Digitale Souveränität und die Sichere Softwarelieferkette mit openCode

Wie openCode und das Badge-Programm Sicherheit, Vertrauen und digitale Souveränität stärken

openCode

Inhaltsübersicht

Warum es uns gibt

Abhängigkeiten und Kostenexplosion

Wie wir wieder Handlungsfähiger werden

Digitale Souveränität

Einfach wechseln

Alternativen bereitstellen

Frei gestalten

Anpassbarkeit sichern

Stark auftreten

Kompetenzen aufbauen

ZenDiS

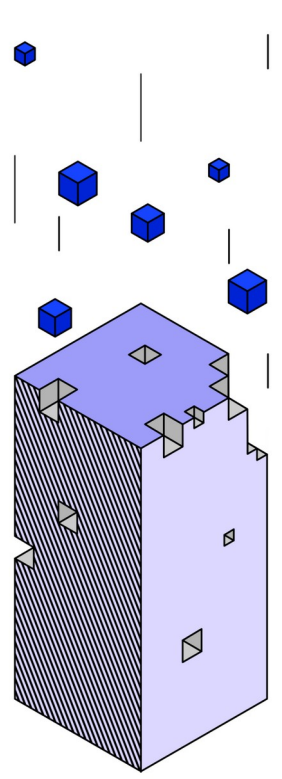
Zentrum Digitale Souveränität

Wir befähigen die öffentliche Verwaltung, sich aus kritischen Abhängigkeiten zu lösen.

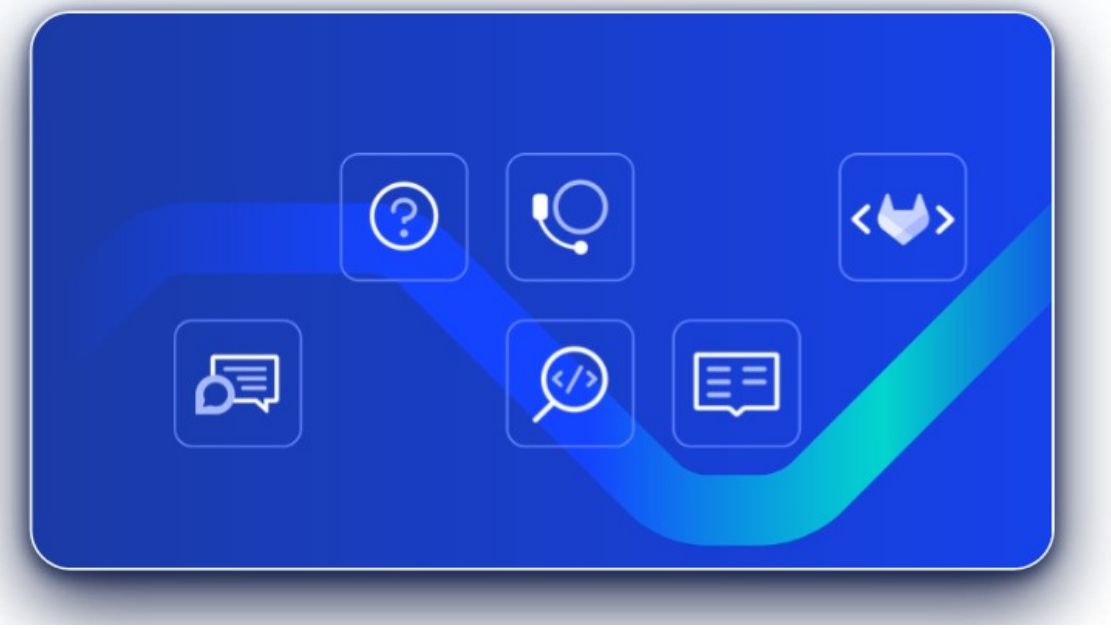
20.05.2026

Problematik/Motivation

- Wachsende Komplexität moderner Softwarelieferketten
- Skalierungsproblem (Geld, Fachkräfte) der öffentlichen Verwaltung
  - i.d.R.: Zeit- und ressourcenintensiven Einzelfallprüfungen nach lokalen Kriterien **steigt stets**
- **Einheitliche Standards in der ÖV (OCI, Deutschlandstack, DVC)**

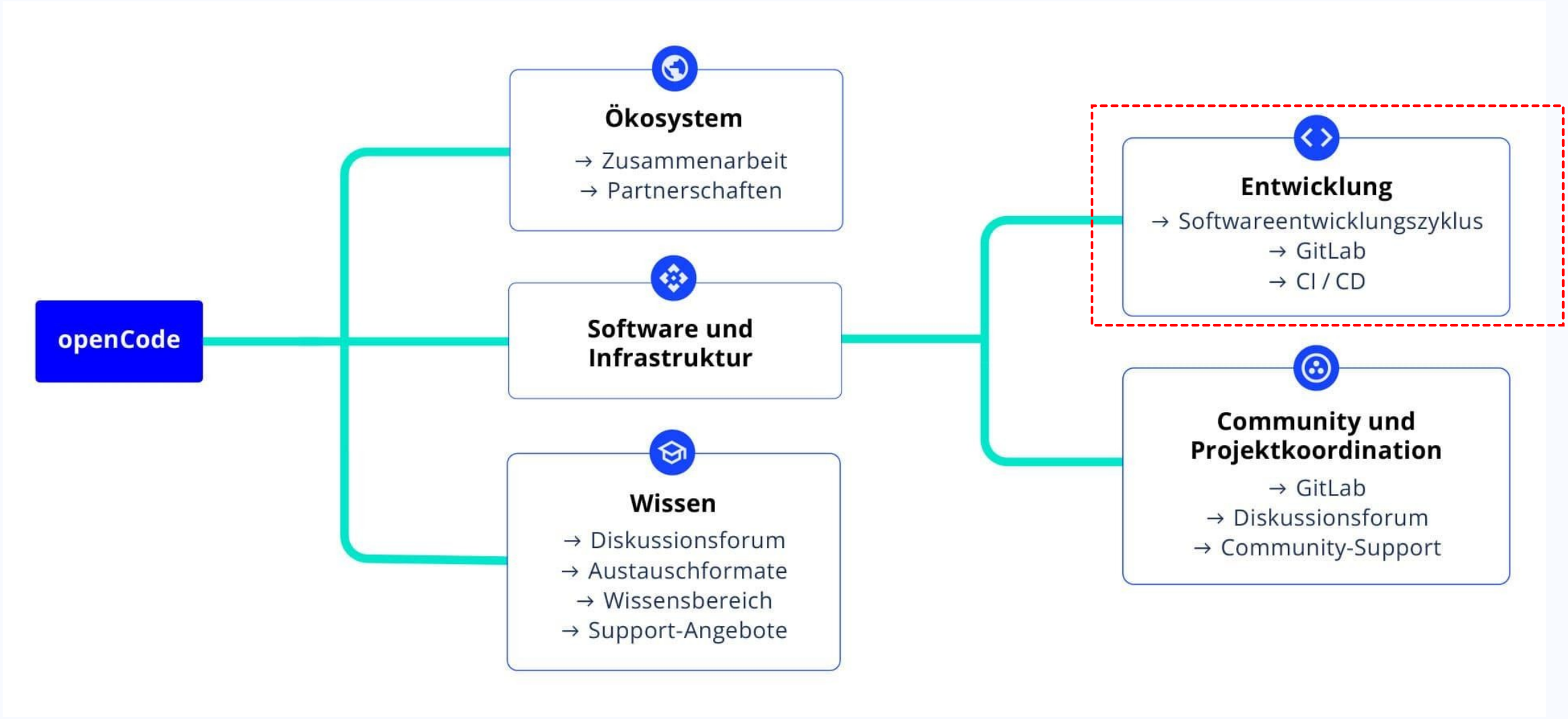


Unsere Missionen

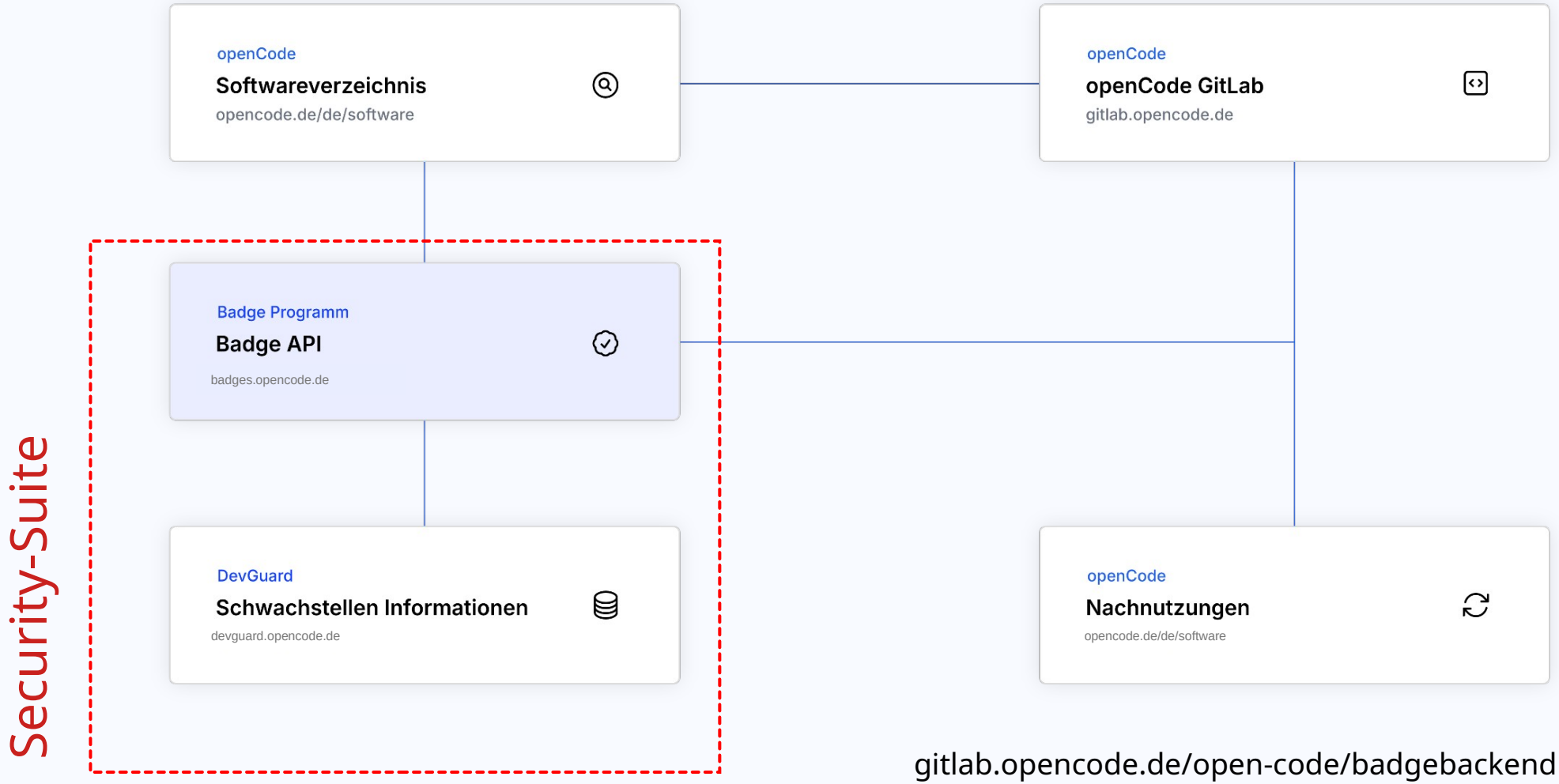


1. 2025: Security Compliance-as-Code
2. 2026: Image-Ökosystem
3. 2027: SSDLC

openCode als Enabler für Digitale Souveränität

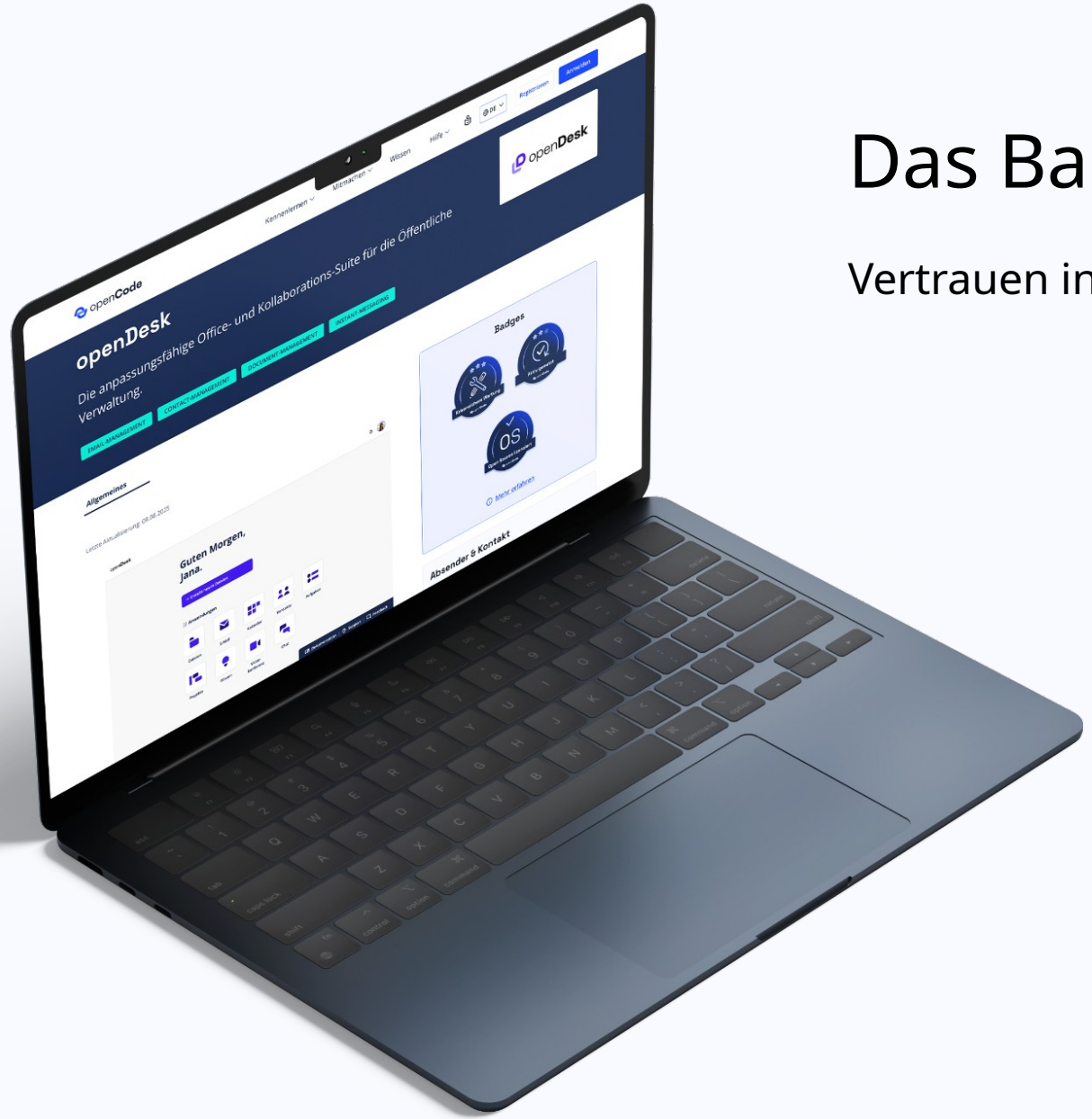


Architektur-Übersicht



gitlab.opencode.de/open-code/badgebackend

openCode



Das Badge Programm

Vertrauen in Open-Source-Software stärken

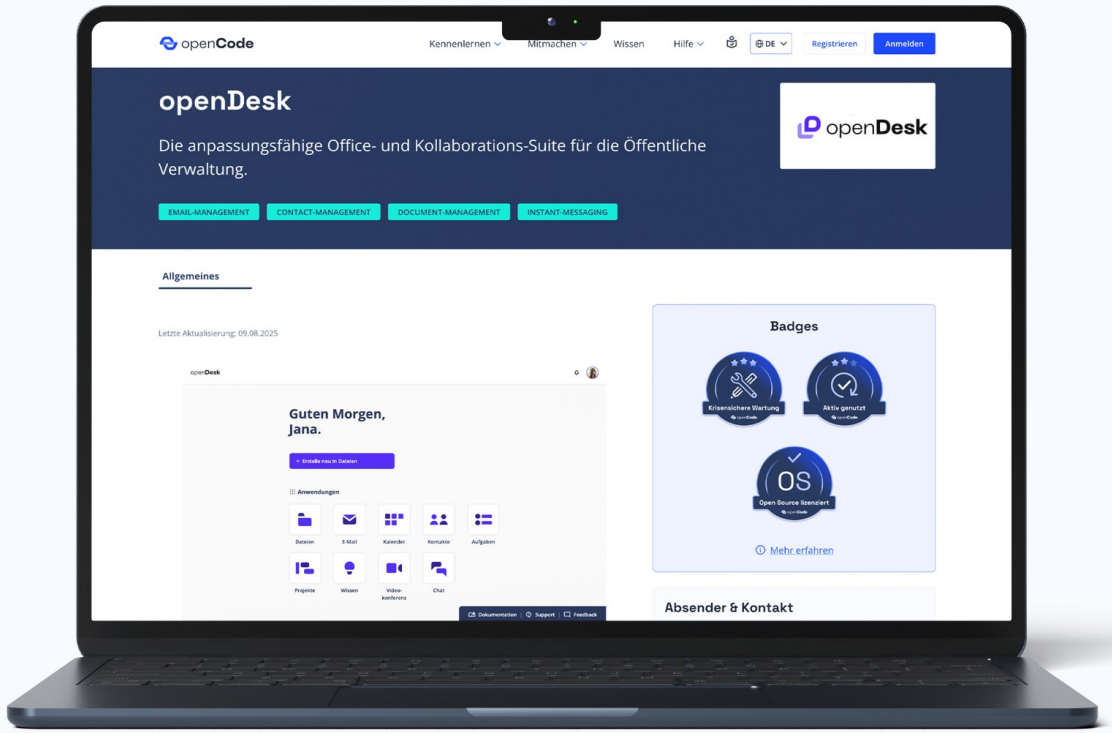
openCode

Das Badge-Programm in der Praxis

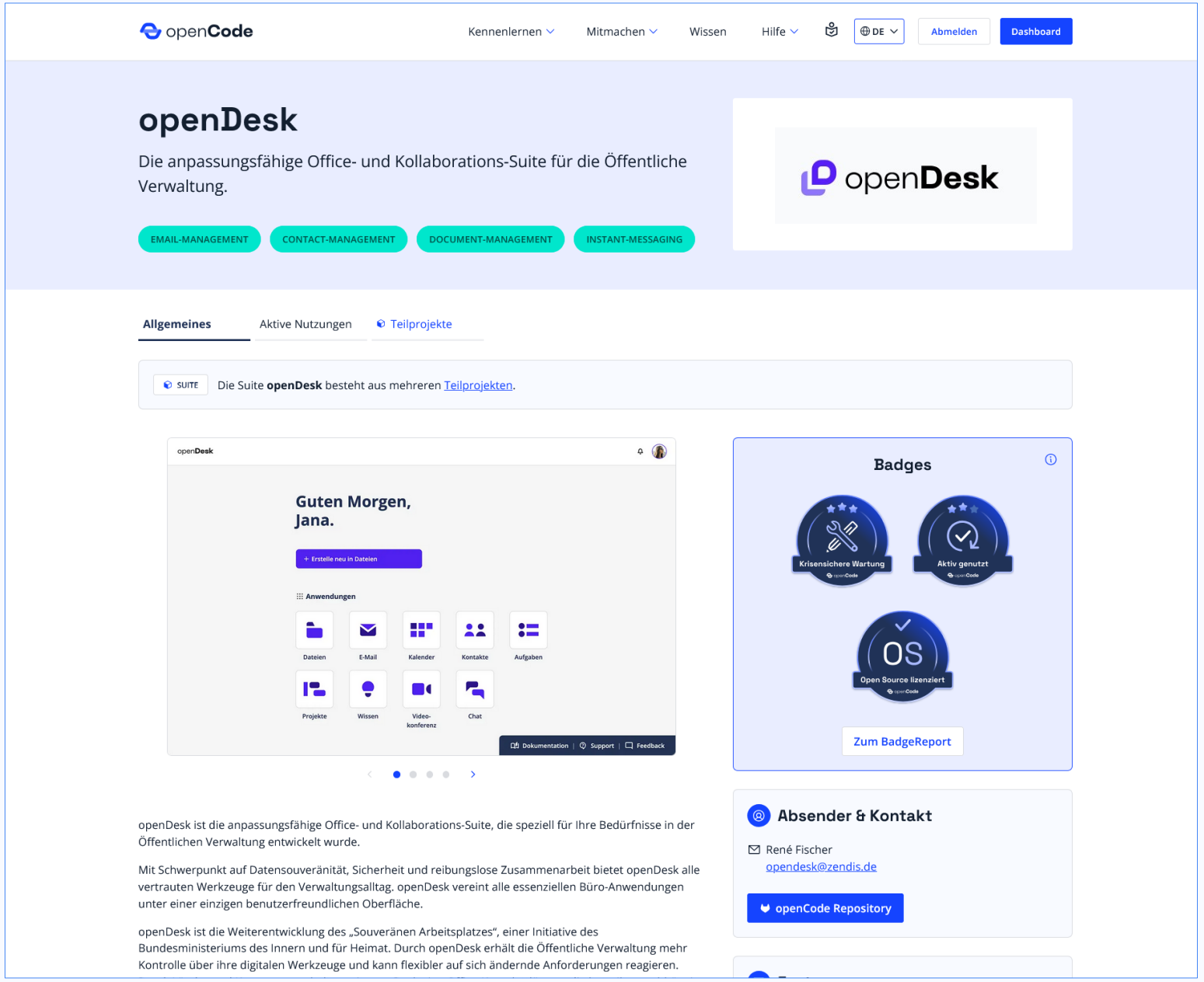
- Automatisierte Prüfung von Software-Repositories nach definierten Kriterien (**Zielgruppe: Beschaffer**)
- Detaillierte Erklärungen zu jeder Bewertung (**Zielgruppe: Maintainer, Developer**)
- Transparente Visualisierung der Ergebnisse durch Badges (**Zielgruppe: Maintainer, Developer, Beschaffer**)
- **Seit April 2026 --> Lieferkettenbadge**

Lieferketten Badge

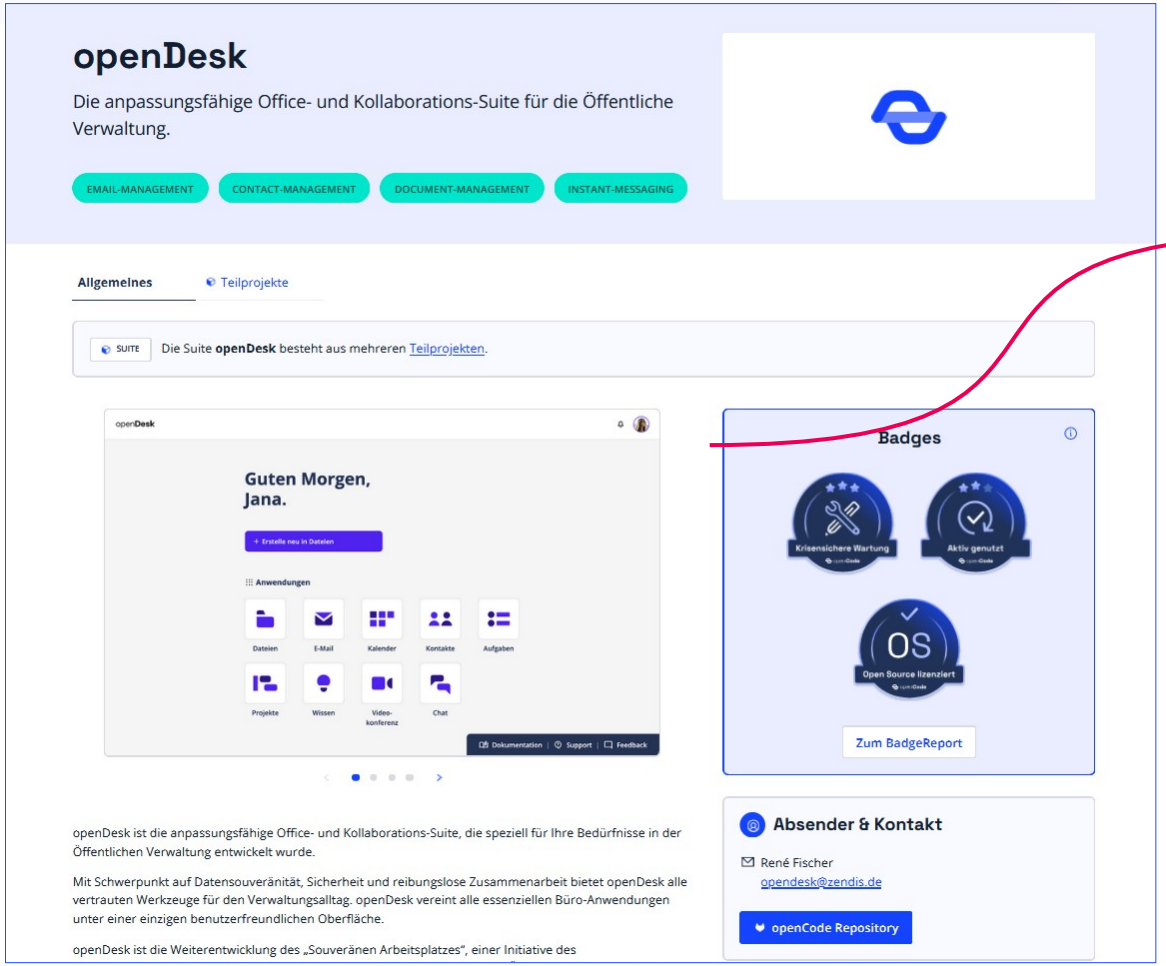
Der Weg zur Badge: Softwareverzeichnis



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


openCode
Kennenlernen
Mitmachen
Wissen
Hilfe
DE
Abmelden
Dashboard
openDesk
Die anpassungsfähige Office- und Kollaborations-Suite für die Öffentliche Verwaltung.
EMAIL-MANAGEMENT
CONTACT-MANAGEMENT
DOCUMENT-MANAGEMENT
INSTANT-MESSAGING
openDesk
Allgemeines
Aktive Nutzungen
Teilprojekte
SUITE
Die Suite openDesk besteht aus mehreren Teilprojekten.
Guten Morgen, Jana.
+ Erstelle neu in Dateien
Anwendungen
Dateien
E-Mail
Kalender
Kontakte
Aufgaben
Projekte
Wissen
Video-konferenz
Chat
Dokumentation
Support
Feedback
Badges
Krisensichere Wartung
Aktiv genutzt
OS
Open Source lizenziert
Zum BadgeReport
Absender & Kontakt
René Fischer
opendesk@zendis.de
openCode Repository
openDesk ist die anpassungsfähige Office- und Kollaborations-Suite, die speziell für Ihre Bedürfnisse in der Öffentlichen Verwaltung entwickelt wurde.
Mit Schwerpunkt auf Datensouveränität, Sicherheit und reibungslose Zusammenarbeit bietet openDesk alle vertrauten Werkzeuge für den Verwaltungsalltag. openDesk vereint alle essenziellen Büro-Anwendungen unter einer einzigen benutzerfreundlichen Oberfläche.
openDesk ist die Weiterentwicklung des „Souveränen Arbeitsplatzes“, einer Initiative des Bundesministeriums des Innern und für Heimat. Durch openDesk erhält die Öffentliche Verwaltung mehr Kontrolle über ihre digitalen Werkzeuge und kann flexibler auf sich ändernde Anforderungen reagieren.

BadgeReport



Aktive Wartung Verliehen

Mehr informationen

Überprüfung	Status	Beschreibung	Nachweis
COMMITS	Bestanden	Mindestens 5 Commits innerhalb der letzten 6 Monate	In den letzten 6 Monaten wurden 264 Commit(s) erstellt.
ISSUE_REACTION_TI...	Bestanden	Reaktionszeit bei Issues in den letzten drei Monaten liegt unter 7 Tagen	Es wurden 29 Tickets/Issues von nicht-Projektmitgliedern erstellt, aber keines von ihnen hat eine Reaktion von einem Projektmitglied erhalten.

Verlässliche Wartung Verliehen

Mehr informationen

Überprüfung	Status	Beschreibung	Nachweis
COMMITS	Bestanden	Mindestens 5 Commits innerhalb der letzten 6 Monate	In den letzten 6 Monaten wurden 264 Commit(s) erstellt.
ISSUE_REACTION_TI...	Bestanden	Reaktionszeit bei Issues in den letzten drei Monaten liegt unter 7 Tagen	Es wurden 29 Tickets/Issues von nicht-Projektmitgliedern erstellt, aber keines von ihnen hat eine Reaktion von einem Projektmitglied erhalten.
RELEASES	Bestanden	Mindestens 1 Veröffentlichung (Release oder Git-Tag) innerhalb der letzten 6 Monate	In den letzten 6 Monaten wurden 11 Tags/Releases gefunden. (11 Tag(s) von denen 11 als Release veröffentlicht worden sind).

Krisensichere Wartung Verliehen

Mehr informationen

Badge für Lieferkette

Stufe 1: Transparente Software-Komponenten

- Changelog vorhanden: Prüft, ob eine Changelog-Datei im Stammverzeichnis existiert für Transparenz über Projektänderungen und Versionsnachverfolgung
- Contribution Guidelines vorhanden: Prüft, ob eine Contribution Guideline-Datei existiert für klare Beitragsrichtlinien und transparente Entwicklungsprozesse
- Container Attestation Bronze: Prüft, ob Container-Images eine SBOM-Attestierung besitzen für vollständige Transparenz über enthaltene Komponenten

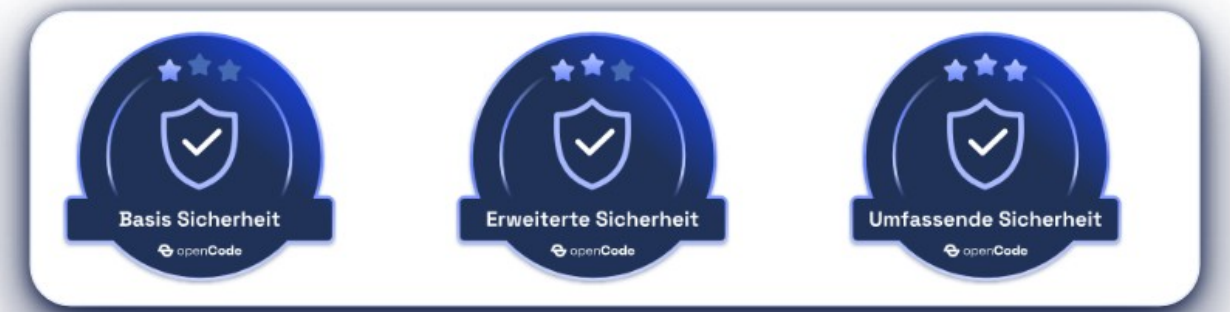
Stufe 2: Transparenter Software-Build-Prozess

- Alle Kriterien aus Level 1
- Container Attestation Silver: Prüft, ob Container-Images eine VEX-Attestierung besitzen für Bewertung der Ausnutzbarkeit bekannter Schwachstellen

Stufe 3: Transparente Software-Lieferkette

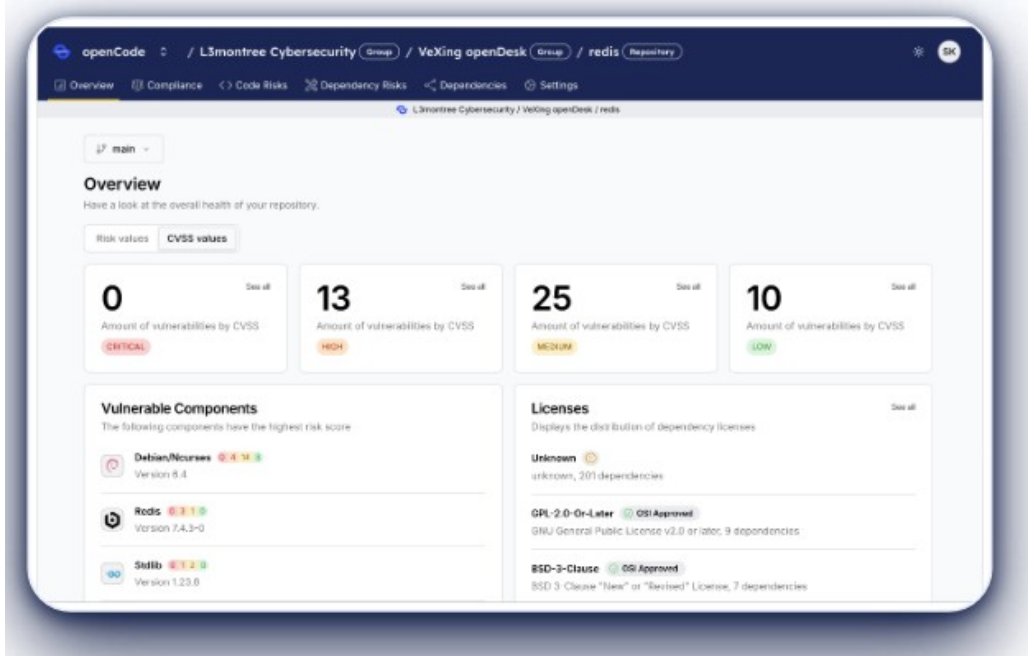
- Alle Kriterien der Levels 1 und 2
- Container Attestation Gold: Prüft, ob Container-Images Build/Source Provenance und SARIF-Attestierungen besitzen für vollständige Nachvollziehbarkeit der Lieferkette

Sicherheit



1. Level 1: Basis Sicherheit
2. Level 2: Erweiterte Sicherheit
3. Level 3: Umfassende Sicherheit

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



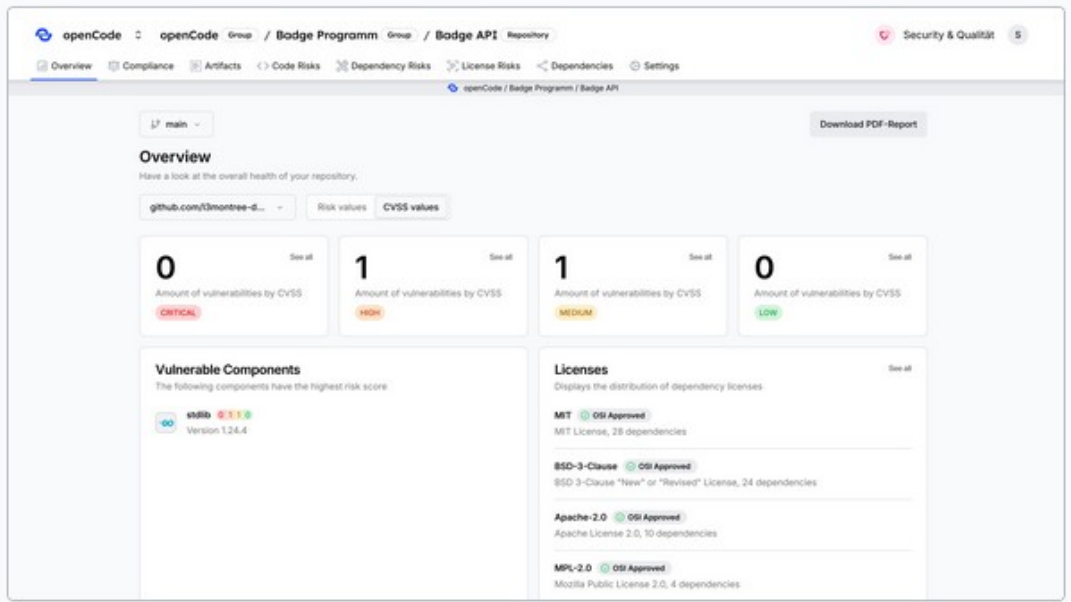
Badge für Sicherheit

Stufe 1: Basis Sicherheit

- Reaktionszeit auf Issues: Die durchschnittliche Reaktionszeit auf Issues der letzten 3 Monate beträgt weniger als 7 Tage
- Geschützte Branches: Der Haupt-Branch (main) ist so konfiguriert, dass er geschützt (protected) ist und es sind keine Force-Pushes auf den default Branch erlaubt.
- Sicherheitsrichtlinie: Prüft, ob eine Datei **SECURITY.md** im Stammverzeichnis des Default-Branches existiert.

Stufe 2: Erweiterte Sicherheit

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



https://devguard.opencode.de/

DEVGUARD
BY L3MONTREE

Sicherheit im Entwicklungsalltag verankern

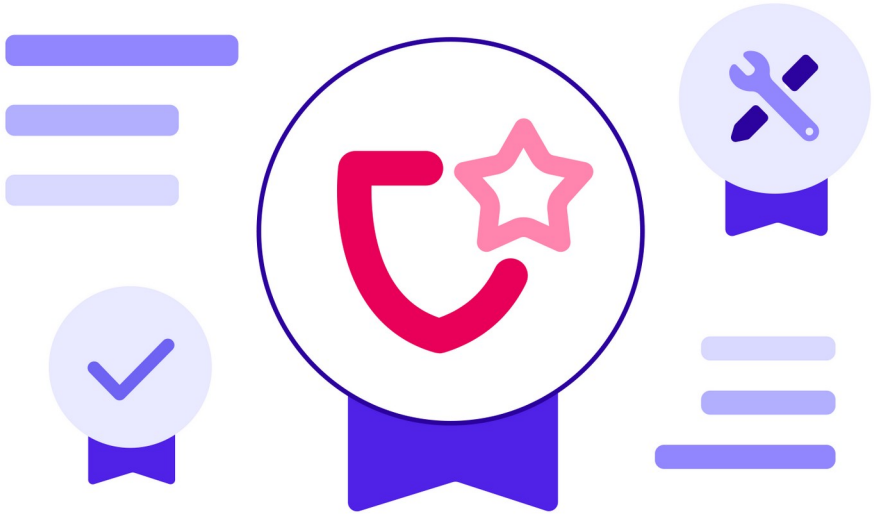
DevGuard macht Software-Sicherheit in der öffentlichen Verwaltung einfacher und alltagstauglich. Entwickler:innen können Sicherheitsmaßnahmen ohne Spezialwissen nutzen, als selbstverständlichen Teil ihres Workflows. Dafür verbessert DevGuard die Nutzbarkeit bestehender Sicherheitstools und senkt so die Einstiegshürden. Sicherheit wird damit zum selbstverständlichen Teil der Softwareentwicklung und Angriffe auf die Lieferkette werden deutlich erschwert.

Zu openCode DevGuard

Security & Qualität

Vertrauen in Open-Source-Software stärken

- **Einfach Softwarequalität prüfen**
- **Einfach Software-Komponenten nachweisen**
- **Sicherheit im Entwicklungsalltag verankern**



Mission 2: Gehärtete Container-Images

20.05.2026

Mission 2:
Gehärtete Container-Images für die ÖV

Aufbau eines Netzwerks zur Entwicklung eines containerbasierten, geprüften und standardisierten Softwarelieferketten-Ökosystems

Veröffentlichung von **gehärteten Container-Images** zur Nachnutzung

Deutliche Reduktion von Sicherheitsrisiken durch aktive Bewertung von Schwachstellen

Konsistent aufgebaute und dokumentierte Container-Images schaffen Klarheit für Entwicklung, Betrieb und Sicherheitsprüfung (z. B. CycloneDX und VEX als OCI-Attestierung).

Container sind isolierte Prozesse und bündeln Anwendungscode sowie alle Abhängigkeiten, damit die Software in unterschiedlichen Umgebungen gleich läuft.

Container-Images sind Archive, die alle notwendigen Bibliotheken, Dateien und Abhängigkeiten enthalten, um den Container zu erstellen und auszuführen.

Container-Härtung reduziert Schwachstellen, indem man beispielsweise mehrstufige Sicherheitskontrollen hinzufügt, Transparenz- und Wartungsanforderungen erhöht oder unnötige Komponenten entfernt.

https://container.gov.de/

Plattform als Teil einer souveränen und sichereren Softwareinfrastruktur

openCode als Baustein einer souveränen Softwarelieferkette

https://opencode.de/de/ssdlc

Bundesamt
für Sicherheit in der
Informationstechnik

ZenDiS