HealthManagement.org
Promoting Management and Leadership

Which 2 Pieces of Health Technology are Essential for the CISO's Arsenal?

Artificial intelligence means using computers and tools to do something that humans do. Machine learning is a subset of overall AI that recognises patterns in data and predicts outcomes based on past experience and data. Most AI systems incorporate machine learning technology to help generate results that replicate human ones.

You might also like : Fighting 'Dark Web' Hackers

True machine learning and artificial intelligence are two pieces of a CISO's arsenal that have become imperative, said Anahi Santiago, chief information security officer at Christiana Care Health System in Delaware.

Many healthcare CISOs struggle to fully staff teams with the expertise and skills necessary to protect their organisation's data and patients. AI can help mitigate these risks by automating some of the tasks and expertise required, though assessing the promises of technology and vendors can be difficult and time-consuming.

"Proving the value requires comparing the results of a tool to existing tools or team members, while keeping in mind that evolutionary steps can be valuable while in search of a revolutionary system," said Dustin Rigg Hillard, vice president of engineering at Versive, which conducts machine learning and artificial intelligence hunting of cyber-adversaries and insider threats. "That can mean testing the capability of malware or intrusion detection to identify new threats, or judging if AI is able to replicate, or accelerate, the capabilities of a hunt team."

For example, machine learning can be used to predict typical network behaviours based on historical network logs; these predictions can then be used to identify anomalous activity in a network. "Connecting these anomalous events together across data sources and time into a full threat case begins to automate and replicate the work of expert hunt teams to help surface adversary campaigns," Hillard explains.

For her part, Santiago says machine learning and AI utilise the behaviours of end users and information systems to learn what is normal activity. When there's deviation from what is normal, AI can be used to take action – without human intervention. She cites this basic example: A user accesses an electronic health record 40 times a day to care for patients. Machine learning understands this to be the norm. When the system detects the user accessing hundreds of records within a short period of time, it can apply AI to block the access and send an alert to the information security team.

As anti-virus, patch management and other point-in-time solutions cannot keep pace with the threat landscape, Santiago says tools that utilise machine learning and AI can help in the prevention and protection from the unknown.

The most important foundational step that cybersecurity teams must take before entering into the artificial intelligence space is to fully understand the business, Santiago points out.

“Too often we implement security without fully understanding the impact on the business,” she says. “In order to gain credibility and to become a true partner with the business, infosec teams need to be intimate with how the business functions. That includes understanding clinical workflows, knowing the dynamics of how a healthcare organisation moves and aligning security controls with the needs of our end users, not in spite of them.”

If infosec teams can achieve that kind of synergy, she adds, they will be well positioned to be successful in implementing machine learning and artificial intelligence.

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Tue, 22 Aug 2017