# IT-SA 2024

OT CYBER SECURITY: VON GEWONNEN ERKENNTNISSEN ZU STRATEGIEN DER ZUKUNFT







# WHY OT CYBER SECURITY TRANSFORMATION PROGRAMS FAIL?

Lack of End-to-End Approach

70 %

failure rate of transformations

Inadequate Organizational Structure

**Insufficient Resources** 

Neglected Change Management

Lack of Alignment with Business Goals

## WHAT HAS CHANGED OVER THE LAST 10 YEARS?



**IN THE PAST** 

Fully air-gapped OT networks

Newly Designed/ Engineered Cyber-Physical Systems

"Retrofitted" Systems Through

IT/OT Convergence



NOW

OT systems partially Connected to Each Other

- Isolated from IT Network
- Ran on proprietary control protocols
- Ran on specialized hardware
- Ran on embedded proprietary operating systems

- Bridged onto corporate networks
- ► Riding on common protocols
- Running on general hardware with IT origins
- Increasingly connected to wireless technologies



# STANDARDIZED PROCEDURE FOR AN OT TRANSFORMATION PROGRAM



Handover





Major cyber security incidents

Industry security incidents and support requests



# OT Security Pre-Assessment

- Evaluation of 10 sites
- Technical and Organizational review
- Major risk identification
- Action Prioritization



- Scope and financial planning based on pre assessment
- Global OT Security Framework
- OT Security Governance and Operating Model
- Risk management, remediation Planning and Technical Execution

#### **Pilot Solution**

- Market outlook and ideation
- Proof of Concept
- Test bed



# OUR OT SERVICE PORTFOLIO TO SECURE OUR CLIENTS

Besuchen Sie uns: Halle

**OT CYBER ASSESSMENTS** 

**PENETRATION TESTING** 

**OT SECURITY STRATEGY** 

**POLICIES, TOMS** 

#### **PMO FOR OT SECURITY**



**AWARENESS & TRAINING** 

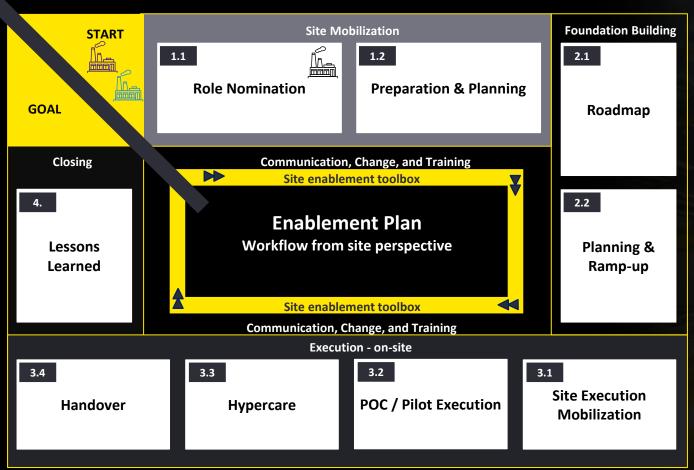
**IMPLEMENTATION** 

ASSET MANAGEMENT
INTRUSION DETECTION
SYSTEM
NETWORK SEGMENTATION
ETC.

**MANAGED SERVICES** 

Besuchen Sie uns: Halle 6, Stand 6-106

# SEE BEYOND THE SURFACE



The approach ensures efficient site execution with clear phases, stakeholder alignment, and tailored implementation.

Example: Asset Management In Phase 1, employees are nominated to support the asset discovery locally and are prepared. In Phase 2, the global roadmap for the site is created, considering specific requirements. In Phase 3, execution is carried out by EY and the site, including hypercare and handover. In Phase 4, a lessons learned workshop is conducted to identify optimizations for the next site.

### THE AHA-MOMENT

**60%** of orgs are here

**30%** of orgs are here

**Decision Point** 

10% of orgs are here

Awareness

Asset Discovery & Mapping

**Oh Wow Moment** 

**Firefighting** 

Integration

**Optimization** 

Driven by:

- Breach
- C-Suite
- Government Bulletins
- Government Intervention

- Internet outreach to understand current OT security governance
- Proof of concept with OT security platform vendors
- Unmanaged devices connecting everywhere!
- OT network isn't segmented
- Open ports everywhere
- OEM remoting in without a policy!
- Windows XP everywhere

- Steering Committee/Org. realignment
- Focus on high value assets
- Deployment of best POC solution
- Network segmentation
- Patching or compensating controls

- Creation of Chief Security Officer to converge siloed security disciplines
- OT security platform data feed to SIEM/ SOAR/central SOC
- Best of breed policy updates

Shift to ORM

implications

- (Operational Resilience Management)
- Realization that a
   lot of the OT data
   gathered for security
   purposes also have
   operational,
   engineering,
   maintenance,
   compliance,
   procurement or C-suite