AYI NEDJIMI Consultants

Wazuh : Plateforme XDR/SIEM Open Source 2026 - Guide Complet

10 mai 2026 • Mis à jour le 17 mai 2026 • 17 min de lecture • 3706 mots • 122 vues •

Wazuh est une plateforme de securite unifiee XDR (Extended Detection and Response) et SIEM (Security Information and Event Management) open source, distribuee sous licence GPLv2, qui agrege la collecte de logs, la detection de menaces, le monitoring d'integrite des fichiers (FIM), l'evaluation des vulnerabilites, l'evaluation de la configuration de securite (SCA) et l'audit de conformite reglementaire dans une stack unique. Maintenue par Wazuh Inc. (Sunnyvale, Californie) depuis 2015 apres son fork de OSSEC, la plateforme atteint la version 4.12 en mai 2026 et compte plus de 20 000 deploiements actifs dans 150 pays. Wazuh repose sur quatre composants : Manager, Indexer, Dashboard et Agents.

Wazuh est une plateforme de securite unifiee **XDR (Extended Detection and Response)** et **SIEM (Security Information and Event Management)** open source, distribuee sous licence **GPLv2**, qui agrege la collecte de logs, la detection de menaces, le monitoring d'integrite des fichiers (FIM), l'evaluation des vulnerabilites, l'evaluation de la configuration de securite (SCA) et l'audit de conformite reglementaire dans une stack unique. Maintenue par **Wazuh Inc.** (Sunnyvale, Californie) depuis 2015 apres son fork de OSSEC, la plateforme atteint la **version 4.12** en mai 2026 et compte plus de **20 000 deploiements actifs** dans 150 pays. Wazuh repose sur quatre composants : un **Wazuh Manager** (correlation et analyse), un **Wazuh Indexer** (fork OpenSearch 2.x pour stockage et recherche), un **Wazuh Dashboard** (interface OpenSearch Dashboards customisee) et des **agents legers** deployes sur les endpoints Linux, Windows, macOS, AIX, Solaris ou HP-UX. La solution rivalise avec Splunk Enterprise Security, Elastic Security et Microsoft Sentinel sur le perimetre fonctionnel mais conserve un avantage decisif : **aucun cout de licence par GB ingere**, contrainte qui plombe les budgets SOC dans les architectures proprietaires.

À RETENIR

A retenir

Wazuh est une plateforme XDR/SIEM open source GPLv2 agregant FIM, SCA, vuln detection, log analysis, MITRE ATT&CK mapping et reponse active.

Architecture quatre composants : Wazuh Manager (analyse), Wazuh Indexer (OpenSearch fork), Wazuh Dashboard (UI), Wazuh Agent (collecte endpoint).

Réponse sous 24h

Devis gratuit →