Resumo da solução

Operacionalizando a Inteligência de Ameaças

Por trás de basicamente todo alerta legítimo recebido pela sua equipe de segurança da informação, está um adversário usando múltiplas técnicas de ataque para penetrar em sua infraestrutura e comprometer seus recursos ou sistemas de dados vitais. Os ataques multifase direcionados de hoje consistem em uma série de etapas que compõem uma cadeia de ataques cibernéticos: reconhecimento, varredura por vulnerabilidades, exploração e, finalmente, exfiltração de dados corporativos valiosos.

Os analistas de segurança estão cientes dessas técnicas e dependem da inteligência de ameaças para coletar informações sobre os métodos e as motivações de ataque. Eles podem detectar e interromper ameaças avançadas, aplicar correção adequada e estar mais bem preparados na próxima vez em que soar o alarme de segurança. Mas, muitas vezes, eles carecem de visibilidade a certos sistemas ou são inundados com dados demais e inteligência de menos. De acordo com o estudo do SANS Institute *Who's Using Cyberthreat Intelligence and How?* (Quem está usando a inteligência de ameaças cibernéticas e como?), "… apenas 11,9% dos entrevistados conseguiram a habilidade de agregar informações de ameaças de virtualmente todas as fontes e somente 8,8% têm a imagem total que pode combinar eventos com IoCs.[1]"

Em um relatório recente, a Forrester observa que 77% dos tomadores de decisão empresarial da América do Norte e Europa relatam que melhorar os recursos de inteligência de ameaças é uma prioridade [2]. A inteligência de ameaças cibernéticas promete fornecer aos profissionais de segurança um aviso antecipado sobre criminosos cibernéticos que estejam visando suas regiões, setores ou até mesmo empresas específicas, para que eles tenham tempo de entrar em ação, mas a segurança de TI ainda enfrenta alguns grandes desafios:

- Como coletar inteligência de ameaças de fontes externas, além das internas.
- Como correlacionar os dados e priorizar riscos.
- Como distribuir inteligência entre controles de segurança de múltiplos fornecedores em toda a empresa.
- Como obter mais visibilidade do panorama de TI para permitir uma ação rápida e adequada.

As empresas modernas precisam de uma arquitetura aberta e integrada que facilite a adoção de inteligência de ameaças e permita que elas colham os benefícios dessa inteligência – de coleta de dados de ameaças básicos para análise forense ao uso da inteligência para enriquecer a análise SIEM. Em outras palavras, os usuários precisam fazer com que a inteligência de ameaças funcione por meio de processos automatizados que ajudem a analisá-la, digeri-la e gerenciá-la.

intel Security

Novas ameaças pedem nova abordagem de inteligência de ameaças

À medida que os ataques crescem em complexidade, precisão e volume, a abordagem de ontem empregada à inteligência de ameaças não é mais adequada. A investigação de ataques direcionados não é uma tarefa fácil. O comportamento dinâmico dos atacantes, a maior variedade e disponibilidade de fontes de inteligência de ameaças locais e globais e a diversidade dos formatos de dados de inteligência de ameaças podem tornar a agregação e a digestão de inteligência de ameaças em ferramentas de centros de operações de segurança (SOC) mais desafiadoras do que nunca.

Um ambiente de fornecedores mistos, comum na maioria das empresas, aumenta a dificuldade de compartilhar dados de eventos e promover visibilidade de eventos em toda a organização. Como apontado pelo Gartner em seu relatório: *Technology Overview for Threat Intelligence Platforms (Visão geral tecnológica das plataformas de inteligência de ameaças)*, "A incapacidade de uma organização de compartilhar inteligência de ameaças é uma vantagem para os agentes de ameaças cibernéticas. O compartilhamento de inteligência de ameaças é um multiplicador de forças e está se tornando um elemento essencial para conseguir acompanhar o número crescente de agentes de ameaça e os ataques utilizados por eles."[3]

Mas somente compartilhar inteligência de ameaças não necessariamente resultará em prevenção e ações corretivas sustentáveis. Os analistas de segurança podem ficar rapidamente sobrecarregados com o excesso de informações. A maioria das equipes de segurança está envolvida em um exaustivo processo manual (veja a Figura 1) de analisar milhões de eventos de segurança e arquivos suspeitos em um esforço para juntar uma enorme quantidade de dados e tentar reconstruir o ataque direcionado. No fim das contas, isso prejudica a minuciosidade e a rapidez do processo de resposta. Com uma compreensão incompleta das ameaças, as equipes de segurança têm problemas para conter ataques em tempo hábil. De acordo com um estudo recente, da Intel Security: *When Minutes Count (Quando os minutos contam – 2014)*, menos de 25% dos participantes declararam que conseguiriam detectar um ataque em poucos minutos[4].

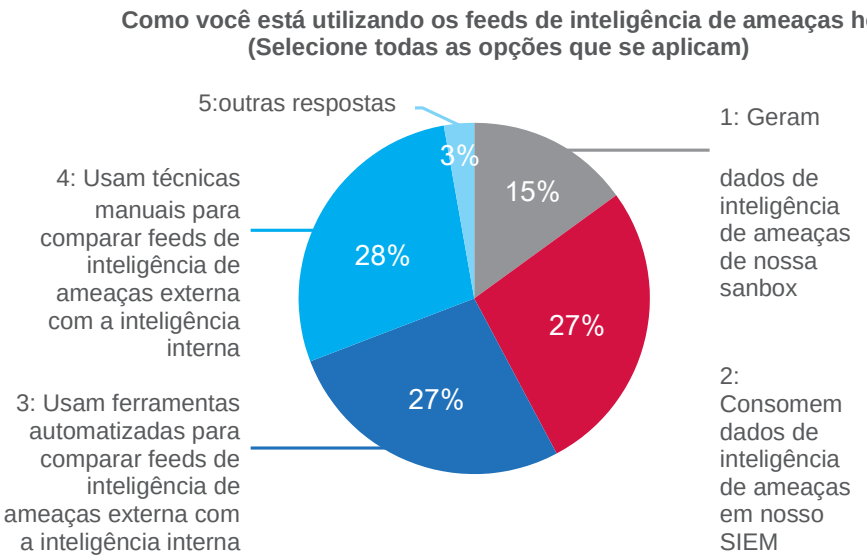

Figura 1. De acordo com uma pesquisa da Intel Security conduzida na BlackHat 2015, um grande grupo de usuários ainda emprega técnicas manuais para comparar feeds de inteligência de ameaças externa com a inteligência de ameaças interna.

"Para nossa infraestrutura de segurança, precisávamos muito mais do que um fornecedor de tecnologia. Foi absolutamente essencial desenvolver uma relação com um parceiro que pudesse nos ajudar a gerenciar nosso diversificado conjunto de requisitos de clientes e uma situação de ameaças em constante evolução.

A McAfee oferece essa parceria e, além disso, a inteligência de segurança contínua que recebemos das soluções McAfee é crucial para nos ajudar a manter nossas operações de negócios na vanguarda."

– Anurana Saluja
CISO e VP de Segurança da Informação, Sutherland Global Services

Operacionalize a inteligência de ameaças

A detecção e a correção de ameaças com base em inteligência requerem muito mais do que a importação manual de endereços de IP de adversários publicados em um site aberto para uma tabela de lista de observação de SIEM uma vez por semana. Em vez disso, é necessária a ingestão de inteligência de ameaças em tempo real e a correlação de todas as facetas de um ataque, incluindo métodos e campanhas globais, para que as empresas possam prever até mesmo as ameaças mais indetectáveis e com a maior capacidade de adaptação. Os SOCs empresariais precisam ter uma maneira de "operacionalizar a inteligência de ameaças" para obter uma visão total dos ataques que afetam seus ambientes. Eles precisam ter um meio de filtrar

as enormes quantidades de dados para analisar, correlacionar e priorizar a inteligência de ameaças e determinar o que é relevante para o setor, região e empresa. E precisam ser capazes de obter informações sobre ataques únicos que possam estar ocorrendo no presente, além de informações sobre tendências com base em dados de eventos de segurança históricos. Como apontado pela Forrester, a operacionalização da inteligência de ameaças é essencial, pois 75% dos ataques se propagam de uma vítima para a outra dentro de 24 horas. As empresas precisam fechar a lacuna entre "velocidade de compartilhamento e velocidade dos ataques"[5].

Aproveite a arquitetura integrada da Intel Security

A Intel Security oferece uma plataforma unificada e colaborativa com todos os componentes necessários para operacionalizar a inteligência de ameaças, incluindo feeds de inteligência de ameaças globais, criação de inteligência local, compartilhamento em tempo real de informações de ameaças entre a infraestrutura de TI, informações de segurança e gerenciamento de eventos, além de fornecimento de proteção automatizada e adaptativa.

Requisitos de inteligência de ameaças	McAfee® Threat Intelligence Exchange	McAfee Advanced Threat Defense	McAfee Enterprise Security Manager	McAfee Global Threat Intelligence
Coleta inteligência de ameaças de fontes externas	STIX, importação de McAfee Global Threat Intelligence (McAfee GTi) e VirusTotal	Importação de McAfee GTI, TAXII/STIX	Importação de McAfee e feeds de ameaças em HTTP por meio do gerenciador de ameaças cibernéticas McAfee Enterprise Security Manager	O McAfee GTI agrega inteligência de ameaças de múltiplos parceiros da aliança de ameaças cibernéticas e fontes públicas. O McAfee GTI extrai inteligência de ameaças de milhões de sensores em produtos Intel Security implementados por clientes tais como endpoint, web, e-mail, Sistemas de prevenção contra intrusão de rede (IPS) e dispositivos de firewall
Coleta inteligência de ameaças interna	Coleta amostras de McAfee VirusScan®, McAfee Application Control, McAfee Web Gateway, McAfee Advanced Threat Defense, McAfee Enterprise Security Manager e de produtos de terceiros que enviam informações para o McAfee Data Exchange Layer	Consume arquivos de amostra para detonação pelo McAfee Threat Intelligence Exchange ou pela rede	Por meio de STIX/TAXII e McAfee Data Exchange Layer	
Produz inteligência de ameaças local	Registra incidentes de arquivos suspeitos e cria um banco de dados local que registra o primeiro contato e a trajetória das ameaças	Disseca e condena malwares, gera inteligência de ameaças local e distribui pelo McAfee Data Exchange Layer ou como API formatada em STIX	Cria listas de observação de inteligência de ameaças, relatórios e visualizações baseadas em eventos correlacionados	
Distribui inteligência de ameaças entre controles de segurança	Por meio do McAfee Data Exchange Layer	Por meio de McAfee Data Exchange Layer e API de produto	Por meio de McAfee Data Exchange Layer, API de produto e integração de scripts	O McAfee GTI é integrado com vários produtos Intel Security, como McAfee Web Gateway, McAfee Enterprise Security Manager e soluções de endpoint McAfee
Oferece visibilidade à inteligência de ameaças coletada	Por meio de dashboards do McAfee Threat Intelligence Exchange	Por meio de relatórios	Por meio de dashboards, exibições e relatórios fornecidos em pacotes de conteúdo ou gerados pelo cliente	Por meio de dashboards do McAfee Threat Center e relatórios de ameaças McAfee trimestrais

Tabela 1. Plataforma de inteligência de ameaças integrada da Intel Security

Consumir, analisar e distribuir

McAfee Global Threat Intelligence

Um bom lugar para começar a desenvolver sua plataforma integrada de inteligência de ameaças é o McAfee Global Threat Intelligence (McAfee GTI), serviço de reputação abrangente, em tempo real e com base em nuvem totalmente integrado aos produtos Intel Security que permite que esses produtos bloqueiem melhor as ameaças cibernéticas em todos os vetores – arquivo, web, mensagem e rede – rapidamente. O McAfee GTI fornece pontuações de reputação para bilhões de arquivos, URLs, domínios e endereços de IP de acordo com dados coletados de múltiplas fontes: milhões de sensores globais monitorados e analisados pela McAfee Labs, feeds de ameaças de parceiros de pesquisa e por meio da Cyber Threat Alliance, além da inteligência de múltiplos vetores de dados de ameaças da web, e-mail e rede. Apoiado por feeds de ameaças relevantes e de alta qualidade, o McAfee GTI oferece um aconselhamento de riscos preciso, que estimula a tomada de decisões de política embasadas e possibilita que os controles bloqueiem, limpem e permitam, conforme necessário.

McAfee Enterprise Security Manager

O McAfee Enterprise Security Manager (SIEM) leva o consumo e a análise de inteligência de ameaças a outro nível, fornecendo uma central de consolidação, análise e ação para cada tipo de inteligência de ameaça. Essa visão em 360 graus possibilita uma visibilidade total e uma percepção situacional completa para acelerar a detecção e a resposta a ataques direcionados. Seu sistema de gerenciamento de dados avançado é feito sob medida para armazenar e assimilar grandes volumes de dados contextuais em tempo real.

O McAfee Enterprise Security Manager coleta dados de atividades e eventos de todos os seus sistemas, bancos de dados, redes e aplicativos. Ele também importa feeds de ameaças globais e consome inteligência de ameaças em formatos padrão e transporta, como Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII) e Cybox, normalmente publicados pela comunidade ou grupos do setor como o Financial Services Information Sharing and Analysis Center (FS-ISAC). Por meio de análises avançadas, ele traduz as informações coletadas em inteligência de segurança compreensível e utilizável. De forma mais significativa, ele fornece uma visibilidade mais profunda a ameaças emergentes por meio de exibições em tempo real e acesso a informações de segurança históricas. Isso permite que você investigue retroativamente para entender o predomínio e os padrões de um ataque e também para criar listas de observação automatizadas para detectar a ocorrência ou reocorrência de eventos no futuro. Ao enriquecer a sensibilidade do seu sistema a eventos conhecidos como maliciosos, você aumenta a sua capacidade de detectar atividades e padrões de atividade suspeitos em diversas fases da cadeia de ataque e, então, prioriza a resposta.

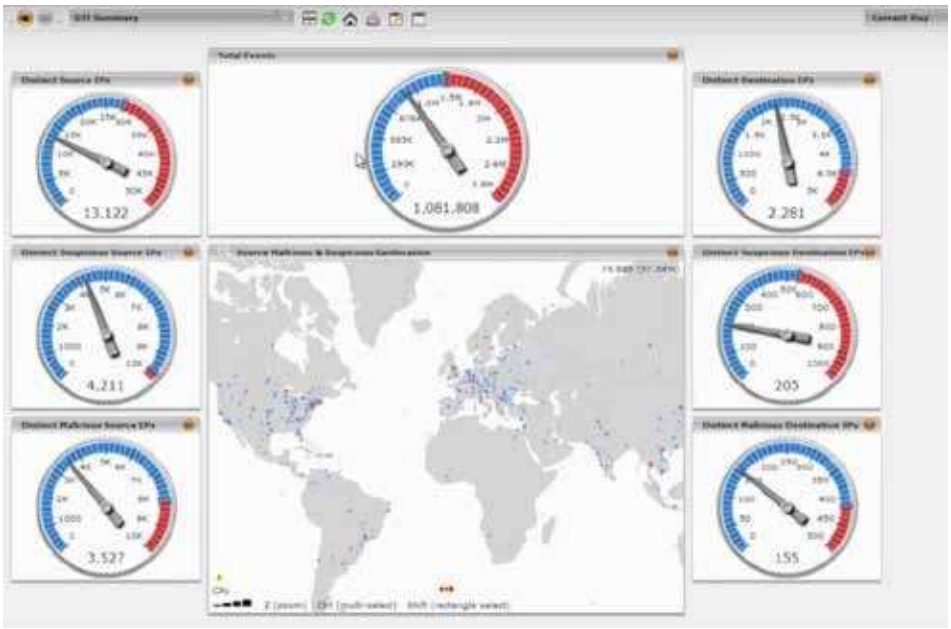

Figura 2. Visualização do McAfee GTI.

O que é a Cyber Threat Alliance?

A **Cyber Threat Alliance** é um grupo de profissionais de segurança de organizações que trabalham juntos para compartilhar informações de ameaças e ajudar a melhorar as defesas contra adversários entre as organizações-membro e seus clientes. A Intel Security está entre os membros fundadores que dedicaram seus recursos para determinar as formas mais eficazes de compartilhar dados de ameaças, estimular colaboração entre membros e progredir de forma unificada na luta contra criminosos cibernéticos sofisticados.

O McAfee GTI para McAfee Enterprise Security Manager leva o poder dos recursos de pesquisa da McAfee Labs para o monitoramento de segurança empresarial. Esse feed rico, e em constante atualização do McAfee GTI, aprimora a percepção situacional possibilitando a rápida descoberta de eventos que envolvam comunicações com IPs suspeitos ou maliciosos e permite que os administradores de segurança determinem quais hosts empresariais se comunicaram ou estão se comunicando no momento com agentes nocivos.

McAfee Threat Intelligence Exchange

O terceiro componente que você pode adicionar à medida que desenvolve um ecossistema integrado de inteligência de ameaças é o McAfee Threat Intelligence Exchange, que agrega e compartilha inteligência de reputação de arquivos entre toda a infraestrutura de segurança. O McAfee Threat Intelligence Exchange recebe informações de ameaças do McAfee GTI, arquivos de importação STIX, feeds de ameaças provenientes do McAfee Enterprise Security Manager e informações provenientes de endpoint, controle de aplicativo, dispositivos móveis, gateway, data centers e tecnologias de sandbox das soluções da Intel Security e das soluções de outros fornecedores.

A coleta de dados de todos os pontos em sua infraestrutura oferece informações sobre ameaças que podem estar presentes somente no seu ambiente, como muitos ataques direcionados tendem a ser. Por sua vez, as informações de reputação de arquivos são compartilhadas instantaneamente entre todo o ecossistema para todos os produtos e soluções conectados ao McAfee Threat Intelligence Exchange por meio do McAfee Data Exchange Layer. Por exemplo, se o McAfee Threat Intelligence Exchange enviar informações sobre um arquivo executável malicioso, o McAfee Data Loss Prevention recebe essas informações pelo McAfee Data Exchange Layer e, em seguida, começa a monitorar esse executável em busca de acesso a arquivos confidenciais.

Os dados de ameaça compartilhados pelo McAfee Data Exchange Layer incluem reputações de arquivos, classificações de dados, integridade de aplicativos e dados de contexto de usuários, que são compartilhados com e entre produtos integrados à malha do McAfee Data Exchange Layer. Qualquer produto ou solução pode ser integrado ao McAfee Data Exchange Layer e, em seguida, configurado para determinar quais informações devem ser publicadas ao sistema e quais informações devem ser monitoradas e assinadas.

O McAfee Threat Intelligence Exchange trabalha em estreita colaboração com a solução de sandbox avançada da Intel Security, o McAfee Advanced Threat Defense, que envia dados de análise de malwares para o McAfee Threat Intelligence Exchange. Se um arquivo for considerado malicioso, o McAfee Threat Intelligence envia uma atualização de reputação de arquivo para todos os sistemas conectados pelo McAfee Data Exchange Layer. Isso também funciona no sentido contrário. Quando endpoints habilitados pelo McAfee Threat Intelligence Services encontram arquivos com reputação desconhecida, eles podem ser enviados ao McAfee Advanced Threat Defense para determinar se o objeto é malicioso, eliminando pontos cegos da entrega de cargas fora de banda. Esses dois produtos trabalham juntos para oferecer proteção automatizada e adaptativa contra ameaças emergentes. As informações sobre ataques descobertos são entregues para todo o seu ambiente para ajudar a bloquear a cadeia de ataques cibernéticos antes que mais danos sejam causados.

Figura 3. Dashboard do McAfee Threat Intelligence Exchange.

O McAfee Threat Intelligence Exchange possibilita que haja detecção e resposta adaptativas a ameaças ao operacionalizar a inteligência em suas soluções de segurança de endpoint, gateway, rede e data center em tempo real. Combinando informações de ameaças globais importadas com inteligência coletada localmente e compartilhando-a instantaneamente, ele permite que as suas soluções de segurança operem como uma só, trocando e agindo de acordo com a inteligência compartilhada.

Interrompa a cadeia de ataques cibernéticos

Independentemente de onde ocorra o primeiro ponto de contato de um arquivo malware, uma vez condenado, todo o ambiente conectado é atualizado imediatamente. Quando um arquivo é condenado pelo McAfee Advanced Threat Defense, o McAfee Threat Intelligence Exchange publicará essa condenação por meio de uma atualização de reputação, que é disseminada pelo McAfee Data Exchange Layer para todos os controles de segurança em sua organização. Os gateways habilitados pelo McAfee Threat Intelligence Exchange impedem que o arquivo entre em sua infraestrutura. Por meio de compartilhamento coordenado da inteligência de ameaças entre todos os seus controles de segurança, torna-se mais fácil interromper a cadeia de ataque e impedir danos adicionais sem necessidade de intervenção manual.

Consumir e aplicar: detectar com precisão e tomar melhores decisões

Após os dados serem consumidos, o McAfee Enterprise Security Manager age como ponto central de visibilidade, correlacionando o McAfee GTI, os feeds do McAfee Threat Intelligence Exchange e indicadores de comprometimento (IoCs) formatados em STIX/TAXII com dados do evento, detectados em tempo real ou historicamente quando nós na sua rede estão se comunicando com agentes nocivos conhecidos ou domínios suspeitos.

O dashboard de gerenciamento de ameaças oferece aos analistas uma visão única e abrangente dos indicadores de ameaça coletados, dos feeds de origem, da taxa de ocorrências contra os indicadores e dos detalhes mais significativos legíveis por humanos sobre indicadores de comprometimento (IoCs).

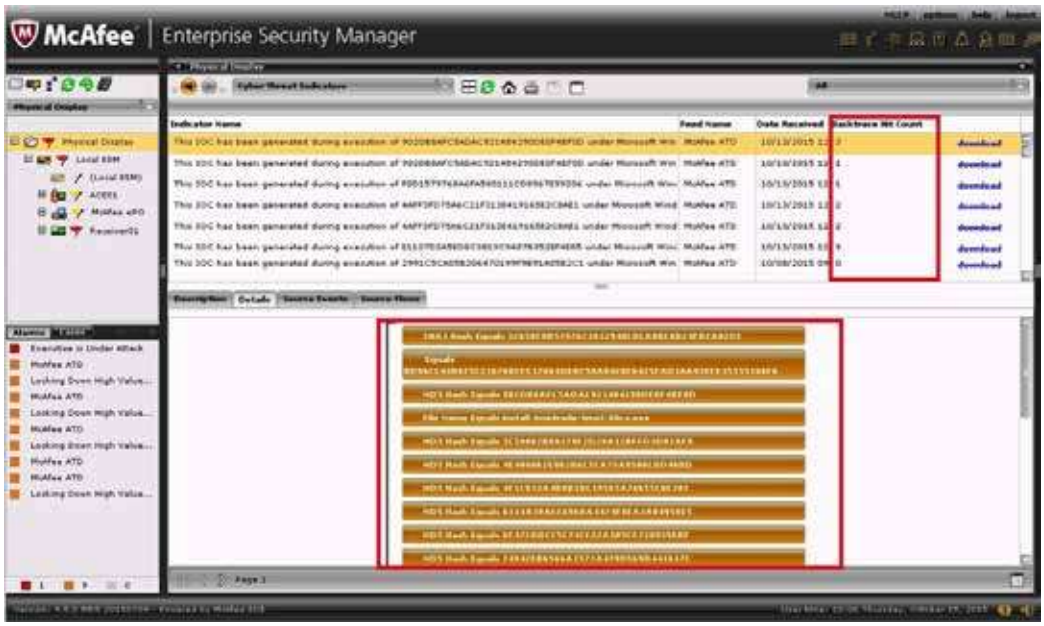

Figura 4. Detalhes de indicadores de ameaças cibernéticas, ocorrências históricas e IoCs do McAfee Enterprise Security Manager.

O uso do McAfee Enterprise Security Manager (SIEM) junto com outras ferramentas colaborativas de inteligência de ameaças resulta em menos gastos operacionais associados à configuração de regras de correlação, que normalmente é um processo manual complexo. Por exemplo, os analistas de segurança podem revisar diretamente as informações de ameaças recém-recebidas em formato legível por humanos, possibilitando maior entendimento de novas ameaças detectadas. E, mais importante, a inteligência de ameaças recebida pode ser adotada automaticamente por regras de correlação em tempo real ou históricas, reduzindo assim o tempo para detectar atividades novas ou contínuas de atacantes. Os usuários também podem acompanhar o progresso de ameaças relatadas ao longo de todo o ambiente de TI, além de por meio de informações contextuais em visualizações de alarmes, permitir tomar melhores e mais bem embasadas decisões. Toda essa inteligência coletada aprimora e acelera a detecção e a investigação de ataques direcionados. Como as ameaças abrem caminho rapidamente através da infraestrutura de TI e são projetadas para mudar ao longo do tempo, o McAfee Enterprise Security Manager pode atualizar periodicamente toda a inteligência de ameaças adquirida, eliminando dados antigos e menos relevantes. Por exemplo, servidores de comando e controle removidos ou sites limpos com pontuações de reputação maliciosa menores são automaticamente liberados para eliminar falsos positivos que possam distrair sua equipe de segurança e impedir que ela vá atrás das ameaças reais.

Os seguintes produtos da Intel Security dão suporte a inteligência de ameaças formatada em STIX:

- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Detection
- McAfee Enterprise Security Manager

Resumo

A inteligência de ameaças integrada da Intel Security operacionaliza o consumo e o gerenciamento da inteligência de ameaças, permitindo que você aumente a precisão da detecção de ameaças, elimine esforços manuais e impeça que adversários prejudiquem seus negócios. Com maior visibilidade e informações aprimoradas sobre atividades maliciosas em todo o seu ecossistema de segurança, você está mais bem preparado para identificar e impedir ataques direcionados hoje e prevenir que ocorram no futuro.

Saiba mais

Para obter mais informações sobre os alicerces da plataforma de inteligência de ameaças integrada da Intel Security, acesse:

- **McAfee Global Threat Intelligence**
- **McAfee Threat Intelligence Exchange**
- **McAfee Advanced Threat Defense**
- **McAfee Enterprise Security Manager**
- **Como usar feed TAXII com o McAfee Enterprise Security Manager**

1. **https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767**
2. **https://www.forrester.com/The+State+Of+The+Cyberthreat+Intelligence+Market/fulltext/-/E-RES123011**
3. **https://www.gartner.com/doc/2941522/technology-overview-threat-intelligence-platforms**
4. **http://www.mcafee.com/us/resources/reports/rp-when-minutes-count.pdf**
5. **https://www.rsaconference.com/writable/presentations/file_upload/cxo-t08r-threat-intelligence-is-like-three-day-potty-training.pdf**

McAfee. Parte da Intel Security. 2821 Mission College Boulevard Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com