

Guide d'utilisation des dashboards

1. Carte du monde des transactions en temps réel

Cette carte affiche en direct l'origine géographique des transactions effectuées.

Elle permet de :

- Visualiser les zones d'activité normales
- Identifier des transactions provenant de pays inhabituels
- Détecter des schémas suspects (ex. : plusieurs transactions rapides depuis différents pays)

C'est un outil clé pour repérer les anomalies géographiques.



2. Top 10 des transactions par montant (aujourd'hui)

Ce module liste les 10 plus grosses transactions du jour.

Il permet de :

- Surveiller les montants élevés
- Détecter des opérations potentiellement frauduleuses
- Prioriser les vérifications manuelles

Les analystes peuvent rapidement repérer les transactions qui sortent de l'ordinaire.

3. Alertes de fraude

Cette section affiche les transactions suspectes identifiées par le système de détection.

Chaque alerte contient :

- Le détail de la transaction
- Le score de risque (ex. : faible, moyen, élevé)
- Le motif de suspicion (ex. : localisation inhabituelle, montant anormal, comportement atypique)

L'analyste peut ainsi décider :

- De bloquer la carte

- De contacter le client
- De lancer une investigation

B. Dashboard Service Client

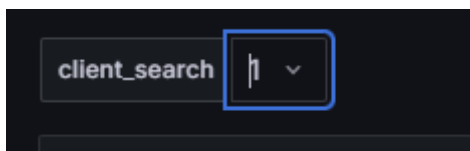
Le dashboard *Service Client* permet aux équipes de support de consulter rapidement les informations essentielles d'un client, d'analyser son activité récente et d'agir en cas de suspicion de fraude. Il centralise toutes les données nécessaires pour un traitement efficace et sécurisé.

1. Recherche client

Ce module permet d'identifier un client à partir de plusieurs critères :

- Nom / Prénom
- Adresse email
- Numéro de compte

L'utilisateur saisit un des champs, et le dashboard filtre automatiquement les données associées au client correspondant.

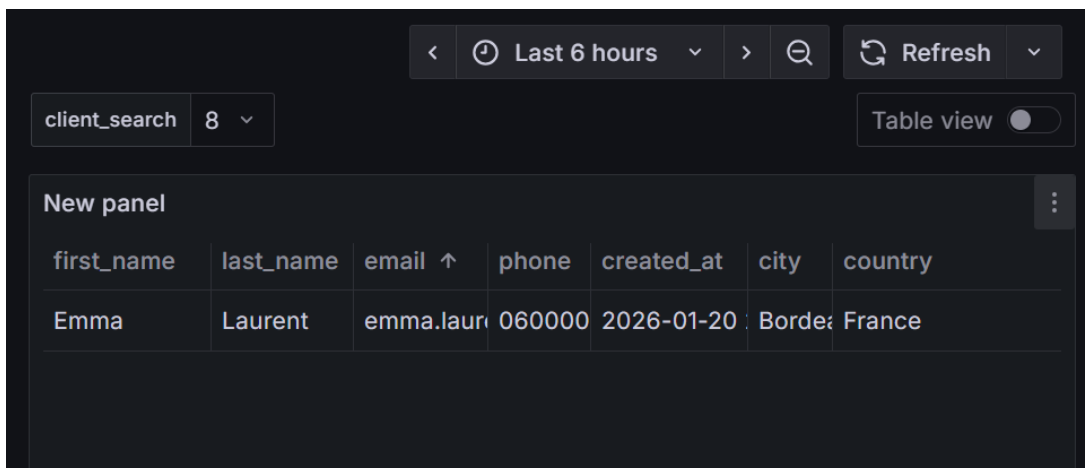


2. Détails du client

Une fois le client sélectionné, le dashboard affiche ses informations personnelles :

- Nom et prénom, Email, Numéro de téléphone, Date d'inscription

Ces données permettent de vérifier l'identité du client et de contextualiser son historique.



Par exemple ici on a pris choisi ce client (client_id=8)

3. Liste des comptes du client

Le dashboard présente l'ensemble des comptes associés au client, avec pour chacun :

- Type de compte, Solde actuel, Statut

Cela permet d'avoir une vision globale de la situation financière du client.

client_search8

Table view

New panel			
account_id	account_type	balance	status
11	checking	1200	active

4. Historique des 20 dernières transactions

Cette section affiche les opérations les plus récentes :

- Montant, Catégorie marchande, Date, Numéro de transaction, Type (dépense, revenu)

Elle est essentielle pour détecter des comportements inhabituels ou des transactions suspectes.

client_search1

Table view

New panel			
transaction_id	account_id	amount	merchant_category
36	1	6000	Luxury
35	1	6000	Luxury
11	1	-12.5	Food & Beverage
16	1	-2500	Electronics
2	1	-120	Travel

5. Bouton Bloquer / Débloquer une carte

En cas de fraude ou de suspicion :

- Le bouton **Bloquer la carte** permet de désactiver immédiatement la carte du client.
- Le bouton **Débloquer la carte** permet de la réactiver une fois la situation clarifiée.

Ce composant est crucial pour la sécurité et la réactivité du service client.

C. Dashboard Monitoring Infrastructure

Le dashboard *Monitoring Infrastructure* permet de surveiller en temps réel l'état des systèmes, la performance des services et la santé globale de l'infrastructure.

1. Métriques système

Le dashboard affiche les indicateurs clés :

- **CPU** : charge processeur
- **RAM** : mémoire utilisée
- **Disque** : espace et activité disque
- **Network** : trafic réseau (entrant/sortant)

Ces métriques permettent de détecter les surcharges, saturations ou anomalies matérielles.

Exemple : CPU



2. Temps de réponse API

Le dashboard présente :

- **Latence moyenne**
- **p95** (95 % des requêtes sont plus rapides que cette valeur)
- **p99** (99 % des requêtes sont plus rapides que cette valeur)

Ces indicateurs permettent d'évaluer la performance réelle du service et d'identifier les ralentissements.

3. Taux d'erreur

Affiche le pourcentage de requêtes ayant échoué. Un taux élevé peut indiquer :

- Un bug applicatif
- Une surcharge serveur
- Un problème réseau
- Une dépendance externe défaillante

4. Nombre de requêtes par minute

Permet de suivre la charge du système et d'identifier :

- Les pics d'activité

- Les périodes creuses
- Les comportements anormaux (ex. : attaque, surcharge)

5. Alertes système

Liste des alertes actives générées par les règles de monitoring :

- CPU trop élevé
- Latence API anormale
- Taux d'erreur critique
- Disque presque plein

Cette section permet une réaction rapide pour éviter les incidents.