Publicatiedatum : 13/05/2024

Opleiding : Forensisch onderzoek Windows

Praktijkcursus - 5d - 35u00 - Ref. FOH
Prijs : 3120 € V.B.

4,2 / 5

Na een computeraanval wordt forensisch onderzoek gebruikt om bewijs te verzamelen en te analyseren voor juridische procedures. Het hoofddoel is daarom het herstellen en analyseren van gegevens die een digitaal misdrijf bewijzen.

Pedagogische doelstellingen

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

- Een digitaal onderzoek beheren op een Windows-computer
- Analyse na de inbraak
- Verzamelen en bewaren van de integriteit van elektronisch bewijsmateriaal

Doelgroep

Mensen die aan de slag willen met forensisch computeronderzoek. Systeembeheerders van Windows. 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

DEELNEMERS

Mensen die aan de slag willen met forensisch computeronderzoek. Systeembeheerders van Windows. 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.

1 Inleiding tot forensisch computeronderzoek

- Reikwijdte van het onderzoek.
- Toolkit, First Responder-methodologie en postmortale analyse.
- Harde schijven, inleiding tot bestandssystemen en tijdstempels.
- Gegevensverzameling (persistent en vluchtig) en gecodeerd mediabeheer.
- Zoeken naar verwijderde gegevens.
- Back-ups, Volume Shadow Copies en de grillen van flashopslag.
- Windows registers en registerstructuren.
- Analyse van logs, gebeurtenissen / antivirus / andere software.

2 Onderzoeksscenario

- Downloaden/toegang tot vertrouwelijke inhoud.
- Sporen van programma-uitvoering, bestands- en mapmanipulatie.
- Verwijderde bestanden, niet-toegewezen ruimte en carving.
- Geolocatie en foto's (Exifs-gegevens).
- SMTP logs: server-side acquisitie, e-mail client analyse.
- WiFi-toegangspunten en USB-apparaten.
- HTML5, e-mails en gebruikers misbruikt door malware.
- Exfiltratie van informatie.

3 Interactie op internet

- Office 365.
- Sharepoint.
- Traces op Windows AD's.
- Presentatie van de belangrijkste artefacten.
- Grondbeginselen van RAM-analyse.
- Gebruik van internetbrowsers.
- Chrome / IE / Edge / Firefox.

4 Linux forensisch onderzoek

- De basis van inforensics op een Linux werkstation.
- De basis van inforensics op een Linux server: Web server logs & correlaties met het bestandssysteem.
- Aanmaken en analyseren van een tijdlijn van een bestandssysteem.

5 Overzicht

- Creatie en analyse van een tijdlijn verrijkt met artefacten.
- Voorbeeld van tools voor het bevragen van grote hoeveelheden gegevens.

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 : 15 juni, 28 sep., 7 dec.

PARIS LA DÉFENSE
2026 : 15 juni, 28 sep., 7 dec.