CÉGEP DE MATANE

FORUM INNOVATION
INGÉNIERIE | INFORMATIQUE |
ENTREPRENEURIAT | UQAR

SOAR IP Analyzer

par Raïssa Domgnim Bopda

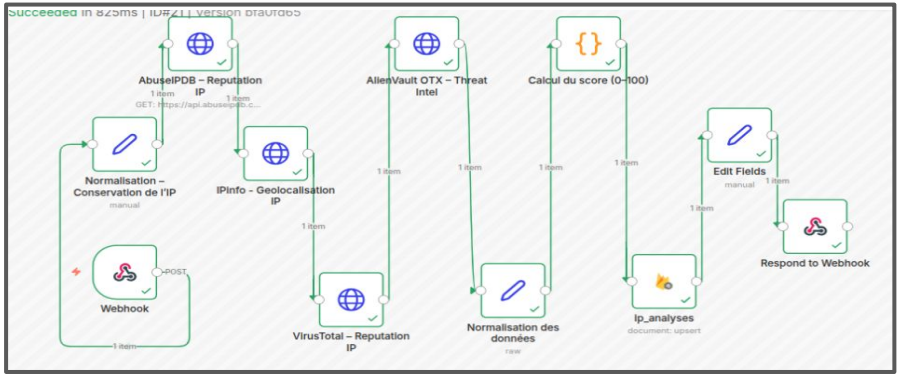
Présenté au FI3E par le Cégep de Matane

FORUM INNOVATION
INGÉNIERIE | INFORMATIQUE |
ENTREPRENEURIAT | UQAR

SOAR IP ANALYZER

avec n8n et opencanary

SOAR IP analyzer analyse vos attaquants à votre place. C'est un analyste virtuel auto-hébergé qui trie les tentatives d'intrusion de serveur sans intervention humaine. La démonstration met en scène une IP malicieuse : le honeypot la détecte, quatre sources de renseignements sont interrogées en parallèle et un score de menace est calculé. Le système rend son verdict en quelques secondes, et lance l'alerte via un simple webhook. Là où les plateformes commerciales de SOAR coûtent des dizaines de milliers de dollars par année, Soar IP fait la même chaîne en outils libres et automatiquement déployables. La cybersécurité devient accessible à une PME ou un étudiant.



Pourquoi ce projet ?

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.

Pourquoi ce projet ? en un coup d'oeil

Le Problème

Un serveur exposé sur Internet reçoit **des centaines de connexions suspectes par jour**.

Le tri manuel est impossible :

- Interroger plusieurs sources
- Croiser les données
- Prendre une décision

La Barrière

Les plateformes **SOAR** commerciales automatisent ce travail mais sont coûteuses.

10 000$+ / an

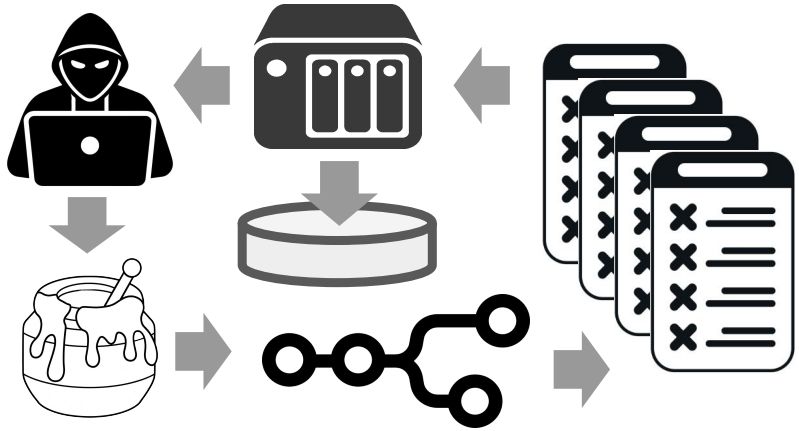
C'est hors de portée pour :

- Les PME
- Les projets étudiants

Objectifs

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



Méthodologie agile

Itération 1
Preuve de concept

Objectif : Prouver que n8n peut recevoir, transformer et écrire de façon fiable les retours des APIs de liste noire.

Résultat : 4 sources de renseignement validées

Itération 2
Algorithme de score

Développement du cœur du SOAR : interrogation de 4 APIs en parallèle, parsing et pondération.

Résultat : Score reproductible de 0 à 100 stocké dans Firestore.

Itération 3
Interface utilisateur

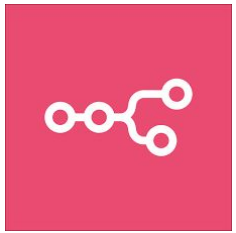
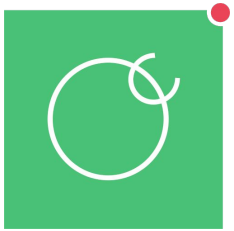
Création d'une interface web simple pour soumettre une IP et lire le verdict.

Déploiement automatisé clé-en-main sur linux avec un script d'installation (Docker, Nginx, Certbot, UFW).

Matériel

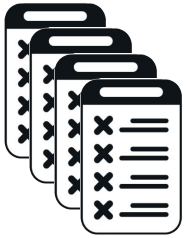
Pour répéter l'expérience, vous aurez besoin des éléments logiciels suivants :

- **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


Preuve de concept : les APIS

Itération 1



Sélection finale des sources de renseignement (Scoring)

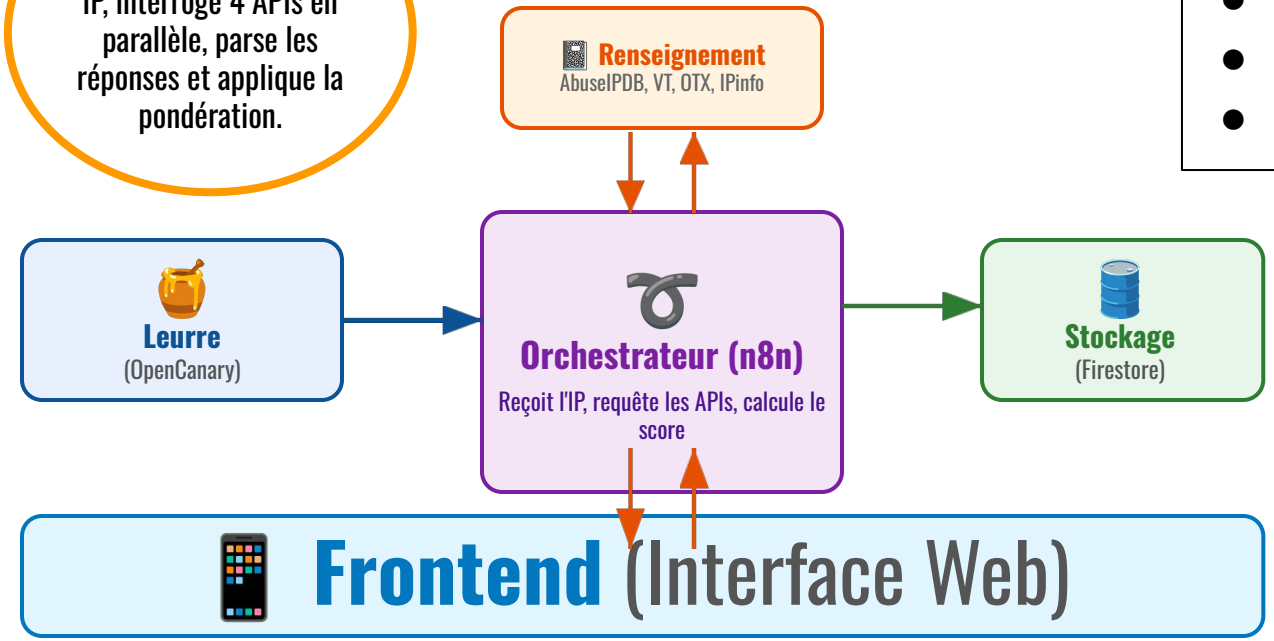
#	Source	Poids max	Rôle
1	AbuseIPDB	40	Réputation communautaire
2	VirusTotal	30	Agrégation multi-moteurs
3	AlienVault OTX	20	Renseignement collaboratif
4	IPinfo	10	Géolocalisation + organisation

Shodan a été écarté (caractérisation d'exposition vs réputation).

Diagramme de flux

Itération 2

Le workflow reçoit une IP, interroge 4 APIs en parallèle, parse les réponses et applique la pondération.



Légende

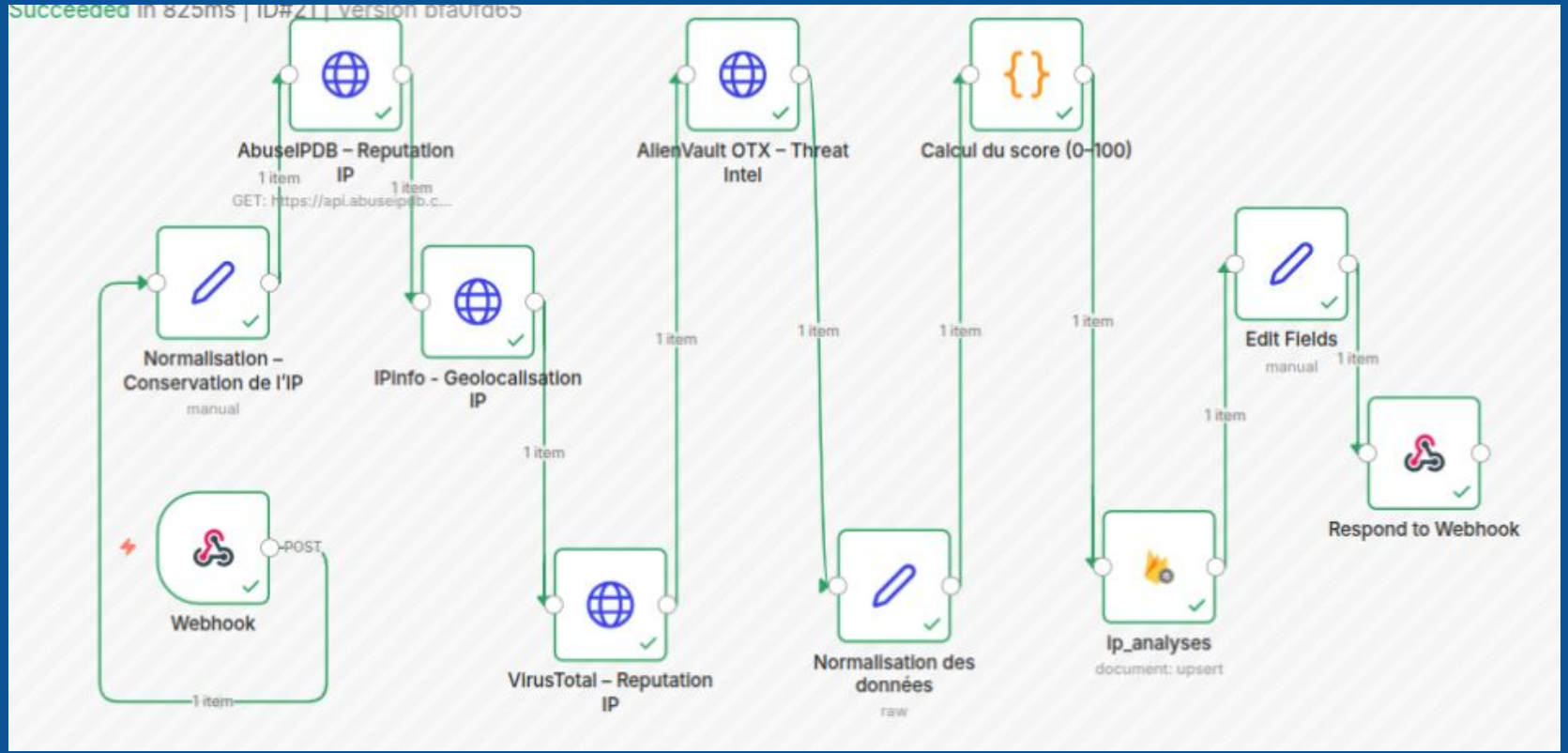
- Orchestrateur
- Leurre (honeypot)
- Liste noire
- Stockage
- Infrastructure
- Frontend

Le résultat est un score reproductible de 0 à 100, stocké dans Firestore.

Itération 2

Infrastructure

Architecture



Interface Web : Objectifs

Itération 3

Création d'une interface web simple pour soumettre une IP et lire le verdict.

Objectif 1 : Interface d'utilisation du système

L'interface la plus simple pour obtenir un verdict immédiat.

- Soumission d'IP publique
- Score de menace (0-100)
- Pays d'origine
- Aucune compétence requise

Itération 3

Objectif 2 : Expérience Utilisateur

Focus sur la simplicité d'usage pour les non-techniciens.

- Parcours : Entrez > Cliquez > Verdict
- Zéro ligne de commande
- Zéro configuration requise
- Verdict visuel en secondes

Itération 3

Objectif 3 : Dualité Admin

Séparation claire entre consultation publique et gestion système.

UI Publique :
Consultation des verdicts IP.

Console Admin :
Workflows n8n, clés API & supervision.

Itération 3

Interface Web : Accessibilité & Gestion

Interface Publique

Consultation simplifiée

Permet de soumettre une IP et consulter son verdict instantanément.

- Score de menace (0-100)
- Niveau de risque (faible, moyen, élevé)
- Aucune compétence technique requise

Itération 3

Console Administration

Gestion & Supervision

Interface dédiée au pilotage technique de la plateforme.

- Gestion des workflows n8n
- Gestion des clés d'API
- Supervision de l'orchestrateur

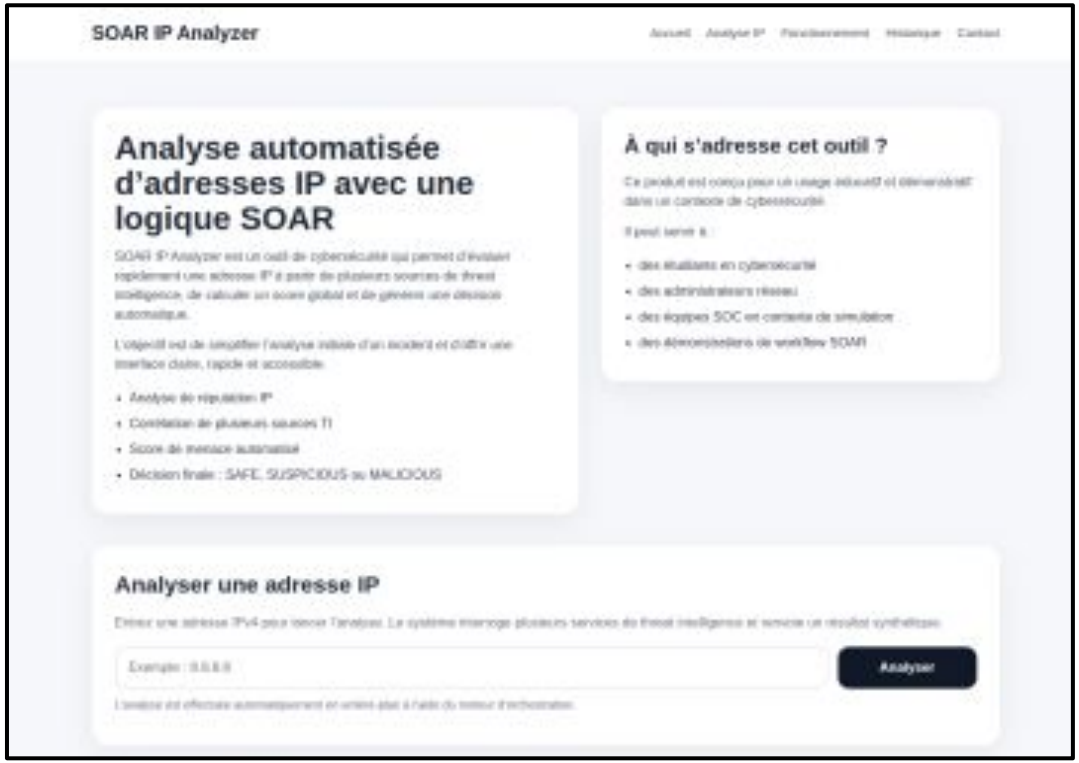
Itération 3

Interface Web : un accès direct à l'outil

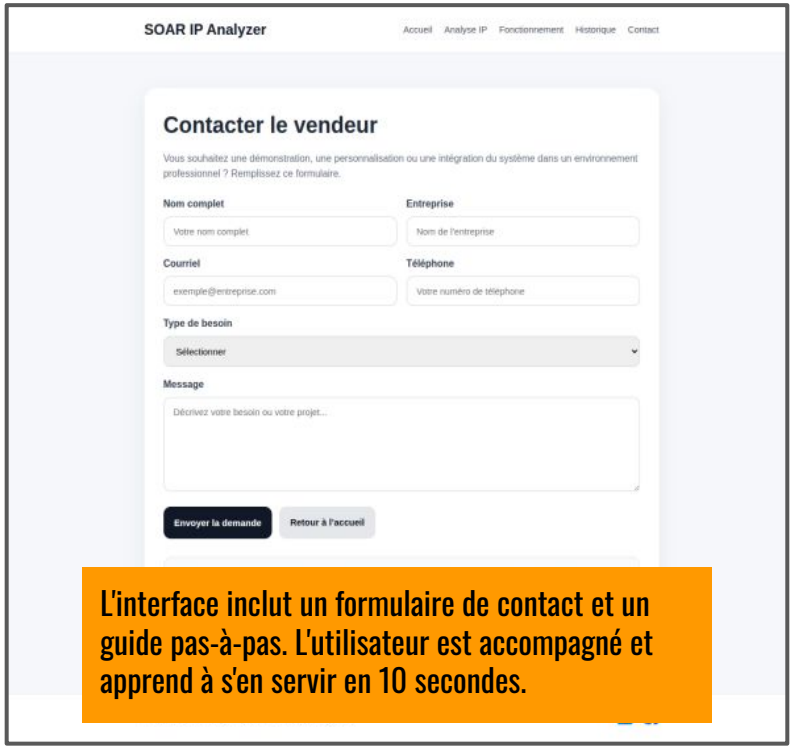
Interface Publique de Consultation simplifiée.

Itération 3

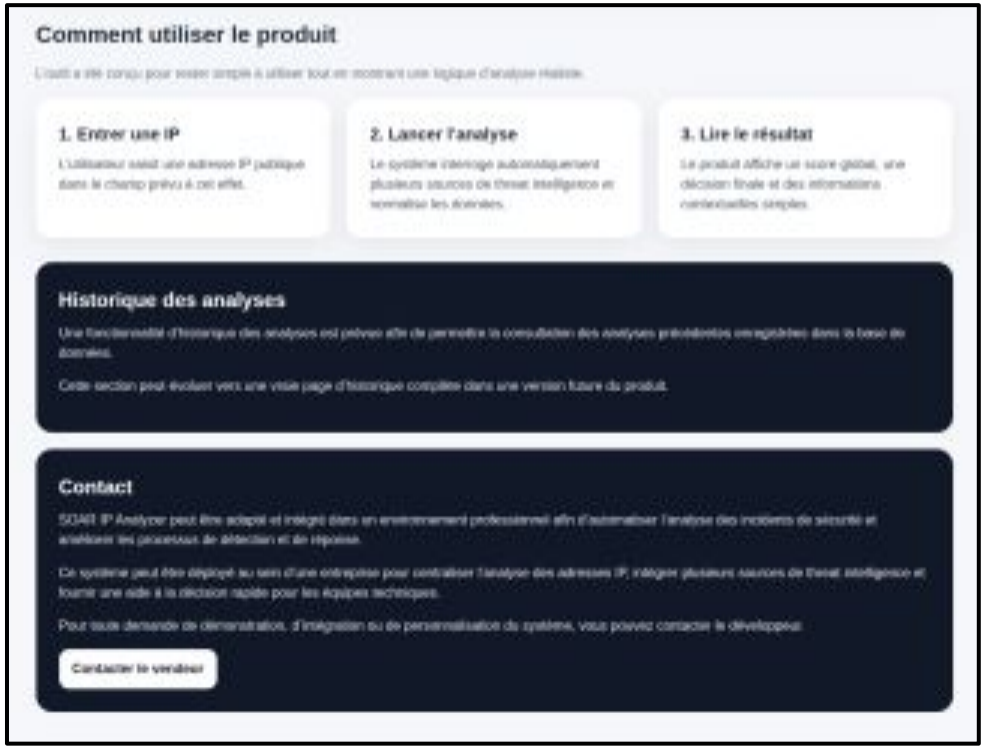
Elle permet de soumettre une IP et de consulter son verdict instantanément, affichant le score de menace (0-100), le niveau de risque (faible, moyen, élevé), et le pays d'origine, sans aucune compétence technique requise.



Interface Web : de l’assistance utilisateur



L'interface inclut un formulaire de contact et un guide pas-à-pas. L'utilisateur est accompagné et apprend à s'en servir en 10 secondes.



Résultats

Réponse Instantanée

Le système SOAR détecte les IPs malicieuses en **quelques secondes**, sans intervention humaine.

Déploiement Agile

L'analyzer SOAR est déployé sur un serveur neuf en **moins de 15 minutes** via script automatisé.

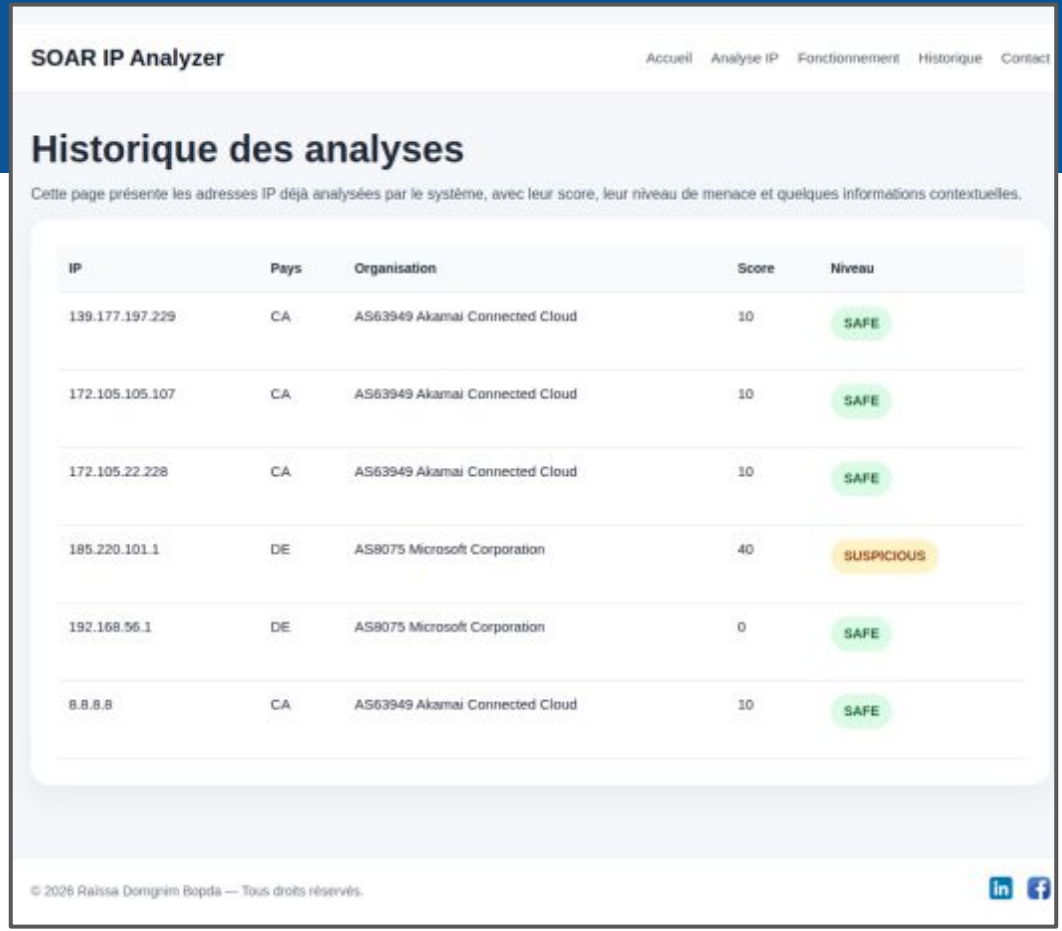
→ Efficacité opérationnelle et automatisation validées

Résultats : Historique

Historique des analyses effectuées pendant les tests. Ces six adresses IP ont servi à valider chaque étape de la chaîne : détection, enrichissement, score, archivage. Les verdicts détaillés sont présentés dans la section Résultats

Six adresses IP testées, six verdicts archivés. Cet historique est le point de départ des résultats présentés plus loin : une IP bénigne (Google DNS), une IP suspecte (nœud de sortie Tor), et quatre IPs d'infrastructure.

Les cas marquants (nœud Tor 185.220.101.1 à 40, Google DNS 8.8.8.8 à 10) sont détaillés dans les diapos Résultats qui suivent.



Résultats
Validation de l'architecture

Déploiement et tests de bout-en-bout

1. Architecture & Sécurité

- **Workflow n8n :** 11 nodes (4 appels API //)
- **Domaines :** UI Publique + Console Admin
- **Sécurité :** HTTPS (Let's Encrypt) + UFW
- **Automatisation :** Script `install.sh` (153 lignes)

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.

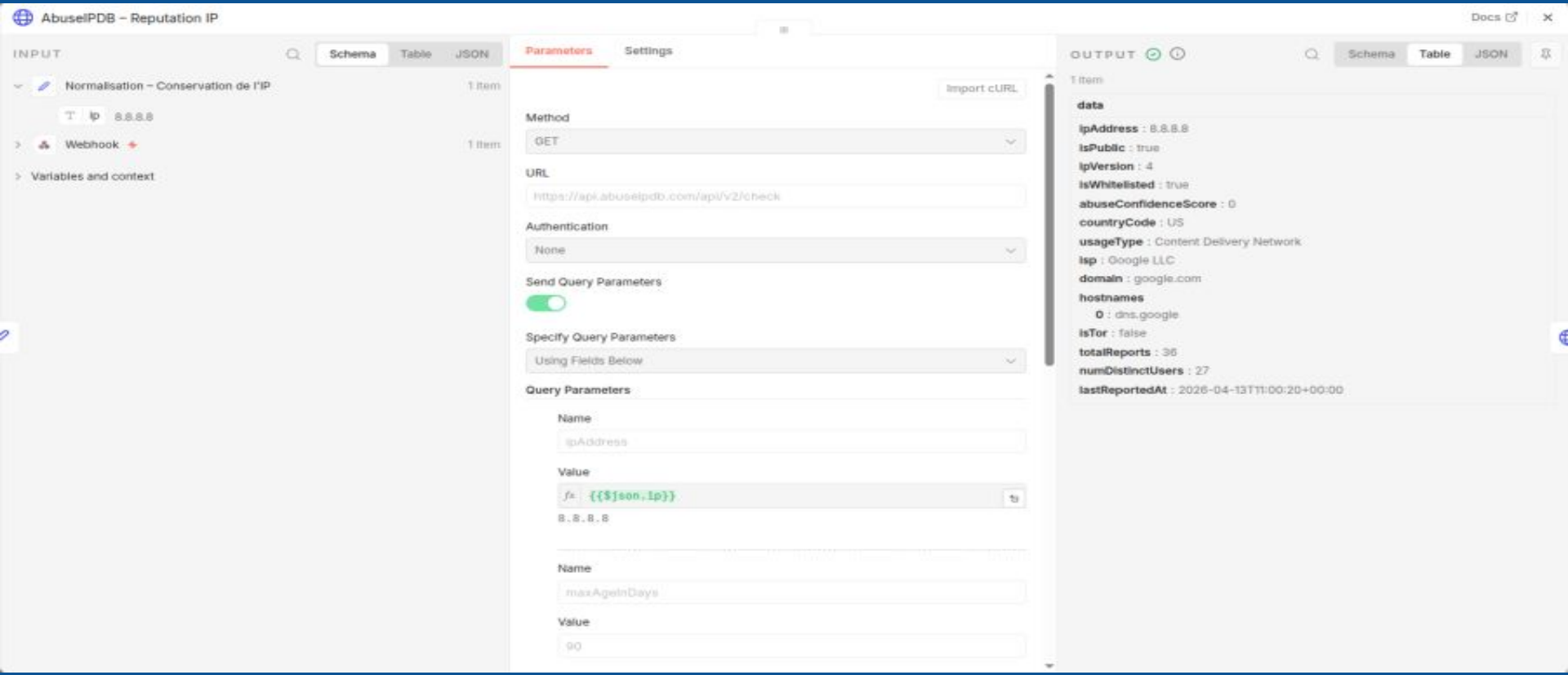
2. Tests & Validation

```
# Test Webhook Local
curl -X POST http://127.0.0.1:5678/...
Payload: {"ip":"8.8.8.8"}
Status: Réponse JSON validée
```

→ Intégrité du système validée

Résultats

Analyse IP bout-en-bout (IP légitime de Google)



Résultats

Analyse IP bout-en-bout (IP légitime de Google)

Paramètres du Test

```
# Analyse de réputation
IP: 8.8.8.8
Type: DNS de Google (Connu)
Score: 10/100
Niveau: Faible
Source: Flag IPinfo (hébergement cloud)
```

Persistance & Validation

- **Stockage :** Document enregistré dans la base Firestore.
- **Collection :** ip_analyses (indexation temps-réel).
- **Workflow :** Validation de la chaîne détection → score → stockage.

→ Chaîne fonctionnelle confirmée

Résultats

Analyse IP bout-en-bout (IP malicieuse)

Paramètres du Test

```
# Analyse de réputation
IP: 185.220.101.1
Type: Tor Exit Node (Connu)
Score: 40/100
Niveau: Moyen
Source: Enrichissement OTX/ABIP
```

Persistance & Validation

- **Stockage :** Document enregistré dans la base Firestore.
- **Collection :** ip_analyses (indexation temps-réel).
- **Workflow :** Validation de la chaîne détection → score → stockage.

→ Chaîne fonctionnelle confirmée

Résultats

Détection réelle capturée par OpenCanary

Logs d'intrusion (18 mars 2026)

```
# opencanary.log
2026-03-18 14:22:01 - SSH.Auth.Started
Port: 2222 (Leurre)
User: fakeuser
Pass: qwerty, 1234
Client: SSH-2.0-OpenSSH_8.2p1
Status: Session intrusion enregistrée
```

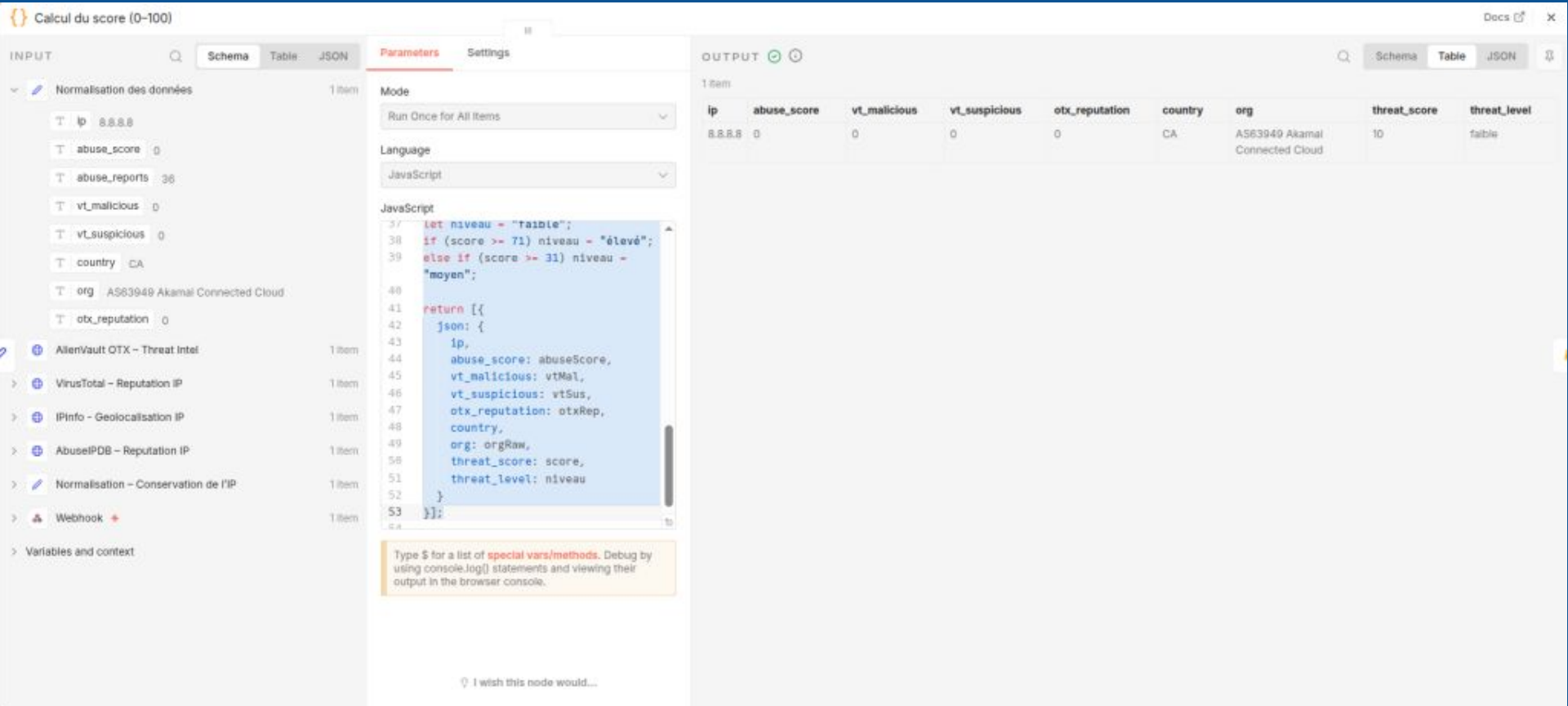
Détails de la capture

- **Service SSH :** Leurre actif sur port non-standard (2222) pour piéger les scans.
- **Credentials :** Capture des dictionnaires de mots de passe courants.
- **Handshake complet :** Métadonnées techniques (version, timestamp) préservées.

→ Preuve de détection et journalisation

Résultats

Calcul du score dans n8n



Résultats : Performance & Sécurité

Workflow & Intégration

- Chaîne : Détection → Score → Décision → Archivage
- 4 sources enrichies en parallèle
- 11 nœuds actifs dans n8n

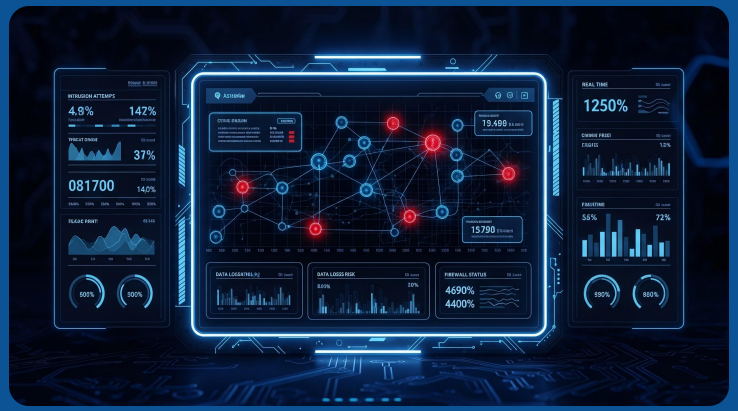
Leurre OpenCanary

Capture réelle de tentatives SSH :

- Mots de passe : `qwerty`, `1234`
- Ex : IP Tor **185.220.101.1**
- Score 40 (Niveau Moyen) → Firestore

Infrastructures & DevOps

- Script `install.sh` (153 lignes)
- HTTPS automatique & Proxy Nginx
- Interfaces : public vs admin



Validation & Déploiement

100%
Tests Webhooks Validés

153
Lignes Script Install

n8n
Workflow Engine

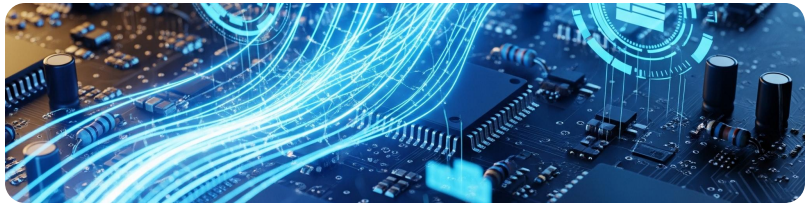
Futur

Optimisations Backend

- Explorer les variations de scoring avec les APIs
- Cacher les informations déjà obtenues (Redis)
- Développer une base de données maison des IPs malicieuses

Expérience & Interface

- Exposer des comptes utilisateurs avec clés d'API
- Visualiser avec des jauges et exports PDF



→ Roadmap évolutive du projet

Perspectives

Évolutions et scalabilité du projet

Améliorations Techniques

- **IA Générative :** Résumé automatique des menaces via LLM.
- **Multi-Cloud :** Redondance entre Google Cloud et AWS.
- **Dashboard :** Visualisation Grafana des pics d'attaques.

Optimisation Performance

```
# Roadmap Performance
- Temps de réponse cible : < 2s
- Cache Redis pour IPs fréquentes
- Parallélisation n8n accrue
Objectif : 1000 requêtes / minute
```

→ Prêt pour la mise en production

Références pour en savoir plus

★ Match parfait avec la technique de scoring

Lewis, J. L., Tambaliuc, G. F., Narman, H. S., et Yoo, W.-S. (2020). IP reputation analysis of public databases and machine learning techniques.

2020 International Conference on Computing, Networking and Communications (ICNC), 181–186. https://doi.org/10.1109/ICNC47757.2020.9049760

Pourquoi :

Ce papier décrit exactement l'approche de cette expérimentation pour le scoring.

- Utilise l'outil **AIPRA** pour interroger plusieurs bases de données publiques de réputation.
- Attribue un score pondéré à chaque IP.
- Implémentation concrète d'une méthode publiée de SOAR.

Références pour en savoir plus

★ Match parfait avec l'architecture SOAR + honeypot

Bartwal, U., Mukhopadhyay, S., Negi, R., et Shukla, S. (2022). Security orchestration, automation, and response engine for deployment of behavioural honeypots.

2022 IEEE Conference on Dependable and Secure Computing (DSC).
https://doi.org/10.1109/DSC54232.2022.9888808

Pourquoi :

Ce papier décrit exactement l'approche de cette expérimentation pour le projet.

- combine SOAR + honeypots
- le cœur conceptuel du projet (OpenCanary + n8n comme orchestrateur).

Références pour en savoir plus

Positionne OpenCanary dans le paysage académique

Ilg, N., Duplys, P., Sisejkovic, D., et Menth, M. (2023). A survey of contemporary open-source honeypots, frameworks, and tools.

Journal of Network and Computer Applications, 220, 103737.
https://doi.org/10.1016/j.jnca.2023.103737

Pourquoi :

- Revue récente des honeypots open source.
- Ancrage académique solide pour OpenCanary.

MERCI