Department of the Air Force

Integrity - Service - Excellence

DoD Enterprise DevSecOps Initiative & Platform One Keynote Presentation

Mr. Nicolas Chaillan

Chief Software Officer, U.S. Air Force

Co-Lead, DoD Enterprise DevSecOps Initiative

Chair, DSAWG DevSecOps Subgroup

V2.0 – UNCLASSIFIED

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/

Why Kubernetes / Containers?

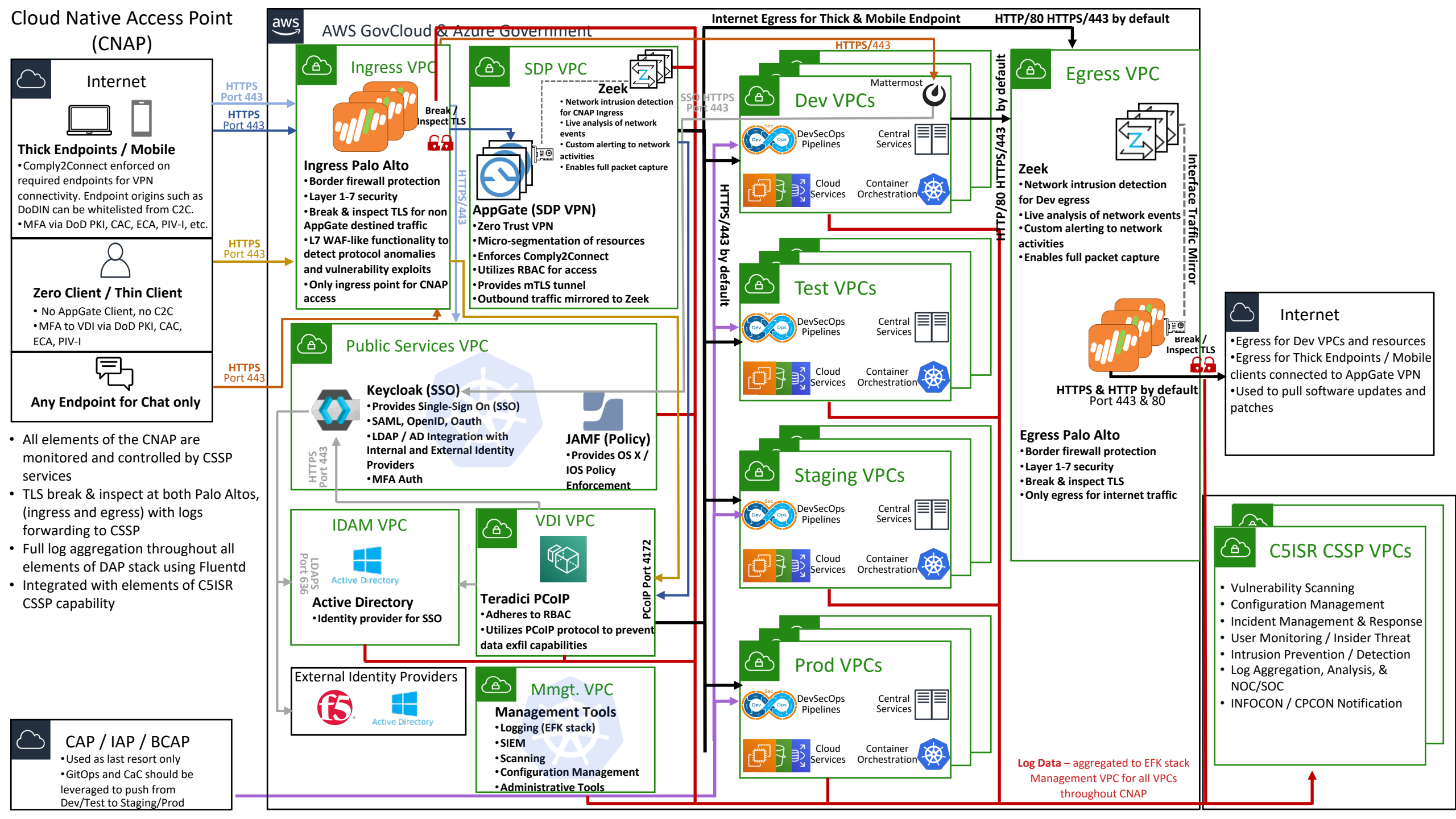
- One of the most critical aspect of the DevSecOps initiative is to ensure we **avoid any vendor lock-in** so the DoD mandated:
  - **Open Container Initiative (OCI) containers** (no lock-in to containers/container runtimes/builders)
  - **Cloud Native Computing Foundation (CNCF) Kubernetes compliant cluster** for container orchestration, no lock-in to orchestration options/networking/storage APIs.
- 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.

U.S. AIR FORCE

Cloud Native Access Point

- Provided by a managed service by Platform One.
- Brings a full Zero Trust stack enforcing device state, user RBAC and Software Defined Perimeter/Networks based on Google BeyondCorp concepts
- Allows access to Cloud One (AWS GovCloud and soon Azure Government) and Platform One without having to go through the DISN/DoDIN
- Allows access from thick clients on BYOD, government owned devices (both mobile and desktop) while enforcing their device states by using AppGate as a zero trust client.
- Allows for VDI options for zero / thin clients
- Enables internet egress at IL5 in Dev enclaves
- Brings DMZ/Perimeter stack with break and inspect, IDS/IPS, WAF capability, full packet capture as an elastic Cloud based stack
- Brings Single Sign On with various DoD PKI options and IL2 MFA options.
- Centralizes/Aggregates logs and pushes to CSSP

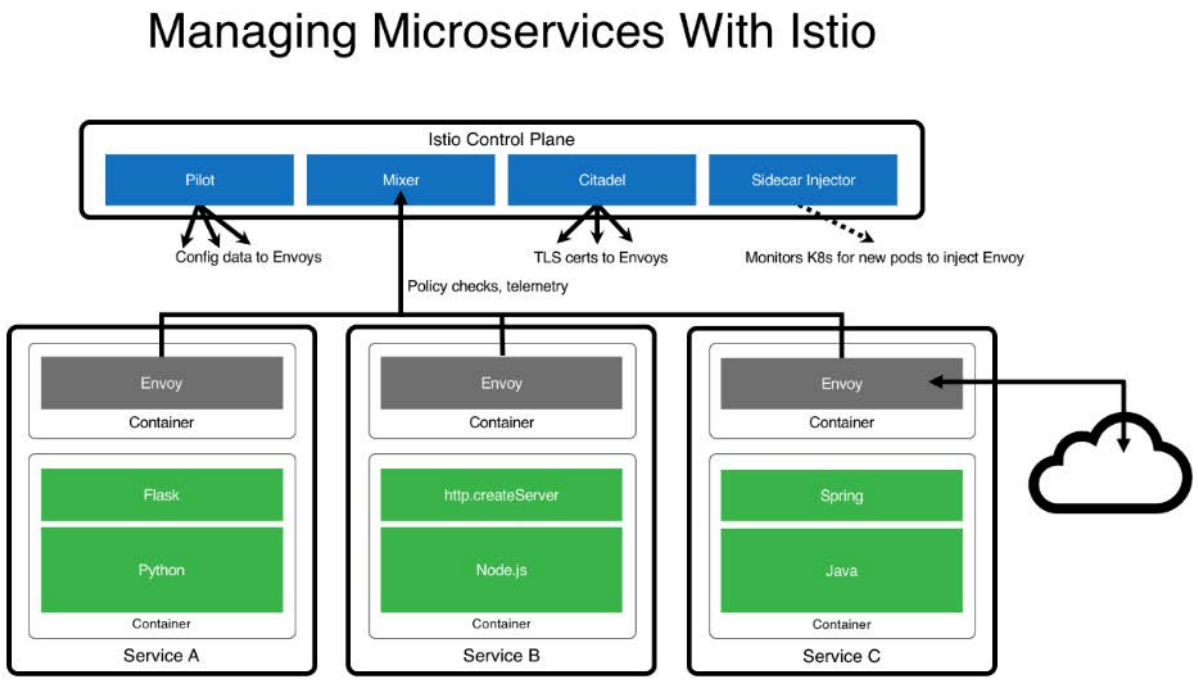
Cloud Native Access Point (CNAP)



- All elements of the CNAP are monitored and controlled by CSSP services
- TLS break & inspect at both Palo Altos, (ingress and egress) with logs forwarding to CSSP
- Full log aggregation throughout all elements of DAP stack using Fluentd
- Integrated with elements of C5ISR CSSP capability

Service Mesh (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.

Continuous Authorization

Traditional Authorization Approach

Authorize System

Industry Average Performance*

(Traditional Development Approach)

Deployment Frequency: 30-180 days

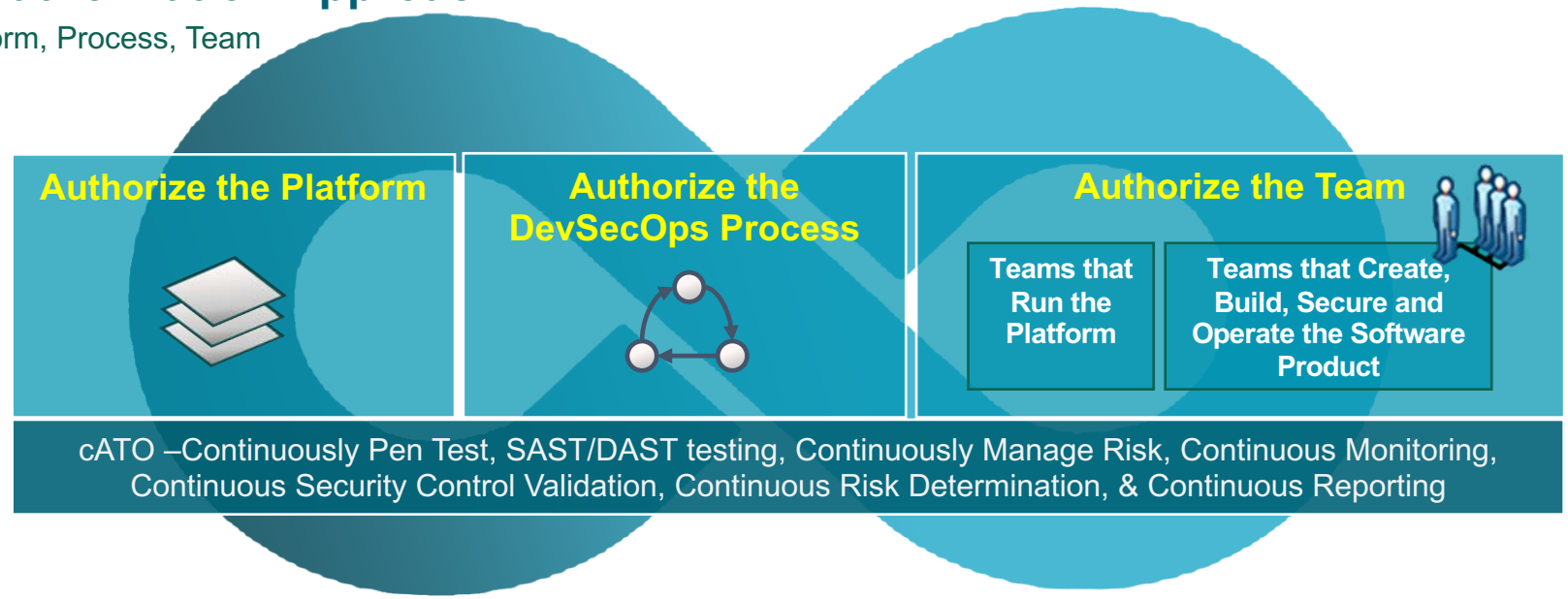
Lead Time for Changes: 30-180 days

Time to Restore Service: 7-30 days

Change Failure Rate: 46-60%

Continuous Authorization Approach

Authorize Platform, Process, Team



cATO Performance Targets*

(Industry Elite DevSecOps Performance)

Deployment Frequency: Multiple/day

Lead Time for Changes: < 1 day

Time to Restore Service: < 1 hour

Change Failure Rate: 0-15%

*DORA Accelerate State of DevOps Report, https://services.google.com/fh/files/misc/state-of-devops-2019.pdf

Continuous Authorization: Overview

Continuous Authorization

1: Authorize the Platform

- Software Factory
- Hardened Artifacts with ATO Reciprocity
- Standard Hosting Environment With Inherited Controls
- DoD Enterprise DevSecOps Reference Design MVP Compliance
- Continuous Monitoring Tools
  - Sidecar Container Security Stack
  - Managed Service

2: Authorize the Process

- Feedback Loops
- Control gates, exit criteria, artifacts
- CI/CD Pipeline
- Continuous Monitoring Operations

3: Authorize the Team

- Teams that Run the Platform
- Teams that Create, Build and Operate the Software
- DevSecOps Culture
  - First Way: Flow
  - Second Way: Feedback
  - Third Way: Continual Learning & Experimentation

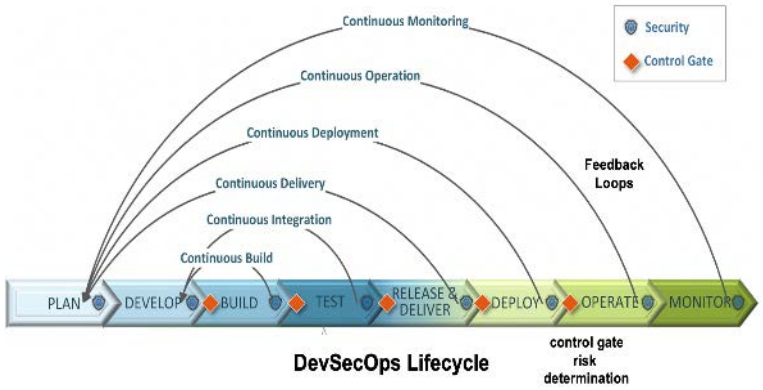
Test & Evaluation

Continuous Risk Monitoring
Continuous Risk Determination

- Key points:
  - Move away from snapshot in time towards auto-generated content displayed in a dashboard showing risk posture in real-time
  - Extensive utilization of SW reuse, reciprocity, & inheritance from underlying infrastructure, platform, SW Factory, and authorized-to-use functional components
  - CI/CD security findings that exceed the risk threshold trigger an event to involve ISSM, assessor or AO then put on the backlog for remediation scheduling in future sprint
  - Continuous validation of security configuration hardening and implementation of controls
  - Use of IaC to create a consistent, secure, and repeatable instance of application support infrastructure
  - Execution of SW Product within a secure authorized Platform based on the DoD CIO Enterprise DevSecOps Reference Design

Through the execution of these practices, the SW Product has been through an automatic risk determination based on the AO's prescribed risk tolerance resulting in the SW Product **automatically authorized for use**

control gates risk tolerance checks



Security Posture Visualization

Result: continuous risk analysis, risk determination, and authorization

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/

Thank You!

Nicolas Chaillan
Chief Software Officer, U.S. Air Force
af.cso@us.af.mil – https://software.af.mil