DATASHEET

BigPanda

Event Correlation, powered by AIOps

BigPanda's Event Correlation prevents incidents from escalating into painful outages.

The typical modern enterprise has invested in 15 or more observability and monitoring tools. These tools provide their IT Ops, NOC, DevOps and SRE teams with deep visibility into critical applications, systems and infrastructure, both on-prem and in the cloud.

But these tools also generate very large volumes of IT alerts that, combined with topology and change data streams, overwhelm those teams. Because they're overwhelmed, these teams can't easily detect IT incidents before they escalate into crippling outages.

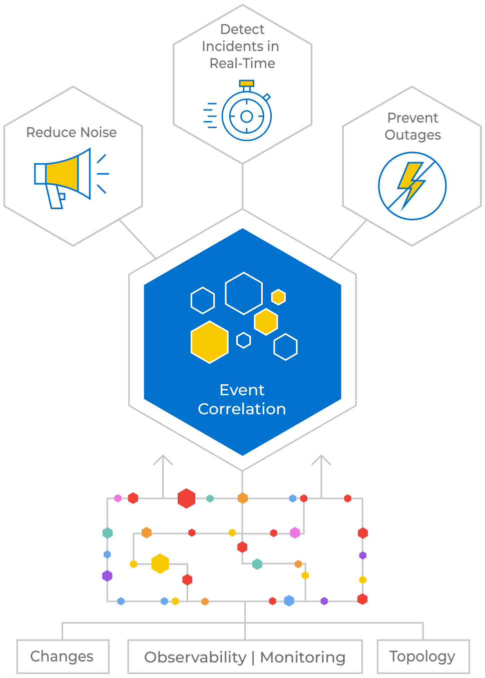
BigPanda's Event Correlation helps these teams detect, investigate and resolve incidents in real-time. By aggregating, normalizing and enriching data from monitoring, change and topology tools, and subsequently correlating this data using AI/ML, event correlation dramatically slashes IT noise and helps IT teams detect incidents as they form.

How it works

BigPanda's Event Correlation aggregates and correlates disparate streams of observability, monitoring, change and topology data into context-rich incidents.

Using 50+ out-of-the-box integrations and powerful REST APIs, BigPanda connects to existing observability and monitoring tools and aggregates their data in real-time. The system normalizes the data into a consistent format and adds context by bringing in topology and operational data.

With Open Box Machine Learning (OBML), BigPanda then correlates the collected alert and topology data into a handful of context-rich incidents, dramatically reducing the noise. By helping teams detect and take action on incidents as they form in real-time, BigPanda prevents those incidents from escalating into outages.



Eliminate noise

Compress alert streams from any source by over 95% with Open Box Machine Learning.

Add context

Enrich alerts with topology, business context and root cause changes.

Gain visibility

Leverage ready-to-go reports and dashboards to measure operational KPIs and trends.

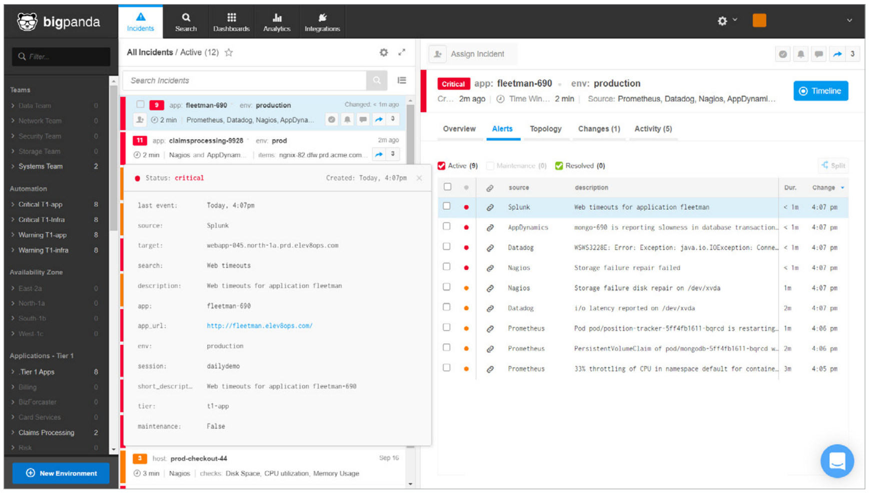
BUNGiE

Bungie, the gaming studio behind blockbuster gaming franchises such as Halo and Destiny, saw a 99% correlation rate during the 2019 launch of ShadowKeep.

DATASHEET

BigPanda

BigPanda's Incident 360 Console creates and names incidents based on likely root cause, shows all of the active alerts that have been correlated into the incident, and highlights enrichment data that provides relevant context for each alert.



9 app: fleetman-690 · env: production — Changed: < 1m ago
2 min | Prometheus, Datadog, Nagios, AppDyna... — 3

11 app: claimsprocessing-9928 · env: prod — 2m ago
2 min | Nagios and AppDynam... | items: ngnix-82.dfw.prd.acme.com... — 3

● Status: critical — Created: Today, 4:07pm

```
last event:          Today, 4:07pm
source:              Splunk
target:              webapp-045.north-1a.prd.elev8ops.com
search:              Web timeouts
description:         Web timeouts for application fleetman
app:                 fleetman-690
app_url:             http://fleetman.elev8ops.com/
env:                 production
session:             dailydemo
short_descript…      Web timeouts for application fleetman-690
tier:                t1-app
maintenance:         False
```

3 host: prod-checkout-44 — Sep 16
3 min | Nagios | checks: Disk Space, CPU utilization, Memory Usage

Critical app: fleetman-690 · env: production
Cr… 2m ago | Time Win… 2 min | Source: Prometheus, Datadog, Nagios, AppDynami…

☑ Active (9) □ Maintenance (0) ☑ Resolved (0)

□	●		source	description	Dur.	Change
□	●		Splunk	Web timeouts for application fleetman	< 1m	4:07 pm
□	●		AppDynamics	mongo-690 is reporting slowness in database transaction…	< 1m	4:07 pm
□	●		Datadog	WSWS3228E: Error: Exception: java.io.IOException: Conne…	< 1m	4:07 pm
□	●		Nagios	Storage failure repair failed	< 1m	4:07 pm
□	●		Nagios	Storage failure disk repair on /dev/xvda	1m	4:07 pm
□	●		Datadog	i/o latency reported on /dev/xvda	2m	4:07 pm
□	●		Prometheus	Pod pod/position-tracker-5ff4fb1611-bqrcd is restarting…	1m	4:06 pm
□	●		Prometheus	PersistentVolumeClaim of pod/mongodb-5ff4fb1611-bqrcd w…	2m	4:06 pm
□	●		Prometheus	33% throttling of CPU in namespace default for containe…	3m	4:05 pm

Key Capabilities

Aggregation

BigPanda connects to all your monitoring, change and topology tools and aggregates their data in real-time. To date, BigPanda has integrated over 300 unique tools. On top of this, BigPanda's SNMP agent lets you collect alerts from tens of thousands of IT systems and devices.

Normalization

BigPanda translates diverse IT datasets (such as alerts, changes and topology) into one consistent taxonomy, represented using general-purpose key-value pairs called tags. BigPanda performs this in real-time using multiple out-of-the-box and custom normalization methods.

Enrichment

BigPanda's Event Enrichment Engine uses out-of-the-box integrations and a REST API to collect contextual data from operational and topology data sources, including CMDBs, APM tools and network maps. Users can easily customize and deploy cross-domain enrichment of monitoring alerts, making correlation and noise suppression highly effective.

Noise reduction

BigPanda uses Open Box Machine Learning to correlate alerts, changes and topology data together, and reduces IT noise by over 95%. This makes it possible to detect evolving incidents as they happen, before they escalate. Users can see the OBML logic in plain English, edit it and incorporate their tribal knowledge, and test and preview results before deploying the logic into production.

Impact analysis

BigPanda's Incident 360 Console provides cross-stack views that filter incidents by severity, and displays business context such as affected services and potential customer impact for each incident. The Real-time Topology Mesh shows dependencies between apps/services and low-level infrastructure, so users can determine how best to prioritize their responses to incidents.

Analytics

BigPanda's Unified Analytics is based on a robust, fully customizable and scalable reporting and visualization back-end that can handle IT Operations data at any scale. It includes a library of dashboards that can track commonly-used IT Operations key performance indicators, metrics and trends in accordance with industry best practices. It also supports data export to all widely-used BI (business intelligence) and DW (data warehouse) platforms.

If you have an opportunity you want to partner on, reach out to info@bigpanda.io or call (650) 562-6555.

BigPanda