Headquarters U.S. Air Force

Integrity - Service - Excellence

DoD Enterprise DevSecOps Initiative (Software Factory)

Mr. Nicolas Chaillan
Chief Software Officer, U.S. Air Force
Co-Lead, DoD Enterprise DevSecOps Initiative

v1.7 – UNCLASSIFIED
Problem Statement

- The Department of Defense (DoD) is mostly still using Waterfall software methodologies with software delivery every 3 to 10 years, making it impossible to keep up with the pace of technology.

- The DoD Authority to Operate (ATO) process to accredit software takes on average 8 months and is mostly manual with several testing and cybersecurity gates.

- Most of the Defense Industrial Base (DIB) (the DoD contractors and developers) have not adopted an Agile and/or DevOps mindset.

- Massive organization with large silos and large workforce.

- Limited Talent pool, IT enterprise services, Cloud access and high speed connectivity.
Must Rapidly Adapt To Challenges
Work as a Team!
A Large Team!
Integrity - Service - Excellence

Must Adapt to Challenges

Work as a Team!

A Large Team!

With Various Technologies
Must Adapt to Challenges

Work as a Team!

A Large Team!

With Various Technologies

Bring It With Us!
Even To Space!
Must Adapt to Challenges

Work as a Team!

A Large Team!

With Various Technologies

Bring It With Us!

To Space!

With a Few Sensors!

With a Few Sensors!
With Their Help!
What is the DoD Enterprise DevSecOps Initiative?


- Technology:
  - **Avoid vendor lock-in** at the Infrastructure and Platform Layer by leveraging FOSS with Kubernetes and OCI containers,
  - Creating the **DoD Centralized Artifacts Repository (DCAR)** of hardened and centrally accredited containers: selecting, certifying, and securing best of breed development tools and software capabilities (over 170+ containers) - [https://dccscr.dsop.io/dsop/](https://dccscr.dsop.io/dsop/) and [https://dcar.dsop.io](https://dcar.dsop.io)
  - **Baked-in Zero Trust Security** with our Sidecar Container Security Stack (SCSS) leveraging behavior detection, zero trust down to the container/function level.
  - Leveraging a Scalable Microservices Architecture with Service Mesh/API Gateway and baked-in security (Istio)
  - Leveraging KNative to avoid lock-in to Cloud provider Serverless stacks

- Bringing **Enterprise IT Capabilities with Cloud One and Platform One** – Cloud and DevSecOps as Managed Services capabilities, on-boarding and support!

- Standardizing metrics and define acceptable thresholds for **DoD-wide continuous Authority to Operate**

- Massive **Scale Training with Self Learning Capabilities** (train over 100K people within a year) and bring state of the art DevSecOps curriculum

- Creating new Agile contracting language to enable and incentivize the use of DevSecOps
From Waterfall to DevSecOps
Value for DoD Programs

- Enables any DoD Program across DoD Services deploy a DoD hardened Software Factory, on their existing or new environments (including classified, disconnected and Clouds), within **days instead of a year**. Tremendous cost and time savings.

- Multiple DevSecOps pipelines are available with various options (no one-size-fits-all)

- Enables **rapid prototyping** (in days and not months or years) for any Business, C4ISR and Weapons system. Deployment in PRODUCTION!

- Enables learning and **continuous feedback** from actual end-users (**warfighters**).

- Enables **bug and security fixes in minutes** instead of weeks/months.

- Enables automated testing and security.

- Enables **continuous Authorization to Operate (c-ATO)** process. Authorize ONCE, use MANY times!

- Brings a holistic and **baked-in cybersecurity stack**, gaining complete visibility of all assets, software security state and infrastructure as code.
“Cloud One” vs “Platform One by LevelUP”

- Cloud One:
  - Centralized team to provide Cloud Infrastructure with baked-in security to DoD programs. Think of it as the Infrastructure team with baked-in security, CSSP and Authority to Operate (ATO).

- Platform One by LevelUP:
  - Centralized team to provide DevSecOps/Software Factory with baked-in security to DoD Programs. Think of it as the Platform Team with the ability to deploy a DevSecOps (Kubernetes compliant) Platform and CI/CD pipeline with a Continuous ATO (c-ATO). You select from accredited tools to accelerate your ability to focus on delivering mission capabilities.
Understanding the DevSecOps Layers

- **Environment Agnostic**: Cloud One Preferred for unclassified (IL2, IL4, IL5) or SC2S/C2S/FENCES or on-premise/classified environments.
- **Development Teams** can build software/microservices leveraging hardened containers.
- Brings baked-in security and Microservices architecture enablement.
- Fully containerized, leverages DoD approved containers from DCAR.
- Development Team selects tools from 172 approved containers or custom containers.
- CNCF compliant Kubernetes (K8S) includes Site Reliability Engineers (SREs) etc.
- Development Team selects between approved K8S stacks.
- Infrastructure Layer
  - 
- Platform Layer
  - Continuous Integration / Continuous Delivery (CI/CD) Layer
  - Service Mesh Layer
  - Application Layer

---

I n t e g r i t y  -  S e r v i c e  -  E x c e l l e n c e
DoD Enterprise DevSecOps Technology Stack (Exemplar)

- **PLAN & DEVELOP**
  - GitHub
  - JIRA
- **BUILD**
  - MSBuild
  - CMake
  - Gradle
  - Maven
- **TEST**
  - JUnit
  - cucumber
- **SECURE**
  - SonarQube
  - OWASP
  - Fortify
  - Qualys
  - Contrast Security
- **STORE ARTIFACTS**
  - Nexus Repository
  - Archiva
- **DEPLOY & OPERATE**
  - GitLab
  - Cloudbees
  - Jenkins
  - Ansible
  - SaltStack
  - Chef
  - Operator SDK
  - Helm
  - Nagios
  - Splunk
  - New Relic
- **SCALE**
  - AWS
  - Azure
  - Google Cloud Platform
  - OpenShift
  - Kubernetes
  - Docker
  - micloud

“Continuous Integration & Continuous Delivery” Orchestration

Container and Container Management
Sidecar Container Security Stack

- Baked-in Zero Trust security down to the Container/Function level with Istio (Envoy) and Knative.
- Centralized logging and telemetry with Elasticsearch, Fluentd, Kibana (EFK).
- Container security: Continuous Scanning, Alerting, CVE scanning, Behavior detection both in development and production (Build, Registry, Runtime) with Twistlock
- Container security and insider threat (custom policies detecting unapproved changes to Dockerfiles) with Anchore
- Automated STIG compliance with OpenSCAP
Turnkey Service Mesh (ISTIO) architecture

ISTIO side car proxy, baked-in security, with visibility across containers, by default, without any developer interaction or code change

Benefits:
- API Management, service discovery, authentication…
- Dynamic request routing for A/B testing, gradual rollouts, canary releases, resilience, observability, retries, circuit breakers and fault injection
- Layer 7 Load balancing
- Zero Trust model: East/West Traffic Whitelisting, ACL, RBAC…
- TLS encryption by default, Key management, signing…
- Air Force Cloud Office with turnkey access to AWS GovCloud and Azure Government at IL2, 4 and 5. IL6 available by December 2019.
- Simple “Pay per use” model with ability to instantiate your own Development and Production VPCs at various Impact Levels within days with full compliance/security and a baked-in ATO.
- Enterprise Solution: we provide the guardrails to the cloud in a standard manner so you can focus on your mission
- Fully Automated: All environmental stand-up is managed by Infrastructure as Code, drastically speeding up deployment, reducing manual work, and human error
- Centralized Identities and Single-Sign-On (SSO): one login across the Cloud stack
- Internet facing Cloud based VPN to connect to IL5 enclaves with a Virtual Internet Access Point (coming within January 2020).
- DevSecOps Focused: secure, mission driven deployments are built into the framework to ensure self-service and seamless deployments. Leverages Zero Trust model.
- Proactive Scaling and System Monitoring: Mission Owners can see all operational metrics and provide rules and alerts to manage each mission their way
- Accreditation Inheritance has been identified in the AF-Cloud One eMASS accounts (AWS & Azure) to include inheritance from the CSP, USAF, DoD and CSSP. All that’s left for the mission is the controls that are unique to them.
“Platform One by LevelUP”

The Air Force Software Factory Team

- Merged top talent across U.S. Air Force from various Factories (Kessel Run, SpaceCAMP and UP).
- Helps instantiate DevSecOps CI/CD pipelines / Software Factories within days at various classification levels.
- Manages Software Factories for Development teams so they can focus on building mission applications.
- Provides Blanket Purchase Agreement (BPA) DoD-wide DevSecOps contracts for Cloud Service, Talent and Licenses. Enables awards every 15/30 days with bulk discounts.
- Decouples Development Teams from Factory teams with DevSecOps and Site Reliability Engineer (SRE) expertise.
- Partners with Cloud One to provide IL2, 4, 5 and 6 access but also uses C2S/SC2S and various on-premise environments!
- Self-learning and training capabilities to enable teams move to Scrum/Kanban/eXtreme Programming (XP) Agile practices.
- Leverages the DoD hardened containers while avoiding one-size-fits-all architectures.
- Fully compliant with the DoD Enterprise DevSecOps Initiative (DSOP) with DoD-wide reciprocity and an ATO. Leverages Zero Trust model.
- Hardens the 172 DoD enterprise containers (databases, development tools, CI/CD tools, cybersecurity tools etc.).
- Provides Software Enterprise Services with Collaboration tools, Cybersecurity tools, Source code repositories, Artifact repositories, Development tools, DevSecOps as a Service, Chats etc. These services will be MANAGED services on Cloud One.
“Platform One by LevelUP”
Managed Services “A La Carte”

- **Hardened Containers Options**
  - Delivery of hardened enterprise containers with accreditation reciprocity (existing containers only).
  - Delivery of custom hardened containers as needed.

- **Continuous Integration / Continuous Delivery (CI/CD) Options**
  - Delivery of existing hardened Kubernetes/OpenShift/PKS playbooks (full Infrastructure as Code).
  - Delivery of a **turnkey CI/CD pipeline** (Software Factory) with complete « Infrastructure as Code » to instantiate on any environment (development teams picks the tools from the approved hardened containers) on various classified/unclassified environment.

- **Training/On-Boarding Options**
  - 1-day training Session: introduction to DevSecOps. Overview and understanding of the vision and activities.
  - A 3 day introduction to LevelUP DevSecOps tech stack. Hands on code and User-Centered Design (UCD) to deploy your first demo app to production.
  - A several week full on-boarding, that concludes with an MVP ready for production.
  - A several month full on-boarding, that concludes with your platform team being able to support your own DevSecOps applications for development and production.
  - Customized training options (both at our locations or on your premises).

- **Contracting Support Options**
  - Ability to leverage the DevSecOps BOAs (Cloud Services, Talent and Licenses).
  - Enable access to DevSecOps engineers/SREs Full-Time-Equivalent (FTEs) (Medics/Counselors) to assist Programs.
DoD Enterprise DevSecOps Architecture
DoD Enterprise DevSecOps Architecture*

*each DoD Program can have its own instantiation of the DoD Enterprise DevSecOps Platform on any Cloud.
** can be installed with single command and deployed on any Cloud.
*** could be deployed inside an enclave or on-premises
**** gives complete visibilities of assets, security/vulnerability state etc. can be integrated to existing cybersecurity shared services.
DevSecOps Platform Stack (continuously evolving)
## DevSecOps Product Stack (1)

<table>
<thead>
<tr>
<th>Source Repository</th>
<th>API Gateways</th>
<th>Programming Languages</th>
<th>Databases</th>
</tr>
</thead>
<tbody>
<tr>
<td>GitHub Government</td>
<td>Kong, Azure API, AWS API, Axway, 3Scale, Apigee, ISTIO (service mesh)</td>
<td>C/C++, C#/.NET, .NET Core, Java, PHP, Python, Groovy, Ruby, R, Rust, Scala, Perl, Go, Node.JS, Swift</td>
<td>SQL Server, MySQL, PostgreSQL, MongoDB, SQLite, Redis, Elasticsearch, Oracle, etcd, Hadoop/HDInsight, Cloudera, Oracle Big Data, Solr, Neo4J, Memcached, Cassandra, MariaDB, CouchDB, InfluxDB (time)</td>
</tr>
<tr>
<td>GitLab</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Container Management technologies:**
- Kubernetes
- Openshift
- VMWare Tanzu
- PKS
- OKD
- Rancher (K8S only)
- D2IQ (K8S only)
- Docker EE (K8S only)

**Container Packagers:**
- Helm
- Kubernetes Operators
## DevSecOps Product Stack (2)

<table>
<thead>
<tr>
<th>Message bus/Streams</th>
<th>Logs</th>
<th>Docker base images OS:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kafka</td>
<td>Logstash</td>
<td>Alpine</td>
</tr>
<tr>
<td>Flink</td>
<td>Logstash</td>
<td>Busybox</td>
</tr>
<tr>
<td>Nats</td>
<td>Splunk Forwarder</td>
<td>Ubuntu</td>
</tr>
<tr>
<td>RabbitMQ</td>
<td>Fluentd</td>
<td>CentOS</td>
</tr>
<tr>
<td>ActiveMQ</td>
<td>Syslogd</td>
<td>Debian</td>
</tr>
<tr>
<td></td>
<td>Filebeat</td>
<td>Fedora</td>
</tr>
<tr>
<td></td>
<td>rsyslog</td>
<td>Universal Base Image</td>
</tr>
<tr>
<td><strong>Proxy</strong></td>
<td><strong>Webservers</strong></td>
<td><strong>Serverless</strong></td>
</tr>
<tr>
<td>Oauth2 proxy</td>
<td>Apache2</td>
<td>Knative</td>
</tr>
<tr>
<td>nginx ldap auth proxy</td>
<td>Nginx</td>
<td></td>
</tr>
<tr>
<td>openldap</td>
<td>IIS</td>
<td></td>
</tr>
<tr>
<td>HA Proxy</td>
<td>Lighttpd</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tomcat</td>
<td></td>
</tr>
<tr>
<td><strong>Visualization</strong></td>
<td><strong>Docker base images OS:</strong></td>
<td></td>
</tr>
<tr>
<td>Tableau</td>
<td><strong>ALpine</strong></td>
<td><strong>Busybox</strong></td>
</tr>
<tr>
<td>Kibana</td>
<td><strong>Ubuntu</strong></td>
<td><strong>Centos</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Debian</strong></td>
<td><strong>Fedora</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Universal Base Image</strong></td>
<td><strong>Knative</strong></td>
</tr>
<tr>
<td>Build</td>
<td>Test coverage</td>
<td>Security</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>MSBuild</td>
<td>JaCoCo</td>
<td>Tenable / Nessus Agents</td>
</tr>
<tr>
<td>CMake</td>
<td>Emma</td>
<td>Fortify</td>
</tr>
<tr>
<td>Maven</td>
<td>Cobertura</td>
<td>Twistlock</td>
</tr>
<tr>
<td>Gradle</td>
<td>codecov</td>
<td>Aqua</td>
</tr>
<tr>
<td>Apache Ant</td>
<td></td>
<td>SonarQBE</td>
</tr>
<tr>
<td><strong>Tests suite</strong></td>
<td><strong>Jenkins (open source)</strong></td>
<td><strong>StackRox</strong></td>
</tr>
<tr>
<td>Cucumber</td>
<td>CloudBees Jenkins</td>
<td>Aporeto</td>
</tr>
<tr>
<td>J-Unit</td>
<td>GitLab</td>
<td>Snort</td>
</tr>
<tr>
<td>Selenium</td>
<td></td>
<td>OWASP ZAP</td>
</tr>
<tr>
<td>TestingWhiz</td>
<td></td>
<td>Contrast Security</td>
</tr>
<tr>
<td>Watir</td>
<td></td>
<td>OpenVAS</td>
</tr>
<tr>
<td>Sahi</td>
<td></td>
<td>Metaspliot</td>
</tr>
<tr>
<td>Zephyr</td>
<td></td>
<td>ThreadFix</td>
</tr>
<tr>
<td>Vagrant</td>
<td></td>
<td>pylint</td>
</tr>
<tr>
<td>AppVerify</td>
<td>Dozens (Need to verify security)</td>
<td>OWASP OpenVAS (check against DISA STIG)</td>
</tr>
<tr>
<td>nosetests</td>
<td></td>
<td>PyLint</td>
</tr>
<tr>
<td>SoapUI</td>
<td></td>
<td>JFrog Xray</td>
</tr>
<tr>
<td>LeanFT</td>
<td></td>
<td>OpenScap (can check against DISA STIG)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OpenControl for compliance documentation</td>
</tr>
</tbody>
</table>

**CI/CD Orchestration**

- Jenkins (open source)
- CloudBees Jenkins
- GitLab

**Jenkins plugins**

- Dozens (Need to verify security).

**Configuration Management / Delivery**

- Puppet
- Chef
- Ansible
- Saltstack

**Security**

- Tenable / Nessus Agents
- Fortify
- Twistlock
- Aqua
- SonarQBE
- Qualys
- StackRox
- Aporeto
- Snort
- OWASP ZAP
- Contrast Security
- OpenVAS
- Metaspliot
- ThreadFix
- pylint
- JFrog Xray
- OpenScap (can check against DISA STIG)
- OpenControl for compliance documentation

**Security (2)**

- Snyk
- Code Climate
- AJAX Spider
- Tanaguru (508 compliance)
- InSpec
- OWASP Dependency-Check
- Burp
- HBSS
- Anchores
- Checkmarx
- SD Elements
- Clair
- Docker Bench Security
- Notary
- Sysdig
- Layered Insight
- BlackDuck
- Nexus IQ/Lifecycle/Firewall

---

*Integrity - Service - Excellence*
# DevSecOps Product Stack (4)

<table>
<thead>
<tr>
<th>Monitoring</th>
<th>Collaboration</th>
<th>Documentation</th>
<th>Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensu</td>
<td>Rocket.Chat</td>
<td>Javadoc</td>
<td>Apache AB</td>
</tr>
<tr>
<td>EFK (Elasticsearch, Fluent, Kibana)</td>
<td>Matter.Most</td>
<td>RDoc</td>
<td>Jmeter</td>
</tr>
<tr>
<td>Splunk</td>
<td>PagerDuty</td>
<td>Sphinx</td>
<td>LoadRunner</td>
</tr>
<tr>
<td>Nagios</td>
<td></td>
<td>Doxygen</td>
<td></td>
</tr>
<tr>
<td>New Relic</td>
<td></td>
<td>Cucumber</td>
<td></td>
</tr>
<tr>
<td>Sentry</td>
<td></td>
<td>phpDocumentator</td>
<td></td>
</tr>
<tr>
<td>Prometheus</td>
<td></td>
<td>Pydoc</td>
<td></td>
</tr>
<tr>
<td>Grafana</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kiali</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Plan</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Jira</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confluence</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rally</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Redmine</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pivotal Tracker</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Secrets</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kubernetes Secrets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vault</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credentials (Jenkins)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CryptoMove</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SSO</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keycloak</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

# Integrity - Service - Excellence
Legacy to DevSecOps => Strangler Pattern

- Martin Fowler describes the Strangler Application:
  - One of the natural wonders of this area are the huge strangler vines. They seed in the upper branches of a fig tree and gradually work their way down the tree until they root in the soil. Over many years they grow into fantastic and beautiful shapes, meanwhile strangling and killing the tree that was their host.

- To get there, the following steps were followed:
  - First, add a proxy, which sits between the legacy application and the user. Initially, this proxy doesn't do anything but pass all traffic, unmodified, to the application.
  - Then, add new service (with its own database(s) and other supporting infrastructure) and link it to the proxy. Implement the first new page in this service. Then allow the proxy to serve traffic to that page (see below).
  - Add more pages, more functionality and potentially more services. Open up the proxy to the new pages and services. Repeat until all required functionality is handled by the new stack.
  - The monolith no longer serves traffic and can be switched off.

Recommended Videos (Part 1)

- Watch our playlists, available at different expertise levels and continuously augmented!
- Kafka / KSQL (message bus, pub/sub, event driven):
  - Beginners: https://www.youtube.com/playlist?list=PLSIv_F9TtLlzz0zt03Ludtid7icrXBesg
  - Intermediate: https://www.youtube.com/playlist?list=PLSIv_F9TtLixXX0oCzt7laO6mD61UIQw
  - Advanced: N/A
- Kubernetes
  - Beginners: https://www.youtube.com/playlist?list=PLSIv_F9TtLlydFzQzkYYDdQK7k5cEKubQ
  - Intermediate: https://www.youtube.com/playlist?list=PLSIv_F9TtLlx8dSFH_jFLK40Tt7KUXTN
  - Advanced: https://www.youtube.com/playlist?list=PLSIv_F9TtLlytdAJiVqbHucWOvn5LrTNW
Self-Learning (2)

- **Recommended Videos (Part 2)**
  - Watch our playlists, available at different expertise levels and continuously augmented!
  - **Service Mesh**
    - Beginners: [https://www.youtube.com/playlist?list=PLSIv_F9TtLixtC4rDIMQ8QiG5UBCjz7VH](https://www.youtube.com/playlist?list=PLSIv_F9TtLixtC4rDIMQ8QiG5UBCjz7VH)
    - Intermediate: [https://www.youtube.com/playlist?list=PLSIv_F9TtLlwWK_Y_Cas8Nyw-DsdbH6v](https://www.youtube.com/playlist?list=PLSIv_F9TtLlwWK_Y_Cas8Nyw-DsdbH6v)
    - Advanced: [https://www.youtube.com/playlist?list=PLSIv_F9TtLix8VW2MFONMRwS_-2rSJwdn](https://www.youtube.com/playlist?list=PLSIv_F9TtLix8VW2MFONMRwS_-2rSJwdn)
  - **Microservices**
    - Beginners: [https://www.youtube.com/playlist?list=PLSIv_F9TtLiZ_U2_RaONTGyLkz0lh-A_L](https://www.youtube.com/playlist?list=PLSIv_F9TtLiZ_U2_RaONTGyLkz0lh-A_L)
    - Intermediate: [https://www.youtube.com/playlist?list=PLSIv_F9TtLxqjuAXxoRmjvspaEE8L2cB](https://www.youtube.com/playlist?list=PLSIv_F9TtLxqjuAXxoRmjvspaEE8L2cB)
    - Advanced: [https://www.youtube.com/playlist?list=PLSIv_F9TtLw4CF4F4t3gVV3j0512CMsu](https://www.youtube.com/playlist?list=PLSIv_F9TtLw4CF4F4t3gVV3j0512CMsu)
Recommended Books

- **A Seat at the Table** – by Mark Schwartz (former CIO of USCIS, leader in Agile)
  
  This book is highly recommended for ALL leadership as it is not technical but focused on the challenges around business, procurement and how leadership can enable DevOps across the organization and remove impediments.

- **The Phoenix Project** – by the founders of DevOps

- **The DevOps Handbook** – by Gene Kim, Patrick Debois.

For those who drive to work like me (for hours), please note that these books are available as Audiobooks.
Thank You!

Nicolas Chaillan
Chief Software Officer, U.S. Air Force
usaf.cso@mail.mil
Nicolas Chaillan is the Chief Software Officer at the U.S. Air Force and the Co-Lead for the DoD Enterprise DevSecOps Initiative.

He is the former Special Advisor for Cloud Security and DevSecOps at OSD, A&S.

He was the Special Advisor for Cybersecurity at the Department of Homeland Security and the Chief Architect for Cyber.gov, the new robust, innovative and holistic .Gov cyber security architecture for all .gov agencies.

Chaillan is a technology entrepreneur, software developer, cyber expert and inventor. He is recognized as one of France’s youngest entrepreneurs after founding his first company at 15 years of age.

With 19 years of international tech, entrepreneurial and management experience, Chaillan is the founder of more than 12 companies, including AFTER-MOUSE.COM, Prevent-Breach, anyGuest.com, and more.

Over the last eight years alone, he has created and sold over 180 innovative software products to 40 Fortune 500 companies.

Chaillan is recognized as a pioneer of the computer language PHP.