CASE STUDY

Optimizing data ingestion & SIEM costs for a US cybersecurity technology firm

$254k

saved annually in SIEM licensing and data storage costs

38%

volume reduction leveraging out-of-the-box volume control library

2 weeks

time taken to deliver savings in SIEM licensing costs

KEY FINDINGS

- A US cybersecurity technology firm which serves institutional clients by providing digital security tools was looking to better manage its ballooning data growth
- Saved **$204k** in SIEM license costs via DataBahn's purpose-built data volume reduction capabilities and an additional **$50k** in data storage and infrastructure costs
- Delivered a **38% reduction** in just **two weeks** by using DataBahn's pre-populated volume control library to filter out irrelevant noise data

Introduction

This US cybersecurity technology firm serves a wide variety of institutional clients with digital security tools. Before the introduction of DataBahn, this company was relying on Microsoft Sentinel as its next-generation System Information and Event Management ("SIEM") solution for SOC operations. They were faced with a high rate of data volume growth, cost management, and data collection challenges.

The customer on any given day ingested data at the rate of 1.15TB daily with a data retention need of 365 days. They had even tried a Data Management and Observability solution for 4 months, but had not achieved substantial log reduction. They faced the following challenges:

Data Growth and Escalating Costs

The firm's security and event data ingestion volume was growing at a rapid rate of 18% annually due to the continuing migration of all their applications and assets to cloud storage. This resulted in increased SIEM licensing and storage costs within a 12-month period.

Unpredictable Data Volumes

Sentinel SIEM licensing costs were not just growing with data volumes, but were also unpredictable due to data spikes. This strained the security budget of the SOC and made allocating bandwidth and resources to strategic initiatives.

Data Collection and Ingestion

The firm found intermittent log collection with on-premise and cloud-to-cloud data collection challenging while using Sentinel forwarders and legacy syslog relay servers.

The Firm needed to **revamp their security data management** to keep up with the data growth, **reduce SIEM licensing and data storage costs**, and **make it easier for the SOC to manage on-premise and cloud data collection.**

They leveraged a **Data Management and Observability tool** to manage and lower their security data costs for 4 months, but the log reduction delivered by that tool was minimal, and was barely able to keep up with the data growth.

What they needed was a tool **designed and built to better manage security data and logs**, to send only **security relevant events to Sentinel**, **route non-relevant data to blob storage**, and **replace legacy log collection**. They also needed volume control rule-sets to segregate relevant and irrelevant data during collection to better manage SIEM and licensing costs.

DataBahn’s Security Data Fabric

In just 2 weeks after deployment, DataBahn was able to optimize log collection for the firm and route non-relevant logs and data to blob storage while sending only security-relevant data to Sentinel. Legacy log collection infrastructure was replaced with a DataBahn-driven data ingestion system.

Reduced SIEM licensing costs

DataBahn enabled the firm to reduce their SIEM consumption by 38% in a 2-week period, resulting in annual savings of $204k. The Security Engineers at the firm leveraged DataBahn’s volume reduction rule library to filter which data was being ingested into the SIEM, focusing on enabling rules which drove only data relevant to their detection and hunting needs. This reduced the noise from the event set.

Efficient and Predictable Data Ingestion

The firm focused on ingesting only essential event types into the SIEM, aligning the data more effectively with compliance and analytics use-cases - and avoiding unpredictable data volumes from being ingested into the SIEM and ballooning Sentinel costs.

Saving on Long-term Storage Costs

The firm saved an additional $50k annually in long-term storage costs by optimizing its storage strategy. They leveraged DataBahn to predict storage needs, remove unwanted metadata from raw messages, and deduplicating data sets presents in multiple data stores.

In summary, the implemention of DataBahn revolutionized the data management landscape for the US cybersecurity firm. The solution not only helped the firm address the challenges posed by rapidly growing data but also contributed to substantial cost savings, improved data quality, and streamlined operational processes, ultimately enhancing their overall security posture.

Delivering such substantial log volume reduction of 38% in just 2 weeks was possible due to DataBahn’s extensive out-of-the-box volume control library of rules. The system is also set up and designed to deliver real-time insights into data usage and track security relevance, so that the SOC can create and implement new rules to ensure even greater optimization on SIEM licensing costs.

DataBahn.ai’s Data Fabric empowers organizations to optimize data management, reduce costs, and enhance security and IT operations. By integrating AI readiness, addressing IT observability challenges, and offering flexible solutions, the platform delivers significant operational efficiencies and strategic benefits, setting a new benchmark for cybersecurity data management in the digital age.

Learn more at **databahn.ai**

DATABAHN