disruptive
.asia

https://disruptive.asia/ai-help-humans-defend-cyber-attacks/

How AI can (and can’t) help humans defend systems from cyber attacks

06/06/18

June 6, 2018 John C. Tanner Features 0

Image credit: Gorodenkoff / Shutterstock.com

As cyber attacks become more prevalent, inevitably artificial intelligence and machine learning are going to play a role on both sides of the firewall. But for the most part, the role of AI and ML will be to assist humans in cyber defense, not replace them.

That was the central theme of a cyber security panel at last month’s NetEvents conference in San Jose that explored ways that AI could help deal with the proliferation of cyber threats that are expected to grow dramatically in the coming years.

Slavik Markovich, CEO of Demisto, noted that the place to start is by understanding that AI as a concept means different things to different people, which can muddy expectations of what AI can and can’t do in a cyber security scenario.

“The big dream of AI is that it will solve all our problems in security and automatically catch everything, but we’re still pretty far from that, because it requires a lot of resources like storage and compute, and we’re just not there yet,” Markovich said. “So we need to focus on specific ways that AI can help.”

One way is to help security analysts do their work more efficiently, he said, "We look at what are the actions and intents that analysts do in their day-to-day job, then we can feed back to the same analysts when a new incident comes in. We learn from the organization's practices, record incidents, and when an incident returns, we can alert the analyst if it's the same incident or a different one, and how different."

Greg Martin, CEO of Jask, said that his company is using AI to help security analysts by automating as many of the processes as possible.

"We're taking those tasks that are repetitive and that we do every day – they're more scripted – and we're giving those now to machines to do that work," Martin said. "Frankly machines are better at some things like high-frequency pattern matching, where you're looking for patterns over time in very large volumes, and where SOC analysts can get tired if they're working an overnight shift and they haven't had enough Red Bull. The machines can then do that and find those patterns more quickly."

Humans vs humans

What AI will *not* do, Martin said, is take the human out of the loop. "I believe that in our lifetime, AI will not surpass the human ability to be the best defense against cyber attacks, at least the complex ones. In the next five to ten years, AI will be able to deal with some of the lower level automated attacks for things like financial crime, but for truly targeted government-grade attacks where there's a human behind the keyboard, the best defense for that will be another human behind the keyboard."

AI will also help by filtering those kinds of attacks from the noise created by lower level cyber crime attacks – which is good because that is where the industry is really struggling right now, Martin said. "Years ago in cyber security we used to say that we're looking for a needle in a haystack, but where we are today, we really have a stack of needles – there's only threats – and the real task is finding the sharpest needle in that stack. That's what AI is going to help us with."

That's also why automation is key to cyber security now and in the near future, he added. "There are not enough skilled workers in cyber security, and there are too many threats that the average organization – whether it be a government, or a bank, or a local small credit union – has to deal with on a daily basis."

If we don't develop AI to automate processes and keep humans focused on the high-level threats, he continued, the good guys will continually fall behind, and we'll see more incidents like the Equifax breach, which at the end of the day was the result of the company not having the appropriate amount of resources to keep up with the threats they were seeing.

Markovich of Demisto concurred. "There's too many alerts and security tools, and too few analysts, the only way to bridge that gap is to automate as much as possible, and make the analysts as efficient as possible. AI can achieve some that."

AI vs AI

Kumud Kalia, CIO of Cylance, said that applying AI to sort out all the data coming into an SOC can also play a preventative role in security.

"The security analysts are often being overwhelmed by information from incidents and security events, and it's hard for them to make sense of that," he said. "As long as there's going to be traditional security, there's going to be a role for AI to make sense of that data."

As an example, Kalia pointed to recent major attacks like Wannacry and NotPetya that were rooted in code and tools that had been stolen from the NSA, weaponized and assembled in new combinations.

"What people may be less aware of is versions of our software that hadn't been updated in two years successfully detected and blocked these new software packages," he said. "That's a demonstration of the efficacy of AI within cyber security – even though these software packages were new, AI was still able to spot the code behind them despite having never seen the new versions.”

While it’s good news that AI and machine learning can help improve cyber security, Jask’s Martin warned that the bad actors will also be leveraging AI – to include stolen AI-powered tools developed by the good guys.

“We’re absolutely certain that government entities are using AI to develop new cyber weapons,” he said. “So if you imagine what happens when the newer pieces of these technologies leak out, whether it comes from the US or another government entity, the ramifications can be quite scary.”

More to the point, he added, the bad guys don’t have to rely on stealing good-guy tools to leverage AI. “With the open-source availability of some of these deep learning toolkits, any advanced actor – whether they work for governments, the military or the cyber criminal underworld – has the same technologies and capabilities as start-ups in Silicon Valley, and they’re well-funded, well-organized, very smart. If you’re automating your defences, you’d better believe they’re going to be automating in AI, too.”