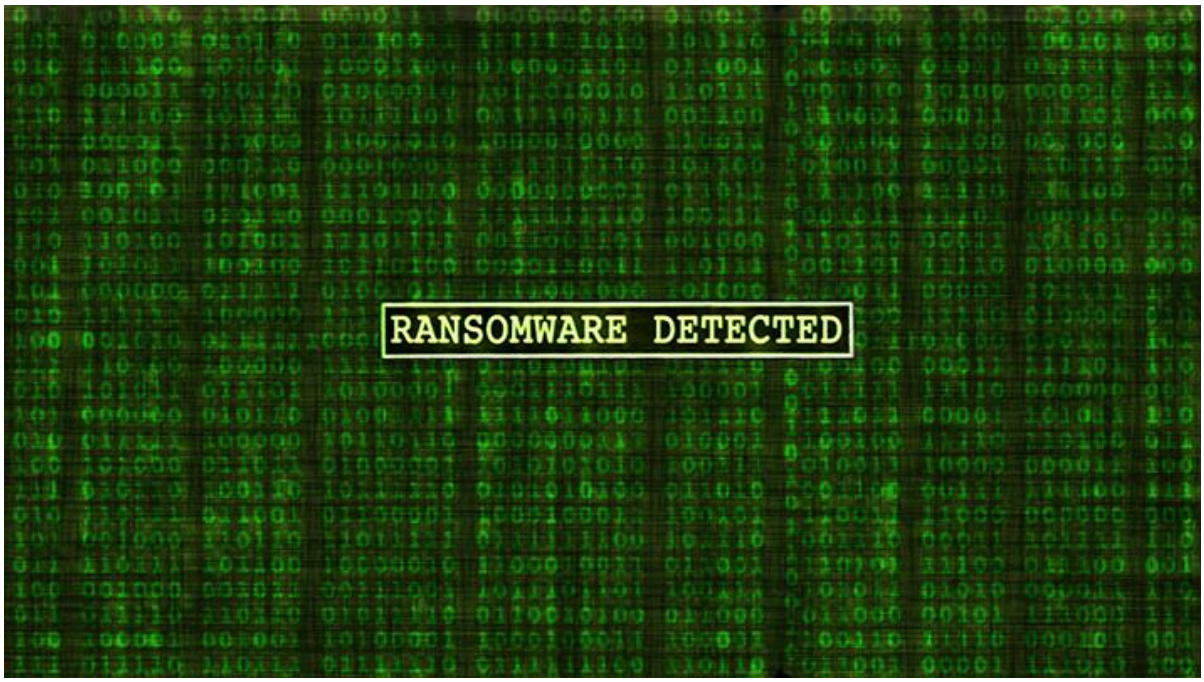
Healthcare IT News

Artificial intelligence is giving healthcare cybersecurity programs a boost

Though not a silver bullet, AI and machine learning can augment security systems to better identify malicious activity and prevent cybercrime, experts say.

By Bill Siwicki
June 29, 2017
10:00 AM



Artificial intelligence is being used in a variety of ways in the healthcare industry, and one area where it is proving to be an effective asset is cybersecurity. Healthcare CIOs and CISOs should recognize that AI has the ability to enhance technology's ability to identify malicious activity and attackers and to protect systems and data, healthcare cybersecurity experts said. And AI does so in different ways.

"Machine learning and artificial intelligence can be used to augment and/or replace traditional signature-based protections," said Robert LaMagna-Reiter, senior director of information security at First National Technology Solutions, a managed IT services

company that, among other things, advises on cybersecurity issues. “One area is security information and event management alerting, or anti-virus solutions.”

[Also: Barracuda unveils AI-driven tech to combat spear-phishing]

With the immense amount of data, security personnel cannot efficiently sift through every event or alert, whether legitimate or a false-positive – machine learning and AI solve this problem by looking at behavior versus signatures, as well as taking into account multiple data points from a network, LaMagna-Reiter explained.

“By acting on behavior and expected actions versus outdated or unknown signatures, the systems can take immediate actions on threats instead of alerting after the fact,” he added.

Artificial intelligence also can assist with “self-healing” or “self-correcting” actions, LaMagna-Reiter said.

[Also: Healthcare AI poised for explosive growth, big cost savings]

“For example, if an antivirus or next-generation firewall system incorporates AI or behavioral monitoring information, assets with abnormal behavior – signs of infection, abnormal traffic, anomalies – can automatically be placed in a quarantined group, removed from network access,” he said. “Additionally, AI can be used to take vulnerability scan results and exploit information to move assets to a safe-zone to prevent infection, or apply different security policies in an attempt to virtually patch devices before an official patch is released.”

Further, if abnormal activity is observed, prior to any execution AI can wipe the activity and all preceding actions from a machine, LaMagna-Reiter explained. “Essentially, every action is recorded and monitored for playback, if necessary,” he said.

Cybersecurity is one of the most prominent use-cases for machine learning and artificial intelligence, said Viktor Kovrizhkin, a security expert at DataArt, which builds custom software for businesses.

“The main niche for applying machine learning and complex AI systems in healthcare cybersecurity is reactive analysis and notification or escalation of potential problems,” Kovrizhkin said. “In combination with other infrastructure components, a machine learning-based approach may respond with actions to anticipate potential data leaks.”

Making use of artificial intelligence is a progressive action, where a system constantly trains and identifies patterns of behavior and can discriminate between those considered normal and those that require attention or action, said Rafael Zubairov, a security expert at DataArt.

“For this, the machine can use a variety of available data sources, such as network activity, errors or denial of access to data, log files, and many more,” Zubairov said. “Continuous interaction with a person and information gathering after deep analysis allow systems to self-improve and avoid future problems.”

But successful use of artificial intelligence in healthcare requires a top-down approach that includes an executive in the know, LaMagna-Reiter said.

“An organization must implement a defense-in-depth, multi-layer security program and have an executive-sponsored information security function in order to fully realize the benefits of implementing machine learning and AI,” LaMagna-Reiter explained. “Without those, machine learning and AI would be under-utilized tools that don’t have the

opportunity to take the security program to the next step. Machine learning and AI are not a silver bullet, or even a one-size-fits-all solution."

Original article can be found here: http://www.healthcareitnews.com/news/artificial-intelligence-giving-healthcare-cybersecurity-programs-boost