

# DESCUBRA LAS VULNERABILIDADES DEL SISTEMA CON PRUEBAS DE PENETRACIÓN

## PREVENGA LA PÉRDIDA DE DATOS, RIESGOS Y VIOLACIONES

Las pruebas de penetración, mejor conocidas como “pen testing”, o el hackeo ético, son unas de las mejores formas para valorar la efectividad real de sus controles técnicos, políticas y procedimientos. En muchos casos, también es un requisito obligatorio para cumplir con regulaciones de cumplimiento o estándares de la industria, tales como la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA, por sus siglas en inglés), los Estándares de Seguridad para la Industria de Tarjetas Bancarias (PCI DSS, por sus siglas en inglés), la Ley de Gramm-Leach-Bliley (GLBA) y otras.

## ENCUENTRE VULNERABILIDADES DE SEGURIDAD ANTES DE QUE LO HAGAN LOS ATACANTES

No todas las pruebas de penetración se crean de la misma forma. Muchas firmas que aseveran ofrecer “pen testing” dependen de una sola herramienta automatizada con poca experiencia en pruebas de penetración más allá de lo que la herramienta pueda hacer por ellos (y, aún más importante: lo que no puede hacer).

Motorola Solutions emplea un acercamiento multifacético; uno que integra la investigación junto con el análisis técnico profundo y las pruebas “manuales”. Nuestro acercamiento apunta hacia la información disponible o filtrada al público, los controles ausentes, las malas configuraciones y vulnerabilidades del sistema justo como lo haría un hacker malintencionado.

## LA ASISTENCIA DE LOS EXPERTOS REVELA LOS RIESGOS DE SEGURIDAD

Quando se lleva a cabo una prueba de penetración, nuestros expertos en seguridad informática simulan los procesos de pensamiento y las acciones de un actor malintencionado externo o interno para obtener acceso no autorizado a los sistemas o para extraer información sensible.

Al utilizar una metodología flexible, la cual incluye procedimientos de pruebas de penetración interna, externa, física y de otros tipos, empleamos cada recurso que tenemos disponible para revelar los problemas que podrían dejar vulnerable a su organización antes de que algún hacker malintencionado las aproveche.



# \$3.9M

DE COSTO PROMEDIO GLOBAL EN VIOLACIÓN DE DATOS EN 2019<sup>1</sup>



## OPCIONES DE PRUEBAS DE PENETRACIÓN



### VALORACIÓN INTERNA

Replica a una amenaza interna o a un usuario puesto en riesgo



### VALORACIÓN EXTERNA

Replica las amenazas externas para encontrar vulnerabilidades



### VALORACIÓN INALÁMBRICA

Encuentra dispositivos no autorizados y sin seguridad

#### CARACTERÍSTICAS CLAVE

Para mantener el paso con las amenazas cibernéticas en constante crecimiento, Motorola Solutions le ofrece una suite de valoraciones de pruebas de penetración. Una vez que se completan, nuestros reportes son meticulosos y le proporcionan un entendimiento de la metodología de pruebas, el alcance de trabajo que se llevó a cabo; documentación amplia sobre los hallazgos y consejos de remediación priorizados.

#### IDENTIFICAR RIESGOS PARA SU INFRAESTRUCTURA INTERNA DE TI

Mientras que la mayoría de las organizaciones piensan inicialmente en defender sus datos y sistemas sensibles de los ataques externos, muchos de los ataques exitosos contra ellas provienen dentro de los confines de la red, convirtiendo a las pruebas de penetración interna en las más críticas para encontrar vulnerabilidades de redes, sistemas, servidores y aplicaciones.

#### PROTECCIÓN DE DATOS DE DIRECCIONES Y REQUISITOS DE CUMPLIMIENTO

Las pruebas de penetración externa valoran los riesgos fuera de su infraestructura, incluyendo a los cortafuegos, servidores web, sistemas de correo electrónico, ruteadores externos y acceso remoto. Estos se designan para replicar las herramientas y técnicas que los hackers malintencionados utilizarían para poner en riesgo a su organización.

#### ENCUENTRE REDES Y DISPOSITIVOS INALÁMBRICOS DESPROTEGIDOS O SIN AUTORIZACIÓN

Determinamos el nivel de seguridad del ambiente inalámbrico de su organización haciendo que nuestros examinadores de penetración hagan un barrido de detección de dispositivos malintencionados e intenten poner en riesgo su estructura inalámbrica. Este acercamiento proporciona resultados cuantificables y puede identificar vulnerabilidades en cualquiera de estas áreas.

#### DESCUBRA LAS AMENAZAS POTENCIALES A SU AMBIENTE FÍSICO

Nuestro acercamiento multifacético para probar la postura de seguridad de su organización también puede incluir pruebas de seguridad física y de ingeniería social para crear una simulación de amenazas completas y realmente "enmascaradas" que podrían poner a su oficina o empleados en una situación de violación o riesgo.

## MOTOROLA SOLUTIONS - SU SOCIO DE CONFIANZA

Como proveedor líder en soluciones esenciales, entendemos que su misión solo puede tener tanta seguridad como la que le proporcionen sus socios. Nuestra meta es proporcionarle la transparencia, responsabilidad y seguridad que se integra desde el inicio. Tenemos la confianza de que nuestro conjunto de personas altamente capacitadas con certificaciones de la industria, las mejores políticas y procedimientos organizacionales de su clase y las herramientas de vanguardia en automatización y análisis, nos permiten entregar soluciones más completas y únicas en ciberseguridad, que satisfagan sus necesidades hoy y mañana.

### EXPERIENCIA Y ESCALA GLOBALES

# 300+

EXPERTOS EN SEGURIDAD ENFOCADOS EN LA RESPUESTA Y MONITOREO 24/7

# 9B

EVENTOS DE SEGURIDAD QUE SE MONITOREAN DE FORMA PROACTIVA CADA DÍA

# 100%

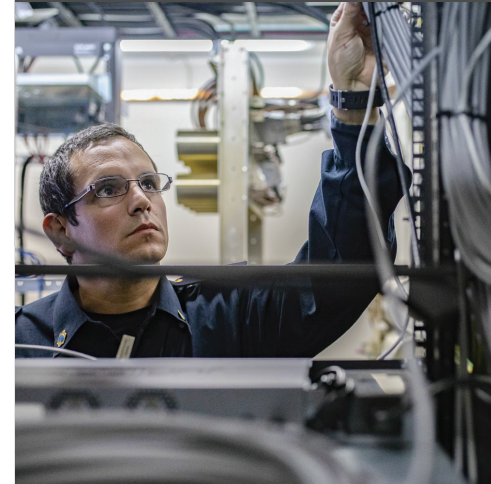
DE ACERCAMIENTO CO-ADMINISTRADO PARA OTORGAR VISIBILIDAD Y CONTROL

# 20+

AÑOS DE EXPERIENCIA DESARROLLANDO SOLUCIONES EN CIBERSEGURIDAD

### IDENTIFIQUE Y REMEDIE LAS VULNERABILIDADES

Nuestro acercamiento altamente personalizable permite que tenga una valoración exacta y meticulosa de las redes y recursos para proporcionar una medida verdadera de su postura de seguridad.



Identifique y remedie las vulnerabilidades antes de que los atacantes las puedan aprovechar.

Para obtener más información sobre nuestros Servicios Avanzados de Detección y Respuesta a amenazas, visítenos en [www.motorolasolutions.com/cybersecurity](http://www.motorolasolutions.com/cybersecurity)



Recursos  
1 Reporte de Violación de Datos de IBM en 2019

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. [motorolasolutions.com](http://motorolasolutions.com)

MOTOROLA, MOTO, MOTOROLA SOLUTIONS y el logotipo de la M estilizada son marcas comerciales o marcas comerciales registradas de Motorola Trademark Holdings, LLC y son utilizadas bajo licencia. Todas las demás marcas comerciales pertenecen a sus respectivos propietarios. ©2021 Motorola Solutions, Inc. Todos los derechos reservados. 03-2021