ENHANCE ITSM WITH CRITICAL ALERTING

Today's IT professionals strive for corporate and business strategy alignment as well as meeting day-to-day objectives – ticket completion and SLA assurance. They want their teams to be perceived as resources for improving overall business productivity rather than the people that are contacted only when something goes wrong. But most IT executives aren't reaching that goal. In a survey conducted by Atlassian[1] only 29% of teams reported that IT is key to business strategy and success.

By focusing on improving incident management, a key component of IT service management, IT teams can become more productive and spend more time and effort on the strategic aspects of their jobs.

To shed more light on incident management, this whitepaper will focus on four components:

- Roadblocks to effective incident management
- Solutions and best practices
- Including incident alert management solutions in the ITSM stack

Here are four common roadblocks experienced by those working in IT organizations:

ROADBLOCK #1: NOT BEING AS PREPARED AS POSSIBLE FOR UNPLANNED INCIDENTS

Without a documented blueprint in place for the most common incidents, the IT organization will waste time searching for resources and records, figuring out who is responsible for completing each task in the resolution process and determining the right priority for each incident. End users will be frustrated by the lack of communication and resolution delay.

A complete incident management plan incorporates the following critical alerting components:

ALERT SETTING

The beginning of an incident is perhaps the point where the team has the most control. Most systems that are under their care will send off an alarm if something is not right. These notifications are typically in the form of an email. Emails, however, are ineffective because most inboxes bury important alerts. Emails tend to be easily ignored because they don't come with a blaring and audible alarm that draws attention. Any system that sends off an email notification should be integrated with a monitoring tool or an alerting app that can be accessed using any smartphone, anywhere.

SMARTPHONES, NOT PAGERS

Smartphones are a miracle to those who work with random things that go bump in the night. The alternative is the antiquated pager. Pagers are unable to continue alerting until the messages are read. Smartphones, on the other hand, are readily available and can host apps that act like pagers.

While there are a lot of pager apps out there the key is to get one that continues to broadcast the alert until it is read so that a response is ensured. Moreover, if the recipient of the smartphone message is unavailable when the page is originally sent, smartphone applications can ensure that the notification continues until

[1] https://www.atlassian.com/it-unplugged/itsm/new-shape-of-modern-IT-teams

read. This is not the case with pagers which are often missed if the intended recipient is unavailable or out of range.

DOCUMENTATION OF INCIDENT DATA AND POLICIES

Experienced IT professionals can more effectively handle incidents if they have information derived from past experiences. Ticketing solutions that track the progress of the incident and everything that happens to it until it's resolved will provide invaluable data that can be leveraged for future incidents. Incident response policies and procedures should also be clearly documented, along with the personnel responsible for carrying them out. That's a good segue to the second roadblock.

ROADBLOCK #2: NO CLEAR DEFINITION OF ROLES FOR INCIDENT MANAGEMENT

To avoid confusion and time wasting a team needs to be assigned to respond to incidents. The first step is to form a centralized incident response team. Digital Guardian has developed a comprehensive guide for building an IR (Incident Response) team[2] that includes:

INCIDENT RESPONSE MANAGER: The IR manager is the point person for overall management, prioritization and assigning responsibilities for each incident. Ideally, the IR manager would administer incidents with the help of a messaging platform that includes advanced alerting capabilities.

SECURITY ANALYSTS: The IR manager relies on security analysts to investigate and act on potential intrusions and other security threats.

THREAT RESEARCHERS: Threat researchers work with security analysts to help develop an intelligence database that includes external research and security trends.

Ticketing tools allow the ITSM team to catalog all the aspects of the unfolding incident so that it can be used at a later instance to provide insight.

ROADBLOCK #3: NOT HAVING A PLAN B

Not having a Plan B means not having a backup person receiving the alerts when the first person alerted is unavailable. Here are steps to solve this roadblock:

SETTING UP AN ESCALATION POLICY

By putting in place an escalation policy the IR manager can ensure that if an incident is not acknowledged or resolved within a pre-determined amount of time, it will escalate to the appropriate person or people. The policy should identify who should receive the alert, the amount of time to wait before escalating to the next user(s), and which user(s) the alert should go to next.

[2] Digital Guardian, Building Your Incident Response Team: Key Roles and Responsibilities

Those who need to receive alerts are put in one escalation group. The order in which the people are alerted is based on who is assigned as the first responder. The escalation interval (time to escalation) and escalation factor (the factor that stops an escalation i.e. the message being read) should be set according to the escalation policy established by the IR manager.

SETTING UP A FAILOVER

In the event an alert is sent to an escalation group and does not reach anyone in the group, the failover policy notifies either the ITSM team leader and/or higher-level managers so that they can take corrective action. This can be as simple as sending an email with details of the unanswered alerts. In a post-mortem of the incident, this kind of failover reporting will be useful to track what happened with the alert and why it was left acknowledged.

ALERTING ACROSS COMMUNICATION CHANNELS

When alerts are set up it is imperative that alert redundancies are set in place in case the original alert sent through the preferred mode of communication fails to get delivered. Preferably, the system should have the capability to send the same alert to a team member's smartphone via push notifications, SMS and an automated phone call describing the alert or via email.

ROADBLOCK #4: NOT HAVING AN INCIDENT ALERT MANAGEMENT TOOL

ITSM ticketing tools are indispensable for cataloging incidents but won't help the ITSM team manage the incident on its own. Furthermore, with most ticketing tools' workflows, the team are only able to receive a text or email when a ticket is created, hindering the alerting process.

By integrating ticketing tools into an incident alert management solution that converts tickets into smart alerts, responder teams and management can be automatically and instantly contacted at the appropriate time and priority level whenever there is an incident.

The incident alert management tool needs to be more than just an alerting service. This checklist details must-have features of a comprehensive solution:

- Ability to integrate into ticketing tools
- An on-call scheduler
- An alert escalation policy
- Failover options
- Secure messaging to aid ITSM team communication
- High and low priority alerting
- The ability to track incoming and outgoing alerts and messages
- Reporting features to summarize and gain insights into historical data

Integrating incident alert management capabilities to ticketing solutions provides these key benefits:

- Increase in the visibility of alerts
- Filtering out unimportant alerts
- Better communication between teams
- Automation of the alerting process

CONCLUSION

IT service management teams invite trouble when they fail to prep for an incident and act in a coordinated fashion. Both these issues can be resolved using a platform that connects to ticketing tools to automate actions for incoming tickets. Furthermore, by bringing together team communications in one platform and defining clear roles, the incident resolution process becomes clearer and more transparent. Finally, the addition of an incident alert management tool to the ITSM tool stack ensures that the right alerts are taken care of by the right people.

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 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** or contact the company at marketing@onpagecorp.com or at **(781) 916-0040**.