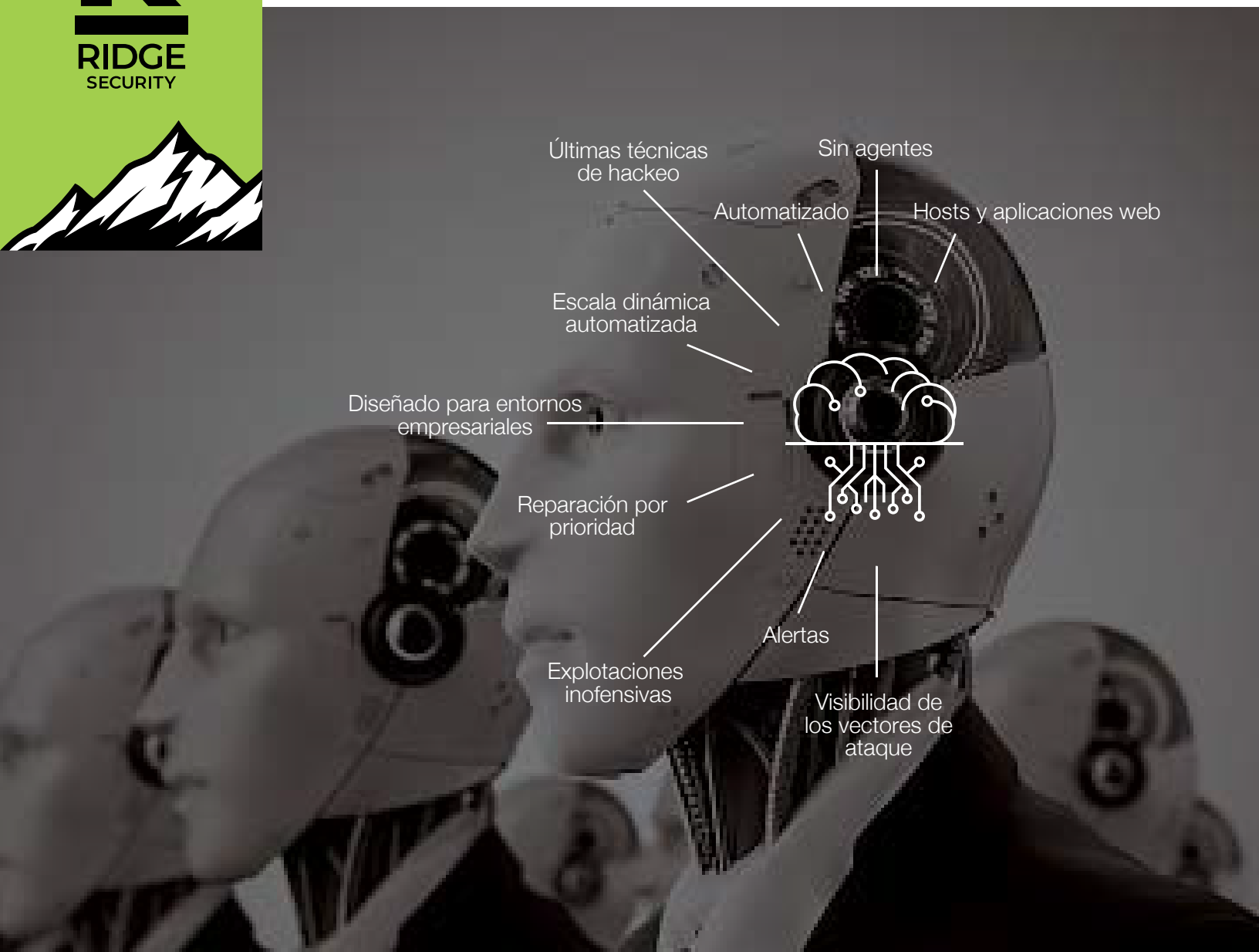
RidgeBot™ Trae Pruebas de penetración asequibles para su organización.

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.

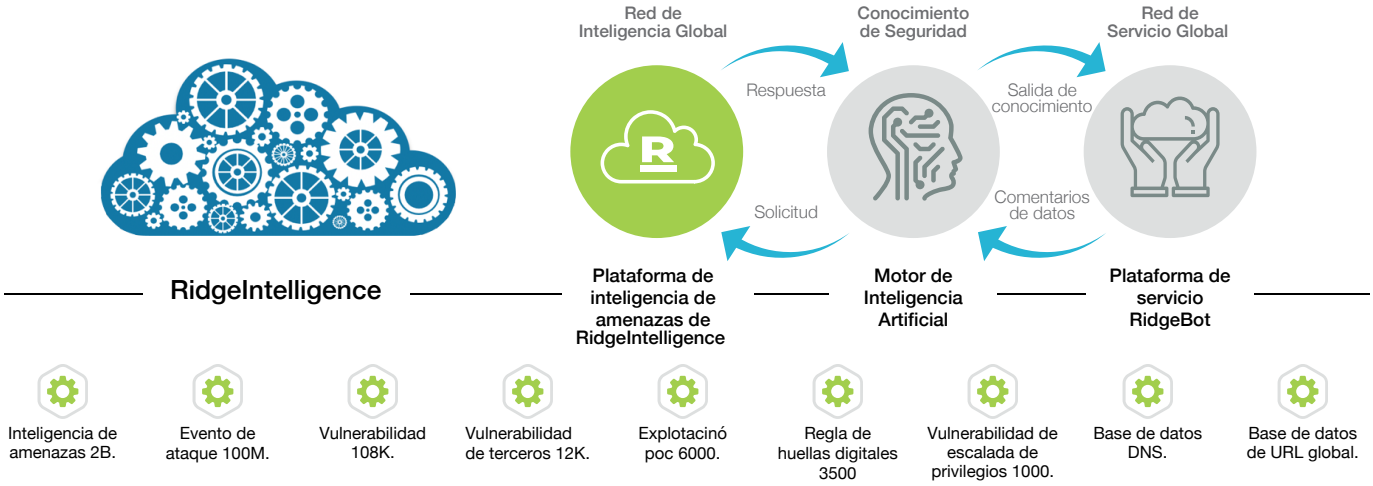
Minería de vulnerabilidades—Utilizando herramientas de escaneo patentadas, nuestra rica base de conocimiento de vulnerabilidades y eventos de violación de seguridad, además de varios modelos de riesgo.

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 Despliegues

Implementación en Intalacion

Para el entorno empresarial: implementar RidgeBot® en las instalaciones del cliente, proporcione el menor riesgo de fuga de datos de seguridad de la información

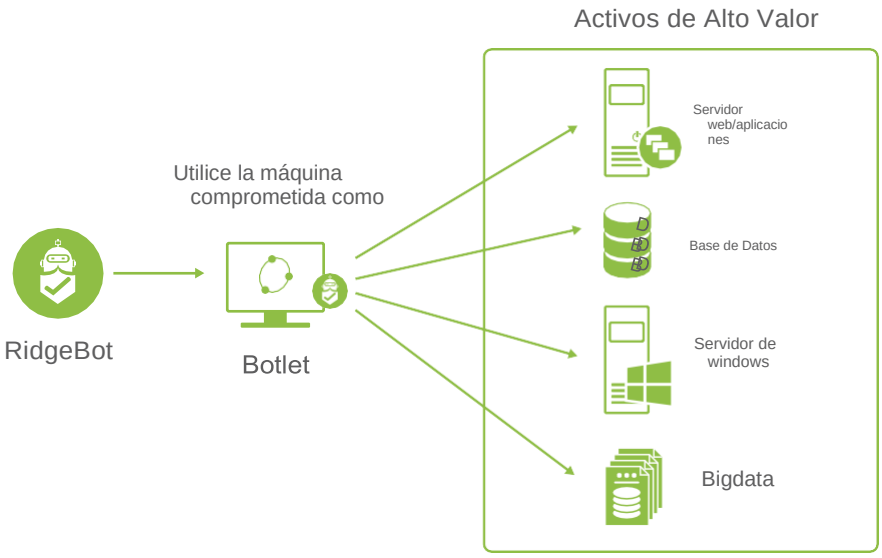
Implementación en Nube

Para clientes de nube y pymes: implemente RidgeBot® en la nube (AWS EC2, Microsoft Azure y Google Cloud), tienen una mayor flexibilidad y minimizan la inversión inicial de CapEx

Escenarios de pruebas de penetración

Ataque Interno. Despliegue ataques desde el interior de la red empresarial con el permiso del cliente, centrándose en explotar las vulnerabilidades descubiertas en la red y los sistemas locales.
Ataque externo. Lance ataques desde fuera de la red empresarial hacia activos de acceso público, como sitios web de organizaciones, recursos compartidos de archivos o servicios alojados en la nube pública/CDN.
Movimiento lateral. Escalar privilegios en un activo comprometido y utilizar el activo comprometido como pivote para lanzar un ataque hacia las redes adyacentes; descubra y explote vulnerabilidades en activos más profundos en la red.

RidgeBot Movimiento Lateral



Métodos de emulación cibernética del adversario (ACE)

Simulación de ataques basada en agentes: RidgeBot® utiliza Botlet basado en agentes para simular ataques de adversarios.

RidgeBot® Botlet se puede implementar en múltiples plataformas de SO y en diferentes segmentos de red para simular amenazas cibernéticas del mundo real de forma continua o bajo demanda.

Evaluación lista para usar: RidgeBot® ofrece plantillas de prueba de evaluación ACE preconstruidas, lo que facilita que todos los niveles de habilidad evalúen la eficacia en diferentes aspectos de sus controles de seguridad. Las pruebas de evaluación son completas y seguras para ejecutar en el entorno de producción.

Alineación del marco MITRE ATT&CK: El marco MITRE ATT&CK es una base de conocimiento accesible a nivel mundial de tácticas y técnicas del adversario basadas en observaciones del mundo real. RidgeBot utiliza ampliamente la base de conocimientos de ATT&CK para crear scripts de prueba de evaluación significativos y realistas para que sus clientes desafíen, evalúen y optimicen sus controles de seguridad.

Requisitos del sistema RidgeBot

RidgeBot® La solución es un paquete de software desplegado en servidores dedicados específicos, máquinas virtuales o en la nube.

RidgeBot® El paquete de software incluye la plataforma RidgeIntelligence, el motor RidgeBrain y Ridge- Bot® complementos Las actualizaciones de software se proporcionan a través de servicios profesionales. Recomendamos la implementación local para que las organizaciones tengan un control total sobre los procedimientos de prueba, los hallazgos y los datos confidenciales involucrados.

Implementaciones en servidores Bare metal	**Esencial**	**Avanzado**
Requisitos Mínimos de Hardware	• Intel Xeon CPU con un mínimo de 4 cores con Hyper-Threadin • 32 GB RAM • 1TB SSD • 1 Ethernet Interface Card	• Intel Xeon CPUs Duales con un mínimo de 6cores cada uno • 64 GB RAM • 2 X 1TB SSD con controlador (RAID 1) • 1 Ethernet Interface Card
Plataformas de Referencia	Dell PowerEdge R340 Rack Server • Intel Xeon E-2278G 3.4GHz, 16M cache, 8C/16T, Turbo (80W) • 32 GB (2 x 16GB 2666MT/s DDR4 ECCUDIMM) • 960GB SSD vSAS Mixed Use 12Gbps512e 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	Dell PowerEdge R540 Rack Server • Dual Intel Xeon Silver 4208 2.1G, 8C/16T, 9.6GT/s,Turbo, HT (85W) DDR4-2400 • 64 GB (2 X 32GB RDIMM, 3200MT/s,Dual Rank) • PERC H730P RAID Controller, 2GB NVCache, Adapter, Low Profile • 2 X 960GB SSD SATA Mix Use 6Gbps 512 2.5in Hot-plug AG Drive,3.5in HYB CARR, 3 DWPD, 5256 TBW, RAID 1 https://www.dell.com/en-us/work/shop/productdetailstxn/poweredge-r540
Bots simultáneos	16	32

Implementaciones de máquinas virtuales/nube	**Demostración/Laboratorio**	**Producción**
Requerimientos Mínimos de Hardware	• 8 vCPU • 16 GB RAM • 100 GB Storage • 1 virtual Network interface	• 8 vCPU • 32 GB RAM • 100 GB Storage • 1 virtual Network interface
Bots simultáneos Compatibles	16	32
Hipervisores y plataformas en la nube compatibles	• VMware Workstation 15 Pro o Superior • VMware Fusion 11 Pro o Superior • VMware ESXi 6.5 o Superior • Microsoft Windows/Hyper-V 2019 o Superior • QEMU KVM 7.2	• Amazon AWS EC2 • Microsoft Azure • Google Cloud Platform

RidgeBot® Caracteristicas Principales

Asistencia de automatización

- **Reconocimiento de objetos:** A través de este módulo de funciones, RidgeBot® identifique automáticamente información como tipos de activos, tipos de contenido de datos, Identificadores de clasificación de registros y luego envíelos a los módulos relevantes, de modo que todo el proceso de ataque puede continuar ejecutándose sin ninguna intervención manual y lograr el proceso automatizado de tareas de validación de seguridad.
- **Simulación de sandbox**: utilizando la tecnología de sandbox, RidgeBot® simula una variedad de entornos operativos en la validación de tareas proporciona una respuesta automática a escenarios interactivos durante el ataque, de modo que se pueda realizar el proceso automatizado de validación de seguridad.
- **Motor de fuzzing integrado:** generación de cargas útiles dinámicas para la detección de vulnerabilidades y explotación

Inteligencia Artificial

- **Confrontación de Turing:** mediante el uso de la tecnología de confrontación de Turing, RidgeBot® puede reconocer el código de validación de caracteres y simular operaciones manuales a través de un sandbox inteligente para evitar la inspección de operación manual requerida por el sistema, de modo que el sistema pueda realizar una ejecución automática de la inspección de seguridad que mejora la eficacia de la seguridad pruebas.
- **Cerebro de Decisión:** RidgeBot® está integrado con muchos tipos de algoritmos de toma de decisiones de inteligencia artificial para proporcionar decisiones óptimas, como selección y clasificación cuando las ejecuciones descienden a rutas de ataque de rama
- **Sistema Experto:** RidgeBot está integrado con un sistema experto. Durante la ejecución de la validación de seguridad, siempre puede hacer referencia a "experiencia experta" para una mejor decisión o un camino más efectivo para penetrar el sistema de destino.
- **Motor Vectorial:** El motor de vectores crea vectores de ataque y uniones no lineales que permiten a RidgeBot® producir un ataque más eficiente con una alta tasa de éxito hacia el sistema objetivo.

Análisis de Riesgo

- **Detalle de la topología:** genere automáticamente un mapa de topología a partir de la información recopilada durante el ataque, etiquete los riesgos identificados en cada parte de la topología y ayude a los administradores en el análisis y la evaluación de riesgos.
- **Conciencia situacional proactiva:** Empuje proactivamente el sistema de destino desde múltiples perspectivas para formar una vista de análisis multidimensional y los modelos gráficos en tiempo real; proporcionar a los administradores una visión global del panorama de la seguridad.
- **Visibilidad de la acción del ataque en tiempo real:** Proporcione visibilidad en tiempo real de cada paso del ataque, desde el descubrimiento, el escaneo hasta los intentos de explotación por seguridad. equipo para seguir analizando.

Minería en Vulnerabilidades

Detección de debilidades: identifique posibles puntos débiles en la superficie de ataque y verifique las vulnerabilidades según el sistema de decisión inteligente, como los modelos expertos y los cerebros de RidgeBot.

Escaneo de vulnerabilidades: acceda y pruebe el sistema de destino mediante el uso de paquetes generados por una herramienta automática y la carga proporcionada por el componente de ataque, el motor vectorial, etc., y el devuelto los resultados se comprueban para determinar si hay vulnerabilidades que se puedan explotar

Vulnerabilidad y Explotación

- **Vector de ataque compatible:**

Ataque de red: Explore la red conectada máquinas de destino, descubra proactivamente y explotar fallas de seguridad en las máquinas de destino para acceder.

Ataque local/Escalada de privilegios: Después obtener un acceso con privilegios más bajos en la máquina de destino, explotar adicionales vulnerabilidades de locales para ganar elevado privilegio.

Movimiento lateral: gana el control de un activo comprometido y utilizarlo como pivote para explotar otro objetivo máquinas en redes adyacentes

- **Cobertura de ataque**

Servidores Host (Windows, Linux, Unix, MacOS y otros), Servidores Web, Servidores de Aplicaciones, Servidores de Bases de Datos (Oracle, IBM DB2, MS SQL Server, MySQL, PostgreSQL y otros), Plataformas de Virtualización, Network

- **Movimiento lateral:** Modo de intervención del usuario de ataque Permita que los Pentester experimentados controlen los ataques de complementos de prueba de penetración de alto impacto, proporcione un mejor control de riesgos y visibilidad de ataques

- **Pruebas de seguridad de aplicaciones**

Admite aplicaciones dinámicas Pruebas de seguridad (DAST) Soporte web autenticado Pruebas de penetración con incorporado grabador de secuencia de inicio de sesión web y modo proxy.

- **Contraseña débil de fuerza bruta** Escenario de validación de seguridad dedicado para sistema operativo, aplicación y base de datos débiles aprovechando la ventaja de la credencial

- **Pruebas automáticas de inyección tipo SQL:**

Automatiza el proceso de detección explotando fallas de inyección de SQL y más de servidores de base de datos.

- **Complementos de pentest personalizables**

Huella dactilar de la aplicación personalizable por el usuario, vector de ataque, carga útil de detección de vulnerabilidades, carga útil de explotación de vulnerabilidades (scripts y reglas), así como sugerencias de remediación

Validacion de Vulnerabilidades

Validación de riesgos: valide si la vulnerabilidad es explotable en el entorno real del usuario mediante el uso de la carga útil de prueba de concepto generada por la base de conocimiento de RidgeBot y el motor de explotación automática. Se proporciona prueba de una explotación exitosa para los riesgos validados, incluye el privilegio obtenido, screenshots, shell terminal, file manager, database name or database table name etc.

Visualización de Kill-Chain: visualice la ruta de ataque completa con información de la secuencia de ataque, incluida la información de la máquina de destino, la exposición de la superficie de ataque, la vulnerabilidad descubierta y la vulnerabilidad explotada.

Evaluación de riesgos: proporcione una evaluación de riesgos en tiempo real para los activos de TI que se están probando, incluida la calificación de puntaje de salud y detalles de vulnerabilidad y análisis de riesgos

Prueba de validación de parches: Vuelva a realizar la prueba después de instalar el parche para verificar si la vulnerabilidad se ha solucionado.

Emulacion cibernéticos del Adversario

- RidgeBot Botlet es compatible con plataformas Windows y Linux de 32 y 64 bits

• Los guiones de las pruebas de evaluación se asignan a Grupos de amenazas y MITRE ATT&CK y Tecnica

Administración de tareas

• Programación de tareas: Soporte 1) Ejecutar ahora, 2) Ejecutar una vez,3) Semanalmente (Diariamente)

4) Programación mensual de tareas

• Admite múltiples ejecuciones dentro de un ciclo de tareas semanal/mensual

• Soporte de pausa programada para tareas de prueba de penetración para minimizar la interrupción del negocio durante una prueba de penetración

• **Control sigiloso:** control de flujo de prueba de penetración de 4 niveles para controlar el volumen de tráfico que se envía a las máquinas de destino y minimizar el impacto en los objetivos de prueba

Gestión de activos

• Un repositorio centralizado para administrar hosts probados y objetivos web,aplicaciones/servicios activos, SO y versiones de aplicaciones, así como nombres de dominio y resoluciones de DNS

• Instalación y estado de Botlet

• Configurar conectores de integración

Informes e integración de sistemas de terceros

• Informe profesional: proporcione informes de pruebas de validación de seguridad profesionales con información detallada de activos, datos de vulnerabilidad y riesgo, resultados de pruebas de evaluación, sugerencias de mitigación y tendencias históricas

• Informes en varios idiomas: Admite informes en inglés, español, italiano y coreano. El cliente puede seleccionar un idioma preferido antes de generar los informes

- Informes de cumplimiento de los 10 principales de OWASP. Admite las versiones 2017 y 2021 de la definición OWASP Top-10. Plantillas de informes OWASP Top-10 dedicadas para tareas de pruebas de penetración web
- Compatibilidad con la validación de resultados de escaneo para escáneres Tenable Nessus Pro y Rapid7 Nexpose VA
- Informes de marca compartida de MSSP: admite la personalización de informes y permite que un usuario de MSSP (proveedor de servicios de seguridad administrados) agregue el logotipo de su empresa en las pruebas

• Integración del sistema: Admite API RESTful y los mensajes de registro del sistema compatibles con CEF, fácil de integrar con la plataforma de administración de seguridad de terceros. Admite la autenticación basada en tokens para la comunicación API

• Integración de DevSecOps: compatibilidad con Jira Software y GitLab para el seguimiento de problemas

System Administration

- Support online and offline software updates
- Support user role-base access control for reports
- Support local management console for system administration and service recovery
- Support two-factor authentication (2FA) or or virtual private cloud (VPC) acces
- Support open VPN for enterprise
- Support security validation tasks and

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