# Formation Microsoft 365 Administration : Fondamentaux + Sécurité

Formation éligible au CPF, contactez-nous au 09 72 37 73 73

| | |
|---|---|
| **Durée :** | 5 jours |
| **Public :** | Administrateurs Systèmes Microsoft avec bonnes connaissances d'Azure |
| **Pré-requis :** | Avoir des connaissances Microsoft / Office 365 et d'administration Windows Server |
| **Objectifs :** | Découvrir le Cloud Computing et la suite de produits et de services Microsoft 365 - Créer et à gérer un compte Microsoft 365 - utiliser Exchange Online pour la gestion de la messagerie électronique et SharePoint Online pour la gestion de contenu et la collaboration - Utiliser Teams pour la gestion de projets et la communication au sein d'une équipe - Mettre en place et à gérer la sécurité de Microsoft 365 - Gérer l'authentification et l'accès conditionnel - Mettre en œuvre des solutions de protection des menaces et des appareils - Gérer la gouvernance et la conservation des données dans Microsoft 365 - Assurer la conformité de la réglementation sur la confidentialité des données dans Microsoft 365 |
| **Sanction :** | Attestation de fin de stage mentionnant le résultat des acquis |
| **Taux de retour à l'emploi:** | Aucune donnée disponible |
| **Référence:** | CLO102218-F |
| **Code CPF:** | RS5443 - contactez-nous au 09 72 37 73 73 |
| **Note de satisfaction des participants:** | Pas de données disponibles |
| **Certifications :** | MICROSOFT : Microsoft 365 Security Administration<br>Pas de données disponibles au 01/07/2024 |

## Introduction

Découvrir le Cloud Computing et le mode SAAS
Découvrir Microsoft 365 : présentation, offres disponibles
Gérer les licences
Créer et configurer un compte Microsoft 365
**Atelier : Configurer un compte utilisateur Office 365**

## Administrer Microsoft 365

Gérer les utilisateurs dans le Cloud
Découvrir les portails administratifs
Gérer Microsoft 365 avec Windows PowerShell
Administrer les accès administratifs
Mettre en place la synchronisation d'annuaire
Gérer Azure Entra Connect et Connect Health
Mettre en place l'authentification unique, principes d'ADFS et du SSO
**Atelier : Mettre en place d'un environnement hybride et configurer les outils de synchronisation AD et Azure AD**

**Utiliser Exchange Online**

Découvrir Exchange Online
Effectuer des opérations d'administration de base
Administrer les stratégies d'accès clients
Gérer les utilisateurs internes et invités, ressources, salles, boîtes aux lettres partagées
Protéger les distributions locales avec EOP (Exchange Online Protection)
Mettre en place la protection des données sensibles avec DLP (Data Loss Protection)
Administrer à l'aide de PowerShell
**Atelier : Configurer une messagerie Exchange et sa sécurité**

**Utiliser SharePoint Online**

Découvrir SharePoint Online
Administrer des collections de sites
Gérer des applications
Accéder aux données de l'entreprise
Administrer des utilisateurs externes
Configurer OneDrive for Business pour SharePoint online
**Ateliers : Créer et utiliser des sites et des listes (contacts, liens) dans SharePoint**

**Collaborer avec Teams**

Découvrir les équipes et les canaux Teams
Mettre en place des connecteurs
Mettre en œuvre du client Teams
Administrer OneDrive et des partages externes
Suivre des partages et mettre en œuvre du client OneDrive
**Atelier : Créer des espaces de collaboration Teams, les administrer et les sécuriser.**

**Administrer la sécurité**

Mettre en œuvre la sécurité de signature du plan
Mettre en œuvre l'authentification multifactorielle (MFA)
Gérer et surveiller la MFA
Planifier et mettre en œuvre des méthodes d'authentification comme Windows Hello
Configurer et gérer les options d'authentification des utilisateurs Azure AD
Mettre en place et gérer la conformité des appareils pour la sécurité des terminaux
Mettre en œuvre et gérer l'accès conditionnel
**Atelier : Mettre en place du MFA et de l'accès conditionnel**

**Mettre en œuvre le contrôle d'accès basé sur les rôles (RBAC) et Azure AD Privileged Identity Management (PIM)**

Planifier les rôles
Configurer les rôles
Vérifier les rôles
Planifier pour Azure PIM
Mettre en œuvre et configurer les rôles Azure PIM
Gérer les missions de rôle Azure PIM
Mettre en œuvre une politique sur les risques pour les utilisateurs
Mettre en œuvre une politique sur les risques de signature
Configurer les alertes de protection d'identité
Examiner les événements à risque et y réagir
**Ateliers : Créer et affecter des autorisations à l'aide des rôles et protéger les accès privilégiés à l'aide de PIM**

**Mettre en œuvre une solution hybride de protection des menaces pour l'entreprise**

Planifier une solution Azure Advanced Threat Protection (ATP)
Installer et configurer Azure ATP
Surveiller et gérer Azure ATP
Planifier une solution Microsoft Defender ATP
Mettre en oeuvre Microsoft Defender ATP
Gérer et surveiller Microsoft Defender ATP
Planifier un accès sécurisé aux données dans Office 365
Mettre en oeuvre et gérer le système Customer Lockbox
Configurer l'accès aux données dans les workloads de collaboration Office 365
Configurer le partage B2B pour les utilisateurs externes
**Atelier : Configurer des scénarios d'ATP**

**Mettre en œuvre et gérer la protection des appareils et des applications**

Planifier la protection du dispositif et de l'application
Configurer et gérer Microsoft Defender Application Guard
Configurer et gérer Microsoft Defender Application Control
Configurer et gérer Microsoft Defender Exploit Guard
Configurer Secure Boot
Configurer et gérer le chiffrement des périphériques Windows
Configurer et gérer le chiffrement des périphériques non Windows
Planifier pour sécuriser les données des applications sur les appareils
Mettre en œuvre des politiques de protection des applications
**Atelier : Mettre en place la protection des applications et des appareils**

**Mettre en œuvre et gérer Microsoft Cloud App Security**

Planifier la mise en oeuvre de la sécurité des applications infonuagiques
Configurer Microsoft Cloud App Security
Gérer la découverte d'applications en nuage
Gérer les entrées dans le catalogue d'applications Cloud
Gérer les applications dans Cloud App Security
Gérer la sécurité de l'application Microsoft Cloud
Configurer les connecteurs Cloud App Security et les applications Oauth
Configurer les politiques et les modèles de sécurité de l'application Cloud
Examiner, interpréter et répondre aux alertes, rapports, tableaux de bord et journaux de sécurité de l'application Cloud
**Atelier : Configurer Microsoft Cloud App Security et exploiter les tableaux de bord et les**

**journaux**

**Gérer la gouvernance et la conservation des données**

Planifier la gouvernance et la conservation des données
Examiner et interpréter les rapports et les tableaux de bord sur la gouvernance des données
Configurer les politiques de conservation
Définir les types d'événements de gouvernance des données
Définir les politiques de supervision
Configurer les retenues d'information
Trouver et récupérer les données Office 365 supprimées
Configurer l'archivage des données
Gérer les boîtes aux lettres inactives
**Atelier : Mettre en place d'un processus de gouvernance et de conservation des données**

**Gérer la conformité de la réglementation sur la confidentialité des données**

Planifier la conformité réglementaire dans Microsoft 365
Examiner et interpréter les tableaux de bord et les rapports du RGPD
Gérer les demandes des personnes concernées (DSR)
Administrer le gestionnaire de la conformité
Examiner les rapports du gestionnaire de la conformité
Créer et exécuter les évaluations et les actions du Responsable Conformité
**Atelier : Personnaliser les outils de conformité Microsoft 365 pour correspondre à son organisation.**