EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Prepared for:

servicenow

Real-world incident response, management, and prevention

January 2024 EMA Research Report

By **Valerie O'Connell**, Research Director
Digital Service Execution

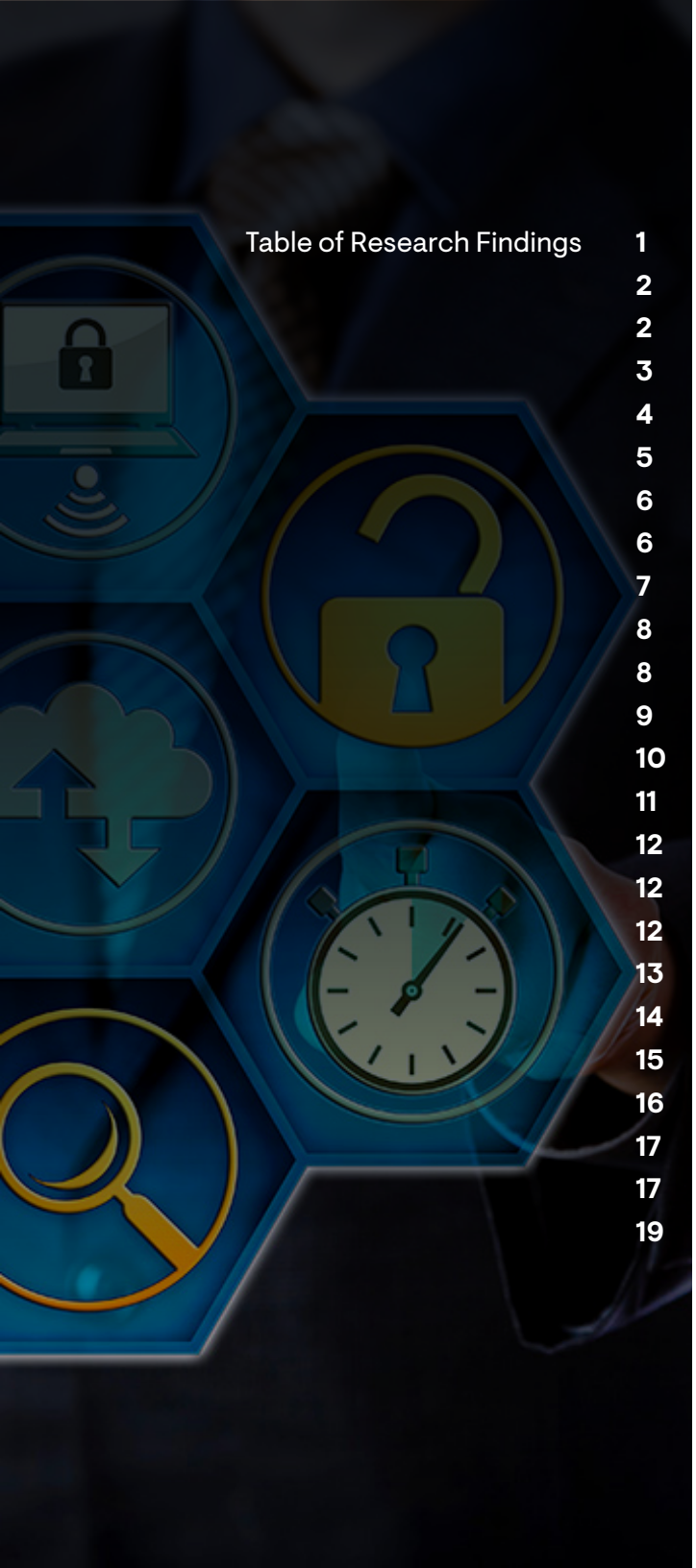


Table of Research Findings

Research overview

Winners and losers

Incidents and outages happen. However, they don't impact all organizations equally. A 2023 EMA survey[1] of 400+ global IT leaders painted a picture of winners and losers when asked about the change in outage impacts year over year.

- An unsurprising 82% of the research panel characterized incidents and outages as increasing every year. In fact, 19% stated that "increased reliance on IT guarantees continued increases."
- An intriguing 18% of that panel ran countertrend, stating that incidents and outages decreased due to proactive systems they've put in place.

Clearly, some organizations feel as if they are fighting a losing battle, while others are successfully taming the beast. To explore the differences, EMA kicked off 2024 with a research initiative focused on incident response, management, and prevention.

High-level findings

Reducing the frequency, duration, and impact of incidents and outages consistently ranks in EMA research as one of the top objectives for IT organizations of all sizes across industries globally. It is often number one. Frequently measured in reduction of MTTR (mean time to repair, respond, restore…), achieving this objective reduces unplanned work, increases IT productivity, cuts costs, and protects business operations.

In this research on incident management, there was a very high correlation between the combination of automation, AI, and unified platform use and the resultant quality of IT service delivered, incident response effectiveness, and well-defined processes that are not only well-documented, but also consistently used. Organizations in which use of an AIOps platform is mature and enterprise-wide (as opposed to early or departmental) most regularly reported the highest level of incident response effectiveness.

The mature AIOps group was the most advanced in predictive use of AI for proactive actions to catch incidents before they impact users or business operations. They were also most likely to move away from a centralized NOC toward a cross-functional, business-defined approach to incident management.

[1] "Automation, AI, and the Rise of ServiceOps," EMA, March 2023

The wish list

Before diving into the quantitative portion of this research, participants were asked an open-ended question: **"If you could improve one thing about your organization's approach to incident response, effectiveness, or tools used, what would it be?"**

Participants frequently mentioned better training, fewer levels of bureaucracy, knowledge sharing, workflow automation, and increased headcount. However, the runaway top response was around the use of AI and automation. Typical comments were:

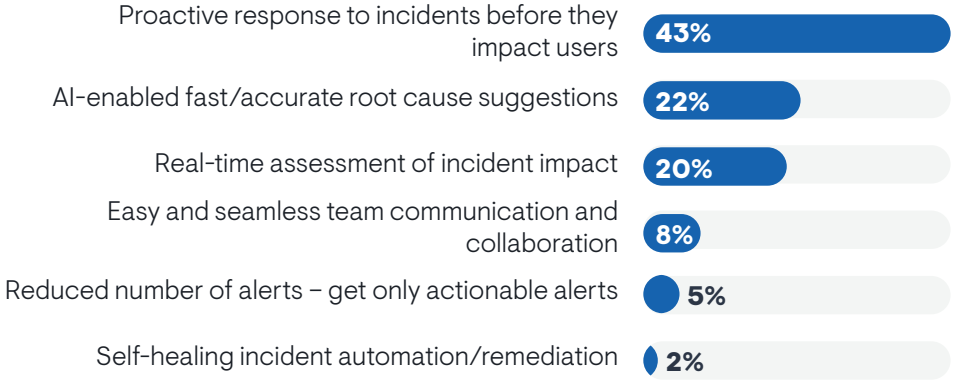
> Preventative monitoring is worth more than incident response after the fact, no matter how good it might be.

> Be proactive rather than reactive. We seem to wait until things happen before we do anything to stop it.

> I would like to see more automation and integration of the tools used. That would help reduce the manual effort and human error that is typical of the incident process.

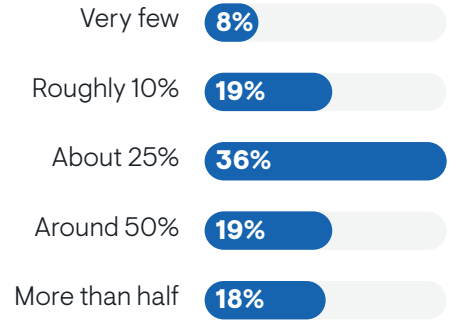
> If I could improve one thing about my organization's approach to incident response, it would be to try to be a bit bolder – a bit more unconventional and try out more innovative methods using AI and automation.

These sentiments were echoed when directly asked, **"If you could choose one thing to do really well, what would have the biggest positive impact?"** Allowed only one choice, 43% of the respondents chose "proactive response to incidents before they impact users."



However, current reality falls short of that vision. Only 18% of the panel successfully intercept more than half of incidents before they impact users. All of that group characterized their use of AIOps as strategic, mature, and implemented on an enterprise-wide platform.

What percentage of incidents are caught before causing an outage/user impact?



A fundamental disconnect

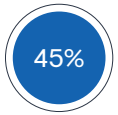
IT is judged by the consistency and quality of service it delivers to the business – both internal employees and customers. Yet, IT tends to define an IT service by technology area (database, network, servers) and to organize along those same technology lines. In this panel, only 19% of respondents state that they define an IT service by the business function the technology supports.

This disconnect between the way business stakeholders evaluate IT and the way IT views itself hampers effective incident response and management. When there is a problem with a business service, IT professionals cobble their expertise together using specialized tools that may very well be disconnected from each other.

These siloes act as barriers to the cross-functional collaboration and workflows that effective incident management demands. In fact, asked to name the biggest challenges to effective incident response, the top contender was the combination of "lack of a unified view/dependency mapping of service elements" and an "understanding of the business context/impact."

Enterprises of all sizes are attacking this problem on multiple fronts, including adoption of platforms to enable cross-functional processes within a unified view of the services. However, the disconnect cannot be solved by the simple addition of technology. It requires organizational support as well. Increasingly, enterprises are reorganizing to take advantage of the advances made possible by AI and automation, moving toward cross-functional approaches and business-focused teams.

Although oversimplified, how would you describe your IT's organizational principle when it comes to service availability/performance and incident management?



Increasingly, IT is moving to a cross-functional approach, putting systems in place designed to prevent incidents

IT is centrally organized along functional and technology lines (network, application, storage, servers…as in a NOC)

Teams that respond to incidents organize around specific business services or lines of business

Process

Incident response process flow

In order to establish a common base of discussion across the diversity of industries participating in this study, EMA presented a possible typical process flow.

Understanding that every organization is different, does the following incident response flow reflect the incident management flow in your organization?

- Detection/identification and logging
- Categorization, triage, prioritization, and routing
- Team engagement, incident communication, and collaboration
- Response for analysis, diagnosis, and resolution
- Closure and post-incident reporting

Of the panel, 76% said it is a typical flow, while 24% responded, "Our flow is more ad hoc – it depends on the incident." Not one respondent said, "no." Although the specifics and vocabulary differ by organization, this basic flow represents the day-to-day realities of today's incident response process.

Process use and effectiveness

The research panel reported a relatively high level of process definition and documentation. Asked, **"Which statement best describes your organization's incident management processes?"**

- 57% stated that they have well-defined processes that are also well-documented
- 36% reported variability, having some processes that are well-defined and documented, but also stating that coverage has many gaps
- 7% characterized their processes as well-known but undocumented

Furthermore, 73% of respondents say that these processes are "widely used, well understood, and frequently updated." Yet, asked to rate the effectiveness of their organization's incident management processes, only 41% self-rated the processes as "very effective." The remainder were split between the faint praise of "meets our needs" (47%) and a straight "needs improvement" (12%).

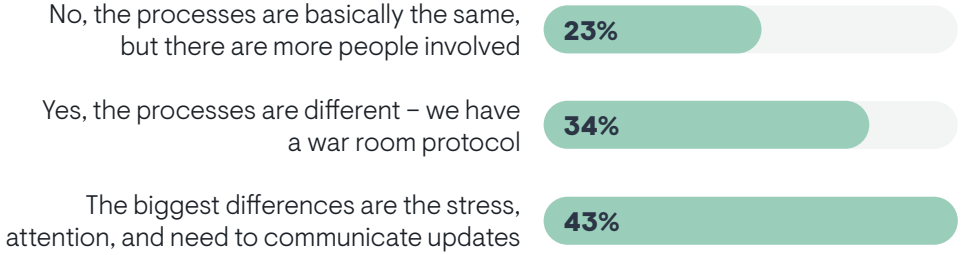
Clearly, there is a math problem here. The apparent mismatch between process adoption and effectiveness has its roots in consistency. Of the group that agreed with EMA's basic process flow but identified their approach as being more ad hoc, drilldown analysis showed that they also:

- Self-rate a lower quality of IT service (only 20% rated service as outstanding compared to 37%)
- Are least likely to use a unified platform
- Have the lowest level of both automation and AI and the least aggressive plans for use of GenAI
- Report incident response processes as less effective than average (26% vs. 47%).
- Have a higher rate of incidents coming through user complaints instead of monitoring tools

Process variations for outages and cybersecurity incidents

Instinctively, people understand the difference between an incident and an outage. There is an urgency and intensity that attends an outage that just isn't there with a routine incident – but are the processes different? It turns out that 66% of the organizations follow essentially the same processes for an incident and an outage. Only 34% of the panel report completely different processes, with an outage receiving war room-like attention.

Does the incident management process change during an outage?



Cybersecurity incidents are a different story. People and processes may differ, and the cybersecurity team takes the lead for 47% of the organizations.

When the incident is due to cybersecurity issues, which statement best represents your organization?

Process pain points and potential

The people problem

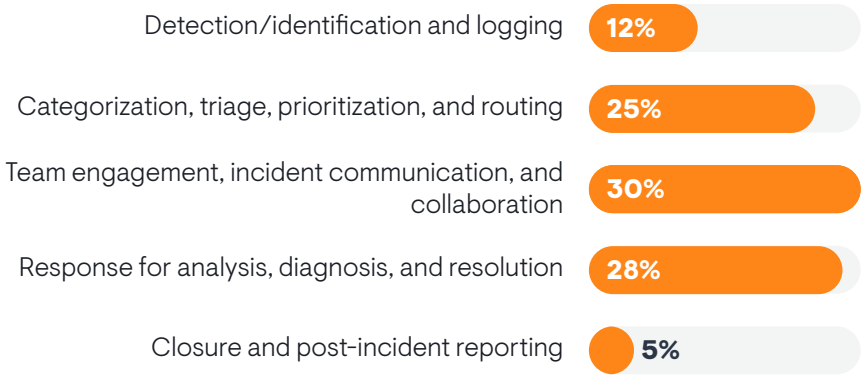
Referencing the incident management flow that was outlined earlier, participants were asked a series of questions specific to phases. Here are some of the more interesting and informative responses.

Which two steps or phases are the most challenging or most in need of improvement? Select two.

Team engagement, incident communication, and collaboration was the phase that took the lead as the step most challenging or most in need of improvement. It also led the pack when participants were asked to identify the single top culprit in total MTTR.

The diversity of incident response teams – essential to resolution in complex environments – complicates the people side of the equation. Not only siloed solutions and tools are problematic – siloed organizations are also a barrier to incident response speed and effectiveness.

Which phase is most time-consuming: biggest contributor to MTTR? Select one.



People and their human natures appeared as a stumbling block in another phase. Asked, **"Which phase is treated as the least important (gets skipped, overlooked, or only done slightly)?"** the clear "winner" was "closure and post-incident reporting."

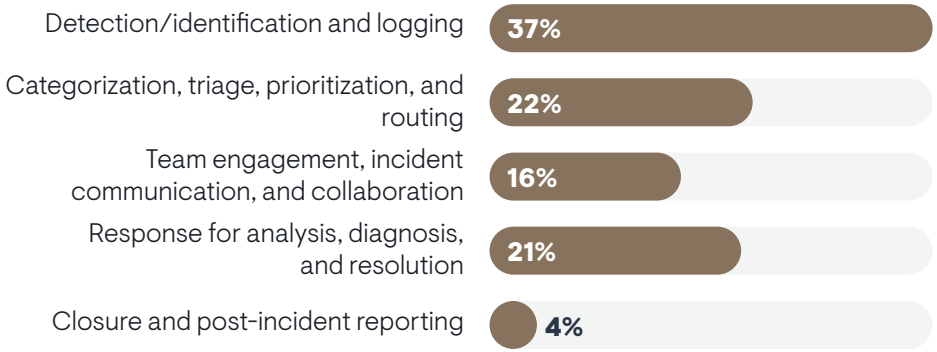
Anyone who has spent more than a day in IT knows firsthand that when an incident is resolved or an outage is restored, the first reaction is not, "Well, let's all sit down and make sure we thoroughly document this situation." No. Human nature is to heave a collective sigh of relief and return to more rewarding planned work – until next time. This understandable instinct leaves a potential treasure trove of insight untapped.

Potential use of automation and AI

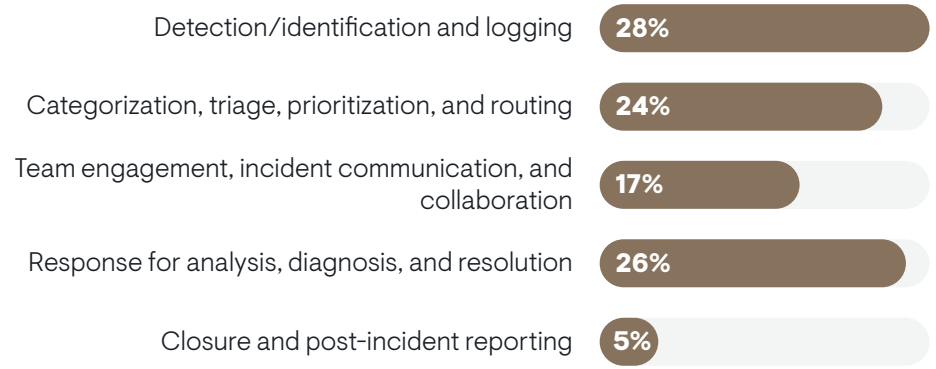
The panel as a whole sees automation and AI as most applicable to areas in which those advances are already commonly used. The combination of AI and automation that typifies AIOps makes great strides in the troika of detection, categorization, and response, but leaves the problematic phases of team engagement and post-incident reporting largely untouched by technology.

Interestingly, very few people identify those weakest areas (team engagement/collaboration and post-incident reporting) as candidates for automation or AI. However, when presented with hypothetical applications of technology in exactly these areas, the potential benefits were rated as delivering very high value or "transformative" results (see sections on AI and automation).

Which phase is most automated or the best candidate for automation?



In which phase is AI, analytics, or ML most used or most likely to get used?



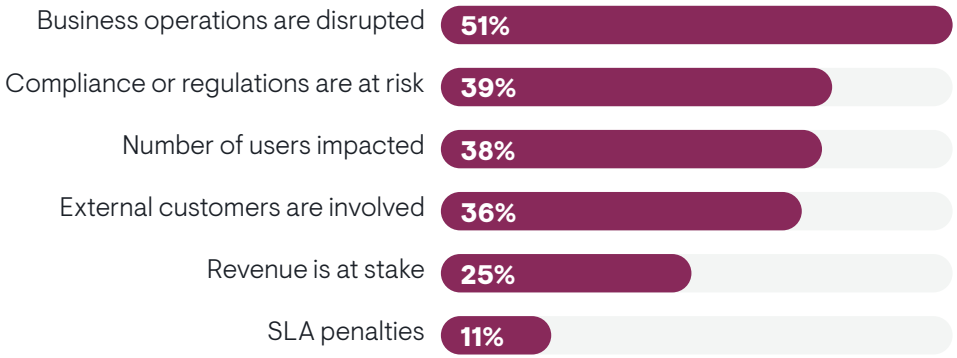
Incidents

Incident basics

Most organizations define an incident as any degradation in IT service or availability, with 35% of the panel specifically including predicted or potential issues and 28% specifying disruption to business operations. Likewise, almost all organizations prioritize incidents by severity. At a minimum, they differentiate between incidents and major incidents, with 42% of respondents stating that there are 4-6 established priority levels with set response and resolution times.

Universally, any incident that disrupts business operations qualifies that incident as a high priority. Almost tied for second place are compliance, number of users impacted, and the fact that external customers are involved.

What determines the priority of an incident? Select two.



Asked how incidents are most often surfaced, monitoring tools are effective at surfacing issues for almost 70% of the organizations. Roughly one-third of that group credit AI/ML proactive identification of potential issues as the main source of incidents. That leaves a significant 31% of respondents who state that in their organization, incidents are most frequently identified through user reports and complaints, usually through the service desk.

It may be surprising to some readers that user complaints are the early warning system for so many in this time of technological advances. However, this percentage is very consistent with dozens of EMA research initiatives conducted with thousands of respondents. This finding means that there is still much room for improvement.

The gap between organizations that rely on users as canaries in the IT mine and those that employ AI/ML to apprehend potential issues is a de facto competitive gap with serious business implications.

However an incident is raised, they are created and tracked through a mix of ITOps/AIOps and ITSM ticketing platforms as follows:

- 35% use a centralized ITOps or AIOps system or platform
- 31% use tickets in the service desk or ITSM system
- 31% use a mix of ITSM tickets and ITOps logs
- 3% use a decentralized DevOps/SRE "you build it, you run it" approach

When there is an incident, the two groups most responsible for identifying and fixing the issue are ITOps and ITSM/service desk followed by a supporting cast of DevOps, engineering/development, and the network team. This confluence of responsibility across diverse groups is reshaping organizations and collaboration in the ServiceOps movement detailed in numerous EMA studies.[2]

[2] "Automation, AI, and the Rise of Service Ops" EMA, March 2023

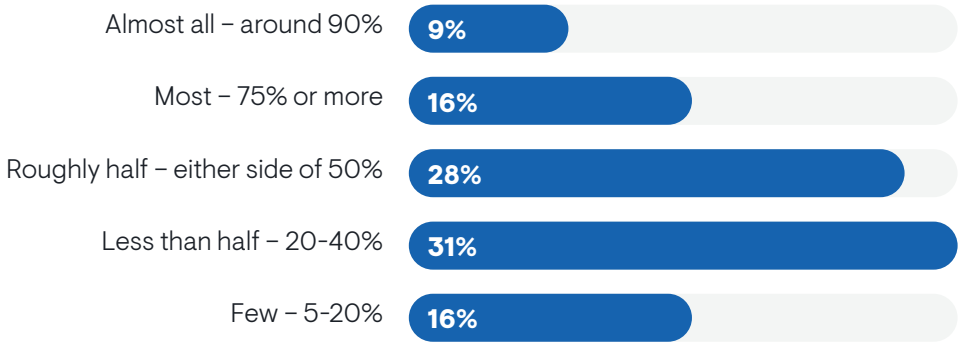
The shape of MTTR

Reducing incidents and outages is the top goal for most organizations across industries. Failing that objective, the next best thing is to significantly reduce MTTR. This research surfaced some interesting findings that suggest productive ways to cut MTTR, whether the "R" is repair, respond, restore, or otherwise revive a troubled service.

Actionable alerts vs. noise

Organizations increasingly use AI and automation as well as AIOps platforms to reduce the number of alerts and the alert fatigue that accompanies a cascade of noise. What's more, these approaches cut MTTR by making the alerts that do demand attention actionable – real and supported by guidance.

On average, what percentage of incidents/events/alerts are actionable (turn out to be a problem that requires a resolution and includes at least one piece of insight on how to respond)?



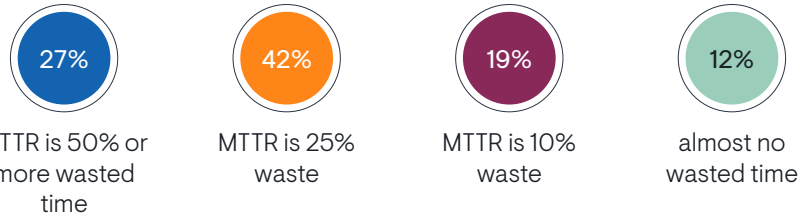
Those respondents who cited the highest levels of actionable alerts not surprisingly also had mature AIOps implementations at an enterprise level. The ability to consolidate, analyze, and deliver useful direction from a complex maze of information sources is critical to saving time and human talent when performance, availability, and business operations are at stake.

The time in MTTR

There was a wide range of answers to the question of MTTR and the divide was along the lines of degree of automation and AI. Answers to the question, **"Once an incident is logged, how long does it usually take to resolve it?"** ranged from minutes to hours, and in some cases, many hours:

- 70% 1-4 hours
- 19% more than 4 hours
- 11% minutes

An EMA client posed an interesting question. The question, **"What percentage of the MTTR is inactive time spent waiting for information or response?"** returned an almost shocking amount of wasted time:

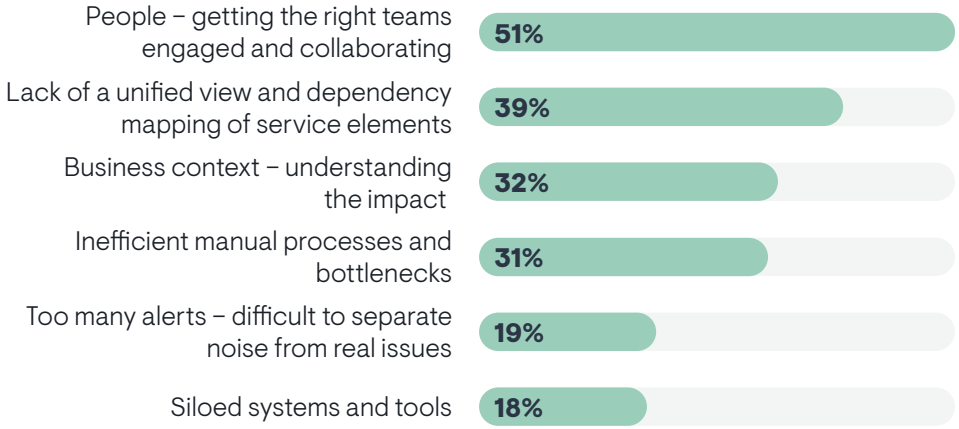


When time is measured in dollars and business gained or lost, wasted time is an outrageous luxury.

MTTR culprits

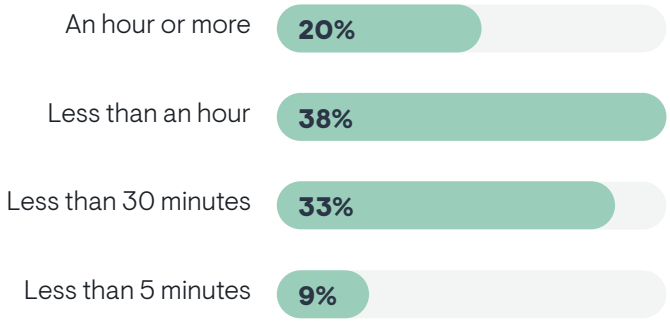
Earlier in the survey, research participants identified "team engagement, incident communication, and collaboration" as the biggest contributors to MTTR – flanked by categorization and response. The people problem again took first place when naming the top two challenges to effective incident response.

What are the biggest challenges to effective incident response and management? Select two.



With MTTR clocking between 1-4 hours for 70% of respondents and a similar majority reporting that 25%-50%+ of that time is wasted in waiting, it seems practical to identify and attack the sources of waste. Asked about the time it takes to identify and engage the right response teams, 58% of this panel answered 30 minutes to an hour or more. That time, whether 45 minutes or two hours, is wasted time. It is also a significant and addressable portion of MTTR.

How long does it take to identify and engage the right response teams from the time an incident is created?



The other biggest challenges to effective incident response and management highlight another addressable problem. "Lack of a unified view and dependency mapping of service elements," "business context – understanding the impact," "too many alerts – difficult to separate noise from real issues," and "siloed systems and tools" are all different symptoms of the same problem.

Disconnected and disjointed processes, systems, tools, organizations, and technologies turn every incident into the technological equivalent of a custom-made jigsaw puzzle. AIOps platforms and solutions that facilitate information sharing, collaboration, and cross-functional workflows can directly address all of these challenges, slashing MTTR with efficiencies and automation.

Automation and AI in incident management

When it comes to IT service and incident management, it's increasingly difficult to discuss the use of automation and AI in isolation from each other. Each powerful in its own right, the use of the two in combination offers a one-two punch that magnifies the benefits of both capabilities. This mutiplier effect is apparent in results that mature AIOps implementations deliver to the enterprise, including the potential to identify issues before they develop into problems that impact users or business operations.

This research explored the use of automation and AI in incident response separately but did analysis to correlate results and draw conclusions. For example, where automation is a high priority with enterprise-wide implementation well underway, there is a high correlation with the following as well:

- AIOps tends to be a strategic enterprise initiative
- Platform use predominates as opposed to siloed systems and tools
- There is a high level of well-defined/documented processes that are widely used
- Far fewer incidents come in through user complaints (24% vs. 53% for lower automation priority)
- 73% of organizations that have automation as a C-level priority have reorganized to take advantage of AI and automation

EMA created distinct lines of inquiries because not all organizations are exploiting the combination. Where possible, this research looked into the contributions of each technology area as practiced today and as planned for the near future.

Automation use in incident management

A small disclosure: if a potential panelist indicated that their organization wasn't prioritizing automation, they were disqualified from participating. After all, the future of incident management is strongly marked by the automation needed to comprehend the complexity that is today's IT landscape.

It turns out that automation is a mature, C-level strategic initiative for 56% of the panel, early for 28%, and a departmental matter for 16% of the organizations. Without exception, the mature automation group greatly outperformed the other cohorts in all incident response metrics including MTTR, reduction in incidents and outages, cost, effectiveness, IT productivity, and use of AI.

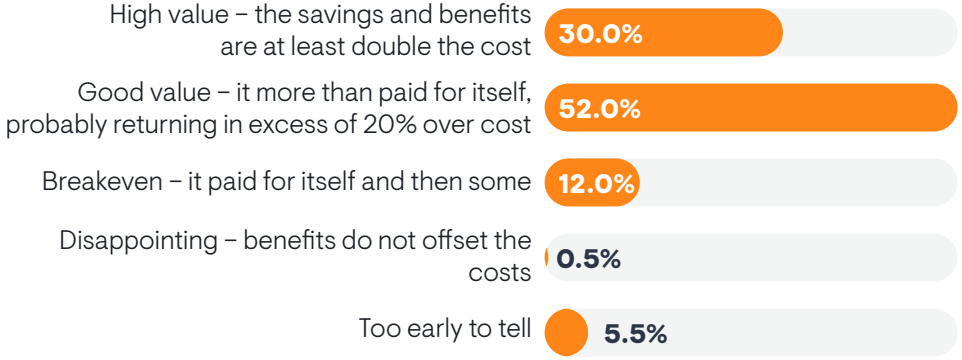
Some general findings on the topic of automation include:

- IT operations is the group most responsible for automation used in incident response and management, followed (in order) by cybersecurity and IT service. DevOps and the executive suite get honorable mention, with 14% of respondents citing a defined incident management team.
- The question, "What's preventing your organization from adopting automation more broadly for incident response and management?" resulted in a tie for top honors. "Data accuracy and accessibility" and "difficulty integrating with other solutions and tools" far outstripped other legitimate impediments including cost, resistance to change, and lack of skills.
- The top metrics used to measure investments in incident management automation in order were: reduction in MTTR, reduction in events and incidents, reduction in downtime, security and compliance metrics, SLA performance, reduction in escalations (L2, L3), reduction in the number of trouble tickets, and mean time to assemble a response team.

Drivers and results

Automation has a very high success rate in incident response and management. All of this year's panel described their automation initiatives as successful, with 25% of the respondents selecting "very successful – improved efficiency, reduction in MTTR, with very high return on investments." Another 52% of respondents described their success as "initial goals have largely been met with good return on investment." A companion question about cost relative to value returned similar results.

Relative to the cost, how would you characterize the return on your incident automation investment?

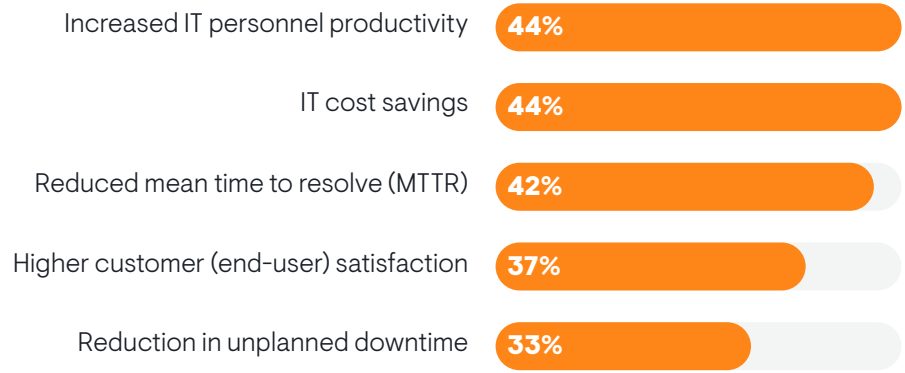


The success of incident response and management automation is further reflected in the alignment of drivers and results delivered. The top drivers of IT automation in incident response and management are tightly grouped in ranking:

- Reduced MTTR and downtime
- Improved user experience
- IT personnel productivity
- Business impact/revenue
- Cost savings
- Cross-functional workflows

As it turns out, the top drivers of automation in incident response and management are a very close map to the top benefits that automation delivers.

What are the top two benefits achieved so far through incident management automation?



AI use in incident management

The use of artificial intelligence (AI) in any of its forms lags far behind the adoption of automation in incident response and management. Roughly half of this research panel characterized the current use of AI/ML and analytics in their organization's incident management processes as "Early – use of AI is strategic and increasingly common but still very early." Another 20% chose "Departmental – different functions and tools use AI, but there is no unified plan."

The remaining third that responded "Mature – use of AI is strategic, well-established, and highly effective" outperformed the other groups in many ways.

- They tended to use a much higher degree of automation in incident management.
- Their incident management was seen as a lot more effective: 55% of this group rated their incident management processes as very effective vs. 21% that are early with AI.
- They allowed more autonomous actions to be taken unattended by humans and also took more proactive actions based on AI predictions. As a result, they report a high percentage of incidents that are caught before causing an outage or impacting users.
- 34% of the mature AI group report actionable alerts at 75% or more vs. 11% for those early to AI
- This group uses AI in change management for incident response and for pre-change impact at a much higher level than those organizations that are early or departmental in their use of AI.
- They are more likely to be in pilot with GenAI and are more aggressive in a timeframe for use in production.

The future is bright for GenAI in incident response

Generative AI (GenAI) in forms such as ChatGPT commands a lot of mindshare in the culture at large and IT in particular. This research panel was no exception. Asked about their personal perception of GenAI, 48% of respondents said, "It's exciting and I can't wait to get hands-on experience with it." The remainder were pretty evenly split between a group that thinks it is moving too fast and another group that sees it as simply another tool in the panoply of options.

Almost all of the participants state that GenAI interest is high in their organization's incident management plans. Only 5% of respondents stated that there are no plans to use GenAI in incident response and management. More common were the 38% of respondents who see their organizations in the research phase, exploring its practicality and use cases. The remaining majority were in pilots/proof of concept (PoC) or actually in production (note: The exact meaning of the phrase "in production" can range from GenAI-written scripts to vendor-supported incident management solutions).

EMA posited some hypothetical use cases for GenAI in several incident management processes. The response was highly positive. Examples of use cases are:

If a real-time solution could accurately determine, in seconds, the impact of incidents across distributed systems and communicate it in clear language, the value would be...

- 38% Transformative – Priority actions could be instantly identified at speed and scale
- 45% High value – All impacted response teams could be immediately identified
- 17% Valuable – It would increase incident response effectiveness

If a real-time solution could generate an accurate summary of alerts and incidents that includes incident title, description, and possible/likely root causes in seconds, the value would be...

- Transformative (27%) – It would cut MTTR by at least 20-30 minutes per incident
- High value (55%) – It would save 10-20 minutes per incident
- Valuable (11%) – It would save 5-10 minutes per incident
- Useful (7%) – It would save time

If knowledge base articles could be automatically and accurately generated/updated and easily searched with normal, everyday language, what percentage of incidents, tickets, and cases might be deflected?

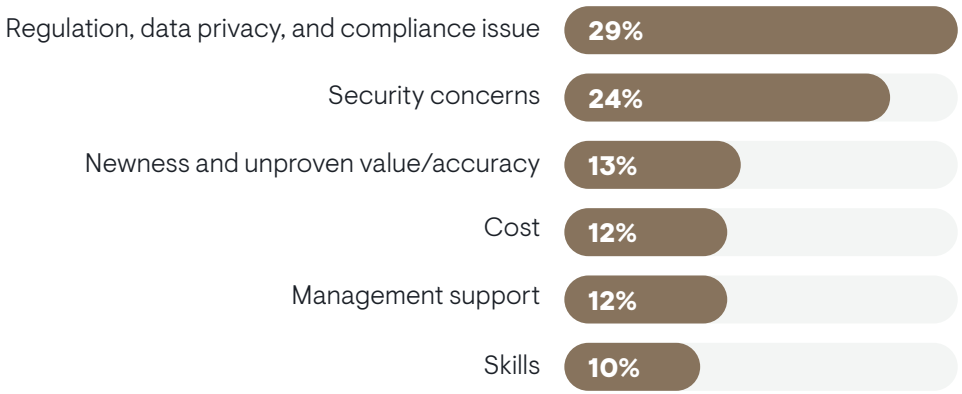
- More than half (25%)
- As much as half (41%)
- 10%-25% (26%)
- Up to 10% (8%)

If comprehensive incident reports could be automatically generated (including alerts, impacts, actions taken, causes, results, and participants), what effect would that have on incident closure and analysis?

- Continuous improvement would become practical and post incident analysis would greatly increase (39%)
- It would be easier to identify underlying problems that cause repeated incidents (31%)
- We would probably discover ways to become more efficient in incident response (29%)
- I don't know because we really don't do much once an incident is resolved (1%)

Clearly, AI and GenAI in particular hold the potential to slash MTTR and reduce the frequency, duration, and impact of outages. Research participants were bullish about the increased adoption of AI in incident response and optimistic about the timeframe for introducing GenAI into incident processes. Surprisingly, hesitation about adoption of GenAI was not its newness, but concerns around regulations and security.

What is the main reason your organization might delay implementing GenAI or ChatGPT?



Concluding thoughts

Incident response and management are practices as old as IT. However, they are in a constant state of reinvention with the advent of technological advancement, especially unified platforms, AI, and automation. The degree to which organizations differ in their exploitation of these advances represents a very real competitive advantage or disadvantage depending on which side of the difference an enterprise finds itself.

This fact of business life is reflected in the automation investments planned for incident response and management over the next two years: 43% of respondents indicate that there will be a strategic growth in emphasis with a very high level of investment and 50% of participants foresee strong growth with matching investment. Interest and investment in AI will follow a similar trajectory propelled by the potential of GenAI.

The game-changing impact of the combined power of AI and automation, such as in AIOps, is already well-established in the initial and analysis/response phases of an incident. The ability to transform a cacophonous cascade of alerts into a few true, meaningful, and actionable alerts not only slashes MTTR, it also saves humans from the mind-numbing, spirit-crushing task of trying to make sense of so many variables. Vendors will continue to refine and increase these capabilities. Additionally, as GenAI becomes mainstream, there will be many innovative use cases that will directly address some of the underserved aspects of incident response and management.

High-performing IT service absolutely relies on these advances. However, technology alone can't deliver excellence. Siloed organizations are as counterproductive as siloed systems. Outdated organizational models constrain the potential advantages that technology can offer.

Organizational agility and unimpeded cross-functional workflows are every bit as much of a business accelerator as advanced technologies. For just that reason, 65% of participants in this research stated that they have reorganized to take advantage of AI and automation. They know that the cornerstone of effective incident response, management, and prevention is effective and innovative partnering of human talent with technology.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT analyst research firm that specializes in going "beyond the surface" to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**

4374.022624