Programme de cours
SC-100T00

Durée :	4 jours soit 28 heures	Référence :	Architecte en cybersécurité de Microsoft

Public visé :

Cette formation est destinée aux professionnels de l'informatique ayant une expérience et des connaissances avancées dans un large éventail de domaines d'ingénierie de la sécurité, notamment l'identité et l'accès, la protection des plateformes, les opérations de sécurité, la sécurisation des données et la sécurisation des applications. Ils doivent également avoir une expérience des mises en œuvre hybrides et Cloud.

Pré-requis :

Pour suivre cette formation les apprenants doivent avoir :

- De l'expérience et des connaissances avancées dans les domaines de l'identité et de l'accès, de la protection des plateformes, des opérations de sécurité, de la sécurisation des données et de la sécurisation des applications.
- De l'expérience avec les implémentations hybrides et cloud.

Objectifs pédagogiques :

A l'issue de la formation les apprenants auront acquis les compétences suivantes :

- Concevoir une stratégie et une architecture Zero Trust
- Évaluer les stratégies techniques de gouvernance et de conformité aux risques (GRC) et les stratégies d'opérations de sécurité
- Conception de la sécurité pour l'infrastructure
- Concevoir une stratégie pour les données et les 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

Modalités d'évaluation et suivi :

Avant
Afin de valider le choix d'un programme de formation, une évaluation des prérequis est réalisée à l'aide d'un questionnaire en ligne ou lors d'un échange avec le formateur(trice) qui validera la base de connaissances nécessaires.
Pendant
Après chaque module théorique, un ou des ateliers pratiques permettent la validation de l'acquisition des connaissances. Un Quizz peut accompagner l'atelier pratique.
Après
Un examen de certification si le programme de formation le prévoit dans les conditions de l'éditeur ou du centre de test (TOSA, Pearson Vue, ENI, PeopleCert)
Enfin
Un questionnaire de satisfaction permet au participant d'évaluer la qualité de la prestation.

Description / Contenu

Module 1 : Élaborer une stratégie et une architecture de sécurité globales

- Introduction
- Présentation de Zero Trust
- Développer des points d'intégration dans une architecture
- Élaborer des exigences de sécurité en fonction des objectifs commerciaux
- Traduire les exigences de sécurité en capacités techniques
- Concevoir la sécurité pour une stratégie de résilience
- Concevoir une stratégie de sécurité pour les environnements hybrides et multi-locataires
- Concevoir des stratégies techniques et de gouvernance pour le filtrage et la segmentation du trafic
- Comprendre la sécurité des protocoles
- Exercice : Construire une stratégie et une architecture de sécurité globales
- Vérification des connaissances
- Résumé

Module 2 : Concevoir une stratégie d'opérations de sécurité

- Introduction
- Comprendre les cadres, les processus et les procédures des opérations de sécurité
- Concevoir une stratégie de sécurité de journalisation et d'audit
- Développer des opérations de sécurité pour les environnements hybrides et multi-cloud
- Concevoir une stratégie pour la gestion des informations et des événements de sécurité (SIEM) et l'orchestration de la sécurité,
- Évaluer les workflows de sécurité
- Examiner les stratégies de sécurité pour la gestion des incidents
- Évaluer la stratégie des opérations de sécurité pour le partage de renseignements techniques sur les menaces
- Surveiller les sources pour obtenir des informations sur les menaces et les atténuations

Module 3 : Concevoir une stratégie de sécurité des identités

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

Module 4 : Évaluer une stratégie de conformité réglementaire

- Introduction
- Interpréter les exigences de conformité et leurs capacités techniques
- Évaluer la conformité de l'infrastructure à l'aide de Microsoft Defender for Cloud
- Interpréter les scores de conformité et recommander des actions pour résoudre les problèmes ou améliorer la sécurité
- Concevoir et valider la mise en œuvre d'Azure Policy
- Conception pour la résidence des données
- Traduire 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 en utilisant des benchmarks
- Évaluer les postures de sécurité à l'aide de Microsoft Defender pour le cloud
- Évaluer les postures de sécurité à l'aide de Secure Scores
- Évaluer l'hygiène de sécurité des charges de travail cloud
- Conception de la sécurité pour une Azure Landing Zone
- Interpréter les renseignements techniques sur les menaces et recommander des mesures d'atténuation des risques
- Recommander des capacités ou des contrôles de sécurité pour atténuer les risques identifiés

Module 6 : Comprendre les bonnes pratiques en matière d'architecture et leur évolution avec le Cloud

- Introduction
- Planifier et mettre en œuvre une stratégie de sécurité dans toutes les équipes
- Établir une stratégie et un processus d'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 de sécurisation des terminaux serveur et client

- Introduction
- Spécifier les lignes de base de sécurité pour les terminaux 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 des services de domaine Active Directory
- Concevoir une stratégie pour gérer les secrets, les clés et les certificats
- Concevoir une stratégie pour un accès à distance sécurisé
- Comprendre les cadres, les processus et les procédures des opérations de sécurité
- Comprendre les procédures d'investigation approfondie par type de ressource

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

- Introduction
- Spécifier les lignes de base de sécurité pour les services PaaS
- Spécifier les lignes de base de sécurité pour les services IaaS
- Spécifier les 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 de 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 applicatives
- Spécifier les priorités pour atténuer les menaces aux 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
- Donner la priorité à l'atténuation des menaces pesant 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