DEMONSTRAÇÃO DO ESG

Por que a MDR tornou-se parte integrante das estratégias modernas de segurança cibernética

Data: agosto de 2022 **Autor:** Dave Gruber, analista principal do ESG

RESUMO: ninguém debate a importância dos recursos de detecção e resposta em um programa de segurança cibernética. O grande problema é a melhor maneira de garantir a detecção e a resposta mais adequadas, precisas, confiáveis e consistentes quando as ameaças estão se multiplicando em quantidade e se transformando em termos de complexidade mais rapidamente do que a maioria das organizações consegue se adaptar. A MDR (Managed Detection and Response, Detecção e Resposta Gerenciada) como um serviço gerenciado de terceiros é uma abordagem que permite às organizações acompanhar o ritmo.

Introdução: a chegada do MDR

Todas as organizações enfrentam uma dura realidade: as ameaças de segurança cibernética estão aumentando rapidamente, as superfícies de ataque estão se expandindo e os processos e ferramentas tradicionais para detectar e responder a ameaças não são mais suficientes. Tanto as próprias ameaças quanto as partes que as perpetram são mais adeptos, ágeis e persistentes, criando um alvo de movimentação digital para profissionais de segurança e TI encarregados de proteger os ativos corporativos.

Uma infinidade de controles de segurança aumenta o custo e a complexidade dos esforços de detecção e resposta, exigindo que as equipes de segurança façam uma triagem manual de um fluxo constante de alertas para extrair ameaças válidas de falsos positivos. Construir um SOC (security operations center, centro de operações de segurança) maior e preenchê-lo com mais ferramentas e mais engenheiros de segurança é caro, supondo que as organizações possam identificar e contratar profissionais de segurança suficientes diante da enorme e crescente falta de habilidades de segurança cibernética.

À medida que os programas de segurança cibernética são reformulados, as organizações recorrem cada vez mais aos provedores de detecção e resposta gerenciados para obter ajuda.

À medida que os programas de segurança cibernética são arquitetados novamente, as organizações recorrem com mais frequência aos provedores de detecção e resposta gerenciados para refinar processos, solucionar deficiências de recursos e habilidades, além de modernizar as ferramentas de operações de segurança. Muitos associam a MDR à segurança de endpoint, pois a pesquisa do ESG revela que a necessidade de um serviço de MDR integrado é um fator importante que faz as organizações mudarem seus fornecedores de soluções de segurança de endpoint (consulte a Figura 1).[1]

[1] Fonte: resultados da pesquisa completa do ESG, *Endpoint Security Trends*, dezembro de 2021. Todas as referências e gráficos de pesquisa do ESG nesta demonstração foram retirados deste conjunto de resultados da pesquisa.

Figura 1. Fatores motivadores da mudança de fornecedores de segurança de endpoint

Fonte: ESG, uma divisão da TechTarget, Inc.

No entanto, à medida que as equipes de segurança expandem os programas de detecção e resposta, atualizando para soluções de XDR (extended detection and response, detecção e resposta estendida) mais abrangentes, as ofertas de MDR proporcionam às organizações um caminho para atualizar a tecnologia e os modelos operacionais capazes de fornecer uma cobertura de superfície de ataque mais abrangente e detecção avançada de ameaças. Novas abordagens são necessárias, combinando monitoramento 24 horas por dia, inteligência global de ameaças em tempo real, automação e análise avançada de aprendizado de máquina, todas capazes de trabalhar com grandes quantidades de telemetria de segurança para oferecer suporte à detecção rápida e busca de ameaças. Enquanto a XDR continua a evoluir e amadurecer, os serviços da MDR podem permitir que organizações de todos os portes e níveis de maturidade de segurança operacionalizem a detecção e a resposta, resultando na redução de ameaças avançadas. Isso é importante à medida que as organizações redefinem o escopo e a escala dos limites de segurança cibernética, desde o data center até a borda e a nuvem. A MDR reúne as pessoas, os processos e as tecnologias necessários para estender os casos de uso de detecção e resposta a ameaças em toda a empresa distribuída.

Principais motivadores para a adoção da MDR

O uso de serviços da MDR está aumentando, oferecendo às equipes de segurança um caminho para estender a cobertura, solucionar problemas de falta de funcionários na equipe e fortalecer os objetivos gerais do programa. Os casos de uso variam, mas os fatores motivadores subjacentes incluem:

- Ambiente de ameaças: a quantidade de ataques cibernéticos e a sofisticação cada vez maior deles têm colocado uma enorme pressão sobre as organizações para detectar e responder de maneira mais rápida e definitiva.
- Intenção do adversário: os adversários se tornaram mais inteligentes, persistentes e ainda mais estratégicos na maneira como planejam e fazem os ataques. Um avançado "ecossistema criminoso" surgiu, em que invasores mal-intencionados compartilham táticas e até mesmo colaboram em ataques.
- Economia: o compromisso do CapEx com a criação e a expansão de um SOC é substancial, normalmente uma despesa de sete dígitos e, às vezes, ainda mais.
- Atualização da tecnologia de segurança cibernética: a pilha de controles de segurança cibernética deve ser atualizada com mais frequência para organizações que executam todas ou a maior parte de suas atividades de operações de segurança internamente. Isso inclui a mudança da detecção e resposta de endpoint de primeira geração para uma estrutura de XDR/MDR mais abrangente.
- Escassez de habilidades: a grande carência de habilidades de segurança cibernética é um problema perene. A incapacidade de posicionar adequadamente a segurança cibernética interna resulta em desafios na detecção e nos objetivos de resposta, colocando os ativos em risco.

Os ataques cibernéticos são indiscriminados. As organizações de pequeno e médio porte, com equipe e orçamento limitados, além de exposição prévia a todos os tipos de ataques, estão em risco. Até mesmo organizações de grande porte precisam de equipes complementares, controles escaláveis e consultoria de nível executivo sobre estratégias para detectar e responder ao ambiente de ameaças em evolução.

O que procurar em um serviço de MDR e um provedor de serviços de MDR

Há alguns requisitos importantes e complexos para qualquer organização que esteja avaliando um serviço de MDR incluindo:

- Inteligência contextual contra ameaças: habilite a inteligência e a detecção de ameaças em tempo real, inclusive a correlação de vários indicadores para identificar ameaças ou descartar falsos positivos.
- Casos de uso proativos: forneça suporte à busca ativa de ameaças conhecidas.
- Telemetria avançada: realize investigações forenses profundas e com lógica analítica sofisticada, que são particularmente importantes para identificar ameaças novas e emergentes.
- Correção: forneça orientação de correção específica ao contexto e orientada por IA.
- Diminuição de risco: avaliação e gerenciamento de vulnerabilidades.

Quando se trata de selecionar um provedor de serviços de MDR, as organizações devem procurar parceiros que possam fornecer recursos específicos e demonstrados incluindo:

- Cobertura 24x7: forneça monitoramento contínuo 24x7.
- Planejamento e consultoria para cenários "e se".

- Conhecimento especializado e experiência por parte do provedor de serviços.
- Orientação para executivos e membros da diretoria.
- Capacidade de garantir a governança, a conformidade e a continuidade dos negócios.

Além disso, as organizações devem perguntar aos possíveis parceiros da MDR sobre os objetivos de nível de serviço. Essas funções incluem o tempo médio para reagir do alerta ao início da investigação, o tempo médio para responder da iniciação da investigação ao momento em que uma análise de incidentes é fornecida à organização e o tempo médio para resolver desde o início da investigação até o momento em que a resolução completa foi realizada.

A abordagem da Dell Technologies para MDR

Identificar, avaliar e fazer parcerias com um provedor de serviços de MDR exige que as organizações se concentrem não apenas em suas necessidades atuais de detecção e resposta a ameaças, mas também em como essas necessidades provavelmente vão evoluir e se expandir no futuro. Embora nenhuma organização consiga prever o futuro das ameaças à segurança cibernética, as organizações devem procurar um parceiro de MDR com capacidade comprovada de dimensionar seus serviços ao longo do tempo com base em tecnologia inovadora, processos comprovados e o conhecimento especializado demonstrado pela equipe.

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 unidade de negócios da Dell. 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.

O Taegis XDR é fortalecido ainda mais pelas habilidades 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 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.

O Dell Managed Detection and Response também monitora, analisa e identifica comportamentos adversários para reduzir o tempo médio de detecção e resposta.

Por fim, como esse é um serviço gerenciado, o Dell Managed Detection and Response reduz drasticamente a necessidade das organizações de buscar e recrutar profissionais de segurança para equipes internas de TI e operações de segurança já sobrecarregadas. Ele foi projetado para complementar e ampliar os recursos das próprias organizações de maneira econômica e estratégica.

A maior verdade

A superfície de ataque em rápida expansão, os ataques repetidos de ransomware e um ambiente de ameaças geralmente mais complexo promovem a força e o investimento no XDR e na MDR à medida que as organizações modernizam os programas de detecção e resposta a ameaças. Embora as estratégias de segurança individuais variem, a necessidade de uma visão mais ampla da superfície de ataque e a capacidade de agregar, correlacionar e analisar grandes quantidades de dados de segurança dos controles de segurança individuais que os protegem são uma etapa importante para obter o controle.

Os serviços gerenciados de detecção e resposta são eficazes e estão prontamente disponíveis, pois as equipes de segurança aproveitam os provedores de MDR para fortalecer habilidades, processos e tecnologias de segurança. A pesquisa do ESG mostra que as organizações que investem em XDR desejam serviços de MDR complementares para ajudar a implementar e operar essas soluções. Isso significa envolver-se com solution providers que tenham um histórico comprovado no fornecimento de soluções e serviços de segurança. Quando aplicado ao longo do tempo, isso pode ajudar as equipes de TI e segurança a desenvolver e dimensionar os programas de segurança.

O ESG recomenda explorar soluções de MDR de empresas como a Dell Technologies, que contam com equipes, processos e tecnologias para ajudar as organizações a atingir esses objetivos.

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