

Opleiding : Cloudcomputing, beveiliging

seminarie - 2d - 14u00 - Ref. OUD

Prijs : 1720 € V.B.



4,4 / 5

Hoe kunnen we de beveiliging van informatie in de cloud garanderen? Dit seminar biedt een uitgebreid overzicht van deze belangrijke cloudkwestie. Deelnemers krijgen een praktisch begrip van de risico's die het gebruik van een cloud met zich meebrengt en van de verschillende standaarden die bestaan voor het beoordelen van de beveiliging van gegevens en leveranciers.



Pedagogische doelstellingen

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

- ✓ De organisatorische aspecten van cloudbeveiliging identificeren
- ✓ De grondbeginselen van IS- en cloudbeveiliging begrijpen
- ✓ Inzicht in de belangrijkste bedreigingen, kwetsbaarheden en risico's van de cloud
- ✓ Kennis van de normen en standaarden voor het beveiligen van de cloud
- ✓ De volwassenheid en het beveiligingsniveau van cloudproviders beoordelen
- ✓ Best practices en beveiligingsoplossingen van cloudbeheerders identificeren

Doelgroep

CIO's, CIO's, projectmanagers, beveiligingsmanagers, consultants, beheerders, iedereen die verantwoordelijk is voor de beveiliging van Cloud Computing.

Voorafgaande vereisten

Algemene kennis van informatiesystemen.

Opleidingsprogramma

DEELNEMERS

CIO's, CIO's, projectmanagers, beveiligingsmanagers, consultants, beheerders, iedereen die verantwoordelijk is voor de beveiliging van Cloud Computing.

VOORAFGAANDE VEREISTEN

Algemene kennis van informatiesystemen.

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 Inleiding tot beveiliging van cloud computing

- Cloud computing-architectuur (NIST, ISO 17788/17889).
- Schaduw-IT: het opsporen en voorkomen van niet-goedgekeurd gebruik van de cloud.
- Het principe van gedeelde verantwoordelijkheid in IaaS, PaaS en SaaS.
- ISO 27017 en 27018 standaarden voor het beveiligen van gegevens in de cloud.

2 Gegevensbeveiliging in de cloud

- Gegevens in de cloud: levenscyclus, classificatie, anonimisering, pseudonimisering, tokenisering.
- De BYOK-benadering (bring your own key) en HSM-oplossingen in de cloud.
- De CASB (cloud access security broker), principes en oplossingen.

3 Cloud beveiligingsalliantie (CSA) standaarden

- De 14 beveiligingsrichtlijnen voor kritieke aandachtsgebieden bij cloud computing.
- CCSK-certificering (certificaat van cloudbeveiligingskennis).
- De cloudcontrolematrix (CCM) en de consensusbeoordelvragenlijst (CAIQ).
- Het OCF-certificeringsraamwerk en de STAR-directory (Security, Trust & Assurance Register).
- De GDPR-gedragscode (CoC GDPR) voor leveranciers.

4 De risico's van cloud computing volgens ENISA

- Risicobeoordeling en -beheer in de cloud met behulp van de ISO 27005-norm.
- De bijzonderheden van risicobeheer in de cloud.
- De belangrijkste risico's die door ENISA zijn geïdentificeerd.

5 Veiligheidsbeoordeling van leveranciers

- Overzicht van certificeringen/kwalificaties (SecNumCloud, SSAE18, HDS, etc.).
- Europese veiligheidscertificering onder de Cybersecurity Act.
- De voordelen en beperkingen van ISO 27001-certificering voor clouddiensten.

6 Beveiliging in cloudcontracten

- Service Level Agreements (SLA's): boetes versus compensatie.
- Beveiligingsclausules die moeten worden opgenomen in een cloudcontract (vertrouwelijkheid, gegevensverwijdering, enz.).
- Upstream en downstream omkeerbaarheidsclausules.

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.

7 Juridische aspecten

- Het wettelijke kader voor persoonlijke gegevens (GDPR, GDT, BCR, enz.).
- Hoe zorg je ervoor dat de RGPD wordt nageleefd in de cloud?
- Amerikaanse wetten en bepalingen (Privacy Shield, Patriot Act, FISA, Cloud Act).
- Hoe is de wet Godfrain (CP 323) van toepassing in een internationale cloudcontext?
- Hosts voor gezondheidsgegevens (HDS-certificering, beveiligingsverplichtingen, lokalisatie van gegevens, enz.)

Data en plaats

KLAS OP AFSTAND

2026 : 16 juni, 16 juni, 29 sep., 29 sep., 24 nov.,
24 nov.

PARIS LA DÉFENSE

2026 : 16 juni, 29 sep., 24 nov.