OT CYBERSECURITY
ADVANCED TRAINING IN A CRITICAL INFRASTRUCTURE

SUMMARY – MAIN TOPICS

1. Introduction to industrial networks within operational terminal OT
2. Main principles in Cybersecurity
3. Case studies – cyber attacks in IT/OT networks

INTRODUCTION TO INDUSTRIAL NETWORKS WITHIN OPERATIONAL TERMINAL OT – SUMMARY

- Industrial Control System (ICS)
- SCADA
- Distributed Control System
- PLC
- Introduction in Remote Monitor and control Systems in IT/OT and SCADA Networks
- ICS Components
- Business Process Control System vs Safety Instrumentation System
- Control System Strengths & Weaknesses
- Process Control Networks: Components and their role
- Communication Protocols used in PCN
- IT vs OT/ICS
- HMI - Human Machine Interface
- OPC and OPC UA
- Data Historians
- Threats to SCADA
- Secure Network Design and Hardening: Equipment and their Role
- VLANs and Subnetting
- VPN and Remote Access Firewall Architectures

MAIN PRINCIPLES IN CYBERSECURITY – SUMMARY

- Main principles in IT/OT Cybersecurity
- SCADA Security Standards Bodies
- IEC 62443
- Purdue Model
- Asset Management
- Network Segmentation
- Data Backup
- Remote Access Security
- IPS/IDS - Network Monitoring and Intrusion Detection/Prevention
- Incident Response Management Program

CASE STUDIES – CYBER ATTACKS IN IT/OT NETWORKS - SUMMARY

- Introduction to Ethical Hacking
- Information Gathering - Footprinting, Reconnaissance
- Scanning, Enumeration
- System Hacking
- Malware Threats
- Sniffing and Session Hijacking
- Social Engineering
- Hacking Web Applications and Web Servers
- Cryptography
- Hacking Wireless Networks

DURATION

- 5 days
- 9 AM -5 PM
- Both practical and theoretical
- More details on demand