IBM QRadar Advisor com Watson

Automatize seu Centro de Operações de Segurança (SOC) com Inteligência Artificial (IA)

Destaques

- Iniciar uma nova parceria entre analistas e suas tecnologias
- Automatizar análises de incidentes e forçar a multiplicação dos esforços de sua equipe
- Promover investigações consistentes e aprofundadas
- Fazer com que a escalação dos incidentes seja mais rápida e decisiva
- Reduzir os períodos de interrupção

Conheça nosso site

Fale com especialista

Desafios Atuais do SOC

Não importa se você tem uma equipe de segurança de 2 ou 100 pessoas, seu objetivo deve ser garantir o sucesso de sua empresa. E isso significa proteger sistemas, usuários e dados críticos, detectar e responder a ameaças, e manter-se à frente dos crimes cibernéticos. Mas há uma série de desafios críticos que prejudicam o SOC atualmente e que podem impedir que você alcance seu objetivo.

Ameaças que Não São Solucionadas

O excesso de informações é ignorado simplesmente porque seus analistas podem não ter conhecimento de como as informações estão relacionadas. É difícil obter insights práticos, por isso, seus analistas podem optar por trabalhar apenas nos casos em que têm mais confiança, o que pode fazê-los perder oportunidades de investigação e, com isso, expor sua empresa a riscos.

Sobrecarga de Insights

Os enormes volumes, variedades e velocidade dos insights a serem analisados dificultam a priorização do trabalho e impedem sua equipe de chegar à causa-raiz. Isso acontece com empresas de todos os tamanhos, não apenas com as grandes corporações. Nenhum analista sabe por onde começar a "montar" o contexto local para identificar com rapidez e eficiência o problema que tem em mãos. Eles acabam se afundando em trabalhos repetitivos e a maior parte desses profissionais sofre com fadiga, o que resulta em falhas nos processos já definidos e em grandes chances de perder um indicador de compromisso (IoC).

93%[1] das empresas não conseguem fazer uma triagem de todas as ameaças relevantes. Quase 1/4[2] delas acham que têm sorte de escapar sem qualquer impacto das consequências de não investigar esses alertas.

Os Períodos de Interrupção Estão Ficando Piores

Uma das métricas mais comuns usadas pelos profissionais de segurança para medir o sucesso da proteção e defesa dos dados é o período de interrupção, principalmente o tempo médio de detecção (MTTD) e o tempo médio de resposta (MTTR). O período de interrupção mede por quanto tempo um ator de ameaça tem seu acesso não detectado em uma rede até que seja completamente removido.

Apesar de hoje termos mais soluções e dados do que nunca, o período de interrupção médio varia entre 50 e 200 dias. Por que isso é tão importante? De acordo com o Ponemon Institute, 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. Do mesmo modo, empresas que detiveram uma violação em menos de 30 dias, economizaram mais de US$ 1 milhão em comparação com aquelas que levaram mais de 30 dias para resolver o problema.[3]

A falta de investigações consistentes, de qualidade e ricas em dados contextuais leva a danos nos processos existentes e a grandes chances de perder insights cruciais, expondo a empresa a riscos.

Falta de Especialistas em Segurança Cibernética e Fadiga no Trabalho

Assim como a maioria dos analistas de segurança, sua equipe provavelmente está com trabalho de mais, pessoas de menos e cansada, e isso não é culpa deles. É humanamente impossível acompanhar o cenário com ameaças cada vez mais numerosas, especialmente se pensarmos em como as equipes estão ocupadas com as tarefas cotidianas de operações de segurança que precisam realizar em seu SOC.

Quando falamos em fadiga nos trabalhos de segurança cibernética, sua empresa não está sozinha. De acordo com a ESG Research, em 2018, 51% das empresas afirmaram ter uma "falta problemática" em termos de habilidades de segurança cibernética. Esse índice era de 45% em 2017.[vi] A fadiga nos trabalhos de segurança cibernética é real e, de acordo com a ESG, 38% dos profissionais da área dizem que a falta de habilidades em segurança cibernética levou a índices elevados de depressão e a brigas na equipe. E a situação só deve piorar à medida que as montanhas de dados continuam a crescer e as falhas de habilidades continuam a aumentar, com uma expectativa de 1,8 milhão de cargos de segurança não preenchidos até 2022.[5]

Os analistas de linha de frente ou nível 1 costumam ser novos no setor e nas equipes. Leva um tempo até que eles realmente desenvolvam habilidades, confiança e maturidade para realizar investigações.

Rápida Adoção de Soluções Mais Específicas

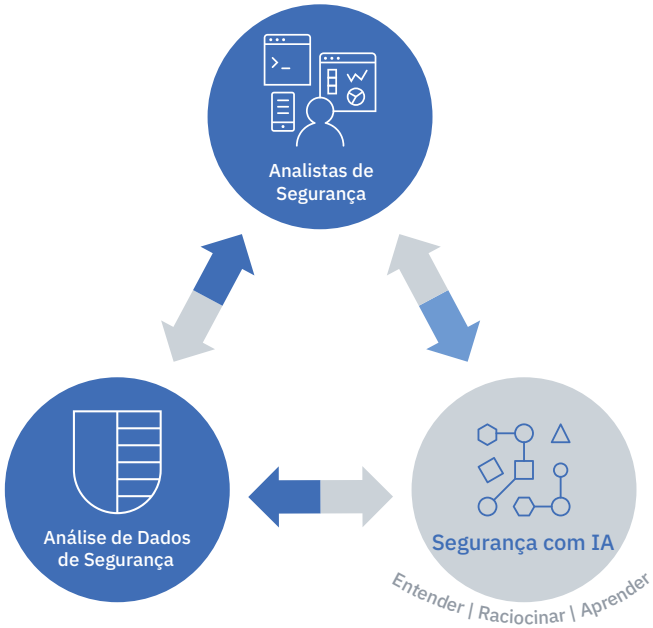
Os diretores de segurança da informação (CISOs) estão adotando soluções mais específicas para impedir as novas ameaças em constante evolução. Seja qual for seu caso de uso — proteger dados críticos, ameaças internas, gerenciamento de identidades e acesso, abuso de credenciais ou outros — em algum momento você encontrará uma solução para isso. Consequentemente, a integração entre soluções, a falta de escalabilidade e a dificuldade de uso está causando graves problemas para as empresas.

Os Riscos São Sempre Altos

As desculpas não pagam as contas, nem ajudam a reconquistar a confiança de um cliente insatisfeito. Segundo o Ponemon Institute, o custo total médio de uma violação de dados subiu de US$ 3,62 milhões para US$ 3,86 milhões, um aumento de 6,4% em relação a 2017.[6] Os líderes da área de segurança também estão enfrentando um exame cada vez mais minucioso por parte de diversas fontes, como liderança executiva, clientes, funcionários, investidores, órgãos reguladores, empresas de seguro e grupos de monitoramento. Com riscos tão grandes o tempo todo, será que sua empresa pode se dar ao luxo de não estar preparada?

Inicie uma Nova Parceria entre Analistas e suas Tecnologias

A inteligência artificial (IA) preenche essa falha e revela uma nova parceria entre analistas de segurança e suas tecnologias. Cada um tem seus pontos fortes, como o bom senso dos humanos e a eliminação de percepções enviesadas e as análises de dados de concessões da IA. Mas, juntos, trabalhando em equipe, eles podem impedir as ameaças e reduzir os períodos de interrupção com mais sucesso.



Benefícios da IA no SOC

Automatizar Análises de Incidentes e Forçar a Multiplicação dos Esforços de sua Equipe

Não desperdice capital humano em análises rotineiras. Em vez disso, deixe que a IA automatize as tarefas repetitivas do SOC, aumente o foco de seus analistas em elementos mais importantes da investigação e aumente a eficiência da equipe.

Promover Investigações Consistentes e Aprofundadas

Você sabia que os analistas só podem acompanhar 8% das informações necessárias para fazer seu trabalho? Melhore as funções de seu SOC deixando que a IA encontre automaticamente pontos em comum entre os incidentes usando raciocínio cognitivo e forneça feedback prático com contexto. Pense na IA como seu conselheiro pessoal: ela deve sair em busca de dados de inteligência de ameaças externas para ajudá-lo a complementar o contexto de sua análise e deve associar diferentes incidentes em potencial que estão relacionados, assim você economiza mais tempo.

Não importa se são 16h30 de uma sexta-feira ou 10h de uma segunda-feira, seus analistas devem estar focados o tempo todo em promover investigações consistentes e completas.

Reduzir os Períodos de Interrupção

Reduza o MTTD e o MTTR com um processo de escalação mais rápido e decisivo. Determine a análise de causa-raiz e conduza as próximas etapas com confiança, mapeando o ataque com seu manual dinâmico, como o modelo MITRE ATT&CK.

IBM QRadar Advisor with Watson: Desenvolvido com IA para o Analista de Segurança de Linha de Frente

IBM® QRadar® Advisor capacita os analistas de segurança a conduzir investigações consistentes e fazer escalações de incidentes mais rápidas e decisivas, resultando em períodos de interrupção menores e em melhor eficiência da equipe.

Forçar a Multiplicação dos Esforços de sua Equipe

- Priorize uma lista de investigações com maior risco
- Filtre e classifique os dados de acordo com a importância
- Tome ações em relação ao feedback aprimorado do IBM Watson® usando informações de inteligência de ameaças internas e externas

Promover Investigações Consistentes e Aprofundadas

- Relacione automaticamente as investigações por meio de pontos observáveis associados usando análises de dados de investigação cruzada e vá além do possível incidente em questão
- Evite a duplicação de esforços
- Determine se você precisa fazer ajustes adicionais em caso de diversas investigações duplicadas acionadas pelos mesmos eventos

Reduzir os Períodos de Interrupção

- Visualize como o ataque ocorreu e progrediu, um nível de confiança para cada progressão, quais táticas foram usadas e quais ainda podem ser usadas através do modelo MITRE ATT&CK
- Aproveite a Easy Incident Scoring (pontuação fácil de incidentes) para fornecer aos analistas um processo de escalação mais rápido e decisivo
- Aumente a eficiência dos analistas e reduza o MTTD e o MTTR

Você não precisa acreditar em nossa palavra. Veja por si mesmo os benefícios que nossos clientes estão tendo com a IA. Os analistas da Sogeti Luxembourg conseguiram reduzir o tempo de investigação de 2 a 3 horas para 2 a 3 minutos. Esse é um tempo valioso que os analistas podem aproveitar com a investigação de ameaças reais e complementando suas investigações com contextos mais ricos.

Muitos outros clientes estão usando a IA para forçar a multiplicação dos esforços de suas equipes. E, com a IA, eles podem usar funcionários menos qualificados para preencher os cargos de analistas de nível 1, promovendo os analistas de nível 1 para que se concentrem nas responsabilidades de nível 2 e forcem a multiplicação dos esforços de suas equipes.

Para saber mais histórias de sucesso e obter informações sobre como você pode aproveitar a IA, acesse ibm.biz/learnAI

Para mais informações

Para saber mais sobre o QRadar Advisor with Watson, entre em contato com o especialista em segurança da IBM.

ibm.com/us-en/marketplace/cognitive-security-analytics

Conheça nosso site

Fale com especialista

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América Novembro de 2018

1 McAfee Labs Threat Report. McAfee. 2016. (https://www.mcafee.com/ content/dam/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2016.pdf)

2 McAfee Labs Threat Report. McAfee. 2016. (https://www.mcafee.com/ content/dam/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2016.pdf)

3 Cost of a Data Breach. Ponemon, 2018. (https://www.ibm.com/security/ data-breach)

4 Cybersecurity Realities and Priorities for 2018 and Beyond. Enterprise Strategy Group. 2018. (https://www.thehaguesecuritydelta.com/media/ com_hsd/report/213/document/ESG-Research-Insights-Paper-Spirent-2018.pdf)

5 Cybersecurity Realities and Priorities for 2018 and Beyond. Enterprise Strategy Group. 2018. (https://www.thehaguesecuritydelta.com/media/ com_hsd/report/213/document/ESG-Research-Insights-Paper-Spirent-2018.pdf)

6 Cost of a Data Breach. Ponemon, 2018. (https://www.ibm.com/security/ data-breach)

Recicle

24021824-BRPT-00