

Ridgebot®

Plataforma de Seguridad Ofensiva impulsada por IA

Validación continua de seguridad, automatización de pruebas de penetración y emulación avanzada de amenazas para entornos empresariales.



Gestión avanzada de validación de seguridad

RidgeBot® es una plataforma de seguridad ofensiva basada en inteligencia artificial que automatiza pruebas de penetración, validación de vulnerabilidades y simulaciones de ataques avanzados.

Diseñada para empresas que buscan **reducir riesgos, aumentar la cobertura de seguridad y optimizar los procesos de ciberseguridad.**

■ PRUEBAS DE PENETRACIÓN AUTOMATIZADAS

Automatiza ataques internos, externos y autenticados para validar vulnerabilidades explotables.

■ EMULACIÓN DE ADVERSARIOS

Simula técnicas reales alineadas con MITRE ATT&CK para medir la efectividad de los controles.

■ PRIORIZACIÓN DE RIESGOS

Clasifica vulnerabilidades según impacto y probabilidad de explotación.

■ VALIDACIÓN CONTINUA

Ejecuta evaluaciones permanentes para identificar nuevas amenazas antes de que sean explotadas.

■ GESTIÓN DE SUPERFICIE DE ATAQUE

Descubre activos, dominios, aplicaciones, APIs y servicios expuestos.

■ AUTOMATIZACIÓN Y ESCALABILIDAD

Permite pruebas continuas en entornos on-premise, nube y arquitecturas híbridas.

Requisitos y compatibilidad

Implementación disponible en servidores físicos, máquinas virtuales y nube.

1. CPU Intel Xeon de múltiples núcleos.
2. 32 GB RAM mínimo recomendado.
3. Almacenamiento SSD desde 100 GB a 1 TB.
4. Compatibilidad con VMware ESXi, Hyper-V, KVM, AWS, Azure y Google Cloud.
5. Soporte para Windows, Linux, Unix, MacOS, bases de datos y dispositivos IoT.

Funciones principales



Descubrimiento automático de superficies de ataque y activos TI.



Validación de vulnerabilidades con explotación ética automatizada.



Pruebas de seguridad para APIs basadas en OWASP Top 10.



Soporte para pruebas DAST en aplicaciones web.



Visualización Kill-Chain y análisis en tiempo real.



Movimientos laterales y escalamiento de privilegios controlados.



Automatización de reportes multiidioma y remediación priorizada.



Capacidad de despliegue en AWS, Azure, Google Cloud y VMware.



Integración con Jira, ServiceNow, GitLab, Nessus y Qualys.



Escaneo de contraseñas débiles y validación de parches.

Escenarios Recomendados

1

Validación continua de postura de seguridad corporativa.

2

Auditorías de cumplimiento GDPR, LGPD y normativas de privacidad.

3

Pruebas ofensivas para DevSecOps y entornos CI/CD.

4

Entrenamiento de equipos SOC y Blue Team mediante emulación de amenazas.

5

Evaluación de infraestructura híbrida y cloud.

En Resumen

Función		Descripción
Pentesting Automatizado	✓	Validación continua y explotación ética.
API Security Testing	✓	Pruebas OWASP API Top 10.
MITRE ATT&CK	✓	Mapeo de tácticas y técnicas.
Reportes Multiidioma	✓	Español, inglés, portugués y más.
Integración DevSecOps	✓	Compatibilidad con Jira y ServiceNow.

Contacto y Recursos

Sitio web oficial:
<https://ridgesecurity.ai/>

Documentación y soporte
técnico disponible bajo
solicitud comercial.