

Neue Akteure in
der Hochschultransformation:

KI-Agenten im Einsatz

Stefan Göllner (KI-Campus), Andreas Sexauer (KIT)



Zentrum für
Mediales Lernen

 **AI Campus**
powered by Stifterverband

Theorie und mehr zum Nachlesen vorweg ...

Organisationale Perspektive



Publikation: Agentische KI im Hochschulsystem

07.05.2026

<https://hochschulforumdigitalisierung.de/news/publikation-agentische-ki/>

Wir stehen an einer Schwelle. Es gilt das Chatfenster zu verlassen und KI bei der Ausführung komplexer Abläufe zu orchestrieren. Ähnlich wie das Aussteuern einer wissenschaftlichen Hilfskraft.

**AGENTIC MODE:
ON**



EXCEL VS. TASCHENRECHNER = KI-AGENTEN VS. KLASSISCHER KI CHAT

KI-AGENTEN: NICHT NUR SCHNELLER – SONDERN FUNDAMENTAL BESSER

TRADITIONELL

TASCHENRECHNER



- Jede Berechnung einzeln durchführen
- Ergebnisse manuell übertragen
- Fehleranfällig
- Zeitaufwendig

EXCEL (TABELLENKALKULATION)



Formeln verknüpfen,
automatische
Neuberechnung
bei Änderungen!



- ✓ Verknüpfte Formeln
- ✓ Automatische Updates
- ✓ Analysen & Auswertungen leicht gemacht
- ✓ **~10x schneller** bei wiederholten Berechnungen!

KLASSISCHER KI CHAT



Jede Aufgabe
einzeln beschreiben,
Kontext immer neu
aufbauen...



- Aufgabe jedes Mal neu erklären
- Kein bleibender Kontext
- Keine Automatisierung
- Manuell und zeitintensiv

KI-AGENTEN

Agenten übernehmen
Workflows, behalten
Kontext, arbeiten
autonom!



- ✓ Autonome Workflows
- ✓ Kontext behalten & nutzen
- ✓ Parallele Aufgaben
- ✓ **~10x schneller** bei repetitiven Wissensarbeit-Aufgaben!

**~10x
SCHNELLER**
bei repetitiven
Wissensarbeit-
Aufgaben!



MERKSATZ: Excel hat nicht nur das Rechnen beschleunigt – es hat das **Denken** verändert.

KI-Agenten werden nicht nur die Arbeit beschleunigen – sie werden das **Arbeiten** verändern.

PROMPT:

»Im Ordner "Aufbereitete-Inhalte" liegt die Aufbereitung eines Diskussionspapiers zu agentischer KI im Hochschulkontext. Ich will ein Projekt vorschlagen, um an meiner Hochschule das Thema voranzubringen, wir haben bisher noch keine strategischen Aktivitäten dazu.

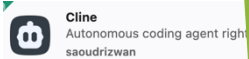
Erstelle ein Verzeichnis, in dem eine erste Projektskizze und jeweils Dokumente für relevante Stakeholder sein sollen. Diese Dokumente sollen jeweils auch eine Executive Summary und Hintergrundinformationen beinhalten, mit dem ich die Stakeholder gezielt ansprechen kann.«

LIVE DEMO

Schritt für Schritt Anleitung Cline in VSCode

Installieren

- VSCode (https://vscode.com/) oder Visual Studio Code (Microsoft App Store) installieren
- In VSCode bzw. Visual Studio Code den Extensions Marketplace öffnen  und nach Cline suchen
- Die Extension



Einrichten

- Cline erscheint in der Seitenleiste als Roboter Symbol . Dieses öffnen und dort in den Einstellungen (Zahnrad oben rechts) die API-Konfiguration vornehmen

Verwenden

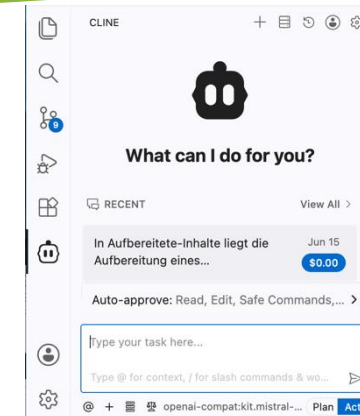
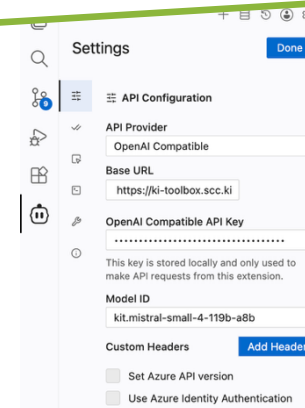
- Aufträge an den Agenten werden im Chatfenster eingegeben.
- Die Modi unten rechts gezielt verwenden:

plant erst, ohne zu ändern
hrt aus und Bearbeitet

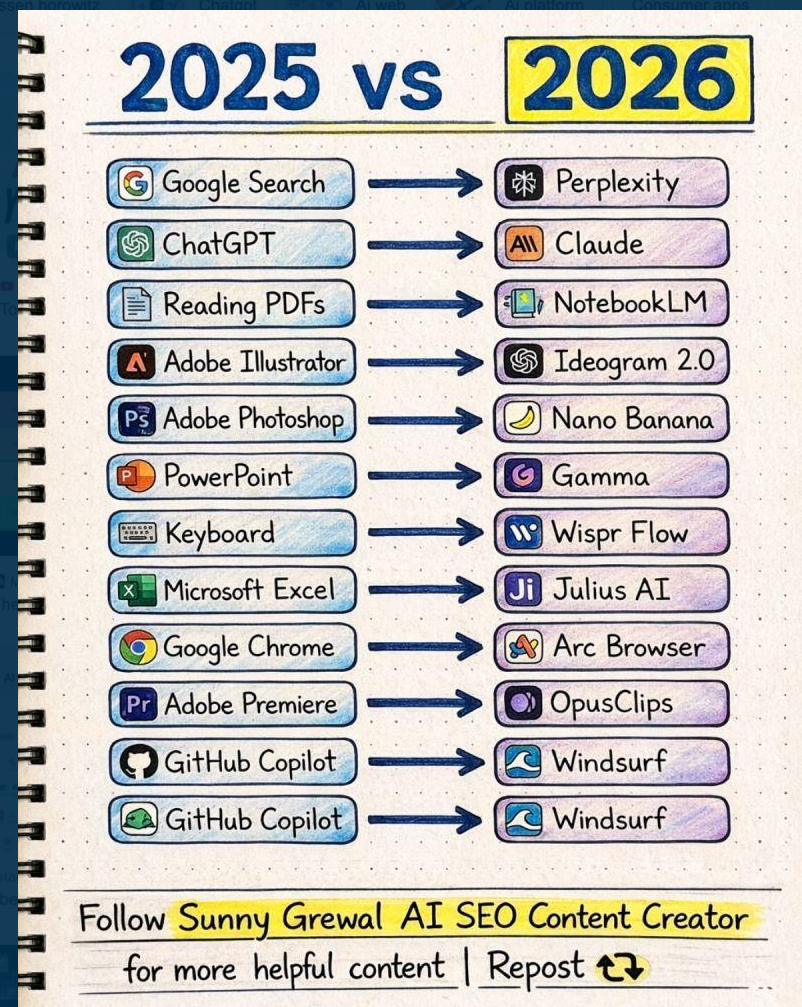
hweise zur Verwendung:
s.cline.bot

<https://www.zml.kit.edu/ki-agenten.php>

Cline-Account
anlegen und
freie Modelle von
dort verwenden.



Mehr Tools lösen nicht das Problem



Quellen: LinkedIn Harish kumar, 04.05.2026, https://www.linkedin.com/posts/harishkumar-sh_artificialintelligence-aitools-futureofwork-share-7457014872862613504-15em und AI for Enterprise, <https://www.linkedin.com/posts/ai-tools-2025-vs-2026-%F0%9D%97%95%F0%9D%97%B2%F0%9D%97%B0%F0%9D%97%BC%F0%9D%97%BA%F0%9D%97%B2-%F0%9D%97%AF%F0%9D%97%B2-share-7454665691665879040-cbGG>

Hinter vielen Tools stehen „nur“ Agenten ...

Perplexity Deep Research

- **Research Agent**
- **Ziel:** Bericht zu einem Thema zu erstellen
- **Analysiert** das Thema führt eine **Suche** im Internet und Fachdatenbanken durch.
- **Bewertet** die Suchergebnisse
- **Passt** bei Bedarf die Suche mehrfach **an** und verwendet dazu bereits ermittelte Informationen
- **Erstellt** einen Bericht dazu
- **Wandelt** diesen in eine Infografik, Word oder PDF-Datei **um**.

Notebook LM

- Ist eine **App mit verschiedenen Agenten**
- Verschiedene Agenten für z.B.:
 - Analyse und Zusammenfassung von Dokumenten
 - Erstellen von Audio- und Videozusammenfassungen
 - Interaktive Mindmaps
 - Erstellung von Präsentationen

Claude Desktop

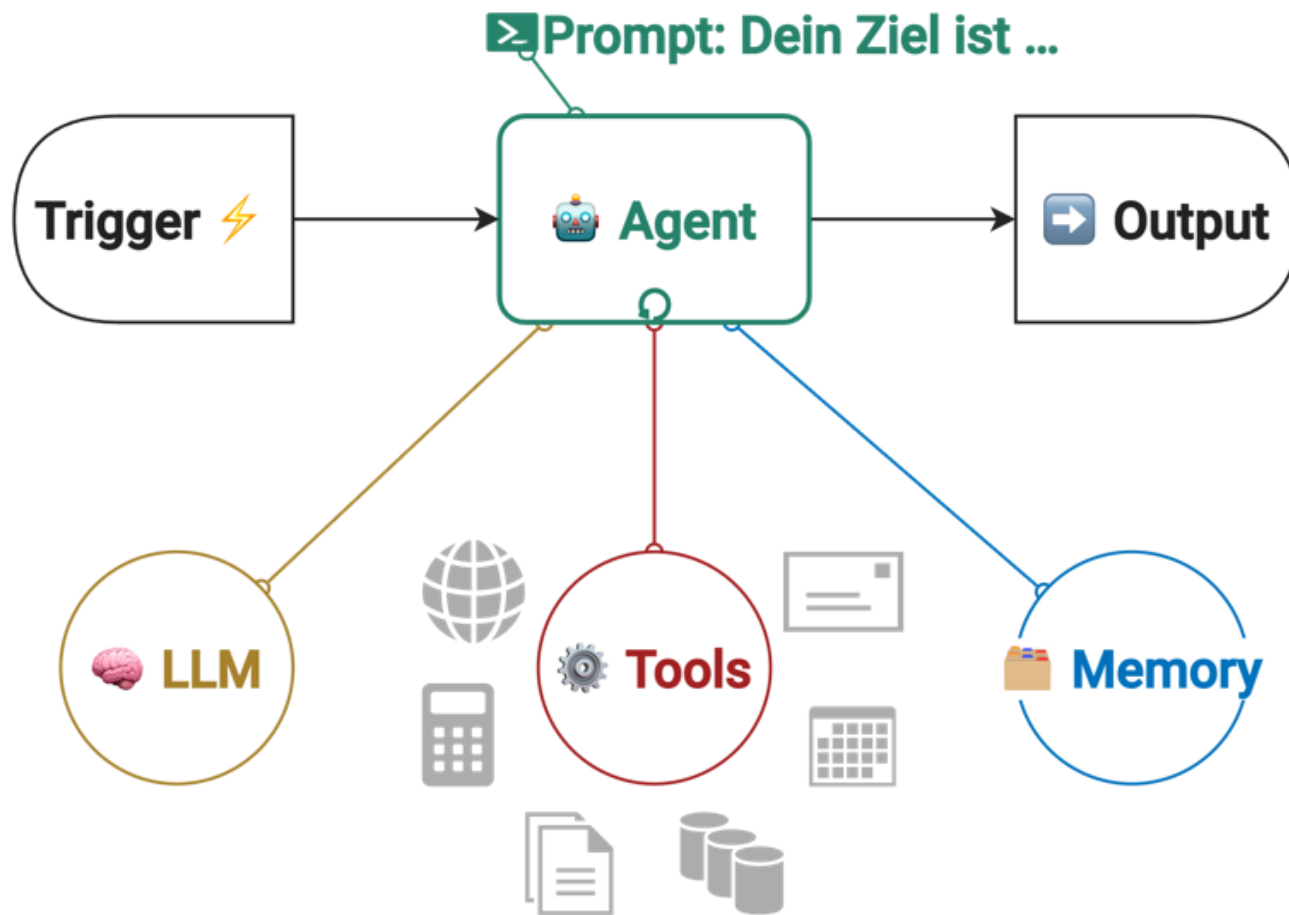
- **KI-Agent** System von Anthropic das direkt auf dem Desktop arbeitet
- Führt unterschiedlichste Aufgaben eigenständig und mehrstufig aus
- Z.B. Lesen, Bearbeiten und Organisieren von Dateien
- Ist ein Beispiel für einen Agent-Harness

Lösung ist: Selbst auf der individuellen Ebene generisch einsteigen, ...

- **Ein universelles Agenten-Tool** (Harness) statt vieler Spezialwerkzeuge
- **Selbst steuern** statt Blackbox mit eingeschränkten Anpassungsmöglichkeiten
- **Ein System** statt zahlreicher Lizenzen oder Abos
- Verwendung **hochschuleigener oder lokaler Modelle** statt fehlenden Datenschutzes und fehlender Informationssicherheit

Den Einstieg wie dies geht, bekommt ihr heute.

Ein Agent verfolgt autonom Ziele, statt Workflows abzuarbeiten.



- Nimmt seine Umgebung wahr.
- Verfolgt komplexe Ziele.
- Trifft auf Basis von Beobachtungen und Zielen eigenständig Entscheidungen über: nächste Schritte; Nutzung verfügbarer Werkzeuge
- Lernt potenziell aus Interaktionen.
- Arbeitet oft in einer Schleife (z.B. Beobachten – Orientieren – Entscheiden – Handeln).
- Nutzt interne Speicher ("Gedächtnis").
- Orchestriert eine Reihe von Tools (Software, APIs, Datenbanken), um Ziele zu erreichen.

Abgrenzung KI-Chatbot, KI-Assistent, KI-Agent

Achtung der Begriff Agent wird häufig auch für Assistenten verwendet!

KI-Chatbot

- **Eine Frage, eine Antwort**
- Generiert Text, Bilder, Code, ...
- Einsatz für Einzelanliegen
- Mensch initiiert und steuert den Dialog
- *Beispiel: Erläuterung eines Sachverhaltes*

KI-Assistent

- **Komplexere vordefinierte Tätigkeiten**
- Generiert Berichte, Präsentationen, Diagramme ...
- Einsatz für wiederkehrende komplexere Anliegen nach bestimmtem Schema
- Mensch konfiguriert, gibt Daten, nutzt Ausgabe
- *Beispiele: Deep Research von Perplexity, NotebookLM*

KI-Agent

- **Generische Bearbeitung von Aufgaben**
- Trifft Entscheidungen, ändert Dateien und Daten, agiert in anderen Systemen
- Einsatz für Aufgaben mit offenen Lösungswegen
- Mensch definiert den Auftrag, die Ziele, prüft und nutzt Ergebnisse
- *Beispiel: Analyse und Organisation von Datei- und Datenbeständen*

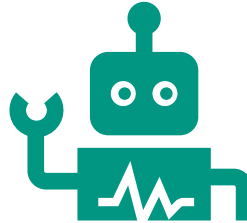
KI-Agenten: unterschiedlich eingesetzt



Klassische Workflows mit Agenten-Unterstützung

Agenten **helfen bei der Erstellung** von Prozessen/Anwendungen als klassischer Business-Prozess in vorhandenen Systemen.

*SAP Joule Studio: Ein **KI-Agent generiert Workflows** für die automatisierte Übertragung von Testergebnissen aus dem E-Prüfungssystem ins Prüfungsmanagement.*



Agenten-Anwendungen (selbstständig agierend)

Agenten **sind das Ergebnis** und werden eingesetzt. Die Agenten selbst können wiederum mit einem Agenten erstellt werden (siehe links).

*Ein **KI-Agent analysiert Rechnungen**, extrahiert Daten und schlägt Buchungssätze vor.*

Agentensysteme genutzt durch die Organisation



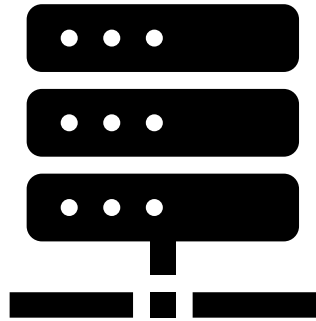
Lokale, generische Agentensysteme (individuelle Verwendung)

Agentic Harness **läuft lokal als generische Anwendung** und wird situativ und individuell in Tätigkeiten verwendet.

*VSCodium + Cline/Hermes: **Lokale KI-Agenten** analysieren Meeting-Protokolle, führen Code-Reviews durch oder extrahieren Wissen aus Projekt-Dokumentationen und erstellen strukturierte Zusammenfassungen – direkt auf dem Dateisystem.*

Individueller, generischer Einsatz von Agenten-Systemen

Die Zutaten für den Einstieg auf der individuellen Ebene



Inferenz per API

Modelle durch die Hochschule
bereit gestellt



Agentische Umgebung (Harness)

Cline in VsCodium/
Visual Studio Code



Vorgehensweisen und Tools

Eigene Kompetenz
in der Verwendung

Use Cases in Breakouträumen weiterdenken:

Der perfekte HIWI

Was ist Dein Traum-Agent? ... und was braucht dieser, um seine Aufgaben perfekt zu erledigen?

Arbeitsphase: 15 Minuten



Titel Deines Agenten



Welche **Ziele** verfolgst du mit Deinem Agenten?

Welche **Aufgaben** soll der Agent lösen?



Welche **Fähigkeiten und Qualifikationen** sollte Dein Agent mitbringen?



Welche **Tools und Schnittstellen**, sollten Deinem Agenten zur Verfügung stehen?

Titel Deines Agenten



Welche **Ziele** verfolgst du mit Deinem Agenten?

Welche **Aufgaben** soll der Agent lösen?



Welche **Fähigkeiten und Qualifikationen** sollte Dein Agent mitbringen?

Welche **Tools und Schnittstellen**, sollten Deinem Agenten zur Verfügung stehen?



Der perfekte HIWI

Ist nur so gut wie du steuerst!

Klare **Zielvorgabe**

Prompt gibt Ziel vor

Zuerst Vorgehen **planen** lassen,
dann **umsetzen**

Erst **Plan-** dann **Act-Modus**

Unverhandelbare **Vorgaben**
machen

Rules geben klare Regeln vor

Arbeitsanweisungen für häufig
benötigtes

Skills sind zu befolgende
Arbeitsanweisungen für öfters
benötigte Dinge

Arbeitswerkzeuge geben

Tools bereitstellen

Eine Aufgabe nach der anderen
(Kopf frei für neues)

Für neue Aufgaben neue Chats
anfangen (kein **Context-Rot**)

Ergebnisse prüfen und
**Zwischenergebnisse definieren und
vorlegen lassen**

Agent in kleineren in sich
geschlossenen Arbeitspaketen arbeiten
lassen (**Human in the Loop**)

Notwendiges **Material mitgeben**

Kontext für die Aufgabe in Form
von Dokumenten ...

Basis-Bestandteile des Harness und Ihre Bedeutung



Rules

als immer einzuhaltende Regeln, z.B. Projektkonventionen für Dateinamen und Verzeichnisstrukturen



Skills

als Fähigkeiten die häufiger benötigt werden, z.B. bestimmte Datenanalysen und für wiederkehrende feste Abläufe, z.B. Dokument konvertieren, analysieren, Analyseergebnisse als Bericht ablegen



Large Language Modell

die „Intelligenz“ eures Agenten. Bei der KI-Toolbox funktionieren gut die lokalen Modelle

`kit.qwen3.5-397b-A17b`

`kit.minimax-m2.7-229b`



Memory Bank

das Projektwissen eures Agenten über die einzelne Sitzung hinaus, z.B. um welches Projekt handelt es sich, was ist schon bearbeitet, was steht noch aus ...

Entwicklung von KI-Agenten: Verantwortungsvoll gestalten

Die neuen Risiken (Vom Chatbot zum Agenten)

Verlust der Kontrolle

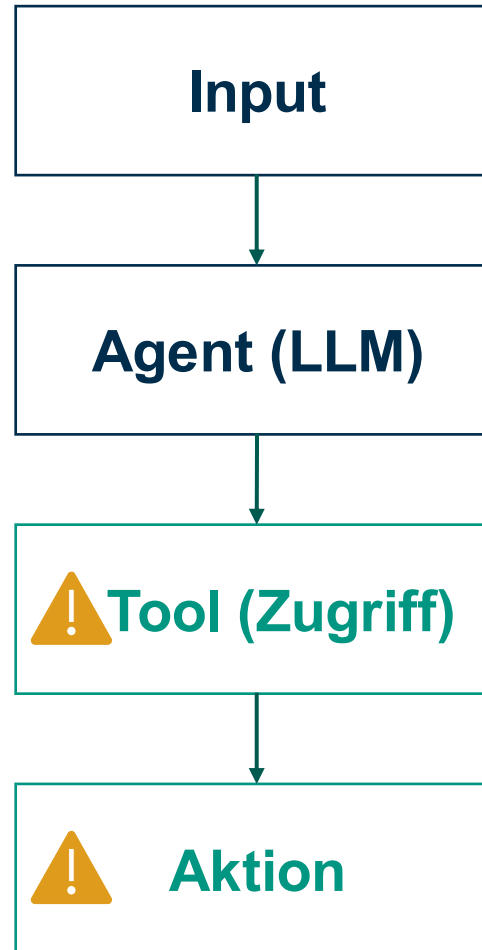
(Autonomie): Schleifen, ungewollte API-Aufrufe, halluzinierte Befehle

Datenabfluss an Dritte: externe LLMs, insbesondere bei sensiblen Forschungs- oder Personaldaten.

Indirect Prompt Injection: Verarbeitete Inhalte werden als Prompt interpretiert

Rechte-Eskalation: API-Key hat zu viel Zugriff.

Unkontrollierbare Kosten durch kontinuierliches "verbrennen" von Tokens



Best Practices (Security by Design)

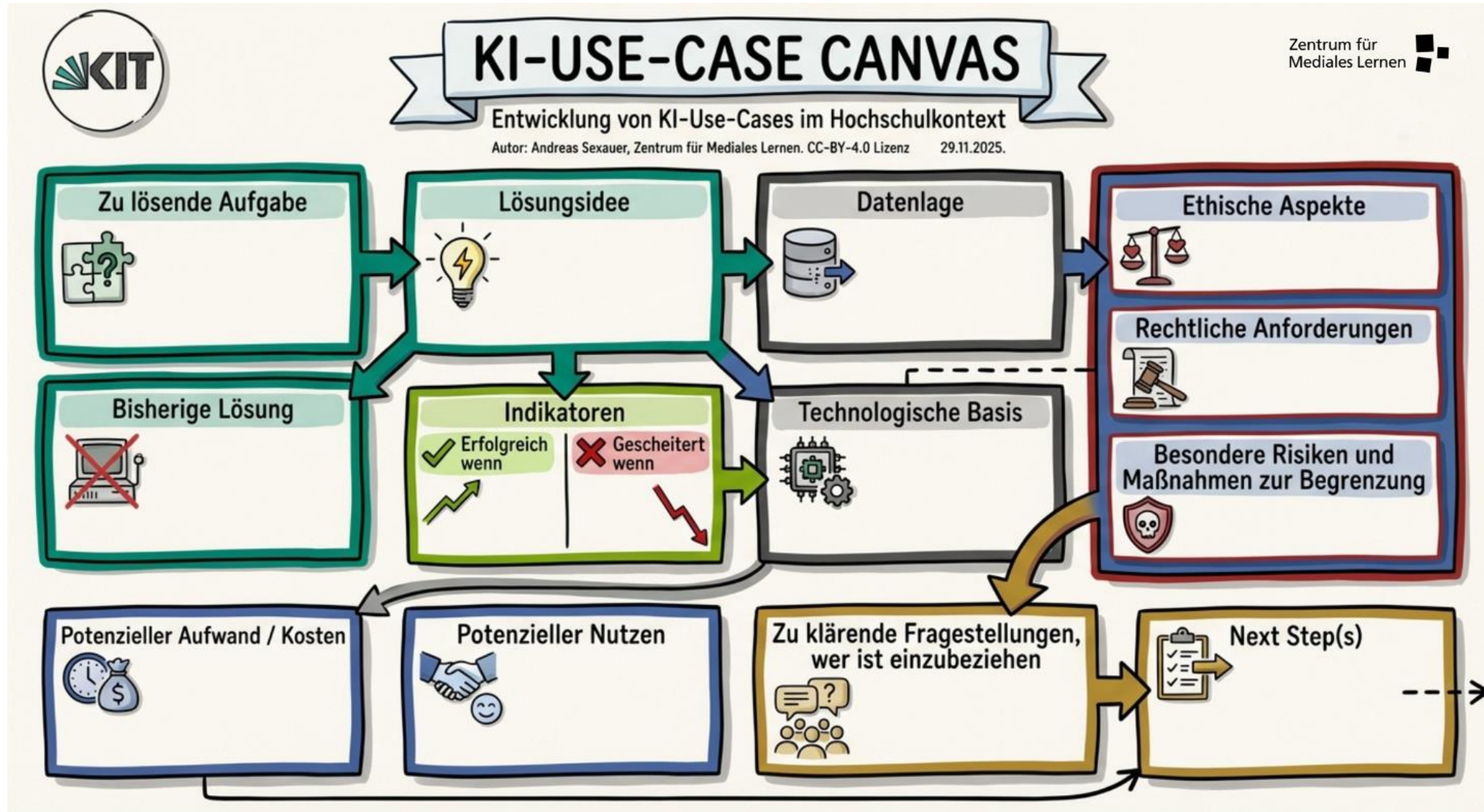
Human-in-the-Loop: Kritische Aktionen benötigen menschliche Bestätigung.

Principle of Least Privilege: Agenten haben nur die *absolut minimalen* Rechte, dedizierte Service-Accounts.

Sandboxing & Isolation: Agenten in Containern (Docker), ohne Zugriff auf interne Ressourcen, sofern nicht zwingend nötig.

Monitoring & Logging: Protokollieren Sie jeden „Thought“ und jede „Action“ des Agenten, um Fehlverhalten sofort zu erkennen.

Den Use-Case vollständig betrachten



Fragen/Diskussion?