

essecome

ONLINE
07/25

Periodico digitale di informazione di security & safety

2025 · ANNO XLV



PASSIONE

INNOVAZIONE

FIDUCIA

BE PROTECTED



ENTUSIASMO

AFFIDABILITÀ



Security & Comfort



Fire & Safety

Tecnologie d'avanguardia, design intuitivo e affidabilità totale
per affrontare le sfide di oggi e anticipare quelle di domani.

TI ASPETTIAMO A FIERA SICUREZZA

**PADIGLIONE 5
STAND B11 A21**

SICUREZZA
INTERNATIONAL SECURITY & FIRE EXHIBITION

19-20-21 Novembre 2025

SCOPRI DAL VIVO A
SICUREZZA
INTERNATIONAL SECURITY & FIRE EXHIBITION
19 - 21 NOVEMBRE 2025 | fieramilano
STAND C01 - D04



SICUREZZA COMPLETA DA OGNI ANGOLO

Il rilevamento intelligente con tecnologia LiDAR inizia con REDSCAN

La pluripremiata serie OPTEX REDSCAN LiDAR ridefinisce il rilevamento di precisione, offrendo copertura totale e massima affidabilità anche nelle aree più difficili da proteggere. Progettata per zone dove i sensori tradizionali non arrivano, la gamma REDSCAN combina la tecnologia LiDAR più avanzata con opzioni di montaggio flessibili, in verticale o orizzontale, per applicazioni interne ed esterne.

Dalla compatta REDSCAN Lite per la protezione a corto raggio, alla REDSCAN mini-Pro con videocamera integrata per la verifica visiva, fino alla REDSCAN Pro a lungo raggio, capace di rilevare oggetti fino a 50 x 100 metri, esiste un REDSCAN per ogni esigenza. Ideale per facciate, lucernari, tetti e recinzioni, offre configurazioni intelligenti e strumenti intuitivi che semplificano l'installazione e ottimizzano la sicurezza, con la maggior parte dei modelli compatibile con ONVIF per una gestione integrata di allarmi e video.

www.optex-europe.com/it

Preparati per il futuro

Segnalazione di allarme certificata con connessione ARC flessibile:
rendi le tue installazioni a prova di futuro con AddSecure IRIS-4.



Leggi di più:



www.addsecure.it/trasmissione-allarme/

For a safer and smarter world

gli eventi di SECURINDEX

DAL 19 AL 21 NOVEMBRE
Padiglione 7 - Stand S19-T20

SICUREZZA 2025
Milano Rho

MERCOLEDÌ 19/11

- 11.00 - 11.30 Norma CEI 79-3:2024 - I corsi ESSAV e RSSAV di securindex formazione
11.30 - 12.00 Manutentori rilevamento incendi IRAI&EVAC - I corsi AISE e AISEP di securindex formazione con AIPS
15.00 - 17.00 securindex PA Academy: La chiusura degli sportelli bancari e postali, ricadute e impatti per i servizi nei piccoli Comuni

GIOVEDÌ 20/11

- 10.00 - 10.30 Norma CEI 79-3:2024 - I corsi ESSAV e RSSAV di securindex formazione
10.30 - 11.30 Manutentori rilevamento incendi IRAI&EVAC - I corsi AISE e AISEP di securindex formazione con AIPS
11.30 - 13.30 Vigilanza privata: le nuove frontiere del HRM, dalla formazione all'employer branding - Talkshow
14.30 - 16.00 securindex PA Academy: Polizie Locali – contributo della tecnologia per la sicurezza nei piccoli Centri urbani
16.20 - 17.00 Italian Security World, la rassegna delle aziende certificate per le centrali di acquisto

VENERDÌ 21/11

- 10.00 - 10.30 Norma CEI 79-3:2024 - I corsi ESSAV e RSSAV di securindex formazione
10.30 - 11.30 Manutentori rilevamento incendi IRAI&EVAC - I corsi AISE e AISEP di securindex formazione con AIPS
11.30 - 14.30 Appalti genuini e intermediazione della manodopera - Talkshow
15.00 - 17.00 securindex PA Academy: Il partenariato pubblico privato, uno strumento per le imprese e gli enti locali per uno scenario di sviluppo. Dialogo costruttivo tra le parti

ISCRVITI

Attestato di partecipazione a richiesta.

Per informazioni:
segreteria@securindex.com - tel 02. 36757931

L'editoriale del direttore



Perché la filiera della sicurezza privata è un partner essenziale per il Sistema Paese

Da mercoledì 19 a venerdì 21 novembre i padiglioni dove si terrà SICUREZZA 2025 verranno invasi dai visitatori che intaseranno i corridoi tra gli stand sfavillanti e di sicuro a sera gli espositori sorrideranno disfatti e soddisfatti per le visite ricevute.

Gli operatori verranno questa volta in fiera non tanto per esporre o per vedere le novità, che ormai seguono altri canali, ma per incontrarsi in un momento positivo unico nella storia del settore, grazie alla convergenza di due potenti fattori globali ai quali sta per aggiungersi un terzo tutto nostrano.

Il primo fattore è sotto gli occhi di tutti: l'apertura della IA all'uso di massa ha spalancato un nuovo, immenso fronte di rinnovamento dei sistemi e dei processi nelle organizzazioni di ogni genere, con gli operatori della sicurezza tecnologica in prima fila a far valere le esperienze maturate nell'analisi delle immagini, il controllo accessi, la centralizzazione allarmi. Esperienze utilizzabili in ennesime altre applicazioni che offriranno opportunità di sviluppo mai verificate prima d'ora.

Il secondo, su scala europea, è conosciuto (almeno si spera!) dagli addetti ai lavori. Si tratta dell'entrata a regime delle norme cogenti comunitarie e nazionali per la cybersecurity che impongono alle grandi aziende con le rispettive supply chain (in pratica, all'intero sistema produttivo nazionale) di adottare misure "adeguate" per proteggersi da minacce combinate (fisiche e cyber) che si moltiplicano e evolvono continuamente.

Le filiere di fornitura ringraziano sentitamente per la promozione al rango di partner essenziale per il core business anche se, in molti casi, sarà la minaccia di pesanti sanzioni economiche in caso di incidente a convincere gli amministratori dei committenti a investire in sicurezza, pur continuando a considerarla un costo improduttivo.

Per il terzo fattore ci vorrà ancora qualche tempo perché si possano sentire gli effetti pratici ma potrebbe essere ancora più potente dei primi due. Parliamo dell'annunciato, progressivo ritiro dello Stato dal presidio del territorio, formalmente per la mancanza di personale che sta affliggendo qualsiasi altra attività.

In realtà è anche una scelta del Governo diminuire il ruolo del pubblico nei servizi essenziali come la sanità, la ricerca, l'istruzione e, per l'appunto, la sicurezza lasciando più spazio alle P.A. locali ed ai privati.

Pertanto, alla riduzione della presenza statale dovrà corrispondere un aumento dei compiti svolti dai Comuni e dalle Polizie Locali in primis, che potrebbero trovare con partner privati soluzioni intelligenti, innovative e sostenibili come, ad esempio, la condivisione intercomunale di risorse e infrastrutture oppure il project financing o altro ancora in relazione alle situazioni locali, senza gravare sulle casse pubbliche né sulle tasche dei cittadini. Lo stesso modello potrebbe venire applicato nei confronti di altre entità pubbliche quali [ospedali](#), università, infrastrutture dei trasporti ecc.

In sostanza, stiamo assistendo all'assunzione da parte della filiera della sicurezza privata di un ruolo essenziale nel Sistema Paese Italiano, un ruolo che dovrà venire riconosciuto primariamente alle persone che ci lavorano portando un camice, una tuta o una divisa.

Di tutto questo e altro ancora parleremo in fiera nella sequenza di incontri, talk e momenti formativi nel nostro stand S19-T20 pad. 7 da mercoledì 19 a venerdì 21 novembre

[Vedi il programma degli eventi e prenota il tuo posto](#)



INIM A FIERA SICUREZZA 2025: LA PROTEZIONE SI EVOLVE, TRA INNOVAZIONE TECNOLOGICA E IDENTITÀ ITALIANA



Appuntamento al Padiglione 5, Stand B11 - A21 insieme a Inim. Il concept scelto per l'anno 2025, che incarna appieno la visione della sicurezza per Inim è: "Be protected. Be evolved". Non si tratta solo di un claim, ma l'espressione di una filosofia progettuale che pone al centro la sinergia tra innovazione tecnologica, affidabilità certificata e vicinanza al professionista e al cliente finale.

Inim in mostra su doppio fronte (Stand B11 - A21): protagonisti Security & Comfort, Fire & Safety ed Emergency Lighting

Tutte le novità che Inim porterà a Fiera Sicurezza 2025 saranno illustrate direttamente dai product specialist, dai tecnici e dai sales manager dell'azienda, per offrire un confronto diretto su caratteristiche, applicazioni e vantaggi dei sistemi. In ambito Security & Comfort, verranno presentati la centrale modulare Prime X per un nuovo livello di protezione e

domotica integrata, le nuove tastiere InTouch in preview per Fiera Sicurezza 2025, i sistemi di videosorveglianza InVista con funzionalità avanzate di videoanalisi e le nuove telecamere integrate nel parco prodotti, le più recenti soluzioni di rivelazione perimetrale, i dispositivi nebbiogeni - recentemente introdotti nella gamma Inim - e le soluzioni antifurto wireless. Tutti i dispositivi Inim sono integrabili nell'ecosistema digitale Inim e gestibili tramite le app Inim Home e InimTech Security - che presenteranno importanti novità - con pieno supporto al My Inim Cloud (gratuito e su base Europea) e agli assistenti vocali.

Sul versante **Fire & Safety**, saranno protagoniste le centrali Previdia, il sistema integrato UltraVox (Fire+Evac) per la gestione sinergica di allarme incendio ed evacuazione, i rivelatori multisensore ad alta precisione, le soluzioni di aspirazione per ambienti complessi, il software di progettazione e un nuovo plugin CAD, ideale per professionisti e progettisti del settore. Completa l'offerta il sistema Public Address Inim, perfettamente integrato con le soluzioni antincendio per una gestione coordinata di comunicazioni ed evacuazioni di emergenza. Particolare attenzione sarà dedicata alla gamma di prodotti wireless della serie Fire Vibes. La comunicazione via radio, estremamente versatile, si combina con l'affidabilità riconosciuta dei dispositivi Inim — una qualità certificata da IMQ — rendendo Fire Vibes la soluzione ideale per tutte le applicazioni in cui rapidità di installazione, semplicità operativa e sicurezza rappresentano requisiti fondamentali.

I sistemi antintrusione Inim – Security & Comfort - sono certificati secondo la norma EN50131 in Grado 3, sono progettati per affrontare gli scenari di rischio reali con infrastrutture intelligenti, robuste e interamente integrabili.

Anche nel mondo della rivelazione incendi, Inim si distingue per un approccio progettuale che va oltre la semplice conformità normativa. I sistemi Fire & Safety non si limitano a "segnalare un pericolo", ma sono concepiti per offrire una gestione evoluta dell'emergenza: centrali intelligenti, rivelatori multi-sensore, soluzioni di aspirazione e tecnologie EVAC integrate, il tutto orchestrato da una piattaforma unificata e supportato da servizi cloud proprietari.

L'appuntamento è in fiera: Inim vi aspetta dal 19 al 21 novembre 2025 a Milano, Padiglione 5, Stand B11 - A21. Per ricevere il biglietto omaggio è possibile registrarsi <https://sicurezza.inim.it/>

06 A FIERA MILANO SICUREZZA 2025

08 AddSecure innova e cresce in Italia

10 Dalla sicurezza all'efficienza operativa:
il processo di digital transformation secondo Axis Communications

12 FonTer sempre al fianco delle aziende del Settore della Sicurezza

14 OPTEx a fiera Sicurezza 2025: innovazione e nuove sfide per il futuro

18 Nasce securindex P.A. Academy, un progetto per la formazione degli Amministratori comunali

22 AISMA: Intelligenza, sicurezza e innovazione per la sanità del futuro

24 Integro, la piattaforma per la sicurezza integrata delle strutture sanitarie

26 Sanità e Sicurezza nell'Era dell'Intelligenza Artificiale: la visione di Base Digitale

28 Sicurezza fisica e cybersecurity per il mondo della sanità da Cyberloop

30 Sicurezza integrata per la Sanità secondo l'Istituto di vigilanza Coopservice

32 Il lato umano della tecnologia: come le bodycam di Reveal supportano gli eroi della sanità

34 L'apporto delle guardie giurate per la sicurezza nei presidi sanitari

38 ERMES, la comunicazione diventa semplice, potente e connessa

40 KEYDOM di FAAC: la piattaforma intelligente che integra sicurezza fisica e logica

42 Wisenet 9, la piattaforma con IA a bordo per offrire servizi a valore aggiunto

44 Il coaching: la CPU della Security.
Quando la sicurezza parte dalle persone e non solo dalle procedure

46 Vivaldi, quando l'audio è anche sicurezza

A FIERA MILANO SICUREZZA 2025

a cura della redazione

Innovazione e formazione: le chiavi della sicurezza del futuro.

La sicurezza, oggi, non è più solo una questione di tecnologie o sistemi avanzati, è, prima di tutto, una questione di competenze. In un mercato in rapida espansione, l'innovazione e la capacità di gestirla grazie a un'opportuna formazione professionale rappresentano il vero punto di svolta per garantire lo sviluppo del settore e la sua capacità di rispondere alle nuove sfide globali. Nell'era della connessione cresce infatti l'esigenza di figure in grado di coniugare protezione fisica e digitale, gestione del rischio, compliance normativa e cultura organizzativa, in ogni campo di applicazione, dai trasporti ai grandi eventi, dal retail al patrimonio culturale. Il nodo cruciale resta quindi il capitale umano: basti pensare che solo nel campo della cybersecurity, in Italia, mancano oltre 100.000 esperti (fonte Censis), mentre la richiesta di tecnici installatori, integratori di sistemi e specialisti della compliance è in costante aumento. Per questo la formazione non è più un'opzione: è una priorità strategica per il futuro della security.

SICUREZZA 2025: soluzioni all'insegna di digitalizzazione e integrazione

Dal 19 al 21 novembre 2025, SICUREZZA torna a Fiera Milano, con un'edizione che sin da ora la riconferma il punto di riferimento del settore security & fire: sono presenti più di 340 aziende da 26 Paesi, con tanti ritorni, ma anche significativi nuovi ingressi, e una crescita del 18% della superficie espositiva rispetto al 2023.

Grazie alla presenza dei principali produttori italiani e internazionali, SICUREZZA 2025 permetterà di osservare da vicino quanto di più innovativo offre oggi il mercato. La digitalizzazione integrata sarà sicuramente uno dei temi trasversali a tutta la manifestazione: l'uso combinato di intelligenza artificiale e Internet of Things trasforma i sistemi di sicurezza in ecosistemi intelligenti, capaci di apprendere dal contesto e adattarsi in tempo reale. Vedremo come videosorveglianza e controllo accessi dialogano con piattaforme edge-cloud per un monitoraggio predittivo sempre più preciso. Centrale sarà anche l'integrazione

tra tecnologie, che consente di gestire reti complesse e, grazie al wireless, estende la connettività a tutti i dispositivi, anche a quelli antincendio, semplificando installazione e manutenzione. Un'area speciale sarà dedicata ai droni che diventano strumenti utili in sempre più numerose situazioni, progettati su misura, personalizzabili in base alle esigenze operative e capaci di raccogliere e analizzare dati in tempo reale. In tema di personalizzazione, sempre più aziende si propongono come partner consulenziali, offrendo soluzioni modulari e tailor made, costruite sulle necessità del cliente e del contesto applicativo.

La formazione che mette al centro le persone

SICUREZZA non sarà solo un evento espositivo, ma un luogo dove si condivide conoscenza, si costruiscono competenze e si formano le figure che renderanno il mondo – digitale e reale – più sicuro, consapevole e sostenibile. Per rispondere in modo mirato alle esigenze dei professionisti e delle imprese, si presenta quest'anno con una proposta formativa rinnovata organizzata in tre giornate tematiche: Cyber Day, Security Day e Job in Security Day. Una scelta che rafforza la vocazione della fiera come piattaforma di aggiornamento, confronto e crescita per chi lavora nella protezione fisica e digitale.

Cyber Day: proteggere il futuro digitale

Il 19 novembre si apre con il Cyber Day, dedicato alla crescente convergenza tra minacce fisiche e informatiche. L'entrata in vigore delle direttive europee NIS2, CER e CRA impone a imprese e installatori nuove responsabilità e un approccio alla sicurezza che coinvolga ogni livello dell'organizzazione. Il focus sarà sulle strategie di resilienza, sulla protezione della supply chain e sull'evoluzione dei modelli di governance, interoperabilità dei sistemi e sinergie tra fornitori e clienti. L'obiettivo è accompagnare aziende e professionisti verso una visione integrata della sicurezza, dove tecnologia, processi e persone lavorano insieme.

Security Day: soluzioni per contesti complessi

Il 20 novembre sarà la volta del Security Day, che porterà al centro dell'attenzione i contesti critici – trasporti, banche,



retail, grandi eventi, beni culturali – e le tecnologie capaci di rispondere alle loro specificità, ma anche i principali temi di evoluzione normativa. Un approfondimento sarà dedicato a banche e retail, settori sempre più convergenti nella gestione del contante, chiamati a elaborare sistemi di sicurezza su misura per un presidio efficace che integri tecnologie fisiche e digitali e ruolo della vigilanza privata e del personale interno. Ampio spazio sarà dedicato anche ai modelli di sicurezza per i grandi eventi, come i Giochi Olimpici e Paralimpici Invernali di Milano-Cortina 2026, e ai nuovi profili professionali emergenti, tra cui i Travel Security Manager e i Cultural Security Manager, chiamati a proteggere persone, patrimoni e infrastrutture con un approccio sempre più multidisciplinare. Grazie alle associazioni di categoria sarà poi possibile approfondire i temi normativi: ANIE Sicurezza e UMAN cureranno un incontro focalizzato sulla nuova normativa UNI su sistemi di evacuazione audio e gli impianti di rivelazione automatica incendi; AIPS si concentra sulla nuova CEI 79-3, la qualificazione dei tecnici manutentori antincendio e la responsabilità degli installatori; ConFederSicurezza e Servizi in collaborazione con la Fondazione Asfàleia promuove un evento di confronto sulla evoluzione normativa e professionale della vigilanza privata.

Job in Security Day: il futuro si forma oggi

Il 21 novembre è il Job in Security Day, dedicato all'incontro tra scuole, ITS e imprese con l'obiettivo di ridurre la distanza tra formazione e mondo del lavoro, facilitando l'ingresso dei giovani in un comparto che offre grandi opportunità, ma richiede competenze sempre più aggiornate. Al centro della giornata ci sarà il Progetto EDU che vedrà coinvolti circa 500 studenti delle classi IV e V degli istituti tecnici. I ragazzi potranno partecipare a workshop, colloqui e momenti di orientamento insieme alle aziende espositrici, che contribuiranno a delineare i profili professionali più richiesti: installatori, integratori, analisti di rischio, data protection officer, project manager e tecnici specializzati nella sicurezza fisica e digitale. Una giornata che guarda al futuro del settore e che si propone come ponte concreto tra formazione e impresa.

Tutti gli eventi formativi si svolgeranno all'interno della Cyber & Security Arena al pad. 5, spazio polifunzionale che ospiterà talk, dimostrazioni e tavole rotonde con esperti, aziende, enti pubblici e associazioni di categoria. A completare l'offerta, i Security Talk associativi al pad. 10 promossi da AISS, AIPS, ANIE Sicurezza e ConFederSicurezza, oltre ai podcast di ASSIV dedicati a innovazione, sinergie pubblico-privato e sviluppo della vigilanza privata.

AddSecure innova e cresce in Italia

intervista ad Antonio Cuccurullo, Country Manager, Smart Alarms Italy, AddSecure

Quali sono le novità che AddSecure presenterà a Sicurezza 2025?

Sicurezza è un momento chiave per mostrare l'innovazione ed incontrare i professionisti del settore. Siamo entusiasti di evidenziare, tra le altre, le seguenti importanti novità di quest'anno:

1. Supporto per un doppio protocollo di trasmissione, sia con IRIS che con SIA DC-09, consentendo un'affidabilità di comunicazione senza pari e la compatibilità con il centro di ricezione allarmi (ARC).
2. Integrazioni certificate a doppio percorso con le centrali antincendio di primari produttori, che offrono una soluzione completamente conforme alla norma EN54-21 per la trasmissione degli allarmi antincendio. Insieme, questi miglioramenti aumentano significativamente la sicurezza e la flessibilità dei nostri sistemi di trasmissione degli allarmi, in particolare per i sistemi di rilevamento incendi e antintrusione presso siti ad elevata criticità con alto rischio sicurezza.

Può spiegare il vantaggio dell'utilizzo di entrambi i protocolli IRIS e SIA DC-09?

In sintesi, il supporto di entrambi i protocolli garantisce la possibilità di collegarsi praticamente a qualsiasi Centro Ricezione Allarmi:

- IRIS è un protocollo proprietario e altamente collaudato che consente ai Centri Ricezione Allarmi, dotati del ricevitore ISA-4, di effettuare le più complete attività di monitoraggio dei collegamenti con i comunicatori IRIS-4.
- SIA DC-09 è un protocollo standard di fatto a livello di settore, praticamente supportato da tutti i Centri Ricezione Allarmi.

Questa duplice possibilità offre agli installatori ed ai clienti la libertà di scelta dei collegamenti e rende i comunicatori della famiglia IRIS-4 collegabili appunto a qualsiasi Centro Ricezione Allarmi.



Qual è il vantaggio principale dell'integrazione diretta con le centrali antincendio ?

Generalmente le centrali antincendio sono collegate ai morsetti di ingresso del comunicatore di allarmi certificato EN54-21 EN50136 per la segnalazione degli eventi di allarme. Con l'integrazione diretta è possibile il collegamento via bus di comunicazione tra la centrale di allarme ed il comunicatore, disponendo non solo della soluzione certificata EN54-21 EN50136 con trasmissione a doppio vettore IP/4G delle segnalazioni di allarme antincendio e di guasto come da normativa in vigore, ma con una descrizione più dettagliata dell'evento.

Si tratta di centrali antincendio di assoluto riferimento nel settore, implementando un sistema di:

- Instradamento degli allarmi con doppio percorso e segnalazione dei guasti in tempo reale, con messaggistica di dettaglio generata dalla centrale stessa

- Supporto per il controllo del sistema estinguente e avvisi di guasto

In definitiva una soluzione ideale per edifici commerciali e pubblici che richiedono un sistema antincendio certificato e conforme alle normative.

In che modo queste innovazioni supportano la crescita futura?

La piattaforma IRIS-4 è stata progettata pensando al successo a lungo termine. Include il supporto per 4G, dual Ethernet e aggiornamenti del firmware, come quello che aggiunge la compatibilità con DC-09. Ciò significa una maggiore scalabilità, sia per le piccole attività che per le grandi imprese.

Quali sono i piani di AddSecure per il 2026 in Italia?

Nel 2026 puntiamo a rafforzare la nostra posizione nel mercato (Italiano della trasmissione certificata di allarmi



antincendio. Investiremo in team tecnici e commerciali per supportare le crescenti esigenze dei clienti. Con una piattaforma di connettività IoT sicura e affidabile unitamente a soluzioni certificate di segnalazione degli allarmi, vediamo una grande opportunità per espanderci e continuare a rappresentare un punto di riferimento in questo settore.

ADD:SECURE®

Contatti:
AddSecure International AB
Tel. +39 347 9977 838
www.addsecure.it

Dalla sicurezza all'efficienza operativa: il processo di digital transformation secondo Axis Communications

di Roberto Briscese, Distribution Account Manager di Axis Communications

Negli ultimi anni la trasformazione digitale è diventata una priorità strategica per le imprese italiane, che mostrano un impegno crescente verso l'innovazione. Secondo i dati dell'Osservatorio Innovazione Digitale nelle PMI del Politecnico di Milano, nel 2025 oltre la metà delle piccole e medie imprese italiane – il 54% – ha dichiarato di investire in tecnologie digitali in modo significativo. Un quadro che evidenzia un sistema produttivo in evoluzione, che si sta attivando per tradurre il valore strategico del digitale in risultati concreti.

In questo scenario di rinnovamento si inserisce anche il settore della videosorveglianza, oggi protagonista di una trasformazione profonda.

Non più solo deterrenza: l'evoluzione della videosorveglianza digitale

Per molto tempo le telecamere sono state installate con un unico obiettivo: garantire sicurezza, prevenire intrusioni, scoraggiare comportamenti illeciti. Nell'accezione comune, si trattava puramente di strumenti di controllo, spesso percepiti più come un costo che come un investimento. Oggi, però, le telecamere non si limitano a "guardare": interpretano, analizzano e generano dati. Diventano, di fatto, sensori intelligenti che partecipano alla digital transformation delle imprese, trasformandosi in alleati per aumentare efficienza, qualità e consapevolezza operativa.

I recenti progressi tecnologici hanno reso possibile questo salto di qualità: l'integrazione di componenti avanzate e di processori studiati ad hoc consente di eseguire algoritmi di analisi direttamente a bordo delle telecamere. Così i dispositivi diventano nodi attivi all'interno della rete, capaci di comprendere e reagire in tempo reale agli eventi, garantendo al contempo elevate prestazioni, sicurezza informatica e riduzione della latenza.



Dai livelli di sicurezza ai livelli di intelligenza

La digitalizzazione della videosorveglianza rappresenta un percorso graduale, che può articolarsi su diversi livelli di sviluppo. Si parte dagli utilizzi più basilari, come la registrazione delle immagini a fini di documentazione, per poi passare al rilevamento automatico di eventi o anomalie, all'attivazione di risposte automatizzate e, infine, alla creazione di metadati utili per l'analisi e la business intelligence.

Questo processo non segue necessariamente un andamento lineare: ogni azienda può trovarsi in un punto diverso del percorso, a seconda delle proprie esigenze e della propria maturità digitale. In molti casi, la digital transformation non è un traguardo futuro ma una condizione già in atto, seppur non sempre pienamente riconosciuta o valorizzata.

Casi d'uso: quando la telecamera diventa un alleato operativo

Gli esempi concreti di questa trasformazione non mancano e attraversano settori molto diversi tra loro.

Nel comparto dei trasporti, ad esempio, le telecamere di rete possono integrarsi con i sistemi di controllo accessi per automatizzare la gestione dei flussi in aree sensibili come aeroporti o terminali logistici. Oggi, in molti casi, l'ingresso dei veicoli non è più gestito da personale fisso, ma da sistemi intelligenti che riconoscono automaticamente le targhe autorizzate, attivano le barriere e, in caso di accesso non consentito, inviano messaggi di allerta. Queste soluzioni, nate con finalità di sicurezza, permettono anche di raccogliere dati preziosi su flussi, tipologie di mezzi e orari di utilizzo, contribuendo a migliorare l'organizzazione degli spazi di parcheggio e a ridurre i costi operativi.

Un'evoluzione simile si osserva nel settore della logistica, dove la videosorveglianza, inizialmente adottata per motivi assicurativi o di sicurezza, si è trasformata in uno strumento di ottimizzazione dei processi. In grandi hub di distribuzione, ad esempio, le telecamere monitorano la permanenza dei veicoli nelle baie di carico, attivando segnali visivi se vengono superati i tempi di sicurezza. Nel tempo, le immagini sono diventate anche una fonte di dati operativi, utili per analizzare il grado di riempimento dei camion o la corretta disposizione delle merci, migliorando l'efficienza complessiva.

Anche nel settore manifatturiero, l'integrazione della tecnologia video nei processi produttivi è ormai una realtà. In alcuni stabilimenti industriali le telecamere ad alte prestazioni sono utilizzate per monitorare le linee di assemblaggio e associare le immagini dei componenti ai relativi codici di produzione. In caso di reclami o verifiche di qualità, è possibile risalire alle registrazioni per controllare la corretta esecuzione del processo. Un approccio che migliora la tracciabilità, riduce le contestazioni e consente di dimostrare in modo oggettivo la conformità dei prodotti. Ma non è tutto: nei servizi pubblici e nelle infrastrutture critiche, come la distribuzione idrica, la digitalizzazione ha introdotto nuove possibilità di monitoraggio e manutenzione. In contesti caratterizzati da impianti remoti o difficilmente accessibili, le telecamere consentono di verificare a distanza

il corretto funzionamento delle apparecchiature e di rilevare anomalie. L'evoluzione verso sistemi intelligenti, dotati di analisi onboard, permette oggi di individuare in autonomia fenomeni come fumo, allagamenti o movimenti sospetti, attivando un intervento solo quando necessario.

Le applicazioni possibili, tuttavia, vanno ben oltre questi esempi, poiché possono essere facilmente replicate e adattate a tante tipologie di contesti.

Nuove opportunità di mercato e sfide future

L'evoluzione tecnologica sta ridefinendo il ruolo della videosorveglianza, estendendola a tutti i settori produttivi, dalla logistica alle infrastrutture e alle utility fino al retail. Il mercato si apre così a nuovi interlocutori, oltre agli operatori della sicurezza e ai system integrator, coinvolgendo produttori industriali, sviluppatori e aziende orientate all'efficienza.

In Italia, ovvero il secondo produttore europeo di macchine e impianti, le prospettive di crescita per Axis risultano particolarmente interessanti nel comparto industriale, che spazia dal tessile all'industria pesante, dal chimico all'energetico, e che offre un terreno fertile per l'applicazione di tecnologie intelligenti.

Resta tuttavia una sfida culturale e organizzativa: molte aziende non dispongono ancora di figure dedicate all'innovazione digitale e si confrontano con un contesto europeo eterogeneo, caratterizzato da diversi livelli di maturità. In questo scenario, la chiave del successo risiede in un approccio modulare e flessibile, capace di adattarsi ai contesti locali valorizzando al contempo il potenziale dell'innovazione tecnologica.

Infine, il futuro della tecnologia video si giocherà sull'AI e sulla capacità di elaborare i dati direttamente all'edge, in modo sempre più rapido, sicuro e autonomo. Le telecamere saranno in grado non solo di rilevare un evento, ma di prevederlo, contribuendo a migliorare la produttività e la sicurezza. La convergenza tra sicurezza, efficienza e sostenibilità darà vita a un nuovo paradigma, in cui l'immagine diventa un elemento cruciale per decidere e agire.



Contatti:
Axis Communications
Tel. +39 02 8424 5762
www.axis.com

FonTer sempre al fianco delle aziende del Settore della Sicurezza

di Massimiliano Marcucci, Direttore generale di Fon.Ter

Negli ultimi anni, il settore della vigilanza sia armata che disarmata ha assunto un ruolo sempre più strategico, per le imprese, per le istituzioni pubbliche, per i privati cittadini, divenendo un supporto di cui è sempre più difficile fare a meno.

Nel 2023 l'osservatorio di ConFederSicurezza evidenziava per il settore un tasso di crescita annuo compreso tra il 4 e il 6% con un fatturato di circa 4 miliardi di euro.

Nel biennio 2025/2026 si prevede una crescita annua che si attesterà intorno al 5% con una significativa richiesta di servizi di alta tecnologia.

In un contesto sociale in cui il rischio ha assunto caratteristiche più sofisticate e molto diverse da quelle del passato, si rende sempre più necessario poter contare su personale altamente qualificato e preparato e non ci riferiamo solo alla figura della guardia particolare giurata. Per fare fronte a questa esigenza è indispensabile la formazione continua e l'aggiornamento tecnologico.

Nel 2023 sono state emanate due normative la UNI11925:2023 e UNI 11926:2023 che hanno definito i requisiti delle figure professionali e dell'organizzazione delle imprese che erogano i cosiddetti servizi ausiliari alla sicurezza che comprendono le attività di portierato, monitoraggio aree, gestione dei flussi (ingresso e uscita di persone, veicoli, ecc.), informazione, controllo dei

titoli in ingresso, accoglienza e assistenza. Un settore in forte evoluzione e che, come quello della vigilanza armata, richiede professionalità elevate e aggiornamento professionale. Lo scopo delle due normative è stato quello di [standardizzare e regolamentare la sicurezza non armata](#), un segmento che con oltre 100.000 operatori occupati di diritto fa parte del sistema sicurezza.

FonTer sin dal 2015 affianca il settore della sicurezza in tutte le sue articolazioni finanziando la formazione del personale delle numerose aziende aderenti. Sono stati messi a disposizione di oltre 1.300 aziende circa 20 milioni di euro che hanno permesso di formare circa 13.000 lavoratori. L'incremento costante delle adesioni e la tipologia delle richieste che risentono fortemente delle innovazioni tecnologiche - come è stato evidenziato nel corso della Fiera della Sicurezza che si è tenuta a Milano dal 19 al 21 novembre - hanno imposto al fondo di partecipare all'evento per presentare agli operatori del settore la programmazione formativa del 2026 che prevede avvisi sempre più rispondenti alle esigenze delle imprese.

Mai come per questo settore vale lo slogan di FonTer **"chi si forma non si ferma"** sei parole che raccolgono la missione del fondo che è quella di sostenere l'evoluzione delle aziende associate garantendo, in modo gratuito, la formazione del personale occupato.



Contatti:
FonTer

m.marcucci@fonter.it - Direttore Generale
a.larocca@fonter.it - Responsabile Marketing
r.loproto@fonter.it - Responsabile Vigilanza
s.asfoco@fonter.it - Responsabile Formazione

 **coopservice**
ISTITUTO DI VIGILANZA
Security services provider

Una nuova visione della sicurezza

- Vigilanza armata
- Servizi ausiliari alla sicurezza
- Antintrusione e Antincendio
- Videosorveglianza con AI
- Localizzazione satellitare GPS

Via Rochdale, 5 | 42122 | Reggio Emilia (RE)

Numero verde 800 129045 | www.vigilanzacoopservice.it

info.vigilanza@vigilanzacoopservice.it

OPTEX a fiera Sicurezza 2025: innovazione e nuove sfide per il futuro

intervista a Marco Censi, Regional Sales Manager Italia di OPTEX

Quali sono le novità portate a questa edizione della fiera?

Quest'anno per noi di OPTEX la partecipazione alla fiera ha un significato speciale. Abbiamo voluto fare un passo avanti su più fronti, investendo energie, risorse e passione per offrire un'esperienza all'altezza di un marchio che da sempre punta all'eccellenza.

Abbiamo ampliato lo spazio espositivo, curato in modo ancora più attento la presentazione dei nostri prodotti e lavorato per rendere evidente, fin dal primo sguardo, la dedizione che mettiamo nell'innovazione e nel perfezionamento tecnologico. Una delle principali novità è la presenza del team internazionale OPTEX: colleghi da tutto il mondo si riuniranno in Italia per questa edizione, a conferma del peso che il mercato italiano ha per il gruppo. È la prima volta che accade, e per noi costituisce un motivo di grande orgoglio. La loro partecipazione non è solo simbolica: sarà un'occasione per condividere esperienze di mercato e valorizzare i contributi forniti da clienti e partner. Un segnale forte, che sottolinea come l'Italia sia diventata un punto di riferimento e un modello anche per altre filiali OPTEX.

Sul fronte tecnologico, porteremo molte novità, alcune già disponibili e altre in anteprima assoluta. In primo piano la gamma REDSCAN, che si arricchisce del nuovo REDSCAN Lite, un dispositivo LiDAR compatto, facile da installare e ideale per ambienti indoor ad alta sicurezza. Pensato per la protezione di spazi complessi (come corridoi stretti, data center a protezione di server, intercapedini o condotti di ventilazione) offre un rilevamento preciso e immediato grazie alla tecnologia time-of-flight (TOF). Tra i suoi punti di forza: prestazioni affidabili anche al buio o in condizioni ambientali difficili, e una procedura di installazione semplificata grazie alle nuove funzioni di allineamento e regolazione.

Un'altra novità di rilievo riguarda Fiber SenSys Point Defender™, il primo sensore perimetrale con cavo in rame con tecnologia tollerante al taglio (E2EC™). Si tratta di una



soluzione che garantisce continuità operativa anche in caso di danneggiamento del cavo, riducendo al minimo i falsi allarmi e assicurando la massima affidabilità del sistema. Un'innovazione che apre nuove possibilità di impiego in contesti complessi, dove la sicurezza e la ridondanza sono fondamentali.

Presenteremo inoltre un nuovo sensore per esterno ad alto montaggio, ancora in fase di preview. Si tratta di una tecnologia che "alza" letteralmente il livello della sicurezza. Sarà protagonista dei prossimi anni, con una strategia di lancio che partirà già nei prossimi mesi. Si tratta di un prodotto unico nel suo genere che riflette l'impegno costante di OPTEX nel perfezionare le proprie soluzioni e nel puntare all'eccellenza. Un'altra iniziativa che abbiamo deciso di introdurre in questa edizione riguarda le collaborazioni: nei tre giorni di fiera, vogliamo incontrare potenziali partner e nuovi talenti. Il nostro obiettivo è individuare persone e realtà con cui condividere progetti, idee e visioni, per crescere insieme e continuare a innovare.

Siamo convinti che il valore di un'azienda non risieda solo nei suoi prodotti, ma anche nella qualità delle relazioni che costruisce nel tempo. Per questo investiamo costantemente

nel dialogo con i clienti, nella formazione e nel supporto tecnico. Vogliamo che chi sceglie OPTEX sappia di poter contare su un interlocutore rapido, affidabile e sempre disponibile.

In sintesi, questa edizione rappresenta per noi un momento di svolta: più presenza, più innovazione, più interazione. È la dimostrazione concreta di come intendiamo affrontare il futuro con passione, competenza e una visione che mette al centro le persone e la tecnologia.

Quali sono i vostri programmi per il 2026?

Guardando al 2026, OPTEX si prepara ad affrontare nuove sfide di crescita ed evoluzione, continuando a innovare in un settore in cui è già un punto di riferimento. Abbiamo intrapreso un percorso di trasformazione che ci porterà a uscire dalla nostra comfort zone, per non limitarci più a essere semplicemente un produttore di sensori, ma un partner tecnologico capace di offrire soluzioni integrate e sempre connesse.

Il primo passo sarà il lancio di una nuova soluzione di sicurezza, progettata per lavorare in modo intuitivo con i nostri sensori, prevista per la prima metà dell'anno. Si tratta di un progetto ambizioso, nato da una collaborazione strategica con partner tecnologici internazionali, che ci consentirà di ampliare il nostro portfolio e aprirci a nuove modalità di gestione e analisi dei dati. Questo cambiamento segnerà l'inizio di una fase nuova: più digitale, più flessibile, più orientata ai servizi.

Parallelamente, continueremo a rafforzare la nostra leadership tecnologica attraverso investimenti mirati nello sviluppo di nuovi prodotti, nella ricerca e nel supporto tecnico avanzato ai nostri clienti. Il 2026 sarà anche un anno di crescita, sia in termini di fatturato che di organico: vogliamo ampliare il nostro team con professionisti appassionati e competenti, in linea con le opportunità che il mercato offre e con la nostra visione di sviluppo sostenibile.

Non meno importante sarà la crescita sul piano delle collaborazioni. Puntiamo a costruire partnership solide e durature con clienti e system integrator che condividano i nostri valori di innovazione, affidabilità e qualità. Crediamo che solo lavorando insieme si possano raggiungere risultati davvero significativi, e per questo continueremo a investire nel dialogo, nella formazione e nella co-progettazione.

Infine, proseguiamo nel nostro impegno di supportare i professionisti del settore, aiutando installatori, progettisti e utenti finali a sviluppare soluzioni su misura, più efficienti e sostenibili. Il futuro di OPTEX passa da qui: dall'ascolto del mercato, dall'innovazione costante e dalla volontà di essere sempre un passo avanti, senza mai perdere di vista ciò che ci distingue: la passione per la tecnologia e la fiducia delle persone che ogni giorno scelgono di lavorare con noi.

In conclusione, questa fiera è solo l'inizio di un nuovo capitolo. Portiamo con noi la forza di un team internazionale, l'entusiasmo per le novità presentate e una visione chiara per il futuro: continuare a innovare, crescere e creare connessioni che durino nel tempo.



Contatti:
OPTEX
Tel. +39 351 9272789
enquiry-it@optex-europe.com
www.optex-europe.com/it



Proteggiamo **persone**,
dati e **strutture**
con soluzioni
integrate di
sicurezza
intelligente.



 aisma

AISMA

Dove tecnologia
e umanità
si incontrano,
nasce la sanità
del futuro



Nasce securindex P.A. Academy, un progetto per la formazione degli Amministratori comunali

Si allarga la proposta formativa di **securindex formazione** con un progetto ambizioso: sviluppare un percorso info/formativo dedicato alle funzioni delle Amministrazioni comunali, in particolare dei centri minori, per supportarle nella gestione delle sfide quotidiane e tutelarle sul piano delle responsabilità soggettive. Nella sostanza, un modo diverso e innovativo per contribuire alla sicurezza delle comunità e dei loro governanti rispetto alle diverse minacce di questo tempo.

Il progetto **securindex P.A. Academy** è affidato alla guida di due professionisti noti e apprezzati nel mondo della Pubblica Amministrazione: l'**architetto Anna Gagliardi** e il **dottor Andrea Galletta**, rispettivamente Direttore e Coordinatore del Comitato Scientifico che ha il compito di sviluppare il piano formativo, erogare i corsi in ogni modalità, realizzare le pubblicazioni e organizzare gli eventi.

“È per noi una forte motivazione lavorare con Anna e Andrea per questo importante progetto formativo - commenta Roberto Dalla Torre, managing director di securindex formazione - che riassume l’impegno e le esperienze maturate dalle persone della nostra squadra in tanti anni di lavoro ai massimi livelli in ambiti diversi della sicurezza”.

securindex P.A. Academy viene presentato a Fiera SICUREZZA 2025 al Pad. 7 stand S19-T20



ANNA GAGLIARDI: FORMARE CHI GOVERNA I COMUNI È UN ATTO DI SICUREZZA

Cosa l’ha spinto a far nascere una nuova proposta formativa per gli Amministratori comunali e per il personale dei Comuni minori?

Nella mia esperienza, prima come tecnico comunale e poi come project manager PNRR in Regione Lombardia, ho imparato che chi lavora in Comune rappresenta il primo e più concreto presidio dello Stato sul territorio. Amministratori, funzionari e tecnici affrontano ogni giorno sfide complesse: bilanci da tenere in equilibrio, problemi di sicurezza urbana e territoriale, gestione dei servizi essenziali, emergenze e richieste dei cittadini. Lo fanno spesso con risorse limitate, personale ridotto e responsabilità enormi, ma con una passione che tiene viva la macchina pubblica e garantisce coesione alle nostre comunità. Sono, a tutti gli effetti, “eroi

civici” che meritano attenzione, sostegno e formazione. Oggi più che mai, la transizione ecologica e digitale, insieme al tema cruciale della sicurezza - fisica, ambientale e informatica - richiedono nuove competenze e un diverso approccio al lavoro pubblico: più organizzato, collaborativo e orientato ai risultati. Da questa consapevolezza nasce un percorso formativo che non si limita a fornire teoria, ma porta ai Comuni strumenti concreti, metodo, buone pratiche e soluzioni operative. Formare chi lavora nei Comuni significa rafforzare la pubblica amministrazione, renderla più attrattiva, efficiente e capace di garantire servizi di qualità e territori più sicuri. È un onore condividere questa iniziativa con il dott. Andrea Galletta, professionista di grande esperienza nella gestione pubblica e nella tutela della sicurezza. È del

tutto evidente che ci crediamo ciecamente in alcuni valori che non si trovano nei classici corsi di formazione.

Perché formare con valore civico, chi amministra non è solo un investimento sulle persone, ma un atto d’amore verso il territorio e verso ogni cittadino. In fondo, formare chi governa i nostri Comuni significa prendersi cura del futuro di tutti noi, è un atto di sicurezza

Quali sono gli argomenti che proporrrete e con quali modalità?

Gli argomenti che proporrremo saranno tanti, ma soprattutto diversi da quelli dei corsi di formazione tradizionali, spesso limitati agli aspetti normativi. Il nostro obiettivo è andare oltre la teoria: offrire una formazione viva, concreta e generativa, capace di creare connessioni vere tra persone, esperienze e competenze. Vogliamo portare un valore aggiunto reale: metodo, strumenti operativi, capacità di pianificazione e, soprattutto, un forte spirito di collaborazione. Perché oggi amministratori, tecnici e professionisti devono imparare a lavorare insieme, condividendo linguaggi e visioni per costruire soluzioni comuni. Il percorso sarà aperto non solo al personale dei Comuni, ma anche ai professionisti privati - architetti, ingegneri, consulenti, esperti di project management e sviluppo locale - che con le loro competenze e il loro entusiasmo sono fondamentali per trasformare le idee in risultati concreti. Tratteremo temi ampi e attuali: affidamenti e gare pubbliche, Partenariato Pubblico-Privato, valorizzazione del patrimonio pubblico, facility

management, manutenzione del territorio, rigenerazione urbana e sostenibilità. Un’attenzione particolare sarà dedicata alla sicurezza e alla cura a tutto tondo dei territori: sicurezza urbana e ambientale, prevenzione del rischio, tutela del patrimonio e protezione dei dati. Perché la sicurezza non è solo un dovere amministrativo, ma una condizione essenziale per la fiducia dei cittadini e la qualità della vita nelle comunità. Ma non ci fermeremo alla tecnica: parleremo anche di etica, responsabilità, valore pubblico e cultura del servizio. Perché la “paura della firma” non deve più bloccare chi amministra e chi gestisce i procedimenti, ma lasciare spazio alla consapevolezza e alla fiducia di poter agire con trasparenza e competenza. Un punto chiave sarà il dialogo con le imprese, vero motore di innovazione e sviluppo, se pubblico e privato collaborano in modo aperto e leale, nascono progetti concreti, comunità più forti e territori più sicuri e attrattivi. L’obiettivo è costruire un ecosistema virtuoso, in cui amministrazioni, professionisti e imprese diventino parte di una stessa rete al servizio del bene comune. La formazione sarà flessibile e accessibile: incontri in presenza, laboratori, webinar, podcast e materiali digitali, per imparare ovunque e con i propri tempi.

In sintesi, non sarà una formazione su “come fare le cose”, ma un vero laboratorio di cambiamento: per imparare a farle meglio, insieme, con metodo, passione e fiducia reciproca. Perché la vera innovazione nella pubblica amministrazione nasce sempre dalle persone - e dal coraggio di costruire ponti tra chi immagina e chi realizza.





ANDREA GALLETTA: UN PROGETTO PER AIUTARE LE AMMINISTRAZIONI DEI CENTRI MINORI NELLA GESTIONE DELLE DIVERSITÀ

Dottor Galletta, in che modo questo progetto condiviso con l'arch. Anna Gagliardi si collega al percorso professionale che l'ha visto prima nell'Arma dei Carabinieri e poi Dirigente in aziende di servizio pubblico?

Il progetto che con l'arch. Anna Gagliardi abbiamo ipotizzato e con attenzione stiamo costruendo, si prefigge lo scopo di essere un concreto efficace supporto alle attività ed ancor più alle responsabilità di coloro che sono preposti all'amministrazione, gestione e servizio dei centri urbani di minor grandezza. L'idea nasce dall'osservare come nel territorio nazionale vi siano molti Comuni con una densità abitativa di poche migliaia di persone e molti altri anche al di sotto del migliaio. Queste realtà - fatta eccezione per quei piccoli centri e borghi che hanno raggiunto notorietà grazie a mirata pubblicità o potenzialità turistiche - sono spesso un po' dimenticate - coloro che a vario titolo e ruolo sono preposti alla loro amministrazione, sono oberati da mille difficoltà aggravate sovente da poca dimestichezza con i meandri della burocrazia. Per loro ogni necessità rischia di divenire un problema a volte anche insormontabile anche per la lontananza degli organismi regionali o statali preposti. Il concentrato dell'idea è questo: fornire ad Amministratori ed operatori di queste realtà un concreto supporto, anche con suggerimenti e proposte di utile impiego della tecnologia, per avviarli ad efficaci processi organizzativi e consentir loro di acquisire maggior confidenza e sicurezza per attraversare spediti gli incroci aggrovigliati della burocrazia.

Ho aderito con immediatezza ed entusiasmo a quest'idea - oggi progetto - e proprio le mie pregresse attività professionali sono state utile memoria di quanto ciò possa essere rilevante. Nella mia vita nell'Arma dei Carabinieri, oltre a numerosi importantissimi anni dedicati a complesse attività investigative, sono stato designato a due comandi territoriali, in differenti Regioni, ciascuno dei quali ricomprendeva alcune decine di Comuni. Quell'esperienza di vita in mezzo alla "gente", assieme a Sindaci ed Amministratori locali,

facendosi carico dei più svariati semplici o complessi problemi, oltre - purtroppo - delle emergenze, mi ha consentito di rafforzare ancor di più quei valori propri della mia Istituzione ed mettere in pratica ogni giorno - con entusiasmo - lo spirito di servizio, l'assunzione di responsabilità, la disponibilità, la solidarietà, l'attenzione nei confronti dei cittadini di quelle comunità che erano a me affidate.

Aspetti di vita professionale che - in misura diversa - ho potuto ripercorrere anche nei successivi ruoli da Dirigente d'Azienda, trovandomi - con diretta responsabilità - ad affrontare emergenze e criticità; organizzare, coordinare movimenti di rilevanti masse di persone in occasione di eventi o manifestazioni. Inoltre un costante impegno di indirizzo professionale dei collaboratori, ha favorito nel tempo il consolidarsi dei rapporti con il contesto istituzionale, con cui quotidianamente si interagiva. In merito posso anche raccontare come l'impiego della tecnologia sia stato un fattore importante, ad esempio sperimentando per primi e con successo l'impiego delle bodycam a bordo treno.

Il progetto in estrema sintesi, partendo da questi presupposti, non vuole essere soltanto un supporto tecnico - informativo, ma ancor più provocare con efficacia un sollecito richiamo a valori, preparazione e responsabile impegno, le cui carenze conducono a tener lontani gli amministratori dal cittadino e il cittadino - a sua volta - da una fattiva volontà di partecipazione alla vita pubblica, nel luogo in cui vive.

La proposta formativa che state sviluppando per la Lombardia verrà estesa anche ad altre regioni, in particolare al Sud?

È proprio ciò che vorremmo poter fare in futuro. Oggi viviamo in complesse realtà multietniche ed anche nei piccoli centri urbani si assiste ad una minore rilevanza e partecipazione alle tradizioni locali cui si dà vita solo in poche circostanze come le feste patronali, le sagre o altri piccoli eventi. Di

contro, osserviamo un incremento di insediamenti di nuove "comunità", sempre più attive nel voler diffondere le proprie tradizioni, abitudini e costumi.

Amministrare oggi queste realtà non è certo semplice. Chi vi è preposto necessita di adeguata preparazione, esperienza, sensibilità, progettuale visione e adeguati supporti sia normativi che tecnologici, per non incorrere in errori di valutazione, salvaguardare la memoria e la storia del luogo e non assumere decisioni che possono pregiudicare la serena, civile convivenza della comunità. In merito si osserva inoltre come in quelle realtà l'Amministrazione abbia spesso anche carenze d'organico che non consentono di far fronte alle quotidiane necessità. Credo che per chi è preposto ad amministrare non sia facile dover scegliere ogni giorno a cosa dare priorità, perché privo delle necessarie risorse da dedicare. Si potrebbe quindi ricorrere a supporti tecnologici nei più disparati settori (sicurezza dei cittadini, controllo della circolazione, erogazione dei servizi primari, sanità, organizzazione degli uffici, raccolta dati, etc.) peraltro oggi acquisibili dalle Amministrazioni con modalità sostenibili. Supporti che osserviamo solitamente più utilizzati con

maggiore dimestichezza al Centro-Nord, probabilmente in ragione di una più diffusa presenza di contesti industriali ed aziendali che possono essere stimolo e veicolo di promozione dell'innovazione.

Considerati questi aspetti di vita quotidiana e le differenze, a volte marcate, tra Nord e Sud, appare necessaria maggior cura nel predisporre argomenti e linee guida che sappiano inglobare le diversità di ciascun territorio ma, al contempo, siano un efficace strumento che non si presti a personalismi o geniali interpretazioni. In estrema sintesi, con questo progetto si vorrebbe supportare coloro che sono preposti al servizio di una Comunità o delegati ad amministrarla, ad esercitare il proprio ruolo con adeguata preparazione e competente professionalità ma anche curiosità per le innovazioni che la tecnologia offre ed un'assoluta primaria attenzione ai reali bisogni del cittadino.

Questa è la sfida più ardua. Se si riuscirà a diffondere con efficacia questi concetti, in un prossimo futuro questo progetto e questa idea di innovazione della Pubblica Amministrazione si potranno estendere sulle diverse realtà del territorio italiano.



AISMA: Intelligenza, sicurezza e innovazione per la sanità del futuro

intervista ad Amir Topalovic, CEO di AISMA

In un momento in cui la sicurezza e l'efficienza dei sistemi sanitari italiani sono messe alla prova da sfide sempre più complesse, dalla carenza di risorse al crescente rischio di minacce fisiche e informatiche, l'innovazione diventa la leva per garantire la continuità delle cure e la protezione delle persone.

AISMA, ente di ricerca accreditato come Centro di Ricerca e Trasferimento Tecnologico (CRTT) presso il MISE e Unioncamere, si posiziona come partner strategico per lo sviluppo di soluzioni integrate, in grado di unire intelligenza artificiale, sicurezza e conoscenza dei processi sanitari.

Ne parliamo con Amir Topalovic, CEO di AISMA, per comprendere come la tecnologia possa contribuire a rendere la sanità italiana più sicura, intelligente e umana.

Dottor Topalovic, come definirebbe la visione di AISMA per il settore sanitario?

La nostra visione nasce da un concetto molto semplice: la sicurezza e la salute non possono più essere trattate come ambiti separati. Oggi serve un approccio integrato, in cui la protezione fisica delle strutture, la sicurezza informatica dei dati e il benessere psicologico di operatori e pazienti convivono in un unico ecosistema digitale.

Il nostro lavoro parte dai dati, ma mira sempre alle persone. L'obiettivo è creare soluzioni che migliorino la qualità della vita all'interno delle strutture sanitarie e rendano il sistema più resiliente e consapevole.

Uno dei temi centrali del convegno Securindex è la sicurezza del personale sanitario. In che modo AISMA affronta questa sfida?

È un tema molto attuale e drammaticamente reale. Noi lavoriamo su sistemi di analisi comportamentale avanzata che, grazie a modelli di intelligenza artificiale, riescono a rilevare in tempo reale situazioni di rischio prima che degenerino.



Penso, ad esempio, ai pronto soccorso o alle sale d'attesa: luoghi in cui il livello di stress è elevato e gli episodi di aggressione, purtroppo, frequenti.

I nostri sistemi analizzano gestualità, linguaggio del corpo, tono della voce, espressioni facciali, persino la temperatura corporea, per individuare comportamenti anomali o potenzialmente aggressivi. In caso di allerta, il personale di sicurezza o medico riceve un avviso immediato, potendo intervenire in modo preventivo.

È un modo per proteggere chi lavora, ma anche per migliorare l'esperienza del paziente, riducendo le tensioni e migliorando la comunicazione.

Parliamo di intelligenza artificiale e prevenzione: in che modo AISMA sta sviluppando soluzioni per la medicina predittiva?

Crediamo molto nell'idea di una sanità predittiva e partecipativa, capace di aiutare le persone a prendersi cura di sé in modo proattivo.

Stiamo lavorando su una piattaforma che unisce i dati clinici, lo stile di vita, le informazioni genetiche e ambientali per costruire un quadro dinamico e predittivo della salute del paziente.

Immagini un'app personale, un vero e proprio assistente sanitario digitale, che raccoglie informazioni da smartwatch, sensori o dispositivi medici e le traduce in suggerimenti concreti: dall'alimentazione all'attività fisica, fino alla prevenzione di malattie croniche.

Non è un sostituto del medico, ma un supporto: un modo per fornire dati affidabili e insight utili, aumentando la consapevolezza e riducendo i costi del sistema sanitario.

Molti dei vostri progetti ruotano intorno alla gestione dei dati. Come conciliate innovazione e tutela della privacy?

È una delle nostre priorità. Tutto ciò che facciamo si basa su principi di privacy-by-design, compliance normativa (nello specifico la rispondenza ai requisiti specifici previsti dall'AI Act).

AISMA ha sviluppato piattaforme che integrano la gestione della compliance legale e regolamentare con la tutela dei dati personali del paziente. Ciò significa che ogni informazione, dal referto clinico al tracciamento dei parametri biometrici, viene gestita nel pieno rispetto della normativa, ma resta allo stesso tempo accessibile ai professionisti in modo sicuro e tracciabile. La nostra forza è la capacità di adattare le piattaforme in modo dinamico ai continui aggiornamenti normativi, un aspetto cruciale in un settore in rapida evoluzione come quello sanitario.

AISMA è un ente accreditato come Centro di Ricerca e Trasferimento Tecnologico. In cosa si traduce concretamente questo status per il mondo sanitario?

Significa che possiamo operare come ponte tra la ricerca e la pratica clinica. L'accreditamento CRTT ci consente di avviare contratti di ricerca con strutture sanitarie pubbliche e private, sviluppando soluzioni su misura in ambienti reali, con una governance dei dati chiara e condivisa. Lavoriamo spesso come facilitatori di ecosistemi: uniamo competenze di aziende tecnologiche, università, start-up e ospedali per creare progetti sostenibili e misurabili. È una modalità che

accelera il trasferimento dell'innovazione e garantisce un impatto tangibile, non solo teorico.

Quali saranno, secondo lei, le prossime frontiere dell'innovazione sanitaria?

La vera sfida sarà trasformare il dato in conoscenza utile. Nei prossimi anni vedremo una convergenza tra AI, automazione e human experience: tecnologie sempre più invisibili, integrate nel lavoro quotidiano dei medici e degli infermieri. Non si tratta solo di digitalizzare, ma di restituire tempo e attenzione alle persone. Se l'intelligenza artificiale ci aiuterà a leggere più velocemente una radiografia o a prevedere un rischio clinico, il tempo risparmiato potrà essere dedicato all'ascolto, alla relazione, alla cura. È questo, per me, il significato più profondo di innovazione: usare la tecnologia per rendere la sanità più umana.

In sintesi, come definirebbe l'identità di AISMA oggi?

"AISMA è un laboratorio di idee che diventano soluzioni reali. Sviluppiamo piattaforme e sistemi intelligenti, ma soprattutto costruiamo ponti: tra ricerca e industria, tra dati e decisioni, tra tecnologia e persone. La nostra missione è semplice ma ambiziosa: creare valore umano attraverso l'innovazione tecnologica."

AISMA in breve

- **Centro di Ricerca e Trasferimento Tecnologico (CRTT)** accreditato MISE-Unioncamere
- **Competenze:** Agentic AI, videoanalisi comportamentale, piattaforme software per la gestione dei dati, compliance normativa, infrastrutture intelligence as a service
- **Progetti:** analisi istologica automatizzata, piattaforme di compliance sanitaria, sistemi di monitoraggio comportamentale, assistenti digitali predittivi
- **Missione:** Integrazione dei dati, sviluppo della knowledge base aziendale ed empowerment umano per una sanità più efficiente e centrata sulla persona.



Contatti:
AISMA Srl
info@aisma.it
<https://aismasrl.it/>

Integro, la piattaforma per la sicurezza integrata delle strutture sanitarie

intervista a Alessandro Ferrari, founder e owner di Alesys

Quali soluzioni proponete per rendere più sicura la permanenza all'interno delle strutture sanitarie dei pazienti e degli operatori?

La piattaforma Integro, sviluppata da Alesys, rappresenta una soluzione innovativa per la gestione centralizzata degli allarmi di sicurezza e protezione negli ambienti sanitari. Il suo design intuitivo consente anche agli operatori non specializzati di intervenire prontamente in caso di emergenza. Grazie alla visualizzazione su mappe interattive, è possibile individuare con chiarezza la fonte del pericolo, facilitando una risposta rapida e mirata.

L'implementazione di una soluzione come Integro è fondamentale in ambito sanitario, dove la rapidità e la proattività nella gestione delle emergenze sono essenziali per garantire la sicurezza dei pazienti e del personale, soprattutto in contesti dove l'evacuazione può risultare complessa.

Integro è particolarmente efficace in strutture di grandi dimensioni, dove la presenza di più squadre antincendio, emergenza e manutenzione richiede una gestione compartimentata e coordinata. L'architettura multi-postazione consente infatti di distribuire le operazioni tra diversi punti di controllo, migliorando l'efficienza dell'intervento.

Un altro punto di forza della piattaforma è la possibilità di associare a ogni evento delle procedure che gli operatori devono seguire. Questo sistema non solo guida l'azione in tempo reale, ma permette anche di tracciare ogni fase dell'allarme, registrando tempi e annotazioni utili per il monitoraggio e la revisione di piani di intervento adottati.

La correlazione automatica tra telecamere di videosorveglianza ed evento semplifica il processo decisionale, dando all'operatore una chiara visione del contesto da verificare.

Spesso, quando si parla di sicurezza in strutture sanitarie, l'attenzione si concentra esclusivamente sulla protezione antincendio. Tuttavia, è importante considerare anche gli aspetti legati alla sicurezza dei dati e degli ambienti



sensibili. Ospedali e cliniche custodiscono archivi contenenti informazioni riservate che devono essere protette per motivi di privacy. Inoltre, aree come le farmacie, le zone decontaminate o quelle radioattive rappresentano ambienti ad alto rischio, dove un accesso non autorizzato può comportare gravi conseguenze.

Un'ulteriore sfida è rappresentata dalla varietà di impianti e dispositivi presenti nelle strutture ospedaliere, spesso frutto di diverse fasi di costruzione o ristrutturazione. In questo contesto, Integro si distingue per la sua apertura e compatibilità con molteplici tecnologie, con caratteristiche ed "anzianità" differenti, offrendo un'interfaccia unica che consente di standardizzare le operazioni e semplificare la gestione.

Avete sviluppato o avete in programma soluzioni tecnologiche e/o servizi per applicazioni in ambito sanitario non di security?

Integro rappresenta una piattaforma evoluta capace di integrare, in un'unica interfaccia intuitiva e personalizzabile, qualsiasi tipologia di dispositivo, superando i tradizionali confini del settore della sicurezza. La sua architettura aperta

e flessibile consente di connettere e gestire tecnologie eterogenee, rendendo possibile una supervisione completa e centralizzata di ambienti complessi, come strutture sanitarie, reparti ospedalieri o edifici pubblici.

Attraverso Integro è possibile, ad esempio, collegare un rilevatore audio con misuratore di decibel per il monitoraggio di pazienti affetti da disturbi mentali: il sistema può individuare eventuali situazioni di crisi in tempo reale, consentendo un intervento tempestivo del personale. Allo stesso modo, l'integrazione di sensori di movimento permette di segnalare uscite sospette dai reparti o aree sensibili, aumentando il livello di sicurezza senza compromettere la libertà di movimento dei pazienti o degli operatori.

Un ulteriore vantaggio deriva dal monitoraggio dei dispositivi di rete all'interno dei padiglioni: Integro può segnalare eventuali disservizi, garantendo la continuità delle comunicazioni, in particolare durante le fasce di apertura al pubblico.

Inoltre, il sistema consente il conteggio dei transiti dei visitatori, fornendo dati utili per analisi dei flussi, pianificazione di interventi infrastrutturali o ottimizzazione della gestione degli spazi comuni.

Infine, Integro potrebbe gestire la centralizzazione delle chiamate provenienti dalle stanze, assicurando che ogni richiesta di assistenza venga gestita in modo rapido, tracciabile e coordinato.

Tutte queste funzionalità, combinate in un'unica piattaforma, trasformano Integro in uno strumento strategico per migliorare sicurezza, efficienza operativa e qualità dei servizi.

In un mondo dove l'automatizzazione è vissuta come prioritaria, la figura dell'operatore che ruolo assume?

In un contesto in cui l'automatizzazione è considerata prioritaria, la figura dell'operatore mantiene un ruolo centrale, seppur trasformato. Nei moderni sistemi integrati di sicurezza la tecnologia consente una gestione più rapida, coordinata e precisa delle emergenze. L'automazione elabora dati, attiva protocolli e segnala anomalie in tempo reale, riducendo i margini d'errore e ottimizzando l'efficienza del sistema. Tuttavia, il funzionamento efficace di queste reti complesse non può prescindere dalla presenza e dal giudizio dell'operatore umano.

È infatti l'operatore a interpretare le informazioni, validare gli allarmi e prendere decisioni in base al contesto, distinguendo tra un rischio reale e un falso positivo. In caso di emergenza, è la competenza umana a coordinare gli interventi, gestire le priorità e interagire con il personale sanitario e le squadre di emergenza. L'automatizzazione diventa quindi un supporto intelligente, ma non un sostituto del pensiero critico.

L'operatore evolve da semplice esecutore a supervisore consapevole, capace di dialogare con la tecnologia, controllarne i processi e garantirne l'affidabilità.

In un ospedale, dove la sicurezza è indissolubilmente legata alla vita delle persone, il valore umano resta il vero centro del sistema: l'automazione amplifica le capacità operative, ma è l'esperienza e la responsabilità dell'uomo a renderla realmente efficace.

ALESYS
SECURITY MADE SIMPLE

Contatti:
Alesys
Tel. +39 0331 219436
www.alesys.it

Sanità e Sicurezza nell'Era dell'Intelligenza Artificiale: la visione di Base Digitale

intervista a Nils Fazzini, Sales Director Area Security Solutions di Base Digitale

Garantire la sicurezza nelle strutture sanitarie significa oggi molto più che proteggere accessi e infrastrutture: significa assicurare la continuità delle cure, tutelare il personale e i pazienti e proteggere un patrimonio informativo e tecnologico sempre più complesso.

In questo scenario, Base Digitale (BD) si propone come partner tecnologico di riferimento per il settore sanitario, grazie a un approccio integrato che unisce competenze di sicurezza fisica, cyber security e intelligenza artificiale adattiva.

Quali soluzioni proponete per rendere più sicura la permanenza all'interno delle strutture sanitarie dei pazienti e degli operatori?

Le strutture sanitarie moderne sono veri e propri ecosistemi complessi, dove la sicurezza non può più essere gestita in modo frammentato.

Base Digitale risponde a questa esigenza con Centrax, la piattaforma Open PSIM (Physical Security Information Management) che integra e governa in un unico ambiente operativo tutte le componenti di sicurezza: videosorveglianza, controllo accessi, antintrusione, rilevazione incendi, gestione emergenze e tracciamento asset.

Grazie a Centrax, gli ospedali e le strutture sanitarie possono:

- centralizzare eventi e allarmi provenienti da tecnologie e fornitori diversi, riducendo i tempi di reazione e migliorando la consapevolezza situazionale;
- automatizzare le procedure operative, garantendo il rispetto dei protocolli e degli SLA anche in contesti ad alta intensità come pronto soccorso o reparti critici;
- coordinare in tempo reale operatori, vigilanza e forze dell'ordine attraverso workflow digitali e tracciati.



Il risultato è un sistema che “vede, comprende e reagisce”, coordinando tecnologie e persone in modo proattivo per garantire la sicurezza e la continuità delle attività cliniche.

Avete sviluppato o avete in programma soluzioni tecnologiche e/o servizi per applicazioni in ambito sanitario non di security?

Oltre alla sicurezza fisica, BD sta lavorando su soluzioni basate sull'Intelligenza Artificiale adattiva e distribuita per migliorare la qualità e la continuità delle cure.

Grazie anche alla collaborazione con società del Gruppo SESA come Var Group e Computergross, e con primari player tecnologici, BD ha sviluppato piattaforme in grado di applicare algoritmi di analisi video avanzata direttamente sui flussi dei sistemi di videosorveglianza già presenti nelle strutture sanitarie.

Questa tecnologia consente di:

- rilevare comportamenti anomali o situazioni di rischio come aggressioni al personale, cadute, deambulazioni notturne o tentativi di fuga di pazienti fragili;

- monitorare da remoto pazienti affetti da Alzheimer o demenza, garantendo sicurezza e privacy senza presidi fisici costanti;
- supportare la teleassistenza post-operatoria, ad esempio nel caso di trapianti o riabilitazioni, tramite analisi video non invasive e anonimizzate;
- anticipare emergenze correlando dati provenienti da sensori IoT, reti antincendio e dispositivi ambientali.

L'adozione dell'AI adattiva “on-top” dei sistemi esistenti permette di valorizzare le infrastrutture già installate, riducendo tempi e costi di implementazione e mantenendo il pieno rispetto delle normative sulla privacy e sul trattamento dei dati sanitari.

Qual è la vostra visione di lungo periodo sul ruolo della sicurezza nel mondo sanitario digitale?

Il terzo pilastro della nostra strategia è la governance dei dati.

La crescente convergenza tra mondo fisico e digitale – con dispositivi medicali connessi, piattaforme cloud e sensori intelligenti – impone un nuovo paradigma di sicurezza basato su interconnessione e resilienza.

Attraverso la suite di servizi gestiti di cybersecurity, BD protegge non solo gli impianti fisici ma anche le infrastrutture IT e OT, garantendo la conformità alle

principali normative europee, tra cui NIS2, AI Act e IT Asset Management (ITAM).

L'obiettivo non è soltanto difendere, ma abilitare: un ecosistema sicuro favorisce la collaborazione tra reparti, riduce gli incidenti, migliora l'esperienza dei pazienti e rafforza la fiducia nelle strutture sanitarie, pubbliche e private.

Parliamo quindi di un futuro human-centered?

Per Base Digitale, la tecnologia è davvero efficace solo se rimane al servizio delle persone.

Ogni progetto viene sviluppato secondo il principio “Human in the Loop”: l'intelligenza artificiale non sostituisce l'operatore, ma ne amplifica la capacità di analisi e decisione, liberandolo da attività ripetitive per concentrarsi su ciò che conta davvero – la sicurezza e il benessere dei pazienti.

Il metodo BD si fonda su tre direttrici:

1. Integrazione dei sistemi, per un controllo coordinato e intelligente;
2. Intelligenza distribuita, per aumentare la capacità predittiva e ridurre i tempi di risposta;
3. Centralità dell'uomo, per mantenere la tecnologia coerente con la missione del settore sanitario: proteggere, assistere, curare.



Contatti:
Base Digitale
www.basedigitale.com

Sicurezza fisica e cybersecurity per il mondo della sanità da Cyberloop

intervista ad Alessandro Molari, Amministratore Delegato di Cyberloop - Gruppo Cittadini dell'Ordine

A fine 2024 i Cittadini dell'Ordine, azienda storica del mondo della vigilanza e della sicurezza in Italia e in Europa, hanno compiuto un passo fondamentale, accogliendo nel loro Gruppo Cyberloop, società specializzata in servizi di cybersecurity. Un'operazione che segna l'evoluzione naturale di una realtà che, da oltre 155 anni, interpreta la sicurezza come valore in continuo cambiamento. Oggi la frontiera non è più solo fisica ma anche digitale: due facce della stessa medaglia che i Cittadini dell'Ordine integrano per offrire protezione completa.

Quali sono le principali minacce legate alla sicurezza informatica che possono colpire le strutture sanitarie?

La sanità è un luogo in cui tecnologia e cura convivono in modo indissolubile. Ogni minuto di indisponibilità di un sistema può diventare un disagio per il personale e un rischio per il paziente. Oggi le minacce più insidiose non sono solo quelle che "bussano forte alla porta", come gli attacchi che bloccano i sistemi e chiedono un riscatto, ma anche quelle silenziose, che cercano le crepe lasciate dall'età delle infrastrutture, dalle integrazioni affrettate o da procedure non sempre aggiornate. Nelle reti ospedaliere convivono applicazioni moderne e apparati storici, reparti con esigenze diverse e fornitori che accedono da remoto per la manutenzione. In questo mosaico, anche un clic su una mail ben fatta o una configurazione dimenticata possono aprire la strada a interruzioni dei servizi, sottrazione di dati sensibili e lunghe giornate di ripristino. C'è poi un capitolo a sé: i macchinari e i dispositivi connessi, dai monitor dei parametri vitali alla diagnostica per immagini. Sono strumenti preziosi, spesso progettati per durare molti anni, che non sempre possono essere aggiornati con la stessa velocità del resto del parco tecnologico. Proteggerli significa tenere insieme continuità clinica, sicurezza del dato e serenità degli operatori, senza rallentare il lavoro di reparto.



Cosa è in grado di offrire Cyberloop come protezione?

La nostra proposta nasce da un principio semplice: la sicurezza deve essere utile al lavoro quotidiano, non un freno. Per questo coniughiamo metodo, tecnologia e presenza continua. Partiamo dall'ascolto delle direzioni e dei reparti, mappiamo ciò che davvero conta per la cura e disegniamo un percorso che renda i sistemi più affidabili giorno dopo giorno. Non ci limitiamo a installare strumenti: costruiamo un presidio che osserva i segnali deboli, individua gli eventi anomali e aiuta a intervenire in modo tempestivo, a qualsiasi ora. Insegniamo alle persone come riconoscere i rischi senza paura, mettiamo ordine nelle procedure, organizziamo il ripristino in modo che un imprevisto non diventi un fermo prolungato. L'appartenenza al Gruppo Cittadini dell'Ordine ci consente di integrare digitale e fisico, perché gli accessi, i varchi, i flussi video e le regole di reparto sono parte dello stesso disegno. Il risultato è una protezione completa che unisce prevenzione, monitoraggio e risposta, pensata per ambienti ad alta intensità operativa dove l'unica vera misura del successo è la continuità del servizio al paziente.

Potete proteggere, oltre i device e le reti, anche i macchinari IoT presenti nelle strutture ospedaliere?

Sì, ed è uno dei terreni in cui portiamo più valore attraverso le nostre soluzioni di IoT Security Monitoring. Trattiamo i macchinari connessi come si tratterebbe un reparto delicato: con attenzione, gradualità e regole chiare. Cominciamo dal conoscere, perché non si può proteggere ciò che non si vede; ricostruiamo quindi chi parla con chi, in quali orari e per quali scopi, rispettando i ritmi della clinica. Da qui definiamo confini intelligenti che separano ciò che deve restare separato, limitiamo le comunicazioni superflue e regoliamo gli accessi dei manutentori esterni. Quando non è possibile aggiornare subito un dispositivo, adottiamo misure che lo mettano al riparo senza interrompere la sua funzione. Tutto avviene in dialogo con l'ingegneria clinica, con la regia del CISO e con il coinvolgimento degli operatori, perché la protezione dei macchinari non è un progetto "IT", ma un'azione condivisa che salvaguarda la qualità del percorso di cura.

Potete raccontare una vostra case history particolarmente significativa?

Penso a un grande ospedale italiano in cui siamo stati chiamati dopo un evento che aveva creato disservizi nelle prenotazioni e tensione in diversi reparti. Non abbiamo portato "una soluzione", abbiamo costruito una squadra con IT, ingegneria clinica e direzione sanitaria. Nei primi giorni abbiamo rimesso in fila le priorità, riportato sotto controllo le aree più esposte e ridato stabilità ai servizi critici. Nelle settimane successive abbiamo ordinato gli accessi dei fornitori, semplificato i passaggi più fragili dei

processi e preparato insieme le prove di ripristino, così che tutti sapessero cosa fare, in quanto tempo e con quali responsabilità. L'effetto più visibile è stato la riduzione degli allarmi inutili e dei tempi di risposta; quello più importante è stato il cambio di clima: meno rincorse, più consapevolezza, più fiducia che i sistemi potessero sostenere il lavoro invece di ostacolarlo. È la dimostrazione che, quando sicurezza fisica e digitale remano nella stessa direzione, la struttura guadagna resilienza reale.

In sintesi, portiamo nelle realtà sanitarie una sicurezza che parla il linguaggio dell'operatività e della trasformazione digitale. Valorizziamo le persone con formazione concreta, rendiamo i processi più chiari e prevedibili, cuciamo la tecnologia sui bisogni di reparto e presidiamo nel tempo per evitare che i risultati si disperdano. Per i nostri clienti questo significa meno interruzioni e più qualità percepita, dati protetti e procedure trasparenti, investimenti che generano valore perché abilitano un ambiente di lavoro affidabile, moderno e centrato sul paziente. È così che la sicurezza diventa un vantaggio competitivo e una promessa mantenuta ogni giorno.

Se dovessi riassumere la nostra proposta in una sola idea, direi che Cyberloop porta nella sanità una sicurezza "operabile", disegnata sui percorsi e non sopra i percorsi. È un lavoro di squadra con le strutture, sostenuto da competenze specialistiche, monitoraggio continuo e una cultura della prevenzione che rende la tecnologia affidabile e l'organizzazione pronta. In questo modo la protezione diventa un abilitatore della qualità di cura e della fiducia dei pazienti, oggi e domani.



Contatti:
Gruppo Cittadini dell'Ordine
info@cyberloop.it
segr.dir.commerciale@cittadinidellordine.com

Sicurezza integrata per la Sanità secondo l'Istituto di vigilanza Coopservice

intervista a Luca Pacitti, direttore operativo di Istituto di vigilanza Coopservice

Quali soluzioni proponete per rendere più sicura la permanenza all'interno delle strutture sanitarie dei pazienti e degli operatori?

Il contesto delle strutture sanitarie è oggi estremamente articolato e in continua evoluzione. Garantire la sicurezza in ambienti come ospedali, pronto soccorso, reparti psichiatrici e case di cura rappresenta una sfida quotidiana, che richiede competenze specifiche, flessibilità operativa e una profonda conoscenza del settore.

Secondo l'Osservatorio Nazionale sulla Sicurezza degli Esercenti le Professioni Sanitarie e socio-sanitarie tra le professioni che registrano un numero crescente di episodi di violenza spiccano quelle sanitarie. Nel 2024 sono state segnalate oltre 18mila aggressioni (+15% rispetto al 2023), per un totale di circa 22mila operatori coinvolti, soprattutto donne (più del 60%). A essere più colpiti sono gli infermieri (oltre il 55%), seguiti da medici (17,3%) e operatori sanitari (9,5%). I luoghi più interessati dal fenomeno sono gli ospedali, in particolare: Pronto Soccorso, Servizi Psichiatrici di Diagnosi e Cura e Aree di Degenza.

In questo scenario, l'esperienza maturata da Istituto di Vigilanza Coopservice in oltre 30 ospedali e presidi sanitari ci consente di offrire soluzioni mirate e di costruire modelli di servizio personalizzati, capaci di rispondere alle esigenze specifiche di ogni struttura. La sicurezza non può essere standardizzata: ogni ambiente sanitario ha caratteristiche proprie, sia in termini architettonici che di tipologia di pazienti e operatori. Una casa di cura, ad esempio, presenta criticità diverse rispetto a un pronto soccorso, e richiede un approccio differente.

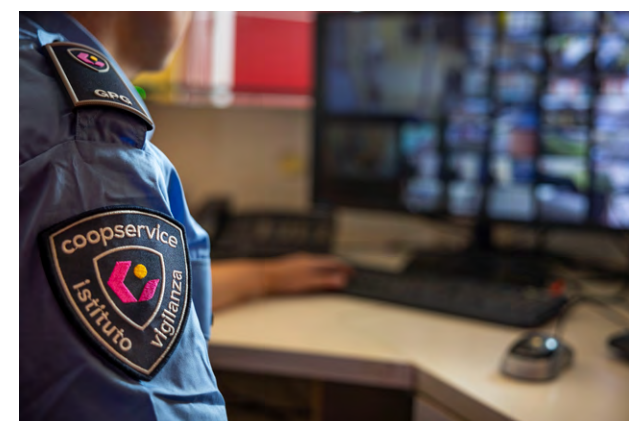
Tra i servizi considerati imprescindibili in determinati contesti, vi sono il presidio fisso e il pattugliamento dinamico da parte di guardie giurate, formate appositamente per operare in ambienti sanitari. Queste figure professionali



non solo rappresentano un deterrente visibile, ma sono anche preparate per gestire situazioni complesse, come accessi non autorizzati, episodi di aggressività o emergenze improvvise. Il collegamento diretto con la Centrale Operativa consente di attivare tempestivamente le forze dell'ordine, garantendo una risposta rapida ed efficace.

A questi servizi affianchiamo altre soluzioni, più tecnologiche, come i sistemi di controllo accessi evoluti, che regolano i flussi di visitatori in entrata e in uscita, e la videosorveglianza con intelligenza artificiale che, opportunamente addestrata, si rivela estremamente efficace nel rilevare comportamenti sospetti o situazioni di rischio, contribuendo in modo significativo alla prevenzione degli incidenti.

Poi ci sono tecnologie, come l'audio detection, che permettono di attivare allarmi in base a parole chiave pronunciate nelle aree sorvegliate, mentre sistemi di deterrenza vocale possono emettere messaggi di avviso automatici in risposta a eventi rilevati dalle telecamere. Queste soluzioni, integrate in un ecosistema di sicurezza, aumentano il livello di protezione e riducono i tempi di reazione.



Avete sviluppato o avete in programma soluzioni tecnologiche e/o servizi per applicazioni in ambito sanitario non di security?

La nostra visione della sicurezza si sta ampliando verso un concetto più integrato, che include l'uso intelligente della tecnologia in altre applicazioni.

Stiamo lavorando a soluzioni già consolidate in altri ambiti, come il sistema "man down", che consente di rilevare automaticamente situazioni critiche, come cadute o malori, sia per il personale sanitario che per i pazienti. Questo sistema può essere integrato con dispositivi wearable e rappresenta un valido supporto nei contesti sanitari.

Un altro ambito di sviluppo riguarda la videoanalisi comportamentale, che permette di monitorare in tempo reale i movimenti dei pazienti e di rilevare eventi anomali, come cadute, immobilità prolungata o comportamenti incoerenti. In caso di rilevamento, il sistema invia un alert consentendo un intervento tempestivo.

Stiamo inoltre esplorando l'utilizzo del segnale Bluetooth per il monitoraggio degli spostamenti dei pazienti, in particolare quelli affetti da Alzheimer o da altre patologie neurodegenerative. Questo tipo di tecnologia consente di rilevare allontanamenti non autorizzati e di intervenire prima che la situazione diventi critica.

In conclusione, come immaginate l'evoluzione del ruolo degli istituti di vigilanza nel settore sanitario nei prossimi anni?

Crediamo che il ruolo degli istituti di vigilanza sia destinato a evolversi da semplice presidio fisico a partner tecnologico e operativo delle strutture sanitarie. La sicurezza sarà sempre più integrata con la gestione dei dati, la protezione delle strutture e la continuità dei servizi.

La sfida sarà quella di anticipare i bisogni, investire in formazione e innovazione, e costruire soluzioni su misura che mettano al centro la persona, la tecnologia e la prevenzione.

 **coopservice**
ISTITUTO DI VIGILANZA
Security services provider

Contatti:
Istituto di Vigilanza Coopservice
Via Rochdale, 5 Reggio Emilia
www.vigilanzacoopservice.it

Il lato umano della tecnologia: come le bodycam di Reveal supportano gli eroi della sanità

intervista a Luigi Lagonigro, Sales Director Europe & Latin America at Reveal Media

Quali sono le proposte di Reveal per il settore sanitario?

Il personale sanitario lavora ogni giorno con impegno per offrire cure e assistenza alle persone nei momenti di maggiore bisogno. Tuttavia, gli operatori in prima linea si trovano sempre più spesso ad affrontare situazioni di abuso e aggressione durante il servizio.

Dal monitoraggio effettuato dall'Osservatorio Nazionale sulla Sicurezza degli Esercenti le Professioni Sanitarie e Sociosanitarie (ONSEPS), nel 2024 è stato registrato un aumento del 15% delle aggressioni, per un totale di oltre 18.000 episodi. Complessivamente, sono stati coinvolti circa 22.000 operatori sanitari in tutto il territorio nazionale.

(Ministero della Salute – Giornata nazionale contro la violenza nei confronti degli operatori sanitari e sociosanitari. Schillaci: la sicurezza del personale è prioritaria)

A seguito dei risultati positivi dimostrati dall'impiego delle bodycam Reveal nel settore sanitario del Regno Unito, il nostro obiettivo è contribuire a migliorare la sicurezza e la fiducia del personale sanitario ovunque.

Le bodycam con schermo frontale si sono dimostrate efficaci nel prevenire e ridurre gli episodi di aggressione, garantendo maggiore sicurezza a chi si prende cura di noi. Reveal offre una soluzione video completa, sicura e collaudata, progettata specificamente per gli ambienti sanitari — inclusi ospedali, servizi di ambulanza, reparti di salute mentale e assistenza domiciliare o territoriale.

La nostra soluzione combina hardware ad alte prestazioni, gestione dei dati conforme al GDPR e formazione dedicata al personale, assicurando privacy, trasparenza e sicurezza in contesti sanitari sensibili.

Avete evidenze dell'impatto reale nel settore sanitario?

Sì. Le bodycam di Reveal sono state implementate con successo in diversi contesti sanitari del Regno Unito, mostrando miglioramenti misurabili in termini di sicurezza, comportamento e benessere del personale.



L'Oxford University Hospitals NHS Foundation Trust ha adottato le bodycam Reveal come parte della propria strategia per migliorare la sicurezza di personale e pazienti nei reparti a maggior rischio, come il pronto soccorso.

Le indagini hanno mostrato che, prima del progetto pilota, solo il 63% del personale riteneva le bodycam necessarie, dopo la sperimentazione, la percentuale è salita al 96%, riflettendo un notevole cambiamento di percezione in seguito all'utilizzo sul campo.

Il Trust ha riportato un chiaro effetto deterrente, un miglioramento del morale del personale e una maggiore fiducia da parte del pubblico, mantenendo al contempo la piena conformità alle norme sulla protezione dei dati e sulla privacy grazie al sistema sicuro DEMS 360.

Il responsabile del progetto ha dichiarato: *“Le bodycam sono visibili – si notano sull'uniforme – quindi, a mio avviso, la loro sola presenza basta a spingere alcune persone a moderare il proprio comportamento. Tuttavia, esistono studi che confermano che le persone tendono effettivamente a calmarsi più rapidamente quando possono vedersi riprese sullo schermo. Lo schermo frontale delle bodycam Reveal è quindi un ottimo elemento di design, poiché può contribuire ad attenuare gli eventi prima che si verifichi qualsiasi forma di aggressione fisica.”*

Questi risultati dimostrano che le bodycam Reveal non si limitano a documentare gli episodi, ma contribuiscono attivamente a prevenire le aggressioni, migliorare il benessere del personale e promuovere ambienti sanitari più sicuri e rispettosi.

Quali sono i principali casi d'uso nel settore sanitario?

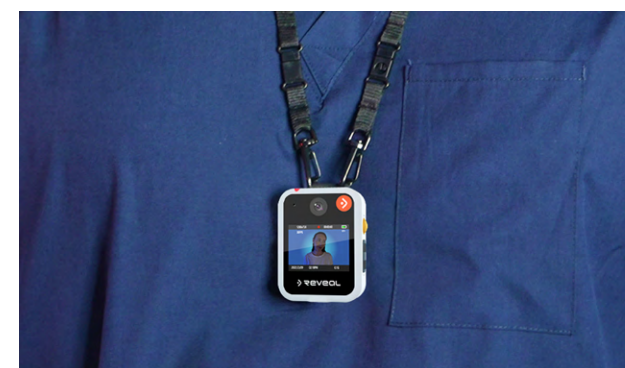
Le bodycam vengono utilizzate sempre più spesso in diversi contesti sanitari per proteggere il personale, supportare la trasparenza e favorire la de-escalation in situazioni critiche. Il loro scopo va oltre la semplice raccolta di prove: svolgono un ruolo attivo nel creare un luogo di lavoro più sicuro e rispettoso, sia per i professionisti sanitari sia per i pazienti.

Casi d'uso tipici:

- Servizi di ambulanza: protezione del personale in prima linea, deterrenza delle aggressioni e documentazione accurata degli incidenti.
- Reparti di emergenza: supporto agli operatori in ambienti ad alta pressione, aiuto nella gestione di situazioni tese e garanzia di trasparenza nelle interazioni con i pazienti.
- Unità di salute mentale: promozione di interventi pacifici e supporto alle strategie di de-escalation durante incontri potenzialmente complessi.
- Assistenza domiciliare e territoriale: tutela degli operatori che lavorano da soli, costruzione di fiducia con i pazienti e garanzia di responsabilità durante le visite a domicilio.

Caratteristiche operative delle bodycam Reveal per il settore sanitario:

- Schermo frontale che funge da deterrente visivo mostrando che la registrazione è in corso.
- Funzione di preregistrazione (fino a 2 minuti) per catturare i momenti chiave prima dell'attivazione.
- Design robusto e leggero con autonomia di 10-12 ore, adatto ai turni più lunghi.
- Registrazione in alta definizione anche in condizioni di scarsa illuminazione, per ottenere prove chiare e affidabili.



- Caricamento e archiviazione sicuri tramite DEMS 360, con gestione dei dati conforme al GDPR e controllo degli accessi. Il nostro modello più recente, la **Reveal R1**, è la bodycam più piccola e leggera mai realizzata, progettata specificamente per il settore sanitario e altri contesti di prima linea. Combina comfort, connettività e affidabilità, mantenendo lo stesso effetto deterrente e lo stesso livello di sicurezza dei dati dei modelli più grandi.

In sintesi, qual è l'impatto complessivo delle bodycam Reveal nell'ambiente sanitario?

Le bodycam Reveal sono molto più che dispositivi di registrazione — sono strumenti che favoriscono una cultura di sicurezza e rispetto all'interno del settore sanitario.

Grazie alla registrazione visibile e frontale, contribuiscono a dissuadere le aggressioni, ridurre i conflitti e diminuire la frequenza e la gravità degli episodi di violenza, proteggendo sia il personale che i pazienti.

Consentono agli operatori in prima linea e a chi lavora in autonomia di contare su una tecnologia affidabile e facile da usare, mentre forniscono prove accurate che supportano le indagini e riducono il rischio organizzativo.

Le bodycam migliorano il benessere, il morale e la fidelizzazione del personale, contribuendo a rafforzare la fiducia del pubblico nelle strutture sanitarie.

In definitiva, una bodycam Reveal diventa un simbolo visibile di cura, professionalità e protezione per coloro che dedicano la propria vita ad aiutare gli altri.



Contatti:
Reveal
sales@revealmedia.com
www.revealmedia.it

L'apporto delle guardie giurate per la sicurezza nei presidi sanitari

intervista a Anna Maria Domenici, Presidente UNIV

Quali compiti possono svolgere le guardie giurate in ambito sanitario?

Partiamo da un assunto: ospedali, aree di pronto soccorso, poliambulatori e residenze sanitarie assistenziali sono contesti complessi, caratterizzati da un flusso costante di persone e da situazioni delicate, dove la tensione emotiva può facilmente sfociare in comportamenti aggressivi o in rischi per l'incolumità del personale e dei pazienti.

In questo ambito le guardie giurate, opportunamente formate e coordinate, possono contribuire in misura determinante a mantenere l'ordine e a prevenire episodi di violenza o danneggiamento. Le guardie giurate presidiano gli accessi, regolano l'afflusso del pubblico, impiegano la videosorveglianza o altre tecnologie anche ad intelligenza artificiale, e infine supportano il personale sanitario in caso di situazioni critiche garantendo il rispetto delle norme di sicurezza, soprattutto in aree sensibili come triage e pronto soccorso, reparti psichiatrici o aree COVID. Cruciale, poi, è la collaborazione del personale di vigilanza con le forze dell'ordine: si pensi solo alla gestione di pazienti sottoposti a trattamento sanitario obbligatorio o potenzialmente pericolosi come i carcerati o le persone mentalmente fragili. Fermo restando che il personale privato di sicurezza non può intervenire fisicamente sul paziente, il fatto di allertare tempestivamente le forze di polizia, assicurare l'area e assistere le forze dell'ordine resta un contributo essenziale.

Fondamentale in questo senso è la capacità di interazione della vigilanza con il personale sanitario e soprattutto con i pazienti: serve un approccio discreto ma deciso, basato su empatia e comunicazione per ridurre la conflittualità, fare de-escalation e gestire le emergenze in maniera controllata e senza generare panico. La formazione è dunque un elemento chiave.



Quali interventi potrebbero rendere più efficace l'apporto della vigilanza privata?

Il settore ospedaliero è finito più volte sotto i riflettori per i ripetuti episodi di cronaca che hanno interessato gli operatori sanitari. Episodi che – con assai minore clamore mediatico – non hanno certo risparmiato il personale di sicurezza, spesso primo filtro tra pazienti e operatori sanitari.

Anche su pressione di UNIV, il decreto 1° Ottobre 2024, n. 137 è venuto in soccorso al settore privato estendendo al personale di vigilanza attivo nei presidi sanitari la stessa aggravante che vige oggi per le aggressioni al personale sanitario. Si tratta di un primo, incerto passo che può aiutare i nostri lavoratori quando la degenerazione violenta è ormai deflagrata.

Ragionando però in una più ampia ottica di prevenzione, si potrebbe cominciare con l'aumentare il personale di vigilanza privata al fine di moltiplicare l'effetto deterrente (si consideri che spesso una sola guardia presidia un intero sito sanitario anche per 10-12 ore consecutive) o con l'autorizzare equipaggiamenti di protezione specifici.

Sarebbe poi utile imporre la figura del Security Manager almeno nelle principali realtà e aziende ospedaliere – cosa che già accade in alcune Regioni italiane. Questa figura professionale, in grado di mappare le criticità e di analizzare i rischi, potrebbe anche impostare e coordinare il graduale affiancamento dei nostri operatori con le forze di pubblica sicurezza. Oltre ad arginare gli episodi di violenza, le ASL ne ricaverebbero un beneficio in termini di qualità del servizio, potendo impiegare guardie giurate già formate senza dover attendere i tempi tecnici legati alle gare e ai concorsi pubblici.

Fondamentale, però, che qualunque iniziativa per elevare la sicurezza delle guardie giurate venga condivisa anche con chi compra i servizi e rappresenti l'occasione per portare all'attenzione delle ASL e delle strutture sanitarie private anche la questione del riconoscimento dei livelli retributivi. Si tenga presente che il rinnovo del CCNL di categoria ha quasi raddoppiato il costo del lavoro, ma le committenze -

soprattutto, ed è cosa allarmante, quelle pubbliche – si sono arroccate dietro le clausole contrattuali per non revisionare i prezzi dei servizi. Un altro aspetto che desta amarezza è la tipologia di personale impiegato nella sanità con funzioni di security: spesso non guardie giurate, ma addetti al controllo accessi, portieri o steward. Ricordo che il DM 269/2010 inquadra le strutture sanitarie tra i luoghi sensibili, imponendo quindi di impiegare soltanto guardie giurate decretate. Queste, assieme a molte altre, storture mettono in pericolo il sistema della sicurezza in un settore critico. Ricordo sommessamente che la sicurezza negli ospedali non è soltanto un problema di ordine pubblico, ma un investimento nella fiducia dei cittadini verso il sistema sanitario nazionale. Le guardie giurate sono spesso le prime a intercettare il disagio, la rabbia o la paura che attraversano i corridoi del pronto soccorso. È tempo di riconoscere il loro ruolo, sia sul piano normativo, sia sul piano del riconoscimento economico.





La sicurezza informatica del Gruppo Cittadini dell'Ordine

CYBERLOOP

PROTEGGIAMO LA TUA AZIENDA
ANCHE NEL MONDO DIGITALE

SOC – Security Operation Center 24/7

Costante monitoraggio dei sistemi informatici e risposta e gestione in tempo reale degli attacchi.

Assessment e Vulnerability Test

Analisi della sicurezza dei tuoi sistemi, individuazione delle vulnerabilità e progetti di cybersecurity mirati ed adeguati alla tua realtà.

Consulenza e compliance

Supporto all'adeguamento alle normative (NIS2, GDPR, ISO) e progettazione personalizzata per migliorare la sicurezza informatica e ridurre i rischi aziendali.

Formazione e cultura della sicurezza

Corsi personalizzati per aziende e dipendenti: dalla consapevolezza dei rischi digitali alla gestione degli incidenti informatici



 GRUPPO CITTADINI DELL'ORDINE

Da oltre **155 anni** i Cittadini dell'Ordine garantiscono **sicurezza e protezione fisica, tecnologica e logistica**. Oggi, con Cyberloop, portiamo la stessa affidabilità anche nella **cybersicurezza**, per difendere i tuoi dati e le tue infrastrutture.

www.cittadinidellordine.com

 800 010 298

www.cyberloop.it

NON IMPROVVISARE...
CI SONO SOLUZIONI ADEGUATE



 **INTÈGRO**
SECURITY MADE SIMPLE

Integro è un sistema completo di supervisione e gestione che integra in una unica interfaccia la gestione di sistemi video, audio, antintrusione, antincendio, controllo accessi e di impianti tecnologici



ALESYS
SECURITY MADE SIMPLE

Alesys srl - Via Padre Reginaldo Giuliani 539, 21044 Cavarina con Premezzo (VA) - Italia - info@alesys.it - www.alesys.it - (+39) 0331 219436

ERMES, la comunicazione diventa semplice, potente e connessa

comunicato aziendale

ERMES introduce la nuova versione del software **SoundLAN.SW** che, congiuntamente agli altoparlanti alimentati in POE di ERMES, è particolarmente adatta alla realizzazione di sistemi di diffusione sonora in IP in grado di ottenere, con la massima flessibilità, le funzioni di:

- Annunci al pubblico (PA)
- Notifiche di emergenza
- Allarmi di sicurezza
- Musica di sottofondo

Configurazione facile. Integrazione totale.

La suite software SoundLAN.SW è composta di due moduli:

il **SoundLAN Scheduler** che gestisce la diffusione sonora

automatica su base di una programmazione temporale e il **EASY.PA** che gestisce la diffusione sonora in modalità manuale. Questi moduli consentono di inviare agli altoparlanti streaming audio di messaggi pre-registrati, playlist di brani memorizzati localmente o anche di diffondere una WebRadio.

Lo streaming audio può essere indirizzato ad un singolo altoparlante, a gruppi di altoparlanti o a tutti gli altoparlanti installati sul sistema rendendo semplicissima la suddivisione in zone dell'impianto.

Grazie all'utilizzo di altoparlanti e trombe in IP, al protocollo di comunicazione Peer-To-Peer ed alla possibilità di utilizzare reti dati esistenti, anche condivise con altri sistemi come ad esempio la videosorveglianza, è possibile disporre di un sistema che si installa semplicemente ed è subito operativo.

Prestazioni al top, ovunque.

I sistemi di diffusione sonora di ERMES, progettati per ambienti acustici difficili, implementano algoritmi di elaborazione del suono che offrono un audio perfettamente intelligibile anche in spazi rumorosi ed in ambienti critici come le gallerie stradali.

Una vera svolta.

Le trombe in IP di ERMES offrono anche la funzione di reversibilità (talk-back) assicurando sia l'ascolto ambientale sia la comunicazione bidirezionale in tempo reale tra team di sicurezza, sale di controllo e personale sul campo.

Dai grandi edifici aziendali, alle infrastrutture per i trasporti o alle aree aperte al pubblico gli altoparlanti IP di Ermes unitamente alla software SoundLAN.SW sono pronti a supportare tutte le esigenze.



Contatti:
ERMES Elettronica
Tel. +39 0438 308470
www.ermes-cctv.com



SOLUZIONI AUDIO IN IP

Soluzione **smart** per colonnine e armadi **SOS** per strade e gallerie

Colonnine SOS in itinere e armadi SOS di galleria che si interfacciano con i sistemi SIV di MOVYON e RMT di ANAS.



Ermes Elettronica – Via Treviso 36, San Vendemiano (TV)
ermes@ermes-cctv.com - 0422-308470 - www.ermes-cctv.com

KEYDOM di FAAC: la piattaforma intelligente che integra sicurezza fisica e logica

comunicato aziendale

In un mondo in cui la sicurezza rappresenta una priorità strategica e trasversale a molteplici settori, la gestione degli accessi ha assunto un ruolo centrale. Controllare chi può entrare, quando e in quali aree, non è più soltanto una questione di protezione degli spazi, ma anche di efficienza operativa, continuità dei processi e governance aziendale. Per rispondere a queste esigenze, FAAC ha sviluppato Keydom, la piattaforma per il controllo accessi pensata per garantire una gestione efficace, flessibile e integrata su qualsiasi scala applicativa.

Scalabilità e controllo totale degli accessi

Keydom è progettata per assicurare una sicurezza completa, in grado di unire, in un'unica infrastruttura, la gestione degli accessi fisici e logici. La piattaforma permette il controllo di fino a 4.096 varchi e di un massimo di 500.000 utenti, garantendo prestazioni eccellenti in un piccolo edificio come in una grande realtà multisito.

L'autenticazione avviene tramite badge, QR code, targhe dei veicoli con lettura ANPR o tag RFID, adattando le modalità di accesso al livello di protezione richiesto o al volume dei flussi. Il sistema è inoltre in grado di identificare, contare e localizzare gli individui all'interno del perimetro protetto, restituendo report aggiornati in tempo reale, fondamentali per audit e verifiche post-evento.

Architettura versatile e gestione semplificata

Keydom è disponibile in versione embedded, ideale per siti singoli e realtà più compatte, oppure enterprise per infrastrutture estese e complesse. L'interfaccia web-based, intuitiva e accessibile anche da remoto, consente la gestione centralizzata dei varchi, riducendo la necessità di presidio fisico e ottimizzando l'impiego delle risorse.

La flessibilità dell'ambiente di configurazione permette di aggiornare rapidamente permessi e ruoli di accesso, migliorando la sicurezza e la capacità di risposta a cambi organizzativi o a mutamenti del livello di allerta.

Integrazione e interoperabilità evoluta

Keydom si integra perfettamente con i prodotti FAAC per la protezione dei varchi pedonali e veicolari, come i tornelli FlowMotion® o i dissuasori a scomparsa delle serie J e JS. Tuttavia, uno dei suoi principali punti di forza risiede nella capacità di interfacciarsi con tecnologie di altri produttori. La compatibilità con protocolli standard e web services consente l'integrazione con piattaforme esistenti — dai sistemi di supervisione (PSIM) al controllo presenze, fino al Building Management System.

Questa interoperabilità:

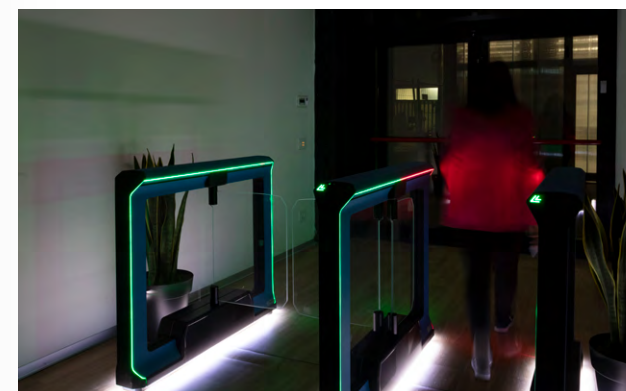
- elimina la necessità di sostituire dispositivi funzionanti
 - riduce i costi di transizione e di infrastruttura
 - permette la costruzione di sistemi di sicurezza personalizzati
- Il risultato è un ecosistema di sicurezza aperto, dinamico e protetto.

Logistica e trasporti: gestione dei flussi come leva strategica

La logistica rappresenta uno degli ambiti in cui Keydom esprime al meglio le proprie potenzialità. La piattaforma gestisce in modo coordinato mezzi e persone, controllando l'identità dei soggetti, la destinazione dei carichi e la permanenza all'interno del sito. Un ruolo chiave è affidato alle colonne veicolari FAAC, con funzioni di lettura targhe, riconoscimento QR code e abilitazione tramite badge, e alle barriere automatiche Magnetic ACCESS XL2 e ACCESS XXL, in grado di controllare anche i varchi più impegnativi, come porti, aeroporti e terminal merci.

Il flusso operativo può essere completamente digitalizzato: il trasportatore prenota l'accesso su portale dedicato, riceve un codice univoco e, all'arrivo, si identifica senza contatto con l'operatore. Keydom assegna automaticamente l'autorizzazione alle baie operative, monitorando ogni movimento fino all'uscita del mezzo.

Tempistiche più rapide, riduzione delle congestioni e maggior precisione dei processi diventano vantaggi reali e misurabili.



Un sistema adatto a ogni settore

La versatilità di Keydom la rende una soluzione ideale anche per:

- **aziende e uffici:** sicurezza e ottimizzazione dell'accoglienza dei visitatori
- **strutture sanitarie:** controllo rigoroso delle aree critiche
- **ospitalità e turismo:** gestione accessi a camere e servizi
- **pubblica amministrazione:** protezione di sedi istituzionali e ZTL
- **infrastrutture critiche:** monitoraggio continuo e difesa dei perimetri sensibili

Ogni ambiente può disporre di policy su misura e aggiornabili in modo dinamico.

Sicurezza, governance e continuità operativa

La forza di Keydom risiede nella sua capacità di superare la visione tradizionale del controllo accessi come semplice sistema di vigilanza, trasformandolo in uno strumento strategico di governo delle infrastrutture.

La centralizzazione dei dati offre una panoramica completa

e aggiornata delle attività, consentendo interventi rapidi, basati su informazioni affidabili. Questo approccio supporta la riduzione dei rischi, la continuità dei processi e il miglioramento dell'efficienza operativa.

Il tutto avviene secondo i requisiti delle normative più avanzate in tema di sicurezza logica e trattamento dei dati personali, inclusa la conformità al Regolamento GDPR per la protezione delle identità e delle informazioni sensibili.

Un investimento solido nel futuro della sicurezza

FAAC, con Keydom, mette a disposizione una piattaforma moderna e pronta a evolvere con le necessità dei clienti. L'integrazione nativa tra hardware e software, unita a un'elevata interoperabilità, permette un controllo intelligente e centralizzato di spazi, persone e mezzi.

Per chi cerca una soluzione avanzata, capace di offrire sicurezza fisica e logica in un unico sistema, Keydom rappresenta un investimento affidabile e lungimirante per la protezione delle infrastrutture e la gestione degli accessi nel futuro.

FAAC

Contatti:
FAAC

www.faac.it/richiesta-informazioni

Wisenet 9, la piattaforma con IA a bordo per offrire servizi a valore aggiunto

comunicato aziendale

Il mondo della videosorveglianza sta attraversando una fase cruciale di trasformazione: non più (solo) semplici telecamere, ma sistemi intelligenti, efficienti e sicuri. In questo contesto, Hanwha Vision propone il suo chip di nuova generazione, Wisenet 9, che diventa il cuore delle telecamere del futuro. Dopo quasi quattro anni di ricerca e test, questa piattaforma promette di ridefinire criteri quali prestazioni, accuratezza e sicurezza.

Nuova architettura: IA al bordo

Uno dei pilastri distintivi di Wisenet 9 è l'adozione di un'architettura dual NPU (Neural Processing Units). Ciò significa che due unità dedicate operano in parallelo: una focalizzata sul processare l'immagine, l'altra sulle analisi, rilevamenti e classificazioni.

Questo garantisce che la qualità video e la videoanalisi non si sovrappongano o compromettano l'una con l'altra.

Secondo Hanwha Vision, rispetto alla generazione precedente (Wisenet 7), le prestazioni di inferenza sono triplicate.

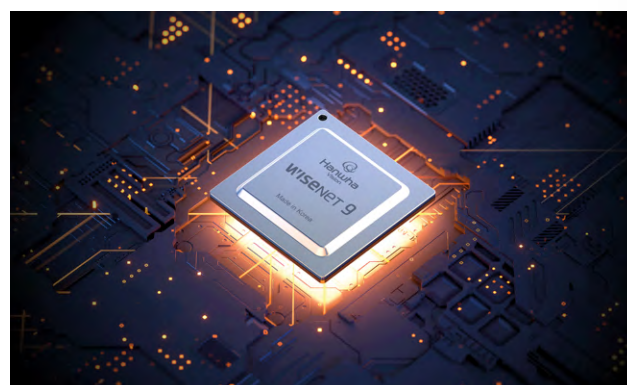
Questa architettura consente un'elaborazione in tempo reale più efficace, essenziale in un mondo dove il volume e la complessità dei dati video – e delle minacce – aumentano significativamente.

Miglioramento della qualità d'immagine

Il chip Wisenet 9 non si limita ad aggiungere "più AI" ma mira a migliorare radicalmente ciò che si vede.

Le caratteristiche principali includono:

- Extreme WDR (Wide Dynamic Range) basato su IA: permette, anche in condizioni di luce molto contrastate, di ottenere dettagli sia nelle zone estremamente luminose che in quelle in ombra.
- Riduzione avanzata del rumore (Noise Reduction) guidata da IA: in ambienti con scarsa illuminazione o condizioni difficili, il sistema utilizza una rete dedicata di denoising separata dalle altre risorse NPU, preservando il dettaglio e riducendo artefatti di movimento.
- Compressione intelligente (WiseStream + H.265): grazie all'IA e all'efficienza del codec H.265, è possibile ridurre sensibilmente il consumo di banda e lo spazio di archiviazione senza sacrificare la qualità video.



Questi aspetti rendono Wisenet 9 particolarmente efficace sia in installazioni ad alto livello tecnico sia in contesti dove la banda o lo storage sono risorse limitate.

Analisi video e attributi intelligenti

Oltre al "solo video" il nuovo SoC mette al centro l'intelligenza applicata ai dati visivi. Tra le funzioni più rilevanti troviamo:

- Analisi degli attributi: colore, presenza di borsa, occhiali, maschera, età, genere.
- Funzioni avanzate come conteggio di persone e veicoli, rilevamento cadute (slip & fall), rilevamento folla, gestione code, heatmap.
- Tecnologie specialistiche:
 - o Re-Identification (RE-ID): abbinamento e riconoscimento di soggetti in riprese non sovrapposte (es. diverse telecamere) anche in caso di variazioni d'aspetto.
 - o Dynamic Privacy Masking (DPM): mascheratura dinamica (opaca o a mosaico) di persone, volti, targhe, per tutelare la privacy in conformità con normative vigenti.
- Classificazione del suono basata su IA: identificazione di eventi critici come spari, vetri rotti, urla, con sensibilità direzionale.

Integrazione e compatibilità

Spesso le nuove piattaforme di sorveglianza richiedono infrastrutture completamente nuove. Wisenet 9 si integra molto bene anche con l'infrastruttura esistente:

- Compatibile con profili ONVIF e standard della sorveglianza, il che facilita l'integrazione in sistemi già operativi.

- Supporta le piattaforme cloud e VMS dell'ecosistema Hanwha: gestione remota, portali cloud, aggiornamenti.
- Realizzato interamente "in-house" da Hanwha Vision, che garantisce controllo sull'architettura e sviluppo del SoC.

Sicurezza end-to-end

In un'era in cui la cybersecurity è importante quanto la qualità video, Wisenet 9 porta alcune novità significative:

- Conserva le funzioni di base già introdotte con Wisenet 7: sistem-boot sicuro, OS protetto, storage criptato.
- Introduce un modulo Secure Element hardware certificato secondo lo standard internazionale FIPS 1403 Level 3: un riferimento elevato per protezione crittografica e gestione sicura dei dati.
- La certificazione FIPS 140-3 Level 3 significa che la protezione del modulo crittografico è a livello hardware, con firma digitale per firmware/software, test pre-operativi e requisiti stringenti per tutto il ciclo di vita. Tutto ciò rende Wisenet 9 idoneo anche per ambienti molto sensibili come enti pubblici e infrastrutture critiche.

Perché Wisenet 9 rappresenta un salto generazionale

Riassumendo, le ragioni fondamentali che rendono Wisenet 9 una piattaforma da considerare sono:

- Architettura dual NPU che separa funzione video da funzione analisi, eliminando compromessi tra qualità immagine e intelligenza.
- Elevate prestazioni IA: inference triplicata rispetto alla generazione precedente.
- Qualità d'immagine rafforzata, specialmente in condizioni critiche di luce o movimento.
- Efficienza nella banda e nello storage grazie alla combinazione AI più H.265 più compressione WiseStream.
- Funzioni analitiche moderne e verticali (RE-ID, Privacy Masking, che ampliano la sorveglianza in intelligence utile).
- Sicurezza hardware di alto livello (FIPS 140-3 L3) e compatibilità con gli ecosistemi esistenti.
- Flessibilità e scalabilità: dalle installazioni più semplici (retail, uffici) a quelle più complesse (traffico, logistica, industria).

Considerazioni per il mercato italiano / Europeo

Per il mercato italiano ed europeo, alcuni punti di attenzione diventano importanti:

- Le normative europee (GDPR, regolamenti privacy) richiedono sistemi che tutelino i dati personali: DPM e Privacy Masking diventano elementi qualificanti.

- L'integrazione con sistemi esistenti (ONVIF, VMS, cloud) è fondamentale per contenere costi e garantire continuità operativa.

- L'efficienza banda/storage è un fattore strategico, specialmente per utenti con infrastrutture limitate o remote. Wisenet 9 risponde bene; secondo Hanwha la riduzione del consumo di banda può arrivare fino all'80%.

- La certificazione FIPS 140-3 L3 può essere un punto di vendita distintivo per settori come governativo, infrastrutture critiche: rispondere alle esigenze di sicurezza informatica oltre quelle operative.

- È opportuno verificare compatibilità firmware e roadmap: come ogni tecnologia evoluta, un buon piano aggiornamenti e supporto diventa fondamentale.

Qualche sfida ed elementi da valutare

Naturalmente, anche le soluzioni più avanzate presentano elementi di attenzione:

- Sebbene la piattaforma sia stata progettata per integrarsi con sistemi esistenti, nelle installazioni legacy potrebbe esserci ancora lavoro di messa a punto (firmware, compatibilità VMS, gestione AI).
- L'effettivo sfruttamento delle funzioni IA avanzate (es. RE-ID, AI Sound Classification) richiede che l'intera catena – telecamera, rete, storage, analisi – sia dimensionata correttamente. In ambienti poco performanti, queste funzioni possono essere sottoutilizzate.
- Anche se il SoC è avanzato, l'intero sistema (ottica, sensore, illuminazione, rete) deve essere coerente con le promesse: una telecamera dotata di Wisenet 9 ma installata in condizioni pessime rischia di non esprimere il suo potenziale.
- Infine, la formazione degli operatori e del personale tecnico resta un elemento chiave: la disponibilità di strumenti di configurazione, dashboard e analisi deve essere accompagnata da competenza.

Conclusione

In un panorama della sorveglianza sempre più "smart", la sfida non è solo vedere, ma capire e agire.

Con Wisenet 9, Hanwha Vision si posiziona forte nel mercato proponendo un chip che unisce elevata qualità d'immagine, IA al bordo, efficienza operativa e cyber-resilienza. Per gli operatori del mercato (installatori, system integrator, responsabili sicurezza), è una piattaforma da valutare seriamente: non solo come "upgrade" tecnologico, ma come leva per offrire servizi ad alto valore aggiunto.



Contatti:
Hanwha Vision Europe
Tel. +39 02 36572 890
hvesecurity@hanwha.com
www.hanwhavision.eu

Il coaching: la CPU della Security.

Quando la sicurezza parte dalle persone e non solo dalle procedure

di Elena Todisco - mental coach

A fronte alla crisi generalizzata di carenza di risorse umane in tutti i settori pubblici e privati, che tocca in modo diretto e indiretto anche aspetti rilevanti di sicurezza, abbiamo avviato un percorso di approfondimento sulle nuove tendenze nel HRM, tese a rivedere il modello tradizionale di relazione tra datore e prestatore d'opera nell'era della IA.

Iniziamo il percorso con un contributo di Elena Todisco, ideatrice del programma "Focus F.E.L.I.C.I.T.À", per aiutare le persone a sviluppare consapevolezza, equilibrio e forza interiore, per vivere la propria felicità come scelta quotidiana e per costruire, dall'interno, le basi di ogni sicurezza esterna.

Quando si sente parlare di sicurezza, si pensa ai sistemi di difesa, ai dispositivi di protezione, alle regole di comportamento. Eppure, ciò che fa la differenza e la rende efficace sono le persone.

La sicurezza non è solo un elenco di procedure, di regole, bensì una cultura che nasce da comportamenti consapevoli e da valori condivisi.

La sicurezza è sempre stata una necessità, ma oggi lo è più che mai.

Se decolliamo da una visione macro per atterrare su una micro, possiamo citare, rispettivamente, questi ambiti di sicurezza: internazionale e nazionale come la difesa da attacchi esterni; aziendale come la tutela delle persone, dei beni e dei processi produttivi; informatica quale la protezione dei sistemi, delle reti e dei dati in essi contenuti e, infine, quella personale come fiducia di sé, delle proprie risorse e delle emozioni.



Il coaching si inserisce proprio in quest'ultimo piano: quello umano e relazionale.

Se il collaboratore della security, a qualunque livello di coinvolgimento gestionale od operativo, è ignaro delle motivazioni del proprio agire e dei valori del proprio gruppo di riferimento, non è in grado di esprimere la propria totale potenzialità.

Diversamente, se conosce il "perché", se ha compreso perfettamente il "come" agire e ha fatto propri i comuni valori, che sorreggono l'azione, allora, dà il proprio massimo personale.

Il coaching aiuta a far sì che in ambito aziendale si sviluppi una comunicazione fatta di fiducia, di rispetto e di presenza mentale.

Un gruppo che comunica in modo aperto, assertivo e collaborativo riduce i rischi di incomprensione e quindi di errore nell'esecuzione delle procedure delegate.

Il leader che è consapevole del proprio ruolo positivo e di aiuto per gli altri, che comunica con chiarezza e che ascolta con empatia, non incontra difficoltà con la propria

squadra, in quanto ogni membro si sente parte attiva e di valore di un tutto.

Il coaching è, quindi, fondamentale in ambito aziendale, perché aiuta sia a rafforzare la fiducia tra i collaboratori e tra loro e il leader, che a sviluppare una leadership empatica, grazie alla quale, chi guida, trasmette sicurezza, capacità, comprensione e sostegno.

Tutto ciò cambia il clima aziendale e porta la sicurezza ad essere vissuta come valore e non come "si deve fare!".

In ogni organizzazione, la sicurezza è fondamentale, ma spesso, non sono la tecnologia e le procedure a fare la differenza, bensì il fattore umano.

È come possedere un computer con schermo e tastiera funzionanti, ma una CPU difettosa. Perciò, manca il cervello che elabora correttamente i dati e li trasforma in risultati precisi.

Ecco che qui è possibile inserire il coaching, una disciplina e, per me, un modo di essere, che permette alle persone di raggiungere la versione migliore di loro stesse e di diventare quella CPU funzionante attraverso domande guida, esercizi scritti e tecniche di gestione delle emozioni.

Il coach, infatti, non è un consulente che suggerisce la propria visione, bensì aiuta la persona a far emergere tutte le risorse che già possiede e di cui non è consapevole.

Quindi, il coaching aiuta a sviluppare la lucidità mentale interiore necessaria per scegliere secondo i valori anche quando la situazione è difficile e complicata. Il che significa, in un contesto di sicurezza, saper rinunciare a scorciatoie e a compromessi, che metterebbero sicuramente a rischio le persone coinvolte e, di conseguenza, gli obiettivi accettati. Ogni persona che viene fatta crescere diventa il primo presidio di sicurezza sia per sé stessa che per tutti gli altri. In conclusione, la security non nasce solo da procedure e da regole, ma anche da persone consapevoli, centrate, presenti e responsabili.

Carl Gustav Jung affermava che "chi guarda fuori, sogna, chi guarda dentro, si sveglia".

La sicurezza è la conseguenza della consapevolezza: più ci miglioriamo e più il mondo, dentro e fuori di noi, diventa sicuro.

Sarà un'utopia? Io credo di no!



Vivaldi, quando l'audio è anche sicurezza

intervista a Martina Degli Agostini, Direzione Commerciale Vivaldi Group

Ci può presentare l'azienda Vivaldi Group?

Vivaldi è un produttore Italiano che vende nel mondo tecnologie audio multimediali integrate, soluzioni EN54 per la voice evacuation alarm security, web server per la Home & Building multimedia automation, sistemi audio Public Address & audio Professional. La nostra mission è semplice da un lato quanto impegnativa dall'altro: trasformare ogni spazio in un'esperienza multimediale unica attraverso le tecnologie all'avanguardia. Vivaldi si impegna a offrire soluzioni innovative che integrano audio e video, anche in ambito sicurezza sempre nel rispetto delle normative vigenti, permettendo così ai nostri clienti di vivere un intrattenimento personalizzato e coinvolgente. La nostra ambizione è di rimanere un punto di riferimento nel settore, contribuendo a definire standard sempre più elevati per l'innovazione tecnologica. Lavoriamo sull'innovazione continua, la personalizzazione delle soluzioni e partnership strategiche. Puntiamo a sviluppare prodotti che non solo soddisfino le esigenze attuali, ma che siano anche pronti a fronteggiare le sfide future del settore.

In che modo Vivaldi Group supporta i manutentori e gli installatori nell'aggiornamento delle proprie competenze, per assicurare un livello di professionalità costante?

In molti modi, messi a punto in diverse decadi di attività. Dai più basilari ma costanti affiancamenti giornalieri nel campo, all'assistenza telefonica, all'assistenza web remota, alla fornitura di documentazione tecnica, schematici, tutorial, passando dalla partecipazione a webinar tecnici. O ancora tramite Service/Cat locali, regionali per un supporto completo ed immediato. Invitiamo poi i clienti in azienda o ad eventi locali per provare con mano le tecnologie, testarle tramite campionature. Fino all'investimento maggiore, per Vivaldi, riguardante la formazione specializzata effettuata da docenti di alto profilo in tutte le materie didattiche trattate dall'azienda.



Quali sono le principali competenze e conoscenze che i partecipanti acquisiscono durante i corsi, e come queste contribuiscono a migliorare la qualità della manutenzione e dell'assistenza sui sistemi Vivaldi per garantire un servizio sempre più affidabile?

Lavoriamo sulla forma mentis, sulle abilità di problem solving, sulle capacità di interagire in situazioni delicate, alla importante preparazione tecnica, evolvendo i nostri clienti / Service su gamme prodotte innovative e tecnologicamente avanzate, parlando di audio, video, multimedia, reti, cyber security, programmazioni, informatica, ecc... senza tralasciare gli aspetti fondamentali della costruzione di un sistema di diffusione sonora certificato.

Potrebbe spiegare come il corso AISE si integri con l'offerta formativa e i servizi specifici di Vivaldi Group, e in che modo questa proposta formativa supporti le strategie di crescita?

Le competenze in tema di sicurezza IRAI ed EVAC sono fondamentali per istruire migliaia di figure cresciute in cantiere ma spesso poco addentro gli aspetti normativi e progettuali.

Capire il contesto ove si opera e saper intervenire non solo con l'esperienza, ma con cognizione di causa (normativa/ legislatura) rende le figure sempre più idonee al ruolo delicato che svolgono. Tutte le crescite, aziendali, di fatturato, di mercato si basano sulle persone. Investire nella formazione di queste è il pilastro per solide e costanti crescite.

Quali altre opportunità di formazione continua o di supporto offre Vivaldi Group ai professionisti che hanno partecipato al corso, al fine di garantire un servizio sempre efficiente, aggiornato e in linea con le normative vigenti?

Coloro che partecipano al corso potranno trovare sempre, in Vivaldi, un partner che li consiglia e li aiuta, si tratti di dare supporto in un progetto di un sistema a norma, controllare e correggere un impianto esistente, fugare un dubbio con

una telefonata, partecipare a nuovi corsi di formazione sulle novità ed evoluzioni normative, o anche chiedere un supporto in cantiere per la realizzazione di relazioni acustiche, studi tecnici, programmazioni, verifiche funzionali, avviamenti e simili.

In relazione ai recenti aggiornamenti riguardanti i sistemi di rivelazione incendio IRAI ed EVAC che i manutentori dovrebbero conoscere, come vengono comunicati e approfonditi attraverso i vostri programmi di formazione?

Tramite la divulgazione personale, la comunicazione scritta (email), gli inviti personali e programmati e la comunicazione web (social, sezione dedicata del sito <https://vivaldigroup.it/it/formazione.html> oppure <https://vivaldigroup.it/it/supporto/assistenza.html>), o ancora le collaborazioni con organizzazioni come la vostra.

VIVALDI





UN MONDO DI SERVIZI, SU MISURA PER TE

Da oltre 50 anni HESA è al fianco dei migliori installatori e distributori come partner affidabile e altamente qualificato. Oggi rinnoviamo questo impegno con HESA For You, il concept che esprime la nostra vicinanza ai professionisti della sicurezza e l'anima più autentica di HESA: offrire una gamma di servizi personalizzati, costruiti intorno alle esigenze di ogni cliente.

HESA For You racchiude una promessa concreta: consegne rapide, prodotti sempre disponibili a magazzino, supporto tecnico avanzato con ingegneri e specialisti al fianco dei professionisti nella progettazione di sistemi integrati, e innumerevoli altri vantaggi pensati per semplificare il lavoro quotidiano, ottimizzare le risorse e far crescere l'attività dei nostri partner.

HESA FOR YOU. PIÙ VICINI, PIÙ FORTI, INSIEME.



HESA S.p.A.

Via Triboniano, 25 - 20156 Milano - Tel. 02.380361

www.hesa.com • e-mail: hesa@hesa.com

Filiale: Scandicci (FI)

SIAMO PRESENTI A
SiCUREZZA
PAD 5
STAND L16 - K11
19-21 NOVEMBRE 2025
Fiera Milano, RHO

Partner

ADD SECURE INTERNATIONAL AB
www.addsecure.it
I romana, 8-9

AISMA S.R.L.
www.aisma.it
17, 22-23

ALESYS
www.alesys.it
24-25, 37

AXIS COMMUNICATIONS
www.axis.com
10-11

BDS
www.basedigitale.com
16, 26-27

CITTADINI DELL'ORDINE S.P.A.
www.cittadinidellordine.com
28-29, 36

COOPSERVICE
www.vigilanzacoopservice.it
13, 30-31

ERMES ELETTRONICA S.R.L.
www.ermes-cctv.com
38-39

FAAC
www.faac.it
40-41

FON.TER
www.fonter.it
12

HANWHA VISION EUROPE
www.hanwhavision.eu
42-43

HESA S.P.A.
www.hesa.it
48

INIM ELECTRONICS S.R.L.
www.inim.biz
I copertina, 4

OPTEX
www.optex-europe.com/it
II copertina, 14-15

REVEAL
www.revealmedia.it
32-33, IV copertina

SANGIORGIO S.R.L.
www.sangiorgioweb.com
III copertina

SICUREZZA
www.sicurezza.it
6-7, 52

UNIV
www.univigilanza.it
34-35

essecome
ONLINE

n. 07/2025
Anno XLV
Periodico fondato da Paolo Tura

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

**HA COLLABORATO
A QUESTO NUMERO**
Roberto Briscese, Elena Todisco

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

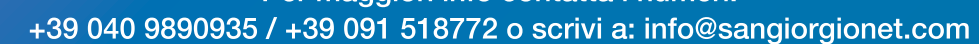
REGISTRAZIONE
- Tribunale di Milano n. 21 del 31 gennaio 2018
- Registro pubblico Operatori di Comunicazione (ROC) n. 34727

GRAFICA/IMPAGINAZIONE
Lilian Visintainer Pinheiro
lilian@lilastudio.it

Appunti

Appunti

19 – 21 NOVEMBRE 2025 | fieramilano





Il futuro della sicurezza sanitaria:
protezione, fiducia, qualità delle cure



Scansiona il codice
QR per saperne di più