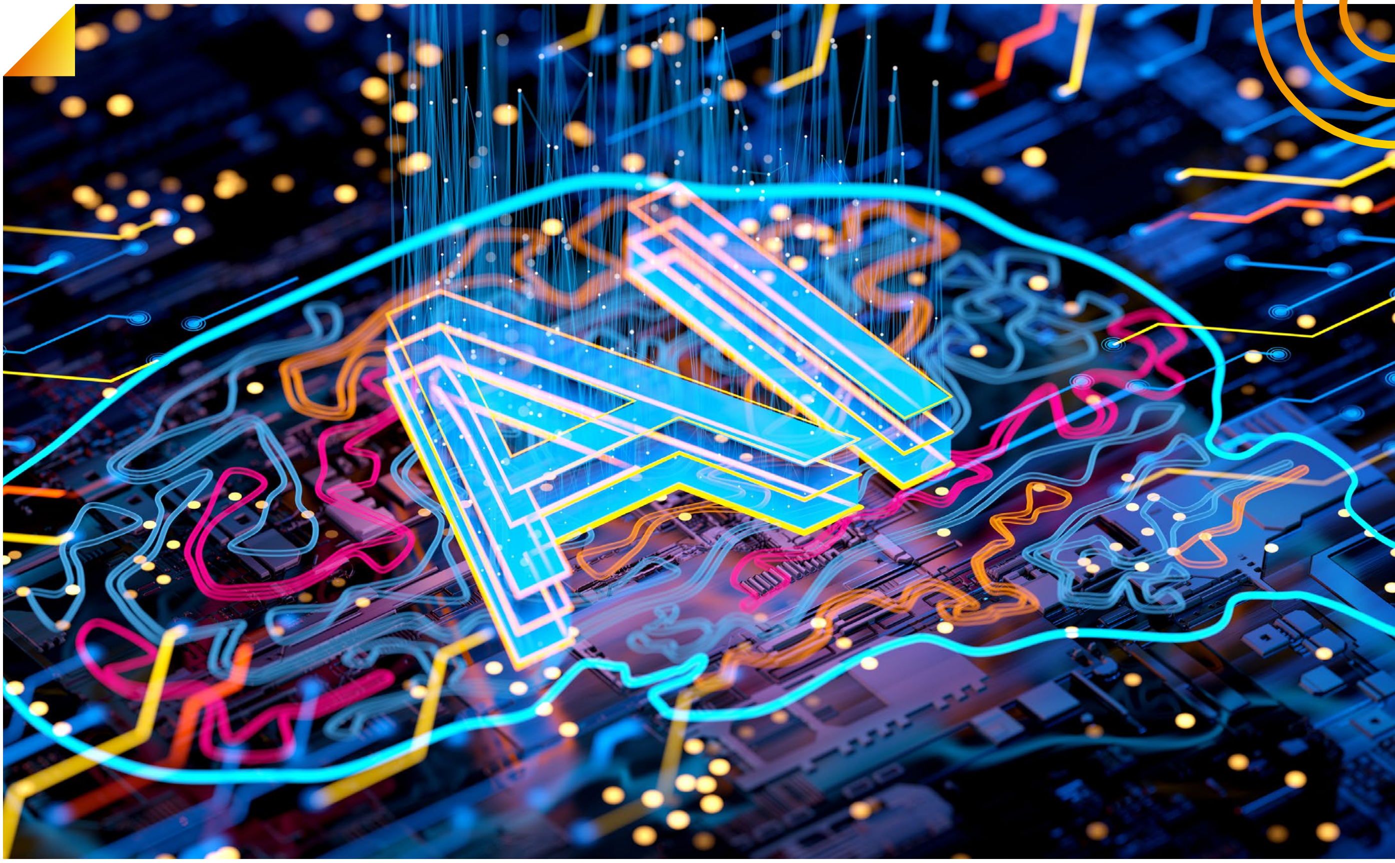
SOLUTIONS GUIDE

FCW | PRESIDIO® FEDERAL Think Mission. | Silver Business Partner IBM

AI BOOSTS SECURITY AND OPERATIONAL CAPABILITY

Artificial Intelligence (AI) is emerging as a potentially potent ingredient for cyber criminals' exploits and malware attacks. On the other hand, AI is also becoming key to defending against those new threats and expanding agency capabilities.

Emerging natural language AI applications, such as ChatGPT-4, leverage artificial intelligence, deep learning, and big data to generate all manner of apps, articles, and other information-based content without human intervention. ChatGPT-4 can also write and debug computer coding.



Hackers are figuring out how to leverage all those capabilities to get around cyber defenses in commercial and government enterprises. News reports in 2023 on ChatGPT use showed that hackers are already using it to infiltrate and export data files, as well as write Java code.

However, emerging AI applications can also reinforce federal agencies' cybersecurity capabilities. AI, deployed comprehensively and coherently across federal agency enterprises, can support the next-step data analytics capabilities, and foster more secure algorithms that can become integral pieces of strong cybersecurity plans, as well as more human-oriented operations.

Secured Data Is AI Key

"The cybersecurity threat from ChatGPT is just emerging, as are a host of AI-driven enterprise applications", said Jon S. Kim, SVP of Solutions and Services at Presidio Federal, a provider of secure mission-critical custom IT products and services to the federal government. A long-standing cyber threat — unsecured data sources — could spur federal agencies to move more securely along on their AI paths, according to Chris Maestas, Chief Executive Architect at IBM, a pioneer of AI technologies and services. IBM's reach with AI-powered services and capabilities, however, is long and wide. IBM is a long-time AI innovator, beginning with the Watson computer system that began harnessing the capabilities in the1990's. Since then, the company's portfolio of AI products, services and capabilities has multiplied, providing AI-enhanced storage, processing, and process automation.

> Doing an initial scan of incoming data can reveal something that could wake up and surprise us."
>
> **Chris Maestas**, Chief Executive Architect at IBM

> In security, AI can look at very long data baselines for even very minor changes, that humans can't do."
>
> **Jon S. Kim**, SVP of Solutions and Services at Presidio Federal

Today, Maestas notes, the triage of incoming data has become a crucial part of using big data to run applications and secure operations.

"We're not thinking in a security mindset about where the data is coming from," said Maestas. "Doing an initial scan of incoming data can reveal something that could wake up and surprise us."

AI, with its digital processes including machine learning and natural language processing, can help agency security teams procure threat intelligence from millions of sources and sort through that intelligence quickly and efficiently.

According to Maestas, efficient processing can also help advance AI applications, setting secure data foundations that those applications draw from. Data at agencies is being generated from all manner of sources, from drones to high-speed cameras and a myriad of other devices. The data captured in those devices is placed in transient storage and tagged, then passed on to AI and other systems that use big data. Drawing data from archives can also have some security issues if it's used to power an AI system. AI can help ensure that data is secured before it is drawn into applications.

Operationalize AI for Security

Using AI to look at incoming data consistently and automatically over long periods can turn up potential data irregularities and help secure IT operations, according to Maestas and Kim. "In security, AI can look at very long data baselines for even very minor changes, that humans c an't do," said Kim. "AI can look for things that might go unnoticed in the big data lakes that cybersecurity needs to work from."

That kind of application of AI capabilities is sometimes referred to as AIOps. AIOps can sharpen data, data analysis and reporting. Along with learning to pick up subtle signals out of huge volumes of security data, AI can help aggregate oceans of data generated by IT infrastructure components, applications, performance monitoring tools and service ticketing systems.

“AIOps can help personnel deal with the increasing volumes of data security, including false positives” that analysis turns up, said Maestas.

AI can also help diagnose root causes of problems and automatically report them to IT and DevOps for rapid response and remediation, and even automatically resolve them without human intervention.

“Ideally,” said Maestas, “AI could help cybersecurity departments do ‘on the fly’ patching that would immediately provide protection from quickly evolving cyberthreats in an increasingly dynamic cybersecurity environment.”

Improve Everyday Processes and Services

“There are less dramatic areas where AI can help make major improvements,” said Kim. IT help desk functions and even employee training programs can leverage AI.

For instance, virtual help desk assistants using the natural language comprehension and processing capabilities inherent in AI, can tackle everyday IT questions and duties for employees, allowing them to get to other, more important tasks. “Help desks powered by AI”, said Kim, “can help sort through support tickets and even suggest or implement solutions.”

Enterprise network engineers can also tap into it to do everyday monitoring and support, he said. Using AI, networks can automatically extend manual processes such as performance monitoring, alarm suppression for maintenance, root cause analysis, and anomaly detection, freeing up network personnel to perform more critical work.

> **AIOps can help personnel deal with the increasing volumes of data security, including false positives that analysis turns up.”**
>
> **Chris Maestas**, Chief Executive Architect at IBM

Comprehensive Platform Solutions Solve Problems

A comprehensive global data platform that harnesses AI can help make sense of data coming into enterprises and agencies, as well as secure it, according to Maestas. For example, AI incorporated into IBM’s Storage Scale platform powers its data handling capabilities for high-performance and next-generation data services. IBM Storage Scale’s high performance unstructured data management solution can connect endpoint technologies, audit incoming data and encrypt it. It can then be coupled with a data cataloging service that can do metadata tagging and deep inspection in real time, which can then be turned over to any other analytics that are necessary, according to Maestas.

Learn More at https://presidiofederal.com/partners/ibm/