Cyber Awareness Training

TRIPLE-S

This training provides a basic introduction to Cyber-security within OT and is based on well proven standards such as IEC 62443 – Cyber Security for Industrial Control Systems and NIST Cyber Security Framework. The training is adapted to people working in OT needing more knowledge about cyber security, and to IT/ Management needing more knowledge about the OT. Instructors have long and real-life experience from OT and are GICSP certified.

Content:

Introduction to Cyber Security in the OT domain

- What is OT, and what are the differences between OT and IT?
- Example of cyber-attacks in OT
- Hacker scenarios (OSINT, Social Engineering and Methods)

Cyber Security Frameworks

- NIST
- MITRE ATT&CK

Standard for Cyber-security in Industrial Control Systems - IEC 62443

- Risk Assessment (IEC 62443-3-2)
- Security and Maturity Levels
- Cyber Security Requirements and Protection (IEC 62443-3-3)

Regulatory Requirements for Cyber-security

Cyber Security Management System

Architecture and Reference Models

- The Purdue Model
- Reference Models for a secure OT Environment

How to protect your ICS/OT?

- Least Privilege and Zero Trust
- Segmentation
- Secure Remote Access
- Monitoring of OT

Incident Response in OT

Recover from a Cyber Incident in OT

Group Assignments and Case Studies

Summary and Quiz

Duration
2 days training

Participants
Up to 15 participants pr. training recommended

Prerequisites
Basic knowledge of the OT environment, but no requirement

Method
Presentation and discussions
Group assignments
Quiz

Training material
Professionally printed compendium
Training certificate

Time and date:
On demand

Price:
Contact us at kurs@triple-s.no

Triple-S AS
Kristoffer Robinsvei 13
0978 Oslo
Tlf: 22 79 05 20
kurs@triple-s.no