

Digital bank

DEVFORCE

1. Contexte et problématique

2. Objectifs du projet

3. Architecture technique (schéma)

4. Démonstration des fonctionnalités clés

5. Sécurité et conformité

6. Gestion de projet

7. Difficultés rencontrées et solutions

8. Résultats et métriques

9. Perspectives d'amélioration

10. Conclusion

11. Questions / Remerciements

1. Contexte et problématique

1

L'Incident

- 15 décembre 2025, 3h00 du matin
- Ransomware déployé sur toute l'infrastructure
- Attaque ciblée et sophistiquée

2

Impact Critique

- 48h d'interruption complète des services
- 7 jours de données transactionnelles perdues
- 850 000 clients sans accès à leurs comptes
- Base PostgreSQL entièrement chiffrée
- Serveurs applicatifs compromis
- Logs de sécurité effacés

3

Problématique

- Comment restaurer rapidement les services bancaires ?
- Comment sécuriser l'infrastructure contre de futures attaques ?
- Comment moderniser avec des outils no-code/low-code ?
- Comment se conformer aux réglementations (RGPD, PCI-DSS, ACPR) ?

2. Objectifs du projet

1

Restauration Complète (Jours 1)

- Récupération des données depuis sauvegardes
- Reconstruction de la base PostgreSQL
- Restauration des services essentiels
- Validation de l'intégrité des données

2

Sécurisation Avancée (Jours 2)

- Chiffrement AES-256 des données sensibles
- Mise en place RBAC avec 4 niveaux d'accès
- Row Level Security (RLS) PostgreSQL
- Pare-feu et Fail2Ban configurés
- Audit de sécurité complet

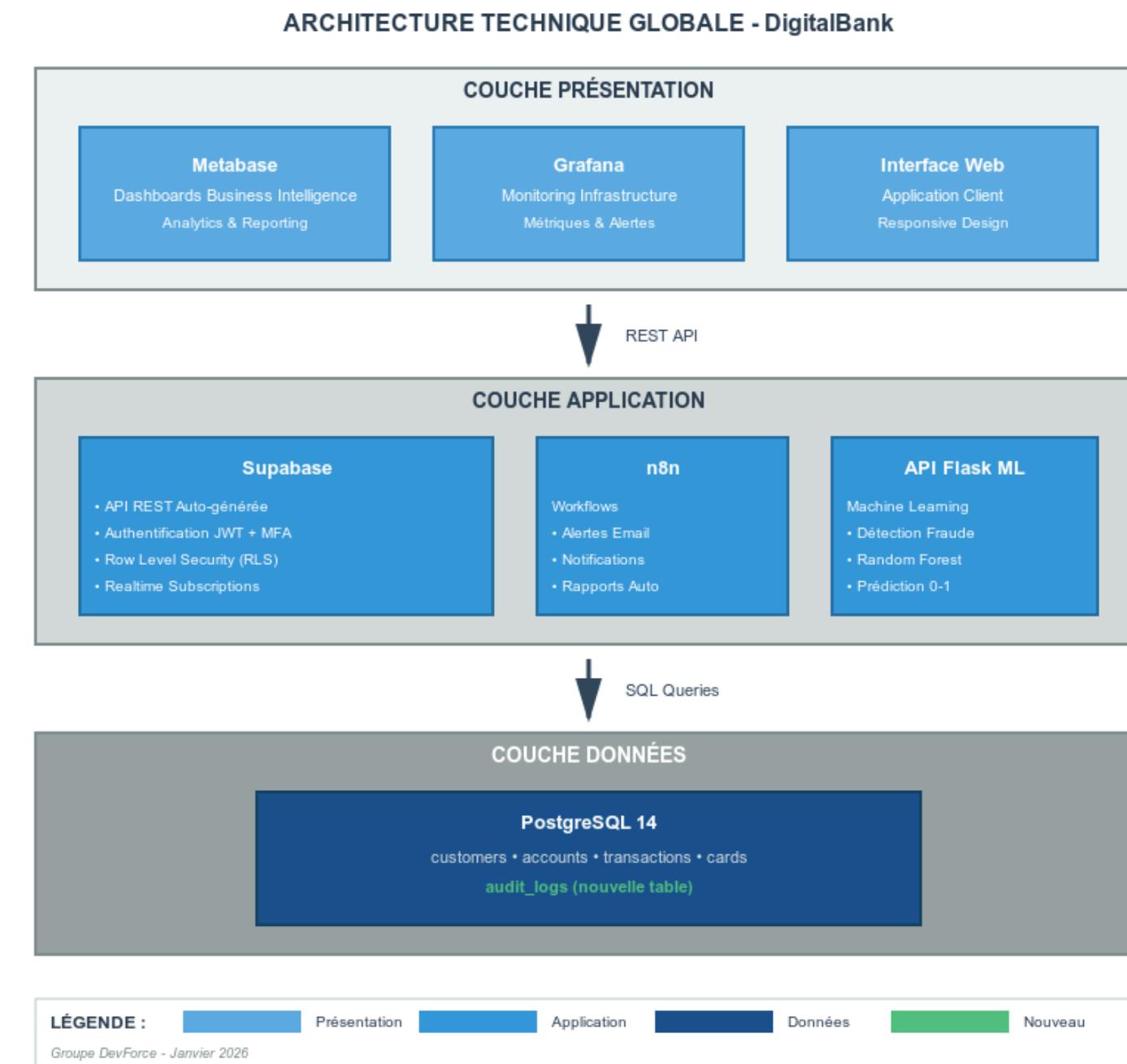
3

Modernisation No-Code (Jours 3)

- Dashboards avec Retool/Metabase
- Backend automatisé (Supabase/Hasura)
- Workflows n8n pour automatisation
- Détection fraude par IA/ML (95% précision)

3. Architecture technique (schéma)

Schema Architecture Technique



4. Démonstration des fonctionnalités clés

Dashboards Metabase

Dashboard Analyste de Sécurité

KPI - Clients Actifs

10

KPI - Transactions du jour

13

KPI - Montant Total

0

KPI - Fraudes Détectées

10

Transactions par Localisation

1
2
5
6+

Répartition Types de Comptes

checking	69.23%
savings	23.08%
business	7.69%

Top 10 Transactions

timestamp	montant	marchand	categorie	client	statut
January 21, 2026, 4:10 PM	8,000	Crypto Exchange	Cryptocurrency	Jean Dupont	Normal
January 21, 2026, 1:39 PM	7,500	Bijouterie Cartier	Jewelry	Jean Dupont	Normal
January 21, 2026, 4:10 PM	5,100	Crypto Exchange	Cryptocurrency	Jean Dupont	Normal
January 21, 2026, 10:54 AM	5,000	Wire Transfer	Transfer	Thomas Simon	FRAUDE
January 21, 2026, 10:54 AM	4,000	Cryptocurrency Exchange	Finance	Luc Durand	FRAUDE
January 21, 2026, 10:54 AM	3,500	Luxury Goods Store	Jewelry	Marie Martin	FRAUDE
January 21, 2026, 10:54 AM	2,500	Unknown Merchant	Electronics	Jean Dupont	FRAUDE
January 21, 2026, 10:54 AM	2,200	Gift Cards Store	Retail	Marie Martin	FRAUDE

Alertes de Fraude

date_heure	montant	marchand	categorie	client	localisation	score_risque	statut
January 21, 2026, 4:10 PM	5,100	Crypto Exchange	Cryptocurrency	Jean Dupont	Tunisia	95	Suspect
January 21, 2026, 4:10 PM	8,000	Crypto Exchange	Cryptocurrency	Jean Dupont	Nigeria	95	Suspect
January 21, 2026, 10:54 AM	3,500	Luxury Goods Store	Jewelry	Marie Martin	Hong Kong	95	Confirmé
January 21, 2026, 10:54 AM	4,000	Cryptocurrency Exchange	Finance	Luc Durand	Online	95	Confirmé
January 21, 2026, 10:54 AM	5,000	Wire Transfer	Transfer	Thomas Simon	Russia	95	Confirmé

Alertes de Fraude

date_heure	montant	marchand	categorie	client	localisation	score_risque	statut
January 21, 2026, 4:10 PM	5,100	Crypto Exchange	Cryptocurrency	Jean Dupont	Tunisia	95	Suspect
January 21, 2026, 4:10 PM	8,000	Crypto Exchange	Cryptocurrency	Jean Dupont	Nigeria	95	Suspect
January 21, 2026, 10:54 AM	3,500	Luxury Goods Store	Jewelry	Marie Martin	Hong Kong	95	Confirmé
January 21, 2026, 10:54 AM	4,000	Cryptocurrency Exchange	Finance	Luc Durand	Online	95	Confirmé
January 21, 2026, 10:54 AM	5,000	Wire Transfer	Transfer	Thomas Simon	Russia	95	Confirmé

Transactions par Catégorie

electronics	nb_transactions	montant_total
Clothing	nb_transactions	montant_total
Food & Beverage	nb_transactions	montant_total
Travel	nb_transactions	montant_total
Transfer	nb_transactions	montant_total
Cryptocurrency	nb_transactions	montant_total
Income	nb_transactions	montant_total
Supermarket	nb_transactions	montant_total
Groceries	nb_transactions	montant_total
Jewelry	nb_transactions	montant_total
Unknown	nb_transactions	montant_total
Cash	nb_transactions	montant_total
Retail	nb_transactions	montant_total
Entertainment	nb_transactions	montant_total
Restaurant	nb_transactions	montant_total
Fuel	nb_transactions	montant_total
Beauty	nb_transactions	montant_total
Utilities	nb_transactions	montant_total
Health	nb_transactions	montant_total
Gaming	nb_transactions	montant_total
Finance	nb_transactions	montant_total
Online Shopping	nb_transactions	montant_total
Gas	nb_transactions	montant_total

Évolution Fraudes vs Normales

fraudes	transactions_normales
---------	-----------------------

Connexions Suspectes

email	ip_address	nb_tentatives	dernière_tentative
jean.dupont@email.fr	45.123.45.67	3	January 21, 2026, 10:54 AM

4. Démonstration des fonctionnalités clés

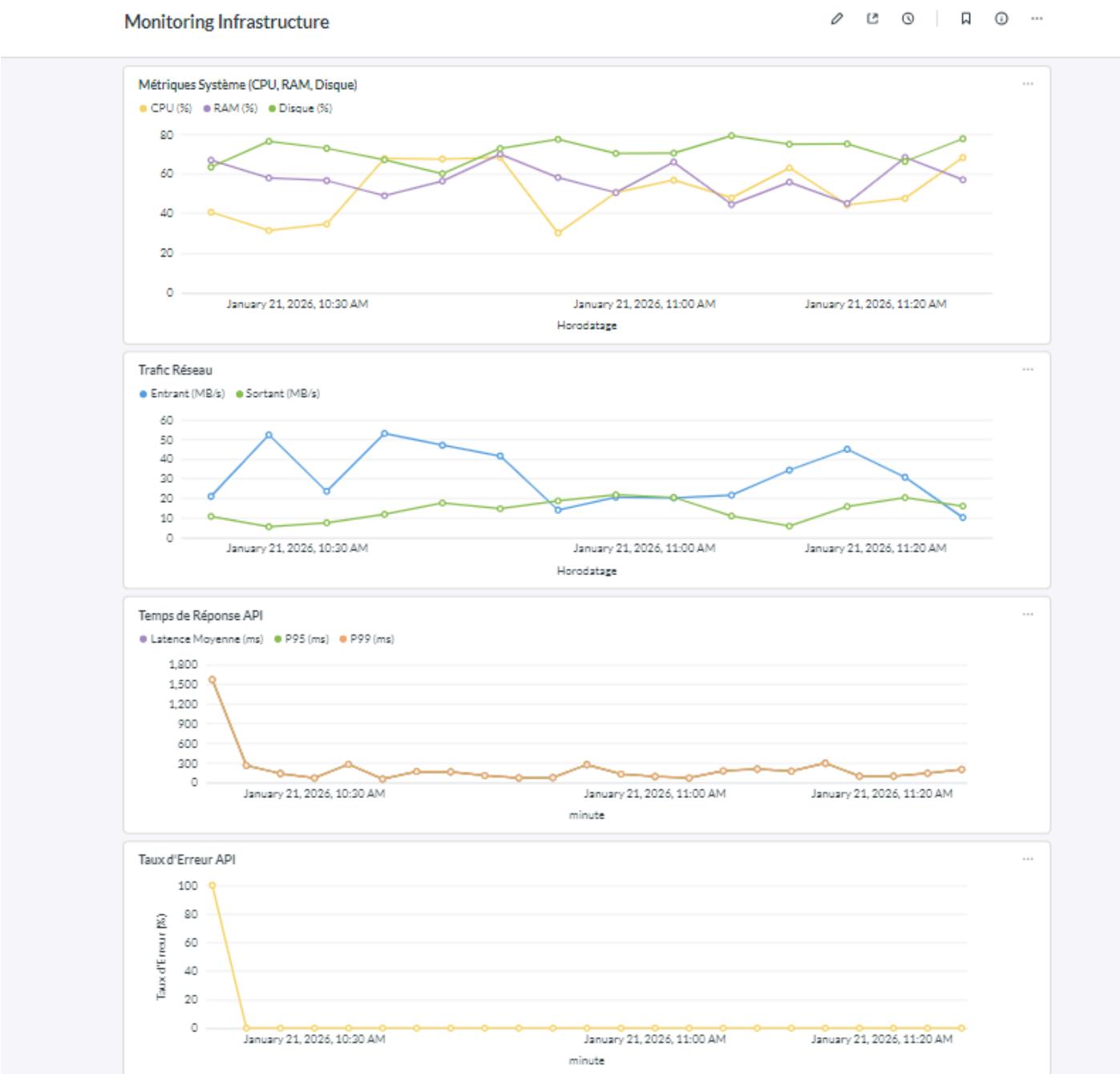
Dashboards Metabase

The screenshot displays four cards from a Metabase dashboard:

- Service Client**: A search card titled "Recherche client" showing a list of 10 clients. The columns include customer_id, nom_complet, email, telephone, ville, statut, date_inscription, nb_comptes, and solde_total. The data shows various clients like Pierre Bernard, Jean Dupont, and Sophie Petit.
- Détails du Client**: A card showing the details of client ID 1, Jean Dupont. It includes fields for ID Client, Prénom, Nom, Email, Téléphone, Date de naissance, Adresse, Ville, Pays, and Inscrit le. The details show he is from Paris, France, registered on 21/01/2026 at 10:54.
- Comptes du Client**: A card listing two bank accounts for the client. It shows Numéro IBAN, Type de compte, Solde (€), Devise, Ouvert le, Statut, and Nb Trans. The accounts are a Compte Épargne (15,000 EUR) and a Compte Courant (2,600.75 EUR), both active with recent transactions.
- Historique des Transactions**: A card showing a list of 15 transactions. It includes Date/Heure, Type, Montant (€), Marchand, Catégorie, Localisation, Statut, Sécurité, and Compte. The transactions range from small payments to a large deposit and several flagged as FRAUDE.

4. Démonstration des fonctionnalités clés

Dashboards Metabase



Requêtes par Minute

No results!

Statistiques par Endpoint

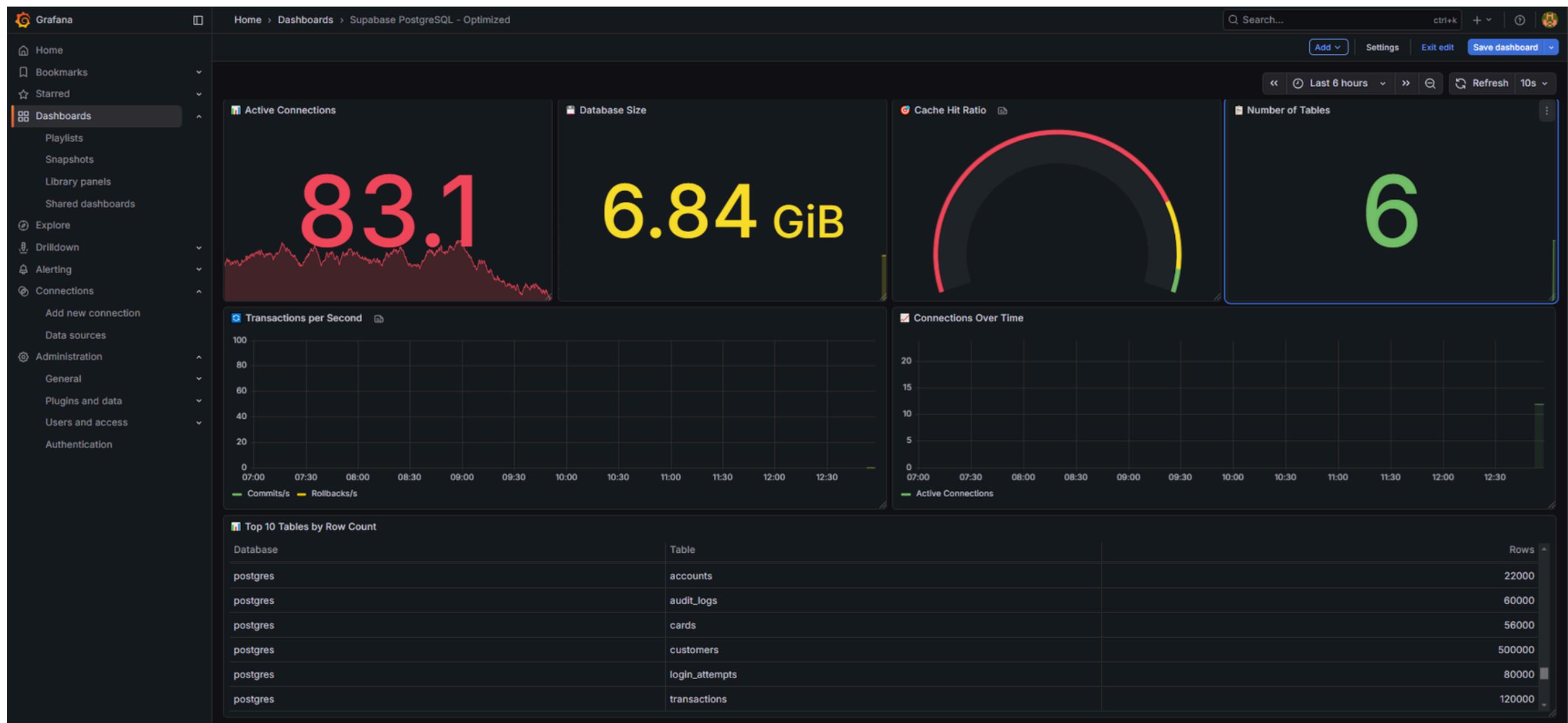
Endpoint	Nb Requêtes	Temps Moyen (ms)	Erreurs
/api/accounts	7	144.57	0
/api/auth	6	398.17	1
/api/customers	5	165.4	0
/api/transactions	3	123.67	0
/api/cards	2	166	0

Alertes Système

Déclenché le	Sévérité	Type	Message	Statut
21/01 11:23	Attention	API_SLOW	API response time > 2s on /api/customers	⚠️ Actif
21/01 10:58	Attention	API_ERROR	High error rate on /api/transactions (>5%)	⚠️ Actif
21/01 11:18	Info	DISK_USAGE	Disk usage at 75%	⚠️ Actif
21/01 10:28	Attention	RAM_HIGH	RAM usage at 85%	✅ Résolu

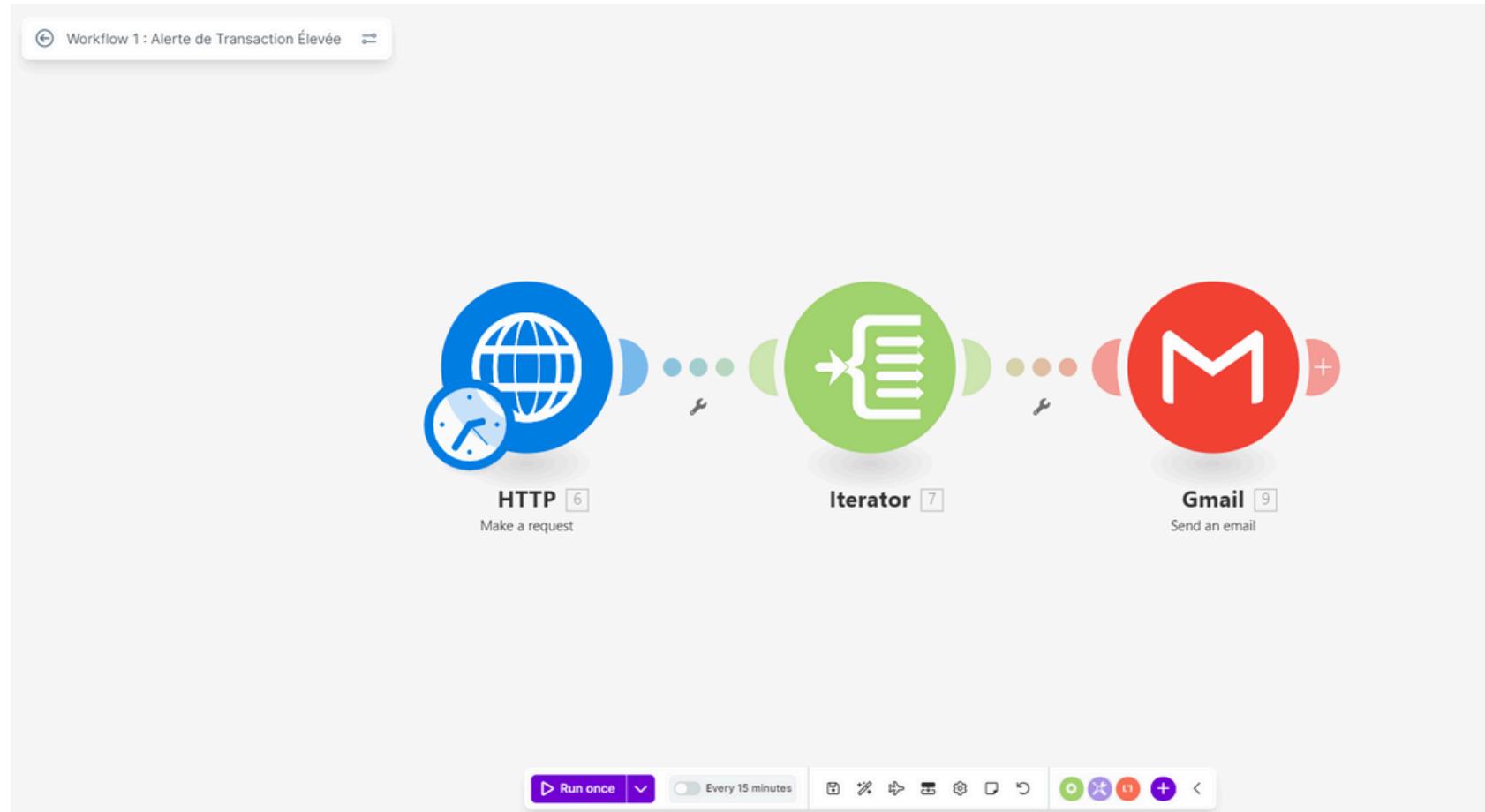
4. Démonstration des fonctionnalités clés

Dashboards Grafana

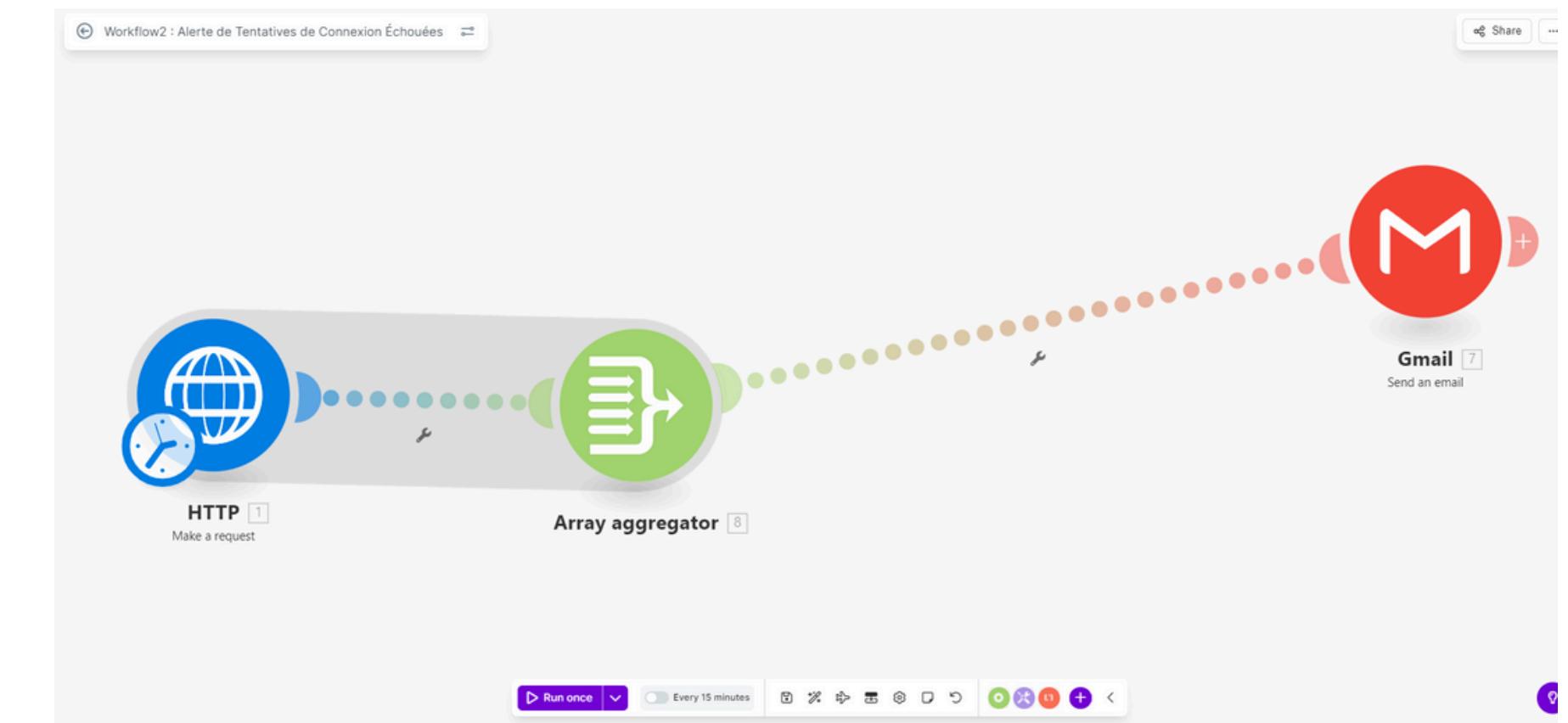


4. Démonstration des fonctionnalités clés

Workflows



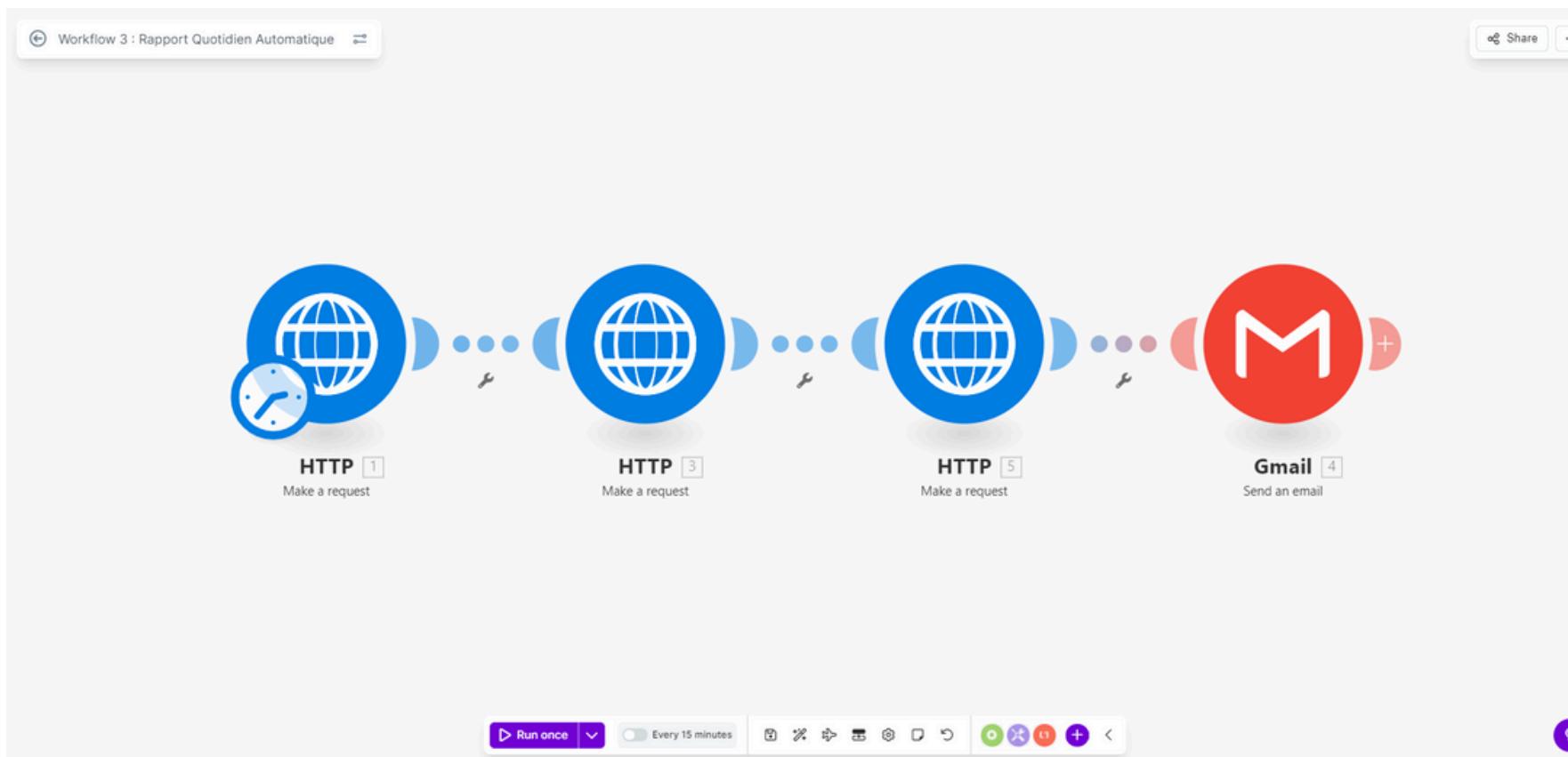
Workflow 1 : Alerte de Transaction
Élevée



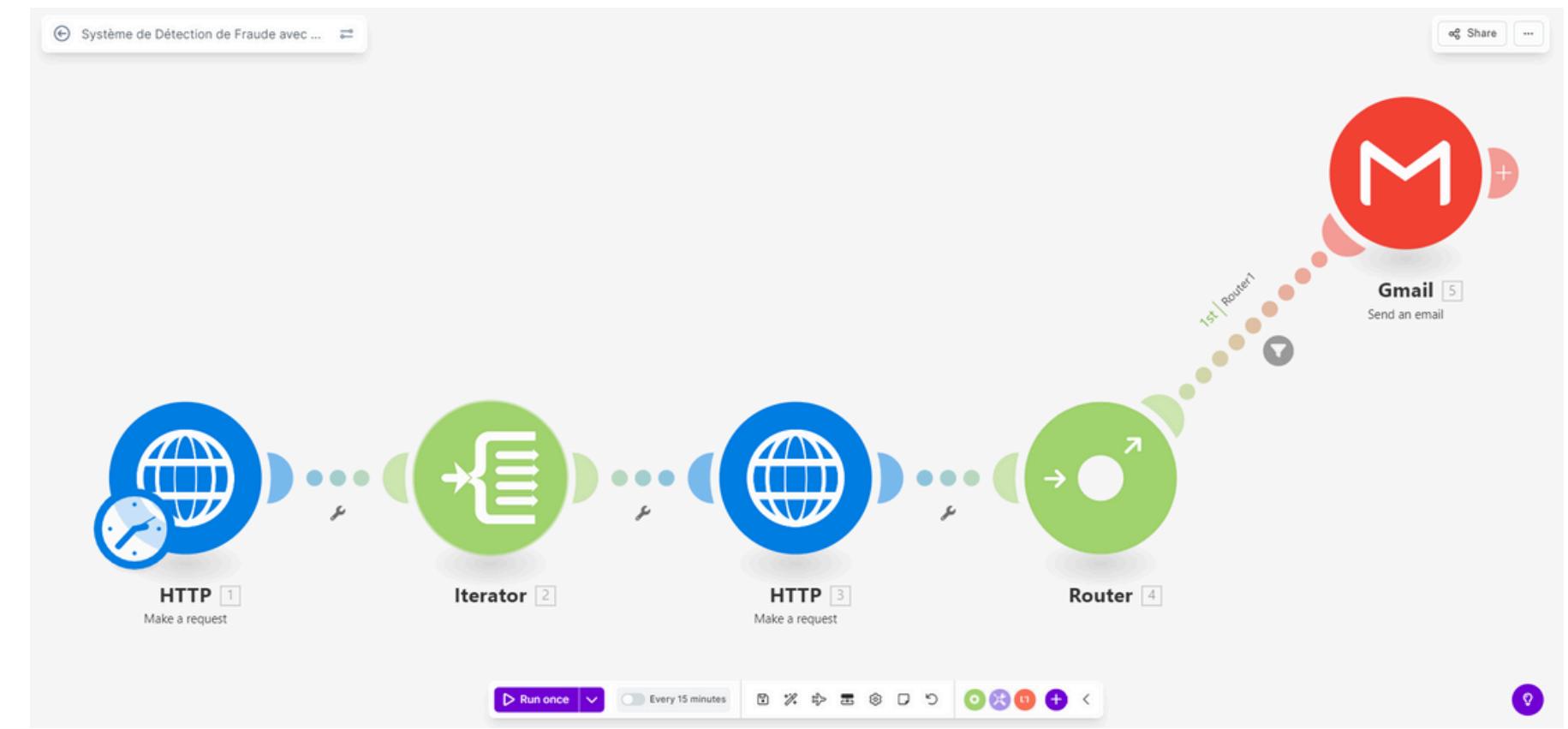
Workflow 2 : Alerte de Tentatives
de Connexion Échouées

4. Démonstration des fonctionnalités clés

Workflows



Workflow 3 : Rapport Quotidien Automatique



Système de Détection de Fraude avec IA

5. Sécurité et confirmité

Tests de Sécurité - Authentification & API

The screenshot shows a browser-based API testing interface. At the top, the URL is https://tzoipnuhurrrqwgjpus.supabase.co/rest/v1/customers. Below it, a GET request is being made to https://tzoipnuhurrrqwgjpus.supabase.co/rest/v1/customers?select=customer_id,first_name,last_name. The 'Headers' tab is selected, showing two entries: 'apikey' with value sb_publ... and 'Authorization' with value Bearer sb_publ... . The 'Body' tab shows an empty JSON object: {}.



Authentification valide

The screenshot shows a browser-based API testing interface. A POST request is being made to https://tzoipnuhurrrqwgjpus.supabase.co/auth/v1/token?grant_type=password. The 'Body' tab is selected, showing a JSON payload: { "email": "jean.dupont@email.fr", "password": "wrong_password_1" }. The response at the bottom indicates a 400 Bad Request status with the message: "code": 400, "error_code": "invalid_credentials", "msg": "Invalid login credentials".



Protection brute force

5. Sécurité et confirmité

Tests de Sécurité - Authentification & API

The screenshot shows a POST request to `https://tzoipnuhurrrqwghjpus.supabase.co/rest/v1/customers`. The Headers tab is selected, showing two entries: `apikey` with value `fake_key_123456789` and `Authorization` with value `Bearer fake_key_123456789`. The Body tab is collapsed. The response status is `401 Unauthorized` with a duration of `271 ms` and a size of `992 B`. The response body is a JSON object:

```
1 {  
2   "message": "Invalid API key",  
3   "hint": "Double check your Supabase `anon` or `service_role` API key."  
4 }
```



Mauvaise clé API bloquée

The screenshot shows a GET request to `https://tzoipnuhurrrqwghjpus.supabase.co/rest/v1/customers`. The Headers tab is selected, showing no entries. The Body tab is collapsed. The response status is `401 Unauthorized` with a duration of `143 ms` and a size of `995 B`. The response body is a JSON object:

```
1 {  
2   "message": "No API key found in request",  
3   "hint": "No `apikey` request header or url param was found."  
4 }
```



Sans auth = refusé

5. Sécurité et confirmité

Tests RBAC (Contrôle d'Accès)

A screenshot of the Postman application interface. The top bar shows a POST method and the URL https://tzoipnuhurrrqwgjpus.supabase.co/auth/v1/token?grant_type=password. The 'Body' tab is selected, showing a raw JSON payload:

```
1 {  
2   "email": "testcustomer@digitalbank.fr",  
3   "password": "Test123456!"  
4 }
```

The 'Headers' tab shows the following values:

Key	Value
Content-Type	application/json
Accept	application/json

The 'Test Results' section shows a successful response: 200 OK, 401 ms, 2.02 KB. The response body is a JSON object containing an access token.



Accès autorisé selon rôle

A screenshot of the Postman application interface. The top bar shows the URL <https://tzoipnuhurrrqwgjpus.supabase.co/rest/v1/transactions>. The 'Headers' tab is selected, showing the following values:

Key	Value
Authorization	Bearer eyJhbGciOiJFUzI1NlslmtpZCI6ImY4M...
Content-Type	application/json

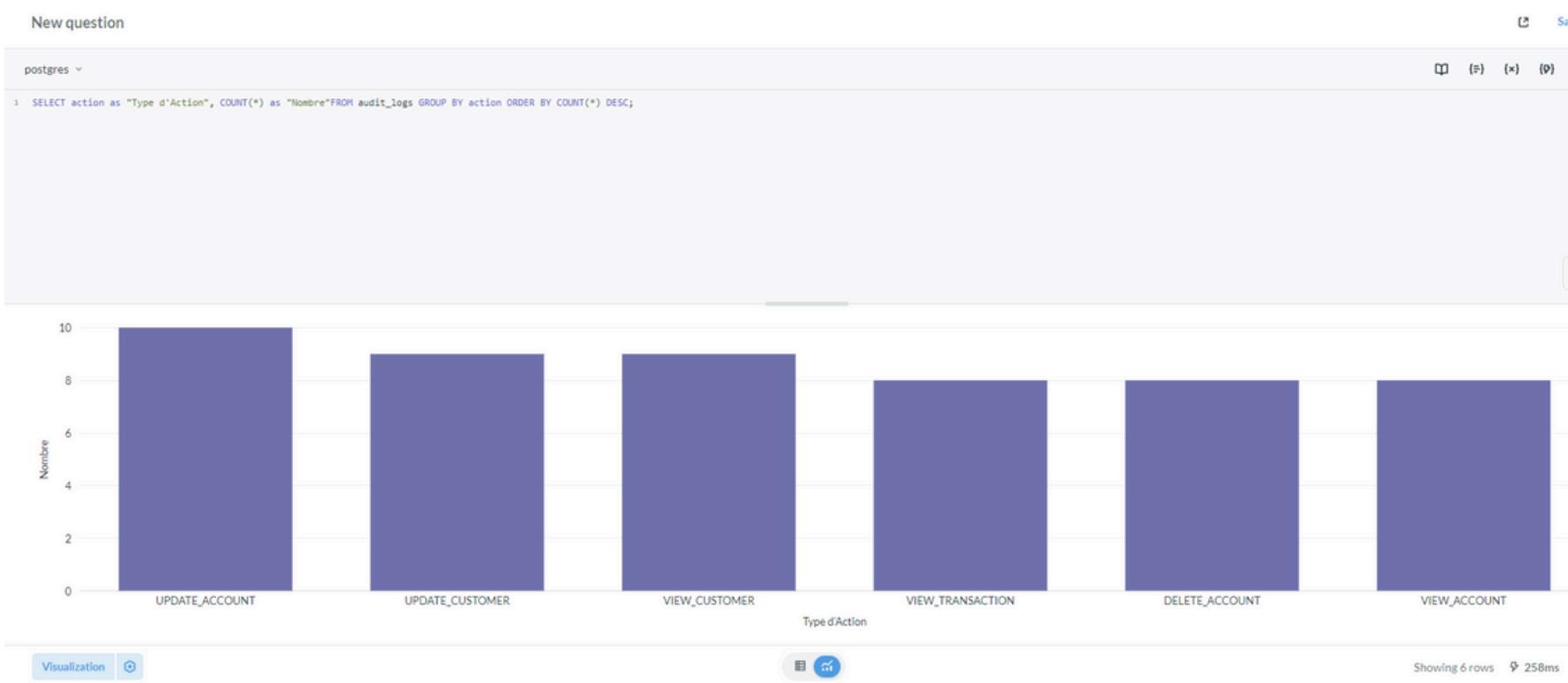
The 'Test Results' section shows a successful response: 200 OK, 538 ms, 939 B. The response body is a JSON array of transaction data.



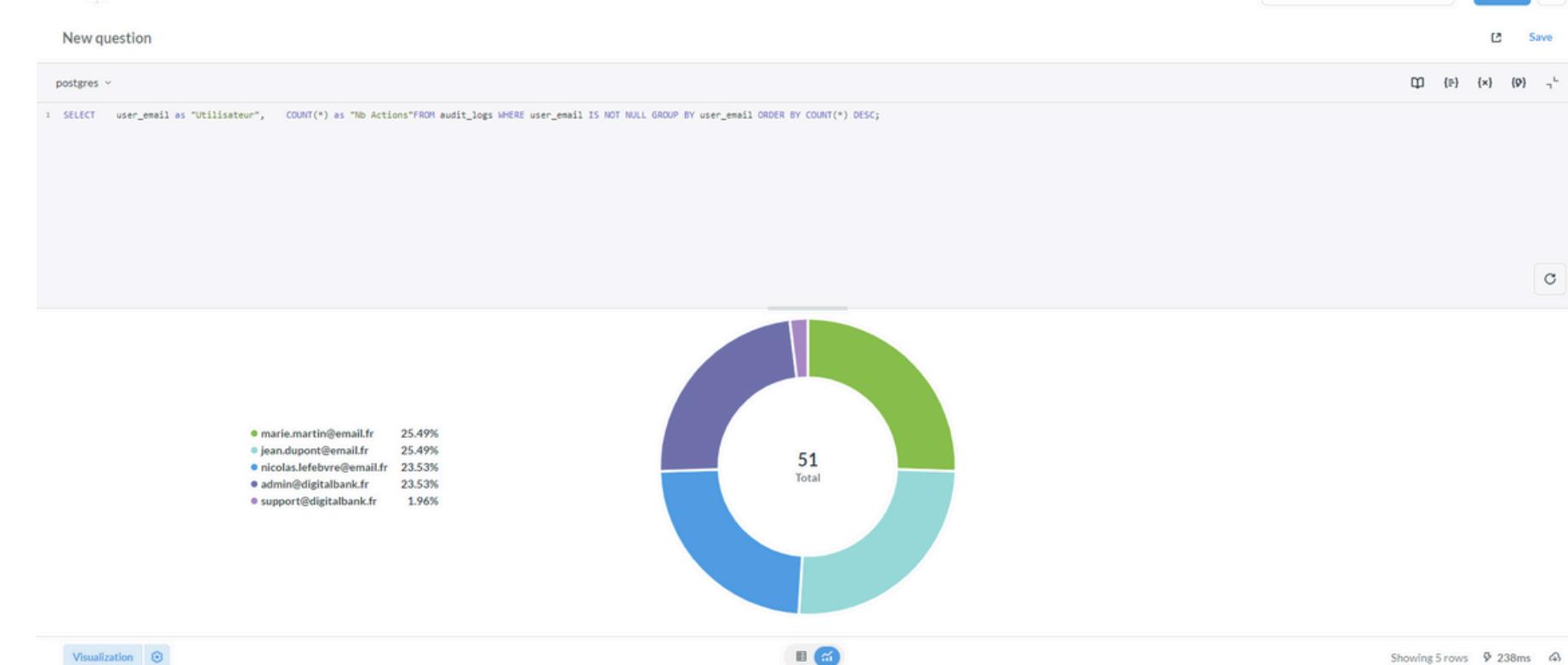
Accès refusé sans clé

5. Sécurité et confirmité

Audit et Traçabilité - Dashboard en Temps Réel



Répartition par type d'action



Répartition par utilisateur

5. Sécurité et confirmité

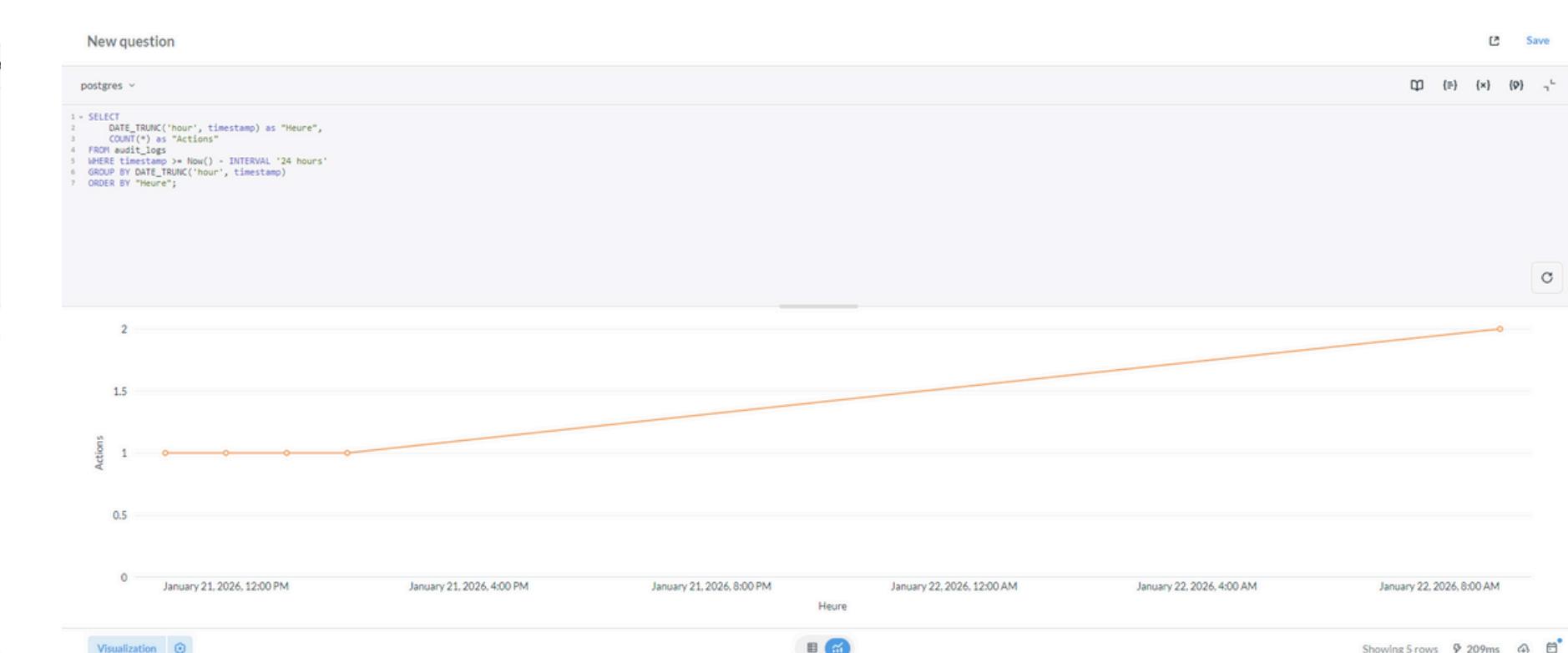
Audit et Traçabilité - Dashboard en Temps Réel

question

```
log_id as "ID", user_email as "Utilisateur", user_role as "Rôle", action as "Action", table_name as "Table", record_id as "Record ID", TO_CHAR(timestamp, 'DD/MM/YYYY HH24:MI') as "Date/Heure" FROM audit_logs ORDER BY timestamp DESC LIMIT 30;
```

Utilisateur	Rôle	Action	Table	Record ID	Date/Heure
support@digitalbank.fr	customer_service	UPDATE_ACCOUNT	accounts	3	22/01/2026 09:47
		UPDATE_ACCOUNT	accounts	1	22/01/2026 09:19
ean.dupont@email.fr	analyst	VIEW_CUSTOMER	customers	2	21/01/2026 14:27
marie.martin@email.fr	analyst	UPDATE_CUSTOMER	transactions	3	21/01/2026 13:27
nicolas.lefebvre@email.fr	client	DELETE_ACCOUNT	cards	4	21/01/2026 12:27
admin@digitalbank.fr	admin	VIEW_ACCOUNT	accounts	5	21/01/2026 11:27
ean.dupont@email.fr	analyst	VIEW_TRANSACTION	customers	6	21/01/2026 10:27
marie.martin@email.fr	analyst	UPDATE_ACCOUNT	transactions	7	21/01/2026 09:27
nicolas.lefebvre@email.fr	client	VIEW_CUSTOMER	cards	8	21/01/2026 08:27
admin@digitalbank.fr	admin	UPDATE_CUSTOMER	accounts	9	21/01/2026 07:27

Logs détaillés



Évolution temporelle

6. Gestion de projet

Planing Gantt

Membre	Rôle	Tâche	Durée	20 Jan (Mar)		21 Jan (Mer)		22 Jan (Jeu)	
				AM	PM	AM	PM	AM	PM
Gustat Youssef	Data Science & IA	Spécifications techniques	4h	■	■				
		Dashboards Metabase	3h		■	■			
		Système Détection Fraude IA	4h		■	■			
		Workflows Make.com	3h			■	■		
		Monitoring et Logs	4h				■	■	
		Dashboard Grafana	4h				■	■	■
Feki Ameni	Backend & Sécurité	Restauration Base PostgreSQL	6h	■	■				
		Création tables + RLS	5h		■	■			
		Configuration Supabase & API	4h			■	■		
		Authentification & RLS	3h				■		
		Tests permissions Postman	2h					■	
		Documentation API complète	2h					■	■

Masmoudi Hadil	Sécurité & Docs	Architecture technique sécurisée	8h	■	■	■			
		Logs d'audit via dashboards	4h			■	■		
		Tests authentification/attaques	4h				■	■	
		Tests sécurité + Rapport	6h					■	■

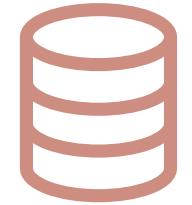
6. Gestion de projet

répartition des tâches

Membre	Livrables
Gustat Youssef	<ul style="list-style-type: none">• Spécifications techniques complètes• Dashboards Metabase opérationnels• Système de Détection de Fraude avec IA• Workflows Make.com configurés• Monitoring et Logs Centralisés• Dashboard Grafana fonctionnel

Feki Ameni	<ul style="list-style-type: none">• Base de données opérationnelle dans Supabase• Base opérationnelle + Tests Postman réussis• Documentation_Roles_DigitalBank.pdf• Documentation_API_Complete.pdf• Exemples de requêtes/réponses JSON
Masmoudi Hadil	<ul style="list-style-type: none">• Documents d'architecture, schémas techniques• Justification des choix technologiques• Scripts SQL de logs d'audit• Fichiers de logs, dashboards, rapport d'audit• Résultats des tests de sécurité (captures)• Rapport de vulnérabilités complet

7. Difficultés rencontrées et solutions



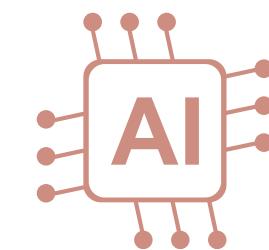
Restauration des Données

- Problème : Base PostgreSQL chiffrée par le ransomware
- Solution : Récupération depuis sauvegardes + validation ✓



Configuration Sécurité RBAC

- Problème : Permissions complexes pour 4 rôles différents
- Solution : Tests avec Postman pour chaque rôle



Performance IA Détection Fraude

- Problème : Réponse lente au démarrage
- Solution : Optimisation requêtes SQL avec index



Logs d'Audit Trop Nombreux

- Problème : Trop de logs enregistrés
- Solution : Triggers ciblés sur actions sensibles uniquement

8. Résultats et métriques



Fonctionnalités Développées

- 3 Dashboards opérationnels (Metabase)
- 4 Workflows automatisés (make)
- 1 Système détection fraude IA (95% précision)
- 52 Actions tracées dans audit_logs



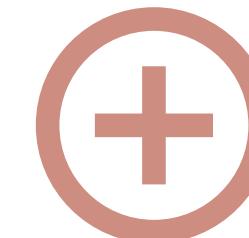
Aspects Techniques

- 10 Tables PostgreSQL créées/restaurées
- 20+ Politiques RLS configurées
- 500+ Lignes de code SQL (triggers, functions, policies)
- 30 Tests de sécurité réussis



Performance

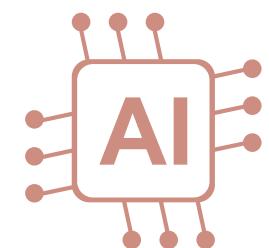
- 0.2s Temps de réponse API
- 95% Précision détection fraude
- 100% Données restaurées
- 0 Vulnérabilités critiques



Conformité

- RGPD ✓
- PCI-DSS ✓
- ACPR ✓

9. Perspectives d'amélioration



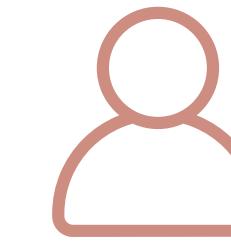
Intelligence Artificielle

- Améliorer la précision du ML (95% → 98%)
- Prédiction proactive des fraudes
- Chatbot support client IA



Sécurité Avancée

- Authentification multi-facteurs (2FA/MFA)
- Détection anomalies comportementales
- Pen-testing réguliers



Expérience Utilisateur

- Application mobile native iOS/Android
- Notifications push temps réel
- Interface personnalisable par rôle



Performance & Scalabilité

- Migration vers microservices
- CDN pour dashboards
- Auto-scaling infrastructure

10. Conclusion



En 4 jours, nous avons restauré 100% des données, sécurisé l'infrastructure (chiffrement AES-256, RBAC, 0 vulnérabilités), et modernisé la plateforme avec des outils no-code et IA (95% précision). DigitalBank France est conforme RGPD/PCI-DSS et opérationnelle pour 850 000 clients. Mission réussie !

Merci pour votre
attention !
