

Accelerating Digital Transformation with DevSecOps

Government agencies look to adapt more secure, innovative software development

DevOps and DevSecOps are philosophies, movements and even cultures of continuous improvement and integrated security – at scale. When successfully implemented, it delivers a powerful advantage for government agencies at all levels, and can be especially supportive for agencies undergoing digital transformation.

DevSecOps is a combination of development, security and operations. It's used to bring security into the development cycle of new software and applications from the start, instead of trying to bolt cybersecurity on after the fact. It requires a lot of communications between all three teams, as well as a unified platform so that everyone is working from the same plan with the same tools.

Moving from a traditional waterfall type development cycle to the more agile DevSecOps is not a quick process, but the rewards of doing so can be immense, especially for government agencies that must consider security in everything that they work on. But DevSecOps benefits go beyond security. A DevSecOps environment is more efficient, fosters innovation and reduces costs, all things that government agencies need to achieve.

As federal agencies begin to adopt DevSecOps, they will continue to improve their ability to build stronger security frameworks and quicker software development times. Four experts recently met

during a **FedInsider webinar** to discuss the best methods for government agencies to achieve those goals, as well as the secondary advantages of DevSecOps that can be achieved while also accelerating their digital transformations.

Focus On Developing Proactive Security Measures & Infrastructure

Cybersecurity issues are constantly brought to the forefront these days thanks to high profile breaches like the ransomware attack on the Colonial Pipeline. But government agencies are always concerned about security. The problem is that most cybersecurity in government is reactive, so it's always by definition a step behind attackers. DevSecOps can change that by baking security into the process from the start, proactively stopping attackers and denying them a beachhead from which to launch their attacks.

"From a security perspective in today's modern world with digital transformation, we can no longer rely on periodic stands and paper based compliance," said Kurt Greening, Leader Public Sector, Prisma Cloud, Palo Alto Networks. "We need to first shift our security to early in the process of development and then focus on the people aspects of DevOps, like collaboration."

As part of that shift to proactive security, government should also re-provision its resources so that they are more agile and built to be resistant to attacks. DevSecOps

Featuring:

■ **David Vergano**

*Systems Development
Division Chief, IRM,
U.S Dept. of State*



■ **Hasan Yasar**

*Technical Director,
CDC Group, SSD Div.,
Software Engineering
Institute, Carnegie
Mellon University*



■ **Bill Church**

*CTO,
F5 Gov't Solutions*



■ **Kurt Greening**

*Leader Public Sector,
Prisma Cloud,
Palo Alto Networks*



can help with that by using it to reprogram and repurpose the key pieces of software that make up and control an agency's infrastructure.

"I think in the federal space a lot of times we've been playing catch up and responding to the most recent data spills. And I think because of that it's difficult to prioritize time and efforts. We're fighting the fire, and we're not able to concentrate on building for the future," said Bill Church, Chief Technology Officer, F5 Government Solutions. "We need to look at refactoring resources into modern apps and using DevSecOps practices to do that."

DevSecOps Can Act as a Foundation for All Collaboration Efforts

One of the best benefits of implementing DevSecOps, and one that is often overlooked, is the foundation of collaboration that it offers, which can be used in other areas like supporting educational programs. Collaboration efforts built on DevSecOps offers the opportunity for internal and external stakeholders to meet on a regular basis, and can form the basis for any collaborative effort.

"It's one of the fundamental principles of DevOps, building up and learning, and we expect everybody to share what they learn from their experience," said Hasan Yasar, Technical Director, Continuous Deployment of Capability Group, SSD Division, Software Engineering Institute, Carnegie Mellon University. "Everything is changing with respect to the system that we are building. And DevOps is bringing that learning piece."

And once you have DevSecOps in place, tapping into the collaborative aspects of it as a foundation of educational or training programs can make it much easier to implement for most agencies.

DevSecOps Allows Agencies More Opportunities To Innovate

One of the most important traits of a strong cybersecurity framework is the ability to adapt and innovate. The threat landscape is constantly shifting and agencies need to have lateral mobility to meet these changing threats. DevSecOps pushes teams to

make small, subtle and innovative changes that make security solutions stronger. Without a strong DevSecOps foundation where security is an important part of every phase of development and deployment, you won't be able to support innovative security ideas or practices.

David Vergano, the Systems Development Division Chief of the Bureau of Information Resource Management with the U.S. Department of State gave an example of one of those small innovations that actually helped to really improve security.

"One of the things that worked out well is, for example, putting documentation into the repository and, honestly to me, that's innovation," said Vergano. "Not having good documentation and then coming in behind somebody else and trying to fix something is incredibly frustrating."

Vergano also said he believes that being able to make slower, smaller changes is another form of innovation. Rather than make large corrections following each newly discovered threat, Vergano believes that making lots of small changes in a DevSecOps environment builds a stronger overall framework compared with traditional security philosophies.

First Define DevSecOps Goals and Build a Great Team

There are a lot of reasons why government agencies should want to support DevSecOps. The key to getting there is to first define which

goals are the most relevant for a particular agency and then use that to convince stakeholders to support the program.

"Ask what is the desired end state and understand other groups' priorities," said Vergano. "Then be able to explain what's in it for them. People can bring in ideas that will surprise you, and it's going to require commitment from everyone."

Getting DevSecOps working within a federal agency won't be a quick process, but it is achievable if you first set defined goals for the program and build a great team to implement it.

"Always start with asking why first," Hassan said. "Then create a team structure and build it up before you get started." If you follow that basic plan, an agency will soon be reaping the many benefits and rewards of DevSecOps and leaving the old, insecure and reactive processes well behind them. 

FEDInsider

Hosky Communications Inc.

3811 Massachusetts Avenue, NW
Washington, DC 20016

- ☎ (202) 237-0300
- ✉ Info@FedInsider.com
- 🌐 FedInsider.com
- 📘 Facebook.com/FedInsiderNews
- 🌐 Linkedin.com/company/FedInsider
- 📱 [@FedInsider](https://Twitter.com/FedInsider)

carahsoft

Carahsoft

14993 Sunset Hills Road, Suite 100
Reston, VA 20190
Contact: [Seamus Bergen](mailto:Seamus.Bergen@carahsoft.com)

- ☎ (703) 230-7425
- ✉ DevSecOps@carahsoft.com
- 🌐 Carahsoft.com/solve/devsecops
- 📘 Facebook.com/Carahsoft
- 🌐 Linkedin.com/company/Carahsoft
- 📱 [@Carahsoft](https://Twitter.com/Carahsoft)

© 2021 Hosky Communications, Inc. All rights reserved. FedInsider and the FedInsider logo, are trademarks or registered trademarks of Hosky Communications or its subsidiaries or affiliated companies in the United States and other countries. All other marks are the property of their respective owners.

carahsoft



MISSION BRIEF | FEDINSIDER.COM