FIREEYE™

**FICHA TÉCNICA**

# Evaluación de la defensa contra el ransomware

## VENTAJAS

- Identificación de activos con mayor riesgo de ser afectados por ransomware
- Identificación de los puntos débiles de seguridad atacados por ransomware
- Identificación de los controles de acceso relajados en archivos compartidos
- Reconocimiento de las deficiencias operativas en la gestión de tareas de ransomware
- Recepción de recomendaciones y orientaciones altamente procesables para mitigar los ataques de ransomware

**Por qué FireEye Mandiant**
FireEye Mandiant ha sido el líder en cuanto a ciberseguridad e inteligencia sobre amenazas cibernéticas desde 2004. Nuestros responsables de la respuesta ante incidentes están en las primeras líneas de las brechas más complejas en todo el mundo. Contamos con un entendimiento profundo de los perpetradores y sus tácticas, técnicas y procedimientos (tactics, techniques and procedures, TPP) que cambian rápidamente ya que aprovechamos nuestras fuentes combinadas de información sobre adversarios, máquinas y víctimas.

La Evaluación de la defensa contra el ransomware se desarrolló con base en una amplia experiencia en la respuesta y reparación de incidentes de ransomware y en la recopilación de información sobre amenazas en ransomware emergente y en evolución.

**Descripción general**
La Evaluación de la defensa contra ransomware de FireEye Mandiant evalúa la efectividad de la capacidad de una organización para prevenir, detectar, contener y remediar un ataque de ransomware. Los expertos de Mandiant evalúan los elementos técnicos y no técnicos de su programa de seguridad para determinar cómo responderá su equipo a un ataque de ransomware.

Los expertos de Mandiant evalúan el impacto técnico que un ataque de ransomware podría tener en su red interna, descubren qué datos podrían estar en peligro o se pierden y prueban las fortalezas y debilidades de la capacidad de sus controles de seguridad para detectar y responder a un ataque de ransomware.

**Metodología**
La Evaluación de la defensa contra ransomware incluye revisión de documentación, análisis de configuración del registro, talleres de inmersión profunda y simulaciones del comportamiento real de ataques de ransomware.

La Evaluación de la defensa contra ransomware se enfoca en cuatro competencias principales sobre ransomware:

- **Arquitectura de seguridad.** Las tecnologías de seguridad, controles y redes necesarias para defenderse contra un ataque de ransomware y continuar con las operaciones comerciales.
- **Respuesta.** La capacidad de una organización de responder y contener rápidamente un ataque de ransomware.
- **Comunicaciones.** Los procesos de comunicación interna y externa se utilizan para entregar mensajes corporativos a las partes interesadas clave. Incluye coordinación con seguros cibernéticos y asesoría legal.
- **Recuperación.** Los procesos y el enfoque para remediar o recuperarse de un ataque de ransomware.

Nuestras simulaciones del comportamiento real de ataques de ransomware:

- Analizan vulnerabilidades de Windows explotadas por ransomware
- Analizan archivos compartidos accesibles a los que el ransomware puede acceder
- Simulan el movimiento lateral del ransomware intentando explotar las vulnerabilidades descubiertas o reutilizar las credenciales recopiladas
- Prueba la segmentación entre redes para determinar si el ransomware puede propagarse a otros entornos, como:
  - Redes de fabricación y planta
  - Redes de infraestructura de copias de seguridad
  - Redes minoristas
  - Otras redes seguras
- Simula el comportamiento de cifrado de ransomware utilizando una herramienta de emulación de ransomware personalizada y no destructiva para imitar el cifrado masivo de archivos
- Realiza técnicas utilizadas por perpetradores para desplegar ransomware


**Duración y resultados**

La Evaluación de la defensa contra ransomware suele durar una semana. Se puede entregar en el sitio o de forma remota.

Después de la contratación, Mandiant proporciona un informe que incluye:

- Resumen ejecutivo con fortalezas y áreas de mejora
- Información técnica sobre el proceso de prueba
- Hallazgos detallados, clasificados por intensidad
- Informe ejecutivo

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



**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 un Estado 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.

FIREEYE™