Administrateur Microsoft Information Protection

Préparation certification Microsoft SC401

DESCRIPTION

Cette formation vous fournira les compétences essentielles pour planifier et déployer la sécurité de l'information sur les données sensibles en utilisant Microsoft Purview et ses services associés. Vous apprendrez à sécuriser les données dans les environnements collaboratifs Microsoft 365, en vous protégeant contre les menaces internes et externes.

Vous maîtriserez la gestion des alertes de sécurité et la réponse aux incidents, en enquêtant sur les activités suspectes, en traitant les alertes DLP et en gérant les situations à risque liées aux utilisateurs internes. Par ailleurs, vous découvrirez comment protéger les données exploitées par les services d'intelligence artificielle dans les environnements Microsoft, tout en mettant en place des contrôles pour sécuriser vos contenus.

OBJECTIFS PEDAGOGIQUES

A l'issue de cette formation, les participants seront en capacité de :

- Implémenter Microsoft Purview Information Protection
- Implémenter et gérer Microsoft Purview Data Loss Prevention
- Implémenter et gérer la Gestion des risques internes Microsoft Purview
- Protéger les données dans des environnements IA avec Microsoft Purview
- Implémenter et gérer la rétention et la récupération de Microsoft 365
- Utiliser l'activité d'audit et de recherche dans Microsoft Purview

PUBLIC CIBLE

- Administrateurs
- Administrateurs de la protection des données
- Opérateurs de sécurité

PRE-REQUIS

Pour participer à cette formation, Il faut avoir suivi la formation « SC-900 : Microsoft Security, Compliance, and Identity Fundamentals » et avoir de solides connaissances sur Azure et Microsoft 365.

Classe à distance
Sécurité

Code :
SC401

Durée :
4 jour(s) (28,00 heures)

Exposés : **40 %**
Cas pratiques : **20 %**
Echanges d'expérience : **20 %**

Inter-entreprises :
Prochaines sessions disponibles sur notre site web.
Tarif : 2 970,00 € HT / participant

Intra-entreprise :
Tarifs et dates sur demande.

Un niveau d'anglais B1 est recommandé, retrouvez les niveaux sur ce lien : Classification des niveaux de langue

METHODE PEDAGOGIQUE
Formation avec apports théoriques, échanges sur les contextes des participants et retours d'expérience pratique des formateurs, complétés de travaux pratiques et de mises en situation.

PROFIL DES INTERVENANTS

Cette formation est dispensée par un·e ou plusieurs consultant·es d'OCTO Technology ou de son réseau de partenaires, expert·es reconnus des sujets traités.

Le processus de sélection de nos formateurs et formatrices est exigeant et repose sur une évaluation rigoureuse leurs capacités techniques, de leur expérience professionnelle et de leurs compétences pédagogiques.

MODALITÉS D'ÉVALUATION ET FORMALISATION À L'ISSUE DE LA FORMATION
L'évaluation des acquis se fait tout au long de la session au travers des ateliers et des mises en pratique. Afin de valider les compétences acquises lors de la formation, un formulaire d'auto-positionnement est envoyé en amont et en aval de celle-ci. Une évaluation à chaud est également effectuée en fin de session pour mesurer la satisfaction des stagiaires et un certificat de réalisation leur est adressé individuellement.

PROGRAMME PEDAGOGIQUE DETAILLE

PROTÉGER LES DONNÉES SENSIBLES DANS UN MONDE NUMÉRIQUE

- Décrire les défis liés à la protection des données sensibles dans les environnements cloud et IA.
- Expliquer comment Microsoft Purview active la classification, l'étiquetage et la protection des données.
- Identifier comment la protection contre la perte de données (DLP) empêche le partage de données non autorisé.
- Découvrir comment Insider Risk Management permet de détecter les menaces potentielles.
- Explorer les outils de surveillance de la sécurité pour détecter et répondre aux risques de données.

CLASSIFIER DES DONNÉES A DES FINS DE PROTECTION ET DE GOUVERNANCE

- Expliquer l'importance de la classification des données pour la

protection et la gouvernance.
- Décrire la façon dont les types d'informations sensibles (SIT) classifient les données structurées.
- Expliquer comment les classifieurs pouvant être entraînés identifient les données non structurées.
- Créer un classifieur entraîné personnalisé pour détecter le contenu spécifique à organisation.

EXAMINER ET ANALYSER LA CLASSIFICATION ET LA PROTECTION DES DONNÉES

- Interpréter les rapports de protection des informations pour évaluer les tendances de classification et de protection.
- Examiner le contenu étiqueté à l'aide de l'Explorateur de données et de l'Explorateur de contenu pour identifier les modèles de classification.
- Analyser l'activité des utilisateurs dans l'Explorateur d'activités pour détecter les violations de stratégie et les risques de sécurité potentiels.
- Utiliser les outils Microsoft Purview pour améliorer la sécurité des données, maintenir la conformité et affiner les stratégies de protection.

CRÉER ET GÉRER DES TYPES D'INFORMATIONS SENSIBLES

- Différencier les étiquettes de confidentialité intégrées et personnalisées.
- Configurer des types d'informations sensibles avec une classification basée sur la correspondance exacte des données.
- Implémenter l'identification par empreinte de document.
- Créer des dictionnaires personnalisés de mots clés.

CRÉER ET CONFIGURER DES ÉTIQUETTES DE CONFIDENTIALITÉ AVEC MICROSOFT PURVIEW

- Comprendre les principes de base des étiquettes de confidentialité Microsoft Purview dans Microsoft 365.
- Créer et publier des étiquettes de confidentialité pour classifier et protéger les données.
- Configurer les paramètres de chiffrement avec des étiquettes de confidentialité pour améliorer la sécurité des données.
- Implémenter l'étiquetage automatique pour une classification et une protection des données cohérentes.
- Utiliser le tableau de bord de classification des données Microsoft Purview pour surveiller l'utilisation des étiquettes de confidentialité.

APPLIQUER DES ÉTIQUETTES DE CONFIDENTIALITÉ POUR LA PROTECTION DES DONNÉES

- Comprendre les bases de l'intégration des étiquettes de confidentialité dans Microsoft 365.
- Gérer l'utilisation de l'étiquette de confidentialité dans les applications Office pour la conformité de la sécurité.
- Sécuriser les réunions Outlook et Teams avec des étiquettes de confidentialité.
- Appliquer des étiquettes aux groupes Microsoft 365, SharePoint et OneDrive pour la protection des données.

CLASSIFIER ET PROTÉGER DES DONNÉES LOCALES AVEC MICROSOFT PURVIEW

- Préparer votre environnement pour prendre en charge le scanneur Microsoft Purview Information Protection.
- Configurer les paramètres du scanneur, l'authentification et les prérequis de déploiement.
- Exécuter des analyses en mode de découverte ou d'application.
- Appliquer des étiquettes de confidentialité et une protection aux fichiers locaux.
- Utiliser des règles de protection contre la perte de données (DLP) pour restreindre l'accès ou les fichiers en quarantaine en fonction de la stratégie.

COMPRENDRE LE CRYPTAGE DE MICROSOFT 365

- Expliquer comment le cryptage atténue le risque de divulgation non autorisée de données.
- Décrire les solutions de chiffrement des données au repos et en transit de Microsoft.
- Expliquer comment Microsoft 365 met en œuvre le cryptage des services pour protéger les données des clients au niveau de la couche applicative.
- Comprendre les différences entre les clés gérées par Microsoft et les clés gérées par le client pour l'utilisation du cryptage des services.

PROTÉGER L'E-MAIL AVEC LE CHIFFREMENT DES MESSAGES MICROSOFT PURVIEW

- Activer Microsoft Purview Message Encryption à l'aide d'Azure Rights Management.
- Appliquer automatiquement le chiffrement à l'aide de règles de

flux de messagerie.
- Personnaliser la marque pour les messages chiffrés et le portail de chiffrement.
- Utiliser Advanced Message Encryption pour contrôler l'expiration et la révocation des messages.

PRÉVENIR LA PERTE DE DONNÉES DANS MICROSOFT PURVIEW

- Comprendre l'objectif et les avantages de Microsoft Purview DLP.
- Planifier, concevoir, simuler et déployer des stratégies DLP.
- Appliquer la protection adaptative pour les contrôles de données dynamiques basés sur les risques.
- Utiliser l'analytique DLP pour améliorer l'efficacité des stratégies.
- Surveiller, examiner et affiner les stratégies à l'aide d'alertes et de suivi des activités.

IMPLÉMENTER LA PROTECTION CONTRE LA PERTE DES DONNÉES (DLP) DE POINT DE TERMINAISON AVEC MICROSOFT PURVIEW

- Comprendre les avantages de la DLP de point de terminaison
- Intégrer des appareils pour la protection contre la perte de données de point de terminaison
- Configurer les paramètres DLP du point de terminaison
- Créer et gérer des stratégies DLP de point de terminaison

CONFIGURER DES STRATÉGIES DLP POUR MICROSOFT DEFENDER FOR CLOUD APPS ET POWER PLATFORM

- Décrire l'intégration de DLP à Microsoft Defender for Cloud Apps.
- Configurer des stratégies dans Microsoft Defender for Cloud Apps.

EXAMINER ET RÉPONDRE AUX ALERTES DE PROTECTION CONTRE LA PERTE DE DONNÉES MICROSOFT PURVIEW

- Examiner les alertes DLP dans Microsoft Purview et Microsoft Defender XDR
- Passer en revue les détails de l'alerte, les activités utilisateur associées et les événements mis en correspondance
- Appliquer des actions de correction et mettre à jour les états d'alerte ou d'incident
- Attribuer la propriété, documenter les décisions et prendre en charge la responsabilité

- Reconnaître quand les stratégies DLP peuvent avoir besoin d'ajustements en fonction des résultats d'investigation

COMPRENDRE LA GESTION DU RISQUE INITIÉ DANS LE CADRE DE MICROSOFT PURVIEW

- Définir les risques internes et leurs effets sur les organisations.
- Comprendre l'objectif de la gestion du risque d'initié dans le cadre de Microsoft Purview.
- Identifier les principales fonctionnalités telles que les stratégies, les signaux, l'analytique, les tableaux de bord et les outils d'investigation.
- Reconnaitre la façon dont ces outils détectent et résolvent les risques potentiels.
- Explorer des scénarios qui illustrent des stratégies de gestion des risques efficaces.

SE PRÉPARER POUR GESTION DES RISQUES INTERNES MICROSOFT PURVIEW

- Collaborer avec les parties prenantes pour se préparer à la gestion des risques internes.
- Comprendre ce qui est nécessaire pour répondre aux prérequis de l'implémentation.
- Configurer les paramètres pour s'aligner sur les besoins en matière de conformité et de confidentialité.
- Connecter des outils et des sources de données améliore la gestion des risques.

CRÉER ET GÉRER DES STRATÉGIES DE GESTION DES RISQUES INTERNES

- Expliquer l'objectif des modèles de stratégie.
- Identifier quand utiliser des stratégies rapides ou personnalisées.
- Créer des stratégies rapides pour les scénarios courants.
- Générer et configurer des stratégies personnalisées pour des risques spécifiques.
- Mettre à jour et gérer les stratégies en fonction des besoins de l'organisation.

EXAMINER LES ALERTES A RISQUE INTERNES ET L'ACTIVITÉ ASSOCIÉE

- Découvrir comment les alertes sont générées et hiérarchisées dans la gestion des risques internes.
- Paramétrer les stratégies et les seuils pour gérer efficacement le volume d'alertes.

- Utiliser le tableau de bord alertes et les détails des alertes pour trier et répondre à l'activité à risque.
- Examiner le comportement à l'aide d'onglets tels que tous les facteurs de risque, l'Explorateur d'activités et l'activité utilisateur.
- Intégrer à Microsoft Defender XDR pour une investigation plus large des menaces.
- Créer, gérer et résolver les cas de gestion des risques internes.

IMPLÉMENTER LA PROTECTION ADAPTATIVE DANS LA GESTION DES RISQUES INTERNES

- Décrire la protection adaptative et son rôle dans l'atténuation dynamique des risques.
- Configurer les paramètres de niveau de risque et personnalisez les niveaux de risque en fonction des besoins de votre organisation.
- Configurer la protection adaptative avec une configuration rapide ou personnalisée.
- Gérer la protection adaptative pour passer en revue les métriques de stratégie, suivre les utilisateurs dans l'étendue et évaluer les niveaux de risque.

DÉCOUVRIR DES INTERACTIONS IA AVEC MICROSOFT PURVIEW

- Expliquer comment Microsoft Purview DSPM pour l'IA et l'audit aident à identifier les risques liés aux données dus à l'IA.
- Configurer DSPM pour l'IA afin de détecter l'activité des outils d'IA tels que Microsoft 365 Copilot et autres outils d'entreprise.
- Utiliser Microsoft Purview Audit pour rechercher et examiner les interactions de Copilot.
- Analyser l'activité et les risques de l'IA à l'aide de rapports et d'insights intégrés.

PROTÉGER LES DONNÉES SENSIBLES CONTRE LES RISQUES LIÉS À L'IA

- Utiliser des étiquettes de confidentialité pour contrôler la façon dont les outils IA accèdent et gèrent le contenu.
- Configurer le DLP du point de terminaison pour restreindre les actions à risque dans les navigateurs.
- Appliquer DSPM pour les recommandations d'IA pour protéger les données sensibles dans les solutions Microsoft Purview.

RÉGIR L'UTILISATION DE L'IA AVEC MICROSOFT PURVIEW

- Appliquer des stratégies de rétention pour gérer le cycle de vie

de Copilot et d'autres contenus générés par l'IA à l'aide de la gestion du cycle de vie des données.
- Examiner et supprimer l'historique des interactions Copilot à l'aide d'eDiscovery (Premium).
- Créer des stratégies pour évaluer les messages Copilot et d'autres communications liées à l'IA à l'aide de la conformité des communications.

ÉVALUER ET ATTÉNUER LES RISQUES D'IA AVEC MICROSOFT PURVIEW

- Détecter l'utilisation générative de l'IA avec la gestion des risques internes.
- Utiliser le scoring des risques pour identifier les utilisateurs qui présentent un risque plus élevé.
- Appliquer des protections dynamiques avec la protection adaptative en fonction du comportement de l'utilisateur.
- Utiliser des évaluations de données pour identifier les risques de sur-partage dans les interactions IA.

COMPRENDRE LA RÉTENTION DANS MICROSOFT PURVIEW

- Identifier les cas d'utilisation courants pour l'application de la rétention.
- Expliquer comment la rétention prend en charge la protection des données aux côtés d'outils tels que la prévention des pertes de données.
- Appliquer les paramètres de conservation à des utilisateurs, sites ou types de contenu spécifiques.
- Reconnaître ce que la rétention contrôle et ce qu'elle ne contrôle pas.

IMPLÉMENTER ET GÉRER LA RÉTENTION ET LA RÉCUPÉRATION DE MICROSOFT 365

- Planifier la conservation et la disposition à l'aide d'étiquettes de conservation.
- Créer, publier et appliquer automatiquement des étiquettes de rétention.
- Utiliser des portées adaptatives pour cibler dynamiquement les utilisateurs, les groupes ou les sites.
- Configurer les politiques de conservation pour les charges de travail Microsoft 365.
- Interpréter le résultat lorsque plusieurs paramètres de rétention s'appliquent.
- Restaurer les éléments supprimés et les versions précédentes du contenu sur SharePoint, OneDrive et Teams.

RECHERCHER ET INVESTIGUER AVEC AUDIT MICROSOFT PURVIEW

- Identifier les différences entre Microsoft Purview Audit (Standard) et Audit (Premium).
- Configurer Microsoft Purview Audit pour optimiser la gestion des journaux.
- Effectuer des audits pour évaluer la conformité et les mesures de sécurité.
- Analyser des modèles d'accès irréguliers à l'aide d'outils avancés dans Purview Audit (Premium) et PowerShell.
- Vérifier la conformité réglementaire par le biais de la gestion stratégique des données.

RECHERCHER DU CONTENU AVEC MICROSOFT PURVIEW EDISCOVERY

- Attribuer les rôles et autorisations pour accéder à Microsoft Purview eDiscovery
- Créer et gérer des cas utilisés pour exécuter des recherches eDiscovery
- Définir l'étendue de recherche et générer des requêtes à l'aide de conditions, de mots clés et d'invites générées par Copilot
- Exécuter des recherches et valider des résultats à l'aide de statistiques ou d'exemples aléatoires

Accessibilité

L'inclusion est sujet important pour OCTO Academy.
Nos référent·es sont à votre disposition pour faciliter l'adaptation de votre formation à vos besoins spécifiques.
Pour les contacter : academy.accessibilite@octo.com