skillsoft global knowledge

Microsoft Partner
Gold Learning

Mettre en place des contrôles de sécurité Microsoft complets pour les charges de travail dans le cloud et liées à l'IA

Durée: 4 Jours **Réf de cours: M-SC500** **Méthodes d'apprentissage: Classe à distance**

Résumé:

Concevoir, mettre en œuvre et gérer des contrôles de sécurité de bout en bout dans les environnements Microsoft Azure et Microsoft 365.

Cette formation vous prépare à la conception, à la mise en œuvre et à la gestion de 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 d'IA et des agents autonomes.

Grâce à une succession de modules animés par un formateur et de travaux pratiques, les participants acquièrent 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.

Mis à jour 4/8/2026

Classe à Distance - site Client

Cette formation peut être suivie à distance en synchrone depuis n'importe quel site pourvu d'une connexion internet (2 Mb/s en symétrique recommandés). Le programme (théorie et pratique) suit le même déroulé pédagogique qu'en présentiel. La solution technologique adoptée permet aux apprenants à distance de suivre les présentations faites au tableau, de voir et d'entendre l'instructeur et les participants en temps réel, mais également d'échanger avec eux.

Public visé:

Les participants sont généralement des ingénieurs en sécurité chargés de protéger les systèmes et les données de l'organisation dans des environnements cloud et hybrides, en mettant en œuvre des contrôles de sécurité complets qui empêchent tout accès non autorisé et atténuent les risques de manière proactive.
Ce poste couvre plusieurs domaines de sécurité, notamment l'identité, le réseau, les applications, les données et les ressources de calcul. Il consiste également à s'assurer que les plateformes, les données, les identités et l'infrastructure utilisées par les charges de travail d'IA sont mises en œuvre et surveillées 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 réseaux.

Vos responsabilités dans le cadre de ce poste comprennent : Sécuriser l'accès aux ressources à l'aide de Microsoft Entra ID et d'Azure Key VaultVeiller au respect des règles de sécurité et de la conformité réglementaire Sécuriser le stockage, les bases de données et les réseauxSécuriser les ressources de calcul Sécuriser les solutions d'IA Gérer et surveiller la posture de sécurité

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Sécuriser l'accès aux ressources à l'aide de Microsoft Entra
- Sécuriser Azure Key Vault grâce à une défense en profondeur pour le cloud et les charges de travail d'IA
- Appliquer la gouvernance de sécurité et la conformité réglementaire
- Mettre en œuvre la sécurité d'Azure Storage pour les ingénieurs en sécurité du cloud et de l'IA
- Mettre en œuvre la sécurité des bases de données Azure SQL
- Mettre en œuvre des contrôles de sécurité réseau dans Azure
- Mettre en œuvre la sécurité de l'IA
- Mettre en œuvre la sécurité des serveurs et des machines virtuelles
- Sécuriser les services de la plateforme d'applications Azure pour les ingénieurs en sécurité du cloud et de l'IA
- Gérer la posture de sécurité à l'aide de Microsoft Defender for Cloud
- Mettre en œuvre la collecte d'activités et d'événements dans Microsoft Sentinel
- Déployer et exploiter Microsoft Security Copilot

Pré-requis:

Il est recommandé aux participants d'avoir des connaissances de base sur les concepts de sécurité dans le cloud, la gestion des identités et des accès, les réseaux et l'administration de Microsoft Azure.

Ils doivent disposer d'une expérience pratique dans l'administration de Microsoft Azure et d'environnements hybrides, notamment en matière de ressources de calcul, de réseau et de stockage. Ils doivent également bien maîtriser Microsoft Entra ID et avoir une bonne connaissance de l'administration de Microsoft 365 et des technologies de sécurité Microsoft.

Test et certification

Ce cours prépare à la certification Microsoft SC500 qui correspond au titre d'ingénieur en sécurité cloud et IA associé (Cloud and AI Security Engineer Associate), qui permet de concevoir, implémenter et gérer des contrôles de sécurité pour les environnements Microsoft Azure, Microsoft 365 et les charges de travail d'intelligence artificielle.

Cet examen est le successeur de l'examen AZ-500 (expirationt le 31 août 2026).

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

- SC-100: Microsoft Cybersecurity Architect

Contenu:

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

- Gérer et mettre en œuvre des méthodes d'authentification dans Microsoft Entra ID
- Mettre en œuvre et configurer la gestion des identités privilégiées (PIM)
- Authentifier votre plugin API pour les agents déclaratifs à l'aide d'API sécurisées

Module 2 : Sécuriser Azure Key Vault grâce à une protection renforcée pour le cloud et les workloads IA

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

Module 3 : Assurer la gouvernance en matière de sécurité et la conformité réglementaire

- Appliquer la gouvernance à l'aide d'Azure Policy et des restrictions de ressources
- Configurer des contrôles de sécurité et mettre en œuvre les recommandations dans Defender for Cloud
- Évaluer la conformité réglementaire dans Defender for Cloud
- Gérer et adapter les attributions de rôles RBAC selon le principe du privilège minimal
- Protéger les données de sauvegarde grâce aux fonctionnalités de sécurité d'Azure Backup
- Mettre en œuvre des contrôles de sécurité dans l'infrastructure en tant que code

Module 4 : Mettre en œuvre la sécurité d'Azure Storage pour les ingénieurs spécialisés dans la sécurité du cloud et de l'IA

- Décrire les services de stockage Azure
- Mettre en œuvre la sécurité et gérer les accès pour Azure Storage
- Configurer la sécurité réseau pour Azure Storage
- Mettre en œuvre Microsoft Defender for Storage

Module 5 : Mettre en place la sécurisation des bases de données SQL Azure

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

Module 6 : Appliquer des mesures de sécurité réseau dans Azure

- Segmenter et isoler les Workloads Azure à l'aide de contrôles de sécurité réseau
- Centraliser et appliquer l'inspection du trafic à l'aide d'Azure Firewall
- Sécuriser la connectivité à distance et hybride à l'aide de passerelles VPN et de Microsoft Entra Private Access
- Éliminer l'exposition des services PaaS Azure dans les réseaux publics

Module 7 : Mettre en place des mesures de sécurité pour l'IA

- Sécuriser l'accès pour Microsoft Entra Agent Identity
- Analyser les risques liés à l'identité dans le domaine de l'IA à l'aide de Microsoft Defender XDR
- Activer la protection en temps réel pour les agents Copilot Studio
- Configurer la sécurité d'AI Gateway dans Microsoft Foundry
- Configurer et gérer les garde-fous dans Microsoft Foundry
- Protéger les charges de travail d'IA avec Microsoft Defender for Cloud
- Activer la protection des charges de travail Defender for AI Services dans Microsoft Defender for Cloud
- Gérer les agents à l'aide de Microsoft Agent 365
- Identifier les risques liés aux données d'IA à l'aide de Microsoft Purview Data Security Posture Management

Module 8

: Mettre en place des mesures de sécurité pour les serveurs et les machines virtuelles

- Mettre en œuvre le chiffrement des disques pour les machines virtuelles Azure
- Configurer les fonctionnalités de sécurité « Trusted Launch » pour les machines virtuelles Azure
- Planifier et mettre en œuvre Azure Bastion
- Gérer la sécurité des serveurs hybrides prenant en charge Arc
- Mettre en œuvre Microsoft Defender pour les serveurs
- Activer et appliquer l'accès « juste à temps » aux machines virtuelles
- Appliquer la configuration de sécurité des machines virtuelles à l'aide d'Azure Machine Configuration

Module 9 : Sécuriser les services de la

Module 10 : Gérer la stratégie de sécurité à l'aide de Microsoft Defender for Cloud

- Connecter des environnements hybrides et multicloud à Microsoft Defender for Cloud
- Identifier les risques de sécurité à l'aide de la gestion de la stratégie de sécurité dans le cloud (Cloud Security Posture Management)
- Détecter les ressources non protégées et les vulnérabilités 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 workloads dans Microsoft Defender for Cloud
- Configurer les paramètres de gestion des vulnérabilités de Microsoft Defender pour les machines virtuelles Azure

Module 11 : Mettre en place la collecte des activités et des incidents dans Microsoft Sentinel

- Créer et gérer des espaces de travail Microsoft Sentinel
- Gérer le contenu dans Microsoft Sentinel
- Connecter à Microsoft Sentinel :
- des services Microsoft
- des sources de données syslog
- des journaux au format CEF (Common Event Format)
- des hôtes Windows
- Mettre en œuvre 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 utiliser Microsoft Security Copilot

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

plateforme d'applications Azure pour les ingénieurs sécurité cloud et IA

- Détecter les risques liés aux conteneurs à l'aide de Microsoft Defender for Containers
- Mettre en œuvre des contrôles de sécurité pour
- Azure Kubernetes Service
- Azure Container Registry, Container Instances et Container Apps
- les applications Azure Functions et les applications Logic
- Azure App Services et le pare-feu d'applications Web
- Mettre en œuvre la sécurité du backend des API à l'aide d'Azure API Management

Méthodes pédagogiques :

Un support de cours officiel sera fourni aux participants.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form"""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement