DELL Technologies

Melhore sua segurança cibernética e maturidade Zero Trust.

Feche as lacunas nos recursos e no conhecimento para fortalecer suas defesas contra ataques cibernéticos.

OPERAÇÕES

INFRAESTRUTURA E DISPOSITIVOS

NUVEM

APLICATIVOS

DE DADOS

As ameaças de hoje em rápida evolução, especialmente com o surgimento da IA generativa, criam desafios novos e inesperados até mesmo para os especialistas em segurança cibernética mais experientes.

Saiba como a parceria com profissionais de segurança experientes pode ajudá-lo a evitar ataques cibernéticos e manter práticas robustas de segurança.

As ameaças cibernéticas são como formigas em um piquenique

Você resolve o problema. Em seguida, aparece outro logo atrás.

Em um mundo cada vez mais interconectado, em que as organizações dependem muito de infraestruturas digitais e os dados se tornaram uma mercadoria de longo alcance, é melhor supor que um invasor sofisticado já tenha violado seu ambiente de TI.

A boa notícia é que existem parceiros experientes especializados na interseção entre tecnologia e segurança cibernética.

A Dell Technologies oferece soluções inovadoras e conhecimento especializado valioso que podem não estar disponíveis internamente para ajudar você a navegar pelo cenário de ameaças em constante evolução.

- Segurança de hardware e software
- Percepções sobre os riscos emergentes
- Noções básicas sobre técnicas avançadas de ataque
- AIOps para atender a ameaças em rápida mudança
- Novas estratégias de segurança e práticas recomendadas

Crie camadas de defesa que fazem evoluir continuamente as práticas de segurança e adotam uma abordagem Zero Trust.

A Dell Technologies é um parceiro de segurança cibernética que oferece serviços profissionais abrangentes, soluções de hardware e software e uma sólida rede de parceiros que limita a oportunidade de ataque, identifica e minimiza vulnerabilidades e ajuda você a restaurar rapidamente as operações de negócios.

Reduza a superfície de ataque →

Detectar e responder a ameaças cibernéticas →

Recuperação rápida de um ataque →

Borda **Núcleo** **Multicloud**

Serviços profissionais

Rede de parceiros de negócios/tecnologia **Cadeia de suprimentos segura**

DELL Technologies

Reduza a superfície de ataque

Crie suas defesas e torne-se um alvo menor, reduzindo as vias que os criminosos cibernéticos adoram explorar.

Para fortalecer sua postura de segurança, você precisa identificar e minimizar vulnerabilidades e pontos iniciais que podem comprometer aplicativos, sistemas ou redes em vários domínios, inclusive borda, núcleo e nuvem.

IDENTIFIQUE pontos de vulnerabilidade

- Vulnerabilidades de software
- Configurações incorretas
- Mecanismos de autenticação fracos
- Sistemas não corrigidos
- Privilégios excessivos de usuário
- Portas de rede abertas
- Baixa segurança física

IMPLEMENTE medidas preventivas

- Trabalhe com fornecedores seguros
- Aplique segmentação de rede abrangente
- Isole dados essenciais
- Imponha controles de acesso rigorosos
- Atualize e aplique patches em sistemas e aplicativos
- Identifique e trate vulnerabilidades usando a IA, avaliações regulares e testes

Adotar uma abordagem Zero Trust

Uma arquitetura Zero Trust significa que sua organização não confia automaticamente em nada dentro ou fora de seus perímetros. Em vez disso, tudo o que está tentando se conectar a seus sistemas é verificado antes de conceder acesso.
É um modelo estabelecido e prescrito pelo Departamento de Defesa dos EUA que incorpora **sete pilares inter-relacionados** que criam maturidade sistematicamente.

1. Confiança dos usuários
2. Confiança dos dispositivos
3. Confiança dos dados
4. Aplicativo e carga de trabalho
5. Rede e ambiente
6. Visibilidade e lógica analítica
7. Automação e orquestração

DELL Technologies

Reduza a superfície de ataque

Identifique os pontos fracos que prejudicam seus sistemas antes que os problemas aumentem.

A segurança cibernética não é uma tarefa única, mas um processo contínuo. Auditorias regulares, testes de penetração e avaliações de vulnerabilidade, com a ajuda de um parceiro experiente em serviços de segurança, podem ajudar a identificar e preencher as lacunas para reduzir os riscos.

Práticas seguras na cadeia de suprimentos	A segurança começa antes do que você imagina. Estabeleça uma base confiável usando dispositivos e infraestrutura projetados, fabricados e entregues usando uma cadeia de suprimentos segura, um ciclo de vida de desenvolvimento seguro e uma modelagem rigorosa de ameaças.
Segurança integrada	Trabalhe com dispositivos e infraestrutura com segurança integrada e baseada em hardware, projetada para detectar e evitar ataques antes que eles causem danos.
Patches regulares e atualizações	Solucione vulnerabilidades conhecidas e minimize o risco de exploração mantendo os aplicativos, o firmware e os sistemas operacionais atualizados com os patches de segurança mais recentes.
Menor privilégio	Limite as contas de usuário e sistema para ter os direitos de acesso mínimos necessários para executar suas tarefas. Essa abordagem restringe o possível impacto de um invasor obter acesso não autorizado.
Segmentação de rede	Isole os ativos essenciais para limitar o acesso à rede usando a segmentação de rede moderna para grupos essenciais de dados e de negócios e aplicativos. Isso contém um ataque impedindo o movimento lateral.
Segurança de aplicativos	Implemente práticas seguras de codificação, realize testes de segurança regulares e análises de código, e use firewalls de aplicativos da Web (WAFs) para ajudar a proteger contra ataques comuns no nível do aplicativo e reduzir a superfície de ataque de aplicativos da Web.
Serviços profissionais e parcerias	Colabore com provedores de serviços de segurança cibernética e faça parcerias com parceiros de negócios e tecnologia para trazer conhecimento especializado e soluções que podem não estar disponíveis internamente.
Conscientização e educação de usuários	Treine funcionários e usuários para reconhecer e relatar possíveis ameaças à segurança, tentativas de phishing e táticas de engenharia social para minimizar os riscos que exploram as vulnerabilidades humanas.

DELL Technologies

Detectar e responder a ameaças cibernéticas

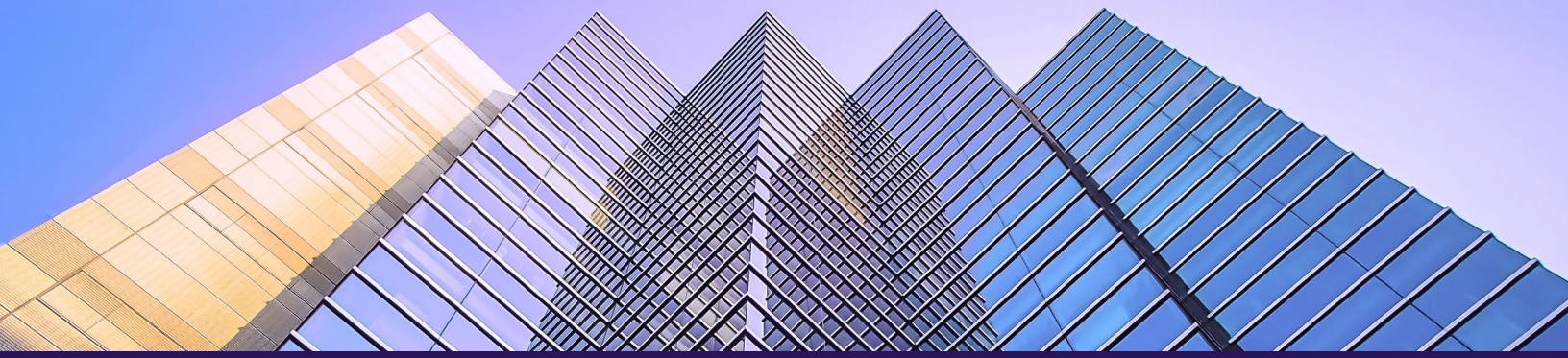
As práticas antigas de segurança são como internet discada, muito lentas e ineficazes no ambiente exigente de hoje.

Para combater ameaças cibernéticas sofisticadas, você precisa de melhores truques de segurança, como IA e ML integrados a aplicativos e metodologias que identifiquem e respondam ao que é conhecido e desconhecido.

Implemente sistemas potentes de detecção e prevenção de violação

Aproveite a IA e a ML para detecção de anomalias

Estabeleça monitoramento em tempo real do tráfego de rede e do comportamento do usuário



Aumente a resiliência ao fazer parcerias com serviços profissionais experientes para obter conhecimento especializado.

Como parceiro de tecnologia experiente, a Dell Technologies pode ajudá-lo a estabelecer protocolos proativos de resposta a incidentes e recuperação que descrevem funções e responsabilidades e garantem comunicação e coordenação perfeitas entre os componentes.

Melhore sua capacidade de detectar e responder proativamente a ameaças cibernéticas usando os seguintes itens avançados:

- Threat intelligence
- Resposta a incidentes
- Gerenciamento de eventos e informações de segurança
- Proteções de endpoints
- Lógica analítica comportamental

Facilite uma recuperação eficiente e rápida e minimize a perda de dados com:

- Um plano de resposta a incidentes bem definido e colaboração
- Backups regulares de sistemas e dados essenciais
- Soluções seguras de armazenamento fora do local e criptografia de dados

DELL Technologies

Detectar e responder a ameaças cibernéticas

Mantenha-se atento e tome providências rapidamente.

Detectar e responder a ameaças cibernéticas significa permanecer alerta e se planejar para o pior cenário. Estabeleça um plano de resposta e recuperação que seja continuamente atualizado e rotineiramente praticado para que toda a organização saiba como reduzir os efeitos de um ataque. É um processo contínuo e iterativo que requer uma combinação de tecnologia, pessoal qualificado, processos bem definidos e colaboração em equipe.

Monitoramento contínuo	Ferramentas de segurança, como sistemas de detecção de violação (IDS), sistemas de prevenção contra violação (IPS), análise de registros e threat intelligence, ajudam a identificar sinais de acesso não autorizado, violações, infecções por malware e violações de dados.
Detecção de ameaças	Aproveite a IA e a ML para analisar dados a fim de identificar padrões, anomalias e indicadores de comprometimento (IoCs) que possam apontar para uma ameaça. Isso inclui reconhecer assinaturas de ataque conhecidas e identificar comportamentos de desvio.
Alertas e notificações	Dê avisos antecipados para solicitar investigação e resposta. Alertas de bolhas e notificações na superfície para uma ação rápida com segurança integrada. Feed de telemetria no nível do dispositivo acima do sistema operacional para ajudar a acelerar a detecção de ameaças e liberar a equipe de segurança ou um Centro de operações de segurança (SOC) quando possíveis ameaças ou incidentes forem detectados.
Resposta a incidentes	Inicie um plano de resposta para investigar e reduzir incidentes de segurança confirmados. Isso envolve conter o impacto, identificar a causa raiz e implementar as ações necessárias para restaurar sistemas e evitar mais danos.
Análise jurídica	Faça uma análise detalhada dos incidentes para entender a metodologia de ataque, determinar a extensão da violação, identificar os sistemas ou dados afetados e coletar evidências para localizar e resolver os pontos fracos de segurança.
Correção e recuperação	Tome medidas para corrigir vulnerabilidades, corrigir sistemas de patches, remover malware e implementar medidas de segurança aprimoradas para evitar incidentes semelhantes. Restaure os sistemas e dados afetados para seu estado normal para concluir o processo de recuperação.

DELL Technologies

Recuperação de ataques cibernéticos

Pressione o pedal no metal e coloque seus negócios de volta na faixa rápida.

A resiliência cibernética é necessária no mundo orientado por dados de hoje e é esperada por clientes e parceiros. Para ser bem-sucedido, é necessário haver várias camadas de proteção para garantir que os dados essenciais sejam protegidos e isolados para que possam ser recuperados rapidamente com confiança após um ataque. Avalie sua resiliência cibernética ›

Tome medidas para reduzir os danos causados por um ataque cibernético

Recrie serviços e dispositivos comprometidos ou interrompidos

Analise o incidente para evitar ataques futuros

Cumpra aos SLAs de negócios e retorne as operações ao normal

Crie uma estratégia abrangente de segurança cibernética para que a organização possa se recuperar com eficiência e eficácia.

A recuperação de um ataque cibernético exige um esforço coordenado envolvendo equipes de TI, profissionais de segurança cibernética, gerenciamento e, às vezes, especialistas externos. O segredo para a recuperação é fazer com que os sistemas e as operações voltem ao normal rapidamente e, ao mesmo tempo, aprender com o incidente a fim de reduzir a interrupção e o tempo de inatividade, restaurar serviços e integridade dos dados, minimizar os impactos financeiros e de reputação e fortalecer a segurança cibernética para evitar ataques semelhantes no futuro.

- Avaliar o impacto de um ataque nas operações de negócios
- Priorizar serviços essenciais
- Implementar sistemas de proteção de dados
- Comunicar qualquer incidente e progresso de recuperação
- Desenvolver um plano e praticar, praticar e praticar para garantir a continuidade

DELL Technologies

Recuperação de ataques cibernéticos

Volte para o chão de fábrica restabelecendo sistemas, redes e dados após um incidente.

Alcançar uma estratégia de resiliência cibernética incorpora pessoas, processos e tecnologia em uma estrutura holística que protege toda a organização.

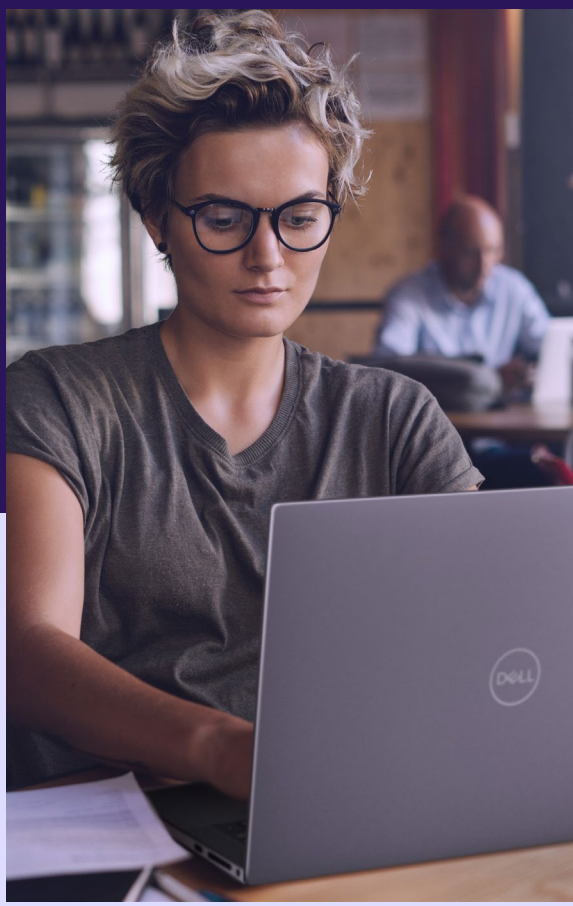
Contenção de incidentes	A primeira etapa é isolar e conter o impacto do ataque cibernético. Isso envolve desconectar os sistemas afetados da rede, desativar contas comprometidas e implementar medidas para evitar mais disseminação ou danos.
Restauração do sistema ou do dispositivo	Depois que um incidente é contido, os sistemas e redes afetados são restaurados para um estado limpo e seguro. Isso pode envolver a recriação de sistemas comprometidos, a reinstalação do software e a aplicação de atualizações e patches de segurança. A automação e a autocorreção podem desempenhar um papel importante na recuperação operacional.
Recuperação de dados	Os dados que podem ter sido comprometidos, criptografados ou excluídos durante o ataque devem ser recuperados. Isso pode envolver a restauração de dados de backups ou a utilização de técnicas especializadas de recuperação de dados para recuperar arquivos perdidos ou criptografados.
Análise jurídica	Após um ataque, é crucial entender como a violação aconteceu, quais vulnerabilidades foram exploradas e as etapas para evitar ataques semelhantes. Sistemas como o Security Information and Event Management (SIEM) e recursos como comparações de BIOS fora do host oferecem percepções úteis.
Avaliação de respostas a incidentes	Após a recuperação, é essencial avaliar o processo de resposta a incidentes e identificar áreas de melhoria. As lições aprendidas com o ataque podem ser usadas para aprimorar as práticas de segurança, atualizar os planos de resposta a incidentes e oferecer melhor proteção contra incidentes futuros.
Serviços profissionais e parcerias	Os provedores de serviços de segurança cibernética e os parceiros de tecnologia trazem recursos e conhecimentos especializados valiosos para ajudar sua organização a se recuperar. Eles podem ajudar com tarefas como análise jurídica, identificação da ocorrência da violação e recomendação de medidas para evitar incidentes futuros.

DELL Technologies

Amplie a segurança cibernética para a borda e ambientes de nuvem

À medida que as redes se espalham do núcleo para a borda e para a nuvem, os ambientes se tornam um ponto crucial de vulnerabilidade.

À medida que você avança em sua estratégia de segurança cibernética, sua organização deve estender os princípios do Zero Trust para a borda e a nuvem para garantir controles de acesso rigorosos, autenticação contínua e visibilidade e controle abrangentes sobre o tráfego de rede. À medida que os ambientes de ameaças evoluem, é aconselhável implementar recursos de IA como uma primeira linha de defesa. Além disso, uma estratégia só será concluída se a rede principal e os ambientes de nuvem tiverem medidas de segurança, como segmentação de rede, criptografia e monitoramento contínuo.



Serviços profissionais de segurança cibernética podem ajudá-lo a adotar uma abordagem holística.

Conectar várias soluções de segurança pode ser um desafio. Colaborando com serviços profissionais especializados em borda, a segurança no núcleo e na nuvem oferece conhecimento especializado para colocar em prática medidas eficazes que protegem sua organização de todos os ângulos.

Borda

Estabeleça várias camadas de segurança na borda, na rede e no hardware e software.

Núcleo

Alinhe sua infraestrutura a uma abordagem Zero Trust usando IA, ML e automação.

Multicloud

Proteja qualquer carga de trabalho em qualquer ambiente, inclusive nuvem pública, contêineres e cargas de trabalho nativas da nuvem.

DELL Technologies

IA generativa: um desafio de ponta dupla para a segurança cibernética

A última geração de IA está nos levando rapidamente em direção a novos riscos, mas também a uma segurança avançada.

Como a próxima fase da IA, a IA generativa abrange sistemas que podem entender, aprender, adaptar e implementar o conhecimento em uma variedade de tarefas.

Por um lado, promete detecção e resposta a ameaças aprimoradas, recursos preditivos e eficiência operacional. Por outro lado, apresenta novos desafios que exigem estratégias de segurança cibernética em evolução que abordam os riscos por meio de medidas de segurança robustas, monitoramento contínuo, atualizações e patches regulares e uma abordagem em constante evolução para a ética e a privacidade dos dados.

Proteger organizações com a IA generativa

A IA generativa tornou-se um parceiro crucial na segurança cibernética, abrindo novas vias para proteger as organizações.

- Melhore a eficácia da detecção e resposta a ameaças.
- Preveja ameaças futuras ou identificar possíveis vulnerabilidades.
- Automatize a detecção de ameaças e ofereça eficiência.
- Análise jurídica para identificar rapidamente padrões, anomalias e indicadores de comprometimento.
- Treinamento em conscientização de segurança personalizada.
- Dimensione as operações de segurança com acesso mais rápido a percepções mais avançadas.

Proteger sistemas de IA generativa

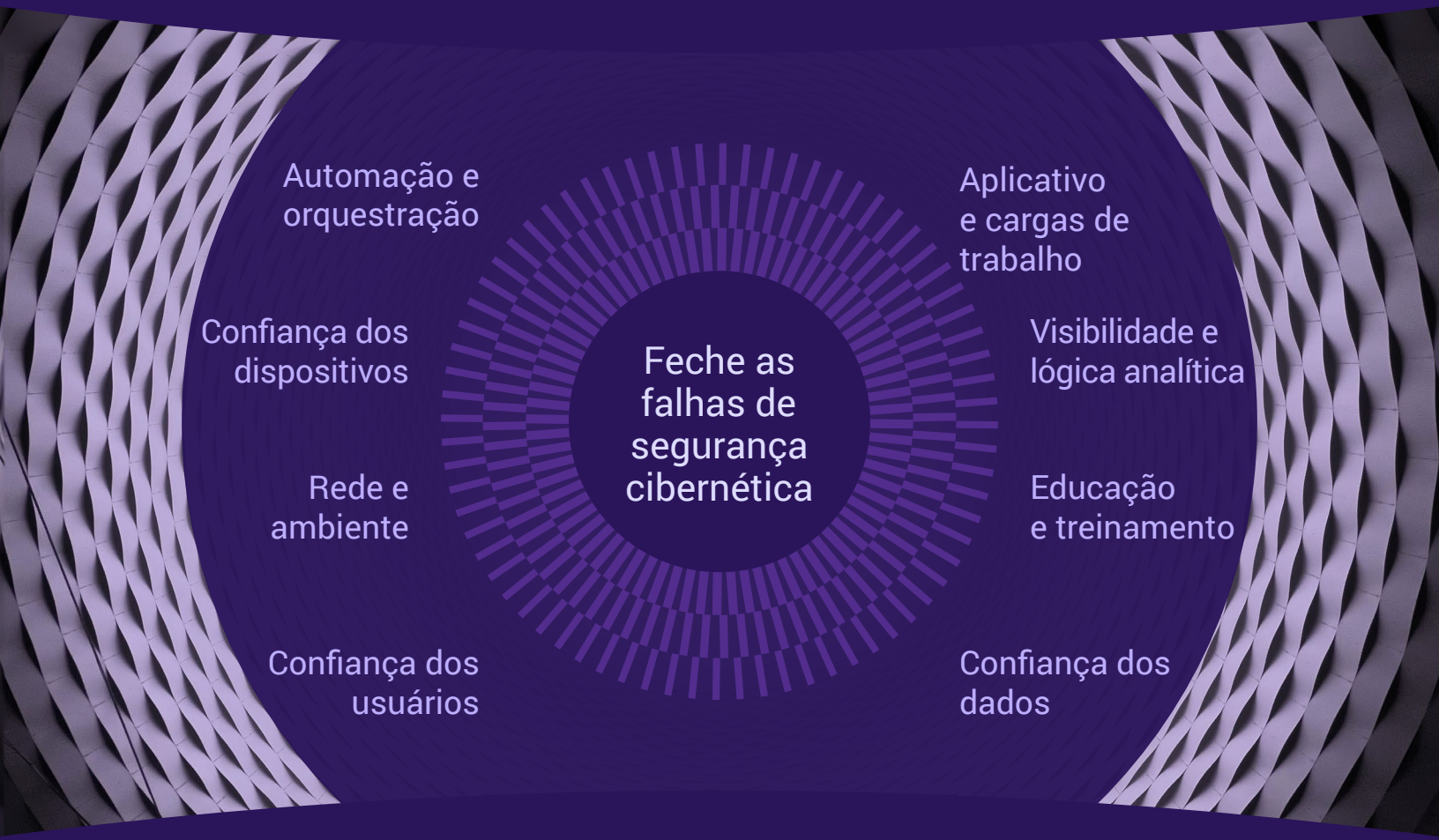
Embora a IA generativa ofereça benefícios substanciais de segurança, sua funcionalidade pode ser usada de modo mal-intencionado se não for adequadamente protegida.

- Garanta a integridade e a privacidade dos dados.
- Reduza os ataques adversários projetados para enganar os sistemas de IA que causam mau funcionamento.
- Detecte e responda ao uso indevido do sistema de IA mal-intencionada.
- Auditoria e redução de problemas e preconceitos éticos.
- Implementação de controles de acesso sólidos para sistemas de IA.
- Proteja e recupere com segurança modelos de idiomas grandes (LLM).

DELL Technologies

A segurança cibernética moderna deve ser inteligente, escalável e automatizada

A Dell Technologies pode ajudá-lo a estabelecer uma segurança abrangente que proteja contra ameaças cibernéticas em evolução. À medida que a tecnologia avança, nossa abordagem à segurança cibernética permanece um passo à frente, aproveitando a capacidade da IA e da ML para proteger suas infraestruturas digitais e manter a confiança no realm digital. Não importa onde você esteja em sua jornada de segurança cibernética, trabalharemos com você para ir além de simplesmente proteger sua organização com etapas que o mantêm ágil e resiliente.



DELL Technologies

Dell.com/SecuritySolutions

Solicitar um retorno

Falar com um consultor de segurança

Ligue para 1-800-433-2393