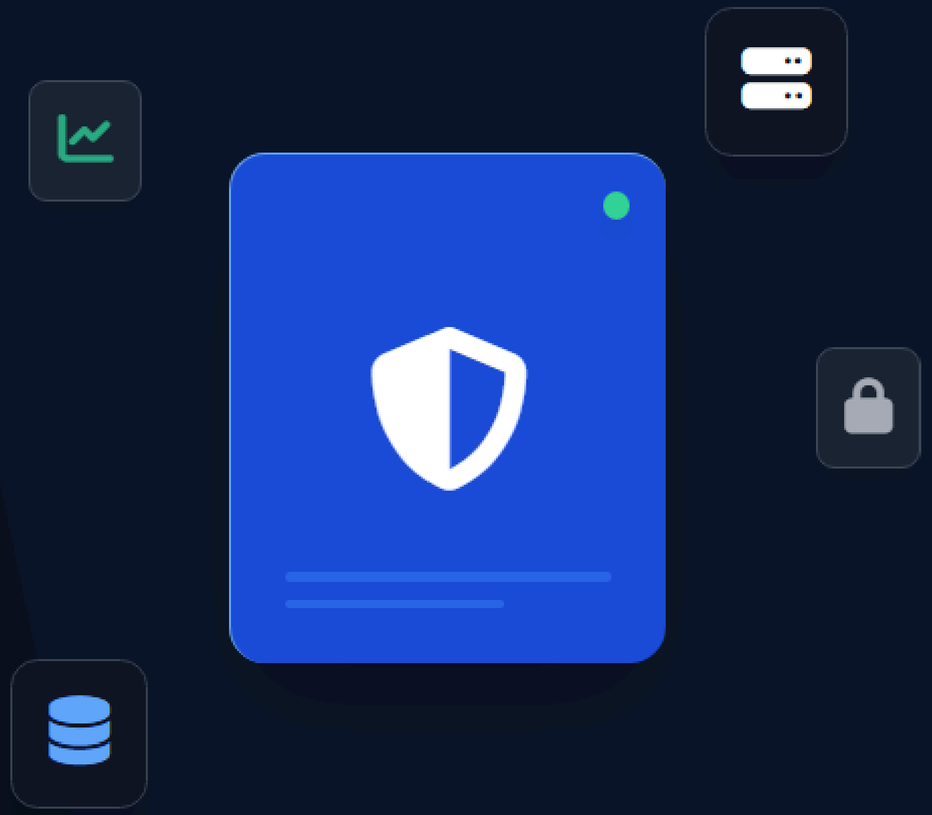
ESIC 2026

Projet de Monitoring & Sécurité des SI



GROUPE

TRIO INFERNAL

FORMATION

Master – Systèmes d'Information & Cybersécurité

VUE D'ENSEMBLE

Sommaire

Projet: DigitalBank

01 INTRODUCTION

Contexte et Problématique

LE CONTEXTE

Les entreprises modernes exploitent des **infrastructures informatiques complexes** générant un volume important de données.

- Logs applicatifs
- Métriques système (CPU, RAM)
- Événements temps réel

LA PROBLÉMATIQUE

Manque de visibilité

Impossible de visualiser l'état du système en temps réel.

Analyse complexe

Logs dispersés rendant l'analyse manuelle difficile.

Détection tardive

Réactivité insuffisante face aux incidents critiques.

Risques de sécurité

Vulnérabilités non détectées et traçabilité limitée.

02 VISION

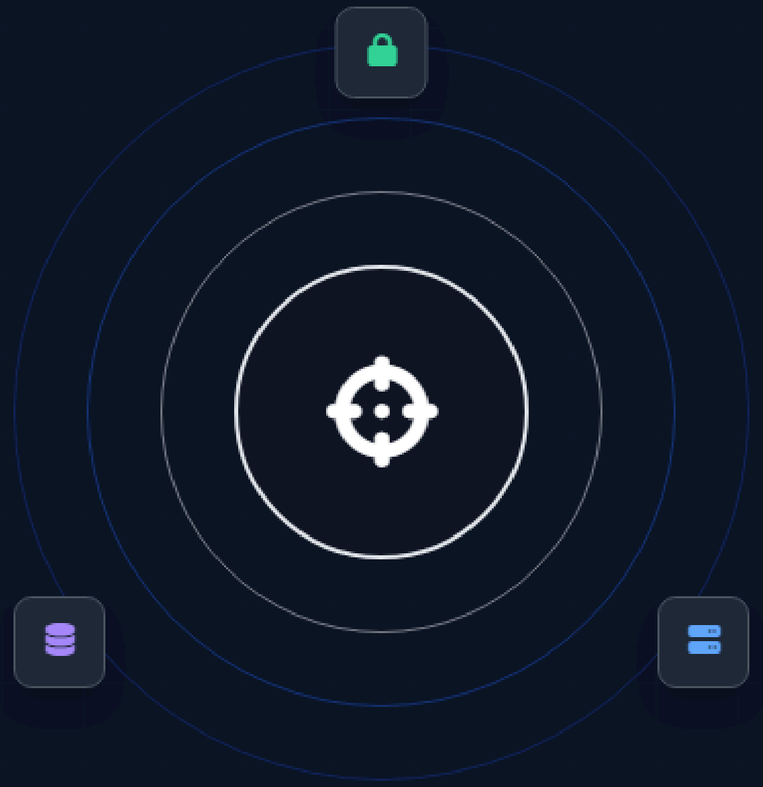
Objectifs du Projet

Centralisation
Centraliser les logs et métriques de l'ensemble de l'infrastructure.

Monitoring Visuel
Mettre en place des dashboards de monitoring interactifs et temps réel.

Facilitation d'Analyse
Simplifier l'analyse des événements système pour les administrateurs.

Sécurité Renforcée
Améliorer la sécurité globale et garantir la traçabilité des actions.



03 SCOPE

Périmètre du Projet

Inclus

FONCTIONNALITÉS LIVRÉES

Logs d'audit utilisateurs
Traçabilité complète des actions

Métriques système
Monitoring CPU, RAM et disque

Activité applicative
Suivi des événements métiers

Dashboards interactifs
Visualisation temps réel centralisée

SCOPE LIMIT

Exclus

HORS PÉRIMÈTRE

Haute disponibilité avancée
Pas de clustering ou failover automatique

Automatisation remédiation
Pas de correction automatique des incidents

Ces éléments pourront faire l'objet d'une version ultérieure (v2.0)

Architecture Technique

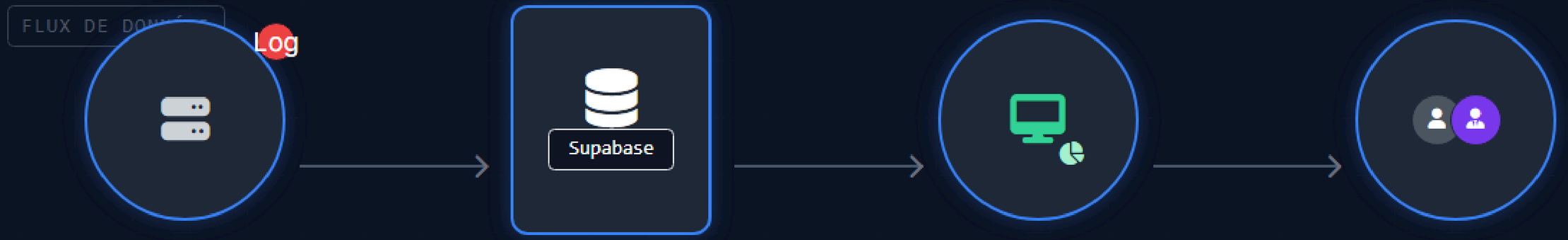
Collecte
Logs & Événements

Stockage
Supabase / PostgreSQL

Traitement
Agrégation des données

Visualisation
Dashboards Interactifs

Sécurité
Accès par rôles (RBAC)



Sources
Système & Apps

Base de Données
PostgreSQL

Frontend
Dashboards

Utilisateurs
Admin & Staff

05 STACK

Technologies Utilisées

Supabase

Backend-as-a-Service Open Source

Auth
Gestion utilisateurs

RLS (Security)
Row Level Security

Edge Functions
Logique serveur

CORE DB

PostgreSQL

Le moteur de base de données relationnel le plus avancé. Fiabilité et extensibilité.

QUERYING

SQL Avancé

Analyses complexes via `GROUP BY`, fonctions de fenêtrage et séries temporelles.

FRONTEND

Visualisation

Dashboards interactifs pour le monitoring temps réel et l'exploration de données.

OPS

Scripts d'Analyse

Scripts automatisés pour le traitement par lots et la détection de modèles.

Monitoring Système

Suivi Ressources

Monitoring en temps réel du CPU, de la RAM et de l'espace disque.

Visualisation Temporelle

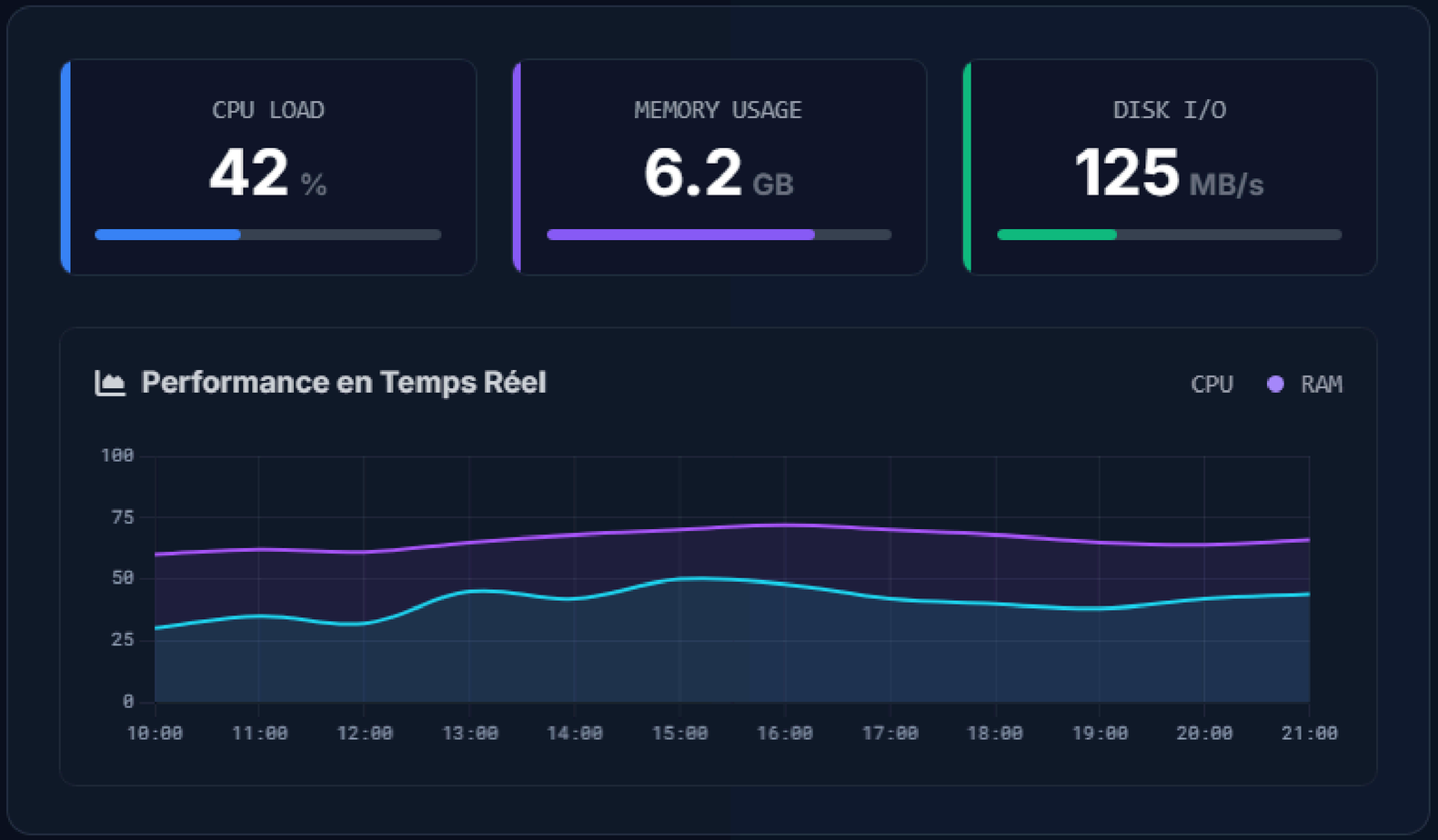
Historique des performances pour analyser les tendances.

Détection Anomalies

Alertes immédiates en cas de dépassement de seuils critiques.

Indicateurs Clés

KPIs synthétiques pour une prise de décision rapide.



09 FONCTIONNALITÉ

Logs d'Audit

Le module d'audit garantit l'intégrité et la non-répudiation des actions effectuées sur la plateforme DigitalBank.

Centralisation

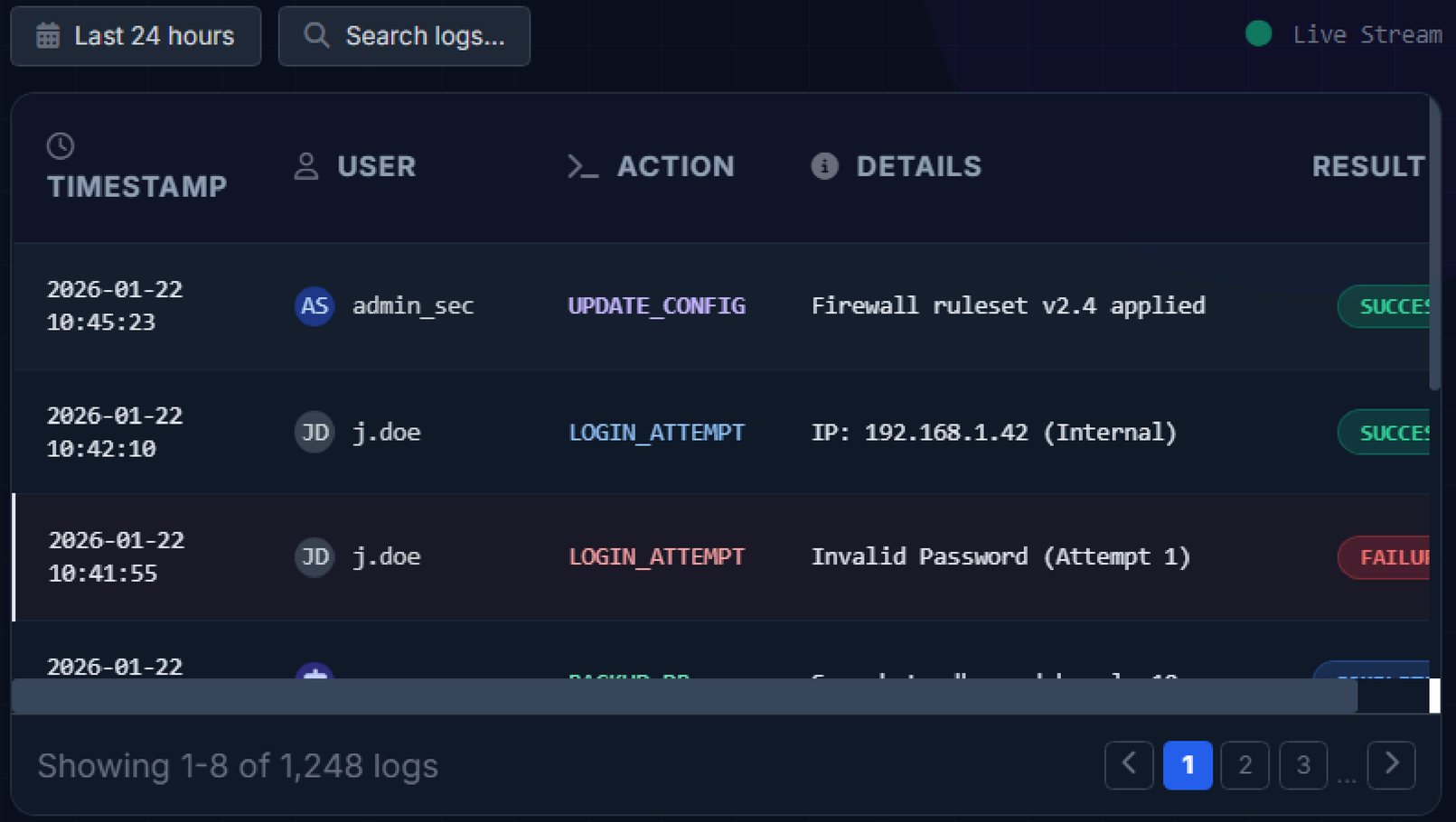
Agrégation de tous les logs (système, application, sécurité) en un point unique.

Traçabilité

Identification précise : Qui a fait Quoi, Quand et depuis Où.

Filtrage Avancé

Recherche multicritères par utilisateur



Statistiques

Transformation des données brutes en informations décisionnelles via des indicateurs synthétiques.

Événements par minute
Mesure de la charge instantanée

Activité Globale
Vue d'ensemble du trafic système

Tendances & Pics
Identification des périodes critiques

Vision Synthétique
Données exploitables pour décideurs

ÉVÉNEMENTS / MIN
1,248
↑ 12% vs. heure précédente

TOTAL JOURNALIER
845.2K
✓ Stable Moyenne nominale

TAUX D'ERREUR
0.42%
↓ -0.1% Performance optimale

Analyse du Trafic (24h)

1H 24H 7D

Sécurité et Conformité

Gestion RBAC

Role-Based Access Control

Contrôle d'accès strict basé sur les rôles. Chaque utilisateur dispose uniquement des permissions nécessaires à sa fonction (Principe de moindre privilège).

Journalisation

Audit & Tracing

Enregistrement systématique et inaltérable des actions sensibles (CRUD, Login, Export). Garantie de non-répudiation et facilitation des enquêtes.

Conformité RGPD

Privacy by Design

Anonymisation des données personnelles dans les logs, droit à l'oubli respecté et chiffrement des données au repos et en transit.

Ségrégation

Admin vs User

Isolation stricte des environnements. Les administrateurs utilisent des canaux sécurisés dédiés (VPN, MFA) distincts des utilisateurs standards.

12 MÉTHODOLOGIE

Gestion de Projet

Adoption d'une approche **Agile / Scrum** pour garantir une livraison itérative, une qualité constante et une adaptation rapide aux contraintes techniques.

01

Planification

BACKLOG & USER STORIES

Découpage fonctionnel du projet en tâches unitaires claires. Estimation de la complexité et priorisation des tickets.

- ✓ Définition des besoins
- ✓ Création du backlog
- ✓ Sprint Planning

02

Collaboration

TEAMWORK & DAILY

Synchronisation quotidienne de l'équipe TRIO INFERNAL. Partage de connaissances et revues de code croisées.

- ✓ Daily Stand-ups
- ✓ Code Reviews (PR)
- ✓ Pair Programming

03

Développement

SPRINTS & ITÉRATIONS

Développement progressif par cycles courts. Livraison régulière de fonctionnalités testables pour validation rapide.

- ✓ Sprint de 2 semaines
- ✓ Livrables intermédiaires
- ✓ Versionning Git

04

Qualité

TESTS & VALIDATION

Stratégie de test continue pour garantir la robustesse. Tests unitaires, d'intégration et de sécurité automatisés.

- ✓ Tests Unitaires
- ✓ Tests de Sécurité
- ✓ Validation Utilisateur

Planning du Projet

Analyse

DES BESOINS

- ✓ Étude existant
- ✓ Cahier des charges
- ✓ Choix stack

Conception

ARCHITECTURE

- ✓ Modèle de données
- ✓ Mockups UI/UX
- ✓ Schéma infra

Développement

IMPLÉMENTATION

- ✓ Backend API
- ✓ Dashboards
- ✓ Intégration DB

Tests

VALIDATION

- ✓ Tests unitaires
- ✓ Tests de charge
- ✓ Correction bugs

Livrables

Juil. 2026

DOCUMENTATION

- ◌ Rapport final
- — Manuel admin
- — Présentation

14 CHALLENGES

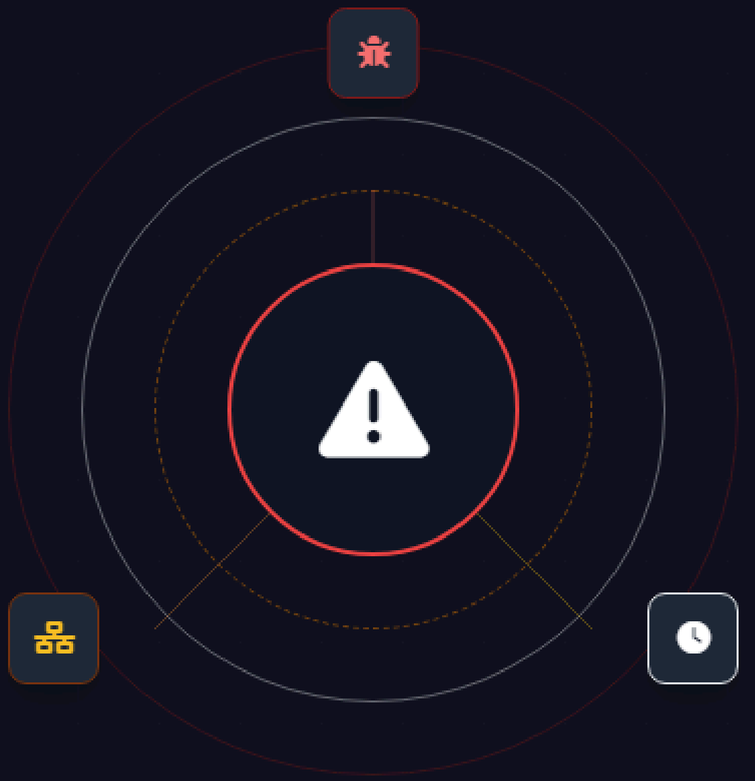
Difficultés Rencontrées

Données Brutes
Compréhension difficile des formats hétérogènes et volume important de logs.

Structuration
Complexité de normalisation et d'organisation des logs d'audit disparates.

Complexité SQL
Élaboration de requêtes PostgreSQL avancées pour les agrégations temps réel.

Pertinence KPI
Difficulté à identifier et sélectionner les indicateurs de sécurité les



TECHNICAL HURDLES

15 RÉSOLUTION

Solutions Apportées

Réponses techniques et méthodologiques directes aux défis rencontrés lors de la phase d'implémentation.

DONNÉES BRUTES

Normalisation des Données

Transformation des logs JSON non structurés en schémas relationnels stricts (PostgreSQL). Typage fort pour garantir la cohérence à la source.

PERFORMANCE SQL

Optimisation des Requêtes

Mise en place d'index composites et utilisation de Vues Matérialisées pour les agrégations lourdes (statistiques temps réel).

STABILITÉ

Tests Itératifs

Cycles de développement courts avec tests unitaires automatisés à chaque commit pour détecter les régressions immédiatement.

PERTINENCE

Validation des Résultats

Comparaison des métriques du dashboard avec les logs bruts (échantillonnage) pour certifier l'exactitude des KPI affichés.

16 PERFORMANCES

Résultats et Métriques

OPÉRATIONNEL

Dashboards Fonctionnels

3 Vues

Déploiement complet des tableaux de bord : Monitoring système, Audit de sécurité et Statistiques métier.

PERFORMANT

SQL Optimisé

-40% Latence

Réduction drastique du temps d'exécution grâce à l'indexation avancée et aux vues matérialisées PostgreSQL.

LIVE FEED

Logs Temps Réel

COUVERTURE

Visibilité Système

17 VALEUR AJOUTÉE

Apports du Projet

Supervision Améliorée

Capacité de monitoring accrue avec une visibilité temps réel sur l'état de santé des systèmes.

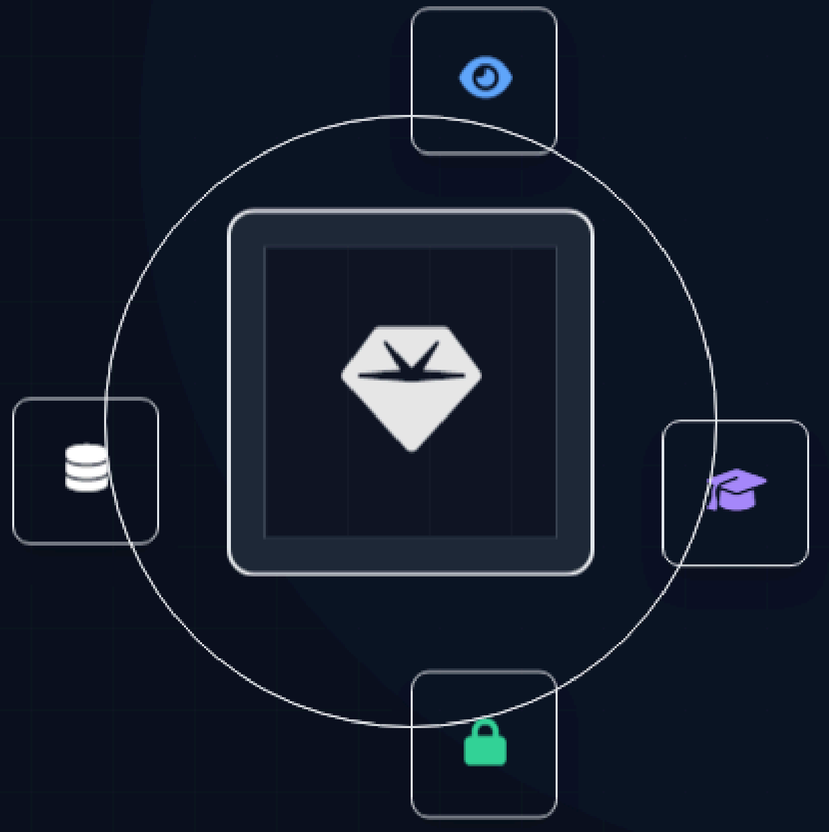
Vision Centralisée

Centralisation de toutes les données d'infrastructure (logs, métriques) en un point unique.

Approche Sécurité

Renforcement de la posture de sécurité par la traçabilité des actions et la détection d'incidents.

Montée en Compétences



Perspectives d'amélioration

COURT TERME • Q3 2026

Alertes Actio

Intégration de notifications push multi-canaux (Slack, Teams, SMS) pour réduire le MTTA (Mean Time To Acknowledge).

MOYEN TERME • Q4 2026

Détection Avancée

Implémentation d'algorithmes statistiques pour identifier les comportements aberrants (outliers) sans seuils fixes.

LONG TERME • 2027

Analyse Prédictive

Usage du Machine Learning sur l'historique des logs pour anticiper les pannes disques et la saturation mémoire.

ÉVOLUTION CONTINUE

Scalabilité

Migration vers une architecture micro-services conteneurisée (Kubernetes) et sharding de la base de données PostgreSQL.

Conclusion

> *"Ce projet a permis de concevoir une **solution complète de monitoring et de sécurité**, apportant une réelle valeur ajoutée en matière de supervision, d'analyse et de protection des systèmes."*

SUPERVISION

Visibilité temps réel sur l'ensemble de l'infrastructure et des flux de données.

ANALYSE

Tableaux de bord interactifs pour une prise de décision basée sur la data.

PROTECTION

Sécurisation des accès (RBAC) et traçabilité complète des actions critiques.

Questions et Remerciements

Merci pour votre attention.

Nous sommes maintenant disponibles pour répondre à toutes vos questions concernant l'architecture, la sécurité ou la mise en œuvre du projet.

Contactez-nous

EMAIL PROJET
contact@trio-infernal.dev

LINKEDIN
/in/trio-infernal-secu