AI and Cybersecurity: Now Inseparable

by Sharon D. Nelson, Esq., John W. Simek, and Michael C. Maschke

Have You Noted the Recent Flood of AI and Cybersecurity Articles?

We saw a smattering of articles about AI and Cybersecurity in 2023, but in 2024 we have witnessed a torrent of such articles. If you follow cybersecurity, you undoubtedly know that AI has been a part of providing cybersecurity for some time. So why all the hoopla now?

As everyone knows, AI has been booming. But it has also been bedeviled by problems. Hallucinations have been problematic for many lawyers, some of whom have found themselves in legal trouble. Giving AI access to private case data has also been a problem since we really don't know what happens to that data. And AI has been known to be given false data and therefore it responded to queries with inaccuracies.

AI is in the Doghouse for Many

For all the reasons above, and many more, AI has not entirely lived up to its promises. It is expensive. Employees must be trained to properly use AI, which has proven to be time-consuming and increases the expense. Some AI companies have floundered or gone under.

There are many complaints that AI hasn't lived up to its hype. By some estimates, according to RAND, more than 80 percent of AI projects fail — twice the rate of failure for information technology projects that do not involve AI.

So Why are we Now Laser-focused on AI and Cybersecurity?

As we noted, we have been using AI in cybersecurity for some time, and with generally very good results. Thanks to AI, we have better data protection by rapidly recognizing patterns, automating processes and sniffing out anomalies.

Using AI can analyze vast amounts of data very quickly, almost instantly detecting possible malware or intrusions. And we note wryly that AI can vastly reduce human error by removing humans from many tasks or processes.

Mind you, AI will never fully replace security professionals – good cybersecurity requires creative human problem-solving and the ability to recognize complex issues that may call for high-level human resolution.

What AI Can Do That Humans Cannot

Prior to the advent of AI, cybersecurity specialists used signature-based detection tools to look for potential cyberthreats. The tools basically compared network traffic to a database which contained known threats of malicious code signatures. Then the system would issue an alert so that the security specialist would block or quarantine the threats.

That worked pretty well with "known" threats. But it wasn't up to the task of dealing with new "Zero Day" threats or other previously unknown threats. Without AI, there were a lot of "false positives" which occupied human time to chase down.

Another problem was that professionals in cybersecurity had to manually investigate security alerts and event logs searching for evidence of a possible breach. This was a tremendous "time suck" which the advent of AI largely resolved.

Cybercriminals Love AI

It may sound very simple, but if cybercriminals can breach our networks with AI, then we need AI to counter the AI-enabled attacks. AI vs. AI rapidly became standard procedure. The odds that we could protect our data became vastly better.

The cybercriminals keep learning – using attack vectors like polymorphic malware, scripting and "living off the land" forays. The latter kind of attack involves using legitimate and trusted system tools to launch a cyberattack and evade detection. Yes, it's complicated – and every time we turn a calendar page, it seems as though a new attack is at hand – this makes AI an invaluable part of cybersecurity.

AI cybersecurity tools can analyze a huge amount of data – and fast. At lightning speed, they can ferret out anomalies and vulnerabilities. With the same speed, they can automate repetitive processes, freeing up the time of cybersecurity specialists.

Final Thoughts

We're in for far more in the future as we struggle to keep up with new developments by cybercriminals – and nation-states. As computer security specialist Bruce Schneier so aptly phrased it: "If you think technology can solve your security problems, then you don't understand the problems, and you don't understand the technology."

***Sharon D. Nelson** is an attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* *snelson@senseient.com*

***John W. Simek** is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm.* *jsimek@senseient.com*

***Michael C. Maschke** is the Chief Executive Officer at Sensei Enterprises, Inc. Mr. Maschke is an EnCase Certified Examiner (EnCE), a Certified Computer Examiner (CCE #744), an AccessData*

Certified Examiner (ACE), a Certified Ethical Hacker (CEH), and a Certified Information Systems Security Professional (CISSP). He is a frequent speaker on IT, cybersecurity and digital forensics and he has co-authored 14 books published by the American Bar Association. He can be reached at mmaschke@senseient.com.