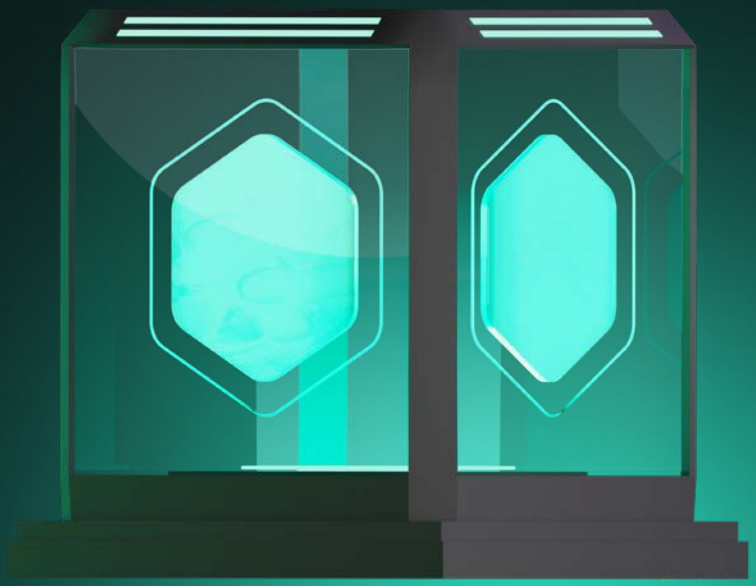
kaspersky

Superando os desafios de SOC com a IA



Superando os desafios de SOC com a IA

A IA já se tornou, sem sombra de dúvidas, um multiplicador de forças. Um único desenvolvedor pode orquestrar um exército de agentes de código IA para trabalhar com diversas tarefas, enquanto profissionais de marketing podem focar na estratégia enquanto aguardam por tarefas de pesquisa profunda ficarem prontas, fornecendo as informações contextuais de que eles precisam. Mas os cibercriminosos também já estão cientes disso e, por isso, o volume de ciberataques continua a crescer. Criminosos mais amadores estão acionando ataques que antes estavam muito além da sua capacidade, enquanto grupos em nível de APT estão automatizando seus mecanismos e processos de ação.

Para grandes empresas, isso significa que o pessoal de cibersegurança também precisa começar a cultivar o poder da IA. Felizmente, isso não significa que eles devem correr para contratar cientistas de dados, que podem ser tão ou mais difíceis de achar do que analistas de centros de operações de segurança (SOC). Em vez disso, o cenário indica que fornecedores de cibersegurança que querem se manter competitivos, devem integrar tecnologias de IA, desde algoritmos de aprendizagem de máquina de eficácia comprovada a ferramentas de IA generativa (GenAI) de ponta.

Separando o joio do trigo

O primeiro desafio no qual as soluções de IA podem ajudar é em relação à quantidade avassaladora de saturação enfrentada pelos SOCs modernos. Infraestruturas modernas de grande porte usadas pelos profissionais geram montanhas de alertas em potencial que consomem o tempo precioso dos analistas, levando à exaustão e ao aumento de risco de uma ameaça verdadeira passar despercebida.

Um exemplo disso é alguém que faz login em um PC corporativo de um local inesperado: será um hacker que penetrou em uma conta de administrador ou apenas o gerente de vendas verificando sua conta durante uma viagem de negócios? Em uma empresa de grande porte, é impossível verificar manualmente todas essas ocorrências. É nesse cenário que a IA torna-se a salvação. Algoritmos especiais, como os usados no Kaspersky MDR e introduzidos no Kaspersky SIEM e XDR, ajudarão a detectar esses casos onde o padrão é interrompido e que exigem atenção imediata.

Outro exemplo é a inteligência contra ameaças. Um analista trabalhando com inteligência contra ameaças pode precisar peneirar dezenas de fontes em diferentes linguagens para entender se um indicador de comprometimento (IoC) em particular, digamos, um endereço da web suspeito, representa uma ameaça para a empresa. Ao integrar soluções GenAI, como o Kaspersky Threat Intelligence Portal, um analista pode compreender melhor esses dados como informações acionáveis, por exemplo, identificar uma gangue de cibercriminosos associada a um IoC e que setores da indústria estão na sua mira. Isso acelera consideravelmente o processo de tomada de decisão.

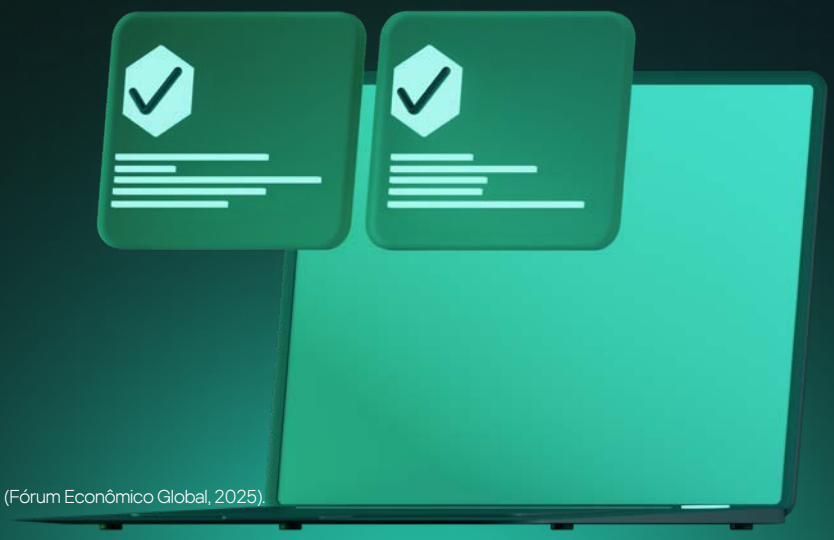
Tais ferramentas, por exemplo, pontuação de alerta e priorização orientada por IA no Kaspersky SIEM e XDR, não substituem os analistas. Em vez disso, a ideia é aumentar a capacidade dos analistas ao permitir que foquem em coisas mais importantes em vez de se perderem em um mar de informações.

Suprindo a lacuna da escassez de talentos

De acordo com o Fórum Econômico Mundial, 67% das organizações informaram contar com uma deficiência de habilidades de nível moderado a crítico em cibersegurança[1]. Devido à escassez aguda de talentos e um alto índice de burnout, o contingente de analistas de SOC é dominado por talentos juniores.

Uma maneira de ajudar empresas é orientar seus analistas em como tratar ameaças desconhecidas, educando-os durante suas operações. É nesse contexto que assistentes de GenAI, como o Kaspersky Investigation and Response Assistant (KIRA) se mostram altamente úteis. Usando uma enorme quantidade de conhecimento acumulada de grandes modelos de linguagem durante o treinamento, esses assistentes são capazes de fornecer insights críticos sobre eventos de segurança durante a análise, facilitando a tomada de decisão.

Por exemplo, o KIRA pode analisar comandos PowerShell complicados (uma maneira comum de executar comandos usados por administradores e criminosos), esclarecendo elemento por elemento e avaliando o nível de ameaça que tais comandos representam. Isso não apenas ajuda analistas juniores, mas também serve como fonte de segunda opinião para profissionais mais experientes. Claro que assistentes de GenAI podem solucionar diversas outras tarefas, desde resumo de incidentes em relatórios acionáveis até a avaliação de riscos de segurança de imagens Docker, e uma gama de casos de uso que continuam a evoluir.



1 Fórum Econômico Global, Cenário de cibersegurança global (Fórum Econômico Global, 2025).

O poder da integração

A IA é conhecida pela sua insaciedade de dados, razão pela qual empresas orientadas por dados geralmente lideram nessa tecnologia. A cobertura global e uma cultura de dados bem desenvolvida se traduz em insights que se tornam novas tecnologias. Por exemplo, graças ao Kaspersky Security Network- KSN, a Kaspersky está posicionada de maneira singular para analisar o comportamento de softwares no ciberespaço em todo o mundo, o que se converte em competências únicas, como a tecnologia de Detecção de Sequestro de DLL no Kaspersky MDR, SIEM e XDR. Esse componente de IA possibilita aos produtos detectarem sequestro de DLL, uma técnica disseminada (especialmente em ataques direcionados) onde agentes malignos usam um código malicioso incorporado em um software confiável. Esse ataque é conhecidamente difícil de detectar, mas com a IA, analistas de SOC podem obter visibilidade imbatível sobre o comportamento anômalo de softwares, lhes proporcionando a capacidade de deter o ataque antes que aconteça.

Não existe uma única solução, seja de IA ou não, que possa solucionar todos os problemas de cibersegurança e satisfazer todas as necessidades de cibersegurança de uma empresa moderna. No entanto, a integração metódica de tecnologias cada vez mais avançadas nos fluxos de trabalho de SOC podem transformar benefícios quantitativos, como tempo reduzido de resposta, em benefícios qualitativos, resultando em uma infraestrutura mais segura. E com a IA, essa mudança qualitativa pode estar mais acessível do que nunca.

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.br.

www.kaspersky.com.br