Tri hebdomadaire — 1 400 alertes

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

Document établi le 09/11/2026

3 signaux, 1 240 motifs écrits · 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 alerte écartée n'est pas une alerte effacée** : chacune conserve son motif, reste consultable et se rouvre d'un clic. Le tri porte sur la totalité des 1 400 alertes de la semaine, pas sur un échantillon.

Ce que la semaine contenait

Catégorie	Nombre	Traitement
Signaux qualifiés à instruire	**3**	**Chaîne d'événements corrélée et horodatée fournie**
Écartées avec motif écrit	**1 240**	**Motif consultable, réouverture en un clic**
dont issues de 3 règles dont le seuil reste à resserrer	**620**	Regroupées, proposition de resserrement chiffrée
Regroupées en familles pour réglage	**157**	9 familles, décision de réglage attendue
Total	**1 400**	**Toutes passées au crible**

Les trois signaux

Signal	Ce qui est observé	Événements corrélés	Élément décisif
1	**214 échecs d'authentification sur 38 comptes, 3 adresses, 11 minutes**	**34 sur 4 sources**	**Une réussite sur un compte de recette**
2	**Compte de service authentifié depuis un poste bureautique**	34 sur 6 sources	**0 occurrence sur les 90 jours précédents**
3	**Volume d'export multiplié par 22, 22 h 40 – 23 h 05**	18 sur 3 sources	**Hors de toute fenêtre de maintenance déclarée**

Le temps déplacé

Poste	Avant	Après
Corrélation des événements	**65 % du temps d'instruction**	**7 %**
Qualification d'une alerte	**40 %**	**6 %**
Alertes réellement examinées par semaine	**41 sur 1 400**	**1 400 sur 1 400**

Seuil de remontée souhaité par le RSSI : _____

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

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

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.