Metodología y Criterios para la Evaluación de Herramientas de Seguridad en el Desarrollo de Soluciones Digitales del Estado Dominicano

Objetivo del Documento

Seleccionar y recomendar herramientas de evaluación de seguridad que permitan fortalecer el desarrollo seguro de soluciones digitales, alineadas con estándares internacionales y buenas prácticas del sector.

Metodología de Evaluación

Se identificaron y evaluaron ocho herramientas reconocidas en la industria, considerando criterios relevantes definidos por el equipo de arquitectura digital. La información fue extraída de documentación oficial, comunidades técnicas, y pruebas en entornos de laboratorio.

Criterios de Evaluación

1. ¿Open Source?: Disponibilidad del código y posibilidad de uso sin licencia comercial.
2. Alcance de evaluación de seguridad: Cuales componentes o capas analiza (código, dependencias, contenedores, IaC, ejecución, etc.).
3. Integración con procesos DevSecOps: Facilidad para integrarse en flujos CI/CD.
4. Tipo de vulnerabilidades detectadas: Si realiza análisis SAST, DAST, SCA, IaC, runtime, secretos.
5. Facilidad de configuración y mantenimiento: Curva de aprendizaje y operatividad diaria
6. Soporte activo o comunidad: Existencia de soporte empresarial o comunidad activa.

7. Reportes comprensibles para Stakeholders: Facilidad de comprensión por distintos perfiles (técnicos, gerenciales).
8. Automatización en CI/CD: Si es posible su ejecución automatizada en pipelines.
9. Costo: Si tiene versiones gratuitas o es de pago.
10. Integración con herramientas usadas: Compatibilidad con herramientas como GitHub, Teams, Plane, Jira, etc.
11. Personalización de reglas o políticas: Posibilidad de definir reglas propias.
12. Cumplimiento de estándares: Si se alinea con OWASP, NIST, ISO 27001, etc

---

Revisión #3
Creado 2025-07-16 17:21:35 UTC
Actualizado 2025-07-16 17:56:13 UTC