Course ID
IOTSEC
Course Duration
1-2 days

Course Title

Internet of Things: IoT & IoT Security Training

Related Courses

- Internet of Things (IoT): IoT Workshop (IOT1, 2 days)
- Internet of Things (IoT): IoT Overview (IOT-OVIEW, 1 day)
- IoT Training: In Depth (IOT3D, 3 days)
- M2M Course with IoT and LTE (M2MIOTLTE, 2-3 days)
- WiFi Training in Depth: Technology, Security, Deployment … with M2M, IoT, 5G (WIFI-DIVE, 2-5 days)

Aimed At

Managers and IT professionals who need to understand the basics of IoT as well as the present and emerging IoT security threats and solutions.

Prerequisites

General familiarity with the Internet and IT. Course does not assume engineering background.

Course in a Nutshell

With the falling costs and increasing capabilities of computer and network hardware and bandwidth, more and more devices are being designed to work with the Internet. Each added device brings security risks for the device user and potentially many other Internet users. This course examines the new and potentially quite serious IoT security issues that must be addressed by all Internet users.

In this course, you will learn the concepts that underlie the Internet of Things (IoT), enabling technologies, how the various hardware/software components work together to power end-user and infrastructure applications, current and projected future applications, IoT application creation, vulnerabilities created by the IoT, types of security issues and threats posed by the IoT, and techniques for prevention, protection, and remediation.

Customize It!

We can tailor this course to your participants' backgrounds and needs. We can include or exclude certain topics and shorten or lengthen the course duration.

Learn About

- What constitutes the IoT
- Visions of IoT
- What is different about the IoT and why it matters

- The creation of IoT applications and security implications
- IoT architectures and related security concerns
- How to address security issues raised by the rapidly growing IoT

Course Outline

- What is the Internet of Things (IoT)?
  - Defining ‘Things’: Hardware, software, data, and services
  - Core ideas
  - IoT objectives
  - Major players
  - Why IoT is important
  - Important IoT terms and trends
  - Major security risks and issues
  - Moore’s Law and its implications
- What is motivating deployment of the IoT and how will security affect it?
  - What needs does IoT fill?
  - The 4th Industrial Revolution
  - Security and IoT deployment
- IoT enabling technologies and associated security vulnerabilities
  - Cheap and ubiquitous telecommunications and computer hardware
  - Cloud Computing
  - Big Data, Event Stream Processing, Real-Time Analytics
  - Machine Learning
  - Wireless Sensor Networks (WSNs)
  - Low power short-range and wide area wireless networks
  - Embedded systems
  - Automation and Control Systems
  - Existing and emerging telecom technologies: Li-Fi, LPWAN, LTE-Advanced, 5G, WiFi-Direct, BLE, Low Energy, ZigBee, Z-Wave, Thread, HaLow, etc.
- Dealing with security concerns
  - Known issues
  - Emerging security vulnerabilities caused by IoT
  - The shifting security landscape and how it affects IoT
- IoT architecture, implementation and security
  - Where IoT fits in
  - Standards and ecosystem

  - Basic architecture concepts
  - Implementation platforms
  - Types of networks used by IoT
  - Designing security into IoT
- What constitutes a secure system?
  - What is a reasonable goal?
  - How much will it cost?
  - What happens when a new threat emerges?
  - How do we know if an IoT system is worth the risk?
- Wrap-up and discussion
  - Course recap
  - How does your organization envision leveraging the IoT?
  - Your organization's IoT security concerns

DCN KfTKf