Politique de journalisation et logs

Référence	Version	Date	Catégorie
POL-CYB-008	v1.0	Avril 2025	Cybersécurité

La journalisation est un composant essentiel de la sécurité des systèmes de vidéosurveillance : elle permet de détecter les incidents, d'investiguer les événements suspects et de fournir des preuves en cas de litige ou de procédure judiciaire. Sans journalisation adéquate, un accès non autorisé peut passer inaperçu pendant des mois. Mileo Technology définit les événements à journaliser, les formats et les durées de conservation applicables à ses installations.

---

01. Événements à journaliser

Les événements suivants doivent être journalisés sur tous les systèmes gérés : connexions et déconnexions (succès et échecs), toutes les modifications de configuration (ajout/suppression de caméras, modification des droits utilisateurs, changement des paramètres d'enregistrement), accès aux flux vidéo en direct et aux enregistrements, exports vidéo, alertes de sécurité (détection de mouvement hors plage normale, tentatives d'accès répétées).

Les événements système sont également journalisés : démarrage et arrêt des équipements, erreurs matérielles (disque défaillant, surchauffe), perte de connexion réseau, synchronisation NTP (pour garantir l'intégrité des horodatages), mises à jour de firmware.

---

02. Format standardisé et horodatage

Les journaux doivent inclure au minimum : horodatage précis (format ISO 8601, synchronized NTP), identité de l'acteur (nom d'utilisateur, adresse IP source), action réalisée, objet de l'action (équipement, configuration, plage vidéo), résultat (succès/échec/erreur). Un format

structuré (JSON ou CEF — Common Event Format) est recommandé pour faciliter l'analyse automatisée.

La synchronisation NTP de tous les équipements sur une source de temps de référence est une exigence absolue pour la validité des journaux. Un équipement dont l'horloge est désynchronisée produit des journaux inutilisables en cas d'investigation. La synchronisation NTP est vérifiée lors de chaque intervention de maintenance.

---

03. Conservation et protection

Les journaux sont conservés pendant 12 mois minimum, conformément aux recommandations ANSSI et aux exigences légales applicables aux systèmes de vidéosurveillance. Pour les sites classés sensibles ou soumis à des contraintes réglementaires spécifiques (OIV, NIS2), la durée de conservation est portée à 24 mois.

Les journaux doivent être protégés contre la suppression ou la modification non autorisée. Les mécanismes de protection incluent : droits d'accès restreints en lecture seule pour les opérateurs, export vers un système de stockage distinct des équipements journalisés, signature ou horodatage cryptographique garantissant l'intégrité.

---

04. Centralisation et analyse

La centralisation des journaux dans un SIEM (Security Information and Event Management) est recommandée pour les sites de taille significative et les clients disposant d'une équipe sécurité. Mileo Technology peut proposer et intégrer des solutions SIEM adaptées, ou transmettre les logs vers le SIEM existant du client.

> **En l'absence de SIEM, une revue manuelle des journaux critiques est réalisée lors de chaque intervention de maintenance préventive. Des alertes automatiques sont configurées sur les équipements pour les événements prioritaires : tentatives d'accès répétées, connexions en dehors**

> **des plages horaires définies, modifications de configuration non planifiées.**

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