Organisme de formation professionnelle continue
Numero agrément 91 30 03332 30
France : +33 (0)188 24 70 33 / 34
Site : www.oo2.fr
Mail : contact@oo2.fr

Microsoft : les fondamentaux de la sécurité, de la conformité et de l'identité (SC-900)

Date et durée

Code formation : SC-900T00
Durée : 1 jour
Nombre d'heures : 7 heures

Formation avec certification

Security, Compliance and Identity Fundamentals

Description

Destinée principalement aux professionnel de l'informatique, cette formation vous permettra de découvrir et de **comprendre les différents éléments de cybersécurité** présents dans les produits et les services de Microsoft. Elle est indispensable pour obtenir d'autres certifications axées sur des rôles spécifiques, telles que l'architecte en cybersécurité, l'administrateur des identités et des accès Microsoft ou l'administrateur de la protection de l'information et de la conformité Microsoft 365.
Le programme comprend 4 modules consacrés aux **principes de sécurité et de conformité de Microsoft**, ainsi qu'aux fonctions de gestion des identités et des accès. Ainsi, vous aborderez à la fois les services de base et les différents types d'identité d'Azure AD, mais aussi les processus d'authentification et de gestion des accès, ou encore la protection et la gouvernance. Enfin, vous vous familiariserez avec la sécurité des points de terminaison, **les fonctionnalités d'audit de Microsoft 365** et la gouvernance des ressources dans Azure.
En suivant cette formation sur les solutions SCI Microsoft vous serez également en mesure de passer l'examen SC-900 compris dans notre offre. Il vous permettra d'obtenir la certification **Microsoft Certified : Security, Compliance, and Identity Fundamentals**.

Objectifs

À l'issue de la **formation Microsoft SC-900**, vous atteindrez les objectifs de compétences suivants :

- expliquer les concepts de sécurité, de conformité et d'identité ;
- connaitre les fonctions liées à la gestion des identités avec Microsoft Azure AD en tant que composant de Microsoft Entra ;
- connaitre les fonctions de sécurité incluses dans les solutions Microsoft ;
- connaitre les fonctions de conformité incluses dans les solutions Microsoft ;
- réussir l'examen SC-900 et obtenir la certification Microsoft Certified : Security, Compliance and Identity Fundamentals.

Points forts

Des cours dispensés par un formateur expert des solutions Microsoft , un programme complet axé sur des travaux pratiques et le passage de l'examen de certification SC-900 compris dans notre offre.

Certification

Cette formation vous permet de passer l'examen SC-900 inclus dans notre offre afin d'obtenir la certification **Microsoft Certified : Security, Compliance and Identity Fundamentals**.
Cet examen atteste de vos connaissances dans les domaines suivants : **les concepts de sécurité, de conformité et d'identité** ; les caractéristiques de Microsoft Azure Active Directory (Azure AD); les caractéristiques des solutions de sécurité Microsoft et les caractéristiques des solutions de conformité Microsoft.
Pour atteindre ces objectifs, vous devrez avoir **une bonne connaissance de Microsoft Azure et de Microsoft 365**. De plus, vous devrez avoir compris dans quelle mesure les solutions Microsoft SCI peuvent être déployées au sein de ces produits afin d'apporter une réponse holistique de bout en bout.
A savoir : *la certification Microsoft Certified: Security, Compliance, and Identity Fundamentals permet de se préparer à passer d'autres certifications Microsoft orientées sur des rôles d'ingénieur.*

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre la **formation Microsoft SC-900** nécessite les prérequis suivant :

- avoir une expérience professionnelle pratique en informatique ;
- avoir des connaissances de base sur les réseaux et le cloud computing ;
- avoir des connaissances de base sur les produits Microsoft Azure et Microsoft 365.

Public

Cette formation s'adresse aux publics suivants :

- toutes personnes qui utilisent les produits et les services Microsoft et qui souhaitent acquérir des connaissances de base en matière de sécurité, de conformité et d'identité.

Cette formation s'adresse aux profils suivants

Administrateur système
Technicien Support / HelpDesk
Chef de projet / Responsable de projet
Chef d’entreprise / Dirigeant

Programme

Module 1 : introduction aux concepts de sécurité, de conformité et d'identité

- Comprendre les concepts de sécurité et de conformité :
    - le modèle de responsabilité partagée ;
    - la défense en profondeur ;
    - le modèle de confiance zéro ;
    - le cryptage et le hachage ;
    - les concepts de conformité.
- Comprendre les concepts d'identité :
    - l'identité en tant que premier critère de sécurité ;
    - l'authentification ;
    - l'autorisation ;
    - les fournisseurs d'identité ;
    - L'annuaire Active Directory.

Module 2 : présentation des fonctions d'identités avec Microsoft Azure AD en tant que composant de Microsoft Entra

- Comprendre les principaux services et les types d'identités d'Azure AD :
    - qu'est-ce que Azure AD ? ;
    - les identités Azure AD ;
    - l'identité hybride ;
    - les différents types d'identité externes.
- Comprendre les fonctions d'authentification d'Azure AD :
    - les différentes méthodes d'authentification ;
    - l'authentification multifactorielle ;
    - la réinitialisation du mot de passe en libre-service ;
    - les différentes fonctions de protection et de gestion des mots de passe.
- Comprendre les fonctions de gestion des accès d'Azure AD :
    - l'accès conditionnel ;
    - les avantages des rôles Azure AD ;
    - les avantages du contrôle d'accès basé sur les rôles.
- Comprendre les fonctions de gouvernance et de protection des identités d'Azure AD :
    - la gouvernance des identités ;
    - la gestion des droits des utilisateurs et les révisions d'accès ;
    - les fonctionnalités de la gestion des identités privilégiées (PIM) ;
    - la protection des identités.

Module 3 : présentation des fonctions de sécurité des produits Microsoft

- Comprendre les principales fonctions de sécurité d'Azure :
    - la protection DDoS d'Azure ;
    - le pare-feu Azure ;
    - qu'est-ce qu'un pare-feu d'application web ? ;
    - la segmentation du réseau avec les réseaux virtuels Azure ;
    - les groupes de sécurité réseau d'Azure ;
    - le système Azure Bastion et l'accès aux machines virtuelles ;
    - les méthodes de cryptage des données.
- Comprendre les fonctions de gestion de sécurité d'Azure :
    - la gestion de la posture de sécurité dans le cloud ;
    - la solution Microsoft Defender pour le cloud ;
    - les fonctions de sécurité améliorées de Microsoft Defender pour le cloud ;
    - les règles de base de la sécurité sur Azure.
- Comprendre les fonctions de sécurité de Microsoft Sentinel :
    - les concepts de surveillance SIEM et SOAR ;
    - les avantages de Microsoft Sentinel pour la gestion intégrée des menaces.
- Comprendre le système de protection contre les menaces de Microsoft 365 Defender :
    - les services de Microsoft 365 Defender :
        - Microsoft Defender pour Office 365 ;
        - Microsoft Defender pour Endpoint ;
        - Microsoft Defender pour Cloud Apps ;
        - Microsoft Defender pour l'identité ;
- le portail Microsoft 365 Defender.

Module 4 : présentation des fonctions de conformité des produits Microsoft

- Comprendre le fonctionnement du portail d'approbation des services de Microsoft et les principes de protection de la vie privée :
    - les offres du portail d'approbation des services ;

    - les principes de confidentialité de Microsoft.
- Comprendre les fonctions de gestion de la conformité de Microsoft Purview :
    - le portail de conformité de Microsoft Purview ;
    - le gestionnaire de conformité ;
    - l'utilisation et les avantages du score de conformité.
- Comprendre les fonctions de protection des informations et de gestion du cycle de vie des données de Microsoft Purview :
    - les fonctionnalités de classification des données ;
    - les avantages de l'explorateur de contenu et de l'explorateur d'activités ;
    - les labels de confidentialité et les stratégies de labellisation ;
    - la prévention des pertes de données (DLP) ;
    - la gestion des enregistrements ;
    - les stratégies de conservation, les étiquettes de conservation et les stratégies d'étiquettes de conservation.
- Comprendre les fonctions de risque interne de Microsoft Purview :
    - la gestion des risques internes ;
    - la conformité des communications ;
    - la séparation des informations ;
    - les fonctionnalités de gouvernance des ressources dans Azure ;
    - l'utilisation de Azure Policy ;
    - l'utilisation des Blueprints Azure ;
    - la gouvernance unifiée des données.