IBM Security

Você precisa de uma estratégia de defesa melhor?

5 perguntas para responder antes de realizar a atualização da sua solução SIEM

Para obter mais informações sobre IBM Security, visite o nosso site.

Porque a segurança improvisada não é boa o suficiente

Equipes de segurança de TI precisam proteger suas organizações de ataques digitais enquanto também abordam requisitos internos e de compliance regulatórios, como ISO 27001, PCI DSS ou RGPD. Não é uma tarefa simples. Se você utilizar um gerenciador básico de logs ou planilhas manuais para armazenar e pesquisar logs, existirá a possibilidade de que você esteja perdendo incidentes críticos. Conforme invasores se tornam mais perigosos e o ambiente regulatório continua evoluindo, ferramentas básicas não são mais suficientes. Essa é a hora de fazer a atualização para SIEM.

Exploraremos cinco perguntas importantes para ajudar você a determinar a melhor solução para sua organização.

> *As soluções de Gerenciamento de Informações e Eventos de Segurança (SIEM) modernas vão além da coleta automática, análise e normalização dos logs. Elas aplicam correlação e análise avançada de dados para detectar ameaças, analisar sua gravidade e filtrá-las através do ruído para alertar você sobre eventos críticos. Essas soluções utilizam automação e inteligência incorporadas para manter você protegido — enquanto, simultaneamente, liberam tempo para maior foco em correção e recuperação.*

“ A equipe de segurança empresarial média analisa *200.000* eventos de segurança por dia.

O que é um SIEM moderno?

Análise avançada de dados para identificação de incidentes

1

Você consegue acompanhar todos os seus dados de segurança em tempo real?

Se você depende de planilhas para pesquisar e gerenciar logs, provavelmente está perdendo mudanças em tempo real, sem falar no gasto de tempo e esforços significativos em uma mera tentativa de manter os sistemas em execução. Um SIEM moderno e centralizado automatiza a coleta, normalização e análise de logs — mas não faz apenas isso.

As informações de fluxo de rede ajudam você a rastrear invasores onde eles não conseguem se esconder

Além dos logs do sistema, um SIEM moderno também analisa fluxos de rede, dados de endpoints, uso da nuvem e comportamento de usuários. Ao combinar esses variados aspectos das atividades, você pode obter uma imagem completa do que está acontecendo no seu ambiente, compreender o que é normal e usar essa linha de base para identificar automaticamente os desvios que possam sinalizar uma ameaça.

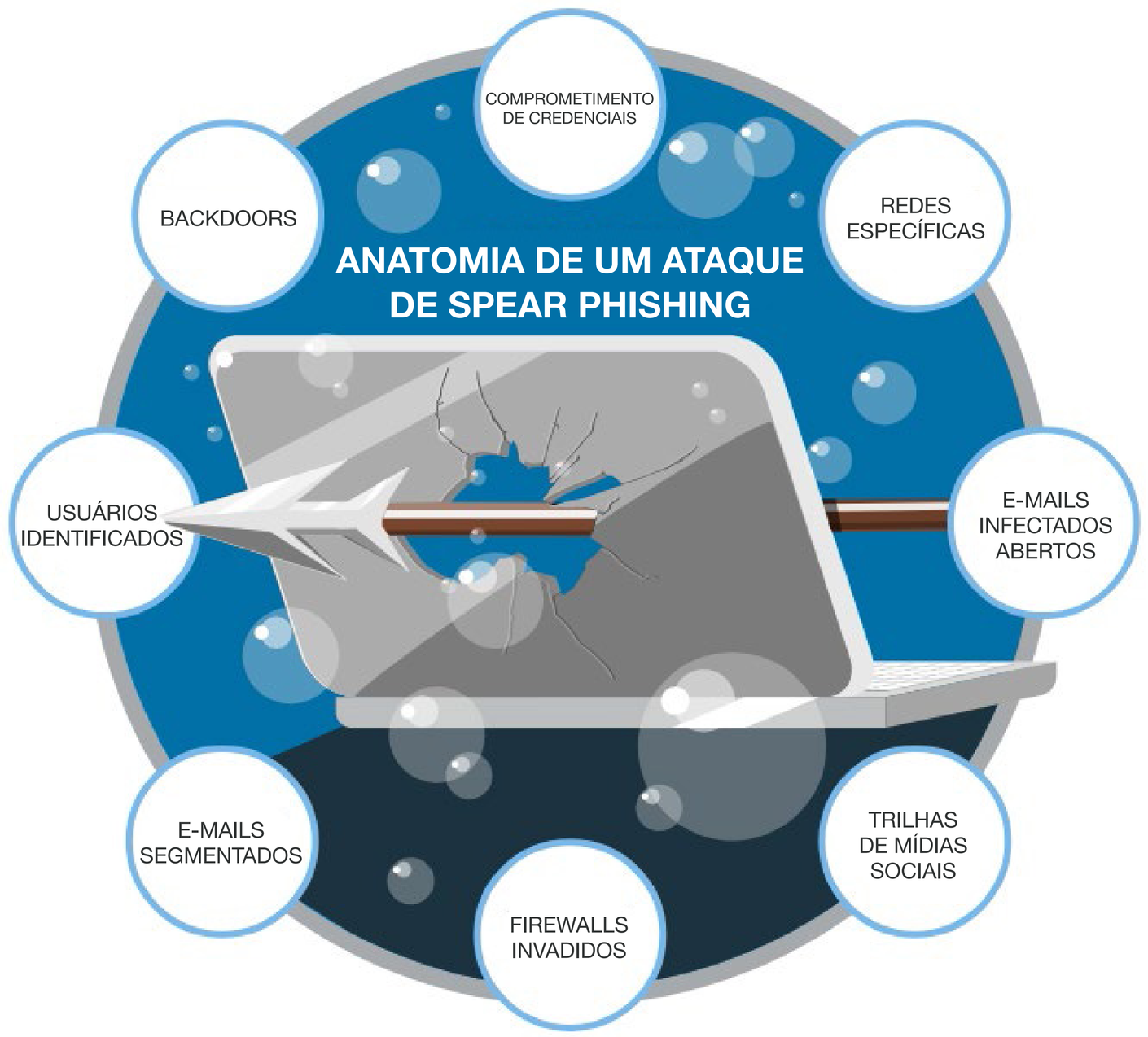
2

Seu programa de segurança monitora o elemento humano das ameaças?

Às vezes, um usuário é enganado para que clique em um link malicioso. Em outras situações, um funcionário simplesmente se volta contra você. Você tem uma solução que ajuda você a compreender o elemento humano?

De todos os ataques foram realizados por pessoas de dentro da organização — seja de forma acidental ou maliciosa.

Usuários comprometidos ou maliciosos exibirão comportamentos diferentes dos outros. Encontrar essas discrepâncias o quanto antes pode ajudar você a evitar danos. Para fazer isso, você precisa compreender o que é normal para os usuários da sua organização e utilizar essa linha de base para identificar anomalias que possam sinalizar uma ameaça. Análises de dados de comportamento de usuários que utilizam aprendizado de máquina podem ser úteis para ampliar a escala da detecção de anomalias em toda a empresa. Quando um SIEM é usado, você pode descobrir atividades de usuários anômalas e priorizar os usuários de riscos mais altos, capazes de causar mais danos.



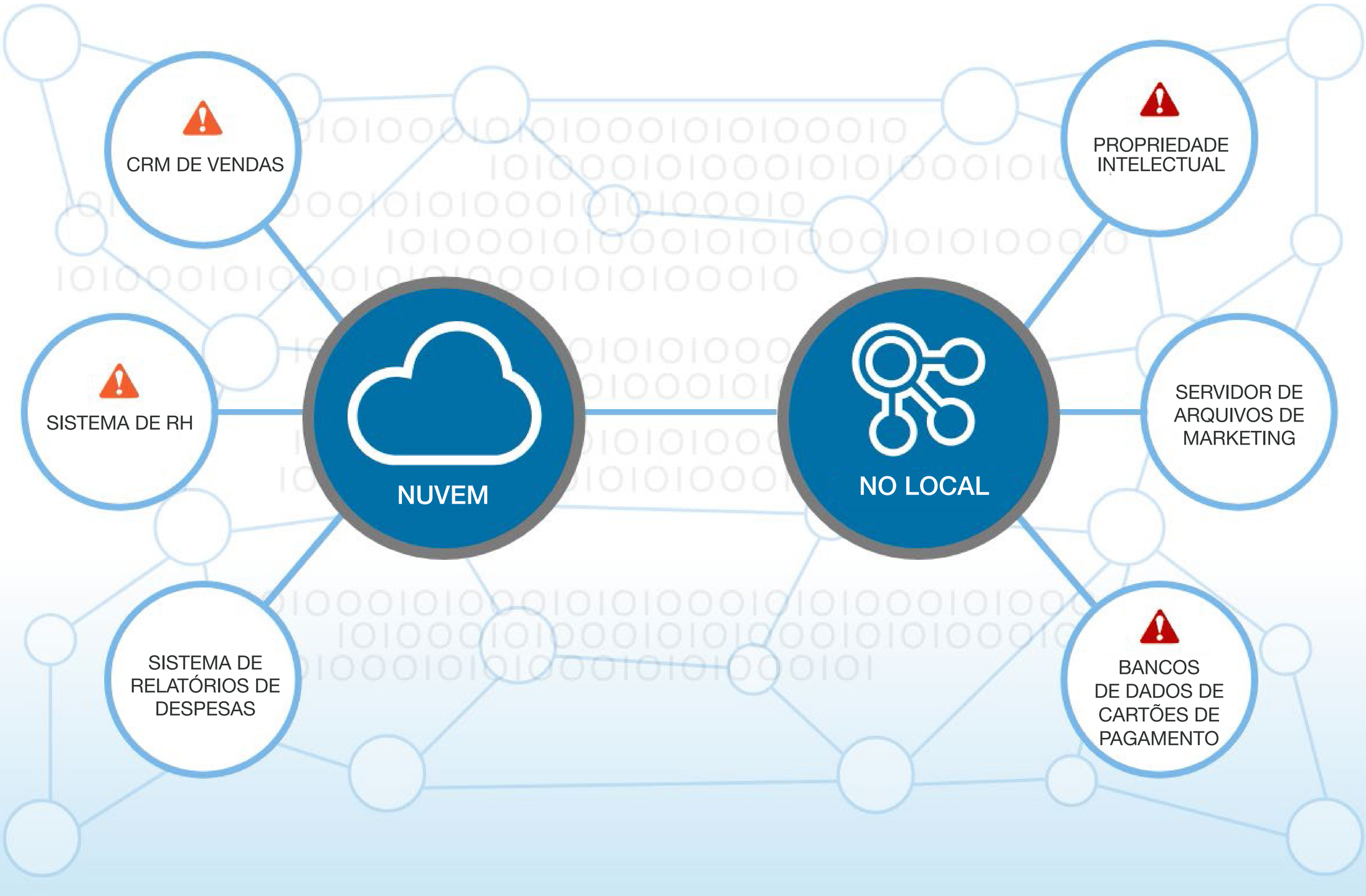
3

Pode ser útil priorizar ameaças em relação aos seus dados e ativos mais críticos?

Um servidor de arquivos usado pelo marketing e um banco de dados do seu ambiente de PCI carregará níveis muito diferentes de riscos se for comprometido. Você precisa de uma solução que compreenda o valor dos seus ativos, priorize automaticamente ameaças com base no risco para os negócios e lhe envie um alerta quando necessário.

Uma boa solução de segurança deve oferecer conhecimento da rede. Ela deve permitir que você defina seus serviços na nuvem, segmentos de rede e ativos mais sensíveis e utilize análise robusta de dados que personalizem alertas com base no risco do seu ambiente exclusivo.

“São necessários, em média, *191* dias para detectar uma ameaça. Outros *66* para contê-la.



4

Seu sistema automatiza processos para tornar você mais produtivo?

Com um conjunto de talentos limitados em alta demanda, a maioria das equipes de segurança tem poucas pessoas e muito trabalho. Uma boa solução SIEM oferece Inteligência Artificial (IA) e automação que ajudam a eliminar processos manuais. SIEMs modernos podem aumentar a produtividade — sem exigir mais funcionários.

> *Uma solução SIEM ideal ajuda a automatizar os processos de detecção, priorização e investigação de ameaças. Ela deve oferecer integrações validadas e prontas para usar com sistemas de resposta a incidentes e gerenciamento de casos que acelerem os processos de contenção, correção e recuperação.*

> **70% dos profissionais de segurança digital relatam que a escassez de habilidades impactou suas organizações.**

> **Até 2020, haverá 1,5 milhão de cargos de segurança digital vagos — quando esse número era de 1 milhão há apenas dois anos.**

5

Até que ponto é fácil começar e integrá-lo ao seu ambiente?

Descubra quais métodos de implantação são suportados. Independentemente de você preferir soluções de hardware, software ou SaaS, um bom SIEM deve ser flexível o suficiente para atender às suas necessidades. Em seguida, antes de obter valor do seu SIEM, você precisa inserir dados nele. Pergunte se ele funcionará com todos os seus sistemas, incluindo ativos no local, aplicações SaaS e ambientes em nuvem pública.

Considere a facilidade de integração, não apenas com fontes de logs mas também com soluções complementares, como feeds de inteligência contra ameaças, scanners de vulnerabilidade, ferramentas de orquestração de resposta a incidentes e sistemas de gerenciamento de casos, entre outros. Um ecossistema aberto para aplicações e integrações pode ajudar você a ficar atualizado e responder rapidamente a riscos e ameaças em constante mudança. Quanto mais integrações prontas para usar, menos horas de funcionários são necessárias para extrair valor.

“ Uma empresa média usa *75* produtos de segurança para proteger sua rede — eles precisam funcionar juntos.

Os criminosos estão ficandomais inteligentes, o que gera mais uma pergunta: Você está preparado?

Soluções SIEM modernas vão muito além de gerenciadores de logs básicos e processos manuais. Com 200.000 ameaças à segurança por dia, você precisa de uma proteção com a velocidade da luz. Um bom SIEM deve ser capaz de detectar uma ampla gama de ameaças e indicadores de ameaças, como ataques de *phishing, malware*, roubo de credenciais, movimento lateral e contrabando de dados, entre outros — e alertar você antes de o dano começar. Mas lembre-se: nem todas as soluções SIEM são criadas da mesma forma.

Procure uma solução que:

- Ofereça análise avançada de dados de segurança para detectar uma variedade de ameaças
- Priorize ameaças e alertas automaticamente para que você possa ver o que é mais importante
- Ofereça integrações prontas para usar com os seus sistemas existentes
- Consolide os insights e dados de segurança em uma única plataforma e interface
- Tenha a capacidade de implementar em diferentes escalas — de pequena a muito grande
- Seja flexível o suficiente para dar suporte ao seu método de implementação preferencial, seja no local, como SaaS ou em uma nuvem pública

Sobre o IBM QRadar

O IBM QRadar Security Intelligence Platform é uma solução de análise de dados de segurança abrangente que reúne gerenciamento de logs, análise avançada de dados, análise de rede, gerenciamento de vulnerabilidades, análise de dados de comportamento de usuários, inteligência contra ameaças e investigações de ameaças com tecnologia de IA em uma única plataforma gerenciada de uma única interface.

Os componentes da solução são totalmente integrados, permitindo que os clientes comecem com uma escala exatamente do tamanho que escolherem e possam ampliá-la ou reduzi-la posteriormente conforme as necessidades mudarem. Com mais de 500 integrações validadas prontas para usar e regras pré-configuradas, os clientes podem adicionar de forma fácil e rápida novos recursos por meio do IBM Security App Exchange.

Saiba mais em www.ibm.com/qradar.

Dê o próximo passo

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

Referências

Investigating Threats with Watson for Cyber Security, **IBM**

The IBM X-Force 2016 Cyber Security Intelligence Index, **IBM**

Ponemon Institute’s 2017 Cost of Data Breach Study: Global Overview, **IBM**

Cybersecurity skills shortage creating recruitment chaos, **CSO**

Cybersecurity labor crunch to hit 1.5 million unfilled jobs by 2021, **ISC**

Defense in depth: Stop spending, start consolidating, **CSO**


IBM Security