MANDIANT®

FICHA TÉCNICA

Segurança Ofensiva para Tecnologia Operacional

Mitigar e detectar ataques a operações industriais de missão crítica

VANTAGENS

- Avalie a eficácia de seus controles de segurança OT existentes contra ataques cibernéticos do mundo real
- Identifique e mitigue problemas de segurança em ambientes de OT complexos antes que um invasor os explore
- Prepare sua equipe de segurança para monitorar, detectar e responder a incidentes cibernéticos específicos de OT, sem o risco de impactos perigosos
- Use insights com base no comportamento global do atacante para proteger seus ambientes críticos de OT e ICS
- Obtenha conselhos baseados em fatos e orientações abrangentes que capacitam você a prevenir e detectar ameaças do mundo real à sua infraestrutura crítica

Os atores de ameaças cibernéticas continuam a desenvolver seus ataques para contornar as proteções de tecnologia operacional (OT) e sistemas de controle industrial (ICS). A proteção da infraestrutura crítica requer testes de segurança rigorosos conduzidos da perspectiva de invasores avançados que visam esses ambientes.

A Mandiant Offensive Security for OT combina a experiência da Mandiant em cibersegurança com um profundo conhecimento funcional de sistemas de controle adquiridos ao longo de décadas de trabalho prático em configurações de ICS e OT. Equipados com a inteligência de ameaças líder mundial da Mandiant e com o conhecimento inigualável dos comportamentos dos invasores, nossos especialistas em OT conduzem testes de segurança avançados e ajudam você a mitigar, detectar e conter ameaças em redes industriais ponta a ponta.

Visão Geral do Serviço

A Mandiant Offensive Security for OT foi projetado para ajudar nossos clientes a identificar ações táticas e etapas estratégicas para mitigar riscos de segurança e melhorar as defesas de segurança em diferentes camadas de um ambiente OT ou ICS.

Cada contrato é feito sob medida para os requisitos de avaliação exclusivos de cada cliente e garante impacto operacional zero para segmentos de rede de alta disponibilidade. Os consultores da Mandiant avaliam ativos OT críticos para problemas de segurança de alto risco, avaliam os controles de segurança existentes quanto à eficácia e fornecem orientação para melhorar a postura geral de segurança do ambiente industrial.

Tabela 1. Ofertas disponíveis por meio da Mandiant Offensive Security for OT.

Ofertas de Serviço	Descrição
Simulação de Ataque Baseado em Cenário de OT (Red Team)	Simulação de um cenário de ataque específico de OT relevante para seu setor ou organização (tipicamente com origem na internet), sem o risco do dano ou impacto associados a um incidente real. Os consultores da Mandiant imitam as atividades dos atacantes e as táticas, técnicas e procedimentos (TTPs) observados no mundo real para determinar o risco de segurança para OT, identificar falhas nos controles preventivo e defensivo e avaliar a capacidade da sua equipe de segurança em responder a um ataque direcionado para seu ambiente de OT.
Teste de Penetração de Segmento de Rede OT	Uso de um teste de penetração direcionado para determinar o risco de propagação de ataque de uma rede periférica de baixa confiança (como um escritório, rede corporativa ou de campo) para sua rede OT/ICS central. Esta avaliação é realizada a partir da perspectiva de um invasor que tem um ponto de apoio na rede periférica, a fim de descobrir lacunas nos controles de segmentação da rede e identificar caminhos de ataque remoto que podem permitir que o invasor violar o perímetro protegido de sua rede OT.
Teste Manual da Rede de Produção OT	Uso de técnicas de coleta de informações passivas e testes manuais não intrusivos para identificar vulnerabilidades de segurança comuns em sua rede OT de produção. Os especialistas em ICS da Mandiant trabalham junto com sua equipe de controle de processo para identificar problemas comuns de segurança e caminhos de ataque em potencial em uma rede OT de produção, sem apresentar o risco de usar varredura de rede ativa ou ferramentas de teste de penetração intrusivas.
Teste de Segurança do Componente OT/Dispositivo Incorporado	Teste de segurança abrangente para um componente específico de OT em um ambiente de não produção (como uma área de desenvolvimento ou ambiente de laboratório) para encontrar fraquezas de segurança complexas, validar a existência de uma vulnerabilidade usando exploração ativa e determinar o nível de risco que ela apresenta para sua infraestrutura OT. Exemplos de componentes OT incluem dispositivo embutido, sistema operacional, aplicativo de software, interface de rádio ou protocolo de comunicação.
Avaliação de Monitoramento de Segurança OT (Purple Team)	Avaliação colaborativa na qual os especialistas da Mandiant trabalham com sua equipe de segurança para simular cenários de ataque controlado e avaliar os recursos de detecção de violação em cada fase do ciclo de vida de um ataque de OT direcionado. Esta avaliação usa o Mandiant Security Validation para emular TTPs do ator de ameaça que representam o maior risco para os ambientes de OT e fornece evidências quantificáveis sobre a eficácia da detecção de violação e recursos de resposta em diferentes camadas do ambiente de OT.

POR QUE ESCOLHER A MANDIANT SOLUTIONS PARA OT?

- Especialistas em segurança com mais de 100 anos de experiência combinada em ambientes OT e ICS
- Abordagem do mundo real orientada para metas, focada em ativos essenciais para seus negócios e operações
- Red Team multiqualificado cobrindo especializações para diversos processos e tecnologias em redes de TI e OT
- Imitações e TTPs do mundo real extraídas de grupos de atacantes que a Mandiant investiga em primeira mão
- Contexto derivado da experiência da linha de frente em diferentes setores e inteligência contra ameaças específicas de OT

Para saber mais sobre a Mandiant Solutions, visite **www.FireEye.com/mandiant**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035, EUA
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

Sobre a Mandiant Solutions
A Mandiant Solutions reúne a inteligência de ameaças líder mundial e expertise da linha de frente com validação de segurança contínua para equipar as organizações com as ferramentas necessárias para aumentar a eficácia da segurança e reduzir o risco de negócios.

MANDIANT®