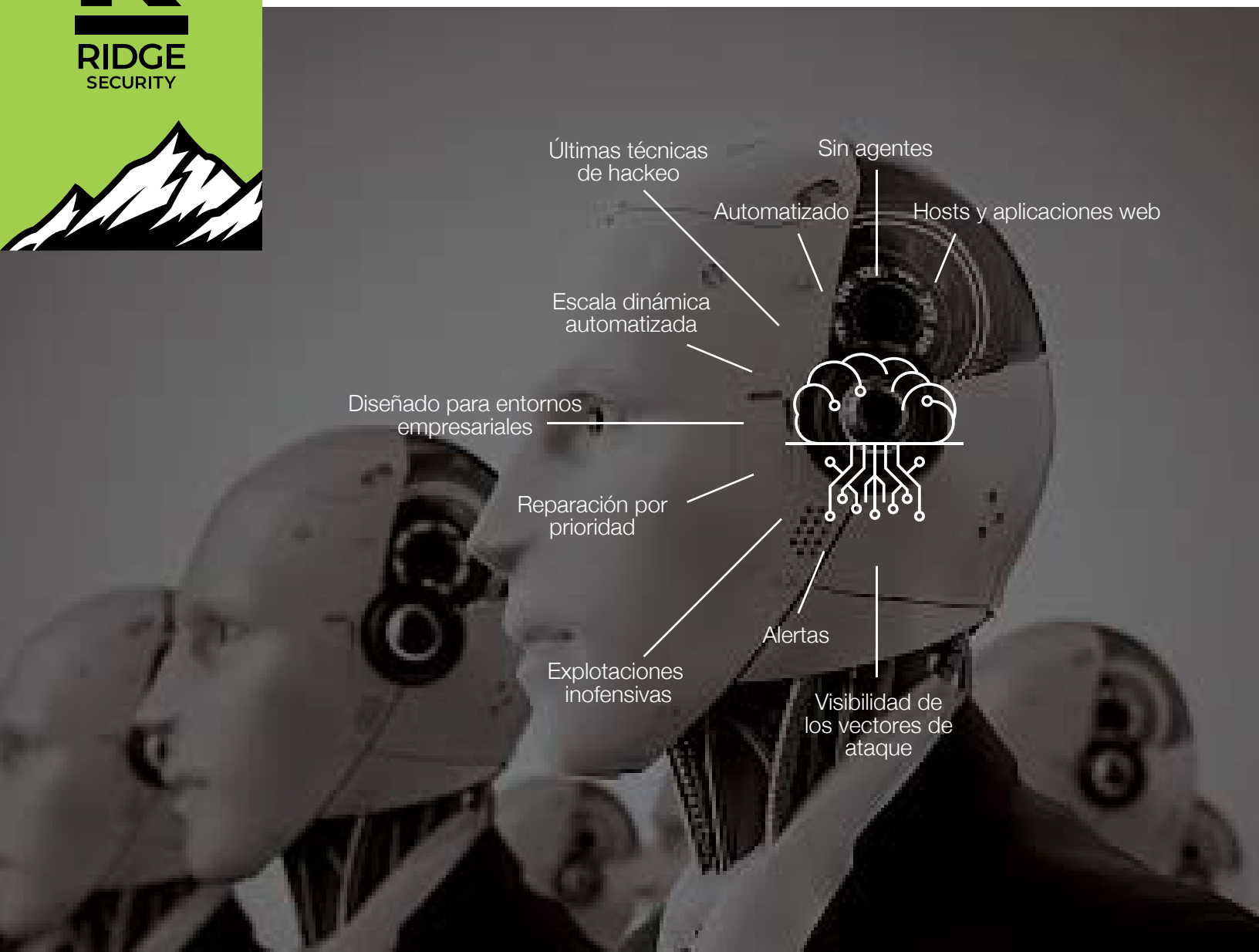
RidgeBot™ Trae Pruebas de penetración asequibles para su organización.

RIDGE SECURITY

RidgeBot™

Prueba de penetración automatizada de clase empresarial usando robots de validación inteligentes



RidgeBot™ automatiza todo el proceso de hacking ético

100 veces más rápido que un probador humano

Ridge Security está cambiando el juego con **RidgeBot**™, un robot inteligente de validación de seguridad. Equipado con las técnicas de hacking más avanzadas, **RidgeBot**™ tiene un conocimiento masivo de las amenazas, vulnerabilidades y explotaciones. Actuando como un verdadero hacker ético, **RidgeBot**™ implacablemente localiza y documenta los exploits. La automatización de las pruebas de penetración lo hace asequible con la capacidad de funcionar a escala. Trabajando dentro de un ámbito definido, **RidgeBot**™ se replica instantáneamente para abordar estructuras altamente complejas.

Ridge Security permite a las empresas y a los equipos de aplicaciones web, DevOps, ISVs, gobiernos, sanidad, educación -o a cualquier persona responsable de garantizar la seguridad del software- probar sus sistemas de forma asequible y eficiente.

Desafíos

La mayoría de las organizaciones utilizan pruebas de seguridad (también conocidas como pruebas de penetración) para validar la postura de seguridad de su red y sus sistemas. En dicha prueba, los probadores de seguridad asumen el papel de un hacker y tratan de entrar en el entorno informático de la organización para encontrar vulnerabilidades y determinar cómo explotan un ataque de hacker en el mundo real.La idea subyacente es que una buena prueba de seguridad debería revelar cómo un atacante podría infiltrarse en los sistemas de una organización antes de que ocurra.

Las pruebas de penetración adecuadas ayudan a los organizadores a abordar los problemas de una manera más manejable y rentable.

Sin embargo, los atacantes siempre están desarrollando nuevos exploits y métodos de ataque, a menudo utilizando el aprendizaje automático (ML) para lanzar ataques automáticamente. Los equipos de seguridad de las empresas y los "probadores de penetración" profesionales están sometidos a una enorme presión para mantenerse al día

La solución y el beneficio clave de RidgeBot

RidgeBot™ proporciona servicios de validación de seguridad automatizados. Ayuda a los encargados de las pruebas de seguridad a superar las limitaciones de conocimientos y experiencia y siempre por formas a un nivel superior consistente. El cambio de las pruebas manuales y de trabajo intensivo a la automatización asistida por máquinas alivia la grave escasez actual de profesionales de la seguridad. Permite a los expertos en seguridad humana dejar de lado el trabajo diario intensivo y dedicar más energía a la investigación de nuevas amenazas y nuevas tecnologías.

- Mejorar la cobertura y la eficiencia de las pruebas de seguridad
- Reducir el costo de la validación de seguridad
- Proteger continuamente el entorno informático
- Producir resultados factibles y fiables para los diferentes interesados

RidgeBot™ trae **pruebas de penetración automatizadas** al alcance de todas las organizaciones.

RidgeBot™ Funciones principales

En una tarea determinada, RidgeBot™ automatiza todo el proceso de hacking ético. Cuando se conecta al entorno informático de una organización, RidgeBot™ descubre automáticamente todos los diferentes tipos de activos de la red y luego utiliza la base de datos de conocimiento colectivo de vulnerabilidades para minar el sistema objetivo. Una vez que RidgeBot™ identifica las vulnerabilidades, utiliza técnicas de piratería informática incorporadas y explota las bibliotecas para lanzar un verdadero ataque ético contra la vulnerabilidad. Si tiene éxito, la vulnerabilidad es validada y se documenta toda la transacción de la cadena de ataques.

RidgeBot™ proporciona un rico análisis para la evaluación de riesgos y la priorización, exportando un informe completo con consejos de remediación, dando herramientas para la verificación de parches.

Perfiles de activos—Basándose en técnicas de rastreo inteligente y algoritmos de huellas dactilares, descubre amplios tipos de activos de TI: IPs, dominios, hosts, SO, aplicaciones, sitios web, plugins y dispositivos de red.

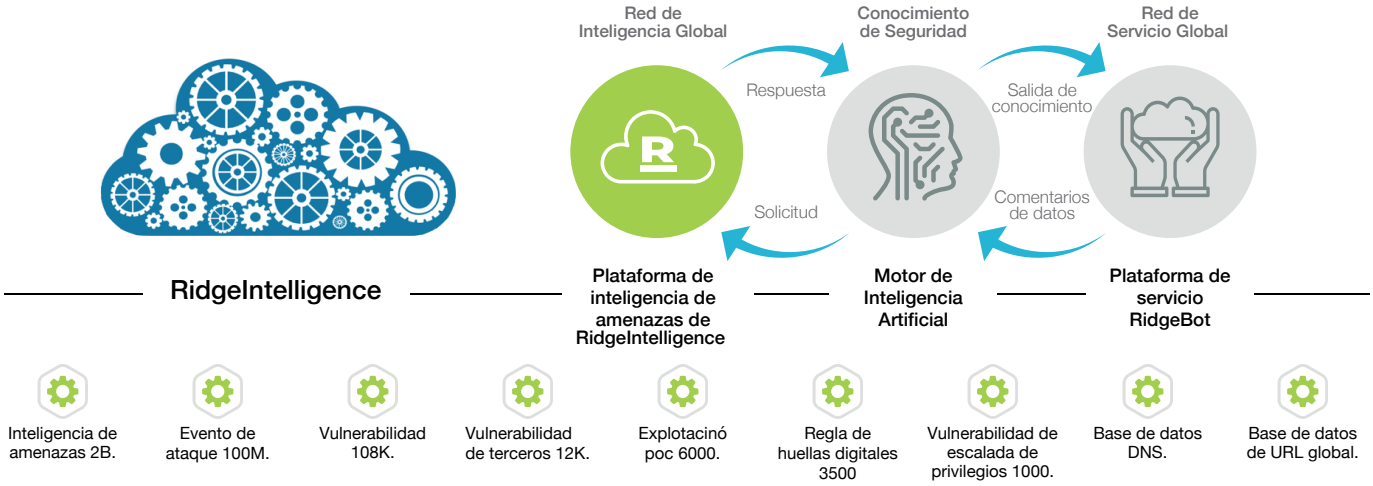
Minería de vulnerabilidades—Utilizando herramientas de escaneo patentadas, nuestra rica base de conocimiento de vulnerabilidades y eventos de violación de seguridad, además de varios modelos de riesgo.

Explotación de vulnerabilidades—utilice una caja de arena inteligente para simular ataques del mundo real con kits de herramientas. Recopilar más datos para un ataque posterior en una etapa posterior a la violación.

Priorización de riesgos—Forme automáticamente una vista analítica, visualice una cadena de asesinatos y muestre un guión de hacker. Mostrar los resultados de la piratería como datos y privilegios escalados de los objetos comprometidos.

Mayor precisión y más descubrimientos con el cerebro de la IA

RidgeBot™ tiene un poderoso "cerebro" que contiene algoritmos de inteligencia artificial y una base de conocimientos expertos que guía a RidgeBot™ en la búsqueda/selección de ataques. Lanza ataques iterativos basados en los aprendizajes del camino, logrando una cobertura de pruebas más completa y una inspección más profunda.



RidgeBot™ Escenario de despliegue

Para el entorno de la empresa, despliegue RidgeBot™ en la premisa del cliente

Escenarios de Pentest

Ataque interno. Lanzar ataques desde el interior de la red de la empresa con el permiso del cliente, centrándose en la explotación de las vulnerabilidades descubiertas en la red y los sistemas locales.

Ataque externo. Lanzar ataques desde fuera de la red de la empresa hacia activos de acceso público como los sitios web de las organizaciones, los archivos compartidos o los servicios alojados en la nube pública/CDN.

Requisitos del sistema en el establecimiento

Para el despliegue en el sitio, nuestra solución RidgeBot™ es un paquete de software desplegado en servidores específicos de metal desnudo o máquinas virtuales. El paquete de software RidgeBot™ incluye la plataforma RidgeIntelligence, el motor RidgeBrain y los plugins de RidgeBot™. Las actualizaciones del software se proporcionan a través de servicios profesionales. Recomendamos el despliegue en el lugar para que las organizaciones tengan un control completo sobre los procedimientos de prueba, los hallazgos y los datos sensibles involucrados.

Implementación de servidores básicos	**Esenciales**	**Avanzado**
Requisitos mínimos de hardware	• CPU Intel Xeon con un mínimo de 4 núcleos32 GB RAM • 1TB SSD • 2 Interfaces de Ethernet	• CPU Intel Xeon duales con un minimo de 6núcleos • 64 GB RAM • 2X1TB SSD con controlador RAID (RAID1) • 2 Interfaces de Ethernet
Plataformas de referencia	**Servidor en Rack Dell PowerEdge R340** • Intel Xeon E-2278G 3.4GHz, caché de 16M, 8C / 16T, Turbo (80W) • 32 GB (2 x 16GB 2666MT/s DDR4 ECC UDIMM) • 960GB SSD vSAS Uso mixto 12Gbps 512e 2.5in con 3.5in HYB CARR Hot-Plug AG drive, 3 DWPD 5256 TBW • https://www.dell.com/en-us/work/shop/productdetailstxn/poweredge-r340	**Servidor en Rack Dell PowerEdge R540** • Dual Intel Xeon Silver 4208 2.1G, 8C / 16T, 9.6GT / s, Turbo, HT (85W) DDR4-2400 • 64 GB (2 RDIMM de 32 GB, 3200 MT / s, rango dual) • Controladora RAID PERC H730P, caché NV de 2 GB, adaptador, perfil bajo • 2X960GBSSDSATAMixUse6Gbps512 Unidad AG de conexión en caliente de 2,5 pulgadas, HYB CARR de 3,5 pulgadas, 3 DWPD, 5256 TBW, RAID 1 • https://www.dell.com/en-us/work/shop/productdetailstxn/poweredge-r540
Bots simultáneos	**16**	**32**

Despliegues de máquinas virtuales	**Demostración/Laboratorio**	**Producción**
Requisitos mínimos de hardware	• 8 vCPU • 16 GB RAM • 100 GB Storage • 2 Interfaces de Ethernet	• 8 vCPU • 32 GB RAM • 100 GB Storage • 2 Interfaces de Ethernet
Bots simultáneos de apoyo	**16**	**32**
Hipervisores compatibles	• VMware Workstation 15 Pro or higher • VMware Fusion 11 Pro or higher • VMware ESXi 6.5 or higher	

RidgeBot™ Características principales

Asistencia a la utomización

- **Reconocimiento de objetos:** Mediante este módulo de funciones, RidgeBot™ identifica automáticamente información como los tipos de bienes, los tipos de contenido de los datos, los identificadores de clasificación de registros y los proporciona a los módulos pertinentes, de modo que todo el proceso de ataque pueda seguir ejecutándose sin una intervención manual y lograr el proceso automatizado de las tareas de validación de la seguridad.
- **Simulación de caja de arena:** Utilizando la tecnología de la caja de arena, RidgeBot™ simula una variedad de entornos operativos en la tarea de validación, proporciona una respuesta automática a los escenarios interactivos durante el ataque, de modo que se pueda realizar el proceso automatizado de validación de la seguridad.

Inteligencia Artificial

- **Reconocimiento de objetos:** Mediante este módulo de funciones, RidgeBot™ identifica automáticamente información como los tipos de bienes, los tipos de contenido de los datos, los identificadores de clasificación de registros y los proporciona a los módulos pertinentes, de modo que todo el proceso de ataque pueda seguir ejecutándose sin una intervención manual y lograr el proceso automatizado de las tareas de validación de la seguridad.
- **Cerebro de decisión:** RidgeBot™ está construido con muchos tipos de algoritmos de toma de decisiones de inteligencia artificial para proporcionar decisiones óptimas como la selección y clasificación cuando las ejecuciones van a bajar a las rutas de ataque de las ramas.
- **Sistema experto:** RidgeBot está integrado en un sistema experto. Durante la ejecución de la validación de seguridad, siempre puede hacer referencia a la "experiencia de los expertos" para un una mejor decisión o un camino más efectivo para penetrar en el sistema de objetivos.
- **Motor vectorial:** El motor vectorial crea vectores de ataque y costuras no lineales que permiten a RidgeBot™ producir un ataque más eficiente con una alta tasa de éxito hacia el sistema objetivo.

Análisis de riesgos

- **Retrato de topología:** Generar automáticamente un mapa de la topología a partir de la información recogida durante el ataque, etiquetar los riesgos identificados en cada parte de la topología y ayudar a los administradores en el análisis y la evaluación de los riesgos.
- **Concienciación proactiva de la situación:** Pro- métase activamente en el sistema objetivo desde múltiples perspectivas para formar una visión de análisis multidi- mensional y los modelos gráficos en tiempo real; proporcione a los administradores una visión global del panorama de la seguridad.
- **Visibilidad de la acción de ataque en tiempo real:** Pro- video visibilidad en tiempo real de cada paso del ataque, desde el descubrimiento, el escaneo para explotar los intentos del equipo de seguridad para analizarlos más a fondo.

Minería de la vulnerabilidad

- **Descubriendo la debilidad:** Identificar posibles puntos débiles en la superficie de ataque y comprobar las vulnerabilidades basadas en el sistema de decisión de inteligencia como los modelos expertos y los cerebros de RidgeBot.
- **Escaneo de vulnerabilidades:** Se accede y se prueba el sistema mediante el uso de un generador de paquetes y la carga util proporcionada por el componente de ataque, el motor vectorial, etc., y se comprueban los resultados devueltos para determinar si existen vulnerabilidades que puedan ser explotadas.

Validación de permisividad

- **Validacion exacta:** Verificar si la vulnerabilidad es real utilizando la carga útil proporcionada por el motor vectorial y el componente de validacion de la vulnerabilidad. La prueba incluye el contenido de la respuesta, los datos o los privilegios obtenidos.
- **Prueba de parche:** Prueba de nuevo despues del parquet para verificar que la vulnerabilidad ha sido corregida.

Explotación de la vulnerabilidad

- **Ataque a la intranet:** Aprovechar las vulnerabilidades verificadas para realizar ataques al mismo nivel de la red.
- **Ataque local:** Obtener un mayor nivel de acceso desde un permiso de nivel de usuario explotando las vulnerabilidades verificadas y las herramientas de explotación.
- **Movimiento lateral:** Despues de obtener una misión por el host objetivo, utilice el host como un pivote para explotar aún más las vulnerabilidades y obtener acceso a otras partes del sistema.

Acerca de la tecnología de Ridge Security

Ridge Security ofrece soluciones éticas, eficientes y asequibles para las pruebas de penetración a empresas, pequeñas y grandes. Nos aseguramos de que nuestros clientes cumplan con las normas, estén alerta y sean seguros en todo momento en el mundo cibernético. El equipo de administración tiene muchos años de experiencia en redes y seguridad. Ridge Security está ubicada en el corazón de Silicon Valley y se está expandiendo a otras áreas, incluyendoAmérica Latina, Asia y Europa.

RidgeBot,™ un sistema de pruebas de penetración robótica, automatiza completamente el proceso de prueba acoplando técnicas de hacking éticas a los algoritmos de toma de decisiones. Los RidgeBots localizan, explotan y documentan los riesgos y vulnerabilidades empresariales descubiertos durante el proceso de prueba, destacando el impacto o daño potencial.

Contacte con Ridge Security para obtener más información.

Sales@RidgeSecurity.ai RidgeSecurity.ai/contact-us

Ridge Security Technology Inc.

www.ridgesecurity.ai

@RidgeSecurityAI

www.linkedin.com/company/ridge-security