**Engineer** Mjukvara

{ Säkerhet för AI-agenter }

# Hålla AI:n borta från det den inte ska röra

Varje agents behörigheter kartlagda och begränsade till det nödvändiga, varje handling loggad där agenten inte kan ändra loggen, och varje skydd prövat i stället för taget för givet.

## Håller ni fortfarande på att reda ut vad ni behöver?

Berätta vad som inte fungerar eller vad ni försöker bygga. Vi säger vad det skulle kräva, ungefär vad det skulle kosta och om vi är rätt personer för uppgiften.

**Från 1 400 DKK i timmen, exklusive moms — och mindre per timme vid en längre bokning.**

**Hör av er** Se vad det kostar

Utvalt arbete som visar den här tjänsten.

### Gör tjänsten till ett resultat

Låt ”Säkerhet för AI-agenter” stödja ett affärsmål. Vi kan knyta det tekniska arbetet till användarna, driften och besluten det ska stödja. Varje agents behörigheter kartlagda och begränsade till det nödvändiga, varje handling loggad där agenten inte kan ändra loggen, och varje skydd prövat i stället för taget för givet.

**Hör av er**

### Granska det relevanta arbetet

Använd arbetet på sidan för att granska vårt angreppssätt. Fråga om avvägningarna och förutsättningarna bakom varje resultat. Byggde hastighetsbegränsning som stänger vid fel — 22 hastighetsbegränsare som stänger vid fel

**Byggde hastighetsbegränsning som stänger vid fel** Hör av er →

### Byggde hastighetsbegränsning som stänger vid fel

Byggde skydd mot missbruk som stänger vid fel — 22 hastighetsbegränsare i Redis, Cloudflare Turnstile, idempotenta anrop och ett ursprungslås — så att plattformen avvisar botar och anropsfloder i stället för att lita på sina anropare.

## Letar ni efter Säkerhet för AI-agenter?

Använd de länkade arbetena för att bedöma relevant erfarenhet. Berätta vad ni behöver bygga; vi kan diskutera omfattning, arbetssätt och överlämning.

**Hör av er** Hela portföljen

Avgränsa uppdraget före beställning

Ta med driftsättningsvägen, driftsriskerna och dem som har jour. Vi kan avgränsa en förändring med kontroller, en väg tillbaka och tydligt ansvar.

**Se vad det kostar** Hör av er →

# Gå igenom era krav med oss

Berätta vad ni behöver inom ”Säkerhet för AI-agenter”, vilken tidsram ni önskar och vilket team som ska förvalta lösningen. Vi kan diskutera en praktisk väg framåt.

**Hör av er**

welcome@engineer.company +45 50 10 61 84 Köpenhamn, Danmark

Ta med dig den här sidan

Visitkort

**Omsorgsfullt skapad med kärlek av D.**

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

**Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.**

**Utskrivet från https://software.engineer.company/sv/services/ai-security/**