AYI NEDJIMI Consultants

Elastic SIEM : Stack Détection Open Source 2026 : Guide

Catégorie : SOC et Detection Lecture : 9 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Guide complet Elastic Security SIEM open source en 2026 : déploiement de la stack ELK, règles de détection, intégration Elastic Agent et cas d'usage.

Résumé exécutif

Ce guide présente le déploiement d'Elastic Security comme SIEM open source pour le SOC en 2026, couvrant l'architecture de la stack, les règles de détection préintégrées, l'intégration Elastic Agent et les stratégies d'optimisation pour les environnements de production. Les équipes de sécurité opérationnelle font face à des défis croissants : multiplication des surfaces d'attaque, sophistication des menaces persistantes avancées, et volumes de données qui dépassent les capacités d'analyse humaine. Dans ce contexte, une approche structurée et outillée devient indispensable pour maintenir une posture défensive efficace. Cet article propose une analyse technique approfondie, enrichie de retours d'expérience terrain et de recommandations concrètes pour les professionnels confrontés à ces enjeux au quotidien. Les architectures, méthodologies et outils présentés ici reflètent les pratiques observées dans les environnements de production les plus exigeants.

La montée en puissance d'Elastic Security comme alternative crédible aux SIEM commerciaux traditionnels représente l'une des évolutions les plus significatives du marché de la détection ces dernières années. En 2026, la solution a atteint un niveau de maturité qui lui permet de rivaliser avec des acteurs établis comme Splunk et Microsoft Sentinel sur de nombreux cas d'usage, tout en offrant un modèle économique radicalement différent basé sur l'open source. Pour les organisations qui disposent de compétences techniques solides et souhaitent maîtriser leur infrastructure de détection sans dépendre d'un éditeur propriétaire, Elastic Security représente une option particulièrement attractive. Cependant, le passage d'une stack ELK de monitoring à une véritable plateforme de sécurité opérationnelle requiert une approche structurée et des compétences spécifiques que ce guide se propose de détailler. De la conception de l'architecture au déploiement des agents de collecte, en passant par la configuration des règles de détection et l'intégration dans les workflows SOC existants, chaque étape doit être planifiée avec soin pour éviter les écueils classiques qui transforment un projet prometteur en une infrastructure sous-exploitée.

Retour d'expérience : Le déploiement d'Elastic Security pour une entreprise de services numériques de 3 000 collaborateurs a été réalisé en 6 semaines avec un cluster de 9 nœuds. Le coût total d'infrastructure (serveurs, stockage, administration) s'élève à 4 200 euros par mois, soit 70% de moins que l'offre commerciale SIEM équivalente évaluée. L'activation de 180 règles de détection préconfigurées a permis de détecter dès la première semaine une compromission de compte de service passée inaperçue depuis 3 mois.

Architecture de la stack Elastic Security

L'architecture d'Elastic Security repose sur les composants fondamentaux de la **stack Elastic**, adaptés et enrichis pour les cas d'usage de sécurité. Le cœur du système est *Elasticsearch*, le moteur de recherche et d'analyse distribué qui stocke et indexe les données de sécurité. Pour un déploiement SOC de production, prévoyez un cluster d'au minimum 3 nœuds master dédiés (pour la stabilité du cluster), des nœuds data dimensionnés en fonction du volume d'ingestion (comptez environ 1 vCPU et 2 Go de RAM par 50 Go de données actives), et des nœuds ingest pour le pré-traitement des données. **Kibana** fournit l'interface utilisateur avec le module Security qui offre un dashboard de détection, un timeline pour l'investigation, un gestionnaire de règles et un outil de case management intégré. **Fleet Server** et **Elastic Agent** constituent le système de collecte unifié qui remplace les anciens Beats, offrant une gestion centralisée des agents et une collecte multi-source via un agent unique par endpoint.

Le dimensionnement du cluster est un exercice critique. Pour un environnement ingérant 200 Go par jour avec une rétention de 90 jours en stockage chaud et 365 jours en stockage tiède, prévoyez environ 18 To de stockage total (les données indexées occupent environ 10% de plus que les données brutes grâce à la compression). Les **data tiers** (hot, warm, cold, frozen) permettent d'optimiser les coûts de stockage en déplaçant automatiquement les données vers des stockages moins coûteux à mesure qu'elles vieillissent, via les *Index Lifecycle Management (ILM)* policies. Utilisez des SSD NVMe pour le tier hot (données des 7 derniers jours) et des disques SATA haute capacité pour le tier warm (7-90 jours). Le tier cold peut utiliser un stockage objet compatible S3 via les searchable snapshots, réduisant drastiquement les coûts pour les données historiques tout en maintenant la possibilité de les interroger pour les investigations rétrospectives. Pour les environnements nécessitant une corrélation avec des données d'attaque Active Directory, consultez notre guide sur les techniques d'exploitation Kerberos.

Déploiement d'Elastic Agent et Fleet

Le déploiement de la collecte via **Elastic Agent** et **Fleet** est l'étape qui détermine la qualité des données disponibles pour la détection. Elastic Agent est un agent unifié qui remplace les multiples Beats spécialisés (Filebeat, Winlogbeat, Packetbeat, Auditbeat) par un agent unique capable de collecter tous les types de données. Fleet est le système de gestion centralisée qui permet de déployer, configurer et mettre à jour les agents à distance via des **policies**. Créez des policies distinctes pour chaque type de système : serveurs Windows, serveurs Linux, postes de travail, contrôleurs de domaine, serveurs web. Chaque policy agrège les *intégrations* pertinentes pour le type de système : Windows Event Logs, Sysmon, endpoint security (la protection intégrée d'Elastic), collecte de logs applicatifs spécifiques, etc.

Pour maximiser la couverture de détection sur les endpoints Windows, activez la collecte des **journaux clés** : Security (événements d'authentification, modification de permissions), System (démarrage de services, erreurs critiques), PowerShell (commandes exécutées, blocs de script), et surtout **Sysmon** si vous l'avez déployé (création de processus, connexions réseau, modifications du registre). L'intégration Elastic Defend ajoute des capacités de protection endpoint natives avec détection de malware, protection contre les ransomwares et visibilité sur les activités processus similaire à un EDR commercial. Cette convergence SIEM + EDR dans une

seule plateforme est un avantage majeur d'Elastic Security pour les organisations qui souhaitent consolider leurs outils. Pour les sources réseau, déployez des intégrations pour les pare-feu (Palo Alto, Fortinet, Check Point), les proxys web et les solutions DNS. Les **custom integrations** permettent de collecter des logs applicatifs spécifiques via des pipelines d'ingestion personnalisées. Consultez notre article sur l'exfiltration DNS pour des cas d'usage de détection réseau.

Composant	Rôle	Dimensionnement (200 Go/j)	Haute disponibilité
Master nodes	Coordination cluster	3 nœuds, 4 vCPU, 8 Go RAM	Quorum 3 nœuds
Data hot nodes	Ingestion et recherche récente	3 nœuds, 16 vCPU, 64 Go RAM, SSD NVMe	Réplication 1
Data warm nodes	Stockage données historiques	3 nœuds, 8 vCPU, 32 Go RAM, HDD	Réplication 1
Ingest nodes	Pré-traitement pipelines	2 nœuds, 8 vCPU, 16 Go RAM	Load balanced
Kibana	Interface utilisateur	2 instances, 4 vCPU, 8 Go RAM	Load balanced
Fleet Server	Gestion agents	2 instances, 4 vCPU, 8 Go RAM	Load balanced

Règles de détection et Detection Engine

Le **Detection Engine** d'Elastic Security est le moteur qui exécute les règles de détection et génère les alertes. Elastic fournit plus de 800 règles préconfigurées maintenues par l'équipe Elastic Security Research, couvrant la majorité des techniques MITRE ATT&CK. Ces règles sont régulièrement mises à jour pour suivre l'évolution des menaces et peuvent être activées en quelques clics depuis l'interface Kibana. Les types de règles disponibles incluent les **custom query rules** (requêtes KQL ou EQL personnalisées), les **threshold rules** (détection de dépassement de seuil), les **EQL sequence rules** (détection de séquences d'événements ordonnées temporellement), les **machine learning rules** (détection d'anomalies comportementales) et les **indicator match rules** (corrélation avec des IOC de threat intelligence).

Le langage *EQL (Event Query Language)* est un atout distinctif d'Elastic Security. Conçu spécifiquement pour la détection de menaces, EQL excelle dans la **détection de séquences d'événements** qui caractérisent les kill chains d'attaque. Par exemple, une règle EQL peut détecter la séquence : création d'un processus PowerShell encodé, suivi d'une connexion réseau vers une IP externe, suivi d'une création de fichier dans un répertoire temporaire, le tout dans une fenêtre de 5 minutes et sur le même hôte. Ce type de détection séquentielle est extrêmement puissant pour identifier des comportements d'attaque multi-étapes que des règles simples manqueraient. Le standard Sigma est également supporté via des convertisseurs qui traduisent les règles Sigma en requêtes Elastic, permettant de bénéficier de la vaste bibliothèque communautaire de règles de détection. Pour comprendre les techniques de persistence que vos règles doivent détecter, consultez notre article sur les attaques Silver Ticket.

Comment intégrer Elastic Security dans les workflows SOC existants ?

L'intégration d'Elastic Security dans les **workflows SOC** existants nécessite de connecter la plateforme avec les autres outils de l'écosystème. Le **case management** intégré à Kibana permet de créer et suivre des incidents directement depuis l'interface de détection, mais pour les SOC qui utilisent déjà un système de ticketing (ServiceNow, Jira, TheHive), l'intégration via les **connectors** Kibana est essentielle. Ces connecteurs permettent de créer automatiquement des tickets dans le système externe quand une alerte de haute sévérité est générée, assurant la continuité du workflow sans obliger les analystes à dupliquer manuellement les informations. Pour l'automatisation de la réponse, Elastic Security s'intègre avec les plateformes **SOAR** via son API REST documentée. Les playbooks SOAR peuvent interroger Elasticsearch pour enrichir les investigations, déclencher des actions de confinement via Elastic Defend (isolation d'endpoint, kill de processus) et mettre à jour le statut des alertes. L'intégration avec les **plateformes de threat intelligence** se fait via les indicator match rules qui vérifient les événements contre des listes d'IOC importées depuis MISP, OpenCTI ou des feeds commerciaux. Consultez notre article sur le Zero Trust pour des cas d'intégration avec l'écosystème Microsoft.

Pourquoi choisir l'open source pour son SIEM en 2026 ?

Le choix de l'**open source** pour le SIEM du SOC est une décision stratégique qui comporte des avantages significatifs mais aussi des responsabilités. Le premier avantage est la **maîtrise des coûts** : pas de licence par volume d'ingestion, ce qui permet de collecter tous les logs nécessaires sans arbitrage financier entre couverture de détection et budget. Le deuxième avantage est la **transparence** : le code source des règles de détection et du moteur est auditable, ce qui est crucial pour les organisations soumises à des exigences de souveraineté. Le troisième avantage est la **flexibilité** : la stack peut être déployée sur n'importe quelle infrastructure (on-premise, cloud privé, cloud public) sans dépendance à un fournisseur cloud spécifique. Le quatrième avantage est la **communauté** : Elastic bénéficie d'une communauté massive de contributeurs qui partagent des règles de détection, des intégrations et des bonnes pratiques.

En contrepartie, l'open source exige des **compétences internes** pour l'administration, le tuning et l'évolution de la plateforme. Contrairement aux SIEM SaaS où l'éditeur gère l'infrastructure, un cluster Elasticsearch de production nécessite une équipe capable de gérer le dimensionnement, les mises à jour, la haute disponibilité et l'optimisation des performances. Le coût caché de l'open source est le coût humain : une équipe de 2 à 3 ingénieurs est nécessaire pour maintenir un cluster de taille moyenne en production. Pour les organisations qui ne disposent pas de ces compétences, la souscription Elastic Gold ou Platinum offre un support commercial et des fonctionnalités supplémentaires (machine learning, RBAC avancé) qui réduisent la charge opérationnelle. Les recommandations de l'ANSSI en matière de souveraineté numérique renforcent l'attrait des solutions open source pour les administrations et les opérateurs d'importance vitale.

Mon avis : Elastic Security est devenu une option crédible pour les SOC de toute taille, mais le mythe du SIEM gratuit est dangereux. Les coûts d'infrastructure et d'administration d'un cluster Elasticsearch de production sont significatifs, et un déploiement sous-dimensionné ou mal administré sera moins efficace qu'un SIEM commercial bien configuré. Mon conseil : commencez par un POC de 3 mois avec un périmètre restreint, mesurez les coûts réels (infrastructure + temps humain) et comparez objectivement avec les alternatives commerciales avant de prendre votre décision définitive.

Quelles sont les limites d'Elastic Security à connaître ?

Malgré ses qualités, Elastic Security présente des **limites** qu'il faut connaître avant de s'engager. La première limite concerne les **fonctionnalités SOAR** : Elastic ne dispose pas d'un module SOAR intégré comparable à Splunk SOAR ou à l'automatisation native de Sentinel, nécessitant l'ajout d'un outil tiers pour l'orchestration avancée. La deuxième limite touche le *multi-tenancy* : la gestion de plusieurs clients ou entités dans un même cluster est plus complexe qu'avec des SIEM conçus pour le modèle MSSP. La troisième limite concerne la **courbe d'apprentissage** : l'administration d'un cluster Elasticsearch performant et résilient requiert des compétences spécifiques qui ne s'improvisent pas. Les problèmes de performance liés à un mauvais dimensionnement des shards, des mappings sous-optimaux ou une gestion inadéquate du garbage collector JVM sont les causes les plus fréquentes d'insatisfaction. Investissez dans la formation de vos équipes et dans un dimensionnement initial généreux plutôt que de devoir reconstruire votre cluster 6 mois après le déploiement. Pour les aspects forensiques complémentaires, explorez notre guide forensics Windows.

À retenir : Elastic Security offre une alternative open source crédible aux SIEM commerciaux, avec une détection puissante basée sur EQL, plus de 800 règles préconfigurées et un modèle économique libéré des coûts de licence par volume. Le succès repose sur un dimensionnement rigoureux du cluster, des compétences d'administration Elasticsearch solides et une intégration soignée avec les outils SOAR et threat intelligence existants.

Avez-vous réellement comparé le coût total de possession d'une stack Elastic auto-hébergée avec celui d'un SIEM commercial, en incluant le temps humain d'administration ?

Sources et références : MITRE ATT&CK · MITRE CAR

Perspectives et prochaines étapes

Elastic continue d'investir dans les fonctionnalités de sécurité avec l'amélioration continue du Detection Engine, l'ajout de capacités d'investigation assistée par IA et le renforcement des intégrations cloud. La convergence SIEM et EDR au sein d'une même plateforme va s'approfondir, offrant une expérience analyste de plus en plus unifiée. Pour démarrer votre projet Elastic Security, commencez par un lab de test avec un cluster minimal de 3 nœuds, activez les règles de détection correspondant à vos 10 cas d'usage prioritaires et évaluez la qualité des alertes générées sur vos données réelles. Cette approche progressive vous permettra de valider la pertinence de la solution pour votre contexte avant de vous engager dans un déploiement de production à grande échelle.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr