FORMATION

MICROSOFT 365 - AZURE AD - ADMINISTRATEUR

OBJECTIFS DE LA FORMATION

À l'issue de la formation, le participant sera en mesure de configurer et administrer Azure Active Directory, de gérer les identités, les accès et les applications, de renforcer la sécurité (authentification et politiques), de superviser l'activité, d'automatiser les tâches et d'assurer la conformité et la protection des identités au sein du système d'information.

Public concerné : Tout Administrateur Réseau et professionnels de l'informatique responsables de la gestion des identités et des accès au sein de leur organisation.

Prérequis

Connaissance de base en administration de systèmes et réseaux avec la gestion des utilisateurs et des permissions

Modalité de la formation

Dialogue constant, alternance théorie pratique.

Capacité d'accueil

1 à 5 personnes

L'évaluation

L'évaluation se fera en deux temps : une évaluation initiale et une évaluation finale.

Un certificat de réalisation sera délivré à la fin de la formation.

PROGRAMME DE LA FORMATION (7 heures)

1. Introduction à la formation Office 365 :

Découvrir l'ensemble des fonctionnalités d'Office 365, comprendre les avantages par rapport aux logiciels installés localement, et se familiariser avec l'interface Office.com pour une utilisation efficace des applications en ligne.

Exploration de l'interface, présentation des différences entre Office 365 et les logiciels traditionnels.

2. Introduction à Azure AD :

Découverte de la vue d'ensemble d'Azure AD, comprendre les différences entre Azure AD et Active Directory dur site

Inculquer les concepts clés concernant les locataires, utilisateurs, groupes et applications

3. Gestion des utilisateurs et des groupes :

Maîtriser la création et la gestion des utilisateurs ainsi que la gestion des groupes et des rôles
Mettre en place la synchronisation avec Activ e Directory sur site via Azure AD Connect

4. Authentification et sécurité :

Appréhender les différentes méthodes d'authentification (MFA, SSPR)
Configurer l'authentification multi facteur (MFA) et intégrer les politiques de sécurité ainsi que les accès conditionnels des utilisateurs

5. Gestion des applications et des accès :

Apprendre à enregistrer et gérer les applications, configurer les autorisations et les consentements.
Utiliser les rôles d'application et les groupes d'accès

6. Surveillance et rapports :

Découvrir et comprendre l'utilisation des journaux d'audit et des rapports.
Mettre en place la surveillance des activités suspectes et configurer les alertes et notifications.

7. Sécurité avancée et conformité :

Apprendre la configuration des politiques de protection des identités.
Initiation à l'Identity Protection ainsi qu'à la gestion des accès privilégiés (PIM)