FEDInsider

Artificial Intelligence Is Playing A Major Role in Federal Cybersecurity

Public & private sectors are adopting AI & automation tools to strengthen their cyber posture & prevent increasingly-sophisticated cyberattacks.

Cyber threats are constantly evolving, and the increase of connected devices only empowers bad actors to become more sophisticated with their attacks and capitalize on new vulnerabilities. To respond, federal agencies are implementing a zero trust architecture, but other IT developments are posing additional cybersecurity risks – like artificial intelligence and its rapid incorporation into software and systems.

As the cyber landscape continually changes, thought leaders from government and industry recently spoke at a FedInsider panel to discuss the growing vulnerabilities, and the implications – or benefits – of using AI to improve cybersecurity.

AI's Place in a Cybersecurity Toolbox

An increase in users and devices, coupled with increased connectivity, has led to a massive uptick in data. The need for advanced IT structures to manage this data influx led to the adoption of cybersecurity practices like patch management, deploying critical zero-day vulnerabilities, zero trust architectures and more.

"That's really where you get into AI, [it] can help with automation," said La'Naia Jones, chief information officer and director of the Information Technology Enterprise at the CIA. "Roughly a decade ago, [there was a] big move for virtualization, cloud-based technologies and moving things to more of an automated fashion. And we're continuing to use that."

Jones said this allows the CIA to deploy the right solutions, tools and capabilities to detect, prevent and mitigate cyber-attacks, and to adopt predictive analytics that can find anomalies or shifts in the IT infrastructure that could signal a problem.

The CIA is also looking at AI as a tradecraft to continue strengthening cybersecurity in the future and augmenting analysts' work to get things done quicker. "Time is very important. If you have something that's looking to create chaos in your infrastructure, you want it to be resolved as quickly as possible. Mitigate your blast radius and lower your risk tolerance, so that way it's not interrupting your day-to-day mission," Jones said.

Joseph Ronzio, deputy chief health technology officer for the Veterans Health Administration, said AI and automation tools allow the agency to see whether authorized users are accessing the correct data. The VHA is also using automation to detect, identity, certify and manage access levels for users.

"Pattern detection algorithms have been very good to establish," Ronzio said. "In fact, we've detected several people that have utilized generative AI technologies within our enterprise against policy. You can start seeing where the trends are and then isolate them. And that actually increases the level of security overall for the organization."

AI's Role in Cyber Threat Response

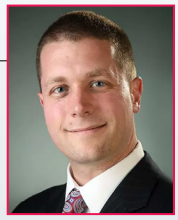
AI will inevitably be used for good and bad, so Sarah Nur, acting CIO for cybersecurity

Featured Experts:

- La'Naia Jones
  CIO & Director, ITE, Central Intelligence Agency

- Sarah Nur
  ACIO-CS & CISO, U.S. Treasury Department

- Joseph "Lucky" Ronzio
  Deputy CTO, Veterans Health Administration



- Jim Donlon
  Director of Solutions Engineering, Oracle

and the chief information security officer for the Department of the Treasury, said agencies must keep their eyes on both aspects of AI capability.

As an example of good uses for AI, it can help to find a needle in a haystack-type of anomaly and then act on it. "That's something that really does plague us," Nur said. She used the Solar Winds attack as an example. "It was discovered that it was a malicious [dynamic-link library] file... but how often are you going to ever look for a DLL file communicating through normal channels?" she asked.

That was a novel attack at the time, and perhaps the only way to have detected it would have been with behavioral analytics or traffic analysis that could contextualize certain behaviors and time frames, Nur added. That is where AI capabilities can be very helpful, when used for consuming large amounts of data and capturing trends.

Jim Donlon, director of solution engineering at Oracle, said AI also allows organizations to respond faster to cyberattacks and provides greater protection of agency data. "Tools are going to continue to evolve," he said. "That means on the other side, bad actors are going to continue to evolve. What I like about zero trust is that it reminds us to think globally but act locally."

Protecting data – especially personally identifiable information and health data – is part of keeping an agency's house in order, as data is often what bad actors go for during an attack. "Lock down your data. Use multi-factor authentication. And use attribute-based access controls. All those things are there," Donlon said.

Keeping that data safe is a big part of why Ronzio is looking at different standards to keep the data local. "One thing I see as a major threat is if we centralize all of that personal data, if we build that big data lake, then that just becomes a fruitful target," he said. Rather, he suggests sending health data-related alerts – not data – to people of interest using cleared devices. That way, an attacker couldn't just target one thing. Instead of compromising one data lake, there could be eight billion devices or more that they would need to try and attack.

Jones agreed with this method, adding that because these solutions are looked at from a federated architecture, each agency can fine-tune access and authentication controls that work best for them.

AI's Ability to Maintain Cybersecurity Resiliency

The CIA moves data and information all around the world, so digital connectedness and communication capabilities are a must. "As generative AI is coming about, we're looking at augmenting the work that we're doing," Jones said. The CIA is currently looking at large-scale cloud vendors – and AI solutions – to help support this capability globally.

"If you combine the computing power and the network capabilities with the power of what [AI] can do, it will revolutionize how we operate, and how we work," Jones said.

Implementing zero trust is also a priority to help prevent cyberattacks and strengthen cybersecurity resiliency.

"Just as you would use AI on a day-to-day basis, we're looking at those tools and applications internally. That's something that will continue to evolve as well," Jones said.

AI capabilities will also make it easier to share data with other partners, further strengthening cybersecurity resilience for the Intelligence Community and all involved. "You can now identify TTPs and IOCs and push that out to your [partners] because it's all about, at this point, where we are in our cybersecurity ecosystem," Nur said. It's critical that agencies work together to stay on top of AI capabilities before bad actors advance further than the government.

Automating simple tasks like data backup and recovery and having the ability to patch and update vulnerable systems can also help prevent failure and data loss unrelated to cyberattacks. "That's just as much of a threat to your organization," Donlon added.

With the inevitable and continual influx of data, especially in the IC, leveraging AI to protect data is critical – and will ultimately strengthen agencies' cyber posture, bolster resiliency, enable IT teams to find network discrepancies and vulnerabilities quicker, and offer better response and recovery from future attacks. Government agencies simply need to keep advancing their AI capabilities and the underlying data that supports it.

For more information on Oracle's available service for Federal Government visit:
Oracle.com/Federal

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

(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

(703) 871-8548
Info@Carahsoft.com
Carahsoft.com/Oracle
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft

ORACLE Cloud

Oracle
2300 Oracle Way
Austin, TX 78741

(855) 618-3114
Oracle@Carahsoft.com
Carahsoft.com/Oracle
Facebook.com/Oracle
Linkedin.com/companyOracle
@Oracle

© 2024 Hosky Communications, Inc. All rights reserved. FedInsider and the FedInsider logo, are trademarks or registered trademarks of Hosky Communications or its subsidiaries or affiliated companies in the United States and other countries. All other marks are the property of their respective owners.