Principes fondamentaux des systèmes de détection en sécurité matérielle

GSMGC-021 (2025)

Préparé par:
La Gendarmerie royale du Canada
Principal organisme responsable de la sécurité matérielle
Sécurité ministérielle
NHQ 73 Leikin Drive Ottawa Ontario, K1A 0R2

Publication publiée : 2025-04-25
Mise à jour : YYYY-MM-DD

Avant-propos

Principes fondamentaux des systèmes de détection en sécurité matérielle est une publication NON CLASSIFIÉE, publiée sous l'autorité de Principal Organisme Responsable de la Sécurité Matérielle (POSM) de la GRC.

Il s'agit d'une publication du gouvernement du Canada qui servira de guide pour examiner les répercussions que le choix des systèmes de détection a sur sécurité matérielle pour les ministères, organismes et employés du gouvernement du Canada.

Les suggestions de modifications et autres informations peuvent être envoyées à l'adresse Principal Organisme Responsable de la Sécurité Matérielle (POSM) de la GRC RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

Reproduction

Date d'entrée en vigueur

La date d'entrée en vigueur du GSMGC-021 (2025) — Principes fondamentaux des systèmes de détection en sécurité physique est 2025-04-25.

Registre des modifications

Amendment No.	Date	Entrée par	Résumé de la modification

Remarque : Le pouvoir de modification ou de dérogation est conféré au principal organisme responsable de la sécurité matérielle de la GRC (PORS de la GRC).

Contenu

1. Introduction

La GRC, en tant que principal organisme responsable de la sécurité matérielle (POSM) pour le gouvernement du Canada (GC), est responsable de fournir des conseils et des directives sur toutes les questions liées à la sécurité matérielle.

1.1. Objectif

Le présent guide a pour objet d'informer les ministères et les organismes sur une variété de systèmes de détection disponibles à utiliser dans un programme ministériel de gestion de la sécurité matérielle. Le présent guide traite de l'application et de l'efficacité de ces systèmes de détection en tant que mesures de protection visant à réduire au minimum les risques pour les personnes, l'information et les biens du GC.

1.2. Applicabilité

Le présent guide s'applique aux spécialistes fonctionnels de la sécurité du GC auxquels on a confié des responsabilités en matière de sécurité matérielle dans les fonctions de protection, de détection, d'intervention et de rétablissement de toute installation ou propriété du GC. Cela comprend également le personnel de gestion des biens et les décideurs ayant un pouvoir de gestion des risques ou d'acceptation des risques au sein du ministère ou de l'organisme.

1.3. Équité, diversité et inclusion dans les systèmes de sécurité matérielle

Tous les employés du gouvernement du Canada (GC) ont la responsabilité de protéger les personnes, les renseignements et les biens du GC. Il est important que les politiques et les pratiques en matière de sécurité ne servent pas d'obstacles à l'inclusion, mais soutiennent et respectent plutôt tout le personnel du GC tout en veillant à ce que les mesures de sécurité appropriées soient maintenues pour protéger le personnel, les biens et l'information du GC.

Les initiatives visant à promouvoir l'égalité et l'inclusion entre les diverses communautés et patrimoines au sein du GC devraient être respectées dans le développement et la maintenance des systèmes de sécurité matérielle. Les ministères et organismes devraient respecter toutes les lois, politiques et directives du GC sur l'équité, la diversité et l'inclusion (EDI) dans la promotion d'un milieu de travail juste et équitable pour toutes les personnes, tout en s'assurant qu'elles s'acquittent de leurs responsabilités en matière de sécurité.

Les ministères et organismes devraient mener un exercice de gestion des risques pour veiller à ce que, même si la dignité de tous est respectée, la protection des renseignements, des biens et du personnel du GC soit maintenue. Toutes les questions sur les politiques et les directives de l'EDI doivent d'abord être adressées à l'autorité ministérielle responsable.

1.4. Considérations aux technologies de l'information

Suite aux menaces qui évoluent constamment et l'intégration de la sécurité matérielle et de la technologie de l'information (TI), il est essentiel d'évaluer le risque de toute application et/ou de tout logiciel connecté à un réseau pour faire fonctionner et soutenir l'équipement dans les bâtiments contrôlés par le gouvernement du Canada.

Avant de mettre en œuvre des applications et/ou des logiciels qui contrôleront et/ou automatiseront certaines fonctions de l'immeuble, votre service de sécurité ministériel exige la réalisation d'une évaluation et d'une autorisation de sécurité (SA&A). Cela permettra de s'assurer que l'intégrité et la disponibilité des composants que les applications et/ou logiciels contrôlent sont maintenues et que tout risque mis en évidence sera atténué. Il est fortement recommandé de commencer le processus SA&A tôt afin de s'assurer que les calendriers de livraison des projets ne sont pas affectés. Pour plus d'informations sur le processus SA&A, veuillez consulter votre service de sécurité ministériel.

2. Coordonnées

Pour plus d'informations, contacter :
Gendarmerie royale du Canada
Principal organisme responsable de la sécurité matérielle
73, promenade Leikin, arrêt postal 165
Ottawa (Ontario)
K1A 0R2
Courriel : RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

3. Acronymes

Acronyme	Signifiant
CCTV	Systèmes de surveillance vidéo. Interchangeable avec CCVE
COS	Centre des opérations de sécurité
DEI	Dispositifs éléctroniques d'intrusion
EDC	Équipement de détection chimique
EMR	Évaluation des menaces et des risques
GC	Gouvernement du Canada
PCCE	Prévention du crime par la conception environnementale
PDIR	Protection, détction, intervention et récupération
POS	Procédures opérationnelles standard
CPV	Chlorure de polyvinyle
ZA	Zone d'accueil
ZHS	Zone de haute sécurité
ZS	Zone de sécurité
ZT	Zone de travail

4. Glossaire

Terme	Définition
Actif	Biens corporels ou incorporels du gouvernement du Canada. Les actifs comprennent, sans s'y limiter, l'information sous toutes ses formes et dans tous les médias, les réseaux, les systèmes, les matériels, les biens immobiliers, les ressources financières, la confiance des employés, la confiance du public et la réputation internationale.
Agents de guerre chimique	Produits chimiques de synthèse extrêmement toxiques qui peuvent être dispersés sous forme de gaz, de liquide ou d'aérosol ou adsorbés sur des particules pour devenir une poudre, et qui ont des effets mortels ou incapacitants sur les humains.
Compartimentation	Un regroupement non hiérarchique d'actifs utilisé pour contrôler l'accès plus finement qu'avec la seule classification de sécurité hiérarchique.
Compromis	Divulgation, destruction, suppression, modification, interruption ou utilisation non autorisée de renseignements ou de biens.
Agents de coupe	Les adultérants ajoutés aux drogues illicites afin de modifier leurs propriétés physiologiques, et/ou les substances inertes qui sont ajoutées uniquement pour augmenter le volume du produit.
Défense en profondeur	Il s'agit du principe selon lequel les zones de sécurité sont mises en œuvre d'une manière progressivement restrictive, allant de la zone la moins restrictive à la plus restrictive.
Installation	Quelque chose qui est construit, installé ou établi pour servir un but particulier. Une installation peut comprendre un bâtiment spécifique (en tout ou en partie) ou le site ou le terrain sur lequel elle est située. Le terme englobe à la fois l'objet physique et son utilisation (c.-à-d. champs d'armes, champs agricoles).
Menace interne	Cas où des membres du personnel, autorisés à entrer ou à travailler dans une installation du GC, prennent délibérément des mesures contre le GC, leur employeur ou leurs collègues. Les actions peuvent comprendre des activités criminelles, des menaces ou des actions physiques, de l'espionnage, de la subversion et du sabotage.
Atténuation	Activités entreprises pour réduire les risques.
Narcotique	Drogue ou autre substance qui affectent l'humeur ou le comportement et sont consommées à des fins non médicales, en particulier une vente illégale.
Besoin d'accès	Le principe selon lequel la personne a besoin d'accéder à la zone ou à la zone pour s'acquitter de ses fonctions. Ceci ne doit pas être confondu avec le besoin de connaître le contenu des informations contenues ou traitées dans cette zone.

Besoin d'en connaître	Le principe selon lequel une personne a besoin d'accéder à l'information et de la connaître pour s'acquitter de ses fonctions.
Précurseurs chimiques	Les précurseurs chimiques sont des produits chimiques essentiels à la production d'une substance réglementée. Les précurseurs chimiques ont une large utilisation légitime dans la production de biens de consommation tels que les produits pharmaceutiques, les parfums, les agents aromatisants, les produits pétroliers, les engrais et les peintures. Par exemple, l'éphédrine et la pseudoéphédrine, couramment utilisées dans les médicaments contre le rhume et les décongestionnants, sont des précurseurs chimiques utilisés pour produire de la méthamphétamine.
Sauvegarde	Actifs ou contrôles externes qui réduisent le risque global pour les employés, d'autres actifs ou la prestation de services en diminuant la probabilité d'un événement menaçant, en réduisant la probabilité de compromission, ou atténuer la gravité du résultat par une interaction directe ou indirecte avec les valeurs de l'actif, les menaces ou les vulnérabilités.
Vulnérabilité	Une insuffisance liée à la sécurité qui pourrait accroître la vulnérabilité aux atteintes ou aux blessures.

5. Systèmes de détection

Les systèmes de détection sont des systèmes mécaniques, électriques ou procéduraux conçus pour alerter la sécurité en cas de conditions particulières qui peuvent indiquer la présence d'un élément ou d'une situation nécessitant une intervention. Un système de détection peut être aussi simple qu'un fil à trépied attaché à une cloche à une extrémité du spectre, avec des systèmes complexes de caméras infrarouges multicouches à l'autre extrémité. Indépendamment de la complexité du système, ils sont tous conçus pour atteindre le même but; la détection des personnes, des objets, des produits chimiques ou d'autres intrus. Divers systèmes de détection courants sont explorés tout au long du présent guide, ainsi que les pratiques exemplaires liées à leur sélection et à leur fonctionnement, et la façon dont ils peuvent s'intégrer dans un portefeuille de sécurité plus vaste.

6. Systèmes d'alarme

Un système d'alarme est constitué de multiples mesures de protection, toutes liées à la création d'un effort d'atténuation qui représente plus que la somme de ses parties. Lors de la conception d'un système d'alarme, chaque composant de Protection, Détection, Réponse, et Récupération devrait être envisagé et, si possible, une partie du système d'alarme devrait traiter de chaque élément. Un système d'alarme complet devrait être en mesure de répondre à toute alarme déclenchée par le déploiement du personnel de sécurité ou des forces de l'ordre. Il est également recommandé de brancher la vidéosurveillance au système d'alarme afin que le personnel de sécurité puisse voir ce qui se passe dans une zone lorsqu'une alarme est

déclenchée ou obtenir des images à utiliser comme preuve. Les systèmes de vidéosurveillance peuvent être programmés pour commencer à enregistrer une zone chaque fois qu'une dispositive de détection est déclenché, ainsi que pour signaler aux opérateurs qu'une zone spécifique nécessite l'observation afin de déterminer si un capteur a détecté une menace réelle ou perçue. Les systèmes d'alarme doivent être raccordés à l'alimentation de secours, le cas échéant, et les connexions sans fil doivent être évitées pour minimiser le risque d'interception, de perturbation ou d'accès à distance non autorisé.

Il y a deux façons de surveiller un système d'alarme, sur site ou hors site. La surveillance sur place est souvent la méthode préférée lorsque c'est pratique, car une réponse peut être générée immédiatement par l'équipe de sécurité sur place. La surveillance sur site minimise également le risque de perte de communication entre le système d'alarme et les opérateurs, car ils peuvent être câblés dans un système fermé. La surveillance hors site présente également des avantages, car elle permet souvent d'économiser des coûts par rapport à une sécurité dédiée sur le site. La surveillance hors site peut être suffisante pour les actifs de moindre valeur, mais est généralement déconseillée pour la protection des actifs très sensibles ou de grande valeur. Les services de surveillance hors site sont souvent fournis par des tiers et il est incroyablement difficile d'obtenir des données précises sur l'efficacité de leurs temps de réponse, car les services de surveillance emploient souvent des sous-traitants pour vérifier le site après qu'une alarme a été déclenchée. Ces multiples couches de sous-traitants externes peuvent compliquer le processus de sélection des intervenants potentiels et ouvrir plusieurs vulnérabilités qui sont incroyablement difficiles à atténuer. Pour cette raison, la surveillance hors site ou par un tiers ne devrait être envisagée que lorsque d'autres options s'avèrent irréalisables.

6.1. Dispositifs électroniques d'intrusion

Les dispositifs électroniques d'intrusion (DEI) sont des systèmes de détection automatique qui font souvent partie du profil de sécurité d'une installation. Les systèmes d'identification électronique fonctionnent en surveillant diverses conditions dans leur zone de travail et en avertissant lorsque les conditions changent de manière à indiquer la présence d'une personne. Les systèmes de DEI ne génèrent généralement pas de réponse par eux-mêmes, ce qui nécessite des systèmes supplémentaires pour enquêter sur la cause de l'alarme. Cela se fait souvent en utilisant la vidéosurveillance et les patrouilles de sécurité pour suivre le déclenchement des systèmes de DEI. Les DEI est un moyen efficace de surveiller les grandes installations où il n'est peut-être pas pratique que le personnel de sécurité surveille constamment l'ensemble du site ; au lieu de cela, on déploie des ressources uniquement dans les zones où des activités non vérifiées nécessitent une enquête. Un autre avantage des DEI est la détection d'accès non planifiés à un site et la notification du personnel de sécurité ou des forces de l'ordre, comme la détection de mouvements dans un bureau lorsque celui-ci est censé être inoccupé. Dans tous les cas, les systèmes de DEI ne fournissent qu'un élément de détection et nécessiteront des mesures de sécurité supplémentaires pour fournir les éléments de réponse et de récupération afin de s'assurer que les menaces sont adéquatement atténuées.

6.1.1. Détecteurs de vibrations

Les détecteurs de vibrations sont le plus souvent installés sur des clôtures, cependant il existe des versions spécialisées qui peuvent également détecter les vibrations du sol, des voûtes, des fenêtres et des coffres-forts. Les détecteurs de vibrations déclenchent une alarme lorsqu'un niveau de vibration défini est détecté. Ces niveaux sont souvent définis sur des paramètres spécifiques pour limiter le nombre d'alarme fausse. Un détecteur de vibrations sur une clôture sera souvent calibré pour déclencher une alarme lorsqu'un humain tente d'escalader la clôture, mais pas lorsque des animaux plus petits ou des conditions météorologiques peuvent causer des niveaux plus faibles de vibration.

6.1.2. Détecteurs de mouvement

Un détecteur de mouvement est un dispositif qui peut détecter le mouvement dans une zone fixe qui a la ligne de vue du détecteur. Les détecteurs de mouvement peuvent souvent être calibré pour déclencher une alarme en fonction du nombre de mouvements détectés. Cela peut limiter les alarmes fausses en déclenchant uniquement des alarmes pour des mouvements qui sont approximativement de la taille d'un humain. Les modèles moins chers ne possèdent peut-être pas une fonction comme celle-ci, ce qui les rend plus susceptibles de fausses alarmes causées par des mouvements non nuisibles (tels que des affiches se déplaçant près d'un évent et/ou des rongeurs).

6.1.3. Capteurs tomographiques

Les capteurs tomographiques sont un type de capteur de mouvement qui utilise des perturbations dans les ondes radio pour identifier le mouvement. Contrairement aux capteurs de mouvement traditionnels qui nécessitent une ligne de visée, les capteurs tomographiques peuvent être placés hors de vue et sont capables de fonctionner à travers des murs et des meubles. Cela se fait en configurant plusieurs capteurs autour de la zone surveillée. Les capteurs tomographiques surveillent les ondes radio entre eux et se déclenchent lorsque ces ondes radio sont perturbées, ce qui indique que quelque chose s'est déplacé dans la zone. Les capteurs tomographiques sont suffisamment sensibles pour détecter un animal de la taille d'un petit chien, mais ne seront pas déclenchés par des mouvements plus petits que cela. Cela minimise les alarmes fausses causées par des rongeurs petits, des insectes ou des courants d'air provenant d'un évent ou d'une fenêtre affectant les rideaux ou autres tissus.

6.1.4. Capteurs de bris de verre

Les détecteurs de bris de verre sont conçus pour détecter le bruit du bris de verre. Comme ils détectent l'audio, un seul capteur de bris de verre peut couvrir une pièce avec plusieurs fenêtres. Un environnement bruyant diminue généralement les capacités de détection du dispositif. Les détecteurs de bris de verre peuvent ajouter une couche supplémentaire de détection et fonctionnent bien dans le cadre d'un système de sécurité plus vaste, mais leurs capacités sont limitées lorsqu'ils sont utilisés indépendamment.

6.1.5. Alarmes du capteur de contact

Les alarmes des capteurs de contact consistent en deux capteurs qui peuvent déterminer quand ils sont en contact ou à plusieurs millimètres l'un de l'autre et alerter un système lorsque le contact est rompu. Ils sont le plus souvent utilisés sur les portes et les fenêtres, avec un capteur installé sur le cadre, et le second installés sur la porte ou la fenêtre. Ils doivent être installés de manière à entrer en contact les uns avec les autres lorsque l'état souhaité de l'équipement est atteint, généralement lorsque la porte ou la fenêtre est fermée. Une alerte est envoyée au système de surveillance chaque fois que le contact entre les deux capteurs est rompu, par exemple lorsqu'une porte ou une fenêtre s'ouvre pendant les heures de silence et qu'aucune activité n'est prévue. Les capteurs de contact peuvent également fournir des informations à une équipe de sécurité, leur permettant de savoir quand les portes sont ouvertes sur le site sans déclencher d'alarme sonore.

Il est possible d'intégrer des alarmes par contact à de plus grands systèmes de sécurité comme couche supplémentaire de détection. Un système de contrôle d'accès pourrait être relié à des alarmes de contact et programmé pour limiter les alarmes fausses. Cela peut être fait en programmant l'alarme pour qu'elle se déclenche seulement si une carte d'accès valide n'est pas scannée avant que la porte ne s'ouvre, ou en désignant des heures où l'alarme est toujours active, comme lorsque le bureau est fermé et qu'aucune activité autorisée n'est prévue.

6.1.6. Capteurs photoélectriques

Les capteurs photoélectriques sont des émetteurs et des récepteurs qui créent un faisceau de lumière entre eux et déclenchent une alarme si le faisceau est perturbé. Cela crée un fil-piège virtuel, capable d'alerter un élément de réponse sans que la personne soit au courant qu'elle a été détectée. Ils peuvent également être configurés pour surveiller un actif physique spécifique en plaçant l'actif directement entre l'émetteur et le récepteur, déclenchant une alarme lorsque l'actif est retiré et que le faisceau relie l'émetteur et le récepteur. Les capteurs photoélectriques peuvent être installés rapidement pour un coût relativement faible et sont particulièrement efficaces pour fournir une détection compartimentée dans une zone où les détecteurs de mouvement peuvent être inefficaces en raison d'un volume élevé de mouvement autorisé. Les musées sont un bon exemple où un capteur photoélectrique serait plus efficace qu'un système de détection de mouvement ; ils peuvent alerter le personnel de sécurité lorsqu'une personne s'approche trop près d'une exposition, mais ne provoqueraient pas d'alarmes fausses en raison du déplacement des autres dans la pièce.

7. Surveillance visuelle

La surveillance visuelle est la forme de détection la plus élémentaire et présente ses propres avantages et vulnérabilités par rapport aux systèmes plus complexes. La surveillance visuelle peut être aussi simple qu'une observation par le personnel de sécurité ou encore être assistée par des systèmes de surveillance électronique, tels que les caméras de vidéosurveillance reliées à

un poste de surveillance. Un avantage pour la surveillance visuelle est la capacité de trier immédiatement les incidents que l'équipement peut ne pas avoir la capacité d'analyser correctement. Les systèmes de détection déclenchent des alarmes en fonction de changements spécifiés dans l'environnement, ils ne peuvent pas déterminer ce qui se passe au-delà et nécessite une enquête pour déterminer ce qui a déclenché l'alarme et si elle est néfaste ou bénigne. La surveillance visuelle permet au personnel de sécurité de prendre des décisions immédiates ; le fait de voir une personne essayer d'escalader une clôture fournit des renseignements plus immédiats qu'un détecteur de vibrations déclenché. Une lacune notable de la surveillance visuelle est l'élément humain ; un gardien ou opérateur CCTV n'est efficace que dans la mesure où son attention et sa formation le permettent. Les équipes de sécurité mal formées ou mal dotées en personnel ne sont peut-être pas en mesure de surveiller efficacement une zone avec seulement la détection visuelle ; elles sont plus efficaces lorsqu'elles sont combinées avec de DEI pour orienter leur attention vers des zones où l'activité n'est pas vérifiée.

7.1. Surveillance assistée par vidéosurveillance

Les systèmes de vidéosurveillance sont des réseaux d'équipements connectés conçus pour capturer, transmettre, afficher et stocker des données d'imagerie. La complexité des systèmes de vidéosurveillance va d'une seule caméra connectée à un moniteur d'affichage, jusqu'aux systèmes en réseau capables de surveiller et de contrôler des centaines de caméras connectées localement, à distance et globalement.

Ces systèmes peuvent être accompagnés d'un logiciel qui peut identifier et alerter les changements à ce que le système observe, fournissant une fonction similaire à la détection de mouvement. Ces programmes fonctionnent en déclenchant une alerte lorsqu'un changement visuel spécifié est observé par le logiciel de surveillance, généralement causé par des mouvements dans la zone observée. Le logiciel détecte les changements visuels et non le vrai mouvement, de sorte que ces programmes sont sujets aux alarmes fausses provoquées par des changements dans les conditions d'éclairage ou d'autres changements non liés au mouvement aux visuels. Cela peut être partiellement atténué en calibrant la quantité de changement nécessaire pour déclencher une alerte et en identifiant des secteurs spécifiques de la zone surveillée pour détecter les changements visuels, tels que les points d'entrée et les itinéraires. Ce logiciel est le plus couramment utilisé pour amorcer l'enregistrement lorsqu'il y a une activité perçue, économiser de l'espace de stockage et prolonger la durée pendant laquelle les enregistrements sont conservés avant que l'écrasement ne se produise. Toute perturbation notable dans une ou toutes les caméras d'un système doit faire l'objet d'une enquête immédiate et approfondie.

Vous trouverez plus d'informations sur les systèmes de vidéosurveillance et leurs applications dans GSMGC-011 Guide des systèmes de surveillance vidéo.

7.2. Surveillance axée sur le personnel

On peut compter sur le personnel ayant une capacité limitée pour détecter les incidents dans un modèle dédié ou passif. Un modèle dédié est le plus couramment utilisé, et

comprend le personnel de sécurité qui effectue des patrouilles, les opérateurs de vidéosurveillance, les sentinelles/gardiens de contrôle d'accès et les employés de réception dûment formés. L'une des principales responsabilités de ce personnel est d'être à l'affût des personnes qui tentent d'entrer dans l'installation, et il devrait être formé sur la façon de réagir ou d'alerter le personnel de sécurité en cas d'observation d'une personne non autorisée ou suspecte. En plus de surveiller les mouvements des personnes, le personnel peut être utilisé pour identifier les objets transportés ou plantés et communiquer cette information au personnel de sécurité au besoin. À titre d'exemple, un individu portant un parapluie par rapport à un individu portant une batte de baseball nécessiterait des approches très différentes de la part du personnel de sécurité. Il s'agit d'une distinction que l'équipement de détection seul ne peut pas être en mesure de faire de manière fiable.

Les modèles passifs de surveillance axée sur le personnel sont le sous-produit d'une main-d'œuvre consciente des risques et formée à la sécurité. Cela comprend le personnel dont les tâches principales ne concernent pas des secteurs de surveillance, mais qui a reçu la formation nécessaire pour identifier et signaler des incidents suspects ou inhabituels au personnel de sécurité aux fins d'enquête. Les modèles passifs de surveillance ne devraient pas être considérés comme des mesures de sauvegarde dédiées, mais plutôt comme une couche supplémentaire de protection pour améliorer les systèmes de détection dédiés en place. La détection passive seule est souvent peu fiable, car elle est proportionnelle à la sensibilisation et à la formation du personnel en matière de sécurité, à sa volonté de signaler une activité suspecte et à la probabilité de remarquer des personnes non autorisées dans les zones d'accès restreint. Ce type de détection est le plus efficace dans les petites installations, où le personnel se connaît et se reconnaît et remarquera tout ce qui n'est pas familier dans leur installation.

7.3. Formation et mise en œuvre

Lorsque la surveillance visuelle est un élément planifié du système de détection d'une installation, il faut mettre l'accent sur la formation et le maintien de ces compétences, en particulier par les employés qui effectuent des patrouilles et surveillent l'équipement de surveillance. La surveillance visuelle est directement proportionnelle à l'aptitude et à l'attention de l'équipe de sécurité. Même le système de surveillance le plus complet est totalement inefficace si la personne qui le surveille ne fait pas attention à lui ou n'est pas formée sur la façon de gérer les incidents observés. Lorsqu'il s'agit de déterminer la capacité de la surveillance visuelle à détecter des menaces, seuls les employés affectés à cette tâche doivent être pris en compte dans les calculs d'atténuation des risques. La surveillance passive par du personnel formé et sensibilisé à la sécurité n'est pas aussi fiable ou mesurable que du personnel formé et employé spécifiquement pour la détection d'individus autorisés ou en infraction. Il existe plusieurs catégories de surveillance visuelle à prendre en compte, présentées dans le tableau 1: Recommandations en matière de surveillance visuelle et de formation.

Tableau 1 : Recommandations de formation sur la surveillance visuelle

Catégorie de personnel	Recommandations
Opérateurs CCTV/COS	• Les opérateurs sont formés sur l'équipement du site ; • Les opérateurs savent qui appeler pour l'entretien de l'équipement • Les POS ont été élaborées pour déterminer qui contacter (la sécurité sur place ou l'application de la loi locale) en cas d'incident ; et • Les opérateurs reçoivent une formation sur la façon de préparer et d'autoriser la diffusion des images pour les enquêtes.
Gardes de patrouille	• Les POS sont disponibles pour s'assurer que les gardes ont des renseignements sur les mesures à prendre lors de différents événements/incidents ; • Les gardiens sont formés et familiarisés avec les privilèges associés à certains badges d'accès ; • Les gardes sont formés et certifiés dans l'usage de la force lorsqu'ils interviennent ; • Les gardiens comprennent le ou les secteurs sur lesquels ils ont autorité ; • Les gardiens sont formés pour savoir à qui qu'ils doivent s'adresser en cas de besoin (services d'urgence, gardes de secours ou superviseur du site) ; et • Les gardes sont formés à la déclaration et à l'escalade des incidents.
Sentinelles/gardes de contrôle d'accès	• Les POS sont disponibles pour s'assurer que les gardes ont des renseignements sur les mesures à prendre lors de différents événements/incidents ; • Les gardes sont formés aux exigences de contrôle d'accès ; • Les gardes sont formés pour assurer un suivi efficace des personnes sur le site ; • Les gardes sont formés et certifiés pour utiliser le niveau de force approprié afin d'empêcher toute tentative d'entrée non autorisée ; et • Les gardes sont formés pour savoir à qui contacter en cas de besoin d'assistance (services d'urgence, gardes de secours et/ou superviseur du site).
Personnel de la réception	• Le personnel reçoit une formation sur la sensibilisation à la sécurité afin de les habiliter à repérer et à traiter les comportements suspects ; • Le personnel reçoit une formation sur les personnes à contacter pour obtenir de l'aide ou pour faire remonter un événement suspect (sécurité du site ou services d'urgence locaux) ; • Le personnel reçoit une formation sur la façon de gérer un incident en toute sécurité dans l'attente d'une réponse de la part des services de sécurité ou des forces de l'ordre ; et, • Le personnel reçoit une formation sur la façon de se désengager

	d'un incident en toute sécurité et de trouver un endroit sûr ou sécurisé pour attendre l'aide au besoin.
Personnel averti de la sécurité	• Le personnel reçoit une formation sur la sensibilisation à la sécurité afin de les habiliter à repérer et à traiter les comportements suspects ; • Le personnel est formé sur le moment et la façon de défier une personne qui ne montre pas l'insigne approprié pour une zone ; • Le personnel reçoit une formation sur la façon de signaler les incidents suspects à la sécurité du site pour enquête ou intervention ; et • Le personnel reçoit une formation en matière de sécurité sur les moments où il doit se désengager ou quitter une situation pour permettre au personnel de la sécurité d'y faire face.

8. Détection de la contrebande

Un élément clé de la sécurité consiste à assurer un contrôle positif sur ce qui peut ou ne peut pas être amené dans/hors d'une installation, ou transporté par une personne. La détection d'articles prohibés au point d'entrée peut contribuer à assurer la sécurité du personnel et des visiteurs, ainsi qu'à limiter la capacité des acteurs de menaces hostiles à introduire des articles qui peuvent être utilisés pour contourner les couches de défense subséquentes. Certains articles communément interdits comprennent ; armes, outils, équipement vidéo et audio, substances intoxicantes et liquides et poudres non identifiés. Bien qu'ils ne soient pas nécessairement illégaux, les articles courants peuvent présenter des risques s'ils sont admis dans une installation sécurisée. Il n'est pas illégal de transporter des outils dans un sac à dos, mais le fait de permettre aux visiteurs de les amener dans une installation augmente considérablement le risque qu'ils soient utilisés pour désactiver ou contourner les efforts d'atténuation ou blesser le personnel. Les articles interdits devraient être clairement indiqués par des panneaux et renforcés par le personnel de sécurité au point d'entrée. Une EMR devrait être effectuée pour déterminer quels articles (le cas échéant) devraient être interdits d'entrée dans une installation.

8.1. Détection des métaux

Les détecteurs de métaux sont couramment utilisés pour détecter et atténuer le risque que des articles interdits soient introduits dans une zone contrôlée. Ils sont souvent utilisés dans des zones ouvertes au public, mais risquent d'être ciblés par des acteurs de la menace. Ils sont couramment utilisés dans les événements sportifs, les sites culturels et historiques, les carrefours de transport, les campus scolaires et les bâtiments gouvernementaux. Les détecteurs de métaux sont un élément d'un poste de contrôle habité, et auront un ou plusieurs gardes de sécurité qui contrôleront l'équipement. Les détecteurs de métaux sont disponibles en deux types communs, souvent déployés ensemble pour une plus grande efficacité. Il s'agit du « détecteur de métaux à pied » et de la « baguette manuelle ». Aux postes de contrôle équipés de détecteurs de métaux, les gens passent en premier et toute personne qui émet une alerte au détecteur est fouillée à l'aide d'une baguette manuelle pour repérer l'objet métallique et déterminer s'il est permis ou interdit.

8.1.1. Présentation

Un détecteur de passage a une personne qui passe à travers un détecteur de la taille d'une porte, ce qui déclenchera une alarme si suffisamment de métal est détecté. Ils sont généralement calibrés pour détecter des objets aussi petits qu'un couteau pliant. Certains modèles plus avancés peuvent identifier la zone dans la zone de détection qui a déclenché l'alarme et alerter l'opérateur à peu près où le métal a été détecté sur la personne. Par exemple, si la partie inférieure du détecteur s'active, cela peut indiquer que des éléments sont cachés dans une botte ou un bas.

8.1.2. Appareil portatif

Les baguettes de sécurité sont des appareils portatifs qui peuvent repérer une zone avec du métal avec plus de précision qu'un capteur à pied. Ils peuvent être utilisés de façon indépendante ou comme vérification secondaire une fois que la personne déclenche un détecteur. Lorsqu'il est utilisé, un agent de sécurité aurait une personne qui se tenait immobile avec les bras écartés et les jambes séparées. Le garde de sécurité déplacerait ensuite la baguette sur les deux côtés de chaque membre, ainsi que sur l'avant, le dos et les côtés du corps. La baguette se déclenche lorsque le métal est détecté directement sous elle. C'est beaucoup plus précis qu'un détecteur de passage, mais il prend du temps.

8.2. Rayons X

Comme les détecteurs de métaux, la fonction principale des appareils à rayons X est de détecter les objets non autorisés avant qu'ils ne soient introduits dans un environnement contrôlé. Ces machines scannent généralement les sacs et l'équipement, mais certains modèles sont conçus pour le dépistage des personnes. Les appareils à rayons X nécessitent un personnel de sécurité formé pour les utiliser. Le personnel de sécurité effectuera également des fouilles secondaires au besoin et saisira les objets qu'il a le pouvoir de confisquer. Les appareils à rayons X révèlent le contenu d'un conteneur ou des objets cachés sur une personne et certains appareils sont capables d'identifier les menaces de façon autonome. Un opérateur bien formé sera en mesure d'identifier avec précision les objets métalliques, les fils et les composants électroniques, les liquides et les plastiques, et de déterminer si la personne ou le contenant nécessite une inspection physique secondaire. Un appareil à rayons X est capable d'atténuer le risque de menaces non métalliques en permettant aux opérateurs de voir la forme et le matériau des objets dissimulés, et peut être efficace pour détecter les dispositifs hostiles qui peuvent ne pas contenir suffisamment de métal pour être identifiés par un détecteur de métaux (comme les armes à feu imprimées en plastique, les lames en céramique, les bombes à pipe en plastique/CPV ou les produits chimiques nocifs dans des contenants non métalliques).

Des appareils à rayons X seront souvent déployés aux côtés de détecteurs de métaux lorsqu'on s'attend raisonnablement à ce que les invités ou les employés transportent des sacs, comme dans les carrefours de transport, les palais de justice et les lieux historiques

ouverts au public. Un appareil à rayons X est moins invasif et prend moins de temps qu'une fouille physique de chaque sac, et il peut identifier les articles cousus dans la doublure des sacs qui peuvent échapper à la détection par une recherche manuelle. Les appareils à rayons X sont une mesure d'atténuation courante et pratique pour les salles de courrier et les quais de livraison, surtout si le public est en mesure d'envoyer des colis ou du courrier directement. Les dispositifs hostiles livrés par la poste sont devenus plus courants au cours des dernières décennies, et tous les ministères et organismes gouvernementaux devraient envisager des mesures d'atténuation pour détecter le courrier potentiellement hostile avant qu'il ne soit introduit dans une installation.

8.3. Planification et fonctionnement des points de contrôle

L'utilisation des points de contrôle, permanents ou temporaires, devrait être envisagée lorsqu'il y a un problème, des personnes présentant une menace ou des articles prohibés entreront dans une installation. Bien qu'elles puissent être impopulaires, elles sont souvent nécessaires pour admettre des personnes sans habilitation de sécurité, lors de rassemblements de masse ou lorsqu'un site a un symbolisme culturel ou politique. Tous ces facteurs contribuent au risque d'être ciblé par les acteurs de la menace. Une EMR devrait être effectuée pour déterminer les articles qui devraient être interdits et les mesures que l'équipe de sécurité devrait prendre s'ils sont identifiés. Certains éléments à envisager d'interdire sont :

- Dispositifs pour victimes massives ;
- Armes ;
- Substances intoxicantes ;
- Propagande ;
- Accessoires de vandalisme ;
- Outils ; et,
- Équipement de surveillance.

Des POS devraient être en place qui décrit clairement comment le personnel de sécurité doit réagir lorsqu'il trouve des articles prohibés ; refus d'entrée, confiscations et même arrestations. Tous les gardiens qui travaillent au point de contrôle doivent être formés à ces procédures et avoir des directives claires sur la façon d'escalader et de signaler tout incident.

9. Équipement de détection des produits chimiques

L'équipement de détection des produits chimiques (EDC) a la capacité d'identifier les éléments et les composés chimiques (même en quantités infimes) et d'alerter un opérateur de leur présence. Ces dispositifs peuvent être étalonnés pour détecter un grand nombre d'éléments chimiques et de composés qui aident les opérateurs à identifier ; narcotiques, explosifs, agents de coupe, précurseurs chimiques et agents de guerre chimique. L'EDC est disponible dans un certain nombre de configurations, beaucoup viennent préchargés avec une bibliothèque des substances connues et la capacité de télécharger plus au besoin. L'EDC peut prélever des échantillons dans l'air ou directement en prélevant un échantillon sur une zone d'intérêt et en

insérant l'échantillon dans le dispositif d'essai.

L'EDC peut être déployé pour surveiller en permanence les produits chimiques nocifs dans des zones pouvant faire l'objet d'une introduction accidentelle ou intentionnelle, comme les sites industriels ou les centres de transport. Les premiers intervenants utilisent des dispositifs mobiles de détection chimique pour identifier rapidement les substances nocives, ce qui peut aider à atténuer les incidents impliquant des menaces chimiques réelles ou perçues.

L'EDC peut être utilisé aux points d'entrée pour dépister les produits chimiques, ce qui peut entraîner une fouille secondaire, un refus d'entrée, etc. Le contrôle implique souvent que le personnel de sécurité prélève des échantillons dans les zones d'intérêt (comme les mains, les chaussures, les sacs ou les appareils électroniques), ou faire passer une personne à travers un portail, semblable à un détecteur de métaux, pour détecter la présence d'éléments traces de produits chimiques. Il devrait y avoir une POS en place pour décrire la réponse à la détection de divers produits chimiques afin d'atténuer adéquatement la menace.

Une EMR devrait être entreprise pour tenir compte des environnements de menace particuliers ou du risque accru d'utilisation de produits chimiques pouvant justifier le déploiement d'EDC, surtout dans les cas où des menaces réelles sont indiquées pour déterminer quel système de détection chimique est le mieux adapté pour atténuer et minimiser les risques impliqués.

10. Considérations de sécurité

Les mesures de sauvegarde peuvent avoir une relation simple de cause à effet avec le risque lorsqu'elles sont analysées indépendamment ; en pratique, il existe de nombreuses variables qui peuvent affecter ces calculs et qui doivent être prises en compte. Les considérations relatives à la sécurité matérielle, qui ont une incidence directe sur les mesures de contrôle et l'efficacité des mesures de contrôle, comprennent ce qui suit :

10.1. Défense en profondeur

La défense en profondeur, également connue sous le nom d'anneaux de protection, est un concept selon lequel un actif devrait avoir plusieurs couches de mesures de sécurité qui deviennent de plus en plus denses à mesure que vous vous rapprochez d'un actif. Une clôture de périmètre est la première couche de défense la plus courante ; elle est efficace pour déterminer où se termine l'accès public, mais elle ne fait pas grand-chose pour empêcher un acteur de menace délibéré de la violer ou de l'étendre. Les efforts de détection courants dans le deuxième niveau comprennent des systèmes de vidéosurveillance, des patrouilles de sécurité, des capteurs de mouvement et des mesures de protection du contrôle d'accès ; ces mesures sont susceptibles d'être efficaces contre la plupart des acteurs de menace peu sophistiqués. Les couches internes seront les plus rigoureuses et les plus difficiles à violer et comprendront probablement de multiples mesures de sécurité matérielle qui travaillent ensemble pour protéger l'actif contre la compromission. En plus d'être très difficiles à pénétrer même pour les acteurs de la menace sophistiqués, ces dernières couches

de défense devraient également être conçues pour atténuer le risque posé par les menaces internes qui peuvent utiliser des identifiants valides pour contourner les premières couches défensives. Ces dernières couches auront probablement un contrôle strict des actifs qui limite l'accès à du personnel spécifique ayant besoin de savoir ou besoin d'accéder.

10.2. Zones

Les zones de sécurité physique, lorsqu'elles sont adéquatement intégrées, devraient améliorer l'environnement général de sécurité d'une installation. Le zonage de sécurité physique devrait promouvoir un sentiment de propriété ou de renforcement territorial, offrir des possibilités de surveillance naturelle et établir une séquence clairement définie de limites à travers lesquelles un visiteur ou un employé dûment contrôlé peut passer.

Avant qu'une personne ne passe d'une zone de sécurité physique à une autre, elle devrait percevoir la limite du zonage (implicite ou réelle) et comprendre les règles ou les limites associées au franchissement de cette limite. Les exigences en matière d'espace fonctionnel du Ministère devraient également être prises en compte lors de l'établissement des limites de zonage.

Pour plus d'informations sur les zones de sécurité physique, voir GSMGC-015 Guide pour l'établissement des zones de sécurité matérielle.

10.3. Protection, détection, intervention et récupération

PDIR sont les quatre composantes essentielles qui composent une posture de sécurité dynamique et efficace. Chaque mesure de sauvegarde ou d'atténuation est conçue pour traiter un ou plusieurs de ces éléments. Consulter GSMGC-019 — Guide de Protection, Détection, Réponse, et Récupération pour un examen approfondi de ces concepts.

10.3.1. Protection

La protection est assurée au moyen de barrières physiques, procédurales et psychologiques pour retarder ou dissuader l'accès non autorisé. Des mesures de protection bien choisies et utilisées empêcheront la survenue d'événements ou d'activités indésirables.

10.3.2. Détection

La détection implique l'utilisation de dispositifs, systèmes et procédures appropriés pour signaler qu'une tentative ou un accès non autorisé a eu lieu. Les mesures de protection qui appuient la détection devraient permettre d'avertir le plus tôt possible d'un événement, afin de réduire le temps nécessaire pour amorcer une intervention.

10.3.3. Intervention

L'intervention implique la mise en œuvre de mesures pour s'assurer que les incidents de sécurité sont traités le plus rapidement et efficacement possible, est signalée aux responsables de la sécurité appropriés, ce qui garantit que des mesures correctives

immédiates et à long terme sont prises en temps opportun. Les priorités d'intervention, dans l'ordre, sont :

1. Préservation de la vie et sécurité du personnel ;
2. Protection de l'information et des biens du GC ; et
3. Protection de la propriété pour permettre une récupération rapide des opérations normales.

Les plans d'intervention et les POS des ministères et organismes devraient être fondés sur une EMR qui comprend les menaces connues et prévues pour l'emplacement et le personnel, les capacités du personnel de sécurité sur place et le soutien disponible des premiers intervenants (police, pompiers, ambulance). Ces exercices devraient être pratiqués (exercés) régulièrement par le personnel de sécurité et le personnel non lié à la sécurité afin de favoriser une plus grande sensibilisation, une meilleure préparation et un rétablissement souple des opérations normales.

10.3.4. Récupération

Le rétablissement fait référence à la restauration de tous les niveaux de prestation des services après un incident. Cela peut inclure la collecte de preuves pour faciliter les poursuites.

10.4. Prévention du crime par la conception environnementale

Prévention du crime par la conception environnementale (PCCE) est une approche multidisciplinaire de la prévention du crime lors de la désignation, de la définition et de la conception de la sécurité des l'environnement. La conception et la gestion des environnements, peuvent permettre aux ministères et aux organismes de dissuader les criminels ou les accusateurs des mesures tout en gérant en toute sécurité le flux de personnes dans une installation. Ces modèles avoir l'intention d'influencer positivement le comportement et les activités tout en décourageant les comportements indésirables actions du personnel, des visiteurs et des adversaires potentiels.

11. Choix du système et considérations relatives à la zone

Les systèmes de sécurité physique bénéficient tous de l'application des défense en profondeur et les systèmes de détection devraient faire partie de chaque zone de transition, les mesures de sauvegarde devenant de plus en plus complètes à mesure qu'elles se rapprochent des actifs précieux. Une EMR fournira de l'information sur la nature et la gravité des menaces pesant sur une installation et devrait être effectuée pour aider à choisir les systèmes de détection appropriés qui répondent le mieux aux besoins du site. Les zones à envisager pour l'utilisation d'équipement de détection sont:

Tableau 2 : Zones et recommandations de sélection

Zone	Recommandations
Public	• Vidéosurveillance (surveillée) — Permet aux équipes de sécurité d'identifier rapidement les conditions dans les espaces publics sur et autour d'une installation, y compris, mais sans s'y limiter, les manifestations, les troubles civils, le harcèlement du personnel approchant ; • Vidéosurveillance (non surveillée) — Ne fournis pas d'élément de détection, mais peut être utilisé dans les enquêtes après l'incident et ne dois donc pas être ignoré entièrement ; et • Détecteurs de vibrations (clôture) — Peut être un moyen efficace d'alerter la sécurité lorsqu'il y a une tentative d'escalade ou de violation d'une clôture périmétrique entre une zone publique et des espaces contrôlés où les méthodes comme la détection de mouvement seraient impossibles en raison de la proximité de voies publiques.
Accueil	• Capteurs de mouvement/tomographie — Un moyen efficace de détecter lorsqu'une personne est entrée dans l'espace alors qu'il n'y a pas d'autres éléments de détection présents. Une zone d'accueil (ZA) est une zone où les visiteurs sont attendus, il est donc de bonne pratique afin de limiter les alarmes liées au système de détection de mouvement aux moments où les visiteurs ne devraient pas être présents ; • Capteurs photoélectriques — Un moyen efficace de compartimenter les zones où les visiteurs et le personnel sont séparés au sein d'une ZA, comme derrière le bureau de service. Les capteurs ainsi installés émettent généralement une alarme sonore lorsqu'ils sont activés, ce qui alerte le personnel et agit comme un moyen de dissuasion psychologique ; • Capteurs de bris de verre — Alerte la sécurité dans le cas où une fenêtre est brisée, et nécessiterait une action immédiate, quelle que soit l'heure ; • Alarmes de contact — Installées sur les portes et les fenêtres, elles peuvent alerter la sécurité lorsqu'une porte est ouverte en dehors des heures d'ouverture. En outre, une alarme sonore peut être activée si une porte est ouverte sans autorisation appropriée qui peut alerter le personnel et agir comme un moyen de dissuasion psychologique ; • Vidéosurveillance — Permet aux équipes de sécurité d'identifier rapidement les conditions dans la ZA et peut fournir des preuves pour aider aux enquêtes après l'incident ; • Point de contrôle (surveillance visuelle) — Cela pourrait être le personnel d'accueil ou le personnel de sécurité dédié. Dans les deux cas, le membre du personnel devrait être formé à la sensibilisation à la sécurité et familiarisé avec les procédures internes d'alerte de sécurité ou d'application de la loi si nécessaire. À un point de contrôle, le contrôle d'accès est souvent nécessaire, comme ; les feuilles d'ouverture de session, les contrôles d'identité/cartes d'accès ou l'attribution d'escortes

	pour les visiteurs ; • Détecteurs de métaux — S'ils sont requis, un détecteur de métaux peut être utilisé de façon permanente ou temporaire pour contrôler le personnel et les visiteurs lorsqu'ils entrent dans l'installation. Les détecteurs de métaux nécessitent des POS et du personnel de sécurité formé pour les utiliser ; et • Rayons X — Souvent utilisés pour scanner les sacs et contenants entrant dans une installation lorsqu'une fouille physique est inappropriée ou inefficace. L'utilisation d'un appareil à rayons X ne sera souvent mise en œuvre que si un EMR le juge nécessaire. Les appareils à rayons X nécessitent des POS et du personnel de sécurité formé pour fonctionner.
Travail	• Capteurs de mouvement/tomographie — Un moyen efficace de détecter lorsqu'une personne est entrée dans un espace où il n'y a peut-être pas d'autres éléments de détection présents. Ces systèmes peuvent être configurés pour être actifs uniquement en dehors des heures d'ouverture afin de limiter les alarmes fausses causées par le personnel en service ; • Détecteurs de bris de verre — Dans les cas où la zone de travail comporte des barrières de verre entre celle-ci et un ZA ou un espace public, ils alerteront la sécurité en cas de bris de fenêtre, un événement qui nécessiterait une intervention immédiate, que cela se produise pendant ou après les heures d'ouverture ; • Alarmes de contact — Installées sur les portes et les fenêtres, elles peuvent alerter la sécurité lorsqu'une porte a ouverte sans avoir d'abord scanné une carte d'accès ou entré une broche, ou lorsqu'elle est ouverte en dehors des heures d'ouverture ; • Surveillance visuelle — Le personnel bien formé et soucieux de la sécurité peut aider à assurer la sécurité du site en signalant lorsqu'il voit une personne dans une ZT sans le bon laissez-passer ou l'escorte. Il devrait s'agir d'une mesure de sauvegarde supplémentaire et ne pas être utilisé à la place de mesures de sécurité officielles ; • Vidéosurveillance — Permets aux équipes de sécurité d'identifier rapidement les conditions et peuvent fournir des preuves pour aider dans les enquêtes post-incidentes ; et • Patrouilles — Le personnel de sécurité formé peut être une méthode efficace pour renforcer le profil de sécurité d'un site, ils utilisent l'équipement de sécurité et effectuent des patrouilles qui augmentent la présence de l'équipe de sécurité et leur permettent de répondre rapidement aux urgences.
Sécurité/haute sécurité	• Capteurs de mouvement/tomographie — Un moyen efficace de détecter lorsqu'une personne est entrée dans un espace où il n'y a peut-être pas d'autres éléments de détection présents. Ces systèmes peuvent être configurés pour être actifs uniquement en dehors des heures d'ouverture afin de limiter les fausses alarmes causées par le personnel en service ; • Alarmes de contact — Installé sur les portes et les fenêtres peut alerter la

	sécurité lorsqu'on est ouvert sans d'abord scanner une carte d'accès/entrer une broche, ou lorsqu'il est ouvert en dehors des heures de fonctionnement. De plus, ils peuvent être utilisés pour compartimenter davantage les actifs dans une zone en les installant sur des conteneurs de sécurité spécifiques, qui peuvent indiquer quand on y a accédé. Dans les cas où le mécanisme est électronique et non manuel, une alarme peut être déclenchée si le conteneur est ouvert sans saisir correctement le code PIN ou scanner une carte d'accès ; • Vidéosurveillance — Permet aux équipes de sécurité d'identifier rapidement les conditions et peut fournir des preuves pour aider dans les enquêtes après un incident. Dans les zones de sécurité (ZS) et les zones à haute sécurité (ZHS), il faut veiller à ce que la vidéosurveillance ne regarde pas les zones où des renseignements sensibles sont traités. Limiter la surveillance aux points d'accès et aux itinéraires de déplacement ; et • Patrouilles — Le personnel de sécurité formé peut être une méthode efficace pour renforcer le profil de sécurité d'un site, utiliser du matériel de sécurité et effectuer des patrouilles qui augmentent la présence de l'équipe de sécurité et lui permettre de répondre rapidement aux urgences. Le personnel de sécurité doit détenir une habilitation de sécurité correspondant au niveau de sensibilité le plus élevé traité dans la zone qu'il patrouille.

En plus d'analyser les exigences de détection de chaque zone, il faut tenir compte des facteurs supplémentaires suivants :

- Heures d'ouverture ;
- Servitudes ;
- Espaces partagés ;
- Densité de la population ; et
- Délais/temps de réponse.

Ces facteurs peuvent modifier les exigences du système de détection et mettre en évidence des complications qui peuvent affecter le choix de l'équipement de détection utilisé. Par exemple, une installation située dans un secteur très peuplé peut ne pas bénéficier de capteurs de mouvement sur le périmètre où les piétons déclencheraient des alarmes constantes. Dans ce cas, un capteur de vibration sur la clôture périphérique peut être plus efficace puisqu'il ne déclencherait une alarme que si quelqu'un tentait d'escalader la clôture. La réalisation d'une EMR est le moyen le plus efficace pour évaluer avec précision les besoins spécifiques de chaque site.

12. Conclusion

Les systèmes de détection sont très modulaires et personnalisables, avec des solutions qui peuvent être ajoutées ou modifiées à différents moments en fonction de la situation. Il est aussi

important de comprendre l'environnement des menaces que de comprendre les dispositifs de détection disponibles pour contrer ces menaces. Une fois qu'une menace a été identifiée, un système de détection approprié peut être sélectionné et mis en œuvre. Les fabricants d'équipement de détection peuvent collaborer avec l'équipe de sécurité physique d'un ministère ou d'une agence pour identifier un produit commercial prêt à l'emploi ou personnalisé afin d'atténuer efficacement une gamme de risques auxquels une installation pourrait être confrontée. La détection est une considération importante pour la sécurité physique et la défense en profondeur de chaque installation.

13. Références et documents connexes

- Politique sur la sécurité du gouvernement — Canada.ca
- Directive sur la gestion de la sécurité — Canada.ca
- Appel à l'action en faveur de la lutte contre le racisme, de l'équité et de l'inclusion dans la fonction publique fédérale — Bureau du Conseil privé — Canada.ca
- Directive sur l'obligation de prendre des mesures d'adaptation — Canada.ca
- Guide à l'intention des employés. e. s deux esprits, transgenres, non-binaires et de la pluralité des genres dans la fonction publique fédérale
- Prévention du crime par l'aménagement du milieu (PCAM)
- Méthodologie harmonisée d'EMR (TRA-1) — Centre canadien pour la cybersécurité
- GSMGC-011 (2024) — Guide des systèmes de surveillance vidéo
- GSMGC-019 (2023) — Guide de protection, détection, réponse, et récupération

14. Promulgation

Examiné et recommandé aux fins d'approbation.

J'ai examiné et recommande par la présente, GSMGC-021 (2025) Principes fondamentaux des systèmes de détection en sécurité physique.

Nattress,Shawn Thomas,000302786 Digitally signed by Nattress,Shawn Thomas,000302786
Date: 2025.04.25 14:09:39 -04'00'

Shawn Nattress, Date
Gestionnaire
Principale Organisme Responsable de la Sécurité Matérielle, GRC

Approuvé

J'approuve par la présente GSMGC-021 (2025) Principes fondamentaux des systèmes de détection en sécurité physique.

St-Pierre,Andre Vincent,000171484 Digitally signed by St-Pierre,Andre Vincent,000171484
Date: 2025.05.20 11:10:08 -04'00'

André St-Pierre, Date
Directeur, Sécurité Matérielle
Gendarmerie royale du Canada