Application Security voor Android

Duur: 5 dagen Prijs: € 3299

Open Rooster

Doelgroep Cursus Application Security voor Android

De cursus Application Security voor Android is bedoeld voor IT professionals die willen leren hoe je Android mobile apps beschermt tegen de vele veiligheidsrisico's.

Voorkennis Cursus Application Security voor Android

Om aan deze cursus te kunnen deelnemen is affiniteit met de ontwikkeling van mobile apps vereist. Ervaring met software development helpt bij de begripsvorming maar is niet vereist.

Uitvoering Training Application Security voor Android

De cursus Application Security voor Android heeft een hands-on karakter. De theorie wordt behandeld aan de hand van presentatie slides en wordt afgewisseld met praktische oefeningen.

Certificering cursus Application Security voor Android

De deelnemers krijgen na het goed doorlopen van de training een certificaat van deelname aan Application Security voor Android.

Inhoud Cursus Application Security voor Android

De cursus Application Security voor Android behandelt hoe het Android operating systeem en mobile apps op Android het beste beveiligd kunnen worden. Aandacht wordt besteed aan de Google Security Services, de security architectuur van het Android platform en kernel en applicatie security. De training gaat ook in op de implementatie van security en de rapportage van security issues.

Intro Security

De cursus Application Security for Android gaat van start met een verklaring van belangrijke security begrippen zoals authenticatie, encryption, data resilience, backup, recovery, confidentiality, integrity en access control.

Google Security Services

Vervolgens wordt ingegaan op de Security Services die door Google worden aangeboden zoals App Services, Safety Net Attestation, Google Play, Penetration Testing en de Android Device Manager.

Platform Security Architecture

Ook wordt aandacht besteed aan de Android Platform Architecture die voorziet in bescherming van Apps, User Data, Networking en Inter Process Communication. Tevens komen dan App Signing en App en User Permissions aan bod.

Kernel Security

Onderdeel van het programma van de cursus Application Security voor Android is ook een bespreking van de kernel security die gebaseerd is op Linux. Daarbij wordt onder andere aandacht besteed aan de application sandbox, safe mode, filesystem permissions, storage encryption en de verified boot.

Application Security

Vervolgens komt application security aan de orde waarbij ingegaan wordt op het Android Permission Model voor het benaderen van Protected API's, het werken met content providers, Sensitive Data Input Devices en Application Signing.

Implementing Security

En ook aan de implementatie van security in Android wordt aandacht besteed. Die security wordt bevorderd door code reviews, het gebruik van Android Lint en het loggen van data. Eveneens komt het beveiligen van SUID files en configuratie files en het beperken van directory en device driver access aan de orde.

Security Updates en Reports

Tenslotte wordt ingegaan op het belang van security updates, de rapportage van security issues en de triaging van bugs. De belangrijkste zaken uit Android Reports en White Papers van de afgelopen jaren worden ook besproken.

Modules Cursus Application Security voor Android

Module 1 : Intro Security	Module 2 : Google Security Services	Module 3 : Platform Security Architecture
Access Controls Authentication Backups and Recovery Data Erasure Data Masking Data Resiliency Encryption Confidentiality Integrity	Google Play Android Updates App Services Verify Apps Safety Net Safety Net Attestation Android Device Manager Penetration Testing Incident Response	App Protection Protecting User Data Protecting System Resources Network Protection Mandatory App Sandbox Secure Inter Process Communication App Signing App Defined Permissions User Granted Permissions
Module 4 : Kernel Security	**Module 5 : Application Security**	**Module 6 : Implementing Security**
Linux Security Application Sandbox System Partition and Safe Mode Filesystem Permissions Verified Boot Cryptography Rooting of Devices Storage Encryption Lockscreen Credential Protection Device Administration	Android Permission Model Accessing Protected API's Binder, Services, Intent Content Providers Cost Sensitive API's SIM Card Access Sensitive Data Input Devices Device Metadata Certificate Authorities Application Signing	Reviewing Source Code Android Lint Signing System Images Signing applications (APKs) Isolating Processes Securing SUID files Logging Data Limiting Directory Access Securing Configuration Files Limiting Device Driver Access
Module 7 : Security Updates	**Module 8 : Security Reports**	
Reporting Security Issues Triaging Bugs Context Types Rating Modifiers Local, Proximal, Remote Network Security Biometric Authentication Android Automotive OS Releasing code to AOSP Receiving Android Updates Updating Google Services	Annual Reviews 2014 Report 2015 Report 2016 Report 2017 Report 2018 Report White Papers 2018 White Paper 2019 White Paper 2020 While Paper 2021 White Paper	