essecome ONLINE 05/25

Periodico digitale di informazione di security & safety

2025 · ANNO XLV

CASSA CENTRALE BANCA
CREDITO COOPERATIVO ITALIANO

securindex.com

IA AL LAVORO IN BANCA

Opportunità, limiti e rischi nelle applicazioni no-core

26 settembre 2025

presso Cassa Centrale Banca
viale Pasubio, 21 - Milano

PROUDLY KOREAN

Hanwha Vision

Powering the next generation of video surveillance

Wisenet 9 System on Chip

- Highest performance with Dual Neural Processing Units
- Next–level image clarity to capture every detail
- Advanced AI for tailored solutions
- Remarkable efficiency – reduce bandwidth and storage needs
- Trusted cybersecurity – FIPS 140–3 Level 3

aisma

AISMA

Innovazione su misura

Sommario

Sicurezza privata, di cosa stiamo parlando?

Avvicinandosi la fiera SICUREZZA 2025, tradizionale momento di riflessione e di analisi delle condizioni del settore, ci troviamo ancora una volta a constatare quanto siano tra loro distanti le componenti più importanti, tecnologie e servizi, che dovrebbero invece integrarsi in un unico soggetto per rispondere alle richieste del mercato adeguandosi al modello di “sicurezza privata” consolidato e funzionante in tutto il mondo (tranne l’Italia).

Le imprese tecnologiche si presentano in ottima forma nei conti e nelle prospettive. A detta degli operatori, la domanda si è mantenuta sostenuta anche nel 2025 e nei prossimi anni dovrebbe continuare al traino della IA, diventata una componente irrinunciabile per qualsiasi applicazione, aprendo scenari intriganti sotto molteplici aspetti.

Invece le imprese di servizi di sicurezza arrivano in pessima forma, con i conti disastrati dagli aumenti del costo del lavoro e dalle difficoltà di adeguare le tariffe pagate dai clienti. La maggioranza degli imprenditori non ha investito in tecnologie e competenze per uscire dalla morsa tariffe/costo del lavoro e si trova senza prospettive e senza progetti davanti ai prossimi, inevitabili rinnovi contrattuali.

Di fatto, è in crisi la componente più voluminosa della sicurezza privata, con 150.000 lavoratori tra gpg e ausiliari non armati e un fatturato stimabile in 7 md di euro. Si delinea una dura selezione della specie che potrebbe riservare sorprese negli equilibri attualmente espressi dalle associazioni di categoria.

Un aspetto curioso di questa situazione è l’asimmetria tra gli assetti normativi e l’andamento delle due componenti: ipernormata la componente della vigilanza in crisi; senza norme specifiche quella tecnologica che si può muovere liberamente solo rispettando le regole generali d’impresa.

Facciamoci delle domande e diamoci le risposte ma non è forse un caso che la prima pensi ancora oggi di affidare al legislatore la soluzione dei propri problemi, ad esempio riesumando le tariffe amministrate mentre la seconda ben si guarda dal solo avvicinarsi al sistema politico/istituzionale.

Di fronte a questo scenario, viene da domandarsi che senso possa avere parlare di “riforma della sicurezza privata” che qualcuno vorrebbe affidare all’attuale maggioranza parlamentare, ritenuta sensibile al tema.

Il problema fondamentale è il committente: il TULPS è stato voluto “dall’alto” da un’Autorità governativa per rispondere ad una visione di sistema che voleva disporre di determinate risorse complementari alle forze dell’ordine per controllare il territorio e i cittadini in una particolare fase politica del Paese.

Come si presenta la situazione adesso, Il TULPS 2.0 verrebbe commissionato “dal basso” non per rispondere ad una nuova visione sistemica di un Governo che sembra lontano anni luce dal problema ma per difendere gli interessi di un ristretto gruppo di imprenditori, peraltro solo dei servizi perché c’è da scommettere che le imprese tecnologiche si chiamerebbero fuori.

E allora, di cosa stiamo parlando?

CASSA CENTRALE BANCA
CREDITO COOPERATIVO ITALIANO

securindex.com

IA AL LAVORO IN BANCA

Opportunità, limiti e rischi nelle applicazioni no-core

26 settembre 2025

presso Cassa Centrale Banca
viale Pasubio, 21 - Milano

Il seminario organizzato da securindex in collaborazione con Cassa Centrale Banca ha due obiettivi:

Condividere le esperienze di chi utilizza nel proprio lavoro la IA nei servizi non finanziarie;

Riflettere sulle opportunità, i limiti e i rischi dell'innovazione tecnologica più dirompente degli ultimi decenni.

9.30 **Apertura dei lavori - Introduzione al seminario**

9.45 **L'intelligenza artificiale al lavoro in banca. Opportunità, limiti e rischi nelle applicazioni no-core.**
conversazione condotta da Raffaello Juvara
con Federico Aguggini (Intesa Sanpaolo), Bruno Forti (psichiatra)

10.30 **Security e facility, le esperienze sul campo**
panel condotto da Pier Luigi Martusciello
con Alessio Bifarini (Poste Italiane), Stefano Piroddi (Cassa Centrale Banca),
Ferruccio Ravelli (Sparim - Sparkasse)

11.30 **Coffee break**

11.45 **Soluzioni eccellenti e buone pratiche**
panel condotto da Nils Fazzini
con i partner Hanwha Vision Europe, Neverhack Italy, AionTeam, AISMA

12.45 **Cosa ci aspettiamo nel futuro dalla IA - Conclusioni**

aionteam committed to your business · AISMA Research & Technology Center · Hanwha Vision · NEVERHACK · VIGILATE

FEDERICO AGUGGINI
He is currenty covering the role of Head of AI Transformation Office in Intesa Sanpaolo, a competence center for the development and management of Machine Learning & AI use cases in collaboration with the other Business Units. With the support of its team he takes care of the business needs by innovating technological architectures, assessing legal and ethical impacts and improving the knowledge of the "AI Culture" in the Bank.

BRUNO FORTI
Laureato in Medicina e Chirurgia, ha ottenuto nel 1990 la specializzazione in Psichiatria presso l'Università degli Studi di Trieste e nel 2006 il Dottorato di Ricerca (PhD) in Psichiatria presso la medesima Università. È stato docente presso la Scuola di Specializzazione in Psichiatria della Facoltà di Medicina dell'Università degli Studi di Trieste e presso il Corso di Laurea in Scienze dell'Educazione dell'Università degli Studi di Trieste. Ha partecipato a numerosi Congressi scientifici nazionali e internazionali in qualità di relatore e chairman.

LEONARDO LEONI - NEVERHACK
Professionista nel settore della cybersecurity e della data intelligence, guida lo sviluppo del mercato privato in Neverhack con focus su banche, assicurazioni e infrastrutture critiche. Vanta esperienza consulenziale in ambito strategico e tecnologico, con progetti che integrano intelligenza artificiale, threat intelligence e sicurezza fisica.

FRANCESCO PARADISO - HANWHA VISION
Ingegnere Informatico con più di 20 anni di esperienza nel settore IT e Security Technology. Attualmente Strategic Sales Manager in Hanwha Vision, sviluppa soluzioni per diversi mercati verticali supportando progettisti, system integrator ed end-user.

MATTEO PIAZZA - AION
Esperto in informatica e soluzioni software, prima di fondare aionteam nel 2016, ha maturato 18 anni di esperienza nello sviluppo di soluzioni software e it in svariati ambiti dagli erp alle soluzioni di governo delle infrastrutture, sino ad occuparsi di enterprise software architecture per grandi realtà enterprise.

STEFANO PIRODDI
Dopo un percorso nell'Arma dei Carabinieri concluso nel Raggruppamento Operativo Speciale, nel 2016 ha assunto il ruolo di CSO presso una delle aziende del gruppo Rheinmetall per approdare nel 2024 in Cassa Centrale, una realtà complessa e variegata con la peculiarità della vicinanza al territorio e alle persone, determinante nella scelta di abbracciare questa sfida professionale.

FERRUCCIO RAVELLI
Laureato nel 2001 in Economia e Commercio presso l'Università degli Studi di Trento, dal 2017 è Direttore presso Sparim SpA, Società di gestione del patrimonio immobiliare del Gruppo Cassa di Risparmio di Bolzano – Sparkasse e dal 2023 è Amministratore Unico presso Sparkasse Energy.

AMIR TOPALOVIC - AISMA
Professionista esperto di nuove soluzioni tecnologiche, transazioni digitali, intelligenza artificiale, finanza agevolata e formazione aziendale. Con un background tecnico (PhD) e finanziario avanzato (dottore commercialista), supporta imprese e startup nell'adozione di soluzioni innovative basate su AI per ottimizzare processi digitali attraverso il paradigma data driven e massimizzare le opportunità di finanziamento agevolato.

CASSA CENTRALE BANCA
CREDITO COOPERATIVO ITALIANO

securindex.com

IA al lavoro in banca: la videosorveglianza secondo Hanwha Vision

intervista a Francesco Paradiso, Strategic Sales Manager Hanwha Vision Europe Ltd | Computer Engineering

La videosorveglianza è un ambito tipico per applicazioni IA. In linea generale, quali sono i principali vantaggi / svantaggi per l'utente banca consolidati a tutt'oggi? E quali potrebbero essere i prossimi, tenendo conto della velocità dello sviluppo della IA?

L'introduzione dell'intelligenza artificiale nella videosorveglianza bancaria ha portato vantaggi significativi. Il primo è la riduzione dei falsi allarmi, grazie a funzioni di deep-learning che filtrano rumori, ombre o foglie in movimento e segnalano solo eventi realmente anomali. Questo migliora l'efficienza degli operatori e consente risposte più rapide. Un secondo vantaggio è la maggiore percezione di sicurezza dei clienti che sente più sicuro quando vede telecamere attive nelle filiali e agli sportelli ATM.

L'IA supporta anche l'efficienza operativa: analisi delle code, gestione dei flussi e monitoraggio dell'occupazione degli spazi consentono di migliorare l'esperienza dei clienti e ridurre i tempi di attesa.

Gli svantaggi riguardano principalmente l'adozione tecnologica: l'IA richiede politiche di compliance solide (privacy, GDPR, AI Act) e formazione del personale. Inoltre, la rapida evoluzione degli algoritmi può creare complessità negli aggiornamenti.

Guardando avanti, i sistemi diventeranno sempre più intelligenti supportando modelli di risk management integrato tra sicurezza fisica e cyber.

Con quale impostazione Hanwha Vision sta sviluppando le integrazioni di IA nella propria gamma di prodotti?

L'approccio Hanwha Vision è basato su due importanti pilastri: edge AI e cybersecurity by design.

Edge AI: la maggior parte delle nostre telecamere integra analisi video e audio direttamente a bordo, senza necessità di server esterni. Questo riduce il traffico dati, accelera le risposte e protegge meglio le informazioni sensibili.

End-to-end cybersecurity: le nostre soluzioni sono progettate "security by design", con certificazioni a standard riconosciuti a livello internazionale.

Hanwha Vision adotta strumenti e metodologie come:

- CVE (Common Vulnerabilities and Exposures) per la gestione proattiva delle vulnerabilità;
- IEC 62443 per la sicurezza dei sistemi di automazione e controllo industriale;
- ISO 27001 per la gestione della sicurezza delle informazioni;
- FIPS (Federal Information Processing Standards) per la crittografia avanzata;
- TPM (Trusted Platform Module) per la protezione hardware delle chiavi crittografiche.

In questo modo offriamo alle banche una protezione completa che copre l'intera catena del valore, dal dispositivo al sistema centrale, assicurando compliance con GDPR, AI Act e NIS2. Questo approccio garantisce che l'adozione dell'IA non comprometta la sicurezza, requisito fondamentale per il mondo bancario.

Quali sono le vostre linee di prodotti con IA di maggiore utilizzabilità in ambito bancario?

Hanwha Vision propone diverse soluzioni che coprono i casi d'uso principali: dalla protezione degli ATM alla gestione di filiali e data center.

- ATM Camera: soluzioni specifiche con telecamere progettate per integrarsi nei bancomat e catturare immagini nitide anche in condizioni di scarsa illuminazione. Consentono di identificare chiaramente utenti e potenziali manomissioni.
- La nuova Serie AI X e multi-sensore: ideali per la copertura di intere filiali con un minor numero di dispositivi, grazie a visione a 360° e algoritmi di analisi avanzati.
- AI analytics: funzioni come rilevamento volto, loitering detection, intrusion detection, virtual line crossing, appaiono dispari detection. L'integrazione di audio analytics consente di rilevare suoni critici come urla, spari o vetri infranti.
- Soluzioni VMS e NVR Wisenet WAVE: pensate per gestire in maniera semplice ed efficiente sia piccoli impianti che architetture distribuite, integrando telecamere AI per ricerche forensi rapide.

Per quali applicazioni sono maggiormente richieste o sono da voi proposte per gli utenti del mondo bancario?

Proponiamo diverse applicazioni che coprono sia le esigenze di sicurezza fisica sia quelle di customer experience e ottimizzazione operativa.

- ATM Security: sistemi discreti per contrastare frodi e manomissioni, con telecamere dedicate e funzioni audio per scoraggiare comportamenti sospetti.
- Queue Management e Occupancy Monitoring: analisi video per ridurre i tempi di attesa e monitorare l'affluenza nelle filiali, supportando anche la conformità alle policy ESG.
- Intrusion & Loitering Detection: monitoraggio in tempo reale di aree sensibili, sale server e caveau, con avvisi immediati per ridurre i tempi di risposta.
- Car Park Management: soluzioni ANPR e riconoscimento veicoli (marca, modello, colore, targa) per controllare accessi e aree di parcheggio di sedi centrali e direzionali.
- Cybersecure Surveillance: garanzia che tutti i dispositivi rispettino standard di protezione e cifratura end-to-end, requisito cruciale per le banche.

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

IA al lavoro in banca: YABE, la piattaforma full-stack by AION Team

intervista a Matteo Piazza, CEO e CTO presso AION Team

Ci può parlare di Aion, chi siete e qual è la vostra mission?
Aion è una software house nata con l'obiettivo di rendere l'Intelligenza Artificiale e l'automazione realmente accessibili alle aziende, grandi o piccole. La nostra mission è creare soluzioni che non richiedano codice e che permettano a business analyst, operation manager e tecnici di lavorare insieme, riducendo complessità e costi. In poche parole: democratizziamo la AI e l'automazione, offrendo strumenti potenti ma facili da usare.

Yabe è il vostro prodotto di punta, quali sono le principali caratteristiche e cosa lo rende unico nel suo genere?
Yabe è la nostra piattaforma full-stack che integra quattro motori in un unico ambiente: Analytics, Automation, Artificial Intelligence, Data Ingestion.
Quello che la rende unica è la convergenza: dove oggi le aziende usano diversi strumenti (BI, RPA, ETL, AI separati), Yabe unisce tutto in un'unica soluzione no-code. Inoltre, gestisce in modo intelligente l'uso delle GPU con un routing dinamico che incrocia logiche tecniche e di business, garantendo performance, resilienza e compliance normativa (in primis l'AI Act europeo).

In un contesto complesso come quello bancario è evidente che l'applicazione della AI può trovare terreno fertile se applicato in diverse aree al fine di migliorare e automatizzare vari processi. Con Yabe voi offrite al mercato un approccio leggermente diverso ma estremamente più proficuo, potete parlarne?
Il settore bancario è un ottimo esempio: la AI non può essere un "pezzo isolato", ma deve inserirsi in processi critici, governati e spesso regolamentati.
Con Yabe portiamo un approccio diverso: non proponiamo solo modelli di AI, ma un AI Fabric completo che unisce dati, automazione e intelligenza artificiale in un'unica regia. Questo significa che la banca può gestire non solo il calcolo o l'analisi, ma anche quando e come allocare risorse (ad esempio GPU o priorità di calcolo) in base a logiche di business, orari, SLA e periodi critici. In questo modo si ha AI utile e governata, che non è mai un collo di bottiglia ma un fattore di vantaggio competitivo.

Un esempio concreto è Illimity Bank, nostro importante cliente, che utilizza Yabe per automatizzare processi di core banking che coinvolgono simultaneamente più piattaforme. Grazie alla combinazione dei nostri strumenti di Digital Automation, Robotic Process Automation e modelli di Intelligenza Artificiale per l'analisi documentale, la banca ha potuto digitalizzare e rendere completamente automatici flussi complessi che spaziano dal retail alla compliance, fino al finance e all'antiriciclaggio.

Cito alcuni dei processi su cui abbiamo applicato con successo Yabe:
- **Onboarding clienti** (riconoscimento in tempo reale documenti e apertura posizione integrata con banking online)
- **Apertura conto corrente** (verifica accredito o video selfie, controlli AML/KYC, apertura effettiva conto)
- **KYC** (raccolta multicanale, validazione automatica, aggiornamento posizione, invio e solleciti periodici)
- **Segnalazioni SOS** (raccolta dati per l'indagine quali movimenti significativi, soggetti collegati e controparti, compilazione schede antiriciclaggio)
- **Checklist carte di credito** (raccolta dati, calcolo punteggio creditizio, creazione relazione per valutazione finale)
- **Contabilizzazione sospesi** (gestione automatica operazioni non andate a buon fine con solleciti multicanale)
- **Censimento controparti istituzionali** (integrazione documenti ufficiali e aggiornamento anagrafiche)
- **Chiusura codici Internet Banking** (blocco accessi per conti estinti)
- **Controlli Open Banking** (verifica automatica coerenza dati censiti e PDF)
- **Conservazione sostitutiva contratti** (archiviazione digitale conforme di contratti e questionari AML)
- **Controlli normativa transazioni** (MAV, RAV, SDD con motivazione automatica di mancati addebiti/pagamenti)
- **Trasferimento servizi bancari** (automazione pratiche di migrazione clienti tra istituti)
- **Autorizzazione bonifici** >30k (validazione automatica secondo parametri predefiniti)
- **Bonifici urgenti** (evasione ticket e normalizzazione commissioni)
- **Automazione schede GIANOS** (creazione e aggiornamento schede con note e giudizio sintetico per clienti a rischio)
- **Flag VIP e recall** (assegnazione priorità e gestione notifiche su richieste di restituzione fondi)

Inoltre, sempre con Yabe, Illimity misura e monitora in tempo reale la qualità dei servizi digitalizzati, garantendo efficienza, affidabilità e pieno controllo.

Come vede il futuro delle aziende, in questo caso banche, che cercano di approfittare di questa rivoluzione tecnologica? Quali opportunità si presentano?
Crediamo che il futuro appartenga alle aziende che sapranno integrare la AI nei processi reali, senza trattarla come un progetto a sé stante.
Per le banche significa maggiore efficienza operativa, minori costi, ma anche più trasparenza e compliance, aspetti fondamentali in questo settore. Le opportunità sono enormi: dall'automazione documentale al supporto ai processi di riconciliazione, fino alla possibilità di offrire servizi più rapidi e personalizzati ai clienti.
Chi riuscirà a sfruttare la AI in modo scalabile, sicuro e governato, avrà un vantaggio competitivo difficile da colmare.

yabe aionteam

Contatti:
AION Team
info@aionteam.it
www.aionteam.it

IA al lavoro in banca: il contributo strategico di AISMA

intervista a Dott. PHD Amir Topalovic – CEO AISMA Srl

AISMA è nuova nel settore bancario, ci parli della sua azienda.
AISMA è una società di ricerca e sviluppo dedicata all'applicazione dell'Intelligenza Artificiale nei processi complessi delle organizzazioni. Nata come centro di competenza tecnologica, AISMA unisce la conoscenza accademica con l'esperienza sul campo per creare soluzioni di automazione intelligenti, sicure e spiegabili. La nostra missione è mettere l'AI al servizio delle imprese, costruendo modelli che non siano "black box", ma strumenti trasparenti, certificabili e in grado di generare valore misurabile. Dopo aver consolidato importanti esperienze nel mondo legale, ci stiamo aprendo al settore bancario, dove vediamo enormi opportunità di applicazione.

Una fucina di talenti e molti progetti innovativi sono la caratteristica principale dell'azienda. Quali sono le aree più importanti che presidiate?
La nostra organizzazione lavora come un laboratorio distribuito di competenze. Siamo estremamente specializzati in quattro aree strategiche:
• **Artificial Intelligence:** sviluppo di modelli avanzati di machine learning, NLP e computer vision per trasformare dati complessi in soluzioni intelligenti;
• **Data Lake:** progettazione di architetture scalabili per unificare e centralizzare i dati aziendali;
• **Data Science:** dalla raccolta alla visualizzazione, estraiamo valore dai dati per supportare decisioni rapide e informate;
• **Data-Driven Applications:** creiamo applicazioni web e software custom, integrando AI e dati fin dalla fase di design;
Dal punto di vista delle soluzioni per le quali partecipiamo all'evento, abbiamo tre aree specifiche che abbiamo sviluppato:

• **Ricerca AI & Explainability:** sviluppiamo modelli basati su reasoning certificabile con validazione integrata (Validation Gate, Evidence Chains, Reasoning Certificate), per garantire la massima affidabilità.
• **Automazione documentale e processi legali:** partendo da LegalDraft, il nostro prodotto core, realizziamo piattaforme in grado di generare documenti difendibili e auditabili.
• **Integrazione enterprise:** API, plugin e connettori che permettono di innestare le nostre soluzioni all'interno di sistemi legacy o di ambienti mission critical come quelli bancari.

Il settore finanziario rappresenta uno dei mercati più importanti per l'AI. In quali aree ritenete di portare il vostro contributo?
Le banche sono sistemi complessi, con esigenze trasversali. Riteniamo che AISMA possa avere un impatto significativo in quattro ambiti:
• **Legal interno:** supporto agli uffici legali nella redazione di pareri e contratti, riducendo tempi e costi senza rinunciare a tracciabilità e difendibilità;
• **HR e Diritto del Lavoro:** partendo dal dominio in cui il nostro modello è già maturo, possiamo assistere le direzioni HR nella gestione dei rapporti di lavoro e nei contenziosi;
• **Compliance e risk management:** sistemi capaci di generare documentazione connessa a evidenze verificabili, in linea con le nuove regolamentazioni (es. NIS2, AI Act).
• **Procurement:** automazione nella revisione e preparazione di contratti e bandi, con analisi comparativa e identificazione automatica delle clausole critiche.

L'automazione in ambito legal è una sfida importante. Come approcciate tecnicamente questa area?
Il nostro approccio parte da una pipeline brevettata: ingestion e indicizzazione dei documenti interni, riconoscimento delle issue tramite motore ibrido (FAISS + BM25), costruzione di catene argomentative, generazione automatica della bozza e validazione semantica. Ogni output è accompagnato da un "reasoning certificate" che consente di dimostrare su quali evidenze si fonda il parere o il documento generato. Questo approccio — evidence-first e domain-specific — ci differenzia dai sistemi generalisti e ci rende particolarmente adatti ad ambiti regolati e ad alta responsabilità come quello bancario.

Il futuro è oggi. Domani come cambieranno le grandi organizzazioni?
Le grandi organizzazioni diventeranno sempre più ecosistemi cognitivi, in cui l'AI non sostituirà le persone, ma le accompagnerà nelle decisioni complesse. La sfida sarà duplice: da un lato governare l'AI con regole chiare e sistemi trasparenti, dall'altro saper trasformare la cultura aziendale affinché l'automazione diventi un abilitatore di crescita e non un vincolo. Le banche, in particolare, potranno beneficiare di una nuova efficienza nei processi di compliance, legal e risk management, liberando tempo e risorse da dedicare al cliente e all'innovazione. AISMA è pronta a essere un partner in questo percorso, mettendo a disposizione le proprie soluzioni di intelligenza artificiale certificabile e i propri talenti.

AISMA
Research & Technology Center

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

IA al lavoro in banca: il modello integrato di Neverhack

intervista a Leonardo Leoni, Head of Private Market Sales di Neverhack

Quali applicazioni di IA avete introdotto nella vostra gamma di sistemi che possono venire utilizzati da realtà bancarie per i servizi di facility e security?
In Neverhack abbiamo introdotto diverse soluzioni di intelligenza artificiale pensate per il settore bancario. Parliamo di algoritmi capaci di rilevare anomalie e potenziali minacce informatiche, sistemi di computer vision che analizzano in tempo reale i flussi delle telecamere di sicurezza, piattaforme di intelligence che incrociano dati da fonti interne ed esterne, fino a modelli predittivi per ottimizzare la gestione energetica e la manutenzione degli impianti critici. L'obiettivo è avere un'unica regia che colleghi sicurezza logica, fisica e facility.

Può descrivere in breve le prestazioni di sistemi con IA?
Le prestazioni si misurano soprattutto in tre aree: velocità, precisione e scalabilità. L'IA riduce drasticamente i tempi di rilevamento di un incidente, filtra i falsi positivi che spesso affollano i centri operativi e, grazie a infrastrutture cloud-native, riesce a servire dalla singola filiale fino a reti bancarie distribuite a livello internazionale.

Quali sono, dal vostro punto di osservazione, i principali vantaggi/svantaggi per l'utente banca consolidati a tutt'oggi?
I vantaggi più evidenti sono una maggiore capacità di prevenire minacce complesse, l'ottimizzazione dei costi operativi e la possibilità di avere un unico quadro integrato per sicurezza e facility. Per contro, restano due sfide: la necessità di investire inizialmente in addestramento e tuning dei sistemi, e quella di far crescere competenze interne capaci di governare la tecnologia.

Per quali applicazioni sono maggiormente richieste o sono da voi proposte per gli utenti del mondo bancario?
Oggi le banche ci chiedono soprattutto soluzioni di cyber threat intelligence integrata con la sicurezza fisica, automazione dei processi di risposta agli incidenti, sistemi antifrode basati su rilevamento di anomalie e computer vision per il controllo accessi. Parallelamente cresce l'interesse per applicazioni di manutenzione predittiva che assicurino continuità operativa nelle filiali e nei data center.

Guardando al futuro, come vede Neverhack l'evoluzione della sicurezza in banca con l'arrivo dell'intelligenza artificiale?
Il futuro della sicurezza bancaria sarà sempre più nell'integrazione tra uomo, dati e intelligenza artificiale. L'IA non sostituirà la capacità decisionale delle persone, ma diventerà un alleato strategico capace di analizzare enormi volumi di informazioni, collegare segnali deboli e supportare scelte rapide in contesti complessi. Le banche che sapranno unire tecnologia e cultura della sicurezza avranno un vantaggio competitivo decisivo, sia in termini di protezione sia di efficienza operativa

NEVERHACK

Contatti:
Neverhack Italy
www.neverhack.com

NEVERHACK

Your cyber performance partner

Let's make cybersecurity a strength for your business. We're here to help with everything from risk management and compliance to training and continuous monitoring, ensuring your growth is always protected.

WWW.NEVERHACK.COM

“IA al lavoro in banca”: l’ecosistema Suite Team di Vigilate

intervista a Stefano Gosetti, Vicepresidente Vigilate srl

Quali applicazioni di IA avete introdotto nella vostra gamma di sistemi che possono venire utilizzati da realtà bancarie per i servizi di facility e security?
Vigilate ha sviluppato un ecosistema “AI-first” chiamato Suite Team, una rete di agenti intelligenti progettati per automatizzare e migliorare la gestione di sicurezza, traffico e impianti in ambienti complessi – tra cui rientrano a pieno titolo le sedi bancarie e i loro ecosistemi infrastrutturali. A differenza delle tradizionali piattaforme di monitoraggio, Suite Team non si limita a mostrare informazioni ma interpreta, decide e agisce.
Per il settore bancario, questo si traduce nell’introduzione di agenti verticali specializzati nella gestione degli allarmi di sicurezza fisica (Agente Security), nel controllo accessi, nella supervisione degli impianti critici (Agente Building), e nella gestione della manutenzione predittiva. Tutti questi moduli collaborano con agenti orizzontali di orchestrazione, notifiche, linguaggio naturale e reportistica.
L’intero sistema può essere installato in cloud, on-premise o in configurazione ibrida, garantendo così compliance normativa e massima flessibilità.

Può descrivere in breve le prestazioni di sistemi con IA?
Gli agenti AI integrati in Suite Team analizzano dati provenienti da telecamere, sensori, sistemi antintrusione, accessi, impiantistica di vario genere e altri dispositivi IoT, valutando in tempo reale la rilevanza degli eventi rilevati e attivando azioni coerenti con le procedure definite dall’ente bancario.
Ad esempio, l’Agente Security è in grado di distinguere tra un falso allarme e una minaccia reale, attivando autonomamente la notifica verso un operatore o la vigilanza, avviando il blocco di accessi o accendendo dispositivi di dissuasione, con tempi di reazione nell’ordine dei millisecondi. Il tutto documentato da un audit trail dettagliato.

L’AI non si limita alla reattività: grazie alla memoria contestuale e all’apprendimento continuo basato sul feedback degli operatori, gli agenti migliorano progressivamente le proprie prestazioni, adattandosi al comportamento reale degli impianti e degli utenti.

Quali sono, dal vostro punto di osservazione, i principali vantaggi /svantaggi per l’utente banca consolidati a tutt’oggi?
I principali vantaggi osservati nell’adozione di Suite Team da parte di realtà bancarie e istituti affini sono molteplici:

- **Riduzione del carico cognitivo** per gli operatori, con minore stress e maggiore affidabilità nelle decisioni.
- **Diminuzione dei falsi allarmi**, grazie alla correlazione multisensore e all’analisi contestuale.
- **Reattività H24 senza interruzioni**, con escalation automatizzate verso le figure competenti.
- **Risparmio operativo**, grazie all’automazione di attività ripetitive e al contenimento delle risorse necessarie in control room.
- **Auditabilità e compliance** garantite da logging dettagliato, rispetto delle policy aziendali e integrabilità con i sistemi di auditing interno.

Tra i potenziali svantaggi iniziali vi è il naturale bisogno di allineare le procedure operative alle logiche degli agenti, richiedendo una fase di co-progettazione e configurazione iniziale. Tuttavia, il nostro framework prevede una personalizzazione completa degli agenti per ciascun impianto o cliente, minimizzando l’attrito operativo.

Per quali applicazioni sono maggiormente richieste o sono da voi proposte per gli utenti del mondo bancario?
Nel mondo bancario le richieste principali si concentrano su:
- **Supervisione proattiva degli allarmi:** l’agente AI valuta ogni segnalazione tecnica o comportamentale secondo parametri dinamici (tipo area, orario, storico) e attiva escalation automatiche in caso di minacce verificate.
- **Controllo accessi intelligente:** analisi comportamentale su badge e varchi, rilevamento di forzature o usi anomali, integrazione con il sistema di videosorveglianza per validazione incrociata.
- **Monitoraggio energetico e ambientale:** nei centri direzionali o agenzie, Suite Team consente di ottimizzare consumi elettrici e impianti HVAC attraverso il rilevamento di anomalie e suggerimenti predittivi.
- **Gestione della manutenzione predittiva:** l’agente identifica pattern di guasto su impianti critici e apre ticket automatici verso le squadre manutentive.
- **Interfaccia conversazionale per gli operatori:** grazie al modulo NLP, il personale può dialogare con gli agenti come farebbe con un collega esperto, richiedendo report, verifiche o attivazioni anche in mobilità.

In sintesi, Suite Team rappresenta per il mondo bancario un alleato strategico per affrontare le nuove sfide legate a sicurezza, efficienza operativa e digitalizzazione dei processi. L’integrazione AI non è più una promessa: è oggi una realtà concreta, già in fase di implementazione con partner del settore finance.

VIGILATE

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

Competenza, esperienza e convinzione del team Sesami

interviste a Federica Brambilla, VP Business Development EMEA per Sesami, Serena Bollati, Senior BD Manager in Sesami Cash Management Technologies Silvia Comolli, Senior Sales BD Executive Retail, Fashion & Luxury | FinTech & Payments in Sesami Cash Management Technologies

FEDERICA BRAMBILLA

Ci può raccontare il percorso professionale che l'ha portata ad assumere l'incarico di VP Business Development EMEA per Sesami?
Il mio percorso professionale ha avuto inizio in una scuola di business a Milano, con il ruolo di Product manager del prodotto formazione per le Banche Retail, esperienza che mi ha consentito di approfondire le tematiche inerenti ai prodotti e soluzioni riconducibili all'area fidi, titoli/investimenti, carte e politiche marketing e commerciali, rivolte ai segmenti di clientela privati e small-medium business proseguendo poi in una società di ricerche di marketing per il settore bancario che si occupava anche della preparazione di piani per l'apertura delle nuove filiali. Ho poi lavorato in multinazionali focalizzate sulla tecnologia abilitante per l'ottimizzazione della rete di sportelli e dei processi legati al ciclo del contante, con l'inserimento degli ATM e della gestione delle transazioni storicamente effettuate agli sportelli delle agenzie. Con l'inserimento dell'automazione sostenuta da cambiamenti organizzativi, le operazioni di sportello venivano gradualmente trasferite sui bancomat spesso fuori dall'agenzia in aree self service e sui TCR/apparecchiature di ricircolo per le operazioni di contanti lasciando più tempo agli operatori di filiale. Queste esperienze maturate in Italia e all'estero, sia Europa che negli USA (mi sono infatti trasferita e ho lavorato per due anni negli Stati Uniti gestendo una delle banche leader americane), mi hanno consentito di esplorare, insieme ai clienti su svariati progetti, tutte le componenti dell'eco sistema contante, aiutando gli istituti bancari a trovare il giusto mix di automazione, aspetti organizzativi e procedurali per sviluppare il business, ottimizzare processi e costi della supply chain con un approccio di collaborazione, indispensabile in ambienti complessi. Negli anni credo che la varietà delle banche con cui ho avuto l'onore di lavorare a livello domestico e internazionale, unito alla molteplicità dei progetti seguiti, abbia contribuito ad ampliare ed approfondire le mie conoscenze, acquisendo dimestichezza in un mercato sfidante, caratterizzato da orizzonti competitivi dinamici, frequenti progetti di cambiamento strategici e organizzativi, che richiedono agilità e flessibilità.

Quali sono le motivazioni che l'hanno portata ad accettare questa sfida?
A livello personale la voglia di mettermi in gioco in una realtà diversa, nata nel 2022 principalmente per acquisizioni di aziende leader di mercato, con un approccio da start up e la possibilità di dare il mio contributo in un ambito come il ciclo del contante che offre ancora molte aree di sviluppo, l'integrazione crescente tra mondo banche, retail e società di trasporti valori che ha individuato una traiettoria di crescita basata sempre piu' su modelli di business caratterizzati da maggiore collaborazione tra le parti.

Per raggiungere gli obiettivi ha formato una linea frontale tutta al femminile. Quali sono aree di competenza e quali obiettivi ha assegnato alle colleghe?
La squadra al femminile è stata casuale, certamente non pianificata. Serena e Silvia hanno seguito un percorso di selezione, sono state scelte sulla base della preparazione, dello loro qualità professionali e capacità di sviluppare il piano ambizioso che Sesami si è data in Italia. Entrambe fanno parte del team business development, e visto l'integrazione sempre maggiore tra i mondi retail e banche, hanno dimostrato l'agilità e la flessibilità richieste per poter interloquire con i due mercati e soprattutto generare occasioni di business con modalità collaborativa.

SERENA BOLLATI

Ci può raccontare il percorso professionale che l'ha portata ad assumere il ruolo di Business Development Manager in Sesami?
Il mio percorso professionale è iniziato più di 20 anni fa nel mondo della consulenza IT per il mondo bancario. Ho gestito progetti complessi che avevano come obiettivi la reingegnerizzazione dei processi aziendali e la razionalizzazione dei data center delle principali banche italiane, governandone le attività e coordinandone l'esecuzione. Questa modalità di lavoro mi ha consentito di vivere l'ambiente dei clienti, conoscerne i processi a fondo e apprezzare sin da subito l'importanza dell'ascolto attivo.
La naturale evoluzione di questa modalità di lavoro è stata quindi affacciarmi a ruoli di natura più commerciale, in ambito bancario e sempre nel mondo dei sistemi di pagamento fisici e digitali, seguendo tutte le fasi della vendita, dalla costruzione del valore fino alle attività di post-vendita e cross selling. Mi sono interfacciata con interlocutori di diverse organizzazioni con modelli di vendita B2B e B2B2B e ho sviluppato capacità di negoziazione evolute in ambito di progetti complessi.
Ho ricoperto nel tempo ruoli commerciali con responsabilità crescenti, passando da un approccio "farming" dei clienti ad un approccio "hunting" che mi ha spinto a dedicarmi sempre più all'identificazione di nuove opportunità di mercato e alla definizione di strategie di espansione.
Oggi mi trovo in una fase del mio percorso in cui sento di poter mettere a frutto sia la visione strategica che ho maturato, sia la capacità operativa di trasformare le idee in risultati concreti. Proprio questo mi ha spinto a scegliere Sesami: il desiderio di contribuire attivamente alla crescita di un'organizzazione che è una fintech ma che, grazie alle acquisizioni strategiche di aziende di primaria importanza sul mercato internazionale, può contare su un'eredità solida e preziosa.

Quali sono le motivazioni che l'hanno portata ad accettare questa sfida?
Ho deciso di accettarla perché rappresenta un'opportunità concreta di crescita, sia professionale che personale. Dopo diverse esperienze in ambito commerciale e di Business Development, sentivo il bisogno di confrontarmi con un contesto dinamico e ambizioso, dove poter fare la differenza in modo tangibile.
L'approccio dell'azienda all'innovazione e la visione a lungo termine – elementi fondamentali per poter costruire strategie di crescita solide – sono stati i veri discrimine.
Inoltre, l'opportunità di contribuire allo sviluppo di un progetto di crescita di un'azienda, portare la mia esperienza e continuare a mettermi in gioco sono state le leve per farmi scegliere Sesami.
Il ruolo che ho assunto mi sta offrendo di lavorare sia a livello strategico che operativo, e questo per me è un aspetto stimolante: mi piace essere coinvolta in tutte le fasi, dall'analisi di mercato alla concretizzazione di nuove partnership o linee di business.

Come valuta l'attenzione al quanto propone Sesami da parte del sistema bancario e del retail?
Sesami è sì una fintech, ma conta su diversi anni di esperienza sul mercato bancario e retail grazie alla presenza capillare sul territorio globale derivante dalle aziende acquisite.
Il fatto di avere mantenuto una strategia in cui c'è il massimo controllo della filiera produttiva e un'attenzione maniacale alla provenienza dei materiali per la produzione è sicuramente un elemento molto più che apprezzato dai clienti. Inoltre, penso che per gli interlocutori con cui ho a che fare, faccia un'enorme differenza sapere che Sesami non è solo un'azienda, ma un'organizzazione che investe su innovazione, persone e processi con una visione a 360 gradi.

SILVIA COMOLLI

Ci può raccontare il percorso professionale che l'ha portata ad assumere l'attuale posizione in Sesami?

Il mio percorso professionale, iniziato oltre 25 anni fa, si è sviluppato nei settori Fashion & Luxury, Fintech e pagamenti digitali, operando sia a livello nazionale che internazionale. All'inizio della carriera ho maturato un' esperienza nel settore Travel & Aviation presso l'Aeroporto di Milano Malpensa, svolgendo ruoli operativi e commerciali per compagnie aeree internazionali e per il servizio di sicurezza aeroportuale.

Successivamente, ho lavorato nel mondo della moda e del lusso, in un'azienda leader nel luxury sportswear, gestendo direttamente i principali clienti wholesale e retail. Nel tempo, ho assunto responsabilità crescenti, arrivando a operare su scala globale, coordinando team internazionali, formando reti vendita, ottimizzando performance commerciali e contribuendo alla definizione di strategie di sviluppo e posizionamento sui mercati esteri.

Il passaggio al settore fintech mi ha permesso di ampliare la visione strategica maturata nel retail. Ho ricoperto ruoli di account management e di business development in un contesto altamente innovativo, in un'azienda leader nei servizi tax free e nei pagamenti digitali ed ho gestito un portafoglio di brand internazionali, costruendo relazioni solide con stakeholder di alto livello e migliorando la customer experience. Successivamente, con un focus sullo sviluppo del new business, ho svolto attività di lead generation e individuazione di nuove opportunità commerciali, proponendo soluzioni digitali ad alto valore aggiunto.

Oggi metto a frutto in Sesami questa expertise per supportare i clienti del retail nel processo di trasformazione della gestione del contante, con soluzioni innovative e personalizzate, contribuendo concretamente al loro sviluppo.

Quali sono le motivazioni che l'hanno portata ad accettare questa sfida?

Ho scelto di affrontare questa nuova sfida in Sesami perché rappresenta un naturale passo avanti nel mio percorso professionale, combinando l'approccio customer-centric maturato nel retail con la spinta verso l'innovazione tecnologica. Ciò che mi ha convinta è stata l'opportunità concreta di contribuire a un progetto ambizioso e innovativo, in un settore in rapida trasformazione come il cash management. Sesami, con la sua visione integrata e globale, offre soluzioni che stanno guidando la digitalizzazione del settore, migliorando l'efficienza dei processi e creando valore tangibile per i clienti ma ciò che più mi ha attratto è la visione a lungo termine dell'azienda e il ruolo centrale che Sesami può giocare nella modernizzazione del retail.

Come valuta l'attenzione verso le soluzioni Sesami da parte del sistema bancario e del retail?

L'interesse del mercato retail verso le soluzioni Sesami è in costante crescita e si traduce in un coinvolgimento sempre più concreto.

Nel retail emerge una forte esigenza di ottimizzare la gestione del contante, ridurre i costi operativi e migliorare la sicurezza. Le soluzioni Sesami rispondono in modo preciso a queste necessità, unendo tecnologia avanzata a un approccio consulenziale che si adatta alle specificità di ogni realtà aziendale. Il valore aggiunto di Sesami è la capacità di offrire soluzioni end-to-end, scalabili e perfettamente integrabili con i processi esistenti.

Particolarmente apprezzato è l'approccio modulare e flessibile, che consente di costruire soluzioni su misura per contesti operativi molto diversi.

SESAMI

Contatti:
Sesami
www.sesami.io

yabe

Data democratization
to improve your business

Digitalizzazione e analisi dei processi
senza una riga di codice

Strumenti self-service con un approccio adatto
a qualsiasi figura professionale

Smart Hyper Automation
Automazione data driven e flow-based

- Connettori per tutte le sorgenti
- Connettori integrati per modelli di AI
- No code Agentic Automation
- Intelligent Document Recognition
- Integrazione IoT
- Enterprise Robot Process Automation

Artificial Intelligence
Intelligenza artificiale Drag & Drop

- GenAI integrata
- Governance e conformità AI Act
- Modelli multi-purpose e zero-shot
- Data insights
- Structured Information Extraction
- Text e Image Classification

Advanced Analytics
Analisi avanzata per Business Analyst

- Strumenti visuali guidati utilizzabili da tutti
- Analisi descrittiva e predittiva
- Tecnologie proprietarie ed avanzate di Data Mesh e Data Fabric per unire e correlare real-time dati da qualsiasi fonte

Data ingestion
Il valore del potenziale nascosto

- Correlazione e trasformazione dati no code e drag & drop
- Integrazione con centinaia di sorgenti e destinazioni
- Data streaming per trasformazioni in tempo reale

Una sola piattaforma collaborativa composta da servizi
completamente integrati per soddisfare ogni esigenza

YABE è un marchio di proprietà di **Aion srl**

aionteam
committed to your business

Via Cavour, 2 \ 22074 Lomazzo
info@aionteam.it
www.aionteam.it

yabe.aionteam.it

Zulu Consulting Group, l'evoluzione della sicurezza integrata

intervista a Alessandro Fasan, Security Manager e Chief Sales

Ci può parlare di Zulu, della sua storia e dei progetti per il futuro?
Zulu Consulting Group nasce dall'incontro tra operatori con esperienza pluridecennale in settori variegati ma sempre inerenti alla sicurezza (sicurezza fisica, intelligence, IT, ricerca), con lo scopo di poter fornire soluzioni altamente specifiche, integrate e personalizzate per i bisogni dei nostri clienti. Siamo presenti sul mercato dal 2018 ed operiamo a livello globale offrendo consulenza strategica in diversi ambiti tra cui cyber security, sicurezza fisica, risk & threat assessment e sviluppo software avanzato.
Per il futuro stiamo sviluppando sempre più gli aspetti inerenti all'innovazione tecnologica (AI, blockchain, comunicazioni sicure, automazione processi) e sul rafforzamento dei servizi di security/risk management negli scenari sempre più complessi del contesto internazionale attuale.

Quali sono i vostri servizi di punta?
I nostri servizi di punta sono:
- Cyber Threat Intelligence: Gli ambiti inerenti il settore della Cyber Threat Intelligence sono molteplici, noi ci siamo specializzati in alcuni settori, ovvero vulnerability assessment, penetration test, monitoraggio dark/deep web, gestione incidenti, protezione dati e identità digitale.
- Security Consulting & Corporate Security: Operiamo sostanzialmente in tutti i continenti e le task che andiamo a svolgere dipendono sempre dai bisogni del cliente e del contesto. Ci occupiamo di realizzare piani per valutare potenziali rischi e minacce, con relativa prioritizzazione e mitigazioni in base a settore, aree, etc. per fornire una protezione adeguata e continuità operativa, ma anche executive protection, sicurezza eventi, information security.
- Risk-IO: Risk-IO è una piattaforma conforme a ISO 31000 che abbiamo creato in primis per noi grazie all'esperienza del nostro gruppo di security manager internazionali per offrire soluzioni su misura e scalabili in qualsiasi contesto, per poter identificare e gestire correttamente rischi e minacce, evitando approcci generici e basata su un monitoraggio continuo e analisi multifattoriale.
- Travel Security: Operiamo a livello internazionale in aree anche ad alto rischio, dove attraverso il nostro metodo operativo ed esperienza garantiamo altissime prestazioni e risultati. Questo sta diventando un settore sempre più cruciale ed in continua evoluzione, dove negli anni ci siamo consolidati come fornitori di servizi di altissima fascia.
- Sviluppo Software Personalizzato: Abbiamo deciso di tradurre la nostra esperienza operativa in una software house per poter creare soluzioni digitali su misura realmente efficaci, per quelli che sono gli effettivi bisogni dei nostri clienti, con lo scopo non solamente di vendere licenze, ma di creare vere soluzioni per gli altri.

In quali mercati verticali siete più presenti?
Lavoriamo in tutto il mondo in settori diversi, quali:
- Infrastrutture critiche
- Energia
- Agroalimentare
- Turismo
- Logistica
- Supply chain globali
- Settore finanziario e assicurativo
- Corporate
- High-profile protection

Può riassumere casi di successo?
Senza entrare troppo nel dettaglio, possiamo citare alcuni risultati rilevanti:
1. Sviluppo di un sistema di sicurezza per una filiera agroalimentare operante a livello internazionale, con notevole riduzione degli incidenti operativi e miglioramento delle performance
2. Miglioramento della struttura di sicurezza di una struttura energetica in cui i costi di mitigazione hanno permesso una riduzione tale del premio assicurativo da poter realizzare un plus a fine anno nel bilancio del dipartimento di security aziendale
3. Molteplici identificazioni e neutralizzazioni di minacce cyber avanzate per diverse aziende (PMI e multinazionali) in tempi rapidi
4. Identificazione di falle critiche nel sistema informatico di molteplici aziende, questo purtroppo è un problema sempre più presente ed evidente a livello internazionale, ma in particolar modo in Italia
5. Esfiltrazione di individui da territori ad altissimo rischio, in tempi rapidi e con grande discrezione

Dal vostro punto di osservazione, qual è il livello di consapevolezza dei rischi informatici nelle aziende? Cosa si potrebbe fare per migliorare la situazione?
Per quanto la consapevolezza risulti in crescita, a livello generale ed in particolar modo in Italia, la consapevolezza dei rischi informatici è spesso limitata a pochi soggetti ed in generale risulta più reattiva che preventiva. Un incidente può avere un impatto finanziario, produttivo ed anche reputazionale molto elevato. Per migliorare la situazione servono formazione continua, procedure di sicurezza ben definite e simulazioni periodiche che rendano la protezione dei dati parte integrante della cultura aziendale.

Come Zulu affronta scenari di rischio complessi e in rapida evoluzione?
Quello che ci contraddistingue è la nostra flessibilità e capacità di adattamento dove attraverso la nostra peculiare combinazione intelligence, tecnologia e capacità operativa riusciamo a fornire soluzione altamente specializzate. Il nostro approccio è multifattoriale, basato sulle esigenze del cliente e del contesto, dove gli esperti vanno a definire le modalità di supporto e concordare con il cliente l'entità dell'impegno ad esso inerente. A supporto di questo processo utilizziamo analisi predittive, strumenti proprietari per riuscire ad anticipare e ridurre quanto più possibile i rischi prima che si concretizzino. Negli anni, tutto ciò ci ha permesso di essere un partner strategico e affidabile per le aziende, che non solo vogliono proteggersi, ma crescere grazie alla sicurezza.

ZULU CONSULTING
· resilient security solution ·

Contatti:
Zulu Consulting Group
www.zuluconsultingroup.com

Dissuasori FAAC, la sicurezza su misura, anche nello stile

comunicato aziendale

In un'epoca in cui la protezione di varchi sensibili e la tutela di beni e persone sono temi sempre più centrali, sia in ambito privato sia in ambito pubblico, i dissuasori rappresentano un fondamentale elemento per la protezione fisica o la limitazione degli accessi. Seppure storicamente pensati per la gestione del traffico nelle aree ZTL, l'impiego dei dissuasori si è progressivamente allargato anche ad altre applicazioni: ambasciate, aeroporti, strutture militari, siti governativi, aree commerciali, centri logistici, industria e manifattura del lusso.
In questo scenario, FAAC è leader nella progettazione e produzione di soluzioni per l'automazione, il controllo e la protezione dei varchi, e punto di riferimento per soluzioni innovative, certificate, robuste, veloci, facili da manutenere e basate sulla storica tecnologia oleodinamica del primo automatismo per cancelli progettato 60 anni fa.
Oggi i committenti pubblici e privati richiedono non solo sicurezza, ma anche una resa estetica superiore e un impatto architettonico in linea con il contesto. Per questo motivo, FAAC offre un'ampia gamma di personalizzazioni, con materiali, finiture e colorazioni diverse.

Una gamma con soluzioni per ogni contesto
La gamma di dissuasori FAAC è progettata per rispondere a ogni esigenza di controllo accessi, dalla regolazione del traffico residenziale o urbano alla protezione di siti ad alta sicurezza. Si articola in tre linee principali: **J200**, **J275** e **JS**, disponibili in versioni automatiche, semi-automatiche, fisse e rimovibili.

• Nei **centri storici** o zone a traffico limitato, i modelli a scomparsa non impattano sull'architettura cittadina, garantendo la limitazione degli accessi, mentre i fissi delimitano le aree permanentemente chiuse al transito delle auto.
• Nei **complessi industriali o logistici**, i dissuasori fissi o mobili fungono da barriera per il controllo perimetrale e, grazie alla velocità di abbassamento e facilità di manutenzione, assicurano alti flussi e continuità operativa.
• Nelle **infrastrutture critiche**, come data center, aeroporti o in siti sensibili come ambasciate, stazioni, palazzi governativi o stadi, assicurano la massima protezione fisica da atti criminosi o attacchi terroristici.
Vediamo i modelli disponibili nel dettaglio.
La serie **J200** è pensata per contesti residenziali e aree a traffico limitato. Comprende tre modelli: **J200 HA**, versione automatica; **J200 SA**, semi-automatica, che si solleva manualmente tramite sblocco a chiave senza alimentazione elettrica; e **J200 F**, versione fissa, ad esempio per delimitare permanentemente percorsi pedonali.
Più robusta e versatile, la serie **J275** è adatta a centri storici, aree urbane e commerciali, siti industriali e logistici, dove il passaggio veicolare è intenso. Anche in questo caso troviamo tre modelli principali: **J275 HA**, automatico; **J275 SA**, semi-automatico senza alimentazione elettrica; e **J275 F**, fisso. A questi si affiancano due dissuasori progettati per la sicurezza perimetrale ad alte prestazioni: J275 HA 2K20, in configurazione doppia, in grado di arrestare un camion di 7.500 kg a 48 km/h, certificato secondo gli standard PAS 68 e IWA 14-1; e J275 F 2K20, la corrispondente versione fissa.

Serie JS – la nuova frontiera della protezione ad alta sicurezza
Tra le soluzioni più evolute di FAAC si colloca la serie JS, progettata per applicazioni ad alta sicurezza; i dissuasori JS – disponibili in versione automatica (HA), rimovibile (R) e fissa (F) – rappresentano un benchmark nel mercato per prestazioni, manutenibilità, compattezza, estetica e sostenibilità. Sia i modelli JS 48 che JS 80 hanno superato con successo i crash test in laboratori accreditati, raggiungendo prestazioni ai vertici della categoria in tutte e tre le certificazioni disponibili secondo standard ASTM, PAS ed IWA, in grado di arrestare un camion di 7.500 kg entro un metro dal punto di impatto, rispettivamente a 48 km/h (JS 48) e 80 km/h (JS 80), rimanendo operativi dopo l'impatto.

Compattezza e flessibilità d'installazione per i dissuasori JS
Altra caratteristica distintiva della serie JS è l'estrema compattezza; il cilindro ha un diametro di soli 275 mm ed un'altezza fuori terra di 1 metro, mentre l'installazione è semplificata grazie all'impiego di un pozzetto unico per tutti i modelli automatici ed è guidata da schemi di posa a disposizione di chi esegue le predisposizioni edili, fornendo le specifiche per le installazioni con più unità affiancate.
JS 48 HA e JS 80 HA garantiscono l'accesso per le operazioni di manutenzione in loco senza mezzi di sollevamento, con possibilità di installare l'opzione "Emergency Fast Operation" per la risalita rapida del cilindro in soli 1,5 secondi. Inoltre, sia i dissuasori fissi JS 80 F sia i rimovibili serie **JS 48 R** e **JS 80 R**, grazie al design **"Shallow Mounted"**, richiedono una profondità di scavo minima, rendendo l'installazione poco invasiva, pur con la medesima resistenza dei modelli automatici.

Design, durabilità e manutenzione facilitata
Oltre alla resistenza ai vertici della categoria, FAAC ha posto grande attenzione al design, alla durabilità ed alla riduzione degli oneri manutentivi durante tutto il ciclo di vita del prodotto.
I dissuasori JS sono disponibili con camicia protettiva in acciaio inox satinato 316L oppure in mDure, un tecnopolimero innovativo, resistente, ampiamente personalizzabile nei colori e facilmente sostituibile da un solo operatore in caso di urti o vandalismi. Le testate dei cilindri dei dissuasori sono trattate con resina Rilsan, materiale ad alta resistenza all'abrasione, ideale per sopportare il passaggio frequente di veicoli anche in condizioni climatiche critiche, mentre le piastre superiori sono in acciaio inox.
Per agevolare la manutenzione e ridurre il fermo macchina, tutti i dissuasori FAAC sono dotati di una centralina oleodinamica che costituisce il cuore pulsante del sistema di movimentazione e che può essere sostituita senza mezzi di sollevamento ed a cura di un solo addetto alla manutenzione.

Personalizzazioni senza limiti
Per i dissuasori serie J200 e J275, il cliente può scegliere tra due finiture principali: con cilindro in acciaio inox 316L satinato o con cilindro verniciato in qualsiasi colore RAL, per armonizzarsi con l'arredo urbano o i colori identitari del committente finale.
La serie JS offre un livello di personalizzazione ancora più raffinato e articolato grazie al cilindro disponibile con camicia in mDure, con verniciatura a scelta oppure in acciaio con camicia esterna in acciaio inox 316L satinato. In occasione di eventi speciali o per esigenze promozionali, è possibile anche applicare un wrapping personalizzato per realizzare un rivestimento grafico che può riportare immagini, loghi o messaggi pubblicitari e trasformare il dissuasore anche in uno strumento di comunicazione; non solo, anche la fascia catarifrangente può essere selezionata in bianco, rosso o giallo o customizzata su esigenze del committente.

Contatti:
FAAC
www.faac.it/progetti

Dallo spray al taser: i “surrogati” che possono uccidere

intervista a Michele Bardi, senior security manager e docente presso San Giorgio Formazione

Il porto non autorizzato di strumenti ritenuti innocui espone le GPG a responsabilità penali gravissime. Gli ultimi casi di cronaca lo dimostrano.
Il tema dell’armamento delle Guardie Particolari Giurate rimane centrale nel dibattito sulla sicurezza privata. Sempre più spesso emergono casi in cui alcuni operatori valutano l’impiego di strumenti ritenuti “meno pericolosi” della pistola, come spray urticanti o taser. Una convinzione che, oltre a non avere alcun fondamento normativo, espone a conseguenze professionali e giuridiche gravissime.
Abbiamo chiesto a **Michele Bardi**, esperto della normativa sulla vigilanza privata, di chiarire l’attuale quadro regolatorio e i rischi connessi al porto non autorizzato da parte delle GPG.

Qual è la cornice normativa che disciplina l’armamento delle GPG?
La legge non lascia spazio a interpretazioni: il Prefetto rilascia una licenza di porto d’armi e un’autorizzazione al porto della pistola esclusivamente per difesa personale. Questo significa che l’unico strumento di cui la GPG può essere dotata e che può legittimamente portare durante il servizio è la pistola autorizzata. Qualsiasi altro dispositivo, dagli spray urticanti ai taser, non è incluso nell’autorizzazione e quindi non può essere portato né utilizzato. Dura lex, sed lex: è la regola che vale per tutti, senza eccezioni. Pena il configurarsi di un abuso

Molti ritengono spray e taser meno pericolosi della pistola. È davvero così?
Si tratta di una convinzione ingannevole. Questi strumenti sono spesso definiti “non letali”, ma la realtà dimostra il contrario. Basti pensare agli ultimi due casi che hanno coinvolto le forze di polizia: l’uso del taser ha purtroppo provocato la morte delle persone colpite. L’esito di uno strumento di coercizione non dipende solo dalla sua classificazione, ma anche dalle condizioni fisiche della persona, dalla distanza, dal contesto e, soprattutto, dall’addestramento di chi lo utilizza.

E le conseguenze per una GPG che decidesse di portare uno strumento non autorizzato?
Pesantissime. Si va dalla violazione penale per porto abusivo di strumenti atti a offendere fino alla responsabilità civile e penale in caso di lesioni o morte. Inoltre, l’uso di uno strumento non autorizzato espone la GPG a una responsabilità professionale diretta, senza alcuna copertura normativa o istituzionale. Non solo si rischia la revoca delle licenze ma si mette in gioco la stessa legittimità del servizio svolto, in propria persona, senza copertura normativa o istituzionale.

Oltre agli aspetti penali, ci sono implicazioni disciplinari?
Certo. Un istituto di vigilanza non può tollerare che un proprio operatore introduca strumenti non autorizzati. In questi casi, oltre al rischio di revoca della licenza individuale, l’istituto potrebbe subire conseguenze da parte della Prefettura per mancata vigilanza sui propri dipendenti: il comportamento di un singolo può ricadere sull’organizzazione, con danni economici e reputazionali significativi.

C’è chi sostiene che questi strumenti dovrebbero essere introdotti anche per le GPG. È una prospettiva realistica?
Il tema è dibattuto ma, allo stato attuale, non ci sono basi normative. L’uso del taser da parte delle forze di polizia è stato introdotto con sperimentazioni e regole molto stringenti, prevedendo formazione specifica, protocolli sanitari e catene di responsabilità precise. Traslare questa esperienza sulle GPG significherebbe aprire una riflessione profonda ma, come già detto, al momento non esiste alcuna previsione normativa in tal senso. Non possiamo quindi confondere il dibattito politico con la realtà giuridica: oggi le GPG non possono portare altro che la pistola autorizzata.

Alla luce dei recenti fatti di cronaca, che lezione trarre per le GPG?
Che non esistono scorciatoie in materia di sicurezza. Se strumenti ritenuti “meno invasivi” possono causare la morte anche quando utilizzati da operatori di polizia formati e autorizzati, ciò dimostra quanto sia illusorio credere che una GPG, priva di autorizzazione e di addestramento specifico, possa usarli senza rischi. La vera professionalità sta nel rispetto delle regole e nella consapevolezza delle proprie responsabilità.

Qual è allora la strada per rafforzare davvero la sicurezza privata?
Investire su formazione, addestramento e cultura della legalità. Una GPG che conosce i limiti del proprio mandato, che sa gestire conflitti senza eccedere e che utilizza correttamente lo strumento autorizzato è una risorsa preziosa. Al contrario, chi si affida a strumenti non autorizzati diventa un problema, non una soluzione.

Negli ultimi anni le GPG sono sempre più impiegate in servizi a contatto con il pubblico. Che cosa comporta questo cambiamento?
È vero, la figura della Guardia Particolare Giurata non è più limitata alla sola tutela dei beni materiali. Oggi, nell’ambito della sicurezza complementare e sussidiaria, le GPG operano in contesti in cui la loro presenza incide direttamente anche sulla protezione delle persone. Ciò implica la capacità di individuare situazioni di pericolo, rilevare elementi di rischio per garantire l’incolumità dei cittadini, saper gestire dinamiche relazionali complesse con il pubblico. Una responsabilità ulteriore, che evidenzia ancor più l’importanza della formazione, dell’equilibrio professionale e del rispetto rigoroso delle regole.

La criminalità con cui oggi si confrontano le GPG è diversa rispetto al passato. Quali riflessioni suscita questo scenario?
Negli anni ’80 o ’90 il rischio prevalente era la microcriminalità predatoria. Oggi, invece, le GPG devono affrontare fenomeni molto più ampi e articolati: criminalità organizzata, furti con modalità evolute, aggressioni in contesti affollati e, non di rado, soggetti in stato di alterazione psico-fisica. Sono sfide nuove, che richiedono strumenti e ruoli adeguati. Per questo, credo sia urgente una riflessione normativa che collochi meglio le GPG all’interno del sistema sicurezza nazionale, valorizzando il principio della sicurezza partecipata. Una collaborazione più strutturata tra pubblico e privato non solo è auspicabile, ma diventa necessaria di fronte alla complessità dei rischi attuali.
In sintesi, la questione non riguarda la ricerca di strumenti alternativi, ma il rispetto rigoroso di un perimetro normativo ben definito. Il porto di spray o taser da parte delle GPG, lungi dall’essere una soluzione “più semplice”, rappresenta una violazione che può generare responsabilità gravi e irreparabili. Il futuro della sicurezza privata passa attraverso professionalità, formazione e rigore giuridico, non attraverso facili scorciatoie.
Rimane inteso che, per casi specifici, è concesso ai Titolari della Licenza dell’IdV presentare richiesta al Prefetto per autorizzare il porto, da parte delle proprie guardie giurate, di strumenti diversi dalla pistola. Solo in presenza di tale autorizzazione le GPG possono esserne dotate ed eventualmente portarlo sulla divisa, che – va ricordato – è anch’essa approvata e non può essere modificata senza il nulla osta dell’autorità competente.

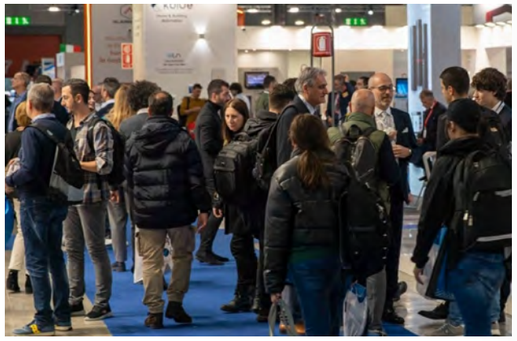
Contatti:
San Giorgio Srl
formazione@sangiorgionet.com
www.sangiorgionet.com

Più grande, più globale, più smart: SICUREZZA 2025 è già un’edizione record

a cura della redazione

La manifestazione torna dal 19 al 21 novembre. Un nuovo format con giornate tematiche sempre più attento allo sviluppo di contenuti, focus su AI e integrazione tecnologica e un respiro internazionale sempre più ampio: così Fiera Milano diventa capitale della security & fire.

Non solo una fiera, ma un osservatorio privilegiato su come sta cambiando la sicurezza a livello globale. In un contesto in cui minacce fisiche e digitali si intrecciano sempre di più, SICUREZZA 2025 si prepara a raccontare la capacità innovativa e le potenzialità di sviluppo del settore, con un’edizione che già oggi, quando mancano pochi mesi all’appuntamento, segna numeri importanti: la superficie espositiva è cresciuta del 18% rispetto al 2023, gli espositori esteri sono aumentati del 28% e sono il 31% del totale, con aziende da 24 Paesi. Segnali che confermano il respiro internazionale della manifestazione e la sua capacità di interpretare l’evoluzione tecnologica, normativa e operativa della security.



Accanto ai ritorni di player consolidati tra cui **Inim, Tecnoalarm, Notifier e Hikvision**, spiccano i nuovi ingressi: tra gli italiani **Gams** (Bettini) e **Combivox**, tra gli esteri **Assa Abloy e Carrier Fire & Security**. Con un layout rinnovato e un format attento ai contenuti, **SICUREZZA 2025** si presenta come un vero e proprio laboratorio di innovazione per videosorveglianza, antincendio, controllo accessi, cyber security e sicurezza passiva.

Al centro della proposta espositiva ci saranno la digitalizzazione e l’uso dell’intelligenza artificiale, che stanno ridisegnando confini e strumenti del comparto. Nuovi sistemi integrati con AI, monitoraggio predittivo, video analytics evoluti, piattaforme edge-cloud e soluzioni data-driven mostrano come la gestione della complessità richieda, oggi più che mai, anche una cyber-resilienza a 360 gradi. Sul fronte antincendio, si va verso impianti a sensibilità crescente, rilevazioni wireless e manutenzione predittiva. Non mancano i droni, ormai strumenti indispensabili per prevenzione incendi e monitoraggio ambientale.

La personalizzazione delle soluzioni emerge come tendenza consolidata: le aziende si propongono sempre più come partner consulenziali, capaci di costruire progetti su misura e modulabili.

TRE GIORNATE TEMATICHE PER FARE SISTEMA

Quest’anno la manifestazione propone un nuovo format formativo scandito da tre giornate verticali. Il **19 novembre** sarà il **Cyber Day**, con focus sulla convergenza tra minacce fisiche e digitali, la cybersecurity come fattore strategico e l’impatto delle direttive europee NIS 2 e CER. Il **20 novembre** sarà il **Security Day**, dedicato alle applicazioni in contesti ad alto rischio – dai trasporti ai beni culturali – e alle nuove figure professionali emergenti. Infine, il **21 novembre** arriva il **Job in Security Day**, che punta a ridurre il divario tra formazione e lavoro attraverso il **Progetto EDU**: workshop, presentazioni e colloqui tra imprese, scuole e ITS.

Tutti gli eventi formativi si svolgeranno nella **Cyber & Security Arena**, con talk, demo e tavole rotonde a cura di esperti, associazioni e aziende leader. A completare l’offerta i **Security Talk** di AISS, AIPS, ANIE Sicurezza e ConFederSicurezza, insieme ai podcast di ASSIV.

LA SECURITY AL CENTRO DELLA EVOLUZIONE DEL BUILDING CON MIBA

SICUREZZA 2025 sarà nuovamente parte di **MIBA – Milan International Building Alliance** e si svolgerà in contemporanea conGEE, Global Elevator Exhibition (mobilità verticale e orizzontale), MADE Expo (edilizia) e SMART BUILDING EXPO (integrazione tecnologica). Una sinergia che trasformerà Fiera Milano in un hub internazionale dedicato all’evoluzione dell’edificio e della città, con un’offerta integrata che mette al centro innovazione, sostenibilità e digitalizzazione.

InFOG: il nebbiogeno che completa il sistema antintrusione

comunicato aziendale

Nel mondo della sicurezza, ogni secondo conta. Ed è proprio in quei pochi istanti decisivi che il nebbiogeno InFOG fa la differenza: un sistema integrato e intelligente, progettato per impedire fisicamente al ladro di portare a termine l'intrusione.
Non un semplice accessorio, ma un elemento plus del sistema di allarme. InFOG nasce ed è pensato per essere parte integrante dell'ecosistema Inim, con una gestione centralizzata, un monitoraggio remoto intuitivo e un livello di integrazione che eleva gli standard di sicurezza professionale.

La sua efficacia sta nell'annullare la visibilità dell'ambiente in pochi secondi, costringendo l'intruso a desistere e guadagnando tempo prezioso per l'intervento delle forze dell'ordine. A differenza dei fumogeni tradizionali, la nebbia prodotta da InFOG è atossica, certificata food-grade e non lascia residui, risultando perfetta anche per ambienti sensibili.

Disponibile in diverse versioni, InFOG copre ogni esigenza: dai piccoli ambienti residenziali ai grandi magazzini industriali, grazie alla sua flessibilità installativa, con connessione cablata o via radio, che si adatta facilmente a qualsiasi contesto.

Per l'installatore, InFOG rappresenta una scelta intelligente e redditizia. La perfetta integrazione con le centrali Prime e PrimeX consente di configurare la protezione in modo semplice e immediato, mentre la gestione avanzata da app InimTech Security, con funzionalità come la prova di sparo e il monitoraggio del livello serbatoio, rende più efficiente ogni fase, dall'installazione alla manutenzione ordinaria. Il sistema antisabotaggio integrato garantisce la massima affidabilità, mentre la gestione da cloud, completamente gratuita – e su server Europei - permette un controllo in tempo reale senza costi aggiuntivi.

InFOG - progettato e prodotto in Italia - rafforza la proposta di valore per i clienti finali, offrendo una protezione realmente proattiva. Non è solo un nebbiogeno, ma una vera difesa attiva, visibile e percepibile, che cambia la percezione stessa della sicurezza.
L'ecosistema Inim integra rivelazione, intrusione, videosorveglianza e domotica in un'unica piattaforma scalabile e intuitiva. In questo scenario, InFOG diventa il naturale complemento, trasformando ogni installazione in una soluzione completa, tecnologicamente evoluta e realmente efficace.

Vedi niente ?

Bene !

Neanche il ladro

InFOG

Security Fogging System

InFOG è il **nebbiogeno integrato Inim** che, azzerando la visibilità in pochi secondi, rende impossibile agire. **Il 90%** dei furti viene sventato prima di iniziare. La sua nebbia è atossica e certificata food-grade: sicura anche in ambienti con presenza di alimenti. **Doppia connessione cablata e via radio**, antisabotaggio immediato, prova di sparo e serbatoio sempre sotto controllo tramite app.

Passa a un livello superiore di protezione con un sistema che cambia le regole della sicurezza.

Scopri di più su **www.inim.it**

inim®
Evolving Protection

La Fondazione Enzo Hruby per l’Isola di San Lazzaro degli Armeni

a cura della redazione

Nel cuore della laguna di Venezia, di fronte al Lido, sorge un’isola interamente occupata da uno dei centri mondiali più importanti per la cultura armena, casa madre dell’ordine dei Mekhitaristi. Si tratta dell’isola di San Lazzaro, che prima di essere abitata in maniera stabile a partire dal Settecento dai monaci armeni in fuga dal Peloponneso e accolti dalla Serenissima, è stata terra dei benedettini di Sant’Ilario, poi lebbrosario e alloggio per i poveri.
Quando nel 1717 la Repubblica di Venezia concesse l’isola al gruppo di monaci armeni in fuga da Modone, che da allora la abitano stabilmente, tra di loro vi era Mechitar, oggi sepolto sull’isola all’interno della chiesa, uno degli artefici della rinascita della letteratura armena, nonché il fautore dello sviluppo della comunità di San Lazzaro e della sua trasformazione in importante centro culturale e scientifico. Fu grazie a lui, infatti, che venne restaurato il monastero e furono sistemati i terreni circostanti, così i monaci poterono iniziare a educare i discepoli e tramandare di generazione in generazione la cultura armena. Nei decenni successivi fu anche costruita una tipografia indipendente da quelle di Venezia e fu edificata la biblioteca. San Lazzaro era un centro così importante che persino durante l’invasione napoleonica fu risparmiata, perché considerata un’accademia di scienze e quindi protetta dall’imperatore. Di particolare interesse sono la pinacoteca, il museo e la biblioteca, dove si trovano volumi, manoscritti e manufatti da tutto il mondo. All’interno della biblioteca sono conservati 170.000 volumi, tra cui 4.500 manoscritti. Nella pinacoteca e nel museo si trovano particolari reperti archeologici, tra cui dipinti e reperti armeni, un gesso di Canova che raffigura il figlio di Napoleone Bonaparte e la mummia egizia di Nemen Khet Amen, dell’800 a.C., completa di sarcofago. Sul soffitto si può ammirare uno splendido dipinto del Tiepolo che raffigura un’allegoria della Giustizia.
I monaci, inoltre, si prendono cura di diversi roseti sull’isola, e dai petali di rosa producono una marmellata, la vartanush, preparata con una tipica ricetta armena.

Per questo luogo che rappresenta uno scrigno dove ogni pietra, ogni libro antico, ogni opera d’arte racconta una storia fatta di cultura, bellezza e dialogo tra i popoli e le religioni, la Fondazione Enzo Hruby ha recentemente sostenuto un importante progetto di sicurezza. L’intervento, realizzato dalla società Umbra Control, azienda Amica della Fondazione, e che si è avvalso di un contributo concreto da parte di Ksenia Security, ha avuto come obiettivo la tutela dell’intero complesso dalle intrusioni agli incendi, fino agli atti vandalici, nel massimo rispetto dei manufatti esistenti.
Il sistema di protezione installato comprende un avanzato sistema antintrusione perimetrale e volumetrico. La protezione perimetrale, affidata a sensori collocati lungo le mura esterne, si affianca a un sistema volumetrico pensato per monitorare le aree più sensibili, come la biblioteca, il museo e gli spazi sacri. A questa si aggiunge una sofisticata rete antincendio, fondamentale in un ambiente dove la presenza di manoscritti, dipinti e materiali antichi rende altissimo il rischio. Il sistema è stato progettato per essere altamente efficiente, andando oltre le richieste normative e prevedendo rilevatori di fumo e calore in ogni ambiente, con particolare attenzione agli archivi e ai luoghi di culto, oltre a pulsanti manuali per l’attivazione diretta in caso di emergenza.
Il convento è inoltre sorvegliato costantemente grazie a un sistema di videosorveglianza composto da telecamere su rete IP ad alta risoluzione, che consente di registrare in maniera continua con archiviazione sicura dei flussi video su server protetti, accessibili solo da personale autorizzato. Il sistema, inoltre, adotta algoritmi di analisi video in grado di generare alert automatici anche durante normali visite guidate e consente di comunicare direttamente con gli ambienti videosorvegliati attraverso messaggi audio da parte di operatori incaricati.
Per facilitare la gestione dell’intero impianto da parte del personale del convento, è stato sviluppato un sistema di supervisione centralizzata che integra in un’unica interfaccia intuitiva tutte le funzioni di controllo. Questo strumento consente anche a operatori non specializzati di visualizzare in tempo reale guasti, allarmi o malfunzionamenti, sia in loco che da remoto, intervenendo in modo tempestivo e mirato. L’interfaccia grafica con mappe dinamiche permette di individuare con facilità l’area interessata da un evento e programmare rapidamente un eventuale intervento.
La progettazione e l’installazione di tutti questi sistemi sono state condotte con un approccio rispettoso, consapevole del valore architettonico e simbolico del luogo. Le soluzioni adottate non solo rispondono agli standard più elevati di sicurezza, ma sono anche non invasive e perfettamente integrate nell’ambiente.

“Il progetto di protezione del Convento Mechitarista di San Lazzaro degli Armeni - dichiara il vice presidente della Fondazione Enzo Hruby, **Carlo Hruby** - *rappresenta un esempio virtuoso dello straordinario valore che la tecnologia può offrire al mondo dei beni culturali. Dopo i progetti sostenuti dalla nostra Fondazione dedicati all’Isola di San Giorgio Maggiore, sede della Fondazione Giorgio Cini, al Teatro La Fenice, al Conservatorio “Benedetto Marcello” e ad altri luoghi e tesori di Venezia, siamo orgogliosi di aver sostenuto questo nuovo progetto importante in questa città simbolo della straordinaria ricchezza del patrimonio culturale italiano. Desidero ringraziare Umbra Control, che da sempre ci affianca in veste di società Amica della Fondazione Enzo Hruby, e Ksenia Security, che ha desiderato offrire un proprio contributo concreto nell’ambito di questo progetto così importante, che si configura come un vero e proprio modello di protezione a regola d’arte applicabile a contesti analoghi”.*

Partner

essecome ONLINE

n. 05/2025
Anno XLV
Periodico fondato da Paolo Tura

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

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

TRAFFIC
THE URBAN TECHNOLOGY SHOW | 2025

8-9 OCTOBER 2025
BOLOGNA EXHIBITION CENTRE - ITALY

TRAFFIC | MOBILITY | CITY

- TRAFFIC MANAGEMENT
- INFRASTRUCTURE
- CITY TECH & SMART CITIES
- PUBLIC & COLLECTIVE TRANSPORT
- PARKING TECHNOLOGY
- LIGHTING TECHNOLOGY
- SMART ROADS, SAFETY & CONTROL
- SMART E-MOBILITY & CONNECTIVITY
- ENVIRONMENTAL ENGINEERING

CO-LOCATED WITH
e-CHARGE
E-BUS EUROPE
IN COLLABORATION WITH
Bologna Fiere
ORGANIZED BY
I51

ISTITUTIONAL PATRONAGES
Regione Emilia-Romagna
Comune di Bologna

GREEN SPONSOR
Sfhera

TECHNICAL SPONSOR
TellusPower

WITH THE SUPPORT OF
ADACI · AISICO ASSOCIAZIONE · ALIS ITALIA IN MOVIMENTO · ANIASA MUOVIAMO IL FUTURO · A.N.S.A.T. · ANIE CONFINDUSTRIA · ASSINTEL · assodel · Collegio Italia · CONFINDUSTRIA EMILIA AREA CENTRO · ENEA · Kyoto Club · MOTUS-E · PIARC · SIPOTRA · TTS ITALIA

WWW.TRAFFIC.SHOW

ermes
freedom to communicate

SOLUZIONI AUDIO IN IP

SOS Spazi Calmi

Sistema di comunicazione bidirezionale per Spazio Calmo conforme a D.M. 03/08/2015 e EN62820-2

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

SAN GIO RGIO

seguici su

Formazione sulla Sicurezza Sussidiaria Dm 154/2009

Safety 81-08 - Antincendi - Primo Soccorso e Blsd

Covert Test Porti Aeroporti e Tribunali

Aviation Security Enac Dm 85-99

Formazione Gpg Dm 269/2010

Security Manager Uni 10459

Dgr Merci Pericolose

X-bag

San Giorgio, La Mossa Giusta.

www.sangiorgionet.com