Architecte de Cybersécurité Microsoft (SC-100T00)

Durée: 4 jours
Public cible: Professionnel TI

À qui s'adresse cette formation ?

Ce cours est destiné aux ingénieurs de sécurité cloud expérimentés qui ont effectué une certification précédente dans le portefeuille de sécurité, de conformité et d'identité. En particulier, vous devez avoir une expérience et des connaissances avancées dans un large éventail de domaines de l'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. Vous devez également être familiarisés avec les implémentations hybrides et cloud. Les étudiants débutants doivent plutôt suivre le cours SC-900 : Principes de base de la sécurité, de la conformité et de l'identité Microsoft.

Objectifs de la formation

- Concevoir une stratégie et une architecture Zero Trust : Apprendre à créer des environnements sécurisés basés sur les principes de la confiance zéro.
- Sécuriser l'infrastructure : Développer des stratégies pour protéger les infrastructures IT contre les menaces.
- Sécuriser les données et les applications : Élaborer des plans pour la protection des données et des applications dans divers environnements cloud.
- Recommander les meilleures pratiques et priorités en matière de sécurité : Identifier et conseiller sur les meilleures pratiques pour renforcer la sécurité.
- Évaluer les stratégies de gouvernance, de risques et de conformité (GRC) : Analyser et gérer les risques, assurer la conformité aux réglementations et gouverner les politiques de sécurité.
- Opérations de sécurité (SecOps) : Mettre en place et gérer les opérations de sécurité pour protéger les infrastructures et les données.

Description sommaire

Il s'agit d'un cours avancé de niveau expert. Bien qu'il ne soit pas nécessaire de participer, vous êtes vivement encouragés à avoir effectué et passé une autre certification de niveau associé dans le

portefeuille de sécurité, de conformité et d'identité (par exemple, AZ-500, SC-200 ou SC-300) avant d'assister à cette classe. Ce cours prépare les étudiants avec une expertise 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. Vous apprendrez 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).

Contenu du plan de cours

Parcours d'apprentissage 1 : Concevoir des solutions alignées avec les meilleures pratiques et priorités en matière de sécurité

- Introduction à Zero Trust et aux cadres de meilleures pratiques
- Concevoir des solutions alignées avec le Cloud Adoption Framework (CAF) et le Well-Architected Framework (WAF)
- Concevoir des solutions alignées avec la Microsoft Cybersecurity Reference Architecture (MCRA) et le Microsoft Cloud Security Benchmark (MCSB)
- Concevoir une stratégie de résilience face à des cybermenaces courantes comme les ransomwares
- Étude de cas 1

Parcours d'apprentissage 2 : Concevoir des capacités d'opérations, d'identité et de conformité en matière de sécurité

- Concevoir des solutions pour la conformité réglementaire
- Concevoir des solutions pour la gestion des identités et des accès
- Concevoir des solutions pour sécuriser l'accès privilégié
- Concevoir des solutions pour les opérations de sécurité
- Étude de cas 2

Parcours d'apprentissage 3 : Concevoir des solutions de sécurité pour les applications et les données

- Concevoir des solutions pour sécuriser Microsoft 365
- Concevoir des solutions pour sécuriser les applications
- Concevoir des solutions pour sécuriser les données d'une organisation
- Étude de cas 3

Parcours d'apprentissage 4 : Concevoir des solutions de sécurité pour l'infrastructure

- Spécifier les exigences pour sécuriser les services SaaS, PaaS et IaaS
- Concevoir des solutions pour la gestion de la posture de sécurité

Approche et méthode pédagogique

Approche pratique et structurée combinant théorie ciblée et ateliers guidés.

Les participants développent progressivement une expertise d’architecte en cybersécurité Microsoft à travers des exercices concrets inspirés de scénarios professionnels, favorisant une mise en application immédiate des apprentissages. Ils apprennent à concevoir des stratégies de sécurité globales, intégrer les solutions Microsoft et mettre en place des architectures de sécurité robustes, alignées sur les meilleures pratiques et les exigences de conformité.

Animée par un formateur certifié Microsoft, la formation privilégie l’interactivité et le développement de compétences stratégiques et techniques directement transférables pour sécuriser efficacement les environnements en contexte professionnel.

Prérequis

- Connaissance conceptuelle des stratégies de sécurité, des exigences, de l'architecture de Confiance zéro et de la gestion des environnements hybrides.
- Expérience pratique avec les stratégies de Confiance zéro, l'application de stratégies de sécurité et le développement d'exigences de sécurité en fonction des objectifs métier.

Recommandations

- Solides connaissances en cybersécurité (principes, menaces, gestion des risques)
- Expérience avec les solutions Microsoft Security (Defender, Sentinel, Entra ID, Purview)
- Compréhension des concepts cloud (Azure, Microsoft 365)
- Notions d’architecture et gouvernance de sécurité
- Expérience en administration ou ingénierie sécurité (fortement recommandée)