# Programme de cours
# Microsoft 365 Mobilité et sécurité

| | | | |
|---|---|---|---|
| Durée : | 5 jours soit 35 heures | Référence : | MS-101T00 |

## Public visé :

Cette formation est destinée :

- Aux personnes qui doivent prendre le rôle d'administrateur de Microsoft 365 au sein de leur environnement professionnel.
- Aux personnes qui souhaitent se préparer au passage de l'examen MS-101.

## Pré-requis :

Pour suivre cette formation, les apprenants doivent :

- Savoir concevoir, configurer et gérer votre locataire Microsoft 365 (cours MS-100T00).
- Maîtriser les fonctionnalité des produits Microsoft 365 (cours MS-100T00).
- Savoir configurer Microsoft 365 (cours MS-100T00).
- Maîtriser la gestion des applications Microsoft 365 pour les déploiements d'entreprises (cours MS-100T00).
- Savoir planifier et mettre en œuvre la synchronisation des identités (cours MS-100T00).
- Savoir mettre en œuvre les applications et l'accès externe (cours MS-100T00).
- Avoir une compréhension parfaite du DNS et une expérience fonctionnelle de base avec les services Microsoft 365.
- Avoir une compréhension parfaite des pratiques informatiques générales.

## Objectifs pédagogiques :

A l'issue de la formation, les apprenants auront acquis les compétences suivantes :

- Microsoft 365 Security Metrics
- Microsoft 365 Security Services
- Microsoft 365 Threat Intelligence
- Gouvernance des données dans Microsoft 365
- Gouvernance des données dans Microsoft 365 Intelligence
- Recherche et examen
- Gestion des appareils
- Stratégies de déploiement dans Windows 10
- Gestion des appareils mobiles

## 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

# Programme de cours
# Microsoft 365 Mobilité et sécurité

**Module 1 : explorez les mesures de sécurité dans Microsoft 365**

- Examiner les vecteurs de menaces et violations des données
- Explorer le modèle de sécurité Zero Trust
- Explorer les solutions de sécurité dans Microsoft 365
- Examiner Microsoft Secure Score
- Examiner Privileged Identity Management
- Examiner la protection des identités Azure

Ateliers :

- Initialiser votre Tenant Microsoft 365
- Workflows des ressources PIM

**Module 2 : gérer vos services Microsoft 365 Security**

- Examiner Exchange Online Protection
- Examiner Microsoft Defender pour Office 365
- Gérer Safe Attachments
- Gérer Safe Links
- Explorez les rapports dans les services de sécurité Microsoft 365

Ateliers :

- Mettre en œuvre une stratégie Safe Attachments
- Mettre en œuvre une stratégie Safe Links

**Module 3 : implémenter le renseignement sur les menaces dans Microsoft 365**

- Explorer le renseignement sur les menaces dans Microsoft 365
- Explorer le tableau de bord sur la sécurité
- Implémenter Microsoft Defender pour Identity
- Implémenter la sécurité des applications Microsoft Cloud

Ateliers :

- Mener une attaque d'harponnage à l'aide du simulateur d'attaques
- Mener des attaques des mots de passe l'aide du simulateur d'attaque
- Se préparer aux stratégies d'alerte
- Mettre en œuvre une alerte des privilèges de boîtes aux lettres
- Mettre en œuvre une alerte des privilèges SharePoint
- Tester l'alerte eDiscovery par défaut

**Module 4 : introduction à la gouvernance des données dans Microsoft 365**

- Explorer l'archivage dans Microsoft 365
- Explorer la conservation des données dans Microsoft 365
- Explorer Information Rights Management
- Explorer le chiffrement des messages dans Office 365
- Explorer la gestion des enregistrements sur place dans SharePoint
- Explorer la protection contre la perte de données dans Microsoft 365

Ateliers :

- Configurer le chiffrement des messages Microsoft 365
- Valider Information Rights Management
- Initialiser la conformité
- Configurer les balises et les stratégies de conservation des données

**Module 5 : gérer la gouvernance des données dans Microsoft 365**

- Évaluer votre préparation en matière de conformité
- Mettre en œuvre des solutions de conformité
- Créer des barrières à l'information dans Microsoft 365
- Créer une stratégie DLP à partir d'un modèle intégré
- Créer une stratégie DLP personnalisée
- Créer une stratégie DLP pour protéger des documents
- Implémenter des conseils stratégiques pour les stratégies DLP

Ateliers :

- Gérer les stratégies DLP
- Tester les stratégies MRM et DLP

**Module 6 : gérer la gouvernance des données dans Microsoft 365**

- Gérer la conservation dans données dans le courrier
- Dépanner la gouvernance des données
- Explorer des étiquettes de confidentialité
- Implémenter des étiquettes de confidentialité
- Implémenter la gouvernance des données

Ateliers :

- Implémenter des étiquettes de confidentialité
- Mettre en œuvre Windows Information Protection

**Module 7 : gérer les recherches et les enquêtes sur le contenu dans Microsoft 365**

- Rechercher du contenu dans le centre de conformité Microsoft 365
- Conduire les enquêtes sur les journaux d'audit
- Gérer Advanced eDiscovery

Ateliers :

- Mener une recherche de données
- Enquêter sur vos données Microsoft 365

**Module 8 : préparer la gestion des appareils dans Microsoft 365**

- Explorer la cogestion d'un périphérique Windows 10
- Préparer vos périphériques Windows 10 à la cogestion
- Transition de Configuration Manager à Intune
- Examiner Microsoft Store pour Entreprises
- Planifier la gestion des applications

Ateliers :

- Configurer Microsoft Store pour Entreprises
- Gérer Microsoft Store pour Entreprises

**Module 9 : planifier votre stratégie de déploiement Windows 10**

- Examiner les scénarios de déploiement de Windows 10
- Explorer des modèles de déploiement Windows Autopilot
- Planifier votre stratégie d'activation des abonnements à Windows 10
- Résoudre les erreurs de mise à niveau vers Windows 10
- Analyser les données de diagnostic Windows 10 à l'aide de Desktop Analytics

**Module 10 : implémenter la gestion des périphériques mobiles dans Microsoft 365**

- Explorer la gestion des périphériques mobiles
- Déployer la gestion des périphériques mobiles
- Inscrire des périphériques à la gestion des périphériques mobiles
- Gérer la conformité des appareils

Ateliers :

- Activer la gestion des périphériques
- Configurer Azure AD pour Intune
- Créer des stratégies Intune
- Inscrire un périphérique Windows 10
- Gérer et analyser un périphérique dans Intune