

Ataques de Prompt Injection e Jailbreak em Agentes Autônomos

Frequência de tentativas de desvio de instruções de segurança em sistemas voltados ao cliente.

1

Portão de P&L & Retorno em 90 Dias
Metas claras de corte de OPEX ou aumento de margem em até 3 meses.

FINANCEIRO

2

Zero Data Retention (ZDR) & Privacidade
Garantia contratual de sigilo sem reaproveitamento de dados para treino.

COMPLIANCE

3

Alçada Human-in-the-Loop em Riscos Críticos
Confirmação dupla humana para movimentações financeiras e contratos relevantes.

RISCO

4

Arquitetura Anti-Lock-in & Roteamento
Capacidade de alternar modelos e provedores de nuvem em menos de 24 horas.

ARQUITETURA

5

Trilha Criptografada de Auditoria (XAI)
Logs imutáveis de cada inferência, raciocínio e ação autônoma executada.

AUDITORIA

GOV

DIRETRIZ PARA CONSELHOS
Governança é o sistema de freios ABS que viabiliza a aceleração máxima com segurança.

CANAL TELEGRAM

t.me/oquevemai

Ataques de Prompt Injection e Jailbreak em Agentes Autônomos

Frequência de tentativas de desvio de instruções de segurança em sistemas voltados ao cliente.

1	Portão de P&L & Retorno em 90 Dias Metas claras de corte de OPEX ou aumento de margem em até 3 meses.	FINANCEIRO
2	Zero Data Retention (ZDR) & Privacidade Garantia contratual de sigilo sem reaproveitamento de dados para treino.	COMPLIANCE
3	Alçada Human-in-the-Loop em Riscos Críticos Confirmação dupla humana para movimentações financeiras e contratos relevantes.	RISCO
4	Arquitetura Anti-Lock-in & Roteamento Capacidade de alternar modelos e provedores de nuvem em menos de 24 horas.	ARQUITETURA
5	Trilha Criptografada de Auditoria (XAI) Logs imutáveis de cada inferência, raciocínio e ação autônoma executada.	AUDITORIA
GOV	DIRETRIZ PARA CONSELHOS Governança é o sistema de freios ABS que viabiliza a aceleração máxima com segurança.	CANAL TELEGRAM t.me/oquevemai