CLUE
CYBER SECURE

# Cyberangriffe stoppen, bevor es kritisch wird

Praxisnahe Sicherheit für Ihre Produktion

Elija Boss

30.10.2025

# Agenda

- Vorstellung CLUE
- Cyber / Survival
- OT Security Challenges
- Lösungsansätze
- Take Aways & Fragen

# CLUE in a Nutshell

**3**
**CLUE Locations**
Baar, Zurich, Munich

**20+**
**Employees**
incl. 13 engineers

**2015**
**Founded in**

## Memberships & Partnerships

swiss made software +swiss hosting · SANS · OWASP · NEXT INDUSTRIES powered by SWISSMEM · ISECOM · DC4131

## Our work in numbers

**18**
Countries covered

**100**
Customers

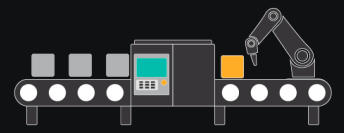
**300+**
Completed projects

**500+**
Managed assets

**>15k**
Protected end points

**>50k**
Protected identities

# Spezialisierung



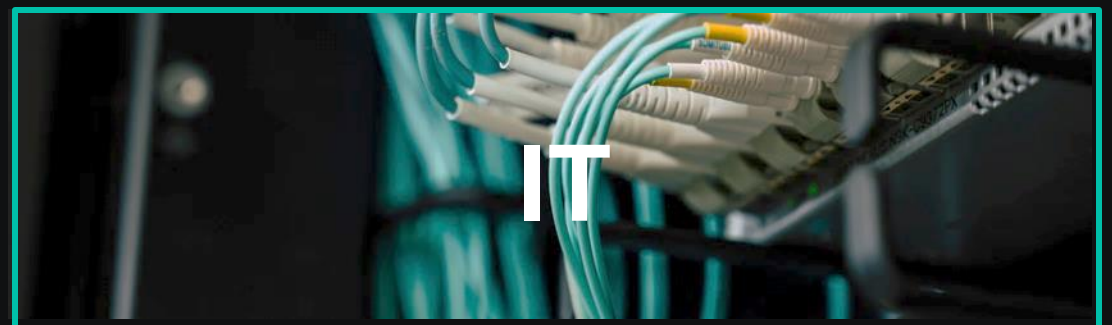
OT Security

Managed Detection & Response

Application Security

# Cyber (/) Survival

# IT vs OT




- ✓ Kurze Lebenszyklen (2–5 Jahre)
- ✓ Automatisiertes Asset Management
- ✓ Remote Support sicher etabliert
- ✓ Automatisiertes Patching möglich
- ✓ Verschlüsselte Kommunikation Standard
- ✓ Security by Design umgesetzt
- ✓ Standardisierte Security-Konzepte
- ✓ Cyber Security priorisiert

- ⚠ Lange Lebenszyklen (10–50 Jahre)
- ⚠ Fehlender Asset-Überblick
- ⚠ Remote Support Sicherheitsrisiko
- ⚠ Patching selten möglich
- ⚠ Kommunikation häufig unverschlüsselt
- ⚠ Security nachgerüstet (reaktiv)
- ⚠ Hohe Herstellerabhängigkeit
- ⚠ Fokus auf Verfügbarkeit (statt Security)

# Attack Chain on OT

Kill Chain Stage 1

Kill Chain Stage 2

### Reconnaisance

- Planning
- Preparation
- Discovery
- Footprinting
- Infiormation Gathering

### Preparation

- Phishing
- Spam
- Malware
- Vulnerabilities in IT

### Intrusion

- Install RAT
- Powershell Tools
- Malware deployment

### Mgmt. and Enablement

- C&C connect
- Multiple backdoors
- Futher access, use internal vulnerabilities

### Attack Deve-lopment & Test

- Tailor specific attack patterns
- Might break more then expected

### Validation

- Test capabilities
- Might happen ofline
- Could lead to Denial of Service

### ICS Attack

- Install or modify system functionality
- Attack on the ICS
- Manipulation of systems
- Light out attack

Cyberattacks on OT environments often originate from traditional IT breaches. In most cases, attackers first exploit vulnerabilities in internet-facing systems or target employees through phishing. These initial intrusions typically occur during the reconnaissance phase.

After finding a “way” into the corporate network, backdoors are opened and multiple backup access paths are implemented. From then on, further reach into the OT networks are the next steps.

In the “Attack Development” and “Validation” steps, OT systems might already be affected by a DOS. Also random OT malware like Stuxnet might be introduced to the network without a active part on the attacker side, that will break things. These steps might be timed over a longer period of time.

At that point, random systems might be out of control. To get back control, a full shutdown and recovery will be required.

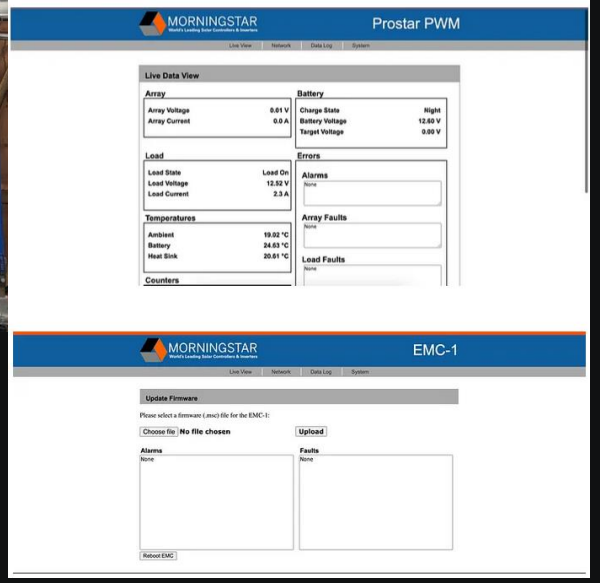
Normal behaviour

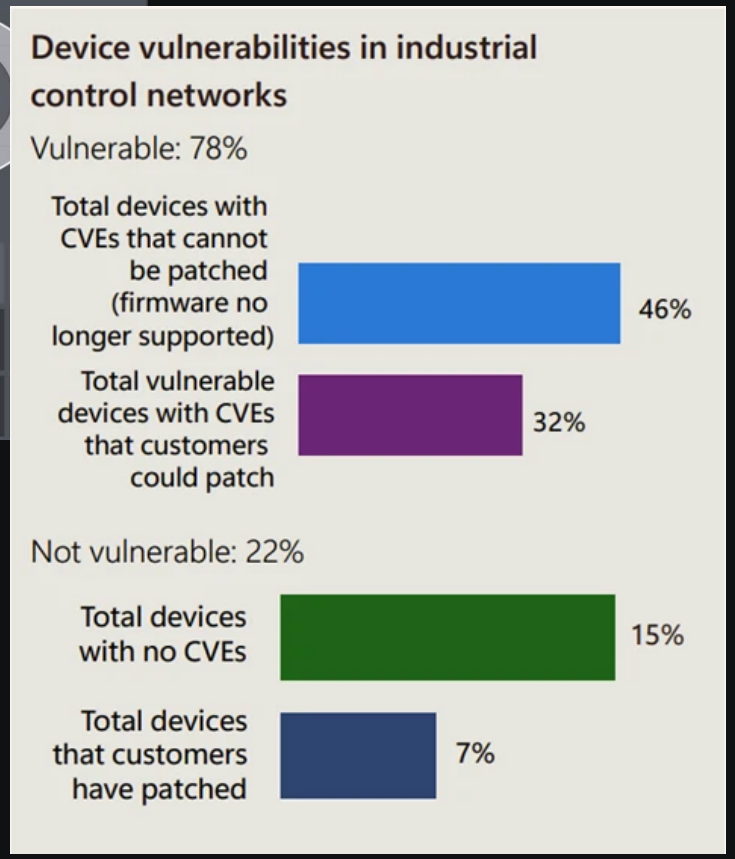
Annomalities

Production outage

# Fallbeispiele

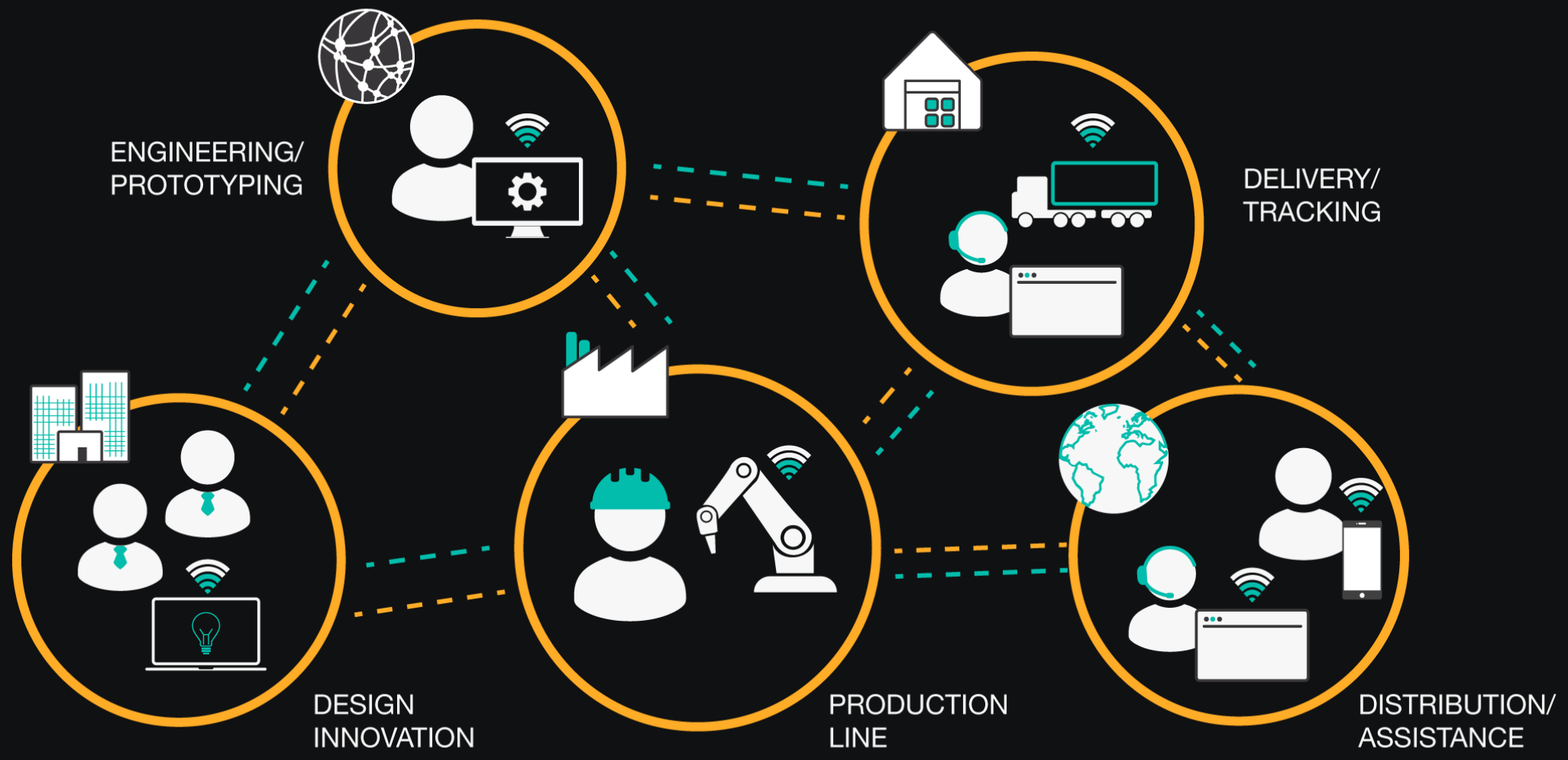
PoC? Just open the IP in a browser — no login, no credentials, full access.



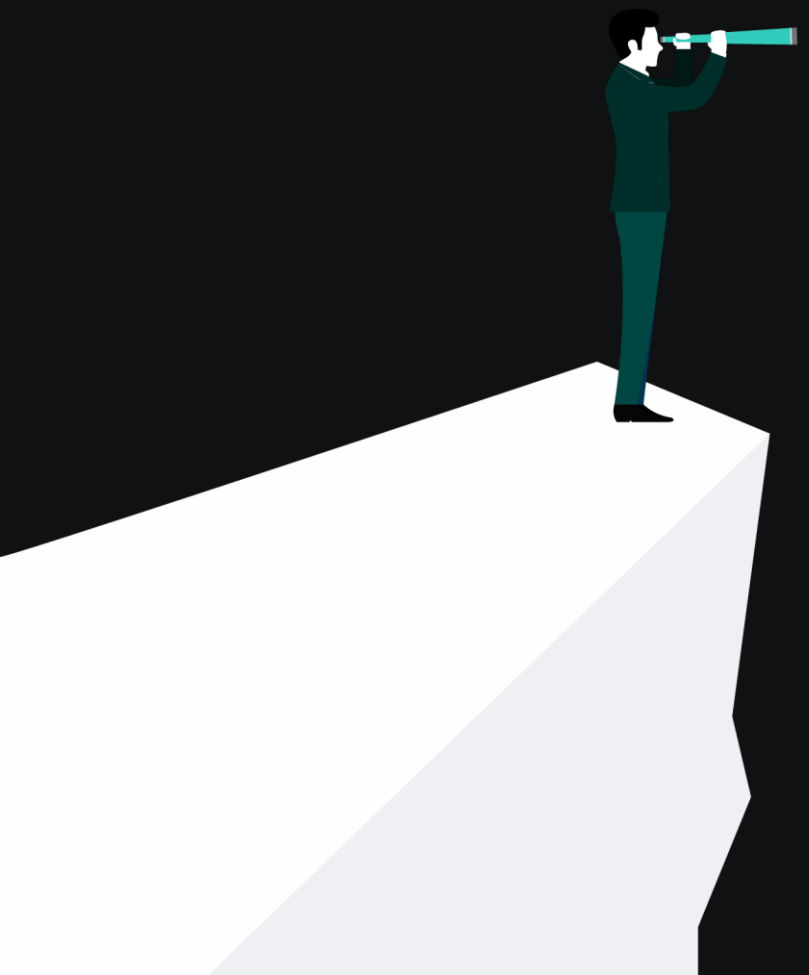
# OT Security Challenges

## Supply Chain Security



# OT Security Challenges

## Entwicklung der Bedrohungslage
## - 2023 vs 2024 -



Zunehmende Digitalisierung & Verschmelzung von IT/OT vergrössert Angriffsflächen sehr schnell

- 2.5x mehr Störungen in OT-Umgebungen im 2024

Vermehrt politisch und staatlich motivierte Angriffe, hoch personalisiert und automatisiert (KI)

- 3x mehr Angriffe aus China, Russland und dem Iran

Bereits bekannte Angriffsmuster nehmen ab, was die Erkennung massiv erschwert

- Drei neue ICS-spezfisiche Malware-Stämme allein im 2024 - halb so viel, wie in den letzten 14 Jahren

# Game of Survival

Schutz

Wasser

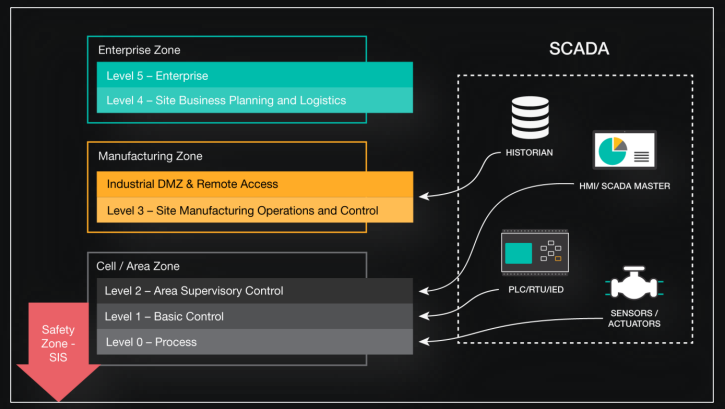
Nahrung

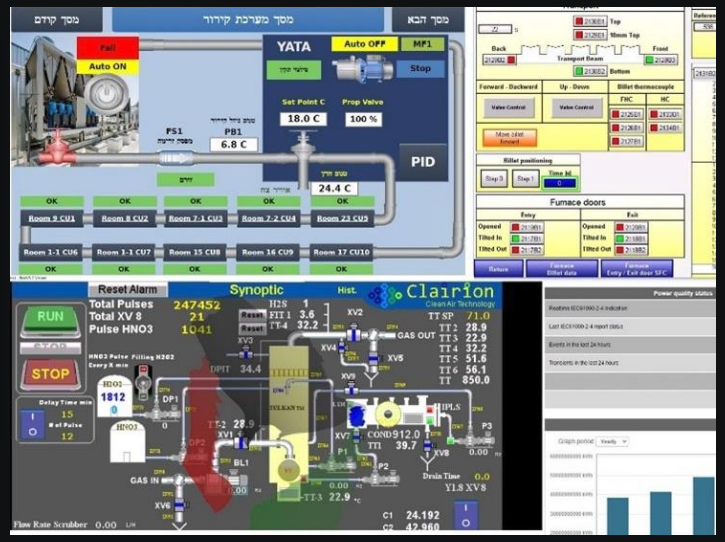
# Game of Survival

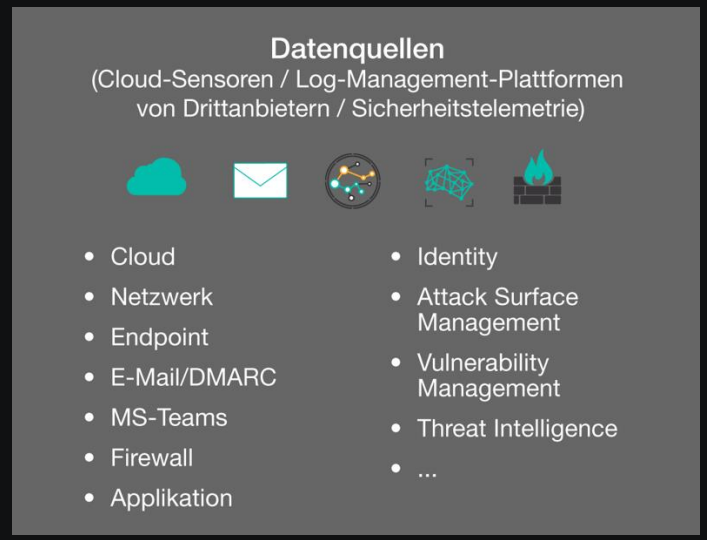
## Schutz

## Wasser

## Nahrung



# Angriff & Verteidigung

**1**
**Initial Access/Infection**

Der Angreifer erhält den ersten Zugriff auf das Zielsystem oder -netzwerk.

**2**
**Establish Foothold**

Der Angreifer etabliert eine stabile Verbindung, um die Kontrolle aufrechtzuerhalten.

**3**
**Privilege Escalation**

Der Angreifer versucht, höhere Zugriffsrechte zu erlangen.

**4**
**Internal Reconnaissance**

Der Angreifer bringt mehr über die Netzwerkstruktur und die Assets in Erfahrung.

**5**
**Lateral Movement**

Der Angreifer erweitert seine Kontrolle im Netzwerk.

**6**
**Exfiltration & Impact**

Der Angreifer stiehlt Daten und führt schädliche Aktionen durch (z.B. Verschlüsselung).

## KILLCHAIN

## NIST / IKT

**1**
**Identify**

Inventar, Geschäftsumfeld, Vorgaben/Zuständigkeiten, Risikomanagement

**2**
**Protect**

Zugriffsverwaltung, Sensibilisierung, Datensicherheit, Unterhalt, Schutztechnologien

**3**
**Detect**

Anomalieerkennung, Überwachung, Detektion

**4**
**Respond**

Reaktionsplanung, Kommunikation, Analyse, Mitigation, Optimierung

**5**
**Recover**

Wiederherstellungsplan, Verbesserungen, Koordination

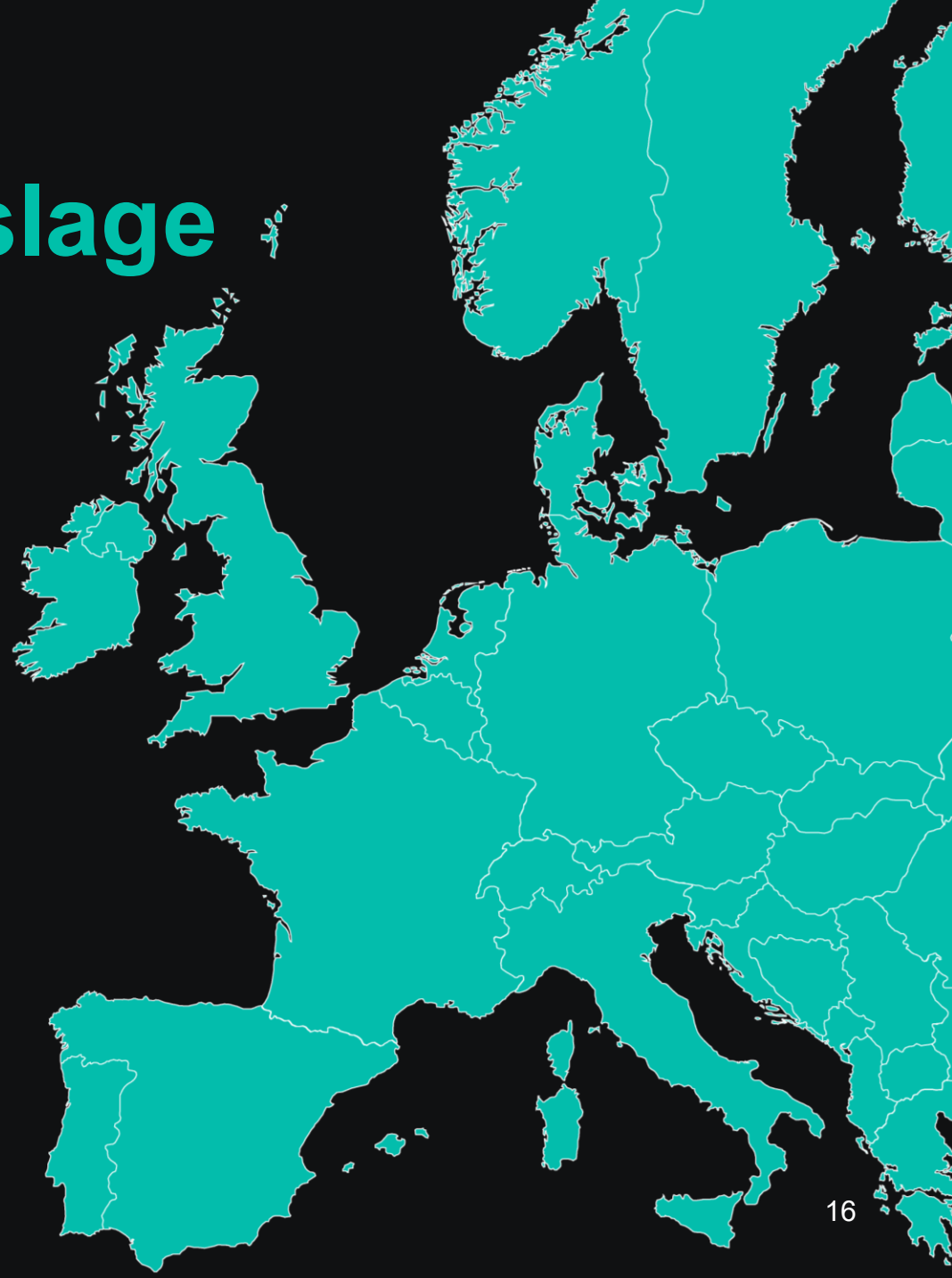
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

# Lösungsansatz auf Herstellerseite & Gesetzeslage

Cyber Resilience Act & Maschinenverordnung

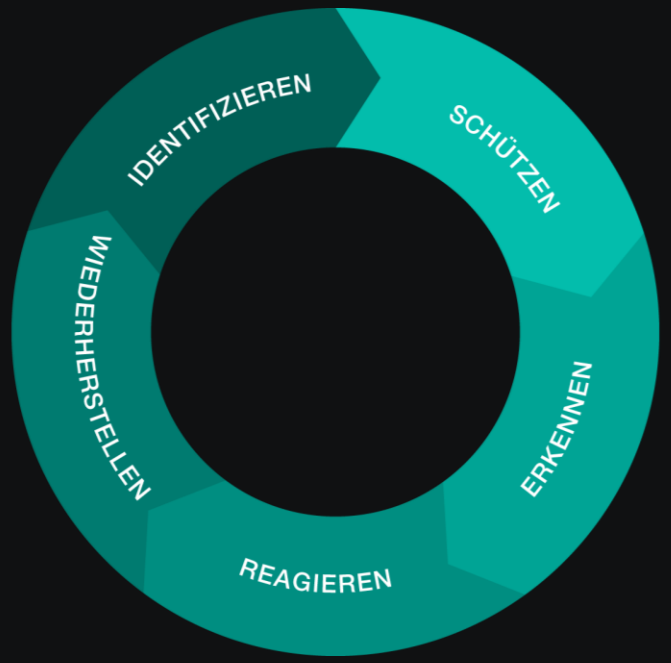
Der Cyber Resilience Act (CRA) und die neue Maschinenverordnung sind bedeutende EU-Gesetzesentwürfe, die sich vor allem an die Hersteller von digitalen Produkten und Dienstleistungen richtet und mitunter darauf abzielen, die Cybersicherheit in Europa zu stärken. Die wichtigsten Punkte umfassen:

- Einheitliche Sicherheitsanforderungen über gesamten Lebenszyklus
  - Schutz vor Manipulation «Secure by Design»
  - Regelmässige Updates & Schwachstellenverwaltung
  - Produkt-Klassifizierung & Risikobewertung
  - Dokumentations- & Informationspflicht
- Konformitätsbewertung
  - Voraussetzung für CE-Kennzeichnung
- Sanktionen bei Verstössen
  - **Inkrafttreten ab Ende 2026 / Anfang 2027**



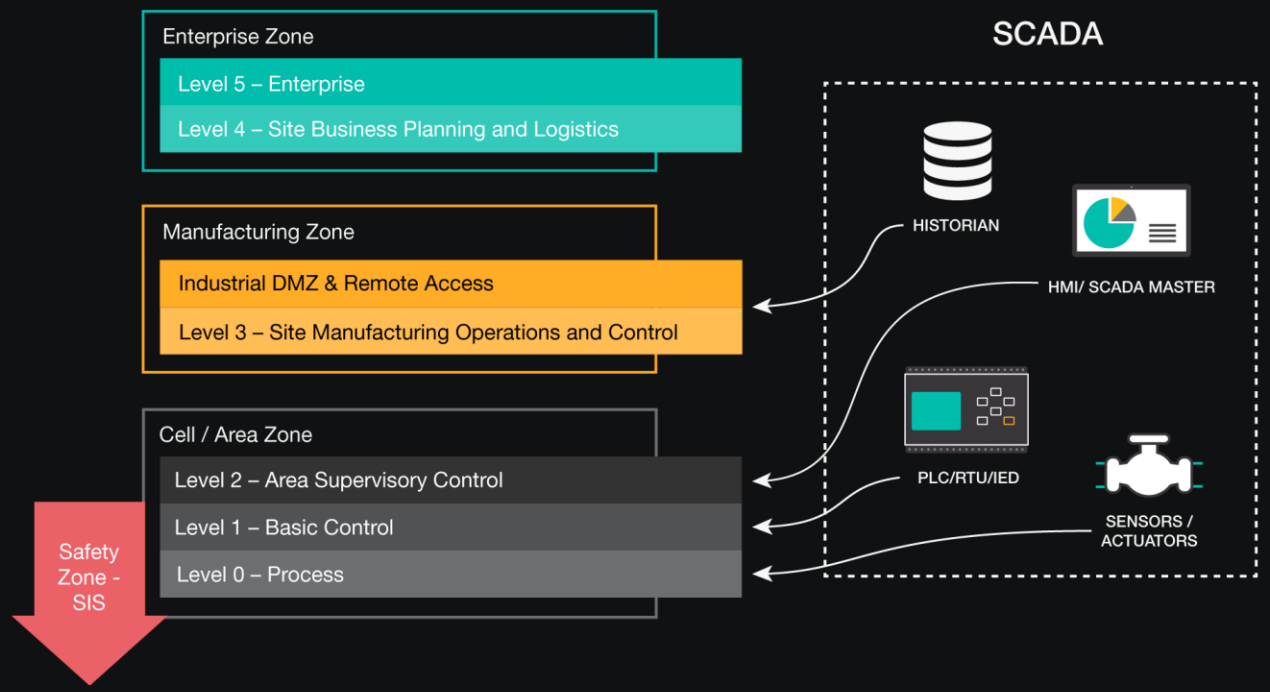
# Massnahmen auf Betreiberseite

- ❑ Asset Management
  - OT Assets Inventar (kennen, was zu schützen ist)
  - Organisation (Verantwortlichkeiten)
  - Prozesse (Anschaffung, Inbetriebnahme, Changes)
- ❑ Prozesse etablieren
  - Desaster Recovery and Planning
- ❑ Klare und transparente Strukturen
  - Mikrosegmentierung
  - Zugriffsberechtigung
  - Netzdesign
  - Standards (IEC62443 / Purdue)
- ❑ Secure Remote Access
- ❑ Verschlüsselte Kommunikation
- ❑ Security Monitoring auf verdächtiges Verhalten auf Ebene Netzwerk/Kommunikation & Betriebssystem

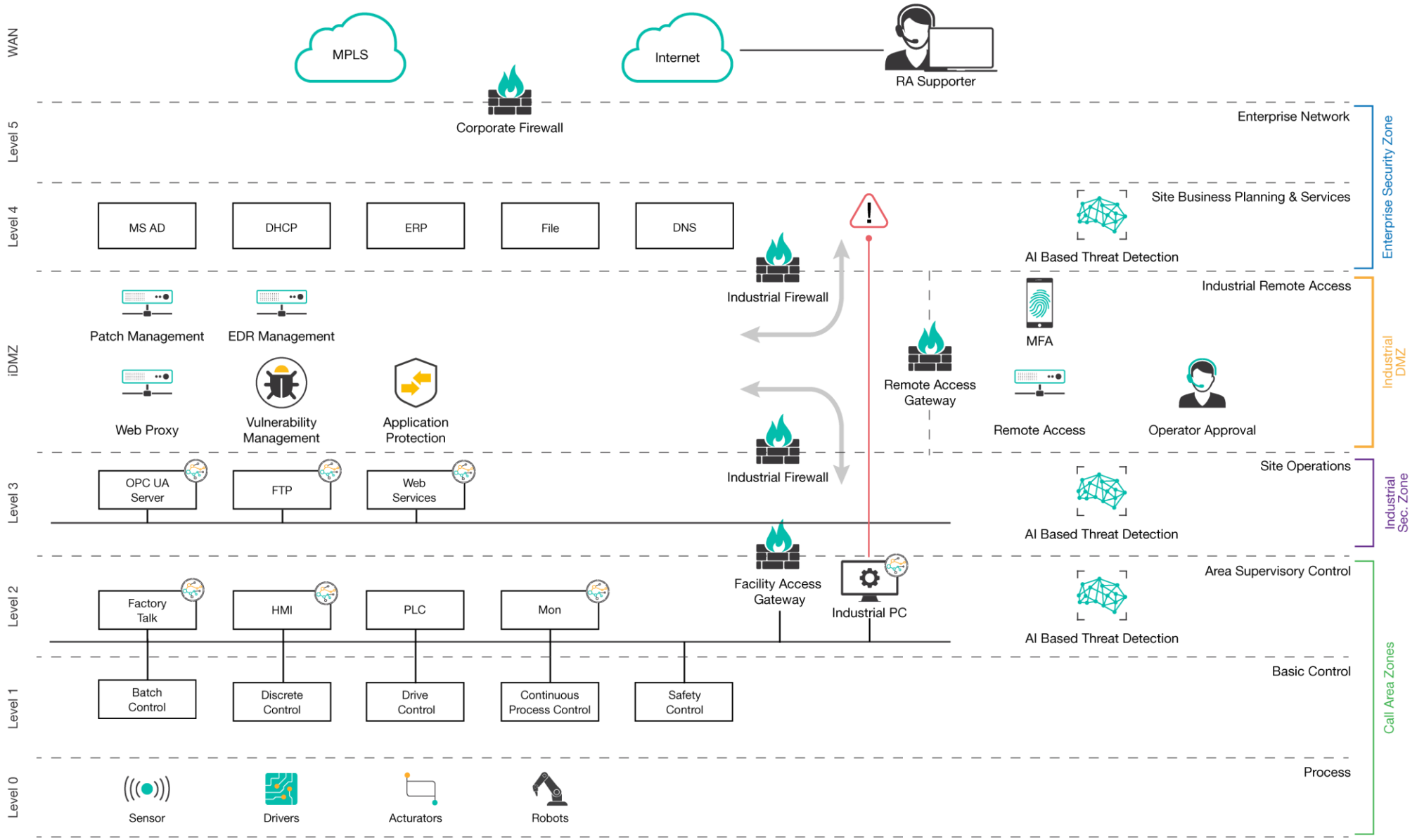


# OT Security Framework (Purdue / IEC62443)

- Das Purdue-Modell ist ein Schichtenmodell, das in der Industrieautomatisierung und im Bereich der IT- und OT-Sicherheit verwendet wird
- Es dient der strukturierten und sicheren Integration von IT- und OT-Systemen in der industriellen Automatisierung
- Das Modell teilt die Netzwerkarchitektur von industriellen Systemen in verschiedene Ebenen, um die Prozesse zu segmentieren und eine bessere Übersicht und Sicherheit zu gewährleisten
- Alle involvierten Komponenten werden in 5 Security Zonen unterteilt
- Ziele des Purdue-Modells:
  - Netzwerksegmentierung
  - Sicherheitskontrollen
  - Klar definierte Kommunikation
- Das Model ist weltweit akzeptiert und wird von kleinen bis zu globalen Unternehmen angewendet
- IEC 62443-Normen stellen detaillierte Sicherheitspraktiken und -richtlinien zur Implementierung des Purdue-Modelles bereit



# Übersicht Purdue-Modell



# Referenz Architektur

**Zonen & Conduits** nach IEC 62443, Purdue

**Remote-Access-Gateway** terminiert Remote Access, erzwingt starke Authentifizierung, optimal mit bestehender Identität, erzwingt Geo und zeitbasierten (Just-in-Time) Zugang

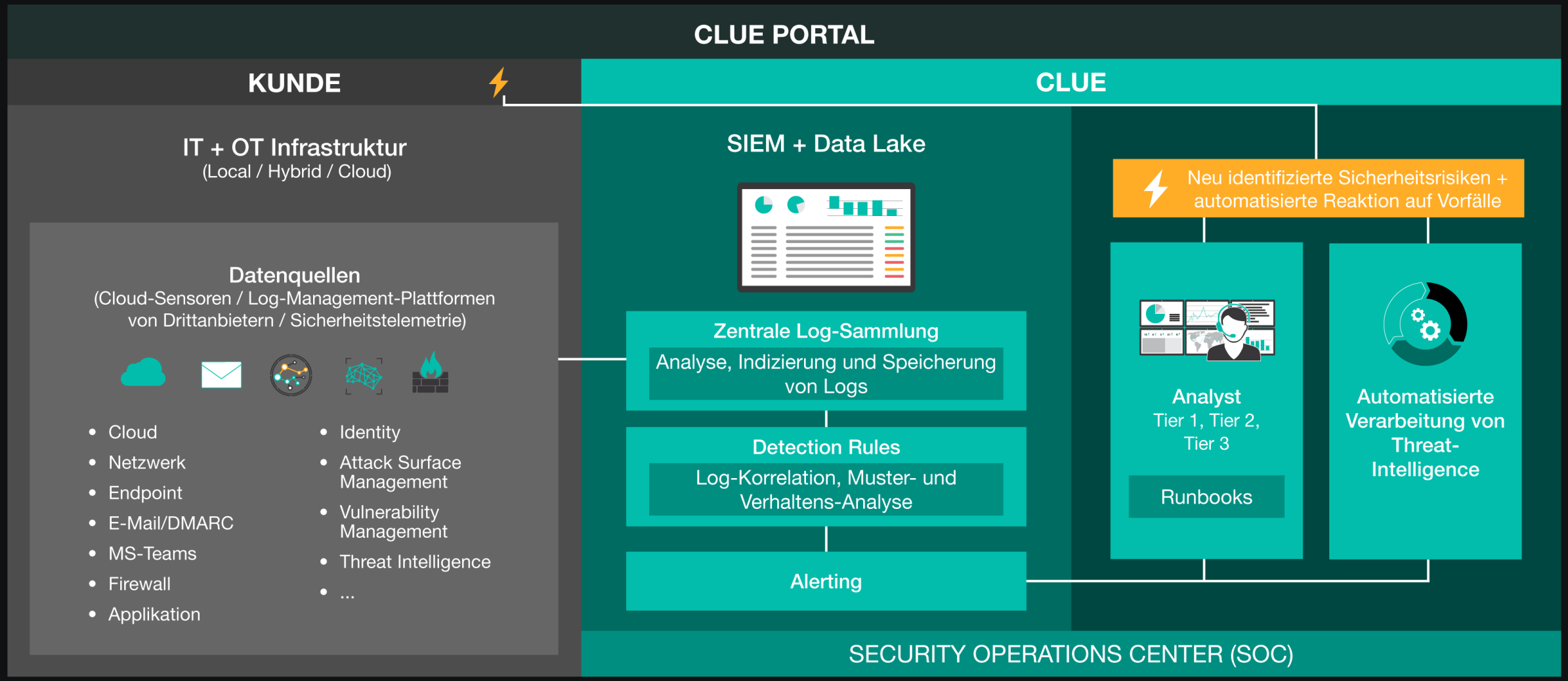
**Jump Host in der OT-DMZ**: Single-Path, Clipboard/Datei-Transfer kontrolliert, Session-Recording

**Privileged Access Management / Credential Broker**, User erhält ein Einmalpasswort, wo möglich z.B. Jump-Host

**ICS-DPI Sensoren**, ICS Protokoll Verständnis (Modbus, S7, OPC UA), verhaltensbasierte Anomalieerkennung und Auswertung, autonome Reaktion bei Fehlverhalten

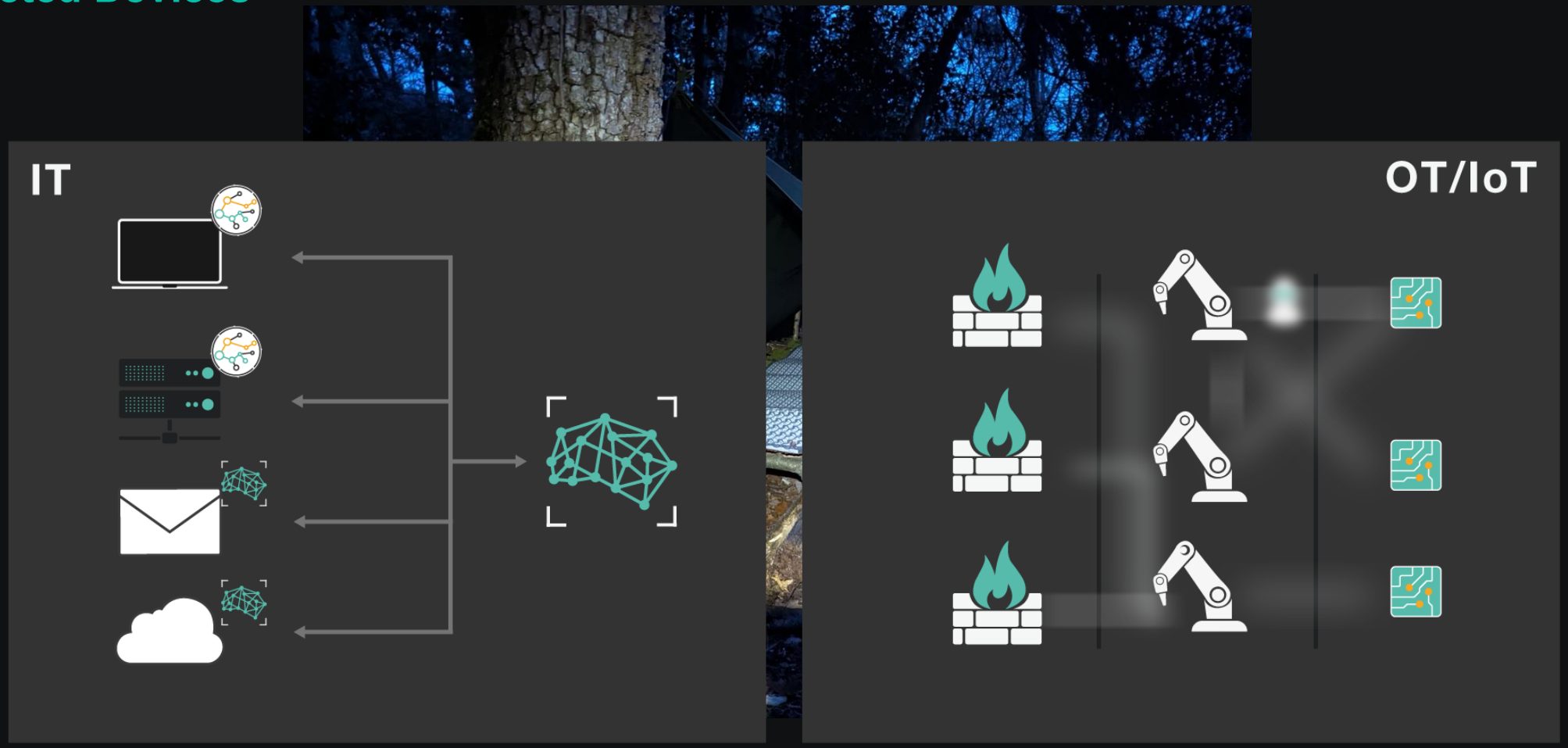
**Security Monitoring / SOC,** Korrelation der verschiedenen Events, Login, Autorisierung, 4-Augen Freischaltung, PAM, Logs auf Jumphost, Incident Daten des IPS und der Verhaltensanalyse

# Security Monitoring



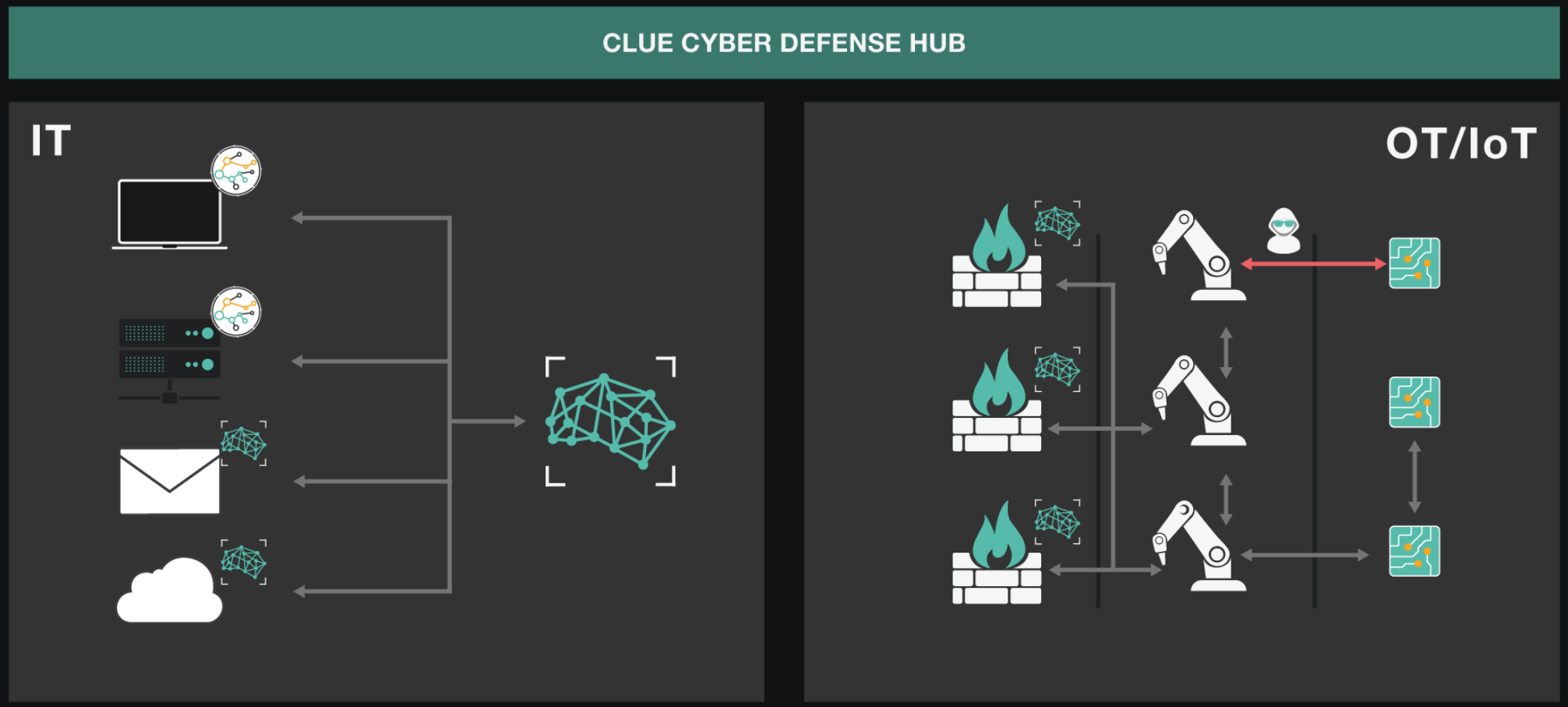
# Cyber Bushcraft

## AI Injected Devices



# Cyber Bushcraft

## AI Injected Devices



# Key Take Aways

Industrieanlagen sind ein lohnendes und häufig **einfaches Ziel** für Angreifer

Die meisten Angriffe beginnen noch immer in der IT, wobei die **Lieferkette** oft vergessen wird

Eine granulare **Segmentierung** und **Zugriffsregelung** ist unerlässlich

**Verordnungen**, **Normen** und **Standards** bringen Herausforderungen, aber auch Chancen

Eine kontinuierliche **Anpassung** und **Überwachung** schafft Ruhe und Vertrauen

# Your CLUE Contact

Elija Boss

Sales Representative

CLUE Security Services AG
Neuhofstrasse 12
6340 Baar

Email: info@clue.ch
Telephone: +41 44 667 77 66