Simplificando a migração do SIEM

IBM Security

IBM

Sumário

Introdução

Você sabe que seus dados estão em risco em todos os lugares: localmente e na nuvem. E, se sua equipe é como 70% dos Security Operation Centers (SOCs), talvez você conte com um software de Security Information and Event Management (SIEM) para detectar e analisar ameaças.1 Considerando o panorama de ameaças, os novos ambientes e as fontes de dados em constante evolução, é essencial que sua solução de SIEM possa fazer o monitoramento perfeito de toda a infraestrutura de sua organização, mesmo à medida que sua empresa cresce.

Se você está lendo este ebook, provavelmente está pensando em migrar para uma solução de SIEM de última geração e sabe que essa não será uma tarefa simples. Uma migração de sucesso para uma solução de SIEM começa com a escolha do provedor de serviços de TI ideal, que possa oferecer a você uma sólida experiência de migração.

A plataforma IBM Security™ QRadar® é uma solução abrangente de SIEM que pode ajudar você a detectar e priorizar rapidamente as possíveis ameaças à sua empresa. O time de especialistas da IBM Security já ajudou muitas empresas a migrarem suas soluções tradicionais de SIEM. A IBM tem a experiência, as habilidades, a tecnologia e os recursos para proporcionar uma jornada estável de migração.

Em média, as empresas levam

279 dias

para detectar e conter uma violação de dados.[2]

Benefícios da atualização para uma plataforma de SIEM de última geração

Por que escolher o QRadar?

Lê enormes volumes de dados de fontes locais e na nuvem

Oferece ampla visibilidade e análise de fluxo do tráfego de rede e dos metadados

Inclui acesso ao IBM Security X-Force® Threat Intelligence sem custo adicional

Aplica análise integrada para detectar ameaças com precisão

Proporciona investigações auxiliadas por inteligência artificial (IA) e priorização de incidentes

Promove um ecossistema, oferecendo mais de 500 integrações simples de instalar

Permite a implementação no local ou na nuvem utilizando uma arquitetura flexível

Correlaciona atividades relacionadas para priorizar incidentes

Oferece integração da estrutura MITRE ATT&CK para processos de detecção de ameaças, investigação e resposta

Inclui modelos comportamentais abertos e personalizáveis para criar perfis de usuários e ativos

Elimina as tarefas manuais analisando dados automaticamente e normalizando registros

Oferece visibilidade abrangente e centralizada

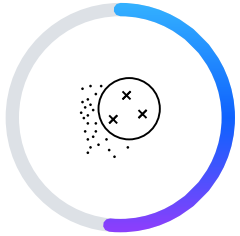
A plataforma QRadar oferece uma solução de SIEM de última geração para monitorar e detectar ameaças de aplicações, usuários, contêineres, endpoints, redes e ambientes de nuvem em tempo real.

A plataforma QRadar SIEM foi projetada para proporcionar visibilidade centralizada às equipes de segurança, para que elas identifiquem ameaças e irregularidades logo ao início do ciclo de vida dos ataques. À medida que os dados são lidos, a solução aplica análises e inteligência de segurança em tempo real para detectar e priorizar ameaças com rapidez e precisão. A equipe de seu SOC terá uma visão centralizada dos registros, fluxos e eventos dos ambientes locais, de software como serviço (SaaS) e de infraestrutura como serviço (IaaS).

"Usar o IBM QRadar SIEM é como ter olhos na nuca. Antes, parecia que estávamos sempre atrasados em termos de segurança. Mas, agora, estamos muito mais proativos".

Michael Warrer
Diretor de informações da NRGi

Leia o estudo de caso →



O QRadar aumenta a capacidade de detectar ataques reais com precisão em

51%[3]

Proporciona análise integrada para detectar ameaças com precisão

A solução QRadar analisa os dados de ameaças para detectar, com precisão, as ameaças conhecidas e desconhecidas não detectadas pelas outras empresas. A análise integrada ajuda a reduzir o tempo para a conquista de valor, sem exigir conhecimentos em ciência de dados.

O QRadar foi projetado para correlacionar atividades em toda a rede e aplicar vários métodos de detecção baseados em assinaturas e comportamentos para identificar ameaças conhecidas e desconhecidas.

As décadas de experiência em SIEM da equipe IBM Security foram integradas diretamente ao QRadar por meio de uma ampla biblioteca de regras baseadas em assinatura e habilmente criadas. A solução usa modelagem comportamental para definir uma linha de base para as atividades dos usuários, ativada por meio de integrações ao Lightweight Directory Access Protocol (LDAP) ou ao Microsoft Active Directory.

O QRadar pode detectar irregularidades comportamentais e comportamentos arriscados que indicam credenciais comprometidas, atividades internas maliciosas ou que uma conta de usuário foi controlada por malware. Os analistas de segurança podem identificar rapidamente os usuários com pontuações elevadas de risco e criar listas de observação priorizadas para usuários, contas de máquina ou executivos privilegiados. O QRadar permite que as equipes do SOC aprimorem rapidamente os programas de ameaças internas com modelos personalizados de detecção comportamental por meio de um criador integrado de modelos de aprendizado de máquina (ML).

Solução IBM Security QRadar SIEM

- Correlação e detecção de irregularidades comportamentais em tempo real
- Inteligência de ameaças e insights sobre vulnerabilidades
- Aprendizado de máquina e criação de perfis de serviços e usuários

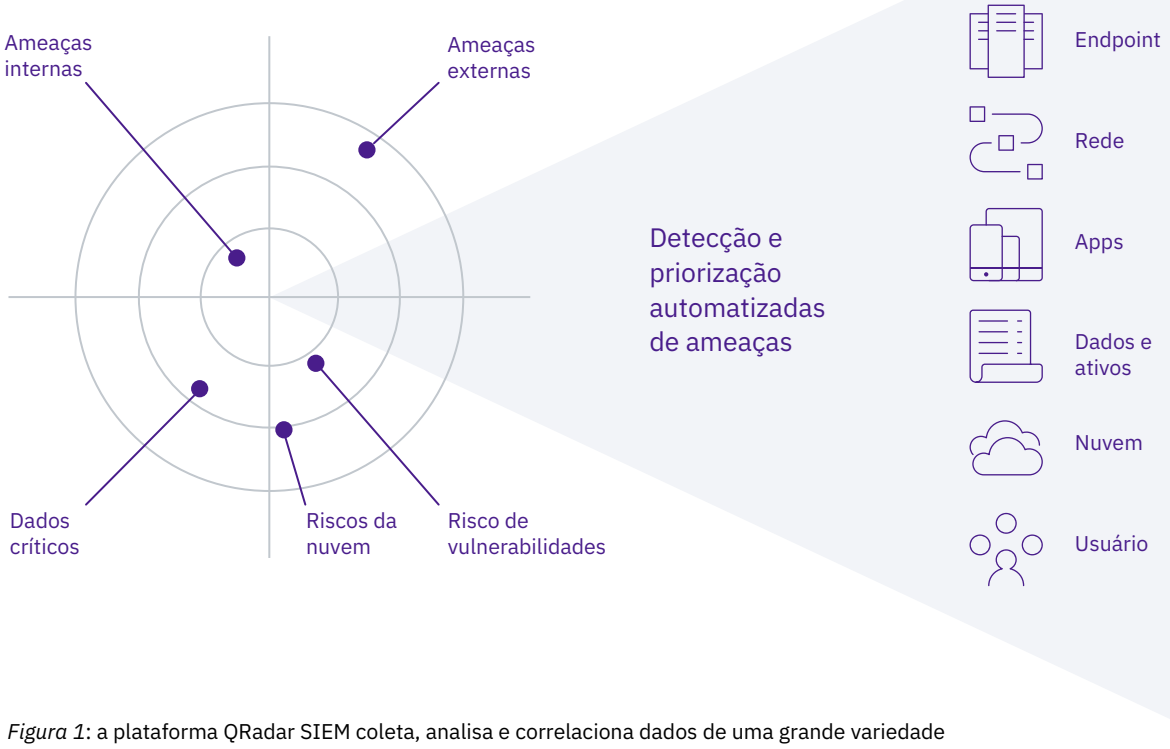


Figura 1: a plataforma QRadar SIEM coleta, analisa e correlaciona dados de uma grande variedade de fontes para detectar e priorizar as ameaças mais críticas que exigem investigação

Proporciona análise integrada para detectar ameaças com precisão

Continuação

Além disso, o QRadar usa análise avançada de rede para detectar alterações no tráfego da rede, como o surgimento de um novo host ou de comunicações anormais entre hosts existentes. A análise de rede oferece à equipe de analistas de segurança uma compreensão mais detalhada do sistema, das aplicações e do tráfego da rede. O QRadar pode detectar o tráfego de leste a oeste que pode indicar movimentos laterais, identificar ameaças avançadas à medida que elas passam pela rede e localizar tentativas de exfiltração de dados confidenciais. A telemetria de rede adicional coletada reduz os falsos positivos e auxilia o responsável pela resposta a incidentes e os caçadores de ameaças, que podem identificar rapidamente os hosts afetados para iniciar a correção.

O mecanismo de analítica da plataforma QRadar inclui encadeamento de violações, que vincula os alertas relacionados em uma só violação consolidada. O encadeamento de violações oferece menos alertas, mas com maior fidelidade, e reduz os falsos positivos, permitindo que a equipe de analistas faça triagens com confiança. Já que todas as informações ficam disponíveis em uma tela, é mais fácil para o usuário ter uma visão geral de atividades suspeitas relacionadas que foram detectadas. À medida que novos eventos acontecem, a aplicação IBM QRadar Advisor with WatsonTM ajuda a priorizar as violações e é atualizada automaticamente com novos dados.

.

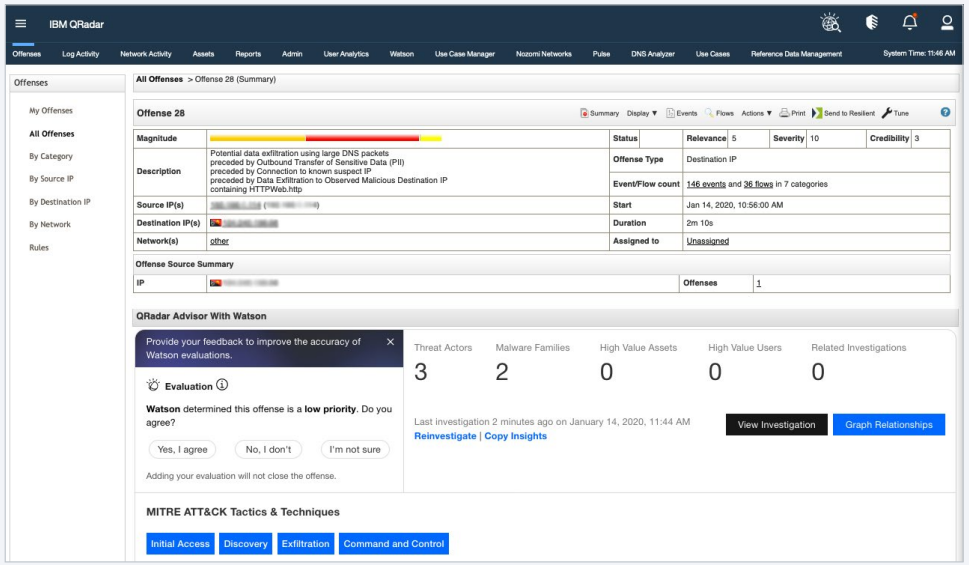


Figura 2: regras personalizadas e violações

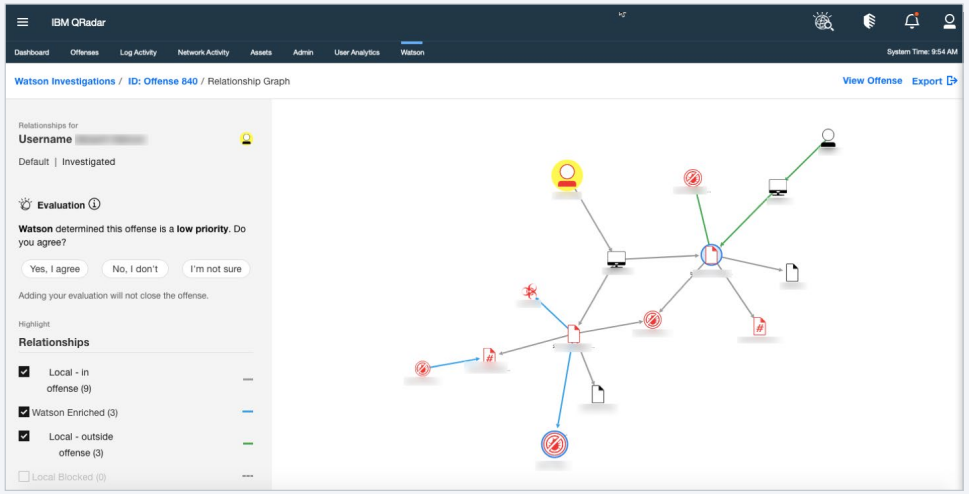


Figura 3: um exemplo de investigação do QRadar Advisor with Watson

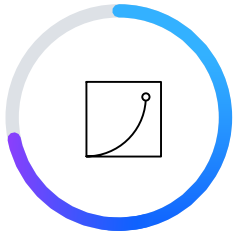
Oferece sólidos recursos simples de instalar

A solução QRadar inclui mais de 500 Device Support Modules (DSMs) pré-integrados que oferecem integrações de configurações padrão às tecnologias comerciais prontas para uso.

Basta que a equipe do SOC aponte registros para o QRadar, e a solução pode detectar automaticamente o tipo de origem do registro e aplicar o DSM correto para analisar e normalizar os dados do registro. Como resultado, sua organização pode começar as atividades muito mais rapidamente que as organizações com soluções alternativas. O QRadar também oferece um DSM Editor com uma interface gráfica do usuário (GUI) intuitiva, projetada para ser fácil de usar e permitir que as equipes de segurança definam facilmente como analisar registros de aplicações personalizadas.

54%

dos entrevistados dizem que é muito fácil inserir registros no QRadar para correlação e análise.[3]



70%

dos entrevistados dizem que as regras de correlação simples de instalar do QRadar são valiosas.[3]

Oferece arquitetura flexível no local ou na nuvem

A solução QRadar SIEM pode ser entregue como hardware, software ou máquinas virtuais (VMs) para ambientes locais ou de IaaS. Comece com uma solução completa ou faça a escalabilidade vertical para um modelo altamente distribuído entre vários segmentos de rede e áreas geográficas.

Além disso, a solução permite a integração a serviços de nuvem, como Amazon Web Services (AWS), Microsoft Azure, SalesForce.com, Office 365 e IBM Cloud™, ajudando os analistas a detectar e responder melhor às ameaças, independentemente de onde elas ocorrerem.

A plataforma QRadar permite a integração a serviços de nuvem, como:

- AWS
- Azure
- SalesForce.com
- Office 365
- IBM Cloud™

Usa a estrutura MITRE ATT&CK

As organizações do mundo todo estão adotando a estrutura MITRE ATT&CK e a utilizam como base para o desenvolvimento de modelos e metodologias específicos de ameaças do setor privado, governamental e de segurança cibernética. MITRE é uma organização sem fins lucrativos que desenvolveu o modelo depois de anos observando como operam os grupos adversários do mundo real.

O software QRadar SIEM permite a integração ao IBM QRadar Advisor with Watson, que mapeia automaticamente as táticas e técnicas da MITRE ATT&CK para enriquecer o incidente, apresentando informações de primeira mão sobre as táticas e fases de um ataque que pode estar sendo utilizado por um invasor. Esse processo reduz significativamente o tempo de investigação, já que os analistas têm uma compreensão imediata das táticas utilizadas pelos invasores. Isso, por sua vez, acelera a resposta e a contenção de ameaças. Os menores tempos de espera também reduzem os custos das violações de segurança.

O IBM QRadar Use Case Manager inclui o Cyber Adversary Framework Mapping Application para substituir os mapeamentos padrão e associar suas regras personalizadas às táticas e técnicas da MITRE ATT&CK. Ao conseguir visualizar a cobertura de ameaças de toda a estrutura MITRE ATT&CK, os analistas de segurança não só podem detectar ameaças com base no comportamento adversário, como também podem identificar proativamente as lacunas e as áreas de cobertura de segurança inadequada, ver mapeamentos predefinidos de táticas e técnicas e adicionar seus próprios mapeamentos personalizados para melhorar a cobertura de segurança.

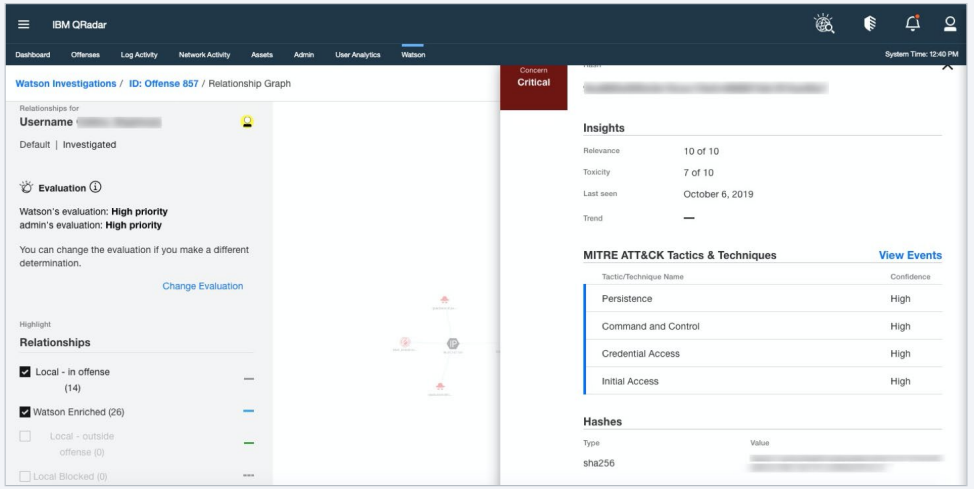


Figura 4: A aplicação QRadar Advisor with Watson mapeia automaticamente as táticas e técnicas da MITRE ATT&CK ao Custom Rules Engine (CRE).

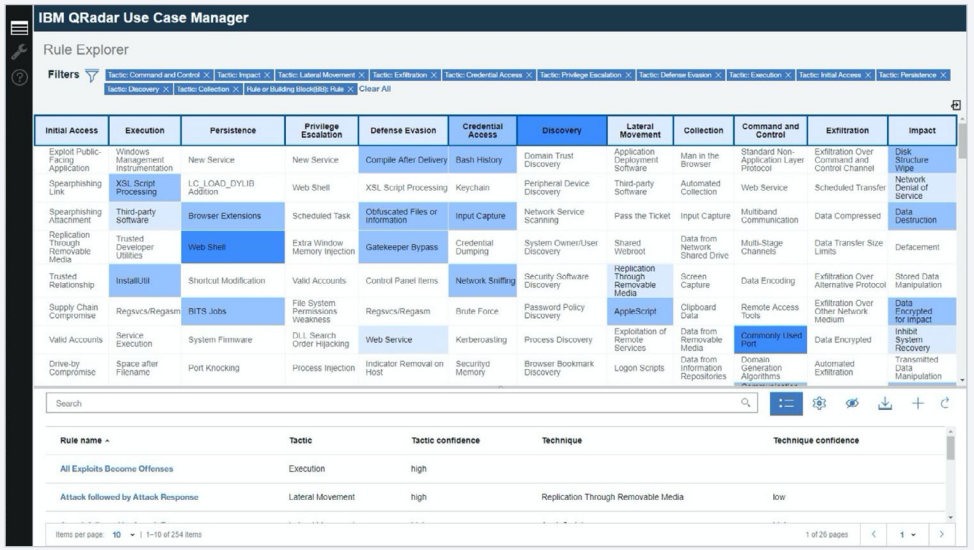


Figura 5: QRadar Use Case Manager

Preenche déficits de competências com IA

O IBM QRadar Advisor with Watson ajuda os analistas a obter rapidamente insights mais detalhados sobre as violações para tomar decisões mais informadas. A solução pode lidar com dados não estruturados e apresentar um gráfico de conhecimentos visuais que mostra todo o escopo da ameaça no ambiente. Esses insights enriquecidos ajudam a reduzir o tempo gasto nas investigações e capacitam os analistas a tomar decisões mais rápidas e mais informadas.

Capacite a equipe do SOC com o QRadar Advisor with Watson →

"O IBM QRadar Advisor with Watson é uma verdadeira inovação para nós e nossos clientes. Usando o Watson em vez de outra solução, nossos analistas podem fazer tarefas com 50% mais rapidez. Ao reunir a especialização de alto nível da Sogeti e da IBM, combinada com uma excelente inovação, estamos ajudando nossos clientes a melhorar e reforçar a segurança cibernética."

Vincent Laurens
Vice-presidente e executivo da divisão de segurança cibernética da Sogeti Luxembourg

Leia o estudo de caso →

Atende aos requisitos de conformidade

Com conteúdo, regras e relatórios pré-integrados, o QRadar SIEM oferece a transparência e a responsabilização necessárias para ajudar as organizações a atender aos requisitos de conformidade do segmento de mercado. A solução oferece pacotes de conformidade simples de instalar para General Data Protection Regulation (GDPR), a lei Federal Information Security Management Act (FISMA), a lei Health Insurance Portability and Accountability (HIPAA), ISO 27001, o Payment Card Industry Data Security Standard (PCI DSS) e muito mais. Esses pacotes são incluídos com uma licença do QRadar SIEM e disponibilizados no IBM Security App Exchange.

Prepare a conformidade de sua organização →

75%
das organizações

dizem que a privacidade de dados é um item estratégico imprescindível para elas. Por causa de regulamentos como o GDPR, os clientes estão mais a par de seus direitos de privacidade.[4]

Impulsiona a resposta para incidentes com orquestração da segurança

O QRadar oferece uma integração perfeita à plataforma IBM Resilient Security Orchestration, Automation and Incident Response (SOAR), que proporciona melhorias significativas na forma como sua organização responde aos ataques cibernéticos, automatizando e orquestrando pessoas, processos e tecnologias.

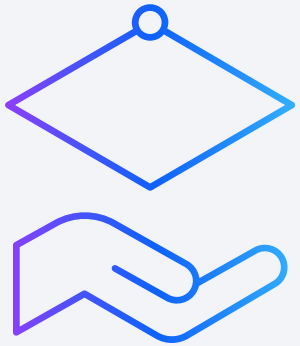
Ao combinar a plataforma Resilient SOAR com uma implementação existente do QRadar, sua equipe de analistas de segurança pode diminuir o tempo de correção de incidentes, encaminhando as suspeitas de violação do QRadar ao Resilient, acionando aprimoramentos automatizados adicionais e gerando processos completos de investigação, tudo de forma rápida e eficiente. À medida que os incidentes evoluem, todas as informações são sincronizadas entre o QRadar e o Resilient, ajudando a garantir a integridade total dos dados e um loop contínuo de feedback para melhorar a precisão da detecção de ameaças.

Explore o IBM Security Resilient →

Ajuda a maximizar seus investimentos em segurança com o IBM Security App Exchange

Explore o IBM Security App Exchange e encontre mais de 200 apps, integrações, extensões e pacotes de conteúdo validados da IBM e de nosso ecossistema de parceiros. Aprenda novos casos de uso e integrações e amplie seus recursos existentes para defender melhor sua empresa.

Descubra novos apps e extensões para melhorar o QRadar →



Processo de migração

Não há dúvidas de que migrar para uma solução de SIEM de última geração pode aumentar a eficiência de seu SOC, ajudar você a proteger melhor sua organização, gerenciar incidentes e atender aos regulamentos de conformidade.

Sua abordagem de migração varia com base nos seus requisitos de negócios. Da mesma forma, o cronograma e os marcos da migração também podem ser diferentes. O cenário mais simples é quando uma organização deixa de usar o SIEM tradicional e avança à plataforma IBM QRadar SIEM. Outro cenário é quando a empresa A, que prefere uma plataforma mais moderna de SIEM, adquire a empresa B, deixa de utilizar os sistemas antigos e implementa o QRadar. Em qualquer um desses cenários, a migração é a escolha lógica.

A IBM Security recomenda um processo de migração em três etapas para que sua organização avance para uma solução de SIEM de última geração. Trata-se de uma abordagem em fases que inclui processos de planejamento, migração e otimização, em que cada fase se baseia na anterior. A equipe IBM Security, com décadas de experiência e práticas recomendadas, oferece as orientações e a especialização necessárias para cada uma dessas etapas da jornada de migração.

Mudança instantânea para o QRadar	**Estratégia de migração** para o QRadar
Implementar o QRadar	
Transferir fontes de registros	Transferir do SIEM atual para o QRadar
Migrar regras e painéis	
Aposentar o SIEM atual; manter para conformidade	Manter o SIEM atual para relatórios limitados
Opções de implementação de pequeno, médio e grande porte	Expandir insights com recursos nativos
Consultoria especializada de acompanhamento e **migração em três etapas →**	

Tabela 1: duas estratégias de migração

Agora, vamos revisar o processo de migração em três etapas:

Avaliar e planejar

Migrar

Otimizar

Avaliar e planejar

Primeiro, o mais importante: saber suas metas e seu plano. Quais são seus desafios de negócios? Você pretende que a plataforma de SIEM seja local ou esteja em uma nuvem pública ou híbrida? Independentemente do modelo de implementação, a equipe IBM QRadar pode trabalhar com sua organização para iniciar o projeto e definir os requisitos.

O resultado dessa fase de planejamento é um plano de migração que descreve como o QRadar será configurado e como a equipe migrará os dados existentes de eventos históricos, se isso estiver no escopo. O plano também incluirá quais casos de uso, relatórios, aplicações, painéis e alertas serão implementados no QRadar depois que ele estiver em operação.

A equipe IBM orientará sua equipe de segurança por meio de um workshop de planejamento de migração ou outros eventos, conforme necessário. Esse processo incluirá a análise e o registro dos requisitos técnicos e de negócios necessários para a migração. Por fim, será criado um plano de migração. Você e a equipe da IBM precisão contribuir com suas especializações como parte da análise e do registro dos requisitos.

Estas são algumas das etapas em que, provavelmente, você terá que trabalhar:

Analisar os requisitos de negócios, avaliando:

- Quais casos de uso existentes precisam ser replicados no QRadar
- Casos de uso adicionais de inteligência de segurança recomendados pela IBM ou desejados pelo cliente
- Necessidades de relatórios de auditoria e conformidade
- Requisitos de relatórios e painéis
- Sistemas de gerenciamento de vulnerabilidades
- Integração a ferramentas de chamados e resposta a incidentes
- Modelos de recuperação de desastres
- Gerenciamento do SIEM pós-migração
- Desenvolvimento de habilidades no QRadar

Determinar os requisitos técnicos, como:

- Informações detalhadas sobre fontes de fluxos e registros, incluindo informações sobre hierarquia da rede, dispositivos e aplicações
- Requisitos dos custom Universal Device Support Modules (uDSMs)
- Como transferir a coleta de dados de outro SIEM para o QRadar
- Considerações sobre infraestrutura de rede, como firewalls e portas
- Funções e acesso dos usuários
- Migração dos dados existentes de eventos históricos

Elaborar um plano de migração que inclua:

- Detalhes dos requisitos técnicos e de negócios registrados durante as sessões de coleta de requisitos
- Design e diagramas arquitetônicos
- Procedimentos necessários para a migração, inclusive para migração de dados e transferência das fontes de registros
- Requisitos ou recomendações de personalização e integração, se houver

Migrar

Nessa fase, os especialistas da IBM implementarão a solução QRadar e migrarão dados e elementos de configuração do SIEM de terceiros. Os ajustes ajudarão você a isolar os resultados e mostrar violações priorizadas, para que possa se concentrar nos aspectos que realmente exigem sua atenção. O resultado final dessa fase é um Guia de Implementação e Arquitetura do IBM QRadar, que será entregue à equipe do cliente após a migração.

Essa atividade inclui as seguintes tarefas:

Configurar e testar os dispositivos do QRadar, VMs, dispositivos baseados em nuvem ou nós de software dessa contratação usando uma lista de verificação detalhada da implementação.

Replicar no QRadar os elementos de configuração do SIEM de terceiros.

Realizar a transferência da coleta de registros do SIEM de terceiros para o QRadar. Um procedimento detalhado para esse processo será estabelecido na fase de planejamento.

Resolver problemas de leitura e análise dos dados.

Criar custom Device Support Modules para analisar os dados das fontes de registros não compatíveis com a aplicação QRadar open-to-buy (OTB).

Migrar dados existentes de eventos históricos ao QRadar, se necessário.

Configurar retenção e backups de dados.

Verificar a coleta de eventos e fluxos da implementação existente para os novos dispositivos.

Verificar as configurações de integridade e desempenho da implementação.

Por fim, elaborar um Guia de Implementação e Arquitetura do QRadar que detalhe todos os aspectos da implementação do QRadar.

Otimizar

Depois da migração, as regras e a análise serão personalizadas para atender às necessidades únicas de seu ambiente. A equipe do QRadar oferecerá treinamento prático e orientação para permitir que sua equipe dê suporte à nova solução de forma eficaz e contínua. Essa abordagem será realizada em um ritmo adequado para clientes individuais, seja uma abordagem radical ou uma abordagem paralela em fases.

À medida que trabalhar nessas etapas, você poderá desativar o sistema antigo e trabalhar na base de seu novo SIEM, evoluindo gradativamente para um novo modelo operacional. Não é incomum que a equipe da IBM decida se devem ser feitas quaisquer atualizações no Guia de Implementação e Arquitetura do QRadar.

Se você ainda não começou a trabalhar na migração de seu SIEM, não espere mais. Como você pode ver, uma migração do SIEM pode apresentar grandes desafios. No entanto, ao adotar uma abordagem estratégica e em fase, como recomendado pela IBM Security, você conseguirá fazer uma transição descomplicada a um estado regular.

Por fim, ao migrar para uma plataforma de SIEM de última geração, você colocará sua organização no caminho para o sucesso. A solução de SIEM pode ajudar na capacidade de sua equipe de segurança de identificar ameaças, defender-se contra possíveis violações e tornar seu SOC mais eficiente.

Essa atividade inclui as seguintes etapas principais:

Configurar o QRadar para atender aos requisitos de negócios documentados. Esse processo inclui a configuração de:

- Regras personalizadas e casos de uso
- Relatórios, alertas e painéis
- Feeds de ameaças
- Apps do QRadar, incluindo, sem limitações, User Behavior Analytics, QRadar Deployment Intelligence e Pulse.

Realizar ajustes para reduzir o ruído branco e os falsos positivos e melhorar o desempenho.

Integrar às ferramentas de chamados e resposta a incidentes.

Oferecer desenvolvimento de habilidades relacionadas ao QRadar para os recursos necessários do cliente.

Fazer a transição à solução de estado regular para a equipe do SOC do cliente ou o provedor de serviços gerenciados.

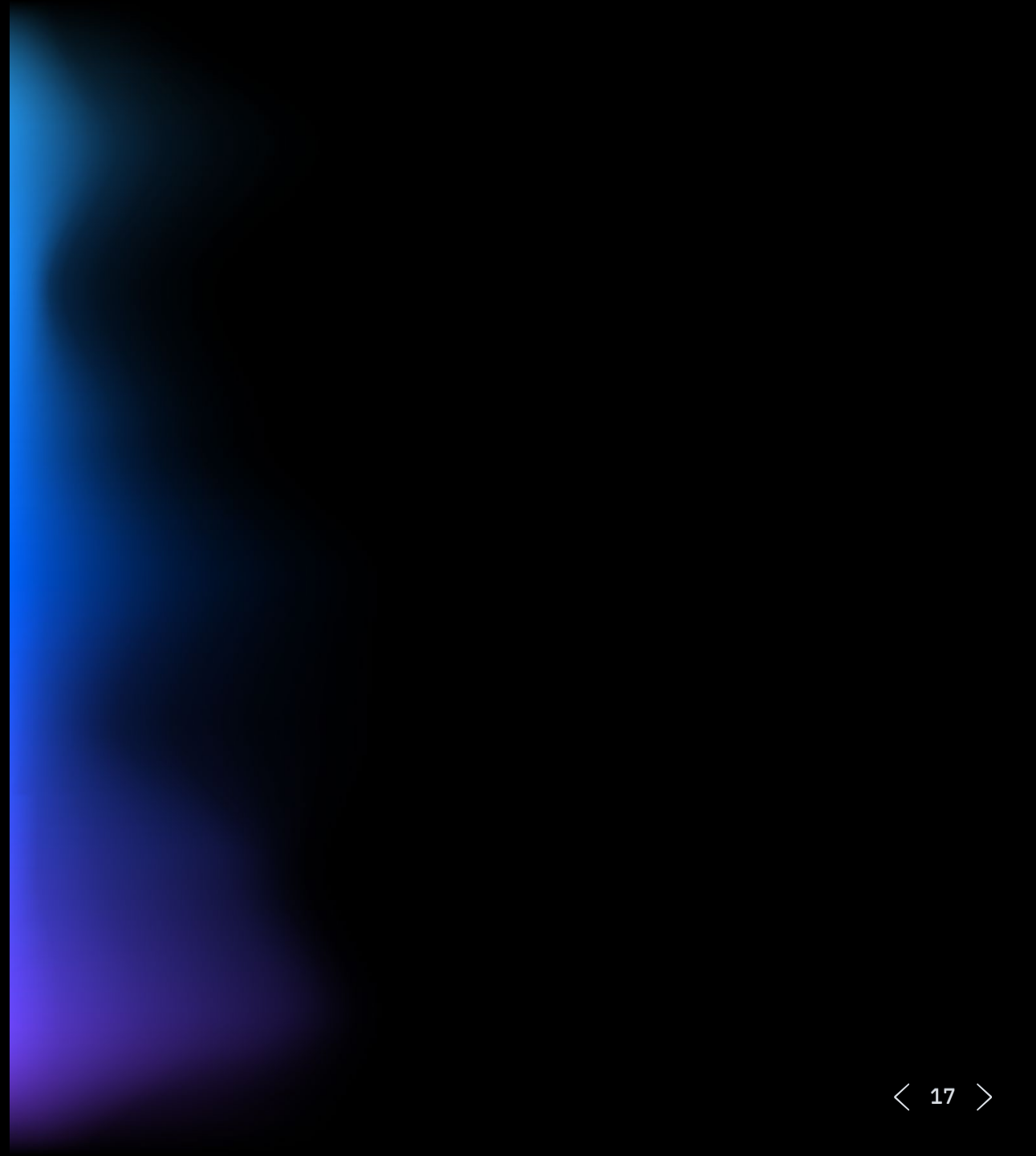
What’s next?

O IBM QRadar pode ajudar você a eliminar as complicações causadas pelas soluções desatualizadas e resolver problemas de segurança, independentemente de onde implementar as aplicações: em um modelo local, híbrido ou de SaaS.

Da obtenção de total visibilidade sobre os dados à rápida detecção de possíveis ameaças e ao cumprimento dos requisitos de conformidade, o QRadar oferece análise, regras de correlação e painéis simples de instalar para ajudar você a se manter à frente nas atividades de SIEM.

Dê as ferramentas certas à sua equipe de segurança.

Faça a atualização para uma plataforma de SIEM de última geração. →



Por que escolher a IBM?

A IBM Security oferece um dos portfólios mais avançados e integrados de produtos e serviços de segurança empresarial. O portfólio, apoiado pela pesquisa de renome mundial do X-Force, oferece inteligência de segurança para ajudar as organizações a proteger integralmente suas infraestruturas, seus dados e suas aplicações. Ela proporciona soluções para gerenciamento de identidade e de acesso, segurança de bancos de dados, desenvolvimento de aplicações, gerenciamento de riscos, gerenciamento de endpoints, segurança de rede

Essas soluções permitem que as organizações gerenciem os riscos efetivamente e implementem segurança integrada para arquiteturas móveis, em nuvem, de redes sociais e outras arquiteturas empresariais de negócios. A IBM opera uma das maiores organizações de pesquisa, desenvolvimento e entrega de segurança do mundo, monitora 15 bilhões de eventos de segurança por dia em mais de 130 países e possui mais de 3 mil patentes de segurança.

Além disso, a IBM Global Financing oferece várias opções de pagamento para ajudar você a adquirir a tecnologia de que precisa para expandir sua empresa. A IBM proporciona o gerenciamento completo do ciclo de vida dos produtos e de serviços de TI, da aquisição ao descarte. Para obter mais informações, acesse ibm.com/financing.

Para saber mais sobre a Plataforma de Inteligência em Segurança IBM QRadar na nuvem, entre em contato com seu representante da IBM ou com o parceiro comercial IBM, ou visite ibm.com/br-pt/products/hosted-security-intelligence.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produzido nos Estados Unidos da América,
em maio de 2020

Este documento está atualizado na data inicial da publicação e pode ser alterado pela IBM a qualquer momento. Nem todas as ofertas estão disponíveis em todos os países em que a IBM atua.

Os dados de desempenho e os exemplos de clientes citados têm fins somente ilustrativos. Os resultados reais de desempenho podem variar com base nas configurações e condições operacionais específicas. O usuário é responsável por avaliar e verificar o funcionamento de outros produtos ou programas com produtos e programas IBM. AS INFORMAÇÕES CONTIDAS NESTE DOCUMENTO SÃO FORNECIDAS “NO ESTADO EM QUE SE ENCONTRAM”, SEM NENHUMA GARANTIA, EXPRESSA OU IMPLÍCITA, INCLUSIVE NENHUMA GARANTIA DE COMERCIABILIDADE, ADEQUAÇÃO A UM FIM ESPECÍFICO E GARANTIAS OU CONDIÇÕES DE NÃO INFRAÇÃO. Os produtos IBM receberão garantias de acordo com os termos e condições dos contratos sob os quais eles são fornecidos.

O cliente é responsável por assegurar o cumprimento das leis e dos regulamentos aplicáveis a ele. A IBM não oferece orientação jurídica nem declara ou garante que seus serviços ou produtos assegurarão o cumprimento de qualquer lei ou regulamento pelo cliente.

Declaração de boas práticas de segurança: a segurança de sistemas de TI envolve a proteção de sistemas e de informações por meio de prevenção, detecção e resposta ao acesso inadequado de dentro e de fora da sua empresa. O acesso inadequado pode resultar em alteração, destruição, apropriação indevida ou uso incorreto de informações, ou pode resultar em danos ou uso indevido de seus sistemas, inclusive para uso em ataques a outros indivíduos. Nenhum sistema ou produto de TI deve ser considerado completamente seguro e nenhum produto, serviço ou medida de segurança pode ser completamente eficaz na prevenção contra o uso ou acesso indevido. Os sistemas, produtos e serviços da IBM foram criados para fazer parte de uma abordagem de segurança legal e abrangente, o que implicará necessariamente em procedimentos operacionais adicionais e poderá exigir outros sistemas, produtos ou serviços para serem mais eficazes. A IBM NÃO GARANTE QUE SISTEMAS, PRODUTOS OU SERVIÇOS SERÃO IMUNES, OU TORNARÃO SUA EMPRESA IMUNE, À CONDUTA MALICIOSA OU ILEGAL DE QUALQUER OUTRA PARTE.

1 Jon Oltsik. “Big Changes Are Coming to Security Analytics and Operations.” *Dark Reading*, 11 de dezembro de 2019. www.darkreading.com/cloud/big-changes-are-coming-to-security-analytics-and-operations/a/d-id/1336565

2 “Cost of a Data Breach Report highlights.” *IBM*. ibm.com/security/data-breach

3 “QRadar Security Intelligence Client Study.” *Ponemon Institute*, Dezembro de 2018. ibm.com/downloads/cas/M9YRMAKZ

4 “Data Privacy Is The New Strategic Priority.” Forrester Opportunity Snapshot: A custom study commissioned by IBM, July 2019. ibm.com/account/reg/us-en/signup?formid=urx-39964

WGW03245-USEN-01