Microsoft 365 - Administration de la sécurité

Référence : MSMS500
Durée : 4 jours (28h)
Tarif : 2400 €
Date à planifier

Certification : Aucune
Code CPF Unique : Aucun - **Code Certif Info :** Aucun

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel.
Le formateur alterne entre méthode* démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).
Variables suivant les formations, les moyens pédagogiques mis en œuvre sont :

- Ordinateurs Mac ou PC, connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

** ratio variable selon le cours suivi*

Modalités d'évaluation des acquis

L'évaluation des acquis se fait :

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation

A l'issue de ce stage vous serez capable de :

- Administrer l'accès des utilisateurs et des groupes dans Microsoft 365
- Expliquer et gérer la protection d'identité Azure
- Planifier et mettre en œuvre Azure AD Connect
- Gérer les identités synchronisées des utilisateurs
- Expliquer et utiliser l'accès conditionnel
- Décrire les vecteurs de menace de cyberattaque
- Expliquer les solutions de sécurité pour Microsoft 365
- Utiliser Microsoft Secure Score pour évaluer et améliorer votre posture de sécurité
- Configurer divers services de protection avancés contre les menaces pour Microsoft 365
- Planifier et déployer des appareils mobiles sécurisés
- Mettre en œuvre la gestion des droits à l'information
- Sécuriser les messages dans Office 365
- Configurer les politiques de prévention de perte des données
- Déployer et gérer Cloud App Security
- Mettre en œuvre la protection des informations Windows pour les appareils
- Planifier et déployer un système d'archivage et de conservation des données
- Créer et gérer une enquête eDiscovery
- Gérer les demandes des personnes associées aux données RGPD
- Expliquer et utiliser les étiquettes de sensibilité.

Public :

Administrateurs Microsoft 365 Enterprise et Security.

Prérequis :

Avoir des connaissances de base sur Microsoft Azure, les autorisations, les authentifications et les réseaux informatiques. Il est également recommandé d'avoir une expérience avec Windows 10 et Office 365 et une connaissance pratique de la gestion des appareils mobiles.

Dernière mise à jour le 02/02/2022

Les plus de la formation :

Le support de cours et les Microsoft Labs Online sont en anglais.

Cette formation :

- bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.
- est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par ALYF

Programme

- **Gestion des utilisateurs et des groupes**

Concepts de gestion de l'identité et de l'accès

Le modèle "Zero Trust"

Planifier votre solution d'identité et d'authentification

Comptes et rôles des utilisateurs

Gestion de l'identité

- **Synchronisation et protection des identités**

Planifier la synchronisation des répertoires

Configurer et gérer les identités synchronisées

Gestion des mots de passe

Protection de l'identité dans l'Azure AD

- **Gestion de l'accès**

Accès conditionnel

Gérer l'accès aux appareils

Contrôle d'accès basé sur les rôles (RBAC)

Solutions pour l'accès externe

- **Sécurité dans Microsoft 365**

Vecteurs de menaces et atteintes à la protection de données

Stratégie et principes de sécurité

Solutions de sécurité pour Microsoft 365

Secure Score

- **Protection contre les menaces**

Exchange Online Protection (EOP)

Protection avancée contre les menaces dans Office 365

Gérer des pièces jointes et les liens sécurisés

Protection avancée contre les menaces avec :

- Azures
- Microsoft Defender

- **Gestion des menaces**

Tableau de bord de la sécurité

Enquête et réponse aux menaces

Azure Sentinel

Analyse avancée des menaces

- **Sécurité des applications Cloud**

Déployer la sécurité des applications Cloud

Utiliser les informations de sécurité des applications Cloud

- **Mobilité**

Mobile Application Management (MAM)

Mobile Device Management (MDM)

Déployer les services des appareils mobiles

Inscrire les appareils au MDM

- **Protection des informations**

Concepts de protection de l'information

Etiquettes de sensibilité

Azure Information Protection (AIP)

Windows Information Protection (WIP)

- **Gestion des droits et cryptage**

Information Rights Management (IRM)

Secure Multipurpose Internet Mail Extension (S-MIME)

Cryptage des messages dans Office 365

- **Prévention des pertes de données (DLP)**

Principes fondamentaux de la DLP

Créer une politique DLP

Personnaliser une politique DLP

Créer une politique DLP pour protéger les documents

Conseils politiques

- **Archivage et conservation**

Archivage dans Microsoft 365

Conservation dans Microsoft 365

Politiques de conservation dans le centre de conformité Microsoft 365

Archivage et conservation sur Exchange

Gestion des documents "in-place" dans SharePoint

- **Recherche de contenu et enquête**

Recherche de contenu

Enquêtes sur le log d'audit

eDiscovery avancée

- **Conformité dans Microsoft 365**

Centre de conformité

Solutions du centre de conformité

Construire des "ethical walls" dans Exchange Online

SUIVI DE L'EXECUTION ET EVALUATION DES RESULTATS

> Feuilles de présence

> Questions orales ou écrites(QCM)

> Mises en situation

> Formulaires d’évaluation de la formation

> Certificat de réalisation de l'action de formation

Dernière mise à jour le 02/02/2022