# Use Generative AI to automate incident analysis and resolve incidents faster than ever

Generative AI for Automated Incident Analysis provides ITOps teams with fast, accurate, and consistent insights into every incident, making it possible to identify the impact and probable root cause across distributed IT systems faster and easier than previously possible.

## Respond faster and resolve quickly

Generative AI from BigPanda automatically extracts meaningful insights from complex IT alerts and incidents in real-time. Incident titles, descriptions, and even probable root causes can be identified within seconds, enabling operations teams to immediately review and verify auto-generated responses, quickly understand causality and impact, and dramatically shorten time-to-resolution.

## Know more, confidentially

BigPanda uniquely ingests multiple sources of enrichment and alert data to rapidly and reliably identify why an incident was created, what changed, and how systems are related so a suggestion on where to fix the issue can be made. Because datasets in BigPanda are tightly curated and pre-processed, they are less expensive to analyze, and even lower-priority incidents can be comprehensively analyzed and presented for resolution.

## Consistent, reliable communications

Every incident receives deep AI-generated analysis that translates complex technical issues into easy-to-understand terms. This translates to consistent, reliable, and explainable insights across all incidents, including the reasoning behind each AI-powered inference, making it easier for response teams to understand the implications and resolution paths regardless of tenure or expertise.

## Key Capabilities

- **AI-generated summary and title:** Identify incidents that require more immediate action by automatically synthesizing complex alert data into clear, crisp incident summaries and titles that can be populated within chat and ITSM tools.
- **AI-proposed incident impact:** Reliably identify the relevancy and impact of incidents across distributed IT systems in clear, natural language within seconds. Easily identify priority actions for ITOps, L2, and L3 response teams across all incidents at scale.
- **AI-suggested root cause:** Automatically surface critical insights and details hidden in lengthy and complex alerts to quickly identify the probable root cause of an incident, as it forms in real-time.
- **Cross-domain enrichment:** BigPanda uniquely ingests multiple sources of enrichment and topology sources to provide Generative AI systems with operational awareness and context to reliably identify where a problem started, what changed, and how systems are related.

## Key Benefits

- **Know what's happening in real-time**
  Quickly deliver rapid, accurate and high-value analysis in natural language. BigPanda exposes important details and automatically generates and populates titles and descriptions of the incident with ITSM and chat tools.
- **Confidently identify impact across IT systems**
  Instantly identify and understand in natural, easy-to-understand language the relevancy and impact of incidents across distributed IT systems. BigPanda Generative AI users report saving up to 10 minutes per incident and a significantly reduced number of incident escalations as a result of AI-generated impact estimates.
- **Automatically reveal root cause**
  BigPanda understands how distributed systems are interrelated and their purpose, giving Generative AI the context needed to reliably identify and explain the probable root cause of an active incident.
- **Transparent reasoning**
  Generative AI from BigPanda provides the reasoning behind AI-powered inferences so your team can better understand how answers are derived, improving the speed of resulting investigations.

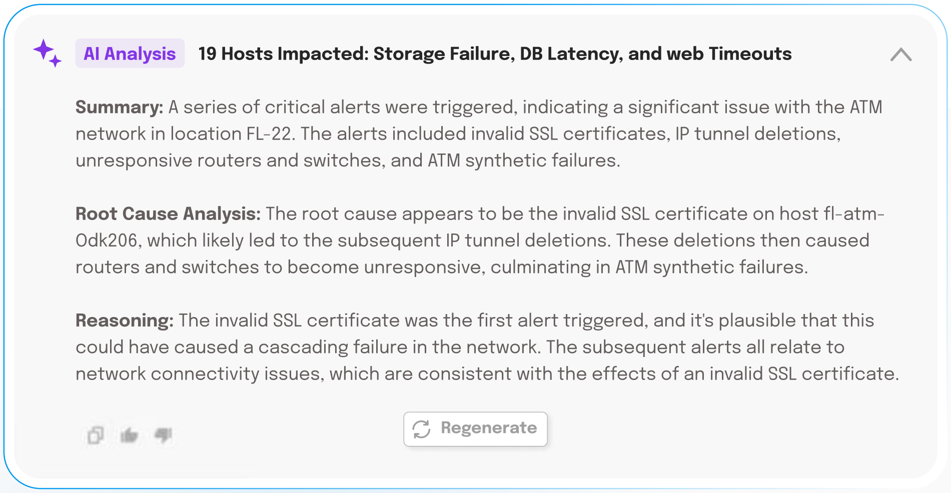
**Get started with BigPanda**

www.bigpanda.io

| | AI-generated summary and title | AI-suggested root cause | AI-proposed incident impact |
|---|---|---|---|
| **Challenge** | Summarizing and analyzing incidents quickly, accurately and consistently to response teams relies on operator tenure and expertise. | Critical insights and details hidden in lengthy and complex alerts go missing. | ITOps needs to consider the type of issue, the impact on the technology stack, and what level of detail to communicate with response teams, which is very hard to do at scale. |
| **Outcomes with BigPanda's Generative AI** | Faster mean-time-to-know | Faster mean-time-to-resolve | Fewer escalations and ITSM tickets |
| **Benefits** | Save up to 10 minutes per incident by automatically sharing easy-to-understand titles and summaries with distributed teams using ITSM or chat tools. | Pinpoint the responsible cause for an outage by automatically identifying changes to distributed infrastructure and applications that are very hard to isolate amongst complex alerts. | First responders quickly understand the context around an incident in natural language, allowing them to quickly resolve low-level incidents themselves. |

> “Generative AI can be an extraordinarily powerful way to save ITOps time and effort. But Generative AI works best when it's given good data such as alert information enriched with other data types to help AI develop accurate conclusions”
>
> – Jon Brown, Senior Analyst, Enterprise Strategy Group

> "BigPanda Generative AI empowers our Ops teams by providing faster incident detection and independent resolution. The rapid, automated extraction of meaningful insights from our complex IT alert environment not only makes us better at L1 response, but also reduces escalations to our L2 and L3 experts."
>
> – Jeremy Talley, Lead Operations Engineer, Robert Half International



AI Analysis **19 Hosts Impacted: Storage Failure, DB Latency, and web Timeouts**

**Summary:** A series of critical alerts were triggered, indicating a significant issue with the ATM network in location FL-22. The alerts included invalid SSL certificates, IP tunnel deletions, unresponsive routers and switches, and ATM synthetic failures.

**Root Cause Analysis:** The root cause appears to be the invalid SSL certificate on host fl-atm-Odk206, which likely led to the subsequent IP tunnel deletions. These deletions then caused routers and switches to become unresponsive, culminating in ATM synthetic failures.

**Reasoning:** The invalid SSL certificate was the first alert triggered, and it's plausible that this could have caused a cascading failure in the network. The subsequent alerts all relate to network connectivity issues, which are consistent with the effects of an invalid SSL certificate.