Cybersecurity in Industrial Automation Training Course

Professional Development Training Course Outline

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

Course Introduction

Industrial environments are rapidly transforming with the integration of Industrial Automation, IoT, SCADA systems, and smart manufacturing technologies under Industry 4.0. While this digital convergence improves efficiency, it also expands the attack surface for cyber threats targeting Operational Technology (OT), Industrial Control Systems (ICS), and critical infrastructure. Modern cyberattacks are no longer limited to IT networks they now directly impact power plants, oil & gas pipelines, manufacturing lines, water treatment systems, and smart factories, making industrial cybersecurity a mission-critical discipline.

Cybersecurity in Industrial Automation Training Course equips learners with advanced knowledge and hands-on skills to secure SCADA, PLCs, DCS systems, IIoT devices, and industrial networks. Participants will gain expertise in threat detection, risk assessment, network segmentation, zero-trust architecture, ransomware defense, and IEC 62443 standards implementation. The course bridges the gap between IT and OT security, enabling professionals to protect critical infrastructure from evolving APT attacks, malware infiltration, and industrial espionage

Programme Curriculum

Cybersecurity in Industrial Automation Training Course

Introduction

Industrial environments are rapidly transforming with the integration of Industrial Automation, IoT, SCADA systems, and smart manufacturing technologies under Industry 4.0. While this digital convergence improves efficiency, it also expands the attack surface for cyber threats targeting Operational Technology (OT), Industrial Control Systems (ICS), and critical infrastructure. Modern cyberattacks are no longer limited to IT networks they now directly impact power plants, oil & gas pipelines, manufacturing lines, water treatment systems, and smart factories, making industrial cybersecurity a mission-critical discipline.

Cybersecurity in Industrial Automation Training Course equips learners with advanced knowledge and hands-on skills to secure SCADA, PLCs, DCS systems, IIoT devices, and industrial networks. Participants will gain expertise in threat detection, risk assessment, network segmentation, zero-trust architecture, ransomware defense, and IEC 62443 standards implementation. The course bridges the gap between IT and OT security, enabling professionals to protect critical infrastructure from evolving APT attacks, malware infiltration, and industrial espionage.

Course Duration

5 days

Course Objectives

1. Understand Industrial Control Systems (ICS) cybersecurity architecture
2. Analyze SCADA security vulnerabilities and mitigation strategies
3. Implement OT network segmentation and secure zoning
4. Apply IEC 62443 industrial cybersecurity standards
5. Detect and respond to Advanced Persistent Threats (APT) in OT environments
6. Strengthen PLC (Programmable Logic Controller) security controls
7. Secure Industrial Internet of Things (IIoT) ecosystems
8. Conduct risk assessment and threat modeling for industrial systems
9. Deploy Zero Trust Architecture in industrial automation
10. Prevent ransomware attacks on critical infrastructure
11. Monitor systems using Security Information and Event Management (SIEM) tools
12. Perform incident response in OT/ICS environments
13. Develop cyber resilience strategies for smart manufacturing

Target Audience

1. OT/ICS Engineers
2. Cybersecurity Analysts & SOC Engineers
3. Industrial Automation Engineers
4. SCADA/PLC Technicians
5. Network Security Administrators
6. Critical Infrastructure Operators
7. IT Professionals transitioning into OT Security
8. Government & Defense Cybersecurity Personnel

Course Modules

Module 1: Introduction to OT & ICS Cybersecurity

- Fundamentals of OT vs IT security environments
- Industrial Control System architecture overview
- Cyber-physical system vulnerabilities
- Threat landscape in smart industries
- Security convergence in Industry 4.0
- **Case Study:** Stuxnet attack on nuclear centrifuges

Module 2: SCADA System Security

- SCADA communication protocols

- Common SCADA vulnerabilities
- Access control and authentication mechanisms
- SCADA intrusion detection techniques
- Secure remote operations
- **Case Study:** Ukrainian Power Grid Cyberattack (2015)

Module 3: PLC & DCS Security

- PLC architecture and attack vectors
- DCS system security challenges
- Firmware integrity and secure coding
- Ladder logic manipulation risks
- Device-level authentication controls
- **Case Study:** German Steel Mill Cyber Incident

Module 4: Industrial Network Security

- OT network segmentation strategies
- Firewalls and industrial DMZ design
- Protocol filtering and deep packet inspection
- Secure remote access
- Network anomaly detection
- **Case Study:** TRITON malware targeting safety systems

Module 5: IIoT & Smart Factory Security

- IIoT device lifecycle security
- Edge computing risks
- Cloud integration vulnerabilities
- Device identity management
- Secure firmware updates
- **Case Study:** Mirai botnet impact on IoT networks

Module 6: Threat Intelligence & Incident Response

- Cyber threat intelligence in OT environments
- Log analysis and SIEM integration
- Incident response lifecycle
- Digital forensics in industrial systems
- Real-time threat monitoring
- **Case Study:** Colonial Pipeline ransomware attack

Module 7: Industrial Cybersecurity Standards & Compliance

- IEC 62443 framework deep dive
- NIST cybersecurity framework for ICS
- ISO/IEC standards for OT security
- Compliance auditing techniques
- Risk governance models
- **Case Study:** European energy sector compliance breach analysis

Module 8: Advanced Threats & Cyber Defense Strategies

- Advanced Persistent Threats (APT) in OT
- Zero Trust architecture implementation
- AI-driven cyber defense systems
- Ransomware defense strategies
- Cyber resilience planning
- **Case Study:** Triton malware attack on petrochemical plant

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
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