

# Wazuh

## Wazuh : Votre SIEM & XDR Open Source

Wazuh est une plateforme de sécurité gratuite et open-source offrant une visibilité unifiée sur la sécurité des endpoints et du cloud. Elle combine les fonctions de SIEM et de XDR.

### Pourquoi utiliser Wazuh ?

- **Detection d intrusions** : Analyse des logs en temps réel.
- **Verification d integrite (FIM)** : Surveille les changements sur les fichiers systeme.
- **Analyse des vulnerabilites** : Inventaire des applications et correlation CVE.

### Architecture et Fonctionnement

- **Wazuh Manager** : Le coeur du systeme.
- **Wazuh Indexer** : Moteur de recherche et d analyse.
- **Wazuh Dashboard** : L interface graphique de visualisation.
- **Agents Wazuh** : Programmes installes sur les machines surveillees.

Documentation officielle : [documentation.wazuh.com](https://documentation.wazuh.com)

---

Revision #1

Created 2026-03-20 15:57:14 UTC by Maxime

Updated 2026-03-20 15:57:14 UTC by Maxime