Automation Can Help Manage Security

Automation is a key element of FedRAMP operations in general and cyber security efforts in particular. In fact, from a cloud security perspective, automation has become essential. It's now a basic requirement to ensuring that a security posture is ideal for cloud services to be consumed by organizations.

Automating cyber security functions "has become imperative, and that's why the FedRAMP framework sort of lends itself to establishing a standardized way of doing things," Raj Parameswaran, president of IT at government services provider Maximus Federal said in a session on the value of automation at a recent FedRAMP Summit.

> **"From the operational efficiency standpoint, it becomes an important imperative for us to make sure automation is embedded through the security management process."**
>
> **— RAJ PARAMESWARAN, PRESIDENT, INFORMATION TECHNOLOGY, MAXIMUS FEDERAL**

Automation is not something that can be done on a partial or temporary basis. "It's actually a lifecycle process," Parameswaran said. "From the operational efficiency standpoint, it becomes an important imperative for us to make sure automation is embedded through the security management process, so that we're not waiting for

people to spend the time and effort to actually identify [issues] before they analyze and then [find] a way to remediate. Without automation this will become a significant challenge."

Manual processes for initiatives such as threat hunting, which can typically take many hours, can be accomplished within minutes because of automation.

Maximus Federal has begun the automation process for cloud security but still has a long way to go, Parameswaran said. The effort can't be rushed, because providers need to make sure a given security process is mature enough to be automated, and also to ensure that automation will not trigger false alarms and other issues. "It is important for us to have a standardized way of doing things," he said.

It's a similar situation to deploying robotic process automation (RPA),

Parameswaran said. Organizations should first make sure that the actual processes are optimized and aligned with business goals before automating them.

"All the governance elements need to be automated; there's no reason we can't do that."

— SHANE BARNEY, CISO AT THE OFFICE OF INFORMATION TECHNOLOGY, U.S. CITIZENSHIP AND IMMIGRATION SERVICES

Automation can help organizations address the "technical debt" that can accumulate over the years, by freeing up time and resources, said Shane Barney, CISO at the Office of Information Technology, U.S. Citizenship and Immigration Services (USCIS), and another panelist at the session.

USCIS was able to remove an entire tier of its security operations center (SOC) because it was no longer needed due to automating certain tasks, Barney said. Rather than eliminating jobs, "we reinvested our time, energy, and training into those people to [make] them better analysts," he said.

An important factor to consider when automating processes is integration of all the various, disparate tools in place that feed data to the SOC.

"You've got a log management tool set, you've got endpoint detection, you may have some behavioral network analysis tool sets," Barney said. Organizations need to begin integrating those systems and data points so that if one detects a certain behavior that corresponds with findings from another tool, security teams can immediately know this.

USCIS is taking cloud security automation quite seriously as it continues to enhance its program. Eventually, "there will be no manual processes to the extent possible," Barney said. "If there is a manual process, I personally have to approve its existence." Automation will extend to areas such as documentation and compliance.

"All the governance elements need to be automated; there's no reason we can't do that," Barney said.

Article Source: FCW FedRAMP Summit | August 18, 2021