



TRÊS ETAPAS PARA MELHORAR SUA ESTRATÉGIA DE DADOS DE SEGURANÇA CIBERNÉTICA



CHAMPION
GUIDES

EBOOK

ÍNDICE

- 3** Introdução
- 4** Etapa 1: assumo o controle de seus dados
- 6** Etapa 2: realize busca proativa de ameaças em todos os seus dados
- 7** Etapa 3: promova a colaboração com sua equipe de dados
- 9** Conclusão: um programa de segurança cibernética bem-sucedido requer uma estratégia de dados moderna
- 10** Sobre o Snowflake

INTRODUÇÃO

As organizações de segurança podem se beneficiar dos investimentos existentes em plataforma de dados para enfrentar melhor as ameaças e reduzir os riscos para os negócios.

Um acesso melhor aos dados pode resolver uma contradição que custa bilhões de dólares no setor de segurança cibernética? De acordo com a **Gartner**[®], em 2021 estima-se que US\$ 150,4 bilhões foram gastos em todo o mundo com tecnologia e serviços de segurança da informação e gerenciamento de riscos. Há 15 anos, esse número chegava apenas a US\$ 3,5 bilhões, segundo a **Cybersecurity Ventures**. No entanto, as violações de segurança cibernética atingiram níveis recordes, e os riscos nunca foram tão grandes. A **IBM** estima que uma única violação de dados pode custar às organizações, em média, US\$ 4,2 milhões, que é o valor mais alto nos 17 anos em que a IBM vem fornecendo informações sobre violações de dados.

Essa contradição entre investimento e resultado vem da crescente assimetria entre os autores de ameaças e as equipes que buscam se defender deles. Os autores de ameaças se adaptaram rapidamente às tendências empresariais, como infraestrutura de nuvem dinâmica, cadeias de suprimentos de software interconectadas e uma força de trabalho que opera em grande parte fora do perímetro do escritório. Eles aproveitam a escala e a complexidade de seus alvos para obter acesso e permanecer incógnitos até atingir seus objetivos. Enquanto isso, as equipes de segurança tentam, em grande parte, entender o novo ambiente empresarial e o cenário de ameaças usando soluções obsoletas.

Ao mesmo tempo em que os defensores estavam ficando para trás na corrida para proteger os negócios, outros departamentos tiveram ganhos

significativos, possibilitados pela inovação na pilha de dados moderna. Dessa forma, surgiu uma oportunidade para os defensores enfrentarem seus adversários tratando a segurança cibernética como um problema de dados. Organizações de segurança cibernética bem-sucedidas serão aquelas capazes de mobilizar os dados sem limitações entre fontes e ao longo do tempo, tirando proveito total dos avanços das plataformas e análises de dados.

No centro dessa nova estratégia está a adoção de um data lake de segurança centralizado, habilitado por uma moderna plataforma de dados na nuvem. Um data lake de segurança permite que as organizações removam limitações tradicionais de visibilidade e restrições de custos relacionadas à quantidade de dados que pode ser ingerida, armazenada e retida, e por quanto tempo. O suporte a linguagens de análise padrão, como SQL e Python, também é fundamental, permitindo a colaboração entre analistas de segurança como especialistas no assunto, analistas de dados para geração de relatórios de autoatendimento e cientistas de dados para modelos comportamentais e aprendizado de máquina. Além disso, o suporte a controles de acesso granulares e compartilhamento seguro de dados para permitir a colaboração dentro de uma organização, entre colegas do setor e com provedores de dados de terceiros, são aspectos essenciais dos data lakes de segurança atuais.

Nas páginas a seguir, compartilharemos três etapas comprovadas que permitem uma transição bem-sucedida para uma estratégia de segurança cibernética baseada em dados.

ETAPA 1: ASSUMA O CONTROLE DE SEUS DADOS

Controlar seus dados significa ter liberdade: para ingerir e reter o máximo de dados que você quiser, para analisar conjuntos de dados recentes e históricos, e para escolher quais soluções de segurança apoiarão sua missão de proteger os negócios.

DESAFIO: OS SIEMS TRADICIONAIS LIMITAM A LIBERDADE E O CONTROLE DOS DADOS

A maioria das equipes de segurança usa uma solução de gerenciamento de eventos e informações de segurança (SIEM) para detecção de ameaças e resposta a incidentes. O SIEM é a fonte da verdade para o programa de segurança. No entanto, os SIEMs legados são integrados verticalmente e exigem o uso de bancos de dados proprietários integrados. Não surpreende o fato de que esses fornecedores não conseguiram acompanhar o desempenho e a escalabilidade de plataformas de dados na nuvem de propósito geral e operam como uma pilha de dados independente para segurança cibernética, separadamente do resto da empresa.

Como resultado, as equipes de segurança devem lidar com análises rudimentares e silos de dados fragmentados. Ocasionalmente, alguns dados de segurança podem ser pesquisados, mas não podem ser combinados facilmente com dados contextuais, o que pode incluir dados comerciais ou quaisquer outros dados que fornecerão às equipes de segurança mais contexto sobre uma ameaça em potencial. Os dados de segurança por si só não são suficientes para avaliar completamente as ameaças em potencial.

Além disso, os altos custos de licenciamento dos SIEMs tradicionais forçam os usuários a armazenar cada vez mais dados de segurança em outros locais, especialmente em buckets na nuvem, que resolvem apenas o problema de armazenamento. Esse método introduz processos complicados e despesas quando os conjuntos de dados precisam ser integrados para análise, aumentando os tempos de resposta durante uma violação e deixando de oferecer suporte aos principais casos de uso, como a busca de ameaças e o trabalho de inteligência contra elas. Os desafios de governança de dados agravam os problemas de proliferação de dados, na forma de níveis de armazenamento autogerenciados.



SOLUÇÃO: CENTRALIZAR EM UM DATA LAKE DE SEGURANÇA CRIADO PARA A NUVEM

Um data lake de segurança moderno é um repositório onde registros e outros conjuntos de dados são retidos em armazenamentos baratos e quase ilimitados na nuvem, onde esses dados podem ser analisados rapidamente. Os data lakes modernos são projetados para fornecer acesso centralizado e seguro aos dados de uma organização. As organizações podem aproveitar uma infinidade de benefícios imediatos quando centralizam seus dados de segurança em uma única plataforma, incluindo:

- **A capacidade de ingerir e reter petabytes de logs de eventos de forma econômica.**
- **A oportunidade de integrar dados de segurança com dados de negócios e aplicativos para contextualizar e, por fim, automatizar operações de segurança.**
- **A liberdade de realizar investigações sem saber com antecedência quais registros de dados podem ser relevantes ou ter de recuperar dados históricos de arquivos velhos.**
- **O poder de controlar quais fornecedores têm acesso a quais conjuntos de dados.**
- **A flexibilidade para migrar soluções de segurança sem precisar mover os dados coletados.**

Um data lake de segurança moderno pode permitir que as equipes de toda a empresa acessem a mesma única fonte de verdade para vários casos de uso de segurança cibernética: detecção e resposta a ameaças, gerenciamento de vulnerabilidades, automação de conformidade e relatórios de risco em nível executivo.

Além de habilitar e acelerar as iniciativas do programa de segurança, um data lake de segurança moderno pode gerar economia de custos e eficiência de orçamento. O armazenamento econômico com compactação em repouso representa custos de armazenamento mais baixos. Ainda mais significativo é o poder computacional flexível e quase infinito, fornecido pelas principais plataformas de dados na nuvem. Não existe mais a necessidade de provisionar recursos em excesso. As plataformas que combinam a elasticidade computacional com preços baseados no consumo permitem que os clientes paguem apenas pelos recursos de que precisam, quando precisam. No contexto de segurança cibernética, que geralmente requer pouca, mas que ocasionalmente pode exigir muita capacidade computacional, esse modelo libera drasticamente o orçamento de segurança para outros usos.

A implementação de um data lake de segurança moderno e criado para a nuvem pode ser transformadora para uma organização. Ao alojar seus dados em uma única plataforma, suas equipes de segurança têm a oportunidade de simplificar a pilha de tecnologia, consolidar armazenamentos de dados distintos e permitir análises avançadas de dados em vários casos de uso. Os recursos de governança e a auditoria centralizada garantem proteção, enquanto as oportunidades de colaboração de dados permitem que as equipes de segurança sobrecarregadas obtenham sucesso em suas iniciativas críticas nos próximos anos.



ETAPA 2: REALIZE BUSCA PROATIVA DE AMEAÇAS EM TODOS OS SEUS DADOS

O cenário de ameaças está mudando rapidamente, com empresas cada vez mais dependentes de terceiros em cadeias de suprimentos e infraestrutura baseada em SaaS. Para reduzir os riscos para a empresa, é necessário assumir uma postura pessimista de que “os ataques vão acontecer”. Infelizmente, a maioria das equipes de segurança depende de uma abordagem de “exterior rígido, centro flexível”, a partir da qual as ameaças que passam pelos sistemas iniciais de defesa podem permanecer dentro do seu ambiente por meses. Essa tendência perigosa é, em grande parte, resultado das limitações impostas pelas soluções SIEM legadas.

DESAFIO: OS INVESTIGADORES DE AMEAÇAS NÃO TÊM ACESSO AOS DADOS E ANÁLISES DE QUE PRECISAM

Embora a detecção básica de ameaças possa ser realizada em tempo real à medida que os logs de eventos são coletados, as detecções avançadas e a busca proativa de ameaças exigem uma combinação de conjuntos de dados entre fontes e períodos de tempo diferentes. Os autores de ameaças, especialmente se já estiverem presentes no ambiente, têm grande vantagem e muitos lugares para se esconder. Isso é o que torna os investigadores de ameaças tão potencialmente valiosos para programas de segurança corporativa.

Infelizmente, os investigadores de ameaças não podem ter êxito se não obtiverem respostas para suas perguntas. Quando os dados estão isolados em silos em vários sistemas de origem, bloqueados no armazenamento frio ou perdidos em políticas de retenção, os investigadores de ameaças não conseguem usá-los. Os investigadores de ameaças também sofrem atrasos quando as consultas levam horas para serem executadas, quando as pesquisas retornam mensagens misteriosas de erro “sem memória” ou quando entram em contenção de recursos com outras equipes.

Por fim, a maioria dos produtos de segurança legados restringe consultas a linguagens de pesquisa proprietárias ou técnicas rudimentares de grep/regex. Isso introduz uma curva de aprendizado para novos membros da equipe e impede que os investigadores de ameaças expressem adequadamente suas hipóteses como código.

SOLUÇÃO: CAPACITAR OS INVESTIGADORES DE AMEAÇAS COM UMA PLATAFORMA DE DADOS NA NUVEM QUE OFEREÇA SUPORTE A ANÁLISE DE DADOS EM ESCALA

Uma arquitetura de dados criada para a nuvem que sustenta um data lake de segurança e elimina silos de dados é fundamental para permitir a busca proativa de ameaças. Uma vez estabelecida, analistas de segurança experientes podem rapidamente começar a descobrir ameaças latentes usando técnicas analíticas padrão e universais. Tendo em conta um mecanismo de consulta suficientemente eficaz, os investigadores de ameaças podem trabalhar em meses ou anos de dados medidos em petabytes.

Até mesmo membros iniciantes da equipe de operações de segurança podem participar por meio de uma parceria com analistas de dados de toda a empresa. Embora os analistas de dados nunca pudessem ajudar na busca de ameaças em um ambiente de nicho, exclusivo de segurança, eles são especialistas em transformar a lógica de negócios em SQL dentro da plataforma de dados empresariais já conhecida. Falaremos mais sobre isso adiante.

As plataformas de dados na nuvem que oferecem um marketplace com ofertas de inteligência de ameaças permitem obter mais recursos para a busca de tais ameaças. Os marketplaces que se baseiam na tecnologia moderna de compartilhamento de dados podem permitir que os fornecedores de inteligência de ameaças e as organizações de pesquisa publiquem indicadores de comprometimento (indicators of compromise, IOCs) e outros produtos de inteligência para uso quase instantâneo. As equipes de segurança que utilizam os feeds de inteligência dessa maneira podem aplicar, de forma otimizada e automática, IOCs atualizados aos seus dados de log. Dessa forma, investigadores de ameaças e ferramentas de automação podem detectar usuários mal-intencionados de forma confiável, sem a sobrecarga de integrações de API ou a busca manual de indicadores em um portal.

O modo como essa abordagem capacita os investigadores de ameaças representa a grande oportunidade que a segurança cibernética tem ao se alinhar à estratégia de dados geral da empresa: à medida que novos recursos e metodologias de análise de dados surgirem, os defensores reduzirão cada vez mais a vantagem dos usuários mal-intencionados.

ETAPA 3: PROMOVA A COLABORAÇÃO COM SUA EQUIPE DE DADOS

A divisão que mais cresce em muitas empresas é a equipe de dados. Analistas de dados, engenheiros de dados e cientistas de dados são os principais agentes de marketing, finanças e outros departamentos da sua organização. Agora, os líderes de segurança estão colocando em prática a tecnologia e os processos que permitem a detecção de ameaças e a redução de riscos por meio da colaboração entre as equipes de segurança e de dados.

DESAFIO: AS EQUIPES DE SEGURANÇA DEDICAM MUITO TEMPO AO TRABALHO NÃO RELACIONADO À SEGURANÇA, INCLUINDO A COLETA DE DADOS E A GERAÇÃO DE RELATÓRIOS PARA PARTES INTERESSADAS

Quando sua equipe está muito sobrecarregada tentando combater invasores, não faz sentido que ela dedique tempo a qualquer tarefa que não exija a expertise que possui. Em vez de fazer triagem de alertas ou investigar ameaças, muitas equipes de segurança dedicam grande parte de seu tempo procurando dados, atualizando planilhas ou dando vida aos clusters de pesquisa.

A segurança também desempenha um papel importante nas certificações e auditorias que as empresas devem manter para vender a seus clientes. Essas certificações e auditorias podem se tornar grandes cargas quando exigem que equipes de segurança cibernética participem de reuniões intermináveis entre as partes interessadas sobre conformidade, TI, DevOps e liderança.

Após três décadas e duas abordagens muito diferentes para permitir a análise de dados efetiva, surgiu a plataforma de dados moderna. Ela representa o poder do armazenamento tradicional de dados, a flexibilidade das soluções de big data e a elasticidade da nuvem, a um custo menor que o das soluções anteriores.



SOLUÇÃO: FORMAR UMA PARCERIA ENTRE ANALISTAS DE SEGURANÇA E PROFISSIONAIS DE DADOS PARA PROTEGER A EMPRESA, JUNTOS

Avalie as diferentes formas como a equipe de segurança investe o seu tempo. Quais tarefas não exigem a expertise que elas possuem? Dessas tarefas, quais estão relacionadas principalmente com preparação, análise ou geração de relatórios sobre dados? Envolve seus colegas na organização de dados em uma discussão aberta sobre essas áreas de colaboração.

Por exemplo, a coleta de registros de RH para enriquecimento em detecção e resposta pode ser uma tarefa de pipeline de dados que será mais bem executada pelos engenheiros de dados. Medir o desempenho do SLA de patches de segurança é algo simples para analistas de dados. E identificar movimentações incomuns de arquivos, considerando os registros de atividade adequados, é uma tarefa simples para cientistas de dados.

A integração de dados de segurança com o restante da organização define a base para uma parceria entre equipes de segurança e profissionais de dados. Essa colaboração pode melhorar muito a capacidade de uma organização de realizar análises de dados de segurança de alta fidelidade, ao mesmo tempo em que aproveita ao máximo os talentos internos.

Os relatórios de autoatendimento de inteligência de mercado (business intelligence, BI) podem ser uma ótima maneira de eliminar reuniões e retirar as equipes de segurança do caminho crítico dos processos rotineiros da empresa. Por exemplo, um programa típico de gerenciamento de patches pode envolver engenheiros de segurança que avaliam o risco de descobertas de vulnerabilidades, e analistas de conformidade que priorizam a correção dessas descobertas. Essa priorização pode ser baseada na localização dos problemas (produção voltada para o cliente versus área restrita interna, por exemplo) e por quanto tempo eles estão presentes. Essas considerações são resultado das estruturas de conformidade às quais a empresa deve aderir se quiser continuar atendendo aos seus clientes.

Painéis acionáveis que aplicam lógica de negócios e conjuntos de dados contextuais a problemas de segurança de forma automatizada e no tempo certo permitem que as equipes de correção solucionem problemas sem precisar de reuniões. As atualizações de status também são eliminadas quando qualquer pessoa autorizada pode ver o status mais recente na ferramenta de BI da empresa. Os analistas de dados fazem isso rotineiramente para outros departamentos, o que significa que você pode trazer essa transformação digital para sua organização de segurança.

Essa abordagem muda a segurança cibernética de uma prática compartimentada e reativa para uma ampla colaboração que visa resolver problemas com soluções baseadas em dados.

CONCLUSÃO: UM PROGRAMA DE SEGURANÇA CIBERNÉTICA BEM-SUCEDIDO REQUER UMA ESTRATÉGIA DE DADOS MODERNA

Agora, você conhece três etapas comprovadas para melhorar sua estratégia de dados de segurança cibernética. Essa é uma parte essencial para a proteção de uma organização moderna em escala de nuvem contra ameaças virtuais.

Para ter êxito, seus analistas de segurança precisam de um data lake de segurança moderno, habilitado por uma plataforma de dados na nuvem e fornecido como um serviço, para obter acesso rápido a dados relevantes em um local central. Isso vale tanto para empresas grandes e extensas, quanto para startups em rápido crescimento. Um único evento de violação pode significar o fim para qualquer tipo de empresa.

Lembre-se de que suas equipes de segurança cibernética não devem mais operar sozinhas, longe das ferramentas de dados e da expertise que atualmente estão presentes em praticamente todas as empresas. Os líderes de segurança podem definir uma base para que sua equipe aproveite a expertise de outras partes da organização e, assim, se concentre em elementos de segurança cibernética que ninguém mais cuidará.

Seguindo as três etapas descritas neste eBook, você pode passar do gerenciamento reativo de segurança cibernética para abordagens de suporte cada vez mais proativas, como busca de ameaças e relatórios de autoatendimento. Com o passar do tempo, uma abordagem baseada em dados permitirá que sua organização de segurança cibernética alcance todo o potencial e converta com sucesso seus investimentos em mais segurança para sua empresa e seus clientes.





SOBRE O SNOWFLAKE

O Snowflake permite que todas as empresas impulsionem seus dados, graças ao Snowflake Data Cloud. Os clientes usam o Data Cloud para eliminar silos de dados, descobrir e compartilhar dados com segurança, capacitar aplicativos de dados e executar inúmeras cargas de trabalho analíticas e de IA/ML. Onde quer que os dados ou os usuários estejam, o Snowflake proporciona uma única experiência de dados em inúmeras nuvens e regiões. Milhares de clientes em diversos setores, incluindo 639 das empresas que aparecem na Forbes Global 2000 (G2K) de 2023 (dados de 31 de julho de 2023), usam o Snowflake Data Cloud para impulsionar seus negócios.

Saiba mais em [snowflake.com](https://www.snowflake.com)



© 2022 Snowflake Inc. Todos os direitos reservados. Snowflake, o logotipo da Snowflake e todos os demais nomes de produtos, recursos e serviços da Snowflake mencionados neste documento são marcas registradas ou marcas comerciais da Snowflake Inc. nos Estados Unidos e em outros países. Todos os outros nomes de marcas ou logotipos mencionados ou usados neste documento são apenas para fins de identificação e podem ser marcas comerciais de seus respectivos detentores. A Snowflake não pode ser associada a tais detentores, nem patrocinada ou apoiada por eles.

CITAÇÕES

¹ A Gartner prevê que os gastos mundiais com gerenciamento de riscos e segurança ultrapassem US\$ 150 bilhões em 2021.

² Os gastos globais com segurança cibernética devem passar de US\$ 1,75 trilhão entre 2021 e 2025.