Guide de durcissement VMS

Référence	Version	Date	Catégorie
GUID-PREM-003	v1.3	Mars 2025	Documents Premium

> ***Premium***

Le serveur VMS (Video Management System) est le composant le plus critique d'un système de vidéosurveillance IP. Sa compromission donne accès à l'ensemble des flux vidéo du site, aux enregistrements historiques, aux configurations des caméras et potentiellement aux autres systèmes avec lesquels il est intégré. Ce guide détaille les mesures de durcissement à appliquer au serveur VMS, à ses composants logiciels et aux équipements périphériques.

---

01. Durcissement du serveur VMS

Le système d'exploitation du serveur VMS doit être durci conformément aux recommandations du CIS Benchmark correspondant (Windows Server 2022 ou Linux selon le VMS). Les étapes essentielles comprennent : la désactivation de tous les services Windows non nécessaires au fonctionnement du VMS (Bluetooth, Windows Search, Remote Registry, Print Spooler si inutile), la suppression des composants optionnels non utilisés, l'activation du pare-feu local avec une règle de liste blanche stricte (seuls les ports nécessaires sont ouverts), et la configuration d'un compte d'administration dédié distinct du compte administrateur local par défaut.

La gestion des mises à jour doit être automatisée : les correctifs de sécurité critiques doivent être appliqués dans les 72 heures suivant leur publication. Pour les environnements nécessitant des tests préalables, un environnement de staging doit être disponible pour valider les mises à jour avant déploiement en production. Les mises à jour du VMS lui-même suivent le processus du constructeur mais ne doivent jamais être différées de plus de 30 jours.

L'antivirus et l'EDR (Endpoint Detection and Response) sont obligatoires sur le serveur VMS, avec des exclusions soigneusement

définies pour les répertoires de stockage vidéo (pour éviter la dégradation des performances d'écriture) sans pour autant exclure les répertoires d'exécutables et de configuration du VMS. Les journaux de l'EDR sont centralisés dans le SIEM si disponible.

---

02. Configuration sécurisée du VMS

Le chiffrement des communications est la première mesure à configurer dans le VMS. Les connexions entre les clients VMS (postes opérateurs) et le serveur doivent utiliser TLS 1.2 minimum (TLS 1.3 recommandé) avec des certificats valides, idéalement émis par une PKI interne ou une autorité de certification reconnue. Les certificats auto-signés sont acceptables en environnement de test uniquement. La durée de validité des certificats ne doit pas excéder 2 ans.

Les accès anonymes doivent être systématiquement désactivés, y compris pour les flux RTSP publics que certains VMS activent par défaut pour faciliter l'intégration avec des afficheurs tiers. Chaque utilisateur ou système accédant au VMS doit s'authentifier avec des identifiants nominatifs. Les comptes de service utilisés pour les intégrations (contrôle d'accès, hypervision) doivent disposer des droits stricts nécessaires à leur fonction, sans droits d'administration.

La journalisation des accès et des actions doit être activée de manière exhaustive : connexions réussies et échouées, exports de vidéos, modifications de configuration, ajout et suppression de caméras. Ces journaux doivent être expédiés vers un système de journalisation centralisé externe au serveur VMS, pour éviter qu'un attaquant ayant compromis le VMS puisse effacer les traces de son passage.

---

03. Durcissement des NVR et caméras IP

Les NVR (Network Video Recorders) et caméras IP doivent faire l'objet d'un durcissement systématique lors de leur mise en service. Les étapes obligatoires sont : changement du mot de passe administrateur par défaut pour un mot de passe conforme à la politique de l'entreprise (minimum 12 caractères, complexité imposée), désactivation des interfaces d'administration non utilisées (Telnet, FTP, HTTP si HTTPS disponible), désactivation des protocoles de découverte automatique non nécessaires (UPnP, Bonjour, ONVIF Discovery si non requis).

La mise à jour du firmware des caméras et NVR doit être réalisée lors de la mise en service et intégrée au contrat de maintenance. Un inventaire centralisé recense la version de firmware de chaque équipement et est mis à jour après chaque intervention. Les équipements pour lesquels le constructeur ne publie plus de mises à jour de sécurité sont signalés au client et font l'objet d'un plan de remplacement.

---

04. Checklist de vérification

La checklist de durcissement VMS est documentée et signée par le technicien responsable de la mise en service. Elle couvre 32 points de contrôle regroupés en quatre catégories : serveur et OS (8 points), VMS applicatif (10 points), NVR et stockage (7 points), caméras IP (7 points). Chaque point est évalué comme Conforme, Non conforme (avec commentaire et délai de remédiation) ou Non applicable (avec justification).

> **La checklist complétée est remise au client dans le dossier de mise en service et conservée par Mileo Technology pendant la durée du contrat de maintenance. En cas d'audit de sécurité, elle constitue la preuve documentaire des mesures de durcissement appliquées à la mise en service. Elle est reprise et mise à jour lors de chaque audit annuel inclus dans les contrats Premium.**