SIEMENS

Learning Journey - Introduction to Cybersecurity for industrial automation (IC-CYBERSEC-LJ)

Short Description

Dangers. Risks. Security. Learn a proven phased model to help you protect your industrial plant against cyber threats. Using this model, you will learn the basics of cybersecurity, solutions and concepts for protecting your industrial automation solution.

An optimal mix of guided live modules (online) and self-learning modules will provide you with all of the content imperative for your work and sustainable learning success. Various practical tasks in our virtual exercise environment throughout the Learning Journey help you to prepare for practical application. The Learning Journey provides curated on-demand content to support you in your own personal practice transfer.

More information on Learning Journeys

Objectives

After this Learning Journey, you can use strategies and concepts for the security of your system. You'll be able to test your assets for security vulnerabilities. To protect your asset, you can apply network segmentation, access controls, system hardening, remote access, security patches, and data backup and recovery measures. With the help of intrusion detection systems, you are able to detect attacks at an early stage. You know how a contingency plan to restore operations works.

Target Group

- Solution Architect
- Consultant
- Automation Engineer

Content

This learning journey consists of:
- 4 live modules (2.5–5 hours each)
- 10 self-learning modules (approx. 10 hours)
- Curated on-demand content
- Individual transfer support in the form of a 1:1 coaching (1 hour)

A Learning Membership | SITRAIN access to work through the self-learning modules and access to on-demand content is included for 1 year.

Topics
- Basics of Cybersecurity for Industry
- Specifications and standards in the field of cybersecurity
- Attack and defense options
- Protection Goals
- Vulnerability Management for assets
- Network Concept for industrial plants
- Secure remote access
- Asset access controls
- Hardening measures, security patching and data backup and recovery measures
- Intrusion detection systems
- Contingency plan to restore operations

Prerequisites

Technical requirements

Note

Participation in the Learning Journey is personal and non-transferable.

Type

Learning Journey

Duration

24 hours

Language

en