

Certifiante

Formation Protéger les informations sensibles avec Microsoft Purview à l'ère de l'IA (SC-401)

Réf. SF34722

Préparez la certification Microsoft Certified: Information Security Administrator Associate en apprenant à classer, protéger et surveiller les données sensibles de votre organisation, jusqu'aux usages de l'IA générative

4 j
Durée

3 000 € HT
Inter / participant

0
Sessions à venir

Objectifs pédagogiques

- ✓ Classer et protéger les données sensibles avec Microsoft Purview : types d'informations sensibles, étiquettes de confidentialité, chiffrement et protection des données locales
- ✓ Implémenter et gérer des stratégies de protection contre la perte de données pour Microsoft 365, les points de terminaison, Power Platform et les applications cloud
- ✓ Configurer la rétention, la récupération et le cycle de vie du contenu Microsoft 365 à l'aide d'étiquettes, de stratégies et d'étendues adaptatives
- ✓ Implémenter la gestion des risques internes et la protection adaptative pour détecter et traiter les comportements à risque
- ✓ Investiguer les activités et localiser le contenu avec Microsoft Purview Audit et eDiscovery
- ✓ Sécuriser les interactions et les environnements IA (Microsoft 365 Copilot, applications IA d'entreprise et de développeurs) avec DSPM for AI et les contrôles Microsoft Purview
- ✓ Réussir l'examen de certification Microsoft Certified: Information Security Administrator Associate (SC-401)

Public visé & prérequis

Public visé Administrateurs systèmes et réseaux

Prérequis- Bonne connaissance opérationnelle des services Microsoft 365 et de leur administration - Pratique de PowerShell pour l'administration Microsoft 365 - Familiarité avec Microsoft Entra, le portail Microsoft Defender et Microsoft Defender for Cloud Apps - Notions de conformité et de gouvernance des données : savoir traduire une exigence réglementaire ou interne en règle technique (classification, étiquetage, rétention) - Compréhension du fonctionnement de Microsoft 365 Copilot et de sa façon d'accéder aux données de l'organisation - Aucune certification préalable n'est exigée pour passer l'examen SC-401

Programme détaillé

Implémenter Microsoft Purview Protection des données

- Protéger les données sensibles dans un monde numérique : enjeux de classification, de protection et de surveillance des données dans les environnements cloud, endpoint et IA
- Classer les données pour la protection et la gouvernance : identifier son paysage de données et traduire les exigences métier en exigences de classification
- Examiner et analyser la classification et la protection des données : rapports Information Protection, Explorateur de données, Explorateur de contenu et Explorateur d'activités
- Créer et gérer des types d'informations sensibles : types intégrés et personnalisés, empreinte numérique de document, correspondances exactes de données (EDM), classifieurs entraînaables et prise en charge de l'OCR
- Créer et configurer des étiquettes de confidentialité : rôles et autorisations, étiquettes pour les éléments et les conteneurs, paramètres de protection et marquage de contenu
- Appliquer des étiquettes de confidentialité pour la protection des données : stratégies de publication, étiquetage automatique, application aux conteneurs Teams, groupes, SharePoint et Power BI
- Classer et protéger les données locales : déploiement du scanneur et du client Protection des données, classification en bloc des partages de fichiers

- Comprendre le chiffrement Microsoft 365 : chiffrement au repos et en transit, gestion des clés et options côté client
- Protéger l'e-mail avec le chiffrement de messages Microsoft Purview : règles de flux de messagerie, chiffrement avancé et personnalisation de l'expérience destinataire

Activités pratiques :

- Création de types d'informations sensibles personnalisés et test de détection sur des documents
- Configuration et publication d'une étiquette de confidentialité avec chiffrement et marquage de contenu
- Mise en place d'une stratégie d'étiquetage automatique et analyse des résultats dans l'Explorateur de contenu
- Configuration du chiffrement des messages et validation sur un envoi externe

Implémenter et gérer la protection contre la perte de données Microsoft Purview

- Comprendre et planifier la protection contre la perte de données : évaluation des risques, décisions de protection et cadrage d'une stratégie DLP qui ne bloque pas le travail quotidien
- Créer et gérer des stratégies de protection contre la perte de données : rôles et autorisations, conditions de détection, étendue, actions, priorité des stratégies et des règles
- Implémenter la protection contre la perte de données de point de terminaison : intégration des appareils, paramètres et extensions, règles avancées, mode simulation, protection juste-à-temps
- Configurer des stratégies DLP pour Defender for Cloud Apps et Power Platform : connecteurs Power Platform, applications cloud tierces et stratégies de fichiers
- Examiner et répondre aux alertes de protection contre la perte de données : traitement des alertes dans le portail Purview et dans Microsoft Defender XDR, actions correctives et documentation des résultats

Activités pratiques :

- Création d'une stratégie DLP en mode simulation, analyse des correspondances puis passage en application
- Intégration d'un poste et configuration de règles Endpoint DLP (USB, impression, chargement navigateur)
- Configuration d'une stratégie DLP pour un connecteur Power Platform
- Investigation d'une alerte DLP et rédaction du compte rendu de traitement

Implémenter et gérer la rétention et la récupération Microsoft 365

- Comprendre la rétention dans Microsoft Purview : conservation, suppression et arbitrages entre conformité, réduction des risques et volume de données
- Implémenter et gérer la rétention et la récupération Microsoft 365 : étiquettes et stratégies de rétention, étendues de stratégie adaptatives, publication et application automatique, priorité des stratégies et récupération du contenu supprimé dans SharePoint et Exchange

Activités pratiques :

- Création d'étiquettes et d'une stratégie de rétention appliquées à plusieurs charges de travail
- Configuration d'une étendue de stratégie adaptative et vérification de son périmètre
- Récupération d'un contenu supprimé et analyse du résultat de priorité des stratégies

Implémenter et gérer la Gestion des risques internes Microsoft Purview

- Comprendre la gestion des risques internes : typologie des risques d'initié, analyse contextuelle des activités et respect de la confidentialité des utilisateurs
- Se préparer pour la Gestion des risques internes : rôles et autorisations, paramètres, connecteurs et intégration à Microsoft Defender pour point de terminaison
- Créer et gérer des stratégies de gestion des risques internes : choix du modèle de stratégie, indicateurs, seuils de déclenchement et cycle de vie des stratégies
- Examiner les alertes à risque internes et l'activité associée : triage des alertes, gestion des cas, preuve d'investigation, flux de travail et modèles d'avis
- Implémenter la protection adaptative : niveaux de risque interne pilotant l'application des stratégies DLP, de l'accès conditionnel et de la gestion du cycle de vie des données

Activités pratiques :

- Configuration des paramètres et des indicateurs de la gestion des risques internes
- Création d'une stratégie à partir d'un modèle et simulation d'une activité à risque
- Triage d'une alerte, ouverture d'un cas et envoi d'un avis utilisateur
- Activation de la protection adaptative et liaison avec une stratégie DLP

Activité d'audit et de recherche dans Microsoft Purview

- Mener des enquêtes avec Microsoft Purview Audit : licences Audit (Premium), recherche dans le journal d'audit, stratégies de rétention d'audit et investigation des activités Microsoft 365, Copilot et applications IA
- Rechercher du contenu avec Microsoft Purview eDiscovery : création de cas, définition des critères de recherche, localisation des messages, fichiers et données de l'organisation

Activités pratiques :

- Recherche d'activités dans le journal d'audit et interprétation des événements retournés
- Configuration d'une stratégie de rétention d'audit
- Création d'un cas eDiscovery et exécution d'une recherche de contenu ciblée

Sécuriser les interactions et les environnements IA avec Microsoft Purview

- Comprendre comment sécuriser des données IA avec Microsoft Purview : prérequis, rôles et autorisations de la gestion de la posture de sécurité des données (DSPM) pour l'IA, évaluation des risques d'exposition et découverte des outils IA utilisés
- Sécuriser les interactions Microsoft 365 Copilot : contrôles de protection appliqués aux invites et aux réponses, gestion de l'activité IA et supervision des usages
- Sécuriser les applications IA d'entreprise et basées sur un navigateur : découverte des usages, évaluation des besoins de conformité, contrôles de protection, de rétention et d'usage responsable
- Sécuriser les environnements IA pour développeurs : découverte des applications, évaluation de l'accès aux données, détection de l'usage d'IA générative et application dynamique selon le comportement utilisateur et la sensibilité des données

Activités pratiques :

- Activation de DSPM pour l'IA et analyse du rapport d'exposition des données
- Configuration d'une stratégie DSPM pour l'IA et suivi des activités remontées
- Audit d'interactions Microsoft 365 Copilot et vérification du respect des étiquettes de confidentialité
- Mise en place de contrôles sur une application IA de navigateur via Defender for Cloud Apps

Préparation à la certification

- Modalités de l'examen : SC-401, 100 minutes, questions à choix multiples avec composants interactifs possibles, examen surveillé, seuil de réussite 700/1000, disponible en français
- Examen blanc : passage d'un test en conditions réelles à partir de l'évaluation pratique officielle
- Stratégies de réponse : gestion du temps, lecture des énoncés, élimination des distracteurs sur les questions de scénario
- Révision ciblée : synthèse des points clés par domaine évalué — protection des informations, DLP et rétention, risques, alertes et activités
- Planification : inscription à l'examen via Pearson VUE, ressources officielles et conseils de préparation post-formation

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de la filière Digital Workplace & Microsoft 365 : 4,9/5 — 89 avis

Esther C. — le programme a été adapté par rapport aux besoins et connaissances des participants, c'était appréciable

Idil O. — La formatrice était très à l'écoute, pédagogue. Elle a pris le temps de nous expliquer chaque exercice et j'ai beaucoup appris en 2 jours.

Ils nous font confiance

Cette année notre filière Digital Workplace & Microsoft 365 a accompagné plus de 150 entreprises dont :

AXA ASSISTANCE FRANCE MEDIABRANDS COVAGE INFRA CEGEDIM GRANT THORNTON FRANCE ALIAPUR BIOMERIEUX SA BOUYGUES TRAVAUX PUBLICS LBC FRANCE SCHNEIDER ELECTRIC +140 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com