WHITEPAPER

DevSecOps Drives Reliable and Secure Software

> **"DevSecOps represents a refinement of DevOps, highlighting the security aspect. It breaks down barriers by providing an operations and security conscious software development paradigm that fuses development, operations, and security into a streamlined process."**

BACKGROUND

Software delivery in the Federal Government is transforming at the fastest pace since the advent of the Internet. With increasingly tight budgets and growing cybersecurity threats, the government must be able to deliver more with less—and do it more securely. However, many software development projects are plagued by fragmented teams that separate development, operations and maintenance, and security teams into silos. This results in numerous adverse effects that may include untimely delivery, defective code, and vulnerable code.

Traditional waterfall methodologies feature a serial chain of phase gates that must be completed in a specific order. Requirements, design, development, and testing are executed as a chain of events, with documentation driving readiness reviews between each phase. In most cases, security scans are executed when software is promoted to production, with vulnerabilities potentially forcing rework and threats to a network.

With DevOps, developers create continuous delivery pipelines enabling them to build, deploy, and test software with every check-in. Code is unit tested, regression tested, deployed, and validated with each build. Highly customized deployment scripts give way to defining infrastructure as code, which massively accelerates application deployment from days to minutes. DevOps reduces technical debt due to deployment throughout development.

DevSecOps represents a refinement of DevOps, highlighting the security aspect. It breaks down barriers by providing an operations and security

conscious software development paradigm that fuses development, operations, and security into a streamlined process. DevSecOps incorporates all aspects of security into every facet of development and deployment. Information assurance and cybersecurity activities are integrated into the agile development process, ensuring steady progression against certification and accreditation requirements.

DevSecOps provides an integrated approach unifying teams, technologies, and processes for faster, more robust, and secure products.

DEVSECOPS EVOLVED: DEVSECOPS CENTER OF EXCELLENCE AND EGT LABS®

eGlobalTech (eGT) established eGT Labs as a forward-leaning research and development environment to solve challenging client problems and to create high-value products and services. eGT Labs, in turn, launched the DevSecOps Center of Excellence to develop best practices and technical guidance on successful DevSecOps deployment. The DevSecOps CoE defined the following best practices as critical to deployment:

- **Establish the Culture –** DevSecOps is not a singular process, nor is it a single lifecycle. It is an innovative approach to system engineering that focuses on teamwork, integration of cross-cutting concerns, and success through frequent repetition.
- **Coaching Is Key –** Coaches should be heavily engaged during early adoption to help transform managers, engineers, and even contracting staff to fully understand DevSecOps and effectively interact with it.
- **Security-First Design –** Security should be applied not only to the code, but also to the processes involved in coding. This provides an accelerant from project initiation that helps streamline deployment and delivery.
- **Automation –** DevSecOps performed the eGT way features automation at all levels, including code generation, deployment, testing, and security testing to maximizing the impact of DevSecOps.
- **Build Often/Deploy Often/Test Often –** One of the key aspects of DevSecOps features daily builds and deployments with testing in every build. Products built with DevSecOps are better tested and more secure than products built without it.
- **DevSecOps Friendly Acquisition –** DevSecOps thrives when teams are fully integrated and encouraged to collaborate. Enhancing acquisition strategies that favor integration of cross-functional teams is essential to reducing costs and developing better products.

WHITEPAPER

GT Labs developed a framework which enables rapid delivery of secure solutions of superior quality by incorporating security and operations readiness from day one. Our leading, end-to-end framework and toolkit, DevOps Factory®, includes the following critical elements:

✓ Implements security-first design and development.
✓ Automates security governance and controls consistent with Ongoing Authorization (OA).
✓ Secures the continuous delivery/continuous delivery pipeline through authentication, secure storage of build artifacts, key management, etc.
✓ Automates security testing, static code analysis, configuration management, incident response and forensics, secure backups, log monitoring, and continuous monitoring and mitigation.
✓ Incorporates compliance with FISMA, NIST, and other applicable federal standards and guidelines.

DevSecOps Applied

A public sector eGT client had a complex geospatial system prototype composed of Microsoft and open source applications with a growing number of ArcGIS services. This prototype was used in a production capacity and encountered frequent outages and performance issues.

To solve this issue, we applied DevOps Factory® to re-engineer the target architecture, implement security-first design, and automate the end-to-end cloud migration process onto our managed AWS infrastructure.

Results included:
✓ Migrated and operationalized a secure geospatial cloud ecosystem to AWS within three months, compliant with federal security standards.
✓ Securely on-boarded over a dozen complex applications and systems.
✓ Seamlessly supported 400+% growth of geospatial services.
✓ Achieved 99.99% operational availability.

CONTACT US AT:

Info@eglobaltech.com if you would like more information on this topic!