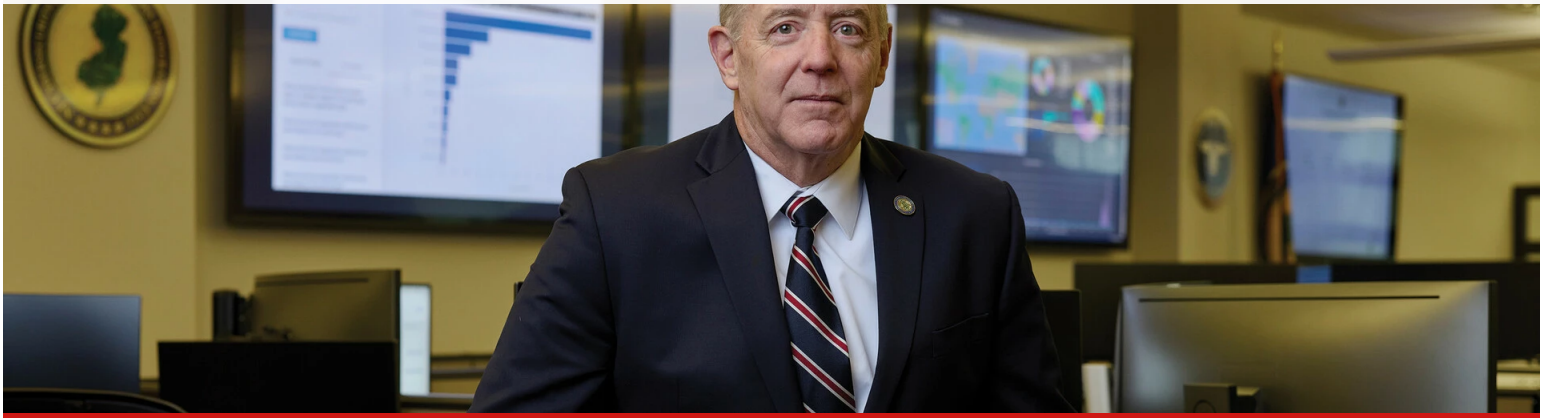


Michael Geraghty, CISO and director of the New Jersey Cybersecurity Communications Integration Cell, oversees threat detection initiatives with artificial intelligence-augmented solutions.

APR
23
2025

SECURITY

Government Security Ops Detect Threats With AI Solutions

States benefit from artificial intelligence software that maintains comprehensive surveillance.

by Erin Brereton

Erin Brereton has written about technology, business and other topics for more than 50 magazines, newspapers and online publications.

Latest Articles

Q&A: CISA's John Bryant Talks No-Cost Critical Infrastructure Services

Self-Healing Networks: How Are They Used In The Public Sector?

Agentic AI At Scale: Use Cases, Costs And Ramifications

NASCIO 2025 Midyear: Mobile Driver's Licenses Fail To Fulfill Potential

LISTEN 08:46

When New Jersey's cybersecurity system identifies a possible email threat, a notification is sent to the security operations center team, and the corresponding account may be disabled automatically. The team can then review the associated data to confirm the threat.

"Our systems kick off a bunch of processes to pull information together," says Michael Geraghty, CISO and director of the New Jersey Cybersecurity Communications Integration Cell. "By the time the analyst gets it, he has a clearer picture of what's happening."

New Jersey receives a comprehensive picture of its threat landscape on demand from several cybersecurity solutions using artificial intelligence capabilities. State governments now use generative AI in cybersecurity operations, according to the National Association of State Chief Information Officers.

Click the banner below *for deeper insight into AI's role in cybersecurity.*

Today, state government IT teams perform procedures such as anomaly and threat detection at scale thanks to AI solutions, says Randy Rose, vice president of security operations and intelligence at the nonprofit Center for Internet Security.

"The biggest win from an AI perspective is being able to find low and slow attacks with a much higher efficiency," Rose says. "machine learning can find things that are really hard to detect because there's a long period of time between one part of the attack and another, and they can do it much more easily than humans can."

AI Detection Can Quickly Spot and Report Issues

The New Jersey Cybersecurity Communications Integration Cell has

SECURITY

Q&A: CISA's John Bryant Talks No-Cost Critical Infrastructure Services

ARTIFICIAL INTELLIGENCE

Self-Healing Networks: How Are They Used in the Public Sector?

used the Google SecOps security information and event management system, which can analyze security data from across an organization's environment, for about five years as part of its cybersecurity approach, Geraghty says.

NJCCIC has also deployed Google's BigQuery data platform, CrowdStrike's endpoint detection and response (EDR) solution and Palo Alto Networks' next-generation firewall.

"They're all using AI to some degree," Geraghty says. "The days of using signatures that are very brittle to detect malware or phishing emails are over. Today, we have endpoint detection and response, which is behavior-based and deals with a lot of machine learning AI models."

NJCCIC cybersecurity professionals employ AI functionality to quickly review lengthy technical reports and other content.

"In Congress, you might have a proposal that's 1,500 pages long," Geraghty says. "It would take quite some time for somebody to read that. Allowing a generative model to pull out key facts and summarize it is really helpful."

> "Today, we have endpoint detection and response, which is behavior-based and deals with a lot of machine learning AI models."
>
> **Michael Geraghty, CISO, New Jersey**

Automation Allows Officials to Focus on Real Needs

Oklahoma IT officials monitor system elements, run the data against possibly suspicious intelligent models and behaviors, and score the data with the assistance of AI-powered solutions.

The state's tech team relies on Zscaler's Zero Trust Exchange cybersecurity platform, which looks for user identity and context elements such as the involved location, device and application to ensure secure connections. Sometimes, the Oklahoma Office of Management and Enterprise Services (OMES) responds to suspected

Trending Now

'El Paso Helps' Places Struggling Residents In Housing Or Shelters

Government Security Ops Detect Threats With AI Solutions

Shoring Up OT Security Starts With Asset Management

Improving

attacks with pre-established security controls, says Oklahoma CISO Michael Toland.

“The more flags that are tripped, the higher our confidence is that something bad is happening,” Toland says. “Our people then do an investigation to determine whether it’s a true event or not actually a threat.”

In-house IT personnel could use a generative AI module that pulls evidence about the incident together and summarizes it, producing a report that’s 80% complete, Toland says.

“Instead of having to write a three-page report, they have to tweak a few paragraphs to make it ready for submission,” he says. “Investigators aren’t spending as much of their time on documentation and can spend more on investigation, which is where we really need them.”

RELATED: *AI isn’t new to cybersecurity, but some of its use cases are.*

Officials Plan for AI’s Role in Security Operations

For AI-powered cybersecurity technology implementations to be effective, clean data is key, Toland says.

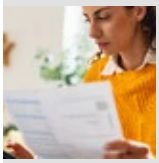
“If you don’t have clean data, the AI will be useless,” he says. “The better we make the data, the better the query engine gets, the better the alerts get, and the more effective my team gets at finding and stopping threats before they become big problems.”

Establishing a uniform data pipeline model for EDR, firewall and other system components can be critical, New Jersey’s Geraghty says.

“When your EDR system says it’s a source IP address, the same vernacular should be used across systems,” he says. “If you have a bunch of different ways to say something, if you’re not all using the same lexicon, the AI tools won’t be able to make sense of it.”

542

The number of cyber incidents reported to the New



Access To Benefits Through Digital Government: A Roadmap

Jersey Cybersecurity and Communications Integration Cell in 2023

Source: cyber.nj.gov, “2024 Cyber Threat Assessment,” Feb. 3, 2025

New Jersey began hiring data science and engineering professionals three years ago to ensure its information is in order.

“Everything is connected to the internet, from your HVAC system to all of the cameras doing security and your building automation system,” Geraghty says. “To get that data, you need the data engineering talent and data scientists to make sense of it and then build out those machine learning models.”

Toland advises government officials who are contemplating an AI deployment to pay close attention to how data will be used, since some elements may be highly sensitive.

“Even system logs can find themselves under the umbrella of regulated data,” Toland says. “Make sure you understand what the data flows are so that if you do have regulated data, you’re not putting it somewhere it isn’t supposed to be.”

PREPARE: *Shadow AI poses a very real risk for the public sector.*

AI Systems May Pay for Themselves in Efficiency

Because Oklahoma faces tens of millions of cyberattacks a day, human beings must rely on automation to effectively defeat them, Toland says.

“It comes down to a simple human capital equation,” he says. “I couldn’t hire enough people to do the job manually, even if I had an unlimited budget; the talent pipeline does not exist. There are not enough human beings trained to do the work.”

However, if AI can assist with some tasks and offer insight, government organizations may be able to hire and train less experienced workers instead of pursuing engineers with decades of experience who might demand salaries that are out of budget.

“There are all kinds of opportunities for cost savings, process optimization and potentially head count reduction,” Toland says.

“Maybe you don’t need as many people doing the busywork aspect of cybersecurity, and you can either retrain those people or find other roles for them.”

KEEP READING: *Can AI replace human intelligence amid federal cybersecurity budget cuts?*

Since coming on board in 2023, Toland has seen OMES’ AI-enabled security system stop dozens of potential attacks. The functionality can prove particularly beneficial, he says, because attempts often don’t happen during business hours.

“It’s usually 2 a.m., when everybody else is asleep,” he says. “But those systems are always watching, and they have a response engine built in. While the on-call tech is staggering out of bed, the AI system has already stopped the attack and is holding it.”

Having reactive processes in place can help meter the damage if a malicious attempt succeeds.

“You don’t know when the next attack is going to happen,” Toland says. “But when it does, if you have those systems, you almost always realize a much lower total cost, lower downtime, less loss of reputation. These kinds of systems pay for themselves when you think about stopping a single cybersecurity data breach.”

TOP AI SOLUTIONS

In a recent report, the National Association of State Chief Information Officers explored artificial intelligence trends for state governments.

78% Creating advisory committees and task forces on AI

72% Implementing enterprise policies and procedures on development and use

67% Developing responsible use guidelines, flexible guardrails, security, ethics

61% Documenting use cases in agencies and applications

PHOTOGRAPHY BY MATT CARR

More On

ARTIFICIAL INTELLIGENCE AUTHENTICATION

DATA PROTECTION ENDPOINT SECURITY

FIREWALLS IDENTITY MANAGEMENT

MOBILE SECURITY NETWORK ACCESS CONTROL

REMOTE ACCESS THREAT PREVENTION

UNIFIED THREAT MANAGEMENT

MACHINE LEARNING SECURITY SOFTWARE