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

Updated on 02/04/2026

Register

Embedded Systems Cybersecurity Training

1 day (7 hours)

Overview

The Cyber Resilience Act (CRA) now requires manufacturers of connected devices to provide a comprehensive cybersecurity risk analysis. Risk analysis is no longer a mere formality: it is the cornerstone of Security by Design and a legal requirement for CE marking.

Our "Cybersecurity & Risk Analysis for Embedded Systems" training course introduces you to the EBIOS RM (Risk Manager) reference method and shows you how to adapt it to the specific constraints of the embedded world (IoT, IIoT, OT). In one intensive day, you will learn how to identify your "Essential Assets," build realistic attack scenarios (including physical and logical attacks), and define security measures proportionate to the challenges.

At the end of the training, you will have the methodological keys to initiate a CRA compliance process and communicate effectively with security experts or ANSSI.

This training course takes a pragmatic approach: we leave heavy theory aside to focus on building concrete scenarios applicable to your products.

Objectives

- Understand the risk assessment obligation imposed by the CRA.
- Learn about the EBIOS RM approach and its five key workshops.
- Adapt risk analysis to embedded system constraints (physical access, safety).
- Know how to construct credible operational scenarios (JTAG attacks, network, supply chain).
- Define a risk treatment plan for technical documentation.

Target audience

- Embedded systems & IoT architects
- Product owners
- Quality/operational safety managers
- CISOs/RSSIs wishing to understand the industrial scope

Prerequisites

- General knowledge of IT or electronic systems.
- No prior knowledge of the EBIOS method is required.

Technical prerequisites

- Laptop for consulting materials and completing workshops.

Our Embedded Systems Cybersecurity Training Program

[Morning]

Regulatory Context and Framework (Workshops 1 & 2)

- The Cyber Resilience Act (CRA): why is risk analysis becoming mandatory?
- Overview of the EBIOS RM method: principles and iterations
- Workshop 1 (The Foundation): Identifying specific support assets (firmware, keys, communication buses)
- Defining the scope and feared events (security vs. privacy impact)
- Workshop 2 (Sources of risk): Who are the attackers? (Cybercriminals, Competitors, States)
- Case study: Framing the analysis for a critical industrial connected object.

[Afternoon]

Attack Scenarios and Response (Workshops 3, 4 & 5)

- Workshop 3 (Strategic Scenarios): Risks related to the digital ecosystem (Cloud, Supply Chain, OTA Updates)
- Workshop 4 (Operational Scenarios): The technical core
- Modeling attack paths: Physical access (JTAG/UART), Network (Man-in-the-Middle), Logic (Buffer Overflow)
- Using knowledge bases (ATT&CK for ICS, CAPEC)
- Workshop 5 (Processing): Choosing security measures (Secure Boot, Encryption, Authentication)
- Validating residual risk and integrating it into the CRA Technical File
- Case study: Complete drafting of a technical attack scenario and selection of protective measures.

Companies concerned

This training is intended for both individuals and companies, large or small, wishing to train their teams in new advanced IT technology or to acquire specific professional knowledge or modern methods.

Positioning at the start of training

The positioning at the start of the training complies with Qualiopi quality criteria. Upon final registration, the learner receives a self-assessment questionnaire that allows us to assess their estimated level of knowledge of different types of technologies, their expectations and personal objectives for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could be problematic for the monitoring and smooth running of the training session.

Teaching methods

Practical training: 60% practical, 40% theory. Training materials distributed in digital format to all participants.

Organization

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

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been correctly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training course.