Azure - Technologies de sécurité (Microsoft AZ-500)

Cours officiel AZ-500T00, préparation à l'examen

Cours Pratique de 4 jours - 28h
Réf : MZO - Prix 2024 : 3 310€ HT

Cette formation vous permet d'acquérir les compétences et les connaissances nécessaires pour mettre en œuvre des contrôles de sécurité, de maintenir la posture de sécurité d'une organisation, d'identifier et de remédier aux vulnérabilités en matière de sécurité. Cette formation aborde aussi la sécurité en matière d'identité et d'accès, la protection de plateforme, les données et les applications, ainsi que les opérations de sécurité.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Comprendre les classifications de données spécialisées sur Azure

Maîtriser les mécanismes de protection des données Azure

Savoir implémenter des méthodes de chiffrement de données Azure

Connaître les protocoles Internet sécurisés et savoir les implémenter sur Azure

Maîtriser les services et fonctionnalités de sécurité Azure

MÉTHODES PÉDAGOGIQUES

Animation de la formation en français. Support de cours officiel au format numérique et en anglais. Bonne compréhension de l'anglais à l'écrit.

CERTIFICATION

La réussite de l'examen permet d'obtenir la certification Microsoft Certified Azure Security Engineer Associate

LE PROGRAMME

dernière mise à jour : 01/2024

1) Gérer les identités et les accès

- Azure Active Directory (infrastructure, utilisateurs, groupes, authentification multi-facteurs).
- La protection d'identité Azure (stratégies de risque, accès conditionnel et vérifications d'accès).
- La gouvernance d'entreprise.
- La gestion de l'identité privilégiée Azure AD.
- L'identité hybride.

Travaux pratiques : Mettre en œuvre : contrôle d'accès en fonction du rôle, politique Azure, verrouillage du gestionnaire de ressources, MFA, accès conditionnel et protection d'identité AAD, gestion de l'identité privilégiée Azure AD, la synchronisation de répertoires.

2) Mettre en œuvre une protection de la plateforme

- Sécurité du périmètre (pare-feu Azure, etc.).
- Sécurité du réseau (groupes de sécurité réseau, groupes de sécurité d'application, etc.).
- Sécurité de l'hôte (protection du point de terminaison, gestion de l'accès à distance, cryptage du disque, etc.).

FINANCEMENT

Ce cours fait partie des actions collectives Atlas.

PARTICIPANTS

Administrateurs Azure qui veulent comprendre, mettre en place et surveiller la sécurité des ressources Azure.

PRÉREQUIS

Avoir suivi la formation "Microsoft Azure – Administration" (AZ-104) ou avoir les connaissances équivalentes.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation…
À l'issue de chaque stage, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Sécurité du conteneur (instances de conteneurs Azure, registre de conteneurs Azure et Azure Kubernetes).

Travaux pratiques : Mise en pratique : groupes de sécurité réseau et groupes de sécurité applications, pare-feu Azure, configurer et sécuriser ACR et AKS.

3) Sécuriser les données et les applications

- Azure Key Vault (certificats, clés et secrets).
- Sécurité des applications (inscription aux applications, identités gérées et points de terminaison des services).
- Sécurité du stockage (signatures d'accès partagé, stratégies de rétention de Blob, et authentification des fichiers Azure).
- Sécurité des bases de données SQL (authentification, classification des données, el masquage dynamique des données).

Travaux pratiques : Mettre en œuvre des données de sécurité en configurant Always Encrypted, sécuriser une base de données Azure SQL, points de terminaison des services et sécurisation du stockage.

4) Gérer les opérations de sécurité

- Azure Monitor (sources connectées, analyse des journaux, alertes, etc.).
- Azure Security center (stratégies, recommandations, accès aux machines virtuelles juste-à-temps).
- Azure Sentinel (classeurs, incidents et playbooks, etc.).

Travaux pratiques : Mettre en œuvre Azure Monitor, Azure Security center et Azure Sentinel.

LES DATES

CLASSE À DISTANCE	PARIS
2024 : 16 juil., 05 nov.	2024 : 09 juil., 22 oct.