

Certifiante

Formation Implémenter des contrôles de sécurité de bout en bout pour les charges de travail cloud et IA (SC-500)

Réf. SF34760

Préparez la certification Microsoft Certified: Cloud and AI Security Engineer Associate en apprenant à sécuriser identités, données, réseaux, calcul et charges de travail IA dans Azure, puis à en surveiller la posture avec Defender for Cloud, Microsoft Sentinel et Security Copilot.

4 j
Durée

2 800 € HT
Inter / participant

0
Sessions à venir

Objectifs pédagogiques

- ✓ Sécuriser l'accès aux ressources avec Microsoft Entra ID (méthodes d'authentification, accès conditionnel, Privileged Identity Management) et protéger clés, secrets et certificats avec Azure Key Vault
- ✓ Appliquer la gouvernance de la sécurité et la conformité réglementaire avec Azure Policy, le RBAC en moindre privilège, Defender for Cloud, Azure Backup et l'infrastructure as code
- ✓ Implémenter la sécurité des comptes de stockage, des bases Azure SQL et du réseau : segmentation, Azure Firewall, connectivité hybride et points de terminaison privés
- ✓ Sécuriser les charges de travail IA et les agents avec Microsoft Entra Agent ID, Microsoft Foundry, Defender for AI Services et la gestion de la posture de sécurité des données pour l'IA
- ✓ Configurer la sécurité du calcul : machines virtuelles, serveurs hybrides Azure Arc, conteneurs, AKS et services de plateforme applicative (Functions, Logic Apps, App Service, WAF, API Management)
- ✓ Gérer la posture de sécurité d'environnements hybrides et multiclouds avec Microsoft Defender for Cloud (CSPM, plans de protection des charges de travail, EASM, gestion des vulnérabilités)
- ✓ Déployer la collecte d'événements et l'automatisation de la réponse dans Microsoft Sentinel, et exploiter Microsoft Security Copilot
- ✓ Réussir l'examen de certification Microsoft Certified: Cloud and AI Security Engineer Associate (SC-500)

Public visé & prérequis

Public visé Ingénieurs DevOps

Prérequis- Expérience pratique de l'administration de Microsoft Azure et d'environnements hybrides, notamment le calcul, le réseau et le stockage - Bonne connaissance de Microsoft Entra ID et de la gestion des identités et des accès - Connaissance de l'administration Microsoft 365 - Aucune certification préalable n'est exigée pour passer l'examen SC-500 - Recommandé : niveau Administrateur Azure (AZ-104) ou équivalent - Recommandé : bases du langage KQL (requêtes dans Microsoft Sentinel et Microsoft Defender) - Recommandé : fondamentaux réseau (adressage IP, routage, DNS, VPN) - Recommandé : notions de conteneurs et de Kubernetes - Recommandé : notions d'infrastructure as code (Bicep ou modèles ARM) et de pipelines CI/CD - Recommandé : repères sur l'IA générative et les agents (Microsoft Foundry, Copilot Studio, Microsoft 365 Copilot)

Programme détaillé

Sécuriser l'accès aux ressources avec Microsoft Entra

- Gérer et implémenter des méthodes d'authentification dans Microsoft Entra ID : force d'authentification, authentification multifacteur par stratégies d'accès conditionnel et emplacements nommés, authentification sans mot de passe (Windows Hello Entreprise, clés d'accès, clés FIDO2), réinitialisation de mot de passe en libre-service
- Implémenter et configurer Privileged Identity Management (PIM) : accès juste-à-temps aux rôles Microsoft Entra, aux rôles de ressources Azure et aux groupes, application aux charges de travail, agents et applications IA
- Identité des applications : applications d'entreprise, inscriptions d'applications, autorisations OAuth et paramètres de consentement,

identités managées pour les ressources Azure

– Authentifier un plug-in d'API pour les agents déclaratifs avec des API sécurisées : intégration par clé d'API et par OAuth

Activités pratiques :

- Configuration des méthodes d'authentification et d'une stratégie d'accès conditionnel exigeant la MFA
- Activation juste-à-temps d'un rôle privilégié avec PIM

Sécuriser Azure Key Vault avec une stratégie de défense en profondeur

- Configurer et sécuriser Azure Key Vault : déploiement avec suppression réversible et protection contre le vidage, accès RBAC et privilèges juste-à-temps, pare-feu, points de terminaison de service et points de terminaison privés
- Gérer les clés et les secrets dans Azure Key Vault : clés protégées par HSM, BYOK, rotation automatique des clés et des secrets
- Gérer les certificats et surveiller Azure Key Vault : émission et renouvellement via des autorités de certification intégrées, journalisation d'audit
- Protéger Azure Key Vault avec Microsoft Defender for Cloud : recherche de secrets exposés avec Defender CSPM, Microsoft Defender pour Key Vault, traitement des alertes

Activités pratiques :

- Déploiement d'un coffre durci (RBAC, réseau privé) et configuration de la rotation automatique d'une clé
- Investigation d'une alerte Defender pour Key Vault

Appliquer la gouvernance de la sécurité et la conformité réglementaire

- Appliquer la gouvernance avec Azure Policy et des verrous de ressources : définitions et initiatives intégrées, définitions personnalisées avec tâches de correction, verrous de ressources
- Configurer les contrôles de sécurité et corriger les recommandations dans Defender for Cloud : normes de sécurité au niveau du groupe d'administration, correction à grande échelle, règles de gouvernance et exemptions
- Évaluer la conformité réglementaire dans Defender for Cloud : Microsoft Cloud Security Benchmark, tableau de bord de conformité réglementaire, affectation de normes, rapports et Microsoft Purview Compliance Manager
- Gérer et ajuster les attributions de rôles RBAC pour le moindre privilège : rôles intégrés Azure, rôles personnalisés Azure et Microsoft Entra, correction des accès surpriviliés (CSPM, CIEM, révisions d'accès)
- Protéger les données de sauvegarde avec les fonctionnalités de sécurité de Sauvegarde Azure : suppression réversible, coffres immuables, autorisation multi-utilisateur avec Resource Guard
- Implémenter des contrôles de sécurité dans l'infrastructure en tant que code : analyse des modèles Bicep et ARM avec Microsoft Defender pour DevOps, stratégie en tant que code

Activités pratiques :

- Affectation d'une initiative Azure Policy et création d'une définition personnalisée avec tâche de correction
- Analyse d'un tableau de bord de conformité réglementaire et correction d'un contrôle en échec
- Identification et correction d'une attribution de rôle surpriviliée

Mettre en œuvre la sécurité d'Azure Storage

- Décrire les services de stockage Azure : comptes de stockage, redondance, services, options de migration et de déplacement de fichiers
- Implémenter la sécurité et gérer l'accès pour Stockage Azure : transfert sécurisé, TLS minimal, accès anonyme, modèles d'autorisation dont l'identité managée, stratégies d'accès stockées, désactivation de la clé partagée via Azure Policy
- Configurer la sécurité réseau pour Stockage Azure : règles de réseau virtuel et d'adresse IP, règles d'instance de ressource et services approuvés, points de terminaison privés
- Implémenter Microsoft Defender pour le stockage : surveillance d'activité, analyse des programmes malveillants, détection des menaces sur les données sensibles, routage des alertes

Activités pratiques :

- Durcissement d'un compte de stockage : désactivation de la clé partagée, stratégie d'accès stockée, point de terminaison privé
- Activation de Defender pour le stockage et test de l'analyse des programmes malveillants

Mettre en œuvre la sécurité des bases de données Azure SQL

- Configurer la sécurité au niveau de la plateforme pour Azure SQL : authentification Microsoft Entra uniquement et identités managées, isolement réseau, chiffrement transparent des données avec clés gérées par le client, masquage dynamique des données et sécurité au niveau des lignes
- Configurer l'audit pour Azure SQL Database et SQL Managed Instance : groupes d'actions d'audit, destinations des journaux, stratégie d'audit conforme

– Implémenter Microsoft Defender pour les bases de données : Defender pour Azure SQL et pour les bases relationnelles open source, évaluation des vulnérabilités, routage des alertes

Activités pratiques :

- Passage d'une base Azure SQL en authentification Microsoft Entra uniquement et configuration de l'audit
- Évaluation des vulnérabilités et définition d'une ligne de base de sécurité

Mettre en œuvre les contrôles de sécurité réseau dans Azure

- Segmenter et isoler les charges de travail Azure à l'aide de contrôles de sécurité réseau : groupes de sécurité réseau (NSG), groupes de sécurité d'application (ASG), règles d'administration de sécurité Azure Virtual Network Manager, vérification des règles effectives avec Network Watcher
- Centraliser et appliquer l'inspection du trafic à l'aide du Pare-feu Azure : collections de règles et stratégie de pare-feu, filtrage par renseignement sur les menaces, hub Virtual WAN sécurisé
- Sécuriser la connectivité distante et hybride à l'aide de passerelles VPN et de l'Accès privé Microsoft Entra : durcissement des connexions site à site et point à site, accès Zero Trust par application
- Éliminer l'exposition du réseau public des services PaaS Azure : points de terminaison privés et DNS privé, service Azure Private Link, application et audit de l'adoption via Azure Policy et Defender for Cloud

Activités pratiques :

- Segmentation d'un réseau virtuel avec NSG et ASG, puis vérification avec Network Watcher
- Déploiement du Pare-feu Azure avec une stratégie de règles
- Remplacement d'un accès public PaaS par un point de terminaison privé

Mettre en œuvre la sécurité pour les solutions d'IA

- Sécuriser l'accès pour Microsoft Entra Agent ID : flux d'authentification des agents, stratégies d'accès conditionnel ciblant les agents, contrôle de l'accès et du cycle de vie
- Analyser les risques liés aux identités IA à l'aide de Microsoft Defender XDR : inventaire des agents IA, rayon d'impact et chemins d'attaque
- Activer la protection en temps réel pour les agents Copilot Studio : activation dans Microsoft Defender, revue des résultats de protection
- Configurer la sécurité de la passerelle IA dans Microsoft Foundry : architecture, création et configuration d'une passerelle, contrôle d'accès et supervision
- Configurer et gérer des garde-fous dans Microsoft Foundry : filtres de contenu, listes de blocage, Prompt Shields, choix et ajustement des garde-fous par charge de travail
- Protéger les charges de travail IA avec Microsoft Defender for Cloud : plan des charges de travail IA, posture de sécurité IA (CSPM), détection des menaces à l'exécution (CWP), investigation dans Defender XDR
- Activer Defender pour les services d'IA dans Microsoft Defender for Cloud : configuration du plan, tableau de bord de sécurité des données et de l'IA
- Gérer les agents à l'aide de Microsoft Agent 365 : inscription des agents, contrôles d'accès, supervision de l'activité et gouvernance
- Identifier les risques liés aux données IA avec la gestion de la posture de sécurité des données Microsoft Purview (DSPM) : surexposition des données SharePoint, risques des interactions Copilot et applications IA

Activités pratiques :

- Création d'une stratégie d'accès conditionnel ciblant des identités d'agents
- Configuration de garde-fous et d'une liste de blocage sur un déploiement Microsoft Foundry
- Activation de Defender pour les services d'IA et lecture du tableau de bord Données et IA

Mettre en œuvre la sécurité des serveurs et des machines virtuelles

- Implémenter le chiffrement de disque pour les machines virtuelles Azure : options de chiffrement des disques managés, chiffrement sur l'hôte avec clés gérées par le client, chiffrement de disque confidentiel, conformité via Azure Policy
- Configurer les fonctionnalités de sécurité du lancement approuvé (Trusted Launch) : démarrage sécurisé, vTPM, surveillance de l'intégrité, migration des machines Gen1
- Planifier et implémenter Azure Bastion : choix de la référence (SKU), déploiement, connexion par le portail et par client natif
- Gérer la sécurité des serveurs hybrides avec Azure Arc : contrôle des extensions, Azure Policy, posture dans Defender for Cloud
- Implémenter Microsoft Defender pour les serveurs : plans 1 et 2, analyse des vulnérabilités avec et sans agent, intégration de Defender pour point de terminaison (EDR), surveillance de l'intégrité des fichiers
- Activer et appliquer l'accès juste-à-temps aux machines virtuelles : stratégies par port, demande et audit des accès, application via Azure Policy
- Appliquer la configuration de sécurité des machines virtuelles avec Azure Machine Configuration : lignes de base Windows et Linux en mode audit et application, configurations personnalisées

Activités pratiques :

- Connexion à une machine virtuelle sans adresse IP publique via Azure Bastion
- Activation de l'accès juste-à-temps et audit d'une demande d'accès
- Intégration d'un serveur à Defender pour les serveurs et revue des vulnérabilités

Sécuriser les services de la plateforme applicative Azure

- Détecter les risques liés aux conteneurs à l'aide de Microsoft Defender pour les conteneurs : vulnérabilités des images ACR, menaces et erreurs de configuration à l'exécution sur AKS
- Implémenter des contrôles de sécurité pour Azure Kubernetes Service : intégration Microsoft Entra ID et RBAC Kubernetes, cluster privé et stratégies réseau, identité de charge de travail, normes de sécurité des pods
- Implémenter des contrôles de sécurité pour Azure Container Registry, Container Instances et Container Apps : contrôle d'accès, isolement réseau, identités managées, gestion des secrets
- Implémenter des contrôles de sécurité pour Azure Functions et Logic Apps : authentification et autorisation, intégration au réseau virtuel, points de terminaison privés, sécurité des connecteurs
- Implémenter des contrôles de sécurité pour Azure App Service et Web Application Firewall : authentification, identités managées, contrôles réseau, stratégies WAF sur Application Gateway
- Implémenter la sécurité du back-end d'API à l'aide de Gestion des API Azure : validation JWT et OAuth, filtrage IP et limitation de débit, mTLS vers le back-end, passerelle IA pour Microsoft Foundry

Activités pratiques :

- Revue des vulnérabilités d'images de conteneurs et des alertes d'exécution AKS dans Defender pour les conteneurs
- Protection d'une application App Service derrière un Web Application Firewall
- Mise en place d'une validation JWT dans Gestion des API

Gérer la posture de sécurité avec Microsoft Defender for Cloud

- Connecter des environnements hybrides et multiclouds à Microsoft Defender for Cloud : modèle de connectivité, stratégie de connecteurs, machines locales via Azure Arc, comptes AWS et projets GCP
- Identifier les risques de sécurité avec la gestion de la posture de sécurité cloud (CSPM) : plans CSPM, recommandations priorisées par le risque, analyse des chemins d'attaque, Cloud Security Explorer
- Découvrir des ressources et des vulnérabilités non protégées avec Microsoft Defender External Attack Surface Management (EASM) : découverte par graines, tableaux de bord, intégration à Defender CSPM
- Conformité par rapport aux frameworks de sécurité : suivi de la posture de conformité dans Defender for Cloud (voir chapitre gouvernance)
- Activer et configurer des plans de protection des charges de travail dans Microsoft Defender for Cloud : catalogue des plans CWP, activation, déploiement à grande échelle et vérification de la couverture
- Configurer la gestion des vulnérabilités Microsoft Defender pour les machines virtuelles Azure : méthodes d'analyse, revue des résultats et règles de désactivation, lignes de base de sécurité et blocage d'applications

Activités pratiques :

- Analyse d'un chemin d'attaque et requête dans Cloud Security Explorer
- Activation de plans de protection et contrôle de la couverture

Mettre en œuvre la collecte des activités et événements dans Microsoft Sentinel

- Créer et gérer des espaces de travail Microsoft Sentinel : architecture, intégration au portail Microsoft Defender, rôles et autorisations, gestion multilocataire avec Azure Lighthouse
- Gérer le contenu dans Microsoft Sentinel : solutions du hub de contenu, déploiement depuis un dépôt
- Connecter des services Microsoft à Microsoft Sentinel : connecteurs Microsoft 365, Microsoft Entra, Microsoft Entra ID Protection et Activité Azure
- Connecter des sources de données Syslog à Microsoft Sentinel : agent Azure Monitor et règle de collecte de données, analyse avec KQL
- Connecter des journaux Common Event Format (CEF) à Microsoft Sentinel : options de déploiement du connecteur
- Connecter des hôtes Windows à Microsoft Sentinel : événements de sécurité Windows via l'agent Azure Monitor et les règles de collecte de données, transfert d'événements Windows (WEF), journaux Sysmon
- Implémenter des règles d'automatisation et des playbooks dans Microsoft Sentinel : règles d'automatisation, playbooks du hub de contenu, playbook personnalisé avec Azure Logic Apps
- Gérer le stockage des données et interroger les journaux d'audit dans Microsoft Sentinel : tables de journaux personnalisées, rétention et archivage, connexion de Microsoft Purview Audit et requêtes dans Defender XDR

Activités pratiques :

- Création d'un espace de travail Microsoft Sentinel et connexion des sources Microsoft
- Collecte des événements de sécurité Windows avec une règle de collecte de données

- Création d'une règle d'automatisation déclenchant un playbook

Déployer et exploiter Microsoft Security Copilot

- Décire Microsoft Security Copilot : terminologie, traitement des invites, éléments d'une invite efficace, activation
- Configurer des espaces de travail pour Microsoft Security Copilot : planification, capacité (SCU) et résidence des données, rôles et autorisations, affectation aux agents intégrés, suivi de la consommation
- Gérer les plug-ins et les agents dans Microsoft Security Copilot : paramètres des plug-ins, agents Microsoft et agents du Magasin de sécurité, gestion des agents

Activités pratiques :

- Configuration d'un espace de travail Security Copilot et des rôles associés
- Activation d'un plug-in et d'un agent Microsoft intégré

Préparation à la certification

- Modalités de l'examen SC-500 : 120 minutes, QCM avec composants interactifs possibles, nombre de questions non publié, seuil de réussite 700/1000, examen surveillé, disponible en français
- Examen blanc : passage d'un test en conditions réelles
- Stratégies de réponse : gestion du temps, lecture des questions, élimination des distracteurs
- Révision ciblée : synthèse des points clés par domaine (identité, accès et gouvernance · stockage, bases de données et réseau · calcul sécurisé · posture de sécurité)
- Planification : inscription à l'examen et conseils de préparation post-formation

Activités pratiques :

- Examen blanc chronométré avec correction commentée
- Atelier de révision par domaine avec quiz

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de l'ensemble de nos formations : 4,9/5 — 735 avis

Berenice P. — formatrice agréable à l'écoute bonne pédagogie j'ai beaucoup apprécié nos échanges

Anne-Lise C. — Très bonne adaptation du formateur au public et au niveau d'attente.

Ils nous font confiance

Cette année notre filière Microsoft Azure a accompagné plus de 28 entreprises dont :

SILAE EPSILON FRANCE GERFLOR SAS LEMONWAY MALAKOFF HUMANIS AMAP ACENSI SANA ALIAPUR ALTECA APSIDE TOP AREAS
ASSURANCES +18 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com