

Projets PFEE

Titre du Projet : « NEXUS » : Conception et Prototypage d'une Plateforme Cloud Souveraine et Cybersécurisée pour Données de Santé Sensibles

Entreprise Partenaire (fictive) : HealthDataGuard (HDG) – Start-up spécialisée dans la sécurité des données de santé, souhaitant se positionner sur le marché européen avec une offre cloud de confiance.

Contexte Métier & Opportunité :

Le marché européen du cloud de santé est en pleine expansion, porté par le RGPD et de nouvelles règlementations (ex: European Health Data Space - EHDS). Les acteurs historiques (AWS, Azure, GCP) sont perçus avec méfiance par les hôpitaux et cliniques européens en raison du Cloud Act américain. HealthDataGuard identifie une opportunité pour une offre cloud **souveraine** (hébergée en UE), **cybersécurisée** de bout en bout et **nativement conforme** au RGPD et aux spécificités du secteur santé (HDS en France).

L'objectif du PFEE est de réaliser l'étude de faisabilité et le **Proof of Concept (PoC)** d'une plateforme innovante.

Objectifs Principaux du Projet :

L'équipe d'élèves-ingénieurs devra mener les travaux suivants :

1. Étude de l'État de l'Art & Conformité :

- Analyse comparative des réglementations (RGPD, HDS, future EHDS, Cloud Act) et de leur impact sur l'architecture.
- Benchmark technique des solutions de chiffrement (homomorphe, porteuse, en transit/repos) et des technologies de confidentialité (Confidential Computing, enclaves TEE - Trusted Execution Environment).
- Rédaction d'une note stratégique sur le positionnement de l'offre.

2. Conception de l'Architecture Cible (Architecture Blueprint) :

- Conception d'une architecture micro-services modulaire et scalable (potentiellement avec Kubernetes).
- Intégration native de la sécurité : *Zero-Trust Network*, chiffrement des données à la source, gestion centralisée des identités et des accès (IAM), journalisation (logging) et traçabilité de toutes les actions.
- *Scénarisation d'un cas d'usage concret* : Le déploiement sécurisé d'un modèle d'IA pour la prédition de maladies à partir de données d'imagerie médicale anonymisées.

3. Développement du Proof of Concept (PoC) :

- Déploiement d'un mini-cloud privé sur une infrastructure dédiée (type serveurs bare-metal).
- Implémentation d'un service cœur : un **stockage objet sécurisé** (type S3) avec chiffrement automatique des données uploadées et journalisation des accès.
- Développement d'une **API de gestion des consentements** permettant à un patient de suivre et révoquer l'accès à ses données via un portail.
- Rédaction de la documentation technique et d'un manuel d'installation.

4. Validation & Tests :

- Rédaction d'un plan de test de charge et de pénétration (pentest) pour évaluer la performance et la résilience de la plateforme.
- Simulation d'une attaque et test du plan de réponse aux incidents.
- Audit de conformité du PoC au regard d'un sous-ensemble d'exigences RGPD/HDS.

Livrables Attendus (Production de l'Équipe) :

- **Livrable 1** : Rapport d'Étude (10 pages) incluant l'analyse réglementaire, le benchmark technologique et l'architecture cible.
- **Livrable 2** : Code source commenté du PoC (dépôt Git) avec documentation technique.