Architecte en cybersécurité Microsoft

Conception et sécurisation des systèmes avec Microsoft

Présentiel ou en classe à distance

Durée : 4 jours (28 h)
+ activité à distance

Réf. : MSSC100

Prix inter : 2.695,00 € HT

Forfait intra : 6.795,00 € HT

Formation officielle

Cette formation prépare à la certification Microsoft Certified: Cybersecurity Architect Expert.

Les objectifs de la formation

- Être capable de concevoir une stratégie et une architecture Confiance zéro
- Savoir évaluer les stratégies techniques et les stratégies d'opérations de sécurité des Risques conformité en matière de gouvernance (GRC)
- Comprendre comment concevoir la sécurité pour l'infrastructure
- Apprendre à concevoir une stratégie de données et d'applications

A qui s'adresse cette formation ?

Pour qui

- Ingénieurs de sécurité cloud expérimentés

Prérequis

- Posséder une expérience et des connaissances avancées en matière d'accès et d'identités, de protection des plates-formes, d'opérations de sécurité, de sécurisation des données et des applications
- Être familiarisé avec les implémentations hybrides et cloud
- Il est conseillé d'avoir passé une certification dans les domaines de la sécurité, de la conformité et de l'identité (par exemple AZ-500, SC-200 ou SC-300)
- Disposez-vous des compétences nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Générer une stratégie de sécurité globale et une architecture

- 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
- 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

2 - Concevoir une stratégie d'opérations de sécurité

- 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

3 - Concevoir une stratégie de sécurité des identités

- 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

4 - 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 de Azure Policy
- Conception pour les exigences de résidence des données
- Translater les exigences de confidentialité en exigences pour les solutions de sécurité

5 - 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
- 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

6 - Comprendre les meilleures pratiques relatives à l'architecture et comment elles changent

avec le cloud

- 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

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

- 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

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

- Spécifier des lignes de base de sécurité pour les services PaaS, IaaS et SaaS
- Déterminer les exigences de sécurité pour les charges de travail IoT
- Spécifier les exigences de sécurité pour les charges de travail données
- Définir les exigences de sécurité pour les charges de travail web
- Désigner les exigences de sécurité pour les charges de travail de stockage
- Définir les exigences de sécurité pour les conteneurs
- Spécifier les exigences de sécurité pour l'orchestration des conteneurs

9 - Spécifier les exigences de sécurité pour les applications

- Comprendre la modélisation des menaces sur les applications
- Spécifier des priorités pour atténuer les menaces sur les applications
- Définir une norme de sécurité pour l'intégration d'une nouvelle application
- Désigner une stratégie de sécurité pour les applications et les API

10 - Concevoir une stratégie de sécurisation des données

- 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

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Cette formation de niveau avancé permet aux participants d'approfondir leur connaissances et compétences au métier d'architecte en cybersécurité.
- Le partage d'expérience de consultants expérimentés.
- La qualité d'une formation officielle Microsoft (support de cours numérique en anglais).

Dates et villes 2024 - Référence MSSC100

Nancy

du 21 mai au 24 mai

Tours

du 21 mai au 24 mai

Toulouse

du 21 mai au 24 mai

Strasbourg

du 21 mai au 24 mai

Sophia Antipolis

du 21 mai au 24 mai

Rouen

du 21 mai au 24 mai

Rennes

du 21 mai au 24 mai

Paris

du 21 mai au 24 mai Session garantie | du 9 sept. au 12 sept. | du 2 déc. au 5 déc.

Nantes

du 21 mai au 24 mai

A distance

du 21 mai au 24 mai Session garantie | du 9 sept. au 12 sept. | du 2 déc. au 5 déc.

Montpellier

du 21 mai au 24 mai

Marseille

du 21 mai au 24 mai

Lyon

du 21 mai au 24 mai

Lille

du 21 mai au 24 mai

Grenoble

du 21 mai au 24 mai

Bordeaux

du 21 mai au 24 mai

Aix-en-Provence

du 21 mai au 24 mai