PRESENTACIÓN DE ESG

Por qué MDR se ha convertido en parte integral de las estrategias de ciberseguridad modernas

Fecha: agosto de 2022 **Autor:** Dave Gruber, Analista principal de ESG

RESUMEN: No hay duda de la importancia que tienen las prestaciones de detección y respuesta en los programas de ciberseguridad. El gran problema es encontrar la mejor forma de garantizar que la detección y la respuesta sean rápidas, precisas, fiables y coherentes, teniendo en cuenta que la cantidad y la complejidad de las amenazas aumenta a tal velocidad que la mayoría de organizaciones no llegan a adaptarse. Adoptar servicios de detección y respuesta gestionadas (MDR) de terceros es un enfoque que permite a las organizaciones mantenerse al día.

Introducción: El auge de la MDR

Todas las organizaciones se enfrentan a una dura realidad: las amenazas de ciberseguridad se multiplican rápidamente, las superficies de ataque cada vez son más grandes y los procesos y las herramientas tradicionales ya no bastan para detectar las amenazas y responder ante ellas. Tanto las amenazas como los atacantes son más eficaces, ágiles y persistentes, y representan un objetivo digital en movimiento para los profesionales de seguridad y TI que se ocupan de proteger los recursos corporativos.

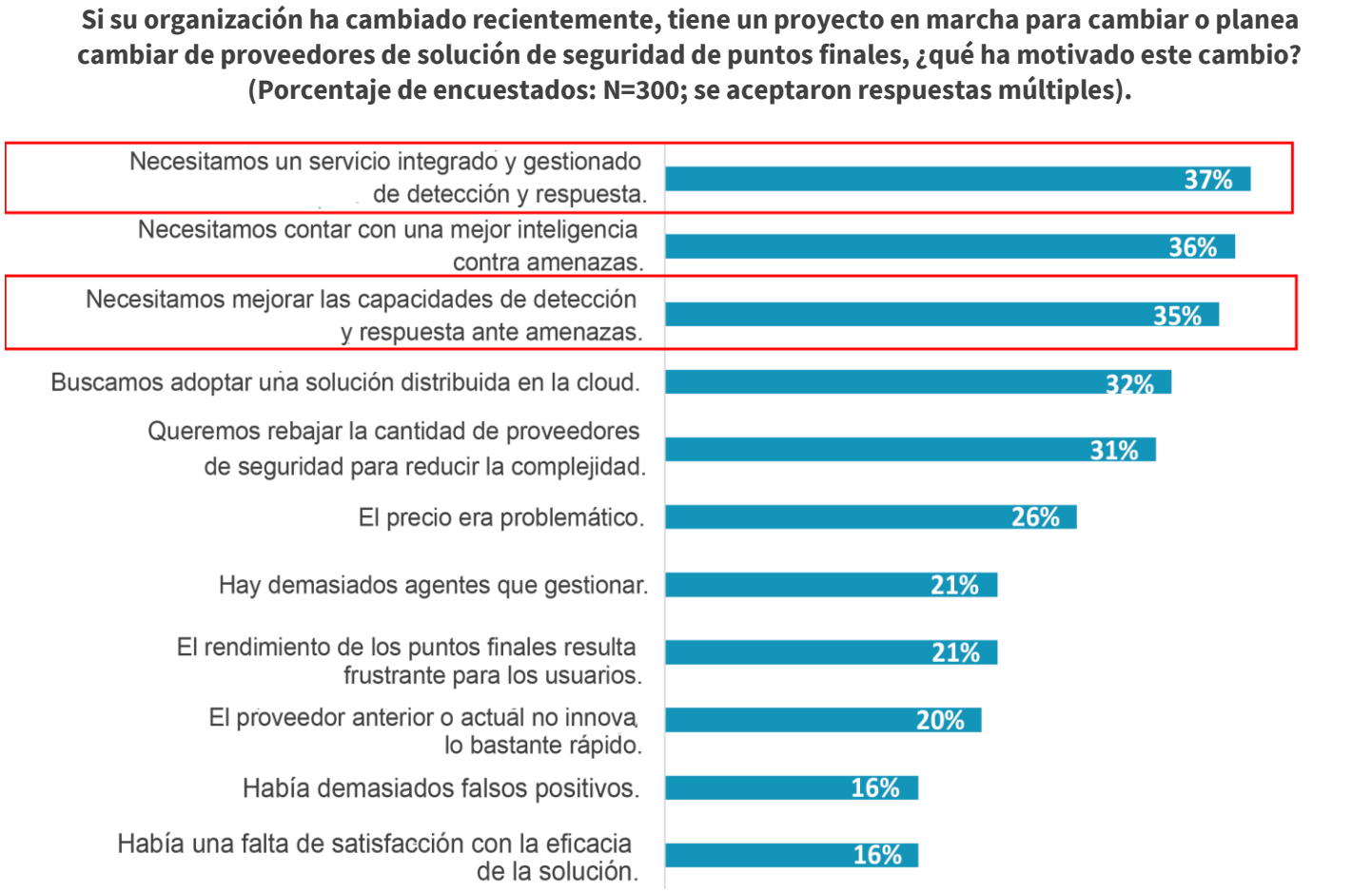
La gran cantidad de controles de seguridad añade costes y complejidad a las tareas de detección y respuesta, ya que implican que los equipos de seguridad tríen manualmente una avalancha constante de alertas para separar las amenazas reales de los falsos positivos. Desarrollar un centro de operaciones de seguridad (SOC) más grande y equiparlo con más herramientas e ingenieros de seguridad resulta caro; suponiendo que las organizaciones logren encontrar y contratar suficientes profesionales de la seguridad, vista la brecha actual en los conocimientos de ciberseguridad.

A medida que se rediseñan los programas de seguridad, las organizaciones cada vez recurren más a los proveedores de detección y respuesta gestionadas.

A medida que se rediseñan los programas de seguridad, las organizaciones cada vez recurren más a los proveedores de detección y respuesta gestionadas a fin de redefinir los procesos, solventar las carencias de recursos y conocimientos y modernizar las herramientas para las operaciones de seguridad. Es habitual asociar la MDR con la seguridad de puntos finales, y la investigación de ESG revela que la necesidad de contar con servicios de MDR integrados es un factor significativo en la decisión de las organizaciones de cambiar de proveedores de soluciones de seguridad de puntos finales (consulte la figura 1).[1]

[1] Fuente: Informe completo de la encuesta de ESG, *Endpoint Security Trends*, diciembre de 2021. Todos los cuadros y las referencias del estudio de ESG incluidos en esta documentación técnica se extrajeron del informe de la investigación, salvo que se indique otra fuente.

Figura 1. Factores que impulsan el cambio de los proveedores de seguridad de puntos finales



Fuente: ESG, una división de TechTarget, Inc.

No obstante, a medida que los equipos de seguridad amplían los programas de detección y respuesta, adoptando soluciones más completas de detección y respuesta extendidas (XDR), las soluciones de MDR ofrecen a las organizaciones una manera de actualizar tanto la tecnología como los modelos operativos capaz de proporcionarles una cobertura más completa de las superficies de ataque y detección de amenazas avanzadas. Se necesitan nuevos enfoques que combinen la supervisión ininterrumpida, inteligencia para la detección de amenazas global en tiempo real, automatización y análisis avanzados de aprendizaje automático, todo ello capaz de procesar grandes cantidades de telemetría de seguridad para respaldar la detección y persecución rápidas de amenazas. Mientras la XDR continúa evolucionando y madurando, los servicios de MDR permiten a organizaciones de cualquier tamaño y con cualquier nivel de madurez de la seguridad poner en marcha la detección y respuesta, lo que hace posible mitigar las amenazas avanzadas. Esto resulta particularmente importante a medida que las organizaciones redefinen el alcance y la escala de los límites de la ciberseguridad para abarcar los centros de datos, el perímetro y la cloud. MDR consolida las personas, los procesos y las tecnologías necesarios para ampliar los casos de uso de detección y respuesta en las empresas geográficamente dispersas.

Factores impulsores clave de la adopción de la MDR

El uso de los servicios de MDR está en aumento y ofrece a los equipos de seguridad la forma de obtener una cobertura más amplia, solventar las carencias de personal y reforzar los objetivos de programa generales. Los casos de uso verían, pero entre los factores impulsores subyacentes se encuentran:

- Panorama de amenazas: la cantidad de ciberataques y su mayor sofisticación ha ejercido mucha presión en las organizaciones, que deben detectarlas y responder de forma más rápida y eficaz.
- Intención adversa: los atacantes son más inteligentes y persistentes, y cada vez utilizan planes más estratégicos para los ataques. Se ha creado un importante "ecosistema criminal", en el que los atacantes comparten tácticas e incluso colaboran en ataques.
- Economía: desarrollar y ampliar un SOC requiere un compromiso importante en forma de CAPEX, que suele constar de decenas de miles de euros o más.
- Actualización de la tecnología de ciberseguridad: la pila de controles de ciberseguridad debe actualizarse más a menudo en las organizaciones que se ocupan internamente de la mayoría de operaciones de seguridad; como, por ejemplo, el paso de una solución de primera generación de detección y respuesta en puntos finales a una infraestructura más completa de XDR o MDR.
- Carencia de conocimientos: se ha hablado mucho de la brecha en conocimientos de ciberseguridad, que resulta un problema perenne. La incapacidad para contratar a profesionales internos de ciberseguridad genera desafíos a la hora de cumplir los objetivos de detección y respuesta, lo que arriesga la seguridad de los activos.

Los ciberataques no discriminan. Las organizaciones pequeñas y medianas, que cuentan con personal y presupuestos limitados, y que ya se han visto expuestas a todo tipo de ataques, corren peligro. Incluso las organizaciones de gran tamaño necesitan complementar el personal, contar con controles ampliables y disponer de asesores a nivel ejecutivo sobre la detección y respuesta en el panorama de amenazas, que no deja de evolucionar.

Qué buscar en un servicio MDR y en un proveedor de servicios MDR

Cualquier organización que evalúe un servicio de MDR cuenta con requisitos importantes e intrincados, como, por ejemplo:

- Inteligencia contextual contra amenazas: aplicar la detección y la inteligencia contra amenazas en tiempo real, incluyendo funciones de correlación entre varios indicadores para identificar amenazas y descartar falsos positivos.
- Casos de uso proactivos: compatibilidad con la persecución activa de amenazas conocidas.
- Telemetría completa: llevar a cabo análisis sofisticados e investigaciones forenses profundos, que resultan particularmente importantes para identificar amenazas nuevas emergentes.
- Corrección: ofrecer orientación para la corrección específica para cada contexto y con tecnología de IA.
- Mitigación de riesgos: evaluar y gestionar las vulnerabilidades.

A la hora de seleccionar un proveedor de servicios de MDR, las organizaciones deben buscar socios capaces de ofrecer capacidades específicas y probadas, como, por ejemplo:

- Cobertura 24x7; supervisión continua de forma ininterrumpida, las 24 horas del día, 7 días a la semana
- Planificación y asesoría sobre escenarios hipotéticos

- Conocimientos y experiencia humanos por parte del proveedor de servicios
- Orientación a ejecutivos y miembros de la junta directiva
- Capacidad para garantizar el control, el cumplimiento normativo y la continuidad empresarial

Además, es recomendable que las organizaciones pregunten a los socios de MDR sobre sus objetivos de nivel de servicio. Estas funciones incluyen el tiempo medio de respuesta, de la alerta al inicio de la investigación; tiempo medio desde el inicio de la investigación hasta la entrega a la organización del análisis del incidente; y tiempo medio de solución, desde el inicio de la investigación hasta el momento en el que se ha completado el proceso de resolución.

Enfoque de Dell Technologies para la MDR

A fin de identificar, evaluar y colaborar con un proveedor de servicios de MDR, las organizaciones deben concentrarse no solo en sus necesidades actuales de detección y respuesta ante amenazas, sin también en cómo es posible que evolucionen y crezcan estas necesidades en el futuro. Pese a que ninguna organización tiene una bola de cristal para predecir el futuro de las ciberamenazas, las organizaciones deben buscar un socio de MDR que haya demostrado su capacidad para ampliar el servicio con el tiempo, basándose en tecnología innovadora, procesos probados y los conocimientos demostrados de su personal.

El enfoque de Dell Technologies de cara a las soluciones de detección y respuesta gestionadas junta una tecnología flexible, inteligente y ampliable con profesionales de la ciberseguridad. Nuestro servicio de subscripción se ha diseñado para permitir a las organizaciones prever los costes y poder pasar sin complicaciones a niveles más altos de servicio, en el momento en el que resulte necesario.

La plataforma tecnológica de Dell Managed Detection and Response es Taegis XDR, un servicio completamente gestionado y nativo de la cloud desarrollado por Secureworks, una unidad de negocio de Dell. Taegis XDR detecta, analiza y actúa contra las amenazas identificadas, en una superficie de ataque diversificada y distribuida, para ayudar a proteger a las organizaciones, ya sean empresas globales gigantescas o relativamente pequeñas.

Reforzamos aún más Taegis XDR con los conocimientos del gran grupo de analistas e ingenieros de seguridad de Dell, cuyos conocimientos abarcan décadas de experiencia y ayudan a proteger a las organizaciones contra las amenazas, conocidas o nuevas. Esta combinación ofrecer una forma eficiente de unificar la detección y la respuesta en toda la arquitectura de TI, en gran parte gracias a la base de datos de inteligencia contra amenazas que actualizamos continuamente. Dell Managed Detection and Response también supervisa, analiza e identifica comportamientos conflictivos para reducir el tiempo medio de detección y respuesta.

Dell Managed Detection and Response también supervisa, analiza e identifica comportamientos conflictivos para reducir el tiempo medio de detección y respuesta.

Finalmente, al tratarse de un servicio gestionado, Dell Managed Detection and Response reduce significativamente la necesidad de las empresas de buscar y contratar a profesionales de seguridad para sus equipos internos de operaciones de TI y seguridad, que ya están al límite. Dell Managed Detection and Response se ha diseñado para complementar y ampliar las capacidades propias de la organización de forma rentable y estratégica.

La mayor verdad

La superficie de ataque, que cada vez crece más rápido; los ataques de programas de secuestro, y el aumento en la complejidad del panorama de amenazas han intensificado las inversiones y la importancia de la XDR y la MDR, a medida que las organizaciones modernizan sus programas de detección y respuesta ante amenazas. Pese a que las estrategias de seguridad individuales pueden varias, contar con una vista más completa de la superficie de ataque; así como de agregar, correlacionar y analizar cantidades enormes de datos de seguridad de los controles de seguridad individuales, resultan pasos importantes para recuperar el control.

Los servicios de detección y respuesta gestionadas son eficaces y fáciles de encontrar, a medida que los equipos de seguridad recurren a los proveedores de MDR para reforzar sus conocimientos, procesos y tecnologías de seguridad. La investigación de ESG muestra que las organizaciones que invierten en XDR buscan incorporar servicios de MDR complementarios para ayudar a implementar y utilizar estas soluciones. Esto implica que colaboran con proveedores de soluciones que cuentan con una trayectoria probada en la prestación de servicios y soluciones de seguridad. Cuando las soluciones se aplican a lo largo de un tiempo, pueden ayudar a los equipos de TI y seguridad a desarrollar y ampliar los programas de seguridad.

ESG recomienda explorar las soluciones de MDR de empresas como Dell Technologies, que cuentan con personal, procesos y tecnologías para ayudar a las empresas a alcanzar estos objetivos.

Enterprise Strategy Group es una empresa de análisis de tecnología, investigación y estrategia integrada que proporciona inteligencia de mercado, información procesable y servicios de contenido de comercialización a la comunidad internacional de TI.

www.esg-global.com contact@esg-global.com 508.482.0188