Document Generated: 11/22/2026

Learning Style: On Demand

Technology:

Difficulty: Beginner

Course Duration: 2 Weeks

IoT Practitioner



About This Course:

This course prepares learners to protect IoT devices, networks, and data across the full IoT ecosystem. Learners explore the IoT threat landscape and apply security-by-design principles to web and cloud interfaces, data, access control, privacy, software and firmware, and physical devices. Hands-on labs and practice questions reinforce each topic. The course aligns with the CertNexus Certified Internet of Things Security Practitioner (CIoTSP) exam

Course Objectives:

- Map the IoT attack surface and identify, prioritize, and respond to security risks
- Apply security-by-design principles throughout an IoT project
- Identify and mitigate web and cloud interface vulnerabilities, including injection, session management, cross-site scripting, and cross-site request forgery flaws
- Choose and apply cryptographic techniques such as encryption, hashing, and digital signatures, and manage cryptographic keys securely
- Protect IoT data in motion, at rest, and in use
- Implement secure authentication, authorization, and security monitoring for IoT resources
- Secure IoT networks using firewalls, intrusion detection and prevention systems, and protections against Wi-Fi and mobile network vulnerabilities
- Apply privacy-by-design principles and handle, protect, and dispose of sensitive data in line with privacy regulations
- Manage software and firmware risks, including installation, configuration, patching, and device operating systems
- Harden IoT devices against physical threats by securing local storage and physical ports

Audience:

- Cybersecurity analysts and IoT security professionals
- Solution architects designing IoT systems
- Network administrators and cloud engineers who manage connected devices
- Software developers, web developers, and platform engineers building IoT applications
- Product managers responsible for IoT products

Prerequisites:

- There are no formal prerequisites, and the course is beginner-friendly

Course Outline:

Module 1: IoT Fundamentals and Architecture

What IoT is and how it creates business value

The IoT ecosystem: devices, edge and fog computing, connectivity, cloud platforms, and applications

Common IoT reference architectures and frameworks

Selecting an architecture for an IoT project

Key benefits, challenges, and constraints of IoT adoption

Module 2: Building IoT Devices

Choosing microcontrollers and processing units based on project requirements

Selecting and managing power sources for IoT devices

Types of sensors and actuators and how they interface with microcontrollers

Assembling prototypes with development boards and breadboards

Lab: Connecting a microcontroller development board via USB

Lab: Installing components on a breadboard

Module 3: Programming and Firmware Development

Embedded programming with C, C++, and Python

Using software development kits (SDKs) to program IoT devices

Firmware structure: bootloaders, kernels, and application code

Updating and maintaining device firmware in the field

Module 4: IoT Connectivity and Communication

Wired communication options and interfaces

Wireless protocols for short-range and wide-area IoT networks

Internet protocols used in IoT, including TCP and UDP

Configuring network settings for IoT devices

Lab: Retrieving TCP settings

Lab: Retrieving UDP settings

Module 5: Processing and Analyzing IoT Data

Handling device input and output

Collecting data and applying filtering, aggregation, and time-series analysis

Processing IoT data in the cloud with platforms such as AWS IoT, Azure IoT, and Google Cloud

Enabling machine-to-machine (M2M) communication

Module 6: IoT Security, Privacy, and Safety

Common threats to IoT devices, networks, and data

Security protocols and hardening measures for IoT systems

Protecting user privacy and handling sensitive data

Identifying IoT safety hazards and applying risk management approaches

Lab: Conducting a DoS attack using a SYN flood

Lab: Identifying virus threats

Module 7: Managing IoT Projects

Real-world IoT applications across industries such as healthcare, agriculture, energy, logistics, and manufacturing

The stages of the IoT development lifecycle

Planning an IoT project: resource allocation, timelines, and risk assessment

Moving from prototype to deployment and ongoing operations

Module 8: CIoTP Exam Preparation

Mapping course content to the ITP-110 exam objectives

Exam format overview and test-taking strategies

Practice questions and review