Operations Leads Share Benefits, Dependencies and Decisions on Security Automation

Treating security like a business function encourages agency leads to get involved early on.

James Mersol

Wed, 10/09/2019 - 10:19

Photo Credit: PhonlamaiPhoto/iStock

A lot of time, money and energy in cybersecurity are spent monitoring systems and networks, collecting data and analyzing the information for malicious activity and other anomalies. Automated processes may offer a solution to drive these costs down.

Automation gives organizations a tool to “deal with some of [cybersecurity’s] problems at scale”, said John Felker, assistant director of the Integrated Operations Division at the Cybersecurity and Infrastructure Security Agency at the Borderless Cyber summit Oct. 8.

Automation can guarantee consistent security processes and routinize mundane tasks, allowing cyber analysts to spend more time on strategic decision-making and other priorities that require high-end talent, said Harley Parkes, the integrated adaptive cyber defense lead at the Johns Hopkins University Applied Physics Lab.

However, Parkes cautioned, any organization looking to introduce automation must be mindful of certain dependencies. First, it needs an organization-wide understanding of its business processes and its risk tolerances. It also must hire or train developers that can build automated systems and integrate them with existing network architecture.

Agencies rarely “start from scratch” when designing networks, Felker said, recommending that an important first step is to understand that existing architecture and the constraints it places on any automated process.

Both speakers said that organizations should treat automation like a business process, not as something for only the IT division to consider. Without a full understanding of the agency’s business processes, risk tolerances and developer talent, which requires organization-wide communication, no organization can build successful, applicable, automated processes.

Treating automation as a business process requires putting business managers in charge of decision-making “from the beginning,” Felker said, even if the IT office is tasked with developing automation and implementing it into the existing network architecture.

“It’s a constant process and people need to be involved all along the way,” Felker said. “Make decisions based on the risk you’re willing to accept.”

This organization-wide perspective is especially important for cybersecurity, Parkes said. He recommended that organizations' leadership boards should look at where they are spending the most money on cybersecurity and viewing automation as a potential solution that would lower that cost, treating cybersecurity and risk as a business problem, not an IT problem.

"Because it is a business problem," Felker echoed, "the CEO needs to own it. They need to understand it. … We're starting to see senior executives, deputies and other positions take more ownership of these issues."

The panel recognized that top leadership does not necessarily have time in their schedules to devote to cybersecurity, but also commended some organizations for creating cybersecurity teams to report on the issue at C-suite meetings so the top leadership remains informed.

Both Parkes and Felker said that the financial and energy sectors have adopted security automation effectively. Parkes explained that the financial sector has been especially "forward-leaning" on designing use cases and taking lessons learned from those cases, while the energy sector is well-positioned to take best practices from industrial control systems and apply those to automated security. There has been particular growth in oil, natural gas and electricity firms, Felker noted, but said he would like to see more progress in the transportation and health sectors.

An opportunity from the private sector that organizations may use to help obtain the code and tools to pursue automation is with the newly created Open Cybersecurity Alliance.

IBM Security and McAfee created alliance to "develop and promote open-source common code, tooling, patterns and practices" and share them amongst vendors and customers to foster greater integration and interoperability of these tools, representatives said at the event.

"This is not just a launch," said Darren Thomas of McAfee, "but a call to action."

View printer friendly version
automation
cybersecurity
DHS
cisa

Standard