COURSE TABLE OF CONTENTS

Introduction to Cybersecurity for industrial automation

OEM: Siemens • Code: IC-CYBERSEC

COURSE DESCRIPTION

Dangers. Risks. Security. Participants will learn about a proven phased model designed to help protect industrial plants against cyber threats. Based on this model, the course covers the fundamentals of cybersecurity and introduces solutions and concepts for securing industrial automation systems. Through practical exercises in TIA Portal, participants deepen their understanding and apply the security concepts directly in practice.

AUDIENCE PROFILE

- Solution Architect
- Consultant
- Automation Engineer

PREREQUISITES

- Basic knowledge about industrial automation
- Basic knowledge about industrial communication
- Basic knowledge in SIMATIC TIA Portal Step 7
- Included in the course price: Free access to the digital learning platform SITRAIN access – starting one week before the start of the course until two weeks after the end of the course. With the Learning Membership, you can deepen or repeat the content of this Learning Event as well as continue your education on other interesting topics.

COURSE OBJECTIVES

By the end of this course, participants will be able to:

- After this course, participants will be able to implement strategies and concepts for the security of their industrial plant. They can systematically analyze and assess their assets for security vulnerabilities. To protect the plant, participants can apply measures such as network segmentation, access controls, system hardening, secure remote access, security patches, and data backup and recovery procedures. With the help of intrusion detection systems, participants will be able to detect attacks early and respond appropriately. In addition, they will understand how an emergency and recovery plan is structured and how operations are restored in the event of an emergency.

COURSE OUTLINE

Module 1: Content

- 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