FIREEYE AS A SERVICE

AMPLIE AS OPERAÇÕES DO SEU PROGRAMA DE SEGURANÇA COM OS MELHORES CONHECIMENTOS, INTELIGÊNCIA SOBRE AMEAÇAS E TECNOLOGIA DO SETOR

VISÃO GERAL

As ameaças à segurança hoje em dia estão cada vez mais sofisticadas em suas maneiras de visar, atacar e infiltrar organizações para roubar seus ativos mais preciosos. A tecnologia, apenas, não basta para derrotar um atacante determinado. Além disso, contratar, treinar e reter especialistas em segurança é difícil e caro. Você precisa de um parceiro confiável para monitorar continuamente a sua rede e os seus sistemas com uma plataforma de tecnologia avançada e a mais recente inteligência sobre ameaças coletada em todo o mundo. Você precisa do FireEye as a Service.

FireEye as a Service

O FireEye as a Service é um serviço gerenciado de detecção, investigação e resposta que minimiza o impacto corporativo potencial de ataques cibernéticos direcionados e cada vez mais sofisticados.

O FireEye as a Service oferece uma segurança em nível de Fortune 50 a uma fração do custo, acelerando a sua defesa ao proporcionar investigação profunda de ameaças, avaliação de comprometimento e recomendações práticas de correção, além de visibilidade sobre campanhas de ataque emergentes.

Como funciona

O FireEye as a Service integra pessoas, tecnologia e inteligência para operacionalizar a detecção e a investigação dos atacantes na rede de uma organização.

O FireEye as a Service aproveita os investimentos em tecnologia existentes, tanto da FireEye quanto de terceiros, para proporcionar visibilidade em tempo real por toda a corporação, incluindo suas filiais mais remotas.

Os especialistas em análise de ameaças da FireEye vão além do monitoramento de segurança tradicional, utilizando técnicas próprias respaldadas por uma inteligência sobre ameaças coletada de adversários, vítimas e máquinas para detectar, investigar e caçar proativamente ameaças antes não detectadas.

DESTAQUES

- **Percepção situacional inigualável:** visibilidade em tempo real sobre avaliação e resposta contínuas a ameaças emergentes por meio de nossos dashboards de proteção comunitária.
- **Respostas, e não apenas alertas:** relatórios de comprometimento detalhados que avaliam a atividade do atacante e mostram evidências em termos de cadeia de destruição, incluindo amplo contexto e recomendações de resposta para que você possa determinar rapidamente o risco e tomar providências.
- **Equipe de especialistas:** milhares de analistas de ameaças, especialistas em malware, encarregados de resposta a incidentes, administradores de inteligência e especialistas forenses.
- **Técnicas avançadas de caça:** os analistas de avaliação de ameaças da FireEye oferecem insights comportamentais profundos que não podem ser reproduzidos.
- **Centros globais de resposta a ameaças avançadas:** (ATRCs) nos Estados Unidos (Virgínia e Califórnia), Irlanda, Alemanha, Cingapura, Sydney e Japão oferecem cobertura 24 horas por dia, sete dias por semana.
- **Inteligência aplicada sobre ameaças:** analistas de segurança aplicam a mais recente inteligência sobre ameaças, coletada de adversários, vítimas e máquinas, para localizar e detalhar ameaças no seu ambiente mais rapidamente.
- **Capacidade de aproveitar os investimentos existentes:** integração com qualquer operação de segurança no local, na nuvem ou em um ambiente híbrido.
- **Gerentes de relacionamento:** viabilização de suporte adicional, como análise de amostras de malware, análise forense detalhada ou resposta a incidentes no local.

Quando validamos indícios de comprometimento, você é notificado imediatamente e recebe um relatório completo com o contexto da ameaça — quem, o quê, quando e como — para ter informações para uma resposta efetiva. Em alguns casos, oferecemos recomendações para colocar em quarentena imediata os sistemas e evitar que os atacantes se movimentem lateralmente na sua organização. Se necessário, os responsáveis pela resposta a incidentes da FireEye, com sua experiência forense, podem ajudar você a solucionar o incidente rapidamente e avaliar seu impacto para uma divulgação imediata e precisa.

Um novo tipo de segurança gerenciada com o FireEye as a Service

Amplie a sua equipe com especialistas em análise de ameaças

Especialistas em análise de ameaças monitoram as suas redes e endpoints 24 horas por dia, sete dias por semana, utilizando a mais recente inteligência e metodologias próprias para procurar indícios de comprometimento e realizar investigações de caçada proativa e triagem por especialistas. Esses especialistas determinam o âmbito do ataque apresentado pela cadeia de destruição do atacante para revelar quais ataques ocorreram, quando e como ocorreram e quem pode estar por trás deles. Eles aplicam seus conhecimentos de grupos de ataque e de como estes operam para oferecer recomendações decisivas, complementadas pelo contexto do atacante.

Visibilidade sobre campanhas emergentes: proteção comunitária

A proteção comunitária oferece aos clientes visibilidade em tempo real e percepção situacional de ameaças emergentes. Quando a FireEye detecta uma ameaça emergente, uma investigação interdisciplinar é iniciada, aproveitando informações de inteligência sobre o adversário obtidas por nossa equipe FireEye iSIGHT, nossa perspectiva de mercados verticais e geopolíticos, visibilidade de linha de frente dos consultores da Mandiant e telemetria de nossos produtos distribuídos por todo o mundo. Os clientes podem visualizar os desdobramentos de resposta a cada evento ao longo de um ciclo de quatro estágios: avaliação, mobilização, sustentação e resolução. Além disso, a proteção comunitária apresenta as técnicas do FireEye as a Service que detectam o evento, as capacidades de detecção de eventos de nossos produtos e os detalhes e contexto que o FireEye iSIGHT Intelligence oferece.

Segurança de nível Fortune-50: fornecida a uma fração do custo

O FireEye as a Service ajuda você a aprimorar sua postura de segurança e a estender as capacidades do seu SOC a um custo 15 a 25% menor do que fazendo você mesmo. Você poderá priorizar as ameaças mais relevantes para aumentar a eficiência do seu trabalho de resposta. Isso torna a equipe existente mais eficaz e a ajuda a se concentrar em tarefas como a caçada proativa, que demandam mais supervisão humana. A detecção e a contenção de ameaças conhecidas e emergentes antes que algum dano seja feito também ajudam a eliminar iniciativas de correção caras e demoradas.

Capacidades

Serviço totalmente gerenciado

Com o FireEye as a Service, você tem um parceiro confiável oferecendo tecnologia poderosa, inteligência decisiva e conhecimentos avançados na forma de um serviço completamente gerenciado, voltado para a prevenção de ameaças avançadas.

Monitoramento por especialistas

A equipe de analistas da FireEye especializados em ameaças monitora o seu ambiente 24 horas por dia, sete dias por semana, aplicando a mais recente inteligência e metodologias próprias para procurar indícios de comprometimento.

Investigação

Quando um alerta é acionado, nossos analistas de ameaças investigam para determinar o âmbito do ataque, inspecionando minuciosamente o tráfego de rede ou o endpoint para determinar a extensão do comprometimento. Utilizando a inteligência da FireEye, esses analistas podem identificar a cronologia da cadeia de destruição para revelar quando e como ocorreu o ataque, quem esteve por trás dele e o que foi visado.

Inteligência aplicada sobre ameaças

Informações de inteligência novas são geradas e aplicadas através de análise por especialistas e compartilhamento automatizado de inteligência, proporcionando visibilidade global sobre ameaças emergentes.

Respostas, e não apenas alertas

Os melhores analistas de ameaças e especialistas em resposta a incidentes do setor aproveitam dados forenses de sistemas e redes para investigar, classificar e analisar riscos em tempo real, gerando relatórios detalhados sobre exatamente o que aconteceu. Recomendações sobre como conter a ameaça são fornecidas imediatamente.

Defesa poderosa

As tecnologias da FireEye, que realizam mais de 50 bilhões de análises de máquinas virtuais e processam 400.000 amostras exclusivas de malware por dia, podem ser distribuídas no seu ambiente. Milhões de sensores que coletam inteligência nova ao redor do mundo são, então, combinados a uma inteligência ricamente contextualizada e atualizam o ecossistema da FireEye a cada 60 minutos, proporcionando uma defesa poderosa por meio de detecção e prevenção.

Cobertura que satisfaz as suas necessidades

O FireEye as a Service oferece dois níveis de serviço para proporcionar a você a flexibilidade necessária para se adaptar conforme suas necessidades mudarem:

Orientação contínua é um serviço gerenciado de detecção que aproveita informações de segurança da FireEye e de terceiros para ajudar os clientes a identificar, validar e priorizar ameaças conhecidas e emergentes.

Após detectar uma possível ameaça, nossos analistas realizam uma validação e uma triagem do incidente, atribuindo um nível de gravidade baseado na inteligência sobre ameaças, na experiência e nos insights acumulados em relação à maneira como os atacantes atuam. Nossas consultorias sobre incidentes proporcionam informações abrangentes, incluindo evidências descobertas e inteligência sobre ameaças relevante para ajudá-lo a compreender o ataque.

Caso investigações adicionais sejam necessárias, a Orientação contínua indica etapas recomendadas para ajudar a determinar o âmbito do ataque. No caso de ameaças conhecidas, oferecemos recomendações de correção para acelerar a sua resposta.

A **Vigilância contínua** soma-se a Orientação contínua, com uma investigação detalhada de ameaças conhecidas e emergentes.

Combinamos nosso amplo conhecimento sobre comportamentos de grupos de ameaças com métodos de investigação próprios para descobrir indícios de intrusão, aprender como os atacantes estão operando e avaliar o alcance de suas capacidades. Também utilizamos técnicas de detecção orientadas por analistas para caçar proativamente indicadores ocultos de realização ou tentativa de comprometimento que passam despercebidos por defesas de tecnologia tradicionais.

Nossas Avaliações de comprometimento oferecem o contexto orientado por ações e definitivo de que você necessita para compreender plenamente as ameaças, avaliar seu risco e realizar as ações recomendadas.

CAPACIDADE	ORIENTAÇÃO CONTÍNUA	VIGILÂNCIA CONTÍNUA
Oferecer proteção comunitária	Sim	Sim
Assimilar alertas da FireEye	Sim	Sim
Resolver alertas benignos, falsos positivos e duplicados	Sim	Sim
Validar e priorizar incidentes	Sim	Sim
Inteligência sobre ameaças	Apenas detalhamento do incidente	Acesso ao portal de inteligência da FireEye
Investigar alertas suspeitos e confirmados	O cliente tem acesso a investigações orientadas via TAP	A FireEye realiza a investigação
Realizar detecção orientada por analistas (caçada proativa)	Não	Sim
Oferecer relatórios críticos	Consultoria sobre incidentes (com recomendações de investigação)	Relatório de comprometimento (com recomendações de correção)
Oferecer gerentes de relacionamento	Não exclusivos	Exclusivos

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

SOBRE A FIREEYE, INC.

A FireEye é líder em segurança como serviço (SaaS) 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 sobre ameaças em nível de país 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 5.000 clientes em 67 países, incluindo mais de 940 empresas da Forbes Global 2000.

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

www.FireEye.com