



Objectifs	Sécuriser l'accès des utilisateurs aux ressources d'une organisation
Participants	Toutes personnes devant jouer le rôle d'administrateur de la sécurité Microsoft 365
Prérequis	Avoir une compréhension conceptuelle de base de Microsoft Azure - Avoir de l'expérience avec les périphériques Windows 10 - Avoir de l'expérience avec Office 365 - Avoir une compréhension de base des autorisations et de l'authentification - Avoir une compréhension de base des réseaux informatiques - Avoir une connaissance pratique de la gestion des périphériques mobiles.
Moyens pédagogiques	1 poste par participant - 1 Vidéo projecteur - Support de cours fourni à chaque participant - Ateliers individuels - Modalités d'évaluation : Ateliers (TP) pendant tout le long de la formation et Evaluation des acquis tout au long de la formation
Méthodes pédagogiques	Approche participative et interactive. - Alternance d'apports théoriques et de mises en situation. - Accompagnement personnalisé du formateur.
Type de formation	Formation présentielle ou distancielle, selon les besoins et les contraintes des participants
Tarif inter-entreprise	2800 € HT
Durée	4 jour(s) - 28 heure(s)
Modalités et délais d'accès	Formations accessibles sous 15 à 20 jours suite à votre demande. Un entretien initial doit être prévu avant votre entrée en formation.

Code : NCI_3A5B6C7D8E

Mis à jour le : 25 mars 2026

Programme :

Gestion des utilisateurs et des groupes

Concepts de gestion des identités et des accès
Le modèle de confiance zéro
Planifier votre solution d'identité et d'authentification
Comptes et rôles des utilisateurs
Gestion des mots de passe

Synchronisation et protection de l'identité

Planifier la synchronisation des répertoires
Configurer et gérer les identités synchronisées
Azure AD Identity Protection

Gestion des identités et des accès

Gestion des demandes
Gouvernance de l'identité
Gérer l'accès aux périphériques
Contrôle d'accès en fonction du rôle (RBAC)
Microsoft Defender for Endpoint
Gestion des identités privilégiées

La sécurité dans Microsoft 365

Vecteurs de menaces et violations des données
Stratégie et principes de sécurité
Les solutions de sécurité de Microsoft
Microsoft Secure Score

Protection avancée contre les menaces

Exchange Online Protection (EOP)
Microsoft Defender for Office 365
Gestion des pièces jointes sécurisées
Gestion des liens sécurisés
Microsoft Defender for Identity
Microsoft Defender for Endpoint

Gestion des menaces

Utiliser le tableau de bord de sécurité.
Enquête sur les menaces et réponse
Azure Sentinel pour Microsoft 365.
Configuration d'Advanced Threat Analytics.

Microsoft Cloud Application Security

Deployer Cloud Application Security
Utiliser les informations de Cloud Application Security

Mobilité

Mobile Application Management (MAM)
Mobile Device Management (MDM)
Déployer les services des appareils mobiles
Enregistrer les appareils sur Mobile Device Management

Protection de l'information et gouvernance

Concepts de protection des informations
Gouvernance et gestion des documents



Labels de sensibilité

Archivage dans Microsoft 365

Conservation dans Microsoft 365

Politiques de conservation dans le centre de conformité Microsoft 365

Archivage et conservation dans Exchange

Centre de conformité

Prévention de la perte de données

Gestion des droits à l'information (IRM)

Extension polyvalente sécurisée de courrier Internet (S-MIME)

Office 365 Message Encryption

Sécurité de l'application dans le cloud

Principes fondamentaux de la prévention des pertes de données

Créer une politique DLP

Personnaliser une politique DLP

Créer une politique DLP pour protéger les documents

Conseils de politique

Gestion de la conformité

Centre de conformité

Gestion des risques d'initiés

Risque d'initié

Accès privilégié

Obstacles à l'information

Construire des murs éthiques dans Exchange Online