essecome ONLINE 04/21

40 ANNI 1981 - 2021

Periodico digitale di informazione di security & safety

2021 · ANNO XLI

ENTRA NEL FUTURO.
SCOPRI L'APPROCCIO EVOLVING SECURITY (ES) DI INIM.

Evolving Security (ES) è il nostro **nuovo payoff**, associato al logo Inim, che esprime l'identità di un'azienda in continua evoluzione.
Ma c'è di più.
ES è anche un approccio che testimonia il rinnovamento in atto dei prodotti e dei servizi Inim.
Parliamo dei numerosi prodotti che sono stati reingegnerizzati, di molti altri che lo saranno a breve e di tutti i nuovi prodotti Inim che nasceranno sotto il marchio ES.
Prestazioni. Sicurezza. Affidabilità. Qualità. Semplicità.
Sono questi i punti di forza alla base della grande operazione di rinnovamento, firmata Inim.
A garanzia di questo nuovo livello di prestazioni - offerto da tanti prodotti Inim - troverai sull'imballo del prodotto e sul prodotto stesso, il logo ES in versione stampata o sotto forma di etichetta rimovibile.
Quali sono le novità dei prodotti ES?
I seguenti prodotti (i primi di una lunga serie) sono già in produzione e offrono prestazioni avanzate di tipo ES.

Prime
Il nuovo hardware delle centrali Prime è già dotato di queste caratteristiche. Più prestazioni, grazie alla portata del BUS aumentata ed a una maggiore resistenza a condizioni ambientali estreme ed a fattori di disturbo. Più sicurezza e affidabilità, grazie al nuovo sistema antisabotaggio.
Air2-KF 100, KF Ergo e KF Pebble
Questi radiocomandi - già in produzione da settembre 2020 - hanno aumentato notevolmente la portata via radio, migliorando le prestazioni e, di conseguenza, la sensazione di affidabilità e sicurezza.
Nexus/4G
Fin dalla sua prima uscita sul mercato, il comunicatore Nexus/4G offre alte prestazioni in termini di portata e protezione, identiche a quelle delle nuove centrali Prime.
Sol 2.0
Stiamo per assistere ad una notevole evoluzione delle centrali Sol 2.0: una rinnovata sezione via-radio che, finalmente, oltrepassa i limiti di cui soffriva Sol e ci pone avanti a molti altri brand sul mercato.
Flex5/S
Prossimo all'uscita, il nuovo modulo Flex5S (al posto dell'attuale Flex5) che apporta innovazioni in fatto di BUS, sicurezza dell'aggiornamento FW e terminali.
InimTech Security e Inim Home
A breve, sarà introdotto l'aggiornamento delle app InimTech Security e Inim Home, con 4 importanti novità.
1. **Attivi un nuovo impianto Sol da app InimTech Security.** E in più, programmi e modifichi i parametri di un impianto già attivo.
2. **Arruoli le centrali Sol al Cloud** in modo molto più semplice e rapido: appena connesse, le centrali Sol sono già su Cloud.
3. **Inviti gli utenti finali via InimTech Security** tramite notifiche da app installatore ad app utente. Senza necessità di connettersi al Cloud via web.
4. **Con la app Inim Home, l'utente finale riceve la notifica push** relativa all'invito dell'installatore. Quindi, l'utente può scegliere di accettare e gestire subito la sua centrale, con la possibilità di invitare anche altri utenti.

Aria/HG
Anche le tastiere Aria/HG si preparano ad introdurre una serie di interessanti innovazioni, relative al BUS: le stesse disponibili sulla nuova Prime.
Marilyn More
La nuova versione del sistema vocale integrato Marilyn, **Marilyn More**, introduce il nuovo approccio **Smart Home**, reso disponibile da Google e Amazon. Così, gestire la sicurezza e la domotica diventa davvero semplice.

Sommario Interattivo

CLICCA SULL'ICONA PER SCARICARE L'ARTICOLO CHE TI INTERESSA

Cybersecurity, non si dica più "non sapevo" e "non pensavo"

È un bene che si stia finalmente parlando della sicurezza informatica dei dispositivi in rete come un problema da affrontare con serietà, in particolare se questi dispositivi sono telecamere piazzate nei siti sensibili del nostro paese.
Altrove lo avevano fatto da tempo e davvero non si capisce perché la questione non dovesse interessare anche l'Italia.
In questo momento, è tuttavia importante evitare semplificazioni di comodo che potrebbero deviare l'attenzione dagli aspetti fondamentali del problema, con un'ovvia premessa: la vulnerabilità cibernetica riguarda ogni oggetto dotato di un indirizzo IP - come ben sa chiunque operi in qualsiasi ambito dell'elettronica e dell'informatica – e non solamente quelli prodotti in un dato paese o da taluni fabbricanti.
Detto questo, il primo aspetto da tenere presente è che la cybersecurity non deriva da un componente in più o in meno a bordo del singolo dispositivo ma, come dicono gli esperti, è l'effetto di un processo che inizia dalle fasi di progettazione *(security by design)* e continua durante l'intera vita operativa di quel dispositivo, a cura del produttore e dell'ecosistema che arriva fino all'utente finale.
Questo significa anche che si potrebbe trovare un prodotto non sicuro "made in qui" e, almeno in teoria, uno molto sicuro "made chissà dove".
Il secondo aspetto deriva proprio dal fatto che la cybersecurity richiede un approccio integrato, con il coinvolgimento e la responsabilizzazione di tutti gli attori della filiera a valle dei fabbricanti: dai distributori che scelgono le marche e i prodotti da mettere in catalogo, ai progettisti ed agli installatori che suggeriscono ai propri clienti cosa mettersi in casa.
E questi ultimi non sono esenti da responsabilità, specie se hanno il compito di gestire la sicurezza o le operazioni di un'organizzazione, pubblica o privata che sia.
Un terzo aspetto è che tutto questo è regolamentato a chiare lettere da normative internazionali e leggi nazionali in vigore da anni, che delineano non solo i criteri qualitativi dei sistemi e delle procedure, ma identificano anche i soggetti che hanno l'onere di attuarli stabilendo le sanzioni che colpiscono non tanto la mera violazione di prescrizioni ma, piuttosto, l'eventuale inadeguatezza delle soluzioni adottate per la sicurezza degli aventi causa.
Dal momento che *"ignorantia legis non excusat"*, nessuno può chiamarsi fuori e dire "non sapevo".
Ultimo aspetto: stiamo parlando, è vero, di sicurezza di dati personali e aziendali ma, in questo momento, non possiamo non pensare a quali conseguenze estreme possa portare quella "inadeguatezza delle soluzioni adottate" quando riguarda la sicurezza delle persone. I principi di consapevolezza e di responsabilizzazione sono i medesimi.
Quindi, anche nella cybersecurity nessuno dovrebbe più permettersi di dire "non pensavo".

Meccanica Quantistica, la nuova frontiera per Cybersecurity e sicurezza delle comunicazioni

intervista a Luca Ciciriello, (Torino, 1968). Fisico teorico che si occupa di calcolo e computer quantistici a livello industriale e soprattutto in ambito Cybersecurity. Autore di pubblicazioni scientifiche sulla gravità quantistica e l'innovazione tecnologica degli algoritmi quantistici in ambito Machine Learning (Quantum Machine Learning) e Security (Quantum Cryptography)

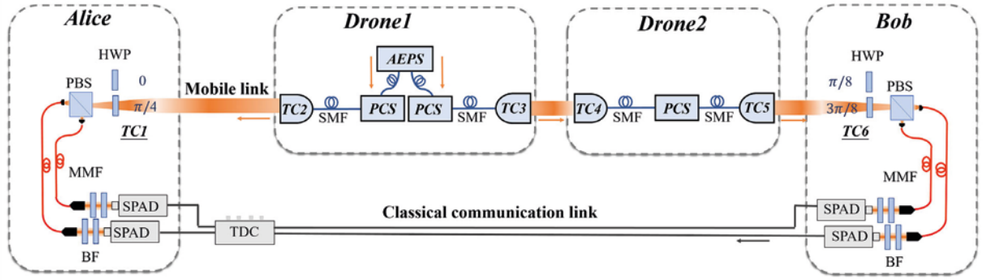
Ci può introdurre alla metodologia QKD che utilizza concetti di Meccanica Quantistica per la sicurezza delle comunicazioni?

La QKD, che sta per Quantum Key Distribution, è uno dei meccanismi per garantire la sicurezza nelle comunicazioni utilizzando concetti di Meccanica Quantistica (Quantum Cryptography). Attraverso la QKD, vengono abilitate due parti a produrre e a condividere una chiave segreta random da usare per crittare e decrittare i messaggi che vorranno scambiarsi. Il vantaggio di questa tecnica è di avere una "sicurezza intrinseca", cioè non dipendente dalla potenza di calcolo messa in campo da un eventuale attaccante. Questo ci consente sia di rilevare la presenza di una terza parte *(eavesdropper)* che tenta di ottenere informazioni sulla chiave, sia di impedire a questa terza parte l'ottenimento di tali informazioni.
La QKD è utilizzata solamente per generare e distribuire la chiave di crittatura e decrittatura, non per trasmettere alcun messaggio; la trasmissione del messaggio avverrà per i canali classici di comunicazione (LAN).

Cosa intende quando parla di "sicurezza intrinseca"?

La sicurezza intrinseca dei sistemi a trasmissione quantistica risiede in un semplice principio base che si può esplicitare in due punti: primo, l'informazione in ogni sistema fisico è finita e, secondo, si può ottenere sempre nuova informazione su un sistema fisico modificando quella esistente.
Quindi, quando acquisiamo nuova informazione su un sistema (ovvero effettuiamo una misurazione), poiché l'informazione rilevante totale non può crescere indefinitamente (primo punto), ne segue che ogni misurazione modifica in qualche modo l'informazione totale, rendendone irrilevanti alcune parti e più significative altre.
È per questo motivo che in Meccanica Quantistica, quando interagiamo con un sistema, in generale non solo acquisiamo parti di informazione su quel sistema ma, allo stesso tempo, "cancelliamo" o modifichiamo una parte dell'informazione sul sistema stesso.
Pertanto se, ad esempio, io sto trasferendo informazione da A a B, se C intercetta questa informazione (osserva il sistema eseguendo una misurazione), l'informazione trasferita cambia e il messaggio che A voleva trasferire a B e che è stato intercettato da C non è più coerente e diventa quindi inutilizzabile sia da B che da C. In termini implementativi, la chiave quantistica (un insieme di fotoni con uno stato quantizzato di polarizzazione) viene distribuita su un canale ottico che può essere una fibra, o attraverso un laser rimbalzato da una serie di specchi (rimbalzi satellitari o terrestri). La soluzione "on-the-air" (con specchi) è sempre preferibile in quanto comporta meno errori dovuti a disomogeneità ed assorbimento da parte della fibra. Per applicazioni di trasmissione di dati sensibili in condizioni di emergenza è possibile utilizzare dei droni come ripetitori del segnale laser che trasporta la chiave quantistica criptata[1]. La figura qui sotto schematizza una tipica architettura QKD con l'utilizzo di droni.

[1] www.researchgate.net/publication/348538158_Optical-Relayed_Entanglement_Distribution_Using_Drones_as_Mobile_Nodes



E' una tecnologia già disponibile sul mercato? Quali sono gli utilizzatori attuali?

Sì, certamente, è una tecnologia consolidata e utilizzata a livello industriale. Ad oggi, ci sono almeno quattro aziende nel mondo che possono fornire un'offerta di prodotti QKD "chiavi in mano". Queste aziende sono la svizzera **ID Quantique**[2], la statunitense **MagiQ Technologies**[3], l'australiana **Quintessence Labs**[4] e la francese **SeQureNet**[5].
L'azienda svizzera è sicuramente la capostipite. È la prima, con più di dieci anni di esperienza. È nata come spin-off dell'università di Ginevra. Ha in catalogo una serie di prodotti specifici, da generatori quantistici di numeri casuali (QRNG) a piattaforme QKD vere a proprie, basate sul protocollo BB84 o COW.
Senza fare nomi, anche un paio tra i più grandi istituti bancari italiani utilizzano oggi la tecnologia QKD per le loro transazioni più delicate.

E' possibile stimare i costi da sostenere per l'impiego di QKD a livello commerciale? Quali infrastrutture e dispositivi sono necessari?

Come detto in precedenza, oltre al normale canale di trasmissione del segnale criptato, è necessario avere un canale ottico (fibra/laser-on-the-air) collegato ad un set di trasmissione e ricezione che comprende un generatore casuale di chiavi e un sistema di polarizzazione dei fotoni trasmessi.
Ad oggi, questo sistema è realizzato da schede apposite che possono risiedere all'interno delle stesse macchine usate per la trasmissione classica del segnale, oppure su macchine dedicate (collegate con le principali).
Non ho elementi per quantificare con precisione il costo di un'infrastruttura completa, ma ritengo che la maggior parte delle spese riguardino la realizzazione della seconda linea dedicata in fibra o tramite collegamento satellitare/terrestre per trasmettere la chiave criptata.

Ritiene sia applicabile a sistemi di sicurezza fisica, quali ad esempio, impianti di videosorveglianza e controllo accessi in siti sensibili?

Il CASD (Centro Alti Studi per la Difesa) e il CeMiSS (Centro Militare di Studi Strategici) stanno già studiando ed implementando sistemi di questo tipo, che riguardano principalmente tecnologie di IoT e per le comunicazioni satellitari strategiche .
In campo civile, penso che non ci siano limitazioni di sorta all'utilizzo della tecnologia QKD. Grazie alla sua versatilità di affiancamento a sistemi classici già esistenti (gli algoritmi di codifica/decodifica della chiave sono algoritmi quantistici che girano su computer classici), questa tecnologia può benissimo essere impiegata per rendere inattaccabili sistemi di videosorveglianza preesistenti di siti sensibili.
In più, come detto all'inizio, se si deve presidiare in condizioni di emergenza un sito mobile temporaneo e trasmettere dati sensibili, è possibile impiegare un ponte ottico formato da uno o più droni.

[2] www.idquantique.com
[3] www.magiqtech.com
[4] www.quintessencelabs.com
[5] www.cbinsights.com/company/sequrenet
[6] www.difesa.it/SMD_/CASD/IM/CeMiSS/DocumentiVis/Rcerche_da_pubblicare/Pubblicate_nel_2019/AO_SMD_06_ITA.pdf

Presente e futuro della security dei data center, dal building ai satelliti passando per l'edge computing

intervista a Marco Carboni, technical security manager

Possiamo fare un punto sullo stato dell'arte della sicurezza dei data center, che qualcuno definisce l'infrastruttura "più critica" in assoluto?
Per fare il punto bisogna considerare le attuali tendenze di crescita di questo settore e dell'edge computing nel breve futuro.
L'argomento sembra semplice a prima vista, in realtà le problematiche che si riferiscono ai dati sono molteplici e investono vari aspetti, dalla loro integrità e disponibilità fino alla loro veridicità. Di conseguenza, riguardano anche i "contenitori" che sono, appunto, i data center (DC).
Intanto, dobbiamo dire che esistono diversi standard internazionali che, tutti insieme, dovrebbero "blindare" correttamente il settore dei DC ma, purtroppo, non è così.
Tra questi, gli standard di riferimento sono TIA 942 e EN 50600 che dedicano uno specifico capitolo alla sicurezza fisica. Entrambi, però, si concentrano sulla struttura del DC, ovvero sul "contenitore", con un approccio molto sbilanciato verso la progettazione del building trascurando gli aspetti gestionali della security.
Non entrando nello specifico della problematica, rimandano gli aspetti di security ad ulteriori standard (controllo accessi, videosorveglianza, antintrusione, ecc) e, non ultimo, al Risk Management al quale, in realtà, si dovrebbero dedicare maggiori energie.
Va inoltre fatta una distinzione tra DC *"in house"* e società che offrono servizi DC a terzi. Sarebbe lecito attendersi che quest'ultimi siano più aderenti ai suddetti standards ma poi avvengono eventi, come **quello di OVH** a marzo di quest'anno in Francia, che ci smentiscono subito.
Ma perché oggi i DC sono diventati così strategici? Molto semplicemente perché contengono il bene più importante per le aziende dopo le risorse umane, ovvero le informazioni.
Oggi, un'azienda che vuole rimanere sul mercato necessita di informazioni puntuali e veloci per essere sempre in grado di soddisfare le necessità del cliente e cogliere ogni piccolo segnale di cambiamento, come viene ben rappresentato

dal modello di "società esponenziale" (consiglio di leggere *"Exponential Organizations"* di Salim Ismail).
Alla stessa stregua, è fondamentale che queste informazioni siano ben custodite e sempre disponibili. Basti pensare a cosa è successo poco tempo fa con il fermo di alcuni servizi di Amazon a livello mondiale.

Possiamo delineare le relazioni tra cybersecurity e sicurezza del DC?
E' fondamentale non confondere la cybersecurity con l'integrità dei dati in quanto, spesso, si pensa erroneamente che basti occuparsi di cyber per disporre di dati "corretti".
Da qui la scelta di molte aziende di intraprendere la via di soluzioni ibride o ridondate su più DC per l'archiviazione delle informazioni, spostando quindi presso terzi i propri dati per abbattere i costi e i problemi dovuti all'implementazione di un DC in house ricercando, nello stesso tempo, maggiori prestazioni.
Purtroppo, avere un DC in house comporta costi abbastanza elevati, specialmente se si vuole salire la scala dei TIER che identifica la capacità di resilienza del data center dal punto di vista della struttura ma, essendo l'Italia basata su piccole e medie imprese, spesso mi sono imbattuto in DC che presentavano vistose problematiche di sicurezza fisica.

C'è pure chi sostiene che, dal momento che i dati sono cifrati e ridondati su più DC, non sarebbe necessario implementare sistemi particolarmente sofisticati di sicurezza fisica dimenticando che, in questo modo, si possono generare disservizi dovuti ad accessi "non desiderati" che potrebbero essere fatali per l'azienda.
Quindi, se il DC è il "forziere" dove teniamo le nostre informazioni, diventa di per sé l'infrastruttura critica dell'azienda, da proteggere in modo adeguato e con tutte le attenzioni del caso.

Dal suo punto di vista, cosa si dovrebbe fare per migliorare il quadro attuale?
Per i DC di terzi mi verrebbe da dire "fare bene il cliente"; per quelli in casa, di dotarsi di figure professionali (consulenti o dipendenti) che sappiano padroneggiare le complesse problematiche di sicurezza fisica in ambito DC.
Nel caso di DC che offrono servizi a terzi, è necessario effettuare più di una visita al centro, verificare i livelli di ridondanza e affidabilità prefissati sia in fase di progettazione che di esercizio, visionare le policy e le procedure del sito e, infine, effettuare degli audit annuali o addirittura semestrali basati almeno sui punti predetti, definendo il modo ed i livelli attesi di operatività con il fornitore del servizio.
Tale pratica può aiutare sia chi fornisce il servizio, sia chi lo riceve ed un episodio come quello accaduto quest'anno a Strasburgo sarebbe stato più contenuto e meno devastante.
Ma non basta: in questo ambito è necessario un costante aggiornamento sulle tecnologie, dall'intrusione fino al sabotaggio. E' quindi consigliabile dotarsi di un network internazionale di informazione, che possa fornire aggiornamenti sullo stato dell'arte con esperti del settore di cui potersi "fidare". Anticipando che sto lavorando ad un progetto di divulgazione e formazione su questi temi, spero si sia notato che, a mio parere, l'aggiornamento sullo stato dell'arte della sicurezza dei DC debba riguardare necessariamente tutte le tre dimensioni della security: fisica, logica e HR.

Cosa ci dobbiamo aspettiamo per il futuro?
L'arrivo del 5G sicuramente costringerà buona parte di fornitori di servizi a duplicare molta dell'intelligenza dai DC nell'edge computing, se vogliono mantenere adeguati livelli di servizio superando i "colli di bottiglia" delle infrastrutture di rete.
Questo è un fenomeno già presente negli USA dove, alla base delle antenne GSM incominciano ad esserci, oltre alle BTU, veri e propri DC in miniatura. E' molto probabile che in Italia questo schema avrà un'importante espansione, considerando la conformazione montuosa del territorio, l'alto numero di PMI presenti sul mercato e, infine, le poche infrastrutture disponibili (dorsali e DC)
A questo punto, si aprono diversi problemi legati sia alla sicurezza che all'integrità fisica dei dati stessi, per non parlare dei problemi reputazionali dovuti ai disservizi causati dagli assalti a questi sistemi remoti.
Finora venivano rubati cavi e batterie, domani saranno router, firewall e computer con un innalzamento della "qualità" del furto e del danno, ma è inevitabile arrivare ai furti di dati veri e propri.
Proteggere un DC è una cosa, proteggere un edge computing posto per strada in un container è tutt'altro, sia dal punto di vista della tecnologia da impiegare che dei tempi di risposta e delle modalità di protezione dei dati.
Il prossimo futuro sarà l'utilizzo dei satelliti, un fronte nel quale si sta già muovendo Starlink di Musk e si incomincia a parlare di *"Cyber-Sat"*.
Sarà una bella sfida per i prossimi anni per chi si occupa di security.

Hanwha Techwin

hanwha-security.eu/it

WISENET 7

Innovazione ed Eccellenza

Scopri come Hanwha Techwin ha nuovamente superato un traguardo tecnologico fissando di fatto un nuovo livello di standard nella Videosorveglianza Professionale per qualità delle immagini, capacità di processo e livello di cybersecurity delle telecamere.

Contattaci per sapere come Wisenet7 può aiutarti a sviluppare oggi soluzioni di videosorveglianza per le esigenze di domani, garantendo **qualità delle immagini** e **sicurezza end-to-end**.

Qualità ed Eccellenza

- Risoluzione fino a 4K
- WDR e Algoritmo di riduzione del rumore avanzati
- Smart codec Wisestream II

Cybersecurity ed Innovazione

- Certificazione UL CAP & Secure by Default
- Firmware Encryption
- Secure Boot Verification
- Secure Firmware
- Secure JTAG
- Video Storage Back-up Encryption
- Private Certificate

OPTEX Sensing Innovation

REDSCAN Pro

SERIE LIDAR PER INTERNO/ESTERNO A LUNGO RAGGIO

Modelli Disponibili:
RLS-50100V: 50 x 100 m
RLS-3060V: 30 x 60 m

Estremamente affidabili e versatili, i sensori di sicurezza REDSCAN PRO utilizzano la tecnologia LIDAR per creare un vero e proprio muro laser virtuale con portata fino a 100 m di lunghezza. La soluzione ideale per proteggere perimetri, edifici, tetti e beni, anche per siti a rischio elevato.

Impieghi

Capannoni

Centrali elettriche

Tetti

Caratteristiche

- ✔ **Regolazione automatica della zona**
- ✔ **Pet Immunity**
- ✔ **Funzionamento in ogni condizione ambientale**
- ✔ **Telecamera per visualizzazione dell'area di rilevazione**
- ✔ **Staffa con regolazione angolo integrata**

HESA®
www.hesa.com

Security by design dei dispositivi di sicurezza fisica: la risposta di Genetec

intervista a Gianluca Mauriello, Regional Sales Manager Italia, Genetec Inc.

L'aumento della consapevolezza da parte degli utilizzatori finali dei rischi cyber dei dispositivi in rete riporta l'attenzione sulle garanzie offerte dai produttori in materia di "security by design". Qual è la linea di Genetec su questo tema?

Genetec pone la privacy e la sicurezza informatica al centro del proprio processo di R&D, con lo scopo di rendere sicuri i sistemi e le reti. Inoltre, forniamo gli strumenti e le funzionalità che permettono al cliente finale di tutelare l'investimento fatto. Ad esempio, i nostri sistemi avvisano l'amministratore quando rilevano che il firmware di un dispositivo non è aggiornato e permettono sia di aggiornarlo dalla piattaforma di gestione, che di conoscere costantemente il livello di sicurezza in base a come è configurato il sistema.

Le nostre misure integrate di privacy e cybersicurezza includono vari livelli di difesa come la crittografia, l'autenticazione multi-layer e le autorizzazioni. Le nostre soluzioni permettono inoltre di oscurare le identità degli individui in video, di automatizzare le politiche di conservazione dati e condividere in modo sicuro le informazioni durante le indagini. Dal dispositivo all'applicazione client, queste funzionalità garantiscono una protezione dalle minacce informatiche e dall'accesso non autorizzato, assicurando al contempo il rispetto costante della privacy.

In che modo informate il canale distributivo delle caratteristiche dei vostri prodotti in materia di cybersecurtiy, affinchè possano a loro volta presentarli correttamente ai rispettivi clienti?

Prima che esca una nuova release inviamo una Newsletter dedicata che riporta tutti gli aggiornamenti fatti. Su un piano "fisico", invece, i nostri Trainer visitano i distributori e li formano rispetto alle nuove caratteristiche e funzionalità delle release in arrivo.

Poi, per garantire un apprendimento continuo, c'è ovviamente la parte "Genetec training" che ora, a causa delle restrizioni imposte dal Covid-19, propone esclusivamente sessioni online. Distributori, System Integrator e clienti possono avere accesso a qualsiasi tipo di materiale per approfondimenti sulle soluzioni Genetec e corsi per la certificazione tecnica in inglese.

Infine, su invito specifico e con i nostri trainer francesi o americani, organizziamo webinar su cybersecurity e altre tematiche di interesse, anche in collaborazione con i nostri partner tecnologici, per restare al passo con le evoluzioni e gli sviluppi della nostra piattaforma.

Gradualmente stiamo sviluppando anche materiale ed eventi in lingua italiana.

Le vostre diverse linee di prodotto offrono le medesime garanzie in materia di cybersecurity o sono diversificate in relazione alla destinazione d'uso o livelli di gamma?

Per quanto riguarda la cybersecurity e, quindi, appunto la "security by design" di tutte le nostre soluzioni software, la garanzia di cybersecurity è la medesima per tutte le linee di prodotto: che si tratti della versione Standard, Professional o Enterprise. La piattaforma è la stessa, cambiano ovviamente solo le funzioni rispetto a quelli che sono gli obiettivi del cliente.

Per quanto riguarda Streamvault™ e l'infrastruttura server, pre-configuriamo oltre 200 setting di sicurezza per proteggere ogni parte dell'infrastruttura. Esiste persino una guida a questa attività di "hardening" affinchè chiunque possa prendere spunto e rendere i propri server ancora più sicuri.

Genetec lavora per offrire un livello di massima affidabilità in tutte le soluzioni lanciate sul mercato, a prescindere dal fatto che tali soluzioni siano on-premise, sul cloud, o ibride. La nostra missione è anche quella di proteggere le persone, le aziende e le comunità.

Contatto:
Gianluca Mauriello,
Regional Sales Manager Italia, Genetec Inc.
Tel. +39 327 739 8560
www.genetec.com

Da Bettini Video videosorveglianza made in Italy e impegno per la cybersecurity della filiera

intervista a Walter Bettini, CEO di Bettini srl

Ci può riassumere la storia e l'attuale struttura di Bettini?
L'azienda Bettini è stata fondata nel novembre del 1996 da mio fratello Massimo Bettini insieme a me, Walter. Inizialmente eravamo impegnati nella sola distribuzione, ma eravamo stimolati dall'intuizione che la videosorveglianza avrebbe beneficiato, di lì a poco, di un futuro molto interessante, sia dal punto di vista delle tecnologie che della diffusione.
Forti di questo, in breve tempo abbiamo potuto annoverare nel nostro organico figure con specifiche competenze nel settore della sicurezza ed una spiccata conoscenza del comparto della TVCC, diventando molto rapidamente un punto di riferimento in un settore in continua e rapida evoluzione.
Passione, entusiasmo, competenza ed impegno erano i nostri valori fondanti.
Nel 2004 abbiamo acquisito il marchio GAMS, pioniere, parallelamente a Comerson, nella produzione tutta Italiana di videoregistratori digitali: si apriva una nuova era digitale.
Alla fine del 2007, abbiamo deciso di incorporare anche il ramo d'azienda della società Initel, costruttore dei prodotti a marchio GAMS.
Iniziava così il percorso di sviluppo che ci ha portato progressivamente alla progettazione di nuove gamme di prodotti e soluzioni con caratteristiche innovative, che hanno consolidato la nostra presenza sul mercato domestico, soprattutto nel mondo bancario, ma non solo, che allora era in forte espansione territoriale.
Alla produzione GAMS, si affiancava, e tutt'ora si affianca, la distribuzione di marchi presenti a livello mondiale, quali Avigilon, Comnet e Flir, che ci consentono di offrire soluzioni complete ed integrate a 360° in partnership con i principali produttori di sistemi di centralizzazione e di supervisione.
Oggi, l'azienda ha un organico di circa 50 persone con la sede principale a Saronno che si estende su circa 5.000 mq e

comprende le unità di R&S e Produzione; da qui nascono le idee e prendono forma i prodotti GAMS, con progettazione e produzione orgogliosamente "made in Italy".
Tre sono le filiali in Italia: Bologna, Firenze e Roma, a cui si aggiungono l'agenzia di Palermo ed i distributori in Sardegna e Piemonte, per offrire presenza commerciale e supporto tecnico capillare in tutta Italia.
Nel 2020 è iniziata l'esperienza estera che, con notevole successo, ci consente di acquisire importanti commesse anche fuori dai confini europei.
Molta attenzione è sempre riservata alla qualità: Bettini è certificata ISO 9001:2015 e ISO 14000:2015, quest'ultima voluta per l'attenzione e la sensibilità che poniamo verso l'ambiente. Altrettanta attenzione viene posta alla Privacy, con la presenza in azienda di una figura con il ruolo di Privacy Officer, certificata dal TUV, per offrire costante supporto e consulenze specifiche ai nostri Clienti, in una materia sempre più complessa, articolata e in continuo aggiornamento.

Quali sono i programmi e quali linee di prodotti proponete in questa particolare fase del mercato della sicurezza fisica?
L'anno appena trascorso, oscurato dalla sciagura della pandemia, ci ha visti molto impegnati nelle forniture di prodotti legati ai concetti di safety, attraverso l'utilizzo degli ormai tristemente famosi termoscanner e lettori, assieme a soluzioni di distanziamento sociale. Oggi riprendiamo a pieno ritmo la nostra consueta attività con l'avvio di numerosi programmi come sempre sfidanti. Stiamo già lavorando allo sviluppo di una nuova video-analisi neurale con logiche d'avanguardia che verrà rilasciata entro l'anno e puntiamo a mercati dove il video è al servizio del marketing, ad esempio con soluzioni di retail analytics e, non ultime, le soluzioni BVI (Business Video Intelligence). Queste utilizzano dati video provenienti dalle telecamere per gestire processi aziendali (ad esempio nella logistica, nel finance, nel retail, etc.) creando valore aggiunto al sistema di videosorveglianza.

Come rispondete alla richiesta che sta iniziando ad emergere dalla filiera della sicurezza, di trasparenza sulla cybersecurity dei dispositivi/sistemi per la sicurezza fisica?
In realtà è un tema ricorrente da sempre. I nostri prodotti e le nostre soluzioni sono stati scelti ed utilizzati in settori molto importanti e particolarmente attenti a questo tema.
Cito ad esempio il settore bancario, il retail, la GDO, il mondo della logistica e non solo, dove siamo molto presenti; gli utenti scelgono il partner tecnologico dopo aver eseguito severissimi test sulla rispondenza alla sicurezza delle reti dei prodotti (i cosiddetti "pen-test") che consistono nel "cyber-bombardare" - consentitemi questo termine - i dispositivi in rete alla ricerca di tutte le fragilità che possono esporli ad attacchi hacker. Questi test ci aiutano a migliorare ma, ovviamente, non ci accontentiamo: noi stessi sottoponiamo i nostri prodotti a stress-test al medesimo scopo, affidati a società esterne, per poi intervenire quando necessario con gli opportuni adeguamenti.
Ci sono però altri metodi per contrastare queste attività, ovvero fare FORMAZIONE, sia tecnica che culturale. Noi da anni ormai - purtroppo nell'ultimo solo on-line - teniamo corsi e training di certificazione GAMS, i GAMS Academy, con grande successo a conferma dell'attenzione del mercato a certe tematiche.

"È necessario un impegno corale da parte di tutti gli attori seri della sicurezza, non esclusi i media, per inondare il mercato di installatori, system integrator, utenti finali, progettisti, consulenti, etc., di messaggi finalizzati a diffondere la cultura del concetto di cybersecurity"

Vogliamo per far conoscere nel modo più dettagliato possibile i nostri prodotti e le rispondenze ai requisiti necessari alla protezione, ma non basta. E' necessario un impegno corale da parte di tutti gli attori seri della sicurezza, non esclusi i media, per inondare il mercato di installatori, system integrator, utenti finali, progettisti, consulenti, etc., di messaggi finalizzati a diffondere la cultura del concetto di cybersecurity.
È una battaglia "guardia-e-ladri" che non potrà mai terminare e che vedrà sempre di più scenari inquietanti che imporranno alle aziende un continuo dispendio di energie, di risorse e di costi ingenti per rispondere sempre e costantemente, con rapidità ed adeguatezza, ad un mondo che cambia in ogni istante.
Noi ci siamo.

Quali parti o fasi di lavorazione dei dispositivi del vostro portfolio sono realizzate in Italia?
Per noi della Bettini, l'Italianità è sempre stata un grande

valore che abbiamo inteso esprimere con le nostre scelte. È per questo che tutti i prodotti a marchio Gams sono “made in Italy”, progettati e realizzati nella sede dell’azienda, confermando una grande tradizione Italiana ed una grande attenzione da sempre dedicata al comparto della TVCC.
Tutti i software ed i firmware sono sviluppati a Saronno. Questo non significa che non ci siano approvvigionamenti dal Far East, ma tutto ciò che non è prodotto da noi, ovvero la sola componentistica elettronica, è comunque realizzato secondo nostre specifiche. In Italia viene prodotta anche una quota importante dei contenitori dei dispositivi, per terminare con gli imballi completamente ecocompatibili e biodegradabili.

L’arrivo in Bettini Video di una persona con competenze specifiche in comunicazione e marketing segnala la volontà dell’azienda di aumentare visibilità e penetrazione sul mercato. Quali sono gli obiettivi che le affidate?
Da diverso tempo cercavamo una figura che si occupasse a 360° del marketing per dare maggior risalto e continuità alla comunicazione aziendale, alla brand identity e, non ultimo, per fornire un contributo al miglioramento continuo dei prodotti e dei servizi resi ai clienti, perché per noi la soddisfazione del cliente è al primo posto.
L’avvento sempre più massivo delle tecniche di comunicazione digitale ci impone la presenza comunicativa in questi canali, ma intendiamo farlo con un approccio strategico e con una pianificazione ben pensata che ci consenta di migliorare la nostra immagine aziendale e di essere appetibili per nuovi potenziali clienti.
La nuova risorsa, che ringrazio per la scelta fatta ed alla quale formulo i migliori auguri per questa sua nuova avventura in un contesto dinamico e stimolante, è una figura giovane

proveniente da settori differenti anche se sempre nell’ambito B2B; caratteristiche che abbiamo considerato al primo posto nella fase di selezione per portare all’interno nuove idee e logiche provenienti anche da altri mercati.
Aggiorneremo i nostri canali di comunicazione e ne lanceremo di nuovi, con un’impronta visiva di maggiore impatto e messaggi mirati. Nel frattempo, sarà definita una strategia a lungo termine per penetrare in nuovi segmenti di mercato e per mappare più approfonditamente il nostro target “storico”.

BETTINI
VIDEO & SECURITY TECHNOLOGY

Contatti:
BETTINI S.r.l.
Tel. +39 0289651000
info@bettinivideo.com
www.bettinivideo.com

AddSecure: protezione di dati e comunicazioni critiche in un mondo connesso

comunicato aziendale

Le soluzioni per la trasmissione di informazioni critiche in maniera sicura, certificata e facile da implementare da un **punto A** (in cui si determina un evento di allarme) ad un **punto B** (in cui 24/7 avviene la ricezione dell’allarme e le azioni conseguenti per la sua gestione), sono di importanza fondamentale per le attività umane, sociali e produttive di tutti i giorni.
Queste soluzioni aiutano, infatti, a salvare vite o a limitare gli effetti di eventi avversi sulle persone, ad aumentare la protezione di beni personali ed aziendali, nonché a sostenere servizi pubblici di primaria importanza.
Ciò che caratterizza e differenzia le soluzioni **AddSecure** sono la loro sicurezza e l’affidabilità, unite alla semplicità di utilizzo della tecnologia, rendendo così quest’ultima facilmente fruibile da parte dell’utente finale anche se si tratta di soluzioni all’avanguardia all’interno del mondo evoluto del cosiddetto “Internet delle cose” sempre connesse (IoT).
I campi di applicazione delle nostre soluzioni coinvolgono svariati ambiti ed ambienti della vita quotidiana, dalle scuole agli uffici aziendali, dalle infrastrutture di trasporto stradale, marittimo, ferroviario ed aereo a quelle di produzione trasporto energetico in rete, dalle case private ai luoghi isolati e difficili da raggiungere, dai siti in costruzione ai centri commerciali ed ai luoghi di aggregazione sociale in genere.

Pertanto, in caso di malore fisico presso il proprio domicilio oppure in caso di incendio, sia che si tratti di persone intrappolate all’interno di un vano ascensore o di altri tipi di situazioni critiche, in tutti queste situazioni è fondamentale che l’allarme e le giuste informazioni correlate possano giungere alle persone giuste nei tempi giusti per le azioni giuste da intraprendere.
Le soluzioni **AddSecure** valorizzano le attività di tutti gli operatori della filiera della sicurezza che concorrono alla migliore gestione possibile degli eventi di allarme e/o di emergenza, dagli installatori ai centri di ricezione allarmi, nel rispetto delle migliori procedure operative e normative in materia.
In particolar modo, i Centri Ricezione Allarmi, nel loro continuo percorso di evoluzione, certificazione e specializzazione possono ampliare la qualità e la gamma dei servizi offerti in modo da “chiudere il cerchio” rispetto alle prescrizioni normative che sono già in vigore ed a quelle che potrebbero essere emanate in futuro, consentendo ai committenti di ottenere la piena conformità di sistema ed operativa necessarie per condurre le proprie attività.

“Ma perché diciamo che, grazie alle soluzioni AddSecure,
è possibile la trasmissione di segnalazioni critiche da un punto A ad un punto B
in maniera sicura, certificata e facile da implementare?”

Soluzione AddSecure IRIS-4 comunicatore / ISA-4 ricevitore

Certificato ed integrato per la trasmissione di segnalazioni critiche a qualsiasi centro ricezione allarmi, **IRIS-4 440** è un comunicatore certificato **EN 54-21 CPR**, caratterizzato da un doppio vettore di trasmissione, in grado di trasmettere sia attraverso una connessione IP sia utilizzando la rete cellulare 4G, a maggiore garanzia della corretta trasmissione della comunicazione.

Adatto alla trasmissione di allarmi antifurto, antincendio e tecnici o una combinazione di questi, IRIS-4 440 offre una soluzione caratterizzata dalla semplicità e dalla flessibilità operativa, sempre in massima sicurezza grazie al protocollo proprietario AddSecure, utilizzato anche in applicazioni in campo militare e di gestione transazioni con carte di credito, mediante il quale ogni dispositivo IRIS-4 dimostra la sua autenticità utilizzando una chiave di sicurezza a 256 bit.

Un nuovo numero casuale generato dal ricevitore ISA-4 viene utilizzato per ogni verifica ciclica di sopravvivenza, quindi non è possibile sostituire il comunicatore utilizzando la riproduzione o la previsione della sequenza.

Sono anche disponibili, qualora le esigenze del sito di installazione lo richiedessero, il modello **400** (solo 4G) ed il modello **420** (solo IP).

La serie **IRIS-4 4xx** è una soluzione universale, grazie all’ampia gamma di interfacce che consente la compatibilità con tutte le centrali allarmi esistenti, di qualsiasi costruttore, ed è rinomata per l’implementazione semplice e rapida, grazie al *touch screen* disponibile di serie che consente la programmazione e la messa in servizio in meno di 3 minuti con menu di configurazione interattivi che guidano rapidamente tutto il processo di installazione.

ISA-4 è un pacchetto software con la funzione di ricevitore rispetto al comunicatore IRIS-4, consentendo ai Centri di Ricezione Allarmi (ARC) di ricevere e gestire opportunamente gli allarmi, gli eventi e le informazioni di stato provenienti in modalità certificata *“Alarm Over IP”* (AoIP).

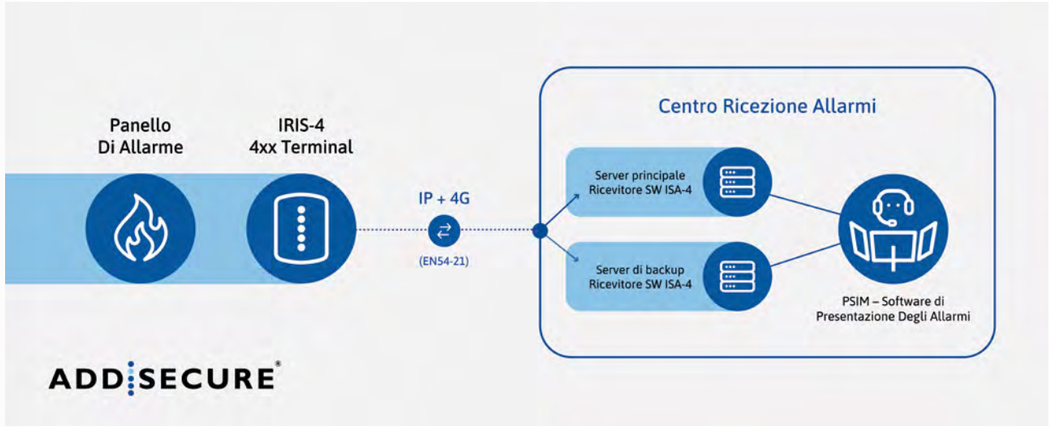
Una delle più importanti caratteristiche del software **AddSecure ISA-4** è il modo in cui vengono suddivisi i dati e fornite le informazioni a ciascuna parte interessata, in base alla funzione svolta da ciascuna di queste.

L’accesso a queste informazioni è sotto il controllo del Centro di ricezione allarmi con le funzionalità chiave:

- Multi-utenza in modalità in *multi-tasking*.
- Accesso sicuro tramite web browser standard e da qualsiasi dispositivo abilitato al web tra cui smartphone, tablet, laptop o personal computer.

AddSecure ISA-4 è stato certificato da enti indipendenti risultando conforme ai più elevati livelli di sicurezza nell’ambito degli Standard Europei (ATS 6, Grado 4) riferiti alla trasmissione di allarmi.

Ecco perché diciamo che, grazie alle soluzioni AddSecure, è possibile la **trasmissione di segnalazioni critiche da un punto A ad un punto B in maniera sicura, certificata e facile da implementare.**



Informazioni su AddSecure

AddSecure è un fornitore leader europeo di soluzioni IoT premium con particolare attenzione alle comunicazioni e ai dati critici sicuri. Più di 50.000 clienti nel settore della security e della safety, servizi di soccorso, sicurezza e automazione degli edifici, assistenza digitale, trasporti e logistica, utility, smart cities e altro ancora, salvaguardano le persone e le applicazioni business-critical con le soluzioni di AddSecure.

Questo aiuta a salvare vite umane, proteggere la proprietà e le funzioni sociali vitali e a creare affari.

Le soluzioni end-to-end sicure e affidabili all’interno delle business unit **Smart Alarms**, **Smart Care**, **Smart Grids**, **Smart Rescue**, **Smart Surveillence** e **Smart Transport**, aiutano a rendere il mondo un luogo più sicuro e più intelligente.

AddSecure ha sede a Stoccolma, Svezia, e ha uffici regionali e una rete di distributori in tutta Europa.

ADDSECURE

Contatti:
AddSecure International AB
Tel. +39 347 9977 838
marketing@addsecure.com
www.addsecure.com

G.S.S.
GLOBAL SECURITY SERVICE
SERVIZI INTEGRATI DI SICUREZZA FIDUCIARIA

La G.S.S. Global Security Service è una Società nata nel 2008 che opera esclusivamente nel settore
SERVIZI FIDUCIARI DI SICUREZZA INTEGRATA
VIGILANZA CONTROLLO ACCESSI PORTIERATO - FRONT DESK - GESTIONE SALE CONTROLLO - GESTIONI DEL RISCHIO.

Negli anni di attività la G.S.S. Global Security Service ha acquisito Clienti nei settori Bancari, Assicurativi, Energetico, Industrie Alimentari, Industrie Meccaniche, Grande Distribuzione, Centri Commerciali, Siti Petroliferi, Siti Portuale, Siti Aereoportuali, Alberghi, Squadre di Calcio Professioniste, Eventi Sportivi, Musei, Opere Religiose.

La G.S.S. Global Security Service si rivolge a tutte le Aziende e Società non solo in Italia, ma anche all'Estero offrendo e garantendo una ampia gamma di servizi di Security, Safety & Tecnology specifici alle esigenze del Cliente, fornendo Servizi e Tecnologie in tempi brevi, con l'obbiettivo ultimo di raggiungere un livello elevato di soddisfazione del cliente.

www.gsssicurezza.it

Sicurezza 4.0 con il sistema MACS Fences

L'intelligenza artificiale per recintare il tuo mondo

Con MACS Fences inizia l'era delle recinzioni intelligenti. La sicurezza passiva delle soluzioni in rete e grigliato di Nuova Defim Orsogril viene integrata da un'elettronica avanzata che porta gli standard di sicurezza ad una nuova generazione. Il risultato è un sistema esclusivo appositamente studiato per la nostra gamma in cui algoritmi elaborati ad hoc interagiscono con la recinzione in modo simbiotico ed efficiente. Discreto ed efficace, rileva puntualmente i tentativi di effrazione e scavalcamento, discriminando con grande precisione eventi naturali o accidentali. Facile da installare con la possibilità di monitoraggio da remoto.

NUOVA DEFIM ORSOGRIL
STEEL & STYLE

SEDE AMMINISTRATIVA E PRODUTTIVA
Via Cavolto, 10 - Anzano del Parco (Co)
Tel. +39 031 33521

SEDE PRODUTTIVA
Via dell'Industria, 199 - int. 1
Alzate Brianza (Co)

www.nuovadefim.com
info@nuovadefim.com

FERALPI GROUP

Perchè Rete Vigilanza Italia

intervista a Giancarlo Liberatore, Presidente Vigilanza Group e Angelo Paolo Pietroboni, Direttore Generale

Perchè Rete Vigilanza Italia? Quali sono gli obiettivi di questo progetto?
(G.L.) Abbiamo messo in cantiere il progetto Rete Vigilanza Italia per diversi motivi.
Prima di tutto, puntiamo a valorizzare e tutelare le eccellenze operative di imprenditori che oggi non possono partecipare agli appalti nazionali, sentendosi prevaricati nei propri territori dai grandi gruppi.

"Prima di tutto, puntiamo a valorizzare e tutelare le eccellenze operative di imprenditori che oggi non possono partecipare agli appalti nazionali, sentendosi prevaricati nei propri territori dai grandi gruppi"

Il secondo motivo è poter dare una risposta concreta all'evoluzione della domanda di servizi di sicurezza che, in particolare in questa fase di ripartenza dell'economia, sta richiedendo un'integrazione sempre più spinta tra tecnologie e servizi con un alto livello qualitativo uniforme sul territorio nazionale, che gli istituti di vigilanza locali difficilmente possono mettere in campo.
Un terzo motivo è l'idea di crescere insieme tra colleghi alla pari sia nei servizi di sicurezza tradizionali che in nuovi ambiti che si valuteranno congiuntamente, sfruttando anche la forza contrattuale di una realtà che copre fin dalla sua nascita gran parte del territorio nazionale, con decine di migliaia di clienti e migliaia di dipendenti

Come sarà strutturata la governance di RVI ?
(A.P.P.) Abbiamo prestato particolare attenzione alla struttura operativa e alla configurazione della Rete per garantire pari dignità ad ogni istituto aderente, valorizzandone allo stesso tempo potenzialità e peculiarità in un un'ottica di sviluppo sinergico e funzionale alla crescita della stessa Rete.
Una rete che, grazie alla sua composita estensione su tutto il territorio ed alla molteplicità di risorse alle quali può far ricorso, potrà presentarsi nelle sedi decisionali rappresentando una compagine omogenea di istituti, in grado di offrire servizi sulla base di requisiti formali, strutturali e organizzativi verificati e garantiti.
Per questa ragione, la definizione del programma delle attività della Rete sono affidate a un Comitato di Gestione formato da tanti membri quante saranno le Imprese. Il Comitato avrà il compito, tra l'altro, di fissare le linee guida e di governo della stessa Rete, nonché quello di approvare nuove adesioni armonizzandole con la struttura già presente. Il Comitato di Gestione nominerà il Presidente della Rete il quale, a sua volta, individuerà fra le imprese alcuni rappresentanti che formeranno il Consiglio di Gestione, con il compito di coadiuvare il Presidente nell'esecuzione del programma. Il Presidente designerà anche un Direttore di Rete per assicurare operatività gestionale e armonizzazione.

Quali costi devono sostenere i partecipanti e come verrà finanziata l'attività di RVI?
(G.L.) Le imprese aderenti alla Rete dovranno partecipare alla costituzione di un Fondo Comune da utilizzare per lo sviluppo della stessa Rete secondo il programma definito dal Comitato di Gestione. Pertanto, ogni impresa dovrà versare una quota mensile dei compensi fatturati ai clienti acquisiti e/o affidati attraverso la struttura della Rete, nella percentuale determinata dal Comitato di Gestione, su proposta del Consiglio di Gestione. Inizialmente, l'impresa che esprimerà protempore le figure del Presidente e del Direttore Operativo, si farà carico di finanziare costi e le spese organizzative per l'avvio dell'attività e il

funzionamento della Rete. Le aziende che subentreranno in corso di esercizio, oltre alla quota mensile dovranno farsi carico dei costi amministrativi di ingresso e registrazione dell'impresa al contratto di Rete.

"Le imprese potranno promuovere servizi di portata superiore alle proprie risorse e potenzialità anche al di fuori dal territorio di competenza autorizzato in licenza"

Come sarà articolata l'attività commerciale?
(A.P.P.) L'attività commerciale sarà aperta e libera secondo le logiche organizzative discrezionali e di territorio che ogni impresa aderente riterrà opportune. Le imprese potranno promuovere servizi di portata superiore alle proprie risorse e potenzialità anche al di fuori dal territorio di competenza autorizzato in licenza, richiamandosi, in questo caso, alla capillare organizzazione della Rete che entrerà in gioco con la sua capacità gestionale garantendo al cliente la corretta e completa esecuzione delle attività.

Per evidenti ragioni di responsabilità e garanzia di risultato, il contratto dovrà essere preventivamente approvato dagli organi di controllo della Rete e sottoscritto congiuntamente dall'impresa proponente e dal Presidente della Rete. Vigilanza Group, promotore e sostenitore di questa iniziativa imprenditoriale, metterà a disposizione della Rete il proprio staff commerciale nazionale, oggi suddiviso in quattro aree geografiche - Nord-Est, Nord-Ovest, Centro Nord e Centro Sud – con importanti potenzialità di sviluppo.

TSec compie 10 anni di ricerca e innovazione per sicurezza “made in Italy”

intervista a Giordano Turati, CEO di TSec srl

TSec compie 10 anni, un traguardo importante in un mercato in continuo e rapido cambiamento. Possiamo ripercorrere le tappe del vostro percorso?
TSec è davvero nata in un garage, grazie all’iniziativa di Alessandro Tosi e Luca Salgarelli, i due soci fondatori.
Lo stimolo venne da un furto subito in casa dei genitori di Luca. Nottetempo e ad impianto di allarme inserito, i ladri avevano eluso con grande facilità i contatti magnetici installati nell’abitazione. Da qui è nata l’idea di ricercare dispositivi e soluzioni che aumentassero il livello di affidabilità dei sensori utilizzati nei moderni impianti antintrusione. Siamo partiti proprio dai contatti magnetici introducendo in Europa la tecnologia “Magnasphere” e, dopo un anno di sperimentazione, test e varie ottimizzazioni, si è realizzata la prima gamma di sensori ad alta sicurezza certificati.
Successivamente, sono nati i sensori di vibrazione basati su un nuovo principio ibrido inerziale/magnetico e le schede di analisi per una gestione innovativa e puntuale del sistema antiscasso.
Poi, a seguito di una lungimirante intuizione, è nato il progetto Inxpect che ha portato alla nascita di una nuova società partecipata dall’attuale gruppo di soci di TSec, Inxpect S.p.A. appunto.
Da qui è nato il nostro MSK-101, un radar di nuovissima generazione pensato per la sicurezza professionale. Con le evoluzioni introdotte, oggi questo sensore ha raggiunto un livello di performance di altissima qualità riconosciuto dagli installatori più evoluti e dagli utilizzatori finali più esigenti.
L’ultimo nato nei nostri laboratori è il sistema perimetrale anti-scavalcamento Macs. Un sistema che ci sta dando grosse soddisfazioni per la sua facilità di impiego, di programmazione e per le prestazioni di rilevazione e di immunità agli agenti esterni. Si può applicare a recinzioni rigide, semirigide e a maglia sciolta.
L’inizio del nostro percorso non è stato facile, ma abbiamo avuto la fortuna di incontrare ad un certo punto installatori e distributori che hanno capito la forza del nostro messaggio di cambiamento: far nascere dal mercato della sicurezza antintrusione tecnologie forti per innalzare le performance dei sensori e dei sistemi di rilevazione.
Un’altra scelta forte sulla quale abbiamo puntato, anche a costo di risultare testardi, è stata la produzione interamente in Italia, in un momento non proprio favorevole per gli investimenti ed i costi. Tutto il processo di ingegnerizzazione e di produzione è creato e sviluppato nel nostro Paese.
Oggi il mercato ci riconosce una professionalità distintiva che ci dà la forza e l’energia per proseguire nella nostra ricerca di innovazione. Per questo siamo molto grati e riconoscenti con i nostri partner.

Qual è la vostra struttura attuale?
Dal punto di vista dell’organico, siamo una quindicina di persone, divise tra produzione e logistica, ricerca e sviluppo, marketing e commerciale. Il team è composto da figure altamente professionali, attive e partecipanti al progetto aziendale, condividendone gli obiettivi con grande determinazione e spirito di squadra: ne siamo molto orgogliosi.
Sul mercato nazionale abbiamo una rete di 34 distributori, 8 dei quali certificati con 74 punti vendita in totale. Abbiamo scelto due anni fa di stimolare i nostri partner selezionati per poter innalzare, attraverso un processo di condivisione, il loro livello di competenza sulle nostre soluzioni, per poter offrire al mercato un servizio puntuale e il più possibile professionale.
L’evoluzione dei mercati e, soprattutto, delle tecnologie esige una grande attenzione alla comunicazione attraverso la filiera. E’ nata così l’idea di certificare i distributori secondo gli standard, la professionalità e la competenza richieste per poter trattare le nostre soluzioni ad alto contenuto di innovazione tecnologica.


Alessandro Tosi


Giordano Turati

Luca Salgarelli

Quali sono i programmi per il futuro?
Per quanto riguarda i prodotti, abbiamo nel cassetto diversi progetti per sviluppare ulteriormente una serie di sensori radar intelligenti che, crediamo, rappresenteranno il futuro non solo nella rilevazione perimetrale antintrusione ma anche nei mercati affini e/o complementari alla sicurezza. L’espansione ulteriore nei mercati esteri è un’altra priorità strategica importante sulla quale stiamo lavorando da tempo su formule di partnership operative che potrebbero modificare gli schemi classici della distribuzione.
Dal punto di vista della strategia aziendale per il futuro, pensiamo che le sfide dei mercati dei prossimi anni impongano investimenti sempre più importanti in ricerca e sviluppo e nell’adeguamento dell’organizzazione aziendale ai nuovi scenari, anche in mercati verticali. Per questo valutiamo alleanze e partnership con aziende che hanno la stessa visione.

Ci può parlare della vostra partecipata Inxpect, che ha concluso di recente un importante deal finanziario?
Inxpect è partita come un’attività di ricerca e sviluppo di TSec, con l’obiettivo di dimostrare che la tecnologia radar potesse fare la differenza nel realizzare innovativi sensori di movimento per l’anti-intrusione. Presto questa attività ci ha portato a comprendere che la stessa tecnologia di base si presta a risolvere problemi in molti contesti diversi, a partire dai mercati della robotica e dell’automazione industriale. A quel punto, è risultato opportuno fare un’operazione di spin-out, configurando quell’attività come una vera e propria azienda indipendente che ad oggi conta oltre 50 collaboratori, quattro uffici in Europa e uno in Israele. La linea di prodotto che oggi la vede più impegnata, ovvero quella della sensoristica radar per applicazioni industriali, si è nel tempo aggiunta alla già citata serie di sensori radar per l’anti-intrusione MSK-101, unica nel suo genere.
Il recente round di equity financing permetterà ad Inxpect di crescere velocemente sia dal punto di vista commerciale che tecnologico, assumendo sempre più il ruolo di leader nel mondo della sensoristica radar intelligente.

Riprendendo il tema più volte affrontato sulle nostre pagine dell’evoluzione del canale distributivo, avete riscontrato cambiamenti prodotti dalla pandemia?
La distribuzione ha reagito prontamente all’emergenza offrendo al mercato soluzioni tecnologiche in gran parte già presenti nel settore controllo accessi e videosorveglianza. L’antintrusione, di contro, ha sofferto per il blocco dei cantieri e per la chiusura di molte attività. I cambiamenti principali nella distribuzione, specie quella specialistica, erano già in atto prima della pandemia e riguardano principalmente il ruolo del distributore nei nuovi scenari tecnologici ed evolutivi del mercato della sicurezza. E’ richiesta sempre più una competenza avanzata a supporto degli installatori ed un’assistenza in campo per l’ottimizzazione delle soluzioni.
Come TSec, abbiamo spinto molto perché si riducessero le distanze proprio tra distributore ed installatore in un’ottica di partnership per l’individuazione delle migliori soluzioni, partendo dal progetto e dalle competenze a 360 gradi del distributore. Come già accennato, dal 2019 abbiamo introdotto nella nostra rete il principio di certificazione del distributore da parte del produttore. L’evoluzione della filiera deve necessariamente passare dalla competenza e, quindi, dalla formazione puntuale di tutti gli attori.

Nova Service e LBM Italia, un'unione strategica per il mondo del trattamento del denaro

intervista a Giuseppe Quartuccio, amministratore unico Nova Service srl – CEO LBM Italia

Ci può presentare Nova Service, la sua storia, i marchi trattati, la struttura organizzativa?
Nova Service S.r.l. nasce dall'evoluzione di quella che circa trent'anni fa era una piccola azienda artigiana che operava come manutentore e rivenditore di macchine microfilmatrici per assegni nel mondo bancario. Questo, unito alla nostra voglia di crescita, porta nel giro di pochi anni ad una specializzazione nell'ambito bancario, creando i presupposti per collaborazioni con importanti brand del settore.
La strada percorsa e l'esperienza acquisita hanno portato la nostra azienda a diventare un'affermata società che opera anche nel settore del trattamento denaro consentendoci, da diversi anni, di fornire i nostri servizi alle banche di tutta Italia.
Dal 2015 l'offerta si è estesa al settore del CIT, prima con il marchio Julong e dal 2019 con il marchio Scan Coin. La partnership con quest'ultima ci ha permesso di spiccare il volo: attualmente siamo in grado di offrire ai nostri clienti (banche, CIT e retail) un alto grado di personalizzazione dei prodotti e dei servizi, garantendo un elevato standard di assistenza tecnica su tutto il territorio nazionale. La nostra struttura non solo offre soluzioni hardware di altissimo livello, ma è anche in grado di offrire soluzioni software adatte alle particolari esigenze dei clienti, trasformando un prodotto standard in un prodotto "cucito" su misura.
Oltre al settore del trattamento denaro, Nova Service è leader nell'office automation. Quali partner "Kyocera Platinum" da oltre 10 anni, vantiamo un parco installato di circa 15.000 apparecchiature tra multifunzioni A3/A4 bianco/nero – colore e stampanti laser per tutte le esigenze mentre, per la gestione documentale, ci avvaliamo di un rapporto diretto con Emmedi (distributore ufficiale per il mondo banche del marchio Fujitsu).
La partnership con Emmedi ci ha permesso di realizzare un software dedicato per la dematerializzazione degli assegni,

dedicato al mondo del trasporto valori, dove abbiamo già iniziato a collaborare con alcuni operatori.
Sottolineo la nostra peculiarità di gestire, in totale autonomia, i tre settori presentati con una rete capillare di vendita, noleggio ed assistenza tecnica diretta.

L'acquisizione della maggioranza di LBM Italia rappresenta un passaggio importante per la vostra azienda ma anche per il mercato italiano degli operatori del contante. Qual è stata la genesi e quali sono gli obiettivi di questa operazione?
E' vero, questa acquisizione rappresenta per noi una crescita importante in un segmento di mercato nel quale siamo presenti da tempo. L'arrivo di Scan Coin in Nova Service aveva favorito l'avvicinamento tra me e l'amico Giuseppe Ferrara, permettendo che la stima ed il rispetto reciproci trovassero sul campo un raggio di azione comune.
Nova Service aveva dato prova di versatilità, duttilità e velocità operativa anche in questo settore, aspetti che Giuseppe aveva molto apprezzato, al punto che si era iniziato un dialogo per progettare utili collaborazioni tra le nostre società.
Purtroppo, questo dialogo è stato prima rallentato dalla pandemia, poi bruscamente interrotto dalla prematura scomparsa di Giuseppe.

A questo punto, la decisione di acquisire la maggioranza di LBM ITALIA è stata quasi il naturale epilogo all'idea di Giuseppe Ferrara di creare una valida e solida alternativa sul mercato del trattamento denaro. Visti l'apprezzamento e la positiva risposta ricevuti in pochi mesi, peraltro molto difficili, mi sento di poter dire che avevamo visto bene: il mondo del CIT aveva necessità di una "ventata di aria fresca" per accompagnare in modo adeguato le aziende nel percorso di grandi cambiamenti imboccato dal settore.

Come pensate di raggiungere questo ambizioso obiettivo?
Come abbiamo sempre fatto, ci poniamo l'obiettivo di mettere a disposizione del mercato la nostra serietà, offrendo ai clienti, oltre a prodotti all'avanguardia (oggi, anche grazie a Industria 4.0), il supporto per la ricerca di soluzioni integrate e customizzate.
Uniamo per questo tutte le nostre competenze: da una parte il bagaglio di conoscenze acquisito nel tempo da Nova Service in settori diversi e in continua mutazione; dall'altra la competenza tecnica specifica di LBM Italia per quanto attiene il mercato del Cash in Transit.
A questo proposito, è importante ribadire che oggi la nostra rete di assistenza tecnica è in grado di operare direttamente su tutto il territorio nazionale.
Per raggiungere l'obiettivo, ci avvaliamo di un team di tecnici con un elevato tasso di preparazione e di esperienza conseguito grazie a continui corsi di formazione presso le aziende produttrici. Un altro tassello parimenti importante, che consideriamo fondamentale e sul quale abbiamo investito molto, è il magazzino ricambi/consumabili, strumento attraverso il quale possiamo garantire tempi di intervento sempre celeri.

Quali linee di prodotti proponete nel 2021 per il trattamento del contante?
Il nostro gruppo ha stretto, negli anni, accordi con aziende affermate e piccole realtà artigianali altamente specializzate, offrendo un ventaglio di servizi molto ampio e permettendo di soddisfare le specifiche esigenze dei nostri clienti.
Parlando strettamente di Cash in Transit, ad oggi la nostra "Line Up" è composta da alcuni dei più importanti produttori su scala mondiale di apparecchiature per il trattamento denaro come Laurel Banking Machines Japan, SUZOHAPP (Scan Coin) e NGZ.
Questi tre marchi sono leader in termini di qualità costruttiva, tecnologia e durevolezza e, come dicevo prima, l'unione di questi prodotti con l'esperienza acquisita negli anni in settori diversi, ci consentono di fornire ai nostri clienti un'ampia personalizzazione dei servizi.

Quali sono i progetti per il futuro?
Vogliamo dare continuità al nostro progetto, rafforzandolo e facendolo crescere, seguendo la strada che ci ha portato fino a questo punto.
Stiamo attraversando un momento storico mai visto prima, ci troviamo di fronte a difficoltà mai incontrate in precedenza, il nostro intento è quello di supportare i nostri clienti con la versatilità di nuove soluzioni tecniche e contrattuali.
Pensiamo che l'unione di NOVA SERVICE ed LBM abbia creato un punto di riferimento importante per questo mercato.
Il nostro auspicio è quello di esserlo sempre di più, sfruttando le caratteristiche che ci hanno sempre contraddistinto: dedizione al lavoro, costanza, impegno e trasparenza.
Desideriamo che in questo momento così delicato, i nostri clienti abbiano la tranquillità di avere un partner affidabile e presente che gli permetta di canalizzare le energie laddove necessario, ovvero verso i clienti finali.
Per finire, desidero sottolineare l'importanza anche strategica di avere nel portfolio della nostra società un produttore importante come Laurel Bank Machines (LBM), un partner che ci pone nella condizione di ambire a scenari diversi e sempre più ambiziosi.

Contatti:
Nova Service srl
Tel. +39 06 9252446
commerciale@novaservicesrl.com
www.novaservicesrl.com

Contatti:
LBM Italia spa
Tel. +39 02 48842953
commerciale@lbm-italia.com
www.lbm-italia.com

ProSYS™ Plus: il sistema super ibrido di RISCO Group con Verifica Visiva Radio

a cura della Redazione

ProSYS™ Plus è la centrale super ibrida di **RISCO Group** con video verifica visiva radio, abilitata da sensori radio da interno e da esterno con fotocamera integrata, e tastiera touchscreen **RisControl**.
Progettata per grandi installazioni commerciali fino a 512 zone anche di Grado 3, **ProSYS™Plus** è una soluzione estremamente flessibile, in grado di offrire performance elevate, che ben si adatta anche a strutture residenziali.

Oltre al nuovo contenitore in policarbonato Grado 3, **ProSYS™Plus** si contraddistingue per la tastiera touch screen **RisControl** che abilita un'esperienza d'uso senza paragoni.
Il display ad alta risoluzione da 8 pollici offre infatti un'interfaccia intuitiva. Grazie a icone simili a quelle di uno smartphone, l'utente ha la possibilità di controllare lo stato del sistema di sicurezza, inserire o disinserire l'allarme e accedere a video live o alle registrazioni delle telecamere **IP VUpoint** in tutta semplicità, per un controllo e una sicurezza senza eguali.
Inoltre, **RisControl** consente di personalizzare la visualizzazione fornendo accesso rapido alle funzioni più utilizzate dall'utente ed è integrata nel Cloud di RISCO, con cui comunica attraverso la rete Wi-Fi.
Il collegamento con la centrale avviene, invece, tramite RISCO Bus.
La tastiera touch screen è progettata per favorire un'installazione e un cablaggio semplificati e veloci grazie a una staffa di montaggio e a un connettore rimovibile.
A breve, la tastiera consentirà di includere il campanello elettronico con telecamera **Doorbell**, per permettere all'utente di beneficiare del pieno controllo della propria abitazione o del proprio ufficio, ovunque si trovi, e di interagire con gli ospiti.

In aggiunta alla video verifica abilitata da VUpoint con telecamere IP, **ProSYS™Plus** offre anche verifica visiva dell'allarme in tempo reale, grazie a sensori radio da interno e da esterno con fotocamera integrata.
I sensori **eyeWAVE™** da interno e **Beyond DT** da esterno possono ora essere implementati anche su **ProSYS™Plus** grazie all'utilizzo della nuova espansione radio dotata di canale video. Al momento del verificarsi di un evento, immagini in alta definizione e a colori o brevi clip video vengono trasmesse direttamente sullo smartphone dell'utente finale o alla vigilanza, insieme alla notifica push, e sono inoltre salvate in **RISCO Cloud** per il tempo impostato.
La funzionalità di video verifica, con fotocamere o telecamere, permette quindi di verificare in tempo reale la causa dell'allarme per poter agire di conseguenza e in modo tempestivo.
Perché **ProSYS™Plus** benefici di questa nuova funzionalità, è sufficiente aggiornare il firmware della centrale, da remoto o in locale, senza alcuna necessità di cambiare la centrale.
ProSYS™Plus è in grado di supportare le più avanzate tecnologie di comunicazione disponibili – tra cui multi-socket IP, 2/4 G e WiFi – per poter configurare più canali contemporaneamente. Si tratta di un requisito fondamentale per assicurare la massima ridondanza e resilienza nel sistema di comunicazione.

eyeWAVE™
eyeWave™ è un rivelatore radio PIR da interno con fotocamera integrata, progettato per la verifica video e facile da installare. La fotocamera acquisisce e trasmette una sequenza di immagini ad ogni evento di allarme o a richiesta inviandoli alle applicazioni RISCO per smartphone e web.
Inoltre, le immagini possono essere richieste dall'utente via web o smartphone per verificare gli eventi e agire nel modo più opportuno: sono memorizzate sul Cloud RISCO e dunque sono sempre disponibili.
eyeWave™ vanta molteplici caratteristiche tra cui copertura PIR 12m a grandangolo; fotocamera con risoluzione VGA con campo visivo di 85° che funziona anche al buio fino a 10m tramite illuminatore ad infrarossi; due canali RF indipendenti con antenne separate: uno per il controllo, l'altro per la trasmissione delle immagini; 2 batterie al litio di lunga durata. Inoltre, la sequenza di immagini può essere configurata per numero e qualità e viene salvata nel rivelatore fino al completamento dell'invio alla centrale. Quando il sistema è disattivato, gli eventi sono ignorati per salvaguardare la durata delle batterie.

Beyond DT
Beyond è il sensore da esterno intelligente di RISCO Group in grado di indirizzare le esigenze e soddisfare i requisiti di case private, siti industriali e remoti. Grazie alla doppia tecnologia (DT) e alla combinazione di due canali a microonda in banda K e due canali PIR, Beyond offre prestazioni elevate riducendo drasticamente i falsi allarmi. Per offrire prestazioni ancora più elevate e garantire

la massima sicurezza, Beyond si avvale di tecnologie di rivelazione esclusive e all'avanguardia progettate dall'azienda appositamente per l'ambiente esterno, in grado di ridurre drasticamente i falsi allarmi. In particolare, grazie alle due microonde, **Sway Recognition Technology (SRT)** permette di riconoscere e ignorare gli oggetti che oscillano senza però spostarsi, come rami e arbusti; **Digital Correlation Technology (DCT)**, invece, assicura che siano considerate minacce solo quei soggetti che causano segnali simili e correlati in entrambi i canali PIR. Inoltre, sempre nell'ottica di ridurre i falsi allarmi, Beyond è dotato anche della tecnologia **Direct Sunlight Immunity** di RISCO che, sulla base di un esclusivo algoritmo, assicura immunità alla luce solare ignorando gli improvvisi sbalzi di intensità luminosa. Beyond è anche protetto da manomissioni grazie all'antimascheramento con IR attivo ed accelerometro (nella versione radio) per evitare il disorientamento.
Infine, essendo conforme al grado di protezione IP65 (nella versione radio), il sensore da esterno Beyond garantisce protezione anche contro polveri e acqua.
Beyond, oltre alla versione radio DT e DT CAM, è disponibile in versione relè e BUS RISCO, che abilita gestione remota e diagnostica.

RISCO GROUP

Contatti:
RISCO Group
Tel. +39 02 66590054
www.riscogroup.it

Wisenet PNM-9022V e PNM-9322VQP, conformi al NDAA e dotate di funzionalità di sicurezza informatica leader del settore

HANWHA TECHWIN EUROPE LTD
(+39) 02 36572 890
www.hanwha-security.eu/it

Due nuove telecamere **Wisenet** dotate del certificato **UL CAP** e conformi al **NDAA** possono contare su un sistema proprietario di emissione certificati per dispositivi **Hanwha Techwin** che memorizza certificati unici nei prodotti **Wisenet7** sia durante la fase di sviluppo che durante il processo di produzione, rendendo le telecamere ancora più resistenti ai tentativi di manomissione del firmware.

Wisenet PNM-9022V

La **PNM-9022V** a 4 canali utilizza la tecnologia "alpha blending" per unire perfettamente le immagini sovrapposte catturate dai 4 sensori Full HD in un'unica immagine a 209° da 8.3 MP. Può anche catturare immagini a 180° permettendo di sfruttare la funzionalità PTZ digitale su due dei canali della telecamera. Grazie al SoC Wisenet7, i 4 sensori della PNM-9022V, ciascuno con obiettivo a focale fissa da 2,8 mm, sono in grado di catturare immagini a colori ad alta definizione con un'illuminazione di soli 0,03 lux.

Wisenet PNM-9322VQP - PTZ e multidirezionale

La **PNM-9322VQP**, dotata di 4 sensori e una telecamera PTZ integrale, è progettata per il rilevamento e il tracciamento di oggetti in ampie aree aperte.

Poter usare moduli obiettivo intercambiabili da 2 e 5 MP consente ai sensori della telecamera di operare in sintonia e acquisire immagini a 360° prive di imperfezioni con una risoluzione fino a 20 MP. Quando viene rilevata un'attività di attraversamento di una linea virtuale, si può configurare la telecamera PTZ del dispositivo per seguire e zoomare sull'oggetto in movimento o per spostarsi in una posizione preimpostata configurata dall'utente.

VXI-CMOD di OPTEX, proposto da HESA in tre vantaggiosi kit

HESA SPA
(+39) 02 380361
www.hesa.com

Il modulo telecamera **VXI-CMOD** di **OPTEX** distribuito da **HESA** è un dispositivo innovativo che, integrato al noto e apprezzato sensore **VXI**, apporta l'importante funzionalità della verifica visiva dell'evento.

La combinazione consente infatti di ottenere una soluzione ancora più completa ed efficace, in quanto l'utente ha il vantaggio di poter comprendere subito da remoto la natura dell'evento che ha fatto scattare l'allarme.

Quando il sensore VXI rileva un intruso, viene attivato il modulo **HD 1080p** con angolazione a 180 gradi e visione notturna VXI-CMOD che registra l'evento e manda un avviso a uno o più smartphone (iOS o Android).

L'avviso è prodotto tramite l'**App OPTEX Vision** e può essere ricevuto da più utenti in contemporanea.

Attraverso VXI-CMOD è inoltre possibile registrare il flusso video su NVR e, dunque, integrare il prodotto agli impianti TVCC per operare anche nell'ambito di sistemi di sicurezza più ampi.

VXI-CMOD viene proposto da HESA in tre vantaggiosi kit:

-VXI-ST/CMOD: Kit composto da un rivelatore passivo di infrarossi per esterno a doppio fascio VXI-ST e da un modulo telecamera VXI-CMOD.

-VXI-AM/CMOD: Kit composto da un rivelatore passivo di infrarossi per esterno a doppio fascio con antimascheramento VXI-AM e da un modulo telecamera VXI-CMOD.

-VXI-DAM/CMOD: Kit composto da un rivelatore a doppia tecnologia per esterno con antimascheramento VXI-DAM e da un modulo telecamera VXI-CMOD.

essecome ONLINE

n. 4/2021
Anno XLI
Periodico fondato da Paolo Tura

DIRETTORE RESPONSABILE E COORDINAMENTO EDITORIALE
Raffaello Juvara
editor@securindex.com

HANNO COLLABORATO A QUESTO NUMERO
Francesca Balducci, avv. Maria Cupolo

SEGRETERIA DI REDAZIONE
redazione@securindex.com

PUBBLICITÀ E ABBONAMENTI
marketing@securindex.com

EDITORE
essecome editore srls
Milano - Via Montegani, 23
Tel. +39 02 3675 7931

REGISTRAZIONE
- Tribunale di Milano n. 21 del 31 gennaio 2018
- Registro pubblico Operatori di Comunicazione (ROC) n. 34727

GRAFICA/IMPAGINAZIONE
Lilian Visintainer Pinheiro
lilian@lilastudio.it