#1 KI-NATIVE AGENTISCHE GRC-PLATTFORM

2026

VamiGRC

Die *KI-native, agentische* GRC-Plattform *für das regulierte Europa*.

Integriertes Managementsystem · OSCAL-konforme Controls · ein abfragbarer Graph — und ein Dialog, der die Arbeit erledigt. Bereitgestellt als SaaS-Plattform, gehostet in der Open Telekom Cloud, made in Germany.

80–95%
Reduktion der manuellen Compliance-Arbeit

Echtzeit
Time-to-Report vs. 2–5 Tage manuell

Powered by

VamiSec

THE AI-driven IT Security and GRC Experts

TRUSTED · HOLISTIC · ENGINEERED

Open Telekom Cloud · T-Systems

Mitglied im bitkom

VamiGRC

Ein System. Alle Domänen. Ein intelligenter GRC-Ansatz.

VamiGRC verbindet integrierte Managementsysteme, agentische Automatisierung und graphbasierte Risiko-Intelligenz in einer AI-native Plattform.

AI-native · Graph-native · Audit-ready · Role-based Lenses

01 · INTEGRIERTES IMS

Ein IMS. Fünf Domänen.

Ein Datenmodell für integrierte Steuerung über mehrere Managementsysteme und Frameworks.

- ISMS · ISO 27001 · NIS2 · TISAX
- AIMS · EU AI Act · ISO 42001
- PIMS · DSGVO · ISO 27701
- CSMS · IEC 62443 · CRA
- BCMS · ISO 22301 · DORA

Einmal modellieren · mehrfach steuern · audit-ready by design

02 · AGENTIC AUTOMATION

Workflows auf Autopilot.

VamiAI unterstützt und automatisiert komplexe GRC-Prozesse – kontrolliert, nachvollziehbar und effizient.

- **Supplier Intelligence**
  OSINT, Ratings, AVV, Fragebögen
- **Risikoanalyse**
  von Kontext zu Register und Maßnahmenplan
- **Multi-Framework Audit**
  domänenübergreifend, weniger Redundanz
- **Trust Center**
  Inhalte mehrsprachig und konsistent bereitstellen

Ein Prompt · ein Workflow · der Mensch behält die Kontrolle

03 · GRC GRAPH

Zusammenhänge sichtbar machen.

Der GRC Graph verknüpft Risiken, Controls, Assets, Lieferanten, KI-Use-Cases und Evidenzen über Silos hinweg.

- Kronjuwelen, Prozesse und Datenflüsse in einem Modell
- Toxische Kombinationen und versteckte Abhängigkeiten sichtbar
- Findings mit Quellen und Evidenzen zurückverfolgbar
- Cross-domain KPIs, Heatmaps und Geo-Posture in einem Kontext

Silos auflösen · Zusammenhänge verstehen · fundierter entscheiden

Ausschnitte aus VamiGRC

Lenses & Domänen

VamiAI Copilot

Geo Posture & Graph View

Für CISO, DPO, AI Officer, Risk & Compliance Leads – modular, prüfungsorientiert und skalierbar.

VamiGRC macht GRC operativ, intelligent und integrierbar.

VamiSec – Ihr Partner für IT-Sicherheit & Compliance

Relevante Expertise

- IT-Sicherheit und Compliance
- ISO 27001, CRA, NIS2, DORA, BSIG & KRITIS, BSI IT-Grundschutz, TISAX
- IEC 62443 & SAE 21434 & OWASP SAMM
- Sichere Softwareentwicklung, DevSecOps, sichere CI/CD-Pipelines
- Application Security, Threat Modeling, OWASP & CWE
- Produkt- und technologieunabhängige Expertise

Zertifizierte Berater

- ISO 27001 Lead Auditor
- ISO 42001 Lead Auditor
- BSIG §8a zusätzliche Prüfverfahrenskompetenz
- KI-Beauftragter (EU AI Act)
- BSI IT-Grundschutz-Praktiker
- Datenschutzbeauftragter (IHK)
- NIS2- und CRA-Berater

Inhabergeführt

Hersteller-, Produkt- und technologieunabhängig

Regulierte Industrien

- Verteidigung & Luft- und Raumfahrt
- Banken & Versicherungen
- Kritische Infrastruktur: Pharma, Krankenhäuser & Versorger
- **Automobil & Transport**
- Industrie & Fertigung
- Softwarehersteller
- Fintech- & Krypto-Unternehmen
- Handel & Immobilien
- Öffentlicher Sektor
- National & international

Unsere weitere Expertise

IT-Sicherheit

- Application Security & SDL & OWASP SAMM
- Penetration Testing & Red Teaming
- IT-Security-Audits & Threat Modeling
- M&A-Cybersecurity-Due-Diligence
- Vulnerability Management & Bug-Bounty-Programme
- Threat Detection: Logging & Monitoring
- Deception-Technologien / Honeypots
- Cloud Security
- Incident Response & Cyber-Resilience-Krisenübungen

GRC

- Compliance as a Service
- ISMS + CSMS + KIMS + DSMS = IMS
- vCISO & vISB & vKI-Beauftragter
- IT-Notfallmanagement & Business Continuity
- Lieferantenmanagement
- Audits & Zertifizierung
- KI-Compliance & EU-AI-Act-Compliance
- KI-Beauftragter
- ISMS AI-MS KI-Assistent
- ISO 27001, CRA, NIS2, DORA, BSIG & KRITIS, BSI IT-Grundschutz, TISAX
- IEC 62443 & SAE 21434

Managed Services

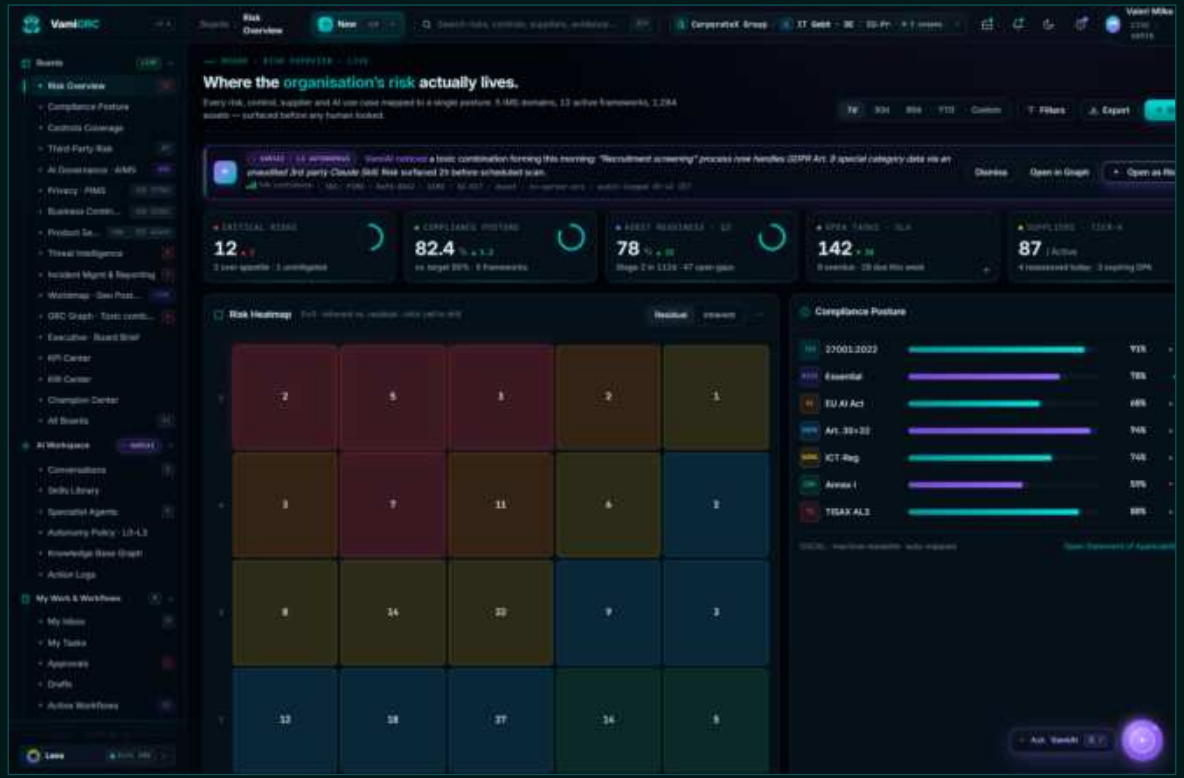
- **GRC Managed Services:**
  - ISMS as a Service
  - KI-Compliance & AI Officer as a Service
  - Compliance as a Service
  - vCISO- & vISB-Services
  - Lieferantenrisikomanagement
- **IT-Security Managed Services:**
  - MDR & SOC
  - Vulnerability Management & Bug-Bounty-Programme
  - Cloud Security Monitoring (CNAPP & CSPM)
  - Deception-Technologien / Honeypots
  - Incident Response & Cyber Resilience

Zertifizierungen

- Training CISO & ISO
- ISO-27001-Zertifizierung für Mitarbeitende
- Awareness-Schulungen
- Zielgruppenspezifische Schulungen
- Schulungen für Administratoren
- Schulungen für Softwareentwickler und -architekten

Risikoübersicht — Ihr tägliches Command Center.

Heatmap, KPIs und Live-Framework-Status auf einen Blick — was Ihr CISO am Montag um 8:00 Uhr sieht.



GRC ist heute ein Engpass.

Dutzende Bildschirme. Eine Frage. Tagelange Verzögerung. Compliance sollte nicht von Heldentaten abhängen.

01

Regulatorische Überlast

CRA · AI Act · NIS2 · DORA · MDR · IEC 62443 — jeweils mit eigenen Nachweisen, Fristen und Audit-Logik.

02

Operative Überlast

Manuelle Risikoanalysen, Fragebögen und Gap-Analysen verbrauchen 60–80 % der Compliance-Kapazität. Teams kämpfen gegen Rückstände, nicht gegen Risiken.

03

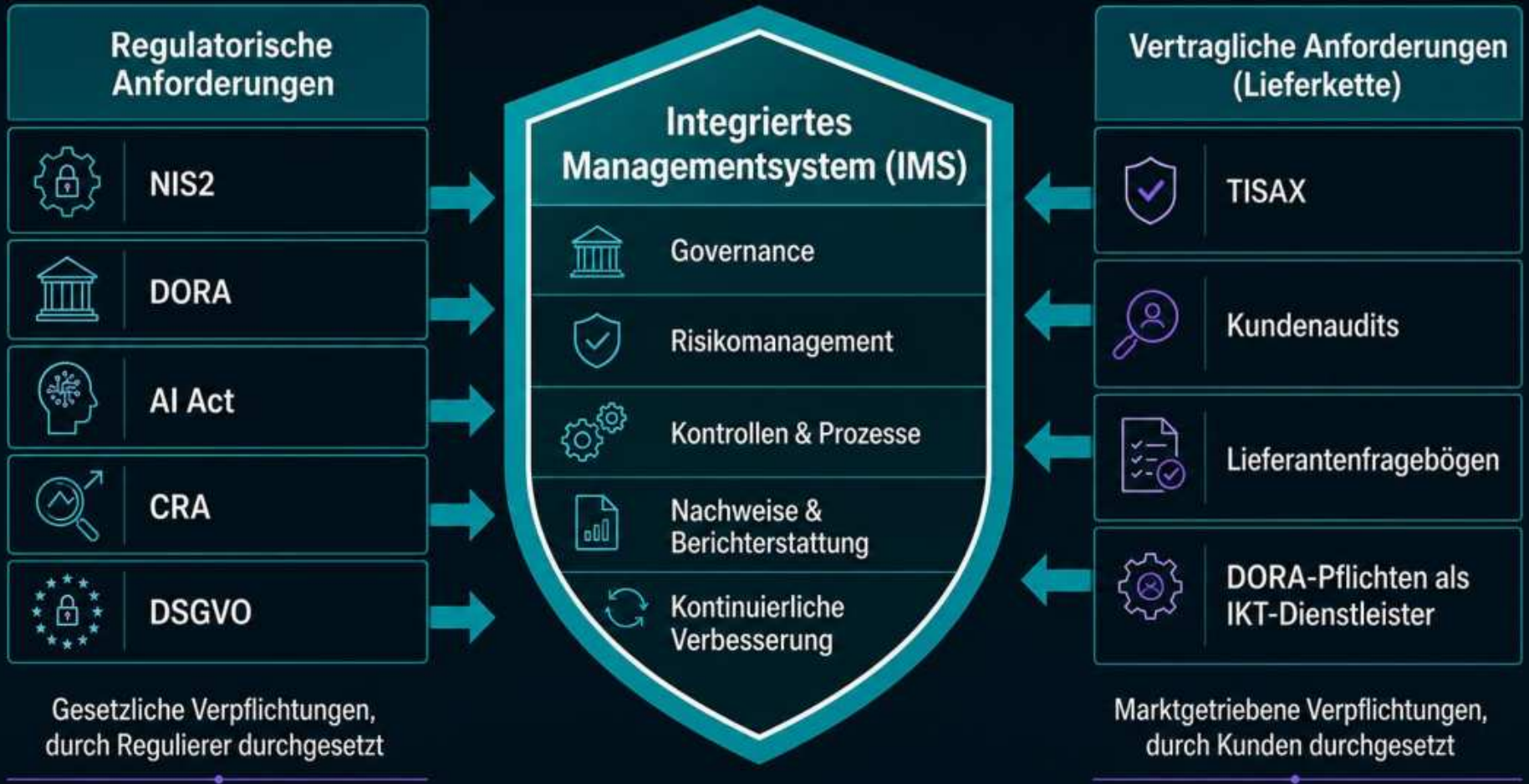
Voneinander getrennte Tool-Silos

ISMS, AIMS, PIMS, BCMS, CSMS — jedes in seinem eigenen Tool, mit eigenem Datenmodell. Redundante Nachweise. Kein einheitliches Bild.

04

Statische Chatbots

Beantworten FAQs, können Ihre Daten nicht abfragen, nicht handeln, nicht schlussfolgern. Tage bis zur Antwort an Auditoren. Wochen bis zum Schließen von Lücken.


Regulatorische Anforderungen
NIS2
DORA
AI Act
CRA
DSGVO
Gesetzliche Verpflichtungen, durch Regulierer durchgesetzt
Integriertes Managementsystem (IMS)
Governance
Risikomanagement
Kontrollen & Prozesse
Nachweise & Berichterstattung
Kontinuierliche Verbesserung
Vertragliche Anforderungen (Lieferkette)
TISAX
Kundenaudits
Lieferantenfragebögen
DORA-Pflichten als IKT-Dienstleister
Marktgetriebene Verpflichtungen, durch Kunden durchgesetzt

EU-Regulatorik für IT-Sicherheit & Compliance

DORA
Digital Operational Resilience Act

NIS2
Network and Information Security 2

AI Act
Artificial Intelligence Act

CRA
Cyber Resilience Act

DSGVO
Datenschutz-Grundverordnung

01

IMS-Fundament

Prozesse · Assets · Organisation · Identitäten · Projekte

Fünf IMS-Domänen. Eine Wissensbasis.

VamiAI versteht die gesamte regulatorische und Control-Landschaft — und wie alles zusammenhängt.

ISMS

Informationssicherheit

ISO 27001 · NIS2 · SOC 2

AIMS

KI-Management

ISO 42001 · EU AI Act

CSMS

Produkt- & OT-Sicherheit

IEC 62443 · CRA

PIMS

Datenschutzmanagement

DSGVO · ISO 27701

BCMS

Business Continuity

ISO 22301 · DORA

Einmal fragen. Antworten über alle Domänen erhalten — mit automatisch sichtbar gemachten domänenübergreifenden Beziehungen.

Mit Vami IMS Framework zur integrierten Steuerung regulatorischer und vertraglicher Anforderungen

Fragmentierte Compliance

Parallele Projekte
Redundante Prozesse und Audits
heterogene Managementsysteme

Vami IMS Framework

Regulierung & Anforderungen → Managementsystem → Standard

Zertifizierbare Compliance

- ISO 27001
- ISO 42001
- IEC 62443
- SAE 21434
- ISO 27701
- BSI IT-Grundschutz
- TISAX

Integrierte Steuerung für nachhaltige Compliance

- Compliance und Nachweisfähigkeit als Vertrauensanker
- Zentrale Risikosicht für das Management
- Mit zertifizierbaren Kombi-Audits zum Wettbewerbsvorteil
- Keine Redundanz & Silos
- Skallerbar für neue Regulierungen
- Nachhaltige Compliance statt Projekt-Compliance

Regulierungen und Anforderungen ändern sich – Vami IMS bleibt.

VamiSec

Prozess-Layer — der Geschäftsprozess ist das Fundament.

DSGVO-relevant? → +PIMS-VVT-Layer. KI-gestützt? → +AIMS-Use-Case-Layer. Alles auf demselben Datensatz.

+ AIMS-LAYER

KI-Use-Case

wenn KI beteiligt · EU AI Act · ISO 42001

+ PIMS-LAYER

Verarbeitungstätigkeit (VVT)

wenn personenbezogene Daten · DSGVO Art. 30 · AVV · DSFA

BASIS · IMMER VORHANDEN

Geschäftsprozess

ISMS · BCMS · CSMS · Hierarchie · RACI · CIA · KPIs · Flowchart

IMS-MODUL-INTEGRATIONEN · BIDIREKTIONAL

Asset-Management
Prozess ↔ Asset · CIA-Kaskade

Controls
→ OSCAL · Lücke = Finding

Risikoregister
CIA → Eintrittswahrscheinlichkeit + Maßnahmen

Lieferanten
PIMS = Art.-28-AVVs

Dokumente
SOPs · Richtlinien · Review

Incidents
Betroffener Prozess · Eskalation

Domains (AIMS)
KI-Erkennung → Prozess automatisch anlegen

Personen · RACI
Owner / Vertretung / Reviewer

Informationswerte
Schutz-Kaskade · VVT

Geschäftseinheiten
BU-Filter · Prozesslandkarte

Einmal erfasst – überall genutzt. Keine Duplikation. Keine Fremdschlüssel-Komplexität.

Drei Rollen. Drei Tools. Drei Widersprüche.

Heute arbeiten CISO, Datenschutzbeauftragter und KI-Beauftragter parallel – aber nicht wirklich zusammen.
Mit VamiGRC: ein Datensatz, alle Sichten.

HEUTE · ISOLIERTE ROLLEN

CISO, DSB und KI-Beauftragter arbeiten parallel – nicht zusammen.

CISO

- Managementsystem: **ISMS**
- Standards & Regulatorik: **ISO 27001 · NIS2**
- Eigenes Tool · eigenes Register

DSB

- Managementsystem: **PIMS**
- Standards & Regulatorik: **DSGVO · VVT**
- Eigenes Tool · eigenes Register

KI-BEAUFTRAGTER

- Managementsystem: **AIMS**
- Standards & Regulatorik: **EU AI Act · ISO 42001**
- Eigenes Tool · eigenes Register

- Derselbe Geschäftsprozess wird dreimal beschrieben – in drei Formaten.
- Befunde widersprechen sich registerübergreifend.
- Abstimmung kostet Zeit – Audit-Woche, Meetings, Reibung.
- GRC bleibt oft papiertigerartig – statt echte Risikoreduktion zu liefern.

MIT VAMIGRC · INTEGRIERTES IMS

Ein IMS. Drei Rollen. Eine Single Source of Truth.

CISO · ISMS

DSB · PIMS

KI-BEAUFTRAGTER · AIMS

VamiIMS

VamiIMS · ein Datensatz, alle Sichten

- Ein Geschäftsprozess – gelesen als VVT, AI Use Case und Asset.
- Einmal umsetzen – NIS2, DORA, DSGVO und AI Act gleichzeitig adressieren.
- Keine Widersprüche. Keine Doppelarbeit. Ein gemeinsamer Graph.
- GRC wird operativ wirksam – und reduziert Risiken tatsächlich.

Von GRC als Excel als Datenbank mit UI zur agentischen GRC-Plattform.

Während andere GRC-Tools Formulare verwalten, führt VamiGRC Workflows aus. Jeder Compliance-Prozess wird zu einem intelligenten Agenten.

Traditionelle GRC

- ✗ Manuelle Prozesse und Pflege des ISMS
- ✗ Silo-Tools für ISMS, PIMS, AIMS
- ✗ Reaktiv
- ✗ Questionnaies und Gap-Analysen dauern Stunden bis Tage
- ✗ Mensch führt aus
- ✗ Formulare, Checklisten, Bildschirme

VamiAI Agentische GRC

- ✓ Autonome Agenten
- ✓ Vereinheitlichte IMS-Plattform
- ✓ Proaktiv & kontinuierlich
- ✓ Questionnaires und Reportings dauern Sekunden bis Minuten
- ✓ KI führt aus — Mensch genehmigt
- ✓ Dialog, Zitat, Aktion

Ein Prompt. Kompletter Workflow. Risikoregister · Mitigationsplan · Audit-Bericht.

Wiz Partner Alliance · gemeinsamer Markteintritt für regulierte Industrien.

Wiz führt Cloud Security auf G2 an. VamiGRC bringt denselben graphbasierten Ansatz in die GRC. Die Partnerschaft vereint beides für regulierte Unternehmen.

WIZ × 

Cloud Security ↔ GRC

VamiGRC

WIZ · CLOUD

Security Graph

Bildet jedes Asset, jede Schwachstelle, jede Identität und jeden Netzwerkpfad ab. Deckt toxische Kombinationen in der Cloud auf.

WIZ × VAMIGRC

Gemeinsame Methodik

Beide ersetzen fragmentierte Befunde durch einen einzigen, abfragbaren Graphen, der toxische Kombinationen über alle Kronjuwelen hinweg sichtbar macht.

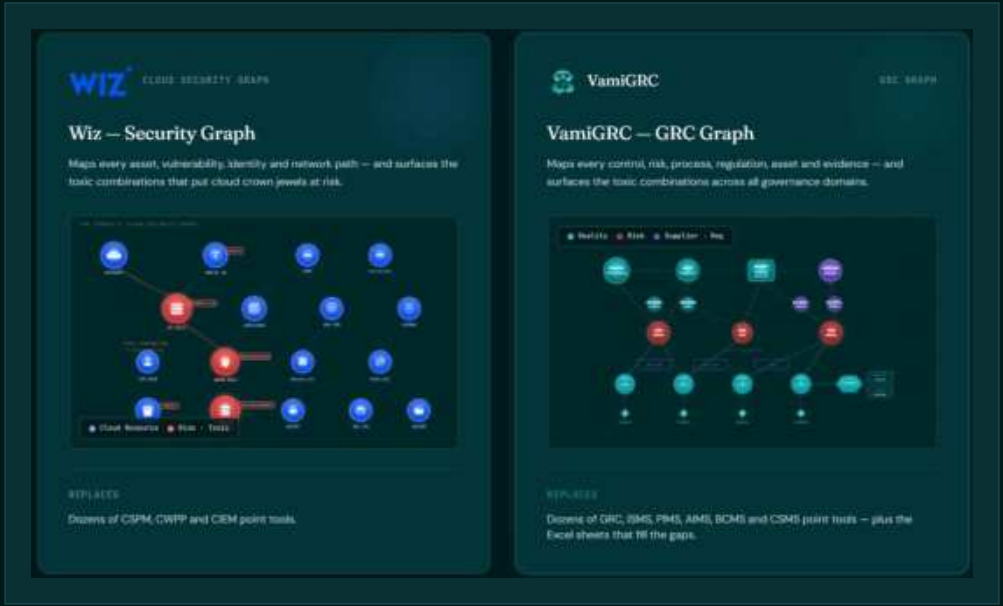
VAMIGRC · GRC

GRC Graph

Bildet jedes Control, Risiko, jeden Prozess, jede Regulierung, jedes Asset und jeden Nachweis ab. Deckt toxische Kombinationen über IMS-Domänen hinweg auf.

Wiz ist für Cloud Security das, was VamiGRC für GRC ist.

Beide ersetzen fragmentierte Befunde, Alarme und Risiken durch einen einzigen, abfragbaren Graphen, der toxische Kombinationen über Ihre Kronjuwelen hinweg sichtbar macht.



WIZ · ERSETZT

Dutzende CSPM- · CWPP- · CIEM-Punktlösungen.

VAMIGRC · ERSETZT

Dutzende GRC-, ISMS-, PIMS-, AIMS-, BCMS-, CSMS-Tools — plus Excel, das die Lücken füllt.

GRC Graph. Wir finden die toxischen Kombinationen über Ihre Kronjuwelen hinweg.

GRC Graph in Aktion.

Jedes Asset, Risiko, jeder Lieferant, jedes Projekt und Control — und die Beziehungen dazwischen. Klicken Sie auf einen Knoten zur Inspektion; auf eine Kante, um zu erklären, warum sie existiert.

WARUM DAS ZÄHLT

- **Toxische Kombinationen sichtbar gemacht**
  Kritische Risiken · überfällige Nachweise · verwaiste Assets — fünf Statusringe, ein Canvas.

- **Fünf Knotentypen vereint**
  Asset · Risiko · Lieferant · Projekt · Control — farblich kodiert über ISMS, AIMS, PIMS, CSMS, BCMS hinweg.

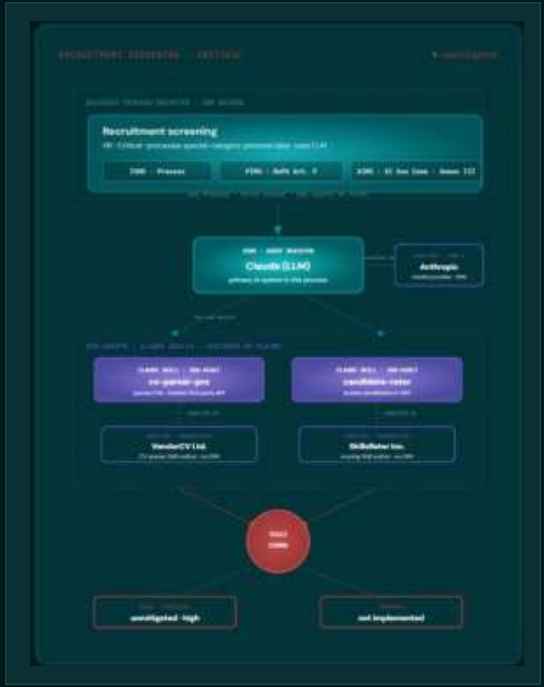
- **Audit-Ready by Design**
  Klick auf einen Knoten zeigt Quellmodul, Owner, letzte Prüfung und verknüpfte Nachweise.

GRC-Graph — Schützen Sie Ihre Kronjuwelen: *1824 Knoten, 4 toxische Kombinationen.*

Domänenübergreifender Blast-Radius automatisch sichtbar gemacht. Der Wiz-for-GRC-Moment.

Bewerber-Screening. Eine toxische Kombination über drei Systeme hinweg.

Ein einzelner Geschäftsprozess — Bewerber-Screening — verkettet stillschweigend DSGVO Art. 9, Hochrisiko-Pflichten des EU AI Act und die gesamte Lieferkette eines KI-Anbieters. Erst die Abfrage des Graphen macht es sichtbar.



EIN PROZESS · EIN DATENSATZ

Bewerber-Screening ist eine Zeile im Geschäftsprozessregister — automatisch gelesen als VVT Art. 9 (PIMS) UND Hochrisiko-AI Use Case nach Anhang III (AIMS).

GESAMTE LIEFERKETTE · ASSET-HIERARCHIE

Claude (LLM) ist im Asset-Register. Anthropic liefert es direkt. Aber seine Skills cv-parser-pro und candidate-rater sind Sub-Assets — geliefert von unabhängigen Marketplace-Anbietern ohne AVV.

DIE TOXISCHE KOMBINATION · KRITISCH

Besondere Kategorien personenbezogener Daten, verarbeitet durch ein LLM über ungeprüfte Drittanbieter-Skills, mit nicht mitigiertem Ursprungsrisiko und nicht implementierten abdeckenden Controls.

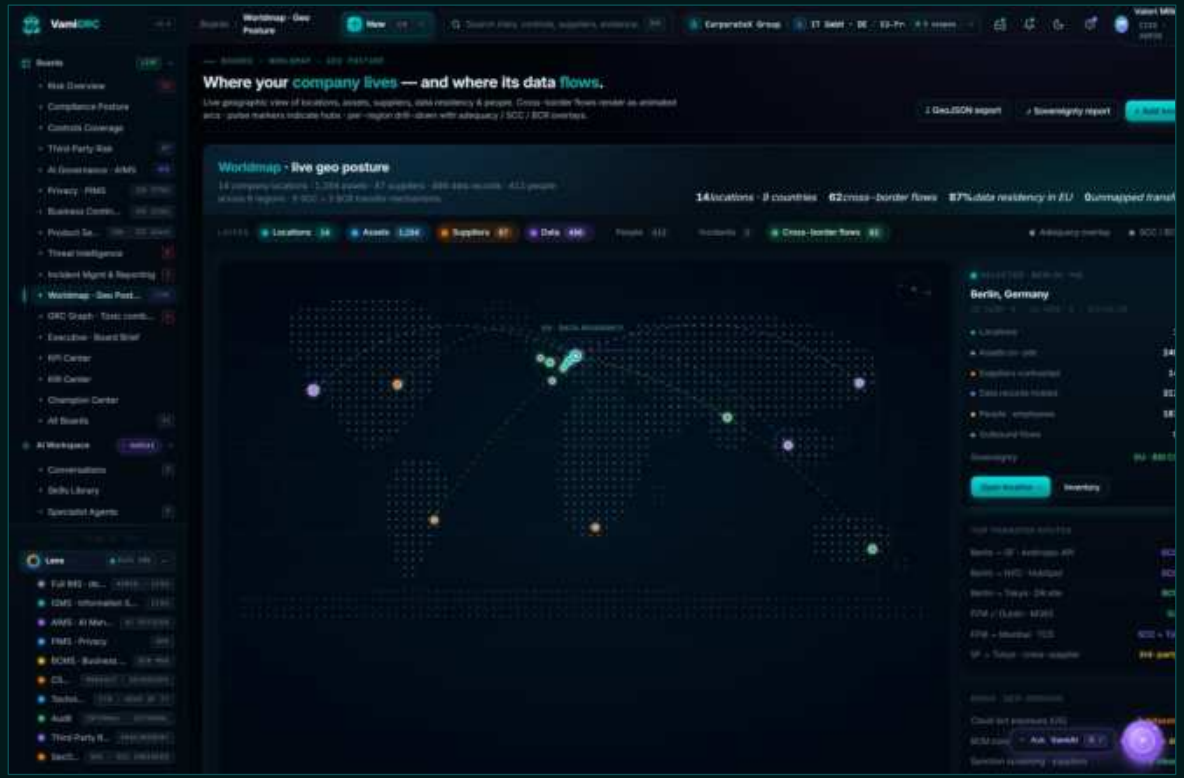
WARUM SIE ES NICHT SEHEN WÜRDEN

Jedes Silo sieht ein Teilstück. Nur der Graph sieht das Ganze. DSGVO Art. 9 · EU AI Act Anhang III · NIS2 Art. 21(2)(d) · CRA · DORA Art. 28.

OSINT-Anreicherung · Breach-Monitoring · Auto-Assessment · Sub-Auftragsverarbeiter-Tracking — sichtbar gemacht, bevor ein Mensch hingesehen hat.

Weltkarte — Live-Geo-Status.

14 Standorte · 9 Länder · 62 grenzüberschreitende Datenflüsse. Adequacy · SCC · BCR Overlays. Souveränitätsbericht auf Knopfdruck.



Integriertes Asset-Management — automatisierte Discovery.

Was Sie nicht kennen, können Sie nicht schützen. Kontinuierlicher Scan · 18 Kategorien · 60+ Felder · BIA auf Autopilot.

Automatisierte Discovery

12+ Quellen: Azure · AWS · GCP · K8s · Wiz · M365 · LeanIX · ServiceNow CMDB · Endpoint · DNS · SaaS.

BIA-Workflow

Owner-getriebenes CIA-Scoring · MTD/RTO/RPO · KI-Vorschläge aus Peer-Daten · Management-Freigabepipeline.

Vollständige IMS-Integration

Jedes Asset klassifiziert über ISMS, AIMS, PIMS, CSMS, BCMS — mit verknüpften Controls, Risiken und Lieferanten.

Schatten-IT-Erkennung

Kontinuierliche Discovery deckt nicht registrierte Cloud-, SaaS- und Dev-Umgebungen auf — leitet automatisch an die Governance weiter.

DISCOVERY → INVENTAR · ≤ 48 H

Erkennen › Dedupe › Klassifizieren › Owner zuweisen › BIA › Risiko › Freigeben › Registrieren

≥95 %
Inventar-Vollständigkeit

≥80 %
Auto-Discovery-Quote

100 %
BIA-Abschluss (kritisch)

<48 Std.
Onboarding-Zeit

≥70 %
Reduktion des manuellen Aufwands

Organisations- & Unternehmensmanagement.

Gemacht für Konzernstrukturen. Ein IMS · viele Einheiten. Policies werden von Konzern an Tochtergesellschaften vererbt. Lokale Autonomie, wo sie zählt.

Policy-Vererbung

Konzern-Policies kaskadieren zu Tochtergesellschaften. Lokales Override erlaubt, wo lokales Recht oder Scope dies erfordert.

Tochtergesellschaft-Autonomie

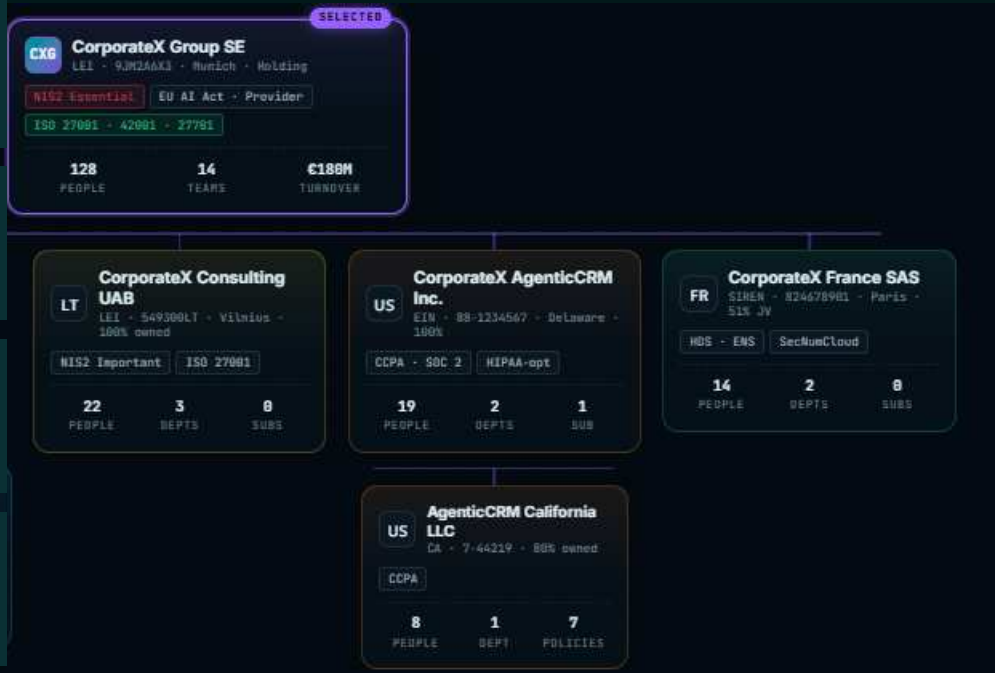
Tochterunternehmen können eigene Policies mit engem Geltungsbereich verfassen — ohne die Konzernkonformität zu brechen.

Rollen & Rechte · Least Privilege

Granulares RBAC: Konzern, Tochter, Geschäftseinheit, Asset. Jede Berechtigung auditierbar.

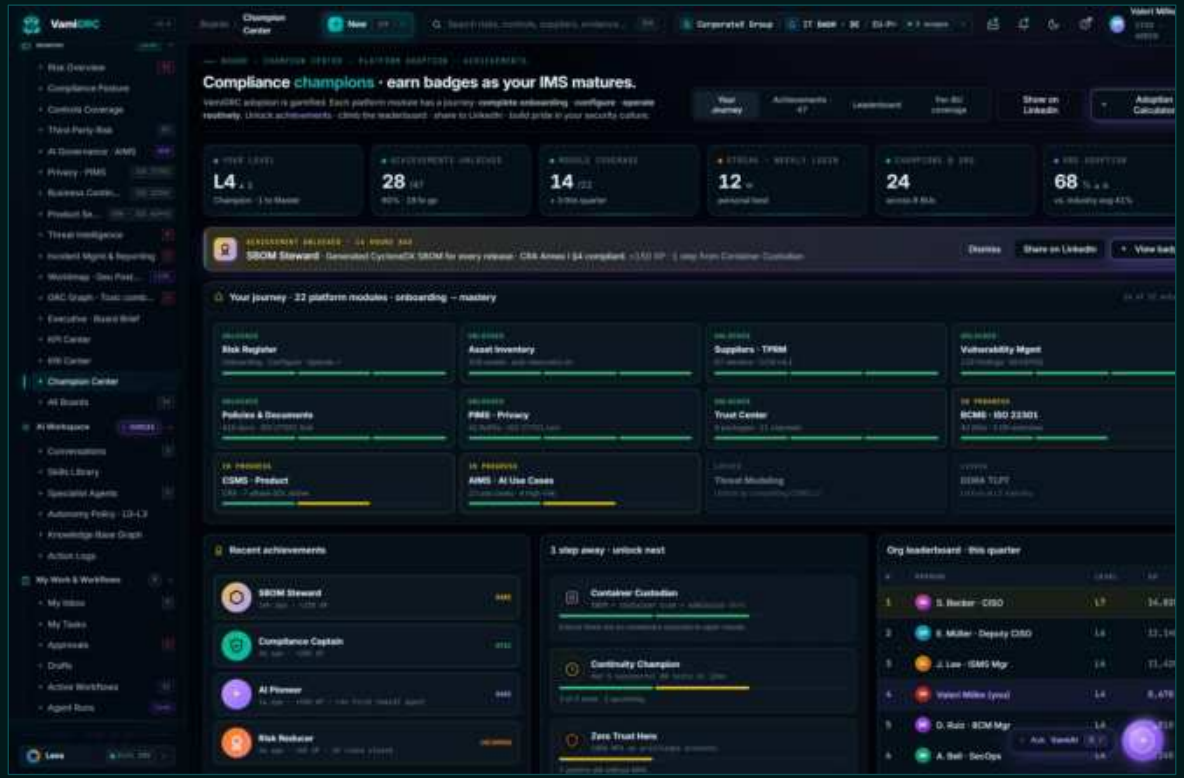
Gemeinsame Assets

Geteilte IT-Systeme, Standorte und Prozesse werden einmal definiert und sind für jede berechtigte Einheit sichtbar.



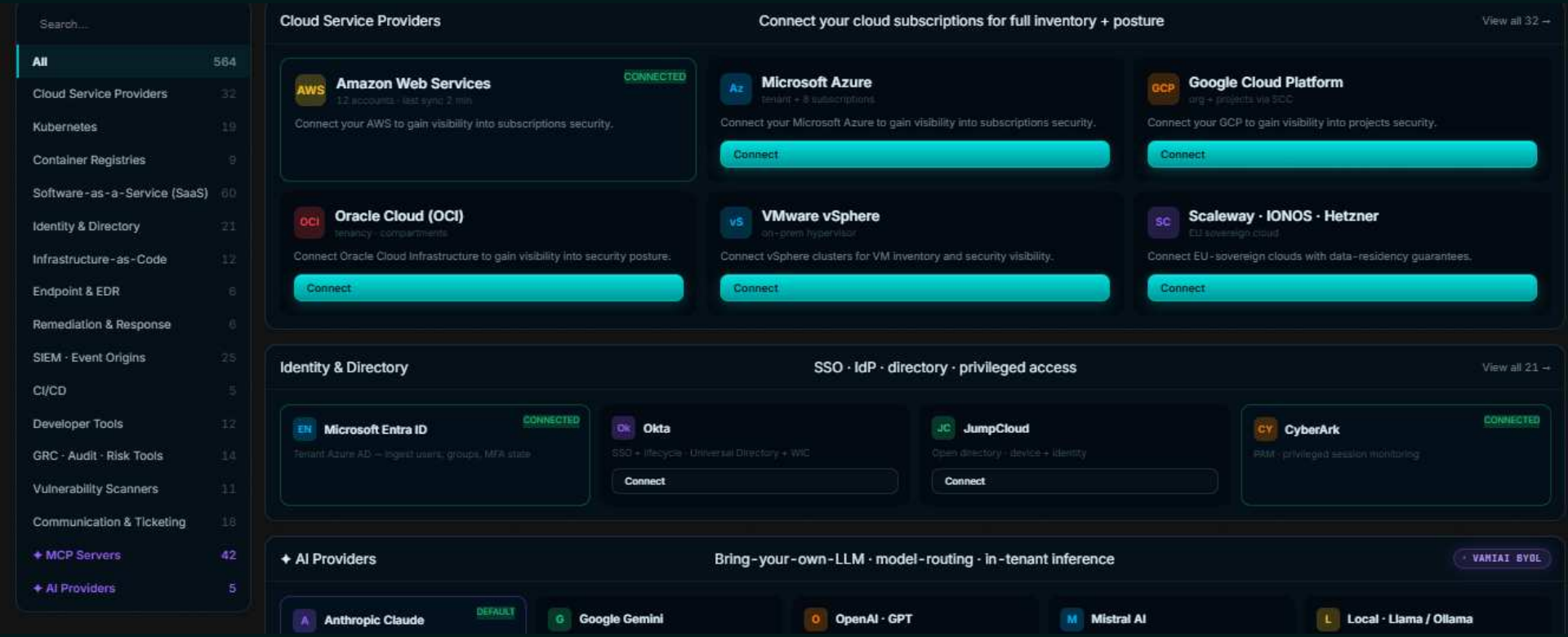
Champion Center — gamifizierte IMS-Einführung.

22 Module vom Risikoregister über BCMS und AIMS bis TLPT. Org-Leaderboard · auf LinkedIn teilen.



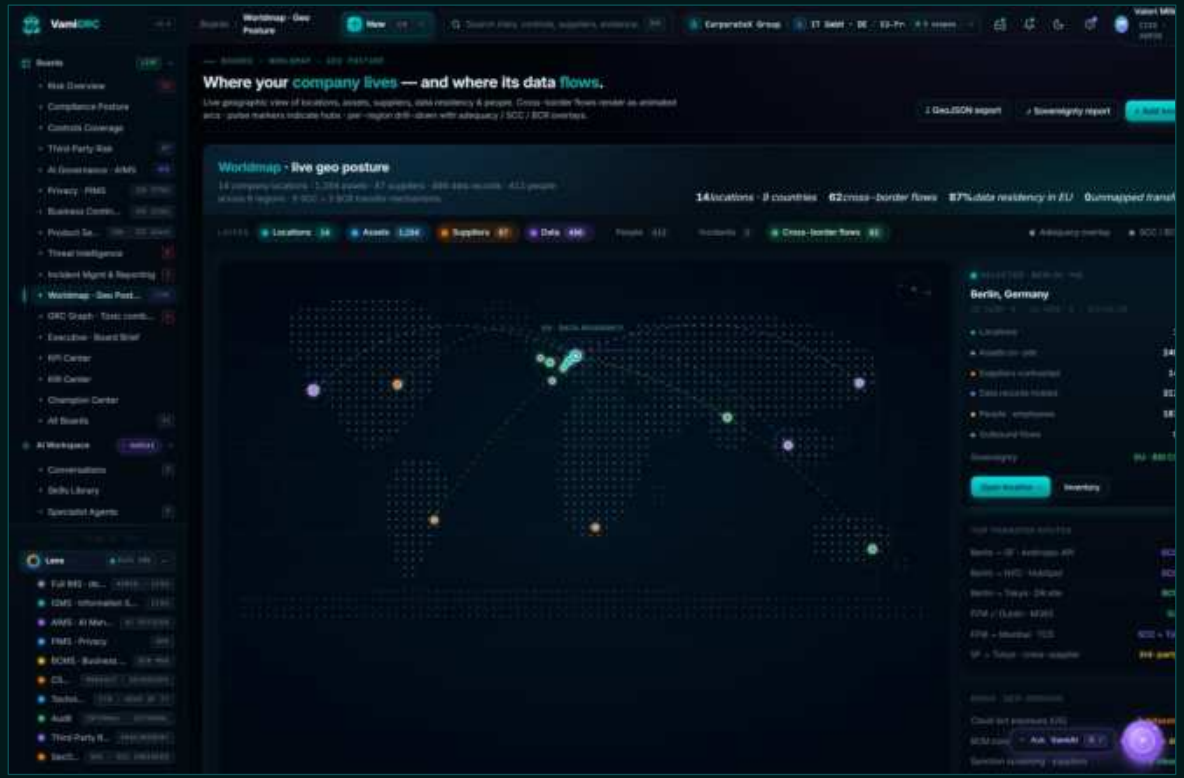
Personen- & Konten-Inventar — Least Privilege.

Azure Entra ID · Google Workspace · HR (SCIM) zusammengeführt in einem Identitätsgraphen. Joiner/Mover/Leaver automatisiert. Least-Privilege-Findings werden ins Risikoregister gepusht.



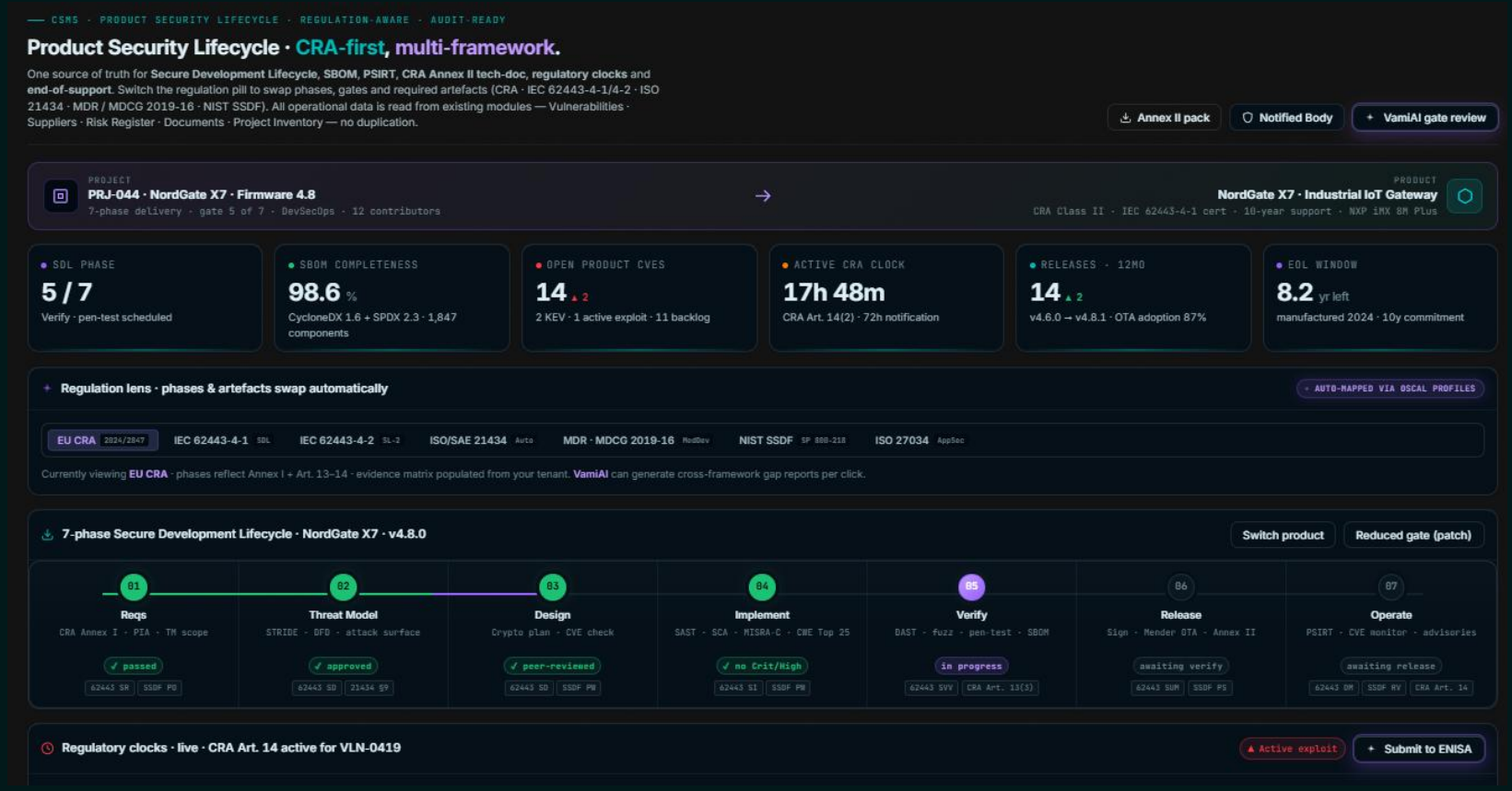
Weltkarte.

14 Standorte · 9 Länder · 62 grenzüberschreitende Datenflüsse. Adequacy · SCC · BCR Overlays. Souveränitätsbericht auf Knopfdruck.



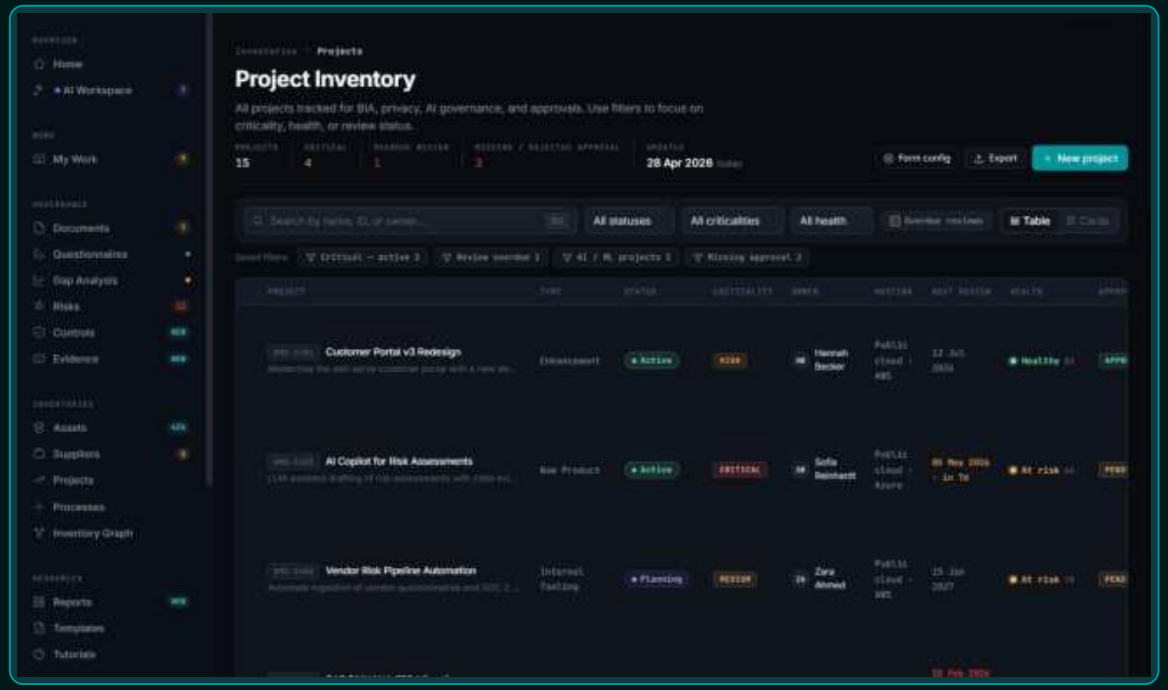
Produkt- & Projekt-Security-Lifecycle und -Management

Intake-Formular · 7-Phasen-Lifecycle mit Phasen-Gates · 81 Baseline-Controls automatisch zugewiesen · VamiRed-getriebenes Threat Modeling und Pentest.



Projektinventar — Governance auf einen Blick.

Jedes Projekt nachverfolgt für BIA, Datenschutz, KI-Governance und Freigaben. Filtern nach Kritikalität, Health oder Review-Status — eine Single Source of Truth.



WARUM DAS ZÄHLT

- **15 Projekte · 4 kritisch**

  Live-Zählung für überfällige Reviews, fehlende Freigaben und Health-Status — kontinuierlich aktualisiert.

- **Gespeicherte Filteransichten**

  Kritisch-aktiv · Review überfällig · KI/ML-Projekte · fehlende Freigabe — je ein Klick.

- **Projekt-Profil**

  Typ · Status · Kritikalität · Owner · Hosting · nächstes Review · Health Score · Freigabestatus.

Integriertes Control-Inventar — eine Bibliothek, jedes Framework.

Cross-Mapping-Engine: einmal umsetzen, mehrfach erfüllen. Statement of Applicability automatisch generiert für ISO 27001 + ISO 42001 + Unified IMS.

QUELL-FRAMEWORK-BIBLIOTHEK

TIER 1 — Kernstandards & Regularien

ISO 27001 · ISO 42001 · NIS2 · DORA · AI Act · DSGVO · CRA · IEC 62443 · ISO 22301

TIER 2 — Erweiterte Standards

ISO 27002 · ISO 27701 · TISAX · BSI Grundschutz · BSIG §8a · SOC 2

TIER 3 — Best-Practice-Frameworks

CIS Controls · NIST CSF · COBIT · OWASP · SOC2 TSC · MITRE ATT&CK

CROSS-MAPPING-ENGINE

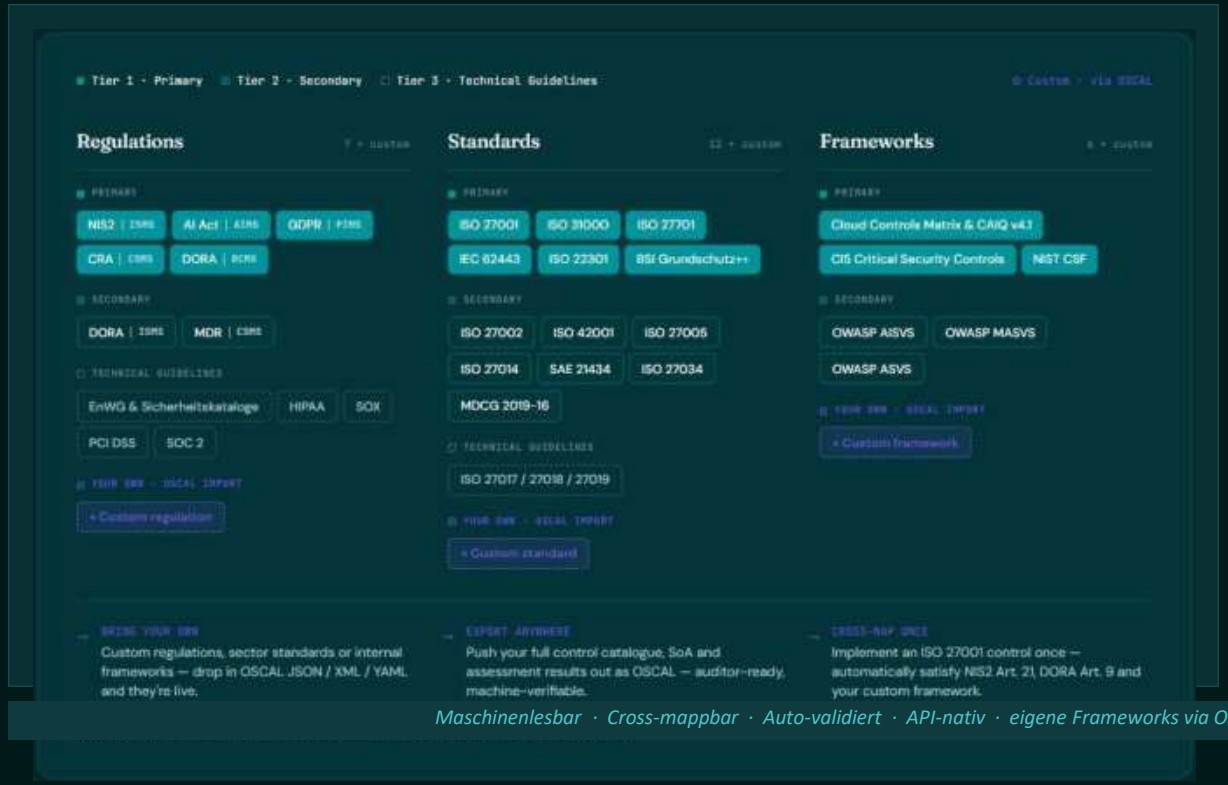
n-zu-n-Control-Beziehungen.

- ISO 27001 A.5.7 ↔ NIS2 Art. 21(2)(h) ↔ DORA Art. 9 — einmal umsetzen, dreifach erfüllen.
- KI-gestützte Control-Discovery: regulatorischer Scan, risikobasiert, Peer-Benchmark, Gap-Analyse.
- Automatisch generiertes Statement of Applicability (ISO 27001 + ISO 42001 + Unified-IMS-Sicht).
- Shared-Responsibility-Modell: pro Projekt, pro Lieferant, pro Control — per RACI nachverfolgt.

Einmal umsetzen. Mehrfach erfüllen. Audit-Ready by Design.

Auf OSCAL aufgebaut. Von Excel zu maschinenlesbaren Controls.

Die vom NIST geführte Open Security Controls Assessment Language als Rückgrat. Jede Regulierung, jeder Standard und jedes Framework als maschinenlesbares XML / JSON / YAML. Audit-Zyklen in Tagen, nicht Monaten.



→ BRING YOUR OWN

Eigene Regulierungen, Branchenstandards oder interne Frameworks — OSCAL JSON / XML / YAML einspielen und sie sind live.

→ EXPORT ANYWHERE

Exportieren Sie Ihren gesamten Control-Katalog, SoA und Assessment-Ergebnisse als OSCAL — auditorbereit, maschinell verifizierbar.

→ EINMAL CROSS-MAPPEN

Setzen Sie ein ISO-27001-Control einmal um — und erfüllen Sie automatisch NIS2 Art. 21, DORA Art. 9 und Ihr eigenes Framework.

Maschinenlesbar · Cross-mappbar · Auto-validiert · API-nativ · eigene Frameworks via OSCAL-Import.

Framework-Anwendbarkeit — was, warum, welcher Scope.

OSCAL-basierter Katalog · drei Anwendbarkeits-Treiber · automatisch abgeleitete Baseline · gap-aware ab Tag eins.

TREIBER 1

Rechtsregister

Vorab geladene EU- & nationale Pflichten. Organisationsprofil (Hauptsitz, Sektor, Größe, KRITIS) wird auf NIS2, DORA, AI Act, DSGVO, CRA, BSI Grundschutz abgebildet.

TREIBER 2

Kundenanforderungen

Verträge, RFPs, Security-Fragebögen. IDP-extrahierte Klauseln binden spezifische Frameworks (ISO 27001, TISAX, SOC 2).

TREIBER 3

Strategische Wahl

Freiwillige Zertifizierungen und Best-Practice-Frameworks (CIS Controls, NIST CSF, ISO 42001), vom Management ausgewählt.

OSCAL-ANWENDBARKEITS-ENGINE · CATALOG → PROFILE → SSP

1

Framework-Katalog

OSCAL-Katalog: vollständige Control-Bibliothek pro Regulierung/Standard.

2

Anwendbarkeits-Profil

Organisationsspezifische Auswahl: welche Kataloge · welches Baseline-Level.

3

Org-Profil-Wizard

Branche · Länder · Größe · KRITIS · KI-Risikoklasse · Cloud-Nutzung.

4

Abdeckungsmatrix

Frameworkübergreifende Sicht: wo ein Control mehrere abdeckt.

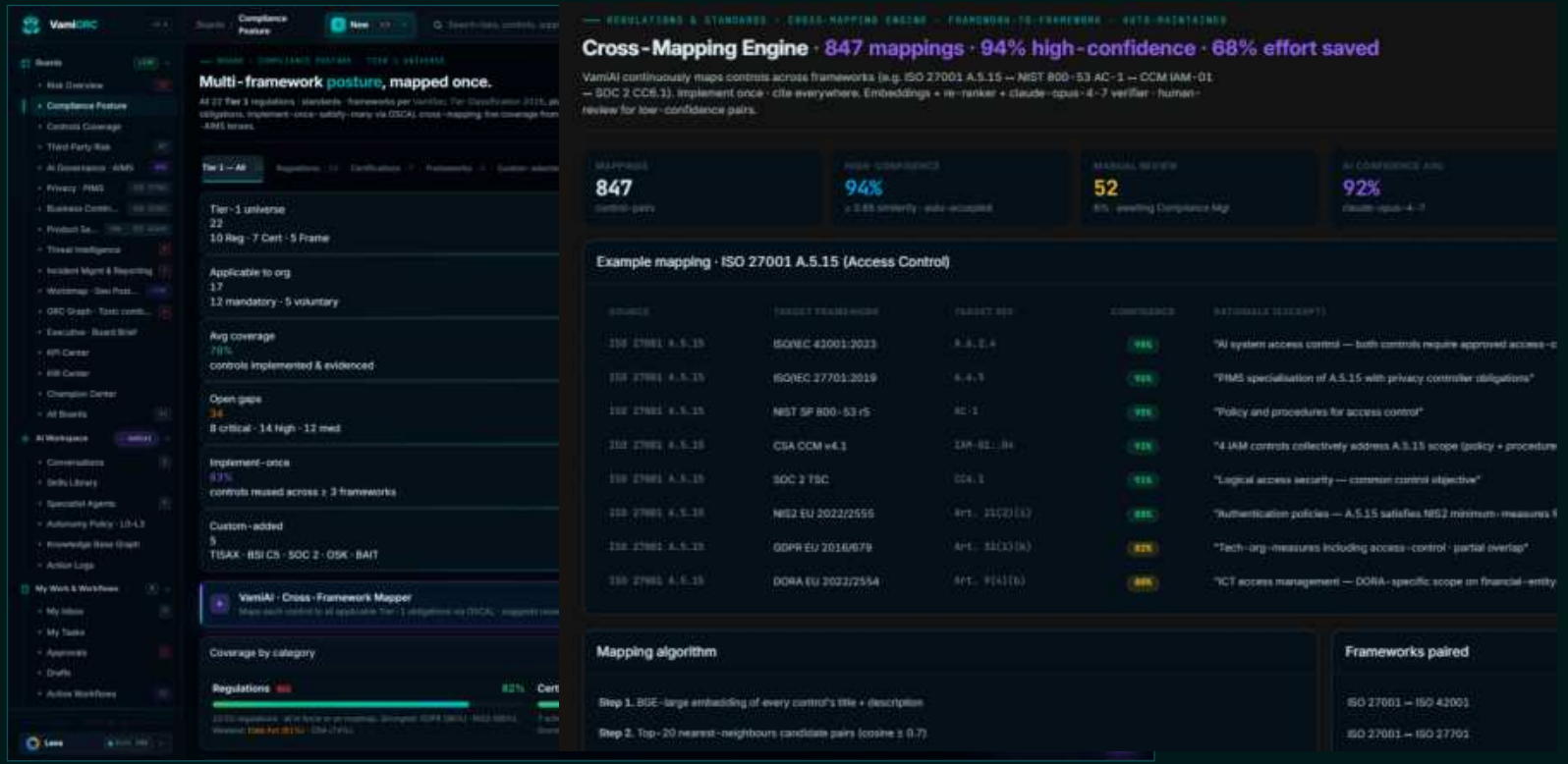
5

Gap-Engine

Ausgewählt ≠ umgesetzt: jede Lücke ein Finding mit Verantwortlichem & Fälligkeitsdatum.

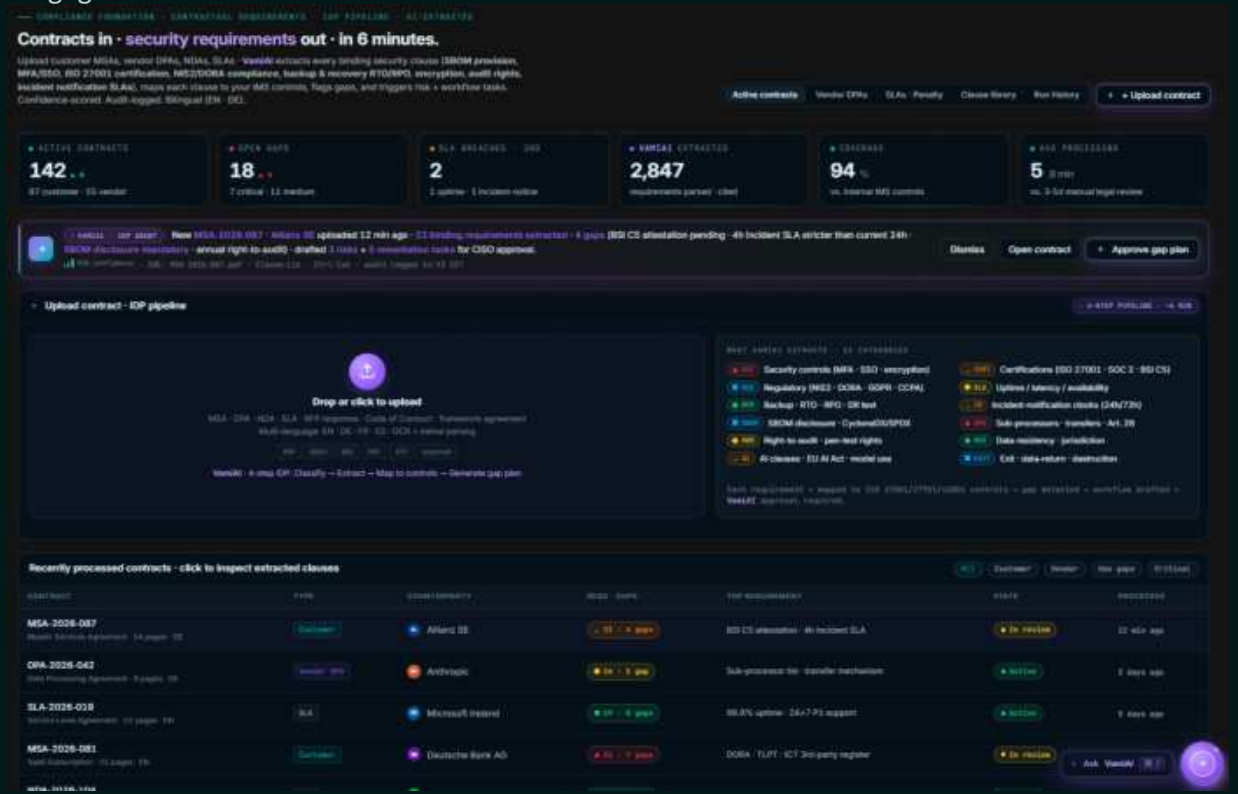
OSCAL Cross-Mapping — einmal umsetzen, mehrfach erfüllen.

22 Tier-1-Pflichten · 81 % Control-Wiederverwendung über 3+ Frameworks · BYO-Frameworks via OSCAL JSON.



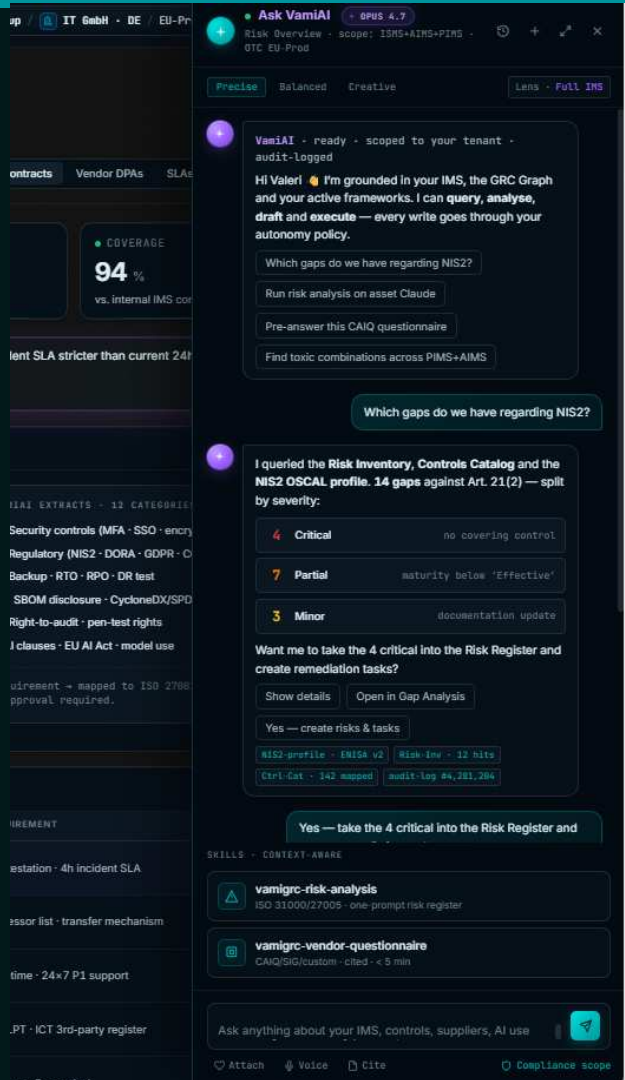
Vertragliche Anforderungen — extrahieren, verifizieren, überwachen.

Intelligent Document Processing für Kundenverträge, Partnervereinbarungen und SLAs. KI extrahiert Sicherheitsklauseln; VamiAI verifiziert sie gegen Ihr IMS.



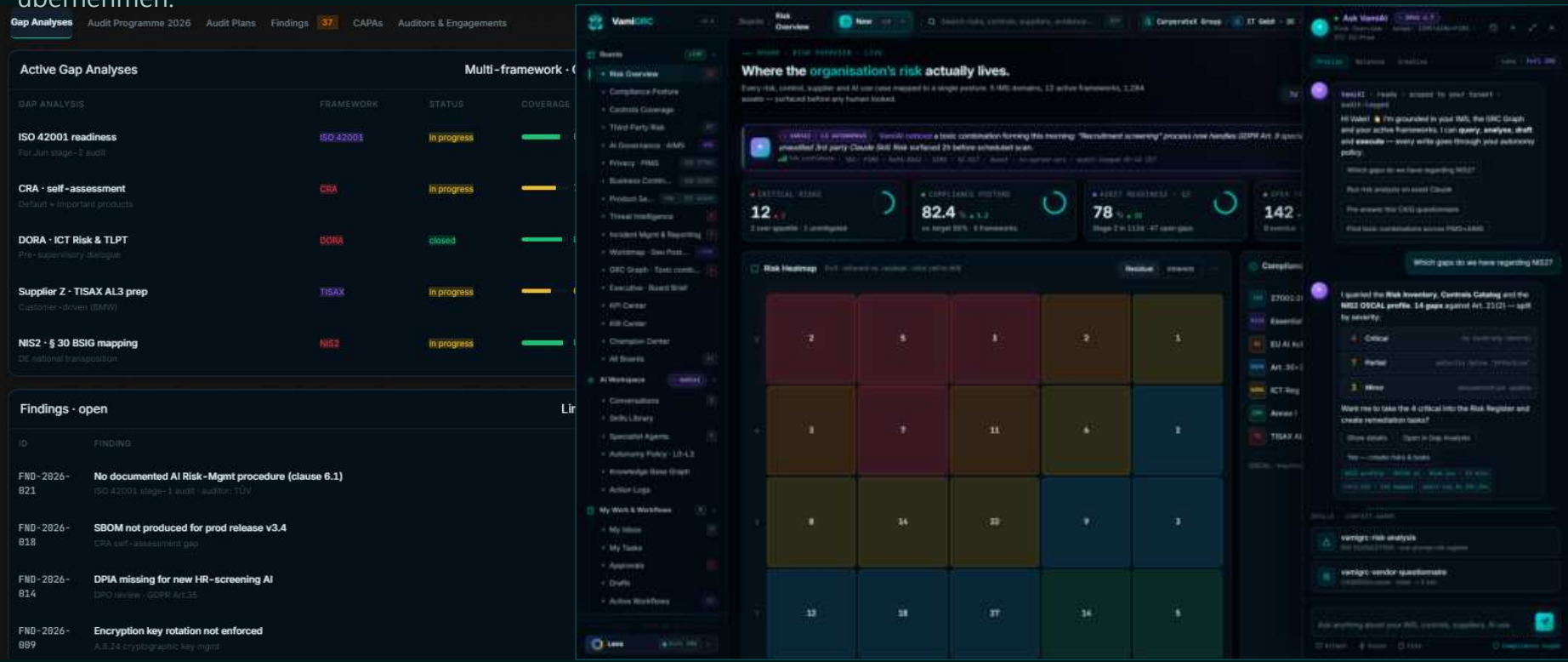
VamiAI – In natürlicher Sprache fragen und Anweisungen geben. Antworten erhalten und ausführen lassen.

VamiAI verwandelt Fragen in Graph-Abfragen — gefiltert nach Ihren Berechtigungen, gestützt auf Ihre Nachweise.

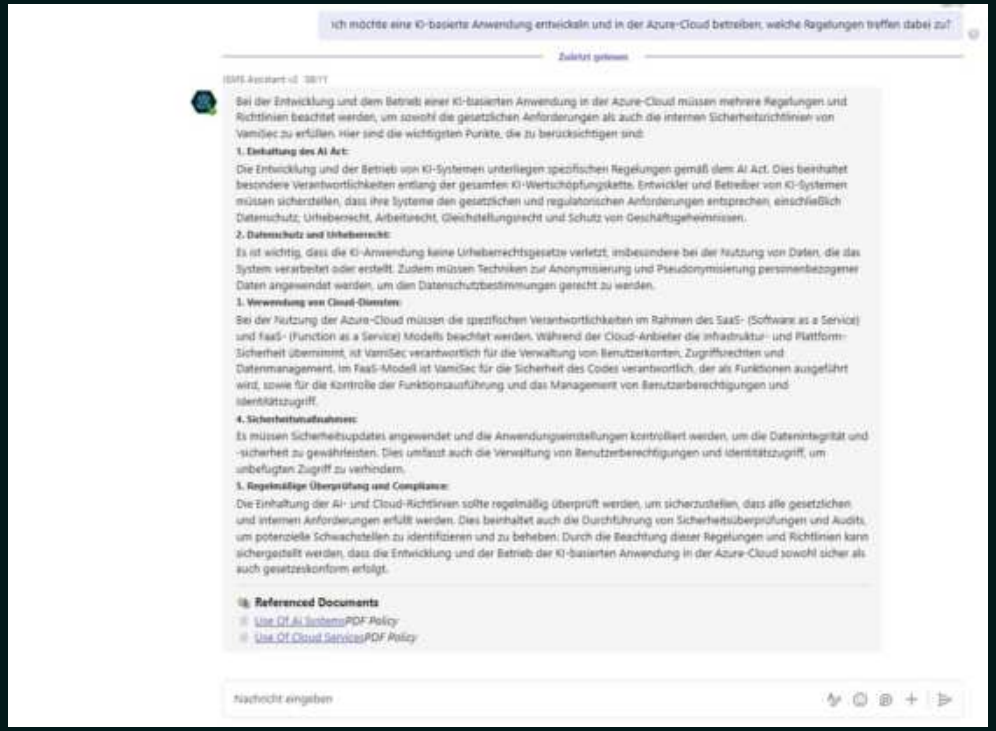


VamiAI — NIS2-Gap-Analyse, zitiert.

Frage in natürlicher Sprache. 14 Lücken in 8 Sekunden mit zitierten Nachweisen. Anschließend 4 kritische ins Risikoregister übernehmen.



VamiAI in Microsoft Teams — Awareness und Sichtbarkeit über die MS-Teams-Integration maximieren.



Vier Autonomiestufen. Sie entscheiden, wo jede Aufgabe verortet ist.

Adaptiert aus OWASP APTS für die GRC-Domäne. Jeder Schreibvorgang fällt in eine definierte Autonomiestufe. Keine stille Automatisierung. Immer auditierbar.

LEVEL	NAME	AUSFÜHRUNG	FREIGABE	USE CASES	RISIKO
L0	**Manuell**	Mensch führt alle Arbeiten aus. KI leistet keine Unterstützung.	Standard-Workflow	Ad-hoc · sensible Entscheidungen · Management-Reviews · Budget-Freigaben	Keines
L1	**KI-unterstützt**	Mensch führt aus; KI liefert Entwürfe und Vorbefüllungen.	Standard-Workflow	Risikobewertungen (KI schlägt Scores vor) · Policy-Reviews · Fragebogenanalyse	Niedrig
L2	**KI-ausgeführt + Freigabe**	KI führt autonom aus. Ergebnis erfordert menschliche Freigabe.	Verpflichtend vor Abschluss	Lieferanten-Assessments · Gap-Analysen · Access-Reviews · Nachweis-Entwürfe	Mittel
L3	**Vollständig autonom**	KI führt aus und schließt ab — ohne menschlichen Eingriff.	Nur Information · auditiert	Kontinuierliches Monitoring · Zertifikatsablauf · OSINT-Anreicherung · Routine-Scans	Hoch

VOLLSTÄNDIGE AUDITIERBARKEIT

Jeder Prompt, Tool-Aufruf und Schreibvorgang wird mit Zeitstempel, Modellversion und Reasoning-Trace protokolliert.

AI ACT READY

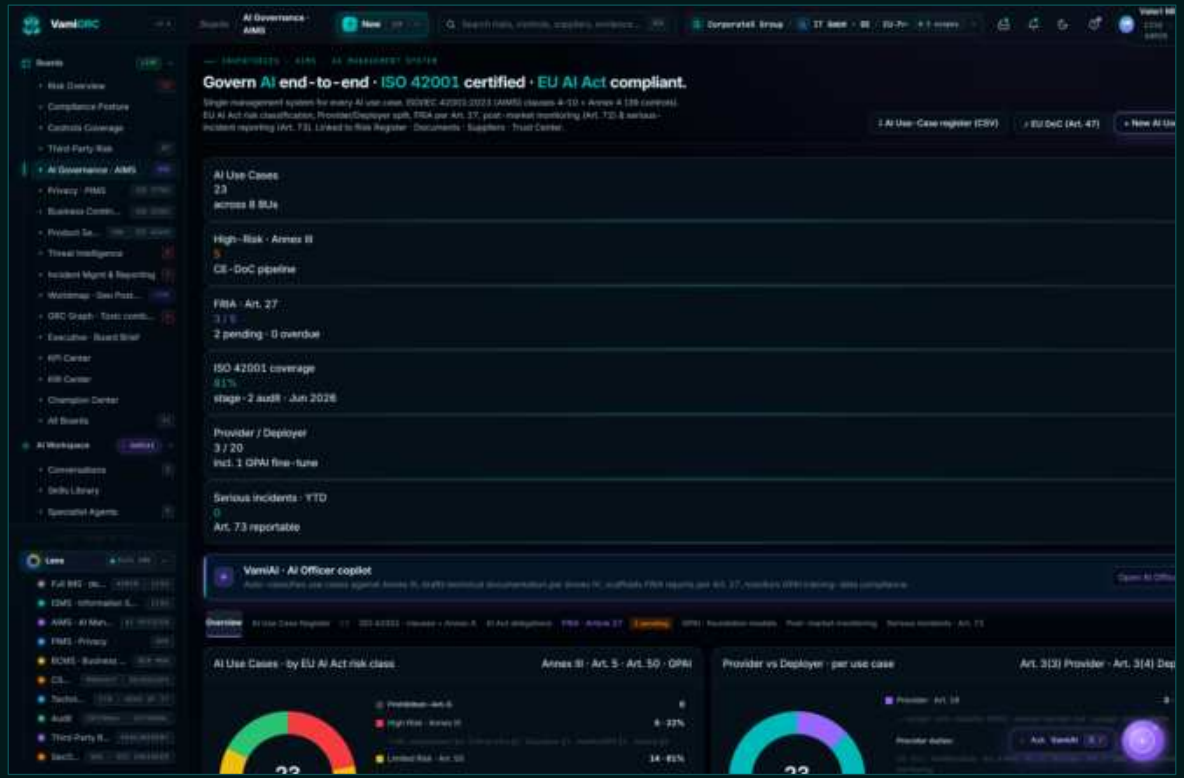
Audit-Trails erfüllen die Logging-Anforderungen aus EU AI Act Art. 12. Exportierbar für Aufsichtsbehörden.

HUMAN IN THE LOOP

L2 erzwingt verpflichtende menschliche Freigabe. L3 kann jederzeit pausiert, überprüft und zurückgesetzt werden.

AIMS — ISO 42001 + EU-AI-Act-Board.

23 KI-Use-Cases · 5 Hochrisiko-Anhang-III · FRIA-Timer · Post-Market-Monitoring · ISO-42001-Abdeckung 81 %.



02

Security Operations

Pentest · VPS · ASM · Risiko · Audit

Pentesting-Management.

Planen. Autorisieren. Durchführen. Verifizieren. — Findings = Schwachstellen, end-to-end gesteuert.

DREI URSPRUNGS-PFADE

01 — Aus einem Projekt

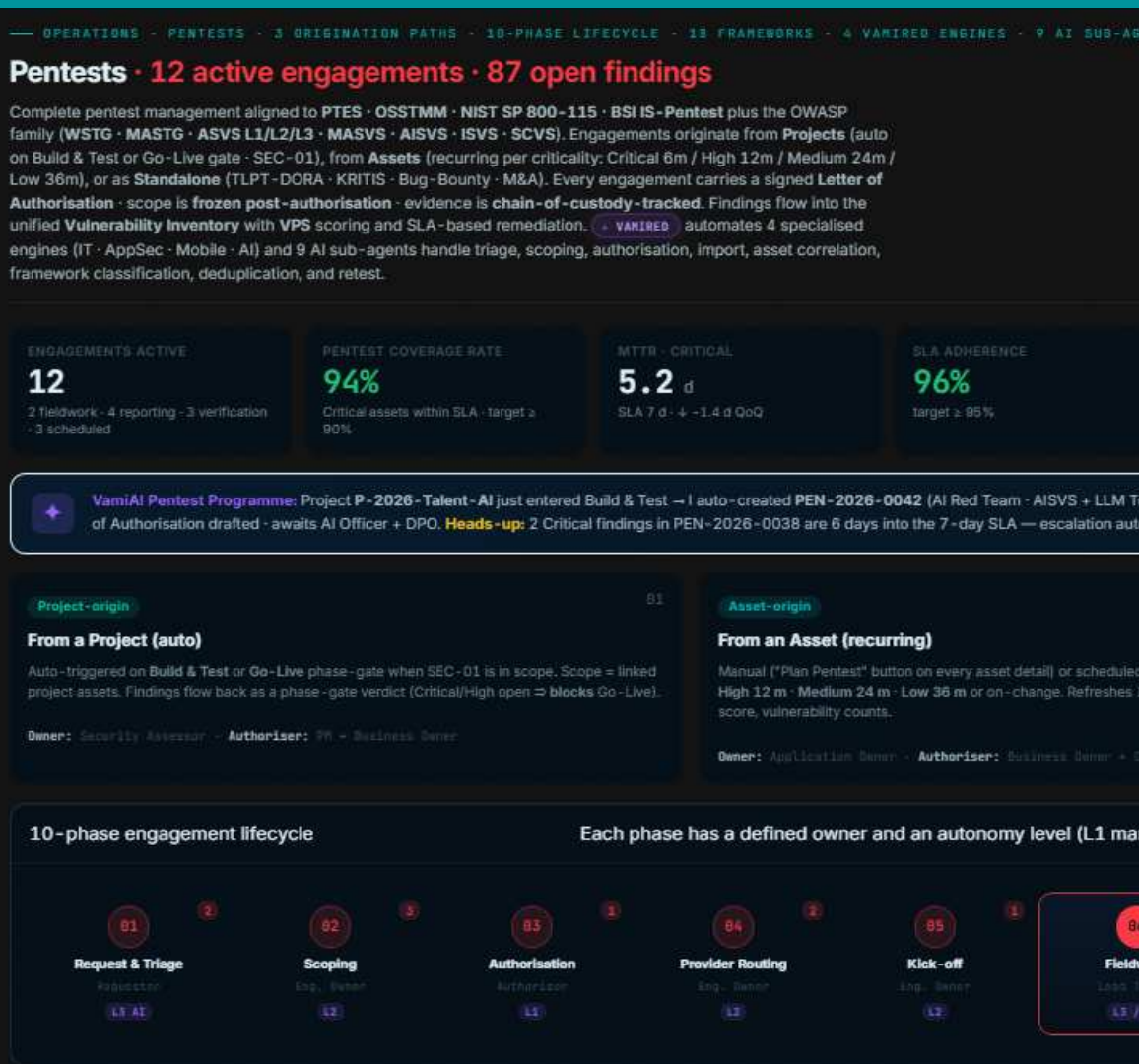
Ausgelöst am Build- & Test-Gate. Findings blockieren Go-Live.

02 — Aus einem Asset

"Pentest planen"-Button pro Asset. Wiederkehrend nach Kritikalität.

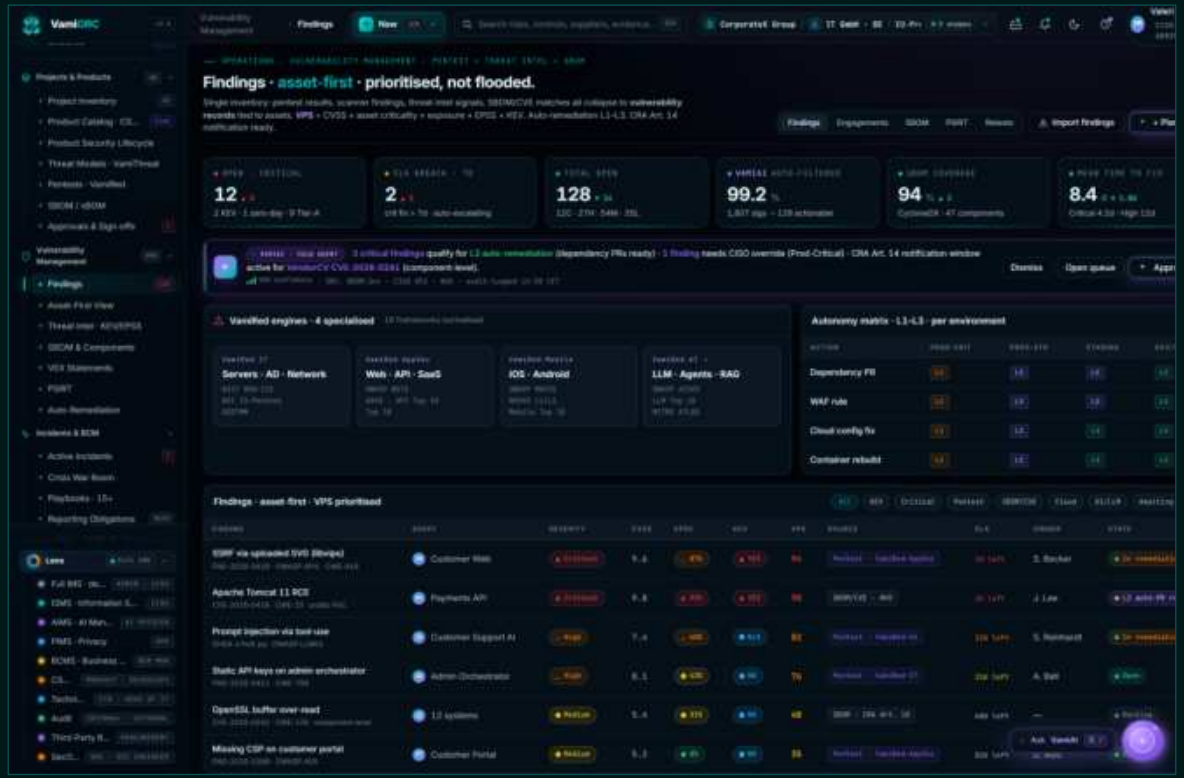
03 — Standalone

TLPT (DORA), KRITIS, M&A, Bug-Bounty-Triage.



VPS — Asset-First Vulnerability Management.

1.800 CVEs/Tag gefiltert auf ~8, die Sie tatsächlich betreffen. Auto-Remediation L1–L3. VEX eliminiert 75 % des Scanner-Rauschens.



Vulnerability Management & Threat Intelligence.

Asset-first-Inventar · Zero-Day-proaktive Abwehr · KI-Korrelation & VPS-Priorisierung · Auto-Remediation mit Autonomie-Matrix.

Asset-First-Inventar

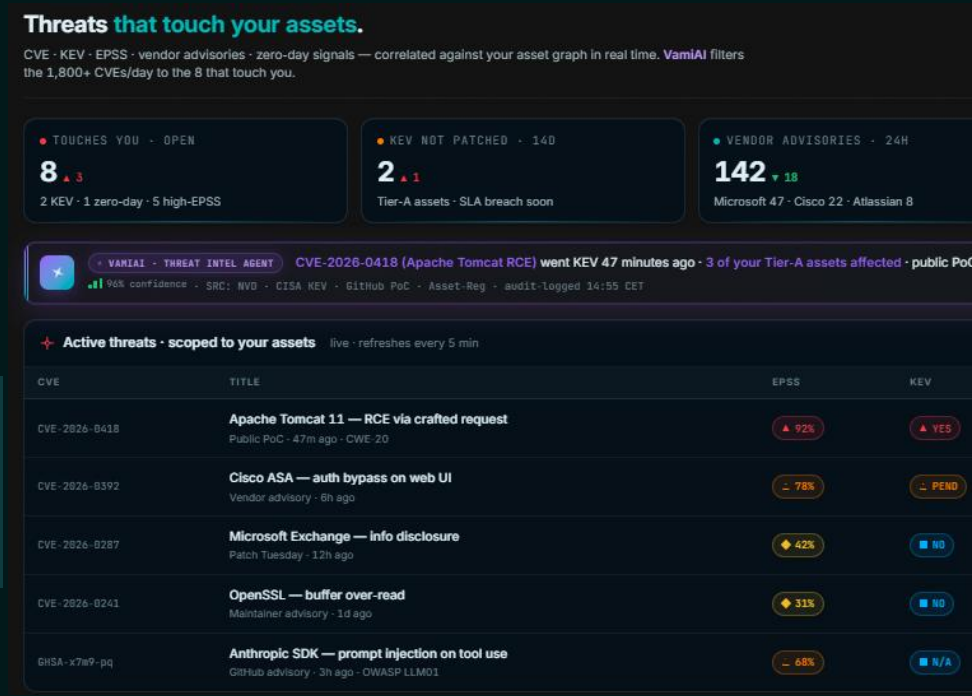
Jede Schwachstelle wird einer Asset-ID zugeordnet. Pentest, SAST, DAST, SCA, Cloud, CVE-Feeds — dedupliziert.

Threat-Intel-Engine

Zero-Day-Workflow: 4-Stunden-proaktive Impact-Analyse · KEV · EPSS · Vendor Advisories · OSV.

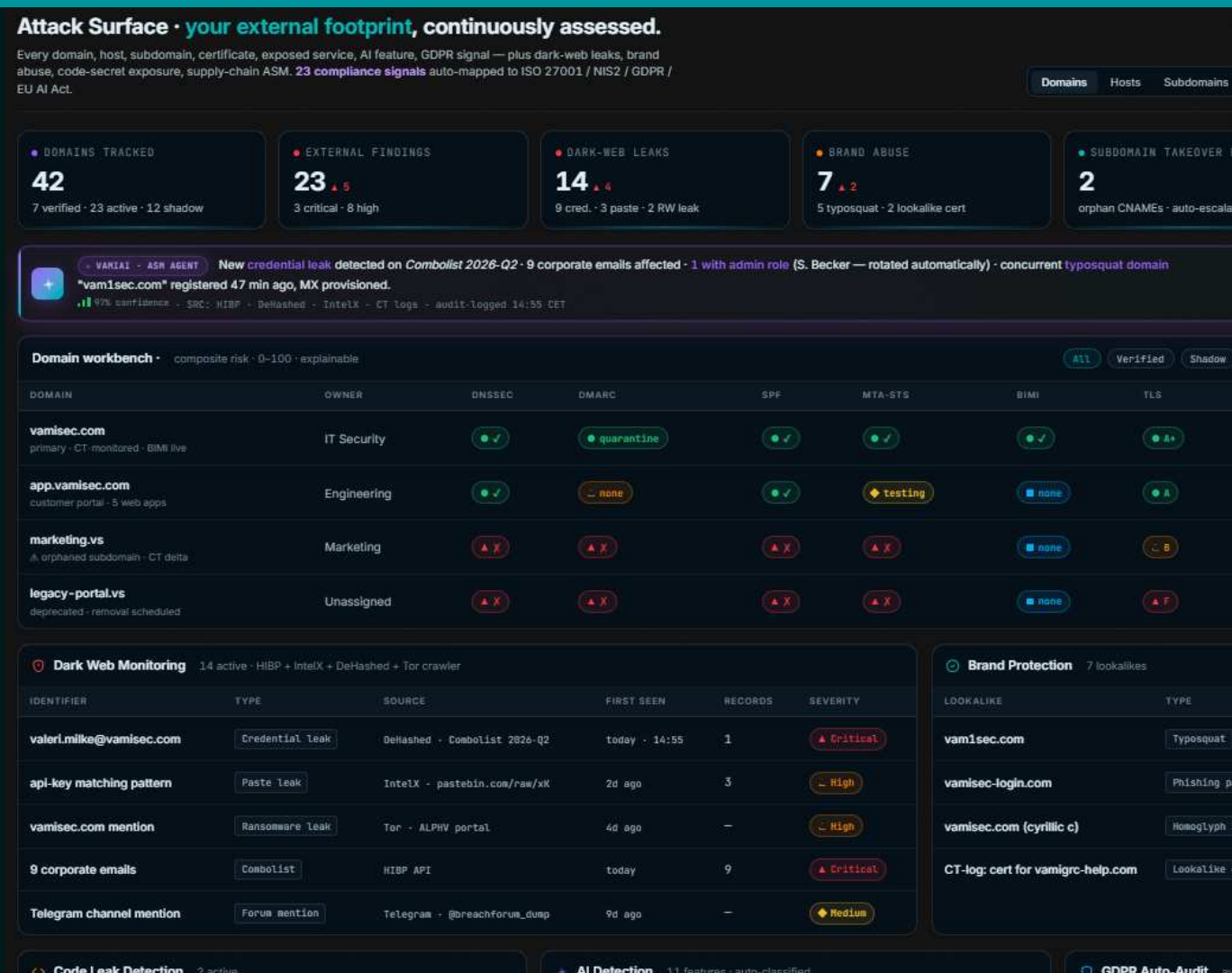
SBOM · KOMPONENTEN-LEVEL-TRACKING

CycloneDX & SPDX pro Release · Sub-Asset-Tracking für CSMS · VEX-Statements · transitive Dependency-Reichweite.



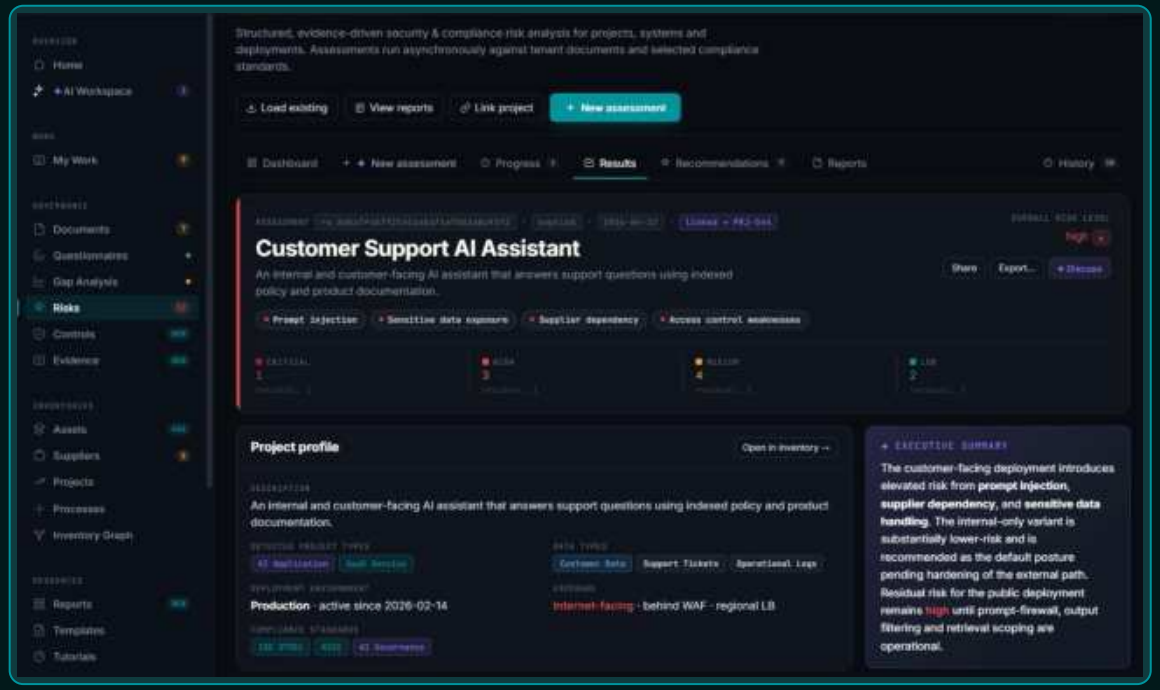
Domains & Attack Surface Management.

Ihr externer Footprint, kontinuierlich erkannt, bewertet und überwacht.



KI-Risikobewertung — kontextbewusst, nachweisgetrieben.

Strukturierte Sicherheits- & Compliance-Risikoanalyse für Projekte, Systeme und Deployments. Verknüpft mit dem Projektdatensatz. Abgebildet auf ISO 27001, NIS2, AI Governance.



WARUM DAS ZÄHLT

- **Risikoansicht je Deployment**

  Customer-Support-KI-Assistent · verknüpft mit PRJ-044 · bewertet Kritisch 1 · Hoch 3 · Mittel 4 · Niedrig 2.

- **Erkannte Risikovektoren**

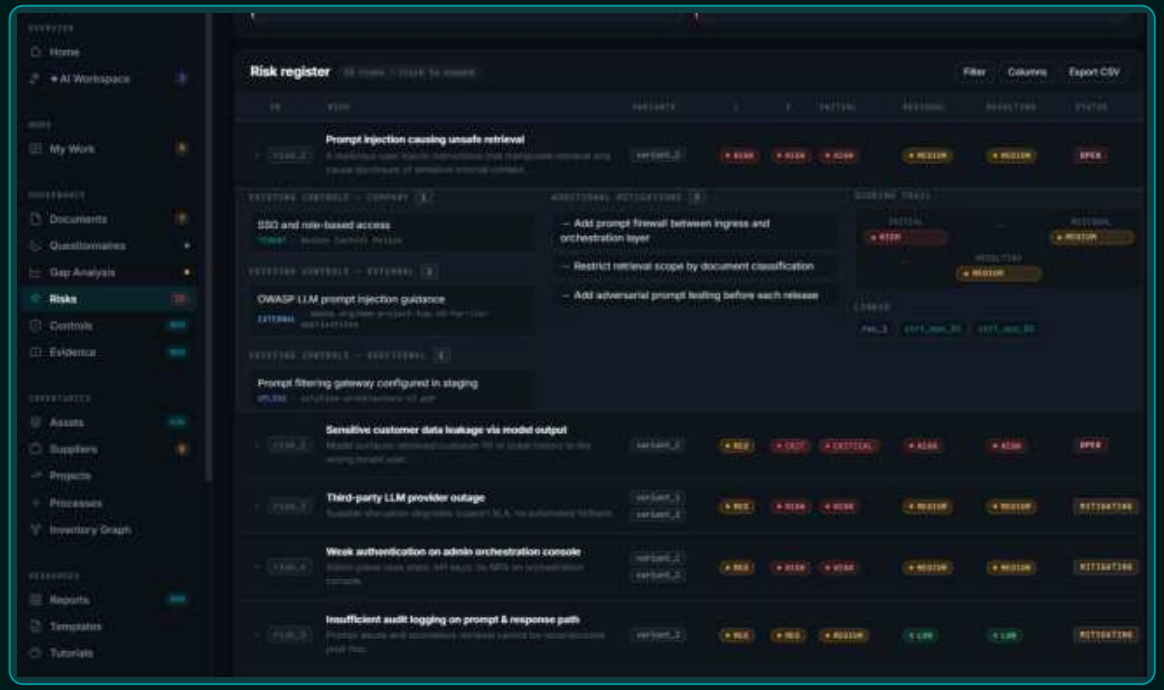
  Prompt Injection · Offenlegung sensibler Daten · Lieferantenabhängigkeit · Schwächen der Zugriffskontrolle.

- **Executive Summary, generiert**

  Klare Erläuterung für den Vorstand — mit Nachweisverweisen und empfohlener Haltung.

Risikoregister — inhärent vs. Rest, mit Behandlung.

Jedes Risiko erhält Owner, bestehende Controls (Unternehmen · extern · zusätzlich), vorgeschlagene Maßnahmen und eine vollständige Scoring-Historie — initial → Rest → resultierend.



WARUM DAS ZÄHLT

- **Bestehende Controls · 3 Ebenen**

  Unternehmens-Controls · externe Leitfäden (z. B. OWASP) · zusätzliche Uploads — alles verknüpft.

- **Vorgeschlagene Maßnahmen**

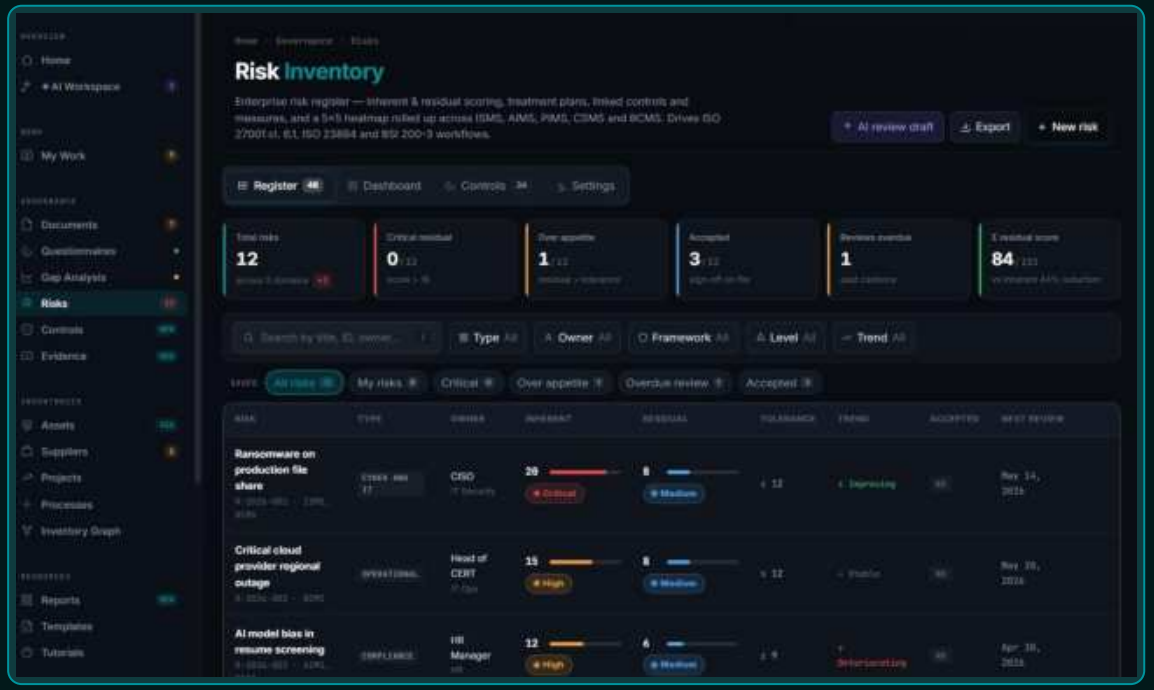
  KI schlägt die nächsten Schutzmaßnahmen vor: Prompt-Firewall · Einschränkung des Retrieval-Scopes · Adversarial Testing.

- **Scoring-Historie sichtbar**

  Initial · Rest · resultierende Stufen werden nebeneinander mit verknüpften Empfehlungen und Controls dargestellt.

Enterprise-Risiko-Inventar.

Inhärentes & Restrisiko-Scoring · 5×5-Heatmap aggregiert über ISMS, AIMS, PIMS, CSMS und BCMS · Trendanalyse · Akzeptanz-Workflow.



WARUM DAS ZÄHLT

- **12 Risiken · 5 Domänen**

  Kritisch (Rest) · über Appetit · akzeptiert · Reviews überfällig — ein Dashboard, sechs Sichten.

- **Inhärent → Rest-Delta**

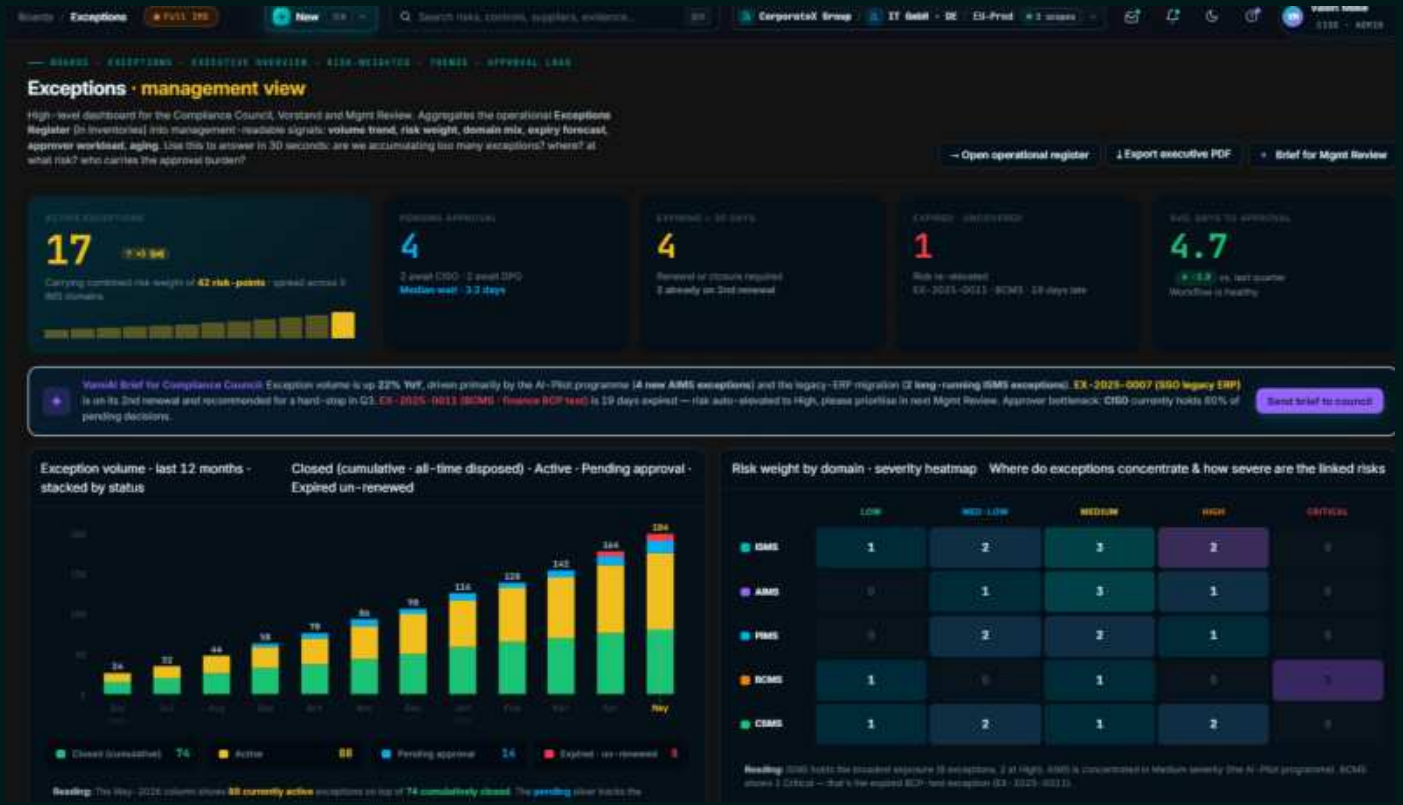
  44 % Reduktion auf Registerebene sichtbar — Score, Typ, Owner und Toleranz pro Zeile.

- **Trend & nächste Prüfung**

  Pfeile für „verbessernd · stabil · verschlechternd". Kadenz erzwungen, akzeptierte Risiken mit Audit-Trail.

Ausnahmemanagement zur Risikofreigabe.

Inhärentes & Restrisiko-Scoring · 5×5-Heatmap aggregiert über ISMS, AIMS, PIMS, CSMS und BCMS · Trendanalyse · Akzeptanz-Workflow.



Risikoanalyse & Multi-Framework-Gap-Assessment.

Risikoregister auf einen Prompt · ISO-31000/27005-konform · auditbereite PDF- + Excel-Exporte.

Internes Audit & Gap-Analyse — drei Modi, Multi-Framework.

Vollautomatisiert · interviewbasiert · hybrid. ISO-9.2-Audits · ISO 27001 + 42001 + NIS2 + DORA + CRA in einem Durchgang.

MODUS 1

Vollautomatisierte KI

Agenten bewerten ISMS/AIMS-Dokumente gegen Framework-Controls. Findings mit Confidence-Score.

`0 Personenstunden`

MODUS 2

Interviewbasiert

Auditee-Portal · strukturierte Interview-Workshops · ISO-19011-Walkthroughs · Stichprobenverfahren.

`Workshop-Stil`

MODUS 3

Hybrid (empfohlen)

KI bewertet alles vor. Auditor prüft und vertieft per Interview nur dort, wo nötig.

`Best of Both`

KOMBINIERT MULTI-FRAMEWORK

ISO 27001 + NIS2 + DORA in einem Assessment.

Cross-Mapping-Engine dedupliziert Auditfragen:

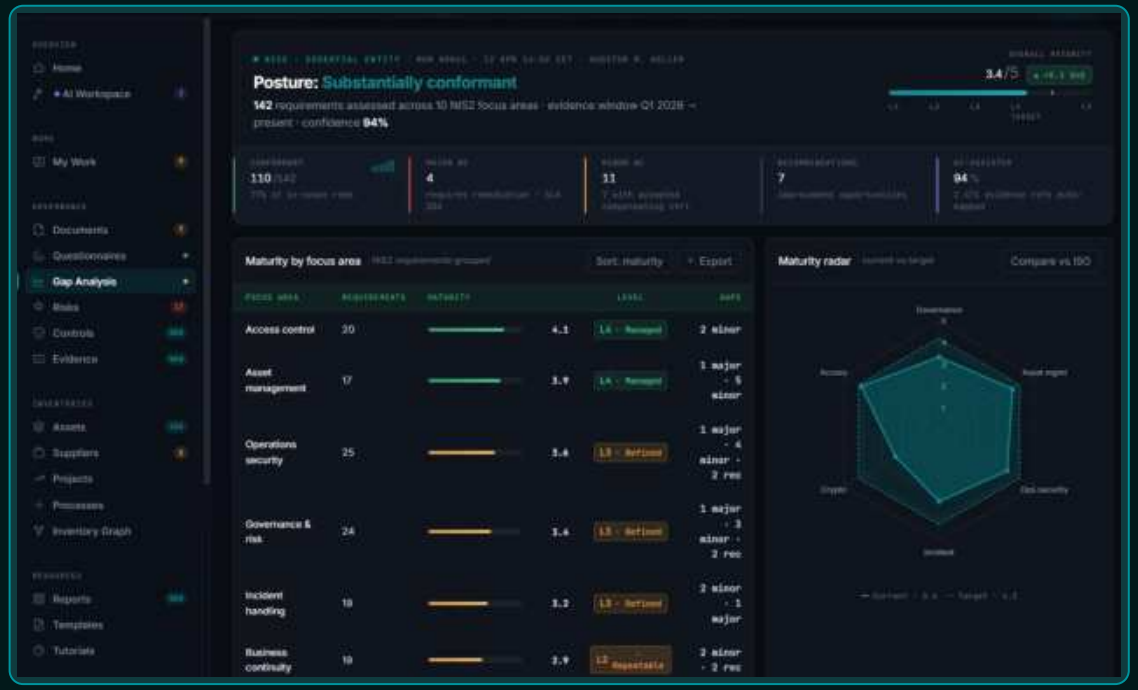
≈ 40 % weniger Fragen · ein Nachweis-Durchgang · ein Berichtssatz

FINDING-REGISTER · CAPA-TRACKING

Major-NK	→ legt automatisch Risiko + CAPA an · Eskalation
Minor-NK	→ Korrekturmaßnahme · Fälligkeit · Owner
Beobachtung	→ nachverfolgt, getrendet, im Management-Review geprüft
OFI	→ Improvement-Backlog · priorisiert

Kontinuierliches Framework-Assessment — Reifegrad in Echtzeit.

Jedes Control, jede Policy und jedes Log gemappt gegen Ihre aktiven Frameworks. NIS2, ISO 27001:2022, CRA — per Klick umschaltbar. Offene Lücken bis zur Behebung verfolgt.



WARUM DAS ZÄHLT

- **Im Wesentlichen konform**

  142 Anforderungen bewertet · 110 konform · 4 Major-NK · 11 Minor · Confidence 94 %.

- **Reife-Radar vs. Ziel**

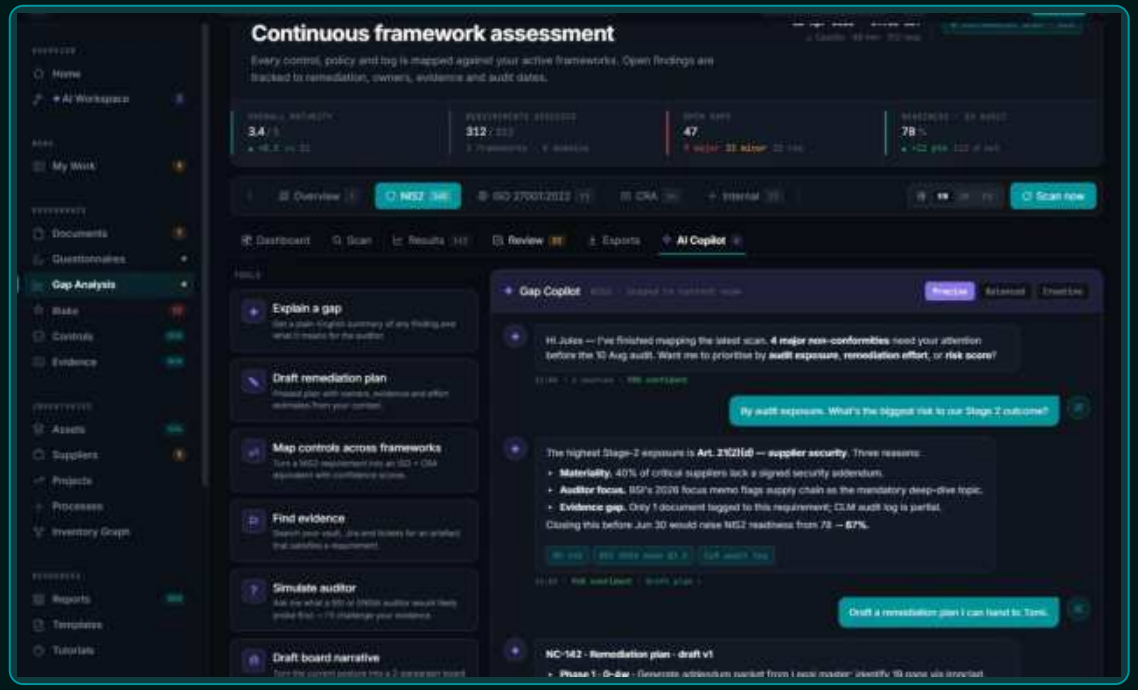
  Pro Fokusbereich aktuelle vs. Ziel-Reife — Governance · Asset · Crypto · Incident · Ops · Access.

- **Audit-Bereitschaft bewertet**

  78 % Q3-Audit-Bereitschaft · +12 Punkte · 112 Tage entfernt — jede Änderung mit Nachweis verfolgt.

Gap-Copilot — sprechen Sie mit Ihren Lücken.

KI-Assistent, eingegrenzt auf den aktuellen Scan. Lücke erklären · Behebung entwerfen · Controls über Frameworks mappen · Nachweise finden · Auditor simulieren — in einem Thread.



WARUM DAS ZÄHLT

- **Priorisierung der Audit-Exposure**

  „Höchste Stage-2-Exposition ist Art. 21(2)(d) — Lieferantensicherheit“ — mit 3 Begründungen, alle belegt.

- **Das Schließen erhöht die Readiness**

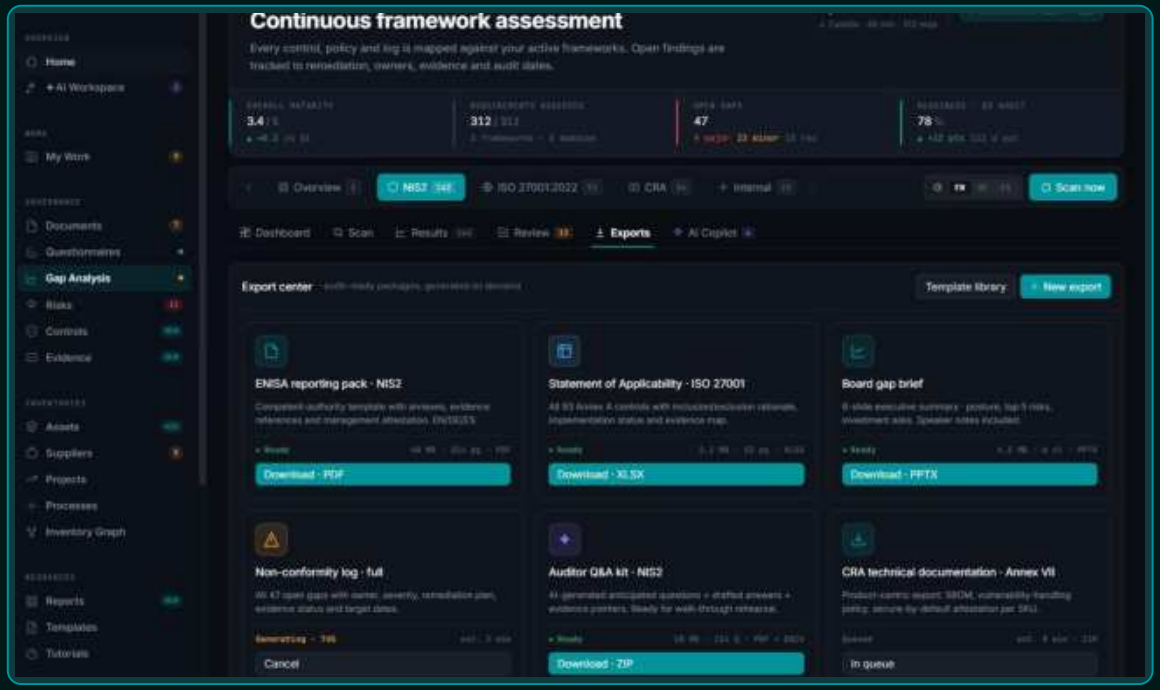
  Konkretes Delta sichtbar: 78 → 87 %, wenn NK-142 vor dem 30. Juni geschlossen wird — umsetzbar, nicht theoretisch.

- **Erstellt den Behebungsplan**

  Phase 1 (0–4 W) · Phase 2 (4–8 W) · Owner und Aufwandsschätzungen aus Ihrem Kontext gezogen.

Export Center — auditbereite Pakete auf Knopfdruck.

ENISA-Reporting-Pack · Statement of Applicability · Board-Gap-Brief · Non-Conformity-Log · Auditor-Q&A-Kit · CRA-technische Dokumentation. Generiert, nicht zusammengebaut.

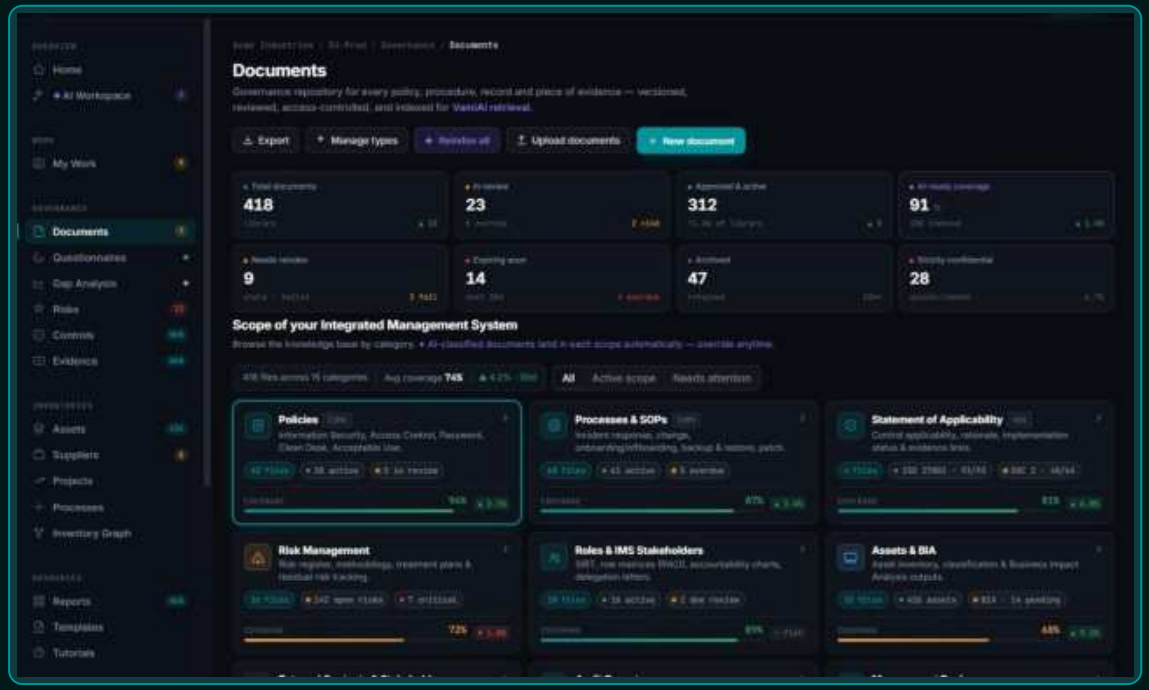


WARUM DAS ZÄHLT

- **Sechs Pakettypen · framework-parametrisch**
  PDF · XLSX · PPTX · ZIP als Output — NIS2, ISO 27001, CRA, intern — gleiche Engine.
- **Multi-Sprach-nativ**
  EN · DE · ES aus einer Quelle generiert. Keine erneute Übersetzung. Kein Drift.
- **Status: bereit oder in Erstellung**
  Echte ETA, echter Fortschritt, echte Bytes — Vorlagen für zuständige Behörden mit Anhängen und Bestätigung.

Dokumenten-Repository — KI-klassifiziert, auditiert.

Governance-Repository für jede Policy, Verfahrensanweisung, jeden Datensatz und Nachweis — versioniert, geprüft, zugriffskontrolliert und für die VamiAI-Suche indexiert.



WARUM DAS ZÄHLT

- **418 Dokumente · 91 % KI-ready**

  Gesamt · in Prüfung · freigegeben · läuft bald aus · archiviert · streng vertraulich — auf einen Blick.

- **Auto-klassifiziert · 15 Kategorien**

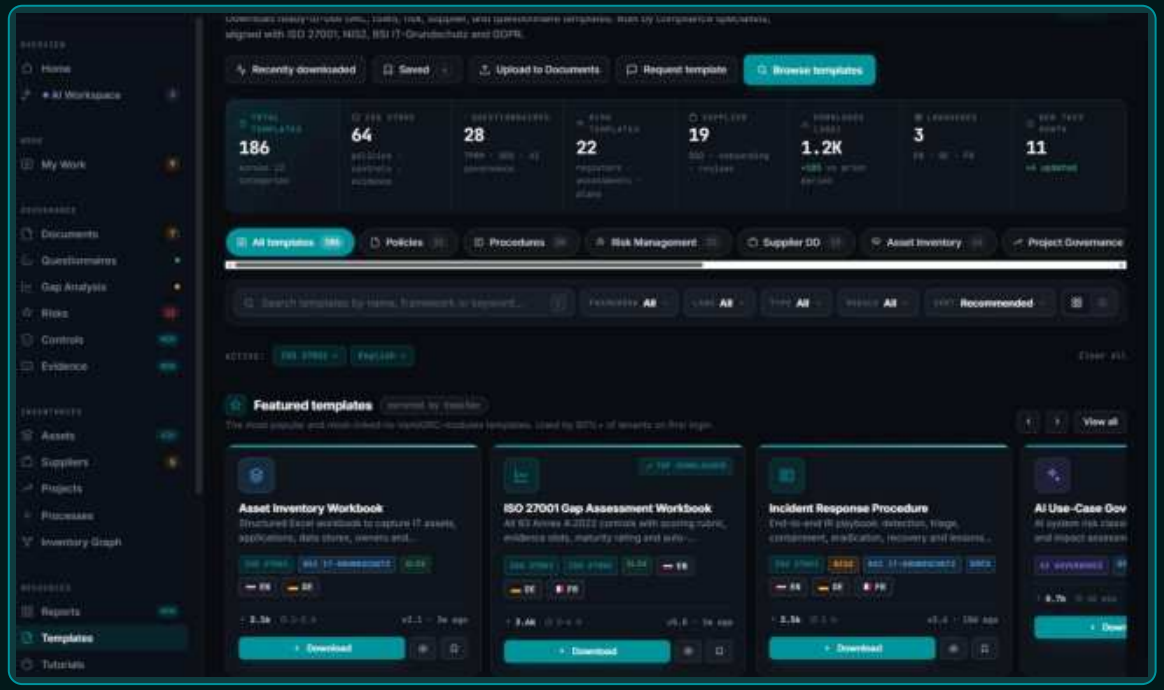
  Richtlinien · SOPs · Statement of Applicability · Risikomanagement · Rollen & Stakeholder · Assets & BIA…

- **Abdeckung pro Kategorie nachverfolgt**

  Live-Abdeckung in % · Trend-Deltas · Anzahl in Prüfung — gekennzeichnet, wenn Aufmerksamkeit nötig.

Vorlagenbibliothek — 186 einsatzbereite, framework-getaggte Vorlagen.

Policies · Arbeitsanweisungen · Risiko · Lieferanten · Fragebögen — erstellt von Compliance-Spezialisten. Ausgerichtet an ISO 27001, NIS2, BSI IT-Grundschutz und DSGVO. Drei Sprachen.



WARUM DAS ZÄHLT

- **Von 80 %+ beim ersten Login genutzt**

  Asset-Inventar-Workbook · ISO-27001-Gap-Workbook · Incident Response · KI-Use-Case-Governance.

- **Filter: Framework · Sprache · Typ**

  ISO 27001 · NIS2 · BSI Grundschutz · DOCX · XLSX · DOCX · EN · DE · FR — gespeicherte Filter.

- **11 neu in diesem Monat · +4 aktualisiert**

  Kuratiert von VamiSec · Download-Statistiken · Versionskontrolle · Kanal für Vorlagenanfragen.

Business Continuity by Design.

BIA-getriebenes Recovery, end-to-end (ISO 22301).

- → BIA-getriebenes Recovery: MTPD · RTO · RPO
- → BCP- & DR-Pläne · Krisen-War-Room · Tabletop-Kalender
- → ISO-22301-Controls · DORA Kapitel V · NIS2-Meldefristen
- → 42 BIA-Prozesse auf Assets und Risiken gemappt
- → DORA-TLPT-Replay-Tooling integriert

Produkt-Security-Lifecycle — CSMS end-to-end umgesetzt.

IEC 62443 · CRA · ISO 21434 · MDR · SaMD. Sieben Phasen von Secure-by-Design bis End-of-Life — orchestriert von 12 spezialisierten KI-Agenten.

0	1	2	3	4	5	6
Governance	**Secure by Design**	**Sichere Entwicklung**	**Verifizieren · Validieren**	**Release**	**Post-Market**	**EoL**
CSMS-Policy	Threat Model · Anforderungen	SAST · DAST · SCA	Pentest · Fuzz · Review	SBOM · Signierung · Supply	PSIRT · CVD · Monitor	Sunset · CRA Art. 13(8)

SBOM · xBOM · PSIRT

- CycloneDX- & SPDX-Generierung pro Release
- Kontinuierliches Re-Scanning verwundbarer Komponenten
- VEX-Statements für betroffen / nicht betroffen
- PSIRT-Triage · CVSS · CRA-Art.-14-Meldungen
- Coordinated-Vulnerability-Disclosure-Portal

FRAMEWORK-ABDECKUNG · EIN PRODUKT, VIELE PFLICHTEN

IEC 62443	*Industrie · OT*
EU CRA	*Produkte mit digitalen Elementen*
ISO 21434	*Automotive-Cybersicherheit*
MDR · SaMD	*Medizinprodukte · IEC 81001-5-1*
NIST SSDF	*Secure-Software-Development-Framework*

BCMS-Lens — ISO 22301 in Bewegung.

Business Continuity als First-Class-Citizen — RTO/RPO über jeden Prozess · Recovery-Standorte · Tabletops.

Agentische Lieferanten-Intelligenz.

Lieferketten-Sicherheit auf Autopilot — von OSINT und Security Ratings bis zum AVV-Management.

OSINT & Trust Center

Domains, ASM, Security Ratings (BitSight, SecurityScorecard, CybelAngel) — automatische externe Sicht.

Fragebogen-Automatisierung

Eingehende Fragebögen werden per KI mit Ihrem ISMS abgeglichen. Konsistente, nachweisbasierte Antworten in Minuten.

NDA · AVV · Verträge

Lieferantenspezifisches Dokumentenmanagement. DSGVO-Art.-28-Tracking. Ablauf- & Erneuerungsbenachrichtigungen.

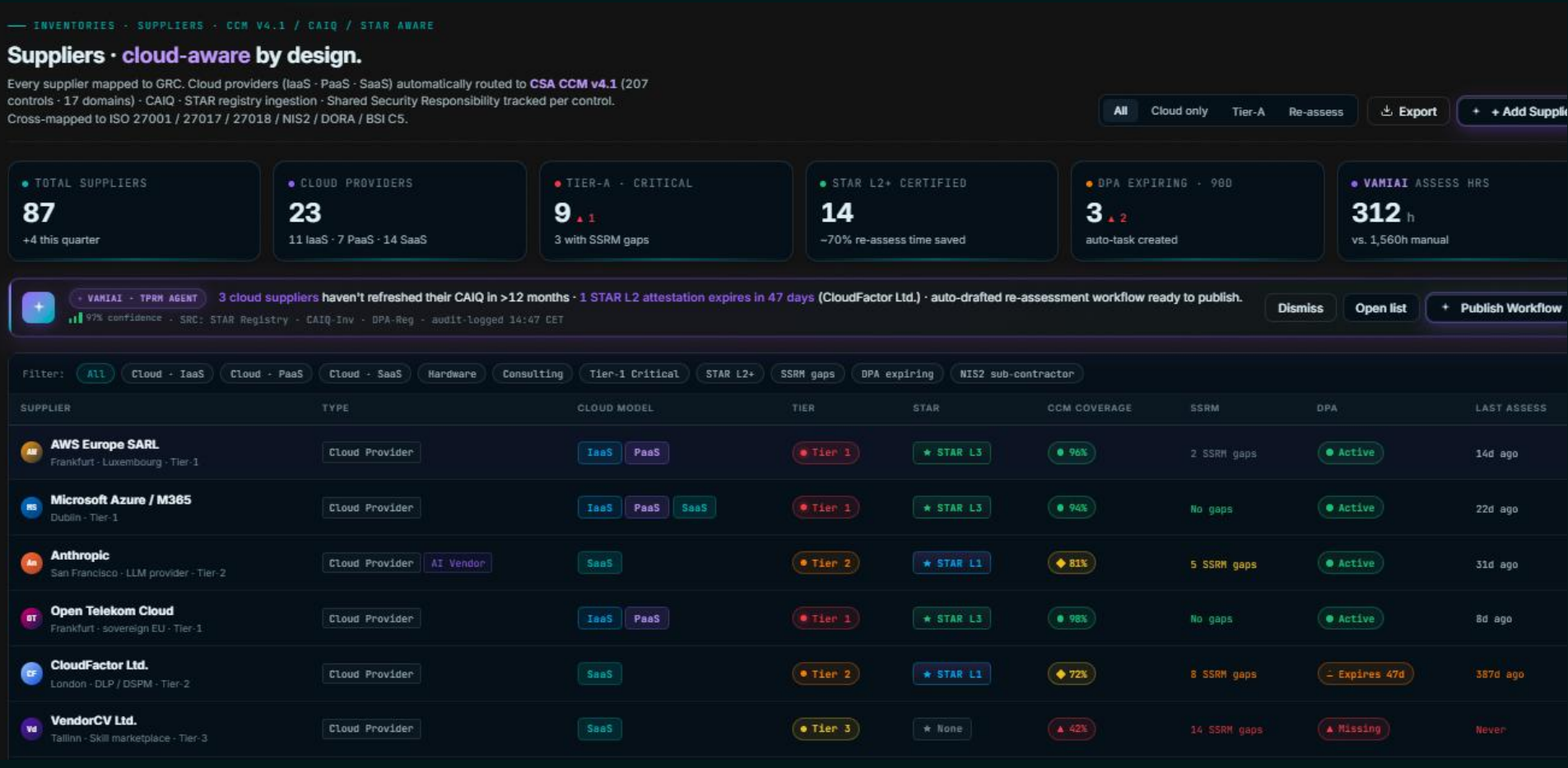
Risikobewertungen

Strukturiert nach NIS2 Art. 21(2)(d). Priorisierte Findings, Maßnahmen, auditbereite PDF/Excel-Berichte.

LIEFERANTEN-ASSESSMENT-WORKFLOW

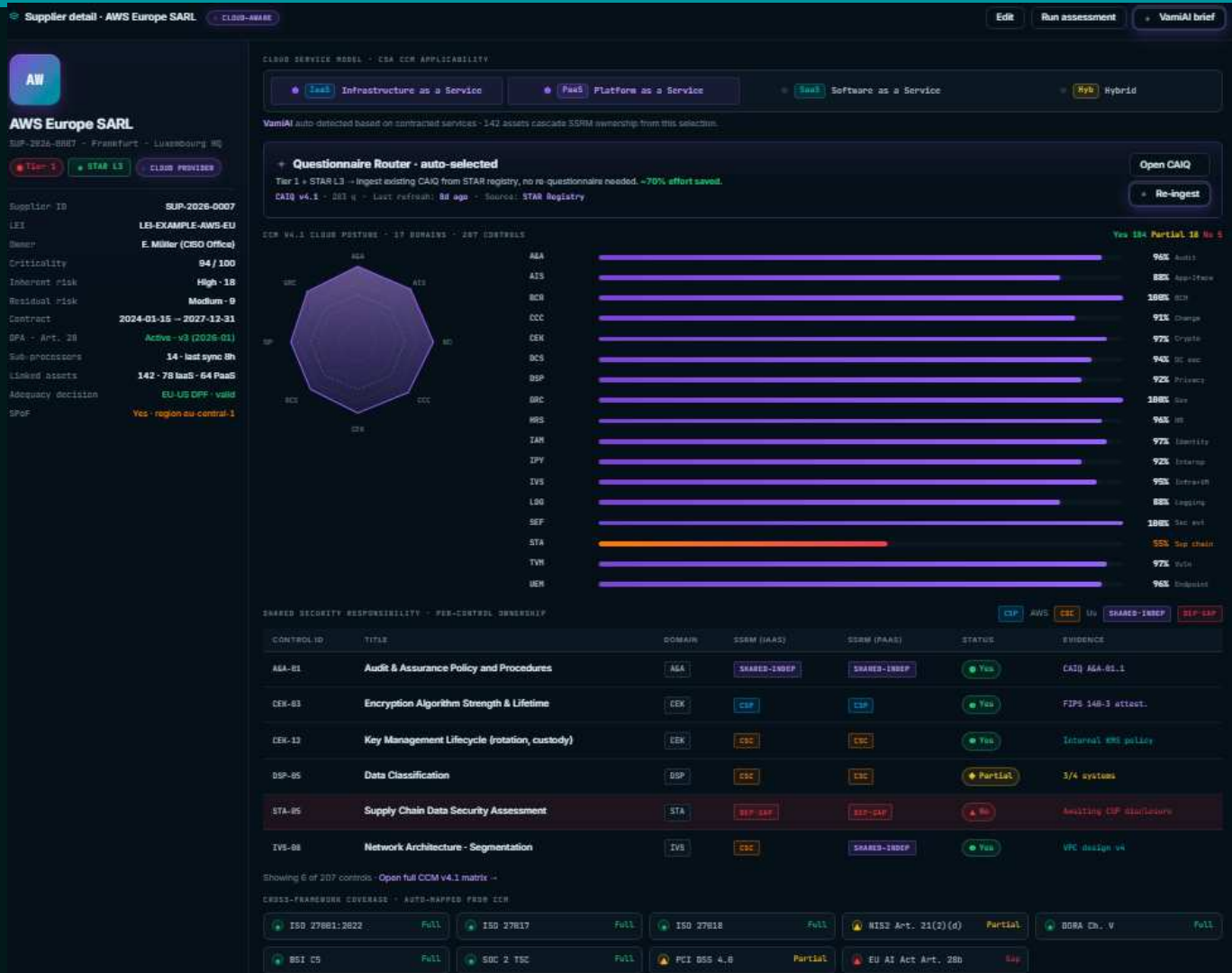
1. Anlegen oder importieren
2. OSINT & Rating
3. Fragebogen
4. Gap-Analyse
5. AVV / NDA
6. Audit-Bericht

Agentische Lieferanten-Intelligenz.



Automatisierte Lieferanten-Assessments.

Lieferketten-Sicherheit auf Autopilot — von OSINT, Fragebögen, CSA-STAR-DB und Security Ratings bis zum AVV-Management.

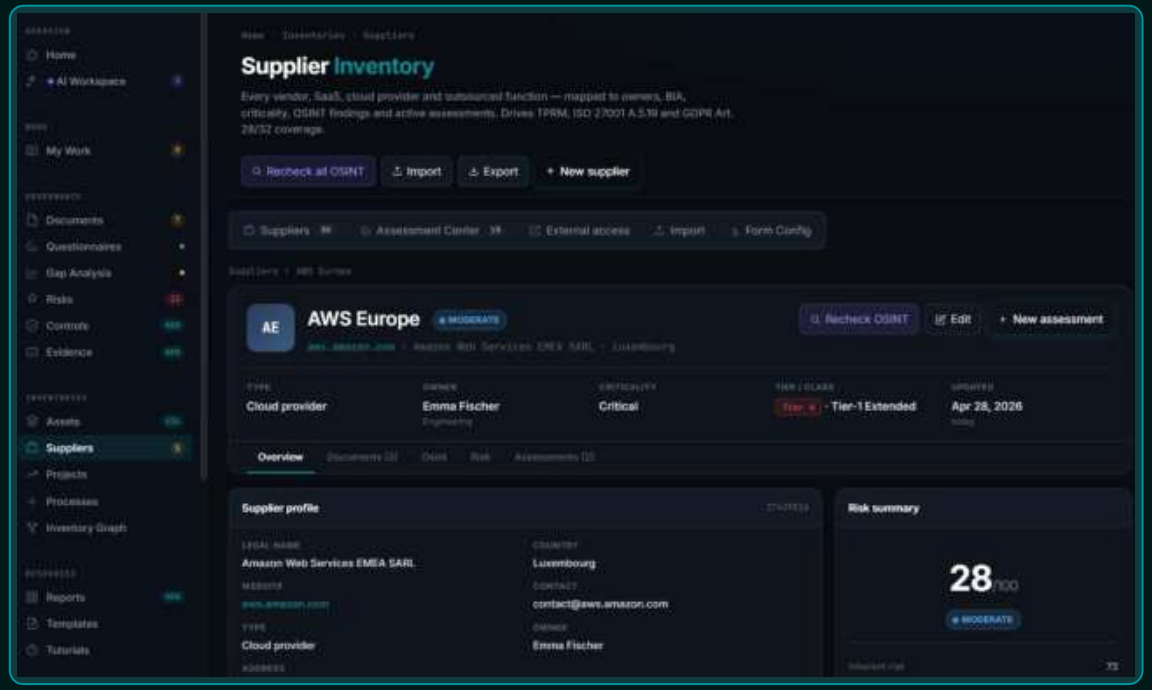


Software-Third-Party-Risiko — xBOM-nativ.

87 aktive Lieferanten · 412 CycloneDX 1.6 eingelesen · 6 Lieferanten-Sub-Agenten auf Streife · STAR-Registry-Sync.

Lieferanten-Inventar — jeder Anbieter abgebildet, bewertet und nachverfolgt.

Jeder Anbieter, SaaS, Cloud-Provider und ausgelagerte Funktion — gemappt auf Owner, BIA, Kritikalität, OSINT-Findings und aktive Assessments. Treibt TPRM, ISO 27001 A.5.19 und DSGVO Art. 28/32.



WARUM DAS ZÄHLT

- **360°-Sicht je Lieferant**

  AWS Europe · Kritisch · Tier-A · Cloud-Provider — Owner, Land, Kontakt, Adresse, Klassifikation.

- **Risiko-Score sichtbar**

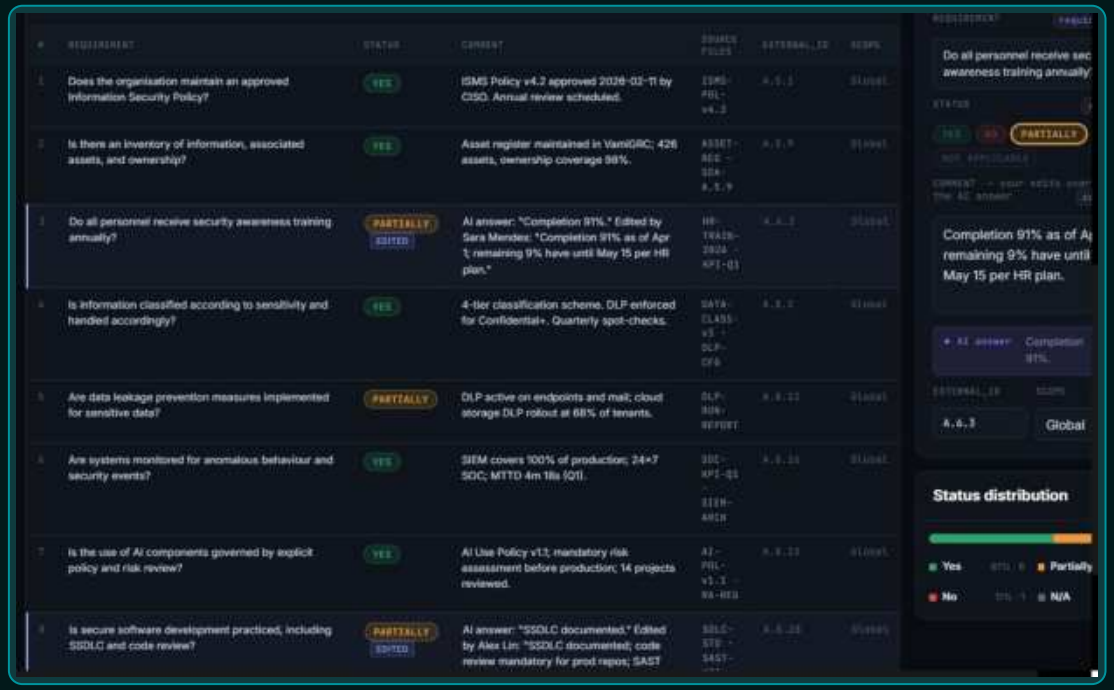
  28/100 · Moderat · inhärent vs. Rest — OSINT per Klick neu prüfen.

- **Reiter: Dokumente · OSINT · Risiko**

  Reiteransicht jeder Lieferanteninteraktion — vergangene Assessments und Findings stets zugänglich.

KI-Fragebogen-Review — Minuten statt Tage.

Eingehende oder ausgehende Sicherheitsfragebögen, KI-vorbeantwortet aus Ihrem ISMS — mit Status, Kommentar, Quelldateien, Framework-Referenz und Scope pro Zeile. Bearbeiten, überschreiben, sperren.



WARUM DAS ZÄHLT

- **KI-erstellt, dort bearbeitet, wo nötig**

  „Fertigstellung 91 %." bearbeitet von Sara Mendes — ursprüngliche KI-Antwort mit Audit-Trail erhalten.

- **Quelldateien pro Zeile zitiert**

  ISMS-POL-v4.2 · ASSET-REG · DLP-CFG — jede Aussage referenziert die Quelle zurück.

- **Statusverteilung live**

  Ja 61 % · Teilweise 25 % · Nein 11 % · n. z. — Vollständigkeit %, Scope und externe IDs auf einen Blick.

CSA · Cloud Controls Matrix v4.1 · Live-Walkthrough.

VamiAI parst jede Frage, fragt Ihr Dokumentenmanagement ab, wählt den korrekten Status, zitiert die Quelle — in Sekunden. 200+ Fragen = 2 Tage → <5 Min.

vamigrc.app — CCM-v4.1 · Audit & Assurance · 6 Fragen — VamiAI · BEANTWORTET

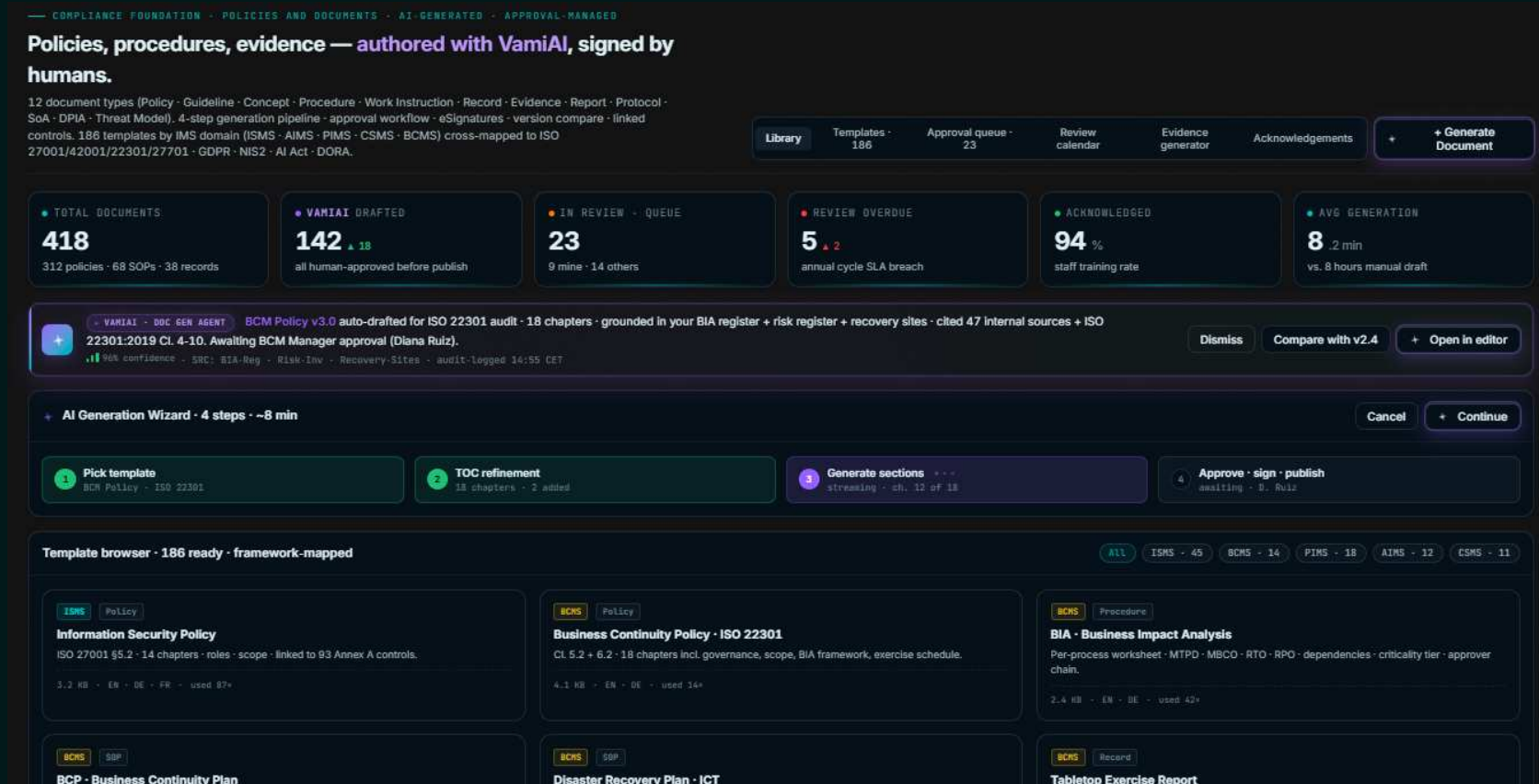
ID	FRAGE	STATUS	CONF.	NACHWEIS
A&A-01.1	Sind Audit- und Assurance-Policies etabliert, dokumentiert, freigegeben und gepflegt?	VOLL	98 %	→ *ISMS-POL-001 · §4.2*
A&A-01.2	Werden Policies mindestens jährlich oder bei wesentlichen Änderungen geprüft und aktualisiert?	VOLL	95 %	→ *Mgmt-Review-2024-Q4*
A&A-02.1	Werden mindestens jährlich unabhängige Audit-Assessments durchgeführt?	VOLL	99 %	→ *ISO-27001-Zert · TÜV Süd*
A&A-05.1	Ist ein Audit-Management-Prozess für Planung, Risikoanalyse und Behebung definiert?	TEILWEISE	91 %	→ *Audit-Proc-002 · Excel*
A&A-06.1	Existiert ein risikobasierter Korrekturmaßnahmenplan und wird er auf Audit-Findings angewendet?	GEPLANT	87 %	→ *Roadmap-2025-Q1 · ETA März*
A&A-04.1	Wird Compliance gegen alle relevanten Standards, Regulierungen und vertraglichen Anforderungen verifiziert?	VOLL	96 %	→ *Legal-Reg-2024 · DSGVO/NIS2*

ERGEBNIS · CCM A&A · 6 von 6 beantwortet · bereit zur Prüfung durch Compliance-Officer

4 VOLL	1 TEILWEISE	1 GEPLANT	0 LÜCKE

VamiGRC kennt alle Ihre Policies und Verfahrensanweisungen

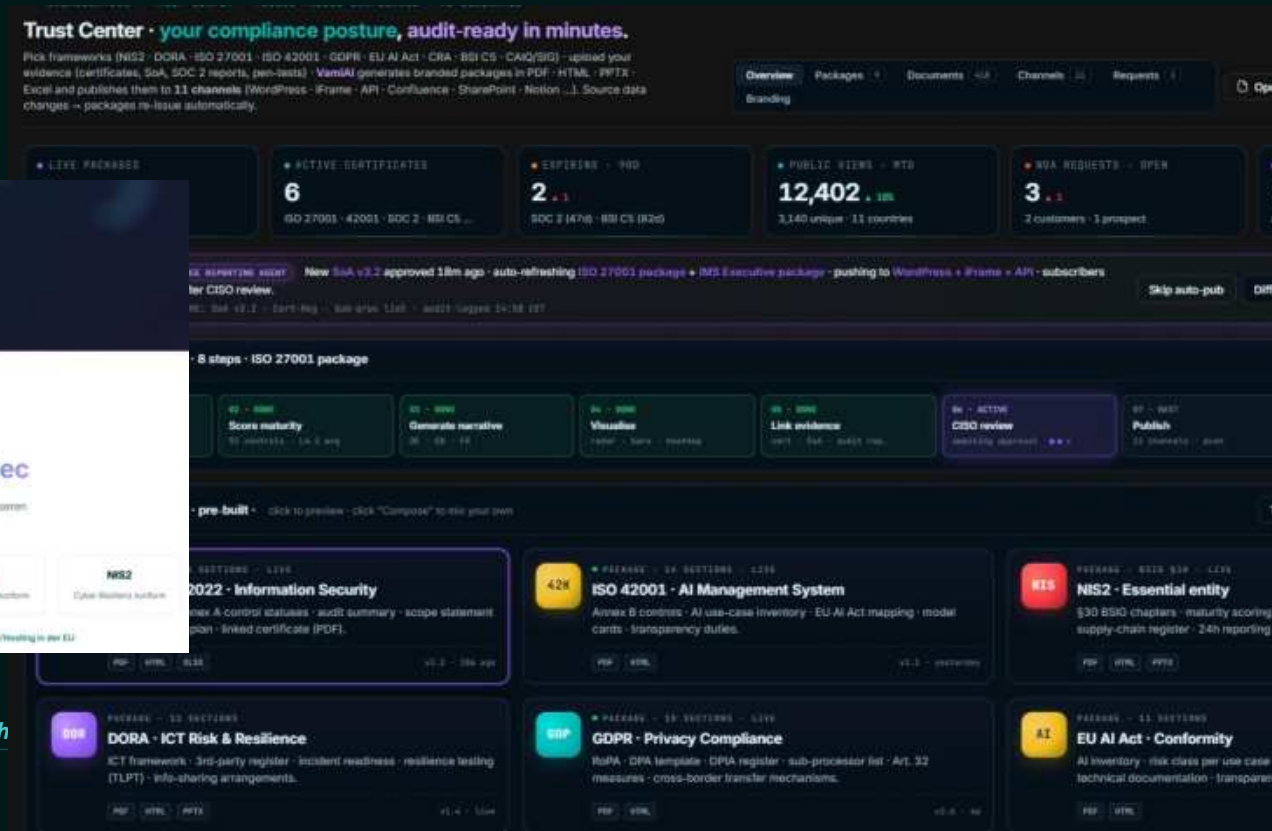
KI-generiertes HTML · mehrsprachig (DE · EN · FR) · tiefe WordPress-Integration · auditbereite Compliance-Pakete auf Knopfdruck.



Trust Center · Compliance-Pakete für Ihr IMS.

KI-generiert. Mehrsprachig (DE · EN · FR). Quelldaten ändern sich → Narrative werden neu erzeugt → Pakete neu ausgestellt → Trust Center neu veröffentlicht — ohne dass jemand ein Word-Dokument anfasst.

https://vamisec.com/de/trust-center



Dort, wo Ihre Teams bereits arbeiten.

ROADMAP

Volle Funktionsparität in Teams, Slack, E-Mail, Mobile, Browser und API.

Microsoft Teams

@VamiAI in Kanälen · Adaptive Cards · Meeting-Intel

Slack

/vami-Befehle · Block Kit · Incident-War-Rooms

E-Mail

Mandantenadresse · weitergeleitete RFIs · Dokumenten-Intake

Mobile (iOS/Android)

Voice-First · Push-Freigaben · Offline-Entwürfe

Browser-Erweiterung

Kontext auf jeder Seite · Regulator- & Anbieter-Websites

API · Webhooks · MCP

Jede Funktion programmatisch · KI-zu-KI-Interoperabilität

Compliance im Fluss des Geschäfts — nicht erst, wenn jemand das GRC-Tool öffnet.

Wählen Sie Ihr LLM. Bewahren Sie Ihre Souveränität.

• ROADMAP

Default: Claude. Alternative: OpenAI/Azure. Souverän: Open Telekom Cloud. Oder BYOL — bringen Sie Ihr eigenes.

DEFAULT

Anthropic Claude

Beste Reasoning-Qualität.
EU-Region verfügbar.

MODELLE

Opus 4 · Sonnet 4 · Haiku 4

ALTERNATIVE

OpenAI / Azure OpenAI

MS-Stack-Organisationen.
Azure Private Endpoints.

MODELLE

GPT-4o · o3 · o4-mini

SOUVERÄN

Open Telekom Cloud

DE Nur Deutschland.
KRITIS / NIS2 / DORA.

MODELLE

Llama 3.1 · Mistral · Mixtral

BYOL

Bringen Sie Ihr eigenes LLM

On-Prem (vLLM, Ollama), Bedrock, Vertex AI.

MODELLE

Jede OpenAI-kompatible API

Mandantenkonfiguration · Modellebene pro Use Case · Auto-Routing · Graceful Fallback.

Lens-Picker — zehn rollenbasierte Sichten.

CISO · DSB · KI-Beauftragter · BCM · Einkauf · Auditor · SecOps. Gleiche Daten. Andere Realität.

03

KPI · Aufgaben · Incidents

KPI Engine · My Work · Incidents · BCM

KPI-Engine, Dashboards & Management Review.

80+ KPIs über 5 IMS-Domänen · 14 interaktive Dashboards · strukturierte ISO-9.3-Management-Reviews · Action-to-Task-Pipeline.

MANAGEMENT REVIEW · ISO 9.3

INPUTS (gemäß ISO 9.3.2)

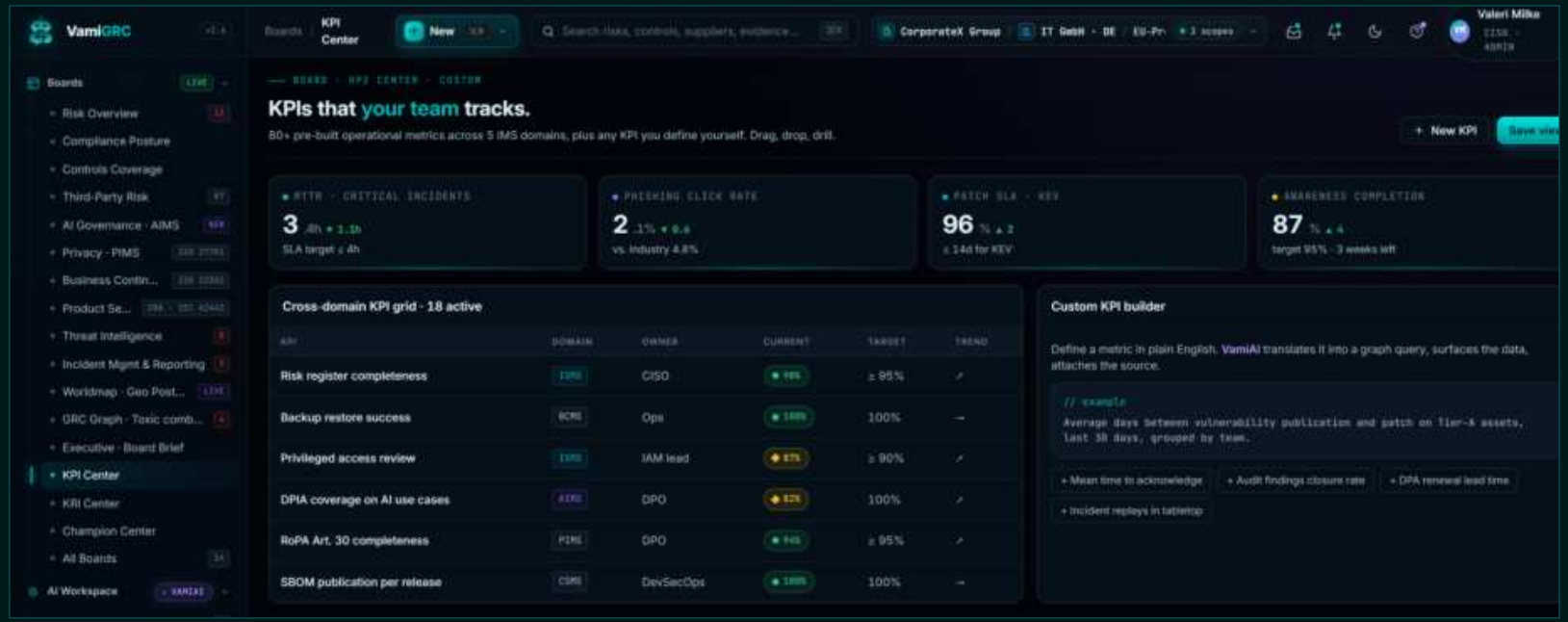
- Auditergebnisse · Finding-Trend
- Änderungen im Risikoregister · Top-Risiken
- Kundenfeedback · Beschwerden
- Prozessleistung · KPIs
- Ressourcenangemessenheit · Verbesserung

OUTPUTS (gemäß ISO 9.3.3)

- → Verbesserungsentscheidungen · CAPA
- → Ressourcenbedarf · Investitionsplan
- → Maßnahmen-Datensätze → Aufgaben (Auto-Pipe)

KPI Center — Metriken in natürlicher Sprache.

Definieren Sie eine Metrik in natürlicher Sprache. VamiAI übersetzt sie in eine Graph-Abfrage und hängt die Quelle an.



Task Management & Agentic Automation.

Mensch- + KI-Aufgaben in einer Engine. Vier Autonomie-Stufen. IMS-Jahreskalender steuert wiederkehrende Arbeit. Multi-Source-Erstellung. Jira & ServiceNow synchronisiert.

L0 Manuell

Nur Mensch-Aufgabe. Agent wird nicht tätig.

L1 Vorschlagen

Agent schlägt vor · Mensch entscheidet über die Anwendung.

L2 Ausführen · Freigeben

Agent erledigt die Arbeit · Mensch gibt vor dem Commit frei.

L3 Autonom

Agent führt innerhalb von Guardrails aus · Audit-protokolliert.

IMS-JAHRESKALENDER · WIEDERKEHRENDE AUFGABEN

Vorgeladen über ISMS · AIMS · PIMS · CSMS · BCMS.

- Governance · Policy-Reviews · MR-Zyklen
- Compliance · Rechtsregister · Pflichten
- Risiko · Register-Review · Behandlungsstatus
- BCM · BIA · BCP · DR-Testfenster
- Lieferanten · Re-Assessments · AVV-Verlängerungen
- IAM · Access-Reviews · Joiner-Leaver
- Audit · intern · Management Review

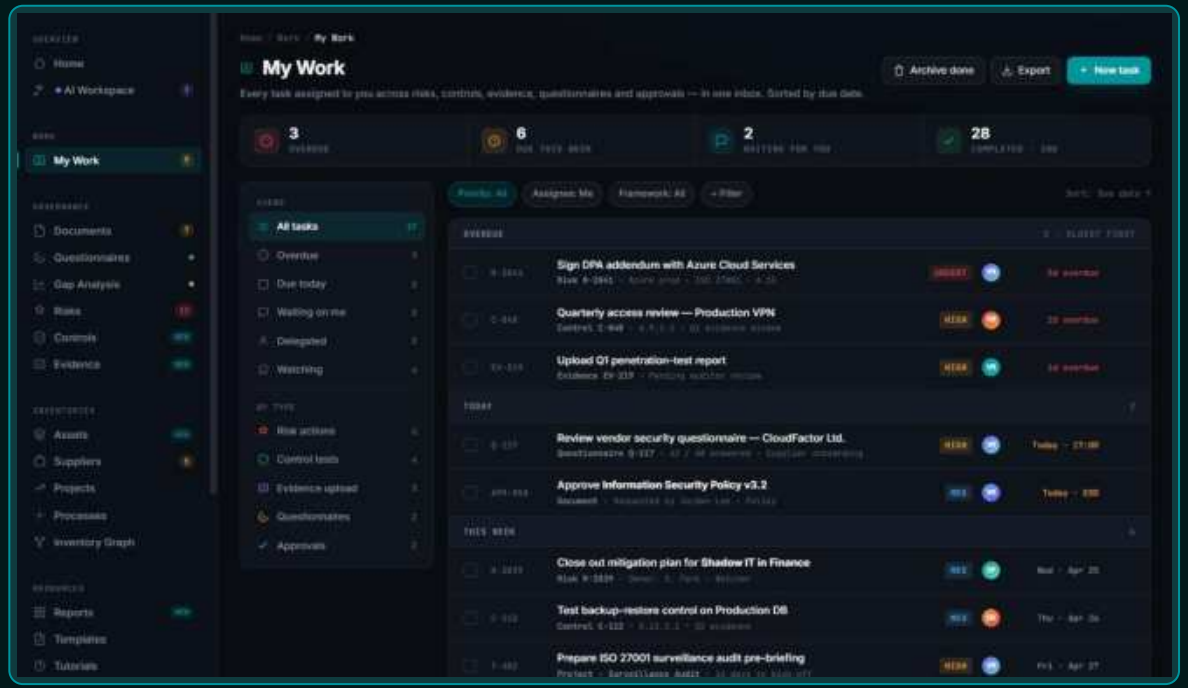
AUFGABEN-ERSTELLUNG AUS MEHREREN QUELLEN

Jedes Modul schiebt Arbeit in die gemeinsame Queue.

- Audit-Findings · Ergebnisse der Gap-Analyse
- Risikobehandlung · Incident Response
- Lieferanten-Assessments · Vertragsverlängerungen
- Schwachstellenbehebung · Least-Privilege-Findings
- → Jira / ServiceNow · Last-Write-Wins

My Work — jede Zuweisung in einer Inbox.

Jede Ihnen zugewiesene Aufgabe über Risiken, Controls, Nachweise, Fragebögen und Freigaben hinweg — sortiert nach Fälligkeit, segmentiert nach Typ und Priorität. Mensch- und KI-Aufgaben teilen dieselbe Engine.



WARUM DAS ZÄHLT

- **Drei Prioritäts-Lanes · live**

  3 überfällig · 6 fällig diese Woche · 2 wartend · 28 in den letzten 30 Tagen abgeschlossen.

- **Modulübergreifende Vereinheitlichung**

  Risiko-Aktionen · Control-Tests · Nachweis-Uploads · Fragebögen · Freigaben — in einer Queue.

- **Gefilterte Ansichten · Smart Sort**

  Priorität · Bearbeiter · Framework · Typ · Fälligkeit — gespeichert oder ad-hoc, exportierbar als CSV.

Incident Management · 6 Module + KI-Layer.

Wenn etwas bricht, läuft die Uhr. NIS2 24 h · DSGVO 72 h · DORA · CRA Art. 14 · AI Act — jede Uhr startet automatisch. 15+ Playbooks · 3 Eskalationsstufen · KI-unterstützt.

NIS2 · 24 h | DORA | DSGVO · 72 h | CRA Art. 14 | AI Act

01 IncidentEngine

CRUD · Lifecycle · State Machine · Audit-Log. Single Source of Truth von der Erkennung bis zum Abschluss.

REST API · Webhook

02 EscalationEngine

Regelbasierte Auto-Eskalation · On-Call-Rotation · SLA-Tracking. 3 Stufen mit Override-Pfaden.

Event-getrieben

03 PlaybookEngine

15+ vorgefertigte Playbooks: Ransomware · Data Exfil · DDoS · Lieferanten-Breach · KI-Missbrauch. KI erzeugt individuelle bei Bedarf.

REST API · KI-generiert

04 RegulatoryEngine

Erkennt Meldepflichten automatisch über NIS2 · DORA · CRA · AI Act · DSGVO. Verwaltet Fristen. BSI-API-Export.

REST API · BSI-API

05 NotificationEngine

Kunden- / Partner-Benachrichtigungen über mehrere Kanäle. Pflichten werden aus den vertraglichen Anforderungen gezogen. SLA-getrackt.

E-Mail · Portal · ServiceNow

06 TabletopEngine

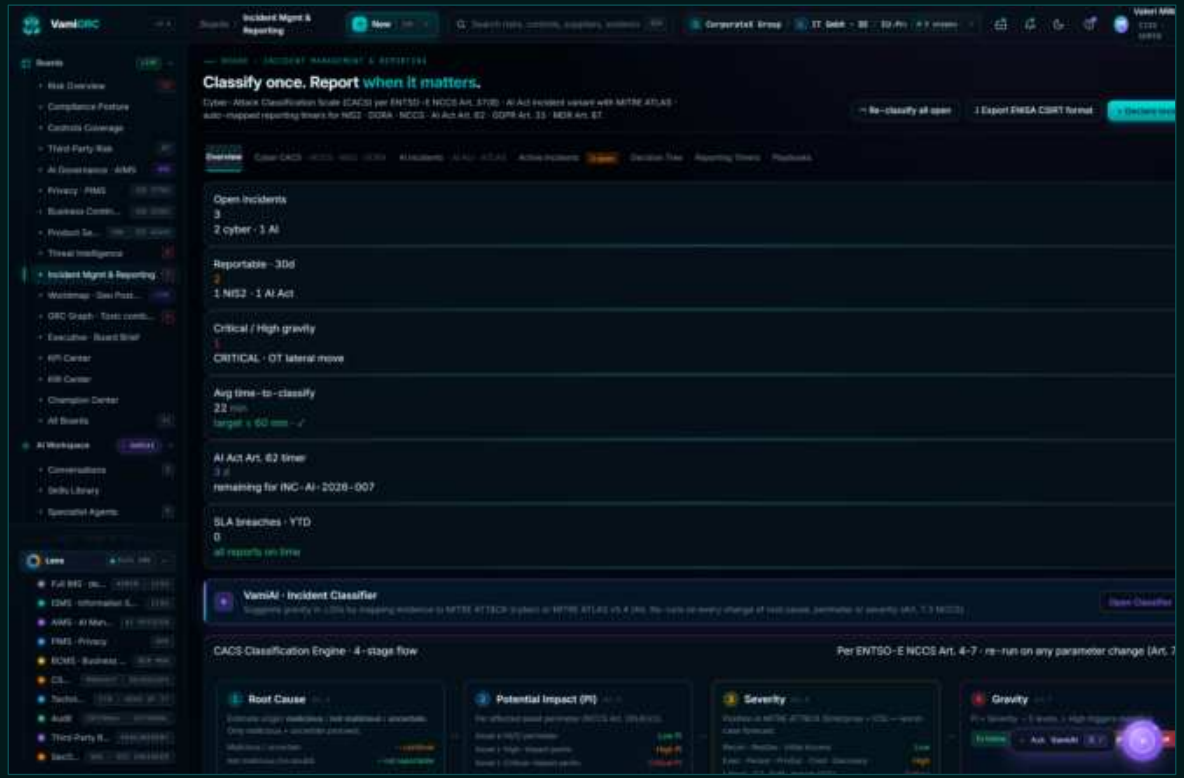
Tabletop-Übungen planen, durchführen und dokumentieren. Auto-Evaluation gegen Playbook-Konformität. ISO 22301 §8.5 Nachweis.

REST API

Eine Incident Engine · eine BCM Engine · eine DRP Engine · ein Graph. Einmal testen → ISO 22301, NIS2 BCM und DORA erfüllen.

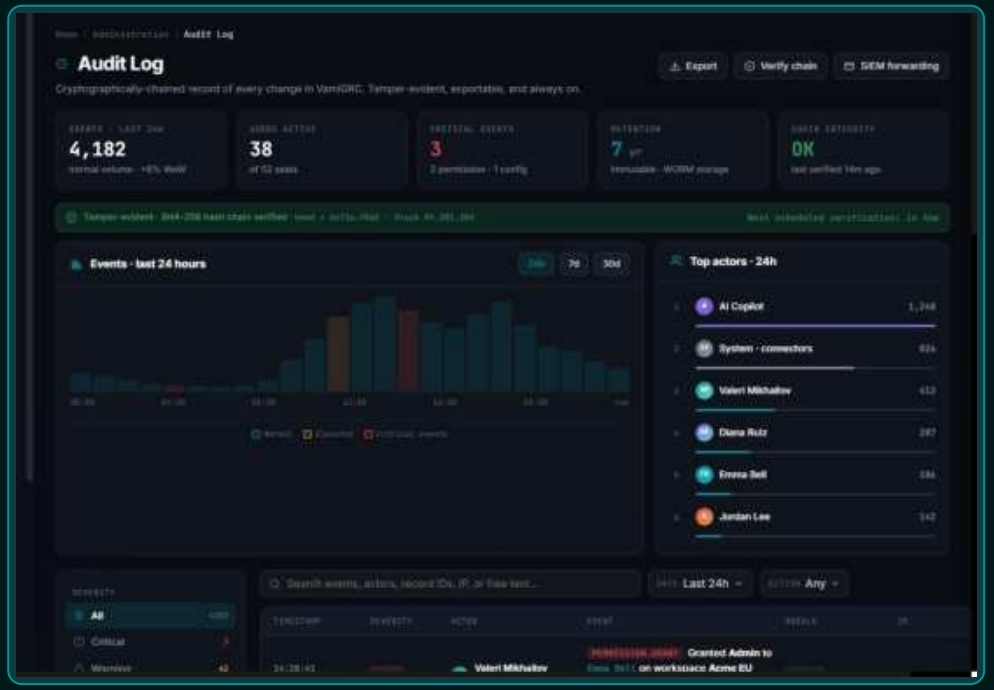
CACS-basiertes Incident Management und Reporting.

Offene Incidents werden automatisch auf NIS2 · DORA · NCCS · AI Act · DSGVO · MDR · CRA gemappt. Ein Timer-Panel. Alle Uhren.



Immutable Audit Log — manipulationssicher, immer aktiv.

Kryptografisch verkettete Aufzeichnung jeder Änderung in VamiGRC. SHA-256-Hash-Chain · WORM-Speicher · 7 Jahre Aufbewahrung · SIEM-Forwarding · regulatorisch geeigneter Export.



WARUM DAS ZÄHLT

- **Chain-Integrität: OK**

  Zuletzt vor 14 Min. verifiziert · Block #4.281.204 · nächste geplante Verifizierung in 46 Min.

- **4.182 Events / 24 h · normal**

  +6 % WoW · 3 kritische Events · 38 aktive Nutzer — Anomalieerkennung standardmäßig an.

- **Top-Akteure · Top-Module**

  KI-Copilot · System-Konnektoren · benannte Nutzer — jedes Event mit Zeitstempel, Schweregrad, IP.

Security & Trust — gebaut für regulierte Branchen.

Deutsche Cloud · Zero-Trust-Isolation · Auditierbarkeit · Zertifizierte Expertise.

Deutsche Cloud · Open Telekom Cloud

- Daten ausschließlich in deutschen Rechenzentren
- DSGVO Art. 44+ — keine Drittlandtransfers
- Infrastruktur von T-Systems / Deutsche Telekom
- ISO-27001-zertifizierter Cloud-Anbieter

Tenant-Isolation & Zero Trust

- Strikte Datentrennung zwischen Mandanten
- Keycloak-JWT-Validierung & Rollendurchsetzung
- Kein mandantenübergreifender Zugriff by Design
- Dedizierte Namespaces für Dokumente & Indizes

Compliance & Auditierbarkeit

- Vollständiger, unveränderlicher Audit-Trail
- Nachweisbasierte Antworten mit Quellenangaben
- Exportierbare Berichte & signierte Downloads
- DSGVO-Art.-32-Logging-Richtlinien

Zertifizierungen & Expertise

- ISO 27001- & ISO 42001-Lead-Auditoren
- AI-Act-konformer Systembetrieb
- BSIG-§8a-Kompetenz
- EU AI Act — KI-System mit begrenztem Risiko

VamiGRC vs. traditionelle GRC-Tools — ein struktureller Unterschied.

Kein Feature-Vergleich. Ein Kategorienwechsel.

Capability	Traditionelle GRC-Tools	VamiGRC
KI-native Automatisierung	*Nein / nur assistierend*	✓ Vollständig agentisch
Multi-Framework in einem System	*Selten; oft Add-on*	✓ ISMS · AIMS · PIMS · CSMS · BCMS
Risikoregister auf einen Prompt	*Nein — manuell*	✓ Vollautomatisiert in Minuten
Agentisches Lieferanten-Assessment	*Nein*	✓ OSINT + Fragebogen auf Autopilot
Deutsche Cloud / DSGVO-konform	*Oft US-basiert*	✓ Open Telekom Cloud, deutsche Rechenzentren
Nachweisbasierte KI-Antworten	*Nein*	✓ Gestützt auf Ihre ISMS-Dokumente
Lens-Funktion (rollenoptimiert)	*Nein*	✓ 9 rollenspezifische Workspaces
Preis-Leistung im Mittelstand	*Oft >50.000 €/Jahr*	✓ Skalierbar ab Mittelstand aufwärts

VamiGRC × Claude-Ökosystem.

ROADMAP

Das GRC-Rückgrat für jeden Claude-Nutzer im Unternehmen — kein Kontextwechsel, keine eigenen Konnektor-Entwicklungen.

1 VamiGRC ALS MCP-SERVER

Externe Claude-Instanzen lesen/schreiben in VamiGRC — in Chrome, Code, Desktop, Excel, Cowork.

2 VamiGRC ALS MCP-CLIENT

Interne VamiAI-Agenten nutzen externe MCP-Server — Wiz, GitHub, Microsoft, SAP, BSI.

3 Claude-native UX-Patterns

Skills, Slash-Befehle, Tool Use, Artifacts — dieselbe Experience wie in jedem anderen Claude-Workflow.

7 CLAUDE-OBERFLÄCHEN · EIN VERTEILTES KI-FABRIC

C	C	C	C	C	C	C
Claude.ai	**Chrome**	**Claude Code**	**Excel**	**Cowork**	**API**	**Skills**
Web · Desktop · Mobile	Agentisches Browser-Plugin	Terminal-Coding-Agent	Spreadsheet-Agent	Desktop-Datei-/E-Mail-Agent	Programmatisch & Batch	Wiederverwendbare Anweisungen

Browser-Plugin + Skills-Bibliothek — Claude lernt GRC.

ROADMAP

Aus jedem Tool erfassen · einmal installieren, GRC-Capability überall.

BROWSER-PLUGIN · ERFASSEN VON ÜBERALL

SAP LeanIX	→ 47 VamiGRC-Assets gemappt
Wiz Findings	→ 8 kritische Risiken in 11 s
BSI Advisory	→ Rechtsregister + Impact
Microsoft Trust	→ Lieferant + 2 Zertifizierungen
ServiceNow	→ Incident + NIS2-/DSGVO-Aufgaben

SKILLS-BIBLIOTHEK · IM GESAMTEN CLAUDE-ÖKOSYSTEM INSTALLIERBAR

- `vamigrc-risk-analysis`
- `vamigrc-audit-finding`
- `vamigrc-regulation-classifier`
- `vamigrc-control-mapper`
- `vamigrc-pentest-interpreter`
- `vamigrc-incident-classifier`
- `vamigrc-vendor-questionnaire`
- `vamigrc-evidence-packager`

MCP-nativ bedeutet: Jedes neue Tool im Claude-Ökosystem wird integrierbar — ohne eigene Entwicklung.

TEIL II

GRC as a Service.

Umfassende IT-Security- und Compliance-Sicherheit mit VamiGRC.

Wir lizenzieren Ihnen nicht nur die Plattform — wir betreiben sie für Sie.

Virtual CISO · kontinuierliches Monitoring · Audit-Vorbereitung · Incident Response · Managed-Pentest-Zyklen · Beantwortung von Kunden-Due-Diligences — mit VamiGRC als Betriebssystem.

Compliance is an ongoing management responsibility — regulatory and contractual requirements evolve continuously.

REGULATIONS & FRAMEWORKS

- NIS2
- DORA
- EU AI Act
- CRA
- ISO/IEC 27001
- ISO/IEC 42001
- ISO 22301
- CSMS-Standards

GRC as a Service

Powered by VamiGRC
AI-native GRC Solution

1. Gap Analysis & Baseline Assessment
2. Roadmap & Prioritization
3. Implementation Support & Evidence Management
4. Continuous Monitoring, Reporting & Improvement

ADDITIONAL SERVICES

- External CISO
- External AI / AI Officer
- Policy & Process Design
- Risk Assessments & Technical Measures

MANAGEMENT BENEFITS

- Continuous Compliance
- Clear Management Transparency
- Reduced Audit Effort
- Scalable for New Regulations
- Audit-Ready at Any Time

Compliance is not completed once — it is continuously managed.

Modular Expert Roles for GRC as a Service

vCISO, vAI Officer, vDPO and vCSIRT/vPSIRT for Governance, Compliance, Data Protection and Incident Readiness

Powered by VamiGRC – AI-native GRC Solution

vCISO

- Security Strategy & Governance
- ISMS Management & Risk Management
- Management Reporting & Board Sparring
- Coordination of Measures & Service Providers

vAI Officer

- AI Governance & EU AI Act
- Use Case Classification & Gap Analyses
- Secure AI Usage & Control Framework
- Policies, Role Model & Evidence

vDPO

- Data Protection Governance & GDPR
- TOMs, Records of Processing & DPIA
- Data Subject Rights & Incident Support
- Advisory, Training & Data Processing Agreements

vCSIRT / vPSIRT

- Incident Readiness & Playbooks
- Triage, Coordination & Crisis Support
- Vulnerability Disclosure & Product Security
- Lessons Learned & CAPA Management

Shared Delivery Elements

- Governance & Policies
- Risk & Action Management
- Evidence Management in VamiGRC
- Reporting, KPIs & Steering
- Audit & Assurance Readiness

Modular and scalable | Close to management | Audit-oriented

Flexible engagement model – as an interim function, co-managed service or strategic support.

04

Business · Roadmap · Trust

GRCaaS · Partner · ROI · Roadmap

Drei Delivery-Modelle. Eine Plattform. Dieselben Daten.

Von der Self-Service-Lizenz bis zum Fully-Managed — Ihr Engagement, Ihre Kadenz, Ihr Scope.

TIER 1

Plattform

Self-Service

VamiGRC SaaS. Ihr Team betreibt. Wir liefern Updates, Support, Schulungen.

- Multi-Tenant-SaaS
- Standard-SLAs
- Onboarding in 4 Wochen
- Ideal für: interne GRC-Teams

TIER 2

Co-Managed

Hybridbetrieb

Ihr Team + unsere Experten teilen sich die Plattform. Wir übernehmen, wofür Ihnen die Zeit fehlt.

- Geteilter Workspace
- Quartalsweise Business Reviews
- Benannter Delivery-Lead
- Ideal für: schlanke Security-Teams

TIER 3

Fully Managed

GRC-as-a-Service

VamiSec betreibt Ihr IT-Security- & Compliance-Programm Ende-zu-Ende auf VamiGRC.

- Dedizierter vCISO
- Alle 6 Service-Säulen
- Monatliches Vorstands-Reporting
- Ideal für: KMU · reguliert · KRITIS

Partnerprogramm — betreiben Sie VamiGRC für Ihre Kunden.

Drei Partnerstufen für Beratungen, MSSPs und Systemintegratoren. Wir liefern Plattform und Methodik. Sie besitzen die Kundenbeziehung.

TIER 1

Referral

Lead-Sharing

Senden Sie qualifizierte Leads an VamiSec. Erhalten Sie eine Referral-Gebühr bei abgeschlossenen Deals. Co-Marketing-Materialien inklusive.

- Gebrandetes Co-Marketing-Kit
- Referral-Gebühr bei Abschluss
- Quartalsweise Enablement-Sessions
- Ideal für: GRC-Beratungen

TIER 2

Implementierung

Co-Delivery

Zertifizierte VamiGRC-Berater auf Ihrer Bench. Gemeinsame Lieferung von Audits, Gap-Analysen, ISMS-Rollouts. Geteilte Marge.

- Bench mit zertifizierten Beratern
- Gemeinsames Delivery-Modell
- Umsatzbeteiligung bei Services
- Ideal für: Boutique-Auditfirmen

TIER 3

MSSP

Run-as-Your-Service

Tenant pro Kunde. Ihr Service, unser Rückgrat. Komplettes VamiGRC-Fabric.

- Isolierter Mandant pro Kunde
- Voller Zugriff auf das VamiGRC-Fabric
- vCISO-Backbone optional
- Ideal für: MSSPs · große Integratoren

Messbarer ROI. Sofort realisierbar.

Harte Zahlen aus den vier Bereichen, in denen GRC traditionell Zeit und Qualität verliert.

80–95%

Reduktion der manuellen Compliance-Arbeit

Echtzeit

Time-to-Report vs. 2–5 Tage manuell

>95 %

Konsistenz bei Sicherheitsfragebögen

ISMS-Teams & CISOs

- Keine manuellen Gap-Analysen mehr
- Fragebögen in Minuten statt Tagen
- Audit-Vorbereitung automatisiert

Management & Vorstand

- Priorisierte Risiken auf Knopfdruck
- Compliance-Dashboard in Echtzeit
- Executive Reporting automatisiert

Fachbereiche

- ISMS-Fragen eigenständig beantwortet
- Kein Warten auf den CISO für Policy-Infos
- Awareness ohne Schulungs-Overhead

Lieferantenmanagement

- Assessments auf Autopilot
- AVV / NDA digital verwaltet
- Lieferketten-Sicherheit im großen Maßstab

Von Zahlen zu Ergebnissen — ein Reality-Check für den Mittelstand.

Kennzahlen · 1.200 Mitarbeitende · 87 Lieferanten · 23 KI-Use-Cases · NIS2 im Scope · TISAX-zertifiziert.

14→2

FTE-Wochen → Tage
NIS2-Audit-Vorbereitung

87

Lieferanten neu bewertet
5 Tage statt 6 Monate

340 k €

Jährliche FTE-Einsparung
vs. manuelle Baseline

4×

Audit-Zyklen / Jahr
ohne Personalaufbau

Audit-Vorbereitung

- 14 FTE-Wochen → 2 FTE-Tage
- NIS2 + ISO 27001 + TISAX in einem Durchgang
- Auditor-Portal · Live-Nachweise

Lieferanten-Onboarding

- OSINT-Scan · Fragebogen · AVV
- 3 Stunden pro Lieferant (vorher 2 Wochen)
- AVV-Ablauf automatisch nachverfolgt

Beantwortung Kunden-DD

- CAIQ/SIG in 4 Stunden beantwortet
- >95 % Antwortkonsistenz
- Gebrandetes Trust Center automatisch veröffentlicht

Risikoregister

- 1.200 Mitarbeitende an 1 Tag erfasst
- ISO 31000- + 27005-konform
- Mitigationsplan automatisch erzeugt

Schluss mit Swivel-Chairing.

Beginnen Sie GRC zu automatisieren – van

Bonn, Deutschland · valeri.milke@vamisec.com

Ihr Ansprechpartner für intelligente GRC-Architektur

Wir freuen uns auf eine erfolgreiche Zusammenarbeit

Valeri Milke
CEO

- 15 Jahre Erfahrung in IT-Sicherheit & Compliance, CISO, Application Security, Pentesting, ISMS und Incident Response & Forensik
- Lead Auditor **(ISO/IEC 27001 & ISO/IEC 42001)**
- **BSI IT-Grundschutz-Praktiker**
- **Experte für NIS2, DORA, CRA und AI Act**
- **Datenschutzbeauftragter (IHK)**
- KI-Beauftragter gemäß EU AI Act

+49 155 6096 2044
valeri.milke@vamisec.com
https://www.linkedin.com/in/valeri-milke/

Die VamiSec GmbH vereint über 15 Jahre Erfahrung in IT-Sicherheit und Compliance mit dem Anspruch, maßgeschneiderte Lösungen zu entwickeln, die Werte schützen und Innovation fördern. 150 erfolgreich abgeschlossene Projekte und über 70 Kunden

VamiSec GmbH, Bornheimer Straße 127, 53119 Bonn

Termin buchen

https://www.vamisec.com/