



NetEye Conference 2026

AI & Human Insight: la coesistenza strategica per le IT Operations

Il SOC aumentato

Analisti umani e AI agentiche
nella difesa quotidiana

Goldoni Lorena & Paternoster Alessio



Agenda

- I problemi dell'analista
- AI Assistant & Attack Discovery
- Analisi manuale vs Workflow AI

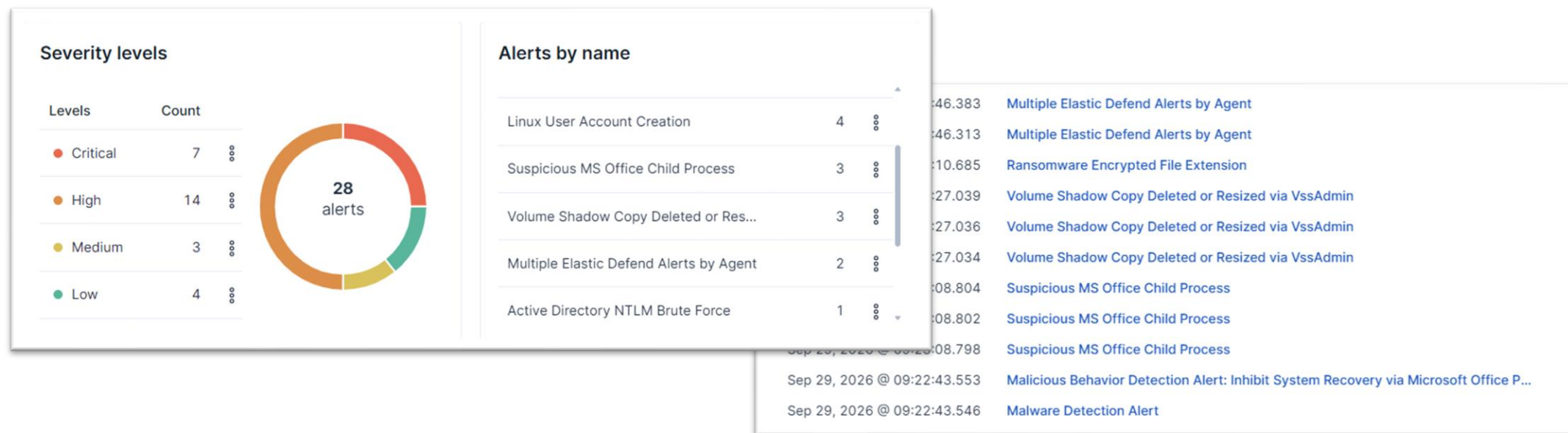
IL FILO CONDUTTORE

**Dalla raccolta
manuale delle prove
alla comprensione
assistita del contesto.**

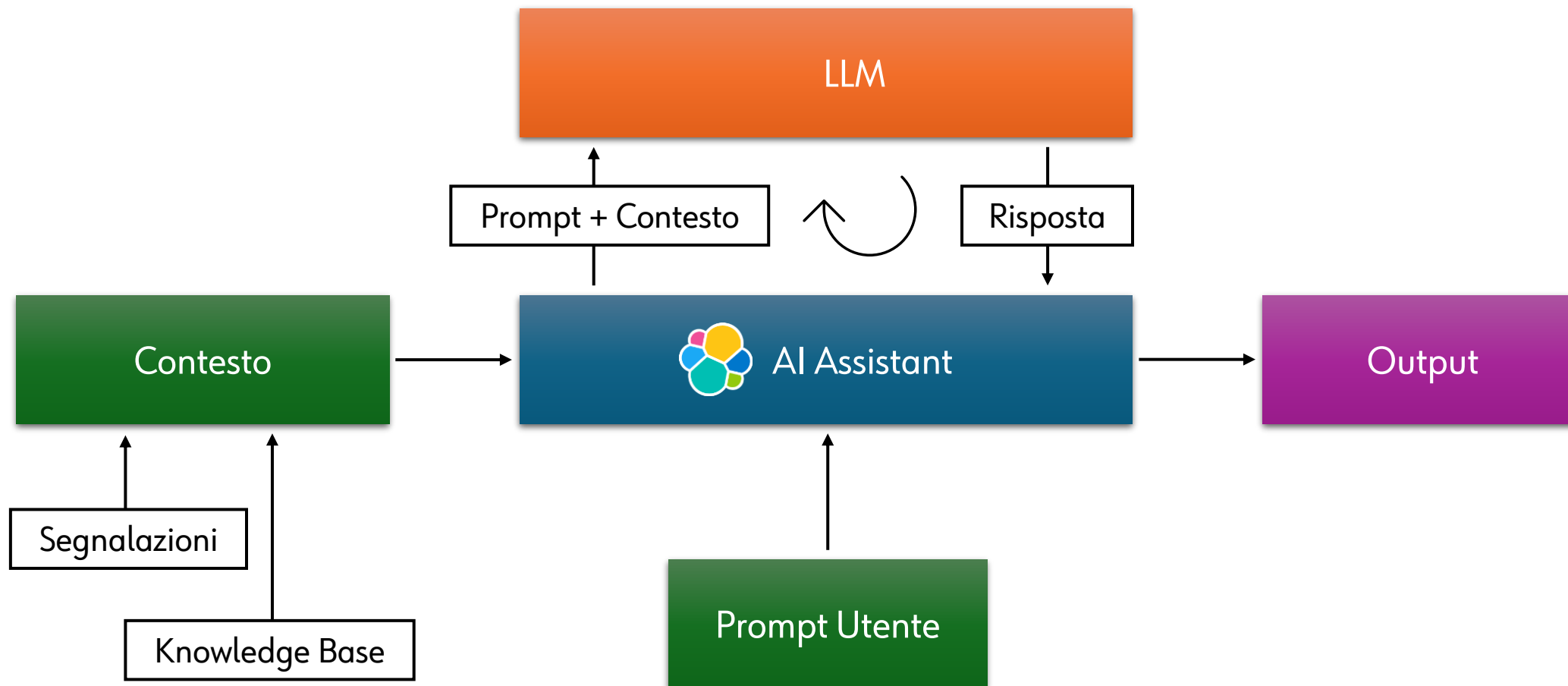
**NESSUNA
BLACK BOX**

I problemi

- Numerose segnalazioni da fonti differenti
- Identificazione dei comportamenti più critici
- Mancanza di una visione globale di ciò che sta accadendo
- Difficoltà nella stesura di una sintesi chiara e strutturata



La soluzione: AI Assistant



Un aiuto ulteriore: Attack Discovery

- Identificazione delle catene di attacco (*Kill Chain*) in modo automatizzato
- Sintesi chiara ed struttura di ciascun comportamento
- Associazione delle tattiche MITRE ATT&CK®

Ransomware Simulation with Shadow Copy Deletion [Open](#)

Detected on Sep 29, 2026 @ 09:56:10.162 | Run by: **W** | Ransomware simulation on **winwks01-sec** by **Administrator**

Attack summary Alerts **5**

Ransomware simulation on **winwks01-sec** by user **Administrator** involved malicious Office execution and shadow copy deletion.

Details

- Initial execution of malicious document **WINWORD.EXE** with command line staging **C:\Users\administrator...** on host **winwks01-sec** by user **Administrator**.
- The **quickbuck.exe** process was launched by **WINWORD.EXE** and executed ransomware simulation commands.
- quickbuck.exe** spawned **vssadmin.exe** with command **vssadmin delete shad...** to delete volume shadow copies, inhibiting system recovery.
- This sequence shows a clear ransomware attack chain from initial access via malicious Office document to impact stage on **winwks01-sec**.
- User **Administrator** is the principal actor in this chain.
- No evidence links this chain to other hosts or lateral movement, indicating an isolated ransomware simulation event.

Attack Chain

Reconnaissance Resource Development **Initial Access** **Execution** Persistence Privilege Escalation Defense Evasion Cr

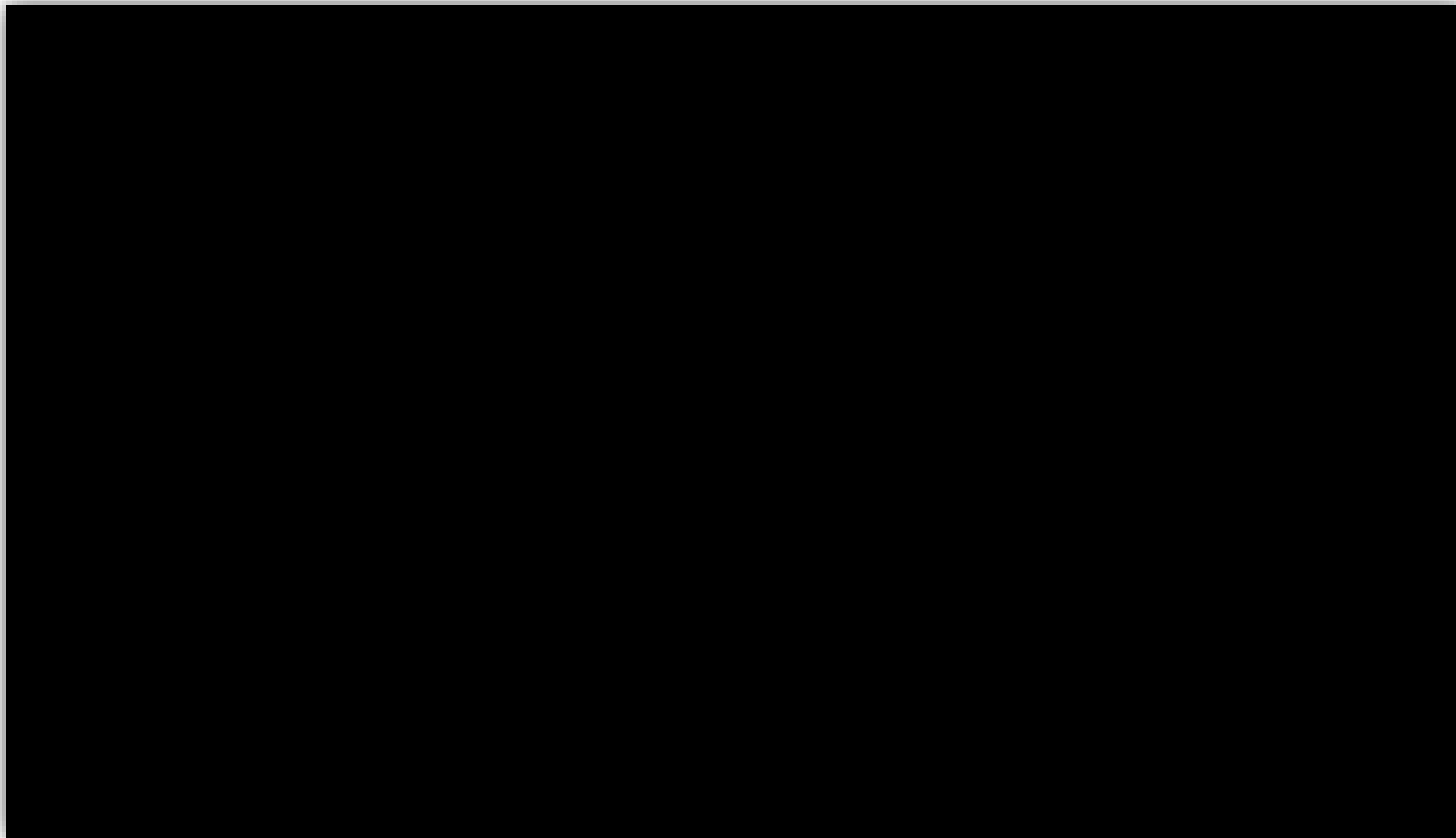
2 attacks detected

Attack name	Alerts count
Ransomware Simulation with Shadow ...	5
Defense Evasion and Admin Enumerati...	4

Rows per page: 10 [<](#) [1](#) [>](#)

Scenario di esempio: QuickBuck

Il simulatore ransomware ideato e sviluppato dal ricercatore Florian Roth





Analisi manuale vs Workflow AI



01 – Analisi manuale

Il problema non è la mancanza di dati. È il costo di ricomporli.

Ogni alert riparte dallo stesso punto: raccogliere, correlare, decidere, aggiornare.



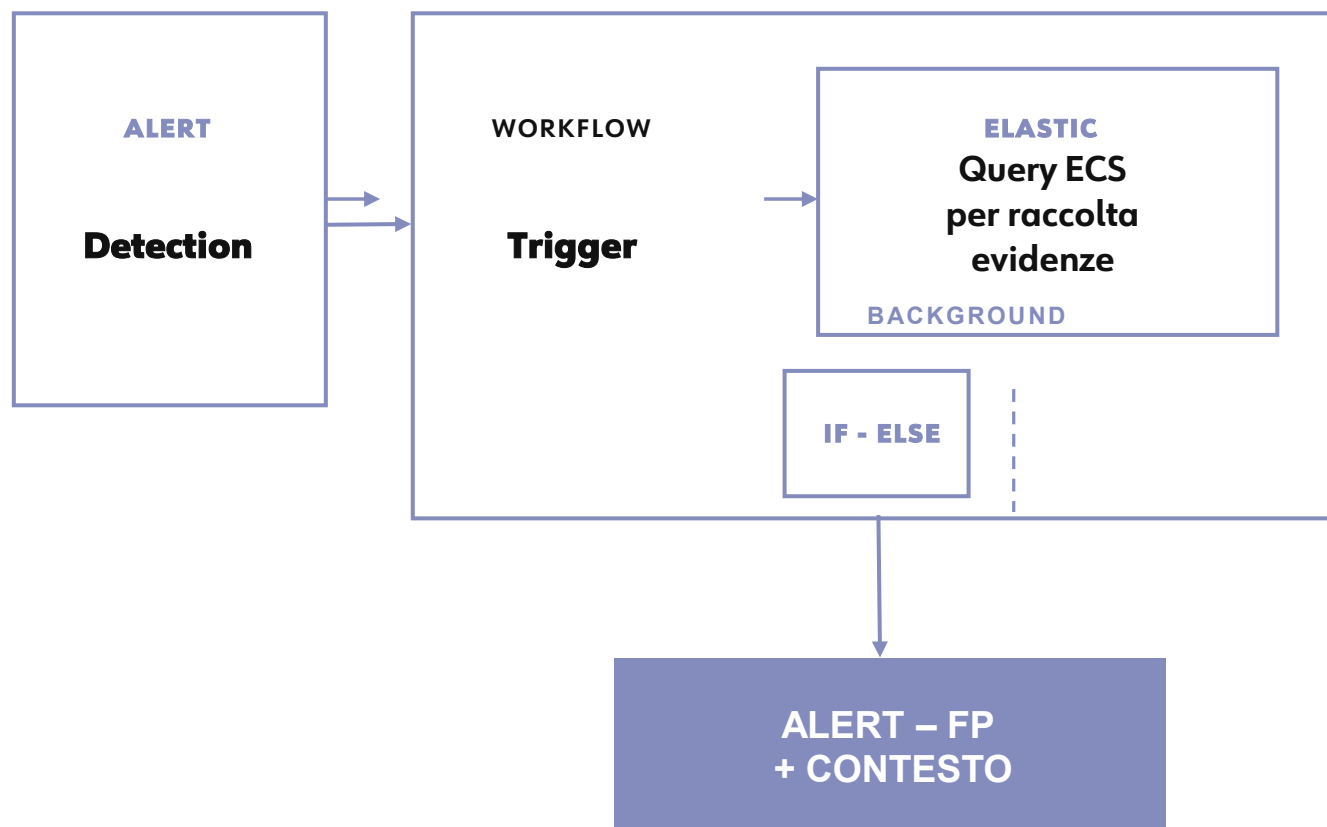
**TEMPO IMPIEGATO
SOLO SU CONTROLLI
RIPETUTI**

EFFETTO attenzione frammentata · tempo assorbito dal prevedibile · qualità dipendente dal carico



02 – Analista + Workflow

Il miglioramento è operativo e deterministico -
stessa policy, stesso controllo, stesso audit.



COSA MIGLIORA

Velocità
Coerenza
Tracciabilità

Il workflow non interpreta
l'ambiguità: esegue bene i
controlli già noti.

AD Brute Force

Un controllo deterministico che mostra cosa significa automatizzare senza perdere il controllo

IL CONTROLLO

È presente un cambio/reset password recente?

EVENT ID	4723 / 4724
IDENTITÀ	stesso user.name
FINESTRA	48 ore precedenti

SÌ

tag + chiusura
controllata
misconfiguration

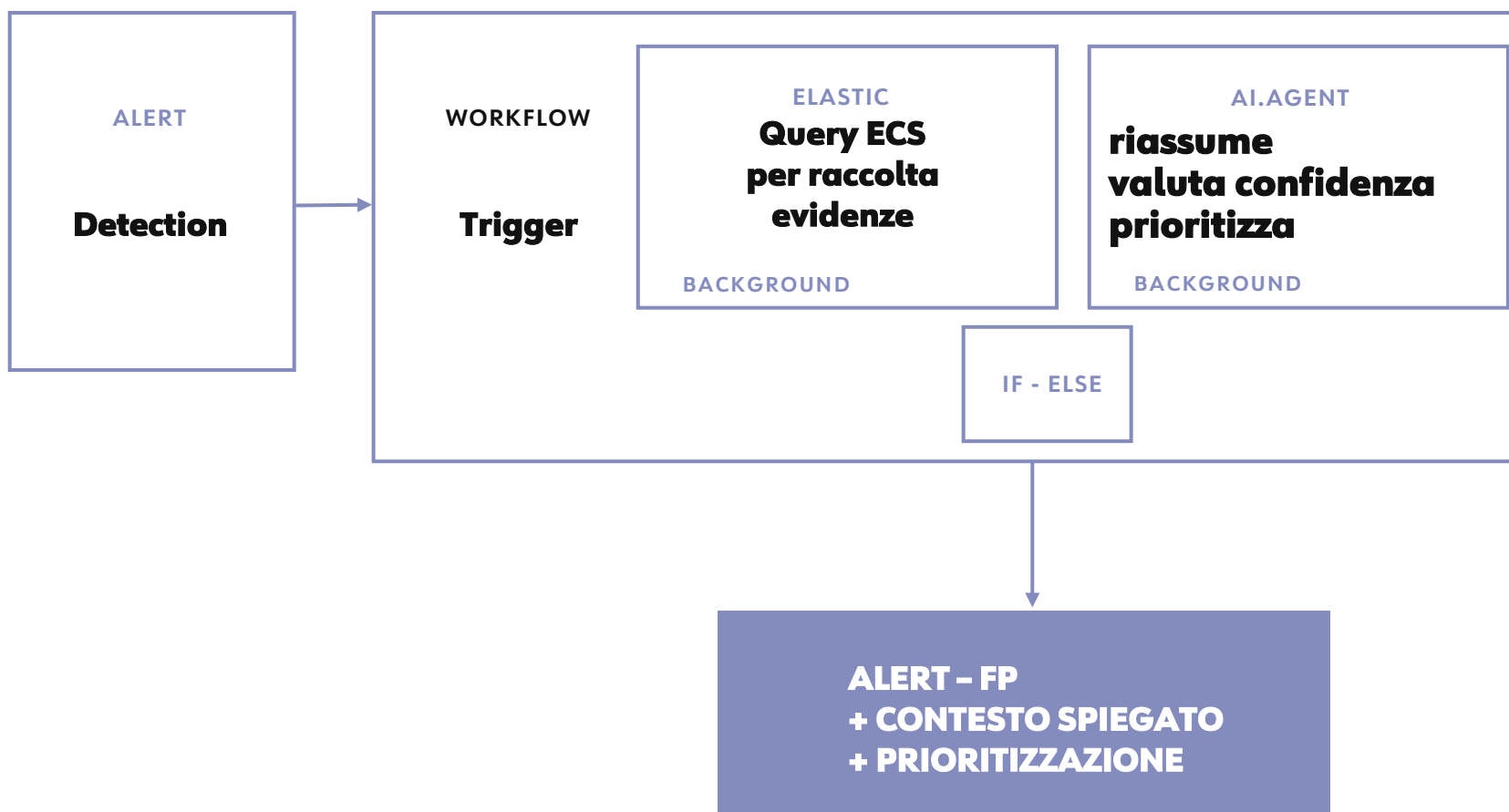
NO

alert aperto
per analisi umana

RETRY · ERROR HANDLING · LOG

03 – Analista + Workflow + AI.agent

L'agente riceve evidenze strutturate dal workflow e produce una proposta



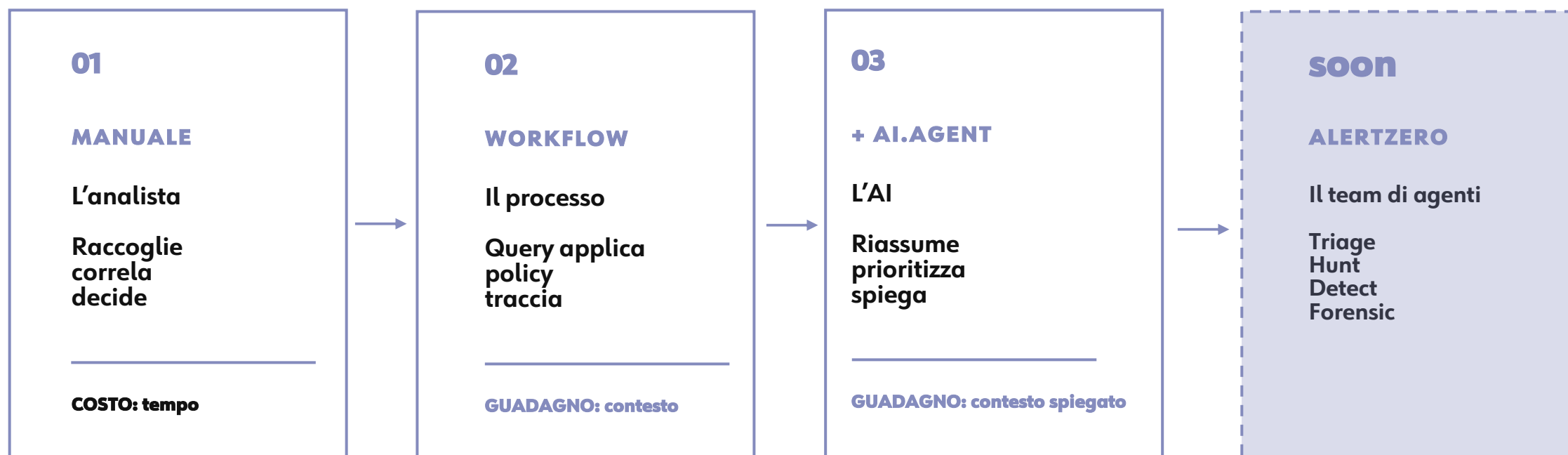
COSA AGGIUNGE L'AI

Comprensione
Priorità
Spiegazione

Non apre una via libera: la soglia e la policy decidono se una proposta può guidare l'azione.

Sintesi

Tre stati, tre miglioramenti diversi



WORKFLOW = esecuzione • AI = interpretazione • ANALISTA = responsabilità



Grazie per l'attenzione!

Domande?

