

# Cyberbeveiliging e-learning kanaal

**Praktijkcursus - 1d - 07h23 - Ref. 8CY**

**Prijs : 190 € V.B.**

Bestrijd cyberbedreigingen met ons gespecialiseerde cyberbeveiligingskanaal. Kom meer te weten over methoden voor gegevensbescherming, technieken om aanvallen te voorkomen en strategieën om kwetsbaarheden in uw digitale infrastructuur tegen te gaan. Bent u klaar om een cyberbeveiligingsdeskundige te worden?

## Pedagogische doelstellingen

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

- ✓ Bekend zijn met informatiebeveiligingsmaatregelen.
- ✓ Het IS-beveiligingsbeleid van het bedrijf promoten.
- ✓ De risico's van het gebruik van digitale hulpmiddelen identificeren.
- ✓ Je werkstation beveiligen.
- ✓ Implementeer versleuteling met BitLocker.
- ✓ Groepsstrategieën opzetten.
- ✓ Beheer het ophalen van de BitLocker herstelsleutel in Active Directory en Azure Active Directory.
- ✓ Installeer en gebruik de Kali Linux-distributie.
- ✓ Kwetsbaarheden analyseren met Nessus.
- ✓ Test je netwerk met Macchanger of Macof.
- ✓ Het concept van Man in the Middle begrijpen, evenals tools voor brute force aanvallen.
- ✓ De beveiliging van een WiFi-netwerk beheren.
- ✓ Een PKI-oplossing implementeren binnen het bedrijf.
- ✓ PKI begrijpen.
- ✓ De concepten van cryptografie kennen.
- ✓ Symmetrische en asymmetrische encryptie begrijpen.
- ✓ Gebruik certificaten en certificaatsjablonen.

## Doelgroep

Systeem- en netwerkbeheerders en iedereen die verantwoordelijk is voor IT-beveiliging in een bedrijf.

### DEELNEMERS

Systeem- en netwerkbeheerders en iedereen die verantwoordelijk is voor IT-beveiliging in een bedrijf.

### VOORAFGAANDE VEREISTEN

Kennis van het gebruik van Linux en Windows.

### 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 vak kennis 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.

## Voorafgaande vereisten

Kennis van het gebruik van Linux en Windows.

## Praktische modaliteiten

### Digitale activiteiten

De IT-structuur: opgenomen cursussen, video's van experts en het delen van best practices.

### Mentorschap

L'option tutorat propose un accompagnement personnalisé par un formateur référent ORSYS, expert du domaine. Adapté aux besoins, aux capacités et au rythme de chaque apprenant, ce tutorat combine un suivi asynchrone (corrections personnalisées d'exercices, échanges illimités par message...) et des échanges synchrones individuels. Bénéfice : une meilleure compréhension, le développement des compétences et un engagement durable dans la formation.

### Pedagogiek en praktijk

Een breed scala aan inhoud, geproduceerd door trainers met een rigoureuze onderwijsaanpak. Tijdens elke cursus worden operationele cases becommentarieerd door experts om leerlingen te helpen het geleerde in praktijk te brengen. Om leerlingen te helpen onthouden wat ze hebben geleerd, is elke les opgedeeld in korte sessies van 3 tot 10 minuten. Dit stelt elke cursist in staat om dynamisch en zelfstandig te leren.

## Opleidingsprogramma

### 1 BitLocker, desktopversleuteling implementeren en beheren in de onderneming

- Ontdek de BitLocker-functionaliteit.
- Encryptie instellen met BitLocker.

### 2 Kali Linux, begin met het analyseren van de beveiliging van uw infrastructuur

- Ontdek Kali Linux.
- Installatie van Kali Linux.
- Kali Linux configureren.
- Kwetsbaarheden ontdekken.
- Nessus installeren en gebruiken.
- Kali Linux en het netwerk onder de knie krijgen.
- Gebruik van netwerktools.
- Brute force aanvallen ontdekken met Kali Linux.
- Gebruik van tools voor brute force-aanvallen.
- WiFi-beveiligingsbeheer.

### 3 PKI, implementeren en gebruiken van een publieke sleutelinfrastructuur in een Windows-omgeving

- Inleiding tot PKI: cryptografie.
- Certificaten in een publieke sleutelinfrastructuur.
- Implementatie van een PKI.
- Certificaatmodellen in een publieke sleutelinfrastructuur.

## 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.