Key Benefits

Data hygiene
Reduce and manage data volumes by standardizing redaction, filtering, and routing processes.

Data manipulation
Normalize and enrich diverse data formats for end-to-end visibility into the full scope of your environment.

IT governance
Standardize a data governance model to consistently populate high-quality, enriched alert data across teams.

At-a-glance analytics
Measure and optimize strategic value across all your tools, in real-time.

BigPanda and Cribl combined delivers greater situational AIOps awareness with less cost

Access more observability data at a lower cost

Cribl's observability pipeline enables organizations to ingest more descriptive observability data that delivers a new stream of actionable events that would have been too costly to otherwise produce. Cribl transforms data in flight by collecting, processing, and routing only priority observability data from multiple destinations into BigPanda, which is used to enrich and correlate complex data into actionable incidents. This combination avoids observability tool costs from extra CPU search cycles or unnecessary data storage fees.

Gain greater awareness of your IT environment

Convert high volumes of complex, unactionable heterogeneous observability data such as logs, traces, alerts, events, changes, topology and relationship telemetry into a single, normalized stream of topology metadata representing your on-prem and cloud IT environments. Use this data to enrich correlated alerts and incidents in real-time which make it easier and faster to respond to alerts before they become incidents. Furthermore, Cribl makes it easy to mask PII data at rest for compliant access to sensitive alert data that broadens the scope of infrastructure awareness within BigPanda.

Reduce observability data complexity to identify actionable alerts

Easily eliminate duplicate fields, null values, and any elements that provide little analytical value. Set parsing rules for incoming alert payloads and use AI tag normalization to pre-process the content to match incoming data requirements before it reaches the BigPanda which improves system performance and reduces storage costs.

Get started with BigPanda

www.bigpanda.io

Key Capabilities

Cribl

- **Data collection:** Cumulate widespread observability data from multiple endpoints and APIs, recall data from low-cost storage, and gain access to otherwise private data sources.
- **Data quality governance:** Eliminate duplicate fields, null values, and elements that provide low analytical value.
- **Accelerate enrichment:** Translate and transform varied data language from all sources to a single normalized format to streamline the enrichment of third-party data.

BigPanda

- **Cross-source correlation:** Use AI and machine learning to correlate high-quality alerts and critical topological context together, collected from all your CI/CD tools, against your incidents in real-time to surface root cause changes and create a small number of incidents.
- **Automation workflow:** Accelerate incident triage by mobilizing the right escalation teams and experts for automated notifications, ticketing, and remediation.
- **Unified Analytics:** Purpose-built analytics and reporting solutions for ITOps provide deep visibility into KPIs, metrics, and trends that can be used to drive continuous optimization.

Cribl and BigPanda offer native integration between both platforms

Business Value	Data governance	Turn insights into action	Automate ITOps workflows
Challenge	Enterprises are now able to collect more data than they can effectively analyze, with some enterprises reporting utilizing less than 2% of collected data. Varied data quality, and siloed monitoring and observability tools trap important insights in closed-off locations, on different systems, and in different formats.	Correlated alerts and incidents that lack descriptive metadata on the nature of the problem, the systems that are impacted, and business priority, for example, make it hard for response teams to triage quickly and efficiently. These delays impact an organization's ability to scale through technology and not headcount.	Manual ticket creation and remediation are both time-consuming, error-prone, and subject to becoming quickly out-of-date as incident status change frequently.
How BigPanda and Cribl help	Dramatically reduce low-value noise by de-duplicating, filtering out false positives, and eliminating benign data by 90% and focus on a broader scope of priority events that are actually related to data you want to monitor or incidents you need to resolve.[2]	Enrich correlated alerts with descriptive metadata that give response teams valuable insights on how to easily sort, filter, visualize, and act on priority incidents. This helps accelerate triage, boost efficiency, and reduce MTTR.	Automate ticket creation and keep dynamically changing status synced between the NOC and response teams in real-time status. BigPanda also notifies the right teams at the right time by automating workflows with chat, on-call notifications, and auto-remediation systems.
Benefits	Manage observability storage needs and control costs by reducing and compressing observability data into only high-quality insights that you are actually interested in.	Accelerate incident triage and increase team bandwidth by lowering MTTR.	Streamlining and automating ITOps activities boosts operational efficiency and reduces costs while allowing ITOps to scale using technology, not headcount.

[1] https://cribl.io/blog/theres-nuggets-in-them-buckets/ [2] https://www.bigpanda.io/our-product/alert-intelligence/