# AWS Security Best Practices – Formation intensive («AWSB09»)

Découvrez comment établir et maintenir une posture de sécurité dans le cloud AWS. Cette formation sur les bonnes pratiques AWS en matière de sécurité vous aide à concevoir et mettre en œuvre des solutions pour garder vos charges de travail sécurisées.

**Durée:** 1 jour
**Prix :** 900.– excl. 8.1% TVA
**Documents :** Support de cours officiel AWS numérique

## Contenu

Actuellement, le coût moyen d'une faille de sécurité peut s'élever à plus de 4 millions de dollars. La formation « AWS Security Best Practices » donne un aperçu des bonnes pratiques d'utilisation de la sécurité AWS et des types de contrôles. Ce cours vous permet de comprendre vos responsabilités tout en proposant des lignes directrices précieuses pour garder vos charges de travail sécurisées.
Vous apprendrez comment sécuriser votre infrastructure réseau en utilisant des options de design fiables. Vous apprendrez également comment renforcer et gérer vos ressources de calcul en toute sécurité. Finalement, en comprenant les méthodes de surveillance et d'alerte AWS, vous serez capable de détecter des événements suspects et de donner l'alerte afin d'initier rapidement un processus de réaction en cas de cyberattaque potentielle.

### Module 1 : Aperçu de la sécurité sur AWS

- Le modèle de responsabilité partagée
- Les défis des clients
- Frameworks et standards
- Établir de bonnes pratiques
- La conformité sur AWS

### Module 2 : Sécuriser le réseau

- Flexible et sécurisé
- La sécurité au sein d'Amazon Virtual Private Cloud (Amazon VPC)
- Les services de sécurité
- Les solutions de sécurité de tiers

Exercice 1 : Contrôler le réseau

- Créer une infrastructure réseau avec trois zones de sécurité
- Mettre en œuvre une segmentation du réseau en utilisant les groupes de sécurité, les Network Access Control Lists (NACLs) ainsi que les sous-réseaux publics et privés
- Surveiller le trafic réseau vers les instances Amazon Elastic Compute Cloud (EC2) en utilisant les journaux de flux VPC

### Module 3 : Sécurité d'Amazon EC2

- Durcissement informatique
- Cryptage avec Amazon Elastic Block Store (EBS)
- Gestion et maintenance sécurisée
- Détecter les vulnérabilités
- Utiliser AWS Marketplace

Exercice 2 : Sécuriser la source (EC2)

- Créer une Amazon Machine Image (AMI) personnalisée

- Déployer une nouvelle instance EC2 depuis une AMI personnalisée
- Corriger une instance EC2 avec AWS Systems Manager
- Crypter un volume EBS
- Comprendre comment fonctionne le cryptage EBS et comment il impacte les autres opérations
- Utiliser des groupes de sécurité pour limiter le trafic entre les instances EC2 aux données cryptées

**Module 4 : Surveiller et alerter**

- Journaliser le trafic du réseau
- Journaliser le trafic utilisateur et de l'API (Application Programming Interface)
- La visibilité avec Amazon CloudWatch
- Améliorer la surveillance et les alertes
- Vérifier votre environnement AWS

Exercice 3 : Contrôle de la sécurité

- Configurer une instance Amazon Linux 2 pour envoyer des fichiers journaux à Amazon CloudWatch
- Créer des alarmes et notifications Amazon CloudWatch pour surveiller les tentatives de connexion échouées
- Créer des alarmes Amazon CloudWatch pour surveiller le trafic du réseau par une passerelle Network Address Translation (NAT)

## Objectifs

- Concevoir et mettre en œuvre une infrastructure réseau sécurisée
- Concevoir et mettre en œuvre la sécurité informatique
- Concevoir et mettre en œuvre une solution de gestion des logs

## Public cible

Ce cours est destiné aux rôles professionnels suivants :

- Solution Architect
- Cyber Security
- CloudOps
- DevOps

**Pourquoi suivre ce cours en particulier ?** Quels sont les avantages de ce cours ? Nos formatrices et formateurs répondent à ces **questions**. Nous avons demandé à notre équipe de formatrices et formateurs d'écrire un petit texte qui explique POURQUOI la formation est particulièrement importante pour le rôle professionnel et ce qui peut être attendu du cours. Vous trouverez ces informations dans la description du cours sous la rubrique « informations complémentaires ».

## Prérequis

Les participantes et participants doivent avoir au préalable suivi les formations suivantes ou s'assurer de posséder des connaissances équivalentes :

- AWS Security Fundamentals
- AWS Security Essentials

- AWS Security Essentials – Formation intensive («AWSE04»)

## Certification

Cette formation couvre des sujets essentiels pour les examens ANS-C01 et SCS-C02 des certifications « AWS Certified Advanced Networking - Specialty » et « AWS Certified Security - Specialty ».

Nous conseillons aux personnes intéressées par la certification « AWS Certified Advanced Networking - Specialty » de suivre également la formation suivante pour maîtriser toute la matière de l'examen associé :

- Networking Essentials for Cloud Applications on AWS

Nous conseillons aux personnes intéressées par la certification « AWS Certified Security - Specialty » de suivre également les formations suivantes pour maîtriser toute la matière de l'examen associé :

- AWS Security Essentials
- AWS Security Governance at Scale
- Security Engineering on AWS

## Informations complémentaires

**Paroles de formatrices et formateurs**
Suivre la formation « AWS Security Best Practices » présente de nombreux avantages pour les individus et les entreprises. En voici quelques-uns :

1. Connaissances accrues de la sécurité : Cette formation permet d'acquérir des connaissances complètes des bonnes pratiques en matière de sécurité AWS. Vous découvrirez divers concepts, techniques et outils de sécurité spécifiques à l'environnement AWS. Ces connaissances vous permettront de sécuriser efficacement vos infrastructures et applications AWS en réduisant le risque de failles sécuritaires et l'accès non autorisé.
2. Protection des données et des biens : AWS est un des fournisseurs de services cloud leader du marché, hébergeant une très grande quantité de données sensibles et des infrastructures critiques pour des entreprises du monde entier. Dans cette formation, vous acquerrez des connaissances en sécurisation de vos ressources AWS, en protection de vos données contre l'accès non autorisé, en mise en œuvre du chiffrement et de configurations de réseaux sécurisés. Vous participerez ainsi à la protection des biens de votre entreprise, à l'établissement d'une relation de confiance avec les clients et à la conformité avec les règles de sécurité qui s'appliquent.
3. Réduire les risques sécuritaires : étant donné que les cybermenaces continuent d'évoluer, il est particulièrement important de rester à jour sur les pratiques de sécurité les plus récentes. Cette formation couvre les risques sécuritaires courants et les vulnérabilités spécifiques à AWS et vous guide pour réduire efficacement ces risques. Vous découvrirez les bonnes pratiques concernant la gestion des identités et des accès, la sécurité du réseau, la surveillance et la journalisation, la réponse aux incidents et bien plus encore. Grâce à l'application de ces bonnes pratiques, vous réduirez de manière proactive les risques sécuritaires et répondrez de manière appropriée aux potentiels incidents.
4. Reconnaissance de l'industrie et carrière : Les certifications et formations AWS ont un poids significatif dans l'industrie informatique. En suivant la formation « AWS Security Best Practices », vous acquerrez des connaissances et compétences précieuses qui pourront être mises en avant dans votre CV et votre profil professionnel. Cela peut vous différencier des autres, améliorer votre image et ouvrir des opportunités de carrière dans la sécurité du cloud et des rôles professionnels AWS.
5. Conformité et préparation à l'audit : De nombreuses entreprises ont des exigences spécifiques en matière de conformité, telles que l'HIPAA dans la santé ou le RGPD pour la protection des données. La formation « AWS Security Best Practices » vous guide pour aligner vos mesures de sécurité AWS avec les standards de conformité qui s'appliquent. Vous apprendrez à implémenter les contrôles nécessaires, effectuer des audits et maintenir une documentation pour assurer à votre entreprise de rester dans le cadre de la conformité et éviter les sanctions.

Le paysage de la sécurité est en constante évolution et rester à jour avec les dernières bonnes pratiques est essentiel. Grâce à la formation « AWS Security Best Practices » vous acquerrez les connaissances et compétences nécessaires pour sécuriser votre infrastructure AWS, protéger vos données et aborder avec confiance les défis de la sécurité du cloud.

## Formations complémentaires

- Security Engineering on AWS – Formation intensive («AWSS04»)
- AWS Security Governance at Scale – Formation intensive («AWSE07»)
- Advanced Architecting on AWS – Formation intensive («AWSA02»)
- Advanced Architecting on AWS with JAM– Formation intensive («AWSA2J»)

## Avez-vous une question ou souhaitez-vous organiser un cours en entreprise ?

Nous vous conseillons volontiers au +41 22 738 80 80 ou romandie@digicomp.ch. Retrouvez toutes les informations détaillées concernant les dates sur www.digicomp.ch/formations-it-providers/amazon-web-services-aws/aws-solutions-architect/cours-aws-security-best-practices-formation-intensive