Analyse Intelligente des Logs Suricata avec n8n et Intelligence Artificielle

Introduction

Bien que les systèmes de détection d'intrusions comme Suricata soient efficaces pour générer des alertes en temps réel, la gestion, l'analyse et l'interprétation des logs générés représentent un défi majeur pour les équipes de sécurité. En effet, Suricata produit un volume considérable d'événements, dont la majorité sont bénins ou répétitifs, tandis que certains signalent des menaces réelles qui nécessitent une intervention rapide.

- **Face à cette problématique, nous avons développé une solution d'automatisation intelligente combinant n8n comme moteur d'orchestration des workflows et une Intelligence Artificielle pour analyser automatiquement les logs générés par Suricata. Cette approche permet de :**

- **Automatiser la collecte et le traitement des logs Suricata**
- **Réduire les faux positifs grâce à l'analyse contextuelle**
- **Classifier automatiquement les menaces en fonction de leur niveau de criticité**
- **Notifier rapidement les administrateurs via email pour les événements critiques**
- **Améliorer la réactivité face aux incidents de sécurité**
- **Ce chapitre détaille l'architecture, les outils utilisés, la configuration et les résultats de cette solution d'automatisation intelligente des logs de sécurité.**

Outils Utilisés

n8n : Plateforme d'Orchestration des Workflows

n8n est une plateforme open source d'automatisation des processus métier (Workflow Automation Platform) qui permet de créer, de gérer et d'orchestrer des workflows complexes sans nécessiter de codage avancé.

Figure 3.1 -- Logo et interface de n8n

Caractéristiques principales :

- **Connecteurs intégrés : n8n dispose de plus de 400 intégrations natives avec des services populaires (emails, bases de données, APIs, stockage cloud, etc.)**
- **Interface visuelle : Création de workflows par drag-and-drop, sans nécessiter de programmation complexe**
- **Déclencheurs et actions : Supports des déclencheurs basés sur le temps (cron), les fichiers, les webhooks, etc.**
- **Traitement de données : Transformation, filtrage, enrichissement et formatage des données entre les étapes**
- **Gestion des erreurs : Mécanismes de gestion d'erreurs, tentatives automatiques et routages conditionnels**
- **Exécution en temps réel : Possibilité d'exécuter les workflows instantanément ou selon un calendrier défini**

Rôle dans notre projet :

n8n joue le rôle d'orchestrateur central dans notre solution. Il :

1. **Surveille en permanence le dossier partagé contenant les logs Suricata**
2. **Déclenche automatiquement un workflow à chaque nouvelle détection de fichier**
3. **Lit et traite les logs**
4. **Formate les données pour transmission à l'agent IA**
5. **Gère les retours de l'IA et l'envoi des notifications**

Agent IA pour l'Analyse des Logs

L'agent IA est un système d'Intelligence Artificielle basé sur un modèle de langage de grande taille (LLM) capable de comprendre et d'analyser le contexte des logs de sécurité. Il utilise des techniques de traitement du langage naturel (NLP) pour :

Capacités d'analyse :

- **Extraction d'informations : Identifier les éléments clés des logs (adresses IP, ports, protocoles, types d'attaques)**
- **Classification du risque : Évaluer le niveau de menace (Critique, Élevé, Moyen, Faible, Normal)**
- **Contextualisation : Interpréter les logs en fonction du contexte de sécurité**
- **Génération de rapports : Produire des résumés lisibles et exploitables par les administrateurs**
- **Recommandations : Suggérer des actions correctives appropriées**

Intégration dans le workflow :

- **L'agent IA reçoit de n8n les logs formatés en texte naturel et produit une analyse structurée comprenant :**
- **La classification de l'événement (normal, suspect, attaque)**
- **Le niveau de sévérité**
- **Les recommandations d'action**
- **Un résumé explicatif**

Dossier Partagé (Shared Folder)

Le dossier partagé constitue le point de transfert des données entre Suricata et n8n.

Fonctionnalités :

- **Emplacement centralisé : Tous les logs Suricata exportés y sont dirigés**
- **Accessibilité : Le dossier est accessible via le réseau pour n8n**
- **Structure organisée : Les logs sont organisés par date ou type d'événement**
- **Rotation automatique : Les anciens logs peuvent être archivés pour ne pas surcharger le système**

Architecture et Workflow

- **Diagramme d'Architecture**

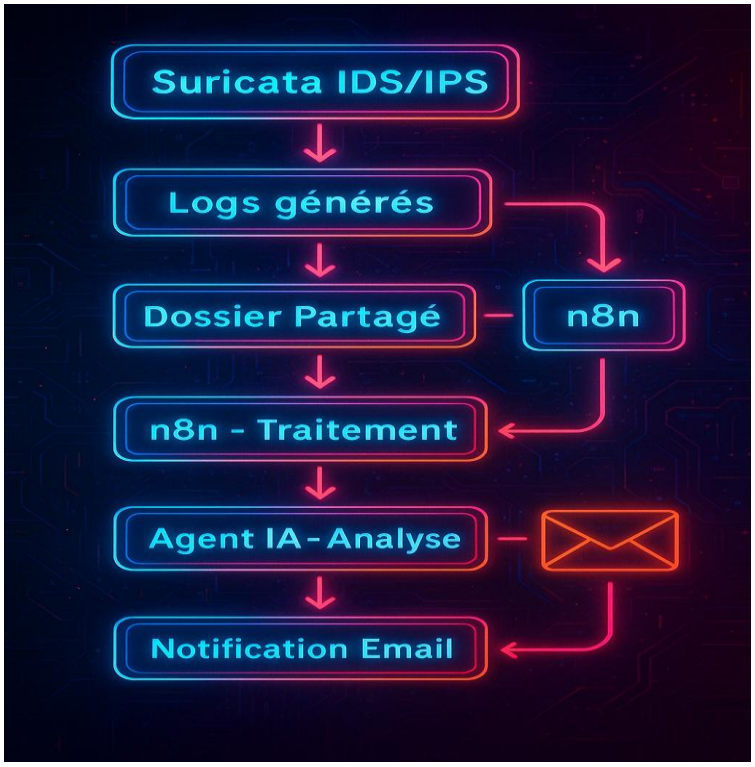


Figure 3.2 -- Flux d'automatisation des logs

Description du Workflow

Le workflow fonctionne selon le cycle suivant :

1. Génération des Logs Suricata analyse le trafic réseau en temps réel sur le pare-feu pfSense. Chaque événement de sécurité détecté est enregistré dans un fichier de log localisé dans le dossier partagé.

2. Surveillance du Dossier (n8n - File Watcher) n8n utilise un nœud de surveillance de fichiers pour détecter automatiquement l'apparition de nouveaux logs ou des modifications de fichiers existants. Cette détection peut s'effectuer en continu ou selon un intervalle défini (ex : toutes les 5 minutes).

3. Lecture et Extraction des Données Une fois un nouveau fichier détecté, n8n le lit et en extrait le contenu. Les logs peuvent être au format JSON ou texte brut et sont parsés pour être structurés.

4. Transformation et Formatage (n8n) Les logs bruts sont transformés en un format lisible et contextualisé :

- **Suppression des données inutiles**
- **Enrichissement avec des métadonnées**
- **Formatage en texte naturel pour l'IA**
- **Ajout de timestamps et informations de contexte**

5. Envoi à l'Agent IA Les logs formatés sont envoyés à l'agent IA via une API, accompagnés de contexte spécifique pour guider l'analyse.

6. Analyse par l'IA L'agent IA analyse les logs et produit :

- **Une classification de l'événement**
- **Un niveau de sévérité**
- **Une explication en français**
- **Des recommandations d'action**

7. Traitement des Résultats (n8n) n8n reçoit les résultats de l'IA et les formate pour notification :

- **Filtrage des événements bénins**
- **Enrichissement des alertes critiques**
- **Création du message email**
- **Vérification des adresses destinataires**

8. Notification par Email Les événements critiques ou suspects sont automatiquement transmis par email aux administrateurs de sécurité, incluant une analyse détaillée et des recommandations.

Configuration Technique

Installation et Configuration de n8n

Étape 1 : Installation de n8n

Via Docker (Recommandé)

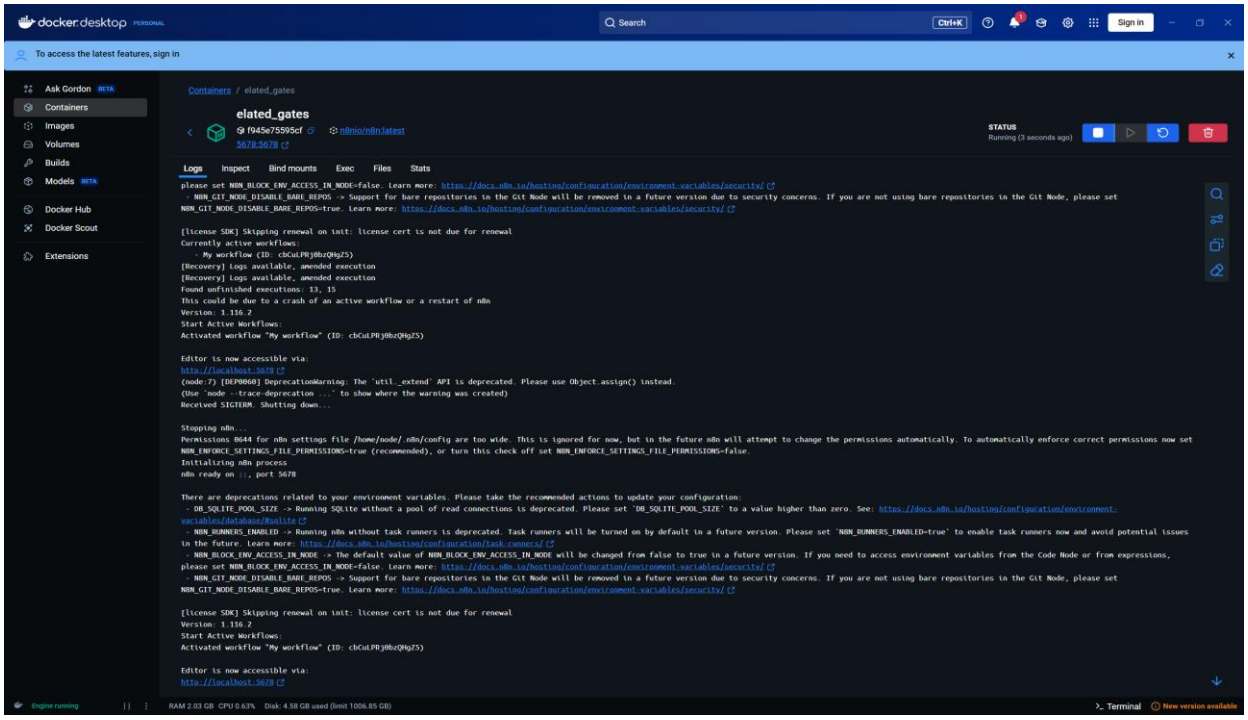


Figure 3.3 -- Installation de n8n via Docker

Étape 2 : Accès à l'Interface Web

Une fois n8n démarré, accéder à l'interface via un navigateur :

http://localhost:5678

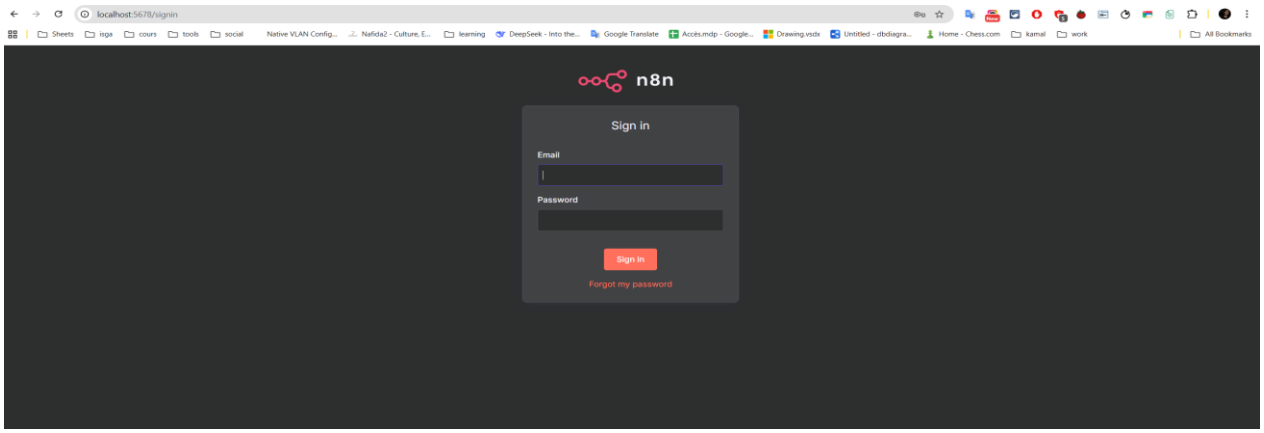


Figure 3.4 -- Interface d'accueil de n8n

Étape 3 : Création du Workflow de Surveillance

3.1 Ajout d'un nœud de déclencheur (File Watcher)

Créer un nouveau workflow

Ajouter un nœud "File Watcher" (Surveillance de fichiers)

Configurer le chemin du dossier partagé contenant les logs Suricata

Définir les critères de déclenchement (ex : fichiers .log ou .json)

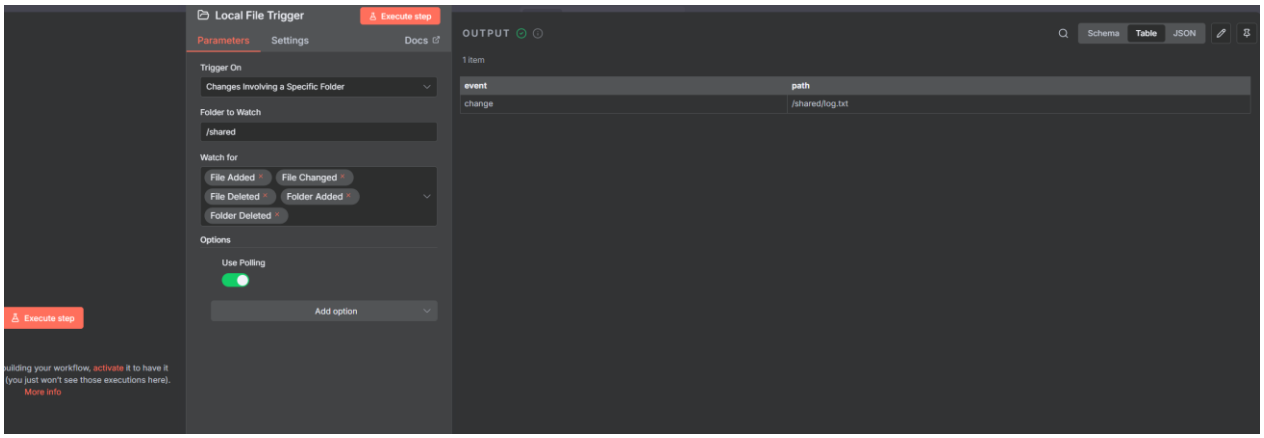


Figure 3.5 -- Configuration du nœud File Watcher

3.2 Ajout d'un nœud de lecture de fichier

Ajouter un nœud "File" pour lire le contenu du fichier détecté

Configurer la lecture du fichier déclencheur

Extraire le contenu en tant que texte

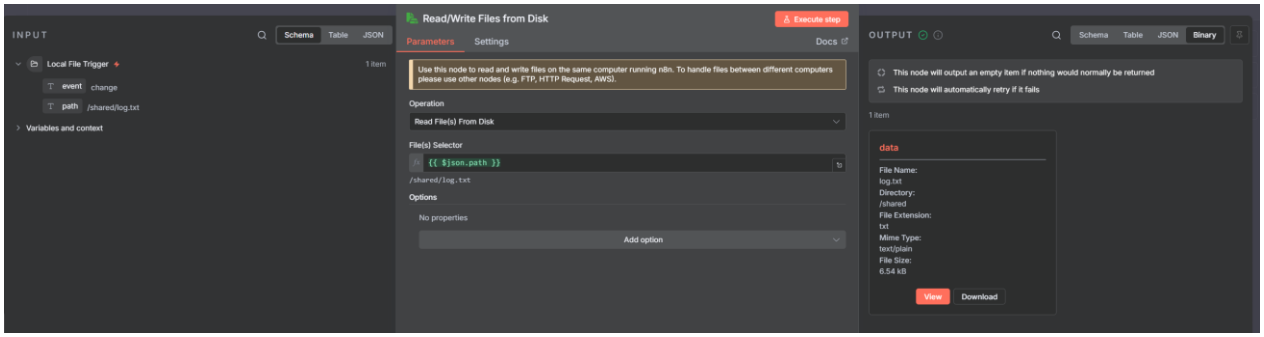


Figure 3.6 -- Configuration de la lecture de fichier

3.3 Ajout d'un nœud de transformation (Function)

Créer une fonction JavaScript pour transformer les logs bruts en format structuré :

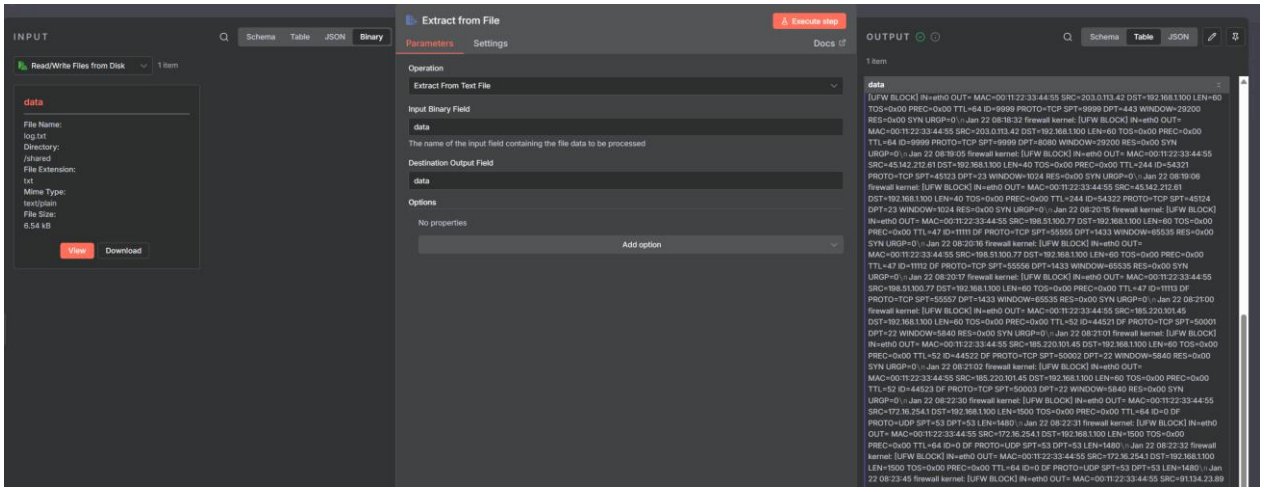


Figure 3.7 -- Configuration du nœud de transformation

3.4.1 Configuration du nœud Edit Fields

1. **Ajouter un nœud "Edit Fields" après le nœud de transformation**
   Le prompt envoyé à l'agent IA doit inclure :

- Les logs à analyser
- Le contexte de sécurité
- Les instructions d'analyse
- Le format de réponse attendu

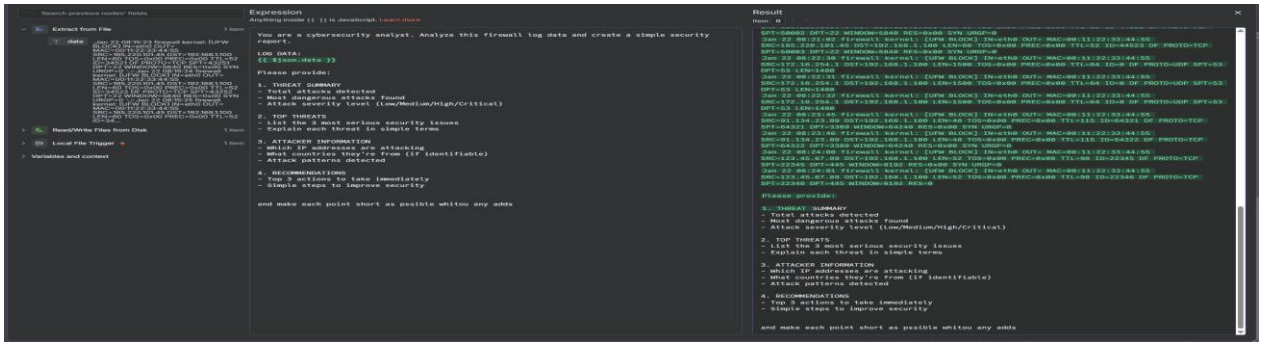


Figure 3.8 -- Configuration du nœud Edit Fields

3.4 Ajout d'un nœud d'appel API

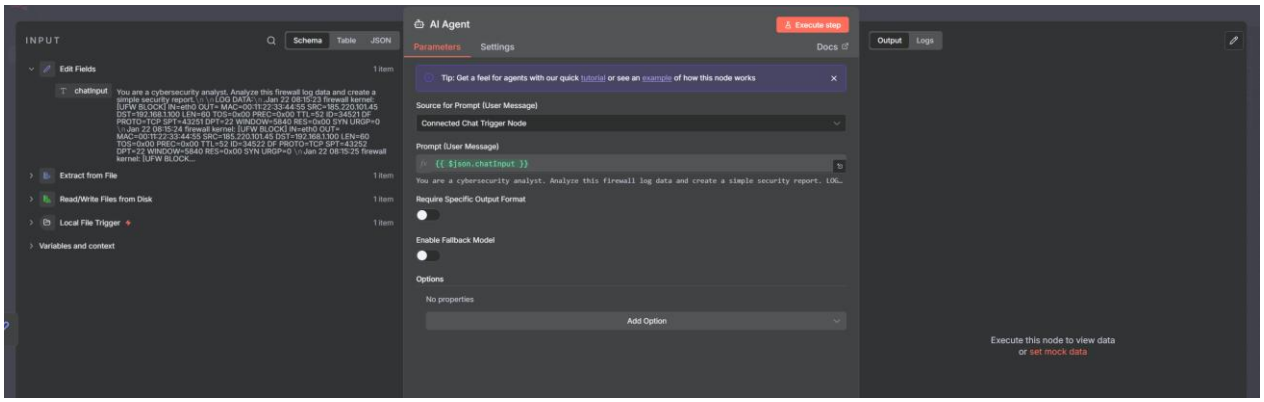


Figure 3.8 -- Configuration de l'appel API à l'agent IA

3.5 Ajout d'un nœud de notification Email

Ajouter un nœud "Send Email"

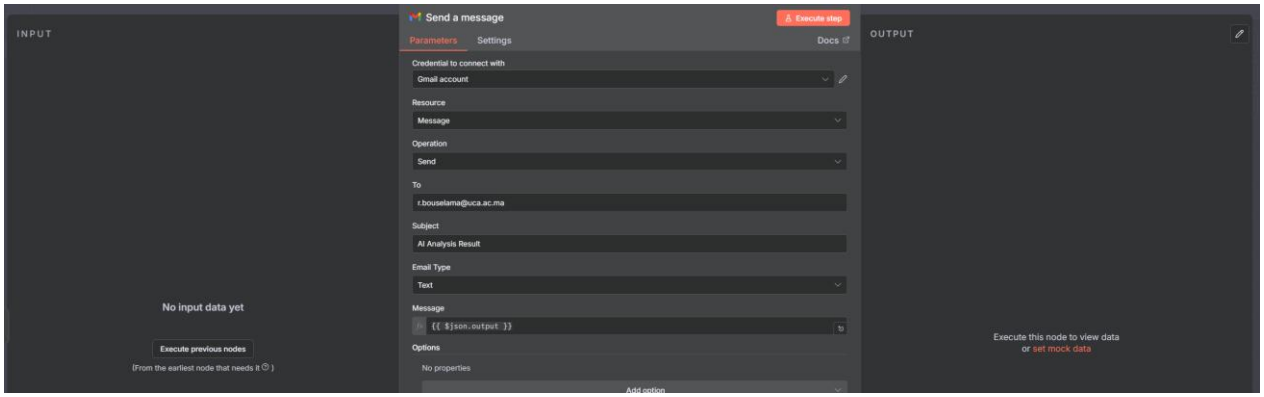


Figure 3.9 -- Configuration du nœud d'envoi d'email

Étape 1 : Partage pfSense

bash

```
# Sur pfSense (SSH)
vi /etc/samba/smb.conf
# Ajouter:
[suricata-logs]
 path = /var/log/suricata
 browseable = yes
 writable = yes
 guest ok = yes
 read only = no
/etc/rc.d/samba_smbd restart
```

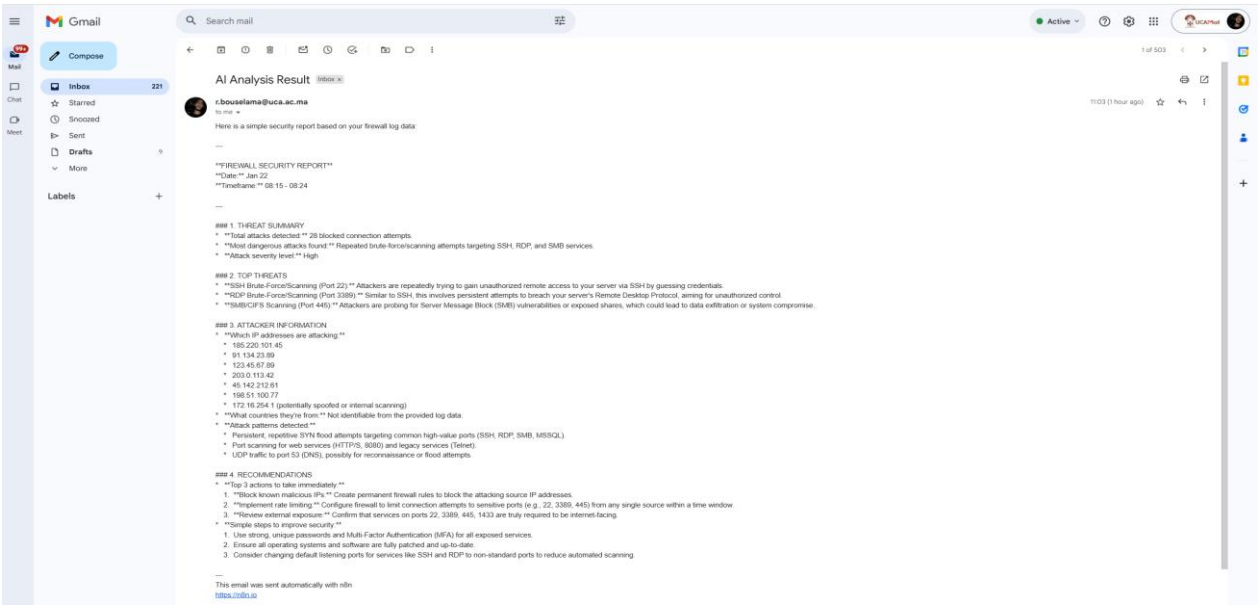
Étape 2 : docker-compose.yml simplifié

yaml

```
volumes:
 - /mnt/suricata-logs:/data/suricata-logs
```

Exemple de Rapport Généré

Email reçu :



4.1--- Exemple de Rapport Généré

Conclusion

La mise en œuvre d'une solution automatisée d'analyse des logs Suricata combinant n8n et une Intelligence Artificielle représente une avancée majeure dans la gestion de la sécurité réseau. Cette approche offre plusieurs avantages significatifs :

Bénéfices réalisés :

- **Automatisation complète : Élimination des tâches manuelles répétitives d'analyse de logs**
- **Réactivité accrue : Notification immédiate des administrateurs en cas de menace détectée**
- **Réduction des faux positifs : L'IA filtre les événements bénins et classe les vraies menaces**
- **Scalabilité : Le système peut traiter des milliers de logs sans dégradation de performance**
- **Traçabilité : Chaque événement est documenté et peut être audité**

Perspectives d'amélioration :

1. **Intégration d'une base de connaissances : Enrichir l'IA avec une ontologie de menaces spécifiques à l'organisation**
2. **Machine Learning adaptatif : Entraîner des modèles spécifiques sur les logs historiques de l'environnement**
3. **Corrélation multi-sources : Combiner les logs Suricata avec d'autres sources (Windows Event Viewer, syslogs, etc.)**
4. **Dashboard de visualisation : Créer un tableau de bord en temps réel pour visualiser les menaces détectées**
5. **Playbooks de réponse : Intégrer des actions de réponse automatique (blocage d'IP, déconnexion de sessions, etc.)**

Cette solution constitue une étape décisive vers un centre opérationnel de sécurité (SOC) autonome et intelligent, capable de détecter, analyser et répondre aux menaces sans intervention humaine constante.

Références

Documentation n8n : https://docs.n8n.io/

Suricata - Format des Logs : https://suricata.readthedocs.io/

Samba - Partage Réseau : https://www.samba.org/

LLM et Analyse de Sécurité : https://arxiv.org/