Certified Internet of Things Security Practitioner (CIoTSP): Exam ITS-110

This document includes instructor led class overview and objectives, identifies target student and prerequisites, course outline, and course specific software and hardware requirements.

Course Length:

3 Days

Overview:

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.

Target Student:

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.

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)

Course Content

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

Lesson 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

Lesson 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

Lesson 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

Lesson 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

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

Lesson 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
- Topic D: Manage Risks Related to IoT Device Firmware

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

Course-specific Technical Requirements

Hardware

For this course, you will need one Windows PC for each student and one for the instructor. Each computer must have the following minimum hardware configurations:

- 1.83 GHz or faster 64-bit (x64) processor with 2 or more CPU cores
- 8 gigabytes or more RAM
- At least 30 GB available hard disk space after Windows 10 has been installed on the computer
- 1280 x 1024 (or higher) resolution monitor recommended
- Network cards and cabling or Wi-Fi for local network access
- Internet access (contact your local network administrator)
- Keyboard and mouse, trackpad, or other pointing device
- Projection system to display the instructor's computer screen

Software

If necessary, software for viewing the course slides. (Instructor machine only.)
Windows 10 (Home, Pro, Enterprise, or Education edition), 64 bit. Oracle VirtualBox version 6.0.6, which is included with the course data files.

While it is possible to run Oracle VirtualBox on other operating systems, this course was written and tested using Windows 10. If your classroom computers will use a different operating system, it is highly recommended that you install and test Oracle VirtualBox and the two course VMs on the computers to make sure you can key through the course successfully before delivering a class. The Linux and Android operating systems are already installed on the virtual machines that will be loaded in Oracle VirtualBox.