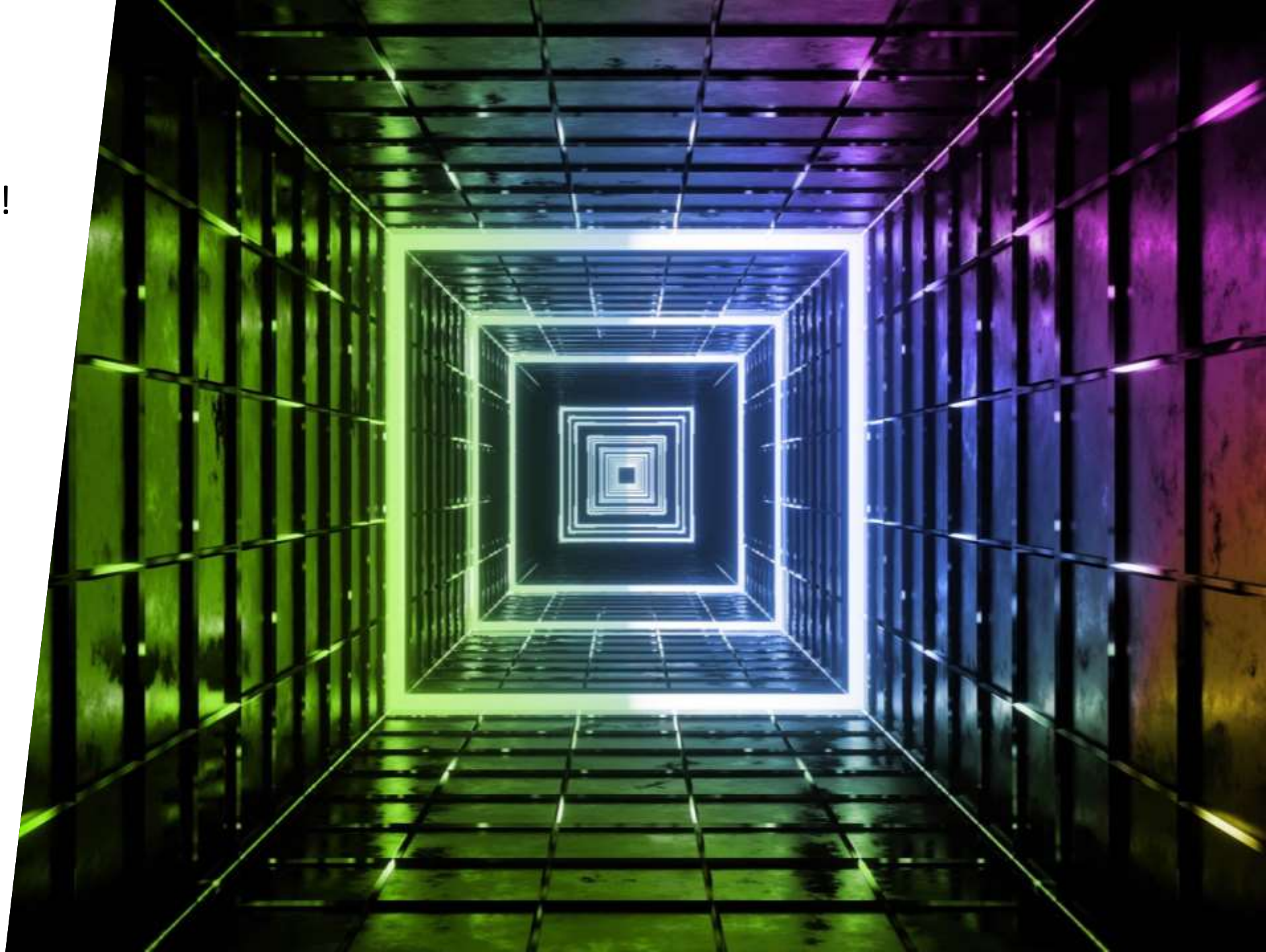
Herzlich Willkommen!

fernaomagellan

secure mode on



Mission Accomplished

„Es gibt etwa 15 bis 50 Fehler oder Bugs pro 1000 Zeilen gelieferten Codes. Dennoch wies die missionskritische Space-Shuttle-Software der NASA keinerlei Codefehler auf. Diese unglaubliche Leistung wurde jedoch mit Kosten von Tausenden von Dollar pro Codezeile erreicht.“

- Steve McConnell

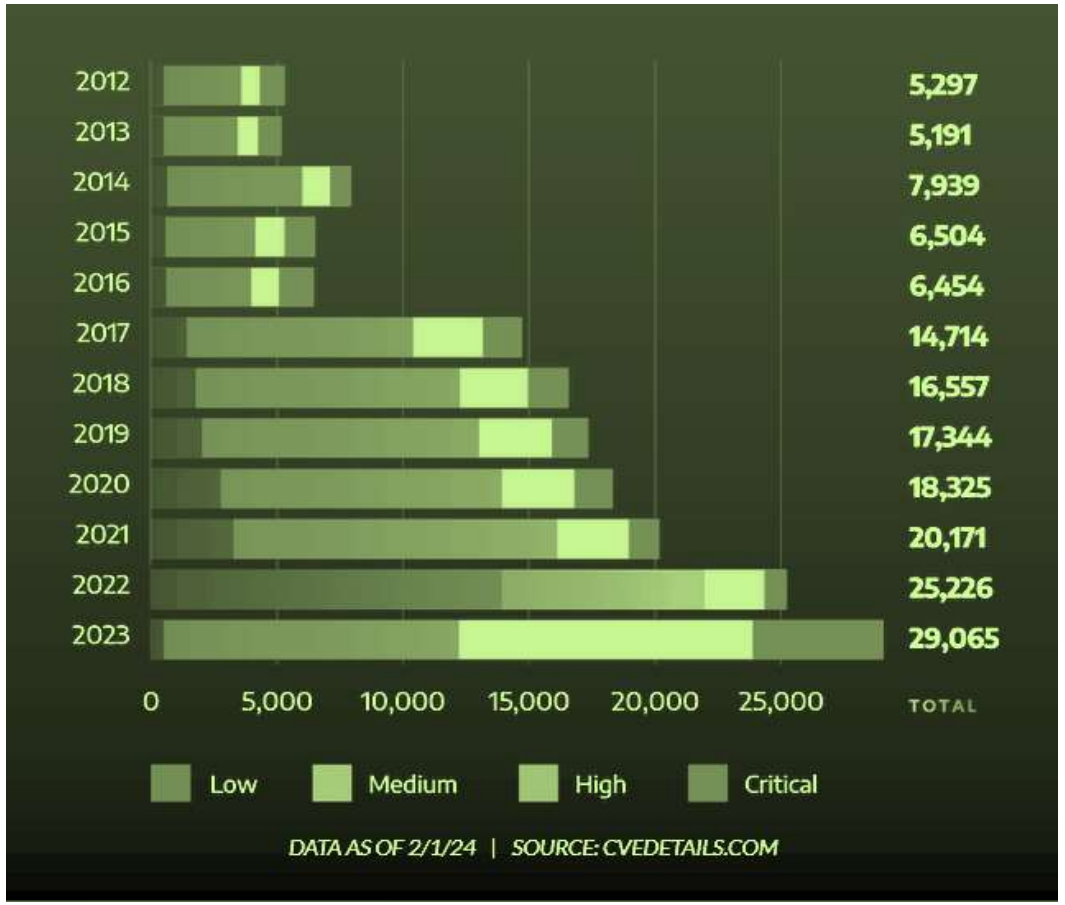
Anstieg von Schwachstellen

VMware vSphere
CVE-2021-21980

Microsoft Sharepoint
CVE-2023-29357

Juniper Networks
CVE-2024-21591

Citrix NetScaler
(Session Hijacking)
CVE-2023-4966



ProxyNotShell
CVE-2022-41082

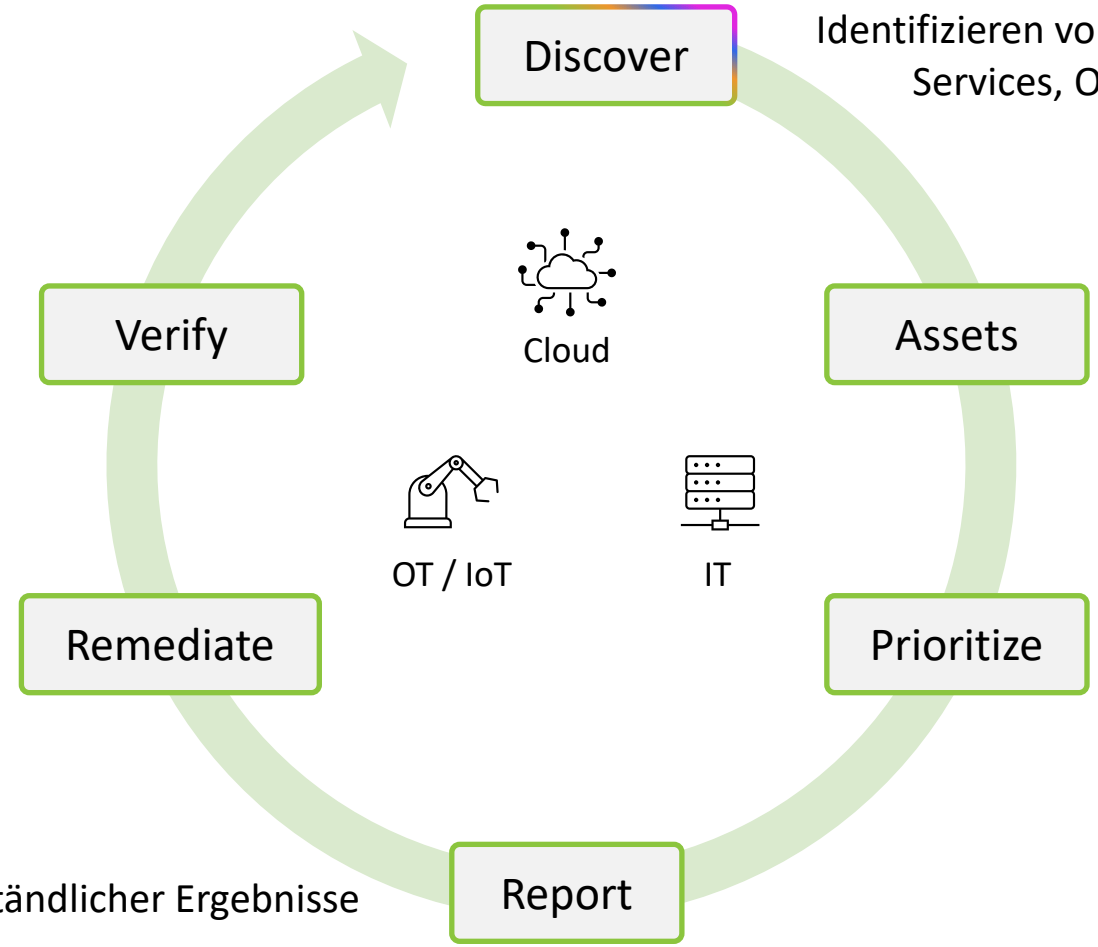
OpenSSL 3.0-3.0.6
CVE-2022-3786

Apache ActiveMQ
CVE-2023-46604

Windows Hyper-V
CVE-2024-21407

Barracuda Email Security Gateway
CVE-2023-2868

Vulnerability Management Lifecycle



Identifizieren von Assets, Applikationen, Services, OS, Konfiguration

Durchführung von Schwachstellen-Scans

Bewerten und Priorisieren

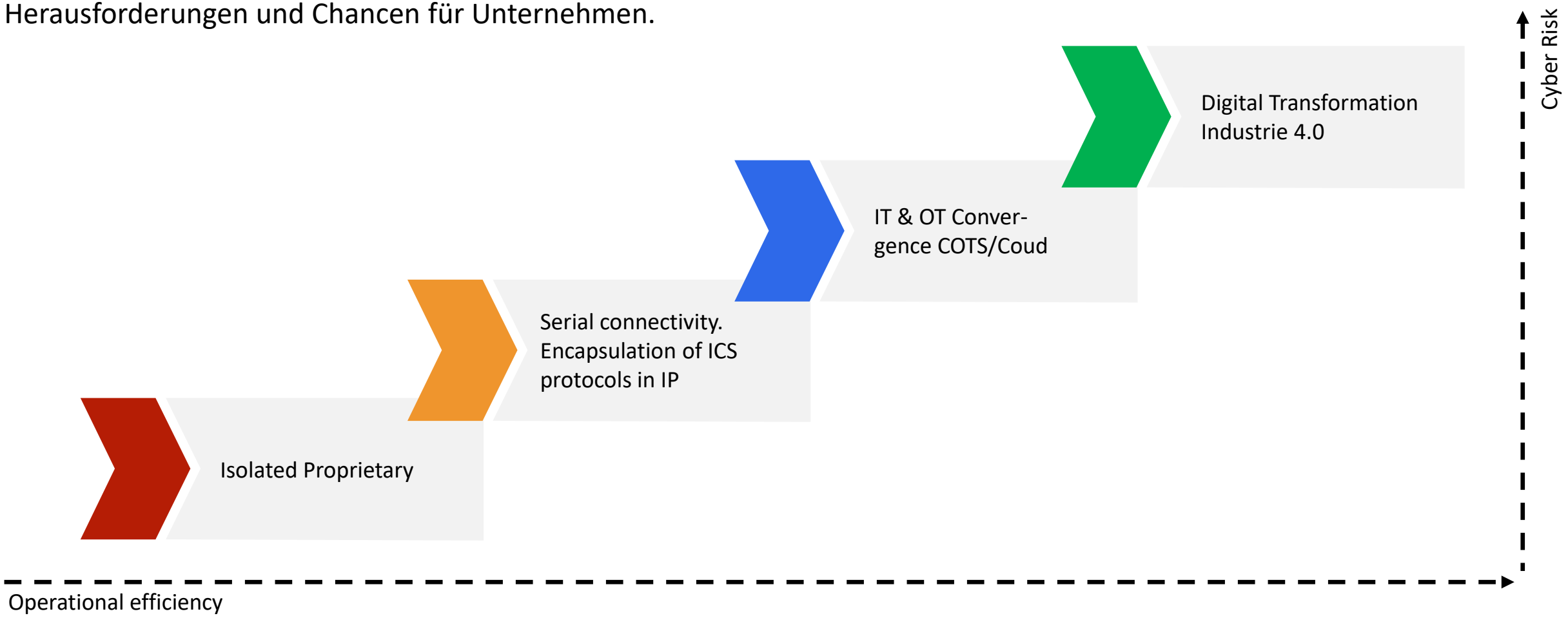
Erstellung verständlicher Ergebnisse

Abhilfemaßnahme erstellen und beheben

Prüfen ob Schwachstellen beseitigt wurden

OT-Evolution

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



Warum?

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 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.

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

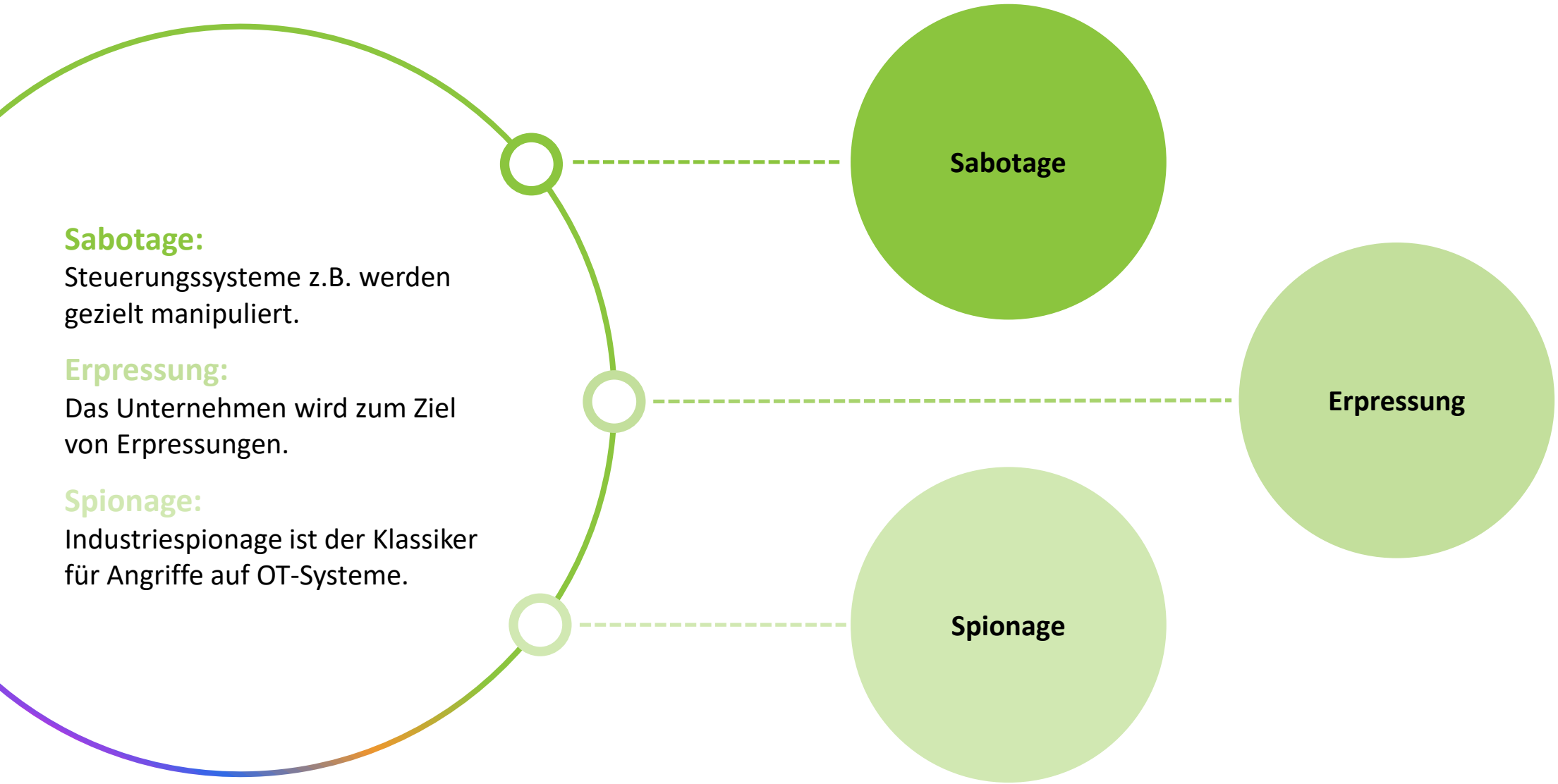
Schutz von geistigem Eigentum:
OT-Systeme enthalten oft wertvolles geistiges Eigentum, wie z. B. Produkt-designs oder Produktionsdaten. Ein Cyberangriff könnte zu Diebstahl oder Missbrauch dieses geistigen Eigentums führen.

Angriffsmotivation?

Sabotage:
Steuerungssysteme z.B. werden gezielt manipuliert.

Erpressung:
Das Unternehmen wird zum Ziel von Erpressungen.

Spionage:
Industriespionage ist der Klassiker für Angriffe auf OT-Systeme.



Vorgehen?

01 Grundlegende Analyse der OT-Landschaften

- Sichtbarkeit erstellen

02 Analyse der Kommunikationswege

- Network Communication Visibility

03 Asset Management aufbauen

- Inventory / Overall Device View

04 Schwachstellenanalyse aufgrund der Daten

- Vulnerability Identification

05

Handlungsempfehlung zur Umsetzung

- **OT-Security-Strategie** -

Top 5 Angriffsziele

01

Historisch gewachsene Systeme

02

Engineering Workstations

03

SPS/PLC´s

04

Automatisierungs-Server

05

Scada Server

fernao magellan im House of Experts

Digital Infrastructure
- Virtualization
- Switching & Routing
- Software Defined Networking (SDN)
- Server & Storage
- Mobility (WLAN Infrastructure)
- Managed Campus Network
- Identity & Access Management (IAM)
- DNS, DHCP & IPAM Security
- Data Center Automation
- Backup Solutions

Data & Analytics
- Logfile Management
- Business Analytics
- Security Information & Event Management (SIEM)

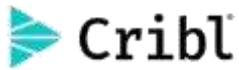
Cyber Security & Defense
- Extended Detection & Response (XDR)
- Endpoint Detection & Response (EDR)
- Next Generation Firewall (NGFW)
- Vulnerability Management
- Web Application Firewalls (WAF)
- Secure Access Service Edge (SASE)

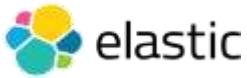
Network Visibility
- Packet Broker & Taps
- OT Network Visibility
- Monitoring Tools

Unsere Services:

- **Managed Network Services**
- **Managed Security Services**
- **Managed SOC**
- **Incident Response Services**
- **Network Visibility Services**

Auszug unserer Technologiepartner





Vielen Dank!

Wir sichern Ihren Geschäftserfolg.
Alles andere ist nur IT.

Follow us on LinkedIn

Daniel Khoshmashrab

Business Manager

Frank Sommerhoff

Managing Consulting Network Visibility

fernao