# Règles rejouées sur douze mois de journaux

LINDBERGH FORMATION — 16 rue de Maillé, 91310 Montlhéry · RCS Evry 817 946 114

Document établi le 09/11/2026

47 règles mesurées, 4 resserrées · document fictif

**Document fictif — exemple de démonstration**

Ce document est produit par le site Blue Lemon Agent pour illustrer ce qu'un agent IA remet à ses utilisateurs. Les sociétés, dossiers, montants et personnes qui y figurent sont inventés. Il n'a aucune valeur juridique, comptable ni commerciale.

**Document fictif**, produit pour la démonstration. **Une règle de détection est la condition écrite qui fait naître une alerte.** Chacune des 47 règles a été rejouée sur **douze mois de journaux archivés** : nombre d'alertes produites, part confirmée après instruction, et ce qu'elle laissait passer.

## Ce que la mesure sur douze mois montre

| Constat | Valeur | Lecture |
|---|---|---|
| **Règles produisant 44 % des alertes** | **3 sur 47** | **0 confirmation en douze mois** |
| **Règles produisant 61 % des confirmations** | **9 sur 47** | **Moins de 5 alertes par mois chacune — vos meilleures règles, que le tri remet en tête** |
| **Incidents réels de l'année** | **3** | **Tous remontés, tous placés dans les 3 premiers signaux de leur semaine** |

## Les quatre règles resserrées, chiffrées sur douze mois

| Règle | Alertes avant | Alertes après | Confirmations conservées |
|---|---|---|---|
| **Échecs d'authentification** | **84** | **19** | **3 sur 3** |
| Connexions hors horaires | 310 | **41** | **2 sur 2** |
| Accès aux partages | 240 | **58** | **1 sur 1** |
| Erreurs applicatives | 186 | **12** | Aucune confirmation à conserver |
| **Total** | **820** | **130** | **6 sur 6** |

**Le raisonnement ne repose sur aucune intuition :** chaque règle proposée est écrite dans la forme des règles existantes, passée sur douze mois de journaux réels, et présentée avec le nombre d'alertes qu'elle produit, la part confirmée et les incidents qu'elle continue de remonter. **Le choix se fait sur des chiffres.**

> **Chaque règle se signe et se retire séparément**, sans toucher aux quarante-six autres. Une règle mise en vigueur le soir peut être retirée le lendemain matin, et le décompte des alertes écartées reste consultable en permanence.

Règles retenues pour mise en vigueur : _____

> **Demandez une démonstration avec vos propres documents**
> Ce document est un exemple fictif. Pour voir l'agent travailler sur vos propres documents, demandez une démonstration depuis sa fiche.
> https://bluelemonagent.ai/entreprises/cas-usage/agent-de-cybersecurite-analyse-de-logs

et au repos, leurs composants et la gestion des clés sont ceux documentés pour l'architecture retenue ; les rôles et permissions sont configurés et recettés pour les identités et systèmes effectivement raccordés ; les événements journalisés, leur contenu, leur durée de conservation et leurs accès sont définis pour le déploiement retenu.