

Opleiding : De beveiliging van cloudservices en MS-Azure beheren, samenvatting

Synthese cursus - 2d - 14u00 - Ref. CAZ

Prijs : 1720 € V.B.

In deze cursus maakt u kennis met de beveiligingsproblemen en -oplossingen met betrekking tot gegevensverwerking in de openbare clouds AWS (Amazon Web Services) en Microsoft Azure. U leert over de verschillende tools en diensten die beschikbaar zijn om restrisiko's te beoordelen en te beheersen.

Pedagogische doelstellingen

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

- ✓ Risico's inschatten en beheren
- ✓ Ontdek de beschikbare tools en services
- ✓ Inzicht in de organisatie die nodig is om het veiligheidsniveau te handhaven en te verbeteren

Doelgroep

IT- en functionele managers. Alle IT-managers.

Voorafgaande vereisten

Basiskennis van technische architecturen en IS-beheer.

Opleidingsprogramma

1 De grondbeginselen

- De relatie tussen virtualisatie en cloud computing.
- De Cloud (IaaS, PaaS, SaaS), markttrends.
- Het laatste nieuws over beveiligingslekken met betrekking tot AWS (Amazon Web Services) en Azure.
- Cloud Computing-beveiligingsbedreigingen (Notorious Nine en Dirty Dozen) volgens CSA (Cloud Security Alliance).
- APT's, de Snowden-onthullingen, NSL (National Security Letters).
- De Franse en Europese context. De positie van het Franse nationale agentschap voor de beveiliging van informatiesystemen (ANSSI).

DEELNEMERS

IT- en functionele managers. Alle IT-managers.

VOORAFGAANDE VEREISTEN

Basiskennis van technische architecturen en IS-beheer.

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.

2 Het model van gedeelde verantwoordelijkheid

- Identiteitsbeheer en toegangscontrole (IAM).
- Multi-Factor Authenticatie (MFA).
- Security Token Service (STS).

3 Beveiliging van virtuele machines (VM)

- Beeldbeveiliging, systeemverharding.
- AWS en Azure LAN beveiliging.
- Virtual Private Cloud (VPC) en Virtuele Netwerkarchitecturen en hun componenten.
- Herinnering aan perimeterbeveiliging, partitionering en soorten firewalls.
- Verschil tussen Network Access Control Lists (NACLs) en Security Groups (SGs).
- WAF en CDN.
- DirectConnect, Express Route en/of IPSEC VPN-verbinding.
- Verdediging tegen DDoS (Route 53 en DNS, LB, CloudFront).

4 Cryptografisch beheer

- Basisconcepten van SSL en TLS.
- Certificeringsautoriteit.
- AWS Key Management Service (KMS), Azure KeyVault HSM.

5 Back-ups van gegevens

- Principe en gebruik.
- Focus op AWS- en Azure-services.

6 Veiligheid controleren

- Amazon Inspector, Azure Beveiligingscentrum.
- AWS: Configuratieregels, Trusted Advisor, CloudWatch Logs en gebeurtenissen, CloudTrail.
- Azure: Log Analytics, Azure Portal.
- Andere logs (S3 Logs, Bucket Logging, CloudFormation Logs, VPC Flow Logs).
- De voordelen van oplossingen voor beveiligingsverbetering van derden.
- Inbraaktests: voorzorgsmaatregelen en voorafgaande autorisaties.
- Een misbruik, kwetsbaarheid of inbreuk op de beveiliging melden.

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.

Data en plaats

KLAS OP AFSTAND

2026 : 24 maa., 4 juni, 17 sep., 19 nov.

PARIS LA DÉFENSE

2026 : 4 juni, 17 sep., 19 nov.