No cenário em constante mudança das ameaças digitais, a inteligência artificial (IA) emergiu como um aliado formidável e um adversário perigoso. À medida que navegamos pelas complexidades do nosso mundo interligado, torna-se cada vez mais claro que a IA não é apenas uma ferramenta, mas uma força que está a remodelar a própria natureza da segurança cibernética.

O mundo da segurança cibernética mudou dramaticamente. Já se foi o tempo em que simples firewalls e software antivírus podiam manter nossos ativos digitais seguros. Hoje, estamos lidando com agentes de ameaças sofisticados que aproveitam a IA para lançar ataques em escala e velocidade sem precedentes. Por exemplo, em 2024, surgiu uma tendência preocupante em que os hackers usaram ferramentas alimentadas por IA para criar deepfakes altamente convincentes, fazendo-se passar por CEOs e outros executivos de alto escalão em 75% desses ataques.

Na Synechron, priorizamos a diligência em nosso processo de pagamento para garantir que tenhamos autoridade de aprovação apropriada, incluindo validação fora de banda de transferências de dinheiro de médio e grande porte. Como medida secundária, estamos agora avaliando algumas ferramentas de detecção de deepfakes que podem ser integradas em nossos aplicativos de produtividade empresarial, em particular para Zoom ou Teams, para detectar continuamente deepfakes.

Usar a IA na segurança cibernética é como tentar jogar xadrez contra um supercomputador: o jogo é familiar, mas as capacidades do oponente estão em um nível totalmente novo. Felizmente, também temos acesso ao supercomputador.

O que você vai ler:

A vantagem da IA

Como exatamente a IA está inclinando a balança em favor dos profissionais de segurança cibernética? Para começar, está revolucionando a detecção e resposta a ameaças. Os sistemas de IA podem analisar grandes quantidades de dados em tempo real, identificando ameaças potenciais com velocidade e precisão. Empresas como a CrowdStrike documentaram que seus sistemas baseados em IA podem detectar ameaças em menos de um segundo.

Mas as capacidades da IA não param na detecção. Quando se trata de resposta a incidentes, a IA está provando ser uma virada de jogo. Imagine um sistema de segurança que não apenas alerta você sobre uma ameaça, mas também toma medidas imediatas para neutralizá-la. Esse é o potencial da resposta automatizada a incidentes baseada em IA. Desde o isolamento de sistemas comprometidos até o bloqueio de endereços IP maliciosos, a IA pode executar essas tarefas críticas rapidamente e sem intervenção humana, reduzindo drasticamente os tempos de resposta e minimizando possíveis danos.

Talvez uma das aplicações mais esperadas da IA na segurança cibernética esteja no domínio da análise comportamental e da análise preditiva. Ao aproveitar algoritmos de aprendizado de máquina, a IA pode analisar o comportamento do usuário e os padrões de tráfego de rede, identificando anomalias que possam indicar ameaças internas ou outras atividades maliciosas. Foi demonstrado que esses sistemas de análise comportamental de ameaças internas orientados por IA detectam 60% de pessoas internas mal-intencionadas com um orçamento de investigação de 0,1% e alcançam detecção completa dentro de um orçamento de 5% em certos casos.

O lado negro da IA

No entanto, como acontece com qualquer ferramenta poderosa, a IA é uma faca de dois gumes. Ao mesmo tempo que melhora as nossas capacidades defensivas, também está a ser transformado em arma pelos cibercriminosos para lançar ataques mais sofisticados. Esses ataques cibernéticos alimentados por IA não são mais uma ameaça potencial – são um perigo muito real e presente.

Por exemplo, os invasores usaram recentemente a IA para se passarem por representantes de uma seguradora. O e-mail informava o destinatário sobre a inscrição nos benefícios e incluía um formulário que precisava ser preenchido com urgência para evitar perda de cobertura e tentativa de enganar o destinatário. A IA pode criar e-mails de phishing como esses, que são tão convincentes que até o usuário mais preocupado com a segurança pode cair nessa. Ele pode até criar malware personalizado que pode se adaptar e evoluir para evitar a detecção. Estes são os tipos de ataques que os cibercriminosos habilitados para IA são agora capazes de produzir. Acabamos num jogo de gato e rato em que ambos os lados estão constantemente a aumentar a aposta.

Os desafios não param por aí. À medida que confiamos cada vez mais na IA para as nossas necessidades de segurança cibernética, expomos estas novas ferramentas de IA a novas vulnerabilidades. O envenenamento de dados e a manipulação de modelos estão surgindo como sérias preocupações para nós que trabalhamos na segurança cibernética. Os invasores podem potencialmente adulterar os dados usados para treinar modelos de IA, fazendo com que eles funcionem mal ou tomem decisões erradas.

Há também o risco de dependência excessiva dos novos sistemas. Embora a IA seja sem dúvida poderosa, não é infalível. Tornar-se demasiado dependente da IA para a segurança cibernética pode levar à complacência e a uma falsa sensação de segurança. Devemos lembrar que a IA é uma ferramenta para aumentar a experiência humana e não para substituí-la totalmente.

O fator humano

A IA não está apenas mudando o conjunto de habilidades necessárias aos profissionais de segurança cibernética, mas também aumentando-o para melhor. A capacidade de trabalhar em conjunto com sistemas de IA, interpretar os seus resultados e tomar decisões estratégicas com base em conhecimentos gerados pela IA será fundamental tanto para utilizadores como para especialistas. Embora a IA esteja melhorando suas capacidades de segurança cibernética, um ser humano emparelhado com uma ferramenta de IA superará a IA por si só dez vezes.

Nossa equipe cibernética na Synechron planeja construir e implantar nossos próprios aceleradores de IA, bem como aproveitar os recursos de copiloto de segurança da Microsoft para aumentar nossa detecção e investigação de segurança de possíveis ameaças. No entanto, esta abordagem também requer interação humana para validar quaisquer conclusões ou recomendações da IA para priorizar as remediações ou respostas necessárias com base na criticidade do ativo. Em outras palavras, os humanos ainda são obrigados a interpretar qualquer informação contextual de negócios que a IA possa perder. Esta falha não deve ser subestimada, pois qualquer discrepância ou análise incorreta da IA pode levar a perdas ou comprometimentos prejudiciais. Além disso, os seres humanos também podem adaptar-se aos contextos empresariais e interpretar melhor as mudanças ou perceções de potenciais perdas ou impactos do que a IA, uma vez que a IA é especificamente programada

para alcançar resultados programados.

À medida que a IA se torna mais predominante nas organizações, há uma necessidade crescente de uma melhor compreensão das dependências de dados e do gerenciamento de ativos. As equipas de cibersegurança terão de reavaliar a importância relativa dos ativos de dados, atualizar os inventários e ter em conta as novas ameaças e riscos que estes sistemas de IA podem trazer às suas organizações.

A promessa que a IA traz

Apesar destes desafios, o potencial da IA na segurança cibernética é verdadeiramente emocionante. Ao contrário das soluções de segurança tradicionais que só podem contar com regras predefinidas, a IA pode aprender com o seu ambiente e evoluir os seus protocolos de segurança em conformidade. E é esta adaptabilidade que será crucial num cenário onde novas ameaças surgem constantemente devido às próprias ferramentas que ajudam a preveni-las.

Olhando para o futuro, a integração da IA com outras tecnologias emergentes, como a computação quântica ou a blockchain, poderá levar a soluções de segurança ainda mais abrangentes. Imagine um sistema de segurança cibernética que combine o poder de processamento da computação quântica, a imutabilidade do blockchain e a inteligência adaptativa da IA. Esta combinação pode criar um sistema de defesa altamente robusto como nunca vimos antes.

A estrada à frente

Ao olharmos para o futuro, fica claro que a IA continuará a desempenhar um papel cada vez mais central na segurança cibernética. Na verdade, 87% dos profissionais de TI prevêem que as ameaças geradas pela IA continuarão a impactar as suas organizações nos próximos anos, sublinhando a necessidade de inovação e vigilância contínuas. O segredo da IA será encontrar o equilíbrio certo – aproveitar os seus pontos fortes e ao mesmo tempo mitigar os riscos e limitações. É certamente um desafio, mas também uma oportunidade para construir um mundo digital mais seguro e protegido.

Precisamos de investir no desenvolvimento de sistemas de IA mais robustos e seguros, resistentes à manipulação e capazes de explicar os seus processos de tomada de decisão. Ao mesmo tempo, devemos continuar a nutrir a experiência humana, promovendo uma relação simbiótica entre a intuição humana e a inteligência das máquinas.

Enquanto nos encontramos nesta encruzilhada tecnológica, uma coisa é clara: na batalha contínua contra as ameaças cibernéticas, a IA não é apenas uma ferramenta – é o futuro de todo o campo de batalha.

Como CISO Global da Synechron, uma empresa líder global de consultoria em transformação digital, Aaron Momin é responsável pela gestão de riscos cibernéticos, segurança da informação, gestão de crises e planejamento de continuidade de negócios. Aaron tem 30 anos de experiência no gerenciamento de riscos cibernéticos e tecnológicos, melhorando a maturidade da segurança e integrando a privacidade para organizações globais. Ele é certificado CISO, CISM e CRISC.