Engineer Софтвер

{ Безпека ШІ-агентів }

Щоб ШІ не чіпав того, чого не слід

Доступ кожного агента описано й обмежено необхідним,
кожну дію записано в журнал, якого агент не може змінити,
і кожен захист перевірено на ділі, а не взято на віру.

Ще визначаєтесь, що саме вам потрібно?

Розкажіть, що йде не так або що ви намагаєтесь побудувати. Ми скажемо, що для цього потрібно, скільки це приблизно коштуватиме і чи ми ті люди, які вам потрібні.

Від 1 400 DKK за годину, без ПДВ — і дешевша година на довшому замовленні.

Зв'язатися з нами Дивитися, скільки це коштує

Вибрані роботи, що демонструють цю послугу.

Перетворіть послугу на результат

Нехай «Безпека ШІ-агентів» слугує меті бізнесу. Ми можемо пов'язати технічну роботу з користувачами, експлуатацією та рішеннями, які вона має підтримувати. Доступ кожного агента описано й обмежено необхідним, кожну дію записано в журнал, якого агент не може змінити, і кожен захист перевірено на ділі, а не взято на віру.

Зв'язатися з нами

Розгляньте відповідні роботи

Використайте роботи на цій сторінці, щоб оцінити наш підхід. Запитайте про компроміси та передумови кожного результату. Побудувала ліміти запитів і захист від зловживань — 22 обмежувачів частоти, які в разі збою блокують доступ

Побудувала ліміти запитів і захист від зловживань Зв'язатися з нами →

Побудувала ліміти запитів і захист від зловживань

Побудувала засоби протидії зловживанням за принципом fail-closed — 22 обмежувачі частоти на Redis, Cloudflare Turnstile, ідемпотентність запитів та прив'язку до origin — щоб платформа відсікала ботів і напливи, а не довіряла тим, хто її викликає.

Потрібна послуга: Безпека ШІ-агентів?

Оцініть відповідний досвід за пов’язаними роботами. Розкажіть, що потрібно створити; обговоримо обсяг, підхід до виконання та передачу результатів.

Зв'язатися з нами Повне портфоліо

Визначте обсяг до замовлення

Опишіть шлях розгортання, експлуатаційні ризики та чергову команду. Ми можемо визначити зміну з перевірками, шляхом відновлення та чіткою відповідальністю.

Дивитися, скільки це коштує Зв'язатися з нами →

Обговоріть свої вимоги

Розкажіть, що вам потрібно за напрямом «Безпека ШІ-агентів», зокрема про строки та команду, яка підтримуватиме рішення. Обговоримо практичний шлях уперед.

Зв'язатися з нами

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://software.engineer.company/uk/services/ai-security/