Publicatiedatum : 13/05/2024

Opleiding : Forensisch iOS

Praktijkcursus - 3d - 21u00 - Ref. FOE
Prijs : 2100 € V.B.

Deze cursus geeft je de kennis die je nodig hebt om forensische analyses op iOS uit te voeren.

Pedagogische doelstellingen

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

- De sporen identificeren die achterblijven wanneer een computersysteem wordt gekraakt
- Onderzoek de verschillende Apple systemen
- Correct het bewijs verzamelen dat nodig is voor juridische procedures
- Leren over verschillende onderzoekstechnieken

Doelgroep

Systeem- en netwerkingenieurs/beheerders, beveiligingsmanagers.

Voorafgaande vereisten

Goede kennis van IT-beveiliging, netwerken/systemen en iOS-systemen.

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

Systeem- en netwerkingenieurs/beheerders, beveiligingsmanagers.

VOORAFGAANDE VEREISTEN

Goede kennis van IT-beveiliging, netwerken/systemen en iOS-systemen.

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.
- Het opzetten van de labs: gereedschappen die nodig zijn voor iOS-onderzoek.
- 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.
- Verzamel en behoud de integriteit van elektronisch bewijs.

Praktisch werk

Dupliceer gegevens bit voor bit, controleer de integriteit, herstel bestanden en analyseer digitale gegevens.

4 Forensische grondslagen voor mobiele systemen

- Inzicht in de architectuur van mobiele systemen en simkaarten.
- Forensische technieken voor mobiele systemen.
- Forensische processen voor mobiele systemen.

Praktisch werk

Analyse des applications et malwares sous mobile. Etude de la distribution forensic Santoku.

5 De basisbeginselen van forensische analyse van iOS-systemen

- Architectuur en beveiliging van iOS-systemen.
- Hardwarestructuur en modellen van Apple systemen: mobiele telefoons, horloges, iPad.
- Bestandssysteem voor Apple systemen.

Praktisch werk

Een iOS forensisch onderzoekslab opzetten.

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.

6 Technieken voor het extraheren en analyseren van gegevens uit iOS-systemen

- Technieken voor het vastleggen en analyseren van gegevens en versleutelde of onversleutelde back-ups.
- Verzamelen van vluchtige en niet-vluchtige gegevens.
- Analyse en herstel van iOS-gegevens.
- Omzeilen van beveiligingstechnieken voor iOS-systemen.
- Verzamel gegevens van een vastgelegde afbeelding en een iCloud-systeem.
- Gebruik van mobiele onderzoekstools zoals Elcomsoft iOS of Oxygen Forensic Detective, NowSecureCE.
- Technieken voor het extraheren van gegevens uit software van derden.

Praktisch werk
Onderzoek een vastgelegd beeld van een iOS-systeem: jailbreak iOS-systemen, omzeil encryptie, verzamel en analyseer gegevens in RAM, extraheer applicatiegegevens.

7 Forensische onderzoeksrapporten

- Het belang van onderzoeksrapporten begrijpen.
- Schrijven van methodologieën en sjablonen voor iOS forensische rapporten.

Data en plaats

KLAS OP AFSTAND
2026 : 3 juni, 19 okt., 7 dec.

PARIS LA DÉFENSE
2026 : 27 mei, 12 okt., 30 nov.