FEDInsider

CyberSmart 2025

Navigating AI-Backed Cybersecurity & Cyber Threats

The rise of artificial intelligence is transforming automated cyber practices, while introducing new risks and threats for agencies to consider

Advancements in artificial intelligence and new technologies are making today's cyber world increasingly more complex – introducing new elements of risk and creating new dangers while also being used to prevent them. AI improves security with preventive attack capabilities, automated threat response and behavior anomaly detection, while also enabling bad actors to generate deepfakes that can circumvent security measures, mimic user identities and penetrate systems.

At a recent **FedInsider webinar**, thought leaders from government and industry discussed the role of AI in cybersecurity. They shared their experiences leveraging AI to combat today's threat landscape and ways in which agencies can do the same.

Countering AI-Fueled Cyber Threats with Automation

As technology evolves and innovations are introduced into any connected ecosystem, the risks also evolve. According to Scott Stephenson, Vice President of Sales and Business Development for Blackwire Labs, a few of the most concerning AI-powered attack vectors include deep fake impersonations, AI phishing and AI-driven malware.

Deep fake impersonations could lead to government officials following a false directive. AI phishing mimics personal information that is believable to the recipient of the email, and AI-driven malware is also becoming more sophisticated.

"Imagine every time you try to defend something, the threat comes up with a creative way to outsmart you, and also learns and adapts," Stephenson said. "That is a risk we are having to face while also trying to implement automation on the defensive side."

Automation and orchestration are critical to understanding what to protect, identifying potential threats and blocking them. Suneel Cherukuri, chief information security officer in the Office of the Chief Technology Officer for the Government of the District of Columbia, said he relies on both.

Automation can alert to and detect malicious attacks based on the system identifying it as a malicious attack. Yet, "how do we know that it is correct? It comes back to the understanding of what we are using. If we take the same approach with orchestration, there is an alert, some triage happens and then there's an organization ready to deal with that," Cherukuri said.

Featured Experts:

- **Suneel Cherukuri**
  CISO, Office of the CTO, Government of the District of Columbia

- **Scott Stephenson**
  Vice President of Sales & Business Development, Blackwire Labs

"Now, the request flags something as malicious with a high severity – and that triggers automation," Cherukuri added. "And that results in a better outcome versus having everything come up on a screen that stays red and gets blocked."

AI-Powered Security

AI is expected to – and already is – improving the protection of critical infrastructure. "It's going to help us a lot provided we have the right talent and the right people to use the talent," said Cherukuri.

Newer generations are inherently more digitally inept, considering the natural evolution of technology and what they had access to. This is promising, Cherukuri

added. And not all of the AI-powered and machine learning technology that Washington is using today is new.

"A lot of existing products that we have today, they are incorporating generative AI to make our lives better and easier from an orchestration perspective, not just automation," he said. In terms of threat analysis and detection, Cherukuri said AI tools are orchestrated together with existing and reliable platforms to provide preliminary information about detected threats. With those elements working together, he no longer has to question whether a threat is real.

"There is some real information-based, factually backed information, and I can use that to make my decisions," he said. "Hence, AI used in the right way will definitely simplify and accelerate our responses to some of those threats that will emerge."

Stephenson said users can even leverage AI to ask about changes in cybersecurity policy, NIST frameworks, LiDAR attacks and so on, to remain up to date and in compliance. "It saves me a lot of research time," he said.

Purpose and Value-Backed AI Security Standards

Protecting users' identities is a critical component For Cherukuri, baking the proper standards and privacy into the technology used by his office in the District of Columbia is critical. When someone is using a keylogger with an AI-powered product, for example, every word typed is recorded and the tool is constantly learning based on what the user is typing.

While the outcome may be impressive, the concern is whether those products are doing what they need to do from a risk perspective in a controlled environment. "Is the product actually approved for you to use in your organization?" Cherukuri asked.

Here's another perspective: AI-powered third- party free tools are everywhere now. Gemini can read emails and provide response options without being prompted by the user. Considering that many users store personal data in their Gmail accounts, this creates security risks.

"Somebody out there has every single piece of information, every good and bad detail that I have in my email. Somebody actually read it and has a catalog of it," Cherukuri said. "That is where privacy gets impacted." While this refers to a personal email account, applying the same logic and safety to a work computer potentially exposes the entire organization to an adversary.

Yet, since AI is here to stay, Stephenson says those at the CIO and CISO level should remain bold while using it, but humble with how they govern it. "AI can become a teammate. It is not just a tool, but it's how you implement it," he said.

Cherukuri agreed, noting that he treats AI like a person he can bounce ideas off. AI is making it so that humans can have more reliance on computers, he said, but that does not mean that the tools come without some risks. Even so, AI is extremely helpful and provides a lot of value if used correctly.

"The AI tools are good. They are good for both work and for your personal use — using them is how we evolve," he said.

TO LEARN MORE, VISIT CARAH.IO/CARAHSOFTAI

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016
Contact: **John Hosky**

(202) 237-0300
Info@FedInsider.com
FedInsider.com
Facebook.com/FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

carahsoft

Carahsoft
11493 Sunset Hills Road, Suite 100
Reston, VA 20190
Contact: **Katherine Mulholland**

(571) 662-4865
Katherine.Mulholland@Carahsoft.com
Carahsoft.com
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft