DataBee™ | COMCAST TECHNOLOGY SOLUTIONS

Datasheet

DataBee™ for Security Threats

Threats aren't vendor specific — your threat detections shouldn't be either. The average enterprise's technology stack is a labyrinth to navigate and can deliver inconsistent security coverage and context. The operational and costly impact of vendor lock-in can also make managing upstream and downstream integration points such as updating log parsers and custom detection content an additional stressor to already limited time and resources.

Introducing DataBee for Security Threats

The DataBee Hive™ is a security, risk, and compliance data fabric platform that enables you to achieve strategic and tactical threat detection and hunting objectives.

Strategic

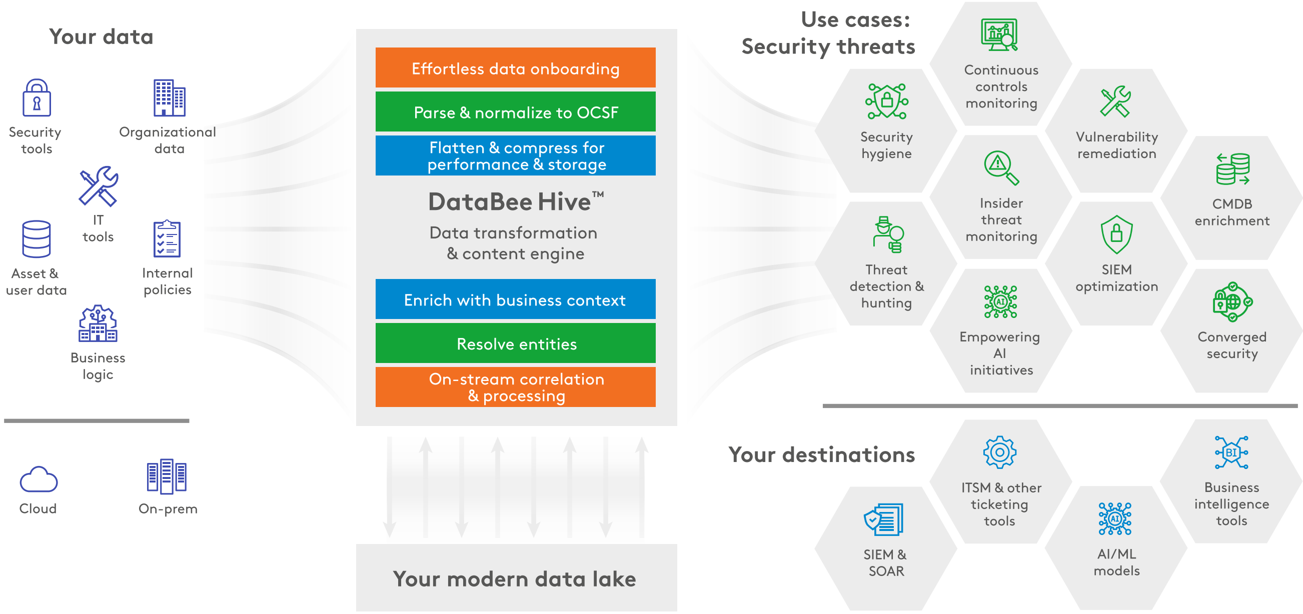
- Reduce SIEM reliance and costs.
- Comply with log retention regulations.
- Ensure sufficient historical data for more conclusive digital forensic investigations.

Tactical

- Enhance detection with high-volume, underutilized logs and feeds.
- Reduce log ingestion costs and total cost of security ownership.
- Automatically apply detection rules using open-source, vendor-agnostic rules.

Threat hunting and insider risk monitoring just got easier with DataBee EntityView™. Leveraging patent-pending entity resolution technology that triangulates users, devices, and their activities, threat hunters have a contextualized view of a user's activity to identify nefarious behaviors and help write AI/ML or other prescriptive algorithms to catch and investigate threats faster. The automated correlation engine improves key metrics like mean time to detect (MTTD) and mean time to respond (MTTR) while eliminating the need for manual data engineering and science resources.

Don't let data go unused and wasted. DataBee™ from Comcast Technology Solutions delivers additional context and faster detection by enabling you to analyze traditionally cost-prohibitive and voluminous data like DNS logs and Window Events logs for connected, actionable intelligence. When time is important for threat detection, as data streams to its destinations, DataBee applies sigma rules, an open-source signature format, for real-time, high-fidelity alerts for additional analysis.



Your data

Security tools

Organizational data

IT tools

Asset & user data

Internal policies

Business logic

Cloud

On-prem

Effortless data onboarding

Parse & normalize to OCSF

Flatten & compress for performance & storage

DataBee Hive™

Data transformation & content engine

Enrich with business context

Resolve entities

On-stream correlation & processing

Your modern data lake

Use cases: Security threats

Continuous controls monitoring

Security hygiene

Vulnerability remediation

Insider threat monitoring

CMDB enrichment

Threat detection & hunting

SIEM optimization

Empowering AI initiatives

Converged security

Your destinations

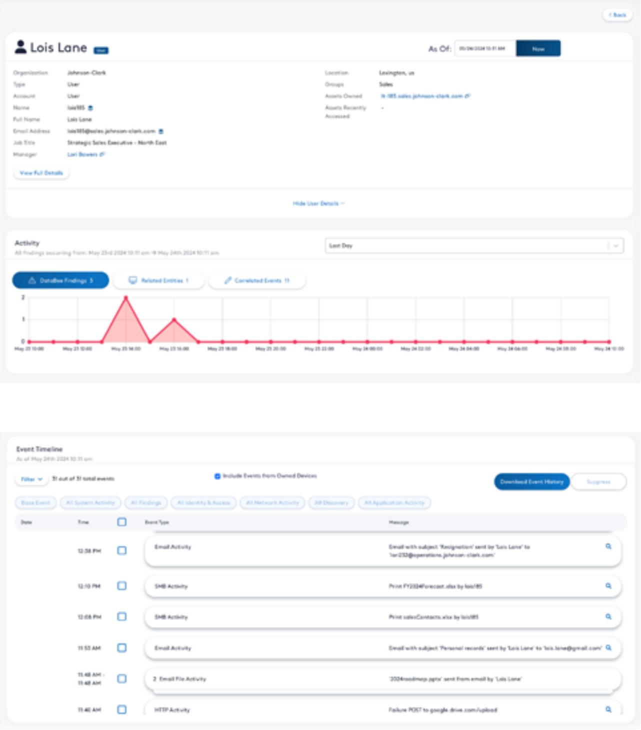
ITSM & other ticketing tools

Business intelligence tools

SIEM & SOAR

AI/ML models

For effective, fast detection and response, enterprise security teams need real-time, reliable insights contextualized with security content and enriched with business logic as data travels to its destinations.



‹ Back

Lois Lane User

As Of: 05/24/2024 10:11 AM Now

Organization	Johnson-Clark	Location	Lexington, us
Type	User	Groups	Sales
Account	User	Assets Owned	lt-185.sales.johnson-clark.com
Name	lois185	Assets Recently Accessed	-
Full Name	Lois Lane		
Email Address	lois185@sales.johnson-clark.com		
Job Title	Strategic Sales Executive - North East		
Manager	Lori Bowers		

View Full Details

Hide User Details

Activity

All findings occurring from: May 23rd 2024 10:11 am → May 24th 2024 10:11 am

Last Day

DataBee Findings 3 | Related Entities 1 | Correlated Events 11

Event Timeline

As of May 24th 2024 10:11 am

Filter 31 out of 31 total events ☑ Include Events from Owned Devices Download Event History Suppress

Base Event | All System Activity | All Findings | All Identity & Access | All Network Activity | All Discovery | All Application Activity

Date	Time	□	Event Type	Message
	12:38 PM	□	Email Activity	Email with subject 'Resignation' sent by 'Lois Lane' to 'lori232@operations.johnson-clark.com'
	12:10 PM	□	SMB Activity	Print FY2024Forecast.xlsx by lois185
	12:08 PM	□	SMB Activity	Print salesContacts.xlsx by lois185
	11:53 AM	□	Email Activity	Email with subject 'Personal records' sent by 'Lois Lane' to 'lois.lane@gmail.com'
	11:48 AM - 11:48 AM	□	2 Email File Activity	'2024roadmap.pptx' sent from email by 'Lois Lane'
	11:40 AM	□	HTTP Activity	Failure POST to google.drive.com/upload

DataBee EntityView aggregates atypical data sources from a user, Lois Lane, and her devices and activities to show malicious insider behaviors.

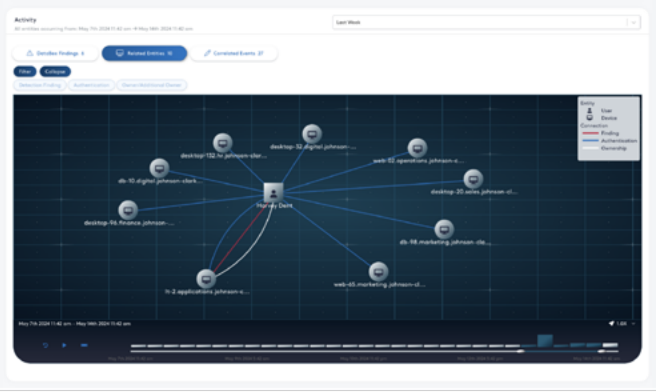
Benefits of DataBee for Security Threats

Automate threat detection and chaining in real-time data streams

DataBee delivers connected insights from large, disparate datasets fast and, with Active Detection Streams, applies up-to-date security content and sigma rules to data as it travels to its destinations. Automatically link together security and non-security events with Detection Chaining to reduce the noise and improve threat hunting and insider risk monitoring. Leverage the Related Entity Graph to visualize an entity's correlated event timeline, including when a detection rule was alerted and how other assets, devices, or users were affected.

Focus on analysis, not data normalization and engineering efforts

DataBee processes and normalizes the data so your security team can spend less time behind a wall of alerts and more time focusing on the most important users, devices, or fields and analyzing your environment for threats. Active Detection Streams from DataBee applies sigma rules without fine-tuning your data streams to create a more effective and flexible workbench for security analytics. Active Detection Streams also automates the management of signatures, making it easier to protect against yesterday's threats and tomorrow's zero-days.

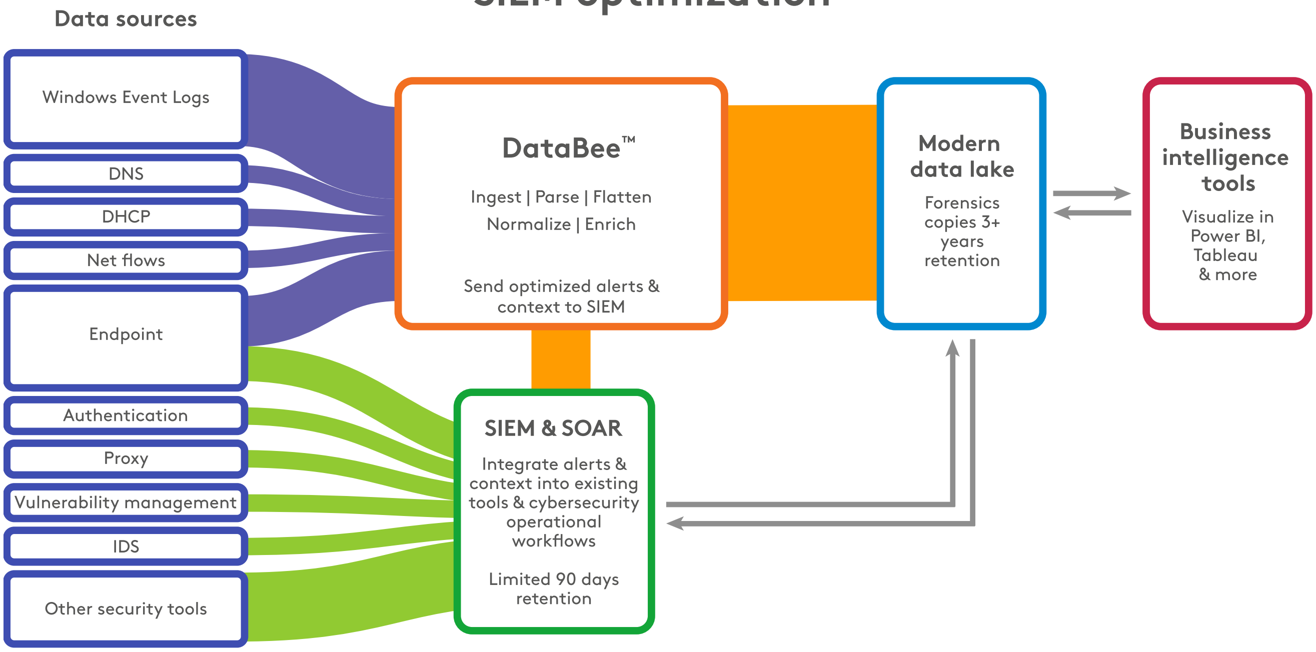

Activity
All entities occurring from: May 7th 2024 11:42 am → May 14th 2024 11:42 am
Last Week
DataBee Findings 6
Related Entities 10
Correlated Events 27
Filter
Collapse
Detection Finding
Authentication
Owner/Additional Owner
Entity
User
Device
Connection
Finding
Authentication
Ownership
desktop-132.hr.johnson-clar...
desktop-32.digital.johnson-...
web-02.operations.johnson-c...
db-10.digital.johnson-clark...
desktop-20.sales.johnson-cl...
Harvey Dent
desktop-96.finance.johnson-...
db-98.marketing.johnson-cla...
web-65.marketing.johnson-cl...
h-2.applications.johnson-c...
May 7th 2024 11:42 am - May 14th 2024 11:42 am
1.6X

Aggregate alerts and optimize SIEMs to control costs

DataBee streamlines the process of identifying and correlating related alerts across different SIEMs, enriching them with additional logs and data sources and adding business context to attain an actionable security event narrative. With DataBee, your analysts aren't wasting time pivoting between multiple interfaces and your data engineers aren't arduously trying to integrate multiple SIEM and SOAR products together.

DataBee enhances threat detection and lowers SIEM costs by redirecting high-volume, underutilized logs to a more affordable data fabric and data lake infrastructure. Reintroduce logs from Windows Event, DNS, DHCP, and EDR for threat detection and insider risk monitoring that was previously too costly to send to SIEMs. Let your SIEM focus on its strengths — analysis, detection, and reporting — while you retain core security logs and access data on demand.

SIEM optimization



Data sources

Windows Event Logs

DNS

DHCP

Net flows

Endpoint

Authentication

Proxy

Vulnerability management

IDS

Other security tools

DataBee™

Ingest | Parse | Flatten
Normalize | Enrich

Send optimized alerts & context to SIEM

Modern data lake

Forensics copies 3+ years retention

Business intelligence tools

Visualize in Power BI, Tableau & more

SIEM & SOAR

Integrate alerts & context into existing tools & cybersecurity operational workflows

Limited 90 days retention

Gain flexibility and begin your vendor-agnostic journey

DataBee helps you break free from vendor-specific query languages and tool lock-in. Designed to future-proof your security investments and enhance your existing technology stack, DataBee aligns with the Open Cybersecurity Schema Framework (OCSF) format, which can be used by multiple personas in the security, risk, privacy, and compliance organization, and the data quality and integrity can be verified within the platform. DataBee handles the translation from sigma to OCSF to help lower the level of effort needed to adopt and support organizations on their journey to vendor-agnostic security operations. With sigma-formatted detections leveraging OCSF in DataBee, organizations can swap out security vendors without needing to update log parsers or security detection content.

Get started with DataBee

DataBee meets you where you are with your data — whether that is on-premises, in the cloud, or applications — and weaves together related data points, normalizing to the OCSF format and enriching with business context. Security operators, analysts, and threat hunters can now use the same time-series dataset rich with business-relevant information for their security workflows.

Inspired and proven at Fortune 20 scale, DataBee unlocks the power of your security data so your enterprise can make data-driven, informed cybersecurity investment decisions based on business and security needs.

Get a custom demo of DataBee for Security Threats →

DataBee™ | COMCAST TECHNOLOGY SOLUTIONS