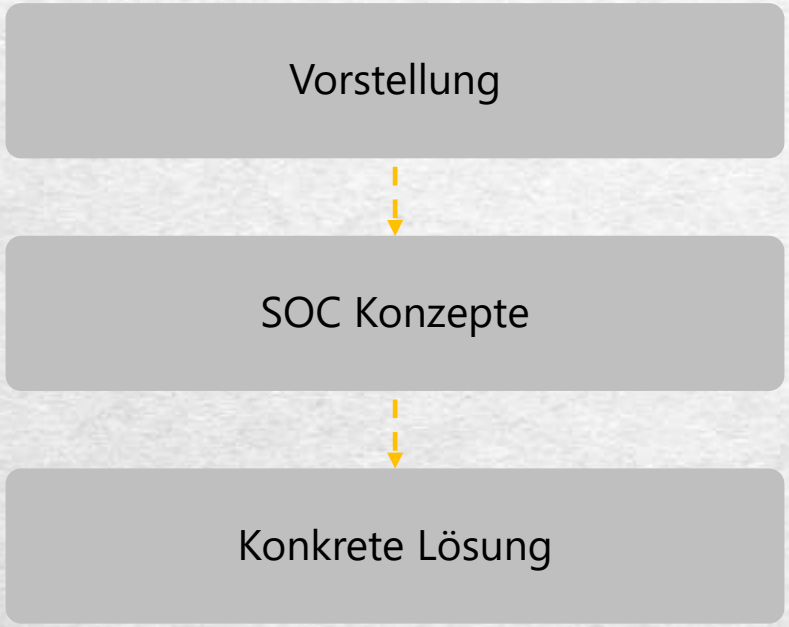
Output Driven SOC – Secure, Efficient, Compliant

Konrad Zacharias
Technical Account Manager

Agenda



doIT solutions

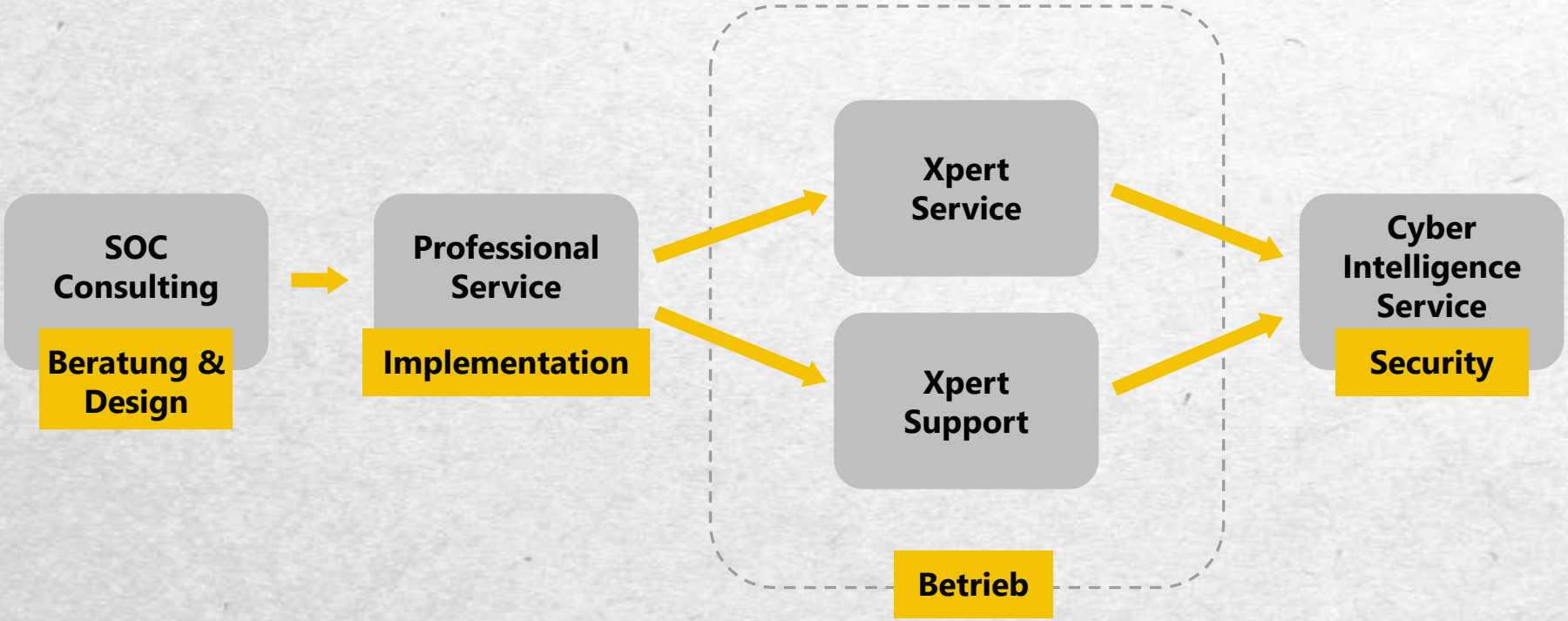
- Gegründet 2010
- Spezialisiert auf moderne Security Operation Center
- Beratung, Implementation und Betrieb
- Managed Security Service Provider

Ihr Partner

doIT solutions GmbH

Altenhaßlauer Str. 21 | 63571 Gelnhausen

doIT Leistungsspektrum



SOC Konzepte

Alarm Driven SOC

- Fokus auf technische Generierung von Alarmen
  - Nicht auf Prozesse
- Fokus auf maximale Mitre Matrix Abdeckung
  - Nicht auf Sinnhaftigkeit
- Viele diverse Alarmquellen
  - Deduplizierung schwierig
- Alarm Tuning / Alarm Fatigue
  - Statt Konzentration auf die wesentlichen Angriffsvektoren

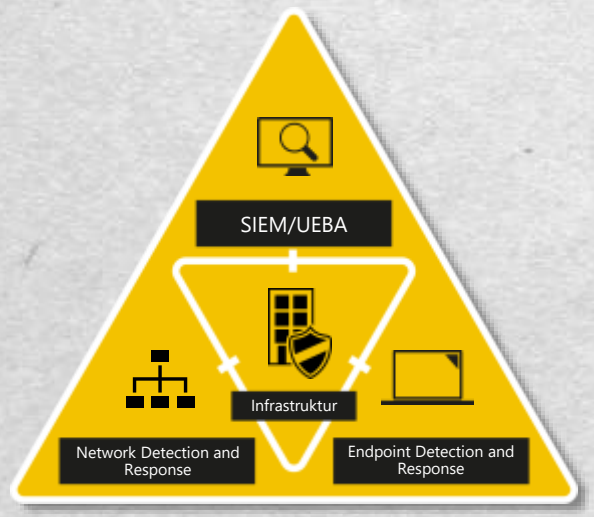
Output Driven SOC

- Fokus auf relevante Use Cases
  - Welche Angriffsvektoren sind relevant
- Sinnvolle Abdeckung der Mitre Matrix
  - Angepasste Auswahl der Methoden zur Angriffserkennung
- Was kann / soll das Team bewältigen und wie?
  - Effiziente und nachvollziehbare Prozesse
- Toolauswahl
  - Soviel wie nötig, so wenig wie möglich
- Langfristige Weiterentwicklung der Security

Was heißt das konkret?

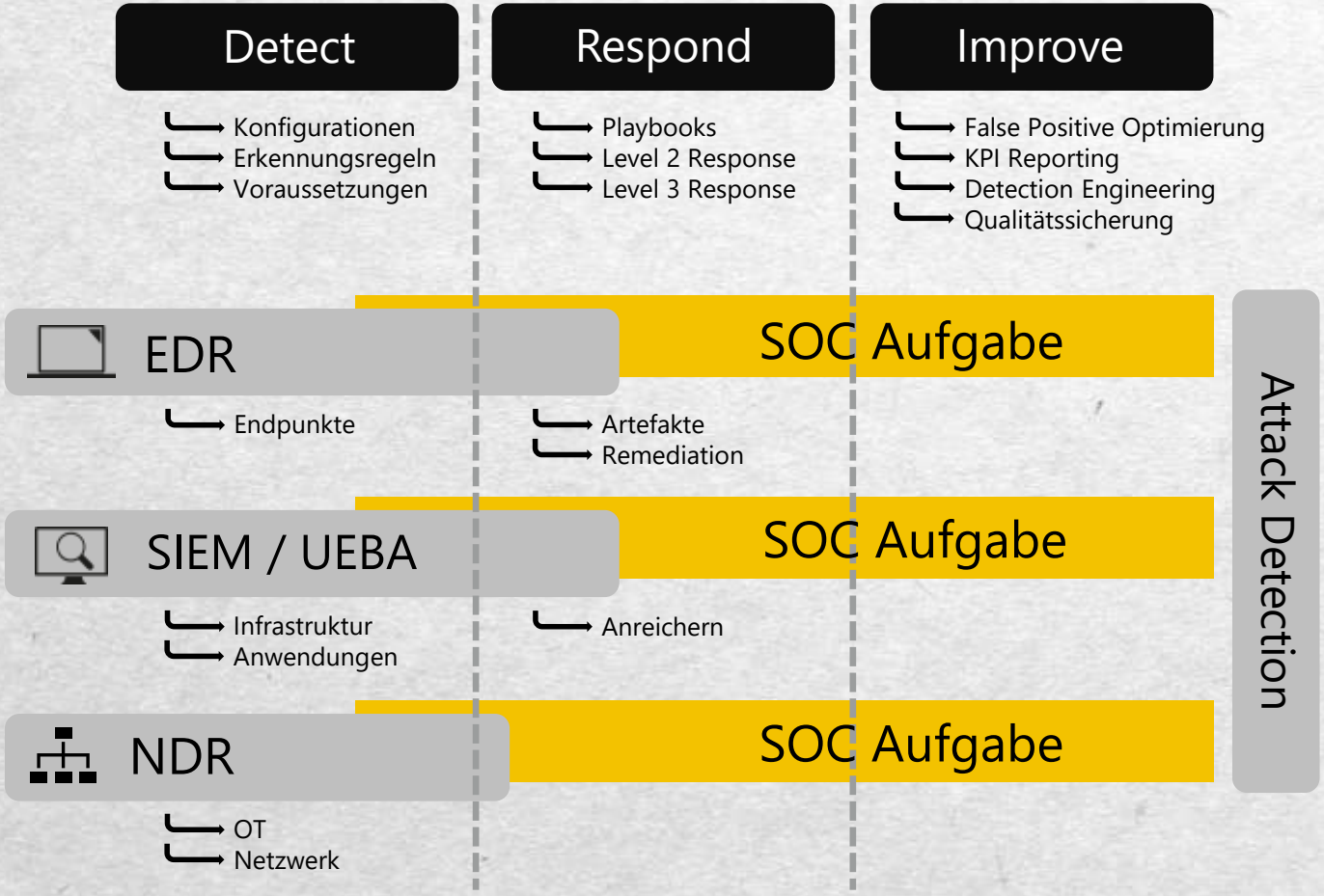
Attack Detection & Prevention

- Attack Detection
  - Erkennung von aktiven Angriffen
  - Basiert auf dem Gartner: “SOC Visibility Triad”

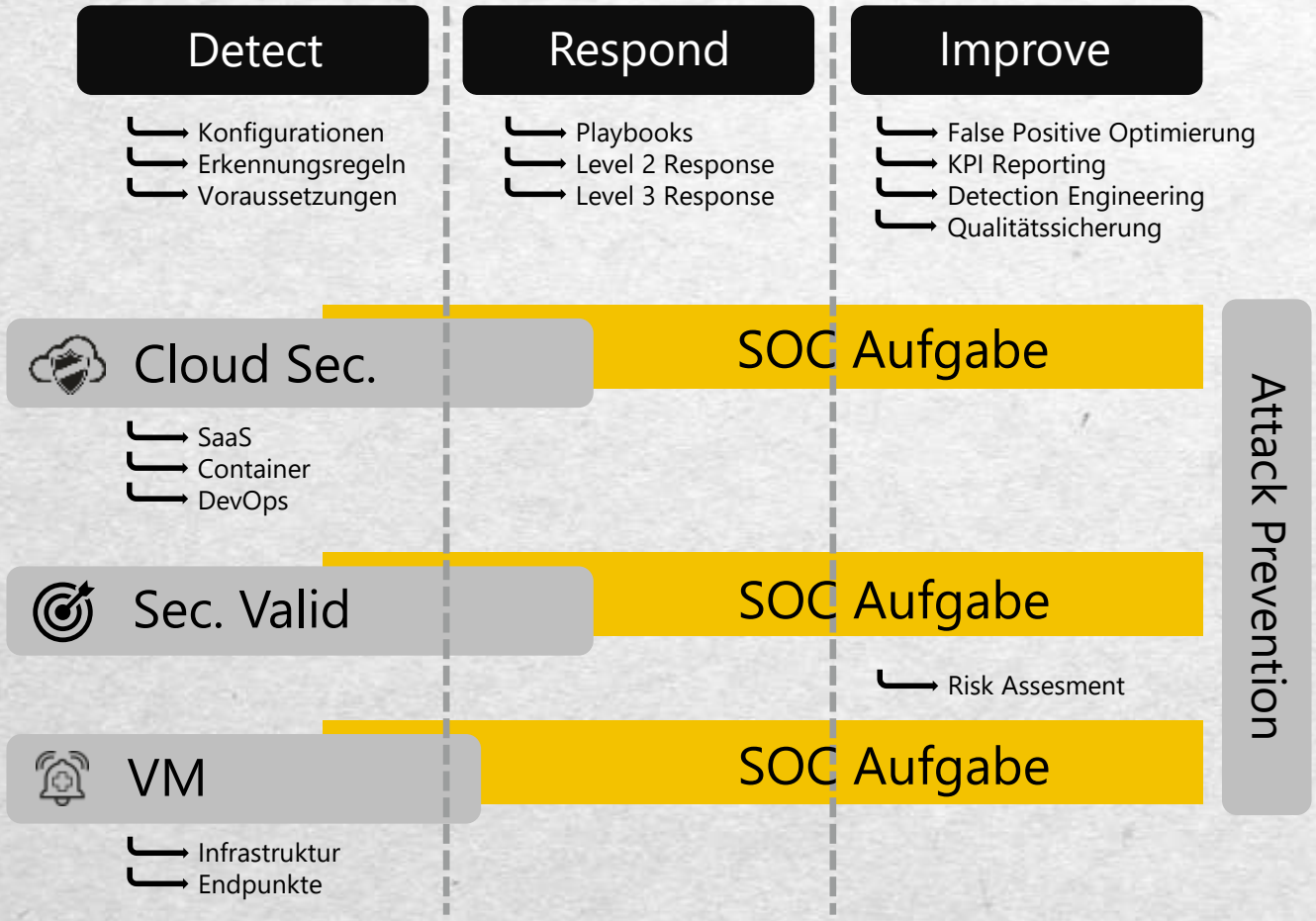


- Attack Prevention
  - Reduktion der Angriffsfläche
  - Verbesserung der Kenntnis der eigenen Infrastruktur und ihrer Eigenheiten
  - Verbesserung der Reaktionsfähigkeit des Security Teams

Attack Detection



Attack Prevention



Viel Aufwand?

We’ve got you covered!

Cyber Intelligence Service

Managed SOC Service

Usecase **Beratung**

- Analyse der Infrastruktur
- Weiterentwicklung

Usecase **Lifecycle**

- Implementation
- Playbooks
- Automatisierung

Response

- Automated Response
- Tier 3 Eskalationen

Xpert Service

Managed SOC Infrastructure Service

Pflege der **Infrastruktur**

- Monitoring
- Updates
- Perfomance Analysen

Tool **Support**

- Hilfestellungen
- Ticket Management

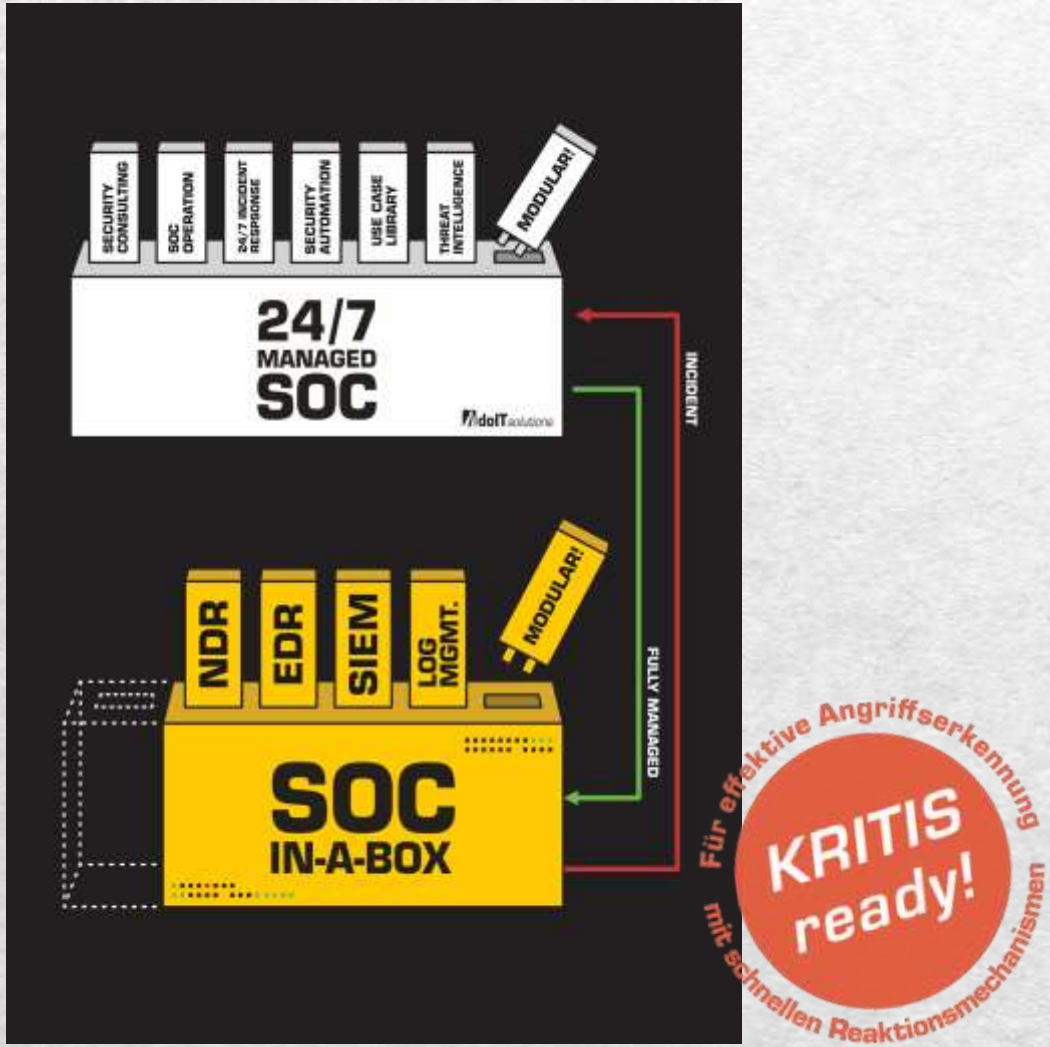
Customization

- Individualisierung der Lösung

Jetzt neu:

SOC in a Box

SOC-in-a-Box



Warum SOC-in-a-Box von doIT solutions?

- 24/7 Incident Response & Security Automation
- On premise und fully managed
- State of the Art Technologie
- Modular und skalierbar

Sie möchten mehr wissen?

Halle 7A, Stand 221

doIT solutions

Cyber Security Experts

Konrad Zacharias
Technical Account Manager

doIT solutions GmbH
Altenhaßlauer Str. 21
63571 Gelnhausen