

CISSO, Certified Information Systems Security Officer, certificering

Praktijkcursus van 5 dagen - 35u

Ref : CEF - Prijs 2024 : € 4 590 excl. BTW

Deze opleiding is bedoeld om kandidaten voor te bereiden op het CISSO-examen, het internationaal certificaat dat wordt uitgereikt door MILE2. De opleiding omvat alle kennis over informatiebeveiliging, verdeeld over 19 gebieden. Ze is afgestemd op de doelstellingen van de belangrijkste ISO 27001-, NIST-, CISM- en CISSP-normen.

PEDAGOGISCHE DOELSTELLINGEN

Na afloop van de opleiding kan de cursist:

De kennis in de 19 gebieden van de gemeenschappelijke basisinhoud verwerven, die nodig is om voor de CISSO- en CISSP-examens te slagen

De kennis verwerven om een organisatie te adviseren over best practices op het gebied van ISS-beheer

PEDAGOGISCHE METHODEN

Een reeks uiteenzettingen over alle gebieden van het examenprogramma. Een reeks vragen/antwoorden op het einde van elk gebied. Ondersteuning en opleiding in het Frans.

CERTIFICERING

Online certificeringsexamen op de website van MILE2 (duurt 2 uur/100 vragen). Vereiste om te slagen: ten minste 70% juiste antwoorden.

HET PROGRAMMA

laatste update: 10/2021

1) Risico- en veiligheidsbeheer, IAM en toegangscontrole

- Risk Management: risicobeheer, evaluaties en antwoorden.
- Security Management: ISMS, rollen en verantwoordelijkheden, frameworks, human resources.
- Identification and Authentication: identity Management, authenticatie, Access Control Monitoring.
- Access Control: soorten toegangscontroles, classificatie-informatie, toegangscontrolemodellen en methoden.

2) Beveiligingsactiviteiten en cryptografie

- Security Models and Evaluation Criteria: beschermingsmechanisme, beveiligingsmodellen.
- Operations Security: operationele incidenten en bedreigingen, verantwoordelijkheden.
- Sym. Cryptography and Hashing: definitie, geschiedenis, grondbeginselen van cryptografie, symmetrische algoritmen.
- Asym. Cryptography and PKI: hybride cryptografie en digitale handtekening, PKI, doeleinden, cryptografische aanvallen.

3) Netwerk- en communicatiebeveiliging, beveiligingsarchitectuur

- Network connections: netwerk- en communicatiebeveiliging, topologieën, netwerktransmissies, bekabeling, LAN/WAN.
- Network Protocols and Devices: OSI-model, protocollen, poorten en services.
- Telephony, VPNs and Wireless: telefonie, VPN's, wifi, netwerkgebaseerde aanvallen.
- Security Architecture and Attacks: architectuurmodellen, systeemaanvallen.

DEELNEMERS

IS-afdelingen, ingenieurs en projectleiders, deskundige beveiligingsconsultants, beveiligingsmanagers, auditors.

VOORAFGAANDE VEREISTEN

Ervaring op het gebied van netwerken, systemen en beveiliging. Technisch Engels begrijpen.

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.

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.

4) Softwareontwikkelingsbeveiliging, databasebeveiliging, malware

- Soft Development Security: softwareontwikkelingsproces, webbeveiliging, PCI-DSS-conformiteit.
- DB Security and System Development: modellen en terminologieën, databasebeveiliging.
- Malware and Software Attacks: virus, Worm, Logic Bomb, Trojan Horse, Timing Attack, Spyware.

5) BCP & DRP, beveiligingsincidenten, wetten en ethiek, fysieke beveiliging

- BCP & DRP: BIA, strategieën, ontwikkelingsplan, test.
- Incident Management, Law and Ethics: Computer Crime, bewijsmateriaalbeheer, ethiek en vertrouwelijkheid.
- Physical Security: ruimten en constructie van gebouwen, perimeterbeveiliging, bedreigingen inzake elektriciteit en brand.

Het CISSO-certificeringsexamen afleggen.

DATA

Neem contact met ons op