

Opleiding : Beveiliging van mobiele apparaten en toepassingen, samenvatting

Synthese cursus - 1d - 7u00 - Ref. SPM

Prijs : 850 € V.B.



4,4 / 5

Mobiele apparaten worden steeds meer een integraal onderdeel van onze werkomgeving en onze projecten, en dit zorgt voor nieuwe uitdagingen op het gebied van beveiliging. Dit seminar biedt een overzicht van de beveiligingsproblemen die deze apparaten met zich meebrengen: communicatie, gegevensopslag, publicatie van toepassingen, enz.



Pedagogische doelstellingen

Aan het einde van de training is de deelnemer in staat om:

- ✓ Beveiligingsdiensten voor mobiele besturingssystemen identificeren
- ✓ Veiligheidsregels definiëren voor mobiel projectbeheer
- ✓ Onderscheid maken tussen beveiligingsoplossingen voor verschillende terminals
- ✓ De criteria bepalen voor het kiezen van een MDM-oplossing
- ✓ De impact van BYOD op beveiliging identificeren

Doelgroep

Projectmanagers, ontwikkelaars, besluitvormers, marketeers en iedereen die behoefte heeft aan een helder, beknopt overzicht van de beveiliging van mobiele apparaten en toepassingen.

Voorafgaande vereisten

Geen speciale kennis vereist.

Opleidingsprogramma

DEELNEMERS

Projectmanagers, ontwikkelaars, besluitvormers, marketeers en iedereen die behoefte heeft aan een helder, beknopt overzicht van de beveiliging van mobiele apparaten en toepassingen.

VOORAFGAANDE VEREISTEN

Geen speciale kennis vereist.

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ... De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

1 Terminals

- Presentatie en specifieke kenmerken van mobiele telefoons en tablets.
- Systemen (iOS, Android, BlackBerry): architecturen, configuratie, beveiliging van gegevens, netwerken en toepassingen.
- Code ondertekenen. Geheugenbescherming.
- Browsers, clienttoepassing (user-agent) en de sandbox daarvan.
- Sandbox-toepassingen.
- USB-aansluiting. Gegevensherstel, SSH-toegang. Grenzen en risico's.

2 Bring Your Own Device - BYOD en beheer van mobiele apparaten

- Vraagstukken rondom BYOD, CYOD, COPE en BYOA.
- De uitdagingen van BYOD (beveiliging, productiviteit, financiën, enz.). Eerste feedback.
- De kwestie van onze persoonlijke professionele gegevens.
- Virtualisatie-oplossingen (vmWare, Citrix, Hyper-V Client), Desktops as a Service.
- Beheer van mobiele apparaten: Presentatie van marktoplossingen (AirWatch, MobileIron, enz.). Apple iPhone configuratie.
- Selectiecriteria voor MDM-oplossingen (software, beveiliging, beheer van hardwareactiva).
- MDM: presentatie van oplossingen van Microsoft, Samsung Knox en BlackBerry.

3 Veiligheidscriteria

- Presentatie van de risico's volgens OWASP (GoatDroid, IOS Project).
- Opslag van bedrijfsgegevens, sessies, verificatie (geheugen, SD, FS, sleutelhanger, enz.).
- Android Root, Jailbreaking begrijpen.
- Serveruitwisselingsprotocollen.
- Invloed van SQL- en XSS-injecties in in-App- en sms-applicaties.
- Oplossingen voor authenticatie, autorisatie en biometrie.
- Oplossingen voor versleuteling (gegevens, bestandssysteem), back-up en herstel van terminals.
- Antivirus, anti-phishing.

4 Een applicatie ontwikkelen in een winkel

- Publicatieregels AppStore, Google Play. Alternatieve winkels, bedrijfswinkels.
- Apple publicatiecertificaten, provisionele bestanden, certificaten.
- Google Licentie LVL.
- IPA-toepassing, APK, demontage.
- Invloed van bibliotheken en frameworks op de beveiliging van applicaties.
- Beheer en controle van inhoud op afstand.
- Hoe test je een applicatie?
- Kennisgeving: uitbesteding, spamrisico, mechanismen.

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

- De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
- Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
- Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

Data en plaats

KLAS OP AFSTAND
2026 : 18 juni, 10 dec.

PARIS LA DÉFENSE
2026 : 18 juni, 10 dec.