

REPORT DOCUMENTATION PAGE					Form Approved OMB No. 0704-0188	
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.						
1. REPORT DATE (DD-MM-YYYY)		2. REPORT TYPE			3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE				5a. CONTRACT NUMBER		
				5b. GRANT NUMBER		
				5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S)				5d. PROJECT NUMBER		
				5e. TASK NUMBER		
				5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)					8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)					10. SPONSOR/MONITOR'S ACRONYM(S)	
					11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT						
13. SUPPLEMENTARY NOTES						
14. ABSTRACT						
15. SUBJECT TERMS						
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON	
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include area code)	

Continuous Authorization with DevSecOps

Mark Smiley, Ph.D.

5 March 2021

Approved for Public Release;
Distribution Unlimited. Case 21-0440.

MITRE | SOLVING PROBLEMS
FOR A SAFER WORLD™

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Software is Foundational

National Defense Strategy (2018):

- **Deliver Performance at the Speed of Relevance**
- **Prioritize speed of delivery**, continuous adaptation, and frequent modular upgrades
- We must **not accept cumbersome approval chains**, ... or overly risk-averse thinking that impedes change

Defense Innovation Board, Software Acquisition and Practices (SWAP) Study (2019):

- The competitor that can realize software-defined military capability the fastest is at an **advantage in future conflicts**
- We must **shorten our development cycles** to ... respond to the changing threats we face. ... **DevSecOps** enables this rapid cycle approach
- Establish new acquisition pathway(s) for **software that prioritizes continuous integration and delivery of working software in a secure manner, with continuous oversight from automated analytics**
- Establish and maintain **digital infrastructure within each Service or Agency** that enables **rapid deployment of secure software to the field** and incentivize its use by contractors
- Create software development units in each Service consisting of military and civilian personnel who **develop and deploy software to the field using DevSecOps practices**
- Create, implement, support, and use **fully automatable approaches to testing and evaluation (T&E)**, including security
- **Make security a first-order consideration** for all software-intensive systems, recognizing that security-at-the-perimeter is not enough



Software is foundational to the modern military

Image Source: MITRE

What is DevSecOps?

- DevSecOps is a culture and an approach to modern software delivery built on alignment of development (**Dev**), security (**Sec**) and operations (**Ops**) groups into an integrated team focused on continuous, incremental delivery of capabilities.
- The main characteristic of DevSecOps is to **automate, continuously monitor, and apply security at all phases of the software lifecycle**: plan, develop, build, test, release, deliver, deploy, operate, and monitor.
- In DevSecOps, **testing and security are shifted to the left** through **automated** unit, functional, integration, and security **testing**.
 - This is a key DevSecOps differentiator, since **security and functional capabilities are tested and built simultaneously**
 - Another key differentiator is **continuous feedback from all phases of the DevSecOps lifecycle**

DevSecOps Lifecycle

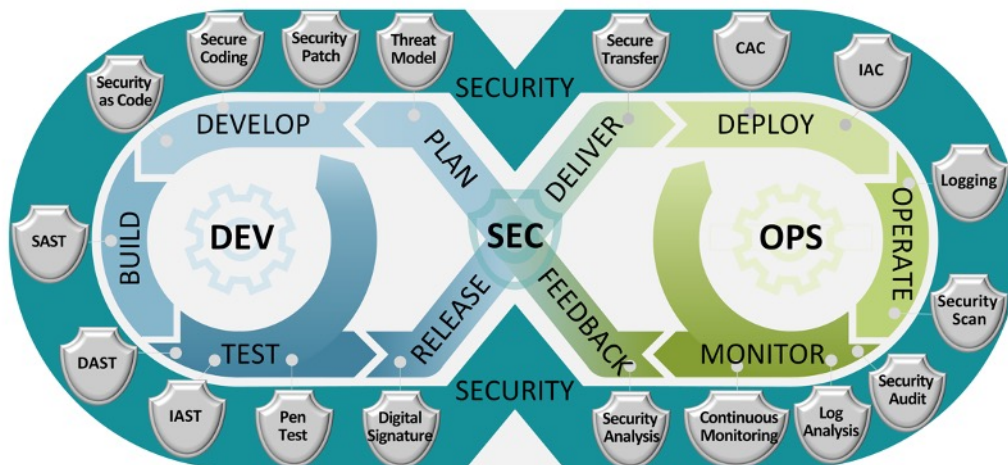


Image Source: MITRE

MITRE

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

4

CAC = Compliance as Code

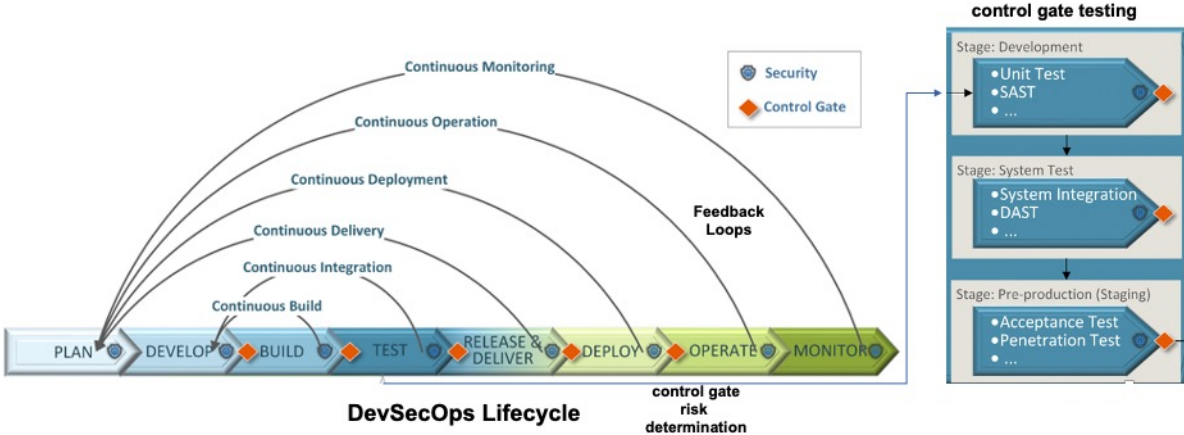
IAC = Infrastructure as Code

DAST = Dynamic Application Security Testing

IAST = Interactive Application Security Testing

SAST = Static Application Security Testing

DevSecOps Lifecycle with Control Gates



Continuous Authorization Method: High Level

- **Authorize the Platform**
- **Authorize the Team** that runs the platform
- **Authorize the Process** to create and monitor the SW Product
- **Authorize the Team** that builds, tests, secures and operates the SW Product
- Through continuous automated risk determination, enabled by security automation and **continuous monitoring**, the SW Product is authorized when it passes all control gate rules and emerges from the pipeline



Image Source: MITRE

MITRE

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

6

The first 4 bullets are about ensuring the organization is set up to effectively and continuously manage risk.

Traditional ATO vs cATO

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>

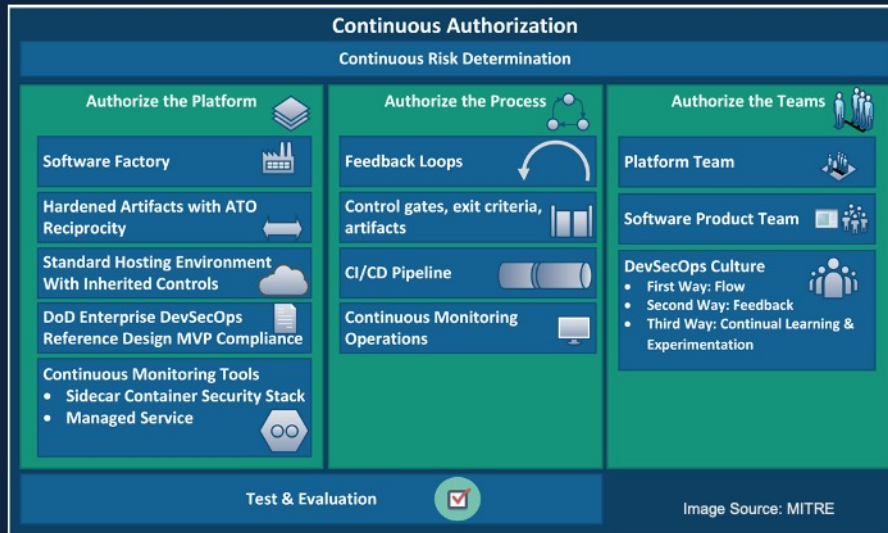
Image Source: MITRE

MITRE

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

7

Continuous Authorization: Overview



What is Continuous Authorization?

It's a...

- state in which **trustworthiness has been established** through assessments & authorizations of the process, the team, and the platform for managing an applications cyber risk coming out of a software factory
- state of **continuous risk determination** of application changes through use of DevSecOps control gate pass-fail rules against security automation findings & analysis
- state of **idempotence and immutability** that provides for consistent, repeatable secure application support infrastructure
- state of **near real-time visualization of the security posture** (e.g., control compliance & effectiveness, change in threat, risk determination, findings to be mitigated, monitoring for malicious activity, and accepted residual risk)
- state of **secure rapid delivery** of authorized applications through the enablement of Continuous Authorization to Operate (cATO)

MITRE

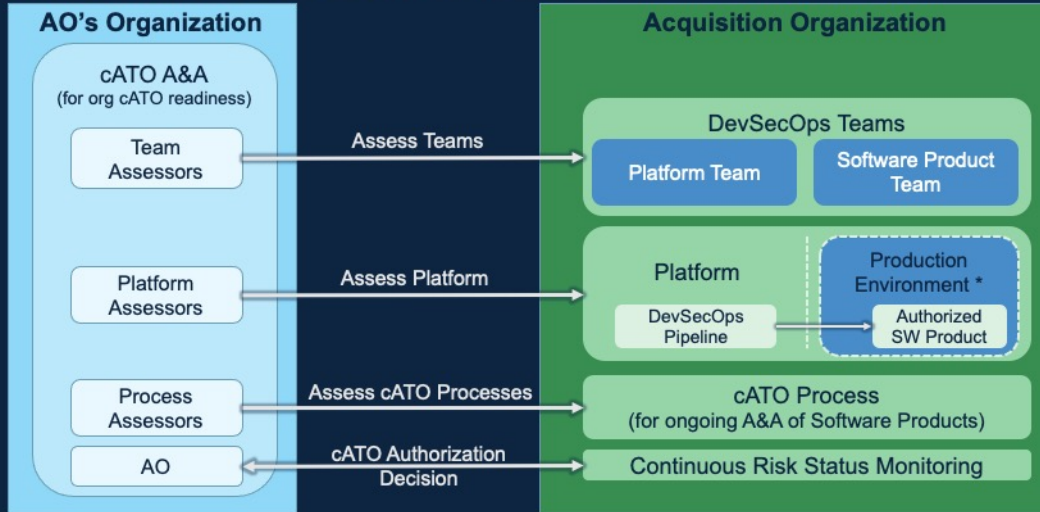
© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

9

Idempotence is the property of certain operations in mathematics and computer science whereby they can be applied multiple times without changing the result beyond the initial application.

In this context, idempotent means that the IaC can be deployed again and again, and the result is the same. For example, if a running VM or container fails or is compromised, it can be killed and redeployed from the IaC. This can be done as frequently as necessary, knowing that the result will be the same.

General cATO Assessment Method



General cATO Assessment Method

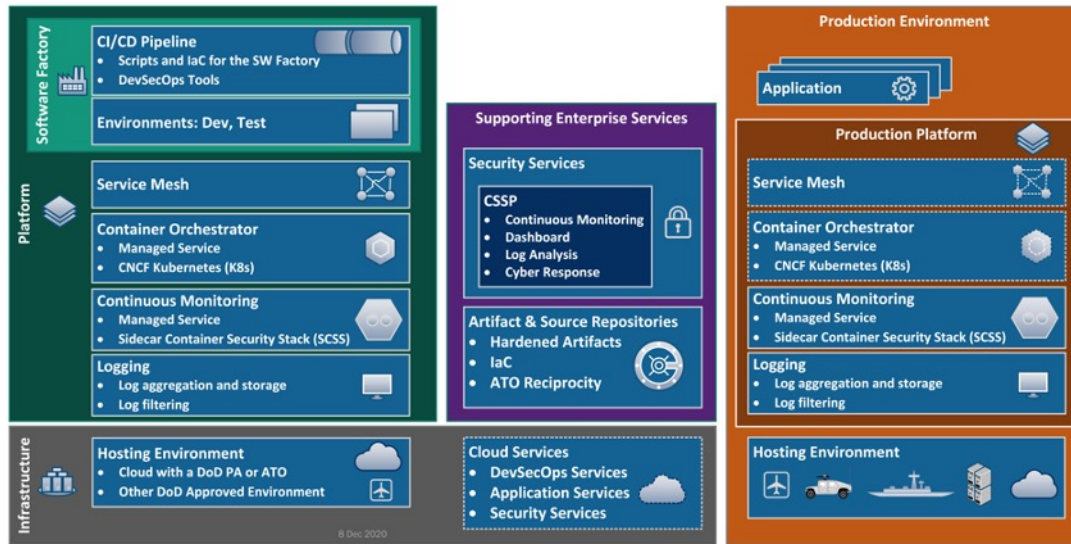


AO = Authorizing Official
PMO = Program Management Office

Image Source: MITRE

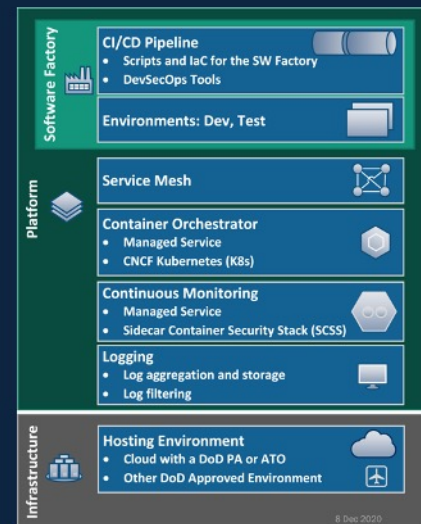
Platform

Authorize the Platform with Traditional RMF



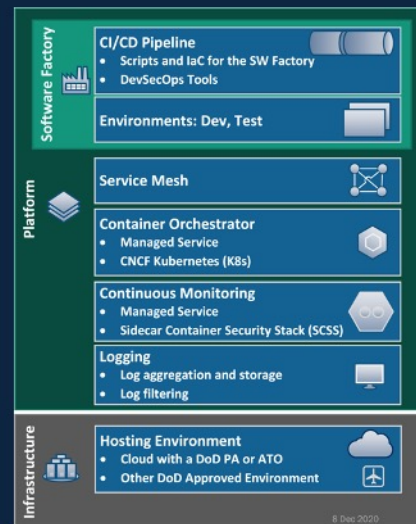
Authorize the Platform

- Use **“standard” RMF process to authorize the Platform** leveraging inheritance from the hosting environment and authorized-to-use components (Iron Bank or CSP)
- Use an **approved hosting environment**, such as a cloud service provider
- Authorize each platform layer to enable **swappable layers**
- Use **Infrastructure as Code (IaC)** to set up the Platform environment (dev, test, staging, prod)
- Use **Compliance as Code (CaC)** to validate compliance to STIGs for platform components
- Verify **control gates** are in place; parameters set by app owner
- Verify **dashboards** are in place and contain all necessary information
- Verify operations are in place, including the **Cybersecurity Service Provider (CSSP)**



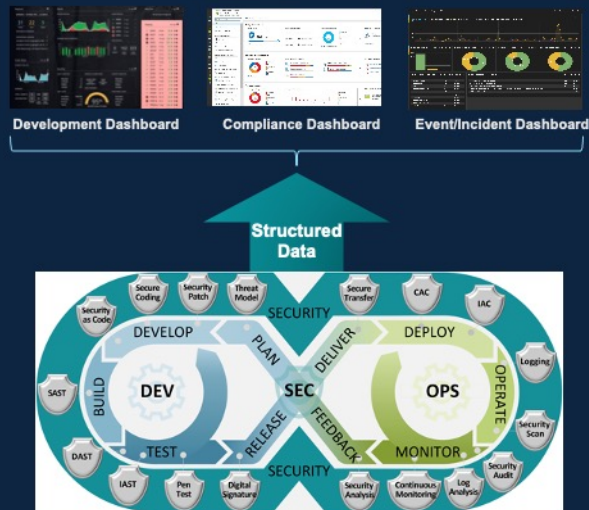
Authorize the Platform

- Platform supports **full life-cycle** from development through operations
- Platform is developed, operated and maintained as a **production system**:
 - Platform (including development, test, pre-production, and production environments) assessed and authorized using Risk Management Framework (RMF) processes
 - Platform incorporates continuous monitoring with integrated Tier 2 CSSP support
 - Continuous monitoring with behavior monitoring/zero trust enforcement
- Platform **implements DevSecOps**
 - Integrated cyber testing, monitoring, and event management for both the platform and components developed and operated on the platform
 - Automation: automated builds, testing, and deployments using Compliance as Code, Dynamic & Static App Security Testing, Pen Testing, Risk Determination with Control Gates
 - Infrastructure as Code: Reusable infrastructure and documentation, including a set of pre-approved architecture, technology stacks, and control implementations
- Software Factory may support **multiple CI/CD pipelines**



Dashboards for Continuous Monitoring

Switch from paper-based documents focused on a single point in time to **machine-generated structured data displayed in dashboards** for near real-time continuous monitoring, analysis, and response



Rather than just stating intentions in a document, **continuously prove software is still secure**

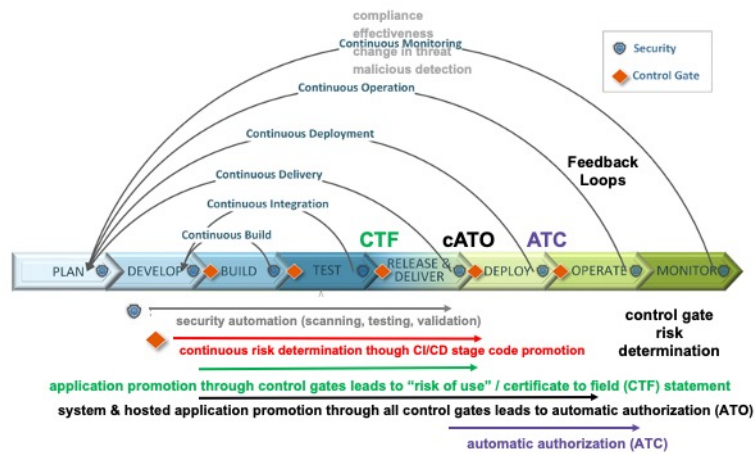
Dashboard Sources:

- [Representative Software Factory / DevSecOps Dashboard Using Hypecia](#)
- Compliance DB source: [Azure Security Center](#)
- [Representative Event / Incident Dashboard Using ELK](#)

Diagram Source: MITRE

Process

Automatic Risk Determination, Authorization, and Connection



MITRE

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED.

Image Source: MITRE

18

CI/CD = Continuous Integration / Continuous Delivery (or Deployment)

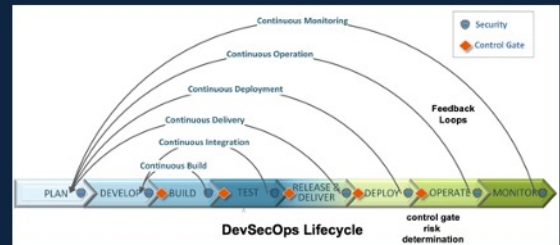
CTF = Certificate to Field

ATO = Authorization to Operate

ATC = Authorization to Connect

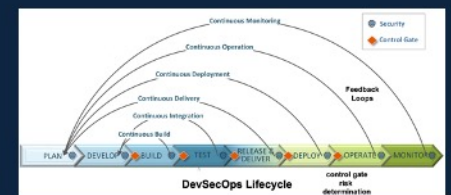
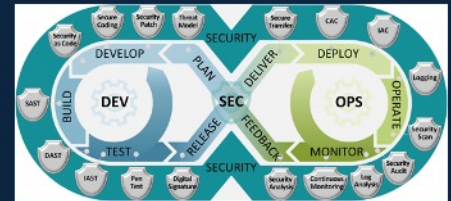
Authorize the Process

- Validate the automated process of building the SW
- Validate the automated workflow of building the SW
- Verify that the **control gates are in place** with appropriate parameters for performing AO's risk determination
- Verify resulting **dashboard** of security posture
- Verify key practices are performed:
 - Security control compliance & effectiveness
 - Use Compliance as Code (CaC) to validate compliance to STIGs for platform components
 - Monitoring threat landscape
 - Monitoring risk tolerance thresholds
 - Monitoring for malicious behavior



Authorize the Process Focus on Outcomes, Performance, & Measurement

- **Move from compliance-driven risk management to data-driven risk management**
 - Default to **structured data, not documents**. Documents generated on-demand from machine-readable and human-readable data
 - Support risk response decisions, security status information, and **ongoing insight into security control effectiveness**
 - **Information security continuous monitoring (ISCM)**: ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions
- **Process adaptable to differences in component/change risk, urgent mission needs, and agreed-to risk tolerance**
- **Transparency and repeatability:**
 - **All parties** (developers, operations, security, senior officials) **can access the information** they need, when they need it
 - **Repeatable, deterministic process**: All parties understand required and optional steps; outcomes are consistent and predictable
- **Enforced configuration and change management on code, artifacts, images, containers, executables through control gate enforcement and least privilege management**
- **ChatOps: Project collaboration for real-time interactive coordination among team members – developers, testers, administrators, cyber security monitors**

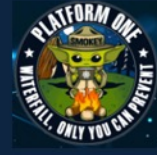


Platform One



Platform One Services

- Nicolas Chaillan, USAF CSO: <https://software.af.mil/dsop/documents/>
- [Platform One – YouTube](#)
- **Repo One – DoD Centralized Container Source Code Repository (DCCSCR)**
 - ❖ Central repository for the source code to create hardened, assessed containers for the Department of Defense
 - ❖ Container source code, Infrastructure as Code, K8S distributions, etc.
 - ❖ Repo One is currently operated at <https://repo1.dso.mil/dsop/>.
 - ❖ DoD activities that create containers which could benefit the DoD at an enterprise scale should publish their containers' source code in Repo One. They should follow the *DoD Enterprise DevSecOps Reference Design*, *Container On-boarding Guide*, and *Container Hardening Guide* requirements.
- **Iron Bank – DoD Centralized Artifacts Repository (DCAR)**
 - ❖ 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.
 - ❖ 300+ containers available.
 - ❖ Iron Bank is currently operated at <https://ironbank.dso.mil/>.
- **DevSecOps Platform (DSOP)**
 - ❖ DSOP – collection of approved, hardened Cloud Native Computer Foundation (CNCf)-compliant Kubernetes distributions, infrastructure as code playbooks, and hardened containers. This collection implements a DevSecOps platform compliant with the *DoD Enterprise DevSecOps Reference Design*, and its source code is hosted on Repo One.



Platform One Acquisition

- **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 developer model)
- **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 cATO. Perfect for large teams/programs that need a dedicated enclave.
 - Build and deliver new hardened containers as needed for program-specific software (pay per use/container).
- See more here: <https://p1.dso.mil/#/products>



Source: <https://software.af.mil/dsop/documents/> DoD Enterprise DevSecOps Initiative – Introduction



PLATFORM ONE | METRICS

Source: <https://software.af.mil/dsop/documents/>

ORGANIZATION

4 MILITARY
14 CIVILIAN
225+ CONTRACTORS
25+ COMPANIES
34 TOTAL CONTRACTS



BIG BANG

DEPLOYMENT PACKAGES

- GBSD
- F-35
- ARMY INSCOM
- CYBER COMMAND
- GPS OCX
- EDGEONE
- 76TH SWEG



COLLABORATION TOOLS

ACTIVE USERS

11,032 DAILY
16,620 MONTHLY



IRON BANK

339 CONTAINERS

PARTY BUS

2,347
PRODUCT DEVELOPERS

2,001
MICROSERVICES

26
APPS IN PRODUCTION

153
PRODUCT TEAMS

CNAP

24,000
DAILY
UNIQUE IPS



DORA

20.8 COMMITS PER DAY

- <2 DAYS FOR LEAD TIME
- 15 MIN TO RESTORE
- <5% CHANGE FAILURE RATE

Teams

Build the Teams

Authorize the Teams



Platform Team

Software Product Team

- Teams are checked against cyber & software workforce role certification / education / experience requirements (as per **DoDD 8140**, and the **DoD Cyber Workforce Framework (DCWF)**)
- Include members with cyber assessment and cyber monitoring experience
- Create a **training plan** for DevSecOps, Risk Management, and CA
- Collect **hiring and training metrics** to ensure team members across the program office are indoctrinated into the organizational DevSecOps and continuous authorization culture

Computers perform repetitive tasks - people solve problems

All team members are responsible for outcomes and relentlessly pursuing continuous improvement

Authorize the Teams

Authorize the Teams



Platform Team

Software Product Team

- Review program office personnel certification requirements, i.e., education, training, experience, against current staffing
- Interview the Teams for:
 - Knowledge of the DevSecOps processes
 - Understanding of agreed-to risk tolerance
- Verify that Teams exhibit DevSecOps culture
- Validate Training
 - Developers trained on developing secure code and tool security findings
 - Cybersecurity people trained on dashboards, machine-generated artifacts, and establishing control gate rule parameters
 - Testers trained on security test tools (e.g., code coverage)
 - ISSO, ISSM, Ops, assessors, AO trained on dashboards
 - Perform an integrated table-top exercise to ensure the individual teams work collaboratively to maintain the continuous authorization process
 - Monitor on-going team performance against the outcome metrics established for the program

Continuous Monitoring

Continuous Monitoring

Continuous Monitoring for DevSecOps			
Security Control Assessment	Security Status Monitoring	Security Status Reporting	Risk Tolerance Monitoring
- Manual risk assessment of sprint backlog - DevSecOps automated tool sprint assessments STIG (Compliance as Code), SAST, DAST, IAST & pen testing - Ops Incident analysis with feedback to DevSec - DevSecOps review of assessment findings	- Review security status: Tier II & III SIEM event log monitoring, control compliance/effectiveness, Analysis of cyber metrics and risk score - Review risk tolerance threshold monitoring: Review of change request impact analysis, Review of cyber findings, Review of threat landscape - Impact of risk to mission - Development of course of actions - Automated compliance checking and reporting	- Ongoing risk score/posture - Tolerance threshold trend data - Backlog list of security stories - Cybersecurity metrics: non-compliance, vulnerabilities, incidents, Sec issues on backlog - Change in threat	- Translate risk tolerance to security scanning / testing results - Assess based on time/event trigger - People certified for maintaining cATO - Process certified & accredited

Continuous Risk Monitoring & Continuous Risk Determination

Key points

- Translation of agreed-to risk tolerance into a set of CI/CD **control gate pass/fail rules** based on security automation findings that control promotion to the next CI/CD phase
- CI/CD **security findings that exceed the risk threshold trigger an event** to involve ISSM, assessor or AO then added to backlog for remediation in a 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
- SW product is under **continuous monitoring and visualization of security posture** by security team, assessor, and AO through the security visualization dashboards

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

control gates risk tolerance checks



Security Posture Visualization



Result: continuous risk analysis, risk determination, and authorization

Summary: Continuous Authorization

- Objective: Enable DoD to achieve elite DevSecOps performance and maintain the Department's technological advantage over near-peer adversaries
- Significant evolution from traditional practices
 - Authorize platform, process & teams, rather than product/system/application
 - Authorized platform supports full lifecycle – development through operations
 - Platform maintained as an operational system with integrated CSSP/Defensive cyber operations
 - Maximize use of automation and near real-time data-driven risk management
 - Immutability of production environment – maximum use of Everything as Code: Infrastructure as Code, Configuration as Code, Compliance as Code

Mark Smiley, Ph.D.
msmiley@mitre.org

in [linkedin.com/in/CloudDirector](https://www.linkedin.com/in/CloudDirector)

MITRE | SOLVING PROBLEMS
FOR A SAFER WORLD™