connexta
IT. Gemeinsam. Stärker.

Thema: Cyber AI – Next Level Netzwerksicherheit mit Künstlicher Intelligenz!

Marcus Junker, IF-Tech AG

Vorstand Anduras AG (Tochter der IF-Tech AG)

IF-Tech AG
Willy-Brandt-Allee 4
81829 München

Tel: +49 851 / 4 90 50-0

marcus.junker@if-tech.de

connexta
IT. Gemeinsam. Stärker.

Cyber AI

Next Level Netzwerksicherheit mit Künstlicher Intelligenz!

14. März 2024 | connexta Security Day | Marcus Junker, IF-Tech AG

Künstliche Intelligenz (KI) in der Cybersicherheit

connexta
IT. Gemeinsam. Stärker.

KI gilt als neue Herausforderung für die IT-Sicherheit

Welcher der folgenden Aussagen stimmen Sie am ehesten zu?

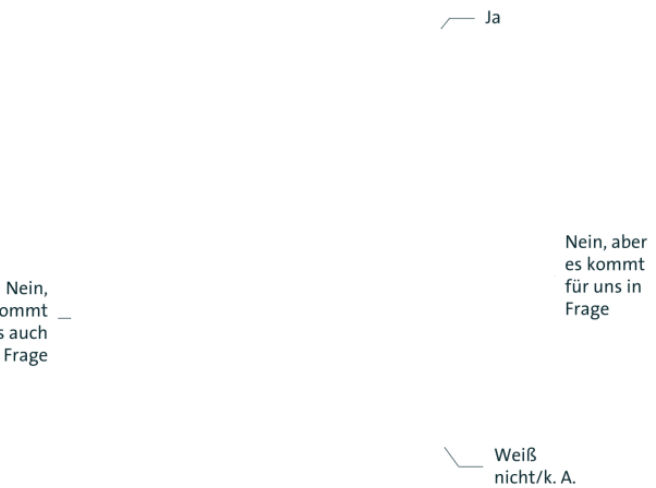
Die Verbreitung von generativer KI wird die **IT-Sicherheit verbessern**, weil sie bei der Abwehr von Cyberangriffen genutzt werden kann.

Die Verbreitung von generativer KI wird die **IT-Sicherheit gefährden**, weil sie von Cyberangreifern genutzt werden kann.

Basis: Alle Unternehmen (n=1.002) | nicht dargestellt: »Weiß nicht/k. A.« | Quelle: Bitkom Research 2023

bitkom

Haben Sie sich in Ihrem Unternehmen bereits mit dem Einsatz von KI zur Verbesserung der IT-Sicherheit beschäftigt?



in Prozent

Basis: Alle Unternehmen (n=1.002) | Quelle: Bitkom Research 2023

bitkom

Typen Künstlicher Intelligenz

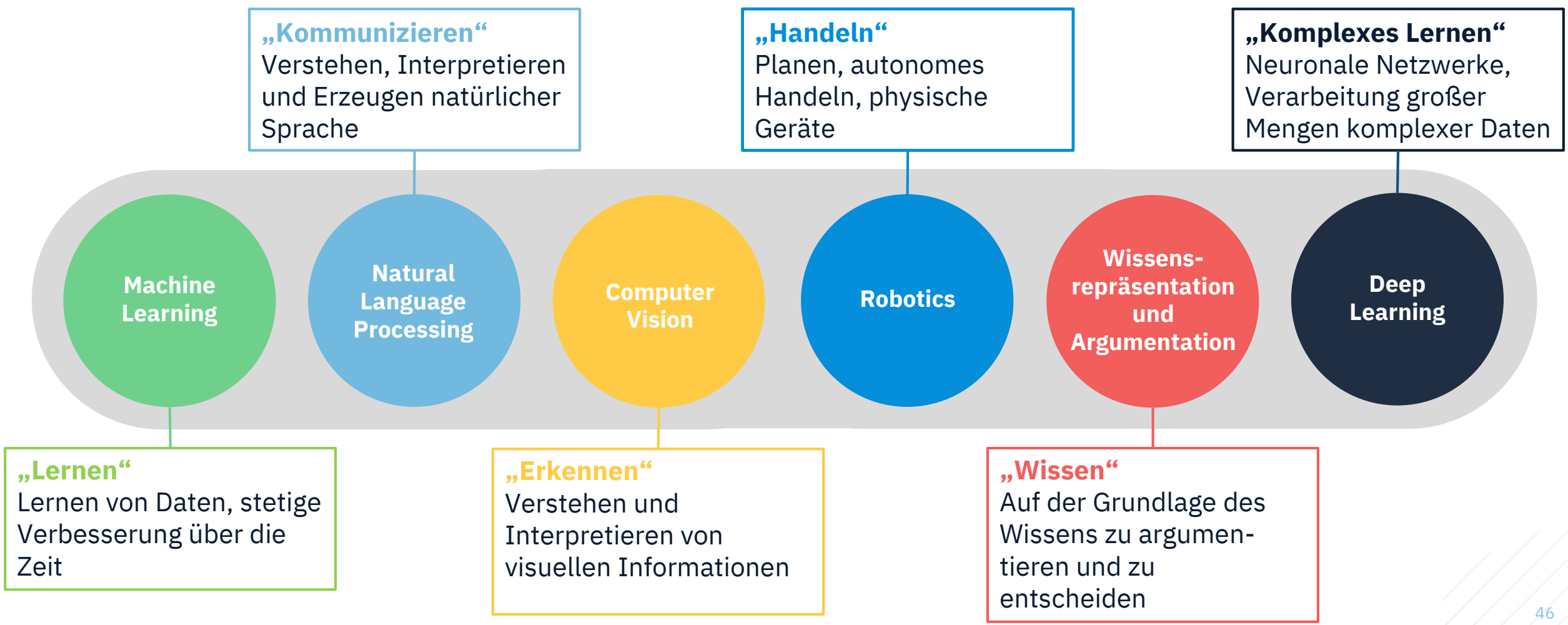
Von Artificial Narrow Intelligence zur Artificial Super Intelligence

connexta
IT. Gemeinsam. Stärker.

	Heute	2030-2070	???
KI-Stadium	 **Artificial Narrow Intelligence (ANI)**	 **Artificial General Intelligence (AGI)**	**Artificial Super Intelligence (ASI)**
Beschreibung	Auf die Ausführung bestimmter Aufgaben trainiert und ausgerichtet.	Fähigkeit, jede intellektuelle Aufgabe zu verstehen oder zu lernen, die ein Mensch ausführen kann.	Form der künstlichen Intelligenz, die die menschliche Intelligenz bei weitem übertreffen würde.

Klassifikation von KI-Systemen

„Fähigkeiten“ von KI



Gefahren und Risiken durch KI

connexta
IT. Gemeinsam. Stärker.

Gefahren und Risiken durch KI

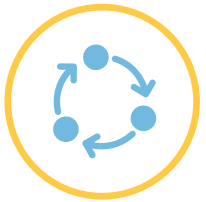
Potenzielle Gefahren KI-basierter Cyberangriffe

Phishing
Täuschend echte, individuell personalisierte KI-gestützte Phishing-Angriffe

Generative Adversarial Networks
Zu deutsch etwa „erzeugende gegnerische Netzwerke“, Optimierung Synthetischer Daten, Deepfakes

Deepfakes
Täuschen echt wirkende Foto-, Video- oder Sprachdateien

Data Poisoning
Einschleusung falscher Daten, um das Verhalten von ML-Modellen zu steuern



Adaptive Angriffe
KI-basierte adaptive „mitdenkende“ Malware mit dynamisch verändertem Code und Verhalten

Automatisierung
Schnelle und effiziente KI-unterstützte Automatisierung vieler Aufgaben bei Cyberangriffen

Passwort
KI-unterstütztes erraten von Passwörtern und lösen von Captchas

Prompt Injection
Einbettung bösartiger Anweisungen in die KI

Vorteile durch KI für die Cybersicherheit

connexta
IT. Gemeinsam. Stärker.

Chancen und Vorteile durch den Einsatz von KI-Technologien

Phishing-Erkennung

Erlernen von Kommunikationsmuster, Inhalte verstehen, Analyse von Anhängen und URLs

Vorhersage

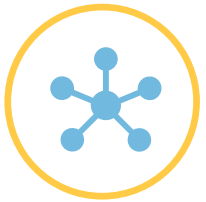
Vorhersage von Angriffen, Bedrohungen antizipieren bevor sie erfolgen

Datenerkennung und -kategorisierung

Daten und Umfeldanalyse: Qualität, Aktualität, Datenketten, ...

Automatisierung

Zeitersparnis bei Analysen, Automatisierung von Routineaufgaben

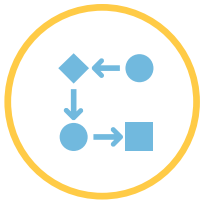


Bot Abwehr

Automatisierte Aufnahme und Analyse von Feeds, Verhaltensanalyse des Datenverkehrs

LLMs als Multiplikator

„Copilot“ Assistenten
Natürlichsprachliche Unterstützung von Sicherheitsanalysen



Sicherheitsorchestrierung

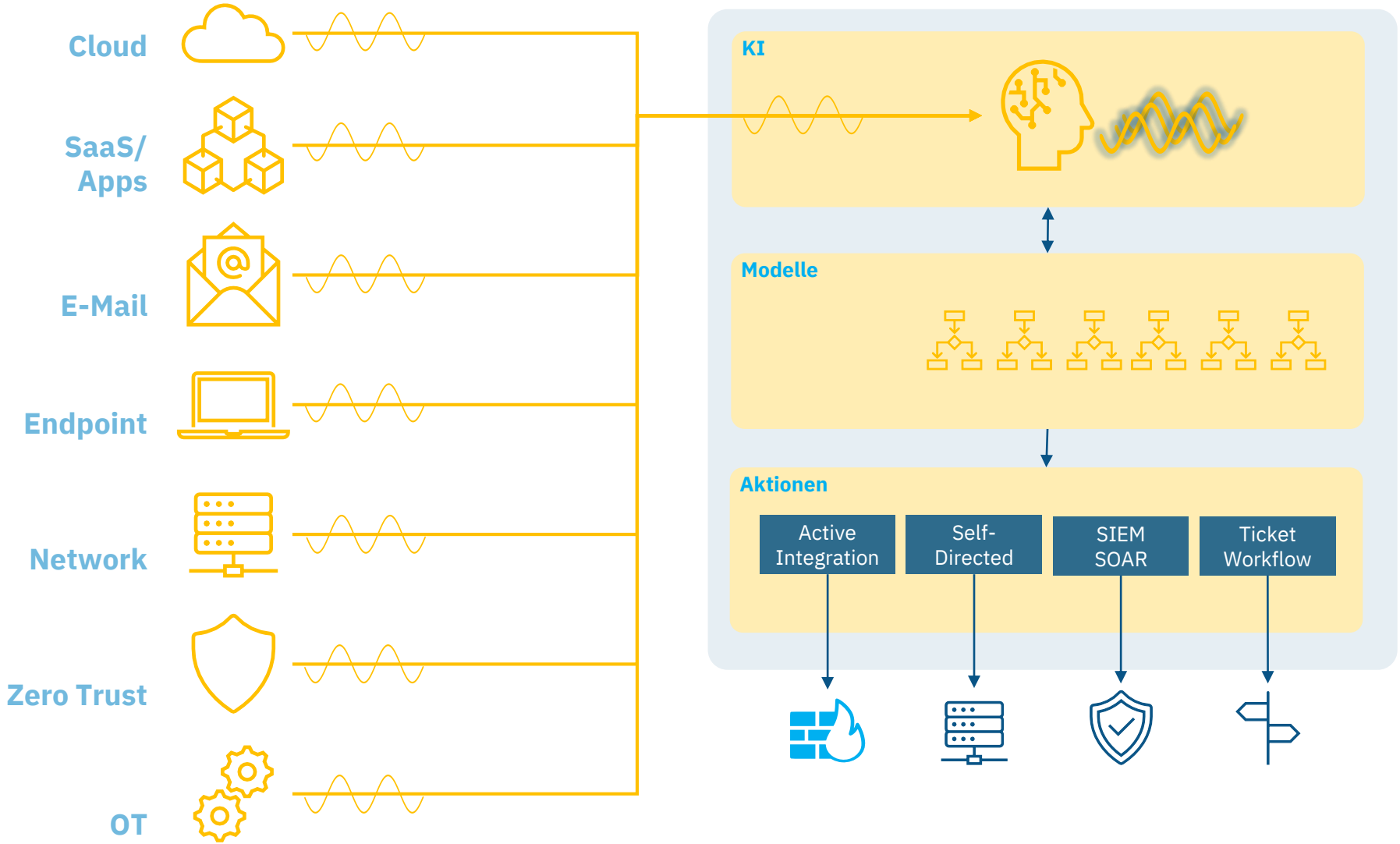
KI bei Security Orchestration Automation and Response (SOAR)

Verhaltensanalyse und Anomalie-Erkennung

Erkennung neuer Angriffsmuster oder Verhaltensweisen

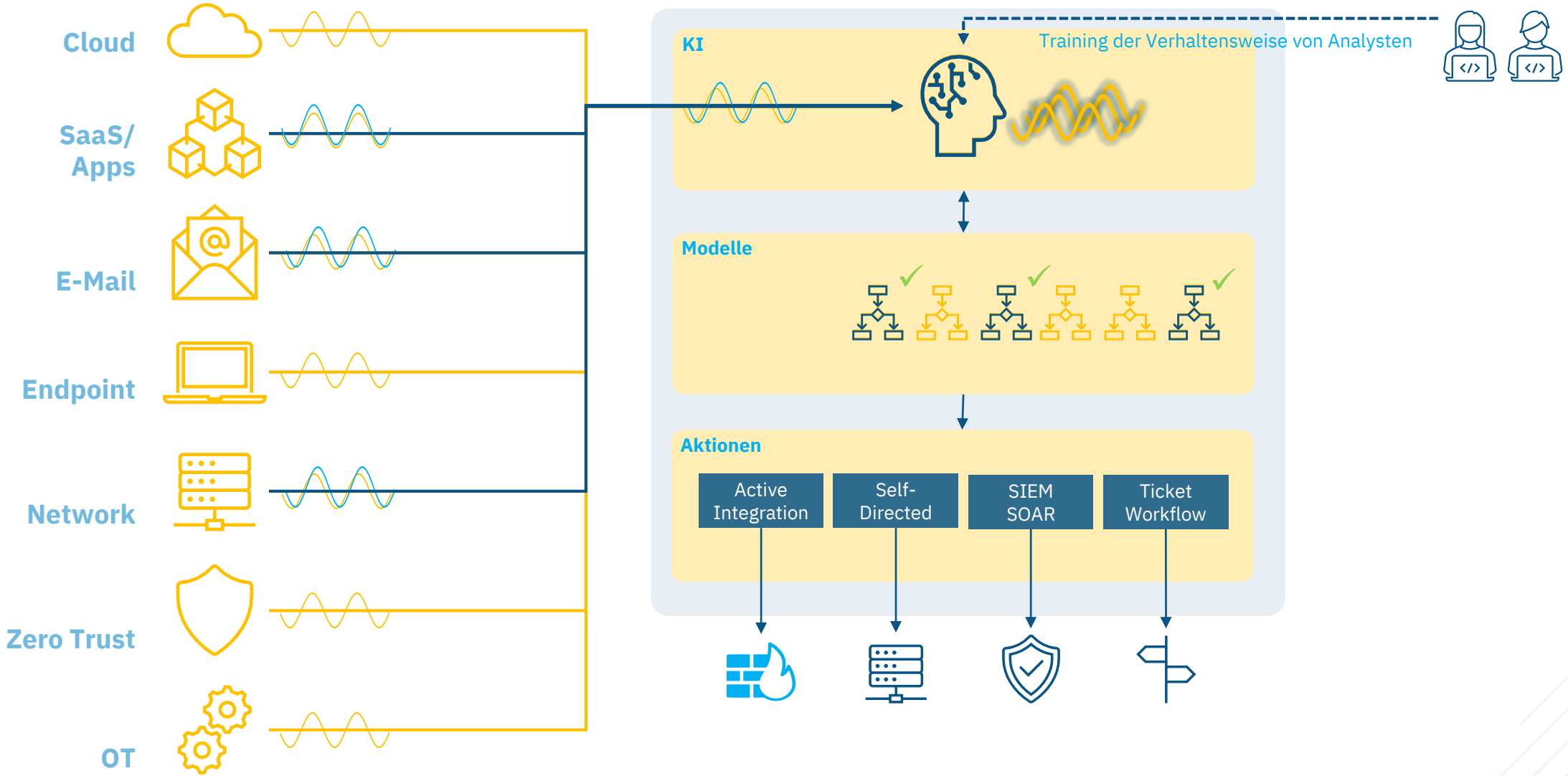
KI-basierte Anomalie-Erkennung

connexta
IT. Gemeinsam. Stärker.



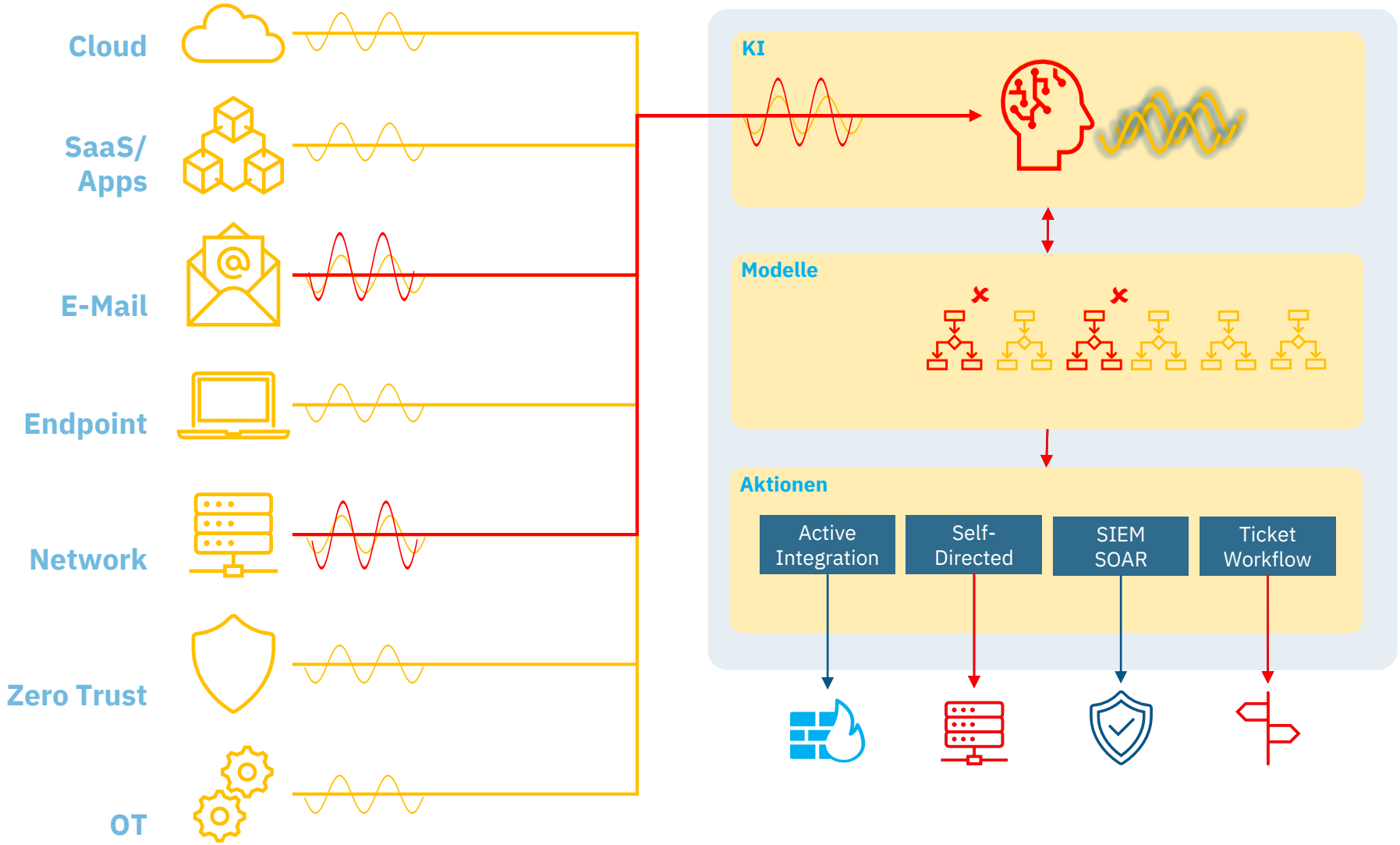
KI-basierte Anomalie-Erkennung

connexta
IT. Gemeinsam. Stärker.



KI-basierte Anomalie-Erkennung

connexta
IT. Gemeinsam. Stärker.



Zusammenfassung und Ausblick

connexta
IT. Gemeinsam. Stärker.

Vorteil durch Cyber AI: **Vorhersagen und Verhindern statt nur Erkennen**

Die Zukunft der Cybersicherheit wird von KI angetrieben sein.
Auf beiden Seiten: Angreifer und Abwehr!

Ausblick: **KI-Manipulation, Fortgeschrittene KI-Technologien, KI gegen KI**

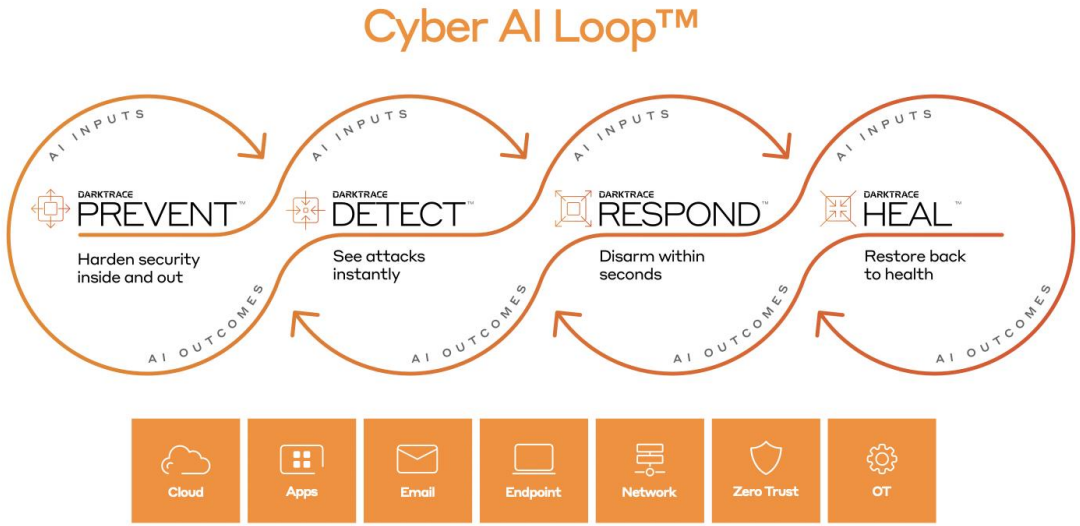
Demo-Time

Cyber AI im Einsatz

connexta
IT. Gemeinsam. Stärker.

Microsoft

DARKTRACE



connexta
IT. Gemeinsam. Stärker.

Fragen?

Sprechen Sie mich an!

Marcus Junker, IF-Tech AG