Best Practices for Improving Incident Response Workflows

Mattermost

Is your team ready to respond to any incident?

Having an incident response plan in place is essential for any engineering organization. A plan helps keep every person, tool, and process involved in your incident response workflow working together cohesively. A well-managed incident response plan also helps your team use time effectively, save money, and keep customers happy. But oftentimes, incident response workflows are reactive, disorganized processes that move slower than what's required to effectively respond to security breaches and other critical incidents.

In this guide, we'll cover what software development and security teams need to know about building and improving high-performing incident response processes. You'll learn how to optimize your incident response processes for better time-to-resolution, from the essential steps to include in your incident response playbook to strategies for improving your existing processes.

PART 1

Anatomy of an incident response plan

Before we dive into the specifics of what an incident response plan should look like, it's helpful to understand the goals of your incident response plan. For most organizations, this includes:

- Alerting the team to an incident and kickoff response activities;
- Communicating with internal and external stakeholders about the incident and how it's being addressed;
- Resolving the incident;
- Fulfilling regulatory and contractual requirements for breach notifications; and
- Improving your response processes for the next time an incident occurs.

You should customize your incident response plan to fit your team, tools, and workflows. But well-crafted incident response plans have a few key elements in common, so it's good to start with a strong foundation and then tweak your processes to fit your needs. For each stage in this section, we've provided a checklist with a few key steps to get you started. Use these as a starting point to build your custom incident response plan.

Stage 0: Alerting

When an incident occurs, your organization needs measures in place to capture and relay the event information to responders. This can be achieved through monitoring, logging, and tracing.

To reduce the delay between the incident and the first response, these observability metrics should be coupled with your team's preferred communication channels, such as push notifications, chat messages, or emails.

Getting the right people looped into incident response as fast as possible is crucial and can mean the difference between a swift, effective response and a slow, disorganized one. Creating a centralized communication channel for stakeholders will keep collaboration streamlined and prevent miscommunication.

Alerting Checklist

- ☐ Create an incident ticket
- ☐ Create a centralized communication channel
- ☐ Run your incident response playbook

Stage 1: Triage

When an incident is alerted, your team needs to kick off the response process quickly and effectively. This stage can feel the most disorganized because there are often many unknowns. What exactly happened? Are customers impacted? How do we fix it? This uncertainty is why a clear process and documentation for the team to follow is so critical to rapid resolution.

Prior to any communication to the larger team or customers about the incident, you'll need to ensure you understand the context of the situation. At this stage, include a few core questions in your incident response playbook to help contextualize the situation and provide your team with the information they need to communicate effectively.

- Who or what was impacted by the breach or outage?
- What type of information (if any) was compromised?
- What mitigation measures are we currently taking to address the situation?
- What criteria must be met to consider the incident resolved?

When communicating to stakeholders both within the organization and outside of it, consistent and clear messaging is important. Some organizations have a dedicated outage landing page that gives users a single source of truth to reference during outages and other incidents. In other cases, organizations opt to reach out directly to customers individually or as a group. Pre-written email templates that can be quickly customized and sent may be a useful addition to your incident response prep materials.

Triage Checklist

- ☐ Notify key stakeholders
- ☐ Communicate with customers
- ☐ Define exit criteria

Henry
@here Here's the situation...

Stage 2: Investigate

Now that you have all the pieces in place, it's time to investigate the source of the incident. Keeping your investigation process streamlined requires continual communication and alignment — all the more reason to use those centralized communication channels you established earlier. This centralization also ensures that any additional members of the team who join in the process after it's already underway can quickly get the context they need to get up to speed.

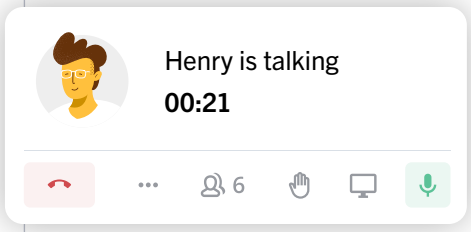
Integration between systems is crucial in this stage; it allows for better transparency as you investigate the issue. Consolidating fragmented information from different tools in your team's workflow in a single channel lets everyone keep track of what's going on without

wasting valuable time switching between tools. This consolidation will also help you create a comprehensive incident timeline, which will become an important resource for stakeholders — especially during the retrospective phase.

As you work to understand and resolve the incident, you may need to communicate updates to stakeholders. Be sure to set and stick to specific timelines for communication. For example, essential stakeholders, such as the CEO, will probably need their first update within 24 hours of identifying a breach. Establishing a regular cadence of check-ins throughout the incident response process — even if the status update is simply "we're still working on it!" — goes a long way in helping assure stakeholders that the incident is under control.

Investigation Checklist

- ☐ Start a bridge call for real-time collaboration
- ☐ Add suspected causes to a shared document and check them off if eliminated
- ☐ Communicate additional updates



Stage 3: Resolution

You've resolved the issue and can breathe a collective sigh of relief. But the job isn't done yet. Make sure that all team members have the right information to communicate the situation.

Your incident playbook should have clear action items for team members to do during and after an incident occurs, with all the information and resources they need to complete those tasks. Be sure to take note of which action items depend on others. For example, perhaps your sales team is responsible for emailing customers about the incident. In that case, they may need an FAQ document or after-action report from the support manager before they can do so.

Resolution Checklist

- ☐ Resolve the incident
- ☐ Communicate resolution to stakeholders
- ☐ Include clear guidelines for downstream communication

Stage 4: Retrospective

The incident is resolved, stakeholders have been informed, and you're in the home stretch. Now, it's time to slow down, take a look back at what happened, and iterate your processes for the next time.

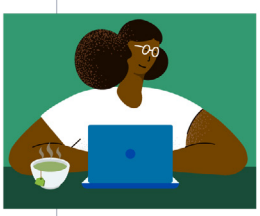
Don't forget to assign the specific people responsible for organizing the retrospective and enacting changes to the process! It's easy to overlook these tasks when everyone feels that the incident is over. Assigning clear owners will ensure that every last task gets wrapped up nicely.

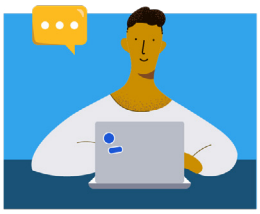
Bring together the people involved in resolving and communicating the incident to discuss your response. Identify what you did well and what can be improved before the next incident occurs.

At last, you've reached the final step: updating your playbook for next time. Lessons learned don't help if they aren't documented and integrated into your processes moving forward.

Retrospective Checklist

- ☐ Hold a retrospective
- ☐ Update your incident playbook
- ☐ Export data for a compliance review if required





PART 2

The best incident response software for your toolkit

You likely already have many of the tools you'll need for incident response as part of your organization's tool stack. The key is understanding the role they play in your processes — and knowing how to bring them together effectively.

Alerting tool

Why It's Important: You need tools that trigger response activities. Alerting tools notify on-call engineers when an incident happens, ensuring that the right people are informed quickly. They can also help your team keep track of escalation paths and manage notifications throughout the response process.

Process documentation/runbook

Why It's Important: The best incident response process is worthless if your team can't reference it quickly and effectively. Incident management software that codifies processes and keeps the next steps in front of the team is essential to any incident response stack.

Playbooks that are integrated into the tools your team already uses for normal daily operations and communications are ideal because they let the team seamlessly switch into incident response workflows without having to leave their workspace.

Observability, monitoring, and tracking tools

Why It's Important: Insight into what's going on across disparate systems is critical to resolving incidents quickly. Integrating different sources of data ensures your team has all the information they need at their fingertips without having to dig through a dozen different tools.

Ticketing/issue tracking system

Why It's Important: Incidents may start (or gain context) with issues flagged by customers. Visibility into issues can help you understand what's going on and know who to follow up with afterward.

Communication and collaboration tools

Why It's Important: Internal and external comms can quickly get confusing; having clear channels for internal communication keeps the team aligned and prevents sidebars that can silo key information away from the main group.

Don't forget about external communication, either! If your organization uses marketing automation or email software to communicate with customers, knowing who within the organization can send emails (and what the process is for doing so) will streamline communications when time is of the essence.

Enterprise development tools

Why It's Important: While not exclusively incident response tools, the systems you use to build, ship, and manage software should be taken into account as you develop your incident response plan. They may be critical to supporting the infrastructure of the organization implementing incident resolution.

Integrating these tools into your collaboration environment will allow first responders and stakeholders to find the information they need from these tools during a mission-critical issue.

PART 3

What teams get wrong about incident response

Building a robust incident response plan is much easier when you're aware of the common mistakes teams make, which we'll examine in this section.

A reactive approach to incident response

When an incident happens, teams need to act *now*. But while the *when* of incidents is variable and unpredictable, *how* you react to them shouldn't be. Reactive, bespoke responses to incidents breed chaos and confusion, and the team can spend more time figuring out how to stay aligned on the next steps than they do addressing the incident.

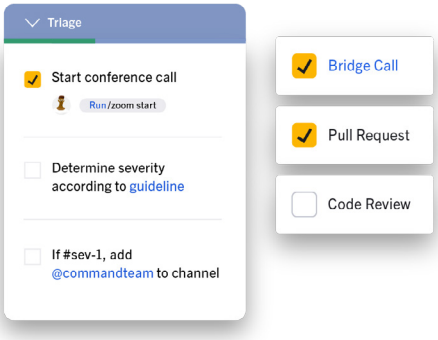
Teams that respond to incidents effectively have well-documented incident response plans ready to go when needed. They may need to tweak their actions to fit the specifics of a given situation, but they aren't building a process from scratch on the fly.

For better incident response, introduce a little chaos

Practicing chaos engineering can be an effective way to proactively improve the resilience of your systems. The engineering team at Netflix uses Chaos Monkey, an open source tool that randomly terminates virtual machine instances and containers that run inside of the production environment. By forcing the engineering team to confront failure more frequently, they are better prepared to react to actual incidents and have greater incentives to build more resilient systems from the start.

Lack of organizational transparency

When information is hard to find, teams can lose critical time during a response. Waiting for someone to grant you access to a critical document, trying to hunt down the right dashboard, or attempting to gain access to the specific repo you need to address the issue shouldn't happen when you're dealing with an incident.



Lack of process iteration

When was the last time you made edits to your incident response playbook? As your team and tech stack evolves, the way you respond to incidents will, too. But updating documentation often takes a back seat to other tasks. Before you know it, your documentation is so outdated that your team doesn't use it — or worse, they introduce inconsistencies that create confusion and slow down response times.

That well-crafted incident response plan that you developed probably isn't perfect. And that's okay! But that's why teams should perform retros after each incident (and each fire drill) and evaluate whether the process needs to be tweaked.

Overly manual processes

Toil is a part of every team's work. But when minutes count, toil-ridden tasks cost your organization time and money. Every manual task is time-consuming and can introduce additional points of friction.

There's an advantage to automating repetitive tasks across many areas of your organization, but the benefits of automation are even more pronounced for time-sensitive workflows. Your response team should be using pre-made scripts, build pipelines, version rollback systems, and other automated workflows. Bad processes rely on one-off terminal commands, manual service management, and direct modifications to production systems.

PART 4

How to improve your incident response plan

So now that we know what *not* to do as you perfect your incident response plan, what should your team do to continue to optimize how you respond to incidents?

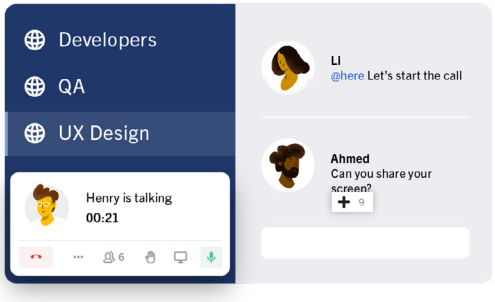
Unify tooling to increase visibility

Keeping information discoverable is key to fast, effective incident response. But every team is using multiple tools to build, manage, and monitor software, so finding a way to bring siloed information together into a single, unified dashboard is critical.

Prioritize internal communication and alignment

The top priority during any incident is to fix what's broken, breached, or buggy. But while the technical resolution of the issue is essential, the communication around the incident is just as important to business outcomes during and after the incident.

Make clear communication with internal stakeholders part of your incident response processes, which will then turn into clear external communication.



Is your incident response plan vacation-ready?

We know that assigning clear owners for tasks is important. As Finagle's law tells us, "Anything that can go wrong, will — at the worst possible moment." So what happens when the SRE responsible for communicating to the sales team happens to be on a flight or the support engineer who runs the retrospective is on maternity leave? Be sure to assign backup owners for critical tasks so your team is prepared for incidents no matter what.

Practice makes perfect

Going through "dry runs" of incidents gives your team a chance to work through the processes, handoffs, and next steps when the stakes aren't as high as a real-world incident.

As Zendesk CISO Maarten Van Horenbeeck said during a talk on running well-managed incident responses:

> "I found it to be incredibly valuable to do these little tabletops where I just take an hour of time and I come up with a scenario, I put some key leaders around the table and we talk through a security incident and they have to make decisions. Even if they don't make the right decision in the scenario, the next time a real incident strikes you can talk to each other about 'Do you remember how we did this in the exercise? You made this decision and it worked out, or it didn't work out?' It's a really valuable time to learn."

Implementing chaos engineering, which we mentioned in the last section, can also help your team build more resilient systems by surfacing scenarios that you might not have considered during planned practice runs.

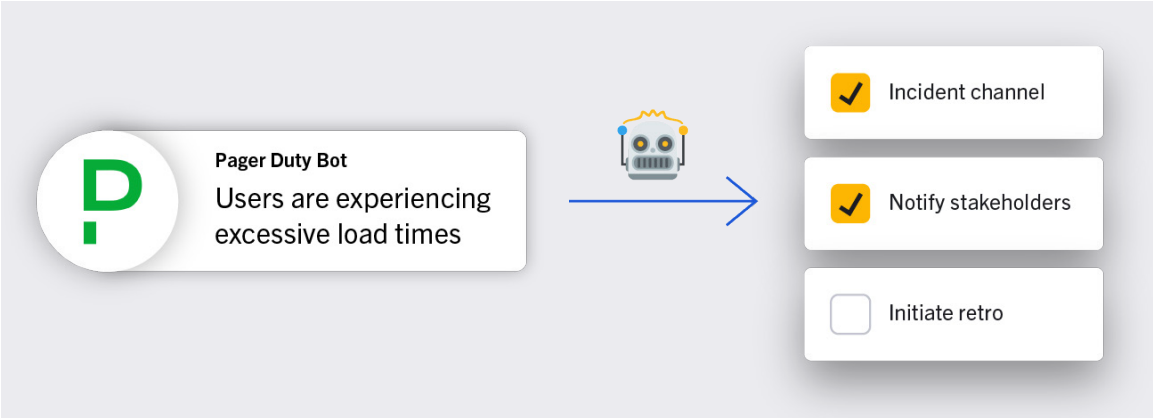
Make sure not to skip the retrospective stage of these fire drills. Practice incident runs are a great opportunity to refine your processes and spot potential issues with your playbook, but it's important to give the team space to reflect and discuss the run to find those issues and iterate your processes.

Lean into workflow automation

It's time to address those overly manual processes. Automating repetitive actions can help streamline incident response times, increase information visibility, and ensure your team stays focused on what matters most.

Some incident resolution workflows to consider automating include:

- Sending notifications to stakeholders when you hit certain milestones/stages;
- Creating a dedicated communication channel when the response process is initiated and adding key team members;
- Pulling in data from different tools into a central location; and
- Kicking off an asynchronous retrospective once the incident is marked as resolved.



PART 5

Final thoughts on incident management best practices

Incident management is critical for every organization. But getting it right can be challenging. We hope this guide has helped you reflect on and refine your incident management practices and that you now understand how to optimize your processes for better incident response in the future.

Essential Takeaways for Improving Incident Response

Know Who's Who: Assigning clear owners to each and every action item ensures that nothing slips through the cracks and everyone knows who's responsible for what.

Keep Everything Together: Integrating systems, centralizing key documents and communication, and keeping process documentation where your team can reference it quickly helps keep the team aligned as they collaborate to resolve the incident.

Learn from Every Incident: Use every incident as an opportunity to improve your processes and respond more effectively next time.

Build Your Incident Response Playbook in Mattermost

Ready to build an incident response playbook for yourself — or want to see how using Mattermost Playbooks can help you supercharge your existing incident response playbook? Start a free trial of Mattermost then check out this tutorial on using Mattermost for incident response to learn more.

Mattermost

Mattermost.com

🎉 9