Enable value driven CyberOps using Databahn.ai's Security Data Fabric for your Securonix Unified Defense SIEM Deployments

SOLUTION BRIEF

DataBahn + Securonix

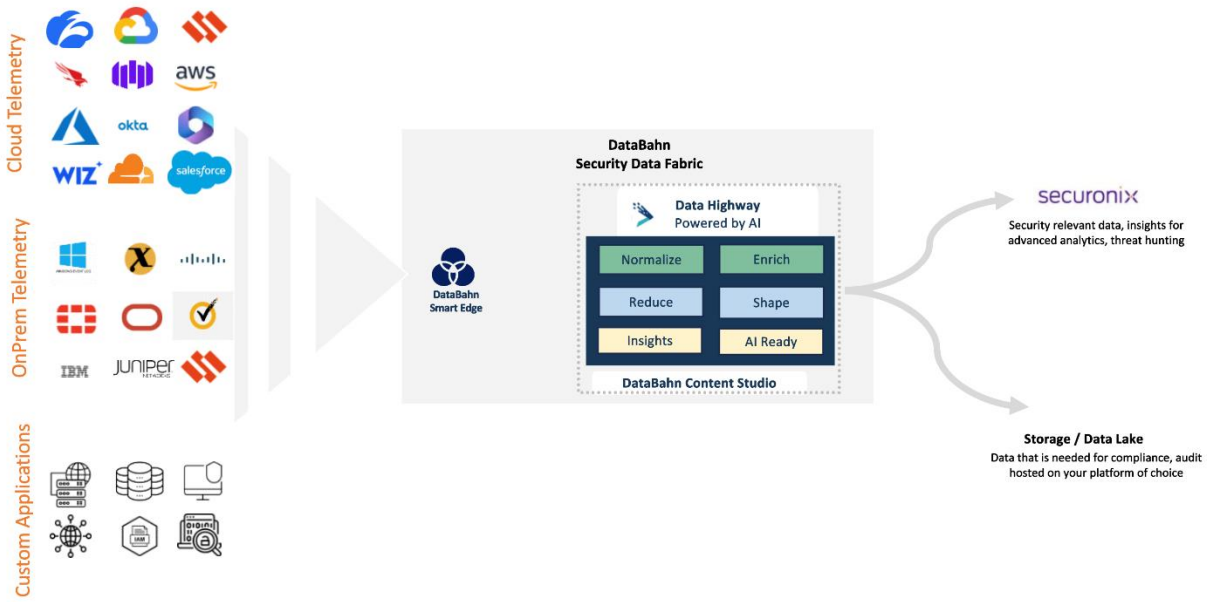
Many security teams are transitioning to a unified Cyber Operations (Cyber Ops) model, prioritizing a proactive, data-driven approach enhanced by AI technology. This move signifies a departure from traditional Security Operations Centers (SOCs), which primarily react to threats as they occur. Unlike SOCs, Cyber Ops utilizes AI to automate processes, prioritize threats, and predict potential attacks, thus transforming how security operations function. In this evolving security landscape, Securonix's Unified Defense SIEM is emerging as a preferred solution for implementing Cyber Ops.

The shift towards a unified Cyber Ops model using solutions like Securonix, while transformative, presents specific challenges that need addressing. Firstly, the prevalent data volume-based pricing model of traditional independent SIEM systems has become a deterrent, as it often leads to reduced overall return on investment (ROI) for executives. This pricing strategy can become cost-prohibitive when data volumes are high, diminishing the attractiveness of maintaining a standalone SIEM solution. Secondly, customers face limitations in the flexibility of managing data streams, as they cannot easily fork data based on its relevance to different downstream systems. This lack of precision can impair the effectiveness of security operations. Additionally, in an independent SIEM approach, moving data from a customer's cloud to a vendor's cloud incurs data transfer charges, further escalating costs.

To address these issues, a security data fabric solution is essential to complement the Unified Defense SIEM, like that offered by Securonix. A security data fabric can help sift through and eliminate unnecessary data, thus managing costs more effectively. Additionally, it provides customers the flexibility to control their data across any platform they choose while still benefiting from the advanced Cyber Ops capabilities provided by Securonix. This integrated approach ensures that organizations can optimize their security operations for efficiency and cost-effectiveness without compromising on the cutting-edge features offered by Securonix Unified Defense SIEM.

The Solution

DataBahn's Security Data Fabric with its purpose built Smart Edge along with the Data Highway products can take data from a wide range of sources (both cloud and on-premise sources), parse and structure them into any format or data model of your choosing, enrich data with any meaningful context (internal and external context), orchestrate the data to extract meaningful insights and deliver security relevant data and insights into your Unified Defense SIEM for optimal querying, analytics and search.



DataBahn helps Securonix Unified Defense SIEM deployments by streamlining data collection and ingestion and removing the onus of your team having to manage log collection infrastructure (Remote Ingesters), build out custom integrations and spend cloud data egress costs incurred by sending logs from your cloud sources and applications into your Securonix SIEM.

Through DataBahn's native capabilities, Security teams can:

- Simplify data collection and ingestion into Securonix
    - By using DataBahn's plug-and-play integrations and connectors with a wide array of products and devices
    - By using DataBahn's native streaming integration for a hassle-free, real time data ingestion into Unified Defense SIEM, eliminating any additional log collection infrastructure in your network
    - By effectively normalizing and structuring complex data formats like nested JSON, multi-line logs using DataBahn's orchestration pipelines before the data is delivered to the SIEM
- Send only security relevant data to your Unified Defense SIEM
    - By using DataBahn's out of the box library of context-aware volume reduction rule sets helping you achieve more than 45% data volume reduction
- Convert logs into insights
    - By using volume reduction functions like aggregation and suppression to convert noisy logs like network traffic/flow into manageable insights that can be loaded into Securonix SIEM reducing both the volume and the overall time for queries to execute
- Increase overall data governance and data quality
    - By identifying and isolating sensitive data set in transit thereby limiting exposure
- Perform split second threat hunting
    - By using the DataBahn's Indicator Index to extract insights such as Security Observables (IP addresses, Domains, URLs, Hashes), Entity Relationships (Processes, Network

execution, Registry modifications), Intel Context to compliment Securonix's Autonomous Threat Sweep and Fast Hunt capabilities
    - By using additionally derived context such as first observed / last observed time / frequency of observation to speed up data exploration and hunting
- Bring best of breed services and technologies
    - By leveraging DataBahn's simplified data orchestration capabilities, Securonix customers can use additional tools to implement a truly cyber mesh architecture without having to worry about locking your data within your vendor cloud
- Get visibility into the health of telemetry generation
    - By using the dynamic device inventory generated by DataBahn to identify devices that have gone silent, log outages and detecting any other upstream telemetry blind spots
- Reduce overall costs of your Unified Defense SIEM deployment
    - By removing the need for any staging locations or custom integrations by taking advantage of DataBahn's library of integrations and connectors
    - By routing less frequently accessed data sets and keeping a copy of your logs using Data Highway to low-cost storage infrastructure such as your cloud storage (S3/Blob/GCP storage) or your data lakes such as Snowflake, AWS while adhering to the same data models to access them only when the need arises

Benefits of using DataBahn with Securonix Unified Defense SIEM

Out-of-the-box connectors and integrations

DataBahn offers effortless integration and plug-and-play connectivity with a wide array of products and devices, allowing SOCs to swiftly adapt to new data sources.

Resilient data collection

DataBahn's highly resilient Smart Edge enables your team to not worry about single points of failures or managing occasional data volume bursts resulting in data outages or data delays

Enrichment against Multiple Contexts

DataBahn enriches data against various contexts including Threat Intelligence, User, Asset, and Geo-location, providing a contextualized view of the data for precise threat identification.

Format Conversion and Schema Monitoring

The platform supports seamless conversion into

Reduced Costs

DataBahn enables your team to manage the overall costs of your Securonix deployment by providing a library of purpose-built volume reduction rules that can weed out redundant and less relevant logs keeping your SIEM costs optimal.

Sensitive data detection

Identify, isolate and mask sensitive data ensuring data security, governance and compliance.

Orchestrate data into different destinations based on relevance

DataBahn's orchestration platform helps tier data based on its relevance so you can put purpose to your data and send security relevant data to Securonix while the rest can be sent to infrastructure or platforms of your choice for threat hunting and compliance use cases.

Get your data AI ready

any data model of your choosing, additionally facilitating flexible and faster downstream onboarding in Securonix and other services.

Schema Drift

Detect changes to log schema intelligently for proactive adaptability and to avoid downstream detection impact.

Use the DataBahn AI Ready framework to get your data cleansed, enriched, features extracted, and embeddings generated to build AI powered apps to augment your Security operations

Risk free data sharing internally and externally

Use DataBahn to fork out data streams to different services beyond the Securonix SIEM to provide the flexibility your teams need to bring in any tool of their choice

With DataBahn and Securonix Unified Defense SIEM, unlock the power of your data to ensure your security operations are both precise and adaptable, while leveraging advanced Cyber Ops features provided by Securonix. Ultimately, our security data fabric enhances data autonomy and operational efficiency, making it an indispensable component in modern cybersecurity strategies.