Operacionalização da inteligência contra ameaças

Por trás de cada alerta legítimo recebido pela sua segurança de TI há um adversário utilizando múltiplas técnicas de ataque para penetrar a sua infraestrutura e comprometer seus sistemas ou ativos de dados vitais. Os atuais ataques de múltiplas fases consistem em uma série de etapas que compõem a cadeia de ataque cibernético: reconhecimento, varredura de vulnerabilidades, exploração e, finalmente, vazamento de dados corporativos valiosos.

Os analistas de segurança estão cientes dessas técnicas e dependem de inteligência contra ameaças para obter insights dos métodos de ataque e suas motivações. Eles podem detectar e interromper ameaças avançadas, aplicar as correções apropriadas e estar mais bem preparados na próxima vez que soar o alarme da segurança. No entanto, frequentemente lhes falta visibilidade sobre determinados sistemas ou eles são inundados com dados demais e inteligência de menos. Segundo o estudo *Who's Using Cyberthreat Intelligence and How?* (Quem está usando inteligência contra ameaças cibernéticas e como?), do SANS Institute, "somente 11,9% dos entrevistados atingiram a capacidade de agregar informações sobre ameaças de praticamente qualquer fonte, e apenas 8,8% têm uma visão completa capaz de associar eventos a IoCs".[1]

Em um relatório recente, a Forrester observa que 77% dos tomadores de decisões de segurança corporativa norte-americanos e europeus afirmam que aprimorar capacidades de inteligência contra ameaças cibernéticas é uma prioridade.[2] A inteligência contra ameaças cibernéticas promete dar aos profissionais de segurança avisos antecipados sobre criminosos cibernéticos que visam sua região, setor ou mesmo empresas específicas, para que eles tenham tempo para tomar providências, mas a segurança de TI ainda enfrenta grandes desafios:

- Como coletar inteligência contra ameaças de fontes externas e internas.
- Como correlacionar os dados e priorizar os riscos.
- Como distribuir inteligência por controles de segurança de diversos fornecedores espalhados pela empresa.
- Como obter melhor visibilidade sobre o cenário de TI de maneira a permitir ações rápidas e apropriadas.

As corporações modernas precisam de uma arquitetura aberta e integrada que facilite a adoção de inteligência contra ameaças e que as permita aproveitar suas vantagens — desde uma simples coleta de dados sobre ameaças para análise forense até sua utilização para enriquecer análises de SIEM. Em outras palavras, os usuários precisam colocar a inteligência contra ameaças para trabalhar através de processos automatizados que ajudem a analisar, digerir e gerenciar as informações.

Novas ameaças exigem uma nova abordagem à inteligência contra ameaças

Conforme os ataques crescem em complexidade, precisão e volume, as antigas abordagens à inteligência contra ameaças tornam-se inadequadas. A investigação de ataques direcionados não é uma tarefa fácil. O comportamento dinâmico dos atacantes, a maior variedade e disponibilidade de fontes de inteligência contra ameaças locais e globais e a diversidade de formatos de dados de inteligência contra ameaças podem tornar a agregação e o processamento dessa inteligência em ferramentas de centro de operações de segurança (SOC) algo mais desafiador do que nunca.

Um ambiente de vários fornecedores, típico da maioria das empresas, aumenta a dificuldade do compartilhamento de dados de eventos e a promoção da visibilidade sobre os eventos por toda a organização. Como a Gartner ressalta em seu relatório *Technology Overview for Threat Intelligence Platforms* (Visão geral de tecnologia para plataformas de inteligência contra ameaças), "A incapacidade de uma organização de compartilhar TI é uma vantagem para os perpetradores de ameaças cibernéticas. O compartilhamento de TI é um multiplicador de forças e está se tornando um elemento fundamental para nos mantermos à altura do número crescente de perpetradores de ameaças e dos ataques que eles utilizam".[3]

Contudo, apenas o compartilhamento de inteligência contra ameaças não resulta, necessariamente, em prevenção e ações corretivas sustentáveis.

"Para nossa infraestrutura de segurança, precisamos de muito mais que um fornecedor de tecnologia. Era absolutamente essencial que construíssemos um relacionamento com um parceiro que pudesse nos ajudar a gerenciar nosso amplo leque de requisitos de clientes e uma situação de ameaças em constante evolução. A McAfee oferece essa parceria. A inteligência de segurança contínua que recebemos das soluções da McAfee é fundamental para nos ajudar a otimizar nossas operações de negócios."

— Anurana Saluja
CISO e vice-presidente de segurança da informação
Sutherland Global Services

Os analistas de segurança podem ficar rapidamente sobrecarregados com excesso de informação. A maioria das equipes de segurança está envolvida em um processo manual exaustivo (veja a figura 1) de analisar milhões de eventos de segurança e arquivos suspeitos, com o objetivo de juntar os pedaços de uma montanha de dados e tentar reconstruir o ataque direcionado. Em última instância, isso prejudica a abrangência e a velocidade do processo de resposta. Com uma compreensão incompleta das ameaças, as equipes lutam com dificuldade para conter os ataques em tempo hábil. De acordo com um estudo recente da Intel Security (atual McAfee) chamado *Quando os minutos contam*, de 2014, menos de 25% dos entrevistados afirmaram poder detectar um ataque em questão de minutos.[4]

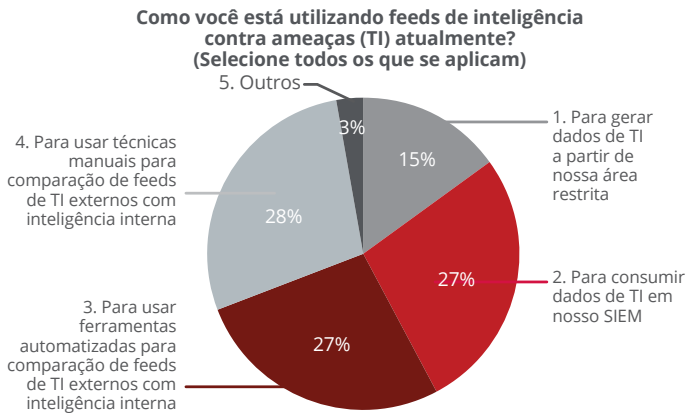

Figura 1. Segundo uma pesquisa da Intel Security (atual McAfee) realizada na BlackHat 2015, um grande contingente de usuários ainda emprega técnicas manuais para comparar feeds externos de inteligência contra ameaças com a inteligência interna contra ameaças.

Operacionalize a inteligência contra ameaças

A detecção de ameaças orientada por inteligência e sua subsequente correção exigem mais do que apenas importar manualmente endereços IP nocivos publicados em um site aberto e incluí-los em uma tabela de observação do SIEM uma vez por semana. São necessárias assimilação de inteligência contra ameaças em tempo real e correlação de todas as facetas de um ataque, incluindo métodos e campanhas globais, para que todas as empresas possam se antecipar até mesmo aos ataques mais furtivos e mais rapidamente adaptáveis. Os SOCs corporativos precisam de uma maneira de "operacionalizar a inteligência contra ameaças" para ter uma visão completa dos ataques que afetam seus ambientes. Eles precisam de uma maneira de examinar minuciosamente esse imenso volume de dados para analisar, correlacionar e priorizar a inteligência contra ameaças e determinar o que é relevante para seu ramo de atividade, sua geografia e sua empresa. Eles também precisam ser capazes de obter insights de ataques exclusivos que possam estar ocorrendo no momento, bem como insights de tendências com base em dados históricos de eventos de segurança. Como ressalta a Forrester, a operacionalização de inteligência contra ameaças é fundamental, pois 75% dos ataques passam de uma vítima para outra em até 24 horas. As empresas precisam fechar a lacuna entre "a velocidade do compartilhamento e a velocidade do ataque".[5]

Aproveite a arquitetura integrada da McAfee

A McAfee oferece uma plataforma unificada e colaborativa com todos os componentes necessários para operacionalização de inteligência contra ameaças, incluindo feeds globais de inteligência contra ameaças, criação de inteligência local, compartilhamento em tempo real de informações sobre ameaças pela infraestrutura de TI, gerenciamento de eventos e informações de segurança e oferta de proteção automatizada e adaptável.

Requisitos da inteligência contra ameaças	McAfee® Threat Intelligence Exchange	McAfee Advanced Threat Defense	McAfee Enterprise Security Manager	McAfee Global Threat Intelligence
Coleta inteligência contra ameaças de fontes externas	STIX, importação do McAfee® Global Threat Intelligence (McAfee GTI) e VirusTotal	Importação do McAfee GTI	McAfee GTI, importação de TAXII/STIX e feeds de ameaças em HTTP pelo gerenciador de ameaças cibernéticas do McAfee Enterprise Security Manager	O McAfee GTI agrega inteligência contra ameaças de múltiplos parceiros da Cyber Threat Alliance e fontes públicas. O McAfee GTI extrai inteligência contra ameaças de milhões de sensores em produtos da McAfee distribuídos para clientes, como sistemas de prevenção de intrusões de rede, e-mail, Web e endpoint, além de dispositivos de firewall.
Coleta inteligência interna contra ameaças	Coleta amostras do McAfee VirusScan®, do McAfee Application Control, do McAfee Web Gateway, do McAfee Advanced Threat Defense, do McAfee Enterprise Security Manager e de produtos de fornecedores terceiros que enviam informações pelo Data Exchange Layer	Consome arquivos de amostras para detonação oriundos do McAfee Threat Intelligence Exchange ou via rede	Via STIX/TAXII e Data Exchange Layer	
Produz inteligência contra 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 o malware, gera inteligência contra ameaças local e a distribui pelo Data Exchange Layer ou como uma API em formatação STIX	Cria listas de observação, relatórios e visualizações de inteligência contra ameaças com base em eventos correlacionados	

Requisitos da inteligência contra ameaças	McAfee® Threat Intelligence Exchange	McAfee Advanced Threat Defense	McAfee Enterprise Security Manager	McAfee Global Threat Intelligence
Distribui inteligência contra ameaças pelos controles de segurança	Via Data Exchange Layer	Via Data Exchange Layer e API do produto	Via Data Exchange Layer, API do produto e integração de scripts	O McAfee GTI integra-se com vários produtos da McAfee, como o McAfee Web Gateway, o McAfee Enterprise Security Manager e soluções de endpoint da McAfee
Oferece visibilidade sobre a inteligência coletada sobre ameaças	Via dashboards do McAfee Threat Intelligence Exchange	Via relatórios	Via dashboards, visualizações e relatórios fornecidos em pacotes de conteúdo ou gerados pelo cliente	Via McAfee Threat Center e Relatórios trimestrais da McAfee sobre ameaças

Table 1. Plataforma integrada de inteligência contra ameaças da McAfee.

Assimilação, análise e propagação

McAfee Global Threat Intelligence

Um bom ponto de partida para a construção da sua plataforma integrada de inteligência contra ameaças é o McAfee Global Threat Intelligence (McAfee GTI), um serviço abrangente de reputação em tempo real com base na nuvem que se integra completamente aos produtos da McAfee, possibilitando que estes bloqueiem melhor as ameaças cibernéticas em todos os vetores — arquivos, Web, mensagens e redes — com rapidez. O McAfee GTI oferece pontuações de reputação para bilhões de arquivos, URLs, domínios, e endereços IP com base em dados de ameaças colhidos de múltiplas fontes: milhões de sensores globais monitorados e analisados pelo McAfee Labs, feeds de ameaças de parceiros de pesquisa e via Cyber Threat Alliance, bem como inteligência multivetorial de dados sobre ameaças de Web, e-mail e rede. Apoiado por feeds de ameaças relevantes e de alta qualidade, o McAfee GTI oferece recomendações precisas sobre risco que viabilizam uma tomada de decisões informadas e que permitem aos controles bloquear, limpar ou permitir, conforme a necessidade.

McAfee Enterprise Security Manager

O McAfee Enterprise Security Manager (SIEM) leva a assimilação e análise de inteligência contra ameaças a um novo patamar, atuando com uma central de consolidação, análise e ação para todo tipo de inteligência contra ameaças. Essa visão de 360 graus permite plena visibilidade e percepção situacional para acelerar a detecção e a resposta a ataques direcionados. Seu sistema avançado de gerenciamento de dados foi desenvolvido especificamente para armazenar e assimilar grandes volumes de dados contextuais em tempo real.

O McAfee Enterprise Security Manager coleta dados de eventos e atividades de todos os seus sistemas, bancos de dados, redes e aplicativos. Ele também importa

feeds de ameaças globais e consome inteligência contra ameaças em transportes e formatos padrão, como Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII) e Cybox, que costumam ser publicados por comunidades e grupos setoriais como o Financial Services Information Sharing and Analysis Center (FS-ISAC).

Através de análises avançadas, ele converte as informações coletadas em inteligência de segurança decisiva e compreensível. O mais significativo é que ele proporciona uma visibilidade mais profunda sobre ameaças emergentes através de visualizações em tempo real e acesso a informações históricas de segurança. Isso permite investigar retroativamente para compreender o predomínio e os padrões de um ataque, além de criar listas de observação automatizadas para detectar a ocorrência e a recorrência de eventos no futuro. Ao enriquecer a sensibilidade do seu sistema a eventos notoriamente maliciosos, você aumenta sua capacidade de detectar atividades suspeitas e padrões de atividade em várias fases da cadeia de ataque e, em seguida, de priorizar a resposta.

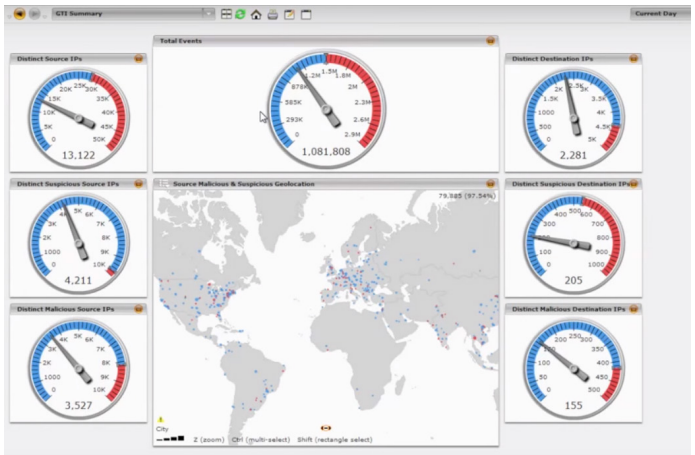

Figura 2. Visualização do McAfee GTI.

O McAfee GTI para McAfee Enterprise Security Manager traz o poder das capacidades de pesquisa do McAfee Labs para o monitoramento de segurança corporativa. Esse feed rico e constantemente atualizado do McAfee GTI aumenta a percepção situacional ao viabilizar uma descoberta rápida de eventos que envolvem comunicações com IPs suspeitos ou maliciosos e permite que os administradores de segurança determinem quais hosts corporativos se comunicaram ou estão se comunicando com agentes notoriamente nocivos.

McAfee Threat Intelligence Exchange

O terceiro componente que você pode adicionar ao desenvolver um ecossistema integrado de inteligência contra ameaças é o McAfee Threat Intelligence Exchange, que agrega e compartilha inteligência sobre reputação de arquivos por toda a infraestrutura de segurança. O McAfee Threat Intelligence Exchange recebe inteligência sobre ameaças do McAfee GTI, de importações de arquivos STIX, de feeds de ameaças oriundos do McAfee Enterprise Security Manager e informações vindas de endpoints, controle de aplicativos, dispositivos móveis, gateways, data centers e tecnologias de área restrita, tanto de soluções da McAfee quanto de outros fornecedores.

A coleta de dados de todos os pontos da sua infraestrutura proporciona informações sobre ameaças que podem estar presentes apenas no seu ambiente, como tendem a ser muitos ataques direcionados.

O que é a Cyber Threat Alliance?

A **Cyber Threat Alliance** é um grupo de profissionais de segurança de organizações que trabalham conjuntamente para compartilhar informações sobre ameaças e ajudar a melhorar as defesas contra adversários nas organizações participantes e seus clientes. A McAfee está entre os membros fundadores que dedicaram seus recursos a determinar as maneiras mais eficazes de compartilhar dados sobre ameaças, promover colaboração entre os membros e fazer um progresso unificado na luta contra criminosos cibernéticos sofisticados.

Em contrapartida, informações de reputação de arquivos são instantaneamente compartilhadas por todo o ecossistema para todos os produtos e soluções conectados ao McAfee Threat Intelligence Exchange via Data Exchange Layer (DXL). Por exemplo, se o McAfee Threat Intelligence Exchange envia informações sobre um arquivo executável malicioso, o McAfee Data Loss Prevention recebe essas informações pelo DXL e, então, começa a monitorar qualquer acesso a arquivos confidenciais por parte desse executável.

Os dados de ameaças compartilhados pelo DXL incluem reputações de arquivos, classificações de dados, integridade de aplicativos e dados contextuais de usuários, os quais são compartilhados com e entre os produtos integrados na malha DXL. Qualquer produto ou solução pode ser integrado no DXL e, em seguida, configurado para determinar quais informações publicar no sistema e quais informações ouvir e assinar.

O McAfee Threat Intelligence Exchange trabalha intimamente com a avançada solução de área restrita McAfee Advanced Threat Defense, que encaminha dados de análise de malware para o McAfee Threat Intelligence Exchange. Quando um arquivo é considerado malicioso, o McAfee Threat Intelligence envia pelo DXL uma atualização de reputação de arquivo para todos os sistemas conectados. Isso também funciona de forma recíproca. Quando os endpoints com McAfee Threat Intelligence Exchange encontram arquivos com reputações desconhecidas, estes podem ser enviados ao McAfee Advanced Threat Defense para determinar se o objeto é malicioso, eliminando pontos cegos na entrega de carga fora de banda. Esses dois produtos funcionam conjuntamente para proporcionar proteção automatizada e adaptável contra ameaças emergentes. Informações sobre ataques descobertos são fornecidas pelo seu ambiente para ajudar a bloquear a cadeia de ataque cibernético antes que mais danos sejam feitos.

O McAfee Threat Intelligence Exchange permite detecção e resposta adaptáveis a ameaças operacionalizando a inteligência pelos seus endpoints, gateways, redes e soluções de segurança de data center em tempo real. A combinação de informações globais de ameaças importadas com inteligência coletada localmente e seu compartilhamento instantâneo permitem que suas soluções de segurança operem como se fossem uma só, trocando e agindo com base em inteligência compartilhada.

Interrompa a cadeia de ataque cibernético

Independentemente de onde ocorra o primeiro ponto de contato com um arquivo de malware desconhecido, assim que este for condenado, todo o ambiente conectado será atualizado imediatamente. Quando um arquivo é condenado pelo McAfee Advanced Threat Defense, o McAfee Threat Intelligence Exchange publica essa condenação por meio de uma atualização de reputação, a qual é disseminada através do DXL para todos os controles de segurança da sua organização. Os gateways com McAfee Threat Intelligence Exchange podem impedir que o arquivo entre na sua infraestrutura. A coordenação do compartilhamento de inteligência contra ameaças com todos os seus controles de segurança torna mais fácil interromper a cadeia de ataque e evitar prejuízos adicionais, sem a necessidade de intervenção manual.

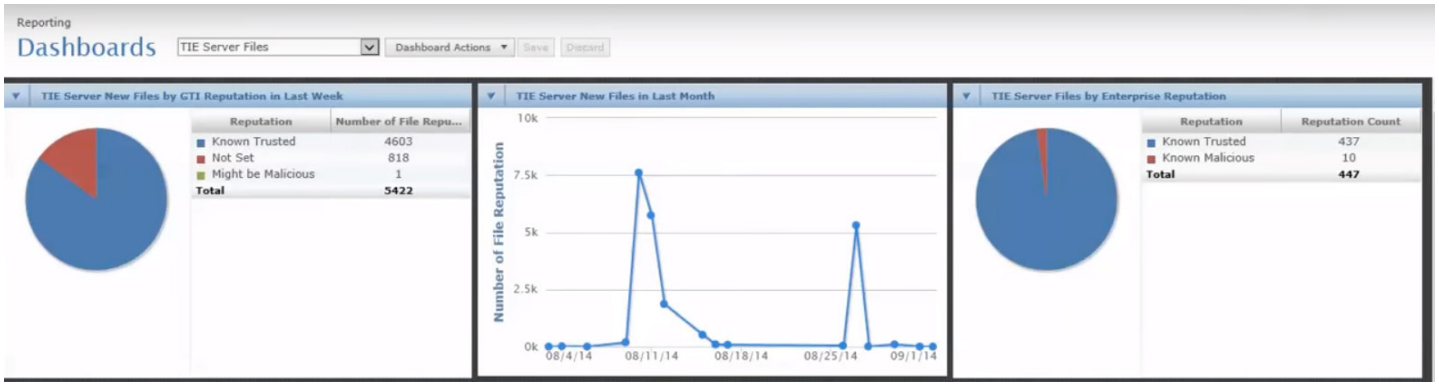

Figura 3. Dashboard do McAfee Threat Intelligence Exchange.

Processamento e aplicação: detecção com precisão e melhor tomada de decisões

Após os dados de ameaças serem consumidos, o McAfee Enterprise Security Manager atua como um ponto central de visibilidade, correlacionando o McAfee GTI, feeds do McAfee Threat Intelligence Exchange e indicadores de comprometimento (IoCs) em formatação STIX/TAXII com dados de eventos, detectados em tempo real ou historicamente, quando nós da sua rede estão se comunicando com agentes notoriamente nocivos ou domínios suspeitos. O dashboard de gerenciamento de ameaças oferece aos analistas uma visualização única e abrangente dos indicadores de ameaças coletados, dos feeds de origem, da taxa de acertos em relação aos indicadores e dos detalhes legíveis mais significativos sobre os indicadores de comprometimento (IoCs).

O uso do sistema SIEM da McAfee conjuntamente com outras ferramentas colaborativas de inteligência contra ameaças resulta em menores despesas operacionais associadas à configuração de regras de correlação, a qual costuma ser um processo manual complicado. Por exemplo, os analistas de segurança podem examinar diretamente as informações sobre ameaças recém-recebidas, possibilitando uma melhor compreensão de novas ameaças detectadas. O mais importante é que a inteligência contra ameaças recebida pode ser adotada automaticamente por regras de correlação histórica ou em tempo real, reduzindo o tempo de detecção de atividades nocivas em andamento ou novas. Os usuários também podem acompanhar o progresso das ameaças relatadas por todo o ambiente de TI, bem como através de informações contextuais em visualizações de alarme, possibilitando decisões melhores e mais informadas. Toda essa inteligência coletada melhora e acelera a detecção e a investigação dos ataques direcionados.

Os seguintes produtos da McAfee são compatíveis com inteligência contra ameaças em formato STIX:

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

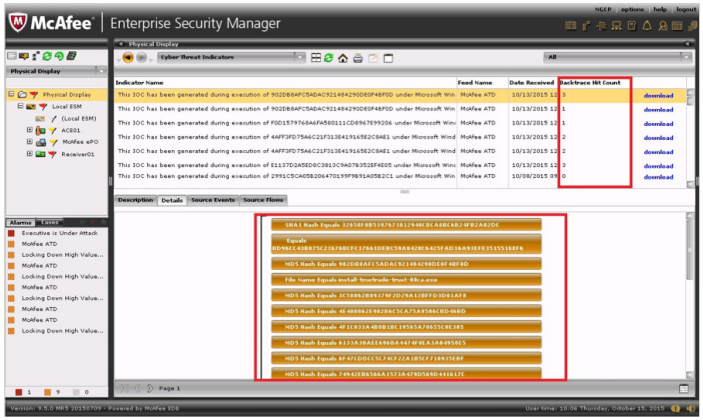

Figure 4. Detalhes sobre ameaças dos IoCs, acertos de rastreamento retroativo e indicadores de ameaças cibernéticas do McAfee Enterprise Security Manager.

Como as ameaças percorrem rapidamente a infraestrutura de TI e são concebidas para mudar com o tempo, o McAfee Enterprise Security Manager pode atualizar periodicamente toda a inteligência contra ameaças adquirida, eliminando dados antigos e menos relevantes. Por exemplo, servidores de comando e controle removidos ou sites que passaram por uma limpeza e que apresentam pontuações mais baixas de reputação maliciosa são automaticamente liberados para eliminar falsos positivos que possam distrair a sua equipe de segurança e prejudicar a busca por ameaças reais.

Resumo

A inteligência integrada sobre ameaças da McAfee operacionaliza a assimilação, o processamento e o gerenciamento da inteligência contra ameaças, permitindo que você aumente a precisão da detecção de ameaças, elimine o trabalho manual e impeça que adversários prejudiquem os seus negócios. Com visibilidade aprimorada e insights melhores sobre a atividade maliciosa em todo o seu ecossistema de segurança, você fica mais bem preparado para identificar e antever ataques direcionados hoje e preveni-los no futuro.

Saiba mais

Para obter mais informações sobre os elementos constituintes da plataforma integrada de inteligência contra ameaças da McAfee, visite:

- **McAfee Global Threat Intelligence**
- **McAfee Threat Intelligence Exchange**
- **McAfee Advanced Threat Defense**
- **McAfee Enterprise Security Manager**
- **How to Use a TAXII Feed with McAfee Enterprise Security Manager (Como usar um 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/br/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
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