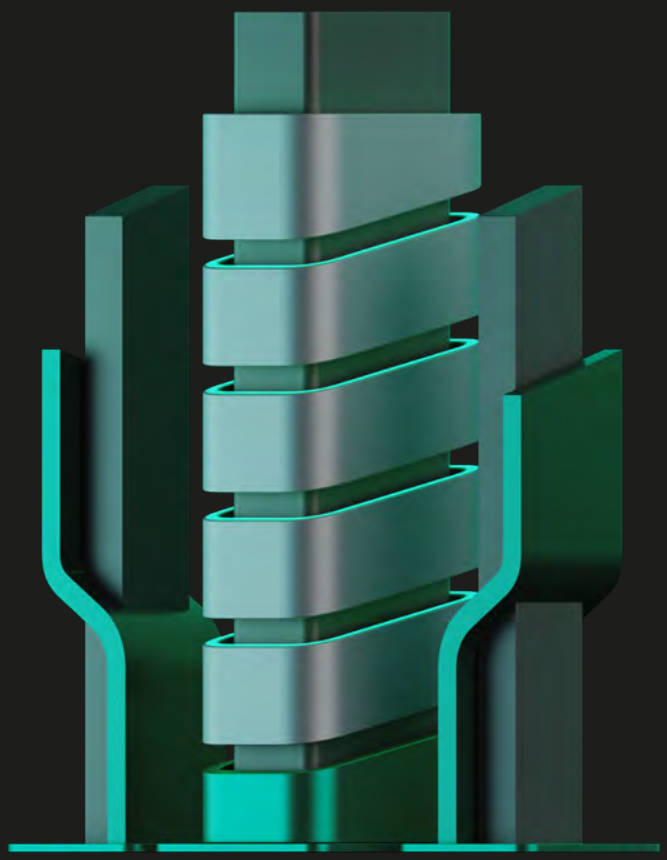
kaspersky



Por dentro da IA da Kaspersky: utilizando aprendizado de máquina para combater as ameaças cibernéticas em evolução

O problema do uso duplo

Nos últimos anos, a inteligência artificial (IA) e o aprendizado de máquina (ML) vêm sido cada vez mais adotados por criminosos para tornar seus ataques mais eficazes e acelerar tarefas de rotina. Exemplos incluem o uso de grandes modelos de linguagem (LLMs) para escrever software malicioso e mensagens de phishing personalizadas, além de criar deepfakes de áudio e vídeo.

Uma pesquisa da Kaspersky mostra que as organizações estão reconhecendo os perigos desses ataques. Uma pesquisa com profissionais de segurança de TI e segurança da informação que trabalham para PMEs e grandes empresas descobriu que quase três quartos consideram o uso de IA por criminosos cibernéticos uma preocupação séria. Muitos dizem que não têm conhecimento especializado externo relevante em cibersegurança à disposição, que suas equipes de TI não são grandes o suficiente e que não acreditam ter soluções de segurança adequadas, o que os expõe a vulnerabilidades potenciais.

Novas ameaças. Defesas transformadoras.

Então, que tipos de recursos o ML oferece para proteção contra esses ataques em evolução?

A Kaspersky utiliza ML em soluções de detecção de ataques de dois tipos distintos: ML supervisionado e não supervisionado. No ML supervisionado, um modelo é treinado com dados relacionados à atividade dos invasores, com o objetivo de identificar comportamentos maliciosos semelhantes. O ML não supervisionado, por sua vez, envolve a criação de perfis de comportamento legítimo de sistemas e serviços para detectar anomalias, desvios e discrepâncias. Isso permite que a Kaspersky desenvolva soluções para lidar com problemas e desafios específicos de cibersegurança.

Três exemplos importantes dessas soluções, todas aprimoradas significativamente desde sua introdução em 2018, são o AI Analyst for Kaspersky MDR, o Adaptive Anomaly Control e o Kaspersky Machine Learning for Anomaly Detection.

1

O "Auto-Analyst", desenvolvido pela equipe de MDR e pelo centro de pesquisas de IA da Kaspersky para ajudar na filtragem inicial de alertas, é um sistema de ML supervisionado treinado em alertas de SIEM, combinado com um veredito do SOC em cada alerta, que permite que a IA identifique com segurança falsos positivos gerados por atividades legítimas de rede.

2

O Adaptive Anomaly Control é uma ferramenta de redução de superfície de ataque que combina a simplicidade de regras de proteção com ajuste automático por meio de análise de comportamento. Usado nas soluções de segurança de endpoint da Kaspersky, ele reúne um conjunto abrangente de regras de controle eficazes baseadas em dados de ML, algoritmos de análise de comportamento para encontrar novas heurísticas potenciais de ações suspeitas e adaptação automatizada com base na análise da atividade do usuário.

3

Com o número de ataques a sistemas industriais e superfícies de ataque aumentando constantemente, o Kaspersky Machine Learning for Anomaly Detection usa uma rede neural para monitorar simultaneamente uma ampla gama de dados de telemetria e identificar anomalias na operação de sistemas ciberfísicos, detectando ataques à tecnologia operacional (TO) em um estágio inicial de desenvolvimento e adicionando uma camada extra e crítica de proteção industrial.

Esses tipos de soluções demonstram a amplitude e a profundidade dos recursos oferecidos pela IA e pelo ML e, desde que foram introduzidos, a Kaspersky tem lançado continuamente novas ferramentas que abordam ameaças e problemas cada vez mais desafiadores. Isso inclui um sistema de quarentena de spam baseado em redes neurais profundas, um sistema de detecção de phishing baseado em ML, IA para SIEM/XDR, resumos de inteligência de ameaças baseados em IA generativa e o Kaspersky Investigation and Response Assistant, com muitos outros em desenvolvimento.

O que a Kaspersky alcançou ao utilizar ML

A Kaspersky vem integrando IA — especialmente ML — em seus produtos e serviços há quase duas décadas, e sua profunda experiência na aplicação dessas tecnologias à cibersegurança, juntamente com seus conjuntos de dados exclusivos, métodos eficientes e infraestrutura avançada de treinamento de modelos, permitem que ela resolva desafios empresariais complexos.

Seu compromisso com a inovação neste campo é reforçado pelos recém-aprimorados recursos de IA em sua solução de informações de segurança e gerenciamento de eventos (SIEM).

Sobre a Kaspersky

A Kaspersky é uma empresa de privacidade digital e segurança cibernética global 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 abrangente de segurança 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.

www.kaspersky.com.br