Checkov

Descripción

Checkov es un escáner de infraestructura como código (IaC) que detecta configuraciones inseguras en Terraform, CloudFormation, Kubernetes, etc.

Uso local

```
checkov -d .    # Escanea el directorio actual
```

Reportes

- CLI, JSON, JUnit, SARIF.
- Puede integrarse con plataformas como Prisma Cloud o DefectDojo.

Integración en CI/CD

- Esta acción de GitHub ejecuta Checkov en infraestructura como código, paquetes de código abierto, imágenes de contenedores y configuraciones de CI/CD para identificar configuraciones incorrectas, vulnerabilidades y problemas de cumplimiento de licencias.

```
    - name: Run Checkov action
      id: checkov
      uses: bridgecrewio/checkov-action@master
      with:
        directory: .
        soft_fail: true
        download_external_modules: true
        github_pat: ${{ secrets.GH_PAT }}
      env:
        GITHUB_OVERRIDE_URL: true  # optional: this can be used to instruct the action to override the global GIT config to inject the PAT to the URL
```

Integraciones

- GitHub, Jira (API), Slack.

- VSCode: extensión oficial para resaltar problemas en tiempo real.

UI

- Checkov OSS no tiene UI propia, pero Prisma Cloud (versión paga) sí.

Licencia

- **Open source (Apache 2.0)**.
- Instalación simple en máquinas virtuales.

Facilidad de uso

- Muy fácil. CLI sencilla y reglas predefinidas muy completas.

Cumplimiento con estándares:

- **OWASP:** Apoya indirectamente la mitigación de riesgos del OWASP Top 10 para aplicaciones cloud-native.
- **NIST:** Compatible con controles de NIST 800-53 (por ejemplo, CM-6: configuración, SC-12: seguridad criptográfica).
- **ISO/IEC 27001:** Apoya la seguridad en configuración de infraestructura (controles A.12.1.2 y A.14.1.3).
- **CIS Benchmarks:** Checkov valida configuraciones directamente contra benchmarks CIS para AWS, Azure, GCP, Kubernetes.

Revisión #10
Creado 16 julio 2025 17:41:41
Actualizado 16 julio 2025 22:37:18