Programme de cours
Microsoft 365 - Security Administrator

Durée :	4 jours soit 28 heures	Référence :	MS-500T00

Public visé :

- Administrateur sécurité

Pré-requis :

Pour suivre cette formation, les apprenants doivent :

- Avoir une compréhension conceptuelle de base de Microsoft Azure.
- Avoir de l'expérience avec les périphériques Windows 10.
- Avoir de l'expérience avec Office 365.
- Avoir une compréhension de base des autorisations et de l'authentification.
- Avoir une compréhension de base des réseaux informatiques.
- Avoir une connaissance pratique de la gestion des périphériques mobiles.

Objectifs pédagogiques :

Compétences obtenues à l'issue de la formation :

- Administrer l'accès utilisateur et de groupe dans Microsoft 365.
- Expliquer et gérer Azure Identity Protection.
- Planifier et mettre en œuvre Azure AD Connect.
- Gérer les identités synchronisées des utilisateurs.
- Expliquer et utiliser l'accès conditionnel.
- Décrire les vecteurs de menaces des cyberattaques.
- Expliquer les solutions de sécurité pour Microsoft 365.
- Utiliser Microsoft Secure Score pour évaluer et améliorer votre posture de sécurité.
- Configurer les services de protection avancée contre les diverses menaces pour Microsoft 365.
- Planifier et déployer des appareils mobiles sécurisés.
- Planifier et déployer des périphériques mobiles sécurisés.
- Mettre en œuvre la gestion des droits à l'information.
- Sécuriser les messages sur Office 365.
- Configurer les politiques de prévention de pertes des données.
- Déployer et gérer la sécurité des applications dans le cloud.
- Mettre en œuvre la protection des informations Windows pour les périphériques.
- Planifier et déployer un archivage de données et un système de conservation.
- Créer et gérer une enquête eDiscovery.
- Expliquer et utiliser les labels de sensibilité.

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure.
La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz.
L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration.
En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Moyens et supports pédagogiques :

Cadre présentiel
Salles de formation équipées et accessibles aux personnes à mobilité réduite.
- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection sur tableau blanc
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel
Session dispensée via notre solution iClassroom s'appuyant sur Microsoft Teams.
- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Modalités d'évaluation et suivi :

Avant
Afin de valider le choix d'un programme de formation, une évaluation des prérequis est réalisée à l'aide d'un questionnaire en ligne ou lors d'un échange avec le formateur(trice) qui validera la base de connaissances nécessaires.
Pendant

Après chaque module théorique, un ou des ateliers pratiques permettent la validation de l'acquisition des connaissances. Un Quizz peut accompagner l'atelier pratique.

Après

Un examen de certification si le programme de formation le prévoit dans les conditions de l'éditeur ou du centre de test (TOSA, Pearson Vue, ENI, PeopleCert)

Enfin

Un questionnaire de satisfaction permet au participant d'évaluer la qualité de la prestation.

Description / Contenu

Module 1 : Gestion des utilisateurs et des groupes

- Concepts de gestion des identités et des accès
- Le modèle de confiance zéro
- Planifier votre solution d'identité et d'authentification
- Comptes et rôles des utilisateurs
- Gestion des mots de passe

Module 2 : Synchronisation et protection de l'identité

- Planifier la synchronisation des répertoires
- Configurer et gérer les identités synchronisées
- Azure AD Identity Protection

Module 3 : Gestion des identités et des accès

- Gestion des demandes
- Gouvernance de l'identité
- Gérer l'accès aux périphériques
- Contrôle d'accès en fonction du rôle (RBAC)
- Solutions pour l'accès externe
- Gestion des identités privilégiées

Module 4 : La sécurité dans Microsoft 365

- Vecteurs de menaces et violations des données
- Stratégie et principes de sécurité
- Les solutions de sécurité de Microsoft
- Microsoft Secure Score

Module 5 : Protection avancée contre les menaces

- Exchange Online Protection (EOP)
- Microsoft Defender for Office 365
- Gestion des pièces jointes sécurisées
- Gestion des liens sécurisés
- Microsoft Defender for Identity
- Microsoft Defender for Endpoint

Module 6 : Gestion des menaces

- Utiliser le tableau de bord de sécurité.
- Enquête sur les menaces et réponse
- Azure Sentinel pour Microsoft 365.
- Configuration d'Advanced Threat Analytics.

Module 7 : Microsoft Cloud Application Security

- Deployer Cloud Application Security
- Utiliser les informations de Cloud Application Security

Module 8 : Mobilité

- Mobile Application Management (MAM)
- Mobile Device Management (MDM)
- Déployer les services des appareils mobiles
- Enregistrer les appareils sur Mobile Device Management

Module 9 : Protection de l'information et gouvernance

- Concepts de protection des informations
- Gouvernance et gestion des documents
- Labels de sensibilité
- Archivage dans Microsoft 365
- Conservation dans Microsoft 365
- Politiques de conservation dans le centre de conformité Microsoft 365
- Archivage et conservation dans Exchange
- Gestion des documents en place dans SharePoint

Module 10 : Prévention de la perte de données

- Gestion des droits à l'information (IRM)
- Extension polyvalente sécurisée de courrier Internet (S-MIME)
- Office 365 Message Encryption

Module 11 : Sécurité de l'application dans le cloud

- Principes fondamentaux de la prévention des pertes de données
- Créer une politique DLP
- Personnaliser une politique DLP
- Créer une politique DLP pour protéger les documents
- Conseils de politique

Module 12 : Gestion de la conformité

- Centre de conformité

Module 13 : Gestion des risques d'initiés

- Risque d'initié
- Accès privilégié
- Obstacles à l'information
- Construire des murs éthiques dans Exchange Online

Module 14 : Découvrir et répondre

- Rechercher du contenu
- Faire l'audit des enquêtes de journal
- eDiscovery avancé