Trivy (by Aqua Security)

Descripción

Trivy es un escáner de seguridad todo en uno para contenedores, código, repositorios Git y más. Identifica vulnerabilidades (CVE), secretos expuestos y configuraciones erróneas.

Uso local

```
# Escanear una imagen Docker
trivy image nginx:latest

# Escanear archivos o repositorios
trivy fs .

# Escanear un repositorio remoto
trivy repo https://github.com/usuario/proyecto
```

Reportes

- Formatos: JSON, SARIF (para GitHub), tabla, plantillas personalizadas.
- Exportables a sistemas como DefectDojo.

Integración en CI/CD

- Ejecuta Trivy como acción de GitHub para escanear la imagen del contenedor Docker en busca de vulnerabilidades. Puede detener el pipeline si encuentra vulnerabilidades críticas.

```
      - name: Generate Trivy Vulnerability Report
        uses: aquasecurity/trivy-action@master
        with:
          scan-type: "fs"
          output: trivy-report.json
          format: json
          scan-ref: .
          exit-code: 0
```

Integraciones

- GitHub.
- Slack (via Webhook).
- Jira: se puede automatizar la creación de tickets con scripts + API.
- Plane, Microsoft Teams: vía Webhooks o bots.
- VSCode: extensión oficial para escaneo local.
- DevSecOps: se puede integrar con DefectDojo, Kubernetes Admission Controllers.

UI

- Tiene una **UI web experimental** en el proyecto Trivy Dashboard.
- CLI amigable.

Licencia

- **Open source (Apache 2.0)**.
- Puede instalarse localmente o en máquinas virtuales gratis.

Facilidad de uso

- Muy fácil. Documentación clara y CLI muy intuitiva.

Cumplimiento con estándares

- **OWASP:** Detecta vulnerabilidades en dependencias alineadas al OWASP Top 10, especialmente el punto A06:2021 sobre componentes vulnerables.
- **NIST:** Compatible con NIST SP 800-53 (controles RA-5, SI-2) al detectar vulnerabilidades técnicas de forma automatizada.
- **ISO/IEC 27001:** Apoya el cumplimiento del control A.12.6.1 (gestión de vulnerabilidades técnicas).
- **CIS Benchmarks:** Escanea configuraciones de contenedores y Kubernetes contra benchmarks de seguridad del CIS.

Revisión #14
Creado 2025-07-16 17:26:48 UTC
Actualizado 2025-07-16 22:32:00 UTC