

CYBER SECURITY FOUNDATION

The first non-profit Italian
foundation in the cyber world



AI SICURA

*Comprendere e mettere in sicurezza il Futuro
dell'Intelligenza Artificiale a livello Nazionale*

Presentazione dell'iniziativa - Febbraio 2026

Iniziativa nazionale promossa da Cyber Security Foundation



AI Security: Una sfida nazionale, una realtà attuale

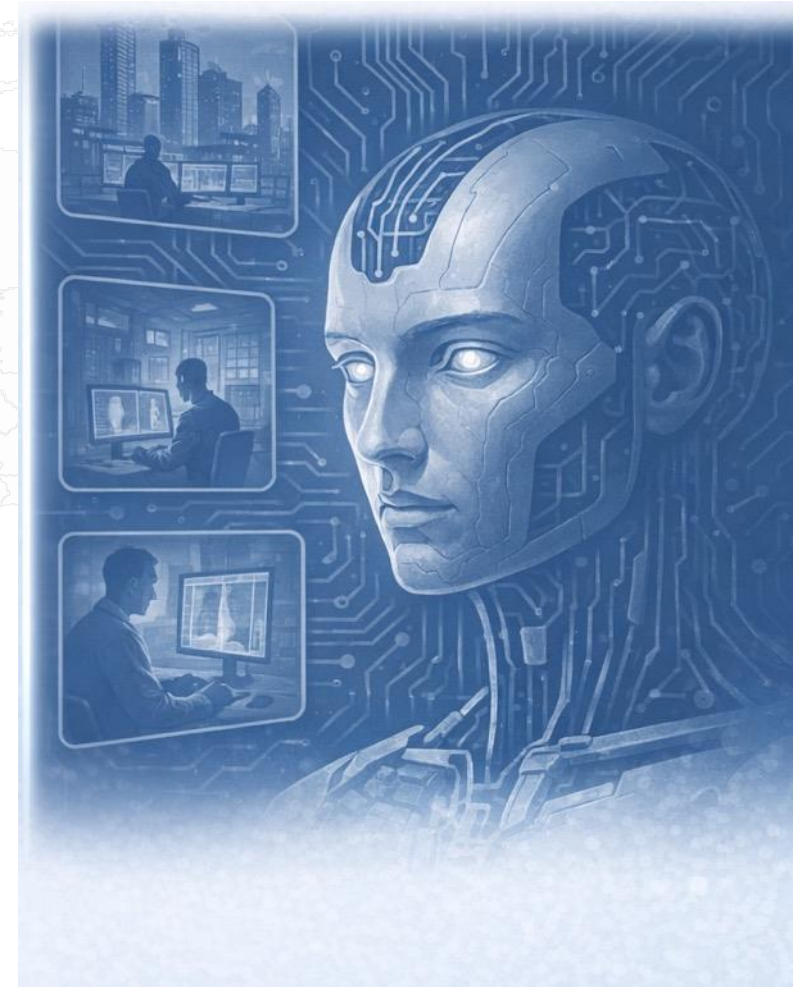
L'AI decide già per noi.

Infrastrutture critiche, diagnosi mediche, operazioni finanziarie, difesa nazionale: i sistemi di intelligenza artificiale influenzano decisioni che impattano milioni di persone ogni giorno.

Il Problema ? La sicurezza viene dopo...

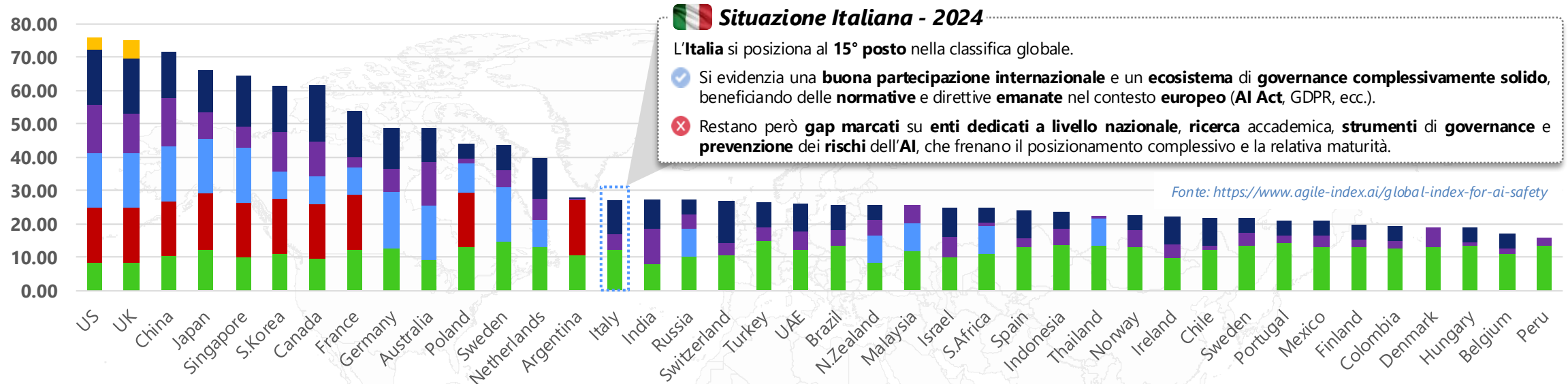
Mentre le capacità dell'AI crescono esponenzialmente, governance e controlli di sicurezza rimangono spesso un principio. Il confine tra decisione umana e automatizzata si fa sempre più sottile, ma le responsabilità restano confuse.

Non è più una sfida per singole organizzazioni.
È una priorità nazionale.



Panoramica Internazionale

Indice Globale per la sicurezza dell'AI



| Pillars | Criterio di valutazione | Parametri considerati |
|--|--|---|
| 1 Governance Environment | Sfide di sicurezza dell'AI affrontate dal Paese. | <ul style="list-style-type: none"> Cybersecurity Status AI Safety Incident |
| 2 National Institutions | Preparazione delle istituzioni nazionali in materia di sicurezza dell'AI | <ul style="list-style-type: none"> National AI Safety Institutes/Networks/Labs/Consortiums |
| 3 Governance Instruments | Completezza ed efficacia delle leggi , delle politiche e degli strumenti del Paese per la sicurezza dell'AI | <ul style="list-style-type: none"> National Laws & Regulations related to AI Safety Technical & Policy Frameworks for AI Safety |
| 4 Research Status | Capacità di ricerca nell'affrontare i rischi legati alla sicurezza dell'AI | <ul style="list-style-type: none"> AI Safety Publications AI Safety Patents |
| 5 International Participation | Livello di partecipazione del Paese ai meccanismi globali di governance della sicurezza dell'AI | <ul style="list-style-type: none"> Government Engagement Industry Engagement Academia & Civil Society Engagement |
| 6 Existential Safety Preemption | Pianificazione strategica del Paese per prevenire i rischi esistenziali posti dall'AI | <ul style="list-style-type: none"> Government Engagement Industry Engagement |

Governare l'AI: contenerne i rischi, sfruttarne i benefici

Nuovi rischi e opportunità



1

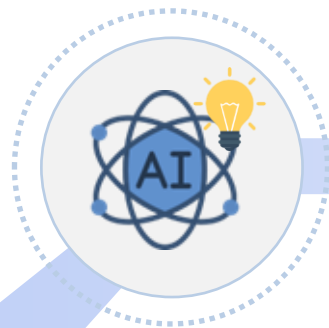
***Rischi di sicurezza
connessi all'AI***



! Minacce cyber rivolte ai sistemi AI e ai suoi utilizzatori



! Minacce cyber potenziate dall'AI



2

***Opportunità di sicurezza
connesse all'AI***



💡 Agenti AI per la sicurezza

CYBER SECURITY FOUNDATION

The first non-profit Italian
foundation in the cyber world



AI SICURA | Overview Iniziativa



AI SICURA: Obiettivo, Approccio e Stakeholders

Un'iniziativa nazionale strutturata per **misurare, confrontare e rafforzare** la **preparazione** alla **sicurezza dell'AI** nei diversi settori



Obiettivo

Valutare il livello di **preparazione nazionale** in materia di **sicurezza AI**, consentire un **benchmarking** continuo tra i **diversi settori** e **promuovere** la **consapevolezza**, insieme a **soluzioni concrete e attuabili**.



Approccio

Definire un **quadro dedicato** di valutazione della **preparazione** alla **sicurezza AI** e valutarlo tramite un'**indagine nazionale** mirata, rivolta ai **CISO** dei principali **settori industriali** e ambiti di attività.



Stakeholders

Amministrazione Pubblica, **Settori economici**, **CISO**, **Mondo accademico** ed **esperti di cybersicurezza**.

AI SICURA: Misurare l'AI Security Readiness

Abbiamo progettato un **sondaggio nazionale** per **CISO** al fine di raccogliere **insight reali** sulle sfide attuali della sicurezza AI nel Paese



Consapevolezza dei rischi di sicurezza AI per settore

Misura quanto le organizzazioni comprendano minacce, vulnerabilità e implicazioni di sicurezza specifiche dell'AI.



Architetture e modelli di AI più diffusi

Identifica le architetture di AI e le tipologie di modelli più comunemente adottate negli ambienti operativi.



Adozione dell'AI nella difesa/gestione cyber

Identifica come le organizzazioni sfruttano l'AI per rafforzare la cybersicurezza, con focus su rilevamento delle minacce, gestione degli incidenti ed efficacia operativa.



Strategie di difesa adottate per proteggere i sistemi di AI

Valuta le misure tecniche, organizzative e di governance implementate per mettere in sicurezza i sistemi di AI.



Minacce legate all'AI più temute dai CISO

Raccoglie gli scenari di minaccia specifici dell'AI percepiti come più critici dai responsabili della sicurezza.

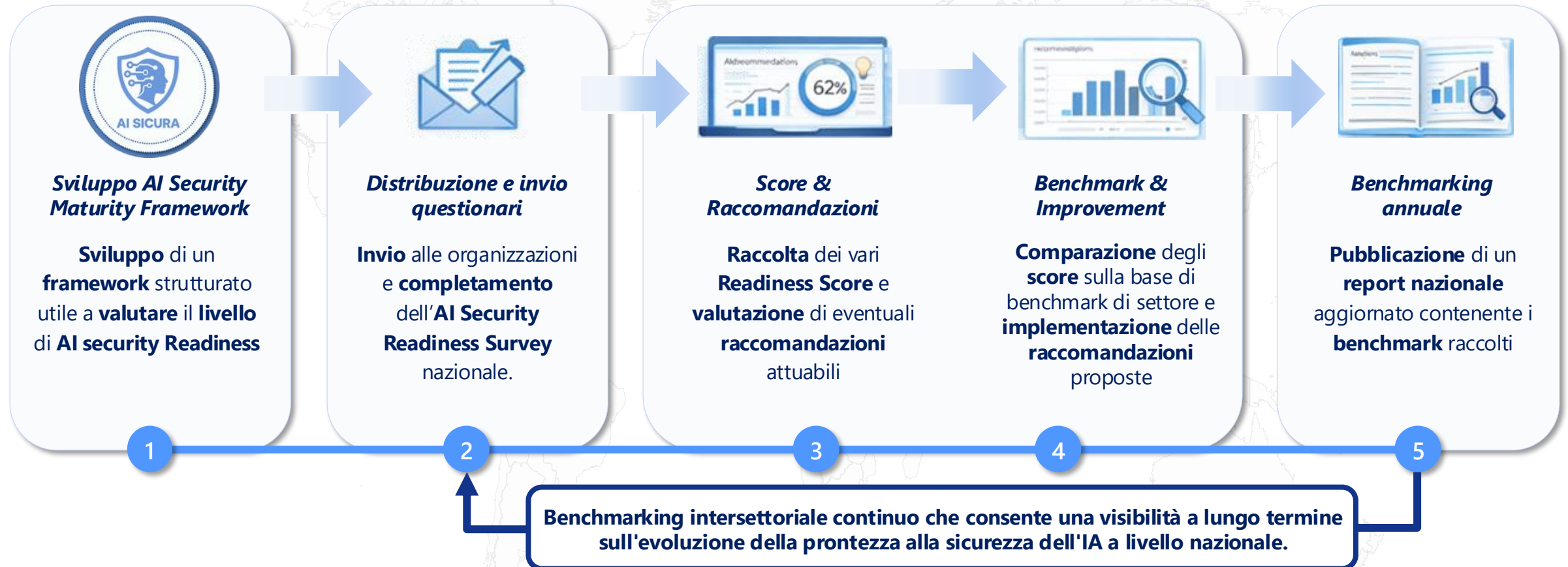


Livello di preparazione del Paese alla sicurezza dell'AI

Fornisce una vista consolidata della maturità nazionale in materia di sicurezza dell'AI, basata su indicatori di readiness trasversali ai settori.

AI SICURA: Flusso operativo

Un **processo** nazionale **end-to-end** per **misurare, confrontare e migliorare** costantemente la **preparazione** alla **sicurezza** dell'IA a livello nazionale



AI SICURA: Questionario Web

L'indagine sfrutta un **framework integrato** e una **valutazione web-based** per **valutare** la **maturità** della **sicurezza dell'AI** nei domini chiave

Web-based Assessment

Industry: Finance & Insurance | Company Size: 251-1000 employees

Questions completed: 1/10

1 Has your organization defined a formal AI strategy and governance for the adoption of artificial intelligence that includes aspects of cybersecurity?

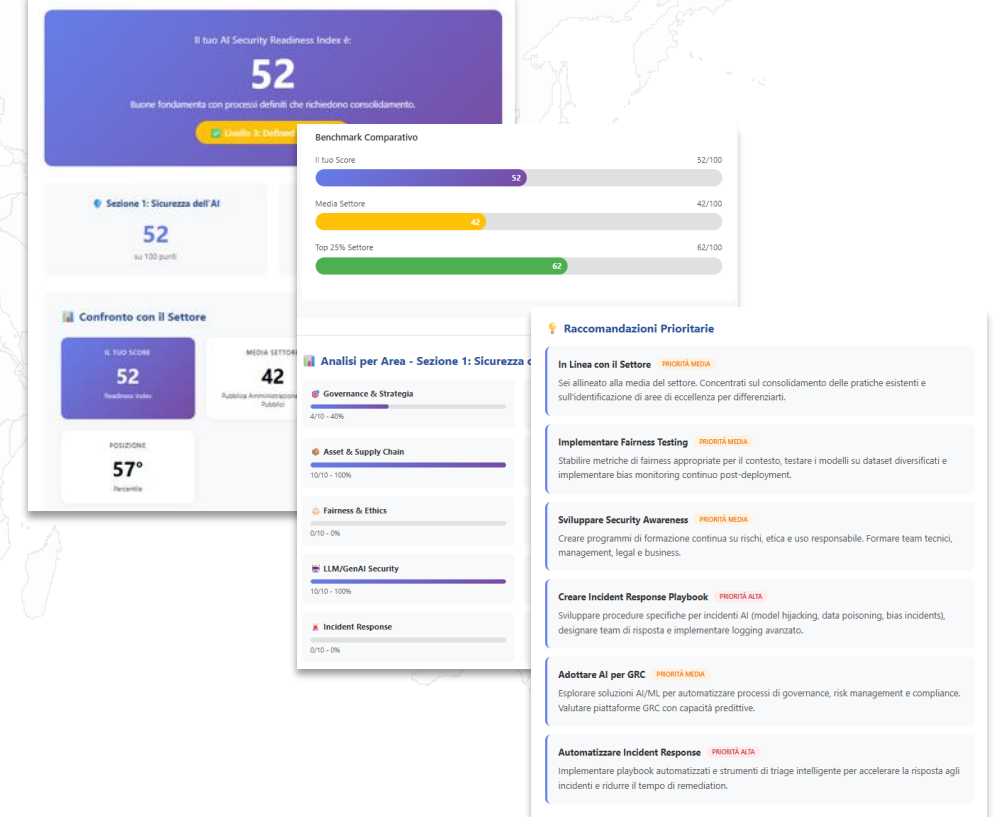
No, we do not have any formal AI strategy

We have started discussing it but have no formal documents

We have a defined strategy that is not yet fully implemented

Yes, we have a defined strategy and active governance with periodic reviews

Esito Valutazione



AI SICURA: the National Report

L'**output** di punta dell'**iniziativa**, che consolida **dati, evidenze** e **benchmark** in un riferimento **nazionale** sulla **sicurezza dell'AI**



Una valutazione completa dello stato attuale della sicurezza dell'AI

Offre una **visione** basata sui **dati** delle principali **sfide** di **sicurezza** dell'**AI** e dell'adozione di soluzioni di sicurezza abilitate dall'AI. Introduce un **AI Security Maturity Index** dedicato per misurare in modo coerente il livello di preparazione nei diversi settori. Consente il **confronto intersettoriale** per identificare **punti di forza, lacune** e **aree di rischio** emergenti.



Raccomandazioni strategiche applicabili

Fornisce **raccomandazioni concrete** e basate su evidenze per aziende, pubbliche amministrazioni e istituzioni. **Supporta** i **decisioni** nel rafforzare **governance** dell'**AI**, **gestione** dei **rischi** e **pratiche** di **sicurezza**.



Framework e strumenti operativi

Presenta **framework, metodologie** e **strumenti pratici** per guidare l'**adozione sicura** dell'**AI**, abilitando al contempo una condivisione strutturata di informazioni su minacce e incidenti di sicurezza legati all'AI. **Supporta** le organizzazioni nel **migliorare resilienza, conformità** e pratiche di **AI affidabile**. Favorisce il **miglioramento continuo** attraverso azioni di sicurezza ripetibili e misurabili.

