elastic

# Extraia mais valor operacional do seu SIEM

elastic.co/pt →

# Índice

# Introdução

À medida que as organizações foram adotando iniciativas de transformação digital para se adaptar às mudanças do mercado, muitas se viram obrigadas a reavaliar sua abordagem de segurança. Novos produtos e serviços da Web, apps para celular e a necessidade de dar suporte a uma força de trabalho remota estão abrindo caminho para novos tipos de ataques cibernéticos. **As equipes de segurança precisam evoluir rapidamente para acompanhar e enfrentar esses ataques.**

Um desafio fundamental para acompanhar é evitar ineficiências que possam ameaçar os negócios, apesar dos melhores esforços das equipes de segurança. A explosão da adoção do SaaS, as exigências contínuas quanto à privacidade e as diretivas para consolidar as funções de segurança aumentam a complexidade operacional.

O segredo para permanecer no controle enquanto mantém a eficiência operacional começa com os dados que você tem prontamente disponíveis na sua plataforma de gerenciamento de informações e eventos de segurança (SIEM). O volume e a variedade de dados de que as equipes de segurança precisam estão explodindo — nuvem, Internet das Coisas (IoT), fontes móveis e dados de observabilidade, apenas para citar alguns. O resultado é um aumento maciço na atividade de eventos, que é crucial para revelar os insights necessários para proteger os negócios.

Essa explosão de dados geralmente apresenta desafios operacionais devido às limitações do SIEM. **Agora pode ser o momento de rever a sua abordagem para o SIEM** a fim de garantir que você esteja pronto(a) para esses novos desafios.

## 175 ZB

O IDC prevê que até 2025, os dados mundiais chegarão a 175 zettabytes

## 41,6 bilhões

Em 2025, 41,6 bilhões de dispositivos conectados gerarão 79,4 zettabytes de dados

## 42 bilhões

Os entrevistados da pesquisa global de 2020 da PwC sobre crimes econômicos e fraude relataram 42 bilhões de dólares no total do prejuízo decorrente de fraude

# Os requisitos de segurança estão evoluindo

Conforme as organizações vão adotando um modelo de negócios mais centrado na nuvem, as equipes de segurança recebem mais responsabilidades para garantir que os ativos mais valiosos dos seus negócios — usuários, aplicações, endpoints e dados — sejam protegidos. Considere as tendências a seguir que estão gerando dificuldades para as equipes de segurança atingirem seus KPIs e métricas.

## Pessoas

Antecipar-se às novas e mais sofisticadas metodologias de ataque é essencial.

- Há escassez de habilidades de segurança
- Equipes de segurança sobrecarregadas estão se esforçando para trabalhar melhor em conjunto, com mais rapidez e eficiência

## Processo

A pressão está aumentando para manter a eficiência operacional e a velocidade à medida que as iniciativas de nuvem explodem.

- Enormes quantidades de dados estão sendo migradas para a nuvem
- Trabalhadores remotos e parceiros precisam de suporte para mais soluções em nuvem

## Tecnologia

O suporte para fontes de dados de alto volume é vital para fornecer visibilidade de atividades evasivas e detalhes necessários para contextualizar uma ameaça.

- É difícil realizar consultas e análises responsivas nos ambientes locais e na nuvem
- Em muitos sistemas, o acesso a fontes de dados de alto volume pode ter um custo proibitivo

As equipes de segurança estão cientes de que a transformação digital adiciona mais superfície de ataque: cada novo dispositivo conectado ou serviço de nuvem pode apresentar um novo vetor em potencial para um adversário explorar e pode resultar em ameaças graves à segurança ou na exposição de ativos, aumentando o risco do negócio. **O requisito mais fundamental é ter o contexto certo no momento certo para tomar decisões melhores e mais rápidas.**

# Repense a sua estratégia de segurança usando os dados como framework

Manter a visibilidade de uma superfície de ataque dinâmica e crescente costuma ser impraticável. Modelos de licenciamento por ingestão ou por evento e/ou arquiteturas que não atendem aos requisitos de escala da nuvem podem forçar você a escolher uma coisa em detrimento de outra. As equipes geralmente gastam tempo e recursos para decidir quais dados incluir e excluir das operações diárias, deixando a organização com visibilidade limitada em seu SIEM, o que resulta em silos operacionais — silos de dados, silos de equipes e silos de processos.

Em vez de trabalhar com compensações e abordagens únicas para preservar dados que são difíceis de incluir no SIEM, como fontes de dados de alto volume ou dados históricos, as equipes de segurança estão cada vez mais adotando uma abordagem diferente, centrada nas necessidades de dados. A base do SIEM moderno deve acomodar todos e quaisquer dados, permitindo, assim, que as equipes de segurança quebrem os silos. **O SIEM moderno permite que as equipes de segurança façam buscas em escala** com velocidade e precisão em grandes quantidades de qualquer tipo de dados — sejam fontes de dados tradicionais, não tradicionais ou de alto volume — em um ecossistema de várias camadas. Uma vez que essa base esteja estabelecida, as equipes de segurança podem obter enormes benefícios para **operacionalizar qualquer caso de uso de segurança em escala**, como monitoramento e conformidade, detecção e prevenção de ameaças, e caça e resposta a incidentes, ao mesmo tempo em que tratam de fraudes, violações de privacidade e outras questões prioritárias que podem colocar a empresa em risco. O segredo está na capacidade das equipes de operações de segurança de **coletar, analisar, visualizar e agir de acordo com os insights de segurança de maneira unificada**.

## Como o seu SOC se beneficia de uma abordagem unificada

Uma abordagem unificada apresenta às equipes de segurança uma série de vantagens. Um único armazenamento, com poderosos recursos de segurança, processamento e visualização de dados, fornece o contexto necessário em ambientes distribuídos para extrair valiosos insights de segurança de todos os seus dados. Com a analítica de segurança certa, como detecções de alta fidelidade, trabalhos de machine learning validados e outros métodos prontos para uso no local e na nuvem, as equipes de segurança podem melhorar a postura de segurança, detectar ameaças conhecidas e desconhecidas, e responder rapidamente para evitar danos e prevenir futuros incidentes. Estrategicamente, **conforme ocorrem mudanças dinâmicas, as equipes de segurança podem evoluir com rapidez**. Os profissionais podem assumir conjuntos de habilidades mais amplos à medida que:

Utilizam mais contexto para manipular melhor os dados e analisar técnicas, métodos e tecnologias

Colaboram para descobrir novas pesquisas ou implementar novas detecções

Desenvolvem novas visualizações e procedimentos operacionais

Traçam o perfil dos atores de ameaças e emulam o comportamento adversário

Mais equipes podem assumir responsabilidades de caça. Recursos robustos de integração no nível da plataforma podem permitir a adoção de procedimentos altamente eficientes que simplificam a adaptação a novas classes de ameaças e exigências regulatórias emergentes.

Com uma abordagem unificada, seu SOC pode resolver problemas complexos de segurança para uma infinidade de funções de segurança, incluindo caça a ameaças, SIEM, pesquisa de ameaças, conformidade, monitoramento e investigação de segurança, análise forense digital e resposta a incidentes, proteção de endpoint, prevenção contra fraude e muito mais.

### Visibilidade holística

Colete insights de segurança e inclua as fontes de dados necessárias para gerar resultados alinhados aos negócios.

### Escalabilidade na nuvem

Obtenha o contexto necessário de toda a organização para verificar as ameaças, incluindo anos de contexto histórico.

### Alta eficiência do SOC

Encontre os problemas de maior prioridade com rapidez e realize a integração com outras ferramentas e tecnologias facilmente para agilizar a investigação e a resposta.

## Valor para toda a equipe de segurança

### Engenheiro de segurança e administrador

- Analise centralmente logs, fluxos e dados contextuais de todo o seu ambiente, mesmo que as fontes de dados sejam muito diferentes
- Busca federada para rápido acesso e busca em um complexo ambiente distribuído
- Indexe e acesse facilmente fontes de dados de alto volume sem custos exorbitantes

### Analista de segurança

- Precisão para detectar ameaças complexas mais rapidamente
- Velocidade para acelerar a resposta e a eficiência
- Realize a detecção automatizada de ameaças e minimize o MTTD

### Gerente de SOC

- Mantenha um alto nível de conscientização em todo o ambiente para melhorar a postura de segurança
- Evite recorrências de problemas conhecidos enquanto identifica problemas desconhecidos
- Atenda aos KPIs de segurança sem incorrer em altos custos

# Seu SIEM está impedindo você?

Hoje, os dados relevantes para a segurança podem vir de serviços em nuvem, atividade da rede e dos usuários, endpoints, aplicações, dispositivos conectados e de muitas outras fontes. Muitas soluções de SIEM que tentam acessar todas essas fontes de dados resultam em análises lentas ou em implantações com custos proibitivos.

Alguns SIEMs são construídos com base em armazenamentos de dados separados para diferentes tipos de analítica de segurança, como um para machine learning e um para correlações baseadas em eventos, deixando para as equipes a tarefa de arquivar dados em outro armazenamento de dados separado para contexto de caça a ameaças ou evidências forenses e assim por diante. Conforme mencionado acima, esses silos causam ineficiências quanto à forma como as equipes compartilham contexto, colaboram, gerenciam casos e respondem a ameaças.

O SIEM deve ajudar seu SOC a evoluir mais rapidamente, mas muitos produtos de SIEM não oferecem escala ou flexibilidade para ajudar as equipes de segurança a quebrar silos de dados ou de tarefas, o que resulta em fluxos de trabalho investigativos limitados por esses silos. Consequentemente, temos silos operacionais que impedem que as equipes de segurança se movam com mais rapidez, inteligência e eficiência.

## Entre os desafios comuns na eficiência operacional das soluções de SIEM tradicionais incluem-se os seguintes:

- As fontes de dados de segurança não são consolidadas e residem em armazenamentos de dados distintos em toda a empresa, tornando difícil ter uma visibilidade holística.
- Os tempos de retenção são muito curtos, impondo a necessidade de reduzir as exigências para detecções, contexto investigativo e caça a ameaças. A definição do escopo das violações em ataques com tempos de permanência mais longos é difícil.
- Os analistas de segurança não têm fontes de dados adequadas necessárias para obter contexto sobre uma atividade que pode não indicar uma ameaça persistente avançada, mas que ainda é uma ameaça real para os negócios.
- As equipes de SOC não conseguem utilizar as ferramentas de machine learning, a menos que tenham cientistas de dados internos para desenvolver modelos e caçadores de ameaças habilidosos para interpretar o contexto.
- Os engenheiros de segurança precisarão fazer enormes investimentos em projetos de normalização de dados e/ou rearquitetar continuamente a malha de dados subjacente de seu SIEM quando precisarem adicionar novas fontes de dados ricas em contexto (como dados de alto volume). Eles já devem “conhecer” seus dados.
- As equipes de pesquisa gastam muito tempo desenvolvendo regras de SIEM que são frágeis, não resilientes a técnicas evasivas e que carecem do contexto de alta fidelidade obtido dos dados certos.
- Os analistas de nível 1 e 2 gastam muito tempo perseguindo alertas que resultam em becos sem saída ou exigem a recuperação de contexto adicional de outros armazenamentos de dados, causando atrasos e ineficiências.
- Os desenvolvedores passam a maior parte do tempo solucionando problemas de integrações ou tentando ficar a par das atualizações dos fornecedores.

# Obtenha uma melhor proteção usando um SIEM moderno

Um SIEM moderno pode acessar todos os dados de segurança, independentemente do tamanho, escala ou localização. Com visibilidade de todo o ambiente, as equipes de segurança têm acesso a um contexto rico e a períodos de lookback históricos necessários para detectar e responder melhor às ameaças, com mais rapidez e maior precisão para priorizá-las.

**Acesso a todos e quaisquer dados**

**Insights históricos e em tempo real**

**Alcance a velocidade máxima do SOC**

# Ganhe eficiência operacional com o Elastic Security como seu SIEM

As equipes de segurança estão gerenciando uma quantidade crescente de dados e precisam ser capazes de buscar, analisar e realizar a detecção automatizada em todos eles, com rapidez e precisão. A resposta a ameaças modernas requer correlação instantânea para realizar de forma eficaz o trabalho investigativo, a caça, a definição do perfil da ameaça e muito mais em dados de segurança tradicionais, infraestrutura de nuvem, dados de aplicações e anos de dados históricos.

As equipes de segurança usam o Elastic Security para acessar dados consolidados, contextualizar descobertas com contexto de ameaças e negócios, e usar dados históricos para encontrar rapidamente o melhor caminho para a resolução. O Elastic Security pode ser usado para SIEM, segurança de endpoint, caça a ameaças, monitoramento de nuvem, detecção de fraude e muitos outros casos de uso. Assim, o seu SOC pode aproveitar o poder da busca e visualização para proteger a organização com uma abordagem unificada para detecção, prevenção e resposta a ameaças.

# Trabalhe de maneira mais inteligente com o Elastic Security

## Ganhe uma visibilidade holística

Colete dados normalizados pelo Elastic Common Schema com os Beats e indexe todos os dados relevantes para a segurança para eliminar silos de dados em toda a organização. Interaja com dashboards intuitivos e prontos para uso, e desenvolva com o Kibana, o Lens e o Canvas visualizações personalizadas de arrastar e soltar que atendem às suas necessidades.

## Obtenha insights sobre a segurança rapidamente

Faça a ingestão de dados usando os formatos de esquema na gravação e esquema na leitura para obter o desempenho ideal nas consultas e a flexibilidade de poder adicionar ou alterar campos após a ingestão. Traga os resultados para os dashboards em questão de segundos com a velocidade pela qual o Elastic Stack é conhecido. Acabe com a fadiga do alerta com correlações priorizadas.

## Inclua anos de dados históricos

Utilize snapshots buscáveis para acessar de maneira econômica todos os dados de segurança necessários para inclusão em detecções, contexto investigativo, caça a ameaças, monitoramento de nuvem e muito mais. Defina o escopo de violações com tempos de permanência de meses ou até anos.

## Reduza os tempos de permanência

Automatize os processos com detecções prontas e mapeadas pela MITRE, desenvolvidas pela equipe interna de pesquisa de segurança da Elastic, e detecções personalizadas que aproveitam a poderosa e intuitiva Event Query Language (EQL) para realizar correlações que detectam ferramentas, táticas e procedimentos de ameaças avançadas.

## Encontre atividades anômalas maliciosas

Aplique trabalhos de machine learning não supervisionados a qualquer fonte de dados com um registro de data/hora para identificar anomalias autônomas ou anomalias associadas que constituam uma ameaça em potencial. Combine machine learning supervisionado e não supervisionado para detectar métodos como algoritmos de geração de domínio (DGAs) com baixas taxas de falso positivo.

## Simplifique os fluxos de trabalho das operações de segurança

Use o espaço de trabalho interativo do Elastic Security para detectar e responder a ameaças, fazer a triagem de eventos e reunir evidências em uma linha do tempo interativa e intuitiva. Aproveite o gerenciamento de caso integrado e a integração com os principais fornecedores de orquestração, automação e resposta de segurança (SOAR) e fluxo de trabalho para acelerar a resposta e a resolução.

## Implemente o SOC moderno

O Elastic Security atua como a base tecnológica das equipes de segurança modernas em todos os lugares. A abordagem de plataforma aberta da Elastic para a segurança proporciona facilidade de integração, flexibilidade e a possibilidade de aproveitar contribuições e colaborações orientadas pela comunidade para ajudar as equipes de SOC a evoluir rapidamente e tomar decisões melhores e mais rápidas.

# Conclusão

Enquanto as equipes de segurança protegem suas organizações contra um cenário de segurança em constante expansão, elas não devem perder de vista a necessidade de permanecer operacionalmente eficientes. Com acesso a todos os dados relevantes para a segurança e métodos econômicos para acessar dados históricos, você pode resolver mais casos de uso implantando o Elastic Security como seu SIEM e aumentar o valor operacional da sua implantação de SIEM de forma geral. **As maiores equipes de segurança estão escolhendo o Elastic Security como seu SIEM porque precisam de uma abordagem unificada para detecção, prevenção e resposta.**

A Elastic fornece visibilidade holística em todo o ambiente com velocidade e eficiência para identificar e resolver problemas, oferece escalabilidade na nuvem em todo o seu ambiente híbrido e permite que seu SOC alcance máxima eficiência, independentemente de como as equipes estejam distribuídas ou em quantos silos operem hoje. Mantenha sua empresa protegida com uma nova abordagem para o SIEM com o Elastic Security.

# Quer conhecer melhor o Elastic Security?

Experimente o Elastic Security no Elastic Cloud (14 dias grátis, sem necessidade de cartão de crédito). Ou implante-o no local — nessa opção, ele é sempre gratuito.

**Iniciar o Elastic Security gratuito** ⟶

Search. Observe. Protect.

© 2021 Elasticsearch B.V. Todos os direitos reservados.

A Elastic torna os dados utilizáveis em tempo real e em escala para busca empresarial, observabilidade e segurança. As soluções da Elastic são desenvolvidas sobre uma única stack de tecnologia aberta e gratuita que pode ser implantada em qualquer lugar, possibilitando a obtenção de insights práticos instantaneamente de qualquer tipo de dados — desde encontrar documentos até monitorar a infraestrutura e caçar ameaças. Milhares de organizações em todo o mundo, incluindo Cisco, Goldman Sachs, Microsoft, The Mayo Clinic, NASA, The New York Times, Wikipédia e Verizon, usam a Elastic para operar sistemas de missão crítica. Fundada em 2012, a Elastic tem suas ações negociadas publicamente na NYSE sob o símbolo ESTC. Saiba mais no website elastic.co/pt.

ESCRITÓRIO DA EMPRESA PARA AS AMÉRICAS
800 West El Camino Real, Suite 350, Mountain View, Califórnia 94040
Telefones: +1 650 458 2620 (geral), +1 650 458 2625 (vendas)

info@elastic.co