



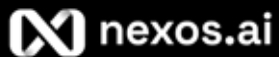
**SECURITY
DAYS**

PATIKIMAS DIRBTINIS INTELEKTAS VERSLE - AR AI SAUGO JŪSŲ PASLAPTIS?



SIGITA JURKYNAITĖ

DI startuolio „nexus.ai“
informacijos saugumo vadovė



An AI orchestration platform for the agentic era



A comprehensive solution for all your enterprise AI needs.

Ar AI saugo jūsu paslaptis?

- Ar AI "suinteresuotas" saugoti paslaptis?



Ar AI saugo jūsu paslaptis?

- Ar AI "sinteresuotas" saugoti paslaptis?
- Ar AI skiria kas yra paslaptis, o kas - ne?



Ar AI saugo jūsu paslaptis?

- Ar AI "suinteresuotas" saugoti paslaptis?
- Ar AI skiria kas yra paslaptis, o kas - ne?

**Patikimas AI versle -
paslapčių nežinantis AI**



Kaip valdome duomenų patekimo į AI procesą?

Techniniai sprendimai

Patikimi tiekėjai

Žmogiškasis faktorius



Techniniai sprendimai



Techniniai sprendimai

Kur atiduodame
duomenis

(paslaptis)

100% SELF-HOSTING

Privatumo 'aukso standartas'

Paslaptys saugios - niekad nepalieka įmonės kontrolės

Techniniai sprendimai

Kur atiduodame
duomenis

(paslaptis)

100% SELF-HOSTING

Privatumo 'aukso standartas'

Paslaptys saugios - niekad nepalieka įmonės kontrolės

GATEWAY

Viena API jungtis - strateginis saugumo valdymo taškas

Jūsų saugumo taisyklės

Techniniai sprendimai

Kur atiduodame
duomenis

(paslaptis)

100% SELF-HOSTING

Privatumo 'aukso standartas'

Paslaptys saugios - niekad nepalieka įmonės kontrolės

GATEWAY

Viena API jungtis - strateginis saugumo valdymo taškas

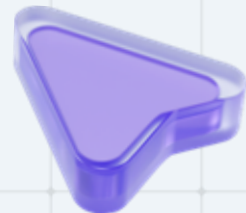
Jūsų saugumo taisyklės

ATSKIRI MODELIAI

Tiesioginės enterprise licencijos

Perku ir naudoju

Patikimi
tiekėjai



Patikimi tiekėjai

AI klausimynas

AI valdysena ir rizikos

Ar turite atsakingo AI politiką?
Ar taikote technines priemones
apsaugoti nuo su AI susijusių rizikų?
Kokias?

Modelio patikimumas

Kaip testuojate modelį?
Ar saugumo testai yra atliekami po
kiekvieno modelio atnaujinimo?

Duomenų privatumas

Iš kur atkeliauja duomenys modelio
mokymui?
Ar promptai saugomi, kiek laiko?
Ar galite nenaudoti mūsų duomenų modelio
mokymui?

Skaidrumas

Ar aiškiai įvardinti modelio ribotumai?
Kokius trečiųjų šalių (AI) įrankius
naudojate patys?

Patikimi tiekėjai

AI klausimynas =

ISO 42001?



Patikimi tiekėjai

ISO 27001

INFORMACIJOS SAUGUMAS

Užtikrinti CIA:

- Konfidencialumas
- Vientisumas
- Prieinamumas

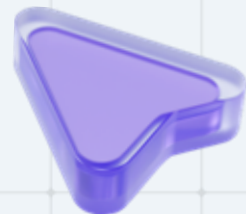
ISO 42001

AI VALDYSENA

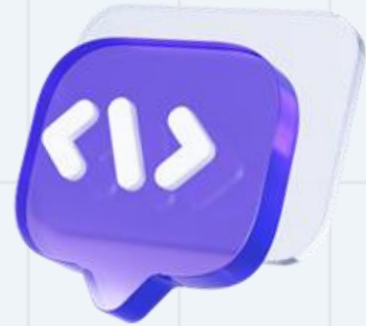
AI sistemos

- Patikimumas
 - Skaidrumas
 - Etiškumas
-
- Atsakomybė už tai, ką AI generuoja, ne tik kur jis veikia
 - Nuolatinis vertinimas - AI sistemos kokybė & patikimumas visame gyvavimo cikle
 - AI veikimo logikos dokumentacija

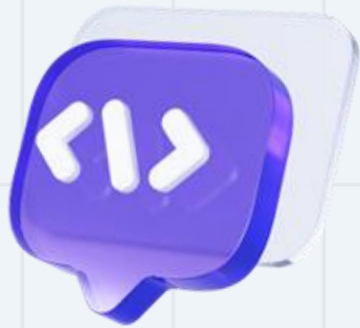
Žmogiškasis faktorių



Kritinis mąstymas



Kritinis mąstymas



Neauga ten, kur
vyrauja baimė

AI raštingumas -
naujoji higiena

Nuo drausti

->

Prie įgalinti

Patikimas AI versle

Tinkamas techninis sprendimas

Infrastruktūra leidžianti valdyti duomenų pateikimo ir saugojimo procesus

Patikimi tiekėjai

Partneriai, kurie ne tik pažada saugumą, bet ir gali tai įrodyti

Įgalinti kolegos

AI - tik galingas asistentas, o galutiniai sprendimai ir atsakomybė lieka žmogaus rankose



**Let's unlock
the power of AI**

Ačiū!

sigita.jurkynaite@nexos.ai

