



NetEye Conference 2026

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

Dalla curiosità alla pratica

*Integrare l'IA nelle attività di red team:
la nostra esperienza con RTO*

Federico Corona

Red Team & Offensive Security Specialist



RTO: il punto di partenza

Red Team Orchestrator. La nostra piattaforma per organizzare e avviare le attività di assessment.



Operatore

Verifica delle evidenze e preparazione del report finale



Siamo partiti da una curiosità

- L'IA può rendere **più rapidi** alcuni passaggi del nostro lavoro?
- Come se la cava quando deve **prendere una decisione**?
- Che cosa **riesce a trovare** usando i nostri tool?



Dove abbiamo coinvolto l'IA

Preparare

un piano di test

Scegliere da dove partire in base all'obiettivo e ai tool disponibili.

Valutare

come proseguire

Leggere i risultati e valutare se e cosa approfondire.

Organizzare

i risultati

Riunire quanto emerso, distinguendo i riscontri dai punti da verificare.



Perché abbiamo scelto questa integrazione

**Partire da ciò
che conosciamo**

Strumenti e processi già presenti in RTO.

**Sperimentare
per gradi**

Affidare all'IA compiti circoscritti e osservarne il comportamento.

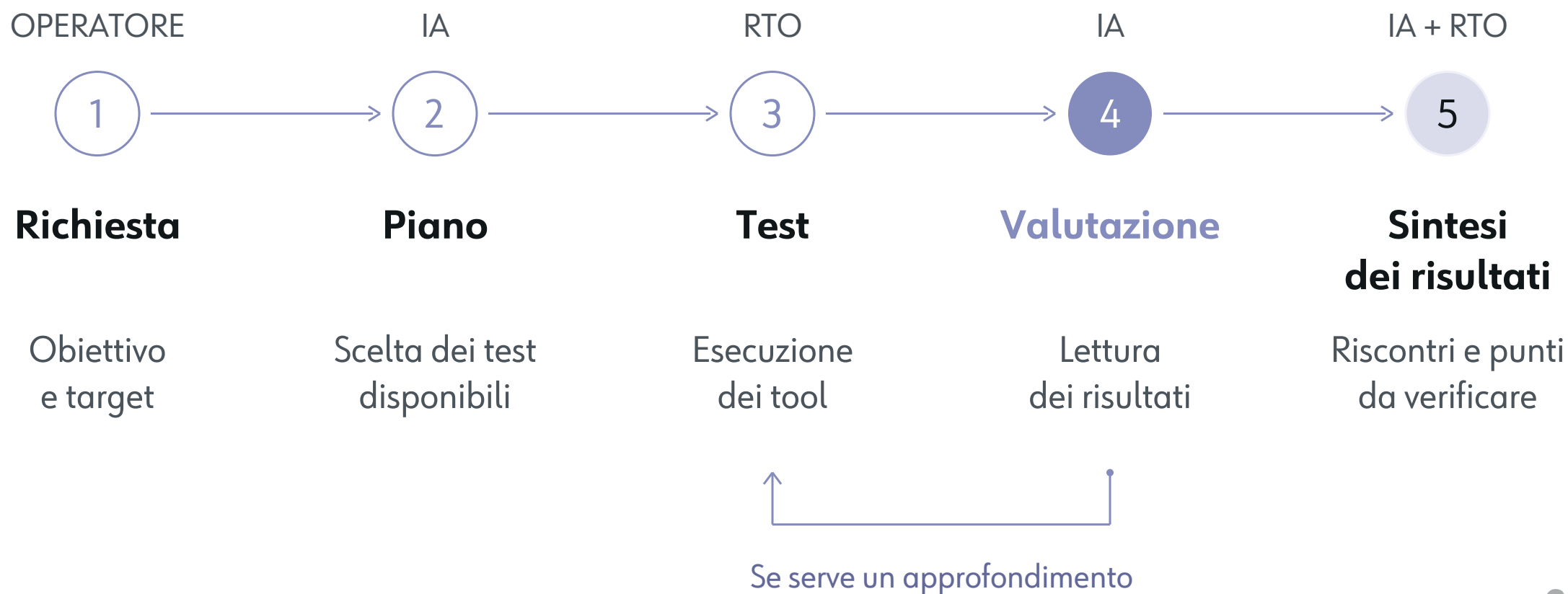
**Mantenere
il controllo**

Decidere quali scelte delegare e come eseguire le azioni proposte.



Come funziona, in pratica

GPT-5.4 via Azure Foundry



Quanta autonomia le concediamo oggi

- **Obiettivo e target**

Definiti dall'operatore.

- **Workflow disponibili**

Solo quelli con tag tool presenti nel catalogo.

- **Test e approfondimenti**

Limiti al numero di esecuzioni e ai cicli di approfondimento.

Verifica finale obbligatoria

Un operatore controlla sempre i risultati e le evidenze.



I primi riscontri

Piani di test più mirati

Un catalogo ben descritto aiuta a scegliere i tool per lo scenario.

Consumo di token elevato

La quantità di log elaborati pesa sul consumo del modello.

Scope da presidiare

I confini dell'assessment devono restare espliciti per tutto il ciclo.



Le prossime sperimentazioni

Fin dove può arrivare un LLM in un'attività di Pentesting?

- Provare modelli con capacità più avanzate
- Dare maggiore flessibilità nell'uso dei tool
- Valutare quali vulnerabilità riesce a individuare e con quali evidenze



Demo: dalla CLI a SysReptor

Il punto di partenza: la CLI

```
4      Set context (create/select)
5      Run command
V      Start VAPT
W      Start WAPT
A      Start VA (host-discovery → Greenbone)
I      Run AI Assessment
```

Richiesta

→ Piano e test

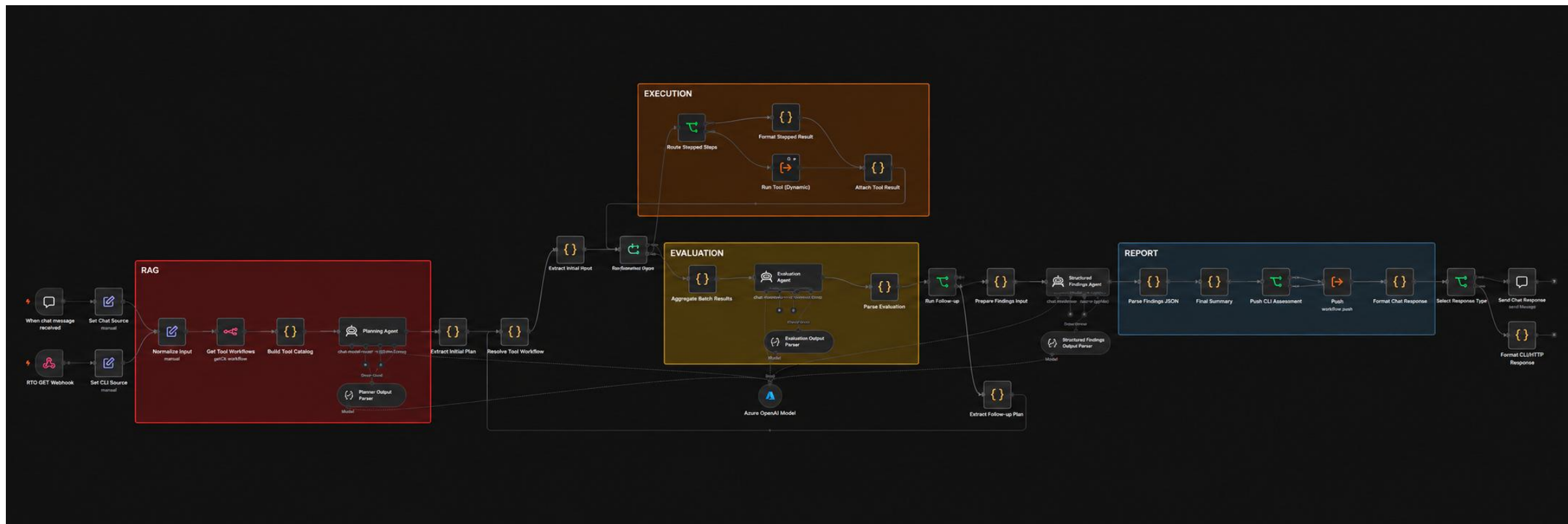
→ Valutazione

→ Sintesi su SysReptor



Il workflow dietro la demo

Pianificazione, test, valutazione e sintesi in n8n.



Seguiamolo dalla CLI fino a SysReptor.



Grazie per l'attenzione!

Domande?

Federico Corona

Red Team & Offensive Security Specialist



Red Team – Questo è ciò che possiamo fare per voi

Assessment e sviluppo

VA/PT

WAPT

SSDLC Assessment

Red teaming

Red Teaming

Threat-Led Penetration Test
(compliance normativa DORA)

Physical Access

Cloud

CSPM (Cloud Security Posture Management)

Cloud Red Teaming

Cloud Threat Emulation

Simulazioni mirate

Social Engineering

Ransomware

DDoS

Credential Dump & Exfiltration

ClickFix & Exfiltration

Scan / Enumeration

Purple Teaming

Sistemi IA

AI Assessment /
Red Teaming

Sicurezza e robustezza
dei sistemi di IA

