+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 17/12/2024

S'inscrire

Formation Certification SC-100©

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

4 jours (28 heures)

Présentation

Dans un monde où les pirates informatiques sont très créatifs, investissez dans la cybersécurité pour assurer un avenir serein à votre entreprise. Avec la certification Microsoft Cybersecurity Architect (SC-100)© vous pourrez prouver vos compétences dans le domaine de la sécurité.

Durant la formation, vous explorerez la sécurisation des identités et des accès avec Azure Active Directory, la protection des données avec Azure Information Protection, ainsi que la gestion des menaces avec Microsoft Defender.

Cette certification développe vos compétences dans la conception et la mise en œuvre de solutions de cybersécurité basées sur les technologies Microsoft, vous dotant ainsi des connaissances nécessaires pour protéger efficacement vos environnements informatiques contre les menaces.

Boostez votre carrière grâce à cette formation spécialisée qui vous assurera de nouvelles opportunités. Nous vous préparerons au mieux pour le passage de l'examen organisé par Microsoft.

Objectifs

- Créer des opérations de sécurité efficaces
- Préparer le passage à l'examen SC-100©
- Maîtriser la mise en place de stratégie de sécurité

Public visé

- Consultant en cybersécurité
- Auditeurs
- Analyste cybersécurité
- Ingénieurs Cloud

Pré-requis

- Expérience pratique dans le domaine de la sécurité informatique
- Bonne compréhension des technologies Microsoft Azure

Note : Ambient IT n’est pas propriétaire de Microsoft Cybersecurity Architect (SC-100)©, cette certification appartient à Microsoft©, Inc.

Programme de notre formation SC-100®

Conception d'une stratégie et d'une architecture de sécurité globale

- Présentation du Zero Trust
- Développer des points d'intégration dans une architecture
- Développer des exigences de sécurité basées sur les 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 aspects techniques et des stratégies de gouvernance pour le filtrage et la segmentation du trafic
- Comprendre la sécurité des protocoles

Créer une stratégie d'opérations de sécurité

- Processus et 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 de gestion des informations et des événements de sécurité (SIEM)
- Évaluer workflows de sécurité
- Examiner les stratégies de sécurité pour la gestion des incidents
- Évaluer la stratégie des opérations de sécurité pour partager des renseignements techniques sur les menaces
- Surveiller les sources pour obtenir des informations sur les menaces et les mesures d'atténuation

Créer une stratégie de sécurité des identités

- Accès sécurisé aux ressources cloud
- Recommander un magasin d'identités pour la sécurité
- Recommander des stratégies d'authentification et d'autorisation de sécurité sécurisées
- Accès conditionnel sécurisé
- Concevoir une stratégie d'attribution et de délégation de rôles

Évaluer une stratégie de conformité réglementaire

- Suivre le cycle de vie des exigences
- Surveiller le progrès des exigences
- Mettre à jour les statuts des exigences
- Communiquer le statut des exigences
- Gérer les changements des exigences

Pratiques d'architecture du Cloud

- Accès sécurisé aux ressources cloud
- Recommander un magasin d'identités pour la sécurité
- Recommander des stratégies d'authentification et d'autorisation de sécurité sécurisées
- Accès conditionnel sécurisé
- Concevoir une stratégie d'attribution et de délégation de rôles

Stratégie de sécurisation des données

- Prioriser 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

Posture de sécurité et stratégies techniques

- Évaluer les postures de sécurité à l'aide de références
- Évaluer les postures de sécurité à l'aide de Microsoft Defender for Cloud
- Évaluer les postures de sécurité à l'aide des scores sécurisés
- Évaluer l'hygiène de sécurité des charges de travail cloud
- Concevoir la sécurité pour une zone d'atterrissage Azure
- Interpréter les informations techniques sur les menaces
- Recommander des capacités ou des contrôles de sécurité

Exigences de sécurité des applications

- Comprendre la modélisation des menaces applicatives
- Spécifier les priorités pour atténuer les menaces pesant 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

Stratégie de sécurisation des points de terminaison des serveurs et des clients

- Spécifier les lignes de base de sécurité pour les points de terminaison serveur et client

- Spécifier les exigences
  - de sécurité pour les appareils mobiles et les clients
  - de sécurité pour les serveurs
  - pour sécuriser les services de domaine Active Directory
- Comprendre les cadres, processus et procédures des opérations de sécurité
- Comprendre les procédures d'investigation approfondie par type de ressource

Stratégies pour réussir l'examen

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.