Digitalisierung souverän gestalten:

von der flexiblen Arbeitsplatzlösung bis zur sicheren Software-Lieferkette mit der Plattform openCode

Leonhard Kugler – Informatik Festival 2025, Potsdam

ZenDiS

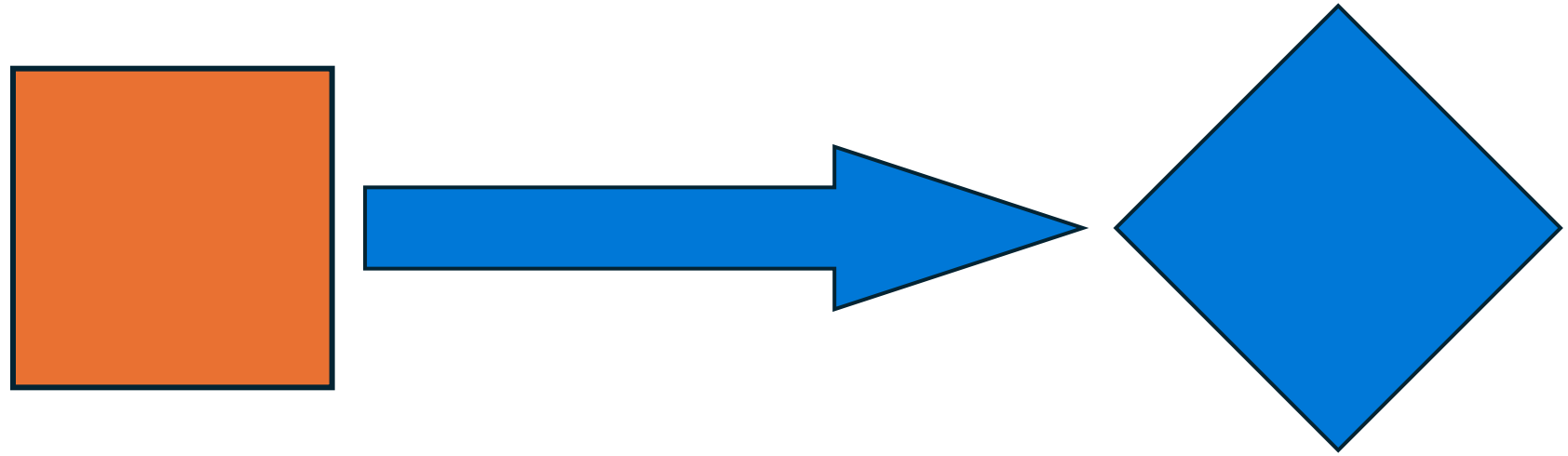
1.300.000.000

1.300.000.000

* (2022) 770.000.000,00 EUR

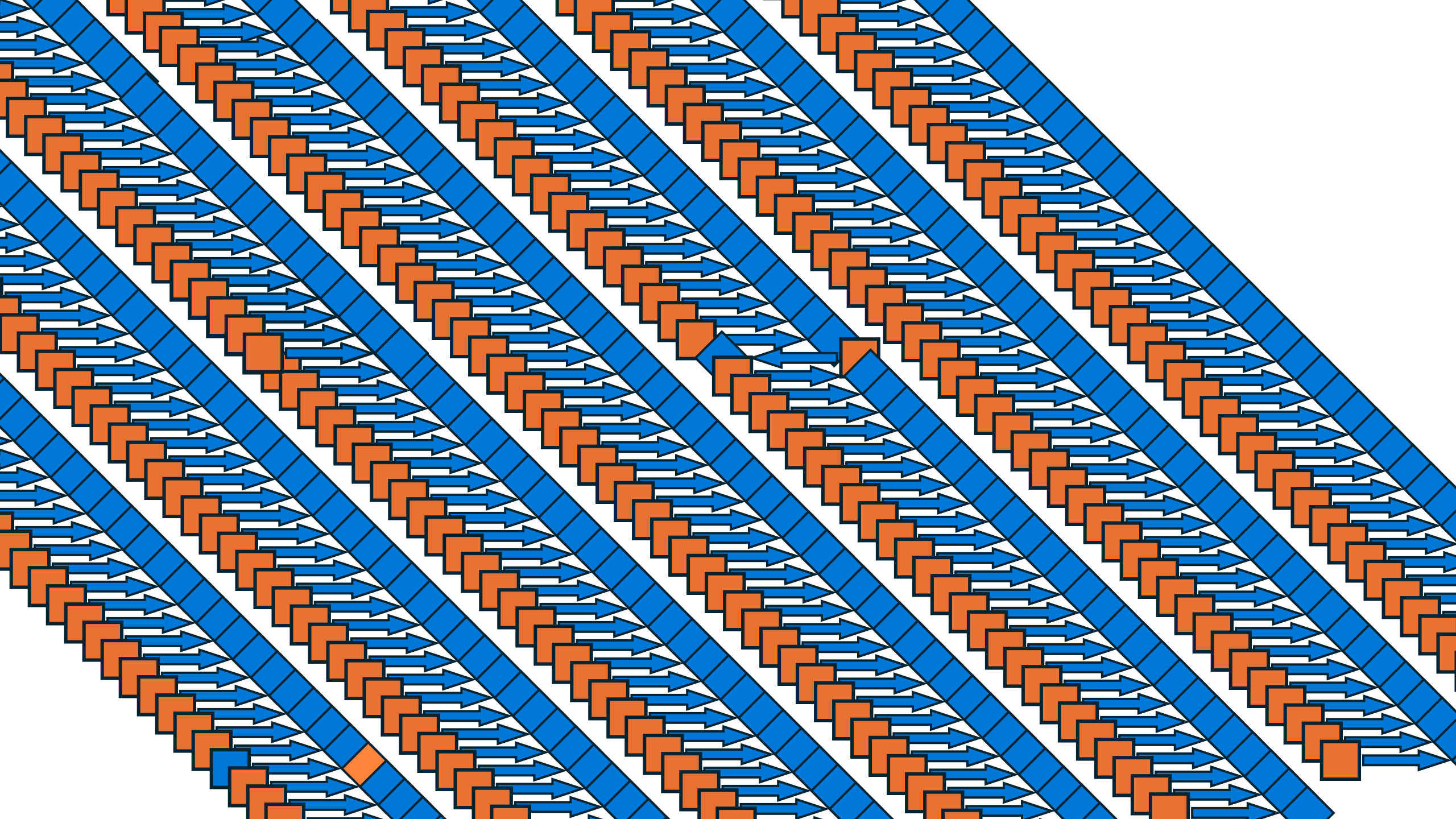
Wir laufen auf einem alten Betriebssystem … Komplex, proprietär – und immer teurer.

Photo: Behnam Norouzi, Unsplash



Problem

Lösung



96 %

Microsoft

75 %

Oracle-DB

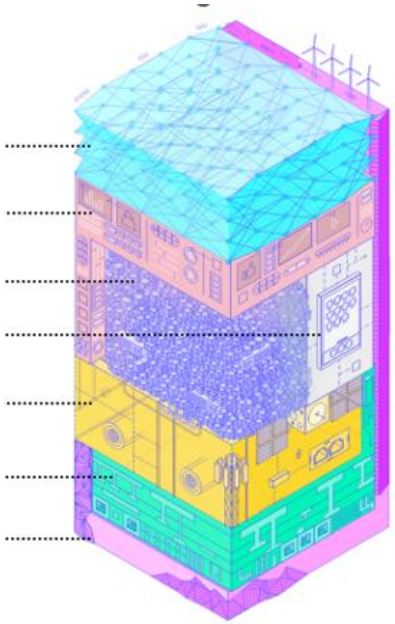
80 %

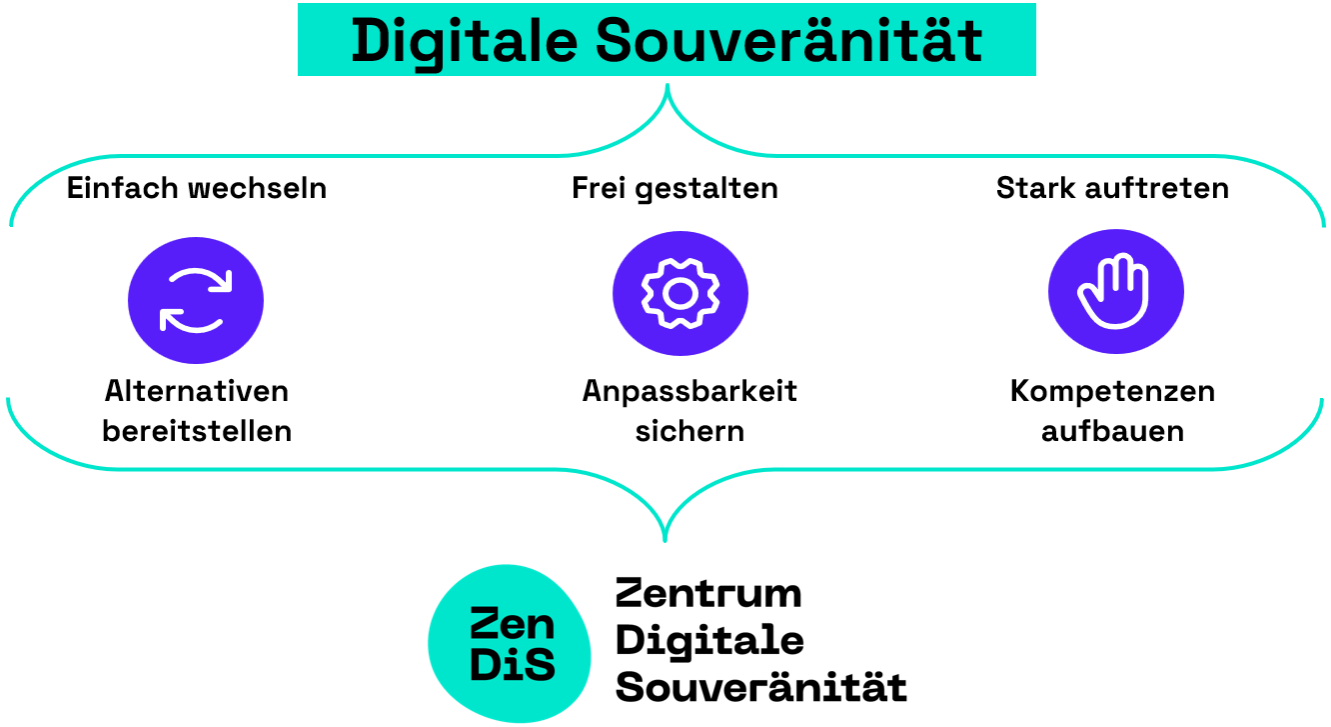
VMWare

101 % *
Lösungen

* wobei 80 % oft mehr als ausreichend wären

Digitale Souveränität ist die Summe aller Fähigkeiten und Möglichkeiten von Individuen und **Institutionen**, ihre Rolle(n) in der digitalen Welt **selbstständig, selbstbestimmt und sicher** ausüben zu können.
IT-Planungsrat, 2020



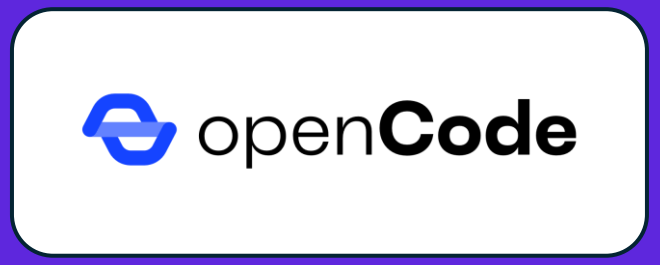


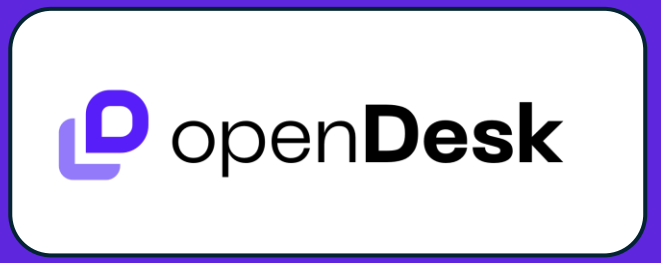
„Wir wollen ein **digital souveränes Deutschland**. Dazu werden wir **digitale Abhängigkeiten abbauen**, indem wir Schlüsseltechnologien entwickeln, Standards sichern, digitale Infrastrukturen schützen und ausbauen. “
Verantwortung für Deutschland – Koalitionsvertrag 2025

Bausteine der souveränen Digitalen Transformation

ZenDiS
(Steward & Enabler)

Produkte / Technologie





Plattform für Digitale Souveränität –
Kooperation / Infrastruktur

Die drei strategischen Bausteine – Der Wandel ist gestaltbar

„Wir müssen Komplexität erkennen und damit arbeiten – nicht sie vermeiden.“

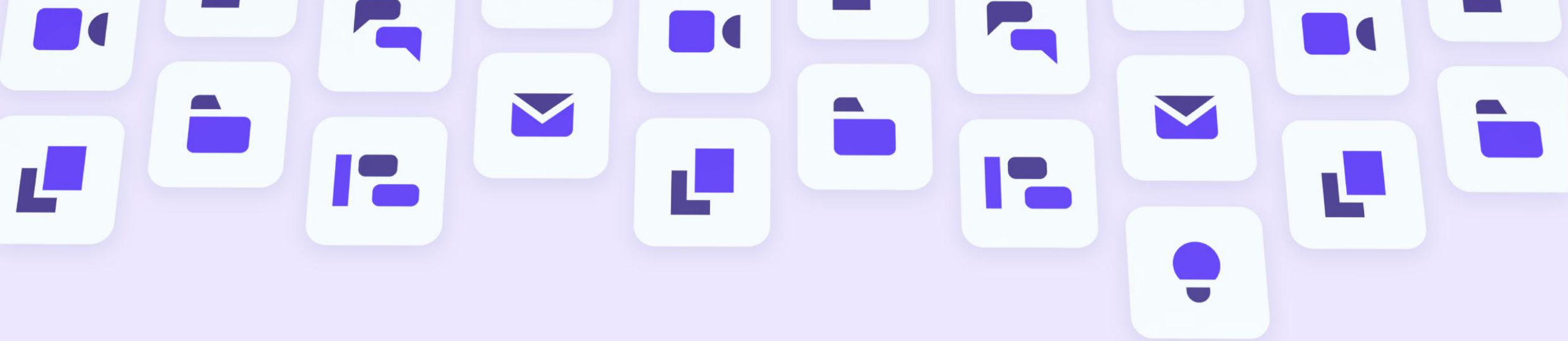
Wir setzen auf drei strategische Bausteine für eine souveräne Digitalisierung:

a) Produkte in den Fokus Weniger Projektdenken – was zählt, ist das Produkt. Nutzerzentrierung, Qualität und Iteration müssen in den Mittelpunkt rücken.

b) Lieferketten kontrollieren Digitale Lieferketten müssen **transparent, sicher und steuerbar** sein.

c) Organisation und Standards etablieren Wir brauchen eine **technologische und organisatorische Baseline** für „Government as a Platform“.

Baustein 1: Produkte – souveräner Arbeitsplatz der Verwaltung



openDesk

Office & Collaboration Suite

Bundesministerium
des Innern

ZenDiS

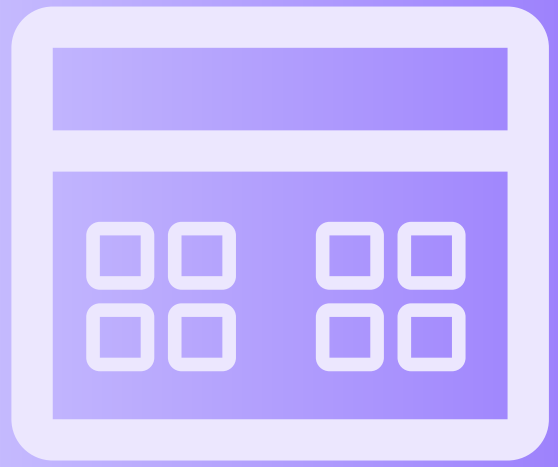
Der erste Schritt hin zu einem vollwertig souveränen Arbeitsplatz.

Schritt für Schritt

heute

openDesk im Browser

morgen



Modularität im Browser

übermorgen

Souveränes Betriebssystem

Baustein 2: Infrastruktur für rechtssichere Kooperation und Softwareentwicklung

Idee,
Angebot

openCode

Qualität und **Funktionsumfang**
Beschaffung und **Compliance**
Sicherheit
Support
rechtssichere **Zusammenarbeit**

Öffentlicher
Sektor

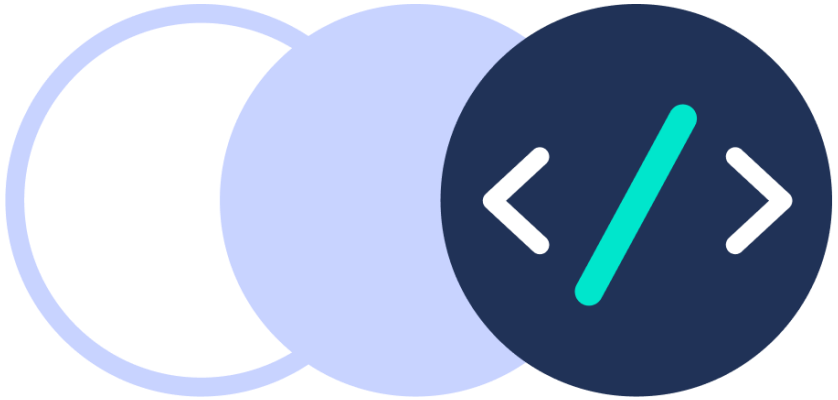
openCode als Enabler für Digitale Souveränität

Fähigkeiten, Dienstleistungen und Lösungen für den öffentlichen Sektor zur Stärkung der Digitalen Souveränität durch Open Source

Ein rechtssicherer Rahmen für die Nachnutzung und den Einsatz von Open Source Software

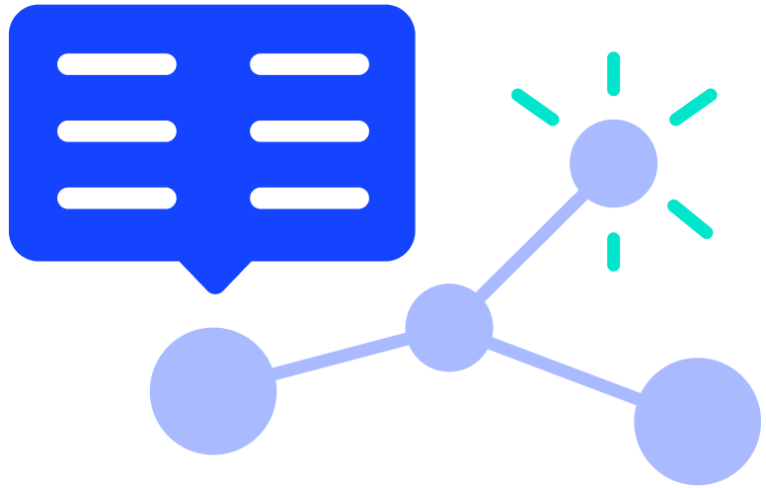
openCode

Open Source entdecken und verstehen



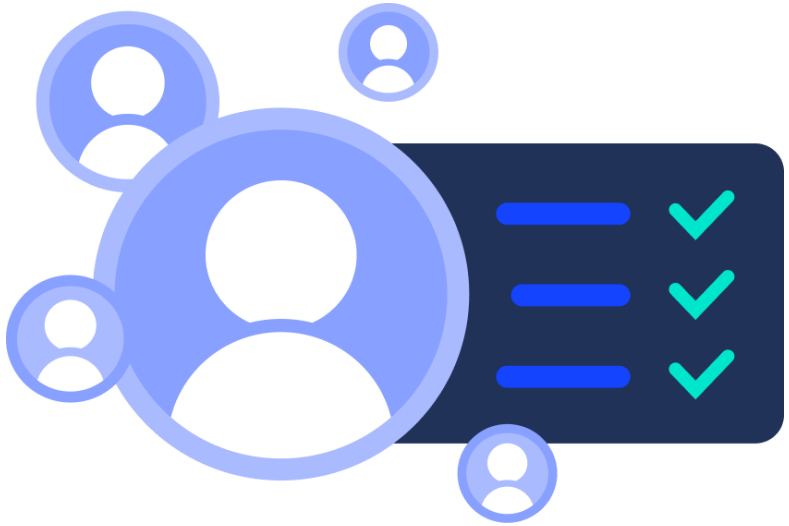
Code teilen und entwickeln

Software finden und nutzen

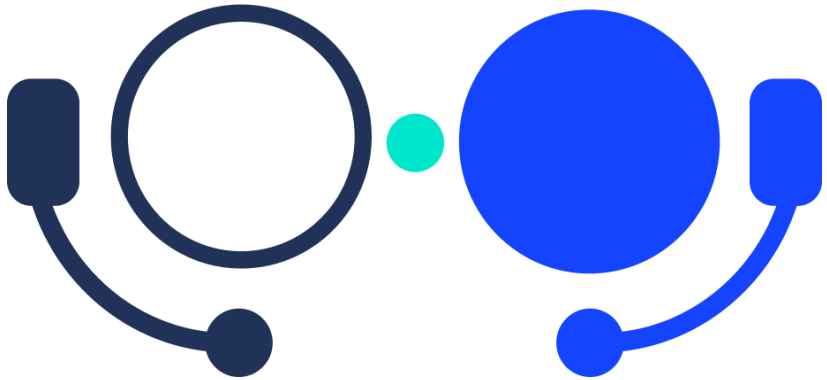


Wissen dokumentieren und vermitteln

Diskurs bieten und partizipieren

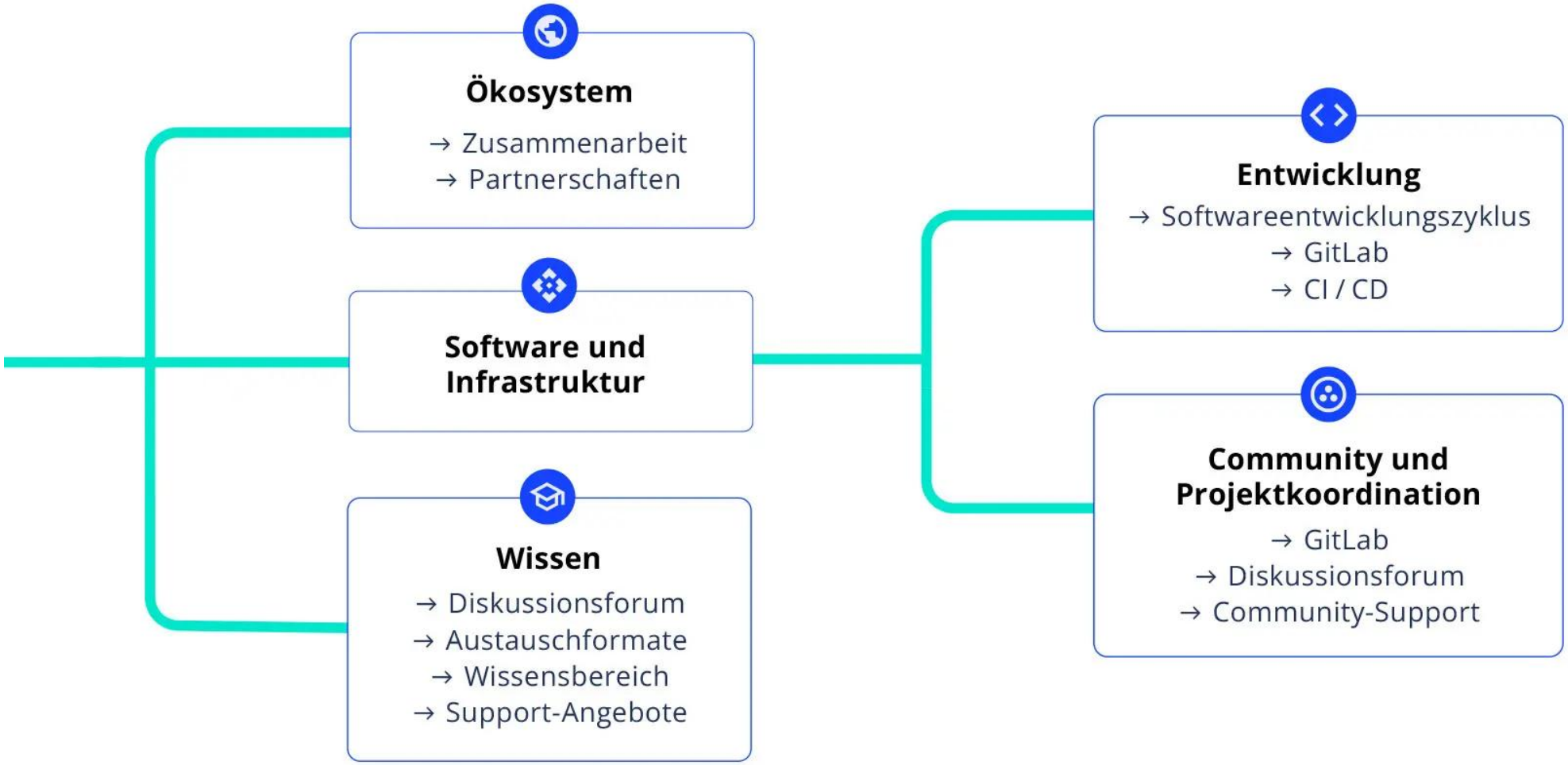


Community pflegen und fördern



Nutzer verstehen und unterstützen

openCode


Ökosystem
→ Zusammenarbeit
→ Partnerschaften
Software und Infrastruktur
Wissen
→ Diskussionsforum
→ Austauschformate
→ Wissensbereich
→ Support-Angebote
Entwicklung
→ Softwareentwicklungszyklus
→ GitLab
→ CI / CD
Community und Projektkoordination
→ GitLab
→ Diskussionsforum
→ Community-Support

openCode

>3.900

Projekte und > **8.000 Nutzende auf der Plattform openCode**. Zusammenarbeit an und Nachnutzung von Lösungen **über alle föderalen Ebenen** – Bund, Länder, Kommunen – hinweg. MPS-Projekte wie **Smart Village App** und **GA Lotse**, Landesinitiativen wie **KERN UX** oder der **Umwelt-Navi**, Projekte im Bund wie der **Bundesmessenger** und **openDesk**. Gemeinsam mit dem **BSI** Strategieaufschlag zur Basis für sichere Softwarelieferketten in Deutschland, vorgesehen als zentrale Infrastrukturkomponente für den **Deutschlandstack** & **internationale Anschlussfähigkeit**.

Baustein 3: Organisation und Governance

Digitale Souveränität

ZenDiS Zentrum Digitale Souveränität

Alternativen bereitstellen

Anpassbarkeit sichern

Kompetenzen aufbauen

openDesk

openCode

Weiterentwicklung eines passgenauen Angebots für die Verwaltung

Community
für Benutzer, Entwickler & Betreiber – Bezugsfähigkeit ausbauen

sSDLC: Compliance, Softwarequalität und -sicherheit kontinuierlich bewerten

Mission von openDesk

openDesk

Bereitstellung einer sicheren Open-Source-Arbeitsplatzlösung für die Öffentliche Verwaltung, die überall eingesetzt werden kann.

- Cloud-Ansatz basiert auf Containertechnologien

Plattform als Teil einer souveränen und sichereren Softwarelieferkette

openCode als Baustein einer souveränen digitalen Infrastruktur

Bundesamt
für Sicherheit in der
Informationstechnik

ZenDiS

Systemische Risiken

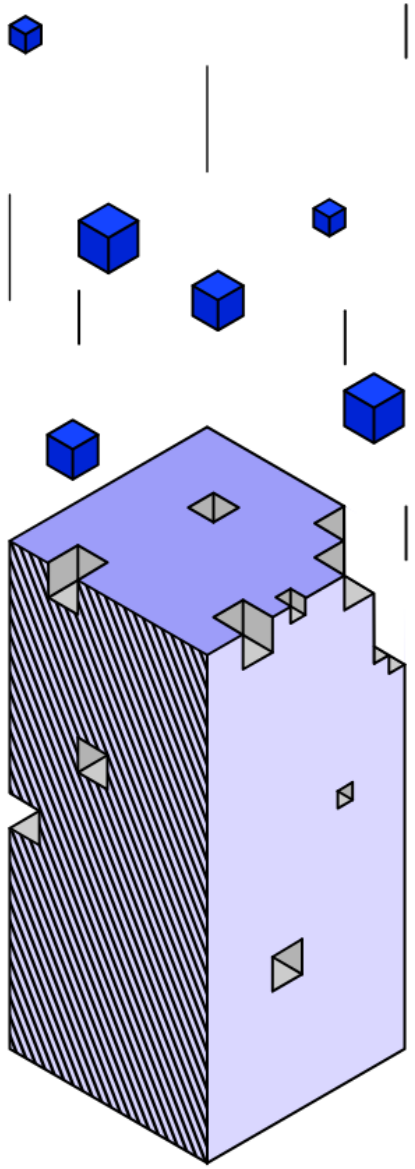
1. **Sicherheitsrisiken:** Kaum Transparenz und Verlässlichkeit in der Lieferkette.

2. **Handlungsunfähigkeit bei Vorfällen:** Behörden können nur allgemein warnen, nicht gezielt reagieren.

3. **Verlust der digitalen Souveränität:** Abhängigkeit von nicht-europäischen Diensten für kritische Infrastruktur, Kontrolle über wesentliche digitale Infrastruktur nicht gegeben.

4. **Fehlende Lagebilder:** Ein zentrales Lagebild der Lieferkette ist hinsichtlich der aktuellen zahlreichen unkoordinierten Teillösungen kaum realisierbar, bzw. die einzigen Lagebilder liegen beim privatwirtschaftlichen Dienstleister der Infrastruktur.

5. **Mangelnde Skalierung:** Manuelle Prüfprozesse können mit der Menge der auszuwertenden Daten im Rahmen moderner Cyberangriffe nicht Schritt halten. Sie erfordern einen unverhältnismäßig hohen Ressourceneinsatz bei gleichzeitig geringerer Zuverlässigkeit.



”**Digitale Infrastrukturen** sind heute ein grundlegender Bestandteil der **Daseinsvorsorge**. Mit ihrer wachsenden Bedeutung wächst auch die **Verantwortung des Staates**, **proaktiv** für ihre Sicherheit und Widerstandsfähigkeit zu sorgen.

Um die digitale Souveränität Deutschlands zu stärken, müssen wir daher einen notwendigen **Paradigmenwechsel** vollziehen: von reaktiven Maßnahmen hin zu **systematischer Prävention durch automatisierte Risikotransparenz**.”

Badge Programm - Vertrauen in Open-Source-Software stärken

Das Badge Programm prüft openCode Repositories und vergibt Badges, die im openCode Softwarekatalog angezeigt werden und den Status der Repositories in Bezug auf Sicherheit, Wartung und Wiederverwendung anzeigen.

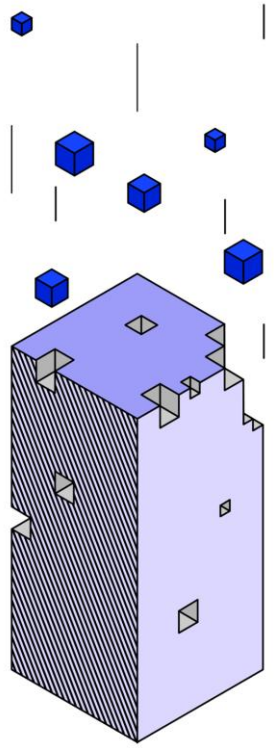
Zur Dokumentation

API Live Demo →

https://badges.opencode.de/de/

Problematik/Motivation

- **Skalierungsproblem** der ÖV im Bezug auf **Compliance und Sicherheit**
  - i.d.R.: Zeit- und ressourcenintensiven Einzelfallprüfungen nach lokalen Kriterien
- **Wachsende Komplexität** moderner Softwarelieferketten, Anzahl an Softwarelösungen wächst schneller als Prüfkapazitäten
- **Transparenz bei Softwarebewertungen:** Sicherheitseinstufung basierend auf vertraglichen Vereinbarungen, Software in erster Linie rechtlich und nicht technisch überprüft.
- **Fehlende Lagebildfähigkeit** da Lieferkettenmetadaten nicht in Open Domain.



Zielrichtung

- Vereinfachung des Weges für diejenigen, die OSS wiederverwenden möchten → Beschaffung und Betrieb
  - Wie können wir **auf einen Blick** zeigen, dass Software ein **Maß an Qualität und Integrität** aufweist?

Das Badge-Programm in der Praxis

- **Automatisierte** und **kontinuierliche** Überprüfung von Software-Repositories nach definierten Kriterien.
- Technologische, statt rechtlicher Prüfung.
- Risikotransparenz und informierte Entscheidungen statt Schadenregulierung.
- Transparente Visualisierung der Ergebnisse durch Badges.
  - Detaillierte Erklärungen zu jeder Bewertung

→ Zertifizierung des Prozesses anstelle jedes einzelnen Produkts

Der Weg zur Badge: Grundprinzipien

1. **„Die Qualität einer Software wird wesentlich durch die Projektorganisation beeinflusst.“ [1]**
   Wir testen auf Metaebene, mit einem gleichen Maßstab für alle.
   Den Code selbst können wir nicht inhaltlich bewerten.

2. **Nur True/False-Ergebnisse; kein Verrechnen**

3. **Unsere Zielgruppe ist nicht technisch → einfaches Ergebnisschema**

[1] Dr. Marc Ohm, Studie zum Vergleich der Sicherheit von Open-Source-Software und proprietärer Software, i. A. OSBA, Juni 2023

Der Weg zur Badge: Konzeption

Bundesamt
für Sicherheit in der
Informationstechnik

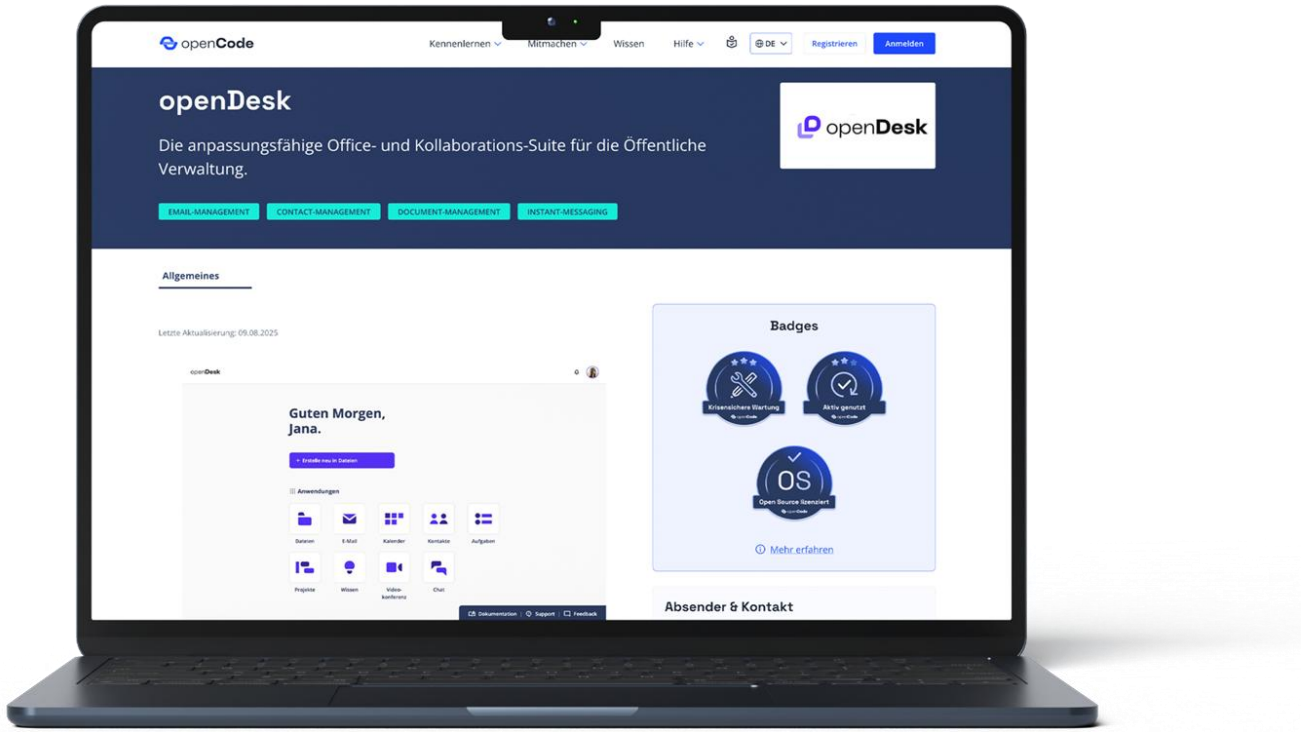
「openssf
scorecard」

Studie zum Vergleich der Sicherheit von Open-Source-Software und Proprietärer Software

Im Auftrag der
Open Source Business Alliance (OSBA)

ausgearbeitet von
Dr. Marc Ohm

Der Weg zur Badge: Softwareverzeichnis



Vertrauen & Verlässlichkeit
bei der Beschaffung von Open-Source-Software

https://opencode.de/de/software/open-desk-351 50%

openDesk

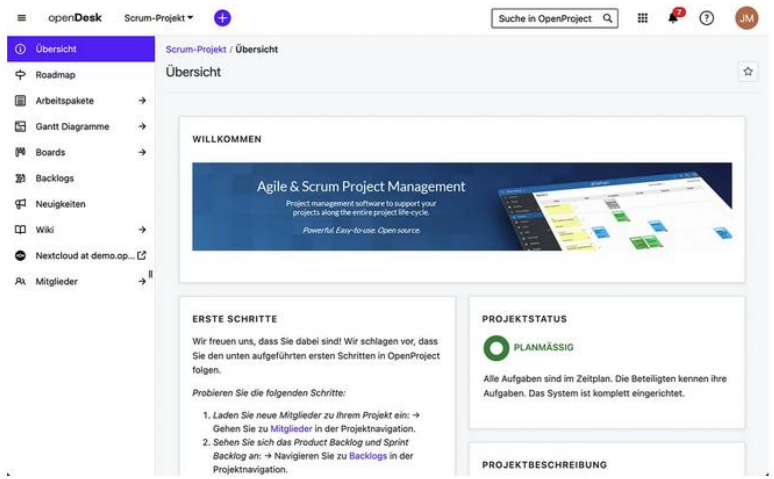
Die anpassungsfähige Office- und Kollaborations-Suite für die Öffentliche Verwaltung.

openDesk

EMAIL-MANAGEMENT CONTACT-MANAGEMENT DOCUMENT-MANAGEMENT INSTANT-MESSAGING

Allgemeines Aktive Nutzungen

Letzte Aktualisierung: 29.01.2025



openDesk ist die anpassungsfähige Office- und Kollaborations-Suite, die speziell für Ihre Bedürfnisse in der Öffentlichen Verwaltung entwickelt wurde.

Badges

Aktive Wartung

Aktiv genutzt

OS
Open Source lizenziert

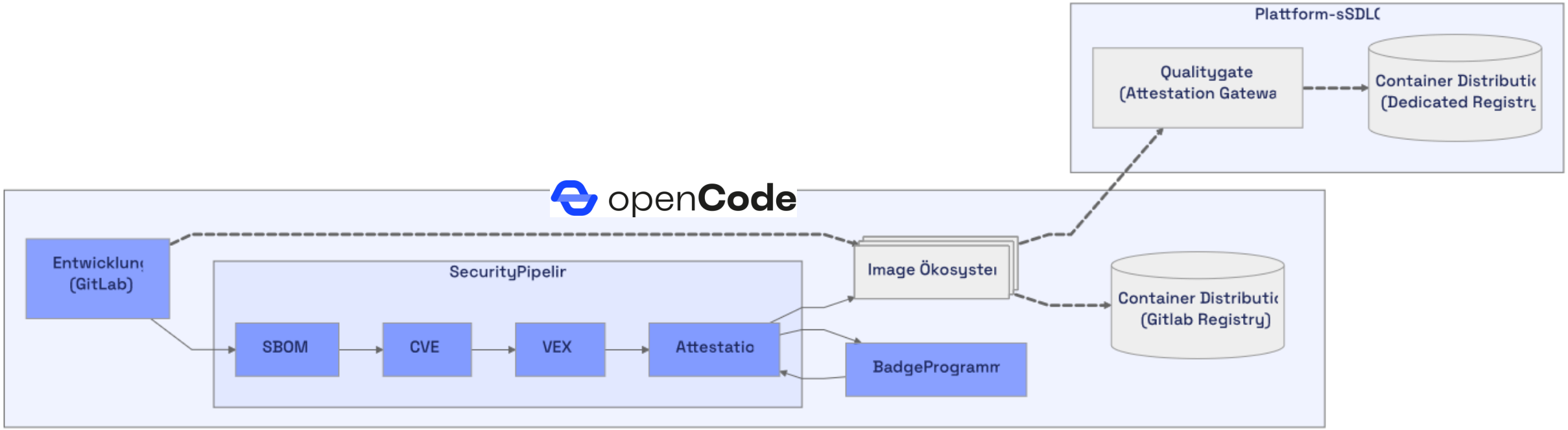
42

Mehr erfahren

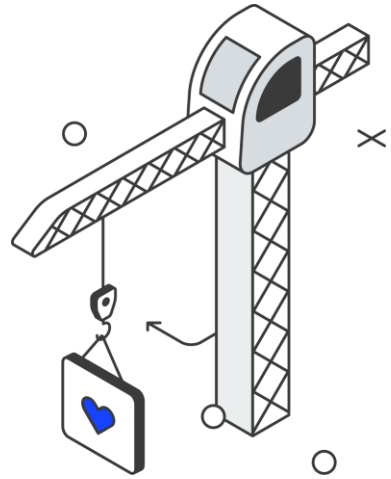
Absender & Kontakt

René Fischer
opendesk@zendis.de

SDLC Mission 1: Compliance as Code



Roadmap: Security Badge Level 3



Level 1: Basis Sicherheit

- Reaktionszeit auf Issues: Die durchschnittliche Reaktionszeit auf Issues, welche innerhalb der letzten 3 Monate entstanden sind, beträgt weniger als 7 Tage.
- Geschützte Branches: Der default Branch ist als `protected` konfuguriert und es sind keine Force-Pushes auf den default Branch erlaubt.
- Sicherheitsrichtlinie: Prüft, ob eine Datei `SECURITY.md` im Stammverzeichnis des Default-Branches existiert

Level 2: Erweiterte Sicherheit

- Alle Kriterien aus Level 1
- Code Review: Prüft, ob mind. 75% der Merge Requeste in den letzten 6 Monaten durch einen Maintainer geprüft wurden.
- Signierte Tags: Prüft, ob mind. 80% der Tags der letzten 6 Monate signiert wurden

Level 3: Umfassende Sicherheit

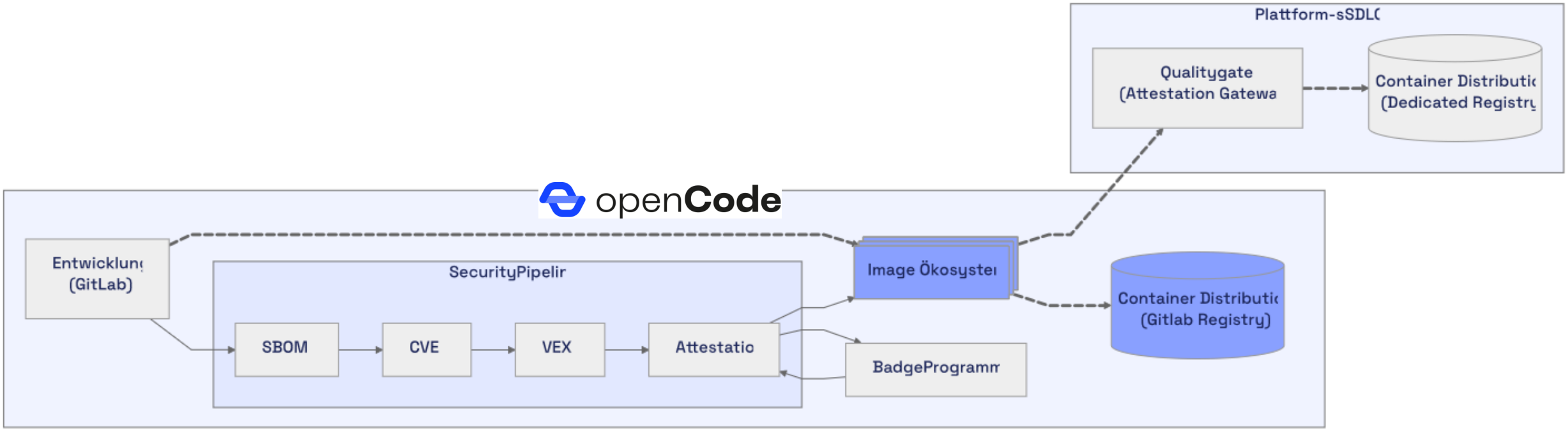
- Alle Kriterien der Level 1 und 2
- Letzte Releases ohne bekannte kritische Schwachstellen: TBD
- Schwachstellenmanagement - Behebungszeit von CVEs: TBD

openCode

Die Vision einer **zertifizierten Verfahrenssicherheit** wird die digitale Souveränität deutlich stärken.

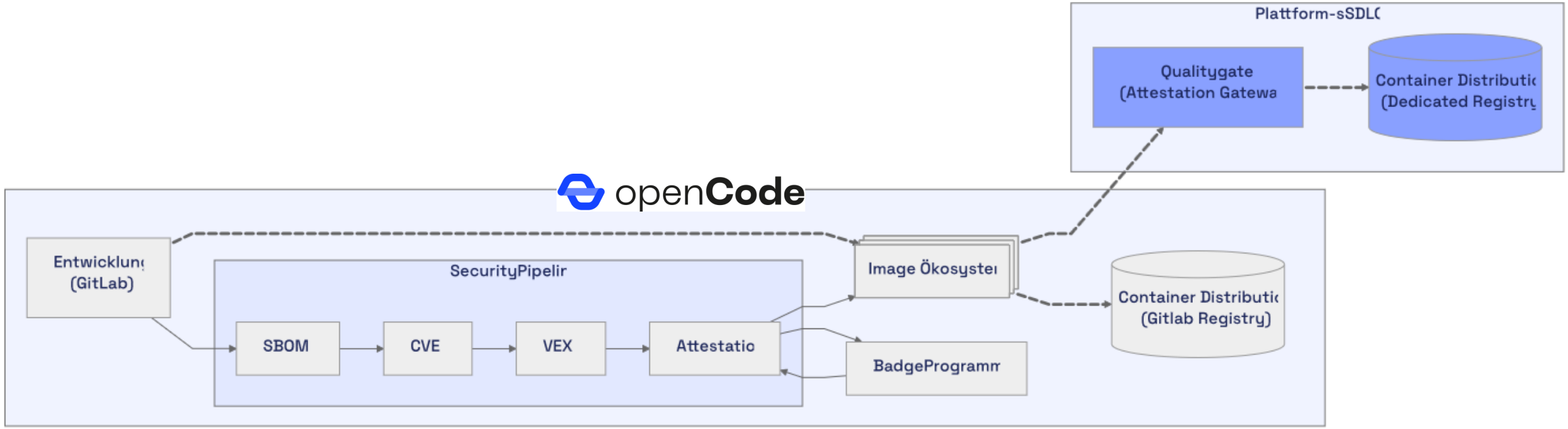
Sie ermöglicht **skalierbare**, **konsistente** und **kontinuierliche Risikobewertungen**, die den dynamischen Anforderungen der modernen Softwareentwicklung gerecht werden und gleichzeitig transparent über die Grenzen automatisierter Prozesse hinaus kommunizieren.

SDLC Mission 2: Image Ökosystem



SDLC Mission 3: sSDLC Distribution

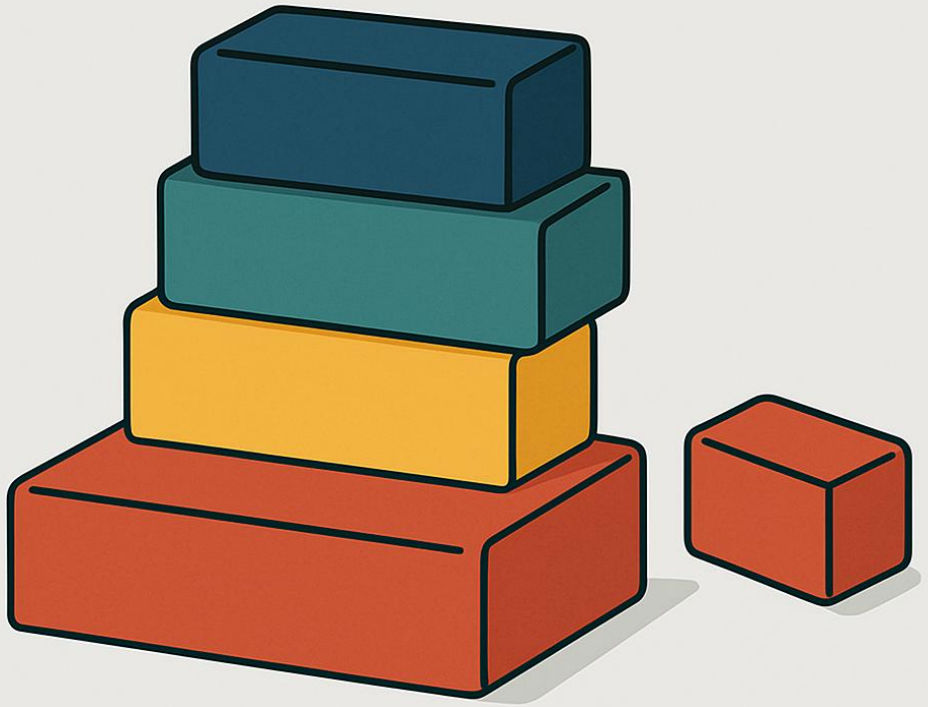
souveräner Quality Gate der ÖV



Souveräne, cloudbasierte Produkte wie openDesk erfordern eine ebenso souveräne Lieferkette – und damit ein langfristiges Investment in die entsprechende Infrastruktur.

Von der Auswahl der Produkte bis zur Definition von Anforderungen: Aufbau des souveränen Gov-Tech-Ökosystems.

www.zendis.de



ZenDiS

Kontakt

Leonhard Kugler
Leitung Plattform und Entwicklung
+49 (0) 151 51237434
leonhard.kugler@zendis.de

Publikation mit dem BSI
https://opencode.de/ssdlc

Zentrum Digitale Souveränität

openCode

openDesk

Ein Produkt des ZenDiS im Auftrag des Bundesministerium des Inneren und für Heimat