

Opleiding : Cyberbeveiliging en nieuwe technologieën, geavanceerde training

Praktijkcursus - 3d - 21u00 - Ref. NYP

Prijs : 2100 € V.B.

Je hebt kennis gemaakt met kwetsbaarheden in gegevens in zowel de big data-wereld als embedded systemen. Wij bieden je de mogelijkheid om je kennis te verdiepen, de beveiliging van blockchain, de cloud en bepaalde gevoelige systemen te analyseren en een beter begrip te krijgen van cyberbeveiliging als geheel.

Pedagogische doelstellingen

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

- ✓ Maîtriser les enjeux de la cybersécurité des nouvelles technologies
- ✓ Leer over best practices in cyberbeveiliging toegepast op nieuwe technologieën
- ✓ De bedreigingen voor blockchain begrijpen
- ✓ Inzicht in de bedreigingen voor de cloud en big data

Doelgroep

Beveiligingsmanagers en -architecten. Systeem- en netwerktechnici en -beheerders.

Voorafgaande vereisten

Kennis van netwerken en systemen. Je moet de training "Cybersecurity en nieuwe technologieën, introductie" hebben afgerond of een gelijkwaardig niveau hebben.

Praktische modaliteiten

Oefening

Elk nieuw theoretisch concept wordt gevolgd door een praktische toepassing.

Leer methodes

Actief onderwijs, presentaties, groepsdiscussies, interactieve uitwisselingen.

Opleidingsprogramma

DEELNEMERS

Beveiligingsmanagers en -architecten. Systeem- en netwerktechnici en -beheerders.

VOORAFGAANDE VEREISTEN

Kennis van netwerken en systemen.

Je moet de training "Cybersecurity en nieuwe technologieën, introductie" hebben afgerond of een gelijkwaardig niveau hebben.

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 Herinneringen aan cryptologie, de historische blockchain

- Basiscryptologie voor blockchain.
- Verschillende hashing-algoritmen.
- De historische blockchain: bitcoin.
- Consensus door mijnbouw.
- Bitcoin in cijfers en afbeeldingen.

Workshop storytelling

Cryptologie en blockchain.

2 Aanvallen en verdediging in blockchain

- Sécurité blockchain vs cloud.
- Blockchain- en IoT-beveiliging (Internet of Things).
- Blockchain et vérification d'identité. Blockchain et supply chain.
- Veelvoorkomende kwetsbaarheden.
- Solidity, le langage des smart contracts.
- Hyperledger, la plateforme open source de développement de blockchain.
- De veiligheid van smart contract ontwikkelingen (taal, methodologie, verificatie).
- Best practices voor het beveiligen van blockchain.

Praktisch werk

Veiligheid analyseren.

3 De "blockchain" Hyperledger

- Principes en terminologie.
- Verschillende soorten knooppunten.
- Servicearchitectuur.
- Vertrouwelijkheid van de operator.
- De basis van Go, de taal van slimme contracten.

Praktisch werk

Bouw van een blockchain en eerste Go-tests.

4 Bedreigingen voor cloud computing

- Risicobeoordeling en -beheer in de cloud met behulp van de ISO 27005-norm.
- De bijzonderheden van risicobeheer in de cloud.
- De belangrijkste risico's die door ENISA zijn geïdentificeerd.
- Beveiligingsanalyse begrijpen.
- Beveiligingstools voor de cloud.

Praktisch werk

Beveiligingsanalyse op Amazon Web Services EC2.

5 Bedreigingen voor big data

- Opslagoplossingen: HDFS, NoSQL databases, Hadoop, HBase, MongoDB, enz.
- De gebruikte architecturen.
- Les différentes vulnérabilités.

Workshop storytelling

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.

6 Kwetsbaarheden van het systeem

- Botnets: hoe ontstaan ze?
- Kwetsbaarheden in domotica: bewakingscamera's, alarmen, tv's, aangesloten sloten, enz.
- Kwetsbaarheden en aanvallen op WiFi-netwerken.
- Malware-aanvallen gericht op pc's, tablets en smartphones: drive-by download...
- Beste praktijken voor het beveiligen van deze systemen.

Praktisch werk

Veiligheid analyseren.

Data en plaats

KLAS OP AFSTAND

2026 : 20 mei, 5 okt., 16 dec.

PARIS LA DÉFENSE

2026 : 20 mei, 5 okt., 16 dec.