Headquarters U.S. Air Force

Integrity - Service - Excellence

U.S. AIR FORCE

DoD Enterprise DevSecOps Initiative
Ask Me Anything Event

Mr. Nicolas Chaillan

Chief Software Officer, U.S. Air Force

Co-Lead, DoD Enterprise DevSecOps Initiative

V1.0 – UNCLASSIFIED

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 **Istio as Service Mesh** and baked-in security
  - 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, contract vehicles 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
- Created new Agile contracting language to enable and incentivize the use of DevSecOps

U.S. AIR FORCE

New Chief Software Officer Website!

- Find more information about the DoD Enterprise DevSecOps initiative on the new CSO website at https://software.af.mil/
  - More information about
    - Cloud One
    - Platform One
    - DevSecOps
    - Training including videos selection
    - Software Factories
    - Our latest documents: https://software.af.mil/dsop/documents/
    - Our Events/News!
  - Yes you can get DNS errors, please thanks DISA for us!

Questions about 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 (looking into StackRox and Sysdig)
- Container security and insider threat (custom policies detecting unapproved changes to Dockerfiles) with Anchore
- Automated STIG compliance with OpenSCAP

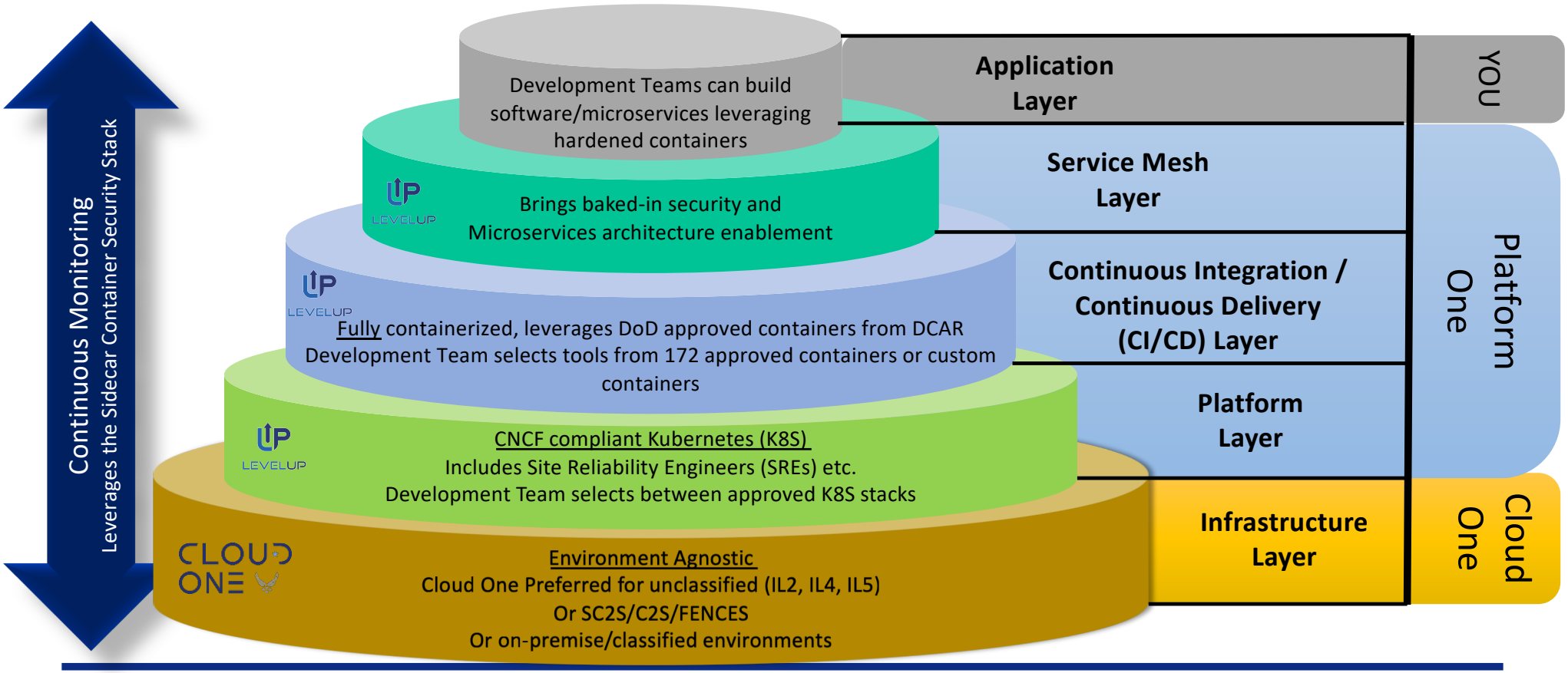
U.S. AIR FORCE

Questions about DCCSCR/DCAR?

- Containers accredited in the DCCSCR/DCAR repository have DoD-wide reciprocity across classifications.
  - Source code repo: DCCSCR: **https://dccscr.dsop.io/dsop**
  - Source code repo: DCCSCR Infrastructure as Code (IaC): **https://dccscr.dsop.io/levelup-automation/aws-infrastructure**
- DCAR (Container binaries): https://dcar.dsop.io
- We are building a container which automatically download container updates into your K8S cluster, checks signatures and pushes them to your local registry (agnostic to your artifact repo)
- By being compliant with the DoD Enterprise DevSecOps Container Hardening guide (last version at https://software.af.mil/dsop/documents/), you can have your containers (FOSS/COTS/GOTS) accredited for DoD use.
- Recommend using the hardened STIG UBI7/8 images (Universal Base Image which is lightweight RHEL but doesn't need a license) from the DCAR repo as your base image so you don't have to STIG your container base OS: https://dcar.dsop.io
- Check out the vendor on-boarding guide at: **https://dccscr.dsop.io/dsop/dccscr/tree/master/contributor-onboarding**
- Questions? Email usaf.cso@mail.mil

U.S. AIR FORCE

Understanding the DevSecOps Layers



CLOUD ONE

LEVELUP CODE WORKS

"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).
  - Only contact Cloud One if you **only** need Cloud compute/storage, if you need a DevSecOps stack (on Cloud One or not), contact « Platform One by LevelUP »
  - Point of Contact: DOLCE, JOSEPH G Maj USAF - joseph.dolce@us.af.mil; Watson, Todd M Lt Col USAF todd.watson@us.af.mil
- 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.
  - **Contact Platform One if you need both Cloud and DevSecOps capabilities!**
  - Point of Contact: Slaughter, Rob Maj USAF - rob.slaughter@afwerx.af.mil; Bryan, Austen R Capt USAF - austen.bryan.1@us.af.mil;

U.S. AIR FORCE

CLOUD ONE

Questions about Cloud One?

- Air Force Cloud Office with turnkey access to AWS GovCloud and Azure Government at IL2, 4 and 5. IL6 available by February 2020.
- 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 February 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.

U.S. AIR FORCE

LEVELUP CODE WORKS

Questions about "Platform One by LevelUP"?

- Merged top talent across U.S. Air Force from various Factories (Kessel Run, SpaceCAMP and LevelUP).
- Helps instantiate DevSecOps CI/CD pipelines / Software Factories **(DoD-wide)** within days, on any environment, at various classification levels.
- Manages Software Factories for Development teams so they can focus on building mission applications.
- Provides DoD-wide DevSecOps contract vehicles (Basic Ordering Agreement (BOA)) 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.

U.S. AIR FORCE

LEVELUP CODE WORKS

"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

Questions about the DevSecOps Basic Ordering Agreements (BOAs)?

- Covers Cloud Services, Talent and Licenses so DoD programs can get everything they need for a DevSecOps environment, completely turnkey.
- Not selected yet? We will have quarterly on-boarding events for new vendors/award opportunities!
- Aims to award each order within 15 days (!!!)
- Available to the entire Department of Defense
- Point of Contact:
  - Paul, Christopher C 2d LT USAF AFLCMC (USA) christopher.paul.3@us.af.mil
  - Slaughter, Robert C Maj USAF (USA) robert.slaughter.3@us.af.mil
  - Wyler, Victoria R Capt USAF SAF-AQ (USA) victoria.r.wyler.mil@mail.mil

U.S. AIR FORCE

Questions about the Agile / SAFe Memo?

- The CSO signed a Memorandum for Record on Nov 26th 2019, sent to all PEOs and PMs regarding the use of DevSecOps and Agile and **highly discouraging from using rigid, prescriptive frameworks such as the Scaled Agile Framework (SAFe)**.
- Why?
  - DoD is still using Waterfall or Water-Agile-Fall so until we can truly implement basic Scrum/Kanban, there is nothing to « SCALE ». Agile should be applied across the entire Program, not just the development team, that includes: Contracting, Program Management, Reporting to leadership (no EVM) etc!
    - You cannot scale if you don't have the "basics" right. At best, such frameworks put us at risk to fall back to what we know and go back to Waterfall because of their "mapping".
  - SAFe might potentially be an useful framework for teams which do not use DevOps/DevSecOps but a key principle of DevSecOps is to decouple work and teams and the only synchronization required should be across Product Owners. Teams shouldn't have to coordinate if they use a Service Mesh/Domain Driven Design/Microservices model. This doesn't require a rigid framework. If you're having issues implement this, you're not implementing the right DevSecOps model.
  - Take what is best from any framework and make it work for your team! Certifications aren't always the answer!
  - Fundamentally, the main "goal" of Software development is NOT to be « SAFE », it is to INNOVATE and CREATE. You do not create by not taking risks… it is quite the opposite:
    - « Continuous Learning: Fail Fast but don't Fail twice for the same reason! » - Small incremental changes which mitigate risks and create safe conditions to implement rapid changes.
  - SAFe isn't used by any successful software commercial organization (Facebook, Google, Netflix, etc.).
  - Bloated overhead functions (Waterfall-like)
  - Looking to coordinate your Product Owners' work? Multiple models exist such as Scrum of Scrum etc. This shouldn't impact the developers.

U.S. AIR FORCE

Thank You!

https://software.af.mil

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

Integrity - Service - Excellence