Programme de cours
Architecte en cybersécurité Microsoft

Durée :	4 jours soit 28 heures	Référence :	SC-100T00

Public visé :

Pré-requis :

Cette formation est destinée :

- Aux professionnels de l'informatique avec une expérience et des connaissances avancées dans un large éventail de domaines de l'ingénierie de la sécurité, notamment l'accès et les identités, la protection des plateformes, les opérations de sécurité, la sécurisation des données et la sécurisation des applications. Ils doivent également être familiarisés avec les implémentations hybrides et cloud.

Objectifs pédagogiques :

Cette formation prépare les apprenants avec une expérience en conception et en évaluation des stratégies de cybersécurité dans les domaines suivants : Confiance zéro, Risques conformité en matière de gouvernance (GRC), opérations de sécurité (SecOps) et données et applications. Les participants apprendront également à concevoir l'architecture des solutions à l'aide de principes de confiance zéro et à spécifier des exigences de sécurité pour l'infrastructure cloud dans différents modèles de service (SaaS, PaaS, IaaS).

Compétences obtenues

- Concevoir une stratégie et une architecture Confiance zéro
- Évaluer les stratégies techniques et les stratégies d'opérations de sécurité des Risques conformité en matière de gouvernance (GRC)
- Concevoir la sécurité pour l'infrastructure
- Concevoir une stratégie de données et d'applications

Compétences acquises à l'issue de la formation :

- Concevoir une stratégie et une architecture Confiance zéro
- Évaluer les stratégies techniques et les stratégies d'opérations de sécurité des Risques conformité en matière de gouvernance (GRC)
- Concevoir la sécurité pour l'infrastructure
- Concevoir une stratégie de données et d'applications

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure.
La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz.
L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration.
En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Moyens et supports pédagogiques :

Cadre présentiel
Salles de formation équipées et accessibles aux personnes à mobilité réduite.
- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection sur tableau blanc
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel
Session dispensée via notre solution iClassroom s'appuyant sur Microsoft Teams.
- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Informations sur l'accessibilité :

Programme de cours
Architecte en cybersécurité Microsoft

Description / Contenu

Module 1 : générer une stratégie de sécurité globale et une architecture

- Introduction
- 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 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
- Comprendre la sécurité des protocoles
- Exercice : générer une stratégie de sécurité globale et une architecture
- Contrôle des connaissances
- Récapitulatif

Module 2 : concevoir une stratégie d'opérations de sécurité

- Introduction
- 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

Module 3 : concevoir une stratégie de sécurité des identités

- Introduction
- 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

Module 4 : évaluer une stratégie de conformité réglementaire

- Introduction
- 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

Module 5 : évaluer la posture de sécurité et recommander des stratégies techniques pour gérer les risques

- Introduction
- 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

Module 6 : comprendre les meilleures pratiques relatives à l'architecture et comment elles changent avec le cloud

- Introduction
- 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

Module 7 : concevoir une stratégie pour sécuriser les points de terminaison serveur et client

- Introduction
- 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

Module 8 : concevoir une stratégie de sécurisation des services PaaS, IaaS et SaaS

- Introduction
- Spécifier des lignes de base de sécurité pour les services PaaS
- Spécifier des lignes de base de sécurité pour les services IaaS
- Spécifier des lignes de base de sécurité pour les services SaaS
- Spécifier les exigences de sécurité pour les charges de travail IoT
- Spécifier les exigences de sécurité pour les charges de travail données
- Spécifier les exigences de sécurité pour les charges de travail web
- Spécifier les exigences de sécurité pour les charges de travail de stockage
- Spécifier les exigences de sécurité pour les conteneurs

- Spécifier les exigences de sécurité pour l'orchestration des conteneurs

Module 9 : spécifier les exigences de sécurité pour les applications

- Introduction
- Comprendre la modélisation des menaces sur 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

Module 10 : concevoir une stratégie de sécurisation des données

- Introduction
- 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