LEARNING MADE EASY

DataBee® Special Edition

Security Data Fabric

for dummies®
A Wiley Brand

Unify security data for insights

Boost threat detection and response

Simplify daily security management tasks

Brought to you by

DataBee®
A COMCAST COMPANY

Stephanie Diamond

Security Data Fabric

DataBee® Special Edition

by Stephanie Diamond

for dummies®
A Wiley Brand

Security Data Fabric For Dummies®, DataBee® Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

The manufacturer's authorized representative according to the EU General Product Safety Regulation is Wiley-VCH GmbH, Boschstr. 12, 69469 Weinheim, Germany, e-mail: Product_Safety@wiley.com.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.dummies.com/custom-solutions. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-24367-9 (pbk); ISBN 978-1-394-24368-6 (ePDF); 978-1-394-31223-8

Publisher's Acknowledgments

Acquisitions Editor: Traci Martin

Senior Managing Editor: Rev Mengle

Client Account Manager: Molly Daugherty

Content Refinement Specialist: Magesh Elangovan

Introduction

The enterprise security setup is complex. Fortune 100 companies use an average of over 100 security tools, each with its own data language. This presents many challenges. Building a custom security data fabric requires significant time, money, and a team of expert data engineers and scientists.

About This Book

This book explores how security data fabrics address security challenges by creating an interconnected data environment that enhances visibility, improves threat detection, enables continuous compliance, and streamlines incident response.

Icons Used in This Book

Throughout this book, different icons are used to highlight important information. Here's what they mean.

TIP

The Tip icon highlights information that can make doing things easier or faster.

REMEMBER

The Remember icon points out things you need to remember when searching your memory bank.

WARNING

The Warning icon alerts you to things that can harm you or your company.

Beyond the Book

This book is an overview, and you're likely to come away with an appetite for more information about security data fabrics. A good place to explore is DataBee.ai.

IN THIS CHAPTER

- » Understanding security data challenges and reviewing common data issues
- » Introducing the security data fabric concept
- » Looking at the basics for resolving common data issues

Chapter 1 Addressing Data Challenges and Introducing Security Data Fabric Concepts

Security teams today face a paradox: Although security data is abundant, it often lacks the clarity and cohesion needed to drive actionable insights. Disconnected systems and fragmented data sources create silos that hinder visibility, making it difficult for security and risk professionals to make timely, informed decisions.

These silos compromise the accuracy of business intelligence and security analytics, leading to mistrust in data quality and integrity.

Traditional log management and security information and event management (SIEM) solutions were not designed to handle massive amounts of data or designed to store data for long periods of time, becoming prohibitively expensive. Additionally, maintaining custom extract, transform and load (ETL) pipelines is both complex and resource intensive.

To support effective decision-making, rapid incident response, and real-time compliance reporting, organizations need complete, high-quality datasets that are readily accessible. Achieving this requires a scalable, cost-efficient analytics architecture that supports long-term data aggregation and retention and empowers users — regardless of technical expertise — to extract meaningful insights. This chapter gives you an overview of how to do that.

Introducing the Security Data Fabric Concept

The security data fabric is an emerging approach that promises to transform security operations by addressing the growing volume and complexity of security data. It provides a unified framework for managing and accessing data, enabling security teams to perform deeper analysis and gain more meaningful insights. Inspired by the data fabric model used in business intelligence, this concept offers a similar level of integration and accessibility to cybersecurity, where data has traditionally been siloed and disconnected from broader business systems.

REMEMBER

The combination of data science expertise with cybersecurity knowledge creates powerful synergies. A security data fabric is a comprehensive architecture that integrates and manages security data from various sources in a unified, secure, and governed approach. This architecture is designed to navigate complex security semantics and streamline security, risk, and compliance workflows.

By aggregating, contextualizing, and correlating vast quantities of data, security data fabrics enable organizations to gain a coherent and actionable understanding of their security postures. The goal is to enhance threat detection, real-time response, and overall risk management by providing a holistic view of security controls and network operations.

TIP

One key aspect of a security data fabric is its capability to combine security and business data for a comprehensive view of an organization's security. Normalizing and analyzing data from various sources provides insights into potential vulnerabilities and threats.

KEY COMPONENTS OF A SECURITY DATA FABRIC

To gain a clear understanding of the power of security data fabric, you need to know what the key components are. They include:

- **Ingesting data:** Collect data from various sources like business applications, SaaS products, identity and HRIS, and other sources.
- **Parsing and flattening data:** Convert complex log data into a flat, easy-to-analyze format.
- **Normalizing data:** Standardize data using frameworks like Open Cybersecurity Schema Framework (OCSF).
- **Enriching data:** Add business context to enrich security data.
- **Correlating data:** Link security events across systems to identify threats and track entities.
- **Storing and analyzing data:** Use scalable cloud environments like AWS Security Lake, Snowflake, and Databricks.
- **Detecting and responding to threats:** Employ advanced analytics and ML for real-time threat detection.

Exploring Data Challenges

Security teams face a never-ending stream of logs and data from many sources. These logs come in diverse formats, making integration, deduplication, and unified search difficult. This avalanche of data often leads to information overload, where critical signals can be buried under enormous amounts of irrelevant noise.

Tackling high volumes of data

To tackle the issue of high data volumes, a security data fabric must support various data sources and formats. This capability enables organizations to integrate logs, alerts, and other security data from a variety of locations, allowing for a centralized approach to security data management.

Advanced security data fabrics ingest data from on-premises log forwarders, cloud storage services like AWS S3 and Azure Blob, and APIs from various software-as-a-service (SaaS) applications. This comprehensive and flexible ingestion capability allows for all relevant security data to be captured and available for analysis.

Identifying valuable data

With the sheer volume of data generated, not all information is needed at the same time. Security teams must identify the critical data points in real-time to detect and respond to threats.

Cybersecurity systems are overwhelmed and stretched far beyond what traditional tools were designed to handle. As a result, security teams are often forced to make difficult tradeoffs, deciding which data to store, for how long, and what to discard. Not all information is needed at the same time, and teams must continually assess which data points are most critical to detect and respond to threats in real-time.

To address this, many organizations are turning to a variety of data storage solutions like data lakes, which offer a flexible, low-cost way to store massive volumes of raw data.

TIP

Although data lakes and other storage options solve some storage and access challenges, they introduce new ones. Without a consistent framework, data can quickly become disorganized, filled with inconsistent and low-quality data from various sources and formats. This lack of structure makes it difficult to extract meaningful insights, especially when data is needed urgently for threat detection or compliance reporting. Additionally, without the necessary frameworks and structure in place, duplicate records can quickly multiply, increasing costs and potentially degrading the performance of the data lake.

This is where a security data fabric becomes essential, as it applies common standards for how data is ingested, stored, and queried. It ensures that data remains clean, consistent, and usable, regardless of its source or format. Security data fabric solutions automate deduplication by continuously monitoring data streams, identifying duplicates, and consolidating records. These standards and automations ensure the dataset remains clean and manageable, allowing security teams to focus on meaningful analysis.

REMEMBER

By combining the scalability of data lakes or other data storage solutions with the governance and intelligence of a data fabric, security teams can store all potentially useful data cost effectively while maintaining the capability to quickly identify and act on high-value insights.

Dealing with complex and diverse security data

Parsing, normalizing, and correlating security data are fundamental actions for transforming raw data into actionable intelligence. Parsing involves extracting relevant information from raw data streams. Normalization ensures that data from different sources follows a consistent format. Correlation links related data points to provide a comprehensive view of security events and incidents. When combined, a security data fabric can consolidate the different ingest streams into a single cohesive center for insights.

Security data fabric solutions address these challenges by implementing advanced data transformation engines. These engines automatically parse and map data to standardized schemas, such as the OCSF, and enrich it with business context and metadata. This process not only simplifies data management but also enhances the accuracy and relevance of the insights derived from the data across multiple use cases.

TIP

Correlating data from various sources can reveal patterns and indicators of compromise that might otherwise go unnoticed in the context of threat detection. By integrating logs, network flows, and user activity data, security teams can build a more detailed picture of potential threats and respond more effectively.

REMEMBER

Two firewall vendors may have very different-looking logs. Parsing may require years of hands-on experience, as well as vendors who are willing to communicate proactively when the underlying log formats change.

Resolving Common Data Issues

A security data fabric helps address common data challenges, enabling security teams to unlock the value of their data, and achieve more effective threat detection and operational efficiency.

Overcoming data silos that hinder connectivity

Data silos are a common problem in large organizations, where different departments and teams use separate systems and tools to manage their data. Business units often store customer data, transaction records, and operational metrics in their own databases, while security teams maintain separate systems for threat intelligence, vulnerability assessments, and incident reports. Additionally, IT departments typically have their own infrastructure monitoring and management tools.

This separation creates information gaps where business context is disconnected from security insights, making it harder to identify and respond to risks effectively.

A security data fabric solution addresses this challenge by breaking down data silos and creating a unified data layer. By integrating data from various sources, including on-premises systems, cloud platforms, and SaaS applications, the security data fabric ensures that all relevant data is accessible and connected. This integrated approach facilitates seamless data sharing and collaboration among departments, thereby enhancing the effectiveness of the security program.

TIP

Security data fabric solutions sometimes include advanced data transformation and enrichment capabilities. These features automatically parse, normalize, and correlate data from different sources, creating a cohesive and enriched dataset that provides a holistic view of the organization’s security landscape. By eliminating data silos and enhancing data connectivity, organizations can improve their ability to detect, investigate, and respond to security incidents.

Lacking data trust between departments

Data silos lead to a lack of data trust, and siloed security data is often viewed skeptically by various teams due to inconsistencies and inaccuracies in the data they receive. This mistrust can stem from using different tools, formats, and processes, resulting in fragmented and unreliable data.

To address this issue, a security data fabric solution ensures that all departments access the same reliable and standardized data. By integrating data from multiple sources and normalizing it using a consistent schema like the OCSF, organizations can provide a single source of truth for security data. This approach helps improve data accuracy and fosters trust among departments, as everyone works from the same dataset.

REMEMBER

Advanced security data fabric solutions often include governance and auditing features that track data lineage and ensure data integrity. These capabilities enable organizations to maintain high data quality standards and provide transparency into data collection and processing. As a result, teams can trust the data they receive and collaborate more effectively on security initiatives.

Relying on static spreadsheets for analysis

Many organizations still rely on static spreadsheets for security data analysis. Although spreadsheets can be useful for ad-hoc analysis, they're not well-suited for cybersecurity's dynamic and continuous nature. Point-in-time snapshots often become outdated quickly, leading to decisions based on stale data and increasing the risk of missing critical security events.

TIP

A security data fabric solution overcomes this limitation by providing real-time, continuous access to security data. Instead of relying on outdated spreadsheets, security teams can leverage live dashboards and automated reports that are updated in real-time. These tools enable teams to monitor security events as they occur and respond more quickly to emerging threats.

Additionally, security data fabric solutions often integrate with business intelligence (BI) tools like Tableau and Power BI, allowing teams to create interactive and dynamic reports. These integrations provide a more flexible and powerful analysis environment than traditional spreadsheets, enabling deeper insights and more informed decision-making.

Pivoting between too many tools

Many organizations struggle with *tool sprawl* (using several security tools that don't communicate effectively with one another).

This leads to wasted time switching among tools, incomplete system visibility, and problems connecting data from different sources.

A security data fabric resolves the challenge of pivoting among too many tools by providing a centralized data integration and analysis platform by:

- **Centralizing data:** Ingesting information from all security tools into a single platform
- **Normalizing data:** Standardizing formats for comparison and analysis
- **Providing a unified interface:** Allowing analysts to access multiple data sources from one dashboard

By resolving the challenge of tool pivoting, a security data fabric enables faster, more effective security operations and improved threat detection.

IN THIS CHAPTER

- » Introducing the benefits of adopting a security data fabric solution
- » Providing stakeholder benefits

Chapter 2 Understanding the Security Data Fabric Architecture and Leveraging Its Benefits

Organizations face a persistent challenge of managing vast amounts of data from various security tools and platforms. Traditional approaches to security data management often result in siloed and diminished information. This hinders threat detection and incident response. By connecting across the security ecosystem, a security data fabric offers a solution by providing unified and expanded access to all security insights and data.

This chapter explores how a well-implemented security data fabric can deliver tangible value across the organization to different departments, from IT and security teams to compliance officers and executive leadership.

How a Security Data Fabric Delivers Organizational Benefits

A security data fabric brings advantages that go beyond just improving cybersecurity. It helps organizations manage costs, use security tools more effectively, and expand access across cybersecurity roles.

Optimizing costs through efficient data management

A security data fabric enables immediate compression of high-volume or low-value data. Organizations can potentially reduce storage costs using data compression, flattening, and deduplication techniques.

TIP

This approach maintains data integrity and accessibility while optimizing resource usage.

Many organizations use multiple security tools, such as security information and event management (SIEMs), endpoint detection and response tools (EDRs), and firewalls. Security data fabric helps improve operational efficiency by creating an integrated layer for multiple security tools. It merges duplicate insights from various tools, enriches data by combining information from multiple sources, and reduces alert fatigue through alert deduplication and correlation.

REMEMBER

This optimization maximizes the value of existing security investments while providing a more comprehensive security perspective.

By aggregating data from various sources, security teams can better detect slow-and-low attacks and insider threats. This enhancement optimizes tool performance without replacing existing investments, increasing the value of the current security infrastructure.

Expanding access across cybersecurity risk, and business functions

Security data fabric centralizes data access for various cybersecurity roles, breaking down traditional silos among different security functions. This unified data platform serves different security needs, from operations to governance, risk, and compliance. This enables more comprehensive and collaborative security management across the organization.

A security data fabric goes beyond simply dismantling security data silos — it establishes a unified, intelligent data layer that ensures seamless access to critical security information across the entire enterprise. By integrating data from diverse environments such as on-premises infrastructure, cloud platforms, and SaaS applications, the security data fabric creates a connected ecosystem where all relevant data is readily available and actionable to teams beyond the security team.

TIP

This holistic visibility empowers teams across departments to build trust and collaborate more effectively, as everyone is working from one source of truth. In essence, a security data fabric transforms fragmented data into a strategic asset, enabling enterprise-wide insight and agility.

Delivering Stakeholder Benefits Through a Security Data Fabric

By leveraging the capabilities of a security data fabric, organizations can provide significant benefits to various stakeholders throughout the organization. These stakeholders include executives, security operations center (SOC) teams, physical and digital security teams, and governance, risk, compliance (GRC) teams. This helps create a strong sense of ownership beyond just the SOC and contributes to a security first culture.

Facilitating collaboration, security hygiene

One of the key advantages of a security data fabric is its ability to enable seamless collaboration by integrating data from previously siloed sources into a unified, reliable dataset. This allows SOC teams, IT, executives, and other stakeholders to access consistent, accurate insights from the same trusted data foundation.

For example, security data fabric platforms combine and standardize data from SIEM systems and other security tools. This eliminates the need for manual correlation and reduces the risk of missing critical alerts.

REMEMBER

By working from a common, holistic view of their security data, teams can better understand risk, streamline investigations, and make more effective decisions together.

Cybersecurity and compliance practitioners using a security data fabric have cleaner and more complete asset and asset owner information within an organization's data estate. Security hygiene using data woven from across IT and security solutions enriched with business context helps answer the "who" and "what" questions about asset inventory.

TIP

The flexible architecture of security data fabrics enables the customization of dashboards and metrics to meet specific needs of different stakeholders. This allows security leaders to tailor insights to various audiences, from mapping to tracking security key performance indicators (KPIs) for executives.

Delivering KPI metrics for executives

Centralizing security data through a security data fabric leads to more consistent and valuable business metrics. It provides a single source of truth for KPIs across the organization. Executives need clear KPIs to understand their security and compliance posture.

Security data fabric solutions offer executive-focused dashboards that provide high-level insights into compliance status, risk levels, and incident response effectiveness. These dashboards are designed to present complex security data in an accessible format, allowing executives to make informed strategic decisions about security investments, like staffing and tooling and deliver consistent, effective communications with the board and other stakeholders.

By integrating and normalizing data from various sources, security data fabrics ensure that executives have a unified view of their organization's security posture, enabling them to identify trends, make data-driven decisions, and demonstrate compliance with regulatory bodies.

Enabling real-time detections for SOC teams

SOC teams require real-time detection capabilities to respond quickly to threats. Security data fabric solutions provide close to real-time detection by constantly monitoring data streams and applying advanced analytics to identify irregularities and potential security incidents.

TIP

By combining related alerts from multiple SIEM systems, security data fabrics make identifying and correlating alerts easier, improving the efficiency and effectiveness of SOC operations.

Threat hunters can use a security data fabric to review and correlate traditionally siloed data, enabling them to use Python, SQL, and other languages to craft artificial intelligence (AI) and machine learning (ML) models that learn from their data.

By parsing, normalizing, and enriching the data collected from disparate sources, threat hunters can create a collaborative yet programmatic workflow by developing use cases, capturing and storing data, creating baselines and launching queries against data to identify anomalies.

By tapping data sources early and lifting compute limits through integration with a data lake, or other data repository, a security data fabric delivers clean, unified data that lets threat hunters run multiple complex hunts in parallel across large-scale historical datasets.

Detecting insider threats

Security data fabric merges physical and digital security insights, creating a comprehensive security view. Insider threats are a major cause for concern for organizations. Employees with authorized access can misuse systems and data. A security data fabric enhances insider threat detection for physical and digital security teams. It accomplishes this by:

- **Integrating data:** Integrates user activity data from multiple sources into comprehensive profiles
- **Correlating data:** Correlates across all sources to identify suspicious behavioral changes that may indicate malicious intent

- **Unifying data:** Provides a unified, time-series view of user and device activity for rapid threat identification

REMEMBER

A security data fabric helps detect insider threats by connecting data from multiple security tools. This gives security teams a more complete view of user activity across the organization and enables faster, more effective responses.

TIP

Seeing the full picture and tracking user behavior patterns over time is key to spotting a variance from the norm that could indicate an insider threat. That way, security teams can address risky insider behavior earlier on.

Supporting governance, risk, and compliance teams

GRC teams benefit from security data fabric solutions to enable true continuous controls monitoring (CCM) — providing real-time visibility, reducing manual effort, and helping the organization move beyond periodic audits.

Implementing a data fabric for compliance efforts enables the GRC team to spend less time on audit preparation and more time accelerating compliance for standards and frameworks. A data fabric for compliance also makes it easier for GRC teams to implement new compliance controls around new regulations.

REMEMBER

The capability to automate data integration and reporting streamlines the compliance process, making it more efficient and less prone to errors.

IN THIS CHAPTER

- » Supporting cybersecurity tools
- » Using OCSF
- » Reviewing enrichment for nontraditional data types
- » Integrating with other tools
- » Creating custom dashboards

Chapter 3 Choosing the Right Security Data Fabric Solution

Picking the right security data fabric solution is crucial to ensuring it meets your organization's needs. It's important to consider factors such as scalability, integration capabilities, and cost-effectiveness.

The right solution should not only address your security challenges today, but also adapt to the future needs of your organization. This chapter discusses key considerations to help guide your decision-making process and ensure you select a solution that fits your organization's unique security landscape and objectives.

Ensuring Diversity of Cybersecurity Tools and Ingestion Capabilities

A robust security data fabric solution must support data ingestion from various cybersecurity tools and platforms. Enterprises can easily have over 100 security tools, some with overlapping solutions or features. The ability to integrate and ingest data from these disparate sources helps ensure comprehensive coverage, while also reducing the risk of blind spots in security monitoring.

DataBee excels in supporting a diverse range of cybersecurity tools and ingestion capabilities. The technology ensures comprehensive coverage and robust security monitoring. This includes:

- **A wide range of supported tools:** DataBee supports integration with over 300 data sources, including SIEM systems, EDR tools, firewalls, intrusion detection systems, and more. This wide range of supported tools ensures that all relevant security data is captured and integrated into the security data fabric.
- **Flexible ingestion methods:** DataBee offers flexible ingestion methods, including application programming interfaces (APIs), on-premises log forwarders, AWS S3, and Azure Blob storage. This flexibility ensures you can easily ingest and process data from various sources, regardless of the deployment environment.
- **Seamless integration:** DataBee's architecture allows seamless integration with security tools and platforms. This capability ensures that organizations can continue to use their preferred security solutions while benefiting from the enhanced data integration and analysis provided by DataBee.
- **Handling of nontraditional data types:** Beyond traditional security tools, DataBee also ingests nontraditional data types such as organizational hierarchy, business context, and external threat intelligence. This comprehensive approach enriches security data, providing deeper insights and enhancing the accuracy of threat detection.
- **Continuous monitoring of data ingestion health and quality:** DataBee continuously monitors the health and quality of ingested data, ensuring that the data remains accurate, up-to-date, and reliable. This constant monitoring capability helps maintain the integrity of the security data fabric and supports effective security operations. You spend less time searching for the right controls and compliance-supporting data.

DataBee's robust ingestion capabilities and support for various cybersecurity tools help organizations achieve comprehensive security coverage.

TIP

By integrating data from multiple sources, DataBee reduces the risk of blind spots in security monitoring and helps improve the overall effectiveness of the security data fabric.

Utilizing a Normalized Schema (OCSF versus Proprietary)

Normalization of data is crucial for enabling seamless analysis and integration. The Open Cybersecurity Schema Framework (OCSF) offers a standardized format that facilitates interoperability among security tools. Utilizing OCSF ensures that data from various sources can be easily correlated and analyzed, reducing the complexity associated with proprietary formats. This standardization is essential for creating a unified view of security data, making it more accessible and actionable.

DataBee leverages the power of data normalization by adopting the OCSF. It accomplishes this by using:

- **A standardized data format:** DataBee uses OCSF to standardize the data format, ensuring compatibility and interoperability among different security tools. This standardized format simplifies data integration and correlation, making it easier to analyze security data from various sources.
- **Enhanced data correlation:** By normalizing data using OCSF, DataBee allows for seamless correlation of security events across different platforms. This enhanced correlation capability provides a more comprehensive view of the security landscape, enabling better threat detection and response.
- **A reduction in complexity:** Utilizing a normalized schema like OCSF reduces the complexity associated with proprietary data formats. This simplification enables the seamless integration of data from disparate sources into a unified security data fabric, making it more accessible and actionable for security teams.

- **Flexibility and scalability:** DataBee's implementation of OCSF provides flexibility in adapting to various data sources and security tools. This approach supports the scalability of the security data fabric, allowing organizations to expand their security infrastructure without facing compatibility issues.
- **Continuous schema updates:** DataBee ensures that the schema used for data normalization is continuously updated to accommodate new security data types and sources. This ongoing update process means that the security data fabric remains relevant and can handle emerging security challenges.

TIP

DataBee's commitment to utilizing a normalized schema through OCSF enhances security data's interoperability and effectiveness.

Enhancing Enrichment Capabilities for Nontraditional Data Types

Modern security data fabric solutions should extend beyond traditional security data to include nontraditional data types such as organizational hierarchy, business context, and external threat intelligence.

Enriching security data with these additional layers of context helps provide deeper insights. As an illustrative example, a large number of command-line activities performed by a nontechnical user in sales versus a system administrator could be a key indicator of compromise or insider threat. Overlaying organizational hierarchy could enable escalation to a manager or supervisor in the event an asset or vulnerability owner is unresponsive.

DataBee enhances enrichment capabilities by incorporating nontraditional data types into the security data fabric. For example, it supplements Azure AD/Identity providers' information with data from HR platforms. DataBee offers:

- **Business context enrichment:** By adding business context to security data, DataBee enables a deeper understanding of the potential impact of security incidents. This enrichment provides information about critical business processes, assets, and their importance, enabling the prioritization of security efforts based on business value.

- **External threat intelligence:** DataBee incorporates external threat intelligence feeds to enhance its security data. This includes information on emerging threats, known indicators of compromise (IOCs), and threat actor tactics, techniques, and procedures (TTPs). Integrating this intelligence allows for proactive threat detection and more informed decision-making.
- **Automated enrichment:** DataBee's enrichment process is automated, ensuring continuous and real-time updates to the data fabric. Automation decreases the manual effort required for data integration. It helps ensure that the security data is always current and comprehensive.

REMEMBER

DataBee's robust enrichment capabilities give organizations a more complete and contextualized view of their security landscape.

Integrating with SIEMs, BI Tools, and Ticketing Systems

Integration capabilities are crucial for a security data fabric solution. It should work seamlessly with existing SIEMs, business intelligence (BI) tools, and ticketing systems to enhance efficiency and streamline workflows.

DataBee offers robust integration capabilities to enhance the efficiency and effectiveness of security analytics and operations. This includes:

- **SIEM integration:** DataBee integrates smoothly with SIEM systems, offloading high-volume logs to reduce costs and improve performance. This helps ensure SIEMs handle high-fidelity data, enhancing threat detection.
- **BI tools integration:** DataBee connects with BI tools like Tableau and Power BI, enabling advanced analytics and dynamic reporting. This allows organizations to gain deeper insights and make data-driven decisions.

- **Ticketing system integration:** DataBee links ticketing systems to streamline incident response. This integration helps ensure efficient tracking and management of security events, improving coordination between security and IT teams.

Offering Out-of-the-Box Content and Dashboards

A security data fabric solution should provide prebuilt reports and dashboards to accelerate deployment and improve usability. These out-of-the-box resources should be customizable to meet the needs of different stakeholders within the organization.

DataBee enhances user experience with a suite of prebuilt dashboards tailored to diverse stakeholder needs, including:

- **Executive dashboards:** These focus on high-level key performance indicators (KPIs) and strategic insights. They help executives make informed decisions and communicate effectively.
- **Security operations center (SOC) team dashboards:** They provide advanced analytics and visualization tools to quickly identify, investigate, and mitigate security threats.
- **Compliance reporting:** These offer preconfigured views for continuous monitoring and reporting, aiding governance, risk, and compliance (GRC) teams in maintaining compliance and preparing for audits.
- **Threat hunting:** These dashboards use advanced algorithms and machine learning (ML) to identify suspicious activities, enabling effective detection and response to emerging threats.

IN THIS CHAPTER

- » **Building or buying your security data fabric**
- » **Enabling simplified integration and management**

Chapter 4 Benefiting from Partnering with DataBee

In today's data-driven security landscape, enterprises are under immense pressure to unify, analyze, and act on massive volumes of security data. The idea of building a custom security data fabric in-house may seem appealing because you'd have complete control, tailored architecture, and internal ownership. But the reality is quite different. It's a long, costly, and resource-intensive journey that can delay your ability to act on threats and insights when they matter most. This chapter shows how partnering with DataBee can shorten that journey and benefit your company.

Building Your Own Security Data Fabric Can Be Expensive

Building a security data fabric from scratch requires a significant investment in time, talent, and infrastructure. To do it, you'd need to assemble a cross-functional team of data scientists (DS), data engineers (DE), infrastructure engineers (IE), UI developers (UI), security engineers (SE), and operations staff (Ops).

REMEMBER

This robust team will likely spend 18 to 24 months designing and building the platform — pulling your top talent away from strategic initiatives or requiring you to go on a hiring spree.

Even after you finish building, you'll still be responsible for:

- Maintaining the data model
- Ensuring OCSF mappings and updates when source data changes
- Building, maintaining, and monitoring ingestion pipelines
- Managing data quality, resiliency, and availability
- Developing detection logic and correlation rules
- Creating dashboards and user interfaces

TIP

You can spend the next 18 to 24 months building a platform that may or may not meet your needs, or you can partner with DataBee and start delivering value to your security, compliance, and executive teams immediately. DataBee empowers enterprises to unlock the full potential of their security data today — not years from now.

Leveraging a Partnership with DataBee

If you partner with DataBee, you'll start generating insights much more quickly than you would if you built a data fabric yourself. The following sections outline six key reasons why partnering with DataBee makes sense.

Accelerating time to value

With DataBee, you can skip the build phase and start leveraging a proven, cloud-native platform designed for scale immediately. Instead of spending a year building infrastructure, you'll spend that year gaining insights, improving detection, and mitigating risk.

Engineering for scale and resilience

DataBee is already battle-tested in large enterprise environments, processing over 60 TB of data daily. It offers:

- High availability and platform resiliency
- Optimized, cost-transparent pipelines
- Patent-pending entity resolution technology
- Real-time enrichment and detection chaining

Providing entity resolution technology

Entity resolution is the process of identifying and correlating information or records of real people, devices, and applications so that security teams can correlate information from various tools across any security event, regardless of log source. This technology, unique to DataBee, automates the manual effort required to manage an up-to-date and ever-changing asset inventory across tools and sources that represent users and devices differently.

Enabling security teams with clean, usable data

DataBee ensures your analysts and threat hunters work with high-quality, normalized data — freeing them from the burden of cleaning and correlating logs. This means:

- Faster threat detection
- Fewer false positives
- More time spent solving problems, not wrangling data

Delivering real-time data and compliance dashboards for GRC teams

DataBee enables your governance, risk, and compliance (GRC) teams to be audit-ready throughout the year with high-quality, normalized data, enabling them access to reliable data all year round. This means:

- Faster answers to compliance questions
- Less time pulling and correlating data for compliance updates and reports
- More time spent mitigating risks and improving compliance SLAs

Benefiting from continuous innovation and support

As a DataBee partner, you benefit from:

- Ongoing platform enhancements and new features
- SLA-backed support
- Seamless integration of OCSF updates
- Custom extensions for your unique use cases
- Influence over the roadmap based on your needs

Providing simplified integration and management

DataBee offers:

- A simple wizard to connect to your data lake or data storage platform
- Managed pipelines for ingesting, writing, and searching data
- Multiple ingestion methods and source mappings
- Built-in data quality monitoring

Chapter 5

Four Ways DataBee Can Help You Get Results

Modern enterprises struggle with fragmented data, reactive compliance, and inefficient threat hunting. DataBee addresses these challenges through a comprehensive security data fabric that helps unify data management, automate compliance monitoring, enable intelligent discovery of assets, and scale threat hunting operations. This chapter presents four ways DataBee can help you get results.

Breaking Down Silos for a Unified View

Large enterprises have fragmented data scattered across dozens of tools, teams, and departments, creating silos that block visibility and undermine trust.

DataBee empowers security, compliance, and business teams to work from a single, accurate, real-time data foundation. By consolidating disparate data sources across networks, applications, endpoints, and organizational hierarchies, DataBee enables a holistic view of the enterprise's security posture and compliance status.

DataBee transforms raw data into actionable intelligence through a systematic approach. It achieves this by:

- Connecting directly to enterprise systems like Microsoft Defender for Endpoint, ServiceNow CMDB, and Workday via application programming interfaces (APIs)
- Processing data through DataBee's parsing, normalization, and transformation engine for consistency
- Depositing structured, normalized data into centralized data lakes or cloud storage
- Updating dashboards daily, tying metrics to responsible parties for accountability

The platform visualizes the full asset estate, including endpoint coverage and ownership hierarchy, links assets to the organizational structure, showing ownership chains, supports EDR compliance reporting with normalized data, and enables daily dashboard refreshes for current visibility. This helps create improved data accuracy across systems, enhanced accountability through individual metrics, reduced manual reconciliation, and scalable analytics via cloud-native infrastructure.

TIP

Enterprises using DataBee have normalized and centralized data from multiple systems, enabling holistic security and compliance views. By integrating business context with technical data, organizations gain deeper insights that drive smarter, more informed decisions.

Enabling Continuous Compliance and Audit Readiness

Traditional compliance efforts are often reactive, leaving teams scrambling to prepare for audits. DataBee delivers continuous, automated compliance visibility instead.

Daily dashboard updates ensure compliance metrics stay current, enabling proactive action rather than reactive reporting. DataBee fosters collaboration among security, compliance, finance, and leadership teams, ensuring alignment and shared understanding.

DataBee helps clients produce trending compliance reports that track progress over time, assign business unit compliance scores for accountability, facilitate data lineage transparency to enhance enterprise trust, and optimize storage costs through data consolidation.

A major enterprise used DataBee to identify a business unit with low endpoint agent coverage, enabling targeted remediation. Collaboration with in-house auditors created self-service compliance dashboards, allowing business units to monitor compliance status weekly or monthly, well ahead of formal audits.

TIP

Self-service dashboards for managers reduce manual reconciliation, save time, and foster trust between compliance, IT, and business units.

Solving the Asset and Vulnerability Puzzle

Asset visibility and ownership clarity are critical for vulnerability management, but they're often elusive. Unknown assets and unclear ownership create remediation delays, excessive ticket reassignments, and operational inefficiencies.

DataBee's patented entity resolution technology delivers intelligent asset discovery and ownership attribution at scale. By weaving together user activity, asset telemetry, and organizational hierarchy, DataBee creates a dynamic, enriched view of the enterprise asset landscape, identifying gaps, assigning accountability, and providing clean data back to the configuration management database (CMDB).

The smart asset discovery process correlates user and asset activity using unique tracking IDs to identify unknown or orphaned assets; suggests multiple potential owners per asset with confidence scores based on behavioral and authentication patterns; automatically updates the CMDB with enriched ownership data; and utilizes artificial intelligence (AI)-driven outreach to notify and confirm ownership, enabling accelerated remediation workflows.

WARNING

Poor asset data leads directly to slower remediation. Without clear ownership, even critical vulnerabilities can remain unresolved.

Empowering In-House Threat Hunting at Scale

Cybersecurity teams spend excessive time cleaning and correlating logs rather than hunting threats. DataBee changes this equation by providing clean, contextualized data, reducing the need for manual preparation overhead.

DataBee ingests, cleans, and normalizes data from across the enterprise into a common schema, giving threat hunters and security operations center (SOC) analysts ready-to-use data. This means analysts spend less time wrangling data and more time solving problems.

The platform ingests and normalizes data beyond the security information and event management (SIEM) tools, including endpoints, cloud services, and identity systems. It combines business context with security telemetry, enriching data with ownership, location, and organizational hierarchy.

DataBee deposits clean, structured data into a centralized repository for fast and flexible querying, and supports historical data for investigating long-dwell threats.

DataBee enables fast threat detection using a cloud-native search engine supporting parallel queries. It helps reduce false positives by surfacing real signals through optimized preprocessing and provides seamless access to non-SIEM data sources for comprehensive investigations.

Automated sweeps of tens of thousands of indicators of compromise across large security data lakes are completed rapidly, enhancing threat intelligence and response.

DataBee helps reduce analyst fatigue by reducing manual data cleaning and correlation. It enables accelerated investigations with ready-to-query, high-quality data; enhances detection accuracy through complete, contextualized environmental views; and enables proactive threat hunting rather than reactive alert triage.

Key benefits include clean, normalized data fueling fast and accurate threat detection; enhanced analyst efficiency, freeing time for deeper investigations; threat hunting that scales across massive datasets; and security teams gaining confidence in their protective data.

REMEMBER

By freeing analysts from data wrangling, DataBee enables proactive threat hunting rather than reactive alert triage.

Transform security ops with data fabric

Security data is scattered and overwhelming. A security data fabric unifies it, turning noise into insight. Discover how to break down silos, stream every source into a single view, and power AI-driven analytics. You'll have sharp threat detection, instant response, and audit-ready compliance. Gain the 360-degree visibility modern teams need to help them act quickly, defend effectively, and stay ahead.

Inside…

- Master security data challenges
- Break down data silos
- Enhance threat detection
- Enhance data quality and trust
- Streamline compliance efforts
- Optimize security tools

DataBee®
A COMCAST COMPANY

Stephanie Diamond is a marketing innovator and author with more than 25 years of marketing experience. She writes retail and custom e-books for Fortune 500 companies and is known for transforming complex ideas into engaging narratives. She is a certified Buzan Mind Mapper.

ISBN: 978-1-394-24367-9
Not For Resale

9 781394 243679

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT