```
# This workflow uses actions that are not certified by GitHub.
# They are provided by a third-party and are governed by
# separate terms of service, privacy policy, and support
# documentation.

name: trivy

on:
  push:
    branches: [ "master" ]
  pull_request:
    # The branches below must be a subset of the branches above
    branches: [ "master" ]
  schedule:
    - cron: '31 0 * * 5'

permissions:
  contents: read

jobs:
  build:
    permissions:
      contents: read # for actions/checkout to fetch code
      security-events: write # for github/codeql-action/upload-sarif to upload SARIF results
       actions: read # only required for a private repository by github/codeql-action/upload-sarif to get
the Action run status
```

```
name: Build

runs-on: "ubuntu-20.04"

steps:

  - name: Checkout code

    uses: actions/checkout@v4


  - name: Build an image from Dockerfile

    run: |

      docker build -t docker.io/my-organization/my-app:${{ github.sha }} .


  - name: Run Trivy vulnerability scanner

    uses: aquasecurity/trivy-action@18f2510ee396bbf400402947b394f2dd8c87dbb0

    with:

      image-ref: 'docker.io/my-organization/my-app:${{ github.sha }}'

      format: 'template'

      template: '@/contrib/sarif.tpl'

      output: 'trivy-results.sarif'

      severity: 'CRITICAL,HIGH'


  - name: Upload Trivy scan results to GitHub Security tab

    uses: github/codeql-action/upload-sarif@v3

    with:

      sarif_file: 'trivy-results.sarif'
```