TESORION

Prompt Security: Veilig gebruik van AI

Houd AI-gebruik veilig door risico's te om te vormen naar beheersbare innovatie

Binnen organisaties komt het gebruik van AI in allerlei vormen voor. Cybersecurityprofessionals worden daardoor geconfronteerd met een nieuw soorten risico's. Medewerkers delen bijvoorbeeld gevoelige gegevens met AI-tools terwijl aanvallers die modellen manipuleren, bijvoorbeeld in klantgerichte applicaties. Toch biedt AI een grote meerwaarde voor organisaties.

Prompt Security stelt bedrijven in staat om veilig en vol vertrouwen AI in te zetten. Het biedt de benodigde veiligheidsmaatregelen en governance om te innoveren. Daarnaast stelt het bedrijven in staat om snel te handelen en het volledige potentieel van AI te benutten. Dit bouwt vertrouwen op bij zowel klanten als werknemers omdat ze leren om te gaan met AI.

Onze missie

Tesorion zet zich in voor een samenleving waarin digitale veiligheid vanzelfsprekend is. Dat doen wij door organisaties te helpen hun continuiteit te waarborgen.

Veranderend aanvalsoppervlak

Met elke nieuwe technologie, nieuw apparaat of nieuwe integratie verandert het aanvalsoppervlak van jouw organisatie. Met Prompt Security kunnen organisaties AI veilig inzetten binnen hun organisatie.

Wil je meer weten over deze oplossing, neem dan contact met ons op. Wij helpen je graag verder.

Reduceer risico's bij AI-gebruik

- **Promptinjectie**
  Detecteert en blokkeert kwaadaardige invoer bedoeld om AI-modellen te manipuleren.
- **Openbaarmaking van gevoelige gegevens**
  Voorkomt dat vertrouwelijke of gereguleerde informatie in AI-tools terechtkomt.
- **Schadelijke LLM-reacties**
  Beschermt gebruikers tegen bloot-stelling aan ongepaste of schadelijke inhoud gegenereerd door LLM's.
- **Jailbreak en promptlekken**
  Blokkeert pogingen om model-beveiligingen te omzeilen of verborgen prompts te onthullen.

Ravenswade 2A, 3439 LD Nieuwegein, Nederland | 088 - 274 78 80 | info@tesorion.nl | www.tesorion.nl

TESORION

Gecontroleerd toepassen van AI binnen organisaties

Organisaties die GenAI duurzaam willen inzetten, moeten verder kijken dan het beschikbaar stellen van een platform. De kernvraag is niet of medewerkers AI gebruiken, maar hoe dit gebeurt en onder welke voorwaarden. Dat vraagt om expliciete keuzes: welke tools worden gebruikt, voor welk doel, en met welke spelregels. Prompt Security helpt organisaties grip te krijgen op deze adoptie. Niet door AI te beperken, maar door inzicht, controle en bewustwording te combineren. Zo wordt GenAI een beheersbaar onderdeel van de digitale werkomgeving, in plaats van een onzichtbaar risico.



Veilig innoveren
Risico's vroegtijdig signaleren, voordat ze leiden tot incidenten.



Inzicht
Weet welke AI-tools er gebruikt worden en op welke manier.



Afgestemd op beleid
Faciliteer het gebruik, door dit af te stemmen op het beleid

Controle en inzicht met Prompt Security

Voor medewerkers: Geef medewerkers de mogelijkheid AI te gebruiken, zonder zorgen om Shadow IT of het lekken van gevoelige gegevens. Eenvoudig in gebruik via een browser-plugin.

Voor software development: Geen zorgen om datalekken, prompt injectie of het tonen van schadelijke antwoorden. Prompt security werkt als het ware als een firewall voor AI en beveiligt eigen ontwikkelde LLM's.

Voor AI code assistenten: Code assistenten zoals GitHub of Copilot inzetten zonder zorgen over het introduceren van kwetsbaarheden. API-keys en secrets toevoegen.

Voor Agentic AI: Realtime inzicht, risicobeoordeling en handhaving op machine-niveau voor AI-systemen. Het Model Context Protocol (MCP) zorgt ervoor dat beveiligde agents zelfstandig acties kunnen uitvoeren.

Ravenswade 2A, 3439 LD Nieuwegein, Nederland | 088 - 274 78 80 | info@tesorion.nl | www.tesorion.nl