DataBee®
A COMCAST COMPANY

Solution Brief |

DataBee® for Vulnerability and Asset Exposure Management

The challenge

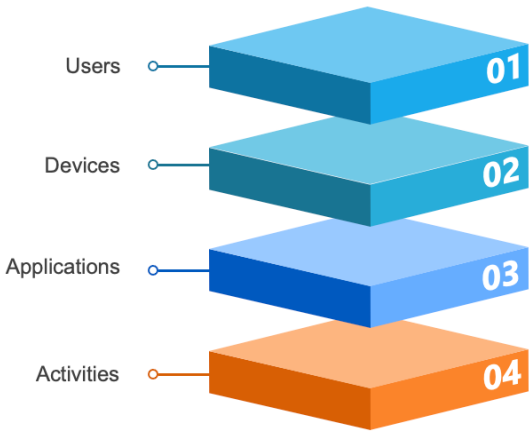
Asset and application inventories are a challenge to keep accurate and up to date. Meanwhile, vulnerabilities for applications are being disclosed at a higher rate every year and with a shorter window of time to patch before threat actors exploit them.

As business needs change, CMDBs can become quickly outdated. Network-based vulnerability scanners tell you about vulnerabilities but don't tell you who can fix them. This slows down remediation efforts, potentially resulting in unresolved vulnerability findings that leave an open door for a successful attack. For modern enterprises already enriching their vulnerability findings beyond IP addresses and hostnames, there is a need to find further efficiencies such as by reconciling findings from multiple scanning tools, cross-correlating vulnerability findings with related detections or intelligence, and more.

Introducing DataBee® for Vulnerability and Asset Exposure Management

The DataBee Platform is a data ingestion, transformation and computation engine that helps security and data analytics teams find answers. It creates analytics-ready datasets by automating data pipelines, reducing complexity among disparate data sets, and creating insights with business and policy context. This means less manual effort on your part to organize data to make it useful to your analysts.

Instead of chasing down and verifying owners manually -- a process that can take days, weeks or even months to complete, leaving vulnerability findings unresolved and inventories incomplete -- let DataBee automate the finding and validation of asset and application owners. With the DataBee BeeKeeper gen AI chatbot feature, DataBee can help you discover assets and applications in your environment, suggest owners for unclaimed or orphaned devices based on authentication logs and usage telemetry, and reach out to those users to validate findings.

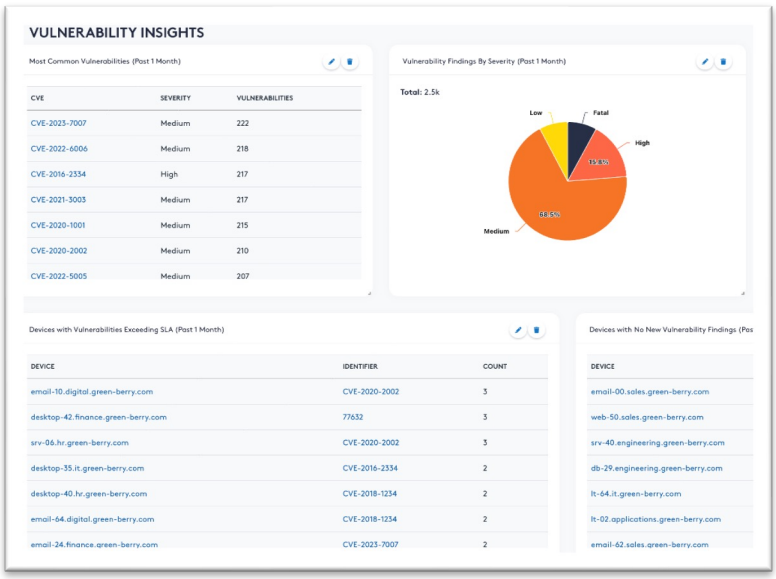


Security and IT teams share the same data views and the dataset they use is normalized to the Open Cybersecurity Schema Framework (OCSF) schema, making it easy for vulnerability management and IT asset teams to take a more collaborative and automated approach that improves operational efficiency and strengthens overall security posture.

Asset and application discovery and visibility

DataBee actively discovers assets and applications in your technology stack by creating a comprehensive inventory of users, devices, and applications. A single identifier is created using a patent-pending entity resolution technology across a single or multiple data source that refers to the same real-world entity. This can be created by ingesting data from traditional sources for asset management like the CMDB, directory services, and vulnerability scanner, but also non-traditional data sources such as authentication logs, or application life cycle events. When a new device or application is discovered or the owner is not indicated, DataBee will leverage the events streaming through the platform to make a suggestion of the potential owners of the device or application.

Fortify your SLA closure rate for vulnerability remediation



The Vulnerability Insights Console in DataBee can be used to customize and track your vulnerability management program, highlighting critical insights such as:

- **Application Owner Discovery:** Quickly find responsible owners
- **Top Offenders:** Identify the owners with the most open vulnerability findings
- **Highlight Past Due Vulnerabilities:** Customize to your SLAs by Severity
- **Devices that Drop Off of Vulnerability Scans:** Define expected scan frequency

Enrich your CMDB and automate vulnerability remediation actions

Keep your source of truth *the* source of truth by integrating DataBee with your CMDB to gain additional business context such as ownership and improve downstream workflows. DataBee understands that not all risks and vulnerability findings are equally critical. Automate your vulnerability remediation with actions that trigger ServiceNow ITSM with ticket creation to kick off workflows.

Gen AI chatbot to find and validate asset and application owners

DataBee supports operational efficiency and analysts' productivity because they no longer have to manually correlate entity information or chase people down to verify device and application owners. By correlating authentication logs with telemetry from the tools, your organization can let DataBee BeeKeeper, our gen AI chatbot, help verify device or application owners as well as suggest potential owners for unclaimed or orphaned entities.

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.