## 👨‍💻 Auteur

**Ilyesse-soc**
💻 **GitHub : [github.com/Ilyesse-soc](github.com/Ilyesse-soc)**

# 🟦 Documentation Technique — SIEM Simplifié

## 📝 Présentation du Projet

**SIEM Simplifié est un système de supervision et d'analyse des logs de sécurité développé à des fins pédagogiques. Il permet de collecter, stocker, et visualiser les événements du système à travers une interface web minimaliste. Il repose sur la stack ELK (Elasticsearch, Logstash-like via script Python, Kibana remplacé par interface Flask) et MongoDB.**

**Ce projet vise à illustrer le fonctionnement d'un SIEM (Security Information and Event Management) de manière légère et compréhensible, notamment pour les étudiants ou les professionnels en reconversion.**

## 🚀 Fonctionnalités

**✅ Collecte de logs système via script Python**
**📤 Envoi des logs vers Elasticsearch pour indexation**
**📦 Sauvegarde des logs dans MongoDB pour usage local**
**🌐 Interface web (Flask) affichant les derniers logs collectés**
**📊 Visualisation simplifiée en temps réel**
**⚠️ Gestion des erreurs de connexion aux bases (Elasticsearch, Mongo)**
**🔁 Rafraîchissement des données sans recharger la page (AJAX possible)**
**🔒 Déploiement local via Docker Compose**

## 🎨 Design UI/UX

**🌑 Thème sombre moderne**
**🟢 Couleurs sobres : gris foncé / vert pour les logs**
**📋 Présentation sous forme de tableau HTML**

💡 Interface responsive avec Flask + Jinja2
📄 Fichier .env pour centraliser la configuration
🖥️ Simplicité et clarté : affichage immédiat des logs utiles

## 🧠 Architecture Technique

⚙️ Backend : Python
🌍 Web framework : Flask
📁 Structure modulaire :

arduino

CopierModifier

collecteur/ → script de collecte des logs

mongo/ → config MongoDB

elastic/ → config Elasticsearch

templates/ → page HTML avec affichage des logs

.env → paramètres d'environnement

🧵 Base NoSQL : MongoDB
🔎 Moteur de recherche : Elasticsearch
🧪 Collecte : script Python simulant l'envoi de logs
📊 Frontend : HTML + CSS via Flask (pas de JS avancé)

## 🛠️ Technologies utilisées

- Python 3.10
- Flask
- MongoDB
- Elasticsearch
- Docker & Docker Compose
- pymongo
- elasticsearch-py
- Jinja2 (templates Flask)

## 🌄 Vue sur le projet

# Logs de Sécurité (SIEM Simplifié)

| Timestamp | Niveau | Message |
| --- | --- | --- |
| 2025-07-16 19:32:54.956000 | INFO | Démarrage de l'application SIEM simplifié. |