Publicatiedatum : 15/07/2024

Opleiding : Inleidende cursus cyberbeveiliging

Praktijkcursus - 10d - 70u00 - Ref. BCS
Prijs : 5840 € V.B.

BEST

Na afronding van de cursus zijn studenten in staat om de fundamentele principes, standaarden en tools van IT-beveiliging op een operationele manier toe te passen.

Pedagogische doelstellingen

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

- Een globale visie hebben op cyberbeveiliging en de omgeving (uitdagingen, ecosysteem, enz.)
- Bekend zijn met de verschillende cyberbeveiligingsrichtlijnen, -standaarden en -tools
- Cyberberberoepen begrijpen
- Inzicht in de wettelijke verplichtingen met betrekking tot cyberbeveiliging
- De belangrijkste risico's en bedreigingen begrijpen en weten hoe je je ertegen kunt beschermen
- Goede praktijken in IT-beveiliging identificeren

Doelgroep

Iedereen die de basisprincipes van IT-beveiliging wil leren en/of in cyberbeveiligingsberoepen wil gaan werken (technici, systeem- en netwerkbeheerders).

Voorafgaande vereisten

Algemene kennis van informatiesystemen en bekendheid met de ANSSI-beveiligingshygiënegids.

DEELNEMERS

Iedereen die de basisprincipes van IT-beveiliging wil leren en/of in cyberbeveiligingsberoepen wil gaan werken (technici, systeem- en netwerkbeheerders).

VOORAFGAANDE VEREISTEN

Algemene kennis van informatiesystemen en bekendheid met de ANSSI-beveiligingshygiënegids.

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.

Composition de la formation

Inleiding tot IT-beveiliging

Ref. ISI - 1 dag ★ 4 / 5

De grondbeginselen van IS-beveiliging

Ref. FTS - 3 dagen ★ 4 / 5

Veiligheid in cyberspace

Ref. SCE - 3 dagen ★ 4 / 5

Cyberbeveiliging, het testen van uw omgevingen

Ref. CTE - 3 dagen ★ 3 / 5

Opleidingsprogramma

1 Bedreigingen en risico's

- Wat is IT-beveiliging?
- Hoe kan nalatigheid een ramp veroorzaken?
- Ieders verantwoordelijkheden.
- IS-architectuur en de potentiële kwetsbaarheden ervan.
- Bedrijfsnetwerken (lokaal, extern, internet).
- Draadloze netwerken en mobiliteit. Toepassingen met een hoog risico: web, e-mail, enz.
- De database en het bestandssysteem. Bedreigingen en risico's.
- De sociologie van piraten. Ondergrondse netwerken. Motivaties.

2 Veiligheid op de werkplek

- Vertrouwelijkheid, handtekening en integriteit. Encryptiebeperkingen.
- De verschillende cryptografische elementen. Windows, Linux of MAC OS: wat is het veiligst?
- Beheer van gevoelige gegevens. Laptopproblemen.
- De verschillende bedreigingen voor het clientwerkstation? Kwaadaardige code begrijpen.
- Hoe ga je om met beveiligingslekken?
- USB-poorten. De rol van de client firewall.

3 Het verificatieproces

- Toegangscontrole: authenticatie en autorisatie.
- Het belang van authenticatie.
- Het traditionele wachtwoord.
- Authenticatie met behulp van certificaten en tokens.
- Verbinding op afstand via het internet.
- Wat is een VPN?
- Waarom sterke authenticatie gebruiken?

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 Het veiligheidsauditproces

- Een continu en uitgebreid proces.
- Auditcategorieën, van organisatorische audits tot penetratietests.
- 19011 beste praktijk toegepast op veiligheid.
- Hoe stel je een intern auditprogramma op? Hoe kwalificeer je je auditors?
- Vergelijkende bijdragen, recursieve benadering, menselijke implicaties.
- Veiligheidsbewustzijn: wie? Wie? Wat? Hoe?
- Definities van moraliteit/Deontologie/Ethiek.
- Het veiligheidshandvest, het juridische bestaan, de inhoud en de validatie ervan.

5 Het noodplan en de kosten van veiligheid

- Risicodekking en continuïteitsstrategie.
- Het belang van rampen-, continuïteits-, herstel- en crisismanagementplannen, PCA/PRA, PSI, RTO/RPO.
- Een continuïteitsplan ontwikkelen en integreren in een kwaliteitsaanpak.
- Hoe veiligheidsbudgetten te definiëren.
- De definitie van ROSI (Return On Security Investment).
- Wat zijn de kostenevaluatietechnieken, de verschillende berekeningsmethoden, Total Cost of Ownership (TCO).
- Het Angelsaksische concept van de "Terugverdientijd".

6 Firewalls, virtualisatie en cloud computing

- Proxyservers, reverse proxy, adresmaskering.
- Firewall-gebaseerde perimeterbescherming.
- De verschillen tussen UTM, enterprise, NG en NG-v2 firewalls.
- Intrusion Prevention System (IPS)-producten en IPS NG.
- DMZ-oplossingen (gedemilitariseerde zone).
- Kwetsbaarheden in virtualisatie.
- De risico's van Cloud Computing volgens ANSSI, ENISA en CSA.
- De cloudcontrolematrix en het gebruik ervan bij het evalueren van cloudaanbieders.

7 Veiligheidstoezicht

- Veiligheidsdashboards.
- Beveiligingsaudits en penetratietests.
- De juridische aspecten van penetratietesten.
- IDS sondes, VDS scanner, WASS.
- Hoe reageer je effectief op aanvallen?
- Leg het bewijs vast.
- Een SIEM-oplossing implementeren.
- ANSSI-labels (PASSI, PDIS & PRIS) voor uitbesteding.
- Hoe reageer je in het geval van een indringer?
- Gerechtelijke expertise: de rol van een gerechtelijk deskundige (in straf- of civiele zaken).
- Particuliere juridische expertise.

8 Webaanvallen

- OWASP: organisatie, hoofdstukken, Top10, handleidingen, hulpmiddelen.
- Ontdek de infrastructuur en bijbehorende technologieën, sterke en zwakke punten.
- Clientzijde: clickjacking, CSRF, cookiediefstal, XSS, componenten (Flash, Java). Nieuwe vectoren.
- Serverzijde: authenticatie, sessiediefstal, injecties (SQL, LDAP, bestanden, commando's).
- Opname van lokale en externe bestanden, aanvallen en cryptografische vectoren.
- Omzeilen en omzeilen van bescherming: voorbeeld van WAF-omzeilingstechnieken.
- Burp Suite, ZAP, Sqlmap, BeEF tools.

Rollenspel
Presentatie en kennismaking met omgevingen en gereedschappen. Implementatie van verschillende webaanvallen onder echte omstandigheden aan server- en clientzijde.

9 Indringers detecteren

- Werkingsprincipes en detectiemethoden.
- Marktspelers, overzicht van de betrokken systemen en toepassingen.
- Scanners voor netwerken (Nmap) en toepassingen (webtoepassingen).
- IDS (Intrusion Detection System).
- De voordelen en beperkingen van deze technologieën.
- Hoe moeten ze worden gepositioneerd in de bedrijfsarchitectuur?
- Marktoverzicht, gedetailleerde studie van SNORT.

Rollenspel
Presentatie en kennismaking met omgevingen en hulpmiddelen. Installatie, configuratie en implementatie van SNORT, schrijven van aanvalshandtekeningen.

10 Informatie verzamelen

- De heterogeniteit van bronnen. Wat is een veiligheidsgebeurtenis?
- Informatiebeheer beveiligingsgebeurtenissen (SIEM). Gebeurtenissen verzameld uit de IS.
- Systeemlogs van apparatuur (firewalls, routers, servers, databases, etc.).
- Passief verzamelen in luistermodus en actief verzamelen.

Rollenspel
Loganalyseprocedure. Een adres geolokaliseren. Logs van verschillende bronnen correleren, bekijken, sorteren en zoeken naar regels.

Data en plaats

KLAS OP AFSTAND
2026 : 4 juni, 17 sep., 19 nov.

PARIS LA DÉFENSE
2026 : 4 juni, 17 sep., 19 nov.