Durée :	4 jours soit 28 heures	Référence :	SC-401T00

Public visé :

Profils et métiers visés :

- **Administrateur de la sécurité de l'information.** C'est le seul rôle nommé explicitement dans le descriptif.
- Administrateur Microsoft 365 ou administrateur systèmes chargé de l'environnement Microsoft 365.
- Ingénieur sécurité ou ingénieur conformité Microsoft 365.
- Analyste sécurité chargé de traiter les alertes DLP et les alertes de risque interne (déduit des modules 14 et 20).
- Consultant ou intégrateur Microsoft 365 spécialisé en sécurité et conformité (déduction).

Profils secondaires, par déduction : RSSI, DPO ou chargés de conformité qui ont un vrai bagage technique. Le contenu est clairement orienté vers la configuration et l'administration, il ne convient donc pas à des profils non techniques.

Niveau attendu : intermédiaire.

La formation ne part pas de zéro : elle suppose de savoir administrer Microsoft 365. Elle ne demande pas pour autant une expertise préalable de Microsoft Purview, puisque chaque grand domaine commence par un module de présentation.

Pré-requis :

Prérequis indispensables

- **Expérience pratique de l'administration de Microsoft 365** (centre d'administration, Exchange Online, SharePoint Online et OneDrive, Teams). La formation configure des éléments dans toutes ces charges de travail : règles de flux de messagerie, étiquettes de sites et de groupes, récupération de contenu, etc.
- **Connaissances de base de Microsoft Entra ID** (utilisateurs, groupes, rôles d'administration). Elles servent à publier les stratégies, définir les étendues adaptatives, configurer l'accès conditionnel avec Adaptive Protection et contrôler les applications d'IA enregistrées dans Entra.
- **Notions fondamentales de sécurité de l'information** (confidentialité, chiffrement, gestion des accès). Le module 1 présente les enjeux, mais pas ces bases.

Prérequis recommandés (non obligatoires)

- Connaître dans les grandes lignes les solutions de sécurité et de conformité Microsoft, au niveau « fondamentaux ». La référence SC-900 est ma suggestion : le document ne la cite pas.
- Avoir des notions d'administration de postes et de serveurs Windows, utiles pour intégrer les appareils à la DLP des points de terminaison et installer le scanneur.
- Avoir déjà utilisé Microsoft 365 Copilot, Microsoft Defender XDR ou Defender for Cloud Apps, ainsi que Power Platform, Power BI et Fabric.
- Savoir lire l'anglais technique, *si les supports ou les ateliers sont en anglais (le document ne le précise pas).*

Objectifs pédagogiques :

À l'issue de la formation, les participants seront en mesure de :

- **Expliquer** les enjeux de la protection des données sensibles (approche Zero Trust, menaces internes et externes, données traitées par l'IA) et le rôle de Microsoft Purview pour y répondre.
- **Classifier** des données avec des types d'informations sensibles intégrés et personnalisés (correspondance exacte des données, empreinte numérique de documents, dictionnaires de mots-clés) et avec des classifieurs entraînables, y compris personnalisés.
- **Analyser** la classification et l'étiquetage des données avec les rapports Information Protection, l'Explorateur de données, l'Explorateur de contenu et l'Explorateur d'activités.
- **Créer et publier** des étiquettes de confidentialité (chiffrement, étiquetage automatique), les **appliquer** dans les charges de travail Microsoft 365 et **déployer** le scanneur Information Protection pour les fichiers locaux.
- **Décrire** les mécanismes de chiffrement de Microsoft 365 (au repos, en transit, chiffrement de service, Customer Key), puis **configurer** Microsoft Purview Message Encryption et Advanced Message Encryption.
- **Planifier, créer et valider en mode simulation** des stratégies DLP pour Microsoft 365, les points de terminaison

(intégration des appareils, extension de navigateur, protection juste-à-temps), Defender for Cloud Apps et Power Platform.

- **Examiner et traiter** les alertes DLP dans Microsoft Purview et Microsoft Defender XDR, notamment avec l'assistance de Security Copilot.
- **Mettre en œuvre** la rétention (étiquettes, stratégies, application automatique, étendues adaptatives), **appliquer** l'ordre de priorité et **récupérer** du contenu dans Microsoft 365.
- **Configurer** Insider Risk Management et Adaptive Protection (niveaux de risque, couplage avec la DLP et l'accès conditionnel), puis **trier** les alertes de risque interne et **gérer** les cas associés.
- **Mener** des recherches avec Microsoft Purview Audit (Standard et Premium) et eDiscovery, et en **exporter** les résultats.
- **Identifier** les risques liés aux données de l'IA et **appliquer** les contrôles Microsoft Purview à Microsoft 365 Copilot, aux applications d'IA tierces et aux environnements de développement d'IA (Microsoft Foundry, applications enregistrées dans Microsoft Entra, agents Copilot Studio, Copilot in Fabric).

Compétences acquises à l'issue de la formation :

- Être capable de classifier les données sensibles de l'organisation avec les types d'informations sensibles (intégrés ou personnalisés, correspondance exacte des données, empreinte numérique de documents, dictionnaires de mots-clés) et les classifieurs entraînables, puis d'analyser les résultats avec les outils de Microsoft Purview (rapports, Explorateur de données, Explorateur de contenu, Explorateur d'activités).
- Être capable de créer, configurer et déployer des étiquettes de confidentialité et leurs stratégies (chiffrement, étiquetage automatique), puis de les appliquer aux contenus Microsoft 365 (applications Office, réunions, Teams, groupes Microsoft 365, sites SharePoint, Power BI) et aux fichiers locaux grâce au scanneur Microsoft Purview Information Protection.
- Être capable de protéger les e-mails avec Microsoft Purview Message Encryption (planification, configuration, personnalisation de l'identité visuelle, Advanced Message Encryption, modèles dans les règles de flux de messagerie), en s'appuyant sur une bonne compréhension des mécanismes de chiffrement de Microsoft 365.
- Être capable de concevoir, déployer et ajuster des stratégies de protection contre la perte de données (DLP) pour les charges de travail Microsoft 365, les points de terminaison, les fichiers locaux, Microsoft Defender for Cloud Apps et Power Platform, puis d'examiner les alertes DLP et d'y répondre.
- Être capable de mettre en œuvre la rétention et la récupération des contenus Microsoft 365 : étiquettes et stratégies de rétention, application automatique, étendues adaptatives, ordre de priorité, récupération de contenu.
- Être capable de mettre en œuvre Microsoft Purview Insider Risk Management (préparation, paramétrage, stratégies), d'examiner et trier les alertes de risque interne, de gérer les cas associés, et d'adapter les contrôles au niveau de risque avec Adaptive Protection.
- Être capable de mener des investigations avec Microsoft Purview Audit et eDiscovery : configurer l'audit et la rétention de ses données, rechercher et analyser les activités, créer, exécuter et exporter des recherches eDiscovery.
- Être capable de sécuriser les données utilisées et générées par l'IA (Microsoft 365 Copilot, applications d'IA d'entreprise ou utilisées dans un navigateur, applications et agents développés en interne) : évaluer les risques, notamment avec DSPM for AI, puis appliquer les contrôles Microsoft Purview adaptés (étiquettes, DLP, rétention, Communication Compliance, audit, eDiscovery).

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure. La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz. L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration. En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Note relative au programme : Les ateliers, démonstrations, travaux pratiques et scénarios présentés dans ce programme sont fournis à titre d'exemples illustratifs et ne sont pas exhaustifs. Afin de garantir une adéquation permanente avec les évolutions technologiques, le contenu pédagogique ainsi que les environnements de travaux pratiques (TP) sont susceptibles d'être adaptés, ajustés ou mis à jour au cours du temps.

Moyens et supports pédagogiques :

Cadre présentiel

Salles de formation équipées et accessibles aux personnes à mobilité réduite.

- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel

Session dispensée via notre solution iClassRoom s'appuyant sur Microsoft Teams.

- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Modalités d'évaluation et de suivi :

Avant

Afin de valider le choix d'un programme de formation, une évaluation des prérequis est réalisée à l'aide d'un questionnaire en ligne ou lors d'un échange avec le formateur(trice), qui valide la base de connaissances nécessaires.

Les stagiaires disposent également, depuis leur extranet, d'un **outil d'auto-positionnement** leur permettant d'évaluer leur niveau de maîtrise des compétences visées par la formation. Cette auto-évaluation est réalisée avant le démarrage de la formation à l'aide d'un curseur de positionnement allant du niveau le plus faible au niveau le plus élevé.

Pendant

Après chaque module théorique, un ou plusieurs ateliers pratiques permettent de valider progressivement l'acquisition des connaissances. Un quiz peut accompagner les ateliers pratiques afin de mesurer la compréhension des notions abordées.

Après

À l'issue de la formation, les stagiaires réalisent une nouvelle **auto-évaluation** sur les mêmes compétences que celles évaluées avant la formation. Cette comparaison permet de mesurer leur perception de la progression réalisée et de visualiser les compétences développées au cours de la formation.

Lorsque le programme de formation le prévoit, un examen de certification est organisé conformément aux modalités définies par l'éditeur ou le centre de certification (TOSA, Pearson VUE, ENI, PeopleCert…).

Le formateur réalise également une **évaluation individuelle des compétences** de chaque stagiaire sur l'ensemble des compétences visées par la formation. Pour chacune d'elles, il indique si la compétence est :

- Acquise ;
- En cours d'acquisition ;
- Non acquise.

Lorsque la compétence est évaluée comme **en cours d'acquisition** ou **non acquise**, le formateur formule des observations précisant les difficultés rencontrées ainsi que les actions ou recommandations permettant au stagiaire de poursuivre sa montée en compétences.

Enfin

Un questionnaire de satisfaction permet au participant d'évaluer la qualité de la prestation de formation.

Informations sur l'accessibilité :

Nos formations sont, dans la mesure du possible, conçues pour être accessibles à toutes et à tous. Afin de garantir les meilleures conditions d'accueil et d'apprentissage pour les personnes en situation de handicap, nous vous invitons à contacter notre référente handicap certifiée :
Céline SOLATGES – 05 61 34 39 80 – csolatges@iform.fr
Nous vous remercions de bien vouloir nous communiquer toute information utile à ce sujet en amont de la formation, afin de mettre en place les adaptations nécessaires et d'assurer un accompagnement optimal.

Pour en savoir plus sur les dispositifs d'accompagnement existants, vous pouvez consulter les sites suivants :

- AGEFIPH
- FIPHFP
- MDPH de votre département

Description / Contenu

La formation Administrateur de la sécurité de l'information vous permet d'acquérir les compétences nécessaires pour planifier et mettre en œuvre la sécurité des informations afin de protéger les données sensibles à l'aide de Microsoft Purview et des services associés. La formation couvre des sujets essentiels tels que la protection des informations, la prévention contre la perte de données (DLP), la rétention et la gestion des risques internes. Vous apprenez à protéger les données dans les environnements collaboratifs Microsoft 365 contre les menaces internes et externes. Vous apprenez également à gérer les alertes de sécurité et à répondre aux incidents en analysant les activités, en traitant les alertes DLP et en gérant les cas de risques internes. Vous apprenez également à protéger les données utilisées par les services d'IA au sein des environnements Microsoft et à mettre en œuvre des contrôles afin de sécuriser le contenu dans ces environnements.

Module 1 : Protéger les données sensibles dans un monde numérique

- Découvrez comment Microsoft Purview aide les organisations à classifier, protéger et surveiller les données sensibles dans les environnements cloud, les points de terminaison et les environnements d'IA. Ce module présente des stratégies permettant de sécuriser les données grâce à la classification, à l'étiquetage, au chiffrement et à la gestion proactive des risques.
- Le besoin croissant de protection des données
- Les défis liés à la gestion des données sensibles
- Protéger les données dans un environnement 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 à des fins de protection et de gouvernance

- Découvrir les informations disponibles pour mieux comprendre votre environnement de données et connaître vos données.
- Présentation de la classification des données
- Classifier les données à l'aide de types d'informations sensibles
- Classifier les données à l'aide de classifieurs entraînables
- Créer un classifieur entraînable personnalisé

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

- Découvrir comment Microsoft Purview aide les organisations à surveiller et analyser la classification et la protection des données. Ce module explique comment les équipes de sécurité peuvent suivre les tendances de classification, examiner les contenus étiquetés et évaluer l'efficacité des stratégies à l'aide des rapports Information Protection, de l'Explorateur de données, de l'Explorateur de contenu et de l'Explorateur d'activités.
- Examiner les informations sur la classification et la protection
- Analyser les données classifiées avec l'Explorateur de données et l'Explorateur de contenu
- Surveiller et examiner les actions effectuées sur les données étiquetées

Module 4 : Créer et gérer des types d'informations sensibles

- Apprendre à utiliser les types d'informations sensibles pour soutenir votre stratégie de protection des informations.
- Présentation des types d'informations sensibles
- Comparer les types d'informations sensibles intégrés et personnalisés
- Créer et gérer des types d'informations sensibles personnalisés
- Créer et gérer des types d'informations sensibles basés sur la correspondance exacte des données
- Mettre en œuvre l'empreinte numérique de documents
- Décrire les entités nommées

- Créer un dictionnaire de mots-clés

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

- Les étiquettes de confidentialité Microsoft Purview permettent de classifier et de protéger les données sensibles dans l'ensemble de votre organisation, notamment dans le cloud et sur les appareils. Ce module explique comment classifier et protéger les informations sensibles afin d'en garantir la sécurité et la conformité.
- Présentation des étiquettes de confidentialité
- Créer et configurer des étiquettes de confidentialité et des stratégies d'étiquettes
- Configurer le chiffrement avec des étiquettes de confidentialité
- Mettre en œuvre des stratégies d'étiquetage automatique
- Suivre et évaluer l'utilisation des étiquettes de confidentialité dans Microsoft Purview

Module 6 : Appliquer des étiquettes de confidentialité pour protéger les données

- Découvrir comment appliquer des étiquettes de confidentialité dans les différentes charges de travail Microsoft 365 afin de classifier et de protéger les données de l'entreprise, tout en favorisant la collaboration et la productivité.
- Principes fondamentaux de l'intégration des étiquettes de confidentialité dans Microsoft 365
- Gérer les étiquettes de confidentialité dans les applications Office
- Appliquer des étiquettes de confidentialité avec Microsoft 365 Copilot pour sécuriser la collaboration
- Protéger les réunions à l'aide d'étiquettes de confidentialité
- Appliquer des étiquettes de confidentialité à Microsoft Teams, aux groupes Microsoft 365 et aux sites SharePoint
- Appliquer des étiquettes de confidentialité dans Power BI

Module 7 : Classifier et protéger les données locales avec Microsoft Purview

- Protéger les fichiers locaux avec Microsoft Purview
- Préparer l'environnement pour le scanneur Microsoft Purview Information Protection
- Configurer et installer le scanneur Microsoft Purview Information Protection
- Exécuter et gérer le scanneur
- Appliquer les stratégies de protection contre la perte de données aux fichiers locaux

Module 8 : Comprendre le chiffrement dans Microsoft 365

- Comprendre comment les données Microsoft 365 sont chiffrées au repos
- Comprendre le chiffrement des services dans Microsoft Purview
- Explorer la gestion des clés client à l'aide de Customer Key
- Comprendre comment les données sont chiffrées en transit

Module 9 : Protéger les e-mails avec Microsoft Purview Message Encryption

- Comprendre le chiffrement des messages
- Planifier la mise en œuvre de Microsoft Purview Message Encryption
- Configurer Microsoft Purview Message Encryption
- Personnaliser l'identité visuelle des e-mails chiffrés avec Microsoft Purview
- Contrôler l'accès aux e-mails chiffrés avec Advanced Message Encryption
- Utiliser les modèles Microsoft Purview Message Encryption dans les règles de flux de messagerie

Module 10 : Comprendre et planifier la protection contre la perte de données

- Comprendre le rôle de la protection contre la perte de données (DLP)
- Comprendre comment la DLP applique la protection Planifier et concevoir des stratégies DLP
- Comprendre le déploiement de la DLP et le mode de simulation
- Évaluer les contrôles DLP avancés adaptés à votre environnement

Module 11 : Créer et gérer des stratégies de protection contre la perte de données

Comprendre l'articulation des différents choix d'une stratégie DLP
Choisir un modèle ou créer une stratégie personnalisée
Définir ce que la stratégie doit détecter
Adapter l'étendue de la stratégie au niveau de risque
Définir la réponse de la stratégie
Valider le comportement de la stratégie à l'aide du mode de simulation
Gérer les stratégies DLP

Ajuster dynamiquement l'application de la stratégie en fonction du risque
Procédure guidée : créer une stratégie DLP

Module 12 : Mettre en œuvre la protection contre la perte de données (DLP) des points de terminaison avec Microsoft Purview

- Comprendre la protection contre la perte de données des points de terminaison
- Comprendre le processus de mise en œuvre de la DLP des points de terminaison
- Intégrer les appareils à la DLP des points de terminaison
- Configurer les paramètres de la DLP des points de terminaison
- Créer et gérer des stratégies DLP des points de terminaison
- Déployer l'extension de navigateur Microsoft Purview
- Configurer la protection juste-à-temps (JIT)

Module 13 : Configurer des stratégies DLP pour Microsoft Defender for Cloud Apps et Power Platform

- Configurer des stratégies de protection contre la perte de données pour Power Platform
- Intégrer la protection contre la perte de données dans Microsoft Defender for Cloud Apps
- Configurer des stratégies dans Microsoft Defender for Cloud Apps

Module 14 : Examiner les alertes de protection contre la perte de données de Microsoft Purview et y répondre

- Comprendre les alertes de protection contre la perte de données (DLP)
- Comprendre le cycle de vie des alertes DLP
- Configurer les stratégies DLP pour générer des alertes
- Examiner les alertes DLP dans Microsoft Purview
- Examiner les alertes DLP dans Microsoft Defender XDR
- Examiner les alertes DLP avec Security Copilot et les agents IA
- Répondre aux alertes DLP
- Exercice - Examiner une alerte DLP et l'incident associé

Module 15 : Comprendre la rétention dans Microsoft Purview

- Présentation de la rétention et du cycle de vie des données
- Comprendre les étiquettes et les stratégies de rétention
- Déterminer quand appliquer la rétention

Module 16 : Mettre en œuvre et gérer la rétention et la récupération dans Microsoft 365

- Planifier la rétention et la suppression à l'aide d'étiquettes de rétention
- Créer et publier des étiquettes de rétention
- Créer et gérer l'application automatique des étiquettes de rétention
- Créer et configurer des étendues adaptatives
- Créer et configurer des stratégies de rétention
- Comprendre l'ordre de priorité des stratégies et des étiquettes dans Microsoft Purview
- Récupérer du contenu dans les différentes charges de travail Microsoft 365

Module 17 : Comprendre Microsoft Purview Insider Risk Management

- Comprendre ce qu'est un risque interne Présentation de Microsoft Purview Insider Risk Management
- Découvrir les fonctionnalités de Microsoft Purview Insider Risk Management
- Étude de cas : protéger les données sensibles avec Insider Risk Management

Module 18 : Préparer la mise en œuvre de Microsoft Purview Insider Risk Management

- Planifier la mise en œuvre d'Insider Risk Management
- Préparer votre organisation à l'utilisation d'Insider Risk Management
- Configurer les paramètres d'Insider Risk Management
- Intégrer Insider Risk Management aux sources de données et aux outils

Module 19 : Créer et gérer des stratégies Insider Risk Management

- Comprendre les modèles de stratégie Insider Risk Management
- Comparer les stratégies de risque interne rapides et personnalisées
- Créer une stratégie Insider Risk Management personnalisée

- Gérer les stratégies dans Insider Risk Management

Module 20 : Examiner les alertes de risque interne et les activités associées

- Comprendre les alertes de risque interne et les investigations
- Gérer le volume d'alertes dans Insider Risk Management
- Examiner et trier les alertes de risque interne dans Microsoft Purview
- Examiner les alertes de risque interne avec Security Copilot et les agents IA
- Analyser le contexte des alertes à l'aide de l'onglet Tous les facteurs de risque
- Examiner le détail des activités à l'aide de l'onglet Explorateur d'activités
- Analyser l'évolution des tendances à l'aide de l'onglet Activité de l'utilisateur
- Examiner les alertes de risque interne dans Microsoft Defender XDR
- Gérer les cas de risque interne et prendre les mesures appropriées
- Exercice - Examiner un vol potentiel de données à l'aide d'Insider Risk Management

Module 21 : Mettre en œuvre Adaptive Protection dans Microsoft Purview

- Comprendre Adaptive Protection et les niveaux de risque interne
- Évaluer et configurer les niveaux de risque interne
- Configurer Adaptive Protection
- Configurer Adaptive Protection avec la protection contre la perte de données
- Configurer Adaptive Protection avec l'accès conditionnel
- Évaluer Adaptive Protection avec Data Lifecycle Management

Module 22 : Mener des investigations avec Microsoft Purview Audit

- Comprendre le fonctionnement de Microsoft Purview Audit
- Configurer et gérer Microsoft Purview Audit
- Configurer la rétention des données d'audit avec Audit (Premium)
- Effectuer des recherches d'audit avec Audit (Standard)
- Examiner les activités avec Audit (Premium)
- Rechercher les activités de Copilot et des applications d'IA
- Analyser les résultats d'audit et générer des rapports

Module 23 : Rechercher du contenu avec Microsoft Purview eDiscovery

- Comprendre les fonctionnalités d'eDiscovery et de recherche de contenu
- Connaître les prérequis pour utiliser eDiscovery dans Microsoft Purview
- Créer une recherche eDiscovery
- Effectuer une recherche eDiscovery
- Exporter les résultats d'une recherche eDiscovery

Module 24 : Comprendre comment sécuriser les données liées à l'IA avec Microsoft Purview

- Comprendre les risques de sécurité liés aux données de l'IA
- Comprendre comment Microsoft Purview sécurise les données de l'IA
- Évaluer les risques de conformité liés à l'utilisation de l'IA
- Identifier les risques d'exposition des données liés à l'IA
- Comprendre comment Microsoft Purview contrôle l'accès aux données de l'IA
- Détecter les activités à risque liées à l'IA et y répondre
- Conserver et rechercher les invites et les réponses de Copilot

Module 25 : Sécuriser les interactions avec Microsoft 365 Copilot à l'aide de Microsoft Purview

- Comprendre comment Microsoft 365 Copilot fait évoluer les besoins en matière de protection des données
- Évaluer la conformité réglementaire de Copilot avec Compliance Manager
- Auditer les interactions avec Copilot à l'aide de Microsoft Purview
- Analyser les interactions avec Copilot à l'aide de Communication Compliance
- Classifier et protéger le contenu Copilot à l'aide d'étiquettes de confidentialité
- Appliquer des stratégies DLP à Microsoft 365 Copilot
- Appliquer des stratégies de rétention aux invites et aux réponses de Copilot
- Examiner et supprimer les activités Copilot à l'aide d'eDiscovery

Module 26 : Sécuriser les applications d'IA d'entreprise et celles utilisées dans un navigateur avec Microsoft Purview

- Comprendre les risques liés aux outils d'IA d'entreprise et non-Microsoft
- Évaluer l'utilisation de l'IA en matière de sécurité et de conformité
- Identifier les violations de stratégie avec Communication Compliance
- Détecter les utilisations à risque de l'IA avec Insider Risk Management
- Protéger les données sensibles dans les applications d'IA avec Microsoft Purview DLP
- Étude de cas : utiliser Adaptive Protection pour répondre aux risques liés à l'IA
- Appliquer des stratégies de rétention aux invites et aux réponses des applications d'IA

Module 27 : Sécuriser les environnements de développement d'IA avec Microsoft Purview

- Comprendre les risques et les responsabilités dans les environnements de développement d'IA
- Découvrir et évaluer les applications d'IA avec DSPM for AI
- Classifier, restreindre et conserver les données des invites d'IA
- Appliquer des mesures de protection dans Microsoft Foundry et Foundry Tools
- Appliquer des contrôles aux applications d'IA personnalisées enregistrées dans Microsoft Entra
- Sécuriser les agents IA créés dans Copilot Studio
- Gérer les risques liés aux données dans Copilot in Fabric
- Examiner les activités d'IA à risque et y répondre