kartos®
XTI watchbots

Controla toda la información que los cibercriminales conocen de tu empresa.

Las filtraciones de información son la llave que desbloquea cualquier defensa.
Una de las principales razones por las que seguimos viendo ataques con éxito en empresas es que los cibercriminales utilizan la información filtrada en Internet, la Deep Web y la DarkWeb para evitar los sistemas de defensa en los que las compañías invierten enormes cantidades de dinero todos los años.
Esto convierte en inútil gran parte de esa inversión.

Kartos es la herramienta de ciberseguridad que de forma no intrusiva y en tiempo real captura toda la información que está públicamente disponible en Internet, la Deep Web y la DarkWeb, y la entrega a las empresas para que puedan plantear una estrategia defensiva antes de que los cibercriminales la utilicen para ejecutar un ataque.

- 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 y funciona de manera autónoma, sin necesidad de configurar parámetros de búsqueda ni de cualquier otro criterio de localización de información.

- Herramienta que permite la monitorización automatizada, objetiva y continúa de los riesgos causados por las terceras partes que pertenecen a la Superficie de Ataque Externa de la empresa.

HOJA DE PRODUCTO

FUNCIONALIDADES

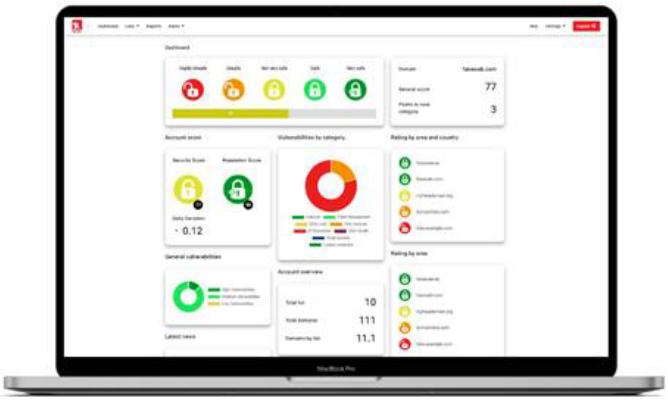
Análisis de 9 Categorías de Amenazas Red
Red
Salud de DNS / Phishing
Gestión de Parches
Reputación IP
Seguridad Web
Seguridad e-mail
Filtración de Documentos
Filtración de Credenciales
Redes Sociales

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.
Detecta conversaciones en redes relacionadas con hacktivismo, fraude, phishing o campañas de fakenews, entre otras.

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

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.

kartos®
XTI watchbots



CASOS DE USO

Detección de Amenazas Propias
Uso de Kartos para la detección de toda información filtrada en la red sobre una empresa para que esta pueda tomar las acciones que le permitan mejorar sus sistemas de defensa y protegerse de posibles ataques.

Riesgos de Terceros
Uso de Kartos como herramienta de EASM (ExternalAttackSurface Management) para establecer y evaluar unos parámetros mínimos de cumplimiento de medidas de Ciberseguridad de los terceros que pueden comprometer a la empresa si no se encuentran bien protegidos.

Evaluación de Proveedores
Uso de Kartos en empresas cuyo principal negocio es la evaluación de proveedores, de forma que a la evaluación de riesgo financiero pueden añadir también una evaluación del riesgo IT como factor crítico de riesgo corporativo.