IBM Security

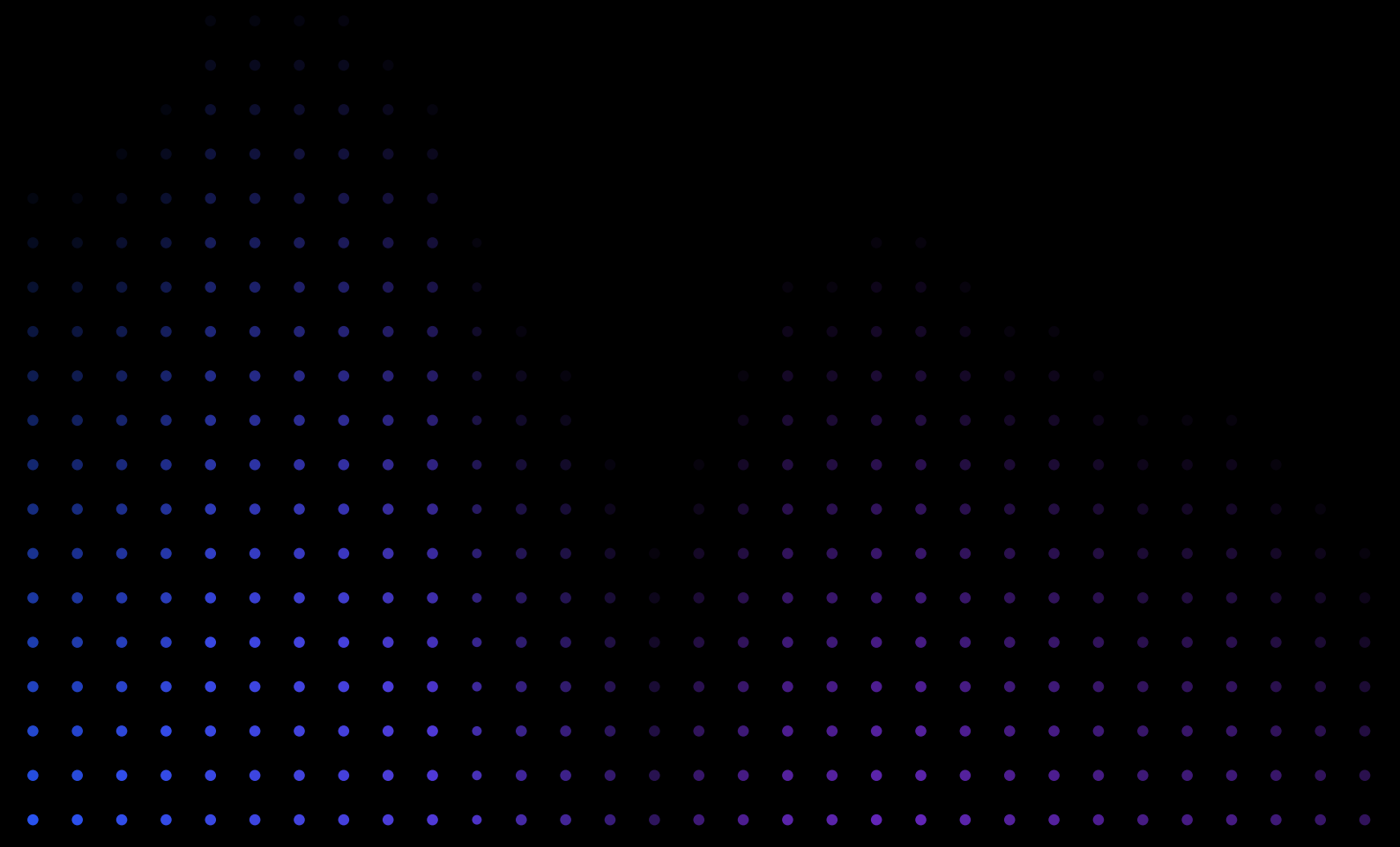
IBM

Além das expectativas: IA no seu SOC

Faça estas 7 perguntas antes de adotar uma solução cognitiva de segurança cibernética.

Visite o nosso site →

Falar com um especialista →



01

Estou confiante em nosso equilíbrio de risco e segurança?

Os CISOs têm os trabalhos mais difíceis em tecnologia: Eles devem permitir que os usuários acessem dados críticos - mas também protegem esses dados contra ameaças internas, abuso de credenciais e erro humano. O trabalho deles é detectar e responder a todas as ameaças - embora a mais difícil de todas - contar com uma equipe sobrecarregada e com falta de pessoal.

Pior, as apostas estão em um nível histórico e as desculpas não serão suficientes. As organizações e seus clientes e consumidores exigem segurança. Os reguladores estão olhando. As taxas de seguro de cibersegurança estão aumentando. Os investidores estão inquietos e os advogados estão à disposição. Todos, desde os Diretores aos funcionários, exigem segurança absoluta e hermética - enquanto eles também são um vetor de vulnerabilidade.

Considere estes três itens na sua lista de sugestões:

Você está com pouco talento

Os analistas de nível 1 ou da linha de frente geralmente são novos no setor. Leva tempo para que desenvolvam verdadeiramente as habilidades, confiança e maturidade em suas habilidades de investigação necessárias em todo o seu SOC. De acordo com ESG Research, 51% das organizações relataram ter uma “escassez problemática” de habilidades em segurança cibernética em 2018. Isso representa um aumento de 45% em 2017. A fadiga no trabalho de segurança cibernética é real e, de acordo com ESG, 38% dos profissionais de segurança cibernética já dizem que a falta de habilidades levou a altas taxas de esgotamento e desgaste da equipe.

Os tempos de retenção são muito longos - e estão custando

Os tempos médios de retenção variam entre 50 e 200 dias. As empresas que identificaram uma violação em menos de 100 dias economizaram mais de US$1 milhão em comparação com aquelas que levaram mais de 100 dias.

Sua equipe tem sobrecarga de informações - e você não está ajudando

Sua organização provavelmente tem fadiga no trabalho de segurança cibernética (não se preocupe, você não está sozinho). Está sobrecarregada por trabalho repetitivo e há uma quebra de processos definidos. Tudo isso aumenta a probabilidade de que um importante indicador de compromisso (IoC) tenha sido esquecido. E quando você adiciona novas soluções pontuais para lidar com as ameaças mais recentes e avançadas, você só está piorando as coisas: Você está criando mais silos de dados, adicionando complexidade de integração e aumentando o número de informações que seus analistas devem analisar.

Um SIEM é necessário para sua operação, mas e a IA? Qual parte é expectativa e qual parte é real?

02

Como a IA me ajuda a encontrar o equilíbrio certo?

Você já ouviu os evangelistas de IA, mas como garantir que a solução de IA em que se investe é uma solução cognitiva inteligente que pode facilitar seu trabalho? A resposta da não expectativa gira em torno de garantir que possa aprender e ser proativa. Deve automatizar suas tarefas repetíveis para mitigar a fadiga e resolver o que pode ser seu maior desafio - as pessoas. É simples assim.

03

Como a IA realmente reforça minha postura de segurança?

O fato é que não é humanamente possível acompanhar o cenário de ameaças em constante expansão, especialmente considerando o quão ocupado você está lidando com a liderança, mantendo a postura de segurança da organização e as tarefas diárias de execução do seu SOC. Você precisa de um arsenal de ferramentas prontamente disponíveis para proteger seu SOC.

Nos últimos anos, a IA foi exagerada e sobrevendida. Entendemos isso. Mas considere o seguinte: a IA correta aplicada corretamente no seu SOC é uma ferramenta altamente eficaz que aprende e se atualiza continuamente, por conta própria. Não é uma solução definitiva, mas se torna uma parte vital do seu arsenal de armas de segurança.

04

A IA substituirá minha equipe? Esta solução ameaçará seu sustento?

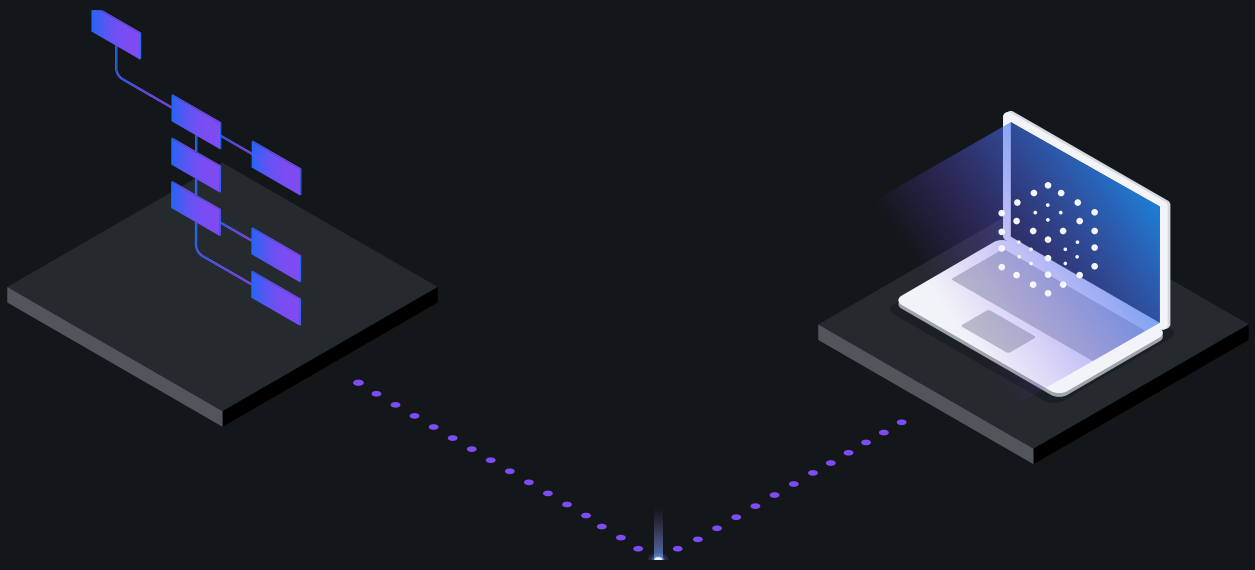
A IA trabalha com sua equipe, não contra ela. Lida com tarefas repetíveis e ajuda a tomar decisões mais bem informadas. Combina proativamente dados externos - informações de todos os lugares - e os combina com o seu ambiente nativo para entender qual deve ser o seu próximo passo. Em todos os casos, você decide quanto trabalho deseja que a IA faça, desde tarefas demoradas até a tomada de decisões de rotina. Em resumo, a IA sempre estará lá, sempre aprendendo - mas você definirá o rumo e estará no comando.

05 Esta solução é IA ou machine learning? Eu sei a diferença?

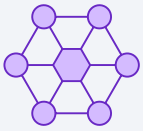
Quando as pessoas usam termos como “IA” e “machine learning”, costumam usá-los de forma intercambiável. Pior, também lançam uma sopa de letrinhas de abreviações, como “ML”, em vez de “machine learning”, ou dizem “inteligência artificial”, em vez de “IA”. Mas não deixe que isso o confunda: IA (inteligência artificial) e ML (machine learning) não são a mesma coisa; portanto, não compre uma solução de aprendizado de máquina quando realmente quiser IA. O aprendizado de máquina concentra-se na capacidade das máquinas de interagir com os dados. Pode “aprender” e até alterar um algoritmo à medida que recebe mais dados, mas é aí que ele para, pois o aprendizado de máquina é um subconjunto da IA.

A IA traz a capacidade cognitiva de crescer, aprender e executar tarefas com base em algoritmos. Capacita o seu SOC, tornando-se cada vez mais conhecedora, à medida que reúne informações de uma variedade quase infinita de fontes - se esses dados são facilmente pesquisáveis em um banco de dados ou gerados por uma máquina (estruturada) ou mídia social ou artigos de revistas (não estruturados). A IA pode aprender com os dados da sua empresa ou externamente através de blogs, relatórios, pesquisas e alertas de segurança - em qualquer lugar e em todos os lugares. São todos esses elementos que separam a IA do aprendizado de máquina.

Com a IA no seu SOC, você tem acesso a um repositório de memória institucional que pode fornecer recomendações projetadas especificamente para sua organização. A IA permite equilibrar suas operações e soluções de segurança - por isso é importante entender se você está comprando uma verdadeira solução de IA.

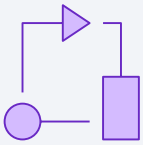


06 Que avanços na postura de segurança posso esperar com a IA?



Encadear Incidentes Potenciais Diferentes, Automaticamente.

A IA é excelente na automação e integração da análise de causa raiz. A IA captura conexões para obter informações sobre ameaças e riscos - e não fica cansada. A IA mostra inter-relações que sua equipe pode perder devido à rotatividade, inexperiência ou passagem do tempo. Sem a IA, os analistas inexperientes podem fechar um alerta porque pensaram que era uma única instância de um ataque. Encontra pontos comuns entre os incidentes usando o raciocínio cognitivo e fornece feedback acionável com contexto - se os pontos comuns são de um ticket fechado ontem ou meses antes. A IA reúne informações de ameaças externas para ajudá-lo a adicionar mais contexto à sua análise e captar o que os outros podem perder.

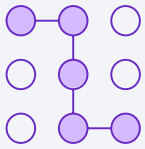


Resolve seu problema de pessoal.

A IA determina a análise da causa raiz e pode orquestrar as próximas etapas com base no conhecimento que construiu sobre as ameaças e sua organização. Não tira férias. Nunca troca você por outro emprego. E você não precisa se preocupar em não reconhecer um IOC significativo.

Realize investigações consistentes e mais profundas, sempre.

A IA pode ler dados não estruturados e estruturados - mais do que humanamente possível de ler. Aprende. Fornece as informações necessárias para reduzir o tempo médio de detecção e o tempo médio de resposta (MTTD e MTTR) - com um processo de escalonamento mais rápido e decisivo. A IA pode fornecer análises avançadas para detectar ameaças conhecidas e desconhecidas. A IA realiza investigações consistentes e mais profundas, sempre, e capacita seus analistas a tomar uma decisão baseada em dados, em vez de confiar em seus sentimentos.



Tenha um fluxo de trabalho de resposta a incidentes (IR) robusto e automatizado que abrange pessoas, processos e tecnologia.

A IA orienta os analistas de segurança através de uma resposta rápida e completa, orientada por dados e evidências. Automatiza o fluxo de trabalho e a correção. Permite que os SOCs avaliem e refinem seus processos de IR, continuamente.

07

Como a IA melhora o SOC antes, durante e após um ataque?

Antes, durante e após uma violação de dados, a IA permite que seu SOC esteja melhor preparado e se recupere mais rapidamente. O IBM® QRadar® Security Intelligence Platform aproveita essa tecnologia e a integra ao seu SOC para fornecer uma solução de análise abrangente - tudo em uma única plataforma.

Antes de um Ataque	Durante um Ataque	Após um Ataque
IBM® QRadar® SIEM fornece visibilidade completa e identifica ameaças e anomalias no início do ciclo de ataque.	IBM QRadar SIEM coleta continuamente evidências em andamento, fornecendo acesso fácil a dados forenses. Prioriza com base no impacto nos negócios.	IBM QRadar SIEM ajusta continuamente os mecanismos de detecção com base nas lições aprendidas.
IBM QRadar Advisor with Watson™ investiga automaticamente todas as anomalias e identifica comportamentos de ataque de alto risco.	IBM QRadar Advisor with Watson multiplica a força da sua equipe com a análise de causa raiz automatizada e ajuda a entender a dimensão completa da ameaça.	IBM QRadar Advisor with Watson adapta modelos para responder com maior precisão a ameaças futuras.
IBM Resilient® permite que os SOCs preparem fluxos de trabalho de IR robustos e automatizados, abrangendo pessoas, processos e tecnologia.	IBM Resilient orienta os analistas de segurança através de uma resposta rápida e completa, e automatiza o fluxo de trabalho de incidentes e as soluções.	IBM Resilient permite que os SOCs avaliem e refinem continuamente os processos de IR.

Sobre o IBM QRadar Advisor with Watson

Com a IA, você pode otimizar suas operações de SOC enquanto frustra com sucesso as ameaças cibernéticas cada vez maiores. O IBM QRadar Advisor with Watson automatiza tarefas SOC de rotina, encontra pontos comuns entre investigações e fornece feedback acionável aos analistas, liberando-os para se concentrarem nos elementos mais importantes da investigação e aumentam a eficiência.

Saiba mais →

Referências

O estado das carreiras profissionais de segurança cibernética, ESG