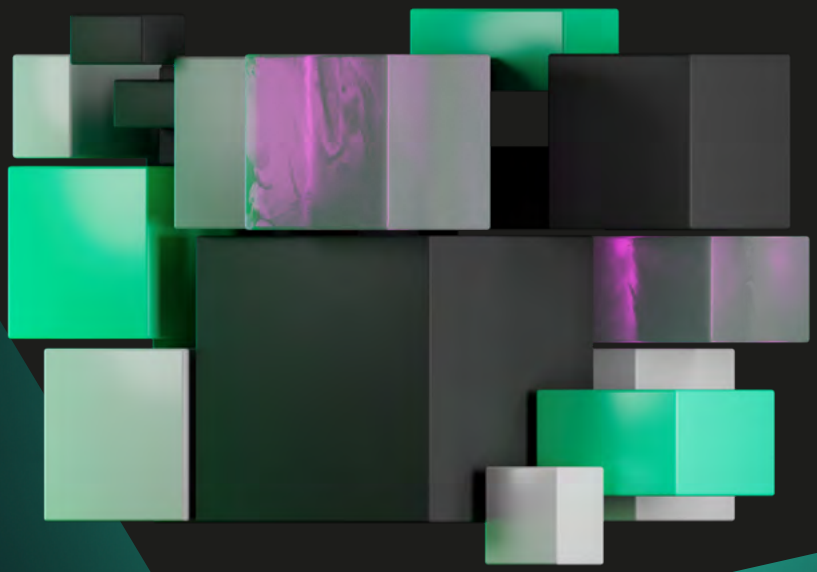
kaspersky



O futuro da IA na cibersegurança: o que vem a seguir?

Uma nova era de cibersegurança chegou

Poucos setores conseguem alcançar a velocidade de crescimento da segurança. A inovação e a persistência do invasor garantem que ela nunca fique parada. Em 2024, por exemplo, o tempo médio para investigar e relatar incidentes cibernéticos aumentou em 48% em comparação ao ano anterior, refletindo um aumento significativo na complexidade dos ataques.[1]

A IA também facilitou o aumento no volume de ataques, com criminosos automatizando tarefas como codificação, redação e reconhecimento. A barreira de entrada também foi reduzida, com adversários menos qualificados conseguindo fazer mais com o mesmo conjunto limitado de habilidades.

Vladislav Tushkanov, gerente de grupo no Kaspersky AI Technology Research Center, diz:

> Aqueles que já são qualificados conseguem trabalhar mais rapidamente – e aqueles que não são adquirem mais capacidade. Isso é chamado de "uplift" - quando um aluno completamente alfabetizado consegue fazer algo que não conseguia antes. Em vez de passar um mês estudando programação, eles podem simplesmente perguntar ao ChatGPT.

1. Kaspersky, MDR Analyst Report 2024, (Kaspersky, 2025)

Não é surpresa que, em 2024, a maioria dos profissionais de segurança da informação tenha visto um aumento notável em ataques cibernéticos em comparação ao ano anterior.[2] Isso ocorreu porque a IA deixou de ter um papel ofensivo periférico para um papel central. O mesmo vale para a defesa, com a IA ajudando a detectar anomalias rapidamente e a diminuir a carga da equipe de segurança de TI.

E assim, a corrida armamentista da IA está em andamento. Uma das pioneiras nessa corrida é a Kaspersky, que vem utilizando IA em suas soluções desde 2004. Ao contrário de muitos fornecedores que ainda estão tentando entender seu potencial defensivo, a Kaspersky já construiu experiência comprovada, conforme demonstrado por seu AI Technology Research Center.

Isso significa que ela está perfeitamente posicionada não apenas para prever ameaças, mas também para moldar o que vem a seguir, garantindo que seus clientes possam prosperar em condições cada vez mais complexas.

As ameaças cibernéticas estão se tornando nativas da IA

Criminosos estão adotando ferramentas de IA para maximizar a velocidade e a discrição de seus ataques. Um proponente particularmente perigoso são os deepfakes, que abrangem conteúdo de imagem, vídeo e áudio gerado por IA. A empresa de engenharia britânica Arup foi vítima desse tipo de conteúdo quando um funcionário foi enganado por uma videochamada gerada por IA e fez com que ele enviasse US$ 25 milhões para criminosos.[3] Em outro lugar, fraudadores desviaram US$ 35 milhões após falsificar e-mails e áudios para convencer um funcionário de uma empresa dos Emirados Árabes Unidos de que um diretor precisava de dinheiro para uma aquisição.[4]

Tushkanov acrescenta:

> A mídia sintética permite que invasores retratem eventos que não aconteceram e os usam contra usuários finais e empresas. A comunidade cripto frequentemente sofre. Por exemplo, golpistas coletam dinheiro que dizem ser para caridade ou se passam por seu chefe e solicitam uma transferência bancária.

Isso tornou os ataques mais pessoais e direcionados do que nunca. Eles brincam com as emoções da vítima – sejam medo, ganância ou confiança – para induzi-la à ação. Mas não são apenas os deepfakes que causam problemas. A IA pode aprimorar ou automatizar vários estágios de um ataque cibernético. Ela pode aumentar significativamente a velocidade, a eficiência e a adaptabilidade do ataque, por exemplo, fornecendo ao invasor recomendações contextuais sobre como evitar a detecção por soluções de segurança.

Ela também pode permitir que invasores menos qualificados façam mais e mais rapidamente. No entanto, esse método de cortar e colar resultou em ataques extremamente parecidos em termos de execução. Então, embora haja um bombardeio constante deles, não é particularmente difícil detectá-los.

Tushkanov explica:

> Para detectar IA e evitar que seus analistas fiquem atolados na rotina na análise diária de um número cada vez maior de alertas, você precisa de aprendizado de máquina (ML). Ele lida perfeitamente com isso – e seus profissionais economizarão tempo para tarefas complexas ou críticas para os negócios.

O aumento no volume de ataques deixou 72% das empresas seriamente preocupadas com o uso de IA por invasores.[5] Eles querem defesas igualmente rápidas e inteligentes, talvez sabendo que as defesas tradicionais têm dificuldades contra ameaças escaláveis e autoevolutivas. Portanto, é crucial que as empresas possam contar com fornecedores com experiência na implementação de IA para ficarem à frente dos invasores.

Vladislav Tushkanov diz:

> Não deveríamos pensar que "tudo está perdido, os cibercriminosos vão hackear todo mundo agora". Deveríamos dizer: "A IA nos deu o mesmo aumento de eficiência", porque todos os envolvidos em ciberdefesa e monitoramento de ameaças gostam de usar IA tanto quanto os caras maus.

2. Kaspersky, Defesa Cibernética e IA: Tudo Pronto para Proteger Sua Organização? (Kaspersky, 2024)
3. Milmo Dan, empresa de engenharia britânica Arup, é vítima de golpe deepfake de £ 20 milhões (The Guardian, 2024)
4. Lemos Robert, Áudio deepfake arrecada US$ 35 milhões em assalto corporativo (Dark Reading, 2021)
5. Kaspersky, Preocupações crescentes, lacunas persistentes: a maioria das organizações teme ataques cibernéticos baseados em IA, mas carece de defesas essenciais, (Kaspersky, 2024)

A IA é a nova pedra fundamental da cibersegurança

Está claro que a IA está se tornando a base da segurança moderna, evoluindo de uma ferramenta de suporte para a inteligência central que impulsiona sistemas de defesa avançados. Seu papel crescente traz uma mudança em direção à análise preditiva e à conscientização contextual como capacidades fundamentais na detecção e resposta a ameaças.

Aproveitar o potencial da IA exige profundo conhecimento, experiência comprovada e uma base de confiança. Também exige a capacidade de se adaptar e aprender com a telemetria global. Isso é algo que a Kaspersky vem fazendo há anos, garantindo que suas defesas estejam um passo à frente em um cenário de ameaças em constante mudança. Seu profundo expertise em aplicar essas tecnologias à cibersegurança, juntamente com seus conjuntos de dados exclusivos, métodos eficientes e infraestrutura avançada de treinamento de modelos, tornaram-se a base de sua abordagem para resolver desafios de negócios complexos.

Mas qual é a real diferença entre um fornecedor como a Kaspersky e um novato qualificado? Vladislav Tushkanov diz:

> É uma diferença de abordagem, claro. Se você faz isso há muito tempo, entende os desafios que pode enfrentar, porque é muito mais provável que já os tenha enfrentado antes. E isso reduz a probabilidade de erros críticos. Você não pode obter essa experiência de nenhuma outra forma – somente aprendendo na prática.

Portanto, embora a IA esteja se tornando cada vez mais importante para os fornecedores de cibersegurança, ela não é tão simples quanto "pegar e usar". É algo que deve ser incorporado às soluções e iterado ao longo do tempo, aproveitando a vasta telemetria global para ser eficaz. É por isso que a Kaspersky consegue analisar e classificar mais de 460.000 amostras maliciosas todos os dias usando tecnologias de IA.

Como a IA do futuro transformará as operações de segurança

Um objetivo fundamental na cibersegurança não é apenas reduzir o tempo médio de resposta, mas também prevenir ataques antes que eles aconteçam. A IA é essencial para atingir esse objetivo, pois permite a detecção mais rápida, respostas automatizadas e recursos preditivos que permitem que as empresas passem de uma defesa reativa para uma proativa. Ao antecipar ameaças e agir em tempo real, a IA pode reduzir significativamente as janelas de resposta e minimizar os danos.

Mas atingir esse objetivo não significa substituir os profissionais de cibersegurança, e sim capacitá-los. A colaboração entre humanos e IA definirá a próxima era da ciberdefesa à medida que a IA lida cada vez mais com tarefas repetitivas e fornece insights que orientam a tomada de decisões. Os analistas poderão se concentrar em investigações complexas e planejamento estratégico, apoiados por sistemas inteligentes que aprendem e se adaptam junto com eles. Tushkanov acrescenta:

> No momento, todo mundo está falando sobre "agentes". Isso se refere a sistemas ou componentes inteligentes que executam tarefas de forma autônoma ou semiautônoma para proteger ambientes. Você diz a eles: "Tenho esse script em execução no host, o que vocês acham?", e eles dizem: "Em condições normais, isso não deveria ser executado". Eu comunicaria a ocorrência".
>
> Então, há uma hipótese: se você puder criar um sistema de agente onde possa carregar contexto suficiente para que um analista humano de primeira linha possa tomar uma decisão informada, então, teoricamente, grandes modelos de linguagem (LLMs) seriam capazes de decidir com igual confiabilidade. Isso significaria mais automação de primeira linha. Há coisas que são fáceis de programar: uma sequência clara de ações necessárias. E, teoricamente, você pode escrever um script que executará essas ações, receberá as variáveis necessárias para a decisão e tomará essa decisão.
>
> Mas muitos cenários não funcionam dessa maneira. Durante a investigação, há várias opções de aonde ir e o que observar. Somente um olho humano pode entender em que direção a investigação deve prosseguir. No futuro, os agentes LLM poderão tomar tais decisões. Mas, no momento, o toque humano é crucial.

Construindo uma IA resiliente e confiável para uma defesa mais inteligente

A Kaspersky não está interessada apenas em manter a segurança humana no despertar da IA. Ela também se dedica ao desenvolvimento de IA confiável e segura capaz de estar sempre à frente das ameaças emergentes. O desenvolvimento e a aplicação seguros da IA são, portanto, essenciais para sua estratégia de negócios porque garantem que seus algoritmos sejam confiáveis e resilientes. Por exemplo, ela treina sua IA sob padrões de segurança rigorosos para que suas detecções nunca sejam manipuladas e trabalha duro para proteger seus modelos de exploração. Isso está alinhado às crescentes expectativas em torno de ética, transparência e conformidade e é especialmente benéfico para os clientes da Kaspersky em setores altamente regulamentados. Para construir ainda mais confiança, o fornecedor abre suas portas periodicamente para revelar seu funcionamento interno.

Conclusão: o futuro da segurança é alimentado pela IA

O futuro da cibersegurança será nativo da IA, moldado não apenas pelo poder dos algoritmos, mas pela confiança, resiliência e julgamento humano por trás deles. À medida que as ameaças se tornam mais complexas e velozes, os líderes desta nova era serão aqueles que conseguirem combinar perfeitamente IA de ponta com décadas de experiência em segurança no mundo real.

O legado da Kaspersky em cibersegurança, aliado ao seu profundo e contínuo investimento em IA, está fornecendo soluções que não são apenas inteligentes, mas também resilientes, adaptáveis e prontas para o futuro. Da detecção preditiva de ameaças à resposta autônoma, estamos construindo sistemas que aprendem, evoluem e defendem, capacitando as organizações a permanecerem à frente, não apenas a se manterem atualizadas.

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.

www.kaspersky.com.br