PROJET ACADÉMIQUE // 2025-2026

CYBER CHAOS ARENA

Plateforme SOC intelligente

Détection · Analyse IA · Visualisation · Remédiation manuelle

RÉALISÉ PAR

Laamri Sayf eddine
Asma Bensassi Nour
Halima Badr
Oussama Bagy
Ikram Laabouki

ENCADRÉ PAR

Pr. Ali Azougaghe

ANNÉE UNIVERSITAIRE

2025 — 2026

Contexte et problématique

01

Menaces en hausse

Attaques web et systèmes plus fréquentes, plus automatisées, plus variées.

02

Détection seule, insuffisante

Les approches classiques s'arrêtent à l'alerte, sans contexte ni décision.

03

Le SOC doit décider

Détecter, analyser, visualiser, et aider à la remédiation.

ATTAQUANT

Payloads, scans, bruteforce

SYSTÈME CIBLÉ

Application web · API · Hôte

SOC

Observe, analyse, décide

PROBLÉMATIQUE | Comment suivre une attaque de bout en bout, de la requête initiale à la décision de remédiation ?

Six objectifs, une chaîne SOC complète

01

Détection temps réel

NGINX + WAF ModSecurity, règles OWASP CRS sur chaque requête entrante.

02

Redirection honeypot

Isolation des comportements suspects dans un environnement piégé.

03

Analyse IA locale

Ollama classifie l'attaque et génère un rapport JSON structuré.

04

Visualisation Grafana

Dashboards SOC : IP sources, types d'attaques, MITRE, criticité.

05

Aide à la décision SOC

L'analyste consulte le rapport IA et choisit l'action de remédiation.

06

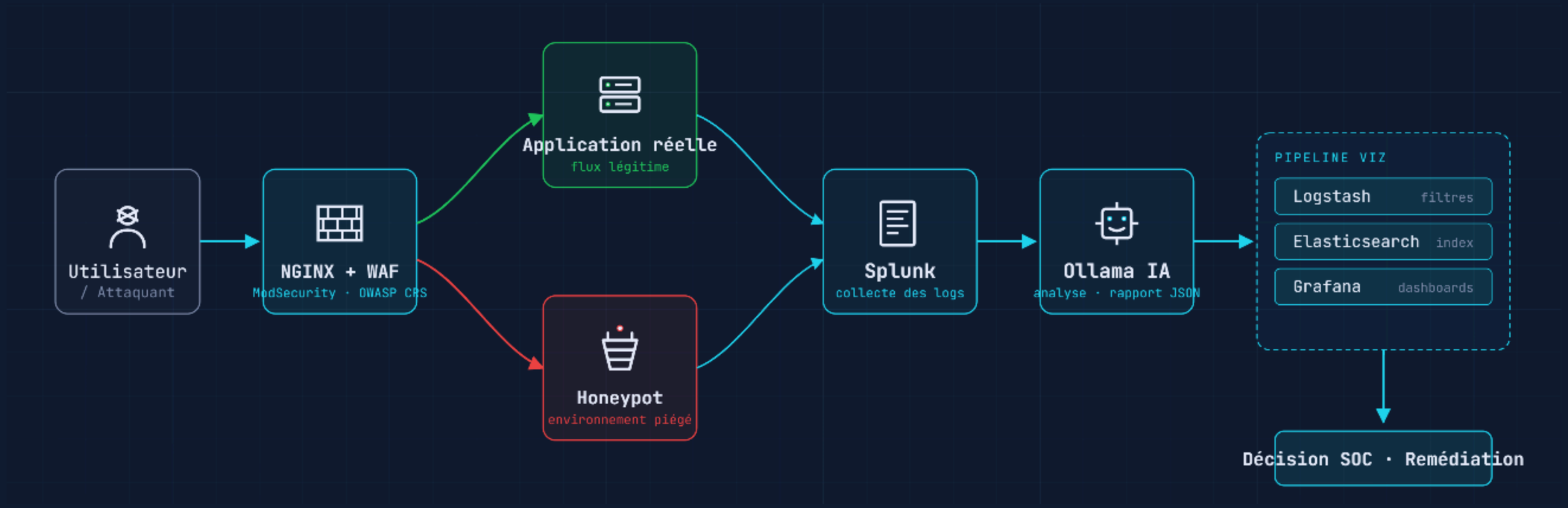
Remédiation réversible

Blacklist manuelle, rollback en un clic pour neutraliser les faux positifs.

Architecture globale du SOC

● TRAFIC NORMAL → APPLICATION RÉELLE

● TRAFIC SUSPECT → HONEYPOT



Passerelle de sécurité NGINX/WAF

Reverse proxy NGINX

Point d'entrée unique du trafic vers les applications back-end.

WAF ModSecurity

Règles OWASP CRS appliquées en temps réel à chaque requête.

Détection des payloads suspects

SQLi · XSS · Path traversal · Brute force · Command injection.

Routage intelligent

Application réelle ou honeypot selon le verdict du WAF.

Passerelle de sécurité NGINX/WAF

Reverse proxy NGINX

Point d'entrée unique du trafic vers les applications back-end.

WAF ModSecurity

Règles OWASP CRS appliquées en temps réel à chaque requête.

Détection des payloads suspects

SQLi · XSS · Path traversal · Brute force · Command injection.

Routage intelligent

Application réelle ou honeypot selon le verdict du WAF.

Utilisateur normal vs attaquant

● UTILISATEUR NORMAL

- Identifiants valides
- Requêtes conformes
- Comportement attendu

ROUTE APPLICATION RÉELLE

● ATTAQUANT

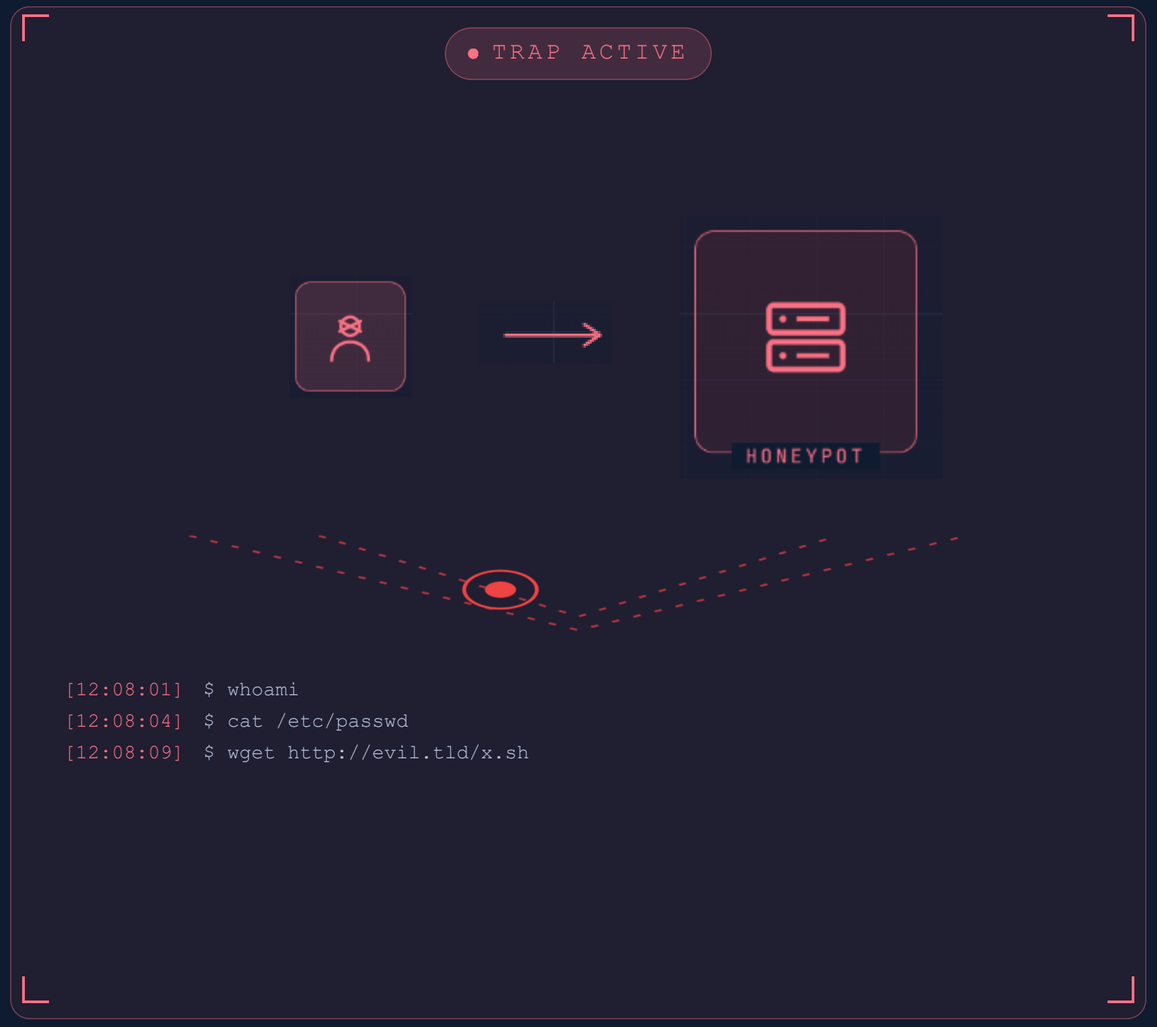
- Payload suspect
- Comportement anormal
- Détection WAF déclenchée

ROUTE HONEYPOT

FAMILLES DÉTECTÉES

SQL INJECTION | BRUTE FORCE | XSS | PATH TRAVERSAL

Honeypot et environnement piégé



MISSION

Attirer, isoler et observer l'attaquant — sans risque pour l'application réelle.

TYPES DE COMPORTEMENTS DÉTECTÉS

01 · EXEC
Command execution
whoami · curl · wget

02 · FILE
Sensitive file access
/etc/passwd · /etc/shadow

03 · PRIV
Privilege escalation
sudo · su · setuid

04 · NET
Network reconnaissance
nmap · ping · netcat

Exemple d'attaque observée dans le honeypot

FLUX DES ÉVÉNEMENTS

01 **Honeypot**
capture des commandes

02 **Logs structurés**
timestamp · src_ip · cmd

03 **Splunk**
centralisation & index

Splunk — collecte et centralisation des logs

NGINX + WAF
access · audit · modsec

Honeypot
commands · file · net

01
Collecte des logs
forwarders & ingestion

02
Recherche des événements
SPL · filters · time-range

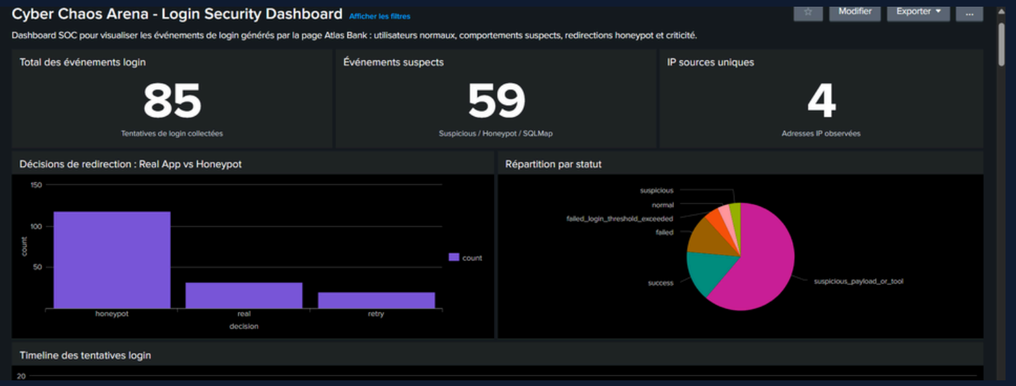
03
Suivi des incidents
corrélation · timeline

Splunk — collecte et centralisation des logs

01

Collecte des logs

forwarders & ingestion



02

Recherche des événements

SPL · filters · time-range

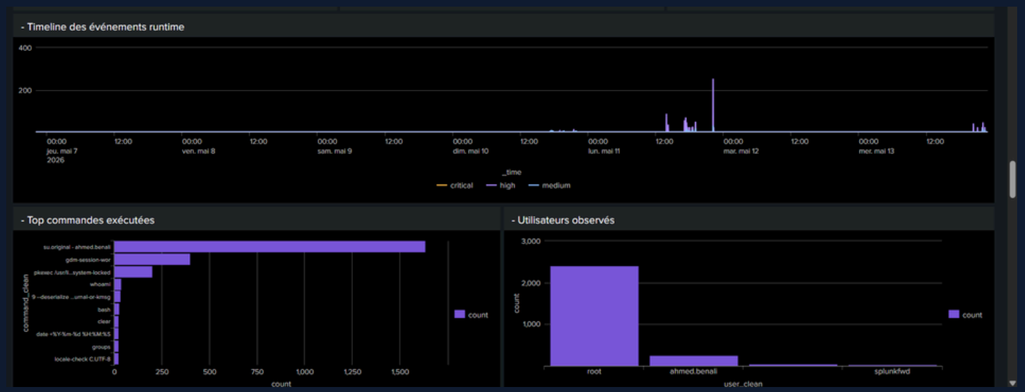
Alertes normalisées pour Ai

_time	source_ip	event	count	time_window	severity	source_module	usernames
2026-05-13 22:26:00	172.17.0.2	command_execution	1	2 minutes	medium	oussama_honeypot_runtime	
2026-05-13 22:22:00	172.17.0.2	command_execution	3	2 minutes	medium	oussama_honeypot_runtime	
2026-05-13 22:20:00	10.79.241.98	failed_login	2	2 minutes	medium	ikram_login_gateway	admin OR 1=1
2026-05-13 22:20:00	172.17.0.2	command_execution	35	2 minutes	medium	oussama_honeypot_runtime	
2026-05-13 22:12:00	10.79.241.63	failed_login	2	2 minutes	medium	ikram_login_gateway	fake3
2026-05-13 22:08:00	10.79.241.63	failed_login	2	2 minutes	medium	ikram_login_gateway	admin
2026-05-13 22:02:00	172.17.0.2	command_execution	6	2 minutes	medium	oussama_honeypot_runtime	

03

Suivi des incidents

corrélation · timeline



DÉFINITION D'OLLAMA ET DU MODÈLE UTILISÉ

01

Ollama : Moteur d'exécution local de LLM

Plateforme open-source exécutant des modèles de langage (LLM) via une API REST, facilitant l'intégration IA sans dépendance cloud.

02

Modèle d'Analyse : Gemma 4B

Utilisation du modèle compact de Google, optimisé pour la détection efficace des schémas d'attaque.

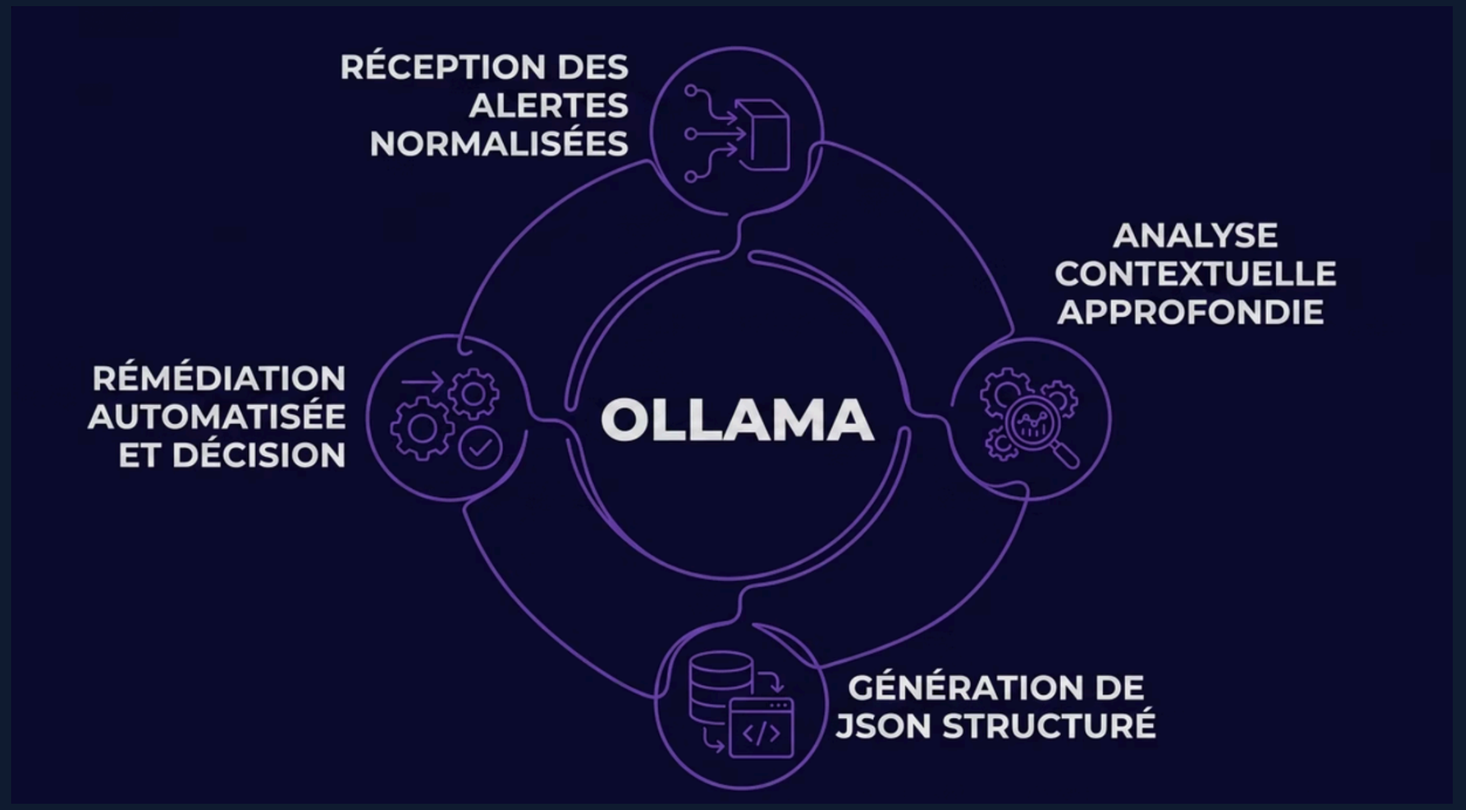
Rôle Clé dans le Projet

Fonctionne comme moteur d'analyse IA pour traiter et qualifier les alertes de cybersécurité normalisées.

Avantages Stratégiques

confidentialité des données grâce au traitement local , faible latence, intégration simplifiée avec Flask et génération de réponses JSON structurées.

OLLAMA AU COEUR DU SOC : OBJECTIF DE L'ANALYSE IA



OLLAMA EST LE MOTEUR D'IA LOCAL CENTRAL DE NOTRE PLATEFORME SOC. SA MISSION EST DE TRANSFORMER LES ALERTES BRUTES EN INTELLIGENCE ACTIONNABLE, PERMETTANT UNE REMÉDIATION RAPIDE ET ÉCLAIRÉE.

rapport généré par l'IA

Après la réception des alertes normalisées, notre moteur d'analyse IA, Ollama, intervient comme le cerveau central de la chaîne SOC. Son rôle est de transformer ces données brutes en renseignements actionnable


```
{   "event_type": "path_traversal",   "severity":
"critical",   "src_ip":     "10.79.241.63",
"attack_type":"Directory Traversal",   "mitre":
"T1083 — File and Directory Discovery",
"confidence": 98,   "recommendation": "Block
source IP and investigate host",   "action":
"ban_ip" }
```


01. Enrichissement des Données

Identification précise du type d'attaque (SQLi, Brute Force), de sa tactique, et mapping aux techniques MITRE ATT&CK.

02. Évaluation du Risque

Génération d'une sévérité (severity), d'un score de confiance (confidence) et d'un score de risque (risk_score) pour chaque alerte.

Recommandations & Actions

Proposition d'actions de remédiation spécifiques et standardisées pour guider les équipes de sécurité ou déclencher des automatisations.

REMÉDIATION & AUTOMATISATION (SOAR)

Blacklist dynamique

Ajout/suppression d'IP via fichier utilisé par NGINX; rechargement dynamique.

Redirection vers honeypot

Orienter les sources suspectes pour observation plutôt que blocage immédiat.

ollama_report_3a91.json

SEV CRITICAL


```
{ "event_type": "path_traversal", "severity": "critical", "src_ip": "10.79.241.63", "attack_type":"Directory Traversal", "mitre": "T1083 — File and Directory Discovery", "confidence": 98, "recommendation": "Block source IP and investigate host", "action": "ban_ip" }
```


TYPE D'ATTAQUE

Directory Traversal

MITRE T1083

CRITICITÉ

Critical · 98%

RECOMMANDATION

Block source IP & investigate host

action: ban_ip

- L'IA ne bloque pas. Elle propose.
- Elle assiste l'analyste SOC.
- L'humain décide de la remédiation.

Chaîne de visualisation SOC

LOGSTASH
Reçoit le rapport JSON, applique les filtres, normalise le schéma.

ELASTICSEARCH
Indexe les événements et autorise la recherche en quasi temps réel.

GRAFANA
Affiche les tableaux de bord SOC en thème sombre, lisible 24/7.

Validation de la visualisation

```
asma@asma:~/cyber-chaos-arena-asma$ curl -i -X POST http://localhost:8088 \
-H "Content-Type: application/json" \
-d '{
  "source_type": "test_visualisation",
  "source_owner": "test_local",
  "event_type": "path_traversal",
  "severity": "critical",
  "src_ip": "10.79.241.63",
  "attack_type": "Directory Traversal",
  "mitre": "T1083 - File and Directory Discovery",
  "risk_score": 9,
  "confidence": 98,
  "message": "Test report sent to Logstash for visualization",
  "recommendation": "Block source IP and investigate host",
  "action": "ban_ip"
}'
HTTP/1.1 200 OK
content-length: 2
content-type: text/plain
```

Tableau de bord SOC

Remédiation manuelle et rollback

01 · ALERTE

Alerte Grafana

dashboard SOC

02 · HUMAIN

Analyse SOC

validation analyste

03 · ACTION

Ajout blacklist

IP source

04 · ISOLATION

Redirection honeypot

trafic isolé

05 · ROLLBACK

Suppression possible

faux positif

ROLLBACK — RESTORE ACCESS

Décision basée sur Grafana

Validation humaine obligatoire

Réversible — pas de point de non-retour

Validation de bout en bout

SCÉNARIO REJOUÉ

- T+00 Attaque entrante (path traversal)
- T+01 Détection NGINX/WAF · redirection honeypot
- T+02 Collecte Splunk · index temps réel
- T+04 Analyse Ollama · rapport JSON
- T+05 Logstash · Elasticsearch · Grafana
- T+06 Décision SOC · remédiation manuelle

● VALIDÉ 7 / 7

- Collecte Splunk
- Analyse Ollama
- Envoi Logstash
- Affichage Grafana
- Ajout blacklist
- Redirection honeypot
- Rollback testé

Conclusion et perspectives

CONCLUSION

- Chaîne SOC complète — détection, IA, visualisation, remédiation.
- Architecture modulaire et démontrable, composant par composant.
- Protection active de l'application réelle via le honeypot.
- Décision finale humaine, garantie par le rollback.

PERSPECTIVES

- Corrélation automatique des événements multi-sources.
- Enrichissement du moteur de règles de détection.
- Remédiation partiellement automatisée, sous validation humaine.
- Alertes temps réel avancées · canaux messagerie / e-mail.
- Classification MITRE plus fine et plus exhaustive.

> Une plateforme SOC intelligente, modulaire et orientée décision.

— MEMERCI