RESUMO DE SOLUÇÃO

A inteligência artificial potencializa os insights de segurança cibernética

Soluções de colaboração homem-máquina que utilizam inteligência artificial, aprendizagem profunda e autoaprendizagem

A velocidade e a fúria predominantes no cenário de ameaças à informação estão quase além da compreensão humana. Os serviços de inteligência sobre ameaças respondem a bilhões de consultas sobre ameaças diariamente e possuem centenas de milhões de amostras em bancos de dados. O número cada vez maior de ataques intensificados pela velocidade e pela complexidade pode sobrecarregar até mesmo os profissionais de segurança mais experientes e eficientes.

Destaques

- Expansão das capacidades de análise para investigar dados em quantidade e complexidade cada vez maiores e apresentar informações de inteligência decisivas.
- Análises de ataque geradas por máquina à disposição dos analistas de segurança.
- Personalização e maximização das defesas corporativas sem exigir aumento do tamanho ou das qualificações da equipe.
- Reconhecimento de padrões e comportamentos causadores de violações de segurança por meio de algoritmos de autoaprendizagem.
- Melhoria da relação sinal/ruído dos indicadores de ameaças.
- Análise avançada do comportamento do malware por meio de redes neurais.
- Integração dos investimentos existentes, incluindo controles nativos e de terceiros.

Conecte-se conosco

Análises e colaboração homem-máquina são a solução. Embora a automação venha há muito contribuindo para o processo de segurança, o aumento da complexidade da TI, o aumento da velocidade dos ataques e a escassez de qualificações estão tornando as tecnologias analíticas um componente obrigatório em planos rigorosos de segurança cibernética. A combinação de inteligência automatizada com insights estratégicos humanos proporciona resultados superiores em segurança.

Com a colaboração homem-máquina (inteligência artificial, aprendizagem profunda e autoaprendizagem), as capacidades avançadas de análise são expandidas, o que possibilita investigar quantidades enormes de dados e apresentar informações de inteligência decisivas. A colaboração homem-máquina, bem como uma abordagem em camadas para a segurança, ajuda a detectar, proteger e corrigir as violações mais simples ou mais complexas, proporcionando uma solução completa para as necessidades corporativas.

A inteligência coletada em ameaças e ataques não pode resolver sozinha os desafios de segurança cibernética de uma corporação. Os insights humanos obtidos pelo uso de inteligência permitem que as equipes de segurança personalizem e maximizem as defesas corporativas para uma proteção otimizada, sem exigir aumento do tamanho ou das qualificações da equipe. A inteligência permite que você reaja ao seu ambiente. Os insights lhe dão o poder de mudá-lo.

Analises por inteligência artificial

Razão e lógica para inspirar insights

A inteligência artificial (IA) imita o cérebro humano ao considerar julgamentos de valor e resultados para determinar o que é bom ou mau, certo ou errado. Esses mesmos processos podem elevar a segurança cibernética acrescentando complexidade à aprendizagem profunda, agregando razão, ações sugeridas e resolução de problemas.

- A inteligência artificial utiliza razão e lógica para compreender o seu ecossistema. A IA utiliza várias análises complexas, incluindo aprendizagem profunda e processamento de linguagem natural (NLP). Embora a autoaprendizagem e a aprendizagem profunda possam abranger análises descritivas e prescritivas, a força da IA está em oferecer análises preditivas e prescritivas mais maduras.
- A IA baseia-se em dados a partir dos quais ela possa ser treinada. A IA só pode aprender como lidar com diversos tipos de situações com base nos dados que lhe são fornecidos. Como em qualquer processo de segurança, é fundamental identificar o caso de uso e determinar o problema que precisa ser resolvido.
- A computação cognitiva pode produzir alertas e iniciar ações apropriadas para conter ameaças.
- A IA pode ser utilizada para múltiplas finalidades por fornecedores, incluindo uma melhor detecção de ameaças.

Principais vantagens

McAfee® MVISION EDR

- A capacidade da auto-aprendizagem de "aprender" e de se tornar mais inteligente com o passar do tempo pode elevar as capacidades descritivas, de diagnóstico, preditivas e prescritivas do seu departamento.
- Ajuda as equipes de segurança a se manterem à frente das ameaças modernas com investigações orientadas por IA que revelam riscos relevantes, além de automatizar e eliminar o trabalho manual de coleta e análise de evidências.
- Caso e-mails suspeitos sejam considerados maliciosos, é possível determinar rapidamente quais máquinas da organização podem ter sido afetadas.
- Utiliza IA para classificar rapidamente as ameaças, permitindo às organizações priorizar seus problemas mais críticos.
- Utiliza uma IA integrada que ajuda a melhorar a relação sinal/ruído dos indicadores de ameaça.

Atualize os recursos de SOC existentes

A inteligência e os insights da colaboração homem-máquina proporcionam uma segurança de endpoint mais eficiente e sustentável. As equipes de segurança, por si sós, não conseguem acompanhar o volume de ameaças, enquanto as máquinas, por si sós, não conseguem produzir respostas com insights.

- A análise avançada expande a detecção e interpreta melhor os alertas. A automação e as investigações orientadas por IA informam até mesmo analistas novatos como analisar em um nível mais elevado, reduzindo o tempo de resposta e liberando os analistas mais experientes para concentrar suas habilidades na caça a ameaças.
- A investigação orientada por IA reduz o conhecimento e os recursos necessários para realizar investigações, além de aumentar a velocidade e a eficiência com as quais os analistas podem verificar o risco do incidente e sua causa raiz. Cada analista pode ser mais eficiente.

Figura 1. Caso sejam detectados e-mails suspeitos ou ameaças, a investigação orientada por IA pode localizar e responder a milhares de endpoints internos e externos.

Principais vantagens

McAfee® MVISION Cloud

- Utiliza autoaprendizagem para criar modelos de comportamento que detectem comprometimento de contas ativas e ameaças internas e que ainda apliquem assinaturas e área restrita (sandbox) para identificar malware na nuvem e deter ameaças.
- A análise comportamental de usuários e entidades (UEBA) constrói automaticamente um modelo de aprendizagem autônoma baseado em múltiplas heurísticas e autoaprendizagem para identificar padrões de atividade característicos de ameaças ao usuário em múltiplos serviços de nuvem, bem como comportamentos maliciosos, incluindo elementos internos que estejam roubando dados confidenciais.
- O mapeador de atividades orientado por IA emprega inteligência artificial para compreender os aplicativos e mapear as ações dos usuários em um conjunto uniforme de atividades, possibilitando controle e monitoramento padronizado dos aplicativos.

Resultados melhores e mais rápidos com autoaprendizagem

Uso de algoritmos para detectar padrões e comportamentos

A autoaprendizagem emprega automação para aprender e se adaptar ao longo do tempo, conforme surgem novos dados. Ela leva a análise de segurança do diagnóstico e da postura descritiva para uma postura preditiva e prescritiva, resultando em uma detecção mais rápida e mais precisa. As equipes de segurança podem aproveitar algoritmos de autoaprendizagem para reconhecer padrões e detectar comportamentos causadores de violações de segurança muito mais rapidamente do que os seres humanos. Como resultado, a autoaprendizagem permite que a segurança de endpoint evolua continuamente, de maneira a deter novas táticas de ataque. Vantagens da autoaprendizagem:

- Pode identificar malware oculto. O reconhecimento de padrões pode detectar comportamentos de ameaça que resultem em violações de segurança, sejam conhecidas ou desconhecidas.
- Mantém as equipes de segurança melhor informadas, de maneira que possam tomar decisões melhores.
- Ajuda os diretores de segurança (CSOs) a obter o máximo de suas equipes e de seus ativos de produto ao livrar os analistas de segurança das tarefas corriqueiras e ajudando até mesmo os integrantes mais novatos da equipe a se tornarem mais eficientes e produtivos.
- Ajuda você a se manter a par das novas técnicas introduzidas pelos adversários. A automatização da descoberta de novas táticas e estratégias de ataque ajuda as equipes de segurança a se manter à altura da resolução de problemas, ao mesmo tempo que fornece informações de inteligência às equipes de segurança para promover insights que resultem em uma resposta mais contundente.

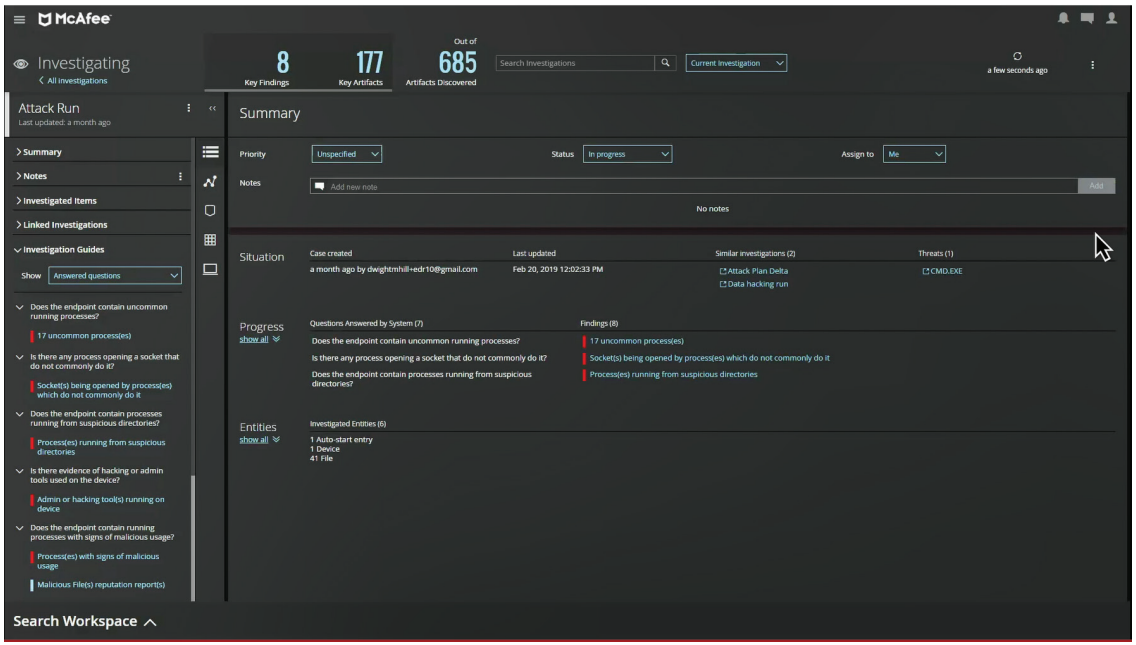

Figura 2. As investigações orientadas por inteligência artificial automatizam e eliminam o trabalho manual de coletar e analisar evidências.

- Torna-se mais precisa à medida que mais dados são disponibilizados. A evolução do desempenho aprimorado e dos aperfeiçoamentos das capacidades permite que a autoaprendizagem aprenda e aumente a precisão das funções de segurança cibernética.
- Ajuda as equipes de TI a analisar falhas. Quando a segurança de endpoint não consegue evitar os danos resultantes de um ataque, a autoaprendizagem acumula elementos de dados relevantes em um único lugar e os coloca à disposição dos analistas de segurança quando necessário.

A aprendizagem profunda baseia-se na autoaprendizagem

A aprendizagem profunda confere a um sistema de defesa de segurança cibernética a capacidade de aprender automaticamente através de bilhões de combinações e observações, reduzindo a dependência de recursos humanos. A aprendizagem profunda ajuda na tomada de decisões relacionadas à defesa, baseando-se na autoaprendizagem para detectar, proteger e corrigir ameaças, tanto antigas quanto novas. A aprendizagem profunda reflete comportamentos multifacetados de segurança em seus múltiplos algoritmos complexos, além de também identificar pontos fora da curva e relacionamentos únicos.

- A aprendizagem profunda é eficaz porque quanto mais vê, mais sabe. As metodologias de aprendizagem profunda empregam algoritmos de redes neurais para chegar a conclusões observando o que aconteceu no passado, aplicando razão e prestando atenção a dados atuais e preditivos.
- Os algoritmos de aprendizagem profunda tendem a ser tão complexos quanto a situação em questão. A aprendizagem profunda pode ser descritiva, de diagnóstico, preditiva e também prescritiva.
- As metodologias de aprendizagem profunda podem trabalhar com informações simbólicas e conceituais para uma tomada de decisões complexa. Elas podem ser direcionadas para neutralizar ameaças com base na análise dos padrões de atividade e na definição de quais atividades parecem normais e esperadas e quais parecem anomalias.
- A eficácia e a efetividade do algoritmo de aprendizagem profunda depende de conjuntos de dados eficazes.

Saiba mais

Para saber mais sobre as vantagens do uso de inteligência artificial, aprendizagem profunda e autoaprendizagem na segurança cibernética, leia o seguinte white paper da McAfee: Introduction to Artificial Intelligence and Machine Learning (Introdução à inteligência artificial e à autoaprendizagem).

Forrester Spotlight: relatório Empower Security Analysts Through Guided EDR Investigation (Empodere os analistas de segurança com investigação de EDR orientada)

SANS: white paper Por que a EDR tradicional não funciona — e o que fazer em relação a isso

SANS: webcast Por que a EDR tradicional não funciona — e o que fazer em relação a isso

Recursos adicionais

Assista o vídeo AI-Guided Investigations with MVISION EDR (Investigações orientadas por IA com MVISION EDR)

McAfee MVISION Cloud
Solicite uma demonstração

McAfee
Together is power.

Av. Nações Unidas, 8.501 – 16º andar
Pinheiros – São Paulo – SP
CEP 05425-070, Brasil
+(11) 3711-8200
www.mcafee.com/br