
[E-BOOK]
Observability na prática:
3 histórias de sucesso da DataRunk
DataRunk

Apresentação

As novas abordagens de desenvolvimento e até mesmo tecnologias dirigiram a transformação digital e inovação, mas têm **impactado a capacidade de visualizar o desempenho e a segurança** do ambiente de TI. É inviável captar, analisar e agir diante da extensão e complexidade.

O preço dos pontos cegos é a **falta de proatividade na gestão, quando não áreas expostas a ataques.** E o cenário não deve estagnar. A complexidade vai aumentar.

Ainda assim, as **ferramentas de monitoramento e análise são fragmentadas na maioria das organizações.** Não há uma fonte única e segura de informação, em tempo real. Ao contrário, as organizações têm dificuldades de correlacionar os eventos capturados pelas várias ferramentas que adotam.

A observability e a segurança, centradas em uma plataforma unificada, com poucas e robustas ferramentas, têm sido a tendência para lidar com essa questão. De acordo com estudo do segmento, 68% das organizações brasileiras entrevistadas citaram esse objetivo.

A DataRunk tem ajudado várias organizações a realizar esse projeto. Neste e-book, você vê **três dessas histórias de sucesso,** que ajudarão a inspirar e direcionar seus esforços.

Boa leitura!

DataRunk

CASE 1:

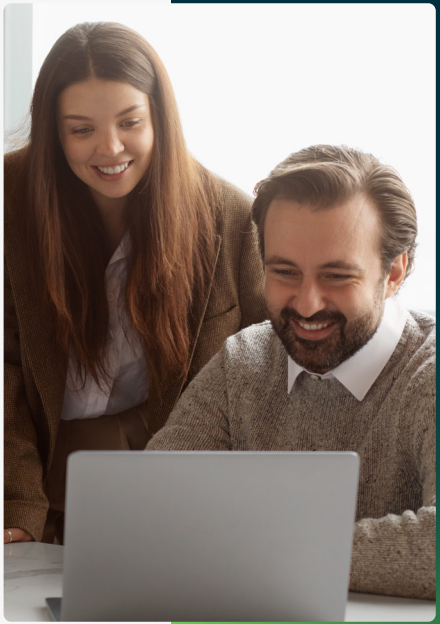
Como uma fintech estruturou o monitoring Splunk com a DataRunk

Segmento:

Financeiro

Soluções:

Cartão de crédito, plataforma de pagamento e serviços bancários, acquiring e prevenção a fraude



DataRunk

Desafios

As ferramentas de monitoramento da fintech eram muito básicas e ineficientes, inviabilizando uma postura proativa na descoberta de anomalias. A empresa dependia da abertura de chamados dos clientes para identificar problemas.

Resultados-chave

Visibilidade sobre anomalias e proatividade na resposta a incidentes antes de que eles produzam paradas nas operações de clientes. Envio de informações sobre infraestrutura para clientes para tomada de decisões de negócio. Setor como referência para a empresa.

Transformando dados em resultados

- Diminuição no tempo de descoberta de anomalias
- Proatividade no gerenciamento de anomalias
- Embasamento de melhorias nas aplicações
- Melhoria reputacional da empresa
- Novos projetos

Como a DataRunk implantou uma abordagem consistente em monitoramento com Splunk

Nesta fintech, o NOC – Centro de Operações de Rede é responsável por manter em funcionamento aplicações que rodam em mais de 600 instâncias.

Porém, antes da Splunk, o setor tinha capacidade limitada de monitorar proativamente esse ambiente, dependo dos chamados dos clientes para saber que algo não estava funcionando.

A equipe **precisava de uma visão centralizada e em tempo real da integridade, bem como de informações sobre o desempenho dos sistemas de forma rápida e simples.**

Implementando Splunk para monitoria dos sistemas

A fintech tinha experiências com Splunk e, inicialmente, criou visões com o que sabia da ferramenta, validando a ideia. No entanto, sozinha, não tinha expertise e pessoal para conseguir escalar e dar a atenção especial ao projeto, de acordo com o IT Manager do projeto.

A empresa encontrou na consultoria em Observability da DataRunk, empresa Splunk Core Certified, o apoio. A DataRunk imergiu no ambiente da fintech, entendendo a operação em todo o seu funcionamento em vivência direta com o time.

As **principais aplicações da fintech foram mapeadas e distribuídas em uma matriz de maturidade em monitoria.**

As necessidades iniciais eram **métricas como maior volume de transações, variações no retorno de erros e variações no tempo de performance.**

O roadmap priorizou a **implementação por camadas, da infraestrutura até o negócio.** Para visualizar essas informações de maneira organizada, a **DataRunk criou os dashboards.**

Para a monitoria levar automaticamente à gestão dos alertas, a DataRunk desenhou a comunicação com as equipes e com os clientes.

> Começamos pelo básico. Primeiro, monitoramos a infraestrutura. Depois, os servidores. Depois, as aplicações. Fomos fazendo passo a passo. Olhamos a camada de infraestrutura, a camada de aplicação e a camada de negócio por partes. Fomos fazendo nessa sequência. A partir do momento que íamos avançando, ganhávamos detalhes e mais efetividade.
>
> **IT Manager**

Monitoria que se reflete na qualidade das aplicações e nas decisões de negócio

A estruturação da monitoria tornou o NOC proativo. **A partir de comportamentos anômalos, eventos são previstos antes de que produzam efeitos** sobre os usuários, dando segurança. De acordo com o IT Manager da fintech, "o cliente passou a olhar o time da operação de outra maneira".

Internamente, os insumos do trabalho são acessados pelas equipes de produto, para melhorias nas aplicações. Para a equipe de antifraude, foi o início de um grande projeto.

Entendemos onde e em que momento podemos atacar. Por meio das informações da monitoria, ajudamos o time de desenvolvimento a acertar a aplicação. Não tínhamos visão do número de alertas por dia. Com a monitoria tivemos noção de quantos alertas recebíamos por dia, quais aplicações tinham mais alertas e precisavam de uma atenção especial.

IT Manager

DataRunk

DataRunk

CASE 2:

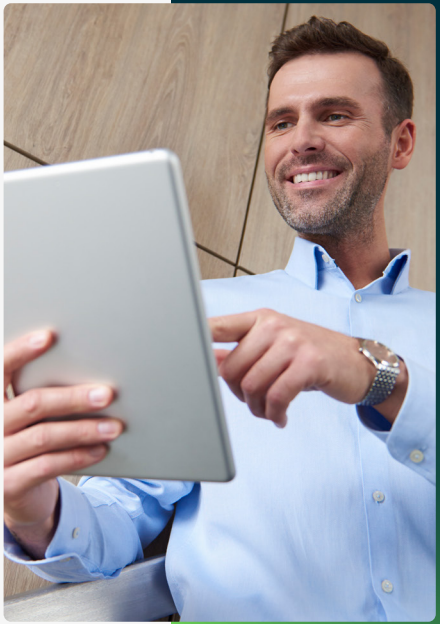
Como a maior plataforma de negociação de dívidas do país passou a monitorar anomalias no comportamento dos usuários, com a consultoria da DataRunk em Splunk

Segmento:

Financeiro

Soluções:

Cartões de crédito, empréstimo, carteira digital, consulta de débitos CNPJ e CPF, intermediação entre consumidor e empresas detentoras de dívidas



DataRunk

Desafios

A empresa queria garantir que a continuidade de cada step das negociações de seus clientes não fosse afetada por incidentes que levassem a comportamentos incomuns ou inesperados dos usuários. Disso surgiu a demanda por um monitoramento no nível de comportamento do usuário na plataforma.

Resultados-chave

Com Splunk, a plataforma tem a capacidade de descobrir problemas na experiência do usuário em tempo real. Refazer o caminho até a causa do problema também é mais fácil, correlacionando com ocorrências em outras camadas da aplicação.

Monitoramento do comportamento do usuário em tempo real

- Facilidade na análise de comportamentos incomuns
- Correlação de problemas entre as várias camadas da aplicação
- Melhorias na experiência do usuário
- Estabilidade na disponibilidade dos serviços
- Aproveitamento adequado dos recursos do Splunk

Como a plataforma de negociação de dívidas monitora o comportamento dos usuários com Splunk

Para a empresa detentora da maior plataforma brasileira de intermediação de dívidas, **compreender os padrões de uso dos usuários é fundamental para analisar preferências e descobrir produtos** mais eficazes, mas também incidentes que podem afetar o sucesso de uma negociação.

Para isso, a empresa **estruturou um projeto para dar foco adicional a essas rotinas,** usando as devidas ferramentas, construindo uma equipe dedicada e desenhando os processos adequados.

Usando Splunk para monitorar o comportamento dos usuários

O Splunk surgiu como uma alternativa natural para o projeto. A empresa começou montando uma **equipe de monitoria de real-user,** responsável pelo levantamento das métricas e eventos a serem monitorados, bem como desenvolvimento da coleta dos dados e criação dos dashboards.

Ao longo do tempo, veio a **necessidade de ajuda especializada.** A DataRunk surgiu como a parceria necessária para escalar o projeto.

Inicialmente, foi feita a **revisão do que já havia sido construído e o levantamento das novas necessidades** de monitoramento.

A equipe desenvolveu as **regras de análise dos dados no Splunk,** bem como **visualizações, funis de evento, dashboards de indicadores, alertas de detecção de anomalias, alertas comportamentais para análise de volumetria dos produtos,** criando uma visão detalhada dos produtos.

A contratação da DataRunk para apoiar no uso do Splunk foi um game changer no projeto. Sozinhos não teríamos conseguido em tão pouco tempo aproveitar a ferramenta do jeito que aproveitamos hoje. Mesmo que eles fizessem a mesma que tínhamos feito, era muito melhor.

IT Manager

Fluxos de negociação dentro do esperado

Se algum incidente ou modificação nos sistemas da empresa leva a um problema no nível do usuário, a **equipe identifica no minuto seguinte.**

A **análise de causa também fica facilitada** dentro do Splunk, acelerando a restauração ou ajuste do serviço.

Comportamentos incomuns no nível do usuário levam a equipe a aprofundar a análise e investigação para entender problemas em outros níveis da aplicação, como na infraestrutura e em segurança.

A nível de negócio, a empresa também consegue extrair dados sobre seus produtos, como volumetria de transações.

Se nós fazemos um release e acontece algum problema no nível do usuário, nós sabemos no minuto seguinte. Com o acompanhamento, a descoberta de incidentes é em tempo real. Mais que isso, nós temos a facilidade de refazer o caminho executado para conseguirmos restaurar novamente o serviço.

IT Manager

DataRunk

DataRunk

CASE 3:

Como o maior ATM manager usa inteligência artificial no monitoramento e operação de TI com Splunk ITSI, com consultoria da DataRunk

Segmento:

Financeiro

Soluções:

ATM manager, switch de pagamento e open banking as a service

DataRunk

Desafios

Mais de 30 ferramentas para fazer a monitoração de um ambiente complexo e multicloud. Monitoramento baseado em thresholds fixos, que levava ao excesso de falsos positivos ou à detecção apenas de situações-limite. Dificuldade de relacionar os alertas com os respectivos eventos, para a distribuição entre as equipes.

Resultados-chave

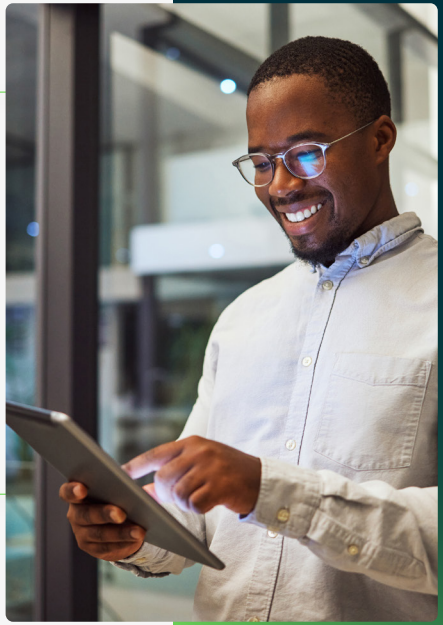
Com os thresholds adaptativos, a empresa ganhou facilidade de visualizar o comportamento de cada servidor individualmente, bem como do todo, por meio de métricas e entidades de monitoração automaticamente acompanhadas.

O comportamento dos servidores é monitorado proativamente e, antes que aconteça algum problema, a equipe já consegue identificar as anomalias comportamentais.

Com mais visibilidade, os alertas vêm com menos ruído. Picos repetitivos são agregados em um único episódio a ser acompanhado de acordo com a severidade. Cada chamado aberto é de fato consumidor de ticket, seja para uma ação proativa, seja para uma reação rápida do time.

Monitoramento e operação de TI com Splunk ITSI

- Integração das diversas camadas de TI
- Thresholds adaptativos
- Machine learning e automação na distribuição de alertas
- Automação de análise de causa raiz e tratativas.



Implantação do ITSI com Splunk dentro de um ambiente multicloud

O primeiro passo do roadmap foi a consolidação das ferramentas, cuja decisão foi **centralizar no Splunk.** A ferramenta foi avaliada como a mais flexível para se adaptar ao negócio da empresa, com diversas aplicações e diversos fornecedores.

O segundo passo foi o **setup do ambiente Splunk e a indexação de dados** para os primeiros projetos de monitoração, que foi realizada com a consultoria da DataRunk. São centenas de GBs de dados indexados na base Splunk diariamente.

O terceiro ponto foi a **construção dos dashboards e de toda a inteligência por debaixo deles para que fossem acionados** de forma automática para todo o ambiente.

Foram desenhados e construídos diversos dashboards. As equipes começaram a ter a **visão pela primeira vez de todas as métricas de infraestrutura reunidas, de forma up-to-date e em tempo real.**

A DataRunk nos ajudou na adequação da configuração do ambiente Splunk. Isso nos trouxe entendimento de diversos processos e, ao mesmo tempo, de que a nossa infraestrutura não tinha capacidade suficiente para atender a quantidade de itens indexados, levando à instalação de novos servidores físicos.

IT Manager

DataRunk

Prepare-se para a observability

A observability não é uma competência que você pensa apenas ao final do projeto. Ela deve ser considerada desde o início e, depois, exige trabalho duro para ser implementada.

Você precisa de **arquitetos** para fazer o design, de **desenvolvedores** para montar a estrutura, de **operações** para garantir os gatilhos de alerta certos, da **empresa** para definir claramente o que ela precisa e de uma **estratégia** para avaliar o comportamento e o impacto nos negócios.

Conforme o projeto avança para as fases de desenvolvimento e teste, você deve continuar a avaliá-lo, buscando **medidas para estabelecer o sucesso,** assegurar que as métricas sejam capturadas em saídas de logs/metrics/traces e se certificar de que suas aplicações não permaneçam em silos, mas sim correlacionadas de acordo com as funções de negócio.

É preciso fôlego, além de grandes ferramentas e experiência, para viabilizar um projeto dessa extensão. Mas **o benefício de transformar dados em valor paga o esforço.**


DataRunk
VAMOS JUNTOS?
Quer contar com a experiência da DataRunk no projeto?
Traga sua ideia para a DataRunk