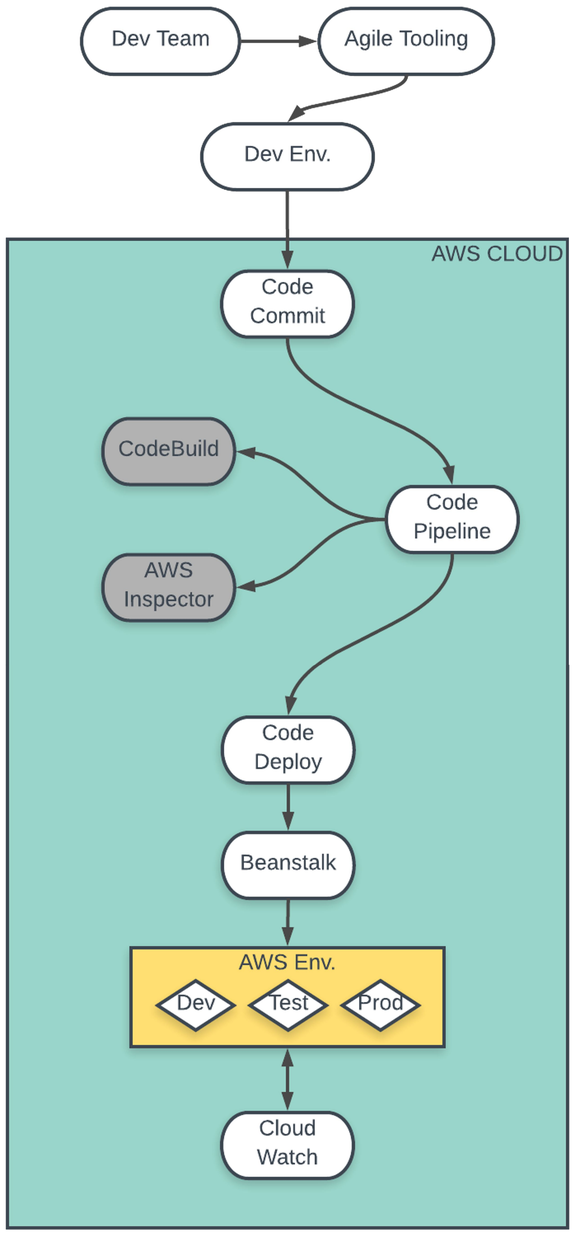
DevSecOps AWS Pipeline

Kalynn Tarpenning, Jeromy Coburn, Taka Nakamura, Matthew Warner, Samantha Caneer, Collin Goss for SAIC



Pipeline Tool Breakdown

- Development Team

The programmers and teams writing the code for the application.

- Agile Tooling

The tools a team uses for project management, documentation, and collaboration.

- Development Environment

The machine local tools the dev teams use to program. This includes IDEs, unit tests, code format tests, and data management.

- AWS Cloud

The overall container for the majority of the toolchain from code uploading to deployment.

- Code Commit

Source control service that hosts secure Git-based repositories.

- Code Pipeline

Continuous delivery service that helps automate release pipelines for application and infrastructure updates.

- Code Build

Compiles source code, runs tests, and produces software packages that are ready to deploy.

- AWS Inspector

Automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

- Code Deploy

Deployment service that automates software deployments to a variety of compute services.

- Elastic Beanstalk

Automatic capacity provisioning, load balancing, auto-scaling to application health monitoring.

- AWS Environment

Holds the following environments:

  - *Development*
    Code is uploaded and prepared here then passed to test
  - *Test*
    Code is run through defined tests and passed to production
  - *Production*
    Code is packaged and sent to necessary locations to be deployed

- Cloud Watch

CloudWatch provides you with data and actionable insights to monitor your applications, understand and respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health.

Elevator Statement

For Developers and Project Managers at SAIC who need a framework or template of a DevSecOps pipeline/toolchain. The SAIC DevSecOps Pipeline is a guide that explains how to develop, automate and use a DevSecOps pipeline. Unlike other DevSecOps guides, our product is a set of resources that defines and explains the tools and process often used for DevSecOps.

Features of the Project

- This pipeline is developed using AWS services, which provides easy integration and guaranteed upkeep.
- Functional DevSecOps pipeline where code will visually travel through AWS environments.
- Videos detailing how to build and implement your own pipeline similar to this one
- An online portal where code can be submitted to the pipeline, reports are posted, and videos can be viewed.

What is DevSecOps?

Until recently, the software development process was covered by two different groups:

- Developers (Programmers)
- Operations (Systems Engineers, Administrators, Operations, and Release Engineers)

A methodology evolved from agile, DevOps, breaks down the wall that separates the development and operations sides of the software lifecycle. This helps speed the development process by reducing the amount of external team communication and dependence while increasing throughput of the operations side. This higher throughput gives the development teams rapid feedback, allowing them to respond with updated code faster and more frequently.

The inclusion of security in DevSecOps adds a focus of keeping code secure throughout the development process. It changes the mindset from secure code after development to secure code during development which encourages developers to program with security already in mind.

This also includes securing the development process itself to make sure no third parties can interfere.

Mockup