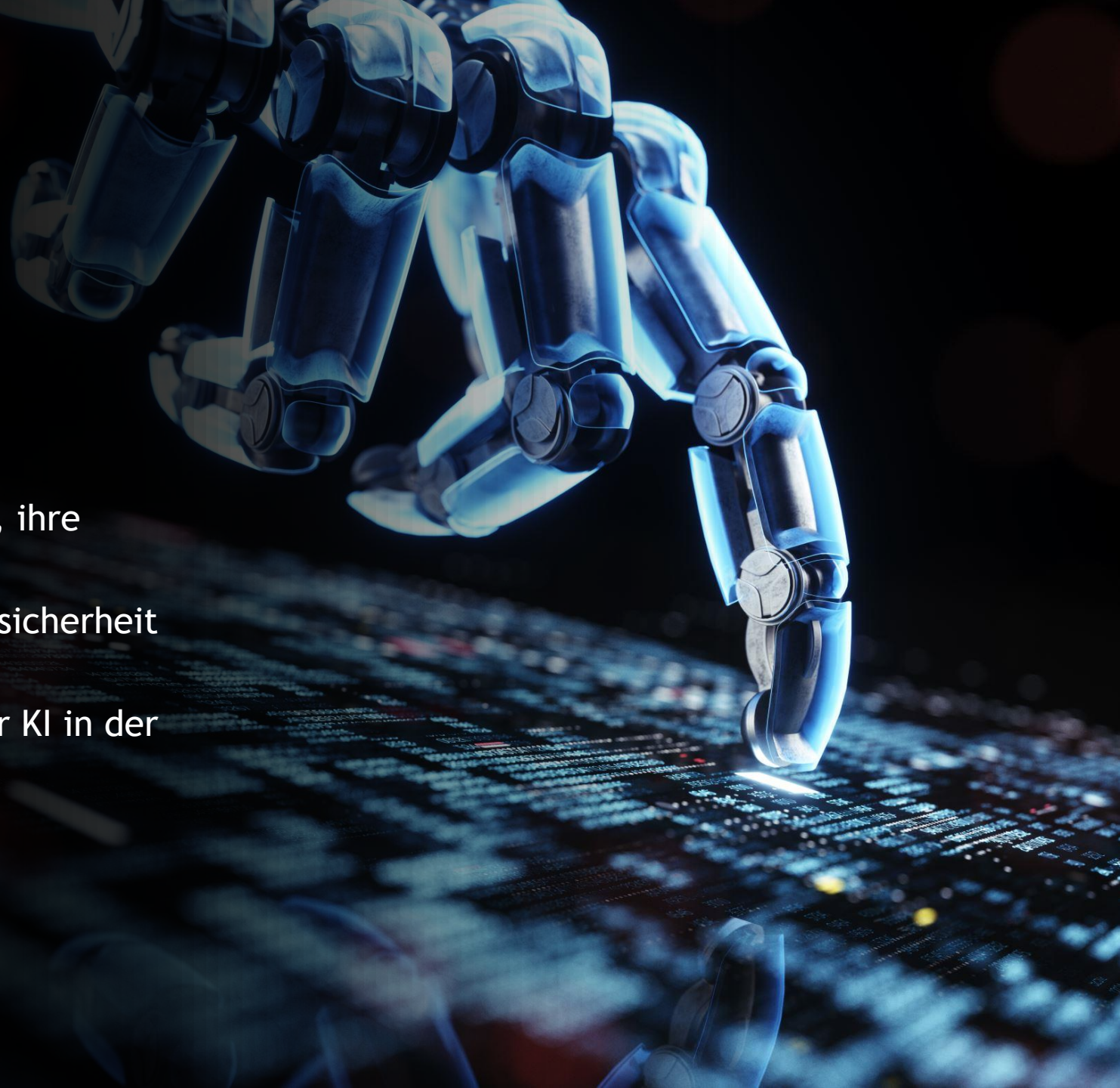
Einsatz von KI zu Erhöhung der Cyber Resilienz

Stefan Marzohl

Srt – 31.10.203

Agenda

- Beantwortung folgender der Fragestellungen
  - Warum tun sich Organisationen schwer, ihre Cyber-Resilienz zu verbessern?
  - Wie kann die Nutzung von KI die Cybersicherheit verbessern?
  - Was sind einige praktische Beispiele für KI in der Cybersicherheit?
- Herausforderungen und Überlegungen
- Zukünftige Trends für AI in Cyber-Security
- Q & A

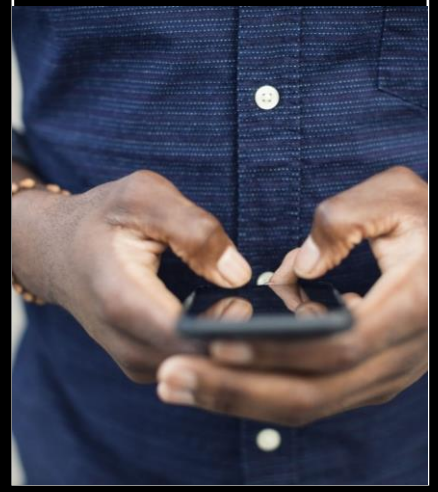
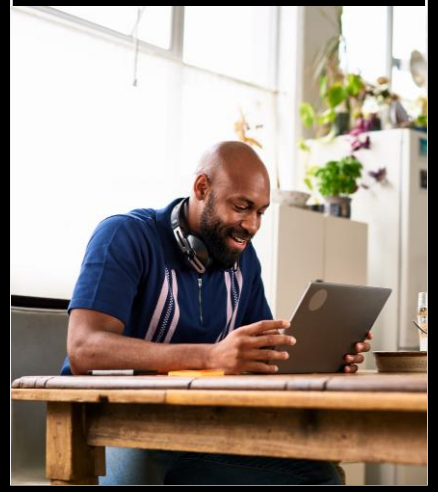


Agenda

- Beantwortung folgender der Fragestellungen
  - **Warum tun sich Organisationen schwer, ihre Cyber-Resilienz zu verbessern?**
  - Wie kann die Nutzung von KI die Cybersicherheit verbessern?
  - Was sind einige praktische Beispiele für KI in der Cybersicherheit?
- Herausforderungen und Überlegungen
- Zukünftige Trends für AI in Cyber-Security
- Q & A

Wachsende Cyber-Bedrohungslandschaft

Die Häufigkeit und Raffinesse von Cyberangriffen nimmt zu.

Vergrösserung der Angriffsfläche	Daten Overload	Arbeiten von irgendwo	Lieferkette & Dritt-partei Disruption	Regulatorische Compliance
				

Definition von Cyber-Resilienz

- Fähigkeit, sich auf Cyberangriffe vorzubereiten, darauf zu reagieren und sich davon zu erholen.
- Schutz vor fortgeschrittenen Bedrohungen
- Minimierung von Ausfallzeiten und finanziellen Verlusten
- Wahrung des Kundenvertrauens und des guten Rufs

Haben Sie Ihr Geschäftsrisiko vollständig im Griff?

In der gesamten Organisation, einschließlich der Lieferkette

Können Sie Ihre Sicherheit und betriebliche Effizienz messen?

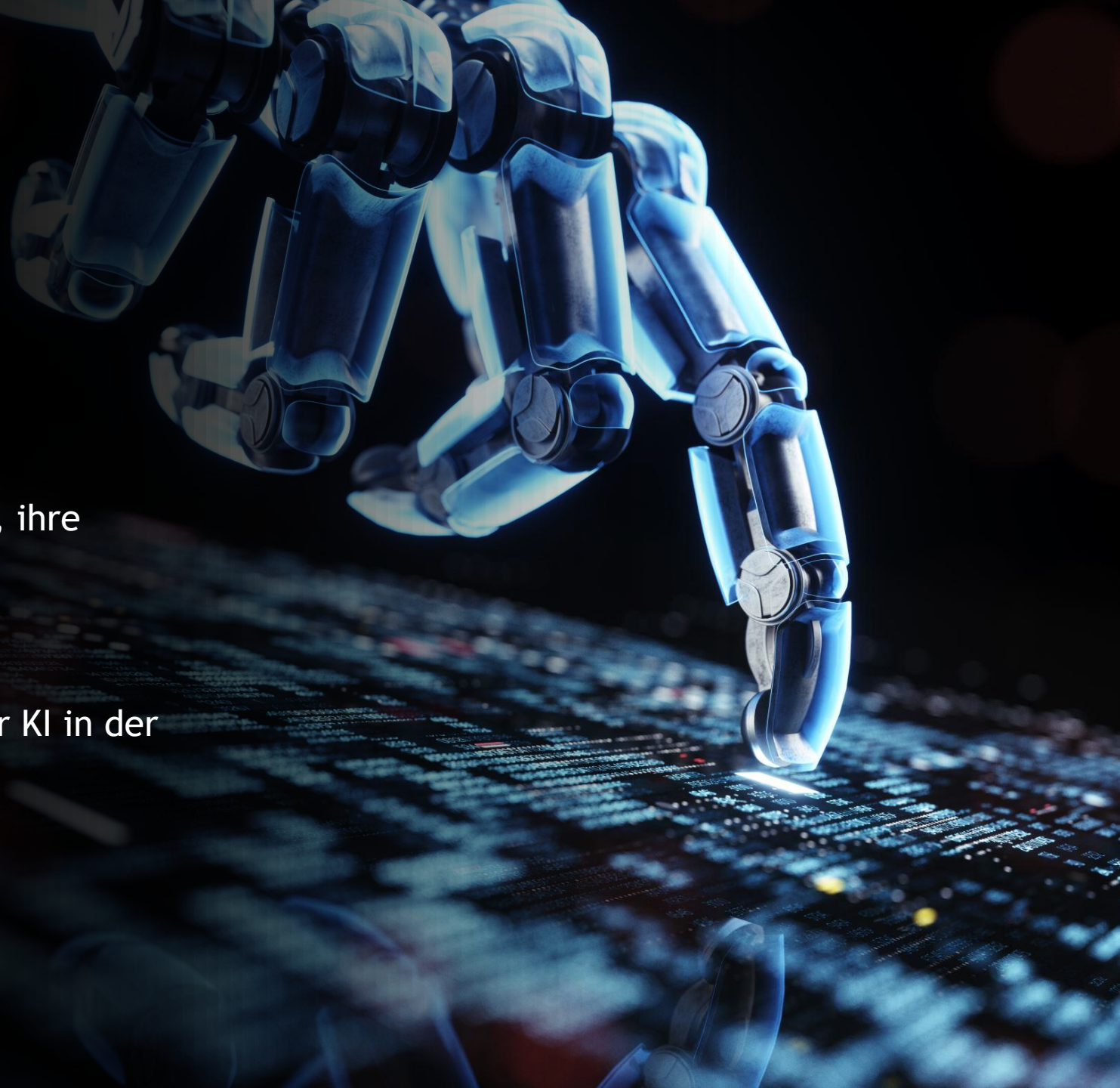
Behebung von Schwachstellen mit hohem Risiko und Verhinderung bekannter/unbekannter Bedrohungen

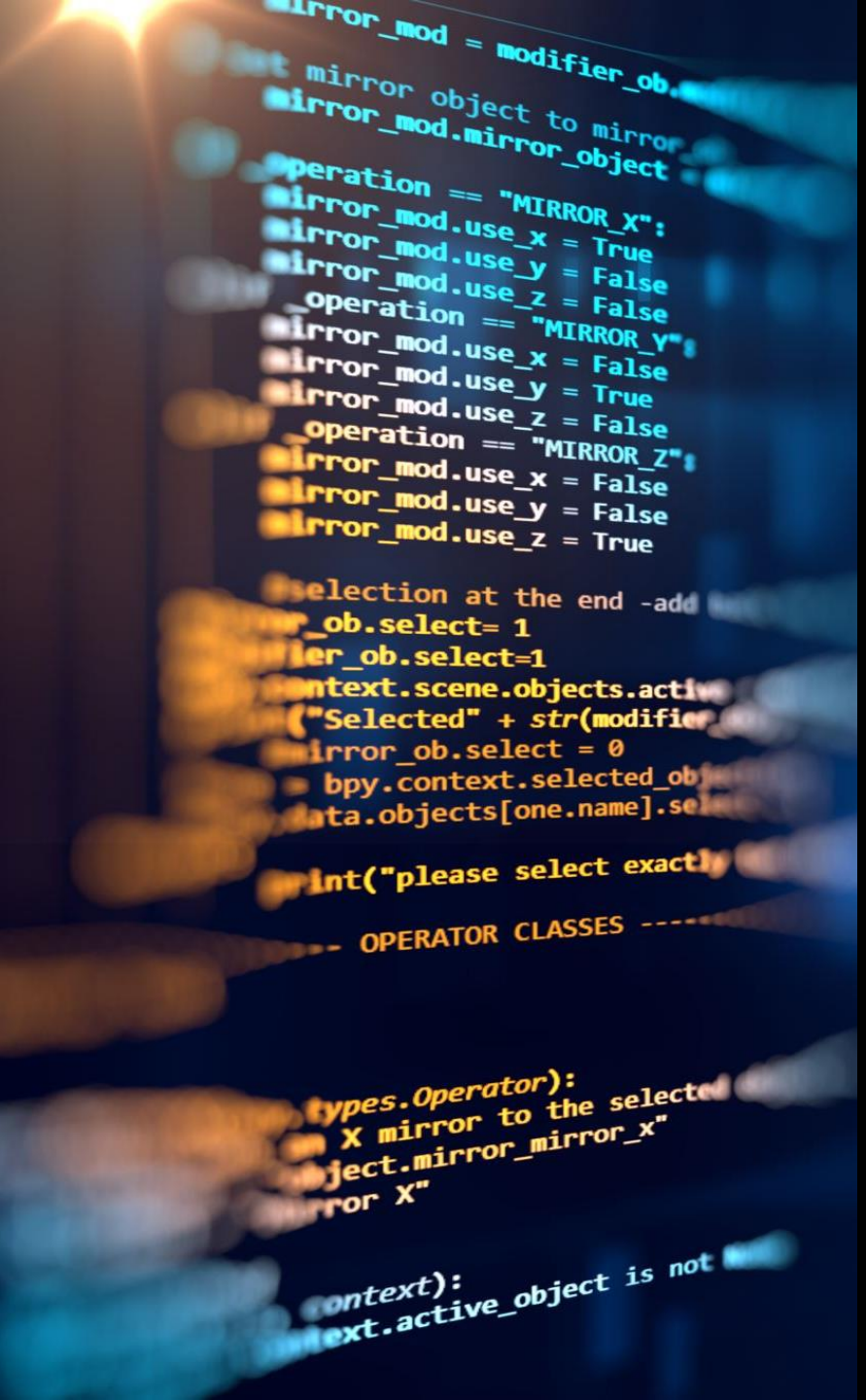
Wie schnell können Sie auf Bedrohungen reagieren?

Mit einem bedrohungsbasierten Ansatz und automatisierten Sicherheitskontrollen
In der gesamten Organisation

Agenda

- Beantwortung folgender der Fragestellungen
  - Warum tun sich Organisationen schwer, ihre Cyber-Resilienz zu verbessern?
  - **Wie kann die Nutzung von KI die Cybersicherheit verbessern?**
  - Was sind einige praktische Beispiele für KI in der Cybersicherheit?
- Herausforderungen und Überlegungen
- Zukünftige Trends für AI in Cyber-Security
- Q & A



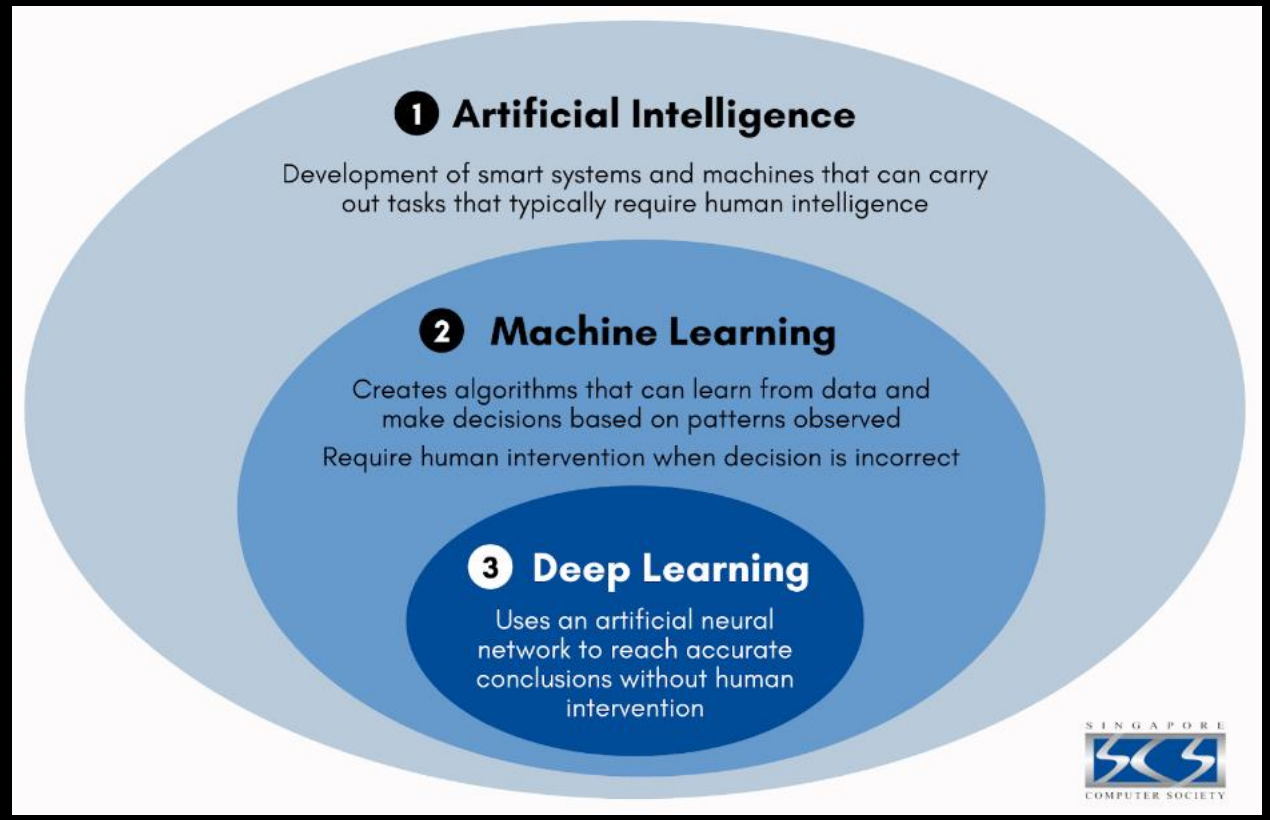


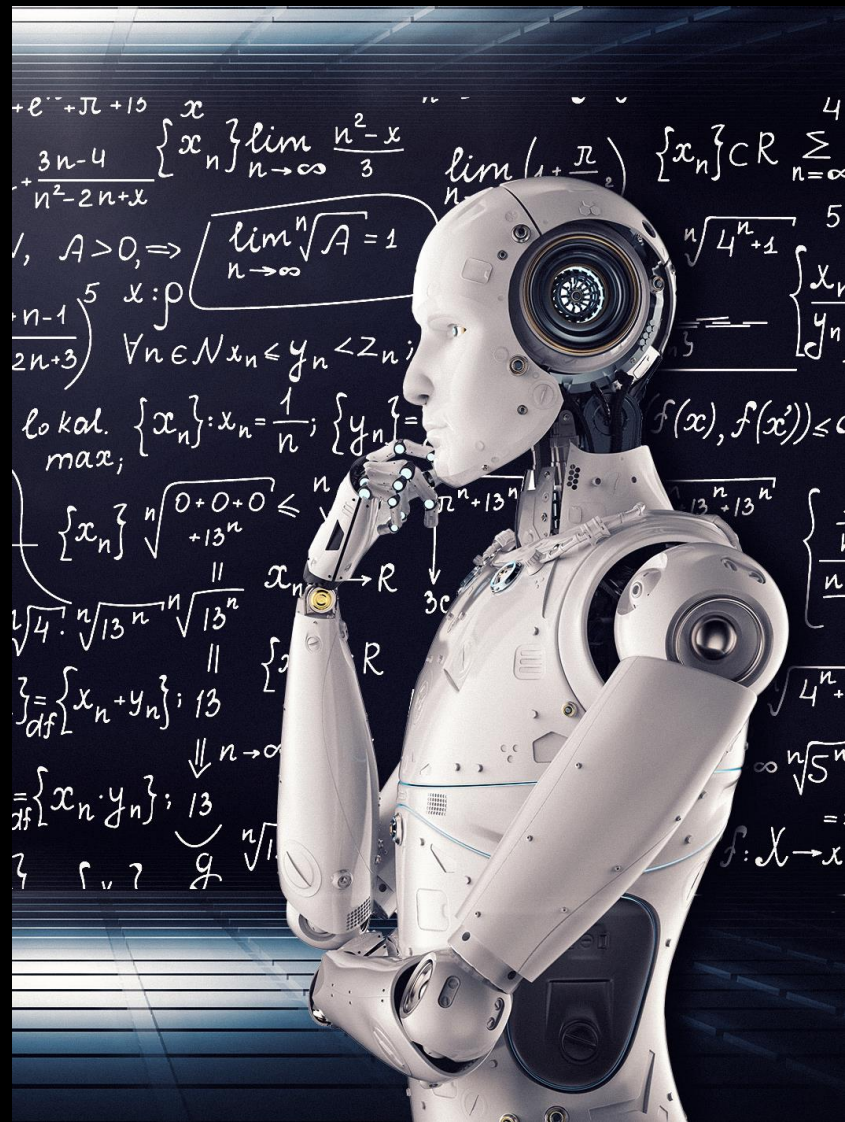
KI in Cyber Security

- **Machine Learning Algorithms**
  - Erkennen von Mustern und Anomalien
- **Natural Language Processing (NLP)**
  - Analyse von Textdaten zur Erkennung von Bedrohungen
- **Predictive Analytics**
  - Vorhersage potenzieller Cyber-Bedrohungen
- **Automated Incident Response**
  - Schnelle Reaktion ohne menschliches Eingreifen

Was ist künstliche Intelligenz (KI)

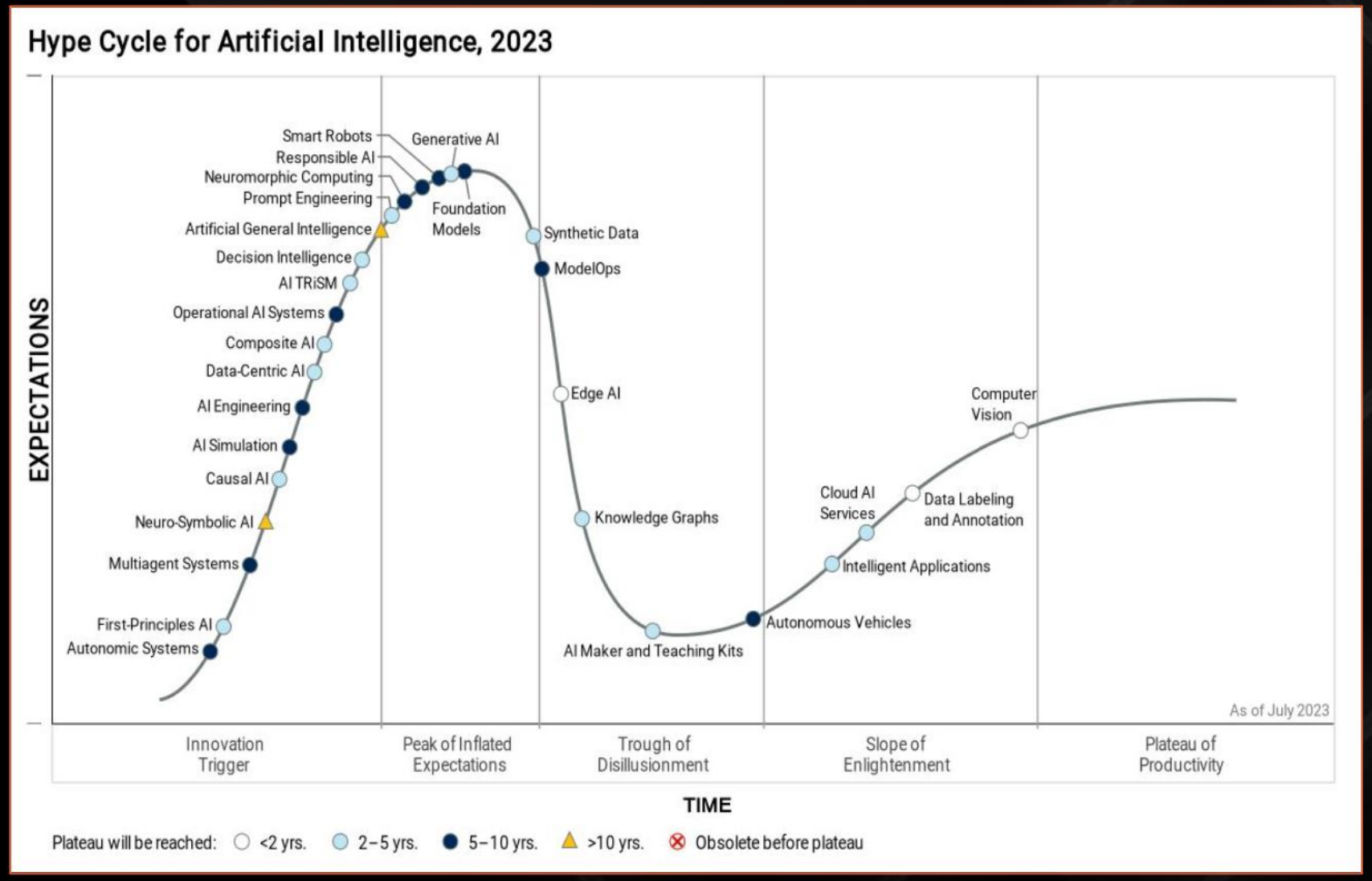
Today mostly as Artificial Narrow Intelligence (ANI) or weak AI – specialising in one area



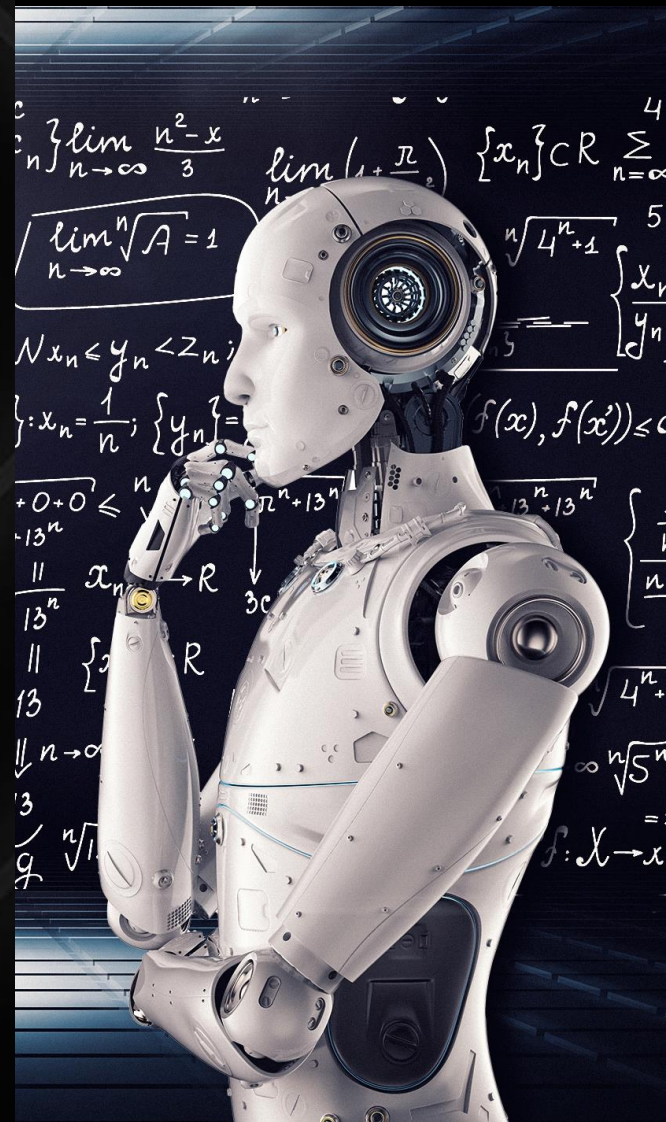


Picture by: mikemacmarketing - https://www.flickr.com/photos/152824664@N07/30212411048/

Gartner Hype Cycle for Artificial Intelligence



Source: Gartner



KI-Fähigkeiten im Umfeld von Cyber-Security

- KI/ML verhindert Bedrohungen in-line
- Autonome Security Operations
- KI unterstützt Expertensysteme für Früherkennund und Mitigation
- KI’s schnelle Reaktion reduziert Auswirkungen einer Cyber Attack

- Predictive Risk Management
- Reduzierte Betriebskosten
- Proaktive Identifikation von Compliance Lücken und vorgeschlagene Massnahmen

Agenda

- Beantwortung folgender der Fragestellungen
  - Warum tun sich Organisationen schwer, ihre Cyber-Resilienz zu verbessern?
  - Wie kann die Nutzung von KI die Cybersicherheit verbessern?
  - **Was sind einige praktische Beispiele für KI in der Cybersicherheit?**
- Herausforderungen und Überlegungen
- Zukünftige Trends für AI in Cyber-Security
- Q & A

Einsatzbereiche von KI in der Cyber Security

- **AI-Powered Threat Detection**
  - Behavioural Analytics, Anomaly Detection, Threat Intelligence
- **AI-Driven Vulnerability Management**
  - Automated Scanning, Prioritization of Threat, Continuous Monitoring
- **AI-Powered Incident Response**
  - Automated Alerts and Notifications, Incident Triage, Threat Containment
- **AI for Data Protection**
  - Data Encryption and Decryption, Data Loss Prevention (DLP), Behaviour-Based Access Control
- **AI and Incident Recovery**
  - Automated Backup and Restore, Incident Simulation, Post-Incident Analysis
- **AI-Enhanced Employee Training**
  - Phishing Simulations, Interactive Learning, Personalized Training

KI verhindert Bedrohungen in-line

Immer mehr Hersteller nutzen KI/ML um aus dem direkten Datenverkehr Bedrohungen zu erkennen und falls möglich zu blockieren; speziell bei Cloud basierten Services

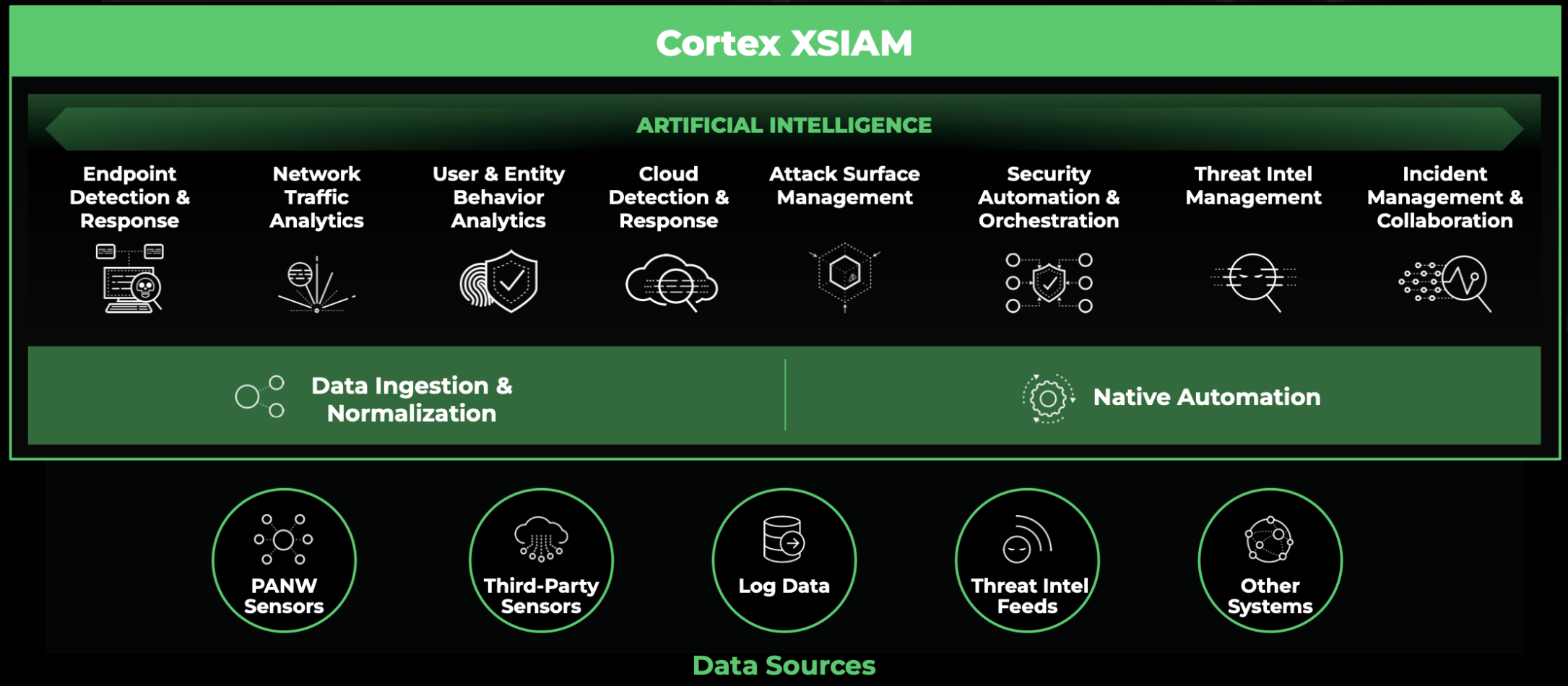
- **Next generation Firewall (IPS)**
- **Secure Service Edge (SSE)**
- **Advanced Sandboxing**
- **Secure Entry Servers**
- **DNS Security**
- **Data Loss Prevention**
- **Email Security**
- **……**

KI in Cyber Security Expertensysteme

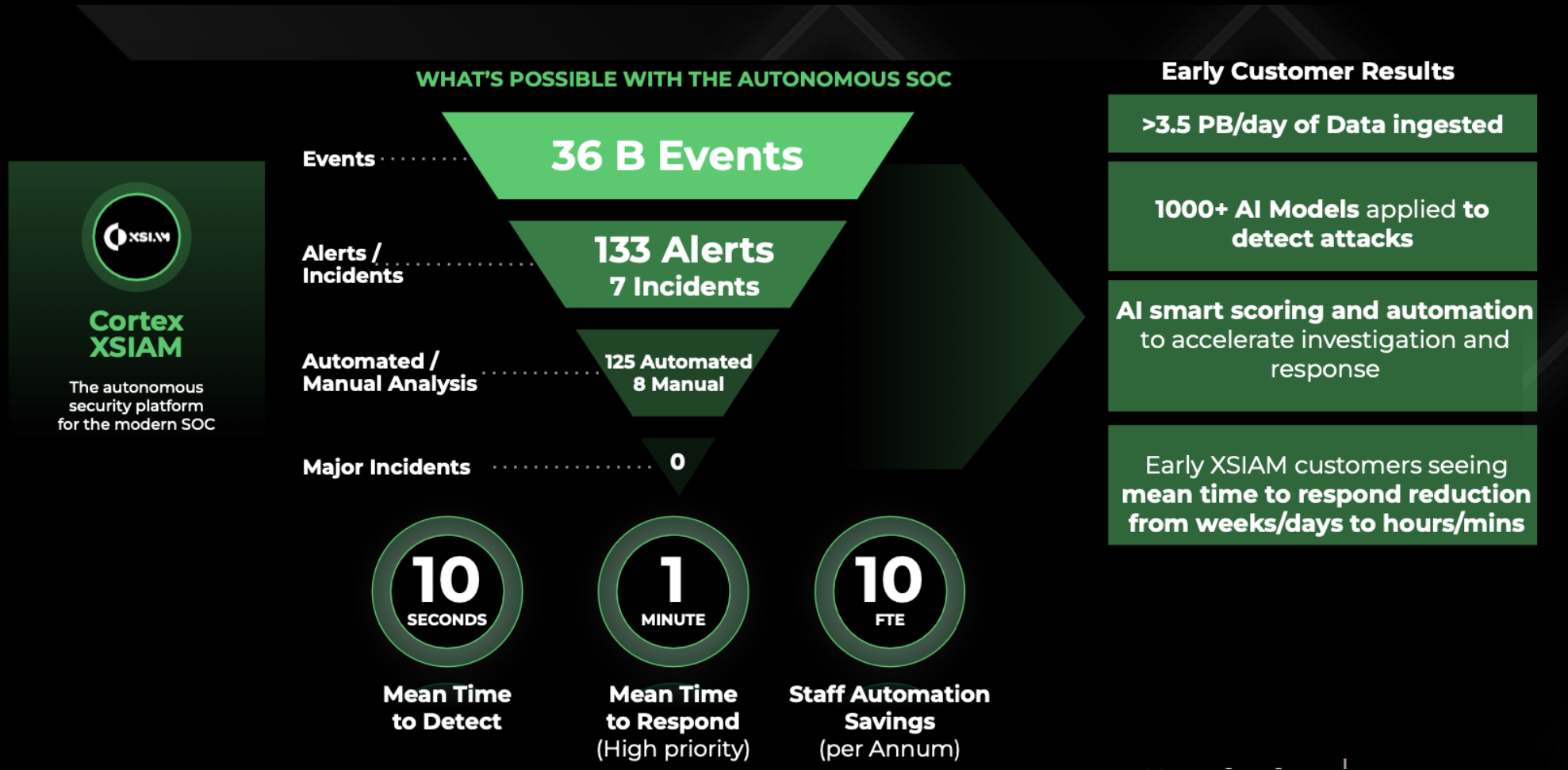
Expertensysteme, die mit KI Anomalien oder Muster erkennen und entsprechen melden oder reagieren können

- **Endpoint Detection and Response (EDR) & Extended Detection and Response (XDR)**
- **Network Detection and Response (NDR)**
- **Threat Intelligence**
- **Vulnerability Management**
- **SOAR – Security Orchestration, Automation and Response**
- **…**

Beispiel für autonomes SOC mit KI

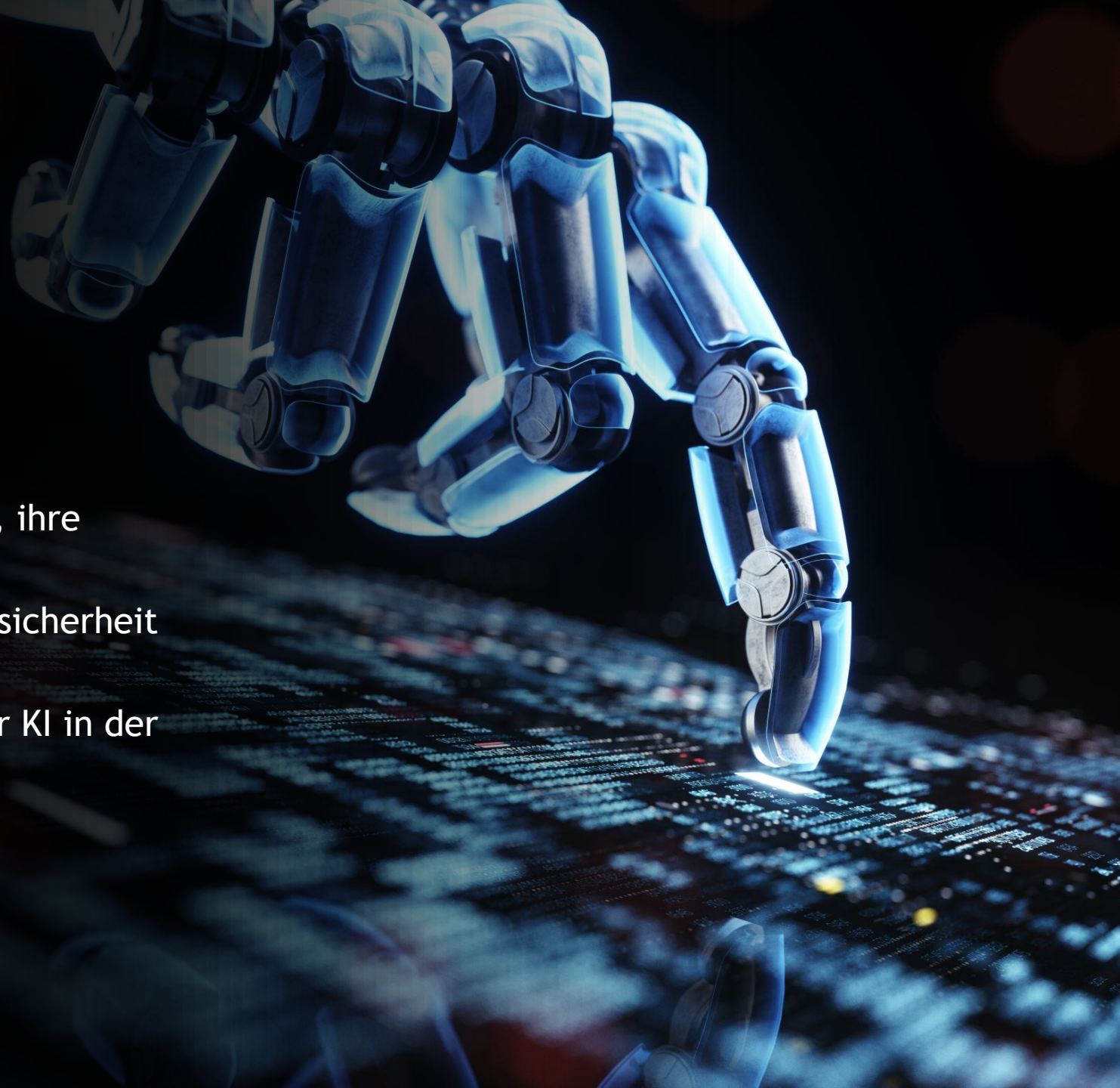


Ergebnis von KI für das autonome SOC



Agenda

- Beantwortung folgender der Fragestellungen
  - Warum tun sich Organisationen schwer, ihre Cyber-Resilienz zu verbessern?
  - Wie kann die Nutzung von KI die Cybersicherheit verbessern?
  - Was sind einige praktische Beispiele für KI in der Cybersicherheit?
- **Herausforderungen und Überlegungen**
- Zukünftige Trends für AI in Cyber-Security
- Q & A

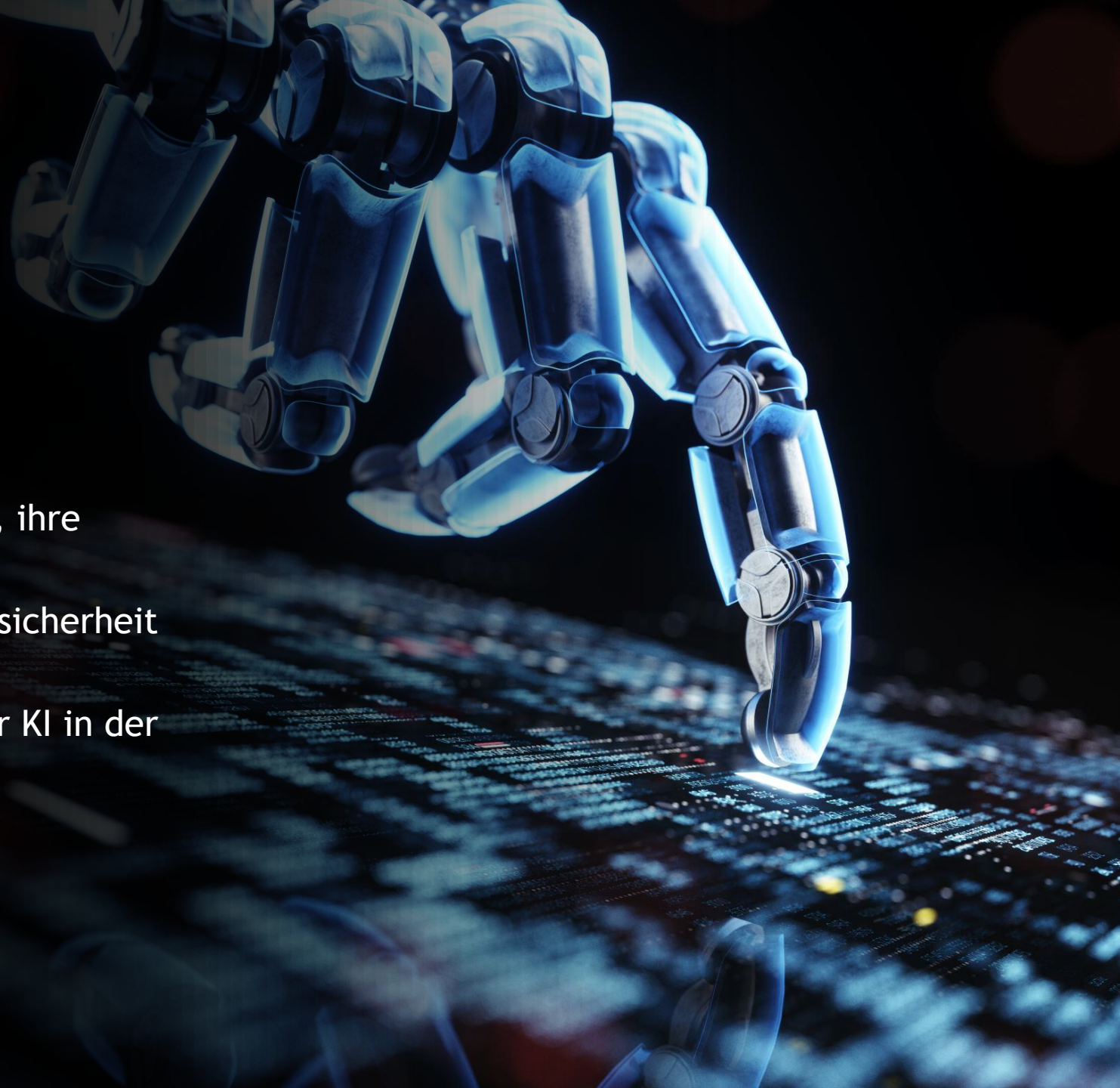


Herausforderungen und Überlegungen

- **Datenschutz und Ethik**
  - Gewährleistung eines verantwortungsvollen Einsatzes von KI in der Cybersicherheitspraxis.
- **Bias in KI-Algorithmen**
  - Umgang mit Bias, die sich auf die Erkennung von und Reaktion auf Bedrohungen auswirken können..
- **Mensch-Maschine-Zusammenarbeit**
  - Ausgleich zwischen KI-Automatisierung und menschlichem Fachwissen für effektive Cybersicherheit.

Agenda

- Beantwortung folgender der Fragestellungen
  - Warum tun sich Organisationen schwer, ihre Cyber-Resilienz zu verbessern?
  - Wie kann die Nutzung von KI die Cybersicherheit verbessern?
  - Was sind einige praktische Beispiele für KI in der Cybersicherheit?
- Herausforderungen und Überlegungen
- **Zukünftige Trends für AI in Cyber-Security**
- Q & A

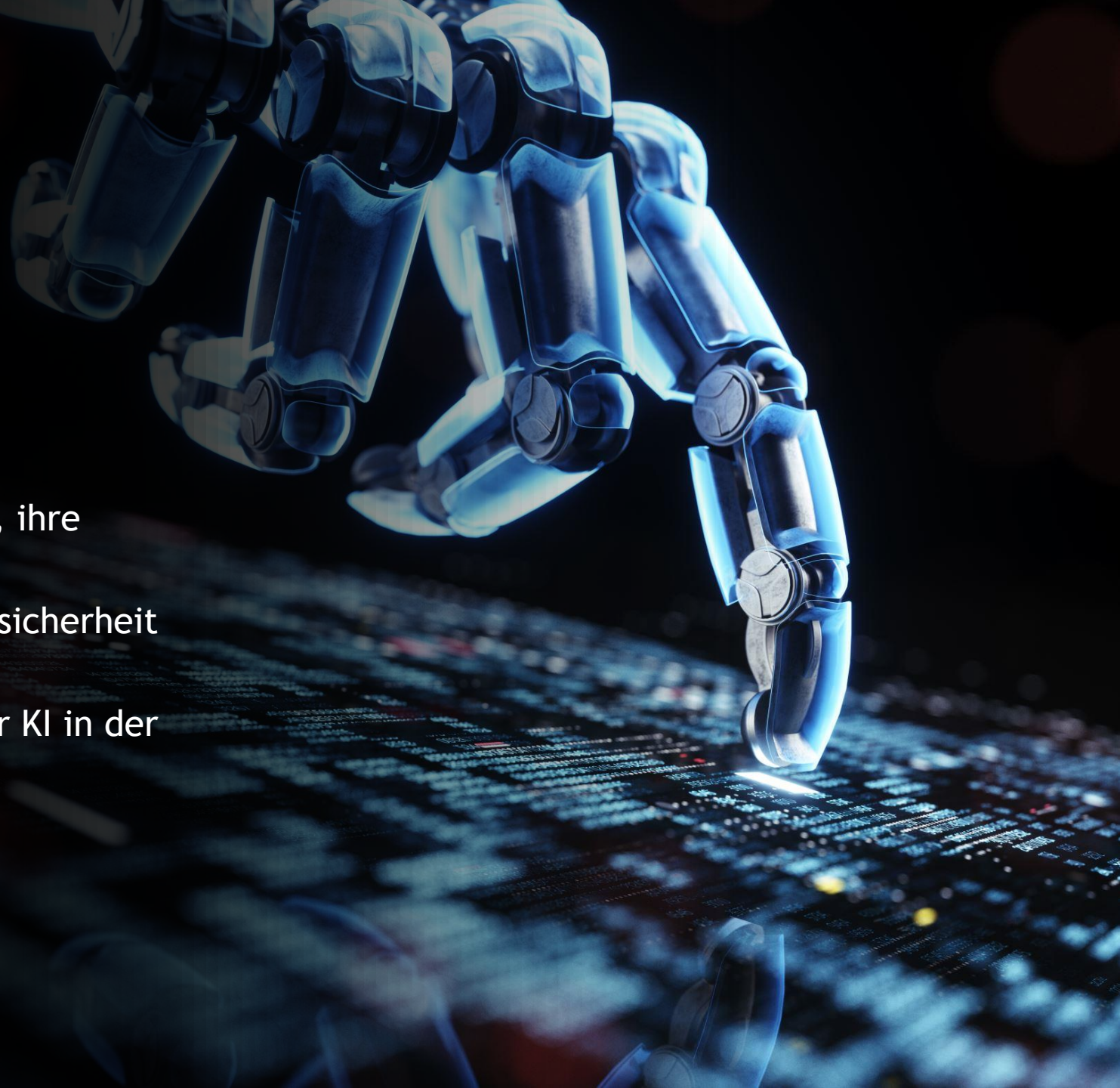


Future Trends

- **Erklärbare KI**
  - Entwicklung von KI-Systemen, die transparente und verständliche Ergebnisse liefern.
- **KI in der IoT-Sicherheit**
  - Integration von KI zur Sicherung des wachsenden Ökosystems des Internets der Dinge.
- **Quantencomputer und KI**
  - Erforschung der Überschneidung von Quantencomputing und KI für fortschrittliche Kryptografie.

Agenda

- Beantwortung folgender der Fragestellungen
  - Warum tun sich Organisationen schwer, ihre Cyber-Resilienz zu verbessern?
  - Wie kann die Nutzung von KI die Cybersicherheit verbessern?
  - Was sind einige praktische Beispiele für KI in der Cybersicherheit?
- Herausforderungen und Überlegungen
- Zukünftige Trends für AI in Cyber-Security
- Q & A



Vielen Dank fürs Zuhören