Programme de formation SC-100 : Microsoft Cybersecurity Architect

(Préparation certification Microsoft SC-100)

DESCRIPTION DE LA FORMATION :

Cette formation vous permettra d'acquérir les compétences nécessaires pour concevoir et évaluer des stratégies de cybersécurité dans les divers domaines tels que : Zéro Trust, gouvernance, risque et conformité (GRC), SecOps, et données et applications. Vous appendrez également à concevoir et à architecturer des solutions en utilisant les principes Zéro Trust et à spécifier les exigences de sécurité pour l'infrastructure du cloud dans différents modèles de services (SaaS, PaaS, IaaS).

OBJECTIFS PEDAGOGIQUES :

A l'issue de cette formation, les participants auront la capacité de :

- Générer une stratégie et une architecture de sécurité globale
- Concevoir une stratégie d'opération de sécurité
- Concevoir une stratégie de sécurité des identités
- Évaluer une stratégie de conformité réglementaire
- Évaluer la posture de sécurité et recommander des stratégies techniques pour gérer les risques
- Comprendre les bonnes pratiques en matière d'architecture et les changements avec le cloud
- Concevoir une stratégie pour sécuriser les points de terminaison serveur et client
- Concevoir une stratégie de sécurisation des services PaaS, IaaS et SaaS
- Spécifier les exigences de sécurité pour les applications
- Concevoir une stratégie de sécurisation des données
- Recommander les bonnes pratiques de sécurité en utilisant Microsoft Cybersecurity Reference Architectures (MCRA) et Microsoft Cloud Security Benchmarks
- Recommander une méthodologie sécurisée à l'aide du Cloud Adoption Framework (CAF)
- Recommander une stratégie face aux ransomwares conformément aux meilleures pratiques de sécurité Microsoft

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 formateur expérimenté 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 :

Générer une stratégie et une architecture de sécurité globale

- Développer des points d'intégration dans une architecture.
- Développer des exigences de sécurité en fonction des objectifs métier.
- Traduire les exigences de sécurité en fonctionnalités techniques.
- 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.

Concevoir une stratégie d'opération 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 Security Orchestration, Automation, and Response (SOAR).
- Évaluer les workflows de sécurité.
- Consulter des stratégies de sécurité pour la gestion des incidents.
- Évaluer les opérations de sécurité pour le renseignement technique sur les menaces.
- Superviser des sources pour obtenir des insights sur les menaces et les atténuations.

Concevoir une stratégie de sécurité des identités

- 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 accès privilégiés.

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 d'Azure Policy.
- Concevoir pour les exigences de résidence des données.
- Traduire 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.
- Concevoir 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.

Comprendre les bonnes pratiques en matière d'architecture et comment elles changent avec le cloud

- Planifier et implémenter une stratégie de sécurité parmi les équipes.
- Établir une stratégie et un processus pour une évolution proactive et continue d'une stratégie de sécurité.

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

- 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 Security Orchestration, Automation, and Response (SOAR).
- Évaluer les workflows de sécurité.
- Consulter des stratégies de sécurité pour la gestion des incidents.
- Évaluer les opérations de sécurité pour le renseignement technique sur les menaces.
- Superviser des sources pour obtenir des insights sur les menaces et les atténuations.

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

- Spécifier des bases de référence de sécurité pour les services SaaS, PaaS et IaaS.
- Spécifier des exigences de sécurité pour les charges de travail web, de stockage, de données et d'IoT.
- Spécifier des exigences de sécurité pour les conteneurs et l'orchestration des conteneurs.

Spécifier les exigences de sécurité pour les applications

- Spécifier des priorités pour atténuer les menaces sur les applications.
- Spécifier une norme de sécurité pour l'intégration d'une nouvelle application.
- Spécifier une stratégie de sécurité pour les applications et les API.

Concevoir une stratégie de sécurisation des données

- Spécifier des priorités pour atténuer les 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.

Recommander les bonnes pratiques de sécurité en utilisant Microsoft Cybersecurity

- Utiliser Microsoft Cybersecurity Reference Architectures pour recommander les bonnes pratiques de sécurité.
- Utiliser Microsoft Cloud Security Benchmarks pour recommander les bonnes pratiques de sécurité.
- Utiliser le plan de modernisation rapide Confiance Zéro pour recommander une stratégie de mise à jour de la sécurité organisationnelle.

Recommander une méthodologie sécurisée à l'aide du Cloud Adoption Framework (CAF)

- Recommander un processus DevSecOps.
- Recommander une méthodologie pour la protection des ressources.
- Recommander des stratégies de gestion et de réduction des risques.

Recommander une stratégie face aux ransomwares conformément aux meilleures pratiques de sécurité Microsoft

- Reconnaître les différents types de ransomware.
- Aider une organisation à atténuer le risque d'attaque par ransomware en créant un plan de récupération.
- Aider une organisation à atténuer les risques d'attaque par ransomware en limitant l'étendue des dommages.
- Aider une organisation à atténuer les risques d'attaque par ransomware en renforçant des éléments d'infrastructure clés.

PRÉREQUIS :

Pour participer à cette formation, Il faut avoir préalablement suivi la formation « SC-900 : Microsoft Security, Compliance, and Identity Fundamentals »

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

PRE-CERTIFCIATION :

Cette formation prépare à l'examen de certification « Microsoft SC-100 : Microsoft Cybersecurity Architect »

DUREE : 4 jours (28 heures)

INTERLOCUTEURS : Opérateurs de sécurité

NIVEAU : Intermédiaire