Publicatiedatum : 13/02/2025

Opleiding : CTI (Cyber Threat Intelligence), niveau 1

Praktijkcursus - 3d - 21u00 - Ref. CYI
Prijs : 2210 € V.B.

4,6 / 5

NEW

Deze praktische training biedt cyberbeveiligingsprofessionals een uitgebreide inleiding tot de grondbeginselen van informatie over bedreigingen. De cursus behandelt de belangrijkste concepten, methodologieën voor het verzamelen en analyseren van bedreigingen en het gebruik van geschikte tools.

Pedagogische doelstellingen

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

- De fundamentele concepten van Cyber Threat Intelligence en de rol ervan in cyberbeveiliging begrijpen
- Inlichtingenbronnen identificeren en technieken voor het verzamelen van bedreigingen beheersen
- Tools voor informatie over bedreigingen gebruiken om aanvallen beter op te sporen en te voorkomen

Doelgroep

Beveiligingsmanagers en -architecten. Systeem- en netwerktechnici en -beheerders, auditors en pentesters.

Voorafgaande vereisten

Goede kennis van TCP/IP en bedrijfsnetwerkbeveiliging. Of kennis die gelijkwaardig is aan die van de cursus "Systeem- en netwerkbeveiliging, niveau 1" (ref. FRW).

Praktische modaliteiten

Praktisch werk

De deelnemers zullen een breed scala aan tools inzetten.

Opleidingsprogramma

DEELNEMERS

Beveiligingsmanagers en -architecten. Systeem- en netwerktechnici en -beheerders, auditors en pentesters.

VOORAFGAANDE VEREISTEN

Goede kennis van TCP/IP en bedrijfsnetwerkbeveiliging. Of kennis die gelijkwaardig is aan die van de cursus "Systeem- en netwerkbeveiliging, niveau 1" (ref. FRW).

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 OSINT en CTI

- Principe van onderzoek en open bron (OSINT).
- Soorten bronnen: media, sociale netwerken, online databases, enz.
- Onderzoeksethiek: respect voor privacy, mensenrechten en de rechtsstaat.
- Inleiding tot de basisprincipes van CTI (Cyber Threat Intelligence).
- Nomenclatuur die wordt gebruikt op het gebied van CTI.
- Technieken, tactieken, procedures en huidige infrastructuren (TTP, ATP, IOC...).
- APT (Advanced Persistent Threat) vs OPSEC (Operationele Beveiliging).
- Gebruik van tools zoals OTX AlienVault, Kaspersky Threat Data Feeds, Shodan, enz.

2 CTI-tools en -technieken

- Tools voor het verzamelen en analyseren van bedreigingen (MISP, OpenCTI, VirusTotal, enz.).
- Methodologie voor het onderzoeken van cyberbedreigingen.
- Identificatie en analyse van compromisindicatoren (IOC's).
- Tactieken, technieken en procedures (TTP) voor aanvallers met MITRE.
- Bedreigingsdetectie en -preventie via CTI.
- Gebruik van MISP voor IOC-beheer.

3 MISP, OpenCTI

- MISP en de functies ervan.
- OpenCTI en de functies ervan.
- Platformconfiguratie en gewenning.
- Bedreigingsbeheer met MISP en OpenCTI.

4 Intelligentie gebruiken en communiceren

- Gegevens omzetten in bruikbare informatie.
- Delen en uitwisselen van informatie (STIX/TAXII-normen).
- Een CTI-inlichtingenrapport opstellen.
- Reactie op een aanval met CTI.

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 : 25 maa., 17 juni, 28 sep., 14 dec.

PARIS LA DÉFENSE
2026 : 18 maa., 10 juni, 21 sep., 14 dec.