[sfeir] Institute

AWS | AWSSECENG

Security Engineering on AWS

3jours / 21h

Objectifs pédagogiques

- Énoncer une compréhension de la sécurité du cloud AWS basée 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 à l'aide des services AWS.
- Surveiller les informations sensibles et protégez les données via le cryptage 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.

Public cible

- Ingénieurs en sécurité
- Architectes de sécurité
- Architectes Cloud

Prérequis

Nous recommandons aux participants de ce cours d'avoir

- Suivi les cours suivants AWS Security Essentials et Architecting on AWS

- Une connaissance opérationnelle des pratiques de sécurité informatique et des concepts d'infrastructure.
- Une familiarité avec le Cloud AWS.

Programme

Jour 1

Module 1 : Présentation et examen de la sécurité

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

Module 2 : Sécurisation des points d'entrée sur AWS

- Décrire comment utiliser l'authentification multifacteur (MFA) pour une protection supplémentaire.
- Décrire comment protéger le compte utilisateur root et les clés d'accès.
- Décrire les stratégies IAM, les rôles, les composants de stratégie et les limites d'autorisation.
- Expliquer comment les demandes d'API peuvent être enregistrées et affichées à l'aide d'AWS CloudTrail et comment afficher et analyser l'historique des accès.
- Mise en pratique : Utilisation de stratégies basées sur l'identité et les ressources.

Module 3 : Gestion de compte et provisionnement sur AWS

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

- Démontrer la capacité à gérer l'accès des utilisateurs de domaine avec Directory Service et IAM Identity Center.
- Mise en pratique : Gestion de l'accès des utilisateurs au domaine avec AWS Directory Service

Jour 2

Module 4 : Gestion des secrets sur AWS

- Décrire et répertorier les fonctionnalités d'AWS KMS, CloudHSM, AWS Certificate Manager (ACM) et
  Gestionnaire de secrets AWS.
- Montrer comment créer une clé AWS KMS multirégionale.
- Montrer comment chiffrer un secret Secrets Manager avec une clé AWS KMS.
- Démontrer comment utiliser un secret chiffré pour se connecter à une base de données Amazon Relational Database Service (Amazon RDS) dans plusieurs régions AWS
- Mise en pratique : Atelier 3 : Utilisation d'AWS KMS pour chiffrer des secrets dans Secrets Manager

Module 5 : Sécurité des données

- Surveiller les données pour les informations sensibles avec Amazon Macie.
- Décrire comment protéger les données au repos grâce au chiffrement et aux 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.
- Mise en pratique : Atelier 4 : Sécurité des données dans Amazon S3

Module 6 : Protection de la périphérie de l'infrastructure

- Décrire les fonctionnalités AWS utilisées pour créer 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 contre les 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.
- Mise en pratique : Atelier 5 : Utilisation d'AWS WAF pour atténuer le trafic malveillant

Jour 3

Module 7 : Surveillance et collecte de journaux sur AWS

- Identifier la valeur de la génération et de la collecte des logs.
- Utiliser les journaux de flux Amazon Virtual Private Cloud (Amazon VPC) pour surveiller les événements de sécurité.
- Expliquer comment surveiller les écarts de référence.
- Décrire les événements Amazon EventBridge.
- Décrire les métriques et les alarmes Amazon CloudWatch.
- Liste des options d'analyse des journaux et des techniques disponibles.
- Identifier les cas d'utilisation pour l'utilisation de la mise en miroir du trafic du cloud privé virtuel (VPC).
- Mise en pratique : Laboratoire 6 : Surveillance et réponse 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 réponse aux incidents.
- Découvrer les sources d'informations pour la réponse aux incidents à l'aide des services AWS.
- Comprendre comment se préparer aux incidents.
- Détecter les menaces à l'aide des services AWS.
- Analyser et répondre aux constatations de sécurité.
- Mise en pratique : Réponse aux incidents