4 Ways the Defense Department Can Leverage DevSecOps **to Enhance the Mission**

As the Defense Department navigates an increasingly complex threat landscape, the organization is eyeing a shift to a DevSecOps mindset to ensure it can securely innovate. At a recent roundtable, we asked the experts how DOD can begin adopting this practice and what it can do to drive the mission forward.

After a year like 2020, the word "security" has taken on a whole new meaning. As terms like "remote work" and "hybrid workforce" enter the public sector vernacular, organizations must determine how to secure their IT infrastructure beyond the traditional perimeter. And, as the complexities of the COVID-19 pandemic continue to take center stage, cybercriminals are disproportionately targeting governments and critical health infrastructure responsible for delivering services to the American people.

These security concerns run rampant across organizations everywhere, but the Defense Department is perhaps the most vulnerable to such threats. After all, a cyber attack targeted at the DOD could have lasting national security consequences. What's more, warfighters and military personnel are stationed in multiple locations, making it increasingly important to prioritize identity and access management. One way to help solve these challenges is for the DOD to shift operations and workflow to follow a DevSecOps mindset, one where security is not an afterthought but a critical piece of the development and operational process. Over the past several years, the DOD has looked to shift toward a more agile and collaborative model. In 2019, **the Pentagon launched the DoD Enterprise DevSecOps Initiative**. The goal: Avoid costly IT catastrophes by identifying flaws early and often in the software development lifecycle.

But there's still work to be done. So, how can the DOD begin to turn DevSecOps from a goal into a reality? At a recent roundtable, produced by Government Executive Media Group and hosted by IBM and Red Hat, we asked the experts working hard to bring DevSecOps to the DOD for insight. Here's what they had to say.

1 MAINTAIN A CONSTANT LINE OF COMMUNICATION

Warfighters and developers often exist in very different spheres. Not only are they separated by miles of physical distance, they also operate in silos that hinder mission success. That's according to Bob Parker, technical director of the Program Executive Office for Command, Control, Communications, Computers and Intelligence (PEO C4I) at the Navy.

"The perceived distance between a sailor and a developer is 24,000 miles," he said at the roundtable. "We've got to give the fleet the right process and the right quality evidence that we're building things correctly. And then we can go faster and give sailors a voice in their own applications and make them more effective."

Parker recommends telemetry as a means to help improve these processes.

"[Sailors] will tell us things, they may not tell us things, but telemetry … kind of looking over their shoulder automatically can tell me which features they're using [and] aren't using," he explained. "So being able to take that into account in the development life cycle."

2 BUILD YOUR WORKFORCE WITH DEVSECOPS IN MIND

Closing the loop between developer and warfighter will also require DOD to invest in the right talent.

"Developers are out in their silos, but there's no real tie back to actual warfighter capabilities or if the warfighter even wanted those capabilities. That's a hard problem to solve, but I'd love to see DOD get more talent in-house, where not everything needed to be contracted," said Red Hat Chief Architect John Osborne.

What should this workforce actually look like? Osborne recommends a mix of traditional IT workers and a newer DevSecOps workforce. Ian Anderson, lead DevSecOps engineer at Naval Surface Warfare Center Dahlgren, concurs.

"Where DevSecOps can come in and really help is ... creating that infrastructure, creating that environment that is up to the compliance of our cybersecurity professionals, but allows developers the flexibility to try new things, try out new software and allow them to experiment," Anderson explained at the roundtable.

> "Developers are out in their silos, but there's no real tie back to actual warfighter capabilities or if the warfighter even wanted those capabilities. That's a hard problem to solve, but I'd love to see DOD get more talent in-house, where not everything needed to be contracted."
>
> JOHN OSBORNE
> Chief Architect
> **Red Hat**

Moreover, the advent of DevSecOps will require DOD to embrace a diversity of roles and skillsets going forward.

"[We need to] look at things like what are the skillsets that teams need to have in order to operate in a DevSecOps environment, which are different than the skillsets of a traditional type of operational environment in terms of application development?" said Daniel Chenok, executive director at the IBM Center for The Business of Government. "And how [do we] think about the application of new technologies, of intelligent automation, artificial intelligence, and how DevSecOps can help speed the development of application?"

To engage a workforce with new ideas and diverse skill areas, many are pushing for DOD to adopt more career training programs. One such advocate is Louis Koplin, deputy CTO for the Department of the Navy Chief Information Office.

"For human capital, there's a lot of recognition about a trades apprenticeship type of model where you're really bringing people in," he said at the roundtable. "We need to think about our trade skills and actually getting practical hands-on [experience]."

He added that some divisions within the DOD, such as the Army Futures Command and Kessel Run, are already taking steps to drive this type of skill-sharing — and this trend will only grow as the Defense Department continues to adopt the principles of DevSecOps.

3 LOWER THE BARRIER TO ENTRY FOR INNOVATION

Of course, innovating is easier said than done. According to Anderson, there are a number of hurdles and limitations that stifle innovation within the DOD.

"Our warfare center is a working capital fund, so we don't get direct funding from the government," he explained. "There isn't a large pot of money for us to allow our developers just to go out there, try new concepts, try all these new things."

Anderson added that some of the processes in place at the DOD make it difficult to innovate. "You have to go through hours and hours of paperwork, make sure you're putting it into the right systems, getting the right approvals," he said.

> “Things can be done different ways. You just have to try and sometimes fail, but things can be improved, no matter how great you think they are.”
>
> IAN ANDERSON
> Lead DevSecOps Engineer,
> **Naval Surface Warfare Center Dahlgren**

4 YOU CAN'T HAVE DIGITAL TRANSFORMATION WITHOUT CULTURAL TRANSFORMATION

Meanwhile, Amy Henninger, senior advisor for software and cybersecurity at Director Operational Test and Evaluation at DOD, rejects the notion that the organization has an innovation problem. Instead, she explained at the roundtable, DOD has an innovation adoption problem.

“I think it's for cultural reasons, programmatic reasons. One of the core problems to getting things integrated is having … data exchange,” she said. “That's a cultural thing that we have to break through.”

Henninger urged leaders to consider what they could accomplish if they removed all of the red tape.

“Because we are the DOD, our software developers are not in-house. We have to work through layers of acquisition bureaucracy to get to them,” she added.

Of course, innovation adoption is possible within the DOD, but it will require a shift in mindset.

“I really see some trauma from past technology acquisition efforts, and people have taken away from that that we cannot do large-scale technology change, they fundamentally don't believe we can. No amount of money thrown at sustainment or integration is going to fix that because it's not a money problem, it's a culture problem,” Koplin explained.

Anderson also cited the legendary Rear Admiral Grace Hopper's famous sentiment that “the most dangerous phrase in the language is ‘we've always done it this way.’”

“[Hopper] had a clock in her office that ran backwards just to prove her point that things can be done different ways,” he explained. “You just have to try and sometimes fail, but things can be improved, no matter how great you think they are.”