pagerduty

Modern Incident Response

The Definitive Guide

The Need for Better Incident Resolution

Complexity is on the rise. To meet the rising demands of customers, organizations are being forced to scale their operations in ways that introduce additional complexity and chaos. More people are involved in operations and in incident response, across an ever-increasing mix of systems, applications, tools, and layers of abstraction, resulting in more and more risk to the business.

As digital operations scale up within an organization — especially when developers are given operational responsibilities to own the services they build in production — one of the core challenges becomes ensuring the best possible customer experience in the face of degradations and outages. Organizations looking to improve their incident response must first establish consistent practices, roles, and terminology. In this guide, we'll walk you through incident best practices, and capabilities you can leverage to embed those best practices into your response process.

The Modern Incident Response Approach

Modern Incident Response is PagerDuty's philosophy for quickly and accurately orchestrating the right response for every incident: routine operational issues, major incidents, and everything in between. The approach is built on battle-tested industry best practices. It provides the foundation for how we help organizations go beyond just paging someone to look into an issue, and instead addresses the full spectrum of response needs.

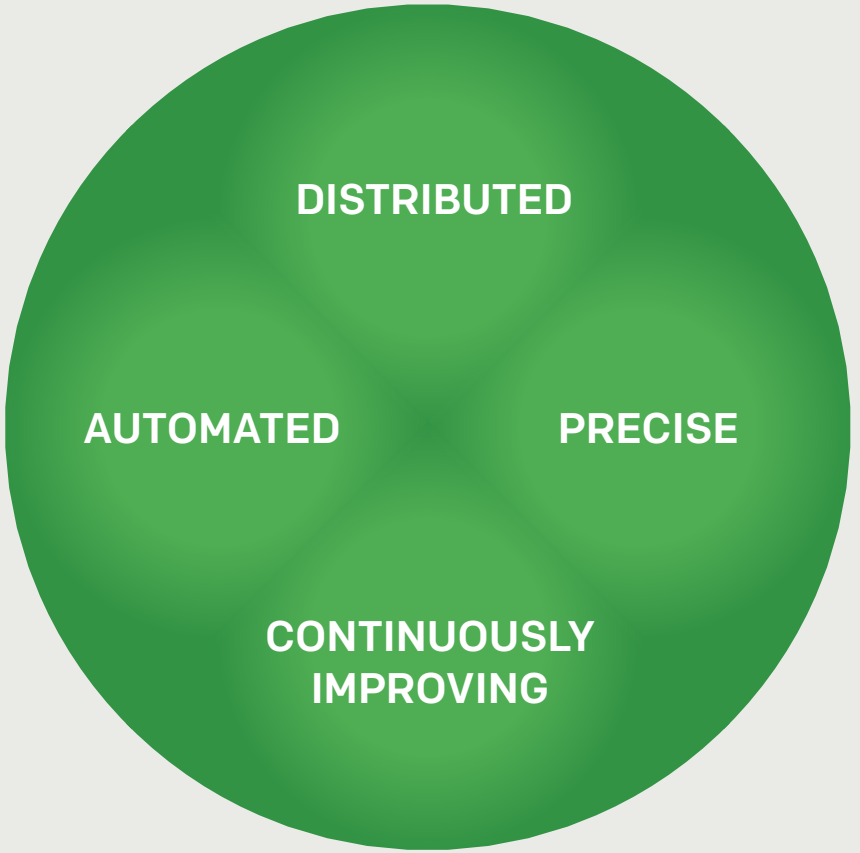
There are four defining characteristics of modern incident response:

It's automated. Manual processes executed by time-pressed responders are both inefficient and error-prone. Automation drives to faster responses that are the same every time, and leaves more time for responders to focus on resolution.

It's precise. Rather than mobilizing 20 or 30 responders and hoping that someone will have the right knowledge, we want to equip organizations to bring in the right responders. Not only are the right people involved, but they can work more efficiently within a smaller response.

It's distributed. A centralized one-size-fits-all command and control approach is inflexible, and also slow to evolve. We empower teams to orchestrate the right response for their incidents, as they are closest to the problems that affect them.

Lastly, it's continuously improving. With accelerating rate of change, there are always new failure modes being introduced -- which means we need tools and techniques to learn from, and prevent, every kind of incident that we experience.



Own the Incident Response Process

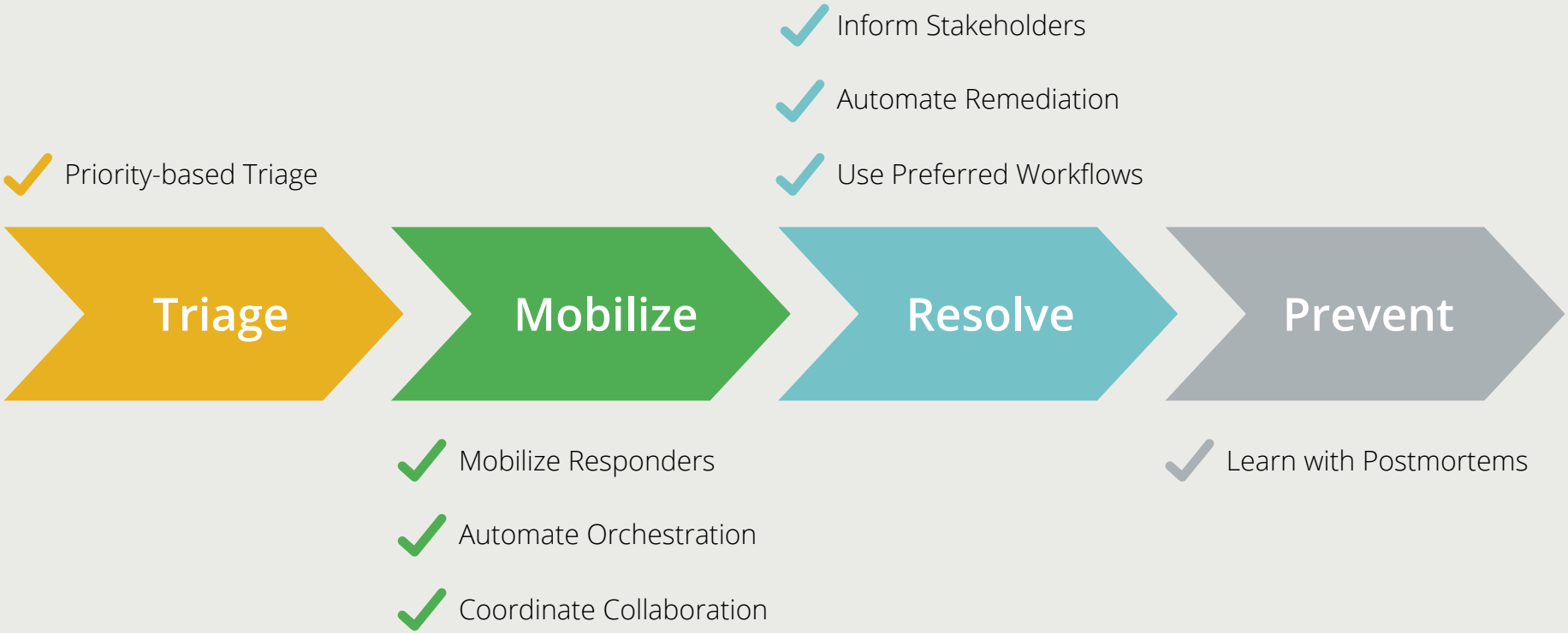
Now that we've discussed the primary characteristics of what mature incident response looks like, let's dive deeper into the processes themselves. Many organizations assign the role of establishing and refining the incident resolution process to one person or team. At PagerDuty, we benefit from working directly with our customers — some of the most mature digital operations teams in the world. Whether you choose to call it "insights engineering" or SRE (site reliability engineering), or simply, "major incident management," the first crucial step is answering this question: what is an incident to your product or service?

What is an incident?
Distinguishing from day-to-day operational maintenance issues and customer-impacting incidents can be difficult, which is exactly why this assessment is best performed by the individual teams in their area of the product. Giving those teams a framework for triage decisions (P1 through P5, SEV-1 through SEV-3, or whatever levels your organization uses) is fundamental to establishing common ground during a firefight. This capability in PagerDuty now helps everyone distinguish major incidents from other minor operational or untriaged issues.

2. How do you respond to an incident?
The next step is establishing how your organization responds to incidents. If you can define clear roles for individuals involved in the response, this goes a long way in ensuring an effective process. Once again, PagerDuty's open-sourced incident response documentation is a great resource for what we commonly see in operationally mature organizations, and what PagerDuty uses ourselves. We practice the response process regularly, including during our Failure Fridays.

3. Own the Tools
The third and final step is also likely the biggest challenge: driving consistency of your response process at scale, while still giving flexibility within that framework for individual teams to do what's best for their incidents. This is why we frequently see incident management process owners build or manage the tools they want the organization to use. In this area, PagerDuty aims to make organizational adoption of your process much easier in two ways: through automation and simplification.

The Incident Response Lifecycle



Here's a look at the four phases of the incident lifecycle, and some best practices that align with each stage to optimize the response process. We'll also share how PagerDuty Modern Incident Response capabilities drive automation at each phase of this lifecycle, to power faster resolution and accelerate learning from major business-impacting issues. These capabilities help you prioritize major incidents over other day-to-day operational issues, and easily adopt best practices to streamline incident resolution and learning in your organization.

IBM **Cloud**

"PagerDuty really helps us automate our IM processes."

Triage | Mobilize | Resolve | Prevent

Triage

All incidents, big or small, start out in this phase. This is where a single responder looks at an issue, and determines whether it's a known issue that has a simple resolution, or if the customer or business impact is broad and needs a more concerted effort to resolve.

With PagerDuty, responders can quickly diagnose local vs. global impact as relevant alerts and context are intelligently grouped into a single incident. And as incidents are tagged by priority (i.e. P1, P2, P3, etc.), responders can easily and transparently communicate that to others.

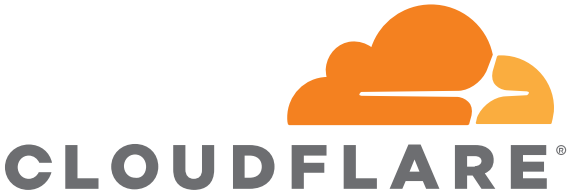
"We now have a way of sending the right alerts to the right people, and at the right time."

Triage | Mobilize | Resolve | Prevent

Mobilize

Once a responder has assessed and understands the priority of an incident, he or she needs to add additional responders to coordinate a resolution. PagerDuty supports the ability to pre-configure Response Plays, which are predefined sets of actions that can be executed automatically during wartime.

For instance, for a certain type of incident, you can define exactly which technical responders need to be recruited (by name or by schedule/escalation policy), and what status updates to send to business stakeholders. All of these actions can then be simultaneously executed either automatically for new incidents, or with the tap of a button from the PagerDuty mobile app during triage. This accelerates the process around previously complex, cross-team mobilization from hours to minutes or even seconds.



"Mean-time-to-action has dropped from multiple minutes to seconds."

Respond

A big part of the equation is engaging the right individuals required for the incident at hand, but it's also essential to empower them to collaborate using the tools and workflows of their choice (such as conferencing, ticketing, chat, etc.) . This enables faster resolution, so it's key that your incident response solution is highly extensible. Additionally, part of the Response Plays capability is the automation of stakeholder communication with other teams such as support, PR, and executives, to orchestrate proactive business-wide alignment and customer & partner responses.

You can also quickly troubleshoot, remediate, or restore service with Custom Incident Actions. This capability allows users to create buttons directly within the incident to execute custom logic housed in other systems, such as reverting a code deploy, restarting a service, running diagnostics, and much more.

BULLETPROOF
MISSION CRITICAL CLOUD

"Our key SLA to our customers is human response time. PagerDuty is the foundation for us to provide that."

paylocity

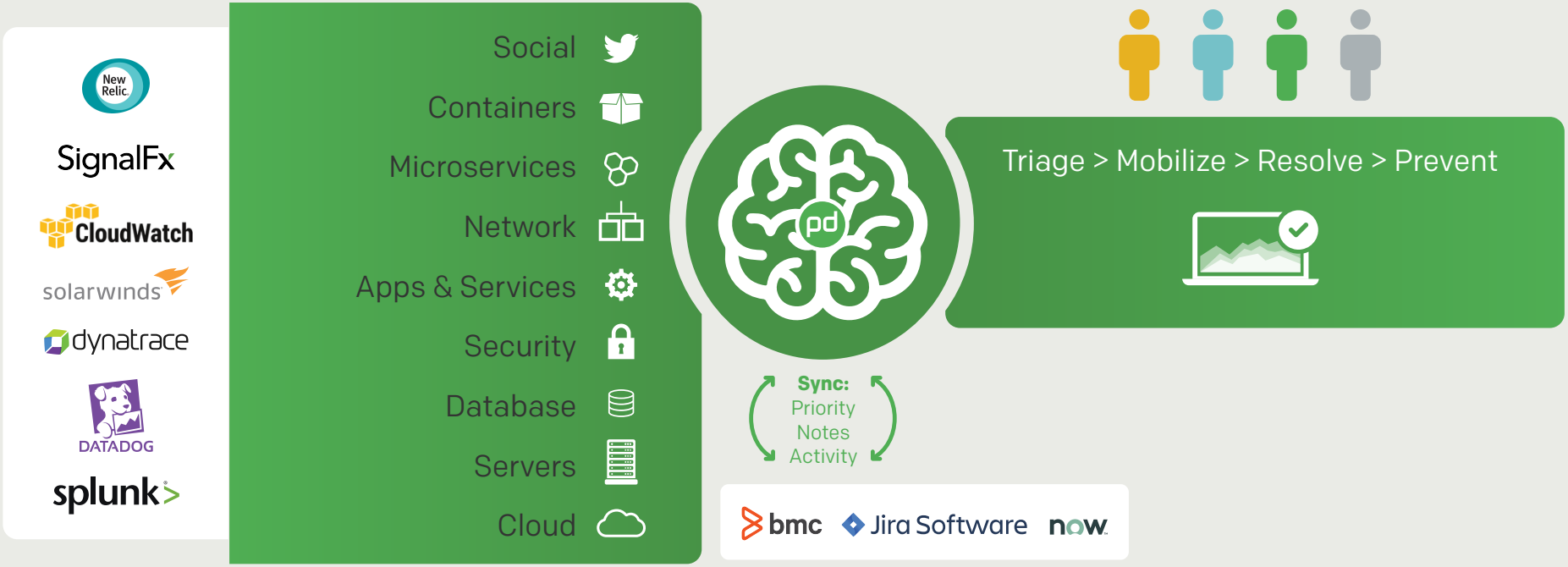
"PagerDuty helps us reach a new level of operational maturity...we are keeping a more accurate timeline and notes in the same product instead of having a lot of disparate places for this information."

Learn

After the incident is resolved, postmortems are the final essential stage of the incident process, by facilitating learning from the end-to-end response. Postmortems are critical for reducing the impact and occurrence of incidents, and promote a positive culture around frequent and iterative improvement of both service quality as well as the incident response process itself.

PagerDuty incident postmortems help teams greatly simplify the act of reviewing and learning from a major incident. The postmortem tool allows you to build chronological incident timelines in minutes rather than hours, by allowing you to point and click to easily pull in incident activity, relevant information from chat tools, and other types of data that are important when learning from an incident. The postmortem tool provides a customizable template that includes an overview of the incident, how it was resolved, root cause, customer impact, what went well and what didn't, and action items. Alongside the timeline, teams can include custom data from github, incident activity, and more to give full end-to-end visibility into the incident. This initiates the conversation on how to learn from past incidents and improve as an organization.

Integrate Your Toolchain



If you are using an ITSM or ticketing solution such as ServiceNow or JIRA software (see all of our integrations), PagerDuty supports bi-directional integrations. In addition to eliminating duplicate tracking effort by responders or incident managers, this also brings PagerDuty's incident response capabilities to ITSM tickets. ITSM tools are not designed for real-time incident response, and PagerDuty's seamless integration brings this critical capability to your existing ticketing infrastructure.

pagerduty

Putting It All into Action

As the leader in digital operations management, PagerDuty helps you scale both your on-call process and your incident resolution process, no matter where you are in your operational maturity. Our mission is to give your organization a pathway to improving your incident response process to keep up with the rapid pace of change and complexity, so that your teams can collectively mitigate customer impact of business disruptions and deliver great customer experiences. Make every second count and elevate work to the outcomes that matter, by connecting the right teams to problems and opportunities in real-time.

Why wait? Supercharge your incident response today by signing up for a free 14-day trial of PagerDuty.

SIGN UP NOW