Principais benefícios

Impedir

- Identifique vulnerabilidades em todo o ambientepara priorizar a aplicação de patches
- Detecte controles de segurança configurados incorretamente ou problemáticos que podem ser explorados
- Inspecione os caminhos de alto risco para ativos ou dados de valor com testes anuais de penetração
- Melhore a vigilância dos funcionários com o treinamento de segurança fornecido em módulos frequentes e pequenos

Responder

- Detecte e responda a ameaças 24x7 em todo o ambiente
- Acompanhe a atividade completa dos agentes da ameaça
- Use telemetria e correlacione eventos de muitas ferramentas de segurança populares

Dell Managed Detection and Response Pro Plus

Solução de 360° para SecOps totalmente gerenciada em endpoints, rede e nuvem

Aborde os desafios críticos das operações de segurança

Muitas organizações de TI adotaram o monitoramento e a detecção de ameaças para acompanhar o ritmo cada vez maior do volume e da variedade de ameaças.

Embora o monitoramento e a detecção de ameaças forneçam cobertura vital, é melhor lidar com falhas corrigíveis antecipadamente, antes que os agentes da ameaça tenham a oportunidades de explorá-las. As equipes de TI podem evitar muitas atividades mal-intencionadas abordando proativamente as vulnerabilidades de software, os controles de segurança configurados incorretamente e o descuido dos funcionários.

Profissionais de segurança experientes sabem aplicar patches a vulnerabilidades, mas, para a maioria das organizações de TI, é impossível corrigir todas elas. Em 2021, mais de 1.500 novas vulnerabilidades foram relatadas a cada mês.[1] Para conseguir gerenciar a carga de aplicação de patches, os clientes devem priorizar as vulnerabilidades que apresentam o maior risco.

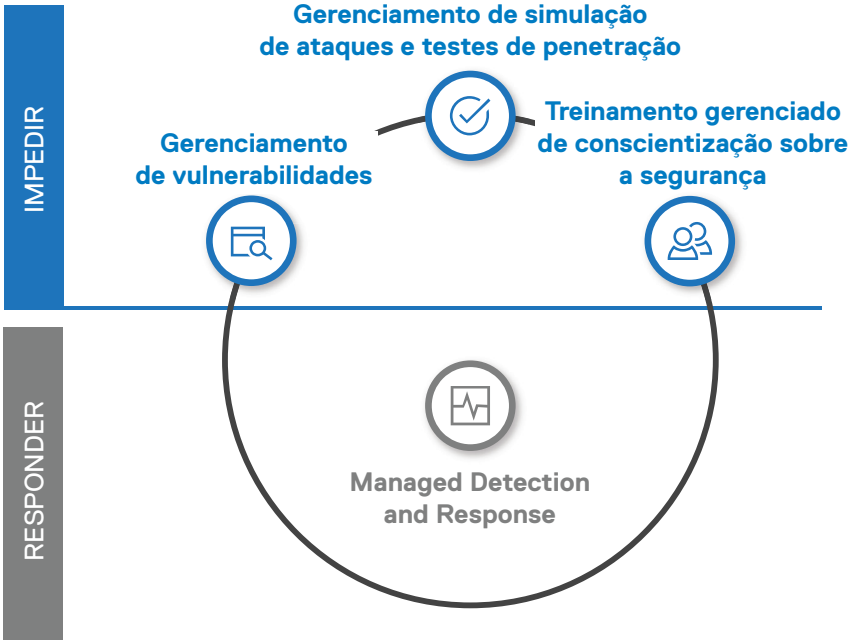
Também é assustador tentar validar todos os controles de segurança, como gateways de e-mail ou firewalls de aplicativos da Web. Com centenas de controles e configurações complexas, as equipes de segurança de TI são pressionadas a confirmar se os controles de segurança estão bloqueando atividades não autorizadas.

Além disso, as organizações precisam que os funcionários reconheçam quando os agentes da ameaça tentam obter credenciais de login, dados confidenciais ou outras informações confidenciais. Um estudo revelou que 83% das organizações entrevistadas enfrentaram um ataque bem-sucedido de phishing baseado em e-mail em 2021.[2]

Managed Detection and Response Pro Plus

Os especialistas em segurança da Dell Technologies examinaram essas questões principais de SecOps para projetar um novo serviço de operações de segurança 360º: o Managed Detection and Response Pro Plus.

O MDR Pro Plus é uma solução de SecOps totalmente gerenciada em que os principais especialistas em segurança utilizam ferramentas de ponta para evitar ameaças, detectar e conter tentativas de ataque rapidamente e iniciar a recuperação em caso de violação. O MDR Pro Plus ajuda você a fortalecer continuamente a postura de segurança de sua organização.



Elimine pontos de falha em controles de software e de segurança

O **Gerenciamento de vulnerabilidades** verifica todo mês se o ambiente está vulnerável e usa o aprendizado de máquina para priorizar as vulnerabilidades com maior probabilidade de serem exploradas e ter um grande impacto. A lista priorizada ajuda a equipe de TI a se concentrar nas vulnerabilidades de maior valor.

Os agentes da ameaça sabem como encontrar vulnerabilidades não corrigidas. Eles buscam controles de segurança configurados incorretamente ou desatualizados. Portanto, as organizações de TI precisam encontrar e solucionar esses problemas primeiro. O **Gerenciamento de simulação de ataques testes de penetração** apresenta simulações mensais de violação e ataque (BAS) automatizadas e testes anuais de penetração.

A BAS detecta controles de segurança defeituosos em dispositivos e software no seu ambiente de TI. O teste de penetração complementa a BAS ao tentar atingir um objetivo específico, como um sistema de alto valor. Os testadores capacitados vão emular técnicas de agentes da ameaça, incluindo mudar e adaptar técnicas para alcançar o objetivo.

A Dell realiza análises de vulnerabilidades e simulações de BAS em bancos de dados atualizados continuamente para ajudar você a garantir que os patches e os controles de segurança permaneçam atualizados.

Ajude os funcionários a permanecerem atentos

Um modelo comum para a conscientização sobre a segurança é uma sessão anual de treinamento de várias horas. Em geral, os funcionários não retêm essas informações, pois pode acabar sendo um exercício do tipo "caixa de seleção". Caso estejam sujeitos a uma tática de engenharia social ou recebam um e-mail com um link mal-intencionado, eles podem não reagir com cuidado suficiente.

Os **Treinamentos gerenciados de conscientização sobre a segurança** de curta duração ao longo do ano mantêm os funcionários ativamente envolvidos com planos de aprendizado personalizados e colocando a segurança em foco. Os planos de aprendizado são criados com base no cargo do funcionário, no nível de exposição a ameaças e no progresso.

Detecte e contenha rapidamente as tentativas de ataque

O Dell MDR Pro Plus apresenta **detecção e resposta gerenciadas** 24/7. Os analistas qualificados monitoram seu ambiente e investigam ameaças usando uma plataforma avançada de lógica analítica de segurança de XDR. Análises orientadas por aprendizado de máquina e aprendizagem profunda usando telemetria e eventos fornecem aos analistas informações avançadas para acompanhar o caminho e as atividades do invasor. Em seguida, a equipe da Dell fornece instruções para conter e resolver a ameaça. Em caso de incidente de segurança, a Dell Technologies ajudará você a iniciar o processo para garantir a retomada das operações da organização.

Eleve o nível das suas operações de segurança com a Dell

O MDR Pro Plus ajuda a evitar atividades mal-intencionadas, informando regularmente sobre falhas de vulnerabilidade, controles de segurança configurados incorretamente e caminhos de alto risco para ativos valiosos. Além disso, fornecemos treinamento de segurança conciso e fácil de reter para os funcionários durante o ano. A detecção e a resposta a ameaças fornecem acompanhamento e monitoramento sempre ativos de atividades suspeitas.

O MDR Pro Plus oferece uma solução inteligente de operações de segurança de TI de 360° com serviços baseados em tecnologia avançada, fornecidos por especialistas. Todas as soluções são gerenciadas pela Dell Technologies: uma empresa que as organizações de todos os tamanhos no mundo inteiro confiam para dispositivos de TI, infraestrutura e serviços inovadores.

Saiba mais sobre o Dell Managed Detection and Response Pro Plus

Entre em contato com um especialista da Dell Technologies

[1] Fonte: Com 18.378 vulnerabilidades informadas em 2021, o NIST registra o quinto ano consecutivo de números de registro, ZDNet, 8 de dezembro de 2021. https://www.zdnet.com/article/with-18376-vulnerabilities-found-in-2021-nist-reports-fifth-straight-year-of-record-numbers/

[2] Fonte: Relatório do ambiente para ataques de phishing em 2020 [Greathorn]. Cybersecurity Insiders. (2020). Recuperado em 15 de novembro de 2022 de https://www.cybersecurity-insiders.com/portfolio/2020-phishing-attack-landscape-report-greathorn/

Copyright© 2023 Dell Inc. ou suas subsidiárias. Todos os direitos reservados. Dell, EMC e outras marcas comerciais são marcas comerciais da Dell Inc. ou de suas subsidiárias. As demais marcas comerciais podem pertencer aos respectivos proprietários. A Dell EMC acredita que as informações contidas neste documento são precisas na data da publicação. As informações estão sujeitas a alterações sem aviso prévio. Março de 2023-LC | Visão geral do Dell Managed Detection and Response Pro Plus