Publicatiedatum : 13/02/2025

Opleiding : CTI (Cyber Threat Intelligence), niveau 2

Praktijkcursus - 3d - 21u00 - Ref. CYJ
Prijs : 2460 € V.B.

NEW

Dit geavanceerde trainingsprogramma in Cyber Threat Intelligence (CTI) is gericht op het verdiepen van de kennis van cyberbeveiligingsprofessionals die zich geavanceerde analysemethoden voor cyberbedreigingen eigen willen maken (technieken voor het verzamelen, correleren en exploiteren van bedreigingsinformatie).

Pedagogische doelstellingen

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

- Analyseer en correleer compromisindicatoren (IOC's) en tactieken, technieken en procedures (TTP's).
- OpenCTI ontwikkelen om CTI-workflows te optimaliseren
- STIX en TAXII gebruiken om informatie over bedreigingen weer te geven
- Geavanceerde technieken beheersen voor het verzamelen en evalueren van inlichtingen over cyberbedreigingen

Doelgroep

Beveiligingsmanagers en -architecten. Systeem- en netwerktechnici en -beheerders, CTI-analisten, SOC-experts, auditors en pentesters.

Voorafgaande vereisten

Kennis die gelijkwaardig is aan die van de cursus "CTI (Cyber Threat Intelligence), niveau 1" (ref. CYI).

Praktische modaliteiten

Praktisch werk

De deelnemers zullen een breed scala aan tools inzetten.

Opleidingsprogramma

DEELNEMERS

Beveiligingsmanagers en -architecten. Systeem- en netwerktechnici en -beheerders, CTI-analisten, SOC-experts, auditors en pentesters.

VOORAFGAANDE VEREISTEN

Kennis die gelijkwaardig is aan die van de cursus "CTI (Cyber Threat Intelligence), niveau 1" (ref. CYI).

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 Inlichtingen over cyberbedreigingen (CTI)

- Een herinnering aan de basisprincipes van CTI.
- Intelligentiemodellen voor cyberbeveiliging (Pyramid of Pain, Diamond Model, Cyber Kill Chain, ATT&CK Framework).
- Geavanceerde analyse van een aanvalscampagne.

2 Bedreigingsanalyse en correlatie

- Technieken voor diepgaande analyse van cyberbedreigingen.
- Geavanceerd gebruik van CTI-tools (MISP, OpenCTI, Threat Intelligence Platforms).
- Onderzoek naar een APT-groep.
- Methodologie voor het correleren en contextualiseren van IOC's en TTP's.
- Ontwikkeling van bruikbare bedreigingsindicatoren.

3 Inlichtingen benutten en integreren in operaties

- Integratie van CTI-inlichtingen in SOC's en CSIRT's.
- Automatisering en orkestratie van CTI-intelligentie.
- Reactie op incidenten op basis van CTI-gegevens.
- Communicatiestrategieën en het delen van informatie (STIX/TAXII, ISAC's).
- Crisismanagement en besluitvorming.

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 : 18 maa., 10 juni, 21 sep., 14 dec.

PARIS LA DÉFENSE
2026 : 11 maa., 3 juni, 14 sep., 7 dec.