

Cybersecurity risicomangement Training voor leidinggevenden (OT-SEC)

Short Description

How to comply to new cyber security regulations for operational technology.

Objectives

Compliant to NIS2 Chapter 20.2 for companies with physical assets.

- Identify risk
- Assess risk management practices
- Assess their impact on the services provided

Target Group

- Tactical & Operational Management
- IT management
- Plant Management
- OT managers
- Group Leads
- Automation Lead
- Security managers
- CISO & ISO / OSO
- other security seniors who need an update for Operational Technology.

Content

Governance

Learn about risk identification & mitigation, with respect to understanding both IT & OT. Gain insight into relevant market standards & guidelines.

IT-OT

Learn how technology fulfils business requirements, how they overlap and differ.

What is OT

Learn how to convert jargon to practical insights to create awareness. Learn to understand the consequence of controlling physical equipment and the corresponding responsibility from management.

Procedural/Organization

Learn how to get started business wise. What does a management framework look like. How to start small but enable to grow based on PDCA circle for security.

- Learn about controlling physical equipment via a network
- Why IT and OT look familiar, but require a different approach
- Understanding priorities of security in OT
- Interpretations of Risk in OT, based on threat and impact
- Gain vendor neutral insight of new regulations for cyber security in OT and how to comply
- How to initiate and get started rolling out a security program for OT
- Compare ISO27000 with OT relevant directives

Note

The documentation of this training will be in English. The training itself will be in Dutch.

The planned courses can only take place if there are sufficient registrations.

Type

Face-to-face training

Duration

1 day

Language

nl