

# CONTRAT DE LIVRAISON - PROJET 2

## Groupe 3 - Safeguard Financial (SGF) - Moteur de Détection de Fraude

Date : 19 décembre 2025

Durée : 9 jours par élève (36 jours/homme total)

---

### MEMBRES DU GROUPE

- **Sébastien Yang** - sebastien.yang@epitech.digital
  - **Virgile Ader** - virgile.ader@epitech.digital
  - **Joséphine Poulin** - josephine.poulin@epitech.digital
  - **Charles Henry Noah** - charles-henry.noah@epitech.digital
- 

### LIVRABLES ATTENDUS

#### MUST (Indispensable)

- **API Gateway opérationnelle** : Ingestion des transactions en temps réel avec validation du format JSON standardisé
- **Moteur hybride complet** : Rules Service (règles déterministes) + Model Serving (ML XGBoost/LightGBM) avec fusion des scores
- **Décision <100ms garantie** : Latence end-to-end mesurée et prouvée (p95 <100ms sous charge 1000 TPS minimum)
- **Case Management Interface** : Dashboard analyste (Alice persona) avec queues high/medium/low risk, priorisation par score
- **Logs immuables conformes** : PostgreSQL avec WORM (Write Once Read Many), audit\_logs signés HMAC-SHA256, rétention 7 ans
- **Conformité RGPD/PSD2** : Anonymisation automatique après 90 jours, SCA dynamique, journalisation DPIA
- **Communication asynchrone** : Kafka pour diffusion résultats sans bloquer la transaction (ou RabbitMQ si justifié)
- **Feature Engineering** : Transformation données brutes → variables numériques pour le modèle (montant normalisé, time diff, geo features)

#### SHOULD (Important)

- **Monitoring temps réel** : Dashboard Marc (persona IT) avec latences (ms), erreurs/seconde, taux de fraude détecté
- **Boucle de réentraînement** : Pipeline automatisé mensuel avec nouvelles données labellisées par analystes
- **Cache Redis** : Deny-lists et allow-lists pour accélération des règles métier (IPs blacklistées, cartes volées)

- **Interface de labellisation** : Permettre à Alice de marquer fraude\_confirmed / false\_positive pour feedback ML
- **Rapports ACPR** : Génération automatique de rapports PDF signés électroniquement pour conformité
- **Multi-tenancy** : Séparation des données par filiale (comme Marc persona le demande pour BNP Paribas)

### COULD (Bonus)

- **Analyse SHAP avancée** : Explicabilité détaillée des décisions ML avec contributions des features
- **Génération données synthétiques** : Utilisation LLM pour créer patterns de fraude réalistes (entraînement)
- **Rapports analytics** : Visualisations Grafana des tendances de fraude, évolution des patterns
- **SCA adaptatif** : Ajustement dynamique du niveau d'authentification selon le score de risque
- **Intégration legacy** : Connecteurs pour systèmes bancaires non standards (hors MVP)

---

### PÉNALITÉS (Maximum -15 points)

**Critères livrabilité CRITIQUE (max -5 pts)** - Livrables non rendus à temps : -3 pts (cahier des charges, code source, ou documentation manquants)  
 - Projet ne démarre pas (erreurs d'installation, dépendances manquantes) : -2 pts

**Critères techniques (max -3 pts)** - Latence p95 >200ms : -2 pts (objectif <100ms affiché, tolérance jusqu'à 200ms) - Moteur hybride incomplet (Rules OU ML absent ou non fonctionnel) : -1 pt

**Critères qualité et sécurité (max -2 pts)** - Logs non signés ou modifiables (pas de HMAC-SHA256, pas d'immuabilité) : -1 pt - Absence totale de tests de charge (aucune mesure de performance publiée) : -1 pt

**Organisation - Participation déséquilibrée au github** : -5 pt (si tous les membres ne participent pas équitablement)

---

### CRITÈRES DE SUCCÈS

**Scénario de démonstration attendu** : 1. **Transaction légitime** : Ingestion → Rules (OK) → ML score 0.15 → Décision APPROVE (<100ms) 2. **Transaction suspecte règle** : Montant 10 000€ nocturne → Rules (BLOCK) → Pas de call ML → REJECT immédiat 3. **Transaction suspecte ML** : Pattern anormal → ML score 0.85 → REVIEW → Alerte Alice (analyste) 4. **Case man-**

**agement** : Alice ouvre l'alerte, voit historique client, marque false\_positive → Feedback stocké 5. **Monitoring** : Marc (IT) vérifie dashboard : 1247 transactions/h, latence p95 = 87ms, 0 erreurs 6. **Conformité** : Kumar (conformité) exporte audit\_logs signés HMAC-SHA256 pour rapport ACPR

**Performance minimale** : - Latence p95 <200ms end-to-end (objectif <100ms si possible) - Throughput 1000 TPS minimum soutenu pendant 5 minutes (objectif 50k TPS documenté mais non exigé pour MVP) - Disponibilité API >99% (tolérance <1% d'erreurs 5xx) - Logs 100% signés et immuables (aucune modification possible)

**Qualité du code** : - README complet : prérequis, installation, lancement, tests - Architecture documentée avec schémas (composants, séquences, déploiement) - Tests de charge avec résultats publiés (JMeter, Gatling, ou k6) - Code commenté sur parties critiques (fusion scores, feature engineering)

---

## JALONS INTERMÉDIAIRES

**Jalon 1** :

**Jalon 2** :

**Jalon 3** :

---

## DOCUMENTATION TECHNIQUE REQUISE

**README.md obligatoire** : - Prérequis (Docker, versions, RAM nécessaire) - Installation pas-à-pas (commandes exactes) - Lancement services (docker-compose up ou scripts) - Exemples d'appels API (curl, Postman collection)

**Architecture documentée** : - Schéma C4 Level 1 (contexte système) - Schéma C4 Level 2 (conteneurs : API Gateway, Kafka, PostgreSQL, etc.) - Diagramme de séquence : transaction suspecte → détection → alerte - Dimensionnement infrastructure (calcul CPU/RAM/network pour 1000 TPS)

**Guide analyste** : - Utilisation dashboard Alice (filtres, priorisation) - Workflow de validation d'alerte - Marquage fraude\_confirmed / false\_positive

**Rapports de tests** : - Tests de charge : configuration, résultats, graphiques latence - Tests de conformité : validation logs immuables, signature HMAC, anonymisation

---

## Signatures

Groupe 3 : \_\_\_\_\_ Date : \_\_\_\_\_  
Évaluateur : \_\_\_\_\_ Date : \_\_\_\_\_

---

**NOTE IMPORTANTE AU GROUPE :**

Votre note au Projet 1 reflète des **problèmes d'exécution graves**, pas un manque de compétences techniques. Vos personas sont excellents, votre compréhension de la conformité bancaire est solide, et vos ambitions techniques (50k TPS, <100ms) montrent de l'ambition.

**Ce qui a échoué** : livrables non rendus, timing explosé, participation déséquilibrée, profondeur technique insuffisante.

**Ce que nous attendons pour Projet 2** : 1. **LIVRER À TEMPS** : Cahier des charges complet rendu AVANT la soutenance 2. **GÉRER LE TEMPS** : 10 minutes MAX, répétition obligatoire 3. **PARTICIPER ÉQUITABLEMENT** : Tous les membres présentent 4. **APPROFONDIR** : Schémas techniques, code fonctionnel, tests de charge réels

Vous avez le potentiel pour un excellent projet. Prouvez-le par l'exécution, pas juste par les slides.