DevSecOps Secrets For a Successful IT Strategy

DHS, the Air Force and the VA discussed strategies for implementing DevSecOps at a GovernmentCIO Media & Research event.

Kate Macri

Thu, 12/03/2020 - 17:16

To successfully execute a DevSecOps strategy, put the customer first. Leaders at the Department of Homeland Security, Air Force and the Department of Veterans Affairs agree.

“We started in 2018 with an Agile mentality, but focused on the data science and data analytics customer more than anything else,” said Col. Charles Destefani, deputy chief data officer of the Air Force at a GovernmentCIO Media & Research DevSecOps event this week.
Ty Schneider, systems engineer at the VA, concurred, “We really want to provide the best customer service possible to the veterans."

Citizenship and Immigration Services CTO Rob Brown said his IT department implemented DevSecOps so successfully that his department sometimes acted as a “marriage counselor” for other USCIS directorates in transition.

“One of the largest challenges across the board ... is really the skills, the training, ensuring folks are continuously improving in those various disciplines,” he said on the panel. “It's ongoing, and I can't stress enough that's probably the No. 1 challenge.”

Destefani and Schneider both highlighted ways DevSecOps improved and streamlined IT operations and security at their organizations. The VA used DevSecOps within a platform-as-a-service (PaaS) cloud environment, which matched the VA’s unique software needs and supercharged the agency's IT modernization.

“It allows people to come on to a common platform and allows us to serve them so much better,” Schneider said. “PaaS really will enable you to make use of scale. With VA there's often spikes in demand and you want to meet those demands. You can quickly scale up, scale down based on what's going on in real time. You're going to have a much more comprehensive and effective solution. When we look at PaaS, we're wanting to have platforms that not only operate on prem, but also operate in the major cloud spaces.”

The Air Force's own DevSecOps initiative resulted in a 90% increase to its software delivery cycle.

“We started with a data science reference architecture that laid out all of the capabilities in a microservices format to do data science and AI projects, and our efforts in the cloud have been to simply make available to the DOD the tools industry takes for granted and combine those with DOD data sets where the ATO comes in, then enabling that for a wide variety of mission sets,” Destefani said. “We are able to put capabilities out into the cloud within 30 to 45 days where it used to take 10 months to a year.”
One of the big challenges facing the VA is shepherding contractors and vendors into the Agile mindset.

“As far as challenges at VA, there's a lot of the older type of thinking with Waterfall and such and that tends to slow things down. It's a little bit inefficient, costs more, puts security on the backburner,” Schneider said. “Moving into this newer way of thinking with Agile, you're going to get a much more cohesive result. It's going to drive teams together rather than apart. It's going to create efficiency throughout the projects and put security at the forefront.”

USCIS solved initial DevSecOps transition challenges by focusing on relationships, Brown said, which he said are paramount to any IT modernization strategy.

“We had security write our cloud formation templates for us," he said. “The approach was setting up a war room where we worked for a couple of weeks and ultimately a full month to get our first workload into production, to ensure we had the right security engineers in the room and part of that pipeline and delivering to production. That was exceedingly important.”

While each agency faces unique challenges as they implement DevSecOps, keeping the customer experience top of mind is the common refrain.

“Treat DevSecOps as you would anything else, and put that experience at the forefront,” Brown said.