psm
PROTECTION SÉCURITÉ MAGAZINE
Les Solutions pour les Professionnels de la Sûreté - Sécurité

VIDÉO-SURVEILLANCE
LA HR EST TRÈS EFFICACE POUR CERTAINES APPLICATIONS. PAS TOUTES.

n° 258
Mars Avril 2020
26 €

Entretien

PETER J. O'NEIL,
FASAE, CAE,
CHIEF EXECUTIVE OFFICER,
ASIS INTERNATIONAL
«LES ENTREPRISES PUBLIQUES ET PRIVÉES ONT COMPRIS QUE L'UNION FAISAIT LA FORCE.»

Contrôle d'accès

BIEN GÉRER SES CLÉS

Intrusion

RADIO OU FILAIRE ?
IL FAUT CHOISIR

DOSSIER

RÉGLEMENTATIONS, NORMES, CERTIFICATIONS, QUALIFICATIONS, LABELS : QUELLE UTILITÉ ?

Wiz Sense

Privilégier l'homme et le véhicule

- Intelligent, simple, intuitif
- Fournir une prédiction précise
- Permettre une réponse de dissuasion instantanée
- Offrir une recherche rapide et fiable
- Économiser le stockage tout en conservant la qualité de l'image
- Protéger la vie privée et offrir une défense contre les attaques

Séries recomandées

WizSense IPC

WizSense NVR

WizSense XVR

WizSense PTZ

WizSense Thermal

DAHUA TECHNOLOGY FRANCE
Add: 49 Rue Auguste Perret, 94000 Créteil, France
Tel : +33 (0)1 48 53 70 53
Email: sales.france@dahuatech.com
www.dahuasecurity.com

CE FC ISO 9001:2000

CONTRÔLE D'ACCÈS

Les acteurs européens du contrôle d'accès se fédèrent autour du SPAC

Les acteurs du contrôle d'accès se fédèrent autour de l'association Smart Physical Access Control (SPAC) pour créer une véritable force et puissance dans la sécurité physique et logique. Sous la présidence de STid, SPAC va représenter et défendre leurs intérêts, notamment en matière de sécurité et de normalisation.

C'est afin de promouvoir le savoir-faire européen en matière de sécurité physique et logique qu'une grande majorité d'acteurs clés du contrôle d'accès se sont regroupés sous la houlette de Stid, pour fonder l'association Smart Physical Access Control (SPAC). Pour le SPAC, les enjeux politiques, sociétaux et économiques démontrent l'importance pour l'Europe de se doter d'une organisation fédératrice des forces existantes pour apporter une réponse à la mise en place des opérateurs d'importance vitale dans le cadre de la loi de programmation militaire en France et de la directive européenne NIS (Network and Information Security) pour définir les OES (organismes de services essentiels), l'impact du RGPD et du décret de la Cnil sur l'authentification biométrique pour le contrôle d'accès physique, mais aussi la mise en œuvre de l'European CyberAct, notamment sur les nouveaux schémas de certification.

Diffuser informer, former, protéger

Dans ce contexte, SPAC a défini plusieurs missions. Tout d'abord, donner accès à des informations indispensables pour identifier une cible de sécurité à la hauteur de leurs enjeux, et permettre aux entreprises d'être indépendantes et autonomes dans la gestion de leur sécurité avec des solutions ouvertes et pérennes. L'association affiche une volonté d'assurer le rayonnement du savoir-faire français et européen dans la sécurisation des solutions de contrôle d'accès physique. Par ailleurs, SPAC entend fédérer ses membres et favoriser les échanges au sein de la profession et avec les partenaires publics et privés, défendre les intérêts des acteurs de la profession au niveau international et règlementaire, mener une veille active permettant d'identifier les technologies de rupture, et anticiper les évolutions et les menaces technologiques.

Promouvoir le protocole SSCP

SPAC va enfin porter le protocole SSCP [Smart and Secure Common Protocol] au niveau international. Ce protocole assure une communication sécurisée entre le lecteur et le système de gestion, grâce au chiffrement des données (AES-128 bits) et l'authentification mutuelle avant toute communication. Son principal atout ? Sa capacité à s'adapter à d'autres interfaces que le RS485 pour répondre à un besoin d'homogénéité (interfaces USB, TCP-IP) et de renforcement des niveaux de sécurité.
Une quinzaine d'adhérents spécialisés dans la sécurité digitale ainsi que l'Alliance pour la confiance numérique (ACN) et l'Agence nationale de la sécurité des systèmes d'information (Anssi) sont déjà membres de SPAC. D'autres partenaires vont également rejoindre l'association pour porter à l'international l'expertise européenne dans la sécurité digitale.

SPAC
Smart Physical Access Control

© DR

2 QUESTIONS À Vincent Dupart,

CEO DE STID, ET PRÉSIDENT DU SPAC

Quel est l'objectif de cette nouvelle association SPAC, Smart Physic Access Control ?
L'association est née d'une volonté de travailler sur une solution d'indépendance et d'autonomie européenne sur les questions de sécurité. En échangeant avec les acteurs de la profession, nous avons décidé de nous regrouper pour mieux faire connaître notre savoir-faire et l'importance cruciale de protéger les protocoles de communication entre les lecteurs et les systèmes. L'Anssi a été la première à certifier le protocole SSCP qui répond aux enjeux de sécurité des entreprises et des gouvernements les plus exigeants. SSCP se distingue également des initiatives américaines par sa capacité à sécuriser des interfaces USB, Ethernet, etc., ce qui permet d'apporter une homogénéité en termes de sécurité multi-applicative.

Quelles missions prioritaires vous êtes-vous fixées ?
La promotion d'une expertise française et européenne dans la sécurisation des solutions de contrôle d'accès physique. Nous allons lancer des actions de formation et d'information à destination des directeurs de sûreté pour les accompagner dans l'identification de leur cible de sécurité qui doit être la hauteur de leurs enjeux. Avec la multiplication des outils connectés en entreprise, l'attente des directeurs de sûreté est de bénéficier en toute sécurité des protocoles homogènes et interopérables. Nous avançons sur la certification du protocole SSCP qui va assurer 100 % de compatibilité entre les équipements et donc une plus grande liberté pour nos clients.

SÉCURITÉ PRIVÉE

Le Groupe Onet poursuit son développement international

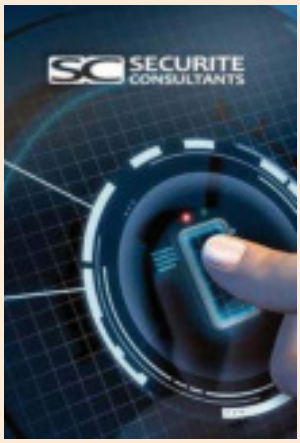
En créant Onet Luxembourg, le groupe français veut faire profiter le Grand Duché de son expertise en sécurité, tout en renforçant sa présence à l'international.

Avec la création d'Onet Security Luxembourg, le groupe Onet poursuit son développement à l'international. Onet est présent depuis quarante-deux ans dans le Grand-Duché, via ses activités de propreté. Désormais, les entreprises luxembourgeoises pourront profiter de l'offre en matière de sécurité humaine et sécurité. Onet Security leur propose d'analyser leurs besoins et risques propres, afin de concevoir et mettre en œuvre des dispositifs de sécurité, de l'audit des risques à la mise en place de la prestation.

« La confiance renouvelée de nos clients dans le secteur de la propreté nous a incité à développer une offre de services plus complète au sein du Luxembourg, explique Pascal Rogé, directeur général d'Onet Luxembourg. *Depuis plus de quarante ans, le groupe Onet a développé un savoir-faire en matière de sécurité humaine et électronique. Grâce à Onet Security, nous pourrons faire bénéficier nos futurs clients du Luxembourg de cette expertise et proposer une offre innovante en matière de sécurité humaine. »*

Onet Luxembourg proposait déjà une large gamme de services aux entreprises, allant de la propreté à la logistique en passant par la gestion des déchets. Onet Luxembourg emploie plus de 650 collaborateurs et réalise un chiffre d'affaires de 16,8 millions d'euros, auprès de plus de 350 clients.

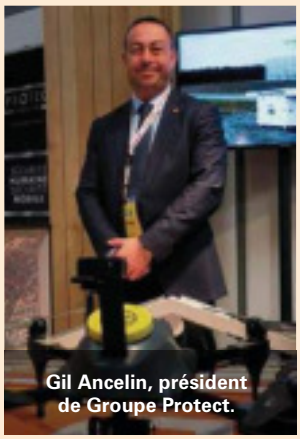
© Sécurité Consultants



© Sécurité Consultants

INTÉGRATEURS
ERYMA ACQUIERT SÉCURITÉ CONSULTANTS

Le spécialiste de la sûreté et de l'intégration de solutions IP, Eryma, vient d'acquérir Sécurité Consultants, société spécialisée dans la conception, l'installation et la maintenance de systèmes de sécurité. Basée à Issy-les-Moulineaux, Sécurité Consultants est présente aussi bien en France qu'à l'international, où elle a déployé ses offres dans une vingtaine de pays. Employant 35 collaborateurs et réalisant un chiffre d'affaires de 7 millions d'euros, cette société s'est notamment spécialisée ces dernières années dans la protection des sites sensibles. Grâce à ce rapprochement, Eryma compte accélérer le développement de ses activités à l'export, tout en consolidant ses positions en Île-de-France auprès d'une clientèle d'administrations et de grands comptes. Cette opération s'inscrit également dans l'ambition d'Eryma, filiale du groupe Sogetrel, de devenir un acteur important de la sûreté IP capable d'accompagner ses clients sur tous les territoires.
« Ce rapprochement nous permet de renforcer mutuellement nos équipes et d'enrichir considérablement l'offre de services proposée à nos clients », confirme Xavier Vignon, président de Sogetrel.



Gil Ancelin, président de Groupe Protect.

© PROTEC

PRESTATIONS DE SÉCURITÉ
PROTEC SÉCURITÉ REPREND ELYTIS

Le Groupe Protec a repris les activités de la société Elytis Sécurité, spécialisée dans la sécurité, le gardiennage et la surveillance. Grâce à cette acquisition, il renforce sa présence en Normandie et en Île-de-France à travers l'intégration de nouveaux marchés, notamment : France Télévision, la cour d'appel de Caen, le Panorama XXL de Rouen, l'hôpital d'instruction des armées, le Val-de-Grâce, et le palais de Tokyo.
Cette acquisition permet aussi à Protec Sécurité de prévoir un chiffre d'affaires supérieur à 20 millions d'euros pour l'année 2020. Gil Ancelin, président du groupe, a fait le choix de sauvegarder l'emploi de la totalité des 168 salariés de la société qui rejoignent ses 400 salariés et porte ainsi la masse salariale de la société à près de 570 salariés.
De leur côté, les deux dirigeants d'Elytis, Arnaud Demaret et Christophe Mathiot rejoignent l'encadrement de Protec Sécurité, respectivement en qualité de chargé d'affaires et de contrôleur de gestion.
À noter que Protec Sécurité a remporté de nouveaux marchés dont la date de démarrage sera fixée en cours de l'année 2020 pour un montant de près d'un million d'euros supplémentaire.

INDUSTRIES DE SÉCURITÉ

CSF Industries de sécurité : sur les rails !

Le lancement du CSF est une étape cruciale pour le développement de la filière des industries de sécurité dont les métiers sont au cœur des enjeux de souveraineté de la France.

Les représentants de la filière « Industrie de sécurité » lors de la naissance officielle du CSF, le 29 janvier dernier.

© DR

Le 29 janvier, en marge du Forum international de la cybersécurité (FIC), à Lille, Agnès Pannier-Runacher, secrétaire d'État auprès du ministre de l'Économie et des Finances, et Marc Darmon, ont donc signé le contrat stratégique de filière « Industries de sécurité ». Il s'agit d'une étape importante pour la filière et son développement car le CSF devra piloter des sujets et des projets très importants comme la sécurité des grands événements et des JO Paris 2024, la cybersécurité et sécurité de l'IOT, les problématiques d'identité numérique, etc.

© DR

« La filière des industries de sécurité est au coeur des enjeux de souveraineté de notre pays. Les acteurs à la fois publics et privés se mobilisent pour répondre aux besoins croissants de sécurité de nos concitoyens, mais aussi pour participer pleinement à l'économie numérique et devenir une vitrine pour la France à l'export. »

MARC DARMON, PRÉSIDENT DU CSF ET DU CICS, ET DG ADJOINT, SYSTÈMES D'INFORMATION ET DE COMMUNICATION SÉCURISÉS CHEZ THALES

Des rendez-vous très importants

La sécurité des grands événements est évidemment un des rendez-vous qui mobilisent le plus tous les acteurs de la filière. Et plus particulièrement la Coupe de rugby de 2023 ou les Jeux olympiques de Paris, en 2024. Ces grands événements internationaux seront – espérons-le – l'occasion de démontrer les savoir-faire des industries de la sécurité en France et la compétence des ses effectifs. Quels qu'ils soient.

Comme l'a souligné Marc Darmon, président du CSF et du CICS, et DG adjoint des systèmes d'information et de communication sécurisés chez Thales, ce contrat renforce *« les perspectives de la filière déjà forte d'une croissance de 6 % (12 % pour la cybersécurité) et concrétisant le potentiel extraordinaire des nouvelles technologies dans le domaine de la sécurité, les innovations issues de ces projets opérationnels seront clés pour la protection de l'industrie du futur, la protection du patrimoine et la souveraineté numérique française. »* Rappelons, pour mémoire, que l'industrie française de sécurité est une filière qui réalise 25 milliards d'euros de chiffre d'affaires, en grande partie à l'exportation, et est aussi la dixième filière industrielle française en termes de valeur ajoutée. Elle compte quelques grands leaders mondiaux, des ETI et des PME très innovantes qui emploient, au total, 130 000 personnes.

DRONES

Levée de 5,5 millions d'euros chez Cerbair

En quelques années, CerbAir s'est imposé comme un des spécialistes des solutions anti-drones. CerbAir assure aujourd'hui la sécurité de très belles références. Forte de ses succès, la société vient de réaliser une nouvelle levée de fonds de 5,5 millions d'euros.

© CerbAir

L'ère des drones est arrivée et l'armée n'en est plus la seule utilisatrice. Aujourd'hui, on estime qu'environ 10 millions de drones civils sont en circulation et que ce nombre – en constante hausse – va dépasser les 50 millions en 2025. Et ces drones peuvent devenir de sérieuses menaces s'ils sont utilisés à des fins de malveillance. D'autant plus qu'il est facile de se procurer des drones, à des prix abordables, et aux performances toujours plus élevées. Pour assurer la sécurité des sites à risques et lutter contre la menace venue des airs, Cerbair a développé des systèmes anti-drone fixes, mobiles, embarqués ou portables, qui peuvent détecter la présence de tout drone civil jusqu'à deux kilomètres. Une fois la menace détectée et caractérisée, les contre-mesures de brouillage peuvent immédiatement neutraliser la menace en forçant les drones à atterrir.
Depuis le début de l'année 2017, la société a commercialisé – avec succès – plusieurs solutions anti-drone, notamment auprès de forces armées (comme le ministère de la Défense, les forces aériennes colombiennes, etc.), de prisons, de sites industriels, d'aéroports internationaux, de sociétés de sécurité, etc.

Déjà 1,5 million en 2017

En décembre 2017, Cerbair avait déjà effectué une levée de fonds de 1,5 million d'euros auprès d'investisseurs comme MBDA (missilier européen représenté par Denis Gardin), Jean-Michel Aulas, par le biais de son family office Holnest, et Technofounders, le start-up studio français deep-tech qui a lancé CerbAir. Aujourd'hui, pour lever ces 5,5 nouveaux millions, CerbAir a pu compter sur la confiance de Boundary Holding, spécialiste de la cybersécurité, Aubé Management, la holding d'investissement de Nicolas Aubé, Weber Roule (holding de Christian Gueunier, cofondateur de la Financière de l'Échiquier) et Norbert Becker, serial entrepreneur luxembourgeois. MDBA coactionnaire historique de CerbAir ainsi que TF Participations (véhicule d'investissement du start-up studio Technofounders) complètent le tour de table.
Cette nouvelle levée de fonds va permettre à CerbAir d'accélérer son développement commercial, d'industrialiser sa solution portable embarquée dans un sac à dos (Manpack) et d'intégrer de nouvelles briques technologiques à sa solution.

© DR

« Notre approche modulaire nous permet de nous adapter aux besoins de clients très variés, avec un des meilleurs rapports qualité-prix du marché. Parmi nos facteurs différenciants figure notre capacité à détecter et clouer au sol un drone avant son décollage et ce, à plusieurs kilomètres de distance ! »

LUCAS LE BELL, CEO DE CERBAIR

INTRUSION

Nouvelle stratégie chez Septam

En quarante ans, le Français Septam s'est imposé comme un des spécialistes de la lutte contre l'intrusion. En 2010, la société a été rachetée par Dominique Pinault, dirigeant d'Accedia. Aujourd'hui, Septam se lance dans une nouvelle stratégie avec pour objectif de renforcer son réseau de distribution.

© DR

« *Septam est une entreprise française qui conçoit, développe et commercialise des solutions de lutte contre l'intrusion 100 % françaises. Nous mettons un point d'honneur à maîtriser toute notre chaîne de production et fabriquer français,* insiste Laurent Binon, directeur commercial de Septam. *Dans notre usine du Val-de-Reuil, dans l'Eure, nous fabriquons nos propres solutions de sécurité électronique : systèmes de lutte contre l'intrusion (centrales, transmetteurs téléphoniques) et, depuis peu, des solutions de contrôle d'accès. »*
Après son rachat par Dominique Pinault, Septam fait partie du groupe Accédia, au sein de son pôle sécurité. Accédia emploie aujourd'hui 370 personnes et réalise un chiffre d'affaires de 80 millions d'euros.
Depuis 2010, le groupe Accédia s'est engagé dans une stratégie de croissance externe en rachetant des distributeurs locaux comme TSF. Désormais, le groupe Accédia dispose de 15 points de vente en France, sous l'entité Accédia Distribution, grâce à la fusion des enseignes Septam, TSF donc, GCAS et Serié. *« Septam qui est aujourd'hui essentiellement une marque de fabricant souhaite renforcer sa présence sur le territoire national et ouvrir la distribution de ses gammes à d'autres canaux de distribution, en dehors du groupe Accédia, »* ajoute Laurent Binon. Avant de conclure : *« Mon rôle, au sein de Septam, est de développer ce nouveau réseau commercial et donc de chercher de nouveaux partenaires distributeurs, reconnus pour leur compétence, leur savoir-faire et leur professionnalisme. Avec pour objectif d'être présent chez quinze nouveaux partenaires d'ici la fin 2024. »*

© DR

2 QUESTIONS À Laurent Binon,

DIRECTEUR COMMERCIAL DE SEPTAM

Septam cherche à mettre en place de nouveaux partenariats avec des distributeurs. Quels types de professionnels recherchez-vous ?
Nous voulons nous rapprocher de professionnels de la sécurité jouissant d'un bon ancrage local et qui sont capables de respecter nos exigences en matière de qualité de prestations. C'est-à-dire qui soient à même d'apporter une assistance avant-vente aux installateurs mais aussi d'assurer auprès d'eux un SAV digne de ce nom. Ce n'est pas une question de taille mais de profil capable de s'adapter à notre vision de la relation client. Notre objectif est d'élargir ainsi notre couverture locale et de porter la marque Septam.

Avez-vous déjà trouvé quelques pépites ?
Tout à fait. Nous avons mis en place des partenariats avec Serviacom et GDV. Et nous sommes aussi en discussion avec d'autres distributeurs spécialisés courants faibles. Toujours dans un souci de proximité avec le client car la sécurité est un marché fait de relations de confiance. La proximité avec le terrain, les utilisateurs, les installateurs y joue un grand rôle.

SERRURES

Pour ses 300 ans, Picard obtient la 1re certification A2P@

Le spécialiste français de la serrurerie a pu célébrer son 300e anniversaire en décrochant la certification du CNPP Cert. pour sa solution Ermétis Tapkey.

Organisme reconnu par les professionnels de la sécurité et de l'assurance, le CNPP Cert. vient de délivrer le premier certificat A2P@ à Picard Serrures pour sa serrure connectée Ermétis Tapkey. Elle devient ainsi la 1ère serrure connectée certifiée A2P@1* en Europe. Cette certification valide les performances suivantes :
- la résistance mécanique à l'effraction de la serrure carénée multipoints Ermétis,
- la robustesse aux attaques numériques du cylindre mécatronique TapKey et de son application mobile dédiée, dont le cryptage de la communication entre les deux supports empêche tout piratage.

À noter que Picard Serrures faisait partie des entreprises sélectionnées pour représenter le savoir-faire français à *La Grande Exposition du Fabriqué en France* qui s'est tenue à l'Élysée, il y a quelques semaines. Après l'Élysée, la serrure Présence 3 de Picard Serrures va rejoindre Bercy et du le ministère de l'Économie et des Finances pour y être exposée dans le cadre de la Dixième semaine de l'industrie qui se déroulera du 30 mars au 5 avril prochains.

De gauche à droite : Fabien Hardy, ingénieur certification CNPP Cert., Julien Maliar, responsable produit serrure de Picard Serrures, Amaury Lequette, directeur CNPP Cert., Thierry Delaume, DG de Picard Serrures et Hervé Le Coq, directeur des laboratoires pôle malveillance CNPP.

© DR

© Anelec

INCENDIE
MADICOB VA EXPLOITER LA MARQUE ANELEC

Depuis 1979, Anelec, fabricant certifié NF, conçoit, produit et commercialise une gamme de matériels pour la sécurité incendie. Elle est dotée d'un savoir-faire en détection incendie, sprinkleurs (extincteurs automatiques à eau) et désenfumage. Parmi ses produits phare, Anelec propose des systèmes de détection incendie conçus pour commander le désenfumage des circulations horizontales communes des immeubles d'habitation. Ses gammes comprennent également des tableaux de détection incendie, des détecteurs autonomes, des déclencheurs, des périphériques, etc.
Cet accord va permettre au groupe AGP (Assistance générale de protection), qui rassemble plusieurs entités (Madicob, Spem, Polet, ACSI et Comtra France), dans le domaine de la sécurité incendie, et emploie une centaine de collaborateurs, de renforcer son offre produits et son positionnement en tant que spécialiste sur le marché de la lutte contre l'incendie.
Dirigé par Frédéric Anfray, le groupe, spécialisé dans la sécurité incendie et le désenfumage naturel (fabrication, mais aussi installation, maintenance, formation, etc.), a opéré dernièrement un tournant stratégique, avec pour ambition de consolider sa notoriété locale et de s'imposer comme un acteur incontournable sur le marché francilien puis national.

© SimonsVoss

CONTRÔLE D'ACCÈS
SIMONSVOSS S'ENGAGE SUR CINQ ANS DE GARANTIE AVEC SES PARTENAIRES

C'est une petite révolution dans le domaine du contrôle d'accès. SimonsVoss propose d'étendre sa garantie à cinq ans pour les partenaires revendeurs – installateurs qui intègreront son tout nouveau programme Keyless World Program Partner. *« Le marché du contrôle d'accès numérique se complexifie,* a expliqué Jean-Philippe Vuylsteke, président de SimonsVoss France. *Il y a une multitude d'intervenants, certains venant du contrôle d'accès mécanique, d'autres de l'électronique…. Pour les revendeurs, il est difficile de s'y retrouver. L'objectif de notre programme est de former les distributeurs et de renforcer leurs compétences pour pouvoir créer des marchés ensemble. En contrepartie de leur implication dans le programme, et notamment du suivi de formations annuelles et de la validation de leurs compétences, nous nous engageons sur cinq ans de garantie sur l'ensemble de nos gammes ! »*
Ce programme qui comporte trois niveaux de compétences (Technic Partner, System Partner, Network Partner), est d'ores et déjà accessible aux distributeurs-installateurs de produits SimonsVoss.

INTÉGRATEURS

En acquérant Azman, Anaveo réaffirme ses ambitions

Avec cette nouvelle acquisition – la cinquième en moins de trois ans, Anaveo continue sa stratégie de croissance organique et externe. Soutenu par Bridgepoint depuis fin 2015, le groupe confirme ainsi sa volonté de devenir un acteur référent de la sécurité électronique.

En plus de vingt ans, le groupe Anaveo s'est imposé sur le marché français de la vidéosurveillance, tout en se diversifiant sur les autres secteurs de la sécurité électronique (contrôle d'accès, anti-intrusion, détection incendie, télévidéosurveillance). Grâce à GlobalSecure, son propre logiciel de supervision (VMS) made in France, Anaveo propose une solution globale qui répond aux besoins d'une clientèle de plus en plus diversifiée (logistique, sites industriels, sièges administratifs et bureaux, concessions automobiles, etc.).
Historiquement centré sur la grande distribution et les entreprises de taille moyenne, le groupe a également souhaité se donner les moyens de ses ambitions en créant le pôle Neoxpert, dédié aux solutions de sécurité sur mesure à destination des grandes entreprises.

Croissance à deux chiffres

Créée il y a plus de dix ans par Cédric Wizman, la société Azman, basée à Maisons-Alfort (94), vend et installe des solutions de sécurité comme la vidéosurveillance, le contrôle d'accès par biométrie, des systèmes d'alarme ainsi que des défibrillateurs. Elle réalise un chiffre d'affaires de plus de 10 millions d'euros et compte une quarantaine de salariés. Spécialisée sur le segment des petits commerces et TPE grâce à une offre packagée et disposant d'un professionnalisme reconnu, la société peut compter sur une forte reconnaissance locale et sur la confiance de plus de 2 300 clients actifs et 5 000 sites équipés dont McDonald's, Biocoop, Keolis, Bazar-Chic et le MIN de Rungis.
« Ces dernières années, les solutions que nous proposons à nos clients ainsi que la qualité de notre service technique nous ont permis de conquérir de nombreuses parts de marché en Île-de-France et d'afficher une croissance à deux chiffres », souligne Cédric Wizman. Avant de conclure : *« Rejoindre le groupe Anaveo est l'opportunité de passer une nouvelle étape en développant notre offre sur le territoire national tout en bénéficiant de la dynamique d'un groupe ambitieux. »*

© DR

© DR

2 QUESTIONS À Laurent Bellot,
PRÉSIDENT DU GROUPE ANAVEO

Quel est l'objectif poursuivi par le groupe Anaveo avec l'intégration d'Azman ?
Cette nouvelle acquisition va venir compléter notre offre actuelle avec une solution packagée et un service de proximité dédiés aux segments des TPE, des petites commerces, etc. Ce modèle de location-vente est bien maîtrisé par le groupe. Notre but est également de laisser Azman se développer de manière autonome en conservant sa marque et en accompagnant le déploiement de son modèle sur tout le territoire national.

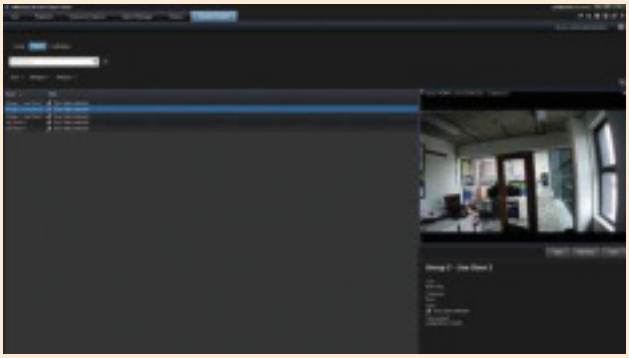
Quel bilan tirez-vous de l'année 2019 ? Quels sont vos objectifs pour les mois et les années qui viennent ?
Nos résultats pour 2019 sont excellents. Nos clients apprécient nos services et nos innovations. Nous sommes dans une belle dynamique avec une croissance à deux chiffres de notre carnet de commandes. Nous allons évidemment continuer notre stratégie de diversification clients et produits pour rester leader sur le secteur du retail et poursuivre notre fort développement sur les marchés des sites de logistique, des industries, des sites tertiaires, des collectivités locales, etc. Cela passera sans doute par d'autres opérations de croissance externe en France et l'étude d'opportunités à l'international.

CONTRÔLE D'ACCÈS

Net2 de Paxton intégré au système vidéo d'Hanwha Techwin

Désormais, les utilisateurs de Net2 peuvent visualiser instantanément des vidéos déclenchées par des événements filmés par des caméras réseau IP haute définition connectées à Wisenet Wave.

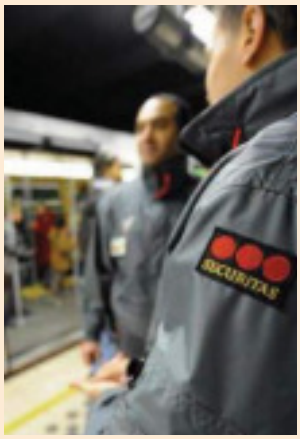
Paxton a annoncé l'intégration de son système de contrôle d'accès en réseau, Net2, au plus récent système de gestion vidéo de Hanwha Techwin, Wisenet Wave. Paxton poursuit ainsi sa politique d'intégration de son système de contrôle d'accès Net2 dans les plateformes de sécurité tierces puisque, à présent, les utilisateurs de Net2 peuvent visualiser instantanément des vidéos déclenchées par des événements filmés par des caméras réseau IP haute définition connectées à Wisenet Wave.
Disponible via un plug-in Net2 gratuit, l'intégration permet également aux utilisateurs de contrôler visuellement toute personne tentant d'accéder à un site, ainsi que de fournir une vérification vidéo des incidents d'alarme à partir du logiciel Net2 Client. Le plug-in simplifie le processus d'intégration des deux systèmes et tout en mettant à disposition des utilisateurs une interface graphique (GUI) améliorée, permettant en direct, relecture et exportation du flux des caméras de vidéosurveillance associées, directement dans l'application Net2 Client. Le plug-in prend en charge les versions 5 et 6 de Net2 et est disponible gratuitement auprès du support technique de Hanwha Techwin.



© Paxton

ROADSHOW PAXTON

Dans quelques jours, Paxton organise son Roadshow Paxton10. Les participants pourront y découvrir le tout-dernier né de la gamme du spécialiste du contrôle d'accès : le Paxton10. Les différentes étapes du Roadshow auront lieu à Paris, Lyon, Bordeaux et Rennes, entre le 10 et le 19 mars.
Pour réserver : www.paxton.info/5583



© Securitas

INDUSTRIE DE LA SÉCURITÉ

SECURITAS REJOINT LE GICAT

Le Groupement des industries françaises de défense et de sécurité terrestres et aéroterrestres (Gicat) représente les intérêts des entreprises de la défense et de la sécurité, terrestres et aéroterrestres. Ce groupement créé en 1978, compte déjà plus de 270 adhérents, avec pour objectif d'organiser le dialogue entre institutionnels et industriels du secteur, d'offrir des services à ses adhérents pour favoriser leur développement en France et à l'international, de créer un environnement favorable aux échanges entre industriels et de valoriser les savoir-faire et l'image de l'industrie du secteur. Fin 2019, il a accueilli quinze nouveaux membres dont Securitas Technologies.
Securitas est présent sur les marchés de la défense et de la sécurité terrestres et aéroterrestres en France : 30 % de son activité sont liés au secteur des sites sensibles. Il était donc logique que la société rejoigne le Gicat. Comme le confirme Laurent Zaffran, directeur commercial de Securitas Technologies : *« Participer au Gicat permettra d'échanger sur les bonnes pratiques, d'améliorer encore notre expertise client dans ce domaine pour pouvoir leur apporter des niveaux de service en phase avec leurs attentes. »*

© HAVR

CONTRÔLE D'ACCÈS

HAVR COMMERCIALISE BRIGHTLOCK : LE SUCCÈS AU RENDEZ-VOUS !

HAVR annonce la commercialisation en milieu industriel de la solution BrightLock, des clés numériques LiFi qui permettent de gérer simplement des accès, mais aussi de sécuriser les équipements. Grâce à BrightLock plus de risque de perte ou de vol, l'utilisateur peut dorénavant, via le flash du téléphone et avec l'appui de l'application et d'une plateforme Web mises à disposition, verrouiller et déverrouiller facilement les portes, partager des accès, vérifier l'état de la batterie en temps réel, visualiser les métriques (partage d'accès, journaux d'entrée, capacités de réservation, occupation des locaux et flux de personnes). Preuve de la pertinence de cette solution, Enedis a choisi BrightLock pour sécuriser ses bases opérationnelles qui contiennent du matériel sensible. BrightLock et son application de gestion permettent ainsi de contrôler les allées et venues et permettent au directeur de site d'accorder des accès à distance lors d'astreintes ou ponctuels lors de la venue de prestataires. *« La BrightLock nous permet de contrôler qui a accès au matériel sensible dans les espaces de stockage. Maintenant, il n'y a plus de disparition de matériel »*, explique Aurélien Lesage, responsable d'équipe, Enedis Picardie.

DRONES

Le NX70 de Novadem est testé par l'armée

La Direction générale de l'armement envisagerait d'acheter un millier de micro-drones pour assister l'armée lors de missions de surveillance. Une première commande d'appareils français NX70 a été passée.

© DR

À en croire un avis de marché, la Direction générale de l'armement (DGA) aurait passé commande d'au moins 2 000 micro-drones pour les cinq ans à venir. Un premier lot de 200 de machines devrait être livré aux militaires dès cette année.
La DGA a tout d'abord choisi d'acheter les modèles de nano-drones Black Hornet 3 du groupe américain Flir et le micro-drone NX70 fabriqué par l'entreprise française Novadem. Avec le NX70, l'armée de terre aura la possibilité d'explorer un terrain ennemi sans risquer de vies humaines. Pour accomplir sa mission, cet appareil pesant un petit kilo embarque une caméra de jour et d'autres capteurs thermiques (ondes de chaleur) à haute sensibilité pour rendre possible la vision nocturne.

2 000 drones

Afin d'éviter que ses données soient interceptées par de potentiels ennemis, le NX70 dispose d'une liaison chiffrée. Il ne stocke aucune information et n'a pas besoin de connexion internet pour fonctionner. Ce micro-drone est capable d'opérer dans un rayon d'action de plus de trois kilomètres, et ce pendant 45 minutes, grâce à sa batterie performante.
Le Black Hornet 3 américain peut assurer les mêmes missions de surveillance que le NX70, mais il est plus petit que son concurrent français. L'appareil mesure seulement 16 centimètres de long pour un poids plume de 33 grammes. Ses capacités sont toutefois plus limitées. La machine miniature ne peut pas dépasser 10 mètres d'altitude et son autonomie est limitée à 25 minutes. Ces deux drones devraient être testés sur le terrain lors de l'opération Barkhane au Mali, par exemple. Si les tests sont concluants, la DGA pourrait ensuite commander les 2 000 microdrones nécessaires à l'armée.

© HD

INNOVATIONS

LE BPMP CHOISIT NOVADEM

Le bataillon des marins-pompiers de Marseille (BMPM) a décidé de se doter de moyens d'appui robotisés. Et disposent désormais de drones Novadem qui viendront en appui de ses interventions.

Par ailleurs, d'ici quelques semaines, le BMPM comptera également dans ses rangs une équipe spécialisée dans l'appui robotisé qui mettra en œuvre une flotte de quatre drones Novadem.

HELLO SIGNO

La gamme signature de lecteurs
de contrôle d'accès HID Global

Rencontrez Signo sur hidglobal.com/fr/**signo**

HID

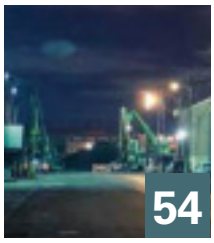
Powering **Trusted Identities**

©2020 HID Global Corporation/ASSA ABLOY AB. Tous droits réservés. HID, HID Global, le logo à brique bleue HID, le motif Chaîne et Signo sont des marques commerciales ou déposées de HID Global ou de ses détenteurs de licences / fournisseurs aux États-Unis et dans d'autres pays et ne doivent pas être utilisés sans autorisation.

psm
Protection Sécurité Magazine

Mars | Avril 2020
n°258

SOMMAIRE



3 **actus prestataires**

14 **actus sûreté**

24 **entretien**
PETER J. O'NEIL
FASAE, CAE, Chief Executive Officer, ASIS International

29 **dossier**
RÉGLEMENTATIONS, NORMES, CERTIFICATIONS, QUALIFICATIONS, LABELS : QUELLE UTILITÉ ?

40 **vidéosurveillance**
La HR est très efficace pour certaines applications. Pas toutes.

46 **contrôle d'accès**
Bien gérer ses clés

52 **focus**
Les VMS

54 **intrusion**
Radio ou filaire ? Il faut choisir

60 **incendie**
L'analyse du risque : une étape incontournable !

62 **risque**
Parc des expositions, des lieux sous haute protection

70 **quoi de neuf ?**
Que proposent les fabricants pour la sécurité et la sûreté ?

74 **c'est vous qui le dites !**
GUILLAUME FARDE, maître de conférences à Sciences Po, spécialiste des questions de sécurité

TP Media
Magazine édité par TP Media
20, rue des Petites Écuries
75010 Paris
Tél. : +33 (0)1 45 23 33 78 Fax : +33 (0)1 48 00 05 03
info@protectionsecurite-magazine.fr

Tous droits de reproduction, textes et illustrations, même partiels, sont soumis à l'accord préalable de la publication.

BIMESTRIEL DE LA SÉCURITÉ ET DE LA SÛRETÉ
Commission paritaire : 0320 T 91736
ISSN : en cours

DIRECTEUR DE LA PUBLICATION
Vincent PERROTTE
ÉDITION/DIRECTION DE LA RÉDACTION : Christophe LAPAZ
Tél. : + 33 (0)6 27 37 29 22
e-mail : cl@protectionsecurite-magazine.fr
CHEF DE RUBRIQUE : Laurence ALEMANNI
Tél. : +33 (0) 6 49 05 83 73
e-mail : la@protectionsecurite-magazine.fr
CONCEPTION GRAPHIQUE : Éric MERKI & Vincent LEVER
MAQUETTE : Vincent LEVER
SECRÉTARIAT DE RÉDACTION : Frédérique GUITTON-DANIELO
PUBLICITÉ : Jérôme PERROTTE ;
Tél. : +33 6 09 17 09 50 / + 33 (0)1 45 23 33 78
e-mail : jp@protectionsecurite-magazine.fr
DIFFUSION & MARKETING Hélène Duval - e-mail : hd@tpmedia.fr
SERVICE ABONNEMENTS PSM - TBS Blue - 6 rue d'Ouessant - 35760 St Grégoire ;
Tél. : + 33 (0)1 76 41 05 88 ; Fax : + 33 (0)1 48 00 05 03
e-mail : abopsm@tpmedia.fr
Abonnement 1 an France : 168 euros TTC
Étranger : 181 euros TTC
IMPRESSION CORLET. Zone Industrielle Ouest - Rue Maximilien-Vox - Condé-sur-Noireau. 14110 Condé-en-Normandie ;
Origine papier : Suède ; Taux de fibres recyclées : 0 % ;
Certification des fibres : PEFC ; Eutrophisation : 0,02 kg/T
CRÉDIT PHOTO COUVERTURE
V. Lever, Getty Images

ÉDITO

© DR

Dommage. Forcément dommage…

En 2023 et 2024, la France va accueillir des événements à l'audience mondiale : respectivement la Coupe du monde de rugby et les Jeux olympiques à Paris. À ces occasions, la sécurité privée, avec ses moyens humains et techniques, sera un auxiliaire précieux des forces de sécurité régaliennes. Or, comme vous pourrez le constater en lisant notre grand dossier consacré à la certification, la normalisation, la labellisation et autres démarches qualité, le monde de la sécurité ne fait pas preuve d'une appétence particulière pour la certification. Pourtant, une démarche qualité est le seul moyen, sur le long terme, d'assurer aux pouvoirs publics qu'ils ont en face d'eux des professionnels compétents, soucieux de déontologie et, donc, de confiance. Malheureusement, loin de soutenir la démarche qualité de certains, les pouvoirs publics ne donnent pas le bon exemple en raison de leur nette propension à favoriser le moins-disant. Au grand dam de certains pros qui refusent d'ores et déjà de répondre à certains appels d'offres publics, dont ceux concernant la Coupe du monde de rugby ou les JO. Dommage et dommageable…

Christophe Lapaz, directeur de la rédaction,
cl@protectionsecurite-magazine.fr

MUNICIPALES 2020

La sécurité, une préoccupation majeure des électeurs

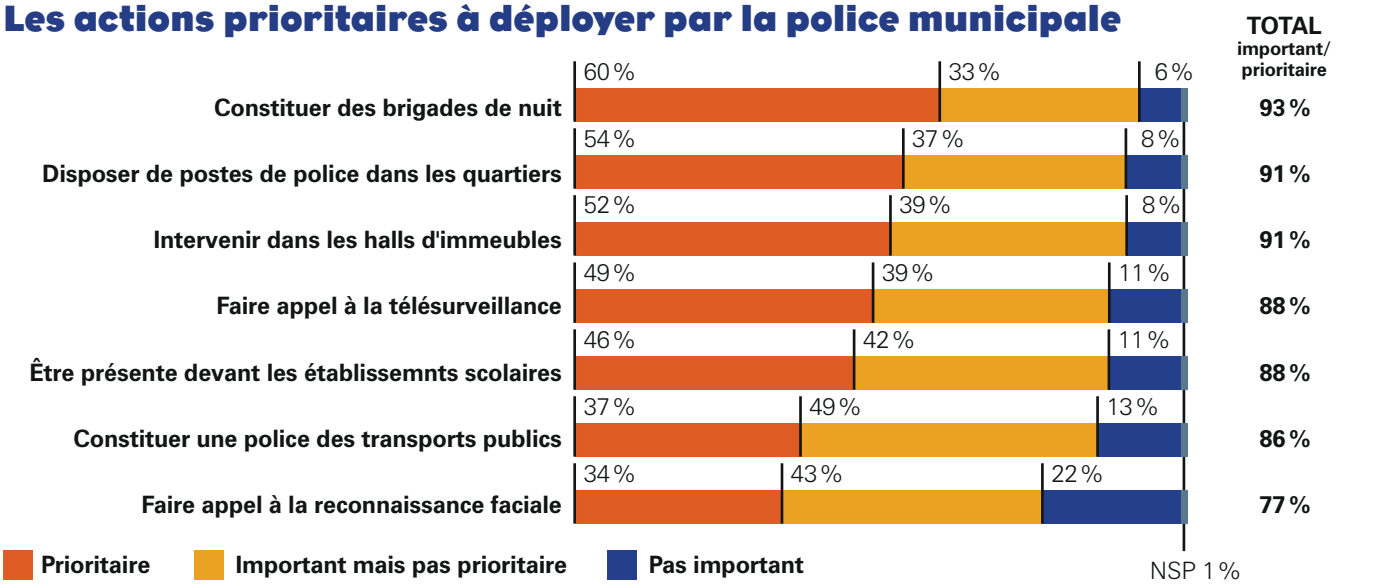
© Getty Images

Préoccupations majeures des administrés, les enjeux de sécurité locale sont au cœur des prochaines élections municipales.

La quinzième édition du « Baromètre Fiducial de la sécurité des Français », réalisé par Odoxa, analyse la satisfaction et les attentes des Français vis-à-vis des actions mises en place par les maires. Globalement, ils sont favorables à une augmentation des prérogatives et des budgets pour permettre aux maires de lutter efficacement contre l'insécurité.

Premier constat du baromètre : l'action des maires en matière de sécurité semble satisfaire les personnes interrogées. Ainsi, 61 % d'entre-elles expriment leur satisfaction à l'égard de l'action de la municipalité en matière de sécurité. Et sont particulièrement convaincues par les actions menées en matière de sécurité des écoles (74 %), de sécurité routière (63 %) et en matière d'agressions (57 %). Les démarches pour réduire les trafics (51 %), la délinquance (50 %) et les cambriolages (49 %) peinent davantage à convaincre. Cependant, en comparaison à juillet 2019, la satisfaction des Français à l'égard de leur municipalité en matière de sécurité a baissé sur l'ensemble des items.

Les actions prioritaires à déployer par la police municipale



***Source** : Baromètre Fiducial de la sécurité des Français » réalisé par Odoxa*

Nouvelles prérogatives pour les maires

Malgré la satisfaction globale exprimée, les Français estiment que le rôle du maire doit être élargi sur les questions de sécurité. Ils jugent en effet que leur élu ne dispose pas suffisamment de pouvoirs en termes de lutte contre l'insécurité et de répression (61 %).

Parmi les nouvelles prérogatives qui pourraient être confiées aux maires, les Français approuveraient très majoritairement que ces derniers aient accès à la liste des fichés S habitant dans leur commune (87 %). Après les récents événements survenus à Villejuif et à Metz, les Français sont également favorables à ce que les maires puissent avoir accès à la liste des personnes atteintes de maladies mentales et qui sont potentiellement dangereuses (79 %).

Pour lutter contre l'insécurité, les Français se prononcent pour un maintien (55 %) ou une augmentation (36 %) du budget consacré à la sécurité par leur municipalité. Les habitants de l'agglomération parisienne (41 %) et des grandes villes (44 %) sont particulièrement favorables à cette augmentation.

Moyens supplémentaires

Ces moyens supplémentaires accordés pourraient permettre de renforcer les équipements et les dispositifs de sécurité à destination des publics fragiles. La protection des femmes victimes de violences conjugales est primordiale pour les Français : 72 % jugent prioritaire la mise en place de bracelets anti-rapprochement ainsi que des places d'hébergement (67 %). Ils sont également 63 % à souhaiter la protection des personnes âgées grâce à la mise à disposition de bips à actionner en cas de danger. Ce dispositif pourrait également être déployé pour les commerçants (56 %).

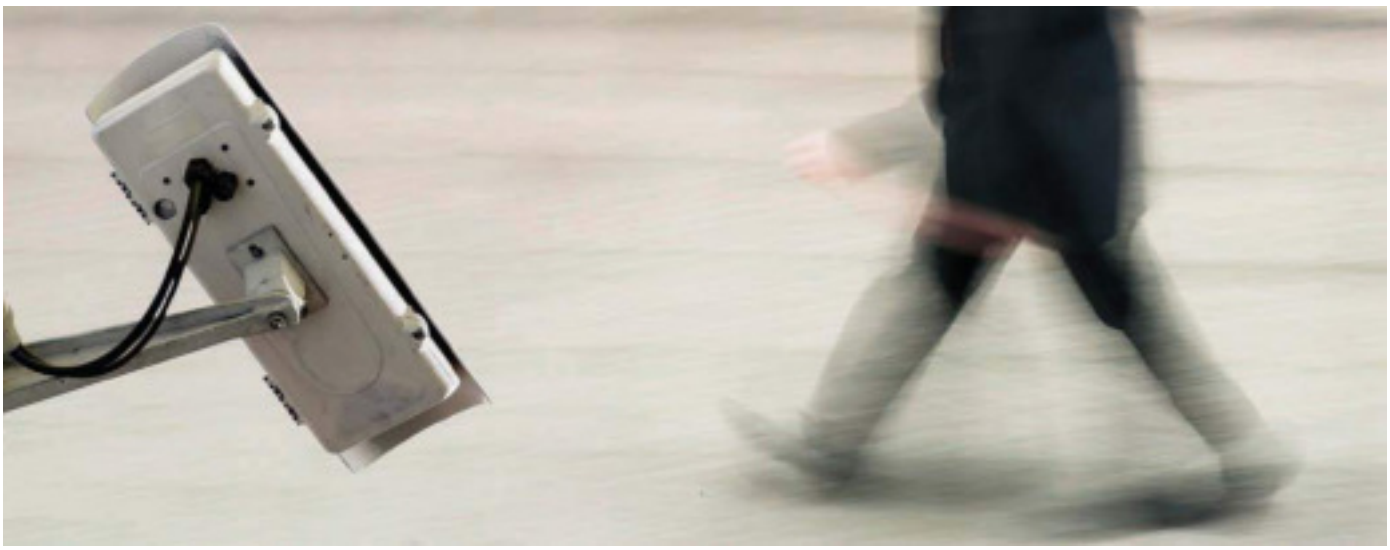
Les mesures en lien avec l'équipement de la Ville ou de la police municipale sont d'une importance plus secondaire pour les Français. Même si le principe d'un système d'éclairage qui s'intensifie au passage des piétons séduit les administrés (57 %) seul un Français sur deux juge prioritaire le développement de caméras de surveillance (49 %) et de bornes d'appel d'urgence de la police municipale (48 %), telles qu'elles ont été installées à Nice. ■

66 % POUR UNE COLLABORATION PUBLIC/PRIVÉ

Pour les personnes interrogées, la sécurité des sites publics doit résulter d'une juste collaboration entre forces de l'ordre et agents de sécurité (66 % contre 51 % en 2016). Les agents de sécurité privée pourraient : intervenir lors de fêtes communales, festivals ou événements sportifs (84 %), surveiller des sites touristiques (82 %), patrouiller dans les rues commerçantes à la demande des associations de commerçants (80 %), surveiller les alentours des établissements scolaires (78 %) ou des Ehpad (76 %).

VIDÉOSURVEILLANCE

Les villes les plus équipées de France



© Getty Images

Selon un classement publié par *La Gazette des communes,* le nombre de caméras de surveillance déployées dans les cinquante villes les plus habitées est passé, en six ans, de 4800 à 11400.

D'après le document de *La Gazette des communes,* qui classe les villes par rapport au taux de caméras* pour 100000 habitants, Nice occupe la première place du podium avec ses 2666 caméras (soit 771 caméras pour 100000 habitants), devant Nîmes, avec 411 caméras (267 pour 100000 habitants). Le haut du classement est complété par Mulhouse (Haut-Rhin), puis Annecy (Haute-Savoie) et Perpignan (Pyrénées-Orientales). Alors que Paris n'arrive que 27e avec 1400 caméras (63 pour 100000 habitants).

Par ailleurs, depuis 2013, douze villes se sont dotées d'un réseau de caméras sur la voie publique. Et si pendant longtemps les villes les plus équipées étaient des municipalités classées à droite ou au centre, parmi ces douze villes, on compte des municipalités de gauche comme Montreuil ou Lille, où huit caméras ont été installées, il y a quatre ans, dans le quartier de Wazemmes. La fin du marqueur « droite » de la vidéosurveillance ?

D'autres villes ont, montre l'étude de *La Gazette*, fortement renforcé leur installation. À l'instar de Toulouse (où le maire Jean-Luc Moudenc (LR) a fait passer le nombre de caméras de 17 à 400 pendant son mandat, et veut, en cas de réélection, en installer entre 50 et 100 de plus).

2500 projets

Selon le ministère de l'Intérieur, entre 2010 et 2017, le FIPD (Fonds interministériel de prévention de la délinquance) a permis de financer plus de 2500 projets de vidéosurveillance. Qu'il s'agisse d'extensions de réseaux, de créations de CSU ou de déploiements de nouveaux réseaux… tous ces projets auraient représenté 25000 caméras sur la voie publique, en zones de police ou de gendarmerie. Pour l'année en cours, ce ne sont pas moins de 16 millions d'euros qui sont prévus au FIPD.

À elles seules, les Bouches-du-Rhône représentent, avec 2147 caméras, 8 % des caméras financées par le FIPD. Elles sont suivies par le Nord avec 1126 caméras, la Seine-Saint-Denis (990 caméras), les Alpes-Maritimes (916), le Var (897), la Seine-et-Marne (848), l'Hérault (847), l'Oise (805), etc. ■

VILLE	PARTIS POLITIQUE	CAMÉRAS EN 2019	POUR 100000 HAB.	ÉVOLUTION 2013-2019
Nice	LR	2666	771	253,6 %
Nîmes	LR	411	267	96 %
Mulhouse	LR	265	240	159,8 %
Annecy	UDI	273	210	493,5 %
Perpignan	LR	260	210	94,0 %
Orléans	DVD	210	178	50,0 %
Argenteuil	LR	180	161	210,3 %
Toulon	LR	273	159	184,4 %
Besançon	LRM	189	157	687,5 %
Saint-Étienne	LR	271	155	238,8 %

Source : *ministère de l'Intérieur et* La Gazette des communes

** L'étude ne prend en compte que les caméras installées sur la voie publique, soumises à autorisation préfectorale. Les caméras déployées dans les bâtiments publics ou dans les transports sont exclues de l'étude.*

RÉSIDENCES UNIVERSITAIRES

Le gestionnaire Easy Student se dote d'une installation autonome

Pour gérer de manière plus sûre, efficace et fluide les accès à la résidence Saint-Côme, Easy Student a opté pour une solution de contrôle d'accès totalement autonome et sans clés.

Les logements étudiants constituent un secteur en pleine croissance et le nombre d'étudiants a augmenté de 10 % en une décennie en France. Ces dernières années, des sommes importantes ont été investies dans les logements étudiants en France. Ces résidences ont des besoins très spécifiques en matière de gestion des accès en raison des flux importants et des différents niveaux d'accès.
Pour équiper sa résidence étudiante Saint-Côme à Rennes, Easy Student, spécialisée dans la gestion et location de résidences étudiantes en France, recherchait un système de verrouillage sans clé fiable garantissant la sécurité des résidents, mais aussi flexible pour assurer une gestion des accès et non contraignante pour les gestionnaires et les prestataires, afin d'éliminer les contraintes afférentes à la gestion des clés.

83 portes et 100 badges

Pour répondre à ces exigences, Easy Student a donc opté pour la solution de contrôle d'accès autonome SMARTair de JPM. Spécialement développée pour le secteur tertiaire, sa solution de contrôle d'accès autonome SMARTair Update on Card fonctionne avec le logiciel TS1000 et garantit la sécurité des personnes et des biens. Flexible, cette solution intelligente est configurée sur-mesure pour optimiser la gestion souvent chronophage des accès des étudiants et assurer leur sécurité avant tout.
Les 83 portes de la résidence sont équipées de béquilles électroniques sans fil avec lecteurs RFID intégrés et les entrées sont sécurisées par des lecteurs muraux SMARTair. Facile à installer, cette solution s'intègre aux logements existants comme aux nouveaux bâtiments par simple remplacement du cylindre mécanique par un système sans fil. À Rennes, environ 100 badges sont actifs simultanément, et en cas de perte ou de vol, l'interface TS1000 permet de les annuler en quelques clics. Les droits d'accès d'un utilisateur sont contrôlés et modifiables en temps réel et à distance, ce qui permet d'agir rapidement en cas d'incident. Le gestionnaire programme le badge de chaque étudiant de manière à pouvoir ouvrir plusieurs portes : sa propre chambre, la porte principale et le parc à vélo 24 heures sur 24. La salle de repos commune et la laverie ne sont ouvertes qu'entre 6 h 30 et 23 h 30. ■

« SMARTair ne nécessite aucune connaissance technique particulière, le logiciel est très intuitif, ce qui m'a permis de me former très rapidement. Sa gestion simple des badges nous permet d'empêcher les allées et venues de personnes ne résidant pas ici. »

CYRIL VERGER, GESTIONNAIRE CHEZ EASY STUDENT À RENNES

© DR

SÉCURITÉ DES ENTREPRISES

Quel rôle pour les directeurs sûreté dans le continuum ?

© DR

De gauche à droite : le journaliste Dominique Rizet, Richard Lizurey, ancien DG de la gendarmerie nationale, Eduardo Cobas, secrétaire général d'Aproser, Fabien Dhainaut, coprésident du conseil national de l'Agora sécurité.

Telle était la question abordée, devant plus des 450 directeurs de la sécurité/sûreté et acteurs du marché, lors de la neuvième édition du Gala des directeurs de la sécurité qui s'est déroulé le 6 février dernier.

Partant du constat fait dans le rapport parlementaire « D'un continuum de sécurité vers une sécurité globale », remis au Premier ministre Édouard Philippe, le 11 septembre 2018, et selon lequel il est nécessaire de « conforter le rôle et le positionnement des directeurs de la sécurité dans les entreprises », dans l'objectif d'accroître la collaboration public-privé, la soirée du Gala a été marquée par une table ronde réunissant, entre autres, Richard Lizurey, ancien directeur général de la gendarmerie nationale (2016-2019) ; Eduardo Cobas, secrétaire général d'Aproser* et président du comité de dialogue social de la Confédération européenne des services de sécurité ; Fabien Dhainaut, responsable sécurité des biens et des personnes à la Caisse d'Épargne Hauts-de- France et coprésident du conseil national Agora sécurité.

Échanger et collaborer avec les services de l'État

« Échanger régulièrement et collaborer avec les différents services et représentants de la force publique, à Paris et en région, est essentiel, a expliqué Laurent Allais, président du Club Agora sécurité Paris. *Ainsi, en 2019, en lien avec l'actualité, les échanges avec les renseignements territoriaux et les forces de l'ordre se sont grandement accentués. »* Pour Fabien Dhainaut, *« ce dialogue est déterminant, la finalité étant de diminuer les taux de délinquance »* et de permettre aux entreprises de faire face à des menaces – vol à main armée, fraude ou cybercriminalité – qui nécessitent des échanges étroits et réguliers avec divers services, comme l'OCLCO, l'OCLDI, l'OCLTIC…

A contrario, l'entreprise, et tout particulièrement le directeur sécurité/sûreté, détient des informations qui peuvent s'avérer très utiles pour les forces publiques dans le cadre d'investigations.

« Nous avons porté ce message et indiqué nos attentes, au nom de l'ensemble des membres de l'Agora des directeurs sécurité, lorsque nous avons été auditionnés par les corapporteurs du groupe Partenariat et continuum de sécurité porté par le préfet Philippe Galli, dans le cadre de la rédaction du Livre blanc de la sécurité intérieure. Le directeur sécurité, donneur d'ordres de la sécurité privée, joue donc indubitablement un rôle clé du continuum, et la relation, au sein de ce continuum, doit nécessairement être tricéphale : sécurité publique/directeur sécurité/sécurité privée », a conclu Marc Viethen, directeur de la sûreté pour l'Europe du groupe Charles River Laboratories et coprésident du collège national de l'Agora des directeurs de la sécurité. ■

** Association professionnelle des compagnies de services de sécurité privee.*

2 QUESTIONS À

MARC VIETHEN

Coprésident du collège national de l'Agora des directeurs de la sécurité

© DR

Vous appelez de vos vœux à une plus grande reconnaissance du rôle des directeurs sécurité/sûreté dans le continuum de sécurité par les pouvoirs publics. D'où vient ce manque de visibilité ?

Les directeurs sécurité/sûreté ne sont pas tous égaux face à l'État et ses services. Ceux qui en sont issus entretiennent naturellement des liens avec leurs ex-collègues et ne rencontrent pas de difficultés à nouer de nouveaux contacts avec les services de police, de gendarmerie ou de renseignement dont ils connaissent bien l'organisation et les missions alors que l'établissement d'une relation de confiance, pourtant à haute valeur ajoutée réciproque, peut s'avérer parfois difficile aux cadres issus du privé. Il est donc indispensable que la fonction – et non l'origine – du directeur sécurité-sûreté soit davantage reconnue dans sa relation avec les pouvoirs publics.

Que faudrait-il faire pour que le rôle des directeurs soit reconnu, comme il devrait l'être, par l'État ?

Avec l'Agora, nous œuvrons pour la reconnaissance d'un véritable statut du directeur sécurité-sûreté qui permettrait de le rendre visible vis-à-vis de l'État. Ce statut doit passer l'organisation d'un socle de formations reconnues ou d'équivalences (VAE), via des partenariats comme ceux que nous avons déjà mis en place avec l'École des officiers de la gendarmerie nationale (MBA) ou l'École nationale supérieure de la police, et par la création de formations universitaires spécialisées de niveaux bac + 3 ou 4 permettant l'accès aux fonctions intermédiaires. Il faudrait aussi réfléchir à une forme de labellisation des directeurs sécurité-sûreté, agrément ou habilitation, qui leur permette de devenir des interlocuteurs légitimes des services de l'État afin d'échanger avec eux, en toute confiance, informations, données, etc., comme cela se fait par exemple au Royaume-Uni dans le cadre des « Information sharing agreement. »

STid Mobile ID®

ON FERME ENCORE MIEUX SES ACCÈS AVEC UN SYSTÈME

OUVERT

STid Mobile ID® est la seule plateforme ouverte au monde :
Avec son hébergement chez vous « on premise » ou chez nous*,
la plateforme répond aux politiques de sécurité les plus exigeantes.
STid vous offre également l'ensemble des interfaces de
programmation (API) permettant d'intégrer simplement
les fonctions STid Mobile ID® à votre écosystème.

11 Awards

www.stid-security.com

* ISO27001 / HDS / PCI DSS

SECURITY & SAFETY MEETINGS

REJOIGNEZ-NOUS
STAND J09

CANNES
DU 17 AU 19 MARS

STid

AÉROPORTS

Des nouvelles technologies pas si rapides que ça

Les systèmes de contrôles automatiques utilisés dans les aéroports pour faciliter les passages aux frontières des passagers ne font pas l'unanimité.

© DR

Raison du mécontentement : les temps d'attente interminables au passage des frontières qui parfois atteignent 90 minutes. Alors que dans la plupart des aéroports étrangers le recours aux solutions digitales et aux moyens de passage automatisés ont permis de rendre plus fluide les contrôles de police…
Il semblerait que le responsable soit le sas Parafe (Passage automatisé rapide des frontières extérieures), système de contrôle d'identité biométrique.
Petit rappel historique. En 2016, face à l'incapacité des pouvoirs publics de trancher quant au financement des sas, le patron d'ADP, Augustin de Romanet, avait décidé qu'ADP financerait lesdits sas. Mais, comme le souligne notre confrère *Le Figaro* dans un article du 17 janvier 2020, *« entre-temps, l'identification par empreintes digitales sur laquelle reposaient ces appareils avait montré ses limites. Les pouvoirs publics imposèrent alors un système par reconnaissance faciale, et il fallut moderniser cette première batterie d'appareils. ADP lança alors un appel d'offres, remporté par la société Gemalto. Leurs appareils n'étaient sans doute pas les plus performants mais ils étaient parmi les moins chers. »*

Imbroglio

Les problèmes viennent de là. ADP se retrouve avec des sas aux technologies mixtes – digitales et physio – et fournis par des fabricants différents. Pourquoi faire simple quand on peut faire compliquer ? D'autant plus que ce type de matériel n'est pas aussi simple à utiliser qu'on le croit… On se retrouve donc face à des situations où un passeport fonctionne sur un sas et pas sur l'autre. À ces problèmes techniques, s'ajoutent certaines réticences des syndicats de police qui voient dans ces systèmes automatiques de contrôle un frein à l'embauche. Les syndicats ont donc réussi à imposer le recours à un fonctionnaire de police pour cinq sas contre un seul policier pour dix sas en Belgique ou en Angleterre. Et bien qu'ADP soit propriétaire des sas, leur utilisation est confiée à la PAF (police des frontières)… Et quand il manque des fonctionnaires de police, certains sas sont fermés… ■

OUTILS

Le pro le plus proche de chez vous grâce à l'Annuaire sécurité & sureté de PSM !

Grâce à l'annuaire online de votre magazine *PSM* (www.annuaire-securite.fr), vous pouvez retrouver tous les prestataires dont vous pouvez avoir besoin : installateurs, intégrateurs, fabricants, distributeurs, prestataires de services…
Par secteur d'activé, catégorie de produits, région, département, localisez rapidement et facilement tous les professionnels près de chez vous. ■

→ **www.annuaire-securite.fr**

CONTRÔLE D'ACCÈS

La FDJ choisit Assa Abloy

Pour assurer le contrôle d'accès de ses six sites majeurs répartis en France, la Française des jeux (FDJ) va déployer 400 serrures électriques Abloy.

En effet, à l'occasion de l'aménagement de son nouveau siège social, un site de 25 000 m² qui regroupe sur les bords de Seine 1 200 salariés, l'opérateur de jeux a souhaité mettre en œuvre un système de management de la sûreté. L'objectif : revoir entièrement, sur une période de cinq ans initiée en 2017, l'architecture sûreté de ses locaux principaux répartis en France, du contrôle d'accès au système de vidéosurveillance, afin d'augmenter leur niveau de sécurité. *« Nous recherchions un partenaire reconnu, avec de nombreuses références, proposant des produits robustes supportant une forte densité de passage et une polyvalence adaptée à de multiples typologies de portes »*, explique Nicolas Brunet, responsable sûreté du groupe FDJ.
« Dans le cadre de ce contrat, Abloy a non seulement travaillé en direct avec la FDJ, mais aussi avec le bureau d'études. Cela nous a permis, d'une part, d'accompagner le bureau d'études en matière de prescriptions techniques des solutions et, d'autre part, de confronter les solutions choisies avec la réalité terrain, explique Franck Lefebvre, directeur commercial chez Abloy. *La FDJ recherchait en effet des solutions techniques, esthétiques, pérennes et robustes, dotées d'un système de reverrouillage automatique pour qu'une fois claquée, la porte soit bien verrouillée ; tout en étant capable de remonter de l'information embarquée sur l'état de portes. »*

500 portes

Pour assurer un verrouillage haute sécurité, le choix s'est donc porté sur Abloy et son offre de serrures électriques, à contrôle de béquille ou motorisées. Ces solutions, qui allient haute résistance mécanique et faible consommation d'énergie, permettent d'équiper des portes à fort passage et de garantir un filtrage efficace dans des locaux sensibles sous contrôle d'accès. Elles permettent en outre de sécuriser des locaux aussi variés que des portes palières à haute densité de passage, des bureaux, des locaux techniques, des datacenters... 150 portes ont ainsi été équipées en 2019 au sein du siège social. Au final, 500 portes le seront sur l'ensemble des sites courant 2020.
« Après un an d'utilisation des serrures électriques Abloy, le constat est très clair. Ces serrures électriques et leur efficience nous apportent une grande sérénité dans l'exploitation de nos sept sites majeurs nationaux », conclut Nicolas Brunet. ■

ABLOY, UNE GAMME COMPLÈTE

Abloy propose une offre très large de serrures électriques où motorisées parmi lesquelles :
- la serrure électromécanique avec lecteur RFID intégré Aperio L100.
- Protec² Cliq, système de contrôle d'accès avec double sécurité mécanique et électronique pour sécuriser des accès sensibles.

Le nouveau siège de la Française des jeux est un des sites équipés avec les serrures Abloy.

© DR

2 QUESTIONS À NICOLAS BRUNET

Responsable sûreté du groupe FDJ

© DR

Dans quel contexte s'inscrit le déploiement des solutions Abloy dans vos différents sites, dont votre siège social ?
Le groupe Française des jeux souhaitait uniformiser la sécurité des ses 38 sites implantés en France (6 sites en Île-de-France et 32 agences en régions) C'est pour cela que le groupe a lancé un grand plan de modernisation de son contrôle d'accès sur cinq ans avec pour date butoir 2022. Ce projet représente plusieurs centaines de serrures – 400 pour Paris et sa région – qui seront toutes fournies par Abloy.

Quel élément vous a convaincu de choisir Abloy ?
Leur capacité à nous accompagner, à nous aider dans le choix des solutions adaptées à nos contraintes a grandement joué en leur faveur. Parallèlement, Abloy nous a permis de tester ses serrures. Ils ont aussi su adapter leurs solutions à la typicité de certaines de nos agences.

CONTRÔLE D'ACCÈS

Enedis retient Dény Security

Pour protéger la population du risque incendie ou explosion d'un de ses postes sources implanté en plein milieu urbain, à Saint-Herblain, Enedis a choisi les serrures multipoints anti-souffle de Dény Security installées sur les bloc-portes Doortal. En effet, compte tenu de leur localisation en zone urbaine et pour des raisons de sécurité, les transformateurs sont enfermés dans des loges en béton. Conformément au cahier des charges, l'intégralité du poste source dispose également de portes anti-souffle qu'Enedis souhaitait sécuriser tout en conservant son organigramme mécanique existant réalisé avec des cylindres ronds Dény. Grâce à son partenariat avec Doortal, un spécialiste des portes métalliques techniques pour lieux publics et sites sensibles, le spécialiste français de la serrure a pu répondre aux exigences de son client. Le site de Saint Herblain est désormais équipé de six bloc-portes simple vantail et trois bloc-portes double vantaux coupe-feu et acoustiques 40 dB sur lesquels sont installées les serrures en applique trois points à sortie libre de Dény. L'ensemble porte Nexus et serrure garantit au poste source électrique Enedis de Saint-Herblain une résistance de deux heures en cas d'incendie et 2 tonnes/m². ■

© DR

VIDÉOSURVEILLANCE

Un cadeau empoisonné pour Valenciennes ?

© DR

La Ville de Valenciennes s'est vu offrir par le géant de l'électronique chinois Huawei, 240 caméras de surveillance. Un « cadeau » estimé à deux millions d'euros. Ce « cadeau », donc, que certains qualifient d'empoisonné suscite quelques inquiétudes… même si les riverains reconnaissent l'utilité des caméras afin de sécuriser l'espace public. Pourquoi cette inquiétude ? D'abord parce que ce geste, gratuit, suppose un intérêt caché pour Huawei. L'absence de contrepartie demandée par le géant chinois cacherait des intentions malintentionnées… Ensuite, parce que ces caméras sont dotées d'un système de reconnaissance faciale. Et, même si le maire de Valenciennes, Laurent Degallaix, insiste sur le fait que cette fonction n'est pas utilisée à Valenciennes, la reconnaissance faciale est très loin d'avoir bonne presse en France. Par ailleurs, on n'ignore les relations étroites – pour ne pas dire intimes – qu'entretient Huawei avec le gouvernement chinois. Risque d'espionnage ? De détournements de certaines données ? On ne saurait trancher. Toujours est-il que depuis l'installation de ces caméras, les services de renseignements de la DGSI se sont déplacés quatre fois à Valenciennes… ■

SÉCURITÉ-SÛRETÉ

Ne manquez pas Security/Safety & Prevention Meetings

Les spécialistes de la sécurité-sûreté des entreprises ont rendez-vous à Cannes dans quelques jours. En effet, du 17 au 19 mars prochains, au Palais des congrès et au Palais des festivals, se déroulera l'édition 2020 du Salon de la sûreté, de la sécurité et de la prévention. Au programme cette année, des débats, entre autres, sur les thèmes suivants :
- Protection périmétrique efficace et durable
- Comment va s'organiser la sécurité des Jeux olympiques de 2024 ?

→ **Inscriptions :** https://matchmaking.weyou-group.com/securitymeetings/2020/top-decideur
www.security-and-safety-meetings.com/

Carnet

HID GLOBAL

BJÖRN LIDEFELT

© DR

HID Global a annoncé la nomination de Björn Lidefelt en tant que président et CEO. Björn Lidefelt a rejoint la société HID Global après avoir occupé le poste de Chief Commercial Officer (CCO) chez Assa Abloy, maison mère de HID, où il a supervisé l'image de marque, la communication, le développement commercial et la stratégie.

TIL TECHNOLOGIES

OLIVIER REYRE

© DR

Olivier Reyre a été nommé au poste de directeur général de Til Technologies France. Diplômé des Arts et Métiers, Olivier Reyre a rejoint Til en 2005 après cinq années dans la conception de logiciels au sein d'une société de conseil. Il a pour mission d'assurer la croissance et la pérennité de Til et pour ambition d'en faire le leader français du contrôle d'accès.

ARD

FRANÇOIS FOULON

© DR

ARD, un des leaders français du contrôle d'accès et de la monétique, et membre du groupe Vitaprotech, annonce l'arrivée de François Foulon au poste de directeur général. Il remplace, à ce poste, Frédéric Spagnou.

ASIS FRANCE

GABRIEL GEDDA

© DR

Gabriel Gedda est le nouveau président du chapitre français d'ASIS International. Il remplace Éric Davoine. Gabriel Gedda occupe actuellement les fonctions de Regional Security Advisor France & SW Europe chez Microsoft (EDP).

GROUPE ANAVEO

LAURENT BELLOT

© DR

Laurent est le nouveau président du groupe Anaveo. Ingénieur et MBA executive EM Lyon, il a, entre autres, accompli une partie de sa carrière dans les secteurs de l'informatique et des télécommunications chez l'intégrateur réseaux Alcatel et SFR business.

Agenda

MARS 2020

Security/Safety Prevention Meetings
Du 17 au 19 mars 2020 – Cannes
www.security-and-safety-meetings.com

Roadshow Paxton10
Le 17 mars – Bordeaux
www.paxton.info/5583

Roadshow Paxton10
Le 19 mars – Rennes
www.paxton.info/5583

1res rencontres de l'Anitec
Du 25 au 26 mars 2020 – Marseille
https://www.anitec.fr/

Mutualisation des dispositifs de sûreté
Le 31 mars 2020 – Paris
https://an2v.org/reunions-thematiques/

MAI 2020

Ifsec
Du 19 au 21 mai 2020 – Londres
www.ifsec.events/international/

Préventica Nord
Du 26 au 28 mai 2020 – Douai
https://www.preventica.com

SEPTEMBRE 2020

Trophées de la sécurité
Le 28 septembre 2020 – Paris
www.tropheesdelasecurite.fr/

Préventica Lyon
Du 29 septembre au 1 octobre 2020 – Lyon
www.preventica.com

NOVEMBRE 2020

Expoprotection
Du 3 au 5 novembre 2020 – Paris
www.expoprotection.com/

ALAJI SAS recherche un

Responsable formation sécurité H/F

RÔLE Encadrement des formations sécurité, coordination des dispositifs sécurité.
- Posséder un diplôme SSIAP et des attestations de recyclage correspondantes
- Posséder une attestation de formation de formateurs Moniteur SST.

DISPOSER
- Soit de 2 années d'exercice professionnel dans le domaine de l'activité concernée ou dans le domaine de la sécurité publique ainsi qu'une attestation de formation en tant que formateur.
- Soit de 2 années d'exercice professionnel dans la formation aux activités privées de sécurité ou dans le domaine de la sécurité publique ainsi que du certificat de qualification professionnelle ou d'une certification professionnelle enregistrée au RNCP, de niveau IV minimum, relatif à l'activité concernée.

PROFIL Diplômes impératifs : MONITEUR SST, SSIAP3, un diplôme dans la sécurité serait un plus. Expérience dans la formation de 3 ans.

SALAIRE 2500 euros brut mensuel à négocier selon expérience

Candidature à envoyer à l'adresse ci-dessous :
candidature@alaji.fr

PETER J. O'NEIL,

FASAE, CAE, Chief Executive Officer, ASIS International

« Les entreprises publiques et privées ont compris que l'union faisait la force. »

© DR

Pour *PSM*, Peter O'Neil revient sur le rôle d'ASIS et nous expose sa vision d'une approche globale de sûreté des entreprises et organisations. Ce qui suppose aussi de collaborer avec les autres organisations professionnelles. Françaises inclues.

Pouvez-vous nous présenter l'organisation ASIS International ?
Fondée en 1955, ASIS International est une organisation professionnelle mondiale qui représente 34 000 professionnels de la gestion de la sécurité. ASIS, c'est aussi quatre certificats professionnels que nous offrons aux professionnels de la sécurité, en fonction de leur expérience. Nos quatre certificats sont : le CPP Certified Protection Professional (CPP) considéré comme le « Gold Standard » pour les professionnels de la gestion de la sécurité ; le Professional Certified Investigator (PCI) permet à une personne de démontrer ses connaissances et son expérience en matière de gestion de cas, de collecte de preuves et de préparation de rapports et de témoignages pour étayer les conclusions ; le Physical Security

Professional (PSP) démontre vos connaissances en matière d'évaluations de la sécurité physique, d'application, de conception et d'intégration des systèmes de sécurité physique ; l'Associate Protection Professional (APP), le premier échelon de nos certifications. Ces certificats certifient une personne, et non une entreprise. Des informations détaillées sur les certificats et les conditions d'admissibilités que l'on doit remplir pour les examens peuvent être trouvées sur www.asisonline.org/certification/asis-board-certifications2/. ASIS International, dans son rôle d'une organisation de développement de normes – Standard Developing Organizations (SDO), établit les normes et directives pour répondre aux besoins des professionnels de la sécurité, en jouant un rôle essentiel pour influencer les normes de sécurité dans le monde entier.

« Les compétences en communication, le sens des affaires et le leadership sont devenus de plus en plus importants pour les directeurs sûreté. »

Quelles sont les questions urgentes sur lesquels les membres d'ASIS travaillent actuellement ?

Nos membres travaillent sur des sujets variés. La gestion des risques liés à la sécurité des entreprises. Citons aussi la problématique des drones ou comment se préparer aux opportunités, menaces et défis que représentent les drones ? Le devoir de diligence – adresser les questions éthiques et juridiques indispensables au soin du personnel lorsqu'il est en voyage d'affaires. La gestion des risques et la résilience pour que la mentalité de gestion de la sécurité soit présente lorsque les entreprises évaluent les risques et élaborent des plans de résilience. Et, enfin, la gestion des crises et continuité des opérations : promotion des normes de résilience organisationnelle et des Best Practices dans le monde.

En France, il existe plusieurs associations professionnelles de la sécurité/directeur de sécurité (Agora, CDSE, etc.), quels liens avez-vous avec elles ?

ASIS International croit qu'il est impératif que les organisations dans le monde collaborent afin de faire progresser la profession de gestion de la sécurité. Nous cherchons à établir des partenariats avec l'Agora, le CDSE et toute autre organisation où il y a un bénéfice mutuel. Nous avons les mêmes missions... protéger les personnes, les biens et les communautés. Ensemble, nous pouvons faire plus.
En 2019, ASIS International a annoncé un nouveau partenariat stratégique avec l'École des officiers de la gendarmerie nationale, permettant à deux membres de ASIS de s'inscrire au prestigieux programme du MBA de gestion de la sécurité. L'accord facilite également la collaboration pour le développement de futurs modules éducatifs sur la base d'une vision partagée et sur la nécessité de mettre en commun connaissances et ressources pour promouvoir la sécurité en tant que fonction stratégique au sein des organisations.

Ces dernières années, le travail et les missions de la sécurité/directeurs de la sécurité ont beaucoup changé. Selon vous, quels sont les changements majeurs ?

Les changements majeurs que nous observons ces dernières années sont la nécessité pour les experts en sécurité physique de comprendre les risques liés aux cybertechnologies et aux experts en cyber de mieux comprendre les risques liés à la sécurité physique. En plus de cela, nous observons aussi que les compétences en communication, le sens des affaires et les solides compétences générales en leadership sont devenus de plus en plus importants. Pouvoir comprendre et expliquer aux dirigeants les risques associés à la gestion des opérations des organisations et positionner la sécurité comme un « atout commercial » est d'une importance primordiale.

En France, on parle beaucoup de sécurité continue (la collaboration entre les forces de l'État et le secteur privé), aussi connue sous le nom de continuum de sécurité. Est-ce une collaboration qui existe ailleurs ?

Oui. Nous voyons ce continuum de sécurité être adopté à travers le monde. Les États-Unis, l'Europe, Israël et ● ● ●

BIO EXPRESS

2006 Fellow d'ASAE, une association créée en 1920 et regroupant 46 000 dirigeants d'associations de 7 400 organisations
2008 CEO d'AIHA, une organisation professionnelle représentant 10 000 experts dans les domaines de la santé et la sécurité au travail
2016 CEO d'ASIS International
2019 70e lauréat du Key Award, la plus haute récompense des dirigeants d'associations professionnelles ■

PETER J. O'NEIL,

FASAE, CAE, Chief Executive Officer, ASIS International

« Nous cherchons à établir des partenariats avec Agora, CDSE et toute autre organisation où il y a un bénéfice mutuel. »

© DR

ASIS INTERNATIONAL EN BREF

- Une organisation professionnelle fondée en 1955
- 34 000 membres professionnels de la gestion de la sécurité
- Quatre certifications reconnues pour les cadres de la sécurité-sûreté dans les entreprises et organisations : Certified Protection Professional (CPP), Professional Certified Investigator (PCI), Physical Security Professional (PSP), Associate Protection Professional (APP).

● ● ● le Moyen-Orient viennent à l'esprit. Après la tragédie du 11 septembre aux États-Unis, ainsi que les attaques de type similaire en France, en Allemagne, au Royaume-Uni, etc., les entreprises publiques et privées ont compris que l'union faisait la force. C'est ainsi que la mise en pratique de ce continuum de sécurité a commencé à prendre forme.

Quelles sont les plus grandes menaces auxquelles les entreprises/organisations sont exposées ?

En général, les menaces internes sont et demeurent un aspect constant de la gestion qui doit être pris en considération, ainsi que les plans de continuité/résilience des opérations. De plus, comme mentionnée déjà, l'aptitude du professionnel de la gestion de la sécurité de comprendre la mission et la vision de l'entreprise, et d'être considérée comme un atout, est également essentielle.

Les cybermenaces sont des risques qui ne peuvent plus être ignorées. Cela devra inclure une meilleure collaboration entre les directeurs de la sécurité et de la sureté et des IT. Ces entités sont-elles prêtes pour ce partenariat ?

Le conseil d'administration de ASIS International a officiellement adopté la notion de gestion des risques pour la sécurité des entreprises (CESM) comme moyen d'assurer une meilleure collaboration entre et parmi tous les acteurs de la gestion de la sécurité, qu'elle soit physique ou cyber. Nous continuons à concevoir des produits, des services et des outils pour soutenir cette philosophie de gestion. En fin de compte, le risque est le risque, et l'évaluation des risques reste l'évaluation des risques. Certaines entreprises adoptent volontiers cette idée, d'autres non. Mais avec le temps, nous croyons que les organisations finiront par adopter cette philosophie.

Dans le contexte actuel, la sécurité des infrastructures clés de l'État, des citoyens... est un problème majeur. Allons-nous vers une surveillance généralisée de tous ? Quelles limites devraient être imposées aux entreprises publiques et privées dans le cadre d'une surveillance légale de leur environnement ?

Ceci est une question multidimensionnelle et un peu difficile à traiter dans ce cadre. En général, oui, le monde avance vers une surveillance plus généralisée. Il y a des différences culturelles, juridiques et réglementaires entre et parmi les pays qui adoptent cette approche de la gestion de la sécurité qui protège les communautés et les citoyens. Les limites pour chaque pays doivent être normalisées à ce qui est « localement » acceptable. Le temps et les gens détermineront où se trouvent ces limites.

Qu'est ce qui différencie ASIS en tant qu'association ?

Notre gouvernance. Avec 34 000 membres dans 140 pays, ASIS s'est engagée vers un modèle de gouvernance mondiale inclusif. Les membres participent au comité de nomination et la représentation au conseil d'administration est en train d'être étendue. Un autre élément clé du succès d'ASIS est la rotation des bénévoles imposant des termes limites de mandat. Cela permet d'apporter continuellement de nouvelles idées, de nouvelles façons de relever les défis persistants. Cela aide à établir en profondeur des contacts mondiaux. Godfried Hendriks, CPP, président 2020 et originaire des Pays-Bas, s'est engagé à faire progresser notre gouvernance mondiale dans le but de mieux représenter les besoins de nos membres. ■

IPS

Intelligent Video Analytics

IPS OUTDOOR DETECTION

Intelligent Video Analytics Software

L'analyse vidéo la plus fiable pour la sécurité périmétrique des organismes d'intérêt vital (OIV)

IPS Outdoor Detection vous avertit en temps réel et avec une haute fiabilité lorsque des personnes ou des objets pénètrent dans une zone sécurisée.

IPS Outdoor Detection permet une protection périmétrique très fiable même dans le brouillard, par fortes pluies et chutes de neige.

La détection précoce d'une intrusion raccourcit considérablement les délais pour l'endiguer ou en limiter les dégâts.

Securiton GmbH
IPS Intelligent Video Analytics
www.ips-analytics.com

deister electronic

Infinity Readers™

Infinity et bien au-delà

Le lecteur qui répond déjà à vos besoins futurs

La gamme de lecteurs INFINITY, première gamme de lecteurs qui évoluent au même rythme que les nouvelles technologies.

- Multi-technologies et Multi-fréquences 125kHz, 13,56MHz et Bluetooth
- Évolutivité technologique par adjonction de module complémentaire
- OSDP et Wiegand simultanés sans action de reprogrammation

DURABLE

PÉRENNE IDENTIFICATION EFFICACE ÉVOLUTIF

ADAPTABLE INFINITY SOUPLE

SÉCURISÉ PERFORMANT

ÉVOLUTIF

FLEXIBLE RFID ELEGANT POLYVALENT

STABLE

www.fr.deister.com

dossier

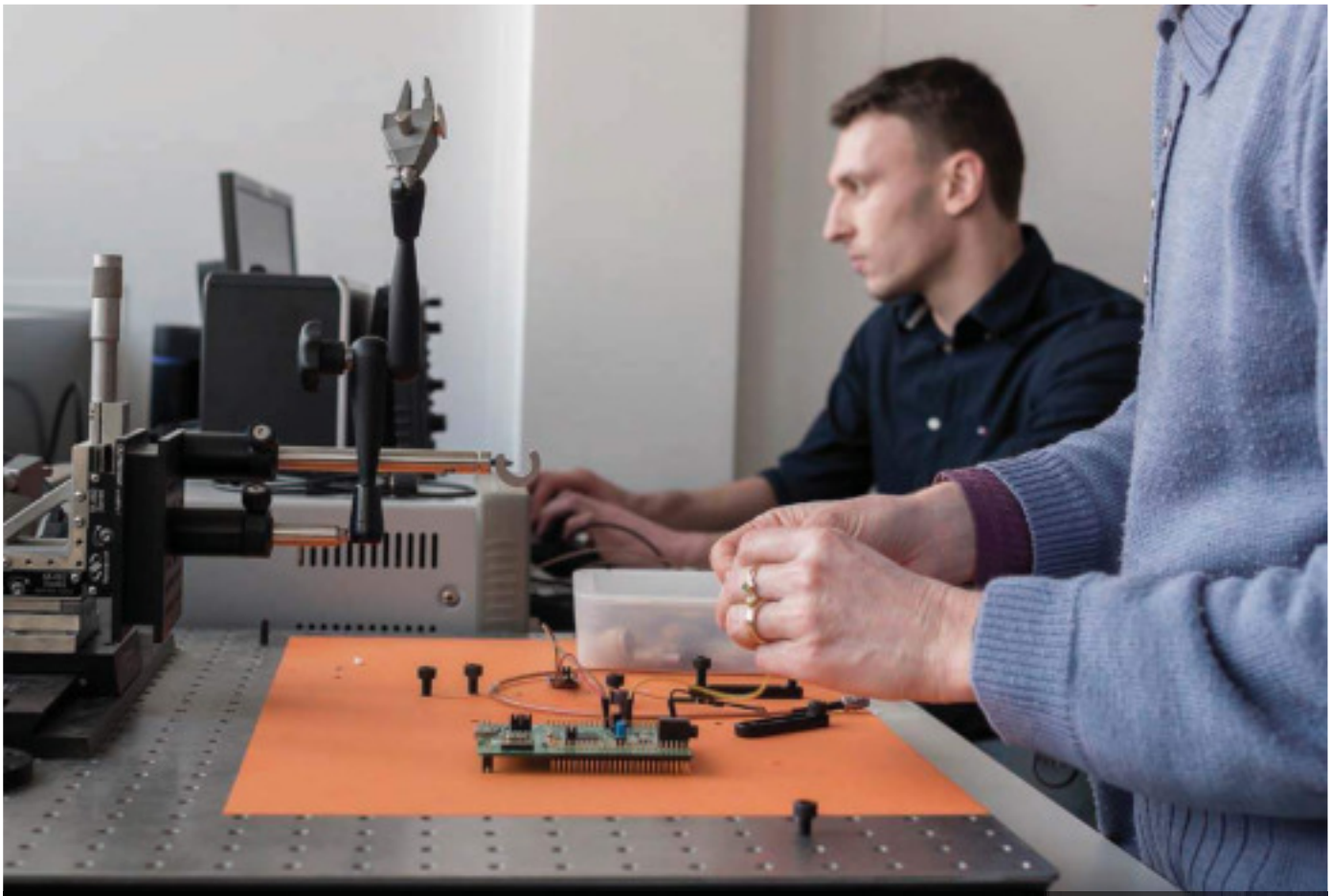
Réglementations, normes, certifications, qualifications, labels : quelle utilité ?

Si certains professionnels de la sécurité s'engagent dans une démarche certification, c'est loin d'être le cas du plus grand nombre. Or, la certification qui prouve une démarche qualité est tout sauf inutile.

© Getty Images

SOMMAIRE

→ La certification : un vrai facteur différenciant 30
→ Sécurité privée et certification : peut mieux faire 34
→ Directeurs sûreté : la certification pour quoi faire ? 38



Les experts de l'Anssi testent la robustesse des matériels en matière de cybersécurité en vue de leur accorder ou pas la certification Anssi.

© DR

La certification : un vrai facteur différenciant pour les fabricants

Bien que de plus en plus de fabricants de systèmes de sécurité électronique ou autres s'engagent, volontairement, dans une démarche de certification par une tierce partie, ce n'est pas encore une généralité. Or, cette certification, imposée ou pas, constitue pour bon nombre de donneurs un facteur différenciant.

« *À l'inverse du monde de la sécurité incendie qui jouit d'une forte culture de la certification qui est devenue un réflexe, le monde de la sécurité électronique ou physique n'a pas encore adopté le même réflexe avec les certifications existantes. Mais la cybersécurité constitue actuellement un enjeu majeur pour lequel la certification est un passeport de confiance,* souligne Amaury Lequette, directeur de CNPP Cert. Avant d'ajouter : *« En effet, si pour certaines gammes de solutions, comme le contrôle d'accès sous l'influence de l'Anssi, les choses bougent, pour le reste des solutions électroniques comme la vidéosurveillance, les fabricants commencent seulement à*

© DR

« Notre démarche qualité rassure nos partenaires. »

CÉLINE STEIN, CEO PROGRAM ASSOCIATE CHEZ SIEMENS

s'intéresser à la certification. La particularité étant, dans ce cas, le caractère volontaire de la certification. Or, dans le contexte actuel, et compte tenu des menaces que font peser sur les systèmes leur connexion aux réseaux, la certification est, non seulement, un bon moyen de rassurer les donneurs d'ordres, mais aussi de permettre aux installateurs de remplir au mieux leur devoir de conseil. »

De son côté, l'Agence nationale de la sécurité des systèmes d'information a fourni un gros travail pour inciter les fabricants à intégrer ses recommandations en matière de cybersécurité. *« L'Anssi qui est raccrochée au Premier ministre, via le secrétariat général de la Défense et de la Sécurité nationale (SGDSN), "chapeaute" la sécurité des administrations, des OIV ou opérateurs d'importance vitale et des OSE ou opérateurs de services essentiels,* rappelle Vivien Mura, chef du bureau politique industrielle et assistance de l'Anssi. *L'agence assume plusieurs missions : la défense afin de réagir en cas d'attaque informatique contre nos systèmes d'information ; la prévention en étant capable d'analyser les menaces et les risques afin de s'y préparer et élever le niveau de sécurité général ; l'information et la sensibilisation afin de partager sa doctrine cybersécurité avec le plus grand nombre d'acteurs concernés. C'est dans le cadre de ces missions que l'Anssi a défini certaines règles et exigences en matière de cybersécurité. »*

CÔTÉ CERTIFICATEUR

VIVIEN MURA

Chef du bureau politique industrielle et assistance de l'Anssi

« LA CYBERSÉCURITÉ EST UN ENJEU POUR TOUTES LES ENTREPRISES. »

« La cybersécurité est l'affaire de tous. Et non du seul ressort des concepteurs de produits de sécurité informatique comme les fabricants de pare-feu. C'est pourquoi l'Anssi a élaboré des exigences précises en matière de cybersécurité et dont la prise en compte permet d'obtenir soit la certification Anssi au sens de "certification délivrée par l'Anssi", soit la qualification Anssi. Elles ont toutes les deux, pour point commun, de permettre d'évaluer la résistance, la robustesse d'un produit, d'un service à la menace cyber. La différence majeure réside dans le fait que la qualification Anssi répond à un besoin étatique de disposer de solutions de confiance sur le long terme. On s'inscrit dans une notion de durée, de confiance et de pérennité. Dans le cadre de la qualification, l'Anssi demande au fabricant, au prestataire, plus de choses que pour la certification mais cela ne veut pas nécessairement dire que le niveau de robustesse des fonctions évaluées du produit, du service est plus grand.
Tout dépend du périmètre évalué et du niveau d'assurance visé. Cette qualification peut être retirée – elle est attribuée pour trois ans – si nous constatons un changement dans le produit, dans la stratégie de l'entreprise, ou un changement d'actionnaire qui peut avoir des conséquences en matière de confiance, car on n'attend pas nécessairement un actionnariat français. La certification est plus "à la main" de l'entreprise demandeuse qui choisit le périmètre de l'évaluation. À charge pour l'Anssi de vérifier que le produit testé répond à la menace définie par le demandeur. »

➔ En savoir plus : www.ssi.gouv.fr

■ *Des utilisateurs de plus en plus sensibles*

Si pour certains, la certification n'est pas encore un critère de choix, pour un nombre croissant d'utilisateurs finaux, donneurs d'ordres, la certification fait partie de leurs exigences. *« D'une manière générale, tous les acteurs concernés prennent conscience de l'intérêt de la certification,* poursuit Vivien Mura. *Par ailleurs, il faut comprendre que la qualification Anssi est aujourd'hui associée à des obligations légales d'approvisionnement pour les OIV (pour leurs systèmes d'importance vitale). On peut en revanche imaginer que les OSE devront un jour recourir à des produits certifiés (au sens de la certification européenne). Pour les autres secteurs d'activités, la certification est un vrai facteur différenciant par rapport à la concurrence. Les utilisateurs y sont de plus sensibles car ils ont compris, qu'en matière de menaces cyber, personne n'est à l'abri. »* ● ● ●

DOMINIQUE AUVRAY

Directeur marketing chez Fichet Group

© DR

« La conformité aux normes fait partie de l'ADN de Fichet et nous concevons et fabriquons nos produits dans cette logique. Mais nous devons encore sensibiliser nos clients à l'intérêt de la certification comme gage de qualité. Il en va de même pour ce qui concerne la cybersécurité. Respecter les exigences de l'Anssi est primordial et cela nous permet d'adresser des marchés, comme celui des OIV, qui nous seraient fermés. Bénéficier de la certification et de la qualification de l'Anssi est un vrai facteur différenciant par rapport à nos concurrents. »

RÉGIS COUSIN

Président de la FFMI

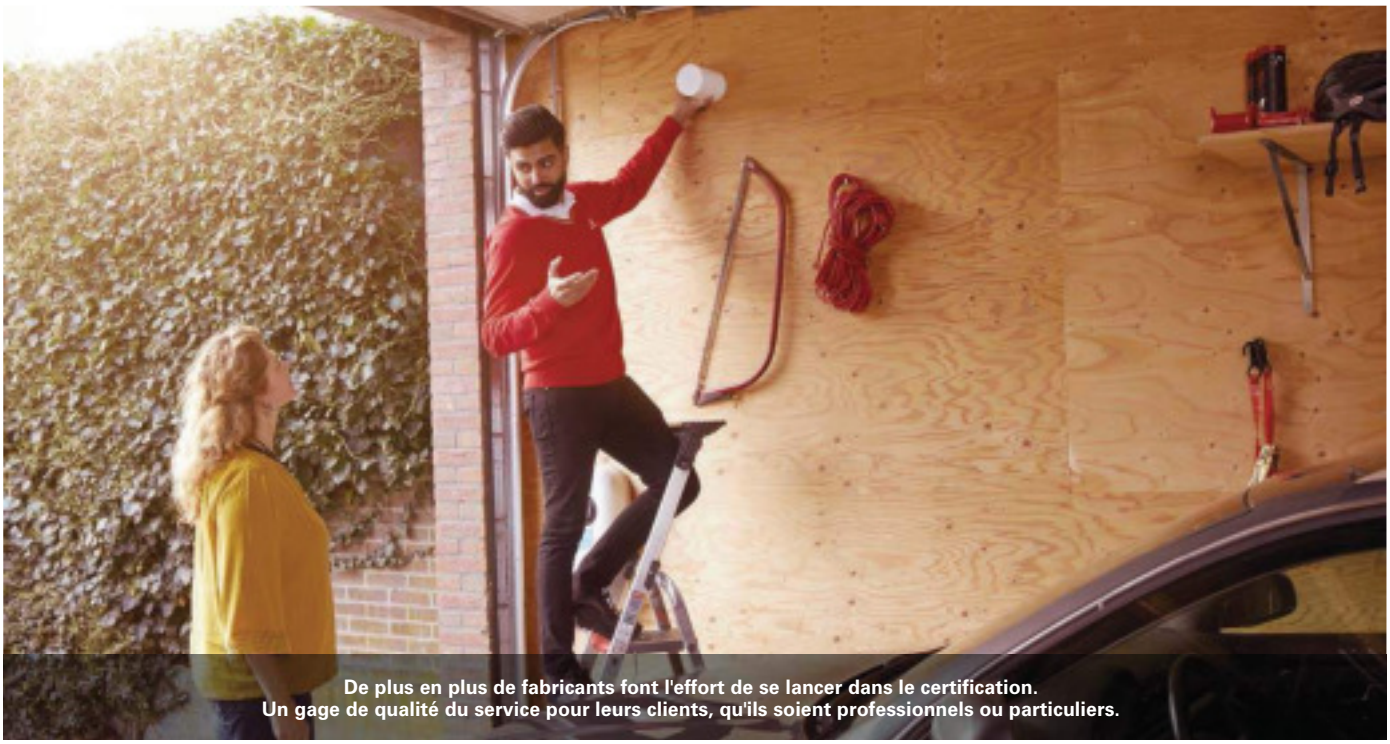
© DR

« Le secteur de l'incendie est soumis à une certification réglementaire qui permet aux produits d'être mis sur le marché : le marquage CE qui confirme que le produit en question est conforme aux textes européens le concernant. S'y s'ajoute une marque volontaire : la marque NF. Son but, dans le cadre d'une collaboration avec les pouvoirs publics, est de garantir la qualité et la performance des systèmes et des produits. Le monde de l'incendie a ainsi mis en place un système vertueux, certes exigeant, mais qui permet de rassurer les utilisateurs finaux. C'est un modèle vertueux qui pourrait inspirer d'autres domaines de la sécurité. D'ailleurs, la démarche de l'Anssi en matière de sécurité cyber est assez proche de ce que nous faisons dans l'incendie. »

© DR

« Dans les marchés publics, la certification devrait être un minimum requis. »

STÉPHANE MATHIEU, RESPONSABLE QUALITÉ DU PÔLE EXPERT CHEZ PRYNTEC



De plus en plus de fabricants font l'effort de se lancer dans le certification.
Un gage de qualité du service pour leurs clients, qu'ils soient professionnels ou particuliers.

© DR

● ● ● Si l'on s'en tient au sujet de la cybersécurité, la certification, incontournable pour certains marchés, au sens non réglementaire, en conséquence d'exigences de la part des utilisateurs/clients, devrait s'imposer. Rappelons que l'Europe travaille actuellement à l'élaboration d'un Cyber Act qui devrait consacrer des schémas de certification volontaire pour la robustesse des systèmes aux attaques numériques. *«Le niveau "high" de ce Cyber Act devrait être assez proche des exigences de l'Anssi,* estime Amaury Lequette. *De notre côté, au CNPP, nous avons fait en sorte que nos certifications soient compatibles avec le texte européen.»*

Des certifications méconnues

Force est de constater que malgré leur existence, les certifications sont assez mal connues. *«Des certifications existent dans nos métiers,* tient à rappeler Luc Jouve, président de GPMSE Installation et président du comité de certification NF service Apsad intrusion et vidéosurveillance. *Citons, par exemple, la NF Services Apsad qui permet aux utilisateurs d'avoir la certitude qu'ils font appel à un installateur contrôlé par un organisme tierce partie. Or, si cette certification est demandée dans la télésurveillance, elle est méconnue pour la partie installation et maintenance.»*

On peut jeter la pierre aux professionnels qui ne s'engagent pas dans une démarche certifiante mais il faut aussi admettre que pour qu'ils le fassent, encore faudrait-il que les certifications soient poussées par certains. Or, dans le cas de la NF Services Apsad par exemple, les assureurs ne font plus ce travail. Pourquoi ? Parce qu'ils disposent tous aujourd'hui de filiales vendant des offres de télésurveillance locatives, pour lesquelles elles utilisent des installateurs non-certifiés…

Comment faire si certains ne font pas leur part du travail ? *«Lors des comités de certification, mes confrères du collège*

LES VISAS DE SÉCURITÉ DE L'ANSSI

Les visas de sécurité que délivre l'Anssi permettent d'identifier facilement les solutions les plus fiables et reconnues comme telles à l'issue d'une évaluation réalisée par des laboratoires agréés selon une méthodologie rigoureuse et éprouvée.

→ **www.ssi.gouv.fr/administration/visa-de-securite/**

LE POINT DE VUE DE L'ANITEC

STÉPHANIE TUCOULET
Secrétaire générale de l'Anitec

© DR

«BIENTÔT UN NOUVEAU LABEL CONFORMITÉ RGPD.»

«À l'Anitec, ce qu'on regroupe parfois abusivement sous le terme de certification, recouvre trois niveaux : label, qualification et certification. Cette dernière (notamment celle délivrée par le CNPP dans nos métiers), le plus haut niveau, valorise les professionnels qui en bénéficient, et les installateurs et intégrateurs ont grand intérêt à se faire certifier. La qualification mise en avant est délivrée par Qualifelec, une organisation certifiée par le Cofrac. Avec l'entrée en vigueur du RGPD, on se rend compte que les donneurs d'ordres commencent à demander des preuves quant à la bonne application des exigences. C'est pour cette raison que l'Anitec, en partenariat avec le CNPP, va publier *Le Livre blanc : bonnes pratiques RGPD à l'attention des secteurs des intégrateurs, installateurs, mainteneurs de technologies connectées, sécurisées et pilotées.* Ce livre blanc sera la base d'un label du CNPP sur la conformité RGPD, prévu pour début avril.»

LE POINT DE VUE DU CNPP

AMAURY LEQUETTE
Directeur de CNPP Cert.

© DR

« LA CERTIFICATION VÉHICULE DE LA CONFIANCE. »

« Pour appuyer et renforcer la confiance véhiculée par les certifications volontaires A2P et APSAD, nous avons complété les caractéristiques fonctionnelles sécurité/sûreté déjà certifiées, avec la robustesse aux attaques numériques. Les travaux cyber menés par CNPP ont été réalisés en liaison avec l'Anssi afin de constituer une réponse adaptée aux produits de sécurité/sûreté, pleinement compatible et complémentaire des reconnaissances spécifiques Anssi (CSPN*, critères communs, etc.). Le but de la certification est de véhiculer de la confiance sur toute la chaîne de la sécurité, des produits aux services. »

** À noter que la CSPN est une certification de premier niveau et non une qualification.*

installateur se joignent à moi très régulièrement pour demander aux certificateurs que sont l'Afnor et le CNPP de communiquer sur cette certification NF Services Apsad. Afin de la faire connaître et qu'elle soit demandée par nos clients », recommande Luc Jouve.

Sortir du moins-disant

« Si certains de nos clients sont sensibles à la certification, la plupart sont assez peu éduqués sur le sujet. Or, la certification est une démarche vertueuse, qui prouve la qualité d'un produit, insiste Stéphane Mathieu, formateur et responsable qualité du pôle Expert chez Pryntec dont la solution Digipryn a obtenu pour ses enregistreurs vidéo numériques la certification CNPP en 2019. *Soit nos clients ne la demandent pas car ils ne la connaissent pas, soit ils craignent que l'exiger réduise le nombre de répondants, éliminant, ainsi, les produits les moins chers. Alors que ces produits faussent le débat ! Ils poussent, en effet, à comparer le prix de solutions non certifiées, et à la qualité incertaine, à des solutions qualitatives intégrant le cout de la certification. »*

Méconnaissance sans doute… Mais aussi logique du moins-disant aux effets pervers. Les professionnels qui s'engagent dans la certification ne sont pas récompensés à la hauteur de leurs investissements. Trop d'appels d'offres, et les marchés publics ne sont pas les moins fautifs, ne tiennent aucun compte des certifications produits.

« Cela est dommageable car si les entreprises publiques et les pouvoirs publics exigeaient certaines certifications, ils permettraient d'enclencher un cercle vertueux qui inciterait les fournisseurs à améliorer leurs pratiques industrielles et commerciales… », ajoute Stéphane Mathieu.

L'État ne joue donc pas assez son rôle en matière de certification. On peut regretter qu'on puisse encore passer des appels d'offres sans mention d'une quelconque certification, *a fortiori* quand il s'agit de sécurité.

Un facteur différenciant

Tous les fabricants le disent : la certification est véritable atout.

De même, engager une démarche de labellisation est aussi vertueux. *« Le fait d'avoir obtenu le label Comité stratégique de filière (CSF) "Industries de sécurité", nous permet d'expérimenter nos solutions dans une démarche de cocréation avec nos clients afin de vérifier qu'elles répondent bien aux besoins de sécurité des infrastructures de grands événements, sportifs par exemple,* explique Céline Stein, directrice sûreté France chez Siemens. *Car nous ne devons pas nous reposer sur la notoriété de Siemens. Afin de répondre aux enjeux de l'avenir, il faut continuellement prouver que nos solutions sont innovantes et sécurisées et éventuellement se faire certifié, être labellisé. Cela rassure nos partenaires, leur prouve que nous sommes engagés dans une vraie démarche continuelle de qualité et de cybersécurité. »* ■

VINCENT DUPART
PDG de STid

© DR

« Lorsque nous avons obtenu, dès 2013, la Certification de sécurité de premier niveau (CSPN) de l'Anssi, cela constituait un vrai facteur différenciant. Depuis, nos partenaires ont des solutions certifiées comme Til Technologies, Alcea, Synchronic… – et ont été certifiés Anssi en intégrant nos lecteurs. L'intérêt de la qualification Anssi est d'instaurer sur des marchés comme celui des OIV une barrière à l'entrée à des acteurs peu soucieux du niveau de sécurité. Mais nous devons aller au-delà des certifications françaises. C'est pour cela que vient d'être créé SPAC (Smart Physical Access Control) pour positionner les savoir-faire français au niveau européen, dans le cadre du Cyber Act. »

ANNE PEREZ
Directrice sécurité et relation client chez Verisure Securitas Direct

© DR

« Dans la télésurveillance, la certification APSAD R3I est essentielle et obligatoire pour une entreprise qui veut protéger les biens et les personnes. Notre certification APSAD R3I P3 assure à nos clients que nos trois stations de télésurveillance sont sécurisées, que les données sont protégées et confidentielles mais également que l'ensemble de nos chargés d'assistance jouissent du certificat "Agent de télésurveillance" et d'un agrément professionnel, renouvelé régulièrement. La certification est nécessaire mais pas suffisante. Il faut y associer des technologies innovantes, des systèmes fiables et des services efficaces. »

VOIR LES PRINCIPALES NORMES PAGE 39

Faute de faire de la certification un critère de sélection, de nombreux appels d'offres publics, comme ceux concernant la sécurité des grands événements, sont "offerts" aux moins-disants...

© DR

Sécurité privée et certification : peut mieux faire

Dire que le monde de la sécurité privée est peu sensible à la certification est une lapalissade. Or, comme dans d'autres secteurs d'activités, une démarche qualité permettrait à ces métiers de s'engager dans une démarche vertueuse, gage de confiance.

Un maître mot dans le monde de la sécurité privée : le continuum. Ce fameux continuum de sécurité qui doit permettre d'articuler les relations entre les forces de l'État – police et gendarmerie – les hommes et services des sociétés de sécurité privée. *« Ce continuum – et les relations qu'il implique entre les pouvoirs publics et les sociétés privées – est un des objectifs du Livre blanc de la sécurité intérieure qui sera le fondement de la loi d'orientation de la sécurité intérieure,* insiste Patrick Butor, responsable de la normalisation au ministère de l'Intérieur, coprésident de la commission normalisation du collège du Cnaps, président de la commission sécurité de l'Afnor. *C'est un sujet d'autant plus important que la France va accueillir – en 2023 la Coupe du monde de rugby et en 2024 les JO de Paris – des événements majeurs qui nécessiteront le recours aux moyens humains et techniques des sociétés de sécurité privée. La sécurité privée doit donc comprendre, pour s'y engager le plus vite possible, que la certification sera nécessaire pour permettre à l'État de s'assurer qu'il aura en face de lui des sociétés privées qui correspondent à ses attentes, à ses exigences… Or, tout le problème réside dans le fait que jusqu'à maintenant, le monde de la sécurité privée – pour des raisons diverses – n'a pas marqué un grand intérêt, une vraie appétence, pour la normalisation et la certification, sauf pour les sociétés engagées à l'export. »*

Le constat de Patrick Butor est partagé par beaucoup. *« Si ces métiers ont connu d'importantes mutations, ils sont longtemps restés exempts de toute forme d'encadrement normatif…,* confirme Christophe Massare, dirigeant du cabinet QCM. *Mais les choses changent : lois, création du Cnaps, amélioration de la formation. Il faut*

2 QUESTIONS À

GEOFFROY CASTELNAU

Président de DPSA Île-de-France

© DR

Selon vous, quels seraient les moyens et les leviers pour inciter les entreprises de sécurité à s'engager dans une démarche qualité, à décrocher une ou des certifications ?

On pourrait très bien imaginer de mettre en place une obligation d'un référentiel qualité pour toutes les entreprises adhérentes du GES. À l'image de ce qui se fait dans le bâtiment. Mais il faut aussi que les donneurs d'ordres nous soutiennent. Certains sont prêts à le faire. Pas tous malheureusement. Pourquoi tout simplement ne pas fermer certains marchés aux entreprises sans référentiel, sans certification ? Vœux pieux sans doute car dans nos pays latins la sécurité est encore perçue comme un coût. À l'inverse des pays anglo-saxons où la sécurité est un investissement comme un autre. Tant que nous aurons face à nous des acheteurs qui considèrent que la sécurité est toujours trop chère, certains de mes confrères pourront profiter de la logique du moins-disant… Comment peut-on encore, en France, accepter de factures des prestations à des taux horaires de moins d'une vingtaine d'euros, alors qu'en Belgique, ils sont à 25 euros/heure, entre 29 et 33 euros en Angleterre et pas loin de 50 euros en Suisse ! Comment certains peuvent-ils prétendre faire de la qualité avec de telles pratiques ?

Les pouvoirs publics donnent-ils le bon exemple en matière de prix d'achat des prestations de sécurité ?

Loin de là. À tel point que je me refuse à répondre aux appels d'offres publics. Tout comme à ceux de la grande distribution. Cette logique qui consiste à toujours vouloir acheter au plus bas a des conséquences terribles. Elle marginalise les entreprises qui ont fait l'effort d'être certifiées, au prix de réels investissements, et a aussi pour effet de nuire à l'attractivité de nos métiers. Alors qu'approchent la Coupe du monde de rugby de 2023 et les JO de Paris en 2024, on se demande encore comment on va satisfaire les besoins en agents de sécurité. Va-t-on devoir recruter des agents de sécurité étrangers sans carte professionnelle pour satisfaire la demande ? Rappelons-nous l'échec de G4S lors des JO de Londres. Sujet d'inquiétude pour le Cnaps car de nombreuses entreprises refusent déjà de répondre à des appels aux prix tirés vers le bas.

aujourd'hui promouvoir mieux encore les opportunités qui s'offrent à la branche professionnelle en termes de qualification et de certification. Par ailleurs, il existe, depuis 1984, des standards internationaux généralistes (ISO 9001, 14001 et 45001), complétés par des normes et référentiels sectoriels comme la NF X 50777 qui n'a jamais été réformée en profondeur. Mais le monde de la sécurité privée, à l'inverse d'autres filières, ne se les est jamais appropriés. »

Une question de souveraineté ?

Depuis 2001, l'ISO s'est emparée de la norme en matière de sécurité. Les États-Unis ont ainsi produit une première norme, l'ISO 18780, régissant l'ensemble des opérations de sécurité privée dans les pays à faible souveraineté. Cette norme est même parfois utilisée pour des pays comme la France lors d'événements accueillant des personnalités américaines comme le Festival de Cannes ou pour les sièges sociaux de grandes entreprises comme Google. *« L'utilisation de cette norme se fait dans un cadre contractuel : on protège des vedettes, des PDG. Mais on pourrait légitimement penser qu'une norme s'appliquant aux pays à souveraineté normale, comme la France, aurait dû voir le jour. Cela n'a pas été le cas,* regrette Patrick Butor. *Car le problème est, qu'en France, pays de droit romain et écrit, la normalisation est peu connue. Elle n'est pas enseignée dans les études de droit. Dans les pays anglo-saxons, elle fait partie intégrante de la vie des entreprises. Leurs représentants participent aux travaux normatifs, siègent dans les comités… C'est dommageable pour les entreprises françaises car ces travaux sont très importants, utiles, et permettent de défendre ses intérêts. »*

Ainsi, à l'inverse du monde de l'incendie qui fait du travail normatif un des leviers pour défendre la conception française de la sécurité incendie, le monde de la sécu-

LE POINT DE VUE DU CNAPS

PATRICK BUTOR

Responsable de la normalisation au ministère de l'Intérieur, coprésident de la commission normalisation du Collège du Cnaps

© DR

« LA SÉCURITÉ HUMAINE EST ASSEZ RÉTIVE À LA CERTIFICATION. »

« Les industriels français ne manifestent pas un grand intérêt pour la normalisation et la certification. Et le secteur de la sécurité privée n'échappe pas à cette tendance. Or, ils doivent se saisir du sujet. Actuellement, beaucoup de travaux de réflexion sont en cours quant à la refonte de certaines normes ou la création de nouvelles. Par exemple, je participe aux travaux sur un projet de norme ISO sur les plans de sécurité et sur une autre concernant les principes de sûreté. Ils auront nécessairement un impact sur les métiers de la sécurité privée. Par ailleurs, le groupe que je préside, au sein de l'ISO, va devoir mener la révision de la norme 18788 afin de la rendre plus opérationnelle. Enfin, il serait sans doute souhaitable qu'au niveau européen soient menés des travaux pour mettre en place une norme sur la sécurité dans les pays souverains et qui pourrait induire une certification des entreprises de sécurité privée. Malheureusement, le monde de la surveillance humaine – mis à part les prestataires haut de gamme – se sent encore trop peu concernés par la certification. »

rité privée néglige cette approche et laisse une certaine vision venue d'outre-Atlantique s'imposer dans leur secteur d'activités. Et la souveraineté dans tout cela ?

Des normes obsolètes et ignorées

Ainsi, aujourd'hui, seuls une dizaine d'opérateurs français sont certifiés NF X 50777. *« Cette norme qui n'a jamais évolué depuis sa création est en voie d'obsolescence. Le marché ne se l'est pas appropriée durablement,* poursuit Christophe Massare. *Par ailleurs, elle n'est pas adaptée au plus grand nombre d'opérateurs du marché auquel elle est censée s'adresser : les TPE et PME qui constituent la majorité des entreprises de la sécurité privée. »*

Alors comment attirer, amener le monde de la sécurité vers la certification ? Pour Christophe Massare, cela passe par la mise en place d'un outil accessible à ce plus grand nombre : *« Dès la fin des années 2007, le monde de la sécurité privée a envisagé de créer un référentiel répondant à cet impératif. Un référentiel techniquement et économiquement abordable. C'est de l'ambition de répondre à ce double défi qu'est né "QualiSécurité" dont l'objectif est d'être un référentiel qui permette aux entreprises de taille modeste ou moyenne de conduire une démarche qualité, reconnue par un organisme tier indépendant, en l'occurrence l'Afnor. Lancé début 2009, QualiSécurité a connu un succès mitigé. Certes, de plus en plus d'entreprises s'y engagent, mais on est encore loin d'exploiter pleinement son potentiel. Pourquoi ? Notamment du fait d'une incapacité de ses divers prescripteurs à en assurer la promotion efficace, pour des raisons multiples : divergence d'intérêts, création du Cnaps qui a mobilisé les énergies… Et aujourd'hui, seulement environ 40 établissements sont certifiés QualiSécurité… »*

Redynamiser les référentiels

Certains professionnels prêchent pour une refonte des deux référentiels (Qualitésécurité et NF X 5077) qui constituent néanmoins un socle précieux en termes de retours d'expérience. *« Elles viseraient à les rapprocher en équilibrant le niveau d'exigences avec pour finalité de le rendre plus compatible, plus "en prise", avec les attentes actuelles du marché. En revanche, l'émergence d'une nouvelle norme enverrait un mauvais signal à ce dernier »*, ajoute Christophe Massare.

« Notre secteur se compose d'environ 10 000 sociétés, dont une bonne partie emploient moins de dix salariés. S'engager dans une démarche de certification peut donc être difficile pour ces TPE. Le sujet est complexe et induit des coûts parfois importants. Entre 50 000 et 70 000 euros dans le cas de NF Services, explique Geoffroy Castelnau, directeur général de DPSA. *Il faut donc réfléchir à quelque chose de plus simple. C'était l'objectif de Qualisécurité : mettre à la portée de tous, en quelques mois de travail et un coût estimé à 5 000 euros, la certification. »*

Avant de poursuivre : *« Une démarche qualité demande du temps, coûte de l'argent alors que nos métiers se caractérisent par une rentabilité assez faible, de l'ordre de 1 % par an… C'est pourquoi le GES devrait travailler à un nouveau référentiel qualité, pour redynamiser la démarche certification dans notre secteur. »*

Une bonne partie de la profession est consciente des enjeux de la certification et de la qualité. Mais certains refusent de jouer le jeu. Qu'il s'agisse de donneurs d'ordres ou de professionnels de la sécurité. *« Si des entreprises comme DPSA, qui ont dès l'origine fait le pari de la qualité, de la certification, veulent maintenir leur modèle économique et leurs marges, elles sont contraintes de refuser de répondre à certains appels d'offres où la logique du prix l'emporte sur la qualité. Situation aberrante dans laquelle les pouvoirs publics ne donnent même pas le bon exemple »*, conclut Geoffroy Castelnau. ■

PAROLE D'EXPERT

CHRISTOPHE MASSARE
Dirigeant de QCM

© DR

« LA CERTIFICATION DOIT SE PAYER AU JUSTE PRIX. »

« Les entreprises de sécurité privée confondent souvent la certification et ce qui conduit à l'obtenir. Elles se font souvent certifier, à tort, pour la seule certification. Or, la justification exclusive de la certification est l'attente du marché, qui doit en exprimer clairement le besoin et accepter l'idée d'un ROI au profit des prestataires. Cette certification coûteuse a vocation à apporter de la valeur ajoutée aux entreprises qui en jouissent ainsi qu'à leurs clients. Les donneurs d'ordres devraient donc accepter de payer un juste prix en adéquation avec le niveau de leurs exigences. Or, la tendance consiste encore à privilégier le moins-disant, encourageant ainsi un nivellement par le bas. Ne serait-il pas plus judicieux de soutenir ceux qui engagent une démarche qualité ? Démarches qualité qui ne sont pas réservées qu'aux grandes entreprises. Elles sont, en fonction du référentiel choisi, tout à fait accessibles aux PME et TPE qui se positionnent sur des marchés prestigieux et qui refusent cette "fatalité" du moins-disant lorsqu'elles répondent aux appels d'offres tant publics que privés. Est-il cohérent de la part des donneurs d'ordres d'exiger des prestations de qualité sans une contrepartie légitime : le juste prix ? La question reste posée. Gageons que la raison finira par l'emporter. »

NORMES

- Au niveau CEN, trois normes concernent directement la sécurité privée : EN 15602 : 2008 – Terminologie (actuellement révisée par le CEN TC439), EN 16082 : 2011 – Services de sécurité dans le domaine aéroportuaire, EN 16747 : 2015 – Services de sécurité dans le domaine maritime et portuaire.
- Au Cenelec, la norme EN 50518 : 2019 concerne les systèmes d'alarme.
- Au niveau de l'ISO, la norme 18788 « Management System for Private Security Operations – Requirements with Guidance » traite spécifiquement du secteur de la sécurité privée dans des environnements où la gouvernance est faible.

© DR

« Les donneurs d'ordres méconnaissent ce qu'on doit attendre d'un service de sécurité. »

CATHERINE PIANA

Directrice générale de la Confédération européenne des services de sécurité (CoESS)

Pour la DG de la CoESS, de nombreux donneurs d'ordres voient dans la sécurité la simple fourniture d'un « produit » et ne se préoccupent pas de la qualité de la prestation.

Quels travaux d'harmonisation sont menés au niveau européen ?

Il n'y a pas actuellement de besoin d'harmonisation pour le sujet général du gardiennage, qui est réglementé dans le détail (ou en voie de l'être) dans la vaste majorité des pays européens. Certes, le degré de sévérité (qui est pour nous synonyme de qualité) de cette législation varie d'un pays à l'autre. Mais on ne peut pas actuellement envisager une norme identique pour tous les pays européens. Cela dit, il est important de tirer la profession vers le haut et de militer pour des prestations de qualité. C'est ce que nous cherchons à faire en parlant aux donneurs d'ordres et en éditant des guides, tels que « Acheter des services de sécurité de qualité », coproduit par CoESS et UNI Europa (syndicat représentant les gardes de sécurité notamment) avec des fonds européens.

La production de normes touchant à des domaines spécifiques, comme l'aéroportuaire et le portuaire/maritime, est nécessaire car nous considérons que la législation en la matière est lacunaire et nécessite donc d'être complétée par des normes détaillées et précises – du reste ce n'est pas l'objectif de la législation de couvrir tous les aspects précis et détaillés des prestations de services de sécurité privée. Pour ce qui est de la directive sur les marchés publics, l'occasion a été manquée par de nombreux pays (enfin tous sauf un, à ma connaissance), lors de la transposition en droit national, d'exiger que les donneurs d'ordres accordent à la qualité plus d'importance qu'au prix. Seule l'Espagne, au prix d'actions intenses de nos homologues nationaux, a fait ce choix. La CoESS a tenté d'inscrire ce principe dans la directive mais le conseil avait laissé le choix aux États membres. Aujourd'hui, nous cherchons à faire respecter ce principe par d'autres biais. Et nous gardons espoir de faire entendre raison aux donneurs d'ordres. Il n'est pas acceptable de protéger ce que l'État a de plus précieux et indispensable – ses infrastructures critiques – en choisissant le prestataire le moins-disant.

Selon vous, pourquoi les donneurs d'ordres publics français sont-ils si peu sensibles à l'intérêt de faire appel à des prestataires certifiés, engagés dans une vraie démarche qualité ?

Il y a plusieurs hypothèses. Hypothèse numéro 1 : le manque d'argent. C'est un bien mauvais et dangereux calcul. Car le coût possible d'une mauvaise prestation de services, de médiocre qualité, est bien supérieur à celui du meilleur rapport qualité-prix. Nous parlons de services de sécurité, pas d'une simple fourniture de produit à usage unique. Cela dit, il peut arriver que l'acheteur n'ait pas toute la marge de manœuvre quant au budget. J'ai pu entendre cet argument de la part, par exemple, de représentants des chemins de fer (dans un autre État de l'UE), dont le budget était fixé par le ministère des Transports et qui, de ce fait, n'avait que peu de marge de négociation. Hypothèse numéro 2 : la méconnaissance du service de sécurité et de ce que l'on doit en attendre. Nous cherchons à remédier à cette méconnaissance, précisément en publiant le guide sur l'achat des services de sécurité en indiquant comment rédiger les offres et les évaluer sur la base de critères de qualité. Ce qui est difficile lorsque l'acheteur des services est un généraliste et ne sait pas faire la distinction entre une société de qualité et une autre. Hypothèse numéro 3 : la vision étroite et à court terme de beaucoup de systèmes aujourd'hui qui, du coup, ne sont intéressés que par les chiffres et non par la réelle qualité ou non d'un service. Malheureusement, c'est une observation fréquente. La réalité est sans doute un mélange entre tout ce qui précède. Je peux aussi imaginer que la profession peut parfois s'enfermer dans ses propres clichés et « n'ose plus » proposer autre chose que « x hommes à x heures ». C'est une remarque que l'on m'a faite récemment en France. Un donneur d'ordres déplorait les offres reçues, y compris d'acteurs très réputés sur le marché, qui restaient sur le modèle « x hommes-x heures ». Il est donc grand temps de réunir toutes les personnes de bonne volonté autour d'une même table et d'avancer ensemble.

➔ **Le guide « Acheter des services de sécurité privée de qualité » peut être télécharger gratuitement en français : www.securebestvalue.org**

VOIR LES PRINCIPALES NORMES PAGE 39

Directeurs sûreté : la certification, pour quoi faire ?

La certification peut participer à une forme de reconnaissance du rôle des directions sûreté. Par ailleurs, on peut se demander pourquoi les acteurs concernés ne se sont pas encore assis autour d'une table pour donner naissance à une certification française.

Il existe assez peu de certifications reconnues mondialement pour les directeurs sécurité-sûreté. Et en France, force est de constater que la majeure partie des cadres de la sécurité dans les entreprises est loin de bénéficier d'une certification. Mais les choses changent comme le confirme Nicolas Le Saux, président d'Atao Consulting : *« Il y a encore trois ans, seuls trois ou quatre membres du chapitre France d'ASIS International jouissaient de la certification CPP d'ASIS International. Aujourd'hui, nous en dénombrons une quinzaine. Soit environ 15 % de nos membres. La France rattrape donc son retard. Cela démontre aussi l'engouement pour cette certification qui, bien qu'Anglo-Saxonne, a le mérite d'exister alors qu'il n'y en a pas beaucoup d'autres en France ou en Europe. »*
Comment expliquer ce constat ? Tout d'abord, il semble bien que les jeunes générations de cadre de la sécurité des entreprises soient plus sensibles à l'intérêt de la certification. Ne serait-ce que pour pouvoir envisager des carrières à l'international ou échanger avec ses pairs. *« La certification CPP reconnaît, non seulement une expertise en anglais, mais aussi facilite l'harmonisation de certaines pratiques car elle définit un socle commun de compétences qui permet à des directeurs sécurité-sûreté de parler le même langage »*, ajoute Nicolas Le Saux.

Un vrai besoin

Il semble donc que le monde du management de la sécurité-sûreté dans les entreprises, en France, ait pris conscience que la certification pouvait participer à une certaine forme de reconnaissance. Pourtant, certains regrettent que malgré cela, les directeurs sécurité-sûreté ne soient pas assez visibles et intégrés dans le continuum de sécurité. Ce fut d'ailleurs le sujet d'un débat lors du dernier Gala de l'Agora des directeurs sécurité (voir actus sûreté p.18).
Mais est-ce que la certification participe de la visibilité du cadre de sécurité-sûreté ? Est-ce qu'elle peut l'aider à être reconnue comme un interlocuteur à part entière des pouvoirs publics, par exemple, dans le cadre du continuum sécurité ? Certains n'en sont pas certains.

CERTIFICATION « JUNIOR » CHEZ ASIS

ASIS International vient de lancer une certification intermédiaire, plus simple, à destination des cadres de la sécurité-sûreté des entreprises juniors et qui n'ont pas encore assez d'expérience (moins de sept ans) pour prétendre à la certification CPP.

© Getty Images

© DR

« La standardisation d'une certification française doit devenir une référence. »

GABRIEL GEDDA, ASIS FRANCE CHAIRMAN

« Je ne suis pas certain que la certification permette au directeur sécurité-sûreté de mieux se positionner dans le continuum sécurité, poursuit le président d'Atao Consulting. *Faut-il mettre en place une sorte de labellisation pour l'aider à occuper cette place ? On peut se poser la question. Il serait en revanche souhaitable que des instances comme le Cnaps réfléchissent à la mise en place d'un registre des directeurs sécurité-sûreté qui permettrait aux forces de l'ordre de savoir qui est son interlocuteur au sein de telle ou telle entreprise et de savoir avec qui dialoguer, échanger des informations. »*
Certains appellent de leurs vœux la généralisation en France d'une pratique venue d'outre-Manche : l'Information Sharing Agreement qui permet aux entreprises et forces de l'ordre britanniques d'échanger des informations. Mais cela se fait déjà en France, dans un certain cadre juridique. Alors que faire ?

Vers une certification à la française ?

Gabriel Gedda, ASIS France Chairman et Senior Regional Security Advisor France & SW Europe (Microsoft), y réfléchit : *« Avant de parler certification, il faudrait déjà se mettre d'accord sur le cursus, les formations, les compétences qui constitueraient le tronc commun permettant d'y prétendre. On doit s'appuyer sur les "best practices". Je veux dire par là qu'il existe un grand nombre de formations dont certaines sont parfaitement connues et reconnues puisqu'elles incitent les entreprises à recruter d'an-*

© DR

« Rien n'empêche les DS français d'élaborer une certification française. »

NICOLAS LE SAUX, PRÉSIDENT D'ATAO CONSULTING

ciens militaires, policiers ou agents des services de renseignement. On pourrait donc définir un ensemble de formations (DU, MBA, BTS, DUT, etc.) qui permettrait de définir le contenu et les exigences de cette certification. La profession doit être proactive sur le sujet et ne pas attendre que ce soient les autres qui se chargent de mettre en place cette certification. »

Point de vue que partage Nicolas Le Saux : *« Qu'est-ce qu'a fait ASIS à ses débuts ? Elle a développé sa propre certification. Qu'est-ce qui interdit les Français d'en faire autant ? Il suffirait de se mettre autour d'une table, de discuter, de travailler à écrire un référentiel et les procédures de certification. Avec pour base un ensemble de formations correspondant au niveau de connaissance qu'on serait en droit d'attendre pour pouvoir prétendre à la certification. Tout cela pourrait déboucher sur un label du Cnaps qui serait accessible à ceux ayant suivi telle(s) ou telle(s) formation(s). Tout cela, sans esprit de chapelle et pour le bien du métier de directeur sécurité-sûreté. D'autant plus que cela participerait évidemment à en définir plus précisément les contours, les missions… »* ■

PAROLE D'EXPERT

OLIVIER HASSID
Associé chez PricewaterhouseCoopers

© DR

« LA NORME PERMET DE RENFORCER LES LIENS ENTRE SÛRETÉ ET OPÉRATIONS. »

« Il y a dix ans, le CDSE avait mené une étude qui montrait que seuls 20 % des directeurs sécurité-sûreté avaient mis en place la norme ISO 27001 sur la sécurité des systèmes d'information. Aujourd'hui, la situation a sans doute peu évolué car de nombreuses directions sécurité-sûreté ne disposent pas des équipes suffisantes pour engager une démarche de certification, somme toute assez lourde. D'autant plus que, pour elles, le ROI n'est pas toujours évident. En revanche, on peut espérer, avec l'apparition de postes de directeurs de la sécurité globale (physique et logique), un certain regain d'intérêt pour l'ISO 27001 puisqu'elle couvre les deux aspects de la sécurité globale. Enfin, la norme permet de renforcer les liens entre sûreté et opérations. La sûreté devient ainsi une vraie valeur ajoutée, un facteur différenciant par rapport à la concurrence. »

LES PRINCIPALES NORMES, CERTIFICATIONS ET QUALIFICATIONS

Pour les fabricants

- Anssi - Certification et qualification : www.ssi.gouv.fr
- CNPP - A2P, Apsad, EEA : www.cnpp.com/Certification
- Norme NFX 50-785 « Services des entreprises de systèmes électroniques de sécurité »
- Séries EN 50131 et EN 50132 en matière de systèmes d'alarmes

Pour la sécurité privée

- Certification NF Service 241 « Service des entreprises privées de prévention et de sécurité »
- Marque « Qualisécurité » ou « Prestation de service des entreprises privées de surveillance humaine » (REF215)

Pour les directions sécurité-sûreté des entreprises

- Norme ISO/CEI 27001 « Management de la sécurité de l'information »
- Norme ISO 22301 « Sécurité sociétale – Gestion de la continuité des activités »
- Norme NF/ISO 18788 « Système de management des opérations de sécurité – exigences et recommandation »
- ASIS International : Certified Protection Professional (CPP), Professional Certified Investigator (PCI), Physical Security Professional (PSP), Associate Protection Professional (APP) : www.ASISonline.org/certification/ASIS-board-certifications2/.

Contrairement à ce que l'on peut croire, la haute résolution n'est pas à déployer partout. En revanche, pour la surveillance de sites étendus, elle est particulièrement pertinente. Par exemple, pour identifier des personnes.

© Dallemeier

La HR est très efficace pour certaines applications. Pas toutes.

La haute résolution est aujourd'hui un des standards en matière de vidéosurveillance. Des caméras haute résolution de qualité, bien installées et paramétrées, vous permettront de profiter au maximum des technologies et fonctionnalités conçues par les fabricants.

Certains s'imaginent, à tort, que disposer de plus de caméras, de toujours plus de résolution… garantit l'efficacité d'une installation de surveillance. Or, cette règle du « plus il y en a, mieux c'est » est trompeuse. *« Que ce soit dans les lieux publics, les gares, les aéroports ou les biens immobiliers d'entreprise : lors de la sécurisation de superficies et d'espace étendus, le défi consiste à obtenir une vue d'ensemble de la totalité du site et en même temps la résolution la plus détaillée, même dans les zones les plus éloignées de l'image »*, rappelle Erik Ashani, directeur des ventes chez Dallmeier et responsable pour le marché français. Avant d'ajouter : *« Même si actuellement, en matière de caméras réseaux, le nombre de mégapixels toujours plus important est un argument de vente pour certains, la résolution seule n'est pas tout. La capacité à détecter des détails et à identifier des personnes, à la fois à proximité de la caméra et dans les zones plus éloignées, est cruciale pour sécuriser de manière fiable de grandes zones. »* Point de vue que partage Nicolas Hess, Key Account Manager chez Hikvision France : *« La haute résolution fait vendre. Et le marché de la vidéosurveillance est dans une phase qui voit ceux qui n'ont pas de compétences techniques utiliser la très haute résolution comme un argument de vente. Mais on doit se poser cette question : à quoi servent tous ces pixels en plus ? Et qu'impliquent-ils comme contraintes techniques et maté-*

2 QUESTIONS À

ERIK ASHANI

Directeur des ventes chez Dallmeier

© DR

Pouvez-vous nous présenter votre système Panomera ?
La technologie brevetée des capteurs multifocaux Panomera se caractérise par un tout nouveau concept d'objectif ou de capteur qui fonctionne avec plusieurs capteurs, chacun ayant une distance focale différente. Cela permet de « graduer » la zone à surveiller, de sorte que même les objets les plus éloignés puissent être visibles avec la même résolution que les objets situés au premier plan de l'image (résolution continue garantie en fonction des besoins, par exemple d'au moins 125 pixels/m). À partir d'un seul emplacement, il est possible de sécuriser très efficacement une immense superficie. Outre les économies considérables en termes d'infrastructure et de TCO (Total Cost of Ownership), cette solution offre également de grands avantages pour le personnel de sécurité : la possibilité de voir toute la zone de surveillance en une seule image continue, sans avoir à passer d'une caméra à une autre, ce qui facilite le fonctionnement du système et réduit les délais d'intervention des services d'urgence.

Quels sont ses autres atouts ?
Les systèmes de capteurs multifocaux n'offrent pas seulement des avantages pour la sécurisation des lieux publics : la technologie MFS améliore fondamentalement le mode d e fonctionnement des systèmes vidéo et leurs applications possibles dans l'industrie et le commerce. L'efficacité d'un système vidéo est considérablement accrue, ce qui signifie cependant : moins, mais nettement meilleur, plus efficace et donc plus rentable. La principale problématique de la technologie de sécurité vidéo a également beaucoup changé entre-temps : on est passé de la simple surveillance à l'optimisation et au contrôle des processus grâce à un gain d'informations important, à l'aide de solutions vidéo intelligentes et analytiques. C'est là que la technologie des capteurs multifocaux comble le fossé des systèmes vidéo classiques.
La technologie MFS est en passe de changer de manière significative l'avenir de la technologie de la sécurité vidéo.

© DR

CÔTÉ SOLUTIONS

De l'IA chez Hanwha Techwin

La caméra TNB-9000 d'Hanwha Techwin est une caméra box réseau 8K. Elle est dotée d'un capteur d'images CMOS plein format de 43,3 mm et propose des résolutions allant de 8K à 15 ips, 24MP à 20 ips, 15MP à 30 ips et 4K à 60 ips. Compatible avec des objectifs à monture EF, elle intègre une fonction d'analyse intelligente de la vidéo basée sur l'intelligence artificielle (détection/classification d'objets) et l'outil de compression WiseStream II, conçu par Hanwha.

rielles ? » Ce à quoi, Philippe Bénard, Business Development Manager A&E chez Axis Communications ajoute : *« Aujourd'hui, s'inscrire dans la logique de la résolution pour la résolution, en faire une fin en soi, est une erreur car on ne tient pas compte des contraintes de la qualité de l'image. La haute résolution n'est pas synonyme de qualité d'images. »* ●●●

LE POINT DE VUE D'UN FABRICANT

NICOLAS HESS
Key Account Manager chez Hikvision France

© DR

« ATTENTION À LA MAÎTRISE DE L'ENVIRONNEMENT DE LA CAMÉRA ! »

« La haute résolution n'est pas une solution miracle en matière de vidéosurveillance. Comme toute technologie, elle est soumise à certaines contraintes. Le 4K, par exemple, fournira de bonnes images, dans des conditions d'éclairage correctes. Mais il nécessite d'être associé à un moniteur 4K si l'on souhaite afficher l'image en temps réel et des moyens de stockage dimensionnés en conséquence pour bénéficier des avantages de la haute résolution en relecture. Les caméras haute résolution sont tout à fait pertinentes pour surveiller de vastes zones, bien éclairées, afin de fournir à l'opérateur le maximum de détails et lui fournir le plus d'informations possible. Quand l'éclairage n'est pas suffisant ou l'environnement pas maîtrisé, il vaut mieux opter pour une caméra avec moins de résolution mais avec une capacité de traitement électronique de l'image plus poussée. Par exemple, dans un environnement très sombre, nos caméras Colorvu ou Darkfighter jusque 4MP compensent électroniquement le manque de lumière pour rester en couleur là où une caméra 4K passera automatiquement en noir et blanc avec un éclairage IR additionnel (perdant ainsi l'information précieuse de la couleur). »

© DR

Les systèmes MFS fonctionnent avec plusieurs capteurs et différentes longueurs focales, de sorte que les objets éloignés sont affichés avec la même résolution que les objets se trouvant dans la zone d'image frontale.

Un principe physique simple

En effet, en matière de vidéosurveillance, il faut tenir compte d'un principe physique très simple que nous explique Erik Ashani : *« Une scène réelle est tridimensionnelle, mais dans l'image de la caméra, elle n'est montrée qu'en deux dimensions. Les pixels de la caméra sont équitablement répartis sur le capteur de la caméra, assurant une résolution définie uniforme sur l'ensemble de l'angle d'image – bien qu'une résolution et une densité de pixels beaucoup plus élevées seraient en fait nécessaires pour les zones plus éloignées, afin d'obtenir, en fin de compte, le même nombre de pixels par mètre que dans la zone proche de la caméra. »*
En d'autres termes, si une caméra fournit une image d'ensemble en haute résolution, celle-ci peut être utilisée pour percevoir des événements en fonction des conditions d'éclairage locales et de la dynamique de la caméra. Toutefois, cela ne signifie pas

CÔTÉ SOLUTIONS

Migrez vers la haute résolution grâce à Bosch

La gamme Flexidome IP starlight 8000i de Bosch Security and Safety Systems dispose d'une fonctionnalité qui permet de distinguer intelligemment les vrais événements de sécurité et les fausses alertes. Il s'agit d'une bonne solution, pas trop chère, pour remplacer des caméras HD et faire migrer peu à peu son installation vers la très haute résolution. Elle dispose d'une gestion optimisée de la bande passante avec les fonctions iDNR (Intelligent Dynamic Noise Reduction), Intelligent Streaming et le format de compression H.265. Elles intègrent nativement toutes nos fonctions d'analyse vidéo.

© DR

LE POINT DE VUE D'UN FABRICANT

CÉDRIC GONZALEZ
Directeur des ventes chez Provision ISR

© DR

« ASSOCIER L'IA À LA HAUTE RÉSOLUTION POUR DES CAMÉRAS PLUS EFFICACES. »

« Notre nouvelle série Eye-Sight s'adresse à ceux qui ont besoin d'une gamme de caméras professionnelles associant grande qualité d'images et une connectivité complète. Ces caméras sont disponibles dans des résolutions allant du 2MP au 8MP, en passant par le 4MP. Autre atout : elles intègrent des fonctions avancées d'analyses vidéo grâce à de l'intelligence artificielle afin de faire de la reconnaissance faciale et de la détection d'objets. Ces caméras sont donc capables de reconnaître des humains, des objets, des voitures et autres véhicules… pour ensuite mettre en place des scénarios pour déclencher des alarmes en cas de franchissement d'une ligne virtuelle par un humain ou un véhicule. »

Le 1er Salon Online
sur la Sécurité et la Sûreté !
e-salon-protectionsecurite.fr

qu'en cas de situation critique, on dispose d'une résolution suffisante sur l'ensemble de la scène pour clarifier les incidents. La condition suivante s'applique ici : selon les exigences et en fonction de la scène et des détails à reconnaître, il doit y avoir un nombre minimum de pixels sur l'objet ou la personne dans l'image. On parle ici de pixels par mètre sur l'objet/personne (px/m) et non pas des pixels fournis par une caméra (par exemple, la spécification « caméra 5 mégapixels »).

Valeurs standards

Il existe des valeurs standards pour les pixels par mètre dans l'industrie vidéo (DIN EN 62676-4) : pour observer, il faut 62,5 pixels/m, pour reconnaître des personnes connues 125 pixels/m, et pour identifier des personnes inconnues 250 pixels/m sont nécessaires – quelle que soit la distance entre la personne et la caméra.
Prenons un exemple. Trois personnes de la même taille se tiennent devant une caméra. La première personne se trouve à une distance de 15 mètres de la caméra, la deuxième à une distance de 50 mètres et la troisième à une distance de 100 mètres. Dans cette perspective, les personnes sont représentées de plus en plus petites lorsque la distance augmente dans l'image. Afin de garantir que la personne située à une distance de 100 mètres soit également reconnaissable dans un zoom numérique ou dans l'enregistrement vidéo, au moins 125 pixels par mètre doivent être présents sur cette personne dans la profondeur de l'image. Ce calcul exact des pixels par mètre garantit la qualité d'image ou de vidéo requise et exigée par le système vidéo.

Attention au surdimensionnement !

Installer de plus en plus de caméras de manière irréfléchie n'est certainement pas la démarche à adopter. Ne serait-ce qu'en raison du volume des images et des données générés pas la haute résolution et un grand nombre de caméras. *« À cela s'ajoutent les coûts considérables qu'entraînerait une telle infrastructure surdimensionnée. Après tout, ce ne sont pas seulement les coûts d'acquisition des caméras elles-mêmes qui sont importants ici – les coûts des mâts de caméra appropriés, du câblage pour l'alimentation électrique et la transmission des données, etc., sont encore plus élevés,* insiste Erik Ashani. *Aux coûts d'acquisition uniques s'ajoutent les coûts de gestion et d'administration courants. Lors des décisions d'achat, les coûts indirects cachés, qui résultent d'une utilisation infructueuse par l'utilisateur final, sont souvent complètement ignorés – ces coûts indirects peuvent représenter près de la moitié des coûts totaux ! L'objectif doit donc être de trouver une solution grâce à laquelle le moins de caméras possible puisse couvrir une vaste étendue de manière plus efficace et plus fiable. C'est ce que nous proposons avec notre solution à capteurs multifocaux Panomera. »*

© DR

Dôme PanoVu DS-2CD6984G0-IHS de Hikvision. Ce dôme, conçu pour des applications en extérieur, jouit d'une résolution maximale de 8160 × 3616 à 30 ips en mode d'affichage panoramique et est doté de 4 leds IR pour voir jusqu'à 20 m de distance.

© DR

CÔTÉ SOLUTIONS

La qualité d'image sans compromis chez Axis Communications

Équipée d'un zoom 4x et d'un capteur CMOS couleur rétroéclairé 4/3, la caméra réseau Axis Q1798-LE est certifiée IP66, IP67 et IK10. Elle peut également supporter des températures extrêmes allant de -40 °C à -60 °C. Axis Communications a équipé cette caméra réseau de fonctions de sécurité comme le firmware signé et le démarrage sécurisé. Elle embarque également la technologie Axis Lightfinder 2.0 qui permet d'augmenter la sensibilité à la lumière, d'attribuer des couleurs plus naturelles dans l'obscurité et d'améliorer la netteté sur des objets mobiles. De plus, l'éclairage IR intégré à la caméra offre une surveillance discrète dans l'obscurité totale, allant jusqu'à 50 m, voire plus selon la scène.

LE POINT DE VUE D'UN FABRICANT

MATTHIEU LUCAS
Chef de marché sécurité chez Bosch Security and Safety Systems

© DR

« TOUT EST AFFAIRE D'ÉTUDES, D'ANALYSES. IL N'Y A PAS DE SOLUTION MIRACLE. »

« Choisir entre la très haute résolution et des caméras plus standards est avant tout affaire d'étude des besoins de l'utilisateur, du site, de son environnement, des pixels par mètre nécessaires pour travailler… Par exemple, une simple caméra Full HD avec une focale adaptée peut suffire pour faire de l'identification. Par ailleurs, jusqu'à maintenant, dans des environnements à fortes contraintes de luminosité, le 720 p ou le Full HD était la solution qui s'imposait. Aujourd'hui, les caméras 4K avec un bon capteur peuvent remplacer le 720 p ou le Full HD. Et des solutions comme notre Flexidome IP starlight 8000i en version 4K permettent de migrer facilement vers la haute résolution. Quoi qu'il en soit, il n'existe pas de solution qui s'impose *a priori.* Sans une étude préalable, on risque de se retrouver avec une installation sur-dimensionnée, nécessitant une infrastructure plus conséquente et aux coûts induits importants… »

2 QUESTIONS À

PHILIPPE BÉNARD

Business Development Manager A&E chez Axis Communications

© DR

Comment choisir entre résolution standard et haute, voire très haute résolution ?
On peut d'abord rappeler un principe simple en se basant sur l'arrêté de 2007 qui définit un élément : les 400 p/m pour faire de l'indentification. Ajoutons à cela qu'il faut disposer de 150 p/m pour faire de la reconnaissance et de 50 p/m pour filmer de l'ambiance. On s'aperçoit donc que le 1080 p peut suffire dans des applications dans lesquelles l'environnement est maîtrisé, comme dans le tertiaire. En revanche, pour des applications urbaines, le 4K peut être utile pour filmer des points de passage plus larges et identifier des personnes. Dans les centres commerciaux où l'on doit souvent surveiller un grand nombre de portes, par exemple, le 4K est aussi pertinent, en tenant compte de certaines contraintes comme les contre-jour, l'environnement qui peut être plus ou moins maîtrisé, les variations de luminosité entre le jour et la nuit… Avant de s'équiper, il faut donc se poser les bonnes questions : les caractéristiques de la caméra sont-elles adaptées à leur environnement ? La caméra est-elle designée pour son environnement ? Etc.

Quels conseils peut-on donner aux potentiels utilisateurs de caméras haute résolution ?
Ils doivent être vigilants et comprendre que la haute résolution n'est pas une panacée, une solution miracle. Mal conçue, une installation sera très chère et induira des coûts indirects importants. L'utilisateur et son installateur doivent faire appel à des fournisseurs disposant d'une large gamme de caméras, en matière de résolution et de design (bullet, box, etc.), afin de choisir celles les plus adaptées à l'environnement dans lequel elles seront déployées, aux besoins de l'utilisateur et à ses contraintes.

© DR

La nouvelle gamme Eye-Sight se compose de caméras dont les résolutions disponibles vont du 2MP au 8MP, en passant par le 4MP.

CÔTÉ SOLUTIONS

La haute résolution panoramique chez Hikvision

La caméra panoramique Fisheye (réf. DS-2CD63C5G0-IVS, avec objectif Immervision) est dotée d'une lentille Panomorphe, d'un capteur CMOS à balayage progressif de 12MP ainsi que de composants électroniques très performants de dernière génération. Elle fournit ainsi des vues à 360° avec des images en haute résolution et en temps réel. Les capacités matérielles et logicielles de « Dewarping » offrent à cette caméra une autonomie idéale et une capacité d'intégration parfaite avec 18 modes d'affichage différents. Les fonctions d'analyse Deep Learning sont également au rendez-vous avec six analyses comportementales, trois détections d'exception, la carte de chaleur « Heatmap » et même l'analyse vectorielle de fréquentation aux intersections pour le retail.

© DR

LE POINT DE VUE D'UN FABRICANT

BRIAN AWAD

Directeur pré-ventes chez Hanwha Techwin France

© DR

« ATTENTION À L'ENVIRONNEMENT LUMINEUX ET À LA BANDE PASSANTE. »

« Nous entendons de plus en plus parler de 4K (8MP) voire, chez Hanwha Techwin, de 8K (32MP) qui sont des résolutions jusqu'à 16 fois supérieures au Full HD. Le 8K permettra d'avoir un champ de vision large avec un maximum de détails et ce même sur de longues distances. Son utilisation est idéale pour protéger de grandes places en milieu urbain, des tribunes de stade ou encore des halls d'aéroports.
Le Full HD peut suffire dans la plupart des cas. Nous utilisons cette résolution sur tous nos marchés verticaux, comme l'urbain, le bancaire, le transport, le retail ou le tertiaire.
Dans certains cas, et avec certaines technologies, comme la détection d'intrusion ou la détection de température dans l'image, nous pouvons descendre sur des résolutions de type QVGA ou VGA. Pour ces besoins, il ne faut pas beaucoup d'information, il faut qu'elle soit juste. Nous utilisons des caméras thermiques ou radiométriques de la gamme Wisenet T pour satisfaire la captation d'image. Le point de vigilance en très haute résolution sera l'environnement lumineux et les optiques doivent être d'une extrême qualité pour laisser passer la lumière et l'image sans la déformer sur le capteur vidéo. Hanwha Techwin fabrique ses propres lentilles et objectifs. Enfin, pour minimiser le débit, il faut exploiter les codecs de compression les plus récents comme le H.265 en les couplant à des algorithmes de compression complémentaires comme notre Wisestream II. »

OPTIMA 360

OÙ QUE VOUS SOYEZ,
GARDEZ LE CONTRÔLE DE VOTRE SYSTÈME
DE SÉCURITÉ EN TEMPS RÉEL.

- OPTIMA 360, nouveau module de Supervision d'OPTIMA Box -

EDEN INNOVATIONS

LA SÉCURITÉ EN TOUTE SÉRÉNITÉ

www.eden-innovations.com

Marques intégrées avec la solution OPTIMA Box :

HIKVISION alhua STid HID RISCO VANDERBILT Honeywell GALAXY UZ Uhlmann & Zacher

Une collectivité ou une entreprise peut avoir rapidement des centaines de clés à gérer. Difficile de s'y retrouver et de tracer les pertes sans passer par des solutions électroniques.

© deister electronic

Bien gérer ses clés

La gestion des clés est un casse-tête qui empoisonne le quotidien de nombreux responsables de site. Savoir en temps réel qui est en possession de quelle clé et pouvoir réagir en cas de perte est un enjeu majeur de sécurité dans les entreprises. Du tableau à clous nouvelle génération à la clé dématérialisée, en passant par les armoires électroniques et les clés électroniques, divers systèmes permettent au gestionnaire de tracer les clés avec efficacité et de limiter les pertes.

Qui a pris la clé ? Où est la clé ? Mais qui n'a pas refermé le local ? Des questions récurrentes qui viennent polluer le quotidien des responsables de services généraux et de sécurité, et qui prennent de l'ampleur – et du temps – lorsque le nombre de clés en circulation augmente.

Sans compter que lorsque la clé a vraiment disparu, la question de la sécurité se pose sérieusement : combien d'accès peut-on ouvrir avec la clé perdue ? Ces accès sont-ils sensibles ? Faut-il changer les cylindres et refabriquer des jeux de clés ? Jean-Marc Brunet, directeur commercial de deister electronics, le reconnaît : *« C'est souvent au niveau des clés que se trouve la plus grande faille de sécurité en entreprise. Au bout de quelques années, il n'est pas rare que les gestionnaires ne soient plus en mesure de dire qui possède des clés, et surtout combien se retrouvent dans la nature. La gestion des clés devient un enjeu de sécurité majeur, y compris pour des PME. »*

Donnant-donnant, un premier pas dans la traçabilité

Le cahier sur lequel sont consignés les emprunts – encore très utilisé – montre rapidement ses limites et ses contraintes : mises à jour aléatoires, manque de disponibilité du gestionnaire, obligation pour le responsable d'être physiquement présent à la collecte et au dépôt. La première solution – la plus aisée – est un tableau mécanique donnant-donnant, comme celui proposé par Gesclés. Le principe est simple : pour pouvoir retirer une clé du tableau, il faut fixer en échange un « tag » ou « peg » identifiant. Une solution facile et efficace pour les petites structures et petits budgets, qui permet d'identifier l'emprunteur, mais qui trouve rapidement ses limites s'il y a trop de « tags » de retrait en circulation.

Qui et quand ? Les armoires électroniques

Les tableaux et les armoires électroniques, comme ceux proposés par Heure et Contrôle ou deister electronics, vont permettre non seulement de tracer l'emprunteur, mais aussi de savoir

3 QUESTIONS À

LAURENT LE BON

Direction Technique & Sécurité, Ville de Malakoff (92)

© DR

Quels sont vos enjeux en termes de gestion de clés ?
Malakoff est une collectivité territoriale de 30 000 habitants et de 50 sites.
Nous recherchions un système de sécurité sur le long terme, adaptable sur nos bâtiments existants, tout en limitant les frais d'installation et de maintenance.

Pourquoi avoir sélectionné iLOQ ?
L'avantage compétitif d'iLOQ a été d'équiper rapidement nos bâtiments, en respectant parfaitement notre cahier des charges, avec une plateforme de gestion simple d'utilisation.
Par son absence de pile dans le cylindre et dans la clé, les coûts d'entretien sont minimisés. Véritable solution écologique et économique, la GreenTech iLOQ est unique au monde.
La possibilité de programmer nos clés, en interne, depuis le logiciel iLOQ S10 Manager (ajout, modification ou suppression des droits d'accès), nous donne une souplesse de gestion adaptée à nos besoins, et nous permettant de maîtriser nos accès. Les clés perdues peuvent être blacklistées, puis reprogrammées si elles sont retrouvées. iLOQ S10 nous permet de résoudre les problèmes de copie ou de perte de clés grâce à une remise en fonction rapide des droits d'accès. Ce sont des avantages non négligeables pour une collectivité puisque nous pouvons désormais répondre au plus vite aux besoins des utilisateurs sur plusieurs sites géographiquement séparés.

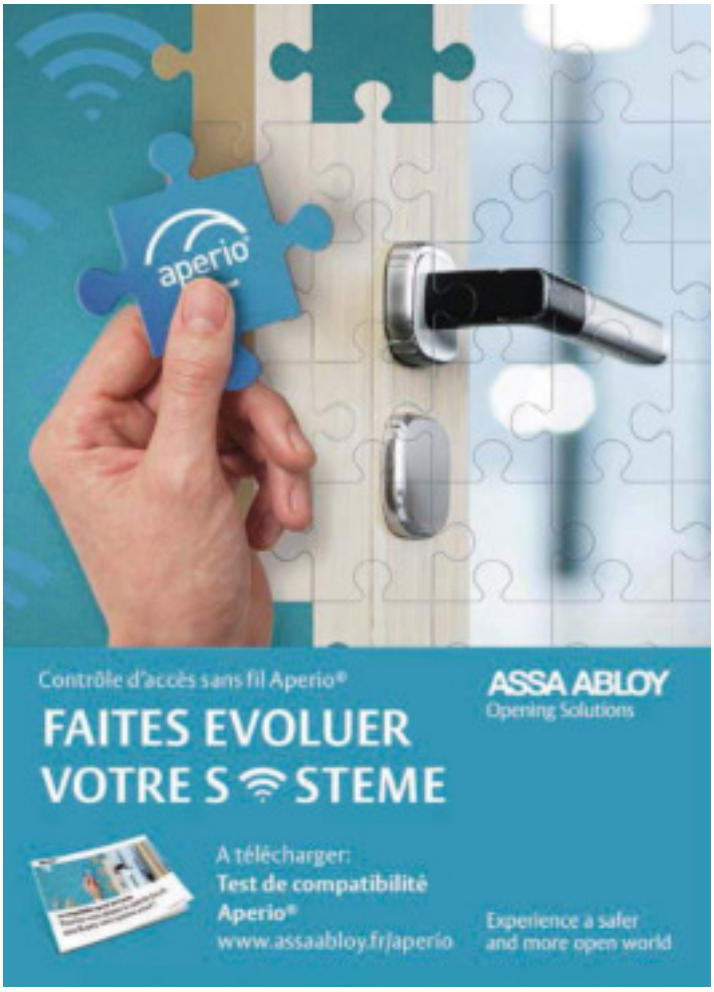
Allez-vous étendre ce système ?
Un premier pilote de 135 cylindres iLOQ S10 a été réalisé sur le centre municipal de santé et son annexe, des bâtiments classés comme sensibles, en raison des différents niveaux de droits d'accès. Le test ayant été entièrement concluant et les utilisateurs satisfaits, davantage d'installations sont en déploiement dans la ville de Malakoff, comme l'hôtel de ville, le centre technique municipal, les groupes scolaires et les équipements culturels et sportifs.

quand les clés ont été empruntées. Ces armoires gérées électroniquement via un logiciel déporté ou directement sur un moniteur intégré à l'armoire, donne également un historique des clés. Les clés sont accrochées à des tags RFID. Pour pouvoir emprunter, l'utilisateur va présenter son badge devant le lecteur de l'armoire, qui va s'ouvrir. La ou les clés pour lesquelles, il a des droits va se libérer – éventuellement indiquées par un signal lumineux. Pour le retour, il suffit de présenter la clé et son tag devant le lecteur pour rouvrir l'armoire et l'insérer à l'emplacement libre. Un outil utile pour savoir quelles sont les ● ● ●

© DR

Logiclés : la gestion des clés en ligne de Dény Security

Ce logiciel est centré sur la gestion de trousseaux. Il permet de mettre en place très simplement un système efficace de traçabilité des trousseaux. Le client peut accéder très facilement à la gestion de son organigramme depuis tout ordinateur connecté. Il lui suffit de se connecter sur son espace sécurisé sur le site de Dény Security. L'organigramme est mémorisé ainsi que toutes les informations concernant les clés et les cylindres. Lorsque le gestionnaire entre des informations ou modifie son organigramme, la mise à jour est automatique. En cas, par exemple, de clé non rendue, une alerte est envoyée à l'administrateur qui peut la rechercher et relancer le porteur.



LA MAIRIE DU PERREUX-SUR-MARNE PASSE AUX CLÉS ÉLECTRONIQUES

« La gestion des clés physiques peut devenir un vrai cauchemar, assure Stevenson Olibrice, référent IT de SimonsVoss Technologies. Par exemple, la mairie de Le Perreux-sur-Marne, possédait plus de 800 clés différentes dans son local, dont une grande partie ouvrait plusieurs portes (pass partiels et généraux). De plus, de nombreuses personnes (associations, intérimaires...) viennent pour des périodes relativement courtes, pour des interventions ponctuelles, ce qui multiplie le nombre de clés à dupliquer – mais aussi le nombre de pertes, avec pour corollaire un budget très élevé pour le remplacement des cylindres et des clés, certaines clés pouvant se facturer à plus de 80 euros. Nous remplaçons peu à peu l'ensemble des cylindres mécaniques ou selon les portes, des béquilles, par des cylindres numériques et béquilles électroniques, ce qui permet une traçabilité et une désactivation facile des badges en cas de perte. La robustesse de nos systèmes a également joué en notre faveur puisque nous nous engageons sur 300 000 manœuvres avant le changement de piles pour notre dernière innovation, la SmartHandle AX. »

● ● ● dernières personnes à avoir accéder à un local ou à avoir emprunté un véhicule. *« Nos armoires,* précise Jean-Marc Brunet de deister electronics, *permettent de savoir en temps réels qui a emprunté les clés, et d'établir une remontée d'événement des retraits et dépôts de celles-ci. De plus, nos armoires sont interopérables avec les systèmes de contrôle d'accès de contrôle d'accès. Le salarié pourra utiliser son badge Mifare, Desfire ou tout autre technologie en place dans l'entreprise (badge dématérialisé, biométrie, ou tout simplement code) pour accéder aux clés. Un système sûr, accessible 24 h/24 qui permet non seulement d'améliorer la sécurité des locaux mais simplifie considérablement la planification des ressources. »*

LA PAROLE À

STÉPHANE ABBOU
Directeur des ventes Assa Abloy

© DR

« LES CLÉS MÉCANIQUES ÉGARÉES SONT UNE DES PRINCIPALES FAILLES DE SÉCURITÉ DANS LE CONTRÔLE D'ACCÈS. »

« Lorsque l'on interroge les clients sur les process en cas de pertes de clés, on se rend compte que, bien souvent, aucune action n'est entreprise en raison du coût que représente le changement de cylindres à chaque perte, coût d'autant plus élevé s'il s'agit d'un pass. La prise de conscience du risque que peut représenter des clés dont on a perdu la trace, amène les clients à considérer le passage d'un organigramme mécanique à un électronique, avec une gestion de droits. En fonction du type d'établissement, on proposera une solution qui pourra être installée progressivement et assurer une traçabilité sur les accès. Par exemple, dans un immeuble tertiaire, déjà utilisateur de contrôle d'accès à badge RFID, on orientera le client vers des lecteurs sans fil Aperio, qui pourront être intégrés au système existant. Pour des sites industriels avec des accès distants, on conseillera plutôt un système de clés électroniques – avec l'énergie portée par la clé comme Cliq ou Cliq Connect. Pour ceux qui ont déjà sur site des clés Assa Abloy, on pourra faire une bascule avec une clé mécatronique Protec2 cliq qui permet d'ouvrir à la fois des accès électroniques et mécaniques avec une seule et même clé. Comme, il est parfois compliqué et onéreux de changer l'ensemble des cylindres, nous préconisons de commencer par les zones les plus stratégiques et d'ouvrir les accès moins stratégiques avec cette même clé en mécanique uniquement sur la période de transition. Le retour sur investissement que nous pouvons calculer et la traçabilité obtenue sont des arguments en faveur d'un basculement sur des systèmes électroniques. »

Gérer les clés et bien plus

Lorsque l'utilisateur remet sa clé, il peut également apporter des informations liées à son activité. Ainsi, dans le cas de gestion de flotte, en rapportant la clé de son véhicule, le conducteur pourra indiquer sur l'écran des informations telles que la nécessité d'une réparation, le niveau de carburant, le kilométrage, comme le propose Heure et Contrôle avec son Vigipad Auto, un outil qui s'interface aux outils de gestion de flotte et contribue à l'amélioration du suivi des véhicules. Outre les meubles, ce sont aussi les logiciels qui assurent la gestion de l'organigramme qui peuvent se présenter sur poste fixe, sur l'armoire de retrait ou même en

SOLUTIONS PRODUIT

Vigipad Auto, pour gérer les clés des flottes de véhicule

Le Vigipad Auto est un gestionnaire électronique de clés de véhicule avec des fonctionnalités qui permettent, via un tableau de bord, de voir les véhicules utilisés, les réservations, rapports, statuts, etc. À chaque mouvement, le Vigipad Auto se synchronise automatiquement. La traçabilité en est ainsi assurée. Le conducteur qui se connecte peut également réserver un véhicule et signaler des événements (réparations à effectuer). L'administrateur peut choisir quel véhicule sera attribué en priorité selon des critères définis à l'avance : carburant le plus élevé, kilométrage le plus bas, droits d'accès, etc. Il peut aussi rendre indisponible des véhicules pour la maintenance ou une réparation. Capacité 8 à 144 clés. Cette armoire peut gérer jusqu'à 10 000 utilisateurs et véhicules.

© DR

ligne. Pour les clés mécaniques, le mot d'ordre est simplicité. Jean Balmy de Dény Sécurity l'assure : *« Nous avons conscience que, dans les PME, les gestionnaires de clés ont d'autres fonctions et que cette activité est particulièrement chronophage. C'est la raison pour laquelle nous avons développé un outil en ligne de gestion d'organigramme, Logiclés. Très simple et ergonomique, son but est de libérer du temps au responsable pour ses tâches essentielles, tout en gardant un suivi optimal des droits d'accès et du parc de clés. »*

Quel usage de la clé ?

Si les systèmes à armoires électroniques permettent de savoir qui a pris la clé et quand, elles n'indiquent pas en revanche si les accès ont ou non été utilisés. Le seul moyen de le savoir est alors de basculer son système d'accès mécanique en système électronique, via des clés électroniques ou mécatroniques, ou même des badges. À première vue, le changement semble onéreux. *« C'est à mettre en regard avec le coût de changement de cylindres en cas de perte de clés,* explique Stéphane Abbou, d'Assa Abloy. *Sur l'année, surtout en cas de perte de clé maître, ce sont plusieurs milliers d'euros qui doivent être investis. Alors qu'en passant à des cylindres électroniques et des clés électroniques ou des badges, on annule simplement les droits du porteur pour en créer de nouveaux. De plus, il n'est pas nécessaire de tout passer en une seule fois en électronique. Le chan-* ● ● ●

2 QUESTIONS À

JEAN BALNY

Chef de produit Dény Security

© DR

Comment peut-on gérer son parc de clés de façon optimale ?
Le plus important dans la gestion des clés est de s'assurer de la traçabilité. La méthode la plus traditionnelle – qui peut convenir pour de petites structures est l'armoire à clés. Par ailleurs, nous avons développé deux logiciels de gestion de clés : un logiciel embarqué sur PC et un géré via un portail Web, Logiclés.

Pourquoi développer un logiciel accessible sur le Web ?
Nous nous sommes rendu compte que de nombreux clients, lorsqu'ils doivent mettre à jour l'organigramme sur un poste fixe, ne le font pas, faute de temps ou de disponibilité. Pour des organigrammes de taille raisonnables (moins de 500 cylindres), le logiciel en ligne prend en charge toute la partie organigramme. Le client n'a plus qu'à remplir la gestion de trousseaux. En cas d'oubli de remise de clés, le gestionnaire est alerté. Un système simple qui soulage le responsable et lui permet de gagner un temps précieux.

3 QUESTIONS À

PHILIPPE WELLARD

Directeur général, Heure et Contrôle

© DR

Pourquoi vous consacrez-vous à la gestion des clés ?
La gestion des clés peut être considéré comme le parent pauvre de la sécurité. C'est une tâche fastidieuse et chronophage qui rebute la plupart des responsables de service généraux ou de sécurité. Il n'est pas rare que dans des sites ultra-sécurisés, les clés soient simplement laissées dans un tiroir ou une armoire sans véritable suivi. Depuis vingt-cinq ans, Heure et Contrôle propose des outils de gestion des clés fiables, qui facilite la tâche du gestionnaire et permet de tracer les clés physiques.

Quels outils proposez-vous ?
Des armoires électroniques spécifiques. Elles présentent l'avantage d'être autonomes, fiables, accessibles 24 heures sur 24 aux personnes autorisées. En un clic, on peut tracer une clé et connaître l'emprunteur. C'est souvent aussi un outil de responsabilisation des utilisateurs qui auront tendance à faire plus attention aux clés. Actuellement, Heure et Contrôle est l'entreprise qui a le parc le plus important d'armoires de gestion de clés implantées en France.

À quels types de clients vous adressez-vous ?
Nos donneurs d'ordres sont des entreprises d'une centaine à plusieurs dizaines de milliers de salariés et nous travaillons dans tous les secteurs : de la grande distribution au nucléaire en passant par des musées ou des municipalités. Des profils très différents qui ont en commun le besoin de fiabiliser la traçabilité de leurs clés physiques avec un outil simple.

gement peut se faire progressivement en ciblant prioritairement les zones sensibles. » Les fabricants proposent des cylindres électroniques qui peuvent s'insérer à la place de la plupart des cylindres mécaniques standards. Le changement peut être fait à l'occasion d'une perte de clé ou d'une rénovation, pour limiter les coûts.

Tester le système

Passer de clés mécaniques à des clés électroniques peut susciter des interrogations sur le bénéfice réel. Lancer un pilote de clés électroniques sur un échantillon de sites, c'est l'approche originale que propose iLOQ, dans le but de démontrer à ses clients les performances du cylindre et de la clé S10. « *Les entreprises sont plutôt étonnées de notre système qui permet à la fois d'avoir une gestion électronique des clés avec traçabilité des accès, et l'absence totale de pile, de batterie ou encore de câblage. C'est l'introduction de la clé qui va fournir l'énergie nécessaire à la reconnaissance des droits d'accès et donc à l'ouverture,* explique Julie Bismuth, responsable marketing iLOQ France. *L'efficacité de notre système est régulièrement éprouvée sur une partie significative du parc, comme dans la Ville de Malakoff, où le test a été réalisé sur les 135 accès du centre municipal de santé. L'implantation est rapide et les frais d'installation et de maintenance limités, puisqu'il suffit de remplacer les cylindres sur une base de profil européen standard. La prise en main du logiciel de gestion des droits d'accès, iLOQ S10 Manager, est très simple. L'administrateur retrouve une gestion de clés électronique classique, tout en éliminant les inconvénients, notamment des changements de pile. Jusqu'à présent, les clients qui ont pu tester notre solution l'ont adoptée. Autre avantage, la modularité native des cylindres avec des rallonges et la progressivité : le changement peut être fait au fur et à mesure et en fonction du budget, ce qui est très apprécié dans le secteur public et privé.* »

La fin des clés mécaniques ?

« *Qu'on le veuille ou non, il y a toujours des clés stratégiques qui ouvrent des accès, des coffres ou des meubles et qui n'entrent pas dans un schéma global du contrôle d'accès à badges ou à clés électroniques. Sécuriser ces clés mécaniques et les tracer reste indispensable et, jusqu'à présent, les armoires électroniques associées à un logiciel de gestion fiable constituent la meilleure solution pour tracer ces clés et leurs utilisateurs.* », conclut Jean-Marc Brunet. ■

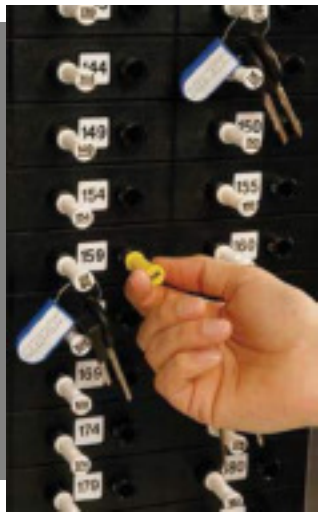
© DR

Commander Connect, le pilote 360 des solutions de deister electronic

Ce logiciel Commander Connect permet de piloter les armoires à clés de deister electronic. Les utilisateurs habilités à se connecter au réseau de l'entreprise, en local ou à distance, disposent ainsi de nombreux outils. La prise et la remise de la clé fait l'objet d'un traitement de la part du système qui va remonter l'information dans le logiciel de sorte que l'administrateur puisse savoir à tout moment qui est en possession de celle-ci. L'administrateur est donc capable de déterminer qui possède les clés, planifier des autorisations ou des restrictions, libérer des clés à distance, etc. Ce logiciel, interopérable avec les solutions de la plupart des fabricants de contrôle d'accès, permet également d'accueillir des modules pour des applications spécifiques : module de management de flotte de véhicules, module de réservation pour salles de réunion.

Clé manager de Gesclés : le high-tech du tableau à clous

Simplissime et bon marché, ce tableau mécanique de gestion de clés fonctionne sur le principe du donnant/donnant. Chaque utilisateur possède un ou plusieurs pegs de retrait identifiés. Ce dernier doit être inséré pour libérer le peg de rétention où le trousseau est accroché. Il restera accroché le temps de l'utilisation du trousseau. D'un simple coup d'œil, le responsable peut savoir qui a emprunté les clés. Une solution idéale pour les petites structures disposant d'un budget réduit.



© gesclés

DU CÔTÉ DES START-UP

Osmokey, la gestion de clés des résidences temporaires

Spécialiste du tourisme connecté des IOT dédiés aux campings et résidences de vacances, Osmozis a développé Osmokey, une serrure connectée qui permet l'accès facile aux logements et services d'un établissement via un bracelet RFID ou un code. Premier utilisateur, le camping Robinson dans l'Hérault (34), qui trouve dans cette solution une réponse efficace à tous les vacanciers qui perdent régulièrement leurs clés. Pour les arrivées tardives, le client reçoit un code par SMS actif jusqu'au lendemain matin 11 heures, le temps de récupérer les bracelets de la famille des résidents. Cette serrure est également installée sur les locaux du personnel et les accès communs, ce qui leur facilite l'usage notamment pour la maintenance. La serrure s'installe facilement sur les portes existantes et fonctionne sur la base d'un réseau LoRaWan, totalement autonome et indépendant des réseaux installés.

© Osmozis

Satyx twin

Haute sécurité et réversible

- Système breveté.
- Protection contre la copie et l'effraction.
- Fonction « 2 en 1 » en cas de perte de clé.
- Pendant les travaux, seule la clé de chantier est fonctionnelle.

CYLINDRE DE HAUTE SÉCURITÉ

Access Control Solutions
and Services

contact@deny-security.com
+33 (0)3 22 30 26 01
www.deny-security.com

dēny
SECURITY

Les VMS (Video Management System)

Les VMS sont de plus en plus puissants et intuitifs pour le confort de l'opérateur devant son mur d'écrans. Quelques solutions actuellement disponibles…

VMS WISENET WAVE – HANWHA TECHWIN

EXPÉRIENCE UTILISATEUR

© Hanwha Techwin

Hanwha Techwin a lancé, l'année dernière, une mise à jour majeure de sa plateforme VMS Wisenet Wave. Dotée d'une longue liste de nouvelles fonctionnalités conçues pour améliorer l'expérience utilisateur, l'interopérabilité et la cybersécurité, Wisenet Wave 4.0 possède une architecture système améliorée qui garantit une haute disponibilité et permet un déploiement évolutif en fusionnant jusqu'à 100 serveurs dans le même système. Wisenet Wave 4.0 donne également la possibilité de fusionner les systèmes enregistrés dans WAVE Sync depuis un tableau de bord en ligne, éliminant ainsi la nécessité de configurer la redirection de ports lors des fusions à distance. L'interface utilisateur de Wisenet Wave a été entièrement repensée, avec notamment une réorganisation complète du volet des notifications, qui comprend désormais des onglets pour la détection des mouvements, les favoris, les événements et les objets, ainsi que des manières simples d'appliquer des filtres ou d'effectuer des recherches dans chaque onglet. Une nouvelle fonctionnalité « Layout-as-an-Action » permet d'ouvrir automatiquement une mise en page prédéfinie de l'écran lors de la détection d'un événement.

SECURITY CENTER 5.9 – GENETEC

PLATEFORME DE SÉCURITÉ UNIFIÉE

La nouvelle version de la plateforme de sécurité unifiée de Genetec, Security Center 5.9, s'enrichit de nombreuses nouveautés, parmi lesquelles une meilleure protection contre le sabotage des preuves vidéo, une fonctionnalité d'adressage public, ou encore une gestion plus facile et efficace des mises à jour du système. Les vidéos exportées utilisent désormais la signature numérique EdDSA, qui protège plus efficacement contre le sabotage et la fraude. Grâce à un tatouage numérique, intégrant notamment en filigrane le nom de l'utilisateur et celui de la caméra, il est possible de retrouver l'origine de toutes les séquences exportées : un bon moyen de dissuasion contre le partage non autorisé de vidéos.

Avec Security Center 5.9, Genetec présente la version 2.9 de Sipelia, son module de gestion des communications unifiées. Cette version s'enrichit d'une fonctionnalité d'adressage public auprès de groupes de radiomessagerie, pouvant intégrer des dispositifs de communication tels que des interphones, des dispositifs de porte et des téléphones VOIP. Les opérateurs peuvent ainsi déclencher des messages enregistrés ou envoyer des communications en direct à des groupes d'appareils directement depuis leur interface de surveillance.

Pour les entreprises dont les cycles de mise à jour sont longs, Genetec Security Center 5.9 propose son nouveau support à long terme (LTS ou Long-Term Support). Grâce à des patchs légers et personnalisables, contenant des correctifs indispensables pour résoudre les défauts logiciels et les vulnérabilités critiques, les entreprises s'assurent d'être toujours protégées contre les menaces de cybersécurité, même entre deux longs cycles de mise à niveau.

© Genetec

Le 1er Salon Online
sur la Sécurité et la Sûreté !
e-salon-protectionsecurite.fr

© Securitron

IPS VIDEOMANAGER – SECURITRON

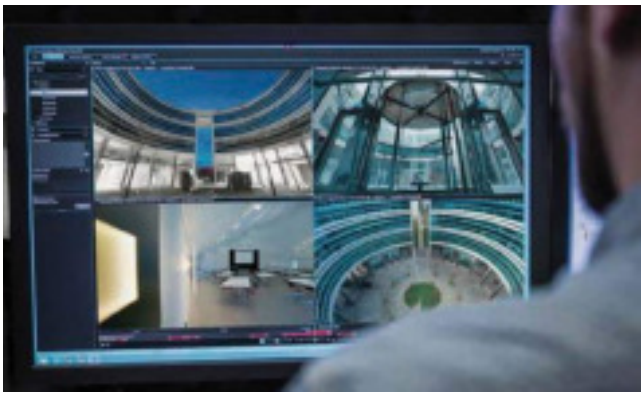
UN VMS QUI RÉDUIT LE STRESS DE L'OPÉRATEUR

IPS fournit un VMS avec suivi entièrement automatisé des objets détectés ce qui aide énormément le personnel de sécurité à toujours rester maître de la situation même en cas de stress élevé.
La technologie 3D innovante d'IPS associe une gestion vidéo puissante à une analyse vidéo de traçage intelligente le tout sous un géoréférencement 3D. La localisation précise et le suivi des objets à l'aide des images de caméra et de cartes géoréférencées sont ainsi grandement simplifiés.
Dans des cas de situations critiques et donc stressantes, votre personnel de sécurité peut se concentrer sur toutes les tâches autres que le contrôle des caméras qui est pris en charge par le VMS 3D d'IPS et se fait entièrement automatiquement. Avec la technologie IPS 3D, les grands sites peuvent être parfaitement et intégralement couverts. De plus, différents systèmes de sécurité (tels que le contrôle d'accès, la détection de clôture, l'alarme vocale, etc.) peuvent être reliés entre eux. En règle générale, le personnel de sécurité n'a pas à traiter quotidiennement des cas d'alarmes critiques. Lors d'un incident critique, on exige beaucoup des opérateurs dans un centre de sécurité. Ils doivent constamment commuter manuellement les caméras ou contrôler les caméras PTZ via le joystick. D'où l'intérêt d'utiliser IPS VideoManager.

SIVEILLANCE – SIEMENS

GESTION DE 4500 MODÈLES DE CAMÉRAS

Siveillance VMS de Siemens permet de gérer plus de 4500 modèles de caméras réparties sur un ou plusieurs sites. Cette plateforme logicielle innovante offre à l'opérateur un large éventail d'outils et de fonctionnalités conçus pour simplifier la gestion des équipements de vidéosurveillance, analyser les vidéos et optimiser le stockage des données grâce à une solution centrale ou décentralisée. La solution permet en effet, à partir d'un seul écran, la visualisation globale d'un site de grande taille et la gestion de l'ensemble des événements du plus simple au plus critique. Siveillance VMS donne accès à une lecture directe ou différée des vidéos avec trois types d'affichages possibles en fonction des compétences des différents utilisateurs (client vidéo, affichage Web et mobile). Le système peut, par ailleurs, être intégré à la plateforme d'hypervision multimétier Desigo CC rendant interopérable toutes les applications du bâtiment (détection incendie, gestion des flux de personnes, détection intrusion et automatisation du bâtiment).
Siemens propose Siveillance VMS dans trois versions différentes, adaptées à toutes les typologies d'entreprises et de sites : VMS 100 pour les petites et moyennes entreprises ; VMS 200 pour une surveillance en temps réel élaborée ; VMS 300 pour de vastes installations de haute sécurité incluant un nombre illimité de caméras et de serveurs.



© Siemens

© CASD

VISIMAX, VERSION 8.8 – CASD

TROIS INNOVATIONS MAJEURES

CASD a lancé sur le marché des VMS le tout dernier VisiMax : la version 8.8. Trois innovations majeures viennent compléter un panel de fonctionnalités déjà impressionnant et au plus près des attentes des utilisateurs : la géolocalisation des patrouilles sur le terrain dans le SIG (en partenariat avec la société Sysoco), la prise en charge de l'accélération matérielle (GPU) et la visualisation du parc caméra via le SIG dans le portail Web, disponible sur n'importe quel smartphone ou tablette.

→ **CARACTÉRISTIQUES :**

- Géolocalisation des signaux de radiocommunication.
- Prise en charge de l'accélération matérielle (GPU).
- Visualisation des caméras via le SIG dans le portail Web.

Pour des sites sensibles ou de grande taille, on privilégiera les systèmes anti-intrusion filaires.

© Getty Images

Radio ou filaire ? Il faut choisir

Le choix n'est pas si simple qu'il n'y paraît. Chacune des technologies – sans fil ou filaire – a de réels arguments à faire valoir. Encore faut-il que la solution retenue soit adaptée à votre site et ses contraintes.

Avant tout, rappelons quelques principes simples. Avant de choisir votre système de lutte contre l'intrusion – radio ou filaire – on ne peut que vous conseiller de faire appel à un professionnel qui viendra chez vous, sur votre site, afin de réaliser une analyse de vos risques qui lui permettra ensuite de choisir la solution et les technologies les plus adaptées. Ce que ne fait pas, malheureusement, la banque-assurances qui vend aujourd'hui des systèmes de lutte contre l'intrusion. Ce qui peut en soi se comprendre car leur modèle économique est de faire du volume en poussant essentiellement des systèmes radio qui s'installent plus vite que les solutions filaires. Il leur est donc difficile d'envoyer chez vous un installateur, certifié ou pas, pour réaliser une analyse de risques digne de ce nom. Ceci posé, comment choisir, arbitrer entre le sans fil (radio) et le filaire ?

Le filaire pour le durci ?

« En matière de solutions contre l'intrusion, il faut distinguer les systèmes sans fil qui pourront être utilisés pour assurer la sécurité dans le résidentiel et pour les petites installations comme les petits commerces…, avec un nombre de points de détection réduit, des systèmes filaires qu'on installe généralement sur des sites plus importants, plus sensibles, avec plusieurs centaines de points de détections, précise d'entrée Ivan Marciano, directeur générale d'ITQ Group et président de GPMSE Technologies numériques. *Par ailleurs, pour choisir son système, filaire ou sans*

UNE RÈGLE EXIGEANTE

La règle Apsad R81 s'applique aux installations de détection d'intrusion réalisées dans tous les types de sites ou de bâtiments quels qu'en soient la surface totale et l'usage. Elle définit les exigences techniques minimales auxquelles doivent répondre les systèmes de détection d'intrusion.

fil, il faut avoir présent à l'esprit que, dans de nombreux cas, les fabricants de solutions sans fil privilégient encore des protocoles "propriétaires". Ce qui n'est pas le cas avec le filaire pour lequel il est tout à fait possible d'associer à une centrale d'une marque des détecteurs d'une autre. »

Chez le Français Septam, Laurent Binon, son directeur commercial, constate que *« depuis une quinzaine d'années, le radio progresse fortement. Son gros point fort étant sa facilité d'installation qui en fait une technologie* a priori *idéale pour être installée dans le résidentiel ou dans les petits commerces, parfois au détriment de la véritable sécurité. Le radio est fortement poussé par le monde de la banque-assurances via des offres locatives adossées à de la télésurveillance. Il faut reconnaître que le radio a beaucoup évolué. Il est aujourd'hui plus fiable chez les fabricants sérieux mais on ne peut que conseiller, en la matière, de choisir des solutions sans fil certifiées NFA2P afin d'éviter bon nombre de produits "exotiques" disponibles sur le marché. »*

Des contraintes

Chaque système, filaire ou sans fil, a ses contraintes et inconvénients. Le filaire nécessite plus de travaux lors de son installation. Le coût de cette dernière sera donc plus élevé. *« En revanche,* ajoute Ivan Marciano, *on pourra déployer un plus grand nombre de capteurs avec le filaire, alors que leur nombre sera beaucoup plus limité pour les systèmes sans fil. Autre atout du filaire : la plupart des VMS proposés par Genetec, Milestone et consorts pourront supporter* ●●●

Chez Bosch Security, les quatre centrales de la gamme B et G Series répondent aux besoins d'applications de moyennes et grandes tailles et peuvent gérer de huit à 96 zones (B Series) et de 16 à 599 zones (G Series).

PAROLE D'EXPERT

LAURENT BINON
Directeur commercial chez Septam

© DR

« IL N'EXISTE PAS DE CERTIFICATION TYPE 3 POUR LE FULL RADIO. »

« Selon moi, et malgré les progrès indéniables en termes de fiabilité des systèmes sans fil, plus les exigences sécuritaires sont fortes, plus on doit s'appuyer sur une solution intrusion filaire. D'ailleurs, il faut souligner qu'il n'existe pas, sur le marché, de solution Full radio certifiée type 3. Leur certification se limite au type 2. Certes, le radio est facile à installer. Mais cette facilité est aussi une faiblesse. Elle encourage certains "installateurs" aux compétences douteuses à se croire capables de déployer ce type de solution anti-intrusion. Ces installateurs, peu professionnels, négligent bien souvent, par ailleurs, de réaliser une étude des risques digne de ce nom… Enfin, à l'heure où tout le monde parle d'écologie, de développement durable…, rappelons que les systèmes radio fonctionnent avec des piles lithium. Soit plusieurs centaines de milliers de piles à recycler… Comment ? »

2 QUESTIONS À

LUC JOUVE

Président de Sécurité Alarme Service et du GPMSE Installation

© DR

Le filaire est-il plus intéressant que le radio ou inversement ?
Chacune de ces technologies a des avantages et des inconvénients. Par exemple, l'atout indéniable du radio est sa facilité d'installation et la possibilité de le déployer dans des locaux terminés, déjà occupés. Si le filaire ou le radio peuvent être déployés sur des sites similaires, il faut savoir que pour certains types de locaux, comme les petits commerces, les produits filaires pourront bénéficier d'une certification de type 3, le niveau le plus haut, alors que le niveau le plus élevé pour le radio sera le type 2. Il est donc difficile de dire, *a priori,* qu'une technologie s'impose. L'arbitrage entre le radio et le filaire ne peut se faire qu'à partir de l'analyse des risques qui est le préalable nécessaire à toute installation, comme le rappelle la règle Apsad R81. L'installateur certifié sera à même de conseiller utilement son client après l'analyse de risque.

Une technologie est-elle plus fiable que l'autre ?
Radio ou filaire, les deux fonctionnent bien. Mais le radio requiert des compétences importantes lors de son installation car il est plus complexe à déployer afin qu'il ne soit pas perturbé par son environnement. Le choix entre l'une ou l'autre ne peut se faire, selon moi, que du point de vue de la conformité avec la règle R81 et en respectant les prescriptions des assureurs.

● ● ● *les centrales filaires. Ce qui n'est pas le cas avec les systèmes radio. Mais ces derniers seront plus faciles et rapides à installer et à paramétrer. »*
Luc Jouve, président de Sécurité Alarme Service et du GPMSE Installation, ajoute : *« L'un des avantages du filaire réside dans le fait que, quelle que soit l'ancienneté du système ou sa marque, il sera possible de changer le matériel. On pourra changer la centrale et venir connecter les anciens détecteurs sur la nouvelle. Avec une installation radio, il y a neuf risques sur dix que les fréquences ne soient plus disponibles… et les systèmes sont la plupart du temps propriétaire. »* Avant de poursuivre : *« L'autre contrainte du radio est liée à la certification des solu-* ● ● ●

CÔTÉ SOLUTIONS

Harmonia 3 : 100 % française et certifiée NFA2P grade 3 !

La gamme Harmonia 3 est entièrement conçue et fabriquée en France, par Septam. Ces centrales sont certifiées NF&A2P 3 boucliers/EN grade 3. Équipée de huit entrées, les centrales Harmonia sont extensibles à 24, 64 et 128 entrées selon les modèles. Elles peuvent gérer jusqu'à 128 points et 122 sorties sur huit secteurs indépendants. Le logiciel H2Vision assure une supervision graphique jusqu'à dix centrales Harmonia ainsi que la gestion de la vidéosurveillance et du contrôle d'accès jusqu'à dix centrales Orchestra.

© DR

PAROLE D'EXPERT

IVAN MARCIANO

DG d'ITQ Group et président de GPMSE Technologies numériques

© DR

« DES AVANTAGES ET DES CONTRAINTES. »

« Outre les systèmes anti-intrusion purement filaires ou sans fil, on trouve aussi sur le marché des solutions hybrides qui permettent d'associer à une centrale filaire des modules radio pour des raisons esthétiques quand on ne peut pas passer de câbles dans un bâtiment ou un local. Mais les modules et la centrale doivent être de la même marque. Il s'agit donc de systèmes assez "fermés". Contrairement à ce que l'on croit, le radio n'a pas que des avantages. Il nécessite de la maintenance. Ne serait-ce que le remplacement des batteries tous les deux ou trois ans. Alors que le filaire ne requiert que peu de "consommables". Avec le sans fil, on doit également tenir compte de l'environnement qui peut perturber la transmission du signal et de la portée entre les différents composants de l'installation. En outre, la communication sans fil peut être brouillée par des brouilleurs. Cependant, l'indéniable avantage du sans fil est son coût réduit lors de l'installation. Le câblage du filaire, quant à lui, n'est pas nécessairement un point faible. Tous les éléments des systèmes filaires sont tous auto-protégés et envoient automatiquement une alarme en cas de rupture du signal ou de tentative d'ouverture. »

AX-HUB
868MHZ

CENTRAL D'ALARME AVEC ACCÈS VIDÉO

UNE PLATEFORME TOUT-EN-UN DE SOLUTIONS ALARME & VIDÉO

- Jusqu'à 32 détecteurs/capteurs sans-fil, 8 Keyfobs et 2 Sirènes Hikvision associables
- IVaas (Intruder Verification As A Service) qui supporte la vérification visuelle des événements jusqu'à 7 secondes pré/post alarme
- Compatible avec les caméras IP Hikvision ou les caméras IP tierce partie conforme aux standards ONVIF
- Intégrable avec iVMS, Hik-Connect et les centres d'alarmes
- Visionnage d'alarme via logiciel mobile/email

www.hikvision.com/fr @HikvisionFrance @hikvisionfr HIKVISION France HIKVISION

LE POINT DE VUE D'UN FABRICANT

HERVÉ HOUY
Directeur France chez Vanderbilt Industries

© DR

« FACILITER LE TRAVAIL DES INSTALLATEURS. »

« La demande de solutions intégrées et l'influence croissante de l'internet des objets (IoT) dans l'intrusion représentent un domaine auquel Vanderbilt accorde une attention particulière. La technologie sans fil atteint un stade de maturité, avec des capacités de communication bidirectionnelle qui renforcent son potentiel et sa fiabilité. La gamme de produits SPC sans fil de Vanderbilt a de nombreux avantages qui permettront de faciliter le travail quotidien des installateurs : portée sans fil plus grande (500 m champs libre) ; durée de vie de la pile plus longue (supérieur à cinq ans) ; pile courante, utilisée pour de nombreux produits (CR123A, AA, AAA), configurable "Over the Air" à travers le cloud SPC Connect (anti-animaux, sensibilité). Par ailleurs, notre centrale SPC permet de protéger les entreprises, les biens immobiliers et les équipements. Il s'agit d'un système de détection d'intrusion polyvalent doté d'un ensemble complet de fonctionnalités de gestion des alarmes. Grâce à l'utilisation de services basés sur le cloud, à des applications adaptées aux utilisateurs finaux et à une suite logicielle dédiée, SPC constitue un système de détection d'intrusion de premier plan. SPC est donc une solution de sécurité professionnelle reposant sur une infrastructure qui s'adapte facilement à l'évolution des besoins, qu'on utilise des composants sans fil ou une technologie filaire. »

● ● ● *tions. Si l'on travaille avec des produits certifiés, il y a de nombreuses contraintes, notamment à cause de la supervision qui peut être perturbée par un grand nombre de choses, et qui demande une forte expertise de l'installateur. Les produits non certifiés sont beaucoup plus simples à installer mais aussi beaucoup plus sensibles à la "casse", aux attaques cyber, au brouillage, etc. »*

Pour Laurent Binon, *« la radio reste de la radio. C'est-à-dire qu'elle sera toujours soumise à des perturbations naturelles, aux risques de brouillage, aux tentatives de fraudes. Et donc être à l'origine de failles de sécurité. C'est ici que le filaire prend toute sa pertinence. Ses failles de sécurité sont limitées et les systèmes filaires fermés déclenchent automatiquement une alarme en cas de rupture du signal. »* ■

CÔTÉ SOLUTIONS

Centrale alarme Vanderbilt SPC zones avec serveur Web intégré

La gamme de centrale d'alarmes SPC de Vanderbilt associe détection intrusion et fonctionnalités de contrôle d'accès dans un seul système qui peut être étendu jusqu'à 512 entrées (huit sur carte mère), 512 sorties (six sur carte mère) 32 claviers, 64 portes d'accès, 32 zones de vérification audio/vidéo IP. Certifiées NFA2P@ risque Cyber, les centrales gèrent jusqu'à deux ports X-BUS (ou une boucle), 60 secteurs, 2500 utilisateurs et badges avec différents niveaux d'accès, une mémoire pour 10000 alarmes intrusion et 10000 événements d'accès, un serveur Web intégré, et une suite logicielle basée sur un service cloud SPC Connect via une interface Ethernet embarquée. Le système est extensible avec des récepteurs radio et supporte jusqu'à 120 détecteurs radio (cohabitant avec les zones filaires).

© DR

LE POINT DE VUE D'UN FABRICANT

MATTHIEU LUCAS
Chef de marché sécurité chez Bosch Security and Safety Systems

© DR

« CHAQUE TYPE DE COMMUNICATION A SES AVANTAGES. »

« Pour les petits sites, les boutiques et autres locaux ou bâtiments où le coût de l'installation peut être important, la radio peut se justifier car elle ne requiert pas de gros travaux pour tirer et passer les câbles. En ce qui concerne les systèmes filaires, une fois le câble masqué ou protégé, il est difficile de perturber les signaux, ce qui ne sera pas forcément le cas des systèmes sans fil. Chez Bosch, quatre centrales composent la gamme B et G Series : B6512, B5512 pour B Series et B9512G, B8512G pour G Series. Répondant aux applications de moyennes et grandes tailles, elles offrent de huit à 96 zones et de 16 à 599 zones. Elles gèrent de quatre à 32 portes en accès et quatre, huit et 16 caméras IP Bosch fixes ou mobiles gérant sur détection de mouvement vidéo, sur analyse intelligente de la vidéo (IVA) et sur masquage ou altération du champ de vision et acte de malveillance. La mixité filaire et/ou radio offre une possibilité de sécuriser une pièce ou un lieu déporté là où le câblage n'est pas possible. »

SIEMENS
Ingenuity for life*
Retrouvez-nous
Stand
J30
SECURITY & SAFETY MEETINGS
Un lieu idéal est un lieu sûr.
Contrôle d'accès, vidéosurveillance, détection d'intrusion, protection périmétrique, hypervision.
Nos solutions innovantes pour la surveillance et le contrôle centralisé de vos accès et espaces pour une sécurité totale des personnes et des biens.
*L'ingéniosité au service de la vie
siemens.fr/perfect-places

Ce sont principalement les sites industriels qui sont soumis à une analyse du risque incendie.

© Getty Images

L'analyse du risque : une étape incontournable !

Dans la plupart des sites industriels, on ne peut pas se passer d'une vraie analyse du risque incendie. Une étape très importante qui déterminera les moyens humains, organisationnels et techniques à mettre en place pour lutter efficacement contre le risque incendie.

L'analyse du risque incendie ou analyse de vulnérabilité incendie est très importante. Elle est généralement confiée à des techniciens ou ingénieurs, jouissant d'une très bonne connaissance de ce risque et de ses exigences, dont la mission est de définir un niveau de risque incendie afin de proposer à l'exploitant des mesures techniques, humaines, organisationnelles… pour éliminer, autant que possible le risque incendie et ses conséquences. Dans les faits, il s'agit d'une forme d'audit de prévention et de conseil incendie (Apci) qui doivent permettre de proposer des mesures adaptées à la prévention et à la maîtrise du risque incendie puis de vérifier périodiquement que les préconisations émises ont été suivies d'effet.

« D'une manière générale, ce sont principalement les sites industriels qui sont soumis à une analyse du risque. Même si, en ce qui concerne les ERP, un règlement définit de manière précise les règles à appliquer (obligation de moyen) pour lutter contre le risque incendie dans ce type d'établissement », explique Philippe Charlot, directeur des solutions extinction chez Siemens BT et président du Gifex (groupement des fabricants installateurs de systèmes d'extinction automatiques fixes). Avant d'ajouter : *« Mais, depuis la loi Essoc, on tend de plus en plus à s'appuyer sur l'ingénierie incendie pour définir et prescrire les mesures de sécurité incendie à déployer dans les ERP. Démarche qui, il faut le souligner, a tendance à se rapprocher de l'analyse du risque incendie . L'objectif recherché est une obligation de résultat, ce qui engendre une plus grande prise de responsabilité de la part des sachants. »*

UN RÉFÉRENTIEL APSAD

Référentiel Apsad R1 : analyse de risque et de vulnérabilité incendie. Règle pour la réalisation des missions d'audit prévention et de conseil incendie. Ce référentiel, édité par le CNPP, concerne les exigences d'organisation s'appliquant à la réalisation des missions d'audit prévention et de conseil incendie.

LE POINT DE VUE D'UN FABRICANT

OLIVIER LE CLOIREC
Président de DEF Ouest et de DEF Marine

© DR

« IL S'AGIT D'UN VÉRITABLE TRAVAIL D'ENQUÊTEUR. »

« L'objectif de l'analyse du risque est de définir, de manière très précise, la vulnérabilité d'un site, d'un bâtiment, par rapport au risque incendie, pour proposer des mesures de sécurité. Il faut travailler selon deux grands axes : la gravité (bénigne à catastrophique) et la vraisemblance du risque. Tout l'enjeu est de déterminer ce qui est névralgique pour l'entreprise – et donc à protéger absolument – et ce qui l'est moins. Cette étude de la gravité et de la vraisemblance (de la probabilité) permet d'élaborer une matrice de Prouty qui fait apparaître les risques prioritaires, à diminuer ou à surveiller. Cela permet de prioriser les actions. Tout cela passe par un gros travail sur le terrain, au plus proche de la réalité de l'activité de l'entreprise. Il faut discuter avec les dirigeants, les techniciens… Visiter le site, les parties accessibles à tous, les combles, définir les points névralgiques, étudier les moyens de secours à disposition, l'environnement du bâtiment, sa gestion des déchets, les conséquences de son activité (création de poussières, par exemple), les délais d'intervention des pompiers, les moyens structurels de l'entreprise (compartimentage, désenfumage)… C'est un véritable travail d'enquêteur. C'est seulement une fois ce travail fait que l'on peut conseiller les moyens matériels qui doivent être adaptés aux risques et capables d'assurer une protection fiable et précoce. On doit mettre en place une vraie relation de confiance avec notre client, nouer une relation intime avec lui, faire preuve d'honnêteté et surtout oser dire qu'on ne sait pas tout faire. C'est à ce prix que nos recommandations seront entendues. »

Une démarche précise

« Dans le cadre de ses formations en vue d'obtenir son agrément, le CNPP aborde la notion de management du risque incendie et parle d'analyse de vulnérabilité, ajoute le président du Gifex. *Et le CNPP en donne une description assez précise. L'analyse de risque et de vulnérabilité a pour but de définir la vulnérabilité d'un site quant au risque incendie et d'identifier les scénarios d'incendie possibles, tout en en évaluant les conséquences pour le fonctionnement de l'entreprise. »*

Comme nous l'avons déjà souligné, l'analyse sera réalisée par des experts, indépendants et certifiés, travaillant pour des bureaux d'études ou de conseils en ingénierie incendie. Certains acteurs du secteur – des fabricants, par exemple – proposent, dans le cadre de leur obligation de conseil, d'accompagner et d'aider les exploitants lors de l'analyse du risque.

Cette dernière consiste à définir les points qui peuvent initier un départ d'incendie et s'ils peuvent venir « croiser » un point névralgique. Par exemple, un produit inflammable qui se retrouverait, lors des process de l'entreprise, à proximité d'un point chaud. *« Cette analyse permet de faire apparaître des points de vulnérabilité pour, évidemment, déboucher sur une hiérarchisation de ceux-ci et la mise en place d'un plan de traitement,* poursuit Philippe Charlot. *Plan de traitement qui passera par des mesures de précaution, de prévention et de protection, allant de la simple signalisation, en passant par des mesures organisationnelles jusqu'à l'installation de mesures de protection préventives ou actives de type mécanique ou électronique (compartimentage, désenfumage, détection, extinction, etc.). Sans jamais oublier la formation qui est un des piliers de la sécurité incendie. »*

Probabilité et gravité

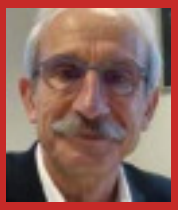
Tout l'enjeu de l'analyse du risque est donc, comme le rappelle le CNPP, *« d'identifier et de hiérarchiser les objets de risque incendie (équipements et activités) selon leur impact sur l'activité globale du site du fait de leur disparition ou indisponibilité. »*

On pourra classer les points névralgiques selon la gravité de leurs conséquences : de bénigne (pour des conséquences internes) à catastrophique (avec pour conséquence l'interruption du fonctionnement de l'entreprise).

L'analyse du risque doit avoir pour but de rechercher les phénomènes pouvant être à l'origine d'un feu et les facteurs qui peuvent y participer : risques internes, risques liés à l'activité de l'entreprise, risques externes. Il s'agit alors de classer ces risques selon leur probabilité pour les hiérarchiser afin de prioriser les mesures à prendre. ■

PAROLE D'EXPERT

PHILIPPE CHARLOT
Directeur des solutions extinction chez Siemens BT et président du Gifex



© DR

« L'ANALYSE DU RISQUE REPOSE SUR UNE CONNAISSANCE INTIME DE L'ENTREPRISE. »

« L'analyse du risque est une étape très importante. Et elle ne s'improvise pas. Cette étape préalable à l'installation suppose une connaissance parfaite du site, de ses problématiques. Il faut passer du temps avec notre client, dialoguer avec lui, rencontrer ses équipes, voir comment fonctionne l'entreprise, quels sont ses procédés, les produits qu'elle utilise, son environnement, les moyens de protection et d'alerte dont elle dispose, les procédures qu'elle a pu mettre en place… Il faut instaurer une vraie relation de confiance avec l'exploitant afin que nos recommandations soient, non seulement pertinentes, mais aussi entendues et acceptées. Il faut aussi faire preuve d'indépendance, d'honnêteté et laisser le client décider. L'objectif de l'analyse est de déboucher sur un cahier des charges qui pourra faire l'objet d'un appel d'offres. Il faut aussi comprendre que, parfois, les entreprises ne peuvent pas tout réaliser en une seule fois. On doit les aider à prioriser leurs risques et les actions liées, selon la probabilité des risques, leur occurrence et la gravité de leurs conséquences. »

La protection commence par la sécurisation des accès avec l'installation de portes blindées et de serrures robustes, et la mise en place d'une alarme anti-intrusion.

© Getty Images

Parc des expositions, des lieux sous haute protection

Chaque année en France, 120 centres de congrès, 60 parcs des expositions ainsi qu'une vingtaine d'établissements multimodaux accueillent plusieurs milliers d'événements. Un secteur qui représente un puissant moteur de l'économie et pour lequel la sûreté est un des enjeux majeurs.

Selon une étude de Médiamétrie menée sur 2015, 1135 salons et foires se tiennent chaque année en France. Ils attirent 21 millions de visiteurs et génèrent 30,5 milliards de chiffre d'affaires pour les entreprises qui y participent en louant plus de 210000 stands. Par ailleurs, 4000 événements professionnels se déroulent sur plus de 200 sites dédiés. Les 2800 congrès français accueillent 1,6 million de participants et les événements corporate sont évalués à environ 10000 par an. Ce secteur d'activité, qui a également des retombées directes dans le secteur du tourisme et de l'hébergement, se doit d'apporter une organisation sans faille, mais aussi pour la sérénité des échanges une sûreté optimale.

Des mesures pendant et hors événements

Avec un taux occupation de l'ordre de 30 % en moyenne pour les parcs d'expositions et les centres de congrès, les gestionnaires de sites vont devoir adapter leur outil de sûreté à des problématiques différentes : en période de non occupation, ou dans les zones non louées, il va s'agir de prévenir les occupations illégales et des éventuelles dégradations. En période de location, c'est la sécurité des centaines, voire des milliers d'intervenants

SÉCURITÉ INCENDIE

LA PRÉVENTION DU RISQUE INCENDIE DANS LES ERP ET LES ERT

Édité par SMACL assurance, ce guide de bonnes pratiques synthétise l'essentiel à connaître sur la réglementation, les responsabilités et les mesures à prendre. Élaboré en partenariat avec l'Association des ingénieurs territoriaux de France (AITF), il s'appuie sur de multiples expériences de terrain pour satisfaire aux quatre grands principes : éviter l'incendie ou limiter ses effets, permettre une évacuation sûre et rapide, faciliter l'intervention des secours.
À télécharger : www.smacl.fr

Le 1er Salon Online
sur la Sécurité et la Sûreté !
e-salon-protectionsecurite.fr

© DR

3 QUESTIONS À

GÉRALD BERGER

Responsable sûreté, centre de congrès d'Épinal

Que représente le centre de congrès d'Épinal ?
C'est une petite structure événementielle : un hectare couvert avec une extension possible en extérieur sur deux hectares. Le site accueille 200 000 visiteurs pour 287 événements mais qui se doit comme tout ERP d'assurer la sécurité des visiteurs et des organisateurs d'événements. La demande de sécurité croissante nous oblige sans cesse à renforcer notre niveau de sécurité, aussi bien au niveau des hommes que de celui des technologies et des protocoles.

Qu'avez-vous mis en place pour assurer la sûreté des manifestations organisées dans vos locaux ?
Comme tout ERP, nous sommes soumis aux consignes Vigipirate et nous sommes en lien régulier avec les autorités. Nous faisons appel à de la sécurité privée et éventuellement selon le type de manifestation, à des maîtres-chiens. Nous avons des caméras en périmétrie et pour contrôler les accès. Nous avons opté pour des caméras optique IP de bonne résolution qui nous permettent, si besoin, de lire les plaques d'immatriculation. Nous envisageons d'installer des portiques pour certaines manifestations, des portiques fixes ou mobiles qui pourront se déplacer en fonction de la configuration de l'événement et de sa sensibilité. Enfin, nous sommes en train d'améliorer le contrôle d'accès.

Quelles modifications avez-vous entrepris sur le contrôle d'accès ?
Nous sommes en train de passer de clés mécaniques à un contrôle d'accès par badge de SimonsVoss, ce qui améliore la gestion des accès. Je peux désormais savoir qui a utilisé un accès et quand. Cela simplifie également la gestion au niveau des exposants et des organisateurs de manifestation auxquels je peux confier un badge pour l'accès de zones données pendant la durée de leur événement. Et la question des pertes de clés est réglée : en cas de perte de badge, j'annule tout simplement les droits. J'ai choisi un système off-line évolutif sur les accès les plus stratégiques : bureau et accès extérieurs. À terme, lorsque nos 115 portes seront équipées nous passerons en online, ce qui me permettra de contrôler tout le parc en temps réel directement depuis mon ordinateur. Autre avantage, en cas de porte mal fermée, je pourrais la verrouiller d'un simple clic depuis mon bureau !

et de visiteurs qui prime ainsi que la prévention des vols. Y compris dans les centres de petite taille, la présence de vidéoprotection en périmétrie est de mise, comme le souligne Xavier Cuttaz, directeur technique de Rochexpo à La Roche-sur-Foron : *« Nos 46 caméras assurent une veille en l'absence de manifestation. Les images transmises à notre PC sécurité permettent d'alerter en cas de tentative d'intrusion. En période de montage et de démontage d'exposition, elles permettent de suivre les flux de véhicules et de repérer les anomalies. Enfin, en période de manifestation, elles permettent d'évaluer les flux de visiteurs pour adapter les ressources humaines, accueil, SSIAP, APS... »*

Une sûreté à configuration fluctuante

Complexe et mouvante, la sûreté des parcs des expositions doit tenir compte des diverses attentes des protagonistes. Tout d'abord, les gestionnaires de sites qui attendent de valoriser leur patrimoine en attirant des manifestations nombreuses et prestigieuses et veulent protéger les valeurs. Les organisateurs qui souhaitent rentabiliser leur investissement sur des opérations souvent coûteuses et attendent une sécurité optimale et sans accroc. Les visiteurs qui veulent profiter au mieux de la manifestation quelle qu'elle soit. Les pouvoirs publics, de leur côté, peuvent s'inquiéter de rassemblement de plusieurs milliers de personnes sur un espace relativement restreint. Or, l'ensemble des mesures prises pour une manifestation sont à réévaluer à chaque nouvelle occupation : *a priori* rien de commun entre un congrès politique, une foire commerciale et un événement corporate. Rien, si ce n'est le lieu qui doit pouvoir s'adapter, et adapter ses mesures de prévention de risques à chaque manifestation. De plus, la sécurité est une tâche partagée : au gestionnaire de site de s'assurer de la sécurité ● ● ●

LA PAROLE À

STÉPHANE GOMEL

Responsable grands comptes, Locken

© DR

« LE CONTRÔLE D'ACCÈS DOIT DÉPASSER LES ENJEUX DE SÛRETÉ ET ENTRER DANS LA CHAÎNE DE VALEUR DU PARC DONT LA FINALITÉ EST D'ORGANISER DES ÉVÉNEMENTS. »

« Présents sur de nombreux parcs d'expositions en France et en Europe, nous sommes, au départ, consultés pour répondre à des enjeux de sûreté : comment éviter la reproduction de clés mécaniques et assurer la traçabilité des accès ? Comment empêcher la pénétration nocturne pour des événements illégaux ? Nos clés électroniques ne sont pas reproductibles et, grâce au logiciel MyLocken, la gestion des droits d'accès est facilitée et leur durée est maîtrisée. Mais le système de contrôle d'accès pour les parcs d'exposition doit dépasser les seuls enjeux de sûreté : il doit aussi entrer dans la chaîne de valeur du parc dont la finalité est d'organiser des événements. Il doit s'intégrer dans la logistique d'accès afin de pouvoir répondre à des cloisonnements des différentes zones. La mise en place d'une solution de gestion des accès sans câblage, par clé intelligente, apporte une réponse tout à fait adaptée à ce type de structure. »

et sûreté sur les espaces communs et entre l'entrée et la porte de la manifestation, à l'organisateur de l'événement de prendre charge la sûreté dans l'espace loué. *« À Viparis,* explique Jonathan Schifano, directeur sûreté du groupe, *nous avons mis en place un schéma directeur qui s'articule autour de trois points : les équipements de sûreté sur lesquels nous avons investi plusieurs millions d'euros notamment dans des innovations, les dispositifs humains avec le renforcement des équipes et le process afin de coordonner les moyens. »*

Technologies : vidéos, anti-intrusion et IOT

La vidéo occupe une place de choix dans la protection des sites d'exposition. *« Les parcs d'expositions,* assure Philippe Bénard, directeur commercial d'Axis Communication, *ont depuis longtemps compris l'intérêt des caméras de vidéoprotection, en périmétrie de leur site et dans les bâtiments. À l'extérieur, la tendance est à l'acquisition de caméras IP de bonne qualité qui permettent la lecture de plaques d'immatriculation. À l'intérieur des halls, le positionnement des caméras, en dehors de celles qui sont placées aux niveaux des accès, est souvent problématique en raison des installations des exposants, stands ou totems qui peuvent masquer la vue. Nos caméras sur certains parcs d'expositions ont été installés sur des rails, afin de les déplacer en fonction des installations pour toujours avoir une prise de vue optimale. Enfin, il est à noter que les parcs commencent à se pencher sur les caméras ayant des capacités de détection de fumée. La hauteur et le volume des halls d'expositions sont souvent problématiques pour les détecteurs de fumée. Les caméras peuvent actuellement faire des détections précoces et lever des alarmes. Il ne s'agit pas de se substituer aux systèmes de détection incendie, mais bien de venir en complément. »* Toujours à la pointe, Viparis, confie : *« Nous avons une veille technologique permanente. Au sein de Viparis, nous avons un laboratoire d'innovations qui étudie toutes les tech-*

LA PAROLE À

MICHEL MAZON
Responsable logistique Préventica France et Afrique

© DR

« LE VOL CONSTITUE NOTRE PRINCIPALE PRÉOCCUPATION, CAR CELUI-CI EST TRÈS MAL COUVERT PAR LES ASSURANCES ET SA PRÉVENTION RESTE DIFFICILE. »

« Nous organisons chaque année deux grands salons régionaux en France et un salon en Afrique (Maroc ou Sénégal). En France – bien plus qu'en Afrique, la prévention du vol reste notre principale préoccupation, car celui-ci est très mal couvert par les assurances, avec, nous le constatons, un risque accru lorsque les lieux d'expositions sont situés en centre-ville. Le matériel audiovisuel est tout particulièrement visé par les délinquants. Les phases de montage et de démontage sont les plus exposées, et c'est la raison pour laquelle nous avons mis en place des bracelets d'identification pour tous ceux qui sont appelés à travailler sur le site (standistes, exposants et prestataires divers). Nous travaillons toujours en étroite collaboration avec les pouvoirs publics et les gestionnaires de site qui vont pouvoir nous alerter sur le niveau de menace et notamment lorsque des bandes organisées opèrent localement. Nous nous appuyons sur des équipes de sécurité locales qui connaissent bien les accès du site, effectuent un filtrage dissuasif, et peuvent mettre à disposition des physionomistes sur des sites sensibles. »

SUR LE TERRAIN

Rochexpo, un parc labellisé Sécuri-site

Situé à la Roche-sur-Foron (74800), le parc des expositions Rochexpo, offre de 95 à 22 000 m² d'espaces modulables et jusqu'à 90 000 m² avec les espaces extérieurs. Ce parc, qui accueille une cinquantaine d'événements et reçoit 250 000 visiteurs par an, a été l'un des premiers parcs des expositions à être labellisés Sécuri-site. *« Délivré en 2018 par la préfecture, ce label garantit que nous mettons en œuvre des moyens pour garantir des événements que nous organisons ou ceux que nous accueillons,* explique Xavier Cuttaz, directeur technique. *Il est le fruit d'une réflexion globale. En amont, nous avions fait faire un diagnostic avec le référent sûreté de la gendarmerie. Ce diagnostic nous a permis d'identifier un certain nombre de vulnérabilités que nous avons corrigées (renforcement des clôtures par endroit, amélioration des portails, éclairages, gestion du transport de fonds, etc.). Nous avons également mis en place de la vidéoprotection en périmétrie avec 46 caméras IP, dont les images sont transmises à notre PC sécurité. Ces caméras assurent une protection du site hors exploitation et nous permettent une bonne réactivité en période de montage et de démontage, moment où les flux de véhicules sont importants. Enfin, lors des événements, elles apportent des renseignements sur les flux de visiteurs et nous permettent d'ajuster les besoins aussi bien en personnel de sécurité que d'accueil.*

© DR

Sécuri-site est la reconnaissance du travail collectif que nous avons mené conjointement avec la gendarmerie et la police municipale pour faire monter en puissance la sûreté. Ce label a aussi ses exigences. Nous nous devons de respecter un cahier des charges précis : agents aux portes d'entrée, parkings surveillés, opérateurs de vidéosurveillance. Il demande aussi un suivi rigoureux, comme un debriefing quotidien en période d'exploitation sur les incidents et accidents. Ce debriefing qui regroupe les intervenants sûreté et sécurité ADS et SSIAP, les services techniques, les services d'urgence s'inscrit dans une volonté d'amélioration continue de la sûreté. »

Depuis plus de 60 ans, le Réseau DEF, réseau international et indépendant d'entreprises expertes en sécurité incendie, est un acteur majeur sur le marché européen. À travers ses entreprises aux expertises complémentaires, il propose une offre complète dans le secteur des Systèmes de Sécurité Incendie et fournit des produits et services pour des projets de toute complexité.

reseaudef

reseaudef.com

© DR

3 QUESTIONS À

JONATHAN SCHIFANO

Directeur sécurité et sûreté de Viparis

Quel est le périmètre d'intervention de Viparis en termes de sûreté ?
Viparis accueille sur ses sites* en Île-de-France plus de 900 événements par an. Que ce soit un salon, un congrès ou un événement corporate, la sûreté est un enjeu majeur. Nous assurons la totalité de la sûreté sur les sites de l'entrée jusqu'aux portes de l'événement et dans les espaces communs. S'il appartient aux organisateurs de mettre en œuvre les moyens nécessaires pour la sûreté de leur événement, notre rôle est de les guider et de les mettre en relation avec les bons interlocuteurs pour répondre à leurs différentes demandes. Nous proposons une offre de services à destination de nos clients organisateurs d'événements. Celle-ci est composée de la mise à disposition de nos infrastructures de sûreté associées à des solutions technologiques pour répondre aux différents enjeux de sûreté de nos clients. L'objectif est de rendre plus efficace et réactif leur dispositif de sécurité, en adéquation avec les risques identifiés pour chaque événement. Pour ce faire, ce sont plusieurs millions d'euros que nous avons investis dans les technologies et l'organisation de la sûreté.

Qu'attendent les organisateurs de votre part ?
Nous offrons un véritable parcours client en matière de sûreté, que les organisateurs ait une réponse personnalisée et des prestations sur mesure. Nos clients réguliers souhaitent la mise à disposition d'une ingénierie sûreté qui les aident à la mise en place de leur process de sécurité dans le cadre réglementaire et en adéquation avec l'état de la menace. Généralement, ils sont préoccupés par les questions de fluidité des visiteurs et l'identification des différents risques liés aux vols sur leur événement. Les clients internationaux, moins au fait de la législation française, attendent un accompagnement global pour la construction complète de leur sûreté allant du choix de prestataires locaux à la mise en œuvre d'une coordination opérationnelle des dispositifs de sûreté et la mise à disposition d'un poste de commandement spécifique intégrant des technologies leur permettant de garantir un niveau de sûreté efficient.

Vous avez reçu deux prix aux derniers Trophées de la sécurité. Que récompensent-ils ?
Nous avons reçu un trophée d'argent pour notre solution IOT qui sécurise rapidement nos bâtiments de grande envergure. Elle intègre des dispositifs de détection d'intrusion non filaire sur notre réseau Lora One sécurisé par des équipements radio combinant des contacts de porte, des barrières infrarouges, des radars volumétriques... Le trophée de bronze nous a été décerné pour la création de notre nouvelle offre «sûreté» s'appuyant principalement sur la capacité à proposer à chaque client un accompagnement personnalisé dans l'élaboration et la coordination opérationnelle du dispositif sécurité/sûreté de son événement, en partenariat avec Cispé. Cela passe par la standardisation des outils, de la phase de diagnostic à celle du retour d'expérience et la mise à disposition de nos infrastructures.

● ● ● *nologies sur le marché susceptibles de répondre à nos enjeux de sûreté ou à celles de nos clients. Les IOT sont un axe de développement et nous avons d'ores et déjà des solutions anti-intrusion comme celle qui a été récompensée aux Trophées de la sécurité 2019. Nous sommes en capacité de centraliser la totalité des flux vidéo de nos 2000 caméras et les informations sûreté de nos sites grâce à notre hyperviseur. En collaboration avec les pouvoirs publics, nous étudions tous les outils qui pourront nous aider à atteindre le niveau de sûreté attendu pour les JO de 2024.»*

Montage et démontage, le maillon faible

C'est le point faible de la sûreté sur les salons. Au moment du montage et du démontage, il est difficile de repérer qui est habilité à pénétrer sur les stands. Les équipes d'agents de sécurité tentent de filtrer les prestataires et exposants, mais comme le reconnaît un organisateur d'événements,« *ce sont des milliers de personnes qui vont aller et venir sur un temps très court, et même avec l'appui du gestionnaire de site, il est irréaliste de pouvoir contrôler toutes les personnes, le matériel et les livraisons qui entrent et sortent. Sans compter que sur certains sites, ce sont de véritables bandes mafieuses qui opèrent, et même les forces de l'ordre ont du mal à intervenir.»* Michel Mazon, responsable logistique de Préventica, reconnaît également que ces phases sont les plus fragiles en termes de sécurité : *« Nous avons mis au point un système d'identification par bracelet pour faciliter la reconnaissance des intervenants autorisés à pénétrer pendant le montage et démontage. Cela limite les vols, mais nous faisons aussi appel au gestionnaire qui connaît parfaitement les risques de son site et peut nous assister.»*

Sécuri-site, un label qui rassure

Axé sur le renforcement des dispositifs de sécurisation des principaux lieux fréquentés par les touristes et les visiteurs internationaux, le label Sécuri-site est de plus en plus revendiqué par des parcs d'expositions qui ont mis la sûreté au cœur de leur préoccupation. Un label qui rassure les organisateurs internationaux sur les capacités des gestionnaires à proposer des moyens de sûreté. C'est aussi un outil d'amélioration continue. Pour Jonathan Schifano, de Viparis : *« le label Sécuri-site reconnaît notre engagement dans les démarches de sûreté en coordination avec la préfecture de police et l'État. Ce label est associé à la notion de performance et nous incite à rester à la pointe de la technologie afin de répondre à l'état de la menace. Cela nous oblige à une veille permanente tant sur le plan de technologies de sûreté que de l'état de la menace. Nous nous appuyons sur Cispé, une start-up incubée à French Event Booster, la plateforme d'innovation de l'événementiel, et disposons ainsi d'un centre d'ingénierie de la sécurité privée des événements pour accompagner nos clients dans le déploiement de leur sûreté dans les meilleures conditions.»* ■

** Viparis est gestionnaire de : Espace Champerret, Espace Grande Arche, hôtel Salomon de Rothschild, les salles du Carrousel, palais des congrès d'Issy, palais des congrès de Paris, Paris expo Porte de Versailles, Paris Le Bourget, Paris Nord Villepinte.*

Avec annuaire-securite.fr trouvez le bon prestataire !

- Trouvez un distributeur près de chez vous.
- Contactez un installateur un intégrateur...
- Découvrez les équipements de sécurité (videosurveillance, contrôle d'accès,alarmes...) que proposent les Fabricants.

Si vous souhaitez faire figurer votre entreprise dans cet annuaire, merci de nous contacter au **01 45 23 33 78** ou à **info@protectionsecurite-magazine.fr**

Guide ANNUEL d'Achat

www.protectionsecurite-magazine.fr

RETROUVEZ PLUS DE PRESTATAIRES, LEURS ÉQUIPEMENTS ET SERVICES SUR LE SALON ONLINE

e-salon-protectionsecurite.fr

Si vous souhaitez figurer dans cette rubrique, merci de nous contacter sur
info@protectionsecurite-magazine.fr
ou au 01 45 23 33 78

DÉTECTION - ALARME

Adetec
8 rue de l'angoumois
95100 ARGENTEUIL
Tél.: 01 39 81 85 45
contact@adetec.com
www.adetec.com

AE&T
www.aet.fr/fr/

ARD
www.controle-acces.fr

BY DEMES FRANCE
www.bydemes.com

BOSCH
www.boschsecurity.fr

FOXSTREAM
www.foxstream.fr

GUNNEBO FRANCE
www.gunnebo.com

HONEYWELL
www.honeywell.com/security/fr

IZYX SYSTEMS
www.izyx-systems.com

LEGRAND
www.legrand.fr

MAGNETA
www.magneta.fr

MWS
www.mws.fr

OPTEX
www.optex-security.com

PROSEGUR FRANCE
www.prosegur.fr

RISCO GROUP
www.riscogroup.com

SCHNEIDER ELECTRIC
www.schneider-electric.com

SCUTUM
www.scutum.fr

SEPTAM
www.septam.fr

SERIS SECURITY
www.seris.be

SERVIACOM
www.serviacom.fr

SORHEA
www.sorhea.fr

SURTEC
www.surtec.tm.fr

SYNCHRONIC
http://www.synchronic.fr

TIL TECHNOLOGIES
www.til-technologies.fr

VANDERBILT
10, place Fulgence Bienvenue
77600 Bussy Saint Georges
Tél. 0825 16 11 77
www.vanderbiltindustries.com

ZENITEL
www.stentofon.fr

VIDÉOSURVEILLANCE

AASSET SECURITY
www.aasset-security.fr

ACALBFI
www.acalbfi.fr

ALL PRODUCTS
www.all-products.com

ARECONT VISION
www.arecontvision.com

AVIGILON CORPORATION
www.avigilon.com

AXIS COMMUNICATION
www.axis.com/fr

BOSCH
www.boschsecurity.fr

bydemes
BY DEMES FRANCE
22/24 rue Lavoisier
Bâtiment B, 1er étage D
92 000 Nanterre (France)
Tél : +33(0) 147240626
france@bydemes.com
www.bydemes.com

CISCO SYSTEMS
www.cisco.com

CITELUM
www.citelum.com/fr

COMPUTAR / GANZ
www.cbc-cctv.com

CASD
Solutions de vidéoprotection
CASD
296 Rue de la Béalière
38113 Veurey Voroize
Tél. +33 (0) 4 76 72 80 59
Fax. +33 (0) 4 76 72 90 24
casd@casd.fr - www.casd.fr

CONSORT NT
www.consortnt.com

D-LINK
www.dlink-com/fr

DAHUA
www.dahuasecurity.com/fr

DELTA SECURITY SOLUTIONS
www.delta2s.fr

DIGITAL BARRIERS
www.digitalbarriers.com

ECCTV
www.ecctv.fr

EET EUROPARTS FRANCE
http://fr.eetgroup.com

ERYMA SÉCURITÉ SYSTÈMES
www.eryma.com

EVITECH
www.evitech.com

EXAVISION
www.exavision.com

FLIR
www.flir.com

FOXSTREAM
www.foxstream.fr

FUJIFILM
www.fujifilm.eu/fr

GENETEC
www.genetec.com

GEUTEBRÜCK
www.geutebruck.com

HANWHA TECHWIN
www.hanwha-security.eu/fr

HIKVISION
www.hikvision.com

HONEYWELL
www.honeywell.com/security/fr

HYMATOM
www.hymatom.fr

IDIS EUROPE
www.idisglobal.com

INDIGO VISION
www.indigovision.com

INEO
www.cofelyineo-securite.fr

IZYX
www.izyx-systems.c

JVC PROFESSIONAL FRANCE
www.jvcpro.fr

MERIT LILIN
www.meritlilin.fr

MILESTONE SYSTEMS
www.milestonesys.com

MOBOTIX
www.mobotix.com

MYFOX
www.myfox.pro

NEXTIRAONE
www.nextiraone.eu/fr

OPTEX
www.optex-security.com

PANASONIC
http://business.panasonic.fr

PELCO
www.pelco.com

PROSEGUR FRANCE
www.prosegur.fr

RSI VIDEO TECHNOLOGIES
www.videofied.com

SAMSUNG TECHWIN EUROPE
www.samsungsecurity.fr

SCUTUM
www.scutum.fr

SERVIACOM
www.serviacom.fr

SONY
www.sony.fr/pro/products/videosecurity

STIM
www.stim.fr

SVD - SYSTÈMES VIDEO DIGITAL
http://svd-france.com

SYNOLOGY
www.synology.com/fr-fr/

TAMRON FRANCE
www.tamron.fr

TEB
www.teb-online.com

TIFALI
www.tifali.com

TIL TECHNOLOGIES
www.til-technologies.fr

VANDERBILT INTERNATIONAL
www.vanderbiltindustries.com

VEDIS
www.vedis.pro

VIVOTEK
Mail: salesvivotekfrance@vivotek.com www.vivotek.com

VIZEO
www.vizeo.eu

WESTERN DIGITAL FRANCE
www.wdc.com/fr/

IDENTIFICATION CONTRÔLE D'ACCÈS

ABIOVA
www.abiova.com

ABUS FRANCE
www.abus.com

ACIE AUTOMATISME
http://aciesecurite.com

AIPHONE
www.aiphone;fr

ALCEA
www.alcea.fr

ASSA ABLOY FRANCE
www.assaabloy.fr

BOSCH
Des technologies pour la vie
32 avenue Michelet
93400 Saint Ouen
Tél. 0 825 12 8000
Tél. 0 825 12 8000
fr.securitysystems@fr.bosch.com
www.boschsecurity.fr

CAE GROUPE
www.cae-groupe.fr

CASTEL
Z.I. St Lambert des Levées
49400 Saumur
Tél. 02 41 40 41 40
info@castel.fr
www.castel.fr

DEISTER ELECTRONIC FRANCE
www.deister.com

DIRICKX GROUPE
www.dirickx.fr

ERYMA SECURITE SYSTEMES
www.eryma.com

FOXSTREAM
www.foxstream.fr

Genetec
Genetec Europe
6 Rue Daru,
Paris 75008
Tél. 01 44 69 59 00
info@genetec.com

GEUTEBRÜCK
www.geutebruck.com

HID GLOBAL
www.hidglobal.fr

HONEYWELL
www.honeywell.com/security/fr

HOROQUARTZ
www.horoquartz.fr

iLOQ
Making life accessible
27 rue du Chemin Vert
75011 Paris
01 81 80 14 30
france@iloq.com
www.iLOQ.com

IZYX SYSTEMS
www.izyx-systems.com

izyx systems
Tél. 03 88 75 32 32
info@izyx-systems.com
www.izyx-systems.com
FABRICANT INNOVANT
Solutions de contrôle d'accès et de sécurité électronique

KABA
www.kaba.fr

LOCKEN SERVICES
www.locken.fr

MYFOX
www.myfox.pro

NEDAP FRANCE
www.nedap.fr

PAXTON
www.paxtonaccess.fr

PRASTEL
ZI ATHELIA II
225 impasse du Serpolet
13600 La Ciotat - France
Tél : 04.42.98.06.06
Mail : info@prastel.com
Site internet : www.prastel.com

Le 1er Salon Online sur la Sécurité et la Sûreté !
e-salon-protectionsecurite.fr

PROSEGUR FRANCE
www.prosegur.fr

REXEL
www.rexel.fr

RISCO
www.riscogroup.com

SALTO SYSTEMS FRANCE
www.saltosystems.com/fr

SCUTUM
www.scutum.fr

SEPTAM
www.septam.fr

SERIS SECURITY
www.seris.be

SERVIACOM
www.serviacom.fr

SIEMENS
www.siemens.fr/buidingtechnologies

SIMONS VOSS TECHNOLOGIES
www.simons-voss.fr

SEWOSY
Fabricant
13b rue Saint-Exupéry
ZA de l'Aérodrome - CS20152
F-67503 Haguenau Cedex
Tél. : +33(0)3 90 59 02 20
Fax : +33(0)3 90 59 02 19
www.sewosy.com

STANLEY SECURITE FRANCE
www.stanley-securite.fr

STID
www.stid.com

SYNCHRONIC
www.synchronic.fr

TECHNICOB
www.technicob.com

TIL TECHNOLOGIES
www.til-technologies.fr

UHLMANN & ZACHER
www.uundz.com

UNIACCESS
www.uniaccess.fr

VANDERBILT INTERNATIONAL
www.vanderbiltindustries.com

ZENITEL
www.stentofon.fr

LUTTE CONTRE LE FEU

ASD
Systèmes de détection incendie
2 ter avenue de France
B.P. 33
91301 Massy
Tél. 01 69 93 81 90
www.asd-incendie.fr

AVISS SECURITE
www.aviss-securite.fr

BOSCH
www.boschsecurity.fr

COOPER SAFETY FRANCE
www.cooperfrance.com

DEF
www.def-online.com

DUBERNARD
www.dubernard.fr

EDC PROTECTION
www.edc-protection.com

EIFI
www.eifi-incendie.fr

EUROFEU
www.eurofeu.fr

FRANCE INCENDIE
www.france-incendie.fr

GROUPE GORGE
www.groupe-gorge.com

INEO
www.cofelyineo-securite.fr

MYFOX
www.myfox.pro

NISCAYAH
www.stanley-securite.fr

PX TECHNOLOGIES
http://pyrexx.com/detecteurs-de-fumee

SERVIACOM
www.serviacom.fr

SLAT
www.slat.com

TYCO FIRE PROTECTION
www.tfppemea.com

ZETTLER
www.zettlerfire.com

CNPP
www.cnpp.com

DEKRA INDUSTRIAL
www.dekra-industrail.fr

EXAVISION
www.exavision.com

SOCOTEC
www.socotec.fr

SCUTUM
www.scutum.fr

PROTECTION PÉRIMÉTRIQUE

GEUTEBRÜCK
www.geutebruk.com

HYMATOM
www.hymatom.fr

OPTEX
www.optex-security.com

OREP
www.orep-securite.com

SORHEA
www.sorhea.com/fr

UTC CLIMATE, CONTROLS & SECURITY
www.ccs.utc.com/ccs/en/worldwide

CONTRÔLE D'ACCÈS

Netatmo dévoile sa Serrure et ses Clés intelligentes

© Netatmo

Lors du dernier CES de Las Vegas, le spécialiste français des objets intelligents a dévoilé ses toutes dernières innovations : sa serrure et ses clés intelligentes.
Elles ont d'ailleurs décroché une récompense dans la catégorie Home Appliances du concours CES 2020 Innovation Awards.
La Serrure Intelligente de Netatmo permet à son utilisateur de gérer et de partager l'accès à sa maison ou son appartement simplement et en toute sécurité. Il verrouille et déverrouille sa porte en insérant la Clé dans la serrure, comme une clé classique, ou en utilisant l'application Netatmo Security.
Par ailleurs, grâce à cette application, l'utilisateur configure autant de Clés intelligentes qu'il le désire pour ouvrir sa porte, et peut désactiver en un seul clic une Clé perdue ou volée. Il peut aussi envoyer, où qu'il soit, une invitation sur le smartphone de ses invités pour leur donner accès à son logement.
Cette nouveauté a été résolument pensée et développée afin d'associer sécurité du domicile, autonomie et simplicité de gestion des Clés et des droits d'accès.

Une serrure sécurisée et résistante
La Serrure Intelligente de Netatmo est conçue pour résister aux attaques physiques et informatiques. Elle est certifiée A2P*, BZ+ et SKG***. La serrure fonctionne en Bluetooth et n'est donc pas reliée à internet. Celle-ci communique en Near-Field Communication (NFC) avec les Clés intelligentes, qui sont inviolables et impossibles à dupliquer. En cas de perte ou de vol de clés, l'accès à la maison reste sécurisé : l'utilisateur les désactive en temps réel sans avoir à changer toute la serrure, d'un seul clic depuis son smartphone.
Enfin, pour assurer la sécurité des données des utilisateurs, les autorisations d'accès et les données d'identification de chaque Clé sont stockées localement dans la serrure et non sur le cloud. Par ailleurs, la serrure est dotée d'un accéléromètre qui détecte les vibrations liées à une éventuelle tentative d'effraction. ■

→ **www.netatmo.com/fr**

CARACTÉRISTIQUES

- La Serrure Netatmo s'installe en remplacement du cylindre de porte existant.
- Elle est équipée de piles d'une autonomie de deux ans. Lorsque la batterie faiblit, l'utilisateur est alerté par un signal sonore lors du verrouillage ou déverrouillage de la porte ou sur son smartphone.

3 QUESTIONS À

HELEEN DE WAAL

Chef produit chez Netatmo

© DR

Pouvez-vous nous présenter Netatmo ?
La société a été fondée en 2011 par Fred Potter. En novembre 2018, Netatmo a rejoint le groupe Legrand. Depuis sa création, Netatmo conçoit des solutions dédiées à la maison intelligente (détecteur de fumée, station météo, caméras, etc.) pour le grand public et codéveloppe, via son programme « with Netatmo » des solutions intelligentes qui s'intègrent à l'infrastructure de la maison en collaboration avec les leaders industriels du bâtiment. Netatmo a lancé 13 innovations. La Serrure et les Clés intelligentes sont les dernières en date.

À l'heure où de nombreux spécialistes du contrôle d'accès font le pari de la clé dématérialisée sur un smartphone, vous lancez une serrure et des clés. Pourquoi ?
Lors de nos travaux préparatoires à la conception de ce nouveau produit, nous avons constaté que le marché de masse du contrôle d'accès résidentiel ne demande pas que des solutions dématérialisées, des téléphones qui servent de clé. Beaucoup de gens veulent encore utiliser des clés physiques. Le smartphone a aussi des inconvénients : batterie vide, téléphone volé… Même si, en cas d'oubli ou de perte de la Clé, on peut, avec notre système, ouvrir sa porte avec son téléphone.

Quand cette solution sera-t-elle disponible ? Comment sera-t-elle distribuée ?
Notre Serrure et ses Clés intelligentes seront commercialisées d'ici la fin de l'année 2020. Elles seront disponibles dans les grandes surfaces de bricolage, chez des enseignes comme Darty, Boulanger, sur internet… Nous disposons aussi d'équipes commerciales qui se chargent de la promotion immobilière afin d'équiper les immeubles et d'intégrer cette solution dans des projets immobiliers.

INTRUSION

Allix, portail pivotant avec motorisation enterrée

© DR

La gamme de portails industriels Allix de Dirickx se compose de portails autoportants, coulissants et pivotants, destinés à la protection des sites industriels, collectifs d'habitation, lieux publics, sites logistiques et sites sensibles. Ce nouveau portail pivotant motorisé en acier Allix est proposé dans deux versions pour répondre à tous les besoins d'accès sécurisés et à toutes les configurations : un portillon et un portail à un vantail, permettant un passage de 1,25 m à 3 m, ; un portail à deux vantaux, autorisant un passage de 2,50 m à 6 m.

Deux types de motorisations enterrées sont disponibles :

- Équipé du moteur autobloquant S800 CBAC, ce portail pivotant répond aux exigences des sites industriels.
En cas de coupure de courant et pour sécuriser les biens, en conservant le portail verrouillé, un déblocage par clé est nécessaire pour assurer l'ouverture.
- Équipé du moteur réversible S800 SBW automatiquement manœuvrable sans clé, afin de libérer les accès en cas de panne de courant, Allix est particulièrement recommandé pour les collectifs d'habitation. ■

→ **www.dirickx.fr**

VIDÉOSURVEILLANCE

Nouvelle caméra zoom box X-Lite Wisenet

© DR

La dernière nouveauté de la gamme de caméras Wisenet d'Hanwha Techwin est une caméra zoom box 32x économique en deux mégapixels. La Wisenet X-Lite XNZ-L6320, équipée d'un objectif varifocale motorisé 32x optique avec autofocus, vient remplacer la caméra zoom box Wisenet SNZ-6320, dans une déclinaison plus compacte et plus économique que son prédécesseur. La caméra Wisenet XNZ-L6320 est une vraie caméra jour/nuit équipée d'un filtre d'arrêt infrarouge amovible (ICR) et qui bénéficie d'une technologie de plage dynamique étendue (WDR) avancée pouvant atteindre jusqu'à 120 dB et produire des vidéos précises de scènes contenant simultanément des zones très lumineuses et très sombres. À la différence des WDR conventionnels qui combinent deux images prises à différentes expositions, la Wisenet XNZ-L6320 utilise quatre images pour produire une image de meilleure qualité. ■

→ **www.hanwha-security.eu**

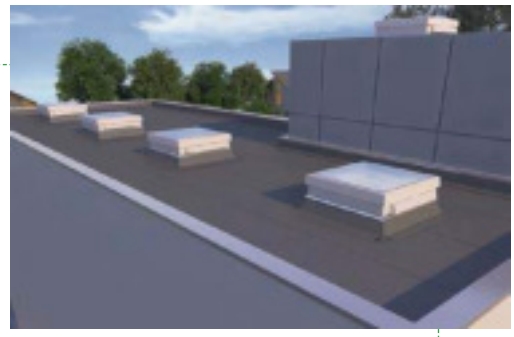
CARACTÉRISTIQUES

- Prise en charge des compressions H.265, H.264 et MJPEG, ainsi que de WiseStream II, une technologie de compression complémentaire exclusivement disponible avec les caméras Wisenet.
- Systèmes d'analyse intelligente intégrés : sabotage, maraudage, détection directionnelle, détection de perte de mise au point, détection de brouillard, disparition, détection de visages et détection de mouvement…
- Classification sonore : un système d'analyse audio qui reconnaît les sons critiques et génère une alerte pour permettre au personnel de sécurité de réagir rapidement en cas d'incident.

quoi de neuf ?

LUTTE CONTRE LE FEU

Lanterneau lumineux et performant



© DR

Blueteck lance le Slick Inside Carré. Slick Inside Carré est le nouveau lanterneau d'éclairement zénithal et d'aération naturelle pour les toitures plates et les couvertures des bâtiments tertiaires, les logements collectifs et l'habitat individuel, en neuf ou en rénovation. Il se décline dans deux modèles : Slick Inside Carré Fix pour l'éclairement zénithal ; Slick Inside Carré Air pour l'aération naturelle. Le remplissage en verre garantit aux utilisateurs une très grande luminosité et une excellente isolation phonique.
En version fixe pour l'éclairement zénithal ou en version ouvrant pour l'aération, ce lanterneau de toiture carré bénéficie d'une costière blanche en polyester avec une isolation thermique renforcée.
En fonction des exigences d'isolation thermique, ce lanterneau est équipé d'un double ou d'un triple vitrage feuilleté. ■

→ **www.bluetek.fr**

© DR

LUTTE CONTRE LE FEU

Simulateur de feu en réalité virtuelle

Le simulateur de feu en réalité virtuelle YouRescue, édité par Wanadev, est un nouvel outil mis à disposition du formateur en face-à-face pédagogique. En quelques minutes seulement, il peut mettre en situation chacun de ses apprenants au plus près du risque, tout en le gardant en sécurité.
Dans le casque, l'apprenant a la sensation de vivre la situation de départ de feu avant même de l'avoir vécue réellement, ce qui a pour effet de lever toute inhibition liée à la peur de mal faire ou à une crainte excessive du feu.
L'objectif consiste à développer la confiance en soi de l'apprenant pour qu'il se sente capable de passer à l'action si le cas se présente réellement, à savoir : éteindre le feu quand il est encore temps, et jauger le moment où il faut absolument évacuer.
> Les scénarios déjà disponibles : travail en milieu tertiaire (type W), travail en magasin (type M), travail en entrepôt, transport de matières dangereuses.
> Les scénarios à venir : transport de voyageurs, travail en hôtellerie/restauration (types N&O), travail en milieu hospitalier (types U&J). ■

→ **www.yourescue.fr**

CONTRÔLE D'ACCÈS

Le cylindre haute sécurité réversible

Le cylindre Satyx Twin de Dény Security est tout particulièrement dédié aux applications de haute sécurité. Il est équipé de nombreux éléments techniques et brevets le protégeant contre la copie et l'effraction comme un double élément mobile et une barre horizontale de blocage. Cette sécurité est accompagnée du confort d'utilisation de la clé réversible et de la possibilité de réaliser des organigrammes complexes. Il comporte jusqu'à 21 éléments de codages différents, neuf pistons verticaux et dix éléments de codage latéraux. Il constitue une protection élevée contre le crochetage et les techniques de bumping. Le corps du cylindre est en laiton massif nickelé, ce qui lui confère une haute résistance à la corrosion et aux températures extrêmes. Il présente une haute résistance au perçage, à la torsion et à l'arrachage. La clé est protégée contre la reproduction par brevet. Cylindre compatible avec les systèmes de contrôle d'accès 125 Khz et Mifare. Classé EN1303 :2018-08. ■

→ **www.deny-security.com**

© DR

NE CHERCHEZ PLUS !
TROUVEZ !

e-salon-protectionsecurite.fr

Visitez le 1er salon online sur la Sûreté et Sécurité, choisissez tranquillement le matériel ou produit dont vous avez besoin et contactez directement le fabricant !

1. Vous sélectionnez les catégories de produit que vous recherchez : vidéosurveillance, identification, contrôle d'accès, détection, alarme.....
2. Vous sélectionnez les produits selon vos critères de recherche.
3. Vous consultez tranquillement les fiches techniques des produits, visionnez les vidéos de démonstration, les documentations techniques, les catalogues, faites en direct des demandes de devis...

Si vous souhaitez faire figurer vos produits sur ce salon online, merci de nous contacter : **info@protectionsecurite-magazine.fr**

© DR

« Le Livre blanc cristallise des attentes collectives fortes. »

GUILLAUME FARDE

Maître de conférences à Sciences Po, spécialiste des questions de sécurité

Guillaume Farde revient sur les enjeux du futur Livre blanc de la sécurité intérieure, les conclusions à en espérer et leur éventuelle transcription dans une loi de programmation.

Contrairement au ministère des Armées, le ministère de l'Intérieur n'est pas, pour sa part, familier de cette rythmique où, chaque début de législature, un Livre blanc fixe de grandes orientations stratégiques que le législateur décline sur un plan budgétaire. En octobre 2011, le Livre blanc sur la sécurité publique avait d'ailleurs été publié en toute fin de législature et, de façon assez contre-intuitive, il avait été suivi d'une loi de programmation budgétaire ; celle-ci, baptisée Loppsi, avait, en effet, été votée dix mois plus tôt.
En 2019, les femmes et les hommes du secteur de la sécurité en France ont connu une année d'engagement et de questionnement. Le niveau d'engagement a été particulièrement intense en raison des manifestations des « gilets jaunes », de la tenue du G7 à Biarritz, du mouvement social contre la réforme des retraites et de la commission de plusieurs attentats terroristes. Ce niveau d'engagement rarement atteint a intensifié leur questionnement sur leurs perspectives et le sens de leur action au quotidien. Le Livre blanc de la sécurité intérieure est censé y répondre.

Des modalités à fixer

Les enjeux afférents à la sécurité privée sont traités par un des quatre groupes de travail constitués pour la réalisation du Livre blanc. Le principe de la coopération public-privé n'est aujourd'hui plus débattu. Plus aucun événement qu'il soit festif, sportif ou culturel ne peut se tenir sans le concours de la sécurité privée. Le Livre blanc en prendra certainement acte. Mais il n'en reste pas moins que les modalités de cette coopération (le fameux qui fait quoi pour combien et sous quel contrôle ?) ne sont pas encore fixées. Le Livre blanc pourrait en partie y répondre et, pour le reste, renvoyer à une loi de programmation.
Or, toute la limite de l'exercice est qu'une telle loi n'interviendrait qu'en 2021, soit un an avant la fin de la législature et que, par conséquent, elle risquerait de ne pas programmer grand-chose. Le Livre blanc cristallise des attentes collectives fortes. Le principal risque est donc qu'il déçoive collectivement, pas tant par ses conclusions que par l'absence de suites qui y seraient réservées par une éventuelle loi de programmation.

Un interlocuteur unique ?

Une des grandes avancées pour le secteur privé de la sécurité au sens large, consiste à avoir regroupé la Délégation aux coopérations de sécurité (DCS) et la Délégation ministérielle aux industries de sécurité et de lutte contre les cybermenaces (DMISC). Cette mesure, qui devance même la publication du Livre blanc, est un signal fort à l'adresse de la filière (prestataires et industriels) qui pourra ainsi compter sur un interlocuteur unique, rattaché au Secrétariat général du ministère.
Aller plus loin impliquerait la création d'un poste de conseiller ministériel, à l'instar du ministère des Armées. Cette proposition est notamment portée par le Gicat. Il est encore trop tôt pour dire si elle sera suivie d'effet.
Enfin, les installateurs de systèmes de télésurveillance et les sociétés de conseil en sûreté attendent d'être reconnus comme des activités privées de sécurité à part entière, au sens du Livre VI du Code de la sécurité intérieure. Le Livre blanc et la loi de programmation qui suivra seraient une excellente occasion de sortir enfin ces professions de l'insécurité juridique. ■

GUILLAUME FARDE ■ **2014** Docteur en sciences de gestion ■ **2016** Conseiller scientifique de la spécialité sécurité-défense de l'École d'affaires publiques de Sciences Po ■ **2017** Chef du pôle sécurité intérieure du think tank L'Hétairie ■ **2018** Directeur de la stratégie du Groupe Risk&Co ■ **2019** Consultant sécurité à BFMTV.

Pour un
environnement de travail
SAIN et SÉCURISÉ

Préventica'20

CASABLANCA
07>09 **AVR**
Ofec

NORD FRANCE
26>28 **MAI**
Parc Expo de Douai

LYON
29 **SEPT**>01 OCT
Eurexpo

preventica.com

WISENET

Bientôt disponible

L'Intelligence Artificielle pour la vidéosurveillance

Caméras WISENET IA

La nouvelle gamme Wisenet IA dispose d'un puissant moteur d'intelligence artificielle (IA) qui peut détecter et classer les personnes et les véhicules en temps réel. Elles sont conçues pour capturer les différents attributs des objets, notamment les personnes, les véhicules, les visages et les plaques d'immatriculation.

Cela permet aux opérateurs d'utiliser des applications d'IA fonctionnant sur un serveur back-end, pour une recherche et une analyse plus rapides des informations dont ils ont besoin.

Elle peut également réduire considérablement les fausses alarmes causées par les arbres qui ondulent, le bruit vidéo et même les ombres en mouvement.

Série de caméras IA

PNO-A9081R, PNV-A9081R, PND-A9081RV, PNB-A9001

Hanwha-security.eu

Hanwha Techwin