DevSecOps: How We Apply Security Into the DevOps Pipeline

Heath J. Ferry

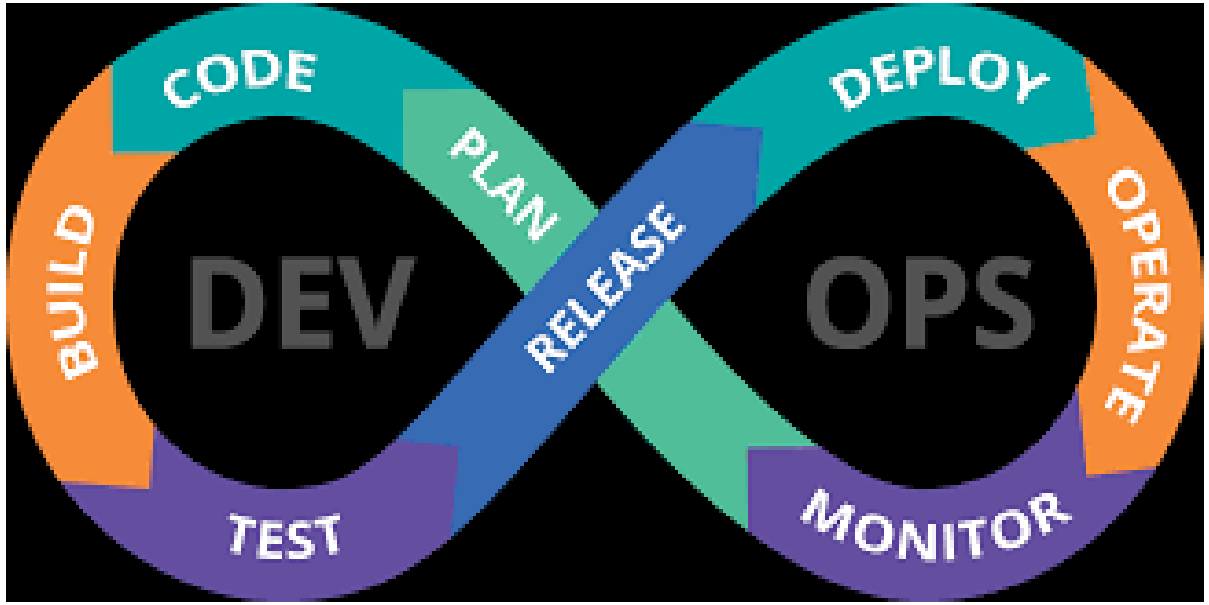
Professor of Cybersecurity

Learning Objectives

- DevOps and it's benefits
- Define DevSecOps
- Why DoD is shifting to DevSecOps
- Additional Training

What is DevOps?

- **DevOps** is a software engineering culture and practice that aims at unifying software development (Dev) and software operation (Ops).
- The main characteristic of the DevOps movement is to strongly advocate automation and monitoring at all steps of software construction, from integration, testing, releasing to deployment and infrastructure management.
- DevOps aims at shorter development cycles, increased deployment frequency, and more dependable releases, in close alignment with business objectives.



DevOps is NOT ENOUGH!

DevSecOps is what must be implemented with the cybersecurity stack built-in into the DevOps pipeline.

Benefits of DevOps

- Implementing DevOps allows organizations to get more done.
- Leveraging DevOps and implementing continuous integration and continuous delivery (CI/CD) allows organizations to see a tremendous improvement in deployment frequency, lead time, detection of cybersecurity vulnerabilities and flaws, mean time to repair and mean time to recovery.
- Allows for rapid experimentation and uncertainty while focusing on mission end goals.
- Enables rapid prototyping and A/B testing or canary releases.
- Makes new services and innovations available.
- Increases frequency of deployments
- Increases collaboration between various departments
- Greatly Reduces time spent maintaining applications and fixing them
- Increases the number of end users who are using organizations' services
- Improves performance and quality of applications
- Reduces time-to-market
- Reduces time needed for testing, development and operations
- Avoids shadow IT by enabling all directorates/divisions/services to reuse the DevSecOps pipeline instead of reinventing the wheel and building their own pipeline without supervision
- Avoids technical debt by continuously fixing bugs and security issues thanks to automated tests and real-time scans.

DevOps Challenges

- Culture
- Test automation
- Legacy systems
- App complexity
- No DevOps plan
- Managing environments
- Skillset
- Budget
- Tools
- Leadership support

Extreme DevOps Risk Management Example — Chaos Monkey (Netflix)

- Chaos Monkey is a tool invented in 2011 by Netflix to test the resilience of its IT infrastructure. It works by intentionally disabling computers in Netflix's production network to test how remaining systems respond to the outage. Chaos Monkey is now part of a larger suite of tools called the Simian Army designed to simulate and test responses to various system failures and edge cases.
- As part of the DevOps movement, special attention is paid to the safe operation of computer systems, thus providing a sufficient level of confidence despite frequent releases. By contributing to the DevOps Tool Chain, Chaos Monkey meets the need for continuous testing.
- They are part of the pattern "Design for failure", "designed to support failure": a computer application must be able to support the failure of any underlying software or hardware component.

https://en.wikipedia.org/wiki/Chaos_Monkey

NETFLIX

SRE/NoOps Telemetry Metrics: DT/ATO gold

- **100s** of microservices (~20 core)
- **1,000s** of daily production changes
  - code pushes / feature toggles
- **10,000s** virtual instances (inside AWS)
- **100,000s** of customer interactions per second
- **1,000,000s** of customers (81.5M+ global users)
- **1,000,000,000s** of time series OPS metrics
  - 2.5B time series metrics / minute
  - delivered processed and stored
- **10,000,000,000** hours streamed every quarter

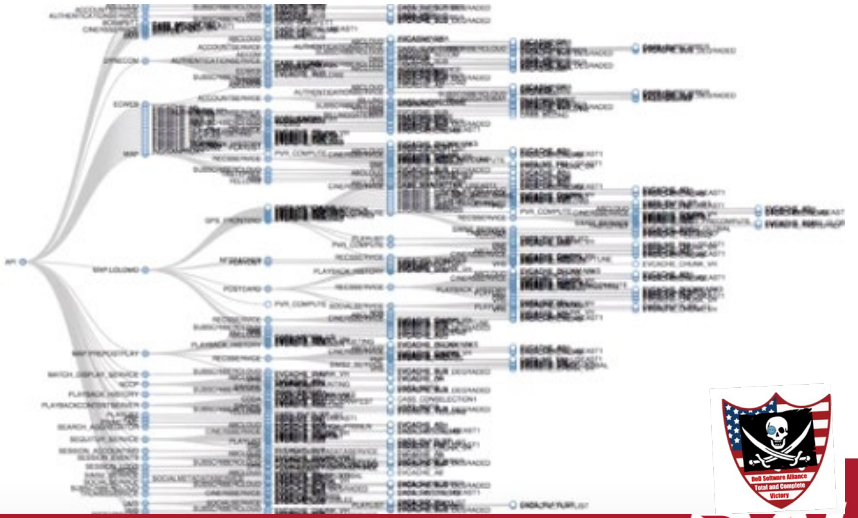
- **10s** of ops engineers
  - **NoOps**: all developers/engineers full access to PROD
  - No push windows
  - Freedom and responsibility
- **0** network ops centers (automation)
- **0** data centers (focus on innovation)

Telemetry +
Chaos Engineering

LARGE DATA & TELEMETRY COMPANY

microservices running in 2014:

breakdown of one service & call paths



DAU

What is DevSecOps?

- DevSecOps is short for Development, Security and Operations. The objective is to make everyone accountable for security with the objective of implementing security decisions and actions at the same scale and speed as development and operations decisions and actions.
- Every organization with a DevOps framework should be looking to shift towards a DevSecOps mindset and bringing individuals of all abilities and across all technology disciplines to a higher level of proficiency in security.
- From testing for potential security exploits to building business-driven security services, a DevSecOps framework that uses DevSecOps tools ensures security is built into applications.
- By ensuring that security is present during every stage of the software delivery lifecycle, we experience continuous integration where the cost of compliance is reduced and software is delivered and released faster.

DevSecOps Concepts

- DevSecOps describes an organization's culture and practices enabling organizations to bridge the gap between developers, security team, and operations team; improve processes through collaborative and agile workflows; drive for faster and more secure software delivery via technology; and achieve consistent governance and control.
- There is no uniform DevSecOps practice. Each DoD organization needs to tailor its culture and its DevSecOps practices to its own unique processes, products, security requirements, and operational procedures.
- Embracing DevSecOps requires organizations to shift their culture, evolve existing processes, adopt new technologies, and strengthen governance.

What are benefits of DevSecOps?

The benefits of DevSecOps are:

- Enhanced automation throughout the software delivery pipeline eliminates mistakes and reduces attacks and downtime.
- With a test-driven development environment in place and automated testing and continuous integration part of the workflow, organizations can work seamlessly and quickly towards a shared goal of increased code quality and enhanced security and compliance.
- For teams looking to integrate security into their DevOps framework, the process can be completed seamlessly using the right DevSecOps tools and processes.

Agile vs DevSecOps

DevSecOps is the next evolution of agile and builds on the agile principles by adding the following:

- Leverages Containers and Microservices concepts
- Leverages Cloud deployment for scalability and prototyping
- Continuous Integration/Continuous Delivery to rapidly prototype, test and deploy
- Leverage A/B testing and canary deployment for rapid feedback loops
- Embed security in the pipeline instead of an afterthought

Automated Testing

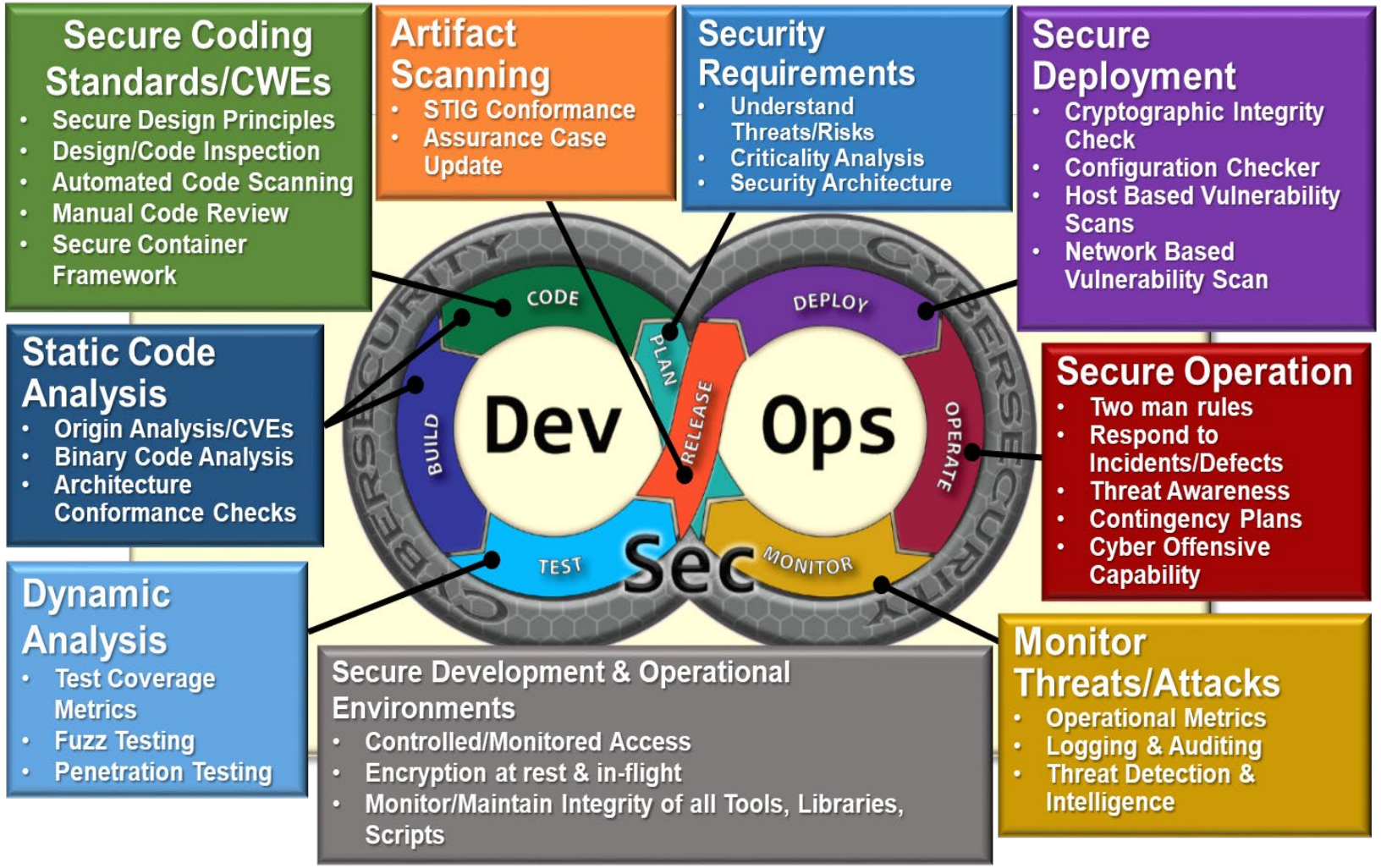
- Automated testing is a key part of DevSecOps. It is enabled by multiple tools that measure both test code coverage and test results. They are fully automated and do not require human action.
- It also enables new concepts like pair programming and peer code review.
- Agile brings several new models for creating the right tests:
- **Test-driven development (TDD)** is a software development process that relies on very short development cycles: requirements are turned into very specific test cases first, then the software is built to pass the tests.
- **Acceptance test–driven development (ATDD)** is a development methodology based on communication between the business customers, the developers, and the testers. ATDD encompasses many of the same practices as specification by example, behavior-driven development (BDD), example-driven development (EDD), and support-driven development also called story test–driven development (SDD). All these processes aid developers and testers in understanding the customer's needs prior to implementation and allow customers to be able to converse in their own domain language.

Why DevSecOps in the DoD

- DevSecOps is DoD's strategy for rapid delivery of secure and reliable software that gives the Warfighter a competitive advantage on the modern battlefield.
- DevSecOps is a modern way of life and approach to software development, security, and operations.
- It supports DoD's strategy to radically increase speed -- and reduce cycle time – to deliver war-winning capabilities.

Secure Software: Compliance Necessary but Insufficient

- Sec in DevSecOps is integrated the planning, architecture & design, and embedded throughout the entire process
- DevSecOps shifts Cybersecurity to the left; true risk managed process
- Cybersecurity risk is continuously scanned, evaluated & monitored – yields accessible, automated artifacts enabling continuous ATO



DevSecOps mindset: "Everyone is responsible for security."

DAU

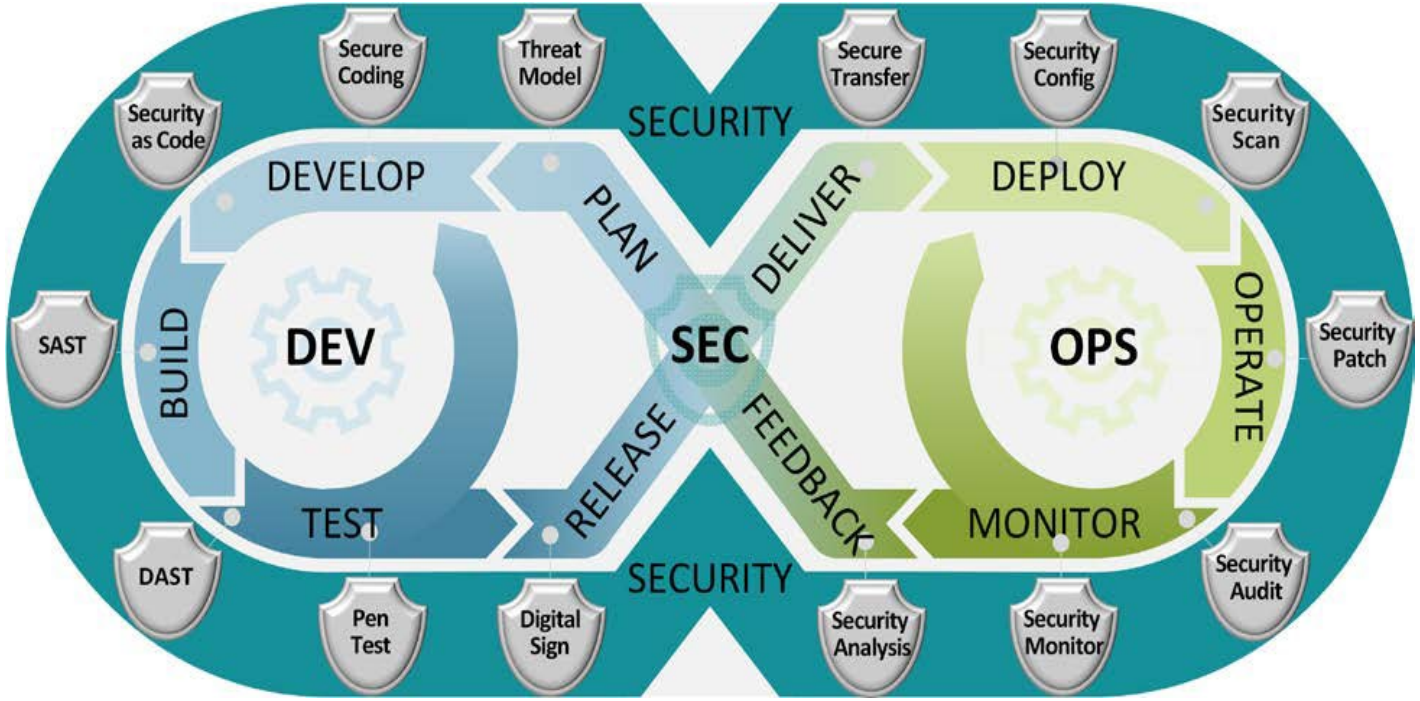
Change from “traditional” to DevSecOps

From	To
Waterfall projects and big heavy releases.	Small batches delivered frequently, leading to more frequent deployments and faster cycle times.
Slow feedback cycles with a lot of manual reviews and approvals; long wait times.	Real-time feedback and metrics driven by automated workflows.
Process-heavy and time-intensive management of change requests. Having to provide context to approvers who are not directly involved with the work.	Collaborative software development, automated delivery pipelines and decisions made by teams doing the work.
Teams are organized by technology or functional boundaries. Manual handoffs between siloed teams. Misaligned incentives.	Early stakeholder involvement across the value stream at every stage of the delivery lifecycle: design, build, deploy, monitor and maintenance. Stakeholders include auditing, compliance, change management, security, network, storage, middleware and enterprise architects. Teams are aligned to business goals.

“ The problem isn't change, per se, because change is going to happen; the problem, rather, is the inability to cope with change when it comes.”

— Kent Beck, Extreme Programming Explained: Embrace Change

DevSecOps Software Lifecycle



With DevSecOps, the software development lifecycle is not a monolithic linear process.

The “big bang” style delivery of the Waterfall process is replaced with small but more frequent deliveries, so that it is easier to change course as necessary.

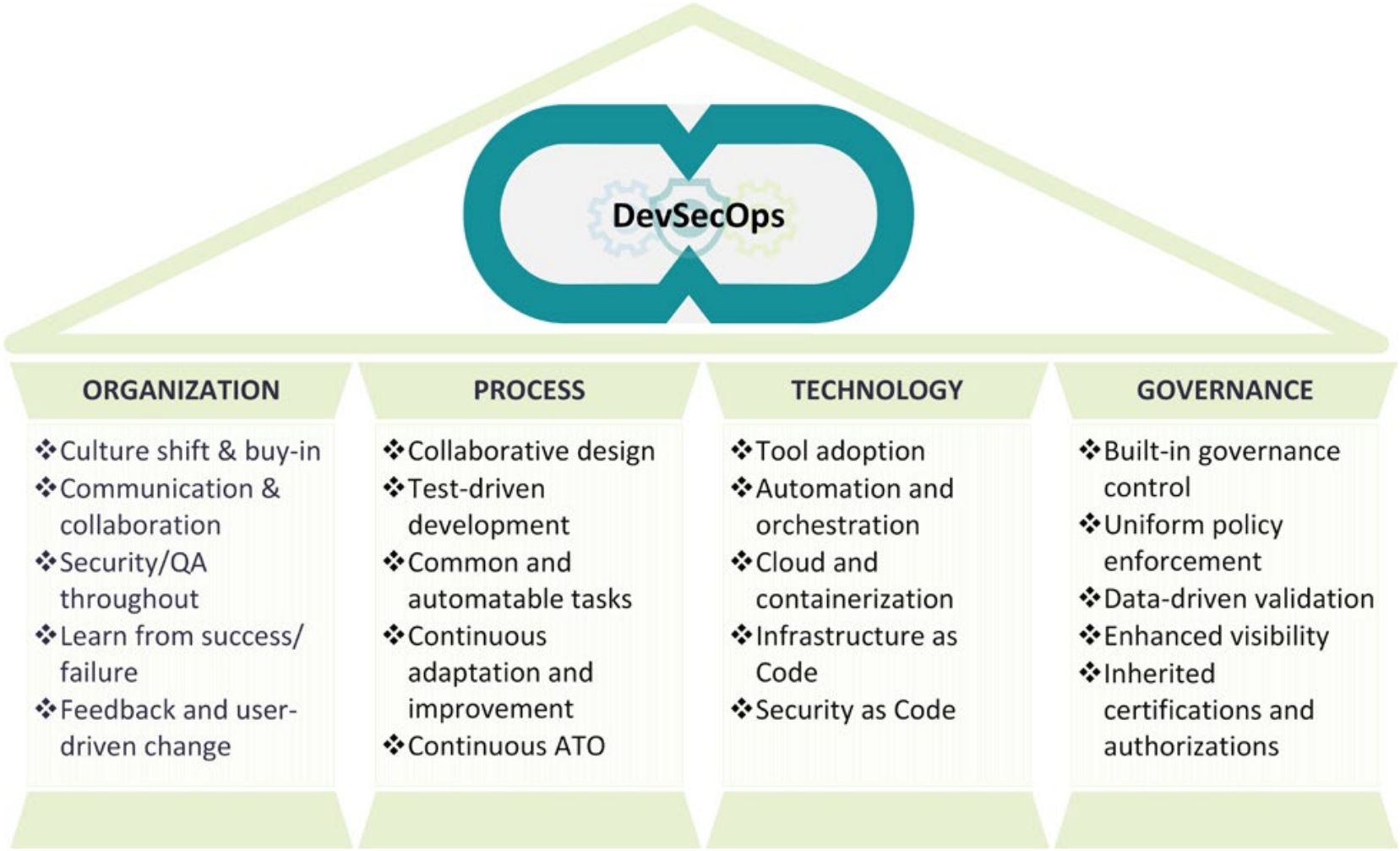
Each small delivery is accomplished through a fully automated process or semi-automated process with minimal human intervention to accelerate continuous integration and delivery.

The DevSecOps lifecycle is adaptable and has many feedback loops for continuous improvement.

DevSecOps Pillars

DevSecOps are supported by four pillars:

- Organization,
- Process,
- Technology,
- Governance

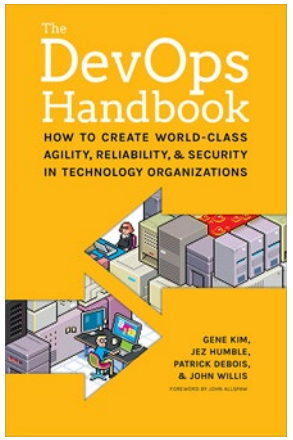


The Three Ways of DevSecOps

The First Way: The Principles of Flow

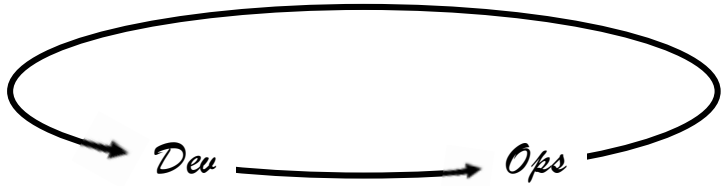
The Second Way: The Principles of Feedback

The Third Way: The Principles of Continual Learning and Experimentation

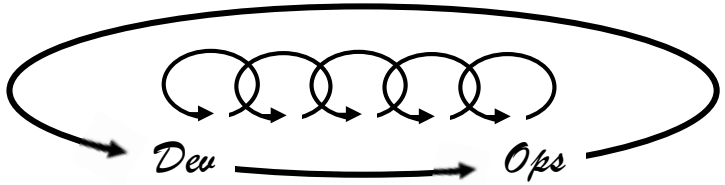


*A set of principles and practices emphasizing **collaboration** and **communication** between software development teams and IT operations staff along with acquirers, suppliers and other stakeholders in the life cycle of a software system.*

The First Way



The Second Way



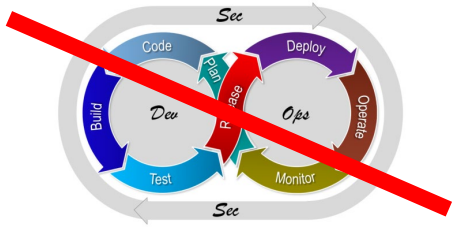
The Third Way

Anti-DevOps

Threat to mission: manual build/test/release

Late Integration / Late Learning / Late Defect Discovery

- Long cycle times between deliveries
  - 18-24 months
- Manual, error prone builds
  - Prone build times measured in weeks, months, or even years
- Lack of modern SW development practices
  - Morale destroying



Our Reality

- Late stage “big bang” integration with manual testing for 5 or more years
- Anti-Parity
  - Varying development, integration and production environments
- Manually deploying and testing code in production environment
  - 6-12 Months
- Code and unit test cycles occurring in weeks as opposed to hours
- End-to-end, system integration testing occurring in months vice days or hours

Defense Science Board Calls for Change

Software Factory

- A key evaluation criteria in the source selection process
  - Efficacy of offeror's software factory
  - **DoD has limited expertise – focus on acquisition**

Continuous Iterative Development

- DoD and defense industrial base partners
  - Deliver minimum viable product (MVP)
  - **Establish MVP in its formal acquisition strategy,**
  - Require of all programs entering Milestone B for all ACATs

Workforce

- Services need to develop workforce competency (prioritize acquisition strategy, source selection)
- DAU develop curricula to develop **SW-informed PMs, sustainers, acquisition specialists**

FY19 NDAA Sec. 868. Implementation of recommendations of the final report of the Defense Science Board Task Force on the Design and Acquisition of Software for Defense Systems.

Not later than 18 months after the date of the enactment of this Act, the Secretary of Defense shall, except as provided under subsection (b), commence implementation of each recommendation submitted as part of the final report

DevSecOps Values & CALMS

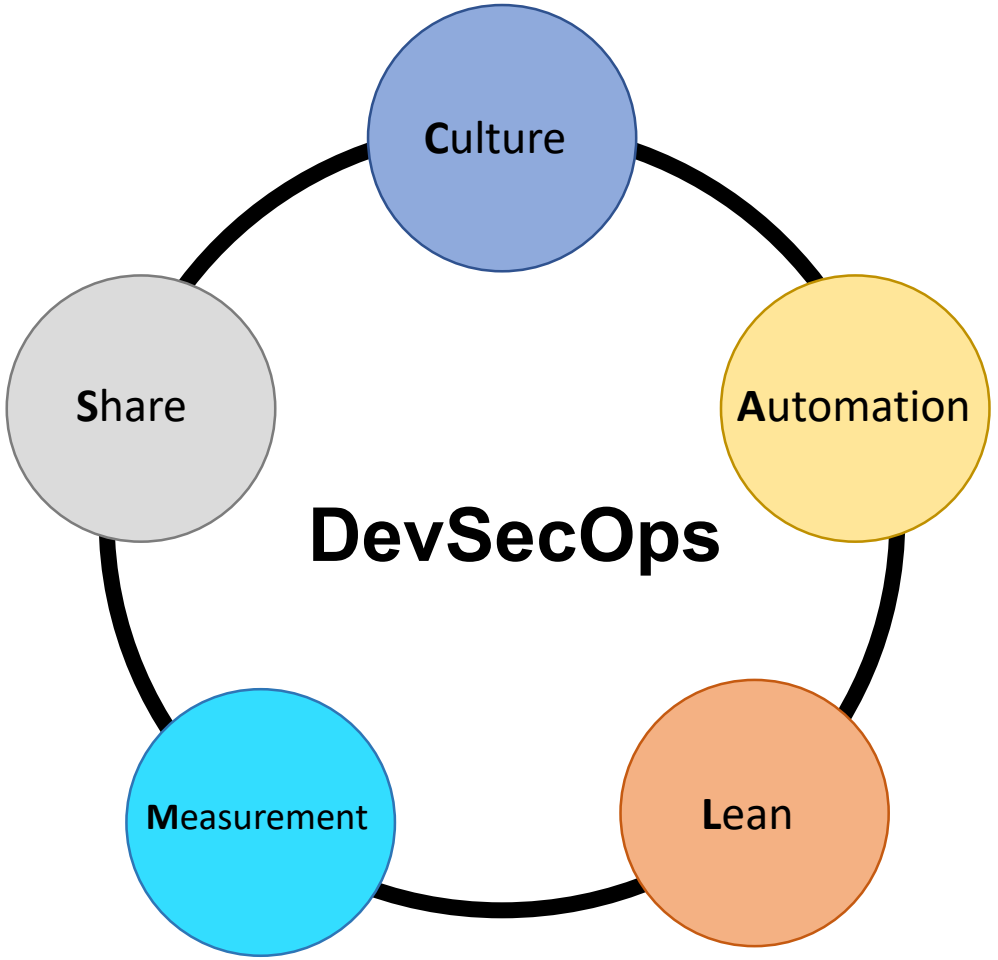
Culture of Teaming

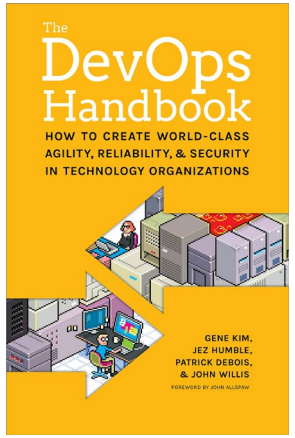
Collaboration
Dev, Operations and Security Partnerships

Infrastructure as Code (IaC)
SW that captures how infrastructure is configured

Automation
Use tools to automate the process as much as possible

Continuous Monitoring
Security & performance monitoring: Dev through Ops





Workshops/Courses

SW Acquisition

- Software Acquisition Pathway (1 hour)

Agile

- ACQ 1700 (2 days)
  - Can customize Agile training (2-3 days)
- SES/ FOGO Brief (90 min)
- Specialized Certification Training
  - From Scaled Agile (SAFe)

DevSecOps DSOD

Intro to DSO for DoD (2 days, 1 day)
DevSecOps for Cyber Professionals (DCP) (2 days)
Featuring Hands-On Demo of DSO Pipeline
DSO SES/FOGO Brief (90 min)

Cloud

Intro to Cloud Services (3 days)
Cloud Security (2 days)

Online Continuous Learning Courses

SW Acquisition

- CLE 078 Software Acquisition for the Program Office Workforce (SAPOW)
- CLE 084 – Models, Simulations, & Digital Engineering

Agile

- CLE 076 Introduction to Agile Software Acquisition

DevSecOps & Cloud

- CLE 075 Introduction to DoD Cloud Computing

Cyber

- CLE 074 – Cybersecurity Throughout DoD Acquisition
- CLE 081 Software Assurance

DBS

- CLE 077 -- Defense Business Systems (DBS) Acquisition
- CLE 083 – Information Technology Service Management (ITSM)

Questions?