kaspersky

Democratizando a cibersegurança: como a IA da Kaspersky está tornando a defesa acessível a todos

A nova grande divisão da cibersegurança

Ameaças cibernéticas são como um trem de carga desgovernado descendo a ladeira. Elas continuam ganhando momento e detê-las é difícil até mesmo para as organizações mais resilientes. A defesa cibernética de nível especializado, antes um privilégio, tornou-se uma necessidade. Mas essa necessidade não pode ser satisfeita facilmente. Há uma escassez de pessoas com as habilidades, o conhecimento e a experiência necessários para intervir, e até mesmo as empresas mais ricas estão tendo dificuldades para recrutá-las.

No entanto, tradicionalmente, o mundo tem contado com esses especialistas para garantir a segurança. Antes que a cibersegurança se tornasse uma função empresarial essencial, quando as ameaças cibernéticas existiam, mas não em tanta abundância, bastava um par de especialistas que soubessem gerenciar antivírus e firewalls básicos. Na última década, no entanto, ataques que ganharam manchetes como NotPetya, WannaCry e SUNBURST aniquilaram a ideia de que defesas básicas são o suficiente.

Um novo pêndulo de segurança agora oscila na forma da IA, e ele é cobiçado tanto por malfeitores quanto por defensores. Ele pode facilitar ataques mais rápidos e abrangentes, mas também pode preencher a lacuna de habilidades de segurança ao equipar usuários comuns e empresas com recursos avançados, reduzindo a barreira de entrada. Se democratizada, a IA na cibersegurança reduzirá – sem eliminar – a necessidade de especialistas para que todas as empresas tenham uma chance justa de se defender.

A Kaspersky está usando seu próprio expertise em IA para concretizar essa visão.

Escassez de expertise em cibersegurança

O mundo está atravessando uma escassez global de profissionais de segurança qualificados e experientes. Mais de 40% dos profissionais de segurança da informação dizem que as equipes de segurança de suas organizações estão sendo "um pouco" ou "significativamente" afetadas com a falta de pessoal, enquanto metade deles diz que o conhecimento teórico adquirido em sua educação formal foi inútil quando se tratou de executar seu trabalho atual. Menos da metade deles teve experiência prática na faculdade ou universidade.[1]

A escassez de profissionais de segurança preparados é só um dos problemas. Muitas organizações não tem condições pagar por eles, o que torna impossível administrar um centro de operações de segurança (SOC) 24 horas por dia, 7 dias por semana. Mesmo aquelas que podem dispor de uma grande quantidade de recursos estão enfrentando dificuldades para recrutar, com 48% dos profissionais de segurança da informação afirmando que mais de seis meses são necessários para o preenchimento de uma vaga.[1]

Infelizmente, mesmo os produtos mais avançados não conseguem proteger uma organização sozinhos. Eles exigem operadores qualificados para serem eficazes, o que significa que a falta de analistas e operadores qualificados deixa as organizações vulneráveis.

A escassez de habilidades se agrava ainda mais com o burnout entre os profissionais de operações de segurança. Ilya Markelov, líder de Plataformas unificadas da Kaspersky, afirma:

> Quando um profissional de cibersegurança faz bem seu trabalho, suas tarefas do dia a dia devem ser em grande parte rotineiras – verificar registros, revisar contas, verificar regras, garantir a conformidade com políticas, etc. Embora essas tarefas possam não ser complexas, elas são essenciais. Fazê-las manualmente leva rapidamente ao burnout e, como resultado, os analistas frequentemente consideram mudar de emprego ou profissão. Um dos objetivos de nossa IA é reduzir a sobrecarga operacional e minimizar as tarefas de rotina.

A escassez de habilidades, combinada com a complexidade das ameaças modernas, tornou o monitoramento e a resposta manuais inviáveis para a maioria das empresas. Os incidentes que poderiam ter sido detectados precocemente estão passando despercebidos e resultando em perdas financeiras para empresas em todos os lugares.

Inteligência artificial da Kaspersky como o equalizador

A Kaspersky desenvolve cibersegurança com tecnologia de IA há mais de 20 anos, e seus modelos de aprendizado de máquina (ML) são treinados com inteligência global de ameaças e utilizam uma enorme quantidade de telemetria. Eles podem identificar os alertas mais críticos de seus sistemas de monitoramento, garantindo que os clientes da Kaspersky tenham tempo para focar nas ameaças mais sérias.

A empresa também treina seus modelos com todo o conhecimento disponível do setor, e não apenas com o próprio. Vejamos por exemplo a matriz MITRE ATT&CK, um enorme banco de conhecimento sobre táticas, técnicas e procedimentos dos invasores. A IA da Kaspersky recomenda ações de resposta a incidentes com base nas descrições da estrutura, o que significa que ela não depende exclusivamente da sua própria experiência.

Markelov diz,

> Outro bom exemplo da nossa IA em ação é o sistema de gerenciamento de eventos de informações de segurança (SIEM) da Kaspersky. Se houver um log contendo um evento de cibersegurança, o usuário verá o evento como uma string criptografada e completamente ininteligível. Isso ocorre porque os operadores de malware tentam ocultar sua presença em logs criptografando seus comandos. Mas nosso módulo de IA decodifica esses comandos das strings distorcidas e explica o que o script fará — em uma linguagem legível e fácil de entender.
>
> Anteriormente, para processar um evento desse tipo e determinar se ele era perigoso, o operador tinha que encontrar um script para decodificar a cifra, como Base64. Isso exigia conhecimento e esforço para identificar o código, descriptografá-lo para ver o comando, como um script do PowerShell com vários parâmetros e abrir a documentação do PowerShell para entender o que aconteceria se o script fosse executado.
>
> Nossa IA garante que nada disso seja necessário. O operador simplesmente clica em um botão na interface e nosso módulo explica o que o script fará, incluindo um alerta de semáforo indicando o nível de risco de cada ameaça.

Tudo o que a Kaspersky se esforça para fazer com IA é pensando no cliente. É por isso que a empresa tem um grande foco em facilidade de implantação, painéis intuitivos e proteção proativa que simplifica a vida das equipes de segurança.

---

[1] Kaspersky. O Retrato do Profissional Moderno de Segurança da Informação. (Kaspersky Daily, 2024).

Por que e como a Kaspersky está tornando a segurança de nível empresarial acessível a todos

A Kaspersky passou anos coletando dados sobre, experimentando com e implantando IA em suas soluções. Mas ela considera esse expertise inútil, a menos que ele possa ser difundido para todos. A filosofia da empresa é que toda empresa tem direito à segurança de classe mundial – seja uma startup de tecnologia, um grande hospital ou um banco digital – e que quanto mais seguras as organizações estiverem coletivamente, mais próximo estará um amanhã seguro.

PMEs

A Kaspersky está particularmente interessada em ajudar pequenas e médias empresas (PMEs) que podem não ter o orçamento ou o expertise necessários para manter uma equipe de segurança dedicada. Suas soluções baseadas em IA podem ajudar essas empresas a detectar ameaças, incluindo malware, ransomware e phishing, automaticamente, sem intervenção humana constante, o que significa que elas podem aumentar muito sua segurança sem contratar pessoas.

Seus sistemas também se integram perfeitamente à infraestrutura de TI existente e podem fornecer alertas em tempo real para atividades suspeitas, e até mesmo adotar medidas automatizadas para neutralizar ameaças. Isso significa que seus clientes PMEs podem se proteger com o mínimo de esforço e custo — quase como ter seu próprio analista virtual.

Markelov diz,

> Utilizamos IA para permitir que pessoas menos qualificadas e experientes realizem tarefas complexas de gerenciamento de produtos de segurança. A IA generativa reduz os requisitos de habilidade porque o sistema explica e orienta extensivamente – aconselhando onde procurar, o que fazer e o que um comando específico faz –, tudo em linguagem simples. Ela fornece o contexto necessário e informações adicionais ao usuário, reduzindo assim os requisitos de habilidade e experiência.

Mas, apesar da forte automação, a decisão final sempre cabe ao operador humano, pois a empresa acredita no direito de toda empresa à autonomia.

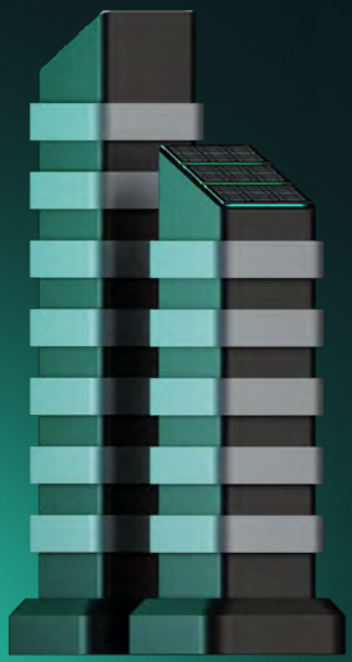
Empresas

Ao contrário das empresas menores, as grandes corporações frequentemente contam com equipes de segurança maduras. A IA da Kaspersky veio para complementar essas equipes, e não para substituí-las.

Markelov continua,

> O valor está na redução da carga de trabalho da equipe, diminuindo os requisitos de habilidade e maximizando a eficiência por meio da automação. A IA não substitui analistas, mas permite que eles se concentrem em tarefas críticas em vez de ficarem atolados na rotina.

As grandes empresas também estão enfrentando uma complexidade cada vez maior, não apenas à medida que adotam novos sistemas, mas também porque são alvos de ataques mais avançados.
A IA e a automação da Kaspersky podem equipar suas equipes de segurança para gerenciar essa complexidade crescente, eliminando a necessidade de crescimento proporcional e, por fim, economizando dinheiro.



O que você recebe: confiança, transparência e desempenho de elite

O desejo da Kaspersky é que a cibersegurança beneficie a todos. E isso significa que aqueles que a utilizam devem poder confiar nela. 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. Ela treina sua IA sob padrões de segurança rigorosos, por exemplo, para que você saiba que suas detecções nunca são manipuladas, e trabalha duro para proteger seus modelos de exploração.

Markelov comenta,

> À medida que nossos modelos de IA continuam aprendendo, nossos especialistas revisam os resultados e os ajustam conforme necessário. Também fornecemos aos usuários o raciocínio completo por trás das decisões da IA. Por exemplo, em vez de apenas indicar que uma luz verde é igual a segurança, explicamos por que a IA a considera segura. Também indicamos se achamos que a IA pode estar alucinando e deixamos todas as decisões finais com o usuário.

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, a empresa abre suas portas periodicamente para revelar seu funcionamento interno.

Em outro lugar, sua unidade de pesquisa dedicada, o Kaspersky AI Technology Research Center, reúne cientistas de dados, engenheiros de ML, especialistas em ameaças e especialistas em infraestrutura para enfrentar as tarefas mais desafiadoras na interseção de IA/ML e cibersegurança. Isso inclui não apenas o desenvolvimento de tecnologias aplicadas, mas também pesquisas sobre a segurança de algoritmos de IA.

Acompanhando essa confiança e transparência está um desempenho de elite, já que a IA é uma das bases de suas soluções premiadas dia após dia. Como exemplo, sua tecnologia de IA fechou mais de 70.000 alertas em seu saMDR service in 2024.[2]

Markelov diz,

> Todas as nossas tecnologias são testadas de forma independente. A Kaspersky participa de muitas comparações de mercado que avaliam os recursos de detecção e resposta de todos os nossos produtos – nas quais lideramos consistentemente em precisão e velocidade de resposta. E não apenas para IA, mas para todo o nosso conjunto de produtos.

[2]Kaspersky. MDR Analyst Report 2024. (Kaspersky, 2025).

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, bem como 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 IA na cibersegurança deixou de ser opcional. Ela tornou-se essencial para acompanhar os criminosos e ajudar a preencher a lacuna de habilidades em cibersegurança. Felizmente, a IA encontrada nas soluções da Kaspersky está disponibilizando cibersegurança de elite para todas as empresas.

www.kaspersky.com.br