Enterprise Strategy Group | Getting to the bigger truth.™

WHITE PAPER DO ESG

Detecção e resposta gerenciadas: um caminho para o crescimento rápido do programa de segurança

Por Dave Gruber, analista principal

Agosto de 2022

Este white paper do ESG foi encomendada pela Dell Technologies
e é distribuída sob licença da TechTarget, Inc.

Conteúdo

Resumo

A aceleração da transformação digital, a rápida adoção da nuvem, um ambiente de ameaças mais complexo e uma escassez contínua de habilidades de segurança estão levando as equipes de segurança ao limite. As soluções de segurança atuais não conseguem acompanhar, forçando muitos a priorizar as iniciativas de modernização do SOC para renovar tecnologias e processos. As megatendências do setor em relação à zero trust e à XDR (extended detection and response, detecção e respostas estendidas) oferecem uma nova visão. No entanto, há uma dificuldade para implementar e operacionalizar implementações eficazes dessas estratégias. Os serviços de MDR (detecção e resposta gerenciadas) estão proporcionando alívio, oferecendo a muitas organizações pessoas, processos e tecnologia necessários para reforçar seus programas de segurança neste ambiente turbulento.

Introdução

À medida que o risco crescente de ataques cibernéticos prejudiciais rouba a participação e o orçamento dos principais objetivos de negócios, as organizações devem responder fortalecendo os programas de segurança cibernética. Para algumas, construir todo o programa de segurança com recursos internos é plausível, mas para a maioria, são necessários recursos de terceiros para permitir o rápido crescimento e a escala do programa.

O ponto central de todos os programas de segurança cibernética são as SecOps (security operations, operações de segurança), responsáveis por monitorar e proteger todos os aspectos da superfície de ataque digital. Abrangendo rede, endpoint, nuvem, identidade, aplicativos e dados, quantidades crescentes de telemetria de segurança e alertas envolvidos em SecOps estão levando as organizações ao seu limite, fazendo com que muitas recorram aos provedores de serviços de MDR para obter apoio.

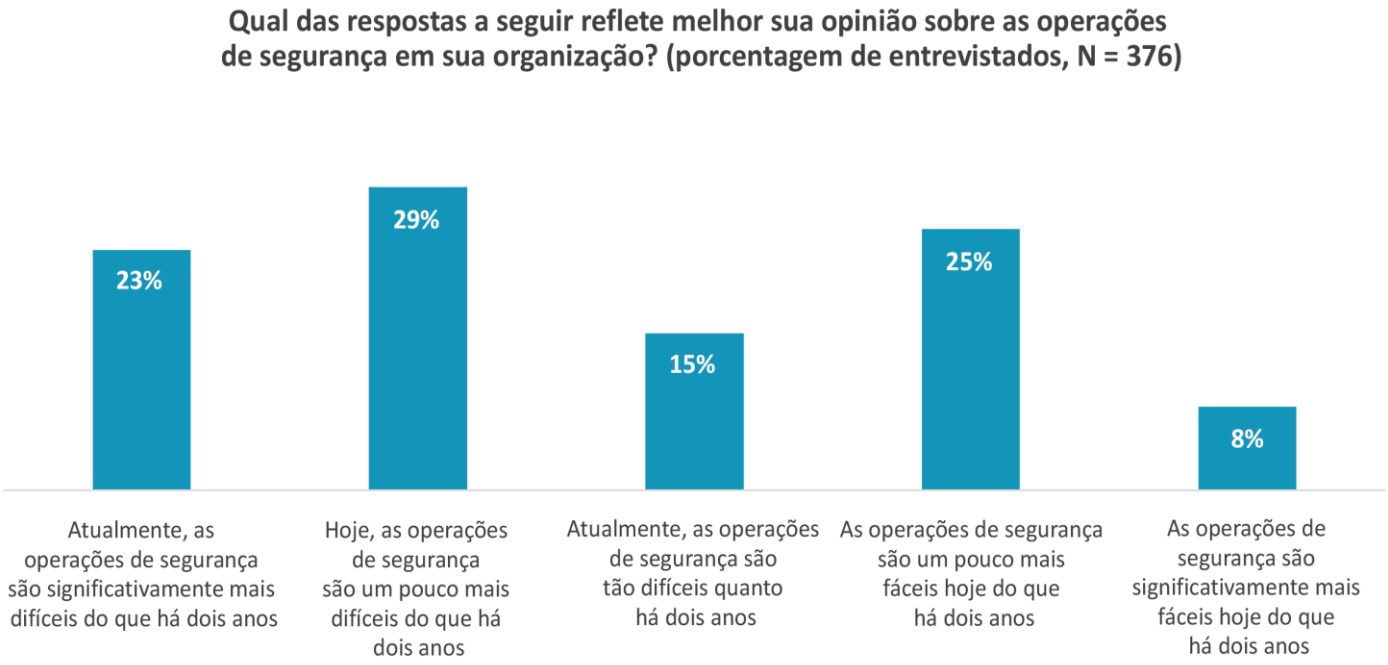
Os provedores de serviços de MDR tornaram-se um mecanismo essencial para essas organizações, fornecendo uma variedade de ofertas de serviços de segurança, como resposta a incidentes, monitoramento ininterrupto, gerenciamento de programas e gerenciamento de riscos. A pesquisa do ESG (Enterprise Strategy Group) indica que os serviços de MDR se tornaram um componente principal das estratégias modernas de segurança cibernética para organizações de todos os tamanhos e maturidade de segurança.

Desafios crescentes das operações de segurança

De acordo com a pesquisa do ESG (consulte a Figura 1), a maioria das organizações reconhece que todo o ambiente de SecOps é mais difícil agora do que há dois anos.[1]

[1] Fonte: resultados da pesquisa completa do ESG, *SOC Modernization and the Role of XDR*, agosto 2022. Todas as referências e gráficos do ESG neste white paper foram retirados deste conjunto de resultados da pesquisa, a menos que indicado de outra maneira.

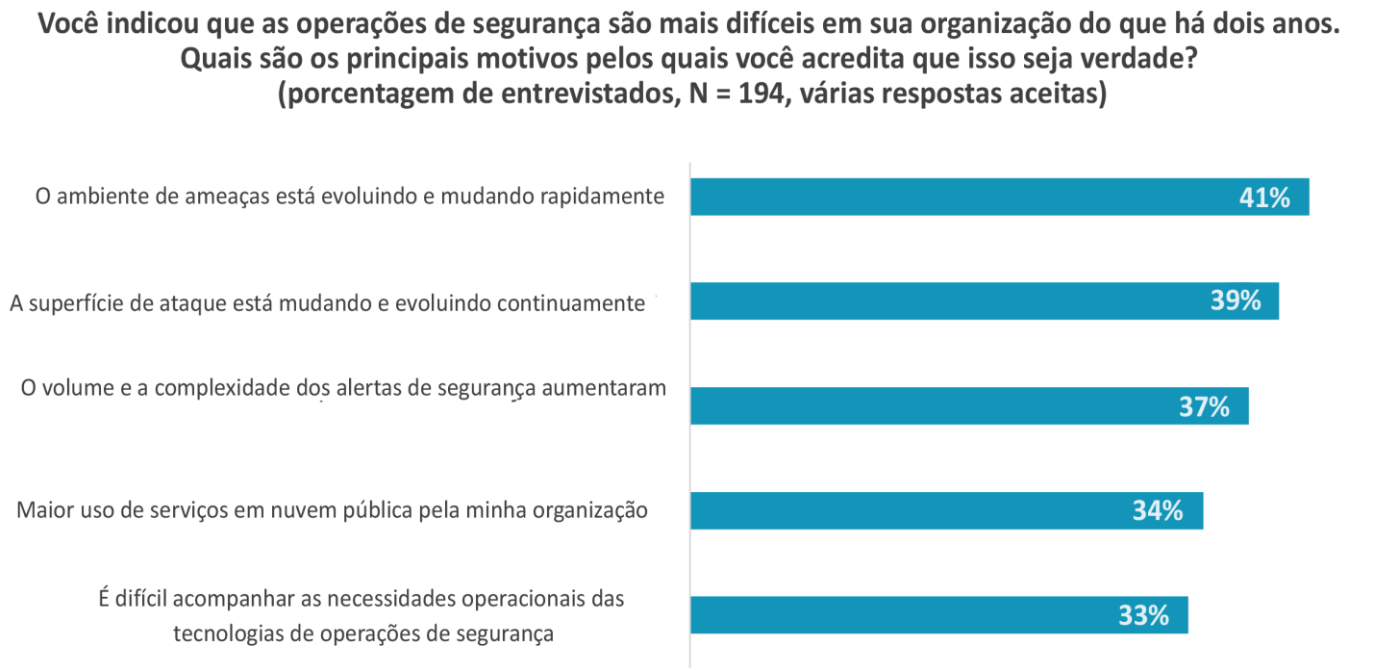
Figura 1. Mais da metade acredita que a SecOps é mais difícil



Fonte: ESG, uma divisão da TechTarget, Inc.

Como mostrado na Figura 2, a pesquisa do ESG também aponta outros desafios que estão tornando a detecção e a resposta mais difíceis do que nunca, como a superfície de ataque em expansão, o crescimento e a diversidade do ambiente de ameaças e o uso cada vez maior de serviços em nuvem para um variedade de aplicações e casos de uso.

Figura 2. Os cinco principais motivos pelos quais a SecOps é mais difícil



Fonte: ESG, uma divisão da TechTarget, Inc.

Modernizar programas de detecção e resposta

As superfícies de ataque e o ambiente de ameaças cresceram em tamanho e complexidade, assim como a utilização de mais controles de segurança, gerando milhares de alertas e grandes quantidades de dados de segurança. Para oferecer suporte à triagem e à investigação de alertas e incidentes, as equipes de segurança devem agregar, correlacionar e analisar esses dados, muitas vezes exigindo imenso processamento manual. Mas é necessário mais além da captura e análise de alertas e dados de segurança.

As equipes de segurança estão repensando as operações gerais do programa para incorporar ainda mais dados de ativos e riscos das equipes de TI e de linha de negócios para se concentrar nas ameaças que representam o risco mais significativo para os objetivos organizacionais. Por exemplo, credenciais de administração de domínio roubadas podem ter uma ampla variedade de potenciais impactos adversos nas operações, nas finanças e na reputação da marca da organização em curto e longo prazo.

À medida que os líderes de segurança repensam as estratégias, cada vez mais organizações transferem as atividades operacionais diárias para terceiros à medida que focam novamente os recursos internos em atividades de segurança mais estratégicas. Como os recursos de segurança internos se concentram na recriação da arquitetura dos processos de operações de segurança, os provedores de serviços de MDR abordam a detecção, a triagem e a resposta de incidentes, tomando medidas rápidas para evitar danos e limitar possíveis disrupções operacionais dos negócios.

Outras organizações buscam de provedores de MDR para obter orientação sobre o desenvolvimento geral do programa, atraindo especialistas e processos comprovados de operações de segurança para otimizar os resultados.

À medida que o movimento de XDR cria ainda mais uma visão e um roteiro para o que é necessário a fim de modernizar os programas de detecção e resposta, outras estão buscando aproveitar os provedores de MDR para ajudar na implementação de soluções de nível de XDR.

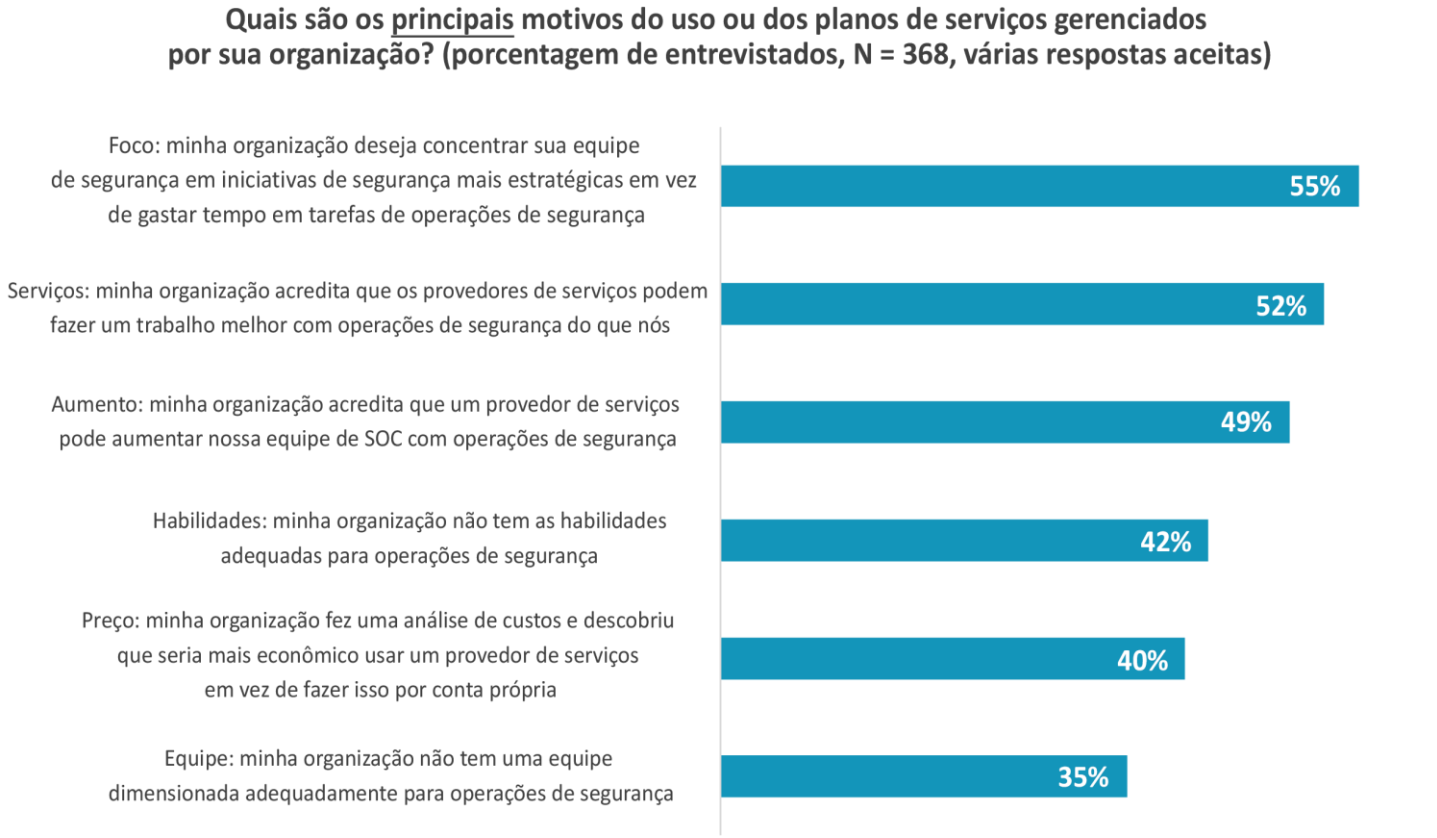
Casos de uso da MDR

Embora muitos provedores de MDR ofereçam uma ampla variedade de serviços de segurança, os principais serviços de detecção e resposta que monitoram, fazem a triagem e investigam alertas geralmente são parte do início dos engajamentos. Os modelos operacionais variam entre os provedores de MDR, portanto, os líderes de segurança devem alinhar cuidadosamente seus requisitos organizacionais individuais com um provedor de MDR que possa cumprir seus objetivos específicos. Por exemplo, alguns líderes de segurança optam por terceirizar totalmente as operações de segurança, envolvendo-se com um provedor de MDR para oferecer cobertura completa da superfície de ataque, monitoramento de ameaças e remediação. Nesse modelo, os provedores de MDR geralmente fornecem a pilha de tecnologia, os processos e os especialistas em segurança necessários para prestar o serviço. Para outros, os serviços de MDR são uma extensão de uma função de operações de segurança interna, adicionando cobertura fora do horário comercial ou especialistas em segurança adicionais a uma equipe interna responsável principalmente pelos conjuntos de tecnologia e pelo processo de operações. Esses são apenas dois exemplos dos muitos casos de uso em que os serviços da MDR são utilizados.

Portanto, a MDR não é uma solução “padronizada”. Em vez disso, geralmente representa um conjunto personalizável de recursos que podem ser aplicados às necessidades de uma organização individual.

Organizações diferentes escolherão um parceiro de MDR para diferentes aspectos de detecção e resposta, dependendo de seus recursos e habilidades internos. A pesquisa do ESG explora os principais motivos na Figura 3.

Figura 3. Por que as organizações estão escolhendo parceiros de MDR



Fonte: ESG, uma divisão da TechTarget, Inc.

Principais motivadores de valor para o engajamento da MDR

O desenvolvimento do programa de segurança exige um foco na eficiência e na eficácia, e os serviços de MDR podem ter um impacto positivo em cada um deles.

- Melhoria operacional e eficiência. A MDR pode ajudar as organizações a reduzir o custo total das operações de segurança de várias maneiras, como infraestrutura, equipe e gerenciamento. Ela também pode resolver o problema de "fadiga de alerta", bem como melhorar a probabilidade de que falsos positivos sejam reduzidos significativamente.

- Maior eficácia da segurança cibernética e redução dos riscos. A MDR pode ajudar as organizações a interromper as ameaças já em andamento, melhorar a detecção de possíveis ameaças e ataques persistentes avançados, ativar a busca proativa de ameaças e detectar controles mais fortes para identificar e impedir ataques futuros.

O que procurar em um Solution Provider de MDR moderno

Lembre-se que as soluções de MDR, em geral, não são novas. Na verdade, elas já existem há algum tempo e estabeleceram um bom histórico de sucesso. Mas muitas soluções de MDR da "geração 1.0" foram projetadas e implementadas para uma era diferente: com menos dados, menos ameaças e detecção mais simples. As soluções de MDR de última geração, e os terceiros que as implementam e gerenciam, devem levar em conta um conjunto mais amplo, profundo e complexo de desafios que tornam a detecção e a resposta mais importantes e difíceis do que nunca.

Ao avaliar soluções de MDR, as organizações devem procurar recursos como:

- Monitoramento 24/7 de eventos e registros, fornecendo informações rápidas e de alta visibilidade sobre atividades e alertas suspeitos por volume, localização e tipo.
- Monitoramento contínuo e escalável de rede e análise de ameaças.
- Recomendações orientadas por IA para opções de resposta contextual.
- Criação de relatórios para obter conformidade com normas.
- Consultores de segurança “humanos” em contato direto com as equipes internas.
- Análise detalhada e em tempo real com base na detecção de ameaças, triagem, investigação e análise forense.
- Avaliações de vulnerabilidades, priorização e orientação de redução.

Ao considerar a grande quantidade de provedores de serviços em potencial que podem oferecer alguns, a maioria ou até mesmo todos os recursos de MDR terceirizados, as organizações devem procurar parceiros que possam oferecer:

- Inteligência de detecção de ameaças contextual.
- Telemetria avançada.
- Histórico comprovado na área de cobertura geográfica da organização, no mercado vertical e no perfil regulamentar.
- Recursos de busca de ameaças demonstrados.
- Um compromisso de longo prazo com a MDR com base em nuvem, utilizando amplos recursos em ambientes de nuvem híbrida e multicloud, zero trust e o modelo de responsabilidade compartilhada de segurança de nuvem.
- Uma capacidade comprovada de dimensionar o serviço ao longo do tempo, com base em tecnologia inovadora, processos comprovados e conhecimento especializado demonstrado pela equipe.

A abordagem da Dell Technologies para MDR

A abordagem da Dell Technologies para detecção e resposta gerenciadas combina tecnologia flexível, inteligente e escalável com profissionais experientes em segurança cibernética. O serviço baseado em assinatura foi projetado para fornecer às organizações previsibilidade de custos e uma mudança perfeita para um nível mais alto de serviço, se e quando for necessário.

A plataforma de tecnologia do Dell Managed Detection and Response é o Taegis XDR, um serviço totalmente gerenciado e nativo na nuvem desenvolvido pela Secureworks, uma empresa da Dell Technologies. O Taegis XDR detecta, analisa e coloca em prática ações considerando ameaças totalmente verificadas em uma superfície de ataque distribuída e diversificada para ajudar a proteger as organizações, que variam de grandes empresas globais a empresas relativamente pequenas.

Os recursos do Taegis XDR são maximizados por meio da experiência e habilidade do grande grupo de analistas e engenheiros de segurança da Dell, cujo conhecimento coletivo abrange décadas de conhecimento especializado, ajudando a proteger as organizações contra ameaças conhecidas e até então desconhecidas. Essa combinação fornece uma maneira eficiente de unificar a detecção e a resposta em toda a arquitetura de TI, em grande parte por meio do seu banco de dados de inteligência de detecção de ameaças atualizado continuamente. O Dell Managed Detection and Response também monitora, analisa e identifica o comportamento do adversário para reduzir o tempo médio de detecção e resposta.

Configurado e implementado como um serviço gerenciado baseado em assinatura, o Dell Managed Detection and Response reduz drasticamente a necessidade das organizações de buscar e recrutar profissionais de segurança para lidar com mais ameaças, ataques e alertas. O Dell Managed Detection and Response complementa e amplia os recursos internos de uma organização de maneira eficiente e eficaz. Como resultado, a equipe interno de SecOps pode concentrar mais tempo e energia em outras tarefas relacionadas à segurança.

Histórias de sucesso: como a MDR funciona no mundo real

O ESG conversou com líderes de TI e segurança dos clientes de MDR da Dell para obter insights sobre casos de uso específicos, modelos operacionais e resultados.

Exemplo nº 1: governo municipal de médio porte

Os recursos de TI e segurança cibernética dos governos municipais raramente correspondem aos de seus colegas do setor privado, mas isso não significa que não enfrentam os mesmos tipos de problemas. Nesse exemplo, um condado de médio porte dos EUA estava se esforçando para enfrentar e superar um número crescente de ameaças à segurança, mas também para manter os gastos dentro de restrições rígidas.

Quando um novo diretor de TI foi contratado, ele imediatamente reconheceu o crescente ambiente de ameaças enfrentado por sua pequena equipe e detectou possíveis vulnerabilidades em seus recursos de detecção e resposta. “Nossa postura de segurança não era boa, mas tínhamos que ser capazes de expandir nossas capacidades sem aumentar a folha de pagamento, um assunto muito delicado para os executivos responsáveis pelas decisões”, disse ele. “Mas eu sei que poderia apelar para suas preocupações de economia fiscal, ao mesmo tempo que apontava a necessidade de abordar nossas vulnerabilidades.”

Ele começou a avaliar o fornecedor de segurança de endpoints do condado, que divulgava um “teste gratuito” de 90 dias de upgrades de software para melhorar a detecção e a resposta. Mas, ao descobrir que o software não tinha funcionalidade para suas necessidades e as comunicações do fornecedor não correspondiam às expectativas, o diretor optou por uma solução de MDR mais abrangente.

“Felizmente, tínhamos um acordo para que a Dell fornecesse um CSO (Chief Security Officer, Diretor de Segurança) virtual. Assim, os líderes dos condados poderiam ficar cientes dos benefícios do uso de uma abordagem de serviços gerenciados, nesse caso, para detecção e resposta.” Ele acrescentou que a equipe da Dell atuou como um complemento, em vez de um substituto, para a pequena equipe interna de profissionais de segurança e TI do condado. “Eles atuaram como uma extensão de nossa equipe e trabalharam com nosso pessoal de maneira perfeita.”

O benefício real do acordo logo ficou claro quando uma campanha global de hackers teve como alvo o webmail do Microsoft Exchange, uma plataforma popular usada por uma ampla variedade de organizações, incluindo o condado. "A Microsoft desenvolveu e enviou um patch assim que descobriu o ataque, mas o dia zero do ataque foi provavelmente um mês antes", disse o diretor de TI do condado. "Fomos contatados pelo nosso CSO virtual da Dell depois do expediente e a equipe de MDR da Dell entrou em ação. Eles nos enviaram scripts para verificar o servidor e rapidamente descobrimos que um deles estava comprometido."

"A Dell (e seus parceiros da Secureworks) realmente sabiam o que estavam fazendo. Participamos de duas a três ligações por dia, diariamente, durante todo o período em que lidamos com a tentativa de violação." Ele diz que a equipe de resposta a incidentes analisou suas descobertas com a equipe do condado, mostrando trechos de código e outras indicações da tentativa de violação e as evidências do comprometimento.

Por fim, eles forneceram uma série de recomendações técnicas e não técnicas que abordaram não apenas o possível impacto da tentativa de violação, mas também reforçaram o perfil de segurança cibernética do país em uma perspectiva e um cronograma mais amplos.

"Nossa experiência nos mostrou que o caminho a seguir ao procurar detecção e resposta aprimoradas é encontrar um especialista em MDR confiável, comprovado e confiável que já tenha passado por isso antes, em vez de tentar encontrar uma maneira barata de fazer upgrade do software de EDR", ele disse. "Não apenas diante dos resultados da tentativa de violação, mas ao trabalhar com eles regularmente, lembro-me da tranquilidade ao saber que temos uma boa equipe trabalhando para nos manter seguros."

Exemplo nº 2: distrito escolar de médio porte

Os distritos escolares historicamente investiram pouco no setor de TI em geral e em segurança cibernética especificamente. Mas, com o ransomware e outros ataques cibernéticos contra distritos escolares em ascensão, as autoridades locais de educação pública têm dificuldade para encontrar maneiras melhores, mais confiáveis e acessíveis de se proteger contra vulnerabilidades.

Por exemplo, um distrito escolar de médio porte dos EUA foi atacado por ransomware e todas as suas operações baseadas em tecnologia foram encerradas. Com 8.500 alunos e equipe espalhados por 21 instalações, o distrito tinha um perfil de TI de tamanho razoável, com 100 servidores físicos e outros 63 servidores virtuais, conectados a mais de 11.000 dispositivos para alunos e funcionários. Claramente, o distrito tinha muitos pontos iniciais em potencial para invasores e precisava de um parceiro que pudesse agir rápido.

Depois de determinar que o ataque de ransomware era real e precisava ser resolvido imediatamente, a equipe de TI do distrito escolar entrou em contato com o Dell Managed Detection and Response. "No segundo dia do ataque, havia dez membros da equipe da Dell aqui", lembrou o diretor de TI do distrito. "Tivemos um relacionamento altamente confiável com a equipe da Dell e eles assumiram o comando imediatamente."

Felizmente, o resultado líquido foi positivo para o distrito. "Dos mais de seis milhões de arquivos em nossos sistemas, apenas seis foram perdidos", afirmou o diretor de TI. "Nunca pagamos a fonte de ameaças. Somos um exemplo real de sobreviventes do ransomware e continuamos a trabalhar com segurança.

"O trabalho com a Dell tem sido uma experiência positiva. Nosso analista de segurança no local está sempre satisfeito depois de conversar com a equipe da Dell. Temos uma postura 95% melhor hoje do que antes de trabalhar com a Dell sobre detecção e resposta gerenciadas."

A maior verdade

À medida que o risco crescente de ataques cibernéticos prejudiciais rouba a participação e o orçamento dos principais objetivos de negócios, as organizações devem fortalecer os programas de segurança cibernética. Embora os casos de uso variem, a maioria está aproveitando os provedores de serviços de MDR para expandir e dimensionar seus programas.

Os provedores de serviços de MDR oferecem um caminho para superar muitos dos desafios reconhecidos na criação de um programa de segurança bem-sucedido, inclusive especialistas em segurança, processos comprovados e tecnologias de segurança escaláveis e fáceis de implementar.

A Dell Technologies reuniu um conjunto totalmente integrado de tecnologia, especialistas em segurança experientes e práticas recomendadas para ajudar as organizações a detectar e responder a ameaças quase em tempo real. Conforme mostrado pelos estudos de caso neste white paper, a Dell Technologies ajudou uma ampla variedade de organizações em diferentes setores e perfis de recursos a impedir o impacto de ameaças emergentes em toda a empresa.

O Enterprise Strategy Group é uma empresa de análise, pesquisa e estratégia de tecnologia integrada que fornece inteligência de mercado, insights acionáveis e serviços de conteúdo de comercialização para a comunidade global de TI.

www.esg-global.com contact@esg-global.com 508.482.0188