essecome ONLINE 03/22

Periodico digitale di informazione di security & safety

2022 · ANNO XLII

Cover Story

CONOSCI SOL DI INIM?
DOPPIA POTENZA VIA RADIO E MOLTO DI PIÙ.

Oggi vi presentiamo la centrale via radio **SOL 2.0.** L'evoluzione di SOL rende davvero evidente il concetto di "Evolving Security".
Il nome è lo stesso, l'estetica anche, ma il cuore ed il cervello della centrale sono profondamente rinnovati. Sono evoluti.
Una evoluzione che rientra nel progetto **ES "Evolving Security"** un approccio che testimonia il rinnovamento in atto dei prodotti e dei servizi **INIM**, in una parola la loro "evoluzione".
Questa evoluzione viene declinata di volta in volta in maggiori prestazioni, maggiore sicurezza, maggiore affidabilità, maggiore qualità, maggiore semplicità.
La sicurezza evolve con **Sol 2.0.** La centrale antintrusione via radio, modulare e integrata, con una portata wireless raddoppiata. In più: attivazione rapida via QR code, programmazione, riprogrammazione, aggiunta utenti. Tutto via app **INIMTech Security**. Tutto più facile. La nuova potenza di Sol è tutta da provare. Non aspettare. Acquistala subito!
Questo significa poter coprire più esigenze di installazione in ambito residenziale, commerciale e oltre.
Con Sol, accensione, programmazione, modifica e controllo totale da app INIMTech Security, via rete LAN e GSM.

Inserimento immediato di utenti su invito via app. Prova subito il doppio della potenza, con Sol: Evolving Security.

Parliamo di riprogettazione della sezione di antenna che ha prodotto notevolissimi incrementi nel range di copertura via-radio.
Un nuovo circuito stampato siglato **IN327**. Una procedura di attivazione e registrazione al Cloud tramite l'app InimTech Security semplificata e rapida. L'aggiunta degli utenti con l'app installatore INIMTech Security tramite un invito con notifica push nell'app INIM Home e la procedura di invito di altri utenti da app INIM Home.
L'arruolamento al Cloud disponibile da LAN e da GSM senza la necessità di alcuna programmazione ma semplicemente scansionando il QR-code di centrale.
La selezione automatica APN della rete GSM per i maggiori operatoti italiani e la programmazione SSID e password rete WiFi da app INIMTech Security (via INIM Cloud). Abbiamo rilasciato una nuova versione di INIMHome (con gestione della notifica push di invito alla gestione della centrale) e una nuova versione di INIMTech Security (per invio invito all'utente, arruolamento rapido tramite QR-code, programmazione e riprogrammazione di centrale) oltre alla versione 2.

Sommario

Competenze e qualità degli impianti contro burocrazia e concorrenza degli incompetenti

Partiamo dalla concorrenza degli incompetenti.

Sotto la spinta delle direttive europee, gli enti normatori nazionali (UNI per l'Italia) stanno producendo a getto continuo norme volontarie sulle competenze delle professioni 'non regolamentate', così definite dalla Legge 4/2013 perché non fanno capo ad Albi o Ordini Professionali che, per l'appunto, sono stati creati e vengono regolati da apposite leggi che impongono i requisiti e le modalità per esercitare le professioni considerate critiche per il buon funzionamento, la sicurezza e la salute delle comunità.

Il carnevale degli incompetenti di Ivrea (foto de La Voce)

Le norme volontarie definiscono in genere i requisiti relativi alle competenze delle figure interessate attraverso *"l'individuazione di compiti e attività e i requisiti di conoscenza, abilità, autonomia e responsabilità"* per garantire la qualità (ovvero la capacità di rispondere alle aspettative) della miriade di servizi oggi necessari per far funzionare qualsiasi cosa, allo scopo di mettere in sicurezza sia gli utilizzatori che i fornitori di quei servizi.

Sicurezza, dunque, non nel senso stretto di safety o di security ma di tutela delle persone e delle organizzazioni dall'incompetenza, dall'improvvisazione e dall'irresponsabilità che, notoriamente, possono provocare disastri maggiori delle calamità naturali o delle azioni volontarie.

La principale, se non unica difesa da questi pericoli viene dalla conoscenza comprovata delle regole dell'arte da parte del fornitore, che potrà così garantire al cliente la qualità del suo lavoro e proteggere se stesso dai rischi di risarcimenti e di sanzioni civili e penali, oltre che dalla pericolosissima concorrenza degli incompetenti.

Di fronte ad un'evidenza così netta, si darebbe per scontato che chiunque eserciti una professione non regolamentata si preoccupi di ottenere le certificazioni previste dalle norme di riferimento del proprio mestiere, ovvero si adoperi in ogni modo per far varare le norme ancora mancanti per mettersi quanto prima in sicurezza ma, a quanto pare, non è scontato per tutti. Escono infatti dal coro le posizioni assunte pubblicamente ed a più riprese negli ultimi mesi dalle maggiori confederazioni dell'artigianato nei confronti della revisione del DM 37/2008 sugli impianti e, più di recente, anche della bozza di norma UNI sulle competenze della filiera dei sistemi di sicurezza, che dell'impiantistica è solo una piccola nicchia.

Posizioni che sarebbero motivate dalla preoccupazione che la normazione dei compiti e dei requisiti professionali per lavorare in un determinato settore diventi un'ulteriore fonte di costi e di inutili incombenze burocratiche per gli artigiani, non percependola invece come un'opportunità di crescita professionale e di difesa delle organizzazioni, soprattutto se familiari.

Senza entrare qui nel merito dei ruoli sempre più spesso ancillari delle imprese artigianali nelle diverse filiere produttive, non possiamo che auspicare un ripensamento da parte delle confederazioni su questo tema, magari attraverso un confronto con il Governo per rivedere finalmente l'intero sistema di lacci e lacciuoli che frenano da sempre la nostra economia, portata faticosamente avanti dalle imprese artigiane quanto dalle PMI e dalle grandi aziende.

Questo momento storico potrebbe essere favorevole, se tutte le parti sociali interessate unissero i propri sforzi.

essecome securindex.com

APR - SECURITY & SAFETY PER LE INFRASTRUTTURE DEL TRASPORTO

Sicurezza fisica e cibernetica negli aeroporti italiani. Il punto della situazione.

23 giugno | ore 14.30 -18.00

NH Collection Roma Vittorio Veneto

Patrocinio:

Partner:

Con il convegno sul tema *"Sicurezza fisica e cibernetica negli aeroporti italiani. Il punto della situazione"* si apre il ciclo **APR – security & safety per le infrastrutture del trasporto** organizzato da **essecome editore**, nel corso del quale verranno affrontati i diversi aspetti della sicurezza delle strutture e degli impianti del trasporto pubblico: **aeroporti, porti, ferrovie, trasporti urbani, infrastrutture stradali e autostradali.**

Il progetto si rivolge agli operatori delle filiere interessate e sarà articolato in eventi in presenza, webinar e approfondimenti editoriali ai quali verranno affiancati percorsi formativi finalizzati al rilascio ed al mantenimento delle certificazioni delle competenze previste per le diverse figure professionali coinvolte.

Verranno invitati i rappresentanti delle istituzioni di riferimento, delle associazioni di categoria e degli operatori pubblici e privati per analizzare gli aspetti di sicurezza rilevanti e attuali assieme ai più noti esperti e docenti delle diverse materie, e per conoscere le migliori pratiche con il supporto di vendor e service provider di livello internazionale.

Il primo appuntamento del ciclo è dedicato ad una valutazione delle minacce di tipo fisico, informatico e combinato che riguardano gli aeroporti che, per le peculiari caratteristiche del trasporto aereo civile, utilizzano in modo condiviso a livello globale i modelli organizzativi, le procedure e le tecnologie più evolute e consolidate, sviluppando in tal modo esperienze ed indicazioni fruibili anche in contesti diversi dal trasporto aereo.

Verrà inoltre fatto il punto della situazione del livello di consapevolezza delle molteplici tipologie di rischio in capo alle diverse figure che operano nel contesto aeroportuale e del ruolo della formazione continua.

Questo il programma del convegno del 23 giugno 2022:

14.30 - *Inizio dei lavori con diretta Zoom*

14.40 - *'Cybersecurity delle Infrastrutture del trasporto, il punto della situazione'*
keynote speech di Corrado Giustozzi

15.00 - *'Sicurezza fisica e cibernetica del sistema aeroportuale italiano'*
con Francesco Di Maio (ENAV), Sebastiano Veccia (ENAC), Emanuela Di Rosa (Assaeroporti)

16.00 - *'Le migliori pratiche a livello internazionale contro le minacce combinate'*
con Everbridge, Genetec, Hanwha Techwin

16.45 - Coffee break

17.00 - *'Eccellenze italiane per la sicurezza integrata degli aeroporti'*
con Rete Vigilanza Italia, TSec, Vigilate

17.45 - *'HR, l'importanza delle competenze e il ruolo della filiera dei fornitori'*
con Giulio Iucci (ANIE Sicurezza), Mauro Mariani (ANSSAIF), Giuseppe Mastromattei (Laboratorio per la Sicurezza)

18.30 - *Tavola rotonda finale con sintesi dei contenuti trattati, proposte e mozioni*

19.00 - *Happy hour*

L'evento è riservato ad appartenenti alle Istituzioni di riferimento, operatori delle infrastrutture del trasporto (società di gestione, handler, service provider) e security manager certificati UNI 10459.
Ai partecipanti all'evento in presenza ed a distanza su piattaforma Zoom verrà rilasciato attestato di partecipazione ai fini dell'ottenimento di crediti formativi.

Per informazioni e pre-iscrizioni:
segreteria@securindex.com | 02.36757931

Sicurezza fisica e cibernetica negli aeroporti italiani. L'analisi di ENAV

intervista a Francesco Di Maio, CISA CISM CRISC, C|CISO Head, Corporate Security Department - ENAV

Ci può fare il punto ad oggi sul livello complessivo della security del sistema aeroportuale italiano?
L'aviazione civile italiana ha da sempre dimostrato di essere un presidio di avanguardia nei processi di sicurezza, ed applica i principi internazionali e della regolamentazione europea con grande serietà. D'altra parte, la security è parte integrante del modo di essere per il mondo aeronautico ed i security manager dei vettori aerei, degli aeroporti e degli altri operatori aeronautici cooperano attivamente tra di loro per innovare e rispondere alla domanda di sicurezza da parte dei passeggeri ed alla facilitazione dei processi di gestione, per ridurre i tempi di attesa con una risposta in termini di efficienza e qualità.

A livello internazionale, quali sono le principali minacce che vengono attualmente percepite per la sicurezza dei voli e dei passeggeri?
Purtroppo l'aviazione civile resta un obiettivo assai appetibile per la diversa platea di attori malevoli che si contendono la scena e non si parla solo della minaccia terroristica, che rimane a livelli consistenti per le diverse matrici ideologiche che si osservano nel campo.
Un aereo, un aeroporto, sono potenziali terminali di attacchi perché, da un lato, raccolgono numeri rilevanti di passeggeri di diverse nazionalità; dall'altro rappresentano la libertà di circolazione, non solo delle persone e delle merci ma, soprattutto, delle idee in un contesto dinamico globale.
La verità è che la minaccia si è progressivamente evoluta, passando dai tradizionali dirottamenti all'uso degli aerei come armi di distruzione di massa, richiedendo un supplemento di attenzione a tutti i livelli ed una più stretta sinergia di tutti gli attori, pubblici e privati, interessati a garantire la protezione della vita umana in volo e a terra.
A questo si affianca anche un contesto geopolitico assai dinamico, che segue una fase critica rappresentata dall'evento pandemico che ha messo a dura prova l'industria aeronautica.
Direi che oggi non esiste "una" minaccia specifica, ma esistono "più" minacce che tra di loro possono combinarsi, con attori pronti a sfruttare le vulnerabilità di punto e di sistema. Fondamentale è presentarsi preparati ad affrontare, congiuntamente, esigenze di sicurezza fisica e di sicurezza logica non dimenticando mai che il cuore del sistema è rappresentato dal fattore umano.

In ambito cyber, quali sono le tipologie di attacchi più frequenti a livello globale e quali eventi hanno interessato il sistema nazionale?
Negli ultimi tre anni, con un picco registrato con la crisi sanitaria globale, sono aumentati in maniera più che significativa i crimini informatici, soprattutto quelli che hanno come sfondo richieste estorsive o, comunque, finalità di natura lucrativa e predatoria, conosciuti soprattutto nella variante del "ransomware".
Nessun settore produttivo e della pubblica amministrazione, purtroppo, ne è andato esente e questo perché gli attori ostili non sfruttano tanto le vulnerabilità tecnologiche, quanto quelle legate al fattore umano, perfezionando sempre di più gli attacchi diventati più subdoli e meno riconoscibili. Con la crisi derivante dalla guerra in Ucraina, stiamo assistendo anche ad una recrudescenza di fenomeni di attacchi, ideologicamente connotati, che mirano a creare impedimenti ai servizi che enti pubblici e privati offrono ai cittadini. Tuttavia, non sembra che, al momento, tali azioni si siano rivelate effettivamente capaci di debilitare il sistema, come invece accadde in Estonia nel 2007 o in Georgia nel 2012. Certamente sono cresciuti anche i livelli di consapevolezza nelle organizzazioni e questo è un fattore certamente abilitante i processi di difesa.

Cosa sarebbe necessario per migliorare la prevenzione e innalzare il livello di resilienza del sistema nei confronti dei rischi cyber, anche nell'ambito del partenariato pubblico/privato?
La parola d'ordine non può essere che una: cooperazione. Mi riferisco ad una collaborazione reale, che sostenga le organizzazioni private con una reale capacità di sostegno, nella fase di analisi del rischio, nella gestione dei processi di scambio di informazioni (quella che comunemente viene definita *threat intelligence*) che deve essere tempestiva, possibilmente automatizzata e non legata ad arcaiche modalità di tipo ministeriale-burocratico.
Le minacce corrono ad una velocità paragonabile almeno a quella degli aerei e le risposte devono essere altrettanto rapide. La comunità aeronautica italiana plaude certamente agli sforzi del Governo per elevare il livello qualitativo di questa collaborazione, ma va fatto molto di più.
Si deve operare per rendere disponibili anche agli operatori minori quegli elementi della tecnologia dell'informazione e quei processi di protezione che sono complessi, non accessibili alle organizzazioni meno strutturate, favorendo processi di aggregazione che vadano al di là della competizione tra imprese.
Noi stiamo facendo, in questo senso, la nostra parte. Con Assaeroporti abbiamo creato una community, facilitata da un programma europeo finanziato che ci siamo aggiudicati, per stabilire un "Information Sharing and Analysis Center" (ISAC) dedicato all'aviazione civile italiana ed aperto a tutta la comunità aeronautica nazionale.
Vediamo con piacere che in una delle 82 misure contenute nella Strategia Cibernetica nazionale, di recente varata dal Governo, vi sia proprio l'accento sulla necessaria cooperazione tra l'Autorità per la Cybersicurezza Nazionale e gli ISAC settoriali.
Ma ciò non basta. I security manager dialogano costantemente tra di loro anche con modalità informali, nate durante la drammatica esperienza del COVID. Vorremmo che questa partecipazione immediata, tempestiva e senza formalità possa venire sviluppata anche con i rilevanti attori pubblici, verso i quali sicuramente possiamo dare tanto.

E in aggiunta c'è il tema dei finanziamenti: la sicurezza costa, ma non è un costo. Anzi è un investimento doveroso, per i privati ma anche per l'intera comunità nazionale, perché i cittadini che viaggiano hanno il diritto di sentirsi tutelati in maniera effettiva e ricevere risposte in termini di sicurezza.

Come valuta in generale il livello di preparazione e di responsabilizzazione sui temi della sicurezza del personale che opera nel sistema?
L'aviazione civile è all'avanguardia in molti settori, tra i quali quelli della formazione. Per noi, in tutti i domini, sia che si tratti di controllo del traffico aereo che di aeroporti, vettori ed operatori aeronautici in generale, la formazione e la sensibilizzazione sui temi della sicurezza (nel suo complesso) è un obbligo che ha radici assai antiche.
Più di recente, si sono imposte, a livello europeo ma anche nazionale, norme vincolanti che dettano ulteriori requisiti d formazione, per esempio nei confronti degli Amministratori di Sistema, ossia coloro che hanno privilegi di accesso ai sistemi particolarmente elevati, che devono essere anche sottoposti a periodici "controlli di sicurezza rafforzati" relativi anche ai precedenti penali e di polizia.
E, in aggiunta, più norme impongono anche ai fornitori di sottostare ad un processo stringente di qualità della security, che serve ad elevare complessivamente il livello di competenze, capacità e di sensibilità verso la protezione di interessi che non sono solo dei privati, ma attengono ad un "dovere di diligenza" di natura pubblica che mira alla salvaguardia di interessi che si trovano nella fascia più alta dei valori di rango costituzionale, come la vita, l'incolumità personale, le libertà fondamentali.
Da membro di questa straordinaria comunità, percepisco lo sforzo che tutti i colleghi svolgono quotidianamente per raggiungere questi risultati di eccellenza anche oltre quanto richiesto dalla norma, per l'oggettiva sensibilità che tutti noi percepiamo come il dovere di base del nostro agire quotidiano.

Le soluzioni di Everbridge per prevenire gli incidenti e mitigare gli effetti nel trasporto pubblico

intervista a Michela Carloni Gammon, Country Account Director di Everbridge

Quali applicazioni ha sviluppato Everbridge per le diverse esigenze di HSS (Health, Safety, Security) negli aeroporti?
Gli aeroporti di oggi sono molto più che semplici hub per i viaggi, in quanto sono diventati anche centri per affari, incontri, divertimento. Gli operatori dell'aviazione devono pertanto salvaguardare in modo proattivo persone, strutture e risorse, mantenendo la continuità operativa.
Con migliaia di visitatori di passaggio che devono salire a bordo degli aerei nel minor tempo possibile, gli aeroporti possono essere bloccati da incidenti meteorologici, interruzioni dell'IT, azioni criminali ed altro ancora. I gestori degli aeroporti hanno quindi la responsabilità di garantire la sicurezza e le informazioni a dipendenti, passeggeri, visitatori, operatori e membri della comunità attraverso avvisi multimodali su situazioni di emergenza, chiusura dei cancelli d'imbarco, variazioni del traffico e così via. Automatizzando le procedure di notifica e integrandosi con gli SCADA e gli allarmi di sicurezza esistenti, gli aeroporti possono comunicare in modo rapido, chiaro ed efficiente con gli interlocutori dovuti - operatori di primo intervento, dirigenti, dipendenti e passeggeri - tramite tutti i metodi di contatto.
La piattaforma Everbridge semplifica la pianificazione e la gestione delle comunicazioni e delle risposte agli incidenti, seguendo procedure operative e protocolli di risposta standard per aiutare a individuare le persone a rischio, determinare chi è al sicuro e garantire che le informazioni corrette siano ricevute da tutto il personale coinvolto per tutta la durata dell'evento critico.
La piattaforma consente inoltre di collegare in modo intelligente l'ampia gamma di tecnologie impiegate negli aeroporti odierni (ad esempio sistemi di rilevamento perimetrale e antintrusione, controllo accessi porte lato terra e lato aria, videosorveglianza, allarmi antincendio, sistemi LPR, rilevamento agenti chimici e biologici, ecc.), a gestire i rischi e ridurre l'impatto degli incidenti in modo proattivo.

Le soluzioni Everbridge vengono utilizzate anche per garantire la conformità alle normative del settore e consentire reporting e analisi efficaci dopo l'azione.

Quali sono le risposte di Everbridge alle esigenze di cybersecurity nei contesti aeroportuali e, più in generale, nel trasporto pubblico?
Gli aeroporti sono esposti ad una serie di minacce alla sicurezza informatica: ransomware, attacchi ai sistemi di pagamento, social engineering, ecc. e, anche considerando solo fattori come il costo finanziario di una flotta immobilizzata, le conseguenze economiche di un aeroporto che opera a velocità ridotta, la rabbia dei passeggeri i cui dati personali vengono rubati, la sicurezza informatica nel settore aeroportuale sta diventando un problema molto serio.
Gli hacker sono implacabili nei loro tentativi di trarre vantaggio da violazioni dei sistemi informatici delle aziende. Everbridge Signal (soluzione OSINT) può avvisare di una varietà di potenziali minacce informatiche: indicazioni di un'organizzazione come bersaglio di un attacco hacker, pubblicazione online di informazioni sull'organizzazione, citazioni di dipendenti e/o tentativi di sollecitazione verso i dipendenti a commettere violazioni informatiche, riservate, ecc. Everbridge aiuta a identificare le minacce informatiche prima che si verifichino e consente una risposta rapida ed efficace alle violazioni informatiche emergenti. Durante gli incidenti informatici, le soluzioni Everbridge possono anche aiutare a riorganizzare la comunicazione e il coordinamento per contenere l'attacco, mitigare i danni e garantire la conformità. Avere un canale di comunicazione completamente separato dal Sistema primario aiuta a tenere lontani gli hacker. Il sistema di messaggistica di emergenza potrebbe venire bloccato dagli hacker; avere un sistema di comunicazione ridondante può essere la chiave per una rapida risoluzione.
Un canale di comunicazione separato può mitigare un attacco ransomware attraverso:

- l'mpostazione di notifiche immediatamente dopo l'attacco per concentrare il personale chiave sul blocco degli effetti dell'attacco;
- il mantenimento dei contatti con i dipendenti durante l'attacco per consentire il funzionamento delle comunicazioni critiche;
- il mantenimento di funzionalità critiche per la salute dei passeggeri;
- la possibilità per i team di continuare a comunicare digitalmente tramite voce, testo e video.

La nostra piattaforma può inviare notifiche e istruzioni tramite messaggi scritti, messaggi vocali ed email in oltre 100 modalità in 22 lingue secondo necessità, organizza conferenze a distanza per consentire alle persone di collaborare e analizza i messaggi di ritorno. L'automazione di questi passaggi consente di completare processi predefiniti in base al tipo di minaccia in modo rapido, altamente affidabile e su larga scala in un momento in cui i minuti spesso contano e fanno la differenza. Everbridge assiste gli aeroporti riducendo al minimo l'impatto delle interruzioni per mantenere i dipendenti e i passeggeri al sicuro e riducendo il tempo medio per la risoluzione degli incidenti.

Ci può dire qualcosa delle esperienze di Everbridge negli aeroporti internazionali?
Everbridge serve globalmente più di 100 aeroporti, fra I quali la totalità dei 25 aeroporti più trafficati in Nord America. Gli aeroporti che utilizzano Everbridge per la gestione degli eventi critici comprendono i più trafficati al mondo: Atlanta International Airport (ATL), Los Angeles International Airport (LAX), Chicago's O'Hare International Airport (ORD), Dallas/Fort Worth International Airport (DFW) assieme al Dallas Love Field (DAL), New York City's John F. Kennedy International Airport (JFK), Newark Liberty International Airport (EWR), LaGuardia Airport (LGA), assieme all'Aeroporto di Torino (TRN), Edinburgo (EDI), Nizza Côte d'Azur Airport (NCE). Tutti questi aeroporti utilizzano le soluzioni Everbridge per gestire la valutazione delle minacce, la risposta e la risoluzione degli incidenti durante gli eventi critici e gli incidenti relativi alla sicurezza che incidono sulle operazioni e sulla safety.
Vorrei citare Justin Cory Bond, Kansas City Aviation Department, che ha commentato: "In una situazione di allarme, le notifiche ai soccorritori aeroportuali che prima richiedevano più di 20 minuti ora ne richiedono meno di due, consentendo al nostro personale di concentrare le proprie energie sulla gestione della crisi, piuttosto che sull'invio delle notifiche. Everbridge offre il prodotto più personalizzato e ricco di funzionalità in circolazione, fornendo allo stesso tempo il massimo in termini di facilità d'uso".
Ed anche Jim Hewitt, DFW Airport Operations ha detto: "In qualità di clienti di lunga data di Everbridge, siamo rimasti costantemente colpiti dalla solidità della loro piattaforma, nonché dalla loro capacità di comprensione dell'ambiente operativo dell'aeroporto, adattando il loro prodotto alle nostre esigenze specifiche".
Vorrei infine sottolineare che, oltre agli aeroporti, i prodotti Everbridge sono utilizzati da alcune delle più grandi compagnie aeree del mondo, dai porti marittimi più trafficati, dalle più grandi compagnie di crociera, nonché dalle maggiori ferrovie del mondo, per migliorare la collaborazione in situazioni gravi, come come episodi di maltempo o attacchi terroristici. Everbridge serve anche molte città che ospitano questi snodi del trasporto pubblico.

everbridge®

Contatti:
Everbridge Italia
www.everbridge.com

Videosorveglianza e sicurezza informatica, una garanzia in più per gli aeroporti da Hanwha Techwin

intervista a Fabio Andreoni, Country Manager Italy & Greece di Hanwha Techwin Europe

Possiamo fare il punto sull'evoluzione tecnologica della videosorveglianza e sulle possibili applicazioni negli aeroporti?

E' prima di tutto necessario premettere che gli aeroporti sono, per loro natura, aree sensibili e ad alto rischio sotto molteplici aspetti. Inoltre, ogni aeroporto è un caso a sé stante, che pone sfide uniche a causa delle peculiarità delle proprie strutture.

In questo scenario, gli ambiti in cui le tecnologie di videosorveglianza possono giocare un ruolo importante nel supporto alle attivitá di Health, Safety, Security sono molteplici.

Oltre al controllo delle aree perimetrali e degli accessi, che sono la prima applicazione a cui viene associata la videosorveglianza, oggi la tecnologia e le logiche di analisi video avanzate consentono di utilizzare sistemi di ripresa anche per la gestione ed il controllo del flusso dei passeggeri identificando, ad esempio, assembramenti o spostamenti anomali, oggetti abbandonati o la presenza di persone non autorizzate in aree definite.

Questa tipologia di analisi viene effettuata tramite algoritmi basati su logiche di Intelligenza Artificiale Deep Learning direttamente a bordo delle telecamere.

Tutto ciò rappresenta un importante passo in avanti dal punto di vista tecnologico, poiché viene garantita una maggiore precisione dell'analisi ed una maggiore velocitá nella rilevazione di anomalie, senza dover appesantire il traffico di dati sulla rete e nel centro di controllo.

Anche l'aumento della risoluzione delle immagini fornite dalle telecamere, ed oggi la risoluzione 4K é ormai un'esigenza consolidata, aiuta ad aumentare ulteriormente il livello di efficienza di un sistema di videosorveglianza.

Tutte queste funzioni e queste caratteristiche sono presenti nelle telecamere di ultima generazione di Hanwha Techwin,

grazie alla capacitá di calcolo dei processori ed alla qualitá dei sensori utilizzati.

In che modo Hanwha Techwin risponde alle esigenze di sicurezza cibernetica?

Hanwha Techwin ha una solida strategia di sicurezza informatica che pone la protezione dagli attachi informatici all'inizio del processo di progettazione di un prodotto.

Abbiamo sviluppato un processore, denominato **Wisenet7**, che ci consente di affermare che il livello di protezione informatica delle nostre telecamere é tra i piú accurati ad oggi sul mercato.

Utilizziamo un firmware criptato, con logiche di controllo e certificazione a garanzia della mancanza di manomissioni o di modifiche indesiderate.

Il sistema operativo é memorizzato in un'area specifica di memoria particolarmente protetta ed anche le procedure di avvio della telecamera sono progettate in modo da non consentire alcun accesso, finché tutte le funzioni di protezione non siano state attivate.

Dal punto di vista dell'utente, abbiamo implementato anche logiche che richiedono accesso tramite password complesse, e che devono essere modificate al primo accesso.

Tutti questi accorgimenti ci hanno permesso di ottenere la certificazione **UL CAP** (Cybersecurity Assurance Program), un programma che valuta potenziali problemi di sicurezza informatica e il possibile livello di esposizione ad un attacco informatico offerto dai dispositivi hardware e software collegabili in rete.

Hanwha Techwin supporta inoltre la conformità allo standard NDAA, la legge federale degli Stati Uniti che proibisce alle agenzie federali statunitensi e ai loro appaltatori di usare apparecchiature di videosorveglianza fornite da una serie di aziende. Un produttore conforme all'NDAA come Hanwha Techwin, pertanto, mostra di possedere i requisiti richiesti dalle agenzie federali: un livello estremamente alto di sicurezza e due diligence che rassicura tutte le altre organizzazioni e organismi governativi. L'ultima generazione di prodotti e soluzioni Wisenet è progettata e realizzata nel rispetto dello standard 'Secure by Default' con l'obiettivo di garantire che i prodotti di videosorveglianza non presentino rischi dal punto di vista della cyber security e della rete per impostazione predefinita, pronti all'uso.

Infine, consideriamo un nostro dovere riconoscere l'importanza di essere aperti e onesti con i clienti quando identifichiamo nuove minacce alla sicurezza informatica. Per questo, ci impegniamo ad agire rapidamente per aggiornare il nostro firmware per combattere nuove minacce, con l'aiuto del nostro team interno S-CERT (Security Computer Emergency Response Team), che è interamente concentrato sull'affrontare qualsiasi potenziale vulnerabilità. I membri del team S-CERT sono stati accuratamente selezionati per la loro esperienza nell'essere in grado di identificare, analizzare e rispondere rapidamente con contromisure efficaci a qualsiasi minaccia alla sicurezza informatica.

Possiamo parlare delle realizzazioni di Hanwha Tecwin in aeroporti internazionali?

Ci sono diverse realtá aeroportuali che utilizzano prodotti Hanwha Techwin per la videosorveglianza. Tra i piú rappresentativi, possiamo citare Heathrow e Manchester nel Regno Unito, Nantes e Nizza in Francia, ma anche Roma Fiumicino, Ciampino, Pisa e Verona, solo per fare alcuni esempi sul territorio nazionale.

Hanwha Techwin Europe

Contatti:
Hanwha Techwin Europe LTD
Tel. +39 02 36572 890
www.hanwha-security.eu/it

SICUREZZA INTEGRATA IN AEROPORTO

Genetec per la sicurezza fisica

intervista a Giovanni Taccori, Commercial Lead Airport di Genetec Inc.

Quali solo le applicazioni sviluppate da Genetec relative alle diverse esigenze HSS in Aeroporto?
Le minacce emergenti e l'aumento del traffico richiedono un miglioramento delle procedure di sicurezza, che purtroppo causano frustrazione nei viaggiatori, sempre meno propensi a fidelizzarsi alle compagnie aeree perché spesso costretti ad attendere in code estenuanti. Questo malcontento ha ovviamente un impatto sui ricavi e sul brand dell'aeroporto. I gestori vengono sommersi da un numero crescente di sistemi e applicazioni, mentre l'IT è sovraccaricato dai requisiti di manutenzione e aggiornamento. Il risultato è un aumento costante dei costi associati alla formazione del personale, alla garanzia di compatibilità dei sistemi e alla manutenzione di più soluzioni.
Genetec aiuta gli aeroporti a mantenere i passeggeri al sicuro con un approccio unificato e guidato alla sicurezza, dai parcheggi ai terminal, alle piste, migliorando al contempo le operazioni grazie a una migliore correlazione dei dati disponibili per monitorare in modo proattivo le situazioni di interesse, anticipando possibili minacce o anomalie e gestendo il flusso dei passeggeri.
I tradizionali sistemi indipendenti e scollegati vengono ora gestiti attraverso un'unica user interface. Questo elimina la compartimentalizzazione di dati e migliora le capacità del sistema di condivisione dei dati con tre obiettivi principali:

- *migliorare le operazioni di sicurezza sfruttando la logica aziendale dell'aeroporto nelle attività di sicurezza quotidiane*
- *tutelare la sicurezza dei passeggeri monitorando il loro flusso (ad esempio, monitorando in modo proattivo l'affollamento degli edifici, i ritardi, lo sbarco dei voli di interesse, ecc.)*
- *aumentare l'efficienza e la conformità grazie al comportamento automatizzato del sistema e al supporto decisionale dell'operatore.*

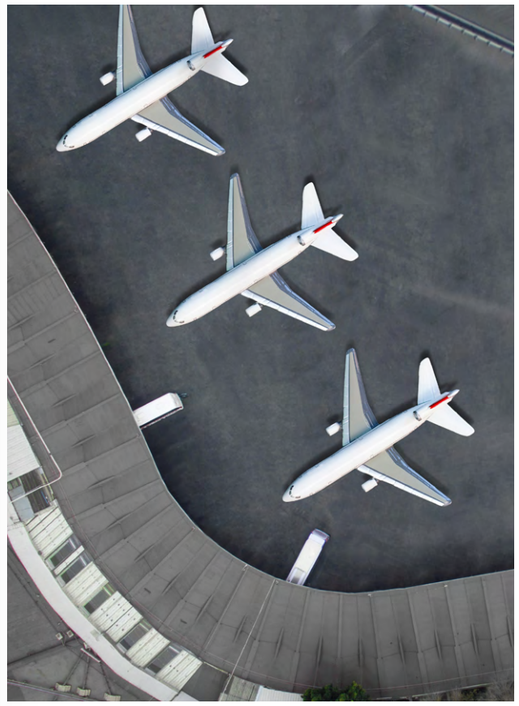
Unificazione dei sistemi video, controllo degli accessi, rilevamento delle intrusioni perimetrali e connessione agli ecosistemi specifici degli aeroporti: tutto all'interno di un'unica piattaforma, Security Center. Questo per dare al team di sicurezza e operativo una visibilità completa sull'intero aeroporto e sulle sue operazioni.

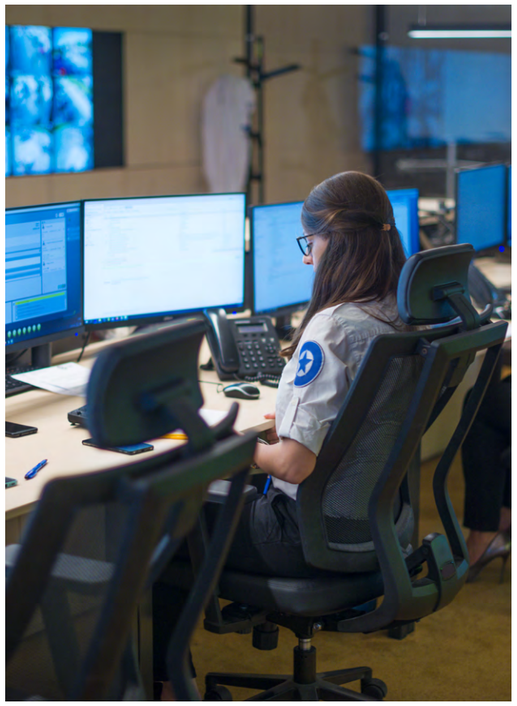
Possiamo parlare delle esperienze maturate da Genetec a livello internazionale?
Le installazioni di Genetec negli aeroporti (possiamo vantare oltre 20 anni di esperienza) vanno da sistemi con poche centinaia a migliaia di telecamere, porte, altri dispositivi e sensori a terra. Una tale quantità di dati provenienti da sistemi eterogenei (infrastrutture di sicurezza, funzionamento degli aeromobili, conteggio dei passeggeri, ecc.) viene convertita in informazioni e approfondimenti significativi per intervenire su attività, situazioni e minacce quotidiane.
Tra i nostri clienti possiamo citare molti grandi aeroporti in qualsiasi area del mondo, come Aéroports de Paris, Aeroporti di Roma in Europa, Dubai e Istanbul in Medio Oriente, Seattle, Montreal e Toronto in America o Auckland e Singapore.

Tra i vari moduli aggiuntivi specifici per gli aeroporti installati sono il BRM (Boarding Route Management) e l'RSA Surveillance. BRM sfrutta la serie completa di funzioni disponibili nel controllo accessi Synergis e garantisce l'apertura o la chiusura di porte specifiche lungo percorsi designati tra il terminal dell'aeroporto e l'aereo. BRM introduce i gate come entità nativa della piattaforma; ogni gate contiene una o un gruppo di porte per il controllo degli accessi, con telecamere di videosorveglianza associate (e/o qualsiasi altra entità disponibile). L'automazione delle procedure di imbarco e sbarco rafforza il controllo delle frontiere e la capacità di identificare rapidamente eventuali anomalie del sistema. Riducendo l'impatto operativo di possibili errori umani, si possono evitare anche costose chiusure dell'aeroporto e interruzioni del servizio.

RSA Surveillance protegge gli spazi aeroportuali integrandosi con una serie crescente di tecnologie di rilevamento delle intrusioni come sistemi di recinzione, dispositivi di tracciamento avanzati come radar (per il lungo raggio) o laser e video analisi di telecamere (per il corto raggio), consentendo di rilevare potenziali minacce in vaste aree per rafforzare la sicurezza di pista, aeromobili, viaggiatori e personale. Tracciate automaticamente su mappe, le intrusioni (i target in movimento rilevati dai diversi sistemi antintrusione) vengono visualizzate in modo intuitivo, in modo che il personale addetto alla sicurezza aeroportuale valuti e risponda alle minacce in minor tempo.

Grazie a RSA Surveillance è anche possibile tracciare la posizione degli aeromobili in tempo reale sulla base dei dati del protocollo ADS-B. Grazie a questa funzione, gli operatori possono monitorare facilmente il traffico di aeromobili in avvicinamento e in partenza dal proprio aeroporto, dall'atterraggio alla piazzola di sosta assegnata, utilizzando il segnale GPS trasmesso tramite il transponder installato sugli aeromobili. La collaborazione senza soluzione di continuità tra tutte le parti interessate sotto un'unica interfaccia aiuta a ridurre al minimo la potenziale congestione, gli incidenti e le incursioni in pista nell'area di movimento dell'aeroporto.





SICUREZZA INTEGRATA IN AEROPORTO

Genetec per la sicurezza cibernetica

intervista a Mathieu Chevalier, Principal Security Architect di Genetec Inc.

Come risponde Genetec alle esigenze di cybersecurity del Sistema aeroportuale e, in generale, dei trasporti pubblici?
Le soluzioni Genetec vengono create tenendo conto dei requisiti di sicurezza informatica. Progettate sin dalla loro concezione per incorporare le migliori pratiche di cybersecurity, includono vari strumenti che possono essere utilizzati per mantenere sempre protetti i sistemi di sicurezza fisica degli aeroporti.
Le più importanti best practice di sicurezza informatica sono ormai note: evitare di utilizzare password predefinite, mantenere aggiornati i componenti del sistema e utilizzare protocolli sicuri come l'HTTPS. Facile a dirsi, ma quando si tratta di implementazione le cose si fanno più complesse. Ed è su quest'ultimo aspetto che Genetec sta lavorando per aiutare i clienti degli aeroporti e dei trasporti pubblici, fornendo i mezzi per implementare le migliori prassi su scala, creando sistemi sicuri con impostazioni predefinite, automatizzando i processi di aggiornamento che devono essere eseguiti continuamente e fornendo indicazioni su come i prodotti debbano essere configurati per essere sicuri. Una cyber-dashboard consente inoltre agli utenti finali degli aeroporti di confrontare in tempo reale lo stato del loro sistema con le best practice informatiche raccomandate da Genetec. Ciò consente di stabilire lo status di sicurezza del proprio sistema e di migliorarlo nel tempo.
Lavorando in aeroporti dislocati in tutte le regioni del mondo, è per noi fondamentale che i partner capiscano l'importanza della sicurezza informatica. Per contribuire alla sicurezza della supply chain dei nostri clienti, scegliamo con cura gli integratori e forniamo formazione in ambito informatico. Genetec promuove inoltre l'innovazione collaborando con altri produttori consapevoli dell'importanza della cybersecurity e introducendo sul mercato nuove funzionalità di sicurezza, come la crittografia video end-to-end.

Genetec™

Contatto:
Genetec
Tel. +39 327 739 8560
www.genetec.com

RVI, il partner di eccellenza per la sicurezza delle IC del trasporto

intervista a Lucio Piccinini, Direttore Tecnico di Rete Vigilanza Italia

Per iniziare, ci può riassumere gli obiettivi, la composizione e la struttura operativa di Rete Vigilanza Italia?
Rete Vigilanza Italia nasce con l'obiettivo di valorizzare le imprese di vigilanza nei rispettivi territori per rispondere, attraverso efficaci azioni di sinergia organizzativa e di coordinamento, alle richieste di servizi integrati, ultra provinciali e di alta qualità che il mercato richiede con sempre maggiore frequenza.
L'organo principale della rete è il comitato di gestione presieduto dal presidente Giancarlo Liberatore, il vice presidente Angelo Paolo Pietroboni, il direttore tecnico nella persona del sottoscritto e 4 consiglieri appartenenti ad altrettante aziende associate.

In che modo Rete Vigilanza Italia, di cui Vigilanza Group è promotore, si propone nel segmento dei servizi di sicurezza per le Infrastrutture del trasporto?
Rete Vigilanza Italia sta sviluppando mirate azioni per uniformare i processi gestionali per un'erogazione di servizi con alti standard qualitativi sull'intero territorio nazionale, in particolare attraverso un percorso di certificazione univoco alle norme di riferimento (UNI 10891, UNI EN 50518). Procedure operative condivise, reattività nella gestione di ogni evento, capillarità e conoscenza specifica dei territori dove le aziende associate operano con efficacia da decenni, centrali operative ad altissimo contenuto tecnologico, sono solo alcuni dei plus offerti da RVI.
Per tutto quanto sopra descritto, RVI si propone come interlocutore di riferimento nel mercato della sicurezza a 360°, capace di analizzare, progettare ed erogare servizi di eccellenza per le aziende pubbliche e private che operano nelle infrastrutture dei trasporti.

Quali sono le risposte di RVI alle esigenze di sicurezza cibernetica?
Il tema della cyber security è molto delicato e l'esposizione alle minacce specifiche delle organizzazioni pubbliche e private è in generale aumentata dalla scarsa sensibilità e conoscenza dei rischi cyber. RVI sta affrontando questo tema così attuale e importante attraverso lo sviluppo di partnership stabili con aziende già consolidate nello specifico mercato, dotate di strumentazione e SOC capaci di analizzare ogni singolo rischio cibernetico. Pertanto, la gamma dei servizi offerti da RVI sarà estesa a breve anche all'ambito cyber su più livelli, per offrire il massimo anche in questo settore.

Quali sono i servizi relativi ai diversi scopi di HSS (Health, Safety, Security) che RVI può offrire?
Altro tema attualissimo quello dell'HSS che Vigilanza Group, capofila di RVI, ha affrontato nel tempo in modalità "pioneristica" in particolare sul piano delle tecnologie, acquisendo competenze ed esperienze che oggi mette a disposizione di RVI.
Servizi di video-analisi centralizzata su PSIM, centralizzazione certificata dei segnali incendio compliant alla UNI EN 9795, servizi di ricezione e gestione segnali di man-down attraverso importanti partnership con produttori nello specifico mercato, accompagnati da un supporto consulenziale di alto profilo focalizzato alle esigenze del cliente, sono alcuni dei fattori che permettono all'intera Rete Vigilanza Italia di proporsi come interlocutori di riferimento per tutto il mercato della sicurezza, in particolare per operatori e gestori delle infrastrutture dei trasporti.

RVI
RETE VIGILANZA ITALIA

Contatti:
Rete Vigilanza Italia
Tel. +39 0307285194
info@retevigilanzaitalia.it

Da Vigilate innovazione e tecnologia per Health, Security e Safety di ferrovie, strade e luoghi ad alta frequentazione

intervista a Stefano Gosetti, Vice Presidente di Vigilate srl

Quali sono le applicazioni relative ai diversi scopi di HSS che Vigilate ha sviluppato per le infrastrutture dei trasporti pubblici?
Vigilate, da sempre impegnata nella Security, negli ultimi anni ha sviluppato nuove soluzioni in ambito Safety rivolte all'osservanza delle nuove regole comportamentali ed al controllo delle persone che, a fine emergenza, si sono mantenute e trasformate in uno standard permanente.
E' stato così progettato e prodotto **v-SHAPE**, un sensore 'lidar' che, tramite analisi tridimensionale, effettua la rilevazione e il conteggio delle persone per il contingentamento ed i piani di evacuazione nei luoghi ad alta frequentazione. Questa soluzione si differenzia dal 'people counting' effettuato con video-analisi delle telecamere in termini di 'reliability', passando da un'accuratezza di circa il 90% a quella del 99,7% medio ottenuto con la tecnologia tridimensionale.
Nel settore ferroviario, Vigilate ha sviluppato un sistema di video-analisi di rilevazione passeggeri e del loro comportamento in stazione, creando particolari allarmi se, ad esempio, vengono attraversati i binari in passaggi non consentiti.

In forza della consolidata esperienza negli apparati di lettura targhe (ALPR), Vigilate fornisce ai gestori autostradali i sistemi **v-LANE A5** e sta sviluppando, assieme ad un primario system integrator, un nuovo sistema di pedaggiamento free-flow alternativo ai caselli di pedaggiamento tradizionali.
A febbraio 2021, Vigilate è entrata nel business delle Smart Road, diventando partner tecnologico di ANAS per la realizzazione di un tratto sperimentale in occasione di un importante evento sportivo.

In questa esperienza, oltre ad offrire le funzionalità 'core' quali la lettura delle targhe e le informazioni connesse al transito, abbiamo sperimentato con successo la prima comunicazione automatica fra veicoli ed infrastruttura C-V2x (Cellular-Vehicle to Everythingh), necessaria a supportare scenari di guida autonoma L3, L4, e L5 che caratterizzeranno il futuro dell'autotrasporto.
Le comunicazioni 'infrastruttura-veicoli' sono sotto la sigla di C-V2x, dove scenari evoluti ad alta automazione mescolano le informazioni dei veicoli con quelle di altri veicoli e dei dispositivi mobili delle persone presenti nell'area, con le informazioni provenienti dalle piattaforme Smart che gestiscono i territori.
Vigilate ha recentemente sviluppato una nuova famiglia di prodotti C-V2x impiegati in una importante commessa 'Smart Road' che verrà attivata nei prossimi mesi. Si tratterà di una delle prime Smart Road europee dove le comunicazioni C.V2x entreranno realmente in servizio.

Su queste nuove tecnologie, verranno anche convertite molte applicazioni tradizionali di controllo del traffico, quali il pedaggiamento autostradale e urbano, i sistemi di parcheggio a pagamento, i sistemi di sanzionamento ('speed enforcement', 'red light enforcement', Traffic Limited Zone, ecc). che oggi utilizzano tecnologie tradizionali come le telecamere di lettura targa o i transponder WiFi.
Il prodotto dispone di un'unità di elaborazione embedded per la gestione della suite di messaggi ETZI C-V2x, per la criptazione e decriptazione degli stessi, per la gestione dello stack e delle policy di sicurezza secondo gli standard definiti dal comitato europeo C-ROADS.
Vigilate ha trasformato queste esperienze in un prodotto di mercato, lo SmarTekPole, una soluzione di palo intelligente modulare presentato ad Intertraffic di Amsterdam lo scorso marzo. **SmarTekPole** permette, tra le diverse funzionalità ALPR, AID (Automatic Incident Detection), C-V2x, IoT, qualità dell'aria, ecc. di scegliere punto per punto lungo la rete stradale quali funzioni si vogliono attivare.

In che modo Vigilate risponde alle esigenze di sicurezza cibernetica?
Secondo le previsioni di mercato, entro la fine del 2022 il 65% del PIL globale sarà digitalizzato. Sebbene le crescenti capacità delle connessioni di rete offrano nuove opportunità, si aprono anche una serie di rischi per la sicurezza delle informazioni.
Vigilate risponde a questa esigenza sia in termini di prodotto che di piattaforme software. La progettazione e lo sviluppo del software dei prodotti non si deve infatti limitare ai requisiti funzionali, ma deve pensare anche alla sicurezza e all'inviolabilità del software in modalità 'security-by-design'. Le tecniche progettate a livello di prodotto hanno infatti portato a sviluppare comunicazioni cifrate e streaming video autenticati; le archiviazioni dei dati e delle immagini sono criptate in AES a 256 bit. Particolare importanza sulla gestione degli utenti che accedono ai sistemi, sia in termini di identificazione digitale univoca effettuata con un token di autenticazione 'single-sign-on', sia in termini di *reputation score* dove, tramite l'integrazione con piattaforme apposite casi di aziende o persone collegate a soggetti inseriti all'interno di liste criminali, politicamente esposte, con precedenti per frodi finanziarie (riciclaggio o corruzione) o soggetti sanzionati per commerci con Paesi non autorizzati, vengono bloccati ed il tentato accesso viene segnalato.
Infine, fondamentale per la certificazione della prova è la marcatura temporale delle immagini tramite metadati che riportino il 'timestamp', il relativo riferimento NTP, e la sorgente univoca che ha generato tali immagini (certezza di 'dove e quando').
Anche se per strutture critiche è tipicamente utilizzata l'installazione 'on-premises', a livello di piattaforma possono essere previste connessioni con la rete pubblica per servizi di 'disaster recovery' e 'business continuity', oppure per l'utilizzo dall'esterno della rete protetta. Il numero crescente di sofisticati attacchi informatici comporta nuovi metodi di organizzazione digitale, ed anche i regolamenti devono andare di pari passo.
Al riguardo, Vigilate sta intraprendendo la certificazione CSA STAR che prevede il passaggio al CCM (Cloud Control Matrix) V4 ai fini dell'implementazione della ISO/IEC 27001.

Possiamo parlare di realizzazioni di Vigilate in questi contesti?
Le soluzioni ferroviarie sono state realizzate per RFI Roma, Ferrotranviaria (Ferrovie Nord Baresi) e Ferrovie Appulo-Lucane. Per le autostrade, i lettori targhe v-LANE A5 sono stati forniti al Ministero dell'Interno per i PON Sicurezza di Sicilia e Puglia, mentre la soluzione free-flow è installata sulla BreBeMi. La prima realizzazione sperimentale di Smart Road è stata installata per ANAS in un tratto sperimentale della Alemagna a gennaio-febbraio 2021 in occasione dei Campionati Mondiali di sci a Cortina.

VIGILATE

Contatti:
Vigilate
Tel. +39 030 8081000
www.vigilatevision.com

Tsec, protezioni perimetrali intelligenti per infrastrutture

intervista a Giordano Turati, CEO di Tsec srl

Quali sono le applicazioni che ha sviluppato TSec idonee per le infrastrutture dei trasporti pubblici?
Principalmente due. Un sensore volumetrico di nuova generazione e un sistema perimetrale per il controllo delle recinzioni. Il primo si basa su un nuovo principio di intelligenza a bordo del sensore stesso, in grado di rilevare la distanza degli oggetti in movimento e di elaborare autonomamente informazioni in grado di distinguere un essere umano da un piccolo animale o da un mezzo meccanico. L'utilizzo principale è la protezione di aree dove è necessaria un'informazione certa della presenza di persone non autorizzate.
Il secondo si basa su sensori con tecnologia 'MEMS' e su un sofisticato algoritmo di rilevazione e gestione studiato e testato da TSec. L'insieme consente al sistema **MACS** di rilevare con grande precisione i tentativi di scavalcamento e di minimizzare eventuali rilevazioni improprie dovute a pioggia e vento, alla presenza di strade, ferrovie o mezzi in movimento situati nelle vicinanze della recinzione e le azioni umane non assimilabili allo scavalcamento. MACS è in grado di riconoscere tentativi di manomissione eseguiti sulle schede di controllo, sui sensori o sul cavo, nonché tentativi di taglio, sfondamento e/o rimozione del pannello della recinzione, sia essa rigida o a rete magliata.
Il sistema permette di identificare in maniera univoca ciascun sensore sia in fase di programmazione sia in fase di monitoring, fornendo una puntuale indicazione del sensore che ha generato l'allarme.
Il sistema è composto da catene di sensori collegati tra loro attraverso bus proprietario; una scheda master posta sul campo, nella quale convergono le catene di sensori; una scheda ethernet, posta in interno, che alimenta tutto il sistema e si interfaccia con la centrale di allarme e il mondo IP. La configurazione e la gestione del sistema avvengono attraverso una semplice ed intuitiva interfaccia web.
Le applicazioni riguardano principalmente la protezione perimetrale delle aree attorno a siti sensibili.

Possiamo parlare di realizzazioni di TSec in questi contesti?
Certamente, abbiamo partecipato a progetti per il monitoraggio di stazioni metropolitane per la protezione dei tunnel da intrusioni di personale non autorizzato. In un caso specifico, c'era la necessità di rilevare persone nei sottopassaggi di metropolitane e stazioni ferroviarie durante le ore notturne.
Di particolare interesse per questo appuntamento di APR, la realizzazione di sistemi per la protezione dei perimetri di aeroporti internazionali.

In che modo TSec risponde alle esigenze di sicurezza cibernetica ?
Ogni nostro dispositivo connesso nasce da un input progettuale ben preciso: la sicurezza della comunicazione sia verso l'esterno sia tra i componenti del sistema stesso. Un esempio si trova nei protocolli di comunicazione usati nel sistema perimetrale MACS e nel sensore radar **MSK-101 POE**. Entrambi i sistemi integrano un co-processore crittografico conforme **FIPS** (Federal Information Processing Standards) con archiviazione sicura delle chiavi e crittografia asimmetrica.

TSec
TECHNOLOGY FOR SECURITY

Contatti:
TSec srl
Tel. +39 030 5785302
www.tsec.it

Da Citel la suite Open PSIM/BMS per la gestione integrata dei Building e delle infrastrutture del trasporto

intervista a Nils Fazzini, CEO di Citel srl

Quali sono le applicazioni relative ai diversi scopi di HSS (Health, Safety, Security) che Citel ha sviluppato per le infrastrutture dei trasporti pubblici, quali aeroporti, porti, stazioni ferroviarie, metropolitane, autostrade?
Negli anni abbiamo sviluppato tantissime soluzioni per infrastrutture critiche di interesse nazionale. La suite Open PSIM/BMS di Citel è stata capace di raccogliere le diverse esigenze dei nostri clienti grazie alle modularità e all'apertura dei vari prodotti che offriamo. La suite oggi risponde alle esigenze di ogni organizzazione tramite la sua architettura che parte dalla raccolta delle informazioni dal campo, l'armonizzazione dei dati e la classificazione, tramite algoritmi di machine learning. Le informazioni, poi, vengono processate tramite i workflow e integrate grazie anche al potente motore di correlazione interno al sistema. Lo scenario, una volta gestito grazie anche alle correlazioni tra i vari sistemi verticali e dipartimentali, viene ulteriormente analizzato tramite la business intelligence e i report che portano il security manager e il suo team ad avere sempre una visione chiara e distinta della situazione generale. Non dobbiamo dimenticare, inoltre che poter prendere decisioni rapide e mirate è fondamentale che gli strumenti usati siano in grado di offrire informazioni chiare, precise e immediate.
La suite Open PSIM/BMS di Citel, oggi conta molti moduli specializzati che consentono di abbracciare diversi contesti tecnologici e procedurali. Alcuni di questi moduli sono sviluppati internamente e altri sono il frutto di collaborazioni tecniche e strategiche con grandi player nazionali e internazionali. Oggi possiamo gestire, oltre all'intrusione, videosorveglianza, controllo accessi e video analisi

(di più di 100 brand), tutti i sistemi tecnologici legati al building management, soluzioni di cyber security, network management e soluzioni di deep learning. Inoltre, grazie all'ingresso nel Gruppo tecnologico SeSa, possiamo anche offrire soluzioni avanzate di assets management dotate di tecniche di manutenzione evolute e predittive; tecnologie all'avanguardia che rispondono alla sempre maggior esigenza di controllo e gestione degli innumerevoli sistemi OT/IOT che vengono utilizzati all'interno delle aziende e distribuiti su scala geografica.
In questi anni è stato sempre più rilevante poter offrire soluzioni multi dipartimentali che vadano dalla security alla safety con una prospettiva che consenta di abbracciare la questione da differenti punti di vista: cyber, maintenance, services. Queste sono sinergie che creano valore e aiutano

a preservare la continuità del business e la resilienza dell'azienda rispetto alle innumerevoli sfide competitive a cui oggi siamo chiamati a rispondere tramite l'innovazione.

In che modo Citel risponde alle esigenze di sicurezza cibernetica delle infrastrutture dei trasporti pubblici?
Le soluzioni di Citel e dei suoi partner sono progettate per essere compliance ai principali e più diffusi standard di sicurezza e di progettazione richiesti oggi dai grandi gruppi industriali del Paese. Oltre, quindi, ad un livello di sicurezza intrinseca ci sono le soluzioni a protezione del perimetro cibernetico che si trovano predisposti presso i clienti o che possiamo offrire anche noi grazie alle soluzioni a catalogo.
La dimensione cyber è inoltre per noi molto importante anche dal punto di vista pro-attivo grazie alla sinergia innescabile tra cyber-physical security. Soprattutto nella correlazione tra accessi digitali e fisici a determinate strutture delle aziende che proteggiamo.

Possiamo parlare di realizzazioni di Citel in questi contesti?
La nostra esperienza è focalizzata su infrastrutture critiche soprattutto nei settori Oil&Gas, Energy e Multiutilities. Abbiamo esperienza anche in contesti pubblici di rilievo molto sensibili. Tutte queste esperienze ci consentono di far crescere costantemente le nostre soluzioni e di anticipare alcune soluzioni sul mercato.

CITEL

Contatti:
Citel spa
marketing@citel.it
www.citel.it

Newton
7-Color 4-Color

Migliora la **customer experience** dei tuoi clienti e potenzia le tue capacità di **comunicazione digitale in negozio**

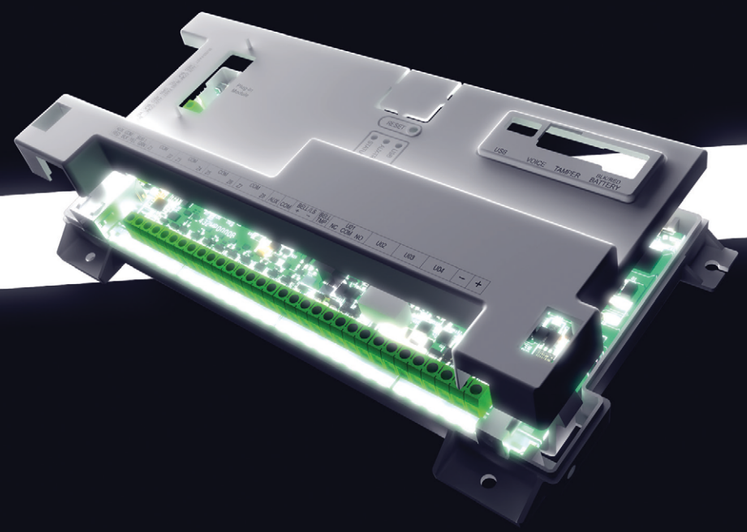
Etichette elettroniche
a 4 e 7 colori
Massime prestazioni
Display ad alta risoluzione

omnisint
around technology

SOLUM
Solution provider.

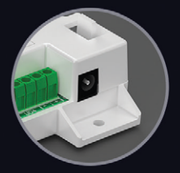
FLESSIBILE. **INTELLIGENTE. POTENTE.**

LightSYS+
La più potente centrale antintrusione ibrida



Moduli IP e Wi-Fi Integrati

Nuovo ingresso per cavo standard USB di Tipo C.



Nuovo guscio protettivo

La nuova LightSYS+ è la centrale ibrida fiore all'occhiello di RISCO, e combina le caratteristiche e i benefici di LightSYS 2 e ProSYS Plus in un sistema di sicurezza dalle grandi capacità. E' progettata per installazioni di ogni tipo o dimensione, Grado 2 o Grado 3 – e può gestire fino a 512 zone!

- Flessibile tanto da gestire situazioni complesse con centinaia di zone.
- Intelligente tanto da discriminare tra eventi reali e falsi allarmi.
- Potente tanto da integrare tipi diversi di componenti.

Una centrale – infinite soluzioni

Per maggiori informazioni su LightSYS+, visitate:
WWW.RISCOGROUP.IT

RISCO
A LIFE TIME OF SECURITY

Proteggere i data center da intrusioni e manomissioni interne

di Marco Censi, Regional Sales Manager Italia per OPTEX

I data center sono fondamentali nella maggior parte delle operazioni istituzionali e commerciali odierne. Con server collegati in rete e apparecchiature di comunicazione, permettono ad aziende e istituzioni di accedere, trasferire e archiviare le informazioni digitali. I computer di questi centri sono raffreddati meccanicamente per evitare surriscaldamenti e si predispongono sistemi di alimentazione alternativa per evitare interruzioni del servizio. Il tipo di dati che gestiscono e proteggono può variare, ma di certo si tratta di dati importanti e sensibili.

Di conseguenza, gli ambienti occupati da sistemi tanto complessi, costosi e interdipendenti devono essere difesi da qualsiasi accesso non autorizzato.

È normale che gli edifici che ospitano i data center siano tutelati da un primo livello di sicurezza costituito da recinzioni perimetrali e barriere ma è indispensabile progettare un secondo livello nelle sale dei generatori e dei rack dei server, onde evitare che criminose intrusioni provochino danni o manomissioni gravi quanto quelli causati dai cyber-attacchi.

Soluzioni di sicurezza perimetrale ed esterna

Come tutti i siti sensibili, i data center richiedono più livelli di protezione tramite la messa in sicurezza di un'eventuale recinzione (che può essere tagliata o scavalcata), la protezione del perimetro mediante barriere e/o dei tetti e delle pareti esterne (protezione da eventuali scalate, perforazioni o semplici ingressi da uscite di sicurezza). Per questo si consiglia una combinazione di più livelli di sicurezza: un sistema recinzione/muri esterni e un "muro virtuale" per rilevare eventuali intrusioni ed essere in grado di fornire una risposta tempestiva.

Tipicamente, i sensori a fibra ottica sono applicabili direttamente su recinzioni o muri oppure a terra, perché registrano le vibrazioni causate dai tentativi di tagliare la linea perimetrale o di scavalcarla. Estremamente affidabile, tale soluzione offre anche un basso costo di gestione.

Mediante i sensori **OPTEX** a tecnologia LiDAR, i **REDSCAN**, è possibile creare delle pareti virtuali nelle varie zone d'accesso come cancelli, tornelli pedonali, banchine di carico, uscite d'emergenza; perfino coprire un'intera parete dell'edificio.

È inoltre capitato che gli intrusi siano riusciti a perforare le pareti o a entrare da lucernari sui tetti degli edifici. Per la protezione delle pareti, OPTEX suggerisce due tecnologie, a seconda dell'uso: i sensori a fibra ottica potranno rilevare le vibrazioni del trapano sul muro mentre il muro virtuale creato dal sensore laser rileverà chiunque si avvicini all'area delimitata. Il laser virtuale LiDAR potrà proteggere il tetto esterno con estrema precisione, dal momento che non risente minimamente delle condizioni di luce o di quelle atmosferiche.

Inoltre, la stessa tecnologia potrà creare un soffitto virtuale per l'interno, funzionando anche nell'oscurità più totale o a basse temperature, condizioni queste comuni all'interno dei data center.

Inoltre, se si desidera aggiungere una verifica visiva e una protezione a lungo raggio, REDSCAN Pro è munito di una telecamera integrata che permette una copertura ideale per le strutture molto ampie.

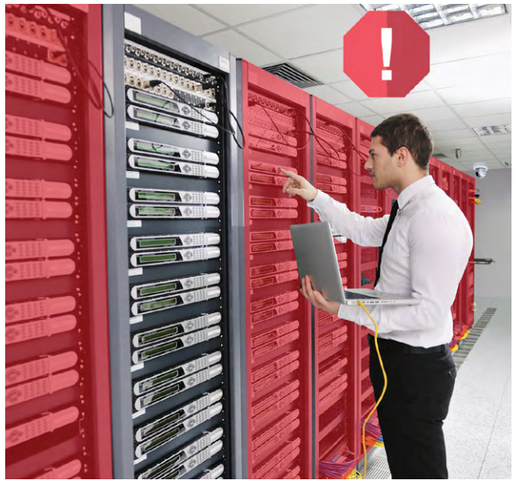
Soluzioni di sicurezza interna e piattaforme software di gestione

I sensori **REDSCAN** forniscono una rilevazione talmente accurata da offrire addirittura le coordinate X, Y esatte dell'intrusione. Ecco perché questo tipo di tecnologia è molto ricercata per proteggere i rack all'interno delle server room: è infatti in grado di individuare esattamente il luogo in cui è avvenuta una manomissione, il che permette di velocizzare i tempi di risposta e affrontare gli incidenti con maggiore consapevolezza.

REDSCAN consente di creare diverse aree di rilevamento, ad esempio corrispondenti ad ogni rack, e disattivare la zona quando un tecnico si sta occupando della manutenzione, mantenendo al contempo in sicurezza tutte le altre aree.

Quando si desidera sfruttare appieno tali e tante informazioni, i sensori vanno utilizzati unitamente a piattaforme software che abbiano le coordinate integrate, come le piattaforme **Genetec**.

Una piattaforma di sicurezza unificata, come il **Security Center Genetec**, può migliorare i tempi di risposta e aumentare la sicurezza del sito. Un sistema unificato con un'interfaccia basata su mappa permette al personale di trovare rapidamente, grazie alle coordinate X, Y e al supporto delle riprese video, il punto esatto dell'intrusione e una visione completa della scena. Grazie all'unificazione, la soluzione inoltre consente di visualizzare sulla dashboard anche il sistema di controllo accessi. In questo modo, le porte nella server room potranno essere chiuse se LiDAR rileverà un accesso non autorizzato o una manomissione.



Il Ministero per l'Innovazione tecnologica e la transizione digitale ha inserito tra le priorità del nostro Paese la *"realizzazione di un Polo Strategico Nazionale per i servizi che trattano dati critici, sotto controllo e indirizzo pubblico, per dotare la Pubblica Amministrazione di tecnologie e infrastrutture cloud che possano beneficiare delle più alte garanzie di affidabilità, resilienza e indipendenza."*[1] In tale ottica è stato lanciato un concorso per la realizzazione del parco data center della Pubblica Amministrazione.

Considerando i rischi che tali infrastrutture possono correre, è evidente come si debba progettare con cura la loro protezione e attraverso sistemi di sicurezza flessibili, precisi e affidabili.

REDSCAN Pro, la nuova generazione LiDAR di OPTEX

OPTEX
Sensing Innovation

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

[1] https://innovazione.gov.it/progetti/infrastrutture-digitali-e-cloud/

Come le aziende di trasporto di massa italiane possono beneficiare delle piattaforme unificate

di Gianluca Mauriello, Regional Sales Manager Italia, Genetec Inc

In questo articolo si spiega perché le aziende che si occupano di trasporto di massa dovrebbero pensare all'unificazione delle piattaforme di sicurezza per ottenere livelli più alti di collaborazione ed efficienza.

Verso la collaborazione nel settore dei trasporti?
L'industria del trasporto di massa in Italia è matura per una rivitalizzazione, poiché molte aziende stanno prendendo atto che i vecchi modi di pensare e lavorare 'in silo' le hanno trattenute per troppo tempo.
Dato che i veicoli e le tecnologie più vecchi stanno scomparendo, c'è l'opportunità di cambiare strategia. L'attenzione si sta spostando verso l'interconnettività e sul modo migliore per distribuire e gestire la sicurezza fisica in tutta la rete dei trasporti. E c'è un nuovo filone di dibattito che ruota intorno all'unificazione.
L'unificazione è un processo che permette di stare uniti e trasformarsi insieme. Dal punto di vista organizzativo, l'unificazione è fondamentale per l'adozione di nuove soluzioni tecnologiche che hanno un impatto su tutti gli aspetti delle operazioni legate ai trasporti. E mentre una struttura interna unificata può aiutare l'implementazione di nuove tecnologie, la tecnologia stessa può aiutare a guidare l'unificazione organizzativa, in particolare per la sicurezza.

Come le aziende di trasporti beneficiano dell'unificazione
Una soluzione unificata per la sicurezza dei trasporti è diversa da un sistema integrato. Al suo centro, vi è una suite di prodotti sviluppati come un'unica soluzione. Questo significa che si può standardizzare tutta l'organizzazione su una singola piattaforma di sicurezza. Su questa nuova piattaforma si possono poi fondere lentamente tutti i sistemi indipendenti, gestendo la sicurezza come una cosa sola.

I vantaggi dell'unificazione nel trasporto di massa sono di vasta portata:

- **Dati di bordo e di struttura unificati:** Basta perdere tempo a raccogliere manualmente i video di bordo o a usare fonti di dati separate per costruire una linea temporale degli eventi. Una piattaforma unificata semplifica le operazioni compilando e sincronizzando i dati, sia a bordo dei veicoli che nelle strutture dei trasporti
- **Accesso indipendente e centralizzato:** Le agenzie dei trasporti possono contare su un team centralizzato per monitorare e gestire la sicurezza in tutta l'organizzazione, pur consentendo a singoli reparti di accedere ai propri sistemi e dispositivi
- **Accesso più rapido alle nuove tecnologie:** Una soluzione di sicurezza unificata permette di mantenere i dispositivi esistenti e aggiungere nuove tecnologie nel tempo. Gli enti possono anche aggiungere licenze e provare nuove funzioni e applicazioni integrate secondo necessità, senza problemi di compatibilità
- **Meno formazione e manutenzione:** Gli operatori devono solo imparare i pro e i contro di un'unica soluzione di sicurezza. E coloro che gestiscono la manutenzione hanno un lavoro più facile perché tutti gli aggiornamenti e le configurazioni del sistema sono gestiti all'interno della stessa piattaforma
- **Costi operativi ridotti:** Controllo centralizzato, processi più efficienti, meno formazione e manutenzione aiutano a ridurre i costi operativi. E c'è solo un contratto di manutenzione del software da rinnovare ogni anno
- **Processi semplificati e più efficienti:** Utilizzando un'unica piattaforma, le agenzie dei trasporti possono fornire agli operatori protocolli di risposta automatizzati per migliorare la risposta alle emergenze. E non importa dove ha avuto luogo un incidente, gli investigatori saranno in grado di recuperare rapidamente le prove e condividerle con le autorità in modo sicuro
- **Aumento del servizio clienti:** Mantenere i clienti felici e sicuri può essere un catalizzatore per generare più entrate. Condividere l'accesso video con altri dipartimenti operativi può garantire che i treni o gli autobus arrivino in tempo, che le procedure di sicurezza vengano seguite e che le richieste di informazioni su oggetti smarriti o rubati siano risolte più velocemente.

Il passo più importante per unificare la sicurezza dei trasporti
L'unificazione non avviene dall'oggi al domani. Le aziende di trasporto di massa di tutto il mondo che hanno già iniziato a unificare le loro soluzioni di sicurezza stanno pensando a lungo termine e adottando un approccio graduale. Ma il passo più critico è il primo, ovvero formare un team centralizzato per supervisionare il progetto di unificazione.
Questo team diventa il punto centrale di contatto per tutti i dipartimenti, gli appaltatori e i fornitori di servizi che stanno gestendo la sicurezza fisica. Supervisionano a un più alto livello la soluzione unificata, mentre considerano anche le esigenze di ogni divisione all'interno dell'organizzazione.

Il futuro della sicurezza unificata dei trasporti
Gli obiettivi di questo team possono anche includere il gettare le basi per l'infrastruttura IT che supporterà la soluzione di trasporto unificata e le espansioni future.
Il che, in parte, significa chiedersi: *come vogliamo che sia la nostra piattaforma di sicurezza fisica tra 5, 10 o 15 anni e oltre?*
Questo è il momento in cui l'architettura aperta della piattaforma unificata entrerà in gioco.
L'apertura della piattaforma fa una grande differenza nella facilità con cui un'azienda di trasporti può accogliere e adattarsi alle mutevoli esigenze, anche in futuro. Permette al team di rimanere sempre flessibile e di accedere alle ultime e più grandi innovazioni, comprese, ad esempio, le nuove analisi perimetrali, o le tecnologie automatizzate dei droni.

Conclusioni
Muoversi verso una piattaforma di sicurezza unificata può sembrare scoraggiante per gli enti dei trasporti di massa. Creando un team dedicato e facendo un passo alla volta, qualsiasi ente può invece iniziare a modernizzare la sicurezza e aumentare la collaborazione. E l'investimento si ripagherà con il passare del tempo.
Impostare la giusta infrastruttura IT e scegliere una piattaforma aperta fa sì che l'investimento vada oltre. Con tutto questo, diventa più facile iniziare a unire le telecamere e i dispositivi esistenti sulla nuova piattaforma di sicurezza, così come portare i sistemi di bordo dei veicoli e altre tecnologie nel quadro più ampio della sicurezza.

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

Nasce JobforVigiles, il portale per la domanda e l'offerta di lavoro nella sicurezza

intervista a Sofia D'Arcangelo, HR Specialist di JobforVigiles

Ci parli di JobforVigiles, una novità assoluta nel panorama della sicurezza.
JobforVigiles è il primo portale web italiano interamente dedicato all'incontro tra la domanda e l'offerta di lavoro per i profili professionali del mondo della sicurezza.
10 profili professionali, un unico luogo dove cercarli e dove proporsi:

- **guardia particolare giurata**
- **addetto ai servizi di controllo delle attività di intrattenimento e di spettacolo**
- **stewarding impianti sportivi**
- **addetto di portierato e controllo**
- **addetto squadra antincendio**
- **installatore impianti tecnologici di sicurezza**
- **addetto attività di contazione denaro**
- **security manager**
- **collaboratore per incarichi investigativi**
- **profili amministrativi di staff**

Chi già lavora nel settore o vuole avviarsi ad una di queste professioni, può accreditarsi sul sito e riceverà le offerte di lavoro delle aziende che utilizzano JobforVigiles per cercare questi profili professionali.
Per le aziende, l'utilizzo è semplice: basta creare una propria pagina dedicata o, meglio ancora, affidarsi al back office dell'organizzazione per effettuare rapidamente tutte le ricerche di cui si ha bisogno. Dei semplici log permettono l'incrocio automatico tra una ricerca caricata da una azienda e le scelte fatte dagli utenti in fase di accreditamento.
JobforVigiles è anche una vetrina per le aziende del comparto, un modo per esserci ed essere riconosciute; per gli utenti è invece garantita la massima riservatezza: i dati caricati vengono veicolati solo se la persona decide di candidarsi ad un annuncio, ovviamente senza alcun costo.
Per gli utenti è poi semplice compilare il form di accreditamento, perché bastano pochi dati; volendo, però, si possono inserire curriculum e ulteriori specifiche, anche sulle competenze e certificazioni acquisite, utili a presentare meglio il proprio profilo.

Quali sono le motivazioni che vi hanno spinto alla creazione di questo strumento?
Jobforvigiles è la risposta ad una serie di necessità che faticavano a trovare sfogo. Di base, la difficoltà a trovare risorse umane da inserire in qualsiasi ambito produttivo, è diventata fortissima ma, anche, il desiderio di creare un punto di riferimento per il mondo esterno, qualcosa che provi a parlare di sicurezza anche a chi sta fuori.
Il portale, quindi, non vuole solo offrire opportunità di lavoro ma anche parlare del comparto e delle aziende che vi operano, per fare un po' di *employer branding* per le realtà di settore. Dare visibilità a cosa viene fatto e a chi lo fa.

Non dimentichiamo, inoltre, che per molti dei profili professionali gestiti dal portale sono anni che si parla di "albo", "elenco", "registro", ecc. Non si vuole arrivare a tanto ma si possono raggiungere ugualmente alcune finalità.

Parlate di settore, ma i profili professionali si riferiscono in realtà a molti settori.
In realtà, il settore di riferimento della sicurezza è formato da molteplici profili, ognuno con le proprie professionalità. Sarebbe stato riduttivo e poco utile riferirsi solo ai cosiddetti portieri o alle guardie giurate, piuttosto che agli steward. Se con il tempo emergerà l'esigenza, si potrà anche procedere a parcellizzare i vari profili ma sarà, comunque, solo un modo per ordinarli in modo differente perché restano parte di un unico mondo: la sicurezza, appunto.

In ultimo ma non ultimo, chi siete?
Dei giovani specialisti dell'HR a cui è stato chiesto di rispondere in modo concreto ad una esigenza specifica: sviluppare canali di reclutamento nuovi e dedicati, fare cultura del comparto per trovare e creare professionalità.

Job for Vigiles | Lavorare nel mondo della sicurezza

Contatto:
Sofia D'Arcangelo
Tel. +39 334 9853520
www.JobforVigiles.it
commerciale@secfm.it

Videocamere di sorveglianza e GDPR: come stare al passo con la legge

a cura di Cittadini dell'Ordine spa

Nel momento in cui installiamo delle videocamere di sorveglianza per proteggere le nostre proprietà, che siano esse di tipo domestico o commerciale, siamo tenuti a rispondere agli adempimenti richiesti dal Garante della Privacy in quanto andremo a registrare e conservare per periodi di tempo variabili i dati di individui a cui non possiamo richiedere il consenso personalmente.
La legge Italiana, infatti, vieta in modo esplicito di effettuare riprese in aree dove non vi sia stata previa segnalazione dell'operatività di sistemi di videosorveglianza.
Il requisito fondamentale richiesto è l'affissione del cartello di avviso di area videosorvegliata.
La sua mancata o errata affissione può conseguire in multe fino al valore di 36.000 euro, in quanto i cartelli devono seguire delle regole rigide che riguardano sia i contenuti (le informazioni scritte su di essi) che la loro posizione.

Contenuti a norma di legge
Per essere a norma, un cartello di avviso di area videosorvegliata deve riportare alcune informazioni obbligatorie:
• Il nome del titolare del trattamento dei dati, ovvero chi effettua la registrazione (nome dell'azienda o privato cittadino)
• La motivazione della sorveglianza
• Informativa sui diritti dei soggetti ripresi
• Informazioni sul trattamento delle immagini: se sono conservate e per quanto tempo, se vengono trasmesse a terzi (istituti di vigilanza, forze dell'ordine, ecc)
Queste informazioni sono definite di "primo livello".
Oltre alle informazioni di primo livello, deve esserci un chiaro riferimento ad una serie di informazioni definite di "secondo livello" e sul dove reperirle. Queste informazioni sono più tecniche e dettagliate, ma devono comunque

essere di facile accesso per l'interessato; potrebbero essere indicate tramite un link o un QRcode.

La posizione corretta di affissione
La funzione del cartello è di rispondere all'esigenza di tutela della privacy, per questo motivo la sua esposizione è obbligatoria e non può venire nascosto.
Per essere a norma rispetto al GDPR, i cartelli di avviso di area videosorvegliata devono essere collocati prima del raggio di azione delle telecamere. Non è pertanto ammesso posizionare un cartello che avvisi della presenza delle telecamere in un punto già soggetto al raggio d'azione delle stesse.

Attività commerciali e aziende
Attività commerciali, aziende e uffici possono installare videocamere di sorveglianza seguendo una procedura specifica. La possibilità di usufruire di sistemi di videosorveglianza è infatti consentita esclusivamente per soddisfare esigenze produttive, di sicurezza sul lavoro e di tutela del patrimonio aziendale.
I dipendenti dovranno firmare un'autorizzazione preventiva all'installazione dei sistemi di controllo dei lavoratori in caso questi siano installati per il monitoraggio della loro attività. Non è possibile controllare i dipendenti a loro insaputa.
Anche per quanto riguarda i contesti aziendali lavoratori, clienti, fornitori e chiunque acceda alla zona videosorvegliata dovrà essere avvisato preventivamente della presenza di telecamere tramite i cartelli.

Aree condominiali
Le aree condominiali rappresentano un'altra situazione particolare per la videosorveglianza.
La presenza di sistemi di videosorveglianza in questi contesti prevede che la maggioranza dei condomini sia favorevole all'installazione. Un singolo condomino può però decidere liberamente se dotare la propria abitazione internamente di un sistema protettivo.

Il duplice ruolo dei cartelli di avviso di area videosorvegliata
Oltre a seguire la normativa di legge, l'affissione del cartello di avviso di area videosorvegliata può svolgere la funzione di deterrente nei confronti dei malintenzionati che intendano introdursi nelle nostre proprietà, soprattutto quando dalle informazioni di primo livello si evince la presenza di un sistema di allarme di sicurezza avanzata con collegamento a centrale operativa.
Naturalmente, è da intendersi che non è sufficiente affiggere un cartello per considerarsi al sicuro. In caso di effrazione, infatti, nulla supera il collegamento diretto dei sistemi di allarme e videosorveglianza alle centrali operative, che mette in condizione gli operatori degli istituti di vigilanza di intervenire prontamente per proteggere i beni a rischio e allertare le forze dell'ordine.

Come scegliere il miglior sistema di videosorveglianza
Al giorno d'oggi la sicurezza personale è a portata di clic cosi come tanti altri prodotti acquistabili online, ma è importate tenere in considerazione che la sicurezza dei nostri beni non è un argomento da affrontare con leggerezza.
Solo per fare alcuni esempi, un'azienda di logistica con 300 dipendenti ha esigenze diverse da una farmacia con 6, cosi come un'abitazione singola fuori dal centro e un appartamento all'interno di un complesso condominiale vicino alla stazione.
Per questa ragione è fondamentale rivolgersi a degli esperti che possano ascoltare le vostre esigenze e costruire valutazioni di sicurezza personalizzate.

Cittadini dell'Ordine è il primo istituto di vigilanza fondato in Italia ed in Europa e da oltre 150 anni lavora per risolvere le esigenze dei suoi clienti. La nostra mission è unire tecnologie di ultima generazione per fornire servizi di sicurezza su misura. Per questo i nostri security manager sono sempre a disposizione per fornire valutazioni ad hoc.
Operiamo sulle aree metropolitane di **Torino e Milano** e nelle Province di **Bolzano, Trento, Verona, Cesena, Rimini e Ravenna**.

CDO A safe world
CDO 150 DAL 1870 VERSO IL FUTURO

Contatti:
Cittadini dell'Ordine S.p.A.
www.cittadinidellordine.com
contatti@cittadinidellordine.com

Il Gruppo COMET ha scelto le etichette elettroniche SOLUM fornite da Omnisint

a cura di Omnisint

Omnisint, azienda specializzata nell'implementazione di soluzioni tecnologiche altamente innovative per il mercato Retail, come partner di **SOLUM** fornisce prodotti e soluzioni per la digital signage, in particolare etichette elettroniche e segnaletica digitale interattiva.
Soprattutto nel settore dell'elettronica di consumo, in cui la velocità di inserimento promozioni o cambi prezzo nelle etichette dei prodotti sono fattori molto importanti, le soluzioni adottate devono essere sempre affidabili, rapide ed efficaci.
Abbiamo intervistato **Roberto Caprini**, responsabile dei sistemi informativi del gruppo **COMET**, per un approfondimento sulle etichette elettroniche SOLUM da loro scelte.

Può presentare la sua azienda?
Comet spa è un'azienda del territorio emiliano nata 50 anni fa da proprietari bolognesi e cresciuta negli anni in maniera esponenziale. il Gruppo Comet opera nella distribuzione di elettrodomestici, apparecchi per illuminazione e materiale elettrico con professionalità per offrire ai clienti la più alta qualità e competenza.
L'innovazione, il servizio al cliente, la dinamicità, lo spirito imprenditoriale e la coesione interna sono i valori che hanno consentito alla nostra azienda una crescita molto elevata, con una copertura territoriale tale da posizionarsi come azienda leader nel mondo della distribuzione.
Il Gruppo Comet è presente in 12 regioni sul territorio nazionale italiano con oltre 110 punti vendita, 3 magazzini centralizzati e oltre 2.000 collaboratori.

Perché avete scelto di passare alle etichette elettroniche?
Le aspettative del mercato e, di conseguenza, le esigenze aziendali interne stanno cambiando ed evolvendo nell'ultimo periodo. Sempre più aziende del nostro settore stanno trasformando i propri punti vendita, digitalizzando le operazioni in-store e permettendo ai clienti di interagire con i prodotti, principalmente attraverso display digitali. Oggi i clienti si aspettano un'esperienza d'acquisto moderna, digitale e personalizzata.
Le ESL consentono non solo di aggiornare i prezzi da remoto con un click e in tempo reale, diminuendo nettamente i tempi per la gestione dei cambi prezzo rispetto alle etichette cartacee ma, anche, di venire incontro ogni giorno alle esigenze dei consumatori, offrendo un servizio e una customer experience più evoluti.
Abbiamo quindi scelto di passare alle etichette elettroniche nei nostri punti vendita in quanto permettono un'esperienza migliore dal punto di vista del consumatore. I nostri negozi si stanno modernizzando, andando verso un'innovazione non solo più tecnologica ma anche ambientale, in quanto ora viene sprecata meno carta. La lunga durata delle batterie delle etichette elettroniche SOLUM permette un utilizzo a lungo termine dei componenti hardware.

Cosa ne pensa delle soluzioni SOLUM?
Le etichette elettroniche SOLUM sono robuste e si installano in maniera molto semplice, anche in negozi attivi già da qualche anno e, quindi, in strutture non nuove e digitalizzate. Dal punto di vista del software, si integrano facilmente con

la struttura esistente. Sono soluzioni tecnologicamente all'avanguardia la cui installazione avviene tramite un elettricista impiantista in pochi giorni; sono dispositivi che si connettono alla rete esistente e non necessitano di lavori di infrastruttura.
Siamo rimasti colpiti dalla qualità dei materiali, dalla resa dei display a livello di grafica e dei colori visualizzati e soprattutto dalla velocità di trasmissione dei dati.
Inoltre, grazie alla velocità di scambio dati e alla robustezza dell'interfacciamento con il sistema, possiamo pianificare aggiornamenti in tempo reale in tutti i negozi e ridurre i costi dell'infrastruttura senza compromettere la sicurezza dei dati.

Cosa vi ha spinto a scegliere Omnisint come partner tecnologico e le etichette elettroniche SOLUM?
SOLUM, come spin-off di Samsung, rappresenta un brand affermato con garanzia sui suoi prodotti, con un background di qualità e di leadership nello sviluppo tecnologico. Questo la rende senza dubbio un partner affidabile nella trasformazione digitale, in grado di fornire una soluzione realmente completa.
La nostra scelta è ricaduta su Omnisint dopo aver fatto una selezione tra i loro concorrenti. Ci sono piaciuti fin da subito perché la proprietà dell'azienda è esposta in prima persona: poiché anche in Comet la proprietà è familiare, e il rapporto umano gioca un ruolo fondamentale. Abbiamo scelto Omnsint perché si rispecchiava molto con la nostra filosofia.
Durante la fase di realizzazione del progetto, Omnisint ci ha permesso di lavorare in maniera serena e tranquilla sapendo di poter contare su un partner che risponde alle nostre esigenze e che ci segue all'interno del processo di realizzazione di questi impianti. Abbiamo trovato in loro il partner ideale che ci avrebbe garantito un'implementazione fluida e rapida di questa sofisticata tecnologia e una gestione controllata della complessità del progetto. In meno di 4 giorni tutte le etichette sono state correttamente posizionate e la soluzione era pronta all'uso.
Omnisint ha fornito supporto locale e formazione al nostro personale. Hanno ascoltato le nostre esigenze, personalizzando le soluzioni SOLUM e adattandole all'infrastruttura IT esistente.
La qualità dei prodotti che offrono, unitamente alla competenza mostrata, rendono la collaborazione con loro un'esperienza piacevole.

Come sfruttate le potenzialità della soluzione SOLUM nel vostro negozio?
La trasformazione digitale ci permette innanzitutto di abbandonare l'etichettatura manuale a scaffale e di aggiornare tutti i prezzi da remoto in tempo reale.
Questa soluzione ci aiuta anche a rafforzare la nostra brand identity, perché le etichette Newton possono essere personalizzate per includere il nostro nome, logo e colori, con una resa grafica eccellente.
Le ESL possono anche essere molto utili per creare promozioni in-store efficaci e più economiche, anzichè stampare sui soliti supporti cartacei.

Quali sono i benefici concreti che avete ottenuto dalla sua implementazione?
Da quando abbiamo introdotto la tecnologia ESL nei nostri punti vendita, abbiamo ottenuto risparmi ed ottimizzazioni in molte aree aziendali, dai costi di manodopera e di stampa al miglioramento dell'efficienza dello staff.
Stiamo sfruttando la tecnologia ESL di SOLUM per migliorare l'esperienza d'acquisto dei nostri clienti; vogliamo offrire il miglior servizio possibile e trasmettere i valori di trasparenza che contraddistinguono il nostro Gruppo. Fornire informazioni sempre corrette aiuta infatti a fidelizzare i clienti.
Inoltre, Omnisint ci ha offerto varie possibilità di utilizzo del software AIMS, centralizzato, local o in cloud.
In COMET abbiamo scelto di utilizzare la soluzione di software AIMS centralizzato perché ci permette di gestire dalla sede centrale il controllo su tutti i negozi. Gli aggiornamenti, anche programmati, sono garantiti grazie alla connettività tra il datacenter, dove risiede l'applicativo, e i gateways installati nei nostri punti vendita.
Le informazioni relative ad aggiornamenti vengono programmate a livello software nello scheduler di AIMS. Nel momento in cui le variazioni di prezzo iniziano ad avere validità, AIMS invia le informazioni ai gateways che poi, a loro volta, le trasmettono alle etichette, senza sprechi di tempo e senza errori.

Qual è il motivo principale per cui raccomanderebbe Omnisint e SOLUM ad altri retailer come partner e fornitore di ESL?
A mio parere, ciò che rende Omnisint e SOLUM i partner ideali per l'implementazione della soluzione ESL è la loro esperienza nella trasformazione digitale e l'orientamento alla soddisfazione del cliente.
Le caratteristiche tecniche delle ESL, come i pulsanti interattivi, la variazione dei colori del display a seconda dell'offerta in corso, la robustezza dell'hardware, la nitidezza del display con 3 colori fissi e l'eccezionale durata delle batterie ci ha portato a prediligere Omnisint e le ESL SOLUM rispetto ad altri brand.

GUARDA L'INTERVISTA A ROBERTO CAPRINI - CIO COMET SPA

Contatti:
Omnisint srl
Tel. +39 02 26708493
marketing@nedapretail.it

Vemcount: Footfall Analysis & Prediction

a cura di Omnisint

Omnisint presenta la piattaforma **Vemcount**, una piattaforma avanzata, modulare, flessibile e intuitiva.
La piattaforma **Vemcount** fornisce dati in tempo reale. Misura i flussi di varchi, corridoi, negozi, centri commerciali e tutti gli spazi strategici al fine di aumentarne performance e vendite. L'accurata tecnologia è l'elemento fondamentale per ottenere dati di alta qualità.

Le caratteristiche:
- Soluzione in Cloud hosted by Amazon
- Disponibile come soluzione cloud privata
- Accesso via browser on PC, Mac e smartphone
- Elaborazione di dati al 100 % anonimi, in linea con la normativa GDPR
- Soluzione Open Source

Integrazione Software:
- Integrazione con sistemi ERP e BI
- Export dati automatico via mail o FTP
- Completa integrazione via API

Vemco Group ha collaborato con aziende integrando le loro tecnologie con il software **Vemcount Analytics**.

Interfaccia di facile utilizzo:
- Dashboard user-friendly e personalizzabile
- Alert e notifiche in real-time
- Diversi livelli di utenza
- Widgets

Le soluzioni Vemcount coprono aree di qualsiasi dimensione e hanno la funzionalità di escludere fattori non necessari dai conteggi. Anche in condizioni difficili, Vemcount rileva le caratteristiche dei clienti con una precisione del 98%.

Come funziona?
Precisione: un sensore raccoglie i dati sul traffico dei visitatori con elevati livelli di precisione.
Tracciamento: il sensore viene posizionato all'interno o all'esterno, dove verrà misurato il traffico dei visitatori.
Risultati: Il nostro software Vemcount Analytics è integrato nel sensore della telecamera per confrontare i set di dati e generare approfondimenti automatici.

Ottieni il massimo dai sensori con Vemcount Analytics attraverso le funzionalità di:
- **People Counting**
- **Filtro altezza**
- **Tempo di permanenza**
- **Mappe di monitoraggio**
- **Livello di servizio**
- **Heatmaps**
- **Numero di veicoli**
- **Distribuzione di genere**
- **Esclusione del personale**

Contatti:
Omnisint
www.omnisint.it

RISCO presenta LightSYS+ il nuovo sistema di sicurezza ibrido

a cura di RISCO Group Italia

LightSYS+ è il nuovo sistema di sicurezza ibrido di **RISCO Group**, progettato per dare agli installatori un'efficienza superiore nella gestione di costi e tempi di installazione: è stata riprogettata per dare una singola piattaforma che gestisca installazioni di ogni tipo e dimensione, Grado 2 o Grado 3, dal momento che può gestire fino a 512 zone. Il sistema è ideale per il mercato residenziale di piccole e medie dimensioni ma è scalabile e può gestire anche ambienti commerciali, incluse infrastrutture critiche dove i requisiti in termini di sicurezza sono molto stringenti.

Un sistema che può crescere nel tempo

I benefici di **LightSYS+** includono la sua scalabilità nel tempo, cioè la capacità di poter facilmente crescere fino a 512 zone e, inoltre, permettere agli installatori di rendere più efficiente il magazzino riducendo i training necessari per apprendere il funzionamento del sistema, la cui logica è la stessa per tutte le installazioni da 0 fino a 512 zone.

LightSYS+ permette aggiornamenti del sistema nel tempo, oltre a fornire agli installatori delle reali possibilità di poter proporre miglioramenti al sistema grazie alla disponibilità di nuove soluzioni come, per esempio, l'integrazione con la tastiera touchscreen **RisControl**, vincitrice nella categoria "Innovazione tecnica dell'anno" ai PSI Award nel 2021, che a breve sarà disponibile in una versione che integra a bordo il nuovo gateway **Z-Wave** e avrà una nuova offerta di accessori smart, che permettono la creazione di scenari personalizzati per gli utenti finali, sempre gestiti da **iRISCO**.

La scheda madre della nuova **LightSYS+** è stata reingegnerizzata ed è ora ospitata in un guscio di plastica protettivo, progettato per minimizzare i rischi di danni all'hardware in fase di installazione. Questa progettazione della nuova centrale la rende più resistente anche nel tempo e semplice da installare.

I **moduli di comunicazione IP e Wi-Fi** sono già integrati nella centrale, per assicurare una connessione sempre disponibile a **RISCO Cloud**, anche per eventuali necessità di configurazione remota. Un modulo di comunicazione opzionale GSM 4G è altresì disponibile, sia come canale di comunicazione primario sia in backup agli altri canali a bordo, IP e Wi-Fi.

LightSYS+ dispone di box di vario tipo, selezionabili a seconda delle esigenze di installazione.

Altre caratteristiche sono la possibilità di aggiornamento del firmware tre volte più veloce, un'opzione di 'Presenza zona' che permette di inviare notifiche agli utenti quando il sistema non è inserito e la possibilità di utilizzare la verifica visive radio grazie a sensori con fotocamera supportati da una linea **FastBus**, che permette la trasmissione dei dati più veloce. Inoltre, un ingresso USB di tipo C permette una connessione più semplice e veloce in loco.

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

Hanwha Techwin presenta le telecamere della serie Wisenet X con capacità di intelligenza artificiale (AI) a bordo

a cura di Hanwha Techwin

Hanwha Techwin Europe ha introdotto una nuova gamma di telecamere della serie **Wisenet X** conformi all'NDAA con capacità di intelligenza artificiale (AI) integrate, con risoluzione da 2 MP, 6 MP e 4K. La nuova gamma di prodotti, che comprende 26 telecamere di diverse tipologie, amplia le opzioni a disposizione degli operatori che vogliono migliorare il proprio sistema di videosorveglianza con il Deep Learning, riducendo il numero di falsi allarmi e lavorando in maniera più efficiente. Le capacità AI a bordo aiutano gli operatori a rilevare elementi dell'immagine come persone, volti, veicoli e targhe, migliorare la qualità delle riprese e fornire dati di business intelligence.

Analisi video basata su AI Deep Learning

Grazie al Deep Learning, le telecamere riescono a soddisfare con maggiore facilità le esigenze operative in vari contesti ed in molteplici applicazioni. L'AI integrata nella gamma della serie X permette di gestire i contenuti video con maggiore facilità, comunicando agli operatori gli eventi quando necessario e consentendo loro di individuare gli eventi e gli oggetti rilevanti con rapidità mediante la ricerca forense, nonché di fornire una business intelligence più approfondita.

La capacità di rilevamento e classificazione degli oggetti permette agli operatori di identificare con rapidità le persone, i volti, le targhe e la tipologia di veicoli (auto, autocarri, autobus e biciclette), garantendo una maggiore consapevolezza della situazione e del contesto dell'evento. Movimenti irrilevanti come quelli dovuti ad alberi, ombre e animali che, con la tecnologia di rilevamento del movimento standard, sarebbero causa di falsi allarmi, vengono ignorati. Così gli operatori possono concentrarsi maggiormente sul fornire risposte a incidenti ed emergenze reali.

L'analisi basata sull'AI trova applicazione anche in ambiti differenti rispetto alla sicurezza, offrendo anche la possibilitá di rilevare un ventaglio di dati utili per applicazioni di Business Intelligence. Con il rilevamento degli oggetti basato su AI, le aziende possono ottenere informazioni relative a conteggi delle persone, dati sulla gestione delle code e heatmap accurate che mostrano modelli del comportamento dettagliati. La gamma offre anche il rilevamento delle intrusioni e dello stazionamento ed è completata dal supporto dei canali virtuali che consente agli operatori di registrare e monitorare contemporaneamente più aree specifiche di una scena oltre alla scena intera.

Immagini di qualità avanzata

In aggiunta a questo, la tecnologia di riduzione del rumore **WiseNRII** utilizza l'AI per identificare gli oggetti in movimento e ridurre la sfocatura in ambienti rumorosi e scarsamente illuminati. La tecnologia **Extreme WDR** sfrutta l'analisi della scena per ridurre gli artefatti di movimento fornendo immagini nitide anche in condizioni caratterizzate da elevata retroilluminazione, mentre **WiseIR** regola l'uscita dell'illuminazione a infrarossi sulla base dell'ingrandimento dello zoom della telecamera. **WiseStreamIII** riduce al minimo la larghezza di banda e lo spazio usato, ottimizzando la compressione dei dati e dei filmati. Ciò permette agli operatori di concentrarsi solo sugli oggetti e sulle aree che richiedono maggiore attenzione con una qualità delle immagini ottimale, una larghezza di banda ridotta al minimo e requisiti di spazio di archiviazione inferiori.

Durata maggiore per prestazioni costanti

La gamma offre opzioni di telecamera dome, dome antivandalo, bullet e box con ogni dispositivo dotato di parte esterna in metallo e, nel caso delle telecamere dome, rivestimenti a resistenza elevata. Ciò consente di prolungare la durata di ogni telecamera e assicura che le immagini non siano distorte da graffi sugli obiettivi. Una valvola consente la fuoriuscita del vapore acqueo prevenendo l'accumulo di umidità e il potenziale danneggiamento del dispositivo.

X-core e X-plus a confronto

La nuova gamma della serie X con funzioni AI è suddivisa in telecamere X-core e X-plus. La gamma X-plus offre un design modulare che semplifica di molto le operazioni di installazione, il supporto fino a 120 fps per un'acquisizione dei movimenti senza interruzioni, una maggiore efficienza dell'illuminazione IR.

Intelligenza Artificiale e Videosorveglianza

Uri Guterman, Head of Product & Marketing per **Hanwha Techwin Europe**, ha commentato il lancio della nuova gamma di telecamere serie X: *"L'analisi video basata su algoritmi AI Deep Learning sta assumendo un ruolo sempre più fondamentale per la sicurezza. Siamo particolarmente soddisfatti dei benefici che la nostra nuova gamma di telecamere puó portare agli utenti, contribuendo a ridurre il numero di falsi allarmi, a integrare la business intelligence basata sull'analisi a bordo camera e garantendo una qualità delle immagini ulteriormente migliorata. Tutto questo consente di rendere sempre piú efficenti le attivitá degli operatori, sia per la notifica di eventi in tempo reale che per la ricerca post-evento. Inoltre, é ora possibile valutare tutti i benefici portati dall' Intelligenza Artificiale in un ottica di ritorno dell'investimento piú breve e piú abbordabile per qualsiasi tipologia di utente. E' un passo in avanti importante, che anticipa il futuro del video nella sicurezza".*

Hanwha Techwin Europe

Contatti:
Hanwha Techwin Europe LTD
Tel. +39 02 36572 890
www.hanwha-security.eu/it

Cultura della legalità, fattore determinante per la sicurezza delle imprese

intervista al Gen. CC (r) Giuseppe Fausto Milillo Presidente Fondazione Legalità e Sviluppo

Possiamo fare una valutazione attuale sui timori di incremento delle infiltrazioni malavitose nell'economia reale a seguito della pandemia prima e dei fondi provenienti dal PNRR dopo?
La malavita vive di illegalità, violenze e terrore ed ancora di più si rafforza nei momenti di maggiore debolezza della società, delle imprese e del commercio.
La pandemia naturalmente ha creato delle grosse falle nel sistema economia-imprese, difficili ma comunque non impossibili a sanare. Nonostante gli ultimi governi abbiano dato dimostrazione di intervento, gli aiuti alle imprese e al commercio sono stati lenti e farraginosi e questo ha permesso facile inserimento della malavita, delle cosche, della criminalità dei colletti bianchi, pronti ad offrire ancor più facili prestiti e finanziamenti per poi, paladini dell'usura, diventare padroni delle loro vittime.
I fondi provenienti dal PNRR fanno gola a tutti, alla politica per gestirne il potere di distribuzione e gestione, e anche alla malavita, alle grandi cosche che, oltre al grande guadagno, sapranno bene riciclare il loro denaro e i loro loschi interessi.
Naturalmente le nostre forze di Polizia, primi in Europa, che già sanno come lottare le nuove mafie dell'economia PNRR, già sono scese validamente in campo per bloccare l'insistenza criminale e già molti sono stati i successi raggiunti a favore e a difesa delle imprese e del commercio.

Quali sono i settori economici e le aree geografiche più a rischio?
I ristoranti, i negozi, il turismo, il libero commercio, le aziende che in questo periodo hanno sofferto anche per colpa degli Istituti Bancari che non hanno agevolato prestiti e richieste, sono le vere vittime delle mafie che, come ho poc'anzi detto, sono state invece facilmente avvicinate

dalla criminalità, sempre pronta ad offrire denaro e aiuti. Il sud, naturalmente, la Lombardia e il Veneto stranamente, così come quasi tutte le grandi città d'Italia sono state e sono tuttora le aree geografiche più a rischio.

Dal vostro punto di osservazione, quale incidenza può avere un'adeguata informazione sui vantaggi per la sicurezza e la continuità aziendale derivanti dal rispetto di regole quali, ad esempio, la sicurezza sul lavoro, le normative anti riciclaggio e anti corruzione, ecc?
Informazione e innanzitutto cultura. Le aziende e le imprese devono sempre imporre la "Cultura della Sicurezza". La continuità aziendale va garantita solo con il rispetto delle regole che vanno a tutelare sia l'azienda che il datore di lavoro, oltre che il lavoratore. Le normative antiriciclaggio e anticorruzione possono sembrare esagerate ma in fin dei conti sono il "toccasana" per le attività da svolgere per la ricercata e dovuta economia di gran valore.

Quali sono in concreto le proposte della Fondazione che presiede per divulgare la consapevolezza su questi temi?
La Fondazione Italiana per la Legalità e lo Sviluppo con il Programma "Strade della Sicurezza e della Legalità, oggi e domani", fedele agli scopi e alle finalità statutarie, è attenta ed intende denunciare la forte influenza sull'economia imposta dal sistema criminale.
Bisogna formulare proposte per combattere la recessione e promuovere crescita e sviluppo. Si deve rafforzare ed affiancare l'operato dello Stato con nuove "sigle di intesa" appositamente ricercate a favore dei vari protocolli di Legalità, per rendere ancora più impermeabili le aziende e le imprese agli interessi delinquenziali.
Un programma improntato non solo su Legalità e rispetto dell'uomo e dell'ambiente, ma anche sulla Sicurezza.
In tale prospettiva verrà istituito un Osservatorio, oggetto di accordo di partecipazione con Federmanager Roma e Federmanager Napoli, molto attente alle problematiche in discussione, dal quale dovrà scaturire maggiore tutela all'operato sociale ed imprenditoriale, finanziario ed economico, nonché il massimo livello di cultura, informazione e protezione del mondo Security. E' giusto, quindi, predisporre e suggerire, con partner d'eccezione, a manager e alle aziende il miglior livello di formazione su business continuity, safety e security management, sicurezza sul lavoro, protezione aziendale, codici etici, travel risk management, trasparenza e processi aziendali e, non per ultimo, cyber security, oggi punto vitale non solo per la sicurezza nazionale ma anche per le imprese, per la singola persona e per la società tutta.
La presentazione del programma della Fondazione, che si terrà il **7 giugno al Campidoglio**, sarà l'occasione per dare corso alla nona edizione del Premio Legalità, che ha visto negli anni illustri nomi a ritirare il riconoscimento.
Il premio è dedicato a coloro che con le loro azioni, il loro impegno e le loro espressioni di alto spessore culturale hanno contribuito a tutelare e promuovere la Cultura della Legalità.

Quest'anno ritireranno i premi:
- Dott.ssa Valeria Grasso, da Palermo, imprenditrice e in atto sotto tutela, Delegata ai Rapporti Istituzionali presso il Ministero della Salute, per il **Premio "Donna Legalità"**;
- Avv. Maria Cristina Grillo, da Roma, libero professionista, fondatrice e Presidente Centro Ascolto SOS Violenza, per il **Premio "SOS Legalità"**;
- Avv. Rita Neri, da Roma, Responsabile e Direttrice Università e-Campus per il **Premio "Mondo Cultura"**;
- Avv. Prof. Gandolfo Maurizio Ballistreri, da Messina, Titolare cattedra di Diritto del Lavoro presso Università di Messina, per il **Premio "Lavoro Legalità"**;
- Gen. CC (r) Dott. Luciano Garofano, da Bologna, Generale dei CC in congedo già Comandante Ris, libero professionista, per il **Premio "Ricerca Legalità"**;
- Dott.ssa Cristina La Marca, da Napoli, imprenditrice, per il **Premio "Ambiente Impresa"**;
- Dott. Andrea Chittaro, da Milano, Responsabile Security Snam e Presidente AIPSA, per il **Premio "Sicurezza e Legalità"**;
- Dott. Max Laudadio, da Milano, Giornalista reporter d'inchiesta per "Striscia la Notizia", per il **Premio "Giornalismo Inchiesta Legalità"**;

Il Premio alla **"Carriera Legalità"** sarà assegnato al Dott. Guelfo Tagliavini, da Roma, Presidente di Tecnologie e Servizi Avanzati (Tesav) e Consigliere di Federmanager Roma.

Distribuzione di sicurezza, quali sono le chiavi del successo nel 2022?

intervista a Tiziano Mantello, founder e CEO di MT Distribuzione | a cura di Raffaello Juvara

Tiziano, nel continuo cambiamento del mercato della sicurezza, qual è secondo te il ruolo attuale del distributore di successo?
Oggi il mercato è in piena evoluzione, stiamo notando la continua acquisizione di realtà come la nostra azienda da parte di "magazzini" di materiale elettrico, ma le fusioni che a mio avviso meritano più attenzione sono quelle tra il settore elettrico e idraulico, segno che i due mondi per alcuni aspetti e prodotti legati alla domotica, stanno convergendo.
Con il mio staff abbiamo deciso di intraprendere la via dell'integrazione, formando e supportando gli operatori di settore nell'utilizzo di prodotti che interagiscono tra di loro per fornire soluzioni chiavi in mano adeguate alle sempre crescenti necessità del mercato della home & building automation.

Quando hai cominciato oltre 20 anni fa a costruire il "tuo" modello, su cosa hai fatto leva per raggiungere gli obiettivi che ti eri dato?
MT Distribuzione opera sul territorio oramai da 26 anni.
Una parte del "modello di business" su cui ho puntato per migliorarci costantemente ed ottenere i risultati che oggi abbiamo raggiunto, è proporci ai nostri clienti come veri partner, non solo come semplici distributori. Il partner, per definizione, è colui che ti accompagna e ti supporta lungo un percorso di vita, esattamente come ci sentiamo noi di MT Distribuzione quando uno qualsiasi dei nostri clienti ci chiede supporto per realizzare progetti più o meno complessi, dal pre-vendita al post-vendita.
Mi capita a volte di fare un riassunto degli anni trascorsi in questo mercato e mi ricordo quando andavo nelle fiere di settore e notavo i primi approcci da parte dei produttori al mondo dell'integrazione. Campeggiavano striscioni

enormi che riportavano payoff del tipo "Sistemi integrati per la sicurezza" o "Sistemi integrati per l'automazione" e allora mi chiedevo: "Ma l'installatore sarà pronto a questo cambiamento? Cosa posso fare per aiutarlo ad evolversi e migrare verso questo tipo di soluzioni?".
Da allora posso dire che una parte fondamentale della nostra missione è stata renderci partecipi del successo dei nostri clienti, ecco perché come anticipato prima, ci definiamo dei veri e propri partner.

Qualcuno ti ha accusato di seguire e supportare anche installatori inesperti. Se è vero, qual è il motivo?
Inutile negare. Si, sono stato accusato da alcuni operatori del settore di fornire troppa consulenza e formazione agli installatori meno "esperti" del settore. Amo farmi delle domande e amo darmi delle risposte, giuste o sbagliate che siano. Chiedendomi il perché di queste accuse, mi sono chiesto anche: "Ma se un insegnante venisse accusato dai genitori di fornire troppe informazioni o di seguire troppo i suoi alunni?". Mi sono risposto che io non sono geloso del mio sapere e metto volentieri a disposizione a chi mi da fiducia la mia struttura, formata da persone competenti e professionali, felici di aiutare chi ha voglia di imparare.

Cosa si deve fare per diventare un aggregatore riconosciuto dai "propri" installatori, come hai fatto tu? Quanto pensi influisca il fattore dell'appartenenza territoriale?
La prima cosa è essere coerenti e affamati di conoscenza, come disse Jobs.
Quando prendiamo in carico un cliente, gestiamo anche le sue problematiche lavorative e lo facciamo sempre con la massima dedizione. Ecco perché i clienti ci scelgono.
Credo che nel 2022 non si possa più parlare di vera e propria appartenenza territoriale.
Esempi come Amazon e Zalando hanno dimostrato che nell'era della tecnologia e della comunicazione immediata è la rapidità e la flessibilità che conta e che rende vincenti.
Già oggi siamo conosciuti e lavoriamo con molti installatori sparsi letteralmente in tutto il territorio italiano e non solo.

Da precursore dell'integrazione tra tecnologie diverse, secondo te i clienti finali oggi apprezzano i vantaggi di rivolgersi ad un unico fornitore per gli impianti del building?
Negli ultimi anni avere un unico fornitore per le soluzioni di building automation è diventata una costante. Chi meglio del tuo partner conosce quello che vuoi realizzare e sa fornirti la giusta soluzione tecnologica? Aiutiamo i nostri clienti nella scelta dei prodotti, oltre ad offrire loro supporto costante in fase di realizzazione.

E come può il distributore scendere direttamente in campo a fianco dei suoi installatori per trovare clienti, progettare impianti, coordinare i cantieri, ecc senza creare conflitti di interesse?
Non vorrei ripetermi, ma la parola "partner" per me ha un significato profondo e la fiducia reciproca è una delle colonne portanti che definiscono una partnership. Noi siamo PRO installatore e non CONTRO. Il nostro lavoro è quello di indirizzarli verso le novità anche al fine di farli crescere. Non vorremmo mai sostituirci al loro operato, non ne saremmo in grado e non è il nostro core business, ma soprattutto verrebbe a meno la fiducia e la stima che regola i nostri rapporti. Uscire nei cantieri con i nostri clienti per verificare insieme i lavori o le problematiche è per noi un vero privilegio perché significa che i clienti si fidano pienamente del nostro operato e della nostra consulenza.
Alcune realtà come la nostra stanno allestendo degli show-room appositamente strutturati, in modo che l'installatore possa portare in visita il proprio cliente finale così da potergli far toccare con mano le ultime tecnologie che poi verranno installare nella sua abitazione.
A mio avviso, questo è un esempio concreto di "coworking", lavorare insieme per ottenere un unico risultato.

MT DISTRIBUZIONE
distribuiamo per passione

Contatti:
MT Distribuzione Srl
www.mtdistribuzione.it

Premio H d'oro 2022: aperte le iscrizioni per partecipare alla sedicesima edizione

a cura della Fondazione Enzo Hruby

La **Fondazione Enzo Hruby** è lieta di comunicare che sono ufficialmente aperte le iscrizioni alla sedicesima edizione del **Premio H d'oro**, ed invita i professionisti della sicurezza e dell'integrazione dei sistemi a inviare le proprie candidature per partecipare a questo concorso così unico nel suo genere che premia le migliori realizzazioni di sicurezza e, con esse, la capacità degli operatori più qualificati di creare soluzioni su misura in grado di rispondere alle più specifiche esigenze espresse dalla committenza nei vari contesti pubblici e privati.
In questa edizione potranno essere presentati i progetti portati a termine nel corso dell'anno 2021, come sempre realizzati con qualsiasi tecnologia di sicurezza. Le candidature - opportunamente corredate da materiale documentario e iconografico che possa illustrare al meglio gli interventi realizzati – verranno valutate secondo i criteri che ispirano l'iniziativa da una Giuria esterna altamente qualificata, composta da personalità istituzionali, da rappresentanti dell'utenza finale, delle associazioni di settore e della stampa.

Il Premio H d'oro 2022 culminerà anche in questa edizione nella tradizionale cerimonia di premiazione dei vincitori e dei finalisti, che si svolgerà in autunno nell'ambito di un evento di grande fascino, prestigio e valore istituzionale, in un luogo altamente significativo del patrimonio culturale italiano.

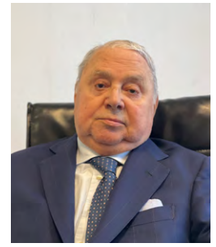
Per partecipare al Premio H d'oro 2022 è necessario presentare le candidature compilando l'apposito modulo scaricabile dal sito **www.accadoro.it**. Il modulo va poi riconsegnato alla Segreteria Organizzativa del Premio H d'oro all'indirizzo e-mail **info@fondazionehruby.org**.

Per ulteriori informazioni è possibile contattare la Segreteria Organizzativa al numero **02.38036625**.

F.P. Vigilanza, urge il rinnovo del CCNL per la crescita del comparto

intervista a Salvatore Stuppia, fondatore di F.P. Vigilanza

Ci può presentare F.P. Vigilanza, la sua storia, l'organizzazione?



Il progetto nasce circa 20 anni fa quando ho terminato il mio rapporto con la Polizia di Stato, in cui ho prestato servizio per oltre 40 anni fino a ricoprire il ruolo di Responsabile della Polizia Giudiziaria del Commissariato Montesacro Fidene fino alla pensione con il ruolo di Sostituto Commissario; non appena terminato il mio lavoro ho voluto dare un seguito a tutti questi anni continuando con le attività di vigilanza privata. Gli inizi non sono stati semplici, come in tutte le attività, ma la volontà di portare avanti questo progetto ci ha portato ad essere oggi una realtà consolidata. L'azienda è organizzata in 5 aree funzionali - commerciale, amministrazione, risorse umane, operativo e tecnico - che dipendono da un direttore generale che risponde direttamente al consiglio di amministrazione. E'una struttura molto snella, in grado di dare risposte immediate e non di perdersi nella burocrazia.
Un altro aspetto da sottolineare è lo spirito coeso all'interno dell'azienda fra tutte le funzioni, che ci ha permesso di raggiungere nell'ultimo biennio importanti risultati e di affermarci nel campo della vigilanza privata romana.

Quali sono i servizi principali che offrite, in quali aree ed a quali categorie di utilizzatori?
I servizi proposti sono quelli propri della vigilanza privata: presidi armati con guardie giurate altamente preparate e formate, televigilanza, telesorveglianza, pronto intervento su allarme, pattugliamento diurno e notturno, scorta valori. Questi sono i servizi principali che proponiamo a enti pubblici, ospedali, rappresentanze estere, grandi aziende. Per il settore retail e privati abbiamo previsto dei kit di allarme con tutti i servizi inclusi in un unico canone: centrale allarme e sensori, collegamento con la sala operativa e pronto intervento su allarme. Una formula che sta raccogliendo consensi proprio per la semplicità.

In base alla vostra esperienza, quali sono le maggiori criticità in questo momento per il mondo dei servizi di sicurezza?
Il settore della vigilanza privata sta vivendo un forte cambiamento con l'introduzione delle nuove tecnologie che richiedono una maggiore professionalità. Purtroppo, è un dato di fatto che il contratto collettivo di categoria è fermo dal 2015 e, con i livelli previsti nel contratto vigente, che sono molto bassi, si fa fatica a trovare personale che preferisce altri settori in cui riesce a guadagnare di più. Abbiamo visto nell'ultimo periodo una serie di agitazioni sindacali per cercare di sbloccare la situazione e fare in modo che governo e parti sociali si incontrino per il rinnovo del contratto, che è fondamentale per restare al passo con i tempi, in quanto viene richiesta una maggiore professionalità che è difficile avere con gli attuali livelli retributivi.

Cosa si dovrebbe fare per migliorare la situazione?
Innanzitutto, rinnovare il contratto prevedendo retribuzioni più alte in modo tale da poter selezionare risorse con una professionalità più elevata affinché si possa innalzare il livello del settore. Un livello più alto significa una qualità maggiore dei servizi che inquadrerebbe questa attività in maniera differente, permettendo anche di vedere il lavoro della guardia giurata come un'attività continuativa e stimolante, in grado di attrarre i giovani che si affacciano a questo mondo.

Addsecure IRIS-4 combinatore telefonico IP/4G EN 54-21 per allarmi incendio/guasto

ADDSECURE INTERNATIONAL AB
(+46) 20 32 20 00
(+39) 347 9977 838
www.addsecure.com

Alloggiabile all'interno del pannello allarmi incendio oppure nell'apposito contenitore anch'esso certificato

La serie IRIS-4 4 di combinatori telefonici rappresenta la soluzione "Swiss Knife" di AddSecure in quanto è adatta alla trasmissione di allarmi antifurto, antincendio e tecnici, o una combinazione di questi.
Caratterizzata dai più elevati criteri di sicurezza, unitamente alla semplicità e flessibilità operativa, la serie IRIS-4 4 prevede 3 possibili modelli:

- IRIS-4 400 trasmissione 4G a percorso singolo
- IRIS-4 420 trasmissione IP a percorso singolo
- IRIS-4 440 trasmissione a doppio percorso IP / 4G

Soluzione universale
Grazie all'ampia gamma di interfacce, la serie IRIS-4 4 è compatibile con tutti pannelli di controllo per allarmi esistenti, di qualsiasi costruttore.

- Connessione Dialport (PSTN emulata) con support di un' ampia gamma di protocolli analogici (Contact ID, SIA, Scancom Fast Format, CESA, Telim, Robofon)
- Connessioni RS-485, RS-232 e TTL bus
- Ingressi logici programmabili con messaggi di allarme e ripristino in protocollo SIA, Contact ID o messaggi di testo SMS
- CAN bus standard industriale per interfacciamento con sistemi HVAC/domotica e integrazione del sistema di allarme con soluzioni di Smart Building Management

Implementazione semplice e rapida
La serie IRIS-4 4 presenta di serie il rinomato touch screen IRIS che consente la programmazione e la messa in servizio in meno di 3 minuti con menu di configurazione interattivi che guidano rapidamente tutto il processo di installazione.
È possibile anche l'utilizzo della suite di software denominata IRIS Toolbox utilizzabile da personal computer collegato direttamente tramite porta USB.

ERMES presenta i citofoni bidirezionali conformi EN 62820

ERMES ELETTRONICA SRL
(+39) 0438 308470
www.ermes-cctv.com

Nella progettazione delle vie di esodo verticali, la normativa prescrive che siano previsti appositi locali, detti "Spazi Calmi", dove possano trovare rifugio le persone con ridotte capacità motorie in attesa di soccorsi.
Tra le attrezzature che sono obbligatoriamente prescritte per lo spazio calmo, è previsto un sistema di comunicazione audio bidirezionale che consenta alle persone bisognose di soccorso di segnalare la propria presenza agli operatori del posto presidiato di soccorso e, allo stesso tempo, consenta al personale di fornire assistenza in attesa dell'arrivo dei soccorsi per evitare situazioni di panico.
ERMES ha sviluppato per tale impiego una gamma di citofoni bidirezionali conformi alle norme **EN62820** che possono essere collegate su rete dati (collegamento in IP su LAN), in GSM o in LTE.
In particolare, gli apparati in IP utilizzano un protocollo di comunicazione peer-to-peer e si prefigurano come terminali stand alone collegati alla LAN direttamente senza la necessità di interfacce, unità ausiliarie o server di alcun tipo; il sistema, inoltre, è continuamente monitorato in modo da fornire in tempo reale una segnalazione di allarme in caso di anomalia.
Questi apparati sono alimentati in POE e, quindi, si prestano ad essere facilmente installati sia su una rete dati già esistente sia su un semplice switch autonomo in grado di fornire anche l'alimentazione di backup in caso di caduta della sorgente di alimentazione principale.

Marilyn More. Non servono altre parole

INIM ELECTRONICS S.R.L.
(+39) 0735 705007
www.inim.biz

Lasciati conquistare da **Marilyn More:** il nuovo sistema vocale domotico e antintrusione, ora con tecnologia **Smart Home**. Questo significa che ogni comando vocale viene subito riconosciuto dal tuo smart speaker Google Home o Amazon Echo. Senza dover apprendere codici linguistici specifici. In pratica, senza stress. Vuoi azionare le tapparelle, consultare il meteo, inserire il sistema d'allarme, o fare tutte e tre le cose insieme tramite routine automatiche? Basta dirlo. In più, puoi visualizzare e interagire con tutti i dispositivi dell'impianto attraverso smart display quali Amazon Echo Show e Google Nest Hub.
Marilyn More è basato sulle centrali Prime e Sol e integrato ai più diffusi smart speaker (Google Home e Amazon Echo) e smartphone. Grazie a **Marilyn More**, ogni comando vocale viene subito riconosciuto grazie alla tecnologia Smart Home e puoi interagire facilmente con il tuo sistema antintrusione/domotico INIM.
Marilyn More è un sistema flessibile ed estremamente semplice da configurare, che permette una rapida integrazione di tutti i dispositivi domotici della tua casa.
Comandare e supervisionare il tuo impianto antintrusione non è mai stato così semplice: è sufficiente associare il tuo account **INIM** a quello Google o Amazon ed il gioco è fatto. L'utente della centrale si interfaccia con il sistema utilizzando i comandi vocali, potendo così effettuare operazioni di gestione e supervisione sull'impianto.
Il sistema **Marilyn More** è accessorio al servizio Cloud di **INIM Electronics**. E' quindi necessario che l'utente abbia un proprio account presso il sito www.inimcloud.com, ed abbia registrate nel proprio profilo le centrali su cui vuole operare.

essecome ONLINE

n. 03/2022
Anno XLII
Periodico fondato da Paolo Tura

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

HANNO COLLABORATO A QUESTO NUMERO
Marco Censi, Gianluca Mauriello

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