Headquarters U.S. Air Force

Integrity - Service - Excellence

How did the Department of Defense move to Kubernetes and Istio?

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

V2.4 – UNCLASSFIED

Must Rapidly Adapt To Challenges


Work as a Team!

A Large Team!


With Various Technologies

Bring It With Us!


Even To Space!

With a Few Sensors!

With Their Help!

What is the DoD Enterprise DevSecOps Initiative?

- Joint Program with OUSD(A&S), DoD CIO, U.S. Air Force, DISA and the Military Services.
- Bringing **Enterprise IT Capabilities with Cloud One and Platform One** – Cloud and DevSecOps as Managed Services capabilities, on-boarding and support! **Brings timeliness, modularity and enables reuse.**
- Technology:
  - **Avoid vendor lock-in** at the Infrastructure and Platform Layer by leveraging **FOSS with Kubernetes and OCI containers (reusable lego blocks)**,
  - Created **Iron Bank**, 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://repo1.dsop.io/dsop/ and https://ironbank.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 (Istio), baked-in security
  - Leveraging KNative to avoid lock-in to Cloud provider Serverless stacks and Kubeflow for AI/ML/Deep Learning
- 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: https://www.dau.edu/cop/it/DAU%20Sponsored%20Documents/Contracting%20Considerations%20for%20Agile%20Solutions%20v1.0.pdf

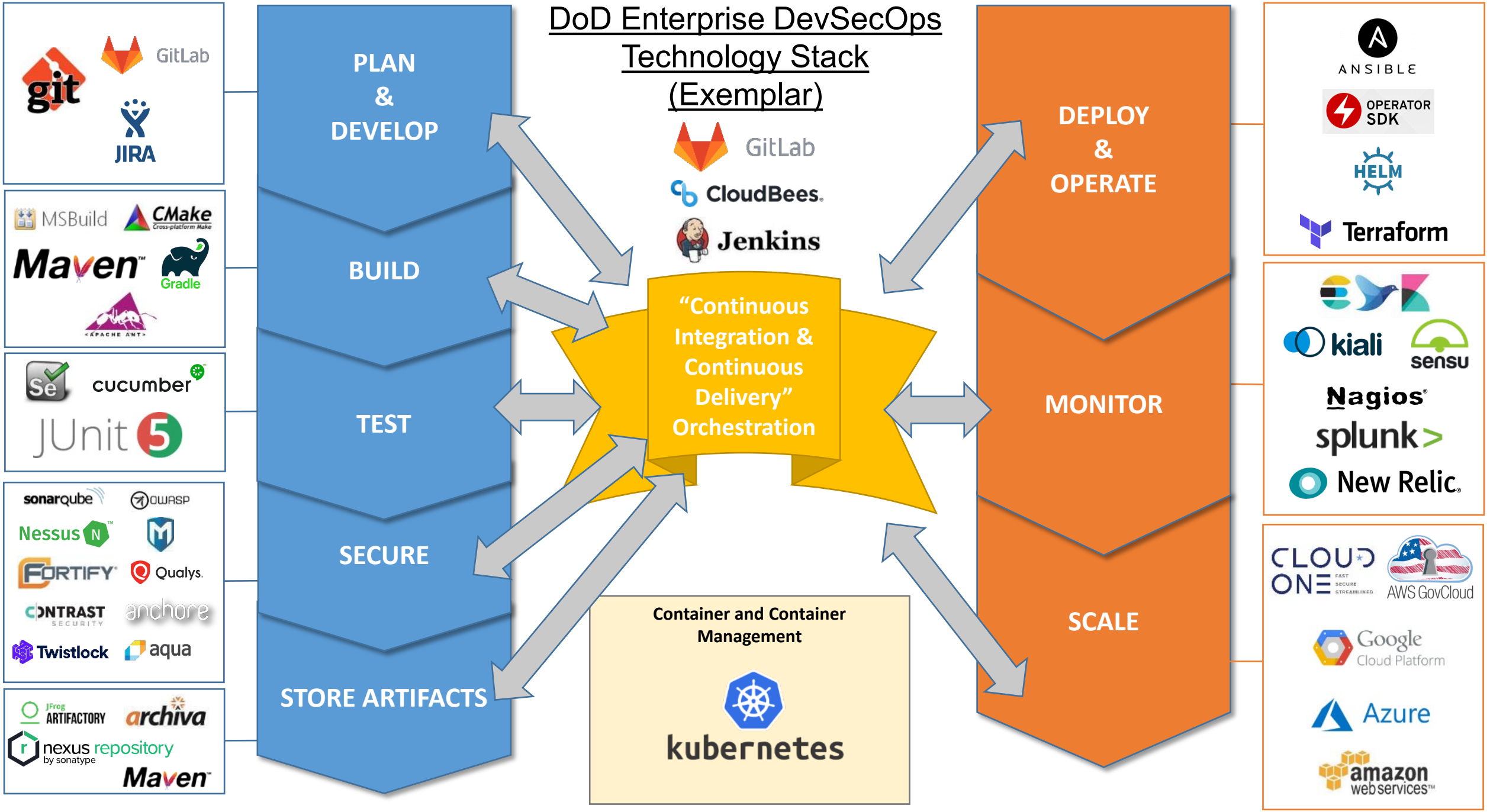
CSO Website – Continuously Updated!

- Want to find information about the DevSecOps initiative and the CSO?
  - **Our latest documents/videos:** https://software.af.mil/dsop/documents/
  - **Our latest training videos/content at:** https://software.af.mil/training/
  - **Platform One Services:** https://software.af.mil/dsop/services/
  - More information about :
    - Platform One On Boarding: https://software.af.mil/team/platformone/
    - Cloud One: https://software.af.mil/team/cloud-one/
    - Repo One: https://repo1.dsop.io
    - Iron Bank: https://ironbank.dsop.io
    - Registry One: https://registry1.dsop.io
    - DevStar: https://software.af.mil/dsop/dsop-devstar/
    - Our Events/News: https://software.af.mil/events/
    - .mil only IL4 Chat (MatterMost): https://chat.collab.cdl.af.mil/

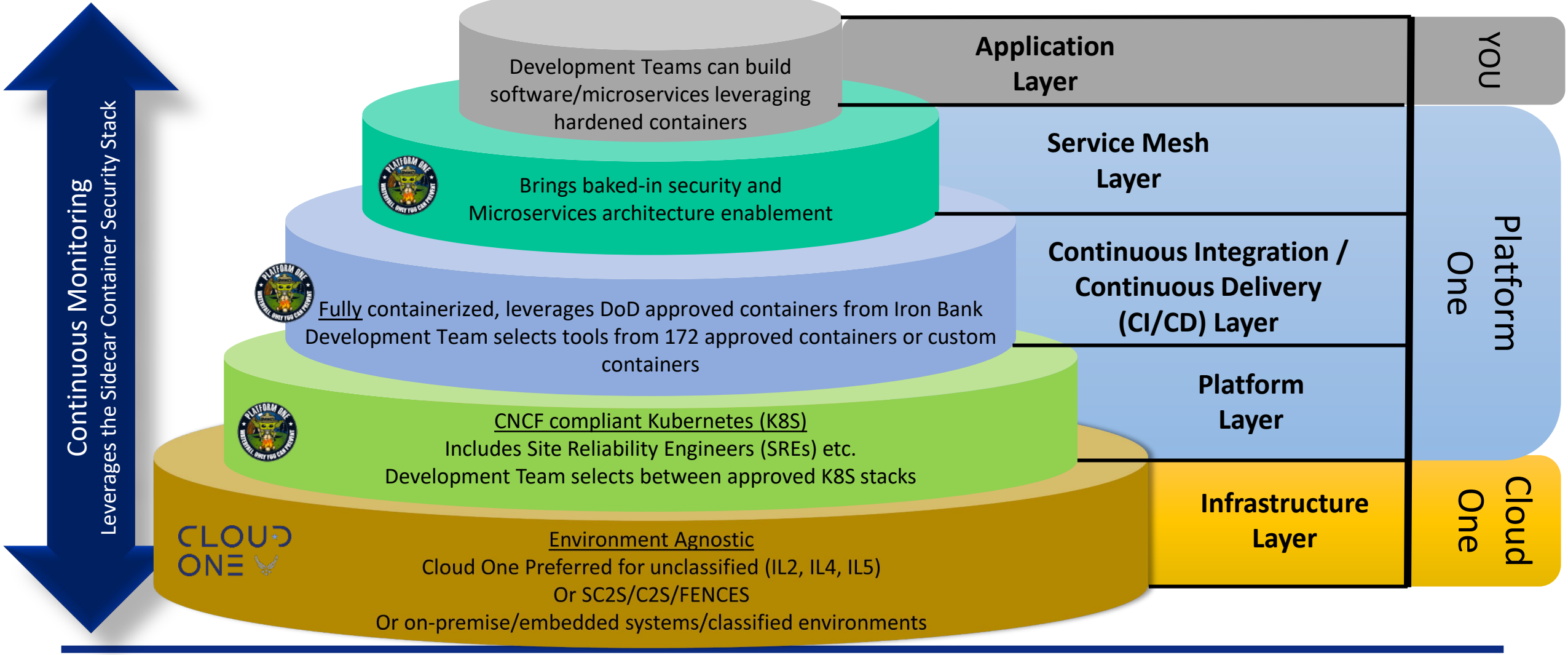
Why Kubernetes / Containers?

- One of the most critical aspect of the DevSecOps initiative is to ensure we **avoid any vendor lock-in** so the DoD mandated:
  - **Open Container Initiative (OCI) containers** (no lock-in to containers/container runtimes/builders)
  - **Cloud Native Computing Foundation (CNCF) Kubernetes compliant cluster** for container orchestration, no lock-in to orchestration options/networking/storage APIs.
- SaaS vs COTS/FOSS containers:
  - SaaS requires FedRAMP certification and will limit you to unclassified environments (IL2 for FedRAMP moderate) which doesn't satisfy most needs for DoD programs. Often takes up to 1 year.
  - COTS/FOSS as containers: can be sold as a managed service deployed in DoD cloud environments (including classified clouds) on Kubernetes and can be accredited at multiple classification levels, within weeks, by following the container hardening guide and vendor on-boarding process!
  - Get your container(s) onboarded on Iron Bank for DoD wide reciprocity? https://repo1.dsop.io/dsop/dccscr/tree/master/contributor-onboarding
- Containers are **immutable** and will allow the DoD to centrally accredit and harden containers (FOSS, COTS, GOTS) (think of a true gold disk concept but that actually scale and works).
- Continuous Monitoring is a critical piece of our Continuous ATO model and the Sidecar Container Security Stack (SCSS) brings those capabilities with Behavior, Zero Trust and CVE scanning.
- Kubernetes will provide:
  - **Resiliency**: Self-healing so containers that crash can automatically be restarted,
  - **Baked-in security**: thanks to **automatic injection** of our Sidecar Container Security Stack (SCSS) to any K8S cluster with Zero Trust,
  - **Adaptability**: containers are "Lego" blocks and can be swapped with no downtime thanks to load balancing and modern routing (A/B testing, canary release etc.),
  - **Automation**: thanks to our Infrastructure as Code (IaC) and GitOps model,
  - **Auto-scaling**: if load requires more of the same container, K8S will automatically scale based on compute/memory needs,
  - **Abstraction layer**: ensure we don't get locked-in to Cloud APIs or to a specific platform as K8S is managed by CNCF and dozens of products are compliant with its requirements.

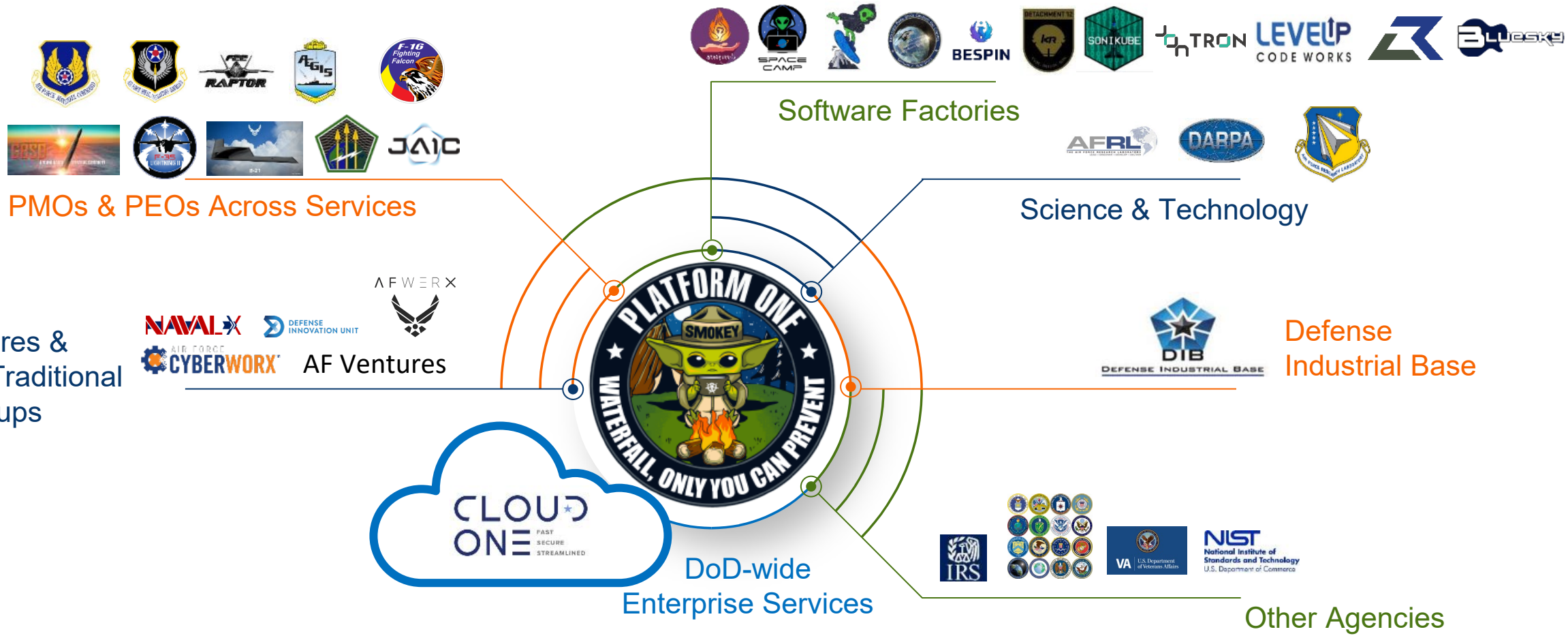
DoD Enterprise DevSecOps Technology Stack (Exemplar)



Understanding the DevSecOps Layers

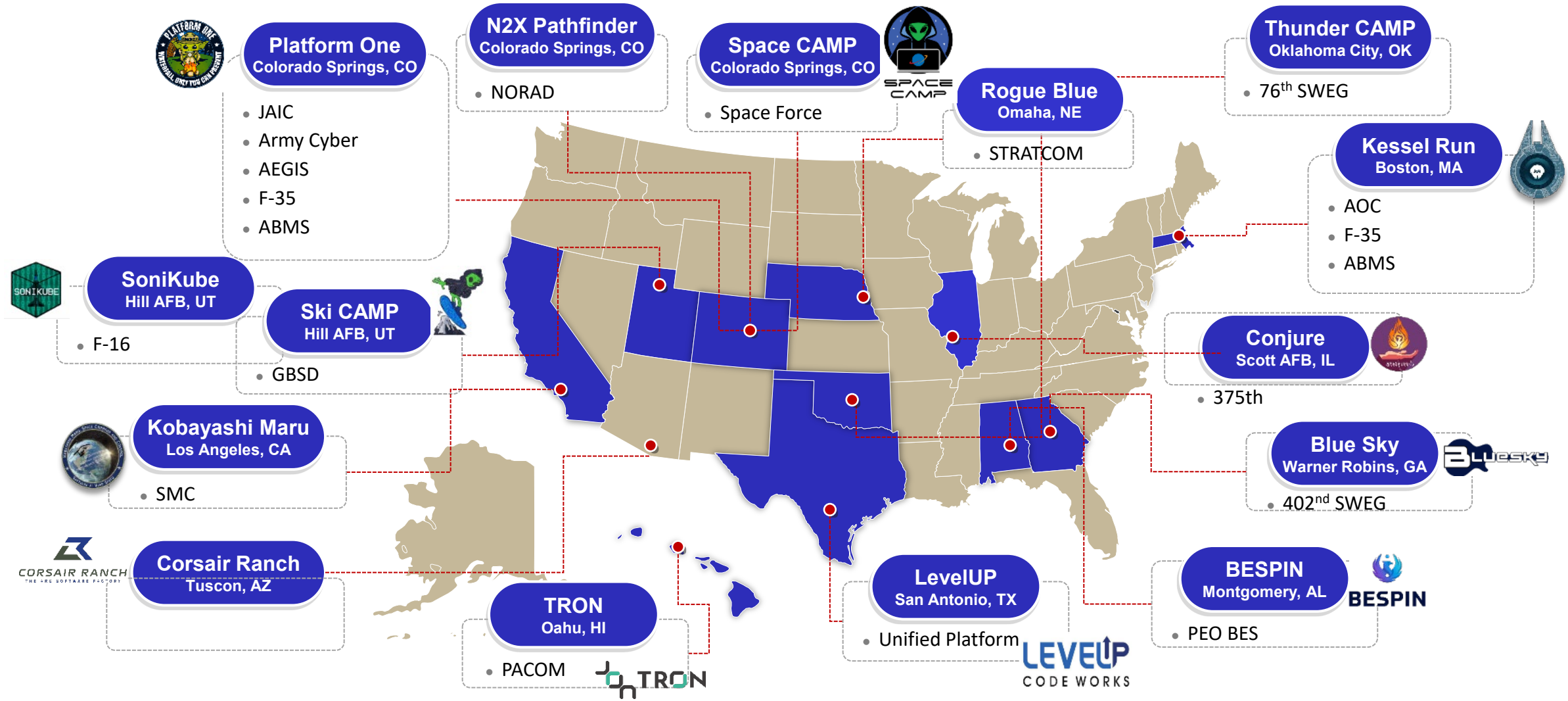


Software Ecosystem
Multiple Innovation Hubs – One Platform



Software Ecosystem

Multiple Innovation Hubs, One Platform



Platform One Services

- **Full details at:** https://software.af.mil/dsop/services/
- **Repo One – DoD Centralized Container Source Code Repository (DCCSCR)**
  - Container source code, Infrastructure as Code, K8S distributions, etc.
  - Repo One is the central repository for the source code to create hardened and evaluated containers for the Department of Defense. It also includes various source code open-source products and infrastructure as code used to harden Kubernetes distributions.
  - Repo One is currently operated at https://repo1.dsop.io/dsop/.
- **Iron Bank – DoD Centralized Artifacts Repository (DCAR)**
  - 130+ containers available, 250 containers by end of 2020.
  - Iron Bank is the DoD repository of digitally signed, binary container images that have been hardened according to the Container Hardening Guide coming from Iron Bank. Containers accredited in Iron Bank have DoD-wide reciprocity across classifications.
  - Iron Bank is currently operated at https://ironbank.dsop.io/.

Platform One Services (continued)

- **DevSecOps Platform (DSOP)**
  The DSOP is a collection of approved, hardened Cloud Native Computer Foundation (CNCF)-compliant Kubernetes distributions, infrastructure as code playbooks, and hardened containers that implement a DevSecOps platform compliant with the DoD Enterprise DevSecOps Reference Design, and its source code is hosted on Repo One.
- Infrastructure as Code (IaC) Repositories:
  - Platform One IaC: https://repo1.dsop.io/platform-one
  - D2IQ: https://repo1.dsop.io/platform-one/distros/d2iq
  - Rancher Federal: https://repo1.dsop.io/platform-one/distros/rancher-federal
  - OpenShift 4.x: https://repo1.dsop.io/platform-one/distros/red-hat
- Kubernetes CNCF-compliant currently supported are: OpenShift 4.x, Kubernetes upstream, D2IQ Konvoy and Rancher Federal RKE. Kubernetes CNCF-compliant to be supported soon: VMWare Tanzu and Oracle Kubernetes.
- Platform One will be supporting the following environments:
  - Amazon Web Services (AWS) IL-2, IL-5, S, S-SAP (when available), TS/SCI, and TS-SAP (FENCES), AWS Outpost
  - Azure IL-2, IL-5, S (when available), S-SAP (when available), Azure Stack
  - On-premise / Edge - VMWare vSphere
- The DSOP includes the various mandated containers of the Reference Design including Elasticsearch, Fluentd, and Kibana (EFK), Sidecar Container Security Stack (SCSS), etc.

Platform One Services (continued)

- **Party Bus – ABMS All Domain Common Environment: Platform One Shared Enterprise Environments (Multi-Tenant) (for Development, Test and Production)**
  - These are environments that benefit from the Platform One Continuous ATO, hosted on Cloud One, SC2S and C2S managed by the Platform One team as multi-tenant environments. Perfect for smaller/medium sized teams. They provide Continuous Integration/Continuous Delivery (CI/CD) and various development tools/capabilities.
  - Impact Level (IL)-2, IL-5, Secret, and TS/SCI environments exist or are in development (pay per user model ($2,000/user/month))
- **Big Bang: Platform One Dedicated DevSecOps Environments**
  - Build, deliver and operate custom Infrastructure as Code and Configuration as Code with the deployment of dedicated environments at various classification levels with CI/CD pipelines and c-ATO. Perfect for large teams/programs that need a dedicated enclave (cost per DevSecOps environment).
  - Build and deliver new hardened containers as needed for program specific software (pay per use/container).

Platform One Services (continued)

- **Cloud Native Access Point (CNAP)**
  - The Cloud Native Access Point is available on Cloud One to provide access to Development, Testing, Staging and Production enclaves at **IL-2, IL-4 and IL-5** that using Platform One DevSecOps environments by using an internet-facing Cloud-native Zero trust environment.
  - The CNAP enables access to **VDI options** and allows **thick endpoints (incl. mobile)**, including BYOD, government owned and contractor owned devices to connect at various impact level while enforcing device state/security.
  - Brings Single Sign On with various DoD PKI options and IL2 MFA options.
  - CNAP diagram: https://software.af.mil/wp-content/uploads/2020/04/CNAP-Data-Flow-Diagram-v5.3-NC.pptx

Platform One Services (continued)

- **Platform One Training/On-Boarding Options**
  - Check out the CSO DevSecOps / DAU training at https://software.af.mil/training/
  - Virtual Platform One Learning Hub that provides self service on-boarding [June 2020 Launch]
  - 1-day training Session: Introduction to DevSecOps. Overview and understanding of the vision and activities. [June 2020 Virtual Launch]
  - A 3 day Platform One Platform Workshop. Hands on code and User-Centered Design (UCD) to create your first Platform One DevSecOps pipelines and deploy a “push button” DoD DevSecOps software factory. [Currently Available]
  - A 6-week full on-boarding, that concludes with own CI/CD pipeline and Minimum Viable Product (MVP) ready for production [Currently Available]
  - A 2-month full on-boarding, that concludes with your platform team being able to support your own DevSecOps applications for development and production [July 2020 Virtual Launch]
  - Customized training options (both at our locations or on your premises) (pay per use).

Platform One Services (continued)

- **Platform One DevSecOps Managed Tools**
  - Platform One Enterprise Chat: provides a collaboration solution suitable for connecting developer teams (pay per use): IL4 (.mil email only) https://chat.collab.cdl.af.mil/
  - Platform One Party Bus (pay per use)
  - Platform One Multi-Level Security Data Transfer (CDS/Diode) (pay per use)
    - Unclassified to Secret (or S-SAR)
    - Unclassified to TS (or TS-SAR)
  - Platform One Stack Exchange: knowledge sharing service for software developers and engineers. (pay per use)

- **Platform One Cybersecurity/Pen-testing Services**
  - Ability to pen-test a DevSecOps environment at various classifications level (pay per use)

DevSecOps Basic Ordering Agreements (BOAs) – Contract Vehicles

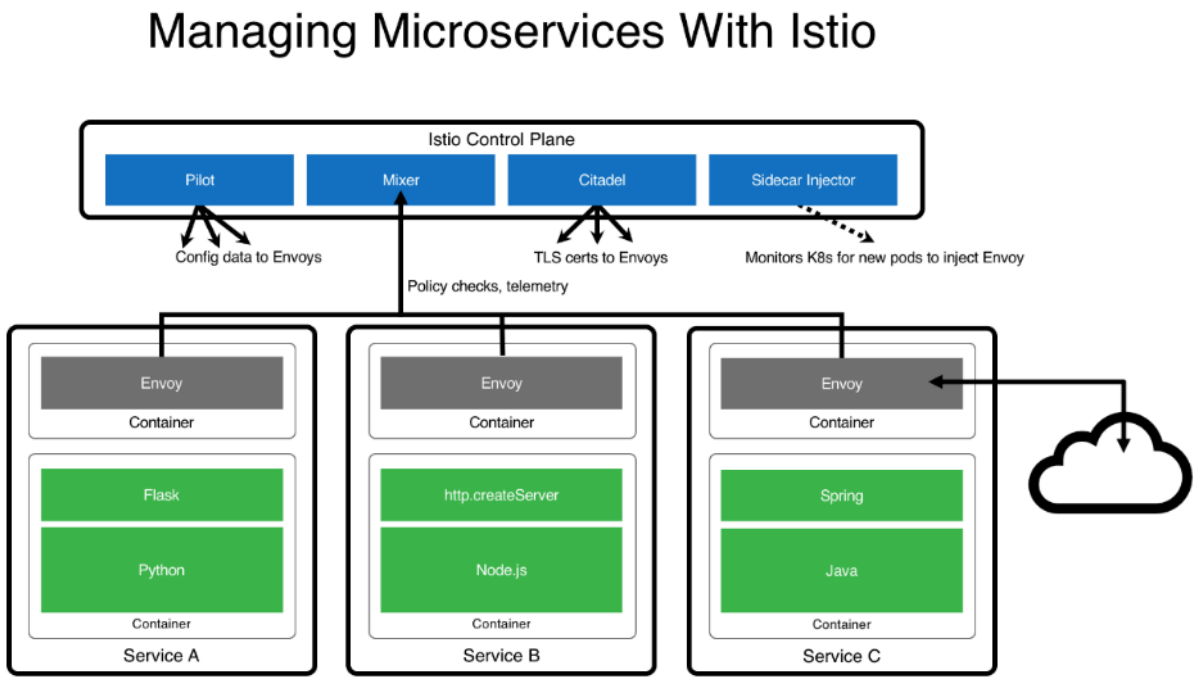
- **BOA 1: Cloud Services**
  - Services to develop and deploy accredited, integrated and tested code at multiple classification levels and hybrid cloud architectures
  - Awarded 1 Nov 2019, 27 companies on-boarded
- **BOA 2: DevSecOps Pipeline and Platform Integration and Licensing Services**
  - DevSecOps pipeline and platform integration and licensing service to support a wide collection of software and programming tools supporting the CI/CD of software products
  - Awarded 1 Nov 2019, 9 companies on-boarded
- **BOA 3: Software DevSecOps Services**
  - Technical services of full-stack DevSecOps engineers, infrastructure engineers, and other key personnel
  - Awarded 15 Jan 2020, 19 companies on-boarded

Key "DevSecOps" Ingredients

- **Abstracted**: to avoid drifts, be agnostic to environment (Cloud/on-premise/classified/disconnected…) and prevent lock-ins with Cloud or Platform layers, we leverage CNCF compliant Kubernetes and OCI compliant containers - open source stacks with U.S eyes on code and continuous scanning,
- **GitOps / Infrastructure as Code (IaC):** no drift, everything is code (including configuration, networking etc.) Instantiate entire stack automatically,
- **Continuous Integration/Continuous Delivery pipeline (CI/CD)**: fully containerized and using Infrastructure as Code (IaC),
- **Hardened Containers**: hardened "Lego blocks" to bring options to development teams (one size fits all lead to shadow IT)
- **Software Testing**: mandated high test coverage,
- **Baked-in Security**: mandated static/dynamic code analysis, container security, bill of material (supply chain risk) etc.
- **Continuous Monitoring:**
  - **Centralized logging and telemetry**,
  - Automated alerting,
  - **Zero trust**, leveraging Service Mesh as Sidecar (part of SCSS), down to the container level,
  - **Behavior detection** (automated prevention),
  - CVE scanning,
- **Chaos engineering**: Dynamically kills/restarts container with moving target defense.

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…



LEVEL UP CODE WORKS

"Infrastructure as Code" Benefits

The "Infrastructure as Code" concept is a critical DevSecOps ingredient to ensure that production environments do not drift from development/testing environments. No human should make changes in production environments. Changes should only be made in source code and redeployed by the CI/CD pipeline.

- No drift between environments, whether classified/disconnected/Cloud/on-premise,
- Immutable,
- Replicable,
- Automated,
- No human in production environments: reduces attack surface (disable SSH etc.), insider threat and configuration drifts,
- Everything is code: including playbooks, networking, tests, configuration etc.

What is GitOps?

- Based on Infrastructure as Code concepts, makes Git the single source of truth of the desired state of your Infrastructure, Platform and Applications.
- Benefits:
  - Everything is code: infrastructure, networking, configuration, sealed secrets etc.
  - Auditability & Compliance
  - Consistent deployments and rollback (no drifts between environment)
  - Configuration Management enforcement
  - Disaster Recovery
  - Baked-in security: Kubernetes clusters **pulls** from Git. CI/CD won't have access to production clusters. Removing human from production environments
  - Declarative manifests and playbooks
- Options:
  - Argo CD, Flux as FOSS. Projects are merging into a single FOSS and be part of CNCF.

What is a Continuous ATO?

- A Continuous ATO is very different from a traditional ATO or a Fast-Track/Accelerated ATO:
  - Platforms have to be compliant with the DoD Enterprise DevSecOps Ref Design to ensure DoD-wide reciprocity, including the use of the Sidecar Container Security Stack (SCSS). Platform controls are mapped to NIST-800-53.
  - We accredit the Platform's **PROCESS** (Continuous Integration/Continuous Delivery (Software Factory)) **with mandated testing and security gates.** The software coming out of the factory and that is RUNNING IN PRODUCTION **on the Platform** (Kubernetes with SCSS) also benefits from the cATO.
  - We accredit **TEAMS** using the Platform so they can produce quality software and be trained to move to DevSecOps
  - A key principle of DevSecOps is the **baked-in security** with:
    - Zero Trust
    - Automation
    - Removal of environment drifts
    - Behavior Detection
    - Continuous Monitoring
    - Pen-testing

Thank You!

Nicolas Chaillan
Chief Software Officer, U.S. Air Force
usaf.cso@mail.mil

Backup Slides

Nicolas M. Chaillan

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

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 Cloud Native Access Point (not using IAP/CAP).
- 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.

DCCSCR/DCAR (DoD Container Repository)

- Containers are centrally accredited by the DSOP team in the DoD repository:
  - **DoD Centralized Containers Source Code Repository (DCCSCR)**: https://dccscr.dsop.io/dsop
  - DCCSCR Infrastructure as Code (IaC): https://dccscr.dsop.io/levelup-automation/aws-infrastructure
    - Allows DoD programs to reuse DevSecOps stack and CI/CD pipelines to ensure pre-hardened deployments.
- **DoD Centralized Artifacts Repository (DCAR)** (Container binaries): https://dcar.dsop.io
- Containers are signed and continuously monitored.
- Community can contribute code merge requests, reviewed by the DSOP team.
- Vendors/DoD Programs can contribute containers that have enterprise benefits to DCCSCR/DCAR and DSOP team will accredit them and maintain them.

Key “Continuous Security” Ingredients

- **Kubernetes hardening.**
  - Automated injection of Sidecar Container Security Stack (SCSS) into all containers/pods running without manual action.
  - RBAC/SSO/SELinux enabled
  - Compliant with CIS Kubernetes Benchmark, mapped to NIST 800-53
  - Nodes, master, etcd are hardened.
  - Automated backups of cluster and persistent storage!
- **Sidecar Container Security Stack (SCSS):**
  - Automated centralized logging and telemetry with Elasticsearch, Fluentd, Kibana (EFK),
  - Service Mesh (Istio):
    - Baked-in **zero trust model** down to the container level!
      - Strong identities automatically generated using certificates.
      - mTLS tunnel injected across all container communication
    - Whitelist enforcement, Layer 7 load balancer etc
  - Container security: Continuous Scanning, Alerting, CVE scanning, **Behavior detection** both in development and production (Build, Registry, Runtime) with Twistlock (looking into StackRox and Sysdig)
  - Container security and insider threat (custom policies detecting unapproved changes to Dockerfiles) with Anchore
  - Automated STIG compliance with OpenSCAP.

DevSecOps Stack implements Zero Trust!

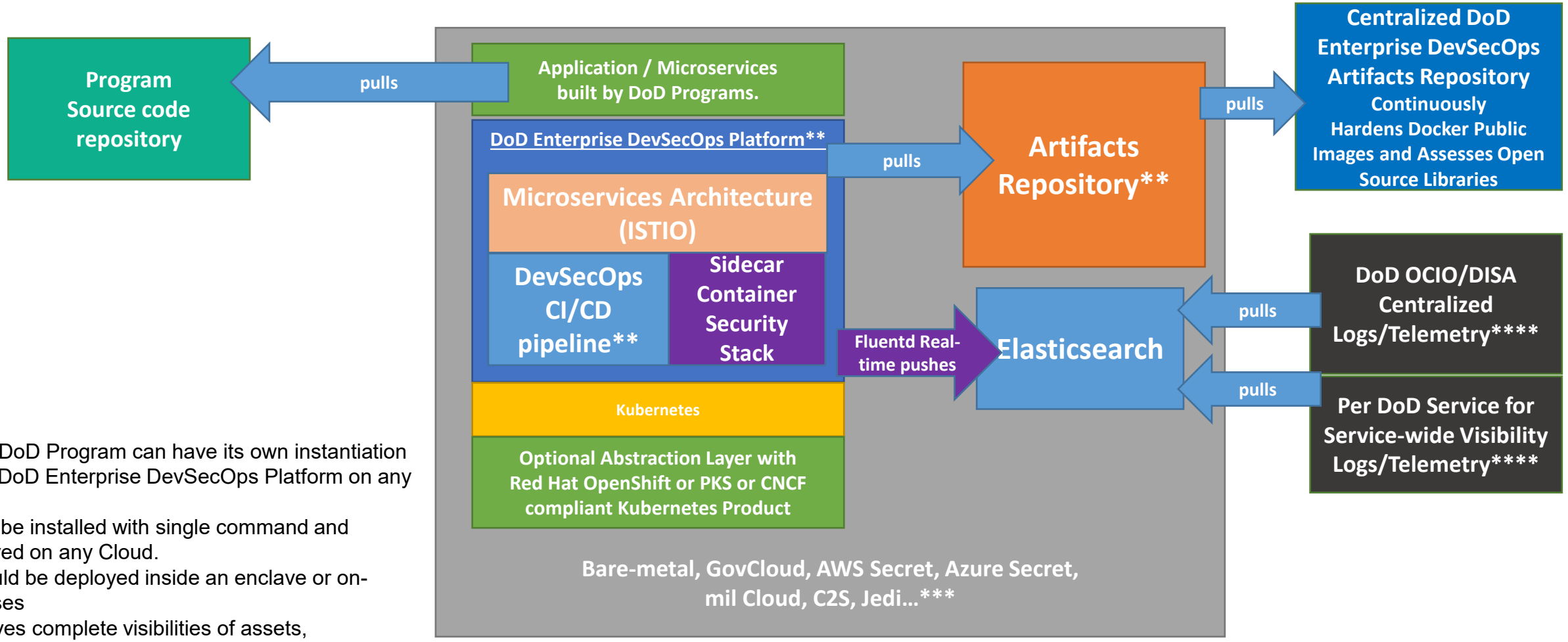
- **Identities**:
  - strong NPE identities are automatically managed by Istio (Service Mesh) for each container to enable zero trust down to the container level.
  - Non-NPE identities are using strong identities with DoD PKI
- **Devices**:
  - Developer endpoints are using VDI options or approved endpoints images
- **Applications**:
  - Apps are containerized and behind the Service Mesh which enforces Zero trust with strong identities per pod/container and .
- **Infrastructure**:
  - Kubernetes is centrally hardened and continuously monitored with centralized logs and telemetry.
  - SCSS monitors container signatures and container state
  - SCSS brings Behavior detection and CVE continuous scanning
- **Network**:
  - mTLS tunnels are automatically injected across all containers/pods by SCSS.
- **Data**:
  - Data is always encrypted in transit and leverages FIPS encryption at rest.

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.

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.

Training Options

- **Our latest training videos from DAU available at:** https://software.af.mil/training/
- Check out our curated YouTube videos on Kafka, Kubernetes, Service Mesh, Microservices, Cloud etc. at https://software.af.mil/training/
- **NEW:** Federal employees/Military personnel (limited number of seats, free of charge): reach out to us at usaf.cso@mail.mil if you want to pilot the access to the **O'Reilly Online Learning Platform** (all O'Reilly content + virtualized K8S env)!
- Platform One 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)
- Follow the CNCF channel: https://www.youtube.com/channel/UCvqbFHwN-nwalWPjPUKpvTA

DevSecOps Platform Stack (continuously evolving)

DevSecOps Product Stack (1)

Source Repository
GitHub Government
GitLab

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

Container Packagers:
Helm
Kubernetes Operators

API Gateways
Kong
Azure API
AWS API
Axway
3Scale
Apigee
ISTIO (service mesh)

Artifacts
Artifactory
Nexus
Maven
Archiva
S3 bucket

Programming Languages
C/C++
C#/.NET
.NET Core
Java
PHP
Python
Groovy
Ruby
R
Rust
Scala
Perl
Go
Node.JS
Swift

Databases
SQL Server
MySQL
PostgreSQL
MongoDB
SQLite
Redis
Elasticsearch
Oracle
etcd
Hadoop/HDInsight
Cloudera
Oracle Big Data
Solr
Neo4J
Memcached
Cassandra
MariaDB
CouchDB
InfluxDB (time)

DevSecOps Product Stack (2)

Message bus/Streams
Kafka
Flink
Nats
RabbitMQ
ActiveMQ

Proxy
Oauth2 proxy
nginx ldap auth proxy
openldap
HA Proxy
Envoy

Visualization
Tableau
Kibana

Logs
Logstash
Splunk Forwarder
Fluentd
Syslogd
Filebeat
rsyslog

Webservers
Apache2
Nginx
IIS
Lighttpd
Tomcat

Docker base images OS:
~~Alpine~~
~~Busybox~~
~~Ubuntu~~
~~Centos~~
~~Debian~~
~~Fedora~~
Universal Base Image

Serverless (FaaS)
Knative

AI/ML/Deep Learning
Kubeflow

DevSecOps Product Stack (3)

Build
MSBuild
CMake
Maven
Gradle
Apache Ant

Tests suite
Cucumber
J-Unit
Selenium
TestingWhiz
Watir
Sahi
Zephyr
Vagrant
AppVerify
nosetests
SoapUI
LeanFT

Test coverage
JaCoCo
Emma
Cobertura
codecov

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
Metasploit
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
Anchore
Checkmarx
SD Elements
Clair
Docker Bench Security
Notary
Sysdig
Layered Insight
BlackDuck
Nexus IQ/Lifecycle/Firewall
RunSafe

DevSecOps Product Stack (4)

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

Collaboration
Rocket.Chat
Matter.Most
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

Self-Learning (1)

- 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_F9TtLIzz0zt03Ludtid7icrXBesg
    - Intermediate: https://www.youtube.com/playlist?list=PLSIv_F9TtLIxxXX0oCzt7IaO6mD61UIQw
    - Advanced: N/A
  - Kubernetes
    - Beginners: https://www.youtube.com/playlist?list=PLSIv_F9TtLIydFzQzkYYDdQK7k5cEKubQ
    - Intermediate: https://www.youtube.com/playlist?list=PLSIv_F9TtLIx8dSFH_jFLK40Tt7KUXTN_
    - Advanced: https://www.youtube.com/playlist?list=PLSIv_F9TtLIytdAJiVqbHucWOvn5LrTNW

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
    - Intermediate: https://www.youtube.com/playlist?list=PLSIv_F9TtLIwWK_Y_Cas8Nyw-DsdbH6vl
    - Advanced: https://www.youtube.com/playlist?list=PLSIv_F9TtLIx8VW2MFONMRwS_-2rSJwdn
  - Microservices
    - Beginners: https://www.youtube.com/playlist?list=PLSIv_F9TtLIz_U2_RaONTGYLkz0lh-A_L
    - Intermediate: https://www.youtube.com/playlist?list=PLSIv_F9TtLIxqjuAXxoRMjvspaEE8L2cB
    - Advanced: https://www.youtube.com/playlist?list=PLSIv_F9TtLIw4CF4F4t3gVV3j0512CMsu

Self-Learning (3)

- 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.

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/