CSA | Bangalore Chapter

Meetup - Oct 2024

In affiliation with

7 ELEVEN GLOBAL SOLUTION CENTER

Application Security

..the key to modernization

7 ELEVEN GLOBAL SOLUTION CENTER BHARTIYA CITY BANGALORE

26 OCTOBER 2024
09:00 AM - 4:30 PM

CSA | Bangalore Chapter

Meetup - Oct 2024

In affiliation with

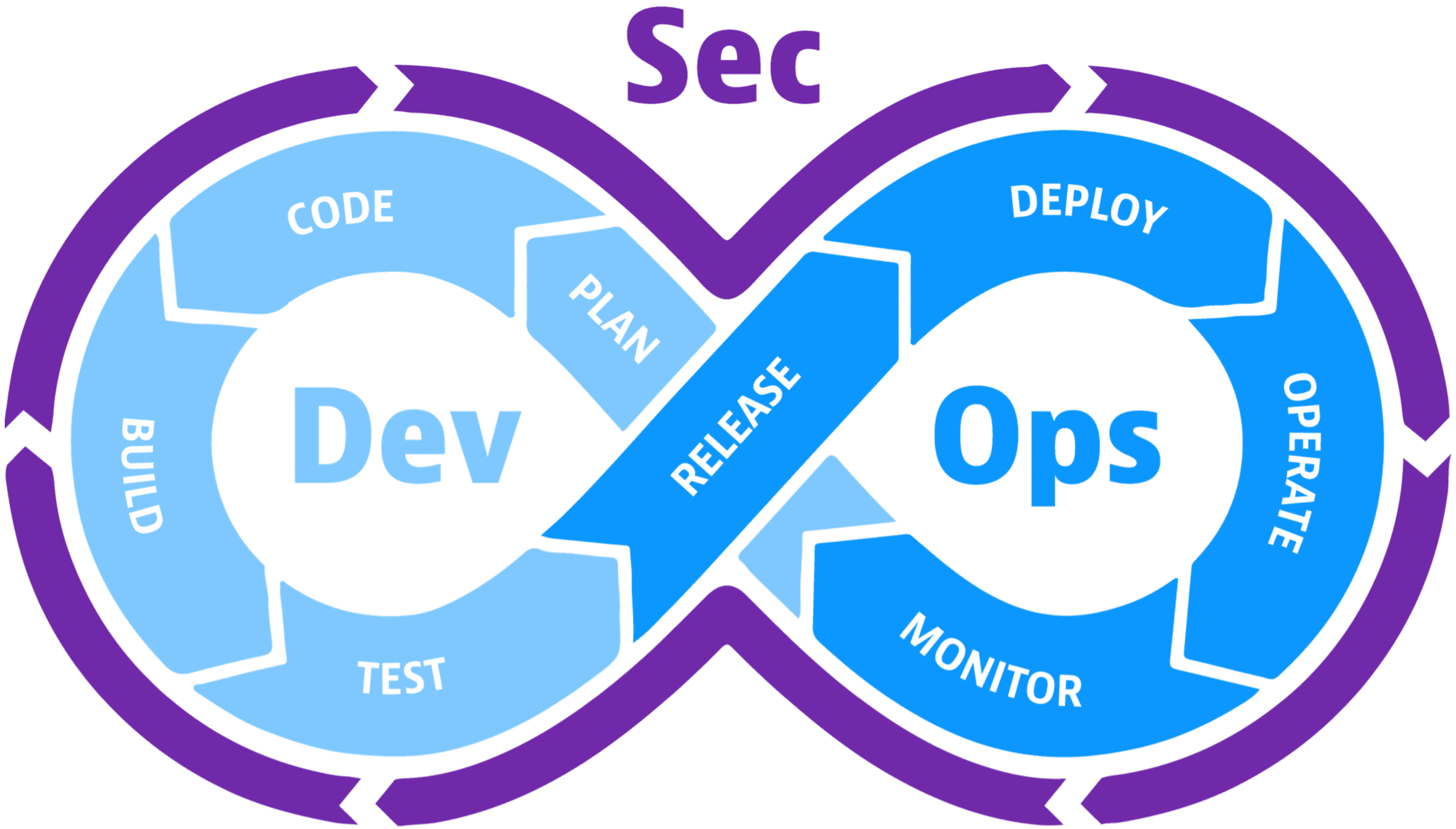
7 ELEVEN GLOBAL SOLUTION CENTER

AWS DevSecOps Integration

Anjali Shukla

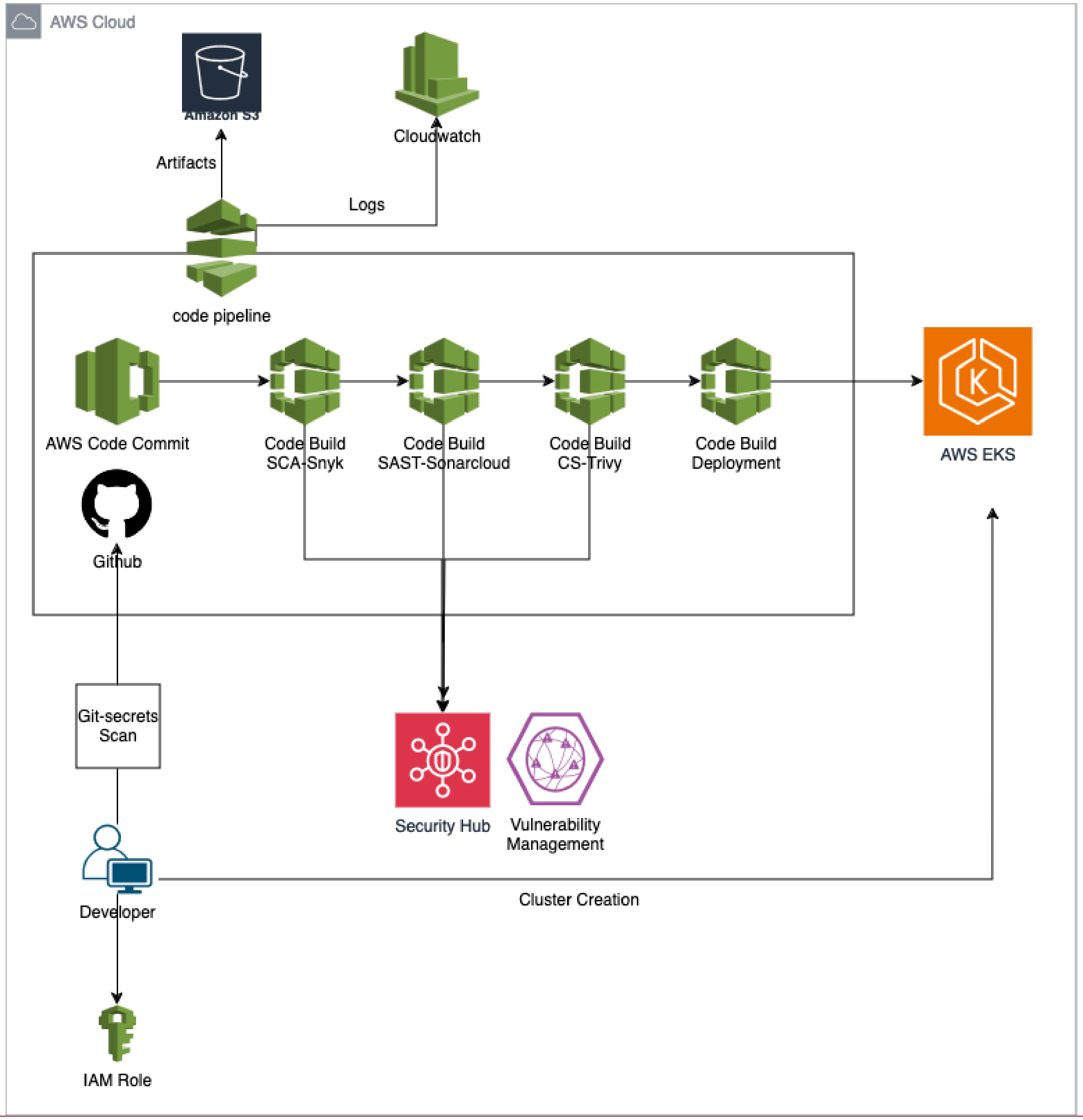
Senior Security Engineer

What is DevSecOps?



Ref: https://www.dynatrace.com/news/blog/what-is-devsecops/

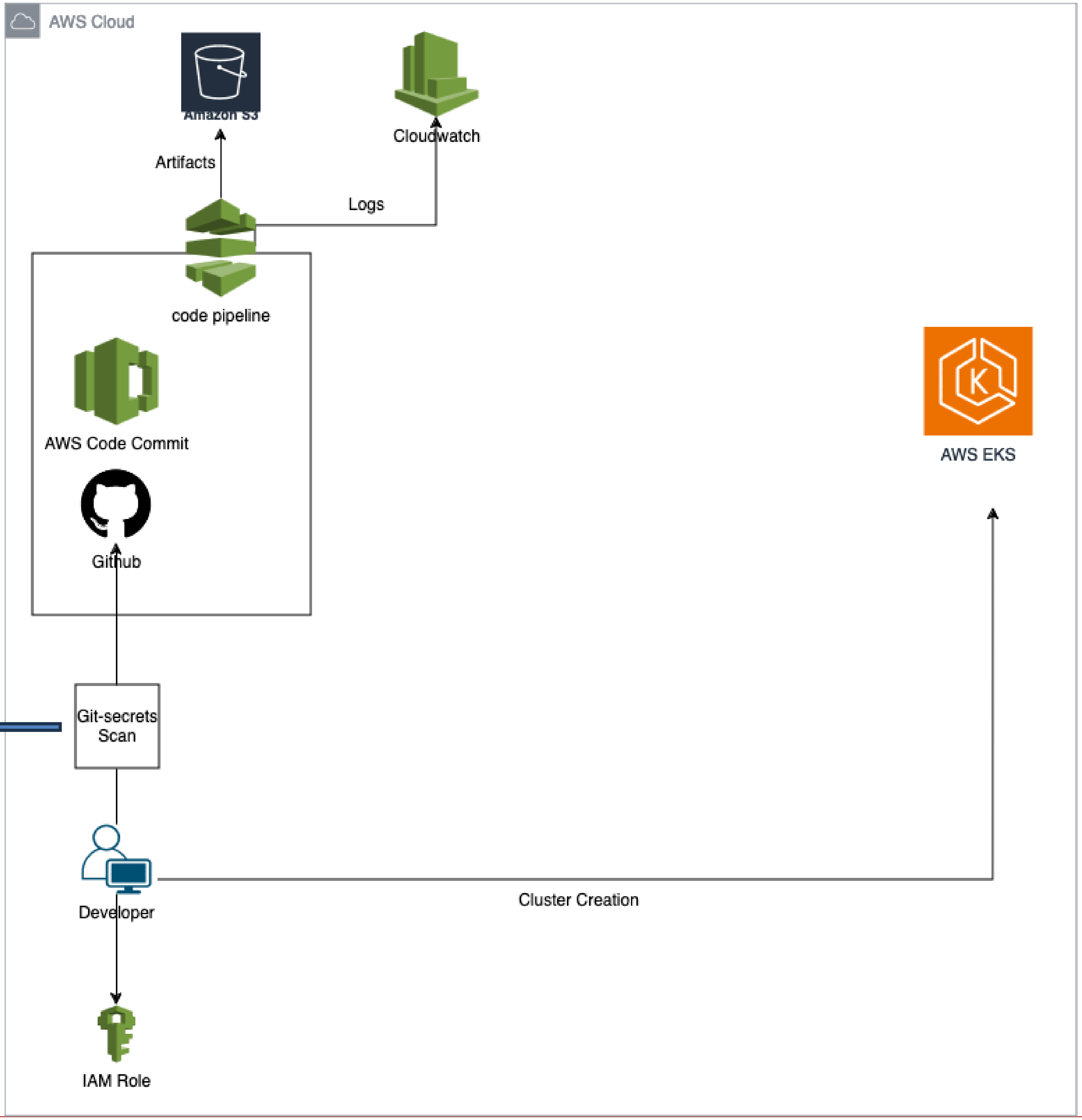
DevSecOps Integration: Architecture



Secret Scanning: IDE

GitGuardian snyk TRUFFLEHOG

git-secret

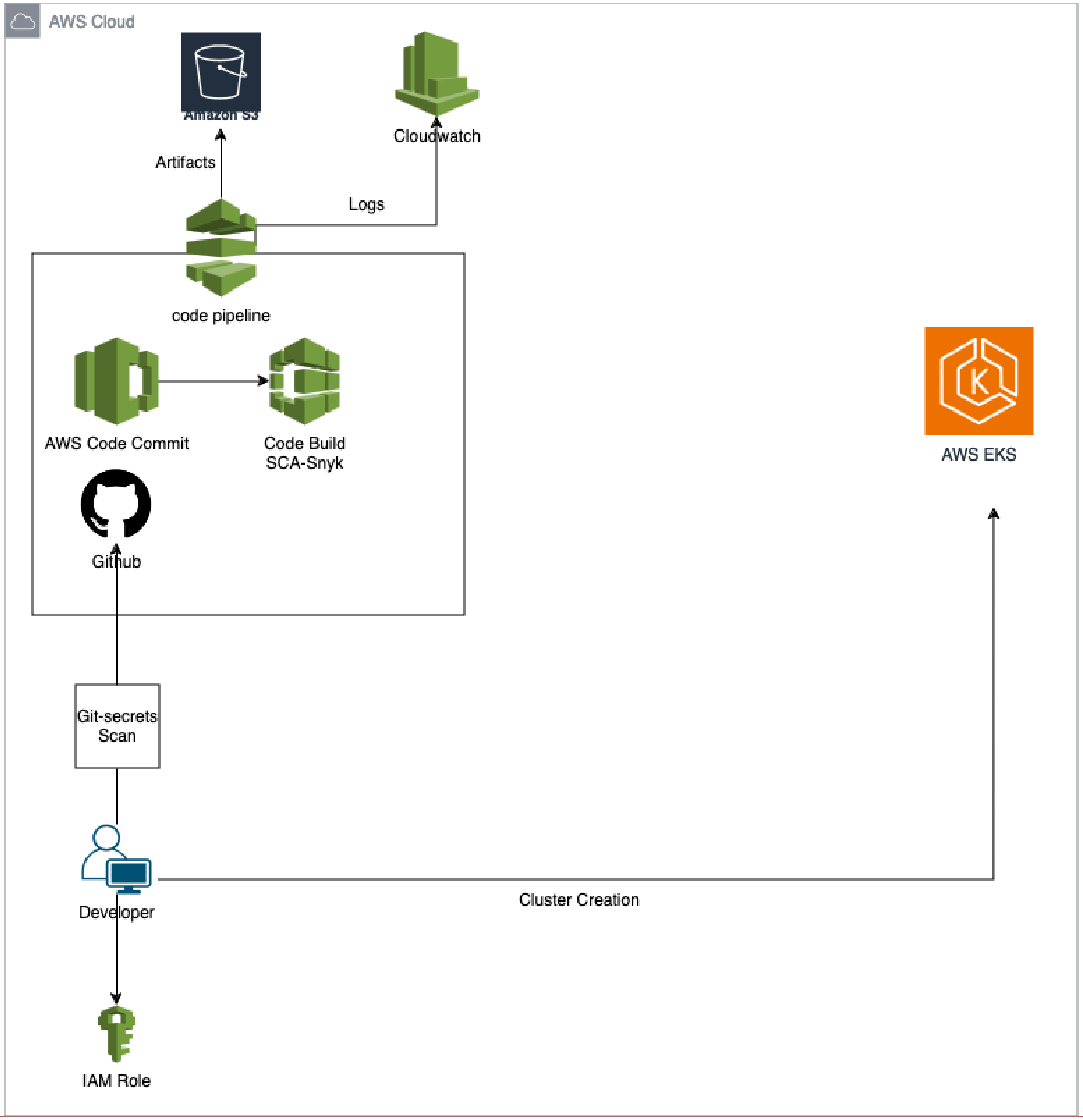


SCA Scanning: Code Build

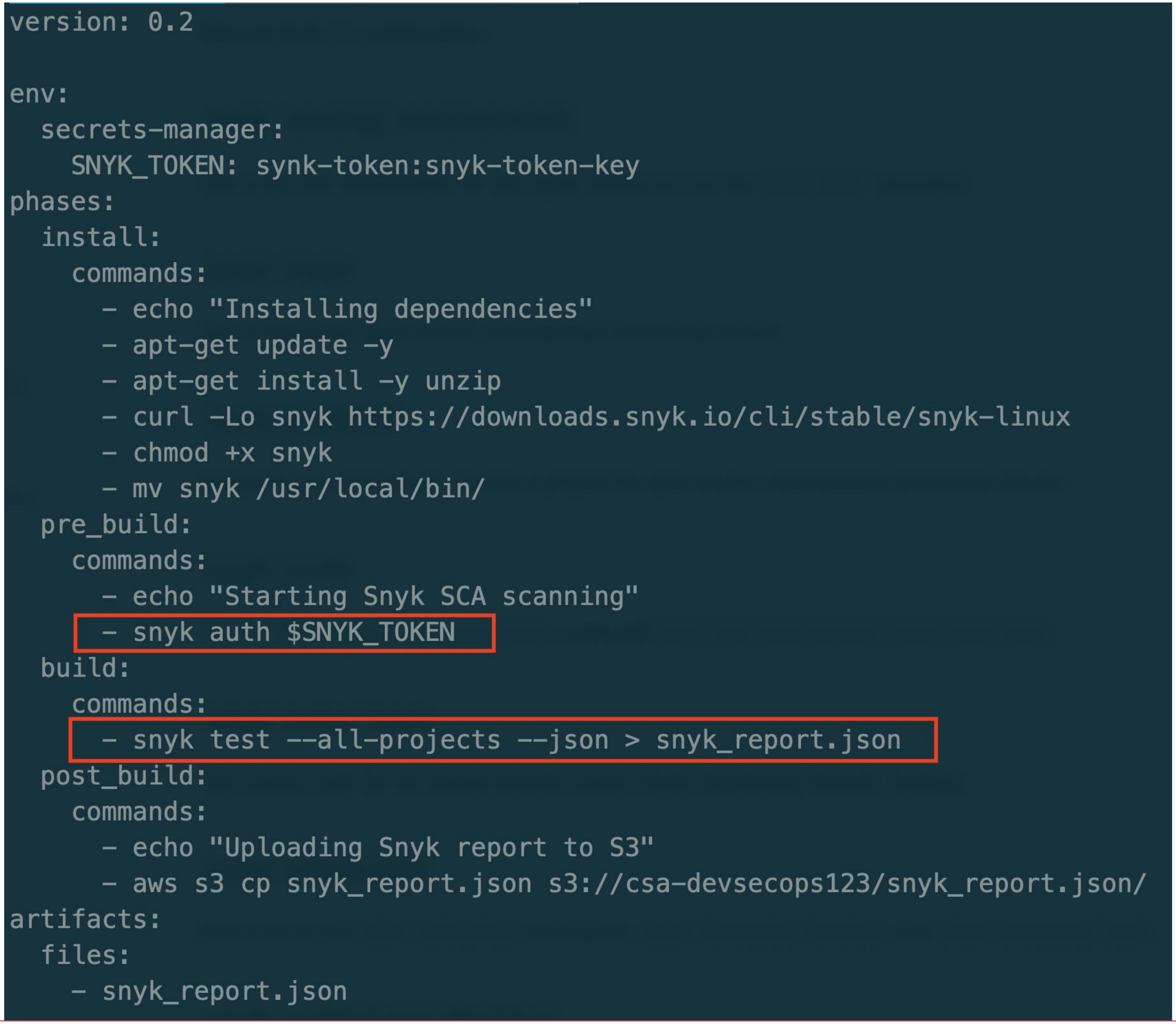
snyk

WhiteSource is now MEND

DEPENDENCY-CHECK



SCA Scanning: Code Build Snyk



```
version: 0.2

env:
  secrets-manager:
    SNYK_TOKEN: synk-token:snyk-token-key
phases:
  install:
    commands:
      - echo "Installing dependencies"
      - apt-get update -y
      - apt-get install -y unzip
      - curl -Lo snyk https://downloads.snyk.io/cli/stable/snyk-linux
      - chmod +x snyk
      - mv snyk /usr/local/bin/
  pre_build:
    commands:
      - echo "Starting Snyk SCA scanning"
      - snyk auth $SNYK_TOKEN
  build:
    commands:
      - snyk test --all-projects --json > snyk_report.json
  post_build:
    commands:
      - echo "Uploading Snyk report to S3"
      - aws s3 cp snyk_report.json s3://csa-devsecops123/snyk_report.json/
artifacts:
  files:
    - snyk_report.json
```

SAST Scanning: Code Build

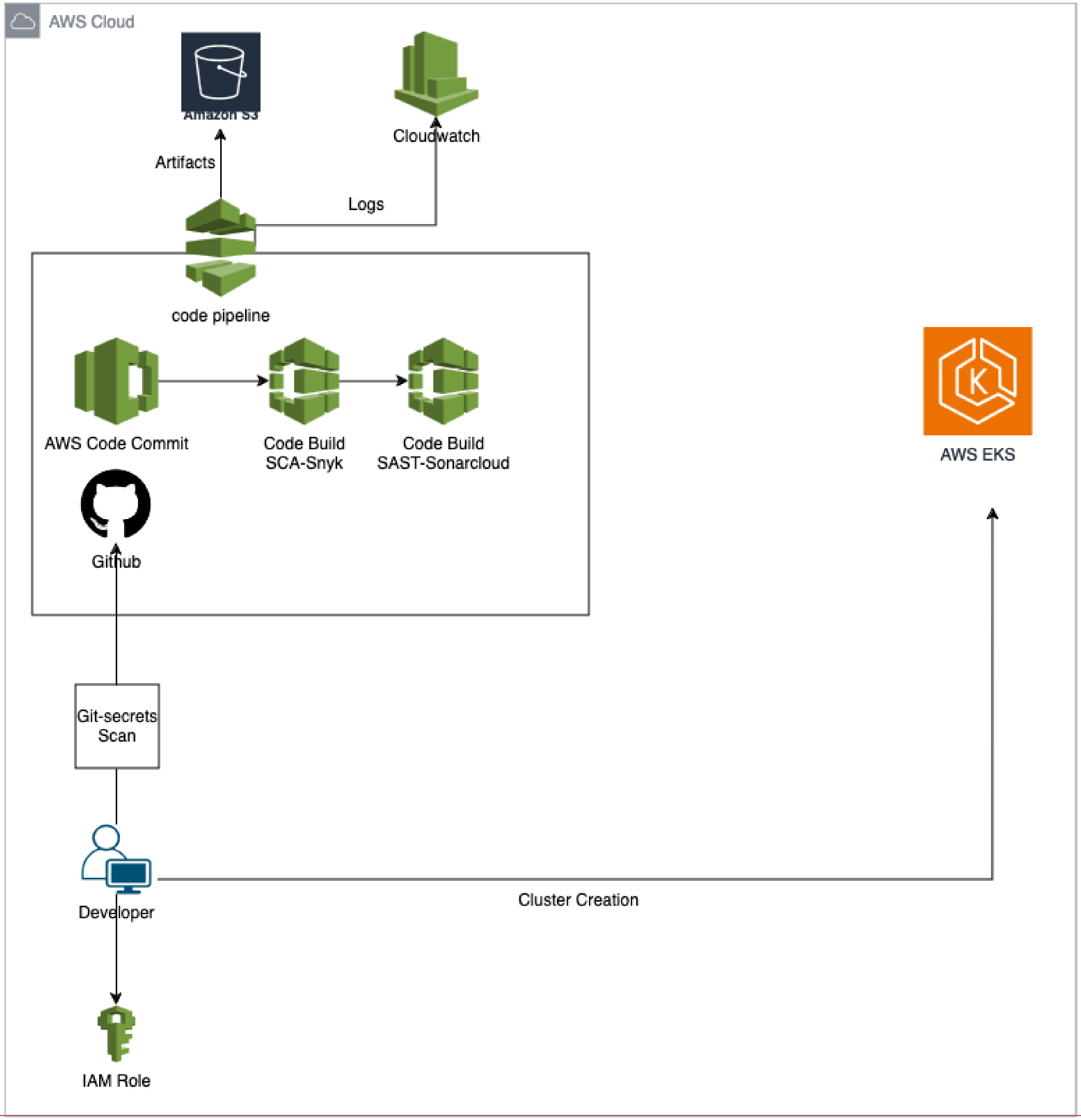
snyk

WhiteSource is now MEND

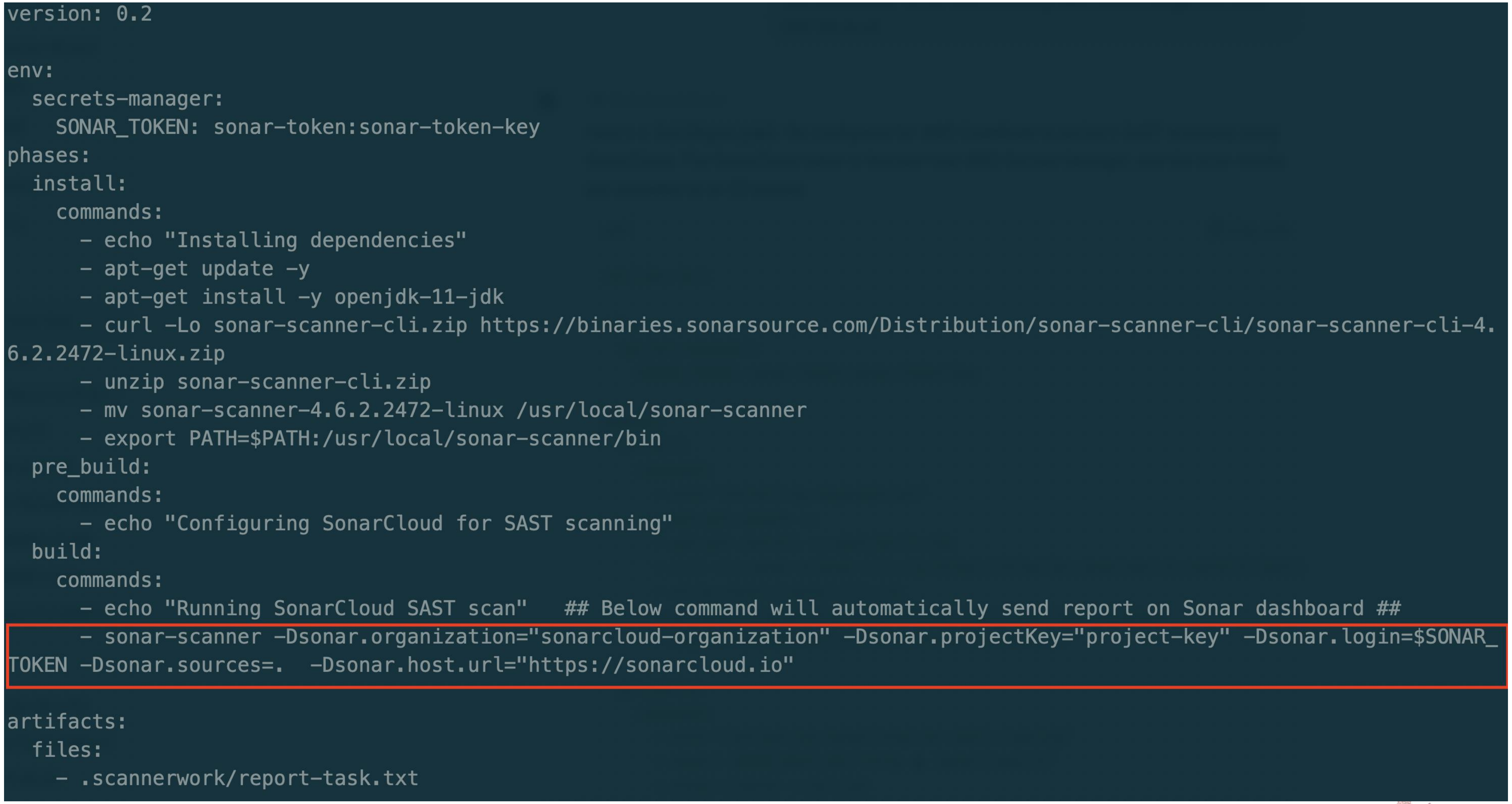
sonarcloud

Checkmarx

VERACODE



SAST Scanning: Code Build Sonarcloud



```
version: 0.2

env:
  secrets-manager:
    SONAR_TOKEN: sonar-token:sonar-token-key
phases:
  install:
    commands:
      - echo "Installing dependencies"
      - apt-get update -y
      - apt-get install -y openjdk-11-jdk
      - curl -Lo sonar-scanner-cli.zip https://binaries.sonarsource.com/Distribution/sonar-scanner-cli/sonar-scanner-cli-4.
6.2.2472-linux.zip
      - unzip sonar-scanner-cli.zip
      - mv sonar-scanner-4.6.2.2472-linux /usr/local/sonar-scanner
      - export PATH=$PATH:/usr/local/sonar-scanner/bin
  pre_build:
    commands:
      - echo "Configuring SonarCloud for SAST scanning"
  build:
    commands:
      - echo "Running SonarCloud SAST scan"   ## Below command will automatically send report on Sonar dashboard ##
      - sonar-scanner -Dsonar.organization="sonarcloud-organization" -Dsonar.projectKey="project-key" -Dsonar.login=$SONAR_
TOKEN -Dsonar.sources=.  -Dsonar.host.url="https://sonarcloud.io"

artifacts:
  files:
    - .scannerwork/report-task.txt
```

Image Scanning: Code Build

snyk

aqua trivy

anchore

clair

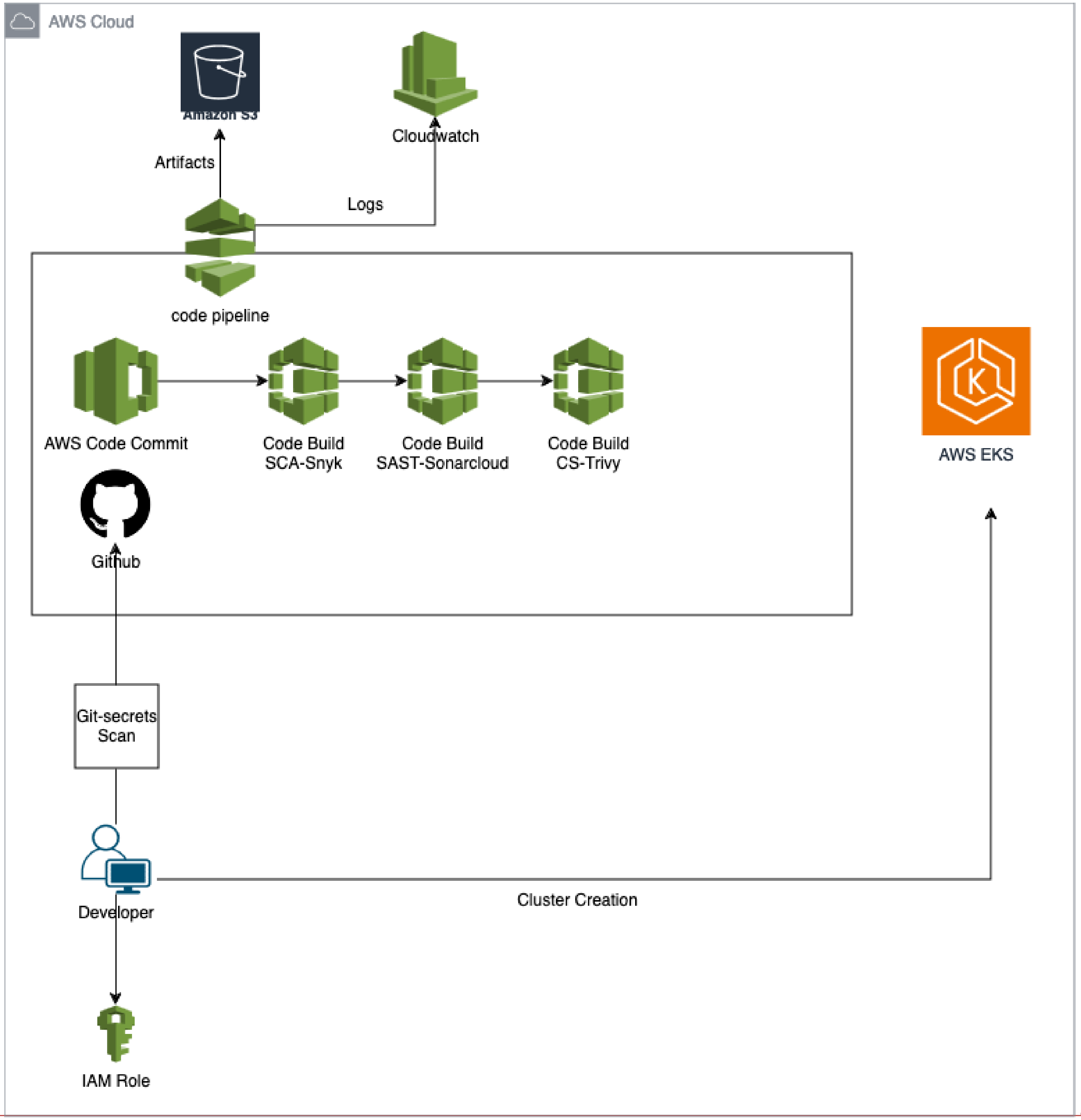
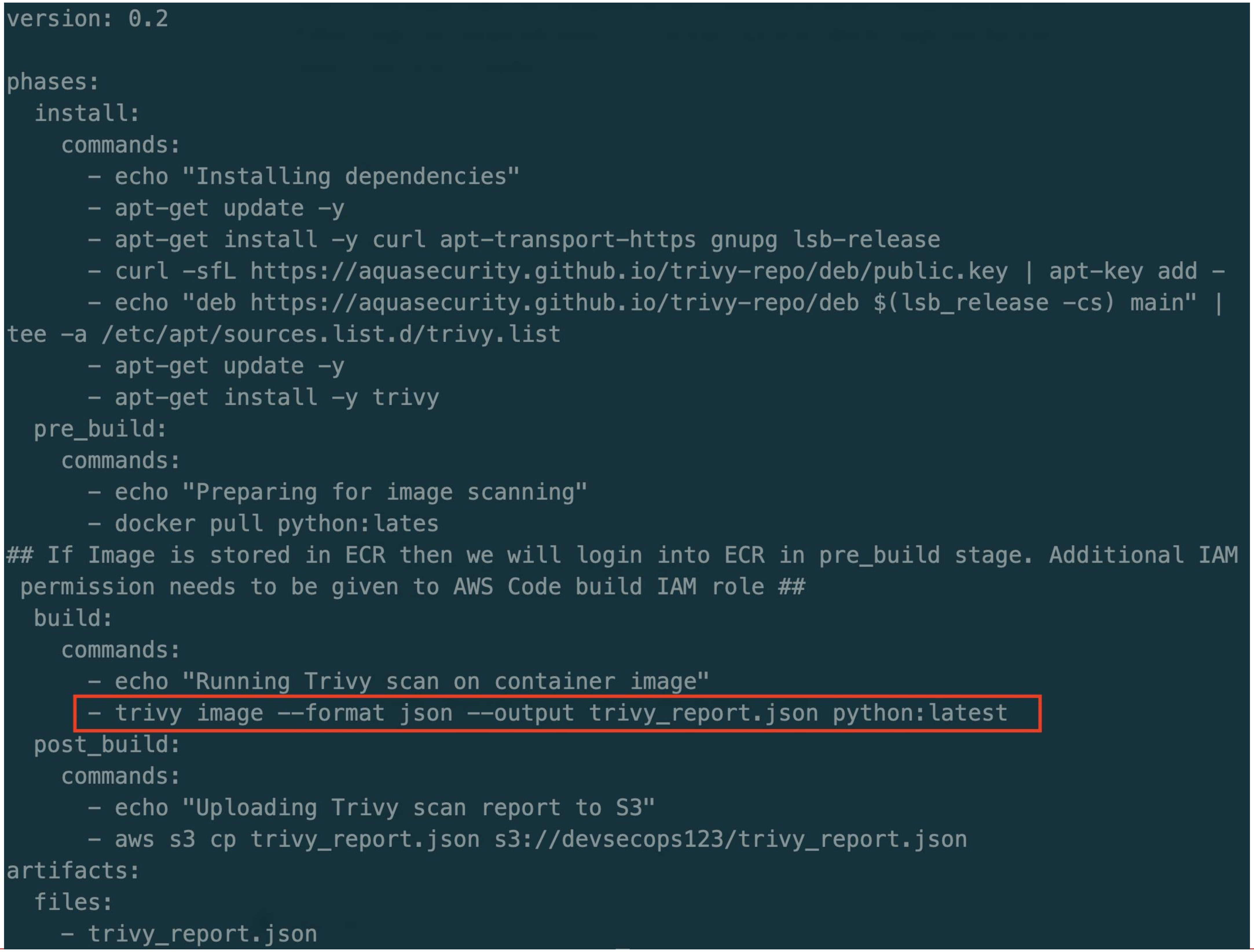


Image Scanning:
Code Build
Trivy

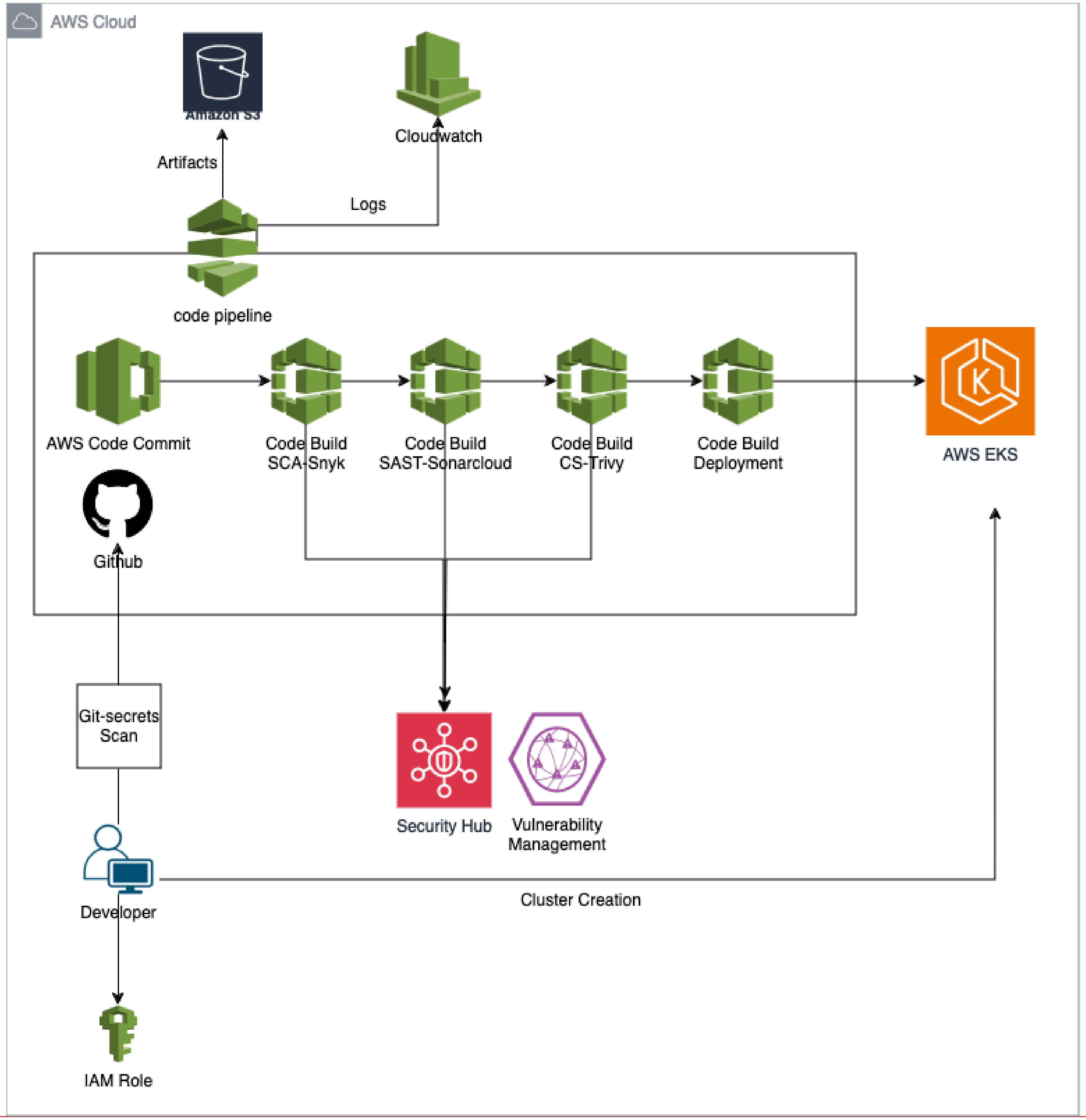


```
version: 0.2

phases:
  install:
    commands:
      - echo "Installing dependencies"
      - apt-get update -y
      - apt-get install -y curl apt-transport-https gnupg lsb-release
      - curl -sfL https://aquasecurity.github.io/trivy-repo/deb/public.key | apt-key add -
      - echo "deb https://aquasecurity.github.io/trivy-repo/deb $(lsb_release -cs) main" |
tee -a /etc/apt/sources.list.d/trivy.list
      - apt-get update -y
      - apt-get install -y trivy
  pre_build:
    commands:
      - echo "Preparing for image scanning"
      - docker pull python:lates
## If Image is stored in ECR then we will login into ECR in pre_build stage. Additional IAM
 permission needs to be given to AWS Code build IAM role ##
  build:
    commands:
      - echo "Running Trivy scan on container image"
      - trivy image --format json --output trivy_report.json python:latest
  post_build:
    commands:
      - echo "Uploading Trivy scan report to S3"
      - aws s3 cp trivy_report.json s3://devsecops123/trivy_report.json
artifacts:
  files:
    - trivy_report.json
```

Vulnerability Management:

- AWS native service Security HUB can be used.
- Snyk & Sonarcloud provides gui.
- ArcherySec & Defectdojo



Challenges So Far…

- We are installing all security tools in buildspec.yaml on fly, wouldn’t it consume time ?
- Should we add all scanning stages in single buildspec.yaml file ?
- Can I integrate findings with Security Hub directly ?
- Can we integrate it with JIRA ?
- Which one is better integration in IDE or VCS repositories ?

READY FOR A
QUIZ?

Q 1: Which of the following tools is specifically used for SCA (Software Composition Analysis) in an AWS CI/CD pipeline?

A. SonarCloud
B. Veracode
C. Snyk
D. Security Hub

Q 2: What role does AWS Security Hub play in a CI/CD pipeline?

A. Provides code quality analysis
B. Aggregates security alerts and compliance checks across AWS services
C. Scans for vulnerabilities in open-source libraries
D. Performs dynamic application security testing (DAST)

Q 3: What is the main purpose of AWS CodeBuild in a CI/CD pipeline?

A. Deploying applications to EC2 instances

B. Running automated tests & building source code

C. To store artifacts

D. Creating and managing infrastructure as code

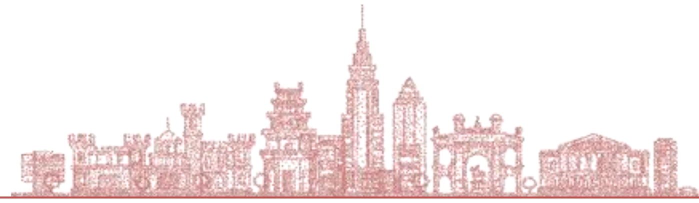
Q 4: Which of the following is NOT a phase that can be defined in a CodeBuild buildspec.yaml file?

A. Install

B. pre_build

C. Deploy

D. post_build



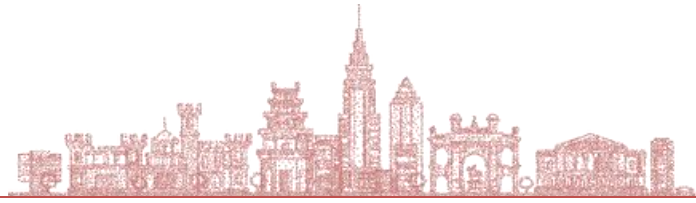
ANSWERS

Q 1: Which of the following tools is specifically used for SCA (Software Composition Analysis) in an AWS CI/CD pipeline?

A. SonarCloud
B. Veracode
C. Snyk
D. Security Hub

Q 2: What role does AWS Security Hub play in a CI/CD pipeline?

A. Provides code quality analysis
B. Aggregates security alerts and compliance checks across AWS services
C. Scans for vulnerabilities in open-source libraries
D. Performs dynamic application security testing (DAST)



Q 3: What is the main purpose of AWS CodeBuild in a CI/CD pipeline?

A. Deploying applications to EC2 instances
B. Running automated tests & building source code
C. To store artifacts
D. Creating and managing infrastructure as code

Q 4: Which of the following is NOT a phase that can be defined in a CodeBuild buildspec.yaml file?

A. Install

B. pre_build

C. Deploy

D. post_build

Questions ??