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

Description

Développez vos compétences en sécurité de l’information avec Microsoft 365

La sécurité des données sensibles est aujourd’hui un enjeu majeur pour toutes les organisations. La formation « Administrateur de la sécurité de l’information (SC-401) » vous prépare à planifier et implémenter des stratégies de protection efficaces grâce à Microsoft 365 et Microsoft Purview. Ce cours vous donne les compétences essentielles pour sécuriser les environnements de collaboration modernes et gérer les risques internes et externes.

En suivant cette formation SC-401, vous apprendrez à prévenir les fuites de données, à appliquer des politiques de rétention, à maîtriser la gestion des risques liés aux collaborateurs et à sécuriser les données utilisées par les services d’IA. Grâce à une approche complète et pratique, vous saurez comment protéger vos informations les plus critiques, gérer les alertes de sécurité et répondre aux incidents en temps réel. Vous serez également capable de configurer des stratégies avancées de prévention contre la perte de données (DLP) et de protéger les communications sensibles.

Renforcez la protection de vos données stratégiques

Le programme est construit autour des outils et services les plus avancés de **Microsoft 365** pour garantir la meilleure protection des données. Vous découvrirez comment classifier, étiqueter et chiffrer les informations sensibles tout en respectant les exigences de conformité de votre organisation. De plus, vous saurez comment intégrer les contrôles de sécurité dans les processus d’utilisation de l’intelligence artificielle.

Niveau
Intermédiaire
Contenu du cours
Module 1 : Protéger les données sensibles dans un monde numérique

- Le besoin croissant de protection des données
- Les défis de la gestion des données sensibles
- Protéger les données dans un monde Zero Trust
- 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

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

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

- Examiner les informations sur la classification et la protection
- Analyser les données classifiées avec l'explorateur de données et de contenu
- Surveiller et examiner 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 et personnalisés
- Créer et gérer des types d’informations sensibles personnalisés
- Créer et gérer des types d’informations sensibles à correspondance exacte
- Implémenter l’empreinte digitale de documents
- Décrire les entités nommées
- Créer un dictionnaire de mots-clés

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

- Présentation des étiquettes de confidentialité
- Créer et configurer des étiquettes et des stratégies d'étiquetage
- Configurer le chiffrement avec les étiquettes de confidentialité
- Implémenter les politiques d’étiquetage automatique
- Utiliser le tableau de bord de classification des données pour surveiller les étiquettes

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

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

Module 7 : Comprendre le chiffrement dans Microsoft 365

- Présentation du chiffrement dans Microsoft 365
- Chiffrement des données au repos
- Comprendre le chiffrement de service dans Microsoft Purview
- Gérer les clés clients avec Customer Key
- Chiffrement des données en transit

Module 8 : Déployer le chiffrement des messages Microsoft Purview

- Implémenter le chiffrement des messages Microsoft Purview
- Implémenter le chiffrement avancé des messages
- Utiliser les modèles de chiffrement dans les règles de flux de courrier

Module 9 : Prévenir la perte de données avec Microsoft Purview

- Présentation de la prévention contre la perte de données (DLP)
- Planifier et concevoir des stratégies DLP
- Déployer et simuler des stratégies DLP
- Créer et gérer des stratégies DLP
- Intégrer la Protection adaptative avec DLP
- Utiliser les analyses DLP pour identifier les risques

- Comprendre les alertes DLP et le suivi des activités

Module 10 : Implémenter la prévention contre la perte de données sur les terminaux

- Présentation de la DLP pour les terminaux
- Comprendre le processus d'implémentation
- Enrôler des appareils pour la DLP
- Configurer les paramètres de la DLP sur terminaux
- Créer et gérer des stratégies de DLP sur terminaux
- Déployer l'extension de navigateur Microsoft Purview
- Configurer la protection Just-in-Time (JIT)

Module 11 : Configurer les stratégies DLP pour Defender for Cloud Apps et Power Platform

- Configurer les stratégies DLP pour Power Platform
- Intégrer DLP avec Microsoft Defender for Cloud Apps
- Configurer des stratégies dans Defender for Cloud Apps
- Gérer les violations DLP dans Defender for Cloud Apps

Module 12 : Comprendre la gestion du risque d'initié avec Microsoft Purview

- Qu'est-ce qu'un risque interne ?
- Présentation de la gestion du risque d'initié
- Fonctionnalités de la gestion du risque d'initié
- Étude de cas : Protéger les données sensibles

Module 13 : Se préparer à la gestion des risques internes avec Microsoft Purview

- Planifier la gestion des risques internes
- Préparer votre organisation
- Configurer les paramètres
- Intégrer des sources de données et outils

Module 14 : Créer et gérer des stratégies de gestion du risque d'initié

- Comprendre les modèles de stratégie
- Comparer stratégies rapides et personnalisées
- Créer une stratégie personnalisée
- Gérer les stratégies de risque d'initié

Module 15 : Gérer les défis de sécurité des données IA avec Microsoft Purview

- Appliquer les étiquettes de confidentialité avec Microsoft 365 Copilot
- Utiliser Endpoint DLP pour empêcher l’exposition des données IA
- Détecter l’utilisation de l’IA générative
- Étude de cas : Protéger les données IA avec une protection adaptative

Module 16 : Gérer la conformité avec Microsoft Purview pour Microsoft 365 Copilot

- Auditer les interactions Copilot avec Microsoft Purview
- Examiner et supprimer les interactions avec eDiscovery (Premium)
- Gérer la rétention Copilot avec Microsoft Purview
- Surveiller la conformité des communications Copilot

Module 17 : Identifier et réduire les risques de sécurité des données IA

- Comprendre les risques de sécurité IA
- Présentation de la gestion de la posture de sécurité des données (DSPM) pour l'IA
- Configurer le DSPM pour l'IA
- Analyser les rapports de sécurité IA
- Utiliser les évaluations de données pour détecter les risques de partage excessif

Module 18 : Introduction à la sécurité et à la conformité des informations dans Microsoft Purview

- Fondements de la sécurité et conformité des données
- Connaître vos données
- Protéger vos données
- Prévenir la perte de données
- Gouverner vos données

Module 19 : Implémenter et gérer la rétention avec Microsoft Purview

- Vue d’ensemble de la rétention
- Créer et configurer des stratégies de rétention
- Créer et configurer des étendues adaptatives
- Créer et publier des étiquettes de rétention
- Appliquer des étiquettes de rétention dans Microsoft 365
- Configurer la rétention basée sur des événements
- Créer et gérer des étiquettes de rétention automatique
- Déclarer des enregistrements à l'aide d'étiquettes de rétention
- Effectuer des révisions de destruction

Lab / Exercices

- Ce cours vous donne un accès exclusif au laboratoire officiel Microsoft, vous permettant de mettre en pratique vos compétences dans un environnement professionnel.

Documentation

- Accès à Microsoft Learn, la plateforme d'apprentissage en ligne Microsoft, offrant des ressources interactives et des contenus pédagogiques pour approfondir vos connaissances et développer vos compétences techniques.

Profils des participants

- Administrateurs de la sécurité de l'information
- Responsables de la conformité et de la gouvernance des données
- Spécialistes en cybersécurité
- Administrateurs Microsoft 365
- Consultants en protection des données

Connaissances Préalables

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

Objectifs

- 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

Description
Administrateur de la sécurité de l'information (SC-401)
Prix de l'inscription en Présentiel (CHF)
3200
Prix de l'inscription en Virtuel (CHF)
3000
Durée (Nombre de Jours)
4
Reference
SC-401