RegulAI ověří odolnost vaší AI aplikace vůči bezpečnostním rizikům i její soulad s AI Act.

A nezůstane u toho, že ochrana existuje — prověří, že skutečně funguje. Místo ujištění dostanete jediné číslo, o které se dá opřít rozhodnutí.

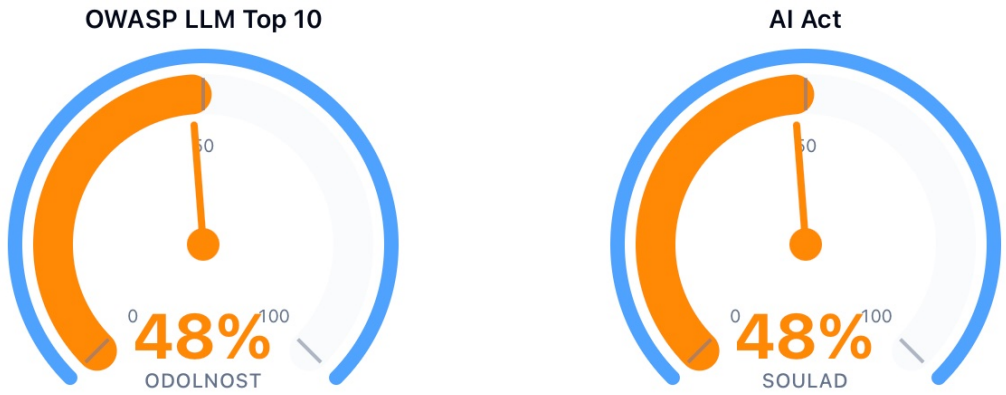
CO REGULAI JE

RegulAI automatizovaně prověří bezpečnost vašich AI aplikací. Žádný jednorázový ruční audit, jehož závěr zastará dřív, než ho dočtete. Místo toho opakovatelný a doložitelný obraz o tom, jak dobře jsou aplikace chráněné.

Funguje jako bezpečnostní pás. Nezáleží jen na tom, že v autě je. Záleží, jestli je zapnutý a jestli vás při nárazu udrží. U AI aplikace je to stejné. Nestačí, že je ochrana nasazená. Podstatné je, jestli zabrání tomu, čemu má. A přesně to RegulAI prověří.

VÝSLEDEK NA PRVNÍ POHLED

Každá prověřená aplikace dostane jasné skóre — zvlášť pro odolnost podle OWASP a zvlášť pro soulad s AI Act. Jedno číslo, kterému rozumí technik i ředitel.



Dvě skóre z jediného prověření.
Technická odolnost (OWASP LLM Top 10) a regulatorní soulad (AI Act) vedle sebe — měřeno, ne odhadováno.

CO REGULAI DĚLÁ

RegulAI jedním prověřením doloží, že ochrana vaší AI aplikace reálně funguje — ne že jen existuje — a současně dá důkaz odolnosti podle OWASP i souladu s AI Act.

Ověří, že je ochrana vůbec na místě. Že je správně nasazená a nakonfigurovaná. Konfiguraci čte nativně z vašeho prostředí — nezasahuje do aplikace ani nespoléhá na to, co o sobě sama tvrdí.

Pak ji aktivně vyzkouší. Aplikaci prověří sadou vysokých stovek promptů, včetně těch, které mají být zablokovány. Když aplikace takový prompt odmítne, je prokázáno, že ochrana zafungovala. Z testů vzniká skóre úspěšnosti v procentech pro každé jednotlivé riziko.

Dva pohledy, které se doplňují. Statická kontrola potvrdí, že obrana existuje; aktivní test prokáže, že skutečně drží.

> ***Nehodnotí se zapnutý pás. Hodnotí se to, že při nárazu udržel.***

DŮKAZ AŽ NA ÚROVEŇ JEDNOTLIVÉHO ČLÁNKU AI ACT

Výstupem není jen souhrnné číslo. RegulAI rozpadne soulad podle jednotlivých článků AI Act a rolí (poskytovatel, provozovatel) a přesně ukáže, kde aplikace požadavkům dostojí a kde je mezera, kterou je třeba zavřít.



Mapa souladu napříč články AI Act.
Každá buňka je změřená míra souladu podle role — zelená drží, oranžová a červená ukazují, kam zaměřit nápravu.

CO TÍM ZÍSKÁTE

Jistotu místo dojmu. Měřitelné skóre, které řekne, jak dobře je každá aplikace chráněná — a kde má slabiny.

Důkaz místo deklarace. Doložitelný a opakovatelný podklad o stavu ochrany. Použitelný pro interní reporting i pro prokázání souladu s AI Act.

Jasné priority. Kde je nastavení slabé, RegulAI ukáže konkrétní mezeru a doporučí, jak ji zlepšit.

Jeden rámec místo dvou. Bezpečnost (OWASP) i regulace (AI Act) z jednoho prověření.

Chcete vědět, jak dobře jsou vaše AI aplikace chráněné?

Ozvěte se nám a domluvíme prověření na vašem prostředí. **tomas.roubicek@orbit.cz**

Zobrazené hodnoty skóre jsou ilustrativní ukázka výstupu nástroje.