# Livre blanc cybersécurité vidéosurveillance

| Référence | Version | Date | Catégorie |
|---|---|---|---|
| **GUID-PREM-002** | v1.0 | Mai 2025 | Documents Premium |

> ***Premium***

Les systèmes de vidéosurveillance IP sont devenus des cibles prioritaires pour les attaquants, tant pour leur valeur informationnelle (accès aux images de sites sensibles) que pour leur capacité à servir de vecteurs d'attaque vers d'autres systèmes du réseau. Ce livre blanc dresse un état des menaces, analyse les vulnérabilités les plus courantes et propose un cadre d'action concret pour les organisations souhaitant sécuriser leur parc de caméras.

---

## 01. État des menaces sur les systèmes de vidéosurveillance

Les incidents impliquant des systèmes de vidéosurveillance se multiplient depuis 2020. Parmi les cas les plus documentés : la compromission de 150 000 caméras Verkada en 2021 par un groupe d'hacktivistes ayant eu accès aux flux en direct de prisons, hôpitaux et entreprises américaines ; les attaques régulières de NVR par des ransomwares ciblant spécifiquement les systèmes de sécurité pour paralyser les capacités de surveillance lors d'intrusions physiques ; et les fuites de flux vidéo d'équipements mal configurés, visibles sur des moteurs de recherche spécialisés comme Shodan.

Les vecteurs d'attaque les plus fréquents sont l'exploitation de vulnérabilités connues non corrigées (firmware obsolète), l'authentification faible (identifiants par défaut, mots de passe simples), l'exposition directe sur Internet sans protection (caméras et NVR avec port de management accessible publiquement) et la compromission via la chaîne d'approvisionnement (mise à jour malveillante, équipement livré avec firmware modifié).

Les botnets de caméras représentent une menace spécifique. Le botnet Mirai, découvert en 2016 et ayant causé des attaques DDoS de plus de 600 Gb/s contre des infrastructures critiques mondiales, était principalement composé de caméras IP et d'enregistreurs DVR exploitant les identifiants par défaut. Ses variantes continuent d'infecter des centaines de milliers d'équipements chaque année. Une caméra compromise peut ainsi devenir à la fois une source de fuite d'information et un soldat d'une armée botnet.

---

## 02. Vulnérabilités courantes

Le firmware obsolète est la première cause de compromission des équipements de vidéosurveillance. Les constructeurs publient régulièrement des correctifs de sécurité, mais leur application est rarement automatisée sur les équipements de surveillance et souvent négligée dans les cycles de maintenance. Une étude de 2024 révèle que 45 % des caméras IP en service dans les PME européennes fonctionnent avec un firmware présentant au moins une vulnérabilité critique connue.

Les mots de passe par défaut restent un problème endémique malgré les années de sensibilisation. Certains constructeurs maintiennent des identifiants identiques pour tous les équipements d'une même gamme, facilement trouvables dans les manuels publiquement accessibles. D'autres implémentent des mots de passe générés à partir du numéro de série, réduisant considérablement l'espace de recherche pour un attaquant ayant accès à l'équipement physiquement.

Les protocoles de communication non chiffrés constituent un vecteur d'interception majeur. Le protocole RTSP (Real Time Streaming Protocol) est encore largement utilisé sans chiffrement, permettant à tout attaquant positionné sur le réseau de capturer les flux vidéo. De même, de nombreuses interfaces web d'administration de NVR et de caméras restent accessibles en HTTP simple, exposant les identifiants de connexion en clair.

---

## 03. Recommandations ANSSI

L'ANSSI a publié en 2023 un guide de recommandations pour la sécurisation des systèmes de vidéoprotection, s'inscrivant dans sa

série de guides de sécurisation des systèmes industriels et des équipements IoT. Les recommandations prioritaires portent sur : l'isolation réseau des équipements de vidéosurveillance, la désactivation des services non indispensables, l'utilisation de protocoles chiffrés pour la supervision et les flux vidéo, la gestion rigoureuse des identifiants et l'obligation de mise à jour des firmwares.

L'ANSSI recommande également la mise en place d'une supervision de sécurité spécifique aux équipements de vidéosurveillance, permettant de détecter les comportements anormaux (connexions depuis des adresses IP inconnues, volumes de trafic sortant inhabituels, tentatives d'authentification répétées) et de déclencher des alertes en temps réel. Cette recommandation s'aligne avec les exigences NIS2 pour les opérateurs soumis à cette directive.

---

## 04. Approche Mileo Technology

Mileo Technology a intégré la sécurisation cyber des équipements dans son processus de mise en service depuis 2022. Chaque installation fait l'objet d'une checklist de durcissement systématique : changement des identifiants par défaut, désactivation des ports et services non utilisés, mise à jour du firmware à la dernière version stable, vérification de l'isolation réseau, activation du chiffrement des communications.

Pour les projets de niveau Renforcé et Premium, un rapport de mise en service cybersécurité est remis au client documentant l'état de chaque équipement au regard des recommandations ANSSI. Ce rapport sert de base à l'audit annuel inclus dans les contrats de maintenance Premium et permet de suivre l'évolution de la posture de sécurité dans le temps.

---

## 05. Mise en œuvre pratique

La sécurisation d'un parc existant doit être abordée de manière pragmatique, par priorités. La première étape est l'inventaire exhaustif des équipements (caméras, NVR, switchs PoE, serveurs VMS) avec leur version de firmware et leur mode de connexion au réseau. Cet inventaire révèle systématiquement des équipements oubliés, des firmwares très anciens et des équipements accessibles depuis Internet sans protection.

> **Sur la base de l'inventaire, un plan de remédiation est établi en trois phases : Phase 1 (urgente, sous 30 jours) — correction des vulnérabilités critiques, changement des identifiants par défaut, isolation des équipements exposés sur Internet ; Phase 2 (dans les 90 jours) — mise à jour de l'ensemble des firmwares, segmentation réseau, activation du chiffrement ; Phase 3 (dans les 6 mois) — déploiement de la supervision de sécurité, test d'intrusion, documentation.**


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