Plan de sécurité et de conformité

1. Chiffrement des données (Data encryption)

- **Données en transit (Data in transit)** :
    - **Utilisation de TLS (Transport Layer Security)** : Toutes les communications entre les systèmes OLTP, OLAP, NoSQL, et d'autres services externes doivent être protégées par TLS (v1.2 minimum) pour assurer la confidentialité et l'intégrité des données en transit.
    - **VPN et Tunnels Sécurisés** : Pour les communications internes entre les clusters de serveurs (OLTP, OLAP, NoSQL), établir des tunnels sécurisés ou utiliser un VPN interne pour protéger les données transitant sur des réseaux non sécurisés.

- **Données au repos (Data at rest) :**
    - **Chiffrement AES-256** : Toutes les données sensibles stockées dans les bases de données (OLTP, OLAP) et les NoSQL (S3, MongoDB, etc.) doivent être chiffrées avec un algorithme de chiffrement fort comme AES-256.
    - **Gestion des Clés (KMS)** : Utiliser un service de gestion des clés (KMS - Key Management Service) pour gérer les clés de chiffrement. Séparer les clés de chiffrement en fonction des environnements (production, test, développement).

2. Contrôles d'accès et authentification

- **Contrôle d'Accès Basé sur les Rôles (RBAC) :**
    - **Définir des rôles spécifiques** : Utiliser des rôles pour accorder des permissions minimales nécessaires aux utilisateurs, équipes, et services (principe du moindre privilège).
    - **Segmentation des privilèges** : Les accès doivent être segmentés entre les environnements de développement, de test, et de production pour éviter que des utilisateurs non autorisés accèdent aux données sensibles.

- **Authentification Multi-Facteurs (MFA) :**
    - **Activer MFA** : Toutes les connexions aux services sensibles (accès à la base de données, portails de gestion cloud) doivent être protégées par une authentification multi-facteurs pour renforcer la sécurité.

- **Accès sécurisé aux bases de données :**
    - **Authentification par OAuth 2.0 ou JWT** : Pour les accès automatisés aux bases de données ou API, utiliser OAuth 2.0 ou des jetons JWT pour garantir que seuls les services autorisés peuvent interagir avec les données.

3. Audit et traçabilité des accès

- **Journaux de connexion et activité (Audit Logs) :**
    - **Surveillance des accès aux données** : Configurer des journaux d'audit pour enregistrer toutes les connexions aux bases de données (OLTP, OLAP, NoSQL) et autres ressources sensibles. Les informations à enregistrer incluent l'horodatage, l'identité de l'utilisateur/service, l'action réalisée, et les données affectées.
    - **Conservation des journaux** : Conserver les journaux pour une période déterminée et assurer une rotation sécurisée des logs pour éviter les fuites de données.

- **Alertes pour activités suspectes :**
    - **Configurer des alertes** : Mettre en place des alertes automatisées pour détecter les activités anormales ou suspectes (Tentatives de connexion échouées, accès non autorisés à des données sensibles).
    - **Analyse comportementale** : Utiliser des outils de détection d'anomalies pour surveiller le comportement des utilisateurs et détecter les tentatives de compromission ou les accès inhabituels aux données.

4. Sécurité des systèmes et services

- **Sécurité des bases de données**
    - **Configuration sécurisée** : Activer les paramètres de sécurité par défaut sur les bases de données (chiffrement, restrictions de port) et restreindre les accès externes.
    - **Mise à jour et patch management** : Mettre en œuvre une stratégie de gestion des correctifs pour assurer que toutes les bases de données et systèmes de gestion de données (OLTP, OLAP, NoSQL) sont mis à jour régulièrement.

- **Protection des API et endpoints**
    - **Protection par pare-feu Web (WAF)** : Protéger les endpoints critiques (API de transactions, dashboards d'administration) avec un pare-feu applicatif (WAF) pour empêcher les attaques (SQL injection, XSS).
    - **Limiter le taux de requête (Rate limiting)** : Mettre en place un système de limitation de taux (rate limiting) pour éviter les attaques de type déni de service (DDoS) sur les endpoints.

5. Gestion des données sensibles et conformité

- **Anonymisation et pseudonymisation des données**

    - **Pseudonymisation des données sensibles** : Appliquer une pseudonymisation aux champs de données personnelles (noms, e-mails) afin de minimiser l'exposition des données en cas de violation.
    - **Anonymisation pour l'analyse** : Si des données sensibles doivent être partagées pour des analyses ou des projets tiers, appliquer une anonymisation complète pour protéger les informations personnelles identifiables.

- **Conformité aux Réglementations** :

    - **Respect de GDPR, PCI-DSS, CCPA** : Assurer que les pratiques de collecte, de stockage, et de traitement des données sont en conformité avec les exigences légales de toutes les juridictions concernées.
    - **Politique de conservation des données** : Mettre en place des politiques de conservation et de suppression des données qui respectent les exigences de confidentialité et garantissent que les données ne sont conservées que pour la durée nécessaire.

6. Surveillance en temps réel et alertes

- **Intégration SIEM (Security Information and Event Management) :**

    - **Collecte des logs et monitoring en temps réel** : Mettre en place un système SIEM pour collecter les logs de sécurité provenant des bases de données, serveurs, et endpoints, permettant une surveillance et une détection des menaces en temps réel.
    - **Alertes en cas de violation de sécurité** : Configurer des alertes automatiques en cas de détection de comportements malveillants (transfert de données inhabituel, violation d'accès).

7. Tests de sécurité et audits

- **Tests de oénétration et audits de sécurité**

    - **Réaliser des tests de pénétration réguliers** : Effectuer des tests de pénétration sur les systèmes de gestion de données pour identifier et corriger les vulnérabilités potentielles.
    - **Audits de conformité** : Conduire des audits réguliers pour vérifier la conformité aux réglementations (GDPR, PCI-DSS) et aux meilleures pratiques de sécurité.

8. Plan de Réponse aux Incidents de Sécurité

- **Élaboration d'un Plan de Réponse aux Incidents (IRP) :**
    - **Détection et réponse rapide** : Élaborer un plan clair de réponse aux incidents, y compris les étapes pour détecter, contenir, analyser, et résoudre les incidents de sécurité.
    - **Communication des incidents** : Prévoir des protocoles de communication pour informer les parties prenantes et les autorités compétentes en cas de violation ou de compromission de données.

- **Simulations et Formations :**
    - **Formations des équipes** : Former régulièrement les équipes aux meilleures pratiques de sécurité et à la réponse aux incidents.
    - **Simulations d'incidents** : Effectuer des simulations de violations de sécurité pour tester la capacité de réponse des équipes et améliorer le plan de réponse.