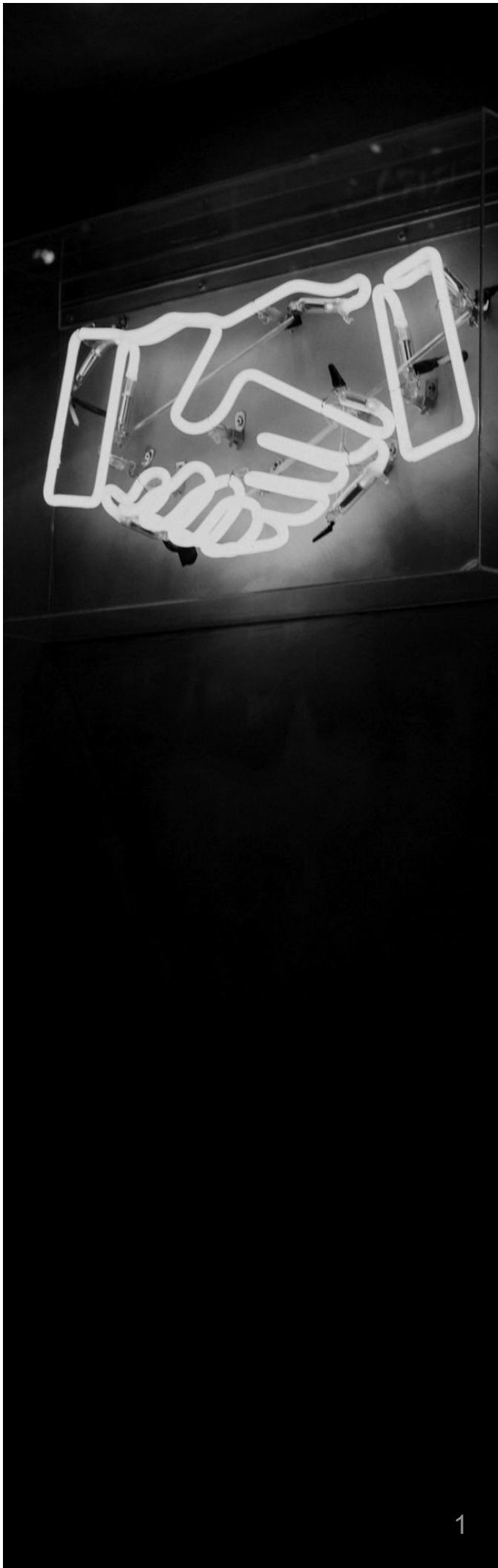
ENTHEC

Programa de Partners



kartos

XTI watchbots

Índice

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

Por un lado, aumenta nuestro alcance comercial y la llegada a clientes.
Por otro, debido a las características de nuestro producto, software de cibervigilancia, necesitamos contar en nuestra red de atención a los clientes con organizaciones que tengan 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 tiene estos recursos *in-house*, pero en la mayoría de los casos, el encargado de realizar esas tareas es un partner que presta servicios gestionados de seguridad. Esto crea una relación simbiótica entre Enthec y sus partners, quienes mediante la incorporación del producto de Enthec a sus servicios gestionados de ciberseguridad pueden proporcionar a sus clientes una estrategia de cibervigilancia XTI (Extended Thread Intelligence), que les permite descubrir y resolver incidencias imposibles de ser detectadas con las estrategias tradicionales de ciberprotección y realizar una valoración del riesgo TI de terceros, aportando valor a su oferta.

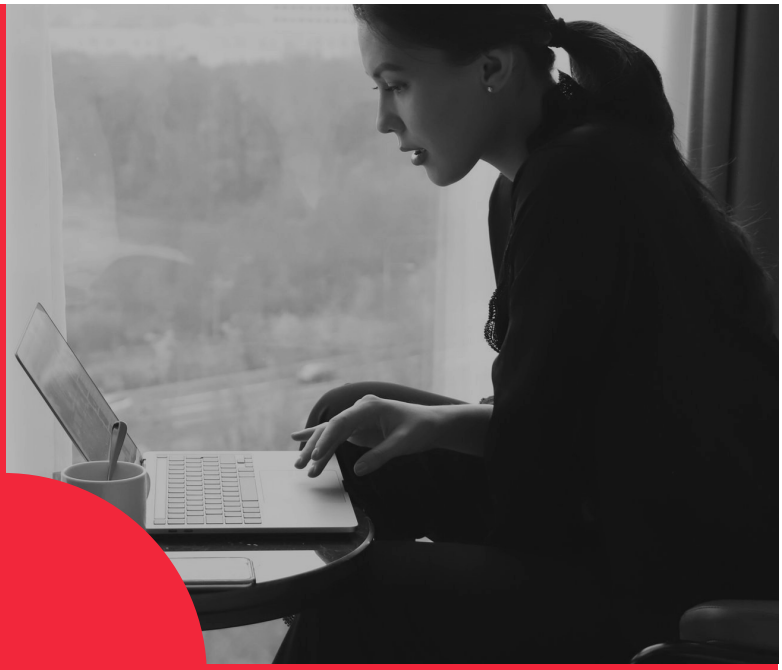
Por eso, dentro de nuestro Programa de Partners contamos dos modalidades:

Reseller Partner

Vende nuestras licencias a nuestros clientes y puede, si así lo desea, prestar sobre ella los servicios para los que esté capacitado según su formación e infraestructura.

MSSP Partner

Utiliza nuestra herramienta para ofrecer a sus clientes el servicio de cibervigilancia XTI y de valoración del riesgo TI de terceros dentro de su portfolio de servicios gestionados de ciberseguridad.



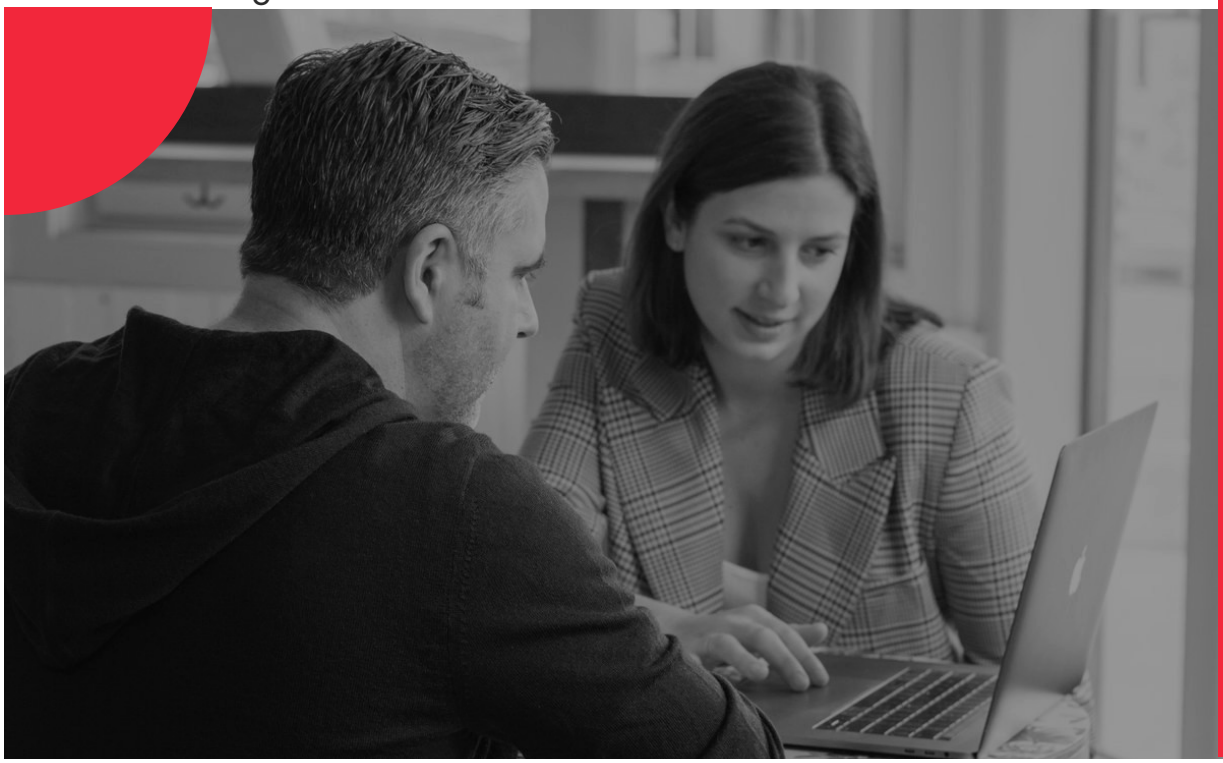
Enthec no tiene canales propios de venta directa o de servicios gestionados de seguridad. Por tanto, Enthec no actúa como competencia de nuestros partners en ninguna de las dos modalidades. Tanto la venta de nuestras licencias como la oferta de remediación de las vulnerabilidades detectadas o de valoración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

Propuesta de valor al cliente

Kartos XTI Watchbots: EASM + DRPS + SRS en una sola plataforma.

Kartos XTI Watchbots es la plataforma de cibervigilancia desarrollada por Enthec para extender el perímetro de seguridad controlado por las organizaciones. Concebida desde un enfoque de estrategia hacker, Kartos está en permanente proceso de I+D para incorporar categorías y capacidades adelantadas a la evolución de los ciberataques.

Kartos está formada por un ejército de XTI Watchbots diseñado específicamente para buscar en los repositorios de Internet, la Deep Web y la Dark Web. El ejército de XTI Watchbots de 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 TI de terceros.



kartos©
XTI watchbots

Capacidades

- **External Attack Surface Management (EASM)**: Detección de activos corporativos e información sobre sistemas, servicios en la nube y aplicaciones que están disponibles y visibles en el dominio público para cualquier ciberdelincuente.

- **Digital Risk Protection Service (DRPS):** Detección de información contextual sobre posibles agentes de ataques, sus tácticas y procesos para llevar a cabo actividades maliciosas. Eliminación de actividades maliciosas en nombre de la organización.

- **Security Rating Services (SRS)**: Evaluación independiente de riesgos propios y de terceros, para una visualización amplia de la madurez en ciberseguridad de cualquier organización utilizando un enfoque externo. Ampliación y ponderación de la información proporcionada por los métodos tradicionales de evaluación de riesgos por terceros.

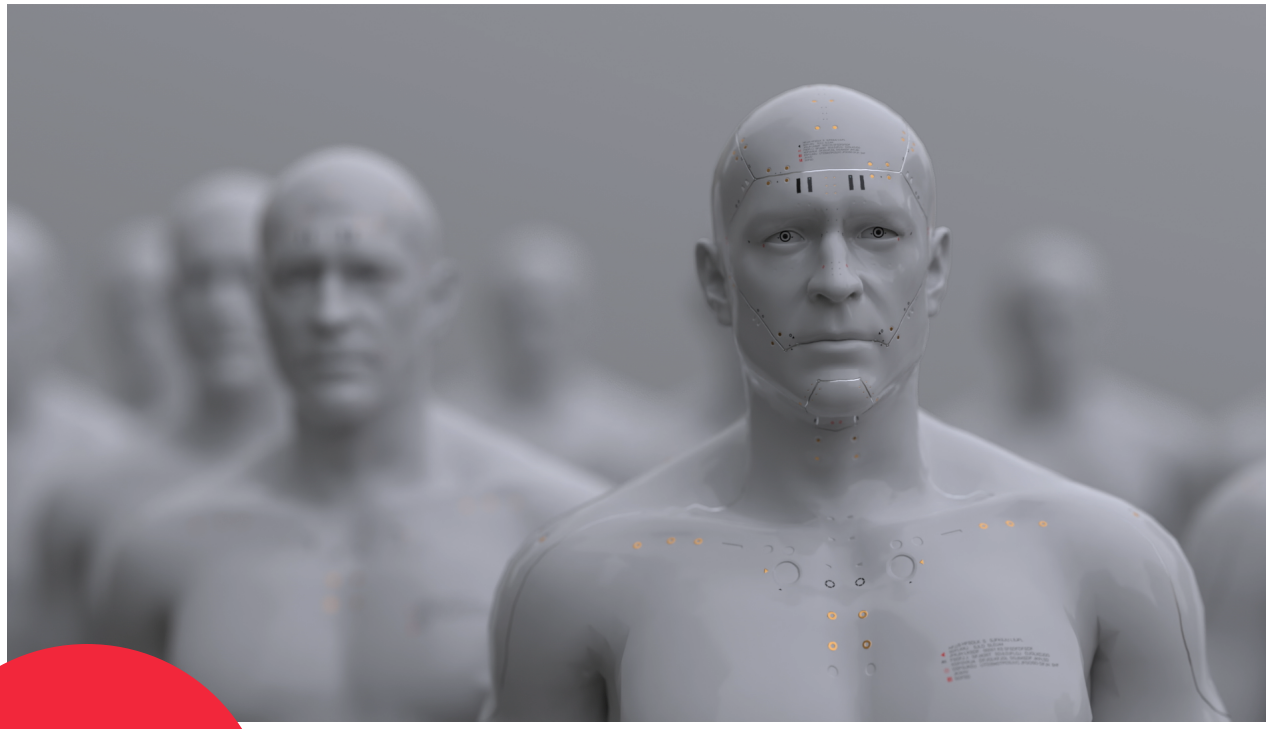
Funcionamiento

Para que el proceso comience, sólo se necesita introducir en la plataforma el dominio de la empresa objeto de la búsqueda.

La información encontrada se organiza en 9 categorías a partir de las cuales se construyen los índices de riesgo de la organización.

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

Uno de los factores diferenciales de Kartos respecto a herramientas similares es que no sólo permite obtener información que suponga un riesgo de ciberseguridad. También permite identificar robos y filtraciones de información confidencial, crítica o sensible que supongan un riesgo legal o reputacional, o de propiedad intelectual que puedan acarrear una pérdida de ventaja competitiva o un riesgo para el negocio.



¿Cuál es la innovación de Kartos frente al planteamiento actual casi homogéneo de la Ciberseguridad?

La forma de enfocar la necesidad de cibervigilancia. Hasta la fecha, los esfuerzos de los sistemas y procesos se centran en intentar garantizar la protección del perímetro interno y la infraestructura, y verificar que esta protección funciona. Es decir, blindar a la organización con una muralla de herramientas que impidan el asalto de la ciberdelincuencia: un sistema de dudosa eficacia a la vista de los datos, que no tiene en cuenta los riesgos de terceros y cuya escalabilidad es complicada a nivel herramientas y costes con la entrada de nuevas tecnologías como la nube o el IoT.

Este enfoque de blindaje interno no resulta suficiente porque no contempla una parte imprescindible en cualquier estrategia de protección: la vigilancia del perímetro externo, que permite adelantarse a los ciberataques neutralizando la potencial ventaja que la información filtrada y expuesta le proporciona a los ciberdelincuentes; detectando las brechas de seguridad en la muralla de herramientas de blindaje interno; valorando el riesgo de terceros; y minimizando los efectos del factor humano, el eslabón más débil de la cadena de protección.

La innovación y la propuesta de valor de Kartos parte exactamente de la perspectiva contraria de la seguridad corporativa tradicional, con una visión mucho más práctica y sencilla nacida del enfoque hacker de nuestra solución: observamos la organización desde fuera, como hace un ciberdelincuente.

Los ataques de penetración y de fuerza bruta son normalmente detectados y neutralizados con facilidad por los sistemas de protección perimetral. El problema de los ciberataques aparece cuando se diseñan y realizan utilizando información corporativa que está filtrada y expuesta de manera pública sin conocimiento de las compañías y que facilita la entrada o el lanzamiento de ataques a las personas.
El ejército de XTI Watchbots de Kartos busca qué vulnerabilidades son las que de forma pública están a disposición de los potenciales ciberatacantes, y descubre su origen para que puedan tomarse las medidas de neutralización y remediación adecuadas

De manera automatizada, continua y en tiempo real, Kartos proporciona al equipo corporativo de seguridad una información a la que no tiene acceso y que necesita para mantener una visión 360º de su situación y poder diseñar un sistema de protección y defensa completo y eficaz.

Propuesta de valor al partner

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

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

- Kartos permite al cliente o al partner detectar vulnerabilidades, brechas de seguridad propias y de terceros e información filtrada y expuesta desconocida por las compañías y que sólo Kartos puede encontrar. Su singularidad facilita tanto la venta de licencias como la aportación de valor a un portfolio de servicios de ciberseguridad, permitiendo su inclusión en la oferta de servicios de remediación, mitigación, protección y valoración del riesgo de terceros no contemplados, con el consiguiente aumento en la facturación.

- Kartos es un sistema automatizado que funciona de forma continua 365x24x7 integrándose con cualquier sistema de gestión, lo que permite la recepción de alertas inmediatas cada vez que se produce una incidencia. Sólo Kartos y sus partners pueden ofrecer y proporcionar esta información de esta forma y con esta frecuencia a sus clientes.

- Kartos proporciona la información a través de un interfaz diseñado en formato entendible a perfiles que abarcan desde aquellos con conocimientos muy básicos de Ciberseguridad a aquellos que pueden entender la parte más técnica y tomar las medidas de remediación necesarias para solucionar los problemas. Además, Kartos puede integrarse mediante APIs en los sistemas de los clientes, SOCs y otros sistemas de gestión de los partners de forma muy sencilla y asequible, logrando que la puesta en producción sea cuestión de minutos.

¿Por qué ser nuestro partner?

Por la diferenciación: La incorporación de Kartos al catálogo de soluciones y servicios de Ciberseguridad aporta una potente y eficaz ventaja competitiva y de diferenciación en innovación de la oferta de nuestros partners frente a sus competidores.

Por el alcance: El ejército de XTI Watchbots de Kartos trabaja 24x7 y traslada la información sobre amenazas en tiempo real, permitiendo la inmediata actuación de remediación de nuestros partners o sus clientes cuando sea necesario y la generación de confianza.

Por la sencillez: Kartos es una plataforma no intrusiva, automatizada, con un atractivo diseño, sencilla de usar y que además proporciona a nuestros Partners o sus clientes diferentes tipos de informes adaptados al nivel de conocimiento tecnológico de cada receptor.

Por el soporte: Estamos siempre al lado de nuestros Partners a través de nuestro excelente servicio de soporte técnico y de ventas, proporcionándoles apoyo técnico, materiales de marketing y venta, formación y asistencia permanente.

¿Qué esperamos de un partner?

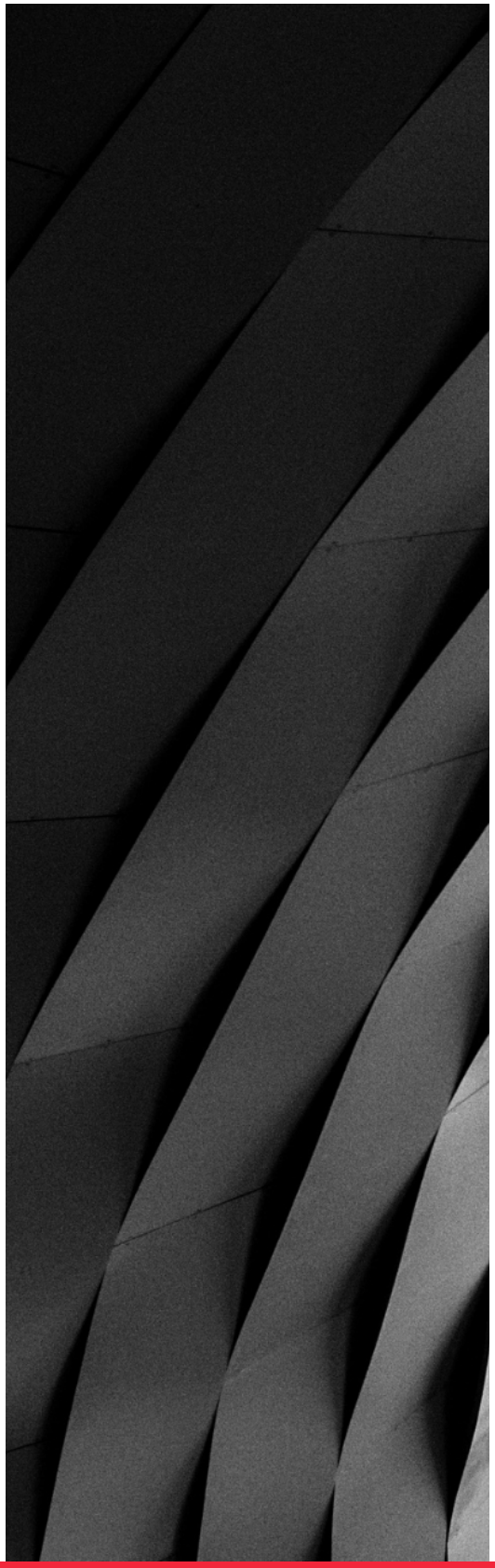
- Desarrollo de negocio y búsqueda de nuevos clientes.
- Relación con el cliente y gestión de las renovaciones.
- Capacitación, experiencia y recursos que le permitan prestar los servicios de Ciberseguridad necesarios para que el cliente perciba la utilidad de la herramienta y su contribución a la disminución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

Niveles de Parnership

Atendiendo a diversos parámetros que incluyen aspectos económicos, estratégicos, formativos y relacionados con la calidad de servicio, nuestros partners pueden optar a cuatro niveles de certificación

Resellers	Silver	Gold
MSSPs	Blue	Red



ENTHEC

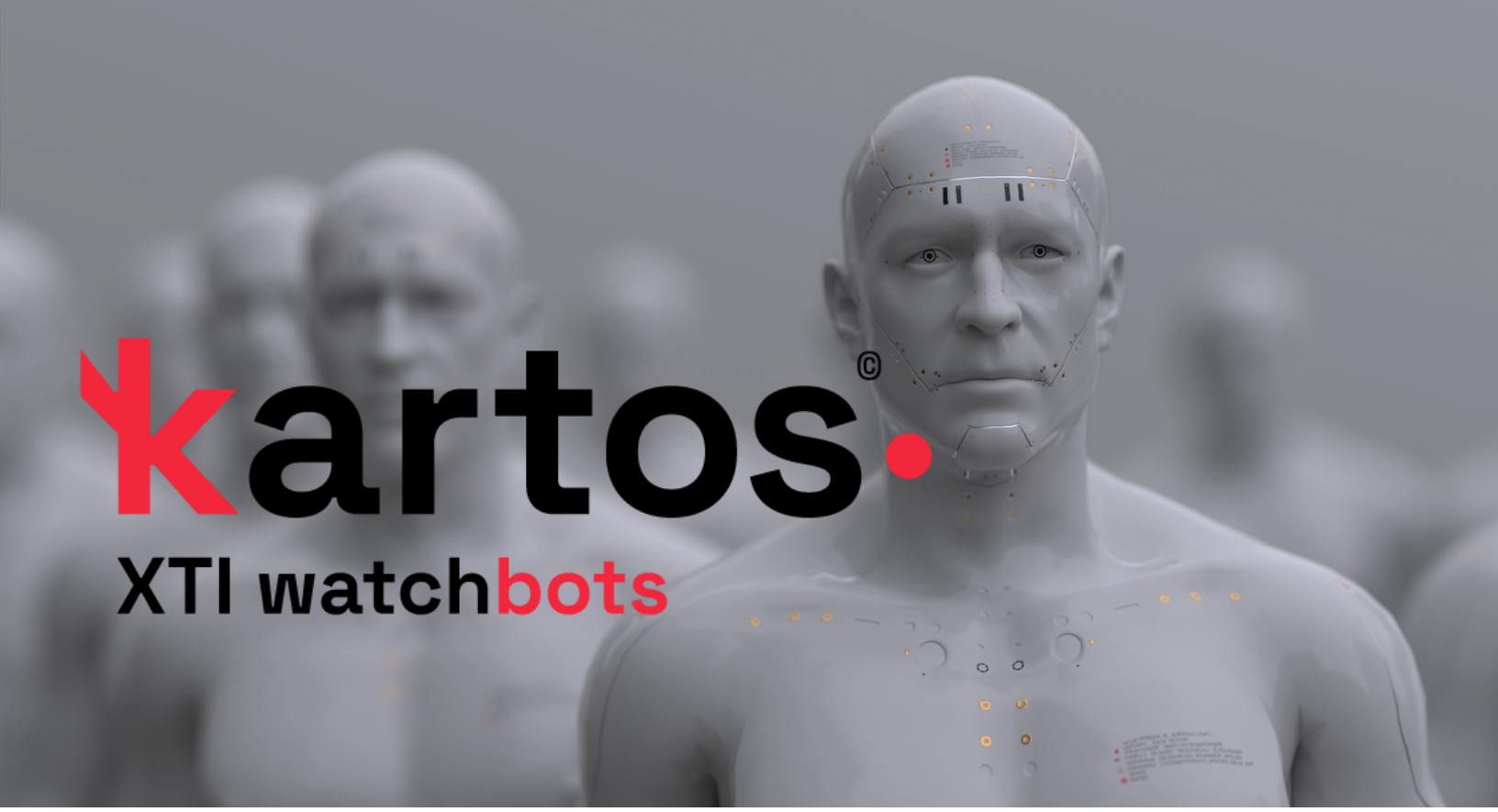
Enthec es una Deep Tech de desarrollo y fabricación de software de Ciberseguridad con enfoque hacker, para extender el alcance de las estrategias de ciberprotección de las organizaciones.

Fundada como startup en 2019 por María Rojo, Enthec ha crecido a través de rondas de financiación y del éxito de su plataforma Kartos hasta consolidarse como una de las Deep Tech con soluciones más innovadoras y eficaces en el campo de la Ciberseguridad.

www.enthec.com

Si quieres ampliar la información sobre nuestro Programa de Partners o probar de forma gratuita nuestra plataforma Kartos XTI Watchbots y descubrir cómo puede proteger a tus clientes y las ventajas competitivas que aporta a tu oferta de soluciones y servicios de Ciberseguridad, puedes ponerte en contacto con nosotros a través de esta dirección de correo:

hola@enthec.com



¡Gracias!