SIEM open source 2026 : Wazuh vs ELK vs OpenSearch vs Graylog

> Comparatif SIEM open source 2026 : Wazuh 4.x, ELK Stack, OpenSearch et Graylog analysés sur 7 critères — performances, déploiement, alerting et coût total.

Le choix d'un SIEM (Security Information and Event Management) est une décision structurante pour toute organisation souhaitant centraliser sa détection des menaces et sa réponse aux incidents. Les solutions commerciales — Splunk, IBM QRadar, Microsoft Sentinel — offrent des fonctionnalités avancées mais à des coûts qui peuvent rapidement atteindre plusieurs centaines de milliers d'euros par an pour des volumes de logs significatifs. Face à ce constat, les SIEM open source ont considérablement mûri depuis 2020, notamment Wazuh qui intègre désormais des capacités XDR complètes, et OpenSearch qui propose une alternative Apache-licensée à Elasticsearch. En 2026, les quatre acteurs principaux de l'écosystème open source — Wazuh 4.x, ELK Stack, OpenSearch et Graylog — couvrent la quasi-totalité des besoins d'une organisation, de la PME de 20 postes au SOC avancé d'une ETI. Ce guide compare objectivement ces solutions sur sept critères clés, propose des recommandations par profil d'organisation, et inclut un guide de déploiement Docker Compose Wazuh 4.x opérationnel en moins d'une heure.

À RETENIR

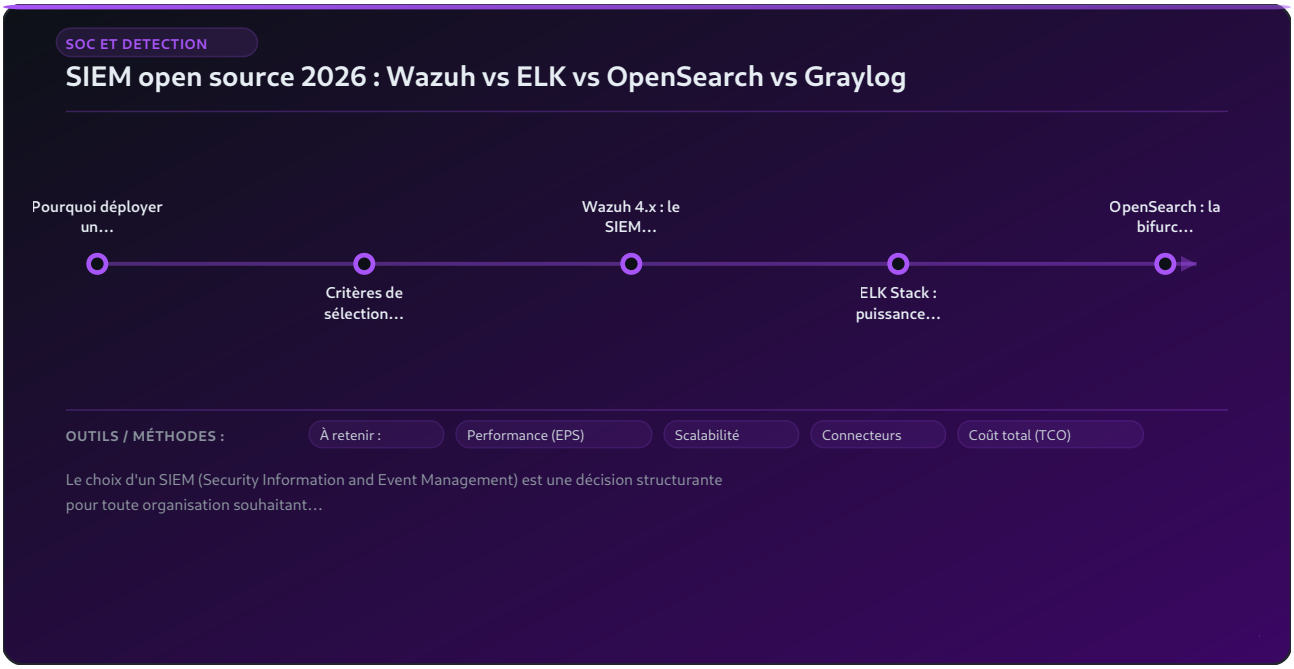
À retenir :

Wazuh 4.x est la solution la plus complète pour les PME et ETI grâce à son XDR intégré et ses règles MITRE ATT&CK préconfigurées.

ELK Stack offre la meilleure scalabilité mais sa complexité de déploiement et ses coûts d'infrastructure le réservent aux équipes techniques avancées.

OpenSearch est le meilleur choix pour les organisations soucieuses de la souveraineté et allergiques aux changements de licence Elastic.

> Graylog se distingue par sa simplicité d'administration et sa courbe d'apprentissage douce, idéale pour les équipes IT débutant en SIEM.



Pourquoi déployer un SIEM open source en 2026

Le coût est l'argument le plus visible, mais pas le seul. Un déploiement Splunk Enterprise pour 50 Go/jour dépasse typiquement 80 000 € par an de licence. Microsoft Sentinel facture à l'ingestion (environ 2,76 € par Go analysé) avec une facture mensuelle imprévisible pour les environnements dynamiques. Les SIEM open source permettent d'allouer ce budget aux ressources humaines — l'analyste SOC qui crée et maintient les règles de détection — plutôt qu'aux licences logicielles.

La souveraineté des données est un second argument structurant. Confier ses logs de sécurité — qui contiennent les activités de tous les utilisateurs, les connexions aux systèmes critiques, les tentatives d'intrusion — à un fournisseur cloud américain soulève des questions de conformité RGPD et de protection des données sensibles. Un SIEM open source hébergé on-premises ou sur une infrastructure cloud souveraine (OVHcloud, Scaleway) élimine cette dépendance.

Enfin, la flexibilité d'intégration des SIEM open source surpasse souvent celle des solutions commerciales. Les connecteurs sont développés par la communauté et couvrent rapidement les nouvelles technologies : conteneurs Kubernetes, fonctions serverless, APIs cloud natives. L'absence de vendor lock-in permet de migrer ou d'évoluer sans pénalités contractuelles.

Critères de sélection d'un SIEM open source

Avant de comparer les solutions, définissons les sept critères d'évaluation :

> ⚡ **Retour terrain**
>
> Pour un groupe de services financiers qui recevait 2 millions d'alertes SIEM par jour et en traitait 3 %, j'ai réalisé une analyse de la valeur des règles de détection sur 6 mois de logs. Résultat : 73 % des alertes provenaient de 4 règles mal calibrées. La suppression ou le réajustement de ces 4 règles a réduit le bruit de 65 % sans manquer aucun incident réel lors des 3 mois de validation. Le ROI d'un tuning SIEM est parmi les meilleurs investissements défensifs possibles.

Performance (EPS) : Capacité à ingérer et indexer des Events Per Second sans perte ni dégradation de la latence d'alerte

Scalabilité : Architecture horizontalement scalable, gestion des clusters, réplication des données

Connecteurs : Nombre et qualité des intégrations natives (agents, syslog, API, cloud connectors)

Alerting : Qualité des règles préconfigurées, facilité de création de règles custom, gestion des faux positifs

Coût total (TCO) : Infrastructure, maintenance, formation, support communautaire ou commercial

Conformité : Mappings MITRE ATT&CK, frameworks PCI-DSS, ISO 27001, NIS 2 natifs

Support : Qualité de la documentation, activité de la communauté, options de support commercial

---

Wazuh 4.x : le SIEM XDR open source de référence

Wazuh est né comme un fork d'OSSEC et a profondément évolué pour devenir une plateforme XDR (Extended Detection and Response) complète. La version 4.x, sortie en 2023 et maintenue activement en 2026, intègre nativement un moteur de détection basé sur des règles XML, un agent endpoint multi-plateforme (Windows, Linux, macOS, conteneurs), et un tableau de bord Kibana/OpenSearch Dashboards personnalisé. Pour un guide de déploiement complet, consultez notre article sur Wazuh SIEM/XDR : déploiement et détection.

Architecture Wazuh 4.x

Wazuh 4.x repose sur trois composants :

Wazuh Manager : Traitement des événements, application des règles de détection, corrélation des alertes. C'est le cerveau de la plateforme.

Wazuh Indexer : Moteur de recherche et d'indexation basé sur OpenSearch, stockage des alertes et des logs bruts.

Wazuh Dashboard : Interface web de visualisation, investigation et configuration, basée sur OpenSearch Dashboards.

Forces de Wazuh : Détection XDR intégrée (SIEM + EDR + CSPM), plus de 3 000 règles préconfigurées avec mapping MITRE ATT&CK, agent léger (2-5% CPU), intégration native VirusTotal, YARA et MISP, modules de conformité PCI-DSS, HIPAA, NIST, TSC, et un déploiement simplifié par rapport à ELK. La communauté francophone est active et la documentation est complète.

Limites de Wazuh : La scalabilité au-delà de 10 000 agents nécessite une architecture distribuée complexe. Les capacités de recherche full-text et de corrélation complexe restent inférieures à

ELK pour les volumes très élevés. Le machine learning intégré est moins avancé que les solutions commerciales.

ELK Stack : puissance et complexité

L'ELK Stack (Elasticsearch + Logstash + Kibana), rebaptisé "Elastic Stack" avec l'ajout de Beats, est la solution de référence mondiale pour la centralisation et l'analyse de logs. Sa scalabilité horizontale permet d'ingérer des centaines de gigaoctets par jour sur des clusters distribués. Cependant, la complexité de déploiement et de maintenance est significativement supérieure aux autres solutions.

Forces d'ELK : Scalabilité exceptionnelle, recherche full-text ultra-performante, écosystème de connecteurs Beats très riche (Filebeat, Winlogbeat, Packetbeat, Auditbeat), Kibana Lens pour des visualisations avancées, et une communauté mondiale massive.

Limites d'ELK : Le changement de licence en 2021 (Server Side Public License - SSPL) a rompu la compatibilité avec l'open source pur. Les fonctionnalités de sécurité avancées (RBAC, alerting ML) sont désormais réservées à la licence Elastic payante. Le coût d'infrastructure est élevé : un cluster Elasticsearch performant nécessite au minimum 3 nœuds avec 16 Go RAM chacun. La complexité de Logstash (pipeline de transformation) représente une courbe d'apprentissage significative.

OpenSearch : la bifurcation libre d'AWS

OpenSearch est un fork d'Elasticsearch 7.10 initié par Amazon Web Services en 2021 en réponse au changement de licence Elastic. Distribué sous licence Apache 2.0, il garantit une compatibilité open source pérenne et inclut nativement des fonctionnalités de sécurité qui étaient payantes dans Elastic. Pour des conseils sur l'écriture de règles de détection compatibles, consultez notre guide sur les Sigma Rules.

Différences avec ELK : Licence Apache 2.0 (vs SSPL Elastic), sécurité native gratuite (authentification, chiffrement, RBAC), OpenSearch ML Commons pour le machine learning distribué, et une API compatible avec Elasticsearch (migration transparente).

Forces d'OpenSearch : Souveraineté des données (pas de dépendance AWS si hébergé on-premises), sécurité native complète sans coût supplémentaire, adoption croissante dans les environnements gouvernementaux et réglementés (notamment en Allemagne et en France), intégration native avec les services AWS si déployé sur AWS OpenSearch Service.

Limites : Écart fonctionnel croissant avec Elasticsearch (les nouvelles fonctionnalités Elastic ne sont pas portées dans OpenSearch), communauté plus petite que ELK, moins de plugins tiers disponibles.

Graylog : la simplicité avant tout

Graylog se distingue par une approche radicalement différente : privilégier la simplicité d'administration sur la scalabilité maximale. Basé sur Elasticsearch ou OpenSearch pour l'indexation, et MongoDB pour la configuration, Graylog offre une interface utilisateur intuitive et des concepts accessibles aux équipes IT sans expertise approfondie en data engineering.

Concepts clés : Les Streams filtrent les messages entrants et les routent vers des destinations ou déclenchent des alertes. Les Pipeline Rules permettent de normaliser et d'enrichir les logs en temps réel. Les Content Packs fournissent des tableaux de bord et des alertes préconfigurés pour des sources communes (Windows Event Logs, Nginx, AWS CloudTrail).

Forces de Graylog : Déploiement rapide (1-2 heures), interface administrative claire, gestion native du protocole GELF (Graylog Extended Log Format) plus riche que syslog, et une version Enterprise disponible pour les organisations nécessitant un support commercial.

Limites : Dépendance à MongoDB ajoute un composant à maintenir, scalabilité limitée au-delà de quelques dizaines de Go/jour sans architecture distribuée complexe, fonctionnalités XDR inexistantes (pas d'agent endpoint, pas de détection comportementale native).

Tableau comparatif sur 7 critères

Ce tableau synthétise l'évaluation des quatre solutions sur une échelle de 1 (insuffisant) à 5 (excellent) :

Critère	Wazuh 4.x	ELK Stack	OpenSearch	Graylog
Performance (EPS)	3	5	4	3
Facilité déploiement	4	2	3	5
Connecteurs	4	5	4	3
Alerting	4	4	3	4
Coût total (TCO)	5	2	4	4
Conformité	5	3	3	2
Support communauté	4	5	3	4
TOTAL	29	26	24	25

Wazuh 4.x émerge comme la solution la plus équilibrée pour la majorité des organisations, grâce à sa combinaison unique de facilité de déploiement, de coût total maîtrisé, et de capacités de conformité natives. ELK domine sur les critères de performance et d'écosystème de connecteurs, mais son TCO élevé le pénalise pour les budgets limités.

Recommandations par profil d'organisation

PME jusqu'à 50 postes : Wazuh 4.x en déploiement monolithique (Manager + Indexer + Dashboard sur un seul serveur 8 vCPU / 16 Go RAM). Coût infrastructure : environ 150-200 €/mois sur VPS. Couverture MITRE ATT&CK native, pas de configuration complexe requise. Graylog est une alternative si l'équipe est très petite et sans expertise sécurité.

ETI (50 à 500 postes) : Wazuh 4.x en architecture distribuée (Manager séparé, cluster Indexer à 3 nœuds) ou stack hybride Wazuh + ELK (décrite ci-dessous). Budget infrastructure : 500-1 500 €/mois. OpenSearch comme moteur d'indexation pour maximiser la souveraineté.

SOC avancé (500+ postes, volumes > 50 Go/jour) : ELK Stack avec cluster Elasticsearch 5+ nœuds, Logstash en pipeline distribué, et enrichissement MISP/TIP. Envisager une migration vers Microsoft Sentinel ou Splunk si le TCO devient plus avantageux que la maintenance de l'infrastructure. Voir notre comparatif avec Microsoft Sentinel.

Stack hybride : Wazuh + ELK pour le meilleur des deux mondes

Pour les organisations qui apprécient les capacités XDR de Wazuh mais ont besoin de la puissance de recherche et de visualisation d'ELK, une architecture hybride est possible. Wazuh gère la collecte et la détection via ses agents, et transfère les alertes vers un cluster Elasticsearch séparé via l'API Wazuh ou un shipper Filebeat.

Cette approche offre le meilleur des deux mondes : agents Wazuh pour la détection comportementale et le monitoring d'intégrité des fichiers (FIM), et Elasticsearch pour le stockage à long terme, les recherches ad-hoc complexes, et les tableaux de bord Kibana avancés. La complexité opérationnelle est cependant doublée. Pour une mise en oeuvre structurée, consultez notre article sur la détection des attaques AD avec Wazuh.

Déploiement Docker Compose Wazuh 4.x en 10 commandes

Ce guide de déploiement rapide permet d'avoir un Wazuh 4.x fonctionnel en moins d'une heure sur un serveur Linux avec Docker et Docker Compose installés (prérequis : 8 vCPU, 16 Go RAM, 100 Go disque SSD) :

```
 # 1. Cloner le dépôt officiel Wazuh Docker
git clone https://github.com/wazuh/wazuh-docker.git -b v4.8.0

# 2. Entrer dans le répertoire single-node
cd wazuh-docker/single-node

# 3. Générer les certificats SSL
docker compose -f generate-indexer-certs.yml run --rm generator

# 4. Ajuster les limites système pour Opensearch
echo "vm.max_map_count=262144" | sudo tee -a /etc/sysctl.conf
sudo sysctl -p

# 5. Démarrer la stack complète
docker compose up -d

# 6. Vérifier le statut des conteneurs
docker compose ps

# 7. Attendre l'initialisation complète (2-3 minutes)
docker compose logs -f wazuh.manager | grep "Wazuh started"

# 8. Accéder au dashboard (HTTPS port 443)
# URL: https://VOTRE_IP — admin / SecretPassword (changer obligatoirement)

# 9. Déployer un agent Windows (depuis PowerShell admin sur le poste client)
# Invoke-WebRequest -Uri "https://VOTRE_IP/packages/wazuh-agent.msi" -OutFile agent.msi
# msiexec /i agent.msi WAZUH_MANAGER="VOTRE_IP" /q

# 10. Déployer un agent Linux
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --dearmor |   sudo tee /usr/share/keyr
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable ma
sudo apt-get update && sudo apt-get install wazuh-agent
sudo WAZUH_MANAGER="VOTRE_IP" systemctl enable --now wazuh-agent
```

Après le déploiement, configurez au minimum les modules de conformité (PCI-DSS, NIST 800-53) et les intégrations VirusTotal pour l'enrichissement des alertes de fichiers suspects. La documentation officielle est disponible sur wazuh.com/docs et le projet OpenSearch sur opensearch.org.

FAQ — Questions fréquentes sur les SIEM open source

Wazuh peut-il remplacer un EDR commercial comme CrowdStrike ou SentinelOne ?

Wazuh couvre un sous-ensemble significatif des fonctionnalités EDR : monitoring de l'intégrité des fichiers (FIM), détection de rootkits, inventaire des processus et connexions réseau, analyse des logs système, et réponse automatisée basique (blocage d'IP via firewall, quarantaine de fichiers). Il ne dispose pas des capacités de machine learning avancé pour la détection comportementale, ni de l'isolation réseau automatisée ou de la télémétrie kernel-level des EDR commerciaux de premier plan. Pour des environnements avec des contraintes budgétaires sévères, Wazuh seul offre une protection substantielle. Pour des environnements critiques ou des secteurs fortement ciblés, la combinaison d'un agent Wazuh (pour les logs et la conformité) avec un EDR léger (Elastic Defend, Microsoft Defender for Endpoint) est l'approche recommandée.

Quel volume de logs peut ingérer Wazuh 4.x sur un serveur standard ?

Un déploiement Wazuh single-node sur un serveur 8 vCPU / 16 Go RAM / SSD NVMe peut ingérer confortablement 5 000 à 10 000 EPS (Events Per Second), soit environ 1 000 à 2 000 agents actifs avec une activité normale. Au-delà, une architecture distribuée avec plusieurs nœuds Wazuh Indexer est nécessaire. Pour référence, 1 000 postes Windows avec l'audit complet activé génèrent environ 1 000 à 3 000 EPS. Les charges de logs réseau (firewall, proxy) peuvent être bien supérieures et nécessitent un dimensionnement spécifique.

Comment choisir entre OpenSearch et Elasticsearch comme backend pour Wazuh ou Graylog ?

Depuis Wazuh 4.4, OpenSearch est le backend officiel par défaut (remplaçant Elasticsearch). Pour les nouveaux déploiements en 2026, OpenSearch est le choix recommandé pour plusieurs raisons : licence Apache 2.0 sans restrictions, fonctionnalités de sécurité natives gratuites (authentification, chiffrement, RBAC), et roadmap active avec Amazon comme contributeur principal. Elasticsearch reste pertinent si votre organisation utilise déjà des fonctionnalités Elastic payantes (SIEM Elastic, ML Elastic) ou si vous avez un contrat de support Elastic en

place. Pour Graylog, les deux backends sont supportés, et le choix dépend principalement des compétences internes de votre équipe.

NIS 2 impose-t-elle le déploiement d'un SIEM pour les organisations concernées ?

NIS 2 n'impose pas explicitement un SIEM, mais les obligations de l'article 21 — supervision des systèmes d'information, détection des incidents, journalisation et corrélation des événements — rendent un SIEM pratiquement indispensable pour démontrer la conformité. L'ANSSI, dans ses guides techniques, recommande explicitement la mise en place d'un outil de centralisation et de corrélation des logs pour les opérateurs essentiels et importants. Un SIEM open source correctement configuré, avec des règles de détection alignées sur les menaces du secteur, constitue une réponse proportionnée et défendable face à un auditeur NIS 2.

Bonnes pratiques et recommandations complémentaires

Au-delà des techniques et outils présentés dans cet article, plusieurs principes transverses guident les professionnels de la cybersécurité dans leur approche quotidienne. La défense en profondeur (*defense-in-depth*) reste le principe fondateur : aucune mesure de sécurité unique n'est suffisante, et la multiplication des couches de protection — même imparfaites individuellement — crée une résilience globale supérieure à la somme de ses parties.

Veille et mise à jour continue

La cybersécurité est un domaine où l'obsolescence est rapide. Une technique ou un outil efficace en 2024 peut être contourné en 2026. Les équipes sécurité maintiennent leur efficacité en s'appuyant sur des sources de veille fiables : bulletins CERT-FR et ANSSI, advisories des éditeurs (Microsoft MSRC, Google Project Zero, Cisco Talos), recherches académiques (USENIX Security, IEEE S&P, CCS), et publications de la communauté (threat intel reports des grands éditeurs, articles de blog de chercheurs reconnus).

Documentation et partage de connaissances

La capitalisation des connaissances est un enjeu organisationnel critique dans les équipes de sécurité. Les runbooks d'investigation, les post-mortems d'incidents, les procédures de réponse documentées, et les bases de connaissance internes permettent de maintenir la cohérence des pratiques indépendamment des rotations d'équipe et de réduire le temps de résolution des incidents récurrents. L'utilisation d'un wiki sécurisé (Confluence, Notion avec contrôles d'accès stricts) pour centraliser ces connaissances est une pratique adoptée par la majorité des équipes SOC matures. La documentation proactive, rédigée juste après les incidents pendant que les détails sont frais, est systématiquement plus précise et utile que la documentation rédigée après coup.

Synthèse et perspectives 2026

Les techniques et recommandations présentées dans ce guide s'inscrivent dans un contexte de menaces en constante évolution. La cybersécurité offensive et défensive sont deux faces d'une même médaille : comprendre les mécanismes d'attaque est indispensable pour construire des défenses robustes et résilientes face aux acteurs malveillants les plus sophistiqués.

Pour les équipes sécurité, l'enjeu de 2026 est double : maintenir une veille continue sur les nouvelles techniques publiées par la communauté de recherche (CVE, exploit-db, GitHub, Secrech, SSTIC) tout en assurant le durcissement progressif de l'infrastructure existante. Le référentiel MITRE ATT&CK reste le fil conducteur le plus efficace pour structurer un programme de détection et de réponse face aux tactiques, techniques et procédures des groupes APT ciblant les secteurs critiques.

La formation continue des équipes, la simulation régulière d'incidents (exercices tabletop, exercices Red/Blue/Purple Team), et l'automatisation des tâches répétitives via des outils SOAR constituent les piliers d'une organisation cyber mature. Les organisations qui investissent dans ces trois axes démontrent systématiquement de meilleures métriques de détection et de réponse (MTTD et MTTR réduits de 40% en moyenne selon les benchmarks sectoriels) face aux incidents de sécurité. Le choix entre ces solutions doit être guidé par une évaluation objective des

ressources internes disponibles pour l'administration et l'optimisation du SIEM, car la valeur d'un système de détection dépend directement de la qualité des règles qui l'alimentent et de la compétence des analystes qui en interprètent les alertes.