Opleiding : Big Data, gegevensbeveiliging

Praktijkcursus - 2d - 14u00 - Ref. SBD
Prijs : 1430 € V.B.

À l'issue de la formation, le participant est capable d'initier une politique de sécurisation des données par une approche technique et légale du sujet. Elle permet de comprendre les enjeux de la sécurité dans les environnements Big Data, d'identifier les risques majeurs et d'y répondre avec des solutions concrètes.

Pedagogische doelstellingen

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

- Inzicht in complexe gegevenskwalificatie
- De belangrijkste risico's identificeren die van invloed zijn op oplossingen voor massale gegevensverwerking
- Inzicht in het wettelijk kader (CNIL en PLA - Privacy Level Agreement)
- De belangrijkste technische basisoplossingen kennen om jezelf tegen risico's te beschermen
- Een beveiligingsbeleid implementeren om risico's, bedreigingen en aanvallen aan te pakken

Doelgroep

Beveiligings- en IB-consultants, systeembeheerders.

Voorafgaande vereisten

Begrip van applicatiearchitecturen. Goede kennis van netwerk- en systeembeveiliging, bekendheid met Hadoop-platforms.

Opleidingsprogramma

DEELNEMERS

Beveiligings- en IB-consultants, systeembeheerders.

VOORAFGAANDE VEREISTEN

Begrip van applicatiearchitecturen. Goede kennis van netwerk- en systeembeveiliging, bekendheid met Hadoop-platforms.

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 Risico's en bedreigingen

- Inleiding tot beveiliging. Belangrijke externe informatiebronnen (ANSSI, CLUSIF, ENISA, enz.).
- De huidige staat van IT-beveiliging.
- IT-beveiligingswoordenschat.
- DICT/P-classificatie: Beschikbaarheid, Integriteit, Vertrouwelijkheid en Traceerbaarheid/bewijs.
- Aanvallen "lagere lagen". Beveiliging op Hadoop. Inlichtingen verzamelen.
- Sterke en zwakke punten van het TCP/IP protocol. HTTP: een blootgesteld protocol (SQL-injectie, Cross Site Scripting, enz.).
- Illustratie van ARP en IP Spoofing aanvallen, TCPSYNflood, smurf, etc.
- Ontzegging van dienst en gedistribueerde ontzegging van dienst. DNS: Dan Kaminsky aanval. Applicatie-aanvallen.

Praktisch werk

De Wireshark netwerkanalyser installeren en gebruiken. Een applicatie-aanval uitvoeren.

2 Beveiligingsarchitecturen

- Welke architecturen voor welke behoeften?
- Beveiligd adresseringsplan: RFC 1918. Adresomzetting (FTP als voorbeeld).
- De rol van gedemilitariseerde zones (DMZ's). Voorbeelden van architecturen.
- Veilige architectuur door virtualisatie.
- Firewall: de hoeksteen van beveiliging, firewalls en virtuele omgevingen.
- Serverproxy en applicatie relay. Proxy of firewall: concurrentie of complementariteit?
- Technologische ontwikkelingen in firewalls (Appliance, VPN, IPS, UTM, enz.).
- Reverse proxy, inhoud filteren, caching en authenticatie. SMTP-relay: een verplichting?

Praktisch werk

Implementatie van een proxy cache/authenticatie.

3 De integriteit van een systeem controleren

- Werkingsprincipes.
- Welke producten zijn beschikbaar?
- Presentatie van Tripwire of AIDE (Advanced Intrusion Detection Environment).
- Kwetsbaarheidsaudits.
- Principes, methoden en organisaties voor kwetsbaarheidsmanagement.
- Referentiesite en overzicht van audittools.
- Definitie van een beveiligingsbeleid.
- Studie en implementatie van Nessus (status, werking, ontwikkeling).

Praktisch werk

Controle van netwerk- en serverkwetsbaarheden met Nessus en Nmap.
Controle op kwetsbaarheden van websites.

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 Wettelijke overtredingen van systemen voor automatische gegevensverwerking

- Herinnering, definitie van een automatisch gegevensverwerkend systeem (ADPS).
- De risico's voor massale gegevensverwerkingsoplossingen.
- Soorten inbreuken, Europese context, de LCEN-wetgeving. De RGPD-verordening, CNIL, PLA.
- Wat zijn de juridische risico's voor het bedrijf, de managers en de CISO?

Data en plaats

KLAS OP AFSTAND
2026 : 18 juni, 19 nov.

PARIS LA DÉFENSE
2026 : 18 juni, 19 nov.