Politique de traçabilité des accès vidéo

Référence	Version	Date	Catégorie
POL-RGPD-003	v1.0	Septembre 2024	RGPD & Conformité Vidéosurveillance

La traçabilité des accès aux systèmes de vidéosurveillance est une exigence fondamentale de conformité RGPD et de sécurité opérationnelle. Elle permet de démontrer que les données personnelles collectées n'ont été consultées que par des personnes habilitées, à des fins légitimes, et de détecter tout accès anormal ou abusif.

---

01. Journalisation obligatoire des accès

Tout accès au système de vidéosurveillance — qu'il s'agisse d'une connexion au VMS, d'une consultation d'archives, d'une extraction ou d'une modification de paramètres — fait l'objet d'un enregistrement automatique dans le journal des accès. Ce journal capture a minima : l'identifiant de l'utilisateur, la date et l'heure de l'opération (avec fuseau horaire), la nature de l'opération (connexion, consultation live, accès archive, export, modification de configuration), et les caméras ou zones concernées.

Pour les opérations d'extraction, le journal précise en outre la plage horaire des enregistrements extraits, le format et la taille du fichier produit, et le motif déclaré par l'utilisateur si le système le permet. Ces informations permettent de reconstituer précisément qui a accédé à quoi et pourquoi, en cas de contrôle ou d'incident.

---

02. Durée de conservation des logs

Les journaux d'accès sont conservés au minimum douze mois à compter de leur génération. Cette durée est recommandée par les référentiels de sécurité des systèmes d'information (ANSSI, CIS

Controls) et permet de couvrir les délais habituels de détection des incidents. Pour les sites soumis à des contraintes réglementaires spécifiques (OIV, secteur financier), une durée de conservation de vingt-quatre mois est recommandée.

La durée de conservation des logs ne doit pas être confondue avec celle des enregistrements vidéo, qui est généralement plus courte (30 jours par défaut). Les logs peuvent et doivent être conservés bien au-delà de la durée de conservation des images elles-mêmes, afin de permettre une reconstitution a posteriori des accès même après purge des enregistrements.

---

03. Protection des logs contre la modification

L'intégrité des journaux d'accès est une condition sine qua non de leur valeur probatoire. Les logs doivent être protégés contre toute modification, suppression ou altération, y compris par les administrateurs système. Pour ce faire, il est recommandé d'exporter les logs vers un système centralisé de gestion des événements (SIEM) ou vers un serveur de logs dédié, séparé du système de vidéosurveillance, avec des droits d'accès distincts.

La cohérence et l'intégrité des logs sont vérifiées périodiquement par un mécanisme de hachage ou de signature numérique. Toute altération détectée fait l'objet d'une alerte immédiate et d'une enquête. Les logs d'audit de l'administrateur système sont eux-mêmes journalisés sur un système distinct, créant une chaîne de traçabilité sans lacune.

---

04. Audit régulier des journaux

Une revue des journaux d'accès est réalisée au minimum trimestriellement par le responsable de la sécurité ou le DPO. Cette revue recherche les anomalies : connexions en dehors des horaires habituels, accès à des zones non habituellement consultées par l'utilisateur, volume inhabituellement élevé d'extractions, tentatives de connexion échouées répétées.

> **Tout accès anormal identifié fait l'objet d'une enquête interne. Si l'accès est justifié (urgence,**

> **remplacement), il est documenté a posteriori. S'il ne l'est pas, les mesures disciplinaires ou de sécurité appropriées sont prises. Les résultats de chaque revue de logs sont consignés dans un rapport conservé cinq ans.**