items

ITEMS SECURITY OPERATIONS CENTER

SICHERHEITSDIENSTLEISTUNGEN FÜR DIE IT- UND OT-INFRASTRUKTUR VON ENERGIEVERSORGERN IN ZEITEN DER DIGITALISIERUNG DER ENERGIEWIRTSCHAFT

KURZE VORSTELLUNG

David Ganser

Teamleiter Connectivity & Security

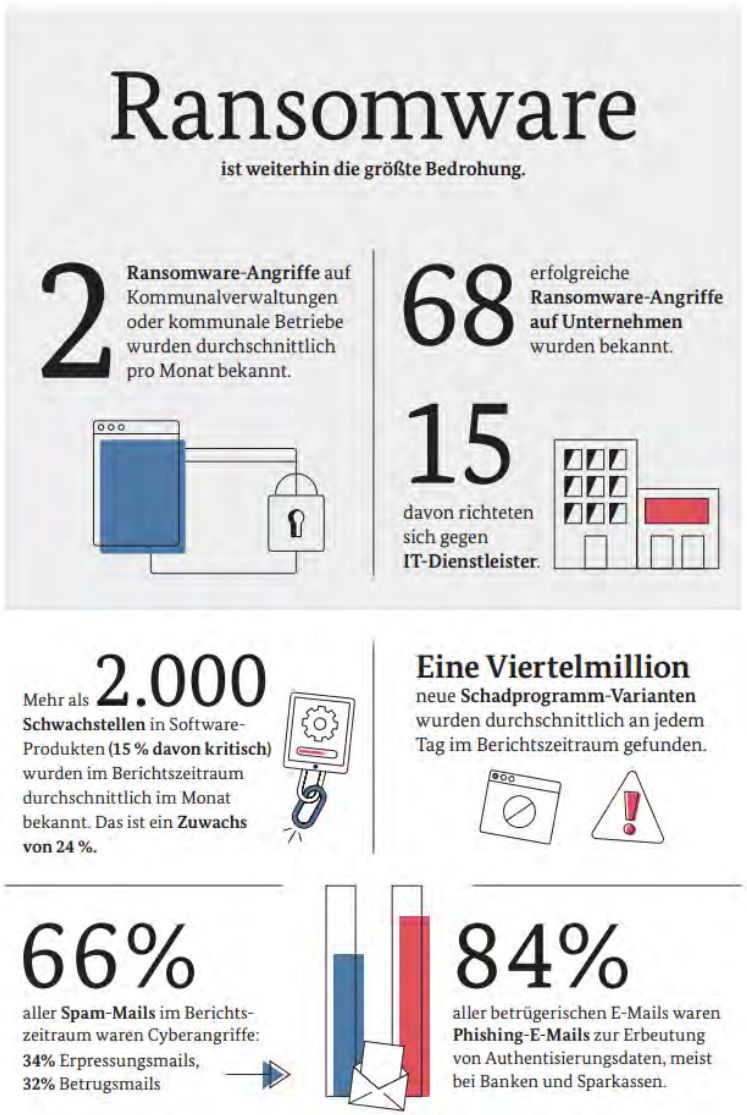
items GmbH & Co KG

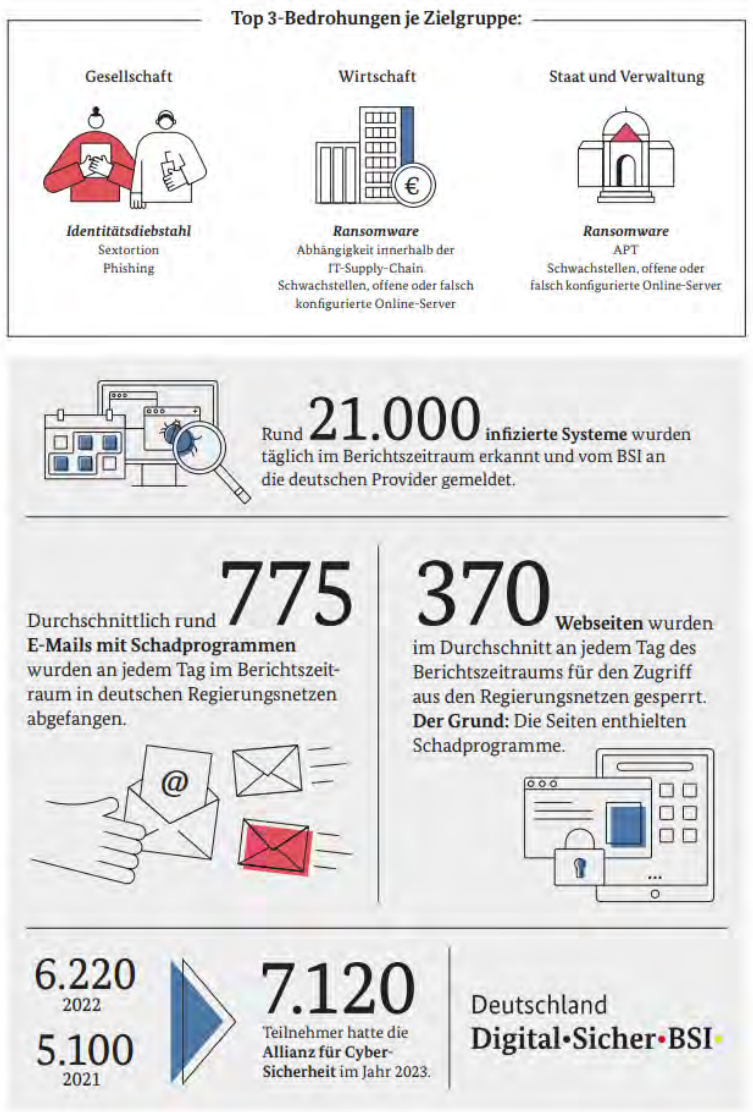
Frank Sommerhoff

Solution Lead

fernao magellan GmbH

IT-SICHERHEITSLAGE DEUTSCHLAND 2023





Forecast 2024

- KI – nicht nur Helfende Hand im Angriffsfall: „KI ist in der wenig technikaffinen Öffentlichkeit angekommen & damit auch bei unseren Kunden & AnwenderInnen
- Schattenseite KI
  - Deepfakes
  - Phishing
  - Erstellung von Schadcode
  - Social Web für Desinformation

TRADITIONELLES SECURITY MODELL

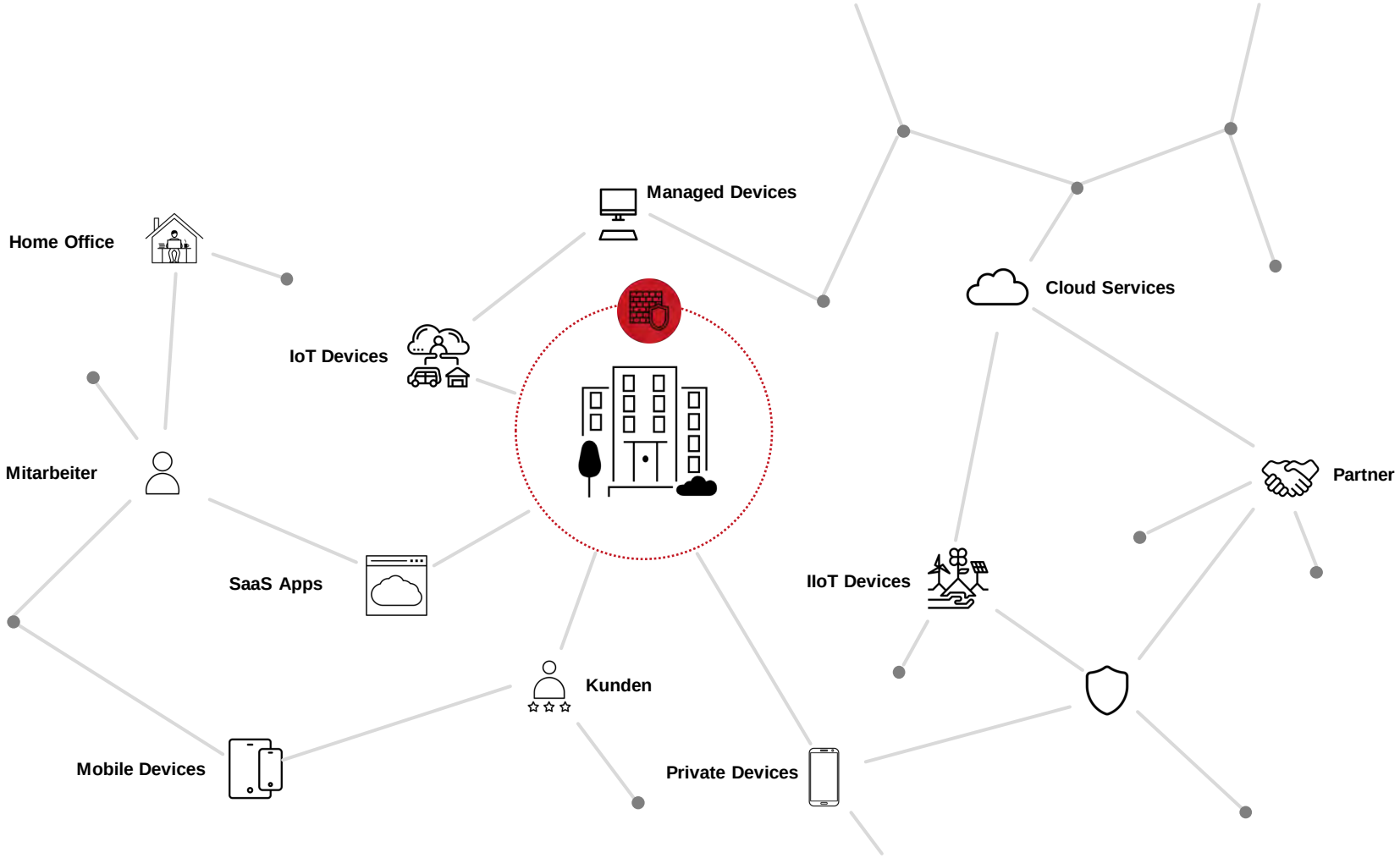
MIT FOKUS AUF ON-PREMISES

Benutzer, Geräte, Apps und
Daten hinter einer Firewall / DMZ

- Schutz der On-Premises Infrastruktur vor dem Zugriff von Außen
- Netzwerktrennungen innerhalb des Perimeters als Bedrohungsschutz
- Benutzer, Geräte, Apps & Daten innerhalb des Perimeters gelten als vertrauenswürdig und sicher

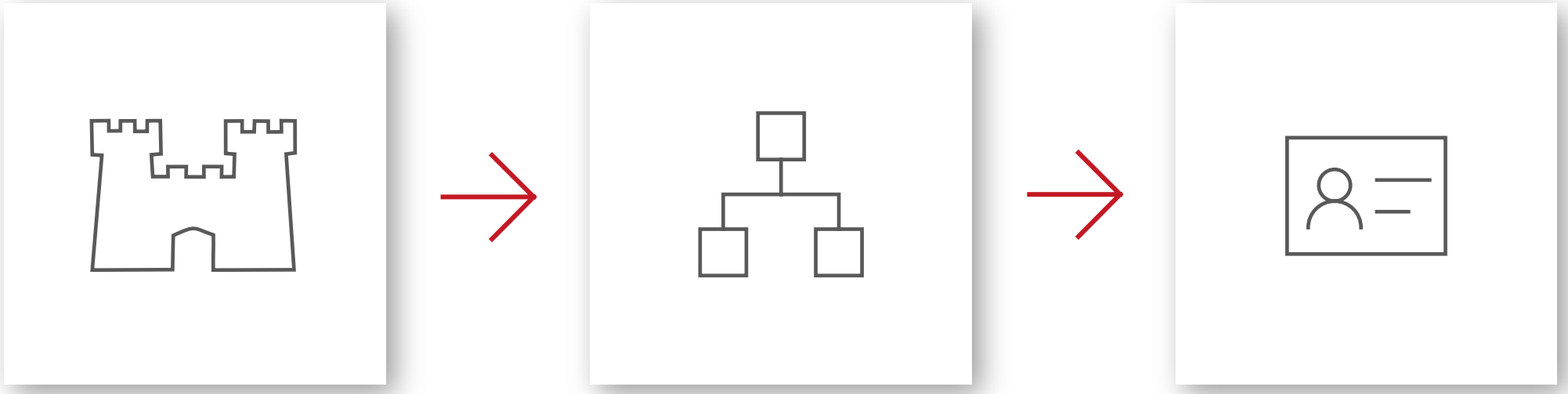
HEUTIGE HERAUSFORDERUNGEN

NETWORK PERIMETER NUR EIN TEIL DER STRATEGIE



EVOLUTION DES SECURITY PERIMETERS

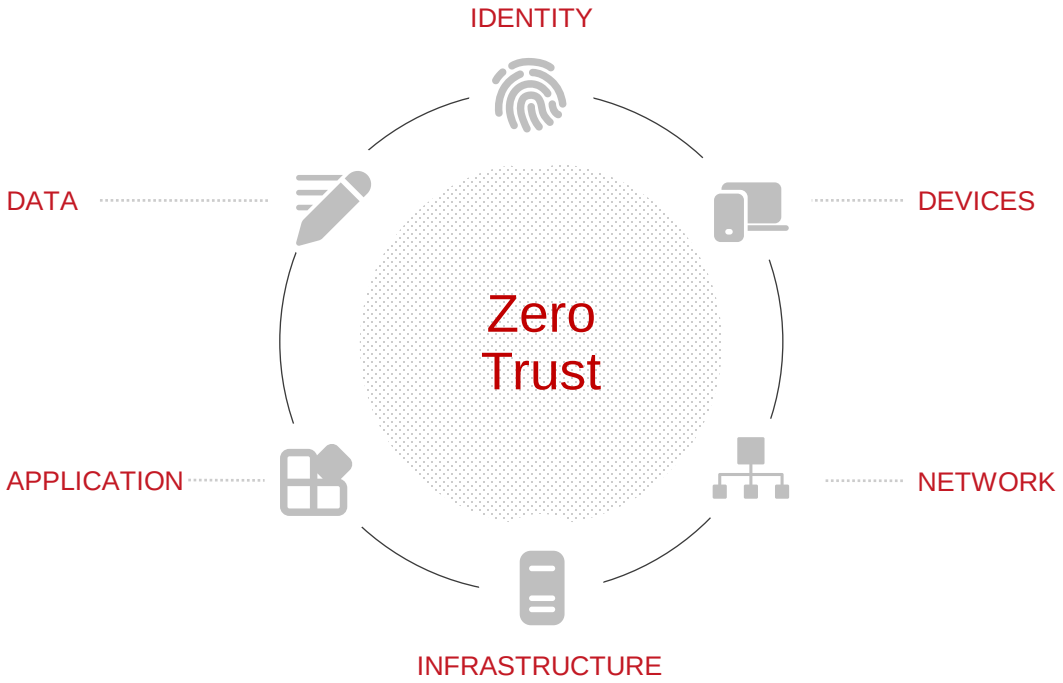
IDENTITY ALS NEUER PERIMETER



Physical **Network** **Identity**

ZERO TRUST

NEVER TRUST, ALWAYS VERIFY



Expliziter Zugriff

Hinzunahme von allen verfügbaren Datenpunkten und Signale zur Sicherstellung der Authentifizierung und Autorisierung.

Identitäten, Gerätestatus, Standort, Anomalien, Verhalten, Datenklassifizierungen

Geringste Berechtigungen

Zugriff auf Daten und Systeme auf geringsten Berechtigungen reduzieren und nur dann wenn er für den Moment benötigt wird.

Just-in-Time & Just-Enough-Access

Von Kompromittierung ausgehen

Ausbreitung vermeiden und Ausmaß reduzieren.

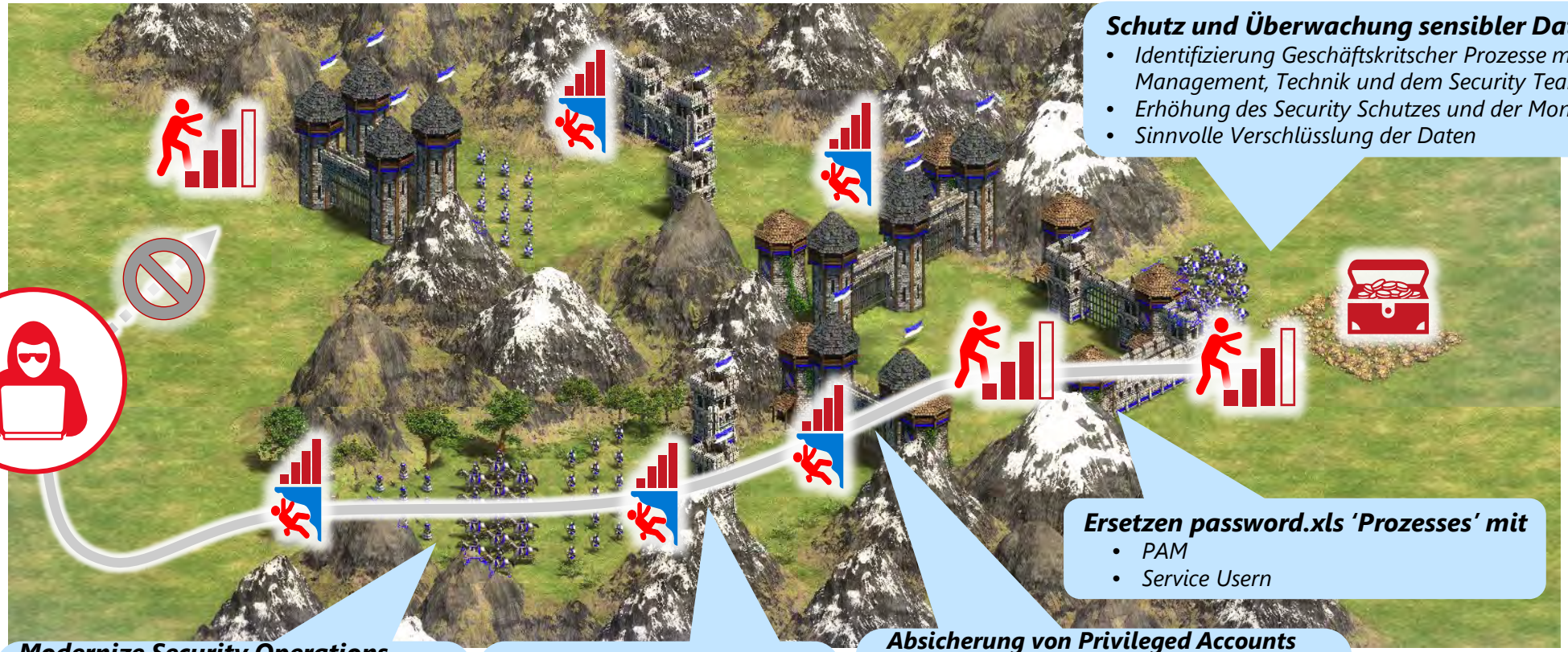
Segmentierung des Zugriffs über Netzwerk, Benutzer, Geräte und Applikationen.

Ende zu Ende Verschlüsselung und Sichtbarkeit mittels Analyse und Erkennung von Bedrohungen

DER WEG DES GERINGSTEN WIDERSTANDES

items

STRATEGISCHE INVESTITION IN ABWEHRMAßNAHMEN



Schutz und Überwachung sensibler Daten
- *Identifizierung Geschäftskritscher Prozesse mit dem Management, Technik und dem Security Team*
- *Erhöhung des Security Schutzes und der Monitoring Prozesse*
- *Sinnvolle Verschlüsslung der Daten*

Ersetzen password.xls 'Prozesses' mit
- *PAM*
- *Service Usern*

Modernize Security Operations
- *Verwendung von XDR für identity, endpoint (EDR), cloud apps*
- *Ständige Weiterentwicklung der SecOps Analysten im Bereich endpoints and identity authentication flows*

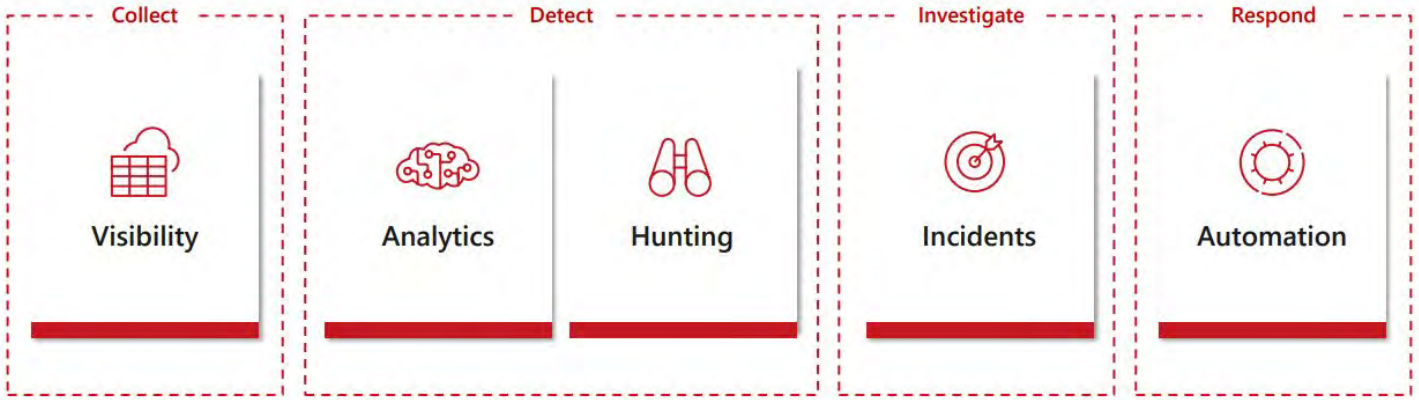
Strenge Sicherheitsvorgaben
- *Schneller Patchzyklus*
- *Sichere Konfigurationen*
- *Sichere Operative Handlung*

Absicherung von Privileged Accounts

Verwendung von dedzierten Adminaccount sowie durchgängiger Verwendung von MFA/passwordless Privileged Access Workstations (PAWs) + enforce with Conditional Access

SECURITY EVENT MANAGEMENT

ITEMS: SECURITY EVENT MANAGEMENT



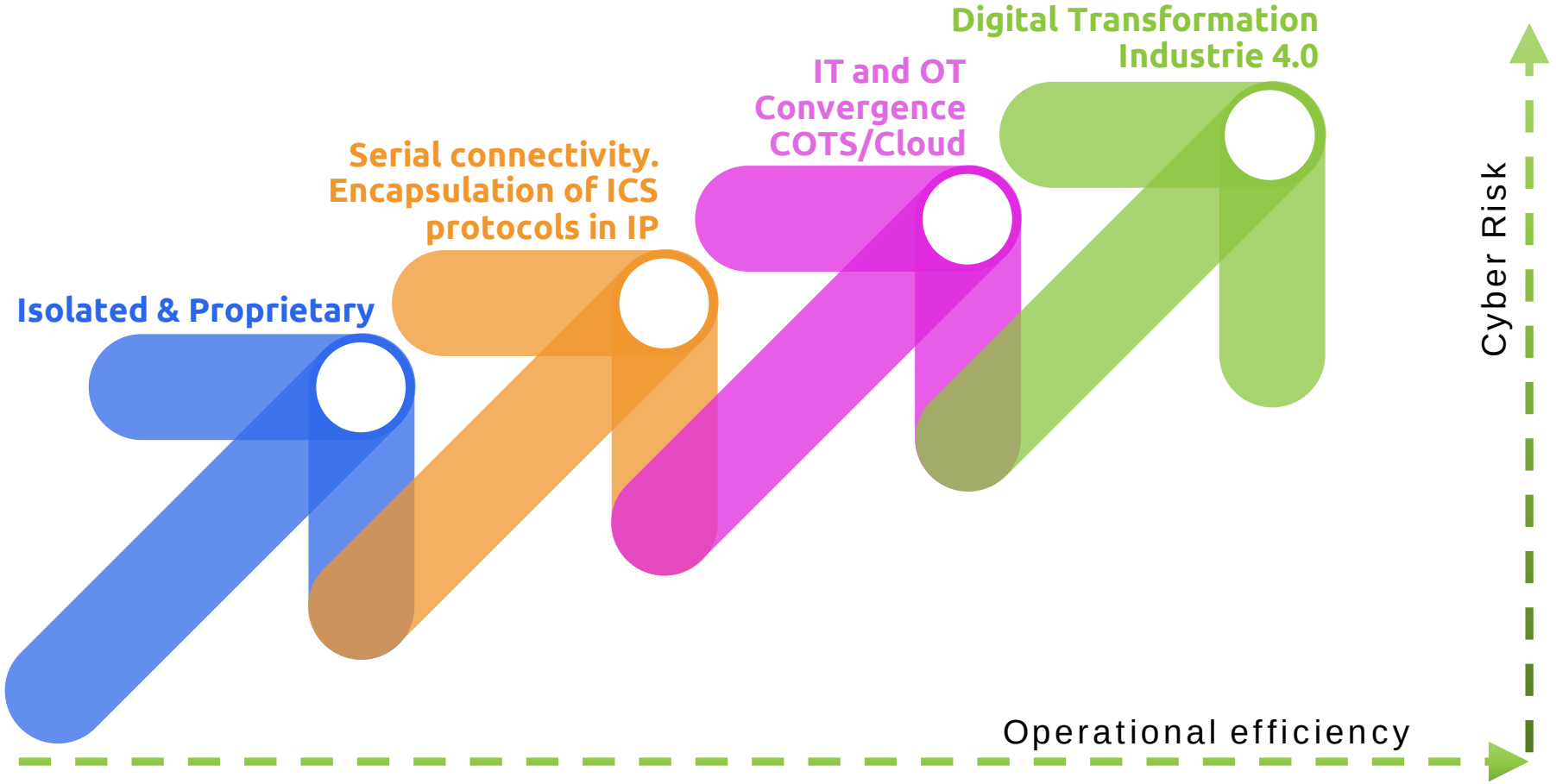
- Security Operations inkl. Security Incident Response
- 24/7 Security Rufbereitschaft
- Forensik Partner

-Security

NETWORK VISIBILITY

Was man nicht sehen kann,
kann man auch nicht schützen!

OT-Evolution



*Die zunehmende Vernetzung von **OT**- und **IT**-Systemen führt zu neuen Herausforderungen und Chancen für Unternehmen.*

Motivation

- **Sabotage:**

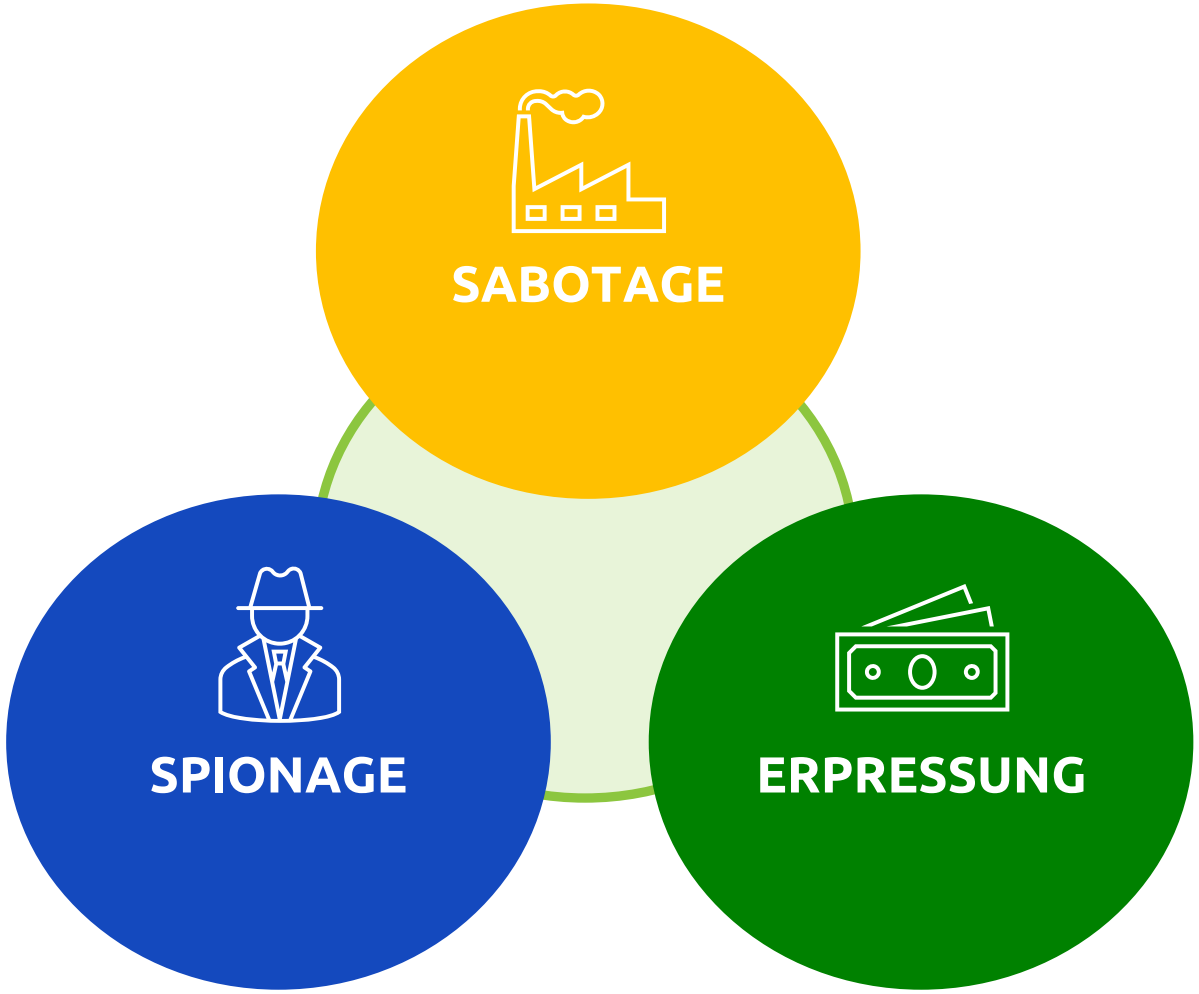
Steuerungssysteme werden gezielt manipuliert und sabotiert.

- **Erpressung:**

Das Unternehmen wird aufgrund von Manipulationen zum Ziel von Erpressungen.

- **Spionage:**

Industriespionage ist eine der klassischen Motivationen für Angriffe auf OT-Systeme.



Argumente

Schutz von Menschenleben und Gesundheit: OT-Systeme steuern kritische Infrastrukturen, wie z. B. Kraftwerke, Krankenhäuser und Verkehrssysteme. Ein Cyberangriff auf diese Systeme könnte zu Verletzungen oder sogar zum Tod von Menschen führen.

Vermeidung von Imageschäden: Ein Cyberangriff auf ein Unternehmen kann zu Imageschäden führen, wenn Kunden und Partner das Unternehmen als nicht sicher betrachten.

Konformität mit gesetzlichen Vorschriften: In vielen Ländern gibt es gesetzliche Vorschriften für die Sicherheit von OT-Systemen. Die Nichteinhaltung dieser Vorschriften kann zu Bußgeldern oder anderen Sanktionen führen.

Vermeidung von Produktionsausfällen: OT-Systeme sind für die Produktion von Gütern und Dienstleistungen unerlässlich. Ein Cyberangriff kann zu Produktionsausfällen führen, die zu finanziellen Verlusten und Reputationsschäden führen können.

Schutz von geistigem Eigentum: OT-Systeme enthalten oft wertvolles geistiges Eigentum, wie z. B. Produktdesigns oder Produktionsdaten. Ein Cyberangriff könnte zu Diebstahl oder Missbrauch dieses geistigen Eigentums führen.

BSI-Reifegradbestimmung

…ist ein Modell zur Bewertung der Reife eines (ISMS) Informationssicherheitsmanagementsystems. Es hilft Organisationen, ihren aktuellen Stand der Cyber-sicherheit zu beurteilen und Bereiche zu identifizieren, in denen Verbesserungen erforderlich sind.

Reifegrad-Stufen nach BSI

Fünf Stufen (1 bis 5) repräsentieren den Fortschritt in der Informationssicherheit .

Die Stufen ***4 und 5*** erfordern eine umfassende Integration von Tools in die Sicherheitsstrategie.

Reifegrad 1: Initialer Aufbau

Reifegrad 2: Definierte Prozesse

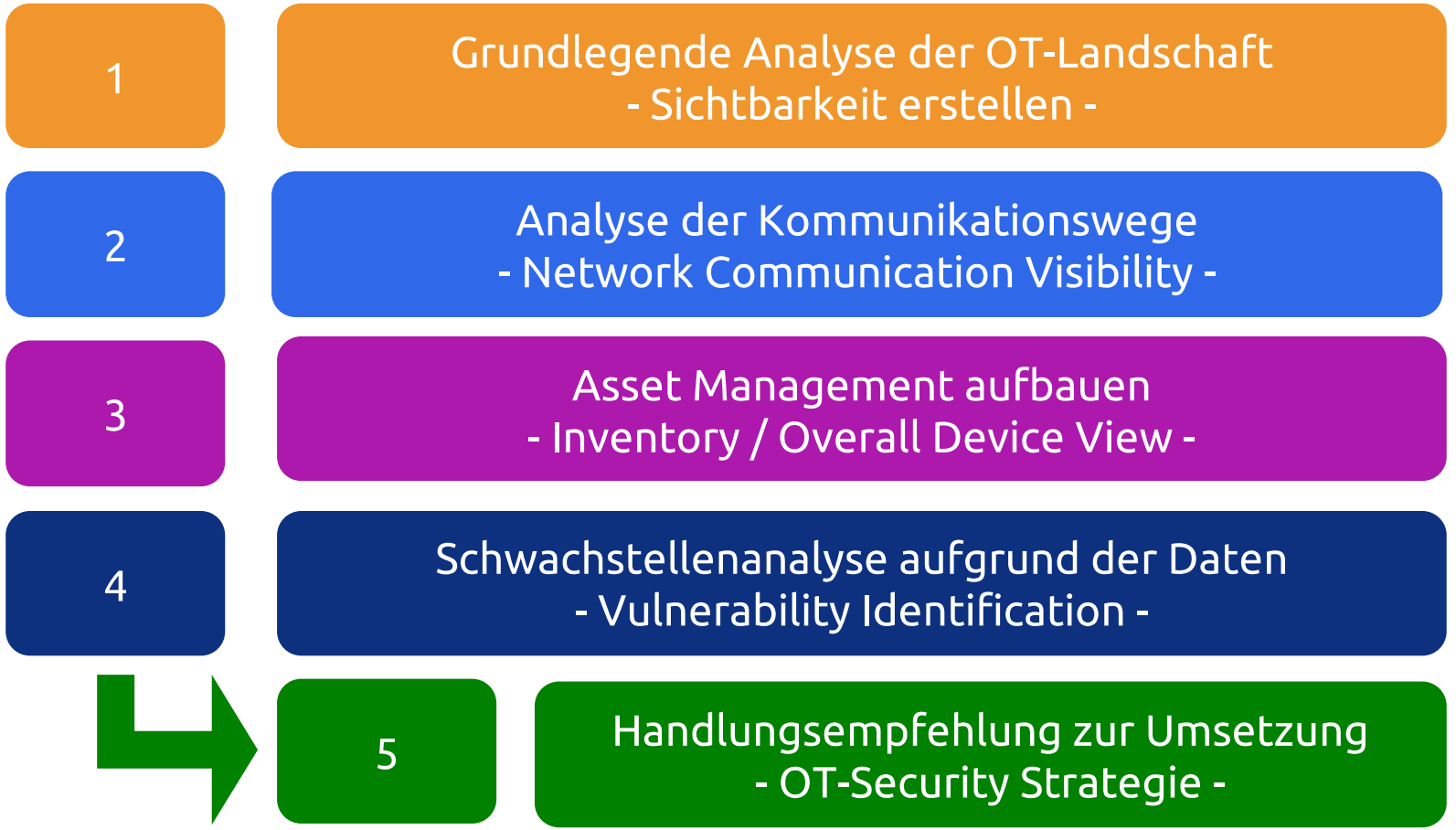
Reifegrad 3: Dokumentierte Prozesse

Reifegrad 4: Gelebtes ISMS – Einsatz von NDR oder Schwachstellenscannern

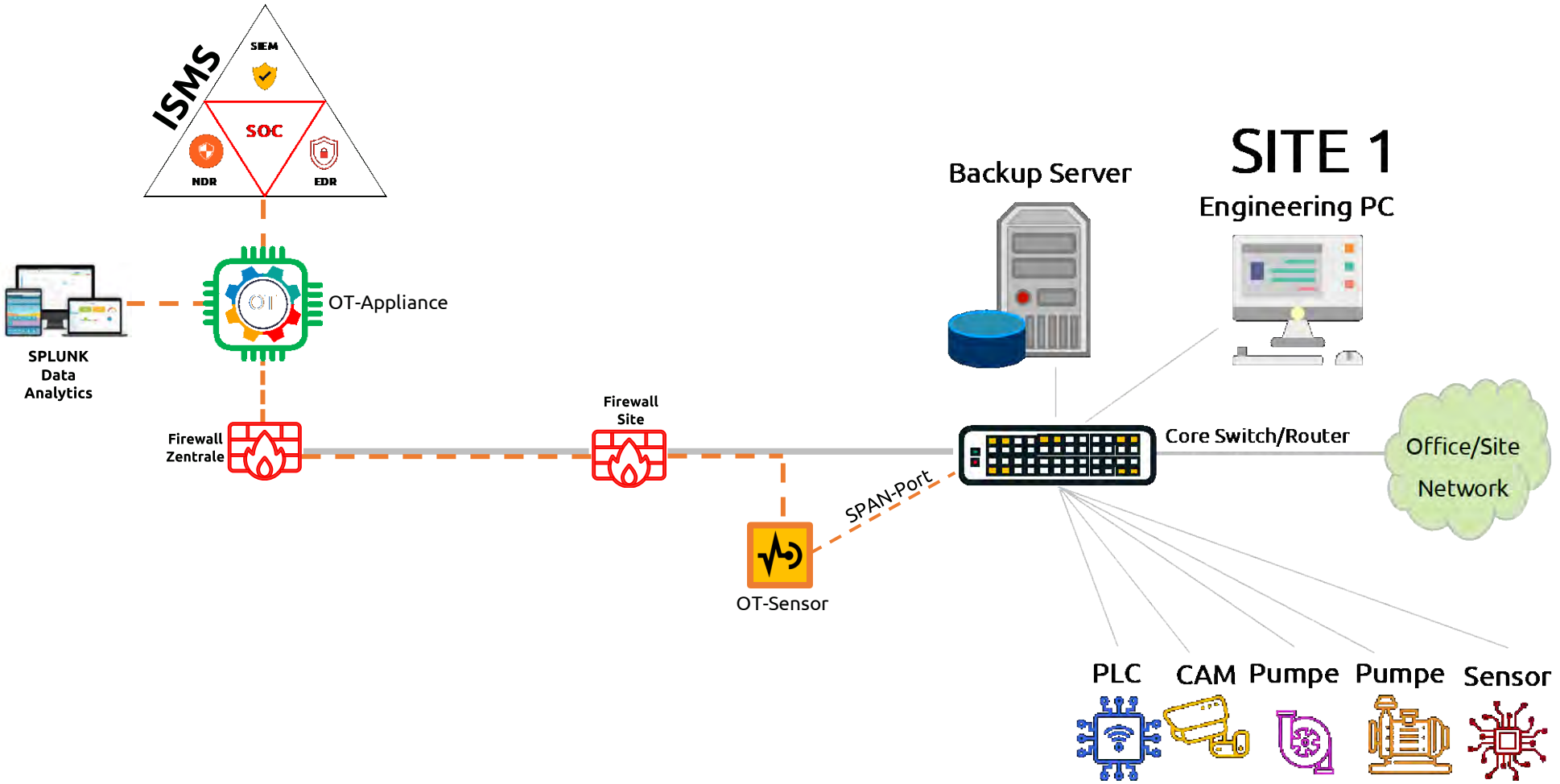
Reifegrad 5: Optimiertes ISMS – Fortlaufender Betrieb einer OT-Security

Die **Bewertung** erfolgt anhand eines Fragebogens und einer Selbstbewertung. Damit wird der aktuelle Reifegrad und der Stand der OT-Security bestimmt.

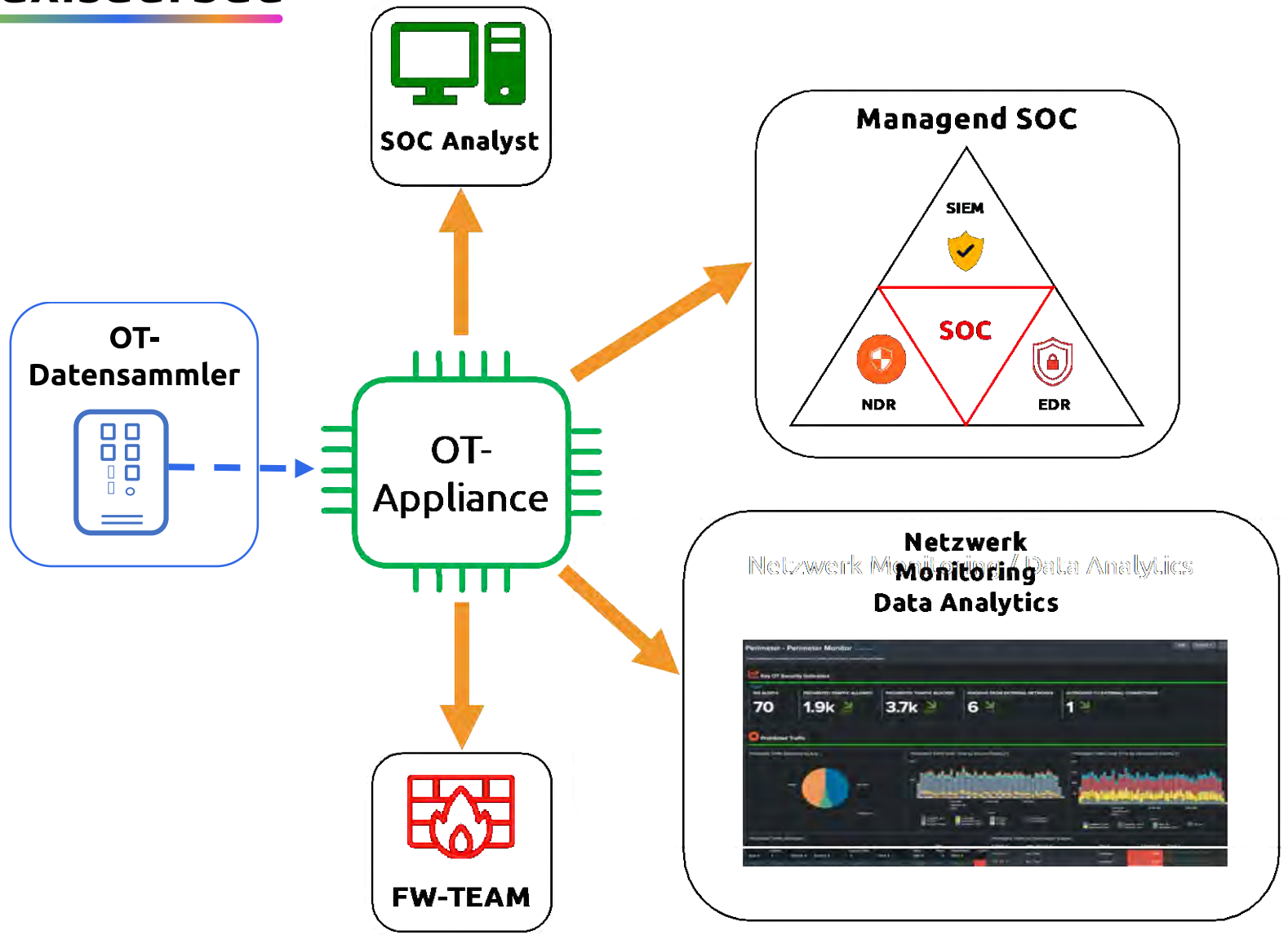
Herangehensweise



Beispiel Praxisaufbau

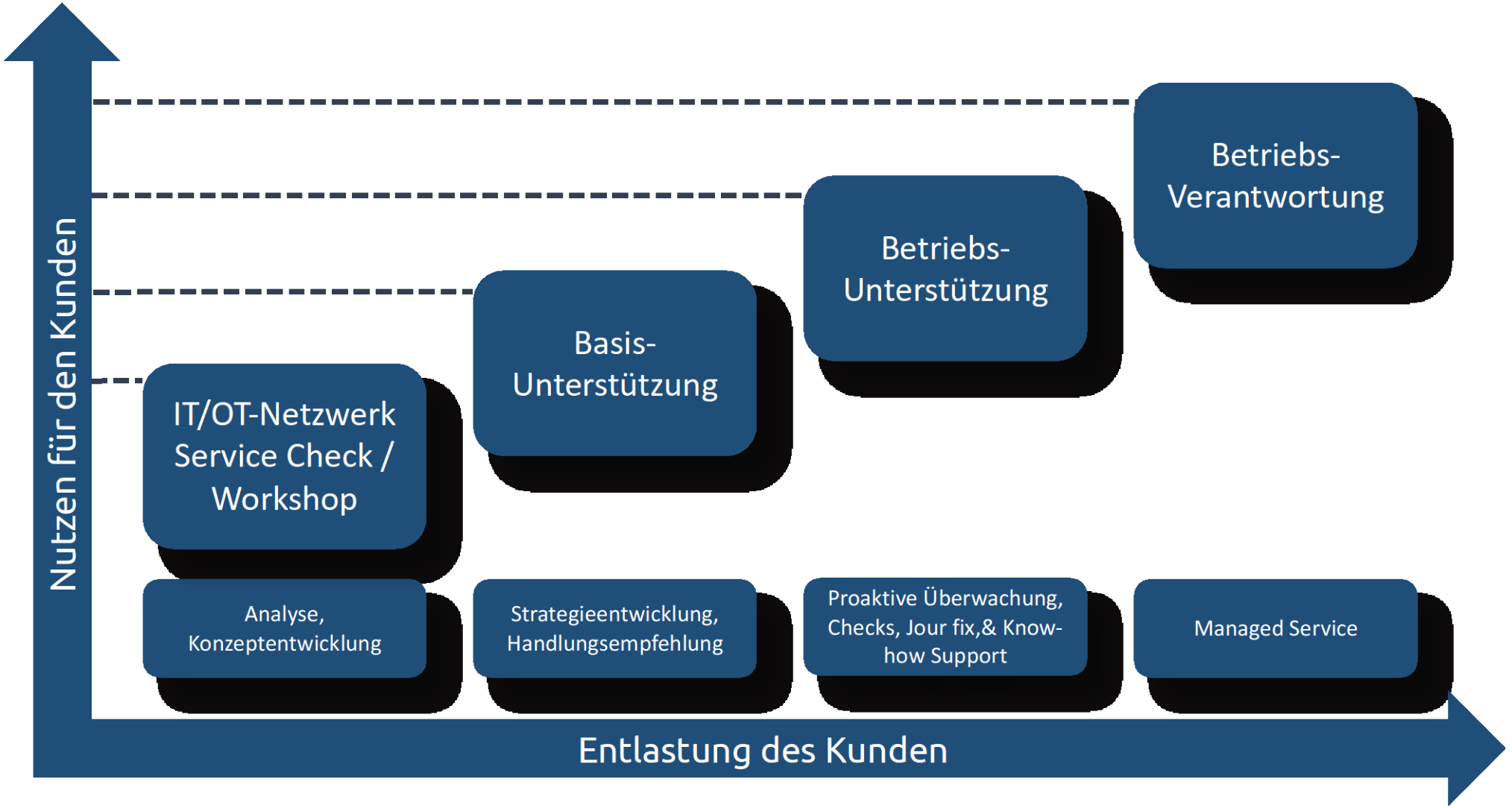


Beispiel Praxisaufbau



Produkte/Partner OT-Security

Fernao-Magellan-Part



Resümee

OT-Security ist ein komplexes Thema. Es gibt keine einfache Lösung, die für alle Organisationen geeignet ist. Unternehmen sollten jedoch die Risiken von Cyberangriffen auf OT-Systeme verstehen und angemessene Maßnahmen zur Absicherung ihrer Systeme ergreifen.

HABEN SIE FRAGEN?

DAVID GANSER

items GmbH & Co. KG
Hafenweg 7
48155 Münster

+49 251 20 83-24 45

d.ganser@itemsnet.de

https://www.itemsnet.de

FRANK SOMMERHOFF

fernao magellan GmbH
Albin-Köbis-Str.5
51147 Köln

+49 2203 922 63-0

+49 160 982523 83

frank.sommerhoff@magellan-net.de

https://www.fernao.com