DELL Technologies

DOCUMENTACIÓN TÉCNICA

DELL MANAGED DETECTION AND RESPONSE

Una completa solución de seguridad gestionada para organizaciones pequeñas y medianas.

DOCUMENTO DE SÍNTESIS

Los ciberataques contra las empresas cada vez son más habituales. Un informe de Internet Complaint Center, del FBI, afirmó en 2021 que se había observado un aumento del 69 % desde el año anterior, y se habían notificado un total de 4200 millones de dólares en pérdidas.[1] Los ataques contra las grandes empresas se publican en portada, pero la realidad es que las organizaciones de todos los tamaños son vulnerables. Las pequeñas empresas, que carecer de los vastos recursos que tienen las granes compañías, corren un riesgo destacado.

La ciberseguridad es fundamental para proteger los recursos de datos, las operaciones y la continuidad empresarial. Las grandes empresas suelen tener equipos de seguridad dedicados que cuentan con lo último en tecnología, métodos e información. Sin embargo, las empresas medianas y pequeñas puede que solo tengan uno o dos especialistas en seguridad, que tienen que gestionar y utilizar conjuntos de dispositivos de seguridad y herramientas de software cada vez más complejos.

Un desafío cada vez mayor para los equipos de TI

La gran cantidad de ataques contra puntos finales, servidores, aplicaciones redes y clouds genera una cantidad inmensa de alertas, que no tardan en agotar a los equipos de seguridad y TI. Al mismo tiempo, los atacantes continúan transformando sus técnicas, evitando hábilmente las defensas que ayer eran eficaces. Para proteger los entornos de TI en la década de 2020 es preciso contar con expertos dedicados que supervisen y respondan de forma ininterrumpida.

Si los responsables de TI en las empresas pequeñas y medianas asignan el suficiente personal y presupuesto de TI a la ciberseguridad, otros aspectos importantes, como el desarrollo de aplicaciones y DevOps, pueden verse impactados. La realidad es que, para protegerse de los atacantes de hoy en día, es necesaria una inversión en profesionales, herramientas y operaciones que muchas empresas no pueden permitirse.

Los ciberataques representan una mayor amenaza que nunca

Un 69 % de aumento en los ciberataques declarados en 2020.[1]

Un 34 % de los ataques en 2020 involucraron a personal interno.[2]

Un 67 % de los encuestados no confían en la capacidad de recuperación.[3]

Un 82 % de los empleadores afirman que existe una escasez de conocimientos sobre ciberseguridad.[4]

Managed Detection and Response ofrece la respuesta

En consecuencia, más empresas se plantean optar por soluciones de detección y respuesta gestionadas (MDR) de proveedor de servicios externos. ¿Cómo pueden los responsables de la toma de decisiones de TI identificar a los mejores socios de MDR?

Un proveedor de soluciones de MDR idóneo debe implementar tecnología que detecte los tipos desconocidos de amenazas, minimice los falsos positivos, correlaciones eventos, haga un seguimiento de la secuencia de actividades de los intrusos y automatice las acciones de aislamiento y prevención. El proveedor debe contar un con equipo de profesionales de la seguridad con experiencia y conocimientos excelentes, que analicen las alertas y aborden las amenazas 24x7, 365 días al año, y que persigan los nuevos tipos de amenaza.

A fin de prestar servicios de MDR, es necesario desarrollar las operaciones de seguridad y establecer y refinar los procesos. Es más, los analistas deben contar con herramientas para compartir conocimientos y formación periódica para estar al día sobre las amenazas y técnicas más recientes.

Pese a que muchos proveedores de servicios anuncian servicios de detección y respuesta gestionadas, solo algunos cuentan con la capacidad y las prestaciones necesarias para ofrecer un servicio excelente.

Dell Managed Detection and Response es una solución completamente integral que funciona 24x7. Supervisa, detecta, investiga y responde ante amenazas en todo el entorno de TI de la organización. No importa si la empresa tiene 50 o 1000 puntos finales, Dell MDR mejora el estado de seguridad de la empresa de forma rápida y significativa, al tiempo que reduce la carga de trabajo del personal de TI. Dell MDR aprovecha la capacidad de Dell para invertir en las personas, los procesos y las herramientas a fin de ofrecer una supervisión y respuesta de ciberseguridad empresarial a las organizaciones pequeñas y medianas.

Motivos principales por los que las empresas utilizan soluciones de detección y respuesta gestionadas (MDR)

- **Acceso a especialistas en ciberseguridad, que son difíciles de encontrar**
- **Cobertura completa de supervisión, detección y respuesta**
- **Reducción de la carga de trabajo del personal de TI, que puede centrarse en DevOps**

PANORAMA DE AMENAZAS ACTUAL

Los atacantes de hoy en día son metódicos; investigan durante semanas o meses, evaluando cómo obtener acceso a las aplicaciones y los datos valiosos. Cuando identifican una oportunidad, aprovechan vulnerabilidades o envían correos electrónicos de suplantación de identidad a fin de tentar a los usuarios para que abran archivos adjuntos maliciosos. Las capacidades de detección y respuesta son indispensables en un programa de ciberseguridad completo, así como la formación de los empleados, las evaluaciones de ciberseguridad, las pruebas de vulnerabilidad y penetración, la resiliencia y la planificación de la recuperación, entre otros elementos.

Si el atacante obtiene acceso, inicialmente buscan establecer una base desde donde ampliar el alcance de su ataque. De nuevo, se toman su tiempo para reforzar su posición dentro de la infraestructura de la empresa. Por ejemplo, además de atacar los sistemas empresariales, los ataques de programas de secuestro suelen intentar desactivar los sistemas de copia de seguridad y bloquear el acceso a estas copias. Algo así puede impedir que la empresa pueda recuperarse, de modo que el pago del rescate es la única manera de volver a poner en marcha la empresa.

Contar con capacidades de detección y respuesta sofisticadas y plenamente actualizadas es esencial para reconocer los ataques y sus signos. Una alerta temprana aporta a la organización la posibilidad de disminuir los daños provocados por el ataque antes de que pueda llegar más lejos.

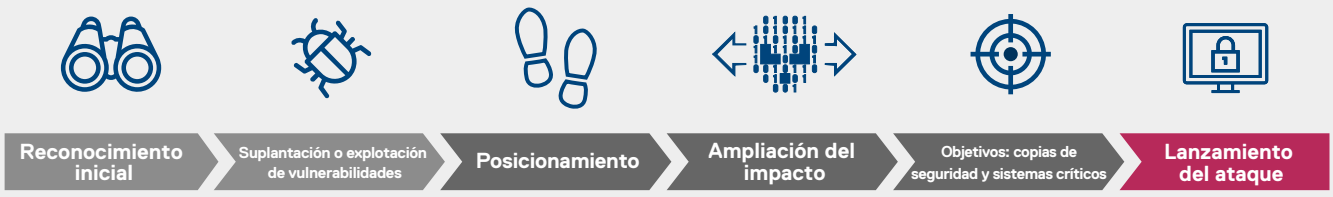
Las organizaciones implementan una amplia variedad de herramientas de ciberseguridad, como evaluación de contraseñas, pruebas de red, escaneo de vulneraciones, cifrado, supervisión y detección de amenazas. El equipo de TI recibe alertas de todas estas herramientas, pero llegan en tal cantidad que representan un desafío, y más aún si se tiene en cuenta la dificultad para correlacionar los eventos en distintas herramientas. Además, contar con los conocimientos necesarios y actualizados para utilizar todas estas tecnologías exige que el personal de TI invierta un tiempo considerable.

La parte humana de la ecuación de la MDR requiere un grupo de profesionales con años de experiencia en ciberseguridad y conocimientos sobre temas como administración de sistemas, análisis forense, investigación de amenazas y pruebas de penetración. Estos profesionales resultan difíciles de encontrar y caros de contratar, y es habitual que las organizaciones con mayor presupuesto y más fama se los arrebaten a empresas más pequeñas. En 2021, la encuesta "State of the CIO" identificó que los puestos de ciberseguridad eran los más difíciles de llenar en el equipo de TI.[5] Conservar a los analistas de seguridad y sustituir a los que se marchan es una batalla inacabable para los responsables de TI.

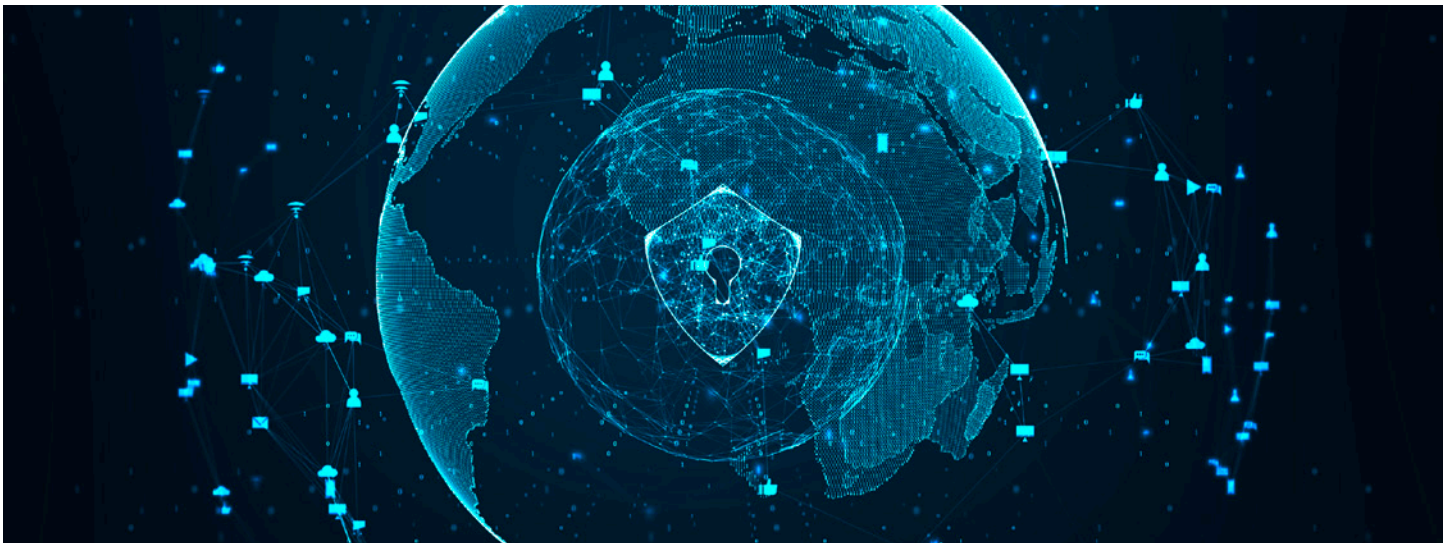
E incluso si obtienen las herramientas y los profesionales indispensables, las empresas deben desarrollar las operaciones y los entornos para la seguridad 24x7.

Figura 1: Estrategia del atacante

Los atacantes permanecen en el sistema una media de más de 100 antes de atacar.



La supervisión y la detección son esenciales para frenar a los atacantes potenciales.



Los servicios Dell Managed Detection and Response ponen capacidades inigualables a su alcance

No resulta sorprendente que las empresas pequeñas y medianas tengan problemas para defenderse adecuadamente. El panorama de ciberseguridad ha aumentado hasta convertirse en un caleidoscopio de ciberamenazas que no deja de cambiar. La avalancha de actividad ha aumentado los requisitos de personal, y la complejidad de los ataques significa que se necesitan profesionales de mayor calibre.

Dell Managed Detection and Response amplía su equipo de seguridad con expertos, herramientas y capacidad para operaciones de ciberseguridad comparable a las de las empresas más importantes. Dell MDR reduce la carga de trabajo de su equipo de TI, mitiga el riesgo y mejora significativamente el estado de seguridad de su empresa, para que pueda concentrarse en las prioridades empresariales.

Dell Managed Detection and Response es una combinación completamente intelligence de tecnología, conocimientos y operaciones. El servicio aprovecha los conocimientos de los analistas de seguridad de Dell Technologies, que han dedicado años a ayudar a empresas de todo el mundo a proteger mejor sus operaciones. Dell MDR aplica la potencia de Secureworks® Taegis™ XDR, una plataforma de software avanzado para análisis de seguridad con más de 20 años de experiencia probada, investigación e inteligencia contra amenazas en el mundo real, y conocimientos en la detección y respuesta ante amenazas sofisticadas.

Secureworks Taegis XDR

Secureworks Taegis XDR es una plataforma de ciberseguridad diseñada para aportar una solución a escala de Big Data a los problemas de seguridad. Taegis XDR, una plataforma nativa de cloud, incluye evaluaciones continuas basadas en el aprendizaje profundo y automático de telemetría y eventos procedentes de distintos vectores de ataque, reforzadas con completa información sobre amenazas.

Motivos para elegir Dell Managed Detection and Response

Personas

- **Expertos en ciberseguridad con experiencia**
- **Analistas con certificación de Taegis XDR**
- **Certificaciones de CEH, GIAC SANS, CISSP y CompTIA**

Tecnología

- **La plataforma de análisis de seguridad líder del sector, Secureworks Taegis XDR**
- **Supervisión continua e integral de amenazas con telemetría de una amplia variedad de puntos finales, redes y clouds**

Procesos

- **Tiempo de resolución más corto**
- **Cobertura 24x7, 365 días al año**
- **Asistencia para la implementación de agentes incluida**
- **Cuarenta horas por trimestre de orientación para correcciones remotas**
- **Cuarenta horas al año de puesta en marcha de la respuesta ante incidentes**

Socio de confianza

- **Con la confianza de empresas de alrededor del mundo para la asistencia de dispositivos e infraestructura**
- **Más de 20 años de innovación en la resiliencia empresarial**
- **Inversión continua en personas, procesos y herramientas**

Figura 2: Inteligencia contra amenazas

La única forma de identificar y responder ante los ataques sofisticados es, en primer lugar, comprender como funcionan los atacantes y qué les motiva. Cada año, el equipo de Secureworks tras XDR participa en más de 1000 respuesta ante incidentes cada año. Esto les aporta la importante ventaja de observar los cambios en las estrategias, técnicas y procesos que utilizan los atacantes para penetrar eficazmente en las empresas de los clientes.

Taegis XDR analiza los datos relevantes para la seguridad que recopilan en puntos de datos, redes, sistemas de cloud y sistemas empresariales locales para detectar amenazas. XDR es una plataforma abierta que complementa la infraestructura de seguridad existente, garantiza una cobertura completa y protege las inversiones existentes.

XDR ofrece prestaciones automáticas de respuesta, corrección e información para mejorar la eficiencia de las operaciones de seguridad, así como brindar a los equipos de respuesta la visibilidad que necesitan para actuar en caso de amenazas. Los clientes de Dell MDR se benefician de una inteligencia contra amenazas desarrollada a partir de miles de puntos de datos, recopilados de distintos clientes, y servicios de inteligencia compartidos en todo el mundo.

Los mejores expertos en seguridad pueden estar a su disposición

Un equipo global de analistas de seguridad con formación avanzada puede dedicarse a buscar vulnerabilidades en su sistema. Los expertos en ciberseguridad de Dell tienen experiencia en todas las fases de la detección y mitigación de amenazas, incluyendo la investigación y persecución de amenazas, la seguridad de puntos finales y la respuesta y recuperación ante incidentes. Los analistas de Dell cuentan con certificaciones de XDR y una amplia variedad de otras certificaciones reconocidas en el sector y por la administración pública, como CEH, GIAC, SANS, CISSP y CompTIA. El centro de operaciones de seguridad distribuido de Dell MDR ofrece cobertura 24x7, 365 días al año, gracias al modelo de asistencia en la oficina que se encuentre abierta.

El equipo de Dell MDR se familiariza con las operaciones y la infraestructura de TI de la empresa. Utilizan el aprendizaje automático y la información filtrada sobre amenazas de miles de entornos de TI, recopilada mediante XDR, para supervisar su entorno. El equipo de Dell MDR salta a la acción al momento cuando aparece una advertencia, investigando los datos de la alerta a fin de identificar conexiones y patrones que solo los analistas de seguridad formas y con experiencia pueden reconocer. A continuación, aconsejan a los miembros del equipo de respuesta de la organización sobre la mejor forma de proceder.

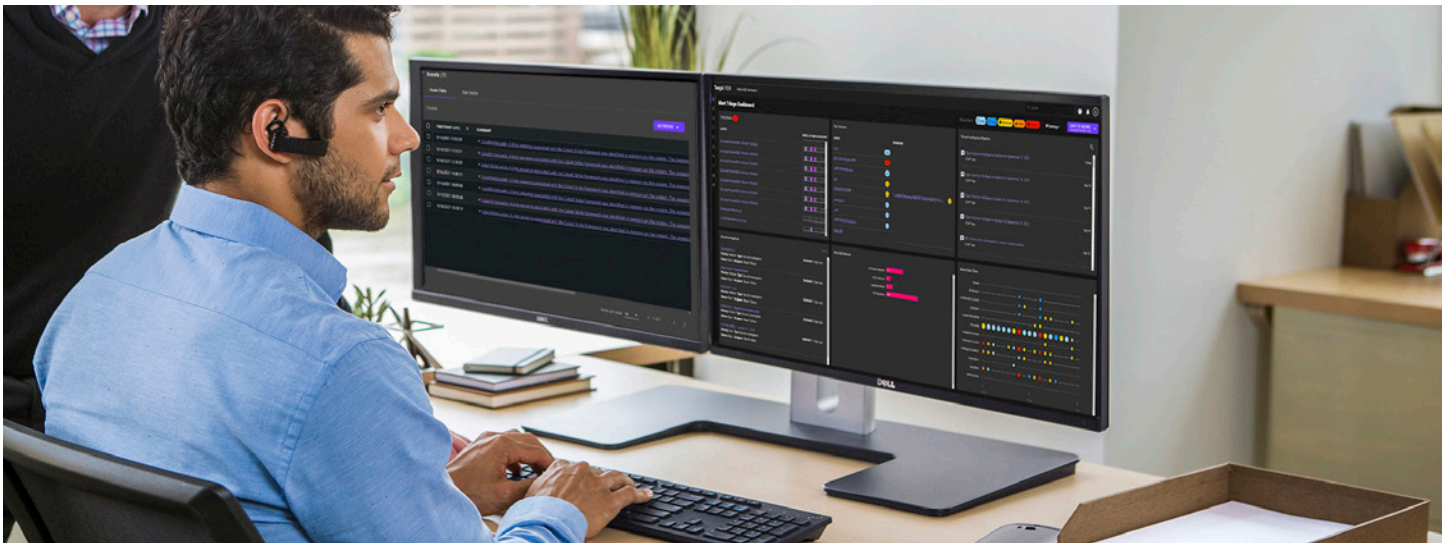
Dell MDR forma parte de una iniciativa que lleva varias décadas desarrollando servicios de TI inigualables en la organización. Esto significa que los expertos en ciberseguridad de Dell MDR no solo ofrecen una orientación excepcional para corregir las amenazas, sino que también cuentan con los conocimientos para gestionarlas en cualquier organización.

Persecución de amenazas: identificación de amenazas que podrían eludir los sistemas automáticos

Los atacantes conocen los sistemas de detección automáticos, por lo que se dedican a desarrollar nuevos tipos de ataques, o variaciones de ataques existentes, a fin de burlarlos. En un sistema como Taegis XDR, es una tarea difícil, pero no imposible.

Los analistas de seguridad aplican la persecución de amenazas para identificar estos ataques "ninja". La persecución de amenazas busca signos de vulneración, como, por ejemplo, una serie de intentos de inicio de sesión fallidos seguidos por un intento con éxito, intentos de inicio de sesión anómalos (fuera del horario laboral normal) o modificaciones constantes a un archivo en un periodo de tiempo breve.

La persecución de amenazas eficaz se logra combinando la tecnología y los profesionales. La plataforma Taegis XDR ofrece una cantidad enorme de información sobre la actividad de los intrusos; los analistas de Dell MDR examinan esta información para identificar incluso las actividades mejor ocultas.



CONOZCA DELL MDR

Las noticias le informan sobre los problemas que tienen las administraciones públicas y las empresas globales para frenar las amenazas de ciberseguridad. Las empresas pequeñas y medianas ya no tienen que enfrentarse a esta situación solas. Con Dell MDR, su organización puede beneficiarse de expertos en seguridad altamente formados dedicados a protegerle a usted, así como de una plataforma de seguridad líder del sector, Secureworks Taegis XDR. Su organización puede aprovechar la capacidad de Dell para invertir en personas, procesos y herramientas y crear un servicio de seguridad gestionado a la medida de las necesidades de su empresa. El servicio Dell Managed Detection and Response ofrece una ciberseguridad de primera clase a todo el mundo.

Más información acerca de Dell MDR.

Póngase en contacto con uno de nuestros expertos de MDR.

1. Los ataques se incrementaron en un 69 %, según el FBI: https://blog.isc2.org/isc2_blog/2021/03/fbi-cybercrime-shot-up-in-2020-amidst-pandemic.html.
2. El 34 % de los ataques involucraron a personal interno: https://www.verizon.com/business/resources/reports/dbir/.
3. El 67 % no confían en la capacidad para recuperarse tras un ciberataque destructivo: www.delltechnologies.com/gdpi
4. El 82 % de los empleadores afirman que existe una escasez de conocimientos sobre ciberseguridad.: https://www.csis.org/analysis/cybersecurity-workforce-gap
5. Los trece perfiles de TI más difíciles de contratar: https://www.cio.com/article/221772/10-most-difficult-it-jobs-for-employers-to-fill.html

DELL Technologies