realprotect

CASO DE SUCESSO

Banco soluciona caso de fraude a partir de análise em Big Data com Splunk Enterprise

A Segurança é hoje uma das maiores preocupações de qualquer empresa do setor financeiro. Bancos, fundos de investimento, seguradoras, dentre outros, precisam proteger suas informações, as informações dos clientes e assegurar que as operações do negócio sejam realizadas de forma segura, algo muito importante para a reputação e para a continuidade do negócio.

Usuários e empresas comunicam fraudes em cartões de crédito

O banco começou a receber uma série de notificações de usuários e empresas alegando que os cartões de crédito foram fraudados e utilizados por criminosos. O grande volume de comunicados gerou um alerta de que essa fraude poderia ser um golpe de um único grupo. Para compreender melhor a ambrangência e o impacto da fraude era necessário coletar e correlacionar uma enorme quantidade de dados de transações bancárias, a fim de identificar o processo de fraude e recomendar as ações de remediamento.

O Desafio

Ao detectar uma grande fraude envolvendo cartões de crédito, o banco precisava receber uma enorme quantidade de dados de diversas transações para realizar o correlacionamento, com o objetivo de identificar: pontos de convergência, abrangência e impacto da fraude e recomendar ações de remediamento.

A Solução

Como a análise dos dados envolvia grande quantidade de dados não-estruturados, vindos de diferentes fontes era preciso uma plataforma que permitisse o correlacionamento desses dados, de forma escalonável, com facilidade e agilidade. Para isso, foi utilizado a plataforma de Big Data Splunk.

Os Benefícios

A partir da facilidade proporcionada pela plataforma Splunk, foi possível coletar todos os dados necessários em apenas 30 minutos. O relatório gerencial para a empresa e para as autoridades, contendo a análise da fraude e as medidas a serem tomadas ficou pronto em 7 dias. O banco obteve inteligência para reavaliar a tecnologia utilizada pelos cartões de crédito.

Splunk é utilizado como plataforma de Big Data

A solução encontrada para cumprir os objetivos do projeto de análise anti-fraude do banco foi a plataforma de dados de máquinas Splunk. O Splunk Enterprise conta com uma grande variedade de possibilidades de busca, visualização e conteúdo pré-elaborado para uso em casos variados, onde qualquer usuário pode facilmente utilizar e extrair insights de acordo com suas necessidades.

Os dados de transações bancárias necessários foram coletados em menos de 30 minutos.
É importante ressaltar que esses dados não estavam estruturados e também era oriundos de fontes diferentes. Por esses motivos a opção por uma plataforma de Big Data foi tão importante.

Análise e recomendações em apenas 7 dias

Após a coleta dos dados, foram analisados aproximadamente 5 milhões de registros. Foi constatado um impacto em 650 cartões corporativos e de usuários finais. Em apenas 7 dias a equipe pode produzir um relatório gerencial para a empresa e para as autoridades responsáveis para a prisão dos fraudadores. A análise de anti-fraude também foi útil para a reavaliação da tecnologia utilizada pelos cartões.

Próximos passos

O próximo passo do projeto para incrementar a segurança do banco é monitorar as transações em tempo-real, a partir de um SOC (Security Operations Center) operado em Big Data com a plataforma Splunk. Dessa forma será possível identificar desvios, gerando alertas de segurança, no momento em que eles ocorrem.

O monitoramento realizado a partir de um SOC é fundamental, pois a análise e correlacionamento de logs feitos por profissionais de segurança, certificados, treinados e especializados, diminui o tempo de identificação de fraudes e outros incidentes de segurança, tornando o processo de mitigação do risco mais inteligente.

Sobre a Real Protect

A Real Protect é referência nacional em Segurança da Informação, auxiliando empresas a conectar a Segurança ao negócio, reduzindo riscos e otimizando seus investimentos em segurança. Há mais de 10 anos no mercado prestando serviços com o mais alto nível de excelência, a Real Protect foi a primeira empresa na América Latina a obter a certicação UCS da MSP Alliance.