

# *Headquarters U.S. Air Force*

---

*Integrity - Service - Excellence*



**U.S. AIR FORCE**

---

## **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**



**U.S. AIR FORCE**

# ***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**

A high-angle, top-down view of two F-16 fighter jets flying in formation over a dark, mountainous landscape. The jets are silver with black markings and are equipped with various missiles and fuel tanks. The lead jet is positioned higher and further into the frame, while the second jet follows closely behind and to the side. The terrain below is rugged and dark, with some lighter patches indicating rocky or sparsely vegetated areas. The overall tone of the image is dramatic and emphasizes the precision and teamwork of the flight.

**Work as a Team!**



**A Large Team!**

An aerial photograph of a military airfield. In the center, a large, dark blue, V-shaped stealth bomber (B-2 Spirit) is parked on a concrete tarmac. To its left and right are several smaller, light blue fighter jets (F-35). A small black service vehicle is positioned below the bomber. The tarmac is marked with yellow and black striped lines. The text "With Various Technologies" is overlaid in white, bold font across the center of the image.

**With Various Technologies**



**Bring It With Us!**

A dramatic low-angle shot of a rocket launch. The rocket is positioned vertically in the center, ascending into a cloudy sky. A massive, bright orange and yellow plume of fire and white smoke billows from the base, filling the lower two-thirds of the frame. To the right, a tall, yellow lattice service tower stands against the sky. The overall scene is one of immense power and scale.

**Even To Space!**



**With a Few Sensors!**

# With Their Help!





U.S. AIR FORCE

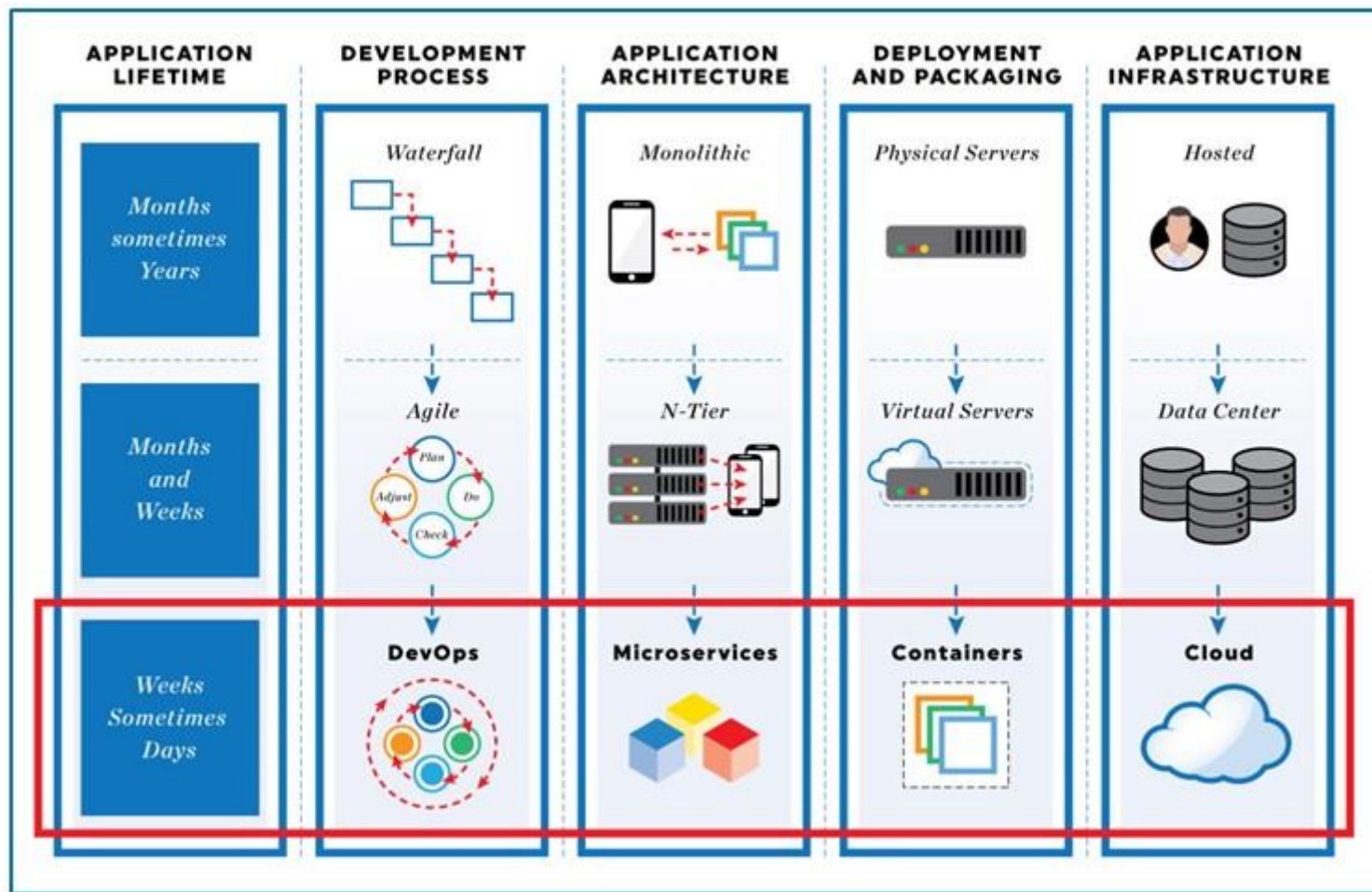
# ***What is the DoD Enterprise DevSecOps Initiative?***

- Joint Program with OUSD(A&S), DoD CIO, U.S. Air Force, DISA and the Military Services.
- 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/> and <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



U.S. AIR FORCE

# From Waterfall to DevSecOps





U.S. AIR FORCE

# 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”***

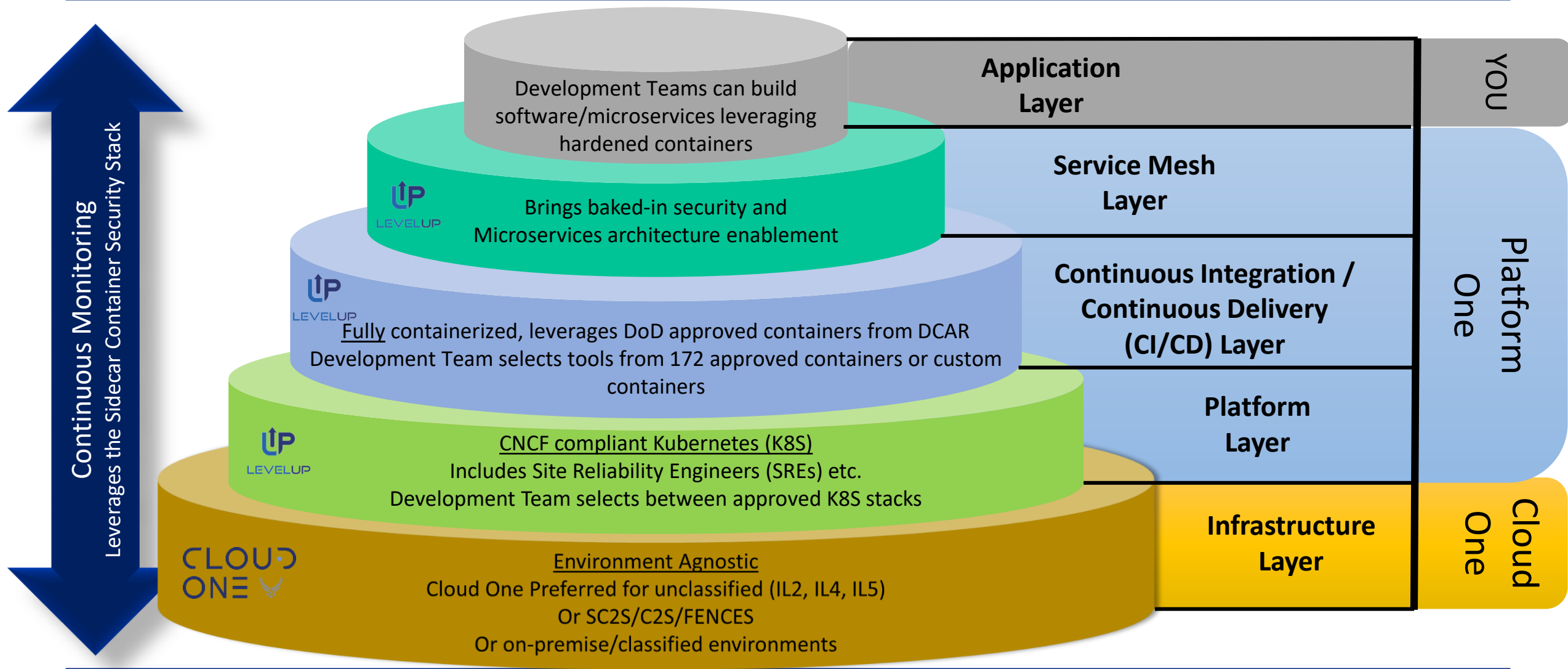
---

- 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.

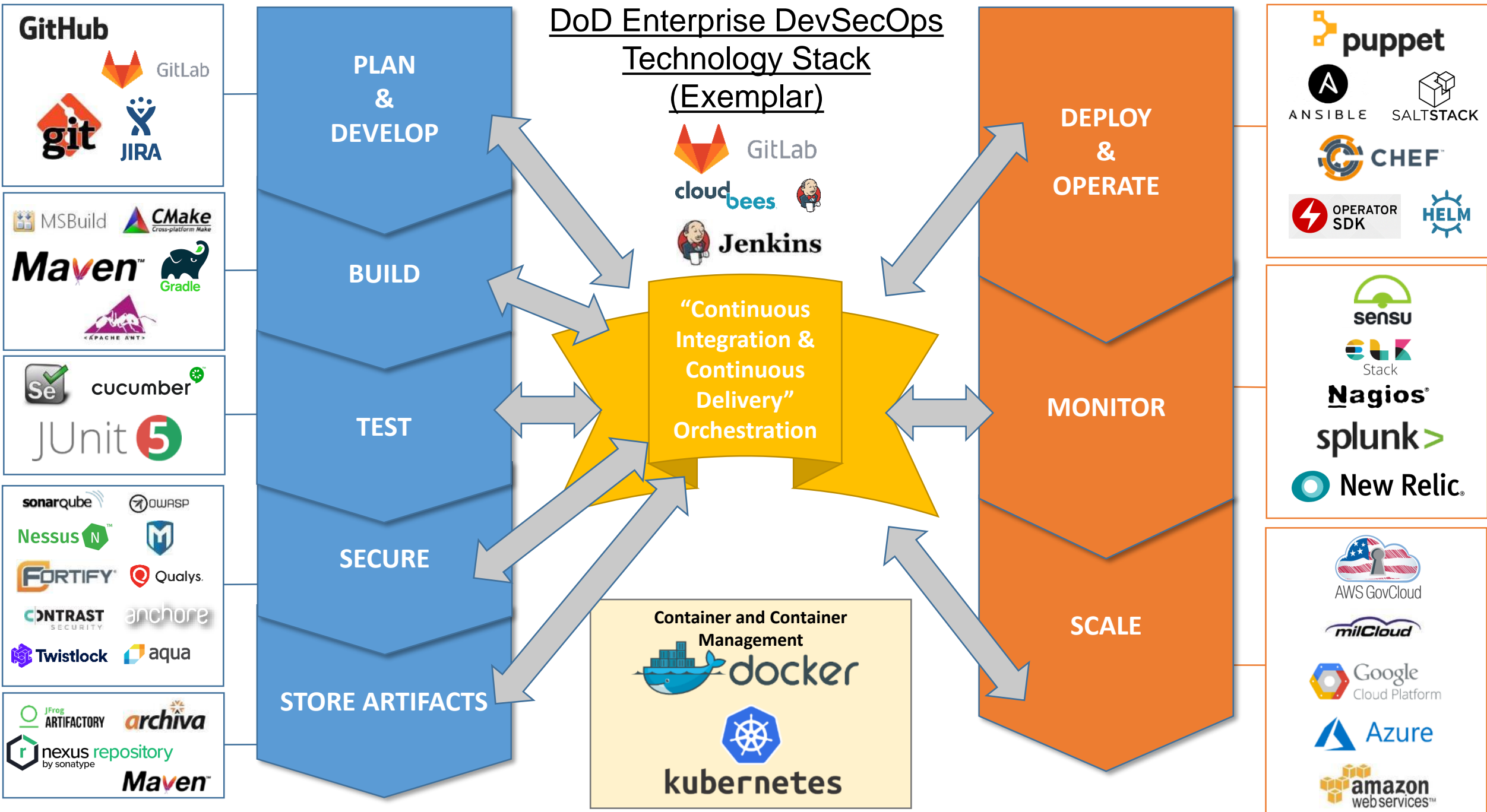


U.S. AIR FORCE

# Understanding the DevSecOps Layers



*Integrity - Service - Excellence*





**U.S. AIR FORCE**

# ***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

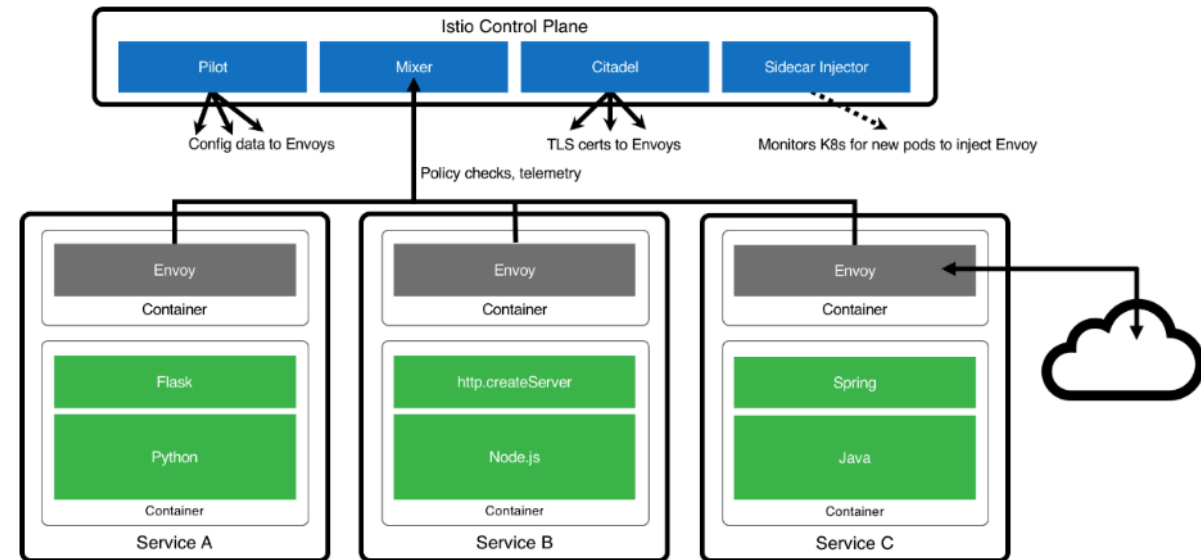


U.S. AIR FORCE

# Microservices Architecture (ISTIO)

- 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...

## Managing Microservices With Istio





**U.S. AIR FORCE**

# Cloud One

- 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.



**U.S. AIR FORCE**

---

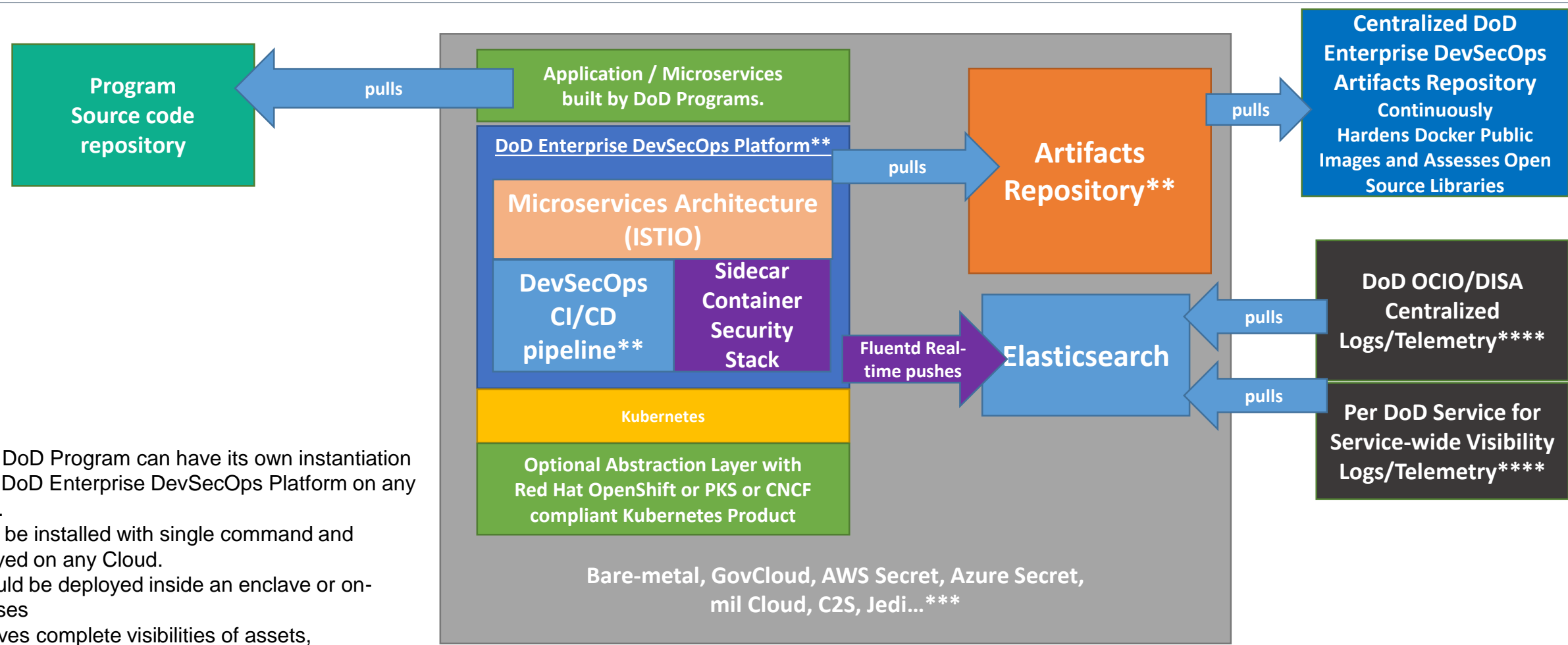


# **DoD Enterprise DevSecOps Architecture**

---

*Integrity - Service - Excellence*

# 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.



**U.S. AIR FORCE**

---



# **DevSecOps Platform Stack (continuously evolving)**

---

*Integrity - Service - Excellence*



U.S. AIR FORCE

# DevSecOps Product Stack (1)

|   |  |  |   |
|---|--|--|---|
| <b>Source Repository</b><br>GitHub Government<br>GitLab   | <b>API Gateways</b><br>Kong<br>Azure API<br>AWS API<br>Axway<br>3Scale<br>Apigee<br>ISTIO (service mesh) | <b>Programming Languages</b><br>C/C++<br>C#/.NET<br>.NET Core<br>Java<br>PHP<br>Python<br>Groovy<br>Ruby<br>R<br>Rust<br>Scala<br>Perl<br>Go<br>Node.JS<br>Swift | <b>Databases</b><br>SQL Server<br>MySQL<br>PostgreSQL<br>MongoDB<br>SQLite<br>Redis<br>Elasticsearch<br>Oracle<br>etcd<br>Hadoop/HDInsight<br>Cloudera<br>Oracle Big Data<br>Solr<br>Neo4J<br>Memcached<br>Cassandra<br>MariaDB<br>CouchDB<br>InfluxDB (time) |
| <b>Container Management technologies:</b><br>Kubernetes<br>Openshift<br>VMWare Tanzu<br>PKS<br>OKD<br>Rancher (K8S only)<br>D2IQ (K8S only)<br>Docker EE (K8S only) | <b>Artifacts</b><br>Artifactory<br>Nexus<br>Maven<br>Archiva<br>S3 bucket                                |  |   |
| <b>Container Packagers:</b><br>Helm<br>Kubernetes Operators   |  |  |   |



# DevSecOps Product Stack (2)

|  |  |  |
|--|--|--|
| <b>Message bus/Streams</b><br>Kafka<br>Flink<br>Nats<br>RabbitMQ<br>ActiveMQ<br><br><b>Proxy</b><br>Oauth2 proxy<br>nginx ldap auth proxy<br>openldap<br>HA Proxy<br><br><b>Visualization</b><br>Tableau<br>Kibana | <b>Logs</b><br>Logstash<br>Splunk Forwarder<br>Fluentd<br>Syslogd<br>Filebeat<br>rsyslog<br><br><b>Webservers</b><br>Apache2<br>Nginx<br>IIS<br>Lighttpd<br>Tomcat | <b>Docker base images OS:</b><br>Alpine<br>Busybox<br>Ubuntu<br>Centos<br>Debian<br>Fedora<br>Universal Base Image<br><br><b>Serverless</b><br>Knative |
|--|--|--|



**U.S. AIR FORCE**

# DevSecOps Product Stack (3)

|   |   |  |   |
|---|---|--|---|
| <b>Build</b><br>MSBuild<br>CMake<br>Maven<br>Gradle<br>Apache Ant | <b>Test coverage</b><br>JaCoCo<br>Emma<br>Cobertura<br>codecov<br><br><b>CI/CD Orchestration</b><br>Jenkins (open source)<br>CloudBees Jenkins<br>GitLab<br><br><b>Jenkins plugins</b><br>Dozens (Need to verify security).<br><br><b>Configuration Management / Delivery</b><br>Puppet<br>Chef<br>Ansible<br>Saltstack | <b>Security</b><br>Tenable / Nessus Agents<br>Fortify<br>Twistlock<br>Aqua<br>SonarQBE<br>Qualys<br>StackRox<br>Aporeto<br>Snort<br>OWASP ZAP<br>Contrast Security<br>OpenVAS<br>Metasploit<br>ThreadFix<br>pylint<br>JFrog Xray<br>OpenSCAP (can check against DISA STIG)<br>OpenControl for compliance documentation | <b>Security (2)</b><br>Snyk<br>Code Climate<br>AJAX Spider<br>Tanaguru (508 compliance)<br>InSpec<br>OWASP Dependency-Check<br>Burp<br>HBSS<br>Anchore<br>Checkmarx<br>SD Elements<br>Clair<br>Docker Bench Security<br>Notary<br>Sysdig<br>Layered Insight<br>BlackDuck<br>Nexus IQ/Lifecycle/Firewall |
|---|---|--|---|



**U.S. AIR FORCE**

# DevSecOps Product Stack (4)

## Monitoring

Sensu  
EFK (Elasticsearch, Fluentd, Kibana)  
Splunk  
Nagios  
New Relic  
Sentry  
Prometheus  
Grafana  
Kiali

## Collaboration

Rocket.Chat  
MatterMost  
PagerDuty

## Plan

Jira  
Confluence  
Rally  
Redmine  
Pivotal Tracker

## Secrets

Kubernetes Secrets  
Vault  
Credentials (Jenkins)  
CryptoMove

## SSO

Keycloak

## Documentation

Javadoc  
RDoc  
Sphinx  
Doxygen  
Cucumber  
phpDocumentator  
Pydoc

## Performance

Apache AB  
Jmeter  
LoadRunner



U.S. AIR FORCE

# 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.
- Learn more: <https://www.ibm.com/developerworks/cloud/library/cl-strangler-application-pattern-microservices-apps-trs/index.html> and <https://www.michielrook.nl/2016/11/strangler-pattern-practice/>



## ■ 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=PLSlv\\_F9TtLIzz0zt03Ludtid7icrXBesg](https://www.youtube.com/playlist?list=PLSlv_F9TtLIzz0zt03Ludtid7icrXBesg)
  - Intermediate: [https://www.youtube.com/playlist?list=PLSlv\\_F9TtLIxxXX0oCzt7laO6mD61UIQw](https://www.youtube.com/playlist?list=PLSlv_F9TtLIxxXX0oCzt7laO6mD61UIQw)
  - Advanced: N/A
- Kubernetes
  - Beginners: [https://www.youtube.com/playlist?list=PLSlv\\_F9TtLIydFzQzkYYDdQK7k5cEKubQ](https://www.youtube.com/playlist?list=PLSlv_F9TtLIydFzQzkYYDdQK7k5cEKubQ)
  - Intermediate: [https://www.youtube.com/playlist?list=PLSlv\\_F9TtLIx8dSFH\\_jFLK40Tt7KUXTN](https://www.youtube.com/playlist?list=PLSlv_F9TtLIx8dSFH_jFLK40Tt7KUXTN)
  - Advanced: [https://www.youtube.com/playlist?list=PLSlv\\_F9TtLIytdAJiVqbHucWOvn5LrTNW](https://www.youtube.com/playlist?list=PLSlv_F9TtLIytdAJiVqbHucWOvn5LrTNW)



**U.S. AIR FORCE**

# ***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=PLSlv\\_F9TtLIxtC4rDIMQ8QiG5UBCjz7VH](https://www.youtube.com/playlist?list=PLSlv_F9TtLIxtC4rDIMQ8QiG5UBCjz7VH)
  - Intermediate: [https://www.youtube.com/playlist?list=PLSlv\\_F9TtLIwWK\\_Y\\_Cas8Nyw-DsdbH6vl](https://www.youtube.com/playlist?list=PLSlv_F9TtLIwWK_Y_Cas8Nyw-DsdbH6vl)
  - Advanced: [https://www.youtube.com/playlist?list=PLSlv\\_F9TtLIx8VW2MFONMRwS\\_-2rSJwdn](https://www.youtube.com/playlist?list=PLSlv_F9TtLIx8VW2MFONMRwS_-2rSJwdn)
- Microservices
  - Beginners: [https://www.youtube.com/playlist?list=PLSlv\\_F9TtLiz\\_U2\\_RaONTGYLkz0lh-A\\_L](https://www.youtube.com/playlist?list=PLSlv_F9TtLiz_U2_RaONTGYLkz0lh-A_L)
  - Intermediate: [https://www.youtube.com/playlist?list=PLSlv\\_F9TtLIxqjuAXxoRMjvspaEE8L2cB](https://www.youtube.com/playlist?list=PLSlv_F9TtLIxqjuAXxoRMjvspaEE8L2cB)
  - Advanced: [https://www.youtube.com/playlist?list=PLSlv\\_F9TtLIw4CF4F4t3gVV3j0512CMsu](https://www.youtube.com/playlist?list=PLSlv_F9TtLIw4CF4F4t3gVV3j0512CMsu)



## ■ 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.



**U.S. AIR FORCE**

---



# Thank You!

Nicolas Chaillan  
Chief Software Officer, U.S. Air Force

[usaf.cso@mail.mil](mailto:usaf.cso@mail.mil)

---

*Integrity - Service - Excellence*



**U.S. AIR FORCE**

---



# Backup Slides

---

*Integrity - Service - Excellence*



**U.S. AIR FORCE**

# ***Nicolas Chaillan - Presenter***



**Chief Software Officer**

- Nicolas M. 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.

— 2018 —  
OFFICIAL MEMBER

**Forbes**  
Technology  
Council