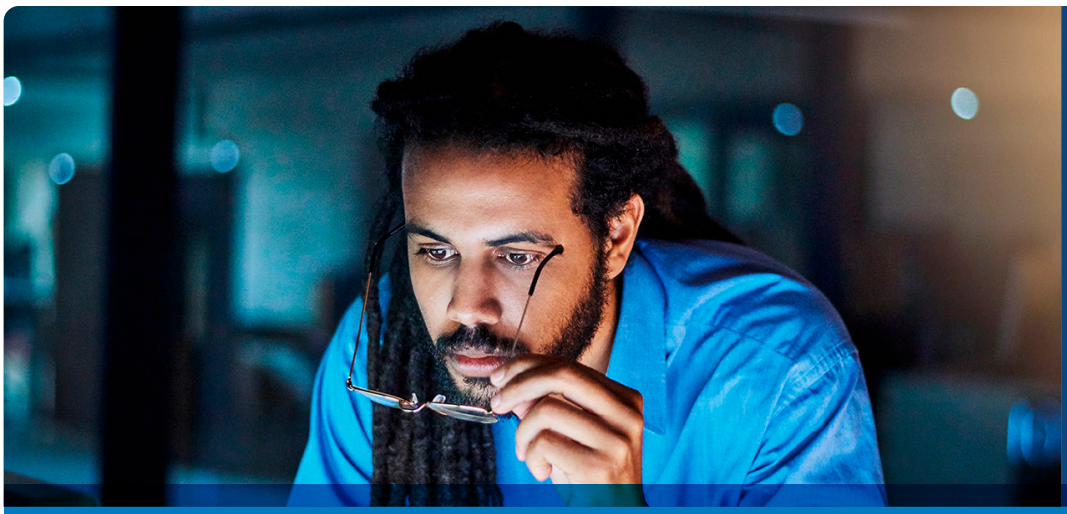
Validar os controles e as políticas de segurança para fechar vetores de ataque



Eles simulam técnicas de invasores para acesso inicial, execução mal-intencionada de arquivos, roubo de dados e muito mais

Pen Testing and Attack Simulation Management

A Dell valida seus controles e políticas de segurança em toda a kill chain

As organizações têm centenas de controles de segurança, de endpoints a gateways da Web e de e-mail. Geralmente, os controles são complexos e difíceis de gerenciar, e uma configuração incorreta pode levar a uma exposição arriscada. Os agentes de ameaças buscam explorar controles danificados ou desatualizados.

Para desafiar e validar a eficácia dos controles de segurança, o Dell Pen Testing and Attack Simulation Management imita minuciosamente as ações de ameaças do mundo real.

O serviço combina:

- simulações mensais de violação e ataque (BAS) para confirmar se os controles estão funcionando corretamente
- um teste de intrusão anual, em que especialistas qualificados tentarão violar defesas de ativos e dados críticos

Simulações de ataque testam os controles de segurança

Os profissionais de segurança da Dell usam a tecnologia BAS avançada para testar diferentes vetores de ataque, por exemplo, tentar colocar malware em um endpoint ou obter informações não autorizadas de um servidor da Web. Os testadores da Dell aplicam o BAS para simular ataques em toda a kill chain[1] contra ameaças, inclusive os TTPs invasores mais recentes[2].

A tecnologia BAS é segura para ambientes de produção e é continuamente atualizada com as informações, os ataques e os comportamentos mais recentes referentes a ameaças.

Testes de intrusão avaliam caminhos para metas de alto valor

Mesmo com a simulação de ataque, alguns invasores têm as habilidades para navegar pelo ambiente, escapando dos obstáculos para alcançar dados valiosos. É nesse momento que os testes de intrusão entram em cena.

Principais benefícios:

- Detectar controles de segurança configurados incorretamente que podem ser explorados usando simulações abrangentes de violação e ataque
- Considerar problemas e falhas que surgiram recentemente com simulações mensais
- Inspecionar estreitamente os caminhos de alto risco para ativos ou dados de alto valor com testes de intrusão anuais
- Relatar resultados de testes, tendências trimestrais e atividades notáveis para ajudar você a melhorar a postura de segurança
- Obter insights rápidos sobre novas ameaças de alto risco com testes ad hoc

Os testes de intrusão complementam o BAS — em vez de testar controles individuais ou conjuntos de controles, os testes de intrusão se concentram em caminhos vulneráveis ou de alto risco para um ambiente. Os testadores de intrusão da Dell podem emular várias técnicas de agentes de ameaça e até mesmo payloads diferentes em seu esforço para atingir um objetivo específico, como capturar um sistema de alto valor ou roubar ou desativar um conjunto específico de arquivos. Como um invasor real, um testador de intrusão experiente pode alterar, imitar e adaptar técnicas para alcançar o destino.

Aplicar as informações do teste para melhorar a postura de segurança

A Dell Technologies Services fornece relatórios mensais dos problemas de controle de segurança a serem corrigidos com base nos resultados da execução das sequências de BAS. A Dell analisa trimestralmente as tendências das várias simulações de ataque, relata atividades notáveis observadas no ambiente de TI e discute as recomendações para melhorar a postura de segurança.

Principais recursos

Breach and Attack Simulation (BAS)

- Executar simulações automatizadas de violação e ataque mensalmente de acordo com o ambiente do cliente
- Validar os controles de segurança no perímetro e nos componentes da infraestrutura interna, inclusive gateway da Web, gateway de e-mail e endpoints
- Atualizar a ferramenta BAS continuamente com as informações, os ataques e os comportamentos mais recentes pertinentes a ameaças
- Fazer alterações no fluxo de trabalho de simulação com base em simulações anteriores e fatores de ambiente de segurança
- Executar simulações ad hoc para problemas de segurança recém-descobertos, com base na inteligência contra ameaças e na avaliação da Dell

Teste de intrusão

- Executar o teste de intrusão anual em relação ao subconjunto definido de gateways da Web, APIs, dispositivos móveis, endereços IP externos, endereços IP internos e configurações de nuvem
- Executar novamente o teste da intrusão depois que os resultados do primeiro teste forem corrigidos (opcional)

Geração de relatórios e análise

- Fornecer relatórios mensais sobre as simulações de violação e ataque conduzidas
- Fornecer um relatório trimestral e análise de tendências e atividades notáveis observadas no ambiente de TI do cliente
- Fazer recomendações para melhorar a postura geral de segurança

Integração

- Conduzir uma reunião de iniciação de serviço
- Analisar a checklist pré-engajamento preenchida pelo cliente
- Analisar do ambiente de TI do cliente
- Ativar o aplicativo BAS para o cliente
- Fornecer assistência de agente para a implementação

Entre em contato hoje mesmo com um representante de vendas.

[1] "Kill chain completa" — Inclui ameaças externas, inclusive phishing, gateways da Web etc., comprometendo endpoints, movimentações laterais para obter credenciais ou espalhar o ataque, exfiltração de dados etc.
[2] "TTPs" — Táticas, técnicas e procedimentos