Procédure de réponse à incident cyber

Référence	Version	Date	Catégorie
PROC-CYB-005	v1.2	Mai 2025	Cybersécurité

> ***Prioritaire***

Un incident de cybersécurité sur un système de vidéosurveillance peut avoir des conséquences graves : atteinte à la vie privée des personnes filmées, interruption de la protection d'un site, accès à l'infrastructure réseau du client. Cette procédure définit les étapes de réponse à incident permettant de minimiser l'impact, de rétablir le service et de satisfaire aux obligations légales de notification. Elle doit être connue de tous les techniciens et chefs de projet.

---

01. Définition d'un incident de sécurité

Un incident de sécurité sur un système de vidéosurveillance est tout événement compromettant la confidentialité (accès non autorisé aux images), l'intégrité (modification non autorisée des configurations ou des enregistrements) ou la disponibilité (interruption du service d'enregistrement ou de surveillance) du système.

Sont considérés comme incidents : la détection d'un accès non autorisé (comptes inconnus, connexions depuis des pays inhabituels), la présence de malware sur un équipement du système, l'exfiltration de données vidéo, la modification non planifiée de configurations, l'interruption inexpliquée de services critiques, et toute alerte de sécurité non résolue dans les délais.

---

02. Phase 1 — Détection et qualification

La détection peut provenir de multiples sources : alertes de la plateforme de supervision, signalement d'un client, découverte par un

technicien lors d'une intervention, notification d'un constructeur ou d'un CERT. Toute suspicion d'incident est immédiatement remontée au référent cybersécurité, qui procède à la qualification initiale.

La qualification détermine : la nature de l'incident (intrusion, malware, déni de service, erreur humaine), les systèmes et sites concernés, le niveau de gravité (mineur, significatif, critique), et si des données à caractère personnel (images de personnes) sont impliquées, ce qui déclenche les obligations RGPD.

---

03. Phase 2 — Confinement

Le confinement vise à empêcher la propagation de l'incident. Les premières mesures sont : isolation réseau des équipements compromis (déconnexion du VLAN, blocage des règles de pare-feu), révocation des credentials potentiellement compromis, déconnexion des accès distants actifs.

Le confinement ne doit pas détruire les preuves nécessaires à l'investigation. Avant toute action de remédiation, des captures d'état (journaux, dumps mémoire si applicable, liste des connexions actives) sont réalisées et conservées. Ces éléments sont essentiels pour l'analyse post-incident et les éventuelles procédures légales.

---

04. Phase 3 — Éradication et reprise

L'éradication consiste à supprimer la cause de l'incident : nettoyage ou remplacement de l'équipement compromis, correction de la vulnérabilité exploitée, révocation et renouvellement des credentials compromis, vérification de l'ensemble des équipements du même parc pour détecter une compromission latérale.

La reprise du service est planifiée avec le client. Avant la remise en service, une vérification complète de l'intégrité du système est réalisée : configuration conforme, firmware à jour, accès non autorisés supprimés, journaux activés. Un suivi renforcé est maintenu pendant les 30 jours suivant l'incident.

---

05. Obligations de notification

En cas d'incident impliquant des données à caractère personnel (images de personnes identifiables), la notification à la CNIL doit être réalisée dans les 72 heures suivant la prise de connaissance de l'incident, conformément à l'article 33 du RGPD. Mileo Technology assiste le client dans la rédaction de cette notification.

Pour les clients qualifiés opérateurs d'importance vitale (OIV) ou entités essentielles au sens de NIS2, la notification à l'ANSSI est obligatoire selon les modalités et délais définis par la réglementation applicable. Le référent cybersécurité de Mileo Technology coordonne cette notification avec le RSSI du client.

---

06. Bilan et retour d'expérience

Dans les 15 jours suivant la clôture de l'incident, un rapport de retour d'expérience est produit. Ce rapport analyse la chronologie de l'incident, les causes racines identifiées, l'efficacité de la réponse et les points d'amélioration. Il est partagé avec le client et intégré au plan d'amélioration de la sécurité.

> **Les enseignements de l'incident sont intégrés aux procédures internes de Mileo Technology et diffusés aux équipes techniques sous forme de bulletin de sécurité interne. Les indicateurs de l'incident (MTTD, MTTR) alimentent le tableau de bord cybersécurité annuel.**