ONPAGE | GUIDE

Six Ways to Reduce IT Alert Noise

OnPage Corporation Tel: 781-916-0040 www.onpage.com

IT teams must reduce alert noise—including false notifications and constant, non-urgent alerts—to improve productivity and efficiency.

IT monitoring tools send alerts when thresholds are passed. Unfortunately, these same thresholds are often responsible for excessive alert noise. Studies show that organizations waste an average of $1.27 million per year responding to false notifications[1].

Due to the excessive number of false notifications, it is common for IT teams to become complacent and unprepared for a real, urgent matter. Consequently, this leads to poor performance, hindering IT teams from meeting goals and satisfying stakeholder interests.

That is why teams need to focus on their monitoring tools, ensuring that noise is eliminated, and appropriate action is taken for urgent alert notifications.

The goal of this guide is to highlight best practices that IT teams can use to reduce monitoring noise and improve alerting effectiveness.

1 – Use Analytics to Learn Normal Behavior

Effective alerting is synonymous with effective monitoring. IT teams must keep an eye on relevant metrics, while also sending alerts on only actionable and urgent matters.

Effective alerting is based on the way monitoring is set up, calibrated and implemented. IT professionals need to ensure that an associated alerting platform matches the system's environment and workflow. Only then can critical events rise to the surface, with alerts that deliver valuable information without the noise[2].

Through error logs and aborted connections, IT teams need to consider and select which statistics or metrics they will closely monitor for effective alerting.

[1] https://www.fireeye.com/offers/stop-the-noise.html

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

2 – Create Actionable Alerts

IT teams need to create alerts that help minimize downtime and maximize productivity. To accomplish this, they need to:

- Receive alerts based on selected, urgent matters (e.g., high disk volume or IT infrastructure issues)
- Set up alerts so that they provide comprehensive information regarding a critical issue, ensuring that a team understands the event prior to taking appropriate action

By creating actionable alerts with detailed information, IT teams can positively impact their mean time to detection (MTTD) as well as mean time to resolution (MTTR).

3 – Send Alerts to the Right Team

Critical alerts need to be delivered to the appropriate individuals or groups. Notifications must be forwarded to qualified team members, guaranteeing that an issue is addressed and resolved quickly.

For instance, if a website is down due to a server overload, then a member of the team in charge of servers needs to be alerted. Additionally, group alerting through an incident alert management platform offers escalations and rotations, ensuring that the right on-call team member(s) receive the notification.

4 – Review Current Alert Monitoring

By reviewing one's monitoring systems, IT teams may find that they are duplicating alerts. These could be alerts that are left over from tests and that replicate the functionality of other alerts.

IT teams need to eliminate these alerts to minimize noise and enhance resolution-based performances.

5 – Bring in Priority Alerting (Low Versus High)

Not every alert is a high-priority incident that requires quick resolution during late night hours. Through a monitoring system's appropriate calibration and its integration with a powerful alerting platform, IT teams can receive distinguishable notifications for high and low-priority issues.

For instance, high-priority issues will provide different audible pings or different levels of persistence than those of lower priority events. Alerting should also be equipped with escalation so that if the first person receiving the alert is unable to answer, there is another team member who gets forwarded the critical, urgent notification.

Low-priority incidents should be calibrated so that they are not triggered outside of a certain time range. These are incidents that do not require urgent care and resolution—great news for overworked IT teams.

6 – Comprehensive Alerting Solutions

Effective alerting is as important as effective monitoring. An ideal and powerful alerting solution should come equipped with:

- Distinguishable alerts – Managers can send alerts to different team members based on severity and need
- Rich alerting – Alerts that provide contextual information with attachments (i.e., voice memos and images)
- Priority alerts – Distinguishable, high and low-priority notifications based on event urgency
- Messaging and communication – Allow for the secure, exchange of messages between colleagues
- Monitor alerts – Time-stamped audit trails, detailing when an alert was sent, delivered and read by responders
- Persistent alerts – Notifications are always acknowledged due to persistent, eight-hour notifications via mobile

Conclusion

The fewer alerts IT teams receive, the happier they will be. This is particularly true if many of the alerts are the result of noise due to (1) the monitoring system or (2) duplicate alerting errors. For effective alerting, teams need more than a robust monitoring tool. They also need a powerful alerting solution that enables them to effectively respond to situations that arise in IT, regardless of their urgency or severity.

About OnPage

OnPage's award-winning incident alert management system for IT professionals provides the industry's only ALERT-UNTIL-READ notification capabilities. Built around the incident resolution lifecycle, OnPage helps teams reduce downtime and costs while improving coordination and performance.

OnPage's escalation, redundancy and scheduling features ensure that a critical message is never missed. Infinitely more reliable and secure than emails, text messages and phone calls, OnPage provides instant visibility and feedback on alerts. As part of IT service management, the solution tracks alert delivery, ticket status and responses, delivering complete audit trail reporting during and after each incident. The OnPage platform includes seamless integration with mission-critical systems, including ServiceNow and other leading platforms, to help deliver optimum service levels and get the most value from IT investments, making sure that sensors, monitoring systems and people have a reliable way to escalate critical alerts to the right person immediately.

IT organizations trust OnPage's incident alert management system to help them reduce downtime, meet SLA commitments and keep teams motivated and performing at a high level.

For more information:

Visit www.onpage.com
Contact sales@onpagecorp.com
Call (781) 916-0040.