DATA SHEET

McAfee Global Threat Intelligence for Enterprise Security Manager

Leve o poder do McAfee® Labs para a percepção situacional.

O McAfee® Global Threat Intelligence for Enterprise Security Manager leva o poder do McAfee Labs para o monitoramento da segurança corporativa. Pela primeira vez, reputações de IPs, coletadas pelo McAfee Labs em mais de 100 milhões de sensores de ameaças globais, são disponibilizadas para uma solução de gerenciamento de eventos e informações de segurança (SIEM). Esse canal rico e constantemente atualizado para o McAfee Enterprise Security Manager aumenta a percepção situacional ao viabilizar uma descoberta rápida de eventos que envolvem comunicações com IPs suspeitos ou maliciosos. Isso permite aos administradores de segurança determinar quais hosts se comunicaram ou estão se comunicando atualmente com malfeitores, bem como identificar rapidamente condições nas quais um malfeitor conhecido foi a origem de uma atividade de ameaça.

A necessidade de contexto externo

Os eventos de segurança proporcionam informações sobre atividades relacionadas à segurança com base em um momento específico no tempo. Embora o SIEM tenha a capacidade de correlacionar esses eventos, restam ainda várias questões para o operador resolver: A atividade é aceitável? Como saber o que é mais urgente? Como detectar ataques sofisticados que não fazem muito barulho? Multipliquemos essas questões pelos eventos diários de uma corporação típica (que chegam a mais de um quarto de bilhão) e veremos claramente que a detecção de padrões conhecidos, na qual se concentram os SIEM tradicionais, é apenas a ponta do iceberg do monitoramento de segurança. Um dos elementos contextuais mais importantes por trás dessa incógnita é compreender a reputação dos sistemas externos. Até recentemente, ter essa compreensão clara dos eventos de segurança era impossível.

Leve o poder do McAfee Labs para o SIEM

O McAfee Global Threat Intelligence for Enterprise Security Manager coloca o poder do McAfee Labs diretamente no fluxo de monitoramento de segurança por meio do SIEM de alta velocidade e elevada inteligência da

Principais vantagens

- Leve o poder do McAfee Labs para o SIEM
- Entenda de maneira precisa os riscos associados aos eventos
- Aproveite o massivo canal de ameaças do McAfee GTI sem prejudicar o desempenho
- Receba e processe automaticamente novas reputações de origem no McAfee Enterprise Security Manager
- Aumente a precisão da detecção de ameaças e reduza o tempo de resposta
- Identifique rapidamente os caminhos de ataques e interações anteriores com malfeitores conhecidos associados a redes de bots, ataques de negação de serviços distribuída (DDoS), malware de envio de e-mail e spam hospedando sondagem de rede, presença de malware, hospedagem de DNS e atividade gerada por ataques de intrusão

McAfee, desenvolvido para grandes volumes de dados de segurança. Esse serviço de assinatura opcional fornece e ajusta continuamente reputações de fontes de mais de 140 milhões de endereços IP, levando o contexto de reputações de sistemas externos diretamente para o fluxo de eventos de segurança e identificando rapidamente interações atuais e anteriores com notórios malfeitores. A reputação de IP do McAfee Global Threat Intelligence (GTI) é derivada da correlação de inteligência sobre ameaças de todos os principais vetores de ameaças, aproveitando mais de 100 milhões de sensores globais e mais de 500 pesquisadores.

Vantagens do McAfee Global Threat Intelligence for Enterprise Security Manager

- **Mais proteção para toda a rede:** o McAfee Global Threat Intelligence for Enterprise Security Manager detecta imediatamente quando qualquer nó da rede está se comunicando com um indivíduo suspeito ou um malfeitor conhecido e determina rapidamente o caminho da ameaça.
- **Priorização com base no risco:** a reputação do IP é incorporada automaticamente ao algoritmo de pontuação de risco sem regras do McAfee Enterprise Security Manager, identificando automaticamente a necessidade de responder.
- **Monitoramento de ameaças, 24 horas por dia, sete dias por semana:** o McAfee Labs está sempre analisando informações sobre ameaças para detectar sistemas maliciosos e recém-infectados (e determinar quando esses sistemas foram limpos), proporcionado às organizações uma compreensão precisa e atualizada do cenário global de ameaças.

Identifique atividade maliciosa em tempo real

Com o McAfee Global Threat Intelligence for Enterprise Security Manager, as organizações agora têm o poder de compreender a reputação de IP de qualquer evento, incluindo firewalls heterogêneos, sistemas de prevenção de intrusões, roteadores e endpoints. Com a capacidade de lista de observação dinâmica do McAfee Enterprise Security Manager, os eventos são associados automaticamente ao índice de reputação da fonte e o risco é ajustado. Conforme as ameaças globais mudam, o McAfee GTI mantém atualizado o McAfee Enterprise Security Manager, garantindo que servidores e sistemas tenham sempre um índice de reputação exato. Isso não apenas ajuda as organizações a compreender o risco, como também identifica problemas urgentes em tempo real, reduzindo a janela do tempo de resposta ao incidente e proporcionando uma análise de risco precisa.

Descubra o que você não sabia

Um ponto forte do McAfee Enterprise Security Manager é sua capacidade de armazenar, recuperar e realizar correlação histórica em dados coletados ao longo de anos. Agora, com o McAfee GTI, os analistas de segurança podem voltar no tempo e analisar dados de anos a fio para compreender interações com malfeitores ocorridas no passado. Isso é fundamental para a detecção de ataques lentos e discretos, atividades repetidas de redes de bots, XSS (Cross-Site Scripting) e tentativas de injeção de SQL.

Redução do tempo de resposta

O McAfee GTI integra-se perfeitamente com os mecanismos de alarme e de alerta do McAfee Enterprise Security Manager, assegurando que as interações com sistemas maliciosos conhecidos recebam a devida atenção.

Apoiado pelo banco de dados da McAfee, criado para grandes volumes de dados de segurança

Fala-se muito no crescimento dos volumes de dados e isso inclui levar o amplo conhecimento do McAfee Labs relacionado à segurança para o SIEM. O McAfee Enterprise Security Manager é único em sua capacidade de armazenar, correlacionar e atualizar a enorme quantidade de dados de reputação de IP do McAfee GTI IP sem uma degradação inaceitável do desempenho.

O McAfee Enterprise Security Manager conta com um banco de dados próprio que, além de eliminar o tempo despendido na administração do banco de dados para o SIEM, também foi criado especificamente para a enorme assimilação e processamento de dados de eventos e relacionais a velocidades extremamente elevadas. Com o McAfee Global Threat Intelligence for Enterprise Security Manager, os usuários têm a confiança de que o conhecimento do McAfee GTI será fornecido em tempo real.

Especificações

Versões compatíveis
McAfee Enterprise Security Manager 9.4 e McAfee Event Reporter Appliance 9.4

- Rede de inteligência sobre ameaças do McAfee Labs: mais de 100 milhões de nós em mais de 120 países
- Reputações médias de IP: variam com base no cenário de ameaças

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

SETEMBRO DE 2014