Equipos técnicos

- Desarrolladores de software: Un equipo de desarrolladores altamente capacitados en áreas como programación, inteligencia artificial, y ciberseguridad será fundamental para la creación, mantenimiento y mejora del software.
- Ingenieros de IA: Dado que tu software estará basado en la protección contra amenazas impulsadas por IA, necesitarás expertos en inteligencia artificial que diseñen los algoritmos capaces de detectar y neutralizar estas amenazas.
- Equipo de soporte técnico: Aunque el software será autónomo, un equipo de soporte técnico estará disponible para ayudar a resolver problemas más complejos y ofrecer asistencia a clientes empresariales.

- Infraestructura de servidores

- Servidores de almacenamiento: Necesitarás servidores robustos y escalables para almacenar los datos de los clientes (en caso de que los datos de usuario sean almacenados o procesados) y las actualizaciones del software.
- Infraestructura de nube: Dependiendo de la escala de tu producto, podrías necesitar servidores en la nube para la distribución del software, la realización de actualizaciones automáticas y el análisis en tiempo real de las amenazas cibernéticas.

- Software y herramientas de desarrollo

- Licencias de software: Algunas herramientas de desarrollo o servicios en la nube que utilices pueden requerir licencias pagas. Esto puede incluir sistemas de control de versiones (como GitHub Enterprise), plataformas de análisis de datos, o entornos de desarrollo específicos.
- Herramientas de análisis de ciberseguridad: Plataformas de análisis de vulnerabilidades, simuladores de ataques, o software para pruebas de penetración podrían ser recursos clave para garantizar que el software esté preparado para detectar amenazas avanzadas.

- Red de distribución y plataformas tecnológicas

- Plataformas de distribución de software: Como mencionamos antes, distribuir el software a través de plataformas como Google Play, Microsoft Store, o tu propia página web será crucial.
- Redes de afiliados y partners tecnológicos: Aunque no planeas tener socios clave, mantener relaciones con proveedores de infraestructura tecnológica y plataformas de marketing puede ser útil para escalar el negocio.

- Propiedad intelectual

- Patentes y derechos de autor: Si desarrollas algoritmos innovadores o métodos únicos para detectar amenazas impulsadas por IA, será fundamental protegerlos a través de patentes, marcas registradas o derechos de autor.
- Marcas y reputación: Desarrollar una marca fuerte será importante para generar confianza en el mercado. Un nombre de marca sólido y una buena reputación de seguridad pueden ser activos clave para tu empresa.

Financiamiento

- Aunque no lo mencionaste específicamente, si el proyecto requiere inversión para el desarrollo inicial o la expansión, los recursos financieros serán

cruciales. Esto podría incluir ahorros personales, fondos de inversores o incluso financiación a través de programas de concursos o premios.