Enterprise Strategy Group | Getting to the bigger truth.™

Como fechar lacunas nas operações de segurança com MDR

À medida que aumenta o risco de ataques cibernéticos prejudiciais que afetam o reconhecimento dos clientes e ocupam o orçamento dos principais objetivos dos negócios, as organizações devem responder fortalecendo os programas de segurança cibernética. Uma parte central de todos os programas de segurança cibernética são as operações de segurança (SecOps), responsáveis por monitorar e proteger todos os aspectos da superfície de ataque digital.

Apesar dos investimentos, as operações de segurança estão mais difíceis

MAIS DA METADE
dos entrevistados acredita que a SecOps é **mais difícil** agora do que há dois anos.

» **Cinco principais motivos que explicam por que a SecOps é mais difícil.**

1. **41%** O ambiente de ameaças está evoluindo e mudando rapidamente
2. **39%** A superfície de ataque está mudando e evoluindo continuamente
3. **37%** O volume e a complexidade dos alertas de segurança aumentaram
4. **34%** Maior uso de serviços em nuvem pública pela minha organização
5. **33%** É difícil acompanhar o ritmo das necessidades operacionais das tecnologias de operações de segurança

Como repensar as estratégias dos programas

As superfícies de ataque e o ambiente de ameaças cresceram em tamanho e complexidade, assim como a utilização de controles de segurança, gerando milhares de alertas e volumes gigantescos de dados de segurança. As equipes de segurança estão repensando as operações gerais dos programas para incorporar ainda mais dados de ativos e riscos das equipes de TI e da linha de negócios para se concentrar nas ameaças que representam o risco mais significativo para os objetivos organizacionais.

98% das organizações já trabalham com um provedor de MDR ou planejam fazer isso nos próximos 12 meses.

88% dessas organizações planejam aumentar o uso de MDR nos próximos 12 meses.

» **Principais fatores da integração de MDR que agregam valor.**

MELHORIA E EFICIÊNCIA OPERACIONAIS.
O MDR pode ajudar as organizações a reduzir de várias maneiras o custo total das operações de segurança, como infraestrutura, equipe e gerenciamento. Ele também pode resolver o problema da "fadiga de alertas" e melhorar a probabilidade de reduzir significativamente os falsos positivos.

MELHORIA DA EFICÁCIA DA SEGURANÇA CIBERNÉTICA E REDUÇÃO DOS RISCOS.
O MDR pode ajudar as organizações a deter as ameaças já em andamento, melhorar a detecção de possíveis ameaças e ataques avançados persistentes, ativar a busca proativa de ameaças e institucionalizar controles mais fortes para identificar e impedir os ataques futuros.

» **Principais motivos pelos quais as organizações usam ou planejam usar serviços gerenciados.**

55%
Foco:
Minha organização deseja concentrar a equipe de segurança em iniciativas de segurança mais estratégicas, em vez de gastar tempo em tarefas de operações de segurança.

52%
Serviços:
Minha organização acredita que os provedores de serviços podem fazer um trabalho melhor do que nós com as operações de segurança.

49%
Ampliação:
Minha organização acredita que o provedor de serviços pode ampliar nossa equipe de SOC com operações de segurança.

42%
Habilidades:
Minha organização não tem as habilidades adequadas para as operações de segurança.

> **Muitas soluções de MDR da "geração 1.0" foram projetadas e implementadas para uma era diferente:** menos dados, menos ameaças, detecções mais simples."
>
> *- Dave Gruber, analista diretor do ESG*

Novos requisitos de MDR

Muitas soluções de MDR da "geração 1.0" foram projetadas e implementadas para uma era diferente: menos dados, menos ameaças, detecções mais simples. A última geração de soluções de MDR deve estar equipada para proteger uma superfície de ataque mais diversificada, detectar ameaças mais complexas e empregar uma abordagem mais centrada em riscos para garantir a priorização e a redução.

- Monitoramento 24x7 de eventos e registros.
- Informações rápidas e de alta visibilidade sobre atividades suspeitas e alertas por volume, localização e tipo.
- Monitoramento contínuo e escalável da rede e análises de ameaças.
- Recomendações orientadas por IA para opções de resposta contextual.
- Geração de relatórios sobre 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 para a redução.

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

- Inteligência de detecção contextual.
- Histórico comprovado na área de cobertura geográfica da organização, no mercado vertical e no perfil regulamentar.
- Recursos demonstrados de busca de ameaças.
- Um compromisso em longo prazo com o MDR baseado em nuvem.
- Recursos abrangentes em ambientes de nuvem híbrida e multicloud, Zero Trust e o modelo de responsabilidade compartilhada da segurança na nuvem.
- A capacidade comprovada de dimensionar o serviço ao longo do tempo com base em tecnologias inovadoras, processos comprovados e conhecimento especializado demonstrado pela equipe.

A grande verdade

À medida que aumenta o risco de ataques cibernéticos prejudiciais que afetam o reconhecimento dos clientes e ocupam o orçamento dos principais objetivos dos negócios, as organizações devem fortalecer os programas de segurança cibernética. Embora os casos de uso variem, a maioria está recorrendo a provedores de serviços de MDR para expandir e dimensionar os respectivos programas.

A abordagem de detecção e resposta gerenciadas da Dell Technologies combina uma tecnologia flexível, inteligente e escalável com profissionais experientes de segurança cibernética, ajudando organizações de todos os portes e perfis de recursos a acelerar e fortalecer os programas de segurança.

SAIBA MAIS

DELL Technologies

Fonte: ESG Complete Survey Results, *SOC Modernization and the Role of XDR*, agosto de 2022.