IoT Security Essentials (ISE) and Device Hardening Training Course

Professional Development Training Course Outline

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

Course Introduction

The Internet of Things (IoT) revolution has introduced unprecedented connectivity, but this massive expansion of devices from smart homes to industrial sensors has simultaneously created a significantly larger and more complex attack surface. This critical training, IoT Security Essentials (ISE) & Device Hardening, provides participants with the foundational and advanced knowledge required to proactively secure the entire IoT ecosystem. Learners will master key concepts like embedded device security, secure boot mechanisms, IoT threat modeling, and zero trust architecture for connected environments. By focusing heavily on practical device hardening techniques and aligning with crucial compliance frameworks, this course is essential for cybersecurity professionals, developers, and engineers tasked with protecting sensitive data and maintaining operational technology (OT) integrity in a hyper-connected world.

IoT Security Essentials (ISE) and Device Hardening Training Course is meticulously designed to bridge the skills gap in IoT cybersecurity by offering deep dives into the latest vulnerabilities and mitigation strategies, utilizing strong keywords like firmware analysis, secure over-the-air (OTA) updates, and network segmentation. Through hands-on labs and real-world case studies, students will gain expertise in securing all layers of the IoT stack: device, network, cloud, and application. Graduates will be equipped to defend against sophisticated threats like IoT botnets and ensure the confidentiality, integrity, and availability of mission-critical IoT deployments, making them indispensable assets in the field of Cyber-Physical Systems (CPS) security.

Programme Curriculum

IoT Security Essentials (ISE) and Device Hardening Training Course

Course Introduction

The Internet of Things (IoT) revolution has introduced unprecedented connectivity, but this massive expansion of devices from smart homes to industrial sensors has simultaneously created a significantly larger and more complex attack surface. This critical training, IoT Security Essentials (ISE) & Device Hardening, provides participants with the foundational and advanced knowledge required to proactively secure the entire IoT ecosystem. Learners will master key concepts like embedded device security, secure boot mechanisms, IoT threat modeling, and zero trust architecture for connected environments. By focusing heavily on practical device hardening techniques and aligning with crucial compliance frameworks, this course is essential for cybersecurity professionals, developers, and engineers tasked with protecting sensitive data and maintaining operational technology (OT) integrity in a hyper-connected world.

IoT Security Essentials (ISE) and Device Hardening Training Course is meticulously designed to bridge the skills gap in IoT cybersecurity by offering deep dives into the latest vulnerabilities and mitigation strategies, utilizing strong keywords like firmware analysis, secure over-the-air (OTA) updates, and network segmentation. Through hands-on labs and real-world case studies, students will gain expertise in securing all layers of the IoT stack: device, network, cloud, and application. Graduates will be equipped to defend against sophisticated threats like IoT botnets and ensure the confidentiality, integrity, and availability of mission-critical IoT deployments, making them indispensable assets in the field of Cyber-Physical Systems (CPS) security.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Analyze the IoT ecosystem and its unique cybersecurity challenges.
2. Implement Secure Boot and hardware-based root of trust mechanisms on embedded devices.
3. Perform IoT Threat Modeling and Risk Assessment using methodologies like STRIDE.
4. Master Firmware Analysis and implement secure Over-The-Air (OTA) update processes.
5. Apply strong Cryptographic Controls and Data-in-Transit protection for IoT protocols.
6. Configure Network Segmentation and micro-segmentation for OT/IT Convergence.
7. Design and deploy Identity and Access Management (IAM) solutions for devices and users in IoT.
8. Identify and mitigate common OWASP IoT Top 10 vulnerabilities in applications and APIs.
9. Apply Security-by-Design principles throughout the IoT Software Development Lifecycle (SDLC).
10. Develop effective IoT Incident Response and forensic capabilities for compromised devices.
11. Implement AI-Driven Threat Detection and anomaly monitoring for large-scale IoT deployments.
12. Ensure Regulatory Compliance with frameworks like GDPR, HIPAA, and NIST for IoT data privacy.
13. Execute Penetration Testing techniques against IoT devices, networks, and communication channels.

Target Audience

1. Cybersecurity Professionals and Security Analysts.
2. IoT Developers and Engineers.
3. Embedded Systems Engineers.
4. Network Architects and Cloud Engineers.
5. IT/OT Security Managers and Product Owners.
6. Vulnerability Researchers and Penetration Testers.
7. Compliance Officers and Risk Managers
8. Industrial Control Systems (ICS) and SCADA security personnel.

Course Modules

Module I: IoT Ecosystem & Threat Landscape

- Define the layers of the IoT ecosystem.
- Analyze the unique attack surface of resource-constrained embedded systems.
- Examine evolving threats, including DDoS botnets and supply chain attacks.
- Understand the risk amplification caused by the scale of connected devices.
- Case Study: The Mirai Botnet Attack-Analysis of how weak default credentials and basic device hardening failures led to massive distributed attacks.

Module II: Embedded Device Hardening

- Implementing hardware root of trust using technologies like TPM/TEE.
- Securing the boot process with Secure Boot and validated firmware.
- Techniques for tamper-proofing and physical security of IoT enclosures.
- Best practices for disabling unused ports and minimizing the device footprint.
- Case Study: Smart Meter Tampering-Reviewing methods used to physically bypass security on utility meters and the necessary hardware/firmware countermeasures.

Module III: IoT Network & Protocol Security

- Securing lightweight protocols like MQTT and CoAP with end-to-end encryption.
- Designing robust Network Segmentation strategies for IoT/OT environments.
- Deep dive into 5G and LPWAN security implications and controls.
- Implementing Zero Trust Network Access (ZTNA) principles for IoT traffic.
- Case Study: Target/Heating, Ventilation, and Air Conditioning (HVAC) Breach-How a seemingly isolated smart device on a flat network was used as an entry point for lateral movement.

Module IV: Firmware and Software Integrity

- Methodologies for firmware extraction and reverse engineering for security analysis.
- Implementing digital code signing to ensure software authenticity and integrity.
- Designing and testing a secure, authenticated Over-The-Air (OTA) update process.
- Mitigating common software vulnerabilities like buffer overflows and command injection.
- Case Study: WannaCry/EternalBlue-Style Firmware Exploits-Analyzing a major unpatched vulnerability in widely used industrial IoT firmware and the patch management failures.

Module V: Cloud & Application Security for IoT

- Securing the data plane and control plane in the cloud backend for IoT platforms.
- Implementing least-privilege IAM policies for devices and microservices.
- Addressing OWASP IoT Top 10 vulnerabilities in the web and mobile applications.
- Focus on data privacy at rest and in transit, including anonymization/tokenization.
- Case Study: VTech Data Breach-Analyzing the exploitation of insecure web APIs connected to IoT children's devices and the subsequent sensitive data exposure.

Module VI: IoT Threat Modeling & Risk Management

- Conducting structured Threat Modeling using frameworks like STRIDE/DREAD on a new IoT device.
- Performing vulnerability assessment and penetration testing specifically for IoT.
- Integrating security practices into the DevSecOps pipeline for continuous assurance.

- Applying the NIST Cybersecurity Framework to IoT deployments.
- Case Study: Connected Car Hacking (Jeep)-Reviewing the threat model of a vehicle's telematics system and the ethical hacking process that forced a major recall.

Module VII: Operational Technology (OT) Security

- Understanding the unique constraints and priorities of IIoT and ICS environments.
- Securing industrial protocols like Modbus, Profinet, and OPC UA.
- Strategies for protecting Critical Infrastructure from cyber-physical attacks.
- Designing a secure demilitarized zone (DMZ) between IT and OT networks.
- Case Study: Stuxnet Worm-In-depth analysis of how a sophisticated attack targeted physical centrifuges using zero-day vulnerabilities in a highly isolated industrial control system.

Module VIII: Incident Response & Forensics in IoT

- Developing an IoT Incident Response Plan (IRP) and playbook.
- Implementing AI-driven Anomaly Detection for non-traditional IoT traffic patterns.
- Collecting and preserving volatile evidence from resource-constrained embedded systems.
- Utilizing Threat Intelligence feeds for proactive defense against botnet campaigns.
- Case Study: Colonial Pipeline Attack-Examining the impact of a Ransomware attack that affected an OT environment and the subsequent response and recovery efforts.

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
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

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

Register Online Now

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