ENTHEC

WHITEPAPER

Riesgo de terceros:
CÓMO GANAR PRECISIÓN A LA HORA DE VALORARLOS

ÍNDICE

INTRODUCCIÓN

La digitalización de las organizaciones ha provocado que la interconectividad de los sistemas y la dependencia de terceros en los negocios sean comunes en el entorno empresarial actual, ganando agilidad y eficiencia. Sin embargo, esta interconexión también da lugar a una mayor exposición al ciberriesgo, lo que obliga a las organizaciones a ser más conscientes de la importancia de la **gestión de riesgos de terceros.**

Los proveedores, socios y otros terceros que tienen acceso a los sistemas y datos confidenciales de una organización representan un riesgo significativo para la ciberseguridad de la misma. Los ciberdelincuentes pueden aprovechar las debilidades de los terceros para burlar la estrategia de ciberseguridad de una organización y acceder a información sensible, robar datos e interrumpir las operaciones comerciales, entre otros. Por esta razón, es crucial que las organizaciones **evalúen y gestionen el ciberriesgo de sus terceros de manera efectiva y precisa, durante todo el tiempo que dure su relación comercial,** para garantizar la seguridad y la continuidad de las operaciones en un entorno cada vez más interconectado.

En este whitepaper vamos a analizar la importancia de la valoración del ciberriesgo de terceros dentro de una organización, los métodos comunes de valoración de ese riesgo, sus déficits y los beneficios de introducir el enfoque de cibervigilancia continua en la valoración del riesgo de terceros como complemento y refuerzo. Además, presentaremos algunos Casos de Uso para ilustrar cómo las organizaciones pueden mejorar la gestión de sus riesgos de terceros.

INFORMACIÓN OCULTA Y ENÉSIMOS

WHITEPAPER

A menudo, las organizaciones se concentran en la seguridad de su propia red y sistemas, pero descuidan la seguridad de los sistemas y datos de terceros con los que trabajan. Los proveedores, socios y otros terceros pueden tener acceso a información confidencial, lo que los convierte en un riesgo potencial para la seguridad de la organización. Tal y como señala Gartner en su informe sobre el modelo de valoración del riesgo de terceros, los líderes de las organizaciones reconocen que la conexión de sus sistemas con terceros es parte fundamental de la operativa de una organización y los riesgos no dejan de crecer por la variabilidad en la madurez de ciberprotección de los terceros, la mayor implicación de esos terceros con los activos corporativos y las crecientes conexiones de esos terceros con sus propias terceras partes. Esta imprescindible conexión con terceros conlleva dos dificultades extremas a la hora de valorar el riesgo: la información oculta y el alcance.

LA INFORMACIÓN OCULTA

Uno de los principales desafíos en la gestión de los ciberriesgos de terceros es la falta de transparencia. Muchos proveedores y contratistas no están dispuestos a proporcionar información completa sobre sus prácticas de seguridad, ya sea porque no tienen los recursos para implementar medidas de seguridad adecuadas o porque no quieren revelar detalles confidenciales sobre sus procesos.

Además, es importante tener en cuenta que, en muchos casos, los terceros pueden también no ser completamente transparentes sobre los incidentes de ciberseguridad, para no poner en peligro la continuidad de los acuerdos ni su reputación. Esto puede incluir la ocultación de brechas de seguridad, la falta de actualizaciones de software o la no notificación de estos incidentes de seguridad, lo que aumenta aún más el riesgo para la organización.

También, las organizaciones pueden no ser conscientes de que ciertos proveedores y contratistas están subcontratando servicios críticos a otros terceros sin la debida notificación. Esto puede llevar a una falta de control sobre quién tiene acceso a los sistemas y datos de la organización, lo que aumenta el riesgo de ciberataques.

EL ALCANCE: LAS ENÉSIMAS PARTES

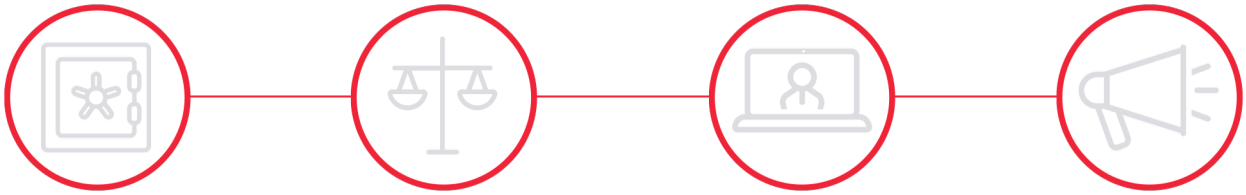
A menudo, la gestión de los riesgos de terceros pasa por alto un aspecto importante: el riesgo asociado con los terceros de terceros, también conocidos como "enésimas partes".

Las enésimas partes son los terceros de terceros, aquellos que tienen acceso a los sistemas y datos de los proveedores y contratistas de la organización original. Este complejo sistema de dependencia añade dificultad a la identificación y gestión de los riesgos de terceros. Además, las enésimas partes tienen sus propios terceros y proveedores, lo que amplía aún más la cadena de suministro y complica la evaluación de los riesgos. La organización original no tiene control directo sobre los enésimos, lo que aumenta el riesgo de que se produzcan vulnerabilidades de seguridad en la cadena de suministro. Además, los enésimos pueden ser menos transparentes que los terceros directos, lo que complica la evaluación de los riesgos asociados.

Dentro de la valoración de riesgo de terceros, el riesgo asociado a las enésimas partes comienza a ser considerado por los responsables de ciberseguridad como crítico para las organizaciones por su aparente imposibilidad no ya de controlarlo, sino simplemente de valorarlo.

LA ORGANIZACIÓN FRENTE A LOS RIESGOS DE TERCEROS

Normalmente, en todas las organizaciones está establecido que los riesgos de terceros son competencia del departamento de seguridad de la información y del departamento legal. Sin embargo, tanto el alcance de la protección como las consecuencias de los riesgos de terceros van más allá de estos dos departamentos.



Seguridad de la información
Estrategia de ciberseguridad corporativa y protección de la información de la organización.

Legal
Cumplimiento legal y efectiva protección de los datos de terceros y de la propiedad intelectual o industrial de la organización.

IT
Correcto funcionamiento, actualizaciones y renovaciones de la infraestructura tecnológica de la organizazión.

Marketing y Comunicación
Reputación de la marca y relación con los clientes.

Operaciones
Continuidad del funcionamiento operativo de la organización.

Financiero
Valoración del riesgo de terceros y sus terceros y relación con ellos.

CEO
Responsable último del negocio.

Para que exista una valoración del riesgo de terceros precisa, todos estos departamentos de una organización han de gestionar las responsabilidades sobre la protección de los riesgos frente a terceros y han de estar implicados en la propia valoración, dentro de los parámetros que implican a su área, liderados por el CISO y el departamento de seguridad de la información.

NECESIDAD DE VALORAR CON PRECISIÓN LOS RIESGOS DE TERCEROS

Una **valoración precisa del riesgo de terceros** es esencial para proteger la seguridad de la organización. Los ciberataques dirigidos a los proveedores, socios, contratistas y otras terceras partes pueden ser muy efectivos en la obtención de acceso no autorizado a los sistemas y datos de la organización. Por lo tanto, cualquier estrategia de ciberseguridad corporativa ha de contemplar la valoración eficaz de los riesgos de terceros.

La valoración de los riesgos de terceros implica **evaluar su capacidad para proteger los sistemas y datos de la organización.** Requiere examinar los procesos y políticas de seguridad, las medidas de seguridad implementadas y su eficacia real, el cumplimiento normativo y otros factores críticos que pueden afectar la seguridad de la organización.

Como punto de partida es necesario identificar y clasificar los riesgos de negocio asociados con la interdependencia de la organización con los terceros, ya que esta interdependencia implica que sus vulnerabilidades pueden tener un impacto significativo en las operaciones y la reputación de la organización.

Valorar con la mayor precisión los riesgos de terceros ayuda a las organizaciones a priorizar la gestión de riesgos y a tomar medidas preventivas adecuadas, frente a la onda expansiva de un ciberataque a un tercero.

La vulnerabilidad de terceros fue el cuarto vector de ataque en las brechas de datos de 2022 en el sector financiero y bancario

Europa Press

El 73% de las organizaciones afirma que sus terceros tienen más acceso a los activos de datos que hace tres años

Gartner

Las organizaciones reconocen dedicar solo un 27% de los recursos a identificar riesgos de terceros en el transcurso de la relación

Gartner

La valoración precisa del riesgo de terceros permite a las organizaciones:

Información

Previamente al inicio de la relación con un tercero, **tomar decisiones más informadas sobre la selección de proveedores y contratistas.** Al evaluar cuidadosamente a los proveedores y contratistas en términos de su capacidad para proteger la seguridad de la organización, las organizaciones pueden tomar decisiones más informadas sobre la contratación y la gestión de su cadena de suministro. Esto puede ayudar a reducir el riesgo de ciberataques y proteger la reputación de la organización.

Compresión

Comprender el alcance completo de los riesgos de ciberseguridad asociados con su cadena de suministro y, por lo tanto, tomar medidas preventivas adecuadas para protegerse. Al evaluar cuidadosamente a los proveedores y contratistas, las organizaciones pueden identificar las vulnerabilidades y los puntos débiles en su cadena de suministro y tomar medidas para mitigar los riesgos.

Cumplimiento

Cumplir con las regulaciones y estándares de seguridad. Las regulaciones de seguridad, como las diferentes leyes de protección de datos, requieren que las organizaciones implementen medidas de seguridad adecuadas para proteger los datos y sistemas de la organización y sus clientes. Al evaluar cuidadosamente a los proveedores y contratistas, las organizaciones pueden garantizar que cumplen con estas regulaciones y estándares.

Foco

Enfocarse en los proveedores y contratistas que representan el mayor riesgo de ciberseguridad. Al priorizar los proveedores y contratistas en función de su riesgo de ciberseguridad, las organizaciones pueden enfocar sus recursos en las áreas más críticas y reducir los costos y el tiempo asociados con la gestión de riesgos.

LA COMPLEJIDAD DE LA VALORACIÓN DEL RIESGO DE TERCEROS

La evaluación del riesgo de un tercero comienza antes de establecerse la relación contractual y debe continuar hasta que la colaboración termine y la interdependencia se extinga. Los métodos comunes de valoración son:

Previo relación

Due Diligence

Implica la valoración exhaustiva de la seguridad de los proveedores y contratistas que tienen acceso a los sistemas y datos de la organización, incluyendo la evaluación de la madurez del programa de seguridad del proveedor, la identificación de las vulnerabilidades de seguridad en los sistemas y la evaluación de la capacidad del proveedor para responder a incidentes de seguridad. Normalmente se realiza a través de cuestionarios elaborados por la propia organización.

Durante relación

Auditorías y Seguridad Ofensiva

Implica la revisión de los informes de auditoría de seguridad y las evaluaciones de riesgos realizadas por el proveedor, así como la realización y comprobación de los resultados de pruebas de Offensive Security (pent testing, Red Team...) llevadas a cabo por el tercero.

DÉFICITS

- Métodos manuales y poco objetivos basados en cuestionarios y pruebas.
- Autorización obligatoria para la realización de pruebas intrusivas.
- Costes elevados de la realización de pruebas (pentests y similares).
- Imposibilidad de verificar la exactitud de la información suministrada y la inexistencia de información oculta.
- Evaluación del riesgo en un momento determinado, sin monitorización continua del riesgo a lo largo de la relación que incluya los cambios en la misma.
- Desactualización de la información en pocos días. Imposibilidad de valorar el riesgo de enésimas partes.

A estos problemas se le añade uno que es principal y supone un riesgo crítico: la **limitación de la valoración del riesgo de terceros al perímetro interno su empresa.** La protección de la superficie de ataque externa es un problema cada vez mayor en las empresas, ya que hasta ahora ha sido imposible controlar el nivel de riesgo del perímetro IT extendido que incluye a proveedores, clientes, socios y otros terceros. Está comprobado que estos son un vector de ataque muy utilizado y, por tanto, cualquier vulnerabilidad que existe en su sistema de ciberseguridad se puede convertir automáticamente en una vía de entrada para las empresas con las que se relaciona.

Esta complejidad hace que, en general, la valoración por medios tradicionales del riesgo de terceros sea poco precisa, poco fiable y, por tanto, no sirva para diseñar una estrategia de protección eficaz frente a los riesgos de terceros.

ENFOQUE DE CIBERVIGILANCIA: CONTROL MÁS ALLÁ DEL PERÍMETRO INTERNO

Una de las principales razones por las que siguen produciéndose ciberataques con éxito en empresas es que los cibercriminales utilizan la información filtrada y expuesta en Internet, la Deep Web y la Dark Web para evitar los sistemas de defensa en los que las compañías invierten enormes cantidades de recursos. Las filtraciones de información son una llave que desbloquea cualquier defensa.

Esta realidad es la que ha dado lugar al nacimiento de un nuevo enfoque dentro de la estrategia de ciberseguridad de las organizaciones: la cibervigilancia para la Gestión Continua de la Exposición a Amenazas (CTEM)

La cibervigilancia es una estrategia de ciberseguridad basada en la **monitorización y el análisis de la Web, la Deep Web y la Dark Web de forma continuada y automatizada** para detectar en tiempo real la exposición de la organización amenazas en curso y detectar vulnerabilidades expuestas. De esta forma, una organización puede conocer en tiempo real qué información corporativa está al alcance de cualquier ciberdelincuente para así controlar y neutralizar su capacidad de ataque.

Una defensa es eficaz solo cuando se conocen de forma precisa todas las amenazas, las propias y las generadas por terceros, y cuando se controlan las vulnerabilidades tanto internas como externas.

CIBERVIGILANCIA CTEM PARA LA VALORACIÓN DEL RIESGO DE TERCEROS

Una de las principales capacidades de la cibervigilancia CTEM es la de poder utilizarse como herramienta de **Security Rating Services (SRS)**: la evaluación independiente de riesgos propios y de terceros para una visualización amplia de la madurez en ciberseguridad de cualquier organización utilizando un enfoque externo.

La herramienta **recopila en la Web, Deep Web y Dark Web datos a través de medios no intrusivos, los analiza y evalúa** la situación de seguridad del tercero utilizando una metodología de puntuación concreta. Esta información proporcionada por la cibervigilancia continua y automatizada sirve para ampliar, **completar y ponderar la información obtenida por los métodos tradicionales de evaluación de riesgos de terceros,** como la Due Diligence o la Seguridad Ofensiva, permitiendo, además, la evaluación continua y en tiempo real de dichos riesgos mientras dure la colaboración entre la organización y el tercero.

VENTAJAS DE LA MONITORIZACIÓN CTEM EN LA VALORACIÓN DEL RIESGO DE TERCEROS

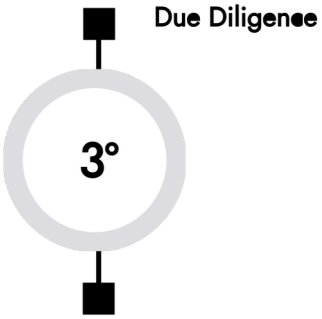
- Método de valoración objetivo que no precisa intervención humana.
- Método no intrusivo que no requiere autorización del tercero.
- Datos precisos de la filtración y exposición de la información del tercero, así como de las brechas de seguridad causantes de la filtración.
- Monitorización y análisis de forma continua y en tiempo real del riesgo de terceros mientras dura la relación comercial.
- Control de la información oculta.
- Capacidad para evaluar los riesgos de las enésimas partes.

APLICACIONES

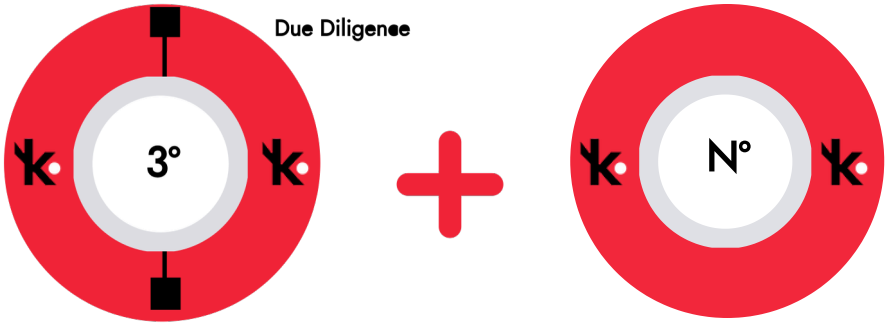
El enfoque de Gestión Continua del riesgo de Amenazas puede utilizarse para la valoración de riesgos de terceros y enésimas partes tanto en una **operación puntual** (adquisiciones, fusiones, ciberpólizas...) como en una **relación comercial duradera en el tiempo,** aportando la precisión y fiabilidad que le falta a los métodos de valoración más comunes.

VALORACIÓN PUNTUAL DEL RIESGO DE TERCEROS

SIN
KARTOS TERCERAS PARTES



CON
KARTOS TERCERAS PARTES



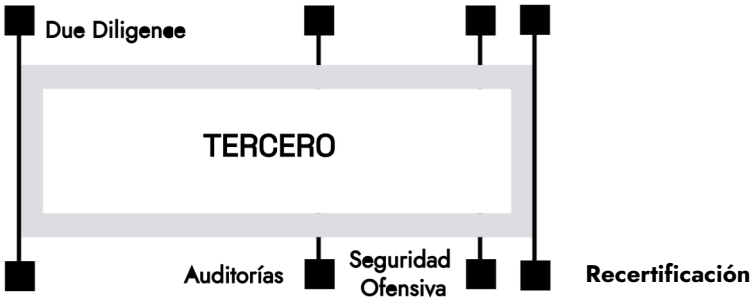
CASO DE USO

Cubrir el riesgo de una Ciberpóliza representa una decisión crítica para las Compañías Aseguradoras. Gracias al enfoque de cibervigilancia continua y automatizada en la valoración del riesgo de terceros, una Compañía Aseguradora obtiene una valoración más precisa y rigurosa del riesgo de cada Ciberpóliza y de la madurez de la estrategia de ciberseguridad del posible cliente, a la vez que puede aumentar su oferta general a sus asegurados con el Servicio de Análisis de Ciberriesgo corporativo.

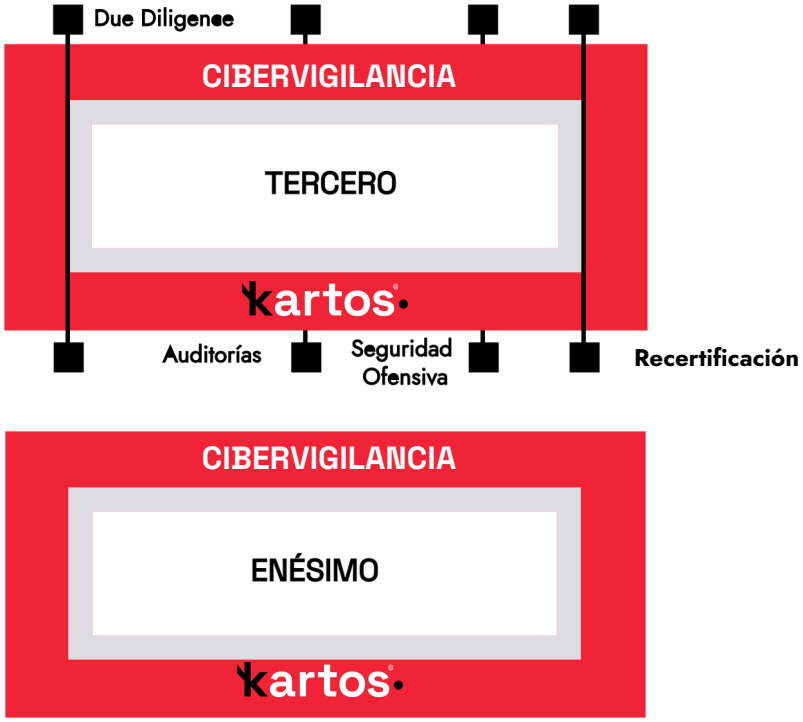
APLICACIONES

VALORACIÓN CONTINUA DEL RIESGO DE TERCEROS

SIN
KARTOS TERCERAS PARTES



CON
KARTOS TERCERAS PARTES



CASO DE USO

Los datos financieros y bancarios son considerados información sensible y cualquier filtración de los mismos, aparte de suponer una amenaza, lleva aparejada fuertes sanciones económicas. Gracias al enfoque de cibervigilancia continua y automatizada de la valoración del riesgo de terceros, un Banco monitoriza de forma continua y en tiempo real el riesgo de sus terceros y enésimos para controlar su protección frente a la fuga de información.

APLICACIONES

ESTRATEGIAS DE VALORACIÓN Y GESTIÓN DEL RIESGO DE TERCEROS CON ENFOQUE DE CIBERVIGILANCIA CTEM:

Previa

Evaluación de potenciales terceros y enésimos

- Due Diligence.
- Monitorización XTI automatizada del dominio del potencial tercero durante el tiempo de evaluación.
- Monitorización XTI automatizada de los dominios de potenciales enésimos críticos durante el tiempo de evaluación.
- Valoración de la información obtenida:
- Capacidad para afectar a la organización.
- Tiempo estimado de remediación del riesgo.

Continua

Evaluación de terceros y enésimos

- Auditorías.
- Pruebas de Seguridad Ofensiva.
- Monitorización XTI continua y automatizada de los dominios de terceros.
- Monitorización XTI continua y automatizada del dominio de enésimos críticos.
- Valoración de la información obtenida:
- Capacidad para afectar a la organización.
- Tiempo de remediación del riesgo.
- Comunicación al tercero cuando la exposición de información detectada a través de la Cibervigilancia XTI afecte a la organización.

APLICACIONES

Añadiendo una estrategia de Cibervigilancia para la Gestión Continua de la Exposición a Amenazas (CTEM) en la valoración del riesgo de terceros, la organización obtiene la capacidad de controlar 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 de los enésimos críticos asociados a ellos.

1. Valoración más precisa del riesgo de potenciales terceros y evaluación de la madurez de su estrategia de Ciberseguridad.
2. Gestión más eficaz del riesgo de terceros y enésimos a lo largo de la relación contractual y evaluación continua de su estrategia de Ciberseguridad.
3. Detección automatizada y en tiempo real de las brechas de seguridad de terceros y enésimos y valoración del grado de amenaza del riesgo para la organización.
4. Comunicación a los terceros de sus brechas de seguridad que afectan a la organización y seguimiento de su remediación.
5. Comunicación a los terceros del riesgo de enésimos asociados a sus organizaciones y seguimiento de su remediación.

ENTHEC

WHITEPAPER

kartos©

Kartos Corporate Threat Watchbots: Gestión Continua de la Exposición a Amenazas (CTEM)

Monitorización automatizada, continua y en tiempo real de la exposición a amenazas de la organización, orientada a criterios de ciberseguridad y de negocio.

SUPERFICIE EXTERNA DE ATAQUE

Localización de la información y las vulnerabilidades abiertas y expuestas de la Compañía en Internet, la Deep Web, Dark Web y las Redes Sociales: Campañas de phishing, fraude y estafa; CVEs; salud de DNS; contraseñas y credenciales filtradas; documentacióny bases de datos filtradas y expuestas.

PROTECCIÓN DEL RIESGO DIGITAL

Detección de información contextual sobre posibles agentes de ataques, sus tácticas y procesos para llevar acabo actividades maliciosas. Eliminación de actividades maliciosas en nombre de la Compañía. Protección de marca, dominio y subdominios. Protección de correo electrónico corporativo. Protección contra ransomware. Seguridad web y eliminación de amenazas.

RIESGO DE TERCEROS

Control en tiempo real del riesgo de terceros. Datos objetivos sobre amenazas en curso relacionadas con la cadena de valor. Visualización amplia de la madurez en ciberseguridad de cualquier organización utilizando un enfoque externo no intrusivo. Ampliación y ponderación de la información proporcionada por los métodos tradicionales de evaluación de riesgos de terceros.

COMPLIANCE

Monitorización de cumplimiento legal corporativo y de terceros basado en datos objetivos tomados en tiempo real. ISO 27001. PCI - DSS. ENS. RGPD. Justificación de cumplimiento de exigencias legales y normativas para asociaciones, fusiones y adquisiciones, auditorías, certificaciones y contratos con la administración

SCORING DE CIBERSEGURIDAD

Permite que la información sobre seguridad salga del despacho del CISO y se presente de manera sencilla a personas que deben participar en la gestión de la seguridad sin tener formación técnica. Scoring de ciberseguridad propio y de terceros para asociaciones, auditorías, fusiones, adquisiciones y contratos con la administración.

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

WHITEPAPER

kartos©

- **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 organizaciones, 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.

Conoce más sobre nuestras licencias.
Prueba de forma gratuita nuestra herramienta.
Empieza a usar Kartos y a controlar el riesgo de terceros.

hello@enthec.com

Enthec Solutions es una compañía tecnológica española que desarrolla software de ciberseguridad para la protección de organizaciones y personas.Enthec Solutions se ha consolidado como una de las Deep Tech con soluciones de Cibervigilancia más innovadoras y eficaces gracias al éxito de su plataforma **Kartos Corporate Threat Watchbots**, que proporciona a las organizaciones Ciberseguridad, Ciberinteligencia, Cyberscoring, Compliance y Capacidades de Gestión del Riesgo de Terceros, y a su innnovadora plataforma **Qondar Personal Threat Watchbots** para la protección online individual de las personas relevantes de la organización.

www.enthec.com