FEDERAL NEWS NETWORK

EXPERT EDITION

DevSecOps

Insights on Digital Modernization from:

- Air Force
- Navy
- Army
- Centers for Medicare and Medicaid Services
- National Geospatial-Intelligence Agency

BROUGHT TO YOU BY: carahsoft

Count on Carahsoft® and Our Partners for DevSecOps Solutions

DevSecOps is an approach to software development where security is integrated at every stage of the lifecycle. Continuous software improvement and automated security integration are established at scale, through collaboration between developers and system administrators. DevSecOps solutions provide agencies with fast and secure software releases, enabling superior delivery for mission-critical operations.

Carahsoft and its partners deliver DevSecOps tools to government agencies, guaranteeing innovative solutions with security built into every phase of the DevOps lifecycle. These solutions support collaborative planning, rapid code builds, iterative testing, rapid release, optimized deployment and monitoring that continuously feeds into the development pipeline. The result delivers a powerful advantage for government agencies who are undergoing digital transformation including faster and more secure releases, greater interoperability and the freedom to focus on their missions.

anchore	ATLASSIAN	CloudBees.	NowSecure™	sonatype
aws	BeyondTrust	ca technologies	CONTRAST SECURITY	f5
FIREEYE™	GitLab	GOLDFINGER HOLDINGS	Google Cloud	HashiCorp
Jama software®	McAfee™	MICRO FOCUS	Microsoft	New Relic.
NUTANIX™	paloalto® NETWORKS	puppet	RAPID7	Red Hat
SAP NS2 NATIONAL SECURITY SERVICES	splunk>	TREND MICRO™	Tricentis™	vmware®

Carahsoft DevSecOps solutions are available through its reseller partners on a variety of contracts including GSA MAS, SEWP V, ITES-SW2 and numerous state and local contracts.

To learn more, contact the Carahsoft DevSecOps Team at **(703) 871-8629** or **DevSecOps@Carahsoft.com**; or visit **carahsoft.com/DevSecOps**

carahsoft® The Trusted Government IT Solutions Provider®

TABLE OF CONTENTS

The trend across civilian and defense agencies when it comes to software development is clear. People and culture matter the most when changing the way an agency develops software.

The Army Software Factory is training soldiers and civilians through a new six-month intensive classroom training effort that leads into a 2.5 year hands-on DevSecOps skilling program.

The Navy and the Air Force have similar programs with an eye toward trying to change the risk aversion that tends to be institutionalized into many servicemembers early on in their career.

"Whereas controlled and smart risk taking and smart failure, if you will, there's a way to learn quickly. But I would say most organizations talk about that, but aren't really willing to actually do it," said Austen Bryan, the chief operating officer of the Air Force's Platform One. "So I think, looking at how we recruit and retain and develop people that understand the skillset is really where the biggest fundamental problems are for the DoD, at least right now."

Even with reskilling and training employees, agencies still aren't guaranteed success in using DevSecOps. Many agencies need to become more comfortable with automating the security controls as well as change the way these projects are funded.

But what this e-book demonstrates is just how far agencies have come and where they still need to go to take fully advantage of DevSecOps to drive modern capabilities to their customers.

Jason Miller
Executive Editor
Federal News Network

What one small software factory is doing for Air Force's DevSecOps

BY SCOTT MAUCIONE

When the United States evacuated from Afghanistan, the Air Force relied heavily on its computer systems to schedule flights, figure out logistics and map routes.

Kessel Run, one of the Air Force's software factories, had a lot of its software involved in the evacuation and the programs were being surged to capacity.

The Air Force's software engineers needed to move fast, and using DevSecOps they responded quickly to kinks and bugs in the software.

"By having a lot of these DevSecOps processes as our natural way of working on a day-to-day basis, we were able to quickly react," Sushil Kumar, director of engineering at Kessel Run told Federal News Network in an interview. "We deployed some new fixes and some changes on the backend to be able to ensure that these activities that are happening in real time could continue to at a much larger scale and be done in an optimal manner."

Experiences like that are just one of the many reasons the Air Force, and Defense Department as a whole, are embracing DevSecOps for nearly all of their software. Innovative and agile organizations like Kessel Run are leading the way.

"By having a lot of these DevSecOps processes as our natural way of working on a day-to-day basis, we were able to quickly react. We deployed some new fixes and some changes on the backend to be able to ensure that these activities that are happening in real time could continue to at a much larger scale and be done in an optimal manner."

— SUSHIL KUMAR, DIRECTOR OF ENGINEERING, KESSEL RUN, AIR FORCE

Gradual movement into a large storm

Kumar said the Air Force is currently at an inflection point when it comes to moving away from traditional waterfall-type software releases and moving toward iterative DevSecOps updates.

"There's a lot of scrutiny on how is this working, and looking at all the results that we've been able to demonstrate and show there's a general switch in terms of ways of thinking, starting with the topmost level, to adopting this across the board," Kumar said.

He said that there will be a gradual movement that will turn into a large storm of adopting DevSecOps in the Air Force as a whole.

Acquisition process still a challenge

The momentum comes with challenges, though. Kumar said there are still hang-ups rooted in the way the military works and old ways of thinking.

One of the biggest issues is the defense acquisition process, which is not made for the speedy cyber world. Kumar said if the Air Force can't field iterative updates fast enough because it's stuck in contracting limbo, then programs will not be able to adapt.

> **"I see huge opportunities where they could leverage a lot more automation in the process, whether it be developing software, whether it be testing it, whether it be deploying it and so on"**
>
> — **SUSHIL KUMAR, DIRECTOR OF ENGINEERING, KESSEL RUN, AIR FORCE**

DoD is working on this after getting some help from Congress. In the past few years, Congress has given DoD the authority to put software in its own faster acquisition process and allocate money specifically for software.

Kumar said other issues revolve around simply changing the culture of thinking in the military about updates and getting rid of legacy systems.

"I wouldn't say these are easy things to tackle and address in a short period of time but, there is a lot of activity related to making those changes," he said. "There are people at various levels within the organization that are very aware and conscious of what changes need to happen and are helping influence and make those changes."

What could come out on the other end of a service that focuses on agility and embraces DevSecOps is something that can make work easier for humans and make programs more beneficial.

"I see huge opportunities where they could leverage a lot more automation in the process, whether it be developing software, whether it be testing it, whether it be deploying it and so on," Kumar said. "There are a lot more opportunities for adopting things like artificial intelligence and human-machine teaming to figure out better ways to adopt AI models based on the data that we collect. As we build and mature a lot of this process to be more proactive we will start seeing trends in our security vulnerabilities. These patterns give us some early indicators. We can adopt our process to be able to quickly react to those and make sure that we're addressing those as we continue to build and deploy software."

Applying DevOps principles to achieve software supply chain security

THIS CONTENT HAS BEEN PROVIDED BY CLOUDBEES

Prakash Sethuraman, chief information security officer, CloudBees

CloudBees.

A recent survey sponsored by CloudBees showed that software supply chain security is top of mind for many senior executives right now. The problem is a general lack of clarity on what to do about it. A recent executive order from President Joe Biden's administration charges several agencies, including the National Institute of Standards and Technology, with releasing guidance around this very issue. NIST's preliminary guidelines were due in early November and not yet released at the time of this article.

But that executive order will have a cascading effect on federal agencies and the contractors who supply them with software. All of these entities are going to need to understand the provenance of the components in their entire supply chain, which will make visibility into their software delivery processes increasingly important. In order to create something like a software bill of materials, they're going to need to wrap their hands around the entire process.

"The current philosophy, and it's been like this for a couple of years now, is to shift security left. Which on the one hand makes sense, because the sooner you can catch problems, the better off everything's going to be," said Prakash Sethuraman, chief information security officer for CloudBees. "But that's placed a huge burden on developers to know and understand what secure and compliant is. But they're not security folks. Security and compliance teams, they've got to try to train developers how to use their tools. And then they also have to figure out how to write that code into all these different tools and keep it current."

The problem is software supply chain security is too big a problem to leave to any one group. It has to become everyone's responsibility. So rather than just shifting security left, in order to truly secure the supply chain and meet the requirements laid out in the EO, agencies and contractors need to go beyond that paradigm and begin thinking in terms of shifting security and compliance everywhere. So how do they do that?

Sethuraman said CloudBees approaches this by applying DevOps principles to the software supply chain through a three-pronged concept: secure in development, secure in delivery and secure in production.

"No one else in the DevOps space is thinking and talking about this triad," Sethuraman said. "One of the problems with DevSecOps is that first off, I believe the 'Sec' is silent; if you're doing it correctly, it's not a separate thing. It's an integral aspect of everything that you do because you've built these controls in. This triad is a lens to view how you apply those things to what's going on. It's getting more into the pragmatic aspects of how we do DevSecOps."

The secure in development part of this triad refers to the code. There are a number of things that have to be done to ensure the code is clean, including verifying that the right tools and libraries are being used.

Secure in delivery refers to the people, the processes, and the controls. It means the right people need to have eyes on it at the right time, and the right controls and processes need to be observed in the approval process.

"There's a concept in software delivery called drift. And this is where a lot of organizations get caught out: Something changes as it goes through the pipeline. And that change isn't detected," Sethuraman said. "So you have to make sure that only immutable, approved objects and components are used for delivering that software, and that if change does occur, it gets detected and stopped, or approved by somebody. And the data and the evidence for that approval should also be attached to that decision."

The final part of the triad – secure in production – is essentially a nod to the fact that these days it's a guarantee that at some point in the future some vulnerability or issue will arise that needs to be addressed immediately. Mean-time-to-detect and mean-time-to-repair are often held up as metrics by which an organization can assess its performance in responding to vulnerabilities. But there's a gap between those two, between when a vulnerability is detected and when it's fixed, when the organization is exposed.

That's why it's important to have systems in place to immediately mitigate that risk. For example, a feature flag can instantly disable a function that's discovered to be compromised, closing that vulnerability so it can't be exploited before it's fixed. Alternately, with the right controls in place, it's possible to do an automated rollback if necessary. It's a question of being able to respond instantly, not necessarily repair instantly, because it will take time to discover what went wrong. But being able to mitigate that risk immediately gives organizations the luxury of time in which to do that.

"The old story about security being the 'Department of No,' or the 'Release Prevention Department' is not relevant in the age of DevOps," Sethuraman said. "Because if you're doing it right, security's built in. You've got the receipts, you've got the evidence there. So you can go faster, securely."

CloudBees®

Compliance, visibility, speed, and so much more - with CloudBees

Build security and compliance into every step of the software supply chain, featuring:

- Continuous Compliance
- Continuous Integration / Continuous Delivery
- Release Orchestration
- Feature Flag Management

Secure and compliant from code commit through production at 5X the speed.

LEARN MORE

cloudbees.com/use-case/streamline-governance-compliance

Navy focuses on people, culture in standing up DevSecOps software factory

BY DAVE THORNTON

While DevSecOps is a philosophy that revolves around delivering software faster, implementation is more about the people than it is about the technology itself. That's why, at the Naval Surface Warfare Center, they're standing up a software factory built on "five pillars … all tied ultimately to the people and the culture," according to Candaice Deloach, senior scientific technical manager for warfare systems software science and technology and development at the NSWC's Dahlgren Division.

"So we think about things like how do we train our software workforce? We think about things like how do we govern data and shift the culture in terms of tagging at the source code level? We think about how do we engage with people from a metrics perspective? And how does enabling automation help them, and then also training in terms of teaching how to study and interpret those metrics," Deloach said during a recent ATARC Defense Department DevSecOps webinar. "So all those things, every pillar that we focus on, it's all tied back to how do we train? How do we motivate? How do we encourage? And how do we build momentum from the ground up?"

That training component is important, because DoD has a training blind spot when it comes to DevSecOps, and software in general, according to Austen Bryan, chief operating officer of the Air Force's Platform One. He said the military trains people to command, which tends to skew towards zero risk acceptance, and policies that facilitate that mindset. That ultimately leads to slowdowns.

Cultural resistance still a roadblock

"Whereas controlled and smart risk taking and smart failure, if you will, there's a way to learn quickly. But I would say most organizations talk about that, but aren't really willing to actually do it," Bryan said. "So I think, looking at how we recruit and retain and develop people that understand the skillset is really where the biggest fundamental problems are for the DoD, at least right now."

"So we think about things like how do we train our software workforce? We think about things like how do we govern data and shift the culture in terms of tagging at the source code level? We think about how do we engage with people from a metrics perspective? And how does enabling automation help them, and then also training in terms of teaching how to study and interpret those metrics"

— CANDAICE DELOACH, SR SCIENTIFIC TECHNICAL MANAGER FOR WARFARE SYSTEMS SOFTWARE SCIENCE AND TECHNOLOGY AND DEVELOPMENT, DAHLGREN DIVISION, NSWC

"I want people, and especially those that I'm working directly with, I want them to be comfortable with being uncomfortable," she said. "If you're comfortable in what you're doing, if you're comfortable with what you're executing, then I'd say you're not on the right track. We should be uncomfortable with the amount of change that we're taking on, we should be uncomfortable with how we continue to shift."

— CANDAICE DELOACH, SR SCIENTIFIC TECHNICAL MANAGER FOR WARFARE SYSTEMS SOFTWARE SCIENCE AND TECHNOLOGY AND DEVELOPMENT, DAHLGREN DIVISION, NSWC

For example, Bryan said Platform One doesn't do tech roadmaps more than six weeks in advance. It doesn't look for three-year periods of funding. And that tends to run counter to the larger DoD culture. And therein lies a major roadblock: cultural resistance.

Leadership can sometimes be disconnected from the teams trying to implement DevSecOps principles. They can be reluctant to give up the authorities necessary to operate at the speeds required by modern software development. That's why training and culture change needs to happen at the top of an organization just as much as at the bottom.

Deloach said data can be useful in pushing back against this disconnect, and this cultural resistance.

"You have to begin to think about what data can we collect so that we can temper that natural pushback from a cultural perspective of not wanting to move fast, of this idea that we have people that want all the answers up front," she said. "Well, the quickest way to shut down that type of culture and that type of pushback is with data. It's hard to argue with numbers."

Air Force successes

For example, Nicolas Chaillan, former chief software officer for the Air Force, said continuous authority to operate has saved 100-years of planned program time, around 12-18 months per program every five years. And the improved feedback loop due to rapid-paced, incremental changes saves 4-to-12 months of time per program, compounding that 100 years saved.

"I would argue, maybe we didn't save [that time], we just didn't waste it," Chaillan said. "That's something to think about."

But that cultural resistance, especially at the top of the organization, can also be interpreted as a sign of progress, according to Deloach.

"I want people, and especially those that I'm working directly with, I want them to be comfortable with being uncomfortable," she said. "If you're comfortable in what you're doing, if you're comfortable with what you're executing, then I'd say you're not on the right track. We should be uncomfortable with the amount of change that we're taking on, we should be uncomfortable with how we continue to shift. But that means to me that we're on the right track. And I always encourage those around me to think bigger, and to always question what's in the realm of possible."

5 ingredients for successful mobile DevSecOps

THIS CONTENT HAS BEEN PROVIDED BY NOWSECURE

Brian Reed, chief mobility officer, NowSecure

NowSecure

Most IT shops within the federal government are familiar with DevSecOps, but fewer have begun applying those principles to mobile application development. But that's becoming more important for federal agencies, especially those with significant portion of their workforces outside traditional workplaces, such as the military, FBI, FEMA or the Food and Drug Administration. In the field, it's easier for those employees to use a smartphone or tablet than a laptop.

For example, Air Force was tasked with developing a mobile app for parts procurement and repair as part of an effort to modernize A-10 maintenance. It needed a mobile app that could be used by airmen with no specific training. The team used DevSecOps principles to deliver in a matter of weeks what traditionally would have taken 18-24 months to bid out and develop.

But applying DevSecOps principles to mobile app development is somewhat different from web.

"If you think about a web application, it basically runs in any browser on any desktop or device in the world. So in terms of developing and testing it, you really just need to test it once or twice for one or two browsers. And in terms of coding, the browser and server provide a ton of security built in and easy for the developer to use," said Brian Reed, chief mobility officer at NowSecure. "For mobile apps, you have to choose iOS or Android. And if you do both, you have to write it twice, effectively. Unlike web browsers, to build apps for mobile devices, the developer has to understand how the mobile device and operating system works, how secure data storage works, how crypto works, how secure network communications works and a myriad of other security application programming interfaces (APIs)."

That means the mobile app coding and security bar is much higher for both developer knowledge and skills. So how can agencies successfully apply DevSecOps principles to mobile development? Reed said there are five ingredients:

1. **Establish secure-by-design:** Security should partner with the development and architecture teams to ensure security and privacy considerations are built into the requirements of the application.

2. **Upskilling the team:** Ensure both the developers and the quality assurance teams are trained in security so that they're not relying entirely on the security team. "Because if every line of code the developer writes is already secure, that makes delivery faster and testing easier," Reed said.

3. **Deploy DevSecOps tool chain:** This, at a minimum, would include a continuous integration, continuous delivery (CI/CD) platform, a functional testing tool, a security testing tool and an issue tracking to start (though some

teams can have upwards of 30 tools). The CI/CD platform is the backbone that allows many of the workflows to be automated.

4. **Configuring environment to run in continuous testing mode:** This means the mobile application will be continuously security tested in the background while it's being built, testing third party code and internally developed code and generating a software bill of materials (SBOM). This is similar to when doctors have patients wear cardiac monitors, to monitor see what's going on at all times and under varying conditions, so they can act when bad things are found.

5. **Make sure your continuous testing feeds remediation information back to developers:** This allows developers to catch and fix bugs much more quickly. Chances are, if a security bug is found early, it's because the developer actually wrote the bug due to a gap in their security knowledge. Feeding this remediation information with embedded training back to developers allows them to not only fix the issues fast before the mobile app is released, but also helps developers learn at the same time for continuous improvement.

There are a few other mobile-specific differences in the development process to keep an eye on as well. The first is that there are sensors in mobile devices that laptops don't have access to. Mobile apps can take advantage of these to create unique experiences, though extra time will have to be spent ensuring the app interacts appropriately and securely with those sensors. Developers also have to ensure that an app stores and transmits data securely as well. Adversaries have tracked the locations of warfighters via exercise apps like Strava and beer-tasting apps like Untapped in the past due to insecure coding practices, lack of developer understanding and lack of proper security testing.

Second, is testing. Reed said mobile apps are notoriously difficult to test, because they can't be tested in a simulator like browser apps. Mobile apps have to be tested on real devices to ensure interactions with the operating system, network and backend are properly investigated, and today there is technology to continuously automate this security testing.

Finally, developers need to remember that public-facing mobile app development has an extra step in the process: Apps have to be reviewed by Apple or Google before they can be posted in the commercial app stores. Some internal-only agency apps won't need to go through Google or Apple stores, but anything public-facing, like a FEMA disaster app, will need to take this extra step into account when designing their release process and estimating delivery times.

One more thing that can make mobile app development faster and easier for agencies: continuous authority to operate (ATO) or continuous ATO. Some programs – like the Air Force's BESPIN, for example – have evolved to achieve ATO as a process, rather than just ATO approval on individual applications. They've done so by applying many of the best-practices outlined here, in order to achieve highly secure, high-speed operations.

"You've got to make sure you have the right approach in secure-by-design and upskilling, then you have to have the right tools, and then you have to run them the right way, which is continuous mode with developer remediation included," Reed said. "And that's how you get velocity and speed with security built in."

To achieve their mission, intelligence, military and civilian agencies rely on mobile apps and devices.

Secure mobile app vetting, **speed** mobile app deployments & **accelerate** ATO across federal agencies with the **NowSecure Mobile App Supply Chain Solution**.

Army Software Factory more about building skills than apps

BY JASON MILLER

Calling the Army's Software Factory a software factory actually is a misnomer. The service isn't building software. It's building soldiers and civilians' skillsets so they can build software.

Yes, in the end, the Army receives modern application to help the warfighter, but this is not your typical DevSecOps workshop.

Hannah Hunt, the chief product and innovation officer for the Army Software Factory, said her office is focused on upskilling and training soldiers and civilians so they can go back to their units and use these skills to create a cadre of software development experts.

"Every six months, we bring in 30 soldiers and civilians to go through a technology accelerator and gain efficiency and proficiency in product management, user experience and user interface (UI/UX) design, platform engineering and software engineering," Hunt said in an interview with Federal News Network. "From a DevSecOps perspective, you need both the product teams themselves as well as your underlying continuous integration, continuous delivery (CI/CD) pipelines, your platform-as-a-service offering to ensure that those applications that the soldiers are delivering get into the hands of users. We own that entire lifecycle, which makes it really easy for us to quickly iterate and deliver software to our user base."

"Every six months, we bring in 30 soldiers and civilians to go through a technology accelerator and gain efficiency and proficiency in product management, user experience and user interface (UI/UX) design, platform engineering and software engineering."

— **HANNAH HUNT, CHIEF PRODUCT AND INNOVATION OFFICER, ARMY SOFTWARE FACTORY**

After six months of intensive training, the 30 students, who are on a three-year assignment with the software factory, are paired with experienced developers and assigned to a project.

Hunt said the goal is to give these students a basic set of skills and then have them continue to learn by gaining real-life experiences.

"Once they finish their training, they're paired with a Silicon Valley expert, and it's very much a train-the-trainer model. They are sitting day-to-day with the Silicon Valley experts, learning the skills that are needed by your typical Silicon Valley product manager or designer engineer," she said. "Eventually, once they have that level of proficiency, they can start to train other soldiers that come in and subsequent cohorts. It builds a model that is self-sustaining over three-to-five years."

Six month training program

The Army has sent the first cohort through the program, the second set of 30 students will finish that initial six months of training in December and a third group is scheduled to begin training in January. Hunt said the goal is to continue to bring in cohorts every six months for the foreseeable future.

"What's really great about our recruitment and hiring process is we bring in a large, diverse group. We are rank and military occupational specialty (MOS) agnostic, which means you can be in any career field and in any rank as long as you have the right attitude and a willingness to learn," she said. "In cohort one, we have everybody from a private first class up to a captain. In cohort two, we have everybody from a specialist to a major. They also come from a variety of skillsets. We have medics and maintenance technicians that have become platform and software engineers. It's really wonderful to see a very diverse skillset of people that is really an untapped talent in the Army who are interested in doing these things or did them in their spare time and want to be able to use those skills to support their force."

The Army found the program popular from the beginning. Hunt said her office received between 250 and 300 applications per cohort.

She said good candidates aren't necessary those folks who have coding experience or come from the signal intelligence field, but students who demonstrate a level of emotional intelligence and teamwork. Hunt said having that aptitude can make or break a development team.

Projects come from crowdsourcing

The first cohort is working on projects that come from ideas or needs of others units or commands in the Army. Hunt said for the first cohort, the software factory received 30 project submissions. For the second one, they received 80 project ideas so word is getting out about the work the factory is doing.

The first cohort was placed in teams of 10—five students and five experts—or as Hunt called them the two-pizza team model, and are working on five projects.

"They are working on 'This is my squad' initiative through the Sergeant Major of the Army. That application is in production already and they have a user base at Fort Hood," she said. "We are working on an application to improve the mobility common operating picture tour of duty website, which is how reservists and guardsmen apply for active duty jobs. Right now, it's very clunky behind a DoD firewall, and you need a NIPRnet computer in order to access it. We want to make that a little bit more accessible and provide a better user experience. We are working on improving and optimizing the preventative maintenance checks and services checklists and services process, which exists for any unit that needs to do maintenance checks. Right now that's all done on paper. You fill out a form, and somebody has to upload that information to the enterprise system for it to be actually be counted. We want to make that accessible on a soldier's phone and make that easier for them. We are working with the 25th Infantry Division on improving their land utilization and land optimization because the island of Hawaii has very limited amount of land for like training and resources. And we're working with the joint program executive office for armaments and ammunitions on automating the build out of ad hoc ammo supply points."

Hunt said for each of these projects, the soldiers and civilians will learn and apply those lessons to the next project, and the software factory will do the same for each cohort and each application the teams develop.

"We took that feedback and integrated it into the training that we offer and ensuring that cohort two has those building blocks in places that when they move to a product team, they've already got that skills that maybe cohort one had to learn along the way or learn," she said.. "As we scope and identify problems that we're going to be working on, we think about viability and longevity of the software factory. We want to make sure that we're not just working on business systems, which are important, but also tactically focused products that really do bring software factories to that other level of being able to demonstrate we are at the future front of the battlefield. We are focusing on those things that make us really successful. There's a bunch of other things we're learning about how to do security more effectively, automating as much as we can and some of the more nuts and bolts of development. But that's the whole point of an organization to be able to take lessons learned, do post mortems, understand what could be improved and then implement that."

"As we scope and identify problems that we're going to be working on, we think about viability and longevity of the software factory. We want to make sure that we're not just working on business systems, which are important, but also tactically focused products that really do bring software factories to that other level of being able to demonstrate we are at the future front of the battlefield. We are focusing on those things that make us really successful."

— **HANNAH HUNT, CHIEF PRODUCT AND INNOVATION OFFICER, ARMY SOFTWARE FACTORY**

Software bill of materials is the first step to improve software supply chain security

THIS CONTENT HAS BEEN PROVIDED BY ANCHORE

Jeremy Bryan, solutions architect and technical lead, Anchore

anchore

A confluence of events, including the SolarWinds breach and the subsequent White House executive order on cybersecurity, has pushed software supply chain security center-stage for the federal government and the ecosystem of contractors that do business with it. It's a top priority for many executives, but traditional notions of cybersecurity are proving inadequate to the current landscape, and the path forward isn't always clear. So where do they start?

Security accelerants

It's important to zero in on the factors that affect how agencies or an organization are impacted by current security risks in the software supply chain. And to do that, organizations need to understand the perfect storm of "accelerants" – as Jeremy Bryan, DevSecOps solutions architect at Anchore, calls them – that led to these current circumstances. Those accelerants would be the evolution of cloud platforms and cloud-native development practices, the increase of software containerization and the adoption of modern build and deployment methods.

"First, cloud platforms have not only allowed innovation at remarkable rates, they are enabling organizations to reach broader audiences faster," Bryan said. "Growing cloud adoption has, in turn, accelerated the use of cloud-native development techniques like software containerization. Using software containers has, in turn, encouraged increased use of open source software. This combination of cloud deployment, modern development techniques and expanded use of open source software is creating new threats for both software producers and software consumers."

Bryan also noted the rise in importance and awareness.

"The intersection of increased software container adoption and increased supply chain security concerns is impacting container initiatives across the board," he said. "We see that in our recent Anchore survey of 425 IT, security and DevOps leaders, that 64% of respondents have been affected by software supply chain attacks in the last year. This issue is growing in size each day."

"In the absence of applying new techniques to secure the software development pipeline, you have the security breaches that we're seeing," Bryan added. "Those elements combined have helped to accelerate the visibility of software supply chain security. Traditional security means just can't keep up, IT security organizations and even accreditation processes really cannot keep up with the pace at which organizations are able to build and release software now. We can consume new releases of software faster than ever before. And it's only going to continue to ramp up from here."

Role of the SBOM

This is where Bryan sees the concept of a software bill of materials (SBOM) squarely fitting into the

picture. Before an organization can make sense of the software supply chain, it has to understand the software building blocks it is using. An SBOM is often compared to the ingredients list on packaged food in the grocery store. It's an articulated list of all of the components that are in that package. That could include open source components, vendor components, or pieces of software a systems integrator built.

Having this level of transparency and visibility into the software supply chain gives organizations new opportunities to assess their risk disposition, and provides new, more secure footing and perspective for performing risk management. But just having an SBOM isn't enough; organizations have to make a plan for how to manage software supply chain security over time. A single software package could have thousands of components or more. That's a lot of information to aggregate, make sense of, and put to use in a meaningful, efficient way on an ongoing basis.

"I think that's a question that we're really sort of in the infancy of figuring out how to do," Bryan said. "Once you start to think about sharing SBOM information between organizations, you need to start thinking about standard formats to exchange the data, as well as tooling to automate the process and leverage the information to improve your security posture."

Supply chain trust

Because an SBOM becomes a foundation for trust between software suppliers and software consumers, it has to be in a format that each can read and understand. The industry has developed several SBOM standards and enabling frameworks, but there is not a definitive singular standard. One key area being developed is new approaches to guarantee that an SBOM hasn't been tampered with, by way of cryptographically signed attestations.

There's also the question of how these artifacts will be folded into existing accreditations and federal requirements, like Defense Department cybersecurity assessments or risk management and cybersecurity frameworks from the National Institute of Standards and Technology.

"The idea of creating this level of component transparency across the software supply chain is foundational to protect against future attacks more effectively," Bryan said. "As the cloud-native software development and containerization efforts continue to mature, traditional accreditation methods have opportunities to make equally significant strides. We are already starting to see new requirements being developed by the US government based on the executive order."

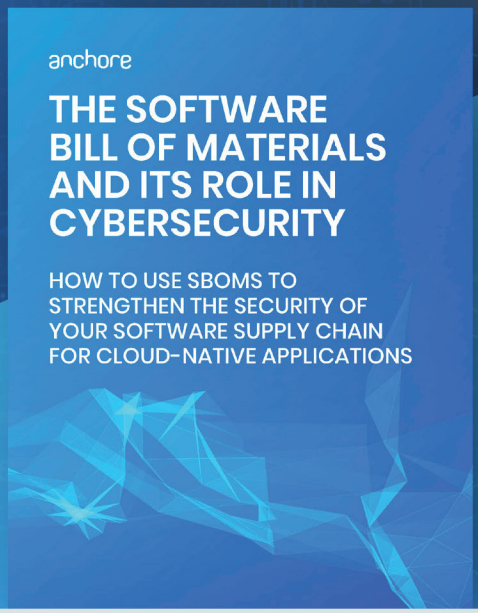
To improve their software supply chain security, organizations need to establish a strong foundation; they need to begin by looking at their development practices, pipelines and tooling, and assess how they can embed security into each step of the development process. That will require input and cooperation from all stakeholders, from security to development to leadership teams.

"It's not a situation where you can say 'I'm done, I did this thing once, and it's complete.' Software supply chain security is evolving, and it's going to be ever evolving. And organizations really have to pragmatically look at their software development practices," Bryan said. "Organizations can begin to formulate their security approach by understanding what an SBOM is, why it is important and how it fits into their current processes. They also must engage both business and technology leaders early so they understand the importance and value of a strong security posture in software development. Ultimately, both software producers and software consumers will need to work together to secure the software supply chain and prevent future attacks."

anchore

SECURE THE SOFTWARE SUPPLY CHAIN: SAVE THE WORLD

Accelerating software development is critical for deploying applications—but not at the expense of security. 64% of organizations surveyed reported they had been affected by software supply chain attacks in 2020. It's never been more important to ensure your software supply chain is secure. The Software Bill of Materials (SBOM) can be the key. Check out our white paper, **The Software Bill of Materials and its Role in Cybersecurity** to learn where to start.



DOWNLOAD THE WHITE PAPER >

CMS rolls out 'BatCAVE' as part of DevSecOps journey

BY JORY HECKMAN

The Centers for Medicare and Medicaid Services, already adopting a DevSecOps approach of continuously delivering secure software, sees the Biden administration's recent cybersecurity executive order accelerating this work.

Robert Wood, the chief information security officer for CMS, said the agency is adopting a multifaceted approach to DevSecOps that builds on the success of its cloud migration.

Wood, speaking at an Advanced Technology Academic Research Center panel moderated by Federal News Network, said CMS is moving toward a "declarative state" through DevSecOps.

"What I mean by declarative state is the state of your environment, the state of the pipeline that builds your environment and builds your code, the source and supply chain of all that stuff is all or maximally built into code, and so you're interfacing with an environment, with a system in a more GitOps-oriented way, as opposed to people just logging into stuff, manually moving build artifacts around, things like that," he said.

Wood said when all of this is built into the code base, it allows CMS to "lint," or check source code for programmatic errors, build release gates and push compliance down to the code base.

"If it's in the code base, it can be inferred automatically, if you're running a thing that was derived from the code base, and it can be just done automatically, instead of having humans go back and check scanning tools and run tools to get artifacts and look at reports and then read and write reports. All that stuff takes time," Wood said.

Groundwork for the SBOM

Wood said CMS is laying the groundwork for the software bill of materials (SBOM) portion of the administration's executive order. The executive order urges agencies to understand and use SBOMs as part of their risk management efforts.

The executive order defines an SBOM as "a formal record containing the details and supply chain relationships of various components used in building software."

Wood said vendors in the federal marketplace have pushed back on producing SBOMs as part of the procurement processes, and questioned how the federal government will hold the accountable to these standards.

However, Wood said he expects to hold his CMS team, which produces lot of custom code, to the same standards, and added that SBOMs ultimately meeting the goals established under the continuous diagnostics and mitigation (CDM) program.

> **"We are starting to lay groundwork for how we ingest Cyclone DX, the more security-oriented SBOM standard, into our data ecosystems so that we can start actually incorporating it into the asset viability functions that programs like CDM are and were intended to drive."**
>
> **— ROBERT WOOD, THE CHIEF INFORMATION SECURITY OFFICER, CENTERS FOR MEDICARE AND MEDICAID SERVICES**

"We are starting to lay groundwork for how we ingest Cyclone DX, the more security-oriented SBOM standard, into our data ecosystems so that we can start actually incorporating it into the asset viability functions that programs like CDM are and were intended to drive," Wood said. "CDM, I believe in the spirit of it. It's not just about what assets are running on your environment, but what is your asset? Or what is your environment actually made of at any given point in time? And if we consider third and fourth-party technologies, SBOMs sort of create that footprint, or that fingerprint, of what that thing is made of. Honestly, we should extend that same sort of practice to our own custom code, producing SBOMs to our own stuff. That way, we just know what makes up everything that is running in production right now, that's driving our mission and touching our data and dealing with our users."

"CMS does a lot of custom application development. Really what we want to do is to enable teams to deploy multiple times a day, if they want – not everybody's ready for that, some teams just don't work that way, they may be slightly slower – but we don't want teams to have to go through a two-to-four week security impact analysis, another multi-month ATO process for changes they want to make. They should be able to deploy iteratively, quickly, learn fast, fail fast – or I guess fail safe – and really just get the code out to where it needs to be faster and safer."

— ROBERT WOOD, THE CHIEF INFORMATION SECURITY OFFICER, CENTERS FOR MEDICARE AND MEDICAID SERVICES

As part of this work, CMS is rolling out the BatCAVE, a continuous authorization and verification engine that's focused on getting software into production faster, while decreasing the time developers spend auditing security risks. (The "bat" part doesn't stand for anything, but Wood said he's a huge Batman fan).

"CMS does a lot of custom application development. Really what we want to do is to enable teams to deploy multiple times a day, if they want – not everybody's ready for that, some teams just don't work that way, they may be slightly slower – but we don't want teams to have to go through a two-to-four week security impact analysis, another multi-month ATO process for changes they want to make. They should be able to deploy iteratively, quickly, learn fast, fail fast – or I guess fail safe – and really just get the code out to where it needs to be faster and safer," Wood said.

Security integration

Davon Tyler, CISO for the U.S. Mint in the Treasury Department, said his agency relies more heavily on commercial off-the-shelf services, but is beginning to adopt DevSecOps.

"We do have applications that would traditionally be developed using a waterfall model, and now we're bringing them over to DevSecOps, but from a size portion, have a very small amount of applications that would actually go through it. We haven't made investments in software to help us integrate the security with the development of applications and now we're going through the pipeline of getting everybody trained up and skilled up to support that demand," Tyler said.

Meanwhile, Tyler said the Mint is adopting endpoint detection and response (EDR) to automate and alert the agency to advance threats to its endpoints.

"We all went through the SolarWinds journey, and one of the things we experienced was that some of these tasks can take us a long time to do, and we this could be a lot more efficient. One of the terms that we used to have, at least in the Department of Defense, is we can't people our way out of every problem. And what that meant to us is that we have to find a software solution that enabled our teams to be more efficient, and not just bring in more people, bigger teams to solve a problem," Tyler said.

4 strategies to overcome obstacles in adopting DevSecOps in your agency

THIS CONTENT HAS BEEN PROVIDED BY ATLASSIAN

Ken Urban, director of technology, public sector

ATLASSIAN

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

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

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

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

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

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

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

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

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

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

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

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

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

Been there.
Scaled that.

ATLASSIAN

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

View the executive DevSecOps Survey

Work smarter and faster, together.

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

Learn More

At National Geospatial-Intelligence Agency, software is 'core to our mission'

BY JUSTIN DOUBLEDAY

The National Geospatial-Intelligence Agency's first ever technology strategy starts out with a simple premise: The agency is a software and data enterprise.

Software is core to its mission of analyzing geospatial data for both the military and the intelligence community, according to Alex Loehr, chief technology officer at NGA.

"We are not implementing DevSecOps because it's fun." Loehr said during the recent GEOINT conference in St. Louis, Missouri. "We're doing it to do our mission better. I worry that sometimes get lost in these technical conversations."

The agency's technology strategy, released last year, has five overarching initiatives, and the first involves "enabling builders and makers." In practice, that means ensuring NGA's software developers have the tools and the environment they need to build cutting edge applications.

"If we really believe that software is core to our mission, then delivering software in a modern way is something we have to do," Loehr said.

"If we really believe that software is core to our mission, then delivering software in a modern way is something we have to do."

— ALEX LOEHR, CHIEF TECHNOLOGY OFFICER, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

> **"We are not implementing DevSecOps because it's fun. We're doing it to do our mission better. I worry that sometimes get lost in these technical conversations."**
>
> — ALEX LOEHR, CHIEF TECHNOLOGY OFFICER, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

The need to balance speed and stability

Earlier this summer, the agency released a draft strategy called "The NGA Software Way." The document lays out how NGA will track three key metrics for each of its software products: availability, lead time and deployment frequency.

The metrics give NGA insight into how it balances "speed" and "stability" during product development and operations. And while those two factors were previously thought to be at odds with each other, research from the DevOps Research and Assessment organization has "conclusively shown that speed and stability are outcomes that enable each other and that high-performing teams do better in both of these areas," the NGA document stated.

NGA is currently pushing seven distinctly product lines to its software developers, including new messaging and workflow tools. The idea is to provide common platforms and reusable tools for every product team at the agency.

And the agency's software leaders are not trying to reinvent the wheel. They pull tools and processes where they can from other Defense Department and intelligence community organizations. For instance, NGA has copied secure containers from the Air Force's Iron Bank repository.

Maintain control of the source code

In the same vein, Air Force's vaunted "Kessel Run" initiative actually started out by using tools that were available at NGA, according to Andy Curtis, technical lead for DevSecOps tooling at NGA.

"It's a small community in some ways," Curtis said. "We always like to build and copy what we can from the other folks."

The agency is also confronting an internal program culture that often has a "built here" mentality.

"The major programs are used to doing these things all themselves," Curtis said. "The shift from owning their entire destiny to having to trust another part of the organization to provide some of their base capabilities is a huge culture shift."

NGA's software team is trying to prove out its model by being a quick problem solver, providing useful tooling and by showing people they can move fast.

Maggie Offholter, digital maker services division chief at NGA, said the agency is pushing both its teams and contractors to use their government-furnished tools and environments. The agency wants to ensure it maintains control over the source code, but Offholter also says development teams don't have to waste time building out their own simulation environments. Instead, they can "test where operate," she said.

"You can just go in, day one, start coding," Offholter said. "That's our goal."

Public-private partnerships ensure ‘innovation flowing both ways’

THIS CONTENT HAS BEEN PROVIDED BY SONATYPE

Dr. Stephen Magill, vice president of product innovation, Sonatype

sonatype

There’s a well-worn stereotype that government can’t innovate as fast as industry, and that’s why it relies on public-private partnerships to update its technologies, because it can’t on its own. But if you dig a little deeper, it turns out that the innovation ecosystem that exists between the public and private sectors is more complex than that, and involves far more give and take.

“There’s always been this technology exchange between the federal government and industry, with innovation flowing both ways,” said Stephen Magill, vice president of product innovation at Sonatype. “There’s high profile examples of these government developed technologies that spawned commercial activities. So GPS is one example of that. Another is what you see in rocket technology, where initial work was all government funded happening at NASA. Now there’s a lot of innovation happening at companies like SpaceX and Blue Origin. We’ve seen the same thing happen in the software security field as well.”

For example, software security technologies like static application security testing and dynamic application security testing originated as government funded research projects. Government requirements around high levels of security and assurance tend to develop earlier than within industry due to the nature of the mission at federal agencies, especially within the Defense Department and intelligence community. That’s because government agencies face a higher risk of compromise from well-funded bad actors like adversarial nation states.

But those technologies that originate out of the needs of agencies and the research they fund to meet those requirements also spawned a large, thriving industry of software security companies and vendors. Those technologies then become widely available, and quickly adopted by the rest of the private sector. Soon every software company cared about security, which sparked further innovation, which then makes its way back into government. The same cycle is currently repeating with secure software development and DevSecOps.

“Government has the ability to spawn investment in new areas via government research programs, things like DARPA, and other research arms and DoD. NASA and DHS also have large research programs, so there’s that ability to push the forefront and drive innovation,” Magill said. “And then, as is always the case with research, some of those bets pay off big time, and some end up being a dead end. But those ones that really gain traction, I think then industry becomes the place where it really develops into a robust capability. In many cases, that capability then flows back to government. There’s a sense in which government is often the incubator of some of these ideas, which is underappreciated.”

That's why practically every government agency currently has a group experimenting with DevSecOps, and some of them are seeing real success with it, like the Air Force's Platform One program. These groups are delivering software faster and under budget. That's especially impressive considering that government often has more than just cloud-based software systems to think about; agencies have complex radio systems, vehicles and aircraft and other physical component systems that have to be integrated seamlessly. That's a tougher environment than most private sector organizations face.

Factor in the fact that governments also rarely have a single pipeline to manage for their development. While industry can set a single template for all its software development, federal agencies often have contractors contributing as well. That means those agencies essentially have multiple different development teams, with different processes, tools, infrastructure and environments operating on the same project. That makes governance a much more complicated proposition.

But that's where that back-and-forth ecosystem comes into play again, because one of government's main roles in that dynamic is to set standards and develop frameworks. Federal guidance like the recent cybersecurity executive order helps ensure everyone is on the same page, and provides methods for alleviating some of those governance issues.

"If you don't have that level of control over the development process, you need a way to check the final product," Magill said. "And so things like a software bill of materials give you that visibility that lets you say, 'I have this product that's coming out at the end of the process, and I have visibility into enough of how it was constructed to check security of components.'"

As government sets these kinds of standards, industry adopts and propagates them. This creates a kind of innovation feedback loop where government innovates, and industry runs with it, while government sets parameters on which direction to run in. You see this dynamic play out across various industries currently, including 5G and internet of things. Even technologies used to test weapons systems which can't safely be tested physically are being adapted to test self-driving cars.

"It's not something you hear often, that the government's innovating beyond industry. I want to push back on that a bit," Magill said. "There really are places where government has spawned innovation. And once something takes off in industry, and there's a large market for that technology to grow, then things can accelerate and take off. But there is a vital role government innovation plays in that advancement of software and technology."

sonatype

Code smarter. Fix faster. Be secure.

Software supply chain security should feel like a no-brainer.

Combating modern-day supply chain attacks is significantly more complicated than in the past. Adversaries are getting craftier and organizations need to be prepared to stop known and unknown risks.

Sonatype's Nexus platform provides precise intelligence for delivering uncompromised applications. It continuously, and automatically, identifies and remediates open source risk across every phase of the software supply chain.

Learn more about how to protect your software supply chains at sonatype.com.