**Casos de uso de IA**

Introdução

À medida que a IA avança, seu potencial para transformar a maneira como você trabalha, vive e interage com a tecnologia se expande rapidamente. Compreender esses casos de uso é essencial para identificar onde a IA pode ser aplicada com mais eficácia, seja na automação de tarefas rotineiras, na melhoria da tomada de decisões, na personalização da experiência do usuário ou no fomento à inovação.

Este treinamento foi desenvolvido para demonstrar aplicações reais de IA, desde otimização e automação de redes até segurança cibernética e IoT. Você obterá insights valiosos sobre como a análise orientada por IA pode prever falhas de rede, otimizar o tráfego e aprimorar as medidas de segurança. Ao compreender esses casos de uso, você estará equipado com o conhecimento necessário para implementar soluções de IA que melhoram a eficiência, a confiabilidade e o desempenho em seus próprios ambientes de rede. Prepare-se para descobrir como a IA pode revolucionar a maneira como você gerencia e protege sua infraestrutura digital.

Análise

Analytics é a análise computacional sistemática de dados ou estatísticas. É usada para tornar os dados significativos e fáceis de entender. Analytics orientada por IA é uma análise alimentada por IA para atingir os mesmos objetivos da análise, mas sem programação explícita. Além disso, a análise orientada por IA pode encontrar padrões ou tendências em dados que os desenvolvedores não teriam conseguido codificar explicitamente porque não sabiam o que estavam procurando.

Os insights analíticos obtidos por meio da IA ​​podem ser usados ​​de diversas maneiras: monitoramento ativo, avaliação ou tomada de ações preditivas. Modelos que realizam ações preditivas identificam padrões em dados em tempo real que ocorreram antes de uma falha anterior, indicando que uma falha semelhante pode estar próxima.

Análise preditiva

A análise preditiva é uma forma avançada de análise de dados que utiliza ML e IA para analisar dados de rede em tempo real, comparar esses dados com dados históricos, relatar os padrões identificados e recomendar ações. Dessa forma, os administradores de rede podem manter o desempenho e a confiabilidade ideais da rede por meio de um gerenciamento proativo e inteligente.

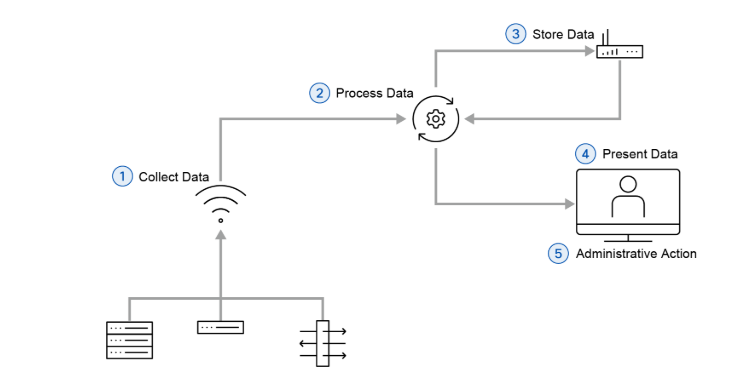
A análise preditiva começa com uma linha de base baseada nos dados coletados durante a operação normal. Essas linhas de base aprendem e se adaptam à medida que os ambientes de rede mudam e o número de dispositivos, usuários e aplicativos evolui. Após definir "normal", você pode comparar os dados de operação em tempo real com essa linha de base para verificar se algo inesperado ou anormal está ocorrendo em sua rede. Com essa abordagem simplificada para analisar dados de rede, você também pode realizar análises de causa raiz orientadas por IA em problemas complexos em sua rede e identificar os mais críticos. Os administradores podem usar esse conjunto de informações, assistência para depuração e sugestões de correção para organizar o trabalho necessário para manter uma rede operando dentro dos parâmetros definidos.

Realizar manutenção com base em insights de IA antes que uma falha ocorra é chamado de manutenção preditiva. Por exemplo, monitorando dados de sensores ou a temperatura interna de um aparelho, um modelo de IA pode detectar um componente degradado antes que ele falhe e recomendar seu reparo ou substituição. Resolver problemas antes que eles atinjam um status crítico sempre produz um resultado melhor, geralmente evitando tempo de inatividade e provavelmente prolongando a vida útil do hardware.

A capacidade de analisar grandes volumes de dados e tomar decisões inteligentes economiza tempo e dinheiro para as empresas. Com a implementação adequada de análises preditivas baseadas em IA, as organizações podem obter um retorno real de valor em termos de:

* Tempo de inatividade da rede reduzido
* Melhor eficiência de custos
* Maior transparência sobre como uma rede está operando
* Melhores insights sobre estatísticas de uso

Processo de análise orientado por IA



Em termos práticos, a implementação de análises orientadas por IA envolve várias etapas importantes. Primeiro, os dados devem ser coletados de vários dispositivos e sensores de rede. Esses dados incluem métricas de desempenho, padrões de uso e condições ambientais. Dados que ainda não foram propostos ou dados recebidos em tempo real devem ser transformados em um formato mais significativo que se alinhe a um determinado caso de uso. A limpeza de dados garante consistência e precisão em um conjunto de dados. Modelos de IA treinados em dados defeituosos derivarão padrões falhos e farão inferências incorretas. Se você treinar um modelo em um conjunto de dados contendo inúmeras falhas e defeitos rotulados como operações normais, o modelo não será capaz de distinguir os padrões que indicam essas falhas dos dados normais.

A segregação de dados, que é o processo de classificar dados em várias categorias com base em atributos ou critérios específicos, é outra consideração importante. A segregação de dados pode ajudar a monitorar os dados e reduzir a sobrecarga envolvida no uso desses dados de forma significativa no futuro. O oposto da segregação é a agregação, um processo no qual dados de várias fontes são combinados em uma única coleção. Um conjunto de dados agregados pode ser usado como conjunto de dados de treinamento para modelos de ML que coletam insights mais profundos sobre o sistema do que seriam facilmente aparentes a partir de um único ponto de dados ou fonte. Os modelos de ML reconhecem padrões nos dados e começam a desenvolver uma linha de base que inclui o seguinte:

* Como os dados aparecem em operação regular
* Como os dados aparecem antes, durante e depois de uma falha
* Como os dados aparecem durante o treinamento dos dados

Após o processamento, os dados são normalmente armazenados e devem ser usados ​​para continuar aprimorando o conjunto de dados de treinamento para versões futuras do modelo de ML. É raro que um sistema permaneça o mesmo. Previsivelmente, novos recursos levarão a mais usuários ou uso, mais solicitações, mais ciclos de CPU e à necessidade de escalabilidade. Os modelos de ML avaliam os dados recebidos em tempo real para detectar padrões que possam indicar que ações devem ser tomadas. Uma vez identificados os padrões, esses sistemas podem apresentar as informações aos administradores de rede por meio de um painel de visualização de dados ou outros meios.

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

**Otimização de rede**

No cenário tecnológico atual, o escopo e a complexidade das redes estão em constante mudança e crescimento. As redes modernas frequentemente incluem softwares de otimização e análise de rotas, como Cisco Secure Network Analytics, AppDynamics e ThousandEyes, para citar alguns. Essas tecnologias ajudam a melhorar a forma como uma rede lida com o tráfego. O roteamento dinâmico simplifica drasticamente o processo de cálculo de rotas complexas. Essa abordagem leva em conta fatores como tráfego de rede atual, capacidade, disponibilidade e outras considerações importantes. A integração da IA ​​à equação auxilia ainda mais na otimização da largura de banda e na melhoria da experiência do usuário final. Neste tópico, você verá como a IA pode ajudar a otimizar o tráfego de rede e evitar congestionamentos, contenção de recursos e interrupções de serviço. Você também explorará como a Meraki, uma plataforma de gerenciamento de rede baseada em nuvem da Cisco, usa IA para gerenciar operações de rede.

Diagrama

O conteúdo gerado por IA pode estar incorreto.

Suponha que um segmento de rede esteja congestionado devido a cargas de tráfego intensas. Usando IA, o tráfego pode ser direcionado por outros caminhos para evitar congestionamentos, garantindo a prevenção de gargalos e a manutenção constante do alto desempenho. A IA pode garantir o provisionamento ininterrupto de serviços para aplicações essenciais em diferentes capacidades de rede, utilizando informações em tempo real e algoritmos sofisticados que priorizam funções críticas.

A IA ajuda a evitar a contenção de recursos e mantém os componentes em condições ideais de funcionamento por meio do monitoramento contínuo da rede e do ajuste das alocações de recursos conforme a necessidade. Esse tipo de previsão orienta investimentos estratégicos em infraestrutura para dar suporte ao crescimento futuro previsto sem afetar os níveis de desempenho atuais.

O que diferencia a IA das soluções tradicionais de gerenciamento de tráfego é sua capacidade de analisar com mais profundidade os dados históricos da rede coletados em diferentes regiões, redes e casos de uso. Essa capacidade permite que uma solução baseada em IA otimize rotas não apenas com base na situação atual, mas também para ocorrências futuras, como feriados, lançamentos de produtos e outros eventos. Quando aliada a soluções de gerenciamento de rede, essa combinação tem o potencial de identificar tendências passadas, prever picos de tráfego, implementar novos dispositivos definidos por software e rotear o tráfego adequadamente. O resultado é a ausência de degradação ou interrupção do serviço e uma experiência otimizada para os usuários finais.

Algumas plataformas modernas de rede de provedores fornecem hardware que custa por hora de uso. Usar a IA para determinar o que as próximas oito horas de tráfego de rede provavelmente implicarão permite ações manuais ou automatizadas que podem liberar esse hardware e encerrar sua obrigação financeira. Alternativamente, se uma organização possui o hardware, ela ainda pode economizar dinheiro e incentivar a inovação, liberando recursos de computação que podem ser usados ​​de alguma outra forma significativa, em vez de ficarem inativos.

**Gerenciamento de tráfego baseado em IA da Meraki**

A plataforma Cisco Meraki, líder em Wi-Fi, roteamento e segurança controlados pela nuvem, conta com gerenciamento baseado em nuvem e telemetria aprimorada. Esse design permite coletar e processar grandes volumes de informações de dispositivos conectados em diversos locais. Os dados são transmitidos para os servidores em nuvem da Meraki, onde modelos de aprendizado de máquina realizam análises em tempo real. Esses algoritmos detectam desvios e padrões que informam o status atual da rede e preveem tendências futuras.

Diagrama

O conteúdo gerado por IA pode estar incorreto.

O Auto RF com tecnologia de IA da Meraki utiliza o Gerenciamento de Recursos de Rádio (RRM) aprimorado por IA para otimizar os parâmetros de rádio e proporcionar conectividade sem fio confiável e de alto desempenho. Esse recurso aprimora a experiência ao personalizar a rede e compreender suas tendências, especialmente em um ambiente corporativo.

Os principais recursos do Auto RF incluem:

* Planejamento de canais de IA, que evita canais mais suscetíveis à interferência.
* Horário de pico, o que evita ajustes desnecessários em horários de pico.

Com essas inovações, a Meraki pode oferecer redes sem fio eficientes e integradas, adequadas e adaptadas aos requisitos e circunstâncias específicos dessas redes. A Meraki também conta com um recurso de análise de causa raiz, alimentado por IA, que permite a solução avançada de problemas e a depuração de problemas de rede. O painel da Meraki coleta e analisa continuamente dados de telemetria de vários dispositivos de rede, utilizando algoritmos de IA para detectar anomalias e degradação do desempenho. Quando um problema é detectado, o Machine Reasoning Engine realiza uma análise de causa raiz para identificar a causa subjacente do problema.

Interface gráfica do usuário, Aplicativo, Word

O conteúdo gerado por IA pode estar incorreto.

Como mostrado na figura, o painel da Meraki identificou um problema com o provedor de internet em uma filial local. A análise de causa raiz, com tecnologia de IA, constata que o backhaul de VPN é a causa, com confiança média. As "evidências" produzidas revelam que sete clientes são afetados pelo tráfego enviado por VPNs. Essas informações permitem que os gerentes de rede localizem com precisão onde os problemas de rede estão ocorrendo e fornecem insights sobre possíveis soluções que podem ser adotadas.

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

Automação de Redes e Redes de Auto-Reparação

Automação de rede é um termo amplo que abrange qualquer atividade automatizada que interaja com os dispositivos que compõem uma rede. A automação de rede normalmente envolve o uso de sistemas para configurar dispositivos, gerenciar políticas e solucionar problemas que tradicionalmente são tratados por administradores humanos.

Os principais benefícios da automação de rede orientada por IA incluem:

* Tomada de decisão mais bem informada
* Tempos de resposta mais rápidos
* Melhor desempenho de rede
* Menos tempo de inatividade
* E taxas de erro mais baixas

Aplicativos como o Cisco Catalyst Center (antigo Cisco DNA Center ou DNAC) usam IA para gerenciar e otimizar o desempenho da rede proativamente por meio da análise de dados. O Catalyst Center é um sistema de gerenciamento poderoso que usa IA para conectar, proteger e automatizar as operações de rede.

Diagrama

O conteúdo gerado por IA pode estar incorreto.

O Cisco AI Network Analytics é uma ferramenta do Catalyst Center que aplica o poder do ML e do raciocínio de máquina para fornecer insights precisos sobre uma implantação de rede específica, permitindo a solução rápida de problemas. Os dados da rede são enviados para a nuvem do Cisco AI Network Analytics no Catalyst Center. A nuvem do Cisco AI Network Analytics usa modelos de ML para fazer inferências sobre os dados e relata esses insights ao Catalyst Center.

Diagrama

O conteúdo gerado por IA pode estar incorreto.

Ao incorporar a IA ao processo de automação, administradores e engenheiros aproveitam o poder do aprendizado de máquina e da análise de dados para executar tarefas administrativas que permitem que uma rede se comporte de forma mais autônoma e eficiente. Ao coletar, processar e armazenar novos dados continuamente, os modelos de IA que auxiliam na automação de tarefas de rede podem ser retreinados, alterando as inferências que fazem com base nas necessidades e no uso da rede. No entanto, essa adaptação contínua traz seus próprios desafios.

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

Redes auto-reparáveis ​​são uma aplicação avançada de automação de redes impulsionada por IA. Seu objetivo é automatizar o processo de identificação de problemas em uma rede, determinar o curso de ação correto e executar as ações apropriadas para remediar ou conter o problema. Atualmente, a tecnologia de IA não atingiu um ponto em que um sistema possa ser usado para lidar com todas essas tarefas com absoluta certeza. No momento, administradores e engenheiros de rede ainda precisam monitorar ou aprovar as ações tomadas ou recomendadas pelos sistemas de IA.

Embora não se possa confiar plenamente na IA, a automação de redes orientada por IA ainda é uma ferramenta poderosa e útil para auxiliar no monitoramento, gerenciamento e manutenção de redes. Os sistemas disponíveis atualmente são recentes, mas os dados produzidos por dispositivos de rede em todo o mundo alimentam constantemente o conjunto de informações. Esse processo será usado para continuar aprimorando a tecnologia de IA, tornando suas redes mais confiáveis, resilientes, disponíveis e seguras.

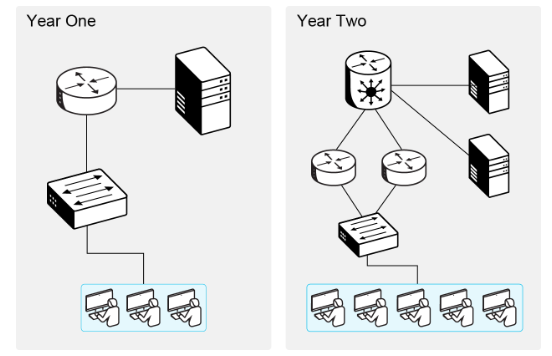
Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

**Planejamento e Previsão de Capacidade**

O planejamento de capacidade é o processo de determinar os recursos necessários para atender às demandas atuais e futuras da rede. Para planejar o futuro, muitas vezes é necessário observar tendências históricas, como o aumento do uso da rede em uma determinada época do ano ou uma maior probabilidade de falha dentro de um período específico de implantação.

No entanto, ao contrário da manutenção preditiva ou da automação de rede, o planejamento e a previsão de capacidade consideram o que será exigido da rede no futuro devido a vários fatores, não apenas dados históricos. Se uma rede tiver dificuldades com tráfego durante um período, evento ou atividade programada específica, essas informações devem ser registradas e incorporadas aos dados de treinamento do modelo de IA. Como exatamente o resultado ficou aquém do esperado e por quê? Quando um conjunto semelhante de circunstâncias surgir no futuro, a IA pode usar esse conhecimento para fazer recomendações específicas sobre dimensionamento, roteamento e outras atividades de rede que ajudarão a rede a lidar com o aumento do tráfego. A IA oferece a capacidade de contabilizar mais do que apenas quantas solicitações foram feitas na primeira vez. A IA pode contabilizar eventos como quantas solicitações foram feitas em comparação com o tráfego diário, quantos usuários ativos existem e outras informações relevantes. Essa abordagem proativa para dimensionar os recursos de rede garante a utilização eficiente dos recursos e melhora o desempenho e a confiabilidade.



Como a maioria das outras aplicações que envolvem IA, o planejamento de capacidade orientado por IA começa com a coleta de dados de dispositivos e sistemas de rede. Esses dados podem incluir métricas como:

* Padrões de uso
* Volumes de tráfego
* Desempenho de hardware
* Condições ambientais

Algoritmos de aprendizado de máquina analisam esses dados para identificar tendências e correlações, permitindo que a IA preveja as demandas futuras da rede com precisão. Além das mudanças que podem ser necessárias para acomodar as tendências futuras esperadas, os insights gerados por modelos de IA desse tipo também podem prever a necessidade de pessoal de suporte adicional de plantão devido ao aumento da incerteza e do potencial de incidentes.

Uma parte essencial do planejamento de capacidade assistido por IA é o balanceamento dinâmico de carga. Nesse processo, um modelo de IA monitora o tráfego de rede e o consumo de recursos, adaptando a distribuição de recursos em tempo real para evitar congestionamentos e aprimorar o desempenho. Por exemplo, se uma área da rede receber repentinamente mais tráfego do que o normal, o modelo de IA pode transferir parte dessa carga para outras áreas menos movimentadas, de modo que nenhum ponto fique sobrecarregado por excesso de tráfego. O foco do balanceamento de carga assistido por IA muda para a distribuição do tráfego de rede ou das tarefas de computação para utilizar recursos adicionais ou diferentes dentro de uma rede ou data center.

Desenho de um cachorro

O conteúdo gerado por IA pode estar incorreto.

Os benefícios do planejamento e da previsão de capacidade orientados por IA incluem o seguinte:

* Os administradores de rede podem antecipar e planejar estrategicamente as atualizações de infraestrutura por meio de decisões de investimento informadas. Essa estratégia ajuda a garantir que o sistema gerencie o aumento de solicitações, mantendo o desempenho de ponta, evitando possíveis gargalos e garantindo uma experiência tranquila para o usuário, mesmo durante os horários de pico.
* Equipados com insights mais detalhados e previsões precisas, os administradores de rede podem executar manutenção e otimização proativas concentrando seu tempo e esforços em áreas de alto impacto.
* Por meio de insights e inferências baseados em IA, as organizações podem evitar o excesso de provisionamento, que leva ao desperdício de recursos, ou o subprovisionamento, que resulta em serviços de baixa qualidade, o que pode levar à insatisfação do usuário. O resultado ideal é um equilíbrio entre a alocação de hardware e a demanda real.
* Além de planejar eventos no futuro imediato, como a preparação para um feriado ou o atendimento a uma nova região, a IA pode ajudar as empresas a se prepararem para demandas futuras distantes. Um modelo de IA pode identificar padrões que indicam tendências de crescimento em um cronograma por meio de análises aprofundadas de estatísticas de uso e outras tendências. Por exemplo, o aumento esperado na demanda por recursos se baseia na identificação de que os usuários em uma região estão interagindo mais com seu produto.

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

**Cibersegurança**

A cibersegurança é outra área da tecnologia que está sendo influenciada pela IA. Ao utilizar algoritmos avançados e técnicas de Machine Learning (ML), a IA pode auxiliar as equipes de SecOps a detectar, responder e gerenciar ameaças e violações de segurança.

A IA está sendo usada atualmente em algumas áreas-chave da segurança cibernética, mas essa lista aumentará com o passar do tempo e a IA se tornar mais avançada. A IA está sendo usada para identificar ameaças como tentativas de ataques de força bruta, malware e tentativas de phishing. Além disso, a IA pode auxiliar na resposta a incidentes, permitindo a mitigação rápida e automatizada de ameaças e o gerenciamento preditivo de riscos, avaliando potenciais vulnerabilidades de segurança. Além disso, uma vez que uma linha de base para o seu sistema tenha sido estabelecida e você comece a monitorar vários componentes, você pode identificar padrões que indicam que um problema ocorrerá no futuro e tomar alguma ação para preveni-lo. Esse processo é chamado de gerenciamento preditivo de riscos. Produtos da Cisco, como Cisco Secure Network Analytics, Secure Endpoint Analytics e Cisco Secure Email Threat Defense, usam modelos de ML para identificar, prevenir e mitigar ameaças à segurança em várias superfícies de ataque.

Diagrama

O conteúdo gerado por IA pode estar incorreto.

Para treinar um modelo de ML para melhorar a postura de segurança de uma rede ou sistema, o treinamento provavelmente incluiria:

* Todas as vulnerabilidades de segurança documentadas
* Dados coletados em vários estágios de violações de segurança
* Estratégias de contenção
* Ações de remediação
* Quaisquer outros dados que possam ser coletados e que estejam diretamente relacionados à segurança cibernética.

Organizações como o NIST (Instituto Nacional de Padrões e Tecnologia) e a ISO (Organização Internacional para Padronização) trabalham para documentar incidentes conhecidos, vulnerabilidades e outras informações relacionadas. No entanto, mesmo com acesso a essas informações, ainda há uma grande lacuna a ser preenchida para implementar efetivamente uma solução de segurança cibernética baseada em IA que as organizações possam esperar ter um desempenho melhor do que uma equipe humana. Por esse motivo, pode ser uma ideia melhor optar por uma solução de ML/IA pronta para uso, como as disponíveis pela Cisco. Essas soluções se baseiam em modelos de ML treinados com base em uma riqueza de dados relacionados à rede.

A crescente complexidade das violações de segurança impulsiona a demanda por um conjunto de ferramentas mais sofisticado para prevenir ou mitigar ameaças e violações. Atualmente, hackers estão treinando ou desbloqueando modelos de IA e os utilizando de maneiras maliciosas, como obter acesso a recursos restritos e criptografar informações críticas para tornar o sistema inutilizável. Se a IA se tornar a nova ferramenta de hacking, a melhor chance de se defender contra ela seria usar IA mais sofisticada ou melhor treinada para proteção.

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

Gestão Preditiva de Riscos

Em segurança cibernética, risco é definido como o potencial de perda ou exposição de um sistema ou rede. Especificamente, risco é uma combinação da probabilidade de um ataque e do dano potencial que um ataque pode causar a uma organização. É importante distinguir risco de vulnerabilidade. Uma vulnerabilidade é uma fragilidade em um sistema que pode ser explorada. O risco é frequentemente o resultado de vulnerabilidades, configurações incorretas ou erro humano, que poderiam ser evitados com análise adequada e due diligence.

Diagrama

O conteúdo gerado por IA pode estar incorreto.

A gestão preditiva de riscos é o processo de avaliação de riscos em um sistema com base na operação normal. Esse processo requer a coleta de dados de vários fluxos de entrada para identificar riscos em um sistema ou rede antes que um incidente ocorra. A IA pode auxiliar nesse processo, comparando os dados do seu sistema com uma grande quantidade de dados relacionados nos quais o modelo de IA foi treinado. O relatório de informações deve então classificar os riscos por dano potencial, determinando a prioridade de abordagem dos riscos na ordem de importância apropriada.

Um método para identificar riscos é por meio da análise de código. Alguns exemplos de riscos em uma base de código incluem:

* Vulnerabilidades de segurança como injeção de SQL
* Script entre sites (XSS)
* Estouro de buffer
* Problemas de qualidade e manutenibilidade do código
* Problemas de desempenho, como vazamentos de memória
* Má adesão às melhores práticas
* Conformidade com os padrões de segurança

Ferramentas como o Snyk, da DeepCode AI, já estão sendo incorporadas a um pipeline de CI/CD, uma série de etapas automatizadas que as equipes de desenvolvimento de software usam para criar, testar e implantar aplicativos. Uma vez implementado, o Snyk utiliza IA e aprendizado de máquina para realizar análises de código estáticas e dinâmicas, reduzindo riscos entre aplicativos.

Outras ferramentas, como o Cisco Network Analytics, dentro do Cisco Catalyst Center, utilizam IA para realizar análises de vulnerabilidades de rede, um subconjunto da análise de rede. Essa análise avalia a rede como ela existe (incluindo as operações após incidentes de segurança já terem ocorrido) em relação a uma linha de base de operação normal e dados históricos. Ao comparar configurações, políticas de rede e comportamento de uma rede antes e depois da exploração de uma vulnerabilidade, essas ferramentas assistidas por IA podem ajudar a detectar problemas e vulnerabilidades futuras, analisar as causas raiz e executar ações corretivas rapidamente.

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

**Detecção de ameaças**

Em segurança cibernética, uma vulnerabilidade é uma fragilidade em uma rede ou sistema de computadores que pode ser explorada por um agente malicioso. Uma ameaça é um ato malicioso que explora uma vulnerabilidade, geralmente com a intenção de danificar ou roubar dados do sistema.

Vulnerabilidades podem existir em vários lugares da sua rede, como:

* Um roteador que foi criado com credenciais padrão
* Uma rede de convidados que pode acessar recursos protegidos
* Um aplicativo interno ou voltado para o cliente
* malware em um computador conectado à rede
* Dispositivos IoT comprometidos

Com vulnerabilidades iminentes e tantas oportunidades para ameaças, é fundamental usar todas as ferramentas disponíveis para garantir a segurança da rede. Neste tópico, você verá como a IA pode ser usada para detectar malware e phishing, bem como como a IA pode aprimorar um sistema de prevenção de intrusões.

Detecção de malware

O malware pode existir em alguns estados que são relevantes para sua detecção:

* malware que está sendo enviado de um dispositivo dentro de uma rede
* malware que está sendo baixado, já foi baixado
* malware que está sendo instalado ou já foi instalado

Algumas das formas mais comuns pelas quais o malware chega a um dispositivo são por meio de e-mail, sites, downloads e muito mais.

Diagrama

O conteúdo gerado por IA pode estar incorreto.

A IA pode ser implementada de várias maneiras para impedir a transmissão bem-sucedida de software malicioso. Primeiro, muitos clientes de e-mail já utilizam alguma forma de IA para avaliar se anexos de e-mail podem danificar os sistemas. A inspeção profunda de pacotes assistida por IA é um método de avaliação de dados que estão sendo transmitidos para ou através de uma rede e pode realizar ações como gerar alertas, bloquear arquivos, redirecionar arquivos ou registrar eventos. Além disso, softwares antivírus tradicionais empregam IA para verificar arquivos em um computador e identificar malware já instalado, muitas vezes realizando correções quando arquivos maliciosos são detectados.

Soluções como o Cisco Secure Endpoint (anteriormente AMP for Endpoints) empregam algoritmos de aprendizado de máquina para analisar o comportamento dos arquivos em tempo real. Utilizando vastos conjuntos de dados de arquivos benignos e maliciosos, os modelos de IA do Secure Endpoint aprendem a reconhecer diferenças sutis e prever intenções maliciosas. Esses modelos são atualizados continuamente com novos dados, garantindo sua eficácia contra as ameaças mais recentes. Quando o Secure Endpoint identifica um arquivo suspeito, ele o bloqueia automaticamente e gera relatórios detalhados para análise posterior. Esse recurso permite que o Secure Endpoint se adapte rapidamente a novas ameaças e forneça proteção robusta contra malwares conhecidos e desconhecidos.

Detecção de phishing

Phishing é uma forma de ataque em que agentes maliciosos se comunicam com indivíduos, muitas vezes se passando por alguém em quem a pessoa confia ou de quem não tem motivos para suspeitar. Devido à complexidade desse tipo de ataque, é menos provável que a vítima reconheça a ameaça antes que ela se torne um problema.

Diagrama

O conteúdo gerado por IA pode estar incorreto.

Além de filtrar anexos potencialmente maliciosos em e-mails, a IA também pode avaliar o conteúdo de um e-mail para determinar a probabilidade de uma tentativa de phishing. A IA pode proteger os usuários examinando o conteúdo do e-mail, a reputação do remetente, as estruturas de URL e outros indicadores para detectar tentativas de phishing.

A solução Cisco Secure Email aplica IA para aprimorar os recursos de detecção de phishing. Ela utiliza processamento de linguagem natural (PLN) para analisar o conteúdo e o contexto dos e-mails. Ao compreender os padrões linguísticos comumente usados ​​em ataques de phishing, a IA pode identificar e-mails suspeitos com precisão. Além disso, algoritmos de aprendizado de máquina avaliam a reputação de remetentes e URLs, sinalizando os itens que se desviam dos padrões típicos. Essa abordagem multicamadas garante que as tentativas de phishing sejam identificadas e bloqueadas antes de chegarem à caixa de entrada do usuário, reduzindo significativamente o risco de ataques bem-sucedidos.

O Secure Email também utiliza uma combinação de detectores especializados (como urgência, chamada para ação, solicitações de credenciais e outros) para atribuir uma classificação de malícia a cada e-mail e agregar essas classificações para determinar se o e-mail deve ser bloqueado. Esse processo aprimora a detecção de ataques de phishing sofisticados, como o Business Email Compromise (BEC), fornecendo uma camada adicional de segurança para as comunicações por e-mail.

**Sistemas de Prevenção de Intrusão**

A IA melhora a eficiência e a precisão de um sistema de prevenção de intrusão (IPS) ao aprender com padrões de tráfego de rede e identificar anomalias que podem indicar violações de segurança. Um IPS tradicional depende de regras e assinaturas predefinidas, o que pode resultar em altas taxas de falsos positivos e detecções perdidas. O IPS aprimorado por IA, por outro lado, utiliza aprendizado de máquina para se adaptar ao comportamento da rede e detectar desvios continuamente em tempo real.

O Cisco Secure Network Analytics (antigo Stealthwatch) utiliza IA para análise de tráfego de rede e detecção de ameaças. O Secure Network Analytics coleta dados de telemetria de vários dispositivos de rede e cria uma linha de base do comportamento normal da rede. Algoritmos de aprendizado de máquina monitoram o tráfego de rede em busca de desvios dessa linha de base que indiquem ameaças potenciais. Transferências de dados ou padrões de acesso incomuns podem disparar alertas para investigação mais aprofundada. O Secure Network Analytics emprega aprendizado de máquina multicamadas para analisar o comportamento do usuário e do dispositivo, detectar malware em tráfego criptografado sem descriptografia e correlacionar dados de ameaças locais com inteligência global de ameaças. Essa abordagem reduz falsos positivos ao se concentrar no comportamento em vez de assinaturas predefinidas, permitindo que as equipes de segurança respondam a ameaças genuínas com mais eficácia. Além disso, o sistema se integra a outros produtos Cisco para fornecer uma visão abrangente da segurança da rede, aprimorando sua capacidade de detectar e mitigar ameaças complexas.

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

Resposta a incidentes

Quando a rede de uma organização é comprometida, o primeiro passo para lidar com o problema é verificar se o ato malicioso ocorreu. Às vezes, o ataque é facilmente perceptível, mas outras vezes pode levar algum tempo para determinar que há um problema devido à exploração de uma vulnerabilidade por um agente malicioso. A IA pode auxiliar as equipes de SecOps e de resposta a incidentes (IRTs) a determinar como o sistema foi comprometido, conter e erradicar o problema para minimizar qualquer dano. A figura a seguir descreve os principais componentes de uma estratégia eficaz de gerenciamento de ameaças que podem ser implementados ou aprimorados com a incorporação da IA. Esses elementos trabalham juntos para identificar e mitigar ameaças, protegendo o sistema contra possíveis danos e violações de dados.

Uma imagem contendo Tabela

O conteúdo gerado por IA pode estar incorreto.

Muitas vezes, um agente malicioso que obtém acesso a um sistema pode não agir imediatamente. Muitas vezes, ele permanece silenciosamente nas sombras, identificando o quanto do sistema pode comprometer antes de ser descoberto. Se o hacker for particularmente habilidoso, ele pode passar despercebido por anos, desviando propriedade intelectual valiosa, dados confidenciais de clientes ou qualquer outra informação que uma empresa possa estar armazenando. Esse comportamento é conhecido como ameaça persistente avançada (APT) e pode ser extremamente prejudicial a uma organização. Os sistemas de IA se destacam na tarefa de caça proativa de ameaças, que é a prática de escanear e analisar ativamente um sistema para procurar ameaças e violações antes que se tornem mais prejudiciais ao sistema. A IA pode monitorar os sistemas em busca de comportamento atípico de login, transferências de dados e outras métricas que podem indicar que algo está errado e identificar APTs antes que mais danos sejam causados.

Quando uma violação de segurança se torna mais evidente, a IA pode auxiliar na detecção, avaliação e resposta por meio de análises de ameaças em tempo real. Ao monitorar a integridade da rede, o desempenho, o tráfego, os alertas e quaisquer outros dados disponíveis, a IA pode identificar rapidamente a ocorrência de uma violação de segurança e correlacionar os dados dos sistemas afetados. Com essas informações, a IA também pode realizar uma análise da causa raiz em sistemas com defeito para ajudar a identificar o escopo e a natureza de um incidente.

A IA também aprimora os mecanismos de resposta a violações de segurança, automatizando algumas das tarefas de resposta e coordenando os esforços de resposta entre diferentes equipes e sistemas. A IA pode executar ações de resposta predefinidas, como isolar sistemas afetados, bloquear endereços IP ou implantar patches em aplicativos vulneráveis. Esse recurso melhora significativamente o tempo de resposta, minimizando danos potenciais e limitando a disseminação de ameaças na rede.

Por fim, a IA aprimora a documentação e os relatórios de incidentes, automatizando a coleta, a análise e a apresentação de dados relacionados a violações de segurança. Utilizando processamento de linguagem natural e aprendizado de máquina, a IA pode analisar grandes quantidades de dados de log, extraindo informações relevantes e gerando relatórios detalhados de incidentes. Esses relatórios podem incluir cronogramas de eventos, sistemas impactados e a natureza do ataque. Para fins de conformidade e auditoria, a IA também pode padronizar os processos de documentação, garantindo consistência e precisão em todos os relatórios.

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

**Colaboração e Comunicação**

Com o desenvolvimento de ferramentas avançadas que aumentam a produtividade, a IA está mudando a forma como os usuários trabalham em conjunto e se comunicam. À medida que mais pessoas começam a trabalhar em casa e as empresas empregam membros de equipe em todo o mundo, assistentes virtuais inteligentes, serviços de transcrição em tempo real e sistemas de tradução de idiomas estão se tornando essenciais. Essas tecnologias não se limitam a automatizar tarefas repetitivas; elas também eliminam barreiras linguísticas e fornecem insights que podem ser aplicados para melhorar a eficiência da comunicação em projetos colaborativos. Neste tópico, você explorará algumas dessas tecnologias e como elas aprimoram a colaboração e a comunicação.

**Assistentes Virtuais Inteligentes**

Ferramentas de assistente virtual inteligente com tecnologia de IA aumentam substancialmente a produtividade e a eficiência organizacional ao otimizar fluxos de trabalho, gerenciar cronogramas e permitir a comunicação.

Tela de computador com foto de homens

O conteúdo gerado por IA pode estar incorreto.

Programas como chatbots e assistentes pessoais podem desempenhar uma série de funções, desde responder a perguntas simples até executar fluxos de trabalho complexos. O Processamento de Linguagem Natural (PLN) permite que esses aplicativos compreendam as perguntas dos usuários para que possam responder de maneira natural e intuitiva, imitando a interação humana. Assistentes virtuais reduzem o tempo gasto pelos funcionários em atividades estratégicas, automatizando tarefas repetitivas, como organizar agendas de reuniões, enviar lembretes ou gerenciar e-mails.

Assistentes virtuais inteligentes são projetados para garantir que os processos de rotina sejam automatizados, resultando em um fluxo de trabalho eficiente e menos sujeito a erros humanos. Por exemplo, a automação da interação com o cliente por meio de chatbots garante um gerenciamento rápido das respostas às dúvidas levantadas pelos clientes. Essa atividade aumenta a satisfação do cliente e proporciona aos trabalhadores a oportunidade de se envolverem em tarefas de nível superior que exigem pensamento criativo e insights humanos.

O potencial colaborativo inerente aos assistentes virtuais inteligentes é bem ilustrado pelo Cisco Webex AI Assistant, parte da plataforma de software de colaboração Cisco Webex. Os recursos do Webex AI Assistant incluem a capacidade de automatizar anotações. O assistente registra pontos importantes levantados durante as reuniões e esclarece as ações de acompanhamento necessárias posteriormente. Além disso, o Webex AI Assistant suporta comandos de voz, permitindo que os usuários controlem vários aspectos do ambiente da reunião sem usar as mãos. Usando comandos de voz, os usuários podem verificar a programação de uma sala de conferência, ingressar em uma reunião, fazer uma chamada, controlar o volume, abrir um novo quadro branco ou compartilhar uma tela.

Com o Assistente de IA Webex, os usuários também podem criar bots personalizados que interagem com os usuários para executar tarefas em seu nome. Alguns exemplos de aplicações práticas incluem bots de atendimento ao cliente que fornecem respostas instantâneas a perguntas frequentes ou ferramentas de fluxo de trabalho de gerenciamento de projetos que atualizam o status e os prazos das tarefas por meio de uma interface de bate-papo.

Por meio de APIs, os bots Webex podem ser conectados a Modelos de Linguagem Pequenos (SLMs) e Modelos de Linguagem Grandes (LLMs), que são cada vez mais extensíveis e podem ser integrados a diversos fluxos de trabalho. Os bots Webex podem ser executados em servidores acessados ​​por webhooks, permitindo interação em tempo real para executar diversas tarefas que executam comandos com base na entrada do usuário.

Interface gráfica do usuário, Diagrama, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

Ao incorporar modelos com capacidade de PNL em um sistema, é possível criar bots extremamente inteligentes que entendem e geram textos semelhantes aos humanos, o que os torna ferramentas úteis para melhorar a colaboração e a comunicação.

Transcrição da Reunião

A transcrição de reuniões é outra faceta das ferramentas de colaboração que estão sendo aprimoradas pela IA. A transcrição de reuniões ajuda a melhorar a produtividade e a acessibilidade no local de trabalho. Utilizando tecnologias avançadas de reconhecimento de fala, os serviços de transcrição de reuniões podem transformar instantaneamente palavras faladas em texto escrito.

Interface gráfica do usuário, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

A transcrição em tempo real permite que os participantes permaneçam engajados na conversa, mesmo em um local barulhento ou mesmo se precisarem se afastar por um minuto. Pessoas com deficiência auditiva também se beneficiam desse recurso, pois ele lhes dá acesso automático ao conteúdo falado por meio de legendas.

A transcrição de reuniões é outro recurso do Assistente de IA do Cisco Webex. Além de realizar transcrições ao vivo, o assistente pode gravar reuniões e fornecer transcrições pós-reunião, indicando os principais destaques e ações a serem tomadas. Informações importantes da reunião tornam-se mais fáceis de revisar e distribuir, pois essas transcrições podem ser editadas, baixadas ou compartilhadas. Ter um registro escrito automatizado das discussões permite que os participantes garantam maior compreensão durante as reuniões, resultando em um engajamento mais dinâmico.

**Tradução de idiomas em tempo real**

A tradução de idiomas em tempo real é outro avanço significativo em ferramentas de colaboração com tecnologia de IA, quebrando barreiras linguísticas e facilitando uma comunicação mais eficaz em ambientes multilíngues. Sistemas de tradução automática com tecnologia de IA podem traduzir a linguagem falada ou escrita em tempo real, permitindo que participantes que falam diferentes idiomas se comuniquem perfeitamente.

Diagrama

O conteúdo gerado por IA pode estar incorreto.

Com o Assistente de IA do Cisco Webex, o Cisco Webex oferece recursos robustos de tradução em tempo real, traduzindo reuniões do inglês para mais de 100 idiomas diferentes. Esse recurso é especialmente valioso para equipes globais nas quais os participantes da reunião têm origens linguísticas diversas. Além disso, a tradução em tempo real pode auxiliar na comunicação escrita, como mensagens de bate-papo e e-mails. A integração da tradução de idiomas em tempo real com a transcrição habilitada por IA garante que todos os membros da equipe entendam e contribuam para as discussões em andamento, permitindo que os participantes revisem a discussão em seu idioma preferido.

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

Internet das Coisas (IoT)

A Internet das Coisas (IoT) consiste em dispositivos menos avançados que um computador ou tablet, como tomadas inteligentes, câmeras, eletrodomésticos, sensores e assim por diante, que podem se interconectar e transmitir seus dados por uma rede como a internet. Atualmente, estima-se que existam 17 bilhões de dispositivos de IoT conectados em todo o mundo, e esse número tende a aumentar com o tempo. Devido à ampla definição de um dispositivo de IoT, o papel da IA ​​no cenário da IoT também é amplo. A IA aprimora os recursos dos dispositivos de IoT processando grandes volumes de dados coletados por eles, aprendendo com eles e tomando decisões inteligentes em tempo real com base nos dados coletados.

O papel da IA ​​na IoT pode ser definido mais claramente com foco nas categorias de dispositivos de IoT. Por exemplo, câmeras de segurança residenciais e comerciais estão conectadas a redes há muito tempo, e os dados de vídeo são frequentemente enviados para um servidor local ou na nuvem. Sistemas de visão computacional de IA podem avaliar fluxos de vídeo em tempo real, realizando tarefas tão simples como identificar movimento até tarefas mais avançadas, como determinar a identidade de uma pessoa. Neste tópico, você explorará como a IA pode melhorar a comunicação entre dispositivos de IoT interconectados e como ela pode conectar esses componentes individuais para criar um sistema coeso, como um edifício ou cidade inteligente.

Dispositivos conectados à IoT

A IA aprimora a comunicação e a coordenação entre dispositivos e redes de IoT controlados por IA, garantindo que funcionem perfeitamente em conjunto para alcançar os resultados desejados. Dispositivos conectados controlados por IA podem se comunicar, compartilhar dados e coordenar ações de forma autônoma, sem intervenção humana, criando ambientes inteligentes onde os dispositivos interagem de forma inteligente para fornecer serviços otimizados.

Diagrama, Desenho técnico

O conteúdo gerado por IA pode estar incorreto.

A IA pode processar e analisar enormes quantidades de dados gerados por dispositivos de IoT. Insights valiosos que impulsionam a tomada de decisões e aumentam a eficiência operacional podem ser extraídos da filtragem, agregação e análise de dados em tempo real usando algoritmos de IA. Por exemplo, em um edifício inteligente, um sistema de IA pode monitorar câmeras de segurança em busca de atividades suspeitas, desligar as luzes em áreas não ocupadas por pessoas e ajustar os sistemas de climatização com base nas condições climáticas e na ocupação, usando informações coletadas por diferentes sensores. Essas interconexões aumentam a eficácia e a eficiência dos sistemas de automação e permitem que esses sistemas se comuniquem com a nuvem e visualizem estatísticas e métricas, bem como consoles de gerenciamento.

Cidades Inteligentes de IoT

Uma "cidade inteligente" é uma área urbana tecnologicamente avançada que utiliza dispositivos conectados à IoT para melhorar a qualidade de vida de seus moradores. Todos os aspectos da vida cotidiana em uma cidade, como a prestação de serviços públicos, o transporte público, a gestão do tráfego, o monitoramento ambiental e a aplicação da lei, podem ser aprimorados por meio do monitoramento e da assistência por IA. Em uma cidade inteligente, qualquer dispositivo de IoT monitorado pode ter seus dados enviados a um sistema de IA projetado para processá-los e fazer inferências sobre eles.

Por exemplo, a IA está sendo usada na gestão de serviços públicos para otimizar a rede de distribuição, reduzir o desperdício e melhorar o tempo de reação a interrupções. No transporte público, a IA está otimizando a programação e o planejamento de rotas para ônibus e trens.

Diagrama, Desenho técnico

O conteúdo gerado por IA pode estar incorreto.

Na gestão de tráfego, a IA pode monitorar o fluxo de tráfego por meio de sensores e câmeras. Ao avaliar os dados dessas fontes, a IA pode relatar com precisão as condições atuais do tráfego e fornecer essas informações a programas como Waze e Google Maps para otimizar rotas para os motoristas. A IA também pode identificar eventos como um veículo inoperante ou um acidente de trânsito e notificar os serviços de emergência. É fácil imaginar um mundo onde as principais vias tenham placas de trânsito de IoT mais complexas que podem ser controladas por IA. Essas placas podem notificar os motoristas sobre uma via ou faixa fechada em resposta a um incidente e redirecionar o tráfego de acordo até que o problema seja resolvido.

Sensores instalados em cidades também podem monitorar diversos fatores ambientais, como qualidade do ar e da água, níveis de ruído, condições climáticas extremas, entre outros. Os dados dos sensores podem ser avaliados em tempo real para alertar serviços de emergência ou sistemas de notificação aos cidadãos sobre eventos como água contaminada em uma área ou má qualidade do ar devido à fumaça de incêndios florestais. Os dados coletados por esses sensores também podem ser usados ​​para identificar tendências em categorias potencialmente prejudiciais, como a poluição do ar. A IA pode prever quais serão os níveis de poluição no futuro se a tendência persistir, permitindo que as autoridades implementem mudanças.

Na aplicação da lei, a IA já está sendo utilizada em cidades ao redor do mundo. Ao posicionar microfones ao redor de uma cidade, a IA pode avaliar os dados dessas fontes para determinar se o som ouvido é um tiro. Utilizando dados de microfones próximos, o sistema de IA pode analisar o nível de decibéis e triangular a fonte do som com alto grau de precisão para enviar serviços de emergência ao local.

Interface gráfica do usuário, Texto, Aplicativo, Email

O conteúdo gerado por IA pode estar incorreto.

Resumo

Reflita sobre as seguintes questões para entender melhor como aplicar os conceitos deste treinamento ao seu próprio ambiente de trabalho, usando IA para impulsionar melhorias e eficiências.

* **Análise Preditiva** : Pense em como você pode implementar análises preditivas orientadas por IA em seu ambiente de rede atual. Como a análise preditiva pode ajudar você a gerenciar e prevenir possíveis falhas de forma proativa? Quais fontes de dados você precisa coletar e analisar?
* **Otimização de rede** : considere como a otimização de rede orientada por IA pode melhorar a eficiência e a confiabilidade da rede da sua organização. Existem ferramentas ou plataformas específicas que você pode integrar para otimizar a rede?
* **Cibersegurança** : Reflita sobre como soluções de cibersegurança baseadas em IA podem ser incorporadas à sua infraestrutura de segurança existente. Como isso pode aprimorar a detecção de ameaças e a resposta a incidentes? Quais vulnerabilidades ou ameaças específicas em seu ambiente podem se beneficiar da análise e mitigação de IA?