Grype + Syft (by Anchore)

Descripción

- **Syft**: genera un SBOM (Software Bill of Materials).
- **Grype**: analiza el SBOM o imagen para encontrar CVEs.

Uso local

```
# Syft - generar SBOM
syft nginx:latest -o json > sbom.json

# Grype - escanear imagen
grype nginx:latest

# Escanear SBOM generado
grype sbom:sbom.json
```

Reportes

- JSON, table, CycloneDX, SPDX, SARIF.
- Puede exportarse a sistemas como Sonatype, DefectDojo.

Integración en CI/CD

- Una acción de GitHub para invocar el escáner Grype y devolver las vulnerabilidades encontradas, y opcionalmente fallar si se encuentra una vulnerabilidad con un nivel de gravedad configurable.

```
- name: Scan current project
  uses: anchore/scan-action@v6
  with:
    path: "."
```

Integraciones

- GitHub (SARIF reports en Security tab).
- Slack, Teams, Jira (mediante integraciones manuales/API).

- VSCode: No oficial, pero puede usarse vía terminal.

UI

- No posee UI propia.
- Compatible con Anchore Enterprise UI (versión paga).

Licencia

- **Open source (Apache 2.0)**.
- Funciona perfectamente en VMs locales.

Facilidad de uso

- Fácil. CLI clara, requiere instalación de dos binarios (`syft`, `grype`).

Cumplimiento con estándares:

- **OWASP:** Ayuda a mitigar riesgos del OWASP Top 10 relacionados con componentes desactualizados o vulnerables.
- **NIST:** Compatible con NIST SP 800-218 (SSDF) por generar y analizar SBOMs; se alinea con controles RA-5, SI-2 de NIST 800-53.
- **ISO/IEC 27001:** Contribuye a controles como A.8.1.1 (inventario de activos) y A.12.6.1 (vulnerabilidades técnicas).
- **CIS Benchmarks:** Aplica indirectamente cuando se usa en conjunto con políticas de seguridad de configuración.

Revisión #11
Creado 16 julio 2025 17:27:03
Actualizado 16 julio 2025 22:38:02