AI Security & Datenschutz Check

Angebot

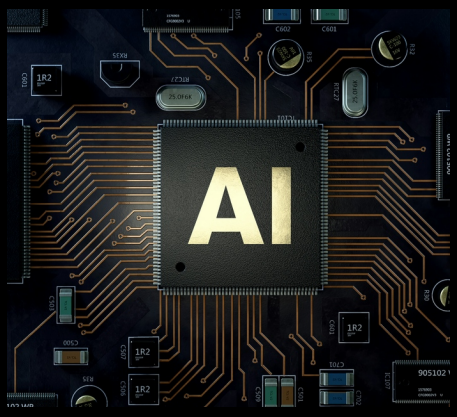
Osmond GmbH
+41 56 511 22 90
Rummelmatt 6, CH-5610 Wohlen
info@osmond.ch
www.osmond.ch

01/09/2025

Überlick und Nutzen

Der AI Security & Datenschutz Check bewertet strukturiert Security und Compliance-Anforderungen beim Einsatz von AI-Systemen wie LLMs, AI Agents, RAG, und VIBE Coding. Ziel ist die sichere, rechtskonforme Nutzung von AI - ohne eigene Modellentwicklung, aber mit hoher Verantwortung für Daten, Prozesse und Governance. Der Check kann präventiv bei der Einführung oder retrospektiv zur Bewertung bestehender AI-Lösungen durchgeführt werden.

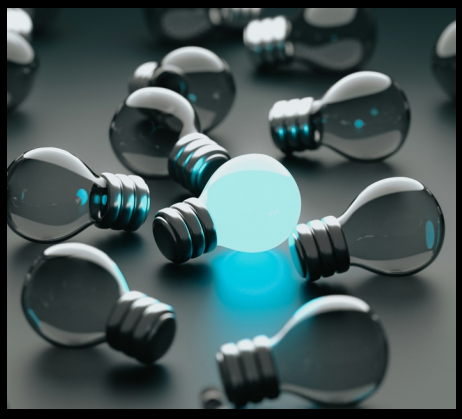
Typische Risiken vor dem Check



- Manipulationen durch Prompt Injection – Risiko für Anbieter und Nutzer bei Agentensteuerung
- Model Poisoning und Adversarial Attacks
- Fehlende Zugriffskontrollen auf APIs, AI-Lösungen
- Datenschutzverstösse bei personenbezogenen Daten
- Intransparente oder nicht erklärbare AI-Entscheidungen
- Fehlende Kontrolle über Agenten und automatisierte Prozesse
- Reputationsrisiken und Haftungsfragen
- Unklare Verantwortlichkeiten bei AI-gestützten Entscheidungen

Vorgehensmodell

- Ist-Analyse mittels Interviews, Dokumentenprüfung und Spot-Checks
- Die Bewertung erfolgt entlang bewährter Leitlinien und Checklisten, die zur Vollständigkeit, als Bewertungs-massstab und Orientierung dienen:
  - Critical AI Security Guidelines (SANS), AI-Compliance Checkliste (VISCHER)
  - EU AI Act Compliance Matrix (iapp) – zur Bewertung der Rolle und Pflichten nach EU-Recht für Unternehmen mit Bezug zur EU
- Ergebnisse werden anhand eines Reifegradmodells (Security, Datenschutz, Governance) aufgezeigt
- Ableitung konkreter Massnahmen zur Risikominimierung und Compliance



Osmond
RISK MATTERS

Unsere Leistungen

- Prüfung technischer und organisatorischer Massnahmen (TOM)
- Datenschutz-Check, bei Bedarf auch Datenschutzfolgenabschätzung (DSFA), Vertragsdurchsicht
- Bewertung von Drittanbieter- und Cloud-Risiken
- Empfehlungen zur Absicherung von AI-Lösungen, Daten und Schnittstellen

Lieferobjekte

- Ergebnisbericht mit Reifegradbewertung
- Management-Präsentation mit Handlungs-empfehlungen
- Massnahmenkatalog zur Verbesserung von AI Security & AI Datenschutz
- Optional: Unterstützung bei Umsetzung und Follow-up-Check

Mehrwert

- Klare Sicht auf AI-bezogene Sicherheits- und Datenschutzrisiken und Massnahmen
- Erfüllung regulatorischer Anforderungen (DSG, EU AI Act)
- Reduktion von Security-, Haftungsrisiken und Reputationsschäden
- Grundlage für sichere und vertrauenswürdige AI-Nutzung