ENTHEC©

Cibervigilancia XTI para Hospitales

Controla la información hospitalaria
al alcance de los ciberdelincuentes

kartos©

XTI watchbots

La ciberseguridad es un problema de Gobierno y Riesgo hospitalario

Si bien 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 los Hospitales, todavía existe la creencia 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 un Hospital, las repercusiones afectan a todos y cada uno de los departamentos -tanto médicos como administrativos- provocan la interrupción de la atención a los pacientes -operaciones, tratamientos, consultas y citas- y causan importantes daños operacionales, reputacionales, legales, de propiedad intelectual y económicos.

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

La ciberseguridad hospitalaria

Es un hecho que la inversión en Ciberseguridad de los Hospitales 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 a Hospitales 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 un Hospital 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 institución. 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 el Hospital.

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

FALTA DE INFORMACIÓN

Los Hospitales no llegan a toda la información hospitalaria 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

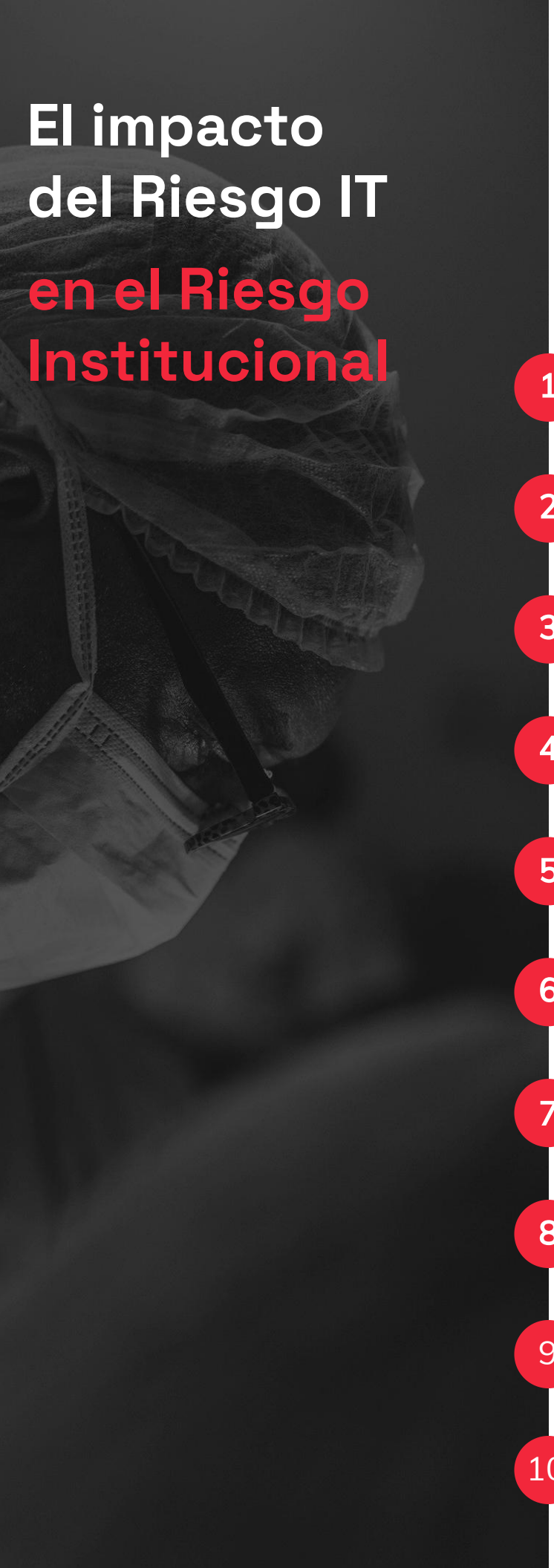
Por muy alto que sea el blindaje del perímetro interno IT, el factor humano es la primera causa desencadenante de un ciberataque a través de la ingeniería social, y es un factor que no puede ser blindado.

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

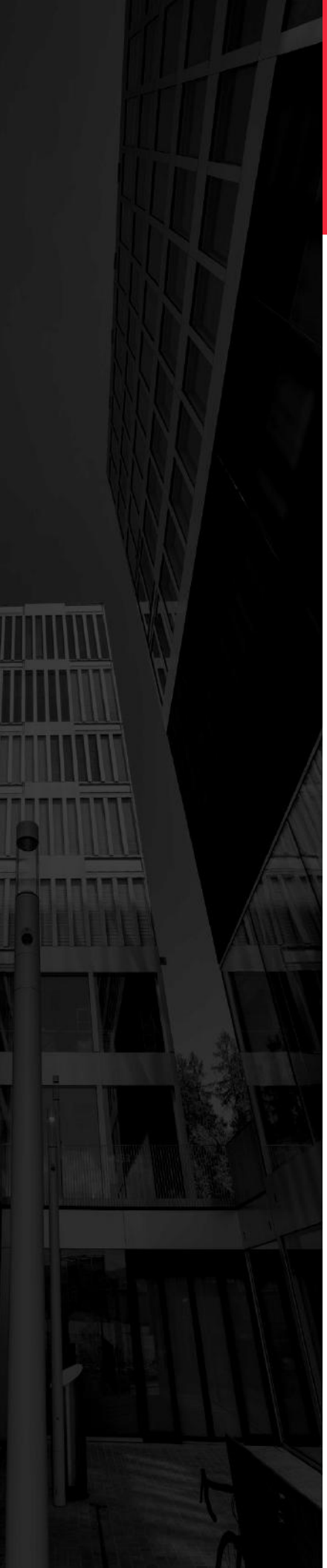
Un factor crítico es la cantidad de tiempo que una vulnerabilidad está abierta o que una información estádisponible, ya que multiplica la posibilidad de que se utilice.



El impacto del Riesgo IT en el Riesgo Institucional

Un evento de ciberseguridad que permita a los cibercriminales simplemente disponer de información de uso restringido o el acceso a los sistemas del Hospital, a sus empleados, pacientes o a los terceros con los que se relaciona, puede provocar:

1. Interrupción del servicio TI y de la operativa de todo el Hospital.
2. Fraude, pérdidas económicas estafas, robo, chantajes.
3. Fallos en el sistema de atención a los pacientes.
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 pacientes por atención o incumplimiento.
8. Daños reputacionales. Pérdida en el valor de marca y disminución de la confianza.
9. Publicación de datos personales de pacientes, profesionales del hospital y terceros.
10. Suplantación de identidad de la institución o personas relacionadas con ella.



Factores de riesgo para cada CXO

Por la propia naturaleza de su trabajo dentro de una infraestructura calificada como crítica, en todos los departamentos de un Hospital se desarrollan tareas que pueden poner a la institución 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 Board.

DIRECTOR GENERAL

Vela por la integridad del Hospital, por su reputación, su propiedad intelectual y por garantizar la continuidad de las actividades de atención al paciente y la protección de sus empleados.

DIRECTOR MÉDICO

Vela por que cada paciente de la institución reciba la atención médica ambulatoria u hospitalaria que precisa en el momento que lo necesita.

CISO

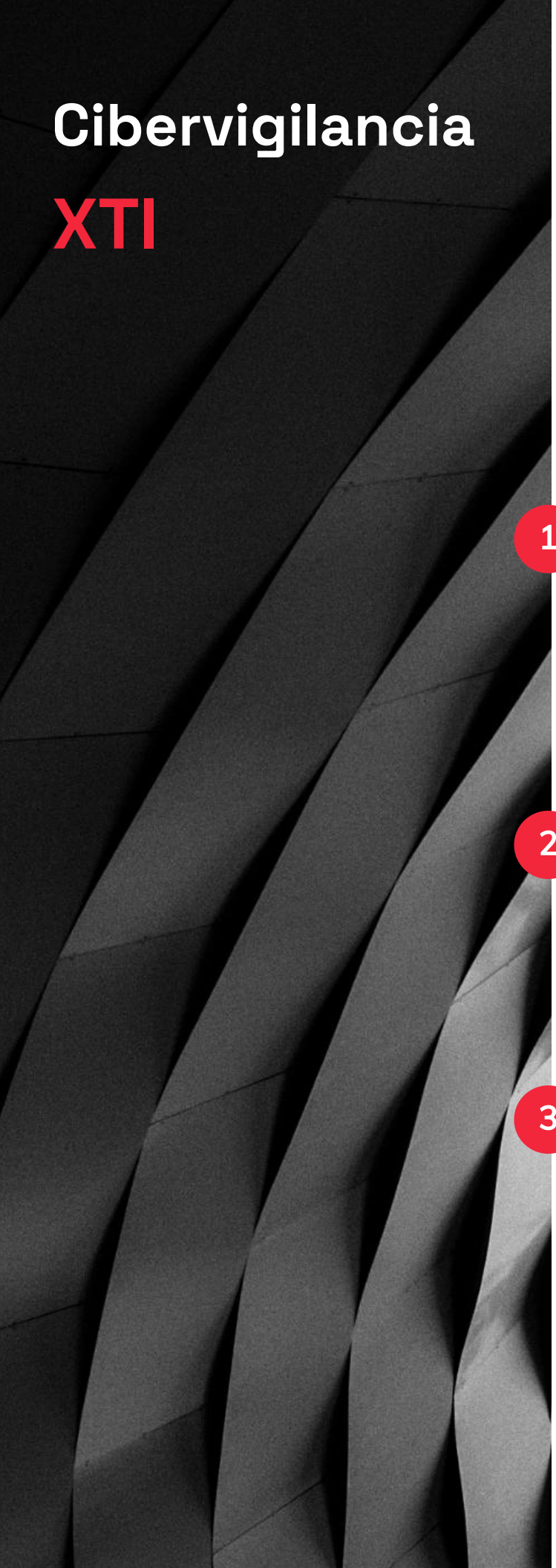
Es el responsable último del Riesgo, la protección de la información hospitalaria y la estrategia de Ciberseguridad de la institución.

CFO

Es el responsable de evaluar el riesgo de proveedores y colaboradores, 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 en infraestructuras críticas.



Cibervigilancia XTI

Cibervigilancia XTI: EASM + DRPS + SRS

Lleva la estrategia de ciberseguridad de la institución hospitalaria más allá de su perímetro interno.

1. **EXTERNAL ATTACK SURFACE MANAGEMENT**: Detección de activos hospitalarios 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, y 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 Institucional

Hacemos posible que los Hospitales puedan conocer en tiempo real la información institucional 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 del Hospital, y que por tanto reflejan de la manera más fiel posible cómo puede ser atacada la institución 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 institución. Por tanto, además de los riesgos relacionados con la infraestructura tecnológica del Hospital, se detectan riesgos relacionados con la protección de datos, el robo de información sensible 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 institucional 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 institución. Esto puede aplicarse al propio Hospital 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 institución 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

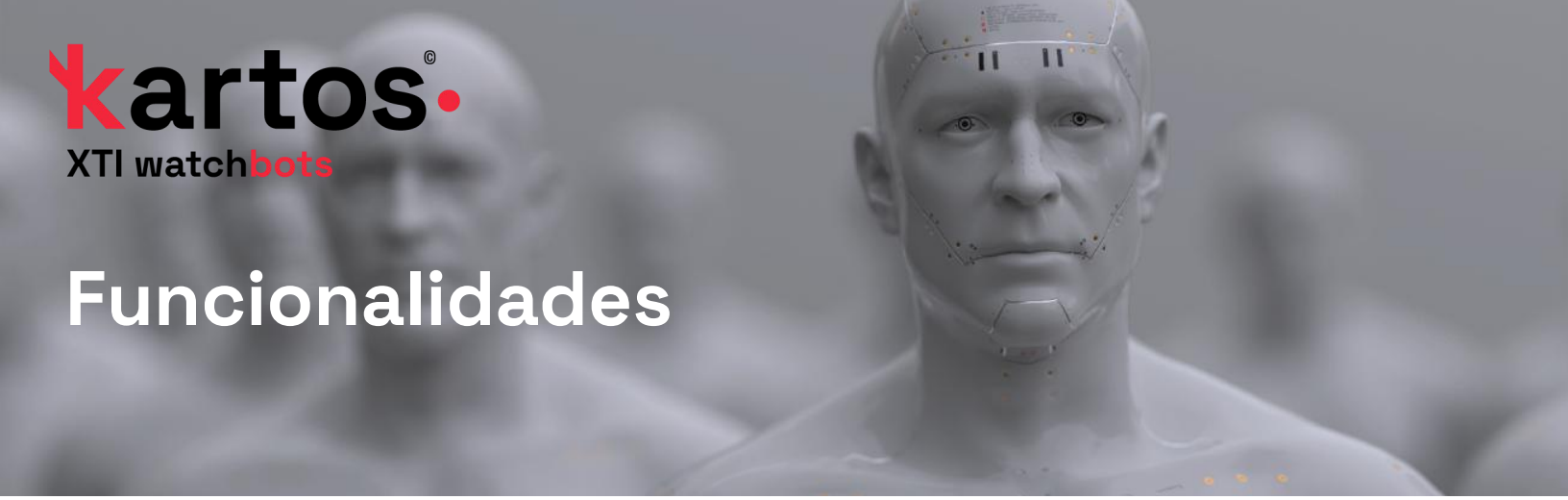
Kartos es la plataforma de cibervigilancia desarrollada por Enthec Solutions para extender el perímetro de seguridad controlado por las organizaciones e instituciones. Concebida desde un enfoque de estrategia hacker, Kartos está en permanente proceso de I+D para incorporar categorías y capacidades adelantadas 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 TI hospitalario ni de complicadas configuraciones, Kartos facilita a los Hospitales el control y la neutralización de la información hospitalaria 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 empresa.

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 hospitalarios y usuarios.
· Personalización de alarmas en tiempo real por vulnerabilidades.

Ciberseguridad en redes sociales

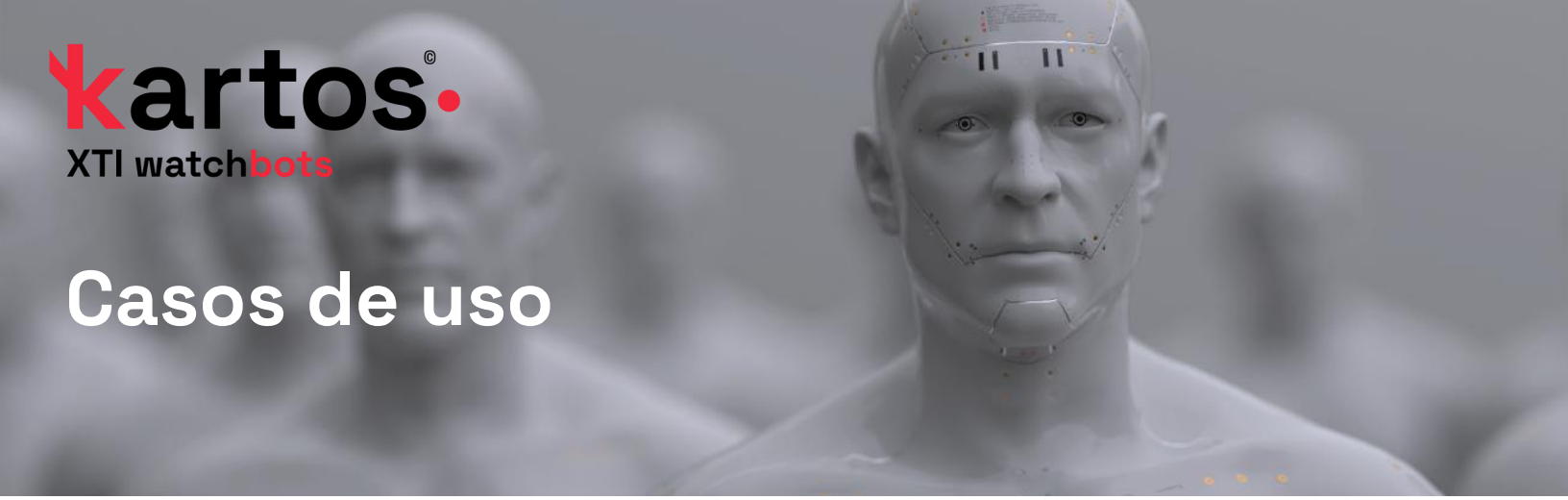
· Enfoque único en el mercado que consiste en el análisis de las principales redes sociales para detectar conversaciones que puedan hacer sospechar de un ataque en preparación.
· Detección de conversaciones en redes relacionadas con hacktivismo, fraude, phishing o campañas de fake news, entre otras.

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

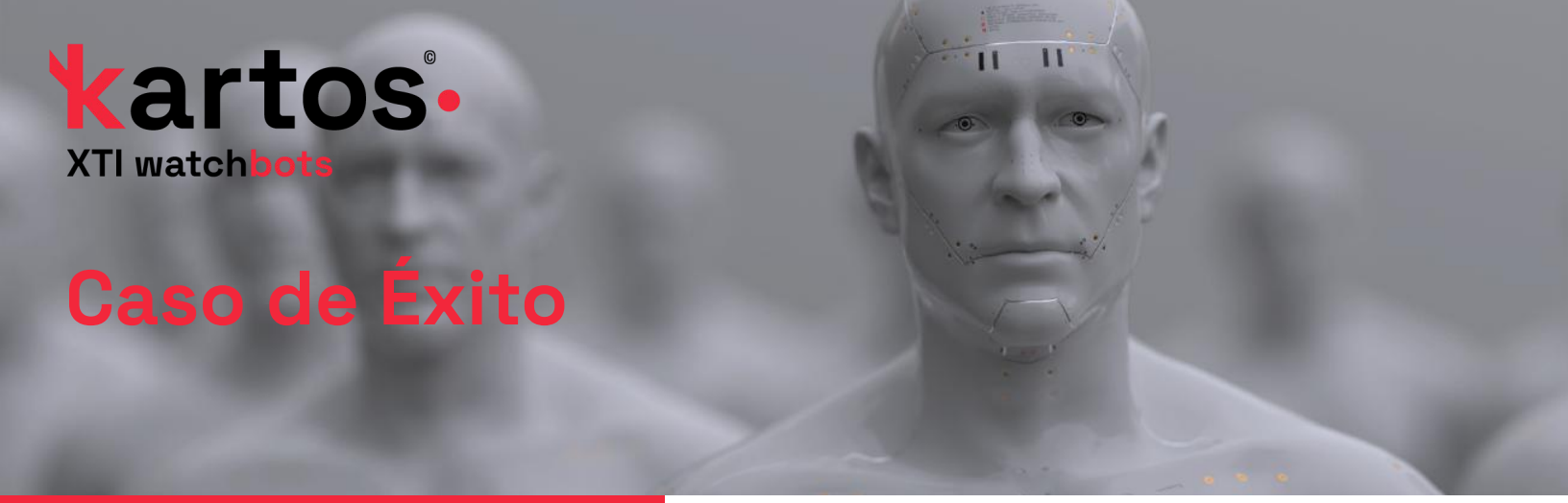
Uso de Kartos para la detección de toda la información hospitalaria filtrada y expuesta en la red, así como de las brechas de seguridad que provocan dichas filtraciones para que la institución pueda tomar las acciones que le permitan mejorar sus sistemas de defensa y protegerse de posibles ataques.

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 institución si no se encuentran bien protegidos

- Localización de historias clínicas filtradas
- Detección de contraseñas comprometidas
- Protección del sistema de consultas y operaciones
- Continuidad del servicio de atención al paciente
- Detección de brechas de seguridad del sistema
- Evaluación de colaboradores y proveedores
- Cumplimiento del GDPR

kartos©
XTI watchbots



Caso de Éxito

Nuestro cliente

Nuestro cliente es el hospital neoyorkino más antiguo de su distrito, en donde brinda servicios de salud, investigación y educación a la comunidad desde mediados del siglo XIX.

Cuenta con casi 500 camas hospitalarias, a las que suma una red de centros de salud familiar, consultorios médicos y puntos de atención ambulatoria. Su objetivo principal es el de garantizar una atención óptima al paciente a través de la cualificación y experiencia de su personal sanitario y del uso de las últimas tecnologías y tratamientos médicos más innovadores.

El reto

Un hospital es una organización que está dentro de la categoría de infraestructuras críticas, por lo que su actividad y seguridad han de estar garantizadas en todo momento. Por ello, nuestro cliente está sujeto al cumplimiento estricto del estándar para la protección de datos confidenciales de los pacientes establecido en la Health Insurance Portability and Accountability Act (HIPAA) y, por tanto, obligado implementar y mantener medidas de seguridad suficientes para sus sistemas, redes y procesos.

Después de un tiempo de observación de funcionamiento anómalo y pérdida de información en algunos de los sistemas de comunicación, la dirección del hospital se plantea la necesidad de determinar o descartar, de forma cierta, la existencia de brechas de seguridad en su sistema de TI. La especial actividad de nuestro cliente, la atención sanitara en su zona de influencia, obliga a que la toma de decisiones en cuanto a asignación de partidas de presupuesto a un gasto extraordinario en seguridad sea fundamentada, ya que la prioridad es siempre la mejora en la atención a los pacientes y la compra de maquinaria médica de última generación.

Por ello, los órganos decisorios y la gerencia del centro hospitalario contactan con Enthec Solutions para obtener una prueba concluyente de que las alteraciones en el funcionamiento de los sistemas de TI del hospital se deben a actividades de ciberdelincuencia que provocan una fuga de información y no a fallos internos de los mismos sin repercusión en la protección de los datos, antes de tomar la decisión de realizar cambios profundos en la arquitectura de ciberseguridad hospitalaria.

La solución propuesta

Tras una serie de reuniones mantenidas con el cliente, se hace evidente que es necesario realizar una investigación exhaustiva sobre los eventos que están ocurriendo relacionados con la filtración y pérdida de información que está sufriendo el hospital.

Se propone a la dirección del Hospital la **utilización de Kartos**, la plataforma de Cibervigilancia XTI, basada en Inteligencia Artificial y Machine Learning que analiza de manera continua Internet, la Deep Web y la Dark Web en busca de cualquier información filtrada sobre la compañía.

Dentro de esa propuesta, **Kartos monitorizará y analizará durante un tiempo determinado el dominio principal del Hospital y otros dominios asociados en las nueve categorías que tiene habilitadas** -Red, Salud de DNS / Phishing, Gestión de Parches, Reputación IP, Seguridad Web, Seguridad e-mail, Filtración de Documentos, Filtración de Credenciales y Redes Sociales- para luego emitir un informe exhaustivo sobre la información encontrada y los riesgos detectados asociados a dichos dominios.

El resultado

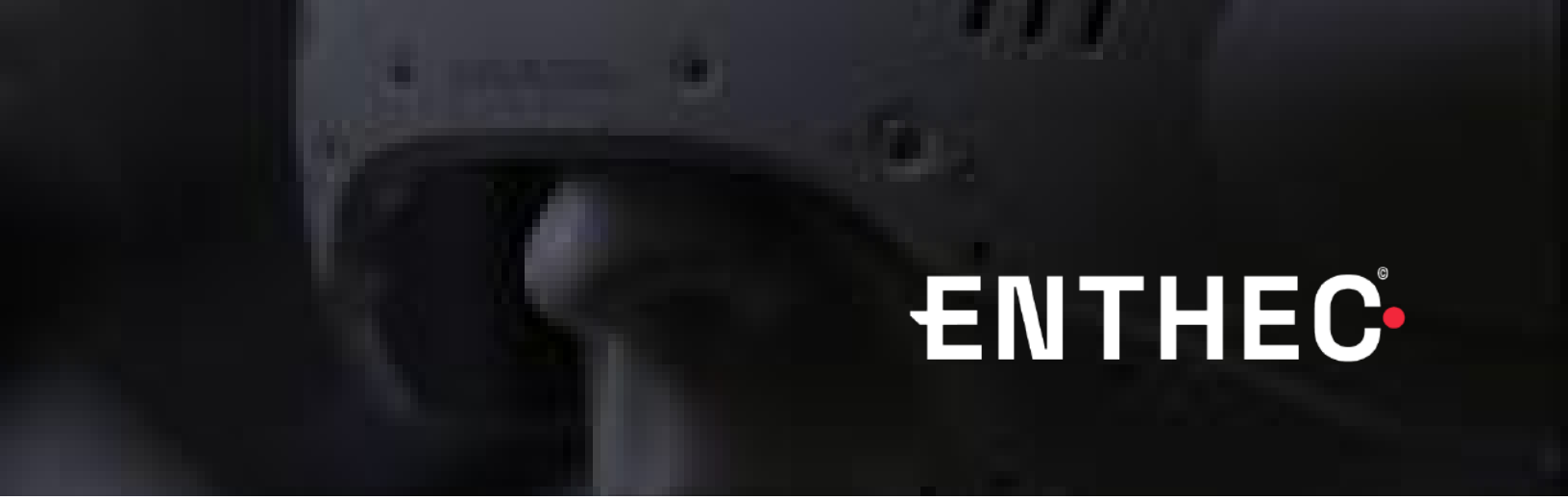
Tras recibir el informe con los resultados del análisis llevado a cabo por la plataforma Kartos de Enthec Solutions, **la dirección del Hospital obtiene la prueba cierta de la brecha de seguridad de su sistema de TI,** que está siendo aprovechada por la ciberdelincuencia para robar información confidencial crítica, y puede actuar para resolverla y acabar con una fuga de datos de la que no era consciente.

Este informe descubrió, entre otras cosas, que existía un fallo en la configuración del sistema de correo, que no había sido detectado, y que era utilizado por ciberdelincuentes como vía de entrada a la información del Hospital.

La detección de las brechas permitió tomar las siguientes **acciones inmediatas de remediación**:

- Reducción de baja encriptación.
- Actualizaciones permanentes del sistema de seguridad.
- Cambios en la política de comunicación y del correo internos.
- Endurecimiento de la política de cumplimiento de los requerimientos del HIPAA.

Una vez comprobada la eficacia de la solución aportada por Enthec Solutions y con el fin de evitar brechas de seguridad futuras, garantizar la integridad de la información confidencial alojada en su sistema y conocer en todo momento la exposición del Hospital en la Web, **el cliente toma la decisión de contratar de forma permanente el servicio de monitorización de Kartos XTI Watchbots**, a través del cual consigue la cibervigilancia XTI constante de la exposición del Hospital en la Web, Deep Web y Dark Web, información recurrente y continua sobre los datos obtenidos a partir de dicha monitorización y la detección inmediata de los fallos de seguridad sobrevenidos.



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.

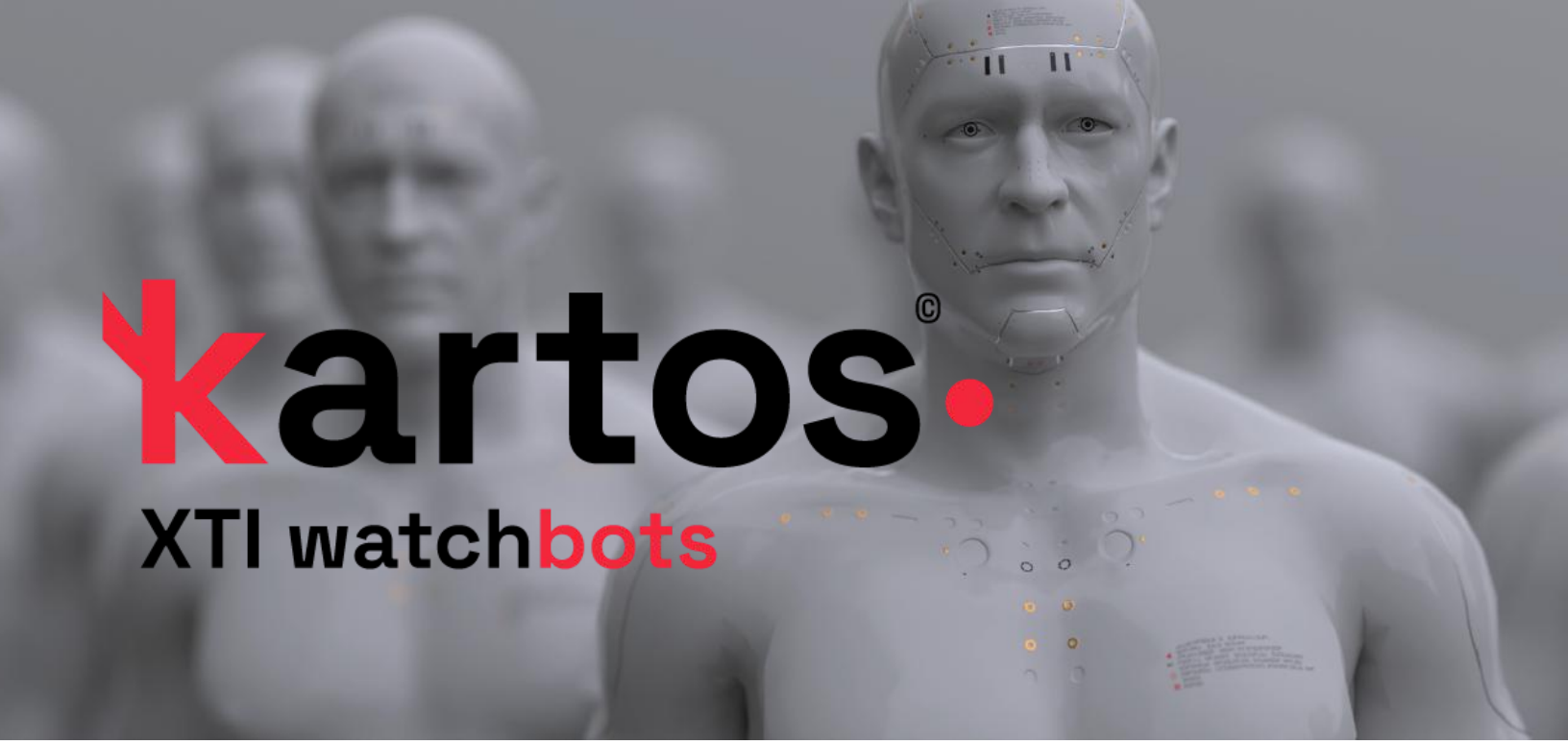
Fundada como startup en 2019 por María Rojo, Enthec ha crecido a través de rondas de financiación y del éxito de su plataforma Kartos hasta consolidarse como una de las Deep Tech con soluciones más innovadoras y eficaces en el campo de la Ciberseguridad.

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 Hospital, puedes ponerte en contacto con nosotros a través de esta dirección de correo y te contaremos los pasos para monitorizar tu dominio.

he@enthec.com



¡Gracias!