MANDIANT®
ADVANTAGE

THREAT INTELLIGENCE SUITE

FICHA TÉCNICA

MANDIANT® ADVANTAGE

A plataforma Mandiant Advantage Threat Intelligence fornece às organizações de todos os tamanhos inteligência de ponta e relevante sobre ciberameaças para que você possa focar nas ameaças que mais importam para seus negócios no momento e tomar providências.

A tenacidade e a desenvoltura dos modernos atores de ameaças requerem atenção e maior conhecimento de todos os membros das equipes de segurança. Com base em uma combinação de inteligência interna de **violações, máquinas, adversários e operacional**, cultivada por mais de 300 especialistas em 23 países e cobrindo mais de 30 idiomas, a Mandiant oferece assinaturas baseadas em cinco casos de uso, fornecendo às organizações **Threat Intelligence atualizada de ponta** para que realizem suas tarefas de segurança mais rapidamente e com maior precisão.

MANDIANT® ADVANTAGE

Madiant Advantage Free

AMEAÇAS E VULNERABILIDADES DE CONHECIMENTO PÚBLICO E GERENCIADAS DE MANEIRA CENTRALIZADA

Destaques para Profissionais de Segurança sobrecarregados com gestão de Threat Intelligence

- **Consciência da situação sobre atores de ameaças de malware em alta**
- **Repositórios centralizados para descrições de vulnerabilidades de conhecimento público com pontuação de severidade CVSS**
- **Procure indicadores de ameaças de conhecimento público e incorpore a pontuação de ameaças exclusiva da Mandiant diretamente em qualquer página da Web com o plugin para navegadores**

Centralizar e gerenciar Threat Intelligence é frequentemente classificado como uma das tarefas que mais consome tempo dos analistas de segurança. O Mandiant Advantage Free oferece às organizações de todos os tamanhos acesso livre a atores, malware e vulnerabilidades de conhecimento público. Além disso, o Mandiant Advantage Free fornece visibilidade de indicadores de ameaças enriquecidos com a pontuação de maliciosidade exclusiva da Mandiant, além de descrições de vulnerabilidades de conhecimento público com as métricas de severidade do Sistema de Pontuação de Vulnerabilidades Comuns (*Common Vulnerability Scoring System*, CVSS). Isso tudo serve para permitir que os profissionais de segurança possam tomar decisões mais bem informadas sem despesas capitais ou operacionais.

O QUE ESTÁ INCLUSO:

- **Painéis globais que fornecem tendências de atividade, vulnerabilidades, malware e atores**
- **Acesso a indicadores de código aberto com a pontuação de maliciosidade da Mandiant**
- **Visualizações e pontuação de vulnerabilidades com base em OSINT**
- **Análises de notícias com comentários e avaliações de especialistas da Mandiant**
- **Threat Intelligence acessível por meio do portal e do plugin para navegadores**

MANDIANT® ADVANTAGE

Mandiant Advantage Security Operations

AUMENTE A EFICIÊNCIA E A EFETIVIDADE DE SOC

Benefícios para Analistas de Segurança, Responsáveis pela Resposta a Incidentes, Gerentes de Operações de Segurança e Analistas de Inteligência

- **Triagem e Priorização de Alertas:** use Threat Intelligence de ponta, atualizada, para priorizar e contextualizar informações de eventos de segurança, reduzindo a fadiga de alertas e melhorando a eficiência geral do SOC
- **Detecte Ameaças Ocultas:** faça o download de indicadores e expanda suas ferramentas de detecção para descobrir atores de ameaças ou atividades de malware que podem permanecer invisíveis no seu ambiente
- **Acelere a Resposta:** capacite as equipes de analistas de seguranças com insights de comportamento de atores com base no MITRE ATT&CK para entender o progresso do possível ataque e ajudar a formular a resposta correta

O pessoal do Centro de Operações de Segurança (*Security Operations Center*, SOC) está sob uma enxurrada de eventos de segurança que requerem atenção contínua e investigações manuais e trabalhosas. A subscrição Security Operations do Mandiant Advantage Threat Intelligence oferece analistas de segurança e responsáveis pela resposta a incidentes com monitoramento de ponta de vulnerabilidades, malware e atores para ajudá-los a priorizar os alertas e entender o atacante, os recursos e as motivações por trás dos seus eventos de ameaças. Ao correlacionar os alertas gerados pelo SOC com o Mandiant e também com os indicadores de código aberto (OSINT), as equipes de segurança obtêm orientação direta durante a triagem, investigação e resposta, melhorando a velocidade e a eficácia da segurança, reduzindo a fadiga geral do alerta. Além disso, a subscrição Security Operations auxilia as equipes de segurança com a detecção histórica de ameaças cibernéticas emergentes ao fornecer dados detalhados de indicadores de malware ou atores, disponibilizados por meio do portal da Mandiant Advantage, além da API.

O QUE ESTÁ INCLUSO:

- **Recursos do Mandiant Advantage Free**
- **Visualizações alternáveis dinâmicas de atores e malware com o mapa do MITRE ATT&CK, explorador de objetos e downloads de indicadores**
- **Acesso a indicadores conhecidos da Mandiant (IP, domínio, hash de arquivo, URL) com métricas de pontuação de maliciosidade**
- **Análises de notícias com comentários e avaliações de especialistas da Mandiant**
- **Briefings Trimestrais de Ameaças e suporte básico (fornecimento mais integração)**
- **Threat intelligence acessível por meio do portal, plugin para navegadores e API**

MANDIANT® ADVANTAGE

Mandiant Advantage Fusion

THREAT INTELLIGENCE ABRANGENTE PARA TODA A ORGANIZAÇÃO DE SEGURANÇA

Vantagens

- **Descubra Riscos Desconhecidos:** acesso personalizável e escalável à inteligência completa da linha de frente. Identifique ameaças globais, fora do perímetro da sua organização, com os recursos da inteligência sobre violações da Mandiant
- **Defesa Cibernética Bem Informada:** melhore sua estratégia de segurança com uma consciência situacional holística de vulnerabilidades, atores de ameaças, sua atividade e o possível impacto nos seus negócios
- **Entenda as Prioridades:** alivie a fadiga de alertas com acesso instantâneo às ameaças específicas que importam para a sua organização conforme elas ocorrem para ajudar a priorizar as atividades de segurança e evitar ataques de maneira eficaz
- **Reduza Riscos de Ameaças:** melhore os controles de segurança e simule táticas específicas dos atores durante exercícios de red team

Para tentar entender cada vez mais sobre seus adversários, as equipes de segurança com frequência analisam montanhas de informações de ameaças, muitas vezes influenciadas pelos fornecedores, que levam a uma sobrecarga de dados e reconciliam dados confiáveis desconhecidos com perfis de ameaças descobertos internamente. A subscrição Fusion do Mandiant Advantage Threat Intelligence é a única fonte de Threat Intelligence que a sua equipe de segurança precisa, fornecendo acesso total e ilimitado à Threat Intelligence da Mandiant, incluindo atividades de ameaças contínuas, passadas e previstas. A subscrição Fusion fornece às equipes de segurança uma visão inigualável e estratégica do cenário de ameaças, que combina várias faces de ameaças como crimes cibernéticos, espionagem cibernética, inteligência estratégica, inteligência física estratégica e inteligência relacionada a operações de adversários. Acesse milhares de relatórios FINISHED INTELLIGENCE (FINTEL) com base na análise estratégica de especialistas da Mandiant, telemetria global FireEye, resposta a incidentes da Mandiant e resultados de pesquisas técnicas, tudo em uma única visualização com busca.

O QUE ESTÁ INCLUSO:

- **Mandiant Advantage Free, Security Operations, Vulnerability e Digital Threat Monitoring**
- **Filtre por tipos de relatório, região, setor, nome do malware ou ator**
- **Relatórios de inteligência completos com narrativa que cobre contexto e pesquisas de análises táticas a estratégicas**

MANDIANT® ADVANTAGE

Mandiant Advantage Vulnerability (Módulo Adicional)

MAXIMIZE OS ESFORÇOS DE REDUÇÃO DA SUPERFÍCIE DE AMEAÇAS

Benefícios para Analistas de Vulnerabilidades, Proprietários de Dados ou Sistemas/TI, Gerentes de Riscos e Analistas de Inteligência

- **Visibilidade:** analise os dados de vulnerabilidade por tecnologia, atores e explore fontes
- **Priorize:** analise os dados pelos riscos e explore a classificação para focar nas vulnerabilidades que importam no momento
- **Notificações:** receba notificações de vulnerabilidades do dia 0
- **Instalação Rápida:** integra-se aos seus scanners de vulnerabilidades por meio do plugin para navegadores ou API

Diante da expansão contínua das infraestruturas de TI, novos aplicativos e localizações geográficas distintas, os Analistas de Risco de Vulnerabilidade podem se sentir sobrecarregados pelo número de vulnerabilidades a serem tratadas em seu ambiente. Analisar informações de vulnerabilidade pode ser um processo trabalhoso e mesmo dispondo de um sistema de classificação de vulnerabilidades simplificado, pode ser difícil saber por onde começar. A subscrição Threat Intelligence Vulnerability do Mandiant Advantage permite que as equipes de riscos de segurança avaliem, priorizem e solucionem vulnerabilidades descobertas no nível das empresas com o mecanismo de pontuação exclusivo baseado na facilidade de exploração, probabilidade da exploração e ameaça ou impacto percebidos.

O QUE ESTÁ INCLUSO:

- Recursos do Mandiant Advantage Free
- Pontuação e visualizações de vulnerabilidades da Mandiant, incluindo classificações de exploração, classificações de riscos, avaliações de dia zero e atividades observadas pelos nossos especialistas da linha de frente
- Relatórios abrangentes de vulnerabilidades incluindo CVE IDs, tecnologias vulneráveis, vetores de exploração e relatórios relevantes
- Briefings Trimestrais de Ameaças e suporte básico (fornecimento mais integração)

MANDIANT® ADVANTAGE

Mandiant Advantage Digital Threat Monitoring (Módulo Adicional)

AVISOS PRECOCES DE EXPOSIÇÕES A AMEAÇAS EXTERNAS

Benefícios para Analistas de Inteligências, Assessores Jurídicos, Comunicações Corporativas/ Relações Públicas, Executivos e Liderança Sênior

- **Visibilidade de Ameaças Externas:** identifique ameaças a ativos fora do perímetro da sua organização, inclusive na dark web
- **Configuração Simples:** com seus parâmetros de busca definidos, o Advantage monitorará continuamente vários fóruns, redes sociais, sites de dados vazados e publicações relacionadas a atores
- **Confiável:** reduza falsos positivos ou negativos com um portal protegido e no qual a indústria confia
- **Acelere a resposta:** prepare a resposta para limitar danos adicionais e defendas os ativos ou informações da empresa

Defesas cibernéticas tradicionais normalmente focam em ativos ou eventos que existem dentro da sua rede. No entanto, no mundo altamente conectado de hoje, você também precisa proteger ativos que se estendem além do seu perímetro, como a marca, as identidades e comunidade de parceiros da sua organização. A subscrição Digital Threat Monitoring do Mandiant Advantage fornece visibilidade precoce de exposições a ameaças externas que seus ativos enfrentam, com monitoramento da dark web que traz tranquilidade ou eliminação de enormes esforços manuais pouco práticos. Defenda-se contra os riscos que ameaçam sua marca, infraestrutura e parcerias de alto valor. Identifique violações, exposições e ameaças digitais na ampla deep e dark web, usando termos de busca de palavras-chave personalizados. Automatize, analise e gere alertas de ameaças em correspondências possivelmente significativas.

O QUE ESTÁ INCLUSO:

- Recursos do Mandiant Advantage Free
- Ferramentas de pesquisa baseadas em palavras-chave personalizadas para reconhecimento personalizado e escalonável e monitoramento da dark web
- Acesso a analistas da Mandiant para suporte a investigações e experiência
- Alertas de ameaças por meio do Painel de Alertas, incluindo atributos de status, fonte e severidade e insights para ajudar a gerenciar seus ativos monitorados.
- Briefings trimestrais de ameaças e suporte básico (fornecimento mais integração)

O PORTFÓLIO DE THREAT INTELLIGENCE DO MANDIANT ADVANTAGE

	FREE	SECURITY OPERATIONS	FUSION
TIPOS DE ACESSO			
Mandiant Advantage Platform e Browser Plug-in	●	●	●
API		●	●
ACESSO A DADOS			
Indicadores – Open Source – com Pontuação da Mandiant	●	●	●
Atores de Ameaças – Open Source e de Conhecimento Público	●	●	●
Malware e Famílias de Malware – Open Source	●	●	●
Painéis em Tempo Real – Atores, Malwares e Vulnerabilidades	●	●	●
Indicadores – Proprietários da Mandiant – com Pontuação e Contexto		●	●
Atores de Ameaças – Proprietários da Mandiant – UNC, Temp, APT, FIN		●	●
Malware e Famílias de Malware – Proprietários da Mandiant		●	●
Visualizações dinâmicas de Atores e Malwares ao Vivo – MITRE ATT&CK e Graph		●	●
VULNERABILIDADE			
Descrições de Vulnerabilidades Públicas/Conhecidas	●	●	●
Classificação de Riscos e Exploração da Mandiant	+ MÓDULO VULNERABILITY		●
Análise de Vulnerabilidade da Mandiant	+ MÓDULO VULNERABILITY		●
DIGITAL THREAT MONITORING (DTM)			
Monitoramento da Dark Web	+ DIGITAL THREAT MONITORING		●
Ferramentas de Busca e Alertas	+ DIGITAL THREAT MONITORING		●
INTELIGÊNCIA SOBRE ADVERSÁRIOS E ANÁLISES			
Análises de Notícias	●	●	●
Briefing Trimestral de Threat Intelligence		●	●
Relatórios Estratégicos – Região, Setor, Tendências			●
Relatórios de Motivações, Métodos, Ferramentas e Comportamentos de Adversários			●
Alertas de Atividades de Ameaças, Ameaças Emergentes e Relatório de Tendências			●
Relatórios de Pesquisas da Mandiant			●

Vulnerabilidade e Monitoramento de Ameaças Digitais podem ser comprados separadamente.

Para saber como a Mandiant Advantage oferece a inteligência sobre ciberameaças mais abrangente do mercado, visite **www.fireeye.com/advantage**

MANDIANT® ADVANTAGE

A complexidade do cenário cibernético continua a aumentar à medida que os adversários se tornam cada vez mais sofisticados e suas táticas se transformam com rapidez. Para reduzir proativamente os riscos dos negócios dos ataques motivados, as empresas precisam de tecnologia de validação contínua apoiada por inteligência relevante e oportuna. Mandiant, parte integrante da FireEye, reúne a Threat Intelligence líder no mundo e dados de resposta a incidentes da linha de frente com sua plataforma de validação de segurança contínua para equipar as empresas com as ferramentas necessárias para aumentar a eficácia da segurança e reduzir os riscos organizacionais, independentemente da tecnologia empregada.

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6500/877.FIREEYE (347.3393)
info@FireEye.com