Azure - Beveiligingstechnologieën (Microsoft AZ-500)

Officiële AZ-500T00-cursus, voorbereiding op het examen

Praktijkcursus van 4 dagen - 28u
Ref : MZO - Prijs 2024 : € 3 310 excl. BTW

Deze opleiding biedt u de noodzakelijke vaardigheden en kennis om beveiligingscontroles te implementeren, de beveiligingssituatie van een organisatie in stand te houden, en kwetsbaarheden op het gebied van beveiliging te identificeren en te verhelpen. Deze opleiding omvat ook identiteits- en toegangsbeveiliging, platformbeveiliging, gegevens en toepassingen, en beveiligingsactiviteiten.

PEDAGOGISCHE DOELSTELLINGEN

Na afloop van de opleiding kan de cursist:

De classificaties van gespecialiseerde gegevens op Azure begrijpen

De Azure-mechanismen voor gegevensbescherming beheersen

Azure-methoden voor gegevensversleuteling kunnen implementeren

De beveiligde internetprotocollen kennen en kunnen implementeren op Azure

De Azure-beveiligingsservices en -functies beheersen

PEDAGOGISCHE METHODEN

De opleiding wordt in het Frans gegeven. Officieel Microsoft-cursusmateriaal (digital MOC) in het Engels.

CERTIFICERING

Wie voor het examen slaagt, behaalt de Microsoft Certified Azure Security Engineer Associate-certificering

HET PROGRAMMA

laatste update: 11/2021

1) De identiteiten en de toegang beheren

- Azure Active Directory (infrastructuur, gebruikers, groepen, multifactorauthenticatie).
- Azure-identiteitsbescherming (risicostrategieën, voorwaardelijke toegang en toegangscontroles).
- Corporate governance.
- Exclusief Azure AD-identiteitsbeheer.
- Hybride identiteit.

Implementeren: op rollen gebaseerde toegangscontrole, Azure-beleid, vergrendeling van de Resource Manager, MFA, voorwaardelijke toegang en AAD-identiteitsbescherming, exclusief Azure AD-identiteitsbeheer, mapsynchronisatie.

2) Een platformbeveiliging implementeren

- Perimeterbeveiliging (Azure-firewall, enz.).
- Netwerkbeveiliging (netwerkbeveiligingsgroepen, toepassingsbeveiligingsgroepen, enz.).
- Hostbeveiliging (bescherming van het eindpunt, beheer van toegang op afstand, schijfversleuteling, enz.).
- Containerbeveiliging (Azure-containerinstanties, Azure-containerregister en Azure Kubernetes).

Praktische toepassing: netwerkbeveiligingsgroepen en toepassingsbeveiligingsgroepen, Azure-firewall, ACR en AKS configureren en beveiligen.

DEELNEMERS

Azure-beheerders die de beveiliging van Azure-resources willen begrijpen, implementeren en controleren.

VOORAFGAANDE VEREISTEN

De opleiding “Microsoft Azure - Beheer” (AZ-104) hebben gevolgd, of over gelijkwaardige kennis beschikken.

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.

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.

3) Gegevens en toepassingen beveiligen

- Azure Key Vault (certificaten, sleutels en secrets).
- Toepassingsbeveiliging (inschrijving voor toepassingen, beheerde identiteiten en service-eindpunten).
- Opslagbeveiliging (handtekeningen voor gedeelde toegang, Blob-retentiestrategieën en Azure-bestandsauthenticatie).
- SQL-databasebeveiliging (authenticatie, gegevensclassificatie en dynamische gegevensmaskering).

Beveiligingsgegevens implementeren door Always Encrypted te configureren, een Azure SQL-database en service-eindpunten beveiligen, en beveiliging van de opslag.

4) Beveiligingsactiviteiten beheren

- Azure Monitor (verbonden bronnen, logboekanalyse, waarschuwingen, enz.).
- Azure Security Center (strategieën, aanbevelingen, Just-in-Time-toegang tot virtuele machines).
- Azure Sentinel (mappen, incidenten en playbooks, enz.).

Azure Monitor, Azure Security Center en Azure Sentinel implementeren.

DATA

KLAS OP AFSTAND
2024 : 25 jun, 03 sep, 22 okt

BRUSSEL
2024 : 03 sep, 22 okt