EBIOS RM, voorbereiding op de certificering

Praktijkcursus van 2 dags - 14h
Ref : EBU - Prijs 2025 : 1 610 excl. BTW

De EBIOS-methode stelt u in staat IS-beveiligingsrisico's te beoordelen en aan te pakken op basis van beproefde ervaring op het gebied van IS-consultancy en ondersteuning voor opdrachtgevers. Deze opleiding zal u alle nodige kennis bijbrengen om deze methode in een reële situatie toe te passen.

PEDAGOGISCHE DOELSTELLINGEN

Na afloop van de opleiding kan de cursist:

De EBIOS-methode begrijpen

De risico's in kaart brengen

De basiselementen van risicobeheer voor informatiebeveiliging onder de knie krijgen met behulp van de EBIOS-methode

Risicobeheer in de praktijk brengen met de EBIOS risk manager-methode

De resultaten van een EBIOS-studie analyseren en meedelen

PEDAGOGISCHE METHODEN

Cursusmateriaal en opleiding in het Frans.

CERTIFICERING

Deze cursus stelt u in combinatie met de cursus EBX (EBIOS RM, certificeringsexamen), op de dag van het examen, in staat om de PECB certified EBIOS risk manager-certificering voor te bereiden en te behalen.

HET PROGRAMMA

laatste update: 01/2024

1) De EBIOS risk manager-methode

- Grondbeginselen van risicobeheer.
- Aandacht voor cyberbeveiliging (prioritaire bedreigingen).
- Voorstelling van EBIOS.
- Belangrijkste definities van EBIOS risk manager.

2) Oriëntering en veiligheidsgrondslag

- Identificatie van de bedrijfs- en technische perimeter.
- Identificatie van gevreesde gebeurtenissen en evaluatie van de ernst ervan.
- De veiligheidsgrondslag identificeren.

De gevreesde gebeurtenissen identificeren.

3) Risicobronnen

- Risicobronnen (RB's) en de beoogde doelstellingen (BD's) ervan identificeren.
- De relevantie van de paren beoordelen.
- De RB-BD-paren beoordelen en de paren selecteren die voor de analyse prioritair worden geacht.
- De ernst van de strategische scenario's beoordelen.

Risicobronnen (RB's) en de beoogde doelstellingen (BD's) ervan identificeren. De RB-BD-paren beoordelen.

4) Strategische scenario's

- Het met de belanghebbenden in verband gebrachte bedreigingsniveau beoordelen.
- Een analyse van de digitale bedreiging van het ecosysteem en de kritieke belanghebbenden maken.
- Ontwikkeling van strategische scenario's.

DEELNEMERS

CISO's of veiligheidscorrespondenten, beveiligingsarchitecten, IT-directeurs of -managers, ingenieurs, projectleiders (aannemer, opdrachtgever) die beveiligingseisen moeten integreren.

VOORAFGAANDE VEREISTEN

Goede kennis van IS-beveiliging en van de 27005-norm.

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.

- Bepaling van veiligheidsmaatregelen voor het ecosysteem.
Het met de belanghebbenden in verband gebrachte bedreigingsniveau beoordelen.
Ontwikkeling van strategische scenario's.

5) Operationele scenario's

- Ontwikkeling van operationele scenario's.
- Evaluatie van waarschijnlijkheden.
- Threat modeling, ATT&CK.
- Common Attack Pattern Enumeration and Classification (CAPEC).
Ontwikkeling van operationele scenario's. Evaluatie van waarschijnlijkheden.

6) Risicobehandeling

- Realisatie van een samenvatting van de risicoscenario's.
- Bepaling van de behandelingsstrategie.
- De beveiligingsmaatregelen in een PACS bepalen.
- Beoordeling en documentatie van restrisico's.
- Implementatie van het kader voor de opvolging van risico’s.
De beveiligingsmaatregelen in een plan voor voortdurende verbetering van de beveiliging (PACS) bepalen. Implementatie van het kader voor de opvolging van risico’s.

DATA

KLAS OP AFSTAND
2025 : 28 juil., 13 oct.

BRUSSEL
2025 : 28 juil., 13 oct.