The security **game changer**

Technology, in concert with talented people and strong processes, can revolutionize the way agencies defend their IT assets

Dennis Reilly
Vice President of Federal Sales, Gigamon

THE GOVERNMENT WILL never be able to outspend increasingly well-financed, highly motivated adversaries, so agencies must get the maximum return on every cybersecurity dollar to buy down that risk. Although there are many models for risk reduction, they all hinge on three factors: people, processes and technology.

People represent the most challenging element. Surveys by the National Institute of Standards and Technology show that of the 780,000 cybersecurity positions in the U.S., 350,000 are vacant. Worldwide, the number of open positions is expected to grow to about 3.5 million by 2021, with about 500,000 in the U.S., according to a Cybersecurity Ventures report sponsored by Herjavec Group.

Despite what the government does to hire, train and retain talented cybersecurity professionals, it will be difficult to close that gap. Therefore, agencies must equip employees with the latest technology and automate lower-value tasks so that cybersecurity professionals can do the high-value activities and strategic thinking necessary to stay ahead of adversaries.

Processes continue to improve, but they generally do so in response to a threat, which means that the real game changer will likely be technology. The number of new cybersecurity tools continues to grow, and the challenge for government and industry is finding the handful of technologies that can make the biggest impact on the cyber fight and turn the advantage from the attacker to the defender.

The role of automation and orchestration

Government security teams are being inundated with data, and they must have the ability to understand and then act on that data. The right technology can help cybersecurity professionals triage indicators and automate some responses so that they can devote their time to making the tougher decisions or conducting the more intense forensic work.

There are potentially hundreds of thousands of threat indicators and approved countermeasures, and it's impossible to staff a security operations center with enough people to handle that volume, so automation and orchestration — performed through a security delivery platform — are essential.

Automation and orchestration are not new ideas. In fact, the intelligence community began developing a program called Sharkseer several years ago that uses commercial threat intelligence, anti-malware and other cybersecurity tools, and some early automation and orchestration techniques. Sharkseer has increased threat detection at the boundary by a factor of 10. Mitigation rates have increased by about 250 percent. The time it takes to analyze and resolve an attempted exploit has decreased from weeks or even months down to a matter of days.

davooda/Shutterstock/GCN Staff

The right technology can help cybersecurity professionals triage indicators and automate some responses so that they can **devote their time to making** the tougher decisions.

Funding the most promising projects

Congress and the White House have made IT modernization a priority, and there's a big push to transform cybersecurity at the same time. The Modernizing Government Technology Act is playing a key role and can have an even bigger impact if we shift the focus from funding many small projects to tackling a handful of bigger projects that have high promise.

If a proof of concept goes well, a project like Sharkseer could be replicated across multiple agencies through the regular budget process or through the Department of Homeland Security's Continuous Diagnostics and Mitigation program.

The government needs to continue funding CDM, Sharkseer, the Defense Department's Joint Information Environment and similar programs to help all agencies create the right balance of people, processes and technology to defend their increasingly complex IT environments. ■

Dennis Reilly *is vice president of federal sales at Gigamon.*