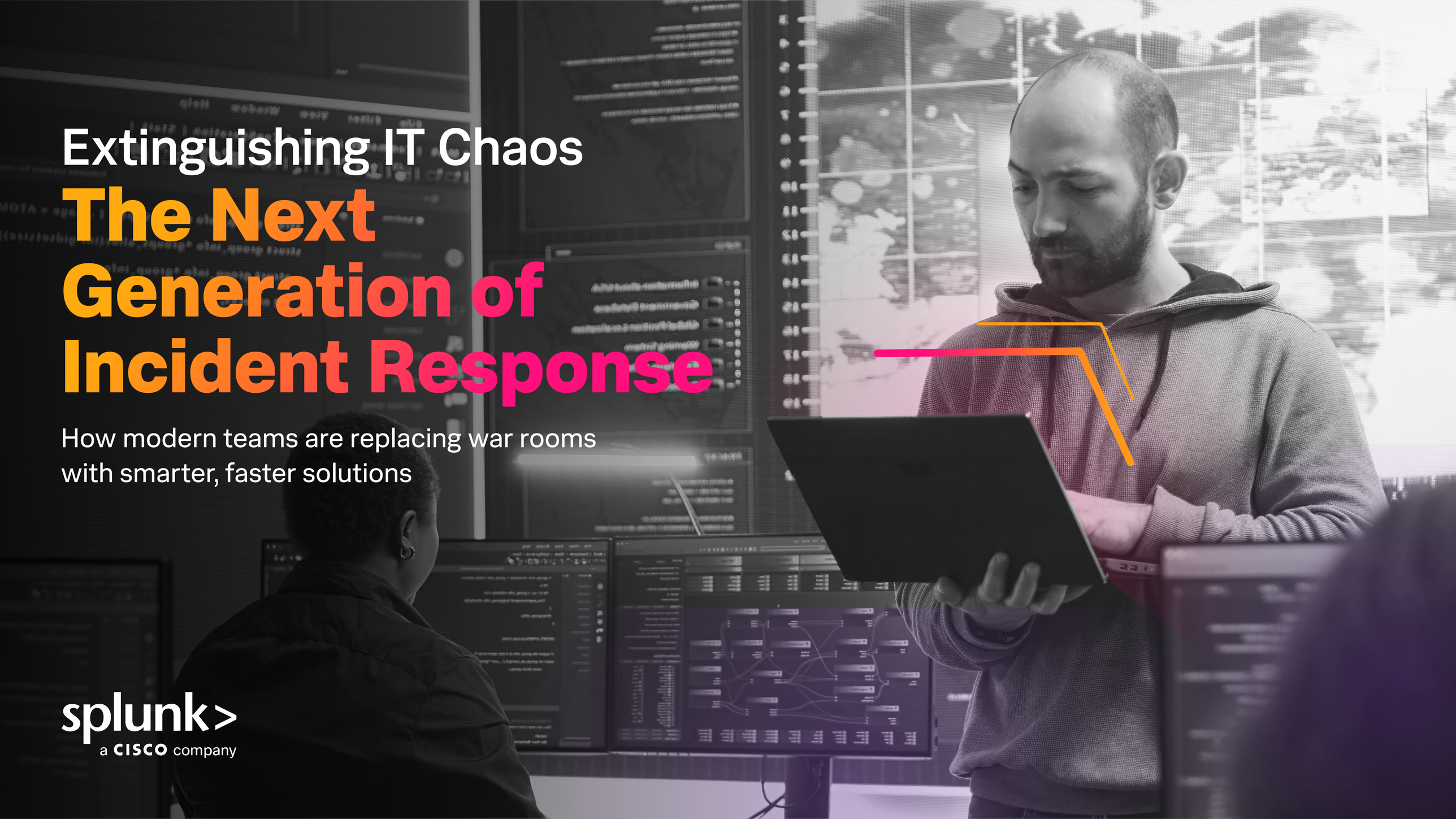

Extinguishing IT Chaos

The Next Generation of Incident Response

How modern teams are replacing war rooms with smarter, faster solutions

splunk>
a CISCO company

Fighting fires in IT

Firefighting has come a long way since the days of bucket brigades and manual alarm bells. Today, smart sensors, automated alerts, and highly specialized teams ensure that fires are detected early and prevented before they spread. IT incident response has followed a similar path, evolving from reactive, all-hands-on-deck war rooms to data-driven strategies that prevent or quickly resolve major incidents in their tracks.

Many seasoned professionals will recall being summoned to war rooms in the early days of IT. Teams created these high-pressure, all-hands-on-deck environments to respond to critical system issues. For some organizations, these war rooms remain a familiar and, hopefully, evolving part of their incident response strategy. Cross-functional teams scrambled to diagnose and fix issues, relying on fragmented data, manual troubleshooting, and institutional knowledge. The chaos often yielded results, but the process was slow, costly, and reactive, verging on being unsustainable.

Fast-forward to today, and while the traditional war room is no longer the gold standard, it still exists in one form or another in many organizations. However, many organizations are recognizing the inefficiencies of this approach. They are exploring alternatives or working to reduce the frequency of war rooms by adopting more proactive and scalable incident response strategies.

Leading IT teams leverage observability platforms, AI-powered diagnostics, and integrated collaboration tools to manage major incidents efficiently, regardless of team members' locations. What once required everyone in the same room is now less frequent as organizations adopt proactive strategies that identify and resolve issues earlier, reducing the need for war rooms in the first place.

While war rooms are becoming increasingly rare, when they do occur, organizations that employ observability tools can reduce their impact — limiting the time they are active, ensuring swift, targeted resolution, and ultimately reducing Mean Time to Resolution (MTTR).

This shift didn't happen overnight. The lessons of yesterday's war rooms, the rise of advanced technologies, and the growing complexity of distributed applications and services drove this transformation. Moving to proactive prevention and expediting response in reactive scenarios wasn't just an innovation. It was a necessity.

Fires are best prevented by measures taken during construction, not after a building's completion. IT systems also need fireproofing — proactive measures enhanced with unified visibility that prevent issues from spreading. Of course, with applications and infrastructure, sometimes the biggest challenge is finding out where the fire actually is.

So, how did we get here, and where is IT incident management headed next? Let's find the source of the smoke.

When IT crises sparked chaos

There was a time when assembling a bucket brigade was the best and only way to put out a fire. Everyone pitched in, but the process was slow, and the fire often reignited when proper firefighting tools weren't available. Early IT war rooms were similarly improvised, urgent, and frequently inefficient, but they were the best strategy at the time.

IT firefighting in the early days

Before IT teams had the tools to prevent problems, crises often ignited without warning. Unfortunately, incidents still happen from time to time for every organization. Outages, system crashes, or failures threw entire organizations into panic mode, forcing teams to rush for answers, typically leveraging their siloed and niche tools to understand better what issues were occurring in their respective domains. These moments, while unplanned, shaped how early incident management operated.

War rooms relied heavily on their siloed and distributed tools, fractured processes, and sheer human effort to define their operation, which remains valid for some teams today. They became the nerve center for problem-solving, where IT practitioners, developers, network engineers, and even more teams huddled to triage issues.

With only the contemporary tools as the best available solutions, these triage teams did what they could. Teams often relied on fragmented data sources, combing through dashboards, logs, and other tools to uncover clues — clues that were often disconnected from true causation. Even well-prepared teams with proper alerting and monitoring struggled to cut through the noise, as a single issue could generate hundreds of related alerts, obscuring the root cause.

Without a unified view, progress was slow and heavily dependent on institutional knowledge, forcing teams to rely on trial and error to piece together the full picture.

The environment was intense. The high-pressure atmosphere of the war room combined with the complexity of troubleshooting IT systems under duress. Teams juggled fragmented tools, real-time troubleshooting, and the pressure to resolve critical issues quickly. Prolonged downtime disrupted customers, damaged revenue, and harmed operational stability, further amplifying the urgency. The war room's centralized approach ensured that everyone could coordinate, but sometimes, this came at a disproportionate cost to time, resources, and team morale.

What worked well (and why it had to change)

While war rooms were stressful and reactive, they weren't without merit. They brought together the right minds working together to achieve the following:

- **Collaboration under pressure:** Teams brainstormed solutions together, combining diverse expertise to pinpoint and fix issues.
- **Real-time problem-solving:** Key decision-makers were in the room, enabling faster resolutions without endless escalation.
- **Knowledge sharing:** War rooms created opportunities for teams to share insights with senior personnel, providing insights to those who were more junior.
- **Historical insights:** Connecting the dots with interdependencies and legacy infrastructure knowledge.
- **Sense of urgency:** The focused environment ensured that problems were treated with the importance they deserved and that executive business updates were quickly consolidated and delivered.

But while these benefits helped when teams were "in the moment," the cracks in the war room approach were evident:

- **Burnout was rampant:** Constant firefighting drained teams mentally and physically. Resources were often required to be present in war rooms to ease communication when needed, even if they were not actively called upon, adding to the strain of being on-call.
- **Misdirected focus:** Chasing false positives often distracted teams from focusing on valid root causes.
- **Lack of scalability:** With everyone relying on manual tasks and institutional memory, war rooms couldn't keep up with the growing system complexity.
- **Siloed knowledge:** Once an incident was resolved, much of the insight disappeared because no formal documentation processes existed.
- **Tool sprawl:** Teams juggled an overwhelming number of tools to understand the health of IT services, requiring extensive expertise to maintain and operate each tool. Without a unified view of data and infrastructure, teams duplicated efforts and manually correlated information across tools, delaying resolution and adding frustration.

Moving beyond the war room mentality

The war room served its purpose as a crisis-response hub, where teams gathered to manage pressing IT issues, and in certain organizations, it still does. However, scaling this reactive model became increasingly tricky as IT environments expanded and applications modernized. New technologies emerged, system complexity grew, and digital transformation accelerated. The old methods — centered on manual processes, isolated teams, and fragmented tools — weren't able to keep up with the complexity of modern applications and operations.

A byproduct of war rooms was the emergence of an unofficial metric: Mean Time to Innocence (MTTI). Rather than streamlining resolution, MTTI became a measure of how quickly teams could prove that their domain wasn't responsible — shifting blame rather than solving the problem. While intended to streamline accountability, this approach often exacerbated the reactive and siloed nature of incident response, leading to inefficiencies and missed opportunities for collaboration.

The war room era taught IT teams valuable lessons, but it also revealed the limits and impacts to MTTR. Teams needed more context, visibility, collaboration, and scalable ways to respond to incidents. This set the stage for a transformation that would forever reshape IT incident response.

Inefficiencies and missed opportunities

- **Manual troubleshooting** took too long for large, distributed systems.
- **Siloed tools and data** made it nearly impossible to see the full picture.
- **Global operations** couldn't rely on a single, centralized physical room.
- **Inefficient use of time** by involving representatives from all parts of the technical organization, often with members not having authority to act.
- **Reactive review processes** forced teams to sift through hundreds, or worse, thousands of emails and alerts after the fact, trying to determine if an issue had been flagged but missed.

When old methods couldn't hold back the flames and lessons learned

In the past, fire alarms only went off after someone pulled the alarm or when the fire had already spread. Today, smart systems detect heat and smoke early, stopping fires before they spread. The same applies to IT incident management — reactive responses are no longer enough.

The strain of the old model

War rooms were not deliberately designed as a long-term solution. Instead, they emerged in the heat of the moment, modeled after how other crises had been handled or how peer organizations managed incidents. While it succeeded in rallying teams during emergencies, its reactive nature and reliance on manual processes exposed its critical flaws as IT environments grew more complex.

The cracks in the war room model emerged from its inability to keep up with evolving IT challenges. Technological factors made this traditional approach ineffective over time:

- **Searching for Critical Data:** Developers and engineers often had to sift through massive volumes of log data manually, searching for a single relevant line — delaying Mean Time to Detect (MTTD) and Mean Time to Resolve (MTTR).
- **Siloed Monitoring Tools:** Fragmented monitoring tools delayed root cause analysis, making issue detection slower and less precise. The lack of contextual awareness often made it difficult to identify causation, as one issue could cascade into others without clear visibility across domains.
- **Ineffective, Missing, or Irrelevant Dashboards:** Legacy monitoring systems couldn't deliver troubleshooting data visuals relevant to specific services or outage details, leaving teams behind the curve.
- **Modern Complexity and Dependencies:** Applications built on microservices and containerized architectures overwhelmed traditional troubleshooting systems. This complexity also contributed to frequent alert storms, the majority of which stemmed from poorly configured tools rather than genuine incidents, adding noise to already overburdened teams.
- **Agile Development:** Daily or hourly application deployments increased troubleshooting complexities by several factors compared to slower build cycles.
- **Lack of Business Context:** Without a clear understanding of how service failures impact critical business functions, teams struggled to prioritize incidents effectively. A failing microservice might generate alerts, but without knowing whether it disrupted core operations — like processing customer orders — engineers lacked the ability to triage efficiently.

The cost of doing nothing

Leaders realized that failing to modernize incident response came at a high cost for organizations, both operationally and reputationally:

- **Rising Downtime Costs:** Service outages could result in millions in lost revenue and irreparable brand damage.
- **Burnout and Loss of Talent:** Frequent war room activations became drains on the humans who respond to incidents.
- **Operational Inefficiency:** Resource-heavy, often overstaffed, and manually-managed war rooms became costly and unsustainable.
- **Reputational Risk:** Repeated, prolonged outages eroded customer trust and brand loyalty. As more services shift to digital-first models, disruptions now impact everyday essentials like grocery delivery and curbside pickup, making reliability more critical than ever.
- **Competitive Edge Loss:** Reactive war room troubleshooting took away resources often devoted to proactive innovations and modernization activities.

Successes to build on

While traditional war rooms had significant shortcomings, they also showcased practices that remain valuable today. Cross-functional collaboration emerged as a defining strength, bringing together IT, development, and operations teams with unique perspectives. This diversity of expertise encouraged creative problem-solving and accelerated resolutions when it mattered most.

Urgency and focus were equally critical. Teams often cut through bureaucracy, prioritized key issues, and took decisive actions based on available, but sometimes incomplete, data. This ability to act swiftly under pressure became a foundational principle for modern IT practices.

Clear communication structures also played a vital role. Management often monitored war room calls and received real-time updates without the need to hunt for a platform to obtain status updates. Unified command systems kept team members aligned toward shared goals, while centralized communication tools and well-defined escalation paths helped reduce confusion during high-stress situations.

Blending the past, present, and future

Today, leading organizations leverage unified observability solutions that incorporate the best aspects of war room practices while addressing long-standing gaps through modern technology:

- **Automation and AI-Driven Insights:** Machine learning detects anomalies, surfaces actionable insights, and proposes fixes, reducing reliance on manual intervention.
- **Integrated Collaboration:** Observability platforms enable cross-functional teams to access real-time dashboards, automate issue ticketing, and share insights via collaboration platforms.
- **Transparency and Continuous Learning:** Open-access knowledge bases, shared incident reports, and post-incident reviews distribute expertise and encourage continuous learning, fostering a culture of shared responsibility.
- **Systematic Dependency Understanding:** Real-time analysis of dependent systems identifies root causes amidst symptom noise. Historically, this relied on tribal knowledge, making it slow and dependent on war room participants. Today, advanced analytics and systematic mapping enable faster restoration and proactive incident management, often supported by a dedicated “dependency expert.”

The lessons learned from traditional war rooms helped shape today’s IT response strategies, blending human expertise with data-driven insights to resolve incidents faster and more effectively.

CHAPTER 3

From fire alarms to smart alerts

Firefighters once relied solely on station alarms and dispatchers. Today, they use GPS, thermal imaging, and remote monitoring for faster, smarter responses. In IT and Engineering, modern observability tools play the same transformative role. They have optimized the use of a central “war room” by correlating metrics, logs, and traces across IT systems, including front-end applications, microservices, and infrastructure. This allows distributed teams to troubleshoot issues in context and respond with precision.

Unified observability has emerged as a game-changer for IT teams tasked with managing incidents. By providing a consolidated view of system health, unified observability tools enable teams to detect, diagnose, and respond to issues faster and with greater precision. For example, distributed tracing allows IT organizations to understand in real-time the interdependencies of their ever-evolving and changing IT service offerings and how those offerings affect the broader business.

Observability transforms reactive troubleshooting into proactive prevention and makes war rooms more efficient if and when they are invoked. IT teams fully realize their potential when they embrace a culture of continuous improvement supported by cutting-edge technology and streamlined processes.

How observability changes the game

Maintaining the zen of having a stable and issue-free IT environment (digital resilience) requires anticipating and resolving issues before they disrupt user experiences. Unified observability solutions are critical to modern IT incident management because they offer clear visibility into system health, enabling teams to avoid war rooms and detect and address issues before they affect users. Effective IT incident management revolves around observability platforms that unify data, automate detection, and provide actionable insights. These solutions provide:

- **Unified Data Streams:** Logs, metrics, and traces converge into a single source of truth, enabling teams to correlate data across environments.
- **Proactive Monitoring and Detection:** Machine learning models detect anomalies early, reducing reliance on legacy approaches like manual monitoring and static thresholding. These advanced techniques provide a better understanding and adaptation to unique business needs.
- **Real-Time Alerts with Context:** Alerts come enriched with relevant diagnostic details, helping teams instantly understand the scope and severity of incidents.
- **End-to-End Visibility:** Unified observability provides insight across infrastructure, applications, and user experiences, ensuring no blind spots.

Better responses, fewer crises

With leading unified observability platforms, IT teams can reduce the occurrence of reactive troubleshooting by adopting proactive and, importantly, contextual incident management strategies. These tools not only detect issues but also streamline response efforts, enabling smarter, faster resolutions:

- **Contextual Escalations:** Incident management tools escalate issues with actionable insights and directed troubleshooting, ensuring the right teams get involved at the right time.
- **Automated Root-Cause Analysis:** AI-driven diagnostics reduce investigation time by highlighting likely root causes based on historical and real-time data.
- **Collaborative Incident Response:** Integrated communication and task-tracking tools enable distributed teams to work seamlessly during crises.
- **Service Dependency Mapping:** Visual representations of system dependencies help teams pinpoint where failures originate, expediting problem resolution.
- **Business Transparency:** Understanding of and adherence to Service Level Objectives (SLO) and Service Level Agreements (SLA).

Implementing unified observability has reshaped IT incident management by redefining how teams detect, diagnose, and resolve problems. It enables proactive, scalable strategies that shift IT teams from reacting to issues to preventing them altogether. By adopting these capabilities, IT teams build a more structured, collaborative, and continuous approach to managing incidents, focusing on readiness, precision, and proactive response.

Building a modern incident response playbook

Putting out fires is only part of the battle. True firefighting begins long before the flames, with meticulous preparation, seamless teamwork, and an unwavering drive to “do even better next time.” In IT, incident management follows the same principle: teams must adopt best practices, refine processes, and leverage the right solutions to ensure operational resilience.

Best practices for modern incident response centers

To handle incidents effectively, IT teams need more than advanced tools — they need well-defined processes and a proactive mindset. The following best practices can help teams respond swiftly, prevent issues before they escalate, and continuously improve how they manage critical events.

Build a culture of preparedness

- ✓ **Cultivate Collaboration:** Encourage cross-functional teams to work closely through integrated communication platforms.
- ✓ **Train Continuously:** Conduct regular incident response simulations to keep teams sharp and ready.
- ✓ **Knowledge Sharing:** Maintain centralized knowledge bases to prevent information silos and ensure team-wide learning.
- ✓ **Focus on Tool Adoption:** Through training and change management strategies, ensure your organization is prepared to fully leverage observability and incident management tools.

Leverage unified observability

- ✓ **Unified and Correlated Observability Pillars:** For faster diagnostics, use platforms that consolidate logs, metrics, and traces into a single view.
- ✓ **Service Dependency Mapping:** Visualize how services are interconnected to identify failure points quickly via distributed tracing.
- ✓ **Actionable Insights:** Use observability tools to contextualize alerts to reduce noise, drive faster resolutions, and enable advanced thresholding mechanisms.
- ✓ **OpenTelemetry™:** Avoid vendor lock-in and ensure interoperability for working with metrics, logs, traces, and more across systems.

Automate where it matters

- ✓ **Pre-Built Automation Playbooks:** Use predefined workflows for common scenarios like restarting services, clearing caches, or reallocating resources, reducing response times and manual effort.
- ✓ **Automated Incident Enrichment:** Automatically enrich incident tickets with key context, including impacted services and recent changes, to ensure teams have actionable information upfront.
- ✓ **Automated Escalations:** Set rules-based triggers to involve the right teams at the right time.
- ✓ **Self-Healing Systems:** Deploy automation scripts that resolve known issues without human intervention.

Enhance collaboration and transparency

- ✓ **Integrated Communication Tools:** Enable seamless communication through built-in chat, video conferencing, and task tracking.
- ✓ **Incident Command Structures:** Define clear roles and responsibilities to minimize confusion during crises.
- ✓ **Post-Incident Reviews:** Conduct in-depth post-mortems to continuously improve response protocols and learn from past incidents.

Prioritize continuous improvement

- ✓ **Metrics-Driven Accountability:** To track team performance, use KPIs like MTTR (Mean Time to Resolution) and MTTI (Mean Time to Identification).
- ✓ **Root-Cause Analysis Audits:** Regularly review past incidents to spot recurring patterns and resolve systemic issues.
- ✓ **Feedback Loops:** Incorporate feedback from team members and stakeholders to refine processes and improve outcomes.

Harness AI/ML for smarter responses

- ✓ **Predictive Incident Detection:** Leverage AI/ML models to identify potential incidents before they escalate, enabling proactive interventions.
- ✓ **Anomaly Detection and Prioritization:** Use machine learning to distinguish critical issues from false positives, focusing attention on what matters most.
- ✓ **Adaptive AI-driven Thresholding:** AI-powered systems adjust alert thresholds dynamically, minimizing noise and improving incident prioritization based on historical patterns and real-time conditions.

Integrate observability throughout your organization

- ✓ **Seamless Alert Integration:** Observability platforms should be tightly coupled with your incident management system to streamline workflows and reduce response times.
- ✓ **End-to-End Automation:** Automate the creation of incident tickets directly from observability alerts, including enriched context for faster triage.
- ✓ **Unified Dashboards for Action:** Provide a single interface where teams can correlate observability data with incident management actions, promoting efficiency and reducing silos.
- ✓ **Change Management Awareness in Observability:** Ensure observability platforms track and correlate incidents with recent deployments and modifications, enabling teams to detect change-related issues faster.
- ✓ **Knowledge Management for Incident Resolution:** Maintain a shared repository of past incidents, resolutions, and best practices within observability tools, improving visibility and reducing redundant troubleshooting efforts.
- ✓ **ChatOps-Driven Observability Collaboration:** Embed observability insights directly into ChatOps platforms, allowing teams to diagnose, escalate, and resolve incidents collaboratively in real time.

The human element: collaboration and culture

While technology accelerates response efforts, human expertise drives meaningful decisions and sparks innovation. Successful teams cultivate a culture of trust by conducting transparent post-incident reviews, where lessons are shared openly without assigning blame. This approach fosters honesty, encourages continuous improvement, and builds resilience for future incidents.

Knowledge sharing is equally essential. Teams ensure vital information is readily accessible through shared reports, best practices, and collaboration platforms. Understanding whether similar incidents have occurred in the past helps teams recognize patterns and anticipate potential problems. When incidents do happen, reviewing root causes and implementing necessary changes prevent recurrence and contribute to the continuous improvement of service quality. Regular training sessions and simulated crisis exercises further strengthen team readiness, boosting confidence and reinforcing a proactive response mindset.

By following these best practices, IT teams can move from reactive firefighting to proactive, data-driven incident management, transforming potential crises into manageable challenges.

From firefights to future-ready IT

Modern IT incident management has evolved from reactive, costly, and inefficient responses, such as the “all hands on deck” panic common to centralized war rooms, to proactive, contextual, end-to-end, data-driven strategies powered by real-time monitoring and predictive insights. Once a hub of urgent troubleshooting, the traditional war room has given way to distributed teams using integrated observability platforms, shared data, and proactive monitoring tools.

Today’s leading IT professionals collaborate through modern observability and incident management platforms supported by cross-functional dashboards and integrated communication tools. Just as firefighters now rely on smart sensors and predictive models to combat fires, IT teams use advanced platforms to stay ahead of system failures and service disruptions.

The following capabilities illustrate how modern IT incident management ensures resilience and agility:

- **Unified insights** drive faster resolutions by consolidating logs, metrics, traces, and service dependency maps into a single view, enabling teams to identify root causes quickly.
- **AI-powered capabilities** like Machine Learning (ML) and Generative AI (GenAI) help automate root-cause analysis, anomaly detection, and contextual recommendations, helping IT teams scale operations while reducing manual workloads.
- **Predictive analytics, automated incident escalation**, and contextual alerts make proactive prevention a reality.
- **Integrated communication platforms and AI-driven task management systems** allow multi-disciplinary teams to collaborate globally, turning even complex incidents into opportunities for continuous improvement and innovation.
- **Integrated observability tools** streamline workflows by linking with incident management systems, providing teams with the necessary context to act quickly and effectively.
- **AI-powered tools** extend beyond root-cause analysis to provide proactive prevention and deeper insights into system dependencies, mitigating issues before they escalate.
- **Advanced automation** combined with human expertise transforms complex incidents into opportunities for innovation and continuous improvement.

The next digital fire might spark without warning. But with the right observability tools, smart automation, and a prepared team, you’ll be ready to detect it early, respond quickly, and keep your critical systems running smoothly.

From war room firefights to business-driven observability

You've learned how modern IT teams are replacing chaotic war rooms with proactive incident management. Now, take it a step further — discover how observability and AIOps can drive business value, optimize performance, and reduce downtime.

Download the e-book: How Observability Can Bring Value to Your Business

splunk> a CISCO company

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk LLC. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2025 Splunk LLC. All rights reserved.

25_CMP_ebook_extinguishing-IT_chaos_v7