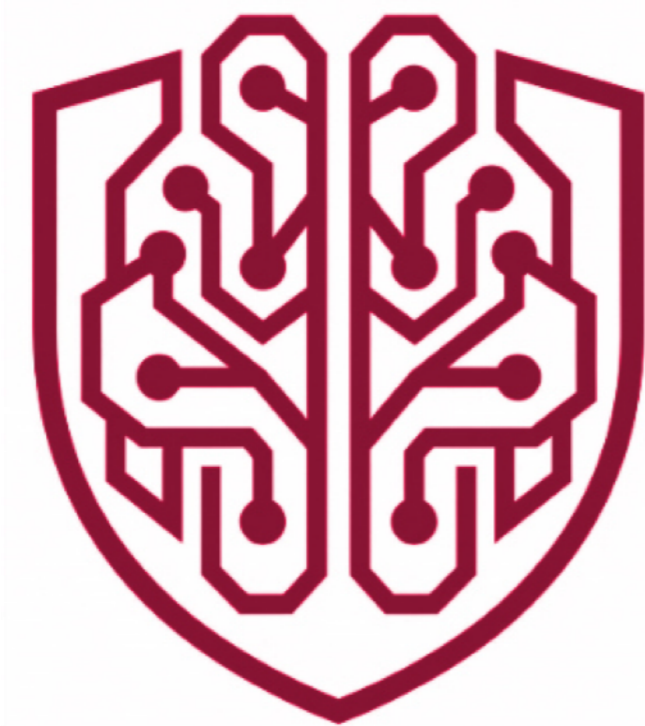




SAPIENZA  
UNIVERSITÀ DI ROMA



Finanziato  
dall'Unione europea  
NextGenerationEU



# AI-Sec Lab

**LABORATORIO DIGITALE CONGIUNTO  
SAPIENZA UNIVERSITÀ DI ROMA - CYBER 4.0**

# AI-SEC LAB - OBIETTIVI



**AI-Sec Lab** è un laboratorio digitale congiunto tra **Sapienza Università di Roma** e **Cyber 4.0**, con un duplice obiettivo:

- ✓ maturare competenze avanzate nelle tematiche di AI e sicurezza
- ✓ costituire un nucleo per formazione, consulenza e sviluppo di asset digitali strategici



## FORMAZIONE

Sviluppare competenze avanzate su AI e sicurezza dei modelli attraverso corsi e seminari specialistici.



## CONSULENZA

Fornire supporto e soluzioni innovative a aziende e istituzioni su tematiche di AI e cybersecurity.



## RICERCA E IMPATTO

Publicazioni scientifiche, whitepaper tecnologici e brevetti per generare valore e innovazione.



## RISORSE E INFRASTRUTTURE

Costruire un patrimonio di competenze, dati, software e hardware specializzato per l'AI e la sicurezza.

# AI-SEC LAB - AMBITI DI INTERVENTO



## LARGE LANGUAGE MODELS (LLM)

Utilizzo di LLM e modelli derivati per l'analisi del codice.



## REVERSE ENGINEERING E BINARY ANALYSIS

Tecniche avanzate per l'analisi di applicativi binari e malware.



## PRIVACY PRESERVING AI

Sviluppo e test di modelli che garantiscono la privacy e la protezione dei dati.



## RILEVAMENTO DI DEEPPFAKE

Individuazione di contenuti sintetici (audio, immagini, video) generati da AI.



## AI GENERATIVA E MEDIA FORENSICS

Studio dell'impatto dell'AI generativa e delle tecniche di media forensics.