THREAT ANALYTICS PLATFORM

DETECÇÃO E INVESTIGAÇÃO DE AMEAÇAS COM BASE NA NUVEM

VISÃO GERAL

As organizações estão lutando uma batalha assimétrica. Os adversários são esquivos, polimórficos, bem financiados e capazes de contornar tecnologias de segurança ultrapassadas para vazar seus dados mais importantes. As organizações estão com carência de pessoal, sobrecarga de alertas e não têm a visibilidade e as informações de que precisam para detectar e investigar ameaças cibernéticas.

A FireEye está transformando a detecção e a investigação de incidentes com nossa plataforma baseada na nuvem, a Threat Analytics Platform (TAP). A TAP proporciona visibilidade em nível corporativo, conhecimento em detecção codificada e fluxos de trabalho de investigação orientada para aumentar sua defesa contra os ataques cibernéticos mais sofisticados.

Desenvolvida por profissionais de segurança

A FireEye desenvolveu integralmente a TAP — de profissionais de segurança para profissionais de segurança. A TAP combina insights sobre ameaças obtidos na resposta às violações de maior repercussão do mundo com análises de segurança de big data e conhecimento em segurança codificada, para que você possa identificar e investigar ameaças cibernéticas com rapidez.

Visibilidade em nível corporativo

Os agressores podem entrar em qualquer lugar. Você precisa de visibilidade em qualquer lugar. A TAP fornece visibilidade em nível corporativo, agregando alertas da grande variedade de tecnologias de segurança existentes na sua organização. Nossos sensores de redes de pequeno porte fornecem visibilidade em tempo real dos ambientes distribuídos, agregando eventos de locais remotos e os enviando a um local centralizado para retenção de registros, análise e investigação de ameaças.

Detecção adaptável

Seus adversários estão sempre mudando. Suas capacidades de detecção e investigação devem evoluir na mesma velocidade. A FireEye tem uma equipe exclusiva para a TAP, formada por cientistas de dados e pesquisadores de segurança que incorporam amplo conhecimento de resposta a incidentes na linha de frente a regras de detecção, análises de comportamento e investigações orientadas. Em questão de horas após a descoberta de um ataque emergente, eles criam novas regras, executam análises retrospectivas de seu ambiente para determinar o impacto possível e incorporam tais regras ao produto da TAP. Ao descobrir atividades nocivas, a TAP gera alertas enriquecidos com dados complementares, como o contexto do agressor, para ajudar o investigador a validar e determinar o escopo do incidente.

DESTAQUES

- **Finalidade específica** – plataforma baseada na nuvem, desenvolvida por profissionais de segurança para profissionais de segurança
- **Respostas, não alertas** – identifique ameaças conhecidas e desconhecidas, implementando informações em tempo real sobre ameaças a fluxos de eventos empresariais
- **Conhecimento em detecção codificada** – aumente suas capacidades de detecção e investigação com o conhecimento codificado dos pesquisadores de segurança e cientistas de dados da FireEye
- **Insights integrados sobre ameaças** – agilize a investigação de incidentes, enriquecendo alertas com contexto detalhado sobre o agressor
- **Pesquisa subsecundária** – um melhor tempo de pesquisa em bilhões de eventos ajuda os analistas de segurança a buscar proativamente por comportamentos ocultos na rede
- **Implementação rápida** – operacional em questão de horas, em vez de meses ou anos
- **Fácil expansão** – infraestrutura flexível e baseada na nuvem, que permite que as organizações se adaptem facilmente a mudanças nas necessidades de negócios ou requisitos sazonais
- **Custos previsíveis** – o modelo "software-as-service" garante a previsibilidade das despesas operacionais com software, suporte, infraestrutura, informações sobre ameaças e conhecimento de segurança

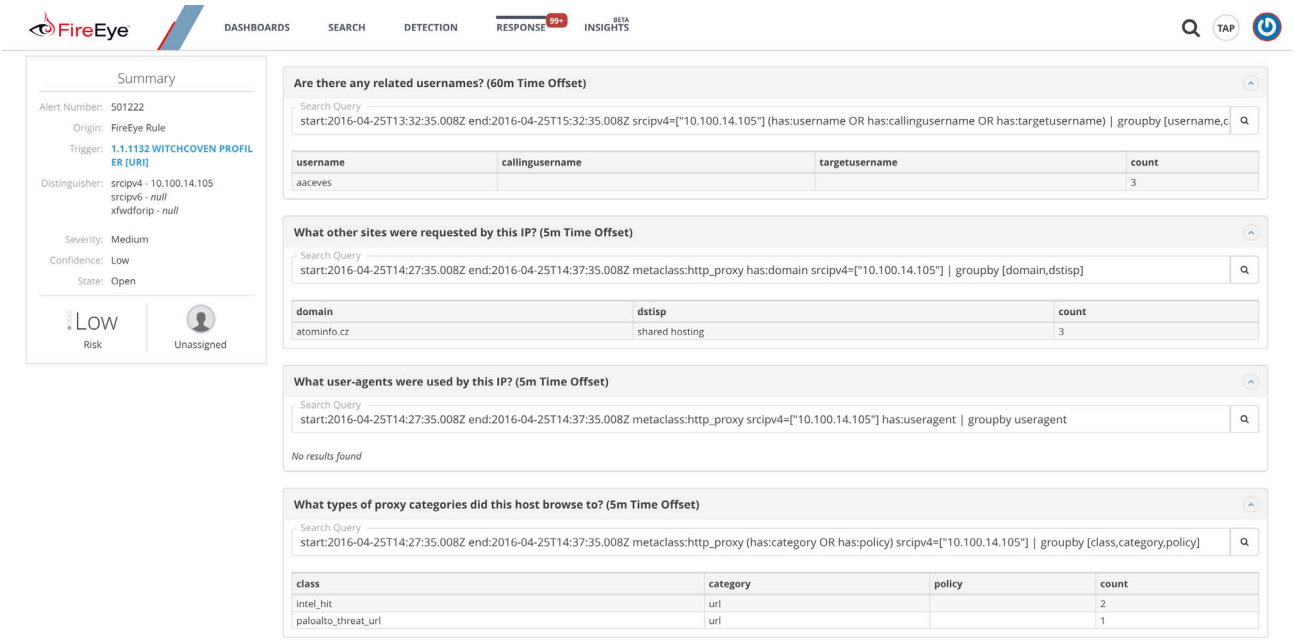
Acelere a investigação de ameaças

A capacidade de sua equipe de responder a um número cada vez mais alto de ataques cibernéticos é forçada até o ponto de ruptura. Você precisa de um aumento significativo na produtividade e na eficácia das operações de segurança, acelerando seu ciclo de vida de resposta a incidentes.

A TAP acelera a investigação, enriquecendo alertas com dados complementares. Informações sobre ameaças, contexto pontual sobre os usuários afetados, ações implementadas e os hosts envolvidos ajudam a validar e determinar o escopo do incidente.

A TAP também oferece investigações orientadas para ajudar a aumentar a eficácia de investigação dos responsáveis pela resposta. Nossa capacidade de investigação orientada guia os analistas por estratégias de investigação líderes do setor, fornecendo consultas previamente preenchidas com base no conhecimento da FireEye sobre cenários de ataque específicos.

Ao receber um alerta, a TAP seleciona e apresenta as próximas consultas relevantes, fornecendo um fluxo de trabalho ideal para orientar e informar sua investigação da ameaça.



Pense como seu agressor

Para passar da resposta reativa à defesa proativa, você deve pensar como seu agressor. A TAP inclui acesso ao Centro de inteligência da FireEye (FIC) para ajudá-lo a compreender os métodos e motivações de seus adversários, além de prever suas próximas ações. O FIC agiliza a investigação de incidentes, fornecendo informações práticas aos usuários. Os abrangentes perfis do FIC detalham as ferramentas, técnicas e procedimentos usados pelos autores de ameaças que visam especificamente o seu setor.

Descubra atividades ocultas

Quando um adversário escapa da detecção, não há evidência de comprometimento, ou seja, não há ponto de partida para a investigação. Para descobrir campanhas de ataque emergentes, você é quem deve iniciar a busca de evidências de comportamento oculto. A TAP proporciona agilidade à exploração de dados por meio da pesquisa subsecundária em bilhões de eventos, permitindo que os analistas de segurança sejam proativos na busca por indicadores ocultos de comprometimento. Uma vez identificados, ferramentas de investigação ágeis ajudam os analistas a passar de um indicador para outro, avaliar o contexto de anomalias recém-descobertas, reconstruir a linha do tempo do ataque e, finalmente, limitar o impacto da violação.

Implementação simplificada acelera a geração de valor

A TAP exige mínima configuração no local, simplificando a implementação e eliminando a contratação de serviços profissionais onerosos. Nossa infraestrutura baseada na nuvem tem flexibilidade de escala, possibilitando uma adaptação rápida a mudanças em necessidades de negócios e requisitos sazonais. A assinatura da TAP inclui software, suporte, infraestrutura, inteligência sobre ameaças e conhecimento em segurança codificada, garantindo que a despesa operacional seja previsível.

FIGURA 1 - FIREEYE THREAT ANALYTICS PLATFORM

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