FEDInsider

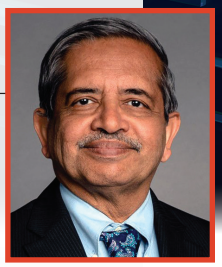
Driving DevSecOps in Government with Digital Transformation

As agencies move to cloud environments, cloud-native tools and DevSecOps are allowing them to automate security and workflow processes.

Featuring:

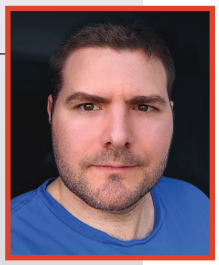
- **Taka Ariga**
  Chief Data Scientist & Director, Innovation Lab, U.S. Government Accountability Office

- **Dr. Ramaswamy Chandramouli**
  Sr. Computer Scientist, NIST



- **Daryl Knopf**
  Sr. Solutions Architect, GitLab

- **Robert Van Voorhees**
  Staff Solutions Engineer, VMware



Government agencies are adopting DevSecOps as they modernize technology systems, and for good reason. The method delivers a powerful advantage in terms of creating more secure software and applications, while also being used to help drive digital transformation initiatives, especially within cloud environments.

With automated, faster and secure releases and greater interoperability, agencies can focus more energy on their missions. Four leading experts in this field talked with FedInsider during a recent **webinar** to discuss the tools behind DevSecOps, and how government and industry are adopting its culture.

The following are some of the most important aspects of those efforts.

The Journey Starts with Digital Transformation

For the Army Futures Command, digital transformation is a core goal, and it starts with a culmination of culture and technology, according to Robert Van Voorhees, staff solutions engineer at VMware. Van Voorhees works with the Army Futures Command on its Software Factory to implement cloud-native software development to enhance capabilities.

The Department of Defense increasingly relies on contractors to have the technical acumen and capability to provide software for the military. However, the Army Futures Command Software Factory is cultivating a soldier-led Silicon Valley-like software company inside the Army so it can keep up with the changes in digital warfare.

By training soldiers and focusing on digital transformation for the armed forces, soldiers will be equipped with the technical capabilities needed to run software development, especially in the event of a crisis where contractors can't be deployed to the edge. This way, they'll have "that necessary technical capability and know-how ingrained into the actual culture and capability of the future U.S. Army," Van Voorhees said.

The Government Accountability Office's Innovation Lab also explores emerging technologies by developing prototypes and using DevSecOps and machine learning to scale solutions across the agency. "It's really our way to try to arrange capability from machine learning to blockchain to IoT to 5G, certainly cloud services as well, as we're tackling some of the evolving oversight challenges," said the lab's Chief Data Scientist and Director Taka Ariga.

For the GAO, driving that transformation is dependent on trusting those capabilities, and applying DevSecOps is critical to putting trust behind the solutions, especially as GAO navigates the various kinds of data it absorbs for oversight purposes.

"To us, DevSecOps is certainly a methodology for sure, but also a mindset for us to really integrate not only the technical components, but also the cultural and changed transformation element that needs to accompany that process," Ariga said.

Guiding the Government Towards DevSecOps

The National Institute of Standards and Technology is developing short-term and long-term technology initiatives to guide federal agencies to DevSecOps. One of those initiatives is to develop an application of the DevSecOps-specific architecture using microservices-based applications,

according to Ramaswamy Chandramouli, senior computer scientist at NIST.

These architecture services introduce containers and utilize a service infrastructure. "For that application, we are actually targeting DevSecOps methodology at great lengths," Chandramouli said. Longer term, NIST is reincorporating DevSecOps into its current software development frameworks best practices.

When looking to implement DevSecOps, Chandramouli said to first keep in mind that security and developer experience are the primary goals. Secondly, focus on the efficacy of the tool itself. Those tools must integrate into all testing and deployment phases seamlessly, because that will promote a better user experience. "It's not enough to implement the pipelines, it should be an efficient pipeline," Chandramouli said.

DevSecOps as a Best Practice in a Modern Developer Workflow

DevSecOps is "absolutely critical" for DevOps, said Daryl Knopf, senior solutions architect at GitLab. The GitLab DevOps platform helps agencies use automation to secure their code. "Automated testing, regular quality verifications and continuous security scanning are really at the core of digital transformation today," he added.

Take transparency and collaboration, for instance. If a developer commits the changes of a source code, pipeline automation will allow the developer to see any number of security or quality-related findings resulting from that commit. These findings, when included in the developer workflow, can be viewed by all stakeholders to ensure proper resolution of the findings. This makes for far better code development for approvals.

With inconsistent environments like those within the DOD (ranging from classified to unclassified networks, and on-premise to cloud), reducing the cycle time between code and application to production is even more critical. Currently, a lack of knowledge around compliance gates and control mapping is slowing developers down. Automating those critical conjunctions in the software development process is key.

VMware was able to enhance NIST's control mappings to create higher secure levels of abstraction. Ultimately, this makes it easier for developers to view the controls while coding, interact with stakeholders to get the code into production and ensure it's the solution the end user needed.

"Creating that process, automating it into what should be a full-fledged DevSecOps pipeline that ends in production, enables those soldiers and other application developers to actually create change in their environment and start interacting with code in production," Van Voorhees said.

Advantages of Advanced Cloud Methods

Cloud environments pave the way for capabilities that make day to day workflow more efficient and cost effective. When government agencies move to microservices, the ability to implement containers to deploy and manage those services without having to manage complete operating systems is essential.

Using Kubernetes in the cloud – an open-source container-orchestration system for automating computer application deployment, scaling and management – is game changing. Kubernetes allow users to spin up environments for team reviews and dynamic security scans, and provide enhanced resiliency via auto-recovery and auto-scaling in production environments.

"Leveraging containers in Kubernetes for government customers and, of course, commercial, accelerates the transformation and application quality without having to write everything from scratch," Knopf said.

As the Army Futures Command partners with the Army's Enterprise Cloud Management Agency, modern day cloud-native software development processes are also coming to the forefront. This is leading to the adoption of container orchestration tools like Kubernetes because using Kubernetes as a substrate creates consistency across various environments. Hosting security tools that are part of a DevSecOps process on a Kubernetes substrate helps organizations achieve that consistency across any deployed cloud environment, which can be particularly helpful for highly regulated organizations like the Army.

As the benefits of combining advanced cloud methods with DevSecOps are being recognized by both the public and private sector, Knopf said they are here to stay.

"If you're not using technologies like containers and Kubernetes yet, now is a good time to at least take a look. Cost savings, up time, resiliency and enhanced security options are all there, just waiting in the wings," Knopf said.

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

carahsoft.

Carahsoft
14993 Sunset Hills Road, Suite 100
Reston, VA 20190
Contact: **Seamus Bergen**

- (703) 230-7425
- DevSecOps@carahsoft.com
- Carahsoft.com/solve/devsecops
- Facebook.com/Carahsoft
- Linkedin.com/company/Carahsoft
- @Carahsoft