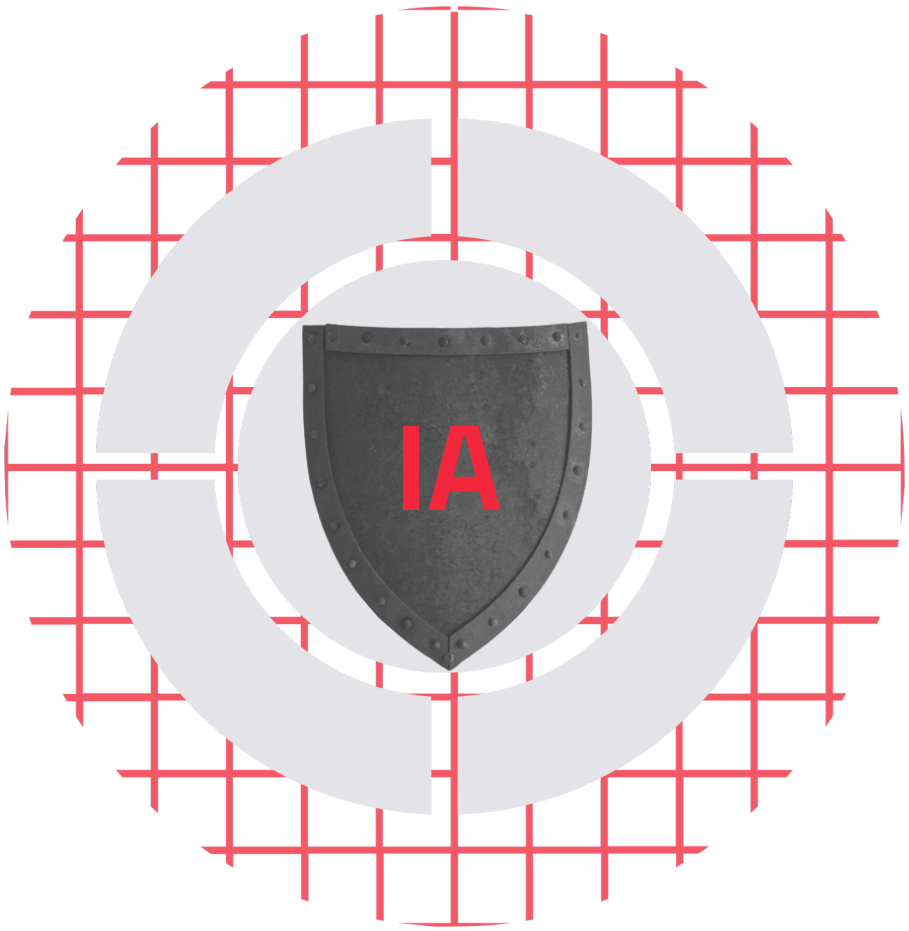
ENTHEC

WHITEPAPER

CIBERINTELIGENCIA DE AMENAZAS

La IA extiende el alcance de la ciberseguridad



ÍNDICE

INTRODUCCIÓN

La ciberseguridad nació ligada a los conceptos de perímetro interno y gestión del riesgo: las organizaciones estaban en la primera fase de su transformación digital, la complejidad de sus sistemas de IT era pequeña, la ciberdelincuencia estaba empezando y los ataques eran poco sofisticados. En ese escenario, el enfoque estratégico de proteger el perímetro interno de las organizaciones a través de su blindaje y gestionar el riesgo era la más efectiva, asequible y racional. No era necesario ir más allá.

Sin embargo, el tiempo ha pasado y la velocidad de la innovación tecnológica y su impacto en los mercados han inyectado complejidad tanto en los sistemas IT corporativos como en las relaciones entre organizaciones y han permitido la sofisticación de los ataques de la ciberdelincuencia.

La operativa en la nube, la entrada de terceros en los sistemas internos, la conexión entre sistemas propios y de terceros y la utilización de las últimas tecnologías por parte de los ciberdelincuentes dejan hoy sin efectividad el enfoque estratégico limitado al perímetro interno y la gestión del riesgo, principalmente por dos factores:

- La poca eficacia de sus resultados, tal y como demuestran la cantidad de ciberataques con éxito que crece imparable cada año y el perfeccionamiento de las técnicas de ingeniería social.
- El coste en recursos de blindar sistemas y gestionar riesgos cada vez más complejos y en continua expansión.

A pesar de esta ineficacia manifiesta, el enfoque inside-out de la ciberseguridad sigue siendo la base de la mayoría de las estrategias de ciberseguridad corporativas, provocando que las políticas corporativas de ciberprotección hayan entrado en una dinámica formada por su coste, sus malos resultados y la resistencia del board a nuevas inversiones en ciberseguridad, que afecta de lleno a la labor del CISO. Pese a que la ciberseguridad es hoy un problema de riesgo empresarial, que afecta directamente a la supervivencia y sostenibilidad del negocio, los CISOS siguen teniendo que pelear por la asignación de recursos.

INTRODUCCIÓN

Cambiar este enfoque, ampliar el perímetro controlado y utilizar nuevas tecnologías como la IA para abaratar los costes es la evolución que necesitan las estrategias de ciberseguridad para superar este bucle y hacer disminuir las cifras de éxito de los ciberataques.

Las organizaciones ya no son pequeñas tribus aisladas que puedan defenderse de ataques que desconocen atrincherándose detrás de una muralla.

Las organizaciones son hoy entidades complejas con perímetros extendidos de difícil delimitación, que necesitan, además de estrategias de defensa y protección, estrategias de inteligencia que le permitan gestionar, junto con el riesgo, la exposición a las amenazas, herramientas capaces de infiltrarse en el territorio donde opera el enemigo para obtener información sobre sus tácticas y recursos. Seguir un mantra grabado en las estrategias militares desde hace miles de años y ejecutado a través del espionaje: en entornos complejos, la información es la base de la estrategia de protección.

En este documento estudiaremos y compararemos las estrategias de ciberseguridad perimetral y de ciberseguridad extendida, el enfoque inside-out tradicional frente al emergente enfoque outside-in y cómo la IA es uno de los factores determinantes del éxito del nuevo paradigma en ciberseguridad: la ciberinteligencia de amenazas.

CIBERSEGURIDAD PERIMETRAL: LA GESTIÓN DEL RIESGO

La estrategia de ciberseguridad perimetral se basa en un enfoque inside-out y la gestión del riesgo: se protege y blinda el perímetro interno corporativo de acuerdo con los datos obtenidos de las hipótesis planteadas en el proceso de gestión del riesgo. Una vez blindado el perímetro se realizan periódicamente diferentes pruebas de simulación de ataques para comprobar la eficacia del blindaje y hacer las correcciones y actualizaciones necesarias.

> La estrategia de ciberseguridad perimetral es la más elemental, funciona con eficacia en entornos simples y es siempre la base sobre la que han de implementarse el resto de las estrategias.

En un entorno simple, con sistemas IT sencillos, perímetros corporativos bien definidos y ciberataques poco sofisticados, la estrategia de ciberseguridad perimetral puede ser suficiente y suponer un coste de recursos asequible para la organización.

Pero ese entorno simple, si alguna vez existió, hoy ha desaparecido y no volverá.

Las organizaciones y sus órganos de dirección han de ser conscientes de que el entorno digital en el que hoy se mueven sus negocios es complejo y no va a dejar de serlo, y por eso nunca van a volver a dar buenos resultados las estrategias de ciberseguridad basadas en hipótesis que así lo consideren.

Blindar el perímetro interno de las organizaciones sigue siendo fundamental y necesario, pero en un entorno complejo como el actual es insuficiente.

CIBERSEGURIDAD PERIMETRAL: LA GESTIÓN DEL RIESGO

·La ciberdelincuencia ha alcanzado un alto nivel de sofisticación y éxitos gracias a la utilización de nuevas tecnologías como la IA y al perfeccionamiento de las técnicas de ingeniería social.

> En 2022 las notificaciones por brechas de datos fueron un 6´3% más que en el año anterior, constituyendo el ransomware y los accesos no autorizados los principales ataques ejecutados.
> Datos de la Agencia Española de Protección de Datos (AEDP).

·Gran parte de las soluciones, operaciones y de la información de las organizaciones se aloja en nubes y aplicaciones de terceros.

> En 2022 aumentó en un 55% el número de usuarios que incrementaron el presupuesto en soluciones cloud. Las previsiones señalan que el mercado cloud crecerá más de un 21% en2023.
> Informe del Mercado Cloud en España 2022. Quint 2023

·Terceros como socios, proveedores y colaboradores con frecuencia tienen entrada en los sistemas internos de las organizaciones.

> 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

LIMITACIONES DE LA CIBERSEGURIDAD PERIMETRAL

Nuestra tribu ha crecido, la muralla que antes servía para mantenerla blindada y segura no alcanza ni a los recursos y armas que se guardan en almacenes de otras tribus, porque en la nuestra ya no caben, ni a las llaves de la muralla con las que cuentan habitantes de otras tribus que colaboran con la nuestra ni a los enemigos disfrazados con nuestros uniformes que consiguen bajo engaño la contraseña para abrir nuestras puertas. Los ciberdelincuentes tienen ahora capacidad de entrar con los mismos medios con los que entra un empleado o un tercero en la organización. ¿Qué capacidad para evitar este tipo de ofensiva tiene la ciberseguridad perimetral?

Pese a constituir la estrategia básica, la ciberseguridad perimetral en entornos complejos tiene unas limitaciones que destruyen su eficacia:

La gestión del riesgo trabaja sobre hipótesis

El cálculo de los riesgos que sirve para dimensionar y diseñar la estrategia de ciberseguridad perimetral se basa en la cuantificación de todos los riesgos y amenazas posibles, incluyendo a los ocurridos y conocidos y a los que se imagina que tienen probabilidad de ocurrir. Esta es la primera serie de hipótesis que afecta al resultado: la de la probabilidad. La segunda, encierra a todos aquellos ataques que ni siquiera se conocen, pero que han de entrar en el cálculo, para contar con lo imprevisto.

De esta forma, las estrategias de ciberseguridad perimetral tienden a manejar datos poco sólidos, a veces deformados por el sesgo del analista y con tendencia al alza para poder cubrir la ciberprotección frente a un número desconocido de riesgos con un grado desconocido de amenaza.

LIMITACIONES DE LA CIBERSEGURIDAD PERIMETRAL

El riesgo de terceros

La ciberseguridad perimetral tiene poca eficacia frente al riesgo de terceros. Un fallo en la seguridad del tercero provoca que la ofensiva del ciberataque se lleve a cabo sin ser detectada. Además, la gestión del riesgo de terceros se lleva a cabo comprobando el cumplimiento de una serie de requisitos a través de cuestionarios y de los resultados de pruebas puntuales de intrusión, a modo de foto fija. Unas comprobaciones y pruebas que no pueden alcanzar a los cuartos o enésimos (terceras partes de las terceras partes de la organización).

La complejidad de los sistemas IT de las organizaciones

La ciberseguridad perimetral tiene poca eficacia frente al riesgo de terceros. Un fallo en la seguridad del tercero provoca que la ofensiva del ciberataque se lleve a cabo sin ser detectada. Además, la gestión del riesgo de terceros se lleva a cabo comprobando el cumplimiento de una serie de requisitos a través de cuestionarios y de los resultados de pruebas puntuales de intrusión, a modo de foto fija. Unas comprobaciones y pruebas que no pueden alcanzar a los cuartos o enésimos (terceras partes de las terceras partes de la organización).

La sofisticación de los ciberataques

El factor determinante de cualquier estrategia de protección y defensa es la capacidad del enemigo. En ciberseguridad este factor se traduce en un adversario que utiliza técnicas en permanente innovación y que cuenta con el factor humano jugando a su favor. La ciberdelincuencia incorpora en poco tiempo y con gran efectividad cualquier innovación tecnológica. Nuevas tecnologías como la IA o el Machine Learning ya son utilizadas para conseguir la información que sirve para abrir el camino de un ciberataque. La capacidad de crear deep fakes impacta de lleno en la vulnerabilidad del factor humano, el eslabón más débil de cualquier estrategia de ciberseguridad. Y la capacidad de rastreo y análisis en busca de información de las organizaciones, perfecciona esta capacidad, contra la que la ciberseguridad perimetral tiene muy pocas defensas.

LIMITACIONES DE LA CIBERSEGURIDAD PERIMETRAL

El coste del blindaje perimetral

El coste de recursos para mantener el blindaje eficaz y actualizado en el que se basa la estrategia de ciberseguridad perimetral es inasumible para cualquier organización, ya que se calcula sobre hipótesis que sobrevaloran los riesgos y los niveles de amenaza para no fallar y, además, tienen que alcanzar a un sistema IT corporativo en permanente crecimiento, lo que conlleva que ese coste tienda a infinito. Esto provoca que la ciberseguridad se termine concibiendo dentro de la dirección como un gasto que ralentiza el crecimiento del negocio y no como una inversión en el mismo.

La incorrecta evaluación del impacto empresarial del riesgo

La consecuencia de que la gestión del riesgo trabaje sobre hipótesis es que la evaluación del impacto empresarial del riesgo también lo hace. Por ellos, la evaluación del impacto empresarial del riesgo adolece de los mismos problemas que la evaluación del mismo a través de hipótesis: trabajo con datos poco sólidos, a veces deformados por el sesgo del analista y con tendencia al alza para poder cubrir la ciberprotección frente a un número indefinido de impactos de un tamaño sin determinar. Esto, además de la natural sobrevaloración de los impactos para cubrirse las espaldas, provoca que el resto de los departamentos y la dirección se impliquen muy poco en la propia valoración y los resultados de la valoración contengan mayor inexactitud.

> La falta de datos significa que no podemos validar una estimación de riesgo o revisar la precisión histórica de estimaciones de riesgo anteriores. Los procesos de evaluación y cuantificación de riesgos formalizados codifican creencias de ciberseguridad erróneas sobre amenazas, vulnerabilidades y vínculos entre la infraestructura y los procesos comerciales.
> Maverick Research: la gestión de riesgos produce mala ciberseguridad. Gartner 2023

Todos estos límites hacen que la estrategia de ciberseguridad perimetral acabe cayendo en una dinámica que impacta de lleno en el trabajo del CISO:

Alto coste en recursos + Baja eficacia =
Resistencia de la dirección a invertir en ciberseguridad

CIBERSEGURIDAD EXTENDIDA: LA GESTIÓN A LA EXPOSICIÓN A AMENAZAS

Un entorno complejo requiere una estrategia de ciberseguridad con capacidad para ser eficiente y asequible con independencia de dicha complejidad y sus variaciones. La estrategia de ciberseguridad perimetral, o enfoque inside-out de ciberprotección, resulta ineficiente y costosa cuando el entorno se vuelve complejo.

La necesidad de ampliar el alcance y cambiar a un enfoque outside-in para recabar información que sirva de base para diseñar la estrategia de ciberseguridad fue detectada hace miles de años en la protección militar: la inteligencia militar. Trasladar este paradigma militar a las estrategias de ciberseguridad es hoy imprescindible para lograr una ciberseguridad avanzada de nivel evolucionado capaz de dar las respuestas en eficacia y costes que necesita el entorno actual.

La ciberseguridad extendida, además de incluir la gestión de los riesgos, se enfoca en gestionar la exposición a las amenazas. Sale más allá del perímetro interno de las organizaciones para encontrar las vulnerabilidades que amenazan a la organización y que están al alcance de cualquier ciberdelincuente, para permitirle diseñar una estrategia de ciberportección contra esa amenaza determinada, detectar cuál es la brecha de seguridad que la ha provocado y eliminarla, y controlar el tiempo de exposición a dicha vulnerabilidad.

La ciberseguridad extendida y el enfoque outside-in centran su eficacia en el valor de la información en cualquier estrategia de seguridad, en extender la ciberinteligencia más allá del perímetro de las organizaciones para trabajar sobre información real y no sobre hipótesis.

CIBERSEGURIDAD EXTENDIDA: LA GESTIÓN A LA EXPOSICIÓN A AMENAZAS

Salir fuera del perímetro de la organización para conocer la información corporativa con la que cuentan los ciberdelincuentes, qué brechas de seguridad están explotando y cuáles son las tácticas asociadas a una vulnerabilidad que pueden utilizar, es decir, gestionar la exposición a las amenazas a través de la ciberinteligencia, permite que la respuesta de la organización sea anterior al ataque, rápida, precisa, eficaz y sin implicar un alto coste de recursos. Estrategia de ciberinteligencia extendida que alcanza la gestión de la exposición a amenazas por causas internas, y también, la exposición a amenazas por causas de terceros.

> Suposición de planificación estratégica de Maverick: para 2030, las juntas directivas se basarán en los datos de exposición a amenazas resumidos por IA para priorizar las inversiones, en lugar de las evaluaciones de riesgos de ciberseguridad, frente a menos del 1% en 2023.
> Maverick Research: la gestión de riesgos produce mala ciberseguridad. Gartner 2023

CIBERINTELIGENCIA DE AMENAZAS: LOCALIZACIÓN Y DEFINICIÓN DEL RIESGO

La ciberseguridad extendida tiene como finalidad gestionar la exposición a amenazas. La base de su estrategia es la ciberinteligencia extendida, que, localiza las vulnerabilidades expuestas y brechas de seguridad corporativas al alcance de cualquier ciberdelincuente para eliminarlas o tomar las medidas capaces de contrarrestarlas en el caso de que sean utilizadas para ejecutar un ciberataque.

Localizar un riesgo permite definirlo, conocer su alcance y diseñar la estrategia más efectiva para eliminarlo.

La misión de la ciberinteligencia extendida es vigilar y rastrear 24x7 el perímetro exterior de la organización donde se mueven los ciberdelincuentes para localizar y definir los riesgos internos y de terceros y trasladar en tiempo real la información al departamento de seguridad corporativo o al MSSP correspondiente.

Si bien en las primeras etapas de la ciberseguridad, esta capacidad quedaba fuera del alcance de las organizaciones, la eclosión de nuevas tecnologías como la IA o el Machine Learning han permitido la aparición de soluciones automatizadas capaces de rastrear la Web, la Deep Web y la Dark Web del mismo modo en el que lo hacen los ciberdelincuentes. La ciberinteligencia extendida permite a las organizaciones ir por delante de los ciberdelincuentes, ya que la vigilancia automatizada y continua permite que las amenazas se localicen y definan en el momento de surgir y así neutralizarlas antes de que un ciberdelincuente haya tenido tiempo de planificar cómo utilizarlas.

CIBERINTELIGENCIA DE AMENAZAS: LOCALIZACIÓN Y DEFINICIÓN DEL RIESGO

La exposición en el tiempo a una amenaza aumenta su peligrosidad de forma exponencial.

Cuando una organización tiene la capacidad de localizar la amenaza y definir el riesgo asociado justo en el momento en el que se crea la vulnerabilidad, tiene la capacidad de adelantarse al ciberdelincuente que haya localizado también esa misma amenaza y se disponga a utilizarla para ejecutar un ataque. La IA permite a las organizaciones contar con capacidad para clasificar las amenazas localizadas por categorías y conocer las actuaciones más eficaces para anularlas, todo ello si intervención humana.

Siguiendo con el símil de nuestra tribu, la ciberinteligencia extendida sería contar con un ejército de espías recabando y trasladando de forma continua información desde el terreno enemigo.

Si la ciberdelincuencia ha ganado eficacia sin un aumento de costes gracias a la utilización de las nuevas tecnologías, a la ciberseguridad no le queda otra opción que evolucionar igual para conseguir hacerle frente.

CIBERINTELIGENCIA DE AMENAZAS: EVALUACIÓN DEL IMPACTO EMPRESARIAL

El cálculo del impacto empresarial es imprescindible para la optimización de los recursos dedicados a la ciberprotección.

Cuando la estrategia de ciberseguridad de una organización se limita a blindar el perímetro, la evaluación del impacto empresarial de los riesgos se hace tomando como base las hipótesis utilizadas para calcular los riesgos. La implicación del resto de departamentos de la organización y de la dirección en el cálculo del impacto empresarial es pequeña, ya que es difícil que trabajar sobre la base de esas hipótesis fuera del entorno de la ciberseguridad. Además, como ya hemos señalado, las hipótesis cuentan siempre con el sesgo del analista y tienden a sobrevalorar tanto los riesgos como sus impactos para asegurar la protección de la organización, con la consecuencia de que las cifras de recursos necesarios para la estrategia de ciberseguridad también lo están.

Cuando una organización opta por la estrategia de ciberinteligencia extendida más allá del perímetro, la capacidad de localizar y definir los riesgos permite a las organizaciones evaluar con precisión el impacto empresarial de los mismos y destinar los recursos necesarios para minimizarlo.

La gestión de la exposición de amenazas a través de la ciberinteligencia extendida facilita el cálculo del impacto empresarial, ya que no se trabaja sobre hipótesis, sino sobre la información obtenida a través de la monitorización automatizada y continua de las amenazas, y permite implicar en el cálculo del impacto a los departamentos que pueden verse afectados y la dirección. La consecuencia es que se obtienen cálculos más precisos del impacto empresarial de cada riesgo determinado y se dedican solo los recursos necesarios para anularlo

EL PAPEL DE LA IA EN LA CIBERINTELIGENCIA DE AMENAZAS

El desarrollo de la ciberinteligencia de amenazas ha sido una de las innovaciones que ha aportado a la ciberseguridad la eclosión de la IA.

La Dark web y Deep web, que junto con la Web conforman el perímetro externo de las organizaciones, son entornos que albergan contenido no indexado por los motores de búsqueda convencionales.

Estas partes de la red son utilizadas por cibercriminales para llevar a cabo actividades ilegales, como el intercambio de información filtrada, la venta de datos robados, la propagación de malware y otros ciberdelitos.

La IA desempeña un papel esencial en la actividad principal de la ciberinteligencia de amenazas: la monitorización y detección de amenazas en la capa visible y en las capas ocultas de Internet.

Utilizando algoritmos de aprendizaje automático y técnicas de procesamiento de lenguaje natural, la IA analiza grandes volúmenes de datos en tiempo real para identificar información corporativa filtrada, detectar patrones y señales de actividades sospechosas. Esto incluye la localización de contraseñas comprometidas, la detección de conversaciones relacionadas con la venta de información filtrada corporativa o la identificación de la organización como objetivo de futuros ciberataques.

Además, la IA puede ayudar en la identificación de fuentes de filtraciones de datos y en la evaluación de su autenticidad.
Mediante el análisis de metadatos, la comparación de información con fuentes confiables y el seguimiento de la cadena de custodia, la IA puede determinar si la información filtrada es genuina y qué medidas deben tomarse para mitigar los riesgos asociados. De esta forma, se evitan falsos positivos y el gasto en recursos que llevan aparejados.

EL PAPEL DE LA IA EN LA CIBERINTELIGENCIA DE AMENAZAS

La detección temprana de información corporativa filtrada más allá del perímetro interno, en la Web, Dark web y Deep web, permite a las organizaciones y a las autoridades competentes tomar medidas proactivas para proteger los datos, cerrar las brechas de seguridad y prevenir el impacto empresarial del ciberataque. Esto incluye la notificación a los departamentos afectados, el refuerzo de las medidas de ciberseguridad necesarias y la implementación de estrategias para rastrear y desmantelar el ciberataque antes de que tenga éxito.

La naturaleza evolutiva de la IA hace que su adaptación a los continuos cambios derivados de la sofisticación de la ciberdelincuencia no sea compleja, revelándose de esta forma como la mejor arma para hacer frente al reto de los modernos ciberataques.

La utilización de la IA ha logrado romper el límite que el perímetro de las organizaciones establecía a las estrategias de ciberseguridad. Complementada con otras innovaciones tecnológicas como la automatización y el Machine Learning, han convertido a la ciberinteligencia de amenazas en una estrategia evolucionada de ciberseguridad que gana en efectividad reduce costes de recursos y es capaz de obstaculizar los ciberataques de última generación.

Ciberinteligencia de amenazas + IA

Localización de vulnerabilidades en tiempo real

Definición del riesgo

Análisis del impacto empresarial

Definición y ejecución de actuaciones

VENTAJAS DE LA CIBERINTELIGENCIA DE AMENAZAS Y EL ENFOQUE OUTSIDE-IN

- Trabajo sobre datos ciertos y no sobre hipótesis ni sesgos.
- Localización de vulnerabilidades en tiempo real.
- Racionalización del uso de recursos en ciberseguridad.
- Implicación de la dirección y el resto de los departamentos en la estrategia de ciberseguridad.
- Utilización de la IA para la localización y definición de los riesgos.
- Utilización de la IA para el análisis del impacto empresarial de las amenazas.
- Localización de vulnerabilidades que pueden ser utilizadas para elaborar técnicas de ingeniería social.
- Innovación y facilidad de actualización y escalamiento de las herramientas de ciberinteligencia.
- Automatización, monitorización, localización de la información y análisis de los riesgos sin intervención humana.
- Localización y definición del riesgo de terceros y enésimos.
- Capacidad de la estrategia de ciberseguridad extendida no dependiente del tamaño o las circunstancias internas de la organización, sino de la potencia de la solución y de su desarrollo.
- Aportación de datos de valor al diseño de las pruebas de intrusión sobre el blindaje interno.

La gestión de la superficie externa de ataque (EASM) proporciona un valioso contexto de riesgo e información procesable a través del análisis continuo, para evaluar y priorizar los riesgos y vulnerabilidades localizados. La gestión de la superficie externa de ataque es una prioridad para los equipos de seguridad y los administradores de riesgos de seguridad. Gartner, Peer Insights

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 des 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

→ 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