Accelerate Adoption of DevSecOps

Proven reference architecture for DevSecOps ensures security in every stage of the development lifecycle.

With more than 12,000 incidents since 2015, U.S. Department of Defense (DoD) systems are an almost constant target for cyber-attacks. The recent cancellation of the Defense Intelligence Information Enterprise (DI2E), a secure tool chain used widely in the DoD, has left defense development teams scrambling to identify new methods for delivering secure software. However, selecting and integrating diverse software development tools to create a secure development environment can be time-consuming and difficult. A DevSecOps approach is essential, combining the accelerated software delivery and deployment of modern DevOps methods with advanced security at every stage of development.

Introducing DevSecOps from Flywheel Data

Flywheel Data has created a DevSecOps reference architecture that addresses the need for a development environment that facilitates secure software development, resulting in fully tested and vetted code that is as secure as possible. Our approach allows software teams to take control of security while adopting modern development practices. Flywheel has selected and integrated a complete set of tools that automate the software development life cycle—including the CI/CD pipeline—to minimize the introduction of error that result from manual operations.

Designed and implemented using best-of-breed components from trusted vendors, this reference architecture increases collaboration, allowing software teams to plan, build, and deploy secure software in less time and with less manual toil.

Solution Benefits

Grounded in the principles of DevSecOps, our solution utilizes a highly adaptive platform capable of supporting diverse use cases. Benefits include:

- **Simplified procurement.** All components are pre-defined. Flywheel offers multiple GWACs for procurement and can provide a single SKU.
- **Rapid deployment.** Because it eliminates the need for component selection, integration, and testing, this DevSecOps solution can be deployed in far less time.
- **Reduced sustainment costs.** Well-integrated, highly elastic, and highly automated architecture reduces management and maintenance.
- **Built-in security.** Best-of-breed components are designed to ensure security during development and facilitate the delivery of more secure software.
- **Increased quality.** Less opportunity to introduce human error.
- **Enhanced productivity.** Provide a golden path for secure software development and automate repetitive tasks to reduce toil.

What is DevSecOps?

DevSecOps evolved out of the need for fast delivery of secure software. It is a security-first development approach that operates in conjunction with a continuous integration and continuous delivery (CI/CD) pipeline to integrate security practices at every stage of the development lifecycle. With DevSecOps, the delivery of secure software is everyone's responsibility, not just the responsibility of the testing team. DevSecOps reduces the likelihood of introducing common vulnerabilities and exposures (CVEs) into operational code, greatly reducing opportunities for exploitation.

Building a DevSecOps Software Factory

DoD development teams need a software assembly line that is secure, efficient, and easy to manage, while enabling you to quickly build, test, and deploy applications. The DoD often refers to this as a software factory. The software factory eases implementation of DevSecOps with a well-defined, repeatable path to create and update applications. An organized, structured approach offers a faster cadence and delivers a more secure software application to production, while also enhancing developer productivity.

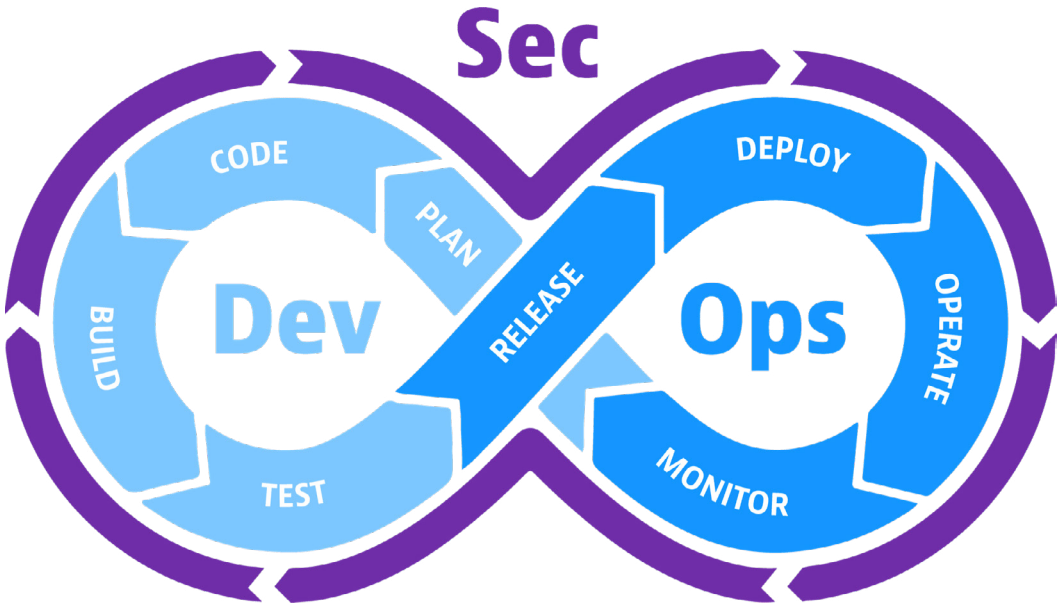
Containers are used to package application services, and application are orchestrated using Kubernetes. Infrastructure as Code (IaC) methods ensure that the required infrastructure is deployed and configured correctly every time, eliminating the time-consuming debugging that is often necessary after a manual or semi-automated infrastructure deployment.

IaC requires three things:

- Infrastructure code written in a language such as YAML, JSON, or HCL.
- A place to store and monitor this code, such as a Git repository.
- A way to run the code to deploy, maintain, and upgrade infrastructure, such as GitOps.

What GitOps addresses:

Advanced	• Security Scans • Ongoing compliance and configuration drift • Updates
Second order	• Who deployed infrastructure and what was deployed
First order	• Deploy infrastructure (IaC)



flywheel DATA

Flywheel Data DevSecOps Technology

The Flywheel Data reference architecture addresses all the requirements for a DevSecOps software factory using IaC. Flywheel has selected the following technologies to establish a secure DevSecOps reference architecture.

GitLab Ultimate is an essential tool for the development of secure applications. Its automation of CI/CD pipelines, collaborative development capabilities, and advanced security features such as 2-factor authentication, LDAP/AD group synchronization and audit logging, enables teams to create and deploy secure applications with confidence.

Terraform simplifies building, changing, and managing infrastructure in a secure repeatable way by allowing infrastructure resources to be defined declaratively in code, provisioned, and managed efficiently

Ansible is a powerful IT automation tool that can configure systems, deploy software, and orchestrate advanced IT tasks such as continuous deployments or zero downtime rolling updates.

Nutanix offers virtualization, data services, and fully integrated Kubernetes management, providing a secure infrastructure foundation that simplifies on-premises deployments of the reference architecture.

- Nutanix Cloud Platform provides simple, powerful hyperconverged infrastructure (HCI) and enables use of the same tools no matter where you operate—on-premises, in the cloud, or at the tactical edge—simplifying management.
- Nutanix Kubernetes Engine (NKE) simplifies Kubernetes lifecycle management so you can deliver and manage Kubernetes with push-button simplicity.
- Nutanix Unified Storage (NUS) provides a single platform for block, file, and object storage services, addressing the storage needs of diverse applications without added complexity or expense.

Getting Started with DevSecOps

The Flywheel Data DevSecOps reference architecture is the fastest and easiest path to increase the security of software development while accelerating delivery. If you are ready to jumpstart your software development efforts, Flywheel Data can help you stand up a DevSecOps solution and have you operational and compliant in the shortest time possible.

Contact Flywheel Data about a customized DevSecOps workshop to gain hands on familiarity.

DevSecOps customer references are available upon request.

About Flywheel Data

Flywheel Data provides elite solution design, system integration, software development, and product resale for data-driven-organizations.

Based on our experiences with the US Government and top commercial companies; Flywheel Data recognizes that data and people are at the center of a successful, data-driven organization.

Our goal is to arm our clients with the right tools, platforms, and culture to accelerate data-driven insights.

If you'd like to learn more about our DevSecOps reference architecture, you can contact Flywheel Data by phone or email.

1818 Library St. Suite 500
Reston, VA 20190
Phone: (703) 647-4137
Email: info@flywheeldata.com

www.flywheeldata.com