Information Security Administrator (SC-401)

Durée: 4 Jours **Réf de cours: M-SC401**

Résumé:

Mettre en œuvre la sécurité de l'information pour les données sensibles en utilisant Microsoft Purview et les services associés.
La formation **Administrateur de la sécurité de l'information** vous permet d'acquérir les compétences nécessaires pour planifier et mettre en œuvre la sécurité de l'information pour les données sensibles en utilisant Microsoft Purview et les services associés. Le cours couvre des sujets essentiels tels que la protection des informations, la prévention des pertes de données (DLP), la rétention et la gestion des risques liés aux initiés. Vous apprenez à protéger les données dans les environnements de collaboration Microsoft 365 contre les menaces internes et externes. En outre, vous apprenez à gérer les alertes de sécurité et à répondre aux incidents en enquêtant sur les activités, en répondant aux alertes DLP et en gérant les cas de risque d'initié. Vous apprenez également à protéger les données utilisées par les services d'intelligence artificielle dans les environnements Microsoft et à mettre en œuvre des contrôles pour protéger le contenu dans ces environnements.

Mise à jour : 28.05.2025

Public visé:

En tant qu'administrateur de la sécurité de l'information, vous planifiez et mettez en œuvre la sécurité de l'information pour les données sensibles utilisant Microsoft Purview et les services connexes. Vous êtes chargé d'atténuer les risques en protégeant les données au sein des environnements de collaboration Microsoft 365 contre les menaces internes et externes, ainsi que de sauvegarder les données utilisées par les services d'IA. Votre rôle consiste à mettre en œuvre la protection des informations, la prévention des pertes de données (DLP), la rétention et la gestion des risques liés aux initiés. Vous gérez également les alertes de sécurité et répondez aux incidents en enquêtant sur les activités, en répondant aux alertes DLP et en gérant les cas de risque d'initié. Dans ce rôle, vous collaborez avec d'autres rôles responsables de la gouvernance, des données et de la sécurité pour développer des politiques qui répondent aux objectifs de sécurité de l'information et de réduction des risques de votre organisation. Vous travaillez avec les administrateurs de la charge de travail, les propriétaires d'applications commerciales et les parties prenantes de la gouvernance pour mettre en œuvre des solutions technologiques qui soutiennent ces politiques et ces contrôles.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Planifier et implémenter la protection des données sensibles
- Classer les données pour la protection et la gouvernance
- Configurer et appliquer des étiquettes de confidentialité avec Microsoft Purview
- Déployer des stratégies de prévention contre la perte de données (DLP)
- Gérer le chiffrement des données dans Microsoft 365
- Identifier et réduire les risques internes et externes
- Sécuriser les données utilisées par les services d'IA
- Assurer la conformité des données avec les outils Microsoft Purview

Pré-requis:

- Comprendre les concepts de base de Microsoft 365
- Avoir des connaissances fondamentales en sécurité informatique
- Connaître les principes de gouvernance des données

Test et certification

Cette formation prépare les participants qui le souhaitent à passer l'examen SC-401: Microsoft Certified : Administrateur Associé en Sécurité de l'Information.

(Non inclus dans le prix de la formation)

Contenu:

Module 1 : Mettre en œuvre la protection de l'information de Microsoft Purview

- Le besoin croissant de protection des données
- Les défis de la gestion des données sensibles
- Protéger les données dans un monde de confiance zéro
- Comprendre la classification et la protection des données
- Prévenir les fuites de données et les menaces internes
- Gérer les alertes de sécurité et répondre aux menaces
- Protéger les données générées et traitées par l'IA

Module 2 : Classifier les données pour la protection et la gouvernance

- Aperçu de la classification des données
- Classifier les données à l'aide de types d'informations sensibles
- Classifier les données à l'aide de classificateurs entraînables
- Créer un classificateur entraînable personnalisé

Module 3 : Examiner et analyser la classification et la protection des données

- Examiner la classification et la protection des données
- Analyser les données classifiées avec l'explorateur de données et de contenu
- Contrôler et réviser les actions sur les données étiquetées

Module 4 : Créer et gérer des types d'informations sensibles

- Vue d'ensemble des types d'informations sensibles
- Comparer les types d'informations sensibles intégrés et personnalisés
- Créer et gérer des types d'informations sensibles personnalisés
- Créer et gérer des types d'informations sensibles correspondant exactement aux données
- Mettre en œuvre l'empreinte digitale des documents
- Décrire les entités nommées
- Créer un dictionnaire de mots-clés

Module 5 : Créer et configurer des étiquettes de sensibilité avec Microsoft Purview

- Vue d'ensemble des étiquettes de sensibilité
- Créer et configurer des étiquettes de sensibilité et des politiques d'étiquettes
- Configurer le cryptage avec les étiquettes de sensibilité
- Mettre en œuvre des politiques d'étiquetage automatique
- Utiliser le tableau de bord de classification des données pour surveiller les étiquettes de sensibilité

Module 6 : Appliquer les étiquettes de sensibilité pour la protection des données

- Fondements de l'intégration des étiquettes de sensibilité dans Microsoft 365
- Gérer les étiquettes de sensibilité dans les applications Office
- Appliquer des étiquettes de sensibilité avec Microsoft 365 Copilot pour une collaboration sécurisée
- Protéger les réunions avec des étiquettes de sensibilité
- Appliquer des étiquettes de sensibilité à Microsoft Teams, aux groupes Microsoft 365 et aux sites SharePoint

Module 7 : Classifier et protéger les données sur site avec Microsoft Purview

- Protéger les fichiers sur site avec Microsoft Purview
- Préparer votre environnement pour le scanner Microsoft Purview Information Protection
- Configurer et installer le scanner Microsoft Purview Information Protection
- Exécuter et gérer le scanner
- Appliquer les politiques de prévention des pertes de données sur les fichiers sur site

Module 8 : Comprendre le chiffrement de Microsoft 365

- Introduction au chiffrement de Microsoft 365
- Apprendre comment les données de Microsoft 365 sont chiffrées au repos
- Comprendre le chiffrement des services dans Microsoft Purview
- Explorer la gestion des clés clients à l'aide de Customer Key
- Apprendre comment les données sont chiffrées en transit

Module 9 : Déployer Microsoft Purview Message Encryption

- Mettre en œuvre le chiffrement des messages de Microsoft Purview
- Mettre en œuvre le chiffrement avancé des messages de Microsoft Purview
- Utiliser les modèles Microsoft Purview Message Encryption dans les règles de flux de courrier

Méthodes pédagogiques :

Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation.
Un support de cours officiel sera remis aux stagiaires au format électronique.

Pour profiter pleinement du support électronique dès le 1er jour, nous invitons les participants à se munir d'un PC ou d'une tablette, qu'ils pourront connecter en WiFi dans nos locaux de Rueil, Lyon ou nos agences en régions.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur