ANALYST BRIEF

Sponsored by: PagerDuty

Executives should consider the role of AI and automation to transform and modernize their incident management processes. A modern approach can solve challenges such as fragmented tools, processes, and high costs while setting the foundation for continuous improvement behaviors that impact the customer experience.

Transforming Incident Management: A Technology Executive Playbook

August 2024

Written by: Stephen Elliot, Group Vice President, I&O, Cloud Operations, and DevOps

High-Performing Customer Experiences Require Modern Incident Management Capabilities

Customer expectations for great experiences have never been higher as competition for revenue growth and competitive differentiation accelerates. Most organizations' technology architecture has become their business architecture; digital transformations have created new business models for digital products, services, and experiences. Customer loyalty, satisfaction, and revenue growth often depend on how well a customer experiences a brand or digital product. Any disruption to the delivery of products or services can become catastrophic, as customers are quick to move to competitive offerings, revenue is impacted, and trust is often harmed. Global IT disruption and outages are the new normal.

Mitigating these business risks is no longer just a CIO or CTO priority — it's risen to the attention of the CEO. To meet demanding customer expectations, technology executives should consider modernizing their digital operations to reduce the technical debt caused by legacy systems and tool sprawl, improve and automate fragmented operational processes, and accelerate cross-team collaboration. Executives can create a foundation for growth by transforming their approach to handling the incident management life cycle by identifying, solving, and preventing issues that impact customer satisfaction.

Incidents can disrupt business and operations, leading to increased costs, significant revenue loss, brand reputation damage, service-level agreement (SLA) penalties, poor product quality, and regulatory noncompliance. Traditional incident management practices often struggle to mitigate these risks effectively because teams have limited access to critical data, are reactive with low levels of automation, lack analytics, and have difficulty enabling preventative incident capabilities.

AT A GLANCE

WHAT'S IMPORTANT

- » Incident management transformation should leverage automation and analytics to empower teams to improve technology and business outcomes that create a critical foundation for delivering great customer experiences.
- » Executives should recognize that their technology architecture is their business architecture; delivering high-performing digital services and products directly depends on an organization's ability to provide effective incident management.
- » Leadership teams have an opportunity to streamline the alerting processes, automate remediation and triages, use AI-powered insights from past incidents and correlated events, and conduct post-incident reviews on a single platform.

In addition, the lack of analytic capabilities inhibits intelligent data analysis, dashboarding, and noise suppression, making it hard for teams to scale and get ahead of incidents.

The speed of business and the complexity of technology will only accelerate. Now is the time to modernize and transform incident management by considering platforms that help build operational excellence on a foundation of resilience that unlocks better business outcomes and great customer experiences.

The Business Impact of Incidents

Most businesses rely on digital services and are dependent on an array of complex cloud environments and legacy systems, which increase operating costs while attempting to mitigate business risks. Standardizing the management of operational processes for these environments, while providing flexibility for their technical context and strengths, can lead to a modern operational approach. Such an approach enables the transformation of incident management processes and capabilities by providing an end-to-end view that includes detecting incidents, mobilizing teams, mitigating situations, resolving issues, and conducting post-incident reviews. Incidents can severely damage a company's brand reputation, which can have a long-lasting impact on customer acquisition and loyalty. Negative publicity and social media backlash can tarnish a brand's image, making it challenging to regain customer trust and confidence.

Industries such as finance, healthcare, utilities, and telecommunications are required to meet regulatory and compliance requirements for data privacy, access, security, and service availability. Incidents that impact these legal requirements can result in fines and reputational damage, further compounding the financial, customer, and legal implications.

Challenges of Traditional Incident Management

Traditional incident management is characterized by manual processes and is usually not focused on business or customer outcomes. It leaves teams in a reactive mode where incidents are addressed in a fragmented, inefficient, and slow manner. This approach often leads to several challenges:

- **Lack of communication:** Fragmented tools and processes lead to limited cross-team communications when teams rely on their own limited data sets, hampering the ability to fully understand customer impact. Business stakeholders are often left in the dark without proactive notification, and customers don't have visibility to outages without contacting their providers.
- **Prolonged downtime:** Poorly managed incident management processes relying on manual steps and fragmented tools can result in longer cycles to identify and resolve incidents. Dependency on centralized teams to hunt down the right team to come in and determine the next steps to remediate the issue can become a critical bottleneck.
- **Limited budgets and resources:** Without new head count and modern tools, teams often struggle to work effectively and efficiently during an incident, impacted by poorly performing processes and legacy tools that enforce a reactive versus proactive model.
- **Missed learning opportunities:** Teams often fail to capture valuable insights and lessons learned from incidents, hindering an organization's ability to prevent similar incidents from occurring in the future.

A Modern Approach: The Benefits of Guided Remediation and Automated Incident Management

Adopting a proactive and preventative approach to incident management can mitigate the risks and provide numerous benefits, such as:

- **Context creation and toil removal:** The newest or least-skilled team members can now effectively respond as effectively as a senior engineer, freeing valuable resources to create new business outcomes.
- **Embedded intelligence:** Generative AI (GenAI)–driven status updates, chatbots for guided next steps, and AI/machine learning (ML) for AIOps will empower teams and supercharge processes to deliver optimal results.
- **Proactive communications:** Better communication builds internal trust with peer groups while improving the customer experience. Teams can use guided incident remediation, with assigned incident types, roles, and tasks for accountability and progress toward establishing a continuous improvement culture and behavior.
- **Better tracking and monitoring of services:** For service-level agreements, service-level indicators, and service-level objectives, this approach provides enhanced analysis and automation aligned with customer-impacting incidents and tighter alignment with CMDBs.
- **Reduction in downtime and revenue loss:** Leveraging machine learning and event-driven automation to correlate events, drive insight to action, and deflect work creates more capacity for teams. They can focus on the incidents that matter and eventually detect and address potential issues before they escalate into major incidents, minimizing downtime, reputational risk, and associated revenue loss.
- **Better customer experience:** Proactive incident management tightly coupled with customer service operations helps maintain service availability and quality and improves team collaboration while enhancing customer satisfaction, experience, and loyalty.
- **Regulatory compliance adherence:** Implementing proactive measures to ensure data privacy, security, and service availability can help organizations maintain regulatory compliance and avoid costly penalties.
- **Efficient resource allocation:** Incident detection enables teams to allocate resources more effectively, ensuring the right personnel and tools are available to resolve incidents promptly.
- **Continuous improvement:** By capturing and analyzing incident data and human response, organizations can identify critical incident patterns and areas for improvement, enabling them to implement preventative measures and apply continuous learning behaviors.
- **Consistent and repeatable results:** By leading with automation, incidents are no longer as good as the best people on the call. Instead, automated event-driven processes ensure predictable and standardized responses to virtually any situation.

Strategies for Applying Automation and AI Capabilities to Transform Incident Management

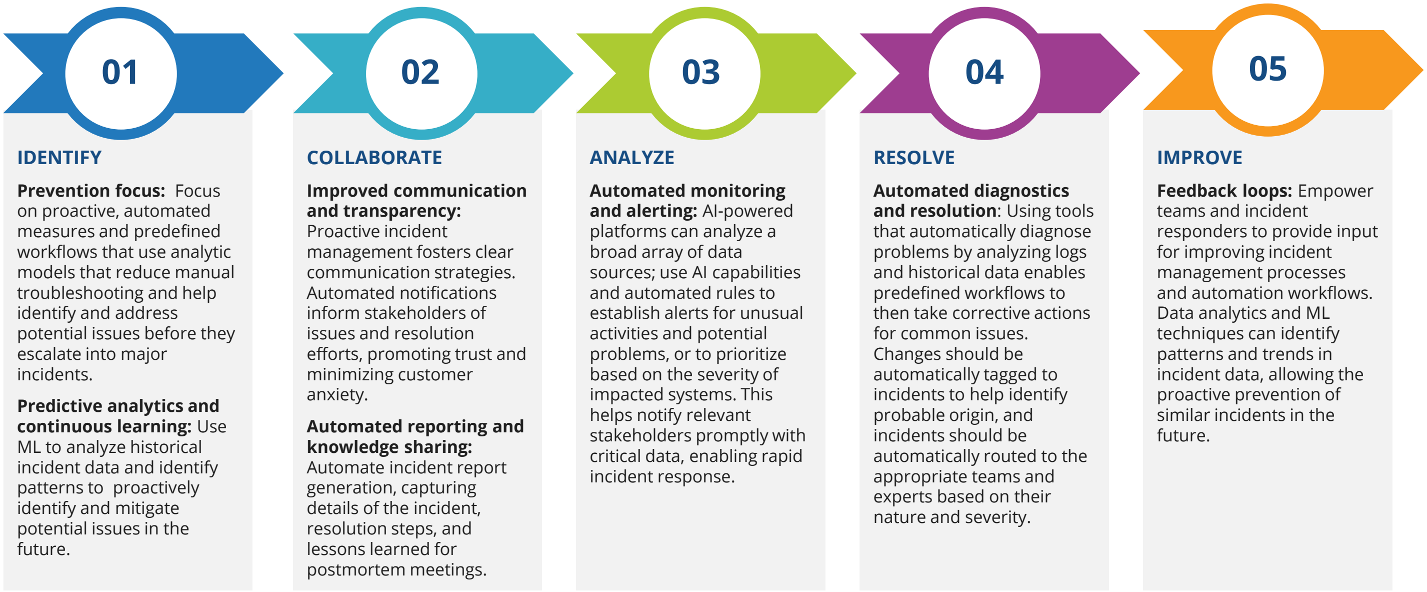
Leveraging automation with AI capabilities throughout the incident management life cycle can significantly enhance an organization's ability to detect, respond, and continuously learn from incidents effectively and efficiently. Some considerations for modernizing incident management using automation and AI capabilities are:

- **Incident detection, correlation, and alerting:** Organizations should implement best-fit comprehensive monitoring solutions that can track system performance, application health, and user experience metrics coupled with AIOps to reduce noise and toil. They should align automated alerting mechanisms that can notify teams promptly when anomalies or potential issues are detected. This will drive a productivity gain and can enable additional benefits, including faster incident resolution.
- **Incident triage and prioritization:** Utilize ML-powered capabilities and event-driven automation to correlate and enrich events with critical context to accelerate incident triage. Prioritizing incidents based on predefined criteria, such as impact severity, affected systems, and SLAs can ensure teams promptly address critical incidents.
- **Standardizing operations:** CI/CD pipelines are leveraged to define operations as code (e.g., escalation policies, orchestrations, links to runbooks, diagnostics, and remediation). These could be further refined to use quality gates for scoring the operational capability of applications or plugging into developer portals for deeper insights.
- **Incident mobilization:** Leveraging automation to mobilize the appropriate response teams and escalate incidents based on predefined workflows and communication channels can ensure efficient coordination and collaboration.
- **Automated diagnostics and troubleshooting:** Organizations should implement automated diagnostics, identifying changes and troubleshooting tools that can analyze system logs, performance data, and other relevant information to identify root causes and potential resolutions.
- **Self-healing and remediation:** Developing automated remediation scripts and workflows that can resolve common issues without human intervention can reduce the time and effort necessary for incident resolution.
- **Incident analysis and reporting:** Consider automating the collection and analysis of incident data, including root causes, resolution steps, and associated metrics. Generating comprehensive reports and dashboards can facilitate post-incident reviews and identify areas for improvement.
- **Continuous learning and feedback loop:** Implementing mechanisms to capture and disseminate lessons learned from incidents will enable teams to update knowledge bases, runbooks, and preventative measures continuously.

Best Practices for Modernizing Incident Management

Technology executives can use the following best practices shown in Figure 1 to transform their incident management process using automation and AI/ML on a single platform. These proven practices help establish a proactive foundation that leverages AI and automation across people, processes, and technologies.

FIGURE 1: ***Transformational Incident Management Best Practices Empower High-Performing Teams and Accelerate Customer-Focused Outcomes***



IDENTIFY

Prevention focus: Focus on proactive, automated measures and predefined workflows that use analytic models that reduce manual troubleshooting and help identify and address potential issues before they escalate into major incidents.

Predictive analytics and continuous learning: Use ML to analyze historical incident data and identify patterns to proactively identify and mitigate potential issues in the future.

COLLABORATE

Improved communication and transparency: Proactive incident management fosters clear communication strategies. Automated notifications inform stakeholders of issues and resolution efforts, promoting trust and minimizing customer anxiety.

Automated reporting and knowledge sharing: Automate incident report generation, capturing details of the incident, resolution steps, and lessons learned for postmortem meetings.

ANALYZE

Automated monitoring and alerting: AI-powered platforms can analyze a broad array of data sources; use AI capabilities and automated rules to establish alerts for unusual activities and potential problems, or to prioritize based on the severity of impacted systems. This helps notify relevant stakeholders promptly with critical data, enabling rapid incident response.

RESOLVE

Automated diagnostics and resolution: Using tools that automatically diagnose problems by analyzing logs and historical data enables predefined workflows to then take corrective actions for common issues. Changes should be automatically tagged to incidents to help identify probable origin, and incidents should be automatically routed to the appropriate teams and experts based on their nature and severity.

IMPROVE

Feedback loops: Empower teams and incident responders to provide input for improving incident management processes and automation workflows. Data analytics and ML techniques can identify patterns and trends in incident data, allowing the proactive prevention of similar incidents in the future.

Source: IDC, 2024

By implementing these strategies, organizations can create a robust, automated incident management system on a unified platform. This proactive approach minimizes the impact of major incidents on customers — helping safeguard the organization's revenue, brand reputation, and overall operational resilience.

Benefits

Automation and AI/ML play a pivotal role in reducing the time and cost associated with modernized incident resolution. Executives should focus on several key business themes that are discussed in the sections that follow.

Accelerated Detection and Response Time

- **Automated incident process and orchestration:** Incident management solutions that apply automation across the incident process, while applying AI for alerting, triage, and diagnostics, can identify potential issues before they manifest as major incidents. Automated alerts notify relevant personnel promptly with the right information, facilitating faster response times.

- **Automated triage and prioritization:** Automation can categorize and prioritize incidents based on predefined criteria, ensuring critical and priority incidents receive immediate attention based on customer requirements.

Faster Resolution and Less Effort

- **Automated diagnostics and troubleshooting:** Automation can analyze logs, performance data, and other relevant information to pinpoint root causes. These processes eliminate manual troubleshooting steps, thereby accelerating resolution and getting the right data to the right person at the right time.
- **Self-healing actions:** Predefined workflows can trigger automation, such as restarting services, scaling, or rerouting traffic, to resolve common issues without the need for human intervention — saving valuable time and resources.
- **Automated reporting and documentation:** Automating the generation of incident reports and updates reduces manual work and ensures consistency in documentation, enabling faster resolution and knowledge sharing.

Improved Efficiency and Cost Savings

- **Reduced mean time to resolution (MTTR):** Automating manual tasks accelerates incident diagnostics and resolution, lowering MTTR and minimizing downtime.
- **Reduced resource consumption:** Automation frees up human resources for more strategic tasks such as reducing technical debt and optimizing resource allocation and team productivity.
- **Cost optimization:** Faster resolution translates into reduced downtime, minimizing revenue loss and operational costs that service disruptions entail.

Considerations

Shifting from a reactive, costly, and static model to a modern, data- and analytics-driven incident management approach requires addressing several key challenges, including:

- **Cultural change:** Transitioning from a reactive culture to a proactive mindset requires buy-in from all levels. Continuous training and communication are crucial to fostering a culture of prevention and continuous improvement.
- **Data silos and lack of visibility:** Fragmented data sources can hinder the identification of patterns and trends that enable the implementation of proactive measures. Implementing centralized data collection and analysis is essential.
- **Resistance to automation:** Some team members may resist automation due to fear of job displacement. Addressing these concerns and emphasizing that automation empowers them through faster resolution is key. Automation should be part of a "blameless culture." Automation can cause mistakes, and mistakes can be corrected. The focus is on removing low-level tasks, not jobs.
- **Skills gap in automation:** Implementing automation tools requires personnel with technical expertise and an understanding of automation workflows. Training existing staff or attracting skilled personnel is necessary.

- **Investment and ROI justification:** The initial investment in proactive tools and processes may require a strong business case that highlights long-term cost savings and improved operational efficiency.
- **AIOps and generative AI:** Customers must believe that turning to AI/ML models can deliver cost-effective behaviors and enable trusted, repeatable outcomes at a high level of scalability with surgical precision, but companies should stay pragmatic with proven use cases for AI/ML in application. For example, ML-powered noise reduction via AIOps and AI assistants to provide summarization to surface insights are two areas to start finding value to help with streamlining the incident life cycle.
- **Lack of a standardized process and defined roles:** Implementing a proactive approach requires establishing clear processes, roles, and responsibilities for incident prevention, detection, and response. Without a standardized framework, teams may struggle with coordination and efficiency.

By addressing these challenges and focusing on the benefits of a proactive, standardized incident management platform, organizations can successfully transition from reactive firefighting to a preventative approach that safeguards their operations and customer experience.

Evaluating Incident Management Solutions

Technology leadership teams should consider the current state of their operational maturity across people and teams, technology adoption, and processes before identifying opportunities to start improving. As stated previously, fragmented tools, poorly integrated technologies, and weak team collaboration are all signs of low levels of operational maturity. Modern platform investments must be supported by automation, analytics, and a continuous improvement team perspective to increase maturity.

When evaluating incident management solutions to support proactive and preventative practices, organizations should consider the following key factors:

- **Detection and correlation:** The solution should ensure integration to robust monitoring capabilities across various systems, applications, and infrastructure components, with customizable alerting and notification mechanisms.
- **Automation, orchestration, and analytics:** Look for solutions that enable secure automation with the use of analytics throughout the incident management life cycle, from detection and triage to resolution and remediation. Some organizations include AIOps as an area of focus that supports a modern incident management approach.
- **Collaboration:** Prioritize solutions that facilitate seamless collaboration and communication among teams, with features such as real-time incident tracking, chat functionality, and integration with communication channels.
- **Reporting and post-incident analysis:** Evaluate the solution's reporting and capabilities, ensuring it can generate comprehensive incident reports, dashboards, and insights to support continuous improvement and learning. This also supports the principle of continuous improvement and team collaboration for post-incident analysis.
- **Scalability and integration:** Consider the solution's ability to scale with the organization's growth and integrate with existing tools and systems, such as monitoring tools, knowledge bases, and service desk platforms.

By implementing a proactive and preventative incident management strategy supported by automation, analytics, and the right tools, organizations can effectively safeguard their revenue and brand reputation and ensure regulatory compliance while enhancing overall operational resilience and customer satisfaction.

Conclusion

By leveraging automation, guided incident remediation, post-incident reviews, and analytics throughout the incident management life cycle, organizations can effectively minimize the business impact of major incidents — safeguarding their revenue, compliance posture, and brand reputation while reducing their overall costs of operations. An incident management platform offers a broad array of benefits and capabilities that can lead to a strong foundation for delivering consistent and high-performing customer experiences.

About the Analyst

Stephen Elliot, *Group Vice President, I&O, Cloud Operations, and DevOps*

Stephen Elliot manages multiple programs spanning IT operations, enterprise management, ITSM, agile and DevOps, application performance, virtualization, multicloud management and automation, log analytics, container management, DaaS, and software-defined compute. Mr. Elliot advises senior IT, business, and investment executives globally in the creation of strategy and operational tactics that drive the execution of digital transformation and business growth.

MESSAGE FROM THE SPONSOR

PagerDuty Operations Cloud

The PagerDuty Operations Cloud is the platform for mission-critical, time-critical operations work in the modern enterprise. Through the power of AI and automation, it detects and diagnoses disruptive events, mobilizes the right team members to respond, and streamlines infrastructure and workflows across your digital operations. The Operations Cloud is essential infrastructure for revolutionizing digital operations to compete and win as a modern digital business. Learn more at: https://www.pagerduty.com/platform/operations-cloud/.

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
blogs.idc.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.