

psm

PROTECTION SÉCURITÉ MAGAZINE

Les Solutions pour les Professionnels de la Sûreté - Sécurité



**VIDÉO-
SURVEILLANCE**

VOIR DANS LE NOIR ? OUI,
MAIS POUR FAIRE QUOI ?

n°259

Mai | 2020
Juin

26 €

Entretien



FRÉDÉRIC
GAUTHEY,
PRÉSIDENT DU GROUPEMENT
DES ENTREPRISES
DE SÉCURITÉ

«LA SÉCURITÉ PRIVÉE EXISTE
EN ELLE-MÊME.»

Contrôle d'accès

INTERPHONIE
AVEC OU SANS FIL ?

Incendie

MAINTENANCE DES
EXTINCTEURS : À NE NÉGLIGER
SOUS AUCUN PRÉTEXTE !

DOSSIER

**CLOUD ET
SÉCURITÉ**

APPLICATIONS GLOBALES

Surveillance de température corporelle par caméra thermique Dahua

- Précis
- Sans-contact
- Rapide



- Une surveillance précise, sûre et efficace
- Dépistage sans contact et un passage rapide
- Détection multiple et accès efficace
- Alerte visuelle pour signaler une alarme et faciliter la captation de température multi-points
- Détection intelligente et automatique d'absence de port d'un masque

Modèles recommandés



DH-TPC-BF5421-T
DH-TPC-BF3221-T

Corp noir



DHI-IVSS7008-11



DHI-NVR5216-16P-I



DSS Express/Pro

DAHUA TECHNOLOGY FRANCE

49 rue Auguste Perret, 94000 Créteil, France

Tel : 01 48 53 70 53

Email : sales.france@dahuatech.com / support.france@dahuatech.com

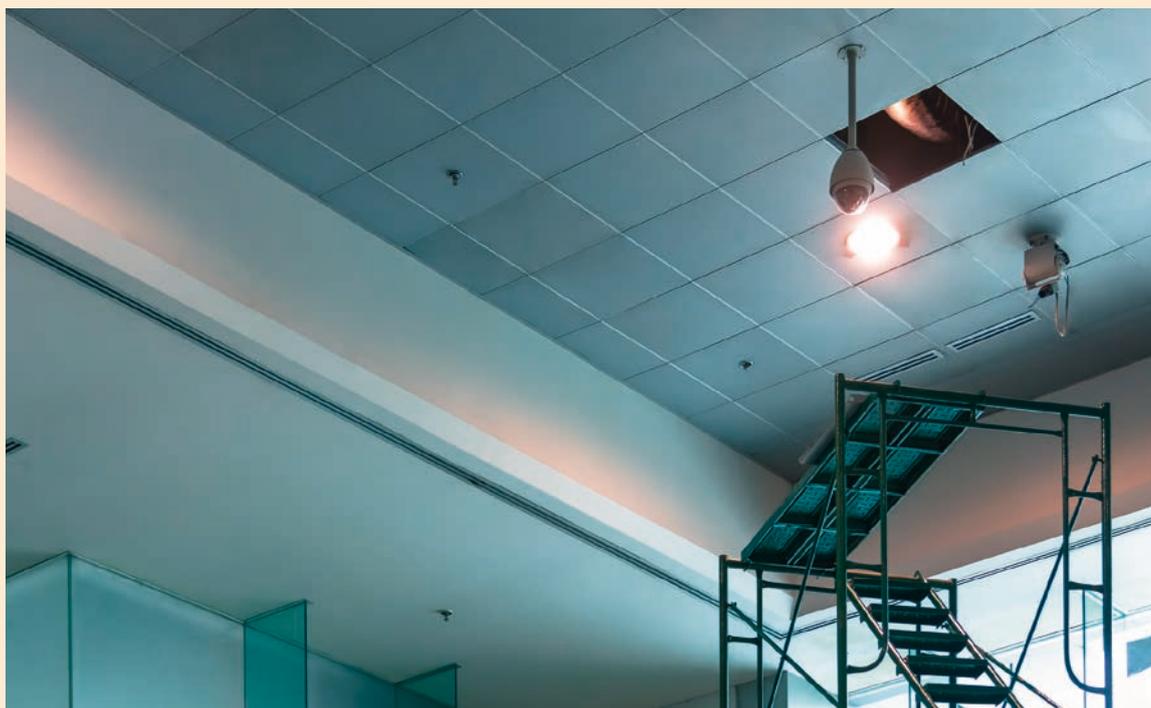
www.dahuasecurity.com





Quel impact sur les métiers de la sécurité électronique ?

Comme de nombreux secteurs, les professionnels de la sécurité électronique – fabricants, installateurs, distributeurs, intégrateurs, télésurveilleurs, etc. – ont vu leur activité perturbée par le confinement décidé par le président de la République. Premier bilan.



© Getty Images

« **L**e monde de la sécurité électronique est divers. Et n'a pas vécu le confinement de la même manière, explique Luc Jouve, président du GPMSE Installation. Par exemple, dans le cadre d'une enquête réalisée par le GPMSE, les opérateurs en télésurveillance, dans leur majorité, ont continué à se rendre à leur poste, dans la centrale de télésurveillance, pour assurer la continuité des services et des prestations assurées par le télésurveilleur. En revanche, l'activité a nettement ralenti pour les installateurs et mainteneurs des systèmes de sécurité électronique. Et seules les interventions urgentes ont été généralement maintenues. »

Les contrôles de déplacements se sont généralement bien passés. Par exemple, seuls 20 % des dirigeants de sociétés de télésurveillance, ayant répondu à l'enquête du GPMSE, ont rencontré des difficultés pour se rendre sur leur lieu de travail. À l'inverse, une forte majorité, 70 %, des dirigeants de sociétés d'installation et de maintenance des dispositifs de sécurité électronique ont eu à déplorer des difficultés, concernant le déplacement de leurs collaborateurs, lorsqu'ils doivent intervenir après signalements de dispositifs défectueux.

Difficultés d'approvisionnement

« Et lorsqu'il s'agit de livraison de matériel, ils sont encore plus nombreux, puisque 90 % d'entre eux indiquent être très difficilement approvisionnés par les fabricants ou les distributeurs, entraînant ainsi de réels enjeux en matière de maintenance, du fait d'une pénurie de pièces ou produits; ceux-ci étant pourtant indispensables à la sécurisation de sites, souvent totalement fermés et pouvant être à tout moment vandalisés », ajoute Luc Jouve. ● ● ●



© DR

« Nous subissons comme tout le monde cette crise sanitaire avec son lot d'incertitudes. Malgré tout, nous espérons confirmer nos résultats de l'année dernière. Notre bonne santé financière nous permettra de répondre sereinement à toutes les demandes en logiciels. »

STEPHAN LAURENT, COFONDATEUR DE CASD



2 QUESTIONS À Luc Jouve, PRÉSIDENT DU GPMSE INSTALLATION

Quel bilan tirez-vous du confinement subi par les Français depuis le 17 mars ?

Pour notre filière, il n'est pas bon. Même si les installateurs qui ont du chiffre d'affaires récurrent avec des contrats de maintenance subissent moins cette crise. À l'opposé du spectre, les PME-PMI qui ne vivent que de l'installation sont beaucoup plus touchées. Le confinement a induit un très net recours au chômage partiel. Chômage partiel encore aggravé après l'annonce de la prolongation du confinement, le 13 avril, par le président de la République. Par ailleurs, force est de constater qu'en ce qui concerne les matériels nécessaires à l'exercice de nos métiers, nous avons beaucoup de mal à recevoir nos commandes. L'approvisionnement est difficile. Aujourd'hui, certains installateurs peuvent se trouver en rupture. Sans un accompagnement des banques et de l'État, certains ne s'en relèveront pas. En outre, au 20 avril, 80 % des entreprises adhérentes du GPMSE n'avaient pas encore reçu le remboursement du

chômage partiel. Tout cela additionné à l'incertitude quant à la fin de la crise, nous ne pouvons pas être totalement optimistes.

Cette situation est-elle la même partout en France ?

Certaines régions sont plus touchées que d'autres comme celles où le tourisme est une des activités importantes pour l'économie régionale et locale. Il est indéniable que la crise est profonde pour les installateurs. Des questions subsistent aussi : La sécurité électronique sera-t-elle une priorité pour les Français dans l'après-crise ? À quelle date l'activité économique va-t-elle vraiment reprendre ? De nombreuses questions restent, mais, s'il faut dire les choses, je souhaite aussi être positif. Nous avons survécu aux crises des chocs pétroliers, à la crise financière de 2008 et aux difficultés d'un marché hétéroclite dans sa structure. Les chefs d'entreprises, que je représente, sauront, j'en suis persuadé, montrer à quel point ils sont performants afin de sortir par le haut de cette crise majeure.

● ● ● Avant de poursuivre : « Concernant ce sujet, il est à noter que si les télésurveilleurs ont constaté une baisse des tentatives de vol chez les particuliers, une augmentation des vols est à déplorer dans les commerces. Nous souhaitons donc alerter les pouvoirs publics quant à la nécessité de permettre la continuité de cette activité, les dirigeants de ces sociétés étant conscients que celle-ci doit rester limitée à des actions urgentes, répondant à des demandes liées à des sites souvent sensibles ou à des risques de faillite économique, en cas de vol de données ou de matériel. »

Des conséquences sociales lourdes

Au-delà des difficultés constatées sur le terrain, l'enquête du GPMSE révèle les conséquences sociales et économiques liées aux mesures prises par le gouverne-



PLUS DE 30 %

La majorité des adhérents du GPMSE Installation estime la perte de chiffre d'affaires supérieure à 30 % en 2020.

ment pour lutter contre cette pandémie. Et elles sont lourdes. Ainsi, 100 % des adhérents du GPMSE Installation ont eu recours au chômage partiel ! Et pour 87 % d'entre eux, cette mesure concerne plus de 70 % des salariés. « Les installations étant quasiment à l'arrêt, seules les urgences étant maintenues, les dirigeants n'ont malheureusement pas eu d'autre choix, déplore le président du GPMSE Installation. De ce fait, 55 % d'entre eux estiment que la perte de chiffre d'affaires sera supérieure à 30 %, en 2020. » Triste perspective. D'autant plus que lorsque le déconfinement sera annoncé, l'activité normale ne pourra pas reprendre avant un ou deux mois, le temps que les commandes soient signées... C'est pourquoi, conclut Luc Jouve, « nous sommes très attentifs aux répercussions sociales et économiques que cette crise sanitaire va entraîner car je rappelle que, pour nombre de nos adhérents, il s'agit de petites et moyennes structures ; leur trésorerie ne leur permettra pas malheureusement, pour beaucoup d'entre eux, de se rétablir rapidement. Aussi, nous nous réjouissons de l'accord économique européen pour faire face aux conséquences économiques de cette pandémie et de la mise en place d'un fonds de 500 milliards d'euros. Par ailleurs, il est évident que les entreprises ne récupéreront pas l'intégralité du CA perdu. Aussi, il nous semble indispensable que le gouvernement annule l'ensemble des charges sociales durant cette crise. » ●

LE POINT DE VUE D'UN INTÉGRATEUR



Laurent Bruyère
DIRECTEUR GÉNÉRAL D'ERYMA

« Les contrats de maintenance nous assurent une certaine activité. »

« La crise du Covid-19 a évidemment un impact sur notre activité. Nous avons par exemple dû retarder l'ouverture de nouvelles agences en France. Cependant, grâce à nos contrats de maintenance signés pour des durées de trois à cinq ans avant le confinement et ceux que nous avons pu signer durant cette période, nous pouvons envisager maintenir notre activité de manière pérenne dans les mois qui viennent. »

VIDÉOSURVEILLANCE

Dahua maintient le contact avec ses partenaires

Tendances technologiques, besoins exprimés par ses clients, confinement... Régis Avenel, responsable commercial de Dahua France, fait le point pour PSM.

« **U**n petit rappel historique tout d'abord : les produits Dahua étaient présents sur le marché français depuis 2006, suivis, en 2017, par la création officielle de Dahua Technology France, se rappelle Régis Avenel. Aujourd'hui, en France, Dahua dispose de services techniques, commerciaux, marketing, administratifs. » Le groupe se porte bien. En 2019, Dahua Technology a ainsi réalisé un chiffre d'affaires de 3,73 milliards de dollars soit une croissance de 26.04% par rapport à 2018. Investissant de près de 10% de son chiffre d'affaires annuel en R&D, l'entreprise poursuit sa recherche dans le domaine des technologies vidéo de l'IdO et possède d'ores et déjà des applications dans les domaines de la vidéoprotection numérique, des systèmes de vidéoconférence, des drones industriels, de la lecture de plaques minéralogiques, de la RFID, de la robotique, etc.

Marché français : trois axes de développement

« Notre stratégie de développement sur le marché français se constitue en trois volets : optimisation du réseau de distribution, mise en œuvre du programme Dahua Partner Program (DPP) pour les installateurs et évolution de fournisseur de produits en fournisseur de solutions en

privilégiant le développement commercial des solutions dans trois industries (retail, transport et Safe City), poursuit Régis Avenel. Ainsi, pour optimiser notre réseau de distribution, nous avons sélectionné sept plus grands partenaires de distribution en tant que distributeurs Gold et leur avons proposé un support de A à Z : conseil sur la sélection de produits, analyse de stock, analyse des ventes, formation commerciale, formation technique, etc. »

En ce qui le programme DPP, les partenaires DPP sont classés en quatre niveaux pour symboliser l'évolution de leur implication dans la vente de nos solutions. Ils se gratifient de leur engagement par une remise de fin d'année et des services complémentaires (accès au support avant-vente et après-vente, aux matériels marketing et à l'assistance technique). Ce partenariat implique des engagements réciproques et proportionnels à chaque niveau.

Nouvelle version de Dahua Partner

Dahua a tout récemment lancé la nouvelle version de l'application « Dahua Partner » qui permet aux distributeurs et installateurs de découvrir les nouveaux produits et solutions, de suivre les actualités de Dahua Technology et de demander l'assistance technique pour les projets.



2 QUESTIONS À Régis Avenel, RESPONSABLE COMMERCIAL DE DAHUA FRANCE

Comment avez-vous géré la période de confinement et comment avez-vous accompagné vos partenaires ?

Pendant la période du confinement, l'équipe Dahua France s'organise pour accompagner nos clients et partenaires à distance. Nous organisons régulièrement les webinaires (au moins trois par semaine) pour les former sur les nouveaux produits, solutions, technologies et outils avec les présentations et les vraies démonstrations. Lors des webinaires, nous répondons à leurs questions, les aidons à résoudre leurs problèmes. Nous trouvons que c'est une très bonne façon d'échanger et de coopérer avec nos partenaires pendant cette période spécifique. Nous diffusons beaucoup plus souvent les informations via les réseaux sociaux, les sites Web, les newsletters, etc., à nos partenaires pour assurer qu'ils ont tous les infos nécessaires pour travailler. En matière d'action solidaire, nous avons envoyé depuis le début de l'épidémie en France plus de 3000 masques de protection à nos partenaires pour les protéger ainsi que leurs familles contre le Covid-19.

Quels sont les besoins exprimés par vos utilisateurs ?

Dahua se concentre sur le développement des technologies AI, Full-color et 4k en temps réel sur le marché. Dans le contexte actuel, les utilisateurs finaux ont exprimé leurs besoins liés à l'épidémie Covid-19 et au confinement. Par exemple, les entreprises ont besoin de la solution « Surveillance de température corporelle » pour continuer leurs activités en protégeant la santé de leurs collaborateurs.



VIDÉOPROTECTION



Malgré la pandémie, CASD est optimiste

L'éditeur français de logiciels a bouclé l'année 2019 sur de bons résultats, avec une forte progression de son chiffre d'affaires. Et, malgré la crise du Covid-19, envisage l'exercice 2020 sous de bons auspices.

« L'année dernière, nous avons réalisé un chiffre d'affaires de 6,5 millions d'euros, en hausse de 30 % par rapport à 2018, se réjouit Stephan Laurent, cofondateur de CASD. D'ailleurs, depuis la création de l'entreprise, nous avons toujours connu une croissance à deux chiffres. Et elle a fortement accéléré l'année dernière. »

Comment expliquer ces bons résultats ? « Clairement, les marchés sur lesquels nous nous situons, comme les collectivités locales, sont très demandeurs et en croissance. Cela favorise notre activité. D'autant plus que nous ne sommes pas très nombreux à pouvoir répondre à la demande... », poursuit Stephan Laurent.

Une solution française : un atout

Autre tendance favorisant l'activité de CASD : la sortie de la logique propriétaire. « Nos clients, par exemple les collectivités locales, recherchent des solutions ouvertes, comme les nôtres, qui s'intègrent plus facilement dans des environnements plus vastes,

insiste le cofondateur de CASD. Par ailleurs, dans un contexte qui voit les questions de souveraineté et de proximité prendre de plus en plus de place, le fait d'être franco-français rassure nos partenaires intégrateurs et les utilisateurs finaux. »

Malgré ces bons résultats, se pose tout de même la question de l'après Covid-19. « Bien évidemment nous subissons comme tout le monde cette crise sanitaire avec son lot d'incertitudes. Nous espérons seulement confirmer nos bons résultats de l'année dernière même si plusieurs mois seront vraisemblablement marqués par une baisse de notre chiffre d'affaires. Cependant, notre bonne santé financière va nous aider à traverser cette période. Nous pourrions donc répondre sereinement à la demande en logiciels sur les différents marchés dans lesquels CASD est positionné. Ainsi, j'ai bon espoir que notre chiffre d'affaires progresse malgré tout en 2020 et que nous puissions confirmer notre place de leader sur le marché des collectivités locales. », conclut Stephan Laurent.



© DR

2 QUESTIONS À Stephan Laurent, DIRIGEANT DE CASD

2020 restera sans doute comme une année particulière. Cependant, les affaires continuent. Et plutôt bien pour CASD si on en croit vos bons résultats. Quels sont vos axes de développement une fois la crise du Covid-19 passée ?

Nous voulons renforcer nos positions en Île-de-France. Nos solutions ont été retenues dans le cadre du marché lancé par Yvelines numériques, devenu depuis Seine et Yvelines Numérique, ce qui nous permet de déployer nos produits dans ces deux départements. Par ailleurs, nous sommes aussi référencés sur d'importants marchés pluriannuels en Île-de-France via nos partenaires intégrateurs. Nous allons donc intensifier notre présence afin d'accélérer notre développement en région parisienne, comme nous l'avons fait dans le Nord-Est avec notre partenaire Nomadys.

Côté solutions, des nouveautés dans les mois qui viennent ?

Tout à fait. Nous allons lancer la nouvelle version de VisiMAX : la v.9. Il s'agit d'une évolution assez lourde qui sera disponible à l'automne 2020. CASD sera également partenaire « Gold » de la soirée de l'AN2V qui se déroulera en janvier 2021. Soirée qui sera pour nous l'occasion d'affirmer notre volonté de développement en région parisienne avec la présentation d'une nouvelle organisation en ce sens.



© DR



© DR

VIDÉOSURVEILLANCE HIKTEC SHOW, L'ÉMISSION DE HIKVISION

Depuis le 28 février, sur YouTube, Hikvision vous propose une émission hebdomadaire à visées pédagogiques sur les technologies de la vidéosurveillance. Grâce à cette émission, le géant chinois reste en contact avec son réseau d'intégrateurs et d'installateurs. Le principe d'HikTec Show est très simple : dans un format de cinq et quinze minutes, l'émission traite des nouvelles technologies et de l'écosystème Hikvision.

Le HikTec Show est diffusé tous les vendredis à 10 heures. Vous trouverez le lien de chaque épisode sur les réseaux sociaux de Hikvision. Vous pouvez également vous rendre sur la chaîne YouTube dédiée pour y retrouver l'ensemble des épisodes #HiktecShow. Quelques-unes des vidéos disponibles :

- Produits thermiques ;
- Convergence & Hik-Connect ;
- Interphonie, comment ça marche ?
- Tout savoir sur AXHub ;
- PanoVu Vs Ultra grand-angle (6984/2T45) ;
- Tout savoir sur Hik-ProConnect ;
- Caméras multidirectionnelles PanoVu ;
- Solutions de détection de température ;
- Thermal Design Tool.

CONTRÔLE D'ACCÈS

Partenariat SimonsVoss/Jeedom

Le spécialiste allemand des serrures électroniques autonomes a donc signé un partenariat avec la jeune pousse française Jeedom, spécialisée dans la domotique B to C et B to B...



© DR

« Nous sommes ravis de nouer ce partenariat d'intégration avec un acteur de renommée qui se distingue par la fiabilité et la qualité de ses produits. Dès les premiers échanges avec les équipes SimonsVoss, nous avons tout de suite identifié l'opportunité de répondre ensemble à des besoins globaux de contrôle d'accès. Nos équipes respectives étaient très enthousiastes quant au projet d'intégration des solutions de contrôle d'accès SimonsVoss dans Jeedom », précise David Bonnamour, président de Jeedom.

Le partenariat avec Jeedom s'inscrit dans la nouvelle stratégie d'intégration de SimonsVoss, qui consiste à développer davantage la notoriété de sa gamme SmartIntego, spécialement conçue pour s'intégrer facilement dans les systèmes de contrôle existants et de sécurité des bâtiments (vidéosurveillance, monétique, intrusion, etc.).



© DR

« Grâce à l'interconnexion de nos technologies respectives, nous donnons la possibilité, à travers le logiciel Jeedom, de proposer aux clients finaux de gérer une multitude de solutions communiquant entre elles. »

JEAN-PHILIPPE VUYLSTEKE, PRÉSIDENT DE SIMONSVOSS FRANCE

S'ouvrir à des nouveaux marchés

Jeedom a donc intégré l'ensemble de la gamme et des fonctionnalités SmartIntego de SimonsVoss. Mais comment les deux solutions s'interconnectent-elles ? Les béquilles, les cylindres et les routeurs radio SimonsVoss (GatewayNode) vont communiquer avec la centrale Jeedom. C'est le logiciel de gestion de contrôle d'accès de Jeedom qui est le cerveau de tout le système : on y définit les autorisations d'accès, les plages horaires, etc. Par exemple, au moment où une personne badge sur une porte pour entrer dans un bureau, les cylindres et béquilles SimonsVoss vont remonter l'information en temps réel à la centrale Jeedom, qui va pouvoir vérifier les autorisations attribuées à la personne en question et éventuellement activer en parallèle l'éclairage, allumer le système de chauffage, ouvrir les volets, etc.

J2C a la solution à la fin annoncée du RTC

En 2021, le RTC sera mort. Or, il ne semble pas que les professionnels concernés par cette disparition et leurs clients aient pris la mesure du changement. J2C peut les aider à franchir le cap grâce à son boîtier MutaKom, conçu en partenariat avec Sigfox.

En 2021, le RTC, qui jusqu'à maintenant avait assuré la transmission des alarmes entre la centrale et le PC de télésurveillance, via le réseau France Télécom, aura vécu. « Et, étonnamment, souligne Jordan Philippon-Lebrec, président de J2C, personne ne semble s'en soucier ou alors tout le monde fait comme-ci de rien n'était. En effet, en 2016, Orange a annoncé l'arrêt de ce réseau. Et on ne peut pas dire qu'on soit débordés par les informations à ce sujet. 12 % des lignes téléphoniques sont dédiées à la transmission d'alarmes, donc de nombreux professionnels de la sécurité et leurs clients sont concernés et doivent anticiper cette date. D'autant plus que le remplacement du RTC par l'IP ne sera pas forcément possible... »

À en croire Jordan Philippon-Lebrec, il semble, que comme toujours en France, on prenne conscience des choses au dernier moment. C'est donc pour aider les télésurveilleurs et leurs clients que J2C propose la solution MutaKom, une alternative à la mort annoncée du RTC.

« MutaKom est né d'une rencontre avec le Français Sigfox, pionnier du réseau 4G et premier fournisseur mondial de solution de connectivité dédiée à l'Internet des objets (IoT). De son côté, J2C est un spécialiste des offres de services sur le marché de la sécurité. Nous avons décidé de collaborer pour développer le boîtier MutaKom. »

Des centrales obsolètes

Avec la fin du RTC, un certain nombre de centrales vont être obsolètes. Alors qu'elles fonctionnent encore. Il fallait donc trouver une solution. « Actuellement, rien ne permet de remplacer vraiment la ligne RTC de France Telecom. D'où l'idée de concevoir un boîtier qui reprend le signal RTC pour l'envoyer, via le boîtier, sur un réseau Sigfox. Le signal est ensuite envoyé au télésurveilleur. C'est simple et transparent pour le client. Pour concevoir ce boîtier, nous nous sommes un peu inspirés de ce que nous avons connu lors du passage à la TNT et les boîtiers qu'il nous fallait utiliser pour la recevoir sur nos postes télé », conclut J. Philippon-Lebrec.



© DR

2 QUESTIONS À Jordan Philippon-Lebrec, PRÉSIDENT DE J2C

On a l'impression qu'on ne parle pas beaucoup de la fin toute proche, annoncée pour 2021, du RTC. Pourquoi ?

De nombreux installateurs partent du principe que les fabricants vont gérer eux-mêmes la disparition du RTC. Or, les fabricants ne produisent pas des centrales que pour le marché français. La fin du RTC n'est pas une de leurs priorités. Loin de là. Les installateurs et leurs clients, s'ils ne font pas l'effort d'anticiper la fin du RTC, risquent de bien mauvaises surprises en 2021... D'autant plus que les installateurs sont souvent mal informés, mal documentés... Ils vont subir les choses.

Pourquoi avoir choisi de travailler avec Sigfox ?

Sigfox a fait la preuve de la qualité de son offre. Il s'agit d'un réseau national qui jouit d'une excellente couverture et sa technologie entre assez loin dans les bâtiments et peut fonctionner dans des environnements où d'autres technologies peuvent être sujettes à des perturbations.

INTÉGRATEURS

Les nouvelles ambitions d'Eryma

L'intégrateur veut s'imposer un peu plus sur ses marchés et se développer sur d'autres. Comment ? Par de la croissance organique et le développement à l'international, et de la croissance externe pour renforcer son offre techno.

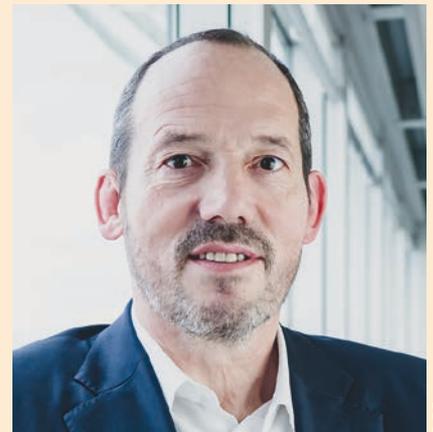
« **A**près le rachat d'Eryma par Sogetrel en 2017, puis l'intégration, en 2019, de la partie "Sûreté numérique" de Sogetrel, Eryma a acquis tout récemment Sécurité Consultants, rappelle Laurent Bruyère, directeur général d'Eryma. *Nous sommes désormais en ordre de bataille pour renforcer notre présence sur certains marchés, nous implanter sur d'autres ou réaliser des opérations de croissance externe qui nous permettront de compléter notre offre solutions et services.* »

Déjà avec Sécurité Consultants, basée à Issy-les-Moulineaux, le spécialiste de la sûreté et de l'intégration de solutions IP se renforce sur le marché de la protection des sites sensibles. « *Sécurité Consultants qui emploie 35 collaborateurs pour 7 millions d'euros de chiffre d'affaires, dont 15 % dans la détection incendie, répond clairement à cette volonté de nous renforcer sur certains marchés comme l'incendie sur lesquels nous pouvons faire beaucoup mieux et*

qui seront pour nous un de nos axes de développement dans les mois et les années à venir », ajoute Laurent Bruyère.

100 millions de CA

Avant l'acquisition de Sécurité Consultants, Eryma réalisait en 2019 un chiffre d'affaires de 70 millions d'euros. « *Notre objectif est clairement de continuer à grandir pour atteindre 100 millions d'euros dans les deux ou trois ans qui viennent*, poursuit le directeur général. *Cela se fera via des opérations de croissance externe ou de croissance organique. La croissance externe devra nous permettre d'acquérir des entreprises dont les savoir-faire ou implantations géographiques nous permettront de renforcer notre présence et de compléter notre offre.* » Avant de conclure : « *La croissance organique, quant à elle, passera par le développement de notre activité à l'étranger et sur des marchés dans lesquels il y a de réelles perspectives de développement pour nous, comme le tertiaire et le luxe.* »



© DR

2 QUESTIONS À Laurent Bruyère, DIRECTEUR GÉNÉRAL D'ERYMA

L'acquisition de Sécurité Consultants marque-t-il une nouvelle étape dans l'histoire et le développement d'Eryma ?

Il est indéniable qu'il nous a fallu nous mettre en ordre de bataille après notre rachat par Sogetrel et l'intégration de sa branche sûreté. Aujourd'hui, nous voulons nous développer et aller conquérir des parts de marchés soit sur des technologies où nous ne sommes pas assez présents comme l'incendie, soit sur des secteurs d'activités où nous avons clairement des arguments à faire valoir. Je pense aux marchés du luxe, des bijouteries, des pharmacies... Notre croissance passera également par le développement de notre activité à l'étranger. Le groupe Sogetrel est déjà présent en Allemagne, en Belgique, en Suisse... mais nous pouvons faire mieux. Nous devons aussi accroître notre présence en France. Depuis novembre 2019, nous avons d'ailleurs ouvert trois nouvelles agences : Clermont, Chartres et Saint-Denis.

Et en matière de technologies, quels sont vos axes de développement ?

Eryma est très orienté marché systèmes. Notre vocation est de proposer et de concevoir pour nos clients les solutions les plus adaptées à leurs besoins à partir de l'offre technique de nos partenaires fabricants. Nos clients recherchent un interlocuteur unique, capable d'associer tous les composants de l'écosystème de la sécurité des bâtiments. L'incendie est l'un de ces composants. Et nous devons muscler nos offres et savoir-faire sur ces techniques. Sécurité Consultants est une première étape. Il y en aura d'autres...



© Sogetrel

VIDÉOSURVEILLANCE

Scutum Group acquiert Kiwatch

Le groupe français dirigé par Franck Namy a finalisé l'acquisition de la société spécialisée dans la conception de solutions intelligentes de vidéosurveillance dans le cloud.

Startup basée en France, Kiwatch développe des services innovants rendant les caméras de surveillance intelligentes et accessibles aux particuliers et aux petites entreprises. Fondée en 2011, la société s'est rapidement développée et pilote aujourd'hui 30 000 caméras connectées.

Avec ce système innovant de sécurité et de plug and play, les clients peuvent sécuriser leur domicile ou leur entreprise de n'importe où, à tout moment. Kiwatch propose également une solution de maintien à domicile par vidéo pour aider les personnes dépendantes ou âgées vivant seules à la maison et s'assurer de leur bien-être à tout moment.

Kiwatch a intégré la technologie de l'intelligence artificielle dans plusieurs applications et ce nouveau partenariat permettra de mutualiser les efforts de développement dans ce domaine des deux sociétés, en vue de

fournir des solutions toujours plus optimales pour répondre aux besoins actuels et mais aussi futurs des clients.

Accélérer le développement

« Nous sommes ravis de ce partenariat avec Scutum Group qui marque une nouvelle étape dans le développement de notre entreprise, se réjouit Olivier Blanchard, directeur général de Kiwatch. L'expertise de trente ans de Scutum Group en matière de sécurité, ses ressources opérationnelles, et l'approche axée sur l'innovation des deux sociétés seront essentielles pour accélérer notre développement. »

Scutum est désormais le premier intégrateur de systèmes dans le secteur de la sécurité à posséder à 100 % une telle solution déployable facilement. Les nouvelles solutions « My Scutum as a Service » pour le segment résidentiel et « Scutum as a Service » pour le segment commercial seront lancées courant 2020.



« L'intégration d'analyses vidéo avancées et de technologies de vidéo intelligente sera cruciale pour fournir des services de toujours plus grande qualité à tous les segments de clientèle du groupe. Kiwatch apporte au groupe une expertise unique dans le domaine des solutions « As a Service » pour offrir des services évolutifs à nos clients – grands comptes, PME, partenaires installateurs, etc. – en plus de nos solutions traditionnelles. »

FRANCK NAMY, PDG DE SCUTUM GROUP



© Kiwatch



© Parrot

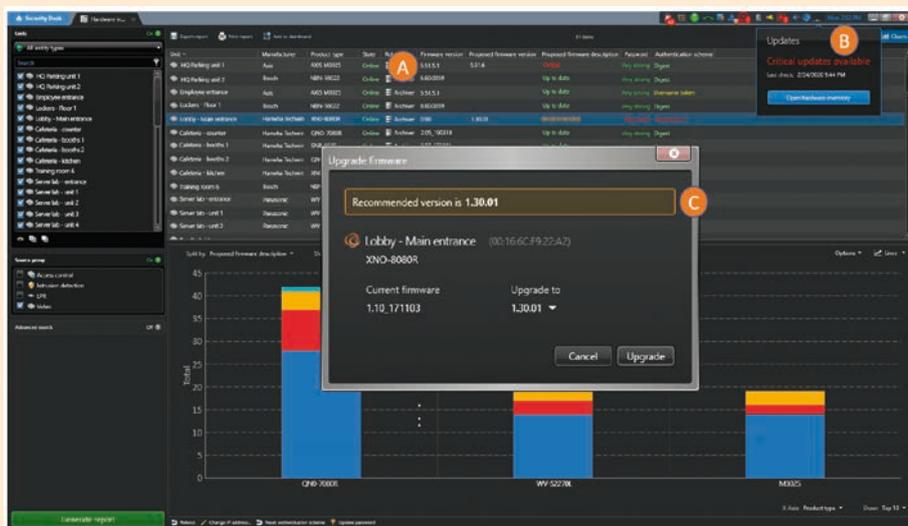
DRONES LE DÉPARTEMENT DE LA DÉFENSE US CHOISIT PARROT

Parrot a franchi une nouvelle étape dans le programme de drone SRR (Short Range Reconnaissance) de l'US Army puisque le Français participera à une évaluation opérationnelle pour appuyer la décision d'attribution de la production de l'US Army. En prévision d'une augmentation de la demande du département de la Défense, Parrot commencera à produire les prototypes du drone dédié à ce programme aux États-Unis. Le prototype final présenté par Parrot, conçu avec des composants sélectionnés pour être conformes aux exigences de l'armée et du gouvernement américain, a donc été approuvé pour entrer en production. C'est avec son partenaire NEOTech que Parrot s'est associé pour finaliser la mise en place de sa chaîne de production aux États-Unis pour fabriquer le lot de prototypes de très haut standard qui seront livrés à l'US Army et à la DIU (Defense Innovation Unit) en juillet 2020. L'assemblage final du prototype se fait également de manière très sécurisée et contrôlée avec l'installation au sein des sites de NEOTech de tous les logiciels développés par Parrot à Paris (France) garantissant ainsi la fiabilité du produit et de sa gestion des données.

VIDÉOSURVEILLANCE

Genetec Firmware Vault prend en charge Axis, Bosch, Hanwha et Panasonic

Firmware Vault permet aux administrateurs informatiques et aux intégrateurs système de maintenir les micrologiciels de leurs caméras à jour et de s'assurer qu'ainsi elles sont protégées contre les cyberattaques.



© Genetec

Firmware Vault, service de mise à jour du micrologiciel des caméras développé par un fournisseur de VMS à architecture ouverte, prend désormais en charge les caméras Axis, Bosch et Panasonic, en plus des caméras Hanwha Techwin. Firmware Vault a été conçu pour aider les administrateurs informatiques et les intégrateurs système à suivre le rythme des mises à jour des micrologiciels de leurs caméras, et permettre ainsi aux entreprises de s'assurer qu'elles disposent de la dernière protection offerte par les fabricants contre les cybermenaces. Les micrologiciels de caméra obsolètes constituent l'une des plus grandes faiblesses des défenses de cybersécurité de

l'entreprise. Mais pour beaucoup d'administrateurs de sécurité, tenir le rythme des mises à jour peut prendre énormément de temps. Selon une récente étude menée par Genetec, 68,4 % des caméras (soit près de sept sur dix) fonctionnent actuellement avec un micrologiciel obsolète.

Déployer la cybersécurité

Firmware Vault simplifie le processus de mise à jour du micrologiciel des caméras afin que les clients puissent déployer les dernières mesures de cybersécurité dès qu'elles sont disponibles, une étape cruciale qui permet de garantir la résilience de leur entreprise contre les cyberattaques. Firmware Vault est disponible gra-

tuitement avec Security Center versions 5.8. et ultérieures.

Firmware Vault fait appel au même dépôt cloud ultra-sécurisé que Genetec Update Service pour donner accès aux mises à jour Windows et Security Center. Lorsqu'un nouveau micrologiciel est disponible, les administrateurs système sont informés via l'outil de configuration de Security Center. Cela leur permet de suivre et de télécharger les nouveaux micrologiciels et les toutes dernières mesures de cybersécurité pour les caméras connectées, en quelques minutes.

Une seule caméra suffit...

Il faut s'assurer que toutes les caméras disposent de la version la plus récente de leur micrologiciel. Même si c'est un processus long et fastidieux. Mais Firmware Vault permet de faciliter le processus de mise à jour des micrologiciels. Grâce à lui, les utilisateurs ont une vision unifiée de toutes les caméras et de leur état de mise à jour. Ils peuvent donc prendre des mesures de correction plus vite et plus efficacement.

« Il suffit que le micrologiciel d'une seule caméra de vidéosurveillance ne soit pas à jour pour qu'un réseau informatique soit exposé au risque cyber. »

MATHIEU CHEVALIER, LEAD SECURITY ARCHITECT CHEZ GENETEC

VIDÉOSURVEILLANCE

Un outil pour trouver le bon endroit pour la bonne caméra

Hikvision a lancé un nouvel outil de conception thermique en ligne pour aider les distributeurs, les intégrateurs et les utilisateurs finaux à trouver le bon endroit pour la bonne caméra thermique dans leur solution.

L'outil gratuit rationalise le processus de conception d'une solution et de préparation d'un devis. L'utilisation de données cartographiques SIG en ligne offre des données précises qui fournissent l'échelle correcte, évitant ainsi ces problèmes qui peuvent être frustrants. Surtout, cela fait gagner du temps car il n'est pas nécessaire d'utiliser une carte manuellement et d'ajuster le champ de vision pour faire le bon calcul. L'outil de conception thermique automatise tout cela. Si les données cartographiques ne sont pas encore disponibles pour un site, l'outil pourra toujours fournir une version 2D.

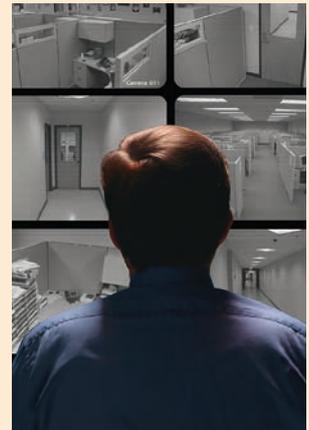
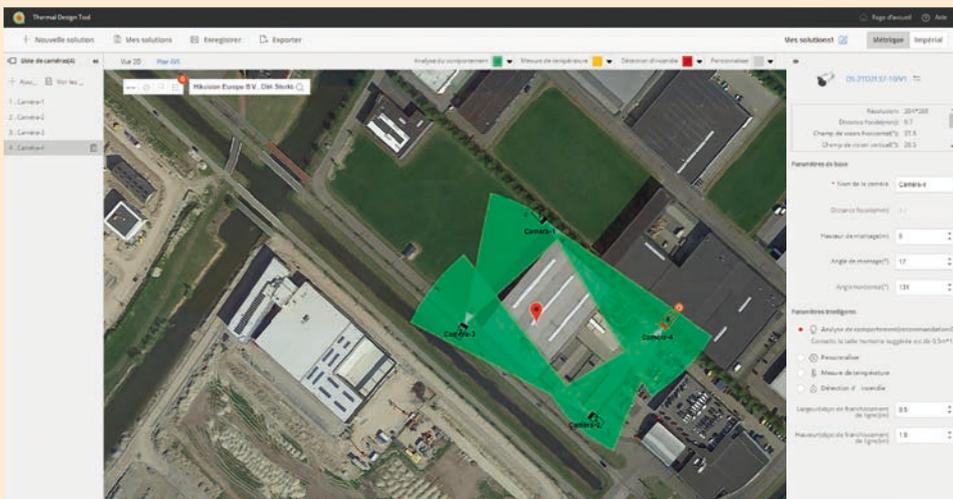
Clair et facile

L'outil crée rapidement un rapport professionnel, ce qui rend une solution technique très claire et facile à référencer. Cela signifie également qu'il peut être utilisé pour une présentation à un client. L'ajustement des plans peut être fait rapidement pour répondre aux besoins du client, et l'impact de tout changement est facile à voir immédiatement. Cela prendra tout son sens pour les solutions de protection périmétrique. Il est également utile dans les scénarios qui nécessitent des caméras avec détection d'incendie (par exemple les incendies de forêt) et la prévention des incendies avec mesure de la température.



« Cet outil de conception thermique simplifie la conception d'une solution thermique, ce qui facilite et accélère la création d'une solution et l'établissement de devis. Désormais en ligne, il n'est pas nécessaire d'installer ou de mettre à jour quoi que ce soit. Cela en fera un outil pratique pour les installateurs et les utilisateurs finaux. »

FRANCK CARETTE, RESPONSABLE DE LA GAMME THERMIQUE CHEZ HIKVISION EUROPE



© Getty Images

VMS NOUVELLE ANNÉE RECORD POUR MILESTONE

Avec un taux de croissance annuel de 14 % au cours des cinq dernières années, les recettes nettes de Milestone Systems ont atteint un peu plus de 138 millions d'euros en 2019. Au cours des cinq dernières années, Milestone Systems a presque doublé le nombre de ses employés pour atteindre plus de 900 personnes. L'année dernière, des investissements accrus ont été réalisés dans la recherche et développement, des équipes d'ingénieurs élargies à Copenhague et à Sofia et la création d'un nouveau pôle d'ingénierie basé à Barcelone. Cependant, en raison de l'apparition du virus Covid-19 au début de 2020, les prévisions, en particulier celles qui concernent les recettes et les bénéfices d'exploitation futurs, sont soumises à des risques et à des incertitudes qui peuvent faire en sorte que l'évolution réelle diffère sensiblement des prévisions.



© DR

SÉCURITÉ ÉLECTRONIQUE ADT RACHÈTE UN DE SES PLUS GROS REVENDEURS

C'est pour la coquette somme de 381 millions de dollars que le géant américain des solutions de sécurité électronique et d'automatisation pour la maison intelligente, a acquis son principal revendeur, Defenders, créé par David P. Lindsey et Jessica A. Lindsey. Fondée en 1998 et basée à Indianapolis, la société Defenders emploie 2 900 personnes, déployées dans plus de 130 succursales. Depuis 2016, ADT Corp appartient à Apollo Global Management qui l'avait acquis pour 6,72 milliards d'euros. Après ce rachat, ADT avait fusionné avec Protection 1, spécialiste de la sécurité domestique acquis en 2015 pour une quinzaine de milliards de dollars. Rappelons qu'ADT était né d'une scission de Tyco International en 2012.



© Seris

SÉCURITÉ MOBILE SERIS SECURITY RENFORCE SA PRÉSENCE EN RÉGION CENTRE

Seris a repris les activités de la société Staff41, basée à Blois, et renforce ainsi sa présence sur le secteur de la sécurité mobile. La reprise du fonds de commerce de Staff41 a eu lieu mi-janvier auprès du tribunal de Blois. Les dix salariés de Staff41 ont intégré le groupe Seris permettant ainsi de préserver des emplois menacés. Comme l'observe Frédéric Allot, directeur des activités de sécurité mobile : « *L'acquisition de Staff41 va permettre au groupe Seris d'intensifier sa présence dans la région de Blois et de proposer davantage de proximité à ses partenaires et futurs clients.* »

Fort de son expertise métier en sécurité et de son expérience, Seris Security propose des prestations sur mesure en adéquation avec le secteur d'activité (aéroportuaire, portuaire, industrie, distribution, tertiaire, événementiel) et la taille des structures demandeuses (TPE/PME, groupes, groupements d'entreprises). Les prestations de sécurité mobile mises en œuvre sont des dispositifs de rondes de sécurité, des patrouilles de proximité, des levées de doute, des interventions sur alarme et des prestations spécifiques à la demande.

INTÉGRATEUR

Contrats pour Spie en Belgique

Ces deux contrats concernent l'installation et la maintenance de caméras de surveillance urbaine pour les zones de police de Vesdre et des Fagnes.



© Getty Images

Spie Belgium, filiale belge de Spie, a remporté de nouveaux contrats dans le domaine de la sécurité urbaine. En l'occurrence l'installation et la maintenance de caméras de vidéosurveillance pour deux zones de police wallonne : celle de Vesdre et celle des Fagnes. Pour la zone de police de Vesdre (communes de Verviers, Dison et Pepinster), Spie Belgium a réalisé l'extension du réseau de caméras de surveillance urbaine et assure la maintenance complète du réseau qui, au total, comprend aujourd'hui 72 caméras dans les rues et un système de « dispatching » sophistiqué. La filiale de Spie a aussi remporté une commande de dix caméras supplémentaires pour la zone de police de Vesdre qui disposera ainsi d'un des réseaux de vidéosurveillance les plus denses de Belgique. Spie Belgium a également obtenu un second contrat en surveillance urbaine de la zone de police des Fagnes (communes de Spa, Theux et Jalhay), pour l'installation et la maintenance de nouveaux systèmes de vidéosurveillance au sein des commissariats et l'extension du réseau de caméras de la zone.



ABONNEZ-VOUS MAINTENANT À PSM!



protectionsecurite-magazine.fr/abonnement



Les solutions pour les professionnels de la Sûreté - Sécurité



SOMMAIRE



26



31



44



56



60

3 actus prestataires

16 actus sûreté

26 entretien
FRÉDÉRIC GAUTHEY
Président du GES

31 dossier
CLOUD ET SÉCURITÉ

40 vidéosurveillance
Voir dans le noir ?
Oui, mais pour faire quoi ?

44 contrôle d'accès
Interphonie avec ou sans fil ?

50 focus
Détection intrusion

52 intrusion
Grâce aux radars,
suivez à la trace les intrus

56 incendie
Maintenance des extincteurs : à
ne négliger sous aucun prétexte !

60 risque
Les datacenters : la sécurité à 360°

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

74 c'est vous qui le dites !
DRISS AÏT YOUSSEF, docteur
en droit, président de l'institut
Léonard de Vinci

TPMedia

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

SECRETARIAT 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

Getty Images



ÉDITO



© DR

À période spéciale, numéro spécial

La crise du Covid-19 n'a pas bouleversé que le monde de la sécurité. Elle a aussi provoqué quelques changements dans votre magazine préféré. Actualité oblige, nous consacrons donc plusieurs articles aux conséquences de cette crise et du confinement sur les métiers de la sécurité, sur son industrie et le célèbre continuum sécurité qui semble bien devoir être une des victimes du virus venu de l'empire du Milieu...

Vous pourrez aussi constater dans notre dossier sur le « cloud et la sécurité », que le confinement a été une excellente occasion de découvrir, pour certaines entreprises, l'intérêt de disposer d'un « nuage ». Ne serait-ce que pour basculer en télétravail et lisser la sortie du confinement. Crise qui a aussi permis à certains patrons de constater l'utilité d'avoir une direction sécurité-sûreté digne de ce nom. Comme quoi, il n'est jamais trop tard. Par ailleurs, depuis le début de la crise du Covid-19, PSM est très présent sur LinkedIn. Sa page (www.linkedin.com/company/11405844/admin/) est entièrement à votre disposition pour y échanger informations, bonnes pratiques, outils, retours d'expériences, infos sur le coronavirus... N'hésitez pas à vous en servir. Enfin, en cette période compliquée, toute l'équipe du magazine tient à remercier ses annonceurs pour leur fidélité. Leur confiance nous honore et nous incite à être aussi à leurs côtés afin de les aider pour relancer leurs activités. Bonne lecture.

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



La crise confirme l'importance des directions sécurité-sûreté



© Getty Images

Tant pour les entreprises et leurs directions sûreté, quand elles en ont une, que pour les professionnels de la sécurité, la crise du Covid-19 aura au moins eu le mérite de révéler certaines choses et d'en confirmer d'autres...

« Cela peut paraître étonnant mais la crise du Covid-19 et le confinement ont agi comme un révélateur : certaines entreprises ont découvert qu'elles avaient, à disposition, à portée de la main, un expert de la gestion de crise : le directeur de la sécurité/sûreté et ses équipes, se réjouit Stéphane Volant, président du CDSE (Club des directeurs de sécurité des entreprises). Dans ces entreprises, certains membres des comités exécutifs ignorent ou méconnaissent parfois le rôle précis de cette direction au sein de leur structure. Ils ont pu ainsi constater le

bien-fondé, l'intérêt pour la continuité des activités, d'avoir à ses côtés, dans la salle de crise, cet expert qui, soit dirige la gestion de crise soit y prend une part active. »

Le constat du président du CDSE en étonnera plus d'un. Mais il n'est pas aussi surprenant qu'il peut en avoir l'air. En effet, les directions sécurité/sûreté sont encore perçues, dans de nombreuses entreprises, comme faisant partie des fonctions supports. Ni plus, ni moins. « Cette crise a donc été, pour certains des adhérents du CDSE, l'occasion de montrer leur utilité dans la gestion de la crise actuelle, mais aussi pour le futur, insiste

Stéphane Volant. Et de nombreux directeurs sécurité/sûreté ont pu démontrer que la sécurité est un investissement à la rentabilité avérée pour le futur, et non un coût. »

Gérer la crise et en sortir

Avant d'ajouter : « Durant cette crise, le CDSE accompagne ses adhérents, les soutient, leur délivre de l'information. Nous avons mis en place une salle de crise virtuelle sur "Citadel", une application souveraine de Thales qui sert aussi en temps normal aux échanges entre les membres du Club. Grâce à notre relation forte avec les

« Nous ne disposons pas d'outils français, réellement souverains, équivalents à ceux des Gafam. »

STÉPHANE VOLANT, PRÉSIDENT DU CDSE

2 QUESTIONS À

STÉPHANE VOLANT

Président du CDSE



© DR

Le 9 avril dernier, dans un communiqué de presse, le CDSE a demandé aux pouvoirs publics de préciser les «conditions nécessaires à la reprise des activités

dans les entreprises». Sur quels points portaient ces précisions?

Je sais, de mes échanges avec Jean Castex, que l'État a commencé à réfléchir à la sortie du confinement dès l'annonce de cette mesure par le président de la République, le 17 mars dernier. C'est pour cela que, début avril, nous avons demandé quelques éclaircissements à l'État sur certaines mesures qui nous paraissent nécessaires pour que la reprise d'activité se passe dans les meilleures conditions.

Nos demandes d'éclaircissements portaient entre autres sur :

- Permettre aux entreprises d'identifier les circuits d'approvisionnement robustes et durables en équipements de protection individuelle et en préciser les conditions d'importations/réexportations ;

- Définir une nomenclature du port des équipements de protection individuelle nécessaires à chaque activité professionnelle (types de masques, etc.) ;
- Définir et organiser la politique de test sérologique par la médecine du travail ;
- Définir les nouvelles règles de contrôle sanitaire qui devront accompagner la reprise d'activité (nettoyage, désinfection des locaux, mesures de distanciation au sein de l'entreprise) ;
- Préciser la doctrine de l'État en matière de prise de température à l'entrée des entreprises et des établissements recevant du public. Et accompagner cette mesure d'une évolution du cadre réglementaire afin d'exonérer le donneur d'ordre en cas de « faux positif », à l'instar de ce qui existe déjà à l'égard de tout citoyen ou salarié utilisant un défibrillateur cardiaque.

Et de façon plus prospective sur l'évolution nécessaire de certaines réglementations relatives à l'élaboration de plans de continuité d'activité dont quelques-unes se sont récemment avérées inadaptées à l'égard des opérateurs d'importance vitale.

Je crois qu'une de vos demandes concernait aussi la souveraineté technologique de la France...

En effet. Cette crise a mis en lumière le manque criant de technologies souveraines capables de garantir la fluidité et la confidentialité des échanges lorsque le confinement rend le télétravail indispensable. Beaucoup de professionnels de la sécurité jugent que cette situation est aberrante. Surtout à une époque où les données générées et utilisées par les entreprises constituent le nerf d'une guerre à bas bruit. Le problème est d'autant plus prégnant que lorsqu'on utilise ces technologies, ces outils – pour la plupart conçus aux États-Unis, on s'expose à passer un jour ou l'autre sous les fourches caudines du droit américain dont la volonté affirmée à l'extraterritorialité est de plus en plus inquiétante. Je plaide donc, mais je ne suis pas le seul, pour que certaines applications utilisées par les entreprises françaises soient contraintes de faire la preuve de leur caractère souverain et que lorsqu'on les utilise on ne soit soumis qu'aux lois et réglementations françaises. Pas à d'autres.

pouvoirs publics, je pense notamment au cabinet du préfet de police de Paris, au centre de crise et de soutien du ministère de l'Europe et des Affaires étrangères, à la DGE de Bercy, cette salle de crise nous permet d'échanger des informations qualifiées afin d'anticiper l'impact de chaque décision gouvernementale. Mais il s'agit également d'un échange de bonnes pratiques et d'une possibilité d'entraide : comme quand il s'agit de trouver une solution pour le rapatriement des collaborateurs d'un confrère... Cette crise a montré que le CDSE était important, qu'il avait un rôle à jouer et à assumer grâce à ses liens avec l'État.»

Maintenant, il s'agit de préparer la sortie du confinement, la reprise de l'activité et l'après-crise, pour en tirer les leçons... «Il fallait très tôt préparer la sortie de cette crise, l'anticiper, afin de pouvoir aider à la reprise de l'activité en douceur», souligne notre interlocuteur.» Pour cela, il fallait mettre en place plusieurs équipes. Tout d'abord, deux équipes qui devaient se relayer pendant la crise. Une troisième équipe

devait être chargée de gérer «la crise dans la crise», c'est-à-dire tous les incidents et actes de malveillance pouvant survenir pendant la crise du coronavirus. On a d'ailleurs pu constater que les hackers et autres pirates n'avaient pas chômé pendant cette période... Enfin, une quatrième équipe devait avoir pour mission la reprise de l'activité, donc de l'après-crise.

Des éclaircissements urgents

«Pour nous aider à sortir de la crise, il va falloir que certains assument leurs responsabilités et prennent des décisions», insiste le président du CDSE. Par exemple sur la prise de température dans les entreprises. Et qu'on nous dise, enfin, qui peut ou doit s'en charger, tout en exonérant chacun – donneur d'ordre, collaborateur ou prestataire - d'une quelconque responsabilité en cas de faux positif ou de faux négatif, comme cela peut être le cas dans le cadre de l'usage d'un défibrillateur. N'est-il pas temps d'élargir le champ de compétences de la sécurité privée? Et de faire en sorte que ces agents,

dûment formés, puissent venir en soutien, en ces temps difficiles, des entreprises?»

Outre la place qu'on doit accorder à la sécurité privée dans ce type de crise – mais nous y reviendrons plus loin – le Covid-19 et le confinement ont mis en lumière l'épineux problème de la souveraineté française pour certains outils et technologies...

«Jamais les échanges numériques n'ont été aussi nombreux que durant la période que nous vivons», constate Stéphane Volant. Échanges qui se faisaient et se font encore via des applications plutôt conçues outre-Atlantique et qui, de facto, peuvent donner accès aux données, aux informations échangées... Et que dire du cloud?* Nous ne disposons pas d'outils français, réellement souverains, équivalents à ceux de Microsoft, Amazon, Apple et consorts! Il va clairement falloir se poser la question de se donner les moyens de reconquérir une certaine forme de souveraineté en la matière! Et se demander si la France veut être souveraine technologiquement.» ■

* Voir notre dossier consacré au cloud page 31.



Les directeurs sécurité-sûreté au cœur de la lutte

Les directeurs sécurité-sûreté sont à pied d'œuvre depuis le début de cette crise, travaillant de concert avec une équipe pluridisciplinaire. Contribuant amplement à la lutte contre le Covid-19, leur rôle est donc majeur durant cette crise.

Pour mieux appréhender le rôle des directions sécurité/sûreté durant cette crise, l'Agora des directeurs sécurité-sûreté, le collège national constitué des présidents des neuf clubs, a sondé ses 450 membres. voici les résultats.

« Les sociétés ayant dû totalement fermer leurs sites durant cette période indiquent avoir renforcé leurs dispositifs de protection et de sécurité. Ce qui s'est traduit, plus particulièrement, par un accroissement de la surveillance humaine (pour 64 % d'entre eux), de la surveillance électronique (pour 42 % d'entre eux), ainsi que, dans une moindre mesure, la mise en place de dispositifs de sécurité électronique innovants. Et si le renforcement de ces dispositifs a largement contribué à la lutte contre la propagation du Covid-19, ils ont quelque peu permis la prévention de certaines incivilités et autres déprédations », souligne Marc Viethen, coprésident du collège national de l'Agora des directeurs sécurité-sûreté.

Renforcement des mesures de sécurité

Les mesures de lutte contre la propagation du Covid-19 concernent également les organisations dites essentielles. Aussi, 74 % des acteurs concernés, ayant répondu au sondage, déclarent un renforcement des mesures de sécurité, via un accroissement des procédures de sécurité/sûreté, dans 92 % des cas, et une augmentation du nombre d'agents de sécurité dans 36 % des cas.

75 % annoncent une modification de la configuration des espaces, comme la fermeture de certains accueils au public et le réaménagement de ceux restés ouverts, avec, parfois, l'instauration d'un filtrage incluant parfois l'utilisation de moyen technologiques supplémentaires. Des hygiaphones ont de nouveau été mis en place, notamment dans les PC de sécurité. Par



© Getty images

« Les sociétés ayant fermé leurs sites ont renforcé leurs dispositifs de sécurité. »

MARC VIETHEN, ACORA DES DIRECTEURS SÉCURITÉ-SÛRETÉ

ailleurs, 92 % des répondants ont mis en œuvre des process particuliers, comme le décalage de prises de postes, de façon à limiter les contacts, le report d'opérations non urgentes dans les centres hospitaliers, l'accueil limité et individualisé de clients avec le respect des distances pour les banques... Certains ont instauré la prise de température, de façon manuelle ou via des caméras thermographiques.

Plans de reprise d'activité

Emmanuel Macron ayant annoncé une sortie du confinement à partir du 11 mai, cette décision donne le signal de la mise en œuvre du plan de reprise d'activité, pour de nombreuses organisations. 70 % des structures, à l'heure où nous imprimons, avaient soit déjà préparé un plan de reprise d'activité (20 %), ou étaient en train de le mettre en place (50 %). Dans 70 % des cas, il s'agit essentiellement de mesures barrières, avec, en priorité, la mise à disposition de masques pour un port obligatoire, ainsi que la mise à disposition de gel (pour 80 % des répondants). En outre, 90 % affir-

ment avoir identifié des circuits d'approvisionnement fiables et durables en équipements de protection individuelle.

Par ailleurs, notons que près de 60 % des sondés annoncent une reprise d'activité progressive, avec un maintien en télétravail dès que cela est possible, la continuation des visioconférences pour limiter les réunions physiques, et une restriction, voire une interdiction de déplacements professionnels, au moins dans un premier temps. Concernant la prise de température, les avis divergent, laissant entendre la nécessité d'analyser les atouts et les risques liés à ces technologies actuellement proposées et l'importance de dialoguer avec les partenaires sociaux, en amont. Quant à la réalisation de tests de détection, ils sont près de 70 % à considérer cette disposition utile, voire nécessaire.

Quelles relations avec les pouvoirs publics, durant la crise ?

Ce sondage met en exergue le fait que, pour 83 % des structures auxquelles ap-

partiennent les membres de l'Agora des directeurs sécurité-sûreté ayant répondu, l'application du continuum de sécurité semble effective, au moins en partie. Ce, parfois de manière informelle; chacun échangeant avec certains acteurs, en particulier. Néanmoins, il apparaît que nombreux sont ceux qui considèrent un manque de communication et d'échanges avec les services de l'État. Ainsi, près de 70 % attendent davantage de visibilité quant aux priorités, dans le cadre du déconfinement. En effet, de nombreuses questions subsistent, portant entre autres sur les transports publics, les réponses juridiques aux solutions électroniques actuellement proposées, notamment pour la prise de température, les enjeux liés à la réouverture des restaurants d'entreprise, des centres commerciaux, la réouverture de frontières, les mesures nationales pour anticiper une nouvelle pandémie...

Près de 80 % demandent une visioconférence avec les représentants du ministère de l'Intérieur et 42 % souhaitent égale-

LE POINT DE VUE DE

MARC VIETHEN

Coprésident du collège national de l'Agora des directeurs sécurité-sûreté



© DR

« De nombreux directeurs sécurité-sûreté regrettent un manque de communication et d'échanges avec les services de l'État. Ils souhaitent donc davantage de visibilité quant aux priorités, dans le cadre du déconfinement. En effet, de nombreuses questions subsistent, portant notamment sur les transports publics, les réponses juridiques aux solutions électroniques actuellement proposées, notamment pour la prise de température, les enjeux liés à la réouverture des restaurants d'entreprise, des centres commerciaux, la réouverture de frontières, les mesures nationales pour anticiper une nouvelle pandémie... »

ment échanger avec des représentants du ministère du Travail. Plusieurs signifient vouloir aussi s'entretenir avec un représentant du ministère de la Santé. « J'appelle de mes vœux l'organisation, sans plus attendre, de visioconférences avec les re-

présentants des pouvoirs publics, pour mettre en place des dispositifs efficaces, dans le cadre de la lutte contre la propagation du virus, lors du déconfinement », conclut Marc Viethen. ■

Paxton10

Contrôle d'accès | Gestion vidéo | Un système



Le système le plus puissant de Paxton



1000
portes



1000
caméras



Identifiants
intelligents Bluetooth



Compatible avec
PaxLock et Entry



Intégration
intrusion et incendie

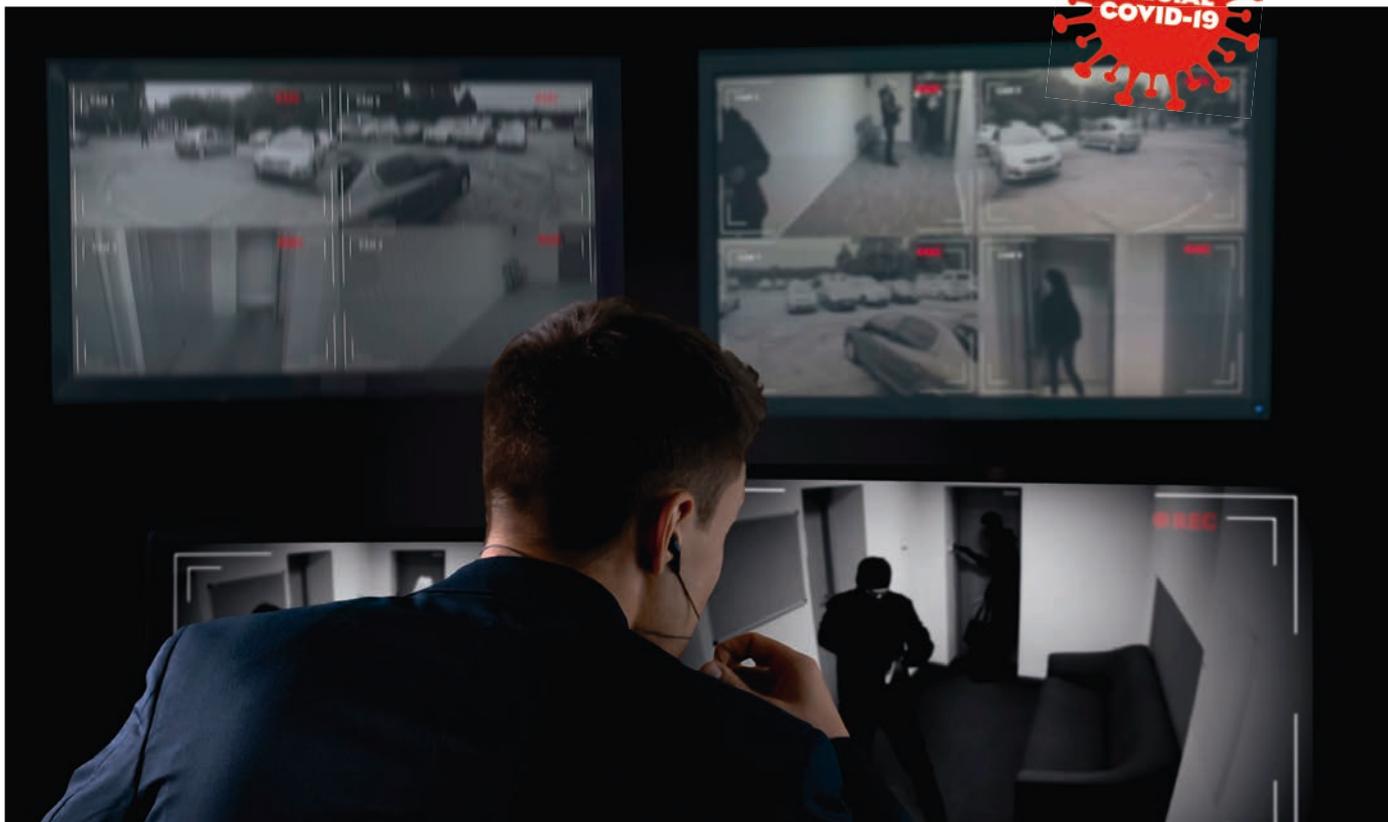


Système
modulaire



Parfaitement
simple

Pour en savoir plus, réservez dès aujourd'hui la formation Paxton10 à paxton.info/5156



© DR

COVID-19/SÉCURITÉ PRIVÉE

Un continuum mis à mal par la crise

Baisse et pertes d'activité, chômage partiel, pénurie d'agents... la crise du coronavirus a malheureusement eu un impact négatif sur le prétendu « continuum de sécurité » et sur l'activité économique de la filière. Tout le monde va-t-il s'en relever ?

Le confinement a évidemment un impact sur l'activité des entreprises comme le montre une enquête réalisée par le GES auprès de ses adhérents dont l'activité aurait connu une baisse de 20 %, en moyenne, en mars 2020, par rapport à février 2020 et mars 2019. Et ce sont les petites entreprises qui sont les plus touchées. Cette réduction d'activité a entraîné un recours à l'activité partielle : 16,5 % des salariés du secteur de la sécurité privée ont été mis en chômage partiel, montrant une modération dans le recours à ce dispositif par rapport à un taux plus important de réduction d'activité. Globalement, près de 30 000 salariés du secteur de la sécurité privée se sont retrouvés en chômage partiel. Les petites entreprises ont eu moins recours à l'activité partielle, en raison de contrats d'une durée plus courte et n'ayant donc pas été reconduits. Les entreprises de plus grande taille ont adapté leur voilure en salariés en propor-

© DR

tion identique, sinon moindre, que la réduction d'activité. Dans le cadre de la réduction globale de 20 % de l'activité, une partie non négligeable des entreprises a connu des demandes supplémentaires d'activités et d'effectifs, majoritairement les grandes et moyennes entreprises, pour 84,5 % d'entre elles. Environ la moitié des petites et très petites entreprises font face à ces demandes supplémentaires. Les lieux et activités concernés sont le retail alimentaire, les établissements de santé, les Ehpad, certains sites tertiaires et industriels et infrastructures logistiques.

Un continuum sécurité mal en point

« Cette crise aura été marquée par la très grande difficulté du ministère de l'Intérieur à la gérer. On peut même parler de catastrophe, souligne Nicolas Le Saux, président d'Atao. Et je ne



NICOLAS LE SAUX, PRÉSIDENT DATAO

« L'État devrait prendre en direct la sécurité des entreprises publiques. »



2 QUESTIONS À

GUILLAUME FARDE

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

Les professionnels de la sécurité privée reprochent une absence de considération et de soutien de la part de leurs autorités de tutelle lors de cette crise. Cette amertume est-elle fondée ?

Les relations entre les professionnels de la filière et leurs interlocuteurs au ministère de l'Intérieur pâtissent d'un manque de vision politique. À considérer que la politique publique de sécurité est mise en œuvre par une diversité d'acteurs, il appartient à l'État de définir le fameux qui fait quoi avec quels moyens et avec quel contrôle. Tant que cet exercice de clarification n'aura pas lieu, les difficultés perdureront. Il ne faut toutefois pas prendre ces difficultés pour prétexte et ressortir les vieilles antiennes anti-État. Est-il besoin de rappeler à quoi ressemblait le secteur avant la création du Cnaps... L'État n'est certainement pas le problème, mais bien la solution aux problèmes !

Que faudrait-il faire pour améliorer les relations entre les pouvoirs publics et la sécurité privée ?

J'évoquais à l'instant l'absence de vision politique. Chacun s'accorde sur le principe d'une coopération public-privé. Il faut donc rapidement en définir les modalités. Le ministre de l'Intérieur doit exposer sa vision politique de ce fameux continuum de sécurité nationale, et fixer une feuille de route à son administration. À cet effet, créer un poste de conseiller à la sécurité privée au cabinet du ministre de l'Intérieur serait de nature à fluidifier les relations et, symboliquement, cela aiderait la sécurité privée à sortir de la vision négative dont elle souffre encore.

parle même pas de la vacance du Cnaps en matière de conseil. Si le ministère et le Cnaps ont réussi le tour de force de faire l'unanimité du secteur contre eux, ce n'est ni sain ni cause de réjouissance... » Il semble que nombreux dans la filière n'attendaient pas grand chose du ministère. À les en croire, ils n'ont pas été déçus. « Je pense qu'il va nous falloir apprendre à travailler avec moins d'État, sans le ministère de l'Intérieur, poursuit Nicolas Le Saux. L'État s'est dispersé et a perdu en efficacité. Compte tenu de la situation économique du pays, qui va sortir très affaibli de cette crise, l'État doit concentrer ses ressources sur des secteurs comme la police, l'armée, la santé, la justice. On ne doit pas espérer qu'il en consacre à la sécurité privée. » Par ailleurs, certains marchés, grands consommateurs de prestations de sécurité privée, sont très fortement touchés et affaiblis par la crise. Les entreprises de sécurité qui travaillent sur ces secteurs – l'événementiel, ● ● ●



« Il ne faut pas demander au Cnaps plus que ce qu'il est censé faire. »

FLORIAN PETTE, FONDATEUR DU GROUPE SCP ET PRÉSIDENT DE SECURALLIANCE

LE POINT DE VUE DE

ELIAS NAHRA

Président fondateur du groupe Triomphe Sécurité



« Nos autorités de tutelle ont été aux abonnés absents. Une surprise pour moi ? Pour d'autres ? Non. Alors qu'il faut souligner que la sécurité privée n'a pas failli. Nos sociétés et leurs agents ont assuré 95 % des missions qui leur étaient confiées.

Il faut tout de même le souligner. Alors, certes, l'État a plutôt bien accompagné l'aspect financier de la crise. Mais pour le reste... On est passé à côté d'une occasion qui aurait pu montrer que la sécurité privée pouvait vraiment venir en soutien des forces de l'ordre, pour les soulager et leur permettre de se concentrer sur d'autres missions. »

HTDS
Hi-Tech Detection Systems

Optez pour des solutions d'inspection efficaces !

- Scanners Rayons X
- Solutions d'inspection des personnes
- Solutions d'inspection véhicules & conteneurs
- Solutions NRBC

HTDS vous propose des solutions **dissuasives, fiables et économiques** pour limiter vos risques

HTDS : 3 rue du Saule Trapu - 91 300 Massy - Tel : +33 1 64 86 28 28
Fax : +33 1 69 07 69 54 - Mail : info@htds.fr - Site : www.htds.fr

LE POINT DE VUE DE LA FFPS

CLAUDE TARLET

Président de la Fédération française de la sécurité privée



© DR

« L'ÉTAT NOUS PERÇOIT ENCORE COMME UNE VARIABLE D'AJUSTEMENT. »

« Cette crise agit comme un révélateur : elle montre, de manière patente, que les pouvoirs publics, l'État... connaissent mal notre filière et ses activités. Ils n'en ont qu'une vision partielle, biaisée, se limitant souvent aux seuls agents de sécurité privée que nous croisons tous dans les centres commerciaux, lors des événements sportifs ou culturels... Or, ce secteur qui rassemble 32 000 entreprises, réalisant un chiffre d'affaires annuel de 12 milliards d'euros, est beaucoup plus diversifié qu'on ne le croit. Ses métiers vont du transport de fonds à la sûreté aéroportuaire, en passant par l'installation et la maintenance des systèmes de sécurité électronique, la télésurveillance de sites parfois très sensibles, la sécurité portuaire, la surveillance par drones... La déception est donc grande. Et nous ne pouvons que regretter ce décalage considérable entre les promesses qui étaient faites lors des travaux parlementaires, il y a encore quelques mois, et la réalité à laquelle nous devons faire face aujourd'hui... Les pouvoirs publics nous considèrent comme une "variable d'ajustement"... sans nous percevoir comme une activité essentielle à la bonne marche de l'économie française. »

● ● ● par exemple – peuvent redouter des jours difficiles. La dépendance risque d'avoir pour elle des conséquences terribles...

Encore besoin de l'État ?

« On peut légitimement se poser la question, confirme le président d'Atao. En revanche, l'État devrait prendre en direct la sécurité des services publics. Il pourrait créer ainsi une force supplétive mobile et adaptable pour les crises, tout en arrêtant, en tant qu'acheteur, de tirer le secteur vers le bas. »

Pour Geoffroy Castelnaud, directeur général de DPSA Île-de-France, « cette crise va avoir de lourdes conséquences sur notre filière. Certaines entreprises ne vont pas s'en remettre. La crise aura au moins eu le mérite de faire comprendre à beaucoup qu'il n'y a pas grand-chose à attendre de nos autorités de tutelle – comme le Cnaps – et que le continuum de sécurité est quasiment une coquille vide. Il a d'ailleurs été mis à mal dès le début du confinement. Il faut tout de même se rappeler que nos agents qui sont "censés participer à une continuité de l'activité économique du pays" étaient très régulièrement arrêtés et contrôlés par les forces de l'ordre. »

Nicolas Le Saux et d'autres souhaitent profiter de cette crise pour revoir l'organisation de la profession. « Pourquoi ne pas mettre en place une guilde, voire ordre – rassemblant donneurs d'ordres, prestataires, experts, groupements professionnels, syndicats – qui serait un outil de conseil, de certification et de bonnes pratiques, dans le cadre de la loi et en complément du Cnaps. Cela permettrait à toute la filière d'avoir plus de poids, de réellement peser sur certaines décisions ayant un impact sur nos métiers. Ce serait aussi un excellent outil pour définir ce qui est souhaitable pour nos métiers et vis-à-vis du client. Sans toujours attendre le soutien de l'État », conclut ainsi Nicolas Le Saux.

À RETENIR

- De 20 % à 25 % de baisse d'activité ;
- Environ 16,5 % de chômage partiel ;
- 75 % des entreprises ont des demandes d'effectifs supplémentaires qui ne couvrent pourtant pas la baisse d'activité.



© DR

« Cette période aurait pu être l'occasion de redéfinir le champ d'action de la sécurité privée... »

GEOFFROY CASTELNAU, DIRECTEUR GÉNÉRAL DE DPSA ÎLE-DE-FRANCE



© Getty Images

Florian Pette, fondateur du Groupe SGP et président de Securaliance, de conclure : « Cette crise a été violente pour tout le monde. Les entreprises de notre filière travaillant dans le retail et l'événementiel vont évidemment être les plus touchées. Vont-elles toutes se relever ? S'en sortir ? À l'inverse, les entreprises travaillant avec la grande distribution n'ont sans doute pas trop subi la crise mais ont vu leurs agents particulièrement exposés au risque. Mais, je veux relativiser le discours alarmiste de certains. Certes, cette crise a et aura un impact économique sur notre activité mais je ne pense pas que nous soyons le secteur le plus à plaindre. Enfin, en ce qui concerne les critiques envers le Cnaps, il ne faut pas lui en demander plus que ce qu'il est censé faire. C'est une autorité de régulation qui contrôle, sanctionne, conseille et assiste la profession. Il a sans doute failli sur ces derniers points mais il a assez vite réagi sur le renouvellement des cartes professionnelles. » ■

LE LECTEUR **BLEU** POUR PASSER AU VERT



Architect® Blue est le seul lecteur de contrôle d'accès haute sécurité sans résine. Une conception doublement efficace qui réduit l'impact environnemental et résiste aux épreuves du temps.

- Un fonctionnement garanti dans tous les environnements (pluie, gel, poussière, détergents...),
- Une résistance aux chocs ou actes de vandalisme (IK10),
- Une conception évolutive et modulaire pour vos besoins de demain.



www.stid-security.com

WE'VE GOT YOUR BACK





COVID-19/VIDÉOSURVEILLANCE

Quand les caméras se font auxiliaires des polices



© DR

Nantes, Le Mans, Annecy, Chambéry... on ne compte plus les villes qui, pour s'assurer du respect du confinement, ont pu compter sur leur réseau de caméras de surveillance. Certaines ont même profité du confinement pour tester de nouvelles technologies de contrôle...

Au Mans (Mayenne), les hommes de la police municipale peuvent compter sur les caméras de surveillance pour s'assurer, par leurs concitoyens, du respect du confinement décidé le 13 mars par le président de la République. En effet, les policiers municipaux se servent des 65 caméras de la ville et des images transmises au CSU (centre de supervision urbaine) pour cibler et contrôler les zones où certains, faisant fi des consignes, continuent à se regrouper. L'aide technique que constitue les caméras est d'autant plus appréciée que la police municipale du Mans, pandémie du Covid-19 oblige, assure ses missions avec des effectifs réduits : six agents sur les trente en temps normal.

À Annecy, les 80 caméras de l'installation de vidéoprotection (couvrant 80 % du territoire de la ville) aident, elles aussi, la mairie à contrôler les « récalcitrants » à respecter le confinement... Le but de tout cela : intervenir là où des groupes de personnes se constituent ou stationnent, pour, finalement, faire respecter les mesures de confinement et lutter contre la pandémie...

Nouvelles technos !

Encore mieux ! Certaines mairies recourent aux drones – équipés d'un haut-parleur pour interpellier les contrevenants – pour contrôler le respect des mesures de confinement coronavirus... Les Chinois l'ont fait. Nice, pareil. Ainsi, dans la Cité des anges, un drone volait en plein confinement pour diffuser de courts messages intimant aux Niçois de rester ou de rentrer chez eux. Nantes encore ! Ne croyons pas que Nice soit un exemple isolé. Nantes a, elle aussi, utilisé un drone pour surveiller un parc fermé aux promeneurs et joggeurs afin d'éviter la propagation du coronavirus.

DES DRONES À NANTES

Les robots volant utilisés à Nantes sont des drones Mavic 2 Enterprise du Chinois DJI. Il s'agit de drones polyvalents, pesant moins de un kilo, pouvant être équipés d'un petit haut-parleur capable de diffuser des messages avec une puissance sonore de 100 dB.



© DR

Pour certains, ces mesures sont exceptionnelles. Certes. Les technologies, quelles qu'elles soient, après un test pour la bonne cause, ont toujours eu tendance à s'incruster... Question d'habitude à prendre. ■

Agenda

Reportés

Security/Safety Prevention Meetings

Du 17 au 19 mars 2020 – Cannes

REPORTÉ DU 15 AU 17 SEPTEMBRE 2020 – CANNES

www.security-and-safety-meetings.com

Ifsec

Du 19 au 21 mai 2020 – Londres

REPORTÉ DU 8 AU 10 SEPTEMBRE 2020 – LONDRES

www.ifsec.events/international/

Préventica Nord

Du 26 au 28 mai 2020 – Douai

REPORTÉ UNE PREMIÈRE FOIS DU 30 JUIN AU 2 JUILLET 2020

<https://www.preventica.com>

Maintenus

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/

COVID-19

En Île-de-France, les drones et les caméras aident la police



Pour contraindre les Franciliens à respecter les règles du confinement, la préfecture de police de Paris a pu compter sur ses effectifs et sur les 1 400 caméras du réseau de surveillance. Grâce à celles-ci, la préfecture a pu piloter en temps réel les policiers présents sur le terrain et les envoyer sur les zones où certains citoyens se rassemblaient. En plus des moyens terrestres, la police pouvait également compter sur ses drones pour surveiller les zones exemptes de caméras. Par exemple, les bois de Vincennes ou de Boulogne. Grâce aux drones, les policiers pouvaient diffuser des messages afin de rappeler à l'ordre les personnes montrant des velléités de se rassembler. ■

SÉCURITÉ PRIVÉE

La fin des « vigiles »

Le GES souhaite qu'on n'emploie plus le terme de « vigile » pour parler des personnels sur le terrain. Et demande donc qu'on lui préfère désormais celui d'agent de sécurité qui correspond plus à la multiplicité des missions qu'ils remplissent, tout en étant moins connoté péjorativement parlant comme le rappelle, dans un communiqué de presse, le GES : « *Le terme "vigile" colporte, à l'inverse, une image de travail, sinon d'occupation, de peu de cas et de mauvaise réputation, alors même que nos concitoyens, désormais et depuis plusieurs années, reconnaissent totalement l'utilité des agents de sécurité privée.* » ■

CONTINUUM SÉCURITÉ

À lire

Début juillet, paraîtra aux éditions Hermann, le dernier livre de Guillaume Farde intitulé *Le Continuum de sécurité nationale*. Guillaume Farde, maître de conférences à Sciences Po, est un spécialiste des questions de sécurité. L'ouvrage est préfacé par Stéphane Volant, président du CDSE. ■



FRÉDÉRIC GAUTHEY,
président du **Groupe**ment des entreprises de sécurité

« *La sécurité privée existe en elle-même.* »



© DR

Pour PSM, le président du GES revient sur la crise du Covid-19 et ce qu'elle a révélé des relations entre les professionnels de la sécurité privée et ses autorités de tutelle. Entre autres...

La crise du Covid-19 et le confinement mis en place par l'État ont révélé, de l'avis unanime des organisations professionnelles représentant les acteurs quels qu'ils soient de la filière sécurité, une vraie défaillance de la part de vos autorités de tutelle. Comment l'expliquez-vous?

C'est vrai, c'est bien le sentiment que ressent le GES, avec de l'amertume, une certaine déception. Mais il faut aussi l'expliquer : peut-être n'avons-nous pas réussi, depuis des années et des années, à apparaître suffisamment sérieux collectivement. Au-delà des discours d'estrade, des gesticulations médiatiques ou des plaintes, au-delà des chiffres hasardeux, le professionnalisme de notre filière doit s'acquiescer par des propositions solides et étayées vis-à-vis des pouvoirs publics : c'est ce que nous faisons, au GES, et c'est ce qui va nous permettre, je l'espère, de sortir des jeux de rôle qui, par le passé, ont trop servi d'ersatz de relations constructives avec l'État. Tous les acteurs publics ne sont pas à mettre sur le même plan : le GES se félicite d'avoir été auditionné par la commission des lois

de l'Assemblée nationale, ce qui a permis de replacer les acteurs légitimes au centre du village.

Quels sont les principaux sujets, problèmes, pour lesquels vos interlocuteurs du Cnaps, du ministère... ont été défaillants ?

Il faut être précis en la matière, et d'abord prendre en compte le caractère inédit, global et multiforme de cette crise : d'abord sanitaire, puis économique, puis sociale, et peut-être même sociétale. Les diagnostics simples ne conduisent qu'à des solutions simples, et fausses.

Je souhaite d'abord mentionner ce qui a fonctionné : le report des autorisations du Cnaps et des SSIAP est arrivé rapidement. Il nous faudra une prolongation, peut-être jusqu'à la fin de l'année. Les attestations de déplacement professionnel ensuite : après un démarrage compliqué, ce problème est désormais derrière nous (nous aurions pu attendre légitimement des facilités plus importantes ; ce sujet sera à remettre sur la table). Autre point qu'il faut mentionner : le dispositif de chômage partiel, avec un départ difficile lié à son aspect massif et soudain. Mais, globalement, il fonctionne pour près de 20 % de nos salariés.

Ce qui n'a pas fonctionné : les EPI, et particulièrement les masques. Au-delà du problème global en matière d'approvisionnement et de la priorisation légitime pour les personnels de santé, nos agents auraient dû bénéficier d'approvisionnements spécifiques soutenus par les pouvoirs publics lorsqu'ils travaillent dans les lieux où d'autres salariés en bénéficient (hôpitaux, établissements de santé, Ehpad). Nous manquons également d'une analyse juridique rapide sur certains sujets émergents, comme les relevés de température. Ici, la multiplicité de prise de position des acteurs suivants, ministère de l'Intérieur, ministère du Travail, ministre de la Santé, Cnil, etc., empêche une interprétation qui colle à la réalité du terrain : qu'on nous dise si cela est possible ou pas ! Et qu'on nous dise, si ce n'est pas le cas, comment et si cela pourrait l'être ? Mais qu'on nous le dise ! Ces questions sont en attente de réponse par le GES, le premier à avoir soulevé le sujet, et désormais par le CDSE, le Medef, les donneurs d'ordre, les agents.

Malgré les discours faisant de la sécurité privée un acteur à part entière du continuum sécurité, il semble que, pour reprendre l'expression de Guillaume Farde, votre filière et ses salariés soient

« Notre ministère de référence ne nous a jamais supporté publiquement, malheureusement. »

encore perçus comme des « supplétifs » des forces régaliennes. Partagez-vous ce point de vue ?

La sécurité privée ne « supplée » pas les forces de l'ordre, mais répond à des clients. Nous n'avons pas les mêmes compétences et donc ne fonctionnons pas sur le principe de la subsidiarité ou de la suppléance. Une fois pour toutes, nous avons des contrats et des marchés. De ce que je sais, les forces de l'ordre ne nous payent pas et ne sont pas les donneurs d'ordres. Cette « suppléance » vient d'analyses anglo-saxonnes, désormais invalidées, déduisant la sécurité privée de la sécurité publique (le « junior partner »), ce qui arrange nos pouvoirs publics et nous maintient précisément dans une relation de tutelle anti-économique. Or, la sécurité privée existe en elle-même, certes reconnue, encadrée, réglementée, mais se déduisant d'un besoin client. Pour cela, avant le continuum de sécurité, nous assurons la continuité d'activité. Si cette crise permet de le faire comprendre, alors nous aurons fait un grand pas.

Certains de vos confrères évoquent une perte de confiance, une rupture dans les relations entre la filière et les pouvoirs publics. Est-ce vraiment le cas ? Si oui, pourquoi ?

La confiance ne peut fonctionner que dans les deux sens. Les pouvoirs publics ont-ils eux-mêmes confiance dans la sécurité privée ? Ses représentants ont-ils favorisé cette confiance ? Mais la perte de confiance actuelle ne doit pas exclure le dialogue, les échanges, les propositions, parce que nous avons des attentes. Celles-ci se matérialisent par des vecteurs dont nous n'avons pas les clés, à savoir la loi. Il ne s'agit pas de se mettre encore plus sous la tutelle de l'État – certains feignent de le croire –, mais d'obtenir nos propres outils de régulation et de transformation. Or, dans un état de droit et pour que tous les acteurs appliquent les mêmes principes, je suis désolé de vous dire qu'il faut une ● ● ●

BIO EXPRESS

Ingénieur des Ponts et Chaussées et titulaire d'un MBA de l'INSEAD.

Depuis 2017 Directeur général France de Prosegur. Auparavant, il occupait les fonctions de directeur général France chez DMG Mori, un des leaders mondiaux de machines-outils d'usinage.

Juin 2019 Président du GES (Groupement des entreprises de sécurité), né de la fusion du Snes et de l'USP. ■



FRÉDÉRIC GAUTHEY,
président du Groupement des entreprises de sécurité

« À défaut de continuum de sécurité, nous avons assuré la continuité d'activité. »



© DR

● ● ● loi, une réglementation. Le tout est qu'elle soit écrite dans le sens souhaité par les acteurs privés.

Il y a presque un an, naissait le GES. Quel bilan tirez-vous des travaux menés depuis cette naissance (avant la crise Covid-19)? Et qu'en reste-t-il aujourd'hui?

Nous sommes désormais installés, avec plusieurs accords signés avec les partenaires sociaux et un agenda social à entamer. Le point majeur, la révision de nos classifications, étape conditionnant la hausse globale des salaires de 10 % pour l'année 2022, entre en négociation fin mai. Nos échéances sont courtes : il nous faut aboutir pour mars 2021. Le GES s'en est donné la méthodologie, en recourant au cabinet « Solange Briet ». Un groupe de travail interne s'est réuni depuis plusieurs mois et nous atteignons là un degré de maturité et de volonté qui nous avait manqué les années précédentes. Nos propositions d'avant crise sont toujours valables, et même d'autant plus avec la crise. Nous avons particulièrement approfondi les modalités de la garantie financière ; la création d'un indice des coûts de revient est encore plus nécessaire qu'avant ; la définition d'un statut juridique des agents de sécurité est impérieuse. À défaut de continuum de sécurité, nous avons assuré la continuité d'activité, en accompagnant nos adhérents sur l'ensemble des dispositifs mis en place par l'État. Avec le GES, les lignes ont donc bougé, même si certains masques sur la volonté de transformer réellement la filière sont tombés.

Il semble que, pour certains, vos métiers soient invisibles ou encore perçus via l'image d'Épinal du « vigile » (terme que vous souhaitez d'ailleurs voir abandonné). Comment changer cette perception?

Nous voulons précisément voir disparaître le terme de vigile pour changer la percep-

tion de nos activités, de nos agents. Le métier d'agent de sécurité privée doit être reconnu, attractif, valorisé. Comme j'ai eu l'occasion de le dire récemment aux députés, c'est un agent de sécurité privée, par son action professionnelle, qui a empêché un carnage au Stade de France le 13 novembre 2015.

Si le terme n'avait pas été, des décennies durant, utilisé de manière péjorative, alors peut-être que « vigile », parce qu'il renvoie à la vigilance, serait acceptable. Il n'est pas acceptable que certains responsables publics emploient encore ce terme ; il n'est pas acceptable que les médias ravalent ce métier au rang des « gros bras ». J'ajoute enfin que notre ministère de référence ne nous a jamais supportés publiquement, malheureusement, comme d'autres ministères ont su le faire avec les professions qui dépendaient de leur champ de compétences.

Finalement, le continuum sera-t-il un jour une réalité?

Je vais le redire : si le continuum de sécurité doit devenir une réalité, c'est à l'État, au ministère de l'Intérieur de nous dire comment ils le conçoivent. C'est l'État qui a besoin de nous. Pas l'inverse.

Les policiers, les gendarmes, les policiers municipaux attendent, sur le terrain, ce continuum, parfois le vivent déjà. Aux autorités centrales du ministère de comprendre pourquoi le continuum de sécurité du quotidien est perçu comme nécessaire par les policiers et les gendarmes. Nous, nous avons mobilisé nos 100 référents départementaux afin qu'ils prennent contact avec les préfets pour échanger sur la situation locale, sur les besoins locaux, sur des dispositifs gagnant-gagnant entre public et privé.

Il nous faudra aussi revenir sur le livre blanc de la sécurité intérieure : il lui manquait une dimension « gestion de crise », que nous allons donc remettre au-devant. Si le continuum doit être une réalité, c'est bien dans la gestion de crise. Enfin, nous proposerons de faire un Retex conjoint avec le ministère de l'Intérieur, et peut-être d'autres administrations, sur la crise. Celle-ci a été une occasion ratée pour le continuum de sécurité. Espérons que le retour d'expérience ne le soit pas. ■

36.5° C



SOLUTIONS THERMIQUES DE DÉTECTION DE TEMPÉRATURE CORPORELLE

PLUS SÛR, PLUS RAPIDE, PLUS INTELLIGENT

- Des solutions Bullet, Turret et Portables conçues pour détecter des températures cutanées élevées pour un dépistage rapide avec une précision de $\pm 0,5^{\circ}\text{C}$
- Plage de mesure de température : $30-45^{\circ}\text{C}$



Sans contact



Détection multiple



Mesure en 1 sec



Algorithme AI

NE CHERCHEZ PLUS! TROUVEZ!



e-salon-protectionsecurite.fr

Visitez le 1^{er} 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.

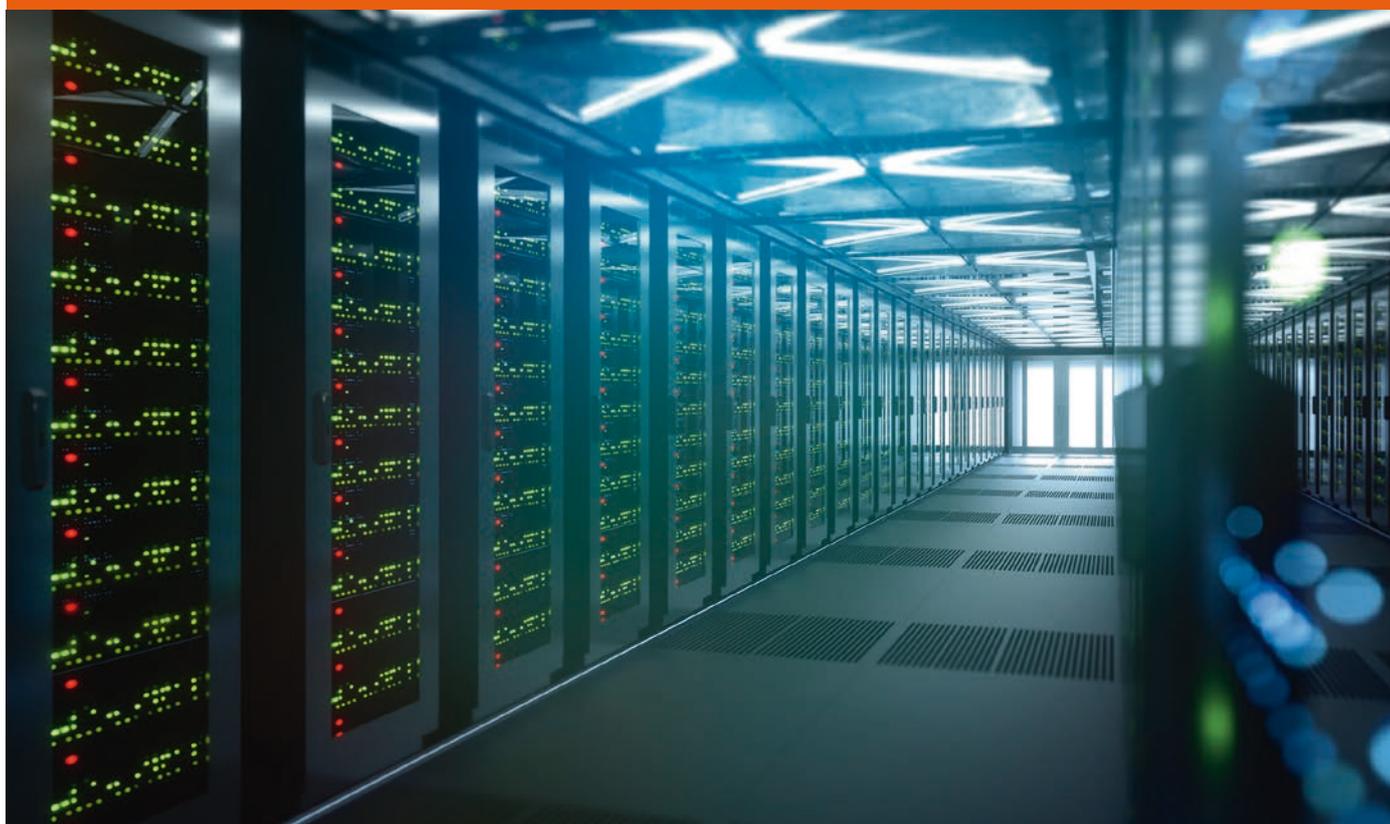
3

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

Cloud et sécurité

À l'occasion de la crise du Covid-19 et du confinement qu'ont dû gérer certaines entreprises, les directeurs sécurité-sûreté ont pu se rendre compte de l'intérêt de disposer d'un cloud. Ne serait-ce que pour organiser le télétravail, gérer leurs applications et autres systèmes de sécurité...



© Getty Images

SOMMAIRE

→ Le cloud, un auxiliaire des entreprises pour affronter les crises	32
→ Un réel engouement donc	33
→ La souveraineté : un vrai problème	34
→ Quelles données sur le cloud ?	35
→ Et la sécurité dans tout ça ?	36
→ Être exigeant et vigilant	37
→ Lutter contre la malveillance	38

Le cloud, un auxiliaire des entreprises pour affronter les crises

Longtemps, le cloud a inspiré de la méfiance au monde de la sûreté des entreprises ainsi qu'à leurs collègues de la sécurité informatique. C'est moins le cas aujourd'hui. Et le cloud devient un auxiliaire précieux des directions sûreté. Sous certaines conditions.



La sécurité du cloud ne constitue plus un frein à son utilisation comme c'était encore le cas il y a quelques années.



Après avoir fait preuve d'une réticence parfois justifiée – nous verrons pourquoi – de plus en plus d'entreprises se laissent séduire par le cloud, son caractère hyperfonctionnel et économique. «*Tout d'abord parce que, hormis leur activité liée à leur cœur de métier, les entreprises génèrent de plus en plus de données, de tout genre, qu'il est nécessaires de stocker*, explique Yves Pellemans, directeur technique d'Axians (certifié Iso 27000 et Anssi). Or, même si le stockage

en tant que tel coûte bien moins cher qu'il y a quelques années, nos clients cherchent avant tout des outils pour stocker facilement leurs données et mettre à jour leurs logiciels et leurs systèmes d'exploitation.» Ainsi, en plus des ses fonctions de sauvegarde, de mise en réseau et d'analyse de données, de mégadonnées ou de big data, d'accès à des applications bureautiques standards ou d'exécution de systèmes opérationnels plus complexes, s'ajoutent aujourd'hui la possibilité de gérer, grâce au cloud, les interactions entre les objets connectés grâce aux progrès de l'intelligence artificielle et une meilleure communication machine to machine (M2M). De nombreuses raisons donc de s'intéresser au cloud...

■ Un réel engouement donc

Selon une récente enquête, environ 70 % des entreprises utiliseraient le cloud (public, privée, mixte). D'ailleurs, à en croire le cabinet 451 Research, «*cette dépendance croissante envers des sources externes de services d'infrastructure, d'applications, de gestion et de sécurité a pour effet de diminuer les dépenses dans l'informatique traditionnel au profit d'investissements massifs dans cette technologie (hébergement et achats de services et de matériels confondus)*».

Pourquoi ce net regain d'intérêt ? La digitalisation des entreprises n'y est pas pour rien. S'y ajoutent, nous l'avons déjà souligné, la rationalisation des coûts en matière d'IT. Et la sécurité. Longtemps considérée comme un frein, la sécurité des données est désormais perçue comme un atout du cloud. La preuve : le cloud est de plus en plus utilisé par la



UNE LISTE DE PRESTATAIRES DE L'ANSSI

L'Anssi met à votre disposition sur son site une liste des prestataires d'informatique en nuage qualifiés.

→ www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/

banque et l'assurance. «*Aujourd'hui, les entreprises veulent non seulement stocker leurs données de manière sécurisée mais aussi trouver des solutions pour que ces données soient toujours disponibles. On n'a pu le constater pendant le confinement : sans le cloud, de nombreuses entreprises auraient été incapables de basculées en quelques jours, voire quelques heures, en mode "télétravail"*», explique Yann Fralo, Country Manager France chez A10 Network.

Stéphane de Saint Albin, président de Rhde & Schwarz Cybersecurity France et vice-président d'Hexatrust, ajoute : «*La sécurité du cloud ne constitue plus le frein à son utilisation comme elle pouvait encore l'être il y a quelques années. Aujourd'hui, on trouve sur le marché des solutions qui permettent de stocker et de gérer sur le cloud ses données, sans pour autant renoncer à y appliquer des mesures de sécurité strictes, et sa souveraineté sur ses propres données.*» ● ● ●

DU CÔTÉ DES FABRICANTS

STEVEN COMMANDER

Directeur de la prescription chez HID Global



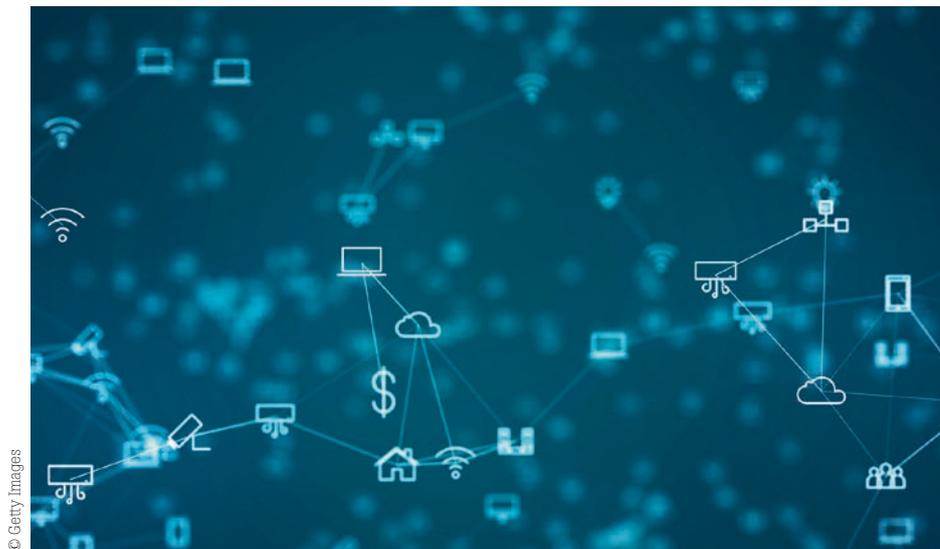
© DR

« LE CLOUD FAIT PARTIE DU QUOTIDIEN DE NOS MÉTIERS. »

«*Le cloud fait aujourd'hui partie du quotidien de nos métiers. Et il sera de plus en plus utilisé. Ne serait-ce qu'avec le recours de plus en plus important au badge dématérialisé sur un smartphone, par exemple. Les technologies du contrôle d'accès seront intégrées dans le smartphone ou directement dans les applications de l'entreprise grâce aux technologies dans le cloud comme le SDK ou l'API...*

Mais tout cela ne pourra se faire que si nous parvenons à rassurer nos clients. Non seulement en respectant certains règlements comme le RGDP, mais en nous appuyant aussi sur les bonnes pratiques.»

© Getty Images



© Getty Images

● ● ● ■ **La souveraineté : un vrai problème**

Stéphane de Saint Albin pointe un vrai problème du cloud : la souveraineté des

données. « On peut accepter le cloud sans pour autant abonner toute forme de souveraineté sur ses données et leur valeur stratégique, poursuit donc le

vice-président d'Hexatrust. *Mais il ne faut pas faire preuve de naïveté. Car les données qui sont stockées dans un cloud américain, par exemple, peuvent susciter l'intérêt... Il faut donc être très vigilant en matière de chiffrement, faire en sorte qu'il soit unique et en possession de personne d'autre que soi.* »

Or, rester souverain est possible. « Les données stockées sur le cloud peuvent être excessivement sensibles, critiques... Structurées ou non, explique Luc d'Urso, président directeur général d'Atempo. Nous devons absolument protéger ce patrimoine. L'alternative aux acteurs américains existe ; nous disposons d'hébergeurs et d'éditeurs souverains de grande qualité et ils ne sont pas assujettis au Patriot Act! Nous devons également nous protéger des lois d'extraterritorialité du droit américain. Nous avons perdu la guerre du hardware, mais nous disposons de tous les atouts pour remporter celles de l'hébergement et du traitement des données

3 QUESTIONS À

DENIS BRUNEL

Directeur sûreté de Capgemini



© DR

Il semble qu'à l'occasion de la crise du Covid-19 et de la mise en place du confinement, certaines entreprises découvrent l'intérêt du cloud. Est-ce votre cas ?

Le cloud est depuis longtemps un des outils dont Capgemini se sert dans le cadre de son activité. Et grâce à sa maîtrise, nous avons pu, dès l'annonce par le président de la République de l'entrée en vigueur du confinement, le 17 mars, mettre, très vite et avec beaucoup d'agilité, 99 % des 25000 collaborateurs travaillant sur les 64 sites du groupe en télétravail... Tout en gérant de manière centralisée nos solutions de contrôle d'accès, de vidéosurveillance, de lutte contre l'intrusion, notre télésurveillance, notre sécurité humaine... Si nous en sommes là, c'est que dès 2019, j'ai entamé une migration majeure de notre système de contrôle d'accès désormais déployé, aussi, dans Security Command Center (CCC).

Quel élément vous a incité à franchir le pas du cloud alors que certains de vos confrères font toujours preuve d'une certaine méfiance à son égard ?

Le cloud me permet de mieux gérer les procédures et de manière centralisée. Il me permet ainsi d'avoir un niveau de qualité homogène en matière de techniques, de respect des procédures, de résilience... Nous pouvons aussi, le cas échéant, basculer en mode supervision réseau pour voir l'état de notre système. Par contre, je ne suis pas prêt à tout virtualiser, à tout mettre sur le cloud. Car s'il est assez simple de sécuriser l'accès physique aux datacenters, d'assurer la sécurité des bâtiments grâce à de la vidéosurveillance, du contrôle d'accès, de l'anti-intrusion..., il faut garder à l'esprit qu'en matière de sécurité le maillon le plus faible est souvent l'humain. Il faut donc prévoir des procédures de sécurité, de contrôle... qui permettent de sécuriser

les données du serveur jusqu'au poste de l'opérateur et de détecter toute menace éventuelle, tout comportement déviant...

Quel bilan tirez-vous du recours au cloud pendant le confinement et comment envisagez-vous la reprise de l'activité au sein de Capgemini ?

Cette période aura évidemment fait apparaître des points d'amélioration. Et le bien-fondé de certaines approches comme la Track Force, une solution dématérialisée de suivi des incidents avec report des informations vers le responsable de site et le responsable sécurité. Nous avons aussi pu, grâce au cloud, gérer de manière très souple le paramétrage de systèmes de sécurité comme celui des alarmes, par exemple. Enfin, je pense que le cloud nous permettra de sortir de la crise aussi facilement que nous y sommes entrés et de reprendre, avec beaucoup de souplesse, notre activité.



professionnelles et de leur sécurité grâce à des logiciels français, souverains.»

■ Quelles données sur le cloud ?

«Toute entreprise génère de la donnée. Dans une usine, une machine, un testeur, un détecteur... produisent de la donnée. Ces dernières peuvent être mises à disposition des managers, des équipes techniques, des opérateurs... pour savoir comment a été produit tel ou tel bien, quel incident a pu survenir lors de la phase de production...», explique Laurent Laporte, président directeur général de Braincube. Il y a donc deux manières d'utiliser ces données: de manière continue afin d'aider à mieux piloter l'usine, ou en les stockant pour faire du big data, du machine-learning... L'intérêt du cloud est de permettre de stocker des données qui pourront être brassées et utilisées pour améliorer les processus de l'entreprise. Pour ●●●

PAROLE D'EXPERT

CHRISTOPHE ROSSI

Président directeur général de CNCR Group



© DR

« CONTRÔLER LE RESPECT DES PROCÉDURES DE SÉCURITÉ. »

« Le cloud modifie profondément les modes de production de l'IT. Il requiert un outil management de la End-User Experience.

Pour comprendre les usages, dimensionner le service et maîtriser le niveau de performance délivré. Pour contrôler la sécurité et la conformité des Workplaces. C'est ce que nous proposons

avec Interact. L'expérience de l'utilisateur est quantifiée et détaillée pour chaque application, chaque site, chaque type de configuration... de bout en bout. Pour la sécurité, certaines données sont focalisées sur le niveau de vulnérabilité du SI depuis les postes de travail : conformité logicielle, état de fonctionnement des dispositifs de protection, comportement à risque des utilisateurs, shadow IT, etc. Interact s'intègre dans l'écosystème en alimentant les outils dédiés à la sécurité du SI comme les SIEM (Security information and Event Management) et les SOC (Security Operation Center). Interact permet par exemple de détecter si l'antivirus est à jour, si le pare-feu est activé, si un PC a une session non verrouillée sans utilisateur actif, si un compte administrateur local du poste est non désactivé, si l'utilisateur a un comportement "à risques"... Tout cela, évidemment, dans le cadre du respect de la réglementation RGPD. »

FLIR K1

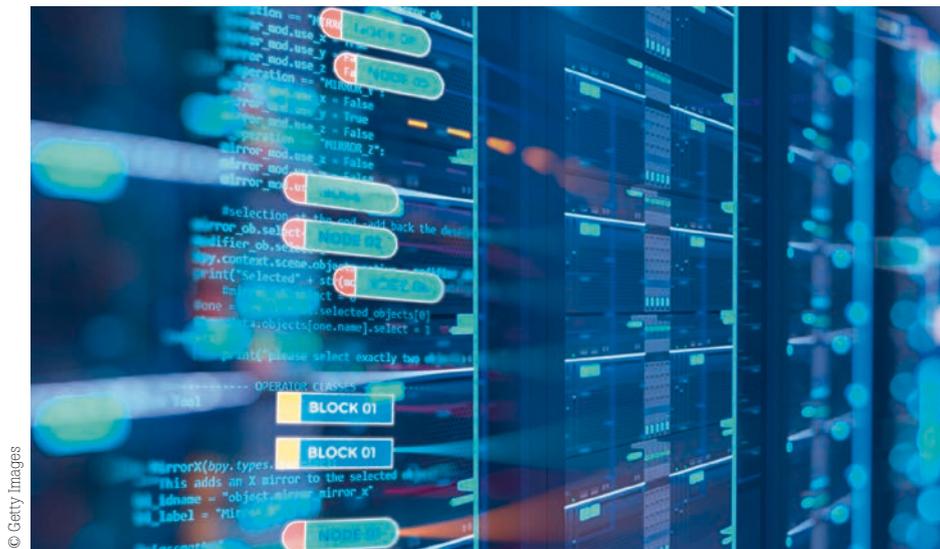
Caméra de perception des situations



GARDEZ L'ŒIL SUR L'INCENDIE

La FLIR K1 est une caméra thermique solide et compacte qui sert de paire d'yeux supplémentaire sur le lieu de l'incendie pour que les capitaines, officiers et inspecteurs puissent profiter rapidement d'une évaluation à 360° dans l'obscurité totale et dans la fumée. Avec sa lampe puissante intégrée, la FLIR K1 éclaire la scène pour aider l'utilisateur à diriger et gérer l'équipe plus efficacement. Elle génère également des images thermiques 160 x 120 pixels qui permettent à l'utilisateur de mieux apprécier la situation, ce qui ne serait pas possible à l'œil nu.

www.flir.fr/products/k1



© Getty Images

● ● ● leur assurer la sécurité de leurs données, nos deux datacenters sont installés en France, à Lyon et à Paris, et nous sommes certifiés ISO 27000 et nous plions aux recommandations de l'Anssi.» Peut-on tout confier au cloud? Pour Stéphane de Saint Albin, «il faut évidemment se poser la question des données qu'on souhaite stocker dans le cloud. Certaines sont plus critiques que d'autres et peuvent revêtir un caractère vital pour l'entreprise.» «Le volume de données va croître au rythme de 60 % annuel sur les cinq prochaines années. Il s'agit d'un gisement énorme qu'il faut absolument sécuriser car il constitue une source extraordinaire de création de valeur pour l'Europe. Nous devons également proposer des solutions souveraines pour corréler ces données pour en tirer la quintessence, insiste Luc d'Urso. Le cloud hybride va donc naturellement s'imposer en distinguant les données chaudes qu'on utilise au quotidien, qui resteront stockées sur site, au plus proche de la puissance de calcul, et les données froides à archiver ou à utiliser ponctuellement. Il faut arbitrer entre les données critiques, vitales, et celles qui le sont moins...»

■ Et la sécurité dans tout ça?

La sécurité ne serait donc plus un frein à l'utilisation du cloud? «Nous nous heurtons moins à des refus définitifs. Et lorsqu'on prend le temps d'expliquer les choses, de faire de la pédagogie, les directeurs sûreté, les DSI... comprennent que ce n'est pas parce qu'on est dans le cloud que tout est moins

sécurisé, insiste David Brillant, Director Sales Engineering South EMEA chez Forcepoint. Par exemple, Forcepoint a reçu le "visa sécurité de l'Anssi". Par ailleurs, je pense qu'il y aura un avant et un après Covid-19. À cette occasion, les DSI se sont rendus compte que le cloud facilitait grandement la continuité de l'activité de l'entreprise. Ne serait-ce que pour le télétravail. Sans nuire à sa sécurité de l'entreprise.»

Il ne faut pas se laisser aveugler par le caractère «nuageux» du cloud. Cela reste du stockage comme un autre. Physique et quelque part. «Avant d'entrer dans le débat sur le stockage en local ou

pas, rappelons qu'il ne faut plus raisonner en termes de sécurité physique. Elle est importante certes mais ce n'est plus, selon moi, le cœur du débat, explique Cédric Cailleaux, responsable technique cybersécurité & RSSI chez Axians. En effet, il est désormais possible de connaître la qualité et la fiabilité des capacités d'hébergement d'un datacenter. Facilement reconnaissable au travers de leur qualification en quatre niveaux : allant de tiers 1 à tiers 4. Ce dernier étant le niveau le plus élevé puisqu'il assure que les données ne seront pas indisponibles plus de 20 minutes par an. Le tiers 4 est assez rare mais pour la majorité des besoins exprimés par les entreprises, on peut tout à fait se satisfaire d'un datacenter tiers 3+, par exemple.»

Yann Fralo ajoute : «Il n'y a aucune raison de faire moins en matière de sécurité sur le cloud que ce qu'on fait localement, sur ses propres réseaux et moyens de stockage. On peut tout à fait demander à son fournisseurs cloud de respecter un cahier des charges précis, ne pas hésiter à l'auditer pour s'assurer des standards sécurité qu'il applique.» Point de vue que partage Philippe Rondel, Senior Security Architect chez Check Point Software : «Il nous faut accompagner les utilisateurs dans la création de leur environnement et outil cloud. Les aider à sécuriser leurs réseaux et à analyser leur environnement, les informations et l'accès à l'ensemble. Checkpoint nous faisons en sorte de leur fournir les outils qui leur

PAROLE D'EXPERT

GABRIEL GEDDA

Président du chapitre France d'Asis International et EMEA Sub-Regional Physical Security Manager France-Benelux chez AP Global Physical Security



© DR

« LE CLOUD PARTICIPE À LA CONTINUITÉ DE L'ACTIVITÉ. »

«Le Covid-19 et le confinement vont aider certains directeurs sûreté et DSI à prendre conscience de l'intérêt du cloud en cas de crise.

Ne serait-ce que pour permettre la continuité de l'activité via le télétravail, par exemple. Le cloud est un disque dur externe à l'entreprise dont l'un des buts, grâce à la digitalisation, est de

basculer, en cas de crise, dans un mode de fonctionnement qui lui permettra de maintenir son activité dans les meilleures conditions. Le cloud permet au directeur sûreté de gérer à distance, et de fermer par exemple, les différentes sites de son entreprise, en supprimant, de manière très souple, simple, rapide, les droits d'accès aux divers sites ou en limitant le nombre aux équipes nécessaires au bon fonctionnement de l'activité tout en ayant une vue holistique de son activité grâce au Dashboard dynamique.»



DU CÔTÉ DES FABRICANTS

VINCENT DUPART

Président directeur général de STid



© DR

« LE CLOUD EST UNE VRAIE TENDANCE DANS LE CONTRÔLE D'ACCÈS. »

« Le cloud est très utile dans les métiers de la sécurité électronique et est devenu une vraie tendance dans le monde du contrôle d'accès. Il permet de gérer de manière dynamique les droits. Le gestionnaire des droits peut ainsi accéder, de partout dans le monde, à une plateforme qui lui permet de gérer et d'accorder des droits à des utilisateurs, à des visiteurs. Chez STid, nous proposons des accès sécurisés par mots de passe forts, un hébergement sécurisé certifié pour les industries les plus exigeantes et un système de confidentialité de bout en bout conforme Cnil et RGPD pour protéger les données sensibles. S'y ajoute du chiffrement des BDD SQL avec possibilité de délégation d'administration sans accès au contenu/dissociation des droits d'accès et journalisation avec gestion des historiques. En ce qui concerne le stockage physique des données, nous proposons une redondance totale avec deux datacenters. Et pour les politiques de sécurité les plus exigeantes, nous proposons des solutions 100 % offline avec l'outil SECard qui permet de programmer vos badges et smartphone en local. »

permettent de "surveiller" leurs réseaux, leur cloud... afin de vérifier que leur fonctionnement et leur utilisation sont conformes aux règles de sécurité de l'entreprise et d'identifier, très vite, en temps réel, les failles sécurité ou les possibles actes malveillants.»

■ Être exigeant et vigilant

Le cloud a souvent suscité une certaine forme de psychose. Et pas toujours à tort. Tout le monde se rappelle du Patriot Act de 2001, du Privacy Shield de 2016 et plus près de nous du RGPD ou du cloud Act... Les Américains se sont do-

tés de moyens de contrôles des données. Et l'extraterritorialité du droit nord-américain peut être un danger lorsque des données sont stockées dans le cloud de Microsoft, Amazon et Apple... « Il existe une vraie problématique sur la confidentialité des données ●●●

Dallmeier

AIRPORT | CASINO | INDUSTRY | LOGISTICS | CITY | STADIUM

VIDEO INFORMATION TECHNOLOGY for the 21st Century

- Haut niveau de rentabilité grâce à la technologie caméra „Panomera®“, unique en son genre, et à une planification en 3D
- Analyse vidéo basée sur l'IA grâce à la qualité image définissable (DIN EN 62676-4)
- Principe de fonctionnement et design récompensés par le prix iF DESIGN AWARD 2020

Learn more: dallmeier.com

DIN EN 62676-4 250 px/M 125 px/M 62,5 px/M

iF DESIGN AWARD 2020

2 QUESTIONS À

STÉPHANE LEMÉE

RSSI et directeur de la sûreté chez Fujitsu France



Quel est l'intérêt du cloud dans le cadre de vos fonctions ?

Pourquoi l'utilisez-vous ?

Les solutions de sûreté telles que la vidéoprotection ou le contrôle d'accès sont

désormais proposées dans le cloud et offrent de déporter l'infrastructure de traitement et de stockage des données pour ne conserver sur site que les caméras, lecteurs de badges et autres dispositifs contribuant à la sécurité des installations. Au-delà du gain financier et d'offrir l'agilité recherchée lors de déploiements (nouveau site, changement de technologie), le recours au cloud permet de simplifier la continuité de l'activité

de l'entreprise et surtout sa reprise après sinistre. L'adoption du cloud permet enfin d'adresser les nouveaux usages comme le travail à distance, voire aux domiciles des intervenants, avec le recours massif au télétravail, y compris pour des profils jusqu'à présent exclus de ces solutions de repli.

Quels sont les freins au recours au cloud ?

En assurer la sécurité est, sans surprise, l'un des plus grands défis à relever pour l'adoption du cloud en France pour des raisons évidentes liées à la conformité (RGPD) et à la confidentialité de données du patrimoine informationnel de l'entreprise.

Ce défi est amplifié par la carence en compétences constatée par près de deux tiers des entreprises au sein des équipes internes (DSI) qu'il faut alors compenser par un accompagnement externe. Si l'adoption du cloud permet de contribuer très fortement à sécuriser des installations de sûreté en permettant, par exemple, un déploiement très régulier des correctifs de sécurité, il convient de s'assurer d'une visibilité sur les informations échangées (DLP, CASB), de renforcer la gestion des identités comme du poste de travail, et d'adapter nos capacités de prévention et de détection (veille, SOC).

● ● ● *liées aux cloud public américains, tient à souligner Cédric Cailleaux. Il faudra donc être vigilant. En outre, il existe de nombreux moyens de s'assurer de la bonne gouvernance, du sérieux des hébergeurs, fournisseurs... : la famille ISO 27000, l'ISO 20000 et ISO 27701..., le respect des règles de l'Anssi et sa liste "SecNumCloud", les préconisations de la Cloud Security Alliance ainsi que l'agrément HDS qui concerne l'hébergement des données de santé... En suite, il faut inventorier ses actifs et savoir précisément où se situe la valeur de l'entreprise...»*

Une fois cela fait, vous pourrez définir des mesures de sécurité physique et logique pour protéger vos données, en transit ou en repos, contrôler les accès à votre réseau et gérer les identités. Puis prendre des mesures opérationnelles vous permettant de surveiller l'utilisation des données, par qui, comment...

■ Lutter contre la malveillance

Une fois vos données sur le cloud, vous pouvez vous doter des moyens de les surveiller, ainsi que le fonctionnement de votre réseau. « Il existe des outils qui permettent d'analyser le contenu de

toutes les données de l'entreprise, stockées sur le cloud ou en transit, afin de détecter tout comportement déviant, tout acte de malveillance, explique David Brillant. On pourra surveiller ce que fait l'utilisateur, ce qu'il télécharge, les documents qu'il consulte, les comportements inhabituels, les matériels qu'on connecte sur le réseau et s'ils sont autorisés ou fournis par l'entreprise, si cer-

tains consultent, sans en avoir le droit, des données confidentielles... »

Cela permettra de signaler très vite au directeur sûreté et au DSI, les comportements suspects, les possibles menaces... afin qu'ils puissent prendre les mesures nécessaires pour préserver le patrimoine matériel et immatériel de leur entreprise. ■

SUR LE TERRAIN

JÉRÔME COMIN

Expert de Resadia du groupe Scopelec usages et services



« ÊTRE TRÈS EXIGEANT EN MATIÈRE DE SÉCURITÉ. »

« Resadia est un réseau regroupant 29 PME locales spécialisées dans l'intégration de services pour l'infogérance IT, les solutions Lan, la sécurité et la sûreté. Les entreprises s'intéressent de plus en plus aux potentialités du cloud en matière de sécurité.

Mais il nous faut faire encore preuve de pédagogie. Le cloud a en effet des avantages. Il permet par exemple de mutualiser les expertises et de réduire les coûts. Mais il faut se poser la question des données qu'on y stocke et sur quel type de cloud : public, privé, mixte... À mon sens, le cloud public proposé par les Gafam pose des problèmes en matière d'extraterritorialité. Par ailleurs, les datacenters ne sont pas toujours en France... Il faut donc être très vigilant quant au choix de son prestataire et de ce qu'on attend de lui en matière de sécurité physique et logique. »



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.

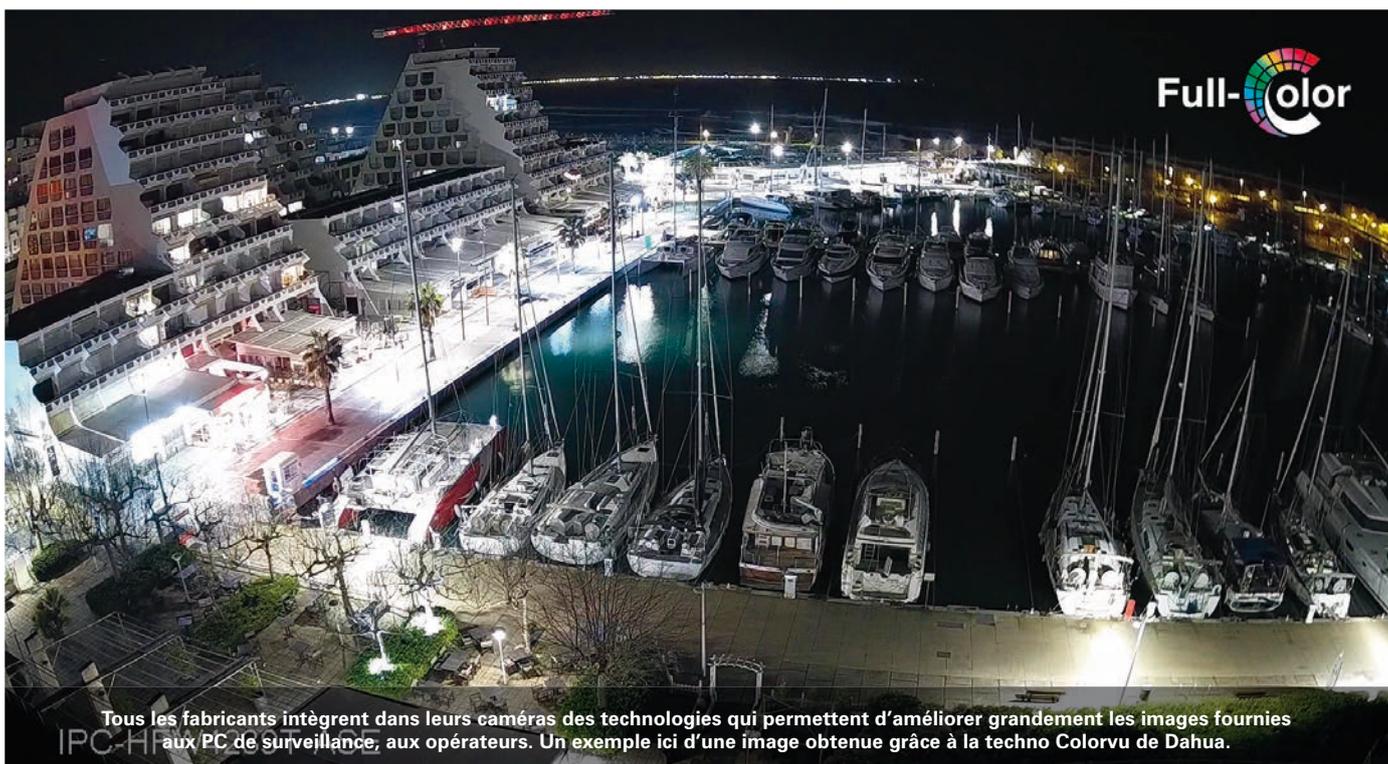


IPS Outdoor Detection permet une protection périmétrique très fiable même dans le brouillard, par fortes pluies et chutes de neige.



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





Tous les fabricants intègrent dans leurs caméras des technologies qui permettent d'améliorer grandement les images fournies aux PC de surveillance, aux opérateurs. Un exemple ici d'une image obtenue grâce à la techno ColorVu de Dahua.

© Dahua

Voir dans le noir ? Oui, mais pour faire quoi ?

Voir la nuit est une contrainte incontournable de la vidéosurveillance. La plupart des fabricants proposent aujourd'hui des solutions qui permettent de « voir » dans des conditions de très faible luminosité. À condition de se poser les bonnes questions.

Pour voir la nuit, vous pouvez opter pour différents types de caméras : jour/nuit, IR ou thermiques. À cela s'ajoutent des technologies qui permettent de voir dans le noir comme les intensificateurs de lumière qui amplifient les sources de faible lumière comme la lune ou les étoiles. Les solutions thermiques, quant à elles, sont sensibles à certaines longueurs d'ondes et traduisent la température détectée, pour faire simple, en niveaux de gris visibles à l'écran. Enfin, l'infrarouge (IR) permet d'éclairer un lieu de rayons invisibles à l'œil nu et ainsi d'obtenir une image parfaite dans le noir total. « Une fois cela dit, et avant de choisir une caméra pour filmer et voir la nuit, il faut d'abord se demander ce qu'on veut faire avec. De la simple détection d'intrusion avec une levée de doute ou de l'identification ? Car cela va évidemment influencer le choix, insiste Nicolas Hess, Key Account Manager chez Hikvision France. D'une manière générale, on a besoin de voir dans le noir pour

CÔTÉ SOLUTIONS

Jusqu'à 0,0005 lux

Les caméras réseau DarkFighterX d'Hikvision utilise des capteurs 1/1,8 de pouce pour augmenter la résolution à 4 mégapixels. Cette image apporte deux fois plus d'informations que les modèles à 2 mégapixels. La caméra peut aussi fournir des images en couleurs à des niveaux de luminosité allant jusqu'à 0,0005 Lux. Cela signifie également qu'à l'avenir, la reconnaissance faciale pourrait être possible, même dans le cas d'un faible éclairage, grâce à la puissance de l'imagerie et à une résolution supérieure à la HD.



© DR

LE POINT DE VUE D'UN FABRICANT

NICOLAS HESS

Key Account Manager chez Hikvision France



© DR

« AVOIR DES CAMÉRAS QUI SACHENT GÉRER LES SUREXPOSITIONS. »

« Pour assurer aux utilisateurs qu'ils verront les détails et les couleurs, nous avons développé et intégré plusieurs technologies dans nos caméras : ColorVu, Darkfighter et Darkfighter X. Elles permettent toutes de rester en couleurs, dans des conditions de luminosité très basses 0,0014 lux pour ColorVu, 0,002 lux pour Darkfighter et 0,0005 lux pour Darkfighter X. Cette dernière étant très utile dans le cadre de la vision urbaine car l'opérateur a, la nuit, presque l'impression d'être en plein jour... »

Dans le cas où l'on tomberait à des niveaux inférieurs à 0,0005 lux, il faudra disposer de caméras capables de basculer en noir et blanc, et dotées de leds IR pour éclairer la scène. Il faut savoir que cela peut perturber la vision si l'éclairage IR n'est pas correctement géré par la caméra. Il faut ainsi disposer de caméras qui sachent gérer les possibles surexpositions, avec des leds focalisées sur la bonne partie de l'image à filmer et avec un éclairage uniforme pour éviter une image présentant un motif circulaire de luminosité au centre de l'image. Les insectes peuvent également obstruer la vision car ils sont attirés par la chaleur des leds lorsque celles-ci chauffent trop. C'est pourquoi nous intégrons dans nos caméras notre technologie EXIR. Il s'agit d'un dispositif IR rendant l'éclairage plus efficace et uniforme, et consommant très peu d'énergie. »

détecter une personne à coup sûr, ou presque. Cela pourra se faire grâce à des solutions thermiques qui permettent de réduire au maximum le nombre des fausses alarmes, afin d'envoyer la bonne information à l'exploitant du site, à l'opérateur... En revanche, il faut souligner le fait que les solutions thermiques ne peuvent pas être utilisées pour identifier des personnes. Pour voir et identifier un intrus, on pourra utiliser des caméras dotées de technologies haute sensibilité qui permettent de rester en couleurs le plus longtemps possible afin de fournir le maximum de détails et qui ne basculent en noir et blanc avec un éclairage IR complémentaire que dans l'obscurité totale. »

■ Des technologies de plus en plus efficaces

Tous les fabricants de caméras vous proposent des caméras avec des capteurs aux capacités toujours accrues. Ce que confirme Didier Duhaubois, support technique et avant-ventes chez Dahua Technology France : « Dahua, ● ● ●

La caméra thermique DH-TPC-BF2221-T de Dahua Technologies est adaptée à la plupart des utilisations de vision de nuit en extérieur.



© Dahua Technology

LE POINT DE VUE D'UN FABRICANT

CÉDRIC GONZALEZ

Responsable des ventes chez Provision ISR



© DR

« NOUS ALLONS LANCER NOTRE GAMME SIRIUS ANALOGIQUE ET IP. »

« Nous allons sortir une gamme, la Sirius, de caméras très basse luminosité IP et analogique qui permet de fournir des images en couleurs, même dans des environnements très dégradés en matière de source de lumière. D'une manière générale, on a le choix, lorsqu'on est confronté à de la basse luminosité, entre le thermique et des caméras classiques. Le problème est que le thermique permet uniquement de faire de la détection. Il sera inopérant pour de l'identification, en milieu urbain, par exemple. »

NE PRÉFÉREZ VOUS PAS VOIR LA NUIT EN COULEUR ?

SIRIUS
FULL COLORS NIGHT CAMERAS

Une excellente luminosité et des images chromatiques éclatantes : telles sont les principales forces de nos toutes nouvelles caméras SIRIUS.

L'ouverture extra large F1.0 de l'objectif permet à plus de lumière d'entrer et deux LEDs intelligentes visibles fournissent à la caméra l'éclairage minimal requis de 0,0001Lux.

Conçues pour améliorer les capacités de surveillance dans l'obscurité, les caméras SIRIUS fournissent des images couleur époustouflantes de jour comme de nuit.

www.provision-isr.com - follow us f y in

● ● ● *comme tous ses confrères, travaille pour concevoir et intégrer dans ses caméras des capteurs de plus en plus sensibles afin qu'ils fonctionnent et qu'ils fournissent des images dans des conditions de très faible luminosité. Dans cette logique, nous avons développé notre solution Starlight+ qui marche dans des conditions de luminosité de 0,001 lux. Ainsi, avec très peu de lumière, Starlight+ permet de restituer une image en couleurs. Ce qui est très utile, par exemple, pour les applications urbaines.* » Même volonté de proposer des solutions pour des conditions de mauvaise luminosité chez Axis: « *La lumière est composée de photons, mais elle possède les propriétés d'une onde électromagnétique dont la longueur d'onde, comprise entre 400 et 780 nm, correspond à la zone de sensibilité de l'œil humain. Le proche infrarouge allant jusqu'à 950 nm. Un capteur de caméra optique dit jour/nuit est sensible de 400 à 950 nm en libérant le filtre IR, explique Philippe Bénard, Business Development Manager A&E. Afin de déterminer le résultat final de l'image, il faut avant tout déterminer le niveau de luminosité de la scène. Celle-ci va influencer le choix des technologies mises en œuvre. En effet, une caméra pouvant rencontrer potentiellement les trois situations dans la même nuit, il faudra donc être très attentif à ses caractéristiques.* » Avant d'ajouter: « *La pleine lune par nuit claire correspond à 0,25 lux. Un ciel couvert sans lune à 0,0001 lux et un parking souterrain à 0 lux. Il existe trois modes de fonctionnement la nuit en fonction du niveau de luminosité. Ainsi, pour 0,25 lux, Axis propose ses caméras basse luminosité Lightfinder qui fournissent une image en couleurs qui basculera en noir et blanc pour des basses luminosités de l'ordre de*

3 QUESTIONS À

FRANCK CARETTE

Product Manager Thermal Products Europe chez Hikvision



Quelles sont les technologies qui permettent de voir et de filmer la nuit ou dans des conditions de très faible luminosité ?

Il y a trois types de solutions techniques pour voir la nuit pour faire simple. Et qui sont toutes au catalogue d'Hikvision. Les caméras classiques, avec une bonne ouverture, qui sont capables de fournir des images couleur de bonne qualité, les caméras à projection de lumière infrarouge, dites «infrarouge» et les solutions thermiques. Le thermique permet d'obtenir exactement la même image la nuit que le jour, quelle que soit la luminosité. Pour résumer, les solutions thermiques sont les seules qui permettent de voir, avec un système passif, quels que soient l'environnement physique de la caméra et le moment de la journée. L'IR peut être efficace car il permet d'illuminer la scène, mais il faut rappeler que l'environnement peut perturber la diffusion de cette lumière particulière et donc le rendu d'image. De plus, le thermique ne permettant pas de reconnaître un individu, il est possible de l'installer en toutes circonstances.

On entend souvent dire que les solutions thermiques sont trop chères par rapport à l'infrarouge ou aux solutions intégrant une caméra «classique» associée à une source lumineuse...

À mon sens, cet argument économique n'a plus lieu d'être. En premier lieu, il faut rappeler que le thermique consomme moins d'énergie que l'IR, environ 5 watts. Deuxièmement, il ne faut pas oublier que l'IR a aussi un coût puisqu'il faut ajouter à la caméra un éclairage IR. Troisièmement, je tiens à souligner que nous proposons aujourd'hui des caméras thermiques dont le prix en entrée de gamme se situe aux alentours de 600 euros, ce qui est sans commune mesure avec les prix qu'on rencontre chez certains fabricants de solutions pour très faible luminosité... Enfin, à partir d'une distance, au-delà des 150 mètres, le thermique est le seul moyen de détecter une intrusion.

Peut-on réellement identifier quelqu'un ou quelque chose la nuit avec une caméra de surveillance ?

Certainement sur de faibles distances, mais c'est à mon avis assez difficile, voire impossible sur de moyennes et longues distances. On est plus ici dans des applications de type détection d'intrusion et levée de doute que dans de l'identification proprement dite. Si on souhaite vraiment identifier loin, il vaut mieux opter pour un gros projecteur et une excellente caméra. Les caméras mobile PTZ disposent de ces prérequis, mais encore faut-il une solution de détection pour leur dire où regarder exactement, comme une caméra thermique par exemple.

PAROLE D'EXPERT

DIDIER DUHAUBOIS

Support technique et avant-ventes chez Dahua Technology France



« SAVOIR CE QU'ON VEUT VOIR ET FAIRE. »

« Avant de choisir sa caméra, il faut se demander pourquoi on veut voir dans le noir. Veut-on faire de la détection ou de l'identification ?

Dans ce dernier cas, il faudrait choisir une solution qui permet de fournir des images en couleurs ou en noir et blanc de bonne qualité. Nos solutions Full-Color répondent à ces besoins puisqu'elles sont conçues pour fournir constamment des images en couleurs, à partir du moment où il y a un minimum de luminosité. Si on a besoin de travailler dans des conditions de très basse luminosité, on pourra se doter d'une solution infrarouge. Enfin, pour la vision nocturne, sans source de lumière, et dans le cadre de la simple détection d'intrusion, la seule solution réellement efficace est la caméra thermique. »



La P1375-E de Axis avec sa technologie Lightfinder et son projecteur IR additionnel est un produit polyvalent qui peut être utilisé de jour comme de nuit dans toutes les situations.

© Axis Communications



Conçues pour améliorer les capacités de surveillance dans l'obscurité et pour fournir des images couleur étonnantes 24 h/24, les caméras HD Sirius s'appuient à la fois sur le capteur Starvis de Sony et sur des objectifs extrêmement avancés.

0,0001 lux. Enfin, 0 lux nécessitera l'utilisation de projecteurs IR afin d'éclairer la zone, l'image sera en noir et blanc dans la zone de portée du projecteur.»

■ La vision dans le noir pour tous ?

Même si les prix des caméras baissent, il ne faut pas espérer voir dans le noir à prix cassé. La vision nocturne ou dans des conditions de luminosité très dégradées a un coût. Malgré cela, la démocratisation des caméras permet aujourd'hui de s'équiper avec ces solutions haut de gamme pour des coûts bien inférieurs à ceux constatés sur le marché il y a quelques années. Désormais, les bonnes solutions de vision nocturne ne sont pas réservées qu'aux sites sensibles ou à gros budget. Si on conçoit bien sa vidéosurveillance et se pose les bonnes questions, il est tout à fait possible de s'équiper avec des caméras visibles ou thermiques pour quelques centaines d'euros... ■

LE POINT DE VUE D'UN FABRICANT

THIERRY ASSANT

Distribution Area Manager - Security chez Flir Systems



« NOTRE GAMME ELARA EST TRÈS EFFICACE. »

« Les caméras thermiques servent à voir dans le noir mais aussi le jour, et sont très efficaces pour détecter un intrus sur un site sensible grâce à de l'analyse vidéo. En revanche, leur efficacité peut être perturbée par un brouillard très dense qui l'empêchera de voir loin. Notre gamme de caméras thermiques de sécurité Elara FB-ID utilise des fonctions d'analyse embarquées pour classifier les intrusions humaines ou de véhicules, ce qui en fait l'idéal pour la détection des intrusions périmétriques et la surveillance des zones stériles. La FB-ID peut également communiquer les intrusions classifiées à des caméras PTZ Flir pour un suivi autonome des intrus. Elles assurent une détection fiable, avec un faible taux de fausses alertes dans les environnements très exigeants. »

EDEN INNOVATIONS

THERMAL SCAN

NOUS ÉVOLUONS POUR AMÉLIORER VOTRE SÉCURITÉ AVEC LE **CONTRÔLE D'ACCÈS SANITAIRE**

Association du **contrôle d'accès** avec la **détection de température**

Accès par **badge de proximité** ou **reconnaissance faciale**

Détection automatique du **port de masque**

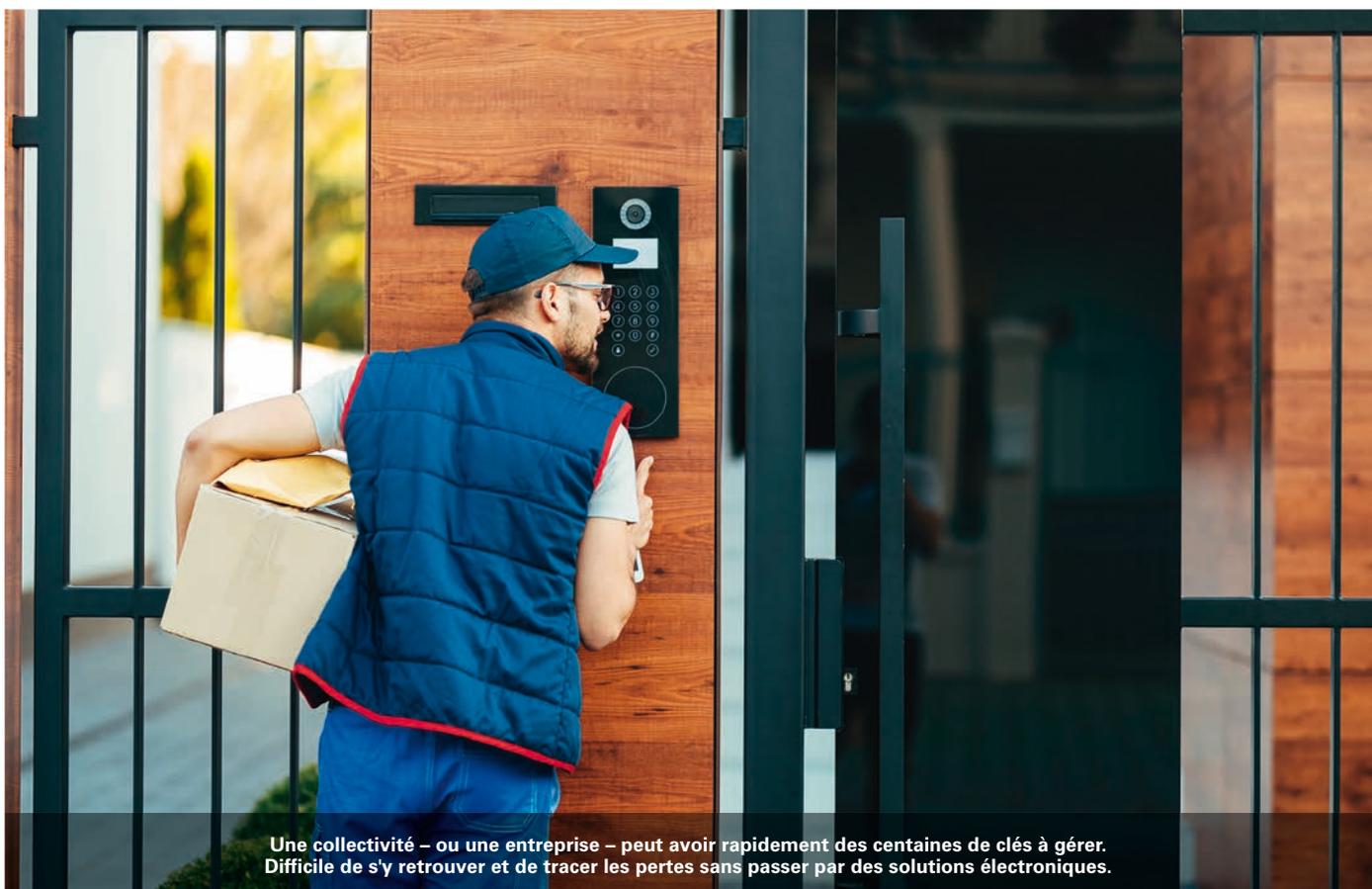
Alerte sur votre logiciel **OPTIMA**

www.eden-innovations.com

04 42 24 70 40

contact@eden-innovations.com / support@eden-innovations.com

contrôle d'accès



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.

© Getty Images

Interphonie avec ou sans fil ?

Dans l'industrie, le tertiaire ou le résidentiel, l'interphone est résolument connecté. Avec ou sans fil, il est bien plus qu'un simple outil de reconnaissance de visiteurs et d'ouverture de portes. Il devient une brique incontournable de l'écosystème de sûreté s'alliant au contrôle d'accès et à la vidéosurveillance. Et avec la portabilité des appels vers des outils mobiles, les fabricants l'assurent : plus aucune visite ne sera manquée !

Savoir qui se présente à la porte de l'immeuble ou de l'entreprise et accorder – ou non, l'accès, tous les interphones savent le faire et bien. La qualité du son et de l'image est au rendez-vous et l'offre des industriels est pléthorique. Poussée par la loi accessibilité, la visiophonie est désormais la règle dans l'habitat collectif et les établissements recevant du public.

■ Filaire, la fiabilité au service de la sûreté

De la simple fonction de filtrage, les interphones sont devenus de véritables outils de gestion de la sûreté. Ils allient lecteurs de

badge RFID, ou Vigik, mais peuvent aussi s'interfacer au système de contrôle d'accès et à la vidéosurveillance. Les caméras peuvent enregistrer les visiteurs et leur message, lesquels peuvent être consultés aussi bien depuis un poste de sécurité en entreprise que d'un smartphone. « Les entreprises, soulignent Teddy Daumur, responsable produit chez Castel, souhaitent que nous nous adossions à leur réseau informatique ou autre, car il est souvent plus fiable et protégé que les réseaux téléphoniques, mais ils demandent de plus en plus de passerelles vers des outils légers GSM ou G3/G4, Bluetooth, pour que les personnes puissent être accessibles même en mobilité. C'est ce que nous proposons avec nos solutions hybrides Xellip. » ● ● ●

3 QUESTIONS À

JEAN-LUC BOISNARD

Directeur des services informatiques Infra/télécom, métropole rennaise

Pourquoi avoir revu le système de contrôle d'accès des écoles rennaises ?

Cela entre dans le cadre de la mise en place des PPMS. Nous avons dû revoir la question de la fermeture et du contrôle d'accès des 157 groupes scolaires. Selon les écoles, il s'est agi de rehausser des clôtures, installer des portails et bien sûr un système d'interphonie avec système d'alerte compatible avec les PPMS.

Quel élément a déterminé votre choix ?

Le choix s'est fait dans le cadre d'un appel d'offre et s'est porté sur les interphones IP Xellip de Castel. À Rennes, nous avons

la particularité de bénéficier du réseau FOR (fibre optique rennais), un réseau public de fibres optiques qui alimente, entre autres, les services publics dont les écoles. Nous souhaitons donc que le système d'interphonie soit IP d'éthernet et qu'il puisse se greffer sans problème sur le réseau FOR. Autre point qui était important, la qualité de la transmission vocale et la facilité d'utilisation.

Quel retour avez-vous des utilisateurs ?

Comme toujours lorsqu'on modifie les systèmes, il y a eu des réticences de certains gardiens et directeurs d'école qui craignaient de devoir faire face

à des contraintes supplémentaires.

En revanche, une fois installé, le système est très apprécié car simple et confortable. Facile à paramétrer, le fait de pouvoir contrôler l'identité du visiteur et d'ouvrir sans avoir à se déplacer, depuis son portable a facilité son acceptation. De plus, nous avons pu faire des scénarios d'ouvertures et de confinement individualisés par école, en fonction de la configuration et des activités qui s'y déroulent (temps scolaire, hors temps scolaire, personnel présent, etc.). Une souplesse très appréciable.

SOLUTIONS PRODUIT

2N IP Verso se décline en Bluetooth

Le 2N® IP Verso est un interphone IP entièrement modulaire. Au-delà de ses fonctionnalités d'interphonie, il assure également un contrôle d'accès fiable dans le bâtiment et il s'interface facilement avec d'autres solutions tierces pour garantir une sécurité optimale. Cet interphone permet l'ouverture par code ou badge et sa caméra HD avec vision nocturne peut être diffusée sur un système VMS comme Milestone ou Genetec. De plus, l'interphone IP permet d'appeler des smartphones et d'ouvrir la porte aux visiteurs à distance. Disponible aussi en noir, il peut intégrer de nombreux modules comme par exemple : lecteur RFID, lecteur Bluetooth, écran tactile avec liste à défilement de contact, lecteur biométrie, etc. Il convient aussi bien à des villas, des immeubles d'habitation ou de bureaux.



© DR

SOLUTIONS PRODUIT

Extel Connect, un visiophone écoresponsable dédié à la maison connectée

Extel Connect est un visiophone au design élégant qui allie confort et sécurité et permet de gérer les accès à distance. Composé d'un écran en couleurs sept pouces, il est équipé de touches tactiles. Relié par deux fils à sa platine de rue, l'interphone vidéo tactile permet une double commande de serrure électrique et de portail ainsi qu'une vision nocturne. La platine de rue et la visière anti-pluie sont en aluminium haute qualité avec un bouton éclairé. Le fabricant a conçu un produit basse consommation de 0,23 watt en veille, soit vingt fois moins qu'un téléphone portable en charge ! L'application Mobile Extel Connect permet une gestion à distance des accès depuis le smartphone. L'utilisateur peut ainsi piloter son appareil à distance pour contrôler les accès de jour comme de nuit, visualiser le flux vidéo de la platine, accueillir et discuter en direct avec un visiteur et enregistrer des photos ou des vidéos sur une mémoire interne.



© DR

LA PAROLE À

CÉDRIC MAZET

Responsable marketing Intratone



© DR

« LA RESPONSABILITÉ ENVIRONNEMENTALE CONCERNE AUSSI LE SECTEUR DE L'INTERPHONIE. »

« Selon l'Ademe, le secteur du bâtiment est globalement le plus grand producteur de déchets professionnels. Il est impensable aujourd'hui de ne pas se poser la question de la réduction des déchets, y compris dans la niche que représente l'interphonie. Depuis longtemps, Intratone s'est engagé dans l'interphonie sans fil. Cette technologie est par certains aspects intéressante sur le plan de la responsabilité environnementale et sociale. Présents sur le marché depuis plus de dix ans, nos produits ont déjà fait leurs preuves tant sur le plan économique que technique,

mais aujourd'hui s'accordent avec une vision d'écologie et de consommation raisonnée. Le principe qui est le nôtre de l'interphonie sans fil déportée sur les téléphones et équipements existants des résidents, évite l'équipement de chaque logement de combinés et de câbles de cuivre. Des matériaux qui peuvent être considérés comme de la surconsommation – puisque non indispensables. Nous avons estimé à 575 tonnes les déchets non générés par Intratone depuis 2008, en équipant plus 1 150 000 logements en solutions sans fil ni combinés spécifiques. Et nous avons décidé d'aller plus loin. »



■ Le sans fil mise sur l'écologie

Et si on se passait de câble et de combinés ? Pour Intratone, spécialisée dans l'interphonie de l'habitat collectif, les solutions sans fil ne présentent que des avantages. « Pour l'installateur, une simple platine de rue avec une carte SIM à placer en quelques heures, assure Cédric Mazet, responsable marketing d'Intratone. Pas de saignée à faire pour relier les appartements, ni de combinés de réception à installer. Les appels arrivent directement sur les téléphones fixes ou mobiles des résidents. Un gain de temps énorme pour l'installateur qui, une fois la platine de rue installée, n'a plus qu'à indiquer au gestionnaire comment entrer et modifier les numéros d'appel. Dans le cadre de la rénovation, c'est aussi une sécurité pour l'installateur qui n'est plus confronté au risque amiante. Enfin, et c'est non négligeable, l'aspect développement durable : ni câble de cuivre ni moniteurs installés : ce sont aussi des déchets qui ne seront pas produits. Un mieux pour la planète. » La

question des zones blanches est balayée : « L'habitat collectif est le plus souvent urbain et très rarement en zone blanche : entre les différents réseaux GSM, 3G/4G, il y a toujours une solution », affirme-t-il.

■ La portabilité pour répondre toujours présent

« Ne manquer aucun appel sans pour autant être bloqué à un poste, c'est vraiment une demande de l'ensemble de nos clients dans le tertiaire ou l'industrie, indique Teddy Daumur, Castel. Le déportement des appels vers d'autres postes ou sur un outil mobile est une fonction désormais incontournable. Y compris sur des systèmes filaires, nous implémentons des passerelles qui permettent de transmettre les appels vers différents types de terminaux, même sur les smartphones, ce qui permet de visualiser le visiteur, mais aussi pour ce dernier de laisser des messages. » Une portabilité qui s'apprécie également dans le

SOLUTIONS PRODUIT

AXIS A8207-VE MkII, le portier vidéo multifonctions

AXIS A8207-VE MkII Network est un portier vidéo qui réunit la surveillance vidéo, la communication bidirectionnelle et la possibilité d'intégrer le contrôle d'accès en un seul dispositif. Ses interfaces ouvertes offrent d'innombrables possibilités d'intégration et peuvent donc être facilement associées à d'autres systèmes de sécurité pour répondre à des besoins spécifiques. AXIS A8207-VE MkII est idéal pour une installation à des entrées fréquentées régulièrement par de nombreux visiteurs connus ou inconnus. Pour une communication bidirectionnelle limpide, il offre une suppression de l'écho, une réduction du bruit et une boucle à induction magnétique pour les aides auditives. Il permet de recevoir des appels vidéo des visiteurs et de contrôler l'accès à distance via un ordinateur, un téléphone fixe ou un dispositif mobile. Il dispose d'un lecteur de contrôle d'accès intégré (RFID) pour une intégration aisée avec le système de contrôle d'accès. Il comprend également un capteur PIR multifonctionnel, permettant par exemple de détecter des personnes en approche, puis de déclencher des événements comme un enregistrement ou une salutation verbale.



© DR

résidentiel, notamment avec le développement des locations entre particuliers : la possibilité d'ouvrir sa porte après avoir vérifié l'identité du visiteur aussi bien depuis son jardin que depuis l'autre bout du monde.

■ La gestion facilitée

« Bien sûr, avoir l'appel directement sur son smartphone est une innovation intéressante et sécurisante pour les résidents, mais qui n'est rien par rapport à de nombreux services complémentaires que peut apporter la vidéophonie IP aux syndicats ou aux bailleurs sociaux, remarque Cédric Mazet, responsable marketing d'Intratone. En quelques clics, le gestionnaire de résidence peut changer un code, créer un badge, changer un nom sur la platine, alimenter un tableau d'affichage dans les halls, mais aussi laisser des messages personnalisés aux résidents. »

■ Les lois accessibilité et PPMS dopent le marché

Si le marché est dynamique, c'est notamment par la mise en application de la loi d'accessibilité. La prise en compte des différents handicaps s'illustre parfaitement au niveau des interphones. De nombreux établissements recevant du public révisent leurs installations, pour être en conformité avec la loi. L'arrêté du 8 décembre 2014 fixe en effet un certain nombre de dispositions ● ● ●

2 QUESTIONS À

TEDDY DAUMUR

Responsable produit, Castel



Comment voyez-vous évoluer la demande dans le secteur tertiaire et dans l'industrie ?

La demande diffère du secteur résidentiel. Beaucoup d'entreprises ou de collectivités disposent déjà de réseaux filaires consacrés à la sûreté,

à l'informatique, au wi-fi ou à de la fibre optique et souhaite l'interconnectivité avec leurs réseaux en place. Dans le secteur professionnel, l'interphone n'est plus un simple outil de communication d'un point A à un point B, mais doit être considéré comme une « brique » de l'écosystème de sûreté plus global incluant le contrôle d'accès et la vidéosurveillance. L'intégration de l'interphonie aux outils de supervision et de supervision est désormais cruciale.

Proposez-vous des solutions sans fil ?

La demande aujourd'hui dans le secteur professionnel est claire : il ne faut pas perdre d'appels et la portabilité de l'appel est vitale. C'est pourquoi, nous développons des solutions IP hybrides qui associent filaire et non filaire. Nous nous appuyons sur les réseaux existants de l'entreprise, et proposons des solutions de déportement sur les réseaux GSM ou 3G/4G. La personne pourra toujours recevoir l'appel sur son smartphone ou sur un autre moniteur, une fonctionnalité qui peut être paramétrée avec notre plateforme SIP Castel.

SOLUTIONS PRODUIT

Full IP/SIP Xellip, sobre et esthétique pour les environnements exigeants



Les derniers nés de la Full IP/SIP Xellip mise sur la qualité vidéo, (définition HD et grand angle) et audio (puissance 10 W). Robuste (IK 09 et IP66), les interphones sont interopérables avec le protocole SIP, les codecs audio les plus répandus, ONVIF et les SNMP V2/V3, RTSP. Full iIP/SIP natif, un seul câble réseau (RJ45) suffit pour gérer l'audio, la vidéo, les datas, l'alimentation (PoE/PoE+). Conforme à la réglementation PMR. Avec lecteur de contrôle d'accès, plusieurs technologies disponibles et notamment Bluetooth.



Contrôle d'accès - Supervision - Intrusion - Vidéosurveillance

- ARD Certifié ISO 9001 -

ARD confirme son engagement à offrir à ses clients et partenaires des solutions adaptées, innovantes, sécurisées, au meilleur coût et respectueuses de l'environnement.

ISO 9001:2015

BUREAU VERITAS
Certification



Une société membre du groupe Vita protect

contrôle d'accès

SOLUTIONS PRODUIT

Osmoz, de Myd'l, une solution simple pour l'accessibilité

La borne Osmoz est une solution de signalétique pensée afin de répondre à la réglementation accessibilité en vigueur tout en offrant une esthétique favorisant son intégration dans le cadre du bâti. Conçu comme un signe de reconnaissance valorisant, simple et discret, elle permet de signaler sa présence et de solliciter une aide. Sans fil, la borne Osmoz est simple d'installation et présente une portée de 50 mètres en champ libre. Jusqu'à trois émetteurs peuvent être connectés au récepteur. Ce kit convient parfaitement à toutes les petites entreprises et tous les commerces recevant du public qui veulent s'équiper sans entreprendre de travaux. Fabriqué en France.



© DR

SOLUTIONS PRODUIT

Interphone sans fil Intratone à boutons affichage digital

L'interphone à boutons Intratone combine le meilleur de la gestion sans fil avec le confort de l'interphone à boutons : Mise à jour en temps réel, programmation de plages horaires, configuration d'accès limités dans le temps, installation simple et rapide. Pas d'installation de combinés : les appels visiteurs sont directement réceptionnés sur le portable ou le téléphone fixe du résident. Avec l'appli Intratone, le résident peut aussi voir le visiteur et consulter des messages en absence. Facile à programmer pour le gestionnaire : pas besoin de se déplacer. Celui-ci peut aussi laisser des messages directement auprès des résidents. L'interphone à boutons digitaux est disponible jusqu'à 56 noms. Compatible Vigik avec détection de badges copiés.



© DR

● ● ● relatives aux accès des établissements recevant du public et notamment du contrôle d'accès. Celui-ci doit permettre « à des personnes sourdes ou malentendantes ou à des personnes muettes de signaler leur présence au personnel et d'être informées de la prise en compte de leur appel. En particulier, en l'absence d'une vision directe de ces accès par le personnel, les appareils d'interphonie sont munis d'un système permettant au personnel de l'établissement de visualiser le vi-

siteur (vidéo). Les appareils d'interphonie doivent comporter une boucle d'induction magnétique, un retour visuel des informations principales fournies oralement. De même, avec la mise en place des PPMS (plan particulier de mise en sécurité) de nombreux établissements mettent à niveau leur interphonie afin d'être compatibles avec les processus de confinement ou d'évacuation et d'alerte. » ■

SOLUTIONS PRODUIT

DECT 603 sans fil d'AES, jusqu'à 350 m de portée en champ libre

Le fabricant britannique AES utilise pour ses interphones sans fil la technologie radio DECT connue pour sa fiabilité. Le modèle DECT 603 a une portée allant jusqu'à 350 mètres en « champ libre » ou 200 mètres à travers les murs de brique ou de béton. Une attention toute particulière a été apportée à la qualité de la transmission vocale. Le système accepte jusqu'à quatre combinés. Une fonction messagerie vocale intégrée permet d'enregistrer les appels manqués à la porte. L'interphone intègre également un lecteur de badge.



© DR



Arrêtez-les dans leur élan.

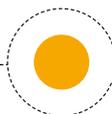
Utilisez le haut-parleur réseau à corne AXIS C1310-E pour avertir les intrus ou fournir des instructions grâce à des messages audio en direct ou préenregistrés. Intelligent et facile à intégrer, l'AXIS C1310-E est le moyen idéal de tirer le meilleur parti de votre système de sécurité. Robuste, il s'intègre parfaitement dans un environnement extérieur.

Pour plus d'info : www.axis.com/fr-fr/products/audio

AXIS[®]
COMMUNICATIONS

Détection intrusion

Infrarouges actifs ou passifs, détection vidéo ou pas, extérieur, intérieur, plug and play, cyberprotégés... Quelques solutions de détection et de lutte contre l'intrusion.



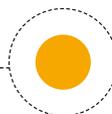
DÉTECTEURS KX – PYRONIX LIMITED

SOLUTION COMPLÈTE

Les technologies brevetées des détecteurs pour installations résidentielles, commerciales et industrielles légères, qui comprennent des modèles PIR (infrarouges passifs), Dual Technology (DT) et antimasquage DT (DT-AM) de Pyronix, propriété d'Hikvision depuis 2016, assurent une excellente protection contre l'intrusion. Détection jusqu'à 30 m, détection volumétrique et en rideau, insensibilité aux animaux jusqu'à 25 kg, sensibilité automatique : n'importe quelle combinaison de détecteurs KX couvre salons, cuisines, couloirs, chambres à coucher, ateliers, garages... un KX parfait est disponible pour n'importe quelle application. Filaire ou sans fil, chaque KX est fourni avec le même boîtier robuste. Grâce à la technologie sans fil bidirectionnelle de Pyronix, l'installation est un jeu d'enfant. Des fonctionnalités telles que l'apprentissage semi-automatique et les indicateurs de puissance de signal permettent à l'installateur d'optimiser celui-ci et de le mémoriser dans le système KX sans devoir se reporter au tableau de commande. ●



© Pyronix



LASER REDSCAN – OPTEX

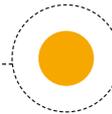
TAILLE, POSITION, VITESSE

Le RLS-2020I, de la gamme Redscan, utilise une nouvelle génération de laser qui permet de couvrir une surface de détection de 20 m x 20 m à 95°, pour identifier un individu ou un objet. En mesurant le temps de retour (Time of Flight) du rayon laser jusqu'au capteur, le RLS-2020I peut analyser la taille, la position et la vitesse de l'objet détecté.

Il est possible de paramétrer le système pour qu'il ne détecte que des objets d'une taille déterminée ou à partir d'une certaine distance. Ne consommant que peu d'énergie, le RLS-2021 jouit d'un design compact et discret qui lui permet de s'installer au plafond ou sur un mur, tout en se fondant dans le décor. Il est possible de choisir sa couleur. ●



© Optex



DÉTECTEURS S312 ET IS312B – HONEYWELL

HAUTES PERFORMANCES

Les détecteurs S312 et IS312B font partie des gammes IS3000 et DT8000 de détecteurs filaires d'Honeywell. Le portefeuille comporte désormais neuf détecteurs de mouvement haute performance qui répondent aux exigences de pratiquement toutes les installations, des applications résidentielles les plus simples à celles commerciales les plus complexes. Ils sont dotés d'optiques à miroir sur certains modèles, pour une détection plus précise, des capacités anti-masquage renforcées, une meilleure immunité aux animaux domestiques, une meilleure performance par hautes températures et bien d'autres aspects encore. Par ailleurs, leur fonction plug & play permet aux installateurs de gagner du temps. Qu'il s'agisse de la période de chauffe inférieure à une minute ou de fonctionnalités qui réduisent le temps passé en haut d'une échelle et rendent le montage facile. ●

→ CARACTÉRISTIQUES :

- Optiques à miroir avancées.
- Détection en présence de hautes températures.
- Immunité aux animaux domestiques.
- Fonction anti-masque.
- Immunité supérieure à la lumière blanche.
- Boîtier à ouverture sans outil spécial, etc.



© Honeywell



B ET G SERIES – BOSCH SECURITY SYSTEMS

JUSQU'À 599 ZONES

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 8 à 96 et de 16 à 599 zones. Elles gèrent de 4 à 32 portes en accès et 4, 8 et 16 caméras IP Bosch. 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. Une gamme complète de claviers permet de répondre aux différentes demandes allant du clavier à touche, au clavier LCD avec touches de pré-sélection et en passant par le clavier tactile ludique et intuitif avec lecteur de badge intégré.

Du contrôle de portes incluant des lecteurs classiques intérieurs et extérieurs et anti-vandales en liaison Wiegand 26 bits utilisant la technologie EM (Electro Marin) ou la double technologie Mifaire et EM. Le clavier tactile B942 intègre la technologie EM. Equipé de base d'une prise Ethernet et d'une prise USB permettant la mise à jour, la maintenance et le paramétrage à distance, les transmissions au centre de télésurveillance un utilisant le réseau IP avec le protocole Contact ID, Connetix IP. Les centrales de la gamme prennent en charge le protocole IPV6 pour la gestion des caméras. ●



GX REMOTE – HONEYWELL CONTROL

POUR LA GESTION DES ALARMES

L'appli mobile GX Remote Control d'Honeywell est conçue pour offrir aux utilisateurs une manière plus facile et intuitive d'accéder, gérer et commander à distance leurs systèmes d'alarme anti-intrusion Galaxy Flex et Galaxy Dimension depuis n'importe où dans le monde. L'appli permet aux propriétaires d'entreprises ou de logements de demander un rapport d'état instantané, de mettre en/ou hors service l'alarme et d'examiner l'historique des événements.

Pour télécharger l'appli : recherchez GX Remote Control soit sur Google Play ou sur Apple, dans l'App store ; cliquez sur l'icône de l'appli et téléchargez-la sur votre mobile ; scanner le QR code sur votre terminal mobile pour être redirigé sur l'App store. ●

➔ CARACTÉRISTIQUES :

- Facile et simple à utiliser : login sécurisé en 10 secondes, accès à l'historique des événements en un clic ;
- Facile à prendre en main et à utiliser via l'interface intuitive et guide utilisateur intégré ;
- Pratique pour gérer jusqu'à cinq sites depuis un seul terminal mobile et personnaliser des groupes.

NEO – FRANCOFA-EURODIS

CERTIFIÉE CYBER

Neo est une centrale vraiment conçue pour résister aux menaces cyber. En effet, le CNPP vient d'attribuer le premier certificat NF&A2P intégrant la dimension cyber à la centrale Neo, du Canadien DSC dont le distributeur exclusif pour la France est Francofa-Eurodis.

Cette certification prouve le haut niveau de protection du produit contre les attaques numériques :

- Sécurisation des transmissions IP et 3G (alarmes, applications, télémaintenance).
- Sécurisation de la centrale et du système contre le hacking (désarmement, programmation, données, composants).

Outre cela, la centrale Neo intègre des technologies de pointe :

- Solution IP, GSM et 3G.
- Solution mixte filaire/radio.
- Haute qualité de la radio Power G.
- Vérification audio et vidéo des alarmes.
- Suite logicielle complète.
- Compatible avec les protocoles de domotique Legrand et Control4. ●





Le radar d'Hikvision utilise une technologie qui lui permet de localiser avec précision la position et la trajectoire des déplacements de 32 intrus potentiels par radar, même dans les conditions météorologiques les plus difficiles.

© Hikvision

Grâce aux radars, suivez à la trace les intrus

Sont-ils l'arme fatale en matière de lutte contre l'intrusion ? Peut-être. En tout cas, les caractéristiques des radars en font un outil très efficace pour détecter les intrus, les localiser précisément et les traquer.

« **C**ontrairement à un détecteur intrusion infrarouge ou hyperfréquence qui donne juste une information de présence d'un intrus, le radar sera capable de vous indiquer, grâce à des coordonnées x et y , la position de l'intrus dans la zone de détection, et d'y associer des moyens de tracking, de zoning, comme des caméras... », explique Julian Martin, directeur commercial chez Optex Security.

Philippe Bénard, Business Development Manager A&E chez Axis Communications, ajoute : « En matière de lutte contre l'intrusion, on protège deux zones : le périmètre et l'intérieur de ce périmètre. La protection du périmètre se fait souvent avec des caméras thermiques avec détection sur zones linéaires. À l'intérieur du périmètre, on pourra aussi recourir à des moyens thermiques, mais leur rendu est assez pauvre. Le radar trouve ici toute sa pertinence. Il permet, grâce à sa technologie Doppler, par exemple, de protéger de grandes surfaces et de lo-

caliser de manière très précise un intrus. »

On l'aura compris, l'intérêt du radar réside dans le fait qu'il permet, associé à des caméras par exemple, de s'assurer un suivi de l'intrus de manière précise. Ce que ne peuvent pas encore faire certaines caméras. D'ailleurs, les fabricants de caméras, pour pallier certaines de leurs carences, proposent de plus en plus des radars pour venir compléter leurs offres...

■ Des contraintes

Pour être efficaces, les radars doivent être déployés en tenant compte de certaines contraintes. « La première de ces contraintes est la fréquence, souligne Julian Martin. Une fréquence trop basse aura un impact sur la sensibilité du radar au brouillard. Il faut privilégier les fréquences assez élevées comme le 24 GHz que nous utilisons pour nos radars. »

À cette première contrainte, s'ajoute le problème des ondes. On n'utilise pas les ondes comme on le souhaite. Et il faut veiller à ce que les ondes du radar ne soient pas perturbées par celles

CÔTÉ SOLUTIONS

Radar réseau Axis

Conçu pour compléter les systèmes de vidéosurveillance, les détecteurs Axis D2050-VE utilisent les technologies radar les plus avancées et des algorithmes intelligents pour détecter les intrus qui pourraient avoir franchi la première ligne de défense pour pénétrer dans les locaux d'un site. Axis D2050-VE détecte les mouvements 24 heures sur 24 même par temps de brouillard ou de pluie. Il est insensible aux éléments qui provoquent souvent des fausses alarmes, comme les ombres ou les faisceaux lumineux, les animaux de petite taille ou les insectes. Doté d'une couverture de détection horizontale de 120 degrés et d'une portée de 50 mètres, ce radar peut par ailleurs résister à des températures extérieures allant de -40 °C à +60 °C.



d'autres équipements ou ne les perturbent pas elles-mêmes. « Il faut aussi prendre en considération les contraintes liées à l'installation des radars, poursuit l'expert d'Optex Security. Le radar a été conçu pour travailler sur un champ de détection donné, large. Il faut donc l'utiliser dans des zones très larges. Dans un espace confiné, le radar pourrait s'éblouir lui-même. En outre, les ondes émises par le radar seront amenées, par exemple, à rebondir sur un mur, ce qui nuirait à la précision de la localisation de la détection. »

■ De réels atouts

« Les radars sont peu onéreux, ne requièrent pas de maintenance puisqu'ils ne contiennent pas de pièces en mouvement, explique Philippe Bénard. Ils sont capables de classifier de manière précise les objets. Ils sont insensibles aux variations de luminosité, aux conditions climatiques... On peut aussi créer des zones de détection et d'exclusion. Ils sont parfaitement adaptées aux contraintes de la lutte contre l'intrusion. » Pour Laurent Scetbon, responsable grands comptes et projets chez ● ● ●

CÔTÉ SOLUTIONS

Le radar anti-drones d'Optex

Le 3D500 SpotterRF offre une couverture radar en trois dimensions. Alors que le radar 2D normal fournit la distance et l'azimut, le radar 3D fournit en plus l'information d'élévation. Le 3D-500 est le premier radar 3D qui crée une zone de détection à dôme complet de 0 à 90 degrés à la verticale et 360 degrés à l'horizontale avec un seul équipement. Le radar 3D-500 mesure la latitude, la longitude et l'altitude de toutes les cibles aériennes dans un dôme d'un hémisphère d'un kilomètre de large, même directement au-dessus du radar sur 500 m sans aucun angle mort. Les applications incluent la détection de drones, la surveillance des oiseaux, la défense et la surveillance intrusion. Le dernier d'une gamme de radars 3D (radars anti-drones) de SpotterRF est le révolutionnaire 3D-500. Insensible à l'éclairage ou à la pollution sonore, le 3D-500 est le meilleur capteur de détection de drone du marché.



An advertisement for the PSM e-newsletter, displayed on a tablet. The background is red with white text. The main headline reads: 'POUR SUIVRE L'ACTUALITÉ DE VOTRE PROFESSION ET RESTER INFORMÉ, RECEVEZ GRATUITEMENT LA E-NEWSLETTER BIMENSUELLE DE PSM'. Below this, a list of topics is shown: 'Nouveaux marchés', 'Actu business', 'Infos people', 'Nouveaux produits', 'Agenda', and '...'. A yellow speech bubble contains the text: 'Pour recevoir tous les 15 jours la e-newsletter de PSM, inscrivez-vous d'un simple clic sur protectionsecurite-magazine.fr'. A hand is shown holding the tablet, which displays the PSM e-newsletter interface. The interface includes the PSM logo, the text 'e-NEWSLETTER', 'PROTECTION SÉCURITÉ MAGAZINE', 'Les solutions pour les professionnels de la Sécurité - Sécurité', 'LETTRE BIMENSUELLE - N°115 - 30/11/2017', 'pour vous Vincent LEVER', and a section titled 'actus' with the sub-heading 'Marché mondial de la sécurité' and 'Accélération des dépenses'. A small image of a person is visible in the bottom right corner of the newsletter preview.

intrusion

CÔTÉ SOLUTIONS

Un radar anti-drones chez Flir Systems

Le Flir Ranger R8SS-3D portable dispose d'une couverture verticale, d'une vitesse de détection minimale et des algorithmes nécessaires pour détecter et suivre jusqu'à 500 drones en simultané, tout en écartant les détections d'oiseaux. Le R8SS-3D peut surveiller la zone de couverture quatre fois par seconde, 24 heures/24 et 7 jours/7, pour détecter toutes les menaces terrestres et aériennes sous pratiquement n'importe quel climat, de jour comme de nuit. Compact et léger, il tient dans un sac à dos, consomme seulement 135 W et coûte beaucoup moins cher que ses équivalents de la taille d'un véhicule. Le R8SS-3D réduit les fausses alarmes déclenchées par les oiseaux et informe l'utilisateur si la cible est une personne, un véhicule, un système aérien sans pilote ou un objet non identifié.



© Flir Systems

● ● ● Hikvision: « Les radars sont parfaits pour la surveillance de grands espaces exposés dans des conditions climatiques difficiles et lorsque le périmètre est trop complexe pour déployer uniquement des caméras de vidéosurveillance (sauf les thermiques pour les grandes distances et les champs étroits). Grâce à leur fiabilité sous toutes les conditions météorologiques, leur grand angle de détection et leurs capacités de détection d'intrusion, ils permettent de sécuriser des sites complexes et sensibles. » ■

PAROLE D'EXPERT

LAURENT SCETBON

Responsable grands comptes et projets
chez Hikvision France



« L'INTÉRÊT : AIDER AU TRACKING DE L'INTRUS. »

« La gamme de radars Hikvision se compose de deux modèles : le PR 60 et le PR 120. Le PR 60 est capable d'assurer une détection jusqu'à 60 m sur 100°, tandis que le PR 120 le fait sur 120 m sur 120°.

L'atout du PR 120 réside dans le fait qu'on peut associer quatre radars, en faisant se chevaucher leurs cônes de détection, afin d'assurer une protection sur 360° sans angle mort. L'intérêt des radars est leur aptitude à traquer l'intrus, à le localiser précisément dans leur zone de détection. Les caméras traditionnelles ou les détecteurs de mouvement comme l'infrarouge actif et la détection de mouvement vidéo ont des limites pour déterminer l'emplacement exact d'un intrus potentiel lié à leur zone de détection. Par ailleurs, ils détectent plus rapidement que les caméras les cibles qui viennent vers eux. Enfin, nos radars utilisent une technologie de formation de faisceaux numérique et des algorithmes d'analyse intelligents pour détecter avec précision tous les mouvements de la cible dans toutes les conditions météorologiques, en minimisant les fausses alarmes. »

2 QUESTIONS À JULIAN MARTIN

Directeur commercial chez Optex Security



Le radar a-t-il encore une utilité à une époque où les caméras, de plus en plus intelligentes, puissantes... semblent répondre à tous les besoins ?

Il est évident que les caméras sont de plus en plus polyvalentes.

Mais elles ne peuvent pas encore tout faire. Ainsi, les caméras thermiques ont du mal à assurer leurs missions dans certaines situations. Par exemple, en cas de pluies violentes ou de brouillard très dense. Dans ces cas, la caméra thermique aura du mal à voir loin. Son champ de vision sera réduit. Les radars permettent d'assurer aux responsables des sites, aux agents de sécurité... que la détection sera faite et qu'ils pourront « voir » l'intrus, le localiser de manière précise.

Pouvez-vous nous présenter quelques-uns de vos radars ?

Les radars de la gamme CK fonctionnent dans la bande des 24 GHz (Conforme norme CE et RED) et par tout temps (pluie, brouillard, neige). Le faible encombrement de ces radars, la faible consommation d'énergie et le temps d'installation rapide les rendent également très adaptés aux sites éloignés et aux installations temporaires. Lors de la détection d'une cible, le radar CK peut piloter à distance une caméra PTZ pour pivoter ou pointer vers la cible tout en alertant l'opérateur. Le radar CK suit ensuite la cible jusqu'à ce que l'opérateur prenne le contrôle de la caméra ou jusqu'à ce que la menace soit passée, enregistrant ainsi l'intrusion pour une analyse ultérieure. La large gamme des radars CK permet de répondre à toutes les problématiques de détection intrusion périmétrique sur de vastes zones (portée jusqu'à 250 m piéton et 400 m véhicules).

LE POINT DE VUE D'UN FABRICANT

PHILIPPE BÉNARD

Business Development Manager A&E
chez Axis Communications



« SUIVRE LE DÉPLACEMENT D'UN INTRUS SUR UNE CARTE. »

« Nous avons lancé
récemment une nouvelle

gamme de radars qui peuvent, pour une zone de 180°, détecter des personnes jusqu'à 60 m et jusqu'à 85 m pour des véhicules. On peut très bien intégrer un radar dans un VMS afin que la localisation de l'intrus et ses déplacements apparaissent sur une carte du site, type Google Earth. On peut aussi envoyer les coordonnées de la détection à une caméra PTZ dont la mission sera d'assurer le suivi, le tracking de l'intrus, du véhicule... »



Les radars CK d'Optex répondent aux problématiques de détection sur les sites militaires, les aéroports, les fermes marines, les sites industriels, les prisons, etc.

© Optex

OFFRE PACK psm

PROTECTION SÉCURITÉ MAGAZINE

- Le magazine PSM
- La e-newsletter tous les 15 jours
- Les archives en libre accès sur Internet
- Le Hors-Série Sécurité Privée
- Le Guide d'Achat
- L'Annuaire de la Sécurité Sureté
- ...



BULLETIN D'ABONNEMENT À RETOURNER À

PSM / TBS Blue - 6, rue d'Ouessant - 35760 St Grégoire. Tél : 01 76 41 05 88. Fax : 01 48 00 05 03. abopsm@tpmedia.fr

Oui, je souhaite m'abonner à PSM pour 1 an (6 numéros) : **103 € TTC au lieu de 168 €**

Je règle : chèque > à l'ordre de PSM à réception de la facture

Mes coordonnées :

NOM _____
PRÉNOM _____
SOCIÉTÉ _____
E-MAIL _____

ADRESSE _____
CODE POSTAL _____
VILLE _____

J'économise + de 65 €, soit + de 45 % de réduction !

Le tarif indiqué est valable jusqu'au 31/12/2020 (TVA : 2.10%) en France seulement. Pour l'étranger, nous consulter.

Conformément à la loi « Informatiques et libertés », vous disposez d'un droit d'accès et de rectification aux informations vous concernant auprès de l'éditeur.

TP Média : SARL au capital de 20.000 € - 488 819 137 RCS PARIS



Faire effectuer la maintenance en temps et en heure relève de la responsabilité du chef d'établissement.

© Getty Images

Maintenance des extincteurs : à ne négliger sous aucun prétexte !

Ils font tellement partie du paysage qu'on ne les remarque pas toujours. Pourtant, en cas de départ de feu, les extincteurs portatifs sont les premiers moyens d'intervention. Autant faire en sorte qu'ils fonctionnent en les maintenant correctement.

« **L'**extincteur portatif est connu de tous. Nous en croisons tous, tous les jours sur nos lieux de travail, lors de nos déplacements, dans des centres commerciaux... ils font partie de notre vie. Ils sont tellement communs qu'on y fait presque plus attention, constate Jérôme Desautel, président directeur général de Desautel et président du Syfex (FFMI). Or, rappelons que les extincteurs portatifs constituent le premier moyen d'intervention en incendie. Utilisés de manière appropriée, ils permettent d'éviter qu'un feu ne devienne un incendie. Les maintenir en état de fonctionner le moment venu est donc primordial. Et les opérations de maintenance doivent se faire correctement, selon les règles en vigueur. »

Avant d'aller plus loin, rappelons aussi que faire effectuer ces opérations de maintenance en temps et en heure relève de la responsabilité du chef d'établissement, du responsable du site. Ceci posé, le but de la maintenance des extincteurs portatifs est de faire en sorte que, quel que soit l'âge de l'extincteur – un an, deux ans, cinq ou neuf ans – il soit en état de

RAPPEL UTILE

Les extincteurs portatifs doivent être conformes à la norme EN 3-7 (avril 2004) qui spécifie les caractéristiques, les exigences de performance et les méthodes d'essai relatives aux extincteurs d'incendie portatifs.

Périodicité des vérifications

	EAU	POUDRE	CO2
Maintenance	1 an	1 an	1 an
Maintenance additionnelle et renouvellement charge	5 et 15 ans	5 et 15 ans	
Révision atelier et renouvellement charge	10 ans	10 ans	10 ans*
Durée de vie	20 ans	20 ans	Non fixée

La norme NF S61-919 porte sur la maintenance des extincteurs. Elle précise la périodicité des vérifications selon le type d'extincteurs.

* Par un organisme habilité

fonctionner le moment venu. « Il faut avoir présent à l'esprit qu'il n'est pas possible de savoir si un extincteur est en état de fonctionner, sauf au moment où on le percute pour éteindre un départ de feu, ajoute Jérôme Desautel. La maintenance permet de garantir à son propriétaire qu'il reste toujours en état de fonctionnement opérationnel. »

■ Des extincteurs normés

Choisir un extincteur est un acte important. Et nous avons la chance, en France, d'avoir encore un certain nombre de fabricants certifiés qui produisent des extincteurs répondant aux exigences de la norme européenne EN 3-7, gérée en France par l'Afnor. « On trouve sur internet ou ailleurs, des extincteurs à des prix défilants toute concurrence. On peut que déconseiller de se laisser tenter par ce genre d'offres, tient à souligner le président du Syfex. L'extinction incendie, et plus particulièrement les extincteurs, sont des produits "sérieux". Et il est profitable de s'équiper avec des produits de fabricants qui ont joué le jeu de la certification de leurs solutions par une tierce partie. »

■ Un double rôle

Le mainteneur joue un double rôle. D'une part, il s'assure que le produit installé à un instant T – pas nécessairement par lui, un, deux ou neuf ans auparavant est toujours à même de remplir son objectif. Au-delà des années, la mainte- ● ● ●

PAROLE D'EXPERT

JÉRÔME DESAUTEL

Président du Syfex et Pdg de Desautel



© DR

« LE MAINTENEUR DOIT ÊTRE FORCE DE CONSEIL. »

« La maintenance des extincteurs est très importante et ne doit pas être prise à la légère. Tout d'abord parce qu'elle permet de vérifier l'état de l'extincteur et, qu'en cas de doute, elle impliquera un remplacement de l'appareil défectueux. Par ailleurs, le mainteneur doit être force de conseil. C'est-à-dire qu'il doit être capable de préconiser une adaptation du parc d'extincteurs installés si ces derniers ne sont plus en adéquation avec le site et son risque incendie. Enfin, le mainteneur doit aussi s'assurer que le client est formé à l'utilisation des extincteurs. »

PAROLE D'EXPERT

MICHEL MESNIER

Vice-président du Sypsi* (FFMI) et gérant de Chronofeu



© DR

« IL FAUT FAIRE APPEL À UN PROFESSIONNEL QUALIFIÉ. »

« Les mainteneurs doivent respecter un cahier des charges précis. Faire appel à un mainteneur certifié est à l'appréciation du client, selon différentes exigences : les réglementations auxquelles il est soumis, les normes de vérification, les recommandations des fabricants et, éventuellement, une demande spécifique de leur assureur. Le mainteneur doit vérifier la pertinence de l'adéquation du type d'extincteur avec le risque à protéger... Il vaut mieux faire appel à un professionnel qui sera capable d'assurer ce devoir de conseil. Il faut aussi signaler que certains fabricants font parfois appel à des sous-traitants. On devra veiller à la qualification du prestataire. La maintenance en elle-même, outre un contrôle visuel de l'appareil, doit comprendre un certain nombre d'opérations qui sont à appliquer lors de la maintenance (détaillées dans l'encadré "documents relatifs à la maintenance"). »

* Syndicat des professionnels de la sécurité incendie



© Getty Images

● ● ● nance garantit donc que les performances de l'extincteur sont égales à ce qu'elles étaient lors de sa sortie d'usine.

L'autre mission du mainteneur est, comme le rappelle Jérôme Desautel, « de vérifier l'installation de l'extincteur et de l'ensemble de l'installation pour s'assurer qu'elle correspond toujours à la sécurité incendie attendue sur le site et en tenant compte de l'éventuelle évolution du bâti, des locaux, de leur destination... »

Si, lors de son intervention, le mainteneur constate qu'un appareil présente un défaut quant à son aptitude à l'emploi, il doit en alerter le client. « La maintenance ne s'improvise pas. C'est un vrai métier qui requiert un vrai professionnalisme car le mainteneur s'engage vis-à-vis de son client qu'après son intervention les extincteurs restent aptes à maîtriser un départ de feu », conclut le président du Syfex. ■



DOCUMENTS RELATIFS À LA MAINTENANCE

- **NF S61-919** : maintenance des extincteurs d'incendie portatifs (juillet 2004)
- **NF S61-922** : activités de service relatives à la maintenance des extincteurs portatifs, mobiles et fixes (juin 1999).
- **Guide pratique** pour la maintenance des extincteurs portatifs, mobiles et fixes (2009), FFMI-Afnor

Source : INRS.

2 QUESTIONS À

JEAN-BERTRAND HEYRAL

Délégué adjoint de la FFMI



© DR

Que doit-on attendre d'un mainteneur digne de ce nom ? Et en quoi la maintenance des extincteurs portatifs est-elle si importante ?

L'extincteur est par définition un appareil qui, le jour où cela est nécessaire, doit fonctionner correctement. On doit être certain de son aptitude à l'emploi, de son efficacité et de son adéquation

au risque couvert. La maintenance a donc pour objectif de s'assurer par un contrôle visuel et mécanique de l'extincteur qu'il pourra fonctionner le cas échéant. Les opérations de maintenance et les règles de l'art sont clairement définies dans des textes comme la norme de maintenance NF S61-919. Par ailleurs, à l'heure actuelle, tout le monde peut prétendre être mainteneur. Cependant, on ne peut que conseiller à tout propriétaire de site, tout responsable d'établissement... de faire appel à un prestataire, certifié par un organisme tierce partie pour l'installation et la maintenance d'extincteurs. Cela assurera que le mainteneur est qualifié, qu'il est titulaire, du CAP « agent vérificateur d'extincteur ».

En quoi les opérations de maintenance consistent-elles ?

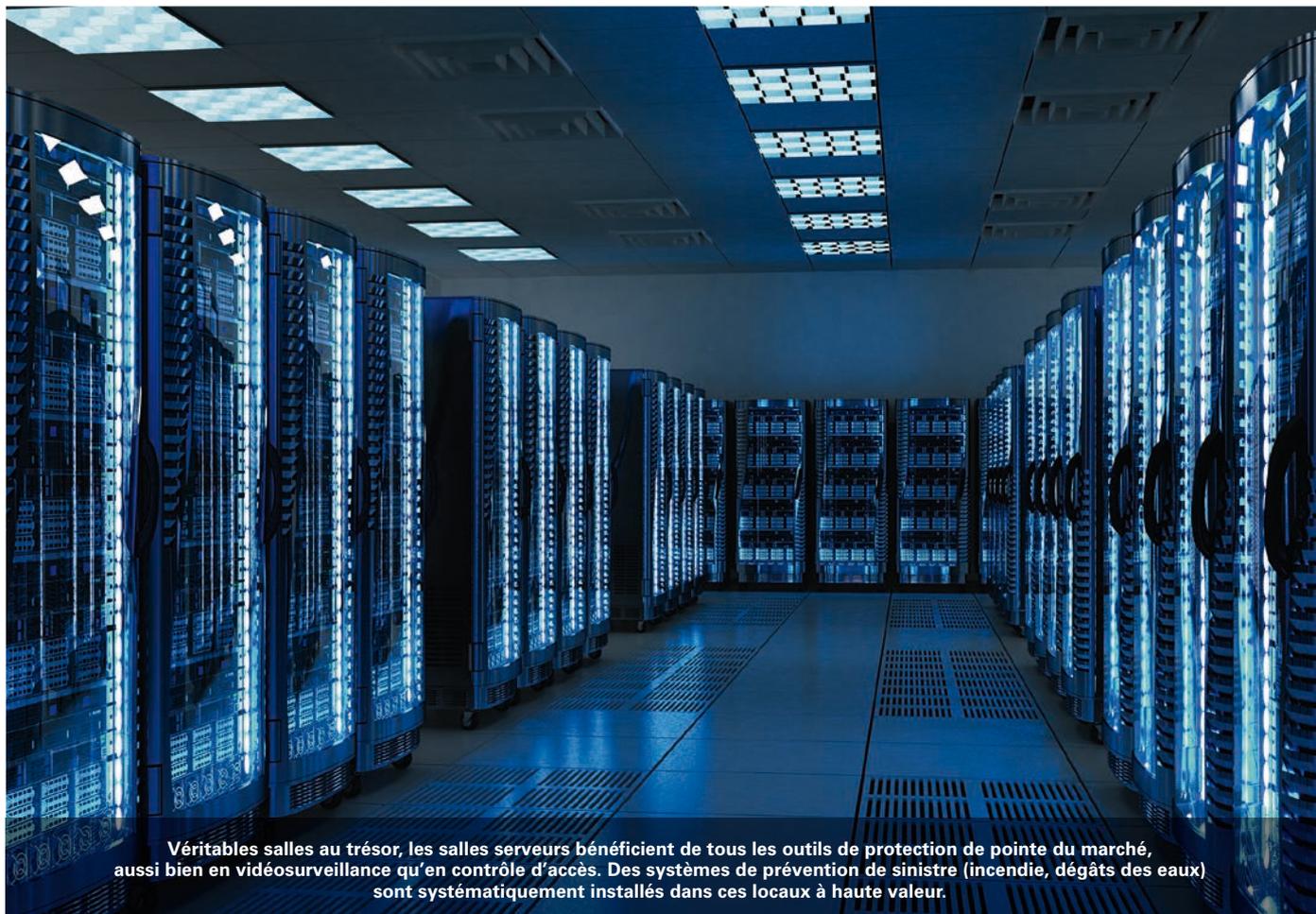
Tout commence par un contrôle visuel de l'appareil. On vérifiera aussi différents composants de l'extincteur comme les flexibles, les joints. On s'assurera aussi que le contenu est encore conforme à ce qui est indiqué sur l'extincteur. Le mainteneur doit aussi s'assurer de l'adéquation entre les extincteurs installés, les types de feux, le changement de destination des locaux... Et si nécessaire, conseiller au responsable d'établissement une modification de l'installation et une formation des occupants du site à l'utilisation des moyens de lutte.

**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 (vidéosurveillance, 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**



Véritables salles au trésor, les salles serveurs bénéficient de tous les outils de protection de pointe du marché, aussi bien en vidéosurveillance qu'en contrôle d'accès. Des systèmes de prévention de sinistre (incendie, dégâts des eaux) sont systématiquement installés dans ces locaux à haute valeur.

© Getty Images

Les datacenters : la sécurité à 360°

Les datacenters France stockent et préservent les milliards de données numériques des entreprises, des collectivités et des particuliers. Données qui, aujourd'hui, sont au cœur de l'économie. La sécurité physique de ces centres met sous haute surveillance les technologies de pointe les plus avancées afin de prévenir les risques de malveillance ou de sinistre qui pourraient avoir des conséquences désastreuses.

C'est un secteur en pleine croissance. Avec la multiplication des données et des échanges numériques, les données doivent être stockées et sécurisées. Les chiffres annoncés par l'association France Datacenter donnent le vertige : entre 2011 et 2016, le trafic mondial a été multiplié par 4,5, et il devrait être multiplié par six cette année pour atteindre les 44 zetaoctets. On compte

aujourd'hui 80 milliards d'objets connectés dont deux milliards en France. Comme l'indique l'association « *Twitter, SMS, Snapchat, emails, services administratifs, vente en ligne, moteurs de recherche, presse, communication, médias, sauvegarde et stockage de données, impôts, espaces clients, cours en ligne, CRM, ERP* : tous ces services utilisés au quotidien ont pour point commun de ne pas pouvoir être assurés sans les trois composantes des systèmes d'information que sont les terminaux utilisateurs, les

3 QUESTIONS À

LAURENT PIQUERET

Responsable grands comptes data centers chez DEF TTD – Comptes Spécifiques



Du point de vue des risques incendie, en quoi les Datacenters se distinguent-ils d'autres types de bâtiments ?

Dans les data centers, on est face à deux zones différentes : les locaux techniques, où l'on peut retrouver les groupes électrogènes et les onduleurs ; et les salles IT qui, elles, concentrent les serveurs. Statistiquement, ces salles présentent un risque incendie relativement faible, mais le moindre dommage peut y entraîner des pertes d'exploitation colossales. De plus, elles abritent du matériel de haute technologie, dont le coût peut se chiffrer en plusieurs dizaines

de millions d'euros. La prévention du risque et la détection précoce d'un départ de feu y sont donc primordiales.

Avez-vous des systèmes de détection spécifiques ?

Tout à fait. Dans ce type de centre, il faut mettre en œuvre une détection haute sensibilité pour pouvoir agir dès les premières fumées. Dans cet environnement, la détection de fumée ponctuelle classique ne convient pas, car la vitesse du brassage d'air liée à la ventilation est trop élevée. Pour répondre à cette contrainte technique, nous avons développé pour un grand opérateur téléphonique un système de détection par

aspiration haute sensibilité, Phénix. Ce système permet une détection très fine et surtout très précoce.

Quant au système d'extinction, que conseillez-vous ?

L'enjeu majeur en cas d'extinction est de préserver les données stockées dans les Data Centers. Dans ce sens, nous proposons plusieurs systèmes d'extinction adaptés à cette contrainte : des solutions basées sur du gaz neutre ou sur du brouillard d'eau haute pression. La solution à privilégier dépendra notamment du volume à protéger et des recommandations de l'assureur du client.

réseaux de télécommunication et les datacenters. Ces équipements et infrastructures permettent de collecter, stocker, analyser, transporter et restituer l'ensemble des données liées à nos usages numériques. » Or, toutes ces données ne se trouvent pas sur un nuage virtuel, mais sont bel et bien présentes physiquement dans un centre, sur des serveurs qui doivent les stocker et les rendre disponibles 24h/24, 7j/7. Et la France séduit de plus en plus les acteurs français et étrangers. La mise en place très précoce, en 1978, de la politique de protection des données personnelles avec la loi Informatique et liberté y est pour beaucoup, tout comme la Cnil dédiée à la protection des données personnelles.

■ Des forteresses sécurisées qui n'ont rien de virtuel

Les bâtiments qui abritent les serveurs sont les véritables forteresses du XXI^e siècle. À commencer par la conception elle-même. Récents, la plupart des datacenters ont intégré la sécurité au niveau de l'architecture : peu ou pas de fenêtres, des accès limités et contrôlés. Implantés – à quelques exceptions près, à l'extérieur sur des zones dégagées, avec un nombre d'accès limité et contrôlé, les datacenters mettent en place de la surveillance périphérique et périmétrique vidéo, doublée par des systèmes de détection d'intrusion sur la clôture. Des forteresses qui bénéficient de climatisation – indispensable au bon fonctionnement du matériel électronique, de systèmes de détection et d'extinction incendie à la pointe, ainsi que de tout un système de contrôle d'accès, de vidéosurveillance et anti-intrusion de pointe. Afin de prévenir les coupures électriques, tous les systèmes y compris de secours sont généralement doublés. Il n'est pas rare que les serveurs soient alimentés par deux sources électriques indépendantes de façon à pallier une éventuelle défaillance.

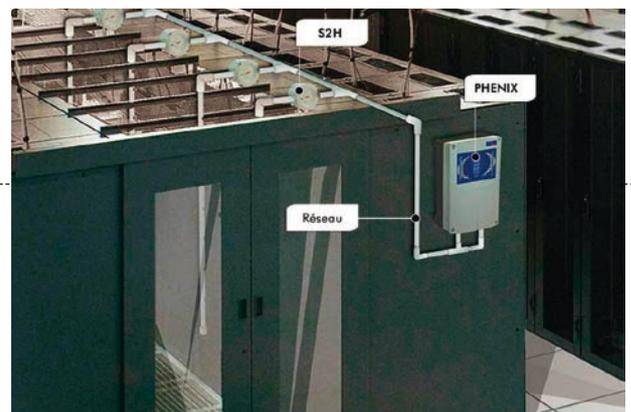
■ Accès : contrôler les véhicules et les hommes

La protection des accès au site est particulièrement sensible dans le cas des datacenters et doit pouvoir très rapi- ● ● ●

SOLUTIONS PRODUIT

Phénix, le système de détection de fumée par aspiration de DEF

Développé pour une entreprise majeure de la téléphonie, ce système a par la suite été standardisé pour répondre aux besoins spécifiques des Data Centers. Ce détecteur aspire l'air ambiant par l'intermédiaire d'un réseau tubulaire doté de points de prélèvement, et l'analyse à travers une chambre de mesure haute sensibilité. La mise en service et le paramétrage s'effectuent manuellement ou par l'intermédiaire d'un logiciel dédié. Cette gamme est déclinée en plusieurs versions, adressables ou conventionnelles, à un ou deux capteur(s). Le Phénix est destiné à la surveillance d'équipements ou de volumes critiques, tels que les Data Centers et salles serveurs, les salles blanches, les blocs opératoires, les musées, etc.



LA PAROLE À

JÉRÉMY REIGNER-DELLA
Régional Sales Manager, Hikvision

« LES CAMÉRAS THERMIQUES RÉPONDENT AUX EXIGENCES DE SÉCURITÉ SOPHISTIQUÉES DES DATASCENTERS, AUSSI BIEN EN PÉRIMÉTRIE QUE SUR LE SITE. »

« Nous utilisons nos caméras thermiques pour quadriller tous les abords du site. Les produits thermiques, spécifiquement ceux du groupe sécurité, répondent aux exigences d'une sécurité sophistiquée. Ils peuvent détecter la chaleur sur de longues distances. Les fonctions de franchissement de lignes et d'intrusion offrent une défense périmétrique de haute précision tout en réduisant les coûts. La facilité d'installation et d'utilisation permet de les implanter et de les prendre en main tout aussi rapidement. Nos PTZ équipés des fonctions Smart Tracking 2.0 sont capables de filtrer les fausses alarmes liées à l'environnement et de choisir le type de cible à suivre en fonction de sa classification (humain vs véhicule).

Nos caméras avec intelligence artificielle Deep Learning vont permettre de détecter un nombre anormal d'individu dans une zone définie, que ça soit un minima ou un maxima. Enfin, à noter nos nouvelles gammes de caméras haute définition Acusence équipées de haut-parleurs et de lumières stroboscopiques ajoutant une nouvelle couche dans la dissuasion et la protection des zones équipées. »

SUR LE TERRAIN

iLOQ sécurise le datacenter Telia, à Helsinki

Inauguré en juin 2018, le datacenter Telia d'Helsinki est le grand centre des pays nordiques.

Il fournit des systèmes de haut niveau pour la sécurité, la sûreté et l'alimentation, et dispose de plusieurs connexions au réseau mondial de Telia qui héberge près de 40 % du trafic internet mondial quotidien. Le centre de données peut accueillir près de 200 000 serveurs et une capacité de 5 000 racks. Avec plus de 30 000 m² déjà disponibles, l'espace des équipements est évolutif en fonction des besoins des clients, allant du quart d'une armoire de données à une salle de données spécifique au client. Il était vital pour Telia de choisir une solution de verrouillage pour les armoires et les salles qui soit également évolutive. iLOQ S50 est une solution de verrouillage sécurisée et entièrement numérique spécialement conçue pour les besoins des installations telles que les centres de données. iLOQ S50 utilise la technologie NFC et fonctionne via une application mobile sur smartphone. « Chez Telia, nous prenons la sécurité très au sérieux et nous apprécions les solutions mobiles. Comparé à une solution traditionnelle, la solution de gestion des accès mobiles S50 de iLOQ, nous a permis d'économiser des millions d'euros. Le système a rapidement été rentabilisé et les économies réalisées ne feront qu'augmenter » a déclaré Pasi



Sutinen, directeur du centre de traitement des données. Telia gère de nombreux sites dans le nord de l'Europe, des effectifs importants et de très nombreuses serrures. Cela signifie traditionnellement qu'un grand

nombre de clés sont en constante circulation. Avec iLOQ S50, les droits d'accès aux racks du datacenter peuvent être partagés et gérés avec un seul logiciel facile d'utilisation et sécurisé.

● ● ● demment repérer aussi bien les personnes que les véhicules. C'est dans cette optique, que Hikvision propose des solutions complètes de vidéosurveillance adossée au contrôle d'accès : « Nos caméras lecture de plaques permettent de vérifier immédiatement tout véhicule se rapprochant de l'entrée d'un site, indique Jérémy Reigner, Régional Sales Manager, Hikvision. La gestion des listes blanches et liste noires permet d'identifier un véhicule instantanément, de lui ouvrir la barrière automatiquement ou de l'orienter si besoin vers l'accueil en lui affichant un message personnalisé. Couplées à nos contrôles d'accès de dernière génération utilisant plusieurs conditions d'identification (reconnaissance faciale et/ou empreinte digitale et/ou badge et/ou code), chaque personne est identifiée et ne peut accéder qu'aux zones autorisées spécifiquement. »

■ Des câbles électriques sous haute surveillance

Si les serveurs sont les valeurs des datacenters les câbles électriques qui parcourent le centre et alimentent les serveurs sont souvent sous haute protection, avec des systèmes de détection d'anomalies. Jérémy Reigner-Della poursuit : « Nos caméras thermiques interviennent pour remonter toutes anomalies de température, aussi bien au niveau des équipements comme les câblages électriques et les serveurs, mais aussi dans la protection et dans la détec- ● ● ●

SÉCURITÉ INCENDIE

LIVRE BLANC LA SÉCURITÉ INCENDIE DANS LES DATACENTERS

L'association France Datacenter a publié en fin d'année 2019 le livre blanc *La sécurité incendie dans les datacenters*.

Le but de cette publication est de permettre aux exploitants d'être accompagnés dans la mise en œuvre des solutions de protection incendie adaptées à ce type de locaux. Ce livre blanc devrait aider le gestionnaire de site à définir la méthode d'analyse du risque la plus adaptée à son environnement de travail et ainsi, à optimiser l'exploitation de son installation. Il a été réalisé dans le cadre d'un groupe de travail réunissant six acteurs de l'écosystème des datacenters en France : 3M, Global Switch, Interxion, Finsecur, Bureau Veritas et Siemens.

Téléchargement gratuit sur le site de l'association France Datacenter : www.francedatacenter.com



SOLUTIONS PRODUIT

Tracetek de nVent pour prévenir les dégâts des eaux

Prévenir les dégâts des eaux causés par les fuites des systèmes de refroidissement dans un datacenter nécessite un système de détection qui assure une fiabilité de 100 %, 24 heures sur 24 ; Le système de détection de fuites d'eau nVent Tracetek est un système modulaire polyvalent avec de nombreux composants interchangeables qui peuvent être configurés pour correspondre à toute application spécifique. La détection de fuites d'eau est directe, rapide et précise, quel que soit le site (ou le lieu). L'équipement comprend différents composants

de détection de fuites pour vous garantir la sécurité absolue, quel que soit le type de bâtiment (ou l'application) : sondes de détection, câbles de détection avec polymères conducteurs, panneaux de surveillance et d'alarme. Durables, certains de ces câbles de détection sont en activité depuis plus de vingt-cinq ans.



© DR

Contrôle d'accès sans fil Aperio®

FAITES EVOLUER VOTRE S  STEME

ASSA ABLOY
Opening Solutions

A télécharger :
Test de compatibilité
Aperio®
www.assaabloy.fr/aperio

Experience a safer and more open world

2 QUESTIONS À

STEVEN COMMANDER

Directeur de la prescription, HID Global



Comment abordez-vous la sécurisation d'un datacenter ?

Comme sur tous les établissements, nous faisons un audit avec une analyse de risques en partant de la périmétrie vers le cœur du centre – là où se trouve les valeurs, c'est-à-dire les salles serveurs avec les baies. Sur la sécurité extérieure, il existe de nombreuses solutions de vidéo-surveillance infrarouges, radars, etc. En ce qui nous concerne, nous intervenons au niveau du bâtiment sur la partie contrôle

d'accès et particulièrement dans le cas des datacenters, nous allons beaucoup plus loin que dans un bâtiment tertiaire, puisque nous sécurisons au-delà des portes, en allant jusqu'aux baies et aux machines serveurs où l'on va sécuriser les armoires avec des serrures équipées de contrôle d'accès. On déploie toute une continuité de contrôle d'accès de l'extérieur vers le cœur de l'installation.

Qu'en est-il du niveau de sûreté ?

Il est évident que sur ce type d'établissement, ce qui est demandé ce sont des authentifications extrêmement fortes

– avec parfois sur certains accès, une double authentification, dont une biométrique. Dans les datacenters, le système de sûreté doit toujours être un réseau indépendant non ouvert sur l'extérieur. Le socle technique qui soutient la gestion des accès est identique à ce que nous proposons sur d'autres sites. En revanche, le gestionnaire doit être plus vigilant sur les habilitations et les droits. Nous attirons toujours l'attention des gestionnaires au niveau du paramétrage des badges pour qu'il respecte les protocoles de sécurité.

● ● ● *tion des incendies. Nos produits du groupe thermographie sont les plus adaptés. Dès qu'une température anormale est détectée dans une zone clé, elle est signalée et remontée pour prévenir les incendies à un stade précoce.* » De son côté, spécialiste de l'incendie, le groupe DEF a développé un système de capteurs haute sensibilité, Phénix, qui détecte précocement la présence de fumée et qui est particulièrement adapté aux datacenters. « Par rapport à d'autres secteurs, le risque incendie est faible, en revanche, la valeur des données conservées et celle du matériel sont telles que les solutions de détection installées sont parmi les plus performantes du marché », précise Laurent Piqueret, directeur adjoint du groupe DEF. ■



SOLUTION PRODUIT

HID Signo, la nouvelle gamme de lecteur haut sécurité

HID Signo est une gamme de lecteurs haut de gamme qui fait figure de nouvelle référence sur le marché du contrôle d'accès en matière d'adaptabilité, d'interopérabilité et de sécurité. Ces nouveaux lecteurs simplifient considérablement le déploiement et la gestion du système, répondent aux exigences de sécurité avancées des environnements dynamiques d'aujourd'hui et permettent aux organisations d'accéder à un système de contrôle d'accès plus intelligent et plus connecté. Les lecteurs sont interopérables avec plus d'une douzaine de technologies d'identification physique et mobile afin que les clients puissent utiliser la technologie de leur choix et migrer facilement vers les dernières solutions à leur propre rythme. Les lecteurs HID Signo sont également équipés de la fonctionnalité ECP (Enhanced Contactless Polling) d'Apple, qui assure la prise en charge des identifiants enregistrés dans Apple Wallet. Ces lecteurs sont dotés de fonctionnalités intelligentes, comme la détection de surface automatique qui permet de détecter la matière du support sur lequel il est installé (métal, etc.) et de se recalibrer automatiquement afin d'optimiser les performances de la distance de lecture. Tous les lecteurs prennent en charge le protocole de communication OSDP (Open Supervised Device Protocol) afin d'assurer des communications bidirectionnelles sécurisées. Chaque lecteur est également conçu pour être connecté et géré via une application mobile chiffrée et sécurisée.





Plus de
45%
de réduction!

OFFRE PACK psm

PROTECTION SÉCURITÉ MAGAZINE



psm • e-NEWSLETTER
PROTECTION SÉCURITÉ MAGAZINE
Les solutions pour les professionnels de la Sûreté - Sécurité
Lettre BIMENSUELLE - N°161 - 12/12/2019
pour vous VINCENT LEVER

psm PROTECTION SÉCURITÉ MAGAZINE
Guide d'Achat ANNUEL 2021
Annuaire DE LA Sécurité Sûreté
psm HORS-SÉRIE SÉCURITÉ Privée

psm PROTECTION SÉCURITÉ MAGAZINE
Toute l'actualité de la Sécurité et de la Sûreté
25/04/2018

Actualités: Sécurité privée. Sédexo se développe dans la sécurité. La Française va développer son activité dans la sécurité, un secteur en pleine croissance.

Direct: Pour lire et feuilleter l'édition numérique du Magazine PSM cliquez ici.

Rechercher: Recherchez un article.

Agenda: Tous les 10 jours.

PROTECTION SÉCURITÉ MAGAZINE

Tous les 2 mois, retrouvez toutes les informations sur la Sécurité et la Sûreté dont vous avez besoin pour agir.



E-NEWSLETTER

Tous les 15 jours, recevez l'e-mail qui résume l'essentiel de l'actualité dans la Sécurité et la Sûreté



LE GUIDE D'ACHAT ANNUEL

Toute l'offre en équipements: l'outil indispensable pour bien acheter!



L'ANNUAIRE DE LA SÉCURITÉ SÛRETÉ

Plus de 1.000 Fabricants, Distributeurs, Installateurs, Intégrateurs, Prestataires de services, ...



LE HORS-SÉRIE SÉCURITÉ PRIVÉE

L'actualité sur la sécurité privée



WWW.PROTECTIONSECURITE-MAGAZINE.FR

24h/24, 7j/7, votre accès illimité aux archives de votre magazine et aux services



BULLETIN D'ABONNEMENT À RETOURNER À PSM

PSM / TBS Blue - 6, rue d'Ouessant - 35760 St Grégoire. Tél: 01 76 41 05 88. Fax: 01 48 00 05 03. abopsm@tpmedia.fr

Oui, je souhaite m'abonner à PSM pour 1 an (6 numéros): **103 € TTC au lieu de ~~168 €~~**

Je règle: chèque > à l'ordre de PSM à réception de la facture

Mes coordonnées:

NOM _____
PRÉNOM _____
ADRESSE _____
CP _____
VILLE _____

SOCIÉTÉ _____

E-MAIL: _____

Le tarif indiqué est valable jusqu'au 31/12/2020 (TVA: 2.10%) en France seulement. Pour l'étranger, nous consulter. Conformément à la loi « Informatiques et libertés », vous disposez d'un droit d'accès et de rectification aux informations vous concernant auprès de l'éditeur.

TP Média: SARL au capital de 20.000 € - 488 819 137 RCS PARIS

J'économise + de 65 €, soit + de 45% de réduction!

Guide ANNUEL d'Achat

www.protectionsecurite-magazine.fr

DÉTECTION - ALARME



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



BY DEMES FRANCE
22/24 rue Lavoisier
Bâtiment B, 1^{er} 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

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

COMPUTAR / GANZ
www.cbc-cctv.com



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



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.com

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



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



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



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 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



27 rue du Chemin Vert
75011 Paris

01 81 80 14 30
france@iloq.com
www.iLOQ.com

IZYX SYSTEMS
www.izyx-systems.com



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



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



PROSEUR FRANCE
www.proseur.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



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



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://pyrex.com/detecteurs-
de-fumee

SERVIACOM
www.serviacom.fr

SLAT
www.slat.com

TYCO FIRE PROTECTION
www.tfpemea.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

quoi de neuf ?

SONORISATION

Axis veut faire des haut-parleurs les auxiliaires de la sécurité

« Longtemps les caméras ont été analogues. Lorsqu'Axis Communications a sorti sa première caméra IP en 1996, il a fait franchir un cap important à la vidéosurveillance. Nous voulons aujourd'hui faire la même chose de ces deux haut-parleurs : tirer le monde de la sonorisation vers le numérique, l'IP, pour lui donner l'opportunité de s'intégrer réellement et efficacement au sein d'une installation plus vaste de sécurité », souligne Jason Higgins-Casey, ingénieur des ventes chez Axis Communications. Avant d'ajouter : **« Ainsi, notre haut-parleur C1310-E réseau a été conçu pour des applications en extérieur. Il permettra de dissuader et de lutter contre les activités malveillantes des individus détectés par les caméras de surveillance. Robuste, il s'adapte facilement dans tous les environnements extérieurs et les différents climats »,** conclut Jason Higgins-Casey.

Voix claire et longue portée

L'Axis C1310-E est une unité tout en un avec amplificateur de puissance et traitement du signal (DSP) intégrés. Grâce à son traitement du signal numérique préconfiguré, il dispense une voix claire. Sa mémoire intégrée prend en charge les messages vocaux préenregistrés. Il offre aussi la possibilité au personnel de sécurité de répondre aux notifications ou de fournir des instructions avec la prise de parole en direct. Il se branche directement sur les réseaux IP standard et prend en charge Power over Ethernet (PoE). Compte tenu de l'unité autonome dont il dispose, vous pouvez le placer n'importe où. Il s'appuie sur des normes ouvertes, pour une intégration aisée avec votre logiciel de gestion vidéo (VMS), avec la téléphonie Voix sur IP (VoIP) (à l'aide de SIP) et avec les outils d'analyse d'Axis et de ses partenaires.

À noter : Axis vous propose aussi le C1410, un haut-parleur IP pour applications en extérieur. ■

➔ www.axis.com/fr/products/axis-c1310-e



3 QUESTIONS À

AZAD KHAMOOSHI

Business Development Manager chez Axis Communications



© DR

Pourquoi avoir décidé de lancer ces deux nouveaux haut-parleurs ?

La sonorisation, la diffusion de messages, l'interpellation sonore doivent passer à l'ère de l'IP et du numérique. Pour enfin venir s'intégrer dans des ensembles plus vastes de sécurité comprenant contrôle d'accès, vidéosurveillance, solutions anti-intrusion, VMS... La sonorisation se doit d'être plus efficace que ce qu'elle est actuellement. Trop souvent, sur le terrain, elle n'est pas digne de ce nom. On doit pouvoir diffuser des messages clairs sur de longues portées, diffuser des messages différenciés par zones, par étages... Nos haut-parleurs permettent tout cela puisque grâce à eux il est très simple de faire du zonage, par exemple.

Quel est le principal intérêt des haut-parleurs IP ?

Comme n'importe quel outil réseau, ils ont une adresse IP. Ils viennent donc s'intégrer très facilement dans un réseau vidéo pour faire de l'interpellation, de la verbalisation... en temps réel. On a aussi la possibilité de paramétrer la diffusion automatique de message en cas de détection d'incident par une caméra. On peut notamment diffuser automatiquement des messages récurrents comme ceux annonçant la fermeture d'un site, d'un magasin... En ces temps de confinement et de sortie du confinement, on peut tout à fait envisager la diffusion de messages informant le public ou les agents de sécurité que le site ne peut plus accueillir personne, qu'il a atteint sa capacité d'accueil...

Pouvez-vous nous présenter rapidement le modèle C1410 ?

Il s'agit d'un haut-parleur réseau conçu pour des applications en intérieur. Il se branche lui aussi sur un réseau IP standard. Basé sur des normes ouvertes, il s'intègre aisément avec un VMS, la téléphonie, VoIP et nos outils d'analyse et ceux de nos partenaires. Il contient également un capteur PIR permettant la détection de mouvement qui peut déclencher un message audio. Cette combinaison de fonctionnalités rend ce dispositif très autonome.

➤ CARACTÉRISTIQUES

- Système de haut-parleur tout en un
- Se connecte au réseau standard
- Installation simple avec PoE
- Tests d'état à distance
- Deux entrées/sorties (GPIO)

SÉCURITÉ PHYSIQUE

Endurance, dispositif de sécurité traité antibactérien

Développée par Iseo, Endurance est une gamme de fermetures anti-panique aux propriétés antibactériennes permanentes.

Pourvus du traitement breveté AntiGerm, ces équipements sont conçus pour tous les bâtiments où l'activité microbienne est légitimement redoutée : collectivités, lieux publics (salles de spectacle, gymnases, piscines, écoles, crèches, bureaux, etc.) et le secteur de la santé, des hôpitaux aux maisons de retraite. Ces produits répondent à deux exigences conjointes en matière de sécurité et de sûreté : évacuation rapide en cas d'urgence et impératif de protection sanitaire. Le traitement antibactérien permanent utilisé par Iseo sur une propriété bien connue des ions d'argent : celle de paralyser la nutrition et la reproduction des micro-organismes. Les ions d'argent, qu'on retrouve notamment dans les pansements, sont relâchés en proportion infinitésimale par le vernis anti-germe qui recouvre les produits de la gamme. L'efficacité de ces dispositifs, testés par des laboratoires indépendants, est avérée sur plus de 600 bactéries, par exemple les légionnelles, salmonelles et listérias. ■

→ www.iseo.com/it/fr/home/



© DR

CONTRÔLE D'ACCÈS

Paxton lance Paxton10

Le système de contrôle d'accès et de gestion par vidéo de la nouvelle génération de chez Paxton, Paxton10, a été officiellement lancé en France le 5 mai dernier. Paxton10 illustre la prochaine étape des systèmes intégraux de sécurité, et combine le contrôle d'accès à la gestion par vidéo sur une seule et unique plateforme. Grâce aux dernières techniques utilisées pour combiner les différentes situations d'entrée dans les locaux et les séquences vidéo en un même point, Paxton10 simplifiera la gestion et la protection des sites tout en apportant aux clients quelque chose dont ils n'ont jamais été témoins auparavant. Nous pensons que ce système est tout à fait inédit. D'après les réactions et commentaires que nous en avons reçus, nos installateurs s'étaient montrés très enthousiastes dans la direction que nous emprunions grâce à Paxton10, et en particulier à la nouvelle technologie. ■

→ www.paxton-access.com

Paxton10



© DR

→ CARACTÉRISTIQUES

- Contrôle d'accès et gestion par vidéo en un seul et même système
- Références intelligentes d'identification de Paxton10 - technologie sans fil Bluetooth permettant aux smartphones ou aux smartwatches d'être utilisés à la place des clés traditionnelles ou des badges électroniques
- Télé accès mondial - donnant aux installateurs la possibilité de proposer un service intégral de gestion de la sécurité à leurs clients
- Système modulaire unique pour portes
- Évolutif de 1 à 1 000 portes et pouvant aller jusqu'à 1 000 caméras
- Intégralement compatible avec les poignées de porte sans fil PaxLock et le système de vidéophonie Entry de Paxton, etc.

quoi de neuf ?

PTI

Bouton d'alerte No Dead Zone : une protection sans « zone blanche »

myDevices, le pôle IoT de Claranova, déploie sa nouvelle technologie de bouton d'alerte No Dead Zone combinant les réseaux cellulaires, Bluetooth, wi-fi et LoRaWAN pour sécuriser le personnel isolé. La diffusion des réseaux cellulaires, Bluetooth et wi-fi

est contrainte à l'intérieur des bâtiments par les matériaux lourds de construction qui bloquent les signaux, créant des « zones blanches » inaccessibles à toute communication. Les algorithmes de la technologie No Dead Zone éliminent les zones blanches en associant aux protocoles de communication traditionnels, le réseau IoT LoRaWAN. Cette technologie de transmission longue distance, à faible puissance et faible bande passante permet une couverture complète de l'ensemble des bâtiments, quelle que soit leur taille et leur configuration. La solution myDevices se caractérise par sa rapidité d'installation, sa facilité d'utilisation et son faible coût de déploiement.

L'architecture edge-to-cloud de la solution No Dead Zone, associée à la sécurité native du protocole LoRaWAN et celle de l'Azure IoT Hub de Microsoft garantit une communication fiable et sécurisée. Soutenue par les plus grandes chaînes hôtelières américaines – dont Marriott, InterContinental, Hilton et Hyatt – No Dead Zone vise à renforcer la sécurité du personnel. 57 chaînes hôtelières, représentant près de 20 000 hôtels et 1,2 million d'employés à travers l'ensemble des États-Unis, ont déjà rejoint l'initiative. Ce bouton d'alerte, « panic button », est une solution de communication d'urgence visant à protéger les employés de tout harcèlement ou agression et à les mettre en sécurité dans les meilleurs délais. ■

→ www.claranova.com



© DR

LUTTE CONTRE L'INTRUSION

Defenso SR4 LPCB, solution certifiée haute sécurité

Les produits EJ sont fabriqués dans leur version standard, avec de l'acier galvanisé selon la norme ISO 1461.

Cette protection anti-corrosion standard est suffisante dans de nombreux environnements. Cependant, pour les chantiers les plus exposés à la corrosion, EJ a également développé des procédés permettant d'augmenter efficacement et durablement la protection anti-rouille. Grâce à une épaisseur accrue de 140 μm de zinc, la durée de vie du dispositif peut être doublée. Enfin, dans des environnements particulièrement hostiles en intérieur comme les applications industrielles ou en extérieur comme les zones côtières, des phénomènes comme une haute fréquence de condensation, une ventilation quasi inexistante, un environnement très pollué, avec des teneurs en SO_2 comprises entre 90 $\mu\text{g}/\text{m}^3$ et 250 $\mu\text{g}/\text{m}^3$, requièrent un revêtement supplémentaire, appliqué par thermolaquage.

> Applications : réseaux de production ou de distribution d'eau potable, assainissement ; réseaux d'électricité ou de gaz ; réseaux de communication électroniques... ■

→ www.ejco.com/global



© DR

VIDÉOSURVEILLANCE

Détection de température chez Dahua

La solution thermique de Dahua mesure la température corporelle du public et gère chaque jour le flux de milliers de membres du personnel. Comparé à la méthode traditionnelle de mesure de la température corporelle (thermomètre frontal), la solution Dahua améliore significativement la cadence et la précision, tout en contribuant à réduire la contamination croisée grâce à une surveillance sans contact humain. ■

➔ www.dahuasecurity.com/fr



© DR

➔ CARACTÉRISTIQUES

- Pour mesurer la température de 5000 personnes, environ 4,2 heures seraient nécessaires avec un thermomètre frontal, étant donné qu'il faut au moins trois secondes pour prendre la température d'une personne. En outre, il ne faut que trente minutes avec la solution thermique de Dahua, qui mesure trois personnes par seconde, et qui garantit une précision élevée ($\pm 0,3$ °C).

CONTRÔLE D'ACCÈS

Nouvelle gamme iLOQ S5 : l'intelligence sans batterie

Avec iLOQ S5, solution de verrouillage flexible et modulaire, vous pouvez choisir quelle « clé » vous souhaitez utiliser : clé digitale iLOQ S5, clé smartphone iLOQ S50 (sous iOS ou Android), badge Key Fob ou code d'accès confidentiel.

Autre avantage : iLOQ S5 actualise les accès en permanence par le biais de la communication inter-périphériques, appelée Device-to-Device (D2D). Cette fonction évoluée permet de mettre à jour et de partager rapidement, et à distance, une grande quantité de données : listes de clés bloquées (blocklist), restrictions horaires, dernières heures d'utilisation, remontées d'événements et historique de la clé. Toutes les communications sont bidirectionnelles entre le logiciel de gestion

et les lecteurs, les clés et les serrures qui équipent un bâtiment avant le déverrouillage d'une porte. Finis les va-et-vient incessants entre les sites et les bureaux d'administration pour importer ou exporter manuellement des données vers les serrures et les clés. Les dépenses liées au câblage du système, les coûts d'exploitation tout au long du cycle de vie, et l'impact environnemental, sont considérablement réduits. La technologie NFC exploitée par iLOQ permet d'associer les serrures iLOQ S50 à un smartphone qui joue à la fois le rôle de clé d'accès et de source d'alimentation. Sur la gamme iLOQ S5, les téléphones pourront bientôt être utilisés comme un canal de communication afin de mettre à jour les droits d'accès des clés iLOQ S5 et iLOQ S50 via l'application exclusive iLOQ S5. ■

➔ www.iloq.com



© DR

quoi de neuf ?

CAMÉRA THERMIQUE

La XI400 d'HTDS pour une mesure cutanée à distance

Dans le cadre de son département « Sûreté et détection », et afin d'aider les différents organismes (collectivités, armées, forces de l'ordre, services de sécurité, etc.) à lutter contre l'épidémie de Covid-19, HTDS a décidé d'accélérer la mise à disposition de la nouvelle caméra thermique XI400, un système innovant de mesure à distance de la température cutanée. Conçu pour la sécurité sanitaire et idéal pour une détection sans contact d'une potentielle fièvre chez les voyageurs et les personnes fréquentant les lieux publics, le système XI400 est basé sur un fonctionnement discret. La caméra de taille réduite permet de distinguer précisément dans la foule les personnes dont la température de la peau dépasse une valeur prédéfinie. Une alarme visuelle donne à l'opérateur la possibilité d'identifier et d'isoler immédiatement les personnes suspectes afin qu'un examen médical puisse être mené rapidement. Doté d'un détecteur FPA, non refroidi (pitch $17 \mu\text{m}$) et d'une résolution optique 382×288 pixels pour une plage spectrale de 8 à $14 \mu\text{m}$, la nouvelle caméra thermique XI400 offre une précision de $\pm 1^\circ\text{C}$ ou $\pm 2\%$. Au niveau technique, la caméra est reliée à un PC qui grâce au logiciel fourni avec la caméra offre la possibilité de prendre automatiquement des images infrarouges instantanées lorsque l'alarme est déclenchée. ■

➔ www.htds.fr



MODÈLES

- Wisenet LRN-410S : NVR PoE 4 canaux avec enregistrement caméra réseau jusqu'à 30 Mbit/s et 1 disque dur SATA (6 To max.)
- Wisenet LRN-810S : NVR PoE 8 canaux avec enregistrement caméra réseau jusqu'à 50 Mbit/s et 1 disque dur SATA (6 To max.)
- Wisenet LRN-1610S : NVR PoE 16 canaux avec enregistrement caméra réseau jusqu'à 100 Mbit/s et 2 disques durs SATA (12 To max.)

CAMÉRAS

Détection de fièvre chez Hikvision



Avec des détecteurs et des algorithmes avancés, les caméras thermographiques de détection de température corporelle de Hikvision sont conçues pour détecter des températures élevées à la surface de la peau et peuvent ainsi être utilisées pour le dépistage rapide et préliminaire de la fièvre dans les immeubles de bureaux, usines, gares, aéroports et autres lieux publics, avec une précision allant jusqu'à $\pm 0,3^\circ\text{C}$.

La gamme comprend :

- Une caméra turre/bullet qui dispose d'une détection AI pour réduire les fausses alarmes causées par d'autres sources de chaleur.

- Une caméra turre/bullet + calibrateur de corps noir : cette solution est améliorée avec un calibrateur de corps noir pour augmenter la précision de $\pm 0,5^\circ\text{C}$ à $\pm 0,3^\circ\text{C}$.

- Une caméra portable avec un module wi-fi, qui peut se connecter à un PC ou à un smartphone. Il dispose également d'un haut-parleur intégré pour l'alarme audio. ■

➔ www.hikvision.com/fr

CONTRÔLE D'ACCÈS

Identifier les personnes à risques avec Genetec

Genetec vous propose une nouvelle fonctionnalité de reporting dans son système de contrôle d'accès Security Center Synergis (Synergis), conçue pour aider les entreprises à trouver tous les individus qui ont emprunté une porte à proximité d'une personne considérée comme contagieuse. Il est possible que celle-ci ait contaminé la poignée de la porte ou d'autres surfaces, ou qu'elle ait laissé des contaminants aérosols sur son passage. Ce rapport permet d'identifier toutes les personnes qui présentent un risque accru d'avoir été en contact avec des contaminants ou des personnes contagieuses. Cette fonction sera également utile aux clients qui manipulent des substances dangereuses et est mise gratuitement à la disposition de tous les clients du système de contrôle d'accès Genetec Synergis.

Développée à la demande de McCormick Place à Chicago, le plus grand centre de congrès d'Amérique du Nord, la fonctionnalité de rapport permet d'établir s'il y a eu proximité physique entre une personne infectée et d'autres employés ou visiteurs badgés, sur la base de leur utilisation du système de contrôle d'accès. Un rapport peut rapidement être généré pour mettre en relation des événements d'accès, tranche horaire par tranche horaire, afin d'identifier les personnes qui présentent un risque accru d'avoir été en contact avec des contaminants ou des personnes contagieuses. ■

→ www.genetec.com



© DR

CAMÉRA

Flir A320 Tempscreen

La caméra Flir A320 Tempscreen est préconfigurée pour surveiller des individus et des groupes de personnes afin de trouver des écarts de température ou une température cutanée élevée, y compris des alarmes de différence de température avec une température de référence mise à jour dynamiquement.

Cette solution de mesure de la température offre une analyse intégrée, une fonctionnalité d'alarme et une communication autonome à l'aide de protocoles standard.

Le Flir A320 Tempscreen possède également des caractéristiques et des fonctions permettant de créer des solutions distribuées à une ou plusieurs caméras en utilisant des protocoles matériels et logiciels Ethernet standards. ■

→ www.flir.com



© DR

CARACTÉRISTIQUES

- Plages de mesures de température : -20° C à +120° C
- Résolutions IR : 320x240 pixels
- Taux de rafraîchissement : 30 Hz
- Types de mise au point : automatique, manuelle



« Le continuum sécurité n'a jamais existé ! »

DRISS AÏT YOUSSEF

Docteur en droit, président de l'institut Léonard de Vinci

Driss Aït Youssef dresse un tableau sans concession des relations entre l'État et le monde de la sécurité privée. Âmes sensibles s'abstenir...

D'aucuns considèrent que la crise du Covid-19 aura des conséquences néfastes sur le fameux continuum sécurité. C'est à mon sens une vue de l'esprit car ce projet de continuité n'a jamais réellement existé car il n'y a jamais vraiment eu de concertation réelle entre les pouvoirs publics et les acteurs de la sécurité privée. Le continuum se matérialise tout au plus comme un transfert de charges du public vers le privé et quelquefois même sans grande concertation. C'est toujours l'État qui, conscient de son incapacité à assumer certaines de ses missions, décide, souvent de manière unilatérale, de les confier au secteur privé. Le continuum au sens noble du terme ne s'est donc jamais réellement matérialisé. Pour être tout à fait honnête, je crains que les professionnels de la sécurité privée ne fondent trop d'espoir sur un terme qui relève davantage d'un mirage plutôt que d'une vision stratégique et organisée de l'État.

■ Un manque de confiance

Pourquoi cela ? Tout simplement parce que, et la crise du Covid-19 vient de le montrer, l'État ne fait pas totalement confiance à la sécurité privée malgré les efforts de cette dernière en se professionnalisant et faisant le ménage dans ses rangs afin de devenir un partenaire crédible et incontournable. Un exemple parlant de ce manque de confiance ? Le cas de la sécurité maritime. L'État, la Marine nationale en l'occurrence, a vite compris, il y a quelques années, qu'il ne pouvait pas assurer la sécurité des navires marchands battant pavillon français. Il a donc décidé de déléguer cette mission à la sécurité privée. Mais qu'a-t-il fait ? Il a tellement contraint ce marché, défini des règles extrêmement strictes, que cette opportunité économique est vite devenue inaccessible pour les

entreprises françaises... Nous ne sommes toujours pas sorti de la logique de la loi de 1983 qui fut une loi de défiance au secteur...

■ La sécurité privée ne facilite pas le travail à l'État...

Cela pourra-t-il changer à terme ? Il faudrait préalablement que l'État définisse une doctrine d'emploi de la sécurité : poser un nouveau débat sur les rôles de la police et de la gendarmerie nationales pour définir ensuite le type de collaboration avec la sécurité privée. Il faudra donc un vrai dialogue sur les missions possibles, les pouvoirs, la formation, les salaires, la réglementation, la déontologie... Ce n'est qu'à partir de ce moment que le continuum s'imposera aux acheteurs pour valoriser une prestation de sécurité au bon tarif. Je reste étonné par la capacité du gouvernement à produire un décret pour fixer le prix d'un gel hydroalcoolique et pas le tarif horaire d'un agent de sécurité. Enfin, pour installer une vraie relation de confiance entre l'État et le secteur, il faut lui opposer un groupement professionnel unique, crédible et représentatif d'une filière apaisée faisant litte des querelles de personnes. Il est donc urgent se sortir de cette relation bricolée entre l'État et la sécurité privée. À défaut, c'est le Cnaps qui se substituera comme c'est un peu le cas aujourd'hui aux organisations pour le représenter auprès des pouvoirs publics. ■

DRISS AÏT YOUSSEF ■ 2009 Président d'un groupe de travail pour le ministre de l'Intérieur sur la formation des policiers et gendarmes ■ 2011 Président de l'institut Léonard de Vinci ■ 2015 Doctorat en droit public « sécurité privée et libertés » ■ 2019 Expert participant au groupe de travail du ministère de l'Intérieur sur la refonte du schéma national du maintien de l'ordre.

Pour un environnement de travail SAIN et SÉCURISÉ

Bien-être des équipes

Performance des collectivités



Préventica

LYON

29 **SEP** > 01 **OCT**

Eurexpo

L'information dont vous avez besoin est ici!

protectionsecurite-magazine.fr

Toute l'actualité de la Sécurité et de la Sûreté

- Infos
- Archives
- Annuaires
- e-salon
- Dossiers techniques

