Publicatiedatum : 16/07/2024

Opleiding : Forensisch onderzoek van smartphones

Praktijkcursus - 4d - 28u00 - Ref. FOB
Prijs : 2460 € V.B.

Deze cursus geeft je de kennis die je nodig hebt om forensische analyses uit te voeren op verschillende mobiele systemen (iOS, Android).

Pedagogische doelstellingen

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

- De instrumenten en methodologie van forensisch telefoononderzoek op basisniveau leren gebruiken
- Analyseren van aanvallen op mobiele systemen.
- Een forensisch onderzoeksrapport schrijven

Doelgroep

Mensen die aan de slag willen met mobiel forensisch onderzoek. Systeembeheerders. Forensisch computer experts.

Voorafgaande vereisten

Een solide basis in de beveiliging van informatiesystemen.

Praktische modaliteiten

Praktisch werk

Training waarin theorie en praktijk worden afgewisseld. Alles wat je leert, breng je in de praktijk.

Opleidingsprogramma

1 Forensische analyse van een mobiel systeem

- Forensisch computeronderzoek.
- Soorten computercriminaliteit op mobiele systemen.
- Rol van de IT-onderzoeker.

DEELNEMERS

Mensen die aan de slag willen met mobiel forensisch onderzoek. Systeembeheerders. Forensisch computer experts.

VOORAFGAANDE VEREISTEN

Een solide basis in de beveiliging van informatiesystemen.

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.

2 Moderne cybercriminaliteit

- Soorten misdrijven.
- Beheerskader voor beveiligingsincidenten, CERT.
- Laboratoria opzetten: iOS-onderzoekstools.
- Analyseren en begrijpen van aanvallen op mobiele systemen.
- Beschermingsmiddelen, Franse wetgeving.

Praktisch werk

Netwerkanalyse van DDOS-aanvallen, infecties en BotNet-verkeer.

3 Digitaal bewijs

- Definitie, rol, types en archiveringsregels.
- Evalueren en beveiligen van de elektronische elementen van een plaats delict.
- Verzamelen en bewaren van de integriteit van bewijsmateriaal.

Praktisch werk

Bit-voor-bit duplicatie, integriteit, bestandsherstel en gegevensanalyse.

4 Forensische bases voor mobiele systemen.

- Inzicht in de architectuur van mobiele systemen en simkaarten.
- Mobiele forensische technieken.
- Mobiele forensische processen.

Praktisch werk

Analyse van mobiele toepassingen en malware. Forensisch onderzoek met Santoku-distributie.

5 Gegevens van mobiele systemen verzamelen en analyseren

- Verzamelen van vluchtige en niet-vluchtige gegevens.
- Hoe het identificatiesysteem werkt.
- Gegevensanalyse.
- Analyse van cache, cookies, browsegeschiedenis, gebeurtenissen.
- Verwerving, analyse en reactie.
- Opstartproces.

Praktisch werk

RAM verzamelen en analyseren. Bestandsintegriteit controleren. Browser- en registergegevens verkennen.

6 De basisbeginselen van forensische analyse van Android-systemen

- Toepassingsanalyse en reverse engineering.
- Studie van architecturen: Kernel, Android Runtime, Bibliotheken.
- Studie van systeembeveiliging.
- Sluittechnieken omzeilen.
- Verkrijg rootrechten.

Praktisch werk

Onderzoek van een afbeelding van een Android-systeem: omzeilen van encryptie, analyse van beeldgegevens.

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.

7 De basisbeginselen van forensische analyse van iOS-systemen

- De hardwarestructuur van Apple systemen.
- Bestandssysteem.
- Architectuur en beveiliging.
- Verzamel gegevens van een afbeelding en van een iCloud-systeem.
- Gebruik van tools zoals Elcomsoft iOS of Oxygen Forensic Detective.

Praktisch werk
Voer een onderzoek uit van een iOS-afbeelding.

8 Forensische onderzoeksrapporten

- Het belang van relaties begrijpen.
- Copywritingmethoden en sjablonen.

Data en plaats

KLAS OP AFSTAND
2026 : 24 maa., 2 juni, 20 okt., 15 dec.

PARIS LA DÉFENSE
2026 : 17 maa., 26 mei, 13 okt., 15 dec.