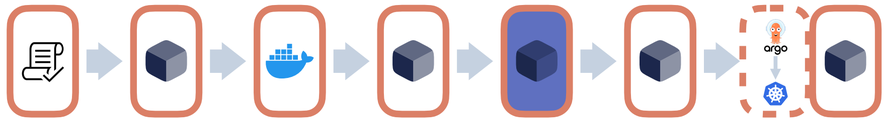
The Foundation of Software Supply Chain Visibility

Metadata	Supplier	Authors	Component		
	Manufacturer	Tools	Lifecycles		
Components	Supplier	Identity	Pedigree	Provenance	Evidence
	Component Type	Licenses	Hashes	Release Notes	Relationships
Services	Provider	Data Classification	Trust Zone		
	Endpoints	Data Flow	Relationships		
Dependencies	Components	Services			
Compositions	Completeness of:				
	Components	Services	Dependencies	Vulnerabilities	
Vulnerabilities	Details	Source	Exploitability (VEX)	Targets Affected	Proof of Concept
	Advisories	Risk Ratings	Evidence	Version Ranges	Recommendations

https://cyclonedx.org/specification/overview/

Tracking

Create SBOMs for vulnerability assessment



OWASP®

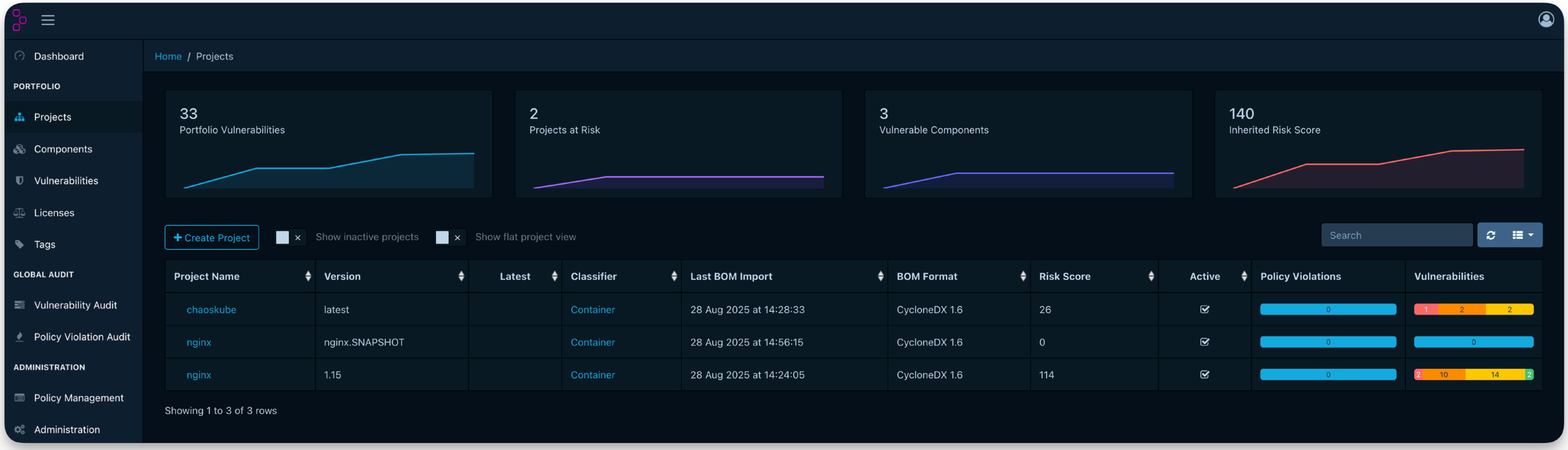
dependency track

Intelligent SBOM analysis platform for managing component risk

https://dependencytrack.org/

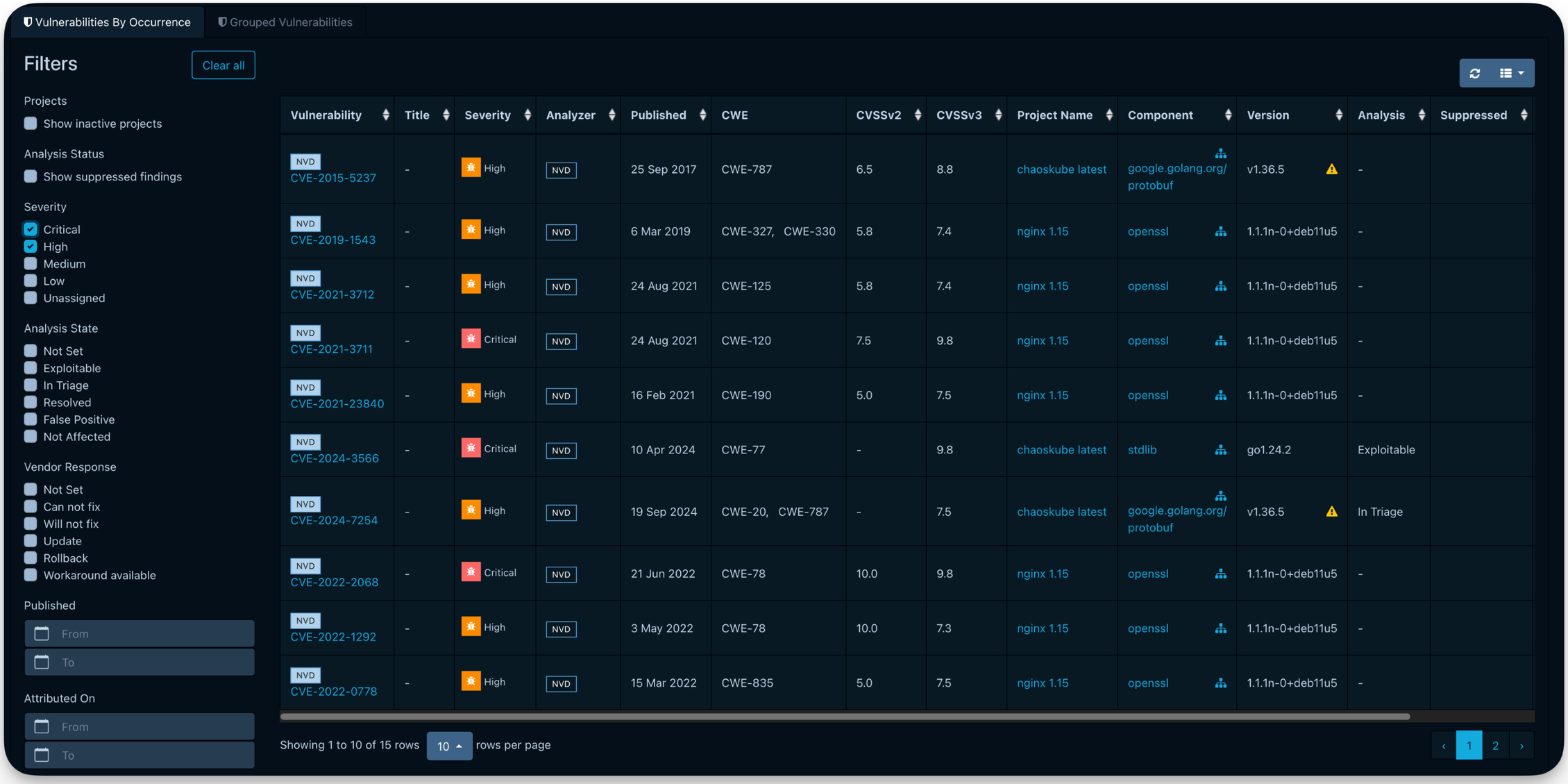
Dependency Track

Centralized platform for all SBOMs



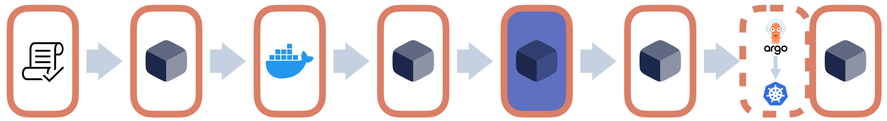
Dependency Track

Vulnerability audit

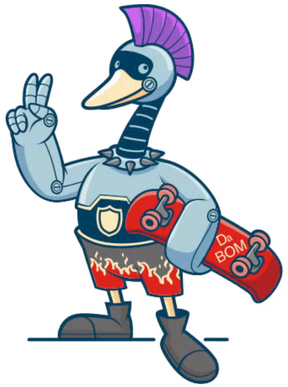


Risk Management

Use VEX to document your findings



Vulnerability Exploitability eXchange



OpenVEX

https://github.com/openvex/spec

Risk Management

Using Dependency Track for analyzing and document your findings

stdlib | go1.24.2 | NVD CVE-2024-3566 | Critical | NVD | 28 Aug 2025 | -

Description

A command inject vulnerability allows an attacker to perform command injection on Windows applications that indirectly depend on the CreateProcess function when the specific conditions are satisfied.

Audit Trail

admin - 1 Sep 2025 at 08:59:45
Vendor Response: NOT_SET → WILL_NOT_FIX

admin - 1 Sep 2025 at 08:59:51
Vendor Response: WILL_NOT_FIX → WORKAROUND_AVAILABLE

Comment

Add Comment

Analysis

Exploitable | Suppress

Justification

Not Set

Vendor Response (project)

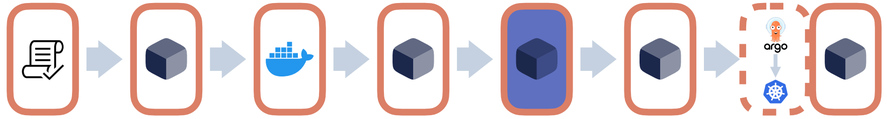
Workaround available

Details

Please use workaround x.y.z

Risk Management

Share your findings



aqua vexhub

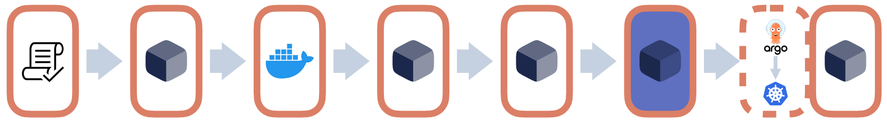
https://github.com/aquasecurity/vexhub

Automated remediation?

https://github.com/project-copacetic/copacetic

Signing

Sign artifacts for supply chain security



sigstore

cosign

https://github.com/sigstore/cosign

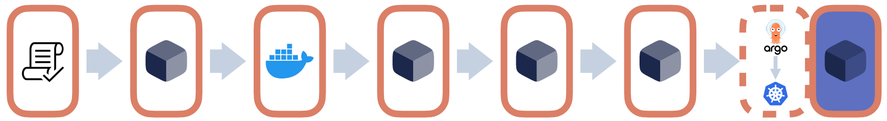
OCI Artifacts

Open Container Initiative

https://opencontainers.org/

Enforcing

Enforce supply chain security policies for Kubernetes

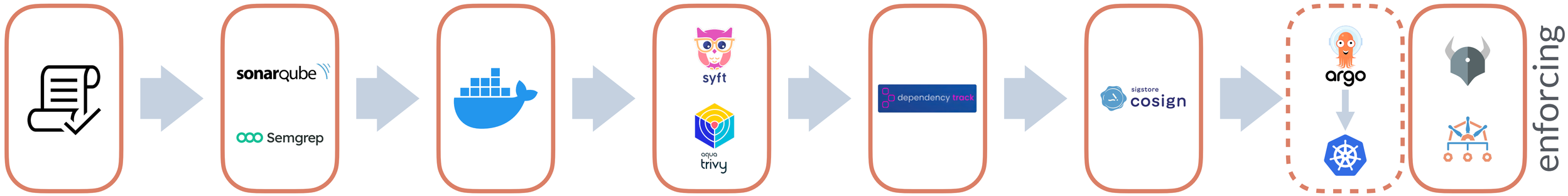


OPA gatekeeper

https://kyverno.io/

DevSecOps Pipeline

Get ready for the CRA using automation and adequate tools



test

code quality

build

vulnerability scanning

tracking

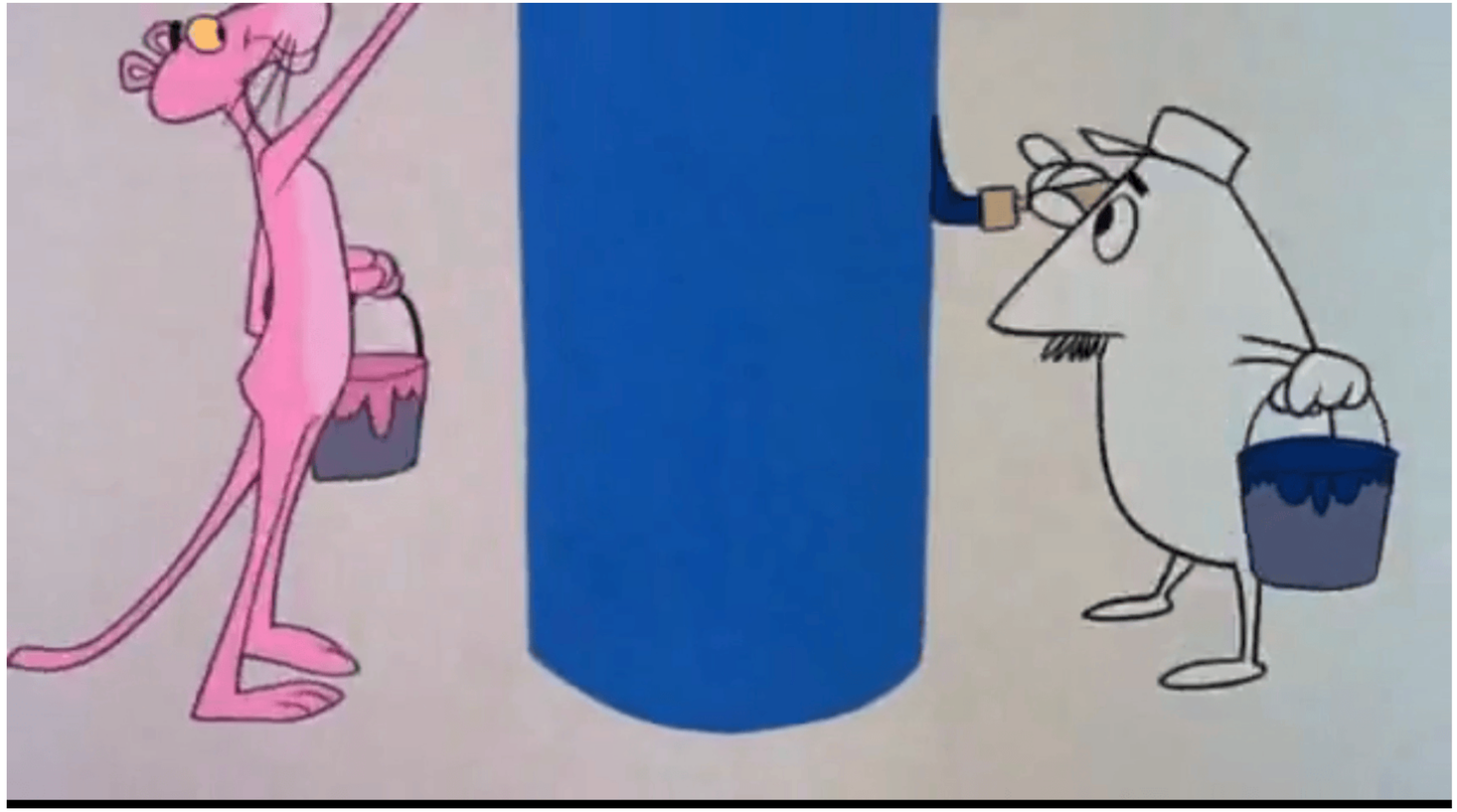
signing

deploy

Beyond Build Pipelines

A development approach is not enough!

There is no absolute security



inspired by controlplane's KubeCon Europe 2025 talk

Beyond Build Pipelines

CRA mandates ongoing security monitoring throughout the product lifecycle

- Create SBOMs an a regular basis (each night) and scan for vulnerabilities
- Use a multilayer approach
- Configure notifications for critical security events that require rapid response
- Configure systems to automatically patch critical vulnerabilities or isolate affected components within CRA-mandated timeframes

A DevSecOps pipeline

is no replacement for proper secure application design and architecture!

The CRA Promise

Preventing Preventable Breaches

Unpatched Open Source Software Flaw Blamed for Massive Equifax Breach

A Baird Equity Research report [PDF] blamed the recent Equifax breach that exposed 143 million consumers' personal information on a security flaw in the open source Apache Struts framework, which is used to build Java Web applications. Contrast Security co-founder and CTO Jeff Williams noted in a blog post that the Struts vulnerability in question [...]

WRITTEN BY

JEFF GOLDMAN

SEP 12, 2017

https://www.blackduck.com/blog/equifax-apache-struts-vulnerability-cve-2017-5638.html

Need more?

European Union

European Cyber Reslilience Act

Linux Foundation Training

CRA topics on FOSDEM

Slides

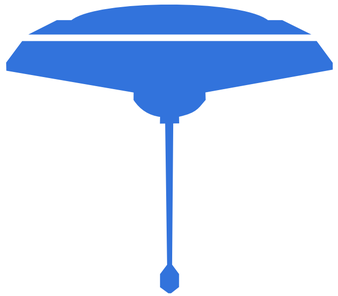
Want more?

A two-day workshop how to successfully integrate security into your DevOps processes

https://www.letsboot.ch/en-gb/course/devsecops

letsboot.ch
swiss dev training

Let's keep in touch



bespinian

Cloud Native Citizens

marc@bespinian.io