Formation Implémenter des contrôles de sécurité pour les charges de travail cloud et IA

Durée :	4.0 jour(s)
Objectifs :	Dans cette formation, vous développerez les compétences nécessaires pour : • Concevoir, mettre en œuvre et gérer des contrôles de sécurité dans des environnements Microsoft Azure et Microsoft 365 (incluant les charges de travail IA et les agents autonomes). • Sécuriser l'identité et l'accès • Protéger l'infrastructure cloud • Renforcer la posture de sécurité et détecter les menaces • Appliquer une gouvernance conforme, avec une approche orientée scénarios et laboratoires
Public :	Ce cours est destiné aux ingénieurs de sécurité, chargés de la planification et de l'implémentation de contrôles de sécurité dans les environnements cloud, hybrides et multiclouds à l'aide de technologies de sécurité Microsoft.
Prérequis :	Bonnes connaissances de Microsoft Azure, Microsoft Entra ID, Microsoft Copilot, Microsoft Purview, Microsoft Defender, Microsoft Foundry
Modalités et moyens pédagogiques	• **Modalités et délais d'accès** : L'inscription comprend : demande d'inscription, étude du dossier et positionnement, validation et contractualisation. L'accès à la formation est effectif après validation administrative et pédagogique. Un délai de rétractation de 14 jours s'applique pour les formations financées à titre individuel. Les délais d'accès peuvent varier selon les modalités et les financements. • **Accessibilité handicap :** La formation est accessible aux personnes en situation de handicap. Des adaptations peuvent être proposées après étude des besoins. Merci de signaler toute situation dès l'inscription. • **Sanction de la formation :** Attestation de fin de formation remise au participant/ Evaluation de la satisfaction réalisée en fin de parcours. • **Moyens pédagogiques :** Démonstrations visuelles et pratiques à travers des exercices d'application et/ou

	des cas concrets des stagiaires. Salle de formation équipée d'un poste PC par personne et de dispositif vidéo Grand Ecran. Portail web : maformation.vaelia.fr
Modalités d'évaluation	Auto évaluation des acquis, exercices pratiques et/ou échanges avec le formateur.
Moyens d'encadrement	Un formateur expert dont les compétences ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou Vaelia.
Satisfaction globale :	/5 *Calculée à partir des évaluations stagiaires sur les 12 derniers mois.*

Jour 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

Sécuriser Azure Key Vault avec les 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

Appliquer la gouvernance de la sécurité et la conformité réglementaire

- Appliquer la gouvernance avec des Azure Policy et des verrous de ressources
- 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

Jour 2

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

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

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

Jour 3

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

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

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

Jour 4

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

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

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