

Herzlich Willkommen zur Online Session –
gleich geht es los

Agentic Coding im Data-Science-Kontext

Welche Rahmenbedingungen braucht es für den
sicheren und erfolgreichen Einsatz?

Experte

Martin Schneider

Chief Data Scientist





Agenda | Agentic Coding im Data-Science-Kontext

Einleitung & Hintergründe

Herausforderungen & Risiken

Potenzial im Data-Science-Kontext

FRAGEN & ANTWORTEN

Wir freuen uns auf Ihre Fragen im Chat.



„Unternehmen verfügen über große Datenmengen.

Wieso nutzen sie das darin enthaltene Wissen nicht besser?“

—

Oliver Bracht | 2010

Mitgründer & CEO



INFRASTRUKTUR

LÖSUNGEN

STRATEGIE

DATA SCIENCE & KI

Mit uns von der Vision bis zum Produktiveinsatz

Aus Daten Mehrwerte generieren

– branchenübergreifend von der öffentlichen Verwaltung bis zum Konzern



Als Teil der VIVAVIS AG sind wir spezialisiert auf die Anforderungen der kritischen Infrastruktur und regulierter Umgebungen.

Agentic Coding: Einleitung & Hintergründe

Agentic Coding – Definition

Agentic Coding bezeichnet einen Ansatz, bei dem **KI-Agenten eigenständig** komplexere Programmieraufgaben übernehmen – sie planen, schreiben, testen **über mehrere Schritte hinweg**, statt nur einzelne Codezeilen auf Zuruf zu generieren. Dabei greifen sie **selbstständig auf Tools** wie Terminals oder Dateisysteme zurück.

KI-gestütztes Programmieren – welche Varianten gibt es?



Chat-Support

KI als „Gesprächspartner“

Ansprechpartner bei Fragen oder Unsicherheiten



IDE-Integration

KI als „Assistent / Sekretär“

Von Code Completion bis zu vollständiger Skriptentwicklung

Tools: Posit Assistant, JetBrains Assistant, Copilot etc.



Agenten

KI als „Junior-Dev“

Umfassendes Coding, reviewen, pushen & ausführen

Tools: Codex, Claude Code, OpenCode etc.

KI-gestütztes Programmieren – welche Varianten gibt es?



Chat-Support



IDE-Integration



Agenten

Hoch

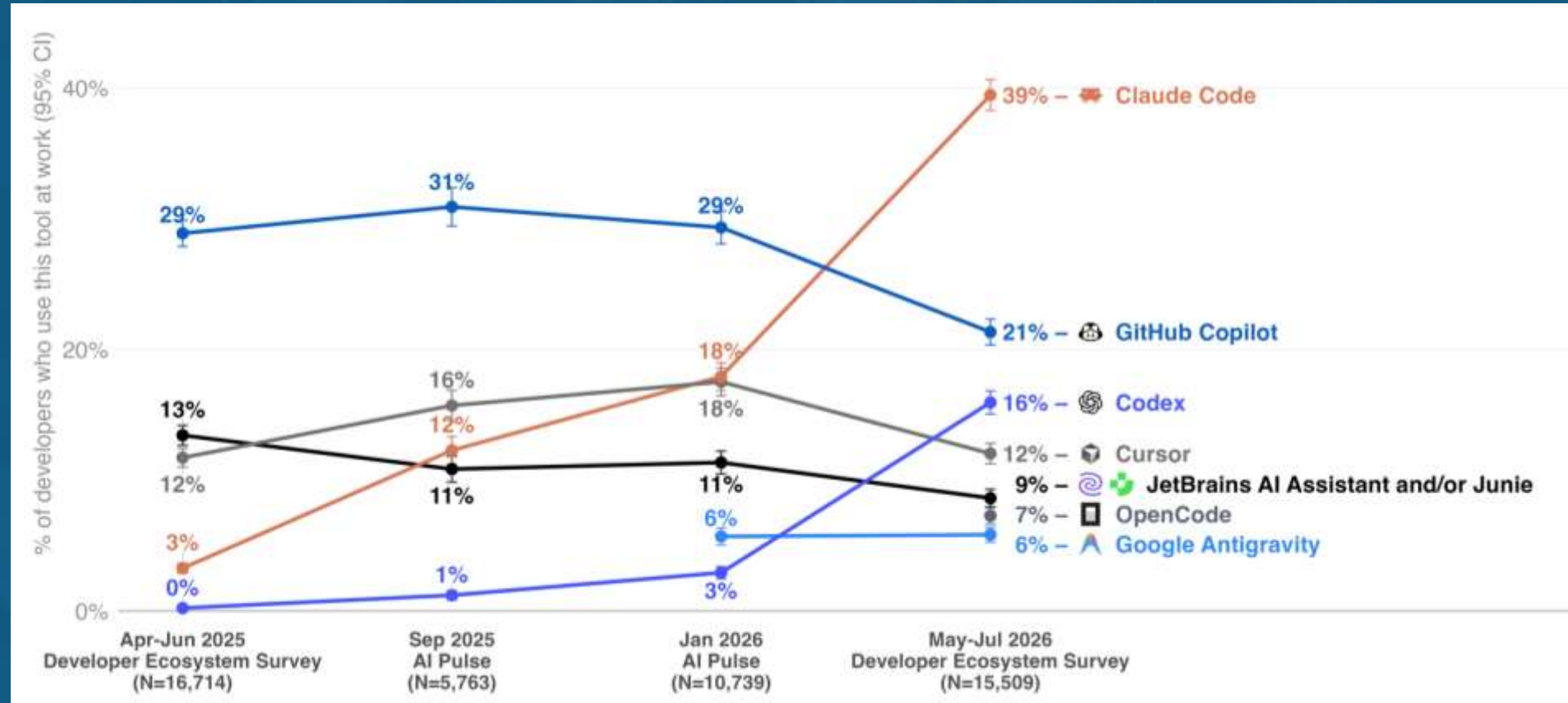
Niedrig

Handlungsautonomie der KI

Agentic Coding – die führenden Lösungen im Überblick



Welche dieser AI-Lösungen nutzen Sie für Coding- und andere Arbeitsaufgaben mit Entwicklungsbezug?



Agentic Coding - Effizienzgewinne

92%

der EntwicklerInnen berichten von
Produktivitätssteigerungen durch
den Einsatz von KI Coding
Assistenten*

8h

gewinnen EntwicklerInnen im
Schnitt pro Woche zurück durch
den Einsatz von KI*

Agentic Coding – Effizienzgewinne?

90%

der Entwicklerteams haben
Probleme mit KI-generiertem Code

52%

haben Engpässe bei der manuellen
Überprüfung des Codes

51%

haben Engpässe bei Sicherheitstests

48%

haben Engpässe bei der
Überarbeitung des Codes

Wie sich die Effizienz fördern lässt

Aufpassen, dass der eigene Produktivitätssprung nicht zu Lasten der KollegInnen geht, die die Ergebnisse kontrollieren und zurechtrücken müssen.



Agentic Coding – Effizienzgewinne?

Erfahrene EntwicklerInnen
profitieren, Nachwuchskräfte
erzielen keine messbaren
Produktivitätsgewinne.*



*

„Who is using AI to code? Global diffusion and impact of generative AI“ *Journal: Science*, August 2026

Wie sich die Effizienz fördern lässt

KI-Unterstützung aktiv und aufmerksam lenken, statt sie frei und ungesteuert laufen zu lassen – so lässt sich die Wartbarkeit fördern.



Agentic Coding: Herausforderungen & Risiken

Agentic Coding – Psychologische Belastung nimmt zu

41% of developers are „hooked“ on AI Coding*

EntwicklerInnen stimmen mindestens drei dieser vier Verhaltensweisen zu



Vergisst die Zeit bei
der Nutzung von KI-
Tools



Haben Schwierigkeiten
aufzuhören, wenn sie
einmal angefangen haben



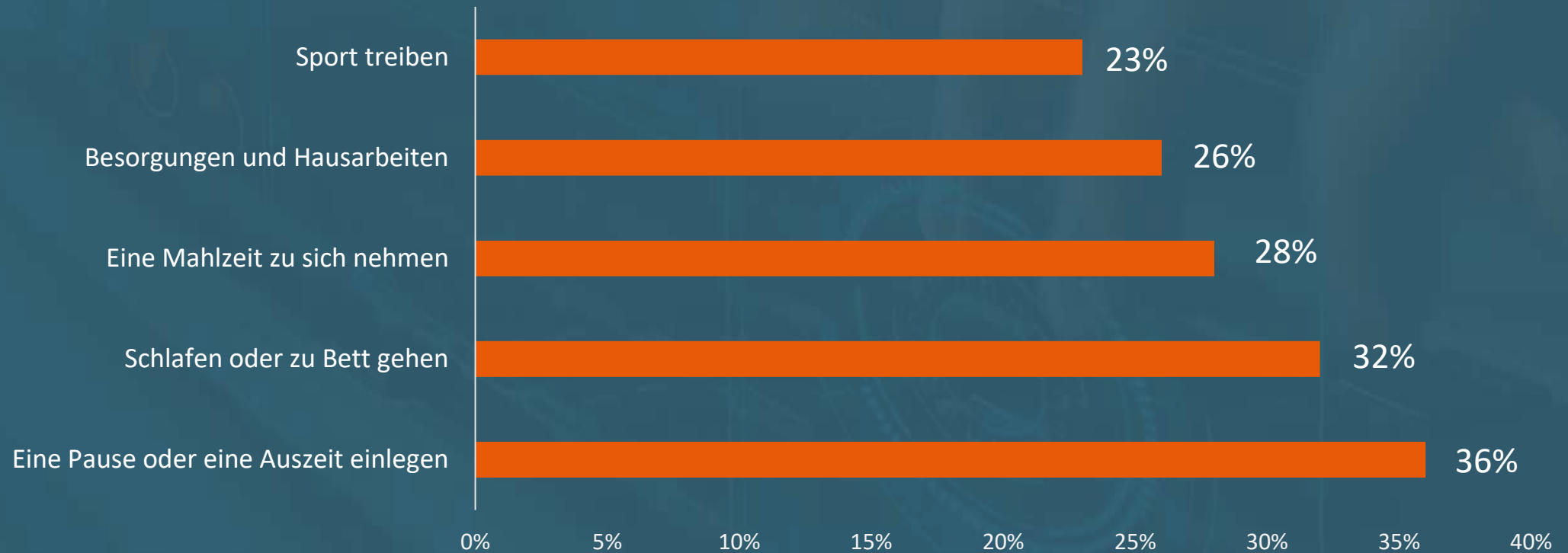
Programmieren nach
Feierabend weiter,
obwohl sie eigentlich
aufhören wollten



Sagen sich selbst
„nur noch eine
Runde“

Agentic Coding – Psychologische Belastung nimmt zu

Was EntwicklerInnen verschieben oder ausfallen lassen, um weiterzuarbeiten.



Agentic Coding: Allgemeine Risiken Sicherheit & Datenschutz



Unbeabsichtigter
Datenabfluss



Hosting- /
Souveränitätsfragen



Package Hallucinations /
Slopsquatting



Re-Identifikation trotz
„Anonymisierung“



Manipulierte Kontext-
Artefakte (Skills/Prompts) als
Angriffsvektor

Agentic Coding: Besondere Risiken im **Data-Science-Kontext**



Methodische
Grundregeln



Unsicherheiten durch
variablen Dateninput und
Phänomene wie Model-Drift



Bias erkennen und
vermeiden



Oftmals komplexere
Testfälle

Agentic Coding: Fallstricke und der richtige Umgang mit ihnen

FALLSTRICKE	LÖSUNGSANSÄTZE
Zugriff auf veraltetes Wissen	Metadaten pflegen
Fehlerhafter Code	Code Review durch KI-Agenten oder menschliche ExpertInnen
Ad-hoc / PoC-Niveau	Professionelle Standards festlegen
Unpassender Stil	AGENTS.md mit Vorlagen / Standards definieren



Data & AI Governance für Agentic Coding

1 Datenklassifizierung

Welcher Code und welche Kunden- oder Personendaten dürfen in welches Modell?
Klare Freigabestufen statt Einzelfallentscheidung im Entwicklungsalltag.

2 Tool- & Modellfreigabe

Geprüfte Werkzeuge, Hosting-Standort, Auftragsverarbeitung und AI-Act-Einordnung:
Positivliste verhindert Schatten-KI in der IDE.

3 Rechte & Sandboxing

Least Privilege für Agenten: abgegrenzte Umgebungen, kein direkter Produktivzugriff, Secrets außerhalb von Prompt und Kontextfenster.

4 Human-in-the-Loop

Definierte Freigabegrenzen: Review-Pflicht für generierten Code, kein automatischer Merge oder Deployment ohne menschliche Bestätigung.

5 Nachvollziehbarkeit

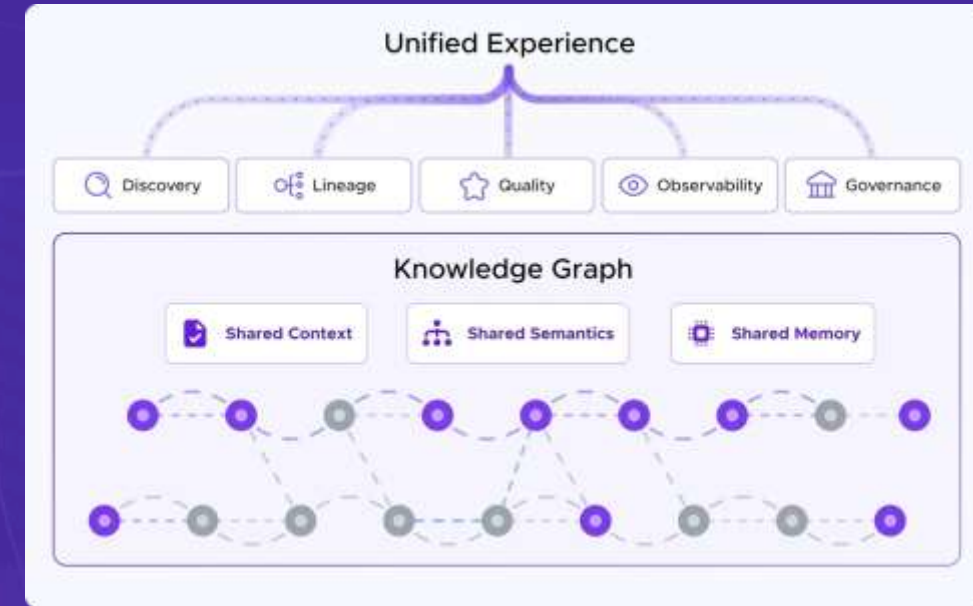
Kennzeichnung KI-generierter Anteile, Protokollierung von Prompts und Agentenaktionen, prüffähige Commit- und Entscheidungshistorie.

6 IP, Lizenzen & Security

Urheber- und Lizenzrisiken bewerten, Abhängigkeiten gegen erfundene Pakete prüfen, verpflichtende Security- und Testgates verankern.

Kontext als Lösungsbaustein: OpenMetadata

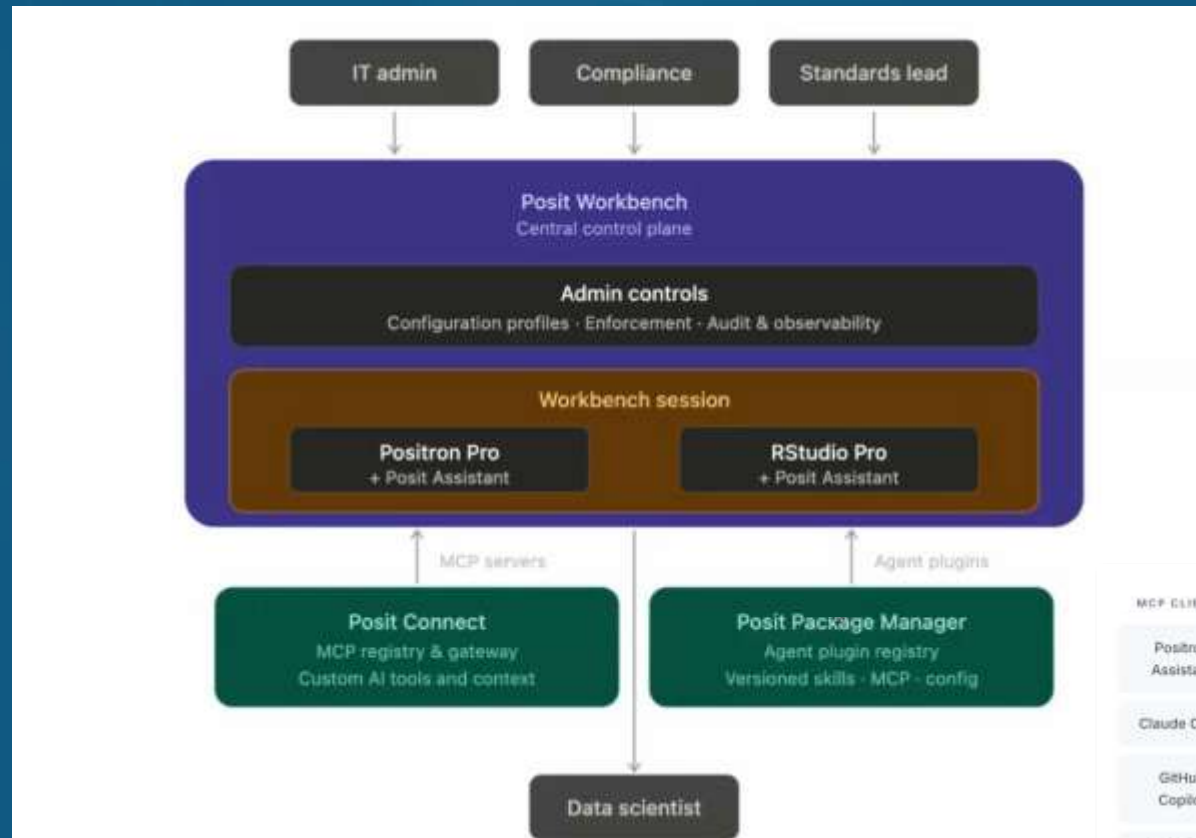
- Context Layer vereint drei Ebenen in einem gemeinsamen Graphen:
 - technischer Kontext (Schemas, Tabellen, Lineage)
 - Semantik (Glossar, Ontologien)
 - Memory (Entscheidungen, Audit-Trail) in einem gemeinsamen
- Schafft geteiltes Verständnis für Menschen und KI-Agenten was Daten bedeuten, woher sie kommen und ob sie vertrauenswürdig sind
- Governance & Security werden dadurch strukturell verankert: Klassifizierung, Owner, Freigaben und Auditierbarkeit sind Teil des Graphen, nicht nachträglich aufgesetzt



Bildquelle Open MetaData



Agentic Coding: Tools für mehr Sicherheit



Bildquelle Posit.co



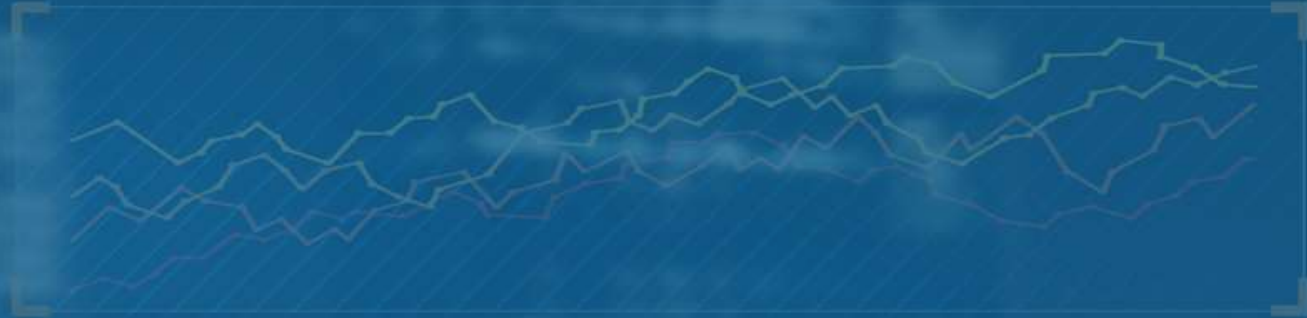
Posit-Demo: [AI Governance in Workbench](#)

Agentic Coding: Tools für mehr Sicherheit



A grid of 9 white cards, each with a header, a small icon, and a description of an Anaconda feature. The cards are arranged in a 3x3 grid.

- The Easiest Path to Production**
Pre-configured workstations, curated packages and models, and developer friendly APIs designed for fast iteration and reliable deployment.
- Anaconda Trusted Models**
Leverage a curated catalog of vetted open source AI models directly inside your workflow.
- Anaconda Packages**
Access thousands of vetted Python packages for trusted inputs into every workflow.
- Fast and Secure Data**
Bring scalable, cost-efficient compute to your existing data platforms.
- Compute to the Max**
Access GPUs and autoscaling compute through a unified, fully managed compute layer.
- Your Platform, Your Policies**
Define policies, secure environments, and tailor governance to your workflows.
- Guaranteed SLAs**
Deploy to production with consistent runtime across offline and online components, with full lineage and traceability at every step.
- Compliant by Design**
Your cloud, your chosen regions, with full support for HIPAA and SOC 2 compliance across every deployment target.
- Agentic AI Workflows**
Support ML pipelines, real-time inference, and agentic workflows, with the same governance and lineage throughout.



Investment banking



Agentic Coding:

Das Potenzial für Data Science

	TYD division			FRT division		
GHT	254	550	254	274	154	415
BDW	650	320	754	273	825	154
TRG	241	450	144	364	954	174
BTG	254	650	874	657	125	274
WEF	784	145	124	752	741	759
HRT	453	784	954	241	741	345



Der zentrale Grundsatz

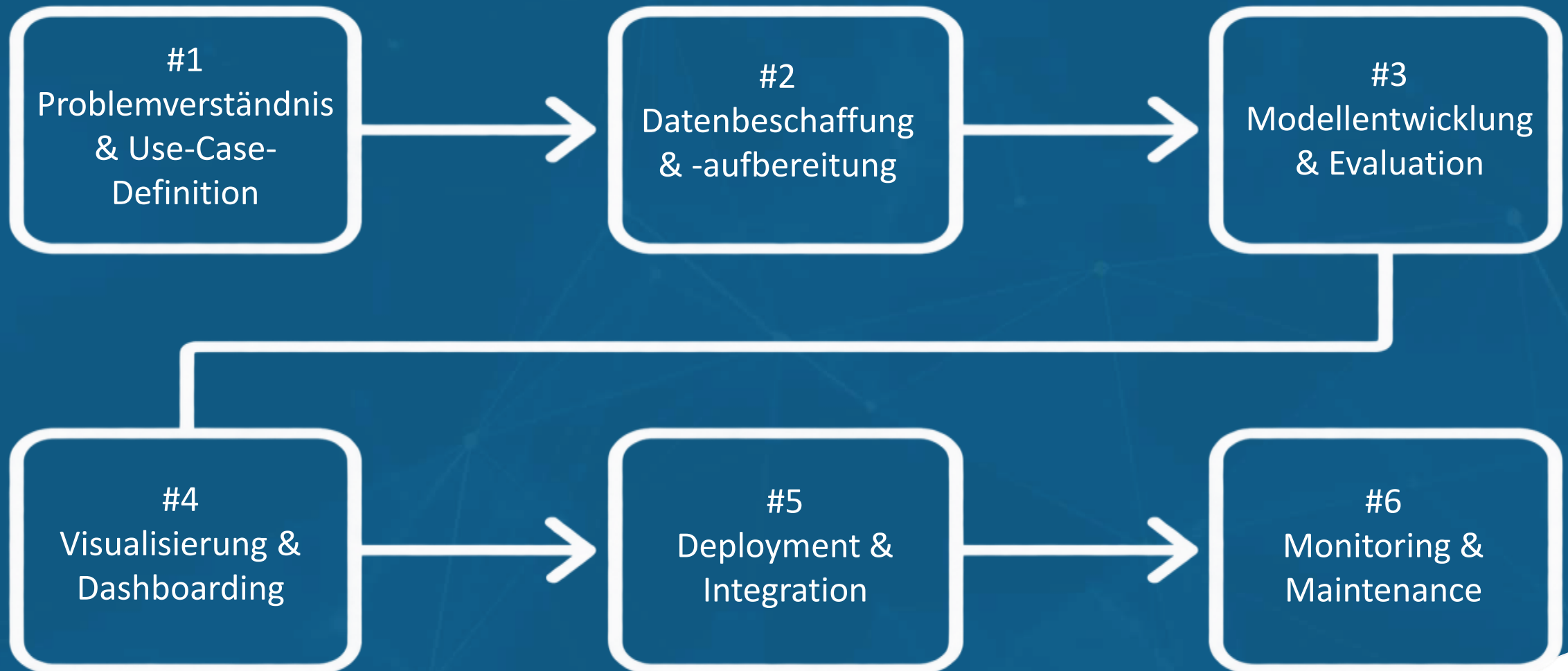
Analysis must be trustworthy and it must be shown to be trustworthy

- Correctness alone is not enough. It has to be demonstrable.
- Whoever receives your results has limited ability to verify them directly, so they have to trust the analysis, and the software behind it.



Agentic Coding:

Das Unterstützungspotenzial im Data-Science-Workflow



Agentic Coding:

Das Unterstützungspotenzial im Data-Science-Workflow

#1
Problemverständnis &
Use-Case-Definition

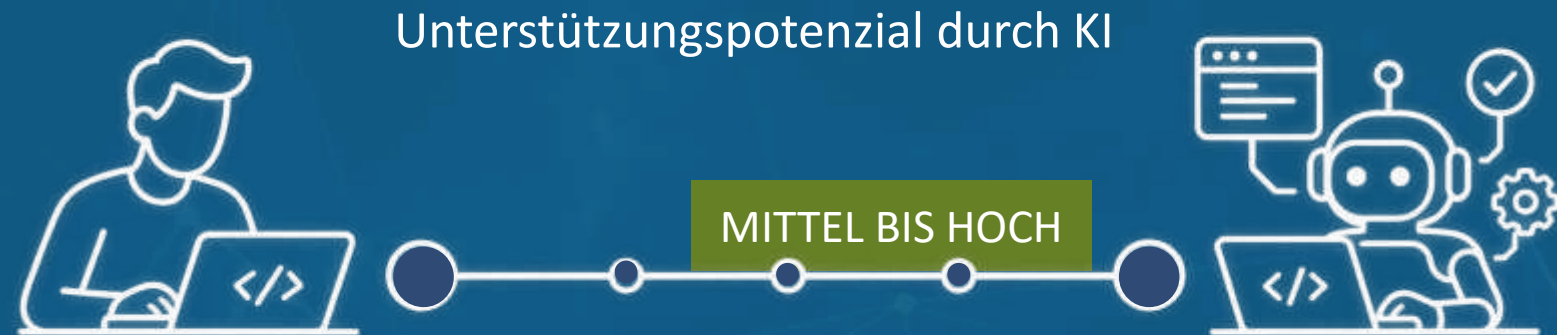


- Strategisch, Stakeholder-getrieben
- Im Fokus steht die Frage nach dem konkreten Problem
- Wenn Problem und Stakeholderanforderungen geklärt sind, hilft KI das Domänenwissen zu vertiefen und den Lösungsweg zu finden

Agentic Coding:

Das Unterstützungspotenzial im Data-Science-Workflow

#2
Datenbeschaffung & -
aufbereitung



KI-Unterstützungsmöglichkeiten

- Schnelle Nutzung von Schnittstellen zum Datenabruf
- Beherrschung von Standards im Data Cleaning (Missings, Filtern, etc.)
- Support bei der Aufbereitung unstrukturierter Daten (Texte, Bilder etc.)
- Schnelles Verständnis bekommen von neuen Daten

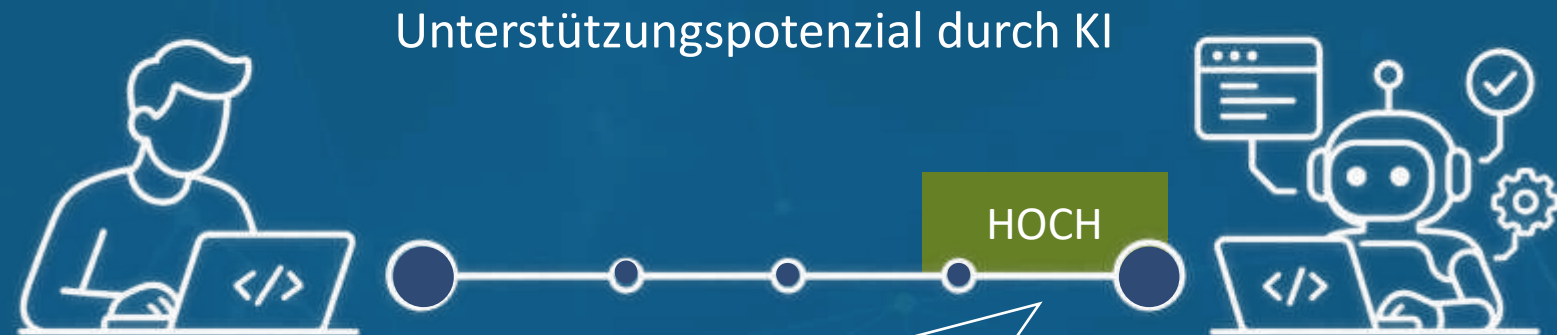
Sensible oder besonders spezifische Cases obliegen weiter den ExpertInnen

- Menschlicher Eingriff / Spezialwissen für Detailfragen nötig
- Austausch mit FachexpertInnen für Datenverständnis
- Restriktiver Zugang / Hochsensible Daten
- Datenauswahl

Agentic Coding:

Das Unterstützungspotenzial im Data-Science-Workflow

#3
Modellentwicklung &
Evaluation



KI-Unterstützungsmöglichkeiten

- Vertiefung des Domänenwissen
- Dynamische Iteration von Modellvarianten

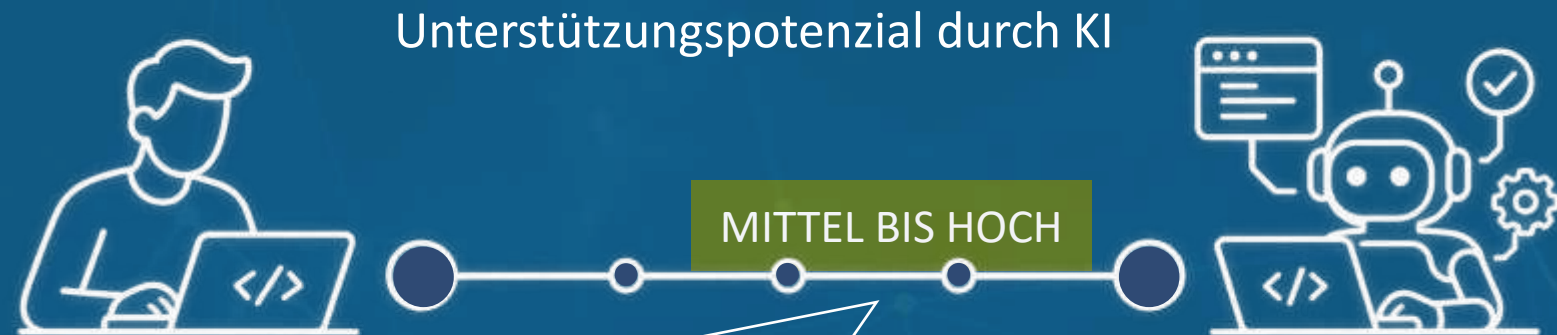
Auf was ist zu achten...

- Agenten setzen teilweise auf die am meisten verbreiteten Methoden, nicht zwingend die passendsten
- Evaluationsdatensatz – viel menschliche Kontrolle nötig, Agent unterstützt

Agentic Coding:

Das Unterstützungspotenzial im Data-Science-Workflow

#4 Visualisierung & Dashboarding



KI-Unterstützungsmöglichkeiten

- Abbildungen gut machbar
- Gute Prüf- und Anpassbarkeit
- Tests ebenfalls gut möglich

Auf was ist zu achten...

- Visualisierungen und Dashboards gelegentlich mit zu hoher Informationsdichte und zu ausgefallen
- KI-Stil/Layout ist Geschmacksache (Defaults nutzen sich ab)
- Manueller Feinschliff empfehlenswert

Agentic Coding:

Das Unterstützungspotenzial im Data-Science-Workflow

#5
Deployment &
Integration

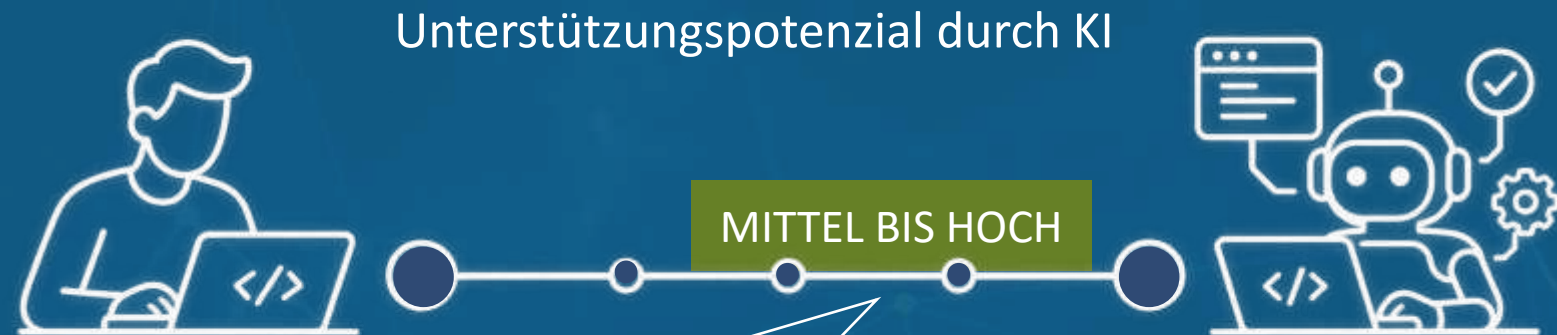


- KI-Unterstützungsmöglichkeiten
- viel Boilerplate automatisierbar
 - Pipelines und Funktionstests
 - Beratend bei
Infrastrukturentscheidungen

Agentic Coding:

Das Unterstützungspotenzial im Data-Science-Workflow

#6
Monitoring &
Maintenance



KI-Unterstützungsmöglichkeiten

- Einrichtung von Logging & Monitoringsystemen
- Zusammenfassung von Logs + Handlungsempfehlungen

Auf was ist zu achten...

- Besonderheiten/Hintergründe müssen mitgegeben werden (Events)
- Änderungsentscheidungen am Produktivsystem

Agentic Coding:

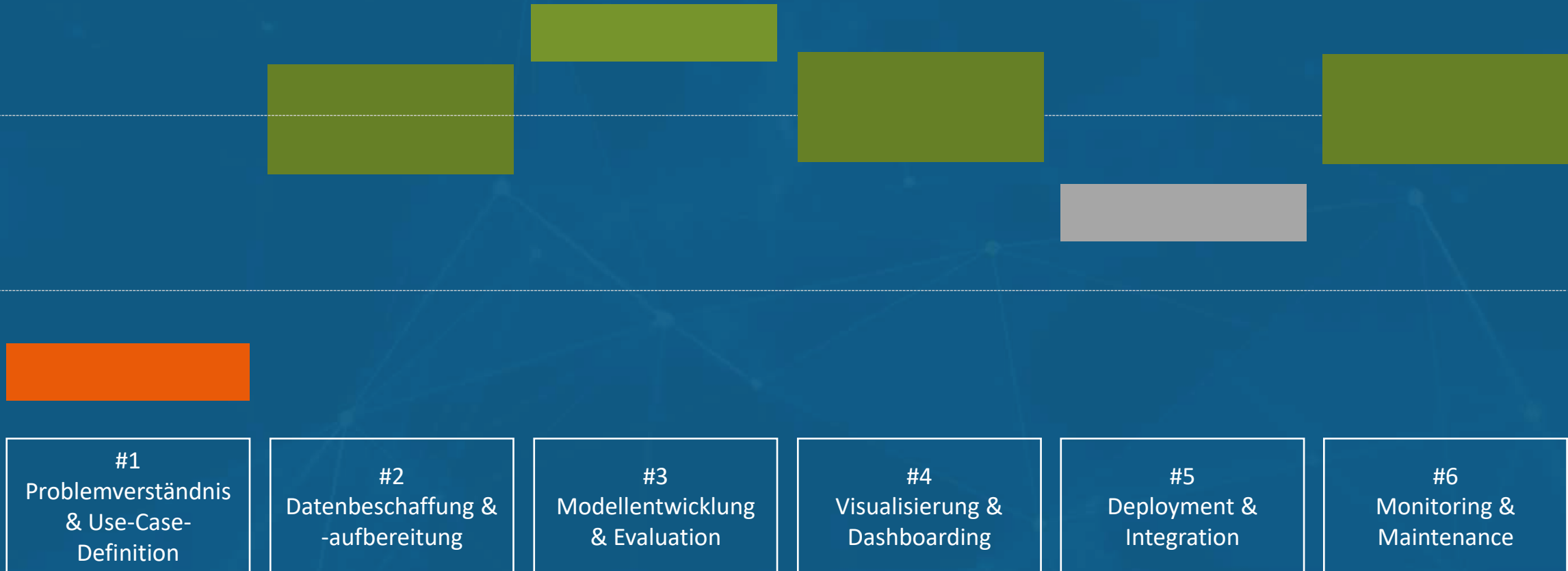
Das Unterstützungspotenzial im Data-Science-Workflow



Hoch

Mittel

Gering



KI-Coding-Agenten im Data-Science-Praxistest

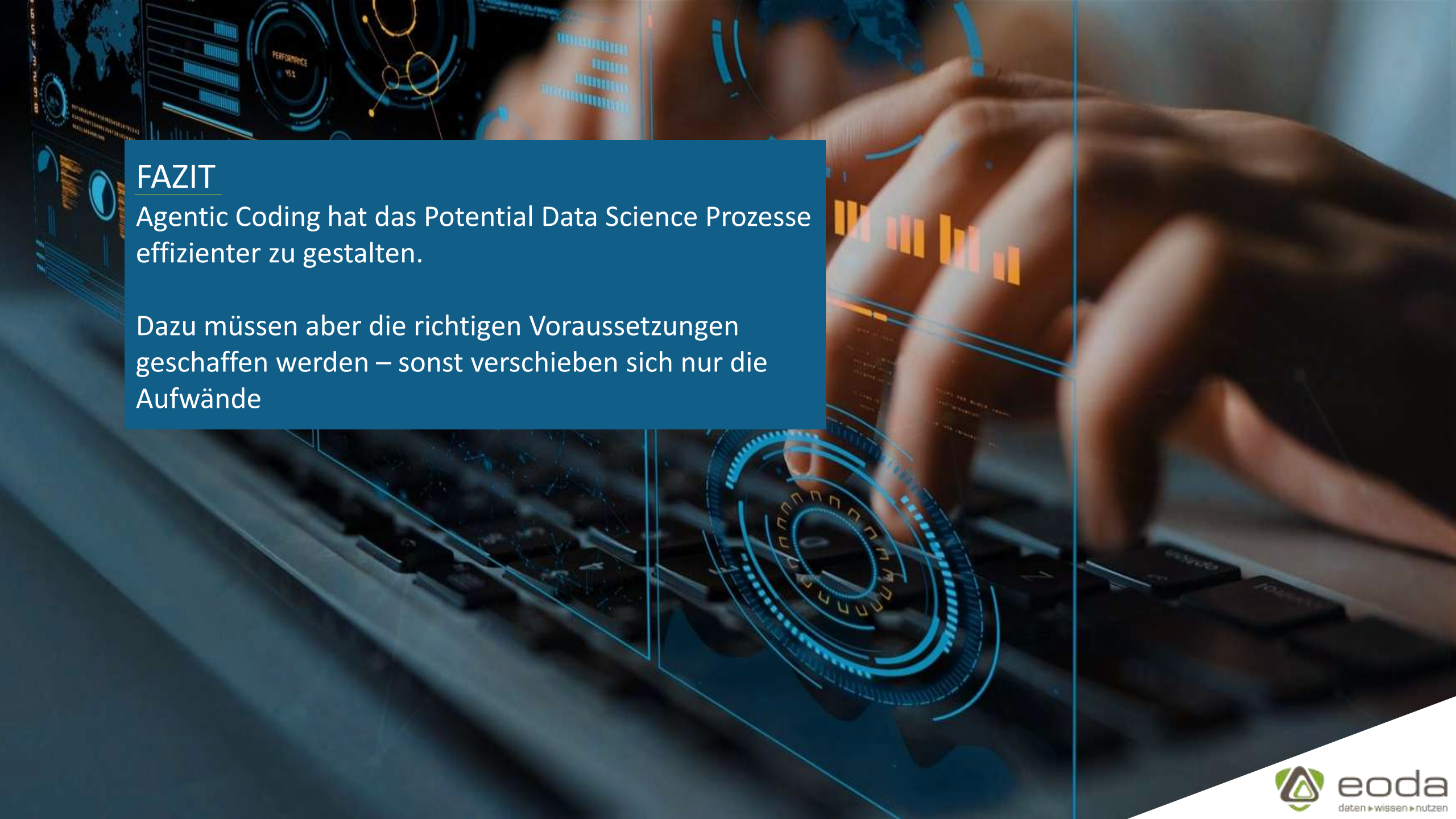
Claude Code, Codex, Junie und Posit Assistant im Vergleich

Aufgabe: Day-Ahead Prognose in der Energiewirtschaft

Fazit:

- Durchgehend positiver Gesamteindruck
- Ergebnisse sind noch ein Stück weit von einer direkt produktiv einsetzbaren Lösung entfernt
- Bemerkenswert: Keines der getesteten Tools hat im Test initial eine Methodenrecherche durchgeführt, um neuste Ansätze proaktiv in Erwägung zu ziehen





FAZIT

Agentic Coding hat das Potential Data Science Prozesse effizienter zu gestalten.

Dazu müssen aber die richtigen Voraussetzungen geschaffen werden – sonst verschieben sich nur die Aufwände



Code first, always

KI-Ergebnisse werden in Form von überprüfbarem, revidierbarem und versionsverwaltetem Code ausgegeben

Governed environments

Das System sorgt für die Einhaltung der Vorschriften, nicht der / die Einzelne

Agentic Coding im Data-Science-Kontext – produktiv und compliant. Wir unterstützen Sie dabei.



Beratung
Aufbau einer Data
Governance & KI-
Richtlinie



Training
Agentic Coding für
Data Scientists



Tools
Verkauf, Implementierung &
Betrieb von professionellen
Data-Science-Lösungen



Danke für Ihre Aufmerksamkeit.

Ihr Ansprechpartner für Ihren
Deep-Dive in die Daten

Martin Schneider

Chief Data Scientist

+49 561 87948-370

martin.schneider@eoda.de



eoda GmbH | Universitätsplatz 12 | 34127 Kassel

We are social

