REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
03/05/2021	Conference Briefing	

4. TITLE AND SUBTITLE
Continuous Authorization with DevSecOps

5a. CONTRACT NUMBER
W56KGU-18-D-0004

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Mark D Smiley

5d. PROJECT NUMBER
0721K10BMD

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER
PRS-21-0440

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
United States Army (ACC-APG)

10. SPONSOR/MONITOR'S ACRONYM(S)
ACC-APG

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES
AFCEA Webinar on Continuous Authorization, online

14. ABSTRACT
Software is a foundational component of the modern defense departments. The current approach to software development is a leading source of risk for the U.S. Department of Defense (DoD): it takes too long exposing warfighters to unacceptable risk. To support national defense priorities, you need to deliver software rapidly and securely. DevSecOps practices and culture help improve both software delivery speed and cybersecurity.

15. SUBJECT TERMS
Maintenance and Enhancement; Software Verification; Software Distribution; security; continuous authorization; DevSecOps

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE		32	Susan Carpenito
					19b. TELEPHONE NUMBER *(Include area code)* 781-271-7646


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

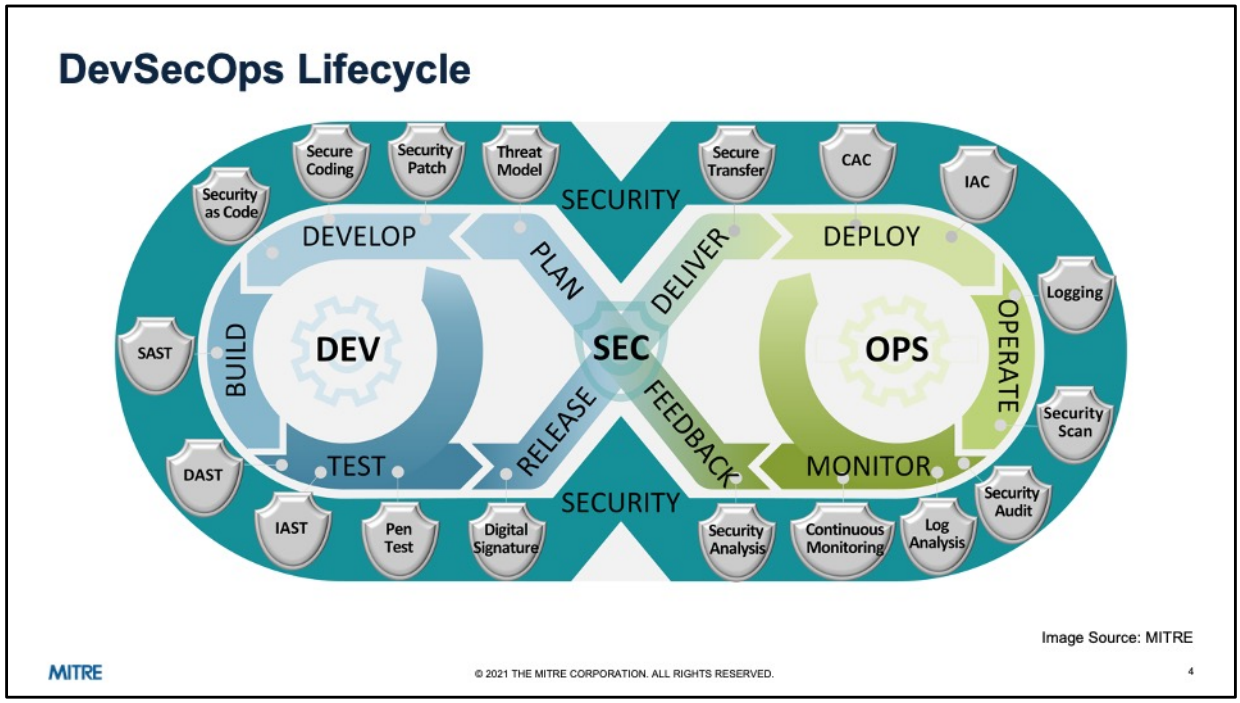
Image Source: MITRE

MITRE

What is DevSecOps?

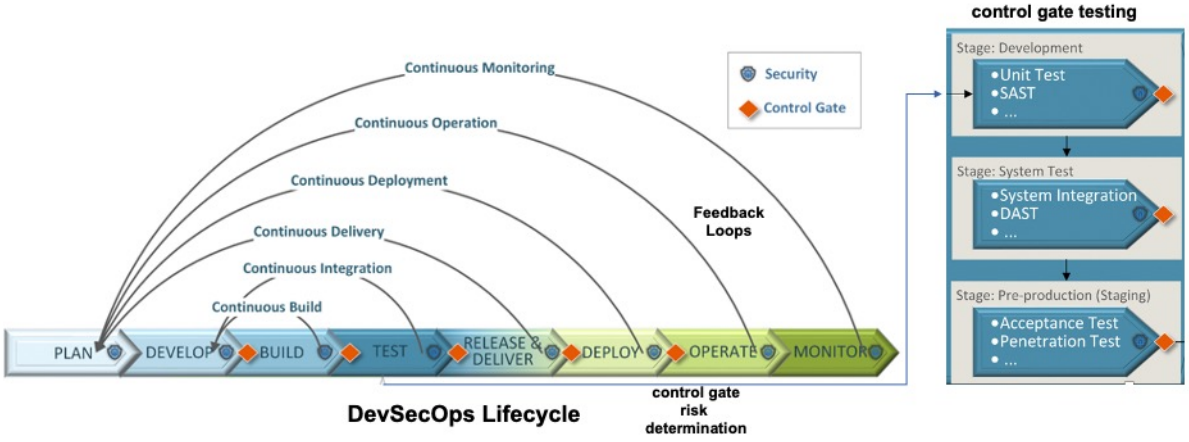
- DevSecOps is a culture and an approach to modern software delivery built on alignment of development (Dev), security (Sec) and operations (Ops) groups into an integrated team focused on continuous, incremental delivery of capabilities.
- The main characteristic of DevSecOps is to automate, continuously 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

MITRE



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



MITRE

Image Source: MITRE

5

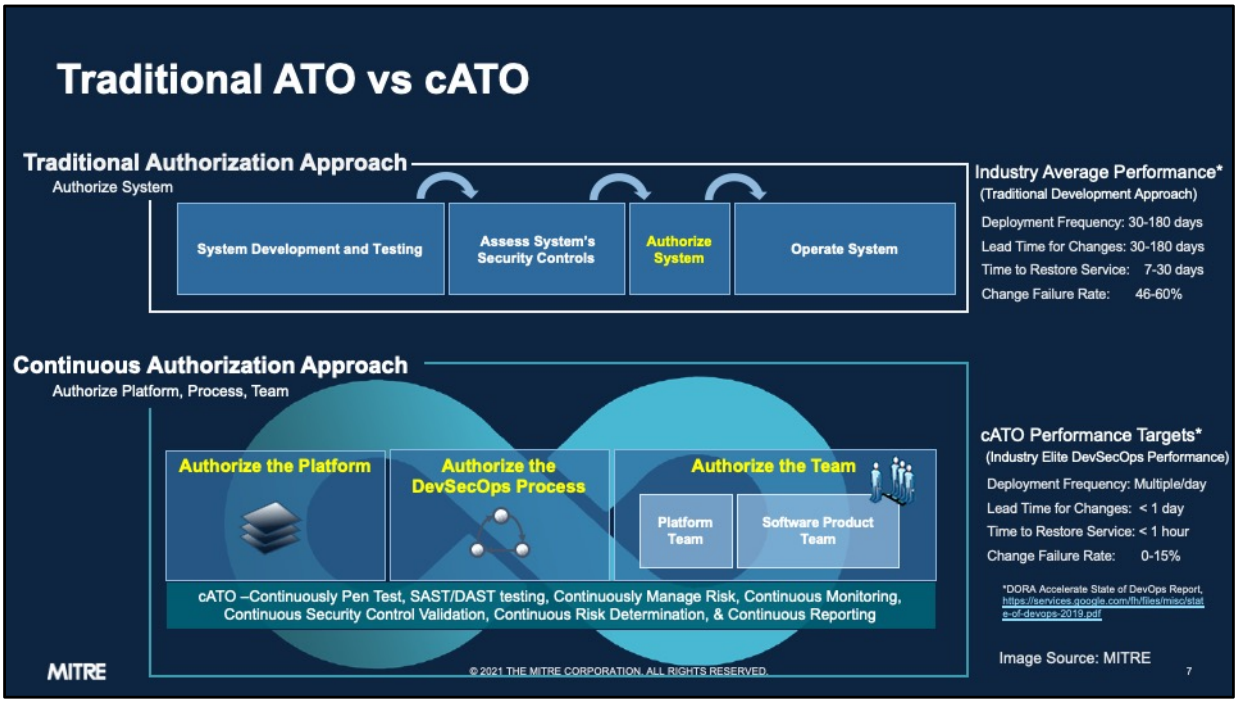
Continuous Authorization Method: High Level

- **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

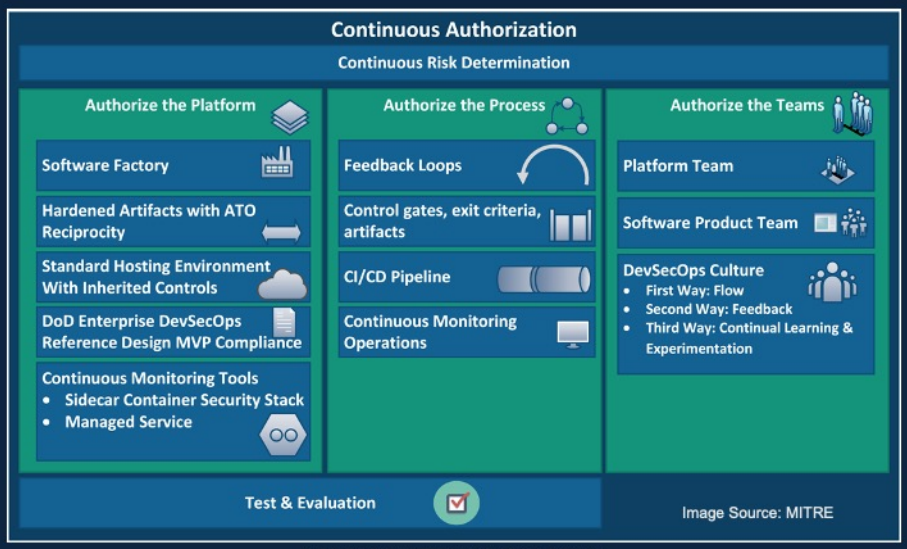
Image Source: MITRE

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

Traditional ATO vs cATO

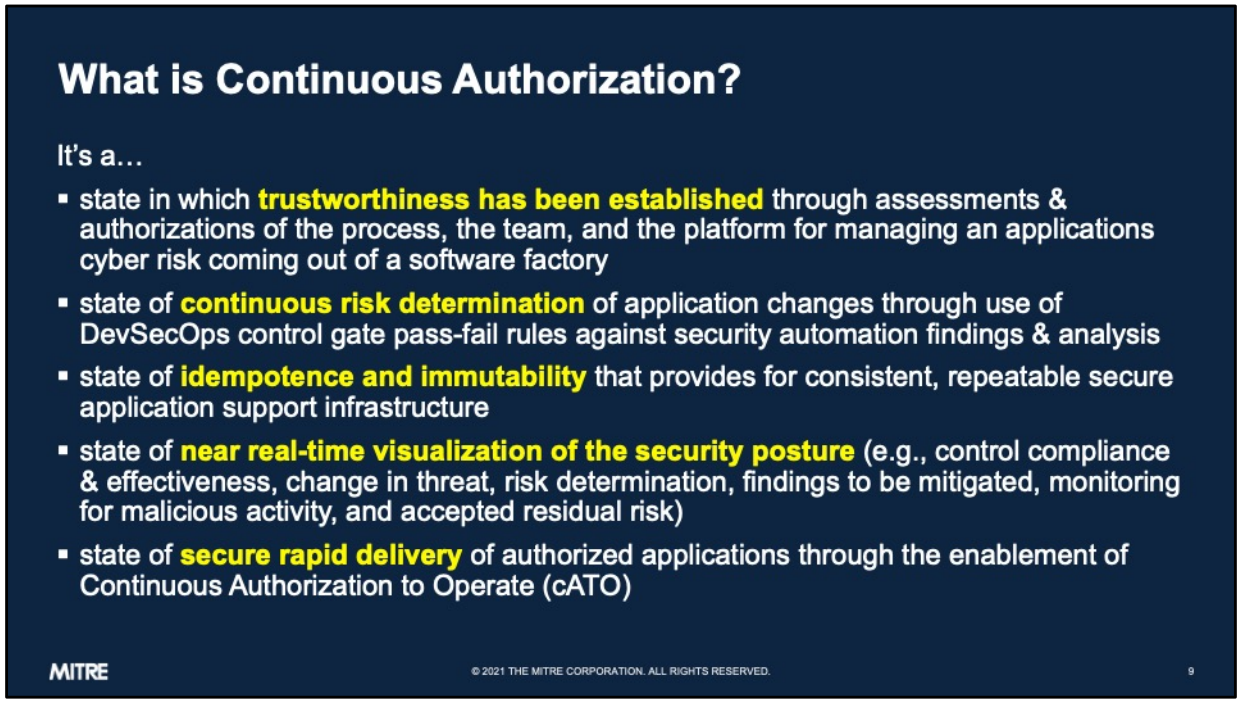


Continuous Authorization: Overview



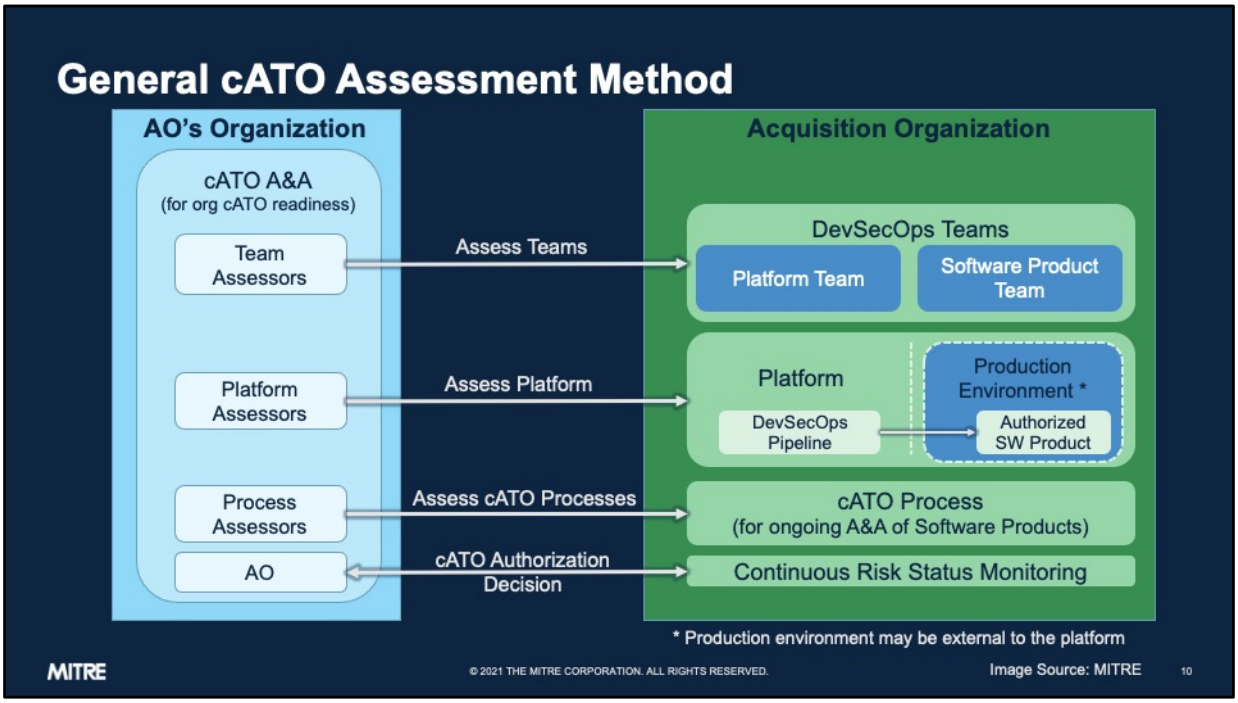
MITRE

8



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 agai n, 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 don e as frequently as necessary, knowing that the result will be the same.

General cATO Assessment Method

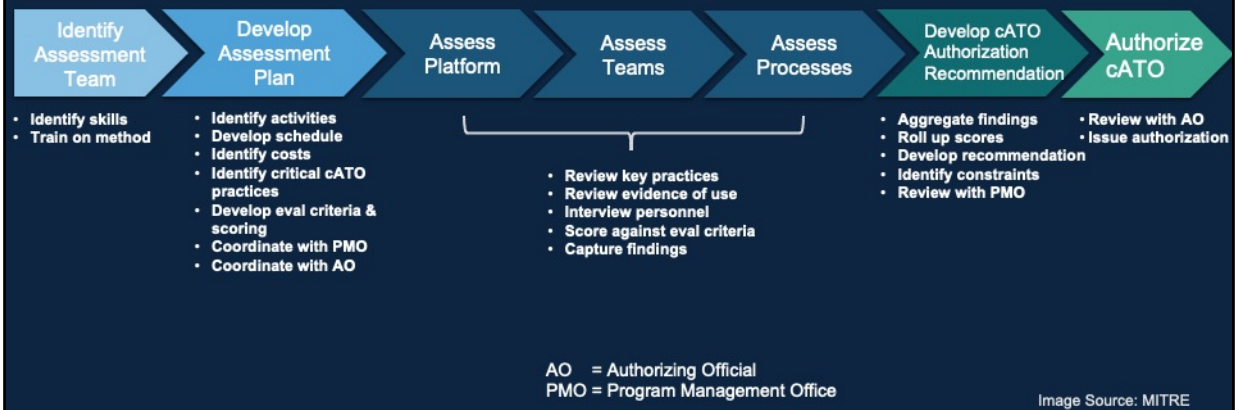


MITRE

Image Source: MITRE

10

General cATO Assessment Method



AO = Authorizing Official
PMO = Program Management Office

Image Source: MITRE

MITRE

Platform

MITRE

Authorize the Platform with Traditional RMF

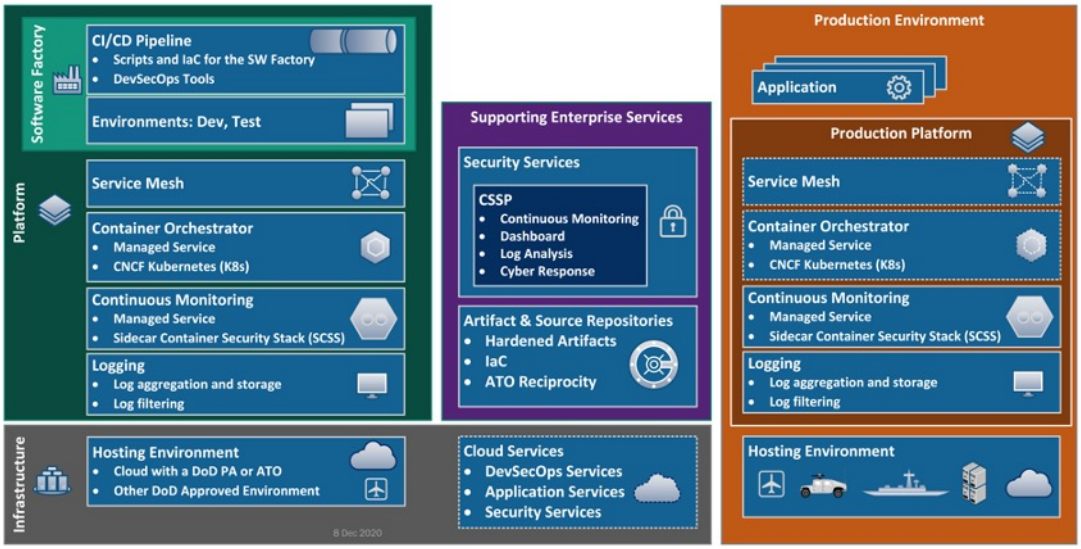


Image Source: MITRE

MITRE

13

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)**

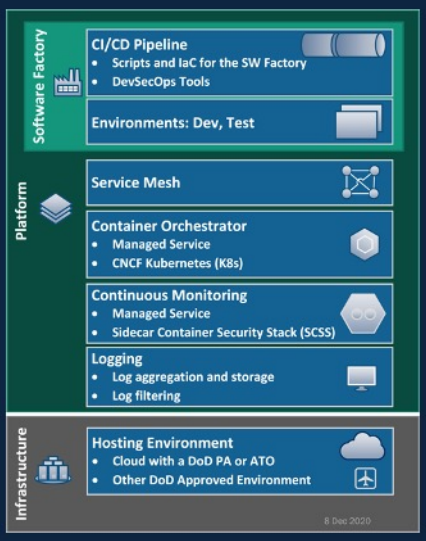


Image Source: MITRE

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**

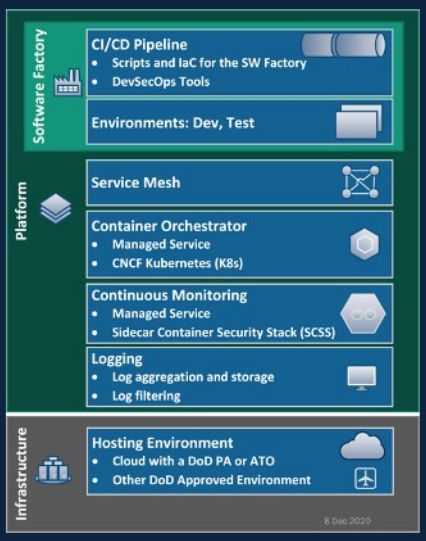
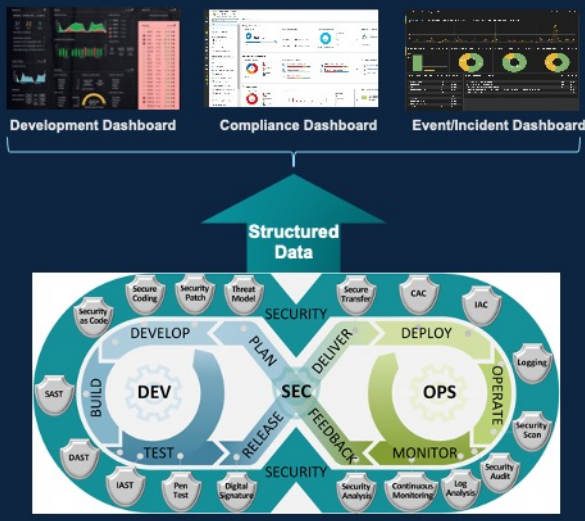


Image Source: MITRE

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 Hygieia
- Compliance DB source: Azure Security Center
- Representative Event / Incident Dashboard Using ELK

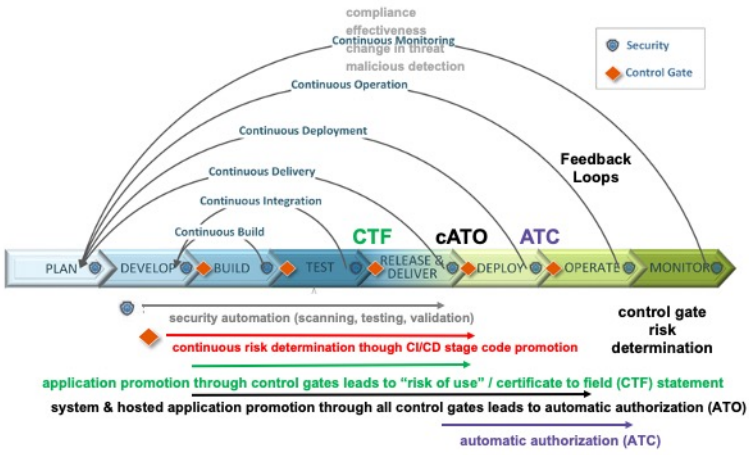
Diagram Source: MITRE

MITRE

16

Process

Automatic Risk Determination, Authorization, and Connection



MITRE

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

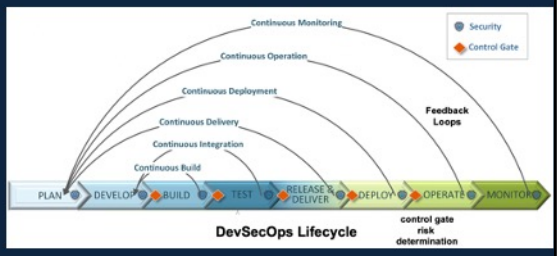


Image Source: MITRE

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**

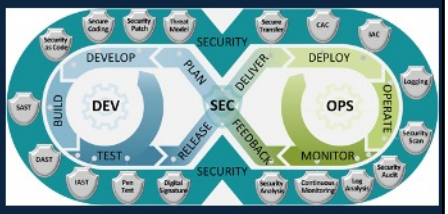


Image Source: MITRE

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 Defens
  - ❖ 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.

Source: https://software.af.mil/dsop/services/

MITRE

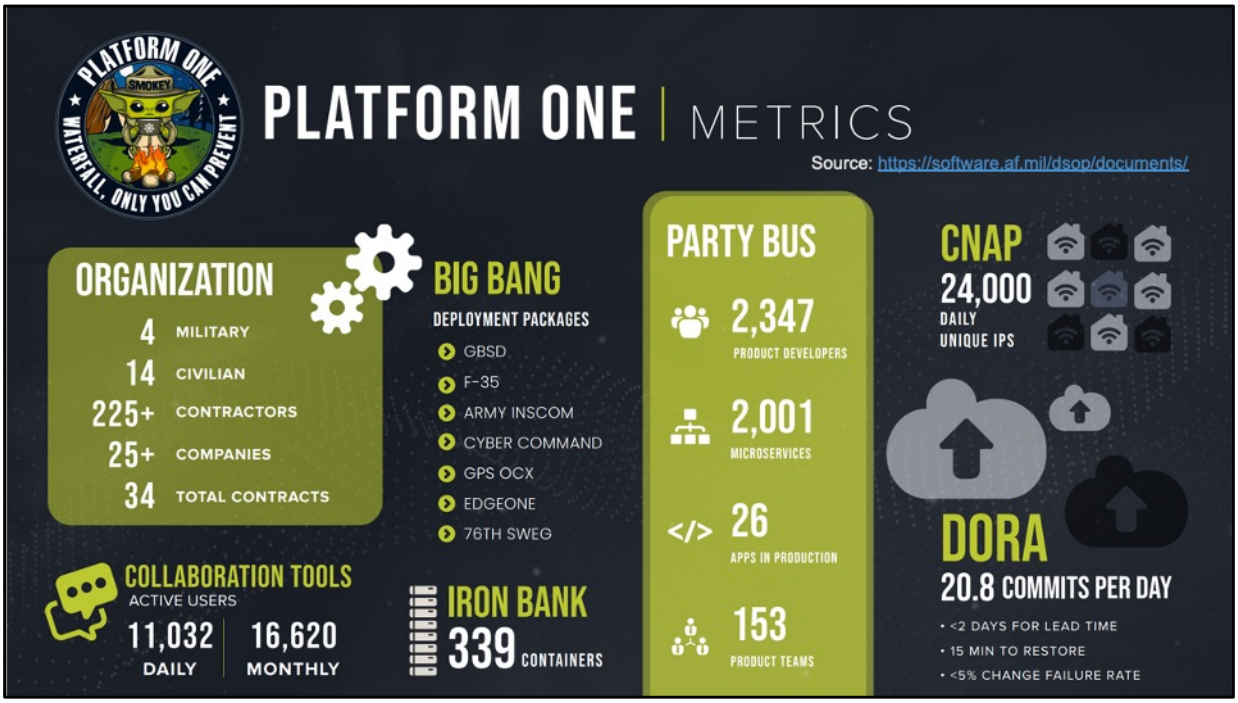
22

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
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
COLLABORATION TOOLS
ACTIVE USERS
11,032 DAILY
16,620 MONTHLY
IRON BANK
339 CONTAINERS

Teams

MITRE

Build the Teams

- 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

MITRE

Image Source: MITRE

26

Authorize the Teams

- **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

MITRE

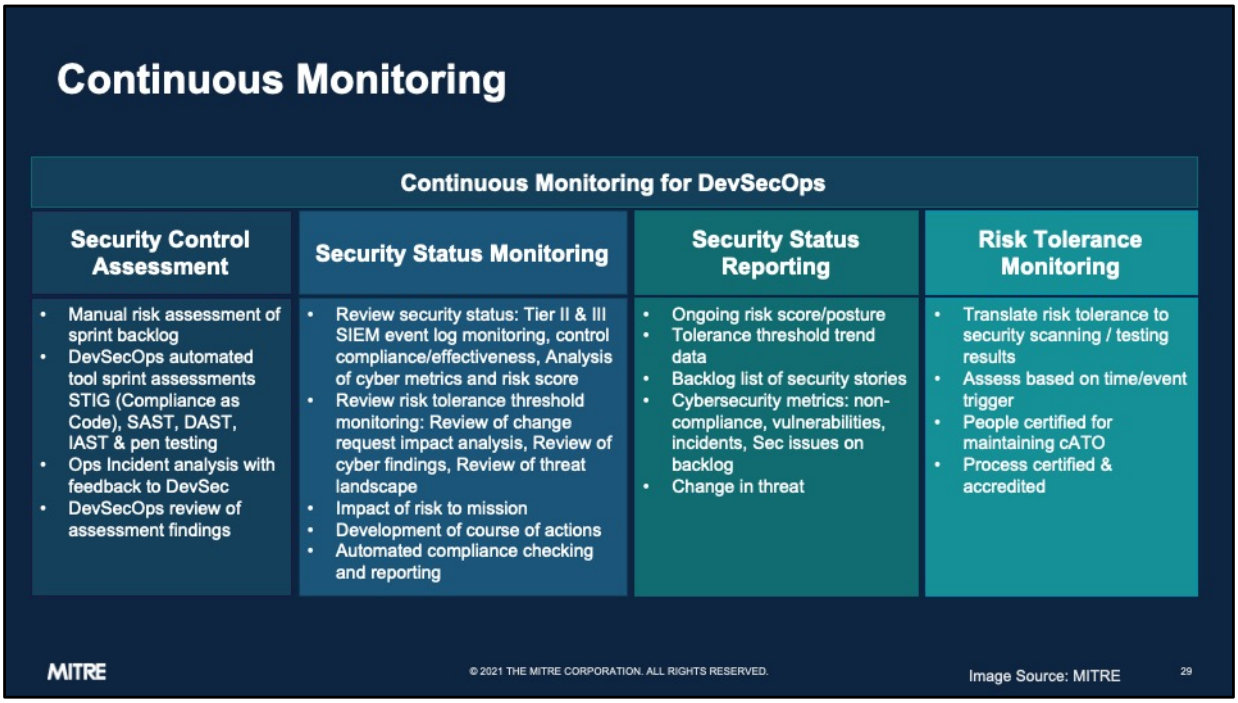
Image Source: MITRE

27

Continuous Monitoring

MITRE

Continuous Monitoring



MITRE

Image Source: MITRE

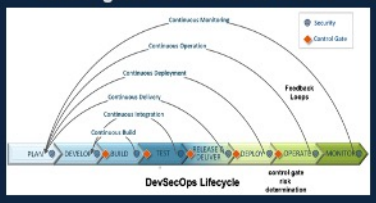
29

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

MITRE

Image Source: MITRE

30

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

MITRE

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

linkedin.com/in/CloudDirector

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™