DOCUMENTATION SUR LES API'S, CONTRÔLES DE SÉCURITÉ ET MÉCANISMES D'ISOLATION DES # MCP

1. Stardog (Base de Graphe Sémantique)

- **API**

Fournit une API web standard (HTTP) pour interroger les données via les langages de graphe (SPARQL, GraphQL) et des bibliothèques pour intégration facile dans diverses applications.

- **Contrôles de sécurité**

Gère l'accès via authentification multiple (dont Kerberos) et contrôle précisément les droits utilisateurs (RBAC) sur les bases et les éléments du graphe; sécurise les connexions (TLS).

- **Mécanismes d'isolation**

Permet de séparer les accès logiques entre différentes bases de données ou graphes via les rôles, et sécurise l'accès aux données externes via les graphes virtuels.

2. Neo4j (Base de Graphe Native)

- **API**

Offre un protocole binaire optimisé (Bolt) pour les requêtes Cypher via drivers, une API web (HTTP) et une interface GraphQL pour la flexibilité d'intégration.

- **Contrôles de sécurité**

Propose authentification variée, contrôle d'accès par rôles (RBAC) extensible à des règles très fines (propriétés) en version Enterprise, et chiffre les données en transit (TLS) et au repos (Enterprise).

- **Mécanismes d'isolation**

Isole les données via les rôles utilisateurs et les permissions très fines sur les éléments du graphe (Enterprise), ainsi que par base de données distincte.

3. Denodo Platform (Virtualisation de Données)

- **API**

Permet l'accès unifié aux données via SQL standard (JDBC/ODBC) et expose facilement ces données comme des services web modernes (REST, OData, GraphQL).

- **Contrôles de sécurité**

S'intègre aux systèmes d'authentification d'entreprise (SAML, OAuth2...), offre un contrôle d'accès très précis (jusqu'à la ligne/colonne), masque les données sensibles et peut déléguer l'authentification aux sources. Sécurise toutes les connexions (TLS).

- **Mécanismes d'isolation**

Cloisonne l'accès aux données de manière très fine grâce aux rôles, aux règles sur les lignes/colonnes, au masquage, et peut appliquer des politiques de sécurité globales basées sur les métadonnées.

4. Sinequa (Recherche & Analyse Intelligente)

- **API**

Expose principalement une API REST pour lancer des recherches et récupérer des résultats structurés, complétée par des outils pour construire rapidement des interfaces de recherche.

- **Contrôles de sécurité**

S'appuie sur l'authentification unique de l'entreprise (SSO) et garantit que les résultats de recherche respectent les permissions des systèmes sources en filtrant selon les ACLs indexées. Sécurise les flux via TLS.

- **Mécanismes d'isolation**

Isole les informations en s'assurant que chaque utilisateur ne voit que les documents autorisés dans les sources, permet de créer des index séparés (collections) et gère les droits d'administration via RBAC.

5. AWS Kendra (Recherche Intelligente Cloud)

- **API**

Fournit une API REST gérée via les outils AWS (SDKs, CLI) pour toutes les opérations, de la requête à l'administration de l'index.

- **Contrôles de sécurité**

Utilise exclusivement le système d'identité AWS (IAM) pour l'authentification et l'autorisation, filtre les résultats selon le contexte utilisateur et les ACLs sources, et chiffre systématiquement les données (TLS, KMS).

- **Mécanismes d'isolation**

Isole fortement les cas d'usage via des index séparés, contrôle les accès administrateurs et utilisateurs via IAM, et assure l'isolation des données au sein d'un index via le filtrage basé sur les ACLs.