

# Microsoft Copilot pour Microsoft 365 pour les administrateurs

Référence : **MSMS4006**Durée : **1 jour**Certification : **Aucune**

## CONNAISSANCES PREALABLES

- 1-Aucunes. • 2-Avoir des connaissances de base en langue anglaise car le support de cours est en anglais et les ateliers seront réalisés sur des VM en anglais.

## PROFIL DES STAGIAIRES

- 1-Administrateurs et Administrateurs de Microsoft 365. • 2-Toute personne aspirant au rôle d'administrateur de Microsoft 365.

## OBJECTIFS

- Maîtriser l'architecture et les composants de Copilot pour Microsoft 365. • Implémenter et sécuriser Copilot dans l'environnement Microsoft 365. • Gérer l'accès sécurisé des utilisateurs et l'authentification. • Configurer et administrer les rôles au sein de Microsoft 365. • Appliquer la classification des données et les étiquettes de sensibilité. • Exploiter les capacités d'intelligence de menace de Microsoft Defender XDR.

## CERTIFICATION PREPAREE

- Aucune

## METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

## FORMATEUR

Consultant-Formateur expert Copilot

## METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

## CONTENU DU COURS

### Examiner la conception de Copilot pour Microsoft 365

- Examiner l'architecture logique de Copilot pour Microsoft 365
- Examiner les composants clés de Copilot pour Microsoft 365
- Explorer le service et l'architecture tenant de Copilot pour Microsoft 365
- Étendre Copilot pour Microsoft 365 avec les connecteurs Microsoft Graph

### Implémenter Copilot pour Microsoft 365

- Se préparer pour Copilot pour Microsoft 365

- Préparer ses données pour les recherches dans Copilot pour Microsoft 365
- Protéger vos données de Copilot pour Microsoft 365 avec les outils de sécurité de Microsoft 365
- Attribuer vos licences Copilot pour Microsoft 365
- Favoriser l'adoption de Copilot pour Microsoft 365 avec un Centre d'Excellence Copilot

### Examiner la sécurité des données et la conformité dans Copilot pour Microsoft 365

- Examiner comment Copilot pour Microsoft 365 utilise vos données commerciales propriétaires
- Examiner comment Copilot pour Microsoft 365 protège les données commerciales sensibles

- Examiner comment Copilot pour Microsoft 365 utilise les contrôles d'isolation et d'accès de Microsoft 365
- Examiner comment Copilot pour Microsoft 365 répond aux exigences de conformité réglementaire

### **Gérer l'accès sécurisé des utilisateurs dans Microsoft 365**

- Examiner les outils d'identité et d'accès utilisés dans Microsoft 365
- Gérer les mots de passe des utilisateurs
- Implémenter les politiques d'accès conditionnel
- Activer l'authentification en transit
- Implémenter l'authentification multifactorielle
- Activer la connexion sans mot de passe avec Microsoft Authenticator
- Explorer la gestion des mots de passe en libre-service
- Explorer Windows Hello pour les entreprises
- Implémenter le verrouillage intelligent de Microsoft Entra
- Explorer les paramètres de sécurité par défaut dans Microsoft Entra ID
- Enquêter sur les problèmes d'authentification à l'aide des journaux de connexion

### **Gérer les rôles et les groupes de rôles dans Microsoft 365**

- Examiner l'utilisation des rôles dans le modèle de permissions de Microsoft 365
- Gérer les rôles à travers l'écosystème de Microsoft 365
- Explorer les rôles d'administrateur dans Microsoft 365
- Examiner les meilleures pratiques lors de la configuration des rôles administratifs
- Attribuer des rôles d'administrateur aux utilisateurs dans Microsoft 365
- Déléguer des rôles d'administrateur à des partenaires

### **Explorer l'intelligence de menace dans Microsoft Defender XDR**

- Explorer Microsoft Intelligent Security Graph
- Explorer les politiques d'alerte dans Microsoft 365
- Exécuter des enquêtes et des réponses automatisées
- Explorer la chasse aux menaces avec Microsoft Threat Protection
- Explorer la chasse aux menaces avancées dans Microsoft Defender XDR
- Explorer l'analytique des menaces dans Microsoft 365
- Identifier les problèmes de menace à l'aide des rapports de Microsoft Defender

### **Implémenter la classification des informations sensibles**

- Explorer la classification des données
- Implémenter la classification des données dans Microsoft 365
- Explorer les classificateurs entraînaables
- Créer et réentraîner un classificateur entraînaable
- Visualiser les données sensibles à l'aide de l'explorateur de contenu et de l'explorateur d'activité
- Détecter les documents contenant des informations sensibles à l'aide de l'empreinte digitale des documents

### **Explorer les étiquettes de sensibilité**

- Gérer la protection des données à l'aide des étiquettes de sensibilité
- Explorer ce que les étiquettes de sensibilité peuvent faire
- Déterminer la portée d'une étiquette de sensibilité
- Appliquer automatiquement les étiquettes de sensibilité
- Explorer les politiques d'étiquetage de sensibilité

### **Implémenter les étiquettes de sensibilité**

- Planifier votre stratégie de déploiement pour les étiquettes de sensibilité
- Examiner les exigences pour créer une étiquette de sensibilité
- Créer des étiquettes de sensibilité
- Publier des étiquettes de sensibilité
- Supprimer et effacer des étiquettes de sensibilité

Notre **référent handicap** se tient à votre disposition au 01.71.19.70.30 ou par mail à [referent.handicap@edugroupe.com](mailto:referent.handicap@edugroupe.com) pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.