Threat Analysis in IoT and Smart Device 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 represents the next massive frontier of network connectivity, seamlessly integrating billions of smart devices from industrial sensors to connected vehicles and home automation systems into our daily lives and critical infrastructure. While this interconnected ecosystem promises unprecedented efficiency and data-driven insights, it has simultaneously opened an enormous, diverse attack surface for malicious actors. Traditional network security models are ill-equipped to handle the unique challenges of resource-constrained devices, proprietary protocols, and fragmented supply chain vulnerabilities inherent to IoT. A proactive, specialized approach to security is not just recommended, it's mission-critical.

Threat Analysis in IoT and Smart Device Training Course is designed to bridge the skills gap by providing a deep dive into the specific methodologies required to secure these complex systems. Participants will gain hands-on expertise in vulnerability assessment, firmware analysis, and protocol exploitation, moving beyond theoretical knowledge to practical, real-world mitigation strategies. By focusing on emerging threats like IoT botnets, zero-day exploits, and physical security risks, we ensure that security professionals are equipped to establish robust, end-to-end security and maintain data integrity across the entire IoT security lifecycle, thereby safeguarding both consumer privacy and critical infrastructure.

Programme Curriculum

Threat Analysis in IoT and Smart Device Training Course

Introduction

The Internet of Things represents the next massive frontier of network connectivity, seamlessly integrating billions of smart devices from industrial sensors to connected vehicles and home automation systems into our daily lives and critical infrastructure. While this interconnected ecosystem promises unprecedented efficiency and data-driven insights, it has simultaneously opened an enormous, diverse attack surface for malicious

actors. Traditional network security models are ill-equipped to handle the unique challenges of resource-constrained devices, proprietary protocols, and fragmented supply chain vulnerabilities inherent to IoT. A proactive, specialized approach to security is not just recommended, it's mission-critical.

Threat Analysis in IoT and Smart Device Training Course is designed to bridge the skills gap by providing a deep dive into the specific methodologies required to secure these complex systems. Participants will gain hands-on expertise in vulnerability assessment, firmware analysis, and protocol exploitation, moving beyond theoretical knowledge to practical, real-world mitigation strategies. By focusing on emerging threats like IoT botnets, zero-day exploits, and physical security risks, we ensure that security professionals are equipped to establish robust, end-to-end security and maintain data integrity across the entire IoT security lifecycle, thereby safeguarding both consumer privacy and critical infrastructure.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Analyze the IoT Architecture stack to identify specific vulnerability domains.
2. Perform Device-Level Penetration Testing, focusing on hardware hacking and physical security bypass techniques.
3. Execute Firmware Extraction and Reverse Engineering to uncover embedded secrets and weak configurations.
4. Conduct Protocol Analysis on proprietary and standard IoT communication layers for exploitation opportunities.
5. Develop effective Threat Models for heterogeneous IIoT and Smart Home ecosystems.
6. Identify and mitigate risks associated with Insecure APIs and Cloud-Backend Services in IoT deployments.
7. Implement best practices for Secure Boot and over-the-air (OTA) Firmware Update mechanisms.
8. Understand and apply concepts of Zero Trust Architecture (ZTA) to segment and secure extensive IoT networks.
9. Investigate and respond to IoT Botnet and DDoS attack indicators using Threat Intelligence.
10. Formulate an IoT Incident Response plan, focusing on device forensics and evidence handling in constrained environments.
11. Design and deploy Identity and Access Management (IAM) solutions for a massive scale of diverse IoT devices.
12. Ensure Regulatory Compliance and data privacy adherence for sensitive IoT data streams.
13. Utilize AI/ML techniques for Anomaly Detection and proactive Behavioral Monitoring of compromised smart devices.

Target Audience

1. Cybersecurity Analysts and Consultants.
2. Penetration Testers.
3. IoT Developers and System Architects.
4. Security Engineers.
5. Product Security Engineers in manufacturing or smart device companies.
6. IT/OT Auditors and Compliance Officers.
7. Incident Responders.

8. Embedded Systems Engineers.

Course Modules

Module 1: Foundational IoT/Smart Device Architecture and Threats

- The IoT Ecosystem.
- OWASP IoT Top 10 vulnerabilities explained and prioritized.
- Protocol deep dive.
- The unique challenge of resource constraints on security controls.
- Case Study: Mirai Botnet ?Çô Analysis of how insecure default credentials and massive scale exploited vulnerable routers and cameras.

Module 2: Hardware and Physical Security Analysis

- Identifying and exploiting hardware debugging interfaces
- Non-invasive and semi-invasive hardware attacks
- Disassembling a device for firmware extraction via flash chips.
- Techniques for making devices tamper-resistant and physically secure.
- Case Study: Smart Lock Bypass ?Çô Demonstration of how readily available tools can exploit exposed debugging pins to gain root access on a commercial smart lock.

Module 3: Firmware Reverse Engineering and Analysis

- Tools and techniques for firmware dumping and extraction.
- Using emulation to safely analyze running firmware behavior.
- Identifying and exploiting binary vulnerabilities
- Patching and re-flashing vulnerable firmware for proof-of-concept exploits.
- Case Study: Router Vulnerability ?Çô Analyzing a manufacturer's proprietary OS firmware to discover a critical unauthenticated remote code execution flaw.

Module 4: IoT Network and Wireless Protocol Exploitation

- Scanning and fingerprinting IoT devices in segmented networks.
- Attacking Bluetooth Low Energy and ZigBee mesh networks.
- Man-in-the-Middle attacks on constrained-node networks.
- Setting up a controlled lab environment for safe IoT exploitation practice.
- Case Study: Vehicle Telematic Hacking ?Çô Exploiting a CAN bus or in-vehicle Wi-Fi vulnerability to remotely control non-critical systems.

Module 5: Cloud, Web Service, and API Security

- Assessing the security posture of cloud backend services
- Exploiting insecure APIs for authentication bypass and mass data leakage.
- Misconfiguration of Identity and Access Management for device authentication.
- Secure configuration of data storage and processing in the cloud
- Case Study: Cloud Camera Breach ?Çô Compromising a central cloud service to access the live feeds and stored data of millions of geographically distributed cameras.

Module 6: Industrial IoT (IIoT) and Critical Infrastructure Threats

- Differences between IT and Operational Technology environments.

- Common threats and attack vectors against SCADA/ICS systems.
- Assessing risk using industry standards.
- Implementing network segmentation and air-gapping techniques for critical assets.
- Case Study: Stuxnet/Colonial Pipeline ?Çô Deep analysis of malware targeting Industrial Control Systems and its real-world impact on infrastructure.

Module 7: Privacy, Legal, and Compliance in IoT

- Data collection, de-identification, and the lifecycle of Personally Identifiable Information (PII) on IoT.
- GDPR and CCPA implications for global IoT device manufacturers and data controllers.
- The role of Privacy-by-Design and default security settings.
- Legal and ethical hacking considerations when performing external vulnerability research.
- Case Study: Fitness Tracker Data Leak ?Çô Examining a case where location and health data from a wearable device led to the exposure of sensitive military personnel movements.

Module 8: Defense, Anomaly Detection, and Incident Response

- Developing and applying Zero Trust principles for micro-segmenting IoT networks.
- Implementing Behavioral Monitoring to detect compromised devices and anomalous activity.
- Best practices for IoT patch management and secure over-the-air updates.
- Digital forensics techniques for collecting and preserving volatile data from flash memory.
- Case Study: Supply Chain Attack ?Çô Analyzing the implications of a compromised third-party component and the subsequent incident response needed.

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