

# Stackable TechTalk

Mastering Software Supply Chain Security  
for Financial Services

27.11.24 | 12:00 – 13:00 CET

[SLIDES](#)



 **Stackable**  
your data, your platform



Lukas Voetmand  
Software Architect

Lars Francke  
Co-Founder & CTO

## Recordings of the Talk are Available

YouTube:

- <https://youtube.com/live/6V-69ezDYbg>

Linkedin:

- <https://www.linkedin.com/events/7259561643087421442>



 Stackable

# Stackable in a Nutshell

## Founded

2020

 OpenCore

 b.telligent

IONOS

## Stackable Data Platform

- Open Source
- Infrastructure as Code
- Cloud-native (Kubernetes)
- On-Premises, Cloud, Hybrid

## Our Team: ~20 People

International  
in Germany & Europe

## Our Services

- Product Support
- Big Data Consulting
- Trainings

## Network - Collaborations

















I'm sorry



 Stackable

# Context: Why are we doing this?

  
Stackable

Data Visualisation	 Superset	Analytics & AI	
Data Processing	 trino	 HIVE	 nifi 
Data Storage	 druid	 HBASE 	
Data Integration	 nifi	 kafka	
Infrastructure Orchestration	 Apache Airflow	 Apache ZooKeeper™	

Security

  
Open Policy Agent

Monitoring

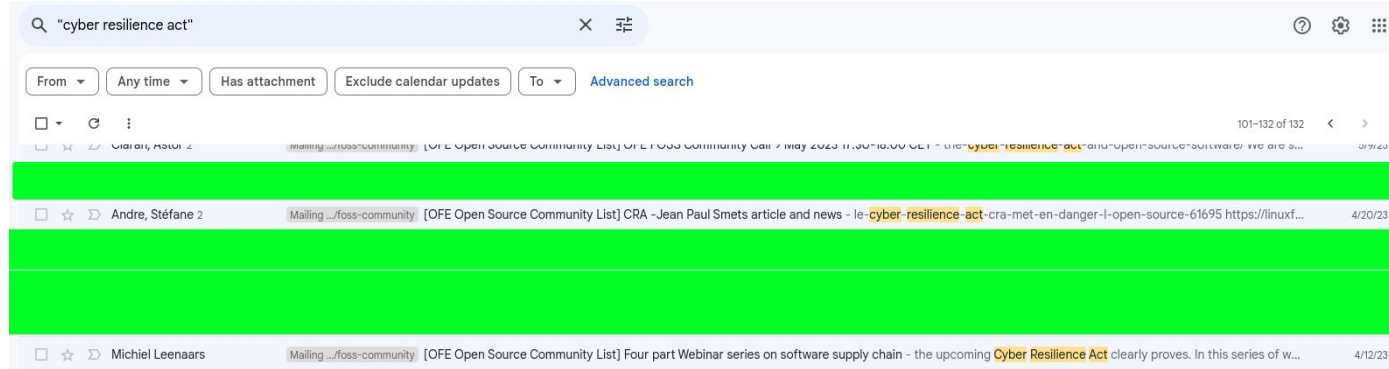


Logging



100% Open Source  
modular and flexible  
In every Cloud and in your own Data Center  
as Managed Service in IONOS Cloud

A long time ago...



The "Cyber Resilience Act" first appeared on my radar in late 2022



Stackable

The story so far...

bitkom



THE  
APACHE®  
SOFTWARE FOUNDATION



OpenForum  
Europe

OSB Open Source  
Business  
ALLIANCE

 Stackable

# Cyber Resilience Act

## Timeline:

- 2022 - At that time:
  - Very little was known
  - *The only certainty is (was) punishment*
- 2022 - 2024: Commenting period, lots of work behind the scenes
- 20 November 2024:
  - Published in the Official Journal of the European Union
- 11 September 2026: Reporting obligations
- 11 December 2027: Fully applicable



## First of its kind:

- Regulation aiming at (almost) all **products with digital elements**
- Previously sector specific regulation did exist (e.g. MDR)

European Commission English Search

## Shaping Europe's digital future

Home Policies Activities News Library Funding Calendar Consultations AI Office

Home > Library > Cyber Resilience Act

POLICY AND LEGISLATION | Publication 15 September 2022

### Cyber Resilience Act

The proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act, bolsters cybersecurity rules to ensure more secure hardware and software products.

Hardware and software products are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of €5.5 trillion by 2021.

Such products suffer from two major problems adding costs for users and the society:

1. a low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and

EU Cyber Resilience Act  
For safer & more secure digital products  
#DigitalEU #CyberSecEU  
© European Union



## If you want all the nitty gritty details

I recently gave a talk on all the details.

From a non-lawyer, trying to answer the practical question of a small "manufacturer": What do I actually (and pragmatically) have to do?

It's in german but if there is interest ping me and I can update and translate it to english



# *Cyber Resilience Act (CRA) und Ich* **Was bedeutet der CRA für mich?**

Bitkom Forum Open Source - 12 September 2024  
Lars Francke - <https://stackable.tech>

[https://drive.google.com/file/d/1XXcR8G371GZv8Tl\\_4vnKmJBfdrbUDbWa/view?usp=drive\\_link](https://drive.google.com/file/d/1XXcR8G371GZv8Tl_4vnKmJBfdrbUDbWa/view?usp=drive_link)

## Cyber Resilience Act - What are we going to do/already doing?

- ✓ SBOMs (<https://sboms.stackable.tech/>)
- ✓ Vulnerability Management
- ✓ Machine readable vulnerability assessments (CSAF)
- ✓ Software Lifecycle Policies
  - Waiting for OpenEoX or OWASP Common Lifecycle Enumeration (CLE) to publish lifecycle information in a machine-readable format
- ✓ Secure by Default and other security practices
- 🧑 Vulnerability Disclosure Policy
- ...

# This lead to...



## Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products

Part 2: Software Bill of Materials (SBOM)



Deutschland  
**Digital•Sicher•BSI**

Die TR lässt sich in ihrem aktuellen Stand nicht anwenden auf Prozesse zur Entwicklung von Software, die üblicherweise als „Open Source Software (OSS)“ oder „Free / Libre and Open Source Software (FLOSS / FOSS)“ bezeichnet werden. Für diesen Zweck müssen die Anforderungen an die Eigenheiten der Entwicklung von Open Source Software angepasst werden.

## Technische Richtlinie TR-03185: Sicherer Software-Lebenszyklus

Version 1.0, Datum 06.08.2024



**CSAF Community Days 2024**

December 12-13, 2024 | Munich, Germany

10:25 - 11:10 CET

[VEX-supported Vulnerability Management with SecObserve](#)

Stefan Fleckenstein & Lukas Voetmand



Need to create SBOMs



# CycloneDX



**Sovereign Tech Agency**

**Rusty SBOMs**

cyclonedx-rust-cargo is emerging as the standard for creating Software Bill of Materials for the Rust ecosystem and the CycloneDX standard

[Rust CI](#) [passing](#) [crates.io](#) [v0.8.0](#) [license](#) [Apache 2.0](#) [https:// cyclonedx.org](https://cyclonedx.org) [Slack](#) [Join](#) [discussion](#) [groups.io](#) [Follow](#)

## CycloneDX Rust (Cargo) Plugin

The CycloneDX module for Rust (Cargo) creates a valid CycloneDX Software Bill of Materials (SBOM) containing an aggregate of all project dependencies. OWASP CycloneDX is a full-stack Bill of Materials (BOM) standard providing advanced supply chain capabilities for cyber risk reduction.

It doesn't end there!



INTERNATIONAL

## About TC54

[Ecma Technical Committee 54](#) is chartered to standardize the [OWASP CycloneDX](#) Bill of Materials specification, standards and algorithms that advance transparency and identity, and the sharing of transparency information across the supply chain.

TC  
54

## Ecma TC54

# Software and System Transparency

Standardizing core data formats, APIs, and algorithms that advance software and system transparency



## CEN/CLC/JTC 13 - Cybersecurity and Data Protection

[General](#) [Structure](#) [Work programme](#) [Published Standards](#)



### CEN/CLC/JTC 13 Subcommittees and Working Groups

Working group	Title
<a href="#">CEN/CLC/JTC 13/WG 1</a>	Chair's Advisory Group
<a href="#">CEN/CLC/JTC 13/WG 10</a>	Cryptography
<a href="#">CEN/CLC/JTC 13/WG 2</a>	Management systems and controls sets
<a href="#">CEN/CLC/JTC 13/WG 3</a>	Security evaluation and assessment
<a href="#">CEN/CLC/JTC 13/WG 5</a>	Data Protection, Privacy and Identity Management
<a href="#">CEN/CLC/JTC 13/WG 6</a>	Product security
<a href="#">CEN/CLC/JTC 13/WG 7</a>	Adhoc group EU 5G Certification scheme support group
<a href="#">CEN/CLC/JTC 13/WG 8</a>	Special Working Group RED Standardization Request
<a href="#">CEN/CLC/JTC 13/WG 9</a>	Special Working Group on Cyber Resilience Act

# Digital Operational Resilience Act (DORA) Network and Information Systems Directive (NIS2) Executive Order 14028

We are not directly affected

BUT: Our customers are/might be  
READ: You?

We help you by making a good and  
secure product, vulnerability  
management and processes around it.

## Digital Operational Resilience Act (DORA)

The [Digital Operational Resilience Act \(DORA\)](#) is a EU regulation that entered into force on 16 January 2023 and will apply as of 17 January 2025.

It aims at strengthening the IT security of financial entities such as banks, insurance companies and investment firms and making sure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption.

DORA brings harmonisation of the rules relating to operational resilience for the financial sector applying to 20 different types of financial entities and ICT third-party service providers.



[Home](#) > [Policies](#) > Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)

## Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)

The NIS2 Directive is the EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.

The EU cybersecurity rules introduced in 2016 were updated by the NIS2 Directive that came into force in 2023. It modernised the existing legal framework to keep up with increased digitisation and an evolving cybersecurity threat landscape. By expanding the scope of the cybersecurity rules to new sectors and entities, it further improves the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole.

[Share](#)

[NIS 2 Directive \(Directive \(EU\) 2022/2555\)](#) [↗](#)

[Questions & answers](#)

## ISO 27001:2022


Control 5.23 (new in the 2022 edition):














*"Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements."*

What better way to have a **cloud exit strategy** than to build your data platform on Stackable?

*No vendor lock-in, runs everywhere Kubernetes runs, migrate between cloud providers easily*

## Context: Why are we doing this?

  
Stackable

Data Visualisation	 Superset	Analytics & AI	
Data Processing	 trino	 HIVE	 nifi 
Data Storage	 druid	 HBASE 	
Data Integration	 nifi	 kafka	
Infrastructure Orchestration	 Apache Airflow	 Apache ZooKeeper™	

Security



Open Policy Agent

Monitoring



Logging



100% Open Source

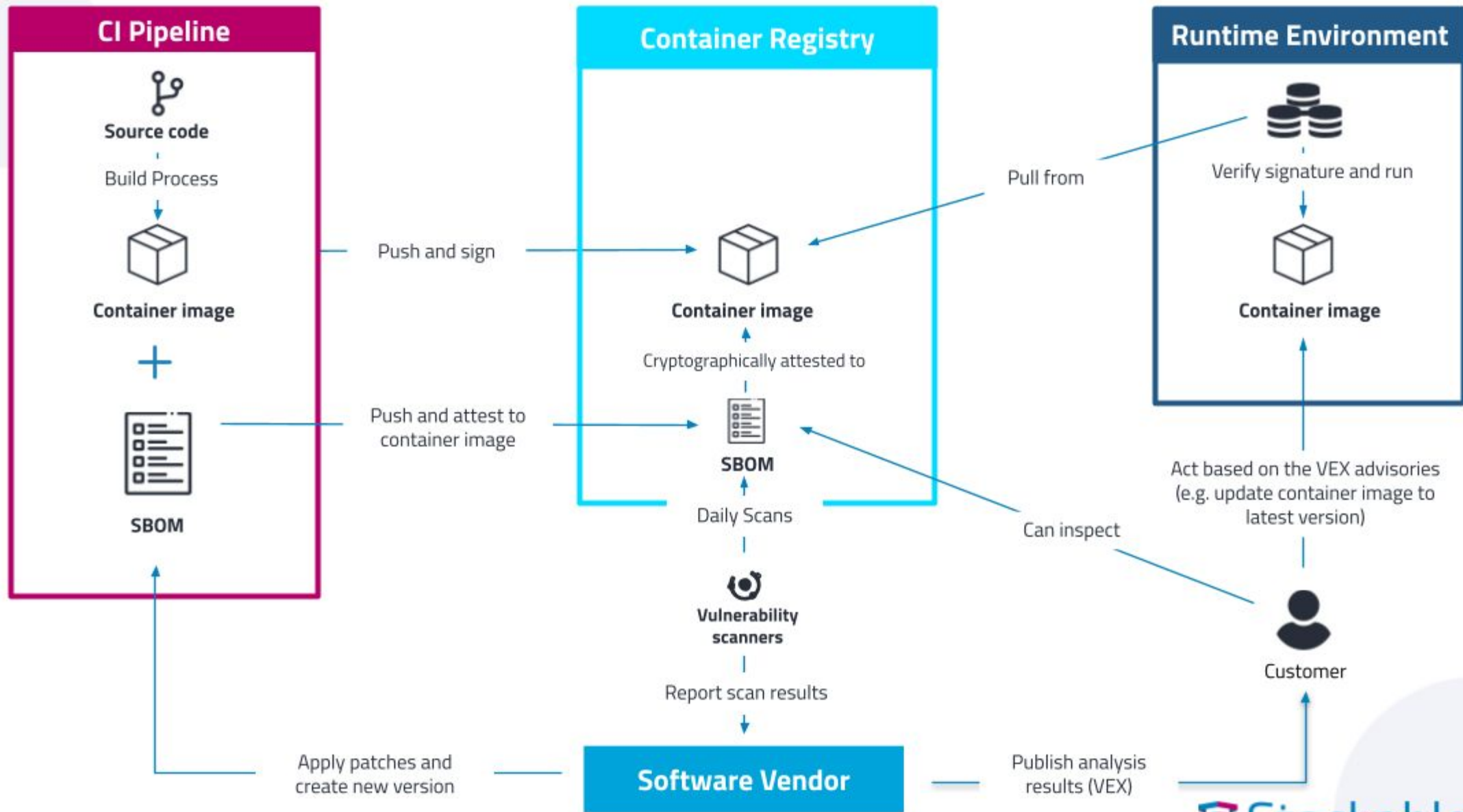
modular and flexible

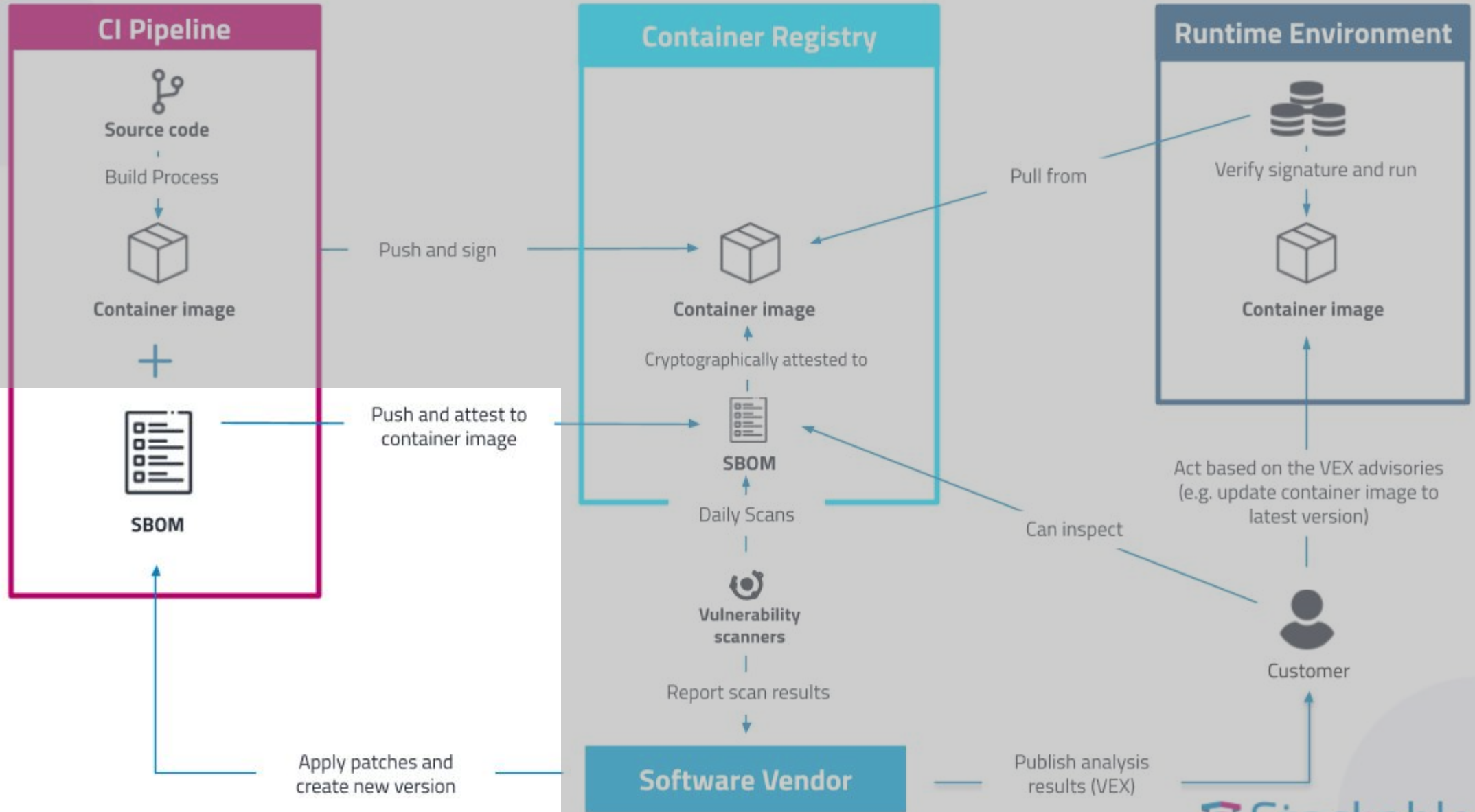
In every Cloud and in  
your own Data Center

as Managed Service in  
IONOS Cloud



**Over to Lukas to show you some of the stuff in action**



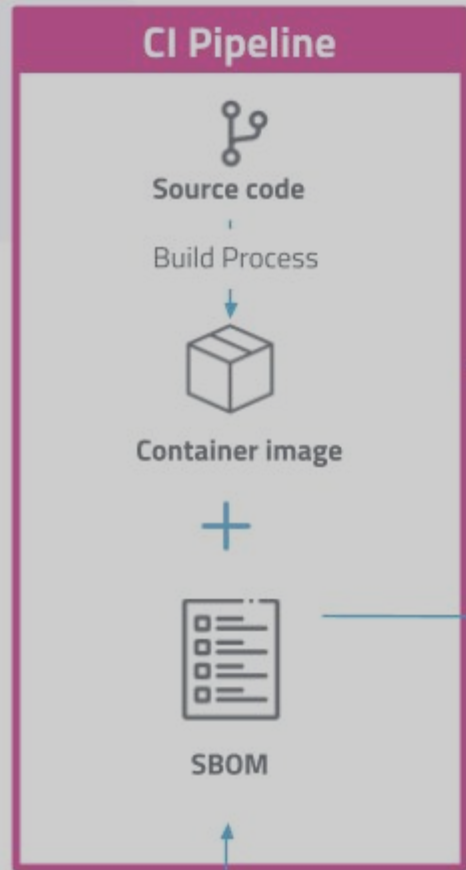


## Software Bill of Materials - SBOMs

### Ingredients:

- Butter
- Sugar
- Eggs
- Flour
- Baking powder
- ...

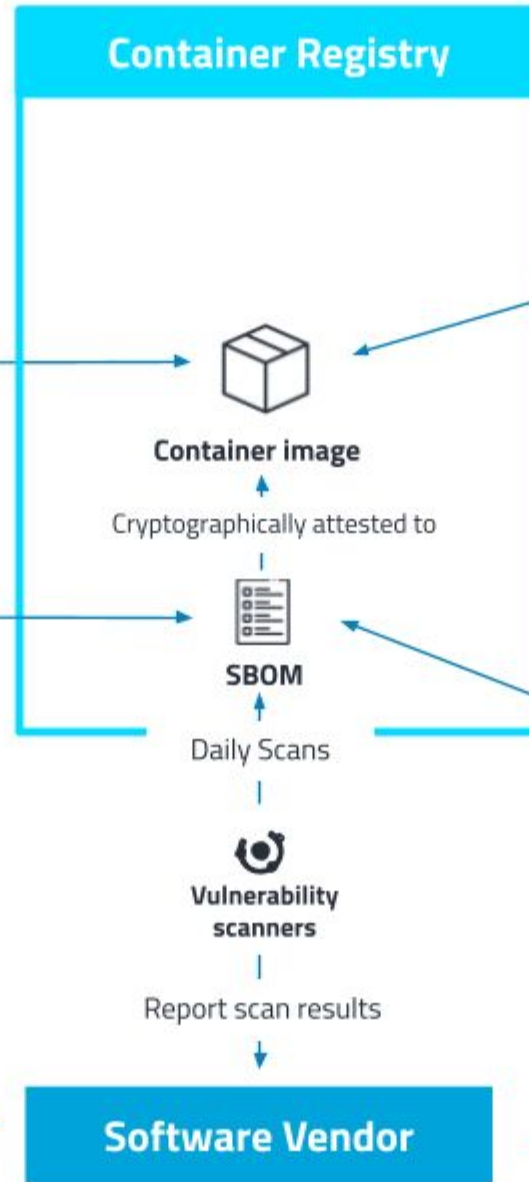




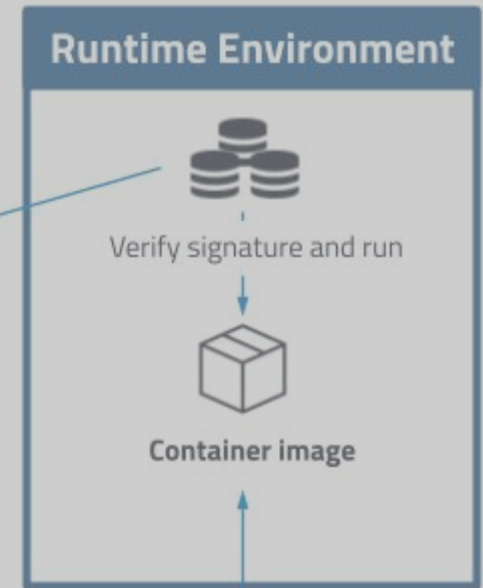
Push and sign

Push and attest to container image

Apply patches and create new version



### Software Vendor



Pull from

Act based on the VEX advisories (e.g. update container image to latest version)

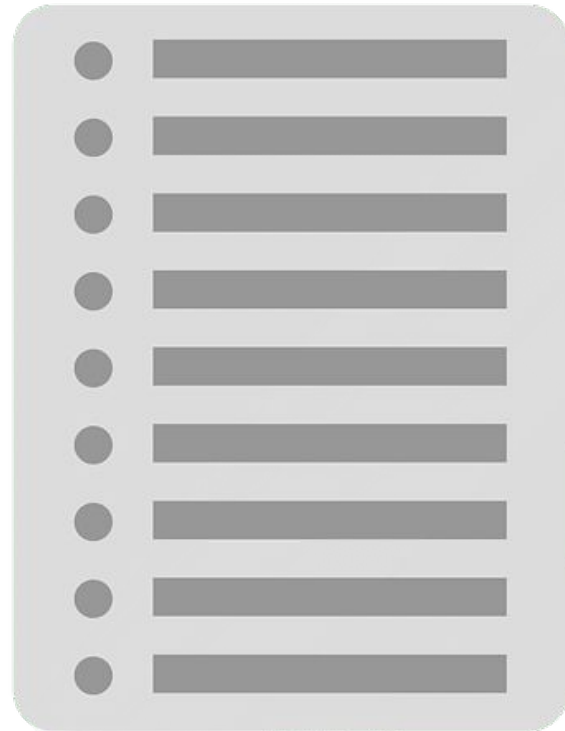
Can inspect

Customer

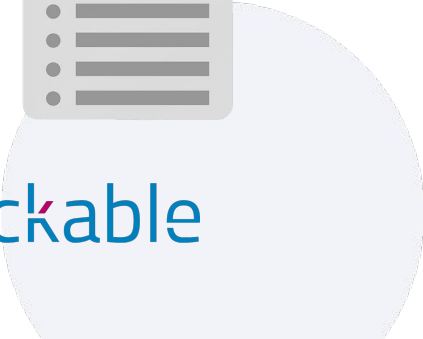
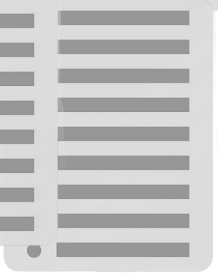
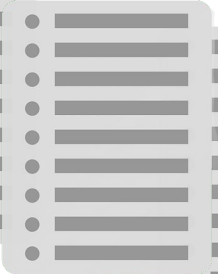
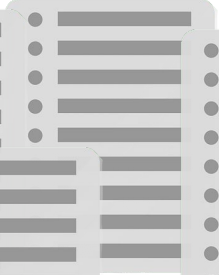
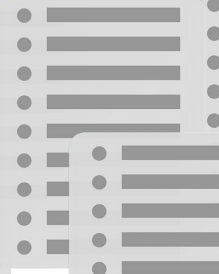
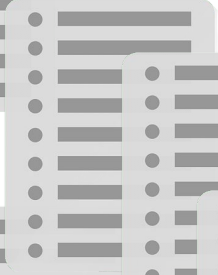
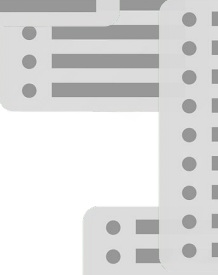
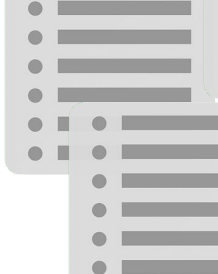
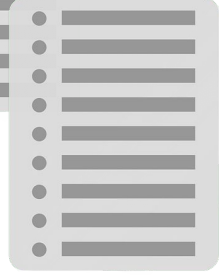
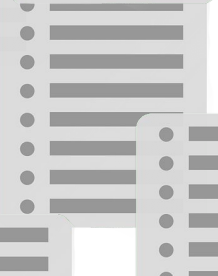
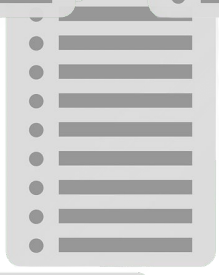
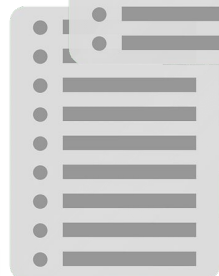
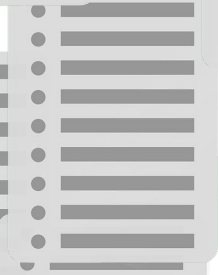
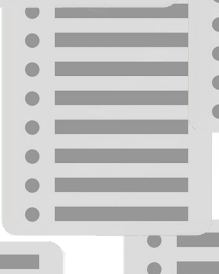
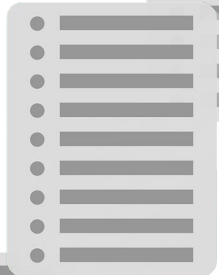
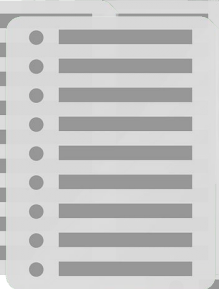
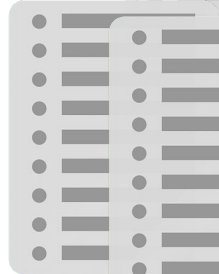
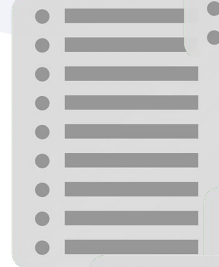
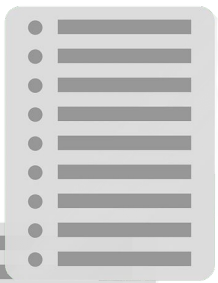
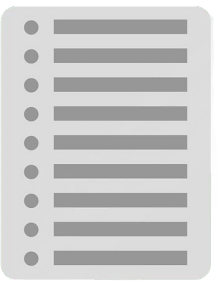
Publish analysis results (VEX)



# Software Bill of Materials - SBOMs



# Vulnerability management



Vulner

manage



# CVSS

9.0 - 10.0	Critical
7.0 - 8.9	High
4.0 - 6.9	Medium
0.1 - 3.9	Low
0	None

# Vulnerability metrics and filters

EPSS: Exploit Prediction Scoring System

CISA KEV: Known Exploited Vulnerabilities Catalog

VulnCheck KEV

Fix available?

# Vulnerability metrics and filters

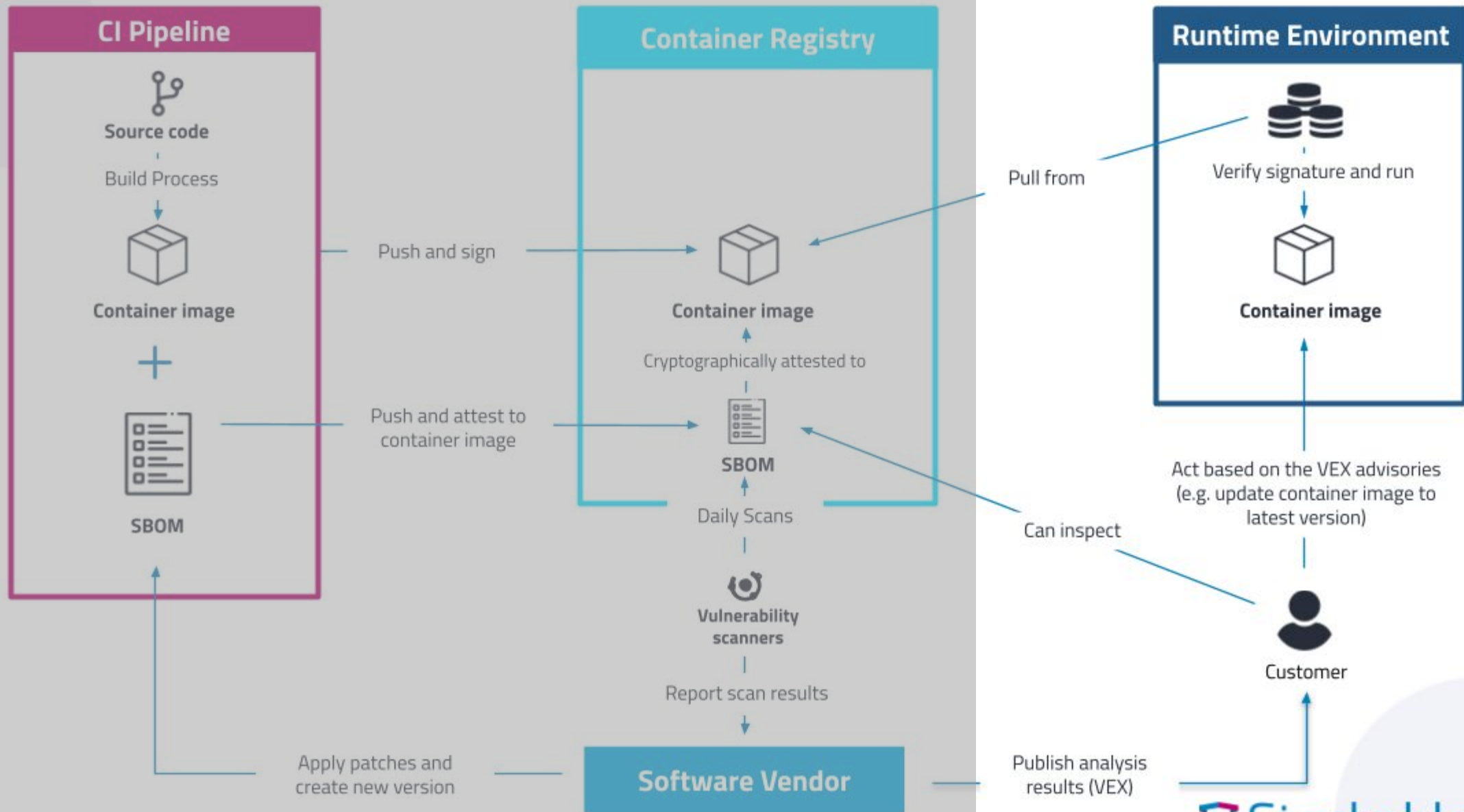
**Observations**

Product:  Product group:  Branch / Version name:  Title:  Severity:

Status:  Component:  Patch available:  Listed in Vulncheck K...:  Component type:

**ADD FILTER**

<input type="checkbox"/>	Product	Group	Branch / Version	Title	Severity	Status	↓ EPSS	Component
> <input type="checkbox"/>	airflow-operator	SDP Operators	24.11.0-amd64	CVE-2019-12900	Critical	Open	1.964	bzip2-libs:1.0.8-8.el9 (rpm)
> <input type="checkbox"/>	airflow-operator	SDP Operators	24.11.0-arm64	CVE-2019-12900	Critical	Open	1.964	bzip2-libs:1.0.8-8.el9 (rpm)



# Vulnerability metrics and filters

## Observation

Severity: **Critical** Status: **Open** Title: **CVE-2019-12900**

Description: BZ2\_decompress in decompress.c in bzip2 through 1.0.6 has an out-of-bounds write when there are many selectors.

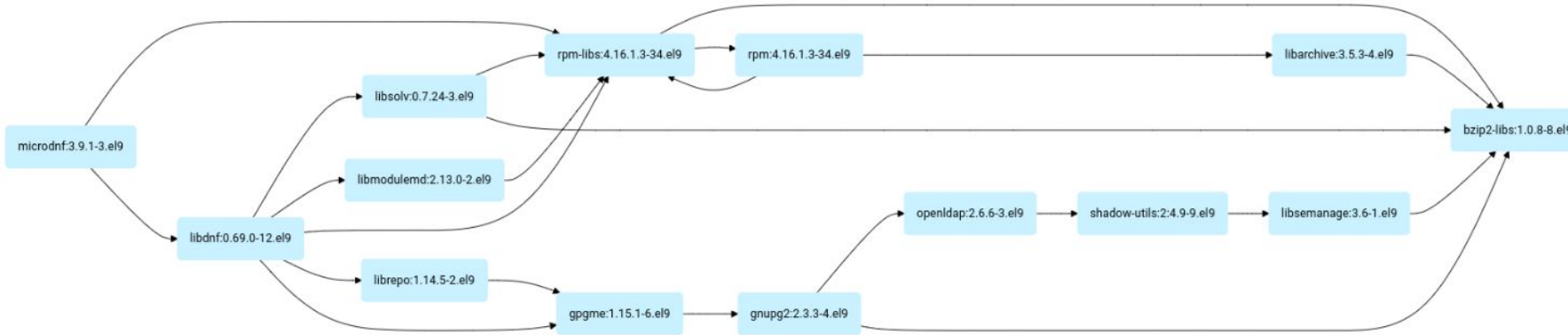
## Vulnerability

Vulnerability ID	CVSS3 score	CVSS3 vector	CWE	EPSS score (%)	EPSS percentile (%)
<a href="#">CVE-2019-12900</a>	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	<a href="#">787</a>	1.964	89.173

## Origins

Component name	Component version	Component PURL	Component CPE
bzip2-libs	1.0.8-8.el9	pkg:rpm/redhat/bzip2-libs@1.0.8-8.el9?arch=x86_64&upstream=bzip2-1.0.8-8.el9.src.rpm&distro=rhel-9.5	cpe:2.3:a:bzip2-libs:bzip2-libs:1.0.8-8.el9:***:***

Component dependency graph



## Metadata

Product: [airflow-operator](#)  
Branch / Version: **24.11.0-amd64**  
Scanner: **trivy / 0.57.0**  
Parser name: **CycloneDX**  
Upload filename: **trivy.json**  
Last change: **11/19/2024, 10:29:06 PM**  
Last seen: **11/21/2024, 4:08:57 AM**  
Created: **11/19/2024, 10:29:06 PM**

## References

- <https://avd.aquasec.com/nvd/cve-2019-12900>
- <http://lists.opensuse.org/opensuse-security-announce/2019-07/msg00040.html>
- <http://lists.opensuse.org/opensuse-security-announce/2019-08/msg00050.html>
- <http://lists.opensuse.org/opensuse-security-announce/2019-11/msg00078.html>
- <http://lists.opensuse.org/opensuse-security-announce/2019-12/msg00000.html>
- <http://packetstormsecurity.com/files/153644/Slackware-Security-Advisory-bzip2-Updates.html>
- <http://packetstormsecurity.com/files/153957/FreeBSD-Security-Advisory-FreeBSD-SA-19-18.bzip2.html>
- <https://access.redhat.com/errata/RHSA-2024:8922>

## Assessing a vulnerability

Status \*  
Not affected

VEX justification  
Vulnerable code not in execute path

✕ CANCEL

💾 SAVE

## Publishing VEX statements



```
[vex] Filtered out the detected vulnerability  
vulnerability-id="CVE-2017-6519"  
product-id="avahi-libs:0.8-20.el9@zookeeper:3.9.2-stackable24.7.0"  
status="not_affected"
```

<https://advisories.stackable.tech>

<https://sboms.stackable.tech>

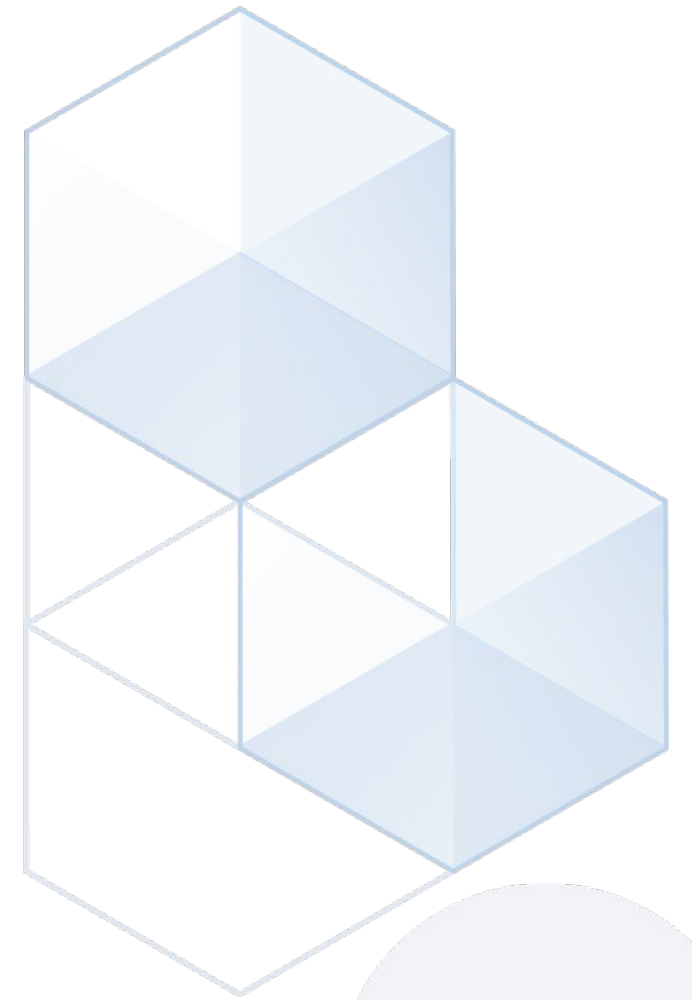


Thank you!

**Lars Francke & Lukas Voetmand**

[info@stackable.tech](mailto:info@stackable.tech)

Stackable



 Stackable

