CERTifAI

KI-native Sicherheits- & Compliance-Plattform

CERTifAI ist eine **DSGVO-konforme, datensouveräne KI-Plattform**, die autonomes Sicherheitsscanning mit intelligenter Compliance-Automatisierung vereint. Wir helfen Unternehmen, ihren **Code abzusichern**, **Compliance skalierbar durchzusetzen** und **volle Datensouveränität zu bewahren** — gestützt auf über 200 atomare Sicherheitskontrollen, KI-gesteuerte Triage und einen lückenlosen Audit-Trail für jeden Befund.

Compliance Scanner

AUTONOMER KI-SICHERHEITSAGENT

- **200+ atomare Kontrollen** — Feingranulare Sicherheitsprüfungen mit vollständiger Herkunftsverfolgung
- **SAST + DAST + SBOM** — Vollumfängliche Sicherheitstests mit Schwachstellenverfolgung
- **KI-gesteuerte Pentests** — Autonome, LLM-orchestrierte Penetrationstests mit verschlüsselten Berichten
- **Automatische PR-Reviews** — Sicherheitsbewusste Code-Review-Kommentare bei jedem Pull Request
- **Audit-Trail** — Unveränderliche Befund-Nachverfolgung von Erkennung bis Behebung
- **LLM-basierte Triage** — Intelligente False-Positive-Filterung mit Konfidenz-Scoring
- **Code-Wissensgraph** — Architekturvisualisierung mit Auswirkungs- & Datenflussanalyse
- **Multi-Tracker-Sync** — Automatische Issues in GitHub, GitLab, Jira, Gitea
- **MCP-Server** — Live-Sicherheitsdaten in Claude, Cursor & anderen KI-Tools

CERTifAI Plattform

SOUVERÄNE GENAI-INFRASTRUKTUR

- **Multi-Provider LLM-Verwaltung** — Einheitliche Schnittstelle für LiteLLM, OpenAI, HuggingFace, Anthropic
- **KI-Agenten-Orchestrierung** — LangGraph-Integration mit Live-Monitoring & Agenten-Registry
- **Enterprise SSO** — Keycloak-basiertes OAuth2/PKCE, LDAP, Multi-Realm-Authentifizierung
- **Nutzungs- & Abrechnungsanalyse** — Token-Tracking, modellbasierte Aufschlüsselung
- **News-Intelligence** — KI-gestützte Nachrichtenzusammenfassung, Trendanalyse, Follow-up-Chat
- **Entwickler-Toolchain** — LangFlow, Langfuse, LangChain sofort einsatzbereit
- **RBAC & Feature Flags** — Rollenbasierter Zugriff mit kontrolliertem GenAI-Rollout pro Org
- **Mehrsprachigkeit** — Vollständige i18n-Unterstützung (DE, FR, ES, PT)
- **RAG-basierter Chat** — Natürlichsprachliche Q&A auf Basis Ihrer Codebasis

15 Mrd.+	200+	80%	10×	100%
APPSEC TAM BIS 2027	ATOMARE SICHERHEITS-KONTROLLEN	ZEITERSPARNIS BEI COMPLIANCE-PRÜFUNGEN	GÜNSTIGER ALS MANUELLE PENTESTS	DATENSOUVERÄNITÄT GARANTIERT

WARUM CERTIFAI GEWINNT

KI-native Sicherheit
LLM-gesteuerte Pentests & Triage ersetzen manuelle Audits (5.000–50.000 €). Kein Wettbewerber bietet autonome KI-Pentests.

Volle Provenienz
Jeder Befund rückverfolgbar zu Kontrolle, Regel und Quelle. Lückenloser Audit-Trail von Erkennung bis Behebung.

Datensouveränität
Keine Daten verlassen Ihre Infrastruktur. DSGVO-konform durch Architektur. EU-Hosting-Optionen verfügbar.

Shift-Left PR-Reviews
Sicherheitsbefunde erscheinen als PR-Kommentare vor dem Merge. Entwickler beheben Probleme direkt am Code.

Entwickelt in Rust
Speichersicherer, hochperformanter Stack. Fullstack-WASM + SSR mit Dioxus. Enterprise-taugliche Zuverlässigkeit.

Einheitliche Steuerung
Sicherheit + KI-Infrastruktur in einem Dashboard. Wettbewerber benötigen 5+ separate Tools.

ROADMAP — IN KÜRZE VERFÜGBAR

SOC2 & ISO 27001
Vorgefertigte Kontroll-Mappings für Zertifizierungsreife

Policy-as-Code
Eigene Compliance-Regeln via deklarative YAML-Policies

CI/CD-Gates
Deployments bei kritischen Befunden blockieren

Executive Reports
Auto-generierte Compliance-Berichte für die Geschäftsführung

GESCHÄFTSMODELL

- → **SaaS Cloud** — Verwaltete Multi-Tenant-Plattform für KMUs
- → **Enterprise-Lizenz** — Dedizierte Bereitstellung mit Support & Integrationen
- → **Professional Services** — Individuelle Regeln, Pentest-Berichte, Compliance-Audits
- → **API-Stufen** — Kostenlose Community-Stufe, kostenpflichtiger Enterprise-Zugang

ZIELMÄRKTE

- → **Regulierte Branchen** — Finanzen, Gesundheitswesen, Behörden (DSGVO, HIPAA, SOC2)
- → **Enterprise DevSecOps** — Shift-Left-Security für Entwicklungsteams
- → **EU-Datensouveränität** — Unternehmen mit souveräner KI-Infrastruktur
- → **Sicherheitsberatungen** — Automatisierte Pentests & Berichtserstellung