BigPanda

Solution brief

BigPanda AI Detection and Response

Take control of incidents before they escalate with autonomous detection, triage, and response.

Benefits

Proactive incident detection

Correlate alerts from internal and external observability, CMDB, and service desk sources to help automate early L1 detection of potential incidents.

Precise incident triage

Automatically unify relevant context and knowledge into an AI-generated summary with clear diagnosis, categorization, and priority, improving your L1 team confidence and accelerating accurate resolution.

More automation, less escalation

Empower L1 teams to resolve incidents with suggested and automated remediation. When escalation is required, automatically assign and equip L2 teams with complete incident context.

Clearly-defined ownership

Establish clear ownership and impact to help in-house operations and outsourced MSPs quickly identify the right contacts.

Reactive, human-driven IT operations (ITOps) workflows—where siloed teams manually detect, triage, and respond to incidents generated by monitoring and observability tools and end-user complaints—can cost enterprises over US$200 billion annually through in-house operations and outsourced managed service providers (MSPs).

Despite significantly investing in observability tools, many organizations still struggle with inadequate detection, often learning of incidents from customers.

Even after detecting incidents, a lack of operational context frequently delays resolution, leading to L1 team bottlenecks during triage, misguided responses, and needless escalations.

Poor detection and visibility

Most L1 teams must manually sift through massive volumes of fragmented, incomplete, noisy data from observability, change, topology, and CMDB tools during incident triage. Without centralized visibility and data-driven insights, they lack the unified context and institutional knowledge they need to find relevant information. This blind spot makes it extremely challenging to identify the impacted service or application and make informed decisions, negatively impacting incident resolution times and accuracy.

Documentation gaps

Outdated, incomplete, or missing runbooks, knowledge base articles, and incident documentation create critical knowledge gaps during response. These gaps lead to manual, error-prone processes where L1 teams are unable to find the right historical context on how similar incidents were previously handled. Without reliable guidance or tribal knowledge, they struggle to take confident action, which hinders first-contact resolution and increases escalations, often to the wrong L2 specialists.

MSP blind spots

Enterprises often rely on MSPs to scale network and service desk operations. However, MSPs frequently have limited access to and integration with their clients' broader observability stack, creating coverage blind spots. In addition, poor communication about infrastructure changes, outdated standard operating procedures, and high turnover lead to inconsistent, delayed, and error-prone alert responses.

How BigPanda can help

The BigPanda agentic ITOps platform enables enterprises to keep their digital world running by transforming manual, reactive, human-driven processes into automated, proactive, AI-driven IT operations that quickly detect, triage, and respond to incidents.

BigPanda AI Detection and Response empowers your L1 teams to identify incidents early, before they impact your business. To accelerate triage and resolution, it automatically detects potential incidents by orchestrating AI agents that gather and analyze relevant real-time data from your monitoring and observability tools, external observability sources, CMDB apps, historical incidents, and service desk tickets. It uses AI to correlate multiple data points, determine whether issues are connected to a broader incident, reduce alert noise, and differentiate true signals from false positives, allowing your teams to proactively prioritize and respond.

Get started with BigPanda AI Detection and Response.

Request a demo

AI Detection and Response instantly unifies this critical context into an AI-powered incident summary, providing L1 teams with a complete and accurate view of the issue.

An agent enriches the incident with:

- **Incident correlation** to connect simultaneous, related events and uncover the complete scope across your services and applications
- **Service desk correlation** to surface end-user impact
- **Historical incident analysis** to reveal your past remediation steps and tribal knowledge
- **Change correlation** to identify any recent changes as the likely root cause
- **External observability** to provide context about third-party failures

This agentic triage process provides clear suggested actions, categorization, and prioritization, eliminating the need for manual investigation. Your L1 teams gain the confidence to resolve a higher percentage of issues, improving first-contact resolution. For necessary escalations, your L2/L3 teams receive a fully enriched ticket, making downstream response immediate and efficient.

	Detection	Triage	Response
Challenge	Visibility gaps delay incident detection, often resulting in customers reporting issues to the service desk.	IT blind spots lead to slow, error-prone triage, missed SLAs, and teams incorrectly categorizing, prioritizing, and assigning incidents.	A lack of documentation and historical insights creates gaps in resolution paths, delaying L1 response and leading to frequent L2 escalations.
Solution and business value	Identify early indicators of potential incidents, regardless of where they originated, and uncover whether individual issues are part of a broader problem.	AI agents automatically gather and summarize relevant context to quickly validate the category, priority, and root cause.	Confidently drive more first-contact resolutions with AI-powered actions tailored to the context of each incident—even as that context evolves.

WEC Energy Group

"BigPanda has enabled us to get more real-time, relevant data about a specific incident. This has significantly reduced our mean time to resolution (MTTR)."

Steve Liegl,
Director of Infrastructure and Operations
WEC Energy Group

Bloor

"Adding context to enrich alert data leads to more effective prioritization and results in faster problem resolution and fewer service disruptions."

Paul Bevan,
Research Director, IT Infrastructure
Bloor Research