Publicatiedatum : 24/02/2026

Opleiding : CISO (Information System Security Manager), niveau 1

Synthese cursus - 4d - 28u00 - Ref. RSD
Prijs : 2670 € V.B.

NEW

De CISO-training bereidt professionals voor op het beheren van de beveiliging van informatiesystemen, door technische vaardigheden te behandelen (regelgevend kader, technische oplossingen, enz.).

Pedagogische doelstellingen

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

- Het beveiligingsbeheerproces onder de knie krijgen
- Als CISO de zakelijke referentiekaders en bijbehorende normen uit de ISO 27K-serie gebruiken
- Het Franse en Europese wettelijke kader kennen (LPM, NIS, RGPD...)
- Een actieplan opstellen om de doelstellingen van het veiligheidsbeleid te bereiken
- Een passende, evenredige reactie ontwikkelen en cyberrisico's beperken, inclusief de bijbehorende technische maatregelen
- Inzicht in IS-processen voor beveiligingstoezicht

Doelgroep

Engineers die de rol van CISO op zich nemen, IT-directeuren of -managers, beveiligingsengineers of -correspondenten, projectmanagers die beveiligingsbeperkingen integreren.

Voorafgaande vereisten

Geen speciale kennis vereist.

Opleidingsprogramma

DEELNEMERS

Engineers die de rol van CISO op zich nemen, IT-directeuren of -managers, beveiligingsengineers of -correspondenten, projectmanagers die beveiligingsbeperkingen integreren.

VOORAFGAANDE VEREISTEN

Geen speciale kennis vereist.

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 De grondbeginselen van de beveiliging van informatiesystemen

- Beveiligingsprincipes: verdediging in de diepte, cyberrisicomodellering.
- DICT/P-classificatie: Beschikbaarheid, Integriteit, Vertrouwelijkheid en Traceerbaarheid/bewijs.
- De opkomst van cyberrisico, de evolutie van cybercriminaliteit.
- Hoe een cyberaanval werkt (Kill Chain).
- Belangrijke externe informatiebronnen (ANSSI, CLUSIF, ENISA, enz.).
- Beveiligingsdoelstellingen: vertrouwelijkheid, beschikbaarheid, gegevensintegriteit en traceerbaarheid.

2 De SSI-taakgroep: meerdere bedrijfsprofielen

- De rol en verantwoordelijkheden van de CISO en de relatie met de IT-afdeling.
- Naar een gestructureerde en beschreven veiligheidsorganisatie, waarbij vaardigheden worden geïdentificeerd.
- De rol van asset owners en de behoefte aan betrokkenheid van het management.
- Profielen van architecten, integrators, auditors, pentesters, toezichthouders, risicomanagers, enz.
- Een team samenstellen dat bekwaam en getraind is en reageert op ontwikkelingen in cyberspace.

3 Normen en voorschriften

- Het integreren van zakelijke, wettelijke en contractuele vereisten. De compliance-aanpak.
- Beveiligingsgebieden: van beleid tot compliance en IT-beveiliging.
- Een voorbeeld van wettelijke regelgeving: NIS-richtlijn/ Militaire planningswet.
- RGPD en de rol van de CISO.
- De 4 pijlers van veiligheid zoals gezien door Europa en ANSSI: Bestuur, Bescherming, Defensie en Veerkracht.
- ISO 27001 in een managementsysteembenadering (Deming/PDCA-wiel).
- ISO 27002 universele goede praktijk, de minimale essentiële kennis.
- Opstellen van een veiligheidsplan voor relaties met klanten/leveranciers.
- Cyberbeheer: ISO-conform dashboard.

4 Het risicoanalyseproces

- Risicoanalyse integreren in het proces van beveiligingsbeheer.
- Identificatie en classificatie van risico's, ongevallenrisico's en cyberrisico's.
- De ISO 27005-normen en de relatie tussen het risicoproces en het ISO 27001 ISMS.
- Van risicobeoordeling tot risicobehandelingsplan: de juiste activiteiten in het proces.
- Bekendheid met vooraf gedefinieerde methoden: FR/EBIOS RM-benadering, US/NIST-benadering, enz.

5 Bewustmaking van gebruikers

- Veiligheidsbewustzijn: Wie? Wie? Wat? Hoe?
- De behoefte aan geprogrammeerde en gebudgetteerde bewustmaking.
- De verschillende vormen van bewustmaking: face-to-face of virtueel?
- Het veiligheidshandvest, het juridische bestaan, de inhoud en de sancties.
- Quizzen en serious games, zoals de ANSSI MOOC.

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 Optimale technische oplossingen ontwerpen - Gegevensbeveiliging

- Cryptografische technieken.
- Openbare sleutel en symmetrische algoritmen.
- Eenvoudige, zout en sleutel (HMAC) hashfuncties.
- Publieke sleutelarchitecturen (PKI).
- Toepassing van cryptografie: TLS-uitwisselingen, beveiliging van gegevens in rust, enz.
- Back-upstrategie (BCP, DRP, enz.).

7 Verificatie en autorisatie van gebruikers

- IAM, een grote uitdaging.
- Biometrische authenticatie en de juridische aspecten.
- Authenticatietechnieken (wachtwoorden, certificaten, UAF- en U2F-standaarden van de FIDO-alliantie (Fast ID Online)).
- De verschillende aanvalstechnieken (brute kracht, keylogger, credential stuffing, etc.).
- Sterke en multi-factor authenticatie (MFA).
- OATH's HOTP- en TOTP-normen.

8 Optimale technische oplossingen ontwerpen - Netwerkbeveiliging

- Partitioneren van gevoelige netwerken, netwerk- en applicatiefirewalltechnologieën.
- LAN-beveiliging: Vlans, NAC ...
- Verschillen tussen UTM, enterprise, NG en NG-v2 firewalls.
- De risico's van Cloud Computing volgens CESIN, ENISA en CSA.
- De cloudcontrolematrix en het gebruik ervan bij het evalueren van cloudaanbieders.
- CASB-oplossingen voor het beveiligen van gegevens en toepassingen in de cloud.
- Beheer netwerkbeveiliging: SSH, bastion, partitionering en best practice.
- Risico's van draadloze netwerken en best practices.
- VPN-oplossingen.

9 Optimale technische oplossingen ontwerpen - Beveiliging van werkstations en servers

- Bedreigingen van endpoints begrijpen.
- Anti-virus/anti-spyware software.
- Kwaadaardige software: payloads (ransomware, exploits), verspreiding (drive-by downloads, kwaadaardige USB-sticks).
- Principe van uitharding.
- Hoe beveilig je verwijderbare apparaten?
- Kwetsbaarheden en best practices voor virtuele architectuur.
- Beveiliging van smartphones en best practices.

10 Actief veiligheidsmanagement en toezicht

- Auditcategorieën, van organisatorische audits tot penetratietests.
- Inbraaktests (black box, gray box en white box).
- Hoe kwalificeer je je auditors? - Voorbeeld met PASSI in Frankrijk.
- Toezichtstrategie: logboek, IPS (Intrusion Prevention System) en IPS NG.
- Een SIEM-oplossing implementeren.
- Het implementeren of uitbesteden van uw Security Operation Centre (SOC).
- Procedures voor incidentenrespons en crisisbeheer.

Data en plaats

KLAS OP AFSTAND
2026 : 26 mei, 8 sep., 24 nov.

PARIS LA DÉFENSE
2026 : 19 mei, 1 sep., 17 nov.