ENTERPRISE SECURITY GROUP AT BROADCOM

Understanding AI's multifaceted role in cybersecurity



The best approach embeds artificial intelligence into agencies' existing security controls while preserving human judgment

Garrett Lee | Enterprise Security Group at Broadcom

Artificial intelligence is changing the cyber landscape for both defenders and attackers. Adversaries are using AI to scale faster, automate elements of their attacks and improve their ability to avoid detection. Meanwhile, government agencies are being asked to defend an increasingly complex environment where data is flowing all over the place. Spotting what normal looks like when normal is changing so fast is incredibly challenging.

Fortunately, AI can dramatically improve the efficiency and effectiveness of agencies' defensive operations. For example, AI can help correlate enormous volumes of security telemetry to create incident summaries, and it can look through large datasets to identify patterns that would otherwise be difficult to spot. The technology can help agencies prioritize which threats they want to focus on while automating routine, repetitive investigative work. In fact, that's where the real promise of AI lies — not in replacing analysts, but in amplifying their abilities.

However, as agencies adopt AI to support their missions, they also create new attack surfaces and new ways for sensitive information to potentially leak out. Consequently, agencies have two responsibilities: using AI to improve their defensive posture and securing the systems that AI tools run on.

Beyond autonomy for autonomy's sake

The key is not to treat AI as another stand-alone security product. Instead, agencies should incorporate AI into their existing security architectures and operational workflows to make them more intelligent and efficient. It's important to remember that AI is only as effective as the telemetry and context that are available to it. Therefore, a security suite that creates a common operating picture across domain, endpoint, network, user and information-centric signals gives AI a much richer understanding of what is happening in the environment.

AI has the potential for great improvements but also for great risk. Therefore, governance and human oversight are essential. There are many areas where AI can autonomously identify, prioritize or respond to threats, but high-consequence decisions should remain explainable, governed and reversible where possible.

The objective isn't autonomy for autonomy's sake. Instead, the goal is to use automation where machines have an advantage and rely on human judgment where people have an advantage.



The need for high-quality, high-fidelity telemetry

Broadcom's portfolio of security solutions gives agencies the flexibility to build intelligence into their existing security infrastructure. With Symantec and Carbon Black, we have visibility and enforcement points spanning endpoint, network, web and information security. That level of control and visibility is vital because effective AI-driven defense depends on high-quality, high-fidelity telemetry and the ability to act on what that telemetry reveals.

Carbon Black applies AI to activities such as detecting threats, investigating breaches and creating incident summaries. We are also developing increasingly predictive and adaptive protection. We've trained private AI models on real-life attack kill chains so agencies can predict what attackers will likely do next based on what is happening in their environment.

Furthermore, Symantec offers data loss prevention and secure web gateway solutions, which help agencies govern which sensitive information users and applications are allowed to send into AI and what AI is allowed to produce as results. And because we support cloud, on-premises and highly controlled environments, agencies don't have to redesign their missions around a particular security delivery model to take advantage of those capabilities.

We want to help agencies use AI to gain more intelligence and power from their existing security operations and infrastructure, so they can respond faster with the resources available to them to better protect their data and mission.

***Garrett Lee** is regional vice president of Broadcom's Enterprise Security Group.*

> AI has the potential for great improvements but also for great risk. Therefore, governance and human oversight are essential."

