

## **Administrateur de la protection des informations sur Microsoft**

**Formation officielle Microsoft SC-400 Information Protection and Compliance Administrator**

### DESCRIPTION

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

- Expliquer les mécanismes de protection de l'information et de gestion du cycle de vie des données dans Microsoft Purview.
- Classer les données à des fins de protection et de gouvernance
- Créer et gérer des types d'informations sensibles
- Expliquer les principes et options de chiffrement disponibles dans Microsoft 365.
- Déployer le chiffrement des messages Microsoft Purview
- Créer et configurer des étiquettes de sensibilité avec Microsoft Purview
- Appliquer des étiquettes de confidentialité pour la protection des données.

### PUBLIC CIBLE

- Administrateurs
- Administrateurs de la protection des données
- Opérateurs de sécurité

### PRE-REQUIS

- 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](#)

### METHODE PEDAGOGIQUE

Formation avec apports théoriques, échanges sur les contextes des participants et retours d'expérience pratique du formateur, complétés de travaux pratiques et de mises en situation.

#### Classe à distance

Sécurité

Code :

**SC400**

Durée :

**4 jour(s) (28,00 heures)**

Exposés : **40 %**

Cas pratiques : **40 %**

Echanges d'expérience : **20 %**

#### Inter-entreprises :

Prochaines sessions disponibles [sur notre site web](#).

Tarif : 2 900,00 € HT /

participant

#### Intra-entreprise :

Tarifs et dates sur demande.

## PROFIL DES INTERVENANTS

Cette formation est dispensée par un·e ou plusieurs consultant·es d'OCTO Technology ou de son réseau de partenaires, expert·es reconnus des sujets traités.

Le processus de sélection de nos formateurs et formatrices est exigeant et repose sur une évaluation rigoureuse leurs capacités techniques, de leur expérience professionnelle et de leurs compétences pédagogiques.

## MODALITÉS D'ÉVALUATION ET FORMALISATION À L'ISSUE DE LA FORMATION

L'évaluation des acquis se fait tout au long de la session au travers des ateliers et des mises en pratique. Afin de valider les compétences acquises lors de la formation, un formulaire d'auto-positionnement est envoyé en amont et en aval de celle-ci. Une évaluation à chaud est également effectuée en fin de session pour mesurer la satisfaction des stagiaires et un certificat de réalisation leur est adressé individuellement.

## PROGRAMME PEDAGOGIQUE DETAILLE

### OUVERTURE DE SESSION

- Accueil des participants et recueil des attentes
- Présentation du déroulé de la formation

### **COMPRENDRE LA PROTECTION DES INFORMATIONS ET À LA GESTION DU CYCLE DE VIE DES DONNÉES DANS MICROSOFT PURVIEW**

- Discuter de la protection des informations et de la gestion du cycle de vie des données et de leur importance.
- Décrire l'approche de Microsoft en matière de protection des informations et de gestion du cycle de vie des données.
- Définir les termes clés associés aux solutions de protection des informations et de gestion du cycle de vie des données de Microsoft.
- Identifier les solutions qui comprennent la gestion du cycle de vie des informations et des données dans Microsoft Purview.

### **CLASSIFIER LES DONNÉES POUR LA PROTECTION ET LA GOUVERNANCE**

- Répertorier les composants de la solution Data Classification.
- Identifier les cartes disponibles dans l'onglet Vue d'ensemble de la classification des données.
- Utiliser l'explorateur de contenu et l'explorateur d'activités.

- Utiliser les types d'informations sensibles et les classificateurs pouvant être entraînés.

#### **CRÉER ET GÉRER DES TYPES D'INFORMATIONS SENSIBLES**

- Différencier les étiquettes de confidentialité intégrées et les personnalisées.
- Configurer des types d'informations sensibles avec une classification exacte basée sur des correspondances de données.
- Implémenter l'identification par empreinte de document.
- Créer des dictionnaires de mots clés personnalisés.

#### **COMPRENDRE LE CRYPTAGE DE MICROSOFT 365**

- Atténuer le risque de divulgation non autorisée de données grâce au cryptage.
- Décrire les solutions de chiffrement des données au repos et en transit de Microsoft.
- Mettre en œuvre le cryptage des services pour protéger les données des clients au niveau de la couche applicative.
- Différencier les clés gérées par Microsoft et les clés gérées par le client pour l'utilisation du cryptage des services.

#### **DÉPLOYER LE CHIFFREMENT DES MESSAGES MICROSOFT PURVIEW**

- Configurer le Chiffrement de messages Microsoft Purview pour les utilisateurs finaux.
- Implémenter le Chiffrement avancé des messages Microsoft Purview.

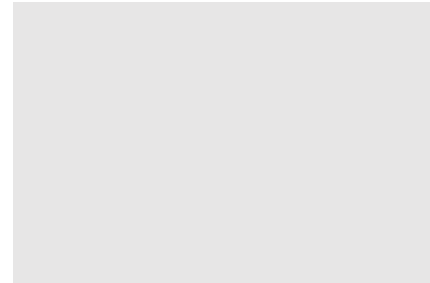
#### **CRÉER ET CONFIGURER DES ÉTIQUETTES DE SENSIBILITÉ AVEC MICROSOFT PURVIEW**

- Comprendre les bases des étiquettes de sensibilité Microsoft Purview dans Microsoft 365.
- Créer et publier des étiquettes de sensibilité pour classer et protéger les données.
- Configurer les paramètres de cryptage avec des étiquettes de sensibilité pour une sécurité améliorée des données.
- Mettre en œuvre l'étiquetage automatique pour une classification et une protection cohérente des données.
- Utiliser le tableau de bord de classification des données Microsoft Purview pour surveiller l'utilisation des étiquettes de sensibilité.
- Appliquer des étiquettes de confidentialité à Microsoft Teams, des groupes Microsoft 365 et des sites SharePoint.
- Surveiller l'utilisation des étiquettes à l'aide de l'analytique d'étiquette.
- Configurer un étiquetage local.
- Gérer les paramètres de protection et le marquage des étiquettes de confidentialité appliquées.
- Appliquer des protections et des restrictions à des e-mails.

- Appliquer des protections et des restrictions à des fichiers.

#### **CLÔTURE DE SESSION**

- Revue des principaux concepts présentés lors de la formation
- Temps d'échange sur les questions et réponses additionnelles



---

#### **Accessibilité**

L'inclusion est sujet important pour OCTO Academy.  
Nos référent-es sont à votre disposition pour faciliter l'adaptation de votre formation à vos besoins spécifiques.  
Pour les contacter : [academy.accessibilite@octo.com](mailto:academy.accessibilite@octo.com)