ENTHEC©

Cibervigilancia XTI para Compañías de Servicios Financieros

Controla la información de tu organización
al alcance de los ciberdelincuentes

kartos©

XTI watchbots

La ciberseguridad es un problema de Gobierno y Riesgo Corporativo

Aunque es cierto que la concienciación sobre el Riesgo Digital y la necesidad de potentes sistemas de Ciberseguridad es cada vez mayor en los Comités de Dirección de las Compañías de Servicios Financieros, en general sigue existiendo la sensación de que es algo que compete exclusivamente al departamento de IT. En lo que se refiere a los aspectos técnicos, esto es verdad. Pero en el impacto de un posible ataque a la organización, las posibles repercusiones pueden afectar a todos y cada uno de los departamentos de la organización y causar a esta importantes daños operacionales, reputacionales, legales, de propiedad intelectual e industrial y económicos.

En este documento vamos a analizar cuáles son los riesgos para una Compañía de Servicios Financieros de seguir una estrategia de Ciberseguridad incompleta y cómo prevenirlos implementando una estrategia XTI de Cibervigilancia Inteligente más allá del perímetro interno de la organización.

La ciberseguridad en las organizaciones

Es un hecho que la inversión en Ciberseguridad del sector de Servicios Financieros no ha dejado de crecer en los últimos años y ninguna previsión indica que esta tendencia vaya a cambiar. Frente a este dato, es también un hecho que, a pesar de ello, el número de ciberataques con éxito realizados a organizaciones del sector tampoco deja de crecer, a pesar de la mejora en los sistemas de detección y defensa.
¿Cuál es la razón para que se den simultáneamente dos hechos aparentemente contradictorios?

Es imposible proteger una organización si no se dispone de toda la información.

Actualmente los sistemas de Ciberseguridad se basan en la información que recopilan de lo que se conoce como perímetro IT. Es decir, la infraestructura tecnológica que puede ser monitorizada y protegida con los recursos y los límites legales de una organización. De vez en cuando, se realizan ataques de intrusión y tests de vulnerabilidades para detectar fallos en los sistemas que puedan ser utilizados por los Ciberdelincuentes. Y con esta información, se intenta blindar la organización.

El enfoque de blindaje sobre información del perímetro interno tiene al menos cinco puntos débiles:

FALTA DE INFORMACIÓN

Las organizaciones no llegan a toda la información corporativa sensible que está en la red a disposición de los cibercriminales y que les puede proporcionar una vía de entrada.

FACTOR COSTE

Si el nivel de protección de la organización se basa en el blindaje de cada elemento este deberá aumentará cada vez que se añada uno nuevo, haciéndolo ineficiente e inabordable.

FACTOR HUMANO

Por muy alto que sea el blindaje del perímetro interno IT, el factor humano es la primera causa desencadenante de un ciberataque a través de la ingeniería social, y es un factor que no puede ser blindado.

PERÍMETRO IT

Los límites de Ciberseguridad van más allá del perímetro IT, ya que se extienden hasta todos los proveedores, colaboradores o terceros con los que se comparte información y que acceden a sus sistemas.

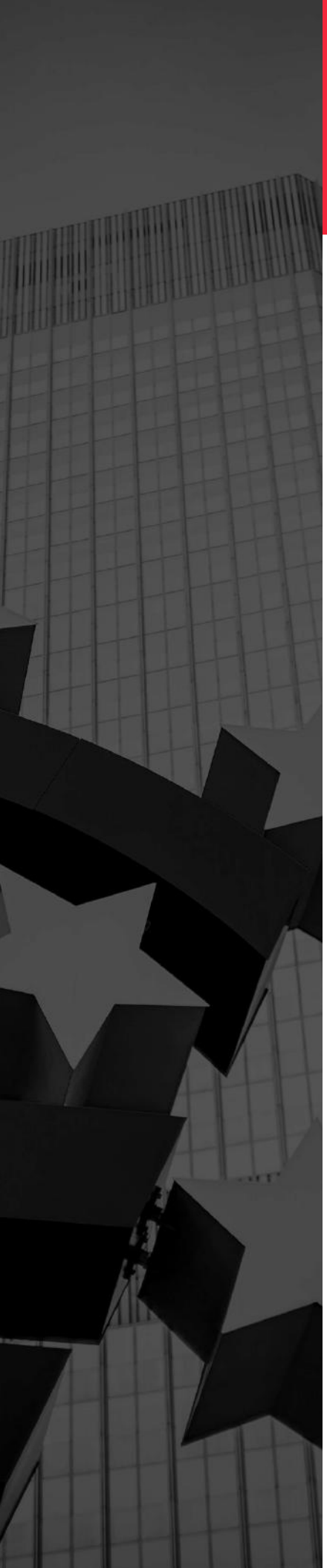
FACTOR TIEMPO

Un factor crítico es la cantidad de tiempo que una vulnerabilidad está abierta o que una información estádisponible, ya que multiplica la posibilidad de que se utilice.

El impacto del Riesgo IT en el Riesgo Corporativo

Un evento de ciberseguridad en el negocio de la Compañía que permita a los cibercriminales simplemente disponer de información de uso restringido o el acceso a la organización, sus empleados o a los terceros con los que se relaciona, puede provocar:

1. Interrupción del servicio TI y de la operativa de la Compañía.
2. Fraude, pérdidas económicas estafas, robo, chantajes.
3. Fallos en el sistema de atención a los clientes.
4. Robo, publicación y venta de propiedad intelectual.
5. Robo de información relacionada con la competitividad, pérdida de posicionamiento.
6. Ataques orientados a causar daño legal aprovechando fallos en cumplimiento.
7. Disminución en la satisfacción de los clientes por falta de atención o incumplimiento.
8. Daños reputacionales. Pérdida en el valor de marca y disminución de la confianza.
9. Publicación de datos personales de empleados, clientes y terceros.
10. Suplantación de identidad de la organización o personas relacionadas con ella.



Factores de riesgo para cada CXO

Por la propia naturaleza de su trabajo, dentro de los departamentos de una organización se desarrollan tareas que pueden poner a la compañía en riesgo de un ciberataque. Por ello, todos son responsables de tomar las medidas protectoras dentro de su área de responsabilidad.

En las estrategias evolucionadas de ciberprotección, la Ciberseguridad y el Riesgo IT han dejado de considerarse responsabilidad exclusiva de CI para confirmarse como una responsabilidad conjunta del Consejo de Gobierno. Un problema de Riesgo Institucional.

CEO

Vela por la integridad de la Compañía, por su reputación, su propiedad intelectual y por garantizar la continuidad de la actividad corporativa y la protección de sus empleados.

DIRECTOR GENERAL

Vela por la integridad y el correcto funcionamiento de su área de servicios financieros

CISO

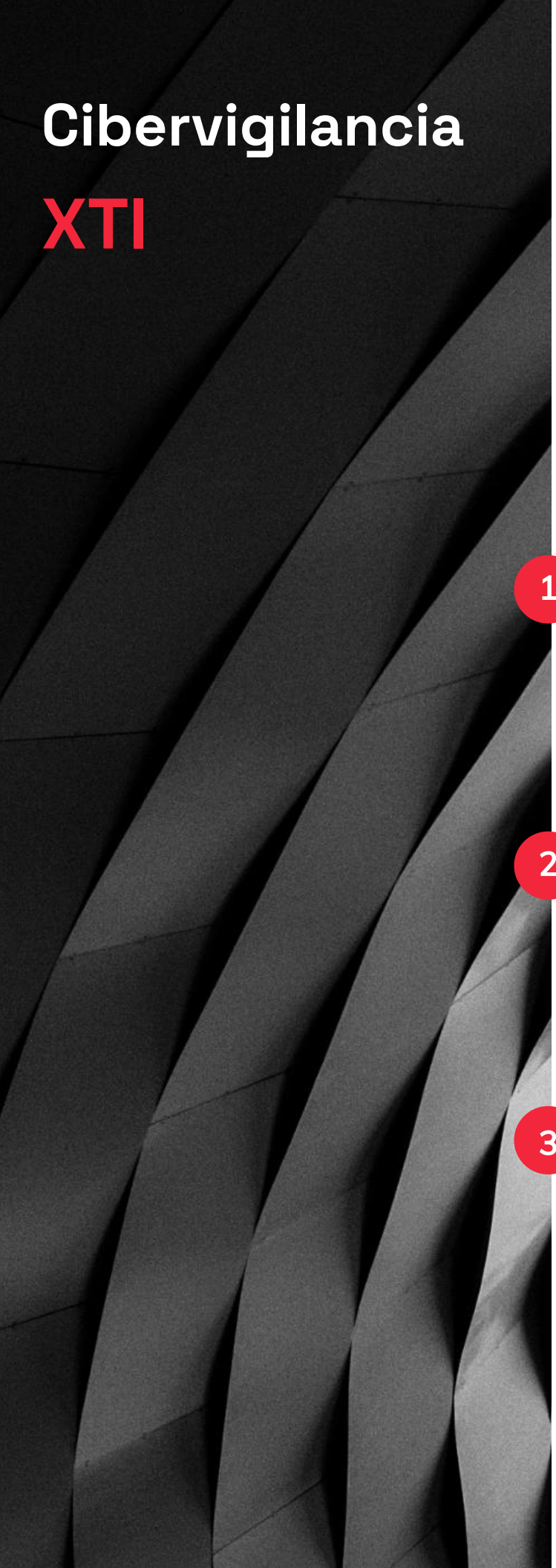
Es el responsable último del Riesgo IT y de la estrategia de Ciberseguridad de la organización.

CFO

Es el responsable de evaluar el riesgo de proveedores y partners, en el que debe considerar el Riesgo IT en los casos de terceras partes.

LEGAL / COMPLIANCE

Vela por el cumplimiento de la legislación específica sobre tratamiento y protección de la información y los datos sensibles que maneje la organización.



Cibervigilancia XTI

Cibervigilancia XTI: EASM + DRPS + SRS

Lleva la estrategia de ciberseguridad de la organización más allá de su perímetro interno.

1. **EXTERNAL ATTACK SURFACE MANAGEMENT**: 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.

2. **DIGITAL RISK PROTECTION SERVICES**: 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.

3. **SECURITY RATING SERVICES:** 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.

Cibervigilancia XTI del Riesgo Corporativo

Hacemos posible que las Compañías proveedoras de Servicios Financieros puedan controlar en tiempo real la información corporativa filtrada y expuesta al alcance de cualquier ciberdelincuente para neutralizar su posible impacto y detectar la brecha de seguridad que ha provocado la filtración.

¿Qué ventajas aporta extender la cibervigilancia al perímetro externo?

Se recibe una indicación global de TI basado en el conocimiento que los cibercriminales tienen sobre las vulnerabilidades y los puntos débiles de la organización, y que por tanto reflejan de la manera más fiel posible cómo puede ser atacada la Compañía y con qué impacto. Además, facilita la detección de las brechas de seguridad, el control de la información expuesta y la valoración del riesgo de terceros.

¿Qué tipo de Riesgos podré controlar?

La información se estructura en nueve categorías diferentes entre las que se incluyen el análisis exhaustivo de documentos filtrados y de lo que se habla en redes sociales sobre la Compañía. Por tanto, además de los riesgos relacionados con la infraestructura tecnológica de la organización, se detectan riesgos relacionados con la protección de datos, el robo de información confidencial o de propiedad intelectual, o riesgos de ataques reputacionales, que son indetectables por los sistemas de Ciberseguridad de las organizaciones.

¿Para quién será de utilidad esta información?

i. La información está diseñada para que cada responsable corporativo de cada riesgo determinado entienda los datos obtenidos por la monitorización y el análisis del perímetro externo en cada categoría y el impacto que pueden tener en la situación de riesgo de la Compañía. Esto puede aplicarse a la propia organización o a organizaciones de terceros de los que se necesite hacer una valoración de la situación de riesgo.

ii. La información proporciona al CISO o responsable de Ciberseguridad una visión del nivel de riesgo en el perímetro externo de la organización que complementa la que le proporcionan sus sistemas.

iii. Finalmente, la información permite al responsable llevar a cabo las acciones de neutralización y protección necesarias para que las vulnerabilidades detectadas no pasen al nivel de amenazas.

kartos©

XTI watchbots

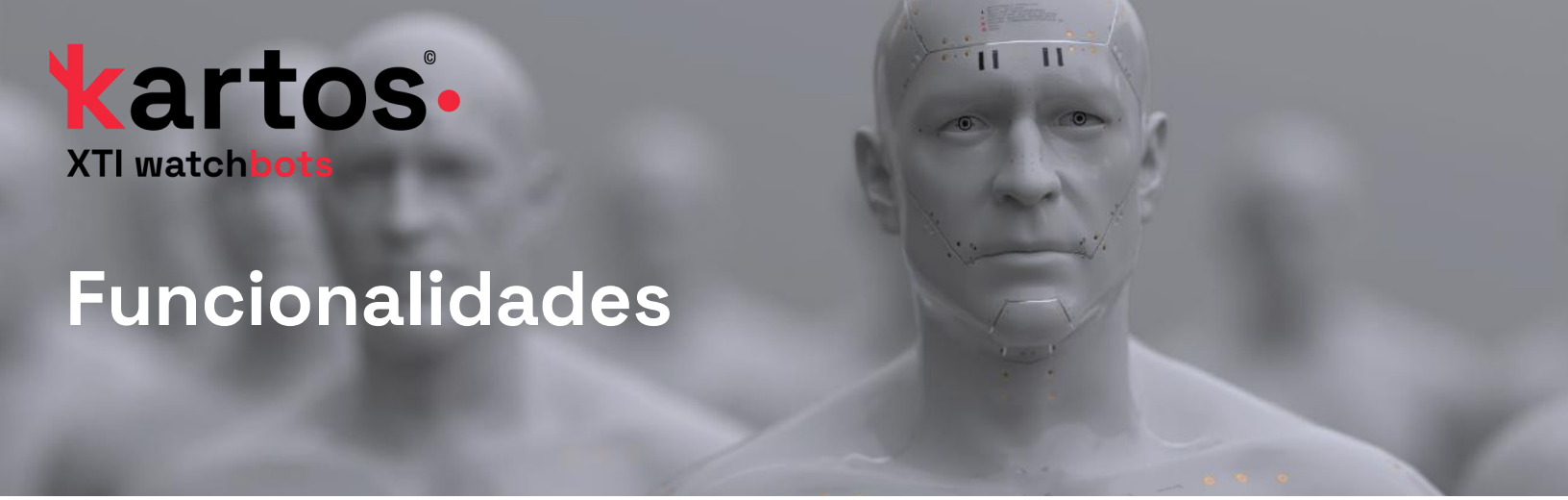
Kartos es la plataforma de cibervigilancia desarrollada por Enthec Solutions para extender el perímetro de seguridad controlado por las organizaciones e instituciones. Concebida desde un enfoque de estrategia hacker, Kartos está en permanente proceso de I+D para incorporar categorías y capacidades adelantadas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

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

A través de la monitorización y el análisis continuo de sus XTI Watchbots por la superficie externa, sin necesidad de implementación dentro del sistema IT corporativo ni de complicadas configuraciones **Kartos** facilita a las organizaciones el control y la neutralización de la información corporativa filtrada y expuesta, a la vez que permite la evaluación de riesgo institucional por causas relacionadas con TI y terceros, de una manera asequible incluso para personas sin formación específica en Ciberseguridad.

- **Capa de IA** que permite el funcionamiento 100% automatizado sin intervención humana en ninguna parte del proceso.
- **Herramienta estrictamente no intrusiva**. La investigación se realiza en Internet, la Deep Web y la DarkWeb y no se ataca el perímetro IT de las compañías, por lo que su funcionamiento y la información obtenida cumplen estrictamente con los límites impuestos por la legislación.
- Única plataforma que analiza las **conversaciones en redes sociales desde la perspectiva de detección de amenazas** y ataques, más allá de la relativa a reputación y branding.
- **Funcionamiento continuo 365x24x7**, lo que permite detectar filtraciones de nueva información prácticamente en tiempo real
- **Máxima sencillez de uso**. No requiere ninguna configuración compleja. Basta con introducir el dominio en la plataforma y funciona de manera autónoma, sin necesidad de configurar parámetros de búsqueda ni de cualquier otro criterio de localización de información.
- **Monitorización automatizada, objetiva y continúa de los riesgos causados por las terceras partes** que pertenecen a la Superficie de Ataque Externa de la organización.

kartos©
XTI watchbots



Funcionalidades

Análisis de 9 categorías de amenazas

- Red
- Salud de DNS / Phishing
- Gestión de Parches
- Reputación IP
- Seguridad Web
- Seguridad e-mail
- Filtración de Documentos
- Filtración de Credenciales
- Redes Sociales

Configuración personalizable

· Personalización de contenidos y permisos de seguridad por departamentos corporativos y usuarios.
· Personalización de alarmas en tiempo real por vulnerabilidades.

Ciberseguridad en redes sociales

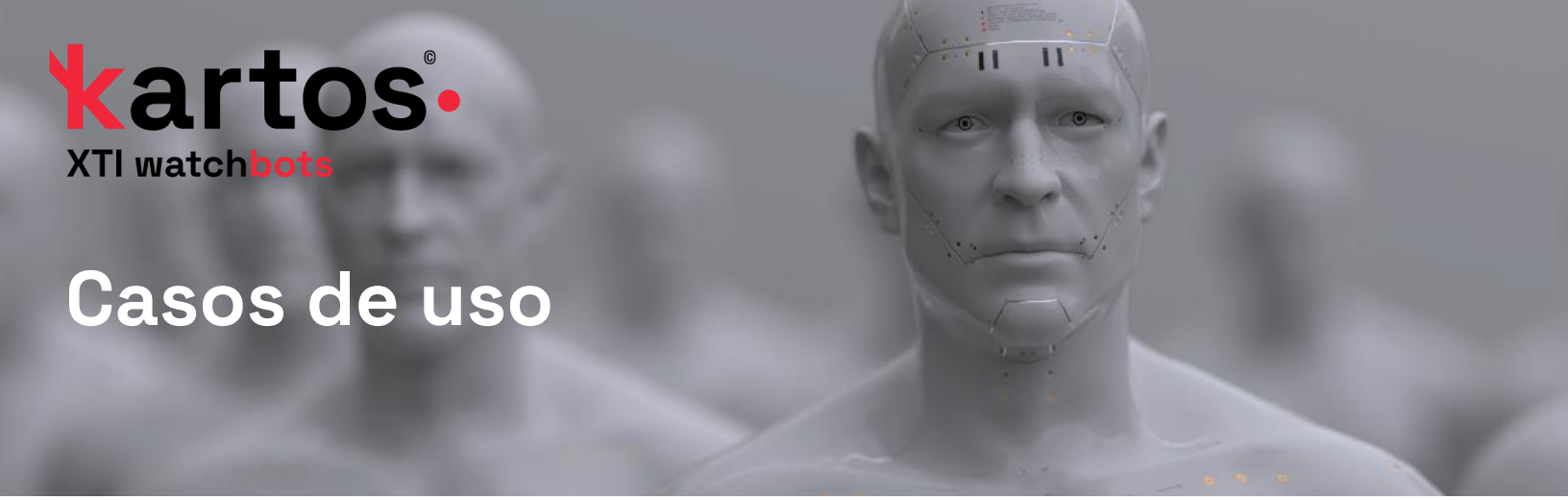
· Enfoque único en el mercado que consiste en el análisis de las principales redes sociales para detectar conversaciones que puedan hacer sospechar de un ataque en preparación.
· Detección de conversaciones en redes relacionadas con hacktivismo, fraude, phishing o campañas de fake news, entre otras.

Sencillez en la interpretación y el uso

· Información dividida en tres niveles y presentada de forma gráfica para que pueda mostrarse a personas sin conocimientos específicos de Ciberseguridad o a los expertos que deben solucionar problemas.

Modelo flexible de licencias

· Estructura de licencias anuales adecuada en coste y funcionalidades a las necesidades de cada organización, de acuerdo a los diferentes casos de uso en los que esté interesada.



Casos de uso

Detección de amenazas propias

Uso de Kartos para la detección de toda la información corporativa filtrada y expuesta en la red, así como de las brechas de seguridad que provocan dichas filtraciones para que la organización pueda tomar las acciones que le permitan mejorar sus sistemas de defensa y protegerse de posibles ataques.

Riesgo de terceros

Uso de Kartos como herramienta de EASM (External Attack Surface Management) para establecer y evaluar unos parámetros mínimos de cumplimiento de medidas de Ciberseguridad de los terceros, colaboradores o proveedores, que pueden comprometer a la organización si no se encuentran bien protegidos

- Protección frente a operaciones u órdenes fraudulentas
- Localización de información sensible filtrada
- Detección de contraseñas comprometidas
- Prevención de usurpación de identidad
- Detección de brechas de seguridad
- Protección de la marca
- Cumplimiento del GDPR
- Evaluación del riesgo de terceros, proveedores y partners.
- Protección de continuidad del servicio y la actividad financiera

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.

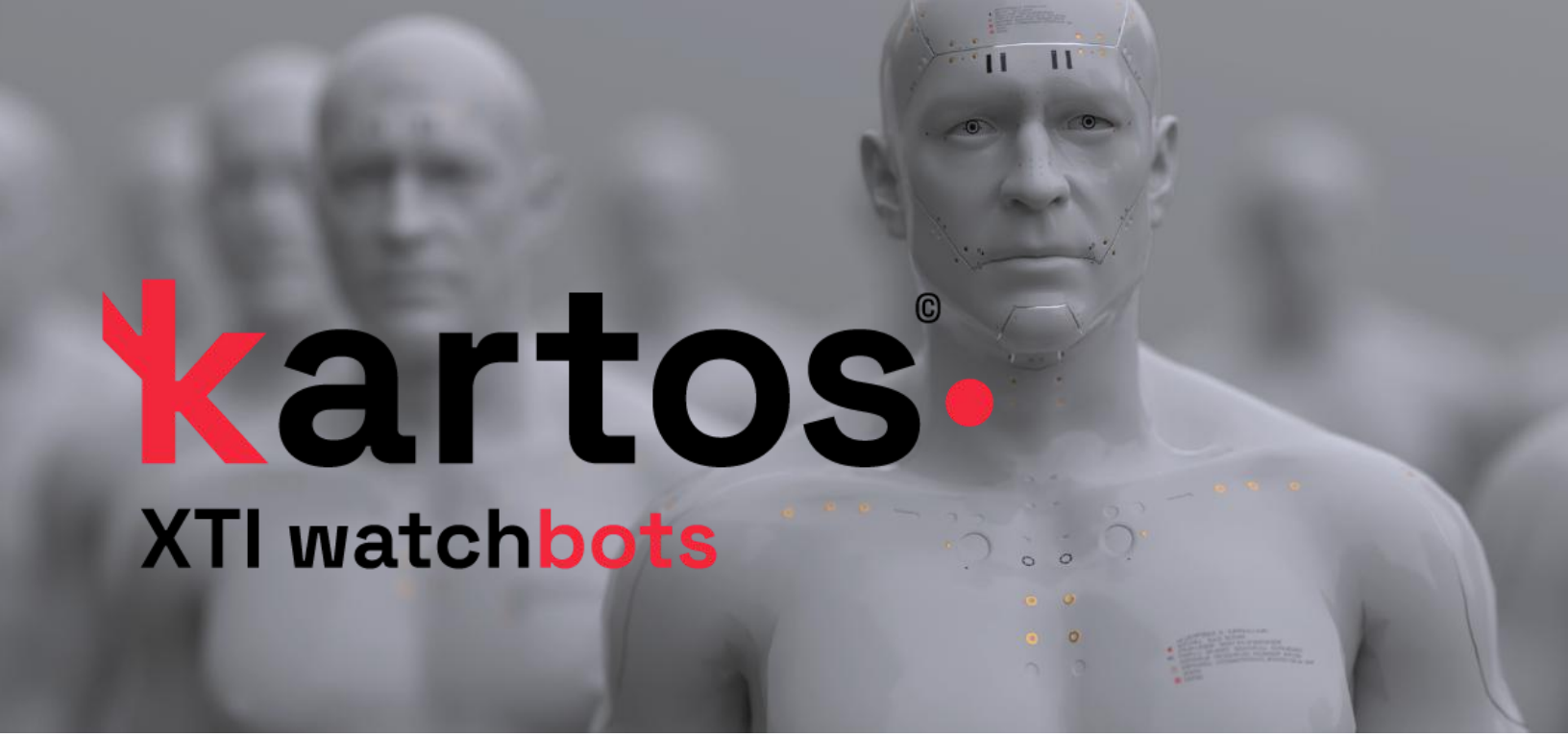
Fundada como startup en 2019 por María Rojo, Enthec ha crecido a través de rondas de financiación y del éxito de su plataforma Kartos hasta consolidarse como una de las Deep Tech con soluciones más innovadoras y eficaces en el campo de la Ciberseguridad.

Para conocer más sobre nosotros, puedes entrar en nuestra web:

www.enthec.com

Si quieres probar de forma gratuita nuestra plataforma Kartos XTI Watchbots y obtener un informe sobre las vulnerabilidades actuales más críticas de tu organización, puedes ponerte en contacto con nosotros a través de esta dirección de correo y te contaremos los pasos para monitorizar tu dominio.

hello@enthec.com



¡Gracias!