

Anomaly Detection and Network Monitoring in OT-Systems with SINEC Security Monitor (IC-ADNMSM)

Short Description

Today, industrial operations without Ethernet connections are no longer imaginable. On the one hand, the use of ethernet technologies in industry-related environments has increased the capabilities to retrieve data from field level devices and its connection to upper levels including IT-environments. On the other hand, this increases the risk of cyber-attacks. Therefore, industrial networks require a high degree of reliability and protection of the data to minimize possible downtimes in production processes. Securing OT-systems includes the application of several control layers including correct network segmentation, traffic monitoring and asset inventory. The implementation of OT-traffic monitoring and asset inventory should evaluate the correct deployment, the less invasive methodology to avoid possible impacts in the automation systems and the most effective way to detect anomalies. This is exactly the sort of knowledge you will gain from the "Anomaly Detection and Network Monitoring in OT-Systems" training.

Objectives

In this course you will learn about OT-intrusion detection system and how can it be connected to real-time-capable systems in theory and in practice. You will gain an insight into industrial cybersecurity concepts and how to monitor OT-data flows to detect possible anomalies and evaluate the security situation in industrial networks. At the end of the course, you will be familiar with the requirements to such solutions and will be able to plan, implement, and manage this cybersecurity controls adding value to daily operations. You can deepen your theoretical knowledge with numerous practical exercises with the SINEC Security Monitor.

Target Group

Plant Engineers
Control Engineers
System Engineers
Commission Engineers
Application Engineers
Service and Maintenance Personnel
Project Engineers
OT and IT Network Engineers
Technical Sales Personnel
COOs
CIOs
Network Planners and Administrators

Content

OT-Cybersecurity Concept
Typical secure network architectures
Recommendations and highlight in the implementation of SINEC Security Monitor
Integration of end devices using protocols like syslog, WinRM and Remote WIM
Asset identification and administration in OT-system
Cybersecurity event detection and management

Prerequisites

Participants shall have basic knowledge of topics like Industrial Ethernet and Cybersecurity. You should be familiar with topologies, transfer processes, addressing, data transport, and understand the associated technical vocabulary. It is also helpful if you are familiar with the principles of operation of routers, switches, the OSI reference model and Cybersecurity standards like IEC-62443. Participants are encouraged to attend the training course „Security in Industrial Networks mit SCALANCE“ and the course „Ethernet Fundamentals in industrial Networks“.

Note

Certification (Siemens CPIN-LEVEL)

After the training course, you have the opportunity to become certified as "Siemens Certified Professional for Industrial Networks – Detection and Monitoring". The certification examination takes place at the end of this training. As an option, the examination may be taken at a later time.

Type

Face-to-face training

Duration

3 days

Language

da, en

Fee

11,250 DKK