Recomendaciones

Herramientas recomendadas para incluir en el stack tecnológico (open source y gratuitas)

Herramienta	Licencia	Motivo para incluir
Trivy	Apache 2.0 (OSS)	Escaneo de imágenes, código fuente, repositorios, configuración IaC, secretos. Rápido y versátil.
Grype + Syft	Apache 2.0 (OSS)	SBOM + análisis de vulnerabilidades. Ideal para cumplimiento con NIST y gestión de inventario.
OWASP ZAP	Apache 2.0 (OSS)	Escaneo de aplicaciones web. GUI, CLI y automatizable. 100% alineado con OWASP.
Semgrep	LGPL (Free tier)	Excelente para escaneo SAST. Reglas YAML personalizadas, muy útil para desarrollo seguro.
Checkov	Apache 2.0 (OSS)	IaC security. Compatible con Terraform, Kubernetes, CloudFormation, etc.
Falco	Apache 2.0 (OSS)	Detección de amenazas en tiempo real en contenedores y Kubernetes. Ideal para producción.

Estas herramientas:

- Son **open source reales** o con licencia suficientemente abierta para entornos empresariales.
- Funcionan bien en **máquinas virtuales** y en local.
- Se integran fácilmente en pipelines CI/CD.
- Cumplen con estándares como OWASP, NIST, ISO 27001, CIS Benchmarks.

Herramientas útiles pero con limitaciones en la versión gratuita.

Herramienta	Licencia	Uso recomendado / limitación
SonarQube	Community Edition OSS	Muy útil para SAST. La versión gratuita no incluye todos los lenguajes ni reglas avanzadas. Instalable en VM.
Snyk	Gratis con limitaciones	Muy potente, pero requiere cuenta. En la versión free se limita el número de escaneos y proyectos privados.

Puedes usarse si:

- Si se esta dispuesto a autohospedarlas (en el caso de SonarQube).
- Aceptas limitaciones funcionales para equipos pequeños (en el caso de Snyk).

Herramientas que podrías descartar (para uso exclusivo OSS / sin costo)

Herramienta	Motivo para descartar o evitar
Snyk (versión cloud)	Aunque potente, sus planes gratuitos son limitados para uso en producción o entornos empresariales. Necesita upgrade para características clave (políticas, tickets en Jira, control RBAC, etc.).
SonarQube (versión Enterprise)	Solo necesaria si necesitas análisis profundo de C++, COBOL, Salesforce, o reglas personalizadas complejas.

Recomendaciones según casos de uso:

- **Para Imágenes Docker y Seguridad general (SCA, IaC, secretos):**
  ➤ *Trivy* (rápido, simple, bien mantenido)
  ➤ *Grype + Syft* si necesitas generar o analizar SBOM
- **Para análisis de código fuente (SAST):**
  ➤ *SonarQube* si buscas reportes detallados por roles
  ➤ *Semgrep* si necesitas reglas personalizadas y flexibilidad
- **Para vulnerabilidades en infraestructura como código (IaC):**
  ➤ *Checkov* (fuerte soporte para Terraform, CloudFormation)
- **Para pruebas activas de aplicaciones web (DAST):**
  ➤ *OWASP ZAP* (ideal para pruebas automatizadas de apps web)
- **Para detección en tiempo de ejecución:**
  ➤ *Falco* (detección de anomalías en contenedores/Kubernetes)

Stack tecnológico DevSecOps recomendado (100% open source / gratuito)

Fase DevSecOps	Herramienta	Funcionalidad
SAST	Semgrep, SonarQube CE	Escaneo de código fuente y detección de bugs
SCA	Trivy, Grype + Syft	Escaneo de dependencias y vulnerabilidades (CVEs)
IaC Security	Checkov, Trivy	Revisión de infraestructura como código
DAST	OWASP ZAP	Escaneo dinámico de aplicaciones web
SBOM	Syft	Generación de lista de materiales de software
Runtime Security	Falco	Monitoreo de comportamiento en contenedores/K8s

---

Revisión #4
Creado 16 julio 2025 22:40:36

Actualizado 16 julio 2025 22:47:23