IBM **Security**

Cinco principais mitos sobre o SIEM

Você pesquisou as soluções SIEM recentemente?
Porque as coisas mudaram.

IBM®

Introdução

Alguns insistem em afirmar que soluções SIEM são complicadas e complexas — e, portanto, voltadas apenas para grandes organizações. É verdade, alguns SIEMs são criados apenas para grandes empresas, mas esse mito desconsidera as soluções SIEM mais avançadas desenvolvidas para empresas de todos os tamanhos.

Não é segredo que o setor de segurança digital está enfrentando uma grande escassez de habilidades. Soluções de segurança — como SIEM ou outras — precisam ser desenvolvidas para permitir que você seja eficaz no seu trabalho, apesar dos seus recursos possivelmente limitados.

Analisaremos os cinco principais mitos sobre os SIEMs e investigaremos o que você deve esperar de um SIEM atualmente.

Mito nº 01

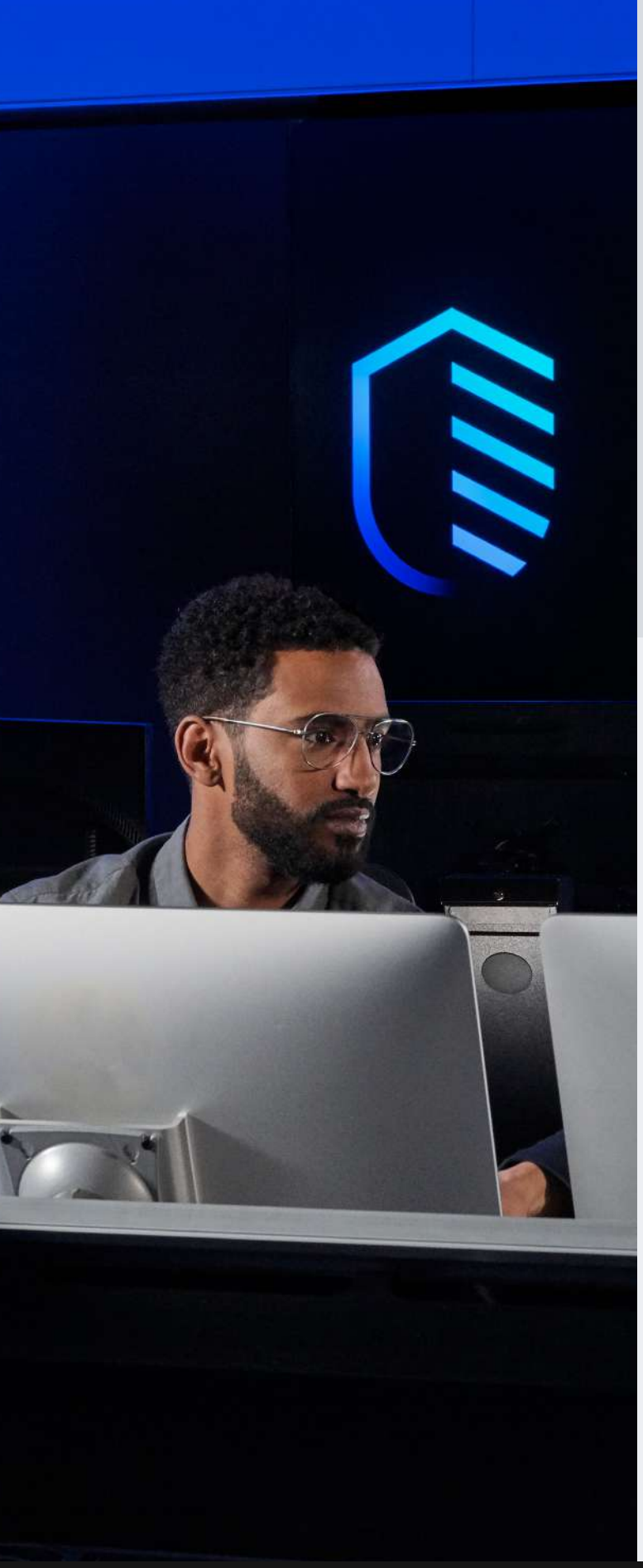
Um SIEM apenas detecta ameaças conhecidas. Ele não ajuda com ameaças desconhecidas.

Soluções SIEM usam apenas regras para detectar ameaças e, para escrever uma regra eficaz, primeiro você precisa saber o que procurar.

Verdade

SIEMs eficazes usam uma combinação de regras, detecção de anomalias, machine learning e análises de comportamentos para encontrar tanto ameaças conhecidas quanto desconhecidas.

Eles também usam correlação avançada para ligar os pontos e compreender atividades de ameaças relacionadas. Quando existe uma combinação de análise de dados avançada e regras pré-incorporada no seu SIEM, ele pode ser aplicado imediatamente às suas atividades de rede, ativos, usuários e aplicações, para que você possa ir além de apenas ameaças conhecidas e também identificar atividades anômalas que possam indicar ameaças desconhecidas.



Mito nº 02

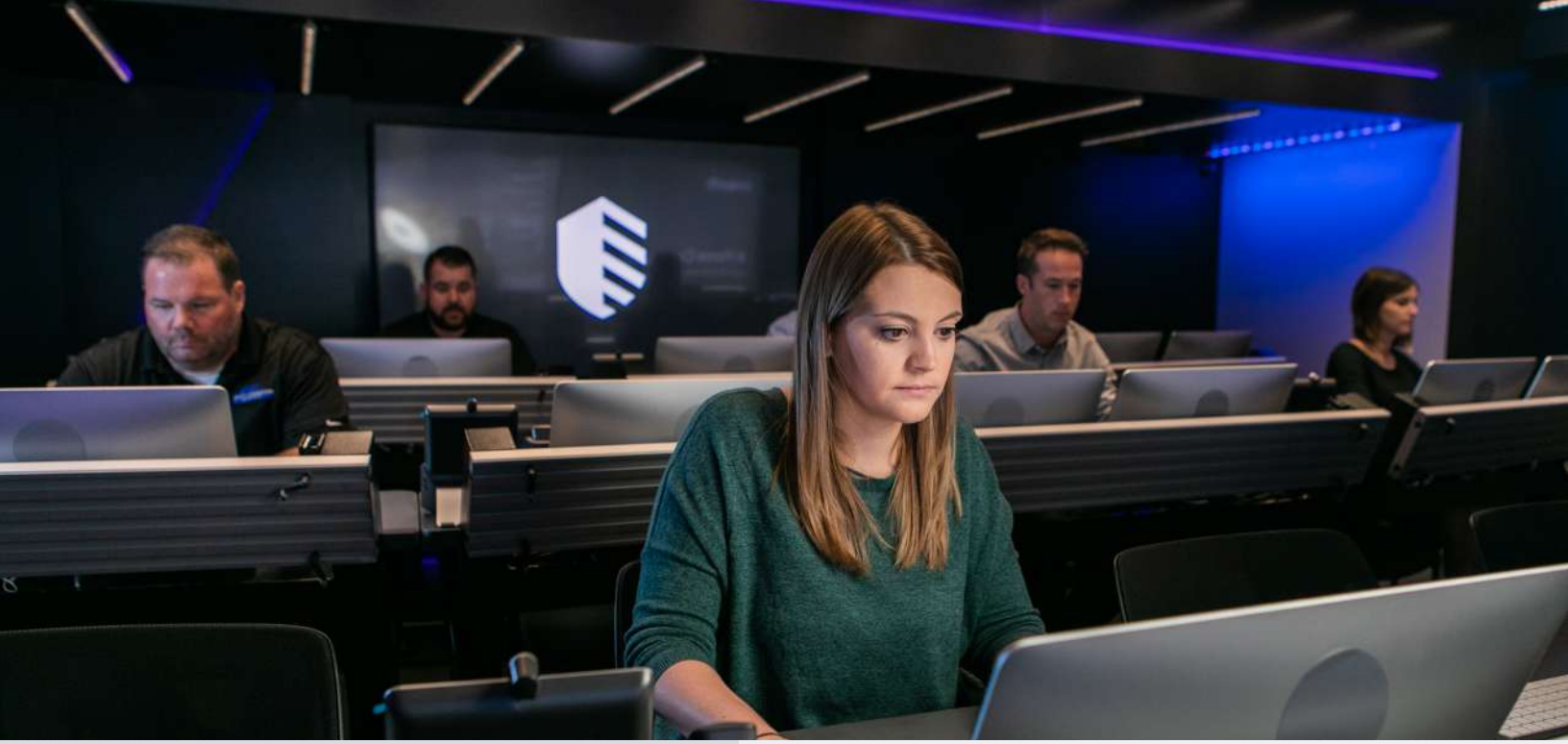
SIEMs são apenas para grandes empresas com equipes de segurança avançadas.

A sabedoria convencional diz que, já que as melhores soluções SIEM do mercado podem ser dimensionadas para dar suporte às maiores organizações, elas foram criadas apenas para as grandes organizações.

Verdade

As melhores soluções SIEM abordam uma ampla variedade de organizações, independentemente de se tratar de uma empresa que ainda está crescendo e dando os primeiros passos no monitoramento de segurança ou uma corporação global da lista Fortune 20 que precisa de casos de uso avançados.

A verdade é que, embora muitas equipes de segurança avançada prefiram ter todos os recursos imagináveis disponíveis para dar suporte a casos de uso avançados e especiais, um bom SIEM não precisa de tudo isso para entregar valor. Uma solução ideal ajuda você a começar com casos de uso padrão, como detecção de ameaças, monitoramento de nuvem e relatório de compliance — assim que você compra o produto.
Conforme sua prática amadurece e seu negócio se desenvolve, seu SIEM deve ser dimensionado para dar suporte a mais ambientes, a múltiplas geografias e a casos de uso avançados, como inspeção profunda de pacotes, análise de dados DNS e orquestração de resposta a incidentes firmemente integradas.



Mito nº 03

SIEMs exigem uma grande quantidade de dados e o custo de coletar todos esses dados é extremamente alto.

Como alguns fornecedores no mercado são conhecidos por se tornarem exorbitantemente caros muito rapidamente, algumas equipes de segurança pressupõem que todos os SIEMs também são assim.

Verdade

Se você estiver considerando fornecedores que cobram com base na quantidade de dados armazenados, poderá ficar muito caro, muito rapidamente. Mas fornecedores diferentes colocam preços em suas soluções de forma diferente.

Antes de se comprometer com qualquer coisa, pense nos problemas que você está tentando solucionar: Você é um varejista com dados de cartões de crédito que precisam ser protegidos? Sua empresa está migrando para a Amazon Web Services e você precisa de visibilidade desse novo ambiente? Os dados coletados para fins de segurança devem ajudar você a abordar seus casos de uso exclusivos. Não caia na armadilha de analisar tudo se você não precisa fazer isso. Dito isso, se você também tiver requisitos de retenção de dados, graças a regulamentações ou políticas organizacionais, seu fornecedor de SIEM deverá ser capaz de fornecer uma opção de baixo custo apenas para armazenamento, pesquisa e relatório. Ao analisar apenas o que é importante para sua organização única e enviar o resto dos seus dados de registros e eventos para um armazenamento de baixo custo, você pode assumir um projeto de SIEM sem consumir todo o seu orçamento.

Mito nº 04

Você precisa de uma equipe de cientistas de dados dedicada em período integral para tornar o SIEM eficaz.

Com frequência, as pessoas dizem que, para o SIEM ser eficaz, é necessário um cientista de dados em período integral ou, ainda, uma equipe deles para desenvolver todas as regras e a análise de dados do zero.

Verdade

Se você não quiser (ou não desejar) encontrar e pagar uma equipe de cientistas de dados que por acaso também entendam de segurança, procure um fornecedor que ofereça esse conteúdo predefinido para uso imediato.

Alguns fornecedores acreditam que, como a solução provavelmente será personalizada, porque não começar com uma tela em branco? Na prática, as equipes de segurança da atualidade simplesmente não têm os recursos disponíveis para assumir um projeto tão gigantesco e que exige tantas habilidades especializadas. Para utilizar qualquer solução SIEM, é necessário alimentá-la com informações sobre sua rede, mas, depois de concluir essa etapa, você deve conseguir aproveitar as vantagens das regras, análise de dados e políticas de correlação predefinidas para começar a detectar ameaças imediatamente. Você não precisa começar com uma tela em branco. E, se ainda está preocupado, muitos fornecedores de SIEM fazem parcerias comprovedores de serviços de segurança gerenciados (MSSPs) para que você possa obter todos os benefícios de um SIEM avançado, com o benefício adicional de ter uma ajuda extra de especialistas em operações de segurança.

Mito nº 05

SIEMs são difíceis de integrar com outras soluções no meu ambiente.

Os SIEMs têm uma reputação de serem difíceis de integrar com outras soluções, embora dependam de dados de outras soluções para fornecer valor.

Verdade

As grandes soluções SIEM precisam ser fáceis de integrar — e, felizmente, muitas são.

Os primeiros SIEMs, que chegaram ao mercado há uma década e não conseguiram evoluir com as necessidades em constante mudança e a tecnologia em evolução são sim difíceis de integrar. No entanto, essas soluções ficaram obsoletas ou estão tendo dificuldades significativas atualmente. As grandes soluções da atualidade oferecem centenas de integrações prontas para usar com tecnologias de TO e de TI comerciais, e oferecem conectores simples para integração e logs de análise de aplicações personalizadas. Se estiver curioso sobre as integrações que existem com suporte total de fornecedores, confira os sites de atendimento ao cliente de diferentes fornecedores ou procure seus intercâmbios de aplicações.

Conclusão

Os estereótipos que existem atualmente tendem a ser baseados em tecnologia desatualizada. Se você avaliasse uma solução SIEM de dez anos atrás — ou até mesmo de cinco anos atrás — muitos desses mitos seriam verdadeiros. Mas, na mesma medida em que as paisagens de ameaças e de tecnologia evoluíram, os SIEMs fizeram o mesmo.

Caso esteja com dificuldades para detectar ameaças ou compreender os logs do seu gerenciador de logs, hoje pode ser o dia perfeito para dar outra olhada em soluções SIEM e descobrir por si mesmo o quanto mudaram.

Sobre o IBM QRadar

O IBM QRadar Security Intelligence Platform é uma solução flexível que oferece visibilidade centralizada de dados de segurança que abrangem toda a empresa, além de oferecer insights acionáveis das ameaças de mais alta prioridade.

A solução é baseada no QRadar SIEM, que inclui centenas de regras e análise de dados configuradas eletronicamente, além de inteligência de ameaças. IBM X-Force. Com mais de 500 integrações prontas para usar e mais de 160 aplicações, os clientes podem adicionar de forma fácil e rápida novos casos de uso de segurança e compliance. Recursos opcionais como componentes totalmente integrados para armazenamento de logs, análise de dados de comportamento de usuários, inspeção de pacotes de rede, gestão de vulnerabilidades e investigações de ameaças com tecnologia de IA podem facilmente ser adicionados e gerenciados em uma única interface, permitindo que os clientes comecem com uma combinação do tamanho que desejarem e possam ampliar ou reduzir a escala conforme a mudança de suas necessidades.

Saiba mais em: IBM QRadar