Détection comportementale — trois règles proposées

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

Document établi le 09/11/2026

Lignes de base sur 90 jours · 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. **La ligne de base est le comportement habituel d'un compte, d'une machine ou d'une tranche horaire**, mesuré ici sur **90 jours glissants**. Elle est calculée par compte et par machine : une moyenne d'entreprise ne montrerait rien.

Deux comportements qu'aucune règle ne décrivait

Comportement	Ligne de base sur 90 jours	Observation	Pourquoi aucune règle ne le voyait
Compte de service authentifié depuis un poste	**4 100 authentifications, toujours depuis 2 serveurs**	**1 authentification depuis un poste bureautique**	**Aucune règle ne dit d'où un compte de service a le droit de venir**

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

Comportement	Ligne de base sur 90 jours	Observation	Pourquoi aucune règle ne le voyait
Volume d'export d'un compte	**4 à 11 Mo par soirée**	**214 Mo en 25 minutes**	**Le seuil fixe existant était bien au-dessus**

Les trois règles écrites, mesurées sur douze mois

Règle proposée	Déclenchements sur 12 mois	Confirmés après instruction	Charge pour les analystes
Un compte de service s'authentifie depuis une machine absente de sa liste	**6**	**4**	1 par bimestre
Un compte dépasse de 10 fois son volume d'export habituel	**11**	**3**	1 par mois
Une authentification réussit après plus de 50 échecs sur la même plage	**4**	**2**	1 par trimestre
Total	**21 par an**	**9**	**Moins d'une par quinzaine**

Une règle proposée ne vaut que par la mesure qui l'accompagne. Chacune des trois est présentée avec ce qu'elle produit, ce qu'elle confirme et la charge qu'elle impose — de sorte que la décision de mise en vigueur se prenne en quelques minutes plutôt qu'en comité.

> **La détection comportementale complète les règles écrites, elle ne les remplace pas.** Les deux mécanismes travaillent en parallèle sur les mêmes journaux, et un signal issu de l'un comme de l'autre arrive avec sa chaîne d'événements

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

horodatée.

Règles comportementales retenues et périmètre : _____

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.