Administrateur de la sécurité de l'information (SC-401)

Date et durée

Code formation : SC-401T00-A
Durée : 4 jours
Nombre d'heures : 28 heures

Formation avec certification

Microsoft Certified : Information Security Administrator Associate

Description

À l'heure où les données des entreprises sont dispersées sur de multiples services cloud et appareils, leur protection et leur conformité réglementaire (RGPD, etc.) sont devenues un enjeu stratégique majeur. Cette formation sur **l'administration de la protection de l'information avec Microsoft Purview** vous apporte les compétences techniques nécessaires pour relever ce défi, en vous apprenant à construire et à gérer une stratégie de gouvernance des données de bout en bout.
Le programme qui se déroule sur 4 jours est conçu pour être très pratique, alternant concepts théoriques et ateliers immersifs. D'abord, vous apprendrez à **classifier vos informations sensibles** avec une grande précision. Ensuite, vous appliquerez des mesures de protection efficaces, telles que le chiffrement et les restrictions d'accès, en utilisant les étiquettes de sensibilité. Vous apprendrez aussi à déployer des **politiques de prévention de la perte de données** (DLP) pour sécuriser tout votre environnement Microsoft 365.
Ce cours vous prépare également au **passage de l'examen SC-401 inclus dans notre offre**, afin de valider vos nouvelles compétences et ainsi d'obtenir la certification Microsoft Certified: Information Security Administrator Associate (*en savoir plus dans l'onglet Certification*)**.**

Objectifs

À l'issue de la formation Microsoft SC-401 vous atteindrez les objectifs de compétences suivants :

- classifier des données pour identifier et localiser les informations sensibles à l'aide de classificateurs intégrés, personnalisés, et basés sur l'apprentissage automatique ;
- mettre en œuvre et gérer des étiquettes de sensibilité pour appliquer le chiffrement, les restrictions d'accès et le marquage visuel aux documents, e-mails et conteneurs des services (Teams, SharePoint) ;
- concevoir et configurer des politiques de prévention de la perte de données (DLP) pour empêcher le partage non autorisé d'informations sensibles sur les services cloud et les postes de travail ;
- gérer le cycle de vie des données en déployant des politiques et des étiquettes de rétention pour conserver ou supprimer le contenu conformément aux exigences de l'entreprise ;
- déployer et gérer la solution de gestion des risques internes pour détecter, investiguer et agir sur les activités potentiellement risquées des utilisateurs ;
- auditer les activités et répondre aux alertes de sécurité et de conformité à l'aide des outils d'investigation de Microsoft Purview ;
- protéger les données dans les environnements qui utilisent des services d'intelligence artificielle (IA) en appliquant les contrôles de sécurité appropriés ;
- réussir l'examen SC-401 et obtenir la certification Microsoft Certified : Information Security Administrator Associate.

Points forts

- **Un formateur expert et certifié Microsoft :** apprenez auprès d'un spécialiste certifié sur Microsoft Purview, expert dans l'administration de la protection de l'information et de la conformité.
- **Une approche pratique et centrée sur les scénarios réels :** mettez en pratique vos connaissances à travers des ateliers pratiques (labs officiels) et des études de cas basés sur des défis concrets de protection des données, de prévention des fuites (DLP) et de gestion des risques.
- **Une préparation complète à l'examen SC-401 :** préparez-vous efficacement à l'examen de certification SC-401 (voucher inclus). Des sessions de révision optimiseront vos chances de réussite.
- **Garantie de certification :** cette formation inclut le "Microsoft Exam Replay", ce qui vous permet de repasser l'examen gratuitement en cas d'échec à la première tentative.
- **Maîtrisez la gouvernance de l'information :** apprenez à traduire les exigences de conformité de l'entreprise en règle technique efficace et à gérer le cycle de vie complet de l'information sensible.

Certification

Cette formation vous prépare activement au **passage de l'examen SC-401**, qui atteste de votre expertise sur la protection de l'information, la prévention de la perte de données et la gestion de la conformité dans Microsoft Purview. La réussite de celui-ci vous permet d'obtenir la certification **Microsoft Certified: Information Security Administrator Associate.** *Un voucher (code coupon) vous sera fourni à la fin du cours, vous permettant de programmer votre examen.*

Modalités pratiques de l'examen :

Pour vous inscrire à l'examen, vous devez créer un compte sur le site web de Microsoft Learn (si vous n'en avez pas déjà un) et lier votre profil à un compte Pearson VUE. Sur le site de Pearson VUE, recherchez l'examen SC-401 : Microsoft information Security Administrator Associate. Choisissez votre mode d'examen, sélectionnez une date et une heure, puis entrez le code du voucher. Cette formation inclut le "Microsoft Exam Replay", ce qui vous permet de repasser l'examen gratuitement en cas d'échec à la première tentative.

- **Code de l'examen :** SC-401
- **Titre officiel :** Administering Information Security in Microsoft 365
- **Type de questions :** un mélange de questions incluant des études de cas, des scénarios à résoudre, des questions à choix multiples (QCM), des réponses multiples et des glisser-déposer.
- **Durée de l'examen :** Environ 100 minutes.
- **Nombre de questions :** Entre 40 et 60 questions.
- **Score de réussite :** 700 points sur un total de 1000.
- **Langues disponibles :** Anglais, Français, Allemand, Espagnol, Japonais, et autres.
- **Lieu de passage :** En centre d'examen agréé (Pearson VUE) ou en ligne avec surveillance à distance (proctoring).

À savoir : *cette certification de niveau "Associate" valide une spécialisation très recherchée. Elle constitue une excellente base pour évoluer vers des rôles d'expert, comme celui validé par la Certification Microsoft Cybersecurity Architect (SC-100). Pour maintenir votre certification active, vous devrez passer une évaluation de renouvellement gratuite sur Microsoft Learn chaque année.*
En savoir plus sur le renouvellement

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre cette formation Microsoft nécessite les prérequis suivants :

- Avoir une expérience pratique des services Microsoft 365, notamment Exchange Online, SharePoint Online et Microsoft Teams.
- Avoir des connaissances sur les concepts fondamentaux de la sécurité et de la conformité des produits Microsoft.
- Avoir des connaissances sur les concepts du cloud computing et de la gestion d'identités, notamment avec Active Directory et Microsoft Entra ID.

Public

Cette formation s'adresse aux publics suivants :

- **Les administrateurs de la protection de l'information** qui sont directement responsables du déploiement et de la gestion des solutions de classification, d'étiquetage et de protection des données.
- **Les administrateurs de la sécurité** qui cherchent à maîtriser les outils de protection de l'information pour renforcer la posture de sécurité globale de leur organisation.
- **Les responsables de la conformité et du risque** qui souhaitent utiliser les technologies Microsoft Purview pour mettre en œuvre les politiques de gouvernance et de gestion des risques internes.
- **Les administrateurs Microsoft 365** qui doivent configurer et maintenir les fonctionnalités de sécurité et de conformité au sein de leur environnement.

Cette formation s'adresse aux profils suivants

Administrateur système
Ingénieur système
Analyste de données

Programme

Module 1 : identification et classification des données sensibles

- L'identification des exigences en matière d'informations sensibles pour les données d'une organisation.
- La transcription des exigences en matière d'informations sensibles en types d'informations sensibles intégrés ou personnalisés.
- La création et la gestion des types d'informations sensibles personnalisés.
- La mise en œuvre de l'empreinte digitale des documents.
- La création et la gestion des classificateurs de correspondance exacte des données (EDM).
- La création et la gestion des classificateurs entraînables.
- La surveillance de la classification des données et l'utilisation des étiquettes à l'aide de l'explorateur de données et de l'explorateur de contenu.
- La configuration de la prise en charge de la reconnaissance optique de caractères (OCR) pour les types d'informations sensibles.

Module 2 : application de la protection par les étiquettes de sensibilité

- L'implémentation des rôles et des autorisations pour l'administration des étiquettes de sensibilité.
- La définition et la création des étiquettes de sensibilité pour les articles et les conteneurs.
- La configuration des paramètres de protection et du marquage du contenu pour les étiquettes de sensibilité.
- La configuration et la gestion des politiques de publication pour les étiquettes de sensibilité.
- La configuration et la gestion des politiques d'étiquetage automatique pour les étiquettes de sensibilité.

- L'application d'une étiquette de sensibilité aux conteneurs (Microsoft Teams, Groupes Microsoft 365, Power BI, SharePoint).
- L'application des étiquettes de sensibilité à l'aide de Microsoft Defender pour les applications cloud.

Module 3 : protection des données sur site et des points de terminaison

- La planification et la mise en œuvre du client Microsoft Purview Information Protection.
- La gestion des fichiers à l'aide du client Microsoft Purview Information Protection.
- L'application d'une classification en masse aux données locales à l'aide du scanner Microsoft Purview Information Protection.
- La conception et la mise en œuvre du chiffrement des messages Microsoft Purview.
- La conception et la mise en œuvre du chiffrement de messages avancé Microsoft Purview.

Module 4 : stratégies de prévention de la perte de données

- La conception des politiques de prévention des pertes de données en fonction des besoins d'une organisation.
- L'implémentation des rôles et des autorisations pour la prévention de la perte de données.
- La création et la gestion des politiques de prévention des pertes de données.
- La configuration des politiques de prévention des pertes de données pour la protection adaptative.
- L'interprétation de la priorité des politiques et des règles en matière de prévention des pertes de données.
- La création des stratégies de fichiers dans Microsoft Defender pour les applications cloud à l'aide d'une stratégie DLP.

Module 5 : contrôle des activités sur les points de terminaison

- La spécification des exigences de l'appareil pour Endpoint DLP, y compris les extensions.
- La configuration des règles DLP avancées pour les appareils dans les politiques DLP.
- La configuration des paramètres DLP du point de terminaison.
- La configuration de la protection juste à temps.
- La surveillance des activités des points de terminaison.

Module 6 : gouvernance du cycle de vie des données

- La planification de la conservation et de la suppression des informations en utilisant des étiquettes de conservation.
- La création, la configuration et la gestion des étendues adaptatives.
- La création des étiquettes de conservation pour la gestion du cycle de vie des données.
- La configuration d'une politique d'étiquette de rétention pour publier des étiquettes.
- La configuration d'une politique d'étiquette de rétention pour appliquer automatiquement les étiquettes.
- L'interprétation des résultats de la priorité des politiques, notamment en utilisant la recherche de politiques.
- La création et la configuration des politiques de rétention.
- La récupération du contenu conservé dans Microsoft 365.

Module 7 : détection et investigation des risques internes

- L'implémentation des rôles et des autorisations pour la gestion des risques internes.
- La planification et la mise en œuvre des connecteurs de gestion des risques internes.
- La planification et la mise en œuvre de l'intégration avec Microsoft Defender pour Endpoint.
- La configuration et la gestion des paramètres de gestion des risques internes.
- La configuration des indicateurs de politique.
- La sélection d'un modèle de politique approprié.
- La création et la gestion des politiques de gestion des risques internes.
- La gestion des paramètres des preuves médico-légales.
- L'activation et la configuration des niveaux de risque interne pour la protection adaptative.

- La gestion des alertes et des cas de risques internes.
- La gestion du flux de travail de gestion des risques internes, y compris les modèles d'avis.

Module 8 : audit, investigation et réponse aux alertes

- L'attribution des licences utilisateur Microsoft Purview Audit (Premium).
- L'investigation des activités à l'aide de Microsoft Purview Audit.
- La configuration des politiques de conservation des audits.
- L'analyse des activités de Purview à l'aide de l'explorateur d'activités.
- La réponse aux alertes de prévention de perte de données dans le portail Microsoft Purview.
- L'investigation des activités à risque interne en utilisant le portail Microsoft Purview.
- La réponse aux alertes Purview dans Microsoft Defender XDR.
- La réponse aux alertes de politique de fichier Defender for Cloud Apps.
- L'effectuation de recherches à l'aide de la recherche de contenu.

Module 9 : sécurité des données pour l'intelligence artificielle (DSPM)

- L'implémentation de contrôles dans Microsoft Purview pour protéger le contenu dans un environnement qui utilise des services d'IA.
- L'implémentation de contrôles dans les charges de travail de productivité Microsoft 365 pour protéger le contenu dans un environnement qui utilise des services d'IA.
- L'implémentation des prérequis pour la gestion de la posture de sécurité des données (DSPM) pour l'IA.
- La gestion des rôles et des autorisations pour DSPM pour l'IA.
- La configuration de DSPM pour les politiques d'IA.
- La surveillance des activités dans DSPM pour l'IA.

Module 10 : préparation à l'examen SC-401

- Révision des concepts clés du cours.
- Séance de conseils et d'astuces pour l'examen.
- Analyse d'exemples de questions d'examen.
- Découverte des ressources complémentaires pour la préparation.

Microsoft®, Microsoft 365®, Microsoft Purview®, Microsoft Defender® et Microsoft Azure® sont des marques déposées ou des marques commerciales de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.