Course : Security for mobile devices and applications, overview

Synthesis course - 1d - 7h00 - Ref. SPM
Price : 990 CHF E.T.

★★★★½   4,4 / 5

As mobile devices become an increasingly integral part of our working environment and projects, they are creating new security challenges. This seminar provides an overview of the security issues posed by these devices: communication, data storage, application publication...

Teaching objectives

At the end of the training, the participant will be able to:

- ✓ Identify security services for mobile operating systems
- ✓ Defining safety rules for mobile project management
- ✓ Differentiating security solutions by terminal
- ✓ Define the criteria for choosing an MDM solution
- ✓ Identifying the impact of BYOD on security

Intended audience

Project managers, developers, decision-makers, marketers and anyone who needs a clear, concise overview of mobile device and application security.

Prerequisites

No special knowledge required.

Course schedule

1 Terminals

- Presentation and specific features of cell phones and tablets.
- Systems (iOS, Android, BlackBerry): architectures, configuration, data, network and application security.
- Code signing. Memory protection.
- Browsers, user-agent application and sandbox.
- Sandbox applications.
- USB connection. Data recovery, SSH access. Limits and risks.

PARTICIPANTS
Project managers, developers, decision-makers, marketers and anyone who needs a clear, concise overview of mobile device and application security.

PREREQUISITES
No special knowledge required.

TRAINER QUALIFICATIONS
The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS
The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

2   Bring Your Own Device - BYOD and Mobile Device Management

- Issues surrounding BYOD, CYOD, COPE, BYOA.
- Challenges of BYOD (security, productivity, financial...). Initial feedback.
- The problem of our private professional data.
- Virtualization solutions (vmWare, Citrix, Hyper-V Client), Desktops as a Service.
- Mobile Device Management : Presentation of market solutions (AirWatch, MobileIron...). Apple iPhone configuration.
- MDM solution selection criteria (software, security, asset management).
- MDM: presentation of solutions from Microsoft, Samsung Knox and Blackberry.

3   Safety criteria

- Presentation of risks according to OWASP (GoatDroid, IOS Project).
- Storage of business data, sessions, authentication (memory, SD, FS, keychain, etc.).
- Understanding Android Root, Jailbreaking.
- Server exchange protocols.
- Impact of SQL and XSS injections in in-App and SMS applications.
- Solutions for authentication, authorization and biometrics.
- Encryption solutions (data, filesystem), terminal backup and restoration.
- Antivirus, antiphishing.

4   Developing an application in a store

- Publication rules AppStore, Google Play. Alternative stores, corporate stores.
- Apple publication certificates, provision files, certificates.
- Google License LVL.
- Application IPA, APK, disassembly.
- Impact of libraries and frameworks on application security.
- Remote content management and control.
- How do I test an application?
- Notification: outsourcing, spam risk, mechanisms.

Dates and locations

REMOTE CLASS
2026 : 18 June, 10 Dec.