Defensa gestionada de la superficie de ataque: Un único programa para todo el ciclo de respuesta

El reto empresarial

En abril de 2026, el Proyecto Glasswing de Anthropic implementó, entrenó y probó un modelo de IA de vanguardia para detectar vulnerabilidades críticas, lo que sacó a la luz miles de fallos hasta entonces desconocidos en todos los principales sistemas operativos y navegadores, algunos de ellos sin detectar durante décadas. Ahora los proveedores se apresuran a aplicar parches siguiendo un calendario de divulgación controlado, lo que ha desencadenado una oleada coordinada de parches sin precedentes en el sector.

Para la mayoría de las organizaciones, el reto no es la concienciación, sino la capacidad. El desarrollo de exploits asistido por IA ha reducido el plazo de instrumentalización de días a horas. Los equipos de seguridad ya están al límite de sus capacidades, sin un departamento dedicado a las operaciones de parches ni personal de refuerzo al que recurrir. Los reguladores esperan una respuesta demostrable ante un incidente conocido. Los consejos de administración ya están planteando preguntas. Y la amenaza no puede esperara largos ciclos de adquisición ni a relaciones inconexas con los proveedores.

Nuestra solución

Insight Managed Exposure Defence es un servicio gestionado integrado, diseñado específicamente para esta situación, que combina cinco capacidades integradas en un único programa que permite a las organizaciones pasar de un estado de exposición a un entorno protegido a la velocidad que exige la amenaza. En lugar de tener que coordinar herramientas puntuales inconexas y proveedores distintos, las organizaciones obtienen una cobertura integral de todo el ciclo de respuesta ante vulnerabilidades con una responsabilidad unificada.

El alcance y el precio del programa pueden determinarse en un plazo de 24 horas desde el primer contacto, y es escalable desde 100 activos gestionados hasta el nivel de una gran empresa sin necesidad de personalizaciones, lo que proporciona un alivio operativo inmediato independientemente del tamaño de la organización.

Características y ventajas

Un contrato. Un equipo. Una respuesta.

Insight cubre las cinco etapas del ciclo de respuesta con un único equipo de ejecución. Sin vacíos de responsabilidad entre proveedores ni costes adicionales de coordinación.

Definición del alcance y presupuesto en 24 horas

Desde la primera conversación hasta un entorno protegido, sin los largos ciclos de contratación que la amenaza no puede esperar.

Escalable desde 100 activos hasta nivel empresarial

Implementación lista para usar a cualquier escala, sin necesidad de desarrollos a medida ni compromise mínimo de complejidad.

Diseñado para Cumplimiento normativo

Alineado con los principales marcos normativos: NIS2, DORA, GDPR, etc. Registro de auditoría integrado desde el primer día.

Resultado

Con Insight Managed Exposure Defence, la mentalidad pasa de «¿Cómo respondemos?» a «Ya está todo bajo control». Las organizaciones obtienen un alivio operativo inmediato frente a una amenaza que supera su capacidad interna, un historial de medidas de defensa que satisface a los organismos reguladores y a los consejos de administración, y la confianza que supone saber que un único socio se encarga de toda la respuesta.

Cinco etapas. Un solo Insight.

Lo que nos diferencia es nuestra oferta integral.

Ofrecemos cobertura en cada etapa del ciclo de respuesta: detección de vulnerabilidades, visibilidad de la cadena de suministro de software, remediación a nivel operativo, corrección a nivel de código, y detección y contención de ataques, todo en un único contrato y con un equipo de ejecución unificado.

Managed CTEM

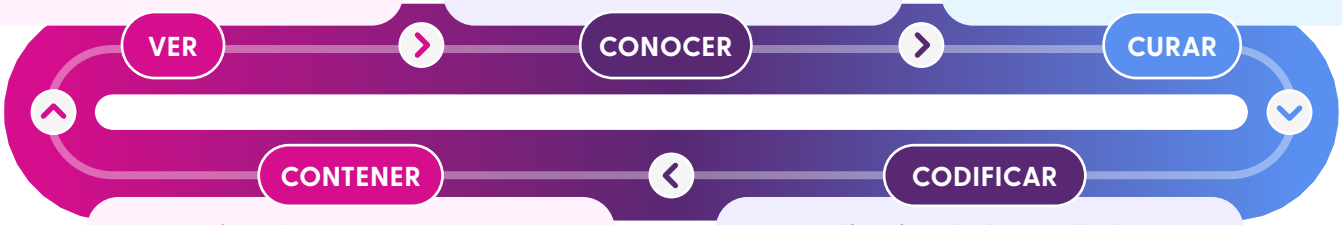
Escaneo continuo de terminales, la nube, identidades y aplicaciones, que ofrece un mapa de exposición en tiempo real y clasificado por niveles de riesgo. La base sobre la que se sustenta toda la respuesta.

Cadena de suministro de software y riesgo de OSS

Generación de SBOM, monitorización de dependencias open source y revisión de las condiciones contractuales de los proveedores. Visibilidad sobre el contenido de lo que ejecutas.

Gestión de parches

Operaciones de aplicación de parches a escala empresarial en Windows®, Linux®, hipervisores y la capa de base de datos. Despliegue con gestión de cambios, con ciclos de prueba, reversión y un registro de auditoría con marca de tiempo.



XDR gestionado

Detección, clasificación y respuesta 24/7/365 desde un centro de operaciones de seguridad (SOC) global con presencia en EE. UU., Reino Unido, India y Manila. La red de seguridad para cuando los parches se retrasan.

Externalización de desarrolladores de software

Aumenta la capacidad de ingeniería para actualizaciones de dependencias, refactorizaciones de bibliotecas y remediación de aplicaciones personalizadas. Resuelve los prolemas a nivel de código sin paralizar la hoja de ruta de tu producto.

¿Quieres ir más allá?

GRC Assessment

Evalúa la postura de gobernanza, riesgo y cumplimiento de tu organización en los principales marcos del sector, identificando las deficiencias y trazando una hoja de ruta clara para estar preparado para las auditorías.

Pruebas de penetración y pruebas de penetración continuas

Consigue una validación proactiva de tu postura de seguridad mediante escenarios de ataque simulados, confirmando que los parches y controles funcionan según lo previsto.

Gobernanza gestionada de la IA

Permite a las organizaciones escalar la IA de forma responsable al proporcionar visibilidad continua, información sobre la gobernanza y recomendaciones prácticas sobre uso, agentes, identidades y costes.

¿Por qué Insight?

Insight Enterprises es un integrador de soluciones líder que ayuda a sus clientes a resolver retos tecnológicos combinando el hardware, el software y los servicios adecuados. Como empresa tecnológica de la lista Fortune 500, respaldada por más de 35 años de experiencia y una amplia red de más de 6.000 partners, ofrecemos soluciones de TI seguras e integrales para organizaciones de todo el mundo.