CASE STUDY

Redefining security data architecture for a US Investment Management firm

$350k

saved annually in SIEM licensing and data storage costs

70%

improvement in time to onboard new data feeds into the SIEM

40%

improvement in overall detection coverage

KEY FINDINGS

- A US investment management firm used DataBahn to revamp their data pipelines and create a new data ingestion layer to orchestrate data to their SIEM, data warehouse, and long-term storage
- Saved **$300k** in SIEM license costs via DataBahn's purpose-built data volume reduction capabilities and **$50k** in data storage and infrastructure costs
- Delivered a **70% improvement** in time to onboard new data feeds into the SIEM, reducing the time and effort internal teams had to put into each integration
- Improved overall detection coverage by **40%**

Introduction

This US investment management firm serves institutional clients including pension funds, endowments, foundations, foreign governments, and central banks. Before the introduction of DataBahn, the firm was relying on two technologies - a leading next-generation Security Information and Event Management ("SIEM") for Analytics and Security Operations Center ("SOC") operations, as well as Snowflake for long-term data storage. These tools played a crucial role in managing security events and data within the organization.

The customer on any given day ingested data at the rate of 60,000 events per second (roughly 4.3TB daily) with a data retention need of 365 days. Before DataBahn, the customer had the following challenges.

Data Growth and Escalating Costs

The firm's security and event data ingestion volume was growing at a rapid rate of 10% annually, resulting in increased SIEM licensing and storage costs within a 12-month period. This increasing cost also strained their budget and came at the opportunity cost of the SOC being able to focus on strategic initiatives to improve their security posture and preparedness.

Monitoring High-Volume Data Feeds

The firm found it challenging to continually monitor high-volume data feeds, particularly from endpoint sources such as Carbon Black and Network data (Flow). These challenges were primarily due to concerns about SIEM license expansion.

Data Duplication and Inconsistencies

Data duplication issues between the SIEM and their data lake led to inconsistencies in reporting and analytics use cases.

Slow Data Onboarding

Adding new data sources and endpoints took up considerable time and effort for the SOC team, especially due to concerns relating to exceeding SIEM license limits as well as the effort involved in normalizing data from different sources

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 add new data sources or find relevant records for threat hunting.**

DataBahn's Security Data Fabric

The DataBahn deployment took a total of 3 weeks at the firm, revamping their data pipelines and using DataBahn to be the centralized data ingestion layer feeding data to their SIEM, data warehouse, and long-term storage systems. Their SOC team experienced the following benefits with DataBahn:

Reduced SIEM licensing costs

DataBahn enabled the firm to reduce their SIEM consumption by 30% in a 3-week period, resulting in annual savings of $300k. 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 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.

Aggregated High-Volume Data Sources

DataBahn allowed the aggregation of high-volume data sources into actionable insights that could be ingested into the SIEM, enhancing security and operational capabilities. This helped reduce data volume of noisy log feeds like network flow by more than 70%.

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 present in multiple data stores.

Streamlined Data Onboarding

With DataBahn, the firm was able to onboard new applications in a matter of hours, free from concerns related to data normalization or exceeding SIEM licensing limits. This significantly reduced the data onboarding lifecycle by more than 70%. With DataBahn writing the events directly using its native integration with Snowflake, the customer was able to avoid additional data ingestion costs in Snowflake previously incurred as a result of using staging locations.

Improved Threat Hunting Experience

The use of DataBahn's Indicator Index in the firm's data warehouse enabled their hunting team to now use these insights for hunting threats going back up to a year. The time taken for finding these Indicators of Compromise ("IOCs") and other artifacts dropped to mere seconds. This additionally reduced their compute costs in Snowflake as hunting queries were now routed to these insights tables.

In summary, the implemention of DataBahn revolutionized the data management landscape for the US investment management 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.

ABOUT DATABAHN

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