# Formation Sécurité du Cloud : concepts et bonnes pratiques (multi-cloud)

| | |
|---|---|
| **Durée :** | 3 jours (21 heures) |
| **Tarifs inter-entreprise :** | 2 475,00 € HT (standard)<br>1 980,00 € HT (remisé) |
| **Public :** | Architectes, ingénieurs systèmes / réseaux, ingénieurs Cloud, RSSI, chefs de projet techniques |
| **Pré-requis :** | Bonnes connaissances générales des systèmes d'information et des notions de virtualisation / Cloud |
| **Objectifs :** | Comprendre les modèles de responsabilité partagée et les principes de sécurité du Cloud - Identifier les principaux risques liés aux environnements IaaS, PaaS et SaaS - Mettre en œuvre les bonnes pratiques de sécurisation des comptes, ressources et données en environnement multi-cloud - Structurer une démarche de gouvernance, de conformité et de supervision de la sécurité dans le Cloud |
| **Modalités pédagogiques, techniques et d'encadrement :** | • Formation synchrone en présentiel et distanciel.<br>• Méthodologie basée sur l'Active Learning : 75 % de pratique minimum.<br>• Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat.<br>• Un formateur expert. |
| **Modalités d'évaluation :** | • Définition des besoins et attentes des apprenants en amont de la formation.<br>• Auto-positionnement à l'entrée et la sortie de la formation.<br>• Suivi continu par les formateurs durant les ateliers pratiques.<br>• Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation. |
| **Sanction :** | Attestation de fin de formation mentionnant le résultat des acquis |

| | |
|---|---|
| **Référence :** | CYB102773-F |
| **Note de satisfaction des participants:** | Pas de données disponibles |
| **Contacts :** | commercial@dawan.fr - 09 72 37 73 73 |
| **Modalités d'accès :** | Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard. |
| **Délais d'accès :** | Variable selon le type de financement. |
| **Accessibilité :** | Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins |

## Comprendre les fondamentaux de la sécurité dans le Cloud

Définir les modèles de services Cloud : IaaS, PaaS, SaaS
Analyser les modèles de responsabilité partagée selon les principaux fournisseurs (AWS, Azure, GCP)
Identifier les menaces spécifiques au Cloud : exposition Internet, erreurs de configuration, fuites de données
Comprendre les enjeux de conformité (RGPD, NIS2, standards sectoriels) dans un contexte Cloud
**Atelier fil rouge : cartographier les usages Cloud de son organisation et identifier les principaux risques associés**

## Sécuriser les identités, les accès et les comptes Cloud

Mettre en œuvre les bonnes pratiques d'authentification forte (MFA, SSO, fédération)
Structurer les rôles et permissions (RBAC, ABAC, comptes techniques, comptes privilégiés)
Séparer les environnements (production, préproduction, tests) et gérer les comptes d'administration
Surveiller et auditer l'activité des comptes (logs, journaux d'accès, alertes)
**Atelier fil rouge : définir un modèle de rôles et bonnes pratiques d'accès pour un tenant multi-cloud fictif**

## Protéger les ressources et les données en environnement multi-cloud

Sécuriser le réseau dans le Cloud : VPC, sous-réseaux, groupes de sécurité, pare-feu applicatifs
Mettre en œuvre le chiffrement des données au repos et en transit (clés gérées par le

fournisseur, KMS, BYOK)
Contrôler la sécurité des stockages objets, bases de données managées et services PaaS
Gérer les sauvegardes, la résilience et la restauration en contexte Cloud
**Atelier fil rouge : analyser une architecture Cloud simplifiée et proposer des améliorations de sécurisation des données**

## Industrialiser la sécurité : gouvernance, conformité et supervision

Mettre en place des politiques Cloud (policies, blueprints, landing zones) pour encadrer les déploiements
Utiliser les services natifs de contrôle et de conformité (Security Center, Security Hub, recommandations CIS)
Centraliser les journaux et mettre en place une supervision de la sécurité (SIEM, alertes, tableaux de bord)
Organiser les revues régulières de configuration et de posture de sécurité Cloud
**Atelier fil rouge : construire un mini-plan de gouvernance et de supervision sécurité pour un environnement multi-cloud**

## Construire une feuille de route de sécurité Cloud

Prioriser les chantiers de sécurisation en fonction des risques et des contraintes métier
Définir les rôles et compétences à développer autour du Cloud security (SecOps, FinOps, DevSecOps)
Intégrer la sécurité Cloud dans les projets, les contrats et les relations avec les prestataires
Élaborer une feuille de route de montée en maturité sur 12 à 24 mois
**Atelier fil rouge final : formaliser une feuille de route Cloud security pour son organisation ou un cas d’école**