



Introduction to cybersecurity

Duration 3 day(s) (INIT-SECU)

Issues, actions and legality

Description

Security is a major issue in the digital world today. A design or security defect can be fatal to a business today: loss of data, resources and trust. This is why it is necessary to train to limit the risk to the maximum and especially to design secure applications (security by design).

Goals

- To provide the basis for understanding security issues today.
- Integrate security into development projects
- Study the main vulnerabilities present on the Web
- Offensive and defensive approach to security
- Understanding legal issues (CNIL, RGPD)

Public

Developer, Architect, TechLead

Prerequisites

Nil

Structure

40% Theory, 60% Practice

Program

Introduction

Network

- Reminder of OSI and TCP / IP models
- Study of different protocols
- Mapping a network
- Network Attack (MITM, Denial of Service)

Cryptography

- Fundamentals
- Symmetric and asymmetric encryption
- Certificate and PKI

SecDevOps

- Source code audit
- Dependency audit

Web

- Authentication methods
- HTTP protection header
- Studies of the main web vulnerabilities

Attack vs Defense

- Intrusion tests
- Social engineering
- SIEM
- SOC

Legal

- CNIL
- RGPD