```yaml
# 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.

# This workflow file requires a free account on Semgrep.dev to
# manage rules, file ignores, notifications, and more.
#
# See https://semgrep.dev/docs

name: Semgrep

on:
  push:
    branches: [ "master" ]
  pull_request:
    # The branches below must be a subset of the branches above
    branches: [ "master" ]
  schedule:
    - cron: '19 7 * * 3'

permissions:
  contents: read

jobs:
  semgrep:
    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: Scan
    runs-on: ubuntu-latest
    steps:
      # Checkout project source
      - uses: actions/checkout@v4

      # Scan code using project's configuration on https://semgrep.dev/manage
      - uses: returntocorp/semgrep-action@713efdd345f3035192eaa63f56867b88e63e4e5d
        with:
          publishToken: ${{ secrets.SEMGREP_APP_TOKEN }}
          publishDeployment: ${{ secrets.SEMGREP_DEPLOYMENT_ID }}
          generateSarif: "1"

      # Upload SARIF file generated in previous step
      - name: Upload SARIF file
        uses: github/codeql-action/upload-sarif@v3
        with:
          sarif_file: semgrep.sarif
        if: always()
```