+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 15/07/2026

S'inscrire

Formation Microsoft Defender for Cloud

2 jours (14 heures)

Présentation

Microsoft Defender for Cloud est une plateforme de sécurité cloud conçue pour renforcer la posture de sécurité, prioriser les risques et protéger les charges de travail Azure,AWS et GCP. Avec le CSPM, le CWPP, les recommandations et le Secure Score, vous pilotez une sécurité plus lisible et plus opérationnelle.

Notre formation Microsoft Defender for Cloud vous permet d'aller au-delà de la découverte de l'outil pour maîtriser les sujets clés rencontrés dans un contexte multicloud et hybride.

Vous apprendrez à structurer une démarche de Cloud Security Posture Management, à analyser les recommandations de sécurité, à interpréter les indicateurs de risque et à exploiter les tableaux de bord de conformité réglementaire.

Vous verrez également comment activer et paramétrer les plans de protection CWPP, comprendre la couverture des workloads, suivre les écarts de configuration et mettre en place des actions de remédiation adaptées aux environnements de production.

À l'issue de la formation, vous serez en mesure de renforcer la visibilité, de mieux prioriser les alertes, d'améliorer la conformité et de déployer une stratégie de sécurité cloud plus robuste, plus cohérente et plus exploitable par les équipes opérationnelles.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Comprendre le rôle de Microsoft Defender for Cloud dans une stratégie de sécurité multicloud.
- Analyser la posture de sécurité d'un environnement et exploiter le Secure Score.

- Interpréter les recommandations, les niveaux de risque et les priorités de remédiation.
- Utiliser les fonctions de CSPM pour réduire les mauvaises configurations et améliorer la conformité.
- Configurer les plans CWPP pour protéger les workloads et suivre leur couverture.
- Mettre en œuvre des pratiques de pilotage, de contrôle et de suivi adaptées à un usage opérationnel.

Public visé

- Ingénieur sécurité cloud
- Architecte cloud
- Administrateur Azure
- Analyste SOC
- Consultant cybersécurité

Pré-requis

- Connaissance des fondamentaux de l'architecture cloud et des modèles de responsabilité partagée.
- Pratique d'Azure et compréhension des ressources, abonnements et groupes de ressources.
- Notions de sécurité informatique, de gestion des risques et de contrôle d'accès.
- Expérience de base avec AWS ou GCP appréciée pour le contexte multicloud.
- Capacité à lire des tableaux de bord de supervision et des indicateurs de conformité.

Pré-requis techniques

- Un ordinateur récent avec navigateur à jour et performances suffisantes pour les consoles cloud.
- Une connexion Internet stable en Wi-Fi ou en Ethernet.
- Un accès à un environnement Microsoft Azure avec droits suffisants pour consulter les paramètres de sécurité.
- Un compte Microsoft ou Entra ID actif pour réaliser les exercices et les connexions.
- En formation à distance, un micro et un casque pour suivre les démonstrations et les ateliers.

Programme de notre formation Microsoft Defender for Cloud

[Jour 1 - Matin]

Découvrir la plateforme et ses usages

- Positionnement de Microsoft Defender for Cloud dans l’écosystème de sécurité Microsoft.
- Différences entre CSPM et CWPP, et articulation avec les besoins métiers.
- Vue d’ensemble des environnements pris en charge, dont Azure, AWS et GCP.
- Lecture des principaux tableaux de bord, indicateurs et zones de navigation du portail.
- Compréhension des notions de posture de sécurité, de conformité et de priorisation.

- Atelier pratique : prendre en main l’interface, repérer les vues essentielles et identifier les informations utiles à un premier diagnostic.

[Jour 1 - Après-midi]

Analyser la posture de sécurité

- Fonctionnement du Secure Score et lecture de son évolution.
- Compréhension des recommandations de sécurité et de leur hiérarchisation.
- Analyse des facteurs de risque liés au contexte, à la configuration et à l’exposition.
- Utilisation des vues par ressource pour suivre les écarts et les actions correctives.
- Détection des mauvaises configurations les plus fréquentes dans un environnement cloud.
- Atelier pratique : analyser un jeu de recommandations, prioriser les remédiations et proposer un plan d’action.

[Jour 2 - Matin]

Exploiter le CSPM et la conformité

- Principes du Cloud Security Posture Management dans Defender for Cloud.
- Utilisation des standards de sécurité et des cadres de conformité réglementaire.
- Lecture du tableau de bord de conformité et interprétation des écarts.
- Gestion des politiques, des évaluations continues et des remédiations associées.
- Suivi de la couverture de sécurité sur un périmètre hybride ou multicloud.
- Atelier pratique : qualifier un périmètre, examiner sa conformité et identifier les écarts prioritaires à corriger.

[Jour 2 - Après-midi]

Déployer la protection des workloads

- Activation et usage des plans CWPP pour protéger les workloads.
- Panorama des protections selon les ressources, avec focus sur les serveurs, bases et stockages.
- Compréhension des réglages de couverture, des périmètres et des options de déploiement.
- Suivi des alertes, des incidents et des signaux utiles au pilotage opérationnel.
- Bonnes pratiques pour organiser la remédiation, le contrôle et le suivi dans la durée.
- Atelier pratique : configurer un scénario de protection, vérifier la couverture et préparer une restitution de sécurité exploitable.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.