May 31, 2017

For cybersecurity industry, it looks like AI revolution is here to stay

Despite privacy tradeoff, machine learning becoming vital to solving complex data issues

INFOGRAPHIC BY RODIKA TOLLEFSON, THIRDCERTAINTY

Artificial intelligence and one of its applications, machine learning, have become cybersecurity buzzwords. Startups as well as established vendors are looking to AI for solving the complex problems that humans can't, and many vendors are seeing it as the answer to industry challenges.

But throughout its 60-year history, AI has had several peaks and valleys. Does it have staying power this time?

"Everyone says this time around is different," says Anand Rao, innovation lead for PricewaterhouseCooper's analytics group. "Computing has increased at an exponential rate and some of the things we couldn't do even three or four years ago are now feasible."

***Related podcast:** Organizations use machine learning to ferret out data anomalies*

The current upswing is different in two other ways, Rao adds. AI developments are taking advantage of the open-source approach to algorithms and the breakthroughs in other technologies like big data analytics.

Most embrace AI

In a recent survey of 2,500 consumers and business decision-makers, PwC found that 63 percent of consumers believed artificial intelligence was important for helping solve complex problems that “plague modern societies.” Additionally, 68 percent of respondents felt it was important to use AI to help solve cybersecurity and privacy issues.

Rao says that there has been more emphasis on using AI in the consumer world—but the enterprise world is catching up.

“One challenge that I think artificial intelligence is going to help solve in enterprise security is the fact that the amount of data that a security analyst is faced with on a day-to-day basis is no longer a problem that can be solved by humans alone,” says Matt Rodgers, head of security strategy at E8 Security.

Like many other vendors, E8 Security is turning to AI for the solution. The company uses machine learning to analyze data from multiple sources, including individual devices and network traffic, to automate learning and find anomalies in behaviors and malicious activity.

Matt Rodgers, E8 Security head of security strategy

Not only are some of those complexities beyond the human capabilities, machines allow for a consistent environment, Rodgers says.

“The nice thing about the (AI) system is that it doesn’t have a good day or a bad day,” he say

Built-in bias

One of the risks of using artificial intelligence is potential bias, Rao notes. Machines are trained based on specific sets of data and characteristics, which may not apply in the next context. For example, hackers trying to breach a municipal system may not have the same motivations as they would for breaching a bank, so their behavior would be different as well.

Anand Rao, innovation lead for PwC’s analytics group

“People are looking at multiple solutions to build AI that’s responsible and has trust and transparency built into the system so it can check for biases,” Rao says.

Scott Zoldi, chief analytics officer for FICO, says there’s a lot of excitement indicating AI is at the height of its cycle, but the race to the market will lead to some failures.

“AI is only as good as its masters that retrieve the data and construct the problems," he says.

FICO has applied artificial intelligence to solve problems successfully for a long time. Its Falcon fraud-management platform has been used in the financial industry around the globe for 25 years, according to Zoldi, who's worked at FICO for more than 17 years. And the FICO credit score is, of course, familiar to anyone who's ever applied for credit.

Now, FICO is applying some of the same ideas to cybersecurity, to offer both cyber-analytics solution and a FICO-like score measuring cybersecurity enterprise readiness.

Powerful analytic ability

Using "self-calibrating analytics" and machine learning, the FICO cybersecurity platform monitors activity across the network, in real time, to find anomalies and detect threats.

Scott Zoldi, FICO chief analytics officer

"What makes AI really powerful is that it learns relationships between features much better than other analytic techniques," Zoldi says. "It finds all these complicated relationships that probably are not readily apparent to most experts."

AI is not going to replace the experts any time soon. It's a symbiotic relationship, and the machines need the humans as much as the humans need the machines.

For one, Rodgers notes, the machines can't decipher the difference in intent and don't understand the business goals of an organization—and without that, AI can't make more definitive decisions on its own.

One concern about artificial intelligence is its reliability on big data and all the privacy implications that stem from that. One example is the definition of personally identifiable information: Should daily behavioral patterns be considered PII?

"Even if it's stripped of all the things that we consider PII today, should those patterns that (individuals) make on a day-to-day basis be considered personally identifiable information?" Rodger says. "Ideas like that are going to have to be considered."

More stories related to artificial intelligence and cybersecurity:

Machine learning keeps malware from getting in through security cracks

Machine learning combined with behavioral analytics can