

## **AWS : Ingénierie de sécurité sur Amazon Web Services**

### **Formation officielle Security Engineering on AWS**

#### **DESCRIPTION**

L'ingénierie de sécurité (Security Engineering) sur AWS démontre comment utiliser les services AWS pour être protégé efficacement et en toute conformité dans le Cloud Amazon.

La formation se concentre sur les meilleures pratiques recommandées par AWS pour améliorer la sécurité de vos données et de vos systèmes hébergés dans le Cloud, que cela concerne les services de calcul, de stockage, de réseau ou de base de données.

Cette formation porte également sur les objectifs communs en matière de contrôle de la sécurité et des normes de conformité telles que les authentifications, les autorisations ou bien encore le chiffrement. Elle permet de préparer l'examen de certification AWS Certified Security - Specialty (certification éditeur).

#### **OBJECTIFS PEDAGOGIQUES**

- Apprendre à tirer avantage du modèle de sécurité en responsabilité partagée d'AWS
- Décrire la gestion des identités des utilisateurs et de leurs accès sur l'environnement AWS
- Employer les services de sécurité AWS dont : AWS Identity and Access Management, Amazon Virtual Private Cloud, AWS Config, AWS CloudTrail, AWS Key Management Service, AWS CloudHSM, et AWS Trusted Advisor
- Mettre en oeuvre de meilleurs contrôles de sécurité pour vos ressources sur AWS
- Décrire la gestion et l'audit des ressources du point de vue de la sécurité
- Superviser et tracer les accès et les usages des ressources AWS, telles que les instances, le stockage, le réseau et les services de bases de données
- Identifier les services et les outils AWS qui permettent d'aider l'automatisation, la surveillance et la gestion des opérations de sécurité sur AWS
- Décrire la gestion des incidents de sécurité sur l'environnement AWS

#### **PUBLIC CIBLE**

- Ingénieur sécurité
- Architecte sécurité
- Tout professionnel de la sécurité de l'information

Sécurité

Code :  
**AWSSE**

Durée :  
**3 jour(s) (21,00 heures)**

Exposés : **30.00 %**  
Cas pratiques : **50.00 %**  
Echanges d'expérience : **20.00 %**

**Inter-entreprises :**  
Prochaines sessions  
disponibles [sur notre site web](#).  
Tarif : 2 370,00 € HT /  
participant

**Intra-entreprise :**  
Tarifs et dates sur demande.

## PRE-REQUIS

- Avoir des connaissances des pratiques de sécurité dans le domaine de l'informatique en général.
- Disposer d'une expérience en gouvernance, évaluation du risque, en contrôle, et de conformité aux normes.
- Pour assister à cette formation, il est recommandé d'avoir suivi les modules "AWS : Notions de sécurité Amazon Web Services de base" (AWS10) et "AWS : Architecture sur Amazon Web Services" (AWS01).

## METHODE PEDAGOGIQUE

Formation avec apports théoriques, échanges sur les contextes des participants et retours d'expérience pratique des formateurs, complétés de travaux pratiques et de mises en situation.

## PROFIL DES INTERVENANTS

Cette formation est dispensée par un·e ou plusieurs consultant·es d'OCTO Technology ou de son réseau de partenaires, expert·es reconnus des sujets traités.

Le processus de sélection de nos formateurs et formatrices est exigeant et repose sur une évaluation rigoureuse leurs capacités techniques, de leur expérience professionnelle et de leurs compétences pédagogiques.

Par ailleurs, pour animer cette formation, nos intervenant·es doivent répondre aux critères imposés par Amazon Web Services

## MODALITÉS D'ÉVALUATION ET FORMALISATION À L'ISSUE DE LA FORMATION

L'évaluation des acquis se fait tout au long de la session au travers des ateliers et des mises en pratique.

Afin de valider les compétences acquises lors de la formation, un formulaire d'auto-positionnement est envoyé en amont et en aval de celle-ci.

En l'absence de réponse d'un ou plusieurs participants, un temps sera consacré en ouverture de session pour prendre connaissance du positionnement de chaque stagiaire sur les objectifs pédagogiques évalués.

Une évaluation à chaud est également effectuée en fin de session pour mesurer la satisfaction des stagiaires et un certificat de réalisation leur est adressé individuellement.

## PROGRAMME PEDAGOGIQUE DETAILLE

Jour 1

**INTRODUCTION À LA SÉCURITÉ DANS LE CLOUD**

- Sécurité dans le cloud AWS
- Modèle de responsabilité partagée AWS
- Présentation de la réponse aux incidents
- DevOps avec ingénierie de sécurité

**IDENTIFIER LES POINTS D'ENTRÉE SUR AWS**

- Identifier les différentes manières d'accéder à la plate-forme AWS
- Comprendre les stratégies IAM
- Limite des autorisations IAM
- Analyseur d'accès IAM
- Authentification multi-facteur
- AWS CloudTrail
- Lab : accès entre comptes

**SÉCURITÉ DES ENVIRONNEMENTS WEB APPLICATIFS**

- Menaces dans une architecture à trois niveaux
- Menaces courantes : accès utilisateur
- Menaces courantes : accès aux données
- Conseiller de confiance AWS

**SÉCURITÉ DES APPLICATIONS**

- Images de machines Amazon
- Inspecteur Amazon
- Gestionnaire de systèmes AWS
- Lab : utilisation d'AWS Systems Manager et d'Amazon Inspector

**SÉCURITÉ DES DONNÉES**

- Stratégies de protection des données
- Cryptage sur AWS
- Protection des données au repos avec Amazon S3, Amazon RDS, Amazon DynamoDB
- Protection des données archivées avec Amazon S3 Glacier
- Analyseur d'accès Amazon S3
- Points d'accès Amazon S3

## Jour 2

### **SÉCURISATION DES COMMUNICATIONS RÉSEAU**

- Considérations relatives à la sécurité d'Amazon VPC
- Mise en miroir du trafic Amazon VPC
- Réponse aux instances compromises
- Équilibrage de charge élastique
- Gestionnaire de certificats AWS

### **SURVEILLANCE ET COLLECTE DE JOURNAUX SUR AWS**

- Amazon CloudWatch et les journaux CloudWatch
- AWS Config
- Amazon Macie
- Journaux de flux Amazon VPC
- Journaux d'accès au serveur Amazon S3
- Journaux d'accès ELB
- Lab : surveiller et répondre avec AWS Config

### **TRAITEMENT DES JOURNAUX SUR AWS**

- Amazon Kinesis
- Amazon Athena
- Lab : analyse des journaux de serveur Web

### **SÉCURITÉ DES ENVIRONNEMENTS HYBRIDES**

- Connexions AWS Site-to-Site et Client VPN
- AWS Direct Connect
- AWS Transit Gateway

### **PROTECTION HORS-RÉGION**

- Amazon Route 53
- AWS WAF
- Amazon CloudFront
- AWS Shield
- AWS Firewall Manager
- Atténuation des DDoS sur AWS

## Jour 3

#### **SÉCURITÉ SUR DES ENVIRONNEMENTS SANS SERVEUR**

- Amazon Cognito
- Amazon API Gateway
- AWS Lambda

#### **DÉTECTION ET INVESTIGATION DES MENACES**

- Amazon GuardDuty
- AWS Security Hub
- Amazon Detective

#### **GESTION DES SECRETS SUR AWS**

- AWS KMS
- AWS CloudHSM
- AWS Secrets Manager
- Lab : utilisation d'AWS KMS

#### **AUTOMATISATION ET SÉCURITÉ PAR LA CONCEPTION**

- AWS CloudFormation
- Catalogue de services AWS
- Laboratoire 06 : automatisation de la sécurité sur AWS avec AWS Service Catalog

#### **GESTION DES COMPTES ET PROVISIONNEMENT SUR AWS**

- Organisations AWS
- Tour de contrôle AWS
- AWS SSO
- AWS Directory Service
- Lab : accès fédéré avec ADFS

---

#### **Accessibilité**

L'inclusion est sujet important pour OCTO Academy.  
Nos référent-es sont à votre disposition pour faciliter l'adaptation de votre formation à vos besoins spécifiques.  
Pour les contacter : [academy.accessibilite@octo.com](mailto:academy.accessibilite@octo.com)