Microsoft Architecte cybersécurité (SC-100)

Référence : **MSSC100** Durée : **4 jours** Certification : **SC-100**

CONNAISSANCES PREALABLES

• 1-Posséder une expérience et des connaissances avancées en matière d'accès et d'identités, de protection des plates-formes, d'opérations de sécurité, de sécurisation des données et des applications. • 2-Être familiarisé avec les implémentations hybrides et cloud. • 3-Il est conseillé d'avoir passé une certification dans les domaines de la sécurité, de la conformité et de l'identité (par exemple AZ-500, SC-200 ou SC-300). • 4-Avoir des connaissances de base en langue anglaise car le support de cours est en anglais et les ateliers seront réalisés sur des VM en anglais.

PROFIL DES STAGIAIRES

• Ingénieurs de sécurité cloud expérimentés.

OBJECTIFS

• Être capable de concevoir une stratégie et une architecture Confiance zéro. • Savoir évaluer les stratégies techniques et les stratégies d'opérations de sécurité des Risques conformité en matière de gouvernance (GRC). • Comprendre comment concevoir la sécurité pour l'infrastructure. • Apprendre à concevoir une stratégie de données et d'applications.

CERTIFICATION PREPAREE

- Microsoft Cybersecurity Architect. Cette formation entre en jeu dans le cursus de certification Microsoft Certified Cybersecurity Architect Expert

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité Microsoft

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Générer une stratégie de sécurité globale et une architecture

- Vue d'ensemble de la Confiance Zéro
- Développer des points d'intégration dans une architecture
- Développer des exigences de sécurité en fonction des objectifs métier
- Translater les exigences de sécurité en fonctionnalités
- Concevoir la sécurité pour une stratégie de résilience
- Concevoir une stratégie de sécurité pour les environnements hybrides et multi-abonnés
- Concevoir des stratégies techniques et de gouvernance pour le filtrage et la segmentation du trafic
- Comprendre la sécurité des protocoles

Concevoir une stratégie d'opérations de sécurité

- Comprendre les infrastructures, processus et procédures des opérations de sécurité

- Concevoir une stratégie de sécurité de la journalisation et de l'audit
- Développer des opérations de sécurité pour les environnements hybrides et multiclouds
- Concevoir une stratégie pour Security Information and Event Management (SIEM) et l'orchestration de la sécurité
- Évaluer les workflows de la sécurité
- Consulter des stratégies de sécurité pour la gestion des incidents
- Évaluer la stratégie d'opérations de sécurité pour partager les renseignements techniques sur les menaces
- Analyser les sources pour obtenir des informations sur les menaces et les atténuations

Concevoir une stratégie de sécurité des identités

- Sécuriser l'accès aux ressources cloud
- Recommander un magasin d'identités pour la sécurité
- Recommander des stratégies d'authentification sécurisée et d'autorisation de sécurité
- Sécuriser l'accès conditionnel
- Concevoir une stratégie pour l'attribution de rôle et la délégation
- Définir la gouvernance des identités pour les révisions d'accès et la gestion des droits d'utilisation
- Concevoir une stratégie de sécurité pour l'accès des rôles privilégiés à l'infrastructure
- Concevoir une stratégie de sécurité pour des activités privilégiées
- Comprendre la sécurité des protocoles

Évaluer une stratégie de conformité réglementaire

- Interpréter les exigences de conformité et leurs fonctionnalités techniques
- Évaluer la conformité de l'infrastructure à l'aide de Microsoft Defender pour le cloud
- Interpréter les scores de conformité et recommander des actions pour résoudre les problèmes ou améliorer la sécurité
- Concevoir et valider l'implémentation de Azure Policy
- Conception pour les exigences de résidence des données
- Translater les exigences de confidentialité en exigences pour les solutions de sécurité

Évaluer la posture de sécurité et recommander des stratégies techniques pour gérer les risques

- Évaluer les postures de sécurité à l'aide de points de référence
- Évaluer les postures de sécurité à l'aide de Microsoft Defender pour le cloud
- Évaluer les postures de sécurité à l'aide du niveau de sécurité
- Évaluer l'hygiène de sécurité des charges de travail cloud
- Conception de la sécurité d'une zone d'atterrissage Azure
- Interpréter les renseignements techniques sur les menaces et recommander des atténuations des risques
- Recommander des fonctionnalités de sécurité ou des contrôles pour atténuer les risques identifiés

Comprendre les meilleures pratiques relatives à l'architecture et comment elles changent avec le cloud

- Planifier et implémenter une stratégie de sécurité entre les équipes
- Établir une stratégie et un processus pour une évolution proactive et continue d'une stratégie de sécurité
- Comprendre les protocoles réseau et les meilleures pratiques pour la segmentation du réseau et le filtrage du trafic

Concevoir une stratégie pour sécuriser les points de terminaison serveur et client

- Spécifier des lignes de base de sécurité pour les points de terminaison serveur et client
- Spécifier les exigences de sécurité pour les serveurs
- Spécifier les exigences de sécurité pour les appareils mobiles et les clients
- Spécifier les exigences pour la sécurisation de Active Directory Domain Services
- Concevoir une stratégie pour gérer les secrets, les clés et les certificats
- Concevoir une stratégie pour sécuriser l'accès à distance
- Comprendre les infrastructures, processus et procédures des opérations de sécurité
- Comprendre les procédures forensiques approfondies par type de ressource

Concevoir une stratégie de sécurisation des services PaaS, IaaS et SaaS

- Spécifier des lignes de base de sécurité pour les services PaaS, IaaS et SaaS
- Déterminer les exigences de sécurité pour les charges de travail IoT
- Spécifier les exigences de sécurité pour les charges de travail données
- Définir les exigences de sécurité pour les charges de travail web
- Désigner les exigences de sécurité pour les charges de travail de stockage
- Définir les exigences de sécurité pour les conteneurs
- Spécifier les exigences de sécurité pour l'orchestration des conteneurs

Spécifier les exigences de sécurité pour les applications

- Comprendre la modélisation des menaces sur les applications
- Spécifier des priorités pour atténuer les menaces sur les applications
- Définir une norme de sécurité pour l'intégration d'une nouvelle application
- Désigner une stratégie de sécurité pour les applications et les API

Concevoir une stratégie de sécurisation des données

- Classer par ordre de priorité l'atténuation des menaces sur les données
- Concevoir une stratégie pour identifier et protéger les données sensibles
- Spécifier une norme de chiffrement pour les données au repos et en mouvement

Certification Microsoft Cybersecurity Architect

- Cette formation prépare au passage de la certification Microsoft Cybersecurity Architect

*Notre **référent handicap** se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.*