PROTECTION DE SITES

GICAT

GROUPEMENT DES INDUSTRIES DE DÉFENSE ET DE SÉCURITÉ TERRESTRES ET AÉROTERRESTRES | WWW.GICAT.COM

EN PARTENARIAT AVEC :

FIEEC
FEDERATION DES INDUSTRIES ELECTRIQUES, ELECTRONIQUES ET DE COMMUNICATION

Club des Directeurs de Sécurité des Entreprises CDSE

Cofis

CICS
Conseil des Industries de la Confiance et de la Sécurité

Editorial du Contre-amiral Frédéric RENAUDEAU, Directeur de la protection des installations, moyens et activités de la Défense

Depuis le début de l'année 2015, le spectre des menaces sur le territoire national a sensiblement évolué. Aux actions d'espionnage ou d'ingérence d'origines étatiques, et au terrorisme djihadiste « haut du spectre » utilisant des modes d'actions de nature militaire, s'ajoute désormais la menace dite « bas du spectre » susceptible de s'en prendre à des cibles plus ouvertes sur l'extérieur. Cette menace terroriste à spectre plus large est potentiellement aggravée par la malveillance interne liée à la radicalisation. En outre, les mini-drones représentent un mode d'action nouveau et, par conséquent, une menace particulière à traiter. Quant aux attaques « cyber », l'actualité nous confirme hélas chaque jour leur forte augmentation, en fréquence, technicité et diversité. Enfin, la conjugaison de ces menaces physique et numériques constitue un facteur aggravant.

Ce changement de paradigme a imposé d'importants efforts de renforcement de la protection des installations, moyens et activités de la Défense. Ceux-ci ont porté sur l'analyse exhaustive des vulnérabilités, la refondation d'une politique de protection adaptée à ces nouvelles menaces, l'élaboration de normes et de standards techniques et, surtout, la mise en place d'un plan ambitieux de renforcement de la protection physique des emprises (avec un effort financier passant d'environ 50 M€ en 2014 à 200 M€ en 2017, ainsi qu'un accroissement sensible des effectifs militaires affectés aux fonctions de protection). Mais l'efficacité de ces efforts est conditionnée par l'indispensable action de sensibilisation, de formation et de responsabilisation de tout un chacun et, plus généralement, par le développement d'une démarche robuste de résilience.

Cette action du ministère des Armées s'inscrit en pleine synergie dans le cadre national de coordination de l'ensemble des acteurs de la sphère publique et privée du domaine de la protection, comme par exemple les travaux du COFIS portant sur les expressions de besoin capacitaire en matière de sécurité, ou encore ceux du CNAPS.

Je ne peux donc que me réjouir des différentes actions menées par le GICAT, et notamment de la publication de cette brochure sur la protection de sites sensibles, qui s'inscrit pleinement dans cette démarche et répond à un réel besoin.

CONTRE-AMIRAL FRÉDÉRIC RENAUDEAU

Directeur de la protection des installations, moyens et activités de la Défense

Protéger ensemble !

Toutes nos entreprises exercent leurs activités, souvent des plus sensibles, dans un environnement aux menaces croissantes et protéi-formes à l'encontre de leur patri-moine matériel, immatériel et humain, ou de la sécurité de leurs affaires.

Afin d'assurer leur développement et garantir leur pérennité, nous nous devons tous d'adapter les dispositifs nécessaires à leur protection.

Nos propres politiques de sûreté ou de sécurité, notamment face à la malveillance, nous permettent de définir les principes, les règles et l'organisation visant à détecter les menaces, maîtriser les risques à l'encontre de nos patrimoines et en minimiser les conséquences.

La sécurité de nos entreprises est une exigence de tous les instants. Elle est également une somme d'exigences qui sont prises en compte par différents acteurs et partenaires répondant tous, à leur niveau, aux préoccupations et aux besoins de chacun.

Au-delà de la nécessaire sensibilisation et des formations adaptées, développées auprès de nos agents et salariés qui constituent toujours notre capital le plus important, la responsabilisation de tous passe également par la définition claire des besoins de chacun dans le domaine de la sécurité ou de la sûreté.

Plus que jamais, la protection de nos sites passe aussi par celle de notre patrimoine immatériel qui constitue une richesse fragile suscitant toutes les convoitises plus ou moins malveillantes.

Chaque site étant un cas d'espèce en lui-même, il importe de rassembler, dans une coproduction parfaite des expertises internes et externes, l'ensemble des solutions qui nous permettront de mieux sécuriser et protéger en réduisant nos vulnérabilités. Cette approche dynamique doit couvrir tous les domaines et toutes les solutions potentielles : de l'audit au commandement de terrain en passant notamment par la simulation, l'intégration, le contrôle d'accès, la détection ou la communication.

Dès lors, sur chacun de nos sites et sur la base d'une analyse fine des risques, un dispositif de sécurité proportionné ne peut être mis à jour qu'en partenariat total avec les entreprises, petites ou grandes, ayant démontré leur degré d'expertise dans des domaines que tous ne peuvent totalement maîtriser.

ÉMILE PÉREZ

Directeur de la sécurité et de l'intelligence économique du Groupe EDF

La protection de sites

On entend par infrastructures critiques les biens et services revêtant une importance capitale pour la population et l'économie, tels que les systèmes gérant l'énergie, les transports, la nourriture ou la sécurité. Le pillage d'un dépôt des forces armées ou la prise de contrôle d'une centrale nucléaire pourrait provoquer des dommages importants pour les populations et être dévastateur pour l'opérateur concerné. Le but de la protection des sites est donc d'éviter autant que possible ce genre d'évènement ou du moins en réduire au maximum la gravité et la durée.

Le développement de nouvelles formes de menaces cherchant à obtenir facilement un impact médiatique maximum a entrainé une réaction des gouvernements. Dans la plupart des pays ceux-ci ont durci les réglementations obligeant les opérateurs d'infrastructures critiques à se protéger. Le présent document traite de la protection physique, étant entendu que la protection cyber revêt une importance égale.

Les mesures de protection peuvent être temporaires ou permanentes et se classent généralement en trois grandes catégories :

- Mesures de protection physique axées sur les composantes physiques d'une infrastructure qui sont l'objet de ce document.
- Mesures de protection humaine qui s'adressent au personnel et à d'autres personnes ayant, sous une forme ou une autre, un lien avec l'infrastructure (sous-traitants, visiteurs, clients…)
- Mesures organisationnelles censées agir sur le mode de gestion de l'infrastructure

Sans oublier, évidemment, les mesures électroniques ou de cyber protection destinées à protéger l'infrastructure informatique et les communications.

Si on regarde le détail du processus concernant les mesures physiques, on voit donc qu'il se définit en quatre grandes phases :
La première est la phase d'analyse et d'étude. Il s'agit d'une part d'évaluer les enjeux : usagers et personnels, biens et équipements, patrimoine immatériel (savoir-faire, image de l'entreprise) ; et d'autre part les risques et menaces liés à ces enjeux. Cette démarche doit en particulier prendre en compte les spécificités du site considéré (Nature des dommages potentiels, importance symbolique, vulnérabilités particulières, voies d'accès, dépendances à l'Energie et à d'autres facteurs, etc.) Elle s'attache également à se mettre dans la peau des différents agresseurs potentiels (terroristes, voleurs, activistes, menace interne…) afin d'imaginer un maximum de scénarios d'attaque possibles. Enfin elle définit les formations nécessaires non seulement pour le personnel de sécurité mais aussi pour l'ensemble des personnels du site.

Cette étude débouchera sur une expression de besoin qui permettra de passer à la deuxième phase, la définition, l'achat et la mise en place des différentes composantes du dispositif de sécurité et de la formation associée.

Dans tous les cas, ce dernier devra répondre a minima à huit grandes problématiques :

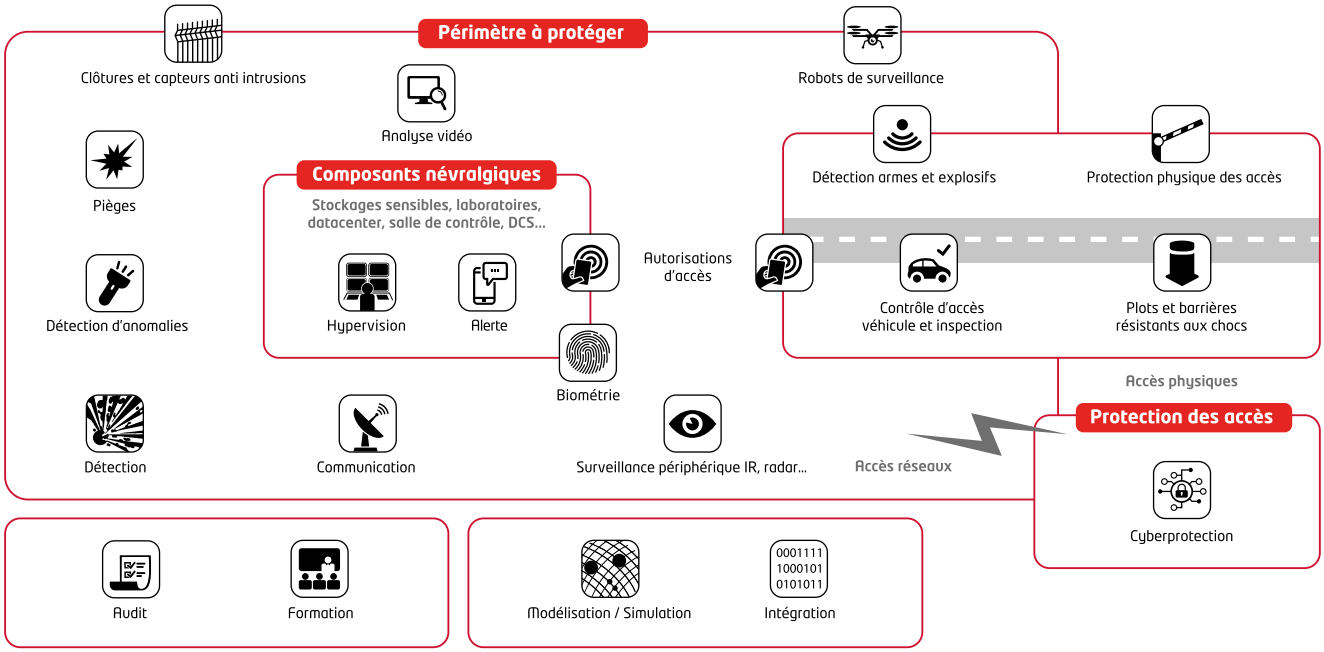
- Contrôle, identification et authentification : cette fonction a pour but de déterminer qui ou quoi a le droit d'entrer dans le site, ou il a le droit d'aller et de vérifier autant que possible que les identités de ces personnes et objets sont véridiques.
- Dissuasion : Une partie du dispositif doit être visible voire affichée, ceci afin d'afin de décourager les velléités d'actions malveillantes
- Retardement : il est fondamental de retarder l'intrusion ou sa progression ceci afin d'augmenter le délai disponible pour une réaction ou une intervention et les chances de succès de cette dernière. On cherche donc en pratique à élaborer un parcours d'obstacle comprenant de multiples barrières à franchir et d'éléments retardateurs.
- Détection de l'intrusion : cette détection doit être la plus précoce possible pour permettre une intervention efficace et à temps. Elle est en général à double objet : détection d'une intrusion et détection de phénomènes anormaux à l'intérieur du périmètre, tels que des incidents d'exploitation ou des comportements anormaux d'entrants « licites »
- Alerte : remontée d'information relative à une détection vers l'opérateur de sécurité du site. Les indicateurs de performance classiques sont la probabilité de détection (la plus élevée possible) et la probabilité de fausse alarme (la plus faible possible)
- Analyse et décision : cette fonction centrale doit permettre de comprendre ce qui se passe et de déclencher les mesures appropriées. Elle comprend également souvent les possibilités de remontée de l'Alerte à un niveau supérieur ou l'appel de renforts.
- Intervention : la nature et la forme de l'intervention dépend de l'alerte (feu, intrusion, accident du travail…). Elle doit être la plus rapide et la plus efficace possible.
- Retour à la normale : cette fonction a pour but de pouvoir constater la fin de l'alerte en vue de revenir à l'activité normale.

Une fois l'installation terminée en place, le dispositif de sécurité passe en phase d'exploitation. Cette phase d'exploitation comprend deux états : exploitation normale et gestion des incidents.

A intervalles réguliers et à la fin de chaque incident défini comme significatif, une fois que le retour à la normale est acquis, la quatrième phase est déclenchée. Cette phase consiste à analyser les logs du système et la réaction face aux incidents afin d'identifier d'éventuels « trous dans la raquette » et de vérifier que les différentes composantes ci-dessus ont fonctionné conformément aux attentes. A l'issue de cette phase, des propositions d'amélioration sont établies en vue d'établir la nouvelle version de l'étude de sureté.

Fonctions capacitaires

La protection physique est le principal objet de ce document. Elle est traditionnellement présentée selon le modèle en couches autour du cœur à protéger et applique le principe « Barrière alarme barrière ». Concrètement, le périmètre à protéger est entourée d'une première barrière. Le périmètre est ensuite surveillé pour détecter toute intrusion. Les actifs à haute valeurs font eux l'objet d'une protection spécifique normalement encore plus difficile à passer.



La nécessité de ménager des accès (physiques et cyber) dans le périmètre crée a priori une vulnérabilité. La protection des accès nécessite donc une attention spéciale. Nous avons donc regroupé l'offre en cinq domaines capacitaires : Conception et mise en place, Protection de périmètre, Protection de zone, Gestion des accès et Exploitation. Cette répartition est parfois un peu arbitraire mais elle permet de ranger les capacités en grands domaines cohérents.

Conception et mise en place

Cette catégorie regroupe les prestations indispensables à l'obtention de la sécurité mais qui ne correspondent pas à des matériels particuliers. Il s'agit en général de tâches de fond ou de mise en place. Elles comprennent l'Audit, la modélisation, L'intégration et la Formation.

Audit et conseil

La protection de sites s'appuie sur des réglementations, des standards nationaux ou internationaux qui évoluent régulièrement. De même, les technologies et les acteurs, ainsi que les menaces et les risques, sont en évolution permanent. Tout ceci rend une connaissance approfondie de cet écosystème très complexe pour les responsables de la protection des sites. Ces derniers ont donc, le plus souvent, besoin de s'appuyer sur les conseils d'experts techniques et opérationnels pour être certain que la protection reste à la pointe de la technologie et adéquate face à l'évolution des menaces.

Modélisation et simulation

La modélisation du site à protéger permet d'avoir une cartographie complète de ce dernier ainsi que la liste des actifs à protéger. Cette modélisation permet ensuite de mener des simulations réalistes et de compiler les données d'entrées des futurs hyperviseurs.
La simulation permet de substituer à des situations réelles rarement accessibles, des situations virtuelles réalistes.
Elle a donc vocation à participer au choix du dispositif et des équipements de sécurité à mettre en place. Elle permet également de définir des procédures opérationnelles plus pertinentes.

Intégration

La conception, le déploiement et la mise en œuvre de systèmes et de solutions techniques, parfois complexes, nécessaires à la protection de sites - centres de gestion, de coordination et de contrôle compris exigent les compétences d'un intégrateur-ensemblier capable de réaliser dans les délais le système global de protection prenant compte la totalité des exigences de sécurité et de protection définies par le maître d'ouvrage.

Formation

L'efficacité des opérateurs doit être maintenue en permanence au plus haut niveau possible. Les missions, souvent difficiles techniquement, physiquement, tactiquement et mentalement, ne peuvent être exercées que par des personnels spécialement entrainés et connaissant parfaitement leur mission, les détails du site et les possibilités de leurs équipements. La formation doit donc être adaptée en permanence en fonction de l'évolution du site, des menaces et des retours d'expérience. La formation doit porter tant sur l'individu que sur les unités ainsi que sur la parfaite maitrise des situations classiques, des techniques et des matériels mis en œuvre. Ces formations peuvent être assurées dans des sites spécialement dédiés à cet effet (écoles) ou sur site.

Protection du périmètre

Cette catégorie regroupe les éléments constitutifs des barrières et de tout ce qui concourt à empêcher l'intrusion. Certaines solutions chères ou contraignantes seront réservées à la protection de sous-périmètres contenant les actifs de haute valeur.

Surveillance

La première chose à faire pour assurer la protection est de surveiller les alentours du périmètre et la zone à protéger. La détection, la reconnaissance et l'identification de vecteurs terrestres, aériens ou maritimes ainsi que d'intrus à proximité ou à l'intérieur de la zone à protéger constituent les éléments primordiaux de la chaîne de décision. Ils permettent la fourniture d'information et d'éléments nécessaires à l'intervention. Il est essentiel de pouvoir détecter, reconnaître et identifier en toutes circonstances, en tout temps et suffisamment en amont toute menace potentielle.
Les solutions optroniques doivent couvrir l'ensemble du spectre visible et thermique et sont en général associées à des capteurs de type Radar, à des solutions d'illuminations (visibles ou discrètes) ainsi qu'à des logiciels de traitement et d'analyse dotés de fonctions associées telles que la reconnaissance de patterns, la désignation d'objectifs et le suivi automatique de scènes et de vecteurs.
Les caméras complètent parfaitement les dispositifs humains qu'elles contribuent à économiser. Elles ont un coté dissuasif très intéressant et fournissent des éléments très fiables de preuve et de vérification.
La détection ne se limite cependant pas à la video. Un grand nombre de détecteurs de mouvements, de passage, de bruit et autres permettent de détecter et de localiser une éventuelle intrusion.

Clôtures et capteurs anti intrusion

Il s'agit d'assurer la protection périmétrique, dans l'objectif de dissuader retarder et, dans tous les cas, de détecter une éventuelle intrusion et de guider les flux de véhicules et de piétons vers les accès sécurisés. Cette protection peut comporter plusieurs éléments successifs et doit être réalisée avec des matériels de protection certifiés comme : grilles, grillages, concertina, murs, obstacles divers, électrification, portes blindées, barrières de rayons, fenêtres et vitres pare-balles, etc… Ces défenses passives seront bien sur équipées de divers capteurs ayant pour but de détecter une éventuelle intrusion.

La protection des actifs de haute valeur doit être particulièrement résistante pour éviter que l'intrus ait le temps de la percer avant l'arrivée de l'équipe d'intervention. Elle doit également couvrir la protection blast et balistique, sans oublier la protection électromagnétique.

Robots de surveillance

Les rondes et les missions de surveillance traditionnelles effectuées par les chiens et les agents de sécurités du site seront de plus en plus effectuées par des robots spécialisés. Ces robots pourront être terrestre (rondiers) ou aéroportés (Drones). L'utilisation de tels robots permet d'éviter d'exposer inutilement la vie des agents, d'augmenter significativement la fréquence des passages, d'assurer des rondes permanentes sans mobiliser d'effectifs et de réserver ces derniers aux missions d'intervention.

Protection des voies d'accès physiques

Les voies d'accès physiques constituent un point de vulnérabilité particulier car il n'est pas possible de les protéger par des systèmes fixes. Elles doivent donc être équipées de divers systèmes (barrières, portails, plots, herses…) à la fois capable de permettre le passage et de fournir très rapidement une résistance élevée à des attaques puissantes telles que des camions béliers.

Ces défenses seront en général doublées de manière à constituer un sas qui pourra permettre les opérations de contrôle d'accès avec une sécurité relative.

Protection de la zone

La surveillance de la zone terrestre ou aérienne est la seconde ligne de défense. Le but est de détecter et localiser tout intrus qui aurait réussi à franchir la protection périmétrique. Mais la protection de la zone ne s'arrête pas à la détection. Elle comprend aussi le suivi des visiteurs entrés officiellement, la reconnaissance de comportements anormaux et tout un ensemble de défenses passives et de pièges permettant de retarder l'intrus. Elle intègre enfin un ensemble de capteurs permettant de détecter des phénomènes risquant de mettre en péril l'installation (fuite, feux, etc…).

Senseurs d'état

Cette catégorie de senseurs regroupe de multiples capteurs de données. Les plus classiques sont les détecteurs de fumée, de chaleur, de fuite de liquide, de gaz, de vibrations, mais aussi de lumière ambiante, d'humidité, de vent, etc ... Dans cette catégorie figurent aussi les indicateurs de l'état des systèmes (pannes d'équipement). Ces senseurs permettent d'assurer une veille permanente sans intervention humaine et dans des endroits potentiellement inoccupés, cachés ou difficiles d'accès (égoûts, batiments techniques…). Ils fournissent au central des informations très diverses qui lui permettent de prendre de meilleures décisions mieux adaptées au contexte. Ils permettent enfin de réduire significativement la maintenance en suscitant des interventions à bon escient.
Ce segment devrait connaitre des bouleversements importants dans un futur proche avec la généralisation de l'Internet des objets.

Analyse vidéo et fusion de capteurs

Ces fonctions devraient bénéficier considérablement des avancées fournies par le deep learning. Ces technologies interviennent à deux niveaux. En temps réel, elles permettent d'analyser les données issues des capteurs pour reconnaitre des situations d'alerte comme des comportements anormaux de visiteurs ou une tentative d'intrusion. Mais elles permettent également de mener des analyses de fond ce qui améliore considérablement la détection de menaces latentes et la détection des signaux faibles.
Dans le futur, cette fonction devrait devenir une couche d'abstraction et d'aide à la décision permettant de ne plus raisonner en termes de données ou de capteurs mais en termes d'événements, tels qu'un incident d'exploitation ou une intrusion. Une telle approche permettra d'intégrer dans le système une logique métier qui aidera les opérateurs en cas d'évènement en leur proposant des décisions et des plans de réaction.

Pièges

Les pièges ont pour but de compliquer la tâche d'un éventuel intrus en le forçant à la prudence et en le ralentissant voire en le neutralisant. Les pièges peuvent êtres de diverses natures (vulnérants, immobilisants, neutralisants…). Ils peuvent être activés en permanence ou à la demande en fonction des circonstances et leur déclenchement doit donner lieu à une alerte au central.

Identification et contrôle d'accès

Cette catégorie regroupe les moyens d'identification, de délivrance d'accès et d'inspection des personnes, des véhicules et des biens qui sollicitent une entrée sur le site. Le but de ces fonctions est de permettre un accès rapide (car une perte de temps génère des pertes d'efficacité opérationnelle et une mauvaise image) tout en garantissant que les entrants ne présentent pas de risque de sécurité.

Contrôle d'accès des personnes

Le contrôle d'accès dans le cadre de la protection de sites permet de s'assurer que les personnes et leurs éventuels véhicules sont autorisés et habilités à accéder au site. Ce contrôle doit porter sur l'ensemble des personnels entrant sur le site y compris les personnels du site et des équipes de sécurité. Chaque entrant correspond à un profil qui lui donne des autorisations particulières. L'affectation à des profils aux prérogatives étendues est en général obtenue après une vérification des antécédents auprès de services internes, privés ou régaliens. La gestion des visiteurs peut demander des capacités de vérification de la validité des documents d'identité ou d'accréditation.

Biométrie

La biométrie permet d'accroître la sécurisation des accès non seulement à des locaux mais aussi à des stations informatiques et aux dossiers et fichiers présents sur ces dernières. Il existe de nombreux systèmes biométriques pour le contrôle d'accès avec ou sans contact physique.
La biométrie avec contact physique comprend (entre autres) la reconnaissance d'empreinte digitale, de la morphologie de la main et du réseau veineux de la rétine ou de la main. La biométrie sans contact inclut la reconnaissance faciale et d'iris, la reconnaissance vocale, et la biométrie comportementale.

Contrôle et inspection des véhicules

Le contrôle d'accès des véhicules repose sur des technologies adjointes aux véhicules comme la reconnaissance des plaques d'immatriculation, des vignettes, des badge RFID, etc.…
L'inspection des véhicules vise à vérifier que ni le véhicule ni sa cargaison ne présente un danger pour la sécurité du site et/ou si cette dangerosité ne peut être évitée (transport de matières inflammables par exemple) à prendre les mesures qui s'imposent. La traditionnelle inspection visuelle est maintenant utilement complété par de nombreuses technologies permettant de détecter la présence de menaces les plus diverses et/ou d'intrus à bord.

Détection armes et explosifs

La détection de matériels illégaux fixes ou mobiles (NRBC-E, armes…) est essentielle pour la protection des sites et doit s'inscrire dans le respect de la réglementation. Au traditionnel scanner viennent s'ajouter de nouveaux moyens de détection permettant de détecter et de caractériser les matériels illégaux à distance et rapidement.

Exploitation

Cette catégorie comprend les réseaux de communication, les centres de commandement mais aussi les moyens d'autoprotection du système et les dispositifs d'alerte.

Communications et coopération

Les moyens de communication entre le central et les équipes de surveillance et/ou d'intervention sont un point majeur d'un projet de protection de site. Ils doivent permettre de transmettre les informations nécessaires à l'évaluation de la situation, à la mise en œuvre des différents moyens de surveillance, à la détection et l'alerte tant vers les forces opérationnelles responsables de la protection du site que vers les autorités de Police ou de secours.
Ils peuvent être redondants, autonomes et mobiles afin de pouvoir garantir une permanence des liaisons, quelle que soit l'évolution de la situation et de l'état des réseaux de télécommunications civils. Il est fondamental que le réseau soit efficace, rapide, sûr et permette d'acheminer la voix, les données et la vidéo, dans les deux sens, sans risque de délai de transmission, de fluctuation ou de perte de données. L'extensibilité doit être prise en compte pour permettre une montée en puissance au fur et à mesure que de nouveaux besoins et usages apparaitront.

Hypervision

Les systèmes d'hypervision et de commandement ont pour objet la tenue de situation de la sécurité globale du site, l'aide à la décision et la coordination de la réponse.
Ils centralisent en temps réel les alertes issues des différents moyens de détection, de surveillance et de contrôle, pilotent les moyens techniques de levée de doute et permettent de coordonner les interventions via les systèmes de communication et de suivi.
Ils permettent également de rendre compte à la hiérarchie, le cas échéant de faciliter l'intervention, d'aleter éventuellement les renforts ou des forces de l'ordre, et d'effectuer des retours d'expérience via le rejeu des événements.
Le Centre de Commandement n'est cependant pas qu'une question de technique. Les équipes opérationnelles doivent y passer de longues heures dans une atmosphère souvent stressée. Il est donc fondamental d'accorder un soin particulier à l'ergonomie, aux interfaces et plus généralement à la qualité de vie des opérateurs.

Protection de l'information

La protection de l'information et le contrôle des accès réseaux doivent être de tout premier ordre pour assurer l'intégrité des systèmes. Pour un malfaiteur décidé, il est plus simple de créer le chaos dans une installation en déclenchant de multiples fausses alarmes, ou en saturant les réseaux que de s'embêter à créer de multiples incidents dans le monde physique. La cyber sécurité ne se cantonne pas aux systèmes de surveillance mais à tous les systèmes et automates de l'installation. Il est en effet possible de déclencher par attaque cyber des dysfonctionnements des installations pouvant dans certains cas aller jusqu'à la destruction de pièces essentielles voire de l'installation entière.

Dispositifs d'alerte

L'alerte peut être très visible ou au contraire discrète. L'alerte publique (alarme, sirène, etc..) a l'avantage de compliquer l'action de l'intrus, de le déstabiliser, voire de le pousser à fuir. A côté de la traditionnelle sirène, d'autres technologies permettent de moduler les alertes en informant les personnels présents des dangers potentiels et des consignes à appliquer. L'alerte discrète permet d'augmenter les chances d'interception mais augmente la durée de l'intrusion et sa gravité potentielle.

Index

Entreprises	Audit et conseil	Modélisation et simulation	Intégration	Formation	Surveillance	Clôtures et capteurs anti intrusion	Robots de surveillance	Protection des voies d'accès	Senseurs d'état	Analyse vidéo et fusion de capteurs	Pièges	Contrôle d'accès des personnes	Biométrie	Contrôle et inspection des véhicules	Détection armes et explosifs	Communications et coopération	Hypervision	Protection de l'information	Dispositifs d'alerte	PAGE
AERACCESS			●		●	●	●			●									●	10
AIR-LYNX					●	●	●	●	●	●		●				●	●	●	●	11
ALTHING	●																			12
AMCO LES ESCAMOTABLES								●												13
APILOG AUTOMATION					●	●		●				●	●		●		●	●		14
ARDANTI DEFENSE	●	●	●		●		●	●		●							●			15
BERTIN TECHNOLOGIES					●					●								●		16
CEGELEC DEFENSE			●		●	●		●	●	●		●				●	●	●	●	17
CERBAIR					●	●				●									●	18
CILAS					●															19
CIVI.POL CONSEIL	●																			20
DEVERYWARE					●											●			●	21
ECA GROUP							●													22
EGIDIUM TECHNOLOGIES		●								●							●			23
ENGIE INEO	●		●	●	●	●			●	●		●	●	●		●	●	●	●	24
EVITECH					●	●		●	●	●							●		●	25
EXAVISION	●		●	●	●					●							●			26
GEOS	●		●	●												●				27
GUNNEBO FRANCE			●		●	●		●		●		●	●				●		●	28
HGH INFRARED SYSTEMS					●	●				●							●			29
GROUPE SDS/SDS GROUP					●		●	●	●			●			●					30
KOPP	●		●		●			●				●	●	●			●			31
LACROIX DEFENSE					●	●		●		●										32
LUCEOR					●		●									●				33
MIRION TECHNOLOGIES					●			●				●		●	●				●	34
NUANCES TECHNOLOGIES	●		●	●	●	●			●		●								●	35
PHOTONIS TECHNOLOGIES					●	●	●			●		●	●							36
PRONERGY					●		●													37
S2E CONSULTING	●		●																	38
SPARTAN-MLE		●		●																39
STERBLUE						●														40
STORMSHIELD																●	●	●	●	41
SYSNAV					●					●		●		●					●	42
THALES	●		●	●	●	●		●		●		●		●		●	●	●	●	43
TEHTRIS																		●		44
URBACO	●			●		●		●									●			45

Shehzaad CALLACHAND
CEO
Mail : callachand.shehzaad@aeraccess.com
Tél. : 01 60 85 81 03

AERACCESS
Base Aérienne 217 - 91220 Brétigny-sur-Orge

www.aeraccess.com

aeraccess®
airborne engineering research

Airborne Engineering Research
Solutions de drones pour la sécurité défense.

La solution autonome de sécurité périmétrique

AERACCESS a mis au point avec ses différents partenaires une solution unique de sécurité périmétrique par drone. En appui aérien, il vient compléter la bulle tactique en tant qu'objet connecté. En complément des équipes et patrouilles terrestres, le drone de sécurité et de surveillance est un outil efficace et redoutable pour renforcer la protection de site sensible, surtout quand il s'agit de plusieurs hectares.

Compatible avec les systèmes de surveillances existantes, et facilement interfaçable avec les centres de commandement, le drone permet d'effectuer une levée de doute en cas d'alerte ou d'intrusion. Il s'interface de manière intelligente avec les capteurs déjà installés (radars, capteurs acoustiques, caméra jour/nuit, …) et permet à l'utilisateur de se rendre sur la zone d'alerte en quelques minutes.

Le système est composé d'un drone intégré dans une base autonome, pouvant fonctionner par capteurs solaires , et capable de recharger ses batteries de manière autonome. La solution peut ainsi être déployer 24/24 7/7 sur site, ou même être commandé à distance par réseau IP.

Equipé d'algorithmes intelligents, le drone détecte automatiquement les anomalies, et ne nécessite donc pas la présence d'un opérateur pour visionner les images.

Bénéfices de la solution de surveillance de site par drone :

- Utilisation 24/24 7/7
- Un drone tous temps pour des missions de surveillance et de sécurité
- Décollage et atterrissage autonome et recharge des batteries
- Intelligence Artificielle pour automatiser les détections d'anomalies et d'intrusions
- Multicapteurs (EOIR, Nocturn, …)
- Intégration dans centre de commandement
- IHM simple d'utilisation et interfaçage avec l'existant

Philippe SAENZ
CEO
Mail : philippe.saenz@air-lynx.com
Tél. : + 33 9 814 434 646

AIR-LYNX
1, avenue de l'Atlantique - 91940 Les Ulis

www.air-lynx.com

Mieux protéger son site grâce à un réseau privé Haut Débit 4G LTE.

Pas de protection efficace de sites sensibles, qu'ils soient militaires ou industriels, sans une connectivité réseau ad-hoc. En complément des technologies actuelles (analogique, numériques, TETRA) ou en remplacement de celles-ci, la technologie 4G LTE, standardisée, est une option intéressante à considérer, pour ses qualités. Elle apporte en effet haut débit et sécurité, deux caractéristiques essentielles. Le haut débit permet par exemple d'envisager des échanges d'images ou de vidéos sans problèmes de débit, et les mécanismes de sécurité garantissent la protection des données échangées.

Une solution simple et résiliente

Air-Lynx, constructeur de réseau radio 4G LTE privé, propose une solution originale sur le marché : un réseau fixe 4G LTE complet, sécurisé, et déployable très facilement. Tout ce qui est nécessaire au déploiement du réseau privé (cœur de réseau, station de base eNodeB, serveurs associés) tient dans un seul multi-rack. Il peut être déployé sur un ou plusieurs sites.

La solution a d'autres atouts : une grande résilience, qui apporte sécurité et fiabilité au réseau, une grande souplesse en fréquences, qui permet de s'adapter aux besoins et possibilités des utilisateurs, en fonction des réglementations et autorisations et une facilité d'exploitation. Enfin, le fait d'être un réseau privé garantit un accès à la ressource à tout moment. Ce réseau peut se connecter à tous types de capteurs à la fois avec du LTE haut débit (caméras, drones, robots…) et bas débit avec le LTE-M ou le NB-iOT.

Air-Lynx a également développé une version nomade de son réseau et une application, baptisée CALM, qui comprend tous les services de la PMR : Push-To-Talk, Vidéo MultiCast (eMBMS), échanges de fichiers, appels d'urgence, etc, utiles à tous les agents de surveillance, de sécurité ou d'intervention. La solution peut-être complétée par des terminaux 4G LTE standards ou durcis comme des smartphones, des tablettes, modems, tous pouvant être également sécurisés.

Des passerelles pour préserver la continuité avec l'existant

Une autre grande force de la solution Air-Lynx, est son interopérabilité avec les réseaux existants. La société propose en effet les passerelles nécessaires (GSM-R, TETRA. etc..) qui permet de faire le lien entre les différents réseaux.

Quelques atouts pour les sites sensibles :

- Disponibilité instantanée de la ressource
- Gestion de nombreux capteurs connectés en haut débit ou bas débit
- Surveillance par caméras fixes ou mobiles via des drones ou robots
- Transmission dans les deux sens de vidéos haute définition et stockage dans le réseau
- Capacité à situer les agents par leur géo-positionnement
- Disponibilité de toutes les fonctionnalités radio : PTT, alarme, préemption, groupes fermés d'usagers,…
- Résilience et Sécurité, avec Chiffrement de bout en bout des communications

Guillaume FARDE
Directeur associé
Mail : contact@althing.fr
Tél. : 01 58 39 30 25

www.althing.fr

ALTHING

SÉCURITÉ & INTELLIGENCE ÉCONOMIQUE

Cabinet de conseil en sûreté et en intelligence économique.

Le cabinet ALTHING sécurité et intelligence économique conseille ses clients dans les domaines du management des risques et de la collecte d'information stratégique.

Nos équipes, formées dans les meilleurs établissements français, ont bâti une approche renouvelée du conseil en sûreté dont les activités d'intelligence économique sont un prolongement naturel. Elles travaillent dans un souci d'éthique et d'efficacité, en associant leurs clients à toutes les étapes stratégiques de leur mission, du diagnostic aux préconisations.

Une politique de sûreté et de prévention des risques inadaptée peut, en cas d'incident, durablement compromettre la sécurité des biens et des personnes. Afin d'assurer leur protection, le cabinet ALTHING accompagne ses clients dans la définition d'un schéma directeur de sûreté.

De même, équiper un espace ou une infrastructure de systèmes de sécurité (contrôles d'accès, vidéo) est une décision lourde. Parfois coûteux, le déploiement de ces systèmes doit répondre à un principe de proportionnalité entre les buts recherchés, les procédés disponibles et les moyens alloués. La rationalisation de la dépense, qu'elle soit publique ou privée, est une exigence de première importance. Quelle que soit la qualification juridique de l'espace à protéger à l'aide de systèmes, le cabinet ALTHING assure l'assistance à maîtrise d'ouvrage et/ou la maîtrise d'œuvre de manière à répondre à toutes les exigences du décisionnaire. Disposant d'ingénieurs, de techniciens et de juristes spécialistes des questions de sûreté, le cabinet ALTHING fournit des dossiers de qualité, respectueux des contraintes juridiques, techniques et financières.

Nos collaborateurs sont ainsi sollicités par les directeurs sûreté pour

La réalisation de diagnostics sûreté opérationnels :
- segmentation des risques par typologies ;
- évaluation de l'exposition aux risques des personnes et des biens ;
- analyse prospective.

La définition d'une stratégie globale de sécurité :
- élaboration de contre-mesures de sûreté adaptées à l'environnement ;
- identification de leviers d'optimisation de la gestion des ressources (humaines, techniques et financières) ;
- mise en place d'un plan de continuité de l'activité en cas de crise.

L'assistance technique a la mise en œuvre des contre-mesures de sûreté :
- rédaction de cahiers des clauses techniques dans le cadre d'appels d'offres ou de procédures d'achats ;
- aide à la sélection des prestataires ;
- suivi de chantier.

Jérome MUROLO
Directeur commercial
Mail : j.murolo@amco.fr
Mobile : +33 6 20 88 81 66

AMCO LES ESCAMOTABLES
ZI Montagne de l'Aspre -
20, Avenue de l'Aspre - 30150 Roquemaure
Tél. : + 33 4 66 33 25 70 - Fax :+33 4 66 33 25 71

www.amco.fr

Sécurisation périmétrique - Protection contre les véhicules béliers.

AMCO Les Escamotables, société Française, conçoit, fabrique et distribue des systèmes de barrages routiers

- Bornes escamotables, fixes, obstacles escamotables et barrières.
- Depuis de nombreuses années, AMCO Les Escamotables propose une gamme complète de produits anti intrusion et anti terrorisme certifiés par crash test.

Conçus pour contrôler et sécuriser les accès véhicules, les produits AMCO Les Escamotables sont parmi les plus efficace et les plus rapide à mettre en œuvre.

La gamme anti-terrorisme AMCO Les Escamotables répond aux normes européennes et Américaines les plus exigeantes en termes de défense contre tout type de véhicule :

- IWA14-1, CWA 16221, PAS 68, ASTM F2656-07 (K12, K8, K4 selon DOS STD-02.01)

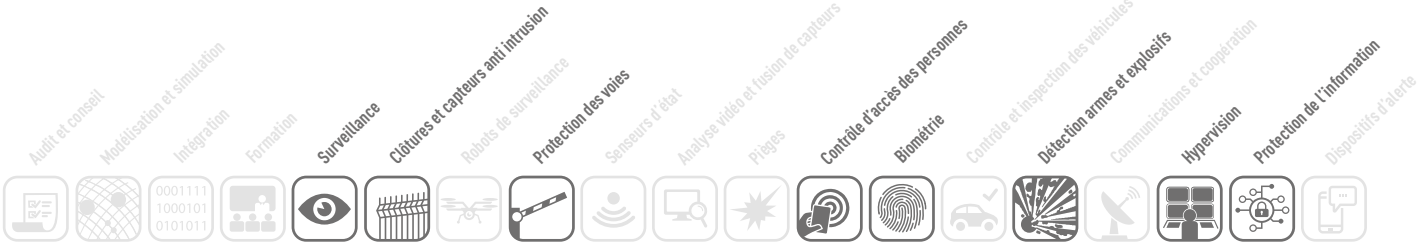
Capable de stopper des véhicules de 2T lancés à 136 km/h, jusqu'à des camions lancés à 80 km/h, les produits de sécurité AMCO Les Escamotables sont testés et certifiés par un laboratoire d'essais indépendant, agréé COFRAC (Comité Français d'Accréditation).

La majorité des produits subissent deux crash tests successifs et restent en état de fonctionnement.

AMCO Les Escamotables intervient dans tout les domaines où le besoin de sécurité est croissant :

- Ambassade, bases militaires, sites de stockage sensibles, sites SEVESO, concessions, centre forts, centre pénitenciers…

De la conception du projet jusqu'à l'installation et le maintien en conditions opérationnelles des systèmes AMCO Les Escamotables met à votre disposition son expérience et son savoir faire.



Pascal CONSENT
Responsable Activité Sureté
Mail : pascal.consent@apilog.com
Tél. : +33 6 43 80 68 35

APILOG AUTOMATION
3 rue Galvani - 91300 Massy

wwww.apilog.com

Notre expertise à votre service - Sureté, Contrôle Commande, Hypervision.

APILOG Automation, filiale du groupe GGC, est expert dans l'intégration de systèmes de sureté et d'automatismes

Spécialiste en sureté, automatismes, régulation, contrôle commande, **expertise et audit**, supervision et **monitoring**, pupitre de gestion d'accès, nous vous proposons des solutions techniques évolutives. APILOG Automation dispose ainsi d'un grand retour d'expérience et d'un choix produits pertinents et certifiés.

Dotée de fortes compétences techniques, APILOG Automation est en mesure de vous écouter, conseiller et de réaliser chacune des étapes de votre projet

Analyses, études de vulnérabilité, développements de concept de sureté :

- Protection périphérique et périmétrique, systèmes anti-franchissement, gestion des obstacles piétons et véhicules, détection-intrusion, contrôle des accès, vidéoprotection, système de communication audio et vidéo, biométrie et gestion des visiteurs.

Le développements d'automatismes :

- Armoires de commandes et pilotages, **pupitres PGE-PCS** et systèmes d'alerte et d'évacuation.
- Le suivi de chantiers par nos experts, tests, mise en service et les formations certifiant les exploitants.

Afin de répondre de la façon la plus complète aux attentes et besoins de nos clients, nos équipes peuvent également effectuer des **développements spécifiques** grâce à notre **R&D**. APILOG Automation permet le maintien en condition opérationnelle **(Mco)** et le maintien en condition de sûreté **(Mcs)** des sites.

Nous bâtissons les architectures de réseaux de communication répondant à vos besoins, déployons les automatismes répartis et centralisons l'ensemble des données vers **un système de supervision** ou **d'hypervision** adapté aux installations distantes de demain.

Nos clients apprécient la **dimension humaine** d'APILOG Automation, sa **réactivité**, sa **flexibilité** ainsi que ses **savoir-faire techniques reconnus**.

François ARDANT
Directeur
Mail : francois.ardant@ardanti.com
Tél. : + 33 (0)1 40 13 04 05

ARDANTI DÉFENSE
3, rue Geoffroy Marie - 75009 Paris - France

www.ardanti-defense.com

3DProtecSites - Renforcer la protection physique des sites sensibles par l'audit des vulnérabilités en simulation, l'optimisation des coûts et du déploiement, la simplification de la conduite, et l'utilisation de moyens robotiques.

Besoin

Pour améliorer la sécurité physique des sites les opérateurs doivent connaitre le niveau de protection de leurs installations et leurs vulnérabilités. Cette évaluation se heurte à la complexité de se représenter la multitude de combinaisons : intrusions possibles / terrain / dispositifs de protection. La connaissance réelle des vulnérabilités étant peu fiable, les renforcements apportés s'avèrent coûteux et inefficaces.

Solution innovante 3DProtecSites

Issue de plusieurs années de travaux d'Ardanti Défense en partenariat avec des laboratoires de recherche, 3DProtecSites permet de mesurer puis d'améliorer la protection des sites, en aidant à répondre à des questions telles que: quelles sont les zones vulnérables, quelle nature de menaces peut être plus néfaste, quelle est la valeur ajoutée de nouveaux moyens envisagés, comment alléger la charge financière et humaine.

3DProtecSites comprend plusieurs modules :

- A/ Création d'une **maquette numérique 3D** de l'ensemble de la zone. Cette maquette 3D orienté protection est produite, précise et parfaitement à jour.
- B/ **Simulation des moyens** existants ou envisagés, positionnés sur la maquette numérique: capteurs, effecteurs, dispositifs, procédures, moyens humains... Via une base de données de dispositifs de surveillance et protection et de leurs performances.
- C/ **Aide à la conception du plan de déploiement**, par la confrontation simulée : intrusions / terrain / dispositif, prenant en compte des conditions spécifiques d'environnement. La pose de moyens permanent ou capteurs déposés est simplifiée.
- D/ **Hypervision et conduite simplifiée de la protection - surveillance**, par un système fusionnant les moyens techniques et humains sur une visualisation terrain unifiée. Cet outil de Commande & Contrôle (C2) peut être fixe ou mobile pour équiper les patrouilles.
- E/ **Robotique de patrouille autonome**, permettant des rondes aléatoires tout temps renforçant le dispositif.

Ardanti Défense PME innovante indépendante dédiée à la protection des sites et des technologies associées, travaille au profit des forces et des industriels de la Défense (Exensor , Thales, Nexter…) et du domaine civil.

Juliette DUAULT
Responsable Communication
Mail : juliette.duault@cnim.com
Tél. : +33 1 39 30 60 00

BERTIN TECHNOLOGIES
10 bis avenue Ampère -
78180 Montigny Le Bretonneux

www.bertin.fr

Bertin, société du groupe CNIM, propose une gamme complète d'équipements et de systèmes conçus et développés pour la protection des sites et zones sensibles, des personnes et des biens.

Détection des menaces NRBC

Bertin propose une offre complète de solutions propriétaires pour la détection et l'identification précoce de menaces NRBC.

Chimique : adaptée à une surveillance et protection jour / nuit contre les menaces chimiques (agents de guerre, composés industriels toxiques), la caméra Second Sight® MS assure la détection, l'identification et la visualisation en temps réel d'un nuage de gaz, à distance jusqu'à 5 km. Une version véhicule est disponible pour des missions de surveillance 360°.

Biologique : Coriolis® RECON est un biocollecteur d'air robuste dédié aux équipes NRBC ou de premiers secours, développé pour des environnements difficiles et la surveillance de points sensibles. Sa collecte liquide permet d'obtenir une réponse rapide et d'identifier la menace biologique.

Radiologique & nucléaire : la sonde autonome GammaTRACER Spider est une solution de surveillance radiologique innovante conçue pour couvrir les besoins des primo-intervenants en scénario d'urgence. Dédiée à la mesure, l'enregistrement et la transmission des débits de dose y, elle procure des données fiables et peut être installée n'importe où grâce à son système de déploiement rapide.

Observation et surveillance

Bertin fournit et développe des solutions optroniques pour détecter, reconnaître et identifier des cibles et menaces :

- PeriSight® est une solution de vision périphérique améliorée pour véhicules militaires. Entièrement modulable et compatible tous réseaux de bords, elle permet une surveillance à 360° jour/nuit, afin d'améliorer l'appréhension de l'environnement et des situations de terrain.
- FusionSight® est un monoculaire portable qui fournit des images numériques couleur Bas Niveaux de Lumière (BNL) et des images thermiques, pour un usage séparé ou fusionné. Cet équipement ergonomique est directement inspiré par les besoins des utilisateurs.

Cybersécurité

Éprouvées pour des besoins élevés de défense, les solutions de Bertin protègent les systèmes d'information sensibles et les infrastructures critiques. Basée sur une technologie gouvernementale certifiée CC-EAL 5+, CrossinG® est une passerelle de sécurisation des interconnexions entre systèmes ou réseaux de différents de niveaux de sensibilité.

MediaCentric® est une plateforme de cyber intelligence dotée de capacités d'acquisition multi-sources dont dark web et d'analyse en profondeur permettant la détection de signaux faibles et l'anticipation des menaces.

Gilles LABORDE
Président
Mail : defense.toulouse@cegelec.com
Tél. : +33 5 62 87 00 00

CEGELEC DÉFENSE
1, rond-point du Général Eisenhower -
31106 Toulouse cedex 1 - France

www.defense.cegelec.com

VINCI Energies - Naissance sous la tutelle de CEGELEC Défense d'un « Groupement Défense » qui fédère CEGELEC Défense à Toulouse, SANTERNE Aéronautique & Défense à Arras, et CEGELEC Défense & Naval Sud-Est Infrastructures Militaires à Toulon.

La protection des sites sensibles constitue un axe historique et stratégique de développement pour le groupement Défense de Vinci Energies

Ce groupement rassemble de nombreuses capacités et compétences industrielles complémentaires adressant l'ensemble du besoin face à tous les risques et menaces :

- Intégration globale et déploiement de systèmes de protection physiques et logiques des infrastructures et des réseaux (y compris protection cinétique, anti-sismique, collective NRBC et electromagnétique), travaux multitechniques sur sites ;
- Sécurité et surveillance, prévention des intrusions, contrôle d'accès, vidéo surveillance interne et externe des infrastructures sensibles et points d'importance vitale tels que les bases militaires, aériennes, navales et stratégiques, les sites logistiques, les plateformes dédiées ;
- Maintien en condition opérationnelle (MCO), le maintien en conditions de sécurité (MCS) et la garantie de disponibilité des systèmes de sécurité et de protection grâce à un savoir-faire multiple et à un large spectre de compétences en ingénierie et management de projet ;
- Maintenance globale, corrective et préventive, des équipements et sous-ensembles constituant les système physiques et logiques de sécurité et de protection.

Avec ce groupement, CEGELEC Défense fédère un réseau d'entreprises au service de ses clients Défense et sécurité depuis 50 ans qu'elle accompagne tout au long du cycle de vie de leurs projets, locaux, multi-sites ou à l'international.

A cette expertise d'intégrateur et d'ensemblier multi technique s'ajoute la capacité de CEGELEC Défense à mobiliser rapidement des équipes performantes dans la plupart des zones sensibles du globe, pour les besoins spécifiques de ses clients, confortée par la densité unique du Groupe VINCI.

VINCI Energies, est un groupe international réalisant un chiffre d'affaires de 9 Mds€ et employant 64 000 collaborateurs à travers le monde.

Lucas LE BELL
Directeur Général
Mail : lucas.lebell@cerbair.com
Tél. : +33.1.71.18.20.32

CERBAIR
48, rue de la Chaussée d'Antin - 75009 Paris

www.cerbair.com

CERBAIR

Solution Complète Anti-Drone
Détecter + Identifier + Neutraliser.

Quelles menaces sur mon site ?

- Aujourd'hui, les drones s'affranchissent complètement des systèmes de sécurité existants : barrières, grillages et contrôles d'accès sont devenus parfaitement inutiles pour lutter contre ces engins.
- Les drones fragilisent donc désormais la sécurité de tous les sites sensibles et font peser sur eux des risques d'espionnage, de contrebande, de collision ou même d'attaque terroriste.
- 10 millions de drones en circulation aujourd'hui, 50 millions d'ici 2025... **La sécurité doit désormais être pensée en trois dimensions**.

Qu'est-ce que CERBAIR ?

Solution complète anti-drone, CERBAIR vous permet de détecter, identifier et neutraliser les drones malveillants avant que ceux-ci ne commettent leur méfait.

Issues de la recherche française, nos technologies d'analyse radiofréquence et de reconnaissance d'image vous protègent contre tous les drones civils.

Enfin, notre système d'alerte et de levée de doute en temps réel vous permet de neutraliser le pouvoir de nuisance des intrus indésirables via le recours à diverses contremesures telles que le hacking, le brouillage intelligent ou le lance-filet.

Notre solution

1 - Détecter : nous combinons plusieurs capteurs Radiofréquences et Optiques afin d'adapter notre solution à votre niveau de risque, à la configuration de votre site ainsi qu'à votre budget.

2 - Identifier : notre approche multi-capteurs couplée à nos algorithmes de traitement assure la détection des intrusions tout en minimisant les fausses alertes

- Suivi optique de la trajectoire du drone
- Levée de doute (visuel HD du drone, enregistrement vidéo de l'intrusion)
- Reconnaissance du type de modèle par signature radiofréquence

3 - Neutraliser : apportez la réponse la plus adaptée à la menace lorsqu'elle se présente

- Contre-mesures actives: neutraliser le drone en forçant son atterrissage par hacking et/ou brouillage intelligent (commandes de vol et géolocalisation) ou capture à l'aide d'un lance filet.
- Actions passives : mettre à l'abri des personnes, interrompre une conversation, déclencher une fouille du site, bloquer la vue du drone etc…
- Paramétrez vos alertes pour une intervention rapide, adaptée (visuelle, sonore, SMS etc…) et intégrée à votre architecture logicielle par notre API.

Jean-Christophe DIAS
Responsable commercial
Mail : dias@cilas.com
Tél. : +33 (0)2 38 64 41 26

CILAS
8, avenue Buffon - CS 16319 -
45063 Orléans Cedex 2

www.cilas.com

cilas
arianeGROUP

Grâce a ses 50 ans d'expertise, CILAS demeure à la pointe d'innovation laser. CILAS développe, industrialise et fournit des produits de haute qualité et des solutions pour les domaines de la défense et la sécurité.

Nos principaux produits de défense et sécurité sont les désignateurs laser, les modules de désignation et télémétrie, ainsi que systèmes de détection avant tir de sniper pour la protection d'infrastructures critiques

Nos produits sont utilisés dans le monde entier, sur différentes plateformes (Air/Terre/Mer), par les forces françaises et étrangères, ainsi que par les forces de sécurité, de police, les gardes royales et présidentielles. Avec des milliers de produits en service dans plus de 30 pays, CILAS propose également tout type de maintenance et service à ses clients.

Afin de protéger des infrastructures critiques ou des zones à risques comme des bâtiments gouvernementaux, des troupes en opération ou des VIP contre des snipers, CILAS a développé un système de détection avant tir de sniper, le SLD 500. Basé sur l'effet « oeil de chat », le système émet un rayon laser invisible qui détecte et localise précisément la lunette du sniper avant que celui-ci ne tire. Le SLD 500 est également capable de détecter tout type d'optiques comme des jumelles ou des caméras.

Le système peut être contrôlé par un opérateur ou configuré en détection tout automatique pour une surveillance 24/24 avec enregistrement photo et vidéo. Lorsqu'une menace est détectée, une alarme retentie, la position exacte de la menace ainsi que sa distance sont communiquées par le système. Ces informations permettent aux équipes de contre-sniping d'agir discrètement et rapidement. Le système peut être proposé avec différentes caméras thermiques et options.

Le SLD 500 est utilisé par les forces armées ou les forces de sécurité en opération. Il faut moins de 10 minutes pour le déployer et ainsi offrir une sécurité maximale aux forces alliées pour protéger une zone de menaces indétectables.

CILAS a également développé une version Long Range (longue distance) adaptée aux environnements complexes appelée SLD 500 LR. Ce dernier est équipé d'une caméra longue distance permettant une identification visuelle claire jusqu'a 1000 m, ainsi que d'une caméra thermique longue distance pour les opérations de nuit. Le SLD 500 LR est déjà en service dans plusieurs forces de sécurité pour les rassemblements de VIP et la protection de bâtiments gouvernementaux.

Olivier VERDEIL
Adjoint du Directeur général
Mail : verdeil.o@civipol.fr
Tél. : +33 (0)1 70 64 11 96

CIVI.POL CONSEIL
9, rue Notre-Dame des Victoires - 75002 Paris

www.civipol.fr

CIVI POL
CONSEIL

Société de conseil et de service du Ministère de l'Intérieur français.

Vous souhaitez

- Tester la sécurité physique et informatique de vos infrastructures ?
- Réaliser un audit de sécurité sûreté de votre site en France ou à l'étranger ?
- Ou encore former vos responsables de sites à la gestion d'une crise ?

CIVI.POL Conseil a développé une gamme de services répondant aux principaux enjeux de sécurité et de sûreté des sites sensibles.

Notre mission

Société de conseil et de service du ministère de l'Intérieur français, nous réalisons la promotion des savoir-faire liés à la sécurité intérieure, la protection civile et la gouvernance. Nous nous appuyons sur un réseau institutionnel et des partenaires pour mobiliser des experts de haut niveau issus notamment des services du Ministère de l'Intérieur.

Notre offre d'audit de site et de conseil

Dans le cadre de la protection des sites sensibles nous réalisons notamment des missions de :

- Diagnostic- audit du niveau de sûreté
- Etude de sûreté de sites/chantiers/bureaux internationaux
- Tests d'intrusion physique et informatique (NOUVEAU)
- Rédaction et aide à la mise en oeuvre du Plan de Sécurité du site (PSE)
- Exercice annuel et tests basés sur des scénarios personnalisés
- AMO sécurité sûreté

Notre offre de formation et de sensibilisation

Etablissement sanitaire ou culturel devant suivre les instructions de votre ministère, site industriel à risque, entreprise gérant des données sensibles, nous apportons des formations à vos responsables de site et à leurs équipes :

- Formation de la direction à la gestion de crise
- Sensibilisation sur les conduites à tenir de l'incivilité à l'attaque terroriste
- Prévention, identification et gestion de la radicalisation
- Sensibilisation sur les conduites à tenir face à la radicalisation

Notre soutien aux entreprises

CIVIPOL accompagne également les entreprises dans leurs projets technologiques nécessitant une compétence liée au ministère de l'Intérieur. Vous souhaitez par exemple adapter votre logiciel aux besoins spécifiques d'une unité de police, nos experts sont à votre disposition pour vous accompagner en France et à l'international.

Delphine ARIAS-BUFFARD
Directrice des Relations institutionnelles
Mail : delphine.arias-buffard@deveryware.com
Tél. : +33 1 82 28 50 42

DEVERYWARE
43, rue Taitbout - 75009 PARIS

www.deveryware.com

DEVERYWARE
Committed to Better Security

Depuis sa création en 2003, Deveryware accompagne au quotidien les professionnels de la sûreté dans leurs missions de sécurisation des personnes et des biens.

Expert de la géolocalisation en temps réel, le groupe conçoit, développe et commercialise des solutions innovantes, en réponse aux besoins évolutifs du marché

Fort de cette expérience, le groupe s'est implanté à l'international en Espagne, en Afrique et au Canada et poursuit sa volonté d'exporter son offre à travers le monde. Sa capacité d'innovation, ses valeurs de respect de la vie privée et sa connaissance historique sur le marché de la Sécurité en font un partenaire de confiance déjà reconnu auprès de nombreux acteurs tels que les Ministères français de l'Intérieur, de la Justice, de l'Économie et des Finances. Centré sur la satisfaction clients, Deveryware déploie depuis 2012 une démarche Qualité-Environnement-Sécurité pour laquelle il a reçu une certification ISO 9001 et ISO 14001.

Depuis plus de 10 ans et pour des milliers d'utilisateurs, Deveryware fournit des réponses efficaces pour contribuer à la sécurité nationale en mettant à disposition des forces de l'ordre et de sécurité les outils de géolocalisation indispensables à la détection et la prévention des menaces ainsi qu'à l'élucidation des affaires criminelles : Deveryloc.

À travers Notico, Deveryware crée en 2016 une offre dédiée aux entreprises et aux collectivités, soucieuses de prendre part à l'évolution « Safe & Smart city ». Celle-ci vise à la fois à la sécurité et au bien-être des populations mais également à l'optimisation des coûts et des ressources dans leur organisation.

Résolument tourné vers l'avenir, Deveryware se mobilise au quotidien pour apporter les dernières innovations technologiques, fournir des solutions toujours plus perfectionnées, et proposer ainsi des services offrant une véritable valeur ajoutée au marché de la Sécurité. Un projet ambitieux et motivant que l'ensemble des équipes du groupe Deveryware placent quotidiennement au cœur de leurs préoccupations.

DEVERYLOC

Notico SAFE

Cyril PEDEHONTAA-HIAA
Directeur Commercial Export
Mail : pedehontaa.c@ecagroup.com
Tél. : +33 4 94 08 90 00

ECA GROUP
262, rue des Frères Lumière - Z.I. Toulon-Est
83130 La Garde - France

www.ecagroup.com

ECA GROUP
make sure

Robotique et systèmes intégrés pour les milieux marins, terrestres et aériens.

Reconnu pour son expertise dans la robotique, les systèmes automatisés, la simulation et les processus industriels, le Groupe ECA développe depuis 1936 des solutions technologiques innovantes et complètes pour des missions complexes dans des environnements hostiles ou fortement contraints. Son offre s'adresse à une clientèle internationale exigeante dans les secteurs de la défense, du maritime, de l'aéronautique, de la simulation, de l'industrie et de l'énergie.

Systèmes maritimes autonomes (AUV, ROV, USV)

Le groupe ECA est activement engagé dans la protection côtière et portuaire. Ses gammes de drones sous-marins (AUV / ROV) et de surface (USV) sont utilisées par de nombreuses marines dans le monde entier. Ses solutions robotiques navales ont des applications civiles et militaires, dans le domaine de la protection des ports, de l'océanographie, de l'hydrographie, de la surveillance offshore et de la lutte contre les mines sous-marines.

Récemment, le groupe ECA a développé un système intégré de protection d'infrastructures critiques (UNCRYSIS), une solution modulaire combinant des équipements classiques fixes (Radar, EOD & Sonar) et des plates-formes autonomes (UAV, USV & UUV) équipées de capteurs, le tout sous le contrôle d'un système d'information centralisé. Ce système utilise des technologies éprouvées pour analyser en temps réel la situation globale d'une manière simple et complète permettant une réponse rapide et efficace aux situations les plus exigeantes.

Véhicules terrestres autonomes (UGV)

Le groupe ECA conçoit et produit des solutions pour la lutte contre le terrorisme, la contre-insurrection ou la répression permettant de détecter et vaincre les menaces IEDD et CBRN. Le groupe ECA fournit une gamme complète de drones terrestres (UGV) capables de mener à bien des missions militaires et civiles. Ils sont conçus pour opérer en zones confinées et disponibles en plusieurs tailles : du petit UGV Cobra MK2 E aux plus grands tels que Cameleon E et Iguana E.

Véhicules aériens autonomes (UAV)

Pour la surveillance aérienne, le groupe ECA propose des drones aériens (UAV) capables de mener des missions de renseignement, de surveillance, d'acquisition et de reconnaissance d'objectifs (ISTAR). Ils peuvent être utilisés de manière autonome ou en captif pour les missions permanentes. Le groupe a également développé le « Paradrone », un UAV pour la neutralisation des drones malveillants. Les systèmes UAV et UGV du groupe ECA sont collaboratifs.

Pierre-Yves LE GUEN
CMO
Mail : pierre-yves.leguen@egidium-technologies.com
Tél. : +33 1 77 93 21 27

EGIDIUM TECHNOLOGIES
86, rue de Paris - 91400 Orsay France

www.egidium-technologies.com

egidium TECHNOLOGIES
La sécurité dans toutes ses dimensions

La supervision unifiée intelligente pour les PC Sécurité des sites sensibles.

Egidium fournit des solutions logicielles d'hypervision pour les postes de commandement de la sécurité des sites sensibles, ouverts ou non au public (sites industriels, gouvernementaux, aéroports, parcs d'expositions, enceintes sportives...). Créée en 2009, Egidium compte parmi ses références le Stade de France, le CEA, EDF, le Ministère de la Défense, Paris Aéroports ainsi que de grands événements comme la COP21, le Salon du Bourget et Eurosatory.

Au-delà de l'hypervision, la tenue de situation pour comprendre et réagir vite

Notre solution Smart Shield™, dédiée au pilotage global de la sécurité des sites à accès contrôlé, s'appuie sur une maquette numérique 3D du site. Elle met ainsi en évidence de manière réaliste la localisation des alertes et des capteurs mobilisés.

Smart Shield™ offre dans une interface utilisateur unifiée l'information essentielle des dispositifs de sécurité, afin de permettre une tenue de situation de tous les instants. Parmi les fonctionnalités disponibles de Smart Shield™ :

- Levée de doute vidéo automatique, investigation vidéo, suivi d'intrus ;
- Gestion des alarmes et des incidents, aide à la décision et au suivi des procédures ;
- Main courante numérique et tableau de bord ;
- Gestion du dispositif humain avec géolocalisation des agents de sécurité ;
- Fonctions mobiles synchronisées avec le PC Sécurité ;
- Édition tactique pour les exercices et situations de crise.

Un middleware qui s'adapte à l'évolution continue du dispositif de sécurité

Smart Shield™ repose sur le middleware d'hypervision ISAP (« Integrated Security Automation Platform »). ISAP fusionne les données de tous types de capteurs et systèmes de sécurité. Ses principales caractéristiques :

- Compatible tous capteurs et objets connectés de sécurité (IoT) ;
- Connectable à l'existant comme aux systèmes les plus récents, qu'il s'agisse de vidéo, contrôle d'accès, détection d'intrusion, sécurité incendie, détection de matières dangereuses, PMR, géolocalisation, cybersécurité etc.) ;
- Indépendant des video management systems (VMS) ;
- Moteur de corrélation d'alarmes réduisant drastiquement le volume de fausses alarmes ;
- Architecture en micro-services pour une scalabilité totale ;
- Customisable par les intégrateurs.

ISAP est aujourd'hui un des logiciels les plus puissants de Physical Security Information Management (« PSIM »). Egidium propose également des versions pour la sécurité des grands événements (Event Monitor™) ou la gestion d'interventions des forces de l'ordre (Tactic Plan™).

Eric BRUDER
Directeur du développement -
INEO HOMELAND SECURITY
Mail : eric.bruder@engie.com
Tél. : +33 6 84 10 79 98

ENGIE INEO
1, place des degrés -
92059 Paris La défense Cedex

www.engie-ineo.fr

Créateur de solutions pour les villes et territoires connectés, ENGIE Ineo intervient au service d'un monde en mutation.

Avec un réseau de 300 agences en France et à l'international, nos équipes innovent pour vous accompagner dans la transition énergétique et numérique. Elles sont à vos cotés pour réaliser vos infrastructures de transport, de télécommunications et d'énergie, vos projets tertiaires et industriels, et ceux liés à la sécurité et à la défense.

Assurer une sécurité optimale avec une vision à 360 degrés

La maintien en sécurité d'un site, d'un événement, ou d'un territoire réclame une analyse globale tenant compte de l'évolution des menaces et des réglementations locales, du niveaux de criticité et de l'environnement des installations à protéger, de l'organisation, des missions, des ressources et des modes opératoires de l'opérateur de sécurité. ENGIE Ineo accompagne ses clients dans leurs démarches de mise en conformité aux décrets et directives propres à leurs métiers : OIV, ports, aéroports, nucléaire, villes et territoires…

Concevoir des outils d'aide à la décision efficaces

Une infrastructure de sécurité nécessite de nombreuses compétences : capteurs intelligents, énergie, réseaux et cybersécurité, automatismes, serveurs et périphériques, logiciels, centres de commandement, télésurveillance... En confiant votre projet de construction, de revamping ou d'extension à ENGIE Ineo, vous bénéficierez de produits et de services fiables, performants et durables, adaptés à vos besoins.

Références

GRTGAZ : sécurisation du réseau Français de distribution de gaz :
- Contrat national sur 10 ans - 48 sites en France
- Conception et déploiement de l'ensemble des systèmes de sécurité Réalisation de l'infrastructure de raccordement de l'ensemble des sites
- Maintenance et télésurveillance
- Formation des opérateurs et intégration des nouvelles procédures opérationnelles

PSA Peugeot Citroën : reconstitution du système de sécurité de contrôle d'accès :
- Conception, mise en œuvre, installation et maintenance - 32 sites dans le monde
- Migration mondiale des données d'accès vers la nouvelle base de données
- Remplacement et déploiement de 3000 nouveaux lecteurs de contrôle d'accès sur l'ensemble des sites
- 600 000 utilisateurs permanents - 400 000 badges fournis

Laurent ASSOULY
Directeur Marketing
Mail : lassouly@e-vitech.com
Tél. : +33 (0)8 20 20 08 39

EVITECH
3, rue Buffon - F - 91400 Orsay

www.evitech.com

EVITECH
Our eyes never close...

Analyse Vidéo pour la Sécurité Globale.

Le logiciel JAGUAR est une solution d'analyse vidéo dédiée à la protection de sites et de périmètres

Il fournit plusieurs applications parmi lesquelles :

- Détection d'intrusion et protection périmétrique
- Tracking automatique d'intrus sur caméras mobiles
- Protection de zone
- Détection de fuites d'hydrocarbures ou de gaz
- Détection de départ de feu ou d'échauffements anormaux
- Détection d'unicité de passage en sas d'accès.

Initialement développé pour le Ministère de la Défense, Jaguar a été déployé avec succès sur des milliers de caméras, et dans un large éventail de situations sensibles, que ce soient dans les domaines de l'Energie, du contexte Régalien, des résidences VIP ou de l'Industrie. Jaguar s'intègre facilement à une infrastructure existante (caméras, systèmes de gestion vidéo, systèmes d'alarmes).

JAGUAR est certifié comme solution de détection principale I-LIDS depuis 2013. Il permet d'atteindre une portée de détection double comparée aux solutions tierces, avec un niveau de performance de détection garanti, pour une efficience budgétaire maximale. La gestion des scènes en trois dimensions et la possibilité de créer des scénarios évolués donne à JAGUAR une flexibilité inégalée pour la mise en œuvre d'une solution de détection dans des environnements complexes.

A propos d'EVITECH

Depuis 12 ans, EVITECH développe et commercialise l'une des solutions les plus fiables et robustes de vidéosurveillance intelligente pour la protection des sites sensibles et la gestion de la foule. Créée à la suite d'un projet financé par la DGA, EVITECH a pour but de fournir des solutions aux performances élevées en analyse d'image, afin d'optimiser l'efficacité des systèmes de protection et pour un coût maîtrisé par l'utilisateur final.

Les solutions d'EVITECH sont les seules aujourd'hui à être à même de garantir leur niveau de performance, afin que l'utilisateur choisisse en connaissance de cause, dans un domaine d'activité complexe et riche.

Egalement, EVITECH est renommée depuis des années pour la qualité de son support, sa réactivité et le soin que nous apportons à la satisfaction de nos clients les plus récents comme les plus anciens.

EVITECH c'est enfin une vingtaine de chercheurs et d'ingénieurs développement pour concevoir et fournir des solutions toujours à la pointe de la technologie et de l'innovation.

Brice KERRINCKX
Directeur Commercial
Mail : Brice@exavision.com
Tél. : 04.66.74.66.00

EXAVISION
8, Avenue Ernest Boffa - 30540 Milhaud

www.exavision.com

EXAVISION : fabricant depuis 1990 de solutions optroniques clés en main pour les environnements les plus exigeants.

Forte d'une expérience de plus de 27 ans en mécatronique, optronique et intégration système

EXAVISION développe et produit des solutions complexes multi-capteurs pour les secteurs de la Défense et de la Sécurité Intérieure. Nos systèmes de vision courte, moyenne et longue distance sont actuellement installés et en activité en France et à l'international.

Gamme NEMOSYS : systèmes optroniques multi-senseurs
La nouvelle gamme NEMOSYS permet une surveillance automatisée de jour comme de nuit et se décline en 4 versions: courte (SR), moyenne (MR), longue (LR) et extra Longue (XR) distance. Ces systèmes optroniques montés sur tourelle 2 axes motorisés, sont composés de différents capteurs au choix : caméras couleur SD ou FHD, caméras thermiques refroidies, bande II, ou non-refroidies bande III. Ces solutions modulaires combinent des capteurs optroniques associés à une détection radar (EXARADAR) et à un logiciel de supervision et de gestion des données (VIGISENS). Ils permettent la détection et le suivi en temps réel de cibles de quelques centaines de mètres à plus de 20 kilomètres.

Gamme EXARADAR : couplage radars aux solutions optroniques
Adaptés à tous les types de terrains, les radars permettent la détection d'intrus ou de véhicules en amont de la zone de protection ou sur des zones définies à l'intérieur du site. La solution EXARADAR gère le couplage des systèmes optroniques développés par EXAVISION avec les principaux radars du marché.

Logiciel VIGISENS : superviseur de gestion multi-senseurs
VIGISENS est un logiciel de supervision développé par EXAVISION et particulièrement adapté à la protection des sites. il intègre un contrôle multi-senseurs (caméras, radars, ….), le suivi automatique de cibles, l'analyse d'images et la gestion des alarmes.

Effecteurs acoustiques et optiques
Associés aux blocs optroniques, EXAVISION propose des effecteurs non létaux de dissuasion, de type projecteurs (ARCLIGHT-SYNCHROBEAM) ou de communications acoustiques LRAD (jusqu'à 5,5 km avec des champs de 15° à 360°).

Solutions de déploiement rapide : remorques & solutions mobiles
EXAVISION a développé une gamme de remorques sur mesure à déploiement rapide qui s'adaptent aux différents environnements et aux récentes exigences des clients pour la protection des infrastructures critiques. Ces remorques personnalisées offrent aux clients un large choix de senseurs. Le déploiement complet s'effectue en 30 minutes (mât télescopique compris). Ces solutions incluent la stabilisation d'image numérique, le positionnement GPS, le suivi automatique des cibles, avec une large gamme de températures de fonctionnement.

Benoît CLAIS
Responsable Développement
Mail : b.clais@groupegeos.com
Tél. : +33 1 77 74 15 39

GEOS
Tour Franklin - 100/101 Terrasse Boieldieu -
92042 La Défense Cedex

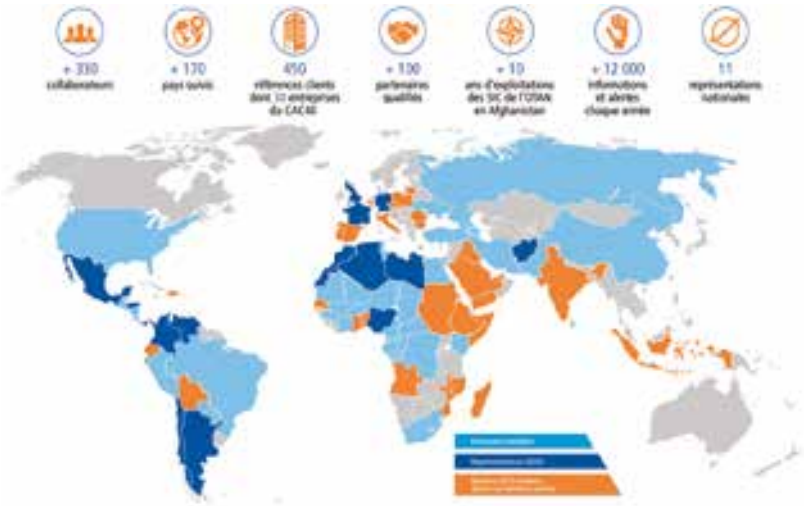
www.groupegeos.com

GROUPE GEOS

Pionnier de la gestion globale des risques depuis 1997.

Le Groupe GEOS accompagne les organismes privés et publiques dans le développement de projets en milieu complexe

Notre présence mondiale en particulier dans les zones instables, associée à notre expertise en matière de sûreté/sécurité des infrastructures, font de nous un partenaire idéal pour assurer la protection des sites stratégiques.



Sur terre et en mer, GEOS met à la disposition de ses clients son savoir-faire et ses équipes d'experts, pour assurer de manière efficace et performante la sécurité des sites sensibles et/ou classifiés.

Nos prestations

Audit et conseil de sureté et sécurité :
- Situation sécuritaire régionale
- Audits de sureté
- Rédaction de plans et procédures
- Formations à la sureté

Accompagnement à la mise en œuvre :
- Intégration des solutions de sûreté
- Suivi réalisation
- Exercice gestion de crise
- Tests d'intrusions

Assistance opérationnelle :
- Opération et maintien systèmes de surveillance
- Security Manager
- Security Officer
- Responsable QHSE

Nos accréditations & adhésions

Viviane BRETAGNE
Directeur Commercial & Business Développement
Mail : viviane.bretagne@gunnebo.com
Mobile : +33 (6) 73 87 33 50

GUNNEBO FRANCE
7, rue Paul Dautier - CS50011 -
78141 Velizy-Villacoublay cedex

www.gunnebo.fr

GUNNEBO®
For a safer world

Ingénierie de sureté pour la protection des sites sensibles.

Filiale du groupe international Gunnebo AB, Gunnebo France a développé un savoir faire unique d'ingénierie de sureté pour la protection des sites sensibles. Cette démarche s'appuie sur une triple expertise de constructeur-intégrateur dans les domaines de la sureté électronique, la gestion des flux de personnes et la protection physique des bâtiments.

Systèmes de Management Intégré de la sureté et des accès

Gunnebo conçoit des systèmes intégrés de sureté électronique destinés à assurer un management opérationnel de la sécurité des sites en combinant la gestion des identités, le contrôle des accès, la détection d'intrusion et la vidéosurveillance. Le système de contrôle d'accès Gunnebo SMI a été **certifié par l'ANSSI** pour répondre aux contraintes d'intégration SSI. Il offre une gestion sécurisée de bout en bout des identités et des droits d'accès.

Contrôle des flux de personnes

Gunnebo est un des leaders mondiaux des obstacles de filtrage des piétons. Nos équipements de tourniquets, couloirs rapides et SAS permettent d'assurer un contrôle effectif d'unicité de passage et s'adaptent à tous les environnements en terme d'esthétique, de flux et de niveau de protection.

Protection physique des bâtiments

Forte d'un savoir faire de plusieurs décennies l'expertise de Gunnebo couvre différentes gammes de menuiserie de sureté :
- Portes, fenêtres, cloisons, SAS, protection de façades,
- Guérites, constructions modulaires, guichets et appareils de transfert

Nos produits sont systématiquement testés dans des laboratoires indépendants pour être certifiés selon les normes européenne :
- Résistance aux attaques manuelles jusqu'au niveau CR6 de la norme EN1627
- Résistance balistique jusqu'au niveau FB7 de la norme EN1522,
- Résistance aux détonations et déflagrations selon les standards EN13123/4 et ISO/DIS 16933

Nos menuiseries peuvent intégrer l'isolation thermique selon la norme RT 2012/27. Elles offrent de larges possibilités d'adaptabilités fonctionnelles et dimensionnelles avec un haut niveau de finition.

Gunnebo développe également des solutions de protection combinée ainsi qu'une gamme de portes spéciales pour faire face aux **attaques par explosifs**.

Edouard CAMPANA
Directeur commercial
Mail : hgh@hgh.fr
Tél. : + 33 1 69 35 47 70

HGH INFRARED SYSTEMS
10, rue Maryse Bastié - 91430 Igny - France

www.hgh.fr

HGH Systèmes Infrarouges - La référence infrarouge depuis 33 ans.

Fondé en 1982, HGH conçoit, développe, assemble et commercialise des systèmes optroniques pour applications industrielles, civiles et de sécurité. En 33 ans, HGH s'est imposé comme une référence internationale pour l'innovation technologique en optronique, à travers le développement de multiples capteurs thermiques. Depuis plusieurs années, HGH réalise plus de 80% de son chiffre d'affaires à l'export. La société possède des bureaux de ventes et des services techniques en Amérique du Nord, en Europe et en Asie, et un réseau d'agents dans plus de 50 pays.

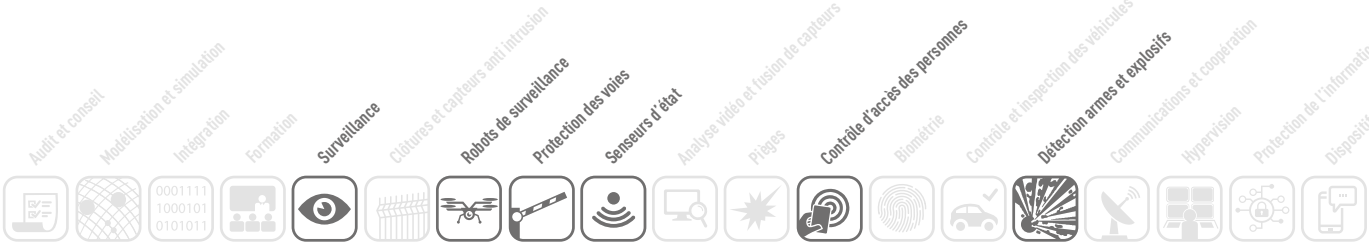
SPYNEL - Système de surveillance panoramique, jour et nuit, de sites étendus

SPYNEL est un système incomparable pour la surveillance continue de zones étendues, par l'acquisition temps réel d'images infrarouge de haute résolution sur 360°. Il fournit une alerte avancée sur tout type de cibles, tels que des hommes rampant, de petites embarcations en bois, des bateaux semi-rigides par mer forte, des drones, des avions furtifs...

Associé à CYCLOPE, logiciel performant de détection automatique d'intrusions, il offre une sécurité en temps réel sans précédent contre les menaces conventionnelles et asymétriques. Entièrement passif, robuste, compact, ce système de surveillance panoramique peut être installé et opérationnel en quelques minutes.

La famille SPYNEL comporte 5 modèles pour couvrir toutes les applications de surveillance :

- Le SPYNEL-X est l'IRST (Infrared Search&Track) avec la meilleure qualité d'image et, de loin, la meilleure portée de détection au monde.
- Le SPYNEL-S capture en temps réel des images infrarouge avec une résolution jusqu'à 30 Mpixels et détecte automatiquement toute intrusion humaine dans un zone de diamètre 12 km.
- Le SPYNEL-C est un système éprouvé, assurant la sécurité de plus de 100 sites dans le monde.
- Le SPYNEL-U combine une caméra infrarouge en bande III (LWIR) non refroidie avec une voie visible 360 degrés haute résolution, solution idéale pour les applications commerciales.
- Le SPYNEL-M est le nouveau modèle de la famille SPYNEL et bénéficie des 15 ans d'expertise d'HGH dans les systèmes de détection et poursuite automatique d'intrusions. Avec une taille inférieur à 12x20 cm et un poids de seulement 1.8 kg, le SPYNEL-M est une solution compacte, robuste et économique pour la surveillance de zones étendues. Un seul capteur SPYNEL-M remplace avantageusement jusqu'à 16 caméras traditionnelles pour avertir de toutes intrusions humaines sur un diamètre d'1.5km, 24h/24.



Bernard LEIBOVICI
CEO
Mail : b.leibovici@groupesds.com
Tél. : 33(6) 73 5218 80

GROUPE SDS/SDS GROUP
53, rue Bourdignon -
94100 Saint-Maur-des-Fossés - France

www.sdshv.com
www.imsrad.com

iMS INNOVATION & MEASUREMENT SYSTEMS
Groupe SDS

Forte expertise dans le développement de produits électroniques complexes par la conception, la fabrication et la commercialisation d'équipements de détection et d'identification de matières nucléaires illicites communément appelés bombes sales.

Réponse préventive à la menace nucléaire et radioactive

Afin de répondre à cette menace, un consortium d'entreprises françaises et de centres de recherche (SNEF Connect, TPL Systèmes, Novitact et le CEA-List), s'est réuni autour d'un projet innovant nommé **« Capacité Opérationnelle de Détection et d'Identification de matières Radiologiques et Nucléaires (CODI-NR) »**.

Le projet vise à prévenir une action malveillante (matières radioactives, événement radiologique ou nucléaire) sur la voie publique ou au contact des infrastructures publiques, en développant pour les personnes en charge de la sûreté et de la sécurité, une solution innovante portable et communicante de détection et d'identification des matières nucléaires et radiologiques, permettant d'engager rapidement les actions de prévention et de protection nécessaires par :

- La détection en milieu ouvert ou clos (sécurisation d'une foule en pleine rue, quai de métro, Fan Zone, métro…)
- La détection en mode inspection / filtrage (palpation,…)
- La connexion au poste de commandement en temps réel selon plusieurs vecteurs de communication, pour déclencher les actions nécessaires de levée de doute et contre mesure.

L'utilisation des drones pour la mesure radiologique

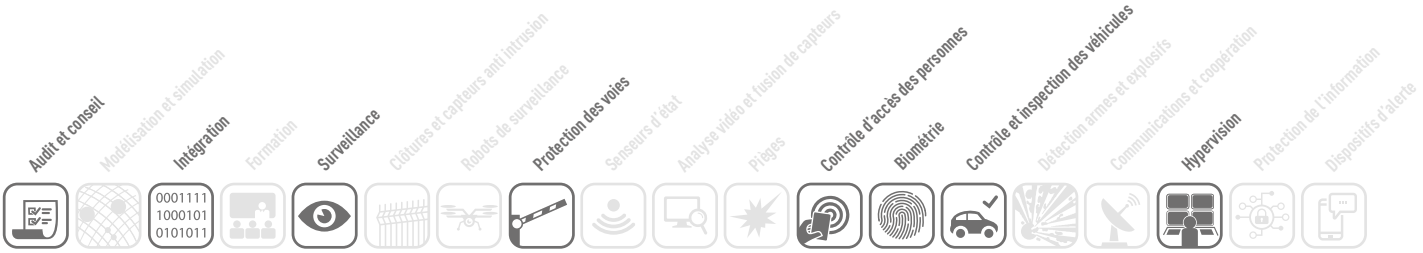
ADT Drone

Cette utilisation permet des économies en termes de temps et de moyens à mettre en œuvre et de sécuriser les prestations de contrôle par la réduction des risques et la limitation de l'exposition des personnels aux rayonnements ionisants.

Cette innovation s'adresse à la surveillance des :

- installations nucléaires de base
- installations critiques en particulier sites sensibles Seveso
- INB en démantèlement nucléaire
- installations de traitement de déchets
- points d'importance vitale
- lieux accueillant du public

Le système SDS-ADT Drones permet à l'opérateur du drone ou à une base arrière (jusqu'à 1 km) de contrôler les paramètres de surveillance, le débit de dose, les spectres et leur identification en temps réel, le positionnement du drone sur une carte et les alarmes déclenchées.



Frédéric BERTOZZI
Président
Mail : kopp-france@wanadoo.fr
Tél. : +33 1 49 40 09 04

KOPP
17, rue de la Poterie - ZAC Delaunay Belleville - 93200 Saint-Denis

www.kopp-france.fr

Sécurisation de sites sensibles.

KOPP intervient dans les zones géopolitiques sensibles pour mettre en œuvre les solutions qui permettent d'assurer à ses clients, le niveau de sécurisation le plus élevé. Les plus hautes autorités de l'État français telles que les Ministères de la Défense, de l'Intérieur, de la Justice et des Affaires Étrangères font appel à KOPP.

Audits et conseils

KOPP réalise in situ les audits des sites institutionnels (Présidence, Ministères, Ambassades, …) ou industriels vitaux (énergie, logistique, fiduciaire, …) en évaluant au cas par cas les risques et les enjeux qui correspondent au site et à la menace.

Études de sites et intégration

KOPP gère l'étude complète de sécurisation du site en sélectionnant les meilleurs équipements et fournit les plans d'implantation, les plans de génie civil ainsi que les schémas électriques.

KOPP effectue l'installation des matériels sélectionnés et assure la mise en service des différents dispositifs ainsi que la formation des agents à leur utilisation.

Fabrication maîtrisée d'obstacles escamotables

KOPP conçoit et fabrique en France des obstacles anti-véhicules suicide depuis 1965.

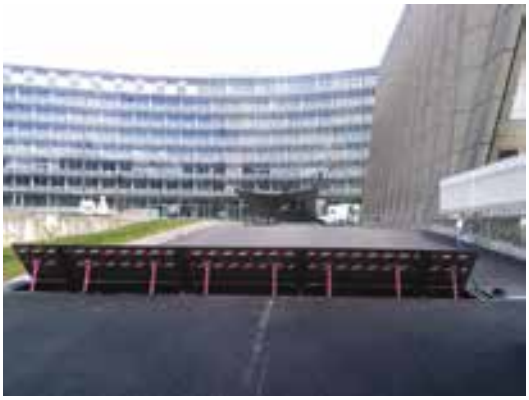
KOPP maîtrise toutes les phases de création de ses produits et peut ainsi s'adapter à toute demande particulière de ses clients.

KOPP propose des obstacles déployables en quelques minutes pour sécuriser des zones périmétriques provisoires (évènements, manifestations, …)

Logiciels d'analyse d'images

KOPP développe également ses propres solutions dédiées d'analyse d'images pour des applications spécifiques :

- Lecteur automatique de plaques d'immatriculation,
- Scanner de châssis de véhicules,
- Drone captif de vidéosurveillance,
- Hypervision de sites,
- Authentification de documents d'identité.



Jean-Luc PAQUIÉ
Mail: jean-luc.paquie@etienne-lacroix.com
Tél. : +33 (0) 561 677 949
Mobile : +33 (0) 609 150 868

LACROIX DEFENSE
Route de Gaudiès - 09270 Mazères - France

www.lacroix-defense.com

LACROIX

Systèmes de protection de proximité.

Le groupe Etienne Lacroix est un fabricant innovant de systèmes réactifs et de munitions associées pour la protection de zones.

Systèmes de protection de proximité

Lacroix développe et fabrique des systèmes de protection de proximité et de zones (LOS / NLOS), afin de protéger les forces sur divers type de zones, des bivouacs temporaires aux camps principaux ou aux infrastructures critiques.

Les systèmes peuvent inclure la détection des menaces par différents types de capteurs, analyser et classifier l'intrusion avec « homme dans la boucle », et permettre des réactions graduées et appropriées (non létal à létal) afin de retarder ou neutraliser les menaces.

Une gamme complète de systems

Lacroix propose une gamme complète de systèmes de protection de proximité (fixe ou mobile, antipersonnel ou anti-véhicule, câblé ou télécommandé, seul ou communicatif) adaptable à différentes situations de crise ou à des environnements de champ de bataille.

Une gamme complète de reaction

Lacroix propose une gamme complète d'effets (Multi-bandes, fumée de masquage, Réaction graduée : alerte, de la dissuasion à la neutralisation).

Efficacité prouvée

La protection de proximité est utilisée dans de nombreux pays, de la detection à la reaction, dans les derniers théâtres d'opération.

LUCEOR
WiMESH NETWORKS

Fabien MAISL
Directeur Marketing
Mail : fabien.maisl@luceor.com
Tél. : +33 (0)1 84 73 13 00

LUCEOR
23, Avenue Louis Breguet - Bâtiment B -
78140 Vélizy Villacoublay - France

www.luceor.com

Réseau IP sans fil haute performance pour la protection de sites.

Les solutions WiMesh Luceor permettent de déployer un réseau de transmission sans fil sécurisé, très haut débit et résilient pour connecter facilement et à moindre coût tous les équipements de protection des sites sensibles : caméras de vidéosurveillance, contrôle d'accès, véhicules de patrouille, mais aussi tous les capteurs de nouvelle génération (drones, détecteurs d'intrusions, systèmes d'alertes, etc.).

Le complément idéal de votre réseau IP

Besoin d'une caméra supplémentaire pour sécuriser une zone aveugle ? De connecter la guérite du gardien sans devoir creuser une tranchée à travers le parking ? Quelle que soit la taille de votre site, un réseau WiMesh de Luceor est la solution pour étendre votre infrastructure de sécurité sans devoir subir le déploiement long et coûteux de réseaux filaires. Un réseau WiMesh s'intègre parfaitement à votre réseau IP existant pour l'amener exactement là où vous en avez besoin, avec la performance et la résilience que vous attendez pour vos applications de sécurité. Et grâce au logiciel MeshTool Suite de Luceor, configurer, gérer et optimiser votre infrastructure sans fil WiMesh n'a jamais été aussi simple.

Sécurité en mobilité

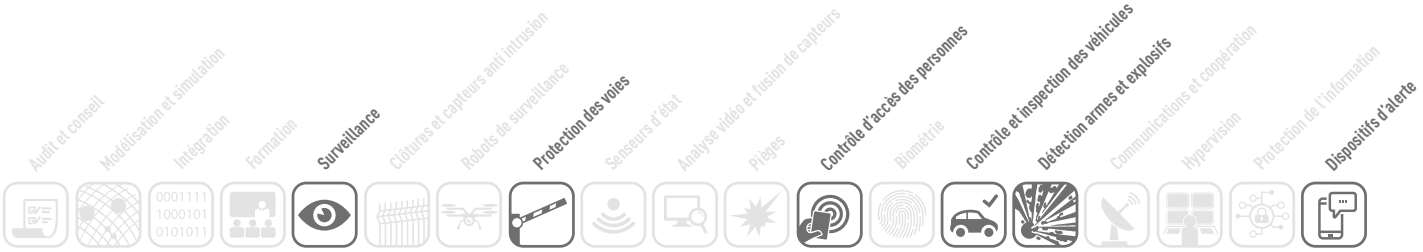
Votre réseau WiMesh est également un réseau mobile privé reliant véhicules, drones, robots et gardes de sécurité à votre réseau IP où qu'ils se trouvent sur site. Grâce au handover instantané et à une latence < 2ms, vous recevez les vidéos HD de tous vos appareils mobiles pour voir en direct ce que voient vos gardes. Pas besoin de licences gouvernementales ou de technologies cellulaires complexes et coûteuses. C'est aussi simple que de déployer votre réseau WiMesh.

Performance et résilience

Parce que la technologie WiMesh de Luceor est issue de concepts militaires et a été mise au point en coopération avec les unités d'élite de la Police Nationale, elle dispose de mécanismes de sécurité et de résilience uniques lui permettant de fonctionner dans les environnements les plus hostiles : réseau très haut débit entièrement dédié à vos applications critiques, chiffrement dynamique des liens, architecture maillée auto-cicatrisante et résiliente aux interférences, etc.

Références

- Sites industriels : Total, LyonDellBasel, EDF, Areva, Engie, SNCF, ArcelorMittal, Airbus…
- Collectivités locales : plus de 200 villes en France dont Paris, Bordeaux, Pontoise, Boulogne, Deauville, Nanterre…
- Forces d'intervention : Ministère de l'intérieur (CRS, RAID, SDIS), Police Fédérale Belge…



Charleene MURACCIOLE
Coordinatrice Marketing
Mail : marketing-fr@mirion.com
Tél. : 04 90 59 66 21

MIRION TECHNOLOGIES (MGPI) S.A
Route d'Eyguières - FR - 13113 Lamanon

www.mirion.com

MIRION
TECHNOLOGIES

60 années d'expertise et d'innovation dans la protection des hommes, des installations et de l'environnement contre les effets néfastes des radiations ionisantes.

Les activités de Mirion Technologies (MGPI) SA sont centrées sur la protection des personnes et des biens, la sûreté des installations et la protection de l'environnement face aux risques industriels et terroristes d'origine nucléaire et radiologique. 60 ans d'expertise ont fait de Mirion une référence internationale dans la fourniture d'équipements de pointe, durcis pour répondre aux exigences militaires et de la défense civile.

Protection des infrastructures critiques (producteurs d'énergie nucléaire, sites industriels)

Pour prévenir l'intrusion de sources radioactives sur des sites sensibles, les produits de Mirion fournissent aux exploitants les outils indispensables pour sécuriser les points d'accès aux bâtiments, prévenir toute sortie ou entrée de matières radioactives sur le site (par des personnes ou via des chargements) et permettre de localiser et de mesurer la menace radiologique présente dans les locaux. La surveillance du périmètre de ces sites appelle la mise en œuvre de solutions performantes de contrôle à distance, fonctionnant de façon autonome sur de longues périodes.

Protection des sites de divertissement, de loisir et de grands événements

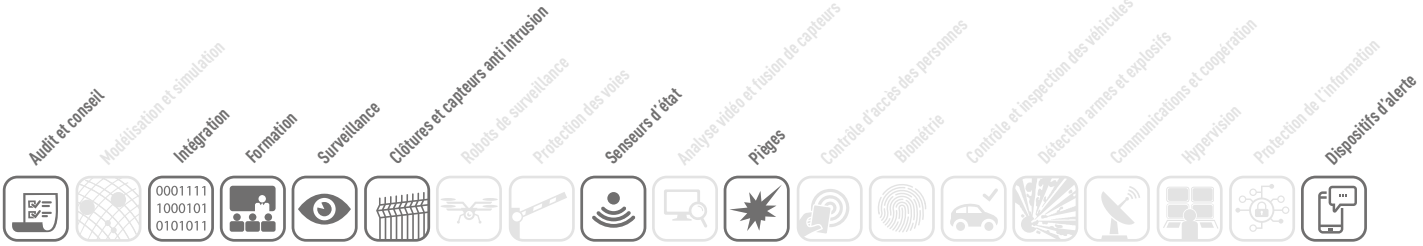
Lors de manifestations de grande ampleur, la forte affluence de visiteurs sur des lieux de divertissement et de loisir confronte les agents de la force publique et les personnels de sécurité à une réelle problématique : rechercher des sources radioactives illicites avec une absolue nécessité de discrétion. Mirion offre des solutions permettant le contrôle des accès lors de forte affluence, le déclenchement d'alarmes discrètes en cas de détection radiologique et le transfert des informations en temps réel aux postes de surveillance.

Contrôle des réseaux de transport et des postes-frontières

Les systèmes de détection et d'analyse radiologique conçus par Mirion permettent un contrôle discret en continu des voyageurs, des bagages, des véhicules et des camions et de leur chargement, sans interruption du flux de circulation.

Cartographie à grande échelle

Mirion offre une large gamme d'équipements et de systèmes mobiles pour répondre au besoin d'une surveillance de larges zones par voies terrestres, maritimes, aériennes ou à dos d'homme. Toutes les mesures sont reportées en temps réel vers un poste de commande. La cartographie globale guide les intervenants qui vont confirmer la localisation des points chauds et mettre en place un périmètre de sécurité.



NUANCES TECHNOLOGIES
Mail : info@nuances.fr
Tél. : +33 (0)1 80 06 80 70
92, avenue de Wagram - 75017 Paris
www.nuances.fr

NUANCES TECHNOLOGIES

Les systèmes développés par Nuances Technologies préviennent les actions malveillantes en contrôlant les communications sans fil.

Discrets et simples d'utilisation, ils peuvent faire l'objet d'une installation fixe pour une sécurisation permanente ou d'une utilisation mobile tactique par des unités d'intervention.

Ces équipements offrent de nombreuses fonctions : surveiller l'activité radioélectrique d'un site, localiser l'origine, interdire les communications, garantir la confidentialité des échanges, protéger les sites et les personnes contre les engins explosifs radiocommandés…

Capacités

- Surveiller le spectre électromagnétique
- Détecter les communications sans fil
- Identifier et localiser les émetteurs
- Bloquer, brouiller ou sélectionner les communications
- Enregistrer et analyser les données…

Solutions

- Systèmes de capteurs RF temps réel pour la détection et la localisation
- Systèmes de lutte anti-drone
- Brouilleurs de communications
- Brouilleurs de RCIED
- Systèmes de filtrage de communications (white/black list)
- Contrôle d'accès et monitoring WiFi
- Réseaux de communications privés mobiles

Services

- Rédaction/analyse de cahier des charges
- Etude de site
- Simulation
- Conception spécifique
- Intégration
- Mesures d'efficacité
- Formation
- Maintenance

Geoffroy DELTEL
Digital Vision General Manager
Mail : g.deltel@photonis.com
Tél. : +33 5 56 16 40 50

PHOTONIS TECHNOLOGIES
18, avenue de Pythagore -
33700 Mérignac - France

www.photonis.com

PHOTONIS

Digital night vision. PHOTONIS est leader dans la conception et la fabrication de capteurs numériques et d'équipements pour la surveillance de jour comme de nuit de sites sensibles et de périmètres à protéger.

Vision numérique de jour comme de nuit et en couleurs

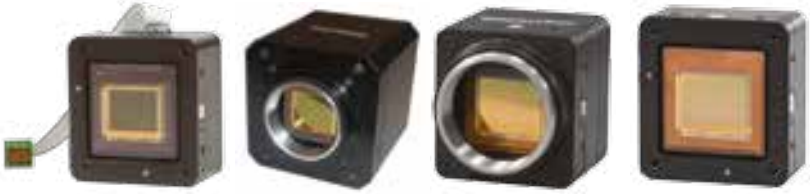
La caméra NOCTURN est une caméra durcie capable de fonctionner à très bas niveau de lumière tout en conservant une haute résolution, une sensibilité très prononcée et une dynamique importante sur la base d'une très faible consommation.

Cette nouvelle caméra filme en temps réel des images noir et blanc ou couleurs de jour jusqu'à des niveaux de nuit 3 correspondant au quart de lune dans le spectre visible et proche infra-rouge. Sa taille très compacte fait de ce coeur de caméra le composant idéal pour intégration dans des systèmes de surveillance fixes ou mobiles, afin d'assurer une protection permanente de jour comme de nuit.

Développé en partenariat avec la société Rochester Precision Optics, le CNOD (CMOS Night Observation Device) est un monoculaire numérique à haute définition permettant aux utilisateurs de voir de jour (soleil intense) comme de nuit (très bas niveau de lumière) avec un contraste élevé.

Développé en partenariat avec BERTIN, le FusionSight est le premier monoculaire compact au monde qui combine à la fois un capteur très bas niveau de lumière couleur et un capteur thermique. Lorsqu'ils sont utilisées simultanément, ces capteurs améliorent significativement l'obtention d'images et de vidéos sur le perimètre observé. Les utilisateurs peuvent choisir de se baser sur l'image thermique uniquement ou sur l'image couleur de jour comme de nuit ou encore de fusionner les informations utiles de chacune de ces deux images pour pouvoir « décamoufler » une cible. Le FusionSight dispose également d'une fonction enregistrement.

La caméra EBNOCTURN est la caméra numérique de nuit la plus puissante au monde dans le spectre du visible. Basée sur le capteur EBCMOS qui capte des images et des vidéos en temps réel même lorsque la luminosité disponible atteint des niveaux de nuit profonde de l'ordre de 10µlux (nuit sans lune avec couverture nuageuse épaisse). Les points forts qui rendent cette caméra nocturne unique sont la fréquence d'acquisition élevée (jusqu'à 100 images par seconde même en nuit très profonde), une image d'une qualité inégalée à ce niveau de nuit, une résolution élevée compatible avec les applications mobiles de surveillance : à bord d'un drone par exemple pour une observation en pleine nuit.




FusionSight


CNOD


Caméra EB-NOCTURN


Caméra NOCTURN

PRONERGY

Florian EECKEMAN
Responsable Commercial
Mail : f.eeckeman@pronergy.com
Tél. : +33(0) 1 69 19 43 03

PRONERGY
12 Bis, Avenue des Tropiques -
91940 Les Ulis - France

www.pronergy.com

E-DOME : station autonome et connectée de rechargement de drone.

Conçu pour réduire les coûts de la protection de sites sensibles

Au travers d'opérations de détection d'intrus, de levée de doute, ronde périodique ou simplement pendant le relayage d'un guidage à distance, la station E-DOME sert de base d'accueil et permet avant tout le stockage et la recharge électrique d'un drone.

L'opérateur dispose ainsi d'un dock relayant ou stockant les données de vol au travers d'une connexion sécurisée câblée et/ou sans-fil.

Cette station permet également au drone de récolter un nombre important d'informations extérieures afin de lancer tout type de missions dans un environnement maitrisé. En effet, elle dispose d'un dispositif de pare-vent et d'une station météo lui indiquant la température, la luminosité, la pluie et le vent.

Afin de faire face aux agressions, la station embarque un système de capteurs informant le drone de tout vandalisme ainsi qu'une centrale d'alarme permettant de dresser un périmètre surveillé.

En option, l'E-DOME propose une alimentation autonome à partir d'énergie renouvelable.

Associé à cette plate-forme d'accueil de drone, la surveillance et la patrouille des sites peut se faire également avec des véhicules autonomes.

Cette nouvelle fonctionnalité des véhicules peut faciliter les rondes sans personne à bord dans un premier temps, en repérage des dysfonctionnements et cas alertes. Pour ensuite en effectuer d'autres avec une personne compétente à bord, lui facilitant d'accéder directement aux espaces nécessitant une intervention.

Le système de communication Machine-Infrastructure permet aux véhicules autonomes de mieux détecter les intrus avec des caméras embarquées.

Associé au drone, la mise en place d'une flotte de véhicules autonomes de surveillance a pour but de gagner en efficacité et réactivité, diminuer les coûts et optimiser les déplacements du personnel de gardiennage.

Thibault JANIN
Directeur du développement
Mail : t.janin@s2ec.fr
Tél. : +33 4 88 78 82 17

S2E CONSULTING
350, Avenue de la Lauzière-
Parc du Golf - Batiment 31 -
13593 Aix en Provence Cedex 3

www.s2ec.fr

S2E Consulting est une société de sûreté familiale dont le métier est de savoir proposer des solutions complètes de conseil et de protection aux entreprises et institutions confrontées à de forts enjeux sécuritaires et politiques à l'international.

Nos missions

Nos activités se structurent autour de quatre missions principales : l'analyse des risques et des menaces, la protection des actifs physiques, le la protection des salariés en déplacement ou des résidents à l'étranger, et l'assistance opérationnelle en cas de crise grave.

Nos equipes

S2E Consulting s'appuie sur une équipe pluridisciplinaire d'experts de terrain disposant d'une expérience moyenne de vingt ans dans la conduite d'opérations sensibles en pays à risques.

La protection des grands projets

S2E Consulting accompagne ses clients dans la sécurisation de grands projets d'ingénierie en pays à risques (infrastructure, eaux, énergie, transport…) en fournissant des solutions complètes de management de la sûreté tout au long du cycle des chantiers.

- Avant projet : analyse des risques, audits de vulnérabilité, étude d'impact 360° (chantiers, bureaux, bases vies, zones de stockage, déplacements), avis de faisabilité, études de coût.
- Assistance à la MOE : définition du schéma directeur de sûreté, conception des plans et procédures de protection et d'alerte, identification et mise en œuvre des moyens de protection (actifs et passifs), formation des personnels.
- Management de la sûreté : supervision et pilotage continu de l'ensemble des moyens de protection, suivi de l'évolution des risques et menaces (veille sécuritaire), ajustements des moyens en fonction de l'évolution des chantiers, gestion sécuritaire des POB.
- Gestion de crise : conception des plans et des procédures, organisation des cellules de crise, exercices de crise, évacuations, PMCO, PCA.

La protection des implantations

S2E Consulting accompagne aussi bien des entreprises (grands groupes et PME) que des administrations dans la sécurisation de leurs implantations à l'international :

- Audits de sûreté
- Mise en protection des emprises
- Fourniture de personnels spécialisés (Security managers)
- Gestion de crise : conception des plans et des procédures, organisation des cellules de crise, exercices de crise, évacuations, PMCO, PCA.

Emmanuel MAURIN
Directeur

SPARTAN MILITARY & LAW ENFORCEMENT
9/11, rue Henri Dunant -
91070 Bondoufle - France

www.spartan-mle.com

SPARTAN
MILITARY & LAW ENFORCEMENT

Calibre d'entraînement 6mm sous licence.

L'idéal pour l'entrainement sur sites combinant souplesse d'emploi et coûts maitrisés

Construites sous licence des plus grands manufacturiers (GLOCK, FN HERSTAL, COLT, SIG SAUER…) nos répliques sont d'un **réalisme saisissant**. Reproduites avec le même poids, le même centre de gravité, une culasse mobile et un effet recul elles sont particulièrement adaptées tant pour la formation à la gestuelle de l'arme que pour les exercices de mises en situation.

La **souplesse d'emploi** de nos répliques d'armes vous séduira vite. Légalement, ce ne sont pas des armes : les mesures de protection pour leur stockage et leur transport, qu'il soit routier, ferroviaire ou aérien, en seront grandement facilitées. La faible dangerosité des projectiles (énergie < 2 joules) dispense des gabarits de sécurité et des aires dédiées pour l'entraînement. Elle autorise à vous entraîner dans n'importe où et quand vous le souhaitez, sans provoquer de dommage sur les sites à protéger ou le mobilier.

Nos répliques permettent également d'**organiser de très réalistes exercices de force contre force** sans avoir recours à de pesants équipements de protection supplémentaires tout en maintenant une véritable sanction du tir.

Le coût de possession d'un parc de calibres d'entraînement 6mm est faible et sans commune mesure avec les autres moyens d'entrainement au tir de combat. Nos répliques sont au minimum 20% moins chères que les autres systèmes d'entraînement. Quant au budget munitions il est sans comparaison. Pour 10.000 coups tirés il passera de l'ordre de 8.000€ - 10.000€ avec les autres systèmes d'entraînement à 150€ grâce aux technologies que nous utilisons qui sont les moins chères du marchés (billes plastiques, batteries électriques ou cartouches de CO_2). Nos billes sont certifiées biodégradables. Le CO_2 utilisé dans les cartouches est directement issu de l'atmosphère et ne génère pas de gaz à effet de serre. Nos batteries électriques sont rechargeables et les cartouches de CO_2, recyclables

STERBLUE ®
SMART DATA, FAR AWAY

Geoffrey VANCASSEL
Président
Mail : geoffrey.vancassel@sterblue.com
Tél. : 0033 (0)6 68 66 94 84

STERBLUE
2, rue Alfred Kastler - 44300 Nantes - France

www.sterblue.com

La solution qui automatise vos inspections de sites sensibles.

Sterblue est le spécialiste de l'automatisation des inspections industrielles par drones. Basé à Nantes depuis 2016, la start-up commercialise une solution automatisant les inspections périmétriques et la surveillance de zones sensibles.

Le challenge

Les clôtures de sites sensibles sont régulièrement endommagées par le vieillissement des structures, la végétation ou les intrusions. Comment garantir qu'un rondier, parcourant des dizaines de kilomètres par jour, ou qu'un drone, générant des milliers d'images pendant son vol, puissent sans faille détecter l'intégralité des anomalies dans la clôture ?

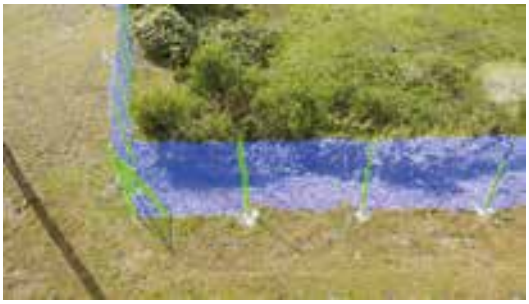
Sterblue a une solution intégrée répondant à ce challenge pour :
- la captation d'images et le vol du drone autour du site
- la détection des anomalies dans l'infrastructure survolée
- la génération du rapport d'inspection en ligne

Les technologies qui composent la solution Sterblue

Perception : l'application permettant de planifier très simplement des plans de vol 2D ou 3D en fonction d'un environnement et d'exigences complexes. Des paramètres tels que la taille de clôtures, la taille de défauts à détecter, les obstacles 3D, etc… sont renseignés afin de **générer un plan de vol optimisé et reproductible**.

Curiosity : la brique logicielle basée sur l'intelligence artificielle permettant de **détecter automatiquement différents types de défauts dans les clôtures** (trous, pylônes cassé, tordus, grillages abîmé, etc.) et d'en détecter le changement par rapport à une inspection précédente.

Le Cloud Sterblue est la plateforme industrielle permettant de stocker, traiter et **visualiser les données traitées** sur des interfaces utilisateurs ergonomiques. Différentes redondances et cryptages sont en place sur toute la chaine de traitement afin d'en assurer un haut niveau de fiabilité et de sécurité.



Service COMMERCIAL
Mail : sales-fr@stormshield.eu
Tél. : +33 (0)9 69 32 96 29

STORMSHIELD
Immeuble Axium -
22, rue du Gouverneur Général Eboué -
92130 Issy-les-Moulineaux - France

www.stormshield.eu

STORMSHIELD
COLLABORATIVE SECURITY

La protection globale pour les infrastructures réseau et les systèmes industriels opérationnels.

Stormshield, filiale à 100% d'Airbus Defence and Space, propose des solutions de sécurité de bout-en-bout innovantes pour protéger les réseaux (Stormshield Network Security), les postes de travail (Stormshield Endpoint Security) et les données (Stormshield Data Security).

Ces solutions de confiance de nouvelle génération, certifiées au plus haut niveau européen (EU RESTRICTED, OTAN et ANSSI EAL4+), assurent la protection des informations stratégiques et sont déployées au travers d'un réseau de partenaires de distribution, d'intégrateurs et d'opérateurs dans des entreprises de toute taille, des institutions gouvernementales et des organismes de défense partout dans le monde.

Détectez et protégez sans impact sur vos activités industrielles

En intégrant les solutions de sécurité Stormshield à la fois dans le domaine de l'OT (Operational Technology) comme dans celui de l'IT (Information Technology), vous bénéficiez d'une combinaison de protections de vos systèmes de production sans impact négatif sur l'activité. L'ensemble de vos systèmes disposent ainsi d'une solution technique unique adaptée aux deux mondes.

Inventoriez vos appareils actifs

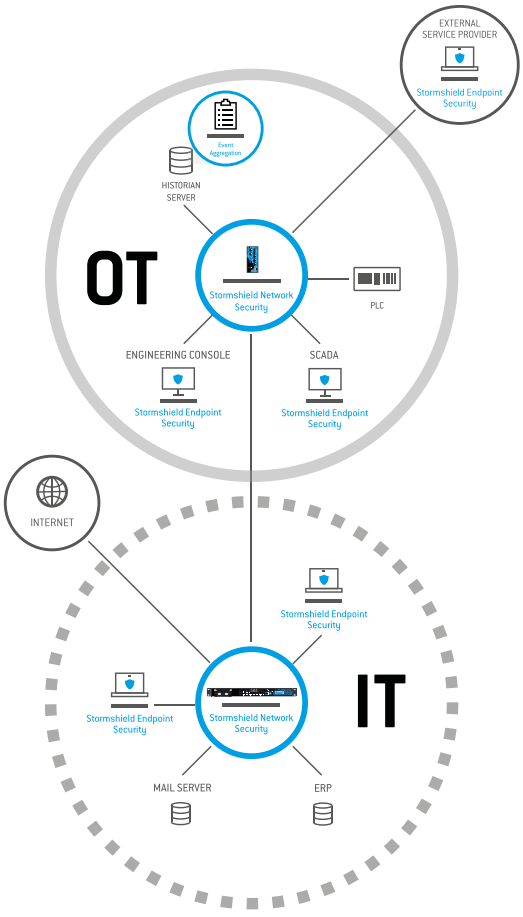
Grâce à notre outil visuel de supervision, vous disposez en temps réel de la liste des appareils actifs sur votre réseau. Cette vue globale de votre réseau vous apporte une aide précieuse dans la gestion régulière de l'inventaire de votre système.

Intégrez un produit adapté à vos environnements

Avec la solution globale Stormshield Network Security, vous intégrez un seul produit logiciel pour une administration unique quel que soit le domaine d'activité (OT ou IT). Ce logiciel est disponible selon vos besoins dans des formats Hardware IT ou OT renforcé pour la protection des PLC (Programmable Logic Controller).

Maîtrisez vos postes opérationnels

Dans un environnement Microsoft Windows, les postes de travail constituent des points sensibles de votre système opérationnel. Pour les sécuriser, la solution Stormshield Endpoint Security vous permet de bloquer les clefs USB ou les supports amovibles. Cette solution proactive est idéale pour les environnements non connectés car elle n'utilise aucune base de signature et donc ne nécessite aucune mise à jour.



Xavier DORVEAUX
Mail : xavier.dorveaux@sysnav.com
Tél. : +33 (0)2 78 77 03 46

SYSNAV
57, rue de Montigny -
27200 Vernon - France

www.sysnav.com

sysnav
NAVIGATION TECHNOLOGIES

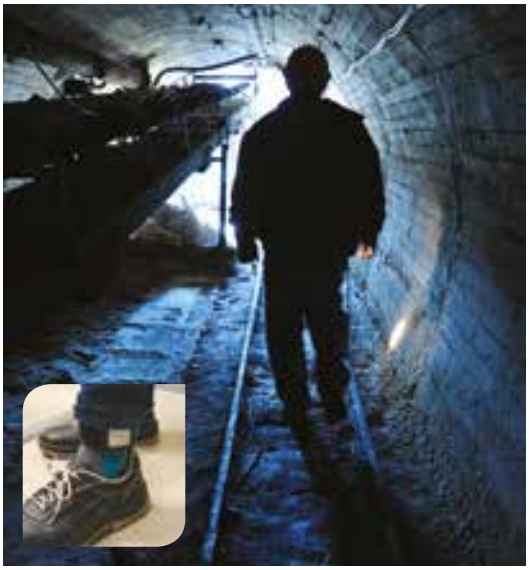
Bénéficiez des avantages de la géolocalisation indoor sans infrastructure pour mieux protéger vos sites !

WATA RTLS (Wearable Ankle Trajectory Analyser)

Un boitier de géolocalisation indoor pour protéger en temps réel les travailleurs isolés.

La solution WATA RTLS est la première solution permettant d'assurer le suivi de vos agents avec une précision inférieure à 1 mètre à l'intérieur des bâtiments. Cet outil unique, conçu pour sécuriser les travailleurs isolés, les fantassins et visiteurs, déclenche des alertes en cas d'incident (chute, mouvement anormal, intrusion dans une zone interdite, etc). En option : disponible sur la plateforme SYSNAV en accès web ou intégré à votre SI.

« La géolocalisation intérieure de précision pour sauver des vies »



Fixation en quelques secondes sur la cheville.

WATA Analytics

La version post-traitement pour accompagner la transformation digitale des sites.

WATA Analytics est conçu pour offrir des indicateurs de performance. Il permet d'optimiser vos procédés, augmenter votre productivité et tester vos changements d'organisation. Le boitier de seulement 28g est livré avec son étui robuste, sa station de charge et de transfert de données.

« Vous nous fournissez le plan, SYSNAV vous fournit la trajectoire »

SYSNAV Tracking

Le suivi des véhicules en conditions extrêmes, y compris en cas de perte des signaux GPS.

Sur les sites les plus sensibles, la traçabilité doit s'étendre aux mouvements des véhicules à l'intérieur des sites. SYSNAV propose dans ce cadre une balise de suivi de véhicule robuste aux contre-mesures attendues visant la localisation par GPS.

SYSNAV est une PME française innovante indépendante, référence européenne des systèmes de géolocalisation et de capture du mouvement sans infrastructure.

SYSNAV conçoit et commercialise des solutions de géolocalisation et de mesure de mouvement robustes, disponibles, précises et intègres pour les environnements et les standards les plus exigeants : défense, sécurité, sûreté, médical, véhicules autonomes…

SYSNAV est certifiée ISO9001 et ISO13485 pour les équipements de navigation embarqués.

Jean-Pierre VIDAL
Critical Infrastructure Protection Product Line Manager
Mail : jean-pierre.vidal@thalesgroup.com
Tél. : +33 1 73 32 16 67

THALES COMMUNICATIONS & SECURITY SAS
20-22, rue Grange Dame Rose -
78180 Vélizy-Villacoublay

www.thalesgroup.com

Des infrastructures, des personnes, des données mieux protégées.

Sites industriels, sites gouvernementaux et militaires, ports, aéroports, sites sensibles publics : Thales propose à chacun la réponse la plus adaptée aux risques et menaces d'aujourd'hui et de demain. À partir du concept opérationnel de chacun de ses clients, Thales conçoit des systèmes de sécurité performants et hautement évolutifs, capables de s'intégrer dans tous les environnements existants, même complexes et de s'adapter facilement aux nouvelles menaces ou exigences règlementaires.

Associant protection physique et sécurité logique, l'offre de bout-en-bout de Thales comprend un large spectre de technologies parfaitement maîtrisées et des solutions innovantes, à forte valeur ajoutée. Afin d'accroître toujours plus les capacités d'anticipation et de détection automatique des événements anormaux pouvant affecter la sécurité des sites critiques, l'offre de Thales repose sur la combinaison de traitements intelligents des données issues de différents sous-systèmes qu'elle intègre. En aidant ainsi l'opérateur à anticiper, à mieux qualifier l'incident et à prendre les bonnes décisions au bon moment, les systèmes Thales contribuent à l'amélioration significative du taux de réactivité dans le traitement des incidents pouvant affecter les infrastructures critiques.

Grâce à ses solutions innovantes et évolutives, Thales assure de manière pérenne et intelligente la sécurité globale des infrastructures, des opérations, des personnes, et des données et préserve ainsi la continuité d'activité en toutes circonstances, tout en optimisant les coûts d'exploitation et les processus opérationnels.

Cybersécurité

Thales conçoit et intègre des solutions de chiffrement, des sondes, et met en oeuvre des services innovants tels que la supervision, la veille, l'administration et le maintien en conditions de sécurité pour faire face à l'extrême évolutivité des menaces.

Réseaux résilients

L'offre Nexium de Thales garantit la disponibilité et l'efficacité du réseau en tout temps et toutes circonstances grâce à une approche de supervision innovante basée sur la résistance aux menaces physiques jusqu'à des niveaux très élevés.

Services critiques

Pour répondre au mieux aux besoins critiques de ses clients, Thales propose également d'opérer ses solutions en mode service. Les équipes mettent à disposition leur expertise de l'écosystème pour intégrer les solutions les plus pertinentes du marché, adaptent le service aux changements de menaces et aux évolutions technologiques tout en maîtrisant le budget de ses clients.

Laurent OUDOT
CEO & Founder
Mail : press(at)tehtri-security.com
Tél. : +33(0)9-72-50-80-33

TEHTRIS
13-15, rue Taitbout - 75009 Paris - France

www.tehtris.com

TEHTRIS

La société TEHTRIS est l'éditeur de la solution « eGambit », le cyber-arsenal défensif français.

Alors que les intrusions malveillantes se multiplient sur Internet, la société française **TEHTRIS**, implantée à Bordeaux Métropole, propose une solution nommée **eGambit**, capable d'unifier des capteurs de Cybersécurité avancés. De nombreuses infrastructures de sites industriels sensibles sont ainsi surveillées et protégées jour et nuit contre les intrusions numériques dans le monde entier : Brésil, USA, Chine, Arabie Saoudite, Europe.

TEHTRIS, société française innovante

L'entreprise fut créée en 2010 par des anciens experts opérationnels du Ministère de la Défense. Avec une récompense internationale de la meilleure solution de cybersurveillance dans sa catégorie, ses consultants apportent une contribution technologique, face aux problèmes récurrents comme le cyber-espionnage et le cyber-sabotage. Son expertise est utilisée par des multinationales et des services étatiques à la recherche de certitudes techniques. Ses activités principales sont les tests d'intrusions avancés, ainsi que la lutte et la surveillance contre les attaques numériques.

Solution logicielle française éditée par TEHTRIS

Nommée eGambit, elle assure une surveillance nominale face aux cyber menaces diverses et avancées. Ce produit est capable de surveiller et d'améliorer la sécurité des systèmes d'information face aux intrusions furtives et complexes. Tel un système d'alarme numérique, eGambit apporte son assistance à des entreprises contre des menaces internes et externes : piratages des données, de la production, de la supervision, de la sécurité physique, des caméras, etc.

En particulier, l'Intelligence Artificielle et les robots numériques embarquée dans la solution eGambit protègent de nombreuses infrastructures sensibles de multinationales. Cette technologie innovante a obtenu une récompense internationale via une évaluation de tiers indépendants avec des tests reconnus, remportant ainsi l'Award de la meilleure des solutions dans la catégorie d'analyse des menaces en temps réel. En effet, son Intelligence Artificielle et tous les capteurs déployés à l'échelle d'une grande infrastructure, sont capables de repérer des virus, des outils d'espionnage, des bombes logiques inconnues, des événements à risque et des comportements anormaux.

TEHTRIS a aussi été décorée du Label France Cybersecurity en 2015, et du Trophée de l'Innovation en France au IT Innovation Forum en 2016. Au niveau du Service Public, eGambit est directement disponible dans le catalogue de la centrale des achats UGAP (Union des Groupements d'Achats Publics).

Dario BARDI
Directeur Général
Mail : dbardi@urbaco.fr
Tél. : 06 37 99 82 24

CAME URBACO
457, Avenue Du Clapier -
84320 Entraigues-Sur-La-Sorgue

www.urbaco.com

CAME URBACO

Solutions de contrôle d'accès et de sécurité des zones urbaines par bornes escamotables.

Acteur historique et incontournable dans le Monde, Came Urbaco conçoit, fabrique, entretient et vend des solutions technologiques pour partager et délimiter les zones urbaines, résidentielles ou non-résidentielles, mais également pour protéger les sites sensibles où le besoin de sécurité des bâtiments et des personnes est crucial. Il fournit à ses clients des produits mais aussi de l'accompagnement de projet à la mise en service en passant par la formation et l'entretien.

Des solutions SAFE AND SMART CITY

La vision de Came Urbaco est de proposer un environnement urbain sûr et confortable pour les personnes, au quotidien. Se promener, travailler, visiter, courir, faire du vélo, en toute sérénité est une priorité. La sécurité des industries et des sites sensibles est plus que jamais devenue un enjeu majeur sur le plan national et international. Came Urbaco apporte des solutions urbaines pour le contrôle d'accès et la sécurité en fonction des besoins des villes. C'est dans cet esprit que la marque a développé une large gamme de produits destinés au contrôle d'accès et à la mise en sécurité des sites et infrastructures sensibles, en développant une offre de bornes Haute Sécurité résistantes aux attaques de camions béliers.

Innovation CAME URBACO : 1er fabricant français de bornes Haute Sécurité certifiées suivant les derniers référentiels internationaux

Après un grand travail d'innovation, les bornes Haute Sécurité de la gamme ONEevo, conçues et fabriquées par Came Urbaco, sont aujourd'hui toutes homologuées selon les dernières normes Internationales IWA14-1 : 2013, PAS68:2013, DOS et ASTM.

Des crash-tests (certifiés) ont montré leur capacité à répondre aux trois niveaux de sécurité suivants :

Nos Références

Nice et sa Promenade des Anglais, le canal de Panama, plusieurs postes-frontières en Pologne ou la Préfecture de Police de Paris comptent parmi les lieux équipés de telles bornes. En France, environ une borne escamotable sur trois est une borne Came Urbaco.

CRASH TESTED PAS 68

CRASH TESTED IWA 14-1

Notes

Le GICAT, groupement professionnel créé en 1978, compte plus de 220 adhérents, grands groupes, ETI et PME. Ces adhérents couvrent un large spectre d'activités industrielles, de recherche, de services et de conseil au profit des composantes militaires et civiles, nationales et internationales impliquées dans la sécurité et/ ou la défense terrestres ou aéroterrestres. Le GICAT représente les intérêts des industriels français de la Défense et de Sécurité terrestres et aéroterrestres autour de quatre objectifs :

- Organiser le dialogue entre institutionnels et industriels du secteur
- Offrir des services à ses adhérents pour favoriser leur développement en France et à l'international
- Créer un environnement favorable aux échanges entre industriels
- Valoriser les savoir-faire et l'image de l'industrie du secteur

Le rayonnement international du GICAT s'appuie sur les salons internationaux EUROSATORY en France, Expodefensa en Colombie et ShieldAfrica en Côte d'Ivoire, organisés par sa filiale le COGES, ainsi que sur un certain nombre de salons de défense et/ou de sécurité à l'étranger.

www.gicat.com

La FIEEC rassemble 22 syndicats professionnels dans les secteurs industriels et technologiques de l'électricité, de l'électronique, du numérique et des biens de consommation. Les secteurs qu'elle représente regroupent plus de 3000 entreprises, emploient près de 420 000 salariés et réalisent plus de 98 milliards d'euros de chiffre d'affaires dont 46 % à l'export.

A la source et au cœur de la transformation numérique, les groupements membres de la FIEEC rassemblent les entreprises fournissant les technologies et les solutions de sécurité numérique (identité numérique, cybersécurité, traçabilité, sécurité physique/contrôle d'accès, vidéosurveillance,...), ainsi que les entreprises intégrant ces technologies et solutions dans leurs offres « smart » (smart grids, smart industry, smart building, smart city smart health, smart mobility, smart life,...).

La FIEEC a pour mission de représenter la profession et d'agir pour une :

- Stratégie industrielle au service de la croissance
- Compétitivité au service de l'emploi
- Innovation au service des marchés du futur

www.fieec.fr

Réalisé en liaison avec le CoFis

Le Comité de la filière industrielle de sécurité (CoFIS) a été mis en place par le Premier ministre en octobre 2013. Il a pour ambition de fédérer les efforts de l'État, des collectivités territoriales, de l'industrie, de la recherche et des grands opérateurs publics et privés, pour développer des solutions de sécurité efficaces et mondialement reconnues.

La filière agit au sein d'un marché international très porteur qui couvre des sujets aussi divers que la protection des grandes infrastructures publiques et privées, la sécurité des transports, la gestion des frontières, le secours aux personnes, la lutte contre le terrorisme et la grande criminalité, la gestion de crise ou la cybersécurité. Comme tous les comités de filière soutenus par le gouvernement, le CoFIS vise à développer la compétitivité de nos grands groupes et PME, qui occupent sur le marché de la sécurité une place de premier plan.

www.cofis.fr

Réalisé en partenariat avec le CDSE

Créé il y a plus de 30 ans, le Club des Directeurs de Sécurité des Entreprises (CDSE) dispose d'une solide expérience dans le domaine de la sécurité/sûreté d'entreprise. Il collabore avec plus de 116 entreprises présentes dans 190 pays.

Le CDSE, c'est...

- un espace d'échanges entre acteurs de la sécurité/sûreté
- un espace de réflexion au service des entreprises
- un vecteur de diffusion de la connaissance en matière de sécurité
- une force de proposition auprès des pouvoirs publics

www.cdse.fr