Formation Sécurité Microsoft 365 - Administration de la sécurité

Description de la formation Sécurité Microsoft 365 Administration

Cette **formation** Sécurité **Microsoft 365** vise à vous apprendre à sécuriser l'accès des utilisateurs aux ressources de votre organisation.

Elle couvre la protection des mots de passe des utilisateurs, l'authentification à plusieurs facteurs, l'activation de Azure Identity Protection, la configuration et l'utilisation d'Azure AD Connect, et vous présente l'accès conditionnel dans Microsoft 365.

Vous découvrirez également les technologies de protection contre les menaces qui contribuent à protéger votre environnement Microsoft 365. Plus précisément, vous découvrirez les vecteurs de menaces et les solutions de sécurité de Microsoft pour atténuer les menaces. Vous découvrirez enfin Secure Score, Exchange Online protection, Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection et la gestion des menaces.

Dans le cadre de ce cours, vous apprendrez les technologies de protection de l'information qui contribuent à sécuriser votre environnement Microsoft 365. Le cours aborde le contenu géré par les droits d'information, le cryptage des messages, ainsi que les labels, les politiques et les règles qui soutiennent la prévention des pertes de données et la protection des informations.

Enfin, vous apprendrez l'archivage et la conservation dans Microsoft 365 ainsi que la gouvernance des données et comment effectuer des recherches et des enquêtes sur le contenu.

Objectifs

Objectif opérationnel :

Savoir sécuriser l'accès des utilisateurs aux ressources de votre organisation.

Objectifs pédagogiques :

Concrètement, à l'issue de cette **formation Microsoft 365 Administration Sécurité**, vous serez en mesure de :

- Administrer la sécurité des utilisateurs et des groupes
- Planifier et implémenter Azure AD Connect et gérer les identités synchronisées
- Planifier la mise en oeuvre des identités fédérées
- Utiliser Microsoft Secure Score pour évaluer la sécurité
- Utiliser les divers services avancés de protection pour Microsoft 365
- Implémenter la protection des informations Azure pour Microsoft 365 et la protection des informations Windows pour les périphériques
- Planifier et déployer un système d'archivage et de conservation des données dans le respect des obligations liées au RGPD

À qui s'adresse cette formation ?

Public :

Ce cours Microsoft 365 Administration Sécurité s'adresse aux administrateurs de sécurité Microsoft 365.

Prérequis :

Pour suivre cette formation Microsoft 365 Administration Sécurité, les participants doivent posséder au préalable les aptitudes suivantes :

- Avoir une compréhension conceptuelle de base de Microsoft Azure
- De l'expérience avec les périphériques Windows 10
- 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

Contenu du cours Sécurité Microsoft 365 Administration

Gestion des utilisateurs et des groupes Microsoft 365

Concepts de gestion de l'identité et de l'accès

Le modèle « Zéro Trust »

Comptes utilisateurs dans Microsoft 365

Rôles d'administrateur et groupes de sécurité dans Microsoft 365

Gestion des mots de passe dans Microsoft 365

Protection de l'identité Azure AD

Synchronisation et protection de l'identité

Introduction à la synchronisation des identités

Planification d'Azure AD Connect

Implémentation d'Azure AD Connect

Gestion des identités synchronisées

Introduction aux identités fédérées

Gestion des identités et des accès

Gestion des demandes

Gouvernance de l'identité

Gérer l'accès aux périphériques

Contrôle d'accès basé sur les rôles (RBAC)

Solutions pour l'accès externe

Gestion des identitiés privilégiées

La sécurité dans Microsoft 365

Vecteurs de menaces et violations des données

Stratégie et principes de sécurité

Solutions de sécurité Microsoft 365

Microsoft Secure Score

Protection avancée contre les menaces

Exchange Online Protection

Office 365 Advanced Threat Protection

Gestion des pièces jointes sécurisées

Gestion des liens sécurisés

Azure Advanced Threat Protection

Microsoft Defender Advanced Threat Protection

Gestion des menaces

Utiliser le tableau de bord de sécurité

Enquête sur les menaces et réponses Microsoft 365

Azure Sentinel pour Microsoft 365

Configuration d'Advanced Threat Analytics

Mobilité

Planifier la gestion des applications mobiles

Planifier la gestion des périphériques mobiles

Déployer la gestion des périphériques mobiles

Enregistrer des périphériques dans la gestion des périphériques mobiles

Protection de l'information et gouvernance

Concepts de protection des informations

Azure Information Protection

Advanced Information Protection

Windows Information Protection

Politiques de conservation dans le centre de conformité Microsoft 365

Gestion des droits et cryptage

Gestion des droits relatifs à des informations

Extension de messagerie Internet polyvalente sécurisée

Cryptage des messages dans Office 365

Prévention de la perte de données

Prévention de perte de données expliquée

Stratégies de prévention de la perte de données

Stratégies DLP personnalisées

Création d'une stratégie DLP pour protéger les documents

Conseils sur les stratégies

Sécurité des applications Cloud

Sécurité des applications expliquée dans le Cloud

Utilisation des informations de sécurité des applications Cloud

Gestion de la conformité

Planifier les exigences de conformité

Construire des murs éthiques dans Exchange Online

Gérer la conservation dans les e-mails

Dépanner la gouvernance des données

Archivage et conservation

Archivage dans Microsoft 365

Rétention dans Microsoft 365

Stratégies de rétention dans le centre de conformité Microsoft 365

Archivage et conservation dans Exchange

Gestion des enregistrements sur place dans SharePoint

Rechercher du contenu et enquêter

Recherche de contenu

Enquêtes du journal d'audit

eDiscovery avancé