AYI NEDJIMI Consultants

Wazuh SIEM/XDR : Guide Déploieme

30 April 2026 • Mis à jour le 30 April 2026 • 45 min de lecture

Guide complet Wazuh SIEM/XDR : architecture, déploiement Docker/K8s, a intégration TheHive/MISP/Shuffle.

Le déploiement d'un **SIEM open source** performant et évolutif est un enjeu stratég cherchant à renforcer leur posture de sécurité sans les coûts prohibitifs des soluti sécurité combinant les capacités de **SIEM** (Security Information and Event Manag de conformité, s'est imposée comme la référence incontestée de la détection des d'agents déployés dans le monde en 2026. Héritier d'OSSEC enrichi par une archi (moteur d'analyse et de corrélation), des **agents** (collecte endpoint), de l'**Indexer** **Dashboard** (visualisation et investigation), Wazuh offre un écosystème complet co **Monitoring (FIM)**, le **Security Configuration Assessment (SCA)**, la **détection de v** l'intégration avec les plateformes SOAR (**Shuffle**, **TheHive**, **MISP**). Ce guide exper infrastructure Wazuh complète — du single node aux architectures cluster multi-n personnalisées pour les environnements Active Directory, Microsoft 365 et AWS, l haut volume, et les intégrations avancées qui transforment Wazuh en plateforme S essentiels et des méthodologies de threat hunting proactif.

À RETENIR

Points clés de cet article :

- Wazuh est une plateforme unifiée SIEM + XDR + Compliance open source
  mondialement
- L'architecture se compose de 4 éléments : Manager (analyse), Agents (col
- Le déploiement supporte le single node, le cluster multi-nœuds, Docker e
- Les capacités natives incluent : FIM, SCA, détection de vulnérabilités, rootk
- Le système de rules/decoders permet une personnalisation complète de la
- Les CDB lists enrichissent les règles avec des IOC, allowlists et contexte ex
- Les intégrations TheHive, MISP et Shuffle SOAR transforment Wazuh en pl
- Le tuning de performance (indexer shards, worker threads, queue sizes) es

Architecture Wazuh : composants et flux de données

L'architecture Wazuh est conçue selon un modèle distribué modulaire où chaque c
chaîne de collecte, analyse, stockage et visualisation des événements de sécurité
indépendant de chaque couche en fonction de la volumétrie et des exigences de p

Wazuh Manager (serveur d'analyse)

Le **Wazuh Manager** est le cœur du système, responsable de la réception des évé
decoders (parsing et normalisation), de l'évaluation des **rules** (détection), et de la
configuration centralisée des agents, la distribution des politiques de sécurité (SC
actions de réponse automatique (Active Response). Le manager maintient une bas