Modèle de rapport cybersécurité VMS

Référence	Version	Date	Catégorie
MOD-CRM-004	v1.0	Février 2025	Commercial & Relation Client

> ***Modèle***

Les systèmes de gestion vidéo (VMS) et les enregistreurs réseau (NVR) constituent des cibles privilégiées pour les cyberattaquants, car ils sont souvent connectés au réseau d'entreprise et insuffisamment durcis. Ce modèle structure les audits de cybersécurité des infrastructures vidéo réalisés par Mileo Technology, en s'appuyant sur les référentiels ANSSI et les meilleures pratiques de sécurité des systèmes industriels connectés.

---

01. Périmètre de l'audit

L'audit de cybersécurité VMS couvre l'ensemble des composants de l'infrastructure de vidéoprotection numérique : le VMS (serveur d'enregistrement et de gestion, incluant l'OS sous-jacent et les applications associées), les NVR et DVR raccordés au réseau, les caméras IP et leurs firmwares, l'infrastructure réseau dédiée à la vidéo (switches, VLAN, VPN d'accès distant), et les postes d'administration et de visualisation.

Sont également inclus dans le périmètre, lorsqu'ils existent : les accès distants au système (VPN, accès web, applications mobiles de visualisation), les interconnexions avec d'autres systèmes de sécurité (contrôle d'accès, hypervision), et les systèmes de backup et d'archivage des enregistrements. Les limites du périmètre audité sont définies contractuellement et documentées en introduction du rapport.

---

02. Points de contrôle et méthodologie

L'audit s'appuie sur une grille de contrôle structurée en 6 domaines. (1) Gestion des accès et authentification : politique de mots de passe (complexité, durée de vie, comptes par défaut non modifiés), authentification multifacteur sur les accès sensibles, revue des comptes utilisateurs (comptes inactifs, privilèges excessifs). (2) Gestion des mises à jour et des firmwares : version des firmwares de chaque caméra et NVR, existence de vulnérabilités connues et non corrigées (consultation des CVE), procédure de gestion des patches. (3) Segmentation réseau : existence d'un VLAN dédié à la vidéo, ségrégation par rapport au réseau utilisateur, règles de pare-feu entre segments.

(4) Chiffrement des communications : chiffrement des flux vidéo (TLS/HTTPS pour l'administration, SRTP pour les flux vidéo si supporté par les équipements), chiffrement des données stockées, certificats valides et non auto-signés. (5) Journalisation et détection : activation des logs d'audit sur le VMS et les équipements, durée de rétention des logs, existence d'une centralisation des logs (SIEM), alertes sur les événements de sécurité critiques. (6) Gestion des accès distants : VPN utilisé, protocoles autorisés, filtrage des IP sources, journalisation des sessions distantes.

---

03. Scoring et résultats par domaine

Chaque domaine fait l'objet d'un score de maturité sur une échelle de 0 à 4 (0 : inexistant, 1 : initial/ad hoc, 2 : défini, 3 : maîtrisé, 4 : optimisé), inspirée du modèle CMMI adapté à la cybersécurité. Ce scoring permet au client de visualiser ses forces et ses faiblesses par domaine et de suivre sa progression entre deux audits.

Le rapport présente pour chaque domaine : le score obtenu, les constats étayant ce score (avec les preuves collectées lors de l'audit), les vulnérabilités identifiées et leur niveau de criticité (selon le score CVSS 3.1 pour les vulnérabilités connues), et les premières recommandations. Un graphique radar synthétique illustre le profil de maturité cybersécurité global du système audité.

---

04. Plan d'action avec responsables et échéances

Le plan d'action liste l'ensemble des actions recommandées, classées par niveau de criticité et par domaine. Pour chaque action : description précise de l'action à mener, vulnérabilité ou risque traité, complexité estimée de mise en œuvre (faible / modérée / élevée), coût estimatif, responsable suggéré (client, Mileo Technology, constructeur de l'équipement), et échéance recommandée.

Les actions critiques (score CVSS supérieur à 7 ou vulnérabilité permettant une prise de contrôle à distance) sont signalées en tête de plan et font l'objet d'une recommandation de traitement immédiat. Mileo Technology propose un accompagnement à la mise en œuvre du plan d'action, avec une révision de l'audit de cybersécurité à 6 mois pour mesurer l'amélioration du score de maturité.

Document Mileo Technology — MOD-CRM-004 — v1.0 — Février 2025
47 Boulevard de Courcelles, 75008 Paris — hello@mileotech.com