Politique de sécurité globale intégrée

Référence	Version	Date	Catégorie
POL-PREM-001	v1.0	Février 2025	Documents Premium

La sécurité d'une organisation ne peut plus être appréhendée comme la somme de dispositifs indépendants. La convergence des menaces physiques et cybernétiques, l'interdépendance des systèmes et la complexité des organisations modernes imposent une approche holistique, où les dimensions physique, numérique et procédurale de la sécurité sont pensées et pilotées ensemble. Ce document expose les principes et la méthode de la politique de sécurité globale intégrée.

---

01. Approche holistique de la sécurité

La sécurité physique (contrôle des accès, vidéosurveillance, clôtures, gardes) et la cybersécurité (protection des systèmes d'information, des réseaux et des données) ont longtemps été gérées par des équipes distinctes avec des budgets et des gouvernances séparés. Cette séparation crée des angles morts : un attaquant qui franchit une porte par manipulation sociale (ingénierie sociale) peut ensuite compromettre des systèmes informatiques depuis l'intérieur du périmètre physique sécurisé.

La dimension procédurale — les processus, les règles, les habitudes et les comportements humains — est souvent le maillon le plus faible. La meilleure infrastructure de sécurité est neutralisée par un collaborateur qui laisse sa session ouverte, qui partage ses identifiants ou qui laisse entrer un inconnu sans contrôle. La politique de sécurité globale intégrée traite les trois dimensions avec une pondération équilibrée.

---

02. Interdépendances entre les domaines

Les systèmes de vidéosurveillance et de contrôle d'accès sont eux-mêmes des systèmes informatiques, soumis aux mêmes vulnérabilités que n'importe quel équipement connecté. La compromission d'un NVR peut permettre à un attaquant d'accéder aux images de l'ensemble du site, de masquer une intrusion physique en rejouant des images antérieures, ou de compromettre d'autres équipements du même réseau. La sécurité physique dépend donc directement de la cybersécurité des équipements qui la mettent en œuvre.

À l'inverse, la sécurité des systèmes d'information dépend de la sécurité physique des infrastructures qui les hébergent : un datacenter dont la salle machine est accessible sans contrôle d'accès n'offre aucune garantie réelle, quelle que soit la sophistication de ses pare-feux. La carte d'accès volée à un collaborateur peut donner accès à un local informatique et contourner l'ensemble des protections logiques.

---

03. Gouvernance intégrée

La gouvernance de la sécurité intégrée repose sur un comité unique réunissant le responsable de la sûreté physique, le RSSI et, selon les organisations, le DPO et le risk manager. Ce comité partage une analyse des risques commune, couvrant les menaces physiques, cybernétiques et procédurales, et définit des plans d'action transverses plutôt que des silos d'amélioration.

Le budget de sécurité est alloué globalement en fonction de la contribution de chaque mesure à la réduction des risques identifiés, qu'elle soit physique ou numérique. Cette approche par les risques permet d'éviter les sur-investissements dans un domaine compensant des lacunes dans un autre, et d'optimiser l'efficacité globale du dispositif.

---

04. Tableau de bord de pilotage sécurité

Le tableau de bord de sécurité intégrée agrège des indicateurs des trois dimensions. Sécurité physique : taux de disponibilité des systèmes de contrôle d'accès et de vidéosurveillance, nombre d'incidents physiques par mois, délai moyen de traitement des alertes. Cybersécurité : score de patch management, nombre d'incidents cyber détectés et traités, résultats des tests d'intrusion. Procédurale : taux de

couverture des formations, résultats des exercices de simulation, nombre d'anomalies comportementales détectées.

Ce tableau de bord est présenté mensuellement au comité de sécurité intégré et trimestriellement à la direction générale. Son évolution dans le temps est la principale mesure du progrès de la maturité sécurité de l'organisation.

---

05. Retour sur investissement de la sécurité intégrée

Quantifier le retour sur investissement de la sécurité est complexe car il repose principalement sur l'évaluation de pertes évitées, par nature hypothétiques. La méthode FAIR (Factor Analysis of Information Risk) permet cependant de modéliser les scénarios de risque avec une probabilité et un impact financier estimés, et d'évaluer la réduction de risque apportée par chaque mesure.

> **Au-delà du calcul financier, la sécurité intégrée génère des bénéfices indirects mesurables : réduction des primes d'assurance cyber et sûreté (les assureurs valorisent les certifications et les audits), amélioration de la réputation auprès des clients et partenaires (de plus en plus d'appels d'offres exigent des preuves de maturité sécurité), et facilitation des audits réglementaires (NIS2, ISO 27001, certification HDS pour le secteur santé).**

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