Industrial Internet of Things (IIoT) Security Training Course

Professional Development Training Course Outline

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

Course Introduction

The Industrial Internet of Things (IIoT) has revolutionized manufacturing, energy, logistics, and other industrial sectors by connecting devices, sensors, and systems to improve operational efficiency, predictive maintenance, and real-time monitoring. While IIoT offers unprecedented opportunities for data-driven decision-making and process optimization, it also introduces critical security risks, including cyber threats, unauthorized access, data breaches, and operational disruptions. Industrial Internet of Things (IIoT) Security Training Course provides a comprehensive overview of IIoT security challenges, best practices, and mitigation strategies to safeguard industrial networks, endpoints, and cloud integrations. Participants will gain practical knowledge in threat modeling, risk assessment, and security framework implementation that aligns with industry standards and compliance requirements.

Participants will explore strategies to secure IIoT infrastructure, protect sensitive data, and manage vulnerabilities across the entire industrial ecosystem. The training emphasizes real-world applications, incident response planning, and regulatory compliance, equipping learners with the tools to implement resilient security measures and maintain operational continuity. By integrating cybersecurity principles into IIoT architecture, organizations can reduce risk exposure, protect critical assets, and ensure the safe deployment of connected industrial technologies.

Programme Curriculum

Industrial Internet of Things (IIoT) Security Training Course

Introduction

The Industrial Internet of Things (IIoT) has revolutionized manufacturing, energy, logistics, and other industrial sectors by connecting devices, sensors, and systems to improve operational efficiency, predictive maintenance, and real-time monitoring. While IIoT offers unprecedented opportunities for data-driven decision-making and

process optimization, it also introduces critical security risks, including cyber threats, unauthorized access, data breaches, and operational disruptions. Industrial Internet of Things (IIoT) Security Training Course provides a comprehensive overview of IIoT security challenges, best practices, and mitigation strategies to safeguard industrial networks, endpoints, and cloud integrations. Participants will gain practical knowledge in threat modeling, risk assessment, and security framework implementation that aligns with industry standards and compliance requirements.

Participants will explore strategies to secure IIoT infrastructure, protect sensitive data, and manage vulnerabilities across the entire industrial ecosystem. The training emphasizes real-world applications, incident response planning, and regulatory compliance, equipping learners with the tools to implement resilient security measures and maintain operational continuity. By integrating cybersecurity principles into IIoT architecture, organizations can reduce risk exposure, protect critical assets, and ensure the safe deployment of connected industrial technologies.

Course Objectives

1. Understand the fundamentals of IIoT architecture and its security implications.
2. Identify common IIoT threats, vulnerabilities, and attack vectors.
3. Apply risk assessment methodologies to industrial IoT systems.
4. Implement access control, authentication, and encryption for IIoT devices.
5. Design secure network protocols and industrial communication channels.
6. Monitor and detect anomalies using IIoT security analytics.
7. Evaluate compliance requirements and regulatory standards for IIoT.
8. Apply incident response and disaster recovery strategies for industrial networks.
9. Integrate security into the IIoT device lifecycle management.
10. Protect cloud-based and edge computing platforms connected to IIoT.
11. Develop policies for secure data collection, storage, and transmission.
12. Implement industrial cybersecurity frameworks and best practices.
13. Assess emerging technologies and trends in IIoT security solutions.

Organizational Benefits

- Enhanced protection of industrial operations against cyber threats
- Improved compliance with IIoT security standards and regulations
- Reduced downtime and operational disruptions due to security breaches
- Increased reliability and trust in connected industrial systems
- Strengthened resilience across networks, devices, and cloud platforms
- Improved threat detection and response capabilities
- Streamlined risk management for IIoT deployments
- Better staff awareness and capability in cybersecurity practices
- Enhanced operational efficiency through secure IoT integration
- Protection of critical intellectual property and industrial data

Target Audiences

- IIoT security engineers and network administrators
- Industrial operations managers and plant engineers
- Cybersecurity and IT risk professionals
- Compliance and regulatory officers
- Industrial systems integrators and consultants

- Industrial automation specialists
- Manufacturing technology managers
- Industrial control system (ICS) technicians

Course Duration: 5 days

Course Modules

Module 1: Introduction to IIoT Security

- Overview of Industrial IoT architecture and protocols
- Key components and connected devices in industrial networks
- Security challenges unique to industrial systems
- Industrial control system vulnerabilities
- Threat landscape and risk exposure in IIoT
- Case Study: Analysis of a ransomware attack on a smart factory

Module 2: Threats, Vulnerabilities, and Risk Assessment

- Common IIoT attack vectors and threat actors
- Device and firmware vulnerabilities
- Risk assessment frameworks for industrial systems
- Identifying critical assets and impact analysis
- Developing mitigation and risk prioritization strategies
- Case Study: Risk assessment in a chemical processing plant

Module 3: Secure Network Architecture and Protocols

- Segmentation and secure network design for IIoT
- Industrial communication protocols and their vulnerabilities
- Network monitoring and intrusion detection systems
- Secure VPN and firewall implementation
- Threat modeling for industrial networks
- Case Study: Securing SCADA communication channels in energy systems

Module 4: Device Security and Access Management

- Authentication and identity management for IIoT devices
- Encryption standards for device communication
- Firmware and software update security
- Endpoint protection and device hardening
- Role-based access control and privilege management
- Case Study: Unauthorized device access incident in manufacturing

Module 5: Cloud, Edge, and Data Security

- Protecting cloud and edge computing platforms connected to IIoT
- Data encryption in transit and at rest
- Secure integration of analytics and machine learning systems
- Ensuring privacy of industrial data streams
- Monitoring cloud-based IIoT applications
- Case Study: Data breach in a cloud-based industrial analytics platform

Module 6: Monitoring, Detection, and Incident Response

- Real-time monitoring of industrial networks
- Anomaly detection and predictive analytics
- Security information and event management (SIEM) for IIoT
- Incident response planning and execution
- Post-incident analysis and lessons learned
- Case Study: Industrial control system attack and recovery procedures

Module 7: Compliance, Standards, and Regulatory Requirements

- Overview of ISO, NIST, and IEC IIoT security standards
- Compliance with industrial cybersecurity regulations
- Auditing and reporting for IIoT systems
- Aligning organizational policies with regulatory expectations
- Implementing continuous compliance monitoring
- Case Study: Regulatory compliance implementation in a smart grid deployment

Module 8: Emerging Trends and Future of IIoT Security

- AI and machine learning in IIoT security
- Blockchain and distributed ledger applications
- Threat intelligence sharing for industrial networks
- 5G connectivity and security implications
- Future challenges in IIoT security management
- Case Study: Predictive security analytics for a manufacturing enterprise

Training Methodology

- Instructor-led sessions with practical demonstrations
- Hands-on exercises using industrial simulation labs
- Group discussions and peer-learning on real-world scenarios
- Case study analysis and collaborative problem-solving
- Practical tools, templates, and checklists for IIoT security implementation
- Continuous assessment and feedback sessions

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
02 Nov 2026	06 Nov 2026	Online	$1,000
02 Nov 2026	06 Nov 2026	Physical	$1,500
02 Nov 2026	06 Nov 2026	Physical	$3,000
02 Nov 2026	06 Nov 2026	Physical	$3,000
02 Nov 2026	06 Nov 2026	Physical	$6,000
02 Nov 2026	06 Nov 2026	Physical	$4,500
02 Nov 2026	06 Nov 2026	Physical	$6,000
02 Nov 2026	06 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