Microsoft Cybersecurity Architect (Microsoft SC-100)
Cours officiel SC-100, préparation à l'examen

Cours Pratique de 4 jours - 28h
Réf : SC1 - Prix 2024 : 2 790€ HT

Avec cette formation, vous disposerez d'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 serez en mesure de concevoir l'architecture des solutions à l'aide des principes de confiance zéro et à spécifier les exigences de sécurité pour l'infrastructure cloud dans différents modèles de service (SaaS, PaaS, IaaS).

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Concevoir une stratégie et une architecture Zero Trust

Concevoir la sécurité pour l'infrastructure

Concevoir une stratégie de sécurisation pour les données et les applications

Recommander les meilleures pratiques et les priorités en matière de sécurité

Évaluer les stratégies techniques de gouvernance et de conformité aux risques (GRC) et d'opérations de sécurité

MÉTHODES PÉDAGOGIQUES

Animation de la formation en français. Support de cours officiel au format numérique et en anglais. Bonne compréhension de l'anglais à l'écrit.

CERTIFICATION

L'obtention de l'une de ces certifications est fortement recommandée pour se présenter à l'examen SC-100 : AZ-500, SC-200 ou SC-300. La réussite de l'examen SC-100 permet d'obtenir la certification "Microsoft Certified Cybersecurity Architect Expert".

LE PROGRAMME

dernière mise à jour : 02/2023

1) Concevoir une stratégie et une architecture Zero Trust

- Créer une stratégie et une architecture de sécurité globale.
- Concevoir une stratégie d'opérations de sécurité.
- Concevoir une stratégie de sécurité des identités.

2) Évaluer les stratégies techniques de GRC et d'opérations de sécurité

- Évaluer une stratégie de conformité réglementaire.
- Évaluer la posture de sécurité et recommander des stratégies techniques pour gérer les risques.

3) Concevoir la sécurité de l'infrastructure

- Comprendre les meilleures pratiques en matière d'architecture de cybersécurité.
- Concevoir une stratégie de sécurisation des terminaux serveur et client
- Concevoir une stratégie de sécurisation des services PaaS, IaaS et SaaS.

4) Concevoir une stratégie de sécurité pour les données et les applications

- Spécifier les exigences de sécurité pour les applications.
- Concevoir une stratégie de sécurisation des données.

PARTICIPANTS

Ingénieurs de sécurité cloud expérimentés qui ont obtenu une certification précédente dans le portefeuille de sécurité, de conformité et d'identité.

PRÉREQUIS

Il s'agit d'un cours avancé de niveau expert. Il est fortement recommandé d'avoir suivi l'une des formations suivantes et obtenu la certification associée : AZ-500, SC-200 ou SC-300.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation…
À l'issue de chaque stage, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

5) Recommander les meilleures pratiques de sécurité

- Recommander les meilleures pratiques de sécurité à l'aide des architectures de référence de cybersécurité Microsoft.
- Recommander les meilleures pratiques de sécurité à l'aide des références de sécurité Microsoft Cloud.
- Recommander une méthodologie sécurisée à l'aide du Cloud Adoption Framework (CAF).
- Recommander une stratégie de protection contre les ransomwares.

LES DATES

CLASSE À DISTANCE
2024 : 09 juil., 08 oct.