Engineer Rådgivning

{ Sikkerhet for AI-agenter }

Holde AI-en unna det den ikke skal røre

Hver agents tilgang kartlagt og begrenset til det nødvendige,
hver handling logget der agenten ikke kan endre loggen,
og hvert sikkerhetstiltak testet i stedet for tatt på tro.

Avklarer dere fortsatt hva dere trenger?

Fortell oss hva som går galt, eller hva dere prøver å bygge. Vi sier hva det vil kreve, omtrent hva det vil koste, og om vi er de rette til oppgaven.

Fra 1 400 DKK timen, eksklusive mva. — og mindre per time ved et lengre oppdrag.

Ta kontakt Se hva det koster

Utvalgt arbeid som viser denne tjenesten.

Gjør tjenesten til et resultat

La «Sikkerhet for AI-agenter» støtte et forretningsmål. Vi kan knytte det tekniske arbeidet til brukerne, driften og beslutningene det skal støtte. Hver agents tilgang kartlagt og begrenset til det nødvendige, hver handling logget der agenten ikke kan endre loggen, og hvert sikkerhetstiltak testet i stedet for tatt på tro.

Ta kontakt

Undersøk det relevante arbeidet

Bruk arbeidet på denne siden til å undersøke tilnærmingen vår. Spør om avveiningene og forutsetningene bak hvert resultat. Drev et løpende program for sikkerhetsskanning — 21 skriftlige sikkerhetsrevisjoner, ved siden av de automatiserte

Drev et løpende program for sikkerhetsskanning Ta kontakt →

Drev et løpende program for sikkerhetsskanning

Etablerte et kontinuerlig sikkerhetsprogram — kodeskanning, DAST, kontroll av avhengigheter og sårbarheter, SBOM-generering, skanning etter hemmeligheter og SHA-låste actions — sammen med 21 skriftlige sikkerhetsrevisjoner.

Skrev en avgrensningsregel etter tilgangslekkasje

Skrev en avgrensningsregel inn i repoet etter at en omstrukturering hadde ført et annet selskaps inventar, brannmuråpninger og tekst inn i det — og holdt de karantenesatte restene under skanneren for hemmeligheter i stedet for å unnta dem.

Leter dere etter Sikkerhet for AI-agenter?

Bruk de tilknyttede arbeidene til å vurdere relevant erfaring. Fortell oss hva dere skal bygge; vi kan diskutere omfang, fremgangsmåte og overlevering.

Ta kontakt Hele porteføljen

Avgrens oppgaven før bestilling

Ta med utrullingsløpet, driftsrisikoene og dem som har vakt. Vi kan avgrense en endring med kontroller, en vei tilbake og tydelig ansvar.

Se hva det koster Ta kontakt →

Gå gjennom kravene med oss

Fortell hva dere trenger innen «Sikkerhet for AI-agenter», inkludert fristen og teamet som skal vedlikeholde løsningen. Vi kan drøfte en praktisk vei videre.

Ta kontakt

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

Ta med deg denne siden

Visittkort

Laget med kjærlighet av D.

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

Opphavsrett © 2025 – nå · Engineer ApS · Alle rettigheter forbeholdt.

Skrevet ut fra https://advisory.engineer.company/nb/services/ai-security/