4 strategies to overcome obstacles in adopting DevSecOps in your agency

THIS CONTENT HAS BEEN PROVIDED BY ATLASSIAN

Ken Urban, director of technology, public sector

ATLASSIAN

A recent survey conducted by Federal News Network in partnership with Atlassian revealed a large disconnect between IT and non-IT staff at federal agencies. Fewer than 10% of respondents said their business or mission area was heavily involved in setting project requirements for IT services. Two-thirds of respondents said they don't get to comment on or review new technology capabilities during development or before they are launched. And 63% said collaboration within the agency was difficult.

It's likely that these issues are familiar to anyone who's spent time working in the federal IT space. Ken Urban, solutions engineer for Atlassian, recognized them from his own time working IT at the National Security Agency. Early in his career there the agency did not have a complete vision of how DevOps could be integrated, and good tooling was effectively nonexistent for the majority of their developers. He helped to build out a solution that introduced the concept of agile development and 'fundamentally altered the course of development' at the agency.

But it didn't happen overnight; Urban said he had the same obstacles to contend with.

"How is it that you can say something like 'mission is not involved in requirements and setting up a program?' It boggles my mind," he said. "Think of it like building an airport. How do you know, to build a small airport or a big commuter airport unless you're talking to the stakeholders involved? I think you need to bring that to all levels of the organization; it starts at the top, and it goes all the way down to the bottom. For DevSecOps to work, you have to - to quote one of Atlassian's core values - play as a team. You all succeed or fail together."

Senior leaders need to understand what's going on in the trenches to understand why a program is succeeding, or isn't. Meanwhile, IT staff often doesn't have the bigger picture, which makes it hard to change how something works. Often, the first, biggest challenge in government is getting everyone on the same page.

That's why Atlassian developed a free Atlassian Team Playbook. The playbook helps agencies learn how to foster the sort of culture of collaboration required to enable DevSecOps. It outlines a series of "plays" that can help agency teams work together to overcome these challenges. But Urban also identified four strategies to help agencies specifically when it comes to adopting DevSecOps:

1. **Foster true cross-team collaboration:** This involves more than co-location and regular team meetings. Agencies need to change the way they work on a fundamental level. For example, baking security into development is quickly becoming standard practice. But what about compliance? Urban said software accreditation can take as long as 6-12 months. However, that can be reduced to weeks or even days by integrating compliance into the development pipeline just like security. Ken's team achieved this, and other efficiency gains, by focusing on integration motions.

2. **Transparency that fuels decision superiority:** Information sharing isn't always a simple process in government, but it's core to just about every mission. Decision superiority is based on information superiority. And when leaders don't have enough -- or all -- of the information, it's difficult to make good decisions. Urban experienced this firsthand when he made a decision about a product direction, and a junior developer on a third-party team pointed out that Urban's assumptions about his team's dependencies that weren't accurate. It changed his entire perspective of where investment needed to be made. Urban quickly changed course, saving weeks of effort in the process. And naturally, sensitivity and restrictions have to be respected, but over-classification can also be an issue. Urban said implementing an automated knowledge management solution can help improve the DevSecOps chain by taking the burden of information acquisition and dissemination off the team.

3. **Repeatability through smart automation:** Utilize automation where appropriate, like the automation suite in JIRA, Urban said. Look at what rote work is still manual; can it be done more efficiently, and can it be done the same way every time? Finding opportunities for and implementing automation requires getting the team on the same page, with similar version control systems. That makes it transparent to other teams, and self-documentation processes make it easier to audit.

4. **Continuous, adaptable training:** This should be adjusted to the role, level of knowledge and developing skills of the workforce, not just a one-size fits all approach. For example, annual trainings are valuable, but they are the bare minimum and often can't deliver the sum total of what a team or individual needs to succeed. As a developer, security often isn't first on the mind; it's how best to implement a feature or fix a bug. Agencies should consider their training like they would consider their security: with an emphasis on continuous. In evaluating DevSecOps training, look for outcomes that help employees perform better, write more secure code, or understand the bigger picture better. Invest in the team. And then set a training schedule and curriculum that helps them to continuously evolve.

Once those strategies are in place, it's time to look at tooling. Agencies need tools with agile methodologies baked in. New DevSecOps tools are powerful and extremely flexible, with clear gains for the mission because they don't require a developer to make a change. Agencies should embrace and invest in these kinds of tools because they allow for changes to be made in the user interface in minutes, saving considerable time and resource allocation across the entire project or program. In this way, adopting the right tools can unleash power of every team and enable teams to work the way they need to work.

"A lot of people have said that tooling is easy. That is, to some extent, true. But good tooling is also a requirement for a successful DevSecOps transformation," Urban said. "You're going to need tools that deliver the transparency, automation, repeatability and collaboration required for true gains. Moreover, you need your tools to be agile alongside of you and adjustable to where your team is today."

However, with such flexibility comes the need for process, guidelines and deep project visibility to ensure that everyone is focused on the same measurable outcomes. And that's where the Team Playbook comes in. No matter where they are in their DevSecOps journey, agencies can rely on Atlassian software solutions and the Atlassian Team Playbook to deliver the framework and modern tools needed to drive real and lasting DevSecOps transformation.

Been there.
Scaled that.

ATLASSIAN

Change is hard, especially for government agencies. Atlassian is here to help ease the pain of shifting to DevOps. Transform your agency workflows and speed application deployment time with open, flexible software.

View the executive DevSecOps Survey

Work smarter and faster, together.

- Unified workflows, centralized dashboards
- Streamlined knowledge management
- Real-time, visual data, task-tracking, and messaging notifications
- Best-in-class security

Learn More