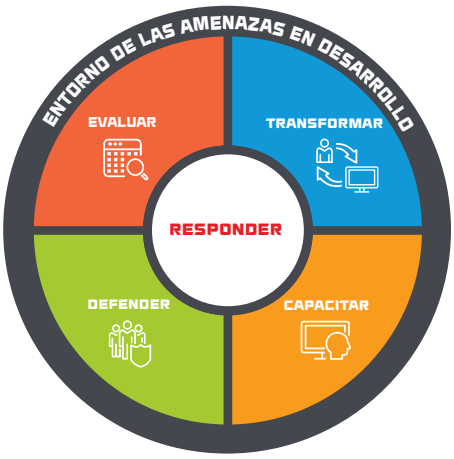
FIREEYE™

FICHA TÉCNICA

Servicios de consultoría y MDR de Mandiant

Respondemos a los ataques serios y capacitamos a las organizaciones para proteger sus activos

Infraestructura de las necesidades de seguridad



"Mandiant es líder en ayudar a las organizaciones a reconsiderar cómo deben prepararse para los ataques a la seguridad".

Michael Chertoff,
ex Secretario de Seguridad Nacional

Mandiant Difference

FireEye Mandiant ha sido el líder en cuanto a ciberseguridad e inteligencia sobre amenazas cibernéticas desde 2004. Nuestros responsables de la respuesta ante incidentes han estado 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.

Brindamos respuesta a incidentes cibernéticos líder en la industria y servicios de seguridad contra riesgos basados en inteligencia para ayudar a las organizaciones a superar a los atacantes, antes, durante y después de un incidente.

Con un profundo conocimiento del comportamiento del atacante, inigualable inteligencia sobre amenazas y tecnología especialmente diseñada, los servicios de evaluación de seguridad, transformación, capacitación y detección y respuesta gestionadas (*Managed Detection and Response*, MDR) de Mandiant ayudan a desarrollar resistencia funcional y cerrar brechas de seguridad para reducir el riesgo comercial.

Experiencia: experiencia de más de 15 años en primera línea respondiendo a los ataques de mayor gravedad. Observamos lo que los agresores hicieron, cómo lo hicieron, las herramientas y técnicas que utilizaron y cuál era su objetivo. Esto nos permite analizar el panorama completo, comprender la conducta cambiante del atacante y sus motivaciones de una forma que otros no pueden.

Inteligencia: el método basado en información que utiliza Mandiant para prestar servicios incorpora información de ciberamenazas líder en la industria proveniente de cientos de expertos, miles de investigaciones de Mandiant, productos de FireEye y nuestro servicio Defensa administrada (Managed Defense) para obtener una visibilidad a nivel mundial del entorno de amenazas que cambia rápidamente.

Tecnología: los expertos de Mandiant aprovechan la tecnología de endpoint de FireEye, los sensores de red y las plataformas de análisis que pueden operar desde la nube o en el sitio, según las necesidades del cliente, en tanto que el sistema operativo sea Windows, Linux o macOS. Esta tecnología permite una respuesta rápida a una escala mayor, lo que minimiza los gastos.

Resumen de los servicios seleccionados de Mandiant.

Función de seguridad	Necesidad de seguridad	Servicios	Descripción general	Ventaja
Responder	**Respuesta ante vulnerabilidades**	**Servicios de respuesta ante incidentes**	Investigar, contener y corregir los incidentes de seguridad críticos mediante velocidad, adaptabilidad y eficiencia.	Resolver graves incidentes de seguridad y establecer soluciones a largo plazo.
		Contrato de servicio de respuesta ante incidentes	Términos y condiciones establecidos para servicios de respuesta ante incidentes.	Reduce de manera considerable el tiempo de respuesta, lo que reduce el impacto general de un ataque.
Evaluar	**Verificar la presencia del atacante**	**Evaluación de riesgos**	Identificar los riesgos anteriores o presentes de su entorno, evaluar los riesgos futuros con respecto a la vulnerabilidades en función de su nivel de seguridad y mejorar su capacidad de respuesta.	Saber si su organización está sufriendo un ataque o lo ha sufrido anteriormente.
	Prepárese para responder	**Evaluaciones del equipo rojo y el equipo púrpura**	Pone a prueba su postura de seguridad con las últimas herramientas, tácticas y procedimientos (*Tools, Tactics and Procedures*, TTP) de los atacantes que vemos en las primeras líneas de Respuesta ante incidentes.	Identifica puntos débiles no detectados previamente antes de que lo haga un agresor.
		Evaluación de la capacidad de respuesta	Evaluación independiente de su capacidad de respuesta y supervisión de la seguridad, basada en nuestra experiencia en la primera línea de la respuesta ante incidentes.	Evaluar la eficacia de su programa de seguridad de la información para mejorar su nivel de seguridad y reducir el riesgo comercial.
		Ejercicio de simulación	Pruebe el plan de respuesta a incidentes cibernéticos de su organización con el escenario simulado	Identifique de manera rápida y eficiente las brechas entre el proceso documentado y la respuesta real.
	Evalúa los controles de seguridad y la postura de seguridad.	**Security Program Assesment**	Evaluación detallada de los programas de seguridad de la información de su organización en diez dominios de seguridad claves, cada uno de los cuales corresponde a marcos de cumplimiento de normativas, seguridad e industria.	Evaluar la eficacia de su programa de seguridad de la información para mejorar su nivel de seguridad y reducir el riesgo comercial.
		Diagnóstico de fallos del sistema de control industrial (*Industrial Control System*, ICS)	Evaluación mínimamente invasiva del nivel de ciberseguridad general de una instalación industrial, cerrando brechas entre la seguridad de TI y TO.	Comprender las vulnerabilidades expuestas del sistema de control industrial (ICS) y establecer un plan para reducir los riesgos de ciberseguridad del sistema.
		Evaluación de seguridad de Active Directory	Mitigar el riesgo de configuraciones incorrectas de Active Directory, debilidades de procesos y métodos de explotación.	Reducir el riesgo y el impacto de un incidente de seguridad al fortalecer una superficie de ataque común.
		Evaluaciones de la infraestructura de la nube	Mejorar las defensas cibernéticas a través de una mejor arquitectura y configuraciones en la nube.	Mitigar el riesgo al reducir la superficie de ataque en la nube de las técnicas de explotación comunes.
Transformar	**Postura de seguridad consolidada**	**Desarrollo de un centro de ciberdefensa (*Cyber Defense Center Development*, CDC)**	Diseñar y desarrollar un programa de operaciones de seguridad para defenderse de perpetradores avanzados.	Mejorar la postura de defensa para reducir el impacto de los incidentes de seguridad; Crear consenso sobre mejoras de seguridad y priorización de recursos
Capacitar	**Capacitar a mi equipo**	**Capacitación en cuanto al producto, la inteligencia y la experiencia**	Capacite a su equipo de seguridad para obtener conocimiento sobre amenazas actualizado y mejorar las habilidades operativas que necesitan para combatir de manera eficaz el cambiante entorno de las ciberamenazas.	Exponga a su equipo a ejercicios de aprendizaje y capacitación que se basan en investigaciones del mundo real, no en escenarios teóricos.
Defender	**Detección y respuesta gestionadas**	**Managed Defense**	Un servicio 24 horas al día, 7 días a la semana dirigido por expertos, que combina experiencia de primera línea con tecnología e inteligencia líderes en la industria.	Identifica las amenazas de manera temprana para ayudar a minimizar el impacto de una brecha.
		Defensa gestionada para el endpoint	Un servicio de 24 horas al día, 7 días a la semana dirigido por expertos, que utiliza Fireeye Endpoint Security para detectar, investigar y contener rápidamente amenazas en el endpoint.	Mejora la visibilidad en toda la red y acelere la respuesta.
		Defensa gestionada para la tecnología operativa (TO)	Un servicio de 24 horas al día, 7 días a la semana que aprovecha la experiencia especializada para identificar riesgos y acelerar la respuesta para los sistemas de control industrial (ICS) y la tecnología operativa (TO).	Mejora la postura defensiva del entorno de los ICS/TO y reduce el impacto de los eventos de seguridad.

Para obtener más información sobre FireEye, visite: **www.FireEye.com**

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

M-EXT-DS-US-EN-000116-02

Acerca de FireEye, Inc

FireEye es una empresa de seguridad basada en información. FireEye, que funciona como una extensión escalable y transparente de las operaciones de seguridad del cliente, ofrece una sola plataforma que combina tecnologías innovadoras de seguridad, inteligencia sobre amenazas similar a la de una nación y los servicios de consultoría de fama mundial de Mandiant®. Gracias a este enfoque, FireEye elimina la complejidad y la carga de la seguridad cibernética para las organizaciones que desean estar preparadas y responder ante los ataques cibernéticos, además de prevenirlos.