



Objectifs	Concevoir, implémenter et gérer des contrôles de sécurité de bout en bout dans Microsoft Azure et Microsoft 365 ; sécuriser les identités et les accès ; protéger les secrets, le stockage, les bases de données, les réseaux, les charges de calcul, les applications et les API ; sécuriser les charges de travail IA et les agents ; gérer la conformité, la posture de sécurité, la collecte d'événements et les opérations assistées par Microsoft Security Copilot.
Participants	Ingénieurs sécurité cloud, administrateurs Azure, architectes sécurité, consultants cybersécurité, ingénieurs systèmes et réseaux, spécialistes DevSecOps et professionnels chargés de protéger des environnements cloud, hybrides, multiclouds et des charges de travail IA.
Prérequis	xpérience pratique de l'administration de Microsoft Azure et d'environnements hybrides, notamment le calcul, le réseau et le stockage ; bonne maîtrise de Microsoft Entra ID ; connaissance de l'administration Microsoft 365 ; compréhension des principes fondamentaux de la sécurité, de la conformité et de la supervision.
Moyens pédagogiques	1 poste par participant - 1 Vidéo projecteur - Support de cours fourni à chaque participant - Ateliers individuels - Modalités d'évaluation : Ateliers (TP) pendant tout le long de la formation et Evaluation des acquis tout au long de la formation
Méthodes pédagogiques	Approche participative et interactive - Alternance d'apports théoriques et de mises en situation - Accompagnement personnalisé du formateur
Type de formation	Formation présentielle ou distancielle, selon les besoins et les contraintes des participants
Tarif inter-entreprise	3320 € HT
Durée	4 jours - 28 heures
Modalités et délais d'accès	Formations accessibles sous 15 à 20 jours suite à votre demande. Un entretien initial doit être prévu avant votre entrée en formation.

Code : NCI_I3FDXX7M

Mis à jour le : 28 octobre 2026

Programme :

Module 1 - Sécuriser les identités et les accès avec Microsoft Entra

Configurer Privileged Identity Management, les rôles et les accès privilégiés.

Mettre en œuvre l'accès conditionnel, l'authentification multifacteur et sans mot de passe.

Sécuriser les applications, les inscriptions d'applications, les autorisations OAuth et le consentement.

Configurer les identités managées pour les ressources Azure.

Lab / Atelier : Configurer une stratégie d'accès conditionnel, activer PIM sur un rôle privilégié et valider l'accès d'une identité managée à une ressource Azure.

Module 2 - Protéger les secrets, les clés et la gouvernance cloud

Déployer et sécuriser Azure Key Vault avec RBAC, pare-feu, points de terminaison privés et journalisation.

Gérer les clés, secrets et certificats, puis détecter les secrets exposés.

Appliquer Azure Policy, les verrous de ressources, les rôles personnalisés et les contrôles de conformité.

Mettre en œuvre des contrôles de sécurité par infrastructure as code et protéger les sauvegardes.

Lab / Atelier : Déployer un coffre Azure Key Vault sécurisé, y stocker un secret, contrôler son accès et appliquer une initiative Azure Policy à

un abonnement de laboratoire

Module 3 - Sécuriser le stockage, les bases de données et les réseaux Azure

Configurer la sécurité des comptes de stockage, les pare-feu, les stratégies d'accès et Defender for Storage.

Sécuriser Azure SQL, activer l'audit et la protection Microsoft Defender pour les bases de données.

Mettre en œuvre NSG, ASG, Azure Virtual Network Manager, VPN et Azure Virtual WAN.

Configurer Private Endpoint, Private Link, Microsoft Entra Private Access, Azure Firewall et Network Watcher.

Lab / Atelier : Sécuriser une architecture de données Azure avec accès privé, règles réseau, audit SQL et diagnostics des règles de sécurité effectives.

Module 4 - Sécuriser les machines virtuelles, serveurs hybrides et multiclouds

Configurer le chiffrement de disque, Azure Bastion et l'accès juste-à-temps.

Étendre les contrôles avec Azure Arc vers les environnements hybrides et multiclouds.

Intégrer les serveurs à Defender for Servers et configurer EDR, analyse de vulnérabilités et analyse sans agent.



Activer le démarrage sécurisé, vTPM, la surveillance de l'intégrité et Azure Machine Configuration.

Lab / Atelier : Intégrer une machine virtuelle à Defender for Servers, activer JIT, analyser les vulnérabilités et vérifier les protections de la machine.

Module 5 - Sécuriser les conteneurs, applications et API

Identifier les erreurs de configuration et les risques d'exécution avec Defender for Containers.

Sécuriser Azure Kubernetes Service, Azure Container Registry, Container Instances et Container Apps.

Configurer l'authentification et l'accès réseau pour Azure Functions, Logic Apps et App Service.

Protéger les applications et les API avec Azure Web Application Firewall et Azure API Management.

Lab / Atelier : Appliquer des contrôles de sécurité à une application conteneurisée, protéger son registre et publier une API derrière une passerelle sécurisée.

Module 6 - Sécuriser les solutions d'IA, Copilot et les agents

Identifier la surexposition des données SharePoint et les risques liés à Copilot avec Microsoft Purview DSPM.

Protéger les agents Copilot Studio et gérer les identités d'agents Microsoft Entra.

Configurer une passerelle IA dans Azure API Management et les garde-fous de sécurité dans Microsoft Foundry.

Activer Defender pour les services IA et superviser la sécurité des données et de l'IA dans Defender for Cloud.

Lab / Atelier : Évaluer un scénario d'agent IA, limiter l'exposition des données, protéger les appels au modèle et configurer les contrôles de sécurité et de supervision.

Module 7 - Gérer la posture de sécurité avec Microsoft Defender for Cloud

Identifier et prioriser les risques avec Defender CSPM.

Évaluer la conformité aux référentiels et traiter les recommandations de sécurité.

Activer les plans de protection des charges de travail et connecter des environnements AWS et GCP.

Découvrir les ressources exposées et vulnérabilités avec Microsoft Defender EASM et Vulnerability Management.

Lab / Atelier : Analyser le Secure Score et les recommandations, corriger une configuration à risque et produire un plan de remédiation priorisé.

Module 8 - Superviser, automatiser et investiguer avec Sentinel et Security Copilot

Créer et sécuriser un espace de travail Microsoft Sentinel.

Connecter les sources Azure, Syslog, CEF et événements Windows, puis gérer tables et rétention.

Mettre en œuvre des règles d'automatisation et des playbooks pour la réponse aux incidents.

Configurer les espaces, rôles, plug-ins et agents dans Microsoft Security Copilot.

Lab / Atelier : Connecter une source de données à Microsoft Sentinel, créer une automatisation de réponse et utiliser Security Copilot pour accélérer l'analyse d'un incident de sécurité.