Why Federal Agencies Turn to DevSecOps to Improve the ATO Process

Leaders discuss execution of cybersecurity is just as important as modernized systems.

Kate Macri
Thu, 11/05/2020 - 12:28

Automating the authorization to operate (ATO) process could save federal agencies time and also enhance IT infrastructure security. DevSecOps and Agile processes could accelerate the ATO process, according to some federal IT leaders at a virtual event hosted by the Institute for Critical Infrastructure Technology (ICIT) last week.

Danny Holtzman, cyber technical director at the U.S. Air Force, said DevSecOps in IT is uniquely positioned to handle gaps in the ATO process.
“One thing that keeps me up at night as an authorizer, if [there is] a known risk in it that I misidentify,” Holtzman said at the event. “That's what I'm concerned about. Can we continuously monitor and watch that risk over time?”

Steve Pruskowski, a security test and evaluation lead at CISA, said adopting a “holistic” approach to IT development and security is key for automating the ATO process.

“We deal with our end users a lot on the development side, and meet demands and get tools the analysts need out the door as quickly as possible,” he said at the event. “But also know we have risks and take a holistic look at this is what the environment looks like, the threatscape looks like, then [telling] our authorizers and customers this is what we found inside your apps, this is how you might want to prevent them, and then what is the business risk to not doing this.”

Speed of delivery is equally important, according to NASA Chief Data Officer and Associate CIO Ron Thompson. Speed of delivery helps quell IT hiccups, which can hinder the agency mission.

“Where the speed of delivery for the ATO process comes in, is the goal of optimizing our operations,” he said. “It's really linking into that authoritative approval chain to make sure that security is baked in upfront. ... Speeding up the ATO process is valuable, it's important, and it's something we're taking a very close look at right now.”

Ron Ross, a fellow at NIST, said agencies should definitely focus on DevSecOps to optimize the ATO process because the cyber threat landscape now evolves at a breakneck pace. Federal agencies, he said, should think about moving to an IT environment where the ATO process is continuous.

“The attack surface for the adversary is humongous,” he said. “Authorization to operate has always been about giving senior leaders credible basis to make risk-based decisions. We authorize systems and common controls. The system is defined as the capability. It's complicated, it has a lot of moving parts. We consider this a paper-based process. The world of DevSecOps is absolutely the right place to make [continuous ATO] happen.”
NASA hopes to use artificial intelligence and machine learning to automate and accelerate the ATO process. Prukowski suggested federal agencies look at the process in “smaller and smaller bites” in order to ensure accuracy and resiliency.

The ATO process should “add value,” not be a “hindrance,” Thompson added.

“I think the common theme you're hearing today is that we're not just doing an evolution of cybersecurity. This is a revolution, from static security to dynamic security,” Ross said. “It's not just about doing things digital versus paper. We need speed, transparency, and information-sharing. It's the execution and efficiency of doing those things.”

View printer friendly version
Department of Homeland Security
CISA
Federal Cybersecurity
ATO
DevSecOps
NASA
Army
NIST
Standard