Enterprise Strategy Group | Getting to the bigger truth.™

Solucione las carencias en las operaciones de seguridad con MDR

El riesgo de sufrir ciberataques dañinos no deja de aumentar y afecta negativamente a la atención y los presupuestos, que deberían dedicarse a los objetivos principales de la empresa; por ello, las organizaciones deben responder reforzando los programas de ciberseguridad. En todos los programas de ciberseguridad, las operaciones de seguridad (SecOps) son vitales, y su cometido es supervisar y proteger todos los ámbitos de la superficie de ataque digital.

Pese a las inversiones, las operaciones de seguridad son más complejas

MÁS DE LA MITAD
de los encuestados opina que las SecOps son **más complejas** en la actualidad que hace años.

» **Los cinco motivos principales por los que las SecOps sonmás complejas.**

1. **41%** El panorama de amenazas cambia y evoluciona rápidamente
2. **39%** La superficie de ataque cambia y evoluciona constantemente
3. **37%** Ha aumentado la cantidad y la complejidad de las alertas de seguridad
4. **34%** Mi organización utiliza más servicios de cloud pública
5. **33%** Es difícil mantenerse al día con las necesidades operativas de las tecnologías de operaciones de seguridad

Rediseñe las estrategias del programa

Las superficies de ataque y la variedad de las amenazas han aumentado tanto en tamaño como en complejidad, y también lo ha hecho la aplicación de controles de seguridad, que generan miles de alertas y grandes cantidades de datos de seguridad. Los equipos de seguridad se están replanteando las operaciones generales del programa para incorporar aún más datos sobre los activos y los riesgos de los equipos de la línea de negocio y de TI, con el fin de centrarse en las amenazas que representan mayor riesgo para los objetivos de la organización.

98% de las organizaciones ya se ha comprometido con un proveedor de MDR o tiene previsto hacerlo en los próximos 12 meses.

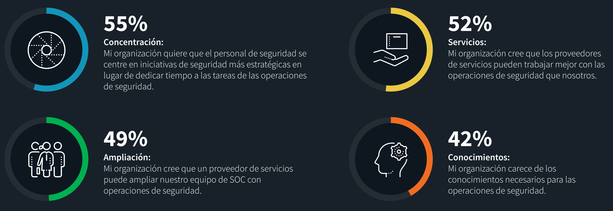
88% de estas organizaciones se plantea aumentar el uso de MDR en los próximos 12 meses.

» **Factores impulsores clave del uso de MDR.**

MEJORA Y EFICIENCIA OPERATIVAS.
MDR ayuda a las organizaciones a reducir el coste total de las operaciones de seguridad en diversos aspectos, como la infraestructura, el personal y la gestión. También puede abordar el problema del "agotamiento por las alertas" y mejorar la probabilidad de reducir significativamente los falsos positivos.

INCREMENTO DE LA EFICACIA DE LA CIBERSEGURIDAD Y REDUCCIÓN DE LOS RIESGOS.
MDR ayuda a las organizaciones a frenar las amenazas activas, mejorar la detección de posibles amenazas y ataques persistentes avanzados, establecer una búsqueda de amenazas proactiva e instaurar controles más eficaces para detectar y prevenir futuros ataques.

» **Principales raisons pour lesquelles votre organisation utilise ou prévoit utiliser les services gérés.**



55%
Concentración:
Mi organización quiere que el personal de seguridad se centre en iniciativas de seguridad más estratégicas en lugar de dedicar tiempo a las tareas de las operaciones de seguridad.

52%
Servicios:
Mi organización cree que los proveedores de servicios pueden trabajar mejor con las operaciones de seguridad que nosotros.

49%
Ampliación:
Mi organización cree que un proveedor de servicios puede ampliar nuestro equipo de SOC con operaciones de seguridad.

42%
Conocimientos:
Mi organización carece de los conocimientos necesarios para las operaciones de seguridad.

> **Muchas de las soluciones MDR denominadas de "Generación 1.0" se diseñaron e implementaron para un escenario diferente,** con menos datos y amenazas, además de procesos de detección más sencillos."
>
> *- Dave Gruber, analista principal de ESG*

Nuevos requisitos para MDR

Muchas de las soluciones MDR denominadas de "Generación 1.0" se diseñaron e implementaron para un escenario diferente, con menos datos y amenazas, además de procesos de detección más sencillos". Las soluciones MDR de última generación deben estar equipadas para proteger una superficie de ataque más diversa, detectar amenazas más complejas y establecer un enfoque más centrado en los riesgos respecto al establecimiento de prioridades y mitigación de las amenazas.

- Supervisión 24x7 de eventos y registros
- Información rápida 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 posibles proveedores de servicios que ofrecen subcontratación de algunas, muchas o todas las prestaciones de MDR, **las organizaciones deben buscar socios que puedan de ofrecer:**

- Inteligencia contextual contra ciberamenazas
- 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 MDR basada en la cloud
- Extensas prestaciones en entornos multicloud y de cloud híbrida, confianza cero y el modelo de responsabilidad compartida de la seguridad de la cloud
- Capacidad demostrada para ampliar sus servicios con el tiempo, con base en tecnología innovadora, procesos probados y conocimientos probados entre su personal

La mayor verdad

El riesgo de sufrir ciberataques dañinos no deja de aumentar y afecta negativamente a la atención y los presupuestos, que deberían dedicarse a los objetivos principales de la empresa; por ello, las organizaciones deben reforzar los programas de ciberseguridad. Aunque los casos de uso varían, la mayoría trabajan con proveedores de servicios de MDR para ampliar y adaptar sus programas.

El enfoque de Dell Technologies relativo a los servicios de detección y respuesta gestionadas combina una tecnología flexible, inteligente y ampliable junto con profesionales de ciberseguridad experimentados, lo que ayuda a las organizaciones de todos los tamaños y diferentes recursos a agilizar y reforzar los programas de seguridad.

MÁS INFORMACIÓN

DELL Technologies

Fuente: Resultados integros de la encuesta de ESG, *SOC Modernization and the Role of XDR*, agosto de 2022.