BigPanda

Solution brief

Improve situational AIOps awareness with BigPanda and Cribl

Access more observability data at a lower cost.

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.

Analytics at-a-glance

Measure and optimize strategic value across all your tools in real-time.

Cribl's observability pipeline enables ingestion of more descriptive observability data, creating a new stream of actionable events that would have otherwise been too expensive to produce. Cribl transforms data in flight by collecting, processing, and routing only priority observability data from multiple destinations into BigPanda, which then enriches and correlates complex data into actionable incidents. This integration avoids observability tool costs from extra CPU search cycles or unnecessary data storage fees.

Increase 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-premises and cloud IT environments. Use the data to enrich correlated alerts and incidents in real-time to simplify and speed response before alerts become incidents. Cribl makes it easy to mask PII data at rest for compliant access to sensitive alert data to broaden the scope of infrastructure awareness within BigPanda.

Reduce observability data complexity

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

Key capabilities

Cribl

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

BigPanda

- **Cross-source correlation:** Use AI and ML to correlate high-quality alerts and critical topological context. Collect data from all CI/CD tools against your incidents in real-time to surface root-cause changes and create a small number of incidents.
- **Automation workflow:** Accelerate triage by mobilizing the right escalation teams and experts to automate notifications, ticketing, and remediation.
- **Unified Analytics:** Use purpose-built analytics and reporting for ITOps to increase visibility of KPIs, metrics, and trends that you can use to drive continuous optimization.

Get started with BigPanda and Cribl.

bigpanda.io

	Data Governance	Actionable Insights	Automated ITOps Workflows
Challenge	You collect far more data than you can access and analyze. (Some organizations report that they utilize less than 2% of collected data.) Varied data quality combined with siloed monitoring and observability tools trap important insights in a variety of systems and in different formats.	Correlated alerts and incidents that lack descriptive metadata make it to triage quickly and efficiently. For example, teams need detail on nature of the problem, the systems impacted, and business priority. These delays impact your ability to scale through technology instead of headcount.	Manual ticket creation and remediation are time-consuming, error-prone, and subject to becoming quickly outdated as incident status changes frequently.
How BigPanda helps	Dramatically reduce low-value noise by de-duplicating, filtering out false positives, and eliminating benign data by 90%. Use BigPanda Alert Intelligence to focus on a broader scope of priority events related to data you want to monitor or incidents you need to resolve.	Enrich correlated alerts with descriptive metadata to give response teams valuable insight into how to easily sort, filter, visualize, and act on priority incidents. Accelerate triage, boost efficiency, and speed mean time to resolution (MTTR).	Automate ticket creation and synchronize dynamically changing status between the NOC and response teams in real-time. Notify the right teams at the right time by automating workflows with chat, on-call notifications, and auto-remediation systems.
Business value	Manage observability storage needs and control costs. Reduce and compress observability data into the high-quality insights that affect your operations.	Accelerate incident triage and increase team bandwidth by reducing MTTR.	Streamline and automate ITOps activities to boost operational efficiency and reduce costs while allowing ITOps to scale without additional headcount.

Copyright © 2024 BigPanda. BigPanda, the BigPanda logo, BigPanda Alert Intelligence, BigPanda Incident Intelligence, BigPanda Workflow Automation, BigPanda Data Engineering, BigPanda UnifiedAnalytics, BigPanda AI Engine, AIOps Incident Intelligence and Automation, and "IT's on." are properties of BigPanda, Inc. All rights reserved. All other trademarks and copyrights are the property oftheir respective owners.