Fortaleça sua postura de segurança com o Managed Detection and Response

Detecte, investigue e responda a ameaças avançadas em todo o ambiente de TI

Dell Managed Detection and Response

Combinando o conhecimento especializado em segurança e o amplo conhecimento dos ambientes de TI da Dell Technologies com sua escolha de plataformas específicas e líderes do setor em lógica analítica de segurança de XDR.

Qual é o nível de segurança dos seus negócios?

É difícil para as equipes de TI acompanharem o crescente volume e a crescente das ameaças à segurança. Em 2022, houve 5,5 bilhões de ataques de malware em todo o mundo, um aumento de 100 milhões em relação a 2021[1].

A proteção completa da organização requer detecção rápida e resposta eficaz a novas ameaças em todo o ambiente. Isso é complicado devido a produtos e ferramentas pontuais que fragmentam a visibilidade, a dificuldade em encontrar e manter profissionais de segurança qualificados e as equipes de TI que já estão totalmente ocupadas com demandas essenciais e operações diárias.

Managed Threat Detection and Response

O Dell Managed Detection and Response é um serviço totalmente gerenciado, de ponta a ponta e 24x7 que monitora, detecta, investiga e responde às ameaças em todo o ambiente de TI, ajudando as organizações com 50 ou mais endpoints a aprimorar com rapidez e eficiência a postura de segurança, além de reduzir a sobrecarga da TI.

O serviço utiliza dois recursos principais:

- O conhecimento especializado dos analistas de segurança da Dell Technologies, obtido ao longo de anos de experiência ajudando organizações de todo o mundo a aumentar a proteção dos negócios
- Plataformas líderes do setor em lógica analítica de segurança de detecção e resposta estendidas (XDR) que incorporam análises de telemetria por IA e eventos de vários vetores de ataque.

Principais benefícios:

- Detecção e resposta unificadas em todo o ecossistema
- O banco de dados de ameaças atualizado continuamente mantém a proteção atualizada
- Até mesmo as táticas dos agentes de ameaça mais furtivos podem ser detectadas
- Exibição abrangente das atividades completas do invasor
- Uma equipe de profissionais de segurança da Dell Technologies, cujo conhecimento especializado inclui segurança, infraestrutura avançada, nuvem e muito mais
- Ajuda especializada para implementar o SaaS XDR nativo da nuvem
- Iniciação rápida de respostas a incidentes cibernéticos quando ocorre uma violação
- Alinhamento contínuo ao mais alto nível de conformidade de segurança para provedores de serviços

Solução de serviço completo

Os analistas de segurança da Dell Technologies auxiliam na configuração inicial, no monitoramento, na detecção, na correção e na resposta, tudo por um preço previsível. Eles trabalham em conjunto com a equipe de TI do cliente para entender o ambiente, aconselhar sobre melhorias na postura de segurança e ajudar a implementar o agente de software XDR nos endpoints.

Os alertas são monitorados e analisados 24x7. Se um alerta precisar de investigação, os analistas determinarão e executarão a resposta apropriada. Se uma ameaça for mal-intencionada ou exigir sua ação, você será informado e, se necessário, receberá instruções detalhadas.

Em caso de incidente de segurança, a Dell Technologies ajudará você a iniciar o processo para garantir a retomada das operações da empresa.

Escolha sua plataforma de XDR

Suas necessidades e preferências de segurança e tecnologia são exclusivas. Oferecemos a você a flexibilidade de escolher entre três opções líderes do setor: Secureworks® Taegis™ XDR, CrowdStrike Falcon® XDR ou Microsoft Defender XDR, para que você tenha a plataforma de XDR que melhor atende às suas necessidades[2].

Principais recursos

Suporte confiável

- Estreita parceria para entender seu ambiente, resolver investigações e aconselhar sobre melhorias na postura de segurança
- Monitoramento 24x7 a plataforma XDR de sua preferência que incorpora análises de telemetria por IA e eventos de vários vetores de ataque
- Consultoria especializada para implantação e configuração da plataforma de XDR

Configuração de segurança e resposta a ameaças

- Utilizando os recursos de XDR, a equipe de SOC da Dell automatizará a correção ou colaborará com você para lidar com as ameaças descobertas durante o monitoramento
- Instruções detalhadas e fáceis de entender para conter a ameaça, mesmo em situações complexas
- Inclusão de até 40 horas de configuração de segurança relacionada ao serviço por trimestre

Detecção e investigação 24x7

- Processos e alertas adaptados ao ambiente de segurança da sua organização e automatizados para operações diárias eficientes
- Busca proativa de ameaças específicas ao ambiente de cada cliente para descobrir novas ameaças ou variações de ameaças conhecidas que burlam os sistemas de segurança
- O resumo diário de alertas menos críticos possibilita à equipe de SOC da Dell focar a atenção em alertas essenciais
- Relatórios trimestrais sobre investigações, lógica analítica de tendências de alerta e orientação sobre a postura de segurança

Iniciação de respostas a incidentes cibernéticos

- As 40 horas de assistência anual para a resposta remota a incidentes permitem que as atividades de investigação comecem rapidamente
- Orientação de especialistas em segurança certificados, que ajudam organizações de todos os portes a se recuperar de eventos graves de segurança

Comece a proteger seu ambiente ainda hoje com a Dell

Com o custo total médio de violação de ransomware chegando a US$ 5,13 milhões (13% maior do que em 2022), agora é a hora de saber se o Dell Managed Detection and Response é ideal para você[3].

Entre em contato hoje mesmo com um representante de vendas.

1. Statista, Annual number of malware attacks worldwide from 2015 to 2022.
2. É necessário ter um mínimo de 500 endpoints para usar o Microsoft Defender XDR.
3. IBM, Cost of a Data Breach Report 2023.