Security Engineering on AWS (AWSSO)

ID AWSSO **Prix** CHF 2 470,– (Hors Taxe) **Durée** 3 jours

A qui s'adresse cette formation

- Ingénieurs en sécurité
- Architectes en sécurité
- Architectes du cloud
- Opérateurs du cloud

Cette formation prépare à la/aux certifications

AWS Certified Security – Specialty (ACSS)

Pré-requis

Il vous est recommandé d'avoir suivi ces formations ou d'avoir les connaissances de ces formations:

- AWS Technical Essentials (AWSE)
- Architecting on AWS (AWSA)

et

- Bien connaître les pratiques de sécurité informatique et les concepts d'infrastructure
- Connaissance du Cloud AWS

Objectifs

A l'issue de ce cours, vous serez en mesure de : :

- Comprendre la sécurité du cloud AWS en se basant sur la triade CIA.
- Créer et analyser l'authentification et les autorisations avec IAM.
- Gérer et provisionner des comptes sur AWS avec les services AWS appropriés.
- Identifier comment gérer les secrets en utilisant les services AWS.
- Surveiller les informations sensibles et protéger les données par le chiffrement et les contrôles d'accès.
- Identifier les services AWS qui traitent les attaques provenant de sources externes.
- Surveiller, générer et collecter des journaux.
- Identifier les indicateurs d'incidents de sécurité.
- Identifier comment enquêter sur les menaces et les atténuer à l'aide des services AWS.

Contenu

Jour 1

Module 1 : Présentation et examen de la sécurité

- Expliquer la sécurité dans le cloud AWS.
- Expliquer le modèle de responsabilité partagée d'AWS.
- Résumer les notions d'IAM, de protection des données et de détection et réponse aux menaces.
- Indiquer les différentes façons d'interagir avec AWS à l'aide de la console, de la CLI et des SDK.
- Décrire comment utiliser le MFA pour une protection supplémentaire.
- Indiquer comment protéger le compte utilisateur root et les clés d'accès.

Module 2 : Sécuriser les points d'entrée sur AWS

- Décrire comment utiliser l'authentification multi-facteurs (MFA) pour une protection supplémentaire.
- Décrire comment protéger le compte utilisateur root et les clés d'accès.
- Décrire les politiques IAM, les rôles, les composants de politique et les limites de permission.
- Expliquer comment les requêtes API peuvent être enregistrées et visualisées à l'aide d'AWS CloudTrail et comment visualiser et analyser l'historique des accès.
- Laboratoire pratique 1 : Utilisation des politiques basées sur les identités et les ressources.

Module 3 : Gestion des comptes et provisionnement sur AWS

- Expliquer comment gérer plusieurs comptes AWS en utilisant AWS Organizations et AWS Control Tower.
- Expliquer comment mettre en œuvre des environnements multi-comptes avec AWS Control Tower.
- Démontrer la capacité à utiliser les fournisseurs d'identité et les courtiers pour obtenir l'accès aux services AWS.
- Expliquer l'utilisation de AWS IAM Identity Center (successeur de AWS Single Sign-On) et de AWS Directory Service.
- Démontrer la capacité à gérer l'accès des utilisateurs d'un

domaine avec Directory Service et IAM Identity Center.
- Laboratoire pratique 2 : Gestion de l'accès aux utilisateurs du domaine avec AWS Directory Service

Jour 2

Module 4 : Gestion des secrets sur AWS

- Décrire et lister les fonctionnalités de AWS KMS, CloudHSM, AWS Certificate Manager (ACM), et AWS Secrets Manager.
- Démontrer comment créer une clé AWS KMS multirégion.
- Démontrer comment chiffrer un secret Secrets Manager avec une clé AWS KMS.
- Démontrer comment utiliser un secret crypté pour se connecter à une base de données Amazon Relational Database Service (Amazon RDS) dans plusieurs régions AWS.
- Laboratoire pratique 3 : Utiliser AWS KMS pour chiffrer les secrets dans Secrets Manager

Module 5 : Sécurité des données

- Surveiller les données à la recherche d'informations sensibles avec Amazon Macie.
- Décrire comment protéger les données "au repos" par le chiffrement et les contrôles d'accès.
- Identifier les services AWS utilisés pour répliquer les données à des fins de protection.
- Déterminer comment protéger les données après leur archivage.
- Laboratoire pratique 4 : Sécurité des données dans Amazon S3

Module 6 : Protection de la périphérie de l'infrastructure

- Décrire les fonctionnalités AWS utilisées pour construire une infrastructure sécurisée.
- Décrire les services AWS utilisés pour créer de la résilience lors d'une attaque.
- Identifier les services AWS utilisés pour protéger les charges de travail des menaces externes.
- Comparer les fonctionnalités d'AWS Shield et d'AWS Shield Advanced.
- Expliquer comment le déploiement centralisé d'AWS Firewall Manager peut améliorer la sécurité.
- Laboratoire pratique 5 : Utiliser AWS WAF pour atténuer le trafic malveillant

Jour 3

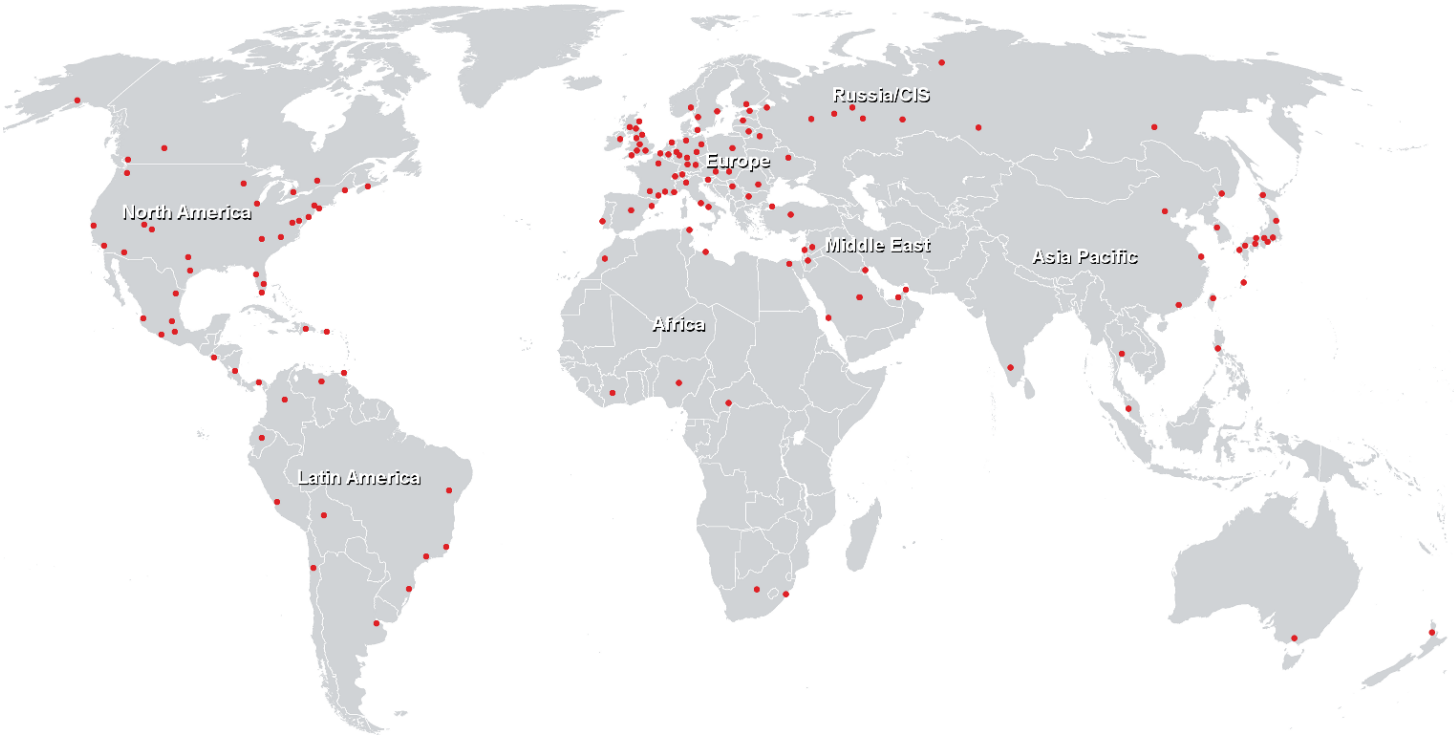
Module 7 : Surveillance et collecte de logs sur AWS

- Identifier l'intérêt de générer et de collecter des logs.
- Utiliser Amazon Virtual Private Cloud (Amazon VPC) Flow Logs pour surveiller les événements de sécurité.
- Expliquer comment surveiller les déviations de la ligne de base.
- Décrire les événements Amazon EventBridge.
- Décrire les métriques et les alarmes d'Amazon CloudWatch.
- Énumérer les options d'analyse des journaux et les techniques disponibles.
- Identifier les cas d'utilisation de la mise en miroir du trafic dans les clouds privés virtuels (VPC).
- Laboratoire pratique 6 : Surveiller et répondre aux incidents de sécurité

Module 8 : Répondre aux menaces

- Classer les types d'incidents dans la réponse aux incidents.
- Comprendre les flux de travail de la réponse aux incidents.
- Découvrir les sources d'information pour la réponse aux incidents en utilisant les services AWS.
- Comprendre comment se préparer aux incidents.
- Détecter les menaces à l'aide des services AWS.
- Analyser les résultats de sécurité et y répondre.
- Laboratoire pratique 7 : Réponse aux incidents

Centres de formation dans le monde entier



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch