Programme de formation

AZ-500 : Azure Security Technologies

(Préparation certification Microsoft AZ-500)

Mis à jour le 15/04/2024

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 :

- Gérer les identités dans Microsoft Entra ID
- Gérer l'authentification et l'autorisation à l'aide de Microsoft Entra ID
- Gérer l'accès aux applications dans Microsoft Entra ID
- Planifier et implémenter la sécurité pour les réseaux virtuels
- Planifier et implémenter la sécurité pour l'accès privé ou l'accès public à des ressources Azure
- Planifier et implémenter une sécurité avancée pour le calcul
- Planifier et implémenter la sécurité pour le stockage
- Planifier et implémenter la sécurité pour Azure SQL Database et Azure SQL Managed Instance
- Planifier, implémenter et gérer la gouvernance pour la sécurité
- Gérer la posture de sécurité en utilisant Microsoft Defender
- Configurer et gérer la protection contre les menaces en utilisant Microsoft Defender
- Configurer et gérer des solutions de supervision et d'automatisation de la sécurité

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 :

Gérer les identités dans Microsoft Entra ID

- Améliorer la sécurité dans Microsoft Entra ID pour protéger les identités et les comptes des utilisateurs.
- Implémenter la sécurité pour la gestion des groupes dans Microsoft Entra ID pour un contrôle d'accès efficace.
- Conseiller sur la gestion sécurisée des identités externes dans Microsoft Entra ID.
- Utiliser la protection des identités Microsoft Entra pour une détection et une réponse proactive aux menaces.

Gérer l'authentification à l'aide de Microsoft Entra ID

- Implémenter l'authentification multifacteur et sans mot de passe pour renforcer la sécurité et la commodité.
- Appliquer des mesures de protection par mot de passe et l'authentification unique pour un accès simplifié et sécurisé.
- Intégrer l'authentification unique à des fournisseurs d'identité et approuver des protocoles d'authentification modernes.
- Configurer Vérification d'identité Microsoft Entra pour la vérification d'identité approuvée.

Gérer l'autorisation à l'aide de Microsoft Entra ID

- Configurer les autorisations de rôles Azure pour des groupes d'administration, des abonnements et des ressources pour le contrôle d'accès.
- Attribuer des rôles intégrés dans Microsoft Entra ID et Azure pour des autorisations utilisateur prédéfinies.
- Créer des rôles personnalisés dans Azure et Microsoft Entra ID pour répondre aux besoins d'accès organisationnel.
- Gérer les autorisations Entra, Privileged Identity Management et l'accès conditionnel pour un contrôle et une conformité affinée.

Gérer l'accès aux applications dans Microsoft Entra ID

- Gérer l'accès aux applications d'entreprise dans Microsoft Entra ID, y compris les octrois d'autorisations OAuth pour le contrôle d'accès.
- Administrer l'intégration d'applications aux plateformes d'identité via les inscriptions d'applications Microsoft Entra ID.
- Configurer les étendues des autorisations d'inscription des applications pour les niveaux d'accès aux ressources appropriés.
- Gérer le consentement d'inscription des applications et utiliser les principaux de service et les identités managées pour la gestion automatisée et la sécurité améliorée.

Planifier et implémenter la sécurité pour les réseaux virtuels

- Implémenter des mesures de sécurité pour les réseaux virtuels Azure afin de protéger les données et les ressources.

- Utiliser des groupes de sécurité réseau (NSG) et des groupes de sécurité d'application (ASG) pour la sécurité du trafic réseau et gérer des routes définies par l'utilisateur (UDR) pour un routage optimal du trafic.
- Établir une connectivité réseau sécurisée via l'appairage de réseaux virtuels, les passerelles de réseau privé virtuel (VPN) et le service Virtual WAN.
- Améliorer la sécurité réseau avec les configurations VPN, le chiffrement ExpressRoute, les paramètres de pare-feu PaaS et le monitoring de Network Watcher.

Planifier et implémenter la sécurité pour l'accès public à des ressources Azure

- Développer des stratégies pour sécuriser l'accès public aux ressources Azure, ce qui empêche l'accès non autorisé et les violations.
- Implémenter TLS pour Azure App Service et Gestion des API afin de chiffrer les données en transit.
- Protéger le trafic réseau avec le Pare-feu Azure et Application Gateway pour optimiser la sécurité et la diffusion des applications web.
- Améliorer les performances des applications web avec Azure Front Door et CDN, et déployer WAF et DDoS Protection pour une défense robuste contre les attaques.

Planifier et implémenter la sécurité pour l'accès privé à des ressources Azure

- Développer des stratégies de sécurité pour l'accès privé aux ressources Azure afin de protéger des données sensibles.
- Utiliser des points de terminaison de service de réseau virtuel et des points de terminaison privés pour sécuriser l'accès au service Azure.
- Gérer les services Private Link pour sécuriser l'exposition des ressources et intégrer Azure App Service et Functions à des réseaux virtuels.
- Configurer la sécurité réseau pour App Service Environment et Azure SQL Managed Instance pour protéger des applications web et des bases de données.

Planifier et implémenter une sécurité avancée pour le calcul

- Améliorer la sécurité des ressources de calcul Azure contre les vulnérabilités et les attaques à l'aide de mesures avancées.
- Sécuriser l'accès à distance via Azure Bastion et l'accès aux machines virtuelles JIT et implémenter l'isolation réseau pour AKS.
- Renforcer la sécurité des clusters AKS, monitorer Azure Container Instances et Azure Container Apps et gérer l'accès à Azure Container Registry.
- Implémenter des méthodes de chiffrement de disque comme ADE et gérer l'accès aux API en toute sécurité dans Gestion des API Azure.

Planifier et implémenter la sécurité pour le stockage

- Développer des stratégies de sécurité pour des ressources de stockage Azure, ce qui permet une protection des données pendant le repos et le transit.
- Gérer l'accès au compte de stockage avec un contrôle d'accès efficace et une gestion de cycle de vie sécurisée des clés.
- Adapter des méthodes d'accès pour Azure Files, Stockage Blob, Tables et Files d'attente à des cas d'usage spécifiques.
- Renforcer la sécurité des données avec la suppression réversible, les sauvegardes, le contrôle de version, le stockage immuable, BYOK et le chiffrement double.

Planifier et implémenter la sécurité pour Azure SQL Database et Azure SQL Managed Instance

- Implémenter la sécurité pour Azure SQL Managed Instance afin de protéger les données sensibles.
- Utiliser Microsoft Enterprise Identity pour l'authentification de base de données et réaliser un audit de base de données à des fins de conformité.
- Utiliser Microsoft Purview pour la gouvernance et la classification des données afin de protéger les informations sensibles.
- Appliquer le masquage dynamique et le chiffrement TDE (Transparent Data Encryption), et recommander Always Encrypted pour la protection des données côté client.

Planifier, implémenter et gérer la gouvernance pour la sécurité

- Appliquer la conformité en utilisant Azure Policy pour créer et gérer des stratégies de sécurité.
- Simplifier le déploiement d'une infrastructure sécurisée avec Azure Blueprint.
- Utiliser des zones d'atterrissage pour une sécurité Azure cohérente et gérer les données sensibles avec Azure Key Vault.
- Améliorer la sécurité des clés avec des recommandations sur les HSM, un contrôle d'accès efficace, et des processus pour effectuer des rotations de clés et des sauvegardes régulières.

Gérer la posture de sécurité en utilisant Microsoft Defender pour le cloud

- Utiliser le degré de sécurisation de Microsoft Defender pour le cloud et l'inventaire pour identifier et atténuer les risques de sécurité, ce qui améliore la posture globale de sécurité.
- Évaluer et aligner des infrastructures de sécurité au moyen de Microsoft Defender pour le cloud pour garantir la conformité aux normes de sécurité et aux meilleures pratiques.
- Intégrer des normes sectorielles et réglementaires spécifiques à Microsoft Defender pour le cloud pour une conformité personnalisée.
- Connecter des environnements hybrides et multiclouds à Microsoft Defender pour le cloud pour une gestion centralisée de la sécurité et surveiller des ressources externes afin de les protéger contre les menaces externes.

Configurer et gérer la protection contre les menaces en utilisant Microsoft Defender pour le cloud

- Utiliser Azure Monitor pour une supervision complète des événements de sécurité cloud.
- Agréger efficacement différentes données de sécurité avec des connecteurs de données dans Microsoft Sentinel.
- Détecter les menaces en utilisant des règles d'analyse personnalisées dans Microsoft Sentinel.
- Évaluer et automatiser les réponses aux incidents dans Microsoft Sentinel pour une gestion améliorée de la sécurité.

Configurer et gérer des solutions de supervision et d'automatisation de la sécurité

- Utiliser Azure Monitor pour un monitoring efficace des événements de sécurité dans des environnements cloud.
- Implémenter des connecteurs de données dans Microsoft Sentinel pour une collecte complète des données de sécurité.
- Développer des règles d'analytique personnalisées dans Microsoft Sentinel pour la détection ciblée des menaces.
- Évaluer et automatiser les réponses aux incidents de sécurité dans Microsoft Sentinel pour améliorer l'efficacité du flux de travail.

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 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 recommandé, 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 : 4 jours (28 heures)

INTERLOCUTEURS : Administrateurs, IT Pro, Responsables sécurité

NIVEAU : Intermédiaire