Security Operations on AWS

Objectifs

- Comprendre et tirer parti du modèle de sécurité à responsabilité partagée d'AWS
- Gérer les identités et les accès des utilisateurs sur l'environnement AWS
- Utilisez les services de sécurité AWS tels qu'AWS Identity and Access Management, Amazon Virtual Private Cloud, AWS Config, AWS CloudTrail, AWS Key Management Service, AWS CloudHSM, Et AWS Trusted Advisor
- Implémentez de meilleurs contrôles de sécurité pour vos ressources sur AWS
- Gérez et auditez vos ressources d'un point de vue sécurité
- Surveillez et suivez l'accès et l'utilisation des ressources AWS, telles que les instances, le stockage, les services de réseau et de base de données.
- Identifier les services et outils AWS pour aider à automatiser, surveiller et gérer les opérations de sécurité sur AWS
- Gérer les incidents de sécurité sur l'environnement AWS

Prérequis

- Amazon Web Services - L'architecture ou des connaissances et compétences équivalentes sont recommandées.
- Connaissance des pratiques de sécurité informatique en général
- Expérience en gouvernance, contrôle, évaluation des risques et conformité aux normes.

Programme de formation

Sécurité AWS

- Principes de conception de la sécurité du cloud AWS
- Modèle de responsabilité partagée AWS
- DevOps avec ingénierie de sécurité

Identifier les points d'entrée vers AWS

- Bonnes pratiques sur les informations d'identification des utilisateurs
- Analyse des politiques IAM
- Authentification multifacteur
- AWS CloudTrail
- Exercices pratiques :
    - Authentification entre comptes

Sécurité dans les environnements d'applications Web

- Menaces dans une architecture à trois niveaux
- Conseiller de confiance AWS

Sécurité des applications

- Considérations de sécurité Amazon EC2
- Inspecteur Amazon
- Gestionnaire de système AWS
- Exercices pratiques :
    - Utilisation d'AWS Systems Manager et d'Amazon Inspector

Sécurité des données

- Protéger les données au repos avec Amazon S3
- Considérations sur la sécurité d'Amazon RDS et d'Amazon DynamoDB
- Protection des données d'archives

Sécuriser les communications réseau

- Considérations sur la sécurité d'Amazon VPC
- Considérations relatives à la sécurité d'Amazon Elastic Load Balancing
- Gestionnaire de certificats AWS

Surveillance et journalisation sur AWS

- ConfigurationAWS
- Amazon CloudWatch
- Amazon Macie
- Collecte de journaux sur AWS
- Exercices pratiques :
    - Surveillance et réponse avec AWS Config

Traitement des journaux sur AWS

- Amazon Kinèse
- Amazone Athéna
- Exercices pratiques :
    - Analyse des journaux du serveur Web avec Amazon Kinesis et Amazon Athena

Analyse des journaux du serveur Web avec Amazon Kinesis et Amazon Athena

- Considérations de sécurité : environnements hybrides
- Connexions VPN AWS
- AWS Direct Connect

Passerelle de transit AWS

- Protection hors région
- Amazonie Route 53
- Amazon CloudFront
- AWSWAF
- Bouclier AWS

Sécuriser les environnements sans serveur

- Amazon Cognito
- Passerelle API Amazon
- AWS Lambda

Détection et enquête des menaces

- Service de garde Amazon
- Centre de sécurité AWS
- Détective Amazon

Gestion des secrets sur AWS

- AWSKMS
- AWSCloudHSM
- Gestionnaire de secrets AWS
- Exercices pratiques :
    - Utilisation d'AWS KMS

Automatisation de la sécurité sur AWS

- Approche AWS de sécurité dès la conception
- AWS CloudFormation
- Catalogue de services AWS
- Exercices pratiques :
    - Utilisation du catalogue de services AWS

Gestion et provisionnement des comptes sur AWS

- Organisations AWS
- Tour de contrôle AWS
- Accès utilisateur fédéré
- Exercices pratiques :
    - Authentification fédérée AWS

-