McAfee Threat Intelligence Exchange

Informações compartilhadas sobre ameaças em várias soluções de segurança

O McAfee® Threat Intelligence Exchange atua como um intermediador de reputação para viabilizar detecções e respostas adaptáveis às ameaças. Ele combina a inteligência local, oriunda das soluções de segurança da sua organização, com dados externos de ameaças globais e compartilha instantaneamente essa inteligência coletiva com o seu ecossistema de segurança, viabilizando soluções para intercâmbio e ações com base na inteligência compartilhada.

Crie um ecossistema colaborativo de inteligência sobre ameaças

O McAfee Threat Intelligence Exchange, como intermediador de reputação, combina inteligência sobre ameaças de fontes globais importadas, como o McAfee Global Threat Intelligence (McAfee GTI), e informações de terceiros sobre ameaça (como VirusTotal) com inteligência de fontes locais, incluindo endpoints, gateways e soluções de análise avançada. Ao utilizar Data Exchange Layer (DXL), ele compartilha imediatamente essa inteligência coletiva pelo seu ecossistema de segurança, permitindo que as soluções de segurança operem como uma só para aprimorar a proteção por toda a organização.

A simplicidade de integração, possibilitada pelo DXL, reduz significativamente os custos operacionais e de implementação de diversas integrações de interface de programação de aplicativos (API) e proporciona segurança, eficiência operacional e eficácia inigualáveis.

Desenvolvido como uma estrutura de trabalho aberta, o DXL permite que todas as soluções de segurança ingressem dinamicamente no ecossistema do McAfee Threat Intelligence Exchange, incluindo produtos de segurança de terceiros.

Adapte-se e imunize-se contra ameaças

Cada insight compartilhado, detectado em qualquer lugar da sua rede, aumenta a profundidade da conscientização na batalha contra ataques direcionados. Como essas ameaças são ataques direcionados com precisão, as empresas precisam de um sistema local de vigilância para capturar as tendências e os ataques únicos que encontrarem. Estes dados contextuais locais reunidos a partir da localização da ameaça e combinados com inteligência global sobre ameaças permitem uma melhor tomada de decisões sobre arquivos nunca vistos antes, resultando em tempos de proteção e detecção menores.

Principais vantagens

- A proteção adaptável contra ameaças reduz o tempo entre a localização e a contenção de ataques direcionados avançados, de dias, semanas e meses para milissegundos
- A inteligência contra ameaças colaborativa é criada a partir de fontes globais de dados de inteligência combinadas com a coleta de dados locais de inteligência contra ameaças
- A inteligência de segurança relevante é compartilhada em tempo real entre endpoints, gateways, redes e soluções de segurança de data center
- Você ganha o poder de tomar decisões sobre arquivos nunca vistos com base no contexto dos endpoints (atributos de ambiente, arquivo e processo), combinado com a inteligência contra ameaças coletiva

Quando um arquivo não identificado é encontrado em qualquer lugar da sua rede, o McAfee Threat Intelligence Exchange é contactado para determinar se há alguma reputação para o arquivo. Metadados descritivos, como idade e organização predominantes, também são mantidos e refletidos na inteligência coletiva. Além de solicitar reputações, as soluções de segurança integradas também podem contribuir com o McAfee Threat Intelligence Exchange com atualizações de reputação baseadas em condenações locais. As reputações atualizadas são então, propagadas para todos os seus sistemas, em tempo real. Esta inteligência local contra ameaças é armazenada para futuros encontros, ou seja, caso a ameaça seja vista novamente em outro dispositivo ou servidor, ela não será mais desconhecida e será detectada imediatamente.

O McAfee Threat Intelligence Exchange possibilita aos administradores personalizar com facilidade a inteligência sobre ameaças. Os administradores de segurança podem montar, sobrepor, complementar e ajustar as abrangentes informações de inteligência, a fim de personalizar a proteção conforme o ambiente e a organização. Estas informações contra ameaças priorizadas localmente e ajustadas fornecem respostas imediatas a quaisquer identificações futuras.

Pontos de imposição melhoram a proteção

Soluções integradas por toda a rede — do endpoint ao perímetro de rede — aplicam a política com base na reputação disponível, nos metadados ou em uma combinação de pontos de dados. O McAfee Endpoint Security, solução fortemente integrada, aproveita a inteligência local combinada (metadados de arquivos, como idade e predomínio organizacional, bem como reputação local oriunda de outros componentes de segurança) e a inteligência global sobre ameaças disponível no momento para tomar decisões precisas. Por exemplo, um aplicativo personalizado sem reputação global, mas com grande predomínio organizacional, não geraria uma reputação composta maliciosa e, provavelmente, teria sua execução permitida. Por outro lado, um arquivo ainda não visto na organização, sem reputação global ou local e compactado de maneira suspeita, muito provavelmente geraria um nível de confiança baixo e daria início a um possível bloqueio ou exigiria uma investigação mais detalhada por mecanismos adicionais do McAfee Endpoint Security ou de área restrita (sandbox) por meio do McAfee Advanced Threat Defense ou do McAfee Cloud Threat Detection.

A capacidade de autoaprendizagem Real Protect do McAfee Endpoint Security e a contenção dinâmica de aplicativos aprimoram ainda mais a detecção e a proteção de endpoints. O Real Protect faz pesquisas na nuvem em busca da inteligência sobre ameaças mais recente, com análise pré e pós-execução, enquanto a contenção dinâmica de aplicativos evita atividades maliciosas no endpoint, protegendo a primeira máquina exposta a uma nova ameaça enquanto análises adicionais são realizadas.

Principais vantagens (continuação)

- A integração é simplificada por meio do DXL. A coordenação das soluções de segurança da McAfee e de terceiros reduz os custos operacionais e de implementação e operacionaliza a sua inteligência contra ameaças em tempo real

Os ataques direcionados avançados são um desafio do mundo real

Desenvolvidos para evitar detecções e estabelecer uma presença duradoura em uma organização, os ataques direcionados avançados continuam atingindo empresas e vazando dados de alto valor. De acordo com dados divulgados recentemente como parte do *Verizon 2015 Data Breach and Investigations Report* (Relatório de investigações de violações de dados de 2015 da Verizon), 70% a 90% das amostras de malware são exclusivas de uma única empresa, indicando que a detecção de indicadores de ameaças únicas é o maior desafio da atualidade.[1]

Para obter mais informações, visite **www.mcafee.com/br/products/threat-intelligence-exchange.aspx**.

Beneficie-se da colaboração

Análise de ameaças avançadas

Caso sejam necessárias mais informações sobre um arquivo, o McAfee Threat Intelligence Exchange pode enviá-las automaticamente para soluções de análise avançada da McAfee — como McAfee Advanced Threat Defense ou McAfee Cloud Threat Detection — a fim de obter imediatamente insights adicionais sobre novas ameaças potenciais e determinar a reputação do arquivo em questão. Tudo isso é automatizado, documentado e compartilhado coletivamente via DXL para proteger todo o seu ecossistema de segurança.

Gerenciamento de eventos de segurança

O McAfee Enterprise Security Manager permite examinar mais profundamente quando indicadores de comprometimento (IoCs) são identificados pelo McAfee Threat Intelligence Exchange. O acesso a informações de segurança passadas e a capacidade de criar listas de observação automatizadas aumentam a eficiência da segurança para as empresas.

1. http://www.verizonenterprise.com/DBIR/2015/

McAfee
Together is power.

Av. Nações Unidas, 8.501 – 16º andar
Pinheiros – São Paulo – SP
CEP 05425-070, Brasil
+(11) 3711-8200
www.mcafee.com/br

McAfee e o logotipo da McAfee são marcas comerciais ou marcas registradas da McAfee, LLC ou de suas afiliadas nos EUA e em outros países. Outros nomes e marcas podem ser propriedade de terceiros. Copyright © 2017 McAfee, LLC. 3059_0517
MAIO/2017