McAfee MVISION XDR

A primeira solução de detecção e resposta estendida, proativa, ciente dos dados e aberta, desenvolvida para ajudar as organizações a deter ataques sofisticados.

Realidades das operações de segurança

O centro de operações de segurança (SOC) é uma função essencial no plano de segurança cibernética de qualquer organização. Seu foco principal está em encontrar e resolver rapidamente as ameaças para evitar danos a ativos e dados. Se o SOC tem dificuldades, é provável que os resultados de segurança sejam dúbios e que as organizações corram risco. Os desafios do SOC continuam a crescer em volume e em escala, apesar do aumento de gastos. Três quartos dos profissionais de segurança afirmam que a detecção e resposta de ameaças é mais difícil atualmente do que dois anos atrás, segundo a empresa de pesquisas ESG[1]. Então, isso significa que os adversários estão vencendo?

É correto afirmar que a função do SOC ainda está amadurecendo. Um estudo recente do SANS Institute[2] constatou que apenas 29% das organizações se consideram maduras ou muito maduras no que se refere a caça a ameaças e que apenas 40% têm resposta a incidentes como parte da função do SOC.

59% das organizações enfrentaram um incidente cibernético grave, mas apenas 26% afirmaram que seu SOC identificou a violação mais significativa.

(Ernst & Young, 2020)

Conecte-se conosco

Cargas de trabalho pesadas e complexidade de gerenciamento no SOC

Na maioria dos casos, o SOC também padece de falta de recursos devido à imensa escassez de talentos em segurança cibernética e à dificuldade de retenção desses talentos. Além disso, o SOC sofreu uma avalanche de ferramentas isoladas umas das outras, o que acrescenta um grau de complexidade que prejudica a capacidade do SOC de detectar e responder com rapidez e adequadamente. Segundo a ESG[3], 66% das organizações afirmam que a eficácia da detecção e resposta a ameaças é limitada por se basear em diversas ferramentas pontuais independentes.

A implicação para o SOC é que o tempo para detectar e responder a ameaças chega a meses, dando aos adversários um tempo mais longo de permanência durante o qual eles podem causar mais danos. Precisamos, portanto, de fácil visibilidade e controle sobre todos os ativos cibernéticos, com inteligência decisiva para passarmos rapidamente à resolução das ameaças. A abordagem de ferramentas fragmentadas precisa ser integrada e simplificada entre endpoints, a rede, a nuvem e os aplicativos para eliminar a complexidade. A fadiga causada pelo excesso de alertas precisa ser aliviada com detecção e análise automática que priorize e faça triagem das ameaças. Os SOCs precisam ser qualificados com capacidades inteligentes e eficientes de detecção, investigação e resposta para prevenir ataques ou resolvê-los antes que ocorram danos significativos.

Melhore a eficiência e a produtividade do SOC

O McAfee® MVISION XDR é a resposta para essas ineficiências operacionais e desafios do SOC. Ele tem a exclusividade de expandir capacidades de detecção e resposta estendidas (XDR) em um gerenciamento de ameaças avançadas baseado em nuvem por toda a infraestrutura de TI, acrescentando uma cobertura diferenciada sobre todo o ciclo de vida dos ataques, com priorização para proteger o que importa e etapas simples para coordenar uma resposta eficiente. O MVISION XDR reduz o risco do dispositivo à nuvem, aprimorando rapidamente a eficácia do SOC ao reduzir os ciclos reativos enquanto economiza até 95% em custos de avaliação de campanhas de ameaças[4] com o primeiro XDR aberto, proativo e orientado por dados.

Os ataques remotos perpetrados por elementos externos contra serviços de nuvem aumentaram 630% em 2020.

(McAfee, 2020)

Principais vantagens

Os SOCs podem fazer mais com o MVISION XDR, graças à sua visão unificada entre endpoints, rede e nuvem. O MVISION XDR ajuda a:

- Reduzir os erros humanos associados à alternância manual entre ferramentas e dados
- Priorizar e proteger o que importa, com um reconhecimento de dados que leva em conta sua criticalidade e confidencialidade
- Minimizar o risco antes e depois dos ataques com inteligência decisiva e proativa, investigações orientadas e automatizadas e contramedidas prescritivas
- Aprimorar a visibilidade e o controle e eliminar tarefas manuais tediosas coordenando facilmente as soluções de segurança para que elas funcionem conjuntamente
- Proporcionar um gerenciamento decisivo de ameaças cibernéticas sem aumentar o tamanho da equipe, mas capacitando-a

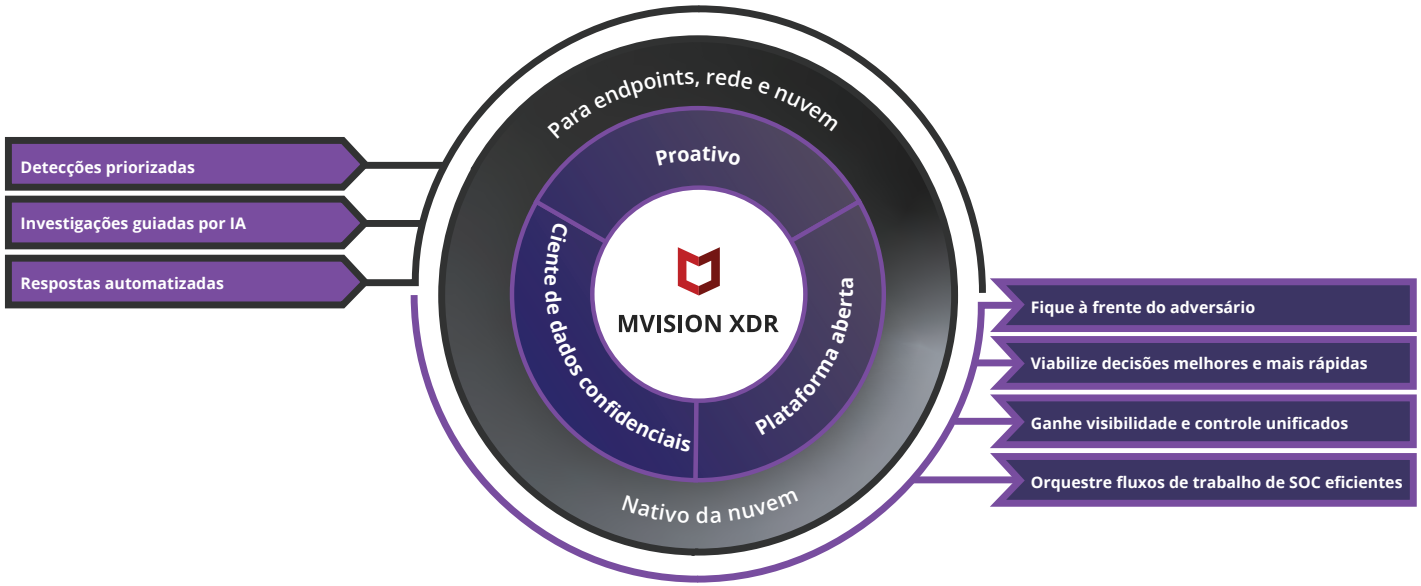

Figura 1. Principais vantagens e resultados do MVISION XDR.

Conte com uma inteligência decisiva e proativa para se manter à frente dos adversários

A maioria das soluções de XDR só oferece suas capacidades após um ataque ter penetrado o ambiente da organização, o que resulta em um SOC altamente reativo, sempre de prontidão para emergências. O MVISION XDR, respaldado pelo McAfee MVISION Insights, é o único XDR que enfrenta todo o ciclo de vida dos ataques com fluxos de trabalho reativos mais fortes após o ataque e novas capacidades proativas antes do ataque. Os SOCs podem atuar nas ameaças externas que importam, antes que o ataque ocorra. As organizações podem priorizar ameaças, prever se as contramedidas funcionarão e prescrever ações corretivas. O resultado é detecção e resposta mais rápidas — em questão de minutos em vez de semanas.

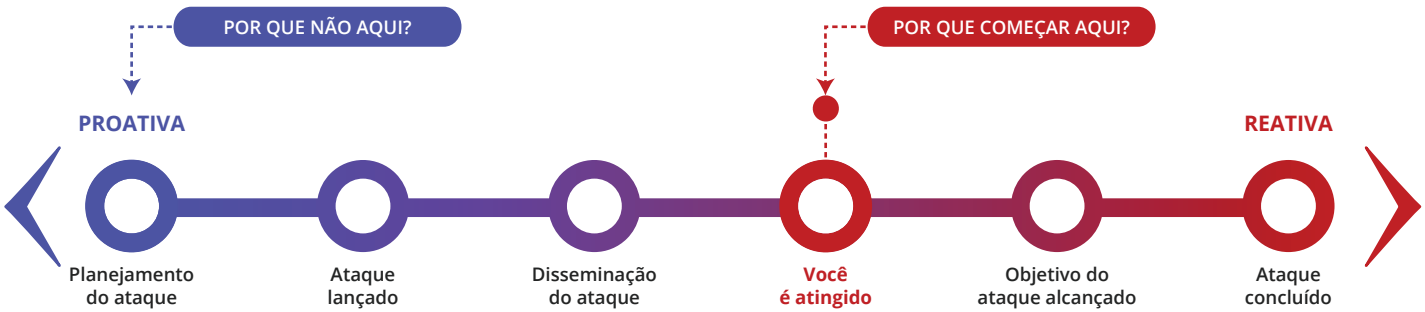

Figura 2. O MVISION XDR enfrenta todo o ciclo de vida dos ataques com capacidades proativas e reativas.

Tenha visibilidade e controle unificados em múltiplos vetores de ataque

A capacidade de ver e correlacionar informações sobre o trabalho do adversário entre diversos vetores é fundamental, considerando-se o quão erráticos podem ser os movimentos do adversário. Ainda mais importante é que, uma vez evidenciada a situação de ameaça, os analistas precisam atuar em diversos vetores para resolver a ameaça.

O MVISION XDR combina telemetria de malhas de sensores no local e na nuvem para proporcionar uma visão holística detalhada dos dados corporativos, bem como dos comportamentos dos adversários. Ao converter um grande fluxo de alertas de toda a empresa em um número menor de incidentes, o MVISION XDR reduz o ruído e conduz os analistas para mais perto da resolução.

Em um dashboard intuitivo, os analistas do SOC têm acesso a descobertas fundamentais relacionadas a seu ambiente, campanhas em destaque e prioridades recomendadas com base em análise e trabalho investigativo automático.

Desse ponto de vista, os analistas podem se aprofundar e facilmente investigar e determinar as ações necessárias a serem seguidas. As opções de resposta afetam múltiplos vetores por toda a empresa.

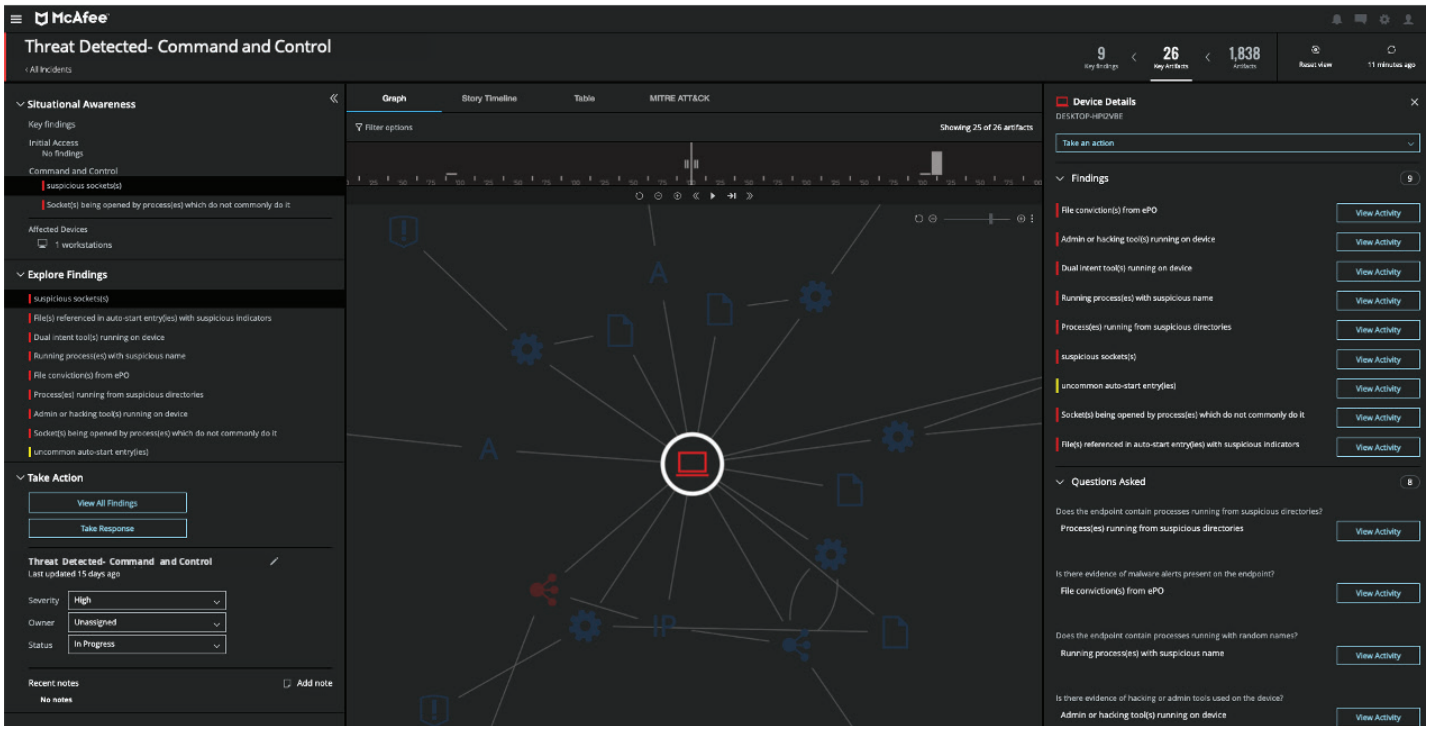

Figura 3. Incidentes priorizados com fluxos de trabalho de investigação e resposta orientados e detalhados reduzem a sobrecarga de alertas e aceleram a resolução.

Viabilize decisões melhores e mais rápidas

Os SOCs precisam tomar decisões rapidamente para resolver ameaças e minimizar danos. Os passos para decisões mais rápidas incluem acelerar o trabalho de investigação e priorizar o que é crítico. O MVISION XDR acelera esse trabalho com investigações automáticas e orientadas por inteligência artificial. Investigações orientadas por inteligência artificial conduzem os analistas do SOC, fazendo e respondendo perguntas automaticamente, enquanto coletam, resumem e exibem evidências de múltiplas fontes. Isso ajuda os analistas do SOC a aprender continuamente enquanto aprimoram suas capacidades de investigação e resposta. Além disso, investigações automáticas derivadas de uma lógica de triagem comprovada podem ser realizadas a qualquer momento. Ambas opções eliminam a necessidade de coletar e analisar evidências manualmente. Elas também acabam com o ruídos dos alertas e capacitam os analistas a chegar prontamente a uma decisão de resposta.

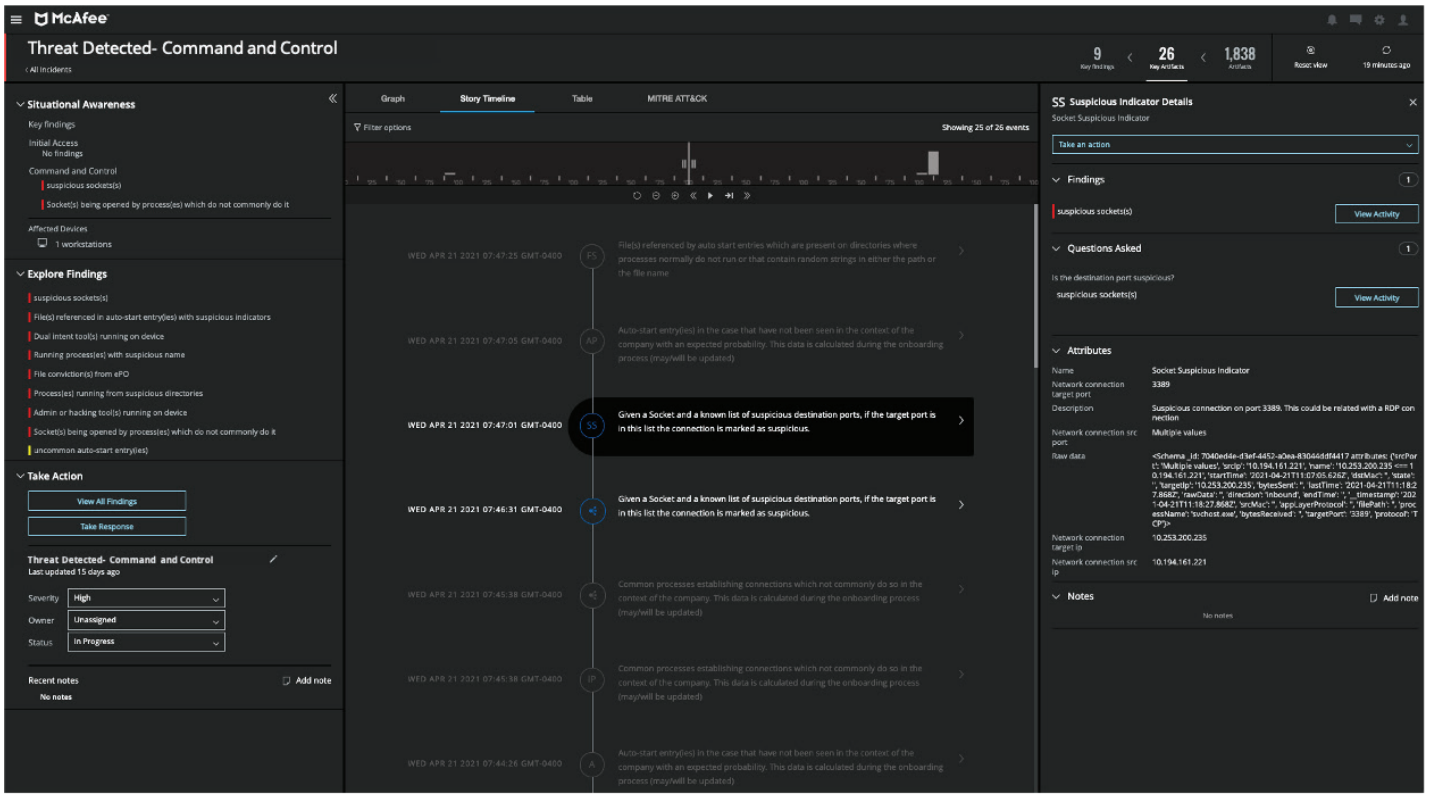

Figura 4. Uma cronologia decisiva proporciona uma visão detalhada dos eventos que constituíram toda a extensão do ataque.

O MVISION XDR assimila inteligência sobre ameaças de uma variedade de fontes, como soluções de gerenciamento de eventos e informações de segurança (SIEM), e oferece uma maneira fácil de pesquisar o "quem" e o "onde" do incidente ou ameaça. A história do adversário é exibida de maneira simples em uma linha de tempo com incidentes e seus respectivos dados e comportamentos correlacionados. Os analistas podem se aprofundar nas descobertas e evidências para avaliar o evento utilizando seu conhecimento e intuição. Ações recomendadas são oferecidas com base nos trabalhos anteriormente realizados pela organização e em insights sobre como outros no mesmo setor responderam.

O MVISION XDR oferece uma gama de opções de priorização para chegar rapidamente a uma decisão crítica. Ameaça e incidentes podem ser priorizados com base no impacto organizacional, como danos ou perda de dados. Uma ameaça que satisfaça determinados critérios baseados em categorias de proteção de dados, identidade e tipo de dispositivo pode receber uma prioridade mais alta. Por exemplo, o dispositivo de um executivo contendo dados altamente confidenciais em risco tem precedência.

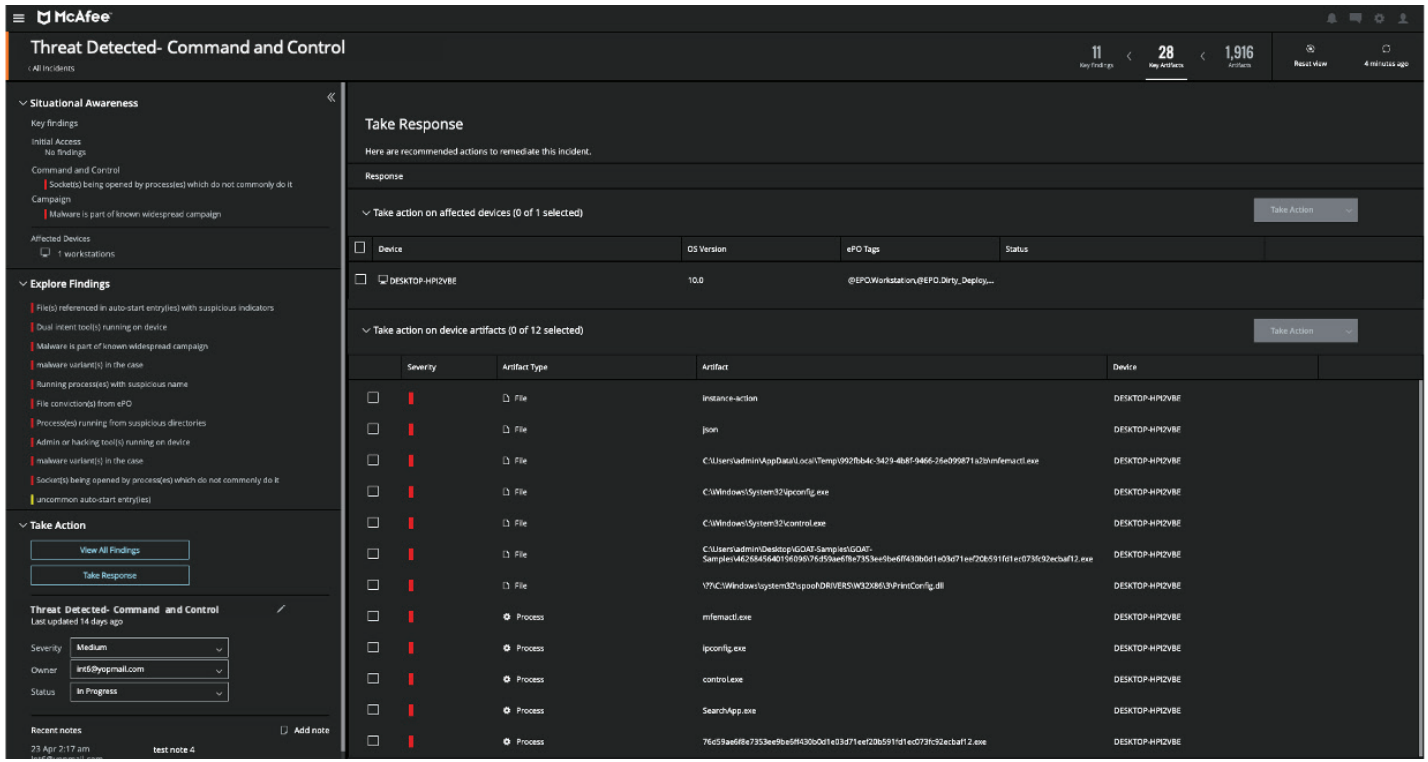

Figura 5. Ações recomendadas ajudam você a agir rapidamente para remediar incidentes e conter ameaças.

Orquestre fluxos de trabalho eficientes e automatizados

O MVISION XDR é uma plataforma aberta e integrada que atua em múltiplos vetores e se conecta a outras funções de segurança. Isso permite à ferramenta de segurança trabalhar conjuntamente de forma unificada para neutralizar o adversário. Não há necessidade de alternar manualmente entre ferramentas e copiar/colar dados e isso economiza tempo e reduz erros humanos. Isso também permite a correlação de detecções entre ferramentas de segurança para que se chegue a alertas e decisões com alto nível de confiança. A interface de programação de aplicativos (API) aberta permite que as organizações simplesmente criem fluxos de trabalho (para caça, investigação, resposta e mitigação) com a McAfee e/ou terceiros em um mercado on-ine de fácil utilização, o que resulta em um gerenciamento simplificado de ameaças cibernéticas.

Outras soluções de terceiros podem incluir geração de tíquetes de TI, resposta por automação da orquestração de segurança (SOAR), SIEM e inteligência sobre ameaças. O MVISION XDR permite que você aproveite os investimentos existentes, sejam estes soluções da McAfee ou não. Não há necessidade de desativar e substituir as suas defesas cibernéticas atuais.

A jornada do MVISION XDR permite que capacidades e fluxos de trabalho sejam integrados no seu ritmo. O compromisso da McAfee com uma segurança aberta e integrada, que facilite o compartilhamento de informações e a coordenação da proteção, reflete-se em sua atuação como co-fundadora da Open Cybersecurity Alliance (OCA), uma iniciativa setorial de segurança, e na sua colaboração na ontologia OpenDXL, um protocolo de intercâmbio de informações e mecanismo de transporte comum.

Em resumo

O MVISION XDR é a primeira solução XDR proativa, ciente dos dados e aberta do mercado que capacita as equipes do SOC a:

- Correlacionar informações de alertas distintos para visualizar todo o ciclo de vida dos ataques, priorizar as ameaças mais importantes e ficar à frente dos adversários.
- Automatizar processos de investigação e resposta para eliminar tarefas manuais e economizar tempo e, com isso, favorecer outras tarefas que se beneficiem mais do seu conhecimento.
- Caçar proativamente as ameaças e atividades de adversários que visem a sua organização e minimizar os riscos associados a ativos e dados desprotegidos.

Saiba mais

Para obter mais informações, visite mcafee.com/xdr.

1. Threat Detection and Response Landscape Survey (Pesquisa sobre o cenário de detecção e resposta a ameaças), ESG, 2019
2. “Is Your Threat Hunting Working?” (A sua caça a ameaças está funcionando?), SANS, 2020
3. Threat Detection and Response Landscape Survey (Pesquisa sobre o cenário de detecção e resposta a ameaças), ESG, 2019
4. Pesquisa interna de clientes da McAfee.

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