FIREEYE™

FICHA TÉCNICA

Evaluación de seguridad remota

Evaluar y mejorar la seguridad del acceso y las operaciones remotas

VENTAJAS:

- Comprenda la exposición de su organización relacionada con el trabajo remoto
- Reduzca la probabilidad y el impacto de los incidentes debido al compromiso de los activos relacionados con el trabajo remoto
- Reciba recomendaciones correctivas y tácticas para ayudar a maximizar la seguridad de la infraestructura remota existente
- Genere evaluaciones con bajo impacto organizacional

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 tácticas, técnicas y procedimientos que cambian rápidamente.

Descripción general

A medida que las organizaciones adoptan y expanden cada vez más los modelos de trabajo remoto, necesitan administrar al personal que trabaja desde casa utilizando una variedad de plataformas de colaboración y computación del usuario final. Si bien las organizaciones se adaptan al modelo de trabajo remoto, los atacantes cibernéticos no se detienen. En todo caso, buscan explotar las organizaciones durante estos tiempos de cambio e incertidumbre. Cualquier aumento repentino en el trabajo remoto tiene el potencial de cambiar la superficie del ataque y la vulnerabilidad de las redes empresariales.

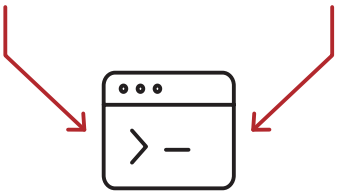
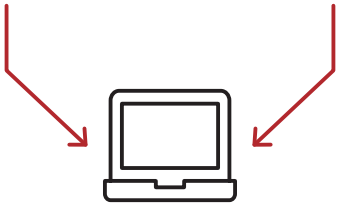
Las Evaluaciones de la seguridad remota de Mandiant están diseñadas para ayudar a su organización a comprender la naturaleza y los cambios en la exposición a la superficie de ataque debido al trabajo remoto. Estas evaluaciones se adaptan a su organización para minimizar el riesgo de afectar la disponibilidad del sistema durante las pruebas y se entregan de forma remota con una participación limitada de su equipo de seguridad. Después de una Evaluación de seguridad remota, Mandiant ofrece recomendaciones para reducir el riesgo al minimizar la probabilidad, el impacto y el costo total de un incidente de seguridad causado por una infraestructura de acceso remoto, estaciones de trabajo remotas y tecnología de colaboración comprometida.

Existen dos variaciones de este servicio disponibles:

Cada una de estas evaluaciones de seguridad remota se puede entregar de forma remota en aproximadamente una semana.

Cada evaluación incluye un informe detallado con:

- Resumen ejecutivo
- Observaciones técnicas
- Recomendaciones viables para mejoras

	Evaluación de la seguridad de acceso remoto	**Evaluación de la seguridad del endpoint remoto**
Descripción	Brinda a su organización una vista de su infraestructura de acceso remoto, herramientas de colaboración, controles de seguridad y políticas. Las organizaciones pueden usar esta evaluación para validar la postura de seguridad de sus soluciones de acceso remoto y plataformas de colaboración y garantizar que se sigan las mejores prácticas de seguridad al asegurar el acceso y los datos en estas plataformas.	Examina la postura de seguridad de las configuraciones y tecnologías de seguridad de correo electrónico y estaciones de trabajo remotas de su organización. La Evaluación de la seguridad del endpoint remoto también demuestra la posible ejecución de código malicioso que puede establecer la entrada inicial en estaciones de trabajo remotas.
Fase 1	**Fase estratégica:** La revisión de la documentación y los talleres se realiza para recopilar información sobre infraestructura, políticas y prácticas, que se comparan con las mejores prácticas recomendadas por los expertos de Mandiant.	**Ejercicio de phishing:** Se lanzan campañas simuladas de phishing por correo electrónico contra el personal dentro del alcance para evaluar la seguridad del correo electrónico y el conocimiento de seguridad de los empleados.
Fase 2	**Pruebas técnicas:** Se simulan ataques individualizados contra la infraestructura de acceso remoto utilizando las últimas técnicas de ataque para validar los hallazgos de la fase estratégica.	**Evaluación del host:** Se simulan ataques individualizados contra endpoints remotos utilizando las últimas técnicas de ataque.
Diagrama	**Infraestructura de acceso remoto** **Política y prácticas de la infraestructura**  **Evaluación de la seguridad de acceso remoto**	**Ejercicio de phishing** **Evaluación del host**  **Evaluación de la seguridad del endpoint remoto**

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.