Plan de durcissement — cinq causes racines

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

Document établi le 09/11/2026

3 correctifs = 61 % d'alertes en moins · 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. **Chaque correctif est présenté avec l'effet qu'il aurait eu sur douze mois de journaux réels**, et non avec un bénéfice annoncé. Le durcissement se juge ensuite semaine après semaine sur les alertes constatées.

Les cinq causes et leurs correctifs

Cause racine	Correctif	Effort	Effet mesuré sur 12 mois
Comptes de service non restreints à leurs machines	**Liste par compte, 7 comptes**	**30 min de fenêtre**	**6 déclenchements historiques sur 6 bloqués à l'authentification**
Droits résiduels d'un projet clos en 2023	Retrait sur 3 postes	12 min	Aucun effet sur l'usage constaté depuis 90 jours
Journaux locaux des postes non collectés	**Collecte lecture seule, 14 postes**	Progressive	**Les 4 investigations restées incomplètes auraient été closes**

Cause racine	Correctif	Effort	Effet mesuré sur 12 mois
3 règles produisant 44 % du bruit	**4 règles resserrées signées**	Immédiat	**620 alertes de moins par semaine, déjà constaté**
Calendrier de changement non rapproché des alertes	**Lecture avant qualification**	Immédiat	**2 signaux de haut niveau évités en trois mois**

Les trois vagues

Vague	Contenu	Durée cumulée	Effet sur la production
1 — cette semaine	Retrait des droits résiduels, lecture du calendrier de changement	**16 minutes**	**Aucun**
2 — prochaine fenêtre	Listes de machines des comptes de service	**30 minutes**	Un redémarrage de service
3 — sur le mois	Collecte des journaux de postes, par lots de 5	Progressive	Lecture seule

> **L'effet de chaque vague est mesuré sur les alertes réelles, semaine par semaine.** Un durcissement qui ne se mesure pas ne se défend pas devant une direction ; celui-ci porte ses chiffres avec lui.

Vagues validées et dates retenues : _____

LINDBERGH FORMATION — Blue Lemon Agent — RCS Évry 817 946 114 —
Mentions légales : bluelemonagent.ai/mentions-legales

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

---

Portée de ce document : le service exploité par Blue Lemon Agent. Pour un agent déployé chez vous, la localisation applicable est celle de l'architecture décrite au devis et vérifiée avant mise en service ; l'exécution locale n'est annoncée que pour la configuration explicitement décrite et recettée au devis ; l'isolation applicable dépend du mode de déploiement décrit au devis, aucune isolation dédiée n'étant présumée ; les mécanismes de chiffrement en transit 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.