



**“KRITISCHE  
INFRASTRUKTUREN”**



**HONEYWELL  
FORGE**

Cybersecurity<sup>+</sup>

**Honeywell  
Cyber  
Insights**

**Honeywell  
Cyber Watch**

**Honeywell  
Cyber Watch  
Governance**

**ECHZEIT “Passive NDR”**

**CYBER-SICHERHEITSPLATTFORM**

**KONFORM MIT DTOPTR & EMRA & INTERNATIONALEN (ISA IEC62443, NIST, NERC, NIS...) VORSCHRIFTEN UNSERE DIENSTLEISTUNGEN IM BEREICH CYBERSICHERHEIT BEI IKS UND KRITISCHEN VERSORGUNGSUNTERNEHMEN**

- Modernisierung des Netzwerks und der Sicherheit dem Digitalen Transformationsprozess
- Industrie 4.0 Digitale Transformation Sichere Datenerfassung und - Analyse
- IKS-Lösungen zur Einhaltung Gesetzlicher Vorschriften (IEC 62443/NIST/NERC/NIS/ISO27001)
- Aufbau eines IT-und OT-Cyber-Intelligence-Zentrum der Nächsten Generation und Kontinuierlicher Überwachung
- **MSSP - IKS Rotes Team SoC - Dienste**
- **MSSP - IKS Blaues Team SoC - Dienste**
- IKS - Anlagenerkennung, Analyse, Architekturdesign
- IKS - und OT - Netzwerk - und Sicherheitsbewertungsservice



ZUGRIFF AUF DOKUMENTE

**OTD BiLiSiM**

GLOBAL VAD



VIDEOS ANSEHEN

# OT-Sicherheit beginnt mit dem Verstehen von SCADA-Protokollen!

Modbus

ICCP

Profinet

OPC DA & UA

BACnet

Siemens Step 7

MQTT

Moxa

MMS

EtherCat

GE SRTP



## HONEYWELL FORGE

### Cybersecurity+



## Warum Honeywell Forge | Cyber Security+?

- Wir kehren uns von den Konzepten der "Geschlossen-isolierte Produktionssysteme" ab!
- OT-Netzwerke mit niedrigem Schutzniveau, empfindlicher Punkt von Unternehmen
- IT-Lösungen sind im OT wirkungslos, IIoTs erhöhen OT ntw Risk
- Die Notwendigkeit einer Segmentierung und einer kontinuierlichen Analyse des OT-Netzwerkverkehrs

## ERKENNUNG UND REAKTION IN ECHTZEIT "Passive NDR"



## TRANSPARENZ

Einschließlich Vermögensdetails verschaffen Sie sich einen vollständigen Einblick in OT- und IoT-Netzwerke, erhalten Sie Kommunikationsmodelle und Einblicke in Sicherheitslücken und Risiken.

## ANLAGENMANAGEMENT

Erhalten Sie eine automatisierte, genaue und echtzeitige Vermögensverzeichnis.

## RISIKOMINDERUNG

Indem Sie mögliche Angriffsvektoren aufdecken und Ihre Netzwerksicherheitshygiene verbessern, minimieren Sie Risiken, ohne Änderungen an Ihrem bestehenden Netzwerk oder Ihrer Infrastruktur vorzunehmen.

## ECHTZEITIGE FESTSTELLUNG VON BEDROHUNGEN

Mit einem nicht-intrusiven Ansatz erkennen Sie passiv Echtzeit-Bedrohungsindikatoren und gewinnen Sie Frühindikatoren für den Lebenszyklus von Cyberangriffen.

## SOFORTIGES EINGREIFEN

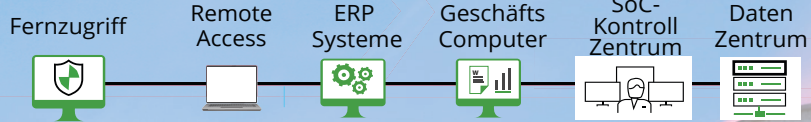
Mit bestehenden Sicherheitskontrollen und SecOps-Verfahren reagieren Sie sofort auf Bedrohungen mit einer nahtlosen Integration.

# OTD BİLİŞİM

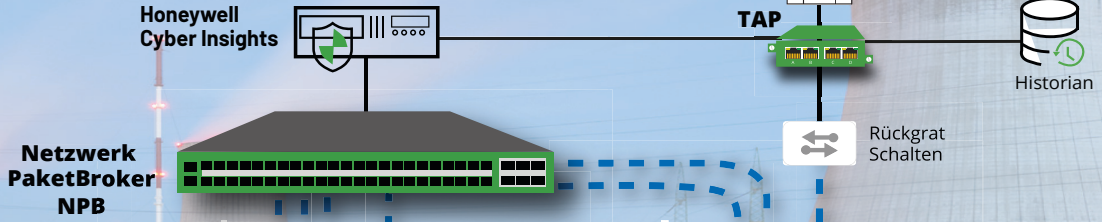
GLOBAL VAD



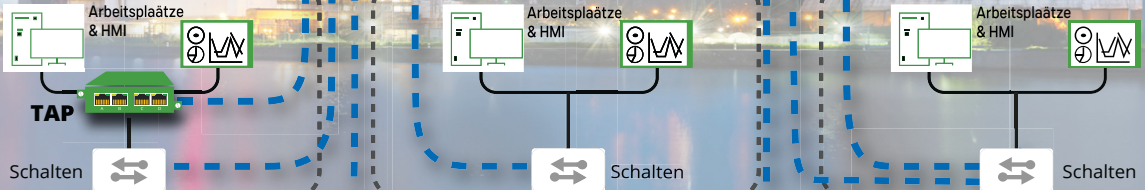
**Stufe 4**  
Unternehmen  
Logistik  
Systeme



**Stufe 3**  
Operationen  
Systeme



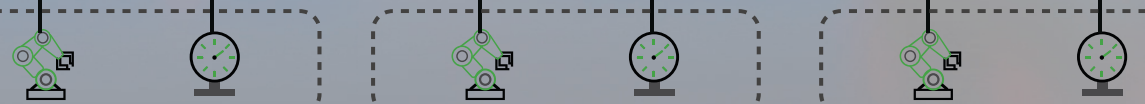
**Stufe 2**  
Kontrolle  
Systeme



**Stufe 1**  
Intelligent  
Geräte



**Stufe 0**  
Körperlich  
Verfahren



Lokale Anlage (SCADA/DCS/PLC)

Standort 2 (SCADA/DCS/PLC)

Standort 3 (SCADA/DCS/PLC)

NETZWERK-TAP-SICHTBARKEIT

SICHTBARKEIT DER TAP/SPAN-AGGREGATION



**INDUSTRIE 4.0**  
DIGITALE  
TRANSFORMATION

**BEDIENTE  
SEKTOREN**



**KRITISCHE  
INFRASTRUKTUREN**

- WASSER
- ÖL & GAS
- VERKEHR
- INTELLIGENTE STÄDTE
- ELEKTRONISCHE KOMMUNIKATION
- TELEKOMMUNIKATION
- BANKWESEN & FINANZENE
- KRITISCHE ÖFFENTLICHE DIENSTE
- FLUGHAFEN



**ENERGIE**

- KOHLE
- ERDGAS
- KERNKRAFTWERKE
- HYDROELEKTRISCHE KRAFTWERKE
- ERNEUERBARE ENERGIE
  - SONNE
  - WIND
  - GEOTHERMIE
- ENERGIEVERTEILUNG



**PRODUKTION**

- AUTOMOBILINDUSTRIE
- MEDIKATION
- LEBENSMITTEL & GETRÄNKE
- RAUMFAHRTINDUSTRIE
- CHEMIE
- GLAS
- ZEMENT
- EISEN - STAHL
- PAPIER



**BMS**

- KRANKENHÄUSER
- HOTELS
- DATENZENTREN
- ORGANISIERTE INDUSTRIEZONEN



**ANDERE**

- LOGISTIK
- BERGBAU
- VERPACKUNG & UMHÜLLUNG
- HAFEN
- VERSICHERUNG
- VERTEIDIGUNG





**HONEYWELL  
FORGE**  
Cybersecurity<sup>+</sup>

**SABOTAGE**

**Identifizierung  
Schützenswerter  
Anlagen**

**Schutz der  
Anlagen Assets**

**DATENPIRATERIE**

**Attacke  
Identifizieren/Identify**

**RANSOMWARE-ANGRIFF**

**Reagieren Sie auf  
den Angriff**

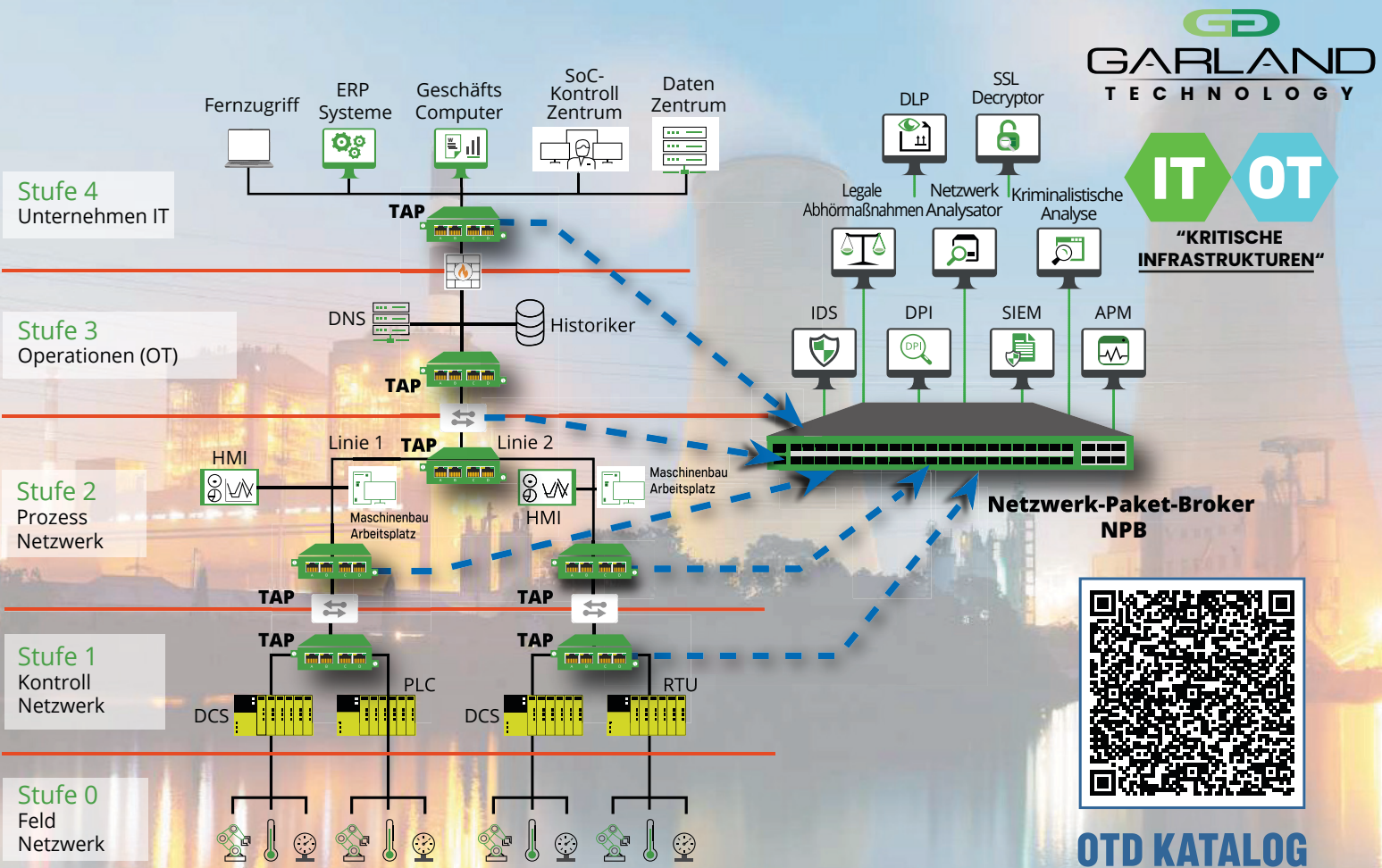
**ABSCHALTUNG DES SYSTEMS**

**Wiederherstellung  
Nach Einem Angriff**

**Sicherheit Beseitigung von Netzwerk  
Es Hinterlässt Keine Blinden Flecken**

“Machen Sie das  
Unsichtbare **SICHTBAR**”

**IT & OT (IKS) Informationsnetzwerks für Cybersicherheit**



**OTD KATALOG**

**TRETEN SIE UNSEREM Honeywell | SCADAfence NETZWERK BEI**  
Für Ihre IKS/OT-Sicherheits- und Gebäudemodernisierungsprojekte im In- und Ausland

**OTD BİLİŞİM**  
GLOBAL VAD

[www.onlineteknikdestek.com](http://www.onlineteknikdestek.com)