Waterfall to DevSecOps in DoD

Nicolas Chaillan,

USAF CSO

Hasan Yasar,

Technical Director, Software Engineering Institute | CMU

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-1118

CMU SEI is a DoD R&D Federally Funded Research and Development Center

Established in 1984 at Carnegie Mellon University

~650 employees (ft + pt), of whom about 70% are engaged in technical work

Initiated CERT cybersecurity program in 1988

Offices in Pittsburgh and DC, with other locations near customer facilities

~$140M in annual funding (~$20M DoD Line funding for research)

We Improve Software-based System Development, Operation, and Sustainment

CMU SEI offers unique expertise and capability

- Work across the software acquisition and cyber operations lifecycle
- Collaborate with CMU academic departments, a top source of basic research in most software-based technologies
- Diverse portfolio of customers and collaborators to share cost and transition practices

CMU SEI strives to make software a strategic advantage

- Demonstrating **Capabilities** that make new missions possible
- Realizing **Timely** acquisition that is responsive to the operational tempo
- Ensuring **Trustworthy** construction and resilience to operational uncertainties
- Improving **Affordability** by reducing cost and increasing predictability

We Serve a Broad Spectrum of Stakeholders

Major government customers

- U.S. DoD
- U.S. DHS

Researchers, developers, users, and acquirers—government, commercial, and academic

Key industries and organizations with the potential to advance software engineering and related disciplines

Nicolas Chaillan - USAF CSO

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.

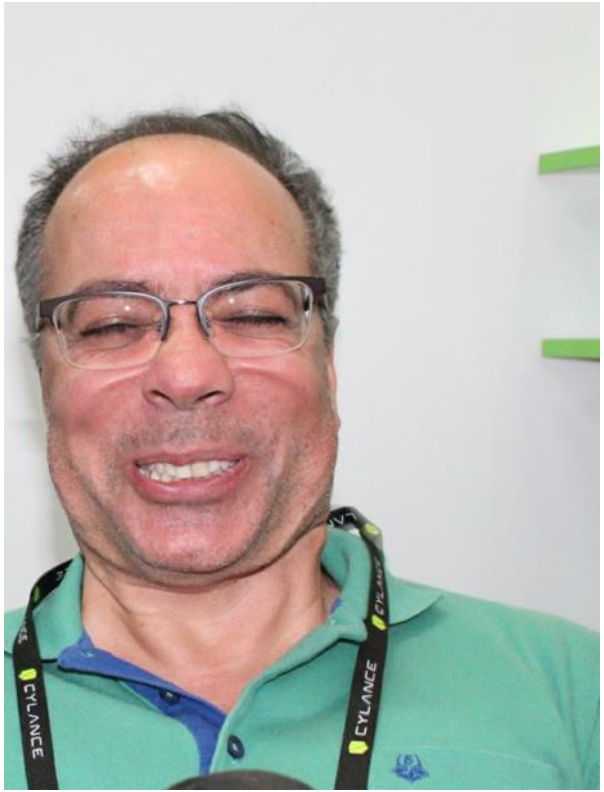
Over the last eight years alone, he has created and sold over 180 innovative software products to 40 Fortune 500 companies.

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

2018
OFFICIAL MEMBER
Forbes
Technology Council

Background: With the speed of DevOps…

It is me!
I felt the speed of
DevOps



- 25+ years of software development experiences
- Certified Scrum Practitioner
- Certified Ethical Hacker
- Various roles throughout SDLC ; Manager, Architect, Tester, Developer, QA, IT Manager, Project Manager, VP…
- Started with waterfall in 1990
- Started with agile in 2003
- Started with DevOps in 2010
- Instructor on delivering DevOps course at CMU, SEI since 2015
- DevOps, DevSecOps community organizer, frequent Speaker
- PC members in various research conferences,
- Editorial board member, IJSS, AJSE
- Vice Chair of IEEE 2675 DevOps study group

Why DevSecOps ?

DoD Depends on Software but Does Not Control Development

Software and system complexity is increasing software cost and vulnerability, jeopardizing military capability

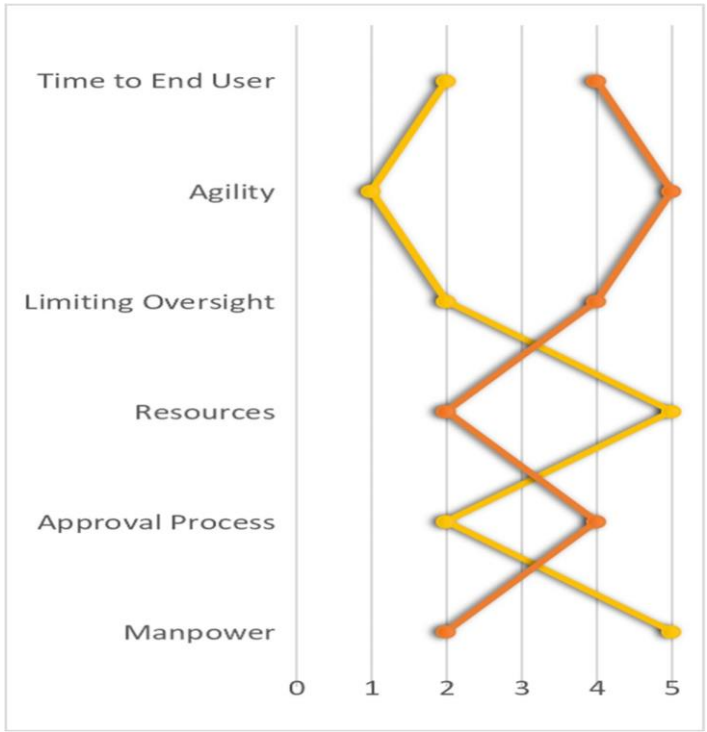
- DoD does not produce most of the software it uses, but it must maintain that software
- More and more capability results from software, and it will evolve for the lifetime of a system
- Latent cyber vulnerabilities, those exposed during operations, and those due to underlying dependencies are putting the DoD at risk
- Finding and fixing problems late causes rework and drives up costs
- Software cost overruns are overwhelming program delivery and sustainment

Modern software development and automated tools are critical

DoD vs Private

Current Acquisition process attribute map

Most important to end user



Least important to end user

*NAVAL Special Warfare Operator study

"Simply delivering what was initially required on cost and schedule can lead to failure in achieving our evolving national security mission — the reason defense acquisition exists in the first place."

Honorable Frank Kendall
Under Secretary of Defense (AT&L)
2015 Performance of The Defense Acquisition System

"As we reorganize the way we do business the thread that runs through all of our programs and all that we do is software and I believe that we need to catch up with the private sector and make sure we are using contemporary software development processes,"

The Honorable Ellen Lord,
Under Secretary of Defense,
Acquisition and Sustainment

The Problems on Development/Integration and Delivery

- Heavy waterfall process on every phases of software development lifecycle,
- Very long cycle times between each deliveries, ***1-2 years***
- Manual, error-prone build, integration and deployment times measured ***in weeks, months, or even years***
- Integration hell on various levels.
- Very late stage integration with manual testing for ***5 or more years***
- ***Anti-Parity*** across development, integration and production environments
- ***6-12 months*** to manually deploy and test code in production environment
- Code and unit test cycles occurring ***in weeks*** as opposed to hours
- End-to-end, system integration testing occurring ***in months*** vs days or hours
- Very long ATO(Authority-to- Operate) process , ***6-18 months***

The Solution: DevSecOps

- **What is DevSecOps?**
  - The software automated tools, services, and standards that enable programs to develop, secure, deploy, and operate applications in a secure, flexible and interoperable fashion.
- **Why should I care?**
  - Software and cybersecurity pervades all aspects of DoD's mission (from business systems to weapons systems to Artificial Intelligence to cybersecurity to space) - establishing DevSecOps capabilities will:
    - Deliver applications rapidly and in a secure manner, increasing the warfighters competitive advantage
    - Bake-in and enforce cybersecurity functions and policy from inception through operations
    - Enhance enterprise visibility of development activities and reduce accreditation timelines
    - Ensure seamless application portability across enterprise, Cloud and disconnected, intermittent and classified environments
    - Drive DoD transformation to Agile and Lean Software Development and Delivery
  - Leveraging industry acquisition best practices combined with centralized contract vehicle for DevSecOps tools and services will enable rapid prototyping, real-time deployments and scalability.

Lots of Barriers…..

- Very complex systems (Safety critical, Realtime, Embedded Systems..)
- Sustainment of DevSecOps pipeline
  - Tool updates, project configuration, tool license cost,
  - Effective usage of the platform, combability with the program needs

- Lack of iterative and incremental mindset cultural issues
  - Blame-Free Culture, Cross-Silo Goals, Optimize Ease-of-Use
- Organizational Structure
  - Siloed on Acq, O&M and Security departments, Org structure based on system architecture
- Legacy Systems
  - Lack of modular architecture, old tools/language
- Aged bureaucracy and waterfall process
- Lack of Metrics and Measurements
- RMF- ATO Compliances
- Inconsistent Environments

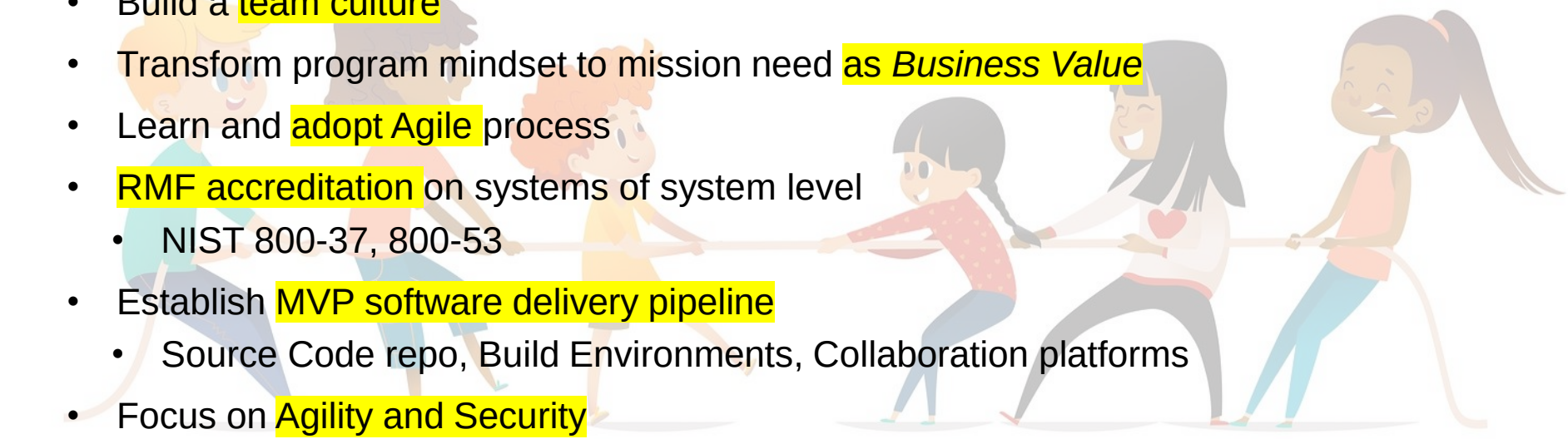
Transformation Journey

“Took 6 years on one of the DoD Program”

First Phase →

Adopt Agile and Risk Management Framework (RMF)

- Build a team culture
- Transform program mindset to mission need as *Business Value*
- Learn and adopt Agile process
- RMF accreditation on systems of system level
  - NIST 800-37, 800-53
- Establish MVP software delivery pipeline
  - Source Code repo, Build Environments, Collaboration platforms
- Focus on Agility and Security



Second Phase →

Mature the enterprise, People, Policy and Agile Process

- Introduce on Kanban&Scrum- based agile development teams
- Bing Agile coaches and streamline the development process
- Introduce new development practices,
  - Continuous integration and delivery pipeline
  - Centralized code repository
  - Remove extraneous documentation : Focus on application delivery
- Establish a “Path-to-Production” to begin process improvements that better meet the customer demand signal

Third Phase →

Modernization (Architecture and Tooling)

- Commoditization of components and introduction of containerization
- Address technical dept in legacy application
- Migration to modular architecture (Microservices, MOSA)
- Improve development and deployment tools
  - Integrated deployment pipeline : from inception to operation)
- Operationalize SRE on infrastructure team
- Develop contracts SLAs and SLOs
- Introduce Audit vs Gate keeper

Fourth Phase →

Operationalize DevSecOps

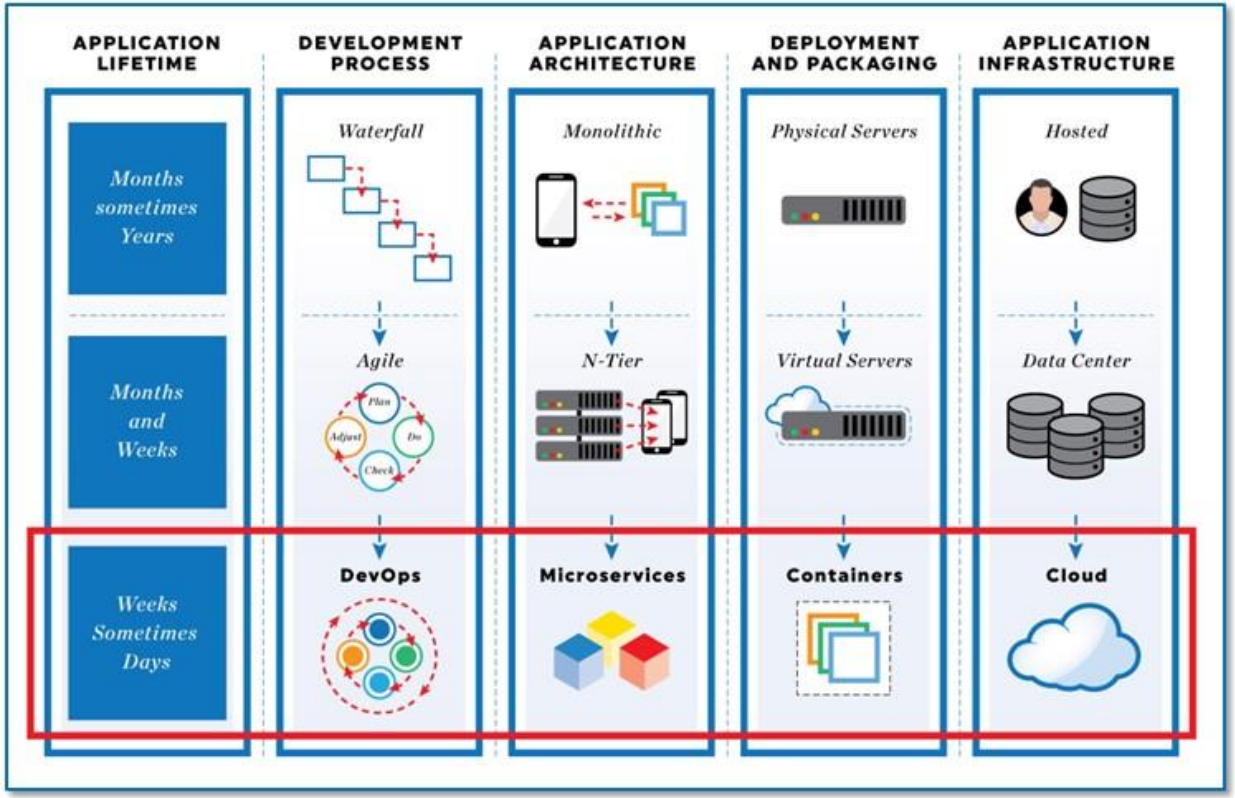
- Codify CI/CD tools, creating DevSecOps Pipeline for Continuous Authorization
- Automation and Immutable Environments:
  - Source controlling Infrastructure-as- Code(IaC)
- Pipeline release supporting a live DoD system
- DevSecOps enabled Data Science workflows and deployments
- Introduce New Governance approach based on DevSecOps
- Select small discreet parts of the enterprise as projects for DevSecOps enablement

Fifth Phase →

Mature DevSecOps and Scale

- Scheduled a Pipeline to GO-LIVE event with Analytic
- Platform and tech refresh
- Orchestrate and extend the on-prem enterprise into the cloud
- Collect Lessons Learned
- Incentivize transparency between contractors and government
- Incentivize smaller releases
- Begin tracking development metrics
- Implement Deployment and Monitoring strategies

Parallel Efforts to DevSecOps



DoD Enterprise DevSecOps Initiative

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:
  - Selecting, certifying, and packaging best of breed development tools and services (over 100 options)
  - Creating the Sidecar Container Security Stack (SCSS) for baked-in zero trust security
  - Creating a Centralized artifacts repository of hardened and centrally authorized containers
  - Designing a Scalable Microservices Architecture with Service Mesh/API Gateway and baked-in security
  - Providing on-boarding and support for adoption of Agile and DevSecOps
  - Developing best-practices, training, and support for pathfinding and related activities
- Standardizing metrics and define acceptable thresholds for continuous ATO
- Working with DAU to bring state of the art DevSecOps curriculum
- Creating new contracting language to enable and incentivize the use of Agile and DevSecOps

Value for DoD Programs (1)

- 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 pipeline exemplars are available with various options to avoid vendor lock-in and enable true DoD-scale as there is not a one-size-fit-all for CI/CD.
- 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).

Value for DoD Programs (2)

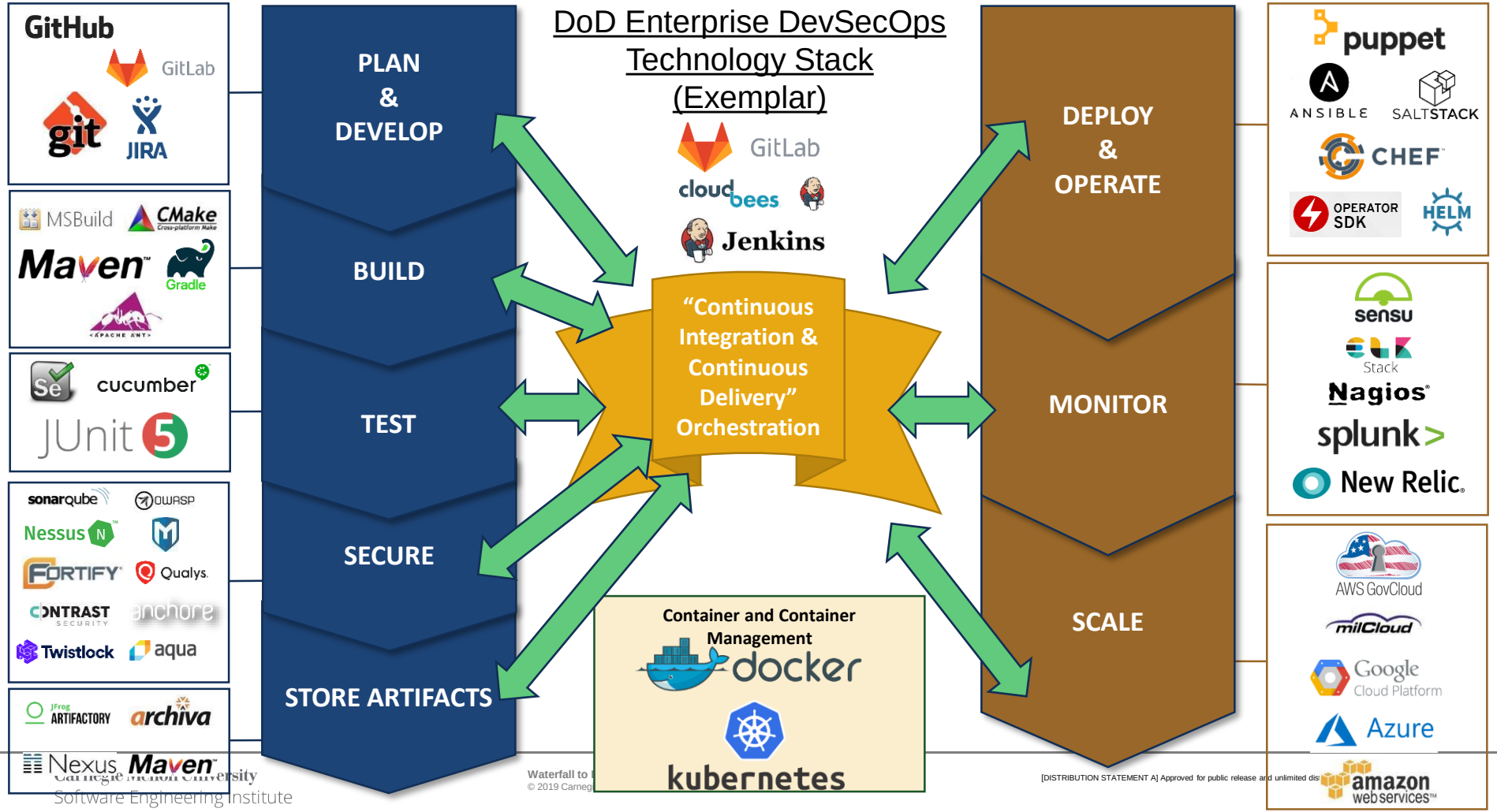
- Enables bug and security fixes in minutes instead of weeks/months.
- Enables automated testing and security.
- Enables continuous Authorization to Operate (ATO) process for rapid deployment and scalability. Authorize ONCE, use MANY times!
- Brings a holistic and baked-in cybersecurity stack, gaining complete visibility of all assets, software security state and infrastructure as code.
- Microservices Architecture to facilitate the adoption of centonization.
- Deployed on any environment, including DoD-approved Cloud and Jedi (when available).

DoD Enterprise DevSecOps Technology

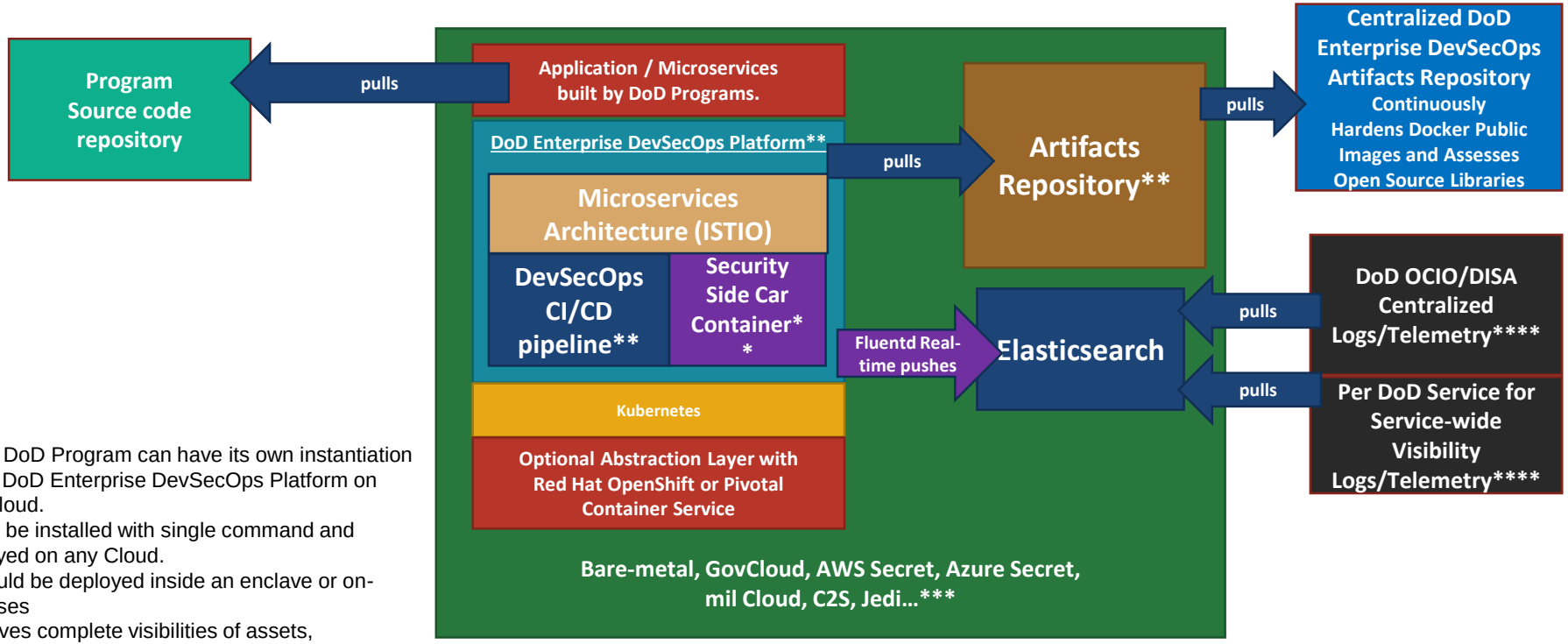
- Create and Maintain DevSecOps pipelines (and not just DevOps) to avoid each DoD services building their own stack and reinventing the wheel.
- Create hardened Container images in a dedicated artifacts repository with security built-in and compliance with FedRAMP/NIST (similar to gold images concept).
- Create a Microservice Service Architecture with Service Mesh (ISTIO).
- Standardize metrics and define acceptable thresholds for test coverage, security, documentation etc. to enable complete continuous deployment with pre-ATO embedded.
- Leverage Kubernetes for Orchestration to ensure automation, rolling-update, scale, security and visibility thanks to the sidecar security container concept.

DoD Enterprise DevSecOps Architecture

DoD Enterprise DevSecOps Technology Stack (Exemplar)



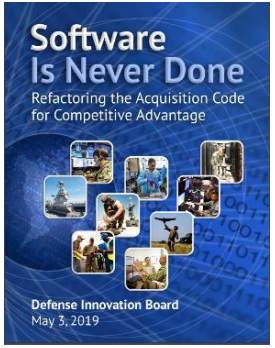
DoD Enterprise DevSecOps Architecture*



*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.

As of today

Defense Innovation Board Study



Line of Effort A: **Tailoring acquisition processes for software**
Line of Effort B: **Digital infrastructure / software factory**
Line of Effort C: **Software workforce / digital talent**
Line of Effort D: **Software security / software provenance**

DecSecOps Academy

Train ~200K professional on “Acquisition, SW Architecture, DevSecOps”

DoD Enterprise DevSecOps Reference Design

Provides logical description of the key design components and process to provide a repeatable reference design that can be used to instantiate a DoD DevSecOps software factory

Current Offerings

- Cloud One: new Air Force Cloud Offering
  - Former Common Computing Environment (CCE), PEO C3I&N
  - Access to AWS GovCloud and Azure Government
  - Pay per use scalable model

- LevelUP: new centralized Air Force Software Factory Team
  - Merged with top talent across U.S. Air Force from various Factories (Kessel Run, Kobayoshi Maru SpaceCAMP and Unified Platform).
  - Leverages the DoD hardened containers
  - Centralizing the Container Hardening of 172 enterprise containers

* DoD Enterprise DevSecOps Platform https://dccscr.dsop.io/dsop

Here are the problems that still remain

- DevOps for embedded/ realtime systems
- Can not fail and learn from safety critical systems
- Train professionals on DevOps and SW engineering skills
- Container based tool supports
- Security built-in products : Baked in RMF/ATO into vendor development tools
- Addressing hybrid deployments
- Build DevSecOps pipeline to support on building AI/ML systems

SEI DevOps GitHub Projects

- Once Click DevOps deployment
  https://github.com/SLS-ALL/devops-microcosm
- Sample app with DevOps Process
  https://github.com/SLS-ALL/flask_api_sample
  - Tagged checkpoints
    - v0.1.0: base Flask project
    - v0.2.0: Vagrant development configuration
    - v0.3.0: Test environment and Fabric deployment
    - v0.4.0: Upstart services, external configuration files
    - v0.5.0: Production environment
- On YouTube:
  https://www.youtube.com/watch?v=5nQlJ-FWA5A

For more information…

DevOps: https://www.sei.cmu.edu/go/devops

DevOps Blog: https://insights.sei.cmu.edu/devops

Webinar : https://www.sei.cmu.edu/publications/webinars/index.cfm

Podcast : https://www.sei.cmu.edu/publications/podcasts/index.cfm

Thank You!

Hasan Yasar

Technical Director,
Continuous Deployment of Capability
hyasar@sei.cmu.edu
@securelifecycle