FIREEYE™

FICHA TÉCNICA

FireEye Detection On Demand

Faça a varredura do conteúdo em busca de ameaças a qualquer momento no seu fluxo de trabalho

DESTAQUES

- Detecte e previna malwares conhecidos e desconhecidos em qualquer lugar
- Implemente plug-ins compatíveis com a FireEye para navegadores e armazenamento na nuvem
- Obtenha uma análise do contexto do malware detectado no formato JSON

Introdução
As ameaças podem vir, e vêm, de toda parte, e cada empresa aborda a segurança de maneira diferente com base nas suas necessidades, setor e ambiente. Mas a única coisa que todas as empresas têm em comum é a necessidade de um recurso de detecção de ameaças validado e apoiado por inteligência, com análise de contexto suficiente para agir.

Com a FireEye Detection On Demand, disponível para clientes da FireEye por uma API (Advanced Threat Intelligence), as organizações podem enviar arquivos de modo seguro para se manter protegidas contra as ameaças atuais que exploram vulnerabilidades dos sistemas operacionais Microsoft Windows e Apple OS X ou de aplicativos.

A FireEye Detection On Demand utiliza o mecanismo de detecção atual FireEye Multi-Vector Virtual Execution™ (MVX) e a Intelligence Driven Analysis (IDA) para chegar rapidamente a um veredito sobre os arquivos enviados. MVX é um mecanismo de análise dinâmica e sem assinaturas que inspeciona tráfego de rede suspeito para identificar ataques que contornam defesas tradicionais com base em assinaturas e políticas. IDA é uma coletânea de mecanismos de regras dinâmicas e contextuais que detecta e bloqueia atividades maliciosas, tanto em tempo real quanto retroativamente, com base na inteligência mais recente obtida de máquinas, atacantes e vítimas.

Detecção de ameaças premium em qualquer arquitetura de segurança
A FireEye Detection On Demand é um serviço de detecção de ameaças nativo da nuvem, que rapidamente faz uma varredura no conteúdo enviado para identificar malwares residentes. Ao contrário das soluções de segurança de arquivos baseadas em algoritmos de integridade do arquivo, controles de política de ameaça interna ou mecanismos de verificação estática, seus envios são processados usando as mesmas tecnologias que alimentam muitas das consolidadas ofertas da FireEye.

O acesso à FireEye Detection On Demand é configurado facilmente por uma API. Ela pode ser integrada ao fluxo de trabalho do seu centro de operações de segurança (*Security Operations Center*, SOC), análise SIEM [*Security Information and Event Management* (Sistema de gerenciamento de eventos e incidentes de segurança)], repositórios de dados e aplicativos web do cliente, entre outros. Ela oferece capacidades flexíveis de análise de conteúdo e de arquivo, para identificar comportamentos maliciosos onde quer que a empresa necessite.

Além de receber um veredito sobre cada arquivo e conteúdo enviado por meio da Detection On Demand, você recebe detalhes de contexto de apoio, como alterações em arquivos, registros, processos e rede, bem como achados relevantes da sempre atualizada FireEye Dynamic Threat Intelligence.

Como a Detection On Demand funciona

A FireEye Detection On Demand compara seu envio com as mais recentes táticas e assinaturas de agentes de ameaças conhecidas utilizando análise estática, inteligência artificial e aprendizado de máquina. A FireEye também determina a possibilidade de efeitos secundários ou combinatórios em diversas fases do ciclo de vida do ataque para descobrir explorações e malwares nunca antes vistos.

Figura 1. Como a Detection On Demand funciona.

FireEye Developer Hub

Você pode visitar o FireEye Developer Hub em https://fireeye.dev para explorar os plugins e códigos de amostras, além de colaborar com a comunidade de desenvolvimento da FireEye sobre a Detection On Demand.

Como comprar

A Detection On Demand está disponível pelos canais convencionais da FireEye ou diretamente pelo AWS (Amazon Web Services) Marketplace (para envios de baixo volume).

Ao adquirir o serviço, você especifica sua necessidade com base no número de envios que espera realizar ao longo de um ano. As compras no AWS Marketplace oferecem uma cota de envio mensal em um modelo de cobrança anual. A taxa de envio de arquivos é limitada a 100/minuto. A taxa de envio de hash é limitada a 200/minuto.

Pode ser atribuído aos arquivos e outros materiais enviados à Detection On Demand um valor de envio superior a um envio; a FireEye informará os valores de envio padrão.

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 reagir a ataques cibernéticos.