Programme de formation AZ-500: Azure Security Technologies

(Préparation certification Microsoft AZ-500)

DESCRIPTION DE LA FORMATION :

Mettez en œuvre des contrôles de sécurité et une protection contre les menaces, gérez les identités et les accès, protégez les données, les applications et les réseaux dans les environnements Cloud et hybrides, au sein d'une infrastructure de bout en bout. Cette formation vous accompagnera étape par étape pour y parvenir.

OBJECTIFS PEDAGOGIQUES :

A l'issue de cette formation, les participants seront en capacité de :

- Sécuriser les solutions Azure avec Azure Active Directory
- Implémenter l'identité hybride
- Déployer la protection des identités Azure AD
- Configurer la gestion des identités privilégiées Azure AD
- Concevoir une stratégie de gouvernance d'entreprise
- Implémenter la sécurité du périmètre
- Configurer la sécurité réseau et configurer et gérer la sécurité des ordinateurs hôtes
- Activer la sécurité des conteneurs
- Déployer et sécuriser Azure Key Vault
- Configurer les fonctionnalités de sécurité des applications
- Implémenter la sécurité du stockage
- Configurer et gérer la sécurité de la base de données SQL et configurer et gérer Azure Monitor
- Activer et gérer Microsoft Defender pour le cloud
- Configurer et surveiller Microsoft Sentinel

MÉTHODES & MODALITÉS PÉDAGOGIQUES :

- Cette formation sera principalement constituée de théorie et d'ateliers techniques qui permettront d'être rapidement opérationnel.
- Support : un support de cours officiel Microsoft sera remis aux participants au format électronique.
- Evaluation : Les acquis sont évalués tout au long de la formation par le formateur (Prérequis évalués avant la formation, questions régulières, travaux pratiques, QCM ou autres méthodes).
- Formateur : le tout animé par un consultant-formateur expérimenté, nourri d'une expérience terrain, et accrédité Microsoft Certified Trainer.

- Satisfaction : à l'issue de la formation, chaque participant répond à un questionnaire d'évaluation qui est ensuite analysé en vue de maintenir et d'améliorer la qualité de nos formations.
- Suivi : une feuille d'émargement par demi-journée de présence est signée par chacun des participants.
- Cette formation peut être dispensée en format inter-entreprises ou intra-entreprise sur demande et en mode présentiel comme en distanciel.

PROGRAMME DE FORMATION :

Sécuriser les solutions Azure avec Azure Active Directory

- Configurer Azure AD et Azure AD Domain Services pour la sécurité.
- Créer des utilisateurs et des groupes qui permettent une utilisation sécurisée de votre locataire.
- Utiliser l'authentification multifacteur pour protéger les identités des utilisateurs.
- Configurer les options de sécurité avec mot de passe.

Implémenter l'identité hybride

- Déployer Azure AD Connect.
- Choisir et configurer l'option d'authentification la mieux adaptée aux besoins de sécurité.
- Configurer l'écriture différée du mot de passe.

Déployer la protection des identités Azure AD

- Déployer et configurer la protection des identités.
- Configurer l'authentification multifacteur pour les utilisateurs, les groupes et les applications.
- Créer des stratégies d'accès conditionnel pour garantir la sécurité.
- Créer et suivre un processus de révision d'accès.

Configurer la gestion des identités privilégiées Azure AD

- Décrire la Confiance Zéro et son impact sur la sécurité.
- Configurer et déployer des rôles à l'aide de Privileged Identity Management (PIM).
- Évaluer l'utilité de chaque paramètre PIM en ce qui concerne les objectifs de sécurité.

Concevoir une stratégie de gouvernance d'entreprise

- Expliquer le modèle de responsabilité partagée et son impact sur votre configuration de sécurité.
- Créer des stratégies Azure pour protéger vos solutions.
- Configurer et déployer l'accès aux services à l'aide de RBAC.

Implémenter la sécurité du périmètre

- Définir la défense en profondeur.
- Protéger votre environnement des attaques par déni de service.
- Sécuriser vos solutions à l'aide de pare-feu et de VPN.
- Explorer votre configuration de sécurité de périmètre de bout en bout en fonction de votre position de sécurité.

Configurer la sécurité réseau

- Déployer et configurer des groupes de sécurité réseau pour protéger vos solutions Azure.
- Configurer et verrouiller les points de terminaison de service et les liaisons privées.
- Sécuriser vos applications avec Application Gateway, Pare-feu d'applications web et Front Door.

- Configurer ExpressRoute pour contribuer à protéger votre trafic.

Configurer et gérer la sécurité des ordinateurs hôtes

- Configurer et déployer Endpoint Protection.
- Déployer une stratégie d'accès privilégié pour les appareils et les stations de travail privilégiées.
- Sécuriser vos machines virtuelles et y accéder.
- Déployer Windows Defender.
- Pratiquer la sécurité en couche en examinant et en implémentant Security Center et des points de référence de sécurité.

Activer la sécurité des conteneurs

- Définir les outils de sécurité disponibles pour les conteneurs dans Azure.
- Configurer les paramètres de sécurité pour les conteneurs et les services Kubernetes.
- Verrouiller les ressources réseau, de stockage et d'identité connectées à vos conteneurs.
- Déployer RBAC pour contrôler l'accès aux conteneurs.

Déployer et sécuriser Azure Key Vault

- Définir ce qu'est un coffre de clés et comment il protège les certificats et les secrets.
- Déployer et configurer Azure Key Vault.
- Sécuriser l'accès et l'administration de votre coffre de clés.
- Stocker les clés et les secrets dans votre coffre de clés.
- Explorer la sécurité des clés, comme la rotation des clés et la sauvegarde/récupération.

Configurer les fonctionnalités de sécurité des applications

- Inscrire une application dans Azure à l'aide de l'inscription d'application.
- Sélectionner et configurer les utilisateurs Azure AD qui peuvent accéder à chaque application.
- Configurer et déployer des certificats d'application web.

Implémenter la sécurité du stockage

- Définir la souveraineté des données et comment les obtenir dans Azure.
- Configurer l'accès au Stockage Azure de manière sécurisée et gérée.
- Chiffrer vos données pendant qu'elles sont au repos et en transit.
- Appliquer des règles pour la rétention des données.

Configurer et gérer la sécurité de la base de données SQL

- Configurer les utilisateurs et les applications qui ont accès à vos bases de données SQL.
- Bloquer l'accès à vos serveurs à l'aide de pare-feu.
- Découvrir, classer et auditer l'utilisation de vos données.
- Chiffrer et protéger vos données pendant qu'elles sont stockées dans la base de données.

Configurer et gérer Azure Monitor

- Configurer et surveiller Azure Monitor.
- Définir les métriques et les journaux que vous souhaitez suivre pour vos applications Azure.
- Connecter les sources de données et configurer Log Analytics.
- Créer et surveiller les alertes associées à la sécurité de vos solutions.

Activer et gérer Microsoft Defender pour le cloud

- Définir les types les plus courants de cyberattaques.
- Configurer Azure Security Center en fonction de votre posture de sécurité.

- Examiner le Niveau de sécurité et l'élever.
- Verrouiller vos solutions avec Security Center et Defender.
- Activer l'accès juste-à-temps et d'autres fonctionnalités de sécurité.

Configurer et surveiller Microsoft Sentinel

- Expliquer ce qu'est la fonctionnalité Azure Sentinel et comment elle est utilisée.
- Déployer Azure Sentinel.
- Connecter des données à Azure Sentinel, comme les journaux Azure, Azure AD et autres.
- Suivre les incidents à l'aide de classeurs, de playbooks et de techniques de chasse.

PRÉREQUIS :

Pour suivre cette formation, vous devez avoir une compréhension et une connaissance :

- Des meilleures pratiques de sécurité et exigences de sécurité de l'industrie telles que la défense en profondeur, l'accès le moins privilégié, le contrôle d'accès basé sur les rôles, l'authentification multifacteur, la responsabilité partagée et le modèle de confiance zéro
- Des protocoles de sécurité tels que les réseaux privés virtuels (VPN), le protocole de sécurité Internet (IPSec), Secure Socket Layer (SSL), les méthodes de cryptage de disque et de données
- Du déploiement de charges de travail Azure.
- Des systèmes d'exploitation Windows et Linux et les langages de script.

Les travaux pratiques de la formation peuvent utiliser PowerShell et l'interface de ligne de commande.

Ce cours ne couvre pas les bases de l'administration Azure, mais le contenu du cours s'appuie sur ces connaissances en ajoutant des informations spécifiques à la sécurité.

Il faut avoir suivi la formation « AZ-900 Azure Fundamentals » et impérativement la formation « AZ-104 : Azure Administrator » pour suivre ce cours ou avoir un niveau d'expérience sur Azure équivalent.

Un niveau d'anglais B1 est requis, retrouvez les niveaux sur ce lien : Classification des niveaux de langue

PRE-CERTIFCIATION :

Cette formation ouvre la porte à la certification Microsoft « AZ-500 – Azure Security Technologies ».

DUREE : 5 jours (35 heures)

INTERLOCUTEURS : Administrateurs, IT Pro, Responsables sécurité

NIVEAU : Intermédiaire