

Programme de formation SC-400 : Administrateur Microsoft Information Protection

(Préparation certification Microsoft SC-400)

DESCRIPTION DE LA FORMATION :

Cette formation vous donnera les clés pour protéger les informations dans vos déploiements Microsoft 365. Cette formation est orientée gouvernance des données, protection des informations au sein des organisations et politiques de prévention des pertes de données.

OBJECTIFS PEDAGOGIQUES :

A l'issue de cette formation, les participants seront en capacité de :

- Mettre en œuvre la protection des informations
- Mettre en œuvre la prévention des pertes de données
- Mettre en œuvre la gouvernance de l'information

MÉTHODES & MODALITÉS PÉDAGOGIQUES :

- Cette formation sera principalement constituée de théorie et d'ateliers techniques qui permettront d'être rapidement opérationnel.
- Support : un support de cours officiel Microsoft en anglais sera remis aux participants au format électronique via la plateforme Skillpipe.
- Evaluation : Les acquis sont évalués tout au long de la formation par le formateur (Prérequis évalués avant la formation, questions régulières, travaux pratiques, QCM ou autres méthodes).
- Formateur : le tout animé par un formateur expérimenté et accrédité Microsoft Certified Trainer.
- Satisfaction : à l'issue de la formation, chaque participant répond à un questionnaire d'évaluation qui est ensuite analysé en vue de maintenir et d'améliorer la qualité de nos formations.
- Suivi : une feuille d'émargement par demi-journée de présence est signée par chacun des participants.
- Cette formation peut être dispensée en format inter-entreprises ou intra-entreprise sur demande et en mode présentiel comme en distanciel.

PROGRAMME DE FORMATION :

Créer et gérer des types d'informations sensibles

- Sélectionner un type d'informations sensibles en fonction des exigences d'une organisation
- Créer et gérer des types d'informations sensibles personnalisés
- Créer des types d'informations sensibles personnalisés avec une correspondance exacte des données
- Mettre en œuvre l'empreinte digitale des documents
- Créer un dictionnaire de mots-clés

Créer et gérer des classificateurs entraînaibles

- Identifier quand utiliser des classificateurs entraînaibles
- Créer un classificateur entraînable
- Vérifier qu'un classificateur entraînable fonctionne correctement
- Recycler un classificateur

Mettre en œuvre et gérer les étiquettes de confidentialité

- Identifier les rôles et les autorisations pour l'administration des étiquettes de confidentialité
- Créer des étiquettes de sensibilité
- Configurer et gérer les politiques d'étiquette de sensibilité
- Appliquer des étiquettes de sensibilité aux équipes Microsoft, aux groupes Microsoft 365 et aux sites SharePoint
- Configurer et publier des politiques d'étiquetage automatique (hors scénarios MCAS)
- Surveiller la classification des données et l'utilisation des étiquettes à l'aide d'outils d'analyse d'étiquettes tels que le contenu explorateur et explorateur d'activités
- Appliquer une classification en masse aux données sur site à l'aide du scanner d'étiquetage unifié AIP
- Gérer les paramètres de protection et le marquage des étiquettes de sensibilité appliquées
- Appliquer des protections et des restrictions aux e-mails, y compris le marquage du contenu, l'utilisation, l'autorisation, cryptage, expiration, etc.
- Appliquer des protections et des restrictions aux fichiers, y compris le marquage du contenu, l'utilisation, l'autorisation, cryptage, expiration, etc.
- Gérer et gouverner les données à l'aide d'Azure Purview

Planifier et mettre en œuvre le chiffrement des messages électroniques

- Définir les exigences pour la mise en œuvre du chiffrement des messages Office 365
- Implémenter le chiffrement avancé des messages Office 365

Créer et configurer des politiques de prévention des pertes de données

- Recommander une solution de prévention des pertes de données pour une organisation
- Configurer la prévention des pertes de données pour la priorité des politiques
- Configurer les politiques pour le courrier électronique Microsoft Exchange
- Configurer des politiques pour les sites Microsoft SharePoint
- Configurer des politiques pour les comptes Microsoft OneDrive
- Configurer des politiques pour le chat Microsoft Teams et les messages de canal
- Intégrer Microsoft Cloud App Security (MCAS) à Microsoft Information Protection
- Configurer les politiques dans Microsoft Cloud App Security (MCAS)
- Mettre en œuvre des politiques de prévention des pertes de données en mode test

Mettre en œuvre et surveiller la prévention des pertes de données Microsoft Endpoint

- Configurer les politiques pour les terminaux
- Configurer les paramètres de prévention de perte de données Endpoint
- Recommander des configurations qui activent les appareils pour les politiques de prévention des pertes de données Endpoint
- Surveiller les activités des terminaux

Gérer et surveiller les politiques et les activités de prévention des pertes de données

- Gérer et répondre aux violations de la politique de prévention des pertes de données
- Examiner et analyser les rapports de prévention des pertes de données
- Gérer les autorisations pour les rapports de prévention des pertes de données
- Gérer les violations de prévention des pertes de données dans Microsoft Cloud App Security (MCAS)

Configurer les politiques de rétention et les étiquettes

- Créer et appliquer des étiquettes de rétention
- Créer et appliquer des politiques d'étiquette de rétention
- Configurer et publier des politiques d'étiquettes à appliquer automatiquement

Gérer la conservation des données dans Microsoft 365

- Créer et appliquer des politiques de rétention dans Microsoft SharePoint et OneDrive
- Créer et appliquer des politiques de rétention dans Microsoft Teams
- Récupérer du contenu dans Microsoft Teams, SharePoint et OneDrive
- Récupérer du contenu dans Microsoft Exchange
- Mettre en œuvre des politiques de rétention et des balises dans Microsoft Exchange
- Appliquer les blocages de boîte aux lettres dans Microsoft Exchange
- Mettre en œuvre les politiques d'archivage de Microsoft Exchange Online

Mettre en œuvre la gestion des enregistrements dans Microsoft 365

- Configurer les étiquettes pour la gestion des enregistrements
- Gérer et migrer les exigences de conservation avec un plan de fichiers
- Configurer la rétention automatique à l'aide des descripteurs de plan de fichiers
- Classer les enregistrements à l'aide d'étiquettes et de politiques de rétention
- Implémenter la gestion des enregistrements sur place dans Microsoft SharePoint
- Configurer la rétention basée sur les événements
- Gérer la disposition des dossiers

PRÉREQUIS :

Pour participer à cette formation, Il faut avoir suivi la formation « SC-900 : Microsoft Security, Compliance, and Identity Fundamentals » et avoir de solides connaissances sur Azure et Microsoft 365.

Un niveau d'anglais B1 est recommandé, retrouvez les niveaux sur ce lien : [Classification des niveaux de langue](#)

PRE-CERTIFICATION :

Cette formation prépare à l'examen de certification Microsoft « SC-400 : Administrateur Microsoft Information Protection »

DUREE : 2 jours (14 heures)

INTERLOCUTEURS : Administrateurs, administrateur de la protection des données, opérateurs de sécurité

NIVEAU : Intermédiaire