Procédure de contrôle des logs VMS

Référence	Version	Date	Catégorie
PROC-VMS-003	v1.1	Avril 2025	Exploitation VMS & Vidéosurveillance

Les journaux d'événements (logs) du VMS constituent la mémoire opérationnelle et de sécurité du système. Cette procédure définit les catégories de logs à contrôler, la fréquence des contrôles, les indicateurs d'anomalie à surveiller et la procédure de signalement en cas de détection d'un événement suspect.

---

01. Catégories de logs à contrôler

Les logs de connexion enregistrent chaque tentative de connexion au système VMS (succès ou échec), l'identifiant utilisé, l'adresse IP source et l'horodatage. Ils permettent de détecter les tentatives d'accès non autorisées, les connexions en dehors des plages horaires habituelles et les attaques par force brute.

Les logs de consultation des enregistrements documentent chaque accès à une séquence vidéo archivée : identifiant de l'utilisateur, caméra(s) consultée(s), plage temporelle visionnée et durée de la consultation. Ces logs sont essentiels pour prouver la légitimité d'un accès en cas de contestation.

Les logs d'export tracent chaque opération d'extraction d'images ou de vidéos depuis le système : identifiant de l'utilisateur, caméra(s) exportée(s), plage temporelle, format et volume de données exportées. Un volume d'export anormalement élevé constitue un signal d'alerte majeur.

Les logs de modification de configuration enregistrent toute modification apportée aux paramètres du système (ajout ou suppression de caméra, modification des règles d'enregistrement, création ou suppression de compte, changement de rôle). Ces logs

doivent être recoupés avec les bons d'intervention et les demandes de changement validées.

---

02. Fréquence et méthode de contrôle

Le contrôle des logs est réalisé chaque semaine par le Responsable Sécurité ou son délégué. La revue hebdomadaire couvre les sept derniers jours et porte prioritairement sur les connexions hors plages horaires, les exports et les modifications de configuration.

Un outil de filtrage et d'alerting automatique est configuré pour notifier le Responsable Sécurité en temps réel en cas de détection d'un événement anormal (voir indicateurs ci-dessous). La revue hebdomadaire ne se substitue pas à ce système d'alerte : elle vise à détecter les anomalies de faible intensité passées sous le seuil d'alerte.

---

03. Indicateurs d'anomalie

Une connexion en dehors des heures d'ouverture du site (définie comme la plage 07h00–20h00 en jours ouvrés, sauf configuration spécifique) constitue un indicateur d'anomalie de niveau 1 nécessitant une vérification. Si la connexion n'est pas justifiée par un bon d'intervention ou une astreinte documentée, elle devient un incident de sécurité.

Un export massif est défini comme une opération d'extraction portant sur plus de 2 heures de vidéo ou plus de 3 caméras simultanées, réalisée en dehors d'une procédure d'export formalisée. Un tel événement déclenche automatiquement une notification au Responsable Sécurité et au DPO.

Plusieurs tentatives de connexion échouées (plus de 5 en moins de 10 minutes sur un même compte) constituent un indicateur d'attaque par force brute ou de tentative d'intrusion. Le compte ciblé est temporairement verrouillé et le Responsable Sécurité est alerté immédiatement.

---

04. Procédure de signalement

Toute anomalie détectée lors du contrôle hebdomadaire ou par le système d'alerte automatique donne lieu à l'ouverture d'un ticket d'incident dans l'outil de gestion utilisé par l'organisation. Le ticket précise la nature de l'anomalie, l'horodatage, les logs bruts associés et le niveau de criticité estimé.

> **Les incidents de niveau 1 (connexion non justifiée hors horaires) sont traités dans un délai de 48 heures. Les incidents de niveau 2 (export non autorisé, modification de configuration sans bon d'intervention) sont traités dans les 24 heures et font l'objet d'un rapport circonstancié. Les incidents de niveau 3 (tentative d'intrusion, accès à des données sensibles) déclenchent une procédure d'urgence impliquant le RSSI, le DPO et, si nécessaire, la CNIL.**

Boulevard de Courcelles, 75008 Paris — hello@mileotech.com