Red Hat Summit

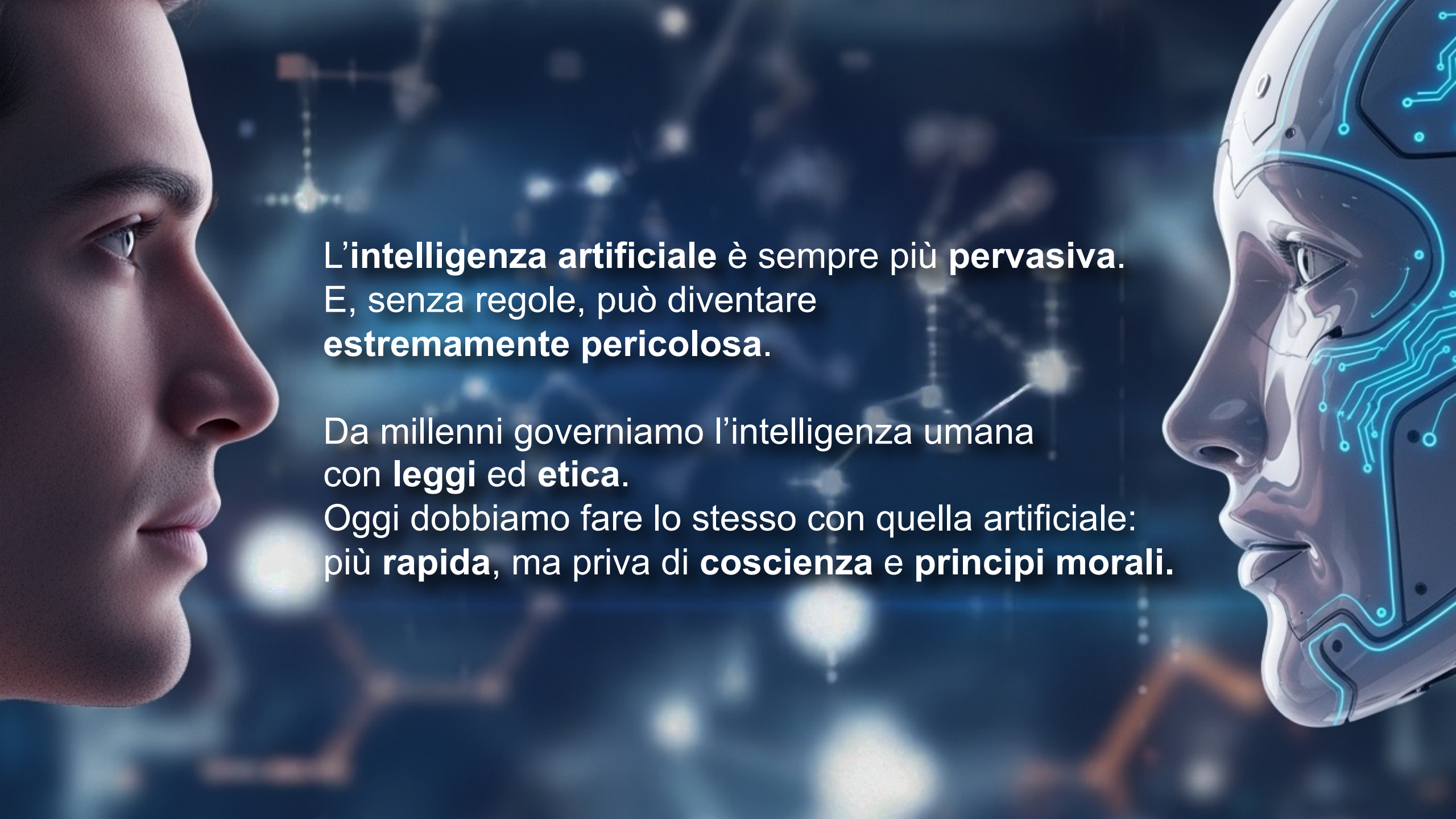
Connect

AI REGOLATA:
Strategie per applicazioni sicure e conformi

Claudia Leati, *Head of Solutions*, Mauden
Daniele De Natali, Technology Leader, Data, AI & Automation, Mauden

mauden
A RICOH Company

Red Hat


L’**intelligenza artificiale** è sempre più **pervasiva**.
E, senza regole, può diventare
estremamente pericolosa.
Da millenni governiamo l’intelligenza umana
con **leggi** ed **etica**.
Oggi dobbiamo fare lo stesso con quella artificiale:
più **rapida**, ma priva di **coscienza** e **principi morali.**

NORMATIVE AI NEL MONDO

Panoramica globale e focus su Europa e Italia

EUROPA (EU)
AI Act (2024)
Prima legge vincolante al mondo. Approccio basato sul rischio con sanzioni fino a €35M

STATI UNITI (US)
Executive Order (2023) + regolamentazioni statali (California, NY).
Framework volontario NIST AI RMF

CINA (CN)
AI Regulations (2023–2024)
Focus su content labeling, algoritmi di raccomandazione e deepfakes

REGNO UNITO (GB)
Pro-innovation approach
Framework flessibile con 5 principi chiave senza nuove leggi specifiche

GIAPPONE (JP)
AI Basic Law (2024) + AI Guidelines for Business
Promozione AI responsabile e trustworthy

ALTRE REGIONI
Canada, Singapore, Australia
Strategie nazionali AI con principi etici e governance frameworks

EUROPA
Il quadro normativo

AI ACT | GDPR | DORA | DORA | DATA GOV ACT | DIGIT SERV ACT

AI ACT
Classificazione basata sul rischio (inaccettabile, alto, limitato, minimo).
Obblighi di trasparenza, documentation, human oversight.
Effettivo dal 1° agosto 2024, piena applicazione entro 2026.

ITALIA
Implementazione Nazionale

LEGGE 132/2025 | STRATEGIA IA 2024–2026 | AUTORITÀ AI

OBIETTIVI PRINCIPALI
Armonizzazione con AI Act, promozione innovazione, utilizzo trasparente e responsabile dei sistemi AI

GOVERNANCE
Autorità nazionale AI per supervisione, certificazione e sandbox regolamentari per sperimentazione

SETTORE GIUSTIZIA
Dimensione antropocentrica, divieto decisioni automatizzate senza supervisione umana nel processo giudiziario

COMPLIANCE INTEGRATA
Coordinamento con GDPR, NIS2 (cybersecurity), DORA (resilienza finanziaria) per approccio olistico

LA NORMATIVA AI IN SINTESI

AI Act (UE) e Legge di Armonizzazione Italiana

EU AI Act: Rischio & Obblighi

Classificazione sul rischio

🚫 **RISCHIO INACCETTABILE**
Social scoring, manipolazione, sorveglianza biometrica massiva
👉 **VIETATO**

⚠️ **RISCHIO ALTO**
Infrastrutture critiche, istruzione, recruiting, giustizia
👉 **Obblighi stringenti**

ℹ️ **RISCHIO LIMITATO**
Chatbot, deepfakes, sistemi di raccomandazione
👉 **Trasparenza**

✅ **RISCHIO MINIMO**
Videogiochi, filtri spam, assistenti virtuali base
👉 **Uso libero**

Italia: Armonizzazione & Strategia

Legge 132/2025 (Armonizzazione)

🏛️ **GOVERNANCE & OBIETTIVI**
Autorità nazionale AI e **Sandbox** regolamentari.
Armonizzazione con AI Act e promozione innovazione.
Integrazione con **GDPR, NIS2, DORA.**

⚖️ **SETTORE GIUSTIZIA**
Approccio **antropocentrico** e supervisione umana obbligatoria.
Divieto di decisioni automatizzate.

Strategia Italiana IA 2024–2026 (Pilasti)

👩‍💼 **Talenti:** Formazione e upskilling forza lavoro.
🔬 **Ricerca:** Investimenti in hub tecnologici.
🏢 **PA:** Adozione AI nei servizi pubblici.
🤝 **Framework Etico:** Sviluppo responsabile.

Sanzioni EU AI Act (Violazioni Gravi)

🔴 **MASSIMO (SISTEMI VIETATI)**
Fino a **€35M** o **7%** fatturato annuo globale.

🟡 **GENERALE (ALTO RISCHIO)**
Fino a **€15M** o **3%** fatturato annuo globale.

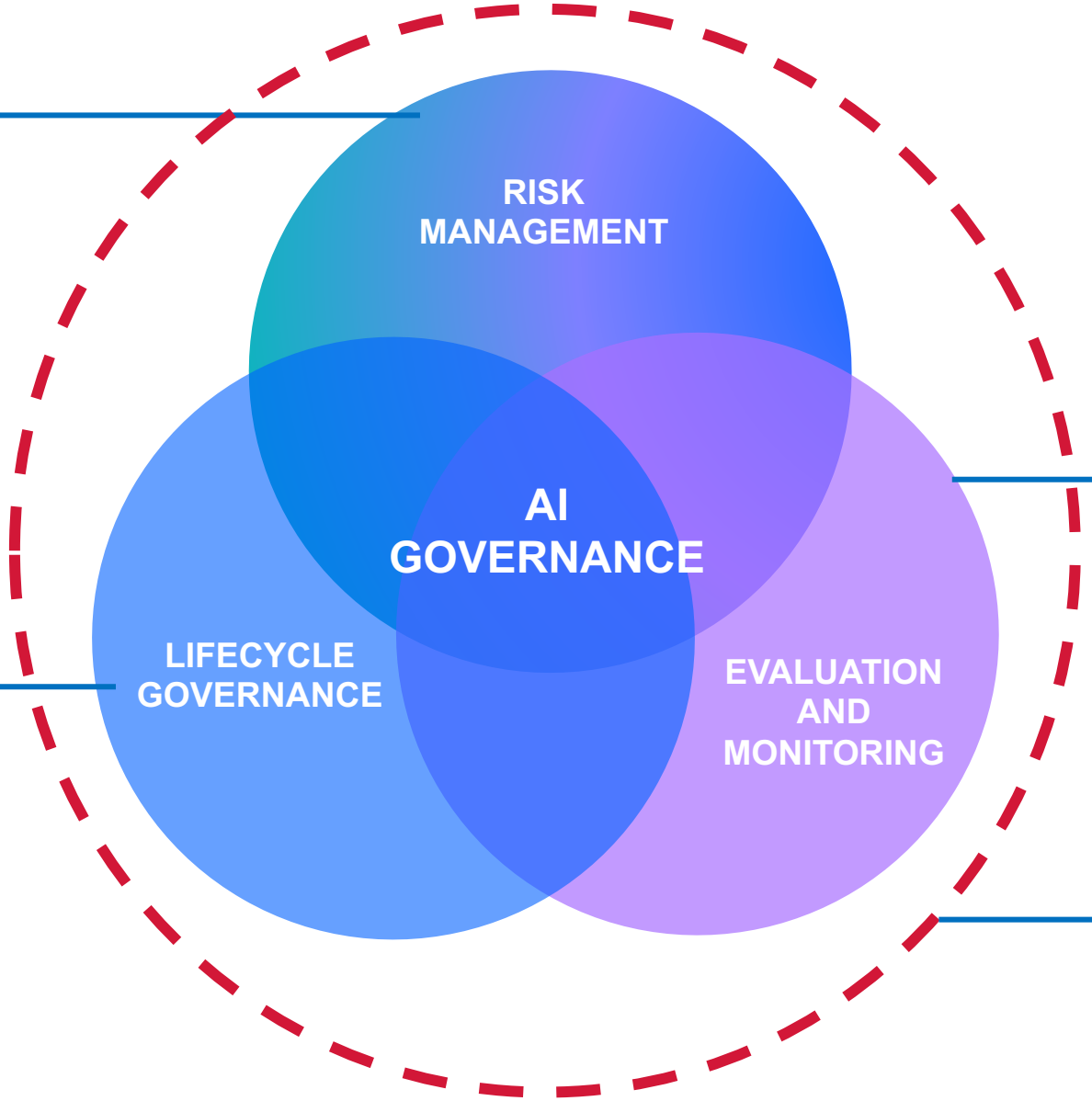
È importante partire da una premessa fondamentale: l'Italia, con il recente DDL Senato 1146-B, e l'Europa, con l'EU AI Act, stanno costruendo un framework normativo essenziale per la governance e la sicurezza dell'AI.

COSA È L'AI SICURA

4 AMBITI

1 CAPIRE
Flussi di lavoro, dashboard per la gestione dei rischi e dei problemi

2 CREARE
Acquisisci i dati salienti del modello durante l'intero ciclo di vita (AIOps)



4 CONTROLLARE
Monitoraggio continuo per accuratezza, deriva, polarizzazione, spiegabilità e prestazioni

3 PROTEGGERE
Sicurezza e resilienza del modello e del processo AIOPs di gestione

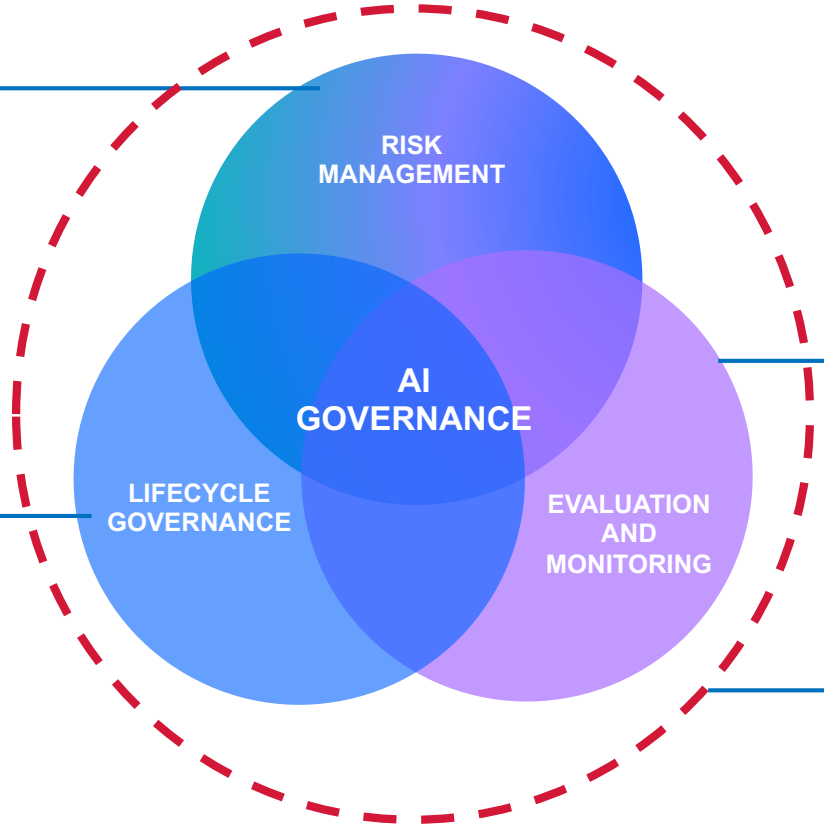
REDHAT PER APPLICAZIONI AD ALTO RISCHIO

1 CAPIRE
Flussi di lavoro, dashboard per la gestione dei rischi e dei problemi

2 CREARE
Acquisisci i dati salienti del modello durante l'intero ciclo di vita (AIOps)

3 PROTEGGERE
Sicurezza e resilienza del modello e del processo AIOPs di gestione

4 CONTROLLARE
Monitoraggio continuo per accuratezza, deriva, polarizzazione, spiegabilità e prestazioni



Red Hat OpenShift AI

Red Hat Service Mesh

Red Hat Quay

Red Hat Advanced Cluster Security

IBM watsonx.governance

RedHat OpenShift Container Platform

Red Hat Developer — Trustworthy AI Framework

IBM — AI Ladder - AI Ethics Framework - DataOps Methodology - Trustworthy AI

STRUMENTI SW E UTILIZZO NELLA GOVERNANCE AI

STRUMENTO	QUANDO USARLO	PERCHÈ USARLO
RedHatOpenShift Container Platform	**Piattaforma di base** su cui tutti gli altri strumenti si poggiano	Astrazione completa della piattaforma, architettura, modalità di deploy, rispetto alla locazione fisica apparati. Fornisce tutti i servizi di HA, scalabilità, DR, bilanciamento, integrazione CI/CD, automazione
IBM Watsonx.Governance	Fornisce le funzionalità di **valutazione e gestione rischio AI**, **gestione documentazione dei modelli** e del loro live cycle, gestione della **misura a runtime della performance etica** dei modelli	Piattaforma integrata sia con gli ambienti di sviluppo che di runtime (inferenza) consente di «governare» il ciclo di vita delle soluzioni AI based ad alto rischio e validazione di contenuto output
RedHat OpenShift AI **+** **IBM Watsonx.ai**	La fase di sviluppo viene **integrata con gli obblighi di governance nelle applicazioni ad alto rischio** . Ambienti di sviluppo integrati al contesto	Integrazione «gentile» sollevando gli sviluppatori da obblighi normativi, fornendo inoltre una serie di wizard, SDK, acceleratori di sviluppo estremamente utili ed efficienti.
RedHat QUAY	Una soluzione AI è costituita da molti container interoperanti, alcuni contenenti componenti AI specifiche (modelli e simili). Il **rilascio di questi è un momento importante e delicato**	Un gestore delle immagini di soluzione sicuro, resilente, scalabile e senza lock–in è un elemento qualificate per una applicazione sicura. Prevenire gli attacchi per non «avvelenare le immagini di base» è una ottima strategia.
RedHat Advanced Cluster Security	La **protezione della applicazione** e della soluzione passa durante lo sviluppo di tutto il ciclo della applicazione containerizzata sia in ambiente on prem ,hybrid e cloud	Prima si protegge l'applicazione, l'architettura e poi si protegge il contenuto (output). Un anello della catena debole, mina la sicurezza della applicazione e delle nostre aziende
RedHat Service Mesh	Una soluzione applicativa AI tende rapidamente a riassumere la struttura «grafi a spaghetti». Il **disordine va organizzato** specialmente in presenza di AI molto veloci e cangianti nel tempo	Governare il flusso dati fra i vari microservizi (strettamente Ai e non strettamente AI) è fondamentale per assicurare soluzioni resilienti, scalabili, controllabili e documentate.

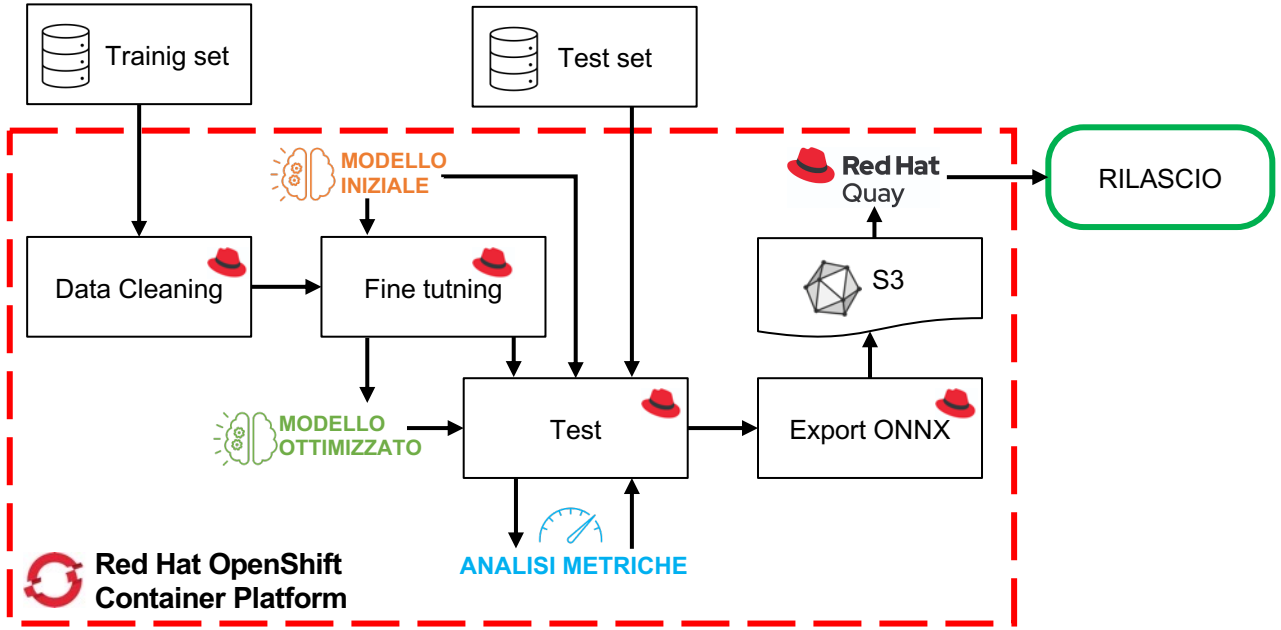
UN ESEMPIO PRATICO DI USE CASE

USE CASE

Piattaforma multi agent a supporto degli operatori di un tour operator su temi relativi a hotel, pacchetti vacanze e tour di viaggi

IMPLEMENTAZIONE

- Attuare le potenzialità di **OpenShift AI** nel supportare i flussi di lavoro AI/ML su infrastruttura enterprise, evidenziando come la piattaforma possa semplificare la gestione dei modelli
- Validare un workflow end-to-end di addestramento direttamente sulla piattaforma, dalla preparazione dei dati fino al deployment dei modelli.
- Mostrare come le pipeline possano rendere il processo riproducibile, garantendo coerenza e qualità nei cicli di addestramento e retraining dei modelli.



Si è dimostrato come sia possibile rendere il *fine-tuning* un **processo riproducibile e reiterabile, con un effort umano molto basso**, attraverso:

- **Notebooks automatizzati** per generazione dataset e valutazione finale (tramite GenAI).
- **OpenShift AI pipelines** per orchestrare l'intero workflow.
- **Serving del modello** allenato direttamente tramite **OpenShift AI**
- **Interazione con registry** certificati

Inoltre, è stato rilevato un **miglioramento delle performance rispetto al modello non addestrato:** questo conferma che il procedimento sviluppato da mauden si è rivelato **efficace e funzionale**, avvalorando la **competenza e capacità nel gestire progetti di AI enterprise end-to-end**.

LA VISIONE DI MAUDEN USE CASE CONCRETO

MAUDEN E LA TOTAL GOVERNANCE DELL'AI REGOLATA

mind INTELLIGENZA DOCUMENTALE

La nuova soluzione RAG di Mauden multi-agent **on premise** o in cloud nativamente integrata (o integrabile in caso di deploy multicloud) con strumenti di governance e protezione dati.

MIND è la piattaforma di intelligenza documentale basata su AI generativa sviluppata da Mauden. Permette di interrogare la knowledge base aziendale in linguaggio naturale, ottenendo risposte immediate e pertinenti Sviluppata su **Red Hat Openshift** e **Red Hat OpenShift AI** gestisce l'intero ciclo di vita dei modelli RAG — dall'addestramento alla distribuzione — migliorando la pertinenza dei risultati, riducendo la latenza e semplificando l'infrastruttura con tempi di valore più rapidi. La compliance è gestita con **IBM watsonx governance**.

Approccio: Piccolo e on Premise First
Mauden ritiene che una soluzione AI debba essere energeticamente sostenibile, rispettosa della sovranità del dato, rispettosa dei principi etici e normativi italiani. Quindi il nostro approccio ricerca sempre soluzioni ottimizzate che non usano «la forza bruta» ma l'intelligenza dei nostri consulenti e analisti.

mauden

A RICOH Company

Viale Martesana 12, 20055 - Vimodrone (MI)

Via Mario Bianchini 13-15, 00142 - Roma

Via Pavia 9/A1, 10098 - Rivoli (TO)

www.mauden.com

info@mauden.com

Red Hat Summit

Connect

 linkedin.com/company/red-hat

 facebook.com/redhatinc

 youtube.com/user/RedHatVideos

 twitter.com/RedHat