ISMG
INFORMATION SECURITY
MEDIA GROUP

GET THE MOST CYBERSECURITY VALUE FROM AI

Brian NeSmith of Arctic Wolf Networks on the Power of Hybrid AI

ARCTIC WOLF

Tom: I'm Tom Field, Senior Vice President of Editorial, with Information Security Media Group. I'm talking today about the right way to use AI for cyber security. It's my pleasure to be speaking with Brian NeSmith. He's CEO and co-founder of Arctic Wolf Networks. Brian, thanks so much for joining us today.

Brian: Thank you, Tom.

Tom: So Brian, to jump right into it, AI and machine learning are widely used buzz words to talk about a next generation version of any new technology. How can artificial intelligence real help in cyber security operations?

Brian: Well, there's no doubt that AI is clearly kind of the term of the year, I think, for a lot of things in this environment. The idea of AI is ... I think we see this picture in the movies of this machine intelligence that's able to look through things, maybe even smarter than a human being. What we know in practice is human beings are the smartest. And the idea with AI and combining it specifically with hybrid AI, is how can you just process the sheer volume of information you have to look at, just to figure out whether there are issues with cyber security in your network. You can't depend on the machines alone. The humans are absolutely needed, and on top of that with hybrid AI, the sources of data, you're seeing things coming from different types of machines, different types of environments, even people in different countries that behave differently. And so you need that mix of machine and human intelligence that goes along with things.

The wonderful thing about AI is it is machine based, and it never gets tired. It's always working. It's always driving. It's always helping identify things, but it's weakness is that the human element can't be removed entirely from the equation.

Tom: Brian, you make a good point. AI has come up as sort of the panacea in the past 12 to 18 months in security circles. But explain to me why AI alone is not enough for cyber security?

Brian: Those people are people. We do lots of random things that, in the cyber security domain, those kind of random behaviors look like indicators of compromise, and in reality it's just people being people. The way we characterize it in the security industry is we talk about false positives, and those false positives are typically driven by people just doing things out of their normal behavior. I normally get up in the morning. I get a cup of coffee. I look at email, but in one particular morning maybe I'm late for a conference call. I log in and start downloading a bunch of data. That kind of information will be typically something that gets labeled as a potential indicator or compromise. It's a false positive. And humans are best at helping machines understand how people work, and in the end, there's other types of attacks. There's bad actors. There's people that are doing things they shouldn't be doing, but actually in some cases might be considered normal behavior. So, AI's not great at eliminating false positives, and on top of that it's not good at finding behavior that's happening for the first time. And that's where people are great.

Tom: Brian, talk to me about hybrid AI. How similar or different is that from AI at a high level?

Brian: Well, hybrid AI is combining the best of that human capability with machine intelligence. There's no question. You need machine intelligence to help you get through just the sheer volume and variety of data sources. But hybrid AI combines the human element. You've got to teach the machines, and the person that teaches the machines, the human, is one that helps the machine learning work in a more effective manner.

What we've seen in practice is when you combine the best of machine with the best of a human, as far as someone that is a security expert and really understands all the dynamics, you eliminate a lot of the noise. You get almost a five times reduction in the number of false positives compared to just the machine. And then on top of that you see a much higher degree of accuracy. You find issues are problems in the environment that a machine's just not going to know how to deal with it. And so you get a much more accurate picture and you get a lot less noise by combining the best of the two. That's security expertise and the human mind with the machine learning and the scalability of computers.

Tom: Now what are the types of event stress you believe can be better detected by hybrid AI that might be missed by traditional AI?

Brian: I think it starts with behavior of people. Super smart hackers recognize that companies are deploying AI technologies to try to catch them. So, what they will do is try to fit into the behavior that's going to allow them to avoid the detection by a straight AI environment. And so what you get by combining both the human capabilities, a security expert, with a machine learning, you can detect unique human behavior. So, someone that's up to something, that looks very normal but in the end case is something that might be problematic. We classify that in our industry as what we call zero day attacks. We talk about it typically in the context of a machine, and how I might compromise a laptop or a server by some sort of bug or problem it has on it.

But zero day attacks apply to people as well. People are very creative. Hackers are very creative, and it takes in some cases the skill and capability of a hacker augmented with somebody that can filter through that noise, and that's where basically you see hybrid AI much better than either AI or human beings alone in its ability to detect these types of attacks.

Tom: Brian, you and I both realize that organizations are having significant trouble finding security experts to manage and fine tune their operations in their controls. Do you find that hybrid AI is more applicable maybe to manage services rather than to a do it yourself security operation?

Brian: In short, I think the answer is yes, but I think it requires maybe understanding of a deeper level. Setting up a hybrid AI capability requires a significant investment, and fundamentally if you're going build it yourself, you've got to, one, hire the security experts. Very expensive. They're difficult to hold on to them. Recruiting them is problematic, and very often they get bored. They work in your environment. We see the typical tenure for a security engineer at a major corporation is 18 months. They come in. They do some work, and then they bounce to the next company, because they just want the stimulation of new things to work on. We find that in a managed service

environment, you can get a lot better leverage, show them a lot more variety, and we're seeing in practice the tenure for this environment makes it better suited for this type of talent.

Tom: Brian, last question for you. Can hybrid AI capabilities be added to any security operation center or product, or do you find it has to be built in ground up?

Brian: I think in the end, when you're thinking about security operations, a fundamental re-think is required here. How do we build out an infrastructure that allows us to detect everything and do that in a cost effective manner. Keep the noise out of the equation. What we see is vendors in this space will typically charge you by the amount of log data you send them, and what we realize is that's just not the way people want to think. We want to be inclusive and rich in the amount of data that we pull in, and what we analyze. We don't want to be subjected to I'm going to charge you more if you send me more data.

And so if you want to build something cost effective that is hybrid AI capable, you really need to do that from the ground up, and you need to reflect and build an infrastructure that can handle large volumes of data, can be customized to the specific environment that the user's worried about, and make it unique for them and specifically to their needs in that environment. Doing that requires something that you have to really build from the ground up.

Tom: Well, very good Brian. I appreciate your time and your insight today. Thanks so much.

Brian: Thank you.

Tom: We've been talking about the right way to use AI for cyber security. I've been speaking with Brian NeSmith. He's CEO and co-founder of Arctic Wolf Networks. For Information Security Media Group, I'm Tom Field. Thank you very much.