IBM Security

QRadar: detectando ameaças conforme os negócios crescem

IBM

O QRadar é preparado para crescer conforme seus negócios crescem

Qual dos cenários abaixo descreve melhor seus negócios?

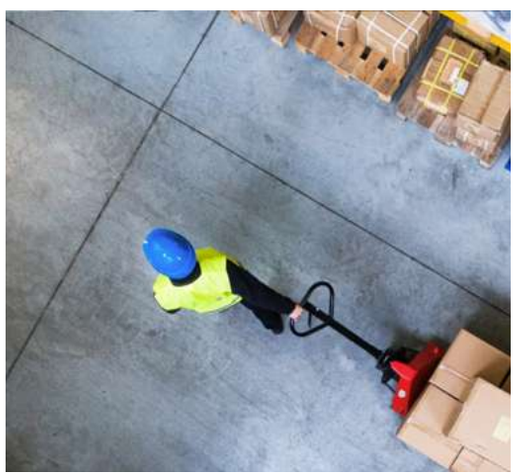
O IBM QRadar capacita você a vencer os desafios de segurança mais importantes, independentemente do tamanho dos seus negócios. Escolha um tamanho de negócio correspondente ao seu para descobrir como o IBM QRadar pode ajudar seus negócios.

O pequeno negócio guerreiro →

Somos um pequeno negócio considerável, no entanto, a segurança não é uma grande prioridadeporque temos uma equipe de TI limitada ou inexistente para configurar a infraestrutura de segurança.

O médio porte pronto para expandir →

Somos uma empresa de porte médio com uma equipe dedicada a operações de segurança, mas nossas configurações de segurança não são personalizadas para os nossos negócios.



A empresa estabelecida →

Temos uma equipe de operações de segurança avançada estabelecida, mas nosso programa de segurança é muito complexo e fica desatualizado rapidamente.

O pequeno negócio guerreiro

Pequeno negócio não significa pequena necessidade de segurança.

43%

das violações de 2019 envolveram os pequenos negócios como vítimas [1]

62%

dos ciberataques são direcionados a pequenos negócios [2]

60%

dos pequenos negócios encerram as atividades seis meses após uma violação [3]

Não deixe que o mundo desconhecido da segurança impeça você de avançar seus negócios. O IBM QRadar pode ajudar.

“ Quero configurar os protocolos de ideais de segurança que ajudarão a proteger meus clientes e meus negócios em crescimento."

O esforço é real para pequenos negócios

Os novos regulamentos exigem ações de monitoramento, de detecção e de relatório de segurança, mas em uma organização pequena com uma equipe de TI limitada, essas ações são difíceis de serem gerenciadas. Não caia na conversa de que um SIEM não consegue ajudar a facilitaressas ações.

5 perguntas a serem respondidas antes de fazer upgrade para um SIEM moderno →

- Os novos regulamentos exigem ações de monitoramento, de detecção e de relatório de segurança
- Aumento da pressão dos clientes tentando gerenciar o risco de terceiros; o monitoramento proativo de segurança está se tornando um requisito para manter e aumentar os negócios
- Equipe de segurança de TI qualificada e limitada (caso haja alguma)

Você precisa ter uma visibilidade clara da segurança

Conforme seu pequeno negócio cresce, você precisa continuar a monitorar os ativos críticos de acordo com o aumento dos regulamentos. Sim, um SIEM pode aumentar a escala para o nível corporativo, mas ele também pode oferecer a visibilidade necessária dos negócios, independentemente do tamanho.

5 perguntas a serem respondidas antes de fazer upgrade para um SIEM moderno →

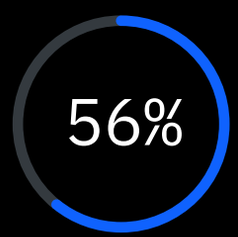
O QRadar pode ser dimensionado de acordo com os negócios

Aproveitando a eficiência de um SIEM nos negócios, o QRadar pode ajudar a solucionar os casos de uso de segurança mais exigentes, sem exigir ações de customização significativas.

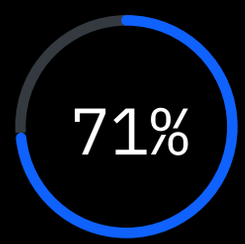
5 perguntas a serem respondidas antes de fazer upgrade para um SIEM moderno →

O médio porte pronto para expandir

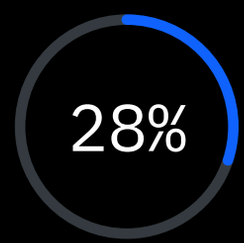
A necessidade de aumento da visibilidade



das violações de 2019 levaram meses ou mais tempo para serem descobertas [1]



das violações de 2019 tiveram motivação financeira negócios [1]



das violações de 2019 envolveram o uso de credenciais roubadas [1]

Assegure-se de que o programa de operações de segurança seja customizado de acordo com seus negócios e suas prioridades.

“ Precisamos que nossa equipe de segurança seja capaz de priorizar atividades, manter a conformidade e ganhar eficiência na solução das dificuldades."

Ofereça mais capacidade de segurança à sua equipe limitada

Embora você tenha uma equipe dedicada a operações de segurança, os alertas contínuos de diferentes detecções de ameaças, que nem sempre são relevantes para os negócios, podem reduzir a capacidade da equipe.

Faça upgrade para um SIEM inteligente →

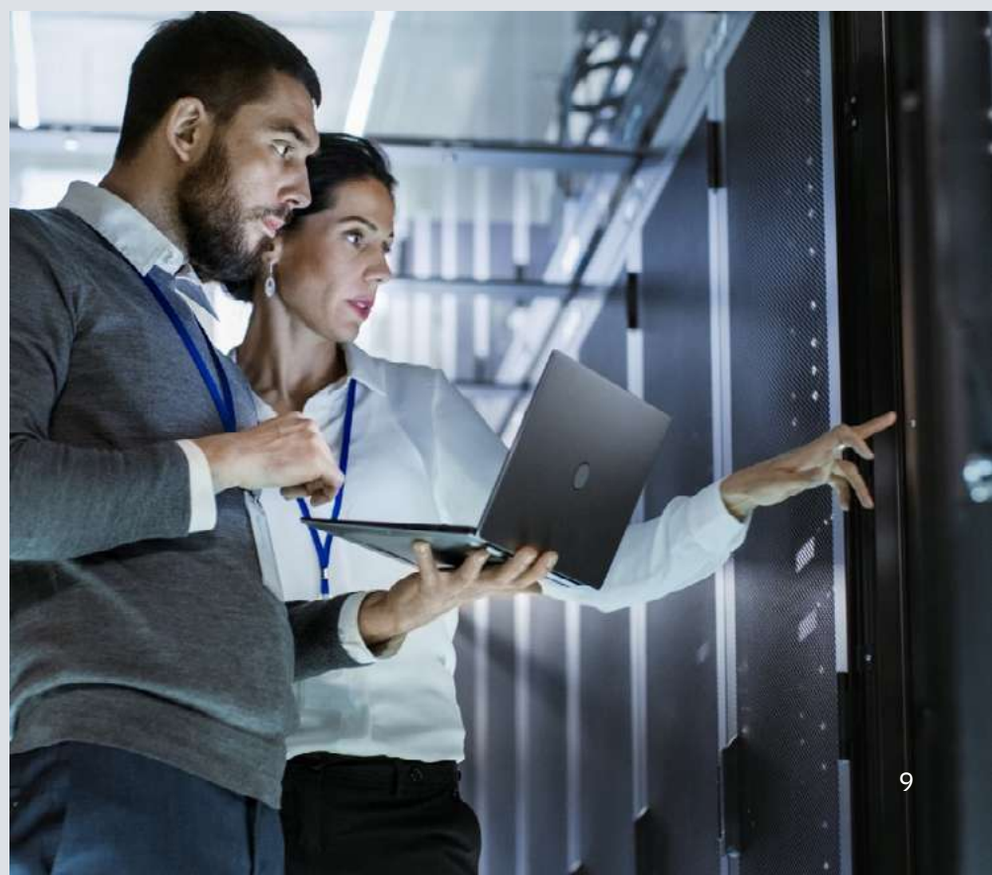
- Necessidade de casos de uso de detecção de ameaça customizáveis e simples de instalar, customizados de acordo com os negócios
- Necessidade de solucionar e relatar questões sobre a conformidade
- Contar com uma pequena equipe de segurança dedicada que exija automação e casos de uso para gerenciar as operações de segurança de maneira efetiva
- Equipe de segurança de TI qualificada limitada (caso haja alguma)

Obtenha insights acionáveis sobre as ameaças

Você precisa de ferramentas que possam oferecer visibilidade do que está acontecendo na rede e ativar a equipe quando necessário. Conforme a equipe cresce, é necessário buscar a automação para ajudá-la a gerenciar as operações de segurança de maneira efetiva.

Faça upgrade para um SIEM inteligente →

- Necessidade de casos de uso de detecção de ameaça customizáveis e simples de instalar, customizados de acordo com os negócios
- Necessidade de solucionar e relatar questões sobre a conformidade
- Contar com uma pequena equipe de segurança dedicada que exija automação e casos de uso para gerenciar as operações de segurança de maneira efetiva
- Equipe de segurança de TI qualificada limitada (caso haja alguma)



Aumente o potencial de sua equipe reduzida

O IBM QRadar ajuda a detectar ameaças conhecidas e desconhecidas, oferece mais que alertas individuais para identificar e priorizar incidentes potenciais e aplica a inteligência artificial para acelerar processos de investigação em até 50%.

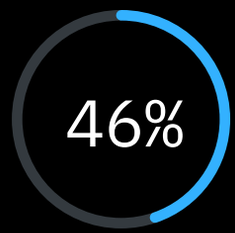
Faça upgrade para um SIEM inteligente →

- Descobre automaticamente tipos de origem de log e inclui mais de 450 integrações para analisar automaticamente e normaliza logs no ambiente
- Inclui mais de 1.600 regras pré-desenvolvidas e algoritmos de detecção de anomalias prontas para uso para gerenciar casos de uso comuns rapidamente
- Correlação em tempo real para detectar ameaças conforme acontecem, conectar automaticamente atividades de ameaça relacionadas e priorizar alertas baseados em criticidade

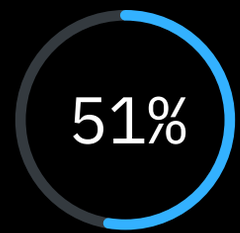
A empresa estabelecida

“ Estamos sempre em busca de possíveis ameaças direcionadas aos nossos negócios e precisamos estar preparados para reagir rapidamente."

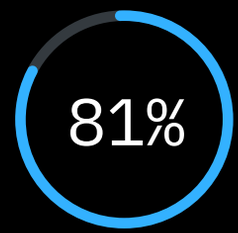
Temos dados suficientes, mas não insights



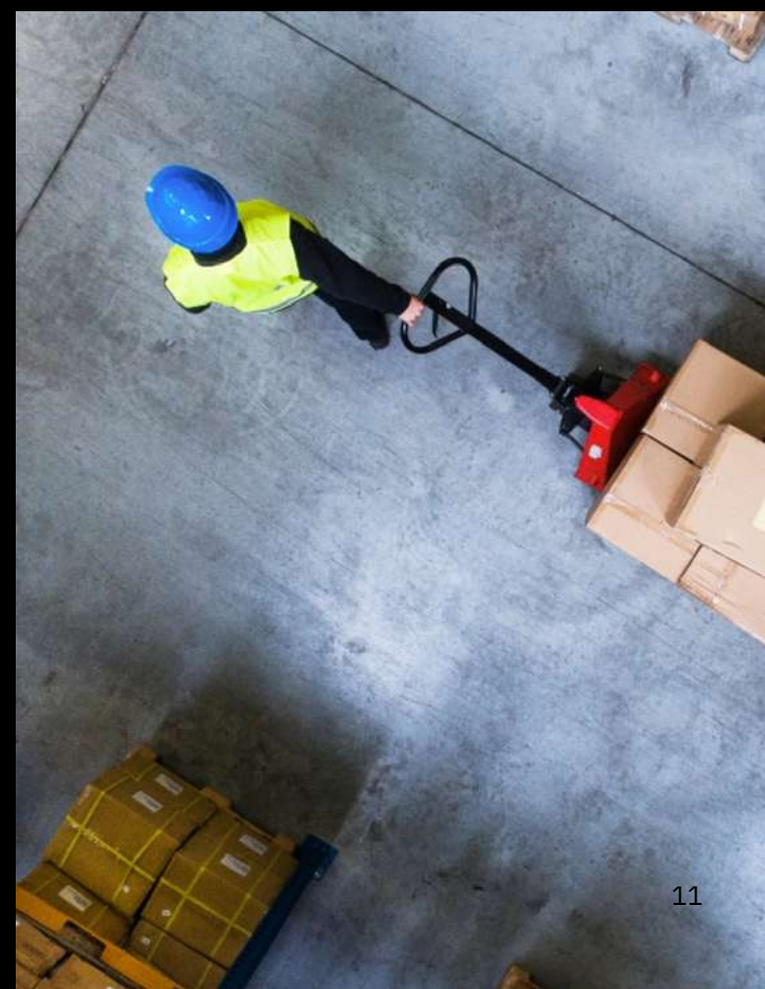
dos alertas de detecção de ameaça não são investigados [4]



dos alertas de ameaça legítimos que podem afetar os negócios não são corrigidos [4]



dos CISOs preocupam-se com a falta de resolução de possíveis violações [5]



Combine automação e o conhecimento do setor para solucionar a complexidade e a escala da segurança.

Colocando as ferramentas certas a serviço da equipe

Mesmo com uma grande equipe de segurança, a investigação e a descoberta dos eventos de segurança certos podem ser um desafio. Você precisa de uma plataforma que possa oferecer à equipe os insights de que ela precisa para priorizar quais ações devem ser tomadas e quando.

Automatize seu SOC com IA →

- No momento, usando uma solução de SIEM provavelmente desatualizada e complexa
- Os custos de gerenciamento contínuo são altos e a complexidade integrada dificulta o ajuste e a customização
- Necessidade de solucionar os casos de uso relacionados à nuvem, mas dificuldade de visualizar, monitorar e analisar dados de multinuvem híbrida
- Necessidade de insights antecipados sobre ameaças avançadas, sorrateiras e desconhecidas

A escabilidade e a flexibilidade devem ser fatores obrigatórios

Você precisa de uma solução que seja dimensionada facilmente para dar suporte a vários ambientes sem exigir uma sobrecarga adicional. Enquanto isso, sua equipe precisa de uma plataforma flexível que possa dar suporte a uma ampla variedade de casos de uso.

Automatize seu SOC com IA →

Enfrentando os alertas de segurança em escala

O QRadar ajuda a dimensionar a segurança por meio da correlação automática de milhões de pontos de dados para identificar uma lista gerenciável de alertas priorizados, devolvendo o poder às equipes para que elas tomem as decisões certas.

Automatize seu SOC com IA →

- Coleta, analisa e correlaciona uma variedade de dados, incluindo logs de terminal, dados de ativos, fluxos de rede, atividades de usuários, informações de vulnerabilidade e inteligência de ameaças
- IA para fornecer insights automatizados mais aprofundados sobre as ameaças ativas, entender melhor os relacionamentos entre as ameaças e saber como os analistas geralmente respondem a determinados tipos de ameaças para ajudar a orientar processos de resposta mais precisos e consistentes
- Melhora a precisão da detecção de ameaça em 51% e gera 50% a menos de falsos positivos do que os SIEMs concorrentes

Para obter mais informação sobre IBM Security, visite o nosso site:

Visite o nosso site →

Dê o próximo passo
Entre em contato com nosso especialista que o ajudará a superar os desafios de segurança cibernética.

Fale com um especialista →

Fontes

1. Verizon, Relatório de investigações sobre violação de dados de 2019, maio de 2019
2. Inc, 60 por cento dos pequenos negócios fecham após seis meses de um ciberataque, Joe Galvin, Maio de 2018
3. Seattle Times, O interesse em seguro cibernético aumenta à medida que os hackers focam em pequenos negócios, Marissa Lang, setembro de 2017
4. Cisco, Relatório de segurança cibernética da Cisco de 2018: edição especial SMB, julho de 2018
5. ServiceNow, O estudo global de CISO, 2019

IBM