Mercado Digital

Patricia Knebel

patricia.knebel@jornaldocomercio.com.br

Confira, diariamente, no blog Mercado Digital, conteúdos sobre tecnologia e inovação. Para acessar, aponte a câmera do seu celular para o QR Code.

jornaldocomercio.com/mercadodigital

Violações dobram com uso de agentes de IA

Relatório do Netskope Threat Labs mostra que as violações de políticas de dados downstream são agora o segundo tipo mais comum de violação relacionada à Inteligência Artificial (IA) nas empresas, representando 924 de cada 10 mil alertas, ou quase um em cada dez. Apenas as violações de políticas de dados upstream ocorrem com maior frequência.

As violações downstream acontecem quando um serviço de IA retorna informações às quais um usuário ou agente não está autorizado a acessar. A frequência desses casos mais que dobrou no último ano, passando de uma média de 12 para 31 ocorrências por organização por semana. Entre os 25% das organizações com maior incidência, o aumento foi ainda mais acentuado, de 72 para 206 violações semanais.

No Brasil, a adoção de IA corporativa acompanha de perto a média global. Segundo o levantamento, 88% das organizações brasileiras já utilizam plataformas de IA e 79% adotam agentes para desenvolvimento de código.

Ao mesmo tempo, o País ainda está em um estágio menos avançado de adoção da IA agêntica. Nas últimas dez semanas, a adoção do Model Context Protocol (MCP) cresceu 233% em número de usuários e 226% em volume de transações.

Esse crescimento está sendo impulsionado pela rápida adoção do Model Context Protocol (MCP), um padrão aberto que permite que modelos e agentes de IA se conectem a fontes externas de dados e ferramentas.

Em um período de dez semanas, o número de usuários acessando servidores MCP remotos aumentou 250%, enquanto as transações via MCP cresceram 375%. Isso permite que sistemas de IA acessem um volume maior de dados corporativos, mas também cria oportunidades para que informações sensíveis sejam retornadas à pessoa ou ao agente errado.

As violações de políticas de dados upstream, nas quais usuários ou agentes enviam informações sensíveis para uma aplicação de IA, continuam sendo o risco mais comum, respondendo por 8.752 de cada 10 mil alertas.

No entanto, o relatório mostra que o conjunto de ameaças envolvendo IA corporativa está se ampliando. Depois das violações downstream, as organizações também detectam violações de filtragem de conteúdo (154), tentativas de prompt injection e jailbreaking (129) e solicitações deliberadas de informações sensíveis (28).

O código malicioso continua sendo a categoria de menor volume, com cinco alertas a cada 10 mil, mas apresenta alta criticidade, pois pode ser executado diretamente por um agente autônomo ou incorporado a uma base de código mais ampla.

O country manager Brasil da Netskope, Claudio Bannwart, analisa que o Brasil está avançando rapidamente na adoção da IA corporativa e começa a entrar em uma nova fase, em que agentes de IA começam a ser incorporados às rotinas de negócio e a se conectar cada vez mais a dados e sistemas internos

Esse movimento amplia as possibilidades de uso da IA nas empresas, mas também exige uma evolução na forma como as empresas protegem suas informações. "Já não basta monitorar apenas os dados enviados às aplicações de IA. É preciso garantir que as respostas geradas por esses sistemas respeitem as políticas de acesso e não exponham informações sensíveis a usuários ou agentes sem autorização", afirma.

ADOBESTOCK/DIVULGAÇÃO/JC

Rápida adoção dessa tecnologia também amplia riscos, diz Netskope

Outras conclusões do estudo:

- O volume médio de prompts de IA triplicou no último ano, passando de 1.498 para 4.731 prompts por empresa por semana. Os 25% das organizações com maior uso geram pelo menos 19.292 prompts semanalmente.

- A adoção de aplicações de IA para desenvolvimento de código aumentou para 84% das organizações no último ano. O Claude Code agora é utilizado por 75% das empresas e o Codex por 58%, embora ambos registrassem taxas de adoção inferiores a 1% um ano antes.

- 41% das organizações utilizam atualmente o Ollama para executar modelos de IA localmente, à medida que as empresas buscam maior controle sobre onde os dados são processados e reduzem a dependência de plataformas em nuvem.

Instituto Caldeira promove imersão de 48 horas

O Instituto Caldeira, instituto privado sem fins lucrativos dedicado ao fomento de inovação, negócios e educação, promove entre os dias 27 e 29 de agosto o Bootcamp Caldeira.

O workshop imersivo é focado em transformar ideias em produtos digitais funcionais (MVP) usando plataformas de Inteligência Artificial conversacional.

A programação inclui validação de problema, construção de protótipo via vibe coding (desenvolvimento sem código, em linguagem natural) e preparação de pitch final.

O evento utiliza ferramentas como ChatGPT, Claude, Supabase e, principalmente, a Lovable, plataforma de destaque global em desenvolvimento no-code.

A imersão conta com mentoria de especialistas em Inteligência Artificial aplicada e negócios, incluindo nomes como Mateus Frattezi (estratégias AI-first para produto), Gabriel Breda (arquitetura segura em IA) e Tássia Pacheco (modelagem de requisitos).

A noite de abertura, no dia 27, traz a palestra "Do hype ao produto: o que separa uma startup de IA com tração de uma com deck bonito", de Laura Gurgel (cofundadora da Soul.Working e analista do Shark Tank Brasil). Nos dias seguintes, os participantes passam pela estruturação do problema e solução (28/08) e pela montagem prática do protótipo e entrega final (29/08).

Os três projetos de destaque receberão prêmios: mentorias de negócios especializadas da Orni e três meses de acesso físico ao Instituto Caldeira para conectar o negócio ao ecossistema de inovação local.

O bootcamp é voltado para empreendedores e profissionais que possuem uma ideia e querem viabilizá-la como produto digital, sem necessidade de conhecimento prévio em programação.

As inscrições estão abertas até o dia 20 de agosto.

INSTITUTO CALDEIRA/DIVULGAÇÃO/JC

Inscrições para o evento estão abertas até o dia 20 de agosto

CTR recebe designação da Senasp

O Centro Tecnológico Randon (CTR) recebeu da Secretaria Nacional de Segurança Pública (Senasp) a designação para atuar como laboratório de ensaios na validação de veículos leves destinados à segurança pública. Com a certificação, o CTR passa a integrar um grupo seleto de laboratórios brasileiros habilitados a realizar todos os ensaios exigidos para que veículos possam ser homologados como viaturas, conforme a Norma Técnica Senasp nº 006/2022.

"A partir de agora, montadoras interessadas em fornecer veículos para órgãos de segurança pública poderão realizar no CTR todas as avaliações necessárias para comprovar o desempenho, a segurança e a adequação operacional dos modelos", afirma o Chief Technology Innovation Officer (CTIO) da Randoncorp, César Augusto Ferreira.

Os testes avaliam desde aspectos estruturais até o desempenho em condições extremas e, assim, garantem que os veículos atendam às exigências do uso policial e de segurança. Entre os ensaios realizados pelo CTR, estão a verificação de características gerais e metrológicas, testes de resistência global (incluindo sistemas de arrefecimento e suspensão), avaliações ergonômicas e testes dinâmicos de frenagem, aceleração, slalom, circuito urbano e operação off-road.

"A centralização dos ensaios em uma estrutura tecnicamente qualificada tende a agilizar processos de validação, elevar o nível de exigência dos veículos e contribuir diretamente para a melhoria das condições de trabalho das forças de segurança", destaca Ferreira.

A norma técnica da SENASP estabelece requisitos operacionais compatíveis com a atividade policial e de emergência, ao contribuir para reduzir riscos de acidentes e falhas mecânicas durante patrulhamentos, perseguições e atendimentos de ocorrências.