

GA4-220501095-AA2-EV02 INFORME DE ENTEGRABLES PARA EL PROYECTO
DE DESARROLLO DE SOFTWARE

JULIANA VALENTINA GAVIRIA MORENO

CAROLINA MEJIA RAMOS

SEBASTIAN PICO ARRIETA

CRISTIAN NEIR QUIROGA ARIZA

JORGE DARIO AGUDELO IDARRAGA

TECNOLOGO ANALISIS Y DESARROLLO DE SOFTWARE

FICHA. 2758290

FREDY CASTELLANOS AVILA

AÑO 2024

INTRODUCCIÒN

En el desarrollo del proyecto nos enfocamos en crear un software que sea intuitivo, amigable, comprensivo, que maneje una base de datos que sea actualizada, que permita a empresas y usuarios independientes, acceder a la información precisa del consumo de internet y la cantidad del mismo, calidad y velocidad también la facturación, a si el cliente puede manejar su economía de una mejor manera, para esto el software ofrece comparar los valores con otras empresas prestadoras de servicios, para que el cliente pueda utilizar una herramienta que le permita elegir el operador que más se ajuste a sus necesidades, y no solo esto que además le permita ahorrar dinero ya que podrá escoger siempre la mejor opción basado en datos reales. Será necesario generar alianzas estratégicas con las empresas prestadoras, para que la información sea absolutamente confiable y precisa, y los clientes estén satisfechos con el software. Este tipo de funciones son muy apetecidas en el mundo moderno, ya que cada vez el uso del internet es más grande e indispensable en los hogares, empresas, etc. Por esto nuestro proyecto tiene una oportunidad muy buena en el mercado, por lo que se ofrece a las empresas y personas naturales siempre con el fin de satisfacer las necesidades del cliente. Nuestro software lo ayudara a encontrar el mejor proveedor de internet en su área al comparar la velocidad el precio y cobertura de cada suministrador. De esta manera, puede estar seguro de que está tomando la mejor decisión para sus necesidades de consumo de internet

ALCANCE

El software de selección de operadores de internet tiene el potencial de revolucionar la industria del internet, al permitir a los usuarios seleccionar el mejor proveedor de servicios de su área, esta herramienta es demasiado útil para buscar la mejor opción, al ingresar su ubicación, el software busca y compara los diferentes proveedores de internet disponibles y muestra los resultados en una interfaz fácil de usar.

- Busca y compara los diferentes proveedores de internet en su área.
- Muestra los planes y precios de cada proveedor para que puedas comparar y elegir el mejor para ti.
- Proporciona información detallada sobre la velocidad de internet la cantidad la cobertura y otros detalles importantes.

Es muy importante el alcance que tiene en la juventud ya que este software estará disponible para todo tipo de persona en general, pero basado en que las nuevas generaciones son las que más consumen internet, serán las que lo utilicen mayormente, debido al gran crecimiento de la tecnología, gracias a esta podremos dar a nuestros usuarios, un análisis detallado del rendimiento y la velocidad de descarga y carga, la tendencia y otros factores que afecten la calidad del servicio, además te proporcionara consejos para mejorar tu conexión a internet, de esta forma esperamos que puedan encontrar el operador de internet o servicios que sea más adecuado para nuestros cliente

Formulación de los requisitos Requisitos de usuario:

1. Rendimiento y estabilidad: El software debe ser capaz de manejar grandes volúmenes de tráfico de red sin afectar y degradar el rendimiento. Además, debe ser capaz de escalar para adaptarse en redes en crecimiento y entornos empresariales mas complejos
2. Actualizaciones de firmas y reglas: El software debe proporcionar actualizaciones regulares de firmas y reglas de detención para mantenerse al día con las ultimas amenazas de seguridad. Estas actualizaciones deben ser fáciles de aplicar y se deben poder realizar de manera automática o manual.
3. Detención y prevención de intrusiones: El software debe de detectar y prevenir intrusiones en la red. Debe contar con algoritmos y técnicas avanzadas de detención para identificar actividades sospechosas o maliciosas en tiempo real.
4. Alerta y notificaciones: El software debe proporcionar alertas y notificaciones inmediatas una intrusión o actividad sospechosa. Estas alertas deben ser claras y comprensibles, y preferiblemente se deben poder enviar a través de múltiples canales, como correo electrónico, SMS o sistemas de mensajería.
5. Análisis de tráfico en tiempo real: El software debe de analizar el tráfico en tiempo global e individual, y realizar un monitoreo continuo de los patrones de tráfico para identificar cualquier anomalía. Esto incluye la capacidad de examinar los paquetes de datos y los protocolos utilizados en la red
6. Facilidad de uso: El software debe ser fácil de instalar configurar y utiliza. Debe contar con interfaz intuitiva y bien diseñada que permita a los usuarios administrar controlar el sistema de manera efectiva incluso sin tener un profundo conocimiento en sistemas
7. Informes y análisis: El software debe ser capaz de generar informes detallados sobre las actividades de intrusión, los eventos de seguridad y las medidas de prevención tomadas. Estos informes deben personalizables y fáciles de entender y deben proporcionar datos relevantes para evaluar la eficiencia del sistema de ISP.
8. Administración centralizada: El software de ISP debe contar una interfaz de administración centralizada configurar y administrar todas las instalaciones de IPS en la red desde un único punto de control, Esto facilita la configuración, implementación y monitoreo del sistema
9. Integración con otros métodos de seguridad: Es importante que el software de ISP puede integrarse con otros métodos de seguridad, como firewalls sistemas de detención de intrusiones (IDS) y sistemas de gestión de seguridad (SIEM). Esto permite una defensa en capaz más sólida y una visibilidad más completa de las amenazas de seguridad

10. Acceso la nube: El software de ISP debe contar con componentes adicionales como un sistema de base de datos y un servidor web para la interfaz de administración

Requisitos del sistema

1. Hardware

1. Procesador: Se requiere un procesador de múltiples núcleos y de alto rendimiento para manejar el análisis en tiempo real de todos los paquetes de red

2. Memoria RAM: Se recomienda tener una capacidad suficiente de memoria RAM para el procesamiento eficiente de todos los datos en tiempo real. Al menos 8GB o más, dependiendo de las necesidades y el tamaño de la red

3. Espacio de almacenamiento: Debe haber suficiente espacio de almacenamiento disponible para los registros de eventos, actualizaciones de firmas y configuraciones. El tamaño necesario dependerá del volumen del tráfico y la retención de registros requeridas

2. Sistema operativo

1. El software de ISP puede ser compatible con varios sistemas operativos, como Windows, Linux o Unix, Verifique los requisitos específicos del proveedor para determinar la compatibilidad.

3. Conectividad de red

1. Interfaces de red: El sistema de ISP requiere al menos un interfaz de red para capturar y analizar el tráfico. Es posible que se necesiten múltiples interfaces de red para monitorear y proteger diferentes segmentos de la red

2. Ancho de banda: El rendimiento del software de ISP dependerá del ancho de banda de la red puede manejar el trafico sin restricciones para evitar cuello de botella.

Requerimientos Funcionales

1. Análisis y protocolos de tráfico: El software debe tener la capacidad de analizar y comprender diferentes protocolos de red (como TCP/IP, UDP, ICMP, etc.) y examinar los paquetes de datos para identificar posibles amenazas. También debe realizar un análisis en tiempo real de tráfico para detectar anomalías.

2. Prevención de intrusiones: Además de detención, el software debe ser capaz de tomar medidas para prevenir las intrusiones bloquear los intentos de ataques. Esto puede incluir la aplicación de reglas de seguridad, filtrado de paquetes, bloqueo de direcciones IP y otras técnicas de mitigación.

3. Gestión de políticas de seguridad: El software debe ofrece funcionalidades para administrar y configurar las políticas de seguridad, lo que incluye definir reglas de bloqueo, establecer niveles de severidad de alertas

4. Gestión de informes y registros de eventos El software debe ser capaz de generar informes detallados y registro de eventos que muestren las actividades de instrucción

detectadas, los eventos de seguridad, las acciones preventivas tomadas etc. Estos informes y registros son fundamentales para el monitoreo, auditoria y el análisis de la seguridad de la red

5. Interfaz de usuario intuitiva: El software debe contar con una interfaz de usuario intuitiva fácil de usar que permita a los administradores configurar, monitorear y analizar el sistema de ISP de manera eficiente. La interfaz debe ser accesible para usuarios con diferentes niveles de conocimiento técnico.

6. Estabilidad y rendimiento: El software escalable para adaptarse a redes de diferentes tamaños. Además, debe tener un rendimiento optimo, garantizado un procesamiento rápido y eficiente de los datos de la red

7. Detención de intrusiones: El software debe tener capacidades para detectar actividades de intrusión o compartimientos maliciosos en la red ya sea mediante la detención de patrones de trafico sospechosos, la identificación de intentos de ataques conocidos o la detención de anomalías en el trafico

Requisitos no funcionales

1. Eficiencia de recursos. El software debe utilizar los recursos del sistema (procesador, RAM, almacenamiento) de manera eficiente y optimizada. Debe evitar consumir recursos innecesarios para garantizar un rendimiento optimo y reducir los costos de hardware asociados.

2. Mantenibilidad: El software debe ser fácil de mantener y actualizar. Debe tener una arquitectura modular y bien estructurada que permita realizar cambios y mejoras sin afectar otras partes del sistema. Además, debe contar con una documentación clara y completa para facilitar el mantenimiento por parte de los desarrolladores y administradores.

3. Disponibilidad: El software debe ser altamente disponible, lo que implica tener una arquitectura robusta y mecanismo de rendimiento para evitar puntos únicos de falla. Debe contar con características de conmutación por error y recuperación automática en caso de fallos.

4. Seguridad: Dado que el software de ISP juega un papel crucial en la protección de la red, debe cumplir con altos estándares de seguridad. Debe ser resistente a los ataques y protegerse contra la explotación por parte de atacantes. Además, debe cumplir con las regulaciones y normativas de seguridad relevantes.

5. Rendimiento: El software de ISP debe ser capaz de manejar grandes volúmenes de trafico de la red sin afectar significativamente el rendimiento del sistema, Debe tener una baja latencia y un procesamiento eficiente de los paquetes de datos. 6. Estabilidad: Debe adaptarse a redes en crecimiento y permitir el aumento del número de dispositivos monitoreados. Debe ser capaz de manejar un aumento en el volumen del trafico sin degradar el rendimiento