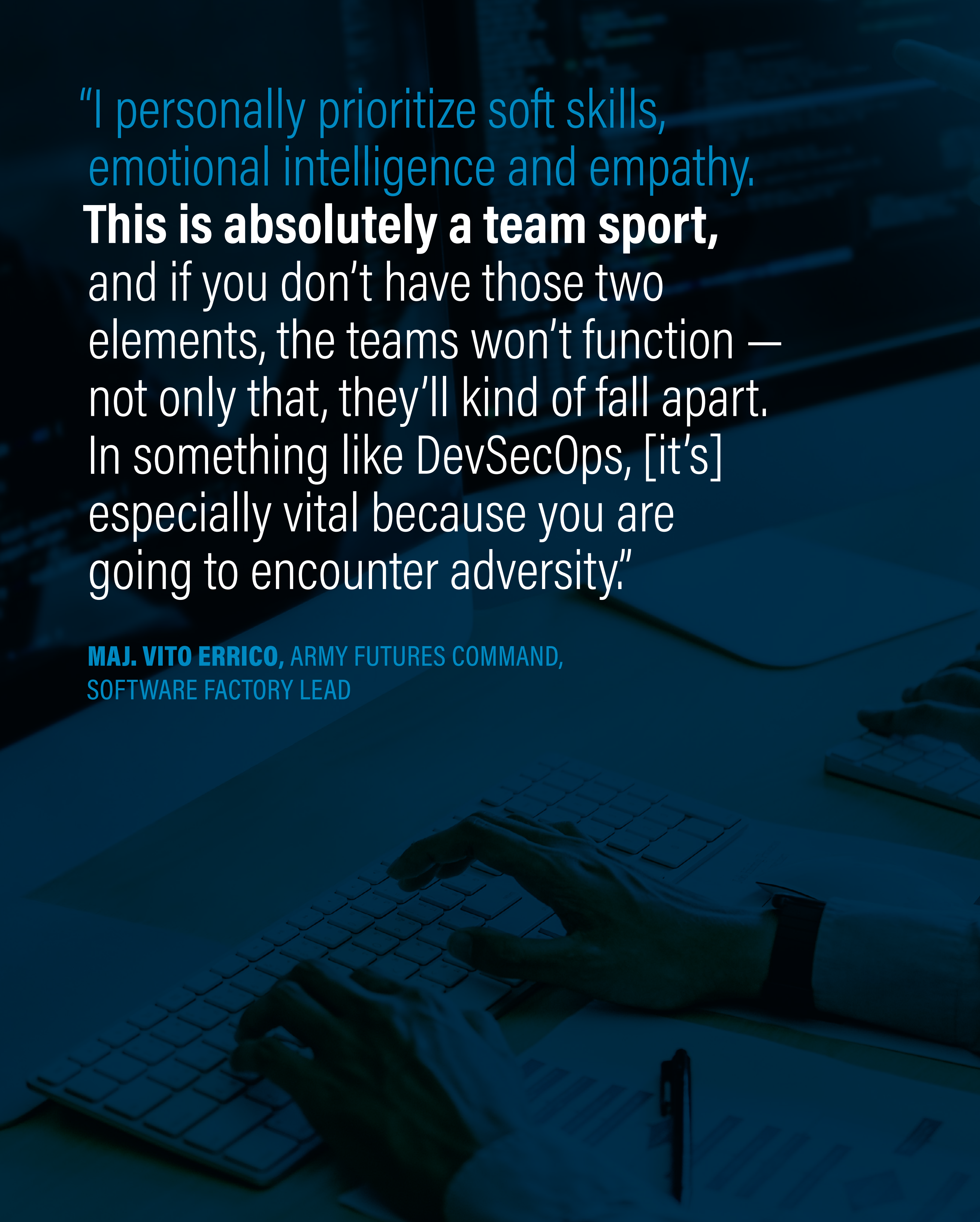
# Agencies Build Foundation for DevSecOps Success

carahsoft.

govloop



“I personally prioritize soft skills, emotional intelligence and empathy. **This is absolutely a team sport,** and if you don’t have those two elements, the teams won’t function — not only that, they’ll kind of fall apart. In something like DevSecOps, [it’s] especially vital because you are going to encounter adversity.”

**MAJ. VITO ERRICO,** ARMY FUTURES COMMAND, SOFTWARE FACTORY LEAD

# Contents

*Carahsoft and GovLoop have partnered to provide resources around the latest federal, state and local DevSecOps initiatives and legislation. The goal is to guide government leaders and stakeholders interested in learning more about improving their software strategies.*

# Executive Summary

Before the advent of the internet, personal computers were first standalone devices. Later, they were tied together in well-defined but closed networks. If there were software bugs, the software applications would have to be updated and replaced — time-consuming and frustrating, but self-contained.

The big change came with the internet. Computers could suddenly communicate with computers outside their dedicated networks, but opening up those networks created an opportunity for hostile parties, something that had not been a problem before — which meant IT development had never accounted for it.

Ever since, IT professionals have been in an "arms race" with bad actors, whether they are simply greedy, corporate spies or attackers from hostile nations.

Nothing really changed in creating the software. Software developers wrote lines of code to execute particular tasks; the bigger and more complex the software got, the more bugs would creep in. In return, the bad actors, became more sophisticated at identifying errors and vulnerabilities in the software that they could exploit.

When those vulnerabilities were discovered — usually after an attack — network operators would pull the software and return it to the developers for patching. The developers would do their best, but shoehorning security features into existing code is both inefficient and often likely to introduce new vulnerabilities someplace else, creating a vicious cycle.

**DevOps — a term combining "development" and "operations" — emerged as a way to restructure the development process by bringing developers and operations teams together to create new applications.**

But security still needed a seat at the table. It is its own IT discipline, with individuals trained in spotting and stopping emerging vulnerabilities, security issues and exploits. **Thus, the newest approach is DevSecOps — both a software engineering approach and a culture that promotes security automation and monitoring throughout the application development lifecycle.**

DevSecOps' primary goal is to break down barriers to collaboration among development, operations and security teams so they all can contribute to creating new applications. Organizations can deploy new apps with secure, efficient, functioning code — but with security as the foundation.

GovLoop and Carahsoft created this guide to provide insight into how to make DevSecOps a reality. The guide discusses the pillars of a DevSecOps strategy, highlights best practices and features interviews with thought leaders on this important topic.

# At a Glance: DevSecOps in Government

## DOD LEADS THE WAY

DevSecOps is gaining a foothold across federal, state and local agencies, but its biggest foothold is in the Defense Department (DoD). The department has long recognized that its existing acquisition and procurement policies and procedures are ill-adapted to the rapidly changing IT landscape. The pace of technological change has accelerated to the point that by the time requirements are drafted, reviewed, revised and released to industry, they verge on obsolete. Although this is true of all IT acquisition, the penetration of software into every aspect of military systems means that the risk of obsolescence is encroaching on everything from weapons to ships and aircraft.

It is not surprising that DoD would embrace DevSecOps. Its model of continuous testing, integration and delivery is seen as the optimal way to deliver capabilities to warfighters as quickly as possible. By definition, DoD focuses on national security and defense. In military parlance, DevSecOps "shifts left" the integration of security; the earlier in app development that security is incorporated, the better — a sound military practice.

It is important to recognize that effective DevSecOps brings about changes not just in app delivery, but in the myriad ways agencies conduct their operations. In February 2019, DoD's Defense Acquisition University (DAU) held a Day of Cyber DevSecOps Academy, because it represents a radically different approach to software acquisition. DAU's presentation noted that "long cycle times between deliveries and manual, error-prone build times…may be measured in weeks, months or even years."

## DEFENSE BOARD HIGHLIGHTS DEVSECOPS BENEFITS

In May, the Defense Innovation Board released its Software Acquisition and Practices Study. The study recommended "the ten most important things to do (starting now!)." They included changes that Congress and the Office of the Secretary of Defense (OSD) needed to carry out, focusing on reworked statutes, regulations and processes for software.

The study included a collection of vignettes, akin to case studies, describing the problems in traditional software acquisition and identifying and quantifying the benefits of DevSecOps. In one, the Joint Improvised-Threat Defeat Organization provided data on some of the tangible benefits of DevSecOps when compared to legacy software development, among them:

- **Lead Time Reduction** (from the start of a development cycle — new code — to deployment)
  - Legacy: 169.83 days
  - DevSecOps: 12 days
  - 93% reduction
- **Deployment Frequency** (delivering new code to customers)
  - Legacy: 11 releases
  - DevSecOps: 98 releases
  - 891% increase
- **Mean Time to Provision** (the average time it takes to add additional services to an environment)
  - Legacy: six months
  - DevSecOps: two hours
  - 99.79% reduction
- **Mean Time to Recovery** (the average time from deployment failure to recovery)
  - Legacy: 15.5 minutes
  - DevSecOps: four minutes
  - 74% reduction
- **Change in operating costs** based on use of open source tooling vs. legacy commercial technologies-dependent architecture
  - Legacy: $1.8 million
  - DevSecOps: $150K
  - 91.66% reduction

Other vignettes, however, outlined the manpower and cultural challenges that implementing DevSecOps poses to the DoD environment.

*This section continues on page 8 »*

# Embracing Machine Identity Management

## An interview with Eddie Glenn, Senior Product Marketing Manager, Venafi

One of the advantages of modern IT services is that they leverage both physical machines (computers and other devices) and virtual machines (e.g., applications, containers and code) to exchange data and execute tasks without human intervention.

That makes it possible to design services that are fast, flexible and reliable. But it also raises an important security question: ***How do you know whether those machines can be trusted?***

That's a question of identity management. Just as humans use passwords, Personal Identity Verification and Common Access Cards to identify themselves, machines use cryptographic keys and digital certificates to identify themselves during a transaction. Just like passwords, those machine identities can be compromised or left to expire. Agencies need to put in place policies, processes and technology to manage that risk.

**"In this digital transformation era where machines create machines, an automated machine identity management program is critical to the delivery, availability and efficiency of any DevSecOps team,"** said Eddie Glenn, Senior Product Marketing Manager at Venafi, which provides solutions for protecting machine identities.

## THREE AREAS OF RISK

Glenn highlighted four key risks associated with machine identities:

- Expired digital certificates can lead to system outages that can bring down critical infrastructure.
- Expired certificates can also lead to system failures, which can be exploited by hackers. According to the Government Accountability Office, an expired certificate played a role in the 2017 data breach at Equifax.
- Unmanaged, unknown and unprotected machine identities might be based on weak cryptographic algorithms, or could be obtained by bad actors to breach systems and access classified or sensitive data.
- Hackers can leverage unprotected keys and certificates to gain access to systems, install and execute malicious code, or remove sensitive data—all without raising an alarm. This is how WikiLeaks is believed to have stolen documents from the CIA in 2017.

## THE KEY PIECE: AUTOMATION

As agencies look to accelerate application delivery, these security and operational challenges increase. DevSecOps—the integration of the development, security and operations teams—is essential. But the DevSecOps team will struggle to keep up with the mounting number of machine identities without the benefit of automation.

"As government adoption of DevOps increases, there are numerous lessons to take away in terms of automating legacy processes that have many slow and manual interventions detrimental to the success of DevSecOps," Glenn said.

Glenn suggested agencies follow four best practices:

- Make it as easy as possible by providing access to machine identity management-as-a-service.
- Integrate machine identity management into tools that DevSecOps teams already use or want to use.
- Maintain visibility of all machine identities, tracking both upcoming expirations and associated risks.
- Enforce machine identity policies consistently, so that teams can request machine identities without needing to worry about which certificate authority to use, which encryption strength is adequate and so on.

Venafi's Trust Protection Platform helps federal agencies manage and secure their machine identities. Using the Venafi Platform, agencies can efficiently orchestrate the entire machine identity lifecycle, keeping communications between machines secure and private.

## GSA'S GOVERNANCE MODEL

The General Services Administration (GSA) has seen a growing number of its team leveraging DevSecOps. To ensure consistent use of good security practices, GSA has developed a governance model, with the Office of the Chief Information Security Officer's DevSecOps Program (ODP) providing agencywide leadership. The governance model has four components:

### Roles and Responsibilities

While noting that well-defined roles and responsibilities are imperative for cross-functional DevSecOps teams, GSA also recognizes the need for agility. With that in mind, GSA recommends the review of roles and responsibilities across the DevSecOps teams before each engagement on a project.

### Security/DevSecOps Engineer

The ODP Security/DevSecOps Engineer serves as the overall security subject matter expert/champion for the assigned system.

### DevSecOps Application Team

The DevSecOps Application Team, which includes integrated security engineers, provides the day-to-day operations of all the aspects of the system and/or application, including development, security and operations.

### System Owner

The system owner provides overall ownership of a system/product/application, including security and compliance.

## COLORADO GOES ALL IN

Colorado is one of the states at the forefront of DevSecOps, launching an initiative in 2019. The project was a finalist for the National Association of State Chief Information Officers' (NASCIO) State IT Recognition Awards.

The initiative, called the Azure DevOps MVP Implementation, focused on "procuring and configuring the Azure DevOps toolset to create a secured single repository for all Colorado state code with an automated, continuous integration and continuous delivery (CI/CD) template," according to the state's award nomination. Four principles guided the program:

- Risk and errors are reduced by injecting quality, security and standards upfront to make each step more consistent and repeatable.
- Changes are broken into smaller increments that make them easier to track, verify, roll back and troubleshoot.
- Faster feedback loops and delivery enable greater alignment with business objectives.
- Increased collaboration and cohesion among the Governor's Office of IT teams, with more time spent innovating and building new solutions, leads to increased employee satisfaction and engagement.

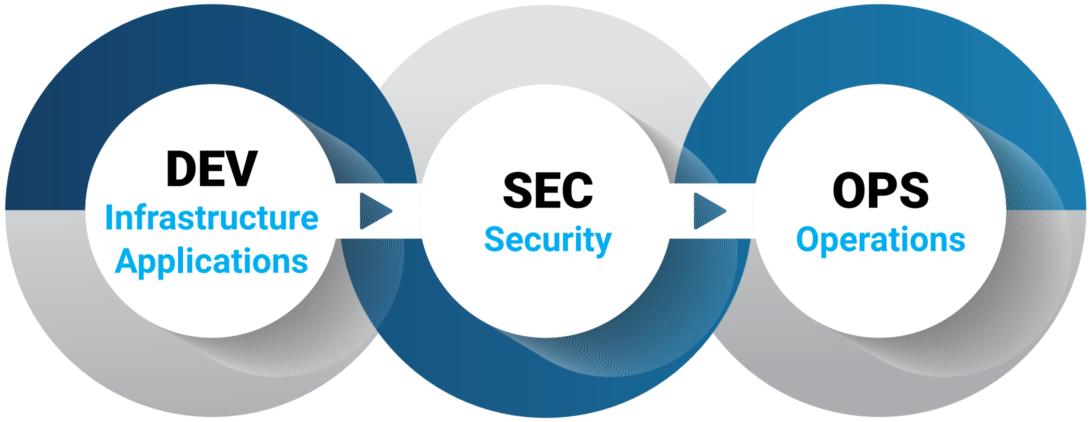
## AN ABUNDANCE OF DEVSECOPS GUIDANCE

Across DoD, organizations have been documenting best practices and guidelines designed to bring consistency to DevSecOps operations. Although aimed at defense organizations, they offer a wealth of insight to any agency looking to get started on DevSecOps. Here are some highlights:

- In September 2019, the department issued its DoD Enterprise DevSecOps Reference Design, which provides both implementation and operational guidance to IT capability providers, consumers, application teams and authorizing officials.
- DoD issued Version 1.0 of its OSD DevSecOps Best Practice Guide in January 2020, including identifying metrics that should be collected on an ongoing basis — "essentially anything that can be monitored should be monitored."
- In April 2020, the Department of the Navy released its Agile and DevSecOps Design Concepts, looking to "bridge traditional gaps between IT and security while ensuring fast, safe delivery of capabilities to the fleet."

# NS2 Secure Cloud
## Secure Innovation Pipeline

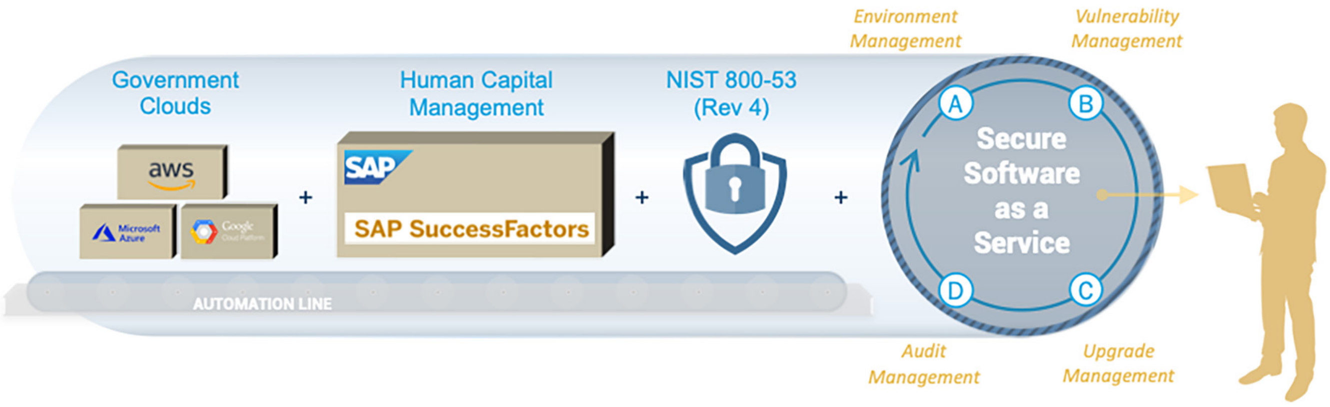
Our most valuable deliverable is not just secure innovation – it's the pace at which we deliver innovation to a secure community.



DEV
Infrastructure
Applications

SEC
Security

OPS
Operations



Government Clouds

+

Human Capital Management

+

NIST 800-53 (Rev 4)

+

Secure Software as a Service

Environment Management

Vulnerability Management

Audit Management

Upgrade Management

AUTOMATION LINE

Learn more **sapns2.com/cloud/**

SAP NS2 NATIONAL SECURITY SERVICES CLOUD

# The Playbook for Innovating Quickly, Expansively and Securely

## An interview with Dean Pianta, Cloud Director, SAP NS2

Playbooks are familiar territory for sports teams and agencies alike. As basketball teams have trotted out motion – instead of isolation – offenses, agencies have taken a page of the same principle: that all parts of IT should be moving in unison.

The old waterfall approach had different parts of the software process working in isolation. First went development, then security and finally operations. Flaws were tossed back to be resolved, and a major incongruence often relegated the product back to square one. The process took a while.

The viability of that approach has trickled off, especially now as agencies use the cloud to promote high-speed innovation and maintain competitiveness with top tech. Agencies prefer DevSecOps as a software motion offense approach that has development, security and operations players all working together simultaneously. DevSecOps is comparatively breakneck.

"The traditional software process can't keep pace with the event of innovation," said Dean Pianta, Cloud Director at SAP NS2, which uses DevSecOps to drive secure innovation.

In an interview with GovLoop, Pianta explained how DevSecOps improves speed, scale and security.

## SPEED

Government adoption times can be taken for granted – people aren't surprised when something takes three years to build or 12 months to implement. Those are common refrains that often go unquestioned. They shouldn't, Pianta said.

Cloud changed the game by allowing agencies to spin up networks instantaneously. And that was just the beginning. Throw in microservices architectures and agile development methods that have security and operations built in; now you're getting down the court, faster than before.

"What used to take six to 12 months can be done in six seconds," Pianta said.

## SCALE

With development, security and operations players all working together, the door is opened to large-scale automation. The application assembly line is geared up with the digital equivalence of conveyor belts, robotic arms and sensors. Identical to Henry Ford's first moving assembly for mass production of an entire automobile, costs are reduced and mass scale is achieved.

"The beautiful thing about code is that it can be part of an automation cycle. And now that everything is code, it can all be scripted," Pianta said.

Many times, the same application needs to be reproduced – with minimal or no alterations – to work in multiple environments. Automation-driven software factories usher applications along in no time, from commercial to government markets. Software engineers can then turn their attention to innovation, not replication.

## SECURITY

Of course, none of that matters if security isn't up to scratch. But just like development, implementation and monitoring, security can be embedded into the assembly line.

Security protocols are activated as soon as applications are. Those protocols make sure that if something happens, servers don't falter. The breach can be stopped at the source.

The biggest risk to agencies is seeing security and innovation at odds. The right industry partner doesn't do that. Rather, they attach security to cutting-edge technology to enable innovation securely.

**"My goal is to make sure that no one protecting the country is using 10-year-old software,"** Pianta said.

# DevSecOps Drives Change at the Air Force

## An interview with Nicolas Chaillan, Air Force, Chief Software Officer and Head of Platform One

Nicolas Chaillan is the head of the highest-visibility DevSecOps initiative in all of DoD, and one of its foremost champions. “It’s the only way to build software in 2020. Doing it without DevSecOps is, to me, borderline criminal,” Chaillan said.

He has led Platform One — the internally developed, centralized DevSecOps program that coordinates 15 software factories nationwide, with each providing DevSecOps services to one or more programs, weapons systems and/or commands — since its inception. In addition, the Office of the DoD CIO earlier this year formally designated Platform One as an Enterprise Service Provider for DevSecOps for the military.

Chaillan said the biggest advantage to DevSecOps over other development methods is that it bakes security in — it cannot be bypassed, ignored or treated as an afterthought — and that means the software and capabilities are secure and can’t be stolen by other nation-states.

“We learn the normal behavior of the system. If you see the system doing things it’s never done before, [the built-in security measures] will kill the bad action going on,” he said. “Having that trust, detecting malicious behavior and a zero-trust implementation — we never had [that] before.”

## A NEED FOR NEW TALENTS

The overarching drawback to DevSecOps is that the need is so vast.

**"The No. 1 thing that I've learned [about DevSecOps] is that self-learning is the only way to scale,"** Chaillan said. "We have to train about 100,000 people this year. So we need to have a self-learning environment — that's really foundational."

Chaillan pointed out that today he believes people must constantly reinvent themselves. Technology innovation is advancing so rapidly, workers must continuously refresh their skills. "Without that capability, you just become obsolete," he said.

There is an upside to that, he said: Because all the technology is pretty new, anyone interested in advancing in the field doesn't need a decade of experience, just a couple of years and a willingness to keep learning. To facilitate that process, team members spend an hour a day learning on the platform and tracking all things happening in the field of DevSecOps.

"We grow them internally and rotate them…embed them into our programs and spread the good stuff across their teams," Chaillan explained. "Obviously, not everyone will become [an] expert overnight, but they have to understand the importance" of DevSecOps.

Platform One is partnering with the Linux Foundation and the Cloud Native Computing Foundation to provide access to a learning hub. "It's not just for DevSecOps, but for AI, machine learning.… It comes with a cloud [simulation] box so they learn by doing," he said. "There are so many who on the side or at home have great skills already."

One big gap he sees in government today is people who understand how to architect software in cloud-native environments. Other areas where skills are needed include decoupling, open architecture of systems, containerization and site reliability engineering.

"All these new titles that come out of Google — they're expensive talent, but also critical talent," he said.

## LONG-TERM CHANGES

Another challenge is how to change the culture at government agencies that are not used to major shifts in culture and may actually be averse to it. DoD is still full of silos, he said in October 2020 during Amazon Web Services' National Security Series.

"It goes down to even like basic partnerships.… We have so many silos and that's really part of the reason as to why we cannot really scale things, and why we reinvent the wheel and why we don't do very well with enterprise services," Chaillan said.

Another part of the culture that needs changing? "Hiring. How do we change policy?" he said. There is an executive order waiving requirements for college degrees, but agencies don't make use of it. "We probably lose 30% of the talent we could get. We have direct-hire authority, but many teams don't know how to use it."

Those who would focus on the cost of changing to a DevSecOps approach are shortsighted, he said. "We're saving 12 to 18 months out of every five years" of a program," Chaillan said. "Just from the taxpayer standpoint, without a rapid feedback loop with the user on the quality of the software you're building, that ends up causing delays. The shorter you can make that feedback loop, the more cost-effective it is."

He offered advice for other federal agencies that want to start a DevSecOps program: Make the upfront investment in the platform and make it broadly available, but "in a particularly large agency, have a central office to bring everything back to the enterprise stack. **You don't want 20 teams all building the same capability. You want [team options], but not too many. You're really investing in the central team, and then centralizing the talent into that team."**

Red Hat | carahsoft

# DevSecOps Powers Public Sector Innovation

Learn more at redhat.com/gov

Stream the Red Hat Podcast to learn more about the impact of DevSecOps in the Public Sector.

Check out the Red Hat Infographic to learn more about continuous improvement and integrated security – at scale.

Download the Red Hat Market Trends Report to learn more about how agencies can implement a working DevSecOps culture.

# How Developers Can Become a Security Asset

### An interview with Michael Ducy, Cloud Native Transformation Specialist, Red Hat

For agencies to realize the full benefits of DevSecOps, they need to apply the DevOps tenet of continuous delivery both to software and security.

This is a big change from a traditional development environment in which security typically operates as a separate function that is brought into play at key points in the development lifecycle. In that model, security also is seen as a drag on the development process and an obstacle to innovation.

Agencies can avoid those pitfalls by fully incorporating security into the DevOps process and, more importantly, into the daily workflow of their developers.

To learn more about this, GovLoop spoke with Michael Ducy, Cloud Native Transformation Specialist at Red Hat. He discussed three ways in which agencies can reduce risk and improve compliance while also driving innovation.

## LET DEVELOPERS DRIVE INNOVATION

When it comes to security, IT experts often talk about the importance of "shifting left," that is, addressing security earlier in the development lifecycle. But it's not just security that shifts left with DevOps.

In traditional IT environments, developers were expected to adhere to a detailed IT architecture, which was updated periodically. To take advantage of today's rapid rate of innovation in technologies and architectural approaches, agencies need to give developers more leeway to decide what languages, toolsets and capabilities they might need to build an application, said Ducy.

"Keeping the state of innovation at the development level is very important, because it helps you further down the line, as you're trying to reach your customer, or your user, in this new digital world," he said.

## LET DEVELOPERS DRIVE SECURITY

Because the DevOps environment is so dynamic, security can keep up only if it is fully integrated into the day-to-day work of developers.

It comes down to continuous delivery. As developers download libraries, JavaScript packages and other tools, they need to ensure that they are running the necessary checks on risk and compliance. Security needs to become just another gate in the continuous delivery process.

In this environment, the role of the security team plays more of a consulting role, helping developers understand security requirements “so that they can make better choices in the future as they go through this more modern way of working," Ducy said.

## ESTABLISH A TRUSTED SOFTWARE SUPPLY CHAIN

Integrating security into the development process provides the foundation for building what Red Hat calls a trusted software supply chain (TSSC).

With a TSSC, all stakeholders can be confident that security, compliance and privacy requirements are addressed throughout the software development lifecycle. Such trust is essential to accelerating a program's ability to achieve authority to operate.

A lot of pieces need to come together to build a TSSC, and it won't be easy if agencies take a piecemeal approach, said Ducy. **"With the Red Hat OpenShift Container Platform, we provide a complete holistic solution that enables you to build a trusted software supply chain rapidly and to onboard new teams quickly to start working in this way,"** he said.

# The DevSecOps Playbook: 5 Tactics for Success

Moving to a DevSecOps environment, no matter how necessary or desirable, is a daunting prospect, especially in government agencies where it seems as if every process and procedure — financial, hiring, documentation, etc. — was designed to hamper fast action. This can be especially challenging with DevSecOps because it's not just a matter of making an organizational or even a policy change. For many organizations, moving to DevSecOps involves a culture shift that changes everything about how they conduct business and deploy software.

In this section are some tactics that have proven to be crucial for successfully implementing DevSecOps in a government environment. Depending on the agency and its mission, some may be of greater significance than others, but each can be customized and all will be important when making such a substantial and important change.

## 1. TREAT DEVSECOPS AS A CULTURE, NOT JUST A PROGRAM.

There are several aspects to this. For decades, security was an afterthought, bolted on or added when a vulnerability was identified — frequently long after it was discovered, leaving the system at risk until a patch could be implemented. For instance, the massive data breach at the U.S. Postal Service (USPS) in 2018 came when the personal data of a staggering 60 million customers was exposed through a critical security vulnerability, even though the susceptibility had been discovered and disclosed to USPS a year earlier.

**The entire government agency must embrace the idea that security is paramount, from political appointees all the way through every branch, office and bureau.** And that includes developers and operations teams, too. Even though they may just be getting comfortable with working together using DevOps to get apps into users' hands faster, the teams have to make room at the table for their security professionals — and they have to listen to them.

Functions within the agency must identify how their processes can help, rather than hinder, DevSecOps. For instance, acquisition professionals need to rethink their contracting approach to software. DevSecOps pioneers such as Platform One within the Air Force are providing guidance and models for this.

Human resources (HR) functions have a major role to play, too. Agencies already face hiring obstacles because of pay differentials between the government and the private sector, and rigid "paper qualifications" such as a college degree or X number of years of work experience. Defense Innovation Board vignettes include the story of a high school student who won a "white hat hacking" competition and wanted to intern at the Pentagon, but it ultimately took intervention from the highest levels to get HR to act.

## 2. CULTIVATE A TEAM MINDSET THROUGH HIRING AND TRAINING.

Remaking the culture leads naturally to the next element — finding ways to identify, hire and continually refresh the skills of DevSecOps team members.

DevSecOps evangelists in the government, such as Chaillan, talk about having to "look under every rock" for prospective team members. They make use of the commercial job sites, such as LinkedIn and Indeed.com, run hacking competitions, ask current employees to refer their friends, and so on.

The best — or at least most reliable — source of new team members is internal. Maj. Vito Errico, the Army Futures Command (AFC) lead for its Software Factory, said it is crucial that recruits into DevSecOps understand the DoD environment and the Army. "Different entities have different rules about risk management frameworks," he said. "I want to make sure they understand the ins and outs of our particular organization."

Reinforcing the connection between culture and recruitment, Errico noted that soldiers typically serve two years in an assignment, then rotate out. "That's one of the things we're trying to fix about how the military leverages technology," he said. "Our goal is to get them working for us for three years, then continue" a working relationship with them when they move on.

These are all critical parts of building DevSecOps teams, but one remaining element may be the most important: finding team members with the "soft skills" to work effectively on those teams.

Christopher Crist, chief of DevOps at U.S. Transportation Command, said he looks for prospective team members with high emotional intelligence (EQ). He identified five components of EQ: self-awareness, self-regulation, motivation, empathy and social skills. "Empathy, or at a minimum sympathy, is important because we should understand and really feel the pain our customers are going through," he said.

Errico made a similar point. **"I personally prioritize soft skills, emotional intelligence and empathy," he said. "This is absolutely a team sport, and if you don't have those two elements, the teams won't function — not only that, they'll kind of fall apart. In something like DevSecOps [it's] especially vital, because you are going to encounter adversity."**

## 3. USE SECURITY AUTOMATION AND MONITORING THROUGHOUT THE DEVELOPMENT LIFECYCLE.

The DoD Enterprise DevSecOps Initiative clearly spells this out: "The main characteristic of DevSecOps is to automate, monitor and apply security at all phases of the software lifecycle: plan, develop, build, test, release, deliver, deploy, operate and monitor."

Automation, which streamlines testing, monitoring and remediation, also facilitates collaboration because different teams can be present during those steps.

GitLab, for instance, automates the CI/CD pipeline, with features such as Auto DevOps, which takes care of manual configuration work like security auditing and vulnerability testing.

In the context of DevSecOps, continuous testing should cover everything, including the front and back ends, application programming interfaces (APIs), databases and passive security. And "continuous" also refers to delivery, version control, monitoring and remediation.

**You measure what you value — and you value what you measure.** GSA's Tech Guide titled "Building a DevSecOps Culture — From a Technical Perspective" identifies several key metrics for continuous development, threat detection and release cycles, such as measuring deployment frequency; lead time; detection of threats, security defects and flaws; mean time to repair; and mean time to recovery. Automation and monitoring of these metrics show the progress being made, areas that need to be addressed and expanded opportunities.

## 4. BUILD TOOLS SUITES FOR THE TASKS AT HAND.

**Many free, open source tools are available for the DevSecOps environment.** For instance, Google's Kubernetes is an open source system to automate deployment, scaling and management of containerized applications and workloads, including sidecar containerization to provide isolation and encapsulation. Git is a free, open source distributed version control system. There are monitoring and container analysis tools, many of them free, along with repositories such as GitHub to facilitate storing and collaborating on software while maintaining version control.

In addition, companies such as Red Hat and Microsoft Azure offer soup-to-nuts tool kits, and myriad smaller companies have specific tools that might suit government requirements.

## 5. START SMALL AND SCALE UP.

The single biggest decision when preparing to implement DevSecOps is, oddly, making sure to start small.

This is, in part, because agencies are unlikely to have a large number of employees with both the soft and hard skills needed to take on a vast project. **A new DevSecOps team should not be set up to fail by being asked to empty the ocean with a teaspoon.**

It also reflects the reality that cultural change is hard, takes time and needs to have successes on which to build.

Getting an initial success provides proof of concept to users and managers who might be skeptical of the DevSecOps concept. It also provides the opportunity to work out how team members can best collaborate for success.

For instance, Platform One recently achieved a high-visibility DevSecOps success when it transmitted upgrades to the Air Force's U-2 spy plane — while it was flying. This actually provides two proofs of concept: that delivering new capabilities while an aircraft is aloft can be done without jeopardizing the craft and crew, and that DevSecOps can deliver value even to older assets. The U-2 first flew in 1955.

Chaillan, at Platform One, estimated that the program will need to train 100,000 team members throughout DoD — 60,000 in areas such as software architecture, and 40,000 to take more advanced technical training — per year. But the groundwork must be laid for all those DevSecOps teams to be successful, in the broadest sense of the word.

Scaling the toolkits is the easy part, at least if the DevSecOps team makes use of the many free, open source tools that are available.

CONTRAST
SECURITY

# EMPOWERING DEVSECOPS FOR FEDERAL AGENCIES

## PURPOSE-BUILT FOR FEDERAL SCALE

Designed for modern software by continuously monitoring and detecting from within software regardless of where the application runs.

## NO COMPROMISES: HIGHEST SECURITY AT DEVOPS SPEED

Eliminates application security tool soup with observability that reveals the complete application surface using patented instrumentation.

## UNMATCHED SCALABILITY WITH NO EXPERTISE REQUIRED

Fully distributed and continuously assessing tens of thousands of applications and APIs in parallel delivers code 10x faster at lower cost.

eBOOK

CONTRAST SECURITY

FEDERAL AGENCIES MUST TRANSITION TO INSTRUMENTATION-BASED APPLICATION SECURITY

DOWNLOAD NOW

WHITEPAPER

CONTRAST SECURITY

OUTDATED APPLICATION SECURITY TOOLS PUT FEDERAL AGENCIES AT RISK

WHITE PAPER

DOWNLOAD NOW

## CONTRAST CERTIFICATIONS

GENERAL SERVICES ADMINISTRATION

SEWP V

NIST 800-53 COMPLIANT

DOD PLATFORM ONE

IRON BANK - DOD CENTRALIZED ARTIFACTS REPOSITORY (DCAR)

AICPA SOC2 TYPE II

# Enabling Agencies to Succeed with DevSecOps

### An interview with Jeff Williams, Co-Founder and CTO, Contrast Security

As agencies adopt a DevOps methodology, they need to adapt their approach to application security. It's not just about "shifting left," it's about approaching security with a DevOps mindset.

The traditional approach to application security relies on several different types of scanning, a penetration test and then an application firewall. None of these techniques were very accurate and relied heavily on experts to manage the process and clean up the results.

Software development velocity increased dramatically with Agile and DevOps. These code updates are put through an automated build pipeline that typically runs in a fraction of an hour. There's simply no way to run legacy scans, triage false positives, deduplicate findings, rate risks and give feedback to developers during a build pipeline that must finish in 15 minutes.

Application security can't succeed unless it's compatible with the way that people are building software, said Jeff Williams, Co-Founder and Chief Technology Officer at Contrast Security, which provides a unified platform for web application and application programming interfaces (API) security observability including security testing, open source security and runtime protection.

Williams discussed three keys to embedding security into DevOps operations.

## GET A UNIFIED PICTURE THROUGH INSTRUMENTATION

Agencies have responded to the increased complexity of modern application development by buying more tools—one tool for scanning custom code, one for open-source libraries, yet another for APIs, and so on.

The result, said Williams, is "tool soup," which provides a lot of data but not a unified picture. In contrast, instrumentation automatically embeds sensors within applications and APIs to monitor for vulnerabilities at every stage of the development life cycle. This creates a real-time, holistic view of application security across an entire agency application portfolio.

## GIVE FEEDBACK DIRECTLY TO DEVELOPERS

Instrumentation provides benefits both to the application security team and to developers. For the application security team, the tool soup approach often results in so much data, and so many false positives, that they have a difficult time gleaning intelligence from it. The unified picture provided by an instrumentation platform eliminates the noise so that the team can identify and remediate problems quickly.

Instrumentation can also provide accurate feedback directly to developers, so that they can fix vulnerabilities as part of their normal work. "Ultimately, that allows you to use the big machinery of software development to drive application security, as opposed to having a siloed team of experts," Williams said.

## BUILD ON A PLATFORM

Rather than adopting the tool soup approach, you can use an integrated application security platform based on software instrumentation to provide vulnerability testing, open-source analysis and runtime protection. By minimizing the need for application security experts in the critical path, this approach enables teams to deliver software into production at high velocity without compromising security.

The Contrast Application Security Platform enables agencies to ensure compliance with key security regulations, including the National Institute of Standards and Technology's 800-53 Cybersecurity Framework. The platform also has been accepted into Platform One, the Defense Department's approved application portal.

"We've seen tremendous increases in the rate at which organizations are fixing vulnerabilities," Williams said. "Instead of just building up a giant backlog of vulnerabilities, they are actually fixing them."

# Army Futures Command Makes DevSecOps a Long-Term Priority

### An interview with Maj. Vito Errico, Army Futures Command, Software Factory Lead

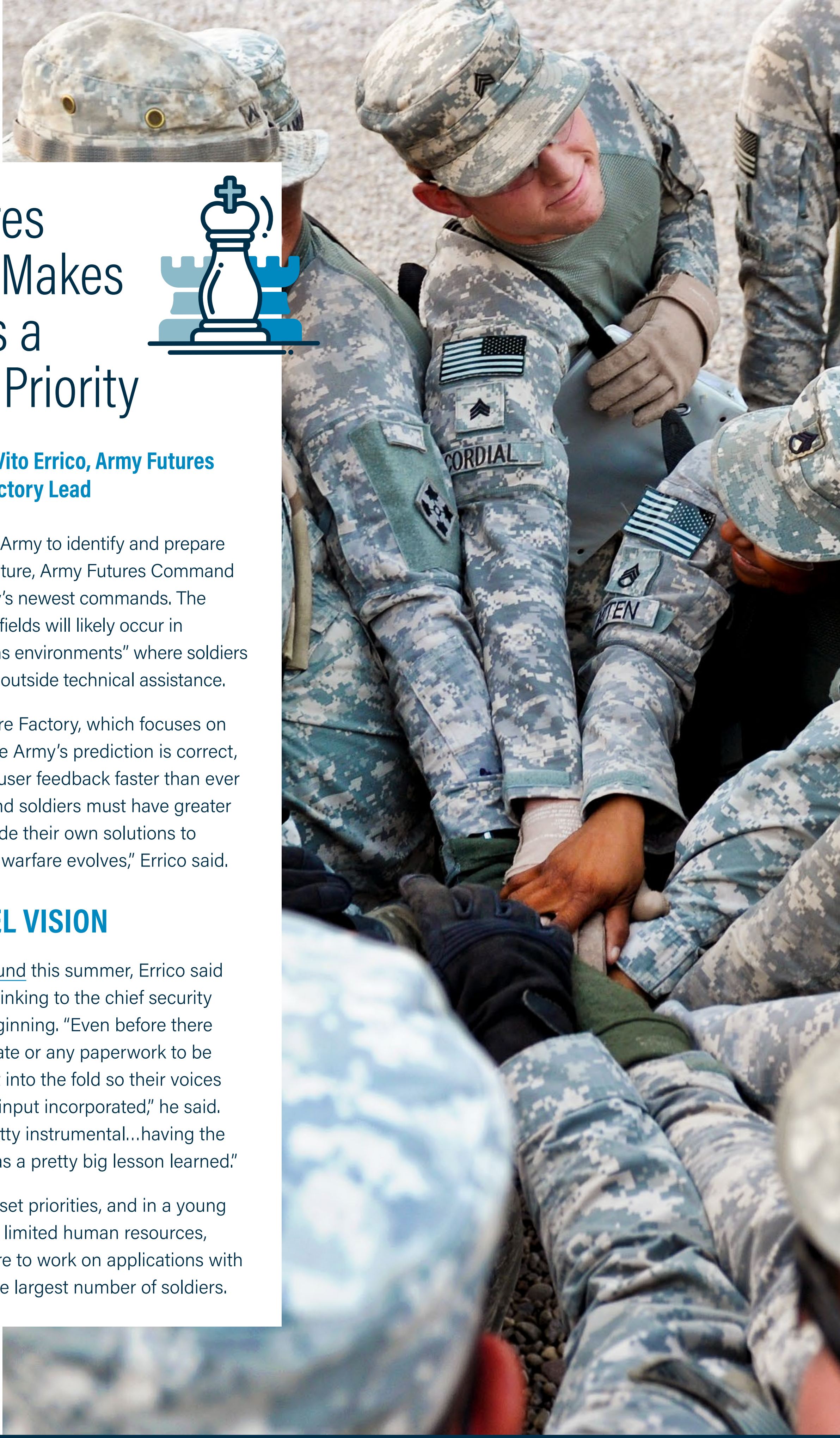
Established in 2018 by the Army to identify and prepare for the battlefields of the future, Army Futures Command (AFC) is one of the military's newest commands. The Army believes those battlefields will likely occur in "contested communications environments" where soldiers may be unable to draw on outside technical assistance.

Errico leads AFC's Software Factory, which focuses on DevSecOps, because if the Army's prediction is correct, "the Army must integrate user feedback faster than ever to field better solutions, and soldiers must have greater ability to diagnose and code their own solutions to problems 'on the edge' as warfare evolves," Errico said.

## AVOIDING TUNNEL VISION

In getting AFC off the ground this summer, Errico said the program started with linking to the chief security professionals from the beginning. "Even before there was any authority to operate or any paperwork to be signed, they were brought into the fold so their voices would be heard and their input incorporated," he said. "That turned out to be pretty instrumental…having the leadership buy-in. That was a pretty big lesson learned."

There is always a need to set priorities, and in a young organization like this, with limited human resources, Errico said the priorities are to work on applications with the widest user groups, the largest number of soldiers.



He said it is not easy to incorporate automation and monitoring into a constantly changing environment.

“I don’t think it’s easy for anyone on a federal budget,” he said. “We stay tied in to multiple entities both inside and outside the government, so we don’t get tunnel vision.” The Software Factory makes use of third-party technologies and tools so the internal DevSecOps teams can concentrate on the 20% of apps that are critical.

## GROWING CAPABILITIES FROM WITHIN

Like his counterpart at the Air Force’s Program One, Errico believes the government needs to grow its DevSecOps capabilities internally.

“There’s got to be a balance,” he said. “You’ve got to have your people exposed to both [internal and external resources], invest in the outside stuff when that makes sense…. We’ll grow capabilities from within because of the essentiality” of particular software.

The difficulty of attracting outside talent with the necessary skill sets also drives the need to develop internal resources, Errico said.

## AN INTENSE HIRING PROCESS

Joining the Software Factory takes effort, Errico said.

“We speak to the candidates, check references [in] a full 360-degree reach,” he said. “It comes at a great time cost. But if you believe people are the most important asset, that 360-degree interview process — which means not just the candidate but also the candidate’s frontline colleagues — that gives us a pretty clear picture of how someone can or can’t work well with others.”

That in-depth understanding of potential candidates is a critical part of making sure they bring a team mindset to their roles.

“Leadership has to foster an atmosphere that conveys true trust, autonomy and bestows responsibility to every member of the team,” he said. “Every team member needs to be treated exactly the same, every team member has to demonstrate respect for one another and leadership has to make sure the organization’s successes are shared across the entire team. Sometimes leadership gets so busy that it can forget to let subordinates know the big picture.”

Once a candidate makes the team, Errico says AFC invests “pretty heavily” in third-party education on an ongoing basis. “When we bring on somebody, they get education as part of their onboarding experience,” he said. “That initial exposure needs to be much more robust. Leadership needs to be prepared to make these investments in people; [it’s] the only way to truly modernize for the foreseeable future.”

## FOCUS ON CONTINUED INVESTMENT

For agencies thinking of starting DevSecOps programs, Errico has advice: “Spend time conducting industry analysis of use cases both inside and outside the federal space. This is very much an emerging technology, and you have to figure out the right way it will fit for your organization. That takes time and thoughtful, honest analysis.”

Once the commitment is made and a DevSecOps program is in place, he said, comes the challenge of maintaining — and expanding — cultural change.

**“Continued investment is vital. Commitment to being a learning organization is also a must,”** Errico said. “Organizations will likely struggle to streamline resourcing until operations are underway for a while. Seniors should commit to that fact early because the investment is worth it. Second, the organization as a whole must operate as an ever-learning team, since you won’t get it right for a while. That’s natural and part of the process.”

# DevSecOps Teams Require a Robust Orchestration Platform

### An interview with Gee Chow, Senior DevOps Solution Engineer, F5

Although DevSecOps has the potential to unify work across teams while reducing the time to develop and deploy applications, that's not a guarantee, as many agencies have discovered.

The challenge is that the automation and orchestration capabilities that agencies initially adopt might not be robust enough as DevSecOps efforts scale up. The result? Teams abandon the tools and resort to manual processes, reducing their gains in speed and agility – which, of course, defeats the whole point.

To learn more about how agencies can avoid these pitfalls, GovLoop spoke with Gee Chow, Senior DevOps Solution Engineer at F5. Chow suggested three ways that agencies can develop an automation and orchestration strategy that will serve their needs over the long haul.

## BUILD A PLATFORM THAT WORKS FOR EVERYONE

Individual teams tend to pick tools that meet their particular needs. As they transition to a DevSecOps environment, however, they should build a platform that addresses common requirements across all teams involved. That includes role-based security, a strong user interface and a monitoring and analytics module.

One key consideration is the application data plane, which plays an especially important role in managing communications in a container environment. Teams often select a lightweight data plane component, because it is quick to configure and deploy. But that ease of use "is only half the picture," Chow said. "The other half is the ability to configure or orchestrate it centrally."

## TAKE AN API-CENTRIC APPROACH

Application programming interfaces (APIs) are essential to automating a DevSecOps pipeline, providing a quick and easy way to draw on reusable assets when developing new applications.

But as applications grow increasingly complex with the use of microservices and containers, API management grows increasingly complex as well. The DevSecOps platform needs to be robust enough to adapt to a wide variety of requirements – and to make it all manageable for developers, Chow said.

## MAKE COLLABORATION THE FIRST PRIORITY

DevSecOps, by definition, is intended to promote collaboration among the development, security and operations team. But Chow emphasized that such collaboration needs to begin at the outset of a project, when defining the goals and strategy for a project.

The idea is to define the overarching goal or mission of the project, then have each team prioritize their own needs and goals as it relates to that mission, said Chow. Those secondary goals become the building blocks for the strategy and shapes the development and orchestration of the application pipeline, he said.

F5's NGINX Application Platform is a suite of products designed to meet these needs. It includes NGINX Plus for load balancing and application delivery; WAF for security; and NGINX Unit for running applications. The platform is monitored and managed by NGINX Controller.

**"NGINX gives our customers a self-service, API-driven platform that integrates easily with their continuous integration/continuous delivery workflows,**" he said. "And it's all for the purpose of making app lifecycles both faster and more secure."

# U.S. Transportation Command Cultivates a Team Mindset

## An interview with Christopher Crist, Chief of DevOps, U.S. Transportation Command

Unlike Platform One or the Software Factory, the DevSecOps program at U.S. Transportation Command is embedded in a unified, functional combatant command that provides support to the other 10 U.S. combatant commands, the military services, defense agencies and other government organizations.

That means it serves many kinds of military organizations, providing strategic mobility capability through its own vast infrastructure of people, information systems, trucks, aircrafts, ships, trains and railcars.

It also means the command may consider itself a transportation organization or a strategic logistics organization, but it doesn't necessarily view software as an essential element of its mission in the way the services do, for instance.

"We have thousands and thousands of IT employees, [in] 77 different programs," Crist said. "Everything is siloed. So that means our primary purpose is to educate others, but that also means lots of collaboration all across the command."

## INTERPERSONAL SKILLS PROVE KEY

Like his peers, Crist said getting the right mix of skills among team members is a real challenge. “Hard skills, the technology skills, can be important. We’re a very large organization, very robust,” he said. “It’s the interpersonal skill set that’s most important to me. It’s very important that I get people who can explain the complexity of DevSecOps to everyone. For example, the iPhone is very intuitive for users, but there’s a lot of very complex stuff going on behind the screen.”

The siloed nature of the organization and its more rigid culture means that getting DevSecOps team members with soft skills is difficult, but even more important, Crist said.

“I was a CIO in the private sector before. I could interview the way I wanted, I could make a hire on the spot,” he said. “In the government we don’t have the same power.… We’re at the mercy of USAJobs. I don’t think this system lends itself to getting the best. [In the hiring process] we don’t even talk about hard skills. We ask, how do you communicate a complex problem, or what kind of challenge you’ve overcome in working with a team.”

To facilitate a team mindset, Crist said he spends at least half his time with his team every week. **“People who empathize need empathy, too,”** he said. “The way I view my job is to [provide it.] Other branch chiefs [evaluate] on technical ability. I have one-on-one conversations with my team members multiple times a week — often just checking in: How are you doing? Often they’re frustrated; they feel like they’re dealing with people who don’t value us. [I’m] consistently reminding them of their purpose and that it’s normal to have friction.”

## BALANCING SECURITY AND RISK

Because the command is so sprawling and siloed, Crist said the biggest challenge in actually implementing DevSecOps is too much top-down security. “It really slows down the pipeline with the number of control gates,” he said. “We’re looking at ways to maybe accept a little more risk.”

He admires Platform One’s ability to accept more risk and move faster, which he attributes to the program being started from a blank sheet. At the command, security is much more top-down.

For example, the command  had pushed to force all its developers into the gov cloud environment, Crist said. “It’s just a nightmare. They go to [bridge domain interfaces], go through us, then they’re within our boundary, which means we have to maintain it, maintain all the tools. It’s just way too much.”

Crist said it was the security professionals who suggested they look at Git as the source of truth. “Source of truth is becoming the industry standard — the source code repository becomes the source of truth repository…whether Gitlab or Jenkins or any of the big players,” he said.

## A PROMISING FUTURE

Despite the challenges of trying to change a well-established culture, Crist is enthusiastic about what DevSecOps can achieve.

“It’s a fantastic thing to finally bring developers together with operations teams and customers, but once they started moving faster they realized security was missing,” he said. “Getting security involved meant it was there from the beginning, pushing it as far left as possible.”

He sees DevSecOps as absolutely essential for DoD programs that require faster and wider deployment.

**“The only resource constraint is the human resource for it. It’s hard to get experts, but all the main tools are free.** You can get your hardware together, get into the cloud, which might cost a little bit of money,” Crist said. “The most respect I have for leaders is for those who help to change that [budget program] mindset.… We still have programs out there that say they’re bound by their contracts [after] we spend months helping them adjust the contract language.”

# Change Management for the DevSecOps era

**Stream** the Atlassian podcast episode to learn DevOps Transformation Tips.

**View** the datasheet on Jira Service Management and how it helps increase flow from Dev to Ops.

**Download** the 2020 DevOps Trend Survey to learn what companies doing DevOps successfully have in common.

Learn more at carahsoft.com/atlassian

# How Culture Drives DevSecOps Success

## An interview with Ken Urban, Public Sector Evangelist, Atlassian

Atlassian, which provides a wide range of software development and collaboration tools, has an important message for agencies looking to build DevSecOps initiatives: Don't just think about the tools.

“In general, there are three pillars of DevSecOps: people, process and technology,” said Ken Urban, Public Sector Evangelist at Atlassian.

"We can build the processes, and we can implement the technology pretty easily," he said. "But in reality, none of that actually matters if nobody’s using it.  You can’t force people to change their mindset."

That is why Atlassian says culture is the number one success factor in DevSecOps.

**"A healthy DevSecOps culture will not only change the way people think about security, but it will also promote good communication and collaboration,"** Urban said. "It will show you how successful you can be if you work together as a team."

Urban identified four key attributes of a good DevSecOps culture.

## 1. EFFECTIVE COMMUNICATIONS

“When people talk about DevSecOps, they often focus on improving communications between developers and the security team. But organizations need to foster open and transparent communications at every layer of management, from the top down,” Urban said.

In particular, developers can benefit from understanding how their work fits into the larger mission – and why particular security constraints are important.

“Good healthy communication means staying as open and transparent as you can be without compromising that security,” he said.

## 2. EFFORTLESS COLLABORATION

In the same manner, collaboration needs to extend beyond any one DevSecOps team, because no project is the result of just one team's efforts. Urban points to the space program in the 1960s as an example.

The effort to land Apollo 11 on the moon "was more than just one team at NASA –  it was the entire agency working together to solve a problem. In fact, it included many teams across industry and academia as well," Urban said.

"Now, if you take that and you look at DevSecOps, can you succeed if you don’t include security or compliance in your collaboration? Probably not," he said.

## 3. SECURE FLEXIBILITY

In DevSecOps, developers always need to be ready to change directions quickly and easily. But agencies can only create an open and flexible DevSecOps environment if their tools are open and flexible.

“That flexibility needs to be provided in the context of good security,” Urban said. “For example, with the Jira suite, you can create cross-team collaboration and still configure the tools to maintain a high degree of security roles, retaining autonomy and flexibility for your team,” he said.

## 4. SEAMLESS INTEGRATION

“Agencies must think about how their application development and project management tools support the culture they want to develop,” he said. “In particular, to support communications and collaboration, they need to select tools that integrate seamlessly.”

Atlassian’s suite of products allows for seamless integrations as well as deep integrations with other tools for release, monitoring, deployment, automation and alerting.

"What you want to do is look at what tools are going to accelerate your transformation and improve the pace of development – and help you develop more secure code," Urban said.

# Best Practices in DevSecOps

## As agencies get more experience with DevSecOps, essential principles have begun to emerge. They include:

☑ **Treat security as a shared responsibility.** Successful DevSecOps teams recognize that security is the responsibility of all team members, not just the security professionals on the team. Not everyone needs to be an expert, but they need to buy into the security objectives.

☑ **Enlist leaders to support cultural change.** Since DevSecOps requires that kind of transformational change, it means getting support from the top of the agency. Key steps — such as developing a comprehensive plan, educating developers, and ensuring cooperation among IT, security, and business teams — depend on leaders' support. And when there is a leadership change, educate the newcomers and earn their commitment.

☑ **Starting small provides room to fail, adapt, learn and grow.** Although Platform One is a very visible success story for the Air Force, DevSecOps started with a single specific project, laying the groundwork for the expansion to come.

☑ **Use automation as much as possible.** Security is essential, but the goal remains to speed up development and deployment times. Automation can do both for software development through tools such as dynamic application security testing, static application security testing and automated configuration. By embedding security controls early in the process, automation can ensure the consistency and reliability of testing and secure coding in a CI/CD deployment environment.

☑ **Teach security as part of the DevSecOps team's ongoing training and skills improvement.** In addition to building team rapport, it helps educate programmers on secure coding practices, which in turn builds team chemistry and further speeds the process.

☑ **Test everything.** Continuous security testing is an essential element of DevSecOps, but it has to apply to everything, including the front and back ends, units, APIs, databases and passive security. Threats exist across a spectrum of techniques and tactics, so security testing has to match.

☑ **Tailor tools to the job at hand.** The suite of tools to be used should be tailored specifically to the job at hand and understood and used by all the team members equally: developers, operations teams and security experts.

☑ **Adapt continuously.** One fundamental lesson in IT operations is that there never is a finish line. Change is the only constant, so agencies need flexible policies and processes that can adapt quickly to changed circumstances.

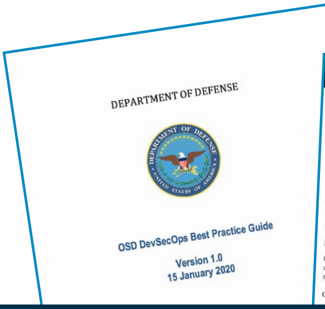
☑ **Plan on building to scale.** Agencies with DevSecOps initiatives need to work with a cloud platform that enables that scalability.

☑ **Emphasize transparency.** At a micro-cultural level, the most successful DevSecOps teams are transparent with one another, understanding each team's core functions, strengths and limitations. And they play to those strengths.

## DOD’S 4 BEST PRACTICES

DoD released its OSD DevSecOps Best Practice Guide in January 2020. At the 30,000-foot level, it identifies four broad best practices. They include:

- Shifting the culture, including building organizational buy-in and creating a “shift left” mentality. This creates a checks-and-balances system of increased touchpoints among the disciplines earlier in the development lifecycle.
- Automation of manual processes, including continuous integration, monitoring and defining metrics as the source of DevSecOps’ value proposition.
- Infrastructure as code — having a scripted and version-controlled infrastructure — provides consistency, repeatability, reviewability and verifiable environments.
- Pitfalls and bad practices to avoid, such as overemphasis of pipeline tools and vendor lock-in, or becoming dependent on an entire suite of tools from a single vendor and creating obstacles if a single service needs to be replaced, risking a break in functionality.



DEPARTMENT OF DEFENSE

OSD DevSecOps Best Practice Guide

Version 1.0
15 January 2020

GSA Tech Guides

All guides » DevSecOps guides

DevSecOps Guide

Standard DevSecOps Platform Framework

Goal: Safer Software Sooner

The following document describes, at a high-level, the expectations, scope of responsibilities, maturity model, and metrics associated GSA.

Baseline Definitions

**DevSecOps:** A cultural and engineering practice that breaks down barriers and opens collaboration between development, security, an using automation to focus on rapid, frequent delivery of secure infrastructure and software to production. It encompasses intake to rele those flows predictably, transparently, and with minimal human intervention/effort.

Common Expectations

## THE DEVSECOPS MINDSET

Transportation Command’s Crist offered his own five recommendations, with an emphasis on coming at DevSecOps with the right mindset:

- Don’t wait; it looks complicated, but start doing the research.
- Realize you’re not alone; reach out to agencies that have already implemented DevSecOps and ask for help. That could be Crist’s office, Platform One, AFC or the Department of Veterans Affairs.
- Don’t reinvent the wheel (another reason to ask for help).
- Recognize that cultural change is harder than program changes.
- You need at least one person whose sole job is pushing the commitment to DevSecOps.

## MEASURES OF DEVSECOPS SUCCESS

As part of its DevSecOps Tech Guide, GSA identifies five metrics for assessing DevSecOps performance:

- Deployment frequency
- Lead time
- Detection of threats, security defects and flaws
- Mean time to repair
- Mean time to recovery

# Modern Cloud Security Requires an Agile Approach

As agencies bring more agility to services development and delivery, they risk increasing vulnerability if they don't also take a more agile approach to security.

Doubtless, agencies can benefit from combining cloud native technologies like containerization and microservices with a DevOps methodology to accelerate application delivery by improving collaboration between the development and operations teams.

But that combination creates a constantly shifting IT environment, making it difficult to apply traditional approaches to security and compliance.

To learn how agencies can adapt, GovLoop spoke with cyber experts at Palo Alto Networks, which offers a cloud native security platform called Prisma Cloud. They recommended three steps.

## SHIFT AS FAR LEFT AS POSSIBLE

Security must be integrated with development. That is, it needs to be addressed in the earliest development stages, not just as a final check before deployment. Moreover, in modern cloud environments, organizations must shift as far left as possible to keep up with the pace of innovation.

"You need to apply security evenly across the entire software development lifecycle: build, deploy and run," said Matt Chiodi, Chief Security Officer, Public Cloud at Palo Alto Networks.

Agencies must monitor the entire development pipeline to ensure it remains compliant with their security policies, even as applications and services evolve.

## LEVERAGE AUTOMATION

The task of monitoring the pipeline grows more challenging as DevOps accelerates the pace of development and cloud native increases the complexity of the environment.

Traditionally, developers worked months or even years on building a monolithic application. Now they break such applications into countless microservices, creating a greater attack surface for the security team to defend.

"The only way security can keep up with that pace is through automation," Chiodi said.

Automation can be used for everything from monitoring server and endpoint posture to detecting, assessing and responding to threats.

## MOVE TO CONTINUOUS ATO

Automation also paves the way to change how agencies approve IT systems for use. In a standard Authority to Operate (ATO) process, a system owner must implement, certify and maintain required security controls. The problem is that certification is based on a snapshot in time, whereas in modern cloud environments, change is constant. Systems can "drift" from compliance over time as new threats arise.

Modern cloud solutions offer architectures leveraging containers that perform discrete tasks within a microservice environment and are in constant flux with application updates, vulnerabilities/threats, policies, etc. “The challenge for any organization implementing microservices is the ability to monitor, identify and address issues in a timeframe that has the least amount of risk exposure,” said Paul Fox, Senior Product Manager at Palo Alto Networks.

Prisma Cloud enables agencies to utilize their existing staff to secure, monitor and protect multiple cloud service provider services without mastering multiple security tools. It has reduced alert volume and configuration errors for many organizations, allowing IT and security operations to spend their time more productively. With support for every major compliance framework, Prisma Cloud enables IT to monitor compliance posture and generate audit-ready reports with a single click.

**“Your security workforce needs visibility into your full cloud environment, with the ability to enforce compliance with security controls and policies, and we do that across multiple cloud service providers,”** said Fox.

# Conclusion

IT has always confronted two intractable problems: The risk of bad actors exploiting vulnerable code will increase, and costs will remain high as agencies try to backfill security into existing solutions.

Moving to a DevSecOps model addresses both of those critical problems. While shifting security solutions to the left may introduce fractional slowdown in developing and releasing new and improved functionality, it's ultimately miniscule compared to the impact of a breach and the scramble to recover.

At the same time, implementing DevSecOps helps everyone. Developers save time by having less code sent back after deployment. Operations teams can focus on system improvements, and security professionals can stop obsessing over patch management and concentrate on guarding against advanced threats that have yet to be seen. The ultimate winner will be end users, who get safer applications faster.

## About Carahsoft

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider®. As a top-performing GSA Schedule, SEWP and ITES-SW2 contract holder, Carahsoft serves as the Master Government Aggregator® for many of its best-of-breed technology vendors, supporting an extensive ecosystem of manufacturers, value-added resellers, system integrators and consulting partners committed to helping government agencies select and implement the best solution at the best possible value.

Visit www.carahsoft.com, follow @Carahsoft, or email sales@carahsoft.com for more information.

## Thank You

Thank you to Atlassian, Contrast Security, F5, Palo Alto Networks, Red Hat, SAP NS2 and Venafi for their support of this valuable resource for public sector professionals.

## About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector. For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop

## Author

Patience Wait, Contributing Writer

## Designer

Kaitlyn Baker, Creative Manager

carahsoft.

# Carahsoft represents and delivers the most proven, innovative solutions needed for every phase of the DevSecOps life cycle.

Tune in to Carahsoft's webinar series featuring the industry's leading DevSecOps solutions providers.

Watch The Series Now

## Sponsors

anchore
ATLASSIAN
aws
CloudBees.
f5
FIREEYE
GitLab
HashiCorp
MICRO FOCUS Government Solutions
Microsoft
paloalto NETWORKS
Red Hat
splunk>
sonatype
vmware

carahsoft.

Carahsoft's DevSecOps solutions are available through its reseller partners on a variety of contracts including Carahsoft's GSA Schedule 70, SEWP V, ITES-SW2, NASPO ValuePoint, NCPA, OMNIA Partners and numerous state and local contracts.

Learn more at Carahsoft.com/DevSecOps.

See the latest innovations in government IT from Carahsoft's vendor partners at Carahsoft.com/Innovation.

govloop

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop