Global Headquarters

Genetec Inc.
2280 Alfred Nobel Blvd.
Montreal, Quebec H4S 2A4
Canada

T: +1 514.332.4000

Media Alert

Especialista da Genetec avalia as implicações dos modelos LLMS (Modelos de Linguagem de Grande Escala) de Inteligência Artificial na segurança física

IA oferece grande potencial para automação e economia de custos. Mas é segura? Ueric Melo, especialista em Cibersegurança e Privacidade da Genetec para a América Latina e Caribe aborda a evolução da inteligência artificial na indústria de segurança

Os Modelos de Linguagem de Grande Escala (LLMs) estão transformando rapidamente o panorama global. Em poucos meses desde o lançamento do chatbot de inteligência artificial (IA) da OpenAI, o ChatGPT, mais de 100 milhões de usuários aderiram a essa plataforma, consolidando-a como uma das aplicações de consumo de crescimento mais acelerado na história recente. A versatilidade dos LLMs, capacitando desde respostas a perguntas e explicação de temas complexos até a redação de roteiros e códigos, tem gerado um intenso entusiasmo e debate global sobre o alcance e as implicações dessa tecnologia de IA.

“Embora os LLMs tenham se tornado um tema quente recentemente, vale a pena notar que a tecnologia já existe há muito tempo. Embora com os avanços em andamento, os LLMs e outras ferramentas de IA estão criando agora oportunidades para gerar maior automação em várias tarefas. Ter uma compreensão fundamentada das limitações da IA e dos riscos potenciais é essencial”, acredita Ueric Melo, especialista em Cibersegurança e Privacidade da Genetec para América Latina e Caribe.

Quais são os riscos de modelos de linguagem grandes?

No início deste ano, Sam Altman, CEO da OpenAI admitiu problemas em torno de pontos tendenciosos que fizeram questionar a segurança do ChatGPT. Mais recentemente, pesquisadores descobriram que alimentar modelos de linguagem de grande escala com identidades como "uma pessoa má" ou até mesmo certas figuras históricas gera um aumento de seis vezes nas respostas tóxicas e prejudiciais do modelo de aprendizado de máquina.

Os modelos de linguagem de grande escala são seguros? Ao ponderar os riscos dos LLMs, é importante considerar o seguinte - grandes modelos de linguagem são treinados para satisfazer o usuário como principal prioridade. Os LLMs também usam um método de treinamento de IA não supervisionado para abastecer um grande conjunto de dados aleatórios da Internet. Significa que as respostas que eles dão nem sempre são precisas, verdadeiras ou livres de ser tendenciosas. Tudo isso se torna extremamente perigoso em um contexto de segurança.

Na verdade, este método de treinamento de IA não supervisionado deu origem ao que é agora referido como 'alucinações da IA’. Isso ocorre quando um modelo de IA gera respostas que parecem plausíveis, mas não se baseiam em fatos ou dados do mundo real. O uso de LLMs também apresenta sérios riscos em termos de privacidade e confidencialidade. O modelo pode aprender a partir de dados que incluem informações confidenciais sobre indivíduos e organizações. Além disso, dado que cada input de texto é utilizado para treinar a versão subsequente, isso implica que alguém que solicite ao LLM conteúdos semelhantes pode ter

acesso a essas informações confidenciais por meio das respostas do chatbot de IA.

Depois, há os abusos mais mal-intencionados dessa tecnologia de IA. Considere como indivíduos mal-intencionados com pouco ou nenhum conhecimento de programação podem pedir a um chatbot de IA para escrever um script que explore uma vulnerabilidade conhecida ou solicitar uma lista de maneiras de hackear aplicativos ou protocolos específicos. Embora esses sejam exemplos hipotéticos, você não pode deixar de se perguntar como essas tecnologias podem ser exploradas de maneiras que ainda não podemos prever.

Como os modelos de linguagem de grande escala estão evoluindo no espaço da segurança física?

Com o crescente entusiasmo em torno dos modelos de linguagem de grande escala (LLMs), há uma percepção difundida de que a inteligência artificial (IA) pode transformar magicamente qualquer ideia em realidade. Entretanto, é importante notar que nem todos os modelos de IA são equivalentes nem evoluem no mesmo ritmo.

Dito isso, ele vale para todos os resultados benéficos dos LLMs. Para aplicações de segurança, pode haver um futuro em que os operadores possam usar um modelo de linguagem IA em uma plataforma de segurança para obter respostas rápidas, como perguntar 'qual a quantidade de pessoas estão no terceiro andar agora?' ou 'quantos crachás de visitante emitimos no mês passado?' Também pode ser usado para ajudar as organizações a criar políticas de segurança ou melhorar detalhes em protocolos de resposta.

Independentemente do uso dos modelos de linguagem de IA, é incontestável que os casos de uso em segurança demandam abordagens onde tais modelos operem em ambientes mais controlados. Assim, embora haja uma grande excitação em torno dos LLMs atualmente, é imperativo um considerável esforço para torná-los seguros e aplicáveis em cenários de segurança física.

Como a IA está sendo implementada no espaço da segurança física?

Os LLMs podem estar em alta no momento, mas o uso de IA na segurança física não é novidade. Existem diversas maneiras interessantes de utilizar IA para dar suporte em aplicações. Entre eles estão:

Acelerar as investigações - vasculhar um vídeo de um período específico para encontrar todas os momentos em que houver objetos, como pessoas e veículos, com as características definida pelo operador, como cor do objeto, direção, velocidade, cor das roupas de uma pessoa etc.

Global Headquarters

Genetec Inc.
2280 Alfred Nobel Blvd.
Montreal, Quebec H4S 2A4
Canada

T: +1 514.332.4000

Automatizar a contagem de pessoas - ser alertado sobre os limites máximos de ocupação em um prédio ou saber quando as filas dos clientes estão ficando muito longas para melhorar o atendimento.

Detecção de placas de veículos - rastrear veículos procurados, simplificar o estacionamento de colaboradores em escritórios ou monitorar o fluxo do trânsito nas cidades.

Melhorar a cibersegurança - fortalecimento da proteção antivírus em dispositivos usando aprendizado de máquina para identificar e impedir que malwares conhecidos e desconhecidos sejam executados em endpoints.

“Para a maioria das empresas, a implementação da IA se resume a alguns fatores determinantes; obter análises de dados em larga escala e níveis mais altos de automação. Em uma era em que todos falam sobre transformação digital, as empresas desejam aproveitar seus investimentos e dados em segurança física para aumentar a produtividade, melhorar as operações e reduzir custos”, afirma Melo.

Segundo ele, a automação também pode ajudar as companhias a aderir a vários padrões e regulamentos da indústria, reduzindo o custo de compliance. Isso ocorre porque o aprendizado profundo e o aprendizado de máquina oferecem o potencial de automatizar muitos processamentos de dados e fluxos de trabalho, ao mesmo tempo em que direcionam os operadores para insights relevantes. Isso permite que eles respondam rapidamente a interrupções nos negócios e tomem melhores decisões. “Embora IA esteja se tornando mais democratizada por meio de várias soluções de analíticos de vídeo, ainda existem muitos mitos por aí sobre o que a IA pode ou não fazer. Portanto, é importante que os profissionais entendam que a maioria das soluções de IA em segurança física não são de tamanho único”, explica o especialista da Genetec.

Automatizar tarefas ou alcançar um resultado desejado envolve um processo de avaliação da viabilidade técnica. Isso requer identificar soluções já existentes, a possível necessidade de outras tecnologias e resolver questões de compatibilidade ou considerar fatores ambientais. "Mesmo ao avaliar a viabilidade, algumas organizações podem questionar se o investimento justifica o resultado. Portanto, embora a IA seja importante para elevar a automação no setor de segurança física, é essencial um amplo planejamento e consideração para garantir resultados precisos", destaca Melo. Em resumo, é crucial abordar novas soluções de IA com cautela, avaliando criticamente os resultados prometidos e exercendo a devida diligência.

Quais são as melhores maneiras de capitalizar a IA na segurança física hoje?

As aplicações habilitadas para IA estão avançando de maneiras novas e empolgantes. São muito promissoras em ajudar as empresas a alcançar resultados específicos, que aumentam a produtividade, a proteção e a segurança em toda a empresa. “Uma das melhores maneiras de capitalizar os novos avanços da IA na segurança física é implementando uma plataforma de segurança aberta. A arquitetura aberta oferece aos profissionais de segurança a liberdade de

Global Headquarters

Genetec Inc.
2280 Alfred Nobel Blvd.
Montreal, Quebec H4S 2A4
Canada

T: +1 514.332.4000

explorar aplicações de inteligência artificial que geram maior valor em suas operações. À medida que as soluções de IA chegam ao mercado, os líderes podem experimentar essas aplicações, geralmente sem custos e selecionar os que melhor se adaptam aos seus objetivos e ambiente", diz Melo.

De acordo com o executivo da Genetec, à medida que surgem novas oportunidades, também surgem novos riscos. É por isso que é igualmente importante fazer parceria com companhias que priorizam a proteção de dados, a privacidade e o uso responsável da IA. Isso não apenas ajudará a aumentar a resiliência cibernética e promover maior confiança em seus negócios, mas também faz parte de ser socialmente responsável.

No Relatório da IBM intitulado Ética da IA em Ação, 85% dos consumidores disseram que é importante que as organizações considerem a ética ao usar a IA para resolver os problemas da sociedade. 75% dos executivos acreditam que acertar na ética da IA pode diferenciar uma empresa de seus concorrentes. E mais de 60% dos executivos veem a ética da IA ajudando suas organizações a ter um melhor desempenho em questões de diversidade, inclusão, responsabilidade social e sustentabilidade.

Como a Genetec considera privacidade e governança de dados usando IA responsável

À medida que os algoritmos de inteligência artificial (IA) processam grandes volumes de dados com rapidez e precisão, a IA torna-se uma ferramenta cada vez mais crucial para soluções de segurança física. No entanto, à medida que a IA avança, ela amplia a capacidade de utilizar informações pessoais, o que pode afetar a privacidade. "Os modelos de IA também podem inadvertidamente gerar decisões ou resultados enviesados com base em diferentes pontos de vista. Isso pode impactar decisões e, em última análise, resultar em discriminação. Apesar do potencial revolucionário da IA na transformação do trabalho e das tomadas de decisão, sua implementação deve ser feita com responsabilidade. É por isso que, na equipe da Genetec™, levamos a sério a questão da IA responsável. Desenvolvemos um conjunto de princípios orientadores para criar, aprimorar e manter nossos modelos de IA", alerta o especialista da Genetec.

Os três pilares que norteiam o uso de IA pela Genetec são:

Privacidade e governança de dados - como provedor de tecnologia, a Genetec assume a responsabilidade de usar IA no desenvolvimento de suas soluções. Isso significa que a utilização ocorre apenas nos conjuntos de dados que respeitam os regulamentos relevantes de proteção de dados. E, sempre que possível, anonimizados e como dados sintéticos. Também trata os dados com o máximo cuidado e mantem a proteção e a privacidade em mente em tudo o que faz. Isso inclui aderir a medidas estritas de autorização e autenticação para garantir que as pessoas erradas não tenham acesso aos dados e informações confidenciais em seus aplicativos orientados por IA. A empresa está empenhada em fornecer aos seus clientes ferramentas

integradas que os ajudarão a cumprir os regulamentos de IA em evolução.

Transparência e imparcialidade - à medida que desenvolve e usa modelos de IA, a Genetec está sempre pensando em como pode minimizar pontos tendenciosos. Seu objetivo é garantir que as soluções sempre forneçam resultados equilibrados e equânimes. Parte de garantir isso significa que testa rigorosamente os modelos de IA antes de compartilhá-los com os clientes. Também trabalha arduamente para melhorar continuamente a precisão e a confiança dos modelos. Por fim, se esforça para tornar explicáveis seus modelos de IA. Isso significa que, quando seus algoritmos de IA decidirem ou entregarem um resultado, pode dizer aos clientes exatamente como chegaram a essa conclusão.

Decisões orientadas por humanos - A Genetec garante que seus modelos de IA não possam tomar decisões críticas por conta própria. Acredita que um ser humano deve estar sempre informado e ter a palavra final. Porque em um contexto de segurança física, priorizar a tomada de decisão centrada no ser humano é fundamental. Pense em situações de vida ou morte em que os humanos compreendem inatamente os perigos em jogo e as ações necessárias para salvar uma vida. As máquinas simplesmente não conseguem entender as complexidades dos eventos da vida real como um operador de segurança, portanto, confiar apenas em modelos estatísticos não pode ser a resposta. É também por isso que sempre busca apresentar os resultados dos modelos de IA de forma que um humano possa fazer as escolhas mais informadas. A IA pode gerar insights, mas os humanos devem sempre ser os tomadores de decisão.

Sobre a Genetec

A Genetec Inc. é uma empresa global de tecnologia que vem transformando o setor de segurança física há mais de 25 anos. Hoje, a empresa desenvolve soluções projetadas para melhorar a segurança, a inteligência e as operações de empresas, governos e comunidades em que vivemos. Seu principal produto, o Security Center, é uma plataforma de arquitetura aberta que unifica vigilância por vídeo baseada em IP, controle de acesso, reconhecimento automático de placas de veículos (ALPR), comunicações e análises. Fundada em 1997 e sediada em Montreal, Canadá, a Genetec atende seus clientes por meio de uma extensa rede de parceiros de canal e consultores certificados em mais de 159 países. Para obter mais informações sobre a Genetec, visite: www.genetec.com/br.

Contatos para a imprensa:
Ink Comunicação
Clezia Martins Gomes / clezia.gomes@inkcomunicacao.com.br / (11) 99112-6942
Guilherme Russo – guilherme.russo@inkcomunicacao.com.br