Enterprise Strategy Group | Getting to the bigger truth.™

DOCUMENTO TÉCNICO DE ESG

Detección y respuesta gestionadas: una ruta para el crecimiento rápido de los programas de seguridad

De Dave Gruber, analista principal

Agosto de 2022

Este documento técnico de ESG fue encargada por Dell Technologies y se distribuye conforme a la licencia de TechTarget, Inc.

Contenido

Resumen

La aceleración en la transformación digital, la rápida adopción de la cloud, la mayor complejidad del panorama de amenazas y la continua carencia de conocimientos de seguridad están llevando a los equipos de seguridad al límite. Las soluciones de seguridad actuales no logran mantenerse al día y obligan a muchas empresas a priorizar las iniciativas de modernización de SOC para renovar las tecnologías y procesos. Las grandes tendencias del sector en torno a la confianza cero y la detección y respuesta extendidas (XDR) ofrecen una visión nueva; sin embargo, muchas empresas tienen dificultades para implementar y poner en marcha estas estrategias de forma eficaz. Los servicios de detección y respuesta gestionadas (MDR) alivian estas dificultas al ofrecer a muchas empresas el personal, los procesos y la tecnología que necesitan para mejorar sus programas de seguridad en esta época difícil.

Introducción

El aumento en el riesgo de sufrir ciberataques que causen daños arrebata atención y presupuesto a los objetivos principales del negocio, por lo que las empresas deben responder reforzando los programas de ciberseguridad. Para algunas, desarrollar un programa de seguridad enteramente con recursos internos es plausible, pero, para la mayoría, es necesario recurrir a recursos de terceros para hacer posible el crecimiento y la ampliación rápido de estos programas.

Las operaciones de seguridad (SecOps) son fundamentales en todos los programas de ciberseguridad; se ocupan de supervisar y proteger todos los aspectos de la superficie de ataque digital. Al abarcar la red, los puntos finales, la cloud, las identidades, las aplicaciones y los datos, SecOps debe gestionar una cantidad cada vez mayor de telemetría y alertas de seguridad, lo que lleva a las organizaciones al límite y causa que muchas busquen ayuda entre los proveedores de servicios de MDR.

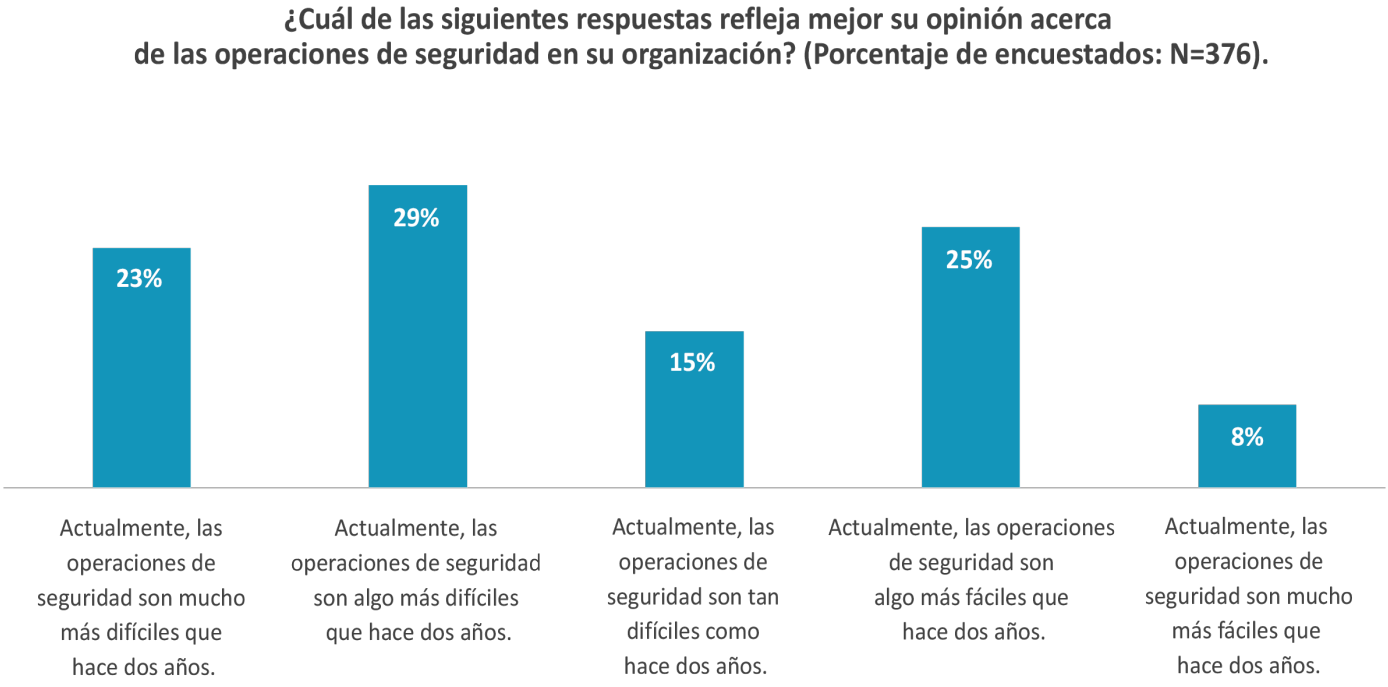
Los proveedores de servicios de MDR se han convertido en un mecanismo esencial para estas organizaciones, ya que proporcionan una amplia gama de ofertas de servicios de seguridad, como respuesta ante incidentes, supervisión ininterrumpida, gestión de programas y gestión de riesgos. La investigación de Enterprise Strategy Group (ESG) indica que los servicios de MDR se han convertido en un componente estándar en organizaciones de todos los tamaños y de todos los niveles de madurez de seguridad.

Crecimiento de los desafíos de las operaciones de seguridad

Según la investigación de ESG (consulte la figura 1), la mayoría de organizaciones admiten que la situación de SecOps es más complicada ahora que hace dos años.[1]

[1] Fuente: Informe completo de la encuesta de ESG, *SOC Modernization and the Role of XDR*, agosto de 2022. Todos los cuadros y las referencias del estudio de ESG incluidos en este documento técnico se extrajeron del informe de la investigación, salvo que se indique otra fuente.

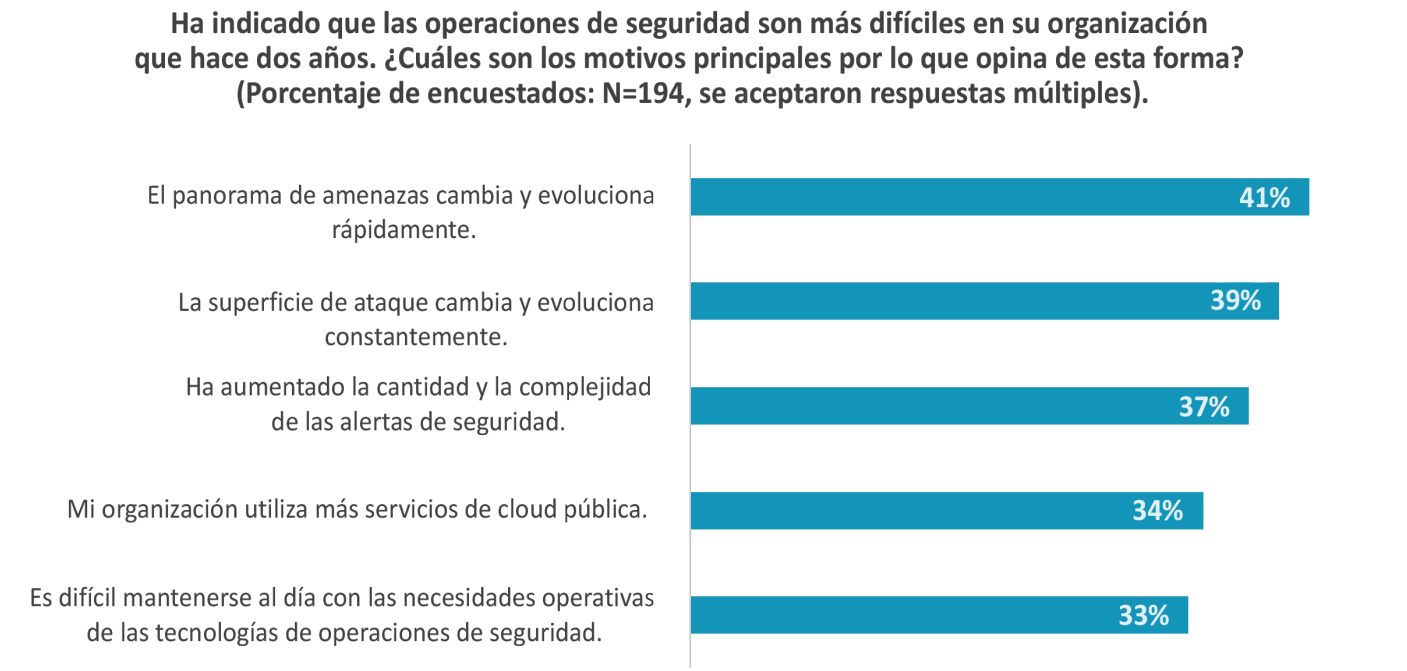
Figura 1. Más de la mitad opinan que ha aumentado la dificultad de SecOps



Fuente: ESG, una división de TechTarget, Inc.

Tal como se muestra en la figura 2, la investigación de ESG también indica otros desafíos que dificultan más que nunca la detección y respuesta, como la expansión de la superficie de ataque, el crecimiento y la diversidad del panorama de amenazas, y el uso cada vez mayor de servicios de cloud para una mayor gama de aplicaciones y casos de uso.

Figura 2. Las cinco causas principales del aumento de la dificultad de SecOps



Fuente: ESG, una división de TechTarget, Inc.

Modernización de los programas de detección y respuesta

El tamaño y la complejidad de las superficies de ataque y el panorama de amenazas han aumentado, por lo que también ha aumentado el uso de más controles de seguridad, lo que genera miles de alertas y cantidades enormes de datos de seguridad. Para respaldar el triage y la investigación de las alertas y los incidentes, los equipos de seguridad deben agregar, correlacionar y analizar estos datos, lo que suele requerir cantidades inmensas de procesos manuales. Pero es necesario ir más allá de la recopilación y el análisis de alertas y datos de seguridad.

Los equipos de seguridad se replantean las operaciones de programa para incorporar más datos de activos y riesgos provenientes de los equipos de TI y línea de negocio con el objetivo de centrarse en las amenazas que representan el riesgo más significativo para los objetivos de la organización. Por ejemplo, los credenciales de administración de dominios robados pueden tener todo tipo de posibles impactos adversos en las operaciones, las finanzas y la reputación de la organización, tanto a corto como a largo plazo.

A medida que los responsables de seguridad se replantean las estrategias, cada vez más organizaciones pasan las actividades operativas diarias a terceros y centran los recursos internos en actividades de seguridad más estratégicas. A medida que los recursos internos de seguridad se centran en rediseñar los procesos de las operaciones de seguridad, los proveedores de servicios de MDR se ocupan de la detección, el triage y la respuesta ante incidentes, actuando rápidamente para evitar daños y limitar las posibles disrupciones empresariales en las operaciones.

Otras empresas acuden a los proveedores de MDR para obtener orientación sobre el desarrollo general de programas, recurriendo a expertos y a procesos de operaciones de seguridad probados para optimizar sus resultados.

El movimiento de XDR está creando una visión y un roadmap de lo que es necesario para modernizar los programas de detección y respuesta, mientras otros recurren a los proveedores de MDR para que les ayuden a implementar soluciones de XDR.

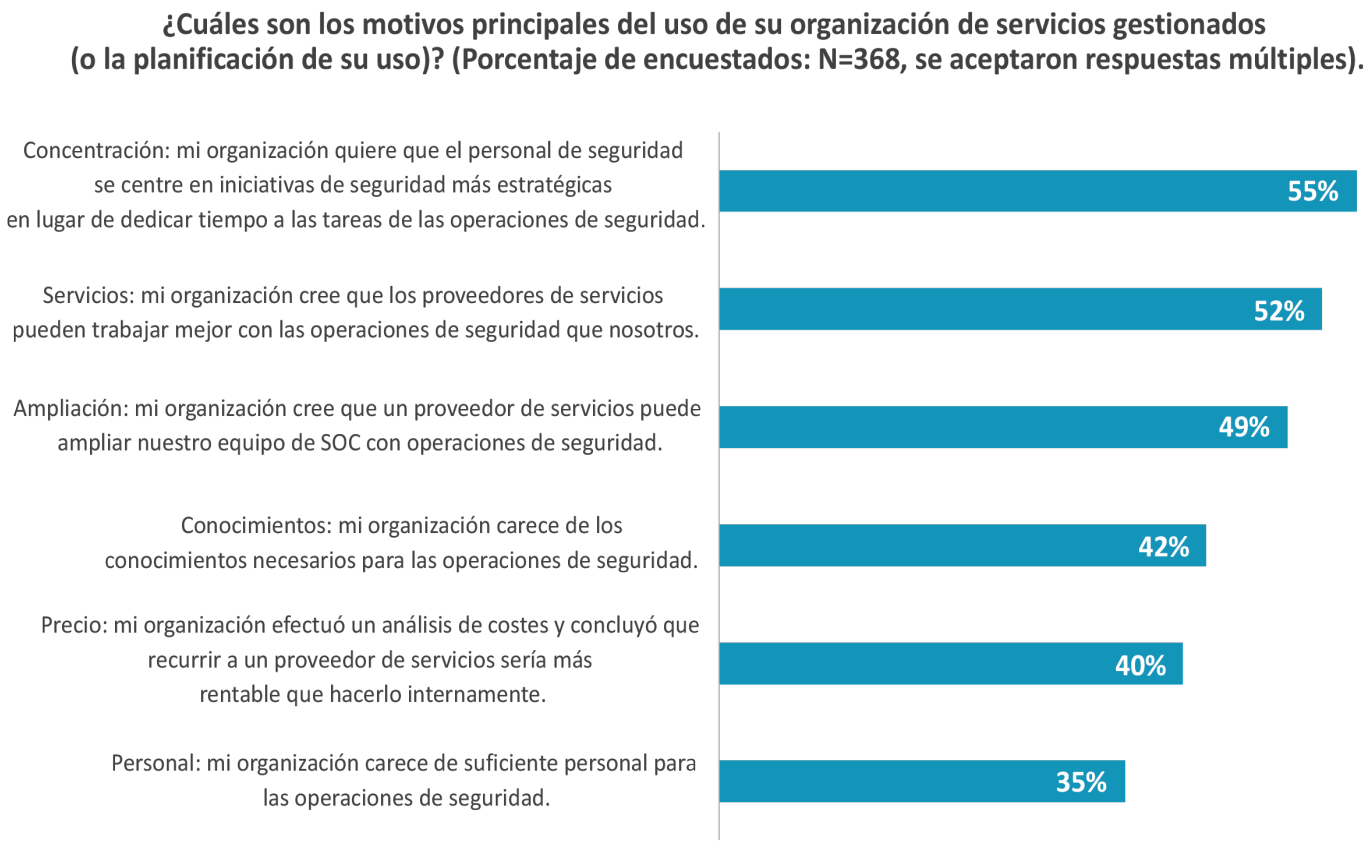
Casos de uso de la MDR

Aunque muchos proveedores de MDR ofrecen una amplia gama de servicios de seguridad, las colaboraciones suelen empezar por los servicios centrales de detección y respuesta que supervisan, trían e investigan las alertas. Los modelos operativos varían entre los proveedores de MDR, de modo que los responsables de seguridad deben coordinar cuidadosamente los requisitos individuales de su organización con un proveedor de MDR que pueda abordar sus objetivos concretos. Por ejemplo, algunos responsables de seguridad optan por externalizar completamente las operaciones de seguridad, contratando a proveedores de MDR que ofrezcan prestaciones completas de cobertura de la superficie de ataque, supervisión de amenazas y corrección. En un modelo así, los proveedores de MDR suelen ofrecer la pila tecnológica, los procesos y los expertos de seguridad necesarios para prestar este servicio. En otros casos, los servicios de MDR actúan como una extensión de la función interna de operaciones de seguridad, aportando cobertura fuera del horario laboral o expertos de seguridad adicionales al equipo de seguridad interno que se responsabiliza de la pila de tecnología y los procesos operativos. Estos son solo dos ejemplos de los muchos casos de uso en los que se emplean servicios de MDR.

En consecuencia, la MDR no es una solución de talla única, sino que suele representar un conjunto de capacidades personalizables que pueden aplicarse según las necesidades de cada organización.

Las organizaciones eligen a sus socios de MDR según distintos aspectos de la detección y respuesta, dependiendo de los recursos y conocimientos internos de los que dispongan. La investigación de ESG explora los principales motivos tras estas decisiones en la figura 3.

Figura 3. Motivos por los que las organizaciones eligen socios de MDR



Fuente: ESG, una división de TechTarget, Inc.

Factores impulsores clave del uso de MDR

Desarrollar programas de seguridad exige centrarse tanto en la eficiencia como en la eficacia, y los servicios de MDR pueden tener repercusiones positivas en ambos aspectos.

- Mayor eficiencia y mejora de las operaciones. La MDR ayuda a las organizaciones a reducir el coste total de las operaciones de seguridad en distintas maneras, relacionadas, por ejemplo, con el personal, la infraestructura y la gestión. También puede abordar el problema de la "fatiga de alertas", así como mejorar la posibilidad de que los falsos positivos se reduzcan significativamente.

- Mejor eficiencia de la ciberseguridad y reducción del riesgo. La MDR puede ayudar a las organizaciones a frenar las amenazas que ya están en marcha, mejorar la detección de posibles amenazas y ataques persistentes avanzados, activar la persecución de amenazas proactiva e instaurar controles más potentes para detectar y prevenir futuros ataques.

Qué buscar en un proveedor moderno de soluciones de MDR

Tenga en cuenta que las soluciones de MDR, en general, no son una novedad. De hecho, hace tiempo que existen y ya cuentan con un historial de éxito. No obstante, muchas soluciones de MDR de primera generación se diseñaron e implementaron en otra época: había menos datos y menos amenazas, y la detección era más sencilla. La siguiente generación de soluciones de MDR (así como los terceros que las implementan y gestionan) debe tener en cuenta un

conjunto de desafíos más grande, profundo y complejo, que hace que la detección y respuesta ante amenazas sea más importante y difícil que nunca.

Al evaluar las soluciones de MDR, las organizaciones deberían buscar capacidades como, por ejemplo:

- Supervisión 24x7 de eventos y registros, generando información rápido y con alta visibilidad de la actividad sospechosa y las alertas, según volumen, ubicación y tipo
- Prestaciones continuas y ampliables de supervisión de la red y análisis de amenazas
- Recomendaciones basadas en la IA con opciones de respuesta contextual
- Generación de informes de cumplimiento de la normativa
- Asesores de seguridad “humanos” que estén en contacto directo con los equipos internos
- Análisis detallados en tiempo real basados en la detección, el triage, la investigación y el análisis forense de amenazas
- Evaluación y priorización de vulnerabilidades, y orientación sobre la mitigación de las mismas

Al considerar la gran cantidad de potenciales proveedores de servicios que pueden ofrecer algunas, muchas o todas las prestaciones de MDR externalizadas, las organizaciones deben fijarse en los socios capaces de ofrecer:

- Inteligencia contextual contra ciberamenazas
- Telemetría completa
- Una trayectoria probada en la zona de cobertura geográfica, el mercado vertical y el perfil normativo de la organización
- Capacidad de persecución de amenazas demostrada
- Compromiso a largo plazo con la MDR basada en la cloud, con todo tipo de capacidades de confianza cero, en entornos multicloud e híbridos, y del modelo de responsabilidad compartida de la seguridad de cloud
- Capacidad demostrada para ampliar sus servicios con el tiempo, con base en tecnología innovadora, procesos probados y conocimientos probados entre su personal

Enfoque de Dell Technologies para la MDR

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 empresa de Dell Technologies. 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 negocios relativamente pequeños.

La potencia de Taegis XDR se maximiza gracias a los conocimientos y experiencia 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.

Al tratarse de un servicio configurado e implementado como solución gestionada y de subscripción, Dell Managed Detection and Response reduce significativamente la necesidad de las empresas de buscar y contratar a profesionales de seguridad para gestionar más amenazas, más ataques y más alertas. Dell Managed Detection and Response complementa y amplía las capacidades internas de las organizaciones con eficacia y eficiencia. Como resultado, el personal interno de SecOps puede dedicar más tiempo y energía a otras tareas de seguridad.

Casos de éxito: Funcionamiento de la MDR en el mundo real

ESG habló con responsables de TI y seguridad de los clientes de Dell MDR para obtener información sobre sus casos de uso, modelos operativos y resultados específicos.

Ejemplo n.º 1: Administración municipal de tamaño medio

Los recursos de TI y ciberseguridad de la administración municipal raramente se corresponden a los de sus homólogos en el sector privado, pero no por ello se enfrentan a problemas distintos. En este ejemplo, un condado mediano de un Estado del sureste de Estados Unidos tenía dificultades para enfrentarse y solucionar una cantidad cada vez mayor de amenazas de seguridad, así como para mantener el presupuesto bajo control estricto.

Cuando contrataron a un nuevo director de TI, este comprendió de inmediato que su pequeño equipo se enfrentaba a un panorama de amenazas cada vez mayor, e identificó vulnerabilidades en sus prestaciones de detección y respuesta. “El estado de seguridad no solo no estaba a la altura, sino que teníamos que ampliar nuestras capacidades sin modificar las nóminas; un asunto que resulta muy delicado alrededor de los responsables de tomar decisiones ejecutivas —dijo—. Pero sabía que podía hacer referencia a su necesidad de ahorrar al tiempo que hacía hincapié en la necesidad de abordar las vulnerabilidades”.

En primer lugar, se propuso evaluar un proveedor de seguridad de puntos finales establecido en el condado, que ofrecía una “prueba gratuita” de 90 días de actualizaciones de software para mejorar la detección y respuesta. No obstante, concluyó que el software carecía de prestaciones que necesitaban, y la comunicación con el proveedor no cumplió sus expectativas. En consecuencia, decidió estudiar una solución de MDR más completa.

“Por suerte, ya teníamos un acuerdo con Dell para que nos proporcionara un CSO (directo de seguridad) virtual, por lo que los responsables del condado ya conocían las ventajas de optar por un enfoque de servicios gestionados, en este caso para la detección y respuesta”. Añadió que el equipo de Dell actuó como un complemento, y no un reemplazo, del pequeño equipo interno de profesionales de TI y seguridad que el condado ya tenía. “Trabajaron como una extensión de nuestro equipo, y colaboraron con nuestro personal sin ningún problema”.

Los beneficios reales de esta estrategia quedaron claros rápidamente, cuando una campaña global de piratas informáticos atacó el correo electrónico web Microsoft Exchange, una plataforma popular utilizada por muchas organizaciones, entre ellas, el condado. “Microsoft desarrolló y distribuyó un parche en cuanto se descubrió el ataque, pero el día cero había ocurrido meses antes —dijo el director de TI del condado—. Nuestro CSO virtual de Dell se puso en contacto cuando ya habíamos cerrado, y el equipo de MDR de Dell se incorporó al trabajo inmediatamente. Nos mandaron scripts para comprobar el estado del servidor, y detectamos de inmediato que uno de nuestros servidores había sufrido una vulneración”.

“Los profesionales de Dell (y sus socios de Secureworks) sabían lo que hacían. Teníamos reuniones dos o tres veces al día, cada día, durante todo el tiempo que tardamos en solucionar el intento de vulneración”. Añadió que el equipo de respuesta ante incidentes compartió todos sus hallazgos con el personal del condado, enseñándoles muestras del código y otras indicaciones de que se había producido un intento de vulneración, así como las pruebas de la vulneración.

Por último, ofrecieron una gran cantidad de recomendaciones, tanto técnicas como no técnicas, que no solo abordaban el impacto potencial del intento de vulneración, sino que además reforzaban el estado de ciberseguridad del condado en un periodo y ámbitos más amplios.

“Esta experiencia nos demostró que lo más recomendable al buscar soluciones de detección y respuesta es encontrar especialistas de MDR fiables, probados y de confianza, que ya tengan experiencia; y no buscar una forma barata de actualizar el software de EDR —dijo—. Lo que más recuerdo de este caso, y no hablo solamente a toro pasado, sino que hablo del momento del ataque, cuando colaborábamos a diario, es la sensación de tranquilidad al saber que teníamos un buen equipo esforzándose por protegernos”.

Ejemplo n.º 2: Distrito escolar de tamaño medio

Los distritos escolares, históricamente, invertían muy poco en el entorno de TI en general, y en ciberseguridad en particular. Pero, debido al auge en los ciberataques y los programas de secuestro que están sufriendo los distritos escolares, los responsables públicos de la educación han tenido que esforzarse para encontrar maneras mejores, más fiables y más rentables de protegerse ante las vulneraciones.

Por ejemplo, un distrito escolar estadounidense de tamaño medio sufrió el ataque de un programa de secuestro; todas sus operaciones tecnológicas se apagaron. Con 8500 alumnos y docentes distribuidos en 21 centros, el distrito tuvo que implementar un entorno de TI de tamaño importante, con 100 servidores físicos y 63 virtuales, conectados a más de 11 000 dispositivos de alumnos y docentes. Claramente, el distrito tenía muchos potenciales puntos de entrada para atacantes, y necesitaba un socio capaz de reaccionar rápidamente.

Tras determinar que el ataque de programas de secuestro era real y tenía que solucionarse de inmediato, el equipo de TI del distrito escolar se puso en contacto con Dell Managed Detection and Response. “En el segundo día del ataque ya teníamos a 10 personal de Dell con nosotros —recuerda el directo de TI del distrito—. Hemos tenido una relación de confianza con el equipo de Dell, que tomó las riendas al momento”.

Por suerte, el resultado final fue positivo para el distrito. “Nuestros sistemas contenían más de 6 millones de archivos, y solo perdimos 6 —dijo el director de TI—. Ni siquiera pagamos el rescate. Somos un ejemplo real de supervivientes de un programa de secuestro que pudieron continuar trabajando de forma segura y con protección”.

“Trabajar con Dell ha sido una experiencia positiva. Nuestros analistas de seguridad in situ siempre quedan satisfechos tras hablar con el personal de Dell, y tenemos una seguridad un 95 % mejor que antes de trabajar con Dell en el ámbito de la detección y respuesta”.

La mayor verdad

El aumento en el riesgo de sufrir ciberataques que causen daños arrebata atención y presupuesto a los objetivos principales del negocio, y las organizaciones deben reforzar los programas de ciberseguridad. Aunque los casos de uso son variados, la mayoría utilizan proveedores de servicios de MDR para ampliar sus programas.

Los proveedores de servicios de MDR ofrecen una forma de superar muchos de los desafíos reconocidos de desarrollar un programa de seguridad exitoso, que incluye expertos en seguridad, procesos probados y tecnologías de seguridad ampliables y fáciles de implementar.

Dell Technologies reúne un grupo integrado de tecnología, expertos en seguridad con experiencia y procedimientos recomendados para ayudar a las organizaciones a detectar las amenazas y responder ante ellas casi en tiempo real. Como hemos visto en los casos prácticos presentados en este documento técnico, Dell Technologies ha ayudado a una amplia gama de organizaciones, en distintos sectores y con diferentes perfiles de recursos, a frenar el impacto de las amenazas emergentes en la empresa.

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