INTELIGÊNCIA SOBRE AMEAÇAS DA FIREEYE

VISÃO INIGUALÁVEL SOBRE ADVERSÁRIOS, VÍTIMAS E REDES NO MUNDO TODO

VISÃO GERAL

As organizações continuam lutando uma batalha assimétrica e estão despreparadas para vencer. Os atacantes são sofisticados, bem financiados, bem organizados e utilizam técnicas altamente direcionadas. As equipes de segurança têm dificuldades constantes para compreender quais ameaças cibernéticas representam maiores riscos para elas e como priorizar as que são realmente enfrentadas.

Quanto à eficácia da segurança, a maioria das organizações conta com canais de inteligência tática legados e baseados em assinaturas, os quais não podem antever ataques ou oferecer contexto para orientar a resposta. Em vez disso, esses canais inflam o volume de alertas com falsos positivos, tornando praticamente impossível detectar os ataques e proporcionando uma falsa sensação de segurança. A inteligência sobre ameaças certa pode ajudar as organizações a melhorar suas capacidades de detecção e resposta, além de reduzir o custo total de propriedade.

FIREEYE ISIGHT INTELLIGENCE: CONTEXTO DETALHADO PARA COMBATER AMEAÇAS

O FireEye iSIGHT® Intelligence é uma oferta em nível de país que proporciona inteligência tática, operacional e estratégica. Ele oferece conhecimentos sobre os adversários e suas motivações, intenções e métodos para ajudar as organizações a:

- Determinar e gerenciar proativamente os riscos enfrentados
- Detectar e prevenir ataques
- Construir um contexto do ataque para os alertas gerados

A inteligência sobre ameaças da FireEye deriva de três áreas principais:

- Das profundezas do ambiente de desenvolvimento do atacante, antes mesmo dos ataques serem iniciados
- Dos primeiros a responder às ameaças cibernéticas mais avançadas da mundo
- Da tecnologia orientada por MVX, que identifica ataques nunca antes vistos

Ao oferecer uma inteligência abrangente e imediatamente decisiva, as organizações podem gerenciar melhor seu risco e a resposta aos ataques de hoje em dia.

DESTAQUES

- Tenha acesso a uma inteligência abrangente sobre ameaças obtida com o rastreamento de mais de 16.000 agentes de ameaças, décadas de casos de resposta a incidentes e milhares de distribuições globais.
- Obtenha visibilidade sobre o ciclo de vida do ataque com inteligência sobre ameaças, tanto anterior quanto posterior ao ataque.
- Assine mais de 100 relatórios a cada mês, incluindo inteligência estratégica relacionada às motivações dos atacantes
- Aprimore investigações e planos de resposta com uma inteligência contextual que oferece respostas

FireEye
SECURITY REIMAGINED

CONJUNTO FLEXÍVEL DE PRODUTOS DE INTELIGÊNCIA SOBRE AMEAÇAS PARA SATISFAZER SUAS EXIGÊNCIAS

Dependendo dos requisitos do seu programa de segurança, a FireEye oferece um conjunto flexível de opções para operacionalizar a sua inteligência:

Inteligência sobre ameaças autônoma

A inteligência sobre ameaças do FireEye iSIGHT pode ser integrada na infraestrutura e nas ferramentas existentes. Essa inteligência é uma oferta em nível de país que proporciona inteligência tática, operacional e estratégica. Ela vai além das informações básicas proporcionadas por "canais de dados", consistindo em informações com perspectiva e altamente contextualizadas, necessárias para se construir defesas proativas, priorizar alertas e recursos, bem como aprimorar a resposta a incidentes.

Ela é oferecida com vários fluxos de inteligência consumível e acesso direto a analistas e suporte dedicado ao cliente. Maneiras de consumir a inteligência sobre ameaças autônoma do iSIGHT:

- Formato de máquina para máquina, por meio da API iSIGHT
- Formato legível para seres humanos, através do portal MySIGHT
- iSIGHT Threat Media Highlights, uma análise diária das principais notícias globais sobre segurança.

As organizações podem fazer assinatura de mais de 100 relatórios de inteligência todo mês, incluindo inteligência estratégica profunda vinculada a motivações dos atacantes e fluxos de inteligência tática e operacional. Esses relatórios permitem que os vários níveis de uma equipe de segurança permaneçam a par de problemas importantes e cientes de questões levantadas pela diretoria executiva.

Inteligência integrada dentro da tecnologia FireEye

Aprimore suas capacidades de detecção, investigação e resposta com assinaturas de inteligência sobre ameaças para a sua tecnologia FireEye. Essa inteligência é oferecida como assinaturas complementares na aquisição de produtos de detecção e investigação da FireEye, sendo fornecida em três variantes.

Dynamic Threat Intelligence (DTI)

Detecção insuperável com autoaprendizagem e análises que codificam as intenções e as ferramentas, táticas e procedimentos (TTPs) do atacante por meio do mecanismo FireEye Multi-Vector Virtual Execution (MVX). O DTI oferece atualizações a cada hora para assegurar que a sua organização encontre os ataques mais recentes vistos pela FireEye em sua rede global de clientes.

Advanced Threat Intelligence (ATI)

Quando a FireEye detecta um ataque, o ATI oferece a você o contexto necessário para priorizar os recursos e desenvolver uma resposta apropriada. A inteligência disponível inclui quem é o agente associado à ameaça, quais são suas motivações prováveis, informações do setor e visões globais sobre o malware e outros indicadores que você pode usar para pesquisar os atacantes no seu ambiente.

ATI+

Aproveite o monitoramento contínuo de alertas críticos e de eficácia de detecção da FireEye.

O ATI+ também oferece acesso a dossiês, tendências, notícias e análises fundamentais sobre grupos de ameaças avançadas, bem como perfis dos setores visados, incluindo informações sobre os tipos de dados visados pelos grupos de ameaças.

O diferencial de nossa inteligência sobre ameaças

- Visibilidade profunda e ampla sobre o ciclo de vida do ataque e as motivações, ferramentas e procedimentos do atacante. Visibilidade prévia e acesso às ameaças mais recentes e mais sofisticadas de centenas de analistas incorporados profundamente no ecossistema de desenvolvimento do adversário, visibilidade de décadas nas linhas de frente das principais investigações de ataques cibernéticos e uma rede global de onze milhões de nós de detecção de ameaças por meio de uma compreensão codificada das intenções do atacante.
- Mecanismo de análise flexível e expansível para rastrear atacantes em constante evolução. Banco de dados gráfico e matemático com mais de 125 milhões de nós que modela dinamicamente os relacionamentos entre as ferramentas e as táticas utilizadas pelos grupos de ameaças, as operações que eles realizam e seus patrocinadores.
- Especialistas de vários domínios que rastreiam e analisam rigorosamente as dimensões financeiras e políticas de mais de 16.000 ameaças cibernéticas em todo o mundo.

Esse alcance de visibilidade e compreensão dos adversários e suas motivações, intenções e métodos é oferecido às organizações através do portfólio de inteligência sobre ameaças da FireEye. Com esse tipo de inteligência sobre ameaças, as equipes de segurança reduzem a superfície de ataque e mudam de uma postura com uso intensivo de recursos para uma postura proativa que trata das ameaças de forma significativamente mais efetiva e eficaz.

	DTI	ATI	ATI+	INTELIGÊNCIA ISIGHT
Estágio do ataque do qual se origina a inteligência	Ataque	Ataque	Ataque	Pré-ataque, ataque, pós-ataque
Tipo de inteligência	Tática	Operacional	Estratégica de base	Ferramentas de análise e inteligência contextual
Detecção por appliances FireEye	✓			
Perfis de detecção para appliances FireEye		✓		
Correlação da FireEye entre alertas e localizações geográficas		✓		
Atribuição, pela FireEye, de alertas a agentes de ameaças conhecidos		✓		
Monitoramento de alertas			✓	
Monitoramento da integridade do sistema			✓	
Perfis de grupos de ameaças			✓	✓
Perfis setoriais			✓	
Perfis de famílias de malware			✓	
Media Highlights			✓	✓
Indicadores de ameaças via API				✓
API e SDK para integração em ferramentas não FireEye				✓
Plug-in de navegador do iSIGHT para varredura, consulta e mudança de etapa para a inteligência do iSIGHT				✓
Atribuição de indicadores de ameaças do iSIGHT a agentes de ameaças conhecidos				✓
Cobertura estendida de agentes de ameaças				✓
Inteligência executiva				✓
Rastreamento de vulnerabilidades em sistemas corporativos				✓
Rastreamento de vulnerabilidades em infraestrutura crítica				✓
Rastreamento de explorações				✓
Contexto para alertas na infraestrutura de TI existente				✓

Para obter mais informações sobre a FireEye, visite:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye