Constellations
Podcast

Episode 101 – Zero Trust, Global Data Interoperability and Breaking Silos

Speaker: Nicolas Chaillan, Chief Software Officer, U.S. Air Force – 22 minutes

John Gilroy: The views expressed in this podcast or on www.constellationspodcast.com, do not officially represent the views of the U.S. Military or the United States government. The appearance of U.S. Department of Defense, DoD visual information, does not imply or constitute DoD endorsement.

John Gilroy: Welcome to Constellations the podcast from Kratos. My name is John Gilroy, and I'll be your moderator. Our guest today is Nic Chaillan, U.S. Air Force Chief Software Officer. We will discuss Air Force's Platform One, a centralized team providing DevSecOps, software factory managed services with baked-in Zero Trust security to duty programs, so they can begin their software work with about a 90% solution. Nic is a self-described serial entrepreneur. Nicolas said, that after starting my 12th company, the terrorist attacks in Paris happened and I decided I wanted to make a difference. I became a US citizen and I got a job at the Department of Defense. Nic, that's a tough story to beat, isn't it?

Nicolas Chaillan: Thanks for having me.

John Gilroy: Can you tell us a little bit about your background and what you did before you joined the Air Force, please?

Nicolas Chaillan: Yeah, of course. As you can tell with my French accent, I was born in France and I created my first company back there when I was 15. I'm a software guy, I'm a savvy guy. So like you said, I ended up creating 12 companies over the last 20 years. I'm 36 now, so I guess, I'm getting older. Like you said, I became a U.S. citizen, I wanted to really make a difference at the time. I actually started first at DHS. I was a Chief Architect at DHS trying to solve some of the issues we're facing with terrorism and also cyber-security challenges, across the critical infrastructure, across the country. And then, like you said, started in DoD to help the government move at the pace of relevance with DevSecOps as well. So that's that, and like I said, it's kind of a unique journey and I wouldn't trade anything, it’s very exciting. Obviously, a very different world moving from kind of the startup commercial industry to the Department of Defense has been fun.

John Gilroy: I think during the conversation, listeners will find out that you bring a lot of that heart and that innovation to the federal government, which is really unique in your background. I want to talk more about your responsibilities in addition to your role as Air Force, Chief Software Officer, you also serve as a co-leader for the DoD DevSecOps initiative, along with the DoD CIO. So what is DevSecOps and why would the DoD even need it?

Nicolas Chaillan: Yeah, so DevSecOps is kind of breaking the silos between development, security testing and operations, and effectively it's shortened the life cycle of software. So you can release software multiple times a day and get feedback loops shorter and faster. So you can learn from your end users, in our case the warfighters, so we can start building relevant software. Obviously you want to make sure you're not building software in a vacuum and you're building features and things that actually make sense to your users. And you want to make sure you're not spending too much time building things without that feedback from the end user. So the faster you can release that, particularly when it's more incremental change and progress, the more you can move at the pace of all of them and accelerate your journey to innovation. And so that's obviously what we call continuous engineering, software is never done, it's always going to evolve to the next thing. So timeliness and baked-in security, that's why we call it DevSecOps and not just Dev Ops. Having that baked-in security baked-in inside of that process is not coming first, it's not coming last, it's really baked-in inside of the life cycle. And we use Zero Trust and all the most advanced cyber principles to do that. That's what its game-changing for the department, and just in over a year now with 37 DoD programs moving to DevSecOps, we have saved a hundred years of plan time. So we effectively in one year have saved a hundred years of what would have taken if we were not using DevSecOps.

John Gilroy: Well, it's so refreshing to hear learning from end users at the DoD. That's really the mantra from startups. And you're applying that in this really difficult environment you're in now, let's take a look at this environment. The military seems to be interested in having global data interoperability across all its domains. It's been said that this goal will require a completely new data architecture, but you have said this new data architecture does not necessarily mean the underlying technology has to change. So how you do one without the other?

Nicolas Chaillan: Yeah, I think it's a little bit foolish to think you can completely modernize an entire enterprise of the size of the DoD, right? That's just never going to happen. We have too many silos and legacy systems and they all will need to start aggregating and federating systems through abstraction layers that enable the aggregation of data across systems while not effectively modernizing the system. The key is to make sure you're protecting your data. Effectively, the minute you start connecting all these silos, that were initially cut to avoid cyber or security risks by having a malicious actor, get access to one system and then be able to then access the entire DoD set of capabilities by segmenting them, obviously you are mitigating the risk of lateral movement, but you are also creating silos, which obviously we know that to be able to be efficient in finding the next walls, you need to have data and you need to have that holistic view of what's going on.

Nicolas Chaillan: So the silos become impediments to the leadership success of making the right decisions. So to move to that connected environment, what we call Zero Trust, is going to be foundational to enable that connectivity across systems and making sure people only have access to what they should have access to. So people can't abuse the access or the malicious actor, can't laterally move across the entire system, that's really how we ended up mitigating risks. And you can implement your trust by adding effectively abstraction layers to the existing systems. So the existing systems are not drastically changing, but what you are doing is federating or aggregating data across those systems through additional capabilities. So, that's effectively what we're doing.

Nicolas Chaillan: You have two options, you can federate, or you can aggregate. Aggregate is expensive. Federation is much easier. So you can connect things together and be able to query the federated system and get results without even knowing where that query goes. As a user, you just get the results of that query and you don't even know, maybe you talked to 50 systems behind the scene. So there are many ways to do this at scale, but the fact is, its just a little bit crazy to think you can modernize something of the size of the department overnight. So, that's just not going to happen.

John Gilroy: You used the word holistic, I want to dive into that topic a little bit more here, global data interoperability. It seems to me that this concept wants to enable the Department of Defense's concept to connect sensors from all the military services, Air Force, Army, Marine Corps, Navy Space Force into a single network. It seems like that's a pretty big goal, isn't it?

Nicolas Chaillan: Yeah. I mean, it's obviously foundational to the success of the Department and in the future and you're talking all domain, right? So obviously space and cyber or big new domains that too often were missed in the past. And, we all know that the next battles are going to really involve these two domains, probably more than others. And so that's very important to be able to have that holistic access across all these domains and be able to share data, but also reuse code and software across these environments. So, effectively a sensor could be used on the ship, on a jet, on the ground, all the way to space with the same piece of code that could be reused across teams. So we don't have to rewrite the entire stack from scratch and enabling the use of code is one of my biggest priorities right now. So we can be more efficient by not having to rewrite every system from scratch, every time we have a new idea.

John Gilroy: Many of the listeners to this podcast have subject matter expertise in satellites or maybe antennas and not all of them are engineers or software developers. So, when we use this term open source data architecture, what does that mean to you?

Nicolas Chaillan: Yeah, so I think people say open tools, but I think what people really mean is open architecture, right? And so it's not always open source, but it's open in a way that at least we know we're not getting locked into a single product, so we're not going to have to completely move the entire data structure into a single one size fits all product. And so, open architecture already means that you know exactly how the data flows and that you're not getting locked into a single product. If you add open source, that's not always the case, but many times many of these products, are open source and effectively, we have access to the source code and we can see exactly how these products are built and secure or not secure. And that gives us obviously more visibility inside of that supply chain and the quality of the code. And, obviously that helps in making decisions and picking the right products. In fact, most of the Platform One DevSecOps stack is based on open source products.

John Gilroy: If you’re in the academic environment classroom, you stand up there and you talk about open source, maybe open architecture, it is pretty much welcomed, but you started with this in the federal government. There must have been some main challenges in just doing that, weren't there?

Nicolas Chaillan: Yeah. Obviously you're facing not only the largest organization on the planet, but also the largest budget, but also the most silos across these teams, which were initially designed to make sure that we're not creating more risk, but effectively create a lot of reinventing the wheel across teams. And that's been a big challenge because, effectively, people are used to not using enterprise services and quite honestly, in a move to DevSecOps and cloud, particularly, you cannot succeed as an enterprise if you don't have enterprise services. So, each team is not reinventing the wheel when it comes to the basics of cyber, of DevSecOps, of cloud adoption, you need to have a cohesive environment to do all this work and you cannot do it in a vacuum. And so some of the big focus I had when I started was to create Cloud One and Platform One, which you know, Cloud One is the cloud office, for my team and then Platform One is a DevSecOps team to help all these DoD teams move to DevSecOps.

John Gilroy: Your name is associated, of course with Platform One. Was collaboration with industry the key to the success of Platform One?

Nicolas Chaillan: Oh yeah. I would argue that, we cannot succeed without industry, but we also don't want to completely outsource all talent and all knowledge to industry without having proper oversight and understanding of the decisions. So, we can do what's right for the taxpayer, both in terms of architecture decisions, and also hands on coding. So, we know how to find the next walls, right? So it is very foundational that we also have a play and a say inside of that software life cycle construct. And so, I think it's all about the right mix: you don't want to be a majority of airmen quarters and you don't want to be a majority of the entire industry team with no airmen baked in. So we're trying to be in the 90%, 10%, 80-20 range, where 80% will be the industry partners and 20% will be government people, whether it's, civilians or military. But that gives us the flexibility we need and the oversight, we need to make sure we make the right decisions.

John Gilroy: You, real quickly, gave a description of Cloud One and Platform One, maybe you expand on a little bit for our audience here. So we understand the differences.

Nicolas Chaillan: Yeah. So Cloud One is providing access to the cloud. So we have access to both Amazon and Azure, the government version of these clouds, both unclassified and classified. So that gives us the ability to have access to cloud in a matter of days for what used to take between 8 to 12 months for a team. That's why, again, enterprise services are so important. Unfortunately, the department got so used to doing enterprise services badly that people almost have an aversion to it, and they don't want to use them even when it's good. So it takes a little bit of convincing to say, Hey, and then they have to try it out to see if it makes sense. And unfortunately, people too often say, Oh, you're missing this 5% thing here. So we're going to rebuild everything from scratch, instead of helping building the 5% delta.

Nicolas Chaillan: So, that's been the number one problem we're facing. We need to really centralize the talent right? To go and tackle these deltas that we have sometimes. Nothing is perfect and nothing can solve every problem on the planet, but by focusing on the delta and not reinventing the entire wheel, that obviously helps move faster. So that's Cloud One, that's the cloud office effectively. And then Platform One is bringing the DevSecOps, continuous integration, continuous delivery of software with that agile construct to the department as well.

John Gilroy: You know, Nic, thousands of people from all over the world have listened to this podcast, go to Google and type in "Constellations Podcast" to get to our show notes page here, you can get transcripts for all 90 plus interviews also can sign up for free email notifications for future podcasts. If you look at the federal government in the last 15, 20 years, one critique has been something called vendor lock-in and an agency signs a contract with vendor A and it's almost impossible to get out. And if they get out, it may be too expensive to get out. So when you talk about cloud migration here, how does it avoid vendor lock-in? Is the answer standards or is it open architecture? How do you get out of a vendor lock-in? And how do you get rid of that?

Nicolas Chaillan: Yeah, so the entire architecture of Platform One was designed to prevent vendor lock in. We extract everything from the cloud provider standpoint so we're not getting locked into a cloud first, all the way to every piece of the stack. So we use Cubase, which is a content orchestration tool. Everything we do is Lego blocks driven. So by cutting into small Lego blocks effectively, you can move things around and swap them to try things out for different use cases. So you don't have a one size fits all. So our entire stack is containerized and, of course gives us the flexibility and the modularity that we need to be able to swap these Lego blocks and try things out. So, we have a central team that's accrediting containers for the department part of Platform One. That team is effectively accrediting and updating and hardening commercial products and open source software.

Nicolas Chaillan: So they can be used inside of the DevSecOps universe. And that gives us that central assessment and abating of that supply chain risk. And that really streamlines the process to get a new startup or a new organization that wants to do business with DoD and that they add a cool commercial product to be authorized for use in the department. So that's really pretty exciting to see, we were able to get the 450 containers accredited in one year with Platform One, which is pretty game-changing. And that also helps us for cyber because we can update these Lego blocks automatically across the departments. And so we can provide these updates in case there is, a new vulnerability, a new zero day, or a new cyber issue that we need to fix immediately. We can do that within four hours. That's pretty game changing as well.

John Gilroy: Well, I'm going to transition from Lego blocks to the Game of Thrones. So Iron Bank, I guess, has a minor role in Game of Thrones. Where does Iron Bank fit in this whole discussion about open source?

Nicolas Chaillan: Yeah, so Iron Bank is a centralized repository of containers. That's where we put all these hardened Lego blocks we were talking about. So those are all effectively the centralized artifact repository of containers for the department, that's where we scan them, we hardened them, and we authorize some full consumption. And if it's open source, they can just use them, by the way, we open source this entire thing. So the entire industry is also using these containers. So we have not only financial institutions, healthcare, other government agencies and other partners using these containers as well. So, it's a two-way street. It's very exciting to see. We have so much adoption by industry of everything that Platform One does because of that open source vision, we thought that by being open and being transparent and, really putting eyes on code , and focusing on security and not just obfuscation and false sense of security by hiding under a rock effectively, we increased the cyber posture of the Department by having more eyes on code and more people to be able to bring back value to us in a faster pace.

Nicolas Chaillan: So as you know, timeliness is foundational to the cyber team, so we don’t get behind. And so being able to move fast and react to change and challenges in a timely fashion, its game changing.

John Gilroy: Well in this discussion so far, we’ve talked about Platform One, Cloud one, and Iron Bank. And, my question is, and I guess the question for the military, is how can you ensure all this is secure? What do you do to create a secure cloud architecture? Do you make sure the containers are secure, then therefore the architecture is secure? How do you do that?

Nicolas Chaillan: Yeah. So there's two pieces to that, right? One is you certainly want to secure your supply chain. So, the Iron Bank and the container hardening process gives us visibility on the risk there, but that's not enough, right? Because you have new findings and new issues that can come up all night and zero days and stuff like that. So, the foundation of our security is about Zero Trust and behavioral detection. So what we do is, not only do we continuously monitor all the stack and see if there's any change of behavior of the container. If it's doing something it's never done before, it's probably a sign of a bad actor of trying to do malicious things. So we will practically kill the container if we see that happening and alert the team that there is something wrong going on, and then we use Zero Trust, so Zero Trust, effectively, reduces the attack surface.

Nicolas Chaillan: So for container A to talk to B it has to be white listed. And it's going to create an encrypted tunnel to communicate between the two containers. So that reduced the ability of a bad actor, if a bad actor can get access to container he can talk to container B, C, D, F, G. You can only talk to A and maybe Z. So that reduces the ability for the bad actor to move laterally across the environment. So that reduces risk of attack surface and the ability to escalate privileges. And by obviously detecting behavior change and killing the container and going back to immutable state of the container, that means the bad actor will lose everything he has done and go back to zero. Every time we find out that he's trying to do something malicious. So obviously it's very difficult for a bad actor to retain access to the system, but also escalate privileges, or move to the crown jewel and laterally move to the crown jewel. So, that effectively reduces drastically cyber risk, and then obviously improves the cyber poster of the systems.

John Gilroy: Well, I have a speed question and it's appropriate. Cause we just have a couple of minutes left here. We know that Platform One can instantiate DevSecs, continuous integration, continuous development pipelines, in days at various classification levels. So, what's the big deal? I mean, why is this a big deal? What happened before?

Nicolas Chaillan: Yeah. Well, before you would have drift between classification levels so effectively, you will have all the fancy stuff and classify, but let's face it. The real meat of what we do is on the high side, on the classified environment. So you end up having to deal with outdated systems and product are 10 years old or whatever. And so by definition this is not a good user experience for the warfighter, you want to have a party between classification levels. So the work you're going to do, you're going to have the same cool tools and the same capabilities, whether it's AI, machine learning, deep learning, all the way to software development tools, or cyber tools, or whatever collaboration tools across classification levels. So by having the containers and the entire stack be able to be instantiated automatically across classification level that's game changing.

Nicolas Chaillan: So we always have the latest, always have the most updated versions and effectively the ability to instantiate a DevSecOps environment at the edge on the jet, on a bomber, anywhere we want on the space system. So we have that access with a push button deployment. So, we know that there isn’t going to be change, there isn’t going to be drift. It's going to be the most updated version with our cyber fixes, and that reduces also cyber risk as well, but also is a drastic improvement of the user experience as well.

John Gilroy: Trying to summarize our conversation, four words, I guess they're going to say that cool tools are game changers. Is that what you're trying to say?

Nicolas Chaillan: Yeah. And obviously it all ties back to the timeliness, right? I think people often miss the fact that IT is moving so fast. And honestly, most of the technology we use is not even three years old. So that tells you that continuous learning and enabling teams to learn continuously, have access to unbiased training. And that's why we give an hour a day to our people at Platform One so they can learn continuously. So we don't get behind so, we invest in our people to make sure that when we're not getting behind. So that's really a critical for us.

John Gilroy: Nic, great discussion. The listeners get to hear from a leader who can apply innovation to a challenging environment. I'd like to thank our guests, U.S. Chief Air Force officer Nic Chaillan.

Nicolas Chaillan: Thanks for having me.