PHASE 3 – Audit, Traçabilité et Journalisation

1. Objectifs de l’audit

L’audit et la traçabilité constituent un pilier fondamental de la sécurité et de la conformité réglementaire.

Ils permettent de reconstituer l’historique des actions effectuées sur les données sensibles.

2. Table audit_logs

Une table dédiée audit_logs a été créée pour centraliser les événements de sécurité.

Chaque entrée contient l’utilisateur, l’action effectuée, la table concernée, l’identifiant de l’enregistrement, la date et l’adresse IP.

3. Triggers PostgreSQL

Des triggers automatiques ont été configurés afin d’enregistrer toute modification critique.

Les opérations UPDATE et DELETE sur la table accounts sont systématiquement journalisées.

Les consultations de données sensibles font également l’objet d’un enregistrement.

4. Exploitation des logs

Les données d’audit sont exploitées via un dashboard dédié.

Ce dashboard permet de filtrer les événements par utilisateur, type d’action et période.

Il constitue un outil essentiel pour les équipes de sécurité et de conformité.

5. Conformité réglementaire

Le dispositif d’audit mis en place répond aux exigences du RGPD et des autorités bancaires.

Il permet notamment de démontrer la responsabilité et la traçabilité des accès aux données personnelles.