AUS DER PRAXIS

INDUSTRIAL MANAGED SECURITY SERVICES

HERBERT DIRNBERGER

.digital dirnberger

HERBERT DIRNBERGER

INDUSTRIAL IOT CONSULTANT

SENIOR AUTOMATION ENGINEER doka

ifh st.pölten LEKTOR SMART ENGINEERING

AUDITOR IoT AUSTRIA

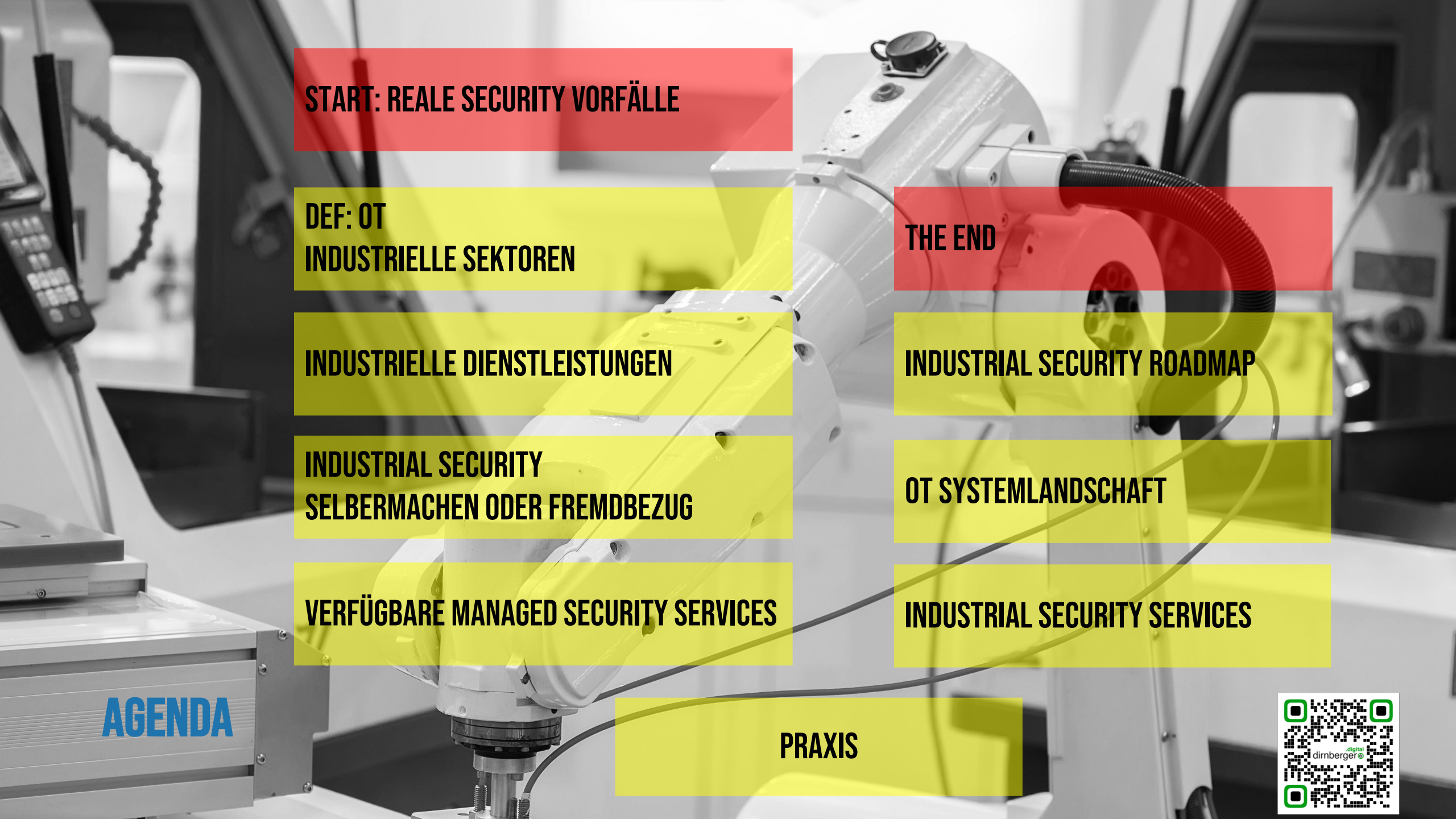
CYBER SECURITY AUSTRIA LEAD INDUSTRIAL SECURITY

CISM Certified Information Security Manager

CERTIFIED DIGITAL CONSULTANT

CERTIFIED DATA & IT SECURITY EXPERT

.digital dirnberger



AGENDA

START: REALE SECURITY VORFÄLLE

DEF: OT
INDUSTRIELLE SEKTOREN

INDUSTRIELLE DIENSTLEISTUNGEN

INDUSTRIAL SECURITY
SELBERMACHEN ODER FREMDBEZUG

VERFÜGBARE MANAGED SECURITY SERVICES

PRAXIS

THE END

INDUSTRIAL SECURITY ROADMAP

OT SYSTEMLANDSCHAFT

INDUSTRIAL SECURITY SERVICES

PUBLIZIERTE REALE SECURITYVORFÄLLE

ZAMG

ANFANG 2016

- KRITISCHE INFRASTRUKTUR
- MEHRERE SERVER FÜR EXTERNEN DATENAUSTAUSCH BEEINTRÄCHTIGT
- ANALYSE DURCH GOVCERT

A1

MÄRZ 2016

- DDOS
- MEHRTÄGIGE BEEINFLUSSUNG VON INTERNETDIENSTEN

WANNACRY MAI 2017

HOTEL/TECHNOLOGIEUNTERNEHMEN (Ö)

BULMOR INDUSTRIES

MÄRZ 2017

- DER OBERÖSTERREICHISCHE SEITENSTAPLERHERSTELLER WURDE GEZIELT DURCH EINEN MITARBEITER AUSSPIONIERT.
- MITARBEITER WOLLTE INFORMATIONEN ZU NEUEN SEITENSTAPLER INS AUSLAND UM 100.000 EUR VERKAUFEN.
- BEDROHUNG FÜR STANDORT MIT 150 MITARBEITERN
- ALARMIERUNG DURCH KONKURRENTEN

HTTPS://INDUSTRIEMAGAZIN.AT/A/SPEKTAKULAERER-FALL-IN-PERG-BULMOR-INDUSTRIES-KANN-SPIONAGE-ABWEHREN

DEUTSCHE BAHN (D)
KRANKENHÄUSER (GB)
RENAULT PRODUKTION (F)

ØSTFOLD KH (NOR)

SOMMER 2018

- WÄHREND DER UNTERSUCHUNG EINES PATIENTEN IN ANÄSTHESIE BEGANN DER PC AUTOMATISCH MIT DER AKTUALISIERUNG.
- UPDATE WAR ÜBERRASCHEND FÜR DIE MITARBEITER IM KRANKENHAUS
- DER VORFALL WAR FÜR DEN PATIENTEN NICHT GEFÄHRLICH
- MAßNAHME: UPDATES MÜSSEN MANUELL GESTARTET WERDEN
- DIE ROUTINEN WURDEN ÜBERPRÜFT UND GEÄNDERT, UND IM PRINZIP SOLLTE ES NICHT WIEDER PASSIEREN.

HTTPS://DERSTANDARD.AT/2000088110214/PC-UPDATE-WAEHREND-NARKOSE-KRANKENHAUS-MUSSTE-UNTERSUCHUNG-ABBRECHEN

INDUSTRIAL → OPERATIONAL TECHNOLOGY

INDUSTRIAL CONTROL SYSTEMS, SCADA, AUTOMATION UND INDUSTRIAL IT

INDUSTRIAL DEVICES/GERÄTE

- SCADA
- MEDICAL DEVICES
- ROBOTER FTS
- CNC
- IIOT
- HMI
- SMART GRID
- PLC

OT IST HARD- UND SOFTWARE FÜR DIE ÜBERWACHUNG, STEUERUNG UND REGELUNG VON PHYSIKALISCHEN EREIGNISSEN, PROZESSEN UND GERÄTEN IN ...

INDUSTRIAL SECURITY

- IIOT SEC
- CYBER SEC
- IT SEC
- RISIKO MANAGEMENT
- MED SEC
- ICS SEC
- SCADA SEC
- BUSINESS CONTINUITY MANAGEMENT

IT/IKT/CLOUD

INDUSTRIELLE SEKTOREN

(KRITISCHE INFRASTRUKTUREN)

- ENERGIE
- PRODUKTION
- TRANSPORT UND VERKEHR
- SMART CITIES
- ERNÄHRUNG
- GESUNDHEIT
- ÖL UND GAS
- WASSER-VERSORGUNG
- GEBÄUDE SMART BUILDINGS

INDUSTRIELLE DIENSTLEISTUNGEN FÜR DIE WERTSCHÖPFUNG

FALLBEISPIEL: UNIT PRODUKTION

OT IST HARD- UND SOFTWARE FÜR DIE ÜBERWACHUNG, STEUERUNG UND REGELUNG VON PHYSIKALISCHEN EREIGNISSEN, PROZESSEN UND GERÄTEN

ENERGIE, ENTSORGUNG
BAUINSTANDHALTUNG
REINIGUNG, WEKSSCHUTZ
GEBÄUDETECHNIK

ENGINEERING
ANLAGENBAU
RETROFITTING
VERLAGERUNG

ARBEITS-
VORBEREITUNG
TRAINING
PLANUNG &
STEUERUNG

ARBEITSSICHERHEIIT | INTRALOGISTIK | FACILITY SERVICES

WERTSCHÖPFUNG / PRODUKTION

IT/OT | INSTANDHALTUNG

INDUSTRIAL SERVICE

INDUSTRIAL APPS
SYTEM INTEGRATION
OT SERVICES

INCIDENT RESPONSE TEAM

MANAGED INDUSTRIAL SECURITY SERVICES

BETREIBER

INDUSTRIAL SECURITY: MAKE/BUY

SELBERMACHEN UND/ODER FREMDBEZUG

 # AUTOMATION **# DIGITALISIERUNG**

SCHNELLES WACHSTUM

→ ENGPÄSSEN IN DER INFRASTRUKTUR / MANPOWER / KNOW HOW

→ CLOUD → EDGE/FOG ZYKLUS

+ NICHT PATCHBARE SYSTEME (LEGACY)

+ LÄNGER OFFENE SCHWACHSTELLEN → SCHLECHT GESCHÜTZT

+ LEICHTE AUFFINDBARKEIT

+ STARKE CONNECTIVITY DER INDUSTRIAL GATEWAYS

→ INDUSTRIAL/IIOT DEVICES INTERESSANTE MITTEL FÜR ANGRIFFE,

DA IN FAST UNENDLICHEN MENGEN VERFÜGBAR UND CLUSTERBAR

- LOCAL/REMOTE
- FACH-/BRANCHEN KNOWHOW
- PROVIDER SKALENEFFEKTE

- AWARENESS
- SPEED / RESSOURCEN / ZEIT
- ABHÄNGIGKEIT
- TRANSPARENZ
- RISIKO/NOTFÄLLE

SICHERHEIT = RESOURCEN BÜNDELN

VERFÜGBARE MANAGED SECURITY SERVICES

(INDUSTRIAL)

ANTIVIRUS

BACKUP

VPN – REMOTE CONTROL

SECURE STANDARDS
SECURE PROTOCOLS
IEC 62443
ISO 27000
NIS

SYSTEM HÄRTUNG

APP WHITELISTING

AWARENESS TRAINING

INDUSTRIAL SECURITY CONSULTING

PATCH MANAGEMENT

SECURITY AUDITS

INCIDENT HANDLING

SECURITY OPERATION CENTER

VULN INFORMATION

RISK MANAGEMENT

PHYSICAL SECURITY

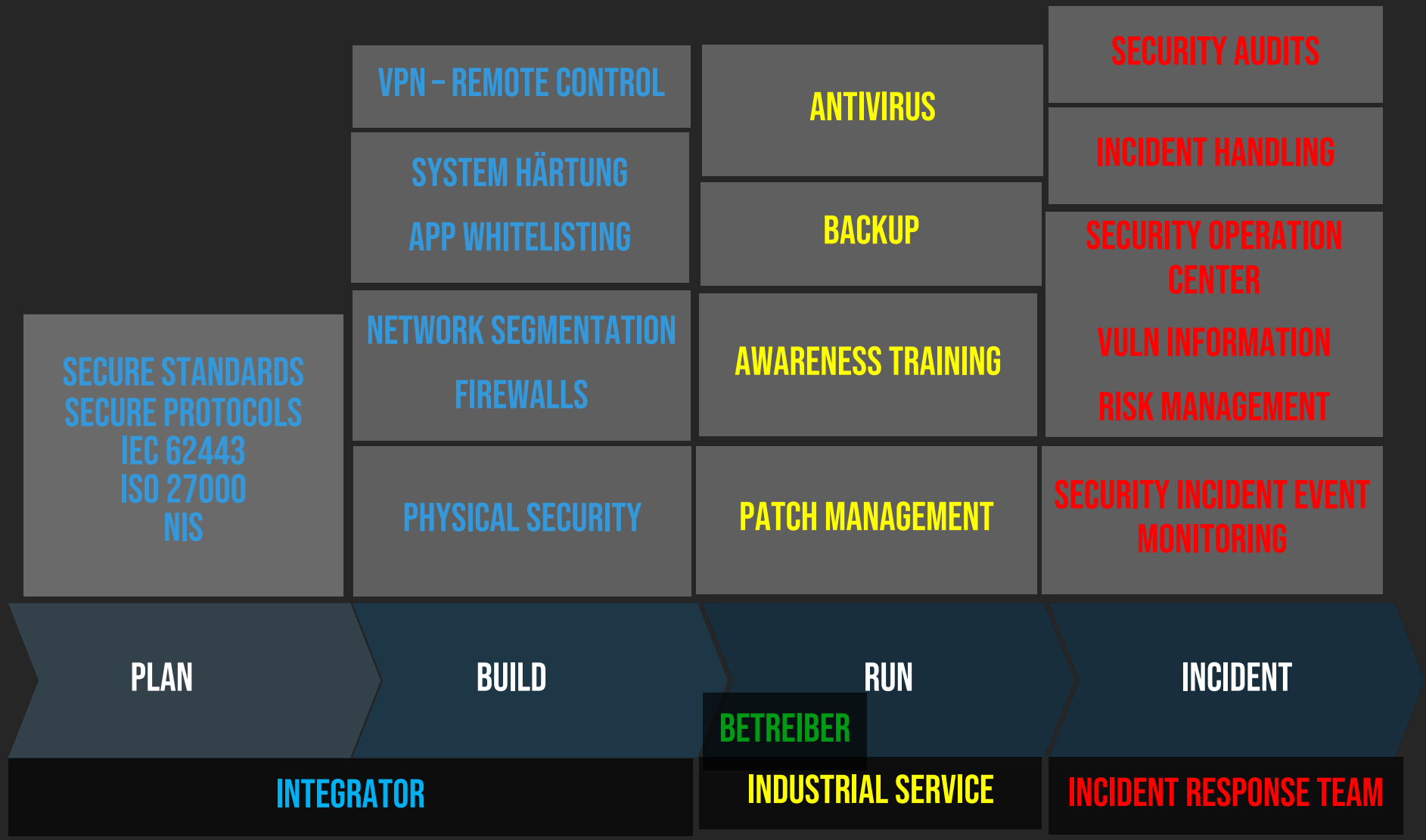
NETWORK SEGMENTATION

FIREWALLS

SECURITY INCIDENT EVENT MONITORING

INDUSTRIAL SECURITY LIFECYCLE

VERFÜGBARE MANAGEMENT SECURITY SERVICES



BETREIBER

INDUSTRIAL SERVICE

"... ODER MACHEN WIR UNS DIE PROBLEME SELBST"

90%

SELBSTGEMACHT

SCHLECHTE DOKUMENTATION, KEINE BACKUPS,
PROTOKOLLFEHLER, KEINE ZEIT, KEIN BEWUSSTSEIN,
ALTSYSTEME, KEIN SICHERES DESIGN, KEIN TIEFENSCHUTZ,
SCHLAMPIGKEIT, IGNORANZ FALSCHEINSCHÄTZUNG, ...

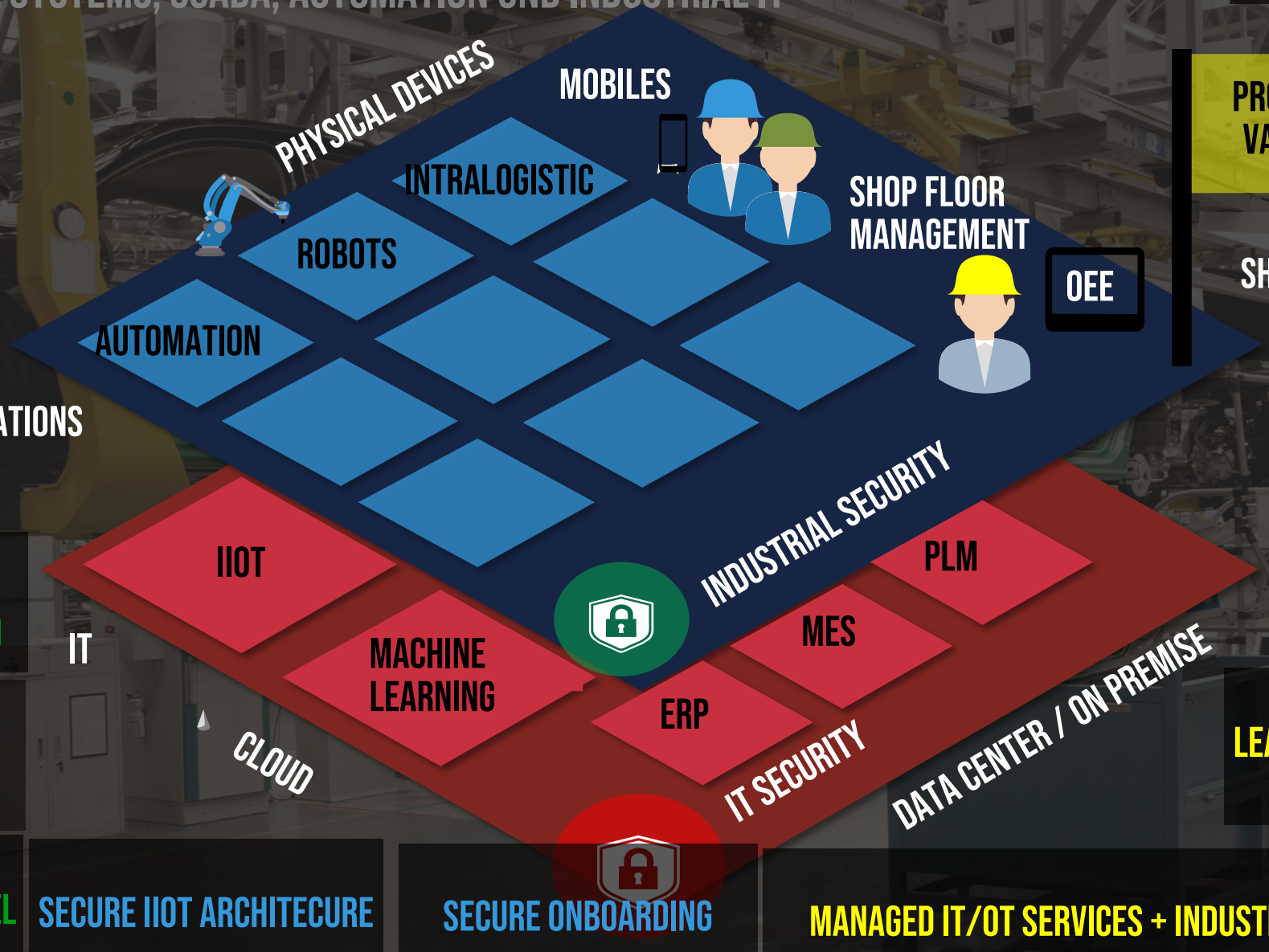
10%

HACKERS, SCRIPT KIDDIES, APT, CYBERCRIME, ...

SECURE OT SYSTEM LANDSCAPE FOR PRODUCTION

INDUSTRIAL CONTROL SYSTEMS, SCADA, AUTOMATION UND INDUSTRIAL IT

AWARENESS TRAIN ON JOB



PRODUCTION VALUE ADD

SHOP FLOOR

DATA

DATA

OPERATIONAL TECHNOLOGY

ENTERPRISE + OT APPLICATIONS
STORAGE, NETTWORKS

BUSINESS IMPACT

KRITIALKALITÄT (PLAN B)

IT

LCC, LEGACY, STRATEGY

LEAN PATCH MANAGEMENT

INDUSTRIAL SECURITY LEVEL

SECURE IIOT ARCHITECURE

SECURE ONBOARDING

MANAGED IT/OT SERVICES + INDUSTRAL SECURITY

INDUSTRIAL SECURITY LIFECYCLE++

BUSINESS IMPACT
KRITIALKALITÄT (PLAN B)

LCC, LEGACY, STRATEGY

SECURE STANDARDS
SECURE PROTOCOLS
IEC 62443
ISO 27000
NIS

VPN – REMOTE CONTROL

SYSTEM HÄRTUNG
APP WHITELISTING

NETWORK SEGMENTATION
FIREWALLS

PHYSICAL SECURITY

ANTIVIRUS

BACKUP

AWARENESS TRAIN ON JOB

LEAN PATCH MANAGEMENT

SECURITY AUDITS

INCIDENT HANDLING

SECURITY OPERATION CENTER
VULN INFORMATION
RISK MANAGEMENT

SECURITY INCIDENT EVENT MONITORING

INDUSTRIAL SECURITY LEVEL | SECURE IIOT ARCHITECURE | SECURE ONBOARDING | MANAGED IT/OT SERVICES +INDUSTRAL SECURITY

DEFINE | PLAN | BUILD | RUN | INCIDENT

BETREIBER

BETREIBER | INTEGRATOR | INDUSTRIAL SERVICE | INCIDENT RESPONSE TEAM

INDUSTRIAL SECURITY ROADMAP

5 ESSENTIALS STEPS FOR INDUSTRIAL END USERS

NORDSTERN (TRUE NORTH)
INDUSTRIAL SECURITY

#0 CHECK RESOURCES

#1 DEFINE
INDUSTRIAL SECURITY LEVEL, LCC, STRATEGY

#2 DESIGN
SECURE ARCHITECTURE, SERVICES

#3 ENABLE
SECURE IIOT ONBOARDING

#4 PRACTICE
MANAGED IIOT (IT/OT) SERVICES
INDUSTRIAL SECURITY

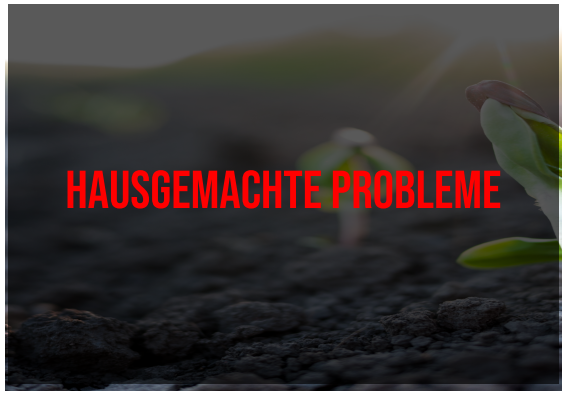
MANAGED SECURITY SERVICES

INDUSTRIAL

SCHNELLES WACHSTUM DURCH DIGITALISIERUNG

OT/IIOT

INDUSTRIAL SECURITY



.digital dirnberger