

# Microsoft 365 Security Administration

## Description

Cette formation vous apprendra à sécuriser l'accès utilisateur aux ressources de votre organisation. La formation couvre la protection du mot de passe utilisateur, l'authentification multifacteurs, la manière d'activer la protection d'identité Azure et de mettre en place et d'utiliser Azure AD Connect, et vous introduit à l'accès conditionnel dans Microsoft 365. Vous découvrirez les technologies de protection contre les menaces qui vous aideront à protéger votre environnement Microsoft 365. Vous découvrirez plus particulièrement les vecteurs de menace et les solutions de sécurité Microsoft pour atténuer les menaces. Vous apprendrez tout sur Secure Score, la protection Exchange Online, la protection avancée contre les menaces (ATP) Azure, la protection avancée contre les menaces (ATP) Windows Defender, et la gestion des menaces.

**Formation retirée officiellement du catalogue Microsoft le 30.06.2023.**

### Prix de l'inscription en Présentiel (CHF)

3200

### Prix de l'inscription en Virtuel (CHF)

3000

### Contenu du cours

#### Module 1 : Protection utilisateur et de groupe

- Concepts de gestion de l'identité et de l'accès.
- Sécurité zéro confiance.
- 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

#### Module 2: Identifier la synchronisation

- Introduction à la synchronisation des identités
- Planifier pour Azure AD Connect
- Mettre en œuvre Azure AD Connect
- Gérer les identités synchronisées
- Introduction aux identités fédérées

#### Module 3: Gestion de l'accès

- Accès conditionnel
- Gérer l'accès aux périphériques.
- Contrôle d'accès en fonction du rôle (RBAC)
- Solutions pour l'accès externe

#### Module 4: La sécurité dans Microsoft 365

- Vecteurs de menaces et violations des données
- Stratégie et principes de sécurité.

- 
- Solutions de sécurité dans Microsoft 365
  - Microsoft Secure Score

### **Module 5: 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

### **Module 6 : Gestion des menaces**

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

### **Module 7 : 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

### **Module 8 : Protection des informations**

- Concepts de la protection des informations.
- Protection des informations dans Azure
- Protection avancée des informations
- Protection des informations Windows

### **Module 9 : Gestion des droits et cryptage**

- Gestion des droits relatifs à des informations
- Multipurpose Internet Mail Extension sécurisée
- Cryptage des messages dans Office 365

### **Module 10 : Prévention de la perte de données**

- La prévention de la perte de données expliquée
- Politiques de prévention de pertes de données
- Politiques DLP personnalisées.
- Créer une politique DLP pour protéger les documents
- Conseils sur les politiques

### **Module 11: Sécurité de l'application dans le cloud**

- Sécurité des applications dans le cloud expliquée
- Utiliser les informations de sécurité des applications dans le cloud
- Après avoir terminé ce module, les étudiants seront capables:
- de décrire la sécurité des applications dans le cloud,

- d'expliquer comment déployer la sécurité des applications dans le cloud,
- de contrôler vos applications dans le cloud grâce à des politiques,
- d'utiliser le catalogue des applications dans le cloud,
- d'utiliser le tableau de bord de la découverte dans le cloud,
- de gérer les permissions des applications dans le cloud.

## Module 12 : Conformité dans Microsoft 365

- Planifier les exigences de conformité.
- Construire une muraille déontologique dans Exchange Online
- Gérer la conservation dans le courrier électronique
- Dépanner la gouvernance des données
- Après avoir terminé ce module, les étudiants seront capables:
- de planifier les rôles de sécurité et de conformité,
- de décrire ce que vous devez prendre en considération dans le GRPD,
- de décrire une muraille déontologique dans Exchange et son fonctionnement,
- de travailler avec les balises de conservation dans des boîtes aux lettres,
- de décrire les politiques de conservation avec des messages électroniques et des fichiers de messagerie,
- Expliquer comment se fait le calcul de l'âge de rétention des éléments.
- Réparer les politiques de rétention qui ne fonctionnent pas comme prévu.

## Module 13 : Archivage et conservation

- Archivage dans Microsoft 365
- Conservation dans Microsoft 365
- Politiques de rétention dans le centre de conformité de Microsoft 365.
- Archivage et conservation dans Exchange
- Gestion des enregistrements sur place dans SharePoint

## Module 14 : Rechercher du contenu et enquêter

- Rechercher du contenu.
- Faire l'audit des enquêtes de journal
- eDiscovery avancé

## Lab / Exercices

- Laboratoires officiels Microsoft

## Documentation

- Support de cours numérique inclus

## Examen

- Ce cours prépare à la certification **MS-500: Microsoft 365 Security Administrator**
- Si vous souhaitez passer cet examen, veuillez le sélectionner lors de l'ajout de la formation dans votre panier

## Profils des participants

- Administrateur sécurité Microsoft 365

## Connaissances Préalables

- Comprendre Microsoft Azure, Windows 10 et Office 365
- Bases des autorisations et de l'authentification
- Bases des réseaux informatiques et périphériques mobiles

### **Objectifs**

- Administrer les utilisateurs et les groupes
- Décrire et gérer les fonctionnalités de la protection d'identité Azure
- Planifier et mettre en œuvre Azure AD Connect
- Configurer les solutions de sécurité
- Configurer Advanced Threat Analytics
- Déployer des périphériques mobiles sécurisés
- Déployer et gérer la sécurité des applications dans le cloud
- Mettre en œuvre la protection des informations Windows pour les périphériques
- Déployer un archivage de données et un système de conservation
- Gérer les demandes des sujets de données RGPD

### **Niveau**

Intermédiaire

### **Durée (Nombre de Jours)**

4

### **Reference**

MS-500T00