CHECK POINT SOFTWARE

In cyber, AI is both friend and foe

In the realm of cybersecurity, artificial intelligence is both introducing new forms of peril into government systems, as well as arming IT teams with powerful new defenses.

Aaron Rose
Check Point Software

"WITH AI, THE DEFENSIVE TEAMS CAN AUTOMATE MUCH OF THE SECURITY OPERATION, CREATING NEW RULES FOR LOG ANALYSIS FOR EXAMPLE, IN ORDER TO TAKE EVEN MORE OF THE LOAD OFF HUMAN OPERATORS."

We can think about AI risk in cyber as a supply chain problem. In the same way that government must have secure sources for the steel in battleships and the code in software, agencies need a secure supply chain for the data that is the lifeblood of AI.

Bad actors know that data is the basic building block of any AI system, and they will look to poison the data. They will aim to leverage the data either to drive nefarious AI outcomes, or as a means to exfiltrate private or secret information.

To implement effective technological controls for preventing data leaks, IT teams need visibility into what they are protecting — such as social security numbers, payment information, or sensitive communications. They must also have deeper insights into data ownership and governance: who owns the data, why it was collected, and whether it has been appropriately tagged. These insights are critical to ensuring that data is not misused or exploited for malicious ends.

Agencies must pay attention to the details of data usage, as they bring AI applications to life. From there, they can consider the ways in which AI may act as either friend or foe, from a cybersecurity perspective.

As a foe, AI represents a formidable new threat vector. Attackers can use AI to write malicious code, develop new ransomware variants, and even automate complex cyberattacks. Even those with minimal technical expertise can use AI to craft convincing phishing emails without the spelling mistakes and grammatical issues that used to serve as red flags.

As a friend, there's much that AI can do to help beat back the rising threat. Check Point Software's ThreatCloud AI system, for example, leverages machine learning for predictive analytics, looking at telemetry information over time to predict what the next form of malware will look like, or how the next ransomware attack may arrive.

AI can also help to drive incident response, filtering out the noise in cybersecurity and helping senior-level analysts to focus on the most significant threats. With AI, the defensive teams can automate much of the security operation, creating new rules for log analysis for example, in order to take even more of the load off human operators.

In addition, Check Point has announced a number of AI-focused capabilities in the arena of cyber defense, including a partnership with NVIDIA that will focus on using the chips themselves to help prevent data-poisoning attacks during the AI training phase. And there are tools that sit in front of the AI systems to watch for things like prompt injection — attempting to manipulate the AI into delivering unintended outputs.

With AI-driven cyber risk on the rise, federal agencies need a capable partner to make the most of AI's defensive capabilities. With deep expertise, Check Point Software can help government make responsible use of modernized tools to prevent any kind of manipulation of the system, whether it's at the training phase, or in actual production.

A global leader in AI-enabled cybersecurity, Check Point works proactively with government both to utilize the latest tools, and to develop and operationalize the governance that is key to ensuring government can use AI in a manner that is safe and secure. ■

ADOBE STOCK// SIZSUS

Aaron Rose *is Check Point Software's security architect manager for vertical solutions in the Americas, supporting government, education, and critical infrastructure sectors, including the U.S. public sector.*