kaspersky

A parceria entre humanos e IA na defesa cibernética: capacitando analistas para produzir resultados melhores

O futuro da defesa é híbrido, humanos e IA trabalhando juntos

Todo mundo já viu filmes em que o homem enfrenta uma máquina em um futuro distópico e reconhecerá isso como ficção. Mas com o surgimento da IA generativa e de robôs cada vez mais capazes, há uma batalha real se formando no mercado de trabalho. As pessoas estão cada vez mais preocupadas que suas funções possam ser usurpadas pela tecnologia, e seus medos não são injustificados. O Goldman Sachs previu que até 300 milhões de empregos podem ser perdidos devido à automação.[1]

No setor de cibersegurança, alguns defendem a capacidade da IA de combater ataques cibernéticos como a resposta à escassez de habilidades. Mais de 40% dos profissionais de segurança de TI afirmam que as equipes de segurança de suas organizações[2] não têm pessoal suficiente e precisam de toda a ajuda possível, humana ou de outra natureza.

Mas, embora a IA possa de fato ajudar especialistas a triar e responder a alertas, ela não é uma panaceia. E não substituirá os analistas humanos tão cedo. Automatizar totalmente um centro de operações de segurança (SOC) exigiria que as máquinas aplicassem conceitos abstratos em diferentes situações e as reformulassem. Esse nível de criatividade e pensamento crítico ainda pertence aos humanos, mesmo que os algoritmos de aprendizado de máquina (ML) possam fazer grande parte do trabalho pesado.

1. Goldman Sachs. A IA Generativa Poderia Aumentar o PIB Global em 7%. (Goldman Sachs, 2023).
2. Kaspersky. O Retrato do Profissional Moderno de Segurança da Informação. (Kaspersky Daily, 2024).

Ilya Markelov, líder de Plataformas unificadas da Kaspersky, afirma,

> Em grandes corporações, a automação total não é possível devido às enormes infraestruturas em constante mudança. Uma equipe dedicada ainda é necessária para monitorar as regras que podem se tornar obsoletas da noite para o dia.

A realidade é que uma combinação de pessoas e IA funciona melhor. Essa última deve complementar o expertise humano – e não eliminá-lo – para aliviar as cargas de trabalho das equipes de segurança e permitir que elas se concentrem em tarefas mais críticas.

Os analistas de segurança estão sobrecarregados e esgotados

Os SOCs estão sendo atormentados pelo burnout enquanto lutam contra ataques cada vez mais complexos e frequentes. A escassez de habilidades está agravando a situação em um momento em que as superfícies de ataque estão crescendo rapidamente à medida que as empresas mergulham cada vez mais em sua transformação digital.

Os principais fatores que contribuem para o burnout dos profissionais incluem fadiga de alerta (muitos dos quais podem ser alarmes falsos), trabalho repetitivo e distúrbios do sono, visto que os profissionais frequentemente trabalham em turnos irregulares.

Volumes elevados de alertas são particularmente problemáticos porque limitam análises profundas, o que é crucial para que as equipes de segurança entendam como as ameaças funcionam. O estresse também aumenta os riscos, pois torna mais provável que um analista não perceba uma ameaça iminente. Isso foi evidenciado em um relatório recente, no qual 83% dos profissionais de segurança de TI admitiram que eles (ou alguém em seu departamento) cometeram erros relacionados ao burnout que levaram a uma violação de segurança.[3]

Os líderes das empresas estão, portanto, investindo cada vez mais dinheiro para aliviar os efeitos colaterais do burnout no SOC. Mas em um mercado de trabalho aquecido em que os profissionais de segurança podem definir seu preço, aumentar as contratações não é necessariamente a resposta — e reter talentos pode ser tão difícil quanto encontrá-los. De fato, um quarto dos profissionais de segurança de TI sentem que devem deixar suas empresas para fugir do burnout.[3] E por que um analista estressado não deveria abandonar o barco, especialmente se for por uma recompensa maior?

A IA da Kaspersky faz o trabalho pesado para que os humanos possam se concentrar em tarefas críticas para os negócios

A escassez de habilidades e cargas de trabalho excessivas estão causando burnout e rotatividade de funcionários nas equipes de segurança. Essas equipes precisam de ajuda, e é aí que a Kaspersky e suas soluções baseadas em IA entram. As soluções da empresa são projetadas para aliviar a pressão sobre as equipes de segurança, gerenciando tarefas que exigem muito tempo, como automatizar a triagem e as etapas de resposta inicial. Elas também permitem que profissionais menos qualificados assumam tarefas mais complexas.

Markelov diz,

> A IA da Kaspersky ajuda a reduzir o burnout minimizando o trabalho de rotina, com o sistema oferecendo ações que o usuário pode simplesmente aceitar ou rejeitar. A automação também economiza recursos. Por exemplo, os playbooks (cadeias de ações totalmente automatizadas) podem ser acionados para lidar automaticamente com ameaças.

Um bom exemplo é o AI Analyst no Kaspersky Managed Detection and Response, que ajuda a reduzir a carga de trabalho das equipes do SOC, filtrando automaticamente os falsos positivos, permitindo que os especialistas respondam a ameaças mais rapidamente e evitem o esgotamento. Em outros lugares, o Kaspersky Machine Learning for Anomaly Detection (MLAD), uma solução de software de análise preditiva, está ajudando as empresas do setor industrial a evitar tempo de inatividade ao captar sinais precoces de falha iminente de equipamentos, interrupção de processos, erro humano ou ataque cibernético em sinais de telemetria. O resultado são fluxos de trabalho mais rápidos, desde a detecção até a decisão.

3. Devo. 83% dos Profissionais de Segurança de TI Afirmam que o Burnout Causa Violações de Dados. (Devo, 2023).

Complementação, não apenas automação: IA e humanos em conjunto

Embora a IA da Kaspersky seja capaz de realizar muitas coisas sozinha, ela pode permitir que as equipes de segurança realizem ainda mais, como bloquear ataques complexos e direcionados. IA com envolvimento humano significa que, embora a IA possa operar de forma semi-independente e fazer sugestões, ela ainda é dirigida por um especialista que sempre terá a palavra final. E há muitas razões pelas quais isso é importante. Primeiro, a IA pode sinalizar um comportamento legítimo como suspeito, o que pode resultar em uma ação ilícita. No entanto, os humanos podem verificar ou descartar alertas com o contexto que a IA não possui (por exemplo, operações comerciais, tarefas pontuais), reduzindo interrupções desnecessárias e liberando tempo para lidar com ameaças reais. Humanos e IA trabalhando em harmonia significa que os analistas podem se concentrar exclusivamente nos alertas sobre os quais a IA não tem certeza.

A tomada de decisões é geralmente uma área em que os humanos se destacam. A IA é ótima em reconhecimento de padrões, mas muitas vezes carece de contexto empresarial ou consciência situacional. Os analistas humanos entendem normas organizacionais, requisitos regulatórios e exceções, o que lhes permite tomar decisões mais detalhadas, especialmente em cenários complexos. E como as decisões de cibersegurança podem ter implicações legais e éticas, manter as pessoas no controle reduz a probabilidade de violações de políticas ou criminalidade.

Decisões mais inteligentes, resposta mais rápida, defesa mais forte – mas ainda "IA humana"

A principal crença da Kaspersky é que sua IA deve tornar a cibersegurança mais humana, e não menos. É uma ferramenta poderosa projetada para usabilidade, com painéis visuais, decisões explicáveis e detecção e resposta automatizadas. É um meio para um fim, não um fim por si só.

Na melhor das hipóteses, a IA não substitui os analistas; ela amplifica seusinsights, filtra o ruído e os ajuda a se concentrar no que é mais importante. O resultado são equipes de segurança que não são apenas mais rápidas, mas também mais inteligentes, mais proativas e mais resilientes. E ao manter os humanos no controle, as decisões são baseadas no contexto empresarial, na responsabilidade ética e no julgamento estratégico.

As soluções baseadas em IA da Kaspersky também podem representar uma grande economia de custos porque reduzem as necessidades de contratação.

Markelov explica,

> O número de ameaças, ataques e amostras de malware únicas aumenta a cada ano. Além disso, a complexidade da infraestrutura também está aumentando à medida que as organizações adotam novos sistemas e abrem novos escritórios. Para lidar com essa crescente complexidade, nossas soluções implementam IA e automação, eliminando a necessidade de as organizações aumentarem suas equipes de segurança proporcionalmente.

Sobre a Kaspersky

A Kaspersky é uma empresa global de cibersegurança e privacidade digital fundada em 1997. Com mais de um bilhão de dispositivos protegidos contra ameaças cibernéticas emergentes e ataques direcionados, a inteligência de ameaças profunda e o expertise em segurança da Kaspersky estão constantemente se transformando em soluções e serviços inovadores para proteger empresas, infraestrutura crítica, governos e consumidores em todo o mundo. O portfólio de segurança abrangente da empresa inclui proteção de endpoint líder, produtos e serviços de segurança especializados e soluções de imunidade cibernética para combater ameaças digitais sofisticadas e em constante evolução. Ajudamos mais de 200.000 clientes corporativos a proteger o que mais importa para eles. Saiba mais em www.kaspersky.com.

Conclusão

A cibersegurança não é um caso de IA versus humanos, mas de humanos mais IA. O objetivo da Kaspersky não é substituir os analistas, mas capacitá-los dando a eles ferramentas para responder mais rapidamente, agir com mais precisão e ficar à frente das ameaças em evolução.

A Kaspersky cria soluções de IA para aprimorar os defensores humanos, permitindo que eles permaneçam focados, atualizados e preparados, mesmo diante de volumes de alertas avassaladores e ataques sofisticados.

www.kaspersky.com.br