

Opleiding : Certified Cloud Security Professional (CCSP), ISC2-certificering

Officiële training afgestemd op ISC2

Praktijkcursus - 5d - 35u00 - Ref. CCN

Prijs : 3440 € V.B.

Nouvelle édition

La certification CCSP (Certified Cloud Security Professional), délivrée par ISC2, est une certification de référence, vendor-neutral, dédiée à la sécurité du cloud computing. Cette formation vous permettra d'acquérir une vision stratégique et opérationnelle de la sécurité cloud afin de réussir l'examen officiel CCSP, en couvrant l'ensemble des 6 domaines du CCSP Common Body of Knowledge (CBK).

Pedagogische doelstellingen

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

- ✓ Cloudconcepten, servicemodellen en referentiearchitecturen beheersen
- ✓ Een veilige, samenhangende en bestuurd cloudarchitectuur ontwerpen
- ✓ Een strategie definiëren en beheren voor de bescherming van gegevens in de cloud gedurende de gehele levenscyclus ervan
- ✓ Cloudplatforms, -infrastructuren en -diensten beveiligen
- ✓ Beveiligingsvereisten integreren in cloudapplicaties en CI/CD-ketens
- ✓ Cloudbeveiligingsactiviteiten organiseren en beheren, inclusief toezicht, incidentbeheer en continuïteit
- ✓ Juridische, risicobeheer- en compliancevereisten toepassen die specifiek zijn voor cloudomgevingen
- ✓ De "cloud security leader"-benadering aannemen die ISC2 verwacht om te slagen voor het CCSP-examen
- ✓ Effectief voorbereiden op het officiële CCSP examen (ISC2 formaat en verwachtingen)

Doelgroep

IT-architecten en -ingenieurs, managers van informatiesystemen en beveiliging, DevOps/SecOps-profielen, beveiligingsconsultants en IT-professionals op het gebied van risico, compliance en contracten.

DEELNEMERS

IT-architecten en -ingenieurs, managers van informatiesystemen en beveiliging, DevOps/SecOps-profielen, beveiligingsconsultants en IT-professionals op het gebied van risico, compliance en contracten.

VOORAFGAANDE VEREISTEN

De CCSP-certificering vereist 5 jaar IT-ervaring, waarvan 3 jaar in cyberbeveiliging en 1 jaar in cloudbeveiliging. Vrijstellingen zijn mogelijk (diploma, CCSK). CISSP valideert het geheel.

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.

Voorafgaande vereisten

De CCSP-certificering vereist 5 jaar IT-ervaring, waarvan 3 jaar in cyberbeveiliging en 1 jaar in cloudbeveiliging. Vrijstellingen zijn mogelijk (diploma, CCSK). CISSP valideert het geheel.

Certificatie

Het officiële examen vindt plaats in het Engels, in de vorm van een 3 uur durende MCQ bestaande uit 100 tot 150 vragen, met een minimumscore van 700/1000.

Opleidingsprogramma

1 Gebied 1 - Cloudconcepten, architectuur en ontwerp

- Fundamentele concepten van cloud computing.
- Cloud servicemodellen (IaaS, PaaS, SaaS) en implementatiemodellen.
- Principes van cloudarchitectuur en veilig ontwerp.
- Een model van gedeelde verantwoordelijkheid.
- Governance en consistentie van controles in een multi-cloudomgeving.
- Orkestratie van cloudservices en integratie van componenten.

2 Gebied 2 - Gegevensbeveiliging in de cloud

- Gegevensbeheer en verantwoordelijkheden in de cloud.
- Classificatie- en gegevensbeschermingsvereisten.
- Levenscyclusbeheer van cloudgegevens.
- Gegevensbeschermingscontroles (beleid, procedures, mechanismen).
- Beheer van lokalisatie, bewaring en verwijdering van gegevens.

3 Gebied 3 - Beveiliging van cloudplatforms en -infrastructuren

- Architectuur en beveiliging van cloudinfrastructuren.
- Beveiliging van cloudplatforms en -diensten.
- Segmentatie, isolatie en cloudinterconnecties.
- Configuratie- en kwetsbaarheidsbeheer.
- Beveiligingscontroles voor infrastructuurdiensten.

4 Gebied 4 - Beveiliging van cloudapplicaties

- Beveiligingseisen voor applicaties in een cloudomgeving.
- Beveiliging integreren in de ontwikkelings- en implementatiecyclus.
- Beveiliging van API's en applicatieservices.
- Risicobeheer van applicaties specifiek voor de cloud.
- Secure-by-design benadering en afstemming op beveiligingsbeleid.

5 Gebied 5 - Beveiligingsactiviteiten voor de cloud

- Organisatie en bestuur van cloudbeveiligingsactiviteiten.
- Toezicht, logging en cloud-native monitoring.
- Beheer van cloudbeveiligingsgebeurtenissen en -incidenten.
- Operationeel toegangs- en identiteitsbeheer.
- Bedrijfscontinuïteit, veerkracht en herstel in cloudomgevingen.

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.

6 Gebied 6 - Juridisch, risico en naleving

- Wettelijke en regelgevende kaders die van toepassing zijn op clouddiensten.
- Contractuele vereisten en verantwoordelijkheden van klanten en leveranciers.
- Risicobeheer in de cloud.
- Naleving, audit en bewijsvoering.
- Toepassing van beleid en procedures om te voldoen aan wettelijke verplichtingen.

7 Voorbereiding op het CCSP examen

- Presentatie van het CCSP examen.
- Methodologie voor het beantwoorden van ISC2 vragen.
- Tijdmanagement en veelvoorkomende valkuilen.
- Quiz en examenvragen.
- Advies van CCSP-gecertificeerde experts.

Data en plaats

KLAS OP AFSTAND

2026 : 8 juni, 21 sep., 30 nov.

PARIS LA DÉFENSE

2026 : 20 apr., 1 juni, 14 sep., 23 nov.