Publicatiedatum : 15/03/2024

Opleiding : Forensische analyse

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

4,8 / 5

Het uitvoeren van een post-mortem analyse (ook bekend als inforensic) van IT-beveiligingsincidenten is essentieel geworden voor het bewaren van bewijs. Na gesimuleerde aanvallen leert u hoe u bewijs verzamelt en bewaart, analyseert en de IS-beveiliging verbetert na de inbraak.

Pedagogische doelstellingen

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

- De juiste reflexen onder de knie krijgen bij een inbraak op een machine
- Verzamelen en bewaren van de integriteit van elektronisch bewijsmateriaal
- Analyse na de inbraak

Doelgroep

Systeem- en netwerkingenieur/beheerder.

Voorafgaande vereisten

Goede kennis van IT-beveiliging en netwerken/systemen. Moet de cursus "Logs verzamelen en analyseren, de beveiliging van uw IS optimaliseren" hebben gevolgd.

Opleidingsprogramma

1 Hoe ga je om met een incident?

- De tekenen van een succesvolle IS-inbraak.
- Wat hebben de hackers bereikt? Hoe ver zijn ze gekomen?
- Hoe reageer je op een succesvolle inbraak?
- Welke servers worden beïnvloed?
- Zoek het ingangspunt en vul het.
- De Unix/Windows gereedschapskist voor het vinden van bewijs.
- Opschonen en terugbrengen naar productie van gecompromitteerde servers.

DEELNEMERS

Systeem- en netwerkingenieur/beheerder.

VOORAFGAANDE VEREISTEN

Goede kennis van IT-beveiliging en netwerken/systemen. Moet de cursus "Logs verzamelen en analyseren, de beveiliging van uw IS optimaliseren" hebben gevolgd.

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 Incidenten analyseren voor betere bescherming: Forensische analyse

- Forensisch computeronderzoek: soorten computercriminaliteit, rol van de computeronderzoeker.
- Moderne cybercriminaliteit.
- Digitaal bewijs.

3 Forensische analyse van een Windows-besturingssysteem

- Verwerving, analyse en reactie.
- Inzicht in opstartprocessen.
- Vluchtige en niet-vluchtige gegevens verzamelen.
- Hoe het wachtwoordsysteem en het Windows-register werken.
- Analyse van gegevens in RAM- en Windows-bestanden.
- Analyse van cache-, cookie- en browsegeschiedenis, gebeurtenisgeschiedenis.

Praktisch werk

Gebruikersinjectie. Wachtwoord kraken. RAM-gegevens verzamelen en analyseren. Alle bestanden doorzoeken en hashen. Browser- en registergegevens onderzoeken.

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 : 8 juni, 16 sep., 12 okt., 23 nov.

PARIS LA DÉFENSE
2026 : 8 juni, 16 sep., 12 okt., 23 nov.