SIEMENS

工业自动化网络安全导论（IC-CYBERSEC）

简要介绍

危险。风险。安全。参与者将学习一种经过验证的分阶段模型，旨在帮助保护工业厂房免受网络威胁。基于该模型，课程涵盖网络安全基础，并介绍保障工业自动化系统的解决方案和概念。通过TIA门户和SINEC安全守卫的实践练习，学员加深理解，并直接将安全概念应用于实践。

培训目的

课程结束后，学员将能够实施工业厂安全的策略和概念。他们可以系统地分析和评估自身资产的安全漏洞。为保护工厂，学员可以采取网络分段、访问控制、系统加固、安全远程访问、安全补丁以及数据备份和恢复程序等措施。借助入侵检测系统的帮助，学员能够及早发现攻击并做出适当响应。此外，他们还将理解应急和恢复计划的结构，以及在紧急情况下如何恢复运营。

培训对象

解决方案架构师
- 顾问
- 自动化工程师

课程内容

行业网络安全基础
- 网络安全领域的规范与标准
- 攻击和防御选项
- 保护目标
- 资产漏洞管理
- 工业工厂网络概念
- 安全远程访问
- 资产访问控制
- 加固措施、安全补丁以及数据备份和恢复措施
- 入侵检测系统
- 恢复运营的应急计划

课程费用包含：免费使用数字学习平台 SITRAIN访问——从课程开始前一周开始至结束后两周。在这里，您可以找到关于 保护工业网络以及其他主题的网络培训，如 工业安全， 工业自动化系统、SIMATIC等。通过学习会员，你可以深入或重复学习本次学习活动的内容，并继续学习其他有趣的主题。

必备条件

工业自动化基础知识
- 工业通信基础知识
- SIMATIC TIA 门户第7步基础知识

注意事项

学习会员资格从课程开始前7天开始，结束后14天结束。在此期间，您可以参加所有可用的网络培训。

课程类型

标准课程

培训天数

3 天

培训语言

en

培训费用

0 EUR

copyright by Siemens AG 2026