Publicatiedatum : 10/01/2024

Opleiding : Forensische analyse en reactie op beveiligingsincidenten

Praktijkcursus - 4d - 28u00 - Ref. AFR
Prijs : 2480 € V.B.

4 / 5

Deze geavanceerde Forensische cursus toont je de essentiële technieken voor het uitvoeren van een analyse na het optreden van IT-beveiligingsincidenten. Aan de hand van een aantal simulaties leer je hoe je bewijs kunt verzamelen, analyseren en vooral bewaren, om zo de IS-beveiliging te verbeteren.

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
- De beveiliging verbeteren na een inbraak

Doelgroep

Systeem- en netwerkingenieurs/beheerders, beveiligingsmanagers.

Voorafgaande vereisten

Goede kennis van IT-beveiliging en netwerken/systemen.

Praktische modaliteiten

Praktisch werk

Onderzoek van alle soorten sporen, massageheugen, verzameling, analyse, verbetering van de algemene beveiliging (implementatie van tegenmaatregelen).

Opleidingsprogramma

1 Forensische analyse van systemen

- Forensisch computeronderzoek. Soorten computercriminaliteit.
- Rol van de IT-onderzoeker.

DEELNEMERS

Systeem- en netwerkingenieurs/beheerders, beveiligingsmanagers.

VOORAFGAANDE VEREISTEN

Goede kennis van IT-beveiliging en netwerken/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.
- Netwerkaanvallen analyseren en begrijpen.
- Netwerkintrusiedetectie.
- Beschermingsmiddelen, Franse wetgeving.

Praktisch werk
Analyseren van netwerklogs van een Volumetrische DDoS, ARP. Implementatie van SNORT.

3 Informatie verzamelen

- Heterogeniteit van bronnen. Wat is een veiligheidsgebeurtenis?
- Security Event Information Management (SIEM), gebeurtenissen verzameld uit de IS.
- Systeemlogs van apparatuur (firewalls, routers, servers, databases).

Praktisch werk
Geolocatie van adressen. Analyse van de geschiedenis van webgebruikers (cookie, POST-verzonden gegevens). Analyse van SQL-injectie weblogs en implementatie van tegenmaatregelen.

4 Logboekanalyse

- Tracks visualiseren, sorteren en doorzoeken.
- Splunk om aanvallen te begrijpen.

Praktisch werk
Splunk installeren en configureren. Weblogs van een Brute-Force on Form analyseren, tegenmaatregelen implementeren.

5 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 integriteit. Verwijderde en/of verborgen bestanden herstellen. Digitale gegevens analyseren.

6 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 : 24 maa., 2 juni, 15 sep., 17 nov.

PARIS LA DÉFENSE
2026 : 24 maa., 2 juni, 15 sep., 17 nov.