pagerduty

Overcoming Alert Fatigue in a Modern Ops Environment.

4 Steps to Better Incident Management

Key Takeaways

01

When your monitoring systems generate too many alerts that require your attention, your organization starts to suffer from alert fatigue.

02

Alert fatigue can be detrimental to a modern operations environment, causing service degradations as teams miss critical notifications.

03

The financial cost of alert fatigue can be great due to the toll it takes on your employees and ultimately your business.

04

There are steps you can take to prevent alert fatigue, including eliminating unnecessary alerts, optimizing alert priority levels, notifying the right people at the right time, and learning from your alert trends.

Alerts from monitoring systems and ticketing tools are a good thing, as they help IT Ops and DevOps teams track the health and performance of core apps and services, and enable responders to react quickly to incidents. But it's possible to have too much of a good thing, and alerts are no exception. When your monitoring systems generate too many issues that require your attention, your organization starts to suffer from the phenomenon known as alert fatigue.

When alert fatigue sets in, operational environments suffer, impacting the services you deliver to employees and customers. Teams become desensitized to alerts, which can cause them to miss critical notifications.

This whitepaper explains why alert fatigue is so detrimental to a modern operations environment and how organizations can avoid alert fatigue by integrating their monitoring systems with a centralized incident management system.

alert **fatigue**

what it is, and what causes it

The basic definition of alert fatigue is simple: When the frequency of alerts exceeds the ability of the operators to effectively triage those alerts, IT Operations' workflows break down, and alerts are missed. It becomes harder and harder to find the real signals in the noise, and consequently, responders can become desensitized to them.

Alert fatigue comes in different forms and can result from several types of problems — or a combination of them.

The most common culprits include:

- **Having multiple monitoring systems within an organization**
- **Having a monitoring system that simply generated too many unnecessary alarms**
- **Alerts being sent to the wrong people**
- **Alerts being sent to more people than necessary**
- **Failing to differentiate between critical and non-critical alerts**

Understanding that alert fatigue can have multiple causes is important, as it's not simply an inevitable result of having too much to monitor. Even with a large and active infrastructure to keep tabs on, alert workflows can be tailored in such a way that your team can handle a high volume of alerts effectively.

Improper management and triaging of alerts — not the sheer quantity of notifications — is the root cause of alert fatigue. Preventing alert fatigue is as simple as having the right management strategy in place.

The Cost of alert fatigue

If your IT team fails to respond to alerts, the consequences can add up quickly. For example, a storage bucket in the cloud that is starting to run out of space over a holiday weekend can be brought under control easily, before customers notice a disruption, if admins receive an alert about the problem in time and act upon it by adding more space. However, if the issue goes unnoticed because they missed the alert, the business's reputation suffers, ultimately leading to lost revenue.

That's only the tip of the iceberg when it comes to the fallout of alert fatigue. When you throw factors such as contractual obligations and your organization's reputation into the mix, many additional problems can result.

Contractual liability

If a specified level of performance is written into a contract, excessive downtime or failure of services may trigger automatic financial penalties. If your client is in a highly time-sensitive business where prompt performance is crucial, or a field in which public safety is at stake, legal and financial penalties may be even more severe. That's bad news for both you and your customers.

Loss of users or customers

For your software to be successful, it not only has to work, it must be available when your clients need it, whenever that may be. If you have too much downtime or loss of functionality, your customers will eventually start to look for a replacement solution. This is as true of software designed for use by the general public, as it is for services provided under contract. For instance, an online store that isn't available when people want to make purchases is going to lose customers to a competitor that is live and available.

Loss of sales

When potential clients are considering buying your products or services, they generally want to know your track record—and with a bit of searching online, it won't take long to uncover any legal problems, reliability issues, lost contracts, or what people are saying about you.

Good morale makes for effective teams

Alert fatigue also has a steep cost in terms of employee satisfaction and your ability to recruit the best talent — an ever-present challenge in today's competitive IT labor market. That's because on-call engineers who find themselves buried in an avalanche of alerts are unlikely to be satisfied with their jobs. They will also experience high levels of stress and report a poor work/life balance if they are expected to respond to an unmanageable number of alerts at all hours of the day.

Loss of staff	Many people react to chronic stress by avoiding the source of that stress. If the stress is job-related, they're likely to look for another job. Once employee burnout reaches a certain level, you can't count on high pay, good benefits, or even a weak job market to keep them from leaving. You can replace the people who leave, of course, but you will need to recruit and train your replacements, which can be a costly and time-consuming task. Moreover, there's a good chance that you'll need to replace your new employees after they inevitably also become burned out if the problem of alert fatigue hasn't been addressed.
Increased sick time	Chronic stress can cause serious health problems. If your employees are in a state of ongoing alert fatigue, they're more likely to get sick, and they're more likely to call in sick even when they have minor health problems just to escape the stress.
Conflict and more problems	If your on-call teams are experiencing alert fatigue, then sooner or later they're likely to let others know what they're going through. If your customers complain about the quality of the service and support that your company is providing, management is going to be under pressure to "crack down" to fix the problem, which is a main ingredient in the classic recipe for endless (and needless) conflict that distracts from your business's main objective.
Poor use of staff time	Your on-call team's time is used most efficiently when employees are proactively working on planned projects, not responding to a series of unanticipated alarms. Since good admins are expensive, requiring them to spend too much of their time on unplanned work translates into a significant hit to your budget.

Reduce the noise

Alert fatigue can result in serious costs for your organization. Fortunately, with the right tools and process, reducing alert fatigue is possible. That doesn't mean turning off all your alerts; it simply requires making sure all your monitoring systems are sending the right issues, with the right urgency, to the right people, at the right time.

01

Eliminate unnecessary noise with proper design

Again, avoiding alert fatigue does not mean simply turning off all your alerts. You do, however, want to take steps to suppress the noise from alerts that do not need to notify — either because they are not critical enough to merit your responders' attention (you probably don't need an alert to say a new user has logged in for the first time), or they don't require action (for instance, you should log data about a backup cycle having completed successfully, but you don't need to be notified on that).

Reducing unnecessary alerts will require you to tweak your various monitoring systems and the endpoints they monitor. You can centralize this process by filtering notifications through a central hub, like PagerDuty, and tuning rules to suppress non-actionable alerts. If you have many monitoring systems, this is an efficient approach.

A central alert management platform also suppresses unnecessary alerts by recognizing which ones are redundant. If you have multiple monitoring systems generating notifications about the same event, you want your team looking at an incident where all the relevant events and alerts are aggregated, so you are not viewing each alert independently. Redundant alerts should be automatically de-duplicated, and related alerts should be consolidated into a single incident that represents a real issue requiring response. This saves time and energy during an outage by centralizing context, communication, and resolution streams.

02

Optimize priority levels

Some alerts are going to be more critical than others. If non-critical events generate crisis-level notifications, your team will suffer from alert fatigue and be less likely to notice the issues that truly require immediate attention.

To avoid this situation, ensure that the alerts your admins receive properly indicate the seriousness of the associated issues. A basic approach is to categorize alerts by their severity or priority levels (for instance, SEV-1 through 5 where SEV-1 is critical and SEV-5 is non-critical).

You can achieve this optimization to a certain extent by configuring the way your various monitoring systems flag notifications. Since different monitoring platforms employ different classification systems for alert severity, and because the type of alert that one monitoring system deems critical might be treated less seriously by another platform, you can save a lot of time by forwarding alerts to a centralized incident management solution like PagerDuty to establish alert priorities. This not only consolidates notifications and alert priorities, it helps standardize your incident management.

This approach also saves your admins the trouble of having to learn different interfaces and configuration formats and schemas for setting alert priority levels on various underlying monitoring systems. You can automatically route or action alerts to adhere to the desired behaviors (such as suppress), with predefined rules. It also optimizes communication within your organization by obviating the need for different departments to rely on different incident management systems. A centralized incident management system ensures that everyone speaks the same language, even if they don't all have the same familiarity with various monitoring infrastructure tools.

"A centralized incident management system ensures that everyone speaks the same language."

03

Send the right alerts to the right people

Unless you have a very small IT team, you probably don't want every notification to go to every member. Instead, you want alerts about a networking problem to reach only the networking admins, to save their colleagues from unnecessary notifications. Security notifications should only reach the security team (and must be locked down so no one else can see them), and so on.

To reduce employee stress, you should also take steps to assure that off-duty admins do not receive alerts unless it is essential. Doing this requires an incident management system that is sophisticated enough to know who is working at a given time, and can decide when an issue is so critical that it should be escalated based on set parameters.

Because you can't count on all monitoring platforms to have this level of sophistication — and it's inefficient and redundant to configure different underlying systems to do the same thing — the best way to manage how alerts are routed is to work through a centralized incident management system.

> **"Analyze the trends revealed by alert data to identify ways to improve your IT Operations."**

04

Learn from your alerts

The primary purpose of an incident management system is to help your team identify and fix problems quickly. In order to get the most from your alerts — and take steps that will help you reduce the number of incidents you have to manage over the long term — you should also analyze the trends revealed by alert data.

Data visualization interfaces and performance analysis tools, which come built into PagerDuty, let your organization derive another layer of value from its notification systems. By aggregating alert data from all of your monitoring systems and providing a user-friendly dashboard for interpreting that data, these tools assure that your alerts don't stop being useful once an incident has passed. Instead, you can examine alert data or see what's been suppressed after the fact to find ways to reduce response time for future incidents, see if there are ways to improve tuning, and identify the most effective strategies for improving your IT operations.

Plus, analyzing operational efficiency metrics in relation to alerts and incidents can help you to identify employees who are most affected or who are being overburdened, allowing you to ensure that they receive the support they need. It also lets you know which team members are doing a stand-out job in responding to issues, so that you can reward them and increase morale.

Better response delivers a better experience

When you apply the right techniques to eliminate alert fatigue, you won't simply solve a problem. You'll go much further by turning your response team into an immense, value-driving asset.

They'll respond quickly to incidents, and they'll have the remediation and contextual information they need to get to fix problems quickly. Your clients will appreciate the level of service you deliver as a result. And your IT Ops and DevOps teams will be happier because they can spend more time doing the work that is truly impactful, instead of being overwhelmed by alarms. In other words, your business performance will improve because you'll derive more value from the resources you already have in place.

You don't have to build a custom system for centralizing and making sense of your alerts. You don't need to update the legacy monitoring systems you may already have in place or spend tons of time tuning those filters. There's no need to hire more staff with expertise in new software. Instead, you can simply add PagerDuty on top of your existing environment and workflows to maximize the value of your current alert and monitoring systems. Your clients will thank you, your IT teams will thank you, and your business will grow.

Try PagerDuty Free for 14 Days