

CyberSécurité

Sécurité Cloud (36 heures)

26_27_4IRC_08_CYBER_UE8_080_MAJ

ACQUIS

- Développer une compréhension approfondie de la sécurité cloud, en abordant les principes fondamentaux tels que le modèle de responsabilité partagée et les architectures multi-tier.
- Configurer des services cloud sécurisés, en mettant l'accent sur la gestion des accès (IAM) et la sécurité des données (S3).
- Appliquer les meilleures pratiques de chiffrement pour sécuriser les données en transit et au repos.
- Identifier les vulnérabilités potentielles et proposer des stratégies efficaces de récupération après sinistre (Disaster Recovery).
- Maîtriser les techniques de chiffrement et leur application à des scénarios réels.
- Rédiger et présenter un rapport technique détaillé.

CONTENU

- Introduction à l'infrastructure cloud et à la sécurité réseau
- Concepts fondamentaux : Régions, Zones de Disponibilité (AZ).
- Virtual Private Cloud (VPC) : sous-réseaux, passerelles, routage.
- Sécurité réseau : Groupes de sécurité et NACL.
- Travaux pratiques : Création et sécurisation d'une infrastructure cloud.
- Gestion des identités et des accès (IAM) (4 heures)
- Utilisateurs, groupes, rôles et politiques IAM.
- Principe du moindre privilège et authentification multifacteur (MFA).
- Travaux pratiques : Configuration et test de politiques IAM.
- Sécurisation des données et chiffrement
- Protection des données au repos (S3) et en transit (TLS, ACM).
- Chiffrement avec AWS KMS.
- Travaux pratiques : Sécurisation et audit des données avec S3.
- Récupération après sinistre (Disaster Recovery)
- Sauvegarde, restauration et haute disponibilité.
- Automatisation des scénarios de reprise.
- Travaux pratiques : Simulation de récupération après sinistre.

PRÉREQUIS

- Compréhension des concepts fondamentaux en réseaux et en sécurité informatique.

- Notions essentielles sur la gestion des rôles et des permissions.
- Bases solides en cryptographie.

PÉDAGOGIE

ÉVALUATION

BIBLIOGRAPHIE