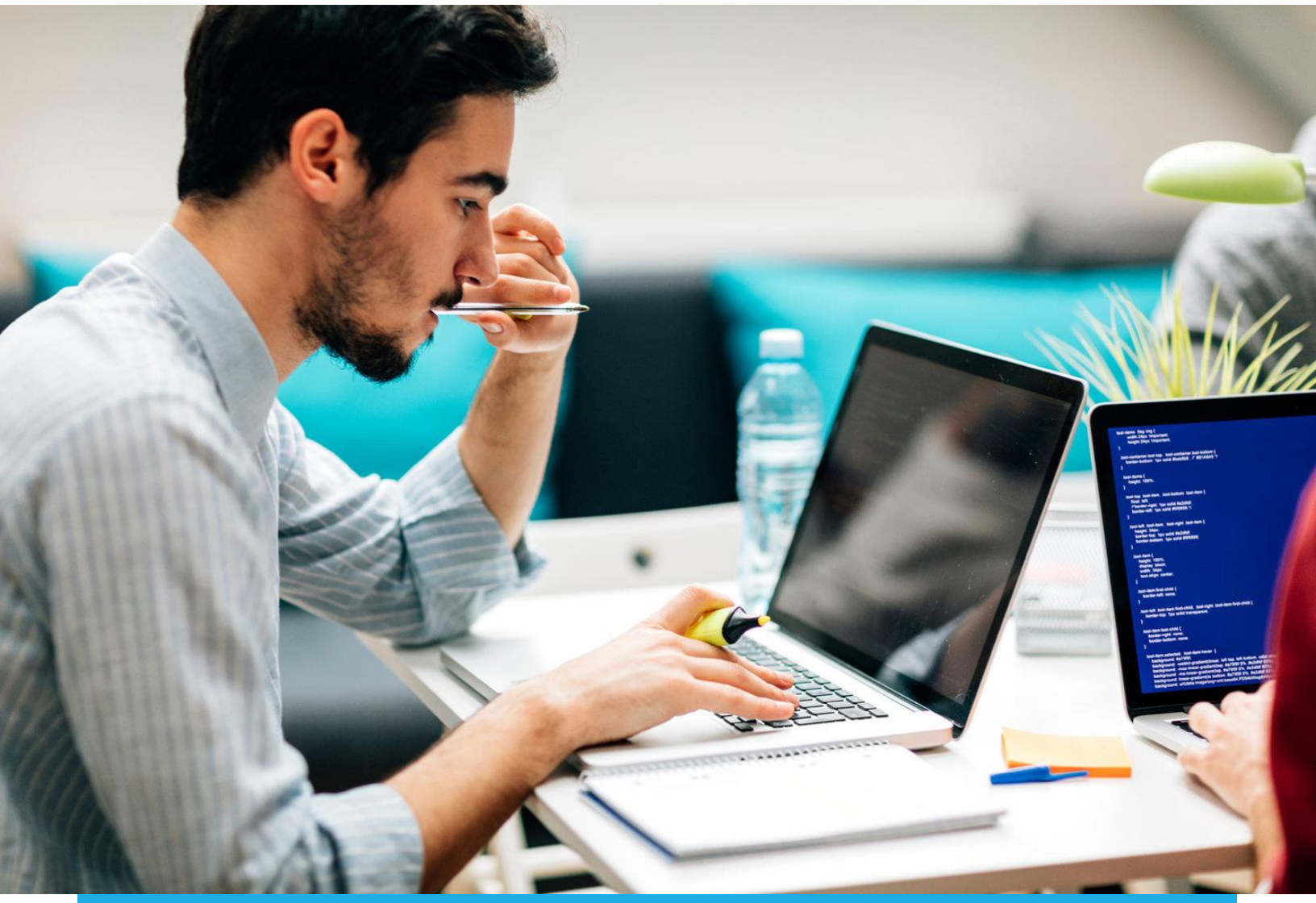
6 WAYS TO IMPROVE INCIDENT MANAGEMENT



THE ON-CALL MANIFESTO

THE 6 WAYS TO IMPROVE INCIDENT MANAGEMENT

INTRO

Effective incident management is concerned with deviations from, and threats to, the standard operation of services. During the course of time, even the best IT of department will experience incidents. How IT reacts to incidents is a key driver of MTTR (mean time to repair) as well as customer satisfaction.

Yet not all IT departments handle incidents similarly. The differences in how IT departments handle these situations account for why some IT teams are more successful than others. Some departments look at each incident as a way to learn how to improve for the future while others attempt to resolve each issue as quickly as possible and not look back.

The goal of this whitepaper is to provide IT departments with concrete suggestions on how they can improve their incident management process. What processes and procedures do teams need to adopt? What tools should they bring on board? Read on to learn more.

EXPERIMENT

The American philosopher John Dewey wrote:

Failure is instructive. The person who really thinks, learns quite as much from his failures as from his successes.

To that end, IT teams need to experiment with their incident management process to see what processes are effective and which are not. Experimentation and iteration are key to making on-call rotations better over time.[1] While this has become gospel for development teams[2], it also rings true for Ops and IT teams who can run simulations of outages to determine how to best manage downed servers, site latency or other similar situations. This practice is indeed the Simian Army[3] protocol at Netflix for managing chaos and it has been responsible for much of their DevOps success.

Experimentation also allows teams to track the usefulness of their alerts. Are parameters actually worth alerting on? Does the alert come with sufficient information to be useful? What actions should be taken when alerts occur to effectively manage the incident? By testing these assumptions in a simulated scenario, IT and Ops can become more effective.

For alerts that are truly actionable, you'll want to consider how easy it is for the on-call engineer to take the necessary actions. Every alert that fires should have a runbook that goes along with it. If an alert is so simple that automation can solve the issue then the alert probably does not require an incident alert. Instead, when the situation arises, an automated fix should resolve the issue.

---

[1] https://increment.com/on-call/crafting-sustainable-on-call-rotations/

[2] http://queue.acm.org/detail.cfm?id=2945077

[3] http://whatis.techtarget.com/definition/Simian-Army

Important questions to ask here are ones such as:

- WHEN WAS THE LAST TIME THIS ALERT FIRED?
- WHO RESPONDED TO IT LAST TIME?
- WHAT ACTION DID THEY END UP TAKING (IF ANY)?
- WHAT OTHER ALERTS TEND TO POP UP AT THE SAME TIME AS THIS ONE, AND ARE THEY RELATED?

The answer to these and similar questions should be recorded so that they can be used the next time a similar event occurs. This way, your IT team *learns* for the next time the event occurs. If the information is not recorded, it ends up living in people's brains and not becoming part of a living document which can inform teams in the future.

REDUCE NOISE

Quick detection of potential issues is the most important objective of monitoring and alerting. The difficulty consists of pursuing two conflicting goals: speed and accuracy.[4] In Target's epic 2013 data breach, staff in Bangalore, India, notified Target staff in Minneapolis that they detected an attack. However, no action was taken because these alerts were included with many other likely false alerts.[5] Target's IT, like many other tech departments, suffered from alert overload as 52% of alerts[6] were false positives. In the case of the 2013 hack, the Minneapolis-based team had become desensitized to actual alerts due to the overwhelming number of false ones.

Effective incident management is also about reducing the noise so IT teams know which alerts truly require a reaction at 2 a.m. too many events and alerts (false positives) will reduce the effectiveness of IT operations. You'll start to overlook important events or alerts[7]. Consequently, it is important to learn what the important statistics to keep track of are. Is it MySQL availability, aborted connections or error logs? Know which ones are important for your organization and alert on them.

USE SMARTPHONES TO INCREASE SPEED OF RESPONSE

The advantages of mobile incident management cannot be ignored. Installing an incident management app to your smartphone means having access to alert information and updates no matter where you are. Furthermore, if you have a specialized app designed for incident management, you will have the additional capabilities of rapid alerting, alert escalation and on-call scheduling. This makes it the ideal device with which to be notified of an issue around the clock.

Rapid alerting is also extremely important in minimizing the potential financial impact of an event. For example, Google calculated in 2012 that by slowing its search results by just four tenths of a second they could lose 8 million searches per day–meaning they'd serve up many millions fewer online adverts.[8] As such, if Google is seeing a delay in site speed then it needs to rapidly address the problem. Email is clearly not designed for rapid response. Smartphones are much more effective at achieving rapid response.

MAKE IT A TEAM EFFORT

[4] https://www.safaribooksonline.com/library/view/effective-monitoring-and/9781449333515/ch01.html

[5] http://www.csoonline.com/article/3191379/data-protection/false-positives-still-cause-alert-fatigue.html

[6] Same as 5

[7] http://www.top10bestnetworkmanagementsoftware.com/filtering-alerts-events-reducing-noice-false-positives/#

[8] https://www.fastcompany.com/1825005/how-one-second-could-cost-amazon-16-billion-sales

The pundits remind us that there's no "I" in *team*. Similarly, there's not "I" in *team effort.* Effective incident management requires bringing the whole team together to respond to incidents that arise. Collaboration is key.

Bringing on-call rotations to the team allows Dev, Ops and IT teams to see how well the product or set up they have created is working. No one in the IT family can simply create their perceived technical masterpiece and walk away. Instead, they need to take responsibility for their creation. Being part of the on-call family helps ensure this level of responsibility.

FOLLOW THE SUN

Follow the sun scheduling allows team managers to create multiple on-call schedules without limitation to location. Follow the sun scheduling works when a company has a large international team that spans several time zones. When an IT technician in Seattle is going to bed, a technician in Dublin is waking up.

By using an incident management application that allows IT teams to create schedules across time zones, teams can minimize alerts outside of business hours and certainly eliminate alerts during sleeping hours. The salubrious effects these sorts of changes can have on your team should not be minimized. A team that is well rested is better able to manage incidents and think of creative solutions.

USE ESCALATION AND REDUNDANCIES

Life is such that not every incident will receive an immediate response from the IT engineer on-call. He or she might be occupied with another task or momentarily unavailable. Consequently, it is necessary to have escalations as part of effective incident management. Escalations mean that the next person on call will be alerted when the primary engineer is unavailable. Effective incident management tools will enable escalations after a pre-defined period.

Additionally, it is important to enable multiple communication channels so that you have redundant alerts in case the primary smartphone-based app alerts are not heard. Using multiple redundant communication channels such as phone, SMS and text ensure recipients are notified in a timely manner.

TOOLS VS. AUTOMATION

Effective IT incident management requires effective use of tools. Most IT teams have an abundance of tools so having them is not as much of an issue as determining which ones are crucial in time of need.

If a task can be automated, then there is no reason an engineer needs to be alerted to the event. For example, if automated backups are available, then the IT team should bring on the technology and tools which enable this to happen. Enabling automation will mean that teams save money on man hours and avoid the potential for mistakes.

Engineers should really only be brought into work on a problem where their knowledge can add value. This is particularly true for issues picked up by monitoring and alerting tools. Indeed, effective identification of problems is the first step in successful incident management. [9] Effective alerting brings the need for incident management to the forefront.

The importance of an effective alerting tool cannot be overstated in terms of its importance for incident management. Effective alerting will allow IT teams to learn of an incident early in the process and manage the incident effectively while it is still a small fire and before it becomes an inferno. Effective alerting will enable IT to realize if an identified incident is low or high priority.

[9] https://ayehu.com/4-essential-steps-for-successful-incident-management/

CONCLUSION

Effective alerting enables the expediting of subsequent repair and recovery. Reporting enables teams to have a record of what they have achieved and bring that knowledge back into the virtuous cycle. Yet effective incident management begins with an understanding of the points outlined above.

To learn more about how effective incident management can help your team, contact OnPage.com

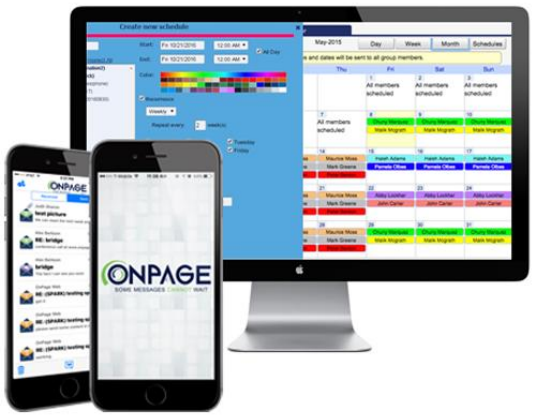
ABOUT ONPAGE

OnPage is a cloud-based, industry leading smartphone application for high-priority, real enterprise messaging. The OnPage application addresses the need for HIPAA compliant, incident response management and secure, time-sensitive messages.

OnPage takes mobile communications to the next level with the latest all-in-one app features. The web-based on-call scheduling tool enables enterprise users to plan ahead and route prioritized messages to the right person, at the right time, every time.

Thousands of healthcare providers, doctors, field engineers, law enforcement, nurses, emergency responders and disaster recovery teams depend on OnPage for rock solid reliability

TO LEARN MORE, VISIT OUR WEBSITE OR CALL: ONPAGE.COM/CONTACT-US 781-916-0040



DOWNLOAD THE ONPAGE APP

AND WE WILL CONTACT YOU TO

SCHEDULE A DEMO!

Download Now