Programme de cours
Mettre en œuvre des contrôles de sécurité de bout en bout pour les charges de travail Cloud et d'IA

Durée :	4 jours soit 28 heures	Référence :	SC-500T00

Public visé :

Ce cours s'adresse aux ingénieurs en sécurité chargés de planifier, d'implémenter et de gérer des contrôles de sécurité dans des environnements cloud, hybrides et multicloud, en s'appuyant sur les technologies de sécurité Microsoft.
Vous êtes un ingénieur en sécurité chargé de protéger les systèmes et les données de votre organisation dans des environnements cloud et hybrides, en mettant en œuvre des contrôles de sécurité complets permettant de prévenir les accès non autorisés et d'atténuer les risques de manière proactive.
Ce rôle couvre plusieurs domaines de la sécurité, notamment la gestion des identités, la sécurité des réseaux, des applications, des données et des infrastructures de calcul. Il consiste également à garantir que les plateformes, les données, les identités et les infrastructures utilisées par les charges de travail basées sur l'IA sont déployées et supervisées de manière sécurisée.
Vous travaillez en étroite collaboration avec les architectes, administrateurs, ingénieurs, analystes et développeurs en charge d'Azure, de Microsoft 365, de la gestion des identités et des accès, de la protection des informations, des opérations de sécurité, du DevOps, du développement d'applications, des plateformes de bases de données et des infrastructures réseau.
Vous devez disposer d'une expérience pratique de l'administration de Microsoft Azure et des environnements hybrides, notamment dans les domaines du calcul, du réseau et du stockage. Une solide maîtrise de Microsoft Entra ID ainsi qu'une bonne connaissance de l'administration de Microsoft 365 sont également requises.

Vos principales responsabilités sont les suivantes :

- Sécuriser l'accès aux ressources à l'aide de Microsoft Entra ID et d'Azure Key Vault ;
- Mettre en œuvre les exigences de sécurité et de conformité réglementaire ;
- Sécuriser les services de stockage, les bases de données et les infrastructures réseau ;
- Sécuriser les ressources de calcul ;
- Sécuriser les solutions intégrant l'intelligence artificielle ;
- Gérer et superviser la posture de sécurité de l'organisation.

Pré-requis :

Objectifs pédagogiques :

- **Sécuriser** l'accès aux ressources à l'aide de Microsoft Entra ID et d'Azure Key Vault
- **Appliquer** la gouvernance de sécurité et la conformité réglementaire
- **Sécuriser** le stockage Azure, les bases de données Azure SQL et la mise en réseau Azure
- **Sécuriser** le calcul (serveurs, machines virtuelles et services de plateforme d'applications)
- **Sécuriser** les solutions et charges de travail IA, y compris les agents autonomes
- **Gérer** et **surveiller** la posture de sécurité à l'aide de Microsoft Defender for Cloud
- **Implémenter** la collecte d'événements et l'activité dans Microsoft Sentinel
- **Déployer** et **exploiter** Microsoft Security Copilot

Compétences acquises à l'issue de la formation :

- Sécuriser l'accès aux ressources avec Microsoft Entra ID (authentification, PIM, accès API des agents)
- Sécuriser les secrets et certificats avec Azure Key Vault
- Appliquer la gouvernance de sécurité, la conformité réglementaire et le moindre privilège (RBAC, Defender for Cloud, sauvegarde, IaC)
- Sécuriser le stockage Azure (accès, réseau, Defender for Storage)
- Sécuriser les bases de données Azure SQL (plateforme, audit, Defender)
- Implémenter des contrôles de sécurité réseau dans Azure (segmentation, pare-feu, VPN, exposition publique)
- Sécuriser les solutions et agents IA (Entra Agent ID, Defender XDR, Copilot Studio, Microsoft Foundry, Agent 365, Purview)
- Sécuriser les serveurs et machines virtuelles (chiffrement, Bastion, Arc, Defender, accès JIT)
- Sécuriser la plateforme d'applications (conteneurs, AKS, App Services, API Management)
- Gérer la posture de sécurité globale avec Microsoft Defender for Cloud (CSPM, surface d'attaque, vulnérabilités)
- Implémenter la collecte de données et l'automatisation dans Microsoft Sentinel
- Déployer et exploiter Microsoft Security Copilot

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.

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 sur tableau blanc

- 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

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

Programme de cours
Mettre en œuvre des contrôles de sécurité de bout en bout pour les charges de travail Cloud et d'IA

Description / Contenu

Ce cours vous prépare à concevoir, implémenter et gérer des contrôles de sécurité de bout en bout dans les environnements Microsoft Azure et Microsoft 365, y compris dans le contexte émergent des charges de travail basées sur l'IA et des agents autonomes.
Grâce à une combinaison de sessions animées par un formateur et de travaux pratiques, vous développerez des compétences concrètes en matière de sécurité des identités, de protection des infrastructures cloud, de détection des menaces et de gestion de la posture de sécurité.

Module 1 : Sécuriser l'accès aux ressources à l'aide de Microsoft Entra

- Gérer et implémenter des méthodes d'authentification dans Microsoft Entra ID
- Implémenter et configurer Privileged Identity Management (PIM)
- Authentifier votre plug-in d'API pour les agents déclaratifs avec des API sécurisées

Module 2 : Sécuriser Azure Key Vault avec la défense en profondeur pour les charges de travail cloud et IA

- Configurer et sécuriser les Azure Key Vault
- Gérer les clés et les secrets dans Azure Key Vault
- Gérer les certificats et surveiller les Azure Key Vault
- Protéger Azure Key Vault avec Microsoft Defender for Cloud

Module 3 : Appliquer la gouvernance de la sécurité et la conformité réglementaire

- Appliquer la gouvernance de la sécurité et la conformité réglementaire
- Configurer les contrôles de sécurité et corriger les recommandations dans Defender for Cloud
- Évaluer la conformité réglementaire dans Defender for Cloud
- Gérer et dimensionner correctement les attributions de rôles RBAC selon le principe du moindre privilège
- Protéger les données de sauvegarde avec des fonctionnalités de sécurité Sauvegarde Azure
- Implémenter des contrôles de sécurité dans l'infrastructure en tant que code

Module 4 : Implémenter la sécurité pour stockage Azure pour l'ingénieur de sécurité cloud et IA

- Décrire les services de stockage Azure
- Implémenter la sécurité et gérer l'accès pour stockage Azure
- Configurer la sécurité réseau pour stockage Azure
- Implémenter Microsoft Defender pour le stockage

Module 5 : Implémenter la sécurité pour les bases de données Azure SQL

- Configurer la sécurité au niveau de la plateforme pour Azure SQL
- Configurer l'audit pour Azure SQL Database et SQL Managed Instance
- Implémenter Microsoft Defender pour les bases de données

Module 6 : Implémenter des contrôles de sécurité réseau dans Azure

- Segmenter et isoler les charges de travail Azure à l'aide de contrôles de sécurité réseau
- Centraliser et appliquer l'inspection du trafic à l'aide de Pare-feu Azure
- Sécuriser la connectivité distante et hybride à l'aide de passerelles VPN et de Accès privé Microsoft Entra
- Éliminer l'exposition du réseau public aux services PaaS Azure

Module 7 : Implémenter la sécurité pour l'IA

- Accès sécurisé pour l'Identité de l'agent Microsoft Entra
- Analyser les risques liés aux identités IA à l'aide de Microsoft Defender XDR
- Activer la protection en temps réel pour les agents Copilot Studio
- Configurer la sécurité de la passerelle AI dans Microsoft Foundry
- Configurer et gérer des garde-fous dans Microsoft Foundry
- Protéger les charges de travail IA avec Microsoft Defender pour cloud
- Activer Defender pour les services d'IA protection des charges de travail dans Microsoft Defender for Cloud
- Gérer les agents à l'aide de Microsoft Agent 365
- Identifier les risques liés aux données IA à l'aide de Gestion de la posture de sécurité des données Microsoft Purview

Module 8 : Implémenter la sécurité pour les serveurs et les machines virtuelles

- Implémenter le chiffrement de disque pour les machines virtuelles Azure
- Configurer les fonctionnalités de sécurité de lancement approuvées pour les machines virtuelles Azure
- Planifier et implémenter Azure Bastion
- Gérer la sécurité des serveurs hybrides avec Arc
- Implémenter Microsoft Defender pour les serveurs

- Activer et appliquer l'accès juste-à-temps aux machines virtuelles
- Appliquer la configuration de sécurité des machines virtuelles avec Azure Machine Configuration

Module 9 : Sécurisation des services de plateforme d'applications Azure pour l'ingénieur sécurité du cloud et de l'IA

- Détecter les risques liés aux conteneurs à l'aide de Microsoft Defender pour les conteneurs
- Implémenter des contrôles de sécurité pour Azure Kubernetes Service
- Implémenter des contrôles de sécurité pour Azure Container Registry, Container Instances et Container Apps
- Implémenter des contrôles de sécurité pour les applications de fonction Azure et les applications logiques
- Implémenter des contrôles de sécurité pour Azure App Services et Web Application Firewall
- Implémenter la sécurité du back-end d'API à l'aide de Gestion des API Azure

Module 10 : Gérer la posture de sécurité en utilisant Microsoft Defender pour le cloud

- Connecter des environnements hybrides et multiclouds à Microsoft Defender for Cloud
- Identifier les risques de sécurité à l'aide de la gestion de la posture de sécurité cloud
- Découvrir des ressources et des vulnérabilités non protégées à l'aide de Microsoft Defender External Attack Surface Management
- Évaluer la conformité réglementaire dans Defender for Cloud
- Activer et configurer des plans de protection des charges de travail dans Microsoft Defender for Cloud
- Configurer les paramètres de Microsoft Defender Vulnerability Management pour les machines virtuelles Azure

Module 11 : Implémenter l'activité et la collecte d'événements dans Microsoft Sentinel

- Créer et gérer des espaces de travail Microsoft Sentinel
- Gérer le contenu dans Microsoft Sentinel
- Connecter services Microsoft à Microsoft Sentinel
- Connecter des sources de données Syslog à Microsoft Sentinel
- Connecter des journaux Common Event Format à Microsoft Sentinel
- Connecter des hôtes Windows à Microsoft Sentinel
- Implémenter des règles d'automatisation et des playbooks dans Microsoft Sentinel
- Gérer le stockage des données et interroger les journaux d'audit dans Microsoft Sentinel

Module 12 : Déployer et exploiter Microsoft Security Copilot

- Décrire le Microsoft Security Copilot
- Configurer des espaces de travail pour Microsoft Security Copilot
- Gérer les plug-ins et les agents dans Microsoft Security Copilot