MANDIANT®

FICHA TÉCNICA

Seguridad ofensiva para la tecnología de operaciones

Mitigar y detectar ataques en las operaciones industriales de misión critica

VENTAJAS

- Evalúe la efectividad de sus controles de seguridad de OT existentes contra ataques cibernéticos del mundo real
- Identifique y mitigue problemas de seguridad en entornos de OT complejos antes de que un atacante los explote
- Prepare a su equipo de seguridad para monitorear, detectar y responder ante incidentes cibernéticos específicos de OT, sin correr el riesgo de impactos peligrosos
- Utilice el entendimiento basado en el comportamiento global de los atacantes para proteger sus entornos críticos de OT e ICS
- Obtenga asesoramiento basado en hechos y orientación integral que le permita prevenir y detectar amenazas del mundo real para su infraestructura crítica

Los actores de amenazas cibernéticas continúan evolucionando sus ataques para eludir las protecciones de la tecnología de operaciones (OT) y los sistemas de control industrial (ICS). Para proteger la infraestructura crítica es necesario realizar rigurosas pruebas de seguridad desde la perspectiva de los atacantes avanzados que apuntan a esos entornos.

La Seguridad Ofensiva de Mandiant para la OT combina nuestra experiencia de primera línea en ciberseguridad junto con un profundo conocimiento funcional de los sistemas de control adquirido a lo largo de décadas de trabajo práctico en entornos de ICS y OT. Nuestros expertos en OT de Mandiant poseen la mejor inteligencia de amenazas y un conocimiento inigualable de los comportamientos de los atacantes, realizando pruebas de seguridad avanzadas para apoyarlo en mitigar, detectar y contener de manera efectiva las amenazas en las redes industriales de un extremo a otro.

Descripción general del servicio

La Seguridad ofensiva de Mandiant para OT está diseñada para apoyar a nuestros clientes a identificar tanto acciones tácticas como pasos estratégicos para mitigar los riesgos de seguridad y mejorar las defensas de seguridad transversalmente en las diferentes capas de un entorno de OT o ICS.

Cada proyecto se adapta a los requisitos de evaluación únicos de cada cliente y garantiza cero impacto operativo en los segmentos de red donde se requiere de alta disponibilidad. Los consultores de Mandiant evalúan los activos de OT críticos en busca de problemas de seguridad de alto riesgo, evalúan la efectividad de los controles de seguridad existentes y brindan orientación para mejorar la postura de seguridad general del entorno industrial.

Tabla 1. Ofertas disponibles a través de la Seguridad ofensiva de Mandiant para la OT.

Oferta del servicio	Descripción
Escenario de Ataque Simulado para OT (equipo de simulación de ataque)	Simule un escenario específico de ataque a la OT relevante para su sector u organización (generalmente originado desde Internet), sin el riesgo de daño o impacto asociado con un incidente real. Los consultores de Mandiant imitan las actividades de los atacantes y las TTP observados en el mundo real para determinar el riesgo de seguridad para la OT, identificar brechas en los controles preventivos y defensivos y evaluar la capacidad de su equipo de seguridad para responder ante un ataque dirigido a su entorno de OT.
Prueba de penetración al segmento de red OT	Realice una prueba de penetración dirigida para determinar el riesgo de propagación de un ataque desde una red periférica de baja confianza (como una red de oficina, corporativa o de campo) a su red central de OT/ICS. Esta evaluación se realiza desde la perspectiva de un atacante que tiene presencia en la red periférica, con el fin de descubrir brechas en los controles de segmentación de la red e identificar rutas de ataque remotas que pueden permitir al atacante romper el perímetro protegido de su red OT.
Prueba manual de la red OT de producción	Use técnicas de recopilación de información pasiva y pruebas manuales no intrusivas para identificar vulnerabilidades de seguridad comunes en su red de producción de OT. Los expertos en ICS de Mandiant trabajan en estrecha colaboración con su equipo de control de procesos para identificar problemas de seguridad comunes y posibles rutas de ataque en una red de producción de OT, sin introducir el riesgo de utilizar herramientas de análisis de red activas o pruebas de penetración intrusivas.
Pruebas de seguridad de dispositivos integrados/ componentes de OT	Haga pruebas de seguridad integrales para un componente de OT específico en un entorno que no es de producción (como un área de desarrollo o un entorno de laboratorio) para encontrar debilidades complejas de seguridad, validar la existencia de una vulnerabilidad mediante la explotación activa y determinar el nivel de riesgo que presenta para su infraestructura de OT. Los ejemplos de componentes de OT incluyen dispositivos integrados, sistema operativo, aplicación de software, interfaz de radio o protocolo de comunicación.
Evaluación de Monitoreo de la seguridad de OT (Purple Team)	Evaluación colaborativa en la que los expertos de Mandiant trabajan con su equipo de seguridad para simular escenarios de ataques controlados y evaluar las capacidades de detección de brechas en cada fase del ciclo de vida de un ataque dirigido a la OT. Esta evaluación utiliza Mandiant Security Validation para emular las TTP de los perpetradores que representan el mayor riesgo para los entornos de OT y brinda evidencia cuantificable sobre la efectividad de las capacidades de respuesta y detección de vulneraciones en diferentes capas del entorno de OT.

POR QUÉ ELEGIR MANDIANT SOLUTIONS PARA OT

- Especialistas en seguridad con más de 100 años de experiencia combinada en entornos de OT e ICS
- Enfoque realista orientado a objetivos y centrado en activos críticos para su negocio y operaciones
- Un Red Team con varias capacidades que cubre especializaciones para diversos procesos y tecnologías en redes de TI y OT
- TTP simulados y del mundo real extraídos de los grupos de atacantes que Mandiant investiga directamente
- Contexto derivado de la experiencia de primera línea en diferentes industrias e información sobre amenazas específicas para la OT

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

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 del lider en inteligencia de amenazas y el conocimiento experto obtenido en la primera línea a la validación continua de la seguridad a fin de equipar a las organizaciones con las herramientas necesarias para aumentar la eficacia de la seguridad y reducir el riesgo comercial.

MANDIANT®