SIEM EVALUATION & MIGRATION

SIEMplified with Security Data Fabric

DATABAHN

SIEM SELECTION

Choosing a new SIEM solution requires meticulous evaluation of various factors, including functionality, performance, scalability, and vendor support. This process can be time-consuming and resource-intensive, particularly when assessing multiple vendors. Each vendor often imposes unique requirements for log collection, necessitating the deployment of specialized agents or collectors across a vast array of applications, servers, and endpoints. This extensive deployment can complicate evaluations and hinder the process of determining whether a new SIEM meets the specific needs of your organization.

The Evaluation Challenge

When evaluating multiple Security Information and Event Management (SIEM) vendors simultaneously or undertaking a bake-off process, the complexity of the evaluation can escalate significantly. Each vendor often has unique requirements for how they prefer to receive data, which adds layers of complexity to the evaluation process.

Some vendors may insist on receiving data in their proprietary, vendor-native formats - this can include unstructured or raw data formats that are specific to their system. Other vendors might require data to be submitted in proprietary formats unique to their platform, which necessitates additional data transformation and formatting. Additionally, there are vendors who accept data in any format but have specific requirements regarding data staging locations or the protocols through which the data is transmitted.

These diverse requirements can result in an extended evaluation period, typically spenning from three to six months. This prolonged timeframe is often a consequence of the difficultly of performing a straightforward, apples-to-apples comparison between SIEM solutions that handle data in varying formats and from different data sources. The complexity of aligning these disparate data handling practices can make it challenging for organizations to determine which SIEM solution will best suit their needs.

On the other hand, some organizations might choose to conduct a limited scope proof of concept (POC) involving only one or two data sources. While this approach would provide some insights into the capabilities of a SIEM solution, it often falls short of assessing the full range of functionalities and performance features that are critical for comprehensive security operations. This limited testing can result in an incomplete evaluation, potentially leading to a mismatch between the SIEM's capabilities and the organization's actual security needs.

THE AUTHOR

Aditya Sundararam

Chief Product Officer at DataBahn.ai

Aditya is a seasoned product leader with an exceptional record of driving vision, strategy, and excellence in the technology startup landscape. He spent 10+ years as a product lead in Cyber Threat Analytics, harnessing a value-driven approach to product management and building innovative solutions. He has overseen global teams dedicated to developing and prioritizing SIEM and Security Analytics content. At DataBahn, he shapes and aligns our platform solution with market demands and customer needs.

SECURITY DATA FABRIC

DataBahn's Solution for Efficient SIEM Evaluation

DataBahn offers a revolutionary approach to evaluating new SIEM solutions by seamlessly routing data from your existing data pipelines in real-time to the new system(s). This allows organizations to compare the effectiveness, performance, and functionality of different SIEM solutions within a controlled environment without the hassles of setting up custom log forwarding or deploying new agents or setting up data stages.

Flexible Data Routing

Route any data from any source - on-premise or cloud - flexibly to any SIEM destination through our vendor agnostic data pipelines. Routing data to multiple SIEMs as part of your bake-off from existing data pipelines saves a lot of your team's time and efforts and helps you get to testing out our SIEMs quickly and effectively.

Seamless Data Onboarding

Through DataBahn's ability to support transforming data to any proprietary SIEM data model, such as CIM, Elastic, UDM, ASSIM, you eliminate any additional overhead of managing complex onboarding efforts otherwise needed during your evaluation. As SIEMs eventually converge to a standard format like OCSF in the future, you can seamlessly update your data pipelines to send data in OCSF format through the click of a button within DataBahn.

Streamlined Transition and Control

When you're ready to make the switch, DataBahn facilitates a smooth transition by handling data forwarding to the incumbent tool and directing it exclusively to the new SIEM. This real-time data redirection ensures uninterrupted security monitoring and incident response, minimizing disruption and downtime during the transition period.

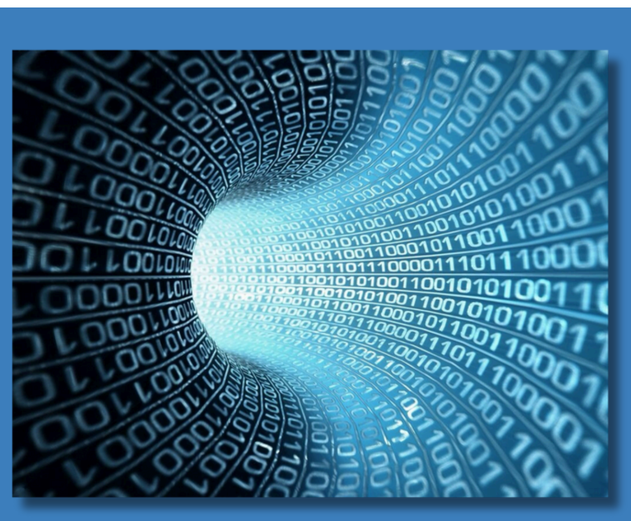
In addition to easing the migration process, DataBahn empowers you with the ability to control data volume. By optimizing and summarizing data, DataBahn can reduce the volume of data sent to the SIEM platform by up to 80% or more. This reduction not only minimizes storage costs but also enhances SIEM performance. Prioritizing relevant data and summarizing routine information ensures that only actionable security insights are forwarded to the SIEM, boosting operational efficiency and providing leverage in negotiating future licence agreements.

With DataBahn, transitioning to a new SIEM solution becomes a seamless, efficient, and cost-effective endeavor, allowing your organization to maintain robust security operations while optimizing resource utilization.

STRATEGIC CONSIDERATIONS

Vendor & Data Lock-in

If history is any indication, most SIEM products have a shelf-life of 3 to 5 years. With SIEMs and proprietary formats, ownership of security data is an important critical consideration. CISOs should make future-proof choices that provide flexibility in adding future security tools. For some businesses, compliance and audit also necessitates historical security data storage - and having a proprietary format or locked-in data can extend the SIEM's lifecycle at a SOC past their best-by date.



Read about how a publicly-traded insurance company had to continue operating 3 different SIEMs while paying full renewal fees due to regulatory requirements mandating 10 years' worth of data - and how **DataBahn's Security Data Fabric helped them own their own data** *and write it into their own security data lake.*

THE CASE FOR OWNING YOUR OWN SECURITY DATA

READ MORE

SIEM Licensing & Cost Reduction

SOCs and cybersecurity teams have to deal with an explosive 10-20% year-on-year increase in security data volume. Managing these costs is challenging for SOCs because of the manual effort involved in effectively filtering security data without reducing security protection and coverage.

Redefining Security Data Architecture for a US Investment Management Firm

$350k	*annual savings in SIEM costs*
70%	*reduction in onboarding time*
40%	*improved detection coverage*

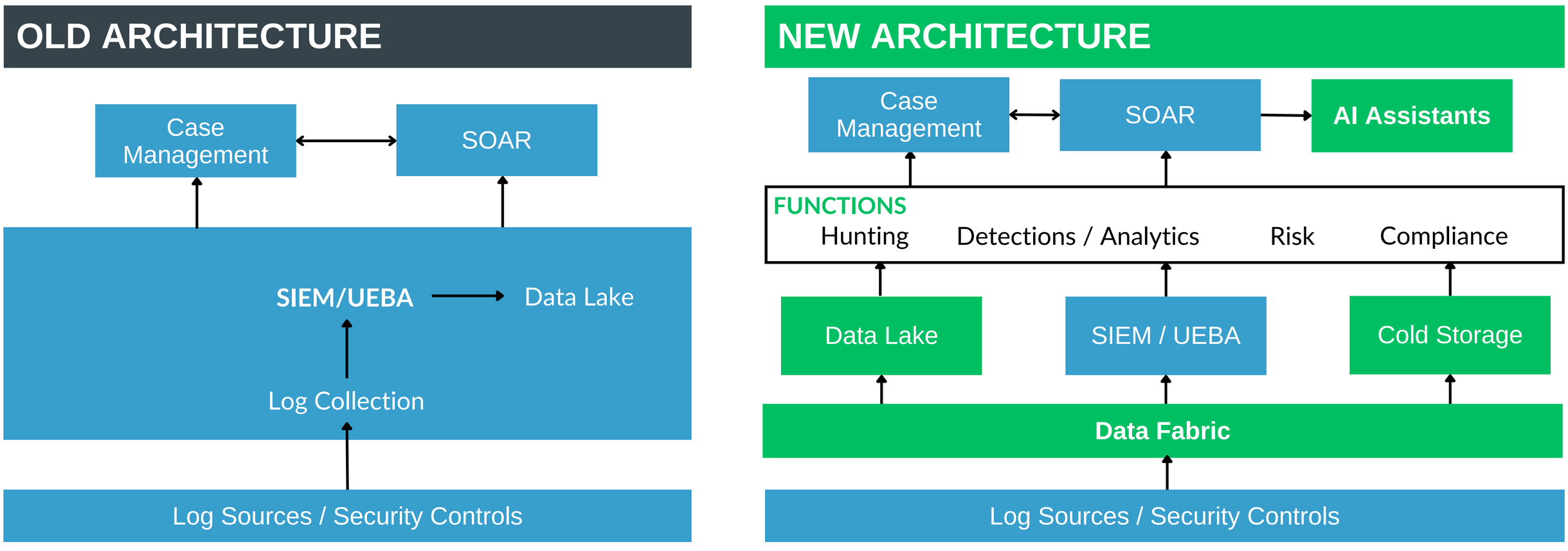
READ MORE

The need for a modular SIEM architecture

Organizations have traditionally relied on their SIEM solution to be their log management system in addition to being the main security data correlation and security monitoring platform.

With data collection being tightly coupled with the SIEM, transitioning to a new advanced technology becomes a costly and usually very time-consuming initiative, impacting the ROI and time to value of the SIEM migration, having to re-architect the data layer, the analytics / processing layer, and the related workflows!

Hence, the value of adopting a horizontal model for your SOC, starting with your SIEM migration, based on a hybrid model of using best of breed and integrated solutions: Security Data Fabric + Data Lake + Security Content and event correction on your SIEM + Security Analytics and Threat Hunting tools as applicable.



Notes: This illustrates a model horizontal / modular security data architecture, where a security data fabric connects log sources and security controls to the SIEM, security data lake, and cold storage. This enables easier adoption and integration of AI-based assistants.

Differences in modular vs legacy SIEM architecture

Introducing a Security Data Fabric

DataBahn's security data fabric is a leading solution which connects, integrates, and governs data across different systems and applications. The key outcome of a security data fabric is to allow security teams to focus on their core function (i.e., threat mitigation, detection, response, and recovery) instead of spending countless hours tinkering with data engineering tasks.

As you can see in the diagram above, the SIEM is decoupled from data collection in the new architecture, giving you true ownership of your data to store in your data lake (on cloud or on-prem), while the data fabric handles the log ingestion (i.e., data collection), and sending ONLY security-relevant data to the SIEM in the expected format.

Non-security-relevant data can still be routed by the DataBahn security data fabric to a cheaper cold storage, reducing your overall cost and freeing space / license on the SIEM for enhanced security monitoring.

MODULAR SIEM - BENEFITS

Streamlined Log Collection

With DataBahn's advanced security data fabric, managing log forwarders and relay servers has become a thing of the past. Our solution simplifies the process by offering seamless cloud log delivery, ensuring that our logs are collected and transmitted efficiently without the overhead of traditional management tasks. This means you can focus on what truly matters - leveraging your data for security insights - while we handle the heavy lifting of log collection.

Accelerated Onboarding & Optimized Data Routing

Speed up the onboarding of new data sources and enhance dual-destination routing with DataBahn's data fabric. Our solution is designed to support a variety of destination systems - whether it's QRadar, Microsoft Sentinel, Google Chronicle, Splunk, Snowflake, or Cloud Cold Storage. We provide native support for routing data in preferred or custom formaqts to each downstream destination. This streamlined approach significantly reduces the time required to integrate and manage logs, allowing for faster deployment and improved operational efficiency.

Comprehensive Data Observability and Governance

Gain unparalleled visibility into your logging health with DataBahn's end-to-end data observability and governance features. Our solution includes silent or whispering device alerting to keep you informed of any issues without disrupting your operations. Additionally, we offer in-line sensitive data redaction and masking to ensure compliance and protect sensitive information. This comprehensive approach ensures that you have complete control over your data while maintaining high standards of security and privacy.

SIEM and Log Management Cost Optimization

Reduce your SIEM and log management costs by leveraging DataBahn's security data fabric. Our solution delivers a minimum of 35% reduction in ingested data by filtering and sending only the security-relevant information downstream. This optimization not only enhances your SIEM's performance but also helps in managing and reducing overall costs. Our out-of-the-box volume reduction rules ensure that you are only paying for the data that truly matters, providing you with both cost savings and improved efficiency.

Optimizing data ingestion, SIEM, and data storage costs for a US Cybersecurity Firm

$254k	*annual savings in SIEM costs*
38%	*reduction in log volume*
14 days	*time-to-value for savings*

READ MORE

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