Marco quest'anno di cosa parliamo?

Pier parla della evoluzione del cambio di passo che la sicurezza fisica dovrà compiere nel ....FUTURO....

…i maggiori cambiamenti della nostra professione

01 La situazione geopolitica in generale unita alla maggiore attenzione normativa per la sicurezza delle infrastrutture critiche ha ridato importanza alla sicurezza fisica

02 Indispensabile nel team avere sempre più competenze di risk analysis, competenze IT e di crisis management.

03 Capacità di gestire ed approfittare delle enormi soluzioni tecnologiche che ci vengono proposte compresa la «pericolosa» Intelligenza artificiale.

04 Cercare di anticipare i problemi con un approccio sempre più risk based avendo come principale obiettivo la prevenzione piuttosto che la reazione.

05 Trasformare la control room dandole funzionalità non solo operative ma anche di governance; la capacità di raccogliere info di vario genere DEVE essere sfruttata per misurare continuamente la postura di sicurezza fisica dell'organizzazione

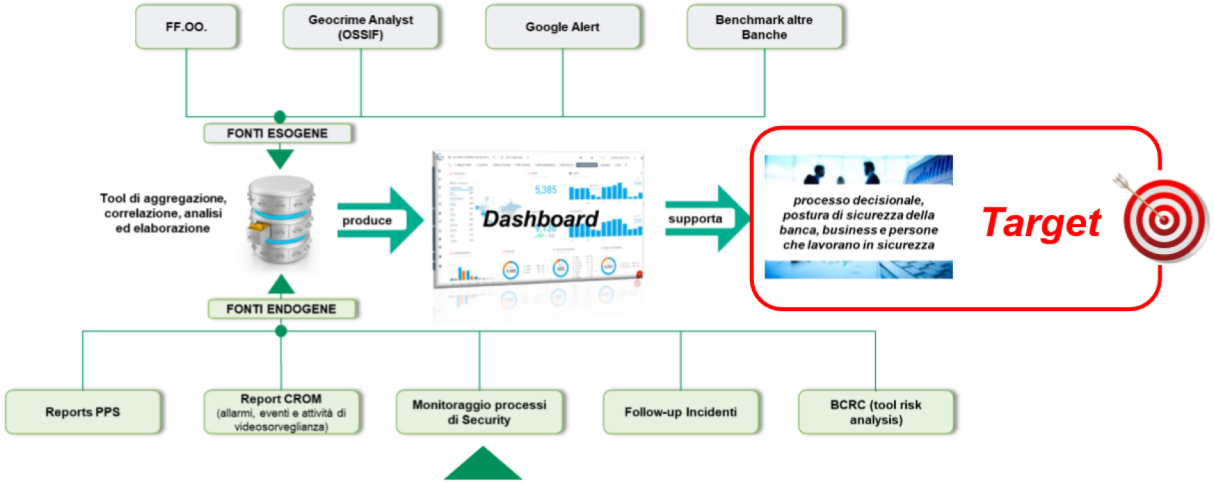
06 Organizzare continui assessment e penetration test sempre diretti alla misurazione continua della postura di sicurezza fisica con particolare riferimento alle infrastrutture critiche, agli HQS ed anche alle agenzie

Come stiamo gestendo l'ondata degli attacchi ATM

- Il team di **Physical Security Governance** emana degli specifici Alert per mutate condizioni di rischio che interessano un perimetro di ATM, da sottoporre ad un temporaneo abbassamento dei limiti di giacenza.
- Il team «**Network Support**» valuta se i limiti di giacenza richiesti da PSG sono applicabili ai punti vendita interessati, attraverso apposite analisi ed elaborazioni (es. tipologia di macchine, erogazioni medie dei dispositivi interessati). Il team «**My Day To Day**» supporta la valutazione del team Network Support fornendo elementi utili quali: regole, vincoli, limiti gestiti dal sistema di cash forecasting ed erogazioni medie dei dispositivi.
- Il team «**My Day To Day**» valuta gli impatti operativi/costi in caso di ATM internalizzati/esternalizzati per i dispositivi interessati (impatto sui costi interni/esterni).
- Il team «**Network Support**» e «**Network Trasformation»** valutano interventi strutturali sull'operatività del punto operativo.
- Se a valle delle valutazioni dei team di Business non vengono individuate criticità particolari, si procede con l'applicazione delle indicazioni fornite attraverso l'Alert. In caso contrario, viene convocata una «cabina regia» al fine di individuare eventuali soluzioni alternative stabilendo il corretto trade-off tra costi e rischi. Il Team «Network Support» da comunicazione alle singole Filiali.

Traguardi Security 2025: realizzazione dashboard di Physical Security Governance

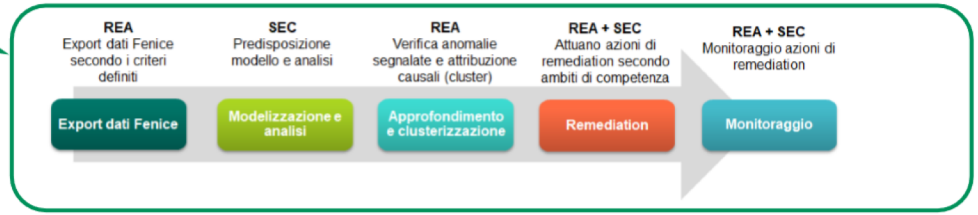
on 2025



Gli output di questo processo confluiranno tra gli INPUT della dashboard e sarà una delle fonti selezionate per il popolamento

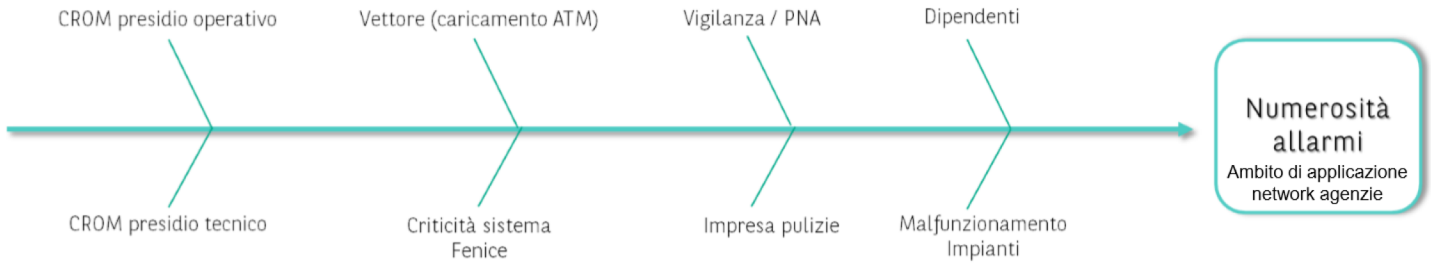
Fattore abilitante

Assicurare un RUN **stabile** del **processo** basato sulla **disponibilità e l'elaborazione affidabile di dati provenienti dalla control room**



Analisi dati della CROM & CRT

Le cause



Chi può intervenire per mitigare o rimuovere le cause

	REA			SECURITY	Riferimenti Nominativi
	Building Security Management	Security Projects and Systems Management	Facility and Energy Projects	Security	
A - PROBLEMATICA TECNICA (IMPIANTI O SISTEMI)		●			Ugolini/Rufini
B - ERRATO COMPORTAMENTO COLLEGA				●	Tutti (BNL -- Ppsitaly)
C - ERRATO COMPORTAMENTO VIGILANZA VETTORE (CARICO ATM)				●	Tutti (BNL -- Ppsitaly)
D - ERRATO COMPORTAMENTO TECNICI ATM				●	Tutti (BNL -- Ppsitaly)
E - ERRATO COMPORTAMENTO VIGILANZA/PNA	●				Florio
F - ERRATO COMPORTAMENTO ACCOGLIENZA CLIENTI	●				Florio
G - ERRATO COMPORTAMENTO PULIZIE			●		Reale
H - ERRATA OPERATIVITA' CROM		●			Miozzi/Rufini
I - ERRATA OPERATIVITA' CRT		●			Ugolini/Rufini
L - NO CLUSTER					NA
M - ALTRO	on demand	on demand	on demand	on demand	da individuare secondo competenza

Analisi dati della CROM & CRT

Overview (dati in aggiornamento)

Cluster	04/11/2024-10/11/2024	18/11/2024-24/11/2024	02/12/2024-08/12/2024	Totale complessivo
A - PROBLEMATICA TECNICA (IMPIANTI O SISTEMI)	17	15	18	50
B - ERRATO COMPORTAMENTO COLLEGA	19	20	19	58
C - ERRATO COMPORTAMENTO VIGILANZA VETTORE (CARICO ATM)		1	1	2
E - ERRATO COMPORTAMENTO VIGILANZA/PNA	1	2	4	7
F - ERRATO COMPORTAMENTO ACCOGLIENZA CLIENTI		1		1
H - ERRATA OPERATIVITA' CROM			2	2
L - NO CLUSTER	1	6	1	8
Totale complessivo	**38**	**45**	**45**	**128**

Perimetro interessato: 80 sedi

di cui 40 remediation **completate** (perimetro cluster A e H)

Le remediation assegnate da Security verranno attivate in occasione di appositi incontri con Rete Unica

Gli assessment di Physical security

Gli **obiettivi dell'assessment** sono:

- **misurare il livello di conformità/efficacia generale del sistema di sicurezza** posto in essere in corrispondenza del sito (misure di sicurezza attive, passive ed organizzative) rispetto agli standard attualmente in uso e applicati presso gli HQ anche effettuando dei penetration test per misurare la validità ed il rispetto delle procedure di accesso, la perfetta funzionalità degli impianti di sicurezza, la reattività della control room.
- **valutare il livello di rischio inerente e residuo** a cui i principali **asset del sito** sono esposti rispetto alle minacce **sabotaggio o furto (beni o informazioni), danneggiamento e atti vandalici, atti dimostrativi,** nonché rispetto ai principali rischi ambientali (fenomeni naturali o derivanti da attività umana)
- **Misurare la attenzione alla conservazione corretta di documenti, dotazioni informatiche (clean desk policy)**
- **Azione congiunta con i team di cybersecurity per verificare la corretta protezione fisica degli apparati IT**

… alla fine definire e **suggerire** i **prossimi passi** da attivare per la **mitigazione** dei **rischi residui** ed il **ripristino delle principali non conformità rilevate**

Processo di assessment

Plan

- Predisposizione dei controlli e pesatura
- Realizzazione degli strumenti a supporto delle verifiche e delle valutazioni
- Definizione della documentazione e delle informazioni da acquisire
- Individuazione dei referenti da coinvolgere per l'esecuzione delle attività
- Predisposizione del piano di Assessment
- Presentazione ed esposizione del piano

Do

- Interviste e raccolta di documenti, informazioni e dati utili ai fini delle verifiche da espletare
- Sopralluoghi presso il sito (totale 3) di cui una attività Clean Desk
- Compilazione di una check list costituita da 102 punti controllo (opportunamente pesati su una scala 1 – 4, dal meno importante al più rilevante) suddivisi nelle seguenti aree tematiche: Perimetro esterno alla sede, Perimetro della sede, Sistemi, Configurazioni e manutenzione, Organizzative.
  La check list costituisce uno strumento fondamentale ai fini della valutazione di efficacia delle misure.

Check

- Valutazione dei punti di controllo (conforme, parzialmente conforme, non conforme, non applicabile)
- Misurazione del livello di conformità per singolo punto di controllo
- Valutazione del livello di efficacia dell'intero sistema di sicurezza in essere (misure di sicurezza di tipo: attivo, passivo ed organizzativo) e reporting
- Asset inventory e valutazione degli impatti
- Valutazione dei rischi inerenti e residui

Act

- Presentazione degli esiti e degli interventi suggeriti per la mitigazione dei rischi e per il ripristino delle non conformità
- Trattamento dei rischi e delle non conformità rappresentate da parte del board

Grazie dell’Attenzione e perdonatemi se dico FORZA NAPOLI!!