

FICHA TÉCNICA

Managed Defense

Detección y respuesta gestionadas (MDR) respaldadas por toda la potencia de Soluciones Mandiant



ASPECTOS DESTACADOS

- **Información sobre amenazas líder en el mercado:** los analistas de seguridad de múltiples equipos en FireEye y Soluciones Mandiant aplican la inteligencia artificial, de víctimas y adversarios más reciente y en tiempo real para localizar y detallar las amenazas en su entorno con mayor rapidez.
- **Priorización de alertas:** identificar las alertas más críticas para enfocarse en aquellas que requieren una respuesta inmediata.
- **Búsqueda exhaustiva:** los analistas buscan atacantes ocultos y actividades de amenazas de forma activa mediante el uso de la tecnología existente, junto con la experiencia analítica y la inteligencia de Mandiant.
- **Expertos en seguridad:** comuníquese con un punto de contacto primario que facilite soporte adicional, como análisis de muestras de malware, análisis forense en profundidad o respuesta a incidentes en el sitio.
- **Cobertura las 24 horas del día, los 7 días de la semana:** los centros de operaciones de seguridad (*Security Operations Center*, SOC) en Estados Unidos (Virginia), Irlanda y Singapur brindan cobertura las 24 horas del día, los 7 días de la semana.

La tecnología por sí sola no puede brindar protección completa contra un atacante determinado, persistente y sigiloso. La experiencia humana puede complementar la tecnología para ofrecer flexibilidad, ingenio y enfoque, especialmente contra ataques avanzados de etapas múltiples y para la actividad relacionada con la respuesta. Sin embargo, es difícil y costoso encontrar, contratar, capacitar y retener a los expertos en seguridad.

Los equipos de seguridad necesitan un socio de confianza para supervisar su red en todo momento, con un enfoque proactivo y orientado a los analistas que utilice la información sobre amenazas más reciente a partir de la experiencia de primera línea.

Mandiant Managed Defense es un servicio de detección y respuesta gestionadas (*Managed Detection and Response*, MDR) que combina la experiencia en ciberseguridad reconocida por la industria, la tecnología de Mandiant y el conocimiento sin precedentes de los atacantes para ayudar a minimizar el impacto de una vulneración.

Detección y respuesta basada en información

Managed Defense se alimenta continuamente de la capacidad mundial de información sobre amenazas cibernéticas más grande del sector, que aprovecha la inteligencia artificial, campaña, adversarios y víctimas adquiridas en la primera línea de los ciberataques de mayores consecuencias en el mundo. Esta inteligencia y experiencia de primera línea impulsa la detección y guía las actividades de búsqueda e investigación de nuestros analistas para revelar incluso al atacante más sofisticado. Los analistas de seguridad proporcionan una evaluación integral de la actividad de los atacantes junto con recomendaciones de respuesta personalizadas y ofrecen el contexto necesario para comprender las amenazas, evaluar los riesgos y tomar medidas definitivas.

Cómo funciona

Managed Defense utiliza nuestro componente tecnológico exclusivo para proporcionar visibilidad en tiempo real en toda la empresa, que incluye un sistema de control industrial (*Industrial Control System*, ICS) e infraestructura en la nube. Los analistas de Managed Defense aprovechan la información sobre amenazas basadas en adversarios, víctimas y máquinas para detectar e investigar amenazas.

Se le notificará de inmediato si se abre una investigación debido a una evidencia de vulneración. Podrá hacer un seguimiento del estado de esas investigaciones realizadas por un portal seguro mientras nuestros analistas continúan trabajando en el problema hasta solucionarlo.

También recibirá un informe resumido detallado que proporciona un contexto de amenaza junto con recomendaciones de corrección para formar una respuesta efectiva y ayudar a prevenir que los atacantes completen su misión.

Opciones adicionales de Managed Defense

Además del servicio disponible las 24 horas del día, los 7 días de la semana, hay otras versiones de Managed Defense disponibles para sus necesidades específicas:

Managed Defense para FireEye Endpoint Security

Aumente su equipo de seguridad para acelerar las actividades de detección e investigación en todos los endpoints. Los consultores de Managed Defense se asociarán con su equipo y aprovecharán FireEye Endpoint Security para manejar las detecciones de amenazas conocidas, detecciones avanzadas que requieren análisis de comportamiento y adquisiciones forenses desde un endpoint vulnerado.

Managed Defense: noches y fines de semana

Obtenga acceso continuo a experiencia en detección y respuesta gestionadas con soporte fuera del horario de servicio (noches, fines de semana, feriados). Es ideal para una organización que busca expandir la visibilidad de su centro de operaciones de seguridad interna a las 24 horas del día, los 7 días de la semana sin tener que aumentar gastos para reclutar, capacitar y retener equipos adicionales.

Managed Defense para tecnología operativa (*Operational Technology, OT*)

Implemente un servicio de detección y respuesta gestionadas (MDR) que aproveche todo el potencial de Soluciones Mandiant y los proveedores de herramientas de tecnología operativa (OT) líderes. Especialmente adaptado para el entorno de OT, Managed Defense para OT utiliza el componente tecnológico exclusivo de FireEye para proporcionar visibilidad en tiempo real en toda la empresa, lo que incluye un sistema de control industrial (ICS) e infraestructura en la nube.

Por qué Mandiant

Mandiant ha sido el líder en el líder en materia de ciberseguridad e inteligencia de ciberamenazas desde 2004. Nuestros responsables de la respuesta a incidentes están en las primeras líneas de las brechas más complejas en todo el mundo. Tenemos una comprensión exhaustiva en lo que respecta a perpetradores existentes y emergentes, además de sus herramientas, tácticas y procedimientos que cambian rápidamente.

POR QUÉ MANAGED DEFENSE

- **Experiencia**
Aproveche la experiencia de los equipos de respuesta a incidentes de Mandiant, que dedican más de 200 000 horas por año a las vulneraciones más impactantes.
- **Detección más rápida**
El tiempo promedio para investigar y brindar una respuesta con Managed Defense es de 67 minutos.
- **Rentabilidad**
El desarrollo y el mantenimiento de las capacidades internas puede requerir mucho tiempo, dinero y recursos.
- **Información**
Acceso a la recopilación de información calibre estado-nación respaldada por más de 150 analistas de información.
- **Defensa potente**
El componente tecnológico exclusivo incorpora la tecnología de FireEye y Mandiant Threat Intelligence.
 - Hay 150 millones de detecciones de productos de FireEye.
 - Ingresan 22 millones de alertas de Managed Defense.
 - Existen 170 000 investigaciones de analistas.
 - El 91 % de amenazas de alta prioridad se resuelven sin una respuesta rápida.
 - El 98 % de los incidentes de respuesta rápida se resuelven sin una respuesta completa a los incidentes.

Para obtener más información acerca de Soluciones Mandiant, visite www.FireEye.com/mandiant

FireEye, Inc.

601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

©2020 FireEye, Inc. Todos los derechos reservados. FireEye y Mandiant son marcas comerciales registradas de FireEye, Inc. Todas las demás marcas, productos o nombres de servicios son o pueden ser marcas comerciales o marcas de servicios de sus respectivos propietarios. MD-EXT-DS-US-EN-000115-03

Acerca de Soluciones Mandiant

Soluciones Mandiant reúne la experiencia de información sobre amenazas y de primera línea más importante del mundo con una validación de la seguridad continua a fin de armar a las organizaciones con las herramientas necesarias para aumentar la eficacia de la seguridad y reducir el riesgo comercial.

