Domine a Cibersegurança com MDR:

O Guia Definitivo para Detecção e Resposta Gerenciada

Cybersecurity
Progress. Protected.

Introdução: Uma Abordagem Preventiva em Camadas

O mundo está mudando mais rápido do que muitos defensores de rede conseguem acompanhar. Eles enfrentam um adversário ágil e determinado, armado com as mais recentes tecnologias. À medida que a superfície de ataque das empresas se amplia com cada novo investimento digital, aumentam as possibilidades e os custos de uma violação grave de segurança. O custo médio de uma violação de dados em todo o mundo atualmente chega a quase 4,9 milhões de dólares..

IPara gerenciar esses riscos crescentes, as organizações devem considerar adotar uma abordagem proativa que priorize a prevenção, projetada para minimizar a superfície de ataque, reduzir os custos e a complexidade, e melhorar a cibersegurança.

Mais da metade das organizações que sofreram violações enfrentam altos níveis de escassez de pessoal de segurança. Esse problema representou

26.2%

entre 2023 e 2024.

Fonte: *IBM: Relatório do Custo de uma Violação de Dados 2024*.

As ciberameaças precisam ter sucesso apenas uma vez para causar danos significativos. Por isso, a abordagem mais avançada da cibersegurança corporativa combina prevenção em camadas com detecção e resposta. No entanto, o desafio enfrentado por muitas organizações é que:

A FALTA DE COMPETÊNCIAS E A ESCASSEZ DE CONHECIMENTO afetam a capacidade de realizar operações de segurança 24/7/365 (SecOps).

A COMPLEXIDADE das ferramentas de detecção e resposta significa que algumas empresas podem não ter ninguém na equipe para operá-las.

AS AMEAÇAS CIBERNÉTICAS SÃO CADA VEZ MAIS SOFISTICADAS e impactantes, permitindo que as ciberameaças alcancem seus objetivos com maior rapidez.

OS ORÇAMENTOS SÃO LIMITADOS, especialmente para grandes aquisições de infraestrutura de detecção e resposta e operadores humanos.

AS PRESSÕES DE CONFORMIDADE ESTÃO AUMENTANDO, o que amplia o impacto negativo dos ataques em caso de não conformidade.

Por isso, **muitas organizações estão recorrendo à Detecção e Resposta Gerenciada (MDR).**Ao fazer isso, podem acessar o poder combinado de uma equipe especializada de SecOps de terceiros que utiliza ferramentas sofisticadas de IA para uma resposta rápida e a contenção de ameaças. Os melhores serviços de MDR automatizam o monitoramento e a geração de relatórios para melhorar a conformidade e a melhoria contínua da cibersegurança. Isso libera as equipes internas para se concentrarem em tarefas estratégicas de maior valor para a empresa.

$4.88 Milhões

Foi o custo médio global de uma violação de dados em 2024, representando o maior aumento desde a pandemia.
Fonte: *IBM: Relatório do Custo de uma Violação de Dados 2024*

Capítulo 1: Por que sua empresa precisa de MDR

As organizações atuais continuam desenvolvendo infraestruturas e aplicações em nuvem, apoiando o trabalho remoto e ampliando suas cadeias de suprimentos digitais e tradicionais. Isso oferece mais oportunidades para cibercriminosos altamente motivados, que cada vez mais utilizam IA e ferramentas automatizadas, ofertas "como serviço" e outros recursos para aprimorar suas habilidades, profissionalizar-se e ampliar os ataques. Nesse contexto, **o MDR está se tornando uma necessidade para empresas de todos os tamanhos**.

DA PREVENÇÃO AO MDR

IAs equipes internas de segurança se esforçam para gerenciar o volume, a variedade, a velocidade e, em alguns casos, a sofisticação das ameaças enfrentadas por suas organizações. O ransomware é uma das mais graves. O ransomware como serviço (RaaS) é uma "indústria" clandestina altamente competitiva, na qual os grupos inovam continuamente para burlar os controles de segurança e aumentar seus lucros. Segundo especialistas em segurança do governo britânico, espera-se que a ameaça aumente à medida que mais adversários tenham acesso a ferramentas de inteligência artificial.

Espera-se que a frequência dos ataques de ransomware a governos, empresas, consumidores e dispositivos aumente

Cada 2 segundos em 2031

Fonte: *Cybercrime Magazine: As 10 principais previsões e estatísticas sobre cibersegurança para 2024*

"Os serviços de IA reduzem as barreiras de entrada, aumentando o número de cibercriminosos, e potencializarão sua capacidade ao melhorar a escala, a velocidade e a eficácia dos métodos de ataque existentes."

James Babbage, Director General for Threats at the National Crime Agency.

Os cibercriminosos estão utilizando essas ferramentas para reduzir o tempo entre o acesso inicial e o roubo de dados ou a implantação de ransomware. Trata-se de um desafio não apenas no contexto do ransomware, mas em toda a gama de ameaças enfrentadas pelas organizações, desde malware de mineração de criptomoedas e redes de bots até trojans bancários e spyware.

O impacto cumulativo dessas tendências deve direcionar a atenção dos responsáveis pela segurança da informação para uma verdade inevitável: a motivação dos cibercriminosos para ter sucesso muitas vezes é maior do que a preparação das empresas por meio de medidas preventivas. Eles fazem de tudo para entrar no ambiente corporativo sem serem detectados. Por isso, as organizações devem **equilibrar a prevenção com detecção e resposta**. É nisso que se concentra a abordagem de prevenção da ESET, **combinando múltiplas camadas de tecnologia de segurança**. O objetivo é proteger bloqueando códigos ou agentes maliciosos antes que entrem ou causem danos ao sistema do usuário.

O phishing foi o vetor de ataque mais caro e frequente em 2024, com um custo de

€4.88 Milhões

E uma taxa de

15% de participação

Entre todos os ataques.

Fonte: *IBM: Relatório do Custo de uma Violação de Dados 2024*.

No entanto, se essas medidas forem burladas por cibercriminosos sofisticados, existe detecção e resposta rápidas e confiáveis para mitigar ameaças avançadas que consigam comprometer um sistema. Pense nisso como trancar todas as portas e janelas, mas também instalar alarmes de movimento para identificar atividades suspeitas caso alguém consiga entrar na casa.

O XDR é um ativo essencial. Ele permite que as equipes de operações de segurança (SecOps) **obtenham visibilidade sem precedentes** de seu ambiente de TI a partir de um único painel e detectem anomalias que indiquem ameaças por meio de alertas de alta fidelidade. O XDR é uma evolução do EDR, que otimiza a detecção, investigação, resposta e caça a ameaças em tempo real.

O XDR unifica as detecções de endpoints relevantes para a segurança com a telemetria de ferramentas empresariais e de segurança, como análise e visibilidade de rede (NAV), segurança de e-mail, gestão de usuários e acessos, segurança em nuvem, entre outros. Trata-se de uma plataforma nativa em nuvem construída sobre uma infraestrutura de big data para fornecer às equipes de segurança flexibilidade, escalabilidade e oportunidades de automação.

O XDR PERMITE RESPONDER A VÁRIAS PERGUNTAS-CHAVE SOBRE UM CIBERATAQUE

Como começou?
Onde começou?
Quando começou?
Quais endpoints estão infectados?
Foi contido?
Como podemos preveni-lo no futuro?

E, mais importante, pode ajudar a tomar medidas corretivas rápidas para resolver incidentes antes que afetem gravemente a organização.

No entanto, mesmo com a ajuda do XDR, as equipes de SecOps enfrentam **grandes desafios** do ponto de vista organizacional, especialmente no que diz respeito à falta de conhecimento, à complexidade das ferramentas, às limitações de orçamento e recursos e à integração entre soluções, sem mencionar a rápida evolução do cenário de ameaças. **Por isso, muitos estão recorrendo ao MDR**; a forma mais eficaz de detectar e conter ameaças sofisticadas e em constante mudança.

COMO O MDR ABORDA AS AMEAÇAS ATUAIS

Embora o MDR varie de um provedor para outro, ele deve incluir pelo menos alguma variação do seguinte:

- **Monitoramento e detecção de ameaças 24/7**:
  Monitoramento contínuo da rede, dos endpoints e dos ambientes em nuvem de uma organização.

- **Caça proativa a ameaças**:
  Diferentemente das medidas de segurança tradicionais que reagem a alertas, o MDR envolve a detecção proativa de ameaças, ajudando a identificar APTs e vulnerabilidades de dia zero.

51%

é o número

de organizações que estabeleceram formalmente metodologias de caça a ameaças em 2024, em comparação com 35% em 2023.
Fonte: *SANS: A evolução da caça a ameaças corporativas: insights detalhados da pesquisa SANS 2024*.

- **Análise e resposta de especialistas**:
  A experiência dos profissionais de segurança permite uma análise detalhada e uma tomada de decisão rápida, o que é crucial para lidar com incidentes de segurança complexos.

- **Inteligência global de ameaças**:
  A telemetria precisa, atual e relevante coletada em todo o mundo fornece inteligência acionável para uma resposta rápida a incidentes e uma detecção de ameaças otimizada.

As organizações que utilizam telemetria podem alcançar até

60% de melhora

em sua capacidade de gerenciar vulnerabilidades e ameaças, em comparação com aquelas que se baseiam apenas em medidas de segurança tradicionais.
Fonte: *Forrester: Os quatro passos para uma segurança mais proativa, 2024*.

- **Melhoria contínua**:
  Ao analisar incidentes passados, utilizar inteligência avançada de ameaças, focar nas ameaças reais e fornecer verificações e relatórios periódicos sobre o estado da segurança, os serviços de MDR ajudam a prevenir a repetição de ataques semelhantes, permitindo que as equipes aumentem a resiliência cibernética.

FUNÇÕES-CHAVE DO MDR

O MDR pode trazer enormes benefícios para organizações que desejam mitigar riscos cibernéticos, mas que não dispõem dos recursos internos necessários, ajudando-as a preencher lacunas de competências, reduzir custos e melhorar a detecção e a resposta. Uma solução de alto desempenho deve permitir que as organizações:

Monitorar
Cibercriminosos experientes acompanham todo o ambiente de TI do cliente e monitoram ativamente malware e grupos APT para fornecer o mais alto nível de consciência situacional.

Detectar
Os cibercriminosos têm inúmeras maneiras de contornar as defesas perimetrais, mas ao aproveitar a análise comportamental, podem ser detectados para uma rápida correção.

Triagem
Uma avaliação inicial e a categorização dos alertas filtram os falsos positivos e coletam as informações necessárias.

Priorizar

Análises inteligentes classificam esses alertas por gravidade para garantir que as ameaças mais críticas sejam tratadas primeiro. Esta é uma fase essencial do fluxo de trabalho de MDR, já que muitas equipes de TI enfrentam sobrecarga de alertas.

Investigar

Ferramentas automatizadas e a experiência humana se combinam para aprofundar as alertas, realizando análises de dados e logs para compreender sua natureza e alcance. Será necessário avaliar se uma alerta é um verdadeiro positivo ou não e quais passos devem ser tomados para resolvê-la.

Responder

Um serviço de MDR eficaz fornecerá ações básicas de resposta para bloquear e conter a ameaça, ou então a contenção e a remediação completa dos sistemas comprometidos. Isso pode incluir redefinição de senhas, aplicação de patches em endpoints específicos ou até a restauração dos computadores.

As vantagens de terceirizar a detecção e resposta são simples, mas contundentes:

- O provedor de MDR cuida de toda a gestão da tecnologia de back-end, liberando a equipe para focar em tarefas estratégicas de alto valor, em vez de lidar com o excesso de alertas de segurança.
- O provedor de MDR também pode otimizar a tecnologia de back-end para alinhá-la ao perfil de risco e à infraestrutura de cada cliente.
- Com a detecção e resposta gerenciadas por um terceiro, não há necessidade de pagar salários elevados para atrair e reter os melhores talentos em cibersegurança.
- Os clientes podem se beneficiar das economias de escala do provedor, de sua capacidade de atrair talentos e do conhecimento adquirido com outras organizações e diferentes cenários de ameaças.

CARACTERÍSTICAS ESSENCIAIS QUE DEVEM SER BUSCADAS EM UMA SOLUÇÃO MDR

Com tantas soluções de MDR inundando o mercado, pode ser difícil saber por onde começar. Considere um provedor capaz de oferecer pelo menos o seguinte:

Integração rápida e precisa

As regras de detecção, as exclusões e os parâmetros devem ser personalizados para cada ambiente de TI e para as ameaças enfrentadas pela organização. Uma integração mais rápida é desejável, mas não se isso comprometer o desempenho da detecção, que deve ser otimizado desde o primeiro dia.

➜ Lembre-se de que a proteção MDR geralmente melhora com o tempo.

Velocidade

Reduza o tempo de detecção e resposta a incidentes de meses para minutos com seu provedor de MDR. É necessário interromper o ataque nas fases iniciais (descoberta, movimento lateral, persistência) antes que a carga útil seja executada.

Serviço 24/7

Os cibercriminosos operam em todos os fusos horários e frequentemente atacam de madrugada, nos fins de semana ou em feriados. Isso significa que o MDR deve trabalhar 24 horas por dia. Os indicadores de comprometimento e ataque devem ser investigados imediatamente, em tempo real.

Solução fácil de usar, com interface simples e curva de aprendizado baixa

É acessível até para quem está começando na segurança da informação. O painel de controle fácil de usar oferece uma visão clara do estado da segurança e dos alertas importantes.

Compatibilidade perfeita com diversas infraestruturas

Integração eficaz com ferramentas como SIEM, SOAR, sistemas de tickets e muitas outras. Seja em ambientes com múltiplos sistemas operacionais, software de segurança já existente ou configurações locais e em nuvem, o ideal é contar com uma integração sem complicações.

Uma plataforma tecnológica completa

Uma parte essencial de uma solução MDR é a tecnologia subjacente. Ela deve incluir detecção e resposta estendidas (XDR), gerenciamento de eventos e informações de segurança (SIEM) e orquestração e resposta de segurança (SOAR). Tudo isso deve ser fornecido pelo provedor de MDR ou por ferramentas de terceiros conectadas por meio de APIs.

Automação e IA

A IA pode desempenhar um papel importante na identificação de comportamentos anômalos e na análise de grandes volumes de dados para detectar sinais de comprometimento ou ataque.

A automação também pode executar rapidamente um conjunto de ações para isolar sistemas e conter ameaças. No entanto, deve sempre ser considerada como um suporte, e não como substituto da experiência dos analistas humanos.

Inteligência humana

Por mais importantes que sejam a IA e a automação, elas têm limitações que apenas especialistas humanos podem abordar de forma eficaz. Profissionais experientes em cibersegurança podem adicionar uma compreensão contextual das anomalias de comportamento identificadas pela IA para determinar se um alerta é realmente malicioso. Isso ajuda a reduzir falsos positivos. Os humanos também são mais capazes de se adaptar a ameaças novas e emergentes em tempo real.

Notificações personalizáveis e opções avançadas

→ de geração de relatórios

Para receber automaticamente ou sob demanda relatórios sobre incidentes, o estado do ambiente e outras atualizações.

Isso facilita a apresentação do status da cibersegurança aos executivos, a recepção de alertas oportunos e a geração de relatórios acionáveis para auditorias e conformidade regulatória.

Correção

Não existe uma norma definida sobre se o provedor de serviços ou o cliente deve ser responsável pela correção ou mitigação após a detecção de uma ameaça. Os compradores de TI devem buscar a solução que melhor se adapte às suas necessidades e capacidades internas.

Inteligência sobre ameaças

A atualização constante das informações sobre ameaças, fornecida pelo provedor de MDR ou por terceiros, é essencial para um serviço MDR eficaz. O XDR integra as detecções de endpoints com a telemetria de ferramentas de segurança e empresariais, como análise e visibilidade de rede (NAV), segurança de e-mail, gestão de usuários e acessos, segurança na nuvem, entre outros. É uma plataforma nativa na nuvem, construída sobre uma infraestrutura de big data, que oferece flexibilidade e escalabilidade para as equipes de segurança.

Alinhamento

Certifique-se de que o serviço MDR esteja alinhado operacionalmente com o restante do ambiente de TI, por exemplo, se os resultados se integram aos sistemas de gerenciamento de tickets e aos fluxos de trabalho internos. Um provedor deve ser capaz de gerar relatórios de incidentes e atualizações de status para garantir total transparência.

Busca

Qualquer serviço MDR deve incluir, como padrão, uma busca contínua e sistemática de ameaças, com o objetivo de erradicar os ataques mais evasivos.

Conformidade

O serviço MDR deve ser capaz de atender aos requisitos de privacidade, residência ou retenção de dados do cliente, assim como às disposições exigidas pelas apólices de seguro.

Espera-se que o mercado de MDR cresça a uma taxa composta de crescimento anual (CAGR) de cerca de

24%

De 2024 a 2029.

Fonte: *MarketsAndMarkets: Mercado de Detecção e Resposta Gerenciada (MDR), 2024*.

Capítulo 2: Implementação de MDR com a ESET

A ESET oferece um dos serviços de MDR mais rápidos e eficazes do mercado. A chave de seu poder é a combinação bem-sucedida de humanos e máquinas. Isso inclui pesquisa de segurança e inteligência de ameaças de classe mundial — construída sobre mais de 30 anos de experiência e 11 centros de Pesquisa e Desenvolvimento — além de capacidades avançadas de IA para identificar comportamentos anômalos que poderiam passar despercebidos aos olhos humanos.

Além disso, as equipes de prestação de serviços do ESET MDR estão distribuídas por todo o mundo, o que ajuda os clientes a superar barreiras linguísticas e torna toda a experiência mais fluida.

Para clientes empresariais: a ESET oferece MDR em dois níveis. O ESET MDR é um serviço poderoso, porém acessível, projetado para atender às necessidades de PMEs a partir de 25 usuários. Já o ESET MDR Ultimate é um serviço altamente personalizado, adaptado aos requisitos específicos e ao perfil de segurança de clientes corporativos.

Ele funciona como uma extensão perfeita da função de TI do cliente, independentemente do seu setor, e oferece uma completa Resposta Digital Forense a Incidentes (DFIR). O resultado é um MDR de nível empresarial, projetado para enxergar mais e agir mais rápido, com o objetivo de detectar e conter proativamente as ameaças antes que possam causar danos.

Para provedores de serviços gerenciados (MSP): a ESET entende que seu negócio também pode enfrentar limitações de recursos, especialmente ao apoiar potencialmente centenas de clientes através de uma superfície de ataque em expansão. Sua organização se torna um alvo cada vez mais atraente, por exemplo, como meio para que cibercriminosos acessem remotamente os ambientes dos clientes.

Com o ESET MDR, é possível diversificar seu portfólio com detecção e resposta rápidas (em potencialmente apenas 20 minutos) e otimizar os recursos internos para continuar oferecendo o melhor serviço possível aos clientes.

MDR COMO PARTE DA SEGURANÇA INTEGRAL

Os serviços ESET MDR ou ESET MDR Ultimate podem ser adquiridos como parte de níveis específicos de assinatura do ESET PROTECT para apoiar a segurança integral em múltiplas camadas. São opções mais completas que combinam produtos e serviços cobrindo prevenção, detecção e resposta.

Gerenciados por meio de um único painel de controle, incluem:

ESET PROTECT MDR

Ideal para pequenas e médias empresas

- Console de gerenciamento
- Proteção moderna de endpoints
- Segurança de servidores
- Defesa avançada contra ameaças
- Criptografia de disco completo
- Gerenciamento de vulnerabilidades e patches
- Detecção e resposta ampliadas
- Autenticação multifator
- **Serviço MDR**
- **Serviço de suporte Premium**

ESET PROTECT MDR Ultimate

Ideal para organizações de nível empresarial

- Console de gerenciamento
- Proteção moderna de endpoints
- Segurança de servidores
- Defesa avançada contra ameaças
- Criptografia de disco completo
- Gerenciamento de vulnerabilidades e patches
- Detecção e resposta ampliadas
- Autenticação multifator
- **Serviço MDR Ultimate**
- **Suporte Premium Ultimate**

Conclusão

A cibersegurança é uma parte essencial das operações de TI das organizações. No entanto, na maioria dos casos, não é — nem deveria ser — o foco principal delas. É necessário poder se concentrar no negócio principal e deixar a batalha contra um grupo diverso, determinado e crescente de cibercriminosos para os especialistas. É aí que entram os parceiros de segurança confiáveis, que oferecem vastos recursos e décadas de experiência no setor.

O MDR pode fornecer uma solução completa, abrangendo prevenção, proteção, detecção e resposta. Serviços personalizados estão disponíveis para atender às diversas necessidades de diferentes organizações, sejam PMEs, MSPs ou grandes empresas. É hora de reduzir o risco cibernético com assistência especializada.

SAIBA MAIS SOBRE MDR

COMO É UMA IMPLEMENTAÇÃO BEM-SUCEDIDA DE MDR?

Electrical Consultants, Inc. (ECI)

A ECI é uma empresa de consultoria de design e engenharia de primeira linha, especializada em projetos de serviços públicos de energia e infraestrutura. Com mais de 37 escritórios regionais nos Estados Unidos e Canadá, a ECI apoia a engenharia e construção de instalações de alta tensão em grande escala, garantindo que cada projeto seja abordado com inovação, precisão e dedicação à excelência.

A ECI enfrentou um desafio significativo de pessoal, contando com apenas uma pequena equipe dedicada à gestão da cibersegurança, o que tornava a monitoração fora do horário comercial e a resposta rápida às ameaças particularmente difíceis.

A organização precisava de uma forma confiável e econômica de monitorar e responder às ameaças 24 horas por dia, a fim de proteger seus ativos e operações.

"O ESET MDR detectou muitas ameaças e incidentes que, de outra forma, teríamos deixado passar despercebidos ou não teríamos respondido de forma tão oportuna. Em pelo menos uma ocasião, a detecção e resposta do MDR evitou que um pequeno incidente se transformasse em um problema muito maior para nossa empresa."

Somos ESET

Defesa proativa. Nosso objetivo é minimizar a superfície de ataque.

Mantenha-se um passo à frente das ameaças cibernéticas conhecidas e emergentes com nosso enfoque de prevenção, impulsionado por inteligência artificial e experiência humana. Experimente uma proteção de primeira classe, graças à nossa inteligência global sobre ameaças cibernéticas, compilada e analisada ao longo de mais de 30 anos, que alimenta nossa extensa rede de Pesquisa e Desenvolvimento, liderada por pesquisadores renomados na indústria. A ESET protege sua empresa para que você possa aproveitar todo o potencial da tecnologia.

Multicamadas, prevenção acima de tudo

Combinação de IA avançada e experiência humana

Inteligência de renome mundial sobre ameaças

Suporte personalizado e hiperlocal

Cybersecurity
Progress. Protected.