Modernizing software development in a fast-changing world

DevSecOps is at the heart of efforts to build, secure and maintain the apps that make digital transformation possible

The cyberthreat landscape is constantly shifting at a time when government agencies face a growing demand for digital services. Agencies can balance those competing priorities by embracing a methodology that speeds and strengthens every aspect of software development, including security. Known as DevSecOps, the methodology allows agencies to create, deploy and maintain apps that are targeted to users' needs, easily updated and continuously monitored for security purposes.

As its name implies, DevSecOps brings together the development, security and operations teams in a cultural shift that emphasizes collaboration over silos. It is also moves security from an afterthought into a key element of software development. Vulnerabilities are identified early so they can be remedied before they make their way into the operating environment, and that security oversight never stops.

In a recent survey of FCW readers, 68% of respondents said the changing cybersecurity landscape is driving the adoption or evolution of DevSecOps at their agencies. Those security concerns crop up at all levels of government. The Colorado Governor's Office of Information Technology illustrates the pitfalls of traditional development processes. In a successful application for the National Association of State CIOs' State IT Recognition Awards, Colorado officials wrote that they created a DevSecOps program in part because "in one instance, two years of development to modernize a system had taken place before a single code security scan. When the pre-go-live security scan was performed, it detected more than 10,000 vulnerabilities, which required mitigation and caused the delay of multiple releases."

A way to improve supply chain security

Another key element — and outcome — of DevSecOps is enhanced supply chain security. One area of concern is the use of open-source elements in modern apps, which can range as high as 90% of a given piece of software.

DevSecOps by the numbers

Sources: Check Point Research, FCW and IDC

$2.6B TO $7.5B

Projected worldwide increase in DevSecOps spending from 2020 to 2025

68%

FCW survey respondents who said cybersecurity concerns are driving the use of DevSecOps at their agencies

49%

FCW survey respondents who said lack of employees with the right skill set was an obstacle to DevSecOps adoption

It's reasonable to avoid re-creating something that already exists, but agencies are typically unaware of the security vulnerabilities that can lurk in their open-source components.

In late 2021, a vulnerability in the Java-based utility Apache Log4j allowed hackers to gain control of third-party systems, with a potentially widespread impact. As the Cybersecurity and Infrastructure Security Agency noted in its guidance: "Log4j is very broadly used in a variety of consumer and enterprise services, websites and applications — as well as in operational technology products — to log security and performance information."

Secure upgrades to Log4j have since been released, but the bug highlighted the ongoing challenges. In January, the White House convened government and private-sector leaders to discuss ways to better secure open-source software, with a particular focus on "preventing security defects and vulnerabilities in code and open-source packages, improving the process for finding defects and fixing them, and shortening the response time for distributing and implementing fixes," according to a White House statement.

The Executive Order on Improving the Nation's Cybersecurity has a section devoted to supply chain security, with recommendations that include the use of secure software development environments and software bills of materials for purchased apps or components.

Central characteristics of DevSecOps

The DevSecOps process is often depicted as a figure eight that loops around in an ongoing cycle of plan, code, build, test, release, deploy, operate and monitor. It is characterized by the use of agile methodology, microservices, containerization, low- or no-code environments, continuous security monitoring, and a heavy reliance on automation of any and all activities, particularly performance and security testing.

Key government agencies provide guidance on how to make the most of the methodology. Version 2.0 of the Defense Department's DevSecOps Fundamentals Playbook lists 10 steps for achieving a successful implementation, and they include adopting infrastructure as code, driving continuous improvement and defining a meaningful DevSecOps pipeline that is "analogous to a manufacturing assembly line." DOD has also embraced the use of DevSecOps-based software factories across the military services as a way to speed the delivery of secure software.

The General Services Administration's comprehensive guide states that "successful DevSecOps teams have processes characterized by repeatability, low redundancy, high collaboration with dispersion of collective efforts; in order to achieve this most efficiently, automation and auditability [are] prized above subjective decision-making. The decisions that would drive successful release should be codified in code" or in checklists with clear yes/no decision points.

In addition, the National Institute of Standards and Technology's Special Publication 800-218 shows agencies how to incorporate the Secure Software Development Framework into their existing practices, explain their secure software development requirements to third-party suppliers and buy software that adheres to the framework. It also provides a common language to describe secure software development practices in a way that all members of the team can easily understand.

Collaborating in pursuit of a common goal

Enabling the development, security and operations teams to communicate clearly is essential to the success of DevSecOps, which hinges on aligning people, processes and tools in pursuit of a common goal. DOD takes it a step further by stating in its playbook that "all stakeholders in the organization must be committed to changing the way they view their job responsibilities and, most importantly, interact with each other."

In FCW's recent survey, participants were somewhat evenly distributed across a scale of 1 to 5 when asked about their agencies' commitment to DevSecOps methodology, with 10% saying they are devoted users of DevSecOps and 13% saying it will never take hold at their agencies. They cited a number of cultural obstacles. The top three were the lack of employees with the right skill set (49%), entrenched processes (45%) and limited understanding of the methodology's benefits (38%).

In what might be a sign of the methodology gaining traction in government, however, only 24% said resistance to bringing together the development, security and operations teams was an obstacle, and 7% said there were no obstacles.

As more agencies adopt DevSecOps to manage all aspects of developing and deploying secure, modern apps, they will build trust between the government and the people it serves, while also boosting employee engagement and productivity. In other words, they will recognize that DevSecOps is a prerequisite for achieving digital transformation. ■