Comparatif Outils Open Source SOC 2026 : Wazuh, TheHive, MISP et Shuffle

Comparatif complet des outils open source pour SOC 2026 : Wazuh SIEM/XDR, TheHive case management, MISP threat intel, Shuffle SOAR et intégration.

Face aux coûts prohibitifs des plateformes SOC commerciales (Splunk Enterprise dépasse souvent 100 000 € par an pour un volume de logs moyen, Microsoft Sentinel facture à l'ingestion), les équipes de sécurité françaises cherchent des alternatives open source crédibles pour construire leur centre opérationnel de sécurité. En 2026, l'écosystème open source SOC a atteint une maturité remarquable avec quatre outils complémentaires qui couvrent les besoins fondamentaux d'un SOC : **Wazuh** pour le SIEM/XDR et la collecte des logs, **TheHive** pour la gestion des incidents et le case management, **MISP** (Malware Information Sharing Platform) pour le partage de threat intelligence et la corrélation d'indicateurs de compromission, et **Shuffle** pour l'automatisation et le SOAR (Security Orchestration, Automation and Response). Ces quatre outils forment ensemble une stack SOC open source complète, déployable on-premise pour les organisations qui ne peuvent pas ou ne veulent pas envoyer leurs données de sécurité dans le cloud d'un éditeur tiers. Ce guide compare les fonctionnalités de chaque outil en 2026, explique leur intégration, leurs limites réelles (il y en a), et donne des recommandations concrètes pour les équipes qui veulent construire un SOC open source sans se perdre dans la complexité. Le contexte France est important : la plupart des grandes entreprises et administrations qui déploient ces outils le font dans le cadre de conformité NIS 2 ou dans le cadre des recommandations ANSSI pour les opérateurs de services essentiels.

À RETENIR

À retenir — Stack SOC Open Source 2026

• **Wazuh** : SIEM + XDR + vulnerability assessment, agents multiplateforme, règles MITRE ATT&CK intégrées

• **TheHive** : case management, observables, responders — le "Jira" des analystes SOC

• **MISP** : threat intelligence sharing, IoC, événements — partage avec CERT-FR et partenaires

• **Shuffle** : SOAR workflows no-code/low-code, intégration native TheHive + Wazuh + MISP et 700 autres apps sécurité

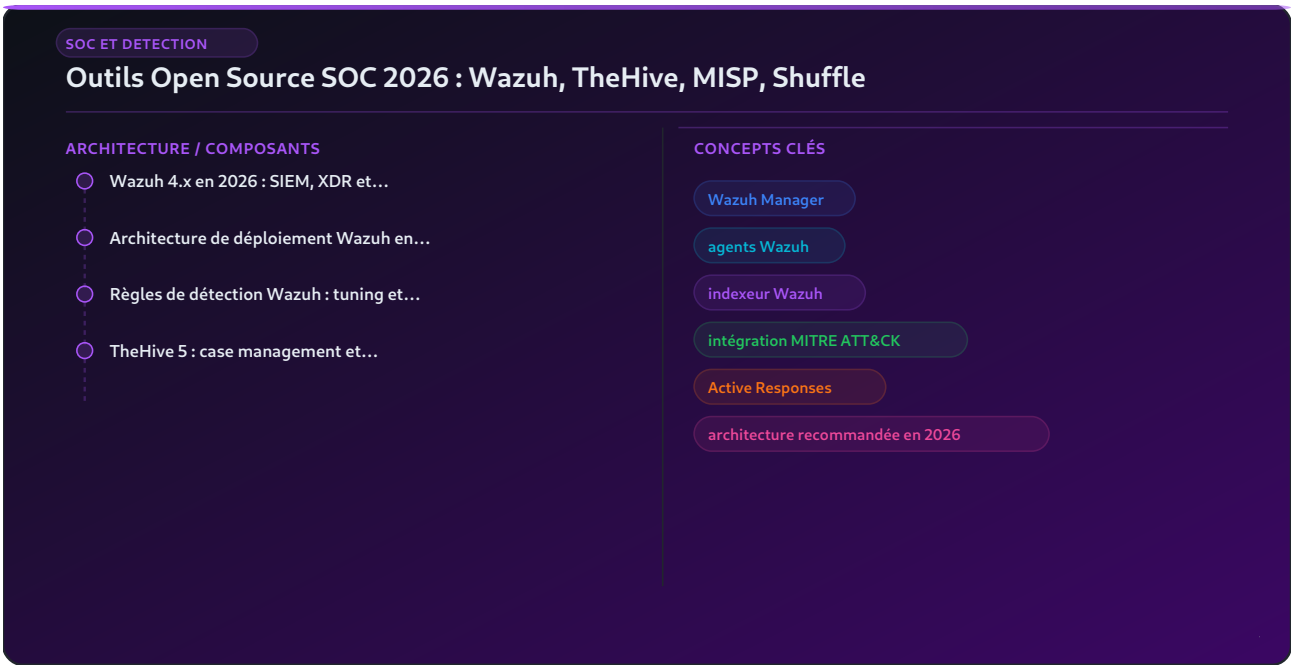
• Stack complète déployable sur 2 serveurs dédiés (16 Go RAM minimum chacun) pour un SOC de 10 à 500 équipements

• Coût licence : **0 €** — coût réel : infrastructure + temps humain de tuning et maintenance

• Suricata IDS/IPS en complément de Wazuh pour la couverture réseau — intégration native via logs JSON EVE

• Cortex (moteur TheHive) : 150+ Analyzers d'enrichissement (VirusTotal, AbuseIPDB, Shodan, Hybrid Analysis)

• NIS 2 : stack couvre collecte logs, détection anomalies, gestion incidents et partage IoCs avec CERT-FR (MISP)



Wazuh 4.x en 2026 : SIEM, XDR et agent unifié

Wazuh est né comme un fork d'OSSEC (Open Source HIDS Security) et s'est transformé en une plateforme SIEM/XDR complète. En 2026, Wazuh 4.x est l'outil open source de détection le plus déployé dans les SOC européens. L'architecture Wazuh se compose de trois éléments : le **Wazuh Manager** (serveur central qui collecte et analyse les logs, exécute les règles de détection), les **agents Wazuh** (installés sur les endpoints Windows, Linux, macOS, les serveurs et les équipements réseau) et l'**indexeur Wazuh** (basé sur OpenSearch/Elasticsearch pour le stockage et la recherche des événements). Wazuh inclut nativement une **intégration MITRE ATT&CK** : chaque règle de détection est taggée avec les techniques ATT&CK correspondantes, permettant de visualiser la couverture de détection du SOC sur la matrice MITRE. Les capacités **XDR** de Wazuh incluent l'évaluation de vulnérabilités (scan des packages installés avec corrélation CVE), la vérification d'intégrité des fichiers (FIM — File Integrity Monitoring), la détection de rootkits, et la conformité CIS/PCI-DSS/GDPR. Wazuh 4.x ajoute les **Active Responses** : des scripts déclenchés automatiquement lors de détections (bloquer une IP avec iptables, isoler un endpoint, lancer un scan, etc.). Un retour terrain d'un SOC interne d'une ETI lyonnaise (2024) : l'installation des agents Wazuh sur 200 endpoints Windows/Linux a pris 2 jours via Ansible, mais

le tuning des règles pour réduire les faux positifs à un niveau acceptable a demandé 3 semaines de travail d'un analyste senior.

Architecture de déploiement Wazuh en production

Pour un déploiement Wazuh en production, l'**architecture recommandée en 2026** distingue trois topologies selon le volume. Pour un SOC jusqu'à 500 agents, une architecture **monolithique** avec Wazuh Manager + Indexer + Dashboard sur 2 serveurs (Manager sur 8 vCPU/16 Go RAM, Indexer sur 16 vCPU/32 Go RAM + 2 To SSD) est suffisante. Pour 500 à 5000 agents, une architecture **distribuée** avec cluster d'indexers (3 nœuds minimum pour la haute disponibilité) et plusieurs workers Wazuh est nécessaire. Au-delà, l'architecture **enterprise** avec séparation complète des composants est indispensable. La **politique de rétention des logs** dans l'indexer Wazuh est critique : par défaut, tout est conservé indéfiniment jusqu'à saturation du disque. Configurer des ILM (Index Lifecycle Management) policies pour archiver les logs froids après 30 jours et supprimer après 12 mois (ou selon les exigences réglementaires). Le **chiffrement des communications** entre agents et Manager via TLS (certificats X.509 auto-signés par défaut dans Wazuh) doit être vérifié et les certificats renouvelés avant expiration. La **sécurité du Dashboard Wazuh** (OpenSearch Dashboards) — accessible sur le port 443 par défaut — doit être restreinte à un réseau de management ou derrière un VPN.

> ⚡ **Retour terrain**
>
> Dans les SOC que j'accompagne, le principal problème n'est pas le manque d'alertes mais l'excès : 'alert fatigue' systématique, analysts qui désactivent des règles jugées trop bruyantes sans documentation, et faux positifs récurrents qui masquent les vrais incidents. J'ai développé un tableau de bord simple — 3 métriques : taux de faux positifs par règle,

MTTD (mean time to detect) sur incidents réels, et ratio alertes/analyst — qui permet en une réunion hebdomadaire de 30 minutes d'identifier les règles à tuner en priorité.

Règles de détection Wazuh : tuning et MITRE ATT&CK

Les **règles Wazuh** sont des fichiers XML définissant les patterns de détection. Wazuh inclut plus de 3000 règles par défaut couvrant Windows Event Logs, Syslog Linux, logs Apache/Nginx, logs SSH, logs de pare-feu, etc. Le **tuning des règles** pour réduire les faux positifs est la tâche la plus chronophage d'un SOC Wazuh : créer des règles d'exception (`rule_exclude`) pour les comportements normaux de l'environnement (scripts de maintenance, comptes de service avec des activités répétitives). La création de **règles personnalisées** pour l'environnement spécifique de l'organisation — applications métier, comportements utilisateurs normaux — est indispensable pour une détection pertinente. Les règles SIGMA peuvent être converties en règles Wazuh via l'outil **sigma-cli** avec le backend Wazuh, permettant d'importer les milliers de règles de la communauté SIGMA. La **corrélation de règles** (règles composites qui s'activent sur la combinaison de plusieurs événements dans une fenêtre temporelle) permet de détecter des patterns complexes comme une série d'échecs d'authentification suivie d'un succès (brute force réussi) ou un processus anormal créé après un email suspect.

TheHive 5 : case management et gestion des incidents

TheHive 5 (version majeure en 2023, maintenue activement en 2026) est la plateforme de case management de référence pour les équipes SOC et CSIRT. TheHive centralise la gestion des incidents de sécurité : chaque alerte devient un **Case** (dossier d'incident) avec des tâches assignées, des observables (IOCs — adresses IP, hash de fichiers, URLs, domaines, emails), une timeline des actions, et un journal d'investigation. Les **observables** dans TheHive peuvent être enrichis automatiquement via des **Analyzers** (modules d'enrichissement) : une IP peut être

soumise à VirusTotal, AbuseIPDB, Shodan ; un hash de fichier soumis à VirusTotal et Hybrid Analysis ; un domaine soumis à WHOIS, PassiveDNS. Ces enrichissements automatiques accélèrent considérablement l'investigation d'un analyste SOC. Les **Responders** TheHive sont des scripts d'action : bloquer une IP sur le firewall, ajouter un IOC dans MISP, isoler un endpoint dans CrowdStrike, envoyer une notification Slack. Intégré avec Wazuh via l'API TheHive et des scripts de webhook, chaque alerte Wazuh au-dessus d'un seuil de criticité crée automatiquement un case TheHive avec les observables associés. TheHive 5 supporte le **multi-organisations** (MSSP-mode) permettant à une équipe SOC de gérer des clients distincts avec une isolation complète des données.

TheHive : configuration et intégration avec Wazuh

La **configuration de l'intégration Wazuh → TheHive** passe par le mécanisme de **Custom Integration** de Wazuh. Un script Python est configuré dans Wazuh (ossec.conf) pour recevoir les alertes au-dessus d'un niveau de criticité (level ≥ 10 par exemple) et créer des cases TheHive via l'API REST. L'intégration inclut le mapping des champs Wazuh vers les observables TheHive : l'IP source d'une alerte réseau devient un observable "ip", le hash d'un fichier suspect devient un observable "hash", etc. La **gestion des doublons** (éviter la création de multiples cases pour la même alerte) est gérée côté script par une vérification de l'existence d'un case similaire ouvert dans les dernières X heures. Le **workflow d'escalade** dans TheHive : Nouvelle alerte → Triage (analyste L1) → Qualification (analyste L2) → Investigation (analyste L2/L3) → Clôture. Les **templates de case** TheHive définissent les tâches pré-remplies pour chaque type d'incident (phishing, ransomware, intrusion, DDoS) — un gain de temps majeur pour les analystes L1 qui suivent ainsi un playbook structuré. Cortex, le moteur d'enrichissement de TheHive Project, gère les Analyzers et Responders de manière centralisée — une seule instance Cortex peut servir plusieurs instances TheHive.

MISP : threat intelligence sharing et IoC management

MISP (Malware Information Sharing Platform) est né d'un projet de l'armée luxembourgeoise et est maintenu par CIRCL (Computer Incident Response Center Luxembourg). En France, le CERT-FR (ANSSI) partage des événements MISP avec les organisations connectées, et de nombreuses communautés sectorielles (santé, finance, énergie) ont des instances MISP privées pour partager la threat intelligence entre pairs. L'architecture MISP est centrée sur les **Événements** (Events) : chaque événement regroupe des attributs (IoCs — IP, URL, hash, email, domaine, CVE, YARA rules) et des objets (Objects — des groupes structurés d'attributs comme un objet "network-connection" ou un objet "malware"). La **taxonomie MISP** (tags standardisés : TLP, PAP, MITRE ATT&CK, secteurs, etc.) permet la classification et le filtrage des événements. Les **Feeds MISP** — sources de threat intelligence externes importées automatiquement — incluent des feeds gratuits (Abuse.ch URLhaus, Feodo Tracker, CIRCL OSINT feed) et des feeds commerciaux (MISP accède à des sources payantes via leur API). La **synchronisation MISP-to-MISP** permet à des organisations partenaires de partager bidirectionnellement leurs événements — le modèle de partage communautaire qui fait la valeur de MISP par rapport à une base d'IoCs statique.

MISP : configuration, feeds et intégration SOC

La **configuration initiale de MISP** pour un SOC comprend : la configuration du serveur d'authentification (LDAP/SAML pour les organisations avec SSO), la définition des organisations (votre organisation et les partenaires avec qui vous partagez), l'abonnement aux feeds gratuits recommandés, et la configuration du **scheduler MISP** pour les tâches automatiques (import feeds, synchronisation, nettoyage). L'**intégration MISP → Wazuh** permet à Wazuh de requêter MISP lors d'une alerte : si une IP détectée dans les logs est présente dans MISP avec une criticité élevée, l'alerte Wazuh est enrichie et son niveau de criticité augmenté. Cette intégration passe par le module **MISP Threat Intel** de Wazuh ou via un script personnalisé interrogeant l'API MISP. L'**intégration MISP → TheHive** est native dans TheHive 5 : lors de l'analyse d'un observable dans TheHive, Cortex peut interroger MISP pour vérifier si l'observable

est connu et réputé malveillant. Les **exports MISP** en format STIX 2.0 permettent l'interopérabilité avec d'autres plateformes de threat intelligence et des outils SIEM commerciaux. Pour les organisations soumises à NIS 2, partager des IoCs dans MISP avec les pairs du secteur et le CERT-FR est une pratique de coopération recommandée par l'ANSSI.

Shuffle SOAR : automatisation des workflows SOC

Shuffle est une plateforme SOAR (Security Orchestration, Automation and Response) open source créée par une startup norvégienne, disponible en SaaS ou self-hosted. Shuffle se distingue des SOAR commerciaux (Splunk SOAR/Phantom, Palo Alto XSOAR) par une interface **no-code/low-code** basée sur des workflows visuels (drag-and-drop) accessibles sans expertise Python. Les **Apps Shuffle** sont des connecteurs vers des outils de sécurité (700+ apps disponibles dans le catalogue) : TheHive, MISP, Wazuh, VirusTotal, Shodan, Slack, PagerDuty, Jira, CrowdStrike, firewall Palo Alto, etc. Un workflow Shuffle typique pour l'automatisation SOC : **Trigger** (webhook TheHive sur nouveau case) → **Enrichissement** (requête VirusTotal sur les observables IP/hash) → **Décision** (condition si score VT > 50) → **Action** (bloquer IP sur firewall + notifier analyste Slack + créer ticket Jira) → **Mise à jour TheHive** (ajouter le résultat VT en commentaire du case). Ces workflows remplacent des heures de travail répétitif d'analyste L1. Le **déploiement self-hosted de Shuffle** utilise Docker Compose et nécessite environ 4 Go de RAM — très léger comparé aux SOAR commerciaux.

Intégration de la stack complète : flux de données SOC

L'intégration des quatre outils forme une stack cohérente avec des flux de données bien définis. Le flux principal : les **agents Wazuh** collectent les logs des endpoints et équipements → **Wazuh Manager** analyse et corrèle → les alertes critiques déclenchent un **webhook vers Shuffle** → Shuffle enrichit les observables (VirusTotal, AbuseIPDB, MISP) → Shuffle crée un **case TheHive** avec les observables enrichis → les analystes investiguent dans TheHive → les IOCs

identifiés sont exportés vers **MISP** pour partage avec la communauté → MISP retro-alimente Wazuh pour les futures détections. La **bidirectionnalité des flux** est la clé de la valeur de la stack : MISP nourrit Wazuh avec de nouveaux IoCs qui améliorent la détection, TheHive exporte les cas résolus vers MISP pour enrichir la threat intelligence communautaire. La **configuration des webhooks** entre les outils (Wazuh → Shuffle, Shuffle → TheHive, TheHive → Cortex → MISP) nécessite une planification soigneuse des URL d'API, des tokens d'authentification, et des formats de données. Un **bus de messages** (Redis ou RabbitMQ) peut être interposé pour découpler les outils et gérer les pics de volume d'alertes.

Coûts de la stack SOC open source vs SIEM commercial

La comparaison de coûts entre une stack SOC open source (Wazuh+TheHive+MISP+Shuffle) et un SIEM commercial (Splunk, Microsoft Sentinel, IBM QRadar) révèle des économies significatives mais pas nulles. **Licence logicielle** : 0 € pour la stack open source vs 80 000 à 300 000 €/an pour Splunk Enterprise selon le volume d'ingestion, ou 150 à 300 €/nœud/mois pour Microsoft Sentinel. **Infrastructure** : 2 serveurs dédiés (ou VMs) de 32 Go RAM / 8 vCPU / 2 To SSD chacun, soit environ 800 à 1500 €/mois en cloud ou 8 000 à 15 000 € en matériel on-premise — ce coût est partagé entre open source et commercial. **Intégration et déploiement** : 10 à 30 jours de consulting pour la mise en place de la stack open source vs 20 à 60 jours pour un SIEM commercial (plus complexe à configurer). **Maintenance continue** : 0.25 à 0.5 ETP d'ingénieur sécurité pour maintenir et faire évoluer la stack open source vs inclus (théoriquement) dans le support commercial. Au total, le TCO 3 ans d'une stack SOC open source pour une organisation de 200 endpoints est environ 150 000 à 200 000 € (infrastructure + services) vs 400 000 à 800 000 € pour Splunk Enterprise — une économie réelle de 50 à 70%.

Limites réelles de la stack SOC open source

Il serait malhonnête de ne pas évoquer les **limites réelles** de la stack Wazuh+TheHive+MISP+Shuffle. La principale limite est la **scalabilité** : au-delà de 1000 agents Wazuh ou de 100 Go de logs par jour, la gestion du cluster OpenSearch/Indexer devient complexe et gourmande en ressources — des compétences d'ingénieur Elasticsearch/OpenSearch sont nécessaires. La **maturité UX** : les interfaces de Wazuh, TheHive et MISP sont fonctionnelles mais moins polies que Splunk ou Sentinel — la courbe d'apprentissage pour les analystes L1 est plus importante. Le **support communautaire** repose sur des forums, Discord, et la bonne volonté de la communauté — pas de hotline 24/7 avec SLA comme avec un éditeur commercial. La **maintenance des intégrations** entre les outils (mise à jour d'un outil qui casse l'API utilisée par un autre) est un vrai risque opérationnel que les éditeurs commerciaux gèrent dans leurs suites intégrées. Mon opinion tranchée : pour une équipe SOC de 3+ personnes avec un ingénieur capable de maintenir des services Linux, la stack open source est le meilleur choix rapport coût/efficacité. Pour une équipe de 1-2 personnes sans compétences devops, Microsoft Sentinel (malgré le coût) est plus adapté car il ne nécessite pas de maintenance d'infrastructure.

Wazuh et détection des menaces cloud : AWS, Azure, GCP

En 2026, les SOC ne surveillent plus uniquement des endpoints on-premise mais aussi des workloads cloud. **Wazuh supporte nativement l'intégration avec les principales plateformes cloud**. Pour **AWS** : collecte des CloudTrail logs (actions API AWS), GuardDuty findings (détections AWS natives), VPC Flow Logs (trafic réseau), et Config changes (changements de configuration). Un agent Wazuh peut être installé sur les instances EC2 pour la surveillance au niveau OS. Pour **Azure** : collecte des Azure Activity Logs, Microsoft Defender for Cloud alerts, Azure AD Sign-in logs, et NSG Flow Logs. Pour **GCP** : collecte des Cloud Audit Logs et Security Command Center findings. Cette intégration cloud permet à un SOC Wazuh de corréler des événements on-premise avec des événements cloud — une capacité essentielle pour les environnements hybrides. Les règles de détection Wazuh pour les environnements cloud sont

taggées MITRE ATT&CK Cloud (sous-matrices AWS, Azure, GCP) permettant une couverture cohérente de la matrice ATT&CK sur l'ensemble de l'infrastructure.

Threat hunting avec la stack open source

Au-delà de la détection réactive (alertes sur des patterns connus), la stack SOC open source permet aussi le **threat hunting** (recherche proactive de menaces non détectées). Dans **Wazuh Dashboard**, les capacités de recherche OpenSearch permettent de requêter des milliards d'événements pour rechercher des patterns suspects : processus inhabituels, connexions vers des pays atypiques, volumes de transfert de données anormaux, etc. Des **requêtes KQL** (Kibana Query Language, compatible OpenSearch) permettent des analyses de type "show me all PowerShell executions with encoded command in the last 7 days" ou "find all lateral movement using PsExec". L'**intégration MISP → Wazuh pour le retrohunting** : quand un nouvel IoC est ajouté dans MISP (par exemple un hash de malware suite à un incident), Wazuh peut rétrospectivement chercher si cet IoC apparaît dans les logs des 90 derniers jours — permettant de détecter une compromission passée non détectée à l'époque. La **création de notebooks Jupyter** connectés à l'API OpenSearch de Wazuh permet des analyses statistiques avancées et la visualisation de patterns d'attaque — une approche adoptée par les équipes SOC avancées pour les analyses long-terme.

Intégration EDR open source : Wazuh et Velociraptor

Pour les capacités EDR (Endpoint Detection and Response) avancées, **Velociraptor** peut compléter Wazuh dans une stack open source. Velociraptor est un outil de collecte de forensique digitale et de chasse aux menaces (DFIR) qui permet une collecte forensique à grande échelle depuis les endpoints (artefacts systèmes, fichiers, mémoire, processus, clés de registre Windows) via des **VQL (Velociraptor Query Language)** queries déployées à distance sur des milliers d'endpoints simultanément. L'intégration Wazuh + Velociraptor : Wazuh détecte une alerte sur un

endpoint → Shuffle déclenche une collecte Velociraptor automatique sur l'endpoint suspect (preuves forensiques, liste des processus, connexions réseau actives, scripts auto-exécutés) → les résultats Velociraptor sont attachés au case TheHive. Cette intégration donne une capacité de réponse à incident comparable à des EDR commerciaux comme CrowdStrike Falcon ou Carbon Black, à un coût infrastructure-only. Pour les organisations avec des budgets limités mais des exigences élevées de réponse à incident, Wazuh + Velociraptor + TheHive forment un trio particulièrement puissant.

Déploiement de la stack avec Docker Compose

Le déploiement de la stack SOC open source via **Docker Compose** est la méthode recommandée pour les environnements de petite à moyenne taille. Les dépôts officiels Docker des quatre outils proposent des fichiers Docker Compose maintenus. La **séquence de déploiement recommandée** : 1) Déployer MISP en premier (il ne dépend pas des autres) ; 2) Déployer Wazuh (Manager + Indexer + Dashboard) ; 3) Déployer TheHive + Cortex (avec une base ElasticSearch/Cassandra partagée ou dédiée selon la taille) ; 4) Déployer Shuffle ; 5) Configurer les intégrations entre les outils. La **persistance des données** doit être configurée avec des volumes Docker sur des disques dédiés (pas sur le disque système). Pour Wazuh Indexer, un volume SSD dédié de 2 To minimum est recommandé avec la politique de rétention configurée. Les **mises à jour de la stack** sont le point délicat des déploiements Docker : mettre à jour un composant peut nécessiter une migration de données (changement de schéma d'index Wazuh entre versions majeures, migration de la base TheHive, etc.) — tester les mises à jour sur un environnement de staging avant la production.

Cortex : moteur d'enrichissement et d'analyse pour TheHive

Cortex est le moteur d'enrichissement et d'action du projet TheHive, fonctionnant comme un service indépendant connecté à TheHive. Cortex orchestre les **Analyzers** (modules

d'enrichissement) et les **Responders** (modules d'action) pour automatiser l'analyse des observables dans les cases TheHive. Le catalogue des Analyzers Cortex disponibles en 2026 comprend plus de 150 intégrations : **VirusTotal** (réputation fichiers, URLs, IPs, domaines), **AbuseIPDB** (réputation IPs), **Shodan** (informations sur une IP exposée sur Internet), **PassiveTotal (RiskIQ)** (DNS passif, infrastructure attaquant), **Hybrid Analysis** (sandbox malware), **CrowdStrike Falcon Sandbox**, **MISP** (lookup d'IoC dans la base locale), **OTX AlienVault** (threat intelligence publique), et de nombreux autres. Un analyste TheHive peut lancer un Analyzer manuellement sur un observable ou Shuffle peut les déclencher automatiquement dans un workflow SOAR. La **notation des Analyzers** (Malicious/Suspicious/Safe/Info) avec un score de confiance permet à Shuffle de prendre des décisions automatiques sur l'action à effectuer. Cortex maintient un cache des résultats d'analyse avec une TTL configurable pour éviter de re-interroger les APIs externes pour les mêmes observables analysés récemment, réduisant les coûts et les délais d'enrichissement.

Collecte de logs avancée avec Wazuh : sources et parsers

La valeur d'un SIEM est proportionnelle à la richesse des sources de logs collectées. Wazuh supporte une **grande variété de sources** via différents mécanismes. Les **agents Wazuh** (installés sur les endpoints) collectent nativement les logs Windows (Event Logs, PowerShell logs, Sysmon), les logs Linux (syslog, auth.log, audit daemon), les logs d'applications (IIS, Apache, Nginx, MySQL, PostgreSQL) via des décodeurs configurables. Le **Syslog centralisé** permet de collecter les logs d'équipements réseau (routeurs, switches Cisco/Juniper, firewalls pfSense/OPNsense, load balancers) et d'équipements de sécurité (WAF ModSecurity, IDS Suricata, AV entreprise) qui n'ont pas d'agent Wazuh disponible. Le **protocole Beats (Filebeat, Winlogbeat)** peut être utilisé pour forwarder des logs depuis des serveurs vers Wazuh Indexer en complément des agents natifs, notamment pour les environnements avec des contraintes d'installation d'agents. Les **décodeurs personnalisés Wazuh** (fichiers XML) permettent de parser des formats de logs propriétaires — si votre application métier génère des logs dans un format spécifique, un décodeur Wazuh peut les rendre exploitables dans le SIEM. La **corrélation multi-sources** est la puissance réelle du SIEM : corréler un log de connexion VPN (depuis le firewall) avec un accès

anormal à des données sensibles (depuis les logs applicatifs) avec une connexion RDP vers un serveur interne (depuis les logs Windows) permet de détecter une compromission que chaque log seul n'aurait pas révélée.

Active Directory et détection des attaques d'identité avec Wazuh

L'**Active Directory (AD)** est la cible principale des attaquants dans les infrastructures Windows — 80% des attaques ransomware passent par une compromission AD. Wazuh, combiné à **Sysmon** (System Monitor Microsoft) déployé sur les contrôleurs de domaine et les endpoints Windows, permet une détection avancée des attaques d'identité. Les **événements Windows critiques** à surveiller via Wazuh pour l'AD : Event ID 4624 (connexion réussie), 4625 (échec de connexion), 4648 (connexion avec credentials explicites — indicateur Pass-the-Hash), 4672 (connexion avec privilèges admin), 4720 (création de compte), 4728/4732/4756 (ajout à un groupe de sécurité), 4768/4769/4771 (Kerberos TGT/TGS requests — détection Kerberoasting et AS-REP Roasting). Les **règles Wazuh pour les attaques AD** couvrent : le **Pass-the-Hash** (connexions avec EventID 4648 depuis des IP inhabituelles), la **Golden Ticket attack** (anomalies dans les tickets Kerberos — durée excessive, comptes inconnus), le **DCSync** (réplication AD non autorisée — event 4662 avec flag GUID de réplication), et les **énumérations LDAP** (requêtes LDAP excessives depuis des endpoints non habituels). L'intégration Sysmon + Wazuh sur l'AD offre une couverture MITRE ATT&CK des techniques d'attaque d'identité comparable à des solutions commerciales spécialisées (Microsoft Defender for Identity, Vectra) à moindre coût.

Gestion des alertes et priorisation : éviter la fatigue des alertes

La **fatigue des alertes** (alert fatigue) est le principal échec des déploiements SOC — quand un analyste reçoit des centaines d'alertes par jour, il commence à les ignorer toutes, y compris les vraies menaces. Wazuh génère par défaut un volume considérable d'alertes que seul le tuning

réduit à un niveau opérationnel. La stratégie de **réduction des faux positifs** dans Wazuh comprend plusieurs niveaux. Le **tuning des règles globales** : désactiver ou baisser le niveau des règles qui génèrent systématiquement des faux positifs dans l'environnement (exemples : règles de scan de ports qui alertent sur les scans légitimes de Nessus, règles de modification de fichiers qui alertent sur les mises à jour applicatives normales). Les **listes d'exceptions** (rule exceptions) : des conditions qui empêchent une règle de déclencher pour des contextes légitimes identifiés (IP de management, comptes de service, plages horaires de maintenance). La **corrélation temporelle** : configurer des règles composites qui n'alertent que sur des fréquences anormales (20 échecs d'authentification en 60 secondes plutôt qu'un seul échec). La **priorisation par criticité d'assets** : les mêmes événements sur un serveur de base de données critique vs un poste de travail standard méritent des niveaux de criticité différents. Shuffle peut automatiquement fermer les alertes de faible criticité après enrichissement négatif (pas de correspondance dans VirusTotal/MISP) pour réduire la charge des analystes L1.

OpenSearch et recherche full-text dans les logs Wazuh

L'**indexeur Wazuh**, basé sur OpenSearch (le fork communautaire d'Elasticsearch post-licence SSPL), offre des capacités de recherche et d'analyse puissantes sur des milliards d'événements. La **recherche full-text** permet à un analyste de chercher une IP suspecte, un hash de fichier, un nom d'utilisateur ou une commande PowerShell dans l'ensemble des logs des 90 derniers jours en quelques secondes. Les **agrégations OpenSearch** permettent des analyses statistiques : top 10 des IPs sources d'alertes, distribution horaire des tentatives d'authentification, évolution du volume d'alertes par règle sur 30 jours. Les **dashboards Wazuh** (Kibana/OpenSearch Dashboards) offrent des visualisations pré-construites pour les principales catégories d'événements (authentification, intégrité fichiers, vulnérabilités, conformité). La création de **dashboards personnalisés** est essentielle pour adapter la vue aux besoins spécifiques de l'organisation : un dashboard dédié aux équipements OT, un dashboard Active Directory (tentatives Kerberoasting, Pass-the-Hash), un dashboard conformité PCI-DSS. L'**API OpenSearch** peut être interrogée directement par Shuffle pour des lookups d'historique lors des

workflows SOAR — "est-ce que cette IP a généré des alertes dans les 30 derniers jours ?" — ajoutant un contexte historique précieux à l'enrichissement des alertes en temps réel.

Sécurité de la stack SOC elle-même : durcissement et accès

La stack SOC est une cible de choix pour les attaquants — accéder à Wazuh donne une visibilité sur toute l'infrastructure, compromettre TheHive expose les données d'investigation sensibles, et accéder à MISP peut révéler les partenariats et les informations d'incident partagées. Le **durcissement de la stack SOC** est donc critique. Wazuh Dashboard et TheHive doivent être exposés uniquement depuis un réseau de management ou via VPN — jamais directement sur Internet. Les **tokens d'API** utilisés pour les intégrations (Wazuh → Shuffle, Shuffle → TheHive, TheHive → MISP) doivent être gérés avec rotation régulière et stockés dans un gestionnaire de secrets (Vaultwarden, HashiCorp Vault) plutôt qu'en dur dans les fichiers de configuration. Les **sauvegardes de la stack SOC** (indices Wazuh, base de données TheHive, événements MISP) doivent être chiffrées et stockées offsite — une plateforme SOC compromise ou corrompue sans sauvegarde représente une perte majeure de mémoire organisationnelle. La **journalisation des accès** aux interfaces de la stack SOC elle-même (qui s'est connecté à TheHive à quelle heure, qui a modifié des règles Wazuh) est souvent oubliée — configurer Wazuh pour surveiller... Wazuh (méta-surveillance) et TheHive pour exporter ses propres logs d'accès vers l'indexer Wazuh.

SOAR avancé : playbooks de réponse à incident automatisés

Les **playbooks de réponse à incident automatisés dans Shuffle** représentent l'état de l'art du SOC moderne en 2026. Pour chaque type d'incident documenté dans le plan de réponse à incident de l'organisation, un workflow Shuffle correspondant peut automatiser les premières heures d'investigation et de containment. Le **playbook phishing** typique dans Shuffle : réception d'une alerte email suspect (depuis un outil anti-spam ou un signalement utilisateur) → extraction des URLs et domaines → vérification dans VirusTotal et URLScan → vérification dans MISP →

si malveillant : blocage de l'URL sur le proxy web (API Squid/Zscaler), ajout à la liste de blocage email, notification Slack de l'analyste et création du case TheHive pré-rempli avec les IOCs, envoi d'un email de sensibilisation à l'utilisateur qui a cliqué. Ce playbook réduit le temps moyen de réponse d'une heure (travail manuel de L1) à 2-3 minutes (automatique). Le **playbook détection ransomware** : alerte Wazuh sur comportement de chiffrement massif → isolation immédiate de l'endpoint via l'API EDR (CrowdStrike, Defender) ou blocage réseau via VLAN → snapshot forensique Velociraptor → notification RSSI + direction → création case TheHive critique → déclenchement du plan de continuité d'activité. La rapidité de containment (quelques minutes vs heures en manuel) peut faire la différence entre un incident limité et une crise majeure.

Métriques SOC et rapports de performance

Un SOC performant se mesure avec des métriques précises. Les **KPI SOC essentiels** à suivre avec la stack open source incluent : le **MTTD (Mean Time To Detect)** — temps entre le début d'un incident et sa détection par le SOC (objectif < 1 heure pour les incidents critiques) ; le **MTTR (Mean Time To Respond)** — temps entre la détection et le containment (objectif < 4 heures pour les incidents critiques) ; le **taux de faux positifs** — pourcentage d'alertes qui ne correspondent pas à un incident réel (objectif < 20% pour un SOC mature avec bon tuning) ; le **volume d'alertes par analyste par jour** (objectif < 50 alertes qualifiées par analyste, au-delà la fatigue des alertes s'installe). TheHive produit des rapports sur les cases (temps de résolution, types d'incidents, analystes impliqués) permettant de calculer MTTD et MTTR. Wazuh Dashboard fournit des métriques sur le volume d'alertes par règle, par endpoint, et par criticité — essential pour identifier les règles qui génèrent trop de faux positifs. Des **dashboards Grafana** connectés à l'API TheHive et à l'OpenSearch de Wazuh permettent des rapports hebdomadaires et mensuels automatisés pour la direction et les RSSI — une visualisation qui facilite les arbitrages budgétaires et la communication sur la valeur du SOC.

Suricata IDS/IPS : complément réseau à Wazuh

Suricata est l'IDS/IPS (Intrusion Detection/Prevention System) réseau open source qui complète naturellement Wazuh (qui opère au niveau des endpoints) en apportant une visibilité au niveau du trafic réseau. Suricata analyse le trafic réseau en temps réel sur une interface miroir (TAP ou SPAN port) ou en inline (mode IPS) pour détecter des signatures d'attaques, des protocoles malveillants, et des comportements suspects. L'**intégration Suricata → Wazuh** est native : les logs Suricata (format JSON EVE) sont collectés par un agent Wazuh et indexés dans Wazuh Indexer, permettant la corrélation des alertes réseau avec les alertes endpoint. Les **règles Suricata Emerging Threats** (disponibles gratuitement pour la version open source) couvrent les principales familles de malwares, les exploits connus, et les comportements C2 (Command & Control). La combinaison **Wazuh (endpoint) + Suricata (réseau) + Zeek (analyse de protocoles réseau)** forme une stack de détection complète qui couvre les angles morts : un attaquant qui se déplace latéralement via des protocoles légitimes (WMI, SMB, RDP) peut échapper à Suricata (pas de signature malveillante dans le trafic) mais être détecté par les agents Wazuh sur les endpoints cibles (logs d'authentification, création de processus). Suricata peut également être configuré en mode **IPS inline** pour bloquer automatiquement le trafic correspondant à des règles à haute confiance — un Active Response réseau complémentaire aux Active Responses endpoint de Wazuh.

Cas d'usage NIS 2 : SOC open source pour les PME-ETI françaises

La **directive NIS 2**, applicable aux entités essentielles et importantes françaises depuis fin 2024, impose des capacités de détection et de réponse aux incidents qui se traduisent concrètement par la nécessité d'un SOC (ou d'une surveillance équivalente). Pour les PME et ETI qui entrent dans le périmètre NIS 2 sans avoir historiquement investi dans un SOC, la stack Wazuh+TheHive+MISP+Shuffle est souvent la voie la plus réaliste économiquement. L'ANSSI ne prescrit pas d'outil spécifique mais attend des **capacités minimales** : collecte de logs de sécurité avec rétention adéquate (12 mois recommandés), détection d'anomalies, gestion des incidents documentée, et notification des incidents significatifs dans les 24 heures. Wazuh couvre

la collecte et la détection, TheHive couvre la gestion et la documentation des incidents, MISP fournit le contexte threat intelligence. La **notification ANSSI** d'un incident NIS 2 significatif peut s'appuyer sur les exports TheHive (rapport d'incident structuré) et les événements MISP (IoCs partagés avec le CERT-FR). Pour les entités qui ne souhaitent pas gérer la stack en interne, des **SOC managés (MSSP)** proposent la stack Wazuh+TheHive en service géré à partir de 2 000 à 5 000 €/mois pour 100-200 endpoints — une alternative viable aux déploiements self-managed.

FAQ — Stack SOC Open Source 2026

Faut-il choisir entre Wazuh et un SIEM commercial ou peut-on combiner les deux ?

Les deux cohabitent fréquemment. Un scénario courant : Wazuh pour la collecte des endpoints on-premise avec agents, et Microsoft Sentinel ou Elastic Security pour les logs cloud (AWS CloudTrail, Azure Activity Logs) et les données O365. Les logs Wazuh peuvent être forwardés vers Elastic Security via le module Elastic Beats. Cette architecture hybride profite des agents Wazuh (meilleurs que les agents Microsoft MMA/AMA pour les plateformes non-Windows) tout en bénéficiant de la puissance analytique de Sentinel pour les environnements Azure-centric.

TheHive est-il adapté à un SOC d'une seule personne ?

Oui, TheHive apporte de la valeur même pour un analyste SOC solo. Le case management structure le travail d'investigation et conserve l'historique des incidents — essentiel pour les audits et la mémoire organisationnelle. La version TheHive Community est gratuite et suffisante pour une organisation de taille modeste. Le retour d'un RSSI d'une collectivité territoriale (300 postes) : TheHive lui permet de documenter chaque incident même mineur, ce qui a permis d'identifier un pattern d'attaques ciblées sur plusieurs mois que la gestion par emails n'aurait jamais révélé.

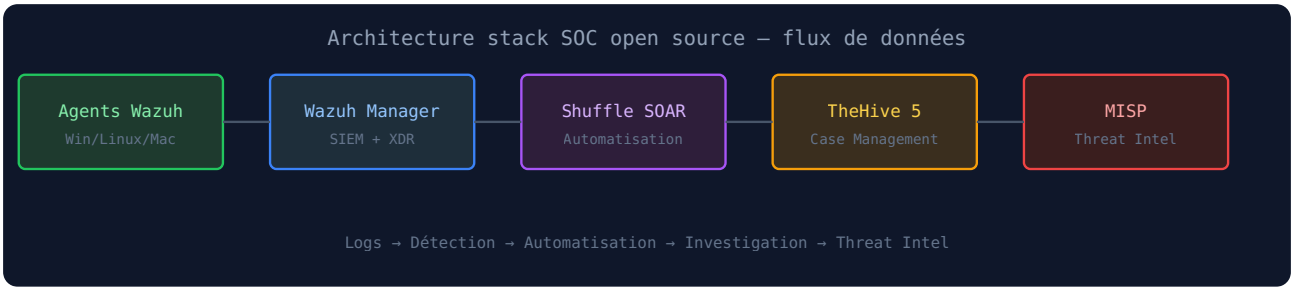
Comment démarrer avec MISP sans communauté de partage préexistante ?

Commencer par connecter MISP aux feeds gratuits publics (Abuse.ch, CIRCL OSINT, AlienVault OTX) pour avoir immédiatement une base d'IoCs utile sans partage de vos propres données. Puis rejoindre les communautés MISP sectorielles françaises — pour la santé (FSSI/CERT Santé), pour les collectivités territoriales (CERT-W), pour le secteur financier (CEIRIS). L'ANSSI gère une instance MISP nationale dont les grandes organisations étatiques peuvent bénéficier. Le partage sortant peut être progressif : commencer par partager des IoCs "nettoyés" (sans informations qui permettraient d'identifier votre organisation) puis augmenter progressivement le niveau de partage.

Shuffle est-il suffisant ou faut-il un SOAR commercial pour les équipes avancées ?

Shuffle couvre 80% des cas d'usage SOAR d'une équipe SOC. Les limites pour les équipes avancées : moins de connecteurs natifs "plug-and-play" que XSOAR ou Splunk SOAR pour les outils de niche, performances sous charge élevée (1000+ exécutions de workflows par heure) à valider selon la configuration. Pour les équipes avec des budgets limités, Shuffle est un excellent choix. Pour les MSSP gérant des dizaines de clients avec des milliers d'alertes par heure, les SOAR commerciaux (XSOAR, Splunk SOAR) restent plus robustes en termes de performances et de support des cas complexes.

Outil	Rôle SOC	Licence	RAM min.	Alternative commerciale
Wazuh	SIEM/XDR/HIDS	GPLv2	16 Go	Splunk, Sentinel, QRadar
TheHive 5	Case management	AGPL v3	8 Go	ServiceNow SecOps, Jira
MISP	Threat Intel	AGPL v3	8 Go	Anomali ThreatStream, STIX/TAXII
Shuffle	SOAR	AGPL v3	4 Go	XSOAR, Splunk SOAR
Velociraptor	EDR/DFIR	AGPL v3	4 Go	CrowdStrike, Carbon Black



La stack SOC open source Wazuh + TheHive + MISP + Shuffle n'est pas une solution magique qui fonctionne parfaitement dès l'installation — c'est un écosystème qui demande un investissement initial de configuration et de tuning, puis une maintenance continue d'une fraction d'ETP. Cet investissement est largement justifié par les économies de licence réalisées et par la flexibilité qu'offre le code source ouvert : personnalisation complète aux besoins de l'organisation, pas de dépendance à un éditeur qui peut changer sa politique tarifaire ou être racheté. En 2026, cette stack est mature, bien documentée, et bénéficie d'une communauté internationale active qui contribue régulièrement de nouvelles règles de détection, de nouveaux intégrations et de nouveaux modules. Pour aller plus loin dans votre SOC open source, consultez notre guide sur le durcissement Proxmox VE 8 pour sécuriser l'infrastructure hébergeant la stack, notre article sur Zabbix 7 pour la supervision de sécurité complémentaire à Wazuh, notre guide sur le pentest OT/ICS pour les SOC industriels, et notre article sur Vaultwarden pour la gestion des secrets et tokens d'API de la stack SOC. Pour les ressources communautaires, la documentation officielle Wazuh et le dépôt GitHub TheHive sont les points d'entrée incontournables de cet écosystème.