VOLANT ASSOCIATES

Case Study B

ENTERPRISE SCALE DEVSECOPS FOR DOD ISR

Since 2017 Volant has worked with the Department of Defense to build, deploy and sustain a robust collaboration environment and cloud-hosted software development tools (DevTools) on the unclassified network (35k+ users and 4k+ projects) and the Secret Internet Protocol Router Network (SIPRNet) network.

Over the past several years, recurring technical tasks involving backup, recovery, deployment and upgrades to the delivered solution been automated by leveraging the APIs and native capabilities of the cloud platforms to increase efficiency and reliability. The successful delivery of these automation features to the DI2E Framework combined with our experience supporting the automation and streamlining of security accreditation processes has enabled Volant to become a key government partner in helping to shape the vision for the emerging Enterprise Scale DevSecOps for DoD ISR initiative.

The Challenge

The environment currently supports much of the tooling and automation necessary for DoD and IC system developers to leverage iterative DevOps software methods in which development and deployment to operations are treated as a continuous process. For example, many development teams using long-standing DI2E Framework provided capabilities (e.g., Jenkins, Nexus) have been successful with continuous delivery of improved functionality based on direct interaction and feedback from end users.

However, based on lessons learned derived from work done on securing the government software supply chain, the government has determined that the existing solution needs to support a full DevSecOps environment. This reflects the importance of integrating security directly into the DevOps cycle rather than "bolting security on" at the end of the deployment process.

The key challenge is to ensure security is included at all stages of the software development and deployment process via an established and maintained DevSecOps toolchain. Once this DevSecOps toolchain is deployed to our environment, the streamlining and automation of the end-to-end Risk Management Framework (RMF) based accreditation process can be realized thereby reducing the time to verify individual security controls and shortening the overall time to deploy secure software in support of the mission.

> **"The DoD should embrace DevSecOps (not just DevOps) and provide policy supported processes, certified libraries, tools, and a toolchain reference implementation to produce "born secure" software."**
>
> *Defense Innovation Board*
> *Federal Advisory Committee*

This reflects the importance of integrating security directly into the DevOps cycle rather than 'bolting security on' at the end of the deployment process.

Our Approach

Volant's approach is to enhance and extend the existing deployed Orchestrated DevOps Pipeline (Figure A) by introducing OpenControl based capabilities built to streamline the security accreditation process.

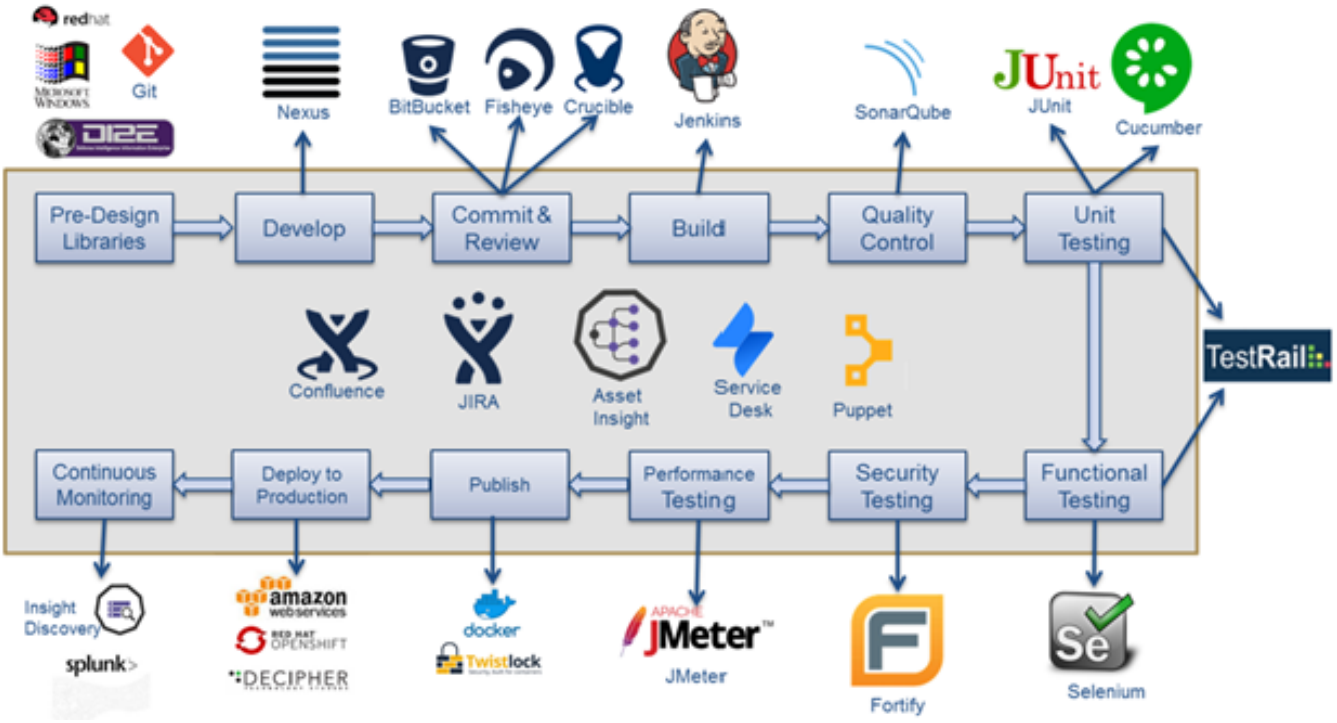

Figure A. - Orchestrated DevOps Pipeline

OpenControl combines technical work done by the government (18f.gsa.gov) and commercial vendors (Docker, Redhat, etc.) to integrate the RMF security cycle with DevOps to arrive at an integrated DevSecOps toolchain. Based on the Volant team's direct experience, OpenControl has been selected to be a core component of the overall DevSecOps toolchain based on several key attributes:

- Technology neutral
- Application testing matched to the technology
- Serves the Developer and the Accreditor
- Works with existing human and DevOps processes

OpenControl also helps unify stakeholder participation throughout the entire DevSecOps toolchain (Figure B). It creates opportunity for continuous collaboration and provides a means to implement, track, and monitor security related controls throughout the entire DevOps process.

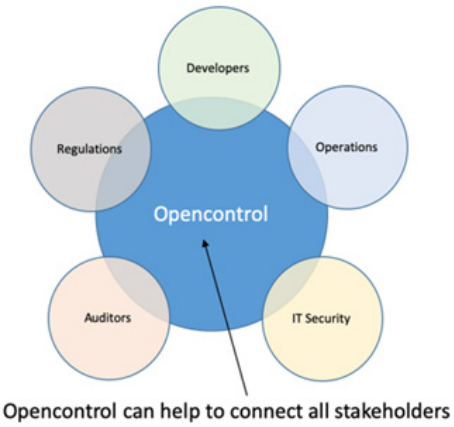

Figure B. – OpenControl enables more effective stakeholder participation

DevSecOps Supports Continuous Accreditation

The DevSecOps toolchain enables the government to ensure software undergoes continuous accreditation by providing key security artifacts and processes. These artifacts and processes include reliably building certification documentation, automating the System Security Plan (SSP) process by modeling security controls and creating a set of security control scripts that are run as part of the software build/test/deployment process. Compliance masonry is also a part of the DevSecOps toolchain which provides a command-line interface (CLI) allowing users to construct certification documentation using Opencontrol structure/schemas.

Continuous Accreditation occurs across three phases of software development and operations:

- Security before development (based on system concept)
    - Encompasses RMF, system design phase and pipeline setup
- Security after development (but before operations)
    - Verification performed in pipeline, gatekeeper for moving to operations
- Security after deployment into operations
    - Alignment of continuous verification tools (ACAS, EVSS, HBSS) with ATO governance

Benefits of the DevSecOps Toolchain

Deployment of a DevSecOps toolchain provides a number of benefits to the DoD ISR enterprise:

- Creates a shared incentive for close collaboration between software development organizations and cyber/RMF inspection organizations
- Maximizes the number of inheritable RMF controls by utilizing shared environments and platforms
- Makes control evaluation as objective as possible encouraging test-driven development against meaningful IT constraints
- Maximizes the opportunity to use common tools across programs
- Maximizes the use of containers and Platform as a Service (PaaS) capabilities enabling immediate deployment of mission application containers

In summary, Volant has extensive experience automating key aspects of the DevTools environment as well as successfully leveraging the Opencontrol open source standards to streamline and automate the government accreditation and authorization processes. This combination of experience and technical know-how enables Volant to function as a thought leader in the emerging DevSecOps domain space. Volant is pleased to be a trusted partner in helping the government define where it needs to be regarding DevSecOps technologies and processes.

For more information contact us at **(571) 210-0030** or **info@volantco.com**