SIEM MIGRATION BEST PRACTICES

Unlock greater value and control via a security data fabric

DATABAHN

INTRODUCTION

Since the early 2000s, cybersecurity and IT teams have continued to rely on standalone SIEMs to collect, aggregate, and ingest security and log data from a variety of sources - endpoints, servers, firewalls, applications, and more. The rapid increase in the volume, velocity, and the complexity of the data being collected has surged beyond the capacity of traditional SIEMs. This has left SOCs and CISOs struggling with legacy systems while trying to deliver scalable, flexible, and dynamic future-ready solutions that deliver security while keeping team bandwidth use and storage costs in check.

CISOs and SOCs should demand more from their security infrastructure. Decoupling essential functions such as data ingestion from your SIEM and building out a modular and horizontal security data infrastructure will ensure that their future cybersecurity capabilities will be well-rounded, more dynamic and capable of dealing with AI and ML-driven transformations to cater to business realities.

This is why the cybersecurity industry is moving towards a modular SIEM architecture and deployment with a security data fabric, next-generation SIEM, and a modern security data lake.

Considerations with Migrating to a new SIEM Solution

Strategic considerations:

- **Reduce Vendor Lock In and Own your data**: If history is any indication, most SIEM products have no more than 3-5 years shelf life. Hence, it is important to maintain or establish ownership of your security data to ensure flexibility to bring in future security tools without significant architecture overhaul

- **Managing growing SIEM licensing cost**: Challenge dealing with limited data filtering options to manage logs more optimally and limited ability to send only security data to the SIEM versus sending all data, impacting licensing cost and SIEM capacity to ingest meaningul data .

THE AUTHOR

Dina Kamal

Field CTO, DataBahn

Dina has 20+ years of experience at the intersection of AI and Cybersecurity. She is widely acknowledged as a leading figure in advising, developing, selling, and implementing leading-edge cybersecurity solutions in North America and globally. Before joining DataBahn, Dina was a senior partner at Deloitte Canada, where she led the Canadian software business, the AI product and data science teams, in addition to leading Deloitte's global threat management team and many large-scale Cyber Security, AI and broader tech transformations.

Tactical considerations:

- **Data collection and Log ingestion migration:** Migrating to a new SIEM usually means establishing a new log collection technology stack. Customers are not always clear on the most efficient transition path in addition to the complexity of managing log forwarders, relay servers and various cloud sources integrations.

- **The need for Multiple log routing of the data during (and probably after) migration**: Needing to seamlessly route data to multiple SIEM destination system (i.e, the old and the new SIEM technologies) in their preferred formats.

- **Dealing with Operational overhead:** There is typically a much higher operational overhead during SIEM migration, that sometimes spans many weeks, if not months, due to having a dual-SIEM architecture, both with their own pipelines and configurations. This is in addition to the need to ensure that the right data is sent to the new SIEM to support effective use cases migration and enhanced threat detection

Why you need to Embrace a Modular SIEM:

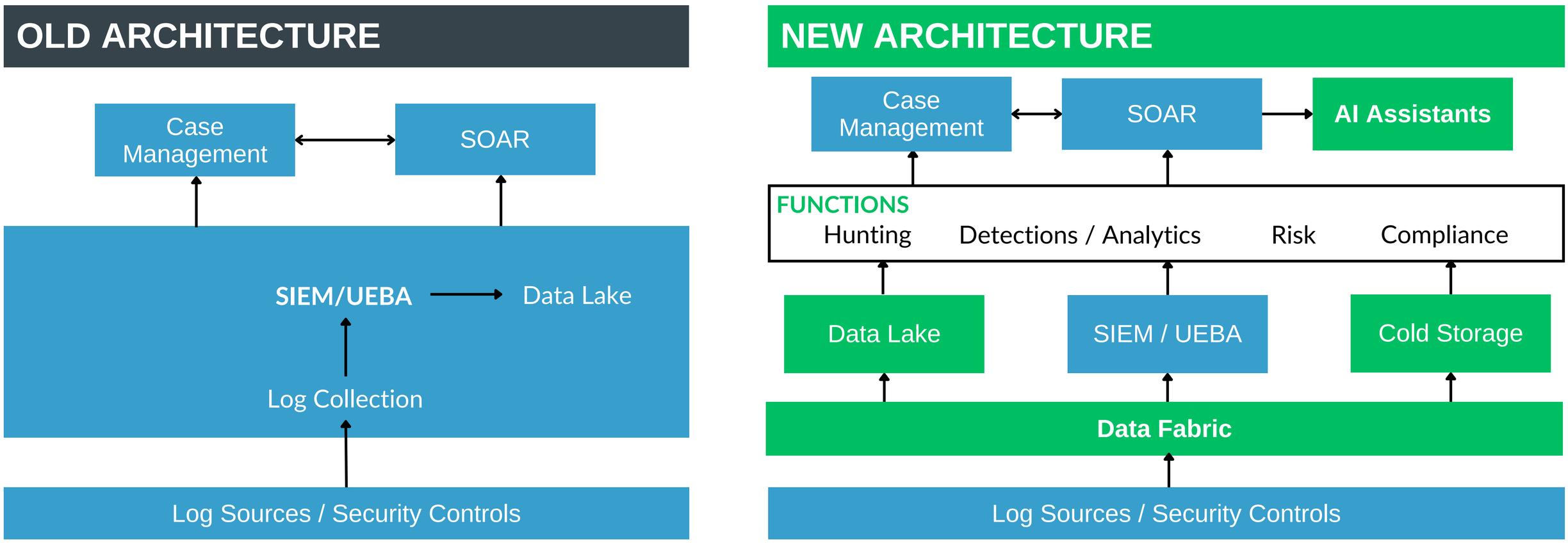
Organizations have traditionally relied on their SIEM solution to be their log management system in addition to being the main security data correlation and security monitoring platform.

With data collection 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. See the graph below for an illustration of this shift.

Differences in modular vs. legacy SIEM architecture

- **Security Data Fabric:** Security Data Fabrics connect, integrate, and govern data across different systems and applications, and allows 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. **DataBahn is a leading Security Data Fabric solution.**
- **SIEM and Data Collection decoupling:** As visible in the diagram showcasing the new architecture, the SIEM is now decoupled from data collection. This gives enterprises true ownership of their data to store in their data lake (on cloud or on-prem), while the data fabric handles the log ingestion (i.e., the data collection). It also sends ONLY the security-relevant dat to the SIEM in the expected format.
- **Non-relevant data routing:** DataBahn security fabric will automatically route the non-relevant security data fabric to a cheaper cold storage, reducing your overall cost and freeing space / license on the SIEM for enhanced security monitoring.



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.

Benefits of using a security data fabric

- **Reduce log collection footprint:** Security Data Fabrics make it unnecessary for SOCs to maintain or manage log forwarders or relay servers, while cloud log delivery will be seamless.

  DataBahn's resilient service mesh architecture which ensures data collection never stops

- **Easier source onboarding and dual-destination routing:** Security data fabrics reduce the effort required to integrate and move security data

  400+ connectors for seamless onboarding; native support for routing data into system s(QRadar, MS Sentinel, GCP Chronicle, etc.) across formats with DataBahn

- **End-to-end data observability and governance:** Come with data observability and governance built in to avoid blind spots or missing data

  DataBahn enables data management and tracking across the observability pipeline with minimized downtime, higher data integrity, automated cataloging and telemetry coverage

- **Reduced SIEM / log management costs:** Security data fabrics should reduce the volume of log data to save on SIEM and storage costs

  DataBahn delivers 45% volume reduction in your SIEM that is scalable (up to 2.5mn EPS), flexible (data replay across sources and destinations), and secure

Doing your SIEM the Right Way

In order to capture these benefits fully for your organization, it is important to consider this new architecture before you begin migrating to a new SIEM. It will also help you negotiate your new SIEM licenses considering how much you can save on your new SIEM by incorporating our security data fabric.

Here are some sample steps to guide your journey:

STEP 1

Introducing DataBahn's security data fabric enables you to easily route your data to multiple destinations, including to two SIEM solutions during the migration phase.

STEP 2

Most customers are moving to cloud-based sources, so it is advisable to start with cloud sources using DataBahn to collect from cloud sources, saving on cloud egress costs.

STEP 3

Deploy DataBahn's highly-resilient on-prem collectors to replace your existing SIEM's collectors / agents.

STEP 4

Leverage DataBahn's volume control library and built-in recommendation engine to assess your existing SIEM use cases to enable easy migration to the new SIEM, while enabling volume reduction and forking of compliance-related and long-term security logs into cold storage.

STEP 5

Use DataBahn's knowledge layer to map existing log sources against MITRE Att@ck framework to assess log coverage against relevant TTPs.

Based on our experience supporting SIEM migrations across many organizations, accounting for the considerations mentioned here and taking the steps above will not only enable you to capture significantly more value of your new SIEM investment, it will also enhance insights from your security data and related threat detection. Using DataBahn will also accelerate your SIEM migration initiative and reduce your time to value of your new shiny SIEM.

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