

Azurblaue Wolke vs. Azure Cloud

Warum KI den Menschen braucht



Guten Morgen! 😊 Wie kann ich dir heute helfen?

Bitte verfasse eine Kurzbiographie auf Basis dieses LinkedIn-Profiles:
<https://www.linkedin.com/in/mende/>



Matthias Mende ist ein deutscher Unternehmer, der seit 2007 in den Vereinigten Arabischen Emiraten lebt. 2016 entwickelte er ein Interesse an Bitcoin und vertiefte sein Wissen in der Blockchain-Technologie. Als Mitbegründer des Dubai Blockchain Centers und Gründer des Bonuz-Projekts hat er sich auf die Entwicklung von Multi-Chain SocialFi- und GameFi-Web3-Ökosystemen spezialisiert. Mit über 300.000 Followern auf seinen Social-Media-Plattformen gilt Mende als einflussreiche Persönlichkeit im Bereich Blockchain und Innovation.

MATTHIAS MENDE

Quellen

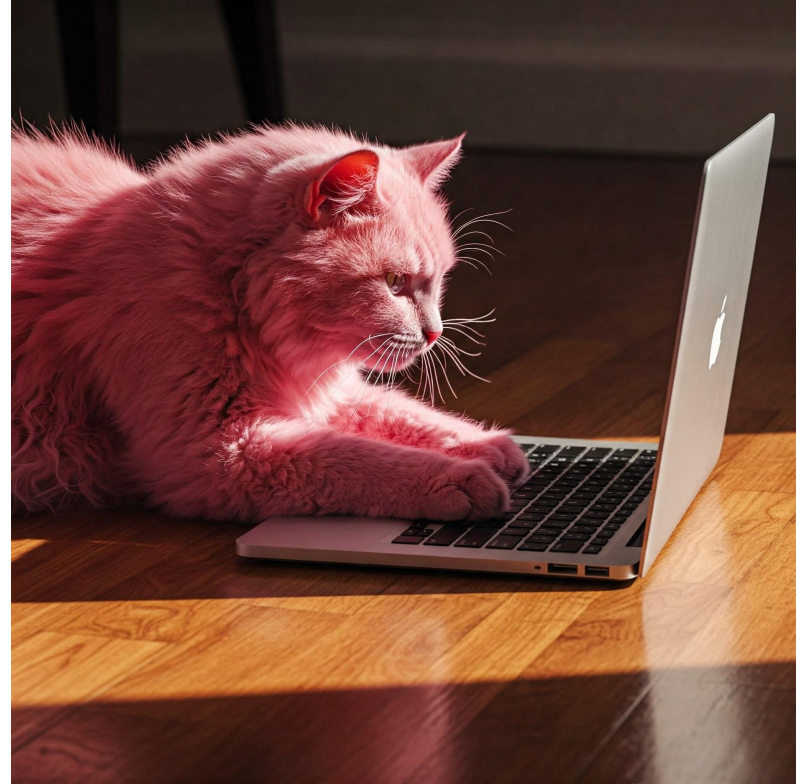
Das war das falsche Profil.



Entschuldige bitte! Da ich nicht direkt auf das verlinkte LinkedIn-Profil zugreifen kann, kannst du mir eine kurze Beschreibung des Profils geben, z. B. die beruflichen Stationen, Tätigkeitsfelder oder besonderen Errungenschaften? Auf Basis dessen verfasse ich gerne die Kurzbiographie für dich! 😊

The Real Me

- Analyst, Berater, Autor, Copywriter, Übersetzer, Podcaster, Trainer
- Schwerpunkte Enterprise-IT, Cybersicherheit und technische Kommunikation
- seit 2012 freiberuflich tätig
- Erstellung von IT-Sicherheitskonzepten und technischer Dokumentation nach ISO 27001 bzw. BSI-Grundschrift
- zertifizierter IT-Grundschrift- und BCM-Praktiker
- zertifizierter Prompt Engineer



Themen

- ★ Prämisse
- ★ Herausforderungen
- ★ Begriffe
- ★ Vorteile
- ★ Einsatzgebiete
- ★ KI-Modelle
- ★ Übersicht LLMs
- ★ KI-Stack
- ★ Auswahlkriterien
- ★ Datenquellen
- ★ KI-Jobs
- ★ Human in the Loop
- ★ Prompt Engineering
- ★ Sicherheit



“Die KI versteht nicht, was ich von ihr will!”

— — —

- KI versteht nicht.
- KI denkt nicht.
- KI ist Mathematik
(Statistik, Analytik,
Theory of Probabilities,
Kalkulation,
Mustererkennung)
- KI ist ein Interpretier.
- KI ist (im Wesentlichen)
ein stochastischer
Papagei.



Vorteile

— — —

- Effizienz
- Verbesserung
- Neue Ansätze / Gesichtspunkte
- Mehr / größere Zusammenhänge
- Kreativität
- Fehlerkorrektur (Rechtschreibung, Grammatik)
- Lernhilfe
- Feedback
- Gesellschaft



Einsatzgebiete

— — —

- Informationsbeschaffung
- Kreativität
- Analysen
- Zusammenfassungen
- Übersetzungen
- No-/Low-Code
- Problemlösung
- Coaching/Training
- Unterstützung
- Automatisierung



Herausforderungen

- Trainingsdaten sind immer nur so vollständig, wie sie zur Verfügung stehen.
 - Pay-/Ad-/Reg-Walls tragen nicht zur Demokratisierung von Information bei
- Verzerrungen und unerwünschte Inhalte
- Je nach Trainingsdaten ist eine KI mehr oder weniger voreingenommen (biased).
- Unklare Instruktionen oder die Verwendung von für den Zweck ungeeigneter Modelle
- Knowledge Cut-Off (zeitliche Einschränkung verfälscht Ergebnisse)
- Korrelation ist nicht zwingend Kausalität.
- Sensible Informationen!
- KI neigt zur Halluzination.
- KI hat keine interkulturelle Kompetenz.
- Authentizität, Tonalität und Zielgruppen!
- Urheberrechte
- Schwachstelle + Sicherheitsrisiko
- Lizenzrecht (Open Weight ist nicht! Open Source)
- Ethische Schranken (schädliche Antworten und/oder verletzend Sprache)
- Betrieb von KI-Infrastruktur



Begriffe

— — —

- Natural Language Processing (NLP)
- Generative künstliche Intelligenz (genAI)
- Große Sprachmodelle (Large Language Model, LLM)
- Neuronale Netze
- Maschinelles Lernen (ML)
- Chain of Thought
- Retrieval Augmented Generation (RAG)
- Token



KI-Modelle

Reasoning AI (o3, R1,
Gemini)

Agentic AI (Claude,
Operator, Macaw, MIST AI)

[CausalAI](#), Deep Research
(o3)



Berühmte LLMs (Auswahl)

- GPT, Strawberry, Q*, o1, o3 (OpenAI)
- Claude: Sonnet, Haiku (Anthropic)
- Inflection (Pi AI)
- Llama (Meta)
- Gemini, BERT, Gemma(1), T5 (Google)
- Phi (Microsoft)
- Grok AI (X)
- Mistral/Mixtral (Mistral)



Open-Source-LLMs (Auswahl)

- R1 (1), V3 (1), VL2 (1) (DeepSeek)
- BLOOM
- MPT-7B (MosaicML Foundation)
- Vicuna-13B (LMSYS ORG)
- Falcon 2 (Technology Innovation Institute Abu Dhabi)
- OLMo 2, MoMo ([Ai2](#))



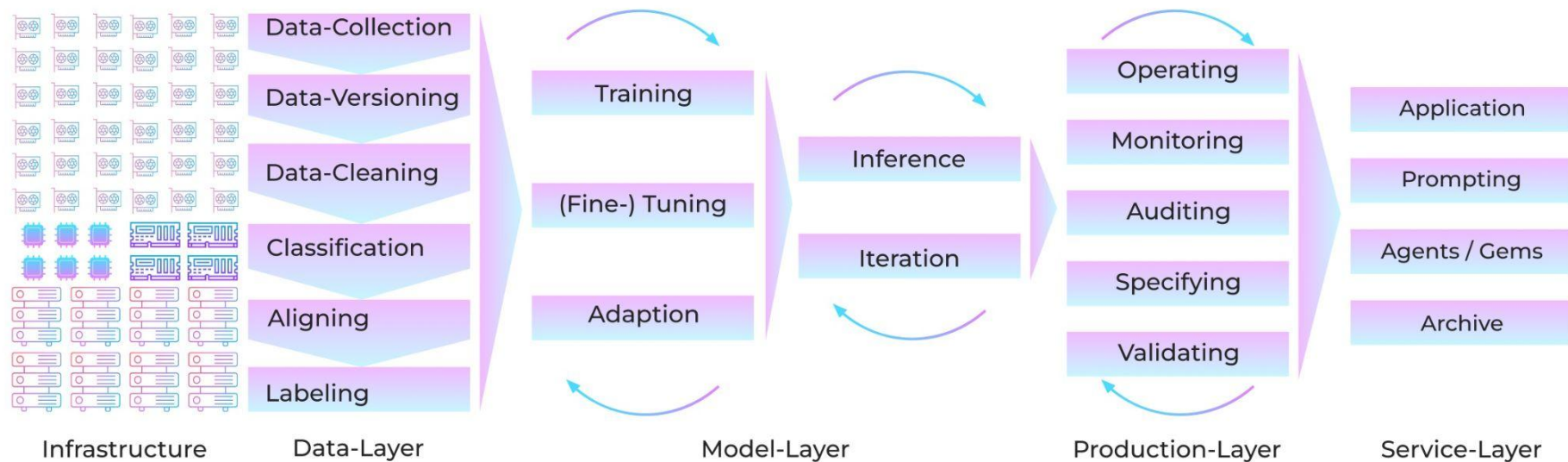
Deutsche LLMs (Auswahl)

- [PhariaAI](#) (Aleph Alpha)
- [MoinAI](#) (knowhere GmbH)
- [Gretchen AI](#) (DFKI)

Mehr bei [OpenEuroLLM](#) und [Occiglot](#)



KI-Stack (High Level)

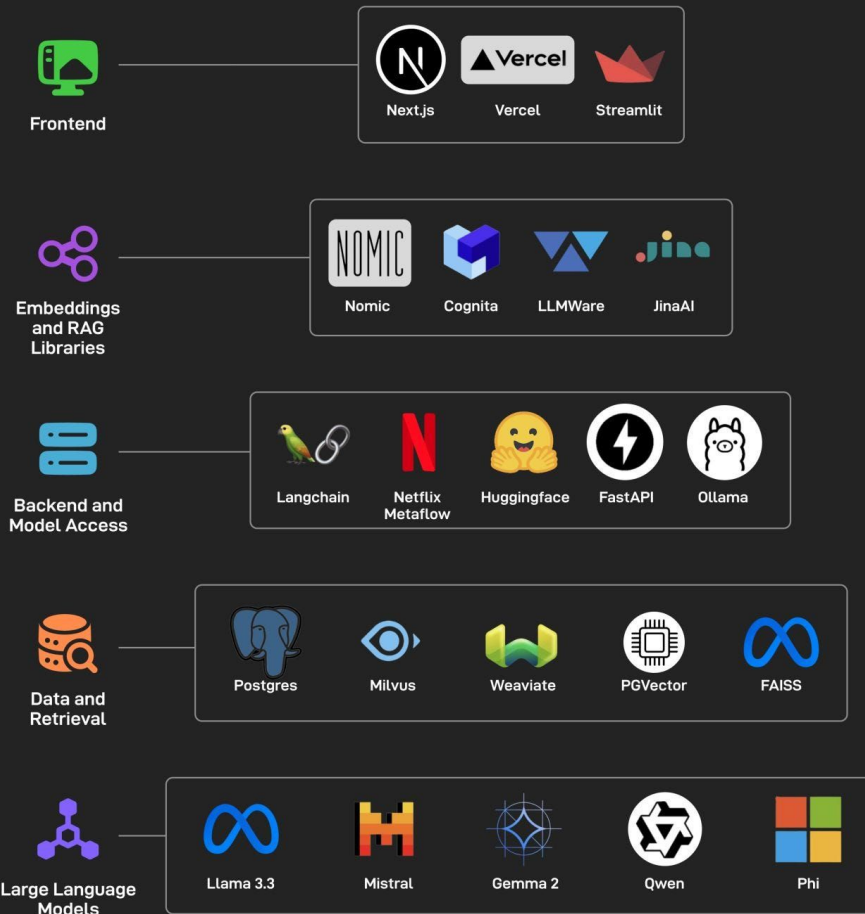


Open Source KI-Stack

- Deployment
 - Google Cloud, AWS, Nebius, Azure, Open Telekom Cloud, Gemini, eigenes RZ
- Monitoring
 - PropmtLayer, Galileo, arize
- Database
 - MongoDB, PostgreSQL, Weaviate
- Orchestrators & Frameworks
 - LlamaIndex, LangChain, Haystack, DSPy, llmware-ai
- Model Access
 - OpenAI, Mistral AI, cohere, Faiss, Hugging Face, together.ai, Ollama
- Programming
 - Python, Go, JS/TS

The Open Source AI Stack

ByteByteGo



Das richtige Modell

— — —

- Modellgröße
- Leistung und Correctness
- General vs. Specific Purpose (Pre-Training)
- Aufwand für Infrastruktur (Beschaffung, Inbetriebnahme, Pflege, Skalierbarkeit)
- Trainings- und Pflegeaufwand des Modells im Betrieb
- RAG-Erweiterung
- Closed Source, Open Weight, Open Source, Proprietär
- App-Unterstützung (siehe AI-Stack)
- Eigenständig vs. Integriert



Benchmarks

— — —

<https://huggingface.co/collections/open-llm-leaderboard/the-big-benchmarks-collection-64faca6335a7fc7d4ffe974a>

<https://livebench.ai>

<https://rank.opencompass.org.cn/leaderboard-llm>

https://tatsu-lab.github.io/alpaca_eval

<https://ailuminate.mlcommons.org/benchmarks>

<https://mlcommons.org/benchmarks/storage>



Daten-Kraken

— — —

[Common Crawl](#)

[OSCAR](#)

[OpenWebSearch](#)



HI für AI

— — —

- Datenaufbereitung
 - Data Strategist
 - Analysten (Datenkrämer)
 - Researcher (Datenjäger)
 - Datenbankexperten
- Modellierung
 - Data Scientist
 - DataOps Specialist
 - AI Specialist
- Produktion
 - MLOps Engineer
 - ML Developer
 - KI-Beauftragter (Ethik, Datenschutz, Sicherheit, Compliance)
 - Prompt Engineer
 - AI-Trainer / -Coach



KI gut, alles gut?

Warum KI jetzt wirklich
den Menschen braucht.



Famous Last Words

Die Texte für unsere Broschüren schreibt ChatGPT.

Playbooks? Schreibt bei uns Claude.

Die Konfig hat Marvis geprüft.

Für Marketing-Kampagnen ist CoPilot zuständig.

Sicherheitskonzept? Hat Gemini geschrieben.

Tickets beantwortet der virtuelle Service-Agent im Jira.

Websites übersetzen wir mit Weglot!



Die AI Operations Plattform für kritische Arbeiten.

Lernen Sie die Operations Cloud kennen

AIOps

Separates Signal
vor Lärm.

[Kostenlos testen →](#)

Automatisierung

Betrieb bei
Maschinengeschwindigkeit.

[Kostenlos testen →](#)

Vorfall Management

Vorfälle verwalten
Ende-zu-Ende.

[Kostenlos testen →](#)

Kunde Servicebetrieb

Brückenunterstützung
und Ingenieurwesen.

[Kostenlos testen →](#)



PagerDuty Advance

Beschleunigen Sie kritische Betriebsarbeiten mit
generativer KI, vom Schreiben von
Statusaktualisierungen bis zum Skalieren von
Automatisierungsaufträgen.

[Jetzt entdecken →](#)

The AI Operations Platform for critical work.

Meet the Operations Cloud

AIOps

Separate signal
from noise.

[Try for free →](#)

Automation

Operate at
machine speed.

[Try for free →](#)

Incident Management

Manage incidents
end-to-end.

[Try for free →](#)

Customer Service Ops

Bridge support
and engineering.

[Try for free →](#)



PagerDuty Advance

From writing status updates to scaling automation jobs,
accelerate critical operations work with generative AI.

[Explore now →](#)

The Human in the Loop

— — —

Zielgruppe

Authentizität

Satzbau

Kulturelle (In-) Kompetenz

Integration

Fehlersuche

Mehr-Augen-Prinzip / Approvals

Design



Prompt Engineering

- Be kind to your AI
- Geeignetes Modell nutzen
- Präzise Formulierungen
- Größere Requests aufsplitten
- Prompt-Bibliothek pflegen
- Schulungen für Anwender
- Kontinuierliches Training
- Kritische Auseinandersetzung



Der gute Prompt

- Aufgabe (Was?)
- Kontext (Wieso? Weshalb? Warum?)
- Zielgruppe (Für Wen?)
- gewünschtes Format (Wie)

ggf. Referenzen oder
Persona (Who am I) für
relevantere Ergebnisse
sowie Ausschlusskriterien



Rumhängende Katzen

- Klare Anweisung
- Auf Wortwahl achten
 - Mehrdeutige Wörter überdenken / vermeiden
- Kurze Sätze
- Aktive Sprache
- Details und Ziel
- Format & Struktur
- Don't trick!
- Zeitraum
- Sichtweisen



Ergebnis checken

- Relevanz
- Aktualität
- Richtigkeit
- Sinnhaftigkeit!
- Logik
- Semantik
- Wiederholungen?
- Tonfall?
- Satzbau?
- Quellen prüfen!
- Layout
- Syntax



Mach's nochmal, Sam!

— — —

- Evaluieren
- Anpassen
- Spezifizieren
- Wiederholen



Feedback geben

- Auf Fehler hinweisen
- Fehler korrigieren
- Auf Unvollständigkeit hinweisen
- Nach Quellen fragen!
- 👍 / 👎



Ich danke dir für die Korrektur und ich werde mich bemühen, meine Antworten genauer und genauer zu machen, um Fehler zu vermeiden. Wenn du weitere Korrekturen hast, bitte teile sie mir mit.

Ich werde mich auch bemühen, die korrekte Information zu speichern, um in Zukunft keine Fehler mehr zu machen.

AI is just a tool!



Bekannte Schwachstellen

— — —

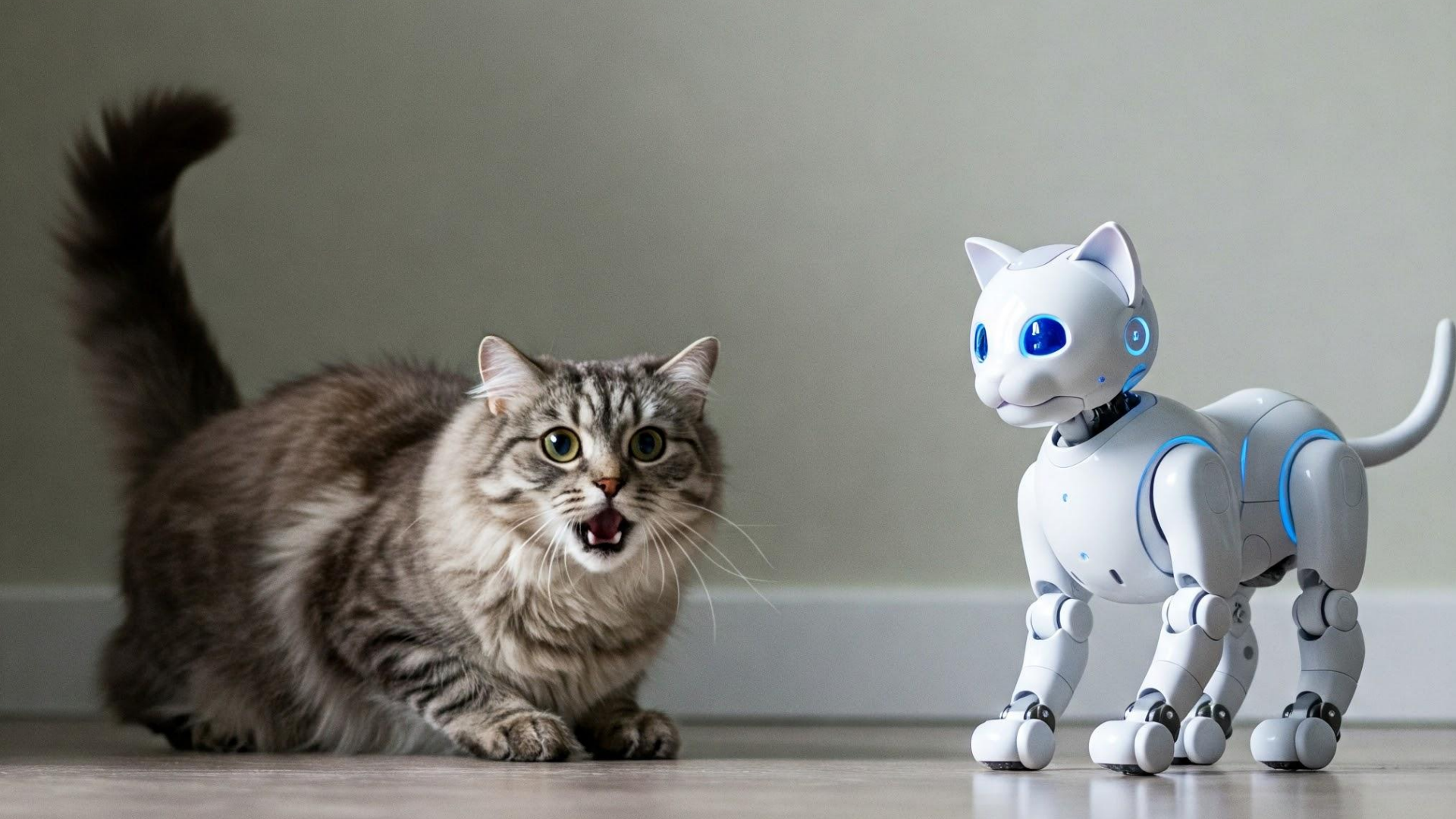
- [CVE-2024-50050](#)
- Hi, [I am DeepSeek](#) 😈
- 😊 [Broken Pickles](#)
- [Jailbreak](#) LLMs mit 🤡
- [Microsoft Copilot](#) ▶
- Prompt Injection, unsichere Plugins, unsicheres Output Handling, excessive Berechtigungen, [SQL-Injection](#), manipulierte Trainingsdaten, Supply Chain-Schwachstellen, [Denials-of-Service](#)
- [Container](#)-Breakout



Informationssicherheit

- KI-Strategie ist Chefsache
- Transparenz bei der Umsetzung
- Sensible Informationen schützen
- Angriffsflächen (er)kennen
- Schwachstellenmanagement
- Information- und Workflow-Management
- Rollen- und Berechtigungsmanagement (RuB)
- Awareness-Training
- Sicherheitskonzept für KI
- KI-Leitplanken
- Einsatz überwachen
- KI-Kompetenz schulen
- Fehler- und Lernkultur!





Trends

- AgenticAI
- Konzentration auf organisationsspezifische Kontexte und Muster
- Bessere Integration in Unternehmensanwendungen und -prozesse
- Mehr LLMs wie DeepSeek
- Mehr Sicherheitsvorfälle und Schwachstellen



Lesestoff

[KI für Einsteiger](#) (A Graphic Novel)

[Einführung in kausale Inferenz](#)

[The Cookbook](#) - Deep Learning for dummies

[Funktion, Begriff, Bedeutung](#)

[Geschichte der KI](#) (Computerwoche)

[Das große KI-Lexikon](#)

[Book of Why](#)

[Inside KI](#)

[Python für Einsteiger](#)

[Generative AI System Design Interview](#)

[When Cultures Collide](#)

[Game over](#)



In der Glotze

— — —

Open Source [AI-Stack](#)

15 Ways to [Break Your Copilot](#)

[Unsere Worte sind unsere
Waffen](#) – Chatbots manipulieren

aus der Videothek 🍿: A. I. |
2001: a space odyssey | I,
Robot | Westworld |
Futureworld | Weird Science |



Zugabe!

— — —

[Schreib mir](#)

Folge mir auf [LinkedIn](#)

Lies meinen [Blog](#) oder Artikel bei [speicherguide.de](#)

[Höre](#) mehr Podcast!

Buche 1 Training oder Workshop.

Human in the Loop as a Service:
Engagiere mich als [Redakteur,](#)
[Autor oder Übersetzer.](#)

[Kauf mir 1 Kaffee](#) (oder Tee ☕)



Quellen & Links

Kommerzieller Einsatz (Beispiele):

- [R-Cloud Developer Platform](#) on HYCU
- [MIST AI](#) für Junipers [Marvis](#)
- AgenticAI mit [Macaw](#) von [fabrix.ai](#)

Infrastruktur:

- Appliances von z. B. [SambaNova](#) (pre-trained für z. B. Banken) oder [Grog](#) (spezielle CPU für Inference -> Tensorstream)
- Infrastructure as a Service von deutschen Anbietern wie [Genesis Cloud](#) bzw. Fullstack KI as a Service von der [Open Telekom Cloud](#)

Open Source AI-Stack:

- [MongoDB](#)
- Open Source ([AI](#)) Initiative
- Frameworks zur Verwaltung des kompletten Stacks [Algorithmia](#)

Studien / Umfragen:

- GenZ und Millenials [lieben](#) KI
- [KI-Tools sind eher als Assistenten denn als Ersatz](#)
- [The Writer-GenAI-Survey](#)

