AI Offers Promise for Security, But Also Risks

IT leaders recommend identifying use cases to apply the technology.

James Mersol

Wed, 12/04/2019 - 15:30

Photo Credit: Charles Taylor/iStock

Artificial intelligence promises to be the tech buzzword of 2019, with multiple agencies exploring automated solutions to myriad challenges and several developing use cases that will allow them to more efficiently achieve their missions. Some IT leaders, however, have cautioned against running after AI as the new shiny object among emerging technologies without first identifying proper use cases or considering its flaws alongside its benefits.

“We’re very concerned about bias,” said Air Force CTO Frank Konieczny, speaking at the FedScoop Security Transformation Forum Tuesday. “When we look at a system — look at the analysis of it, based on the baseline data. What data are you going to give to it to actually utilize it … especially when we get to life-saving systems, we’re very concerned about that.”

The Air Force is looking at artificial intelligence and machine-learning capabilities, but has concerns about some of the risks involved in the technology, especially considering the baseline data required for ML.

“The issue for a baseline for security is, ‘Is the enemy already in the baseline?’ and you baseline the enemy into your system,” Konieczny said. “It’s a question that you have to ask. The other question is, ‘Does your baseline ever change?’ Our baseline changes all the time. So therefore, how do you use an ML system to detect a change if the change is always occurring?”

Asking these questions has enabled the Air Force to choose AI and machine-learning applications wisely, ensuring it is a force multiplier rather than an add-on that does not actually provide any benefit to users, Konieczny explained.

Department of Transportation CIO Ryan Cote was similarly hesitant to implement AI without first considering the benefits.

“I think we’re in the early, early stages of applying AI to cyber,” he cautioned. “I think the best we can do today is look at machine learning and try to automate some of the basic steps of cyber hygiene.”

Cote was quick to shut down the hype around AI/ML, encouraging customers to separate out those capabilities from data analytics and other similar services.

“I would say marketing hype is at a 10, and delivery is at a 1,” he joked. He did appreciate, however, that many companies are showing commitment to their products by offering software-as-a-service (SaaS), rather than a one-time purchase. This new model allows companies to make continual updates to their products rather than “check in” once every few years to sell a newer version.

Risks aside, AI and its near-term cousin automation do offer some promising use cases. One is augmenting the work of current cybersecurity professionals to mitigate the workforce gap.

“Even if we had enough [professionals], there’s no way we could [analyze] the volume of data that we see coming into any SOC … and quickly take action,” explained Department of Justice CISO Nickolous Ward. “If we can’t take an action within minutes, a good nation-state actor is already hopping to other systems once they’ve made their initial compromise.”

Ward said the DOJ is exploring automated security solutions in the near term, including robotic process automation and orchestration to fill that gap and recognize the growing technical challenge.

“I can’t hire enough people, I can’t train them fast enough in order to be able to look at the volume of data that we’re dealing with every day,” he said. “Being able to have [automation in place] … it’s impossible for us to win the fight without it.” Ward estimated that the DOJ gets “high millions” of logs and alerts every day.

Department of Veterans Affairs CISO Paul Cunningham agreed that emerging technology helps to close the gap.

“We’re not going to solve [the workforce issue] overnight,” he said, “but certainly, it’s probably not going to be people. It’s going to be looking at technologies to help us decrease the amount of people we need to do sound cybersecurity and making sure we have the right people in place to look at the things are most important. That’s where I think AI is going to be part of the solution — but not the only part.”

The bottom line for the VA, Cunningham said, is to “protect the record and the experience all the way through, from end to end.”

In the long term, Ward said, the critical focus is ensuring that cybersecurity professionals understand the offensive and defensive aspects of AI and machine learning.

“My workforce is going to have to evolve,” he said. “Attackers are using [AI] to evade my security technology more and more. We have to use it to attack them and stop them. But not just that. Attackers are starting to learn how to defeat AI by taking advantage of the weaknesses of AI itself. My security team needs to be able to understand AI well enough so they can combat the attacks against AI itself and … leverage it to speed up how they do detection and defense.”

Oki Mek, senior advisor to the CIO for the Department of Health and Human Services, proposed using blockchain as a way to protect datasets against attacks and simultaneously leverage them for AI and machine learning.

“We need to evolve and make sense of where our datasets are,” he said. “I think we need machine learning not only to make sense of the data, but to categorize datasets as well. That’s why I say blockchain is key … I think blockchain is the missing link to the internet.”

Mek gave the example of patient data as one way to mitigate risk through blockchain. Currently, patients trust that their health care providers will properly handle and secure their data, he said, but blockchain provides the transparency to “trust but verify” that that data is being handled in accordance with regulations.

Automation will also shorten the authority to operate (ATO) process to “a matter of seconds,” Mek said, limiting the amount of “pushing paper” that goes into security management.

Konieczny emphasized that one of the most important goals right now is to avoid lionizing AI and machine learning or thinking of it as a panacea.

“Remember that AI is just somebody who’s programming,” he said. “This is a program. This is people doing this. This is not magic.”

The use cases are promising, but if improperly built or aligned, the risks will outweigh the ostensible benefits, he said.

View printer friendly version
AI
machine learning
automation
Federal Cybersecurity

Air Force
DOJ
Veterans Affairs
Health Human Services
Standard