+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 29/11/2023

Sign up

IoT and 5G security training

2 days (14 hours)

PRESENTATION

The emergence of the web and connected objects has revolutionized the way we live. Demand for connected objects has grown considerably in recent years.

The security of the IoT (or Internet of Things) is a crucial issue for protecting our environment (securing our home, our car, etc.).

A recent study shows that 90% of consumers show little confidence in security flaws in the IoT. A 2019 survey in 6 developed countries including France found that 63% of consumers find connected devices "scary".

Our IoT security training course will teach you the best practices for protecting your IoT architecture so that your consumers or employees have confidence in using connected devices.

OBJECTIVES

- Best practices for protecting your IoT architecture
- Learn about the various security vulnerabilities affecting the Internet of Things.

TARGET AUDIENCE

- IT security professionals
- People interested in hardware or embedded security issues
- Electronics enthusiasts or professionals

Prerequisites

- Command-line proficiency in Linux is a plus
- Windows/Linux administration

OUR IOT SECURITY TRAINING PROGRAM and 5G

The foundations of a secure IoT architecture

- A brief review of the history and evolution of IoT technologies
- The Data Model in IoT systems - definition and architecture of sensors, terminals and communication protocols
- Risks associated with supply chain services
- The IoT ecosystem - Terminal providers, gateway providers, analytics providers, platform providers, integrators - Associated risks
- Introduction to IoT communication protocols - Zigbee/NB-IoT/5G/LORA

Review of IT threats to connected objects

- Firmware Patching
- Detailed security review of known risks on these communication protocols (Zigbee/NB-IoT/5G/LORA) and application layers (MQTT)
- Gateway vulnerabilities
- Vulnerabilities with connected terminals - Gateway communication
- Vulnerabilities in the application layer
- Log management risk

The OSASP model

- I1 Insecure web interface
- I2 Autentication or insufficient authorization
- I3 Unsecured network services
- I4 Lack of transport encryption
- I5 Confidentiality issues
- I6 Insecure Cloud interface
- I7 Unsecured mobile interface
- I8 Insufficient configurability
- I9 Unsecured software/Firmware
- I10 Low physical security

Case studies

- Case study of the attack on October 21, 2016
- Buffer overflow attacks on surveillance cameras
- The ZigBee protocol hack
- SQL injections
- Cross-Site Scripting (XSS)

Best practices for a secure IoT architecture

- Track and identify all services connected to a Gateway
- Using MAC addresses
- Using identification hierarchies for terminals
- Securing the risks of IoT management portals
- Securing APIs
- Identify and integrate safety principles into the supply chain
- Minimizing IoT vulnerabilities through Patch Management strategies

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.