Healthcare Cybersecurity: Can Artificial Intelligence Provide a Real Solution?

In 2017, the Health Care Industry Cybersecurity Task Force released a report on cybersecurity in healthcare, and it's not a stretch to say that the prognosis was poor.

Included in the report was the revelation that 75% of hospitals lack permanent, full-time security leaders, compelling some providers to try the less-than-ideal fix of asking other health entities to loan them their security personnel to act as part-time security officers. Additionally, 75% of providers participating in a recent Ponemon report stated that their IT security teams are not adequately staffed, and, exacerbating the problem, they have trouble finding qualified people to fill the vacant positions.

Perhaps this shortage of staff wouldn't be such a dire issue if cybersecurity breaches and attacks weren't ongoing and pervasive, but they are. And that urgent backdrop has some industry experts opining that perhaps the solution isn't in finding more people to do the jobs, but rather, whether artificial intelligence can shore up the vulnerabilities in the healthcare cybersecurity landscape.

"Automation doesn't mean the elimination of people…"

David Finn is the Vice President of Strategic Innovation for CynergisTek. He explained to Health IT Security that using machi learning or other types of artificial intelligence (AI) can streamline complex, predictable processes such as password criteria (i length and format), password resets, and applying updates and patches.

"In the 'old' days this was a very labor-intensive issue: You had to talk to a human being," Finn said. "Today, because we can identify and authenticate a user and/or device, password resets can be accomplished online, at any time, without a call and without having to tie up another person who may be dealing with a user who is having issues with their computer or an application they've never used before."

However, Finn also added that automating certain processes doesn't mean that it's human hands-off for good. Quite the contrary: AI depends upon human attention — both well-defined cyber-protocol at the outset and interactive oversight over th long haul.

Otherwise, without security leaders who set up definitive IT rules and outcomes, Finn warned that "automation efforts may res in more chaos, more work, bigger issues and perhaps less security. You also need to have defined steps for when the proces 'breaks.' We've all been frustrated when we can't get something done and there is no person to talk to."

Finn further reminded us via that Health IT Security interview: "Automation doesn't mean the elimination of people, it means th re-deployment of people to do the work that can't be automated — work that requires real-time decision-making outside of the prescribed rules."

Despite low confidence now, SOAR will be spreading in the near future

Indeed, results from the Ponemon report echo Finn's words. Just over three-quarters of the providers participating in the study said that automation may actually be widening the security skills gap in that AI services require more highly skilled security sta not less, which exacerbates the staffing issue.

Also from that report, just over one-quarter of healthcare organizations reported employing AI as an aspect of cybersecurity. A

even less than that — a mere 15% — are even sold on automation at all, saying that they believe that AI should be relied upo and trusted for cybersecurity . . . which means that a whopping 85% don't see AI tools as a solution to the problem of vulnerab healthcare data. However, perhaps surprisingly in light of that statistic, just over 40% of providers say the insufficient number specialized, highly trained workforce have compelled them to invest in some form of AI for cybersecurity for the future.

Outside of fanciful sci-fi, AI isn't in line to replace people. But security experts believe it can help in the fight against security threats and attacks. A recently-released Gartner report found that by 2020, 15% of healthcare organizations employing five or more security personnel will implement the SOAR program (Security Orchestration, Automation and Response).

The report cited a spike in security alarms and not enough staff to handle them as the impetus for that projected adoption of th SOAR protocol. As it stands now, security teams must manually review large amounts of security data and gather threat information, an incredibly time-consuming, painstaking process that, without sufficient manpower to carry it out, results in healthcare entities all too often being one step behind the bad actors.