Application Security for iOS

Duration: 5 days **Price: € 3299**

Open Schedule

Audience Course Application Security for iOS

The course Application Security for iOS is intended for IT professionals who want to learn how to protect iOS mobile apps against the many security risks.

Prerequisites Course Application Security for iOS

Affinity with the development of mobile apps is required to participate in this course. Experience with software development helps in understanding the subject matter but is not required.

Realization Training Application Security for iOS

The course Application Security for iOS has a hands-on character. The theory is treated on the basis of presentation slides and is interchanged with practical exercises.

Certification Course Application Security for iOS

After successfully participating in the training, the attendants receive a certificate of completion in Application Security for iOS.

Content Course Application Security for iOS

The course Application Security for iOS discusses how the iOS operating system and mobile apps on iOS can best be secured. In the training attention is paid to hardware, system, application, services and network security. The various forms of encryption, secure device management and the use of developer kit security are covered as well.

Intro Security

The course Application Security for iOS begins with a discussion of key security concepts such as authentication, data resilience, encryption, confidentiality, integrity and access control.

Hardware Security

Next hardware security in iOS systems is discussed, with attention being paid to biometrics and the role of Face ID and Touch ID. The architecture of the specialized subsystem Secure Enclave on the chips in Apple systems is also treated.

System Security

The built-in system security in the iOS operating system is also covered including secure boot, signed system volume security, operating system integrity and secure software updates.

Encryption and Protection

The protection of data through encryption, passcodes and passwords is an important part of iOS security. Attention is paid to File and Data vaults, line-speed encryption and the use of digital signing.

App Security

App Security is also part of the Application Security for iOS course. Here the app code signing process, the security of runtime processes and the secure features of apps such as notes and shortcuts are treated.

Services Security

Then it is time to pay attention to the security of services on iOS such as iCloud, Facetime, Apple Pay and Apple Wallet. Secure messages for business and Continuity that allows you to seamlessly switch between devices with an Apple ID are also covered.

Network Security

And network security is a program component as well. The security of various network protocols such as TLS, IPv6, Wi-Fi, AirDrop and Bluetooth are explained. The Single Sign On functionality is also covered.

Secure Device Management

Finally attention is paid to how devices such as the camera and routers are secured. The security features of various Developer Kits such as HomeKit, SiriKit, DriverKit, ReplayKit and ARKit are on the program as well.

SpiralTrain BV
Standerdmolen 10, 2e verdieping
3995 AA Houten

info@spiraltrain.nl
www.spiraltrain.nl
Tel.: +31 (0) 30 – 737 0661

Locations
Houten, Amsterdam, Rotterdam, Eindhoven, Zwolle, Online

Modules Course Application Security for iOS

Module 1 : Intro Security	Module 2 : Hardware Security	Module 3 : System Security
Access Controls Authentication Backups and Recovery Data Erasure Data Masking Data Resiliency Encryption Confidentiality Integrity Availability	Biometrics Hardware security overview Apple SoC security Secure Enclave Face ID Touch ID Memory Protection Microphone Disconnect Express Cards Power Reserve	System security overview Secure boot Signed system volume security Secure software updates Operating system integrity Storage Encryption More system security capabilities System security for watchOS Random number generation Apple Security Research Device
Module 4 : Encryption and Protection	**Module 5 : App Security**	**Module 6 : Services Security**
Encryption Protection Data Protection Passcodes and passwords File Vault Data Vault User personal data Protection Digital signing and encryption Secure Enclave Line-speed Encryption	App security overview App security in iOS iPad OS Security App code signing process Security of runtime process Supporting extensions App protection and app groups Secure features in Notes app Secure features in Shortcuts app	Apple ID and Managed Apple ID iCloud Passcodes and Passwords Apple Pay Using Apple Wallet iMessage Secure Messages for Business FaceTime security Continuity
Module 7 : Network Security	**Module 8 : Developer Kit Security**	**Module 9 : Secure Device Management**
Network security overview TLS and IPv6 security VPN security Wi-Fi security Bluetooth security Single sign-on AirDrop security Firewall security	Developer kit security overview HomeKit security Camera Security Securing Routers SiriKit security DriverKit security ReplayKit security ARKit security	Secure Device Management Overview Pairing Model Security Mobile device management Apple Configurator security Screen Time security BYOD Program Apple File System Automated Device Enrollment