Introducción al proyecto

Este documento trata acerca del software CHARLYN, podrán encontrar todo lo relacionado al software respecto a información empresarial, además de poder ver información relevante sobre pláticas y eventos en los que CHARLYN ha participado de manera activa.

Objetivos

Objetivo general

- Desarrollar un software de protección contra amenazas o virus cibernéticos que sea fácil de usar para los usuarios.

Objetivos específicos

- Debe tener un Ui/Ux intuitivo.
- Debe permitir administrar la red a la que se instale.
- Debe monitorear todo lo que sucede y notificarle al usuario de eventos y amenazas de seguridad.

Alcances

Protección de Redes: Ofrece protección para redes domésticas o empresariales contra amenazas cibernéticas como malware, virus, phishing, etc.

Monitoreo Continuo: Supervisa constantemente la actividad de la red en busca de comportamientos sospechosos o actividades no autorizadas.

Interfaz Amigable: Proporciona una interfaz fácil de usar, diseñada para personas sin experiencia en redes o seguridad informática.

Gestión de Dispositivos: Permite administrar todos los dispositivos conectados a la red, facilitando su configuración, control y supervisión.

Seguridad para Usuarios Novatos: Ofrece herramientas simples para mantener segura la red y los datos, incluso para aquellos usuarios con poca experiencia en seguridad informática.

Administración de Servicios Internos: Permite gestionar los servicios activos en la red, facilitando su configuración y asegurando su funcionamiento adecuado.

Notificaciones de Seguridad: Informa a los usuarios sobre posibles amenazas o problemas de seguridad a través de alertas claras y comprensibles.

Limitaciones

Complejidad de Amenazas Avanzadas: Puede tener limitaciones para detectar y mitigar amenazas cibernéticas altamente sofisticadas o avanzadas.

Dependencia de Actualizaciones: La eficacia del software depende de actualizaciones regulares para enfrentar nuevas amenazas y vulnerabilidades.

Requerimientos de Conectividad: Puede necesitar una conexión a Internet constante para recibir actualizaciones de seguridad y funcionar correctamente.

Escalabilidad Limitada: Puede tener dificultades para gestionar redes muy grandes o complejas con múltiples dispositivos y configuraciones avanzadas.

Requisitos de Hardware: Podría requerir ciertos requisitos mínimos de hardware para funcionar de manera óptima, lo que puede limitar su uso en ciertos dispositivos más antiguos.

Soporte Limitado para Personalización Avanzada: Las opciones de configuración avanzada podrían ser limitadas para usuarios con experiencia en redes y seguridad que buscan personalización detallada.

Justificación

Actualmente la tecnología ha estado avanzando a gran velocidad y con ella también la cantidad de hackers y virus que hay en la web y ahora con la introducción de la Inteligencia Artificial, los peligros son aún mayores, las empresas grandes pueden contratar expertos en ciberseguridad y mantenerse protegidos en su día a día, pero los hogares y negocios que no cuentan con el dinero o no saben que la probabilidad de ser hackeado es más grande cada día no tienen manera de defenderse, y los antivirus actuales son muy caros y solo funcionan por equipo, además no protegen el modem quien es también parte importante y debe ser protegido.

CHARLYN es un software de protección y monitoreo de redes, el cual está diseñado para ser amigable y simple de usar, de manera que personas sin experiencia en redes y temas de seguridad puedan mantener seguras sus casas o negocios, además de poder administrar todos los dispositivos conectados a su red y servicios internos activos.

Obtención de requerimientos

Entrevistador: Buenos días, ¿cómo ha estado? Me alegra tener la oportunidad de hablar sobre sus necesidades en seguridad informática. Para empezar, ¿podría contarme un poco sobre su negocio y las preocupaciones actuales que tiene en cuanto a la seguridad cibernética?

Cliente: Buenos días, gracias por la oportunidad. Claro, soy el director de una empresa de mediano tamaño que maneja información sensible de nuestros clientes. Nuestra principal preocupación radica en la protección de esta información contra posibles amenazas cibernéticas, como malware, phishing y otras vulnerabilidades que puedan afectar la integridad de nuestros datos y la continuidad de nuestras operaciones.

Entrevistador: Entiendo, la protección de la información es crucial. ¿Qué tipo de solución en seguridad informática está buscando? ¿Hay algún aspecto específico que considere vital para el funcionamiento óptimo de su negocio?

Cliente: Claro, necesitamos una solución que no solo detecte y mitigue amenazas cibernéticas, sino que también monitoree continuamente nuestra red para identificar comportamientos sospechosos y actividades no autorizadas. Además, es fundamental que la interfaz sea amigable, ya que no todos en nuestro equipo tienen experiencia en seguridad informática. También, nos gustaría poder administrar fácilmente todos nuestros dispositivos conectados y supervisar los servicios activos en nuestra red para garantizar su correcto funcionamiento.

Entrevistador: Entendido, esos aspectos son cruciales para mantener la seguridad. ¿Hay algún otro punto que considere esencial para su empresa?

Cliente: Por supuesto, la seguridad y la confiabilidad del software son fundamentales, así como su eficiencia en el uso de recursos. Además, necesitamos que esté disponible en todo momento y sea fácilmente compatible con nuestros dispositivos y configuraciones existentes.

Entrevistador: Entiendo completamente. Basándome en lo que me ha compartido, parece que la prioridad es una solución integral que proteja sus datos, sea fácil de usar y tenga un rendimiento eficiente. Estos requerimientos son clave para garantizar la seguridad y continuidad de sus operaciones.

Cliente: Exactamente, necesitamos una solución que se adapte a nuestras necesidades y nos brinde tranquilidad en cuanto a la seguridad de nuestra información.

Entrevistador: Agradezco mucho su tiempo y la información proporcionada. Basándome en sus requerimientos, estoy seguro de que podemos ofrecerle una solución a medida que cumpla con sus expectativas en seguridad cibernética y facilidad de uso.

Requisitos funcionales

- **Protección contra amenazas cibernéticas:** El software debe ser capaz de detectar y mitigar una amplia gama de amenazas cibernéticas, incluyendo malware, virus, phishing, etc.
- **Monitoreo continuo:** El software debe monitorear constantemente la actividad de la red en busca de comportamientos sospechosos o actividades no autorizadas.
- **Interfaz amigable:** El software debe tener una interfaz fácil de usar, diseñada para personas sin experiencia en redes o seguridad informática.
- **Gestión de dispositivos:** El software debe permitir administrar todos los dispositivos conectados a la red, facilitando su configuración, control y supervisión.
- **Administración de servicios internos:** El software debe permitir gestionar los servicios activos en la red, facilitando su configuración y asegurando su funcionamiento adecuado.

- **Notificaciones de seguridad:** El software debe informar a los usuarios sobre posibles amenazas o problemas de seguridad a través de alertas claras y comprensibles.

Requisitos no funcionales

- **Seguridad:** El software debe ser seguro y confiable, protegiendo los datos y la infraestructura de la red.
- **Eficiencia:** El software debe ser eficiente en el uso de recursos, como la CPU, la memoria y la red.
- **Disponibilidad:** El software debe estar disponible cuando sea necesario, con un tiempo de inactividad mínimo.
- **Facilidad de uso:** El software debe ser fácil de usar, incluso para personas sin experiencia en redes o seguridad informática.
- **Soporte:** El software debe ser compatible con una amplia gama de dispositivos y configuraciones.