EBOOK INTERATIVO SOBRE CENÁRIOS DE SEGURANÇA CIBERNÉTICA

Cenários reais. Decisões mais inteligentes. Defesas mais fortes.

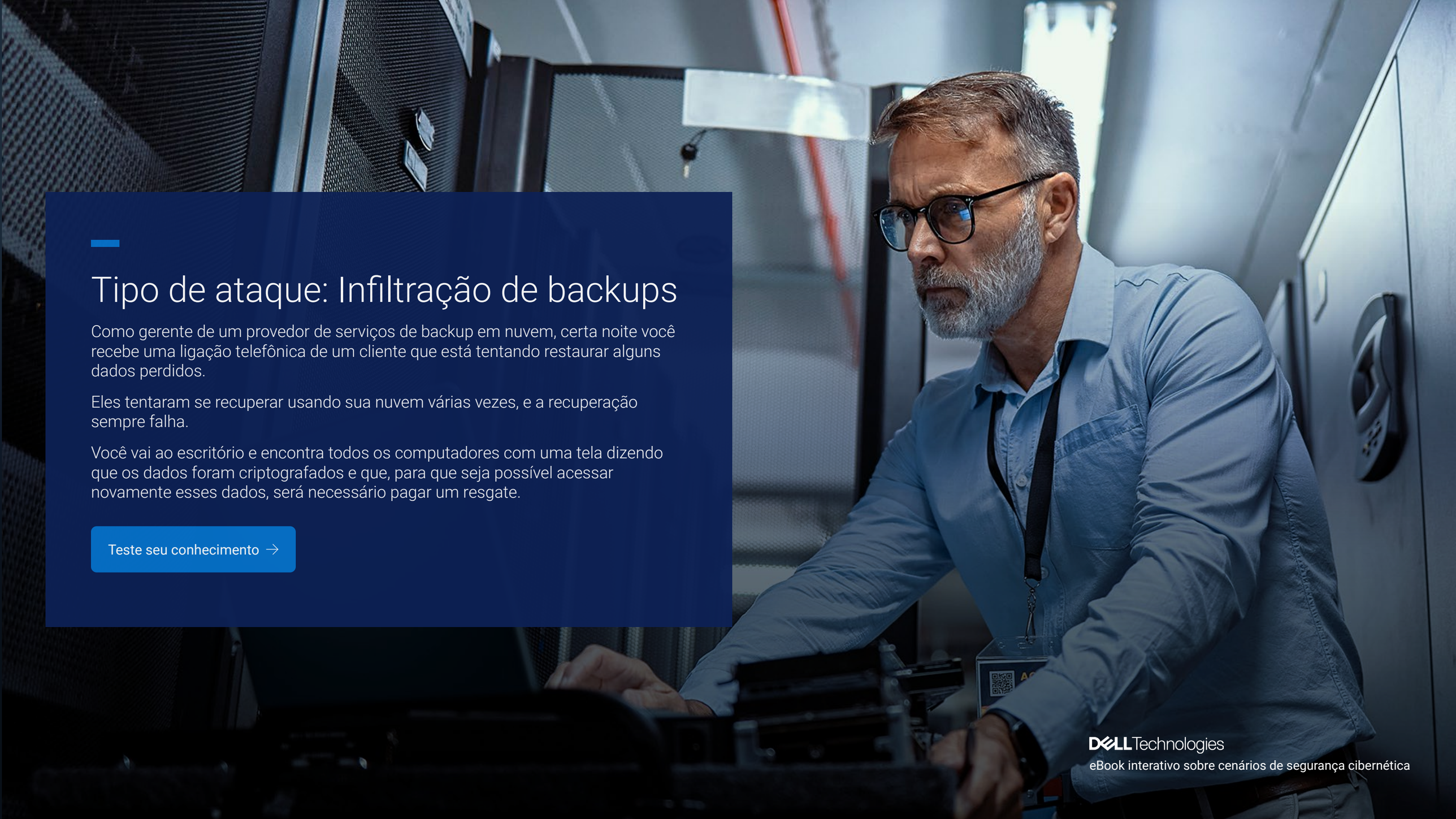
O compromisso da Dell com a segurança está no centro de tudo o que fazemos. Ao compartilhar insights, práticas recomendadas e tecnologias inovadoras, este eBook visa capacitar você com as ferramentas e o conhecimento necessários para se manter à frente dos riscos cibernéticos emergentes.

Escolha um cenário de ataque

As ameaças à segurança cibernética estão em constante evolução e as organizações precisam responder com eficiência para proteger seus dados. Para melhor preparar sua organização, mergulhe em exercícios de simulação do mundo real para ajudar a navegar em suas estratégias de segurança cibernética e combater ataques cibernéticos.

Explore uma ampla variedade de tipos de ataque e desafios específicos do setor, em setores como governo federal, estadual e local, serviços financeiros e saúde. Ao longo do caminho, você descobrirá como as soluções integradas de segurança da Dell — de notebooks e desktops a sistemas empresariais — são desenvolvidas para proteger contra essas ameaças.

- Infiltração de backups →
- Ransomware →
- Negação de serviço distribuído (DDoS) →
- Hardware da cadeia de suprimentos →
- Agente interno mal-intencionado →
- Software da cadeia de suprimentos →
- Man-in-the-Middle (MITM) →
- Dia zero →
- Injeção de Prompt/SQL →



Tipo de ataque: Infiltração de backups

Como gerente de um provedor de serviços de backup em nuvem, certa noite você recebe uma ligação telefônica de um cliente que está tentando restaurar alguns dados perdidos.

Eles tentaram se recuperar usando sua nuvem várias vezes, e a recuperação sempre falha.

Você vai ao escritório e encontra todos os computadores com uma tela dizendo que os dados foram criptografados e que, para que seja possível acessar novamente esses dados, será necessário pagar um resgate.

Teste seu conhecimento →

Tipo de ataque: Infiltração de backups

1: Reduzir a superfície de ataque — 2 — 3 — 4

Você não tem certeza de quais sistemas de backup ou clientes foram afetados. Qual deve ser o seu primeiro passo?

- [ ] Notificar as autoridades
- [ ] Desligar todos os sistemas
- [ ] Tentar conter e isolar a ameaça
- [ ] Identificar se você tem um backup limpo para restaurar

Veja a resposta correta →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

Tipo de ataque: Infiltração de backups

1: Reduzir a superfície de ataque — 2 — 3 — 4

Você não tem certeza de quais sistemas de backup ou clientes foram afetados. Qual deve ser o seu primeiro passo?

- ✗ Notificar as autoridades
- ✗ Desligar todos os sistemas
- ✓ Tentar conter e isolar a ameaça
- ✗ Identificar se você tem um backup limpo para restaurar

Conter e isolar imediatamente uma ameaça evita maior disseminação ou mais danos e permite tempo para avaliar o escopo do incidente, minimizando potencialmente o impacto de todos os tipos de ataques cibernéticos, incluindo aqueles que envolvem IA.

Próxima pergunta →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

Tipo de ataque: Infiltração de backups

1 — 2: Detectar e responder a ameaças cibernéticas — 3 — 4

Sua prioridade é disponibilizar rapidamente os dados dos seus clientes. Qual seria a ação correta para conseguir isso?

- [ ] Pagar o resgate
- [ ] Identificar o tipo do ransomware
- [ ] Notificar as autoridades
- [ ] Identificar quais dados foram comprometidos

Veja a resposta correta →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

Tipo de ataque: Infiltração de backups

1 — 2: Detectar e responder a ameaças cibernéticas — 3 — 4

Sua prioridade é disponibilizar rapidamente os dados dos seus clientes. Qual seria a ação correta para conseguir isso?

- ✗ Pagar o resgate
- ✗ Identificar o tipo do ransomware
- ✗ Notificar as autoridades
- ✓ Identificar quais dados foram comprometidos

A identificação dos dados comprometidos ajuda a concentrar os esforços de recuperação na restauração das informações mais essenciais do cliente, garantindo disponibilidade mais rápida dos dados e evitando trabalho desnecessário em sistemas não afetados.

Próxima pergunta →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

Tipo de ataque: Infiltração de backups

1 — 2 — 3: Recuperar-se de um ataque cibernético — 4

Você identificou que precisa recuperar um backup. Qual deve ser o primeiro passo do seu processo?

- [ ] Priorizar a restauração dos sistemas essenciais
- [ ] Usar a análise forense para confirmar que o ataque está totalmente contido
- [ ] Alterar todas as senhas e revogar as credenciais comprometidas
- [ ] Implementar os princípios de Zero Trust

Veja a resposta correta →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

Tipo de ataque: Infiltração de backups

1 — 2 — 3: Recuperar-se de um ataque cibernético — 4

Você identificou que precisa recuperar um backup. Qual deve ser o primeiro passo do seu processo?

- ✗ Priorizar a restauração dos sistemas essenciais
- ✓ Usar a análise forense para confirmar que o ataque está totalmente contido
- ✗ Alterar todas as senhas e revogar as credenciais comprometidas
- ✗ Implementar os princípios de Zero Trust

Antes de restaurar os sistemas, você precisa garantir que o ataque esteja completamente contido para ajudar a evitar reinfecções acidentais e mais danos, evitando a perpetuação ou aumento das ameaças em seu ambiente.

Próxima pergunta →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

Tipo de ataque: Infiltração de backups

1 — 2 — 3 — 4: Melhores práticas em geral

Quais são as possíveis maneiras de reduzir o risco de que isso aconteça no futuro?

- [ ] Utilizar os princípios do Zero Trust
- [ ] Habilitar os recursos de Detecção e resposta de endpoint (EDR)
- [ ] Implementar backups imutáveis e isolados com air gap
- [ ] Todas as alternativas acima

Veja a resposta correta →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

Tipo de ataque: Infiltração de backups

1 — 2 — 3 — 4: Melhores práticas em geral

Quais são as possíveis maneiras de reduzir o risco de que isso aconteça no futuro?

- [x] Utilizar os princípios do Zero Trust
- [x] Habilitar os recursos de Detecção e resposta de endpoint (EDR)
- [x] Implementar backups imutáveis e isolados com air gap
- [x] Todas as alternativas acima

O uso de uma estratégia de defesa de várias camadas pode reduzir riscos, minimizar danos e melhorar a resiliência organizacional, pois nenhuma medida isolada é suficiente.

Veja as soluções →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

TIPO DE ATAQUE: INFILTRAÇÃO DE BACKUPS

Recapitulação

A infiltração de backups ocorre quando criminosos cibernéticos exploram vulnerabilidades em sistemas de backup para comprometer, destruir ou criptografar dados críticos de recuperação. Esses ataques sofisticados podem coincidir ou ocorrer após outros incidentes, como a implementação de ransomware ou malware, ampliando as consequências operacionais e financeiras.

Na Dell, acreditamos na capacitação das organizações a permanecerem resilientes diante das ameaças cibernéticas em constante evolução. Com nossas soluções de ponta, serviços especializados e parcerias confiáveis, estamos aqui para ajudar você a proteger o que é mais importante.

Saiba mais sobre nossas soluções e como estamos enfrentando os desafios cibernéticos mais difíceis da atualidade.

Explore o resumo da infiltração de backup →

Voltar para Cenários

Portfólio do PowerProtect ›

Nossos cofres de backups criptografados, imutáveis e isolados com air gap contam com a lógica analítica do CyberSense orientada por IA e garantem detecção e recuperação rápidas para que você possa permanecer resiliente.

Servidores PowerEdge ›

Com inicialização segura, raiz de confiança de hardware e bloqueio do sistema, a Dell oferece a infraestrutura em que você pode confiar para proteger seus backups.

Espaço de trabalho confiável ›

As proteções SafeBIOS e SafeData reduzem os riscos, garantindo que seus sistemas de backup permaneçam inalterados e prontos quando você precisar deles.

Serviços de segurança e resiliência ›

Da implementação segura à resposta proativa a incidentes, nossos especialistas e parceiros ajudam você a criar resiliência e se recuperar com mais rapidez.

Soluções de rede ›

Com segmentação de rede, autenticação baseada em vários fatores (MFA) e configurações de privilégios mínimos, a Dell ajuda você a bloquear o acesso e proteger seus dados essenciais.

Tipo de ataque: Negação de serviço distribuído (DDoS)

É terça-feira à tarde em uma agência governamental estadual, em um dia em que uma grande nevasca era esperada.

A equipe de TI do Departamento de transporte recebe uma enorme quantidade de chamadas de agentes que não conseguem acessar os sistemas para:

- Renovar as carteiras de habilitação
- Obter autorizações de circulação rodoviária
- Pagar impostos
- Verificar as condições da estrada
- Ativar os sistemas de resposta a emergências, atrasando as equipes de manutenção no trabalho de remoção de neve/gelo das estradas

devido aos sistemas apresentarem tempo de espera excedido.

Teste seu conhecimento →

Tipo de ataque: Negação de serviço distribuído (DDoS)

1: Reduzir a superfície de ataque — 2 — 3 — 4

Qual é o primeiro lugar para procurar o que pode estar acontecendo?

- [ ] Verificar os dispositivos de rede em busca de picos repentinos e inexplicáveis no tráfego de entrada
- [ ] Verificar os dispositivos de rede em busca de tráfego incomum de um único endereço IP ou de um número limitado de endereços IP
- [ ] Verificar se há um elevado número de conexões com falha ou eventos de bloqueio de tráfego nos logs das ferramentas de visibilidade de rede ou firewall
- [ ] Todas as alternativas acima

Veja a resposta correta →

Tipo de ataque: Negação de serviço distribuído (DDoS)

1: Reduzir a superfície de ataque — 2 — 3 — 4

Qual é o primeiro lugar para procurar o que pode estar acontecendo?

- [x] Verificar os dispositivos de rede em busca de picos repentinos e inexplicáveis no tráfego de entrada
- [x] Verificar os dispositivos de rede em busca de tráfego incomum de um único endereço IP ou de um número limitado de endereços IP
- [x] Verificar se há um elevado número de conexões com falha ou eventos de bloqueio de tráfego nos logs das ferramentas de visibilidade de rede ou firewall
- [x] Todas as alternativas acima

Para diagnosticar adequadamente as interrupções generalizadas do sistema, você precisa analisar simultaneamente a atividade do dispositivo de rede e os logs das ferramentas de firewall ou visibilidade para identificar rapidamente padrões incomuns ou eventos de bloqueio. Isso permite uma resposta a incidentes mais rápida e precisa, pois permite distinguir entre incidentes cibernéticos e problemas de infraestrutura.

Próxima pergunta →

Tipo de ataque: Negação de serviço distribuído (DDoS)

1 — 2: Detectar e responder a ameaças cibernéticas — 3 — 4

Você suspeita que este pode ser um ataque de DDoS. Qual é o primeiro passo?

- [ ] Redirecionar todo o tráfego de rede por meio de um serviço de mitigação de DDoS
- [ ] Ativar as regras do firewall de aplicativos da Web (WAF) para filtrar padrões mal-intencionados
- [ ] Verificar se o pico de tráfego se deve a fontes legítimas
- [ ] Comunicar interna e externamente o que está acontecendo

Veja a resposta correta →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

Tipo de ataque: Negação de serviço distribuído (DDoS)

1 — 2: Detectar e responder a ameaças cibernéticas — 3 — 4

Você suspeita que este pode ser um ataque de DDoS. Qual é o primeiro passo?

- ✗ Redirecionar todo o tráfego de rede por meio de um serviço de mitigação de DDoS
- ✗ Ativar as regras do firewall de aplicativos da Web (WAF) para filtrar padrões mal-intencionados
- ✓ Verificar se o pico de tráfego se deve a fontes legítimas
- ✗ Comunicar interna e externamente o que está acontecendo

Antes de ativar as contramedidas de DDoS, é essencial verificar a legitimidade de um pico de tráfego. Isso permite evitar o bloqueio acidental de usuários genuínos, evitar a interrupção de partes interessadas essenciais e garantir que quaisquer outras ações de proteção sejam apropriadas e direcionadas com precisão — minimizando o impacto negativo nas operações públicas e na continuidade geral dos negócios.

Próxima pergunta →

Tipo de ataque: Negação de serviço distribuído (DDoS)

1 2 3: Recuperar-se de um ataque cibernético 4

Quais são as medidas que você pode implementar para tentar evitar um ataque DDoS no futuro?

- [ ] Bloquear os endereços IP do ataque
- [ ] Realizar testes regulares de violação com simulações de DDoS
- [ ] Mover todos os aplicativos para a nuvem, pois os provedores de serviços em nuvem geralmente não sofrem ataques de DDoS
- [ ] Implementar os princípios de Zero Trust

Veja a resposta correta →

Tipo de ataque: Negação de serviço distribuído (DDoS)

1 — 2 — 3: Recuperar-se de um ataque cibernético — 4

Quais são as medidas que você pode implementar para tentar evitar um ataque DDoS no futuro?

- ✗ Bloquear os endereços IP do ataque
- ✓ Realizar testes regulares de violação com simulações de DDoS
- ✗ Mover todos os aplicativos para a nuvem, pois os provedores de serviços em nuvem geralmente não sofrem ataques de DDoS
- ✓ Implementar os princípios de Zero Trust

Os testes proativos de violação com simulações de DDoS identificam e fortalecem lacunas em suas defesas, enquanto os princípios de Zero Trust se concentram em minimizar riscos, impondo o acesso com privilégios mínimos em todos os momentos. Isso ajuda a reduzir o risco de interrupção de sistemas essenciais, como coordenação de resposta a emergências ou controles de semáforos em tempo real, que devem permanecer funcionais mesmo durante um ataque.

Próxima pergunta →

Tipo de ataque: Negação de serviço distribuído (DDoS)

1 2 3 4: Melhores práticas em geral

Como parte do seu plano geral de resposta e recuperação de incidentes (IRR), quem você deve notificar?

- [ ] Sua equipe jurídica
- [ ] Seu fornecedor de seguro cibernético
- [ ] CISA (Cybersecurity and Infrastructure Security Agency), FBI e MS-ISAC (Multi-State Information Sharing & Analysis Center)
- [ ] Todas as alternativas acima

Veja a resposta correta →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

Tipo de ataque: Negação de serviço distribuído (DDoS)

1 — 2 — 3 — 4: Melhores práticas em geral

Como parte do seu plano geral de resposta e recuperação de incidentes (IRR), quem você deve notificar?

- [x] Sua equipe jurídica
- [x] Seu fornecedor de seguro cibernético
- [x] CISA (Cybersecurity and Infrastructure Security Agency), FBI e MS-ISAC (Multi-State Information Sharing & Analysis Center)
- [x] Todas as alternativas acima

Durante um incidente cibernético de grande escala, considere contar com a colaboração de órgãos jurídicos, governamentais e de seguros para questões de conformidade, reivindicações e aplicação da lei. Após garantir que todos os requisitos regulamentares foram atendidos, sua organização poderá conter, resolver e se recuperar do incidente com eficácia.

Veja as soluções →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

TIPO DE ATAQUE: NEGAÇÃO DE SERVIÇO DISTRIBUÍDO (DDOS)

Recapitulação

Um ataque DDoS busca interromper o funcionamento normal de uma rede, serviço ou servidor, sobrecarregando-o com um grande volume de tráfego de várias fontes. Esses ataques são executados explorando botnets, que são redes de dispositivos infectados controlados remotamente por invasores.

Na Dell, ajudamos as organizações a se manterem resilientes contra ataques de DDoS, combinando tecnologias avançadas de detecção e mitigação com serviços especializados e uma abordagem Zero Trust, garantindo resposta rápida, interrupções mínimas e defesas fortalecidas.

Saiba mais sobre estratégias avançadas de resiliência cibernética e como a Dell pode ajudar você a proteger sua organização contra DDoS.

Explore o resumo sobre DDoS →

Voltar para Cenários

Soluções de rede >

Ative a segmentação de rede, a microssegmentação e a aplicação de privilégios mínimos para isolar ativos essenciais, limitar a disseminação do ataque e garantir a rápida contenção de DDoS.

Servidores PowerEdge >

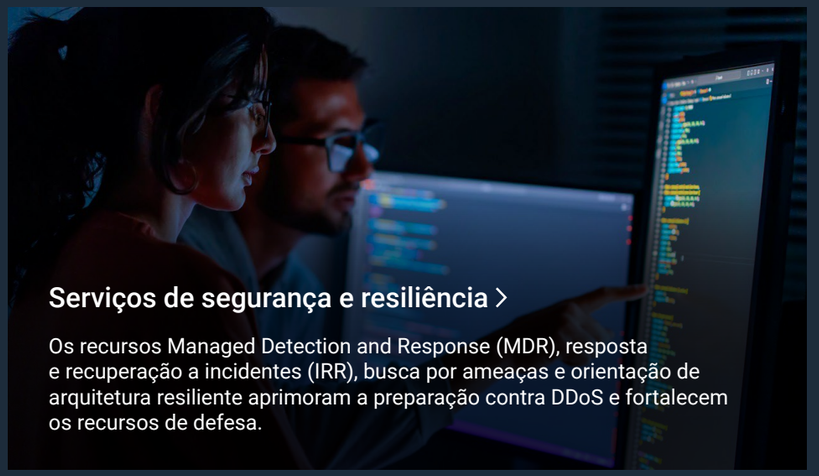
Com raiz de confiança de hardware, inicialização segura, bloqueio do sistema e evidência de violação em tempo real, a Dell oferece proteção resiliente e de alto desempenho contra DDoS e recuperação acelerada.

Dispositivos confiáveis >

A integração de SafeBIOS, SecureData e detecção e resposta automatizadas reduz as superfícies de ataque de endpoints em até 70%, evitando que distrações orientadas por DDoS se tornem vetores de violação.

Portfólio do PowerProtect >

Ambientes de backup criptografados, imutáveis e isolados, com tecnologia de lógica analítica de ameaças orientada por IA, garantem restauração rápida e validada, e mantêm a continuidade dos negócios durante interrupções de DDoS.



Serviços de segurança e resiliência >

Os recursos Managed Detection and Response (MDR), resposta e recuperação a incidentes (IRR), busca por ameaças e orientação de arquitetura resiliente aprimoram a preparação contra DDoS e fortalecem os recursos de defesa.

Tipo de ataque: Usuário interno mal-intencionado

São 8h da manhã de uma terça-feira. O dia de trabalho está apenas começando para os funcionários de uma empresa de saúde dos EUA.

Uma funcionária de nível sênior que trabalha com dados altamente confidenciais de pacientes faz log-in depois de uma noite de trabalho no escritório.

Ela percebe alterações em uma pasta na qual estava trabalhando na noite anterior. Após consultar sua equipe, ela abre uma solicitação junto ao setor de TI.

Depois de investigarem, eles descobrem que um funcionário júnior de TI com conexões com um sindicato criminoso persuadiu um funcionário de nível sênior a inserir um USB Rubber Ducky em seu dispositivo para fazer downgrade do sistema básico de entrada/saída (BIOS) para uma versão vulnerável, comprometendo o sistema.

Teste seu conhecimento →

Tipo de ataque: Usuário interno mal-intencionado

1: Reduzir a superfície de ataque — 2 — 3 — 4 — 5

O usuário interno mal-intencionado iniciou esse ataque usando dois métodos rastreados pela estrutura MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK). O que são?

- [ ] Relacionamento de confiança + replicação via mídia removível
- [ ] Engenharia social + replicação via mídia removível
- [ ] Engenharia social + serviços remotos externos
- [ ] Relacionamento de confiança + adições de hardware

Veja a resposta correta →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

Tipo de ataque: Usuário interno mal-intencionado

1: Reduzir a superfície de ataque — 2 — 3 — 4 — 5

O usuário interno mal-intencionado iniciou esse ataque usando dois métodos rastreados pela estrutura MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK). O que são?

- ✗ Relacionamento de confiança + replicação via mídia removível
- ✓ Engenharia social + replicação via mídia removível
- ✗ Engenharia social + serviços remotos externos
- ✗ Relacionamento de confiança + adições de hardware

Ao alinhar-se às técnicas MITRE ATT&CK para manipulação humana e replicação por meio de armazenamento portátil, o invasor aproveitou a engenharia social para persuadir um funcionário sênior a conectar um USB Rubber Ducky, entregando dados adulterados por meio de mídia removível.

Próxima pergunta →

Tipo de ataque: Usuário interno mal-intencionado

1 — 2: Detectar e responder a ameaças cibernéticas — 3 — 4 — 5

Por que o invasor precisou usar os dois métodos?

- [ ] Para entrar na rede como um administrador global e fazer downgrade do sistema básico de entrada/saída (BIOS)
- [ ] Para realizar phishing contra o administrador e induzi-lo a fazer downgrade do BIOS
- [ ] Para alterar o provedor do Domain Name System (DNS) do dispositivo para obter as credenciais necessárias para acesso único à rede
- [ ] Para instalar malware em um dispositivo e obter as credenciais necessárias para acesso contínuo à rede

Veja a resposta correta →

Tipo de ataque: Usuário interno mal-intencionado

1 — 2: Detectar e responder a ameaças cibernéticas — 3 — 4 — 5

Por que o invasor precisou usar os dois métodos?

- ✗ Para entrar na rede como um administrador global e fazer downgrade do sistema básico de entrada/saída (BIOS)
- ✗ Para realizar phishing contra o administrador e induzi-lo a fazer downgrade do BIOS
- ✗ Para alterar o provedor do Domain Name System (DNS) do dispositivo para obter as credenciais necessárias para acesso único à rede
- ✓ Para instalar malware em um dispositivo e obter as credenciais necessárias para acesso contínuo à rede

O invasor precisava usar os dois métodos — a instalação de malware por meio do USB Rubber Ducky para comprometer o dispositivo e as credenciais a fim de ter acesso contínuo à rede — para estabelecer um controle persistente e não autorizado sobre o ambiente alvo do ataque.

Próxima pergunta →

Tipo de ataque: Usuário interno mal-intencionado

1 — 2 — 3: Detectar e responder a ameaças cibernéticas — 4 — 5

Qual é a maneira de detectar atividade irregular na rede?

- [ ] Controle de aplicativos
- [ ] Detecção e resposta estendidas (XDR)
- [ ] Antivírus de última geração (NGAV)
- [ ] Geofencing de endpoint

Veja a resposta correta →

Tipo de ataque: Usuário interno mal-intencionado

1 — 2 — 3: Detectar e responder a ameaças cibernéticas — 4 — 5

Qual é a maneira de detectar atividade irregular na rede?

- ✗ Controle de aplicativos
- ✓ Detecção e resposta estendidas (XDR)
- ✗ Antivírus de última geração (NGAV)
- ✗ Geofencing de endpoint

Quando se trata de fornecer visibilidade ampla e correlacionada para detecção rápida de ameaças, a XDR é ideal para detectar atividades suspeitas na rede, pois monitora e analisa continuamente a atividade em endpoints, redes e ambientes de nuvem.

Próxima pergunta →

Tipo de ataque: Usuário interno mal-intencionado

1 2 3 4: Recuperar-se de um ataque cibernético 5

Que segurança integrada do PC pode detectar atividades suspeitas no início da cadeia de ataque?

- [ ] Gerenciamento de eventos e informações de segurança (SIEM)
- [ ] Detecção e resposta estendidas (XDR)
- [ ] Indicadores de ataque (IOA)
- [ ] Controle de acesso com base em funções (RBAC)

Veja a resposta correta →

Tipo de ataque: Usuário interno mal-intencionado

1 2 3 4: Recuperar-se de um ataque cibernético 5

Que segurança integrada do PC pode detectar atividades suspeitas no início da cadeia de ataque?

- ✗ Gerenciamento de eventos e informações de segurança (SIEM)
- ✗ Detecção e resposta estendidas (XDR)
- ✓ Indicadores de ataque (IOA)
- ✗ Controle de acesso com base em funções (RBAC)

O IOA se concentra na detecção de comportamentos de invasores e padrões de atividades suspeitas à medida que ocorrem, permitindo que as equipes de segurança identifiquem ameaças mais cedo do que os métodos baseados em assinaturas e intervenham antes que danos significativos ocorram.

Próxima pergunta →

Tipo de ataque: Usuário interno mal-intencionado

1 2 3 4 5: Melhores práticas em geral

Após identificar o método de acesso inicial, que medida você poderia tomar para se recuperar e evitar violações futuras semelhantes?

- [ ] Atualizar o BIOS para a versão mais recente
- [ ] Desativar a opção de downgrade do BIOS
- [ ] Desativar as portas USB
- [ ] Implementar controle granular para permitir o uso seguro de dispositivos USB e evitar a disseminação de malware
- [ ] Todas as alternativas acima

Veja a resposta correta →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

Tipo de ataque: Usuário interno mal-intencionado

1 2 3 4 5: Melhores práticas em geral

Após identificar o método de acesso inicial, que medida você poderia tomar para se recuperar e evitar violações futuras semelhantes?

- [x] Atualizar o BIOS para a versão mais recente
- [x] Desativar a opção de downgrade do BIOS
- [x] Desativar as portas USB
- [x] Implementar controle granular para permitir o uso seguro de dispositivos USB e evitar a disseminação de malware
- [x] Todas as alternativas acima

Ao lidar com vetores de ataque distintos para garantir que o hardware esteja seguro e os downgrades sejam bloqueados, as ameaças baseadas em USB podem ser contidas e a disseminação de malware é interrompida em vários pontos para ajudar a criar uma defesa abrangente e em camadas, que recupera os sistemas afetados e protege contra futuras violações.

Veja as soluções →

TIPO DE ATAQUE: USUÁRIO INTERNO MAL-INTENCIONADO

Recapitulação

Um ataque de usuário interno mal-intencionado ocorre quando um indivíduo dentro de uma organização usa indevidamente seu acesso para comprometer dados, interromper operações ou extrair informações confidenciais para objetivos pessoais, financeiros ou da concorrência. Esse indivíduo pode ser um funcionário, contratado, parceiro ou qualquer pessoa com acesso legítimo aos sistemas e redes da empresa.

A Dell se defende contra ataques cibernéticos de usuários internos mal-intencionados por meio de uma combinação de tecnologias avançadas e protocolos de segurança rigorosos.

Saiba mais sobre estratégias avançadas de resiliência cibernética e como a Dell pode ajudar você a proteger sua organização contra ataques de usuários internos mal-intencionados.

Explore o resumo de usuário interno mal-intencionado →

Voltar para Cenários

Infraestrutura e dispositivos confiáveis >

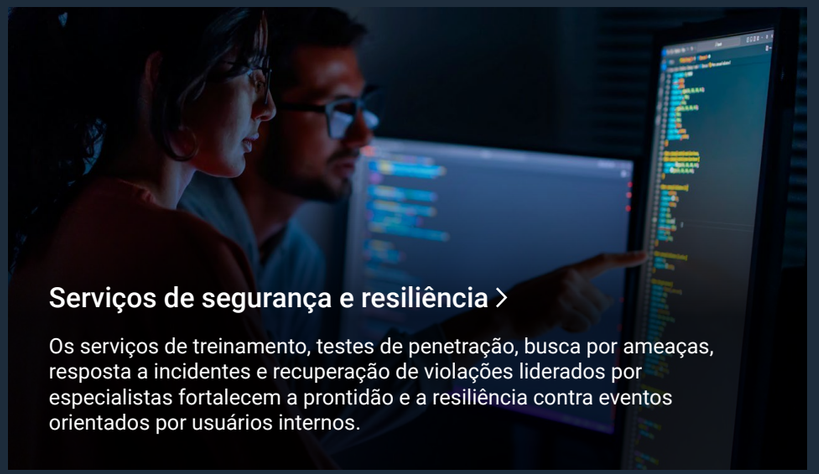
As proteções integradas de privilégio mínimo, autenticação baseada em vários fatores (MFA), controle de acesso baseado em função (RBAC), autenticação dupla e Zero Trust protegem endpoints e infraestrutura, reduzindo os riscos de ameaças internas.

Servidores PowerEdge >

A raiz de confiança de hardware, a inicialização segura, o gerenciamento dinâmico de portas USB e o bloqueio do sistema protegem contra adulterações e impedem ataques internos físicos ou baseados em firmware.

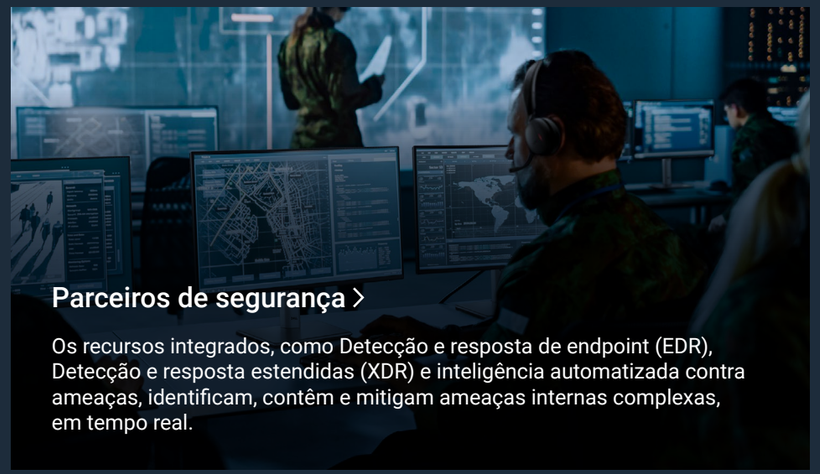
Portfólio do PowerProtect >

Os backups isolados e não modificados garantem a integridade dos dados, restauração rápida e detecção precoce de tentativas de manipulação de dados, permitindo a recuperação de incidentes internos.



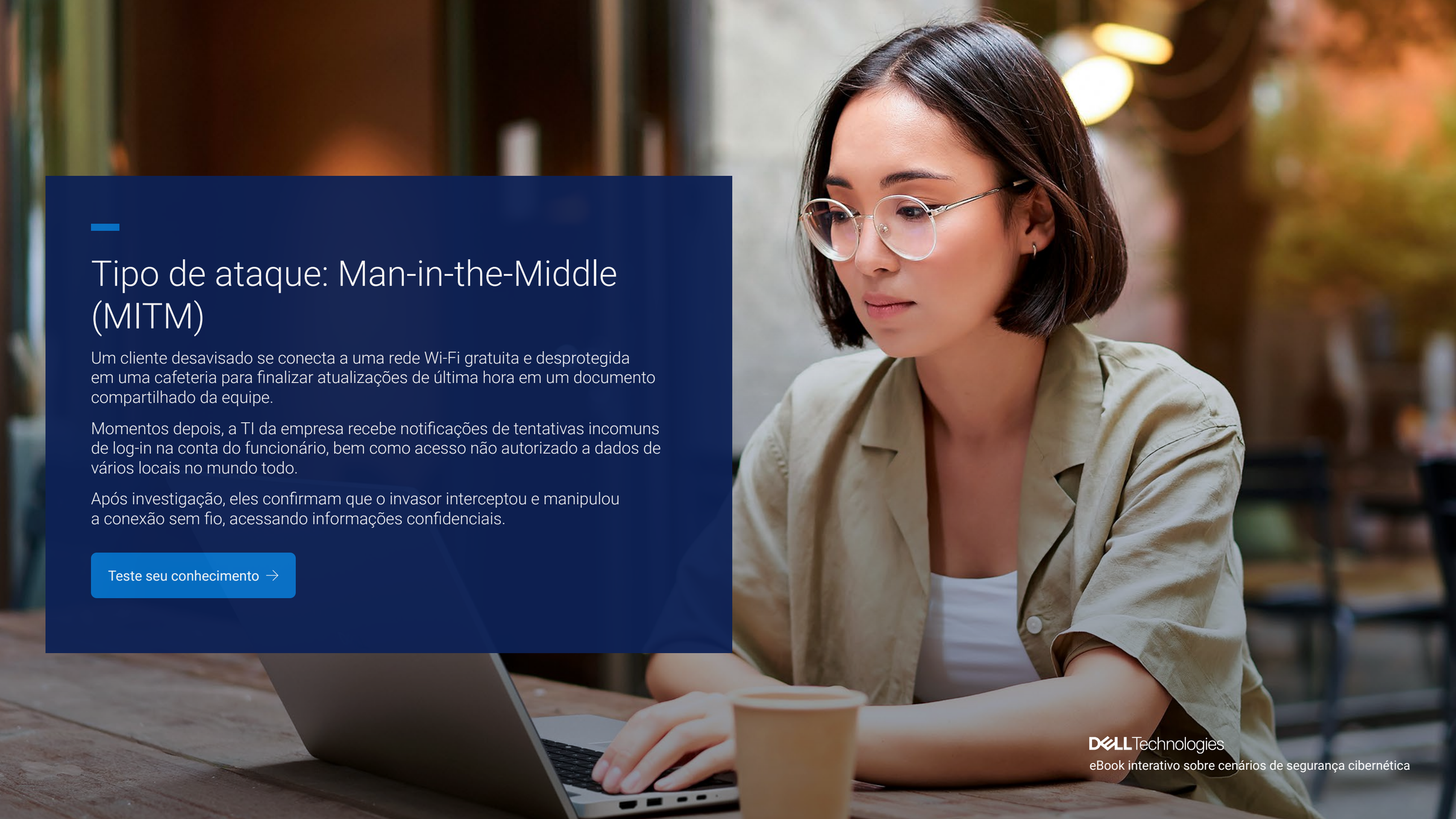
Serviços de segurança e resiliência >

Os serviços de treinamento, testes de penetração, busca por ameaças, resposta a incidentes e recuperação de violações liderados por especialistas fortalecem a prontidão e a resiliência contra eventos orientados por usuários internos.



Parceiros de segurança >

Os recursos integrados, como Detecção e resposta de endpoint (EDR), Detecção e resposta estendidas (XDR) e inteligência automatizada contra ameaças, identificam, contêm e mitigam ameaças internas complexas, em tempo real.



Tipo de ataque: Man-in-the-Middle (MITM)

Um cliente desavisado se conecta a uma rede Wi-Fi gratuita e desprotegida em uma cafeteria para finalizar atualizações de última hora em um documento compartilhado da equipe.

Momentos depois, a TI da empresa recebe notificações de tentativas incomuns de log-in na conta do funcionário, bem como acesso não autorizado a dados de vários locais no mundo todo.

Após investigação, eles confirmam que o invasor interceptou e manipulou a conexão sem fio, acessando informações confidenciais.

Teste seu conhecimento →

Tipo de ataque: Man-in-the-Middle (MITM)

1: Reduzir a superfície de ataque — 2 — 3 — 4

Qual é o primeiro lugar que a equipe de TI deve investigar após detectar tentativas de log-in incomuns?

- [ ] Logs do firewall, Sistema de detecção de invasão (IDS), Sistema de prevenção contra invasão (IPS) e Detecção e resposta estendidas (XDR)
- [ ] O notebook do funcionário afetado
- [ ] O tráfego de rede na rede Wi-Fi desprotegida da cafeteria
- [ ] Os logs de autenticação dos sistemas da empresa

Veja a resposta correta →

Tipo de ataque: Man-in-the-Middle (MITM)

1: Reduzir a superfície de ataque — 2 — 3 — 4

Qual é o primeiro lugar que a equipe de TI deve investigar após detectar tentativas de log-in incomuns?

- ✓ Logs do firewall, Sistema de detecção de invasão (IDS), Sistema de prevenção contra invasão (IPS) e Detecção e resposta estendidas (XDR)
- ✗ O notebook do funcionário afetado
- ✗ O tráfego de rede na rede Wi-Fi desprotegida da cafeteria
- ✓ Os logs de autenticação dos sistemas da empresa

Ao analisar esses logs do firewall, IDS/IPS e de autenticação, as equipes de TI podem rastrear tentativas de acesso não autorizado, avaliar contas comprometidas e obter uma melhor compreensão do escopo do incidente.

Próxima pergunta →

Tipo de ataque: Man-in-the-Middle (MITM)

1 — 2: Detectar e responder a ameaças cibernéticas — 3 — 4

Qual ação imediata deve ser tomada pela equipe de TI após a confirmação do ataque MITM?

- [ ] Desconectar o dispositivo do funcionário comprometido da rede imediatamente e o isolar para análise
- [ ] Atualizar as regras de firewall e as configurações de rede para impedir novos acessos não autorizados
- [ ] Redefinir as senhas de todas as contas de funcionários
- [ ] Desativar os sistemas afetados para evitar a exfiltração de dados

Veja a resposta correta →

Tipo de ataque: Man-in-the-Middle (MITM)

1 — 2: Detectar e responder a ameaças cibernéticas — 3 — 4

Qual ação imediata deve ser tomada pela equipe de TI após a confirmação do ataque MITM?

- ✓ Desconectar o dispositivo do funcionário comprometido da rede imediatamente e o isolar para análise
- ✓ Atualizar as regras de firewall e as configurações de rede para impedir novos acessos não autorizados
- ✗ Redefinir as senhas de todas as contas de funcionários
- ✗ Desativar os sistemas afetados para evitar a exfiltração de dados

Desconectar e isolar imediatamente o dispositivo comprometido interrompe o acesso do invasor e preserva as evidências forenses, enquanto a atualização das regras de firewall e de rede bloqueia novas conexões mal-intencionadas e protege a rede mais ampla contra comprometimento contínuo.

Próxima pergunta →

Tipo de ataque: Man-in-the-Middle (MITM)

1 — 2 — 3: Recuperar-se de um ataque cibernético — 4

Quais medidas preventivas poderiam ter reduzido a vulnerabilidade ao ataque MITM?

- [ ] Obrigar o uso de rede virtual privada (VPN) para todos os funcionários
- [ ] Implementar princípios de segurança Zero Trust como autenticação baseada em vários fatores (MFA)
- [ ] Evitar redes Wi-Fi públicas
- [ ] Criptografar arquivos confidenciais compartilhados por e-mail

Veja a resposta correta →

Tipo de ataque: Man-in-the-Middle (MITM)

1 — 2 — 3: Recuperar-se de um ataque cibernético — 4

Quais medidas preventivas poderiam ter reduzido a vulnerabilidade ao ataque MITM?

- ✓ Obrigar o uso de rede virtual privada (VPN) para todos os funcionários
- ✓ Implementar princípios de segurança Zero Trust como autenticação baseada em vários fatores (MFA)
- ✗ Evitar redes Wi-Fi públicas
- ✗ Criptografar arquivos confidenciais compartilhados por e-mail

Aplicar o uso de VPN em redes desprotegidas criptografa o tráfego de Internet dos funcionários para evitar interceptações, enquanto a implementação de segurança Zero Trust e a MFA garantem que cada solicitação de acesso seja verificada continuamente.

Próxima pergunta →

Tipo de ataque: Man-in-the-Middle (MITM)

1 2 3 4: Melhores práticas em geral

Após lidar com a violação, quais estratégias de longo prazo sua organização deve implementar?

- [ ] Fazer auditoria e corrigir os sistemas regularmente
- [ ] Aumentar a segmentação da rede para isolar dados e sistemas confidenciais
- [ ] Implementar soluções de Detecção e resposta de endpoint (EDR) e Managed Detection and Response (MDR)
- [ ] Implementar treinamento robusto e regular para os funcionários
- [ ] Todas as alternativas acima

Veja a resposta correta →

Tipo de ataque: Man-in-the-Middle (MITM)

1 — 2 — 3 — 4: Melhores práticas em geral

Após lidar com a violação, quais estratégias de longo prazo sua organização deve implementar?

- [x] Fazer auditoria e corrigir os sistemas regularmente
- [x] Aumentar a segmentação da rede para isolar dados e sistemas confidenciais
- [x] Implementar soluções de Detecção e resposta de endpoint (EDR) e Managed Detection and Response (MDR)
- [x] Implementar treinamento robusto e regular para os funcionários
- [x] Todas as alternativas acima

Para se proteger contra diferentes ameaças, essas estratégias de longo prazo se combinam para criar uma postura de segurança abrangente e resiliente que impede que invasores explorem lacunas e garante uma resposta rápida e eficaz às violações.

Veja as soluções →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

TIPO DE ATAQUE: MAN-IN-THE-MIDDLE (MITM)

Recapitulação

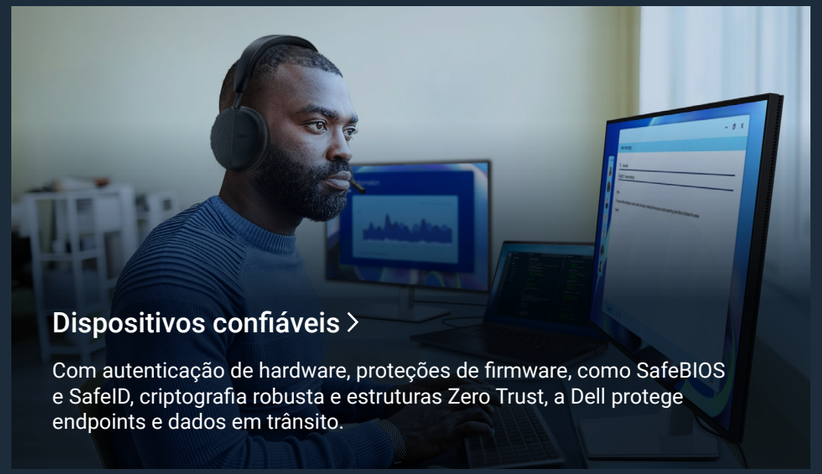
Um ataque MITM acontece quando um criminoso cibernético intercepta secretamente comunicações entre duas partes, como entre um funcionário e um servidor corporativo ou um cliente e um site empresarial. O objetivo do invasor pode variar, mas o resultado é o mesmo: uma quebra de confiança e segurança.

Na Dell, oferecemos soluções de segurança inovadoras e escaláveis, capacitando as organizações a neutralizar ameaças MITM, proteger ativos e manter a integridade dos negócios com as ferramentas e o conhecimento necessários para detectar, responder e se recuperar com confiança.

Saiba mais sobre estratégias avançadas de resiliência cibernética e como a Dell pode ajudar você a proteger sua organização contra ataques MITM.

Leia o resumo sobre ataques MITM →

Voltar para Cenários



Dispositivos confiáveis >

Com autenticação de hardware, proteções de firmware, como SafeBIOS e SafeID, criptografia robusta e estruturas Zero Trust, a Dell protege endpoints e dados em trânsito.

Servidores PowerEdge >

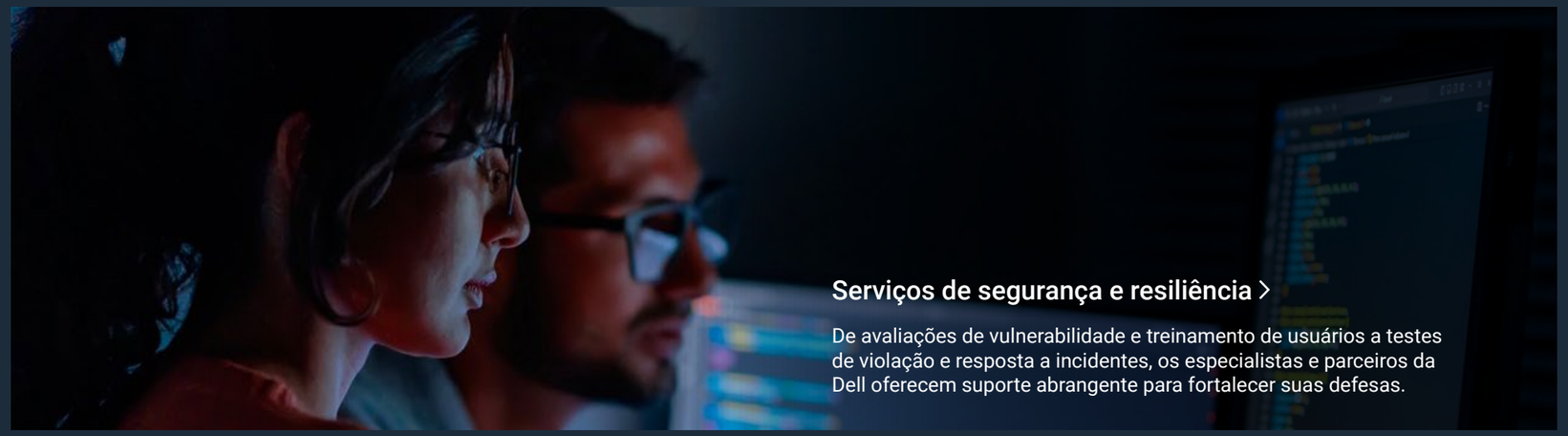
A inicialização segura, a raiz de confiança de chip, o gerenciamento dinâmico de portas USB e os bloqueios do sistema garantem a integridade do hardware e protegem cargas de trabalho essenciais contra ameaças baseadas na rede.

Soluções de armazenamento >

Os dados criptografados em repouso e em trânsito, combinados com snapshots isolados e recursos de recuperação rápida, garantem que os arquivos permaneçam seguros e possam ser restaurados rapidamente após um ataque MITM.

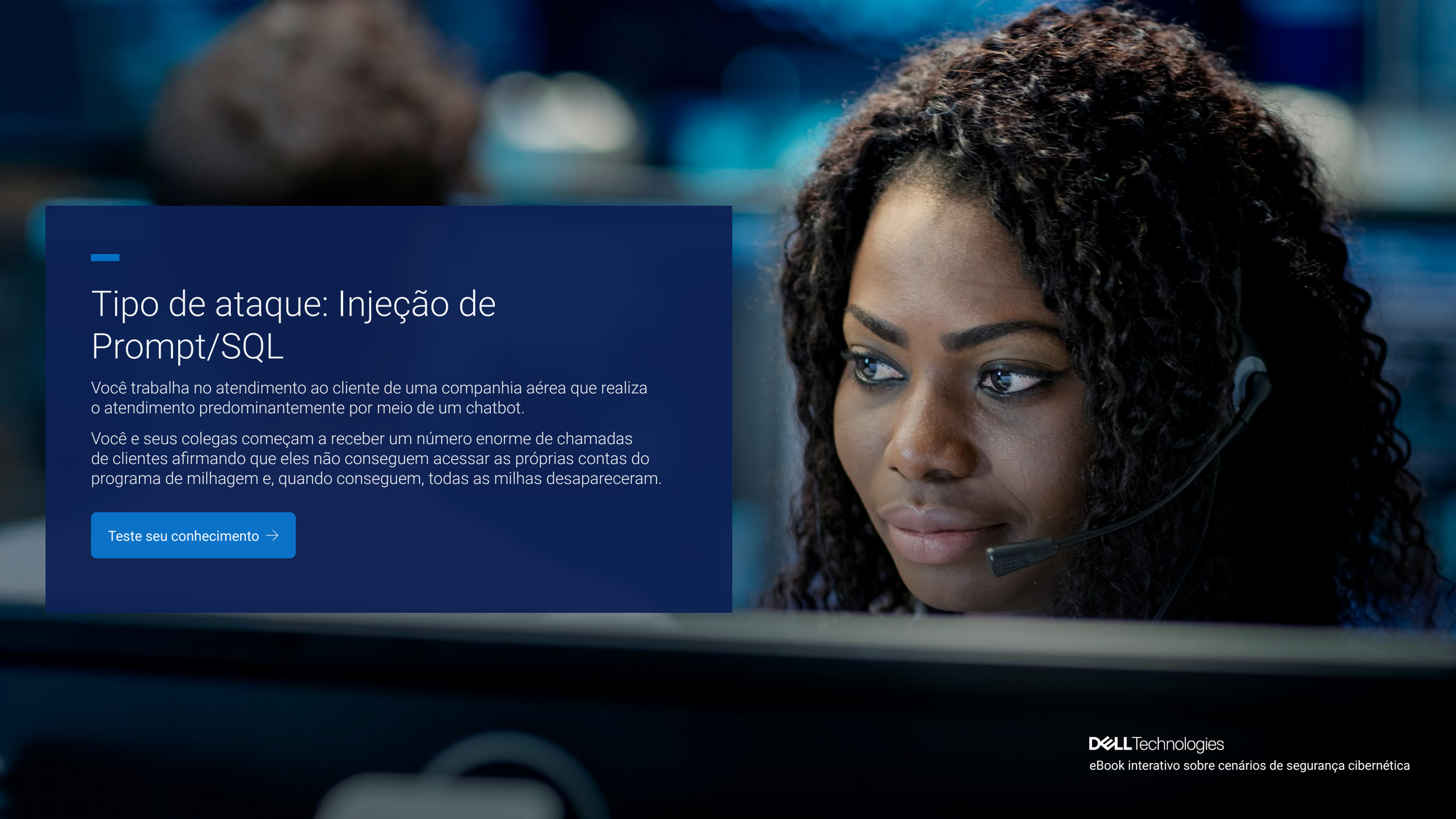
Portfólio do PowerProtect >

Os backups isolados e não modificados e a lógica analítica do CyberSense orientada por IA permitem recuperação rápida e restauração confiável de dados em caso de um ataque MITM.



Serviços de segurança e resiliência >

De avaliações de vulnerabilidade e treinamento de usuários a testes de violação e resposta a incidentes, os especialistas e parceiros da Dell oferecem suporte abrangente para fortalecer suas defesas.



Tipo de ataque: Injeção de Prompt/SQL

Você trabalha no atendimento ao cliente de uma companhia aérea que realiza o atendimento predominantemente por meio de um chatbot.

Você e seus colegas começam a receber um número enorme de chamadas de clientes afirmando que eles não conseguem acessar as próprias contas do programa de milhagem e, quando conseguem, todas as milhas desapareceram.

Teste seu conhecimento →

Tipo de ataque: Injeção de Prompt/SQL

1: Reduzir a superfície de ataque — 2 — 3 — 4

Após a investigação, você vê alguns erros nos logs; *erro de sintaxe na instrução Structured Query Language (SQL) ou nome de coluna "admin" inválido*. Que tipo de incidente cibernético é esse?

- [ ] Credenciais roubadas
- [ ] Injeção de Prompt ou SQL
- [ ] Ataque Man-in-the-Middle
- [ ] Phishing

Veja a resposta correta →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

Tipo de ataque: Injeção de Prompt/SQL

1: Reduzir a superfície de ataque — 2 — 3 — 4

Após a investigação, você vê alguns erros nos logs; *erro de sintaxe na instrução Structured Query Language (SQL)* ou *nome de coluna "admin" inválido*. Que tipo de incidente cibernético é esse?

- ✗ Credenciais roubadas
- ✓ Injeção de Prompt ou SQL
- ✗ Ataque Man-in-the-Middle
- ✗ Phishing

"Injeção de Prompt e SQL" é a resposta correta porque erros de log, como "Syntax error in SQL statement" ou "Invalid column name 'admin'", revelam que os invasores exploraram os campos de entrada do chatbot com código SQL malicioso para acessar ou alterar dados da conta do cliente. Esses são indicadores técnicos claros de um ataque de injeção de SQL, correspondendo à atividade suspeita descrita.

Próxima pergunta →

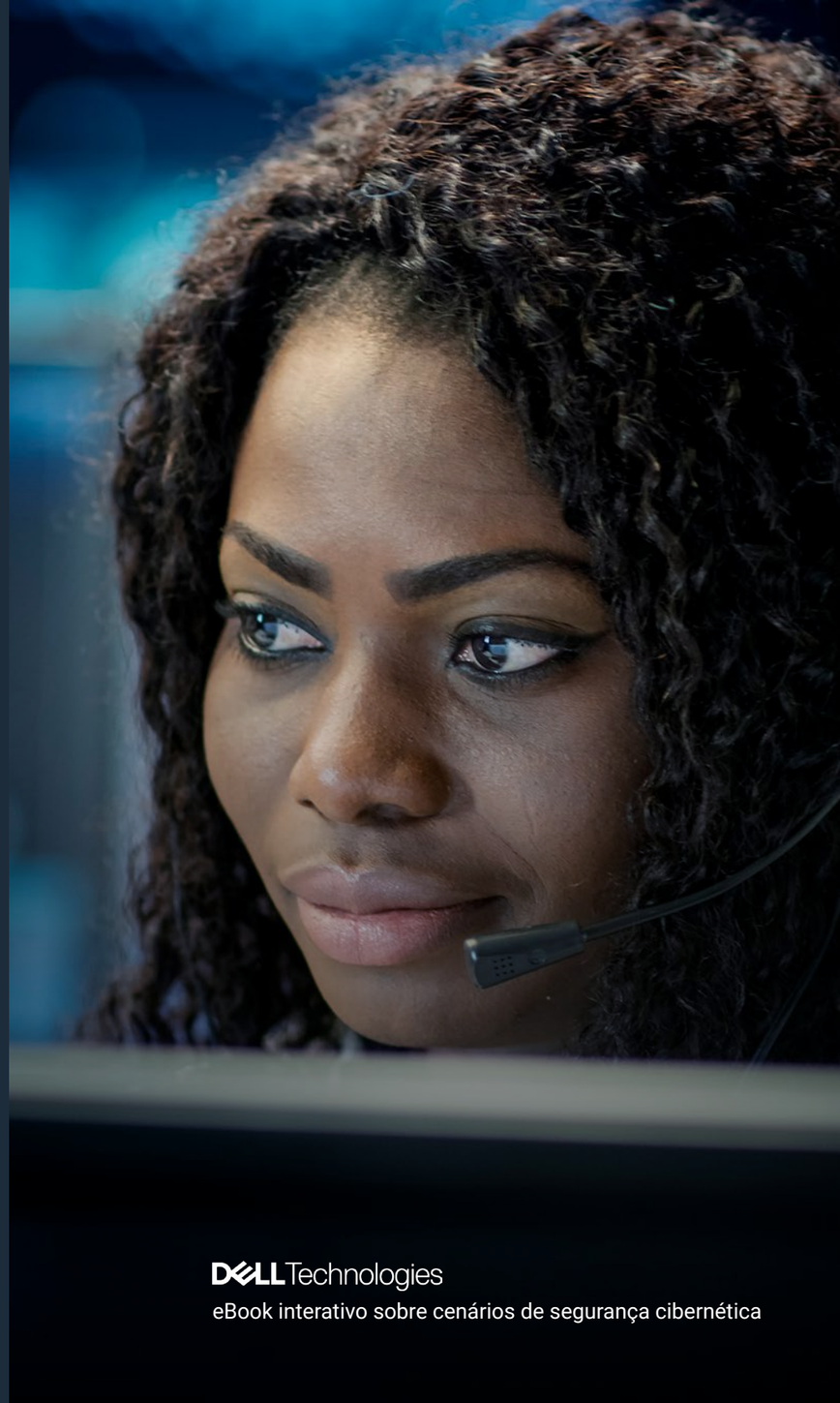
Tipo de ataque: Injeção de Prompt/SQL

1 — 2: Detectar e responder a ameaças cibernéticas — 3 — 4

Você percebe que foi atingido por um ataque de injeção de Prompt/SQL por meio do chatbot de atendimento ao cliente. O que você deve fazer?

- [ ] Deixar os bots off-line
- [ ] Investigar logs do banco de dados em busca de acesso não autorizado e dados roubados, modificados ou excluídos
- [ ] Cumprir todas as leis de divulgação de violação de dados
- [ ] Todas as alternativas acima

Veja a resposta correta →



DELL Technologies

eBook interativo sobre cenários de segurança cibernética

Tipo de ataque: Injeção de Prompt/SQL

1 — 2: Detectar e responder a ameaças cibernéticas — 3 — 4

Você percebe que foi atingido por um ataque de injeção de Prompt/SQL por meio do chatbot de atendimento ao cliente. O que você deve fazer?

- [x] Deixar os bots off-line
- [x] Investigar logs do banco de dados em busca de acesso não autorizado e dados roubados, modificados ou excluídos
- [x] Cumprir todas as leis de divulgação de violação de dados
- [x] Todas as alternativas acima

A resposta a um ataque de injeção de Prompt/SQL requer deixar o chatbot off-line, verificar nos logs de banco de dados se há acesso não autorizado e garantir a conformidade com as leis de divulgação. Estas etapas são essenciais para interromper a exploração, avaliar os danos e cumprir as obrigações regulatórias e éticas.

Próxima pergunta →

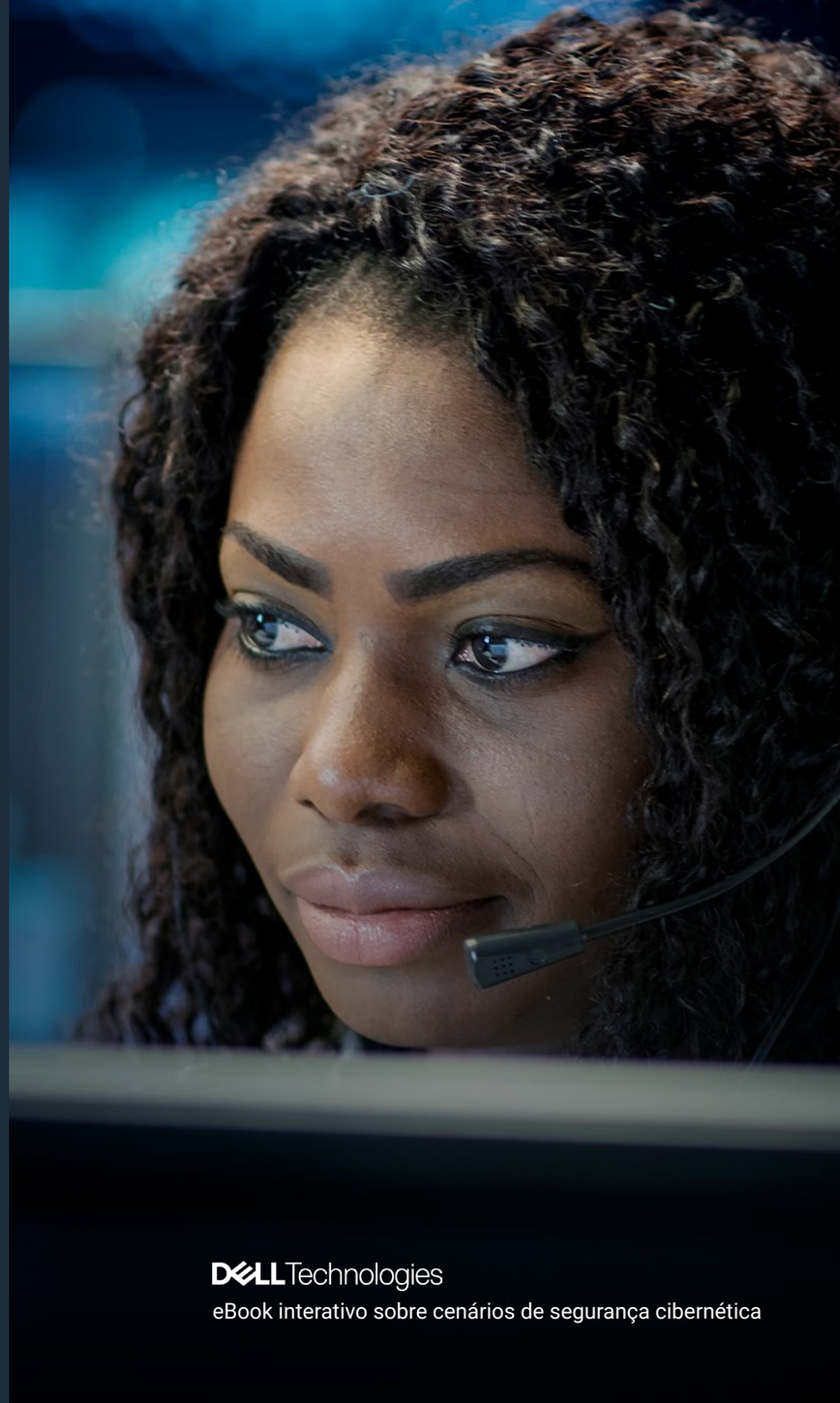
Tipo de ataque: Injeção de Prompt/SQL

1 — 2 — 3: Recuperar-se de um ataque cibernético — 4

Que recursos você deve implementar para ajudar a interromper injeções de prompt/SQL?

- [ ] Instruir as equipes de desenvolvimento a usar instruções preparadas e consultas parametrizadas como prática de codificação
- [ ] Ferramentas de Managed Detection and Response (MDR)
- [ ] Implementar acesso com privilégios mínimos, como autenticação baseada em vários fatores (MFA), controle de acesso baseado em função (RBAC), firewall de aplicativos da Web (WAF) etc.
- [ ] Segmentar bancos de dados de back-end/bases de conhecimento

Veja a resposta correta →



DELL Technologies

eBook interativo sobre cenários de segurança cibernética

Tipo de ataque: Injeção de Prompt/SQL

1 — 2 — 3: Recuperar-se de um ataque cibernético — 4

Que recursos você deve implementar para ajudar a interromper injeções de prompt/SQL?

- ✓ Instruir as equipes de desenvolvimento a usar instruções preparadas e consultas parametrizadas como prática de codificação
- ✗ Ferramentas de Managed Detection and Response (MDR)
- ✓ Implementar acesso com privilégios mínimos, como autenticação baseada em vários fatores (MFA), controle de acesso baseado em função (RBAC), firewall de aplicativos da Web (WAF) etc.
- ✗ Segmentar bancos de dados de back-end/bases de conhecimento

O treinamento das equipes de desenvolvimento para usar declarações preparadas e consultas com base em parâmetros bloqueia ataques de injeção de SQL na origem, enquanto impõe controles de acesso com privilégios mínimos, como MFA, RBAC e WAF, e limita o impacto de qualquer tentativa de injeção, impedindo que invasores escalem privilégios ou se movam lateralmente.

Próxima pergunta →

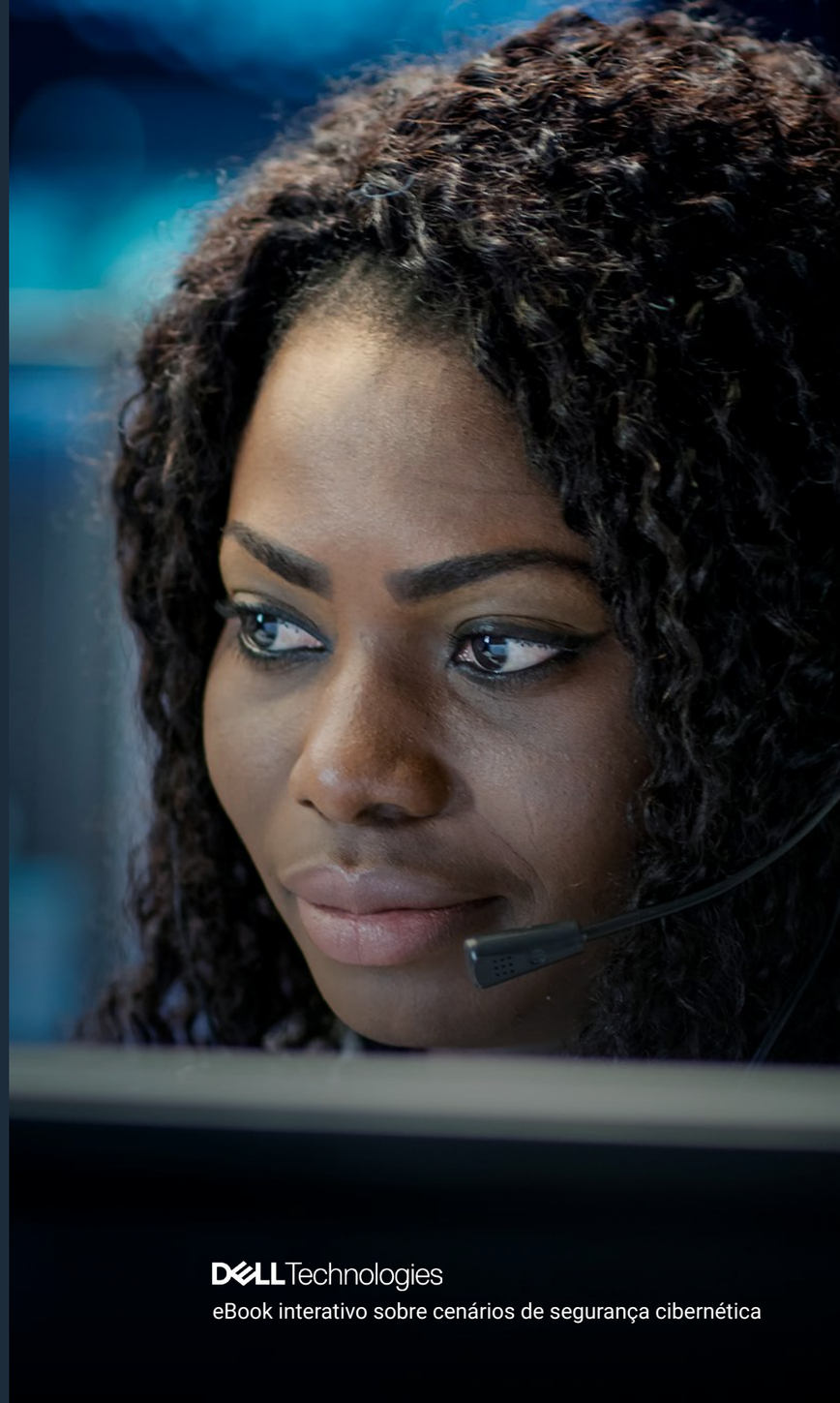
Tipo de ataque: Injeção de Prompt/SQL

1 2 3 4: Melhores práticas em geral

Quais medidas você tomaria para recuperar os dados dos clientes da companhia aérea?

- [ ] Rastrear os dados roubados
- [ ] Pedir aos clientes para reconstruir seus perfis
- [ ] Comprar os dados de volta dos invasores cibernéticos
- [ ] Fazer a restauração a partir do backup não comprometido mais recente para recuperar as milhas dos clientes e solicitar que eles alterem a senhas e verifiquem os cartões de crédito

Veja a resposta correta →



DELL Technologies

eBook interativo sobre cenários de segurança cibernética

Tipo de ataque: Injeção de Prompt/SQL

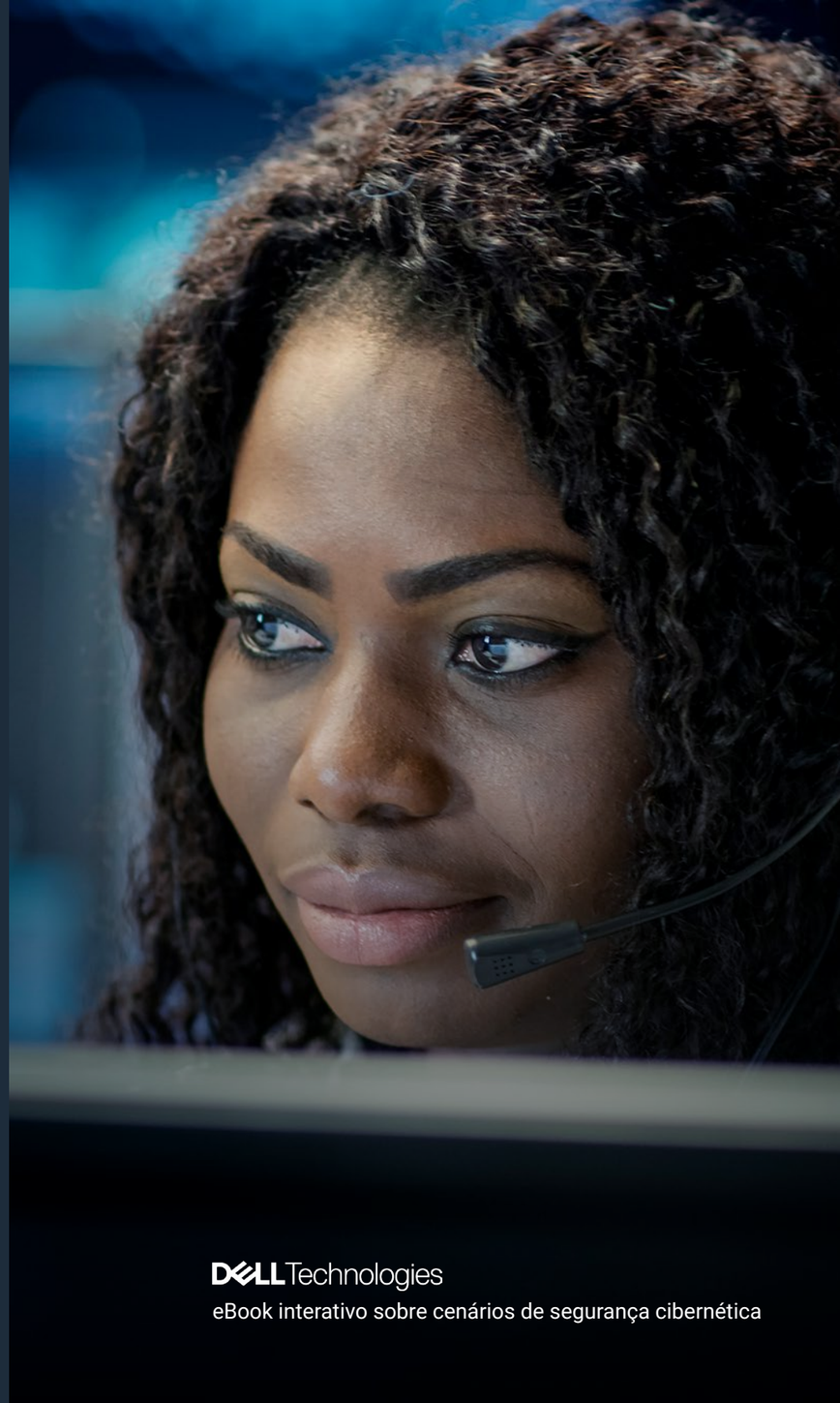
1 — 2 — 3 — 4: Melhores práticas em geral

Quais medidas você tomaria para recuperar os dados dos clientes da companhia aérea?

- ✗ Rastrear os dados roubados
- ✗ Pedir aos clientes para reconstruir seus perfis
- ✗ Comprar os dados de volta dos invasores cibernéticos
- ✓ Fazer a restauração a partir do backup não comprometido mais recente para recuperar as milhas dos clientes e solicitar que eles alterem a senhas e verifiquem os cartões de crédito

A recuperação de dados perdidos da conta a partir do backup não comprometido mais recente ajuda a manter a integridade dos dados e a reduzir o tempo de inatividade. Solicitar imediatamente que os clientes redefinam suas senhas e monitorem a atividade de seus cartões de crédito contribui para a conformidade regulatória após um ataque de injeção destrutivo.

Veja as soluções →



TIPO DE ATAQUE: INJEÇÃO DE PROMPT/SQL

Recapitulação

Ataques de injeção de prompt e SQL têm se mostrado repetidamente entre os métodos mais prejudiciais e difundidos de ataques cibernéticos usados por cibercriminosos. Esses ataques exploram vulnerabilidades em sistemas de banco de dados ou consulta do usuário, permitindo que agentes mal-intencionados manipulem servidores, roubem dados ou interrompam fluxos de trabalho.

A proteção de sua organização contra ameaças e ataques de injeção de Prompt/SQL em evolução faz parte do compromisso contínuo da Dell com a segurança cibernética. Dessa forma, fornecemos as ferramentas e a experiência necessárias para detecção, resposta e recuperação.

Descubra estratégias avançadas de resiliência cibernética e veja como a Dell pode capacitar sua organização para se defender contra ataques de injeção de Prompt e SQL.

Explore o resumo de injeção de Prompt/SQL →

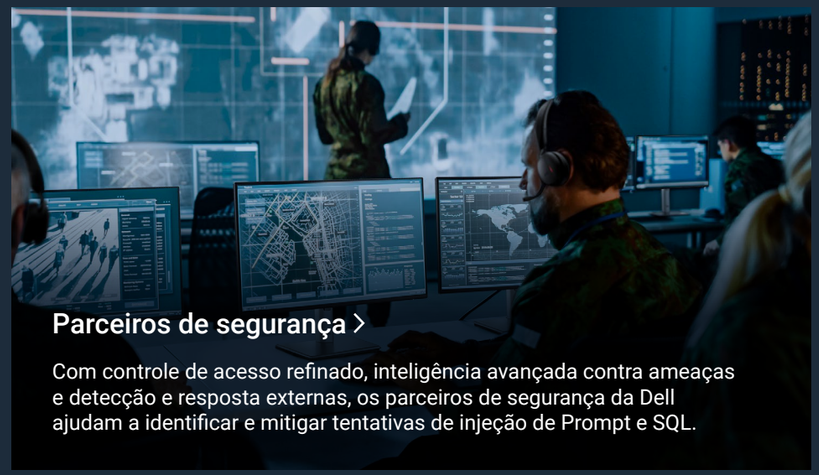
Voltar para Cenários

Espaço de trabalho confiável e infraestrutura confiável >

Protege os endpoints e reduz o risco de que credenciais comprometidas sejam exploradas em ataques de injeção.

Servidores PowerEdge >

Com raiz de confiança de hardware, inicialização segura, segurança baseada em chip e validação de configuração em tempo real, os servidores Dell PowerEdge garantem uma infraestrutura resistente a violações que executa apenas código confiável.



Parceiros de segurança >

Com controle de acesso refinado, inteligência avançada contra ameaças e detecção e resposta externas, os parceiros de segurança da Dell ajudam a identificar e mitigar tentativas de injeção de Prompt e SQL.

Portfólio do PowerProtect >

Os backups imutáveis com air gap e a lógica analítica avançada de recuperação cibernética da Dell fornecem pontos de restauração confiáveis, permitindo a recuperação rápida de corrupções ou exfiltrações de dados.

Serviços de segurança e resiliência >

Do treinamento de desenvolvimento seguro e testes de violação até busca de ameaças e resposta a incidentes, os especialistas e parceiros da Dell ajudam a validar proteções e permitem correção rápida de ataques de injeção.

Tipo de ataque: Ransomware

Você é um profissional de TI em um hospital regional reconhecido pelos sistemas médicos conectados — incluindo prontuários médicos digitais (EHR), bombas de infusão inteligentes e imagens de radiologia, tudo conectado a uma rede centralizada.

Na noite passada, vários sistemas começaram a falhar simultaneamente. Pela manhã, a equipe clínica relatou que estava impedida de acessar os registros de pacientes.

Vários terminais exibiam a seguinte nota de resgate:

"Seus arquivos estão criptografados. Pague 20 bitcoins em 72 horas ou os dados dos pacientes serão divulgados."

Teste seu conhecimento →

Tipo de ataque: Ransomware

1: Reduzir a superfície de ataque — 2 — 3 — 4

O help desk recebe mais de 100 relatórios de criptografia de arquivos e erros de aplicativos. Os logs de segurança mostram atividades incomuns de renomeação de arquivos de uma conta de domínio interno. Qual é o primeiro passo?

- [ ] Pagar o resgate imediatamente para restaurar serviços críticos
- [ ] Notificar as autoridades policiais e a assessoria jurídica
- [ ] Começar a recriar imagens de todos os endpoints afetados
- [ ] Desconectar os sistemas infectados da rede

Veja a resposta correta →

Tipo de ataque: Ransomware

1: Reduzir a superfície de ataque — 2 — 3 — 4

O help desk recebe mais de 100 relatórios de criptografia de arquivos e erros de aplicativos. Os logs de segurança mostram atividades incomuns de renomeação de arquivos de uma conta de domínio interno. Qual é o primeiro passo?

- ✗ Pagar o resgate imediatamente para restaurar serviços críticos
- ✗ Notificar as autoridades policiais e a assessoria jurídica
- ✗ Começar a recriar imagens de todos os endpoints afetados
- ✓ Desconectar os sistemas infectados da rede

Desconectar e isolar imediatamente os sistemas hospitalares infectados impede a disseminação do ransomware, protege dispositivos médicos essenciais e dados confidenciais de pacientes, preserva evidências para investigação e ganha tempo vital para uma resposta e recuperação coordenadas.

Próxima pergunta →

Tipo de ataque: Ransomware

1 — 2: Detectar e responder a ameaças cibernéticas — 3 — 4

A equipe de Resposta a incidentes descobre que o ataque provavelmente começou a partir de uma conta comprometida, que foi usada para acessar um servidor sem autenticação baseada em vários fatores (MFA). Qual das seguintes opções contribuiu mais diretamente para o ataque?

- [ ] Definições de antivírus desatualizadas
- [ ] Um banco de dados de registros eletrônicos de saúde (EHR) exposto
- [ ] Falta de MFA no acesso remoto
- [ ] Filtragem fraca de e-mails

Veja a resposta correta →

Tipo de ataque: Ransomware

1 — 2: Detectar e responder a ameaças cibernéticas — 3 — 4

A equipe de Resposta a incidentes descobre que o ataque provavelmente começou a partir de uma conta comprometida, que foi usada para acessar um servidor sem autenticação baseada em vários fatores (MFA). Qual das seguintes opções contribuiu mais diretamente para o ataque?

- ✗ Definições de antivírus desatualizadas
- ✗ Um banco de dados de registros eletrônicos de saúde (EHR) exposto
- ✓ Falta de MFA no acesso remoto
- ✗ Filtragem fraca de e-mails

A falta de MFA no acesso remoto possibilitou a violação do servidor, permitindo que invasores efetuassem log-in com credenciais roubadas ou adivinhadas sem uma etapa extra de verificação. Com a MFA, até mesmo contas comprometidas exigiriam um segundo fator, reduzindo drasticamente o risco de acesso não autorizado.

Próxima pergunta →

Tipo de ataque: Ransomware

1 2 3: Recuperar-se de um ataque cibernético 4

A equipe médica agora depende de fluxos de trabalho em papel. Pacientes com cirurgia agendada para hoje não podem ser verificados no sistema. Qual é a melhor ação de curto prazo para oferecer suporte às operações do hospital?

- [ ] Reiniciar o servidor principal do banco de dados para tentar a reinicialização
- [ ] Habilitar todos os backups antigos, mesmo que tenham seis meses
- [ ] Ativar os procedimentos manuais de tempo de inatividade do hospital e encaminhar o caso para a equipe de resposta a emergências
- [ ] Deixar a equipe decidir como proceder caso a caso

Veja a resposta correta →

Tipo de ataque: Ransomware

1 2 3: Recuperar-se de um ataque cibernético 4

A equipe médica agora depende de fluxos de trabalho em papel. Pacientes com cirurgia agendada para hoje não podem ser verificados no sistema. Qual é a melhor ação de curto prazo para oferecer suporte às operações do hospital?

- ✗ Reiniciar o servidor principal do banco de dados para tentar a reinicialização
- ✗ Habilitar todos os backups antigos, mesmo que tenham seis meses
- ✓ Ativar os procedimentos manuais de tempo de inatividade do hospital e encaminhar o caso para a equipe de resposta a emergências
- ✗ Deixar a equipe decidir como proceder caso a caso

A ativação de procedimentos manuais de inatividade e o encaminhamento para a equipe de resposta a emergências garantem a continuidade imediata de fluxos de trabalho clínicos críticos, protegem a segurança do paciente e estabelecem um processo padronizado para verificar e documentar o atendimento. Essa abordagem minimiza erros, gerencia riscos e recursos com eficiência e oferece suporte a especialistas na restauração segura de sistemas digitais.

Próxima pergunta →

Tipo de ataque: Ransomware

1 2 3 4: Melhores práticas em geral

O caso ganhou a atenção da mídia local. A liderança quer saber se deve emitir uma declaração pública, e o departamento jurídico está perguntando sobre as obrigações da lei Health Insurance Portability and Accountability Act (HIPAA). Qual é a próxima etapa mais apropriada?

- [ ] Negar o incidente publicamente até que mais informações estejam disponíveis
- [ ] Emitir um comunicado à imprensa culpando o fornecedor terceirizado de TI
- [ ] Notificar os órgãos reguladores e iniciar procedimentos internos de notificação de violação
- [ ] Pagar o resgate imediatamente e evitar a atenção do público

Veja a resposta correta →

Tipo de ataque: Ransomware

1 — 2 — 3 — 4: Melhores práticas em geral

O caso ganhou a atenção da mídia local. A liderança quer saber se deve emitir uma declaração pública, e o departamento jurídico está perguntando sobre as obrigações da lei Health Insurance Portability and Accountability Act (HIPAA). Qual é a próxima etapa mais apropriada?

- ✗ Negar o incidente publicamente até que mais informações estejam disponíveis
- ✗ Emitir um comunicado à imprensa culpando o fornecedor terceirizado de TI
- ✓ Notificar os órgãos reguladores e iniciar procedimentos internos de notificação de violação
- ✗ Pagar o resgate imediatamente e evitar a atenção do público

Denunciar imediatamente as violações de informações de saúde protegidas às autoridades e aos indivíduos afetados, conforme exigido pela lei HIPAA e pelas leis estaduais, garante a conformidade regulatória, a proteção jurídica e a transparência das práticas recomendadas para evitar danos legais e à reputação, cumprindo as obrigações de divulgação obrigatórias e estabelecendo a comunicação adequada com os pacientes, a equipe e as partes interessadas.

Veja as soluções →

TIPO DE ATAQUE: RANSOMWARE

Recapitulação

Ransomware é um tipo de malware que bloqueia o acesso aos dados ou ao sistema de computador até que um resgate seja pago. É um dos tipos mais disruptivos de ataques cibernéticos. 50% das organizações em todo o mundo foram atingidas por ransomware pelo menos uma vez no ano passado e o tempo médio de inatividade após um ataque de ransomware é de três semanas, levando a interrupções operacionais significativas.

Na Dell, priorizamos a proteção de sua organização com estruturas Zero Trust, proteção de endpoints e segmentação de rede para bloquear a entrada de ransomware e limitar sua disseminação. Com o planejamento de resposta a incidentes liderado por especialistas, ajudamos você a se manter resiliente e a se recuperar rapidamente de ataques.

Saiba mais sobre estratégias avançadas de resiliência cibernética e como a Dell pode ajudar você a proteger sua organização contra ataques de ransomware.

Explore resumos de ataques de ransomware →

Voltar para Cenários

Infraestrutura confiável >

Bloquear ransomware no nível da infraestrutura com autenticação de hardware, autenticação baseada em vários fatores (MFA), controle de acesso baseado em função (RBAC) e estruturas Zero Trust.

Rede e servidores PowerEdge >

Restringir a movimentação de ransomware. Com segmentação de rede, inicialização segura, raiz de confiança de chip, gerenciamento dinâmico de portas USB e bloqueio do sistema.

Espaço de trabalho confiável >

Integrar ferramentas SafeBIOS, SafeID, SafeData e Detecção e resposta de endpoint (EDR) para oferecer inteligência proativa contra ameaças, detecção em tempo real e contenção automatizada de malware no nível do dispositivo.

Portfólio do PowerProtect >

Proteger dados essenciais com backups com air gap e não modificados, lógica analítica inteligente de recuperação cibernética e recursos de restauração rápida para prevenir extorsão e permitir resiliência.

Serviços de segurança e resiliência >

Fazer parcerias com especialistas como a CrowdStrike para ajudar com avaliações, gerenciamento de vulnerabilidades, treinamento de conscientização de segurança, testes de violação e resposta a incidentes.

Tipo de ataque: Hardware da cadeia de suprimentos

Sua empresa compra 500 novos notebooks em seus escritórios globais. Para acelerar o processo, você terceirizou a preparação de imagens e hardware para um fornecedor terceirizado de logística de TI. Eles enviam máquinas pré-configuradas diretamente aos funcionários.

Em alguns dias, você recebe várias chamadas do campo informando:

- As solicitações de autenticação baseada em vários fatores (MFA) não estão sendo exigidas e não estão funcionando corretamente.
- A equipe de segurança observa vários logins de administrador não autorizados em horários estranhos.
- Eles também observam tráfego de rede virtual privada (VPN) de usuários que supostamente estão off-line.

Teste seu conhecimento →

Tipo de ataque: Hardware da cadeia de suprimentos

1: Reduzir a superfície de ataque 2 3 4

Um funcionário relata receber notificações por push de autenticação baseada em vários fatores (MFA) sem estar tentando fazer log-in. O painel de segurança de sua organização mostra que o log-in se originou de um dispositivo com uma etiqueta de inventário emitida pela empresa. Qual é o primeiro passo mais lógico para a equipe do centro de operações de segurança (SOC)?

- [ ] Desativar a conta do usuário e limpar o notebook remotamente
- [ ] Comparar o IP de log-in e a impressão digital do dispositivo com outros usuários comprometidos conhecidos
- [ ] Fazer o encaminhamento para o RH presumindo que o usuário é o responsável
- [ ] Emitir um alerta para toda a empresa para que as senhas sejam alteradas imediatamente

Veja a resposta correta →

Tipo de ataque: Hardware da cadeia de suprimentos

1: Reduzir a superfície de ataque — 2 — 3 — 4

Um funcionário relata receber notificações por push de autenticação baseada em vários fatores (MFA) sem estar tentando fazer log-in. O painel de segurança de sua organização mostra que o log-in se originou de um dispositivo com uma etiqueta de inventário emitida pela empresa. Qual é o primeiro passo mais lógico para a equipe do centro de operações de segurança (SOC)?

- ✗ Desativar a conta do usuário e limpar o notebook remotamente
- ✓ Comparar o IP de log-in e a impressão digital do dispositivo com outros usuários comprometidos conhecidos
- ✗ Fazer o encaminhamento para o RH presumindo que o usuário é o responsável
- ✗ Emitir um alerta para toda a empresa para que as senhas sejam alteradas imediatamente

Quando sua equipe de SOC determina que uma atividade suspeita faz parte de um ataque mais amplo ou isolado para permitir o reconhecimento rápido de padrões, a resposta direcionada a incidentes e a contenção de outros riscos é a primeira etapa lógica ao identificar um ataque de hardware da cadeia de suprimentos.

Próxima pergunta →

Tipo de ataque: Hardware da cadeia de suprimentos

1 — 2: Detectar e responder a ameaças cibernéticas — 3 — 4

Sua equipe de resposta a incidentes descobriu que vários notebooks afetados estão executando versões de firmware da SSD que não correspondem às notas oficiais da versão do fornecedor. O recurso Detecção e resposta de endpoint (EDR) não mostra processos mal-intencionados. O que isso provavelmente indica?

- [ ] Um erro de configuração do fornecedor de TI
- [ ] Um novo tipo de ransomware que se exclui automaticamente
- [ ] Um comprometimento da cadeia de suprimentos no nível do firmware
- [ ] Comportamento normal durante a criação de imagens

Veja a resposta correta →

Tipo de ataque: Hardware da cadeia de suprimentos

1 — 2: Detectar e responder a ameaças cibernéticas — 3 — 4

Sua equipe de resposta a incidentes descobriu que vários notebooks afetados estão executando versões de firmware da SSD que não correspondem às notas oficiais da versão do fornecedor. O recurso Detecção e resposta de endpoint (EDR) não mostra processos mal-intencionados. O que isso provavelmente indica?

- ✗ Um erro de configuração do fornecedor de TI
- ✗ Um novo tipo de ransomware que se exclui automaticamente
- ✓ Um comprometimento da cadeia de suprimentos no nível do firmware
- ✗ Comportamento normal durante a criação de imagens

O firmware de SSD não autorizado em vários notebooks, não detectado pela EDR e incompatível com as versões oficiais indica adulteração deliberada de hardware ou firmware — marca registrada de um comprometimento da cadeia de suprimentos no nível do firmware.

Próxima pergunta →

Tipo de ataque: Hardware da cadeia de suprimentos

1 — 2 — 3: Recuperar-se de um ataque cibernético — 4

Você isolou 100 dispositivos suspeitos com o firmware de SSD nocivo. Você precisa decidir como prosseguir sem alertar o invasor, que pode ter acesso remoto. Qual é o melhor próximo passo?

- [ ] Desligar todos os dispositivos e enviá-los para a perícia forense
- [ ] Realizar dumps de memória ao vivo e investigar enquanto os sistemas estão em execução
- [ ] Notificar ao fornecedor terceirizado que os dispositivos foram violados
- [ ] Apagar todos os dispositivos e reenviar novos notebooks para todos os usuários globalmente

Veja a resposta correta →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

Tipo de ataque: Hardware da cadeia de suprimentos

1 — 2 — 3: Recuperar-se de um ataque cibernético — 4

Você isolou 100 dispositivos suspeitos com o firmware de SSD nocivo. Você precisa decidir como prosseguir sem alertar o invasor, que pode ter acesso remoto. Qual é o melhor próximo passo?

- ✗ Desligar todos os dispositivos e enviá-los para a perícia forense
- ✓ Realizar dumps de memória ao vivo e investigar enquanto os sistemas estão em execução
- ✗ Notificar ao fornecedor terceirizado que os dispositivos foram violados
- ✗ Apagar todos os dispositivos e reenviar novos notebooks para todos os usuários globalmente

Os dumps de memória em tempo real são cruciais para preservar evidências voláteis, como malware e rootkits ativos, permitindo uma resposta direcionada a incidentes com a detecção de ameaças e pontos de acesso ocultos antes que eles sejam perdidos ou que os invasores sejam alertados.

Próxima pergunta →

Tipo de ataque: Hardware da cadeia de suprimentos

1 2 3 4: Melhores práticas em geral

O diretor de segurança da informação solicita um resumo de como esse ataque entrou em seu ambiente. Você precisa apresentar uma explicação concisa para a equipe executiva. Como você deve explicar o ataque?

- [ ] Um vírus foi baixado acidentalmente de um link de phishing
- [ ] Tivemos uma configuração incorreta de rede que permitiu acesso externo
- [ ] O firmware mal-intencionado foi introduzido por um fornecedor de hardware comprometido durante o provisionamento de notebooks
- [ ] Um de nossos desenvolvedores enviou código não seguro para a produção

Veja a resposta correta →

Tipo de ataque: Hardware da cadeia de suprimentos

1 — 2 — 3 — 4: Melhores práticas em geral

O diretor de segurança da informação solicita um resumo de como esse ataque entrou em seu ambiente. Você precisa apresentar uma explicação concisa para a equipe executiva. Como você deve explicar o ataque?

- ✗ Um vírus foi baixado acidentalmente de um link de phishing
- ✗ Tivemos uma configuração incorreta de rede que permitiu acesso externo
- ✓ O firmware mal-intencionado foi introduzido por um fornecedor de hardware comprometido durante o provisionamento de notebooks
- ✗ Um de nossos desenvolvedores enviou código não seguro para a produção

As versões de firmware incompatíveis e a ausência de malware ativo confirmam que esse foi um ataque no nível de firmware, proveniente do fornecedor, e não de erro do usuário ou de configuração incorreta.

Veja as soluções →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

TIPO DE ATAQUE: HARDWARE DA CADEIA DE SUPRIMENTOS

Recapitulação

Os ataques à cadeia de suprimentos aumentaram substancialmente nos últimos anos. Ao adulterar dispositivos físicos durante a produção, envio ou implementação, ou ao encontrar vulnerabilidades em provedores de software, os invasores obtêm meios de injetar componentes ou códigos mal-intencionados, corromper sistemas ou exfiltrar dados confidenciais. As vítimas podem variar de pequenas empresas a multinacionais, com resultados que incluem perdas financeiras graves, comprometimento da confiança do cliente e repercussões legais.

A Dell reduz os ataques de hardware na cadeia de suprimentos integrando avaliações rigorosas de risco de fornecedores e incorporando princípios Zero Trust, juntamente com validação contínua de dispositivos e verificações independentes de integridade. Fortalecemos a integridade do hardware em todo o seu ciclo de vida.

Saiba mais sobre estratégias avançadas de resiliência cibernética para ver como a Dell pode ajudar você a proteger sua organização contra ataques de hardware na cadeia de suprimentos.

Explore o resumo de ataques de hardware na cadeia de suprimentos →

Voltar para Cenários

Garantia da cadeia de suprimentos >

Com proveniência avançada, logística à prova de adulteração e fornecimento transparente, a cadeia de suprimentos da Dell garante que hardware, firmware e fornecedores sejam rigorosamente verificados antes de chegar à sua organização.

Secure Component Verification (SCV) >

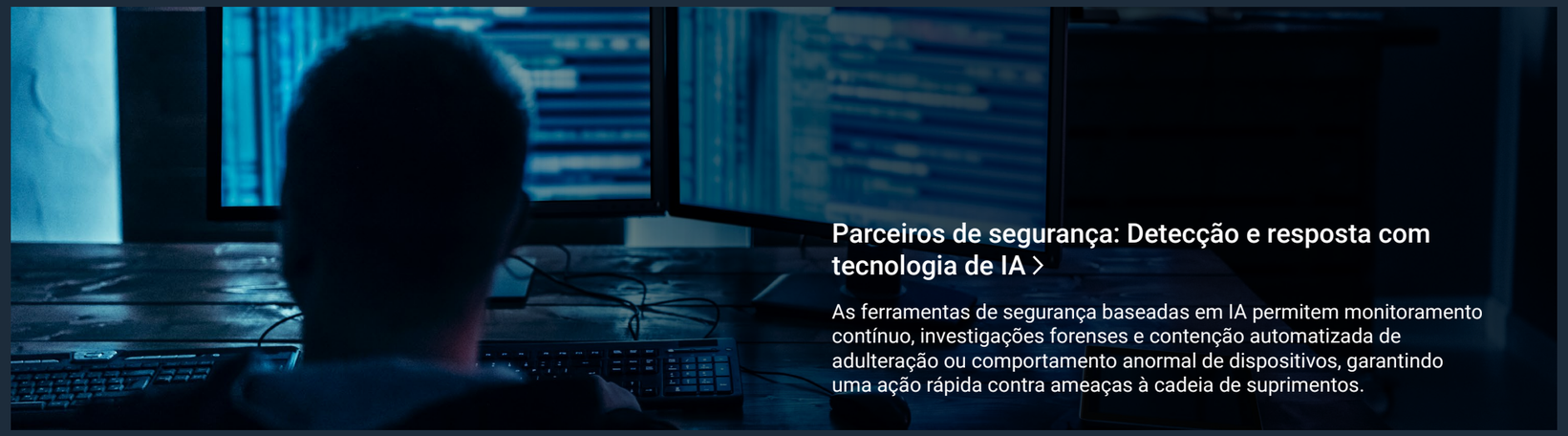
A verificação criptográfica dos componentes do PC na fábrica e durante a instalação garante a autenticidade, detecta alterações ocultas e reduz os riscos de adulteração da cadeia de suprimentos.

Espaço de trabalho confiável e infraestrutura confiável >

A autenticação baseada em hardware e as verificações contínuas de integridade do firmware protegem os endpoints, alertando você sobre alterações não autorizadas ou implantações mal-intencionadas antes que se tornem ameaças.

Rastreamento de ativos e ProSupport Suite com SupportAssist >

O rastreamento abrangente de ativos, o monitoramento em tempo real da proveniência do dispositivo e a verificação proativa da integridade garantem a detecção rápida de anomalias e a segurança em todo o parque de dispositivos.



Parceiros de segurança: Detecção e resposta com tecnologia de IA >

As ferramentas de segurança baseadas em IA permitem monitoramento contínuo, investigações forenses e contenção automatizada de adulteração ou comportamento anormal de dispositivos, garantindo uma ação rápida contra ameaças à cadeia de suprimentos.

Tipo de ataque: Software da cadeia de suprimentos

Sua empresa fornece software de lógica analítica baseada em nuvem usado por hospitais. Os serviços de back-end dependem de uma biblioteca de logs de código aberto amplamente utilizada e mantida por um desenvolvedor terceirizado confiável no GitHub.

Sem o conhecimento da equipe de desenvolvedores, os invasores comprometeram a conta do GitHub e inseriram uma atualização mal-intencionada que inclui código oculto projetado para:

- Exfiltrar variáveis de ambiente, incluindo chaves de interface de programação de aplicativos (API) e segredos de tokens da Web de JavaScript Object Notation (JWT)
- Criar um shell reverso quando IPs específicos fizerem solicitações
- Permanecer inativo, a menos que seja acionado remotamente

Teste seu conhecimento →

Tipo de ataque: Software da cadeia de suprimentos

1: Reduzir a superfície de ataque 2 3 4

De repente, sua API começa a retornar erros 500 aos principais clients. O monitoramento em nuvem indica conexões de saída dos seus serviços em contêineres para um domínio não visto anteriormente. Qual é a sua primeira resposta?

- [ ] Desativar todo o tráfego de rede de saída dos contêineres
- [ ] Reinicializar os serviços afetados para eliminar quaisquer problemas de memória
- [ ] Verificar se há confirmações recentes de código em seu repositório do GitHub
- [ ] Entrar em contato com o provedor de hospedagem do domínio

Veja a resposta correta →

Tipo de ataque: Software da cadeia de suprimentos

1: Reduzir a superfície de ataque — 2 — 3 — 4

De repente, sua API começa a retornar erros 500 aos principais clients. O monitoramento em nuvem indica conexões de saída dos seus serviços em contêineres para um domínio não visto anteriormente. Qual é a sua primeira resposta?

- ✓ Desativar todo o tráfego de rede de saída dos contêineres
- ✗ Reinicializar os serviços afetados para eliminar quaisquer problemas de memória
- ✗ Verificar se há confirmações recentes de código em seu repositório do GitHub
- ✗ Entrar em contato com o provedor de hospedagem do domínio

A desativação de todo o tráfego de rede de saída dos contêineres impede imediatamente que os invasores exfiltrem dados confidenciais ou estabeleçam acesso remoto por meio da biblioteca de logs comprometida, isolando seu ambiente em tempo real e ganhando um tempo crucial para investigar, proteger chaves e segredos de API e impedir a ativação de mecanismos de ataque inativos.

Próxima pergunta →

Tipo de ataque: Software da cadeia de suprimentos

1 — 2: Detectar e responder a ameaças cibernéticas — 3 — 4

O líder de engenharia confirma que o aplicativo extraiu o código automaticamente do GitHub três dias antes do início dos problemas. Essa versão ainda não foi marcada como mal-intencionada em nenhum banco de dados público. Qual é a ação imediata mais responsável?

- [ ] Entrar em contato com o mantenedor da biblioteca diretamente via GitHub
- [ ] Excluir todas as dependências do projeto local e reconstruir
- [ ] Aguardar as vulnerabilidades e exposições comuns (CVE) antes de tomar outras medidas
- [ ] Reverter para a última versão segura conhecida do código

Veja a resposta correta →

Tipo de ataque: Software da cadeia de suprimentos

1 — 2: Detectar e responder a ameaças cibernéticas — 3 — 4

O líder de engenharia confirma que o aplicativo extraiu o código automaticamente do GitHub três dias antes do início dos problemas. Essa versão ainda não foi marcada como mal-intencionada em nenhum banco de dados público. Qual é a ação imediata mais responsável?

- ✗ Entrar em contato com o mantenedor da biblioteca diretamente via GitHub
- ✗ Excluir todas as dependências do projeto local e reconstruir
- ✗ Aguardar as vulnerabilidades e exposições comuns (CVE) antes de tomar outras medidas
- ✓ Reverter para a última versão segura conhecida do código

A reversão para a última versão conhecida de código seguro remove imediatamente a atualização comprometida, elimina a presença do invasor e restaura a integridade operacional para conter proativamente riscos e proteger dados confidenciais.

Próxima pergunta →

Tipo de ataque: Software da cadeia de suprimentos

1 — 2 — 3: Recuperar-se de um ataque cibernético — 4

A análise confirma que a biblioteca estava exfiltrando chaves de API e credenciais de nuvem. Você identificou vários contêineres criados com a versão comprometida. Qual etapa é mais crítica em sua estratégia de contenção?

- [ ] Revogar e alternar todas as credenciais nos ambientes afetados
- [ ] Recriar a imagem dos contêineres usando uma imagem atualizada do sistema operacional (SO)
- [ ] Limpar os notebooks da equipe de desenvolvimento
- [ ] Registrar um aviso de remoção para o repositório do GitHub

Veja a resposta correta →

Tipo de ataque: Software da cadeia de suprimentos

1 — 2 — 3: Recuperar-se de um ataque cibernético — 4

A análise confirma que a biblioteca estava exfiltrando chaves de API e credenciais de nuvem. Você identificou vários contêineres criados com a versão comprometida. Qual etapa é mais crítica em sua estratégia de contenção?

- ✓ Revogar e alternar todas as credenciais nos ambientes afetados
- ✗ Recriar a imagem dos contêineres usando uma imagem atualizada do sistema operacional (SO)
- ✗ Limpar os notebooks da equipe de desenvolvimento
- ✗ Registrar um aviso de remoção para o repositório do GitHub

Revogar e alternar credenciais é a primeira etapa essencial após um comprometimento da nuvem, bloqueando o acesso de invasores aos serviços, interrompendo o roubo de dados e protegendo os sistemas, independentemente do escopo da violação.

Próxima pergunta →

Tipo de ataque: Software da cadeia de suprimentos

1 2 3 4: Melhores práticas em geral

Você deve explicar o que aconteceu ao Diretor executivo de tecnologia e às equipes jurídica/de conformidade. Qual é a explicação mais precisa e clara? Como você resume o incidente?

- [ ] Nossas ferramentas internas de integração contínua e implementação/entrega contínua (CI/CD) falharam, permitindo a implementação de códigos inválidos
- [ ] Uma dependência de software de terceiros foi comprometida e nossa automação a colocou em produção
- [ ] Um desenvolvedor incluiu código não testado em uma versão apressada
- [ ] Um invasor realizou um ataque de força bruta em nosso repositório do GitHub

Veja a resposta correta →

Tipo de ataque: Software da cadeia de suprimentos

1 — 2 — 3 — 4: Melhores práticas em geral

Você deve explicar o que aconteceu ao Diretor executivo de tecnologia e às equipes jurídica/de conformidade. Qual é a explicação mais precisa e clara? Como você resume o incidente?

- ✗ Nossas ferramentas internas de integração contínua e implementação/entrega contínua (CI/CD) falharam, permitindo a implementação de códigos inválidos
- ✓ Uma dependência de software de terceiros foi comprometida e nossa automação a colocou em produção
- ✗ Um desenvolvedor incluiu código não testado em uma versão apressada
- ✗ Um invasor realizou um ataque de força bruta em nosso repositório do GitHub

A causa raiz foi um ataque à cadeia de suprimentos: os invasores comprometeram uma dependência de software de terceiros e o processo automatizado de compilação colocou a atualização mal-intencionada diretamente para a produção, impactando a integridade do aplicativo e os ambientes sensíveis, e destacando o risco de atualizações mal-intencionadas em dependências externas confiáveis.

Veja as soluções →

TIPO DE ATAQUE: SOFTWARE DA CADEIA DE SUPRIMENTOS

Recapitulação

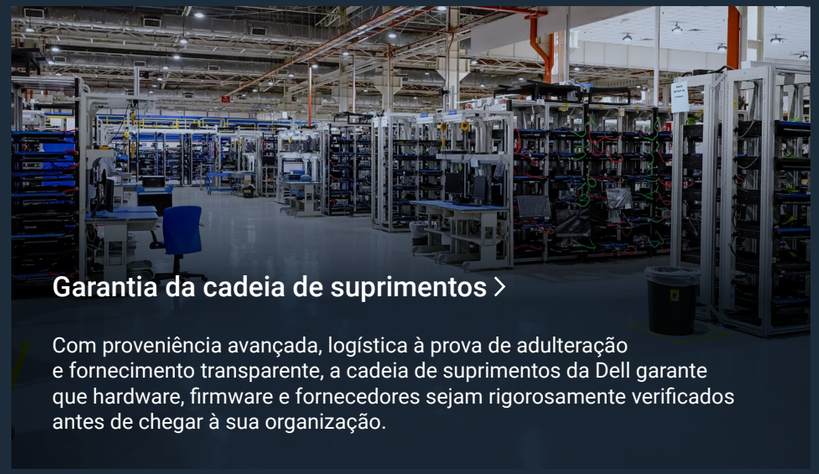
Os ataques cibernéticos a softwares da cadeia de suprimentos exploram vulnerabilidades em atualizações de software, integrações de terceiros e ambientes de desenvolvimento para incorporar códigos mal-intencionados que se espalham pelas redes. Esses ataques podem causar violações de dados generalizadas, interrupções operacionais e comprometer ecossistemas inteiros, impactando empresas de todos os portes.

A Dell se dedica à resiliência cibernética, enfatizando a transparência, o desenvolvimento seguro e o monitoramento contínuo, mantendo um plano robusto de resposta a incidentes para garantir a recuperação rápida e a comunicação com as partes interessadas.

Saiba mais sobre estratégias avançadas de resiliência cibernética para ver como a Dell pode ajudar você a proteger sua organização contra ataques de software na cadeia de suprimentos.

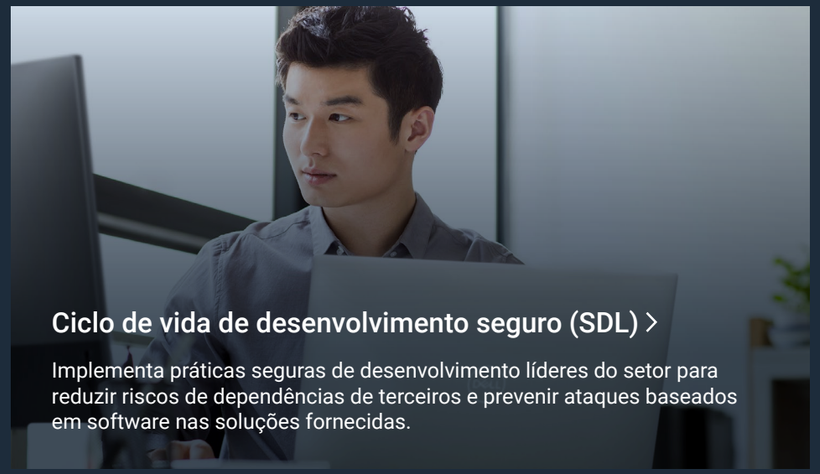
Explore o resumo de ataques de software na cadeia de suprimentos →

Voltar para Cenários



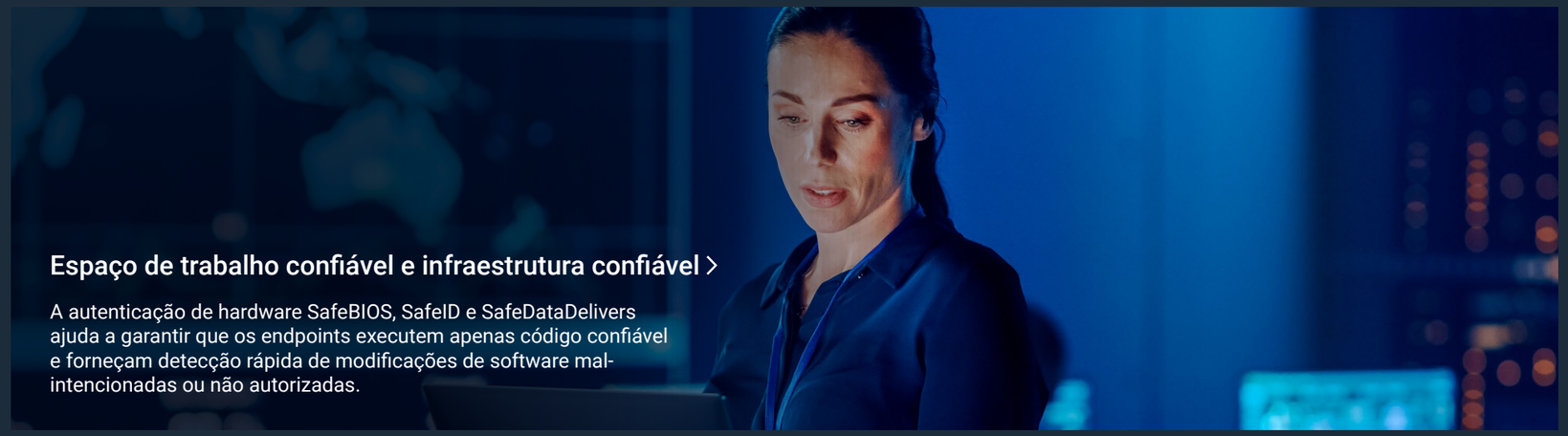
Garantia da cadeia de suprimentos >

Com proveniência avançada, logística à prova de adulteração e fornecimento transparente, a cadeia de suprimentos da Dell garante que hardware, firmware e fornecedores sejam rigorosamente verificados antes de chegar à sua organização.



Ciclo de vida de desenvolvimento seguro (SDL) >

Implementa práticas seguras de desenvolvimento líderes do setor para reduzir riscos de dependências de terceiros e prevenir ataques baseados em software nas soluções fornecidas.

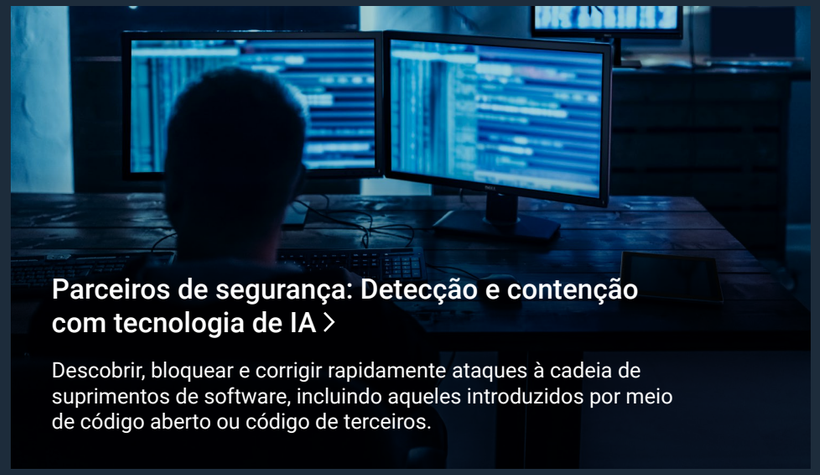


Espaço de trabalho confiável e infraestrutura confiável >

A autenticação de hardware SafeBIOS, SafeID e SafeDataDelivers ajuda a garantir que os endpoints executem apenas código confiável e forneçam detecção rápida de modificações de software mal-intencionadas ou não autorizadas.

Rastreamento de ativos e ProSupport Suite com SupportAssist >

O monitoramento em tempo real de dispositivos e softwares permite resposta e detecção rápidas a anomalias introduzidas na cadeia de suprimentos.



Parceiros de segurança: Detecção e contenção com tecnologia de IA >

Descobrir, bloquear e corrigir rapidamente ataques à cadeia de suprimentos de software, incluindo aqueles introduzidos por meio de código aberto ou código de terceiros.

Tipo de ataque: Dia zero

Você é um analista de segurança monitorando os logs de autenticação de uma empresa. Recentemente, usuários relataram acesso não autorizado às suas contas, mesmo sem compartilhar suas credenciais.

Ao investigar os logs, você encontra a seguinte atividade:

```
[INFO] 2025-04-02 14:05:12 - User Login - UserID: 1023 - IP: 192.168.1.15 - JWT Token Issued
[INFO] 2025-04-02 14:07:35 - User Login - UserID: 1023 - IP: 5.62.60.12 - JWT Token Reused
[INFO] 2025-04-02 14:08:00 - User Login - UserID: 1023 - IP: 203.0.113.45 - JWT Token Reused
```

Ao mesmo tempo, um pesquisador de segurança identifica uma vulnerabilidade na interface de programação de aplicativos (API):

- Os tokens da Web de JavaScript Object Notation (JWT) nunca expiram.
- Os tokens ficam no armazenamento local, e não nos cookies somente HTTP.
- Nenhuma autenticação baseada em vários fatores (MFA) é aplicada.

Teste seu conhecimento →

Tipo de ataque: Dia zero

1: Reduzir a superfície de ataque 2 3 4

Como integrante da equipe de segurança, já que nenhuma sinal advertência foi acionado, você suspeita que se trata de um ataque de Dia zero. Qual seria o procedimento para confirmar isso?

- [ ] Desconectar todos os usuários de seus sistemas
- [ ] Identificar os principais comportamentos anômalos de autenticação nos logs
- [ ] Ligar para amigos em outras empresas para verificar se eles estão tendo o mesmo problema
- [ ] Tentar correlacionar com outras atividades anormais de segurança

Veja a resposta correta →

Tipo de ataque: Dia zero

1: Reduzir a superfície de ataque — 2 — 3 — 4

Como integrante da equipe de segurança, já que nenhuma sinal advertência foi acionado, você suspeita que se trata de um ataque de Dia zero. Qual seria o procedimento para confirmar isso?

- ✗ Desconectar todos os usuários de seus sistemas
- ✓ Identificar os principais comportamentos anômalos de autenticação nos logs
- ✗ Ligar para amigos em outras empresas para verificar se eles estão tendo o mesmo problema
- ✓ Tentar correlacionar com outras atividades anormais de segurança

A identificação de comportamentos anormais de autenticação, como horários de log-in incomuns, reutilização de credenciais ou acesso de dispositivos atípicos, e correlacioná-los com outras atividades anormais de segurança, como anomalias no acesso a dados ou escalonamento de privilégios, confirma um ataque coordenado de Dia zero.

Próxima pergunta →

Tipo de ataque: Dia zero

1 — 2: Detectar e responder a ameaças cibernéticas — 3 — 4

Como a vulnerabilidade é desconhecida, as equipes de segurança devem limitar os danos durante a investigação. Como você faria isso?

- [ ] Invalidar todas as sessões de autenticação em todo o sistema
- [ ] Concentrar todos os recursos no ponto de entrada do ataque
- [ ] Forçar log-ins apenas com autenticação baseada em vários fatores (MFA)
- [ ] Confiar nas regras atuais de firewalls estáticos ou de firewall de aplicativos da Web (WAF)

Veja a resposta correta →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

Tipo de ataque: Dia zero

1 — 2: Detectar e responder a ameaças cibernéticas — 3 — 4

Como a vulnerabilidade é desconhecida, as equipes de segurança devem limitar os danos durante a investigação. Como você faria isso?

- ✓ Invalidar todas as sessões de autenticação em todo o sistema
- ✗ Concentrar todos os recursos no ponto de entrada do ataque
- ✓ Forçar log-ins apenas com autenticação baseada em vários fatores (MFA)
- ✗ Confiar nas regras atuais de firewalls estáticos ou de firewall de aplicativos da Web (WAF)

Juntas, essas ações fortalecem a segurança e minimizam os riscos, ao mesmo tempo em que bloqueiam o acesso de invasores para que as equipes de segurança possam investigar e resolver a vulnerabilidade subjacente.

Próxima pergunta →

Tipo de ataque: Dia zero

1 2 3: Recuperar-se de um ataque cibernético 4

Os PCs da Dell possuem tecnologias como inicialização segura, trusted platform modules (TPM), proteção de senha do sistema básico de entrada/saída (BIOS) e SafeBIOS. Como elas podem ajudar em um ataque de Dia zero?

- [ ] Protegem contra ataques de dumping de credenciais que roubam tokens de interface de programação de aplicativos (API)
- [ ] Impedem que um invasor com acesso físico ignore a segurança do sistema operacional (SO) para instalar malware que rouba tokens de autenticação
- [ ] Garantem que invasores não consigam manipular as configurações do BIOS para enfraquecer a segurança do sistema operacional, o que pode levar ao sequestro de sessão de APIs
- [ ] Todas as alternativas acima

Veja a resposta correta →

Tipo de ataque: Dia zero

1 2 3: Recuperar-se de um ataque cibernético 4

Os PCs da Dell possuem tecnologias como inicialização segura, trusted platform modules (TPM), proteção de senha do sistema básico de entrada/saída (BIOS) e SafeBIOS. Como elas podem ajudar em um ataque de Dia zero?

- [x] Protegem contra ataques de dumping de credenciais que roubam tokens de interface de programação de aplicativos (API)
- [x] Impedem que um invasor com acesso físico ignore a segurança do sistema operacional (SO) para instalar malware que rouba tokens de autenticação
- [x] Garantem que invasores não consigam manipular as configurações do BIOS para enfraquecer a segurança do sistema operacional, o que pode levar ao sequestro de sessão de APIs
- [x] Todas as alternativas acima

Essa abordagem em camadas oferece proteção abrangente contra ataques de Dia zero direcionados ao BIOS, firmware, credenciais e configurações do sistema. Ao impedir a manipulação, acesso não autorizado e roubo de credenciais, essas tecnologias permanecem eficazes mesmo quando novas vulnerabilidades são descobertas por invasores.

Próxima pergunta →

Tipo de ataque: Dia zero

1 2 3 4: Melhores práticas em geral

Qual é a melhor maneira de tentar evitar que ataques de Dia zero aconteçam?

- [ ] Não usar software de código aberto
- [ ] Aproveitar os princípios de Zero Trust
- [ ] Manter tudo atualizado, incluindo sistemas operacionais (SO), firmware, interfaces de programação de aplicativos (APIs), bibliotecas e contêineres
- [ ] Instalar um portão eletrificado ao redor da empresa para impedir a entrada de agentes de ameaça

Veja a resposta correta →

Tipo de ataque: Dia zero

1 2 3 4: Melhores práticas em geral

Qual é a melhor maneira de tentar evitar que ataques de Dia zero aconteçam?

- ✗ Não usar software de código aberto
- ✓ Aproveitar os princípios de Zero Trust
- ✗ Manter tudo atualizado, incluindo sistemas operacionais (SO), firmware, interfaces de programação de aplicativos (APIs), bibliotecas e contêineres
- ✗ Instalar um portão eletrificado ao redor da empresa para impedir a entrada de agentes de ameaça

Se existirem vulnerabilidades desconhecidas ou sistemas não corrigidos, os princípios de Zero Trust evitarão ataques de Dia zero removendo a confiança implícita de usuários e dispositivos, impondo autenticação contínua, restringindo o acesso apenas às informações necessárias e controlando a movimentação de adversários para reduzir significativamente o risco organizacional de ameaças não detectadas.

Veja as soluções →

DELL Technologies

eBook interativo sobre cenários de segurança cibernética

TIPO DE ATAQUE: DIA ZERO

Recapitulação

Um ataque de Dia zero envolve a exploração de uma vulnerabilidade de segurança não divulgada em software ou hardware antes que um patch ou uma correção esteja disponível. Os invasores aproveitam a janela de oportunidade, muitas vezes causando uma interrupção generalizada antes que a vulnerabilidade seja descoberta e abordada.

A Dell lida com ataques de Dia zero usando controles de Zero Trust, segmentação de rede, contenção rápida e treinamento do usuário para fortalecer ainda mais as defesas contra ameaças emergentes.

Saiba mais sobre estratégias avançadas de resiliência cibernética e como a Dell pode ajudar você a proteger sua organização contra ataques de Dia zero.

Explore o resumo de ataques de Dia zero →

Voltar para Cenários

Espaço de trabalho confiável e infraestrutura confiável >

Defender endpoints e infraestrutura. Com as proteções SafeBIOS, SafeID e SafeData e as estruturas Zero Trust, como autenticação baseada em vários fatores (MFA) e controle de acesso baseado em função (RBAC), a Dell oferece defesas em camadas para limitar caminhos de exploração e garantir a autenticação de hardware.

Servidores PowerEdge >

A inicialização segura, a raiz de confiança de chip e a segmentação de rede no SmartFabric restringem o movimento lateral, garantindo que apenas o código confiável seja executado em sua infraestrutura.

Parceiros de segurança >

Inteligência avançada contra ameaças, managed detection and response (MDR), Detecção e resposta estendidas (XDR) e controles de acesso detalhados ajudam a detectar, rastrear e conter ataques de Dia zero antes que eles se espalhem.

Portfólio do PowerProtect >

Os backups imutáveis, os cofres isolados de recuperação cibernética e a lógica analítica do CyberSense orientada por IA garantem restauração rápida e resiliência após violações de Dia zero.

Serviços de segurança e resiliência >

Do gerenciamento de patches à resposta a incidentes, os especialistas da Dell oferecem contenção rápida, investigação forense e planejamento de resiliência para combater ameaças de Dia zero.


DELL Technologies