Publicatiedatum : 01/10/2024

Opleiding : NIS 2-richtlijn Hoofduitvoerder, PECB-certificering

Praktijkcursus - 5d - 35u00 - Ref. NI2
Prijs : 3270 € V.B.

4,3 / 5

Cette formation vous permettra d'acquérir une connaissance approfondie des exigences de la directive NIS 2, des stratégies de mise en œuvre et des bonnes pratiques qui protègent les infrastructures critiques contre les cybermenaces. Vous apprendrez à évaluer les risques de cybersécurité d'un organisme, à élaborer des plans robustes de réponse aux incidents et à mettre en œuvre des mesures de sécurité efficaces pour répondre aux exigences de la directive NIS 2.

Pedagogische doelstellingen

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

- De basisbegrippen van de NIS 2-richtlijn en de bijbehorende vereisten uitleggen.
- Inzicht in de principes, strategieën en tools die nodig zijn om een cyberbeveiligingsprogramma te implementeren
- De vereisten van de NIS 2-richtlijn interpreteren en implementeren in de specifieke context van een organisatie.
- De implementatie van de vereisten van de NIS 2-richtlijn initiëren en plannen met behulp van de PECB-methodologie.
- Een cyberbeveiligingsprogramma plannen, implementeren, bewaken en onderhouden in overeenstemming met de NIS 2-richtlijn.

Doelgroep

Cyberbeveiligingsprofessionals, IT-managers die kennis willen opdoen over het implementeren van veilige systemen, overheidsfunctionarissen en regelgevende instanties

Voorafgaande vereisten

Een fundamenteel begrip hebben van cyberbeveiliging.

DEELNEMERS

Cyberbeveiligingsprofessionals, IT-managers die kennis willen opdoen over het implementeren van veilige systemen, overheidsfunctionarissen en regelgevende instanties

VOORAFGAANDE VEREISTEN

Een fundamenteel begrip hebben van cyberbeveiliging.

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.

Certificatie

Overgang naar certificaties op afstand

Raadpleeg de officiële documentatie van de certificerende instantie om de voorafgaande vereisten voor het afleggen van het online certificatie-examen te raadplegen.

Opleidingsprogramma

1 Inleiding tot de NIS 2-richtlijn en start van de implementatie ervan

- Inleiding tot de NIS 2-richtlijn en start van de implementatie ervan
- Normen en regelgevende kaders.
- NIS 2-richtlijn.
- Vereisten van de NIS 2-richtlijn.
- Start van de implementatie van de NIS 2-richtlijn.
- De organisatie en haar context.

2 Analyse van het NIS 2-nalevingsprogramma, activabeheer en risicobeheer

- Cyberbeveiligingsbeheer.
- Rollen en verantwoordelijkheden op het gebied van cyberbeveiliging.
- Vermogensbeheer.
- Risicobeheer.

3 Cyberbeveiligingscontroles, incidentbeheer en crisisbeheer

- Cyberbeveiligingscontroles.
- Veiligheid van de toeleveringsketen.
- Incidentbeheer.
- Crisisbeheer.

4 Communiceren, testen, bewaken en continu verbeteren van cyberbeveiliging

- Bedrijfscontinuïteit.
- Bewustmaking en training.
- Communicatie.
- Cyberbeveiliging testen.
- Interne audit.
- Prestaties en indicatoren meten, controleren en erover rapporteren.
- Voortdurende verbetering.

5 Certificering

- Competentiegebieden waarop het examen betrekking heeft :
- Gebied 1: Basisbegrippen en definities van de NIS 2-richtlijn.
- Gebied 2: Planning van de implementatie van de vereisten van de NIS 2-richtlijn.
- Gebied 3: rollen en verantwoordelijkheden op het gebied van cyberbeveiliging en risicobeheer.
- Gebied 4: Cyberbeveiligingscontroles, incidentbeheer en crisisbeheer.
- Gebied 5: communicatie en bewustmaking.
- Gebied 6: Testen en monitoren van een cyberbeveiligingsprogramma.

Data en plaats

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.

KLAS OP AFSTAND
2026 : 16 maa., 29 juni, 12 okt., 7 dec.

PARIS LA DÉFENSE
2026 : 9 maa., 22 juni, 5 okt., 14 dec.