FIREEYE™

Ficha técnica

Assinaturas da Threat Intelligence

Informe a sua empresa, não apenas seu appliance

DESTAQUES

- Oferece inteligência contra ameaças abrangente e decisiva em uma ampla variedade de temas
- Oferece visibilidade além do ciclo de vida típico do atacante, adicionando contexto e prioridade a ameaças globais
- Melhora a proteção de ativos e informa as melhores decisões para riscos dos negócios
- Alinha os recursos e programas de segurança contra as ameaças e agentes mais prováveis
- Lida com os casos de uso táticos, operacionais e estratégicos
- Melhora a priorização e a remediação dos alertas de segurança e a aplicação de patches de vulnerabilidades de segurança

Muitas vezes, os invasores cibernéticos são mais bem treinados, mais financiados e têm mais pessoal do que muitas organizações de segurança. Os ataques cibernéticos estão cada vez mais complexos e os danos resultantes mais severos. Encontrar e manter um profissional de segurança qualificado já é bastante difícil, mas encontrar o número necessário para atender por completo esses desafios seria financeiramente impossível.

As empresas de segurança estão procurando formas de aumentar sua própria experiência e eficácia de segurança. Elas precisam melhorar suas capacidades de resposta e garantir que suas defesas estejam alinhadas contra as ameaças mais prováveis. Tudo isso sem ir à falência.

As Assinaturas da FireEye Threat Intelligence atendem a esses desafios: são acessíveis — e contam com uma ampla variedade de insights de segurança eficazes e decisivos nos níveis estratégico, operacional e tático.

Tabela 1. Vantagens da FireEye Threat Intelligence.

A Intelligence identifica...	Vantagem
Quais ameaças e agentes você está enfrentando em seus negócios, setor ou região	Permite que você invista e implemente as medidas de segurança adequadas para lidar com elas
Quais alertas precisam ser investigados primeiro com insight contextual associado	Reduz o tempo para detecção e a fadiga de alerta, bem como aumenta o conhecimento da equipe
Em quais vulnerabilidades aplicar patches primeiro com base nas que estão sendo exploradas contra empresas semelhantes	Prioriza esforços de patch e reduz a probabilidade de ataques bem-sucedidos

As Assinaturas da FireEye Threat Intelligence são personalizadas conforme as necessidades da sua organização. Os tipos de assinaturas incluem:

- **Fusion:** Insights abrangentes sobre as atividades de ameaças do passado, presente e futuro. Inclui Operational, Cyber Crime, Cyber Espionage, a maioria dos conteúdos de Cyber Physical e uma versão anexada do FireEye Digital Threat Monitoring.
- **Operational:** Análise técnica de malware e táticas, técnicas e procedimentos (TTPs) relacionados de agentes maliciosos conhecidos, incluindo acesso a uma biblioteca de perfis de malware, visões gerais de agentes e indicadores de comprometimento (indicators of compromise, IOCs) legíveis por máquina para uma estrutura contextual aprimorada das ameaças.
- **Cyber Physical:** Insights decisivos sobre as ameaças cibernéticas e os ambientes industriais e tecnologia operacional (operational technology, OT) que enfrentam os riscos. Inclui toda a inteligência focada nos sistemas de controle industrial (industrial control systems, ICS) e na OT da FireEye.
- **Cyber Crime:** Avaliação aprofundada e rastreamento dos agentes de ameaças que focam em crimes financeiros: o que eles querem, quem eles visam e como operam.
- **Cyber Espionage:** Inteligência sobre grupos de ameaças persistentes avançados (advanced persistent threats, APT) associados a estados específicos, incluindo quem eles visam e quais TTPs eles usam, para ajudar as equipes de segurança a entenderem e lidarem com as ameaças iminentes e em curso.
- **Strategic:** As avaliações de ameaças em importantes setores da indústria e regiões, inclusive geopolítica, desenvolvimentos que afetam o cenário de ameaças cibernéticas e previsões sobre como os problemas de ameaça cibernética significativos evoluirão a curto e longo prazo.
- **Vulnerability:** Avaliações de inteligência de vulnerabilidades de software em muitas tecnologias, combinadas com avaliações proprietárias da probabilidade das recomendações de exploração e de mitigação.

De modo geral, a inteligência é apresentada na forma de relatórios. Estão disponíveis IOCs e inteligência legível por máquina, sempre que aplicável, para integrar com seus produtos de segurança existentes, como SIEMs e gerentes de vulnerabilidade. As Assinaturas da FireEye Threat Intelligence também incluem diversos recursos:

- **FireEye Intelligence Portal:** Acesso on-line a seus relatórios de inteligência e biblioteca de histórico completo da FireEye Threat Intelligence relacionados à sua assinatura específica. IOCs associados aos tipos específicos de inteligência podem ser baixados, e você pode fazer pesquisas para encontrar inteligência sobre agentes, malwares, setores e outras áreas de tópicos.
- **Acesso dos analistas:** Acesso dos analistas à Inteligência técnica e contra ameaças da FireEye e compreensão profunda sobre agentes, atacantes e riscos. Você entenderá melhor como algumas inteligências ou eventos se relacionam diretamente com seus interesses.
- **Opções de entrega:** Determina como você quer que sua inteligência seja entregue e com que frequência, inclusive alertas por e-mail e compilações.
- **Análise diária de notícias:** Um e-mail diário que rastreia as atuais notícias sobre segurança sendo cobertas pela mídia, para dar a você uma compreensão detalhada sobre o cenário da segurança. Isso inclui a cobertura de notícias pela mídia, avaliação da precisão das notícias pela FireEye e inteligência relacionada da FireEye para aumentar sua compreensão e capacidade de resposta.
- **API de Inteligência:** Este ponto de integração máquina-a-máquina permite que você use a inteligência da FireEye e nosso IOCs altamente eficiente nas suas operações de segurança e de rede, gestão de vulnerabilidade e sistemas de resposta a incidentes.
- **Plugin do navegador:** Este plugin expande a integração técnica da FireEye Threat Intelligence a qualquer página da internet que você acessar. Ele varre automaticamente a página da internet em busca de indicadores técnicos (tais como endereços de API, domínios e hashes), consulta a API de Inteligência em busca de qualquer inteligência relevante para a FireEye e, em seguida, cria um hiperlink para aquela inteligência.
- **Ferramentas de análise:** Os clientes usam esses serviços on-line ligados à inteligência para questionar sobre nomes de domínio específicos, endereços de IP e ameaças, bem como para fazer o upload de arquivos suspeitos para análise.

Nem mesmo os melhores profissionais de segurança sabem tudo sobre cada área do conhecimento (inclusive agentes, ameaças, vulnerabilidades, remediações efetivas, caça a ameaças). Com as Assinaturas da FireEye Threat Intelligence, você consegue obter o conhecimento, a experiência, a visibilidade e a capacidade analítica da FireEye, empresa líder em inteligência contra ameaças do mundo. E agora, todos da sua empresa podem ter acesso ao tipo de informações que os melhores profissionais passaram anos aprendendo.

A vantagem da FireEye

A FireEye sabe mais sobre ataques cibernéticos e sobre as pessoas responsáveis por eles do que qualquer outro. O motivo disso é o nosso incomparável acesso à atividade cibernética e às nossas extensas 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. Nossa inteligência se fundamenta em:

- Pesquisadores de campo em 22 países no mundo todo, em mais de 30 idiomas, que garimpam a deep web e a dark web em busca de informações sobre os métodos, motivações e infraestruturas dos adversários
- Mais de 15 mil sensores de rede em via de mão dupla no local do cliente, que fornecem dados sobre quais ameaças estão atingindo nossos clientes no mundo todo
- A FireEye Mandiant, empresa líder em resposta a incidentes no mundo, oferece informações de investigações de falhas sobre os TTPs usados por agentes avançados para ataques bem-sucedidos
- O maior banco de dados de histórico do setor de atividades relacionadas a ameaças, criado a partir de dados coletados nos eventos e incidentes cobertos por todos os nossos especialistas e tecnologia
- A FireEye foi considerada a única líder pelo The Forrester New Wave™: Serviços externos de inteligência contra ameaças, 3.º trimestre de 2018

SUPORTE DEDICADO AO CLIENTE

Três níveis de suporte e viabilização de inteligência para escolher:

NÍVEL 1

Linha de base: Materiais e processos básicos exigem o uso do FireEye Intelligence Portal e configuração do API de inteligência na sua empresa.

NÍVEL 2

Coordenação da inteligência: Linha de base + um gerente de viabilização de inteligência designado, acesso para consulta com analistas de inteligência da FireEye, resumos de ameaças trimestrais e revisões formais semestrais.

NÍVEL 3

Otimização da inteligência: Coordenação da Inteligência + um analista de otimização de inteligência designado, consultas de analistas adicionais, relatórios de ameaças personalizados, workshops estratégicos e informes sobre ameaças.

Para saber mais, acesse: **https://www.fireeye.com/solutions/cyber-threat-intelligence-subscriptions.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

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.