FICHA TÉCNICA

FireEye iSIGHT Threat Intelligence

Inteligência sobre ameaças com perspectiva e análise altamente contextual

VANTAGENS

- Tenha uma inteligência decisiva sobre ameaças adaptada à sua missão de segurança
- Proteja a sua organização de todas as categorias de ameaças, inclusive espionagem cibernética, crime cibernético e hacktivismo
- Ganhe conhecimento sobre o ciclo de vida estendido de um ataque cibernético por meio da visão incomparável da FireEye de adversários, vítimas e redes no mundo todo.
- Escolha o nível de suporte e integração de inteligência sobre ameaças mais adequado às suas necessidades

Visão geral

As assinaturas do FireEye iSIGHT Threat Intelligence proporcionam uma inteligência abrangente e decisiva para ajudar você a defender proativamente contra ameaças cibernéticas novas e emergentes, bem como alinhar o seu programa de segurança com metas de gerenciamento de risco corporativo. Personalizamos a inteligência para a sua equipe e missão de segurança, dando a ambas as equipes de segurança experientes e em crescimento o contexto crítico sobre a atividade e a intenção do atacante.

A vantagem do FireEye iSIGHT Threat Intelligence

O FireEye iSIGHT Threat Intelligence é o único no setor. Mais de 150 especialistas e pesquisadores de segurança da FireEye de todo o mundo aplicaram décadas de experiência na coleta de inteligência com perspectiva, de alta fidelidade e com foco no adversário. Com uma visão inigualável dos adversários, vítimas e redes ao redor do mundo, a inteligência de ameaças iSIGHT proporciona visibilidade do ciclo de vida estendido de um ataque cibernético em todos os níveis do seu empreendimento.

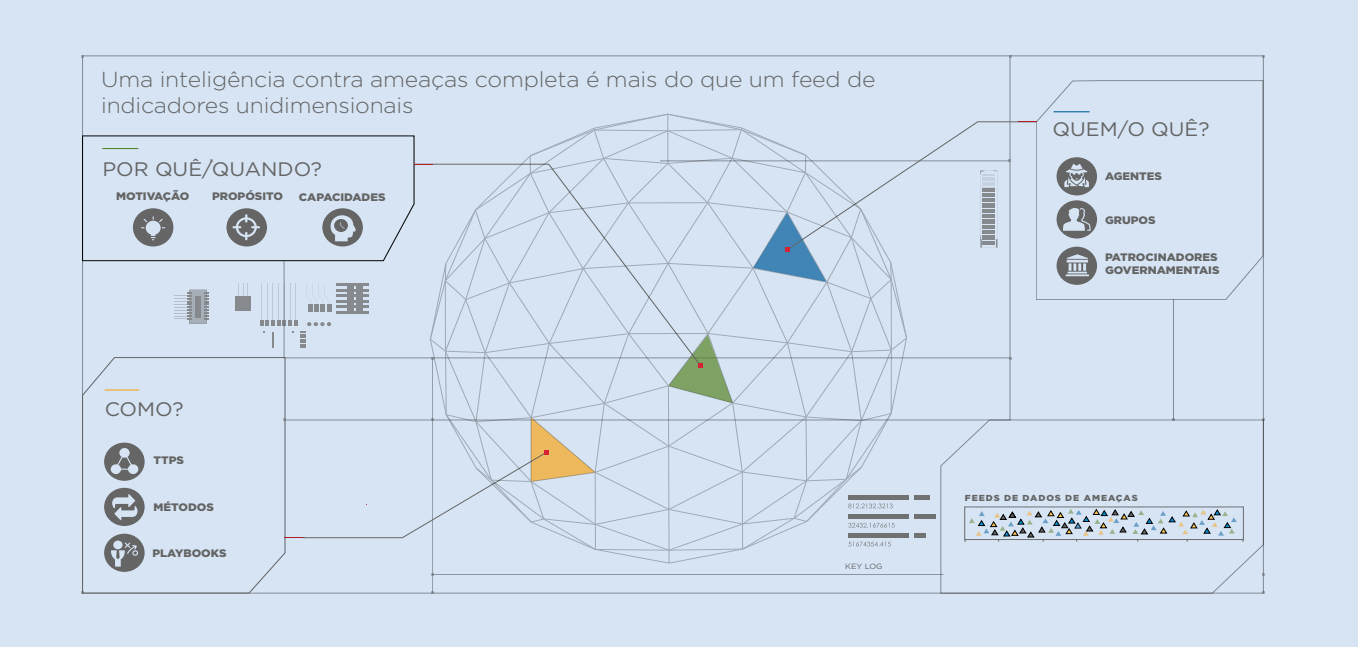
"O conhecimento sobre os seus inimigos ajudará você a vencer. Portanto, trate a inteligência sobre ameaças com o respeito que ela merece e utilize-a para proteger a sua organização de todos os adversários relevantes."

How to Collect, Refine, Utilize and Create Threat Intelligence (Como coletar, refinar, utilizar e criar inteligência sobre ameaças),
Gartner, outubro de 2016

Assinaturas do FireEye iSIGHT Threat Intelligence

As ofertas de assinaturas do iSIGHT Threat Intelligence são personalizadas para as necessidades da sua organização.

A **inteligência sobre fusões** proporciona uma percepção situacional abrangente do cenário global de ameaças com informações sobre atividade de ameaças atual, passada e prevista. Ela traz à sua equipe um profundo entendimento das atividades passadas, presentes e futuras do adversário, inclusive tendências e ferramentas, táticas e procedimentos típicos (typical tools, tactics and procedures, TTPs). A assinatura oferece às organizações os processos, cenários de defesa, aprofundamentos e análises do setor necessários para uma postura de segurança proativa. Ela inclui inteligência operacional. A inteligência sobre fusões é utilizada pelo centro de operações de segurança avançadas (security operations center, SOC) ou colaboradores de resposta a incidentes (incident response, IR) que proativamente caçam adversários e querem det alhes sobre autores de ameaças, seus motivos e TTPs.	A **Inteligência sobre espionagem cibernética** proporciona profunda análise e conhecimento de adversários cujos alvos sejam órgãos governamentais e empresariais para obter vantagem estratégica. Essa assinatura oferece perfis de políticas, estratégias, doutrinas e arte operacional de adversários emergentes. A inteligência sobre espionagem cibernética é utilizada por SOC avançado ou colaboradores de IR que proativamente caçam adversários e querem detalhes e TTPs dos autores de ameaças cuja motivação é a espionagem.	A **Inteligência sobre o crime cibernético** proporciona profundo conhecimento e análise técnica que permitem melhores respostas aos abusos de sistemas de computadores, operações de crime cibernético e ações cujo alvo é o dinheiro, bens ou serviços das vítimas. Com essa assinatura, você entenderá melhor as operações de roubo de credenciais, ransomware, ataques distribuídos de negação de serviço (“Denial-Of-Service”, DoS), comprometimentos de rede e malware, incluindo malware móvel e do ponto de venda (point-of-sale, POS). A inteligência sobre crime cibernético é utilizada por SOC avançado ou colaboradores de IR que proativamente caçam adversários e querem detalhes e TTPs dos autores de ameaças cuja motivação é o crime cibernético.
A **Inteligência operacional** proporciona aos analistas de segurança contexto decisivo para alertas que lhes permitem priorizar e informar suas respostas. Ela proporciona acesso à biblioteca FireEye completa de relatórios de inteligência de malware, bem como relatórios indicadores e visões gerais dos autores. A Inteligência operacional é utilizada pelo SOC ou equipes de IR que querem entender em quais ameaças devem se concentrar e quando.	A **Inteligência executiva** comunica riscos organizacionais aos responsáveis pelas decisões que dirigem a estratégia e o investimento em segurança. Ela inclui análises de conhecimento de setores, regiões e ameaças às redes empresariais. Melhora a comunicação no nível executivo sobre tópicos de segurança relevantes para a sua empresa. A inteligência executiva é utilizada por executivos de nível C, tais como diretores de segurança da informação (chief information security officers, CISOs), que queiram entender os riscos comerciais associados às ameaças cibernéticas.	A **Inteligência sobre vulnerabilidades** prioriza os fluxos de trabalho de gerenciamento de patches com base em exploits de vulnerabilidades ativas e em evolução nos seus sistemas corporativos críticos. Essa assinatura ajuda você a identificar vulnerabilidades não resolvidas, priorizar ciclos de aplicação de patches, aumentar a eficiência dos patches e muito mais. Relatórios incluem toda a inteligência sobre ameaças e vulnerabilidades relacionadas à infraestrutura crítica. A inteligência sobre vulnerabilidades é utilizada por profissionais de TI e analistas de vulnerabilidades que desejem melhorar a eficiência e focar seu tempo nas principais prioridades.



Mecanismos de entrega do iSIGHT Threat Intelligence

O acesso à inteligência e relatórios das assinaturas do iSIGHT Threat Intelligence pode ser feito de muitas formas.

Alertas e resumos via e-mail oferecem recursos designados por e-mail, como configurado através do Portal iSIGHT.	A **Ameaças em destaque na mídia** oferece um e-mail diário que acompanha histórias atuais sobre segurança, responde perguntas recebidas de executivos corporativos e inclui análises proativas de eventos importantes para seus executivos e membros da diretoria. Esse e-mail correlaciona destaques com relatórios do iSIGHT Intelligence para que você tenha um entendimento detalhado do cenário da segurança.	A **iSIGHT API e SDK** permite que você utilize a nossa inteligência com a sua infraestrutura de segurança e tecnologias de gerenciamento de risco e conformidade.
O **Portal da Inteligência** oferece acesso sob demanda à biblioteca on-line completa de relatórios anteriores para a sua assinatura específica.		**Plugin do navegador** faz varredura de páginas da web em busca de indicadores técnicos (IP, domínio, hashes) e consulta o iSIGHT API para inteligência iSIGHT relevante.
Onboarding e provisionamento fornecem usuários e API/chaves de plugin do navegador, bem como uma análise empresarial anual formal.		As **Ferramentas de análise** permitem o recebimento de informações contextuais sobre nomes de domínios, endereços IP e ameaças e carregam arquivos suspeitos para análise.

Integração e viabilização do iSIGHT Threat Intelligence

Seus analistas podem explorar o iSIGHT Intelligence para fazer consultas, conduzir pesquisa estendida e desempenhar análises detalhadas. Há três níveis de viabilização:

Nível 1: onboarding e provisionamento fornecem os materiais e o envolvimento que você precisa para utilizar as nossas soluções de inteligência, inclusive um portal de autoatendimento, suporte ao cliente e provisionamento da API. Está incluído no preço de compra de todas as assinaturas.	**Nível 2: coordenação de inteligência** proporciona um gerente de conta de inteligência FireEye designado que atua como concierge, guia e facilitador para o seu investimento FireEye.	**Nível 3: otimização de inteligência** oferece um gerente de conta de inteligência designado e um analista de ameaças que ajudam a integrar FireEye iSIGHT Threat Intelligence com as suas operações de segurança. Estão incluídos três workshops de inteligência por ano.

Tabela 1. Níveis de viabilização do iSIGHT Threat Intelligence

Serviços fornecidos	Nível 1 Onboarding e provisionamento (incluídos nas assinaturas)	Nível 2 Coordenação da inteligência	Nível 3 Otimização da inteligência
Onboarding	Sim	Sim	Sim
Portal de autoatendimento	Sim	Sim	Sim
Suporte ao cliente	Sim	Sim	Sim
Coletânea de consultas sobre ameaças			Sim
Provisionamento da API do iSIGHT	Sim	Sim	Sim
Exames corporativos formais	Remoto	Remoto	Remoto ou no local
Esclarecimento do acesso a analista		Sim	Sim
Requisições originais de acesso a analista		10 por trimestre	25 por trimestre
Requisições prioritárias de acesso a analista			2 por trimestre
Integração técnica da API do iSIGHT		1 hora para 1 caso de uso	4 horas para 2 casos de uso
Resumo genérico de ameaças		Sim	Sim
Resumo específico de ameaças			Sim
Workshops de inteligência			3 por ano

Para saber mais sobre a FireEye, visite: **www.FireEye.com**

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 de 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. A FireEye tem mais de 5.300 clientes em 67 países, incluindo mais de 845 empresas da Forbes Global 2000.

FireEye®