

## FICHA TÉCNICA

# Portfólio de inteligência contra ameaças

## Maximize o valor e o impacto da sua inteligência contra ameaças



### DESTAQUES

- Serviços e assinaturas de inteligência decisiva contra ameaças adaptada à sua missão de segurança
- Visibilidade além do ciclo de vida típico do atacante, incluindo contexto e prioridade a ameaças globais
- Mais proteção de ativos para que se tome decisões mais bem informadas sobre o risco dos negócios
- Alinhamento dos recursos e programas de segurança contra as ameaças e agentes mais prováveis
- Conceba, construa e otimize a sua capacidade de consumir, analisar e utilizar a inteligência contra ameaças
- Acesso a inteligência e análise personalizada para tomadores de decisão e defensores de rede de linha de frente

Muitas vezes, os invasores cibernéticos são mais bem treinados, mais financiados e mais bem organizados do que muitas organizações de segurança. Os ataques cibernéticos estão cada vez mais complexos e os danos mais severos.

Por esses motivos, muitas organizações procuram reduzir seus riscos e aumentar sua segurança com os serviços de inteligência contra ameaças externas. No entanto, muitas organizações não sabem por onde começar, enquanto outras contratam sem entender quais inteligências de ameaças necessitam ou como devem ser usadas. De modo geral, os resultados são ineficazes e dispendiosos.

A FireEye Threat Intelligence é a resposta.

A FireEye Threat Intelligence é um portfólio de assinaturas e serviços criado para tratar de todos os aspectos das suas necessidades de inteligência contra ameaças. Esteja você iniciando sua jornada de inteligência contra ameaças ou já tenha uma equipe de inteligência dedicada, esta solução oferece os insights que melhoram a proteção de ativos, aprimoram a eficácia dos programas de segurança e informam o processo de riscos dos negócios. Ele oferece:

- **Assinaturas de inteligência:** Acesso a relatórios de inteligência publicados que cobrem inteligência estratégica e operacional, crimes cibernéticos e ameaças de espionagem cibernética, operações de informações, inteligência de vulnerabilidade e de ameaças do sistema de controle industrial.
- **Viabilização da inteligência:** Os analistas e gerentes da Inteligência contra ameaças designados normalmente trabalham com você como consultores confiáveis, para garantir que você obtenha o máximo do seu investimento de inteligência. Os tópicos incluem onboarding e provisionamento, integração de API com seus sistemas de segurança, acesso de analista, workshops estratégicos e de geração de relatórios de ameaças personalizados.
- **Desenvolvimento de recursos de inteligência:** Esses serviços e avaliações de consultoria ajudam você a perceber e sustentar o valor que você obtém da inteligência contra ameaça cibernética, já que ela permite que você avalie, construa e amadureça um programa de segurança conduzido por inteligência. Os serviços de ICD incluem avaliar as capacidades e exposição a ameaças do programa de inteligência contra ameaças existente, criando planos estratégicos para melhorias no programa e desenvolvendo uma estrutura operacional para o seu programa de inteligência contra ameaças.
- **Monitoramento das ameaças digitais:** Monitoramento proativo e sob medida e análise de ameaças à sua marca, suas VIPs e sua comunidade de parceiros integrados.
- **Acesso avançado à inteligência:** Essa capacidade permite buscas diretas dentro da visibilidade global, insights e inteligência da FireEye. Isso inclui acesso a um analista dedicado que pode ajudá-lo a realizar pesquisas e análises relevantes às suas necessidades específicas.

## Segurança que cresce com você

Não importa onde você esteja no seu programa de segurança, ou quais sejam as suas necessidades de inteligência, o portfólio da FireEye Threat Intelligence tem a solução para você. Se você estiver apenas começando, podemos ajudá-lo a avaliar onde você está e trabalhar junto com você para descobrir aonde precisa ir. Se você sabe de qual inteligência precisa e quem são as partes interessadas, nosso amplo leque de assinaturas de inteligência darão melhores informações sobre suas decisões de segurança. Por fim, se você precisar aprimorar as habilidades da sua equipe de inteligência ou estender as capacidades da sua equipe, a FireEye Threat Intelligence tem a solução para cuidar disso também.

### Avaliar

Determine onde você está em seus esforços de inteligência contra ameaças e prepare-se do jeito certo para obter o máximo valor da sua inteligência contra ameaças no futuro. Nós ajudamos a responder perguntas como:

- Qual é minha exposição a ameaças cibernéticas?
- Como a inteligência pode ser usada aqui?
- Quais são as lacunas no nosso atual programa de inteligência?

### Informe

Utilize inteligência abrangente e acionável para apoiar uma melhor defesa contra ameaças cibernéticas novas e emergentes. Uma ampla variedade de assuntos e casos de uso dão às suas equipes de segurança experientes ou em crescimento, um contexto essencial sobre a intenção, métodos e atividade do atacante. Nós ajudamos a responder perguntas como:

- Com base nos meus negócios, setor ou região, que ameaças estou mais propenso a sofrer?
- Que alertas preciso tratar primeiro e como posso compreendê-los melhor?
- Que vulnerabilidades devo corrigir primeiro com base na probabilidade de serem usadas contra mim?
- Como posso aprender mais sobre as ameaças à minha marca, VIPs, infraestrutura e comunidade de parceiros antes que elas aconteçam?

### Melhorar

Desenvolva melhores práticas e conhecimento do setor para aumentar a eficácia das suas operações de inteligência. Os serviços vão da criação da sua organização de inteligência ideal ao fornecimento de acesso a todas as ofertas de FireEye Threat Intelligence com o suporte de analistas dedicados. Nós ajudamos a responder perguntas como:

- Como podemos melhorar os recursos dos nossos analistas de inteligência?
- Como podemos melhorar os nossos recursos de caça de ameaças?
- Como posso complementar o nível de inteligência e conhecimento ao qual minha equipe tem acesso?

## RAZÕES PARA USAR A FIREEYE INTELLIGENCE

A FireEye sabe mais sobre ataques cibernéticos e sobre as pessoas responsáveis por eles do que qualquer outro. Temos acesso incomparável às atuais atividades cibernéticas, e as informamos diretamente às nossas operações de inteligência contra ameaças. A FireEye combina informações do adversário, da vítima e da campanha com dados de telemetria do produto, para produzir inteligência decisiva contra ameaças que nenhum concorrente consegue superar. Outras vantagens incluem:

- Mais de 12 anos de experiência em coleta, análise e consultoria de inteligência
- 180 indivíduos para buscas dentro de salas de operações em 23 países, falando mais de 30 idiomas nativos e locais
- Identificada como única líder no "The Forrester New Wave™": Serviços externos de inteligência contra ameaças, 3.º trimestre de 2018"
- Os serviços de desenvolvimento de recursos de inteligência baseiam-se em anos de compromisso com o cliente e desenvolvimento gradativo da função FireEye Threat Intelligence

Para saber mais, acesse: [www.fireeye.com/solutions/cyber-threat-intelligence.html](http://www.fireeye.com/solutions/cyber-threat-intelligence.html) e leia o **relatório da Forrester**.

### FireEye, Inc.

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

©2019 FireEye, Inc. Todos os direitos reservados. FireEye é uma marca registrada da FireEye, Inc. Todos os outros nomes de marcas, produtos e serviços são ou podem ser marcas comerciais ou marcas de serviços de seus respectivos proprietários. I-EXT-DS-US-EN-000003-03

### Sobre a FireEye, Inc.

A FireEye é a empresa líder em segurança orientada por inteligência. Atuando harmoniosamente como extensão expansível das operações de segurança dos clientes, a FireEye oferece uma plataforma única que mescla tecnologias de segurança inovadoras, inteligência contra ameaças em nível governamental e a consultoria mundialmente reconhecida da Mandiant®. Com essa abordagem, a FireEye elimina a complexidade e o fardo da segurança cibernética para organizações empenhadas em se preparar, prevenir e responder a ataques cibernéticos.

