MANDIANT®

Validación de la Seguridad

Comprobar el valor de la ciberseguridad

Los CISO deben comprobar la eficacia de la seguridad
El entorno empresarial consciente de los riesgos de hoy en día está ejerciendo una presión sin precedentes sobre los directores de seguridad de la información (Chief Information Security Officer, CISO) y sus equipos para que protejan los activos corporativos, la postura financiera y el valor de la marca de las organizaciones. Los mismos deben comprobar a los líderes el valor de las inversiones en ciberseguridad y la eficacia al momento de evitar que los adversarios vulneren los sistemas críticos.

Sin embargo, al carecer de las herramientas que se necesitan para validar la eficacia de la seguridad, cuantificar los riesgos y demostrar competencia operativa, los mismos dependen de escáneres de vulnerabilidades, pruebas de penetración, equipos de emergencia o simulaciones de brechas y ataques. Debido a las limitaciones inherentes, estos enfoques no evalúan en grado suficiente la eficacia ni proporcionan a la organización información pertinente y oportuna con respecto a las amenazas específicas y de alta prioridad.

La solución es Mandiant Security Validation, una cartera basada en información que es automática y continua, que está conformada por módulos de rendimiento únicos y la plataforma de instrumentación de seguridad de Mandiant.[1]

Compruebe la eficacia de su programa de ciberseguridad y cuantifíquela
La validación de la seguridad que se realiza de manera correcta se basa en una metodología de cinco pasos que brinda información con respecto a lo que es más

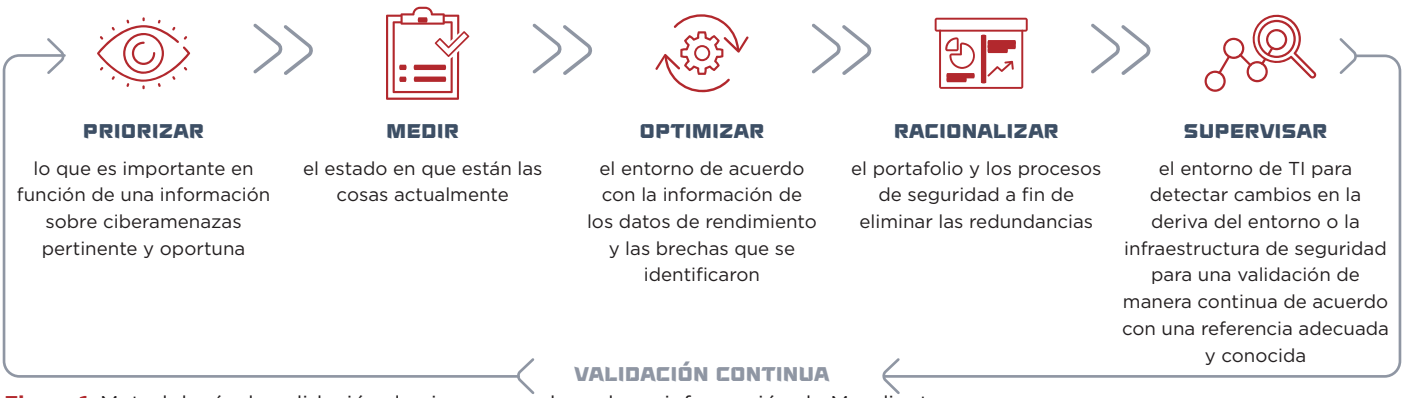

Figura 1. Metodología de validación de cinco pasos basada en información de Mandiant.

1 Conocida anteriormente como la plataforma de instrumentación de seguridad de Verodin.

importante a fin de realizar pruebas de defensa y cómo optimizarlas de acuerdo con el conocimiento de quién o qué podría estar atacando a una organización o sector.

Esta metodología requiere de la capacidad de aprovechar los datos sobre amenazas en tiempo real. Mandiant Security Validation utiliza los datos de respuesta ante incidentes y Mandiant Threat Intelligence para lograr una visibilidad de adversarios sin precedentes que revela lo que los atacantes están haciendo actualmente. Gracias a que Security Validation es basada en información, los equipos de seguridad pueden identificar las amenazas de alta prioridad para sus organizaciones y crear una estrategia de validación en función del conocimiento de quién o qué representa una amenaza para la organización. Con Mandiant, los líderes de seguridad y sus equipos pueden llevar a cabo una validación completa y continua de los controles de seguridad a nivel de todas las tecnologías, los procesos y las personas.

Mandiant Security Validation utiliza la plataforma de instrumentación de seguridad, su tecnología de validación de controles, con el objetivo de ayudar a que los equipos de seguridad ejecuten comportamientos de ataques reales contra los controles de seguridad a fin de cuantificar y comprobar rápidamente la eficacia del programa de seguridad y su capacidad de defenderse contra los ataques de adversarios más sofisticados.

Funcionalidades básicas de la plataforma de instrumentación de seguridad de Mandiant:

- Priorizar las amenazas y los controles de adversarios más importantes
- Medir la eficacia de los controles de seguridad con respecto a los ataques de adversarios reales
- Ejecutar de manera segura los ataques relevantes que se reportan mediante los datos de respuesta ante incidentes y Mandiant Threat Intelligence
- Descubrir las brechas no detectadas en la infraestructura de seguridad de la organización
- Identificar las oportunidades de optimización más importantes
- Cuantificar las mejoras de defensas con el tiempo
- Racionalizar con evidencia cuantificable el valor de las inversiones para los ejecutivos

La plataforma de implementación de seguridad de Mandiant presenta funcionalidades avanzadas:

- **Módulo de seguridad contra agresores (TAAM):** hace que la información sobre amenazas sea viable de forma tal que es posible probar el rendimiento de los controles con respecto a perpetradores reales, en especial, aquellos que con mayor probabilidad atacarán a una organización. El TAAM se integra con envíos de información de terceros líderes en la industria.
- **Análisis de cambio/deriva del entorno automático:** adaptación de la supervisión continua de la infraestructura de TI cuyo objetivo es eliminar la deriva del entorno e impulsar la validación continua con respecto a las regresiones de defensa para garantizar el estado de la infraestructura de seguridad de una organización.
- **Teatro protegido:** valida la eficacia de los controles de endpoint mediante la ejecución segura de malware, ransomware y otros ataques destructivos para permitir una protección proactiva contra las amenazas emergentes y más recientes.
- **Teatro de correo electrónico:** prueba los controles que ofrecen las plataformas de seguridad del correo electrónico.

El portafolio de Mandiant Security Validation incluye varias opciones de implementación:

Figura 2.

La plataforma ayuda a visualizar y generar pruebas de que los controles protegen a los activos críticos.

- **Propiedad del cliente:** Basado en la nube (seguridad como servicio (SaaS)) o implementado como un dispositivo virtual en las instalaciones.
- **Modelos de gestión total y gestión conjunta:** En función de los resultados empresariales que el cliente desea, los equipos de Mandiant desarrollan programas de validación que se ajustan a casos de uso particulares y brindan, de forma continua, informes detallados a las partes interesadas del cliente.
- **Validación a pedido:** Permite que los clientes adquieran un caso de uso individual para una evaluación única de la capacidad de bloquear o evitar un ataque predefinido o la acción de un agresor y obtener recomendaciones sobre investigaciones adicionales que se necesiten con el objetivo de mejorar la defensa y disminuir la exposición al riesgo.

Ventajas comerciales de la Validación de la Seguridad

Medir la eficacia y el retorno de la inversión (Return on Investment, ROI)

Obtener datos cuantificables que ayuden a determinar la inversión que se requiere para aumentar la eficacia de la seguridad con respecto a los tipos de ataques priorizados y cuantificar el perfil de riesgo general. Los equipos de seguridad también pueden utilizar esta evidencia para racionalizar el valor de las inversiones de seguridad ante el liderazgo ejecutivo y la junta directiva.

Fusiones y Adquisiciones

Comprenda con claridad cómo las empresas que atraviesan una fusión o adquisición pueden tener superposiciones o brechas en los controles. A través de la finalización de los gastos, puede calcular la posible cantidad en dólares de la consolidación y el nivel de riesgo que se podría estar asumiendo como resultado de la fusión.

Contratación y capacitación del talento en seguridad

Revise años anteriores de experiencia y evalúe el potencial de un profesional de seguridad con respecto al aprendizaje, el tipo de experiencia que tiene y que también su conjunto de habilidades coincida con el entorno de la organización en escenarios reales. Al ejecutar de forma segura ataques reales en entornos de producción, los líderes de TI pueden supervisar la forma en que responden y reaccionan los posibles solicitantes. Los líderes de TI también pueden llevar a cabo evaluaciones regulares en forma de ejercicios de capacitación, a fin de ver si los equipos demuestran tiempos de respuesta y habilidades requeridas aceptables en escenarios de ataques reales.

Protección de la Marca

Mide de manera proactiva y continua la eficacia de la seguridad para disminuir el riesgo de experimentar una vulneración o ataque y preservar la reputación de la marca y la lealtad de sus clientes.

Privacidad y Protección de los Datos

Proteja los datos de los clientes y garantice el cumplimiento de los mandatos reglamentarios, corporativos y de terceros.

Informes de validación de la seguridad de Mandiant Threat Intelligence

En los últimos 15 años, a través de investigaciones, consultoría sobre incidentes y ejercicios de simulación de ataque en todo el mundo, Mandiant creó y seleccionó un portafolio exclusivo de información sobre amenazas que se actualiza de manera constante mediante nuevas técnicas profesionales de datos de evidencias, experiencia humana y análisis exclusivo. Actualmente Mandiant domina el campo de la información sobre ciberamenazas mediante el siguiente conjunto equilibrado de fuentes:

- **Información sobre vulneraciones** que se recopila a través de las investigaciones sobre respuesta ante incidentes de los servicios de consultoría de Mandiant
- **Información sobre adversarios** que se obtiene a través de los investigadores de Mandiant
- **Inteligencia artificial** de los productos de seguridad de FireEye
- **Información operativa** que se obtiene de los servicios de Mandiant Managed Defense

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

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