Rapport d’avancement du projet SIEM minimaliste

1. Introduction

Ce rapport présente l'état d'avancement de mon projet “SIEM minimaliste” développé en Python. Il couvre les travaux réalisés, la conception finalisée, et les prochaines étapes prévues.

2. Travaux réalisés

1. **Collecte de logs**
    - Implémentation d'un agent pour extraire les événements Windows.
    - Extraction des champs clés (EventID, TimeCreated, Computer, Channel, ProcessID, ThreadID, Level).
2. **Base de données**
    - Création de la table `logs` dans SQLite .
    - Fonctions d'insertion et de requête avec filtres et pagination.
3. **Serveur Web**
    - Mise en place d'un serveur HTTP en python servant l'interface statique.
4. **Interface Utilisateur**
    - Dashboard en HTML/CSS/JS avec onglets Logs et Analyses.

3. Conception finalisée

La conception retenue est une **architecture à agents modulaires** avec un **module central de traitement** :

3.1 Agents de collecte

- **Fonction** : Surveillance continue de fichiers de logs (Windows EVTX ou autres) et extraction en temps réel des nouvelles entrées.
- **Déploiement** : Plusieurs agents peuvent tourner sur différentes machines ou en local, chacun dédié à un ou plusieurs fichiers de logs.
- **Communication** : Envoi asynchrone des événements extraits sous forme JSON à un point d'ingestion central, via HTTP POST ou un broker de messages (Kafka, RabbitMQ).

3.2 Module central de traitement

- **Validation et enrichissement** : Vérification des données reçues, ajout de méta-informations (horodatage serveur, labels de criticité).
- **Stockage** : Insertion dans la base SQLite.
- **Traitements complémentaires** : Filtrage, agrégation, calcul de statistiques.

3.3 Interface Dashboard

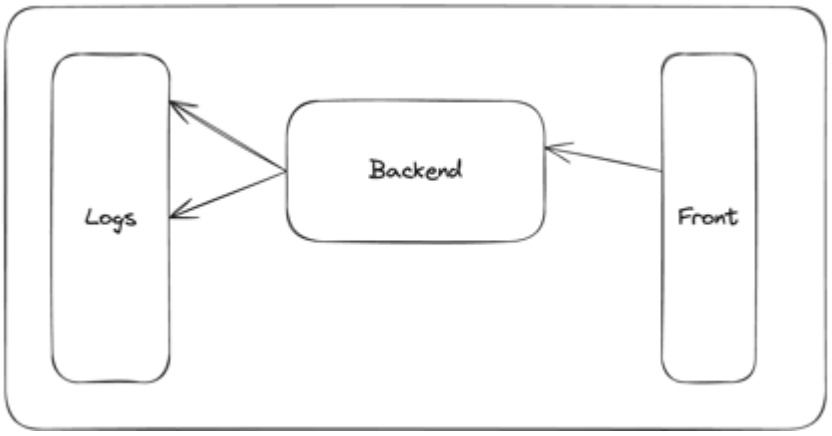
- **Frontend** : Onglets Logs et Analyses (statistiques, tendances, graphiques).
- **Extensibilité** : Possibilité d'ajouter différents fichiers de logs en “.evtx”.

4. Prochaines étapes

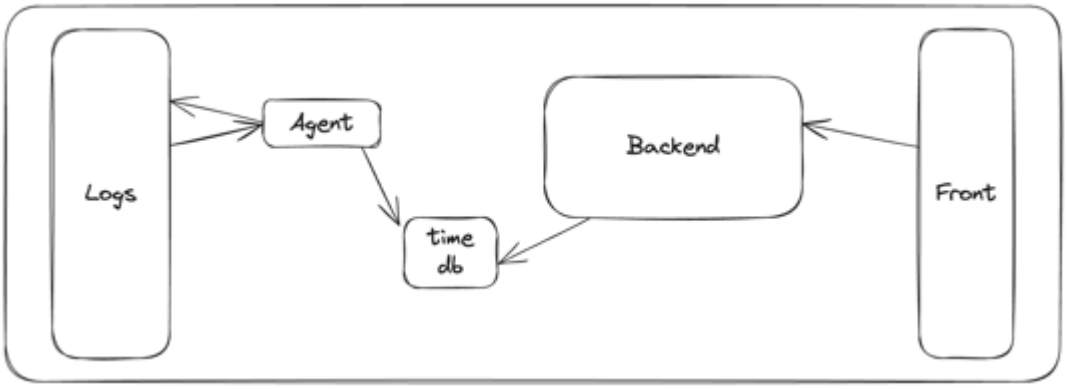
- **Gestion des erreurs**.
- **Mise en place d’analyses plus avancées.**
- **Gestion des notifications.**

5. Schéma des agents

Première version :



Version actuelle :



Version dans un système plus complexe :