Durée :	1 jour soit 7 heures	Référence :	SC-5009

Public visé :

Profils concernés

- Professionnels chargés de la sécurisation des environnements d'IA dans Azure.
- Responsables de la sécurité cloud.
- Équipes en charge de l'exploitation ou de l'administration des plateformes d'IA.
- Équipes techniques participant au déploiement de solutions utilisant Microsoft Foundry ou les services d'IA Azure.

Métiers visés

- Ingénieur sécurité cloud
- Administrateur Azure
- Ingénieur plateforme Cloud
- Architecte cloud
- Architecte sécurité
- Ingénieur DevSecOps
- Ingénieur IA / AI Platform Engineer
- Responsable sécurité des environnements Azure

Niveau attendu

- Intermédiaire.
- Participants disposant déjà de connaissances de base sur Azure, la sécurité cloud et les concepts d'identité et de gestion des accès.

Pré-requis :

Prérequis indispensables

- Avoir une connaissance générale de l'environnement Microsoft Azure et de son modèle de ressources.
- Comprendre les concepts fondamentaux de la sécurité cloud (contrôle d'accès, protection des ressources, gestion des risques).
- Posséder des connaissances de base sur les identités et les accès dans Microsoft Entra ID (anciennement Azure AD).
- Être familiarisé avec l'administration ou l'exploitation de ressources Azure.

Prérequis recommandés (non obligatoires mais constituant un plus)

- Connaissance générale des services d'IA proposés dans Azure.
- Expérience préalable de l'administration de Microsoft Defender for Cloud.
- Connaissance des principes RBAC, des identités managées et d'Azure Key Vault.

Objectifs pédagogiques :

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

- Identifier les risques de sécurité associés aux workloads d'IA déployés dans Azure et comprendre les mécanismes de gouvernance disponibles.
- Configurer Microsoft Defender for Cloud pour évaluer la posture de sécurité et surveiller les workloads d'IA.
- Déployer et administrer les garde-fous et contrôles de sécurité proposés par Microsoft Foundry.
- Sécuriser un environnement Microsoft Foundry à l'aide des mécanismes d'identité, de gestion des secrets, de segmentation réseau et de journalisation.
- Mettre en œuvre les contrôles d'identité et d'accès nécessaires à la protection des workloads d'IA avec Microsoft Entra et Azure RBAC.
- Configurer l'accès conditionnel et les mécanismes de protection des identités afin de renforcer la sécurité des utilisateurs et des charges de travail.

Compétences acquises à l'issue de la formation :

- Être en mesure d'évaluer les risques de sécurité propres aux workloads d'IA dans Azure et d'identifier les mécanismes de gouvernance, de protection et de surveillance adaptés.

- Savoir mettre en œuvre la protection des workloads d'IA avec Microsoft Defender for Cloud en exploitant les fonctionnalités de gestion de la posture de sécurité (CSPM), de protection des workloads (CWP) et d'analyse des alertes de sécurité.
- Être capable de configurer et d'administrer les garde-fous et contrôles de sécurité de Microsoft Foundry afin de sécuriser les interactions avec les modèles d'IA et de réduire les risques liés aux contenus et aux usages.
- Maîtriser la sécurisation d'un environnement Microsoft Foundry en appliquant des contrôles d'accès, des mécanismes de gestion des secrets, des protections réseau et des dispositifs de journalisation.
- Être capable de concevoir et appliquer une stratégie d'identité et de contrôle d'accès pour les workloads d'IA à l'aide de Microsoft Entra, du RBAC Azure, des identités managées et des mécanismes d'authentification.
- Savoir mettre en œuvre des contrôles de sécurité basés sur l'identité en utilisant l'accès conditionnel et Microsoft Entra ID Protection afin de renforcer la protection des utilisateurs, des identités de workload et des ressources d'IA.

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

Vue d'ensemble

Sécuriser les solutions d'IA dans le cloud en configurant les workloads d'IA, en appliquant des protections cloud natives et en renforçant la sécurité grâce à des contrôles d'identité. Découvrez comment les workloads d'IA s'authentifient, comment les limites de confiance sont établies et comment la gestion de la posture de sécurité et la protection des workloads permettent de réduire les risques avec Microsoft Defender for Cloud et Microsoft Foundry. Étendez ces protections en utilisant Microsoft Entra pour concevoir et appliquer des contrôles d'identité et d'accès qui permettent d'expliquer et de renforcer les décisions de sécurité prises précédemment.

Résultats de la formation :

- Mettre en œuvre la gestion de la posture de sécurité et la protection des workloads pour les services d'IA avec Microsoft Defender for Cloud
- Configurer et sécuriser les environnements Microsoft Foundry à l'aide de contrôles de sécurité cloud natifs
- Concevoir et appliquer des contrôles d'identité et d'accès pour les workloads d'IA avec Microsoft Entra

Cette formation s'adresse aux professionnels responsables de la sécurisation et de l'exploitation des workloads d'IA dans le cloud. Elle s'adresse notamment aux ingénieurs en sécurité cloud, aux ingénieurs plateforme et aux équipes applicatives travaillant avec des services d'IA, qui doivent comprendre comment la protection des workloads, la posture de sécurité et les contrôles d'identité s'appliquent aux environnements d'IA. Une connaissance d'Azure, des concepts de sécurité cloud native ainsi que des principes fondamentaux de l'identité et des accès est recommandée.

Module 1 : Comprendre comment Microsoft Defender for Cloud contribue à la sécurité et à la gouvernance de l'IA dans Azure

Microsoft Defender for Cloud joue un rôle central dans la sécurisation des workloads d'IA dans Azure. Découvrez

comment Microsoft Defender for Cloud contribue à la sécurité de l'IA dans Azure. Explorez les différentes couches d'un workload d'IA, les risques spécifiques introduits par les systèmes d'IA et les garde-fous qui protègent les entrées et les sorties des modèles. Découvrez comment Microsoft Purview, Microsoft Entra ID et Microsoft Foundry collaborent pour mettre en œuvre une stratégie unifiée de sécurité et de gouvernance.

- Comprendre les services d'IA dans Azure
- Comprendre les risques liés à la sécurité de l'IA dans Azure
- Garde-fous et protections de l'IA dans Azure
- Comprendre comment les outils de sécurité et de gouvernance Azure prennent en charge les workloads d'IA

Module 2 : Protéger les workloads d'IA avec Microsoft Defender for Cloud

Microsoft Defender for Cloud contribue à sécuriser les workloads d'IA en combinant la découverte, la gestion de la posture de sécurité et la protection en environnement d'exécution au sein d'une même plateforme. Découvrez comment activer le plan dédié aux workloads d'IA, consulter les informations du tableau de bord de sécurité des données et de l'IA, évaluer la posture de sécurité à l'aide de Cloud Security Posture Management (CSPM), détecter les menaces en environnement d'exécution avec Cloud Workload Protection (CWP) et examiner les incidents dans Microsoft Defender XDR. Ces fonctionnalités fonctionnent conjointement pour identifier les problèmes de configuration, détecter les comportements suspects et fournir une visibilité de bout en bout sur vos environnements d'IA.

- Activer le plan dédié aux workloads d'IA
- Consulter les informations du tableau de bord de sécurité des données et de l'IA
- Évaluer et améliorer la posture de sécurité de l'IA avec Cloud Security Posture Management (CSPM)
- Détecter les menaces liées à l'IA en environnement d'exécution avec Cloud Workload Protection (CWP)
- Examiner les alertes de sécurité liées à l'IA avec les éléments de preuve issus des prompts dans Microsoft Defender XDR

Module 3 : Configurer et gérer les garde-fous dans Microsoft Foundry

Les garde-fous de Microsoft Foundry contribuent à sécuriser les workloads d'IA en appliquant des contrôles de sécurité configurables qui évaluent à la fois les prompts et les réponses. Découvrez comment comprendre les modèles de sécurité intégrés, tester et affiner les garde-fous, créer des listes de blocage, configurer des filtres de contenu et vérifier que les protections fonctionnent comme prévu. Ces fonctionnalités permettent aux organisations de prévenir les interactions dangereuses ou non conformes aux politiques, de protéger les données sensibles et de maintenir la confiance dans les applications utilisant l'IA.

- Comprendre les garde-fous et Microsoft Content Safety
- Comprendre les contrôles de sécurité dans Microsoft Foundry
- Tester les garde-fous intégrés
- Créer et gérer des listes de blocage dans Microsoft Foundry
- Configurer et appliquer les garde-fous dans Microsoft Foundry
- Choisir et affiner les garde-fous adaptés à vos workloads d'IA

Module 4 : Sécuriser les environnements Microsoft Foundry

La sécurisation des environnements Microsoft Foundry nécessite des protections multicouches qui contrôlent les accès, sécurisent les identifiants, isolent les communications réseau et assurent une visibilité sur les ressources connectées. Cette approche consiste notamment à définir des limites d'accès avec Microsoft Entra ID et les rôles de projet, et à intégrer Key Vault pour la gestion des secrets. Elle s'appuie également sur les réseaux virtuels managés, Private Link et la journalisation des diagnostics afin de préserver la confidentialité, la visibilité et la conformité. Ces pratiques permettent de créer des environnements d'IA sécurisés et traçables, qui favorisent la collaboration sans compromettre la protection.

- Contrôler l'accès à Microsoft Foundry avec Microsoft Entra ID
- Gérer les accès au sein des projets Microsoft Foundry
- Sécuriser les secrets Microsoft Foundry avec Azure Key Vault (préversion)
- Isoler les réseaux avec un réseau virtuel managé et Private Link
- Activer la journalisation des diagnostics dans Microsoft Foundry

Module 5 : Comprendre l'architecture des identités pour les workloads d'IA

L'architecture des identités définit qui peut déployer, appeler et gérer les workloads d'IA dans Azure. Microsoft Entra ID régit les accès aux plans de gestion et de données, les flux d'authentification établissent les limites de confiance pour les endpoints d'IA, et les décisions relatives à l'étendue des rôles

déterminent le périmètre d'impact. Les types d'identités, les attributions de rôles et les limites d'étendue influencent les résultats en matière de sécurité de l'IA bien avant l'application des contrôles de sécurité.

- L'identité comme couche de contrôle pour les solutions d'IA
- Accès aux plans de gestion et de données dans les workloads d'IA
- Flux d'authentification pour les endpoints d'IA dans Microsoft Foundry
- Identités humaines et identités de workload dans les workloads d'IA
- Attributions de rôles et étendue dans les environnements d'IA
- Erreurs courantes de configuration des identités dans les déploiements d'IA

Module 6 : Mettre en œuvre la gestion des accès aux ressources Azure

Découvrez comment utiliser les rôles Azure intégrés, les identités managées et le RBAC basé sur des stratégies pour contrôler l'accès aux ressources Azure. L'identité est la clé de la sécurisation des solutions.

- Attribuer des rôles Azure
- Configurer des rôles Azure personnalisés
- Créer et configurer des identités managées
- Accéder aux ressources Azure avec des identités managées
- Analyser les autorisations des rôles Azure
- Configurer les stratégies RBAC d'Azure Key Vault
- Récupérer des objets depuis Azure Key Vault

Module 7 : Planifier, mettre en œuvre et administrer l'accès conditionnel

L'accès conditionnel permet de contrôler avec précision quels utilisateurs et quelles identités peuvent effectuer certaines activités, accéder à quelles ressources et selon quelles modalités afin de garantir la sécurité des données et des systèmes, notamment pour les identités des agents d'IA gérées via Microsoft Entra Agent ID.

- Planifier les paramètres de sécurité par défaut
- Exercice – Utiliser les paramètres de sécurité par défaut
- Planifier les stratégies d'accès conditionnel
- Mettre en œuvre les contrôles et les attributions des stratégies d'accès conditionnel
- Exercice – Mettre en œuvre les rôles et les attributions des stratégies d'accès conditionnel
- Tester et résoudre les problèmes liés aux stratégies d'accès conditionnel
- Mettre en œuvre les contrôles des applications
- Mettre en œuvre la gestion des sessions et l'évaluation continue de l'accès
- Exercice – Configurer les contrôles des sessions d'authentification
- Agent d'optimisation de l'accès conditionnel Microsoft Entra

Module 8 : Gérer Microsoft Entra ID Protection

La protection de l'identité d'un utilisateur par la surveillance de son utilisation et de ses habitudes de connexion contribue à garantir la sécurité d'une solution cloud. Découvrez comment concevoir et mettre en œuvre Microsoft Entra ID Protection.

- Revoir les principes fondamentaux d'Identity Protection
- Mettre en œuvre et gérer une stratégie de risque utilisateur
- Exercice – Activer une stratégie de risque lié aux connexions
- Exercice – Configurer une stratégie d'inscription à l'authentification multifacteur Microsoft Entra
- Surveiller, examiner et corriger les situations impliquant des utilisateurs présentant un niveau de risque élevé
- Mettre en œuvre la sécurité des identités de workload
- Découvrir Microsoft Defender for Identity
- Découvrir l'agent de gestion des risques liés aux identités