DOCUMENT DE SPÉCIFICATIONS

Phase 1.1 : Analyse des Besoins

Plateforme de gestion et de monitoring post-cyberattaque

20 janvier 2026

1 Introduction

1.1 Contexte du projet

Le 15 décembre 2025, DigitalBank France a subi une attaque par ransomware ayant entraîné l'indisponibilité de plusieurs systèmes critiques : base de données principale, services applicatifs et outils de supervision. La banque doit désormais se doter d'une nouvelle plateforme de gestion et de monitoring permettant de reprendre le contrôle sur son activité, de renforcer la sécurité et de restaurer la confiance des clients et des régulateurs.

La plateforme à concevoir doit s'appuyer sur des briques *no-code / low-code* afin de permettre une mise en place rapide, une maintenance plus simple et une meilleure collaboration entre équipes techniques et métiers. Elle doit couvrir à la fois les besoins de supervision technique, de détection de fraude et de support aux clients.

1.2 Objectif du document

Ce document a pour objectif de formaliser les besoins fonctionnels de la future plateforme à travers :

- la définition des principaux **personas** utilisateurs ;
- la rédaction de **user stories** décrivant les attentes de ces personas ;
- la **priorisation** des fonctionnalités selon la méthode MoSCoW (Must / Should / Could / Won't).

Il sert de base de référence pour les phases suivantes : conception technique, implémentation des API et dashboards, mise en place des workflows d'alertes et tests de sécurité.

2 Définition des Personas

Afin de couvrir l'ensemble des cas d'usage, quatre personas principaux ont été identifiés. Ils représentent les profils qui interagiront le plus avec la plateforme.

2.1 Persona 1 : Administrateur Système

Nom	Nicolas Bernard
Âge	37 ans
Fonction	Administrateur Système / Infra
Expérience	12 ans dans l'administration de systèmes et bases de données dans le secteur bancaire
Objectifs principaux	— garantir la disponibilité et la performance des systèmes ; — contrôler les accès aux environnements sensibles ; — anticiper les incidents d'infrastructure.
Besoins	— vision centralisée de l'état des serveurs et services ; — gestion simple des rôles et permissions ; — alertes proactives en cas de dépassement de seuils critiques.
Frustrations	— outils de monitoring dispersés ; — manque de traçabilité sur les changements d'accès ; — découverte tardive de problèmes de performance.

2.2 Persona 2 : Analyste de Sécurité

Nom	Lina Kader
Âge	30 ans
Fonction	Analyste Sécurité / Détection de fraude
Expérience	6 ans en cybersécurité, dont 3 ans sur la lutte contre la fraude bancaire
Objectifs principaux	— repérer rapidement les comportements anormaux ; — qualifier les alertes de fraude ; — réduire les pertes financières liées aux attaques.
Besoins	— tableaux de bord clairs sur les alertes et incidents ; — possibilité de filtrer et prioriser les alertes ; — accès rapide à l'historique des transactions d'un compte.
Frustrations	— trop de faux positifs ; — alertes peu explicables ou mal contextualisées ; — devoir passer par plusieurs outils pour investiguer un cas.

2.3 Persona 3 : Agent du Service Client

Nom	Emma Laurent
Âge	27 ans
Fonction	Conseillère Service Client Digital
Expérience	4 ans en relation client, dont 2 ans sur des services bancaires en ligne
Objectifs principaux	— traiter rapidement les demandes des clients ; — résoudre les problèmes liés aux comptes et cartes ; — rassurer les clients après l'attaque.
Besoins	— moteur de recherche de clients performant ; — vue d'ensemble des comptes et opérations d'un client ; — action simple pour bloquer ou débloquer une carte.
Frustrations	— perte de temps à jongler entre plusieurs écrans ; — manque d'informations pour répondre aux questions des clients ; — dépendance aux équipes techniques pour des actions simples.

2.4 Persona 4 : Client (Consultation limitée)

Nom	Thomas Pereira
Âge	41 ans
Fonction	Entrepreneur, client DigitalBank depuis 5 ans
Expérience	Utilise quotidiennement les services de banque en ligne et l'application mobile
Objectifs principaux	— suivre ses soldes et mouvements ; — être informé en cas d'activité inhabituelle ; — continuer à faire confiance à la banque malgré l'incident.
Besoins	— interface simple pour consulter ses comptes ; — historique clair des transactions ; — notifications en cas de suspicion de fraude.
Frustrations	— inquiétude sur la protection de ses données ; — manque de visibilité sur les mesures de sécurité mises en place ; — difficulté à comprendre certains blocages de carte.

3 User Stories

Les besoins fonctionnels sont exprimés sous forme de *user stories* selon le format : *« En tant que [persona], je veux [action], afin de [bénéfice]. »*

3.1 User Stories – Analyste de Sécurité

US-001 : Vue synthétique des alertes de fraude
En tant qu'analyste de sécurité, je veux voir une liste des alertes de fraude classées par niveau de gravité, afin de traiter en priorité les cas les plus critiques.

US-002 : Visualisation des transactions par zone géographique
En tant qu'analyste de sécurité, je veux visualiser l'origine des transactions sur une carte, afin d'identifier rapidement des zones atypiques ou à risque.

US-003 : Détail d'une transaction suspecte
En tant qu'analyste de sécurité, je veux accéder au détail d'une transaction signalée (montant, horaire, canal, localisation, historique du compte), afin d'évaluer si la fraude est avérée.

US-004 : Indicateurs quotidiens de sécurité
En tant qu'analyste de sécurité, je veux consulter un tableau de bord avec le nombre de transactions, le nombre d'alertes générées et le taux de fraude détectée dans la journée, afin de suivre l'évolution de la situation.

3.2 User Stories – Agent du Service Client

US-005 : Recherche de client multi-critères
En tant qu'agent du service client, je veux rechercher un client par nom, identifiant ou adresse email, afin de le retrouver rapidement lorsqu'il appelle.

US-006 : Fiche client centralisée
En tant qu'agent du service client, je veux voir sur un seul écran les informations principales du client (coordonnées, comptes, cartes actives), afin de pouvoir l'accompagner efficacement.

US-007 : Historique de transactions pour assistance
En tant qu'agent du service client, je veux consulter les dernières transactions d'un client avec les détails associés, afin de l'aider à comprendre une opération ou à contester un paiement.

US-008 : Blocage et déblocage de carte
En tant qu'agent du service client, je veux pouvoir bloquer ou débloquer une carte en quelques clics, afin de protéger le client en cas de suspicion de fraude ou de perte de carte.

3.3 User Stories – Administrateur Système

US-009 : Suivi des ressources techniques
En tant qu'administrateur système, je veux surveiller l'utilisation du CPU, de la mémoire, du stockage et du réseau, afin de détecter toute dégradation de performance.

US-010 : Gestion centralisée des rôles
En tant qu'administrateur système, je veux gérer les rôles et les permissions des utilisateurs via une interface RBAC, afin de limiter l'accès aux données sensibles.

US-011 : Alertes d'infrastructure
En tant qu'administrateur système, je veux recevoir des notifications lorsque certains seuils (par exemple CPU ou espace disque) sont dépassés, afin d'agir avant une panne.

3.4 User Stories – Client

US-012 : Consultation des comptes
En tant que client, je veux consulter le solde de mes comptes et un résumé de mes dernières opérations, afin de suivre mes finances en temps réel.

US-013 : Notification en cas d'activité inhabituelle
En tant que client, je veux être notifié (par email ou SMS) lorsqu'une opération atypique est détectée sur mon compte, afin de pouvoir confirmer ou contester rapidement.

US-014 : Historique détaillé des opérations
En tant que client, je veux pouvoir filtrer mon historique de transactions par période et par type d'opération, afin d'analyser mes dépenses.

4 Priorisation des User Stories (MoSCoW)

La méthode MoSCoW permet de hiérarchiser les fonctionnalités selon quatre niveaux : *Must have*, *Should have*, *Could have*, *Won't have*.

4.1 Must Have (indispensable – MVP)

Ces fonctionnalités sont considérées comme le socle minimal pour une première mise en production de la plateforme.

- US-001 : Vue synthétique des alertes de fraude
- US-003 : Détail d'une transaction suspecte
- US-005 : Recherche de client multi-critères
- US-006 : Fiche client centralisée
- US-007 : Historique de transactions pour assistance
- US-009 : Suivi des ressources techniques
- US-010 : Gestion centralisée des rôles
- US-012 : Consultation des comptes

Justification : ces user stories couvrent les besoins essentiels des trois profils internes (administrateur, analyste, service client) ainsi que la consultation de base pour les clients. Sans elles, la plateforme ne répond pas aux enjeux de sécurité et de continuité de service.

4.2 Should Have (important – version 1.1)

Ces éléments renforcent fortement l'efficacité opérationnelle et la qualité de service, mais peuvent être livrés juste après le MVP.

- US-002 : Visualisation des transactions par zone géographique
- US-004 : Indicateurs quotidiens de sécurité
- US-008 : Blocage et déblocage de carte
- US-011 : Alertes d'infrastructure
- US-013 : Notification en cas d'activité inhabituelle

Justification : ces user stories améliorent la réactivité face aux incidents, la capacité d'investigation et la perception de sécurité du côté client.

4.3 Could Have (souhaitable – version 2.0)

Fonctionnalités apportant une valeur ajoutée mais non critiques pour la reprise post-attaque.

— US-014 : Historique détaillé des opérations (filtres avancés)
— Personnalisation des dashboards par utilisateur
— Export automatique de rapports en PDF
— Intégration d'indicateurs de performance métier (KPI business)

Justification : ces évolutions contribuent à l'analyse fine et au confort d'utilisation, mais peuvent être planifiées dans un second temps.

4.4 Won't Have (hors périmètre actuel)

Fonctionnalités explicitement exclues du périmètre de cette phase de projet.

— Application mobile dédiée à la plateforme interne
— Chatbot de support basé sur l'IA
— Prédiction de churn client ou de valeur vie (LTV)
— Intégration avec des agrégateurs externes de comptes

Justification : ces sujets relèvent d'une roadmap produit de plus long terme et nécessitent des ressources supplémentaires, non compatibles avec le cadrage de l'examen.

5 Synthèse et recommandations

5.1 Résumé de la priorisation

La priorisation aboutit à :

— 8 user stories en **Must Have** (cœur du MVP) ;
— 5 user stories en **Should Have** (version 1.1) ;
— 4 items en **Could Have** (version 2.0) ;
— 4 items en **Won't Have** (hors périmètre).

Cette répartition permet de concentrer les efforts initiaux sur les besoins critiques liés à la sécurité, à la supervision et au support client, tout en laissant une trajectoire d'évolution réaliste.

5.2 Recommandations

— Valider régulièrement les écrans et parcours avec au moins un représentant de chaque persona (administrateur, analyste, service client).
— Mettre en place un canal de remontée de feedback utilisateurs pour ajuster la priorisation des fonctionnalités *Should* et *Could*.
— Documenter systématiquement les décisions de sécurité (RBAC, alertes, seuils) afin de faciliter les audits futurs.
— Privilégier des outils no-code / low-code permettant aux équipes métiers d'ajuster les dashboards sans dépendre systématiquement des développeurs.

5.3 Conclusion

L'analyse des besoins présentée dans ce document fournit un cadre fonctionnel clair pour la conception de la plateforme de gestion et de monitoring de DigitalBank. Les personas, user

stories et priorisation MoSCoW structurent la feuille de route produit et permettront de guider les choix techniques lors des phases suivantes (architecture, implémentation, tests).