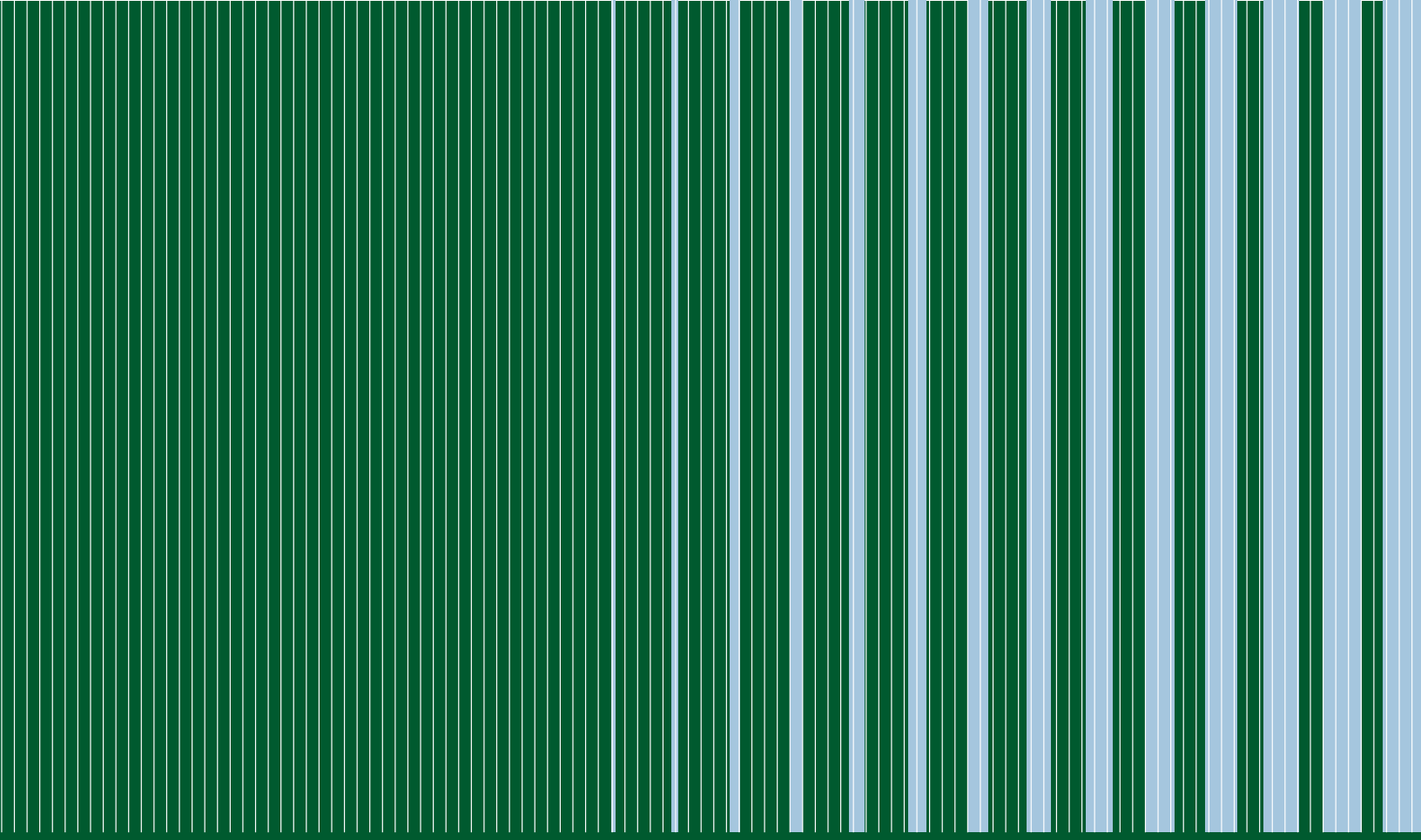


PagerDuty

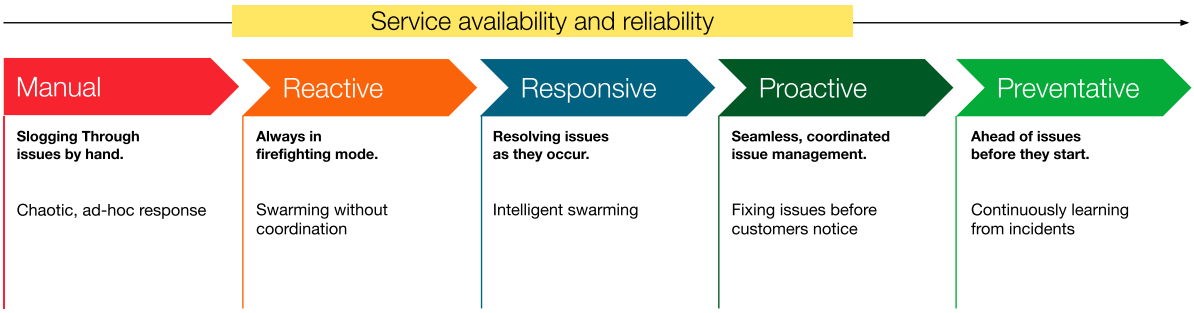
The definitive guide to incident response

Table of contents

The need for better incident response

Times have changed. We're all getting asked to do more with less: How can we become more efficient? How can we automate more often? Meanwhile, we're more distributed than ever - working from home, from a local coffee shop, and, occasionally, from the office. This combination of hybrid work styles and digital transformation initiatives heavily reliant on the cloud continues to add more layers of complexity. To cope, organizations need to focus on building more efficiency and resilience into their processes and operational practices. One approach that organizations can take to do this by investing in improving their digital operations maturity.

PagerDuty operational maturity model: incident response



Moving the needle from manual methods of incident response to adopting a more preventative posture is no small task. It requires internal buy-in, tool and process reviews, and an emphasis on making work better for all people. By all people, we mean your responders, stakeholders, and customers. In this eBook, we'll share what an automated incident response process looks like, best practices for achieving this, and PagerDuty capabilities you can leverage to codify those best practices.

Defining characteristics of manual vs automated incident response

From our platform data, we can see what the modern responder is up against. And burnout is top of mind. According to the State of Digital Operations Report 2022, "54% of responders are being interrupted outside of normal working hours." These interruptions lead to exhausted teams who are continuously firefighting rather than resting or innovating. It slows companies down and forces organizations to invest even more resources in recruiting, hiring, and training new employees. And these new employees take time to onboard, meaning the retained team members are under even more pressure to perform with less support. This is why the difference between manual and automated ways of incident response is so stark.

The manual way involves interrupting humans from whatever they're doing and asking them to find the root cause of an incident all by themselves. They take action only after they've come up to speed, and those actions are often toilsome and repetitive. Even if the right person is resolving the problem, the incident takes longer to close than it should. The right humans at the right time are no longer enough.

Automated incident response is about preventing humans from being the first line of defense. It introduces ways to leverage machines to shoulder some of the burden and help humans balance critical workloads. And it works in real-time or on-demand to address a multitude of use cases that you can right size based on what each team is ready for.

PagerDuty

Own the incident response process

Now that we've discussed the primary characteristics of what automated incident response looks like, let's dive deeper into the processes behind the concept. One important part of improving incident response is understanding the process from an organizational standpoint and codifying key points. Teams need guidance on what the golden standard of incident response looks like within a company. And, since many high priority incidents today require multiple teams to work together, the organization needs to align on what the business' response to incidents looks like. Here are three places to begin:

1. 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 (Priority 1-5, Severity 0-3, or whatever levels your organization uses) is fundamental to establishing common ground during a firefight.

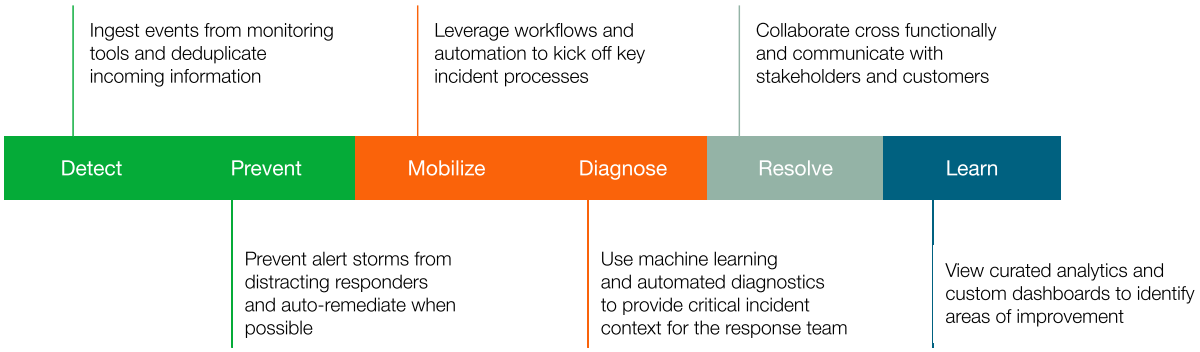
2. Who does what during an incident?

The next step is establishing who does what during an incident. If you can define clear roles for individuals involved in the response, this goes a long way in ensuring an effective process. You can even determine necessary roles by incident priority. For instance, you can stipulate that for P1 or P2 incidents, you need a dedicated incident commander, but for P3 or P4, the responder who acknowledges the incident can fill that role. For more information on incident response roles and responsibilities, you can visit our Ops Guide.

3. Own the tools

Automated incident response requires a toolkit. This toolkit contains a combination of monitoring and observability tools, private and public cloud infrastructures, systems of record, CollabOps, and more. One key piece that cannot be overlooked is your incident response tool. This tool should act as a bridge that connects your people, tools, and processes for a seamless response process.

The incident response lifecycle



Here's a look at the six phases of the incident lifecycle. We'll break down what happens in each of these stages. We'll also share how PagerDuty's capabilities help you respond to incidents faster and more efficiently throughout the process while improving your operational maturity.

"PagerDuty gives us a call and ensures we never miss a critical issue."

Groww

Detect

Detection is the first phase of an incident, and it can take many forms. Ideally, your monitoring tools identify anomalous behavior and transmit the data to your first line responder. But incidents can be detected in other ways, as well. Sometimes this might be from your customer support agents who have been notified by customers of an issue. Other times, an incident might be detected internally by your technology teams.

However you detect an incident, it's key that the tool you use to orchestrate your incident response can take all the data you gather to create an incident. With PagerDuty, teams can use our over 700+ integrations to import data from a variety of tools. And, with our Customer Service Operations, support agents can be involved in the incident response process and even let incident response teams know when they're receiving complaints.

"The ability to reduce the noise and clear out alerts within the platform really frees up a lot of time for people on our SRE team to focus on higher-impact tasks."

CTC®
CHICAGO TRADING COMPANY®

Prevent

When an incident occurs, there's often more data than responders know what to do with. Alerts come in rapid-fire, creating what many call an alert storm. A responder is notified, and notified again, and notified further that something is wrong with the system. During this phase, it's important to avoid excessive noise so that the responder can concentrate on the important task at hand. And, it's also a great phase to deflect noise and unnecessary interruptions from humans entirely wherever possible. This could mean silencing transient alerts that typically autoresolve themselves. It could also be a perfect stage to introduce auto-remediation efforts so that humans don't have to do work that machines are capable of.

With PagerDuty, responders can leverage AIOps capabilities to curb alert storms and group all related alerts into one single incident. Teams can leverage machine learning to avoid interrupting responders with transient alerts. And sometimes a responder doesn't even need to be involved at all. With PagerDuty Process Automation, teams can leverage automation to attempt to resolve the incident without human intervention. This way, a responder is only required to remediate when absolutely necessary.

"Improved quality of life for our employees is a key benefit we've achieved by using PagerDuty. PagerDuty has made things a lot easier for the operational people who support our applications."

IG GROUP

Mobilize

Once it's clear that a human needs to take action, it's time to mobilize the response. This process is two-fold: you need the right people working on the incident, and you need the right processes in place to help them work as efficiently as possible. And, you need to do this with as little waste as possible, both in people's effort and time.

Teams can use PagerDuty to accomplish both these goals. With our service-based architecture, you always know who is responsible for the service that's experiencing an incident and you can loop them in seamlessly without needing to add extra people. Additionally, you can leverage incident workflows to kick off crucial processes, like spinning up an incident-specific CollabOps channel or conference bridge, adding responders based on priority, and more. These tailored workflows help teams codify their response efforts and create replicable success across an organization.

"We've not only lowered execution times, but we've democratized that ability to anyone, not just those from the specialized skill set."

Diagnose

The right people are looking at the problem. They're following established processes and are ready to fix what's broken. But it's difficult to know where to begin, and it's toilsome to run routine diagnostics to fix it by yourself. In the diagnose phase of incident response, you need information quickly and with as little responder effort as possible.

That's where automated diagnostics and machine learning come in. With AIOps, teams can look at past and related incidents and use contextual information to help them resolve this incident faster. And, with automated diagnostics via PagerDuty Process Automation, teams are able to run diagnostics against any technical service and receive important data back, all with just one click of a button.

"With PagerDuty, we're able to engage the right people, on the right issues, at the right time. As a result, we've reduced the number of people needed to resolve major incidents by 25% in just two months."

SAP

Resolve

The resolution part of incident response is often the longest and most difficult. During this time, teams are working to bring the incident to a close. But in the background, there's more to it. The incident responders need to also communicate constantly with other teams, business stakeholders, and even with customers. It's important that the response team sets clear expectations with those who are depending on them. And that these updates are simple to give from a responder's point of view. Afterall, if a responder is constantly fielding questions, they're not able to resolve the incident as quickly.

PagerDuty helps teams work cross-functionally and communicate with stakeholders and customers. Our integrations with CollabOps tools such as Slack and Microsoft Teams enables everyone to work together on an incident. And, with Status Update Notification Templates, teams can leverage pre-written and reusable templates to share key information with other line of business teams. Last but not least, with PagerDuty Status Pages, responders can proactively update customers about incidents, preserving customer trust.

"PagerDuty helps us disseminate responsibility to specific engineers, giving clear ownership and transparency, and enables us to track what teams are working on and which incidents are still outstanding."

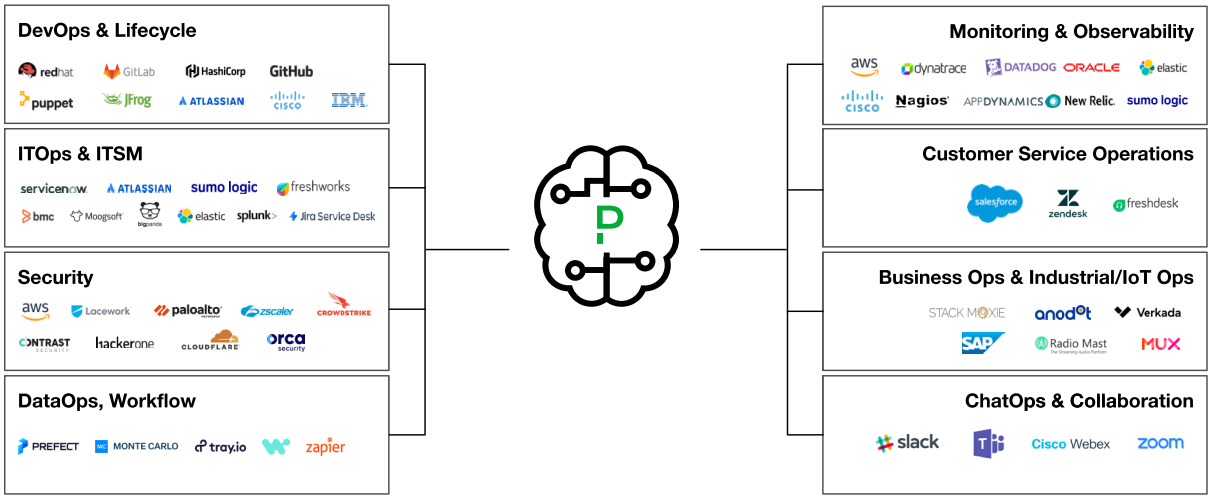
Learn

After an incident comes to a resolution, it's still not "over." Rather, this is a time for learning and reflection. By incorporating learnings back into the response process, teams are better able to respond to future incidents and prioritize improvements in processes and systems that will benefit the entire organization.

Learning goes beyond tools; it's an organizational commitment. That said, PagerDuty does provide data that can help you better understand your incidents and systems as a whole. With our analytics tool, teams can run customized reports that share responder data, noisy services, and more.

Integrate your toolchain

Platform for real time operations



PagerDuty helps organizations make the most of their tools by providing 700+ integrations. Any part of your incident response toolkit, from your CI/CD platform to your communication tools can be added into your workflow. You can work in the tools that you prefer with our bidirectional integrations and get the data you need to resolve problems faster without needing to context switch between a variety of interfaces.

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.

PagerDuty, Inc. (NYSE:PD) is a leader in digital operations management. In an always-on world, organizations of all sizes trust PagerDuty to help them deliver a better digital experience to their customers, every time. Teams use PagerDuty to identify issues and opportunities in real time and bring together the right people to fix problems faster and prevent them in the future. Notable customers include Cisco, DocuSign, Doordash, Electronic Arts, Genentech, Shopify, Zoom and more.

To learn more and try PagerDuty for free, visit www.pagerduty.com. Follow our blog and connect with us on Twitter, LinkedIn, YouTube and Facebook.

PagerDuty