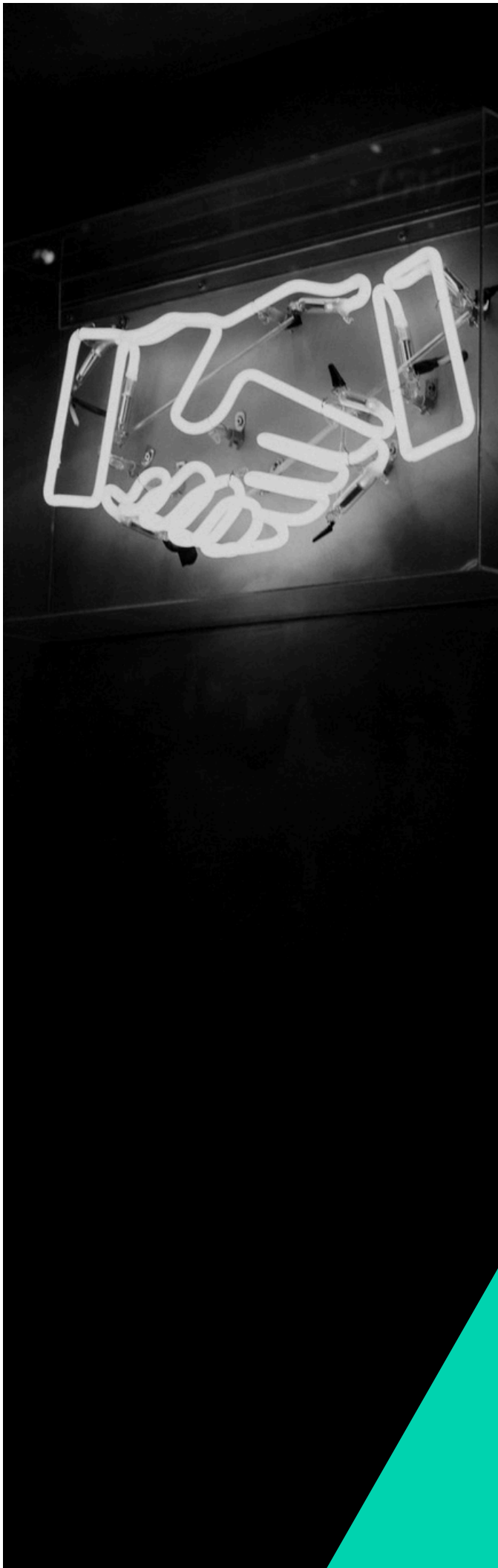
ENTHEC©

Programa de Partners



kartos©

qondar

Tabla de contenido

La red de Partners de Enthec es una parte imprescindible de nuestro modelo de negocio.

Por un lado, aumenta nuestro alcance comercial y el alcance de nuestros clientes.

Por otra parte, por las características de nuestro producto, el software de cibervigilancia, es necesario contar en nuestra red de atención al cliente con organizaciones que cuenten con los recursos para iniciar los procesos de remediación, mitigación y protección una vez detectadas las vulnerabilidades y brechas de nuestros clientes.

En ocasiones, el cliente dispone de estos recursos *in-house*, pero en la mayoría de los casos, el encargado de realizar estas tareas es un partner que le proporciona servicios de seguridad gestionada. Esto crea una relación simbiótica entre Enthec y sus partners, quienes, al incorporar el producto Enthec a sus servicios de ciberseguridad gestionada, pueden proporcionar a sus clientes una estrategia completa de cibervigilancia, que les permite descubrir y resolver incidentes imposibles de detectar con las estrategias de ciberprotección tradicionales y realizar una evaluación de riesgos de TI de terceros y la protección de personas relevantes, añadiendo valor a la oferta.

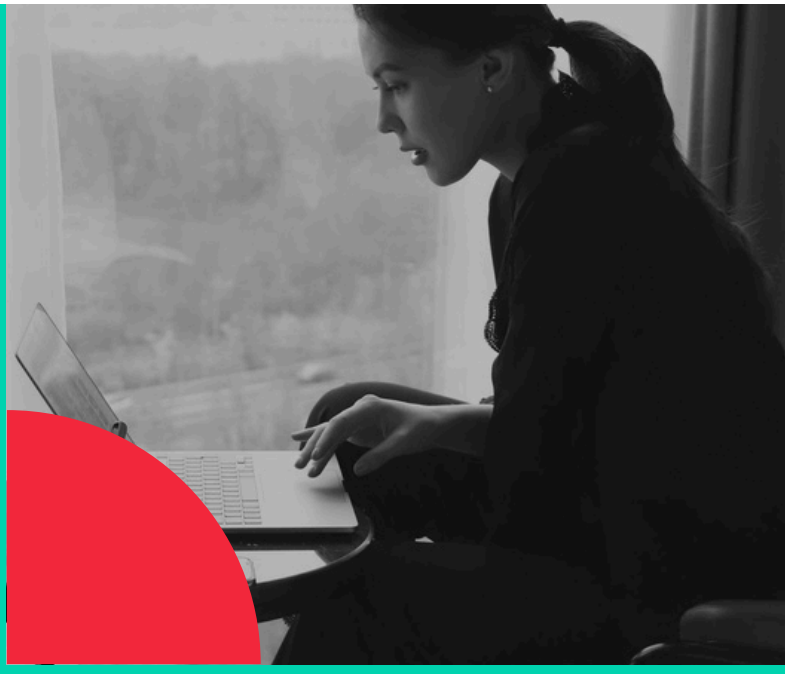
Por eso, dentro de nuestro Programa de Partners contamos dos modalidades:

Reseller Partner

Vende nuestras licencias a nuestros clientes y puede, si así lo desea, prestarles los servicios para los cuales está capacitado de acuerdo a sus capacidades e infraestructura.

MSSP Partner

Utiliza nuestra herramienta para ofrecer a sus clientes el servicio de cibervigilancia, valoración del riesgo IT de terceros y de protección online de personas relevantes dentro de su portfolio de servicios gestionados de ciberseguridad.



Enthec no tiene canales propios de venta directa o de servicios gestionados de seguridad. Por tanto, Enthec no actúa como competencia de nuestros partners en ninguna de las dos modalidades. Tanto la venta de nuestras licencias como la oferta de remediación de las vulnerabilidades detectadas o de valoración de riesgos TI de terceros se realizan al 100% a través de nuestra red de partners.

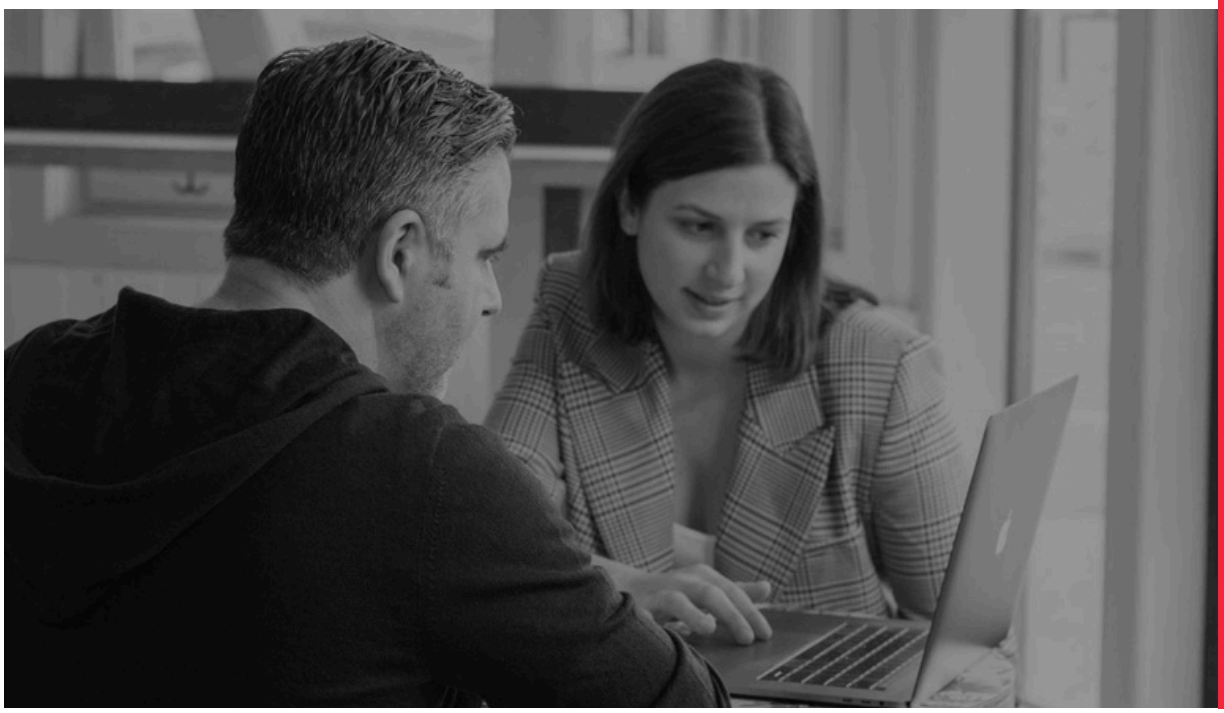
Propuesta de valor al cliente

Kartos Corporate Threat Watchbots

Kartos está formado por un ejército de Watchbotsbots diseñados explícitamente para proteger a las organizaciones que buscan en Internet, la Deep Web y la Dark Web brechas abiertas y vulnerabilidades expuestas. Kartos trabaja de manera continua 365x24x7 monitorizando y rastreando para encontrar toda la información filtrada y expuesta de la empresa cliente, ayudar a detectar las brechas de seguridad que han provocado la filtración y valorar el riesgo IT de terceros.

Qondar Personal Threat Watchbots

Qondar está formado por un ejército de Watchbots diseñados explícitamente para proporcionar a las personas información continua y en tiempo real sobre su identidad y activos digitales y las actividades en curso relacionadas con ellos en Internet, la Deep Web y la Dark Web, para que puedan controlar su seguridad en línea.



Capacidades

Ciberinteligencia

Para descubrir vulnerabilidades latentes

Localiza la información abierta y expuesta de la organización y sus vulnerabilidades en Internet, Deep web, Dark web y Redes Sociales. Campañas de phishing, fraude y estafa, CVE y salud de DNS. Contraseñas y credenciales filtradas, documentación o bases de datos.

Ciberseguridad

Para mantener seguros los activos digitales

Amplía la estrategia de ciberseguridad más allá del perímetro de TI corporativo. Protección de marca, dominio y subdominio. Protección de correo electrónico corporativo. Protección contra ransomware. Seguridad web y eliminación de amenazas.

Evaluación de riesgos de terceros

Para controlar riesgos de la cadena de valor

Controla de forma automatizada, continua y en tiempo real la información expuesta de un tercero o potencial tercero y la detección de sus brechas de seguridad, así como las enésimas críticas asociadas a las mismas.

Cumplimiento

Para cumplir con la normativa vigente

Cumplimiento corporativo y de terceros basado en datos objetivos tomados en tiempo real. ISO 27001. PCI

Cómo funciona

Para iniciar el proceso solo es necesario ingresar el dominio de la empresa que se está buscando.

La información está organizada en 11 vectores a partir de los cuales se construyen los índices de riesgo de la organización.

El administrador de la herramienta puede personalizar los usuarios autorizados y los permisos otorgados.

Una de las principales diferencias entre Kartos y herramientas similares es que no solo permite obtener información que suponga un riesgo de ciberseguridad, sino que también permite identificar robos y filtraciones de información confidencial, crítica o sensible que supongan un riesgo legal, reputacional o de propiedad intelectual que puedan suponer una pérdida de ventaja competitiva o un riesgo para el negocio.

qondar

Capacidades

- **Protección de los bienes personales:**

Cuentas bancarias, tarjetas de pago, billeteras de criptomonedas

- **Protección de las comunicaciones personales y profesionales:**

Correo electrónico, teléfonos, redes sociales

- **Protección de la reputación personal.**

Nombre y apellido, apodos, fecha de nacimiento

- **Protección contra actividades sospechosas en línea que tratan datos personales:**

DNI, tarjeta sanitaria, pasaporte, carnet de conducir

- **Protección contra el robo de identidad digital.**

Nombre y apellido, apodos, nicks sociales

- **Protección de la integridad de los perfiles personales en las redes sociales:**

LinkedIn, Facebook, X, Instagram, Telegram, TikTok

Cómo funciona

Para iniciar el trámite solo es necesario ingresar el nombre, datos y activos de la persona que se busca.

La investigación se realiza en Internet, Deep Web y Dark Web y únicamente sobre la persona que ha emitido la autorización de protección, por lo que su funcionamiento y la información obtenida cumplen estrictamente con los límites impuestos por la legislación.

El administrador de la herramienta puede personalizar los usuarios autorizados y los permisos otorgados.

Toda la tecnología utilizada por Qondar es desarrollada internamente y no depende de aplicaciones de terceros para su funcionamiento. De esta manera, los datos personales obtenidos nunca son desviados a un tercero ni salen de la plataforma y son entregados directamente al cliente.

¿Cuál es la innovación de nuestras herramientas frente al enfoque casi homogéneo actual de la Ciberseguridad?

Hoy en día, los esfuerzos de sistemas y procesos se centran en asegurar la protección del perímetro interno y de la infraestructura y verificar que dicha protección funciona. Es decir, blindar a la organización con un muro de herramientas que impidan el asalto del cibercrimen: un sistema de dudosa eficacia dados los datos, que no tiene en cuenta los riesgos de terceros, de las personas relevantes de la organización y cuya escalabilidad se complica a nivel de herramientas y costes con la entrada de nuevas tecnologías como la nube o el IoT.

Este enfoque de blindaje interno no es suficiente porque no incluye una parte esencial de cualquier estrategia de protección: la vigilancia del perímetro externo, que permite anticipar los ciberataques neutralizando la potencial ventaja que la información filtrada y expuesta proporciona a los ciberdelincuentes; detectar brechas de seguridad en el muro de blindaje interno; evaluar el riesgo de terceros; y minimizar los efectos del factor humano, el eslabón más débil de la cadena de protección.

La innovación y propuesta de valor de nuestra plataforma parte precisamente de la perspectiva opuesta a la seguridad corporativa tradicional, con una visión mucho más práctica y directa que nace del enfoque hacker de nuestra solución: observamos la organización y las personas desde fuera, como lo hace un cibercriminal.

Los ataques de penetración y fuerza bruta suelen ser fácilmente detectados y neutralizados por los sistemas de protección perimetral. Sin embargo, el problema de los ciberataques aparece cuando se diseñan y llevan a cabo utilizando información corporativa o personal que está filtrada y expuesta públicamente sin el conocimiento de las empresas y que facilita la entrada o el lanzamiento de ataques. Nuestras herramientas buscan vulnerabilidades al alcance de cualquier ciberatacante y descubren el origen de la brecha de seguridad para poder tomar las medidas de neutralización y remediación adecuadas.

De forma automatizada, continua y en tiempo real, nuestra plataforma proporciona al equipo de seguridad corporativa la información a la que de otra manera no tiene acceso, para tener una visión 360º de la situación y poder diseñar una estrategia de protección y defensa completa y adecuada.

Propuesta de valor al partner

¿Qué valor debe aportar un fabricante o un aliado tecnológico a un partner?

- Contribuir a brindar más y/o mejores servicios facturables a sus clientes.
- Ayudar a retener a los clientes existentes.
- Incorporación al portafolio que no suponga una gran inversión ni en términos económicos ni en términos de tiempo, curva de aprendizaje o formación.

- Nuestra plataforma permite al cliente o partner encontrar vulnerabilidades corporativas o personales, brechas de seguridad de terceros e información filtrada y expuesta de forma desconocida por empresas que sólo nuestras herramientas pueden encontrar. Su singularidad facilita tanto la venta de licencias como la aportación de valor a un portfolio de servicios de ciberseguridad, permitiendo la inclusión en la oferta de servicios de remediación, mitigación, protección y evaluación de riesgos de terceros no contemplados, con el consiguiente incremento de facturación.
- Nuestra plataforma es un sistema automatizado que funciona de forma continua 365x24x7 integrándose con el sistema de gestión, lo que permite la recepción de alertas inmediatas cada vez que se produce una incidencia. Sólo Kartos, Qondar y sus partners pueden ofrecer y proporcionar esta información de esta forma y con esta frecuencia.
- Nuestra plataforma proporciona la información a través de una interfaz diseñada en un formato que va desde aquellos con conocimientos fundamentales de Ciberseguridad hasta aquellos que pueden entender la parte más técnica y tomar las medidas de remediación necesarias para resolver los problemas. Además, Kartos y Qondar pueden integrarse a través de APIs en los sistemas de los clientes, SOCs y otros sistemas de gestión de socios de una manera sencilla, haciendo que la producción sea cuestión de minutos.

¿Por qué ser parte del Programa de Partners de Enthec?

Por la diferenciación: La incorporación de Kartos y Qondar al catálogo de soluciones y servicios de Ciberseguridad proporciona una ventaja competitiva convincente y una diferenciación en la innovación de las ofertas de nuestros Partners frente a sus competidores.
Por el alcance: Nuestra plataforma funciona 24/7 y transfiere información sobre amenazas en tiempo real, permitiendo a nuestros Partners o sus clientes tomar acciones de remediación inmediatas cuando sea necesario y generar confianza.
Por la simplicidad: Nuestra plataforma es una plataforma no intrusiva, automatizada, con un diseño atractivo, fácil de usar y que además proporciona a nuestros Partners o sus clientes diferentes tipos de informes adaptados al nivel de conocimientos técnicos de cada destinatario.
Por el apoyo: Estamos siempre al lado de nuestros Partners a través de nuestra excelente capacidad técnica y Servicio de soporte de ventas, brindándoles soporte técnico, materiales de marketing y ventas, capacitación y asistencia permanente.

Beneficio	Descripción
Nueva fuente de ingresos	Ofrecer Kartos™/ Qondar™ como marca blanca o Servicios de marca compartida para ampliar su cartera de seguridad
Integración Sencilla	Basada en API, multi-tenant, compatible con los principales entornos SOC/SIEM.
Rápido Go To Market	Programa piloto de 2 meses con soporte técnico y materiales de marketing
Alta demanda del mercado	Alta relevancia para clientes en industrias reguladas (finanzas, manufactura, sector público).
Soporte a Partners	Onboarding técnico y comercial, marketing conjunto, habilitación de ventas e incentivos de margen para socios

¿Por qué ser parte del Programa de Partners de Enthec?

Modelo de Partnership

1. Fase Piloto (0-2 Meses): Acceso de prueba gratuito para 1-3 clientes finales, Demostración de Valor, capacitación e integración
2. Salida al Mercado (3-6 Meses): Integración en la cartera de MSP, marketing conjunto, marca compartida, casos prácticos, posible exclusividad.

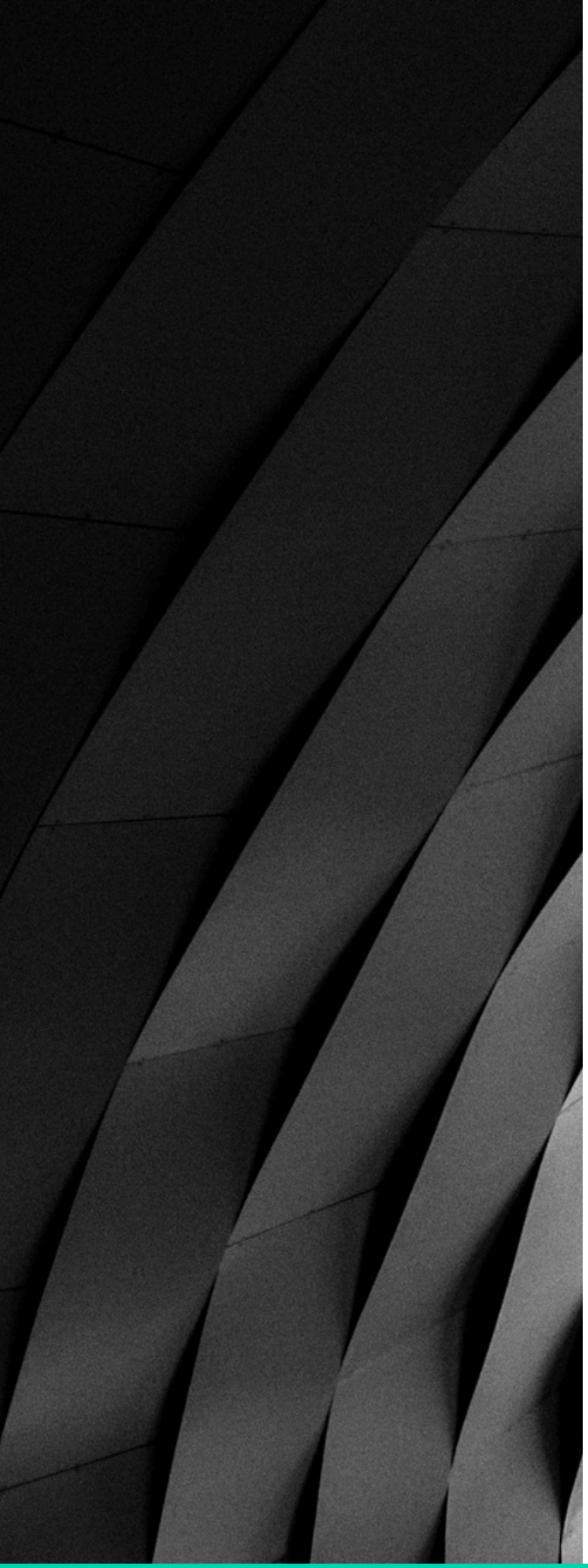
Clientes Objetivo

- Medianas y grandes empresas con infraestructura crítica
- Finanzas, seguros, manufactura, energía y sector público
- Organizaciones con requisitos de cumplimiento de las normas ISO 27001 / TISAX / BSI

¿Qué esperamos de un Partner?

- Desarrollo de negocio y búsqueda de nuevos clientes.
- Relación con el cliente y gestión de las renovaciones.
- Capacitación, experiencia y recursos que le permitan prestar los servicios de Ciberseguridad necesarios para que el cliente perciba la utilidad de la herramienta y su contribución a la disminución del nivel de riesgo y exposición de la organización.
- Compromiso a largo plazo.

Buscamos Partners tecnológicos que quieran comprometerse con el proyecto de Enthec, que nos ayuden en la búsqueda de clientes y que tengan los conocimientos y capacidades técnicas en Ciberseguridad que les permitan desarrollar las acciones de Remediación, Mitigación y Protección necesarias, así como de valoración del riesgo TI de terceros, convirtiéndose en una parte integral de nuestra cadena de valor.



Enthec Solutions es una Deep Tech que desarrolla software de ciberseguridad para extender la ciberprotección de las organizaciones más allá del perímetro de IT. Enthec Solutions ayuda a las organizaciones a implementar y expandir su estrategia de ciberseguridad basada en IA para controlar cualquier filtración de datos, exposición y brecha de seguridad en Internet, la Deep Web y la Dark Web.

Enthec Solutions se ha consolidado como una de las Deep Techs con soluciones de Cibervigilancia perimetral externa más innovadoras y efectivas a través del éxito de su Plataforma **Kartos Corporate Threat WatchBots,** que brinda a las organizaciones capacidades de Ciberseguridad, Ciberinteligencia, Cumplimiento y Evaluación de Riesgos de Terceros, y su último e innovador producto, **Qondar Personal Threat Watchbots Platform,** software de Cibervigilancia para la protección de la información en línea y los activos digitales de las personas.

www.enthec.com

Si quieres conocer más sobre nuestro Programa de Partners o probar nuestros Kartos Corporate Threat Watchbots o Qondar Personal Threat Watchbots en una demo y descubrir cómo pueden proteger a tus clientes y las ventajas competitivas que aportan a tus soluciones y servicios de Ciberseguridad, puedes contactarnos a través de esta dirección de correo electrónico:

hola@enthec.com

¡Gracias!