

Industrial Cyber Security

Professional training programme



SPARK TRAINING

Professional training courses for leaders, specialists, and organizations seeking practical capability development.

info@sparktraining.eu

+31 85 115 0004 | sparktraining.eu

— Workshop Overview

Cyber attacks pose a global threat impacting individuals, businesses, and nations alike. Safeguarding your organization from these threats requires not only the ability to protect your technology but also to effectively identify, analyze, respond to, and investigate cyber incidents. The consequences of an information security breach, such as the notorious attack on the Ukraine power station, can be catastrophic, undermining operational technology controls and exposing critical vulnerabilities. As cyber attacks increase in frequency and sophistication, understanding the nature, motives, and methods of cyber threat actors becomes crucial. Implementing best practices, utilizing appropriate countermeasures, and applying effective management techniques are essential for mitigating these risks and protecting your assets. With cyber security emerging as a core responsibility, leaders—including boards of directors, corporate officers, chief engineers, and frontline employees—must recognize the personal and organizational implications of cyber breaches and integrate robust security measures into their strategies. This Industrial Cyber Security training course will help you understand Information Security, and how this is deployed in an Operational Technology Environment. This training course will feature:

- An understanding of Cyber Security issues
- Approaches to Cyber Security within an Operational Technology environment.
- An introduction to Cyber Security Frameworks
- Current Best Practices for Cyber Security Response
- Approaching Cyber Security Response Plans

Why Attend

This course uses instructor-led sessions, guided discussion, and practical exercises built around Day One: What is Cyber Security?, Day Two: Assessing Your Cyber Security Posture, Day Three: Cyber Security and Industrial Control Systems Management, and day four: cyber security controls.

Who Should Attend

Legal Professionals
System Engineers
Security Administration
Operational Staff
Those whom have involvement with and responsibility for operational technology, information technology, & risk assessment

— Learning Objectives

- Understand Information Security, and how this is deployed in an Operational Technology Environment
- Understand a range of Cyber threats and assess a security posture within an Operational Technology environment

- Appreciate the leading legislation, International Standards and Governance models for Cyber Security and current best practice
- Understand the approaches for Crisis and Incident Management for Cyber Security Breaches

Course Outline

DAY
1

Day One: What is Cyber Security?

- Overview of Cyber Security for Industries
- Cyber Crime and Attacks
- Technology, Policing, and Investigation of Electronic Crime
- Ethical Hacking and Cyber Crime
- Civil and Criminal Considerations

DAY
2

Day Two: Assessing Your Cyber Security Posture

- Cyber Security and Risk Assessment
- Information Security and Standards
- ISO7799 - Information Security Management - Code of Practice
- ISA99 - International Standards for Automation Cyber Security Standard
- Reducing Your Security Risk and Increasing Your Security Capabilities

DAY
3

Day Three: Cyber Security and Industrial Control Systems Management

- Information Security and Operational Technology
- Emerging Industrial Technology Trends
- Metcaf's Law
- Moore's Law
- Mirrors World

DAY
4

Day Four: Cyber Security Controls

- Selecting Security Controls and Best Practice
- Considerations for Enhancing Security
- Detection, Prevention and Offensive Responses
- Securing and Assessing OPERATIONAL TECHNOLOGY Environments (OTE)
- OTE User Management, System Integrity, Data Confidentiality & Restricted Data Flow

DAY
5

Day Five: Building a Cyber Response Plan

- Defining a Cyber Response Strategy
- Composing Cyber Response Plan
- Cyber Response Team Compilation and Service Vendor Support
- Cyber Preparedness and Corporate Governance

- Operational Security Centers

— Upcoming Classroom Dates

DATE	LOCATION	FEE
5 - 9 October 2026	London - United Kingdom	€2,100
12 - 16 October 2026	Vienna - Austria	€2,125
9 - 13 November 2026	Barcelona - Spain	€1,925
16 - 20 November 2026	Istanbul - Türkiye	€1,425
7 - 11 December 2026	Vienna - Austria	€2,125
14 - 18 December 2026	Rome - Italy	€2,125
18 - 22 January 2027	Amsterdam - Netherlands	€2,125
15 - 19 February 2027	Istanbul - Türkiye	€1,425

— Certificate and Registration

Participants who attend and complete the full programme receive a SPARK Training Certificate of Completion. For registration, in-house delivery, or availability questions, contact info@sparktraining.eu or +31 85 115 0004.