SIEMENS

Applied Cybersecurity for Industrial Automation (US-IC-CYBERSEC2)

Type

Instructor-led Learning

Duration and Continuing Education Units (CEU)

Face-to-face: 4.5 Days ; Virtual: 4.5 Days (Schedule varies)
3 CEUs

Target Group

- Cybersecurity Professionals
- Engineers
- IT/OT Technicians

Short Description

This course provides engineers and technicians with a practical, risk-based framework for securing industrial environments. Moving beyond theoretical concepts, this course focuses on the "Attacker's View" to help participants prioritize defenses where they matter most.

Participants will gain hands-on experience with Siemens SCALANCE and SIMATIC technologies, learning to implement robust network segmentation, VLANs, and industrial firewalls. The primary focus of the course is the Hardening of Industrial Components, ensuring that PLCs and Field IO are not only configured for performance, but are fortified against modern cyber threats.

Objectives

- Analyze Risk & Mitigation: Apply a comprehensive framework to understand how OT/IT interconnection impacts plant-level security.
- Adopt the Attacker's View: Identify prime targets within an automation system (PLCs and Engineering Workstations) and understand initial intrusion vectors like social engineering and phishing.
- Implement Defense-in-Depth: Design and deploy segmented architectures using zones, conduits, and best practices for manufacturing environments.
- Master Technical Configuration: Configure port-based VLANs and firewall functions on Siemens SCALANCE XC-200 switches and security modules.
- Execute Field Hardening: Perform critical hardening procedures on Siemens SIMATIC PLCs to ensure a secure and resilient field environment.
- Navigate Standards & Compliance: Align technical security measures with global industrial cybersecurity standards and norms.

Content

- Introduction to Industrial Risk & The Attacker's View

SIEMENS

- Network Fundamentals, Segmentation Strategy, and VLANs
- Ethical Hacking Theory, Vulnerability Analysis, and Defense Standards
- Hands-on Hardening of PLCs and Firewall Implementation
- Siemens Ecosystem Overview, Final Labs, and Course Wrap-Single level list of top-level topics

Note

Student should have basic knowledge of Ethernet communication and industrial networking. Also, the student should be familiar with Siemens SIMATIC automation components. These suggestions are recommended but not required.

Language

English

Course descriptions are Siemens Intellectual Property and copyright protected. Do not modify without written permission from SITRAIN US. ©2023 Siemens Industry, Inc.