BigPanda

Turbocharge your AIOps maturity

How leading companies go from reactive to proactive incident management

Stages of AIOps maturity

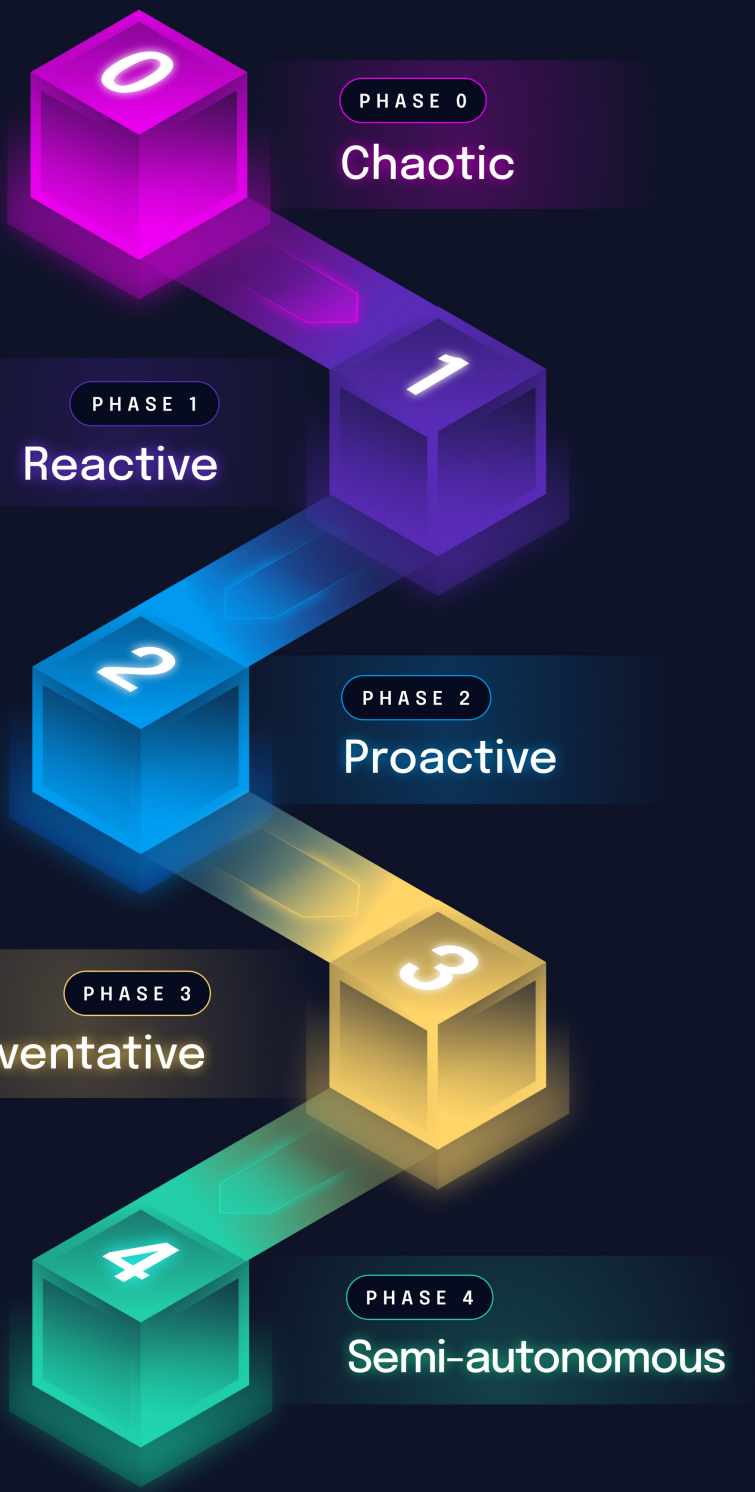


Table of contents

The average cost of an outage is $12,900 per minute.

Enterprise Management Associates. (2022). The Modern IT Outage: Costs, Causes, and "Cures."

It's 10:45 pm, and you're just about to go to bed. Suddenly, your phone vibrates, and a distinct ring tone signals another major incident concerning a critical billing application. As the Incident Commander, you swiftly prepare for the war room, joining the bridge call to assess your fourth major incident in two months. Compounding the stress of these major incidents and outages are the escalating costs. On average, a critical outage costs $12,900 per minute, but for larger companies, it can be as much as $25,402 per minute.[1] You know there must be a more efficient, less stressful approach to maintaining operational stability and delivering better critical system reliability.

The solution lies in embracing AIOps (Artificial Intelligence for IT Operations). AIOps allows organizations to automatically identify important and actionable alerts from your observability data, proactively prevent incidents, and automate incident response steps to resolve incidents before outages occur – so you can finally sleep soundly.

This guide draws on our extensive experience helping hundreds of ITOps teams embark on this transformative AIOps journey. This guide will identify critical milestones, challenges, and benefits for each stage of your AIOps deployment. With this, you'll understand the value of leveling up AIOps for your operations, discover how to transition from reactive to proactive incident management, and ultimately keep your ITOps and DevOps teams happy too.

High-performing organizations leverage AIOps platforms to achieve peak performance in three main areas:

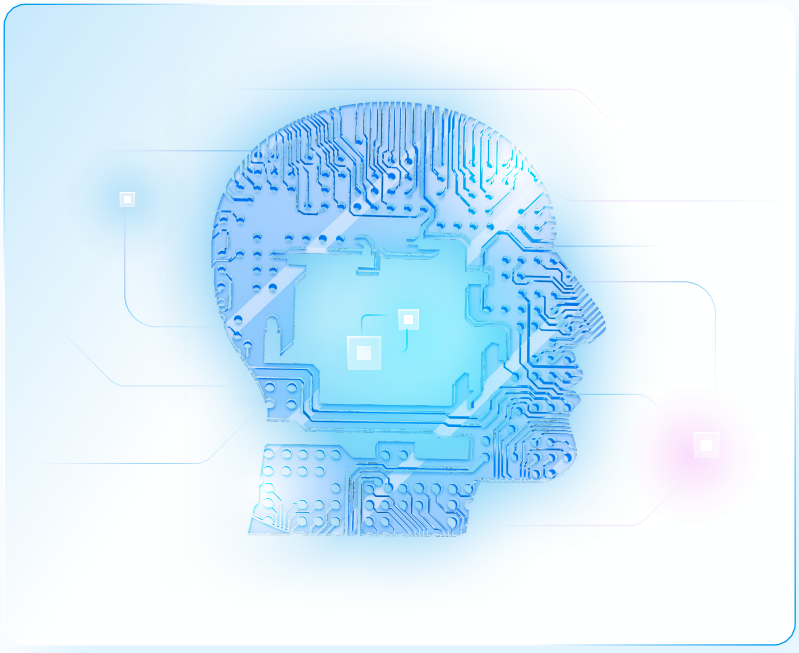
1. To gain operational awareness of disconnected IT systems
2. To detect user-impacting and performance incidents early on
3. To automate incident response steps to reduce escalations and interruptions

[1] Enterprise Management Associates. (2022). The Modern IT Outage: Costs, Causes, and "Cures."

Diagnose your AIOps maturity level to discover your action plan

At BigPanda, we've helped hundreds of clients improve their AIOps maturity to reduce IT alert noise by more than 95%, utilize advanced AI/ML to detect issues before incidents occur, and automate incident response workflows to ensure the highest service availability.

Now we want to share what we've learned from our customers to help you evaluate your AIOps performance and assess the effectiveness of your current AIOps solution. Use this guide to identify your gaps and uncover the metrics that matter to accelerate your AIOps operational excellence.



PART 01

Quiz to diagnose your AIOps maturity phase

Elevating your AIOps maturity from a reactive to a proactive ITOps practice involves a journey across five critical phases of AIOps maturity. These phases progress from the least mature Chaotic, where users report frequent incidents and long outages, to the most advanced Semi-Autonomous Operations, where companies rarely experience any outages with their ability to gain comprehensive visibility into the health of distributed tech stacks and auto-remediate incident triage before problems escalate.

What phase is your organization currently in? In the quiz below, just check any boxes that apply to your organization. Your AIOps Maturity phase is determined by the phase with the most checked boxes.

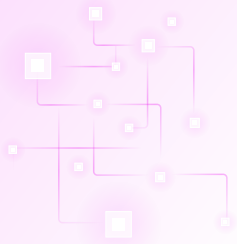
Once you've figured out your phase, move forward in this guide to Part 2: Speed Towards AIOps Maturity to learn the actionable steps you can take to level up your AIOps.

PART 01

Quiz to diagnose your AIOps maturity phase

PHASE 0

Chaotic



During the Chaotic phase of AIOps maturity, organizations typically lack a centralized Network Operations Center (NOC) or approach to aggregate and correlate event and alert data into a single pane of glass. Frequent incidents occur as a backlog of distributed IT alerts spread across different L2 and L3 response teams, overwhelming their capacity to understand what is critical and pinpoint the source of the incident. Disconnected systems and processes between teams exacerbate the pain of identifying critical incidents, resulting in disruptions and inefficiencies. Your organization may be in this phase if you have the following characteristics:

- Frequent incidents occurring multiple times daily [2]
- Most incidents and outages reported by users or customers
- Monitoring silos and ad-hoc incident handling process
- Frequent customer outages, long bridge calls
- Disorganized teams with coverage gaps and lack of visibility
- Incident triage requires domain experts at each instance
- Monitoring alerts are ignored

"Don't wait to start your AIOps journey once you are overwhelmed with alerts. Start early to get a single pane of glass to understand which monitoring tools you really need."

– Sanjay Chandra, Vice President of Information Technology, Lucid Motors

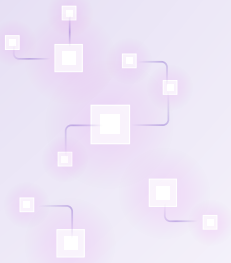
[2] Enterprise Management Associates. (2022). The Modern IT Outage: Costs, Causes, and "Cures."

PART 01

Quiz to diagnose your AIOps maturity phase

PHASE 1

Reactive



Most organizations find their response teams in this phase, reacting to incidents. While organizations may now have a centralized operations team to aggregate and correlate alerts, they continue to suffer from overwhelming alert noise and an inability to identify actionable or high-priority alerts that can prevent incidents from escalating. Manual incident response and escalation processes don't reduce the backlog of persistent IT incidents, resulting in customer complaints and costly outages. If your organization frequently experiences the following, you may be in the Reactive Phase:

- Significant incidents occurring every week [3]
- 25% of incidents are identified from alerts, 75% from users [4]
- Frequent escalations require domain experts
- Increasing noise from non-actionable alerts
- Operations teams are overworked
- Reliance on manual processes
- High-priority alerts missed or delayed

[3] BigPanda. (2022). A Practical Guide to IT Ops Maturity.
[4] BigPanda. (2022). A Practical Guide to IT Ops Maturity.

PART 01

Quiz to diagnose your AIOps maturity phase

PHASE 2

Proactive

In this phase, organizations leverage AIOps to aggregate and correlate cross-domain alerts and reduce alert noise from monitoring and observability platforms. However, teams must improve in identifying what is actionable and important to further reduce alert noise. Once this is achieved, operations teams can get ahead of customer issues. You may be at Phase 2 if you experience the following:

- Significant incidents occurring every other month [5]
- 50% of incidents identified from alerts, 50% from users [6]
- Support teams can handle alert volume
- Reduction in major outages, some minor issues
- All alerts captured or actioned
- Operations aware of issues before customers
- Defined support process but inconsistent escalation

"For us, an alert is not actionable unless it comes into BigPanda, is enriched, and is potentially correlated with the other alerts in the system."

– Jon Moss, Head of Edge Software Engineering at Zayo

[5] BigPanda. (2022). A Practical Guide to IT Ops Maturity.
[6] BigPanda. (2022). A Practical Guide to IT Ops Maturity.

PART 01

Quiz to diagnose your AIOps maturity phase

PHASE 3

Preventative

Organizations using AIOps in the Preventative Phase proactively address problems, which frees up time and resources for essential projects. Some of these organizations leverage AI/ML to operate semi-predictively, semi-autonomously. In contrast, others rely on sizable teams to minimize disruptions and ensure a smoother operational environment. Do these characteristics sound like your company's experience?

- Significant incidents occurring quarterly [7]
- 95% of incidents are identified from alerts, and 5% user reported [8]
- Workflows are automated, and alert volumes are decreasing
- First line resolves the majority of issues, major issues are rare
- Resources can be reallocated for less firefighting, more innovation
- Centralized data, automation, and reporting

"We've automated an average of 83% of alerts that come into BigPanda; now, the bulk of our alerts get resolved automatically or receive a ticket without our team having to manually investigate it."

– Mark Peterson, IT Operations Supervisor at Cambia Health Solutions

[7] BigPanda. (2022). A Practical Guide to IT Ops Maturity.
[8] BigPanda. (2022). A Practical Guide to IT Ops Maturity.

PART 01

Quiz to diagnose your AIOps maturity phase

PHASE 4

Semi-autonomous

The Semi-autonomous AIOps phase represents the ideal state of AIOps excellence. In this phase, customer-impacting incidents are minimal. Incidents rarely escalate and can even be resolved using zero-touch automation with third-party auto-remediation platforms.

Some may wonder if fully autonomous IT operations could be possible. However, even with the most sophisticated AIOps tech, there must also be skilled human operators to solve problems and supervise automated decision making.

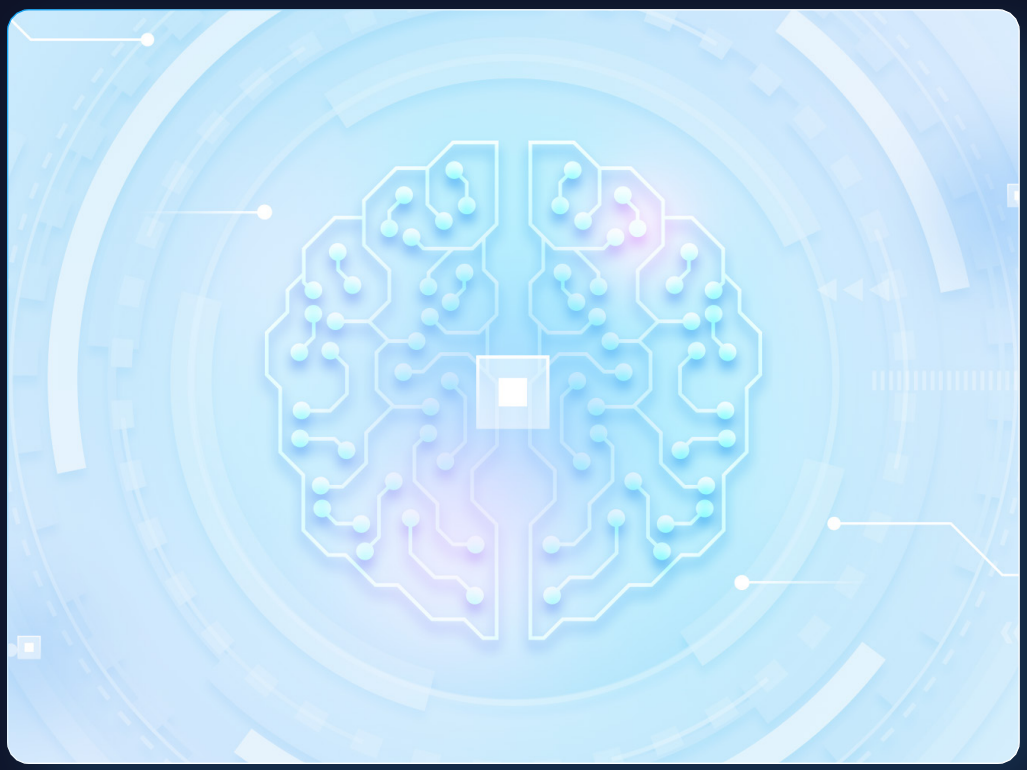
Read on to see if you are one of the few companies to achieve Semi-autonomous AIOps:

- Significant incidents occur once or twice a year [9]
- 99% of incidents are identified from alerts, 1% from users [10]
- Team bandwidth is fully reclaimed
- Incident processes and reporting are fully optimized
- Incidents have rich payload data that includes both technical and business metadata
- Auto-remediation implemented within the organization

[9] BigPanda. (2022). A Practical Guide to IT Ops Maturity.
[10] BigPanda. (2022). A Practical Guide to IT Ops Maturity.

PART 02

Speed towards AIOps maturity



Now that you've gauged your current maturity level, let's take your AIOps to the next level. To get there, we must identify the elements in the lowest phase and prioritize bringing them up to speed with the rest of your AIOps processes. We'll guide you through the steps below, so you can rapidly achieve improved AIOps milestones.

PART 02

Speed towards AIOps maturity

PHASE 0 >>> 1

Reduce alert noise and identify actionable alerts

Overwhelming IT alert noise can make detecting and resolving critical problems extremely difficult. For success, it's essential to have a single platform that can serve as the foundation for response teams to build visibility and insight into the health of your services and applications across your distributed technology stack. Begin by reducing alert noise and establishing a baseline of incident management metrics by taking the following steps:

- Integrate monitoring and observability into a single console
- Normalize, deduplicate, and filter out noisy, benign events to reduce alert volume
- Assess the impact of alerts by normalizing and enriching them with context (like location, host, or affected service) to increase their quality
- Create basic incident environments aligned with team responsibilities and business priorities
- Baseline your MTTX metrics through Unified Analytics

PHASE 0

AIOps will reduce workload even if your NOC or ITSM is developing

Even if you don't have a fully functional NOC or ITSM system, you can use AIOps at Phase 0 to reduce the workload of your current teams and help give them time to build cross-functional processes. Learn more on our AIOps 101 Series and tips for running a successful NOC.

PART 02

Speed towards AIOps maturity

PHASE 1 >>> 2

Identify actionable and important alerts to improve MTTR

In this phase, organizations build the foundations for automating incident management workflows by breaking down the silos between teams and tools by grouping related alerts into a single incident. AIOps can effectively and accurately correlate alerts to dramatically reduce your monitoring noise by as much as 90 – 99% for some environments. Correlations occur in under 100ms, giving updates in real-time for maximum visibility into critical problems.

Here are the actions you can take to identify high-quality, actionable alerts so your response teams can quickly respond to incidents.

- Create cross-domain correlation patterns based on known patterns that match seemingly disconnected alerts into one incident
- Improve alert correlation impact using data-driven insights on the effectiveness of patterns deployed
- Apply concrete rules to check for defined attributes contributing to actionability
- Know what's happening in real-time in natural language using AI
- Connect outbound systems for automatic paging, notification, and ticket creation
- Measure and improve your mean times to detect, classify, diagnose, remediate and close/resolve using dashboards and analytics

PHASE 1

AIOps improves MTTR without developed monitoring and observability

Even if your monitoring strategy is not fully developed, or your observability is a mess, AIOps is specifically engineered to help you quickly organize and clean your monitoring data so you can reduce toil and take action. The BigPanda AIOps Starter Packs are designed to deliver quick time to value through an accelerated onboarding that connects with your highest priority monitoring and chat systems.

PART 02

Speed towards AIOps maturity

PHASE 2 >>> 3

Increase team productivity by optimizing operational workloads

Alerts from monitoring and observability tools contain plenty of low-level technical information but no operational, contextual, or topological information. Without this vital metadata, response teams don't understand the impact of incidents on downstream dependencies or which incidents need to be prioritized. That's where AIOps comes in, by improving teams' workloads with insights into how complex IT assets are interrelated and by revealing customer-impacting incidents.

- Ingest topological data and enrich alerts with meaningful context
- Improved correlation through topological relationships
- Automate incident prioritization
- Confidently identify impact across IT systems using Generative AI
- Establish basic incident workflows
- Identify recurring issues and hotspots through analytics

PHASE 2

AIOps enriches for accurate and reliable analysis

Deploying AIOps is critical to filling information gaps, standardizing workflows between distributed DevOps teams, and ensuring downstream dependencies and impacts are clearly identified. It's also essential to feed AI systems with the necessary data to make correct and reliable analyses of complex IT data. Read the whitepaper on 'Cutting Through Alert Noise With High-Quality Alerts' to learn how to get started.

PART 02

Speed towards AIOps maturity

PHASE 3 >>> 4

Reduce minor issues that impact customer satisfaction

Your customers expect your services to always work, so you'll need to optimize your service availability to keep them happy. Automating mundane tasks to help reduce minor service issues impacting customer health is critical to customer success. Improving this KPI indicates enhanced AIOps capabilities, including faster incident detection, diagnosis, and resolution. Here are the actions you can take to improve:

- Aim for 99%+ service availability [11]
- Conduct impact analysis via dependency maps
- Automate incident workflows bi-directionally with ITSM, chat, and paging tools
- Identify root cause through change correlation
- Identify auto-remediation candidates through analytics
- Further reduce noise through event filtering
- Automate incident prioritization

PHASE 3

AIOps solves complexity for less firefighting, more innovation

Many successful IT organizations learn to manage the complexity of hybrid IT with standards, processes, AI, and automation. Need help figuring out where to get started? Discover the specific steps BigPanda customer Intercontinental Hotel Group (IHG) took to achieve 99.8% service availability.

[11] BigPanda. (2022). A Practical Guide to IT Ops Maturity.

PART 02

Speed towards AIOps maturity

PHASE 4 AND BEYOND

Few incidents and even fewer tickets

In Phases 1-3 organizations can confidently use context-based automation. However, in Phase 4, semi-autonomous automation workflows enable teams to identify and respond to incidents before they become customer-impacting. L2 and L3 response teams are rarely paged to respond to incidents; ticket creation is greatly reduced. Here is how you can get there:

- Ingest all relevant data streams to gain comprehensive insight into distributed app/service health
- Leverage analytics to identify hot spots, recurring issues, and remediate at the source
- Build knowledge base articles to reduce escalations
- Trigger auto-remediation for zero-touch resolutions
- Automate escalation paths
- Automate post-mortems

PHASE 4

AIOps means fewer incidents and tickets

AIOps delivers data-driven insights and analytics to identify hot spots and recurring issues to remediate at the source. At this phase, AIOps also measures and improves on KPIs to streamline and optimize incident management workflows. Organizations can use out-of-the-box dashboards or even create visualizations to explore interrelated data to understand where standardization efforts drive business impact. Learn more about Unified Analytics or contact us to see a demo.

Speed towards AIOps maturity with BigPanda

Your AIOps maturity is a never-ending journey, where even minor adjustments can lead to remarkable destinations. And you don't need to have a NOC, a new monitoring strategy, or wait for perfect observability – you only need to begin your journey now.

Sometimes, it only takes a few critical AIOps enhancements to make a significant impact. Consider how gaming company Bungie compressed alerts by 99% with BigPanda Alert Intelligence or the communications infrastructure platform Zayo unified their technology stack with BigPanda to filter out 99.9% of events.

The BigPanda platform is critical for organizations across industries and enterprises of all sizes–small, medium, and Fortune 500 companies – to power their digital services. Optimizing your IT Operations will always be a journey, but partnering with BigPanda as your AIOps partner will dramatically improve your operational excellence.

> *"BigPanda's platform returned significant value within weeks and helps us take a significant step towards our strategic objective of establishing intelligent automation."*
>
> – Jenny Kim, Global NOC Manager, Riot Games

Stages of AIOps maturity

How to move to the next stage

PHASE 0 Chaotic

- Frequent incidents occurring multiple times daily
- Most incidents and outages reported by users or customers
- Monitoring silos and ad-hoc incident handling process
- Frequent customer outages, long bridge calls
- Disorganized teams with coverage gaps and lack of visibility
- Incident triage requires domain experts each at instance
- Monitoring alerts are ignored

- Integrate monitoring and observability into a single console
- Normalize, deduplicate, and filter out noisy, benign events to reduce alert volume
- Assess the impact of alerts by normalizing and enriching them with context (like location, host, or affected service) to increase their quality
- Create basic incident environments aligned with team responsibilities and business priorities
- Baseline your MTTX metrics through Unified Analytics

PHASE 1 Reactive

- Significant incidents occurring every week
- 25% of incidents are identified from alerts, 75% from users
- Frequent escalations require domain experts
- Increasing noise from non-actionable alerts
- Operations teams are overworked
- Reliance on manual processes
- High-priority alerts missed or delayed

- Create cross-domain correlation patterns based on known patterns that match seemingly disconnected alerts into one incident
- Improve alert correlation impact using data-driven insights on the effectiveness of patterns deployed
- Apply concrete rules to check for defined attributes contributing to actionability
- Know what's happening in real-time in natural language using AI
- Connect outbound systems for automatic paging, notification, and ticket creation
- Measure and improve your mean times to detect, classify, diagnose, remediate and close/resolve using dashboards and analytics

PHASE 2 Proactive

- Significant incidents occurring every other month
- 50% of incidents identified from alerts, 50% from users
- Support teams can handle alert volume
- Reduction in major outages, some minor issues
- All alerts captured or actioned
- Operations aware of issues before customers
- Defined support process but inconsistent escalation

- Ingest topological data and enrich alerts with meaningful context
- Improved correlation through topological relationships
- Automate incident prioritization
- Confidently identify impact across IT systems using Generative AI
- Establish basic incident workflows
- Identify recurring issues and hotspots through analytics

PHASE 3 Preventative

- Significant incidents occurring quarterly
- 95% of incidents are identified from alerts, and 5% user reported
- Workflows are automated, and alert volumes are decreasing
- First line resolves the majority of issues, major issues are rare
- Resources can be reallocated for less firefighting, and more innovation
- Centralized data, automation, and reporting

- Aim for 99%+ service availability
- Conduct impact analysis via dependency maps
- Automate incident workflows bi-directionally with ITSM, chat, and paging tools
- Identify root cause through change correlation
- Identify auto-remediation candidates through analytics
- Further reduce noise through event filtering
- Automate incident prioritization

PHASE 4 Semi-autonomous

- Significant incidents occur once or twice a year
- 99% of incidents are identified from alerts, 1% from users
- Team bandwidth is fully reclaimed
- Incident processes and reporting are fully optimized
- Incidents have rich payload data that includes both technical and business metadata
- Auto-remediation implemented within the organization

- Ingest all relevant data streams to gain comprehensive visibility and insight into the health of distributed applications and services
- Leverage analytics to identify hot spots and recurring issues and remediate them at the source
- Build knowledge base articles to reduce escalations
- Trigger auto-remediation for zero-touch resolutions
- Automate escalation paths
- Automate post-mortems

BigPanda

www.bigpanda.io