Hoja técnica

ThreatDown
Powered by Malwarebytes

Detección y Respuesta Gestionada de ThreatDown

Protege tu organización con monitorización gestionada de amenazas 24x7x365, investigación y remediación por parte de nuestros expertos analistas MDR

Resumen

Para los equipos de seguridad de organizaciones pequeñas y medianas, ofrecer servicios de seguridad de alta calidad y mantener los entornos empresariales libres de amenazas requiere un equipo cualificado que pueda ofrecer cobertura las 24 horas del día, los 7 días de la semana. Sin embargo, muchas organizaciones se enfrentan a recursos limitados de personal y carecen de una profunda experiencia en ciberseguridad. Además, están constantemente sobrecargados con responsabilidades de triaje de alertas. Añadir
A esto se suma el coste y la complejidad disparados de gestionar múltiples soluciones para descubrir amenazas ocultas, lo que conduce a ineficiencias y tiempos de respuesta a incidentes prolongados.

Los equipos de seguridad restringida necesitan una forma sencilla, eficiente y rentable de detectar y responder a amenazas

ThreatDown, impulsado por Malwarebytes, alivia estos desafíos con una oferta de detección y respuesta gestionada (MDR) diseñada específicamente para ese propósito. ThreatDown MDR ofrece una opción potente y asequible de detección y remediación de amenazas con monitorización e investigaciones 24x7x365 por parte de nuestros analistas de seguridad de primer nivel. Tu empresa adoptará una postura de ciberresiliencia con servicios expertos que aceleran la detección de amenazas y realizan la respuesta a incidentes con precisión. ThreatDown MDR ofrece opciones flexibles de respuesta a amenazas que se adaptan tanto a las necesidades de tu empresa como a tu entorno de seguridad, asegurando que mantengas plena visibilidad y control sobre tus endpoints.

Ventajas de ThreatDown MDR

- **Monitorización 24x7x365**: Monitorizamos endpoints y realizamos investigaciones expertas día y noche, entre semana, fines de semana y festivos. Siempre estamos vigilando.

Retos

- Recursos limitados para cubrir necesidades de seguridad – el 67% reportó escasez de personal en ciberseguridad1
- Demasiadas alertas provocan fatiga de alerta: el 80% de las alertas EDR son detectadas por IT[2]
- La respuesta lenta permite a los atacantes tener más tiempo en tus endpoints : 277 días de media para identificar y contener una brecha3

Beneficios

Protege los puestos de trabajo, servidores y más de tu organización con ThreatDown MDR

- Mejor Seguridad – Mitigar proactivamente el riesgo antes de una brecha
- Menos esfuerzo – Ahorra recursos a tu equipo confiando en analistas de seguridad expertos de ThreatDown para ayudarte a monitorizar, investigar y remediar actividades sospechosas
- Mejor relación calidad-precio – Lograr tiempos de respuesta y remediación más rápidos, a un coste significativamente menor en comparación con los propios esfuerzos de gestión de los clientes

[1] informe sobre el estado de malware de Malwarebytes. [2] investigación de ThreatDown. [3] coste de un informe de brecha de datos 2023.

- **Analistas MDR cualificados**: Nuestro equipo de expertos en seguridad es un cazador de amenazas experimentado con amplia experiencia en respuesta a incidentes y décadas de experiencia en la clasificación y mitigación de amenazas complejas de malware.

- **EDR galardonado**: Impulsado por nuestra plataforma ThreatDown Endpoint Detection and Response (EDR) y enriquecido con múltiples fuentes de inteligencia de amenazas, incluyendo MITRE y otros.

- **Opciones flexibles de remediación**: Nuestro equipo MDR puede remediar activamente las amenazas a medida que se descubren o ofrecer un gran alcance, Guía práctica para que los equipos de TI sigan en sus propios esfuerzos de remediación.

- **Caza activa de amenazas**: Nuestro equipo MDR busca amenazas no vistas basándose en indicadores pasados de compromiso (IOC) y sospechosas actividad observada en los puntos finales.

- **Despliegue rápido**: ThreatDown EDR es conocido por su facilidad de configuración, permitiendo que tu equipo de seguridad integre rápidamente nuevos endpoints en nuestro servicio MDR 24/7 en cuestión de minutos.

¿Cómo funciona?

Una vez desplegados los agentes de endpoint, el servicio MDR se activa en cuestión de minutos y los analistas de ThreatDown pueden monitorizar el entorno del cliente. Los datos de detección se ingieren en la plataforma de Gestión de Información y Eventos de Seguridad (SIEM) y de Orquestación, Automatización y Respuesta de Seguridad (SOAR) de MDR, donde se enriquecen con fuentes de inteligencia de amenazas internas y externas. Este proceso acelera la identificación, análisis y triaje (priorización e investigación de respuestas) de los eventos de seguridad. En este punto, la plataforma MDR SIEM/SOAR verifica las alertas de actividad sospechosa como amenazas reales o detecciones benignas y puede aumentar la calificación de gravedad de ciertas detecciones EDR basándose en inteligencia de amenazas. Los casos que requieren remediación son completados por el analista o se proporciona orientación al cliente o al MSP si han optado por realizar sus propias acciones de remediación.

Reconocimientos de la industria de ThreatDown

La clasificación constante de la certificación de Nivel 1 en las pruebas MRG Effitas 360 degree y la #1 Endpoint Security Suite por G2 validan la solución eficaz y fácil de usar de ThreatDown.

Más información

Para saber más sobre cómo ThreatDown MDR puede ayudar a reducir el riesgo cibernético de tu organización, visita threatdown.com/mdr.