CERTIFIED INTERNET OF THINGS
SECURITY PRACTITIONER
CIoTSP

Exam: ITS-110
Duration: 3 days; Instructor-led | Virtual Instructor-led

WHAT WILL YOU LEARN

This course is designed for practitioners who are seeking to demonstrate a vendor-neutral, cross-industry skill set that will enable them to design, implement, operate, and/or manage a secure IoT ecosystem.

OBJECTIVES

In this course, you will learn how to apply Internet of Things technologies to solve real-world problems. You will:
- Plan an IoT implementation.
- Construct and program an IoT device.
- Communicate with an IoT device using wired and wireless connections.
- Process sensor input and control an actuator on an IoT device.
- Manage security, privacy, and safety risks on IoT projects.
- Manage an IoT prototyping and development project throughout the development lifecycle.

PREREQUISITES

To ensure your success in this course you should have a fundamental understanding of IoT ecosystems, which you can obtain by taking the following CertNexus course:
- Certified Internet of Things (IoT) Practitioner (Exam ITP-110)

AUDIENCE

This course is designed for IoT practitioners who are looking to improve their skills and knowledge of IoT security and privacy. This course is also designed for students who are seeking the CertNexus Certified Internet of Things Security Practitioner (CIoTSP) certification and who want to prepare for Exam ITS-110.

COURSE CONTENTS

Module 1:   Managing IoT Risks
- **Topic A:** Map the IoT Attack Surface
- **Topic B:** Build in Security by Design

Module 2:   Securing Web and Cloud Interfaces
- **Topic A:** Identify Threats to IoT Web and Cloud Interfaces
- **Topic B:** Prevent Injection Flaws
- **Topic C:** Prevent Session Management Flaws
- **Topic D:** Prevent Cross-Site Scripting Flaws
- **Topic E:** Prevent Cross-Site Request Forgery Flaws
- **Topic F:** Prevent Unvalidated Redirects and Forwards

Module 3:   Securing Data
- **Topic A:** Use Cryptography Appropriately
- **Topic B:** Protect Data in Motion
- **Topic C:** Protect Data at Rest
- **Topic D:** Protect Data in Use

Module 4:   Controlling Access to IoT Resources
- **Topic A:** Identify the Need to Protect IoT Resources
- **Topic B:** Implement Secure Authentication
- **Topic C:** Implement Secure Authorization
- **Topic D:** Implement Security Monitoring on IoT Systems

Module 5:   Securing IoT Networks
- **Topic A:** Ensure the Security of IP Networks
- **Topic B:** Ensure the Security of Wireless Networks
- **Topic C:** Ensure the Security of Mobile Networks
- **Topic D:** Ensure the Security of IoT Edge Networks

Module 6:   Ensuring Privacy
- **Topic A:** Improve Data Collection to Reduce Privacy Concerns
- **Topic B:** Protect Sensitive Data
- **Topic C:** Dispose of Sensitive Data

Module 7:   Managing Software and Firmware Risks
- **Topic A:** Manage General Software Risks
- **Topic B:** Manage Risks Related to Software Installation and Configuration
- **Topic C:** Manage Risks Related to Software Patches and Updates

Module 8:   Promoting Physical Security
- **Topic A:** Protect Local Memory and Storage
- **Topic B:** Prevent Physical Port Access