Semgrep

Descripción

Semgrep es un escáner de análisis estático que detecta vulnerabilidades, errores de seguridad, problemas de estilo, etc., mediante reglas personalizables.

Uso local

```
# Escaneo básico
semgrep scan --config=p/ci .

# Escaneo con reglas personalizadas
semgrep scan --config=rules/mi_regla.yml .
```

Reportes

- JSON, JUnit, SARIF.
- Integración con GitHub Security tab.

Integración en CI/CD

- Semgrep Action ejecuta Semgrep en entornos de CI. También puede conectarse a la aplicación Semgrep para configurar reglas y revisar hallazgos en una interfaz web.

```
- uses: returntocorp/semgrep-action@v1
```

Integraciones

- GitHub, Jira (con integración pagada o scripts).
- Slack, Teams, Plane.
- VSCode: extensión oficial para ejecutar reglas locales.

UI

- Dashboard web gratuito (requiere cuenta).

Licencia

- Versión gratuita OSS.
- Versión empresarial con dashboard avanzado.

Facilidad de uso

- Fácil. Reglas YAML simples de entender.

Cumplimiento con estándares:

- **OWASP:** Las reglas pueden alinearse al OWASP Top 10, detectando problemas de seguridad en el código fuente.
- **NIST:** Compatible con el marco NIST CSF y NIST 800-53, específicamente en prácticas de desarrollo seguro (SA-11).
- **ISO/IEC 27001:** Apoya controles como A.14.2.5 (control del desarrollo de software) y A.14.2.8 (pruebas técnicas).
- **SOC 2 / PCI DSS:** Puede integrarse en pipelines para cumplimiento de requisitos de seguridad de código seguro.

Revisión #10
Creado 16 julio 2025 17:41:20
Actualizado 16 julio 2025 22:37:28