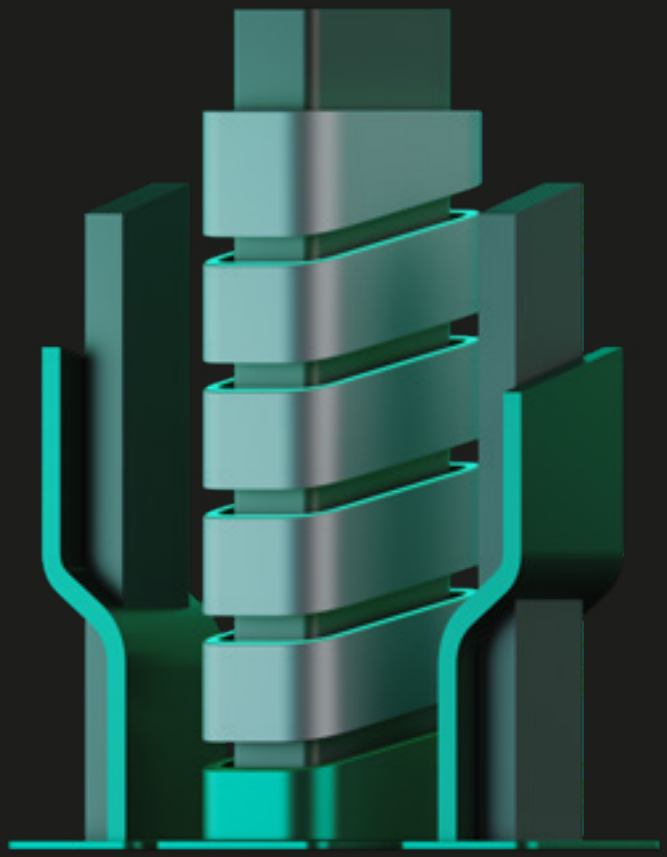
kaspersky



Inside Kaspersky AI: leveraging machine learning to combat evolving cyberthreats

The dual-use problem

In recent years, artificial intelligence (AI) and machine learning (ML) have increasingly been adopted by bad actors to make their attacks more effective and speed up routine tasks. Examples include using large language models (LLMs) to write malicious software and personalized phishing messages, and creating audio and video deepfakes.

Research by Kaspersky shows that organizations are recognizing the dangers of these attacks. A survey of IT security and information security professionals working for SMEs and enterprises found that almost three-quarters consider the use of AI by cybercriminals a serious concern. Many say they don't have the relevant external cybersecurity expertise at their disposal, their IT teams aren't large enough, and they don't think they have adequate security solutions in place, exposing them to potential vulnerabilities.

New threats. Transformative defenses.

So what kinds of capabilities does ML enable to protect against these evolving attacks?

Kaspersky has been using ML in attack-detection solutions of two distinct types – supervised and unsupervised ML. In supervised ML, a model is trained on data related to attackers' activity, with the aim of identifying similar malicious behavior. Unsupervised ML, meanwhile, involves profiling the legitimate behavior of systems and services to detect anomalies, deviations and outliers. This enables Kaspersky to develop solutions addressing specific cybersecurity issues and challenges.

Three prime examples of these solutions, all of which have been significantly enhanced since their introduction in 2018, are AI Analyst for Kaspersky MDR, Adaptive Anomaly Control, and Kaspersky Machine Learning for Anomaly Detection.

1

The "Auto-Analyst," developed by Kaspersky's MDR team and AI research center to help with initial filtering of alerts, is a supervised ML system trained on alerts from SIEM, combined with a SOC verdict on each alert, which enables the AI to confidently identify false positives generated by legitimate network activity.

2

Adaptive Anomaly Control is an attack surface reduction tool combining the simplicity of hardening rules with automatic tuning via behavior analysis. Used in Kaspersky's endpoint security solutions, it unites a comprehensive set of effective control rules based on ML data, behavior analysis algorithms to find new potential heuristics of suspicious actions, and automated adaptation based on user activity analysis.

3

With the number of attacks on industrial systems and attack surfaces constantly increasing, Kaspersky Machine Learning for Anomaly Detection uses a neural network to simultaneously monitor a wide range of telemetry data and identify anomalies in the operation of cyber-physical systems – detecting attacks on operational technology (OT) at an early stage of development, and adding an extra, critical layer of industrial protection.

These kinds of solutions demonstrate the breadth and depth of capabilities delivered by AI and ML, and since they were introduced, Kaspersky has continually released new tools that address increasingly challenging threats and issues. These include a spam quarantine system based on deep neural networks, an ML-based phishing detection system, AI for SIEM/XDR, GenAI-based threat intelligence summaries, and Kaspersky Investigation and Response Assistant – with many more in the pipeline.

What Kaspersky has achieved by leveraging ML

Kaspersky has been integrating AI – particularly ML – into its products and services for nearly two decades, and its deep expertise in applying these technologies to cybersecurity, coupled with its unique datasets, efficient methods and advanced model-training infrastructure, enable it to solve complex business challenges.

Its commitment to innovation in this field is underlined by the recently enhanced AI capabilities in its security information and event management (SIEM) solution.

About Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. With over a billion devices protected to date from emerging cyberthreats and targeted attacks, Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection, specialized security products and services, as well as Cyber Immune solutions to fight sophisticated and evolving digital threats. We help over 200,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

www.kaspersky.com