Sécurité cloud : architecture

Modèle de responsabilité partagée AWS

AWS fonctionne selon un modèle appelé :

- “Security of the Cloud” (AWS)
- “Security in the Cloud” (Client)

La sécurité est partagée entre AWS et le client.

Responsabilités d’AWS → Security OF the Cloud

AWS est responsable de la sécurité de l’infrastructure cloud.

Cela inclut :

Infrastructure physique

- Centres de données
- Sécurité physique des bâtiments
- Contrôle d’accès biométrique
- Alimentation électrique, climatisation

Infrastructure réseau

- Réseau mondial AWS
- Matériel réseau
- Isolation entre clients

Matériel et virtualisation

- Serveurs physiques
- Stockage
- Hyperviseur (ex: Nitro)

En résumé : AWS protège l’infrastructure sous-jacente.

Responsabilités du Client → Security IN the Cloud

Le client est responsable de tout ce qu’il déploie et configure. Cela inclut :

Gestion des accès

- IAM (Users, Roles, Policies)
- MFA

- Gestion des mots de passe

Configuration des services

- Groupes de sécurité
- NACL
- Paramètres S3 (ex: éviter les buckets publics)

Données

- Chiffrement
- Classification des données
- Sauvegardes

Systèmes d’exploitation (selon le service)

- Patchs
- Mises à jour
- Antivirus