


# SECURE FLOW

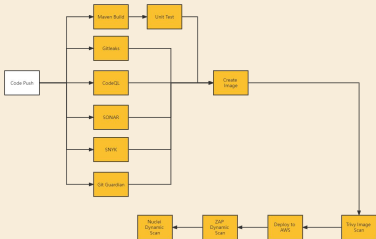
DevSecOps Pipeline with GitHub Actions



# GitHub Action Review


- Continuous integration / continuous delivery (CI/CD)
  - Any language
  - Matrix builds
  - Linux, macOS, Windows, ARM, and containers
- 

# Secure Flow






# Sonar

- A cloud-based code analysis service designed to detect code quality issues
  - Static analysis
  - Detect:
    - Bad Code Smells
    - Bugs
    - Vulnerabilities
  - GitHub Action Integration and Other platforms
- 



# Amazon ECR


Elastic Container Registry

- An AWS managed container image registry service
  - Image scanning
  - Cross-region and cross-account
- 




# Amazon ECS

Elastic Container Service

- AWS Fargate
  - Integration with Access Management (IAM).
  - Support for service discovery.
- 



# Git Guardian

- Detect more than 200 types of secrets
  - As well as other potential security vulnerabilities & policy breaks
  - Uses public API to scan issues in code
  - Fails if there are secret leaks
- 

# Git Guardian


- Acquire api token from server
- Choose methods to store the result

```
GitGuardian:
name: Secret Scan using GitGuardian
runs-on: ubuntu-latest
steps:
  - name: Checkout
    uses: actions/checkout@v2
    with:
      fetch-depth: 0 # fetch all history so multiple commits can be scanned
  - name: GitGuardian scan
    uses: GitGuardian/ggshield-action@master
    with:
      args: -v --all-policies
    env:
      GITHUB_PUSH_BEFORE_SHA: ${ github.event.before }
      GITHUB_PUSH_BASE_SHA: ${ github.event.base }
      GITHUB_PULL_BASE_SHA: ${ github.event.pull_request.base.sha }
      GITHUB_DEFAULT_BRANCH: ${ github.event.repository.default_branch }
      GITGUARDIAN_API_KEY: ${ secrets.GITGUARDIAN_API_KEY }
```






# Nuclei




- Fast and customizable vulnerability scanner
  - Templates are updated regularly and automatically
  - It is capable of scanning various protocols: DNS, HTTP and etc.
- 



# Nuclei

- Assign templates for the scanner
  - Method to reserve the result
  - Url of the scan target
- 


# Nuclei

- ☐  **Tomcat Detection (tomcat-detect)** found on <http://ecsloadbalancer-1600554619.us-west-2.elb.amazonaws.com/jpetstore> Low master  
#66 opened 1 hour ago • Detected by nuclei in :1
- ☐  **WAF Detection (waf-detect)** found on <http://ecsloadbalancer-1600554619.us-west-2.elb.amazonaws.com/jpetstore> Low master  
#65 opened 1 hour ago • Detected by nuclei in :1
- ☐  **HTTP Missing Security Headers (http-missing-security-headers)** found on <http://ecsloadbalancer-1600554619.us-west-2.elb.amazonaws.com/jpetstore> Low master  
#62 opened last week • Detected by nuclei in :1

- Failing from preventing unencrypted connections
- Tech-detection




# Gitleaks

- A fast, light-weight, portable, and open-source secret scanner for git repositories, files, and directories.
  - Static analysis tool
  - Detect:
    - passwords
    - api keys
    - tokens
- 




## Results of Gitleaks

- if detected leaks
  - if no leaks detected
- 




# Trivy

- Trivy (tri pronounced like trigger, vy pronounced like envy) is a simple and open-source container image scanner.
  - Static analysis tool
  - Target: docker image
  - Well integrated with GitHub
- 



# Documentation for open source project

- README.md
  - SECURITY.md
  - CONTRIBUTE.MD
- 



**THANKS!**

