MANDIANT®

FICHA TÉCNICA

Plataforma de Instrumentación de Seguridad

Conozca la verdadera medida de su seguridad

ASPECTOS DESTACADOS

- **Priorice las amenazas importantes** en función de una información pertinente y oportuna sobre ciberamenazas
- **Evalúe la eficacia de las herramientas de seguridad actuales** con respecto a ataques de adversarios reales
- **Descubra en su infraestructura de seguridad las brechas** que no se detectan y se superponen
- **Mida el tiempo que tarda su equipo** en detectar y responder
- **Identifique las oportunidades** de optimización más importantes
- **Cuantifique las mejoras** de las defensas con el tiempo
- **Racionalice con evidencia el valor** de las inversiones para los ejecutivos
- **Simplifique las comunicaciones** sobre el estado del nivel de seguridad en toda la empresa

El entorno de amenazas cada vez es más dinámico y los directores de seguridad de la información y sus equipos se enfrentan al desafío de mantener protegidos los activos corporativos. Se espera que ellos conozcan y brinden evidencia del valor de las inversiones en ciberseguridad y de la eficacia de las defensas cibernéticas contra los ataques de adversarios actuales y emergentes.

Las pruebas de penetración, la formación de equipos de emergencia y las simulaciones de vulneraciones y ataques no son suficientes: estos elementos no brindan la prueba cuantificable que los directores de seguridad de la información y los líderes empresariales exigen para comprender la exposición al riesgo y su preparación cibernética. Sin evidencia basada en datos de rendimiento, los equipos de seguridad tienen dificultades para optimizar las defensas de manera satisfactoria y generar informes sobre su nivel de seguridad de forma confiable.

La Plataforma de Instrumentación de Seguridad de Mandiant, un elemento crítico de la tecnología de validación de los controles basados en información de Mandiant, le brinda la evidencia que necesita. La Plataforma de Instrumentación de Seguridad es una plataforma de evaluación y gestión de riesgos de ciberseguridad que permite a los equipos garantizar que los activos críticos estén protegidos en todo momento.

Mayor eficacia de los controles

La Plataforma de Instrumentación de Seguridad de Mandiant cuenta con la tecnología de datos de información sobre amenazas y respuesta ante incidentes globales de Mandiant, que es una visibilidad única y sin precedentes de los datos sobre amenazas y adversarios que representan lo que los atacantes están haciendo en la actualidad. Esta combinación de tecnología de validación de la seguridad y Mandiant Threat Intelligence proporciona a los equipos de seguridad una estrategia de validación que se basa en el hecho de conocer quién y qué probablemente está atacando a la organización.

La tecnología de validación de la seguridad basada en información de Mandiant empieza al priorizar las amenazas críticas y pertinentes, y después evalúa de forma segura y captura evidencia discreta y cuantificada de la eficacia de la arquitectura de seguridad general con respecto a ataques de adversarios reales. Los resultados destacan los ataques individuales específicos e incluso áreas completas en la cadena letal extendida que neutralizan o evaden las tecnologías de seguridad. Puede utilizar esta información para determinar dónde y cómo optimizar sus controles, trabajar con datos de rendimiento y proveedores específicos, según sea necesario, y en última instancia transformar su programa completo.

Con la Plataforma de Instrumentación de Seguridad de Mandiant, tiene la posibilidad de cuantificar y comprobar rápidamente la eficacia de su programa de seguridad contra los adversarios sofisticados más recientes de todo el mundo. Esta tecnología puede utilizarse en arquitecturas en las instalaciones, de nube e híbridas.

Cuantificar las mejoras de la eficacia permite probar al liderazgo empresarial el valor de las inversiones en seguridad con respecto a la tolerancia a los riesgos de la empresa.

Con la Plataforma de Instrumentación de Seguridad de Mandiant, el proceso se realiza de forma automática y continua, lo que le permite enfocarse en defender su negocio de una forma más estratégica al tiempo que la plataforma supervisa de manera constante y mide la eficacia general de la seguridad.

Gane confianza en su nivel de seguridad

Los expertos de Mandiant Security Validation trabajan con usted para configurar rápidamente la plataforma, vincular perpetradores, una fuente de alertas y cualquier control específico para obtener profundidad adicional. Gracias a la facilidad de integración, puede visualizar el rendimiento de su componente defensivo cuando los comportamientos de ataque se ejecutan de manera segura.

Una vez configuradas, puede seleccionar tareas discretas o secuencias preconfiguradas de pruebas a partir de la vasta biblioteca de Mandiant de ataques reales, de técnicas, tácticas y procedimientos de adversarios, y diversos tipos de malware. A medida que estas pruebas se ejecutan de manera segura, puede validar de forma inmediata y continua que controles específicos funcionen apropiadamente. Los paneles se rellenan en tiempo real para mostrarle las tasas de detección, alertas, omisiones y prevención a medida que se ejecutan las pruebas.

La plataforma también valida que los eventos presenten registros de fecha y hora de manera apropiada y que se analicen de forma correcta, y en caso de que se hayan definido reglas de correlación y modelos de amenazas, los eventos generan las alertas adecuadas. Se pueden visualizar y exportar informes que describen la eficacia general de la seguridad en el tiempo. Gracias a la validación continua y permanente, puede obtener las pruebas que necesita para lograr y mantener la confianza en el programa, no solo para usted mismo, sino también para los ejecutivos y la junta directiva.

Detalles de la Plataforma

La plataforma abierta, personalizable y extensible de Mandiant ofrece descubrimiento de controles automático y una arquitectura que permite utilizar binarios de ataques reales a fin de probar de manera segura los controles de seguridad. Incluye seis componentes principales.

Director

Este controlador y administrador central de validación continua de todo su entorno de producción dinámico está disponible como una plataforma basada en la nube (seguridad como servicio) o en las instalaciones como un dispositivo virtual o software instalable.

Perpetradores

Los mismos realizan pruebas de forma segura en entornos de producción con el fin de validar la eficacia de los controles del endpoint, correo electrónico y seguridad de la nube de la red, Windows, Mac OS y Linux, y garantizar que la infraestructura esté configurada de manera correcta.

Integraciones

Las integraciones enriquecidas y listas para usar con tecnologías de defensa e infraestructura de seguridad pueden alcanzar una validación más profunda de los controles.

Biblioteca de Ataques

La biblioteca de contenidos representa miles de ataques en todas las etapas del ciclo de vida del adversario, incluida la cadena letal extendida, y se basa en los comportamientos de ataques de adversarios y TTP actuales y emergentes que se reportan mediante la información sobre amenazas, adversarios y vulneraciones globales de Mandiant.

Marcos

Los ataques se alinean con los marcos MITRE™ ATT&CK y NIST a fin de vincular con mayor facilidad la eficacia a los programas de evaluación de seguridad. Mandiant Security Validation es única debido a que su contenido proporciona información sobre las tácticas del marco de ataque que son pertinentes con respecto a una organización y se puede utilizar para ejecutar validaciones de tácticas
MITRE ATT&CK de modo de garantizar que se realicen pruebas integrales y pertinentes y se obtengan resultados precisos.

Paneles e Informes

Pantalla gráfica en vivo con los resultados de las pruebas que se ejecutaron en su entorno e informes sobre las mejoras en la eficacia con el tiempo que contienen datos reales y cuantitativos que se pueden utilizar para informar a los ejecutivos (Fig. 1).

Figura 1. Los paneles ayudan a validar los controles de seguridad en todo el ciclo de vida del ataque a fin de identificar las áreas de riesgo.

Metodología de validación basada en información

La Plataforma de Instrumentación de Seguridad de Mandiant realiza supervisión, validación y optimización completas de los controles de seguridad mediante una detección de la deriva del entorno automática. Este proceso de validación continuo se lleva a cabo a través de una metodología de cinco pasos basada en información (Fig. 2)

Figura 2. Metodología de validación de cinco pasos basada en información de Mandiant.

Capacidades 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 (Fig. 3).
- **Análisis de cambio/deriva del entorno automático (AEDA):** 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 a fin de garantizar el estado de la infraestructura de seguridad de una organización.
- **Teatro Protegido:** valida la eficacia de los controles del endpoint mediante la ejecución segura de malware, ransomware y otros ataques destructivos de modo de 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.

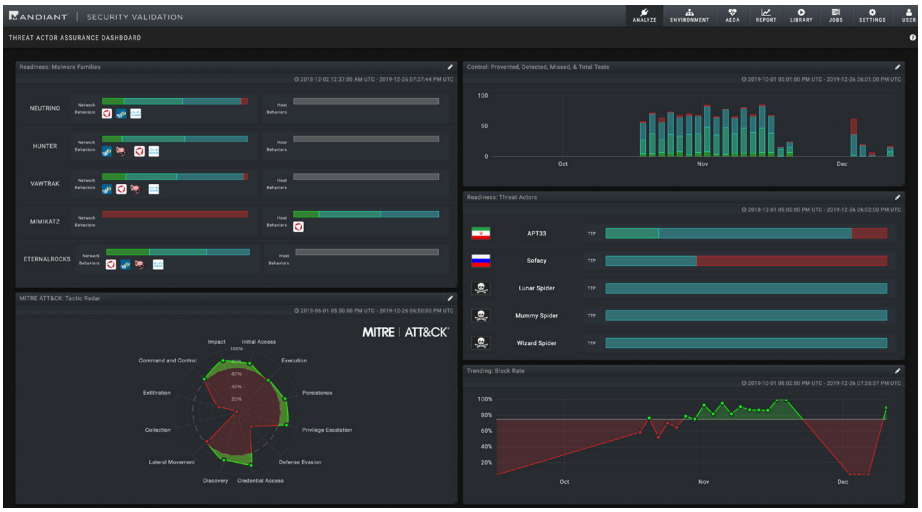

Figura 3. Módulo de Seguridad Contra Agresores (TAAM).

La cartera de Mandiant Security Validation incluye varias opciones de implementación:

- **Modelo perteneciente al y gestionado por el cliente:** Basado en la nube (como 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/evitar un ataque predefinido o la acción de un agresor y obtener recomendaciones sobre investigaciones adicionales que se necesiten con el objetivo de mejorar las defensas y disminuir la exposición al riesgo.

Informes de Validación de la Seguridad por Mandiant Threat Intelligence

Durante 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 una cartera exclusiva 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®