Business Chief

USA EDITION

OCTOBER 2019

www.businesschief.com

U.S. AIR FORCE

A DIGITAL REVOLUTION IN THE US AIR FORCE

Nicolas M. Chaillan discusses the launch of the DevSecOps initiative amid technological change

EXCLUSIVE VIDEO

SAP

HARNESSING THE POWER OF 5G

AURORA

GROWING INTO A SMART CITY

TOP 10 Hotels in North America

City Focus

HOUSTON

Space-centric startups

U.S. AIR FORCE

12

DRIVING T
DevSecOps I
THE US A

WRITTEN BY
SEAN GALEA-PACE
PRODUCED BY
MIKE SADR

THE
NITIATIVE AT
R FORCE

NICOLAS M. CHAILLAN, CHIEF SOFTWARE OFFICER AT THE US AIR FORCE, DISCUSSES THE LAUNCH OF THE DEVSECOPS INITIATIVE AMID TECHNOLOGICAL CHANGE IN WASHINGTON DC

The US Air Force needs little introduction. Operating with the mission: 'to flight, fight and win... in air, space and cyberspace', the organisation affirms that only the best is good enough. With serving the American people at the forefront of decision-making, the US Air Force has established three essential core values to which it adheres: 'Integrity First, Service Before Self and Excellence in All We Do.'

Sitting down with Business Chief in the US capital of Washington DC, Nicolas M Chaillan, Chief Software Officer at the US Air Force and Co-Lead of the US Department of Defense (DoD) Enterprise DevSecOps Initiative, is responsible for overseeing the successful launch of Cloud One, supporting all business and weapon systems in the Air Force and the DoD Enterprise DevSecOps Initiative. Introduced by the Chief Software Officer and Gen. Schmidt in July 2019, a combination of both Microsoft and Amazon Web Services' cloud

Secure Your Federal Software Supply Chain with the Sonatype Nexus Platform

A better way to build software and manage open source security risk.

Control.

Define open source component policies by organization, team, and application type.

Automate.

Automatically and contextually enforce policies across your entire software development lifecycle.

Secure.

Decrease false positives and negatives and reduce gaps in security and quality assurance

Integrate.

Continuously visualize component intelligence within your favorite tools.

sonatype

Federal Software Supply Chains are Most Susceptible

A series of high profile and devastating cyber attacks have demonstrated that adversaries have the intent and ability to exploit security vulnerabilities in the software supply chain. Never was that so apparent than in the massive breach at Equifax. But, Equifax was not alone. Hackers quickly attempted to exploit the Struts vulnerability elsewhere. According to David Hogue, a senior technical director for the NSA's Cybersecurity Threat Operations Center (NCTOC), "We had a nation-state actor within 24 hours of scanning for unpatched [Struts] servers within the DoD." The government is not immune to these issues, and may often be a great target for adversaries.

The 2019 DevSecOps Community Survey, taken by thousands of IT professionals, found that 20% of respondents from government agencies believed they had a breach stemming from the use of vulnerable open source components in the past 12 months. That's an alarming number when you consider what those attempted breaches may have been trying to uncover.

As government developers and contractors work towards digital modernization goals, they are consuming hundreds of billions of open source components and containerized applications to improve processes and catch up with their commercial counterparts. The good news: they help create efficiencies and enhance innovation within the government. The bad news: many of the components and containers they are using are fraught with defects including critical security vulnerabilities.

In today's world, understanding what's in your supply chain, as supported by the Mitre's Deliver Uncompromised report, is critical to national security.

Using the Sonatype Nexus Platform, aligns security professionals and developers on the same team and empowers organizations and agencies to continuously identify and remediate open source risk, at all points in the software supply chain.

"[Nexus] has given us visibility into security issues and made us more proactive. It scans and gives you a low false-positive count."

— **EDWIN K.** (IT CENTRAL STATION REVIEW)

NEXUS REPOSITORY: Analyze the quality of components inside your parts warehouse.

NEXUS LIFECYCLE: Automate open source governance at scale with precise and actionable intelligence.

NEXUS FIREWALL: Confidently quarantine bad parts from entering your software supply chain.

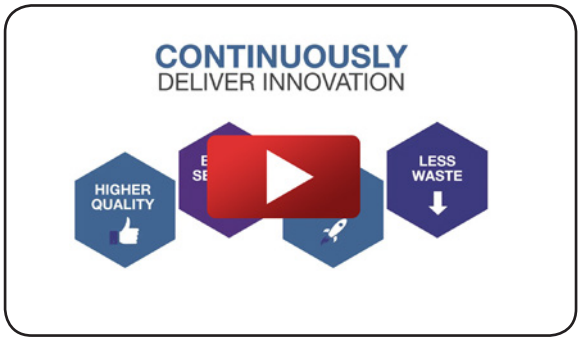
NEXUS AUDITOR: Efficiently monitor production and third-party apps for open source security.

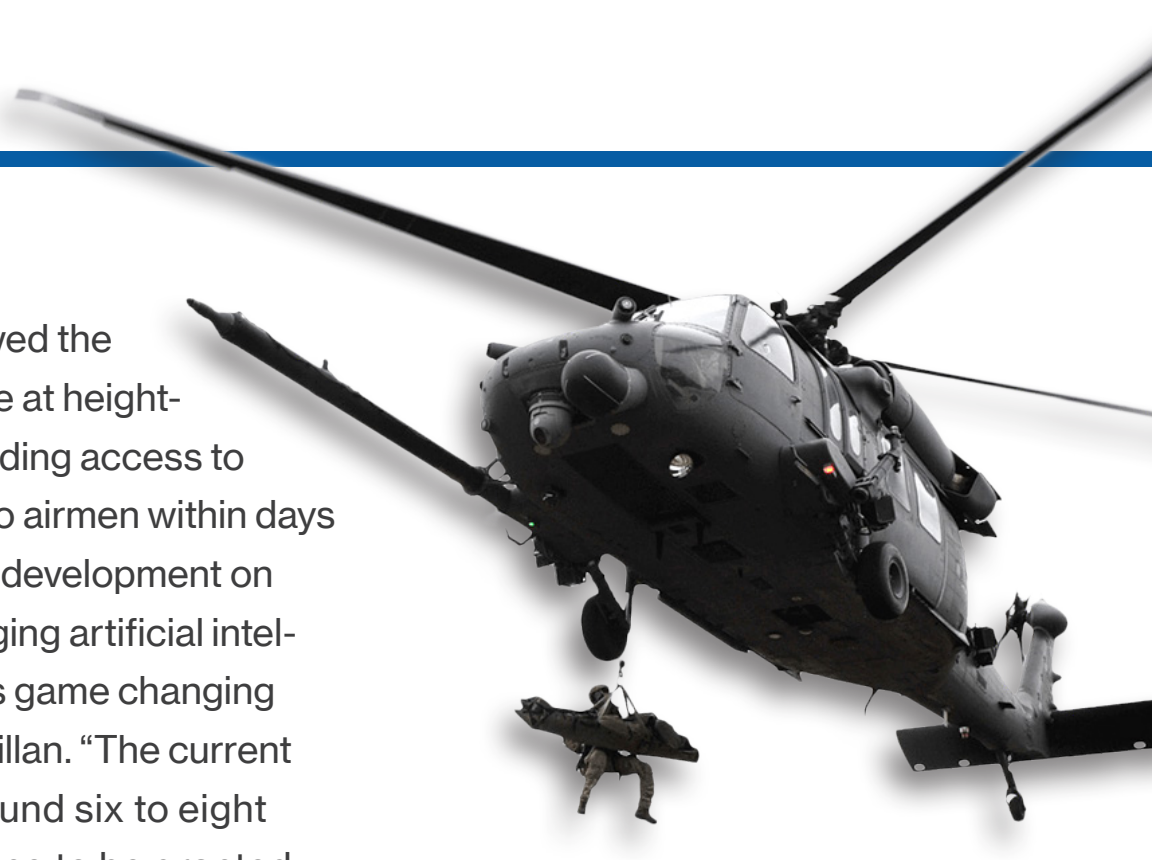
NEXUS INTELLIGENCE: Precisely identify open source components to accurately classify security vulnerabilities, licensing risks, and versions.

We are laser focused on helping federal agencies and contractors continuously harness all of the good that open source has to offer, without any of the risk. Those equipped with Nexus products make better decisions, innovate faster at scale, and rest comfortably knowing that their applications always consist of the highest quality open source components.

Visit **sonatype.com/government** to learn more about Open Source Security.

Watch this video to learn more about the Nexus Platform:





platforms has allowed the Air Force to operate at heightened speeds, providing access to cloud capabilities to airmen within days to enable software development on the cloud or leveraging artificial intelligence (AI). “This is game changing for us,” affirms Chaillan. “The current process takes around six to eight months for someone to be granted access to a cloud to deploy software there.” With the initiative focusing on marrying automated software tools, baked-in cybersecurity, services and standards to the DoD program, it is set to enable fighters in the field to create, deploy and operate software applications in a secure and flexible way. “Having started nine years ago, DevOps has become the evolution of

CLICK TO WATCH: 'NICOLAS M. CHAILLAN ON THE IMPORTANCE OF HAVING DIVERSE PARTNERS WITHIN THE US AIR FORCE

"DEVSECOPS ENABLES US TO SECURELY DEPLOY SOFTWARE MULTIPLE TIMES A DAY"

—

Nicolas M. Chaillan,
Chief Software Officer,
US Air Force

agile and is now able to use automation, both in testing and cybersecurity, to help bring software into production," explains Chaillan. "By removing the impediments we have in order to build software faster and better, DevOps enables us to deploy software on the commercial side multiple times a day. For us in the DoD, cybersecurity is vital because of the continuous monitoring side of the house. That is why we call it DevSecOps. It's important that we're able to constantly see what's going on in production in real-time

"PROACTIVITY IS THE ONLY WAY, PARTICULARLY IN TERMS OF CYBERSECURITY BECAUSE YOU CAN'T AFFORD TO BE REACTIVE"

Nicolas M. Chaillan,
Chief Software Officer,
US Air Force

EXECUTIVE PROFILE

Nicolas M Chaillan

Having begun his role as Chief Software Officer of the US Air Force in May 2019, Chaillan is an experienced Senior C-Level Executive with 19 years of domestic and international experience with strong technical and subject matter expertise in cybersecurity, software development, product innovation, governance, risk management and compliance. He is an expert in numerous technological fields such as cybersecurity, DevSecOps, multi-touch, mobile solutions, IoT, Big Data, Mixed Reality, VR, Cloud Computing and wearables. Chaillan has successfully launched and managed 12 companies throughout his career.

"KUBERNETES IS CLEARLY WINNING THE BATTLE WHEN IT COMES TO CONTAINER ORCHESTRATION AND SCALE"

Nicolas M Chaillan,
Chief Software Officer,
US Air Force

with a zero-trust model down to the container level, with behavior detection and centralized logging so we can obtain the data and get the telemetry back to development teams."

With the task of implementing DevSecOps, the Air Force has begun implementing software factories such as the Kessel Run Laboratory over the past few years. Through Kessel Run, Chaillan believes the Air Force has transformed the way it develops and delivers software capabilities. "Back in 2017, the Air Force was already very innovative and decided to develop Kessel Run while also building software and mission capabilities to use the Kessel Run factory," he says. "The goal wasn't just to build a factory for the sake of having a factory – it's been to create mission software and bring tangible value to the warfighters."

Chaillan began work at an early age in his native France. At 15, he created

and developed his first company. "I've been on the commercial side for a long time, I ended up selling 12 companies and building robust teams in cybersecurity and software innovation," he explains. "I moved to the US around 10 years ago and, after selling my companies, I decided I wanted to make a difference and have a real impact. Building mobile applications and other cool technologies is fun, but it's not the same impact as we have in the federal government." Due to new technology such as Big Data, machine learning (ML) and AI becoming increasingly influential globally, businesses worldwide are adopting innovative, modern processes in order to remain current. The case also applies to the US Air Force, with Chaillan understanding the impact that technology has had on the way his organisation conducts operations. "I think the entire future of war is going to be

CLICK TO WATCH: 'LEVERAGING DEVSECOPS AND CLOUD ONE AT THE US AIR FORCE'

something that's driven by embracing these kinds of technologies, whether it's AI, ML, Big Data or cybersecurity offence and defense," affirms Chaillan. "If you can't adapt while in production, then you're stuck in time and there's nothing worse in software than that. It's important to bring in new capabilities as well as adapting existing capabilities to make sure you can fix problems as they arise."

Cybersecurity is perhaps the dominant factor at the forefront of Chaillan's decision-making. With the importance of keeping highly-confidential information secure at all times being crucial to both the DoD and the Air Force, the government must remain proactive rather than reactive to counteract any potential threats. "Proactivity is the only way, particularly in terms of cybersecurity because you can't afford to be reactive," he says. "If you're not being proactive, you're not doing a good enough job. You have to combine what's already stable enough to use versus something that's new but just a little too early." Striking a fine balance

between the risk of embracing disruptive technology to accelerate current processes and sticking to previously successful approaches is challenging. However, Chaillan believes one of the biggest hurdles to overcome is continuously training staff with the latest trends.

"You really have to understand the risk, because technology is accelerating at an incredible pace at the moment. In IT, you have the ability to completely change the way you're doing business; sometimes it's going to last and sometimes it may not."

In order to arrange and manage software containers, the Air Force has deployed Kubernetes, originally designed by Google and now maintained by the Cloud Native Computing Foundation (CNCF), as part of its DevSecOps platform. "As a government, it's important that we don't get locked into a particular cloud provider or platform," says Chaillan. "When I started, I wanted to ensure that whatever we built was abstracted so we weren't reliant on a single vendor or product. It was a key reason why we initially chose Kubernetes and decided to abstract our entire stack because, whatever application you use, you want to ensure you understand the costs and the impact of the lock-in with that specific application."

"Kubernetes is clearly winning the battle when it comes to container orchestration and scale. It's an open

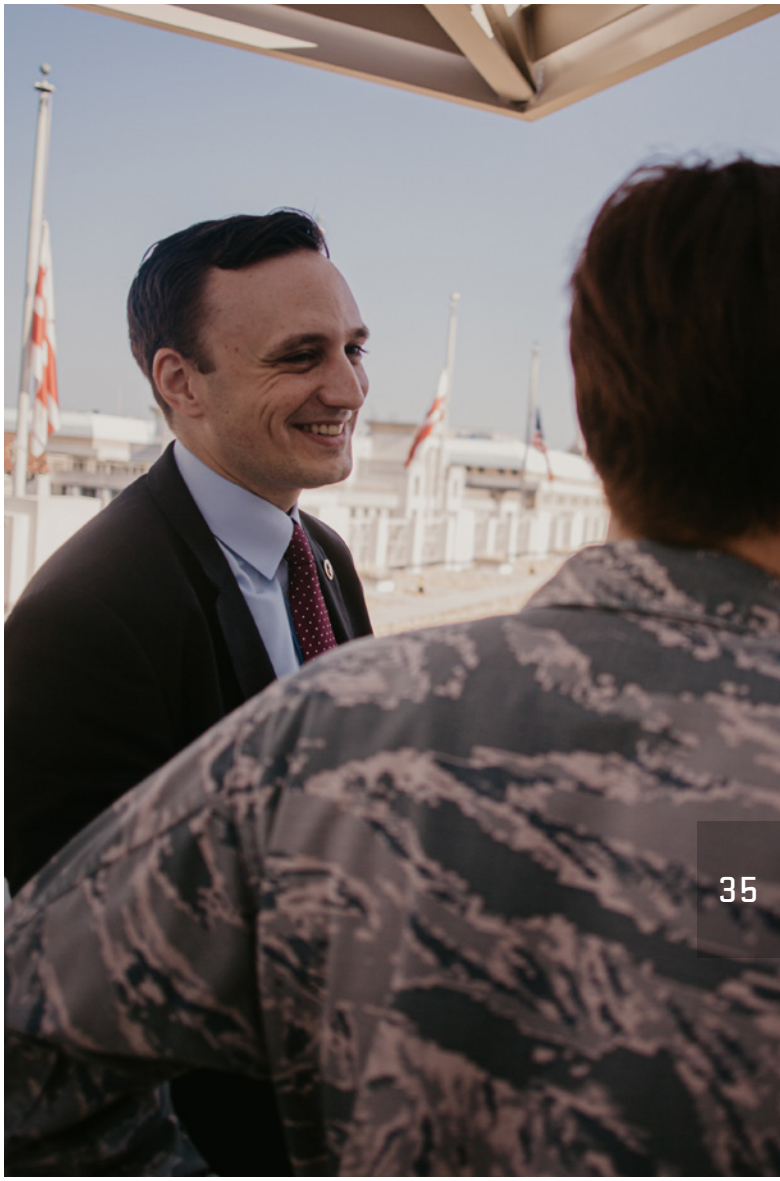
5,328
Number of manned aircraft as of 2018

1947
Year founded

327,215
Approximate number of active duty airmen

"MY JOB IS TO MAKE IT EASIER FOR STARTUPS TO WORK WITH THE US GOVERNMENT"

Nicolas M. Chaillan,
Chief Software Officer,
US Air Force



Kobayashi Maru, LevelUp, Bespin that were all utilising a very limited set of talent to create the factory, and this then enabled them to build the software. We just decided to decouple development teams from factory teams and now we only have two factory departments – LevelUp and Kessel Run. The development teams can simply use these two factories so they don't have to reinvent the wheel. The more development

US AIRFORCE FACTS

Along with conducting independent air and space operations, the U.S. Air Force provides air support for land and naval forces and aids in the recovery of troops in the field. As of 2017, the service operates more than 5,369 military aircraft, 406 ICBMs and 170 military satellites. It has a $161bn budget and is the second largest service branch, with 327,215 active duty airmen, 141,800 civilian personnel, 69,200 reserve airmen, and 105,700 Air National Guard airmen.

teams we are integrating into our DevSecOps platform and migrating our existing software factories the better, because they can simply piggyback on them and on Cloud One."

The US government has a process for software approval called an Authority to Operate (ATO) which takes between six months to a year. "Thanks to Dana Deasy, the DoD CIO, Bill Marion the Air Force CIO, Lauren

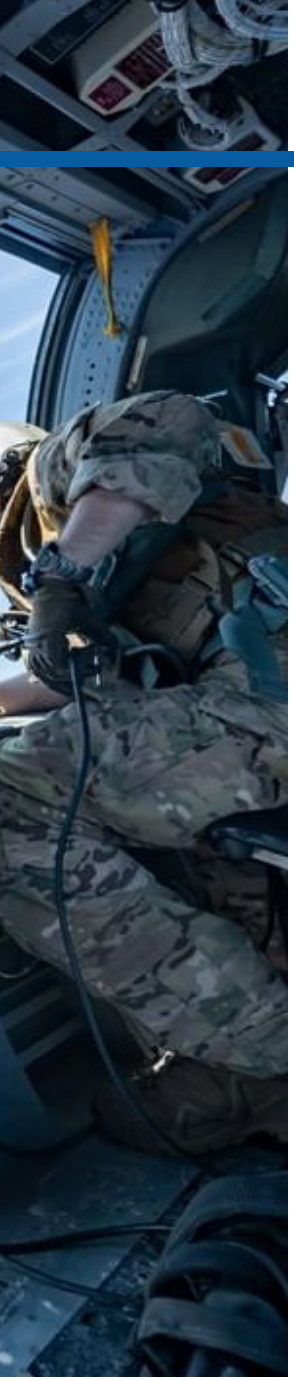
Knausenberger, the Air Force Chief Transformation Officer, Daniel C. Holtzman, Cyber Security Engineering and Resilience Senior Leader, we implemented the concept of a DoD-wide continuous ATO to allow us to push software to production continuously within a software factory," he explains. "The continuous ATO (cATO) enables us to automatically take software from development to production multiple times a day, without having to reassess the software manually. This becomes an automated process and is a clear, well-defined, step-by-step procedure that takes software from unit, integration, regression and end-to-end testing all the way to cybersecurity scanning and deployment." Regarding partnerships, Chaillan hopes it will become easier for startups to work with the US government to ensure the Air Force continues to achieve success in the technological space over the next few years. "We're trying to tap into every company that is interested in working with us," says Chaillan. "My job is to make it easier for startups to work with the US government. Getting access to technology is critical, if we

"THE MOST IMPORTANT THING IS THAT EVERY-THING THAT IS DESIGNED HAS TO BE SUSTAINABLE – IT MUST BE SOMETHING THAT WILL LAST AFTER I'M GONE"

Nicolas M. Chaillan,
Chief Software Officer,
US Air Force

get behind it's going to have a major impact on our mission capabilities. If we don't have access to the latest technologies because startups find it too hard to work with the US govern-ment, then we're going to fail. The second aspect is the real partnership with the airmen and the DoD programs. We have to build mission capabilities with the implementation of programs such as AEGIS, JAIC, F16, F22 and F35 because they need to build software and they have to do it now. That's my partnership – it's teamwork."

With the future in mind, Chaillan



U.S. AIR FORCE

hopes to create a legacy that will last long-term. “The most important thing is that everything that is designed has to be sustainable – it must be something that will last after I’m gone. You have to ask the question: is it something that can scale? If I don’t do that, I could stay 10 years and I wouldn’t have made a big impact. You need to change the system, not just go around the system. You have to make that change last,” concludes Chaillan. ■