FORUM INNOVATION | UQAR
INGÉNIERIE • INFORMATIQUE • ENTREPRENEURIAT

SOAR IP ANALYZER avec n8n et opencanary

Raïssa Domgnim Bopda, étudiante finissante au DEC informatique

Problématique

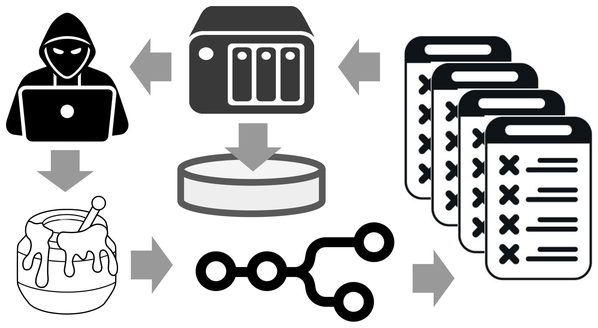
Un serveur exposé sur Internet reçoit **des centaines de connexions suspectes par jour**. Les trier à la main est impossible : il faudrait, pour chacune, interroger plusieurs sources de renseignements, croiser les données et décider.

Les plateformes commerciales qui automatisent ce travail - les **SOAR** (Security Orchestration, Automation and Response) - coûtent des dizaines de milliers de dollars par année. C'est hors de portée pour une PME ou un projet étudiant.

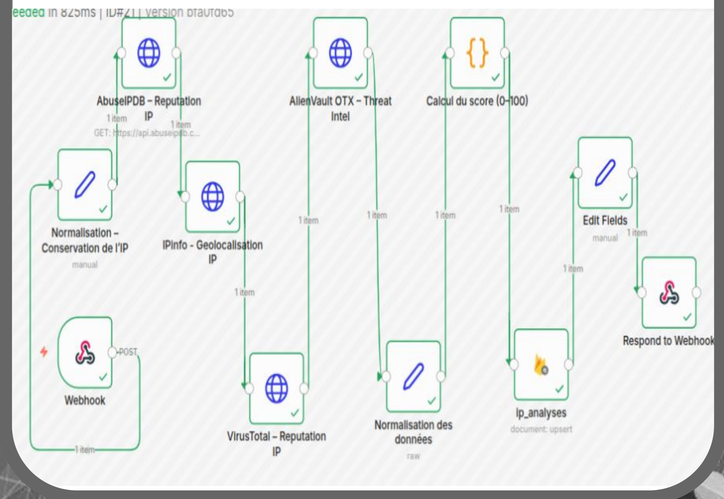
Objectif

Bâtir un **SOAR open source** et résilient qui, face à une adresse IP suspecte :

1. **détecte** l'incident avec un honeypot
2. **interroge** 4 APIs de liste noire en parallèle
3. **calcule** un score de menace de 0 à 100
4. **décide** : sûre, suspecte ou malveillante
5. **archive** le dossier complet pour audit



Flux des données



Méthodologie

Itération 1 - Preuve de concept:
Objectif : prouver que n8n peut recevoir, transformer et écrire de façon fiable les retours des APIs de liste noire.

Itération 2 - Algorithme de calcul de score:

Source	Poids
AbuseIPDB	40
VirusTotal	30
AlienVault OTX	20
IPinfo	10

Développement du cœur du SOAR. Le workflow reçoit une IP, interroge 4 APIs en parallèle, parse les réponses et applique la pondération. Le résultat est un score reproductible de 0 à 100, stocké dans Firestore.

Itération 3 - Interface utilisateur:
Mise en place d'une interface web simple. L'utilisateur soumet une IP et consulte le verdict. Déploiement automatisé clé-en-main sur linux avec un script d'installation (Docker, Nginx, Certbot, UFW).

Matériel & Logiciel

Pour répéter l'expérience, vous aurez besoin des éléments logiciels suivants :

- **Orchestrateur** : n8n (libre, auto-hébergé)
- **Leurre (honeypot 🍯)**: OpenCanary
- **Renseignement (liste noire)** : IPinfo - AbuseIPDB · VirusTotal · AlienVault OTX
- **Stockage** : Google Cloud Firestore
- **Infrastructure** : Docker · Nginx · Let's Encrypt · UFW - Ubuntu server - Linode
- **Frontend** : page web simple pour soumettre ou consulter une IP

Résultats & Futur

Le système SOAR détecte les IPs malicieuses en quelques secondes, sans humain dans la boucle. Le script de déploiement déploie l'analyzer SOAR sur un serveur neuf en moins de quinze minutes.

Les améliorations futures du projet sont :

- Explorer les variations de scoring avec les APIs
- Cacher les informations déjà obtenues (Redis)
- Développer une base de données maison des ips malicieuses et l'utiliser prioritairement
- Exposer des comptes utilisateurs avec clés d'api
- Visualiser avec des jauges et exports PDF

SCANNEZ ce QR code pour expérimenter et voir les statistiques !

https://soar.raissa-domgnim-portfolio.dev/