DataBee®
A COMCAST COMPANY

Solution Brief |

DataBee® for Security Threats

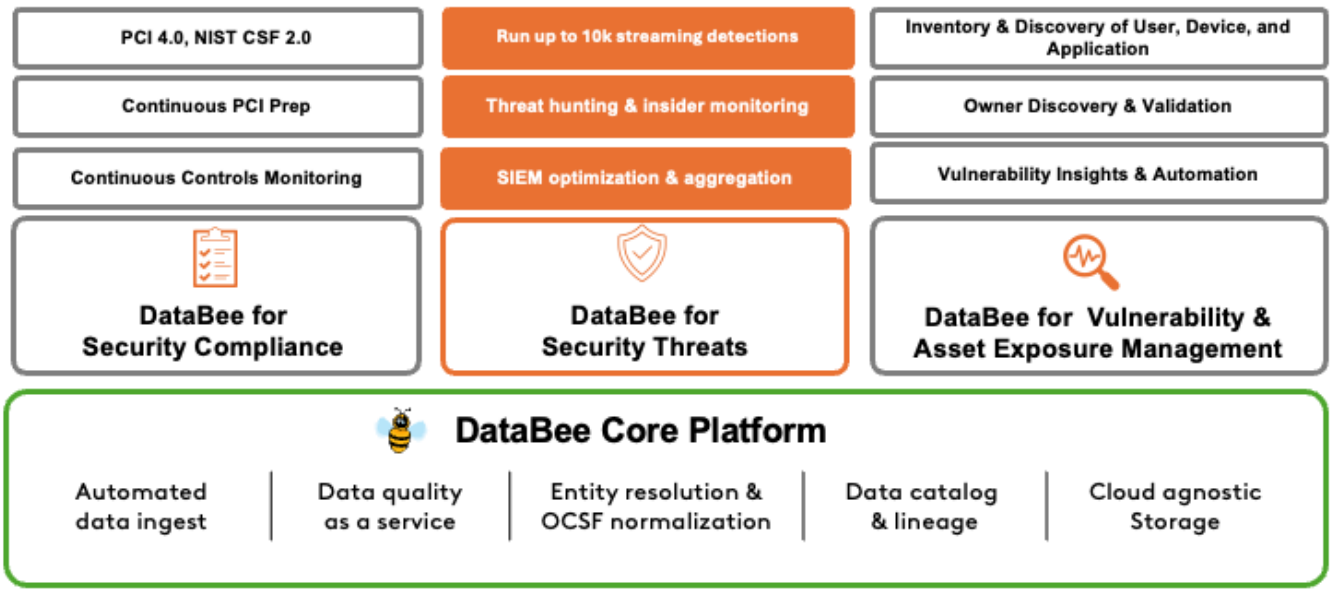
The challenge

Security analytics processes and technologies have existed for decades, but we are still chasing satisfactory insights. Existing approaches, like SIEM, are falling out of fashion due to rising costs and limited retention capabilities. Home-grown ETL processes are expensive to build and maintain as technology stacks change. And systems that are meant to aggregate alerts and enact controls, like XDRs, haven't lived up to expectations. Security analytics teams need accurate answers quickly, and increased coverage and visibility while staying within budget constraints. This means they need to be in possession of data that is complete and accurate, in an analytics-ready state, and working with the right algorithms.

Introducing DataBee® for Security Threats

DataBee® for Security Threats helps security teams work faster and more efficiently. You no longer have to be selective about what logs you'd like to retain and analyze to keep costs down. DataBee's cost-effective computation engine and automated ingestion that supports 275+ data sources from hybrid on-premises and cloud environments means you can include everything, from your org chart hierarchy to your Windows event logs, to a CSV file in the data set.

DataBee widens your detection coverage against the MITRE ATT&CK framework with its streaming architecture, Sigma rules and detection engine, which supports running up to 10,000 detections concurrently for near real-time insights. DataBee takes care of automating entity correlation and enrichment, creating a single time-series data view. Security and analytics teams can use the related entity graph feature to visualize when a detection rule was alerted and how other assets, devices, or users are affected.



Hunt with context

DataBee eliminates the need for manual correlation work on data sets or resolving overlapping entities to prepare them for threat hunting. With DataBee, you can threat hunt without advanced skillsets or tools and catch low-and-slow attacks before they build up with an entity-centric, time-series view of user activity.

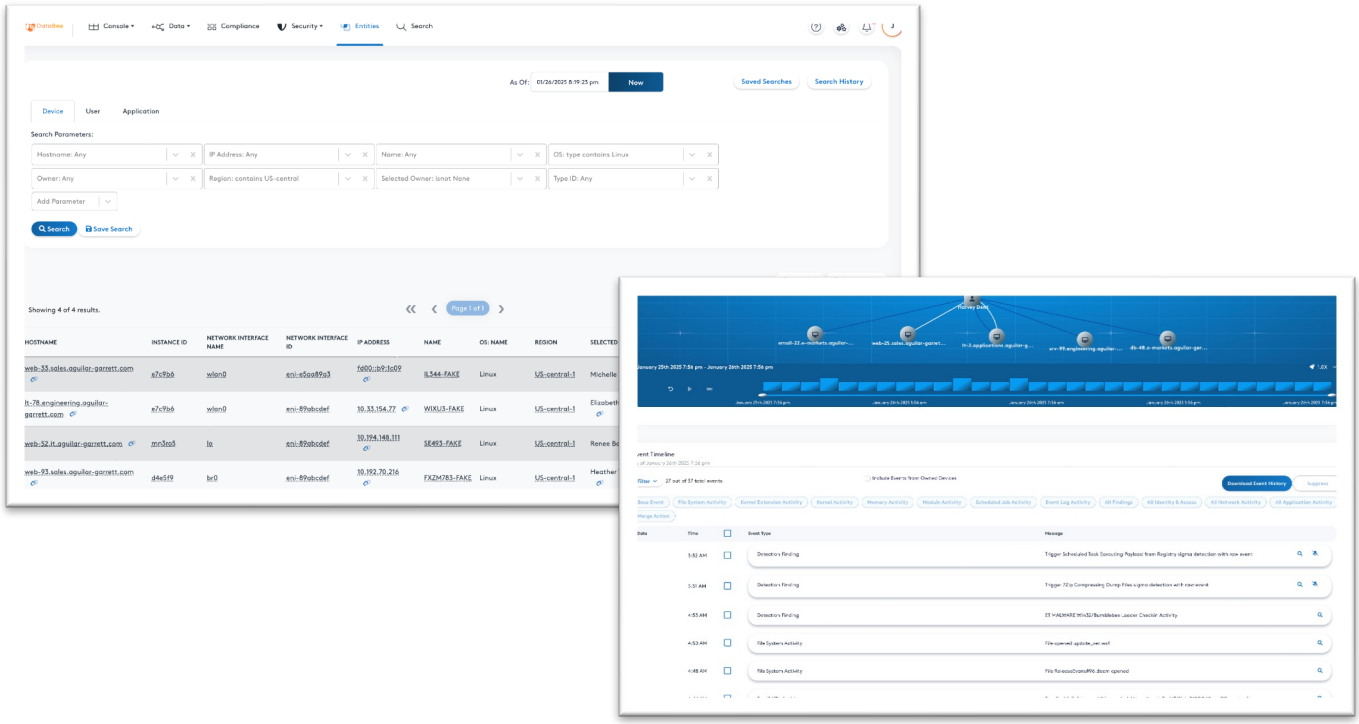
Patent-pending entity resolution technology creates a consolidated, single record of users, devices and applications across all data sources. With DataBee's detection chaining feature, any OCSF based activity and insights from all detection tools are correlated and organized into timelines for each unique entity.

DataBee EntityViews™ for faster answers

Analysts and threat hunters are a quick click away from a contextualized, time-series view of a user, device, or application's activity. This happens in real time, continuously and across any data source. In just five clicks, get insights that would take up to 24 hours and 100+ queries in a traditional SIEM. Analysts have higher fidelity detections because they are based on a complete activity timeline.

Reduce SIEM costs and simplify analysis

Shrink or eliminate your dependencies on SIEMs and MSSPs with our cost-effective, streaming data fabric architecture that allows you to store the data in your mode of choice. Unlike typical SIEMs, add insights from high-volume event data sources without additional cost. Also, aggregate alerts from multiple SIEMs, or output to a SIEM or SOAR platform for playbook execution. We use OCSF which we keep updated for you with the latest additions from the community.



Are you ready to take advantage of a security data fabric? Let's talk.

Request a custom DataBee demo at DataBee.buzz

DataBee®, a Comcast Company, offers the DataBee cloud-native security, risk and compliance data fabric platform, and BluVector®, an on-premises network detection and response (NDR) platform, to some of the world's large enterprises and federal agencies. We help our customers work smarter with an evidence-centric approach to security that prepares them for what's next. Developed and proven at scale, DataBee delivers connected security and compliance data and insights that can work for *everyone* in an organization. Built to protect critical government and enterprise networks, BluVector delivers AI-powered NDR for visibility across network, devices, users, files, and data to discover and hunt skilled and motivated threats.