Snyk

Descripción

Snyk es una herramienta para detectar vulnerabilidades en dependencias, contenedores, código IaC y código fuente.

Uso local

```
snyk test     # Escaneo de dependencias
snyk code test  # Escaneo de código fuente
```

Reportes

- JSON, CLI, UI Web.
- Excelente presentación en su portal online.

Integración en CI/CD

- Un conjunto de acciones de GitHub para usar Snyk y buscar vulnerabilidades en tus proyectos de GitHub. Se requiere una acción diferente según el lenguaje o la herramienta de compilación que uses.

```
      - name: Run Snyk to check for vulnerabilities
        uses: snyk/actions/node@master
        env:
          SNYK_TOKEN: ${{ secrets.SNYK_TOKEN }}
        with:
          command: monitor
```

Integraciones

- GitHub (Security Tab), Jira, Slack, Microsoft Teams.
- VSCode: extensión oficial con análisis en tiempo real.

UI

- UI Web muy amigable.

Licencia

- Versión gratuita limitada (para proyectos públicos o uso individual).
- Planes comerciales.
- Instalación en máquinas virtuales posible.

Facilidad de uso

- Muy fácil. Requiere cuenta en Snyk.

Cumplimiento con estándares:

- **OWASP:** Compatible con el OWASP Top 10 a través de escaneo de código y dependencias vulnerables.
- **NIST:** Alineado con NIST SSDF (Secure Software Development Framework) y NIST 800-53 (RA-5, SI-2).
- **ISO/IEC 27001:** Aporta cumplimiento en controles de gestión de vulnerabilidades (A.12.6.1) y desarrollo seguro (A.14.2.5).
- **CIS Benchmarks:** Soporta escaneo de infraestructura como código conforme a CIS Benchmarks.
- **SOC 2 / GDPR / HIPAA / PCI DSS:** Ayuda en auditorías de cumplimiento mediante remediación continua y visibilidad.

Revisión #9
Creado 2025-07-16 17:42:01 UTC
Actualizado 2025-07-16 22:36:28 UTC