Industrial Cybersecurity in Manufacturing Training Course

Professional Development Training Course Outline

Category	Manufacturing	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Industrial Cybersecurity in Manufacturing is now a mission-critical discipline as global factories rapidly adopt Industry 4.0, IIoT (Industrial Internet of Things), and smart automation systems. With increasing convergence of IT (Information Technology) and OT (Operational Technology), manufacturing environments are becoming prime targets for cyberattacks, ransomware, supply chain breaches, and industrial espionage. Industrial Cybersecurity in Manufacturing Training Course provides a comprehensive foundation to understand, assess, and defend industrial environments against evolving cyber threats.

This program equips professionals with practical skills in OT security architecture, SCADA protection, PLC hardening, threat intelligence, and risk mitigation frameworks. Participants will gain hands-on exposure to real-world industrial attack scenarios and learn how to implement global standards such as IEC 62443, NIST Cybersecurity Framework, and Zero Trust Architecture for industrial systems, ensuring resilient and secure manufacturing operations.

Programme Curriculum

Industrial Cybersecurity in Manufacturing Training Course

Introduction

Industrial Cybersecurity in Manufacturing is now a mission-critical discipline as global factories rapidly adopt Industry 4.0, IIoT (Industrial Internet of Things), and smart automation systems. With increasing convergence of IT (Information Technology) and OT (Operational Technology), manufacturing environments are becoming prime targets for cyberattacks, ransomware, supply chain breaches, and industrial espionage. Industrial Cybersecurity in Manufacturing Training Course provides a comprehensive foundation to understand, assess, and defend industrial environments against evolving cyber threats.

This program equips professionals with practical skills in OT security architecture, SCADA protection, PLC hardening, threat intelligence, and risk mitigation frameworks. Participants will gain hands-on exposure to real-world industrial attack scenarios and learn how to implement global standards such as IEC 62443, NIST Cybersecurity Framework, and Zero Trust Architecture for industrial systems, ensuring resilient and secure manufacturing operations.

Course Duration

5 days

Course Objectives

1. Understand Industrial Cybersecurity & OT Security Fundamentals
2. Analyze IT/OT Convergence risks in Smart Manufacturing
3. Implement SCADA Security Best Practices
4. Secure PLC (Programmable Logic Controller) systems
5. Apply IEC 62443 Industrial Security Standard
6. Design Zero Trust Architecture for Industrial Networks
7. Identify Ransomware threats in Manufacturing Plants
8. Conduct Industrial Risk Assessment & Vulnerability Analysis
9. Deploy Network Segmentation in OT environments
10. Use Threat Intelligence for Industrial Systems
11. Strengthen IIoT Device Security & Firmware Protection
12. Develop Incident Response Plans for OT Cyber Attacks
13. Ensure Compliance with Global Cybersecurity Regulations

Target Audience

1. OT Engineers & Control System Engineers
2. Cybersecurity Analysts & SOC Teams
3. Manufacturing Plant Managers
4. Industrial Automation Engineers
5. IT Infrastructure Professionals in Manufacturing
6. Risk & Compliance Officers
7. SCADA System Administrators
8. Government & Defense Industrial Security Teams

Course Modules

Module 1: Introduction to Industrial Cybersecurity & Smart Manufacturing

- Overview of Industry 4.0 & digital transformation
- IT vs OT security differences
- Cyber risk landscape in manufacturing
- Common attack vectors in industrial systems
- Case Study: 2021 global manufacturing ransomware disruption analysis

Module 2: OT Network Architecture & Security Design

- Industrial network topology fundamentals
- Purdue Model implementation
- Secure communication protocols (Modbus, DNP3)

- Network segmentation strategies
- Case Study: Segmentation failure in automotive plant cyber incident

Module 3: SCADA & ICS Security

- SCADA system architecture
- Common SCADA vulnerabilities
- Secure configuration and patch management
- Monitoring SCADA traffic anomalies
- Case Study: Ukrainian power grid cyberattack simulation

Module 4: PLC & Industrial Device Security

- PLC programming risks and exposure
- Firmware integrity protection
- Device authentication mechanisms
- Secure remote access to PLCs
- Case Study: PLC manipulation in water treatment facility

Module 5: IIoT & Smart Sensors Security

- IoT device lifecycle risks
- Edge computing security challenges
- Secure firmware updates (OTA)
- Authentication for connected devices
- Case Study: Smart factory IoT botnet infiltration

Module 6: Threat Detection & Incident Response in OT

- OT threat intelligence frameworks
- Real-time anomaly detection systems
- Incident response planning for factories
- Forensics in industrial environments
- Case Study: Ransomware containment in manufacturing plant

Module 7: Industrial Risk Management & Compliance

- Risk assessment methodologies
- IEC 62443 compliance framework
- NIST CSF in industrial environments
- Audit and governance strategies
- Case Study: Compliance failure leading to production shutdown

Module 8: Advanced Defense Strategies & Zero Trust OT Security

- Zero Trust model for industrial systems
- AI-driven cybersecurity monitoring
- Security automation in manufacturing
- Advanced persistent threat (APT) defense
- Case Study: Prevented cyber-espionage in smart factory deployment

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com