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

- Expliquer le modèle de responsabilité partagée d'AWS et l'appliquer pour définir les responsabilités et contrôles de sécurité adaptés à son contexte.
- Décrire la gestion des identités des utilisateurs et de leurs accès sur l'environnement AWS
- Mettre en œuvre les services de sécurité AWS (IAM, VPC, AWS Config, CloudTrail, KMS, CloudHSM, Trusted Advisor) afin de sécuriser, auditer et optimiser un environnement.
- 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
- Surveiller et auditer les accès et usages des ressources AWS (compute, stockage, réseau, bases de données) à l'aide des outils de traçabilité et de monitoring.
- 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

Sécurité

Code :
AWSSE

Durée :
3 jour(s) (21,00 heures)

Exposés : **30 %**
Cas pratiques : **50 %**
Echanges d'expérience : **20 %**

Inter-entreprises :
Prochaines sessions disponibles sur notre site web.
Tarif : 2 380,00 € HT / participant

Intra-entreprise :
Tarifs et dates sur demande.

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

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 ET RAPPEL DES FONDAMENTAUX

- Présenter les principes de la sécurité dans le cloud AWS.
- Expliquer le modèle de responsabilité partagée sur AWS
- Résumer les concepts liés à IAM, la protection des données, la détection des menaces et les réponses adaptées
- Présenter les différentes façons d'interagir avec AWS : console, CLI et SDKs
- Expliquer l'utilisation de l'authentification multifacteur (MFA) pour renforcer la sécurité
- Présenter les bonnes pratiques pour sécuriser le compte root et les clés d'accès

SÉCURISATION DES POINTS D'ENTRÉE SUR AWS

- Décrire comment utiliser l'authentification multifacteur (MFA) pour plus de sécurité
- Présenter les mesures de protection du compte root et des clés d'accès
- Expliquer les politiques IAM, les rôles, les composants des politiques et les frontières de permissions
- Présenter la journalisation et la consultation des requêtes API via AWS CloudTrail, ainsi que l'analyse de l'historique des accès
- Mise en pratique : Utilisation des politiques d'identité et des politiques basées sur les ressources

GESTION ET APPROVISIONNEMENT DES COMPTES AWS

- Expliquer la gestion multi-comptes avec AWS Organizations et AWS Control Tower
- Mettre en oeuvre un environnement multi-comptes à l'aide d'AWS Control Tower
- Montrer comment utiliser des fournisseurs d'identité et des courtiers pour accéder aux services AWS
- Présenter AWS IAM Identity Center (successeur d'AWS Single Sign-On) et AWS Directory Service

Jour 2

GESTION DES SECRETS SUR AWS

- Présenter et comparer les solutions : AWS KMS, CloudHSM, AWS Certificate Manager (ACM) et AWS Secrets Manager
- Démontrer la création d'une clé AWS KMS couvrant plusieurs régions
- Chiffrer un secret dans Secrets Manager à l'aide d'une clé KMS
- Utiliser un secret chiffré pour se connecter à une base de données Amazon RDS dans plusieurs régions AWS
- Mise en pratique : Chiffrement des secrets dans Secrets Manager à l'aide d'AWS KMS

SÉCURITÉ DES DONNÉES

- Surveiller les données sensibles avec Amazon Macie
- Protéger les données au repos grâce au chiffrement et au contrôle d'accès
- Identifier les services AWS utilisés pour la réplication des données à des fins de protection
- Protéger les données après archivage
- Mise en pratique : Sécurité des données dans Amazon S3

PROTECTION DES INFRASTRUCTURES À LA PÉRIPHÉRIE

- Présenter les fonctionnalités AWS pour une infrastructure sécurisée
- Décrire les services garantissant la résilience en cas d'attaque
- Identifier les services AWS protégeant les workloads contre les menaces externes
- Comparer AWS Shield et AWS Shield Avanced
- Expliquer comment le déploiement centralisé avec AWS Firewall Manager améliore la sécurité
- Mise en pratique : Protection contre le trafic malveillant avec AWS WAF

Jour 3

SUPERVISION ET COLLECTE DES JOURNAUX SUR AWS

- Expliquer l'importance de la génération et collecte des logs
- Utiliser les VPC Flow Logs pour la surveillance des événements

de sécurité
- Surveiller les écarts par rapport au comportement normal
- Présenter les événements Amazon EventBridge
- Décrire les métriques et alarmes Amazon CloudWatch
- Présenter les techniques et solutions disponibles pour l'analyse des logs
- Identifier le cas d'usage de la mise en miroir du trafic VPC
- Mise en pratique : Supervision et réponse aux incidents de sécurité

RÉPONSE AUX MENACES

- Classifier les types d'incidents et les workflows de réponse à incident
- Identifier les sources d'information pour la gestion d'incidents via les services AWS
- Préparer efficacement une organisation à la gestion d'incidents
- Détecter les menaces à l'aide des services AWS et analyser les résultats pour y répondre
- Mise en pratique : Gestion de la réponse à incident

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