Herzlich willkommen! Ihre Online-Session startet gleich.

Schön, dass Sie dabei sind. Hören Sie uns einfach per Kopfhörer oder Lautsprecher zu.

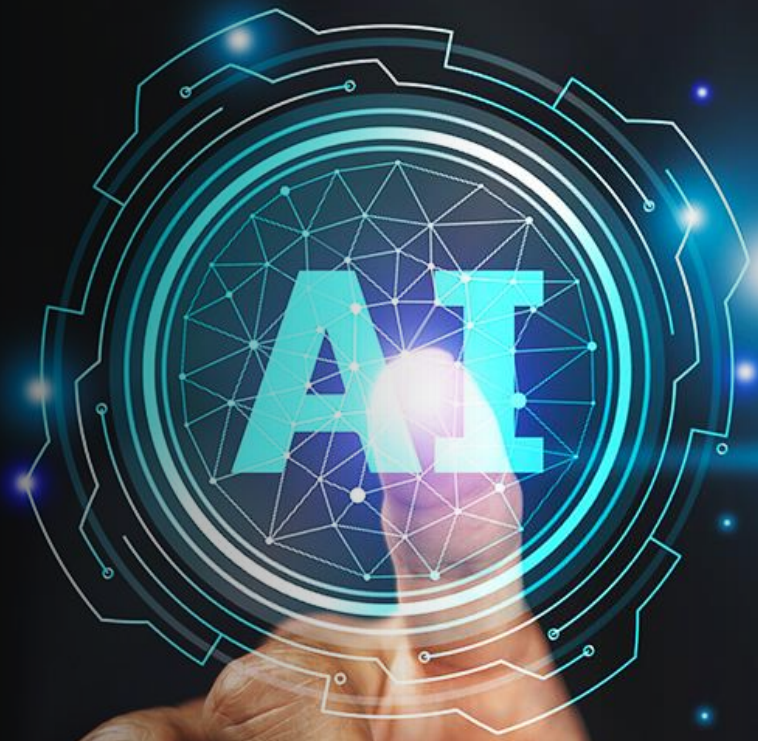
Wir schalten die Mikrofone der Teilnehmer:innen stumm. Dann hören Sie alles besser. Auch alle Webcams sind automatisch deaktiviert.

Ihre Fragen können Sie über das Fragen-Fenster stellen. Der/die Moderator:in bringt Ihre Fragen entsprechend ein.

Session wird aufgezeichnet

Educational Month |

Cyber Security



VODAFONE BUSINESS EDUCATION

Online-Session

Cyber Security im Zeitalter der KI: Strategien und Best Practices

26.09.2024

vodafone business

Herzlich willkommen!

Schön, dass Sie dabei sind. Hören Sie uns einfach per Kopfhörer oder Lautsprecher zu.

Wir schalten die Mikrofone der Teilnehmer:innen stumm. Dann hören Sie alles besser. Auch alle Webcams sind automatisch deaktiviert.

Ihre Fragen können Sie über das Fragen-Fenster stellen. Der/die Moderator:in bringt Ihre Fragen entsprechend ein.

Session wird aufgezeichnet

Heute für Sie dabei:

Fabian Flanhardt

PCG

Thomas Schmidt

PCG

PCG x Microsoft AI Security.

Security in der KI-Ära

Public Cloud Group

Ihr heutiger Referent.

Fabian Flanhardt
Head of Data/AI Microsoft

germany@pcg.io

Public Cloud Group

Fabian Flanhardt

Let's automate the world!

Ihr heutiger Referent.

Thomas Schmidt
CISO | Business Unit Director CaaS

thomas.schmidt@pcg.io

Public Cloud Group

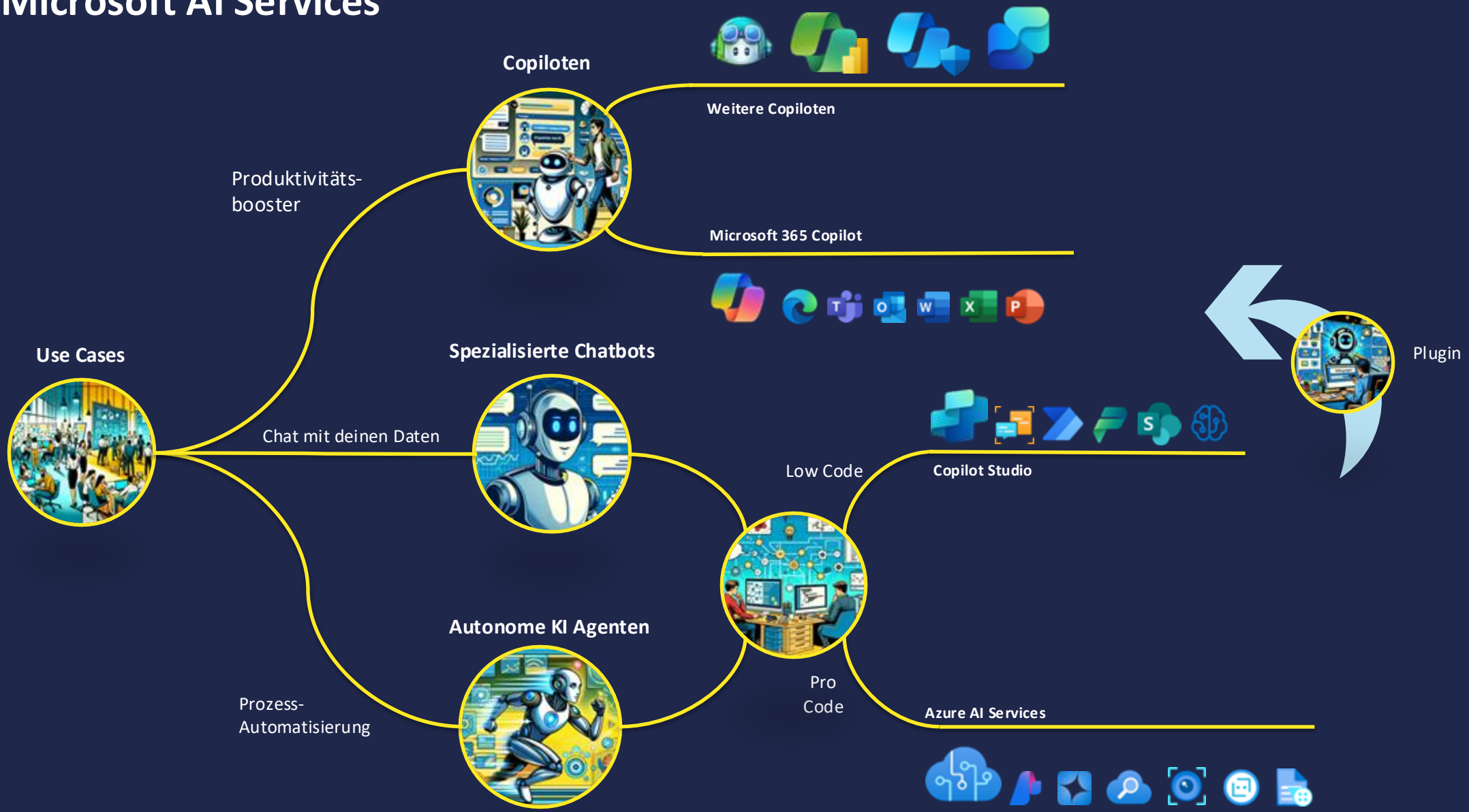
Thomas Schmidt

Business Architect | Trusted Advisor | CyberSec Expert | Pathfinder for your Cloud...

Portfolio.

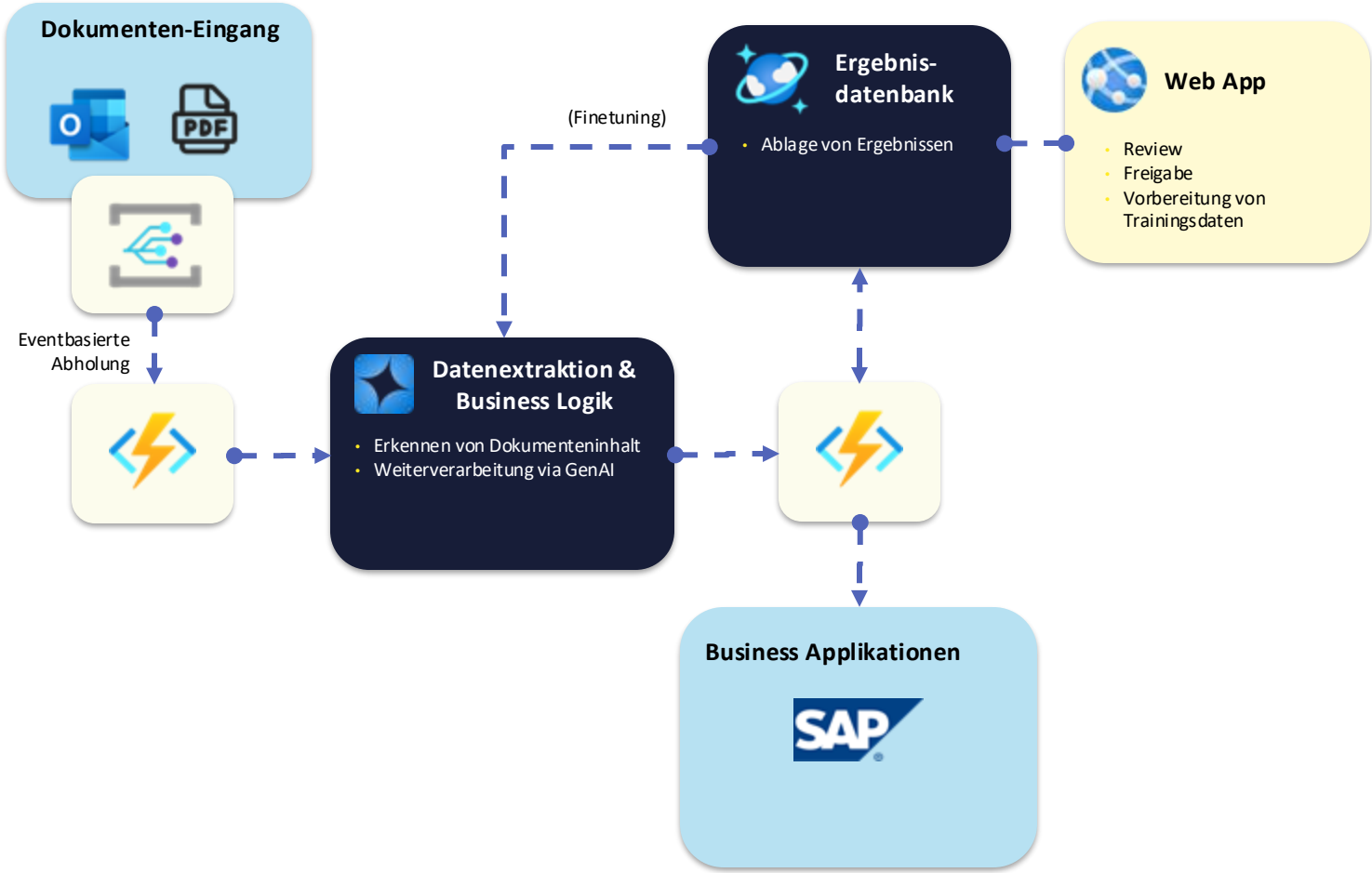
- Managed Cloud Operations (MCO)
- SAP Cloud Services
- Cloud Security
- Cloud Development
- Modern Workplace
- Public Cloud Consulting
- Data & AI

Microsoft AI Services



Autonomer KI-Agent

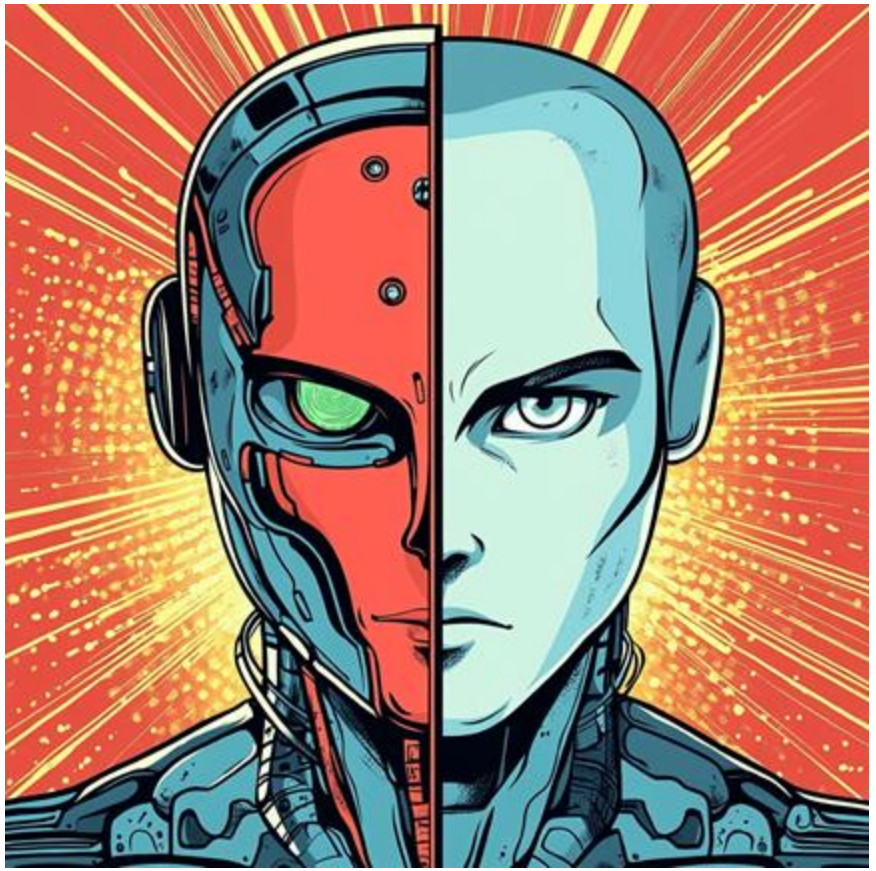
- Ki-gestützte Verarbeitung von unstrukturierten Dokumenten
- Emails inklusive Anhang
- PDF Dokumente



AI
Risiken

Generell werden zwei Risiken unterschieden:

- Risiken durch den **ungeplanten** Einsatz von AI
- Risiken durch **Manipulation** der AI



Azure AI Security & Compliance

Einsatzzweck:

- Absichern von Microsoft KI Services
- Vorbereitung und Begleitung von Audits

Erweiterte Security und Compliance Tools

- Prompt Shields für die Erkennung und das Blocken von Prompt Injections
- Groundedness detection um Halluzinationen aufzudecken
- Safety system messages um das Verhalten von Modellen zu steuern
- Safety evaluations um die Anfälligkeit für Jailbreak und andere Attacken zu identifizieren.
- Risk and safety monitoring für die überwachung von Content filtern

AI Compliance

- Compliance Prüfungen für Ki-relevante Anforderungen wie z.B. AI Act, IDW PS 861, BSI AIC4, ISO 23053 / 23894
- Unterstützung bei der Vorbereitung auf Audits

Co-Pilot for Security Operation Teams

- Nahtlose Einbindung des Co-Pilot Chatbot in die Microsoft Security Produkte: Defender XDR, Purview, InTune, Sentinel
- Bisher erst in USA verfügbar, Global Roll-Out soll zeitnah erfolgen

Guiding questions - Data Protection

Data Protection		Welche Art von Daten möchte ich verarbeiten (öffentlich, vertraulich, streng vertraulich)?
PII		Verarbeite ich personenbezogene Daten (persönlich identifizierbare Informationen)?
Corporate Data		Enthalten die Daten sensible Unternehmensinformationen?
Intellectual Property		Enthalten die Daten geistiges Eigentum?
Prevention		Welche Daten kann ich entfernen oder für die Weiterverarbeitung anonymisieren?
Decision		Meine Entscheidung, sollte ich die Daten mit einer KI-basierten Technologie verarbeiten?
Data Location		Wo werden die Daten verarbeitet und gespeichert?
Data Use		Wofür verwendet der Anbieter meine Daten?

IHRE FRAGEN.

Vielen Dank für Ihre Teilnahme!

Bei Fragen
melden Sie sich gern
bei Ihrem:r Vodafone-
Ansprechpartner:in.

Sie sind neu bei uns?
Schreiben Sie uns an
online.sessions@vodafone.com
eine E-Mail.

Die Aufzeichnungen und
Unterlagen aller Sessions
finden Sie hier.

TIMETABLE 2024

Educational Month Cyber Security

VODAFONE BUSINESS EDUCATION

KW 38

19.09. | 10:00 IT-Sicherheit ist Chefsache: Schützen Sie Ihre Unternehmenswerte und minimieren Sie die (persönliche) Haftung
Dr. Hauke Hansen (FPS Law)

20.09. | 10:00 KI-gesteuerte Security: Ende-zu-Ende-Sicherheit mit Microsoft
Andreas Wach (Microsoft)
Thomas Schmidt (PCG)

KW 39

24.09. | 10:00 Human Firewall – aus Sicht eines White-Hat-Hackers
Immanuel Bär (Prosec Networks)

25.09. | 10:00 Live Hacking: Die Methoden der Hacker und wie Sie sich gegen Ransomware Attacken schützen können
Lukas Garlik (Accenture)
Emil Stahr (Accenture)

26.09. | 10:00 Cyber Security im Zeitalter der KI: Strategien und Best Practices
Fabian Flanhardt (PCG)
Thomas Schmidt (PCG)

KW 40

30.09. | 10:00 Kampf der Ransomware! Wie Sie sich mit Zero Trust richtig schützen
Thanh Trieu (Zscaler)

Together we can

vodafone business