IoT Security and Device Hardening Training Course

Professional Development Training Course Outline

Category	Defense and Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The Internet of Things (IoT) has revolutionized connectivity by linking billions of devices across industries, homes, and cities, providing unprecedented access to data, automation, and operational efficiency. However, the rapid adoption of IoT devices exposes organizations to significant security risks, including unauthorized access, data breaches, device hijacking, and cyber-physical threats. IoT Security and Device Hardening Training Course equips participants with the knowledge, tools, and best practices required to secure IoT ecosystems, protect device integrity, and implement robust device hardening strategies. Participants will gain a comprehensive understanding of IoT architectures, threat landscapes, security protocols, and regulatory frameworks necessary to safeguard interconnected systems and data.

The course emphasizes practical skills for designing, configuring, and maintaining secure IoT devices and networks. Participants will learn to apply encryption, authentication, firmware updates, intrusion detection, and risk mitigation strategies across IoT infrastructures. Through detailed case studies, hands-on exercises, and scenario-based simulations, learners will understand real-world vulnerabilities and develop proactive defense mechanisms. By integrating industry standards and emerging trends in IoT security, this training ensures that participants can implement scalable, resilient, and compliant device security frameworks to protect critical assets and maintain business continuity.

Programme Curriculum

IoT Security and Device Hardening Training Course

Introduction

The Internet of Things (IoT) has revolutionized connectivity by linking billions of devices across industries, homes, and cities, providing unprecedented access to data, automation, and operational efficiency. However, the rapid adoption of IoT devices exposes organizations to significant security risks, including unauthorized access, data breaches, device hijacking, and cyber-physical threats. IoT Security and Device Hardening

Training Course equips participants with the knowledge, tools, and best practices required to secure IoT ecosystems, protect device integrity, and implement robust device hardening strategies. Participants will gain a comprehensive understanding of IoT architectures, threat landscapes, security protocols, and regulatory frameworks necessary to safeguard interconnected systems and data.

The course emphasizes practical skills for designing, configuring, and maintaining secure IoT devices and networks. Participants will learn to apply encryption, authentication, firmware updates, intrusion detection, and risk mitigation strategies across IoT infrastructures. Through detailed case studies, hands-on exercises, and scenario-based simulations, learners will understand real-world vulnerabilities and develop proactive defense mechanisms. By integrating industry standards and emerging trends in IoT security, this training ensures that participants can implement scalable, resilient, and compliant device security frameworks to protect critical assets and maintain business continuity.

Course Objectives

1. Understand IoT architectures, protocols, and device communication standards.
2. Identify vulnerabilities and threat vectors in IoT ecosystems.
3. Apply device hardening techniques and secure configuration practices.
4. Implement strong authentication, access control, and encryption mechanisms.
5. Evaluate IoT network security, segmentation, and monitoring strategies.
6. Conduct risk assessments and threat modeling for IoT deployments.
7. Apply firmware and software update management for IoT devices.
8. Integrate intrusion detection and anomaly detection systems.
9. Ensure compliance with IoT security standards and regulations.
10. Implement endpoint security and endpoint monitoring frameworks.
11. Develop policies and procedures for IoT lifecycle management.
12. Plan for incident response, breach management, and disaster recovery.
13. Explore emerging technologies and trends in IoT security.

Organizational Benefits

- Reduced risk of cyberattacks targeting IoT infrastructure
- Enhanced protection of sensitive device and network data
- Improved compliance with security standards and regulations
- Strengthened operational resilience and continuity planning
- Increased stakeholder and customer confidence in IoT deployments
- Standardized device hardening and configuration protocols
- Improved incident response and threat mitigation capabilities
- Optimized monitoring and logging of IoT networks
- Enhanced governance and policy enforcement for IoT security
- Proactive adaptation to emerging IoT security trends

Target Audiences

- IoT security engineers and architects
- Network administrators and system integrators
- Cybersecurity analysts and threat hunters
- IT operations and infrastructure managers
- IoT solution developers and firmware engineers
- Risk management and compliance professionals

- Technical consultants and auditors
- Senior management overseeing IoT initiatives

Course Duration: 10 days

Course Modules

Module 1: Introduction to IoT Security

- Overview of IoT architectures, devices, and protocols
- Common security challenges in IoT deployments
- Risk exposure in consumer, enterprise, and industrial IoT
- Security frameworks and governance models
- Industry trends and regulatory requirements
- Case Study: Security breach in a smart home IoT system

Module 2: Threat Landscape and Vulnerability Assessment

- Identifying common attack vectors on IoT devices
- Vulnerability scanning and assessment techniques
- Threat intelligence sources and analysis
- Prioritization of vulnerabilities based on risk impact
- Mapping threats to device types and deployment scenarios
- Case Study: IoT botnet attack on smart meters

Module 3: Device Hardening Fundamentals

- Principles of secure device configuration
- Disabling unused ports, services, and protocols
- Secure boot and hardware root of trust implementation
- Applying security baseline standards for IoT devices
- Logging and monitoring device activity
- Case Study: Hardening industrial IoT sensors

Module 4: Authentication and Access Control

- Implementing strong password and credential management
- Multi-factor authentication for IoT devices
- Role-based access control and privilege separation
- OAuth, certificate-based authentication, and PKI for IoT
- Managing device identity and lifecycle securely
- Case Study: Compromised access in an enterprise IoT network

Module 5: Encryption and Secure Communication

- Encryption methods for data at rest and in transit
- Secure communication protocols (TLS, DTLS, MQTT-S, HTTPS)
- Key management and distribution in IoT ecosystems
- Protecting firmware updates and OTA communications
- Evaluating encryption performance on constrained devices
- Case Study: Eavesdropping vulnerability in connected medical devices

Module 6: Network Security for IoT

- Network segmentation and zoning for IoT devices
- Firewalls, VPNs, and secure tunneling techniques
- Monitoring network traffic for anomalies
- Secure integration with cloud and enterprise networks
- Managing edge-to-cloud security challenges
- Case Study: Compromised smart factory network due to poor segmentation

Module 7: Firmware and Software Security

- Secure development lifecycle for IoT applications
- Firmware update management and patching
- Code signing and integrity verification
- Vulnerability scanning and remediation in firmware
- Threat mitigation in embedded software
- Case Study: Exploit from unpatched IoT camera firmware

Module 8: Intrusion Detection and Anomaly Monitoring

- Implementing intrusion detection systems for IoT networks
- Anomaly detection using machine learning and analytics
- Alerting, logging, and forensic analysis of security events
- Correlation of security events across devices and gateways
- Continuous monitoring and alert prioritization
- Case Study: Detecting malicious activity in a smart grid

Module 9: IoT Risk Assessment and Threat Modeling

- Conducting comprehensive risk assessments
- Asset inventory and threat mapping for IoT ecosystems
- Quantifying risk likelihood and impact
- Developing mitigation strategies for high-risk assets
- Aligning risk assessment with business objectives
- Case Study: Risk model for connected industrial equipment

Module 10: Compliance and Regulatory Requirements

- Understanding GDPR, HIPAA, NIST, and industry-specific regulations
- Compliance frameworks for IoT security
- Documentation and audit readiness
- Reporting obligations for incidents and breaches
- Regulatory risk management and assessment
- Case Study: IoT compliance audit of a healthcare deployment

Module 11: Endpoint Security Management

- Securing individual IoT devices and endpoints
- Anti-tampering, anti-reverse engineering, and malware protection
- Device monitoring, logging, and alerting
- Threat intelligence integration at the device level
- Endpoint risk scoring and prioritization

- Case Study: Unauthorized firmware modification in IoT gateways

Module 12: Incident Response and Breach Management

- Creating IoT-specific incident response plans
- Breach detection, containment, and mitigation strategies
- Communication protocols for internal and external stakeholders
- Post-incident analysis and lessons learned
- Continuous improvement of response plans
- Case Study: Breach response for connected industrial robots

Module 13: Secure Cloud Integration for IoT

- Security challenges in IoT-cloud integration
- Secure APIs, endpoints, and data pipelines
- Authentication and encryption for cloud services
- Monitoring and audit for cloud-connected devices
- Shared responsibility models between cloud and IoT owner
- Case Study: Cloud misconfiguration leading to data exposure

Module 14: Emerging IoT Threats and Security Trends

- Zero-trust architecture for IoT networks
- AI-based attacks and automated threat campaigns
- Security in 5G-enabled IoT environments
- Blockchain and decentralized security approaches
- Threat forecasting and proactive defense strategies
- Case Study: Predictive threat mitigation in smart city infrastructure

Module 15: Scaling Security and Organizational Best Practices

- Developing enterprise-wide IoT security policies
- Staff training, awareness, and governance structures
- Security metrics and reporting dashboards
- Security by design for future IoT deployments
- Continuous evaluation and improvement strategies
- Case Study: Enterprise rollout of an IoT security program

Training Methodology

- Instructor-led sessions with interactive lectures
- Hands-on labs for device configuration and hardening
- Group exercises for threat modeling and risk assessment
- Case study analyses and scenario-based problem solving
- Practical tools, templates, and checklists for participants
- Action plan development and presentations for organizational adoption

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	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now