Administration de la protection et de la conformité des informations dans Microsoft 365

Durée: 4 Jours **Réf de cours: M-SC400** **Méthodes d'apprentissage: Classe à distance**

Résumé:

Cette formation permet aux participants d'acquérir les connaissances et compétences pour protéger les informations dans votre déploiement Microsoft 365. La formation se concentre sur la gouvernance des données et la protection des informations au sein de votre organisation. Elle couvre la mise en œuvre des politiques de prévention des pertes de données, les types d'informations sensibles, les étiquettes de sensibilité, les politiques de conservation des données et le cryptage des messages Office 365.
Mise à jour : 06.09.2023

Public visé:

Cette formation s'adresse aux administrateurs de la protection de l'information, praticien du risque et ingénieur en sécurité.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Expliquer la configuration des politiques de prévention des pertes de données
- Appliquer la sécurité dans des messages dans Office 365
- Décrire le processus de configuration de la gouvernance de l'information
- Expliquer l'explorateur de contenu et l'explorateur d'activité
- Décrire comment utiliser les types d'informations sensibles et les classificateurs formables
- Examiner et analyser les rapports DLP et identifier et atténuer les violations de la politique DLP
- Décrire l'intégration de la DLP avec Microsoft Cloud App Security (MCAS) et le déploiement de la DLP des points finaux
- Expliquer la configuration de la rétention en fonction des événements
- Créer des dictionnaires de mots-clés personnalisés
- Mettre en œuvre l'empreinte digitale des documents

Pré-requis:

Avant de suivre cette formation, les participants doivent avoir :

- Une connaissance de base des technologies de sécurité et de conformité de Microsoft
- Une connaissance de base des concepts de protection de l'information
- La compréhension des concepts de l'informatique dans le Cloud
- La compréhension des produits et services Microsoft 365.

Test et certification

La formation prépare à l'examen Microsoft Information Protection Administrator SC-400 dont la réussite permet d'obtenir la certification **Microsoft Certified: Information Protection Administrator Associate**

Contenu:

Mise en œuvre de la protection des informations dans Microsoft 365

- Introduction à la protection et à la gouvernance des informations dans Microsoft 365
- Classer les données pour la protection et la gouvernance
- Créer et gérer des types d'informations sensibles
- Décrire le chiffrement dans Microsoft 365
- Déployer le chiffrement des messages dans Office 365
- Configurer les étiquettes de sensibilité

Appliquer et gérer les étiquettes de sensibilité

Lab : Mise en œuvre de la protection des informations

- Attribuer des autorisations pour la conformité
- Gérer le cryptage des messages d'Office 365
- Gérer les types d'informations sensibles
- Gérer les classificateurs formables

Gérer les étiquettes de sensibilité

Implémentation de la prévention de la perte de données dans Microsoft 365

- Prévenir la perte de données dans Microsoft 365
- Mettre en œuvre la prévention des pertes de données au niveau des points d'extrémité
- Configurer les politiques DLP pour Microsoft Cloud App Security et Power Platform

Gérer les politiques et les rapports DLP dans Microsoft 365

Lab : Mise en œuvre de la prévention des pertes de données

- Gérer les politiques DLP
- Modifier la DLP des points d'extrémité
- Tester les politiques DLP

Modifier les rapports DLP

Mettre en œuvre la gouvernance de l'information dans Microsoft 365

- Gouverner l'information dans Microsoft 365
- Gérer la rétention des données dans les charges de travail Microsoft 365

Gérer les enregistrements dans Microsoft 365

Lab : Mettre en œuvre la gouvernance de l'information

- Configurer les étiquettes de rétention
- Mettre en œuvre des étiquettes de rétention
- Configurer la rétention basée sur les services
- Utiliser l'eDiscovery pour la récupération
- Configurer la gestion des documents

Surveiller et examiner les données et les activités à l'aide de Microsoft Purview (Monitor and investigate data and activities by using Microsoft Purview)

Explorer la conformité dans Microsoft 365

- Aider les organisations à gérer les risques, à protéger les données et à rester en conformité avec les réglementations et les normes avec Microsoft 365
- Planifier vos premières tâches de conformité dans Microsoft Purview
- Gérer vos exigences de conformité avec Compliance Manager
- Gérer la posture de conformité et les actions d'amélioration à l'aide du tableau de bord du gestionnaire de conformité
- Expliquer comment le score de conformité d'une organisation est déterminé

Rechercher du contenu dans le portail de conformité Microsoft Purview

- Utiliser la recherche de contenu dans le portail de conformité Microsoft Purview
- Concevoir et créer une recherche de contenu
- Prévisualiser les résultats de la recherche
- Afficher les statistiques de recherche
- Exporter les résultats et le rapport de recherche
- Configurer le filtrage des autorisations de recherche

Gérer Microsoft Purview eDiscovery (Standard)

- S'appuyer sur la fonctionnalité de recherche et d'exportation de base de la recherche de contenu de Microsoft Purview eDiscovery (Standard)
- Décrire le workflow de base d'eDiscovery (Standard)
- Créer un cas de découverte électronique

Labs :

- Explorer le gestionnaire de conformité
- Enquête de cas avec eDiscovery (Standard) et recherche de contenu
- Configurer la conformité des communications
- Configurer la gestion des risques internes
- Configurer les barrières d'information

Gérer les risques internes et de confidentialité dans Microsoft 365 (Manage Insider and Privacy Risk in Microsoft 365)

Préparer la conformité des communications Microsoft Purview

- Répertorier les améliorations apportées à la conformité des communications par rapport aux stratégies de surveillance d'Office 365 qu'elle va remplacer
- Identifier et corriger les violations de la politique relative au code de conduite
- Répertorier les conditions préalables avant de créer des stratégies de conformité des communications
- Décrire les types de modèles de stratégie prédéfinis et intégrés

Gérer les risques internes dans Microsoft Purview

- Prévenir, détecter et contenir les risques internes dans une organisation avec Microsoft Purview Insider Risk Management
- Décrire les types de modèles de stratégie intégrés et prédéfinis
- Répertorier les conditions préalables avant de créer des stratégies de risque interne
- Expliquer les actions à entreprendre dans un cas de gestion des risques internes

Mettre en œuvre les barrières d'information Microsoft Purview

- Décrire comment les barrières d'information et les composants pouvant restreindre ou permettre la communication et la collaboration entre des groupes spécifiques d'utilisateurs
- Activer les barrières à l'information
- Découvrir comment les barrières d'informations aident les organisations à déterminer les utilisateurs à ajouter ou à supprimer d'une équipe Microsoft, d'un compte OneDrive et d'un site SharePoint
- Empêcher les utilisateurs ou les groupes de communiquer et de collaborer dans Microsoft Teams, OneDrive et SharePoint grâce aux barrières d'informations

- Créer une conservation eDiscovery pour un cas eDiscovery
- Rechercher du contenu dans un cas, puis exportez ce contenu
- Fermer, rouvrir et supprimer un cas

Gérer Microsoft Purview eDiscovery (Premium)

- Décrire comment Microsoft Purview eDiscovery (Premium) s'appuie sur eDiscovery (Standard)
- Décrire le workflow de base d'eDiscovery (Premium)
- Créer et gérer des cas dans eDiscovery (Premium)
- Gérer des sources de données consignataires et non consignataires
- Analyser le contenu du cas et utiliser des outils analytiques pour réduire la taille des jeux de résultats de recherche

Gérer l'audit Microsoft Purview (Standard)

- Décrire les différences entre un Audit (Standard) et un Audit (Premium)
- Identifier les principales fonctionnalités de la solution Audit (Standard)
- Configurer et implémenter la recherche dans le journal d'audit à l'aide de la solution Audit (Standard).
- Exporter, configurer et afficher des enregistrements du journal d'audit
- Utiliser la recherche dans les journaux d'audit pour résoudre les problèmes de support courants

Gérer l'audit Microsoft Purview(Premium)

- Décrire les différences entre un Audit (Standard) et un Audit (Premium)
- Configurer et implémenter l'Audit Microsoft Purview (Premium)
- Créer des stratégies de rétention des journaux d'Audit.
- Effectuez des enquêtes à propos des comptes d'utilisateurs compromis.

Gérer les exigences réglementaires et de confidentialité avec Microsoft Priva

- Créer et gérer des politiques de gestion des risques pour la surexposition des données, le transfert de données et la minimisation des données
- Examiner et corriger les alertes de risque
- Envoyer des notifications aux utilisateurs
- Créer et gérer les demandes de droits d'objet
- Estimer et récupérer les données du sujet
- Examiner les données du sujet
- Créer des rapports sur les droits des sujets

Implémenter la gestion des accès privilégiés (si le temps le permet)

- Différencier la gestion des accès privilégiés et privileged identity management
- Décrire le flux de processus de gestion des accès privilégiés
- Décrire la configuration et l'activation de la gestion des accès privilégiés

Gérer les Customer Lockbox (si le temps le permet)

- Décrire le flux de travail du Customer Lockbox
- Approuver ou refuser une demande d'accès au Customer Lockbox.
- Auditer les actions des ingénieurs Microsoft lors de demande d'accès approuvées

Labs :

- Explorer le gestionnaire de conformité
- Enquête de cas avec eDiscovery (Standard) et recherche de contenu
- Configurer la conformité des communications
- Configurer la gestion des risques internes
- Configurer les barrières d'information

Méthodes pédagogiques :

Accès fourni au contenu digital officiel Microsoft
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 Lille.
Important
Microsoft a sécurisé ses offres de formation en ajoutant l'authentification multi-facteurs (MFA) pour accéder aux tenants de Microsoft 365 et Dynamics 365.
Pour accéder à certains TP, les stagiaires devront activer la MFA. Ils auront besoin d'un téléphone portable pour configurer et vérifier la MFA. Ils auront également besoin d'une application capable de générer des codes d'authentification. L'application suggérée est Microsoft Mobile Phone Authenticator, qui est gratuite.
Voici le lien de téléchargement de l'application ainsi que la procédure d'installation :
Download the Microsoft Mobile Phone Authenticator App
Set up your Microsoft 365 sign-in for multi-factor authentication

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 compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement