>RESUMO DA SOLUÇÃO_

Cribl Search

O DESAFIOE

Tradicionalmente, as equipes de TI e segurança que buscavam obter respostas a partirde seus dados precisavam enviar, ingerir e armazenar os dados antes de consultá-los, o que resultava em menor visibilidade dos dados, custos mais altos e maior complexidade logística.

A SOLUÇÃO

O Cribl Search realiza consultas de busca federada diretamente no local, em quaisquer dados, em qualquer formato e em qualquer lugar, aumentando o escopo da análise sem exigir o custo ou a complexidade do envio, ingestão e armazenamento prévios dos dados.

OS BENEFÍCIOS

- Obtenha acesso a dados que você não tinha antes ter acesso a antes.
- Implemente uma funcionalidade de busca única e independente de sistema para facilitar o uso.
- Reduzir custos e horas de trabalho É necessário contar com uma equipe dedicada para gerenciar cada ferramenta de busca proprietária.
- Permite resultados de pesquisa concentrados serem reinseridas em sistemas de análise existentes ou armazenadas para fins forenses ou de auditoria.
- Elimine a sobrecarga mental e operacional de determinar o que fazer com seus dados.with your data.

O Cribl Search revoluciona o processo de busca tradicional, oferecendo um mecanismo de processamento federado de busca in-place que acessa dados de qualquer fonte ou meio de armazenamento em qualquer formato, usando uma interface de consulta única e intuitiva. Ele permite explorar dados em qualquer lugar e trabalhar com outros produtos para encaminhá-los no formato correto, uma funcionalidade cha.

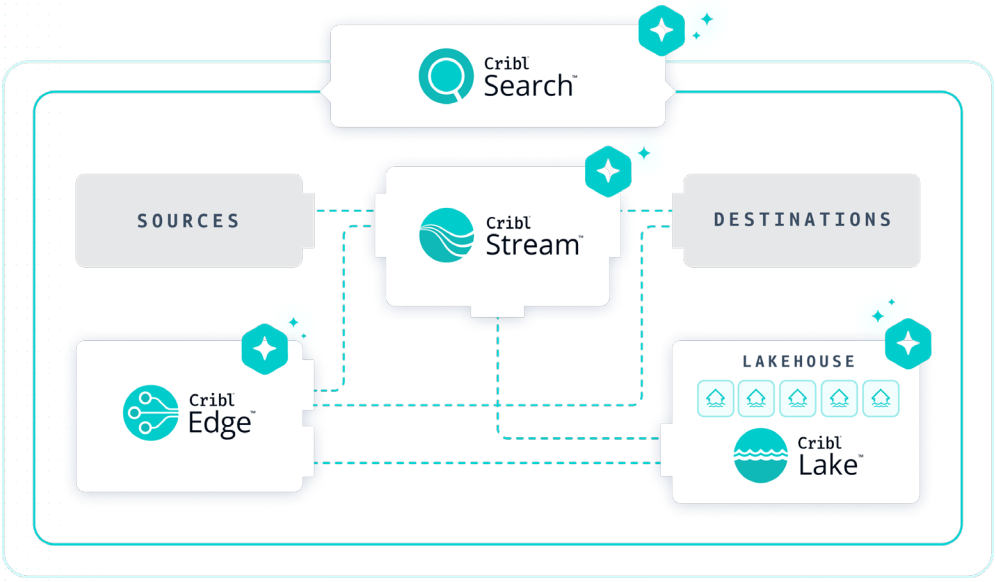
O desafio

O volume de dados — e o número de fontes de dados — está crescendo ano após ano, mas As empresas estão utilizando cada vez menos dados, em alguns casos menos de 2%. A grande maioria dos dados permanece invisível e inutilizada porque é caro e impraticável pesquisá-los. Pense bem: você precisa coletar os dados em questão, pagar para movê-los e armazená-los em algum lugar e, em seguida, consultar esses dados — tudo isso enquanto reza para que a divindade de sua escolha encontre a agulha no palheiro.

Além disso, as ferramentas atuais têm dificuldades para realizar consultas universais. A busca federada não é um conceito novo, mas muitas das principais tecnologias de busca ainda se limitam a consultar com eficiência dados armazenados em um único fornecedor. As equipes de segurança e TI precisam de uma maneira independente de fornecedor para consultar seus dados de forma eficiente e com bom custo-benefício,aumentando a eficiência e melhorando os resultados do SOC.

A Solução Cribl

Cribl Search é uma nova abordagem inovadora para encontrar e acessar dados, independentemente de onde estejam armazenados, em qualquer formato ou localização — na borda da rede, em um data lake ou até mesmo em um endpoint de API. Isso amplia o escopo de análise dos usuários sem a necessidade de enviar, ingerir e armazenar os dados previamente, fornecendo informações relevantes e valiosas que são encaminhadas para análises adicionais somente quando necessário.



Fornecedor da Cribl Search- abordagem agnóstica para busca federada simplifica custos e garante que sua equipe tenha tempo para trabalhar no que Realmente importa.

A Busca Cribl utiliza a busca federada, permitindo que os usuários consultem múltiplas fontes de dados simultaneamente, apresentando os resultados em uma única interface unificada. A busca oferece uma maneira simples e econômica de consultar seus dados, para que você obtenha os insights de que precisa. Em grande escala.

O Cribl Search oferece integração imediata com todo o conjunto de produtos da Cribl, bem como com Amazon S3, Amazon Security Lake, Azure Blob, Google Cloud Storage, AWS OpenSearch e outros armazenamentos de dados compatíveis. Além disso, utilize a busca em endpoints de API, com diversas configurações padrão, bem como um coletor REST genérico definido pelo usuário.

A integração com o Cribl Lake oferece uma solução completa de data lake que permite às organizações armazenar, gerenciar, aplicar políticas e pesquisar dados com facilidade. O Cribl Lake utiliza formatos abertos — sem necessidade de esquemas predefinidos —, unifica a segurança com controles de acesso avançados e centraliza o acesso a todos os dados de TI e segurança. O Cribl cuida de toda a parte complexa, permitindo que os dados sejam armazenados, pesquisados e encaminhados facilmente para as equipes e ferramentas necessá Preciso disso.

A integração com o Cribl Stream e o Edge proporciona roteamento, modelagem e busca de dados adicionais entre os quatro sistemas, bem como busca de dados entre os quatro produtos. O Cribl Edge também permite o teletransporte direto dos resultados da busca para os endpoints, para investigação adicional.

Aspectos da Busca Cribl

Obtenha visibilidade de dados aos quais você não tinha acesso antes.

Quanto mais dados você tiver, mais difícil será visualizá-los por completo. Dependendo de onde esses dados estiverem armazenados, você pode não conseguir acessar os dados necessários para a sua consulta. O Cribl Search oferece às equipes de TI e Segurança o poder de coletar, processar e consultar dados em qualquer lugar — seja em trânsito, em um data lake ou na borda da rede.

Pesquise facilmente dados de vários fornecedores em uma única interface.

Os fornecedores de mecanismos de busca tradicionais geralmente têm limitações quanto ao número de ferramentas que podem utilizar para realizar consultas. Administradores e desenvolvedores, então, precisam criar painéis de controle para avaliar os resultados de forma abrangente, o que consome tempo que poderia ser dedicado a iniciativas estratégicas. O Cribl Search oferece às equipes o poder da busca federada, permitindo que os usuários consultem várias fontes de dados simultaneamente e reúnam os resultados em uma única interface de usuário.

O Cribl Search oferece às equipes de TI e Segurança o poder de coletar, processar e analisar dados em qualquer lugar – seja em trânsito, em um data lake ou na borda da rede.

A integração com o Cribl Lake, incluindo o nível de alto desempenho do Lakehouse, fornece uma solução de data lake pronta para uso que permite às organizações armazenar, gerenciar, aplicar políticas e pesquisar dados com facilidade.

A logística de dados é cara e demorada. Fazer perguntas aos seus dados é um processo que exige investimento: pagase para coletar, para armazenar e por consulta. E a execução de tudo isso costuma ser complexa, exigindo muitas horas de trabalho e experiência específica da equipe com ferramentas proprietárias. A abordagem agnóstica de fornecedores da Cribl Search para busca federada simplifica os custos e garante que sua equipe tenha tempo para trabalhar no que realmente importa.

Elimine a sobrecarga mental e operacional de determinar o que fazer ou onde armazenar seus dados.

Quando você usa ferramentas legadas ou precisa coletar, armazenar e consultar dados em várias plataformas, muitas perguntas surgem. De qual fonte esses dados serão coletados? Qual a melhor maneira de coletá-los? Depois de obtêlos, onde devo armazená-los? Quanto essa outra ferramenta cobrará por consulta? O Cribl Search elimina a sobrecarga mental e operacional de descobrir o que fazer com seus dados. Use uma única ferramenta para consultar dados onde quer que eles estejam, reduzindo o estresse, os custos e a complexidade.

Os Pacotes de Busca permitem acelerar a integração e tempo para obter valor.

Os pacotes são conjuntos predefinidos que fornecem um mecanismo para empacotar, compartilhar e instalar painéis e configurações que se alinham a uma determinada fonte de dados ou são construídos em torno de casos de uso comuns. Os pacotes também fornecem exemplos de referência que os clientes podem inspecionar, analisar por meio de engenharia reversa e aproveitar para atender a requisitos organizacionais específicos. Os pacotes podem ser baixados do nosso repositório e implementados em suas instâncias de Busca. Os usuários também podem criar novos pacotes para compartilhar funcionalidades facilmente com outros usuários e equipes. Os pacotes são a maneira mais rápida de maximizar o valor do seu investimento em Busca..

O Notebook reúne pesquisas, visualizações e anotações em um único espaço de trabalho para investigações mais rápidas e colaborativas.

Os analistas podem combinar consultas, gráficos, texto e histórico de pesquisa para explorar os resultados em profundidade — sem precisar consultar repetidamente as fontes de dados subjacentes — economizando tempo e dinheiro. As equipes podem refinar as pesquisas, segmentar os dados para obter insights mais profundos e aplicar Enriquecimento e transformações conforme necessário. Anotações integradas, edição colaborativa, indicadores de presença e controle de versão criam um histórico de investigação colaborativo e auditável. A assistência de IA resume os principais resultados e insights. Juntas, essas funcionalidades fornecem um histórico de investigação claro que melhora a eficiência, a precisão e a colaboração nos fluxos de trabalho de resposta a incidentes, além de ajudar as equipes a responder às suas perguntas mais complexas sobre dados.

Resumo

A maior parte dos dados criados é subutilizada, o que leva à diminuição da visibilidade dos dados. Além disso, pesquisar todos os dados é caro e impraticável: primeiro é preciso coletá-los, armazená-los e indexá-los. Ademais, muitas das principais tecnologias de busca ainda se limitam a consultar com eficácia dados armazenados em um único fornecedor.

O Cribl Search é uma ferramenta de análise independente de fornecedores que realiza consultas de busca in-place, permitindo a pesquisa em múltiplas fontes de dados simultaneamente, apresentando os resultados em uma única interface unificada. Quando as equipes usam o Cribl Search, elas:

- Obter acesso a dados aos quais eles não tinham acesso antes.
- Implemente uma funcionalidade de busca única e independente de sistema para facilitar o uso.
- Reduzir custos e horas de trabalho necessárias para que uma equipe dedicada gerencie cada ferramenta de busca proprietária.
- Elimine a sobrecarga mental e operacional de determinar o que fazer com seus dados.

Cribl Search: primeiros passos.

Para começar a usar o Chronicle e a Busca do Cribl hoje mesmo, **clique aqui para se inscrever no Cribl.Cloud. Comunidade do Cribl no** Slack É também um ótimo lugar para se conectar com líderes de outras equipes que utilizam o conjunto de produtos Cribl.

SOBRE CRIBL

A Cribl, o mecanismo de dados para TI e segurança, capacita as organizações a transformarem sua estratégia de dados. Os clientes usam as soluções independentes de fornecedores da Cribl para analisar, coletar, processar e rotear todos os dados de TI e segurança de qualquer origem ou destino, oferecendo a escolha, o controle e a flexibilidade necessários para se adaptarem às suas necessidades em constante mudança. O conjunto de produtos da Cribl, usado por empresas da Fortune 1000 em todo o mundo, foi desenvolvido especificamente para TI e segurança, incluindo o Cribl Stream, O principal pipeline de observabilidade do setor, Cribl Edge, um agente inteligente independente de fornecedores e a Busca Cribl, A primeira solução de busca local do setor. Fundada em 2018, a Cribl É uma empresa com foco em trabalho remoto, mas com um escritório em São Francisco, Califórnia.

Saiba mais: www.cribl.io | Experimente agora: Caixas de areia Cribl |
Junte-se a nós: Comunidade Slack | Siga-nos: LinkedIn and X

SB-0014-PT-7-1125