



Plataforma de Inteligência em Segurança IBM QRadar

Fornecendo inteligência proativa para segurança e conformidade corporativas

Destaques

- Integre security information and event management (SIEM), gerenciamento de logs, detecção de anomalias e configuração e gerenciamento de vulnerabilidades em uma solução unificada
- Utilize uma única arquitetura para analisar dados de log, fluxo, vulnerabilidade, usuários e ativos
- Use correlação em tempo real e detecção de anomalias comportamentais para identificar ameaças avançadas
- Identifique incidentes de alta prioridade entre bilhões de pontos de dados
- Tenha uma visão de 360° da rede, dos aplicativos e da atividade do usuário
- Automatize a conformidade regulamentar com coleta, correlação e relatórios

A Plataforma de Inteligência em Segurança IBM® QRadar® integra SIEM, gerenciamento de logs, detecção de anomalias e configuração e gerenciamento de vulnerabilidades em uma solução unificada. Ao usar inteligência, integração e automação para oferecer insight de segurança de 360°, esta solução fornece a melhor detecção de ameaças, maior facilidade de uso e menor custo total de propriedade.

Entregando inteligência, integração e automação

A Plataforma de Inteligência em Segurança QRadar proporciona benefícios de segurança e conformidade que são inestimáveis no mundo atual, no qual empresas instrumentadas, interconectadas e inteligentes coletam, processam, usam e armazenam mais informações do que nunca.

Detecte ameaças que poderiam passar despercebidas

As organizações de hoje estão expostas a um maior volume e variedade de ataques do que antigamente. Criminosos avançados são inteligentes e pacientes e deixam apenas singelos sinais de sua presença. A Plataforma de Inteligência em Segurança QRadar é uma família integrada de produtos que ajuda a detectar ameaças e nos defende contra elas, através da aplicação de analítica sofisticada a vários tipos de dados. Ao fazer isso, a plataforma identifica incidentes de alta prioridade que poderiam passar despercebidos em meio ao todo.





A IBM QRadar Security Intelligence Platform entrega inteligência em segurança de 360°.

Consolide silos de dados

Embora haja muitas informações em logs, flows de rede e dados de negócios dentro das organizações, essas informações são frequentemente mantidas em silos e ignoradas ou subutilizadas. O QRadar reúne visualizações de rede, segurança e operações em uma solução unificada e flexível. Esta plataforma quebra as separações entre os silos através do correlacionamento de logs com flows de rede e diversos outros dados, apresentando todas as informações relevantes em uma única tela. Isso permite detectar melhor as ameaças e visualizar muito mais ampla das atividades corporativas.

Detecte fraude interna

Algumas das mais graves ameaças a uma organização vêm do seu interior, mas para muitas organizações falta a inteligência necessária para detectar funcionários maliciosos ou pessoas de fora que possuem contas de usuário comprometidas.

Ao combinar monitoramento de usuários e de aplicativos com visibilidade de rede na camada de aplicativo, as organizações podem detectar melhor anomalias em relação à atividade normal, podendo interromper um ataque antes de sua conclusão.

Previna e solucione riscos com o gerenciamento de vulnerabilidades

Para gerenciar melhor o risco, as equipes de segurança, rede e infraestrutura identificam vulnerabilidades e priorizam a remediação antes que ocorra uma violação. A Plataforma de Inteligência em Segurança QRadar integra gerenciamento de configuração e vulnerabilidade com recursos de SIEM, incluindo correlação e análise de flows de rede, para oferecer um melhor insight sobre vulnerabilidades críticas. Em resultado disso, as organizações podem remediar riscos de forma mais eficiente e eficaz.

Atender a requerimentos de conformidade regulatória

Muitas organizações têm dificuldade em passar por auditorias de conformidade e, ao mesmo tempo, realizar coleta de dados, monitoramento e relatórios com recursos cada vez mais limitados. Para automatizar e simplificar as tarefas de conformidade, o QRadar oferece coleta, correlação e relatórios sobre atividades relacionadas a conformidade, com base em vários modelos de relatórios prontos para uso.

Usfruindo de recursos analíticos de segurança fáceis de utilizar

A Plataforma de Inteligência em Segurança QRadar é uma arquitetura unificada para armazenar, correlacionar e consultar dados de log, flows de rede, vulnerabilidade, usuários e ativos, e para criar relatórios sobre eles. A plataforma combina recursos analíticos sofisticados com regras, relatórios e painéis prontos para uso. Embora ela seja eficiente e escalável o suficiente para empresas Fortune 500 e grandes agências do governo, ela também é intuitiva e flexível o suficiente para organizações de pequeno e médio porte. Os usuários contam com retorno mais rápido, menor custo de propriedade, maior agilidade e maior proteção contra riscos de segurança e conformidade.

Inteligência

Ao analisar mais tipos de dados e usar mais técnicas analíticas, o QRadar pode muitas vezes detectar ameaças que outras soluções não detectariam e proporciona visibilidade da rede que outros não conseguiriam.

Integração

Com uma plataforma de aplicativo, banco de dados e interface com o usuário comuns, esta plataforma oferece uma escala massiva de gerenciamento de log sem comprometer a inteligência em tempo real do SIEM e a análise comportamental da rede. A plataforma oferece uma solução comum para todas as funções de pesquisa, correlação, detecção de anomalia e relatórios.

Uma única interface intuitiva com o usuário dá acesso a todas as funções de gerenciamento de log, análise de flows de rede, gerenciamento de incidentes, gerenciamento de configuração e vulnerabilidade, painel e relatórios.

Automação

A Plataforma de Inteligência em Segurança QRadar é simples de implementar e gerenciar e oferece vários módulos de integração e conteúdo de inteligência em segurança prontos para uso. Ao automatizar a descoberta de ativos, a normalização de dados, as funções de ajuste fino e ao mesmo tempo oferecer regras e relatórios prontos para uso, a solução pode reduzir drasticamente a complexidade que muito atrapalha outros produtos.

Por que a IBM?

A IBM opera a maior organização de pesquisa, desenvolvimento e entrega de soluções de segurança do mundo. Isso inclui 10 centros de operações de segurança, nove centros de Pesquisa IBM, 11 laboratórios de desenvolvimento de segurança de software e um Instituto de Segurança Avançada, com escritórios nos Estados Unidos, Europa e Ásia-Pacífico. Com as soluções IBM, as organizações podem reduzir suas vulnerabilidades de segurança e concentrar-se no sucesso de suas iniciativas estratégicas. Essas soluções baseiam-se no conhecimento sobre inteligência de ameaças da equipe de pesquisa e desenvolvimento IBM X-Force® para fornecer uma abordagem preventiva. Como parceiro confiável em segurança, a IBM entrega as soluções para manter toda a infraestrutura corporativa (incluindo a nuvem) protegida contra riscos de segurança.

Para mais informações

Para saber mais sobre a Plataforma de Inteligência em Segurança IBM QRadar, entre em contato com o seu representante da IBM ou Parceiro Comercial IBM, ou visite: ibm.com/security



© Copyright IBM Corporation 2013

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América
Janeiro de 2013

IBM, o logotipo IBM, ibm.com, QRadar e X-Force são marcas registradas da International Business Machines Corp., registradas em muitas jurisdições em todo o mundo. Outros nomes de produtos e serviços podem ser marcas registradas da IBM ou de outras empresas. Uma lista atual das marcas registradas da IBM está disponível na Web sob “Copyright and trademark information” em ibm.com/legal/copytrade.shtml

Este documento entra em vigor a partir da data inicial de publicação e pode ser alterado pela IBM a qualquer momento. Nem todas as ofertas estão disponíveis em todos os países nos quais a IBM opera. AS INFORMAÇÕES NESTE DOCUMENTO SÃO FORNECIDAS "COMO ESTÃO" SEM QUALQUER GARANTIA, EXPRESSA OU IMPLÍCITA, INCLUINDO GARANTIAS DE COMERCIALIZAÇÃO, ADEQUAÇÃO PARA UM PROPÓSITO PARTICULAR E QUALQUER GARANTIA OU CONDIÇÃO DE NÃO VIOLAÇÃO. Os produtos IBM são garantidos de acordo com os termos e condições dos contratos sob os quais são fornecidos.

O cliente é responsável por cumprir as leis e regulamentos que se aplicam. A IBM não oferece orientações jurídicas e não declara ou garante que seus serviços ou produtos assegurarão que o cliente esteja em conformidade com qualquer lei.

A segurança de sistemas de TI significa proteger sistemas e informações através da prevenção, detecção e resposta ao acesso impróprio de dentro ou de fora da empresa. Em caso de acesso impróprio, as informações podem ser alteradas, destruídas ou furtadas, ou pode haver danos ou má utilização do sistema, incluindo ataques a outros. Nenhum sistema ou produto de TI deve ser considerado completamente seguro e nenhum produto ou medida de segurança pode ser completamente eficiente na prevenção de acessos impróprios. Os sistemas e produtos IBM destinam-se a fazer parte de uma abordagem abrangente de segurança, que envolve necessariamente outros procedimentos operacionais e pode exigir outros sistemas, produtos ou serviços para ser efetiva. A IBM não garante que sistemas e produtos estejam imunes contra conduta maliciosa ou ilegal de outros.



Recycle
