

Settembre.2026

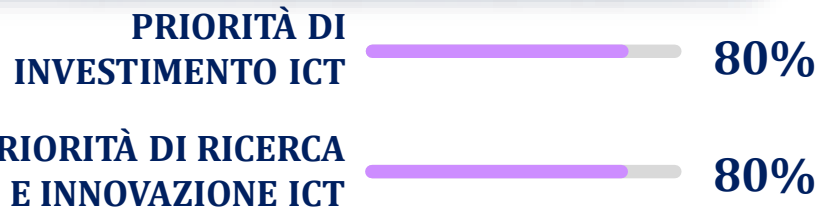
# AI Vs AI

LA NUOVA GUERRA SILENZIOSA DELLA CYBERSECURITY BANCARIA

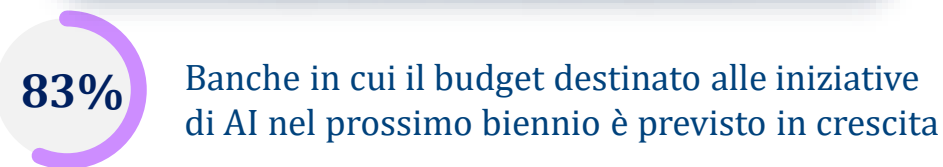
Marco Rotoloni, *Ricerca ABI Lab*



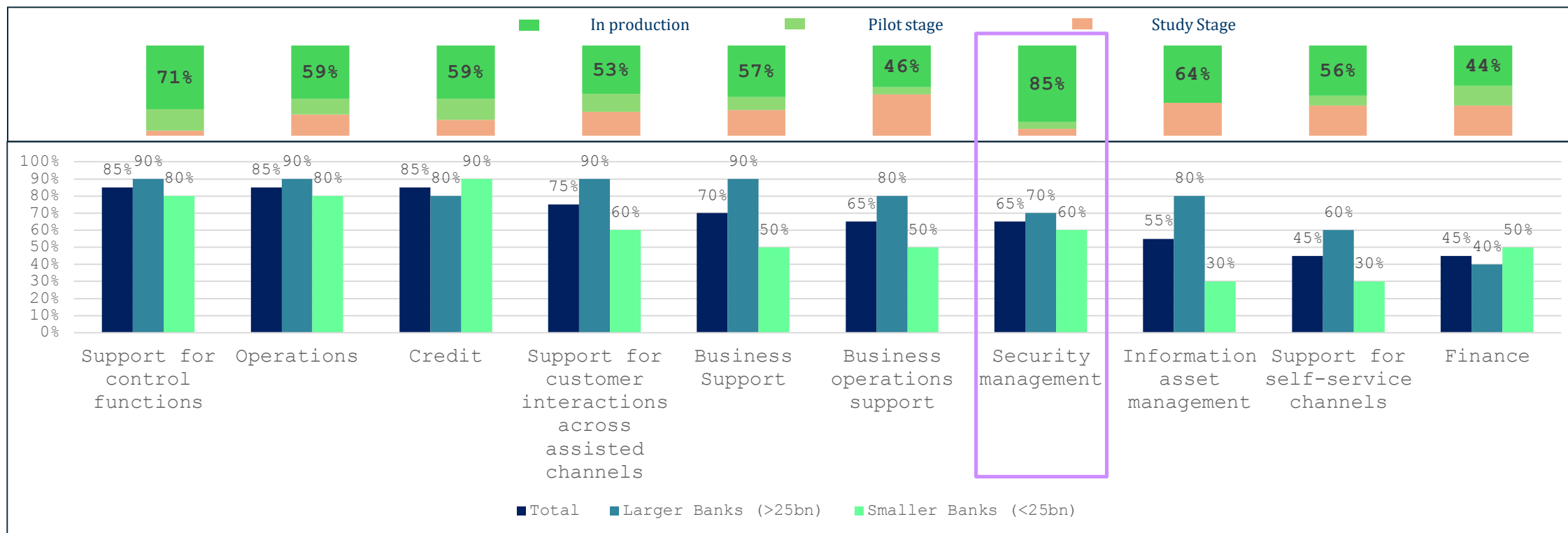
## AI: UNA PRIORITÀ STRATEGICA



## TREND DI INVESTIMENTO



### AMBITI DI APPLICAZIONE DELL'AI



# Nei SOC il vincolo all'adozione dell'AI è l'integrazione, non il modello

Dalle risposte raccolte emerge una domanda di automazione supervisionata, spiegabile e misurabile su indicatori operativi: tutti i rispondenti scelgono modelli che mantengono l'analista nel processo decisionale.

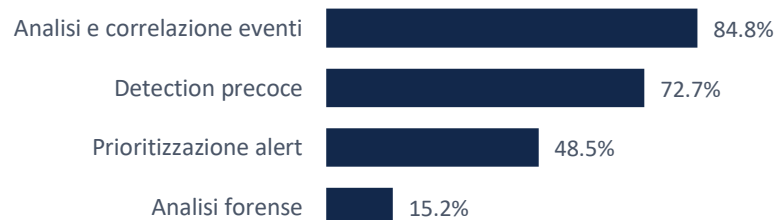
**39,4%** usa AI in SOC o CERT  
(15,2% in modo esteso)

**51,5%** la sta valutando,  
senza averla adottata

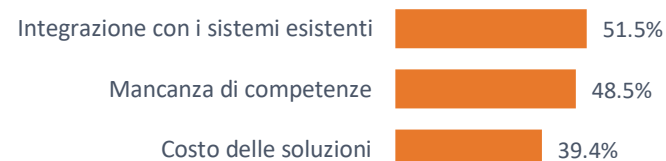
**30,3%** osserva l'espansione di  
attacchi  
automatizzati tramite AI

**72,7%** segnala il SOC spesso  
sommerso  
da falsi positivi (12,1%  
sempre)

## Attività in cui l'AI è ritenuta più utile



## Principali barriere all'adozione indicate



## Preoccupazioni di governance più ricorrenti

Scarsa trasparenza e spiegabilità 59,4% · responsabilità per azioni automatiche errate 53,1% · output distorti o bias 50,0%.  
32 rispondenti su 33 ne indicano almeno una.

## Livello di automazione preferito

**66,7%** automazione con supervisione dell'analista  
**33,3%** suggerimenti assistiti, decisione manuale  
**100%** *in entrambi i casi l'analista resta nel processo decisionale*

## Integrazioni più citate (n=23)

**82,6%** integrazione con il SIEM

TIP e MISP 47,8% · vulnerability management 43,5%

## Metriche di valutazione critiche (n=33)

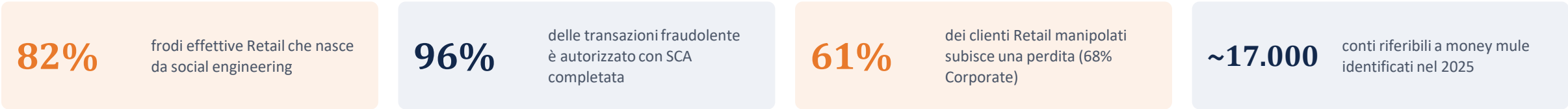
**75,8%** misurazione sul MTTD

**72,7%** riduzione dei falsi positivi

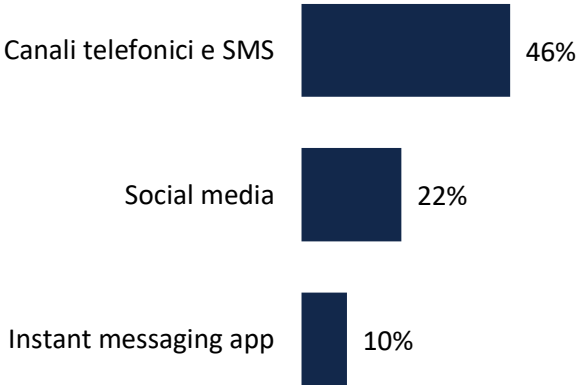
**Chiavi di lettura e questioni aperte per le banche.** Le evidenze sembrano indicare che il contributo dell'AI nei SOC dipenda meno dal singolo modello e più dall'integrazione con SIEM, TIP e vulnerability management e dalla disponibilità di competenze. Può risultare utile definire in anticipo le metriche di valutazione (MTTD, tasso di falsi positivi) e il livello di spiegabilità richiesto agli output. Resta aperto il tema dell'attribuzione delle responsabilità sulle azioni automatiche e del raccordo con i presidi di governance e di controllo già esistenti.

# Sul fronte frodi l'asimmetria è nella scala della manipolazione, non nei controlli

L'attacco si sposta su canali digitali facilmente industrializzabili e sfrutta il cliente autenticato; sul lato difesa l'AI è presente in un quarto delle soluzioni di monitoraggio, in linea con la rilevazione precedente.



## L'innescò si sposta su canali digitali scalabili (Focus su Retail)



L'abuso dei canali telco scende dal 60% (2024) e dall'87,5% (2023). Tra le tecniche Retail prevalgono falsi investimenti (36%) e task scam (25%); nel Corporate la Business E-mail Compromise pesa per il 23% delle frodi effettive.

## Il presidio automatizzato oggi in esercizio



## Il tempo utile si accorcia

Il bonifico istantaneo nazionale concentra quasi il 50% delle frodi effettive Retail per numerosità: la finestra di valutazione si riduce a pochi secondi e la decisione ricade sui sistemi automatici prima che sull'analista.

## Che cosa sposta il baricentro dell'AI in difesa

Lettura ABI Lab delle evidenze

- Il punto di applicazione non è più il blocco dell'accesso, ma il riconoscimento del comportamento anomalo di un cliente autenticato.
- Una parte della manipolazione avviene fuori dai canali bancari, dove la banca non ha visibilità diretta sul contatto iniziale.
- Con l'istantaneo la decisione si sposta sul modello: aumenta il peso di falsi positivi, spiegabilità e gestione delle contestazioni.
- La cooperazione tra PSP (+50% di importi recuperati) alimenta segnali e scenari condivisi, oggi poco valorizzati in chiave automatica.