SIEMENS

Security in Industrial Networks - Virtual (IEN-SEOILCINS1A)

Type

Virtual Instructor-led Learning

Duration and Continuing Education Units (CEU)

6 Hours (Schedule varies)
0 CEUs

Target Group

- Engineer
- Commissioning

Short Description

This virtual course is for users who are involved with developing or sustaining automation networks in an industrial environment. This includes, but is not limited to the following: • Plant Engineers • Control Engineers • System Engineers • Commission Engineers • Application Engineers • Operations or IT Network Engineers • Facility Managers • Project Engineers

This virtual course is one of three certification courses offered under the Siemens Certified Professional for Industrial Networks (CPIN) program. The curriculum includes an introduction of the potential threats and risks associated with industrial networks, as well as a deep dive into defense in depth strategies. Students will be shown numerous ways to implement access control measures to protect and mitigate security incidents.

Objectives

- Current trends and security risks
- Defense in depth strategies
- Update and replacement of security components
- Potential threats in a network
- Basic security measures (ports, passwords, protocols, etc.)
- Network segmentation (VLAN, routing)
- Cell protection concept
- Access restriction
- Remote access via VPN
- Diagnostics / troubleshooting
- Comprehensive exercises using the SIMATIC NET product portfolio

Content

- Comprehensively protecting productivity
- Maintenance
- Risks
- Basics of security
- Cell protection
- Access protection
- Standard machines

- Remote maintenance

Language

English