

L'IA E BIG DATA ANALYSIS OPPORTUNITÀ E RISCHI

UN CONTINUO ABBATTIMENTO DI FRONTIERE

Milan, 16/05/2023

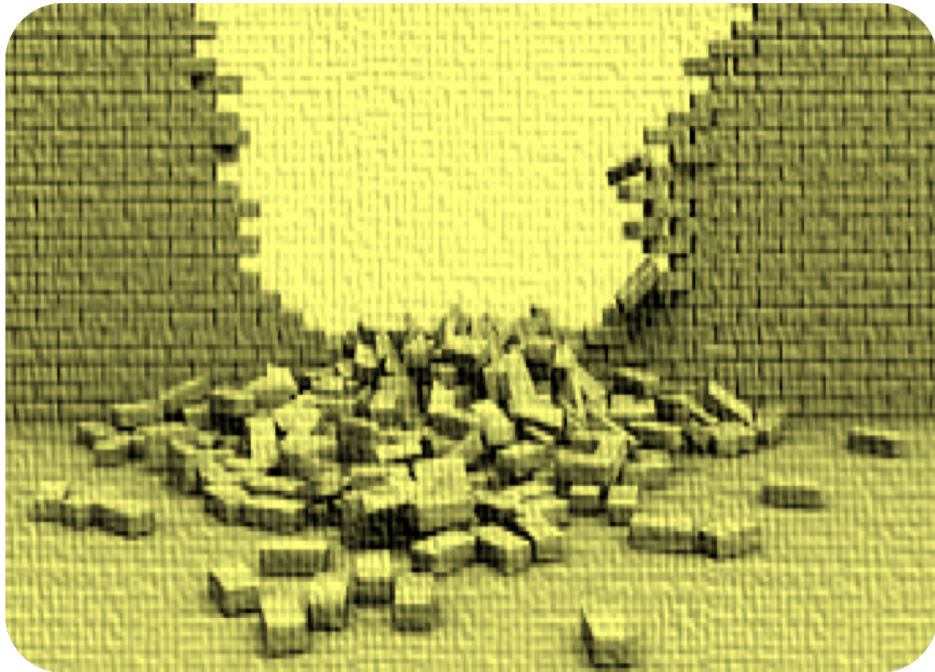


BNL

BNP PARIBAS

La banca per un mondo che cambia

Cosa è già cambiato



In questi ultimi anni abbiamo assistito ad una serie di abbattimenti di confini che per decenni sono stati ben saldi; i due più evidenti sono:

- ❖ **Il confine tra Safety e Security**
- ❖ **Il confine tra Sicurezza fisica e sicurezza logica**

Le spinte che hanno portato all'abbattimento sono state principalmente il cambiamento delle esigenze di business e l'incredibile evoluzione tecnologica che corre sempre più velocemente ad offrirci nuove soluzioni.

Adeguarsi alle nuove esigenze del business bancario

Cambia il modello
di filiale

Cambia l'esigenza
gestionale della
sicurezza fisica

Cambia
l'esigenza di
sicurezza fisica

In sintesi

- Non solo analisi dei sistemi antintrusione-antifurto e dei sistemi di videosorveglianza connessi a sistemi di centralizzazione più o meno evoluti;
- Necessaria anche la capacità di analizzare in modo intelligente un evento o un insieme di eventi e di discriminare gli stessi in funzione di parametri gestionali diversi;
- Non basta più la semplice generazione di un semplice output di allarme;
- Bisogna analizzare un insieme di elementi o situazioni anche se provenienti da tecnologie diverse, al fine di ottenere un output di segnalazione dettagliato e che consenta immediatamente di capire la natura della anomalia.

Le nuove agenzie bancarie cominciano ad assomigliare a dei punti vendita - Caratteristiche

- Cash management esternalizzato;
- Divisione fisica tra le cash machine ed il personale;
- Spariscono le bussole si passa alle sliding doors;
- Aumenta la tecnologia in campo con telecamere fornite di video analisi;
- Aumenta la tecnologia a disposizione del cliente che in molti casi può interagire con il personale banca grazie ad un monitor multimediale interattivo connesso ad una control room di servizi bancari.

Nelle piccole agenzie si può anche lavorare da soli ed in questo caso la safety diventa il tema centrale con l'utilizzo della analisi video con questo approccio.

La risposta tecnologica della sicurezza si concretizza attuando il concetto di intelligenza distribuita ponendo in unica piattaforma il governo della sicurezza fisica, della sicurezza logica e della safety.

- La sicurezza antintrusione
- La sicurezza antifurto
- La video-registrazione
- La video-sorveglianza
- La video-analisi
- L'audio bi-direzionale
- Il controllo degli accessi
- La safety



Approccio olistico alla sicurezza del sito e delle risorse che vi lavorano

Il limite delle tecnologie abilitanti

Cosa abbiamo:

- ❖ Un Sempre più grande numero di informazioni;
- ❖ Grande Capacità di stivaggio delle stesse;
- ❖ Velocità di analisi delle info e del loro continuo aggiornamento;
- ❖ Capacità di mettere in relazione le informazioni tra loro e nel più breve tempo possibile.



Il problema vero che ci si pone, e che è anche la sfida di adesso, è cosa farcene di tutta questa marea di informazioni, come utilizzarle, come renderle strumentali ad i nostri obiettivi.

Attualmente è ancora enorme il GAP che c'è tra la infinita serie di informazioni che possiamo avere e quelle che riusciamo ad usare in modo davvero utile e funzionale ai nostri obiettivi.

Un esempio : Utilizzo della IA nelle control room ed opportunità

- 1. Rilevamento automatizzato delle minacce:** L'IA può essere **addestrata** per analizzare flussi di video provenienti da telecamere di sorveglianza e **rilevare automaticamente** comportamenti sospetti o anomalie. Ad esempio, può identificare intrusioni, oggetti lasciati incustoditi, movimenti insoliti o comportamenti violenti. Ciò consente agli operatori di sicurezza **di rispondere rapidamente** alle minacce e di prendere le misure appropriate.
- 2. Monitoraggio e analisi dei dati in tempo reale:** L'IA può **elaborare e analizzare grandi quantità di dati provenienti da diverse fonti**, come sensori, telecamere e sistemi di controllo degli accessi. Questa analisi in tempo reale consente di **individuare rapidamente** le anomalie, identificare modelli di comportamento e segnalare situazioni di potenziale rischio.
- 3. Integrazione dei sistemi di sicurezza:** L'IA può integrare i diversi sistemi di sicurezza presenti in una control room, come telecamere di sorveglianza, allarmi antintrusione, rilevatori di fumo, ecc. Ciò consente di **centralizzare e coordinare la gestione delle minacce**, semplificando la visualizzazione e la risposta agli eventi di sicurezza.
- 4. Supporto decisionale:** L'IA può fornire **suggerimenti e raccomandazioni** agli operatori di sicurezza sulla base dell'analisi dei dati e delle situazioni correnti. Ad esempio, può suggerire azioni appropriate da intraprendere in determinate situazioni di emergenza o fornire indicazioni sulla risposta più efficace a un evento di sicurezza.
- 5. Automazione dei processi:** L'IA può **automatizzare** alcune delle attività ripetitive e di routine all'interno della control room di sicurezza, come la verifica dei permessi di accesso, la gestione delle credenziali degli utenti e la generazione di report. Ciò consente agli operatori di concentrarsi su compiti ad alto valore aggiunto e **riduce il rischio di errori umani**.

I grandissimi rischi che vedo

- Sempre più numerose le società di cyber security che propongono moduli di intelligenza artificiale applicabili alla qualsiasi;
- Sempre più grande il gap di knowledge e skill su questi temi, tra chi deve decidere i partner di cui avvalersi e gli aspiranti partner che si propongono;
- La contemporanea attuale tendenza/tentazione da parte delle aziende a esternalizzare le attività di sicurezza purtroppo ancora troppo spesso viste come un centro di costo;
- Vulnerabilità supply chain perché magari lì le conoscenze specifiche potrebbero essere in qualche caso ulteriormente lacunose;
- La convinzione errata di poter dare al tool dei dati, fargli delle domande ed accontentarsi delle risposte apparentemente corrette...
- **...A PROPOSITO... la precedente slide la ha scritta CHATGPT**



...Ecco la prova...

17:50 Gio 11 mag

AA chat.openai.com

IA per control room sicurezza

New chat

Yesterday

New chat

IA per control room sic

April

Cloud migration for public ad

Normative Approaches to AI

February

PPP per sostenibilità.

Rischi percepiti dagli italiani.

PI

Applicare moduli intelligenza artificiale alle control room di sicurezza fisica

L'applicazione di moduli di intelligenza artificiale alle control room di sicurezza fisica può apportare diversi vantaggi. L'intelligenza artificiale può essere utilizzata per automatizzare e migliorare i processi di sorveglianza e controllo, consentendo una maggiore efficienza e reattività nell'identificazione delle minacce e nella gestione degli eventi di sicurezza. Ecco alcune delle modalità in cui l'IA può essere applicata alle control room di sicurezza fisica:

1. Rilevamento automatizzato delle minacce: L'IA può essere addestrata per analizzare flussi di video provenienti da telecamere di sorveglianza e rilevare automaticamente comportamenti sospetti o anomalie. Ad esempio, può identificare intrusioni, oggetti lasciati incustoditi, movimenti insoliti o comportamenti violenti. Ciò consente agli operatori di sicurezza di rispondere rapidamente alle minacce e di prendere le misure appropriate.
2. Monitoraggio e analisi dei dati in tempo reale: L'IA può elaborare e analizzare grandi quantità di dati provenienti da diverse fonti, come sensori, telecamere e sistemi di controllo degli accessi. Questa analisi in tempo reale consente di individuare rapidamente le anomalie, identificare modelli di comportamento e segnalare situazioni di potenziale rischio.

New Chat

IA per control room sic

April

Cloud migration for public ad

Normative Approaches to AI

February

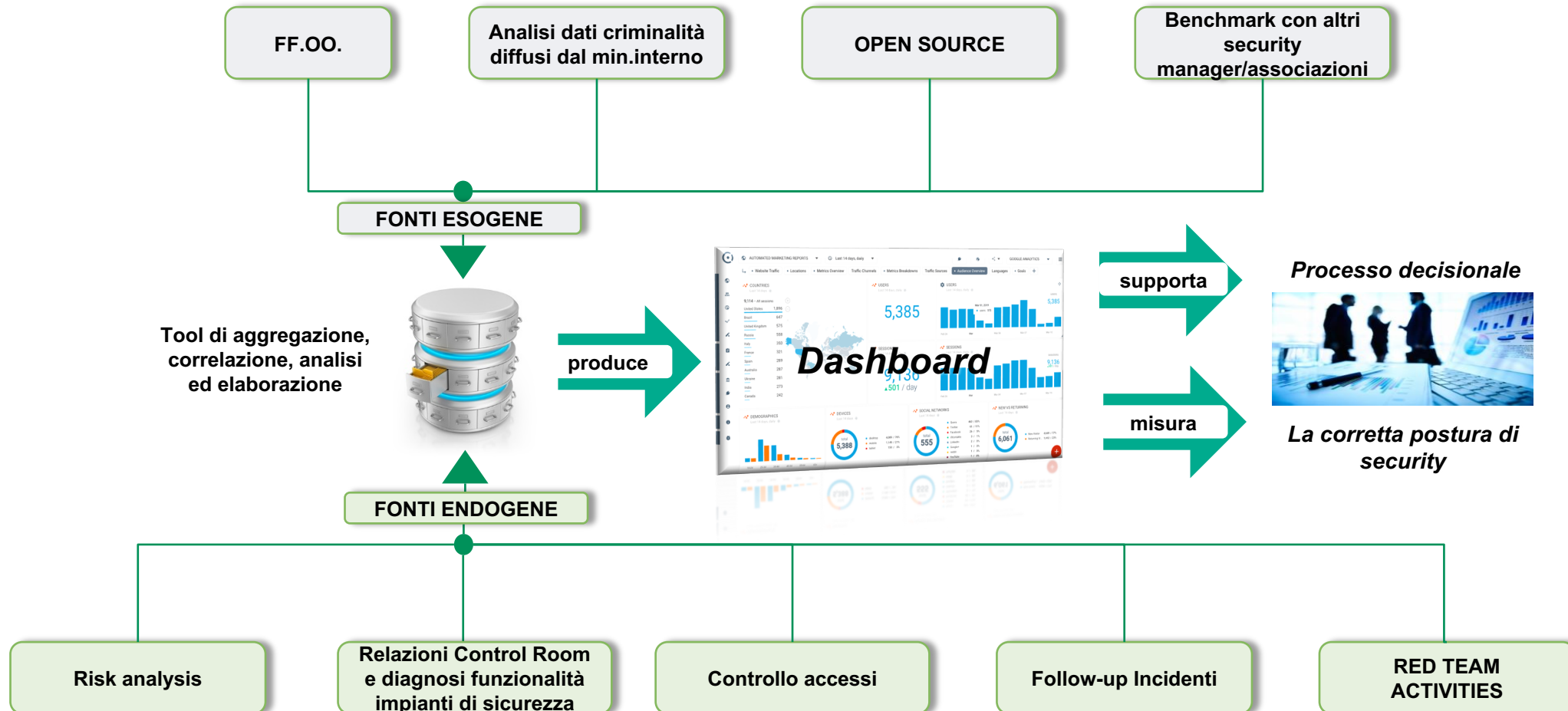
PPP per sostenibilità.

Rischi percepiti dagli italiani.

3. Integrazione dei sistemi di sicurezza: L'IA può integrare i diversi sistemi di sicurezza presenti in una control room, come telecamere di sorveglianza, allarmi antintrusione, rilevatori di fumo, ecc. Ciò consente di centralizzare e coordinare la gestione delle minacce, semplificando la visualizzazione e la risposta agli eventi di sicurezza.
4. Supporto decisionale: L'IA può fornire suggerimenti e raccomandazioni agli operatori di sicurezza sulla base dell'analisi dei dati e delle situazioni correnti. Ad esempio, può suggerire azioni appropriate da intraprendere in determinate situazioni di emergenza o fornire indicazioni sulla risposta più efficace a un evento di sicurezza.
5. Automazione dei processi: L'IA può automatizzare alcune delle attività ripetitive e di routine all'interno della control room di sicurezza, come la verifica dei permessi di accesso, la gestione delle credenziali degli utenti e la generazione di report. Ciò consente agli operatori di concentrarsi su compiti ad alto valore aggiunto e riduce il rischio di errori umani.

È importante sottolineare che l'implementazione di moduli di intelligenza artificiale richiede una pianificazione accurata e una buona integrazione con i sistemi esistenti. È necessario definire gli obiettivi specifici, raccogliere dati di qualità per l'addestramento dell'IA e garantire la privacy e la sicurezza delle informazioni trattate.

Il principale obiettivo di ogni manager: Dashboard Security Governance



Centralità dell'uomo

Il Security Manager è ancora centrale e ringraziando Dio serve ancora per impostare la governance e per farlo deve essere in grado di :



Una volta impostato il lavoro, lo strumento principe sarà la control room che dovrà essere sempre più somigliante ad un SOC e con ciò cambierà anche lo skill dell'operatore che si avvicinerà ad un analista con il valore aggiunto che avrà da gestire un allarme sempre meno generico ma ben diagnosticato perché a monte il sistema ha già valutato ed incrociato tutte le info utili e, quindi, se lo propone come allarme è molto probabile che sia reale.

Ovviamente centrale sarà anche il system integrator in grado di creare e proporre un device tailor made per il cliente.

...Per finire

Dopo che si è abbattuto un muro...
ci si parano davanti una infinita
serie di rischi e di opportunità.

- Attenzione a non cercare «scorciatoie» tramite i moduli di IA che si corre il rischio di schiantarsi
- Abbiamo, a tutti i livelli, il vantaggio della nostra esperienza e delle nostre conoscenze che non sono rimpiazzabili con nessuna altra cosa.
- Fondamentale individuare i partner flessibili pronti ad adattarsi ai nostri mindset ed alle esigenze del nostro business facendo attenzione che rispettino le peculiarità delle nostre esigenze



Una considerazione di 70 anni fa... più che mai attuale

**Temo il giorno in cui la tecnologia andrà
oltre la nostra umanità:**

il mondo sarà popolato allora da una
generazione di idioti.

Albert Einstein