```yaml
---
name: Codacy

on:
  push:
    branches: ["master"]
  pull_request:
    branches: ["master"]
  schedule:
    - cron: "0 0 * * "

permissions:
  contents: read

jobs:
  codacy-security-scan:
    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: Codacy Security Scan
    runs-on: ubuntu-latest
    steps:
      - name: Checkout code
        uses: actions/checkout@v4
      # Execute Codacy Analysis CLI and generate a SARIF output with the security issues identified
```

```yaml
        during the analysis

      - name: Run Codacy Analysis CLI

        uses: codacy/codacy-analysis-cli-action@97bf5df3c09e75f5bcd72695998f96ebd701846e

        with:

          # Check https://github.com/codacy/codacy-analysis-cli#project-token to

          # get your project token from your Codacy repository

          # You can also omit the token and run the tools that support default configurations

          project-token: ${{ secrets.CODACY_PROJECT_TOKEN }}

          verbose: true

          output: results.sarif

          format: sarif

          # Adjust severity of non-security issues

          gh-code-scanning-compat: true

          # Force 0 exit code to allow SARIF file generation

          # This will handover control about PR rejection to the GitHub side

          max-allowed-issues: 2147483647

    # Upload the SARIF file generated in the previous step

    - name: Upload SARIF results file

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

      with:

        sarif_file: results.sarif
```