



Navigating the EU Cyber Resilience Act

A DevSecOps Approach

Who am I ?



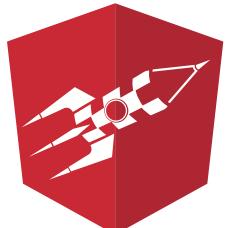
bespinian

Cloud Native Citizens

Platform Engineer



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...

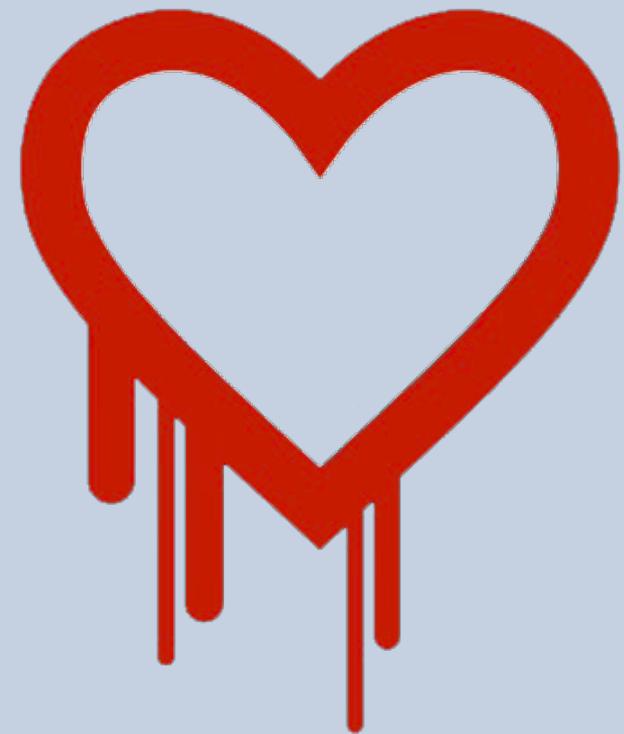


- ▶ I'm sharing my technical understanding of these regulations
- ▶ This isn't legal advice - I'm not a lawyer!
- ▶ Every organization's situation is different
- ▶ Always consult legal experts for compliance decisions

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



2 years later

38% of applications still use
vulnerable Log4j versions.

www.veracode.com

Who is responsible



for a secure digital product ?

Manufactures

- ✖ 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

EU Cybersecurity Strategy



16 December 2020

EVERYONE should be able to
safely live their digital lives.

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)



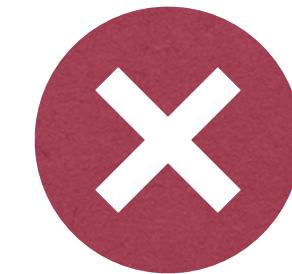
Hardware products



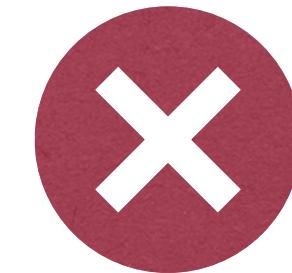
Software products

...including their remote data processing solutions!

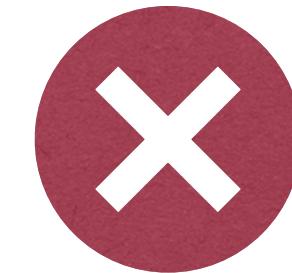
Outside the scope



Non-commercial products



Services



Outright exclusions

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**

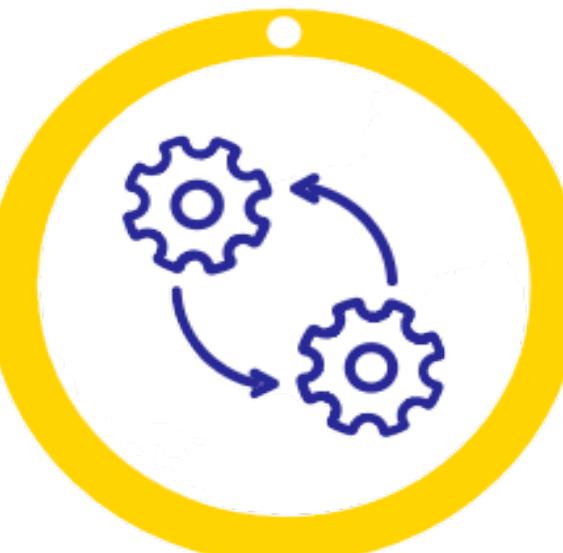
Manufacturer's obligation



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

Is the CRA relevant for ?

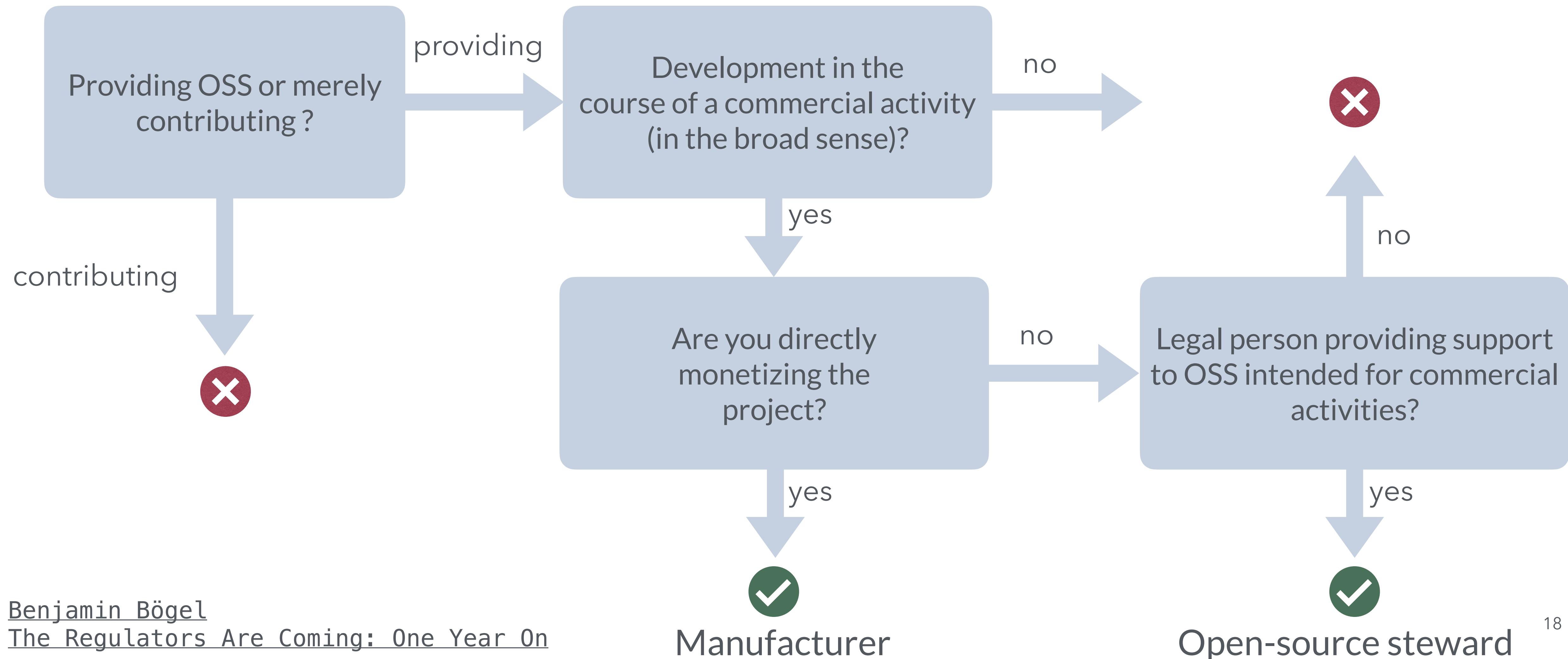


Swiss companies exporting to
EU must comply with CRA

Open-source projects



Does your open-source project fall under the CRA?

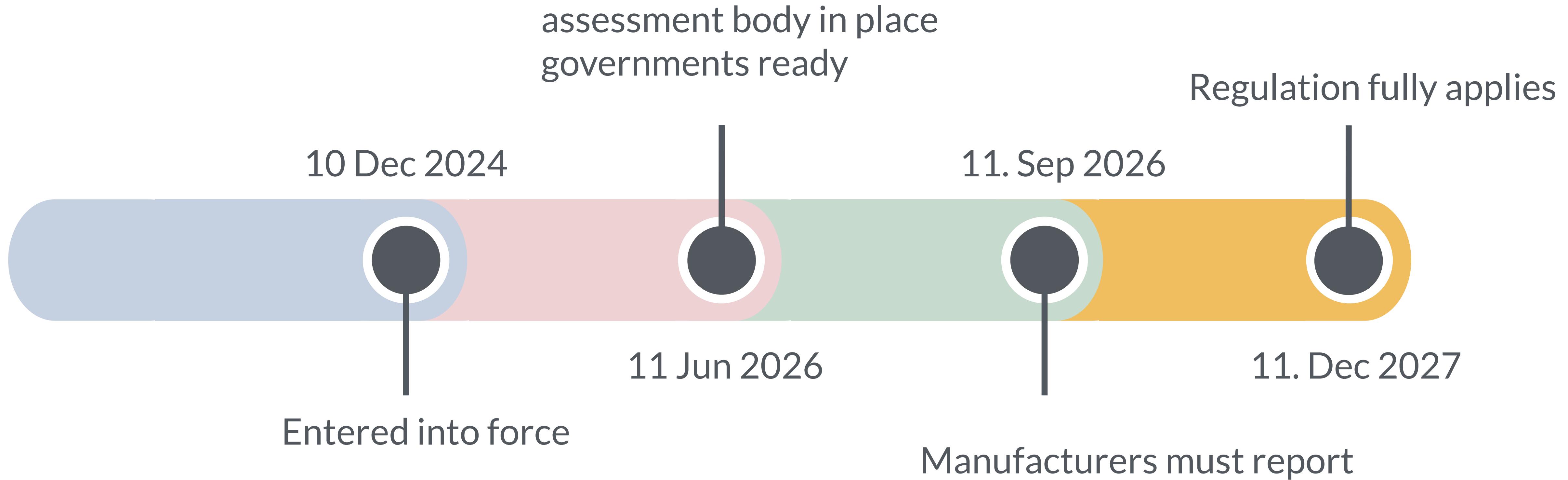




What organisations can expect



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

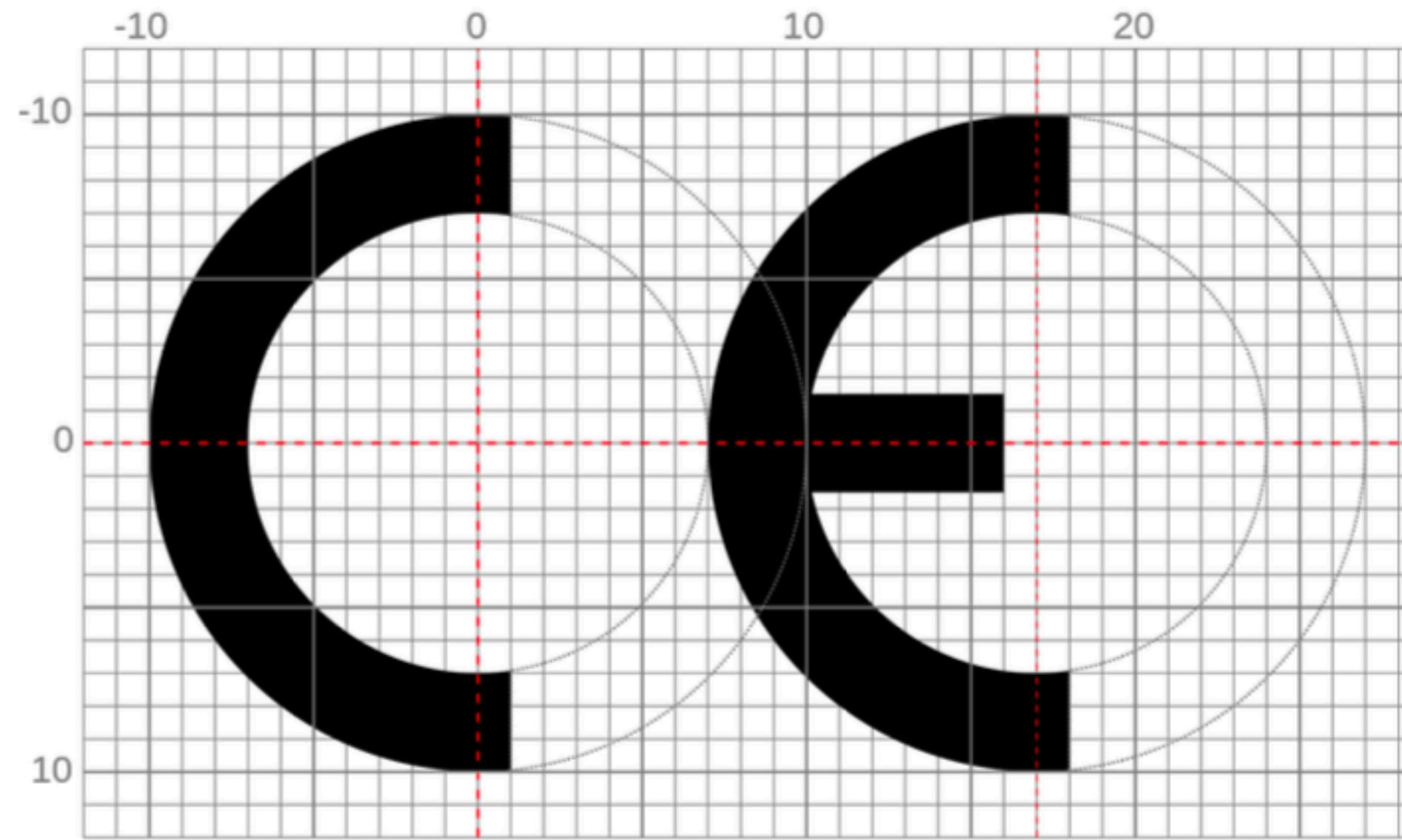


- ▶ **Essential requirements** Up to €15M or 2.5% turnover
- ▶ **Other obligations** Up to €10M or 2% turnover
- ▶ **Misleading info** Up to €5M or 1% turnover

CE marking



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





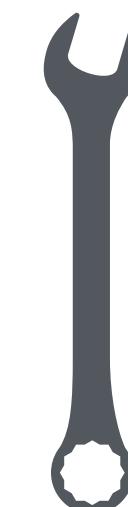
A DevSecOps approach to address the CRA



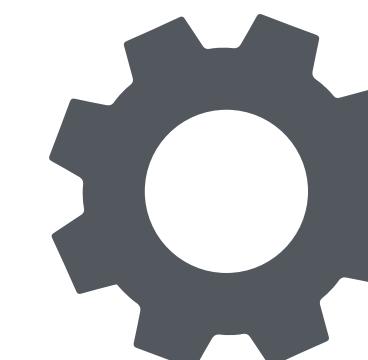
From DevOps



you build it



you run it



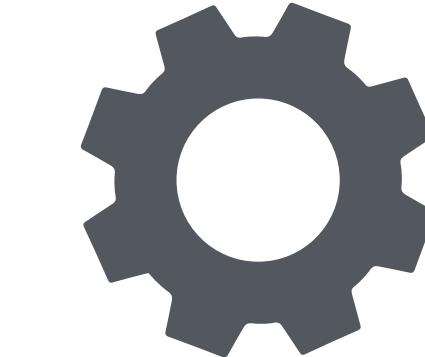
to DevSecOps



you build it



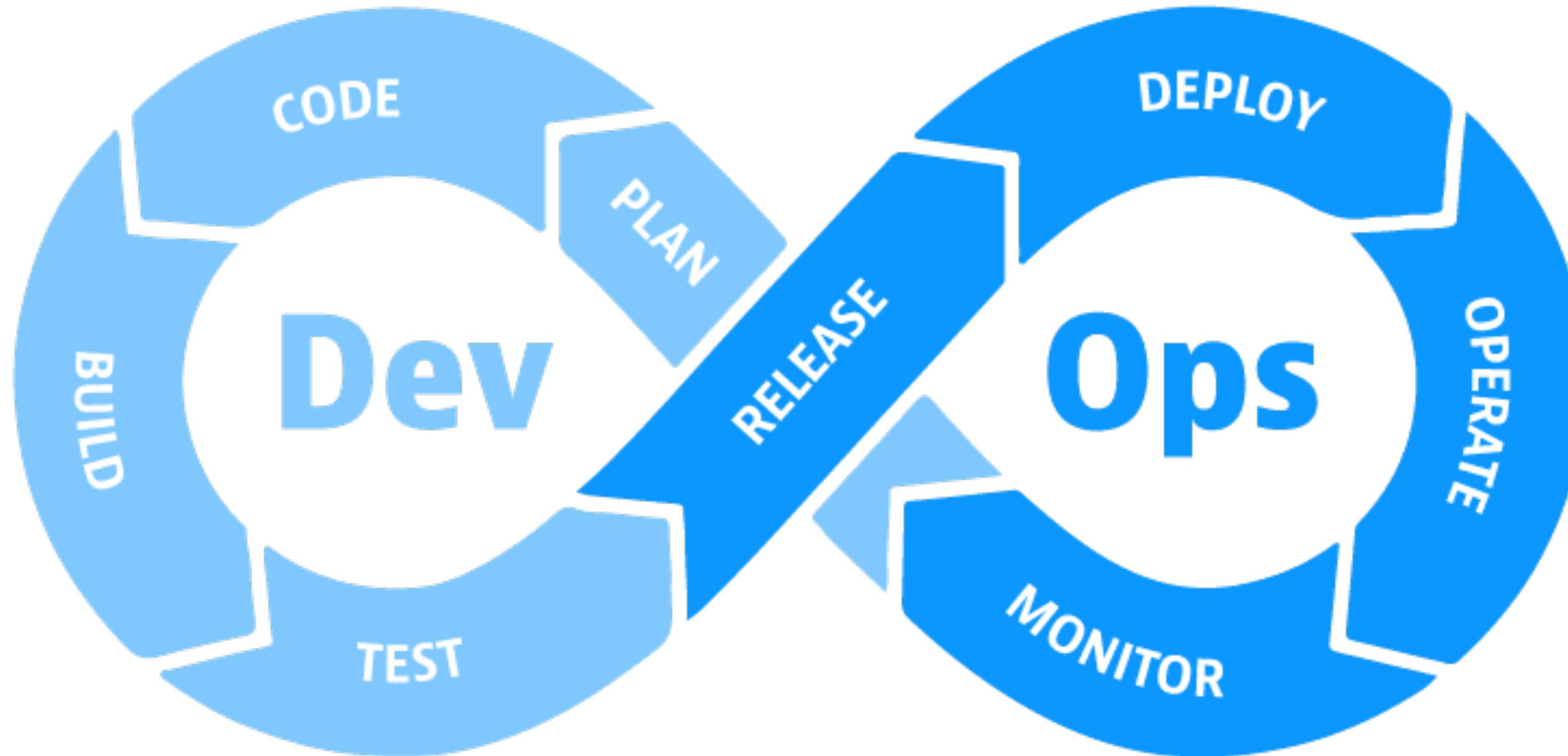
you run it



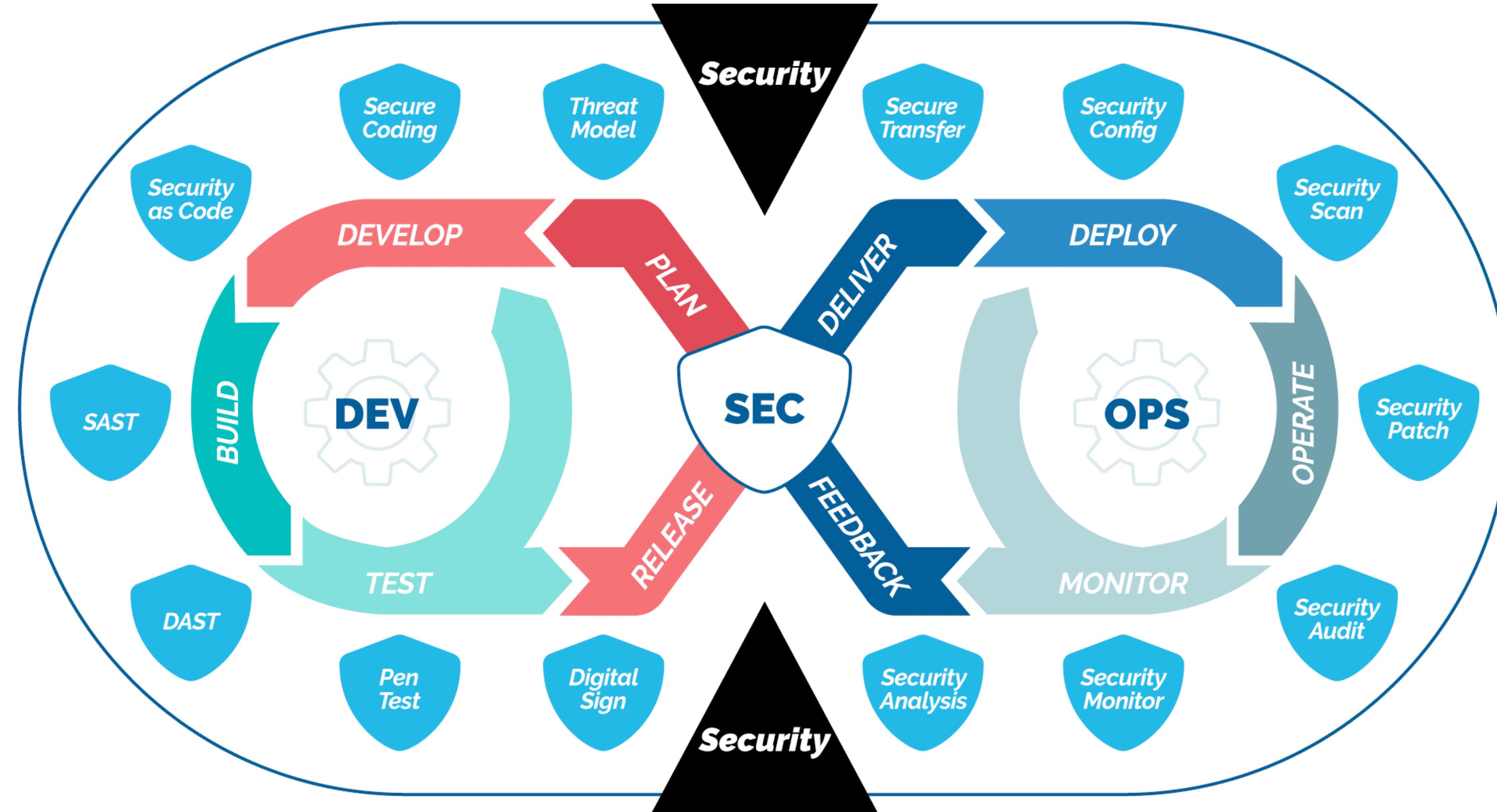
you care
you protect it
about it



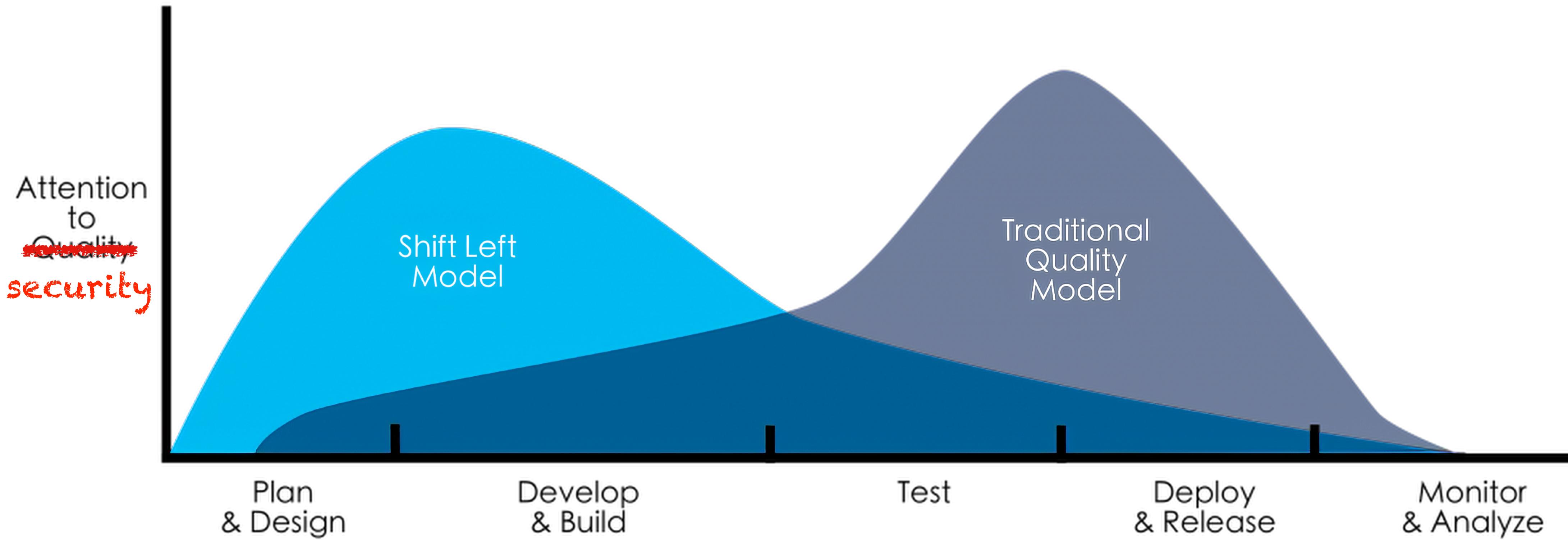
From DevOps



to DevSecOps



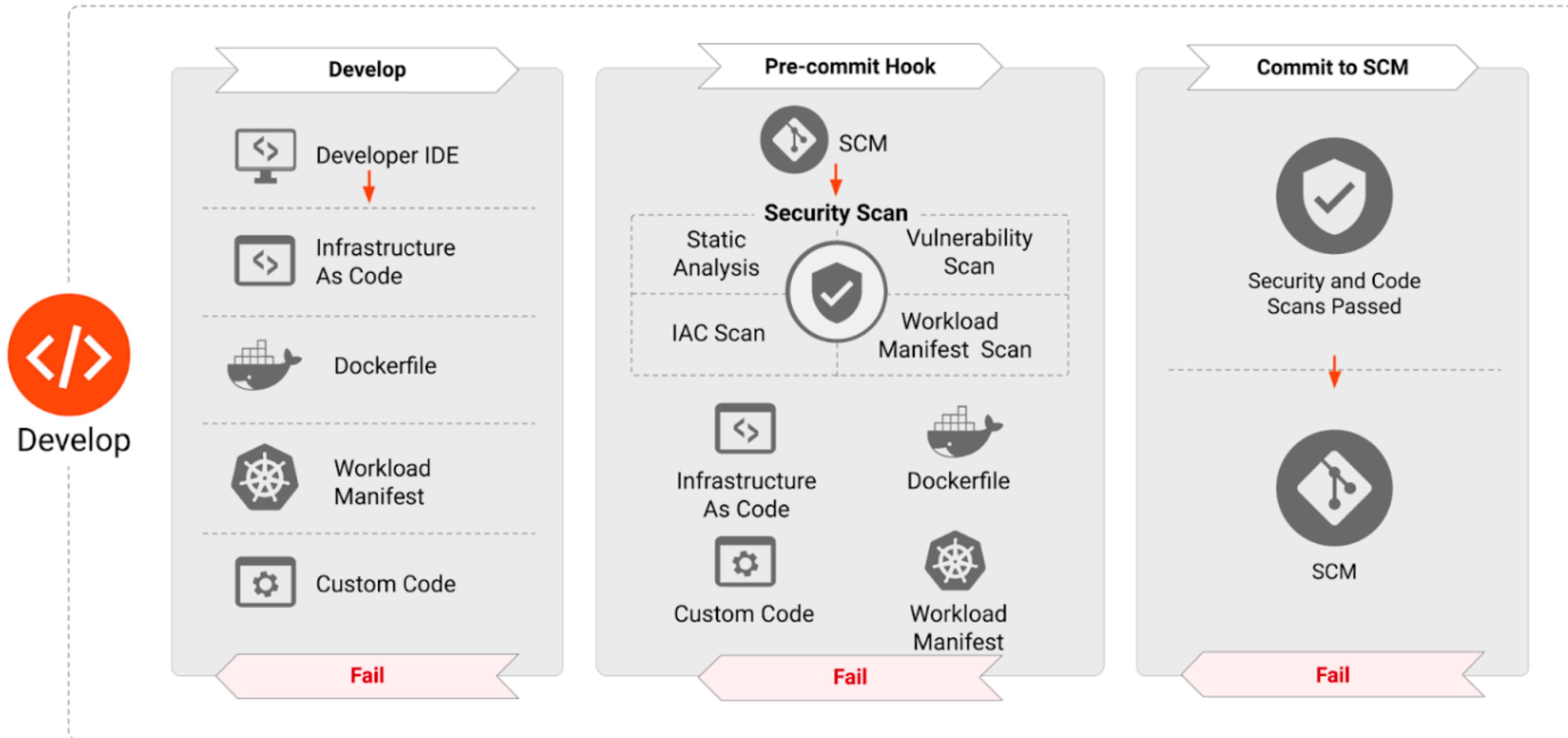
Shift Left



Shift Down



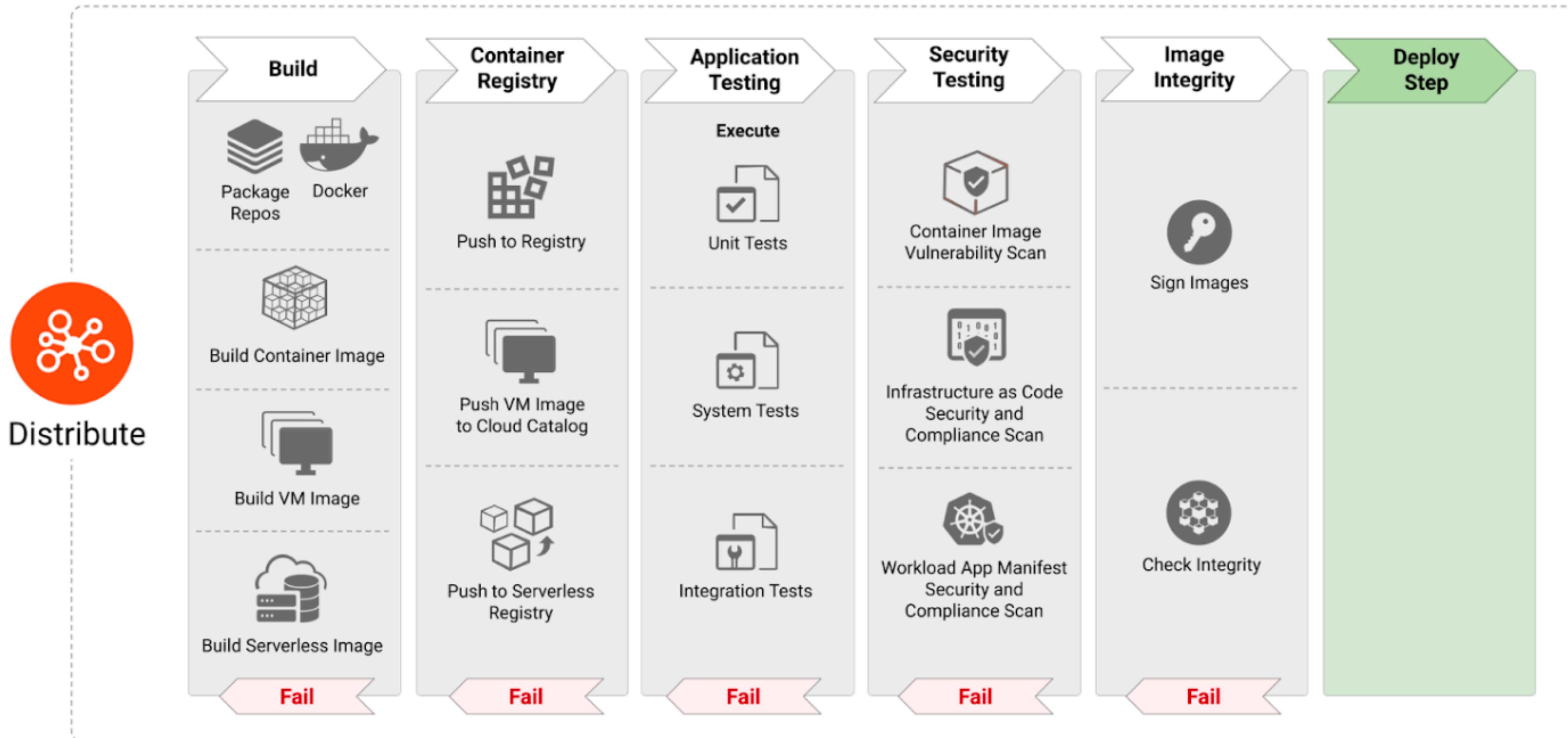
CNCF white paper on cloud native security



Shift Down



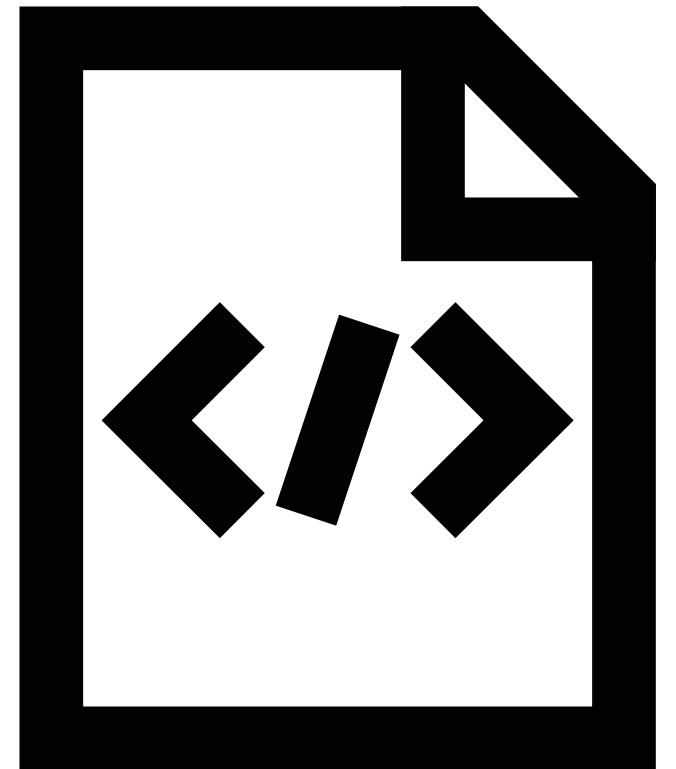
CNCF white paper on cloud native security



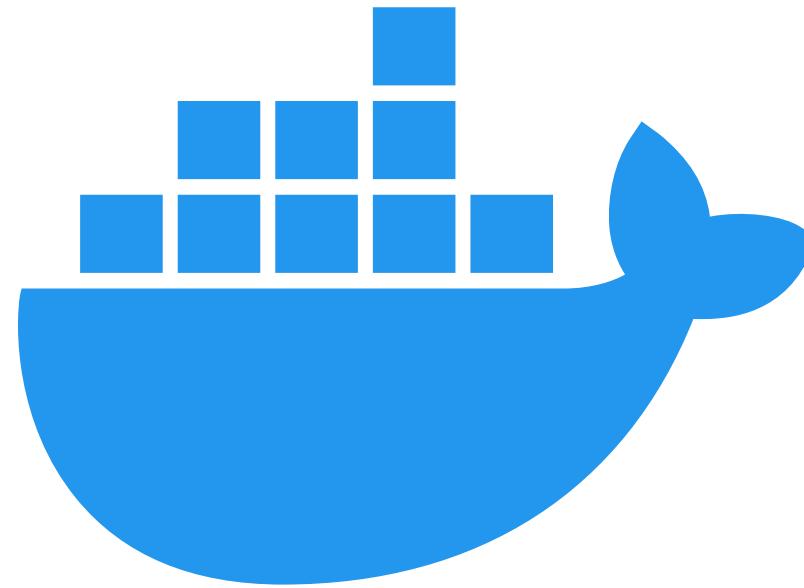
The 4C Security Model



Kubernetes security best practices



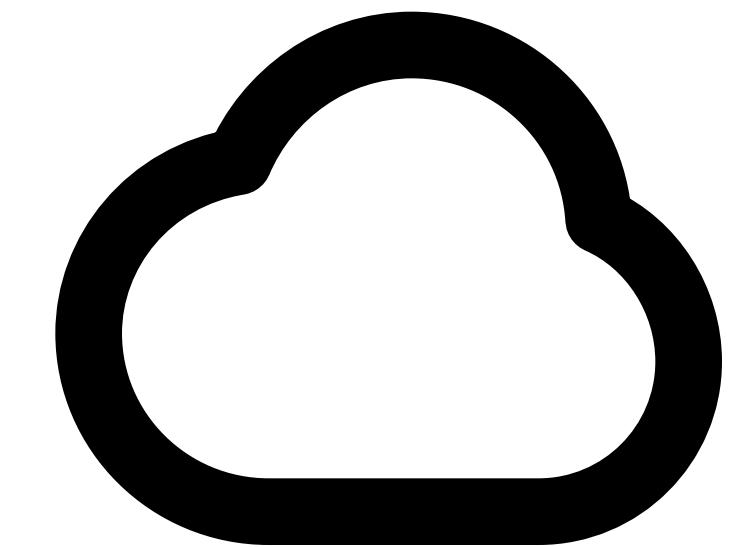
Code



Container



Cluster

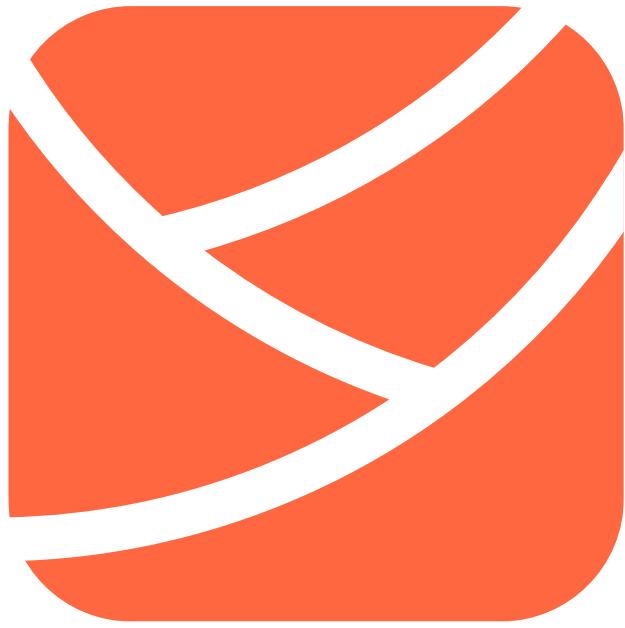


Cloud

SLSA



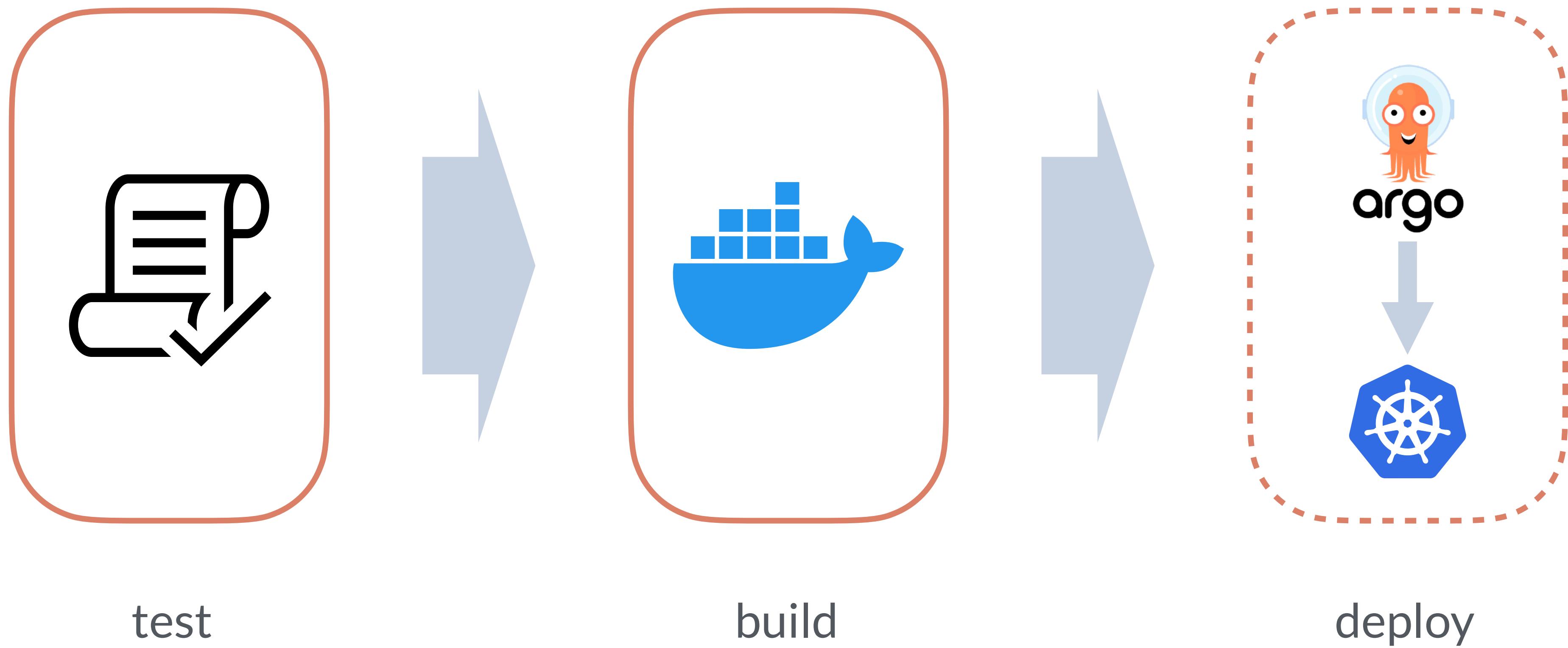
Supply-chain Levels for Software Artifacts



SLSA

<https://slsa.dev/>

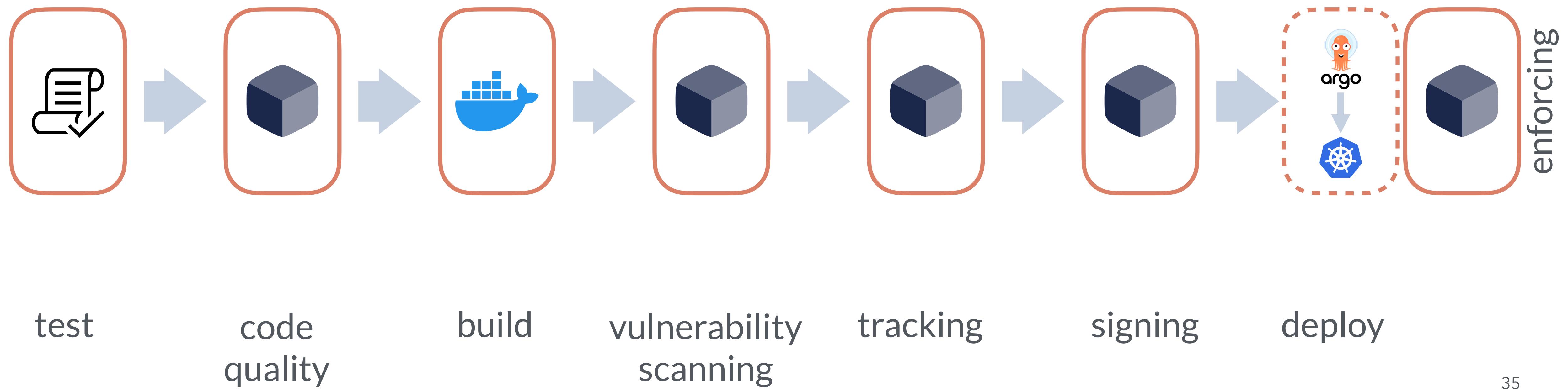
Basic CI/CD Pipeline



DevSecOps Pipeline



Get ready for the CRA using automation and adequate tools



Let's replace the black boxes

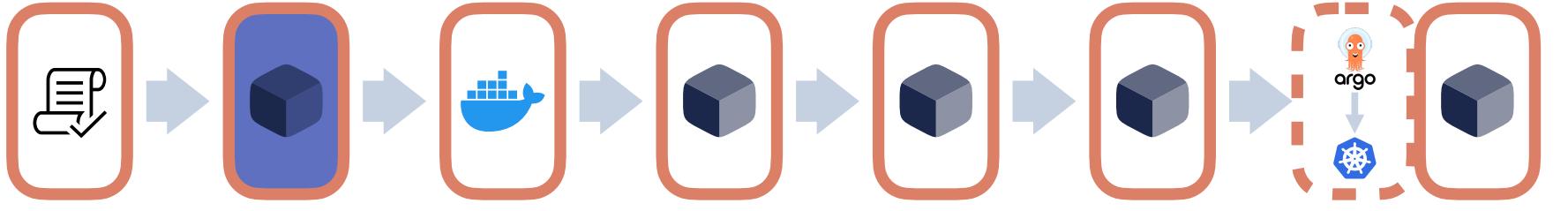


Examples based on open-source tools
- many more exist, both free and commercial

Code quality



Quality and security checks at the lowest level



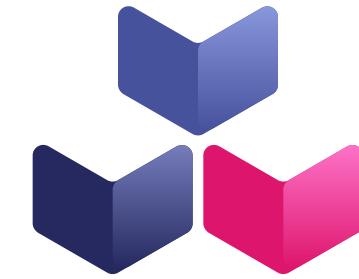
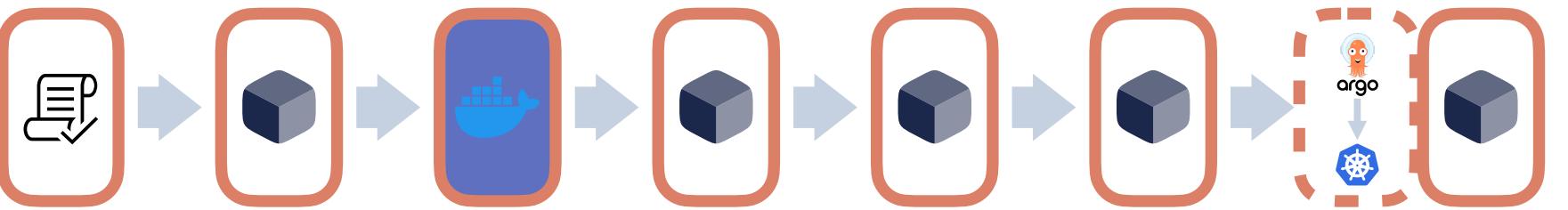
 Semgrep

 sonarqube

Base container



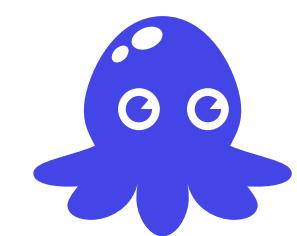
Quality and security checks at the lowest level



Buildpacks.io



Distroless

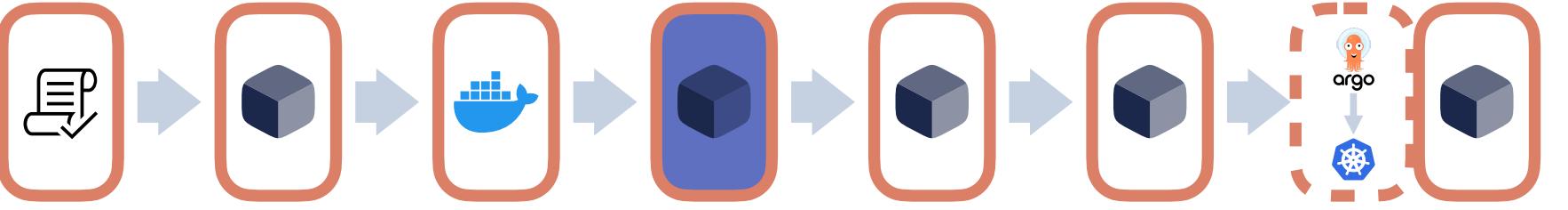


Chainguard

Vulnerability scanning



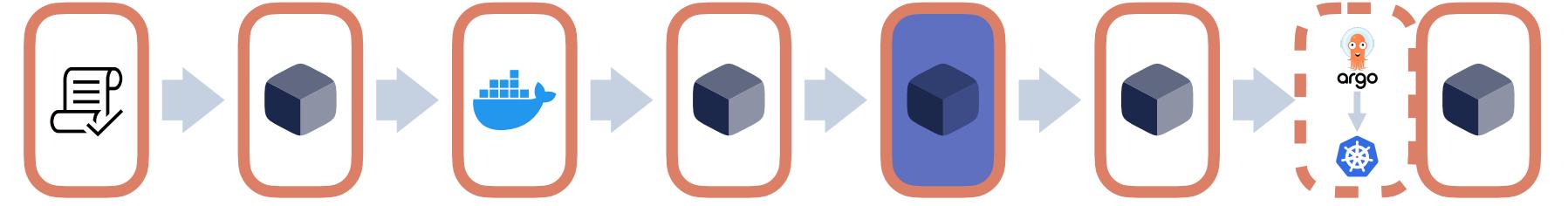
Create SBOMs for vulnerability assessment



Tracking



Create SBOMs for vulnerability assessment



dependency track

Intelligent SBOM analysis platform for managing component risk

<https://dependencytrack.org/>

Dependency Track



Centralized platform for all SBOMs

Home / Projects

33 Portfolio Vulnerabilities

2 Projects at Risk

3 Vulnerable Components

140 Inherited Risk Score

+ Create Project Show inactive projects Show flat project view Search

Project Name	Version	Latest	Classifier	Last BOM Import	BOM Format	Risk Score	Active	Policy Violations	Vulnerabilities
chaoskube	latest		Container	28 Aug 2025 at 14:28:33	CycloneDX 1.6	26	<input checked="" type="checkbox"/>	<div style="width: 100%;"><div style="width: 100%;">0</div></div>	<div style="width: 100%;"><div style="width: 1%;">1</div><div style="width: 2%;">2</div><div style="width: 2%;">2</div></div>
nginx	nginx.SNAPSHOT		Container	28 Aug 2025 at 14:56:15	CycloneDX 1.6	0	<input checked="" type="checkbox"/>	<div style="width: 100%;"><div style="width: 100%;">0</div></div>	<div style="width: 100%;"><div style="width: 0%;">0</div></div>
nginx	1.15		Container	28 Aug 2025 at 14:24:05	CycloneDX 1.6	114	<input checked="" type="checkbox"/>	<div style="width: 100%;"><div style="width: 100%;">0</div></div>	<div style="width: 100%;"><div style="width: 2%;">2</div><div style="width: 10%;">10</div><div style="width: 14%;">14</div><div style="width: 2%;">2</div></div>

Showing 1 to 3 of 3 rows

Dependency Track



Vulnerability audit

[Vulnerabilities By Occurrence](#) [Grouped Vulnerabilities](#)

Filters [Clear all](#) [↻](#) [☰](#)

	Vulnerability	Title	Severity	Analyzer	Published	CWE	CVSSv2	CVSSv3	Project Name	Component	Version	Analysis	Suppressed
Projects	NVD CVE-2015-5237	-	High	NVD	25 Sep 2017	CWE-787	6.5	8.8	chaoskube latest	google.golang.org/protobuf	v1.36.5	⚠	-
Analysis Status	NVD CVE-2019-1543	-	High	NVD	6 Mar 2019	CWE-327, CWE-330	5.8	7.4	nginx 1.15	openssl	1.1.1n-0+deb11u5	-	
Severity	NVD CVE-2021-3712	-	High	NVD	24 Aug 2021	CWE-125	5.8	7.4	nginx 1.15	openssl	1.1.1n-0+deb11u5	-	
Analysis State	NVD CVE-2021-3711	-	Critical	NVD	24 Aug 2021	CWE-120	7.5	9.8	nginx 1.15	openssl	1.1.1n-0+deb11u5	-	
	NVD CVE-2021-23840	-	High	NVD	16 Feb 2021	CWE-190	5.0	7.5	nginx 1.15	openssl	1.1.1n-0+deb11u5	-	
	NVD CVE-2024-3566	-	Critical	NVD	10 Apr 2024	CWE-77	-	9.8	chaoskube latest	stdlib	go1.24.2	Exploitable	
Vendor Response	NVD CVE-2024-7254	-	High	NVD	19 Sep 2024	CWE-20, CWE-787	-	7.5	chaoskube latest	google.golang.org/protobuf	v1.36.5	⚠	In Triage
	NVD CVE-2022-2068	-	Critical	NVD	21 Jun 2022	CWE-78	10.0	9.8	nginx 1.15	openssl	1.1.1n-0+deb11u5	-	
Published	NVD CVE-2022-1292	-	High	NVD	3 May 2022	CWE-78	10.0	7.3	nginx 1.15	openssl	1.1.1n-0+deb11u5	-	
Attributed On	NVD CVE-2022-0778	-	High	NVD	15 Mar 2022	CWE-835	5.0	7.5	nginx 1.15	openssl	1.1.1n-0+deb11u5	-	

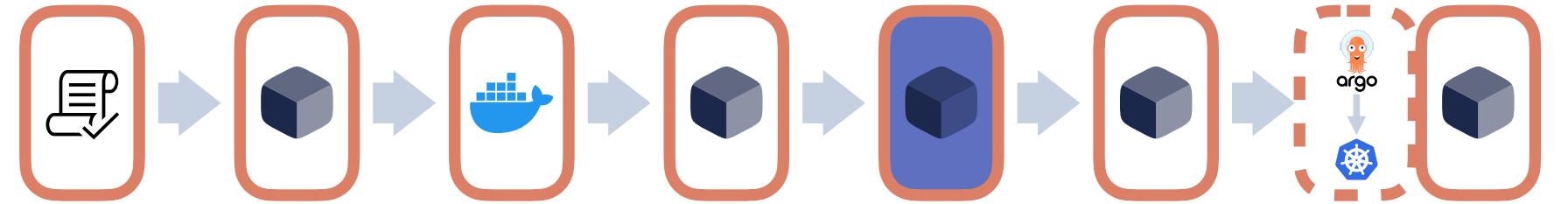
Showing 1 to 10 of 15 rows [10](#) rows per page [From](#) [To](#) [From](#) [To](#)

42

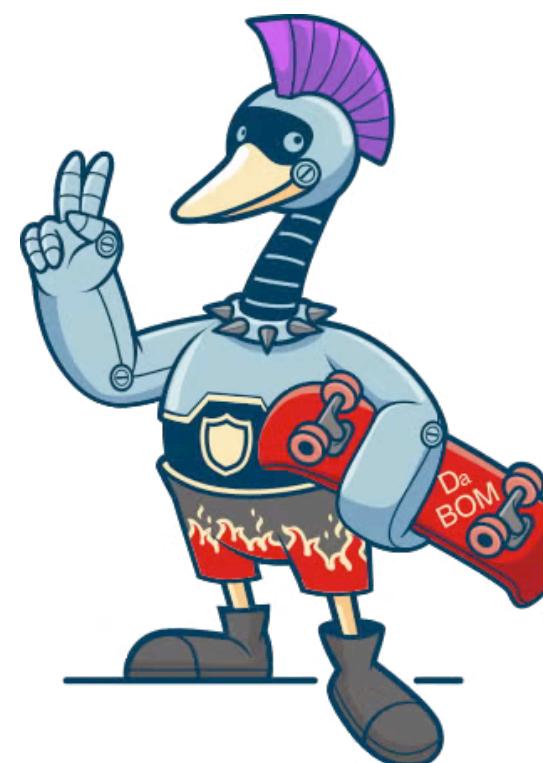
Risk Management



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

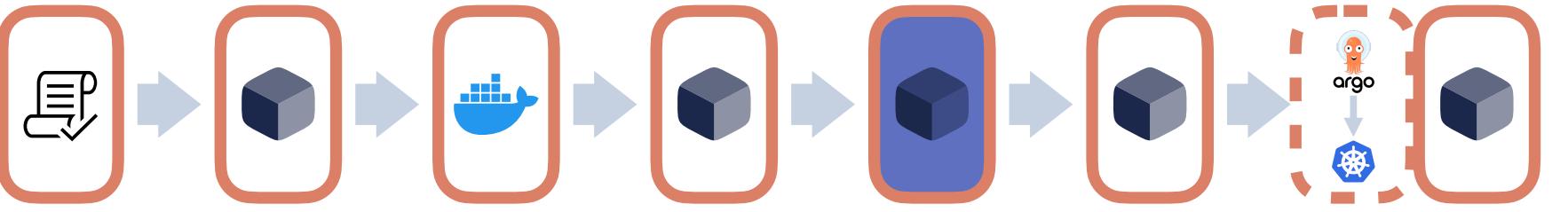
The screenshot displays a detailed view of a vulnerability entry in the Dependency Track application. The top navigation bar includes project names (stdlib, go1.24.2), dependency icons, and version information. The central header provides the NVD ID (CVE-2024-3566), severity (Critical), and last update date (28 Aug 2025). The main content area is divided into several sections:

- 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:** Shows two audit entries from an administrator, dated 1 Sep 2025 at 08:59:45 and 08:59:51, indicating vendor responses: NOT_SET → WILL_NOT_FIX and WILL_NOT_FIX → WORKAROUND_AVAILABLE.
- Comment:** A large text input field for comments, with a "Add Comment" button.
- Analysis:** Status dropdowns for "Exploitable" (selected) and "Suppress".
- Justification:** A dropdown menu currently set to "Not Set".
- Vendor Response (project):** A dropdown menu currently set to "Workaround available".
- Details:** A text area containing the note: "Please use workaround x.y.z".

Risk Management



Share your findings



<https://github.com/aquasecurity/vexhub>

Automated remediation?

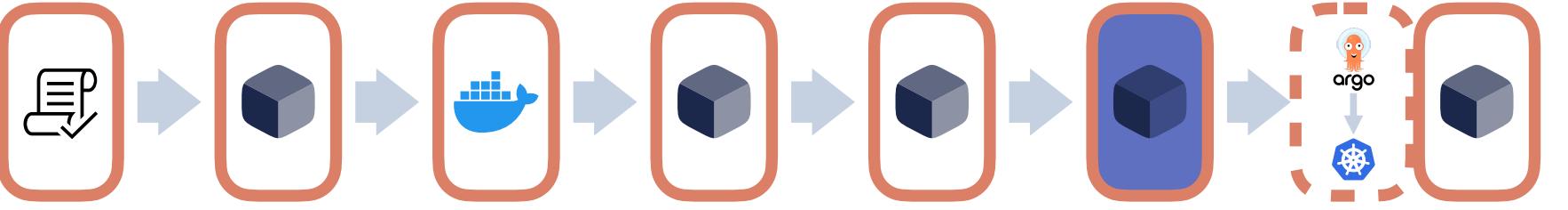


<https://github.com/project-copacetic/copacetic>

Signing



Sign artifacts for supply chain security



sigstore
cosign

<https://github.com/sigstore/cosign>

OCI Artifacts



Open Container Initiative

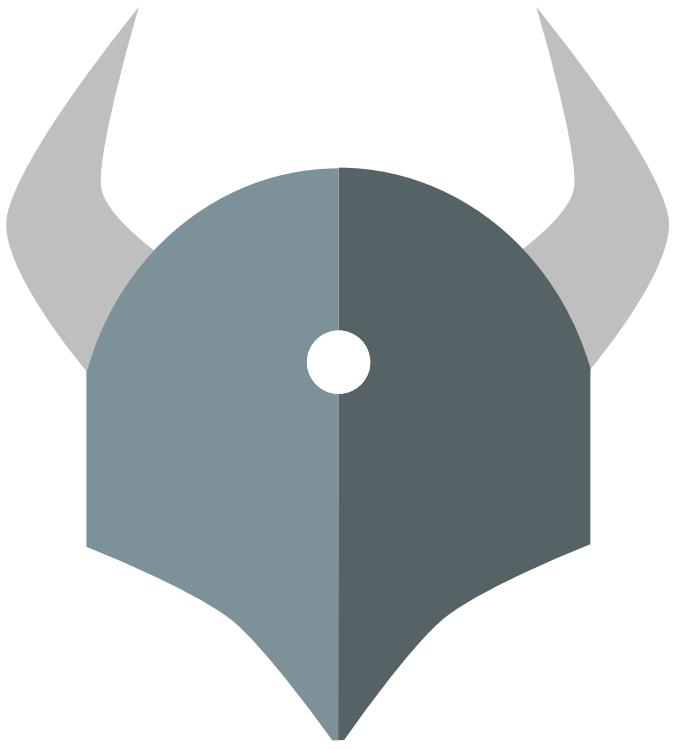
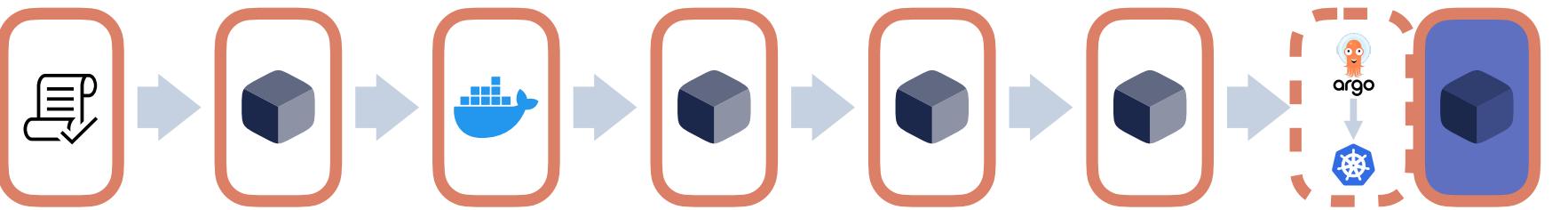


<https://opencontainers.org/>

Enforcing



Enforce supply chain security policies for Kubernetes



OPA gatekeeper

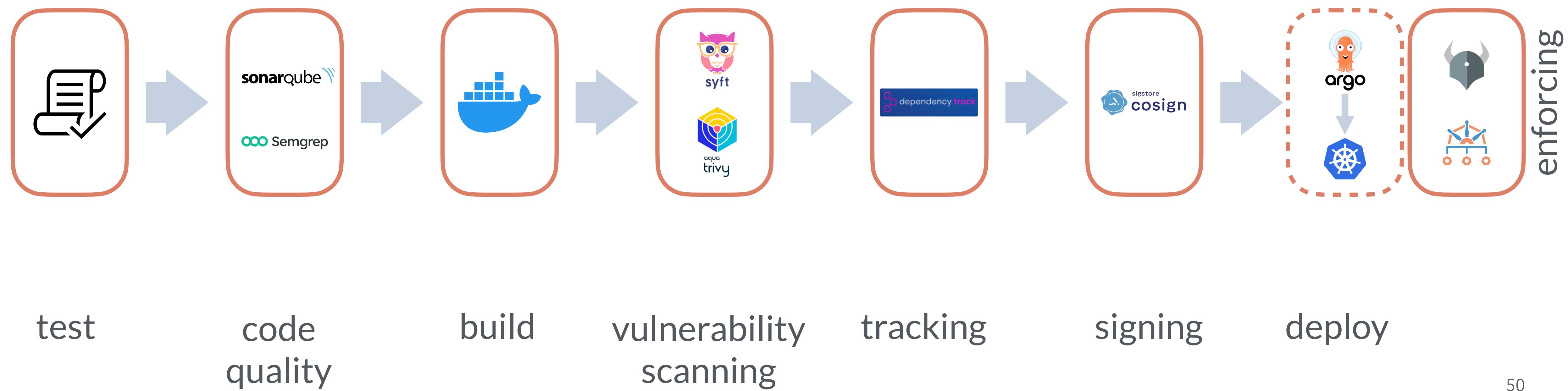


<https://kyverno.io/>

DevSecOps Pipeline



Get ready for the CRA using automation and adequate tools

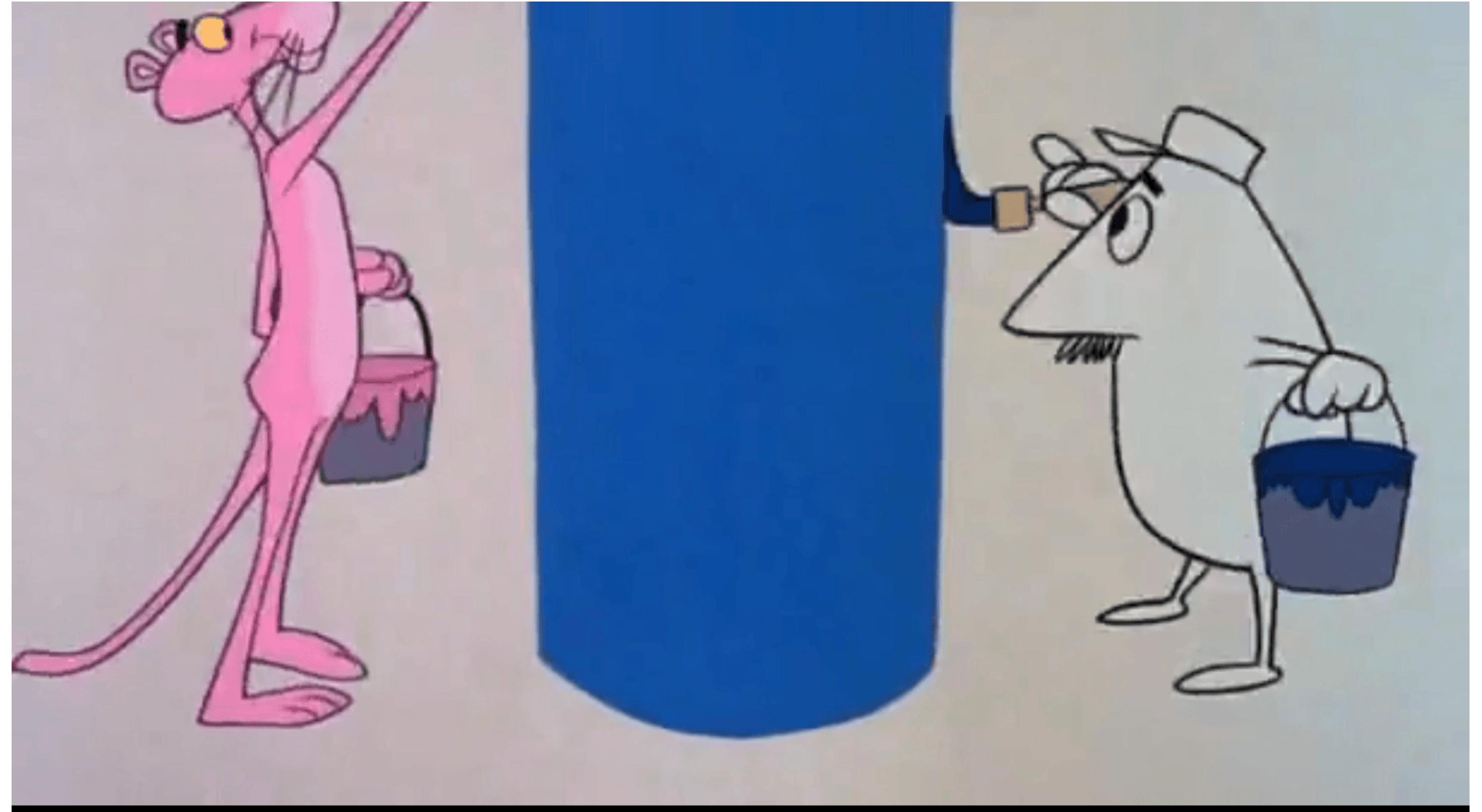


Beyond Build Pipelines



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



SEP 12, 2017

The thumbnail features the NBC peacock logo and the text "CNBC". On the right side, there's the "solarwinds" logo with a stylized arrow. Below the logos, the title "HOW THE BIGGEST HACK OF 2020 WENT DOWN" is displayed in large white letters against a dark background. In the bottom right corner, it says "SWI LISTED NYSE". At the very bottom, there's a small image of the New York Stock Exchange (NYSE) building with American flags in front. Below the main title, the text "The SolarWinds Hack And The Future Of Cyber Espionage" is visible, along with the date "Hochgeladen: 22.01.2021 · 5.137 Positive Bewertungen" and a blue button labeled "Ansehen >".

Need more?

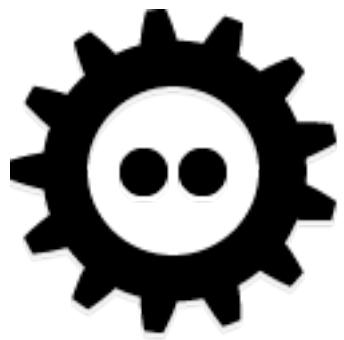


European
Union

[European Cyber Resilience Act](#)



[Linux Foundation Training](#)



[CRA topics on FOSDEM](#)



Slides

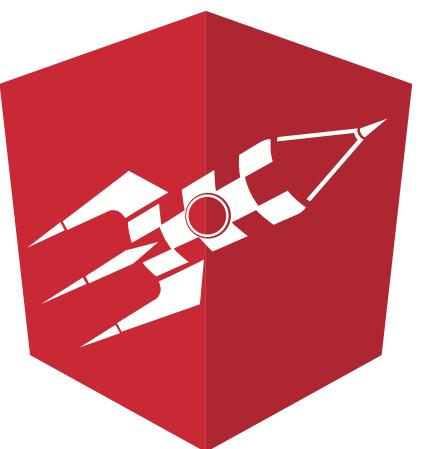
Want more?



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

