

Wie AI den Markt verändert und welche Herausforderungen ergeben sich für die Produktsicherheit

Wie AI den Markt verändert und welche Herausforderungen ergeben sich für die Produktsicherheit

Kurz zu mir:



Alexander Müller

Consultant: Cyber Security & Regulatory Affairs

Tel.: +49 1516 1148581

Alexander.mueller@seppmed.de



Wie AI den Markt verändert und welche Herausforderungen ergeben sich für die Produktsicherheit

Agenda:

1. Fähigkeiten von AI
2. Spezifische Risiken

Potentiale durch AI sowie Automationtools
und CRA-relevante Herausforderungen



Motivation

Jetzt offiziell: Berliner AI-Agent-Startup N8n mit 2,5 Milliarden bewertet

Antonia Remmerbach, Nina Anika Klotz
09 Okt 2025



Von 300 Millionen auf fast 2,4 Milliarden Dollar in vier Monaten: Accel soll die Unicorn-Runde des KI-Startups angeführt haben.

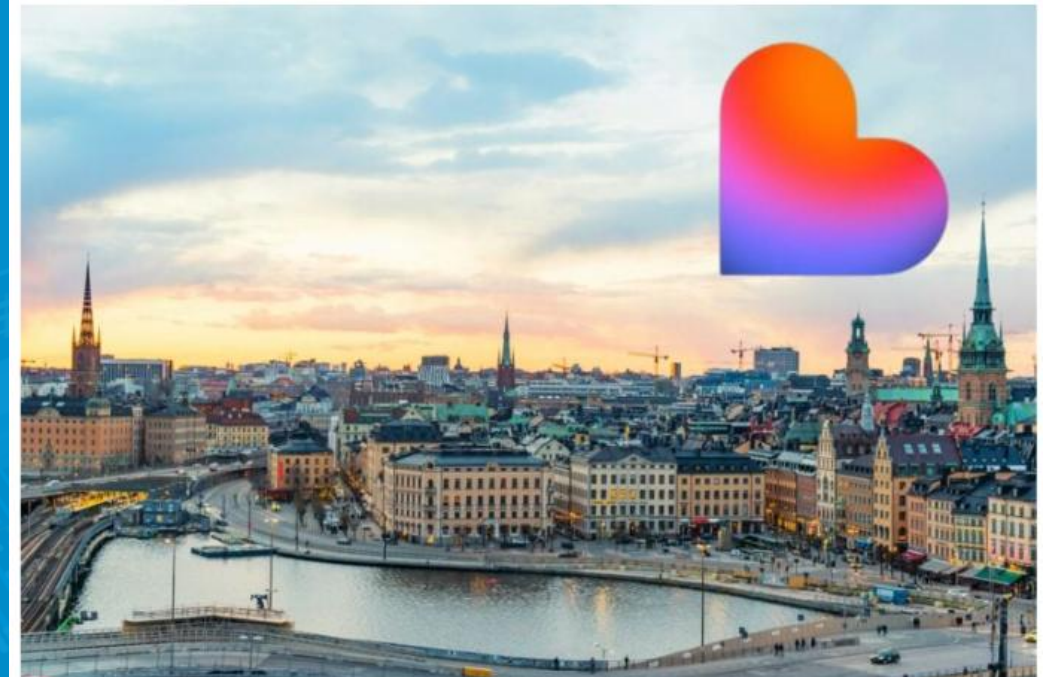


8 Monate nach Launch: KI-Startup Lovable erreicht Unicorn-Status

Nicole Plich
18 Jul 2025



Europa hat nun ein weiteres Unicorn: Lovable. Das KI-Startup hat laut Medienberichten eine Series-A in Höhe von 200 Millionen US-Dollar abgeschlossen.



Die Series-A-Runde von Lovable sei die größte überhaupt in Schweden. © Stefan Cristian Cioata/Getty/Lovable

1. Fähigkeiten von AI



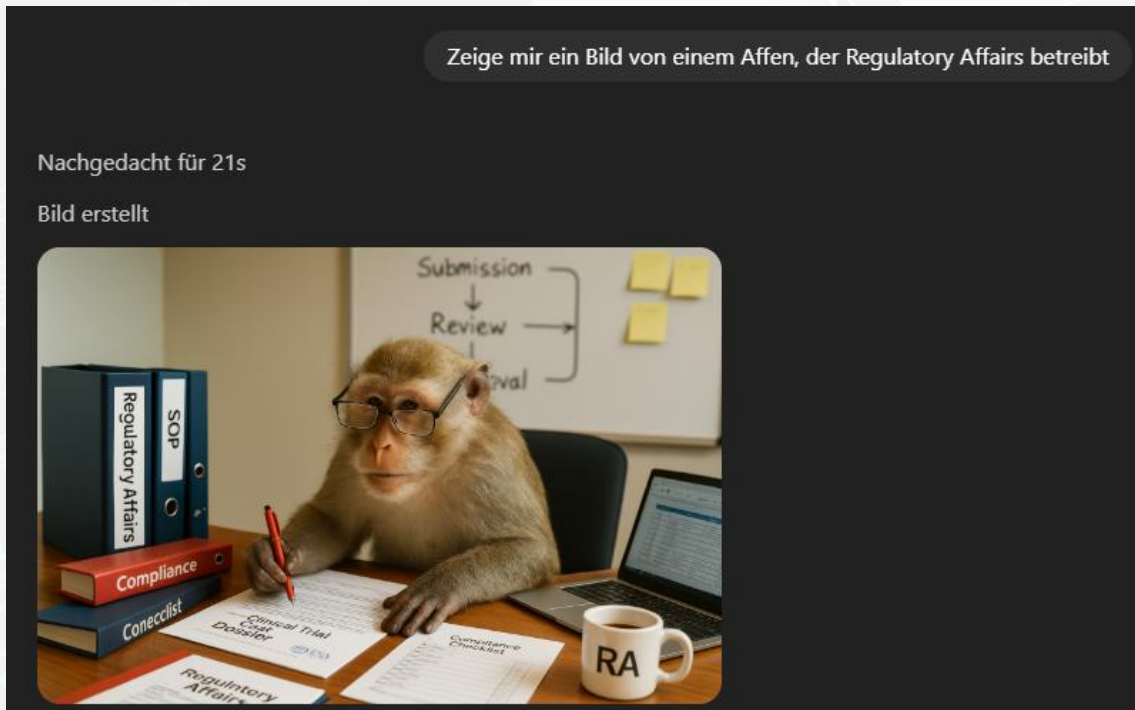
1. Fähigkeiten von AI AI Chat



AI System / LLM



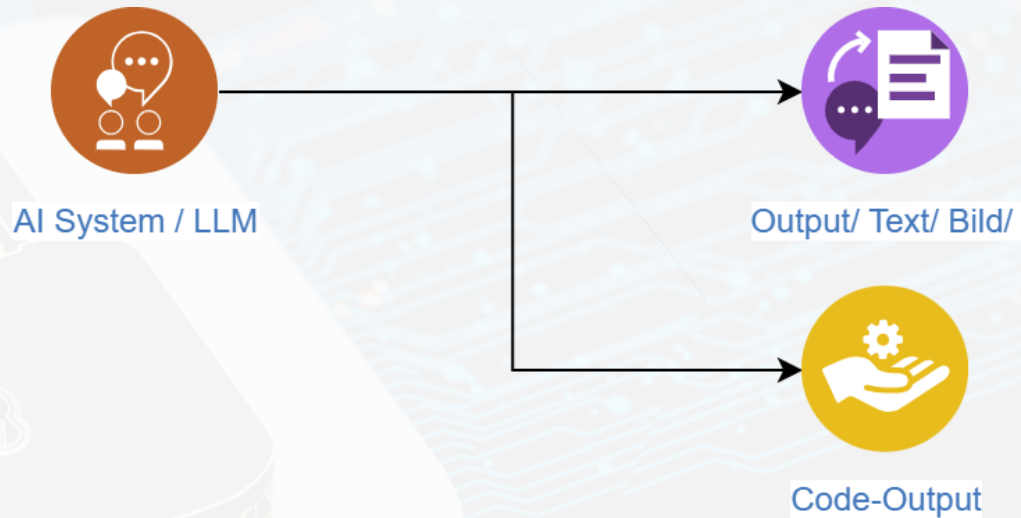
Output/ Text/ Bild/



- Texteingabe und Textausgabe
- Ausgabe in verschiedenen Medien möglich (Ton, Video und Bildausgabe)

1. Fähigkeiten von AI AI Agent

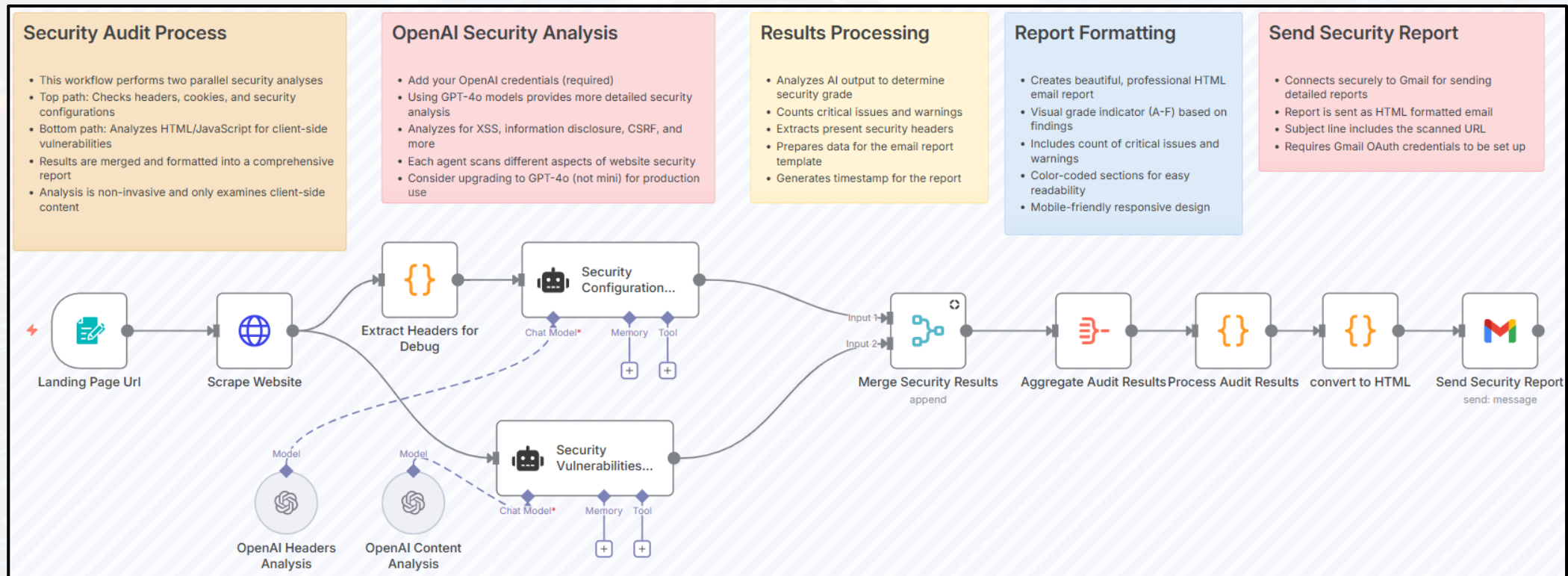
- Prompt → Code-Ausgabe / oder Funktion
- Code kann live kompiliert werden
- Code-generierung für Laien (Vibe Coding)
- Befehle werden in Funktionen ausgeführt
 - Systemsteuerung (z.B: Akku-Laufzeitverlängerung)
 - Assistenten und Bedienhilfen in Apps
 - Systemeinstellungen
 - Frameworks ausführen



**AI kann Codes und damit
Aktionen ausführen.
Sie wird handlungsfähig!**

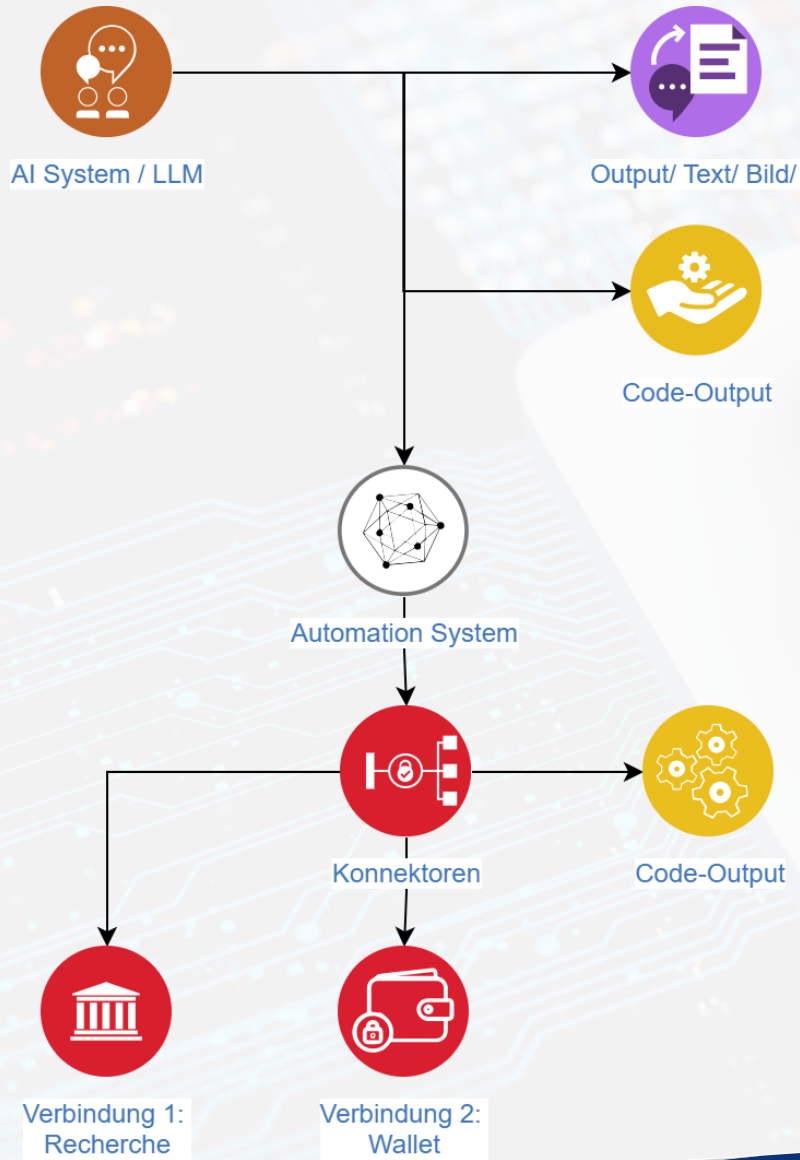
1. Fähigkeiten von AI AI + Automation

- Prozesse werden in Workflows automatisiert
- Verschiedene Dienste können in Wolkflows vereint werden



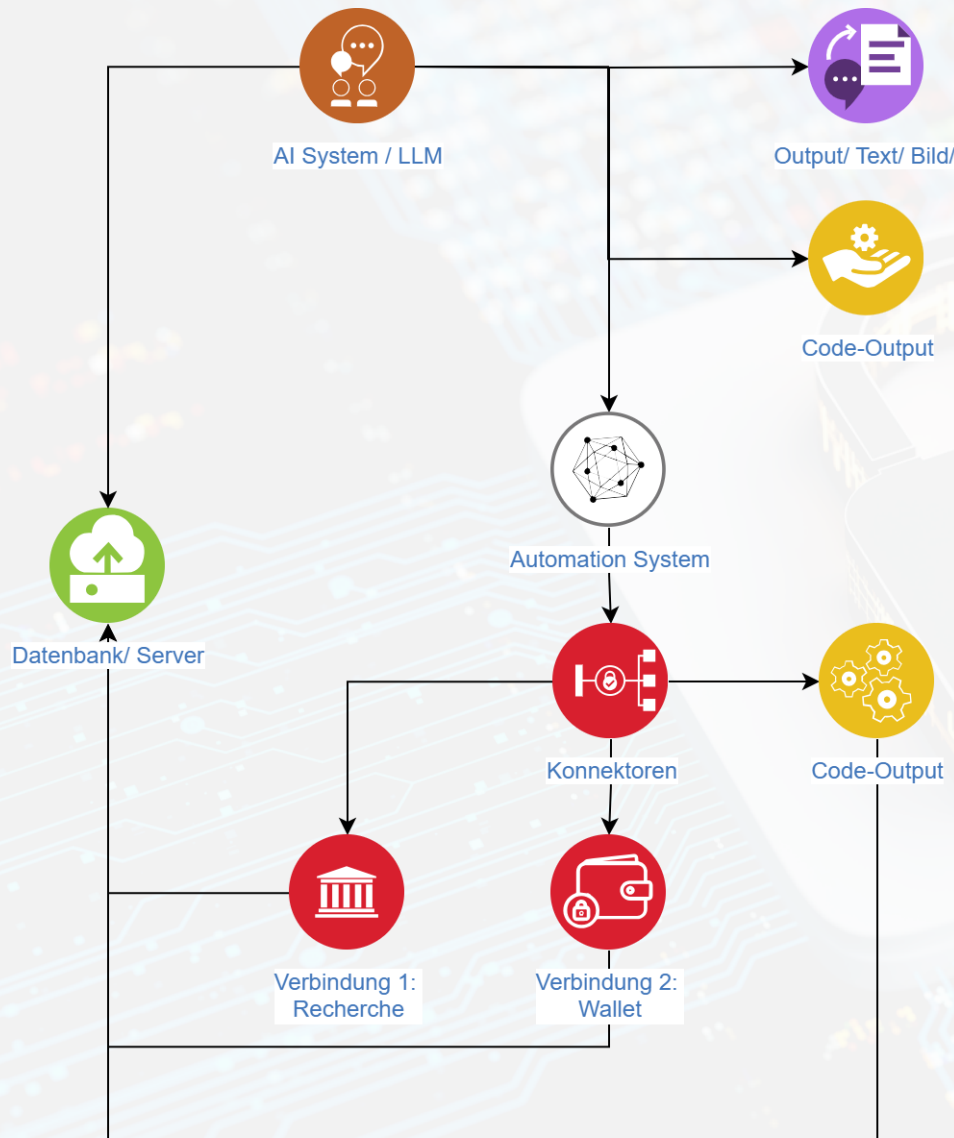
1. Fähigkeiten von AI

AI + Automation



- Mittels Automationtools können Aktionen verbunden werden
- Automatische Steuerung und Ausführung
- Kleine kreative Aufgaben können von Chat-Bots übernommen werden
- Verschiedene Dienste können eingebunden werden
- Komplexes API-Netzwerk entsteht

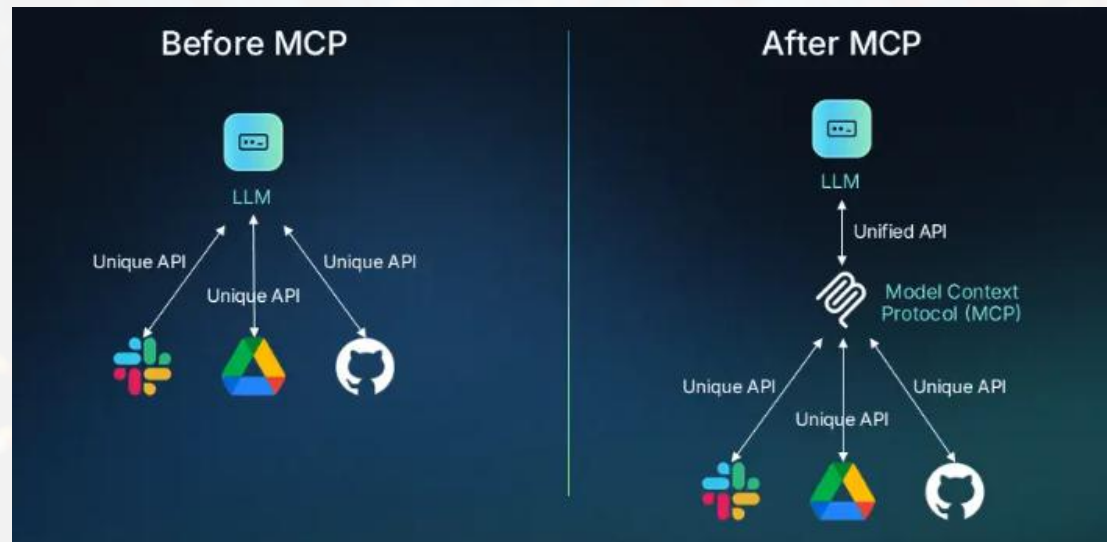
1. Fähigkeiten von AI RAG



RAG (Retrieval-Augmented Generation)

- Automatisierte AI-Systeme greifen aus Datenbanken und Systemen Daten ab, sowie legen Output ab.
- Workflows verbinden Aktionen für Systeme wie Prozesse einer SOP
- AI basierte IT- und Dokumentationssysteme sind möglich
- Komplexe Zugriffssysteme führen weitreichende Prozesse aus
- Enormer Unterstützung und Ressourceneinsparung
- Daten können live bereitgestellt werden
- JSON als Format der Zukunft

1. Fähigkeiten von AI Multiple Automation & MCP Clints



- Verschiedene AI-Systeme können verbunden werden
- MCP = Model Context Protocol
- Revolutionäre Vibe-Coding
- Mit Prompts in vielen SW-Sprachen agieren
- Komplexe Schnittstellen können individuell designt werden

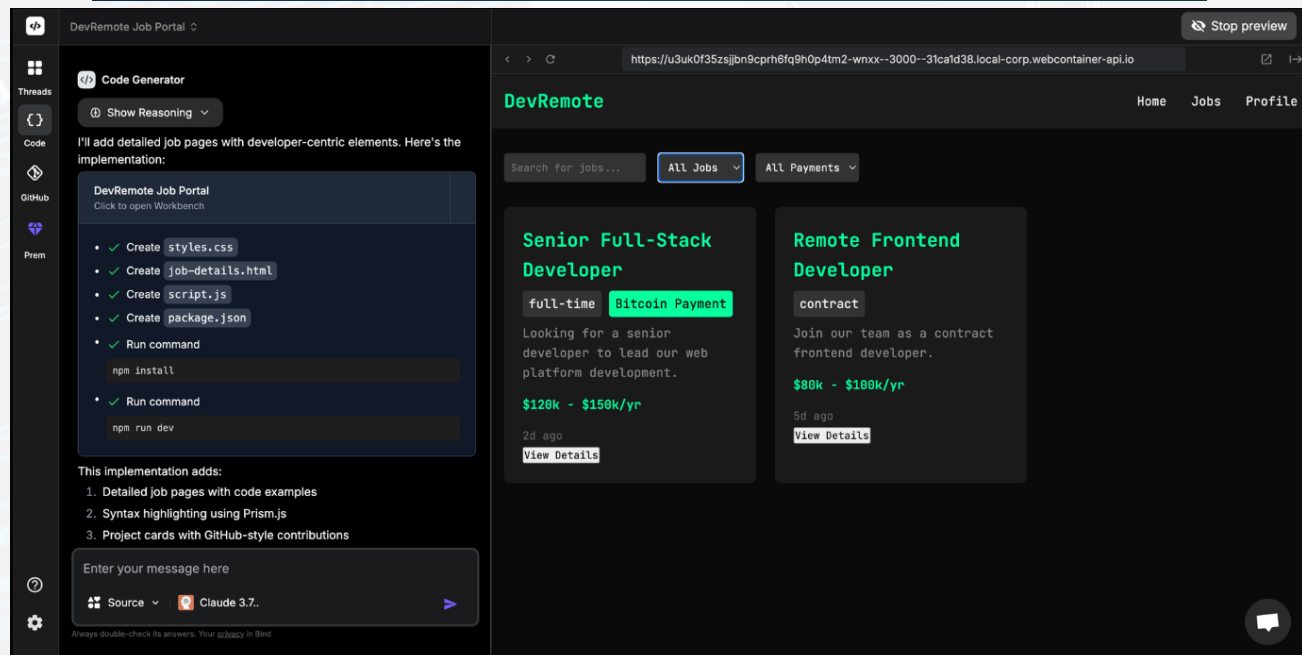


Abb.: [5],
[6]

1. Fähigkeiten von AI

Potentiale von AI



Code-Generierung

Schneller coden +
Laien und andere
Berufsgruppen
können nun coden.



Optimierte Prozesse

Prozesse können
verschlinkt werden.



Automatisierung

Mit menschlichen
Fehlern belastete
Prozesse können
automatisiert
werden.



Kreative Aufgaben

Kleine
Denkaufgaben und
kreative Prozesse
können
übernommen
werden.



SaaS-Lösungen

Verschiebung von
Dienstleistern zu
SaaS-Lösungen.



Beschleunigte Marktlage

Methoden liefern
Potential für
Beschleunigung der
Marktzugänge



Erhöhte Abhängigkeiten

Abhängigkeiten zu
AI-kompatiblen
Dienstleistern steigt.

- IT-Infrastruktur wird zum Herzstück, Werkzeugsammlung und zur Schwachstelle moderner (AI-driven) Unternehmen

2. Spezifische Risiken



2. Spezifische Risiken Security Testing

- Praktischer Ansatz: IEC 81001-5-1 als Guideline für CRA-Compliance
 - (Threat Modeling, Secure Coding & SBOM, stat./dyn. Tests, Pen-Tests, Wartung).
- Trend: Security-by-Design wird Pflicht
 - Kulturthema: Geschwindigkeit vs. Sicherheit – Governance als Enabler.
- MDR ist vielen bekannt, CRA oft unbekannt

CRA und ISO 81001-5-1

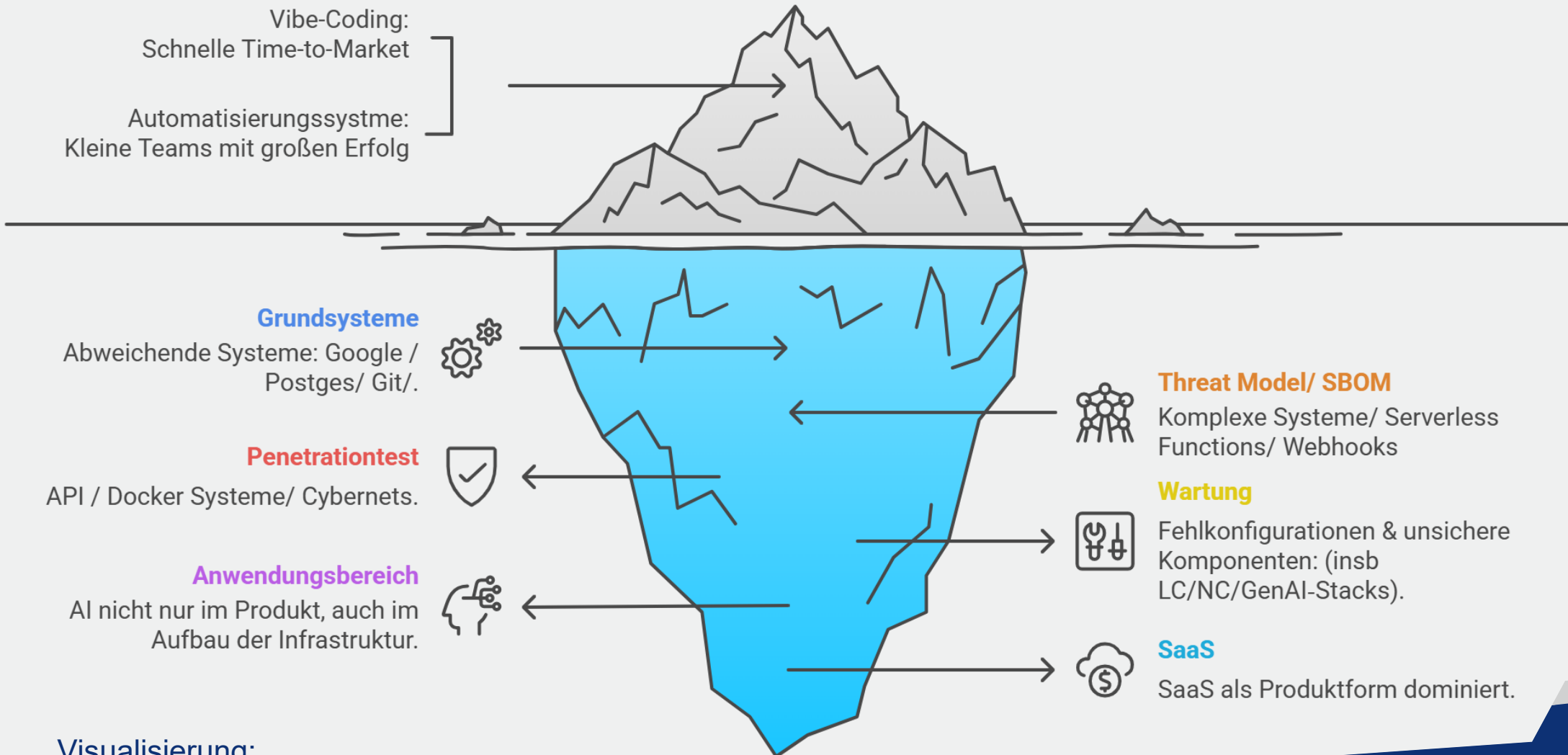
CRA
Verbindliche
Produktanforderungen,
Marktaufsicht und CE-
Konformität.

IEC 81001-5-1

Bietet Tiefe im Secure
SDLC für
Gesundheitssoftware.

Visualisierung:
Eigene Darstellung:
CRA und IEC 81001-5-1

2. Spezifische Risiken Security Testing



Visualisierung:
Eigene Darstellung: Testspezifika

2. Spezifische Risiken

TOP 10 Risiken: AI/ LLM

- Schwachstellen für AI werden von OWASP gerankt:
- Stringente Vorgaben an Systemprompts und Limitation von In- und Output

1. LLM01:2025 Prompt Injection
2. LLM02:2025 Sensitive Information Disclosure
3. LLM03:2025 Supply Chain
4. LLM04:2025 Data and Model Poisoning
5. LLM05:2025 Improper Output Handling
6. LLM06:2025 Excessive Agency
7. LLM07:2025 System Prompt Leakage
8. LLM08:2025 Vector and Embedding Weaknesses
9. LLM09:2025 Misinformation
10. LLM10:2025 Unbounded Consumption

- **Prompt-injection, Datenabfluss, Lieferkette, unvalidierte Outputs, überprivilegierte Agenten und unkontrollierten Ressourcenverbrauch**



2. Spezifische Risiken

TOP 10 Risiken: Low Code/ No Code

- Schwachstellen für Automatisierungstools werden bereits verfolgt
- Top 10 Schwachstellen für Low-Code / No-Code (OWASP)
- Kernschwächen sind:
- Autorisation/ Zugangsrechte der Accounts und Konnektoren (Risiko 1 – 7)
- Konfiguration und Privilegierung der Konnektoren
- Sichtbarkeit Secrets und Loggings



Abb.: [8]

1. LCNC-SEC-01: Account Impersonation
2. LCNC-SEC-02: Authorization Misuse
3. LCNC-SEC-03: Data Leakage and Unexpected Consequences
4. LCNC-SEC-04: Authentication and Secure Communication Failures
5. LCNC-SEC-05: Security Misconfiguration
6. LCNC-SEC-06: Injection Handling Failures
7. LCNC-SEC-07: Vulnerable and Untrusted Components
8. LCNC-SEC-08: Data and Secret Handling Failures
9. LCNC-SEC-09: Asset Management Failures
10. LCNC-SEC-10: Security Logging and Monitoring Failures

2. Spezifische Risiken

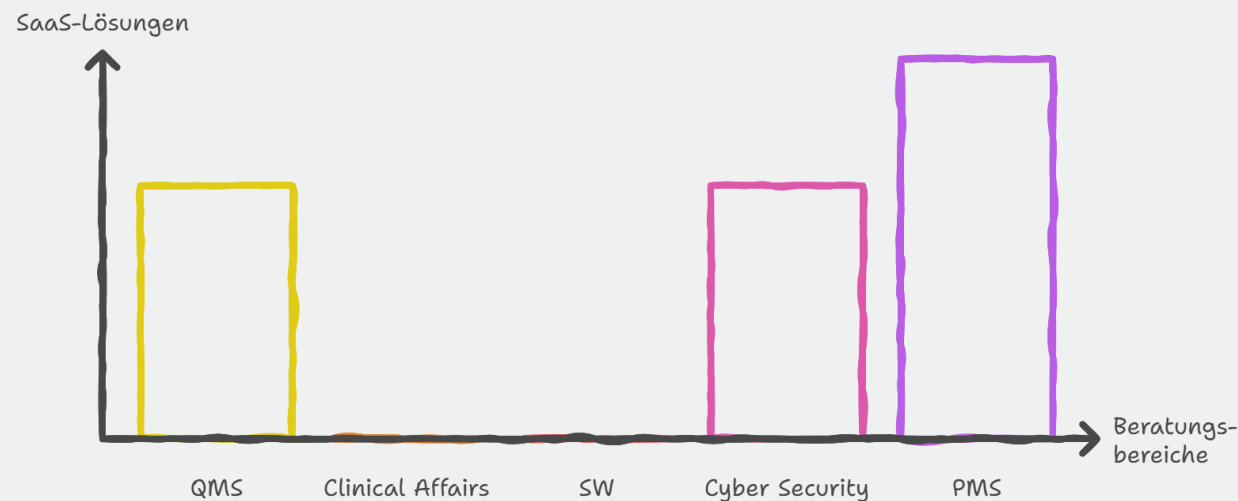
Fazit

- Vibe Coding (KI/Low-/No-Code) beschleunigt Entwicklung, Markteintritt und ermöglicht frühe klinische Evaluation.
 - erhöht jedoch Anforderungen an Governance & Security.
 - APIs und LLMs sind häufige Angriffsflächen.
- Zunahme kleiner, hochproduktiver Teams; klassische Rollen verschieben sich Richtung DevSecOps.
- Investoren fragen aktiv nach belastbarer Security-Governance (CRA-Readiness als Qualitätsmerkmal).
- AI -und Automationtools sind Kulturfrage von Start-Ups.



PS: Marktänderungen auch für Berater

- Beratungsmarkt ändert sich auch unter AI:
 - Früher Vermittlung Erfahrung und Fachwissen/
Heute: Mehr Guidance zum Lifecycle
 - Weniger Problemlöser/ mehr Prüfer
 - AI Siegerfelder: Monitoring, Schulung, Coding
 - Beratungssegmente werden durch SaaS-Lösungen verdrängt





Referent:

Alexander Müller

Consultant: Cyber Security &
Regulatory Affairs

Tel.: +49 1516 1148581

Alexander.mueller@seppmed.de



Wer sind wir

- Schulung, Training
- Agil Fabrik und SW-Entwicklung
- SW-Testing und Test-Management
- Regulatorische Beratung
- Cyber Security

Literaturverzeichnis

1. <https://www.trendingtopics.eu/n8n-berliner-ai-startup-wird-unicorn-bewertung-bei-24-milliarden-dollar/>
2. <https://www.businessinsider.de/gruenderszene/technologie/8-monate-nach-launch-ki-startup-lovable-erreicht-unicorn-status/>
3. Gupta S. The Effects of AI on Companies: AI-driven Research and Innovation to AI-driven Market Deployment and Future Business Model Changes. IJFMR [Internet]. 2025 Jun 15;7(3). Available from: <http://dx.doi.org/10.36948/ijfmr.2025.v07i03.48442>
4. Bimantara Putra R. Artificial Intelligence in Business: From Research and Innovation to Market Deployment Bridging the Gap Between Cutting Edge AI and Real World Applications. ISCEBE [Internet]. 2024 Dec 30;1(1):115–21. Available from: <http://dx.doi.org/10.33830/iscebe.v1i1.4232>
5. Menzies J, Sabert B, Hassan R, Mensah PK. Artificial intelligence for international business: Its use, challenges, and suggestions for future research and practice. Thunderbird Intl Bus Rev [Internet]. 2024 Feb 9;66(2):185–200. Available from: <http://dx.doi.org/10.1002/tie.22370>

Literaturverzeichnis

6. Kubiczek J, Roszko-Wójtowicz E, Koczy J, Waszkiewicz I, Woś K. Harnessing AI for business transformation: strategies for effective implementation and market advantage. SiTns [Internet]. 2025 Jun 13;26(2):199–213. Available from: <http://dx.doi.org/10.59139/stattrans-2025-022>
7. BSI. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html
8. **(CRA) VERORDNUNG (EU) 2024/2847 DES EUROPÄISCHEN PARLAMENTS UND DES RATES** vom 23. Oktober 2024. über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung)
9. IEC 81001-5-1:2021 Health software and health IT systems safety, effectiveness and security Part 5-1: Security — Activities in the product life cycle
10. PETRYSHYN N, NOVYTSKA S. The key issues of implementing artificial intelligence tools in business operations when entering foreign markets. Econ Fin Law [Internet]. 2025 Jun 30;6/2025:74–6. Available from: <http://dx.doi.org/10.37634/efp.2025.6.16>

Literaturverzeichnis

11. Schmidt J, Schutte NM, Buttigieg S, Novillo-Ortiz D, Sutherland E, Anderson M, et al. Mapping the regulatory landscape for artificial intelligence in health within the European Union. npj Digit Med [Internet]. 2024 Aug 27;7(1). Available from: <http://dx.doi.org/10.1038/s41746-024-01221-6>
12. <https://genai.owasp.org/resource/owasp-top-10-for-llm-applications-2025/>
13. <https://owasp.org/www-project-top-10-low-code-no-code-security-risks/>

Abbildungsverzeichnis

1. <https://www.trendingtopics.eu/n8n-berliner-ai-startup-wird-unicorn-bewertung-bei-24-milliarden-dollar/>
2. <https://www.businessinsider.de/gruenderszene/technologie/8-monate-nach-launch-ki-startup-lovable-erreicht-unicorn-status/>
3. Auszug: Chat-GPT: Eigener Prompt mit Bild-Output (OpenAI Chat GPT 5)
4. <https://n8n.io/workflows/3314-websecscan-ai-powered-website-security-auditor/>
5. <https://www.descope.com/learn/post/mcp>
6. <https://www.getbind.co/>
7. <https://genai.owasp.org/resource/owasp-top-10-for-llm-applications-2025/>
8. <https://owasp.org/www-project-top-10-low-code-no-code-security-risks/>

Vielen Dank für Ihre Aufmerksamkeit

