MANDIANT®

FICHA TÉCNICA

Evaluación de riesgos

Identificar actividad maliciosa continua o anterior en su entorno

¿POR QUÉ ELEGIR MANDIANT SOLUTIONS?

Mandiant Solutions ha sido el líder en materia de ciberseguridad e información sobre amenazas cibernéticas desde 2004. Nuestros responsables de la respuesta a 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 tácticas, técnicas y procedimientos que cambian rápidamente.

VENTAJAS

- Análisis exhaustivo de su entorno específico centrado en encontrar evidencia de riesgos presentes o pasados
- Proporciona visibilidad a riesgos y exposiciones sistémicos
- Identifica los problemas en materia de seguridad
- Brinda recomendaciones para mejorar aún más la capacidad de su organización de responder de manera eficaz a los incidentes futuros
- Flexibilidad para implementar tecnología en el sitio o albergada en la nube

En nuestro actual estado de ciberseguridad, las vulneraciones de seguridad son inevitables.

– Kevin Mandia
Director Ejecutivo de FireEye

Mandiant Compromise Assessment combina nuestra vasta experiencia de respuesta a las intrusiones realizadas perpetradores avanzados, la inteligencia ante amenazas líder en la industria y la tecnología de FireEye para entregar una evaluación que brinde lo siguiente:

- Identificación de intrusiones en curso o anteriores dentro de su organización
- Evaluación de los riesgos al identificar los puntos débiles de la arquitectura de seguridad, las vulnerabilidades, el uso inadecuado por las violaciones de la política y los errores de la configuración de seguridad del sistema
- Aumenta la capacidad de su organización de responder de manera eficaz a los incidentes futuros

La necesidad de Compromise Assessments

Las infracciones de datos de alto nivel que aparecen en las noticias representan solo una fracción de las actividades de intrusión que se llevan a cabo en todo el mundo. Saber si su organización ha sido objeto de una intrusión e identificar formas para reducir los riesgos es algo fundamental para evitar que su organización se convierta en la siguiente infracción de datos importantes que aparezca en los titulares de los periódicos.

Nuestro método

Combinamos nuestra vasta experiencia en cuanto a respuesta a intrusiones y la inteligencia de amenazas líder en la industria con un componente modular de la tecnología de FireEye para entregar una evaluación que satisfaga sus objetivos comerciales con rapidez, escala y eficiencia. Además de identificar evidencias de actividad maliciosa pasada o presente, la evaluación ofrece lo siguiente:

Contexto que deriva de la inteligencia de amenazas

Brinda una perspectiva con respecto a la atribución y motivación del atacante para que las organizaciones sepan si están siendo objeto de ataques.

Identificación de riesgos

Identificar los puntos débiles en la arquitectura y configuración de seguridad, como por ejemplo, parches o software de seguridad faltantes.

Facilitación de investigaciones futuras

Recomienda opciones estratégicas que pueden preparar mejor al equipo de seguridad de su organización en su respuesta a las intrusiones.

Los consultores de Mandiant utilizan las tecnologías de FireEye para realizar búsquedas en los endpoints, monitorear el tráfico de la red, inspeccionar los correos electrónicos y analizar los registros de otros dispositivos de seguridad para detectar evidencia de actividad maliciosa. Los consultores también utilizan técnicas de análisis de datos sin firma para encontrar actividades maliciosas inadvertidas anteriormente. Los clientes optan por la combinación correcta de tecnologías que sea la más adecuada para su entorno.

- Inspección del endpoint: los agentes de FireEye Endpoint Security se utilizan para brindar protección en tiempo real de las actividades maliciosas, como por ejemplo malware y otras tácticas, técnicas y procedimientos, y para investigar los endpoints de Windows, macOS y Linux. Los expertos de Mandiant brindan la flexibilidad que significan las implementaciones in situ y en la nube.
- Inspección de redes: los sensores de FireEye Network Security se implementan en ubicaciones estratégicas de supervisión en su empresa a fin de detectar actividades de vulneración como comunicaciones de comando y control de malware, acceso remoto no autorizado y robo de datos.
- Inspección de correo electrónico: la supervisión de FireEye Email Security se realiza en el sitio o desde la nube y se puede configurar para que inspeccione de forma pasiva el correo electrónico entrante y saliente. La inspección dinámica de archivos adjuntos permite que los expertos de Mandiant identifiquen las campañas de intrusión antes que otros productos basados en firmas.
- Inspección de registros: los consultores de Mandiant hacen uso de varias tecnologías para realizar revisiones de registros desde las aplicaciones y la infraestructura a fin de identificar la actividad maliciosa.

INSPECCIÓN DEL ENDPOINT

- Alertas en tiempo real de actividades sospechosas o maliciosas en curso
- Detección de malware común mediante la utilización del motor antivirus integrado del agente de FireEye
- Soporte de múltiples sistemas operativos
  - Windows
  - macOS
  - Linux
- Identificación de anomalías que podrían indicar la presencia de malware avanzado

INSPECCIÓN DE REDES

- Captura de paquetes completos combinada con firmas de detección personalizadas
- Detección y decodificación automáticas de comandos del atacante y tráfico de control

INSPECCIÓN DE CORREO ELECTRÓNICO

- Detecta ataques de phishing específico que utilizan los atacantes para volver a obtener acceso al entorno después de un evento de remediación
- Aprovecha el motor Multi-Vector Virtual Execution™ (MVX) sin firma para analizar archivos adjuntos de correo electrónico y URL en función de una matriz cruzada integral de los sistemas operativos, aplicaciones y navegadores web
- Admite el análisis de las imágenes de los sistemas operativos Microsoft Windows y macOS
- Analiza las amenazas ocultas en archivos, como archivos adjuntos protegidos por contraseña y cifrados

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

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

Acerca de Mandiant Solutions
Mandiant Solutions 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.

MANDIANT®