Publicatiedatum : 18/04/2024

Opleiding : Cybersecurity-referentiekaders en normen: begrijpen, vergelijken en effectief kiezen

NIS 2, NIST CSF 2, ISO 27001:2022, PCI DSS, SecNumCloud...

seminarie - 2d - 14u00 - Ref. NST

Prijs : 1850 € V.B.

4,5 / 5

De strijd tegen cybercriminaliteit, een essentieel onderdeel van het beheer van informatiebeveiliging, heeft geleid tot een explosie in de publicatie van richtlijnen en vereisten voor best practices. Geconfronteerd met deze veelheid aan hulpmiddelen, is het doel van dit seminar om een breed overzicht te geven van de beschikbare normen, en om hun reikwijdte en specificiteit te verduidelijken om de keuze van degenen die verantwoordelijk zijn voor cyberbeveiliging te begeleiden. U zult zien welke vragen u zichzelf moet stellen als u keuzes maakt en het hoofd moet bieden aan de groeiende cyberdreiging.

Pedagogische doelstellingen

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

- Inzicht in cyberrisicoproblemen en reacties Stand van zaken
- Bekend zijn met de belangrijkste internationale cyberbeveiligingsnormen
- Een beveiligingsraamwerk integreren in de beste IT-praktijken
- Leren over de implementatie en inzet van repositories aan de hand van casestudies
- Vergelijk en kies de meest effectieve manier om uw veiligheidsdoelstellingen te bereiken
- Inzicht in de certificerings-/conformiteits- en goedkeuringsprocessen
- De implementatiekosten evalueren als onderdeel van een algeheel informatiesysteem

Doelgroep

CISO's of beveiligingscorrespondenten, beveiligingsarchitecten, IT-directeuren of -managers, ingenieurs, projectmanagers, auditors die beveiligingseisen moeten integreren.

DEELNEMERS

CISO's of beveiligingscorrespondenten, beveiligingsarchitecten, IT-directeuren of -managers, ingenieurs, projectmanagers, auditors die beveiligingseisen moeten integreren.

VOORAFGAANDE VEREISTEN

Basiskennis van cyberbeveiliging, of kennis die gelijkwaardig is aan die van de BYR- of SSI-cursussen.

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.

Voorafgaande vereisten

Basiskennis van cyberbeveiliging, of kennis die gelijkwaardig is aan die van de BYR- of SSI-cursussen.

Opleidingsprogramma

1 Het Europese model: Netwerk Informatiebeveiliging 2 (NIS 2)

- Nieuwe Koude Oorlog Oost/West, VS/China West/Rusland.
- Georganiseerde hackers en de rol van inlichtingendiensten.
- APT (Advanced Persistent Threat), ransomware, gerichte risico's.
- Referentiesystemen in kaart brengen: van specialist naar generalist.
- Europese cyberbeveiligingskwesties.
- Toepassingsgebieden EE, EI, OSE, FSN, nieuwe subsidiabiliteitscriteria.
- Voor welke ecosystemen - Nieuwe bedrijfssectoren en ESN/IT ingeschreven.
- De belangrijkste beveiligingsmaatregelen: gebaseerd op de 23 regels van NIS 1 en nog veel meer...
- Het risicobeheer en het gecontroleerde goedkeuringsproces.
- Een systeem van getrapte straffen gebaseerd op omzet, zoals de RGPD.

Casestudy

Een NIS 2-project implementeren, gebaseerd op NIS v1, met als doel certificering.

2 Het Amerikaanse model: NIST CSF 2.0

- De kern met zijn reeks categorieën en subcategorieën.
- De nieuwe GOVERN-functie en de relevantie ervan voor strategisch cyberbeheer.
- Implementatiegidsen voor de 800 en 1800 series ter ondersteuning van het CSF.
- Implementatieniveaus van het kader: niveaus 1 tot 4.
- Leer hoe u uw beveiliging kunt aanpassen aan uw doelstellingen en het kritieke karakter van uw activiteiten.
- Veilige ontwikkeling integreren met het aanvullende SSDF-raamwerk.
- Creëer een profiel op basis van de veiligheidsdoelstellingen van de business lines en de vereisten van belanghebbenden.
- Een profiel opstellen van cyberbedreigingen voor het ecosysteem.

Casestudy

Een governanceprofiel implementeren met het nieuwe NIST CSF 2.0

3 Het universele model ISO 27001:2022

- ISO 27001 in een managementsysteembenadering (Deming/PDCA-wiel).
- ISO risicobeheer: ISO 31000/ISO 27005.
- Het opstellen van het risicobeheerplan en de verklaring van toepasselijkheid.
- De universele goede praktijken van ISO 27002:2022.
- De veiligheidsdomeinen en de kenmerken die bij de 93 maatregelen horen.
- Een documentbeheer- en bewijsbasis opbouwen.
- Inzicht in het ISMS-auditproces (eerste partij en derde partij).

Casestudy

Een continu verbeteringsproces implementeren met ISO 27001.

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 Een IT-cloudmodel van SecNumCloud

- ANSSI's visie op veilig cloudcomputing en de nieuwste ontwikkelingen in 2023.
- De belangrijkste best practices voor het beschermen en verdedigen van vertrouwde hostingservices.
- Een beveiligingslabel dat ISO 27001 en ISO 27017/27018 omvat voor een soevereine cloud.
- Beschermingscriteria met betrekking tot niet-Europese wetten.
- Naar een Europese kwalificatie voor EUCS-leveranciers van cloud computing-diensten?

5 Een model voor de gezondheidszorg: HDS (hosts voor gezondheidszorggegevens)

- De HDS-standaard: ISO 27001 als basis.
- Gezondheidsgegevens: beschermingsvereisten en verband met de RGPD.
- Extra vereisten.
- Kader voor certificering van hostingproviders.

6 Een model voor financiën/betalingen : PCI DSS v4

- De PCI-kaartbetalingsindustrie en haar kaders voor vereisten.
- De belangrijkste spelers in de sector: merken, banken, winkeliers, PSP's.
- Het ecosysteem van PCI-spelers: QSA, ASV, gecertificeerde uitgevers, enz.
- Specifieke cyberbedreigingen voor CB-gegevens: diefstal, skimming.
- Een project leiden tot naleving, eerste stappen met de SAQ.

7 Beveiliging volgens COBIT®, ITIL® en ITIL®.

- COBIT®: een raamwerk voor het afstemmen van IT-governance op bedrijfsdoelstellingen.
- COBIT® risicobeheerprocessen.
- Organisatie- en HR-modellen.
- COBIT® beveiligingsprincipes.
- Veiligheidscontrolesjablonen.
- ITIL®: een raamwerk voor IT-servicelevering.
- ITIL® processen.
- Het informatiebeveiligingsbeheerproces.
- ITIL® en de verbanden met ISO 27001.

8 Welke strategie moet je kiezen?

- Voor- en nadelen van elk van de referentiesystemen.
- Vergelijkingen en selectiecriteria.
- Hybride en aanvullende benaderingen.
- Vergelijkende kosten en multi-referentiële uitlijningen.

Data en plaats

KLAS OP AFSTAND
2026 : 10 juni, 1 okt., 8 dec.

PARIS LA DÉFENSE
2026 : 9 juni, 24 sep., 1 dec.