SOPHOS
Cybersecurity delivered.

Cinco principais motivos para usar os Serviços MDR

Documento técnico Sophos. Setembro, 2022

Introdução

Com o aumento em volume, complexidade e impacto das ameaças cibernéticas, as organizações estão buscando cada vez mais os serviços MDR de detecção e resposta gerenciadas para detectar e neutralizar os ataques avançados que as soluções tecnológicas por si só não conseguem evitar. De fato, a Gartner prevê que, até 2025, 50% das empresas estarão usando MDR para o monitoramento, detecção e resposta a ameaças[1].

Porém, a proliferação de soluções de defesa que o mercado oferece pode dificultar o entendimento exato do significado de MDR, como o MDR se enquadra no seu ecossistema de segurança cibernética geral, e quais os benefícios que um serviço MDR pode oferecer. Este documento responde a essas perguntas e oferece um guia prático sobre o que considerar ao escolher um serviço MDR.

Sophos MDR

O Sophos MDR é o serviço MDR mais confiável do mundo, protegendo mais de 11.000[2] organizações contra as ameaças mais avançadas, incluindo ransomwares. Apresentando a mais alta pontuação no Gartner Peer Insights™[3] e reconhecida como Top Vendor do 2022 G2 Grid® em serviços MDR direcionados ao mercado de empresas de médio porte[4], com o MDR da Sophos suas defesas cibernéticas estarão em boas mãos.

A definição de MDR

Para entender os benefícios do MDR e o que está por trás do aumento na demanda por serviços MDR, é importante entender o que é MDR – e o que não é.

A detecção e resposta gerenciadas (MDR) é um serviço totalmente gerenciado – 24 horas por dia, sete dias por semana – entregue por peritos especializados em detectar e responder a ataques cibernéticos que as soluções tecnológicas por si só não conseguem evitar.

Não confunda MDR com EDR (detecção e resposta de endpoint) ou com XDR (detecção e resposta estendidas). Ainda que MDR, EDR e XDR sejam voltados à caça a ameaças, EDR e XDR são ferramentas que permitem que os analistas saiam no encalço de ameaças e investiguem possíveis comprometimentos; já com o MDR, os analistas de segurança do fornecedor buscam, investigam e neutralizam as ameaças por você.

Como o próprio nome sugere, as ferramentas EDR trabalham com pontos de dados provenientes da tecnologia de proteção de endpoint, enquanto as ferramentas XDR estendem suas fontes de dados para englobar toda a pilha de TI (incluindo firewall, e-mail, nuvem e soluções de segurança móvel) para oferecer maior visibilidade e insights. Na Sophos, usamos nossas soluções de EDR e XDR líderes do setor ao promover nossos serviços MDR.

O que o MDR não faz é o dia a dia do gerenciamento da segurança cibernética, como, por exemplo, implantar suas tecnologias de segurança, atualizar políticas, aplicar patches ou instalar atualizações. Os provedores de serviços gerenciados (MSP) fornecem serviços gerenciados de segurança de TI a organizações que buscam suporte nessa área.

Quem usa os serviços MDR

Todos os tipos de organizações em todos os setores usam os serviços MDR, desde pequenas empresas com recursos de TI limitados até grandes empresas com um grupo interno de SOC. A pergunta é: como as organizações trabalham com serviços MDR? Existem três modelos principais de resposta MDR:

- Uma equipe de MDR gerencia completamente a resposta a ameaças para o cliente
- Uma equipe de MDR trabalha com a equipe interna, cogerenciando a resposta a ameaças
- Uma equipe de MDR alerta a equipe interna e fornece diretrizes para remediação

Na Sophos, trabalhamos com todas essas três abordagens, adaptando-as a cada cliente de acordo com suas necessidades individuais.

1 Gartner Market Guide for MDR 2021
2 Em agosto de 2022.
3 Comentários registrados nos últimos 12 meses, em 1º de agosto de 2022. O conteúdo do Gartner Peer Insights consiste em opiniões de usuários finais individuais baseadas em suas próprias experiências com fornecedores listados na plataforma e não deve ser interpretado como uma declaração de fato nem como representação da visão da Gartner ou de suas afiliadas. A Gartner não endossa fornecedores, produtos ou serviços representados neste conteúdo nem estabelece qualquer garantia, expressa ou implícita, em respeito a este conteúdo, sua precisão ou completude, incluindo garantias de comercialização ou de um propósito de uso específico.
4 A Sophos é reconhecida como Top Vendor do 2022 G2 Grid® em serviços MDR direcionados ao mercado de empresas de médio porte.

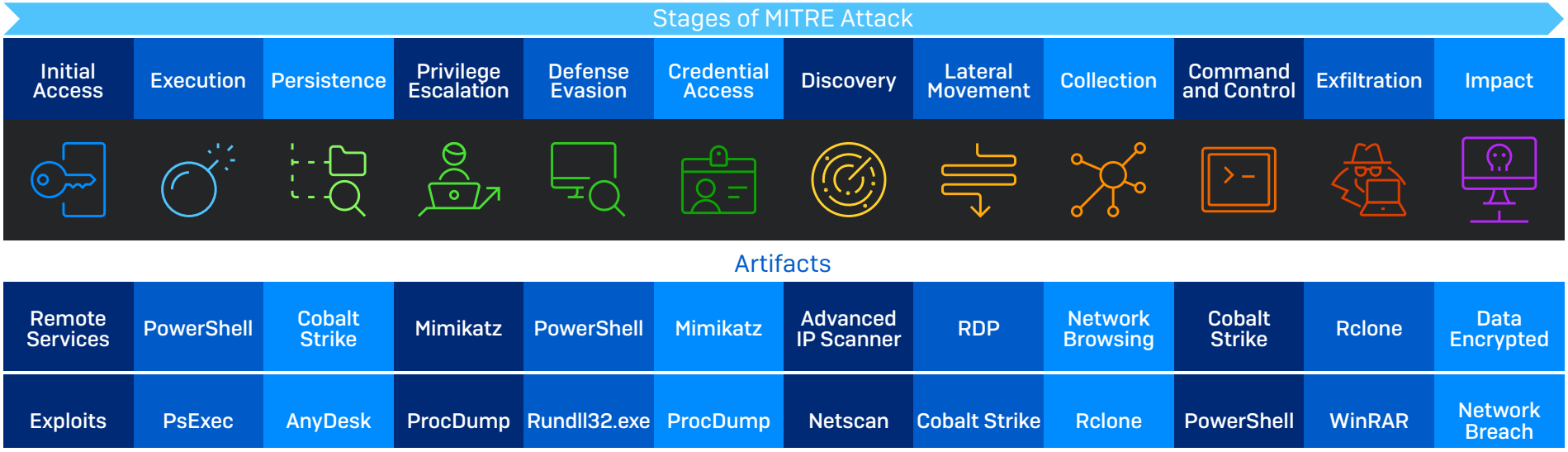
A necessidade da detecção e resposta lideradas por humanos

A verdade é que as soluções tecnológicas por si só não conseguem evitar todo e qualquer ataque cibernético. Para evitar a detecção pelas soluções de segurança cibernética, os agentes mal-intencionados se utilizam cada vez mais de ferramentas de TI legítimas, explorando credenciais e permissões de acesso roubadas e se aproveitando de vulnerabilidades não corrigidas para formar seus ataques. Ao emular usuários autorizados e se aproveitar dos pontos fracos nas defesas de uma organização, os agentes mal-intencionados conseguem evitar o acionamento das tecnologias de detecção automatizadas.

A imagem abaixo detalha os principais artefatos (ferramentas) usados pelos invasores em cada estágio da cadeia MITRE ATT&CK, conforme observado pelos caçadores de ameaças na linha de frente da Sophos em 2021. Como você pode ver, as ferramentas usadas regularmente pelas equipes de TI, como PowerShell, PsExec e RDP, são frequentemente usadas indevidamente pelos adversários. As tecnologias automatizadas têm dificuldade para diferenciar quando essas ferramentas são usadas pelo pessoal de TI para uma causa genuína ou quando são usadas por golpistas que tentam explorá-las usando credenciais roubadas.

Interromper esses ataques avançados do tipo "living-off-the-land" exige uma combinação de tecnologia e perícia humana. Toda vez que um impostor se empenha em uma ação, ela gera um sinal. Ao combinar perícia humana às poderosas tecnologias de proteção e modelos avançados de Machine Learning alimentados por IA, os analistas de segurança podem detectar, investigar e neutralizar mesmo os ataques mais avançados conduzidos por humanos e evitar a violação de dados.

Enquanto a caça, investigação e resposta podem ser desempenhadas exclusivamente pela equipe interna usando ferramentas de EDR e XDR, são grandes os benefícios de usar um serviço MDR para complementar a sua equipe interna ou como um serviço



Principais artefatos usados em cada estágio da cadeia de ataque Mitre. Playbook dos Adversários Ativos 2022, Sophos

Tecnologias de proteção continuam a desempenhar um papel vital nas defesas atuais

Enquanto a detecção e resposta gerenciadas e conduzidas por humanos representam uma fase essencial da defesa cibernética, tecnologias de proteção de alta qualidade permanecem críticas. Tecnologias de segurança de endpoint, rede, e-mail e nuvem continuam a desempenhar um papel vital nas defesas atuais – e as soluções certas podem aumentar a eficácia e o impacto de um serviço MDR:

- Tecnologias de proteção automatizadas permitem que o pessoal incumbido da sua defesa se mantenha à frente do volume crescente de ataques, com os adversários se aproveitando das ofertas de automação, IA e malware como serviço para proliferar suas ameaças. O Sophos Endpoint Protection bloqueia 99,98% das ameaças automaticamente, antes que possam impactar a organização.
- Um dos maiores desafios práticos que os caçadores de ameaças enfrentam é o ruído: com um volume de indícios muito grande, pode ser difícil separar alhos de bugalhos. Tecnologias superiores de prevenção reduzem o número de alertas que os analistas humanos necessitam investigar. Ao permitir que os caçadores de ameaças se concentrem em detecções menos frequentes e mais precisas, as tecnologias de prevenção de alta qualidade aceleram a resposta a ameaças liderada por humanos.
- Analistas humanos usam detecções e indícios lançados pelas tecnologias de prevenção para identificar e investigar atividades suspeitas. Quanto mais alta a qualidade das detecções e melhores os insights contextuais, mais rápidas e adequadas são a investigação e a resposta.

Com isso em mente, vamos agora analisar os cinco maiores benefícios registrados pelas organizações que usam os serviços MDR.

1. Eleve as suas defesas cibernéticas

Uma das maiores vantagens de usar um provedor de serviços MDR em lugar de contar apenas com programas internos de operações de segurança é elevar o seu nível de proteção contra ransomwares e outras ameaças cibernéticas avançadas.

Com o MDR, você se beneficia da variedade e abrangência da experiência dos analistas do provedor. Os fornecedores de MDR enfrentarão um maior volume e variedade de ataques do que qualquer organização individual, conferindo-lhes tal nível de expertise que será quase impossível replicar internamente.

As equipes de MDR também investigam e respondem a incidentes todos os dias, o que lhes dá uma agilidade muito maior no uso das ferramentas de caça a ameaças. Isso lhes permite responder com maior rapidez e precisão em todos os estágios do processo – da identificação dos indícios importantes até a investigação de possíveis incidentes e a neutralização de atividades maliciosas.

Trabalhar como parte de uma grande equipe também permite que os analistas compartilhem seus conhecimentos e percepções, acelerando ainda mais a resposta. A equipe do Sophos MDR documenta as informações pertinentes a cada ameaça ou agente específico com que se depara em runbooks. Quando um adversário é identificado durante uma investigação, em lugar de realizar uma imensa pesquisa no momento do ataque, nossa equipe pode consultar o runbook e entrar imediatamente em ação.

Os runbooks são atualizados continuamente, e os analistas registram informações distintas sobre cada engajamento, como:

- TTPs (táticas, técnicas e procedimentos) comuns ou específicos a um determinado ataque ou agente de ameaça.
- IOCs (indicadores de comprometimento) relevantes.
- Provas de conceito conhecidas das explorações vinculadas a vulnerabilidades abertas.
- Questões úteis sobre a caça a ameaças ao lidar com um determinado ataque ou agente de ameaça.

Outra vantagem do serviço MDR é que ele aplica a inteligência de um cliente a outros clientes que apresentem o mesmo perfil de "vítima", o que permite prevenir proativamente ataques semelhantes a uma mesma comunidade. Exemplos de cenários quando a equipe do Sophos MDR investiga as instalações virtuais e o patrimônio digital dos clientes incluem:

- Um cliente em uma indústria vertical específica que foi feito alvo de uma maneira particular.
- O Sophos X-Ops oferece inteligência sobre um ataque significativo direcionado a um determinado perfil de indústria ou organização.
- Um evento significativo ocorre em um cenário da segurança, e queremos averiguar se algum dos clientes foi afetado.

Caso nossos analistas detectem algum indício suspeito, eles são capazes de investigar e remediar rapidamente a situação, criando uma imunidade comunitária para o grupo-alvo.

A grande experiência adquirida e a capacidade de aplicar os ensinamentos aos ambientes de nossos clientes permitem que a equipe Sophos MDR eleve as defesas das organizações muito além do que conseguiriam obter por si só.

"Retornos tangíveis do Sophos MDR incluem 90% de redução no tempo para detectar ameaças de alto risco que exigem investigação, 95% de redução no tempo para identificar a origem do ataque e o tipo da ameaça, e precisão melhorada das detecções."
Chitale Dairy, Índia

"O pessoal de pen-test ficou abismado de não conseguir achar um jeito de se infiltrar. Foi aí que constatamos que podíamos usar o serviço da Sophos com absoluta confiança."
Universidade de South Queensland, Austrália

"Com o Sophos MDR, reduzimos drasticamente o nosso tempo de resposta a ameaças."
Tata BlueScope Steel, Índia

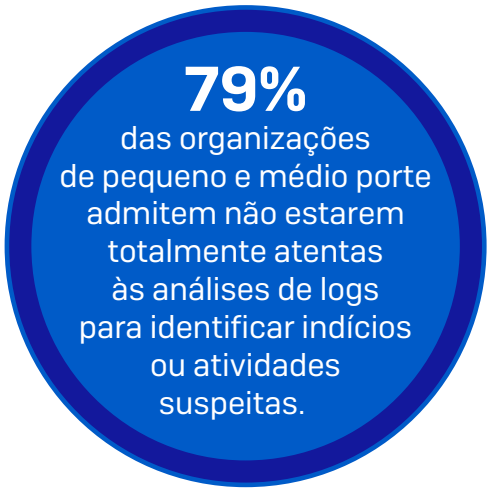
"Recebemos notificações de ameaças em tempo real."
Bardiani Valvole, Itália

2. Libere a capacidade de TI

A caça a ameaças é demorada e imprevisível. Para os profissionais de TI que precisam lidar com diferentes tarefas e prioridades, pode ser difícil superar o desafio: 79% das equipes de TI admitem não estarem totalmente atentas às análises de logs para identificar indícios ou atividades suspeitas[5].

Dado o potencial de impacto de um ataque a uma organização, quando algo suspeito é detectado, você precisa parar tudo o que está fazendo para que a ameaça possa ser investigada e tratada imediatamente. A natureza urgente do trabalho pode impedir que as equipes se concentrem em situações mais estratégicas – e, geralmente, mais interessantes.

Trabalhar com um serviço MDR permite que você libere o pessoal de TI, que passa a ter maior capacidade para cuidar de iniciativas mais direcionadas aos negócios. As organizações que usam o Sophos MDR registram ganhos consistentes em eficiência devido ao uso do serviço, o que, por sua vez, permitem que ofereçam melhor suporte aos objetivos de suas empresas.



"Desde que implementamos a solução da Sophos, conseguimos liberar horas de trabalho operacional, o que permitiu que nossas equipes se concentrassem em iniciativas que aumentaram a satisfação de nossos alunos."
Universidade London South Bank, Reino Unido

"A capacidade do Sophos MDR em remediar e remover ameaças de modo rápido e nos manter informados nos deixa livres para focar em tarefas mais rentáveis."
Tomago Aluminium, Austrália

"Com a presença do Sophos MDR, podemos testar e avançar em outras áreas da organização, como gerenciamento de vulnerabilidades, patching e conscientização em segurança."
The Fresh Market, EUA

"A Sophos mantém o controle das recentes atividades e ameaças, assim podemos focar na entrega de serviços de qualidade a nossos clientes e artistas."
CD Baby, EUA

5 Pesquisa independente com 5.600 profissionais de TI, janeiro-fevereiro de 2022. Comissionada pela Sophos e realizada pela Vanson Bourne.

3. Proteja-se com assistência 24 horas

Os maus elementos estão espalhados por todo o planeta, portanto um ataque pode acontecer a qualquer hora. Os adversários estão mais ativos quando a sua equipe de TI está menos propensa a estar online, ou seja, à noite, nos fins de semana e nos feriados. Isso mostra que a detecção e resposta a ameaças é uma tarefa incessante; se você ficar alerta apenas durante o horário de expediente, deixará sua organização exposta.

Ao disponibilizar assistência 24 horas por dia, sete dias por semana, os serviços MDR lhe dão uma excelente garantia de um sono tranquilo. Para as equipes de TI, isso significa, literalmente, uma boa noite de sono, pois seu pessoal pode descansar sabendo que os cuidados estarão nas mãos do provedor de MDR – e, assim, todos podem retomar suas vidas.

A assistência de especialistas de alto nível 24 horas, sete dias por semana, garante às equipes de liderança e aos clientes um alto nível de prontidão e pontualidade na poderosa proteção cibernética de seus dados e também da sua organização.

"Saber que a equipe de MDR da Sophos está na retaguarda me devolveu o prazer de um sono tranquilo, porque sei que estamos protegidos as 24 horas do dia."
Vancouver Canucks, Canadá

"O pessoal da Sophos está sempre no gol, protegendo a nossa rede com suas habilidades e profissionalismo e garantindo nossa retaguarda."
Inspire Education Group, Reino Unido

"Agora estamos mais confiantes graças à natureza robusta e abrangente da nossa instalação de segurança."
Aligned Automation, Índia

"A empresa ficou muito mais resiliente com o Sophos MDR."
McKenzie Aged Care Group, Austrália

4. Aumente os conhecimentos, não o número de pessoal

A caça a ameaças é uma operação altamente complexa. As pessoas que trabalham nesse nicho precisam ter um conjunto específico de habilidades, e as características típicas de um caçador de ameaças incluem:

- **Curiosidade e criatividade** – a busca de ameaças pode se comparar a procurar uma agulha no palheiro; os caçadores de ameaças podem passar dias procurando ameaças, usando inúmeros métodos para trazê-las à tona.
- **Experiência em segurança cibernética** – a caça a ameaças é uma das operações mais avançadas na segurança cibernética, portanto, experiência anterior no campo de atuação e conhecimentos básicos são essenciais.
- **Conhecimento do panorama de ameaças** – saber discernir as novas tendências em ameaças é essencial para procurar e neutralizar entidades desconhecidas.
- **Mentalidade antagônica** – a habilidade de pensar como um hacker é fundamental para combater abordagens comandadas por humanos.
- **Habilidade de escrever tecnicamente** – caçadores de ameaças devem registrar suas descobertas como parte do processo de investigação. Portanto, a habilidade de comunicar essas informações complexas é um fator crítico para acompanhar a caçada do início ao fim.
- **Conhecimento de redes e sistemas operacionais** – conhecimento avançado sobre redes e sistemas é essencial.
- **Experiência com scripts e codificação** – necessária para ajudar os caçadores de ameaças a criar programas, automatizar tarefas, analisar logs e realizar tarefas de análise de dados para auxiliar e avançar nas investigações.

Essa lista representa uma rara combinação de competências, exacerbada pela notável falta de pessoal capacitado no setor de TI, o que faz do recrutamento e contratação de especialistas em caça a ameaças uma tarefa árdua – podendo chegar a impossível – para várias organizações.

Os serviços MDR oferecem a perícia de que você precisa. Na Sophos, temos centenas de analistas especializados que fornecem serviços MDR contínuos a clientes mundo afora. O Sophos MDR permite que os clientes aumentem sua capacidade de operações de segurança sem aumentar seu quadro de funcionários.

"Temos uma extensão de nossa própria prática de segurança já existente, sem precisar construir uma estrutura interna."
Hammondcare, Austrália

"O Sophos MDR nos ajudou a enfrentar o crescente volume e sofisticação das ameaças cibernéticas sem aumentar a nossa equipe de operações de segurança."
Tourism Finance Corporation of India Limited, Índia

"Com a Sophos, economizamos de contratar outros cinco novos funcionários para fazer o trabalho."
AG Barr, Reino Unido

5. Aumente o ROI em segurança cibernética

Manter uma equipe de caça a ameaças 24/7 é caro. Para ter cobertura contínua, são necessários pelo menos cinco ou seis profissionais de segurança cibernética trabalhando em turnos alternados. Mas ao aproveitar a economia que os serviços MDR dimensionados oferecem, você assegura uma melhor relação entre custos e benefícios para a sua organização e gera um maior retorno do seu orçamento em segurança cibernética.

Além disso, ao elevar sua proteção, os serviços MDR reduzem significativamente o risco das dispendiosas violações de dados e um possível colapso financeiro de ter que lidar com incidentes ainda maiores. Com a média de custo da remediação de um ataque de ransomware a organizações de médio porte atingindo US$ 1,4 milhão em 2021[6], investir na prevenção é uma sábia decisão.

Se você trabalha com um fornecedor de MDR que também oferece outras formas de segurança cibernética e de endpoint, poderá usufruir de excelentes vantagens do TCO (custo de propriedade), consolidando tudo com um único provedor e canalizando as práticas de gerenciamento do seu fornecedor.

Por fim, ao escolher um fornecedor que se integre às suas tecnologias de segurança, você pode aumentar o retorno de investimentos já existentes. Na Sophos, temos uma abordagem autônoma em relação a fornecedores e serviços MDR, o que nos permite utilizar os seus produtos existentes para a detecção, investigação e resposta a ameaças, aumentando o seu ROI. Com o Sophos MDR, você pode usar nossas excelentes ferramentas de altíssimo nível, ferramentas de outros provedores ou uma combinação dessas ferramentas.

"A Sophos oferece cobertura e trabalho que equivalem a seis equipes em tempo integral, pelo preço de uma."
Detmold Group, Austrália

"Colocar todos os nossos produtos de segurança sob um mesmo teto nos permitiu economizar dinheiro e aumentar nossa eficiência."
Independent Parliamentary Standards Authority, Reino Unido

"O Sophos MDR se paga por si só. Se bloquearmos um incidente sério ao ano, isso já vale dez vezes o investimento, se não mais."
Hammondcare, Austrália

"Economizamos 15 horas por semana e ganhamos 2,6 vezes em produtividade."
Tourism Finance Corporation of India Limited, Índia

6 O Estado do Ransomware 2022, Sophos. Pesquisa independente com 5.600 profissionais de TI em 31 países

O que considerar ao escolher um serviço MDR

Os serviços MDR são diferentes de provedor para provedor. Há muito a considerar quando se trata de avaliar os serviços disponíveis, portanto, esteja certo de explorar as quatro áreas abaixo.

1. **Níveis de suporte e interação oferecidos**

   Você quer um fornecedor de MDR que gerencie totalmente a resposta a ameaças por você, que faça o cogerenciamento com a sua equipe ou que alerte a sua equipe quando uma ação for necessária? Identifique o nível desejado de suporte e interação e compare os fornecedores entre si.

   Na Sophos, trabalhamos como uma extensão das equipes de TI de nossos clientes, nos posicionando de acordo com as suas necessidades. Do suporte total gerenciado 24/7 ao respaldo diversificado à sua equipe interna, estaremos ao seu lado quando e onde for preciso.

2. **Experiência adquirida no tratamento de ameaças**

   Uma experiência profunda em resposta a ameaças cibernéticas leva a melhores defesas. Saiba mensurar o nível de experiência que os analistas de MDR podem acessar e como aplicam seus conhecimentos coletivos às instalações digitais de seus clientes.

   Explore também o nível de expertise em segurança por trás das equipes MDR do fornecedor e a qualidade de seus insights contextuais disponibilizados para ajudar os analistas a priorizar e investigar alertas.

   O Sophos MDR protege mais de 11.000 organizações de diferentes setores em todo o mundo, como saúde, educação, manufatura, varejo, tecnologia, financeiro, governo, serviços e muitos outros setores. Essa grande experiência nos permite oferecer a nossos clientes um nível de proteção inigualável.

   Por trás do Sophos MDR está a equipe Sophos X-Ops. Com mais de 30 anos de expertise em malwares e recursos de IA que lideram o mercado, o Sophos X-Ops oferece insights e análise detalhada para ajudar os agentes de MDR a identificar e neutralizar ataques com grande rapidez.

3. **Experiência diária do cliente**

   Um fornecedor de MDR eficiente se torna uma extensão da sua própria equipe – certifique-se de que você quer realmente trabalhar com eles antes de assinar o contrato. Fale com clientes existentes do fornecedor para saber sobre suas experiências e visite sites independentes de análise para conhecer o feedback a seus serviços.

   O Sophos MDR é o provedor mais bem contado e comentado no Gartner Peer Insights, conforme dados de 1º de agosto de 2022, registrando uma pontuação média de 4,8/5*. Leia depoimentos independentes de clientes aqui.

4. **Experiência adquirida em telemetria**

   Os adversários não seguem uma veia tecnológica única – o mesmo se aplica aos caçadores de ameaças do seu provedor de MDR. Quanto maior a visibilidade analítica do seu ambiente, melhor o trabalho dos analistas em detectar e responder a atividades mal-intencionadas. Pergunte aos fornecedores sobre suas integrações de segurança e a amplitude de integração dos indícios registrados em seu ambiente de TI que eles têm a oferecer.

   O Sophos MDR oferece integrações que se estendem por toda a sua pilha de TI, incluindo integrações nativas e de terceiros a endpoint, rede, nuvem, e-mail e tecnologias Microsoft 365. Nossa abordagem autônoma capacita nossos analistas a terem uma visibilidade ampla do ambiente do cliente, independentemente do seu fornecedor, o que, por sua vez, eleva o nível de detecção, investigação e resposta.

Resumo

Seguindo a evolução desenfreada das ameaças cibernéticas, o MDR rapidamente se transformou em uma peça de proteção indispensável para qualquer tamanho de organização. Trabalhar com um fornecedor de MDR de confiança e altamente reconhecido oferece vários benefícios, independentemente se você terceiriza toda a sua operação de caça a ameaças ou se complementa e aprimora suas operações internas:

1. Eleve as suas defesas cibernéticas.
2. Libere a capacidade de TI.
3. Proteja-se com assistência 24 horas.
4. Aumente os conhecimentos, não o número de pessoal.
5. Aumente o ROI em segurança cibernética.

Para mais informações sobre o Sophos MDR, fale com o seu parceiro Sophos ou acesse www.sophos.com/mdr

www.sophos.com/mdr

A Sophos oferece soluções de segurança cibernética líder do setor para empresas de todos os tamanhos, protegendo-as em tempo real de ameaças avançadas como malware, ransomware e phishing. Com recursos comprovados de última geração, seus dados comerciais ficam protegidos de modo eficiente por produtos que incorporam inteligência artificial e machine learning.

2022-09-16 PTBR-WP (DD)

SOPHOS