LAZAR SOFT

Expert Partner ManageEngine

FICHE SOLUTION · GESTION DES INFORMATIONS ET DES ÉVÉNEMENTS DE SÉCURITÉ (SIEM)

ManageEngine Log360

Une seule console pour toute votre sécurité.

Journaux, annuaire, postes, serveurs de fichiers et environnements cloud : Log360 rassemble la détection, l'investigation et la réponse au même endroit. Vos équipes cessent de recoller des consoles entre elles et travaillent sur des incidents déjà qualifiés.

- Contrôleurs de domaine
- Serveurs de fichiers Windows
- Sources de journaux
- Comptes cloud
- Postes de travail
- Sauvegarde et restauration AD

DEUX ÉDITIONS SUR SITE · LICENCE PAR COMPOSANT

Gratuite · Professionnelle

Tarif éditeur **à partir de 245 €/an** par composant, en abonnement ou en licence perpétuelle — grille complète en page 5.

2 000+
RÈGLES DE DÉTECTION PRÊTES À L'EMPLOI

750+
ANALYSEURS DE JOURNAUX INTÉGRÉS

30+
MODÈLES DE CONFORMITÉ PRÊTS POUR L'AUDIT

1 000+
WIDGETS D'ANALYSE

LAZAR SOFT
Distributeur & intégrateur ManageEngine en France

TÉLÉPHONE
+33 (0)1 76 21 60 43

E-MAIL
sales@lazarsoft.com

Moins d'alertes. Davantage de décisions.

Ce qu'est Log360

Log360 est la plateforme de gestion des informations et des événements de sécurité de ManageEngine. Elle collecte les journaux de l'ensemble du parc, les enrichit, les corrèle, et restitue des incidents qualifiés dans une console unique. La prévention des fuites de données et le contrôle des accès cloud y sont intégrés d'origine, sans brique additionnelle.

La plateforme est modulaire : chaque périmètre surveillé se licencie séparément. On démarre sur les contrôleurs de domaine, on ajoute les serveurs de fichiers puis les comptes cloud, sans changer d'outil ni rejouer le paramétrage.

Ce que la solution rend possible

- Réduire le volume d'alertes traitées à la main, en écartant l'activité connue comme bénigne.
- Reconstituer une chronologie d'attaque complète sans quitter la console.
- Repérer un compte compromis par l'écart au comportement habituel.
- Tenir un dossier d'audit RGPD, PCI DSS, HIPAA, SOX ou ISO 27001 sans le reconstruire à la main.
- Savoir si des identifiants de l'organisation circulent sur le dark web.

COMPOSANTS SOUS LICENCE

- Contrôleurs de domaine
- Serveurs de fichiers Windows
- Sources de journaux
- Comptes cloud
- Postes de travail
- Sauvegarde et restauration AD

EXIGENCES SYSTÈME

Serveur dédié recommandé, espace d'archivage non compris.
Minimum 12 cœurs · 32 Go RAM · 1,2 To SSD · 750 IOPS
Recommandé 24 cœurs · 48 Go RAM · 2,5 To SSD · 1 500 IOPS
Base PostgreSQL fourni ; en externe PostgreSQL 10 à 14 ou MS SQL 2012 et supérieur
Capacité d'un nœud 250 Go de journaux par jour ou 2 To de données de recherche ; au-delà, architecture distribuée

Le périmètre couvert par la plateforme — quatre chantiers

DÉTECTION

- Détection, investigation et réponse (Vigil IQ)
- Analyse comportementale (UEBA)
- Maîtrise du bruit et des faux positifs

JOURNAUX ET DONNÉES

- Collecte, analyse et archivage
- Renseignement sur les menaces
- Surveillance du dark web

PROTECTION

- Prévention des fuites de données
- Sécurité du cloud et contrôle des accès
- Posture de sécurité et des risques

RÉPONSE ET PREUVE

- Orchestration et automatisation
- Gestion des incidents
- Conformité réglementaire

Le détail de chaque chantier figure aux pages 3 et 4.

Plateformes prises en charge

SERVEUR LOG360

- Windows Server 2012 à 2025
- Ubuntu 14+, Red Hat 7+, CentOS 7+

PÉRIMÈTRES SURVEILLÉS

- Active Directory, Entra ID, serveurs, postes, pare-feu, routeurs, IDS/IPS
- AWS, Azure, GCP, Salesforce, Microsoft 365

COMPOSANTS INTÉGRABLES

- ADAudit Plus, ADManager Plus, PAM360
- Exchange Reporter Plus, DataSecurity Plus, Cloud Security Plus

Détecter, trier, enquêter

Détection, investigation et réponse automatisées

MODULE TDIR VIGIL IQ

- **Bibliothèque de plus de 2 000 règles** — règles de détection, de corrélation et d'anomalie, distribuées depuis le cloud et cartographiées sur le référentiel MITRE ATT&CK.
- **Mise à jour continue** — le catalogue suit l'apparition de nouveaux schémas d'attaque sans intervention sur l'installation.
- **Console d'incidents centrale** — la télémétrie de l'annuaire, des flux de menaces et des autres outils de sécurité se rassemble sur un même écran d'analyse.
- **Chronologies générées automatiquement** — reconstitution du parcours d'un utilisateur ou d'un incident, et suivi des filiations de processus.
- **Playbooks de réponse** — enchaînements de remédiation prédéfinis, déclenchés dès la qualification de la menace.

Analyse comportementale des utilisateurs et des entités

COMPOSANT UEBA

- **Référence apprise, pas déclarée** — le comportement normal de chaque compte et de chaque machine s'établit par apprentissage, puis se réévalue en continu.
- **Score de risque** — chaque écart alimente une note qui hiérarchise les utilisateurs à examiner en priorité.
- **Regroupement dynamique par pairs** — un comportement s'apprécie au regard de celui des collègues occupant la même fonction, ce qui réduit les fausses alertes.
- **Mise en correspondance des identités** — les comptes multiples d'une même personne sont rapprochés pour donner un contexte complet.
- **Menaces lentes** — les dérives qui s'installent sur plusieurs semaines restent visibles là où une règle de seuil les manque.

Maîtrise du bruit et des faux positifs

RÉGLAGE DES RÈGLES · SEUILS ADAPTATIFS

- **Réglage sans langage de requête** — chacune des règles s'ajuste depuis une interface visuelle, sans écrire de KQL, de SPL ni d'AQL.
- **Exclusions au niveau objet** — un utilisateur, un groupe, une unité d'organisation ou un appareil se retire d'une règle sans la désactiver.
- **Seuils adaptatifs** — l'apprentissage automatique distingue une variation saisonnière normale d'une véritable anomalie, et ajuste les bornes de lui-même.
- **Diagnostic d'optimisation** — les règles les plus bavardes sont identifiées, avec la correction à leur appliquer.
- **Sans angle mort** — l'objectif affiché est de réduire les faux positifs tout en maintenant une couverture complète des menaces.

Surveillance du dark web

SÉCURITÉ PROACTIVE

- **Veille sur les fuites d'identifiants** — le deep web et le dark web sont scrutés en continu à la recherche des comptes de l'organisation.
- **Périmètre étendu à la chaîne logistique** — la recherche couvre aussi les identifiants des prestataires et fournisseurs.
- **Données personnelles** — les expositions de données à caractère personnel sont signalées dès leur détection.
- **Exploitable, pas seulement informatif** — les résultats se reprennent dans la console d'incidents pour lancer une investigation.
- **Agir avant l'exploitation** — la démarche vise à traiter l'exposition pendant qu'elle n'a pas encore servi à une intrusion.

Renseignement et analyse avancée des menaces

FLUX PARTENAIRES

- **Flux de menaces mondiaux** — les indicateurs de compromission proviennent des partenaires technologiques de l'éditeur et sont rafraîchis en continu.
- **Réputation des adresses, domaines et URL** — une note de réputation accompagne chaque entité rencontrée dans les journaux.
- **Contexte d'enquête** — géolocalisation et éléments d'environnement sont joints à l'alerte pour accélérer le tri.
- **Résumés en langage naturel** — Zia Insights synthétise journaux, alertes et incidents, situe les techniques d'attaque et propose des mesures correctives.

Analyse de sécurité en temps réel

TOUTES LES SOURCES

- **Visibilité de bout en bout** — annuaire, serveurs de bases de données, équipements réseau, applications, terminaux et plateformes cloud alimentent le même référentiel.
- **Plus de 1 000 widgets d'analyse** — chaque équipe compose ses tableaux de bord autour des indicateurs qu'elle suit réellement.
- **Plateforme ouverte** — des interfaces de programmation standard couvrent l'ingestion, l'analyse et la réponse depuis des outils tiers.
- **Écosystème décloisonné** — appareils, applications et flux de renseignement se raccordent sans développement spécifique.

Collecter, protéger, répondre

Gestion et analyse des journaux

SOURCES DE JOURNAUX

- **Plus de 750 analyseurs intégrés** — les formats des équipements et applications les plus répandus sont reconnus sans configuration.
- **Analyseur personnalisé** — tout journal lisible par un humain se découpe en champs exploitables, y compris ceux d'applications internes.
- **Collecte avec ou sans agent** — l'agent sert notamment à traverser les liaisons étendues et les pare-feu.
- **Enrichissement à l'ingestion** — flux de menaces, géolocalisation et identité utilisateur sont ajoutés avant indexation.
- **Recherche avancée** — opérateurs booléens, expressions exactes, plages de valeurs, jokers et recherches groupées sur les journaux bruts.
- **Archivage probant** — les archives sont chiffrées et horodatées, avec des durées de conservation paramétrables par usage.

Prévention des fuites de données

SERVEURS DE FICHIERS WINDOWS

- **Découverte automatisée** — les données sensibles présentes sur le réseau sont recensées, avec des politiques de recherche adaptables au métier.
- **Classement par risque** — les fichiers sont hiérarchisés selon leur sensibilité et le type de données personnelles qu'ils contiennent.
- **Contrôle d'intégrité des fichiers** — création, accès, modification, suppression et changement de droits sont tracés sur les répertoires critiques.
- **Détection des exfiltrations** — les sorties anormales de données sont signalées par la détection d'anomalies.
- **Preuve pour l'audit** — les accès aux informations sensibles alimentent directement les rapports RGPD et PCI DSS.

Sécurité du cloud et contrôle des accès

COMPTES CLOUD · CASB INTÉGRÉ

- **Plateformes majeures couvertes** — AWS, Microsoft Azure, Google Cloud Platform et Salesforce remontent dans la même console.
- **Shadow IT** — les applications cloud utilisées hors validation sont identifiées, ainsi que les utilisateurs qui les sollicitent.
- **Surveillance des accès** — les connexions aux comptes cloud sont suivies et les tentatives non autorisées signalées.
- **Filtrage web** — l'accès aux applications et sites reconnus comme malveillants se bloque depuis la même politique.

Orchestration, automatisation et réponse

MODULE SOAR

- **Tâches répétitives automatisées** — affectation des incidents, enrichissement des données et étapes d'investigation s'exécutent seuls.
- **Playbooks** — les enchaînements de remédiation se construisent en glisser-déposer, sans développement.
- **Intégration à la gestion de services** — les tickets se créent et se mettent à jour dans l'outil ITSM en place.
- **Suivi du délai de résolution** — le tableau de bord des incidents restitue le temps moyen de traitement.
- **Réponse décloisonnée** — l'orchestration s'appuie sur l'outillage de sécurité déjà en place plutôt que de le doubler.

Posture de sécurité et gestion des risques

CONTRÔLEURS DE DOMAINE · MS SQL

- **Vue d'ensemble des failles** — les environnements critiques, à commencer par Active Directory et Microsoft SQL Server, sont évalués en continu.
- **Erreurs de configuration** — les écarts aux référentiels de durcissement sont remontés avec le geste correctif associé.
- **Hiérarchisation** — un niveau de risque global situe les points faibles à traiter en premier.
- **Corriger avant l'incident** — la démarche est préventive, en amont de toute détection d'attaque.
- **Sauvegarde de l'annuaire** — un module complémentaire couvre la sauvegarde et la restauration d'Active Directory.

Conformité réglementaire

TOUS LES COMPOSANTS

- **Plus de 30 modèles prêts pour l'audit** — les cadres réglementaires courants sont couverts d'origine, RGPD, PCI DSS, HIPAA, SOX, ISO 27001, GLBA et FISMA compris.
- **Profils internes** — les politiques propres à l'organisation se modélisent au même endroit que les référentiels publics.
- **Alertes de violation** — un écart aux exigences déclenche une notification sans attendre la campagne d'audit.
- **Rapports sur mesure** — les critères de génération se définissent librement pour couvrir une exigence non prévue par les modèles.
- **Preuve conservée** — les journaux archivés, chiffrés et horodatés restent produisibles pendant toute la durée exigée.

03 — ÉDITIONS ET TARIFS

Une licence par composant. On dimensionne avec vous.

ÉDITION GRATUITE

Jamais expirée

- Périmètre limité à 25 postes de travail
- Collecte, recherche, alertes, rapports planifiés et archives chiffrées
- Sans contrôle d'intégrité des fichiers, corrélation en temps réel, analyse universelle des journaux, base MS SQL externe ni agent de collecte à travers les pare-feu
- L'essai de 30 jours bascule automatiquement vers cette édition

ÉDITION PROFESSIONNELLE

Tarification par composant

- Nombre d'appareils au choix, sans plafond
- Corrélation en temps réel et contrôle d'intégrité des fichiers
- Analyse universelle des journaux et constructeur d'expressions régulières
- Architecture distribuée, supervision multi-sites, agent traversant les pare-feu
- Base Microsoft SQL en arrière-plan, authentification AD ou RADIUS, marque blanche

MODÈLES DE DÉPLOIEMENT

Sur site ou cloud

- Installation sur site : licence par composant, en abonnement ou en perpétuel
- Log360 Cloud : facturation à la source de journaux, éditions Free, Professional et Enterprise
- Log360 MSSP : déclinaison destinée aux prestataires de services managés
- Essai gratuit de 30 jours dans tous les cas

COMPOSANT DE LICENCE	PÉRIMÈTRE DE DÉPART	ABONNEMENT ANNUEL	LICENCE PERPÉTUELLE
Contrôleurs de domaine	2 contrôleurs	**945 €**	2 866 €
Serveurs de fichiers Windows	2 serveurs	**495 €**	1 486 €
Sources de journaux serveurs, pare-feu, routeurs, commutateurs, bases de données…	10 sources	**795 €**	2 386 €
Comptes cloud AWS, Azure, Google Cloud Platform, Salesforce	1 compte	**995 €**	2 986 €
Postes de travail	100 postes	**245 €**	736 €
MODULE COMPLÉMENTAIRE			
Sauvegarde et restauration Active Directory	2 contrôleurs	**245 €**	736 €

Tarifs publics éditeur au périmètre de départ de chaque composant, source : ManageEngine, page de tarification Log360, consultée le 1er septembre 2026. Chaque composant se décline ensuite par paliers de volume ; les montants ci-dessus correspondent au plus petit palier publié. Prix indicatifs et non contractuels : le montant applicable dépend des composants retenus, des volumes réels et du mode de déploiement. La licence est modulaire, chaque périmètre surveillé se souscrit séparément. Devis personnalisé LAZAR SOFT sur demande.

Contactez-nous.

Une question ou un chiffrage précis : un #RocketExpert vous répond sous 24 h ouvrées.

TÉLÉPHONE
+33 (0)1 76 21 60 43

E-MAIL
sales@lazarsoft.com