Strongbridge Cloud Practice

Cloud-based DevSecOps

DevSecOps is an evolution in the development of software that emphasizes open communication and more effective collaboration across teams and functions in an organization that focuses on creating and operating software capabilities.

CMMI LEVEL 3

ISO 9001 20000 27001

amazon web services | Partner Network

Microsoft Partner

DevSecOps is an evolving style of application development that strives to seamlessly combine several contemporary development trends, aiming to shorten the time in which new application capabilities are available to customers. A DevSecOps approach is supported by three essential features: 1) the application of Agile development builds, 2) a greater use of automation, and 3) enhanced cooperation and interaction across development, security, quality assurance, and operations groups in an organization.

Agile Development Cycles

With our DevSecOps approaches, the application release cycles are short and often, and follow the spirit of an Agile project. In contrast, a traditional waterfall approach might many months until a release is published. Strongbridge staff are experts with several schools of Agile development which can serve as the cornerstone of a contemporary DevSecOps approach. DevSecOps projects tend to have a greater number of smaller releases and the need for a higher degree of automation for these releases to maintain schedule efficiency.

Applying Greater Degrees of Automation

To be in the spirit of a DevSecOps culture, the organization applies more automation tools that aid in the moving of "Agily"-coded builds, through the testing process and into a cloud production ecosystem. Given the current state of the market, DevSecOps projects usually do not rely on a one single tool, but instead, are supported by many tools, scripts and processes that tie the development and operations processes together, end-to-end. As the market matures, we can expect greater integration of tools across the entire development, control verification, QA, and operations processes.

Cross-team Participation

In a DevSecOps culture, software developers, security experts, QA staff, and operations staff work together, across traditional team boundaries. (This does not mean they literally have to have the same manager, but rather that there are some agreed, structured communications that support the formation of a virtual team or a matrixed team to get the end-to-end job done.)

Strongbridge LLC is an innovative and certified Small Business providing Agile software development and systems engineering services, with specializations in the application of cloud computing services and highly automated DevSecOps processes.

Success Stories

Department of Transportation Volpe Center

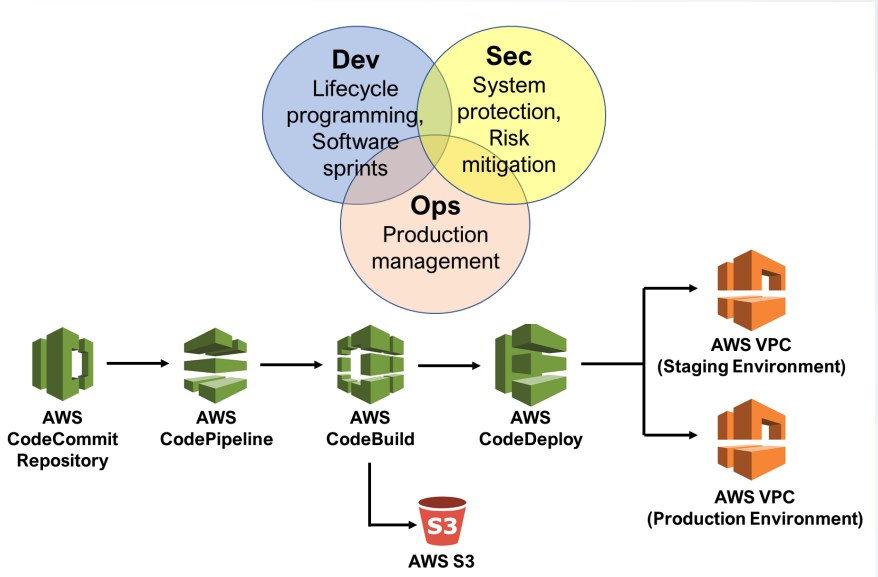
Strongbridge staff are supporting the migration of key National Highway Traffic Safety Administration's (NHTSA's) capabilities, databases and systems for storing safety defect data to the cloud using DevSecOps processes. For the Artemis project we are supporting the Volpe Center with business analysis, and cloud native development, where we are redesigning and building essential functions to run natively in a commercial cloud. AWS GovCloud is the target cloud ecosystem for the migration and we use a full DevSecOps toolset to automate the Agile software development lifecycle process, from code check-out and check-in, through several types of suitability, security, and integration testing, to deployment. We provide DevSecOps teams supported by high degrees of automation and cloud-based toolsets to implement Infrastructure As Code and a Continuous Integration / Continuous Delivery (CI/CD) capability.

The Strongbridge Cloud Practice continues to be a leading voice in the application of cloud computing solutions to Federal applications.

Strongbridge LLC

21355 Ridgetop Circle
Suite 200
Sterling, VA 20166

Phone: 571-257-2370
E-mail: info@SB-LLC.com



Considerations for Cloud-based DevSecOps

As shown in the AWS-based example above, when we apply DevSecOps team concepts in a contemporary cloud development environment, several topics and new opportunities deserve further consideration:

- **Infrastructure As Code** - Market leading cloud ecosystems offer infrastructure resources that are programmable via API, allowing them to be provisioned through code as opposed to browser interfaces. The advantage to capturing the infrastructure resources and their configuration as code is that what was once a tedious and error prone process can now be configuration controlled and saved as a repeatable deployment event.
- **Continuous Integration** - Current toolsets, that exist natively in leading clouds, allow a distributed team to frequently check-in code changes and integrate them into the sprint baseline, helping to identify coding defects quickly, lowering integration failures and increasing deployment frequency.
- **Cloud-based Performance Monitoring** - The cloud provides a DevSecOps team with a strong suite of production operations monitoring tools. Robust performance monitoring is often a combination of application component monitoring combined with measuring the end user experience.

How Does Strongbridge Help?

As part of our primary goal to provide technical leadership in the identification, development, and application of software best practices/technologies for Federal customer's software projects, Strongbridge stands ready to provide our lessons learned, and expertise for cloud native development using DevSecOps approaches, with advantages such as:

- **Commercial Partnerships** with leading cloud providers such as Amazon Web Services (AWS), and Microsoft Azure.
- **Corporate and Staff Certifications**–Strongbridge staff maintain the Agile, CMMI development and cloud vendor certifications to remain the experts in cloud native development. We can give you expert options in the cloud.
- **Federal Past Performance** - We understand government security requirements in approved clouds and we apply DevSecOps processes to deploy secure applications.