AWG CI/CD Pipeline

Current Status and Future Development

March 9, 2021

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

Current Status

We have **two** pipelines serving two different purposes. Adding new functionality to our Github pipeline will create some duplication/overlap of what happens in the AWS pipeline.

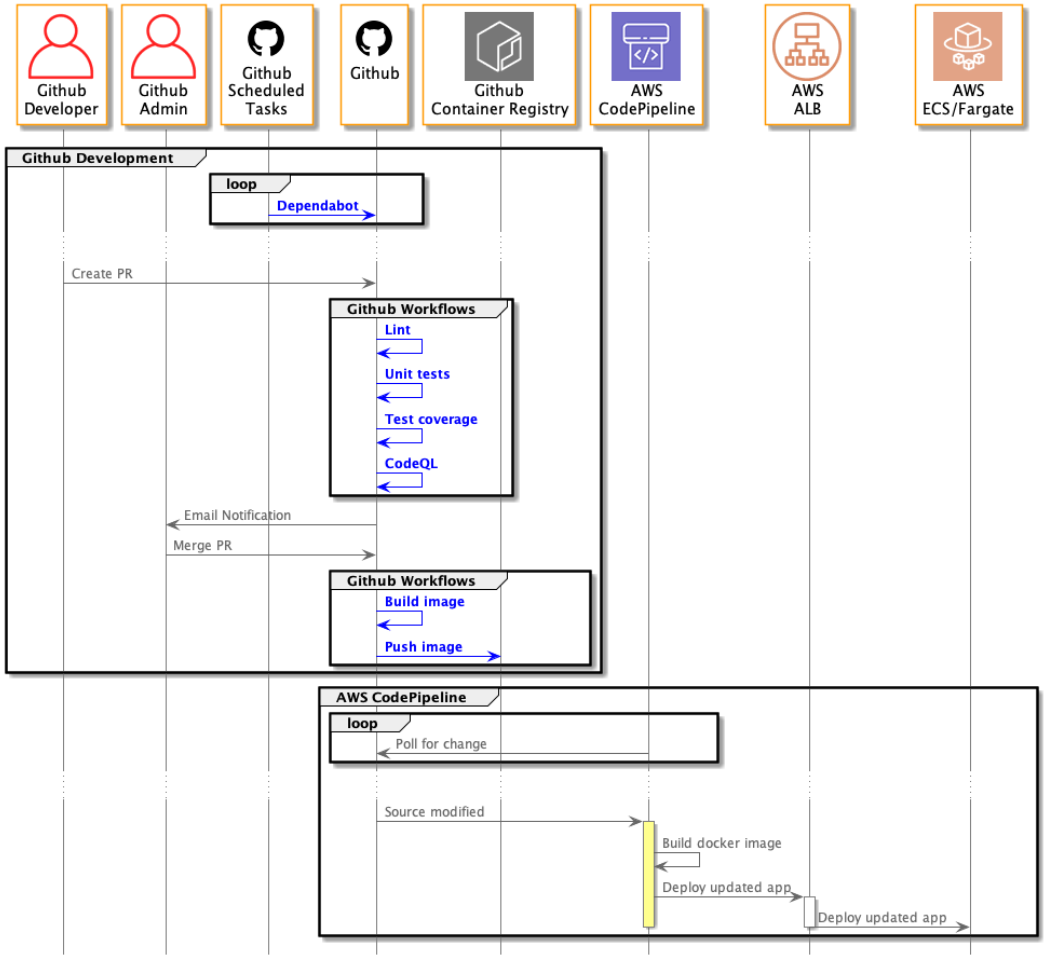
The **Github pipeline supports the development process** (CI) and provides the AWG community access and transparency. **Community members can contribute to the pipeline**.

- Implemented with Github workflows
- Viewable by any Github user, who can contribute changes via pull requests
- Currently implemented workflows: unit tests, CodeQL code analysis, test coverage report, code linting, docker image build

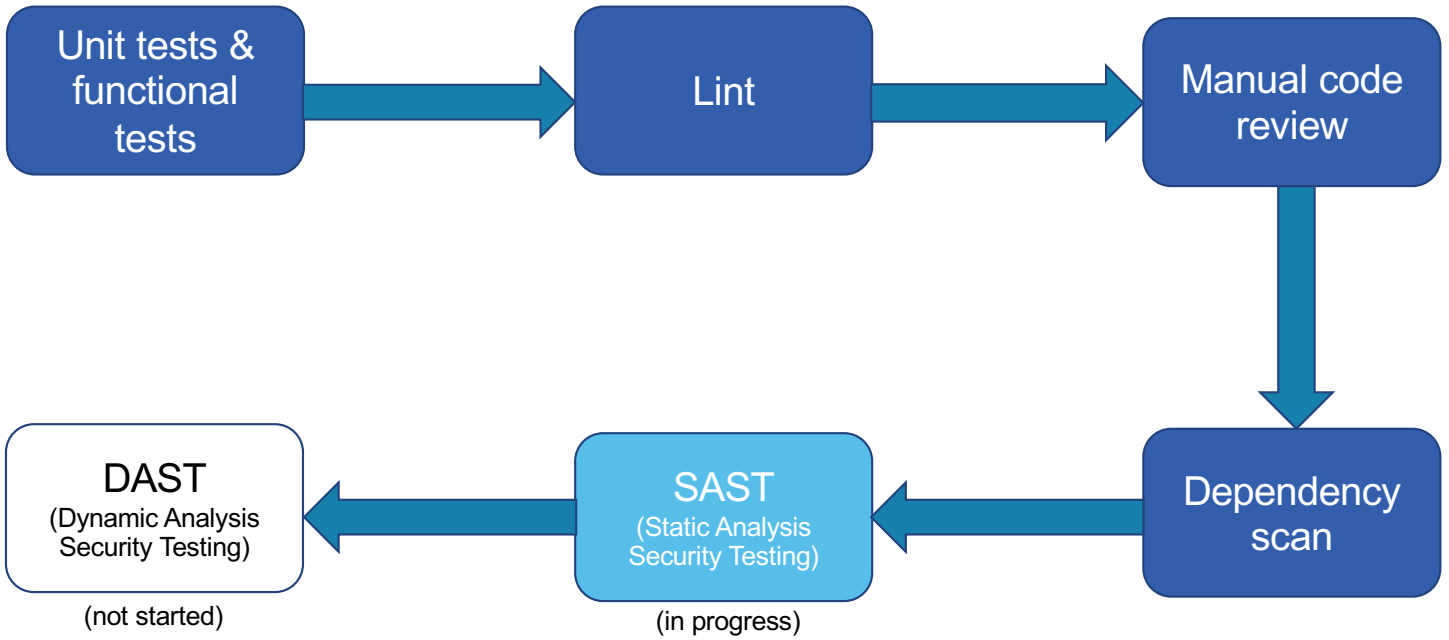
The **AWS pipeline supports the deployment process** (CD) for DEV, INT, PRD.

- Implemented using AWS CodePipeline.
- Restricted to only a handful MITRE staff with no community transparency (MITRE policy).
- There is no AWS source code repository. All AWG source code is pulled in from Github.
- There are 3 distinct pipelines (DEV, INT, PRD) created using CloudFormation (infrastructure as code). These 3 pipelines support 3 distinct deployment targets.
- We are exploring providing an additional instance to enable development access to the community.

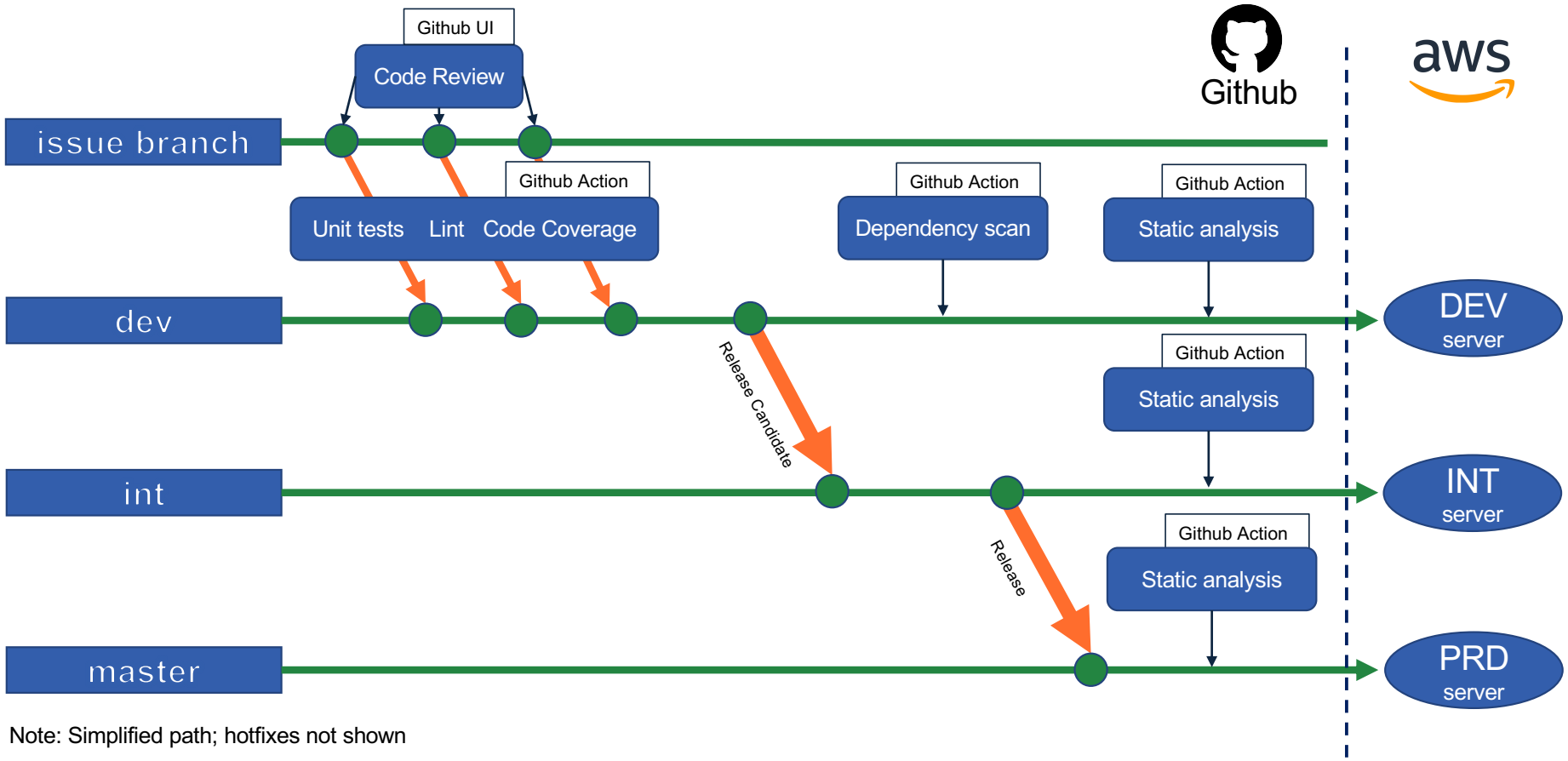
CI/CD Pipeline Sequence Diagram



AWG Code Quality and Security



Source Code Change Propagation



Note: Simplified path; hotfixes not shown

Code Quality and Security

	Status	Tools
Automated unit tests	Complete	Custom code
Automated functional tests	In progress	Custom code
Lint	Complete	ESLint
Code coverage	Complete	NPM
Manual code review	Complete	Github PR process
Dependency scan	Complete	Github Dependabot
SAST (Static analysis security testing)	In progress	CodeQL, SonarQube, DevSkim, SonarCloud
DAST (Dynamic analysis security testing)	Not started	OWASP ZAP

Colors: Currently in use, exploring use

2021 Objectives

- Improve transparency for AWG community
  - Allow community to contribute to pipeline
- Improve our software development process
  - Improve code quality (catch issues early) with additional automated tests
  - Improve unit test coverage
  - Improve software delivery process
  - Mature static analysis action
  - Add dynamic analysis action
- Leverage new services provided by Github (Github Container Registry)
- Support new CVE website's pipeline