LIVRE BLANC

Protection périmétrique grâce à la surveillance intelligente

Étude des options de capteur, des applications et des points essentiels à envisager pour garantir une solution de sécurité à l'épreuve du temps dans un large éventail de secteurs.

Juillet 2021

AXIS COMMUNICATIONS

Table des matières

1 Avant-propos

Une clôture est souvent un composant essentiel de la « couche extérieure » de la sécurité d'un site. Elle peut agir comme une barrière, un écran ou un outil de dissuasion pour les personnes et les animaux. D'autres fonctionnalités peuvent être intégrées pour améliorer l'efficacité d'une clôture, car une barrière physique ne pourra que retarder ou gêner une intrusion.

Plusieurs types de détecteurs sont utilisés le long des clôtures. Des détecteurs par câbles peuvent suivre l'itinéraire de la clôture, et les capteurs radar (à micro-ondes), les lasers et barrières infrarouges peuvent être positionnés à des emplacements stratégiques.

Tous les types de détecteurs peuvent produire de fausses alarmes, provoquées, par exemple, par des animaux, des plantes ou des arbres en mouvement et des conditions météorologiques peu clémentes. Il peut également exister d'autres facteurs de contrainte, tels que des conflits de fréquence lorsqu'on utilise les capteurs à micro-ondes, ou les limitations physiques de l'environnement de l'installation.

Les caméras offrent un avantage évident aux personnes désireuses de contrôler de grands espaces ou plusieurs emplacements. Les solutions réseau modernes associent le traitement informatique et l'intelligence artificielle dans la caméra. L'évolutivité, l'efficacité et la nature dissuasive inhérentes à la technologie signifient que les caméras vidéo sont potentiellement un ajout très rentable à un système de sécurité.

Bien que les caméras et les logiciels de détection de mouvement aient développé la portée et les capacités de protection périmétrique, ces solutions peuvent être limitées par une incapacité de détection en cas de très mauvaises conditions météorologiques. Les caméras thermiques, lorsqu'elles sont correctement calibrées et associées aux analyses vidéo, fournissent une surveillance et un contrôle efficaces, sans être affectées par les conditions d'éclairage et pratiquement pas entravées par les conditions météorologiques extrêmes.

L'analyse vidéo a beaucoup évolué au fil du temps et est désormais monnaie courante, même dans les caméras destinées au marché de la sécurité domestique. Les analyses peuvent réduire les besoins en stockage en n'enregistrant que les vidéos qui contiennent des activités dignes d'intérêt. En traitant l'essentiel de la vidéo enregistrée directement dans la caméra elle-même, la charge sur le réseau est considérablement réduite car seules les vidéos nécessaires sont diffusées à partir des caméras. Ceci représente des avantages évidents dans un scénario de salle de contrôle.

Comme pour toute mesure de sécurité, l'étude d'une solution de protection périmétrique doit être adaptée et proportionnée. Comme toujours, la menace est au cœur de l'attention.

Une approche combinée de la sécurité qui inclut les données et l'examen attentif des autres services, tels que le service informatique et le service des opérations, représente actuellement la meilleure pratique. Il est par ailleurs nécessaire d'inclure les personnes concernées par les besoins techniques, aussi tôt que possible dans la procédure.

Il est notoirement difficile de démontrer le retour sur investissement (ROI) d'une solution de sécurité conçue pour prévenir un incident. Et ceci principalement en raison de l'absence de revenu potentiel à comparer aux coûts engagés. Démontrer un retour sur investissement plus tangible est possible. On peut citer en exemple des solutions qui non seulement alertent le personnel d'un comportement suspect ou d'une intrusion, mais qui produit également des réponses automatisées.

2 Introduction

Les solutions électroniques de protection périmétrique ont traditionnellement été le domaine des sites commerciaux et gouvernementaux haute sécurité ou l'apanage des plus riches. Grâce aux avancées

technologiques, à un marché plus compétitif et à une importante réduction des coûts, les solutions de haute technologie sont à présent disponibles à un plus grand nombre.

Donc de quoi se compose une solution de protection périmétrique moderne ? Quelle est la technologie à l'œuvre et comment peut-elle offrir à la fois réconfort et véritable protection ?

Ce livre blanc examine certaines options actuelles basées sur les capteurs pour la protection périmétrique et offre un aperçu de la technologie derrière les solutions.

3 Solutions de protection périmétrique

3.1 Solutions physiques

Les solutions physiques sont souvent le composant de base de la « couche extérieure » d'une approche compartimentée de sécurisation d'un site, qui comprend généralement une clôture périmétrique, souvent composée d'un treillis métallique ou d'un grillage soudé dans des panneaux soudés ou des panneaux de béton. Une clôture périmétrique a plusieurs objectifs, l'un des principaux étant de représenter une barrière physique qui retardera ou évitera les intrusions. Une clôture peut également empêcher la surveillance en faisant écran à un bien ; elle sert également de moyen de dissuasion et empêche les animaux d'entrer. Des dispositifs tels que l'anti-escalade, l'anti-franchissement, les itinéraires d'accès délimités pour les véhicules, et les brise-vues peuvent également être ajoutés pour améliorer l'efficacité de la clôture périmétrique.

En revanche, n'importe quelle barrière physique ne fera que retarder une intrusion. Le périmètre doit donc être également équipé d'une technologie de détection automatique des intrusions, capable de fournir des alertes, des données de localisation, le suivi de la cible, éléments vérifiables en temps réel et la possibilité de rassembler des preuves et des données pour l'enquête post-incident.

3.2 Détection des intrusions sur un périmètre physique

Plusieurs types de « détecteurs » par câbles sont souvent utilisés pour sécuriser les périmètres étendus. Ces détecteurs basés sur des câbles sont habituellement enterrés dans le sol ou montés sur la clôture, ils suivent l'itinéraire de la clôture et n'ont pas à être en ligne droite. Ils offrent également une couverture des coins et des **angles morts**. Certains fournisseurs proposent des clôtures équipées de solutions de détection automatique.

Comme toute solution de détection, les détecteurs basés sur les câbles peuvent générer de fausses alarmes, qu'on appelle « faux positifs ». Les raisons fréquentes de ces faux positifs sont les animaux, les plantes et les arbres en mouvement et les conditions météorologiques extrêmes. Les solutions basées sur les câbles fonctionnent mieux lorsqu'elle sont améliorées par la vidéosurveillance. La vidéo peut être utilisée non seulement pour vérifier une intrusion, mais également pour déterminer la cause d'une alarme. Une solution basée sur les câbles sera seulement capable de fournir une alerte de l'intrusion mais elle ne pourra pas fournir d'informations sur le nombre d'intrus ou tout autre détail nécessaire pour préparer une réponse.

3.3 Autres capteurs de détection des intrusions

D'autres détecteurs d'intrusion, tels que les capteurs radar (à micro-ondes), les barrières ou les lasers infrarouges peuvent être positionnés à des emplacements stratégiques autour du périmètre. Mais ces technologies peuvent être limitées par des problèmes tels que des fausses alarmes et des capacités de détection limitées en termes de distance et de hauteur si les règles d'installation ne sont pas correctement respectées.

L'utilisation du radar sur le périmètre peut être particulièrement problématique dans un environnement qui utilise d'autres dispositifs électroniques. Ceux-ci pourraient fonctionner sur la même fréquence et le même spectre, et tandis qu'un choix minutieux de la fréquence ou la réduction de la puissance pourrait réduire les interférences, cela gênera également la portée efficace du dispositif.

4 Solutions basées sur la vidéo

4.1 Application des caméras vidéo

Les technologies de CCTV autonomes traditionnelles du passé ne ressemblent que peu aux solutions de caméra réseau haute technologie disponibles aujourd'hui. Les solutions réseau modernes sont capables d'associer le traitement informatique et l'intelligence artificielle dans la caméra. Ce niveau de technologie, cependant, n'existe que depuis très récemment et n'en est qu'à ses débuts.

Les caméras offrent un avantage évident à ceux qui souhaitent surveiller de vastes zones ou plusieurs sites. L'évolutivité, l'efficacité et la nature dissuasive inhérentes à la technologie signifient que les caméras vidéo sont potentiellement un ajout très rentable à un système de sécurité.

En fonction de la législation locale, la technologie des caméras peut être utilisée pour contrôler au-delà du périmètre physique, ce qui crée une zone tampon de surveillance supplémentaire et offre éventuellement à l'opérateur plus de temps pour réagir. Les solutions qui exploitent les analyses vidéo permettent le déclenchement d'une alarme en fonction de règles définies. Par exemple, une alarme retentit si une personne s'approche à moins de 50 mètres d'une clôture, un niveau plus important d'alarme pourrait être déclenché si cette même personne continue à marauder ou pénètre dans une zone à moins de 10 mètres.

4.2 Solutions de vidéosurveillance thermographiques

La combinaison des caméras de vidéosurveillance et d'un logiciel de détection de mouvement a développé la gamme et les fonctionnalités des solutions de protection périmétrique d'une simple détection à l'analyse d'intrusions complexes. Cependant, l'efficacité de la vidéo peut être sérieusement limitée par son incapacité de détection lorsque les conditions météorologiques sont défavorables.

La disponibilité accrue de la technologie des caméras thermiques a conduit à la prédominance de leur utilisation sur le périmètre. Les caméras thermiques (ou thermographiques), lorsqu'elles sont correctement calibrées et associées aux analyses vidéo, peuvent fournir une surveillance et un contrôle efficaces, sans être affectées par les conditions d'éclairage et pratiquement pas entravées par les conditions météorologiques extrêmes. Les capteurs utilisant la technologie thermique offrent un contraste supérieur à celui d'une caméra classique à lumière visible et sont par conséquent bénéfiques pour la protection des périmètres en raison de capacités de détection des intrusions nettement améliorées.

Les capteurs thermiques créent une image à l'aide de la radiation infrarouge émise par les objets tels que les véhicules ou les personnes. Lorsqu'elles sont associées à l'analyse vidéo, les caméras thermiques modernes dotées d'une puissance de traitement suffisante peuvent faire la distinction entre les différents types de cibles d'intrusion et peuvent alerter l'opérateur en fonction d'une liste définie de conditions. Parmi ces conditions, on trouve la direction et la vitesse d'une personne ou d'un véhicule. Les caméras traditionnelles sont également capables de cela mais pour ce faire, elles ont besoin de la lumière visible. Ces caméras sont examinées dans la partie suivante.

4.3 Caméras à lumière visible

Toutes les caméras de surveillance à lumière visible standard ont besoin de la lumière naturelle ou d'un éclairage augmenté pour fournir des images. L'éclairage dans le domaine de la vidéosurveillance est un domaine d'expertise en soi et des livres distincts ont été rédigés sur cet important sujet. Cependant, il nous faut toujours répéter le point évident et essentiel que les caméras standard ont besoin de lumière visible. L'éclairage peut représenter un défi quel que soit l'environnement, avec des effets évidents lorsque la qualité d'éclairage change. Les conditions météorologiques ne sont pas toujours prises en compte ou comprises, en particulier par ceux qui spécifient la solution.

Les caméras thermiques ont leurs avantages, mais cela ne veut pas dire qu'elles doivent ou peuvent remplacer directement les caméras à lumière visible, loin de là. Ces deux technologies fonctionnent mieux lorsqu'elles sont intégrées dans la même solution. Les caméras traditionnelles ne peuvent détecter des objets aux mêmes portées que les caméras thermiques, mais les caméras thermiques ne peuvent apporter le niveau de détails nécessaire aux investigations policières fournis par les caméras à lumière visible. Les deux technologies sont souvent combinées, la caméra thermique fournissant l'alarme de détection et l'avantage du niveau de détails de la caméra à lumière visible fournissant à la fois les preuves et le suivi de la cible.

4.4 Analyse de contenu vidéo

La vidéosurveillance sur IP a apporté une ampleur sans précédent aux opérations de sécurité. Une hiérarchie d'autorisations efficace permet l'accès, la répartition et le stockage vidéo contrôlés d'un nombre théoriquement illimité de parties prenantes. Une avancée technologique en particulier développe encore plus les niveaux d'évolutivité : l'analyse vidéo.

L'analyse vidéo a considérablement évolué avec le temps, notamment en raison du développement de la technologie des caméras sur IP. C'est le cas des caméras destinées au marché de la sécurité domestique, dont beaucoup intègrent désormais un certain niveau de fonction analytique, leur permettant, par exemple, de détecter les mouvements dans la scène. Des fonctionnalités supplémentaires peuvent être intégrées à la caméra, telles que la détection de passage, les objets déplacés ou même le décompte de personnes.

Les analyses vidéo peuvent éliminer le besoin d'espace de stockage en n'enregistrant que les vidéos contenant une activité. En outre, en traitant l'essentiel de la vidéo enregistrée directement dans la caméra elle-même (ce qu'on appelle « intelligence en périphérie de réseau »), la charge sur le réseau est considérablement réduite car seules les vidéos pertinentes sont diffusées à partir des caméras. Ceci représente des avantages évidents dans le cas d'une salle de contrôle, avec un personnel de sécurité qui ne doit examiner la vidéo que lorsqu'il reçoit une alerte. Cela représente un développement majeur pour le personnel de sécurité et pour l'efficacité opérationnelle de l'entreprise.

Deux architectures de systèmes sont possibles pour le traitement de l'analyse vidéo : centralisée ou distribuée. Dans une architecture centralisée, les données vidéo et les autres informations sont recueillies par les caméras et les capteurs, puis transmises à un serveur central pour être analysées. Dans une architecture distribuée, les équipements de périphérie (caméras réseau et encodeurs vidéo) traitent eux-mêmes les vidéos pour en extraire les informations utiles. Les analyses en périphérie de réseau éliminent le recours à des serveurs d'analyse dédiés, et comme la compression n'est utilisée que lors du transfert des données vidéo vers un serveur central, les analyses peuvent dorénavant être réalisées sur le flux vidéo non compressé. L'architecture qui en découle est alors plus rentable et plus souple. En fait, les mêmes serveurs, qui pourraient habituellement traiter uniquement quelques flux vidéo en raison de la puissance de traitement requise, peuvent à présent gérer des centaines de flux vidéo lorsque l'essentiel du traitement est réalisé par les caméras.

4.4.1 Vitesses de traitement et processeurs graphiques

Bien que la prédiction exacte de Gordon E. Moore (alias la loi de Moore) concernant l'amélioration exponentielle des vitesses et des capacités de traitement ait été annoncée par certaines grandes entreprises technologiques comme devant ralentir dans un avenir proche, l'augmentation actuelle de la puissance combinée à la réduction de la taille a permis aux fabricants et aux développeurs d'appareils photo de modifier la façon dont la puissance de traitement est exploitée.

Jusqu'à récemment, toute capacité de traitement supplémentaire était utilisée pour améliorer la qualité d'image, offrant une meilleure résolution et une compression vidéo plus efficace. Pour le moment, cependant, le marché semble avoir presque atteint un plateau en termes de demande d'une résolution d'image encore meilleure. Par conséquent, les fabricants utilisent dorénavant la puissance de traitement pour fournir des niveaux d'intelligence inédits en périphérie de réseau. Dans de nombreux cas, cela signifie que les puissantes analyses vidéo basées sur serveur peuvent à présent bénéficier d'un traitement dans la caméra.

Le fait que les processeurs modernes soient plus petits et plus rapides signifie que les caméras peuvent accueillir des processeurs graphiques (GPU), ce qui offre des capacités de traitement parallèles et ouvre de nouvelles opportunités et possibilités d'analyse. Cette nouvelle capacité a incité les développeurs de logiciels à s'intéresser à la conception de nouvelles versions d'analyses existantes et éprouvées basées sur des serveurs dans des variantes basées sur la périphérie, contribuant ainsi à stimuler la demande de caméras plus intelligentes, capables d'apporter une valeur ajoutée allant bien au-delà de la simple sécurité et de la vidéosurveillance.

4.4.2 Deep learning et intelligence artificielle (IA)

Les processeurs graphiques ont permis aux performances d'analyse en périphérie de réseau de faire un bond en avant mais la demande est en pleine croissance pour les autres types de technologie s'appliquant dans le domaine de la surveillance, qui offrent des fonctionnalités telles que le comptage de personne ou la gestion de l'occupation. Les progrès de l'IA et de l'apprentissage automatique ont permis d'intégrer des unités de traitement d'apprentissage profond (DLPU) dans les caméras, ce qui change la donne.

Un DLPU est spécialement conçu pour la plus vaste application d'analyse d'apprentissage profond. Les analyses basées sur l'apprentissage profond peuvent offrir une précision supérieure pour la détection et la classification, car l'algorithme est effectivement formé à ce à quoi ressemble un ensemble d'objets prescrits. Cela signifie qu'une solution de détection des intrusions dans un périmètre peut être configurée pour n'émettre des alertes que pour des objets et des scénarios très spécifiques, une version avancée de l'If-this-then-this (ITTT).

Dans certains cas, seule une partie d'un objet est visible, telle que le pare-chocs arrière d'une voiture, mais le système d'analyse le reconnaîtra et l'identifiera quand même. Au moment où nous rédigeons ce document, et malgré certaines réclamations, les solutions éprouvées sur le marché sont limitées à l'identification et la discrimination entre les personnes et les types de véhicules. Toutefois, des exemples de modèles analytiques basés sur des caméras et capables d'effectuer une discrimination plus détaillée, comme la couleur des vêtements portés par une personne, sont à un stade avancé de test.

Ces avancées technologiques pourraient éventuellement conduire à des systèmes de détection hautement ciblés, capables d'identifier et de faire la distinction entre les employés, les clients, les membres du public ou les menaces potentielles. Du point de vue de la sécurité, l'analyse avancée dans un environnement où la sécurité physique est bien appliquée ne peut qu'aboutir à un système encore plus efficace et précis de détection et de prévention des délits. L'évolution vers la prochaine étape n'est peut être pas si lointaine.

5 Coûts

5.1 Estimation et mesure du retour sur investissement

Comme pour toute mesure de sécurité, que ce soit du point de vue de la vulnérabilité ou de la résistance, l'étude d'une solution de protection périmétrique doit être adaptée et proportionnée. Comme toujours, la menace doit être au cœur de l''attention. Pour presque tous les sites gouvernementaux ou d'entreprise quelle que soit leur taille, de nos jours, cette menace peut prendre diverses formes allant des intrus accidentels aux manifestants et aux terroristes.

Une approche combinée de la sécurité qui inclut les données et l'examen attentif des autres services, tels que le service informatique et le service des opérations, représente actuellement la meilleure pratique. Il est par ailleurs nécessaire d'inclure les personnes concernées par les besoins techniques, car elles doivent être impliquées aussi tôt que possible dans la procédure. Lorsqu'on étudie les mesures à appliquer, traditionnellement, un bon point de départ en ce qui concerne le périmètre aurait été les mesures les plus traditionnelles, qui habituellement dissuadent et retardent un éventuel intrus. Uniquement par la suite, le concepteur de la sécurité aurait intégré les systèmes de détection techniques en option. Mais avec de nombreuses mesures et de nombreux systèmes qui s'intègrent dorénavant les uns aux autres, il est nécessaire d'avoir une approche plus réfléchie et plus holistique.

Il est notoirement difficile de démontrer le retour sur investissement (ROI) d'une solution de sécurité conçue pour prévenir un incident. Et ceci principalement en raison de l'absence de revenu potentiel à comparer aux coûts engagés. En général, le personnel de sécurité travaille avec ses collègues du département financier pour illustrer le coût des différents types d'incidents de sécurité, qu'il s'agisse de coûts directs dus à la perte ou à la destruction de biens, ou de coûts moins immédiats mais tout aussi dommageables liés à la perte de réputation.

Cependant, démontrer un retour sur investissement plus tangible est possible, en particulier en utilisant certaines technologies qui diminuent l'activité manuelle spécifique ou qui permet au personnel de sécurité d'être redéployé sur d'autres tâches. Des exemples peuvent être trouvés dans les solutions qui non seulement alertent le personnel des comportements suspects ou des intrusions, mais qui peuvent également produire des réponses douces automatisées. Ces solutions peuvent inclure des systèmes audio sur IP qui peuvent émettre des annonces pré-enregistrées, ou des panneaux lumineux informant un potentiel intrus qu'il a été détecté et lui donnant l'ordre de quitter la zone.

Si les caméras de surveillance sont intégrées à la solution, on peut ensuite augmenter l'efficacité en montrant aux intrus des preuves de leur identification, par exemple un écran indiquant que leur plaque d'immatriculation a été enregistrée ou même une image de l'intrus. Ce n'est que lorsque ces mesures préliminaires n'ont pas produit l'effet souhaité qu'il est nécessaire que l'équipe de sécurité soit envoyée sur place pour enquêter ou pour une action plus directe. Cette approche par étape pour répondre aux alertes pourrait être plus adaptée à une utilisation en dehors du périmètre, mais elle permettra de diminuer le recours au personnel de sécurité à un stade précoce, libérant ainsi de la main d'œuvre ce qui représente un avantage non négligeable.

5.2 Estimation des coûts

L'estimation des coûts devra se baser sur le calcul du coût total de possession (CTP). Le CTP comprend tous les coûts associés à la solution tout au long de son cycle de vie : les coûts matériels et humains, les coûts d'études, les coûts d'installation du système, les coûts de fonctionnement, les frais d'entretien, les frais de mise hors service et de recyclage. Cela peut nécessiter un changement d'approche de la part des

services financiers et des achats, car il faudra peut être réaffecter le capital entre les budgets de dépense d'établissement et de charges d'exploitation.

Comme pour tout bien tangible, l'entreprise devra connaître la durée d'utilisation prévue de la solution de détection périmétrique. Les responsables de la sécurité et de l'informatique peuvent aider leurs collègues des finances en expliquant et en démontrant comment l'acquisition de la bonne technologie comme plate-forme pour les solutions futures permettra de réaliser des économies. Une caractéristique des dispositifs de surveillance intelligents perfectionnés, est qu'ils sont, dans une certaine mesure, à l'épreuve du temps. C'est-à-dire que ces dispositifs dotés d'une puissance de traitement adaptée sont capables de profiter à maintes reprises des avancées technologiques au fil du temps, plus particulièrement grâce au traitement d'analyses basées sur l'IA et le machine learning.

6 Proposition d'Axis Communications

L'approche ouverte d'Axis en matière d'intégration avec des solutions partenaires signifie que ses capteurs en réseau, combinés à des analyses vidéo éprouvées et à l'exploitation de l'IA, permettent aux clients de mettre en œuvre des solutions de protection du périmètre intégrées et performantes, cyber-sécurisées et rentables dans toute l'entreprise et pendant toute la durée de vie du système.

Lorsque les capteurs thermiques pourraient ne pas être appropriés, la technologie des micro-ondes (radar) représente une formidable alternative, car elle offre de nombreux avantages similaires à la technologie thermique, en limitant potentiellement les fausses alertes. La technologie radar d'Axis bénéficie du même machine learning (apprentissage automatique) et deep learning (apprentissage profond) que les caméras de surveillance les plus avancées. Les appareils radar d'Axis peuvent détecter, classer et suivre avec précision les personnes et les véhicules avec un taux presque nul de fausses alarmes.

La technologie radar fonctionne 24 h sur 24 et 7 j sur 7 et elle n'est presque pas affectée par les déclencheurs habituels tels que les ombres en mouvement ou les faisceaux lumineux, les petits animaux ou les insectes ou les mauvaises conditions météorologiques. Par conséquent, le fonctionnement est très rentable, car le personnel de sécurité peut se concentrer sur les véritables menaces confirmées. Le radar peut également indiquer la vitesse d'un objet, ce qui permet un calcul précis d'un point de contact ou même pour faire respecter les limitations de vitesse.

Les performances d'une solution représentent souvent la première partie de toute demande d'informations ou d'un questionnaire d'analyse de marché. Les caméras Axis sont équipées des propres processeurs ARTPEC d'Axis, offrant la meilleure capacité du secteur, ce qui permet l'intégration dans la caméra (en périphérie) des solutions d'analyse vidéo de protection périmétrique les plus avancées. Il est important de noter que cela apporte également la garantie que la solution exploite la puissance de la technologie interne et ne fait pas appel à des composants de tiers.

Cette intelligence « en périphérie » signifie que plusieurs caméras peuvent par conséquent suivre plusieurs événements qui se produisent en même temps à différents endroits. Cette architecture que l'on nomme architecture technique répartie permet d'étendre la solution à autant de caméras que nécessaire, tout en éliminant les investissements dans une technologie de serveur centralisé.

Grâce à AXIS Perimeter Defender (APD) approuvé par le gouvernement britannique, quatre types d'événement différents sont détectés, pour un ou plusieurs individus ou véhicules :

- • Intrusion dans une zone prédéfinie
- • Franchissement de zones dans un ordre et un sens déterminés
- • Franchissement de zone conditionnel

- • Présence de maraudeurs

APD peut fournir plus qu'une simple alarme d'intrusion et la vidéo correspondante. Il fournit également des métadonnées qui peuvent être utilisées pour afficher une incrustation sur la vidéo, montrant les limites du terrain et les trajectoires des personnes et des véhicules en mouvement. Pour une approche plus intégrée, les caméras Axis (à lumière visible ou thermiques) fonctionnent également avec des haut-parleurs sur IP pour diffuser des messages automatiques lorsqu'un événement est détecté et peut être une solution potentiellement autonome. Ce type d'avertissement automatisé permettra une « intensification » des mesures et des contremesures, point important pour déterminer les intentions d'un intrus et la réponse consécutive nécessaire.

APD peut être intégré directement dans les logiciels fréquemment utilisés dans les plateformes d'entreprises (par ex. Genetec, Milestone, SeeTec, Prysm, Qognify et d'autres).

Axis offre à titre gracieux des outils de conception pour aider à l'organisation après étude préalable et une assistance à toutes les étapes du projet, de la sélection des bons produits en fonction de critères spécifiques au calcul précis des besoins de stockage, à l'installation et à la gestion des systèmes. En tirant parti des outils d'Axis, les consultants pourront planifier et estimer, et un intégrateur pourra gérer les projets de manière plus fluide et plus efficace. Ces outils permettent même de garantir la sécurité des systèmes installés, car le logiciel intégré simplifie l'installation de mises à niveau et de correctifs de sécurité.

Tandis que les menaces et les contremesures évoluent, un point essentiel reste constant, l'intégrité et la sécurité du périmètre. Le périmètre est un point d'attention fondamental pour les personnes qui mettent en œuvre l'obligation d'une entreprise de fournir un environnement sain et sûr pour le personnel, les visiteurs et les membres du public. Ce livre est destiné à promouvoir auprès des entreprises les avantages d'une approche de technologie intégrée en matière de sécurité périmétrique. Il souligne également le fait que l'investissement dans la technologie de sécurité doit être appuyé par un retour sur investissement démontrable. Dans tous les cas, comprendre les capacités technologiques adéquates actuelles, et pouvoir apprécier les tendances futures est une approche d'achat et de sécurité opérationnelle sûre pour tout professionnel de la sécurité, quel que soit son service, son titre ou son secteur.

Références des produits

Caméras thermiques sur IP :

AXIS Q19 et plus de modèles sur www.axis.com/en-gb/products/thermal-cameras

Logiciel d'analyse :

AXIS Perimeter Defender

www.axis.com/en-gb/products/axis-perimeter-defender

Haut-parleurs externes sur IP :

AXIS C1310-E www.axis.com/en-gb/products/axis-c1310-e

Radar de sécurité sur IP :

D2110-VE www.axis.com/en-gb/products/axis-d2110-ve

À propos d'Axis Communications

En concevant des solutions qui améliorent la sécurité et les performances de l'entreprise, Axis crée monde plus clairvoyant et plus sûr. En tant qu'entreprise de technologie de réseau et leader de l'industrie, Axis propose des solutions de vidéosurveillance, de contrôle d'accès, d'interphonie et de systèmes audio. Les performances de ces solutions sont améliorées grâce à des applications d'analyse intelligentes et une formation de haute qualité.

Axis emploie près de 4 000 personnes dans plus de 50 pays et collabore avec des partenaires technologiques et d'intégration de systèmes dans le monde entier pour fournir des solutions clients adaptées. Axis a été fondée en 1984 et le siège social se trouve à Lund, en Suède