RidgeBOT

Robot Inteligente de Validación de Seguridad

RIDGE SECURITY

Visión General

Muchas organizaciones utilizan pruebas de seguridad (también conocidas como pruebas de penetración) para validar la postura de seguridad de su red. En dicha prueba, los testers de seguridad asumen el papel de un hacker y hacen todo lo posible para entrar en el entorno de TI de la organización. El propósito es encontrar vulnerabilidades y determinar cómo se explotan las vulnerabilidades en un ataque de piratas informáticos del mundo real. La idea subyacente es que una buena prueba de seguridad debería revelar cómo un atacante podría abrirse camino a través de los sistemas de la organización antes de que suceda. Las pruebas de penetración adecuadas ayudan a las organizaciones a abordar los problemas de una manera más manejable y rentable.

Sin embargo, hoy en día, los atacantes siempre están desarrollando nuevos exploits y métodos de ataque, y a menudo utilizan el aprendizaje automático (ML) para lanzar ataques automáticamente. Los equipos de seguridad de las empresas y los “testers de penetración” profesionales están bajo una enorme presión para mantenerse al día.

RidgeSecurity está cambiando este juego con RidgeBOT, este es un robot inteligente de validación de seguridad. RidgeBOT se presenta como un robot con conocimiento colectivo de amenazas, vulnerabilidades y exploits, y está equipado con técnicas de piratería de última generación. RidgeBOT actúa como un verdadero atacante, localiza, explota y documenta implacablemente sus hallazgos. RidgeBOT automatiza las pruebas de penetración, lo que lo hace asequible con la capacidad de ejecutarse a escala. Trabaja dentro de un alcance definido y se replica instantáneamente para abordar estructuras altamente complejas.

RidgeSecurity permite a las empresas y equipos de aplicaciones web, DevOps, ISV, gobiernos, atención médica, educación, o cualquier persona responsable garantizar la seguridad del software, probar sus sistemas de manera económica y eficiente.

RidgeBOT proporciona servicios continuos de validación de seguridad. Ayuda a los evaluadores de seguridad a superar las limitaciones de conocimientos y experiencias desempeñándose siempre al más alto nivel. El cambio de las pruebas manuales a las asistidas por máquina alivia la grave escasez actual de profesionales de la seguridad. Esto les permite a los expertos en seguridad abandonar el trabajo intenso que tienen a diario para poder dedicar más energía a la investigación de nuevas amenazas y tecnologías.

- Mejora la cobertura de prueba de seguridad y la eficiencia
- Reduce el costo de validación de seguridad
- Protege continuamente el entorno de TI
- Produce resultados procesables y confiables para las diferentes partes interesadas

Funciones Clave de RidgeBOT

En una tarea determinada, RidgeBOT automatiza todo el proceso de ataque. Cuando se conecta al entorno de TI de una organización, RidgeBOT descubre automáticamente todos los diferentes tipos de activos en la red y luego utiliza la base de datos de conocimiento colectivo de vulnerabilidades para extraer el sistema de destino. Una vez que RidgeBOT descubre vulnerabilidades, utiliza técnicas de piratería integradas y explota bibliotecas para lanzar un ataque real contra la vulnerabilidad. Si tiene éxito, la vulnerabilidad se valida y documenta toda la transacción de kill-chain. RidgeBOT proporciona análisis exhaustivos para la evaluación y priorización de riesgos, exportando un informe completo con consejos de remediación. 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 rutas de ataque, lanzando ataques reiterativos que se basan en los aprendizajes a lo largo del camino para lograr una cobertura de prueba mucho más amplia e inspección más profunda. Debido a su facilidad de uso amigable y escalabilidad ilimitada, RidgeBOT es adoptado tanto por grandes organizaciones como por equipos de desarrollo de aplicaciones web más pequeños.

- **Autodescubrimiento de activos** RidgeBOT puede identificar automáticamente grandes tipos de activos, incluidas redes, hosts, aplicaciones, complementos, imágenes, dispositivos IoT y dispositivos móviles, por ejemplo.
- **Minería de vulnerabilidades** RidgeBOT aprovecha la plataforma Threat Intelligence de RidgeSecurity que incluye 2 mil millones de datos de inteligencia de seguridad, 100 millones de bibliotecas de ataque y 150K bibliotecas de exploits.
- **Explotaciones de vulnerabilidad** RidgeBOT admite varios modos de ataque que satisfacen las diferentes necesidades de los clientes, verifica automáticamente la eficacia de los hallazgos de vulnerabilidad y garantiza que los resultados de las pruebas sean precisos, confiables y utilizables.
- **Priorización de riesgos** RidgeBOT visualiza la cadena de eliminación y cuantifica los riesgos en función de múltiples factores, dando a las organizaciones una idea clara de en qué centrarse primero.

Descubrimiento de activos: Basado en técnicas de rastreo inteligente y algoritmos de huellas digitales, descubra amplios tipos de activos de TI: IP, dominios, hosts, SO, aplicaciones, sitios web, complementos y dispositivos de red.

Minería de vulnerabilidades: Utilice 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 un entorno limitado inteligente para simular ataques del mundo real con kits de herramientas. Recopile más datos para un ataque adicional en una etapa posterior a la violación.

Priorización de riesgos: Cree automáticamente una vista analítica, visualice una cadena de interrupción y muestre el guion de un hacker. Mostrar resultados de piratería como datos y privilegios escalados de los objetos comprometidos.

Arquitectura del Sistema de RidgeBOT

El sistema RidgeBOT está diseñado en una estructura en capas. Hay un total de seis capas: una capa de recopilación, una capa de datos, una capa de algoritmo, una capa de extracción, una capa cognitiva y una capa de servicio. Cada capa sirve a su capa superior y la hace funcional.

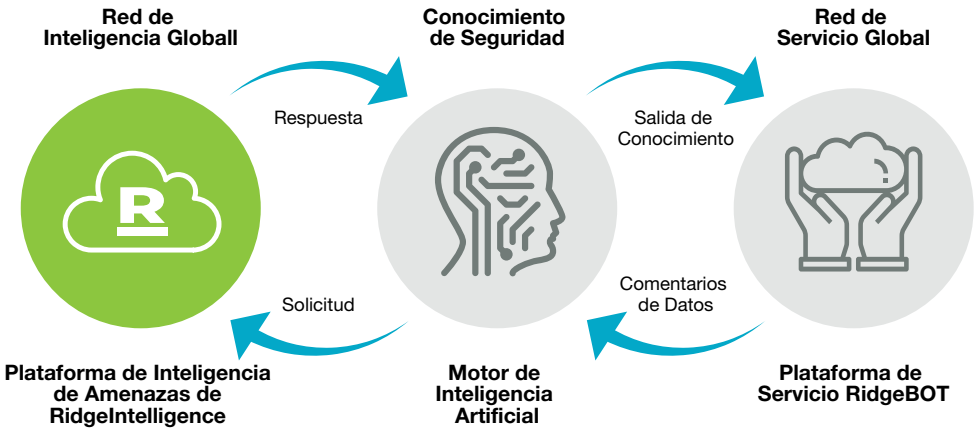
- **Capa de recopilación**: Importa datos de inteligencia de amenazas de la Plataforma de inteligencia de seguridad de Ridge o bases de conocimiento de terceros.
- **Capa de datos**: La capa de datos recopila datos de los sistemas comerciales que se van a probar. Rotula y analiza los datos combinándolos con la inteligencia de amenazas.
- **Capa de algoritmo**: La capa de algoritmo proporciona una variedad de algoritmos de inteligencia artificial para construir modelos para activos, amenazas, ataques y muchos otros.
- **Capa de extracción**: La capa de extracción utiliza varios modelos que se crean a partir de la capa de algoritmo para identificar huellas digitales y vulnerabilidades de los objetos. Esta capa planifica cómo atacar y explotar bajo la guía de la "Base de conocimientos de expertos."
- **Capa cognitiva**: La capa cognitiva alimenta los nuevos aprendizajes de un ataque exitoso al mapa de conocimiento de RidgeBOT y completa el perfil de un sistema objetivo. Este ciclo de retroalimentación evoluciona la plataforma de RidgeBOT.
- **Capa de servicio**: La capa de servicio visualiza el resultado de la prueba con gráficos fáciles de usar. Por ejemplo, el Puntaje de riesgo cuantificado ayuda a los clientes a priorizar problemas urgentes, y la vista Cumplimiento de seguridad ayuda a los usuarios a cumplir con las regulaciones de parches. En el modo de Validación de seguridad continua, RidgeBOT decide si se necesitan pruebas de validación repetidas o iterativas sobre la marcha. Una vez que se activa la condición predefinida, el sistema informático programa un subproceso para reiniciar la tarea desde el principio: la capa de recopilación.

Capa de Servicio	Cuantificación de Riesgos	Cumplimiento de Seguridad	Validación Continua de Seguridad	
Capa de Cognitiva	NLP	Mapa de Conocimiento	Retrato Objetivo	
Capa de Extracción	Huella Dactilar	Vulnerabilidad	Método de Explotación	Método de Detección
Capa de Algoritmo	Aprendizaje Automático	Aprendizaje Profundo	Aprendizaje Aumentado	
Capa de Datos	Recopilación de Datos	Etiquetado de Datos	Análisis de los Datos	
Capa de Colección	Plataforma de Inteligencia del Top de Amenazas	Plataforma de Inteligencia de Amenazas de Terceros		

Plataforma Inteligente de RidgeSecurity

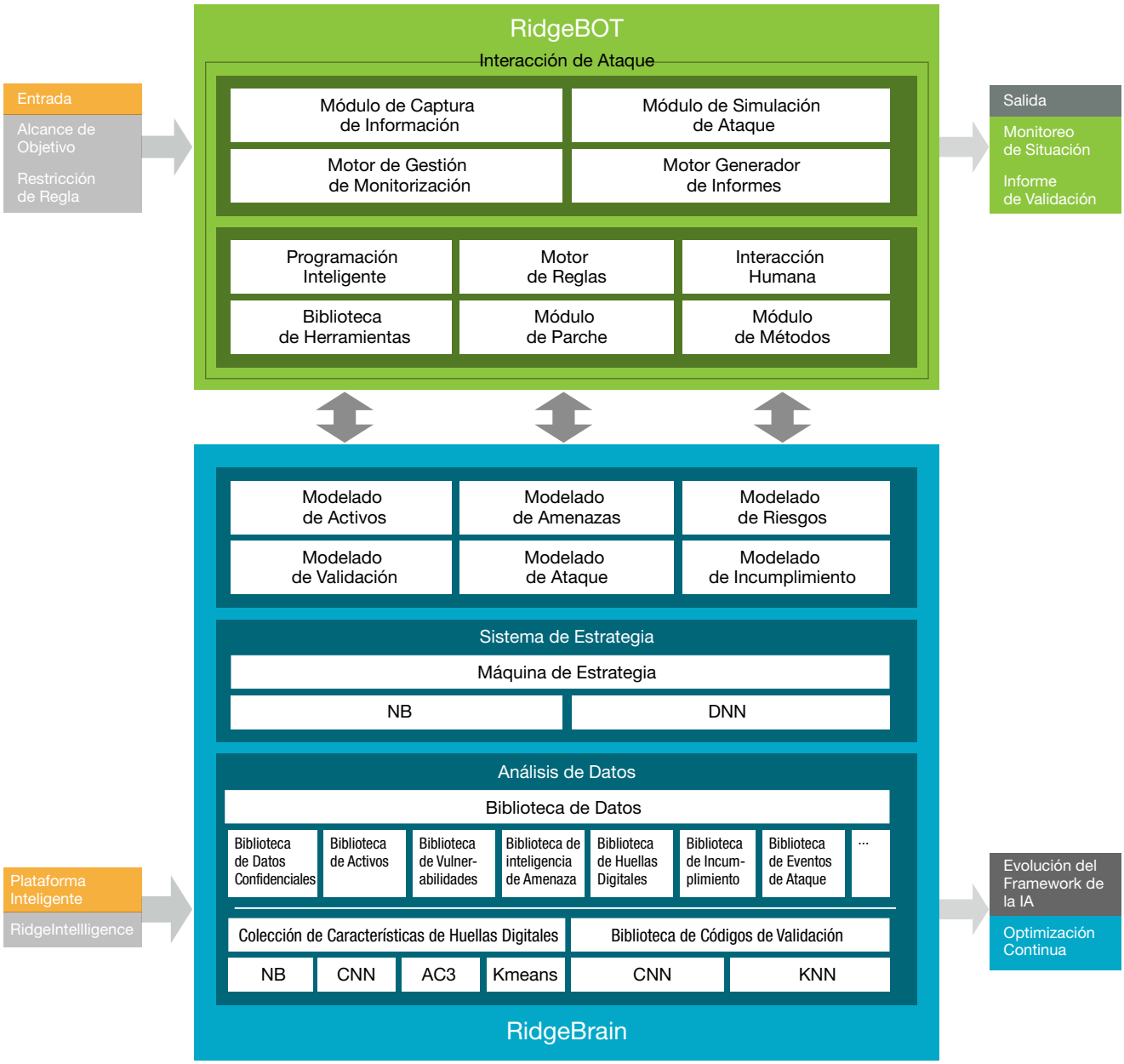
Plataforma de Backend

- **RidgeIntelligence-Plataforma de Inteligencia de Amenazas**: Una red patentada con nodos que se implementan en todo el mundo para recopilar información de amenazas y malwares en tiempo real y eventos de incumplimiento.
- **RidgeBrain-Motor de Inteligencia Artificial**: Un centro de comando central para la toma de decisiones. Es un sistema de aprendizaje profundo que construye el mapa de conocimiento multidimensional y de polimorfismo de RidgeSecurity basado en la información recopilada de la plataforma de Inteligencia. Planea qué camino tomar, qué método usar y qué secuencia seguir. Exporta su "conocimiento" de seguridad y sus decisiones a Ridge Service Platform para que las ejecute.
- **RidgeBOT-Plataforma de Servicio**: La plataforma de servicio Ridge es el brazo de ejecución, RidgeBOT, es el robot de validación de seguridad. Implica y lanza implacablemente ataques del mundo real y muestra cómo se explota una vulnerabilidad y sus consecuencias.



Marco de Aprendizaje Automático

RidgeBrain presenta numerosos algoritmos de aprendizaje automático en diversas tareas, incluidos los algoritmos de reconocimiento de imágenes (como CNN, KNN, etc.); reconocimiento de funciones y algoritmos de clasificación (como NB, CNN, A3C, KMeans, etc.); y algoritmos de toma de decisiones (NB, DNN, etc.). Es compatible con una amplia gama de escenarios mediante el uso de combinaciones de algoritmos.



Diferencias de RidgeBOT

Mayor Precisión, Más Descubrimientos

RidgeBOT, construido con una de las bases de datos de exploits más grandes del mundo, adopta los hallazgos de la comunidad abierta, la inteligencia de terceros, así como la investigación global de RidgeSecurity. RidgeSecurity ha desplegado una gran cantidad de nodos globales, especialmente en la región donde los ataques son prolíficos. Además de su red de inteligencia global, la plataforma RidgeBOT admite la integración con cualquier sistema de inteligencia de terceros a través de API.

RidgeBOT está impulsado por RidgeBrain: Un sistema experto inteligente con aprendizaje automático patentado y reconocimiento de funciones, y algoritmos de IA. Con algoritmos de reconocimiento de imágenes y técnicas de piratería, RidgeBOT evita de forma inteligente las comprobaciones de seguridad, obtiene credenciales y obtiene privilegios escalados al igual que un pirata informático experimentado. Además, guiado por su mapa de conocimiento, RidgeBOT puede lanzar ataques sofisticados como ataques de objetivos asociados, movimientos laterales y vulnerabilidades conjuntas de vulnerabilidad para lograr penetración de múltiples capas y ataques iterativos en objetivos y activos de TI asociados. Maximiza el valor de las pruebas de seguridad e informa con precisión sobre qué y cómo podría aprovecharse la vulnerabilidad.

Equipado con RidgeIntelligence y RidgeBrain, RidgeBOT no solo descubre más vulnerabilidades que las herramientas de escaneo tradicionales, sino que también logra una mayor precisión en la validación de vulnerabilidades.

Escalabilidad Ilimitada, Alta Eficiencia.

RidgeBOT proporciona servicios de monitoreo en línea 7/24 y está listo para aceptar órdenes de trabajo en cualquier momento. Admite la ejecución concurrente de múltiples tareas en ejecución continua. Su arquitectura distribuida admite escalabilidad lineal a través de clusters y equilibrio de carga. Su rendimiento se escala sin límites en la plataforma en la nube o en la implementación de máquinas virtuales.

Rango de Cobertura Más Amplio

RidgeBOT admite la identificación de activos en la más amplia gama de tipos en dominios de TI, incluidos IP, redes, hosts, aplicaciones, complementos, páginas web, sistemas operativos, dispositivos móviles y dispositivos IoT. También puede lanzar ataques desde local o global, desde Intranet, Internet o Extranet. Mientras la conexión de red sea accesible, RidgeBOT puede hacer el trabajo.

Análisis de Datos Multidimensionales, Alertas Autodefinidas

RidgeBOT realiza evaluaciones cuantitativas de múltiples tipos de activos desde dimensiones como superficies de ataque, cadena de muerte, vulnerabilidades y puntuación de riesgos, proporcionando múltiples vistas de una perspectiva de seguridad para satisfacer diferentes necesidades de varios niveles de partes interesadas.

RidgeBOT brinda a los clientes comentarios inmediatos sobre cómo sus redes responden a una amenaza específica al imitar un ataque del mundo real, lo que permite a los clientes proteger los activos de amenazas específicas y malware de manera proactiva. Los clientes pueden configurar alertas autodefinidas para informarse una vez que se desencadena una condición para que puedan estar al tanto de los eventos de seguridad que les conciernen. Los clientes también pueden integrar a la perfección esta parte de las capacidades de RidgeBOT en su infraestructura existente.

Escenarios de Implementación

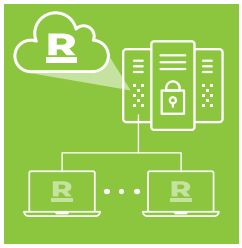
Hay tres formas de implementar RidgeBOT: modo SaaS, modo VPN o modo local.

Modo SaaS

RidgeSecurity ofrece validación de seguridad como un servicio desde su plataforma en la nube. Los clientes pueden suscribirse a su servicio y usarlo según sea necesario.

Modo VPN

RidgeSecurity La plataforma de nube RidgeBOT SaaS admite una opción de configuración de red privada virtual (VPN). Los usuarios se conectan a la plataforma SaaS de RidgeBOT a través de túneles VPN designados e inician el servicio de validación de seguridad en sus redes y sistemas. La plataforma en la nube RidgeBOT SaaS también admite el uso combinado de los modos SaaS y VPN.



Modo Local

Debido a las normas o regulaciones de seguridad, el acceso remoto a través de la plataforma en la nube o el túnel VPN no está permitido, o los sistemas específicos de negocios críticos tienen acceso restringido desde una red externa. En este escenario, RidgeSecurity proporciona implementación local. El sistema RidgeBOT puede ofrecerse en un dispositivo de hardware especializado o como una imagen de software para ejecutarse en cualquier máquina virtual con servidores en las instalaciones.

El dispositivo de hardware RidgeBOT o la imagen de software están precargados con la base de datos de Inteligencia RidgeThreat y los algoritmos RidgeBrain. Con una licencia comprada, se activa el dispositivo de hardware o la imagen virtual.

El sistema RidgeBOT se implementa en la ubicación especificada por el cliente y con una configuración aprobada. Se conecta a la red de TI del cliente con la autorización correspondiente.

Uno o varios dispositivos de hardware / máquinas virtuales forman la plataforma RidgeBOT, que realiza varias tareas de validación de seguridad en función de las necesidades del usuario.

CASO DE ESTUDIO

Servicios Financieros

Perfil de Cliente

La organización es un eje central en el que se conectan varios bancos a través de interfaces de confianza mutua. Se completan transacciones de pago masivas todos los días. Sus sistemas comerciales contienen una gran cantidad de información confidencial de los usuarios, y muchos de ellos están calificados como un sistema altamente seguro. Los sistemas comerciales evolucionan continuamente con desarrollos ágiles; Se requiere validación de seguridad antes de que cada sprint se conecte. El oficial de seguridad de la organización está bajo una presión tremenda, ya que varias agencias reguladoras realizan inspecciones de seguridad en sus sistemas con regularidad, y perderá su trabajo si se descubre una vulnerabilidad de alto riesgo y no se la atiende a tiempo.

Requisitos Principales del Cliente

Servicio a pedido y de alta disponibilidad para monitorear y validar continuamente su postura de seguridad, según lo estipulado por las reglamentaciones.

1. Servicio a pedido y de alta disponibilidad para monitorear y validar continuamente su postura de seguridad, según lo estipulado por las reglamentaciones.
2. El sistema debe configurarse fácilmente hacia diferentes objetivos para servir a múltiples departamentos y satisfacer diferentes niveles de partes interesadas.
3. No pueden permitirse ninguna fuga de datos. Esta organización está obligada a proteger la información confidencial de sus usuarios. Por lo tanto, requiere un sistema de servicio que evite estrictamente cualquier pérdida de datos.

Solución RidgeSecurity

La organización eligió implementar la plataforma de hardware RidgeBOT64 en las instalaciones con el servicio profesional de RidgeSecurity. Un consultor senior de seguridad de RidgeSecurity realizó pruebas de penetración e informó el resultado con sugerencias de corrección.

Beneficios del Cliente

La solución RidgeBOT beneficia al cliente de las siguientes maneras:

1. Los servicios basados en la plataforma de RidgeBOT pueden estar “de guardia” 7/24. Los clientes pueden realizar pruebas y ejecutarlas en cualquier momento con monitoreo continuo. Y, con los algoritmos de aprendizaje automático inteligentes integrados, RidgeBOT profundiza para descubrir más problemas potenciales que otros sistemas utilizados antes. Maximiza el valor de la prueba. Su enfoque de evolución automática se mantiene al día con el cambio del panorama de seguridad y el entorno de TI de los clientes. Ofrece pruebas de alta calidad con consistencia.
2. RidgeBOT es fácil de configurar. Su usabilidad y escalabilidad lo hacen adecuado para que esta gran organización lo adopte a través de toda la empresa. El programa de prueba basado en máquina de RidgeBOT siguió un proceso definido y generó un informe estandarizado con diferentes niveles de detalles y desde múltiples perspectivas. La consistencia del informe en los formatos y las diversas opciones en los contenidos facilitaron las conversaciones entre organizaciones y diferentes niveles de partes interesadas.
3. Los datos estuvieron en control total durante la prueba; No ocurrió ninguna pérdida. RidgeBOT evita la pérdida de datos:
   - Mantuve un registro completo durante la prueba. RidgeBOT registró cada paso durante la prueba y almacenó la información en una base de datos disponible para auditoría. Cada operación fue rastreable y puede analizarse a fondo.
   - RidgeBOT se instaló en un entorno físico seguro y controlado designado por el cliente. Durante la prueba, la plataforma RidgeBOT fue la única entrada que se conectó a la red del cliente; Toda la información y los datos se registraron y almacenaron en un servidor RidgeBOT. El servidor RidgeBOT residía en un área física segura y tenía el control total del cliente.
   - RidgeBOT es una plataforma patentada; RidgeSecurity tiene control total sobre cómo funciona. Por lo tanto, RidgeSecurity puede asegurar al cliente que no hay conexión más allá de la premisa del cliente y que los datos son seguros.

CASO DE ESTUDIO

Servicios de Seguros

Perfil de Cliente

Algunas de las empresas de esta compañía de seguros utilizan aplicaciones basadas en la web que se ofrecen a través de Internet. Se enfrentaban a varios desafíos en ciberseguridad antes de usar RidgeBOT:

1. Su infraestructura de seguridad era bastante débil; No se estableció un sistema de defensa completo.
2. Carecían de personal de seguridad: solo “unas pocas manos en el equipo de seguridad.”
3. Su equipo de seguridad estaba bajo una presión de tiempo extrema cuando había nuevas actualizaciones y actualizaciones de software. Y es fácil imaginar que tales lanzamientos son bastante frecuentes.

Objetivo Comercial

Para superar los desafíos anteriores, el cliente necesitaba alcanzar los siguientes objetivos con el servicio de validación de seguridad:

1. Minimizar los esfuerzos de mitigación haciendo los mejores esfuerzos antes de que se lance su software. La prueba abarcará tanto la amplitud como la profundidad.
2. Minimizar la carga de trabajo de su personal de seguridad.
3. Un buen ROI que equilibra la inversión y el rendimiento.

Solución RidgeSecurity

El cliente implementó el RidgeBOT en modo SaaS. La prueba se realizó a través de Internet, pero todo el proceso fue iniciado, rastreado, visto y luego terminado por el equipo de seguridad del cliente. Con el modo SaaS de RidgeBOT, el servicio se puede solicitar y ejecutar cuando sea necesario.

Beneficios del Cliente

Como la plataforma está basada en la nube, esto ha satisfecho al cliente con la comodidad de uso y el alto costo-rendimiento. Eso presentó un gran retorno de la inversión. RidgeBOT redujo los esfuerzos requeridos por el equipo de seguridad del cliente al automatizar todo el proceso de prueba, brindando muchas funciones fáciles de usar, como una nueva prueba con un solo clic e informes generados automáticamente con estrategias de corrección. RidgeBOT realizó ataques iterativos de varias capas que aseguraron una inspección exhaustiva de cualquier software antes de su lanzamiento al mercado.

CASO DE ESTUDIO

Manufactura

Perfil de Cliente

El cliente es una marca líder de electrodomésticos. Cuenta con múltiples plantas y líneas de productos en diferentes sitios. En sus fábricas modernas, la programación, la planificación y la gestión de suministros han hecho que sus sistemas de TI sean cada vez más complejos. Sin embargo, la seguridad no era una prioridad en el pasado y ahora el riesgo cibernético es alto.

Prioridad Máxima del Cliente

1. Crear capacidades de validación de seguridad interna en lugar de utilizar servicios de seguridad externos temporales.
2. Ser capaces de identificar una amplia gama de activos, incluidos los sistemas de TI, dispositivos móviles y dispositivos IoT. Además, deben inspeccionar una gran cantidad de activos en un corto período de tiempo.
3. Proporcionar validación precisa y remediación efectiva

Solución RidgeSecurity

El cliente implementó una solución combinada de RidgeScan y RidgeBot128 en su intranet corporativa. A través de la interfaz de gestión unificada, RidgeScan y RidgeBot pueden coordinar la distribución de tareas. Trabajando así en paralelo y racionalizando las vulnerabilidades de la minería y la validación. La inspección del gran número de activos del cliente se completó a tiempo.

Company Profile

RidgeSecurity está transformando la validación de seguridad con RidgeBOT, un robot inteligente de validación de seguridad. RidgeBOT se modela utilizando técnicas utilizadas literalmente por millones de hackers que penetran en los sistemas. Cuando los RidgeBOT se implementan dentro de un sistema son implacables en su búsqueda para localizar, explotar y documentar sus hallazgos. Trabajan dentro de un alcance definido y se replican instantáneamente para abordar estructuras altamente complejas. RidgeSecurity permite a las empresas y equipos de aplicaciones web, DevOps, ISV, gobiernos, atención médica, educación o cualquier persona responsable de garantizar la seguridad del software, probar sus sistemas de manera rentable y eficiente.

Ridge Security Technology Inc.
www.ridgesecurity.ai