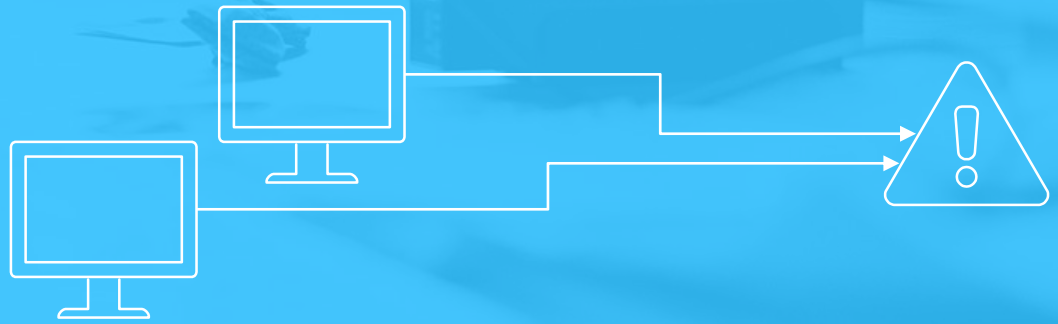

Maximize your IT Team’s Incident Response Speed

# INTRO

The reality of IT teams supporting the uptime of infrastructure is that they cannot avoid downtime incidents.

No matter how responsible managers are in ensuring regular maintenance and repair, incidents will happen.

Servers will fill. Backlogs will occur. APIs will fail. When these incidents do occur, it is important that IT teams are well trained and have the necessary equipment to ensure a rapid incident response.



# INTRO

The challenge though is more than simply creating an appropriate check list for teams to follow. Rather, in the wake of incidents there are often conflicting priorities between restoring availability and investigating the causes of the incident.

For example, Security incident response teams (SIRTs) and infrastructure teams operate with different sets of assumptions and priorities when resolving issues. If these separate priorities are not effectively managed, there can lead to the duplication of work, delays in handoffs and faulty results.

The goal of this e-book is to highlight how an incident response (IR) team can prepare to effectively respond to IT issues in a way that avoids duplication, delay and error.

# 1.
# Establish Teams

## Step 1: Establish teams

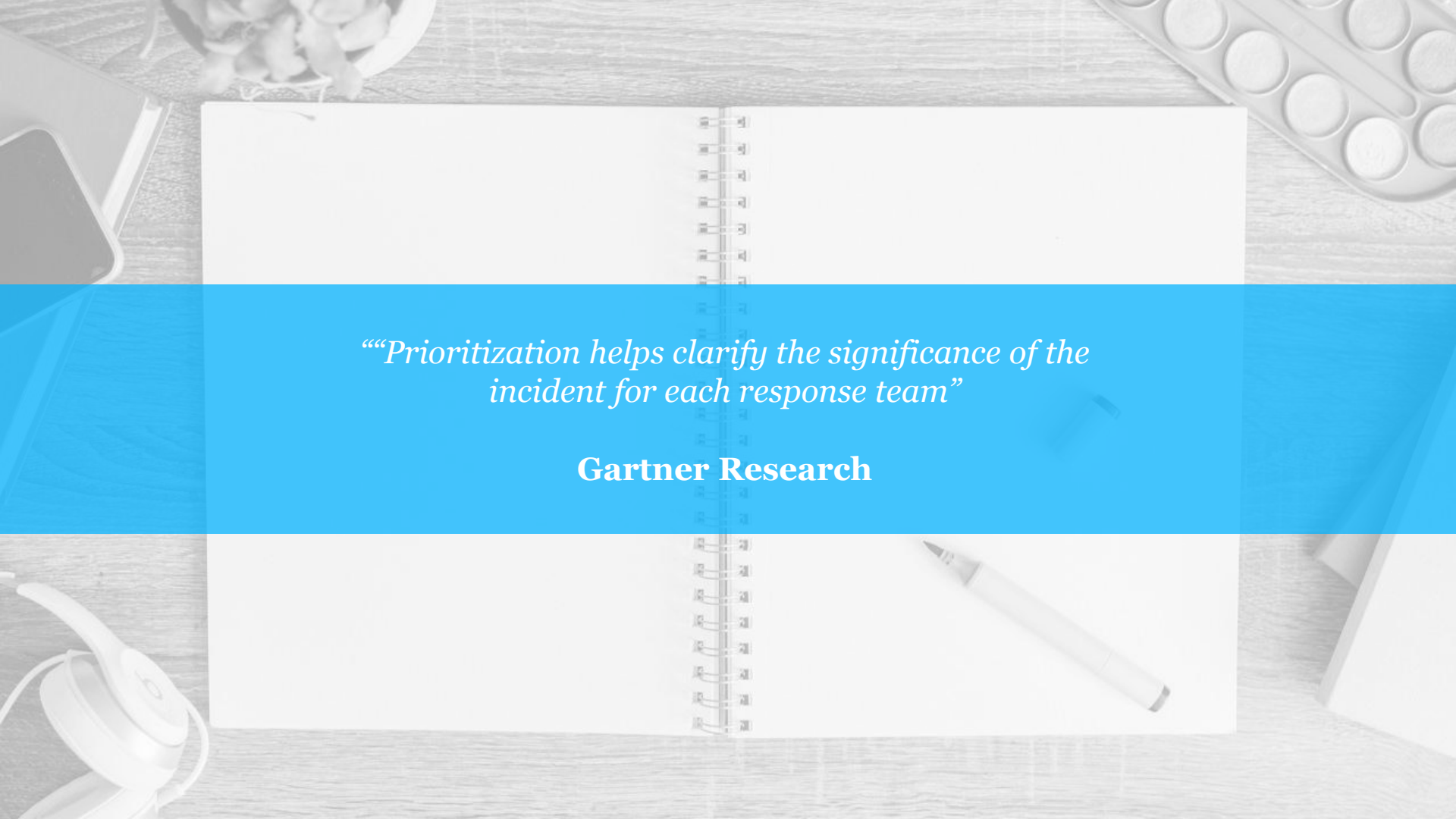
Effective response to incidents does not start when the incident arises. Instead, effective response begins long before there is any knowledge of a problem at all. The first step in effective incident response is establishing teams that include members from the various groups within the company such as security, infrastructure and development.

Some believe that incidents are best handled by those with the most expertise and capability. However, according to Gartner Research, the response is actually best if teams result from a bringing together of security and I&O personnel, working together to collaborate response focuses and the best and most relevant staff, skills and resources to an incident.

Together, these individuals from the various teams need to develop a shared framework for responding to incidents and leverage their individual skills to improve response. The goal is not to create a new entity but rather to allow an organization to draw from strengths.

Leaders of all teams must be able to engage meaningfully with other IT leaders and response team members to arrive at an efficient incident response model.  Harmonized response facilitates collaboration, improves sharing of knowledge and reduces response times to improve operational resiliency.

# 2.
# Priorities, Planning and Preparation



*““Prioritization helps clarify the significance of the incident for each response team”*

**Gartner Research**

## Step 2: Priorities, Planning and Preparation

Each company will have a different understanding of what functionalities are important to the company and to the individual teams. Around these functionalities, teams need to create metrics that determine the level of deviation from normal. When technologies stray from these means by the amount determined by the teams then action is required.

Teams need to establish and agree to a common framework for setting incident response priorities based on business impacts by aligning response priorities to business objectives. Teams also need to determine resources that will be used and which resources can be shared.

By determining metrics, teams will automatically have a sense if this is a high priority issue and what coordination is required from the beginning. Teams should create an analysis of where they are in terms of ability to respond and what is needed in terms of training and technology to achieve the level of preparedness they desire.

A key part of planning and preparation is having teams prepare for potential scenarios and develop a response based on these potential incidents.  Teams should prepare with runbooks and anticipate common scenarios. They should highlight priorities in writing

# 3.
# Monitoring

## Step 3: Monitoring

As noted in the introduction, systems will break or be attacked. There is no way to prevent this outcome from happening. Consequently, it is imperative that incident response teams have ways to monitor technologies and learn of these eventualities as quickly as possible.

There are multiple ways that teams can monitor their technologies. They can monitor through the use of logs or end-user reports. This information should be collected and filtered.  Additionally, teams can learn of incidents through their NOC or SOC.

# 4.
# Alerting

## Step 4: Alerting

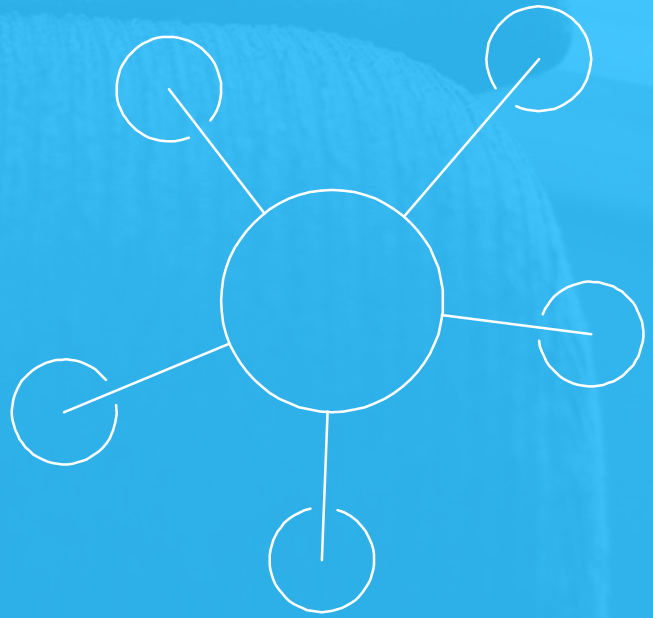
With proper preparation, teams know which incidents are priorities and require rapid resolution. In order to quickly learn about these incidents, teams need incident management platforms. Incident management platforms like those provided by OnPage are ideal in this incidence as they enable teams to quickly learn when technologies have failed and subsequently jump on conference bridges to discuss resolutions.

With proper preparation, alerts can be assigned to the teams who have the responsibility to resolve the issue. While there will be pressure to restore functionality to whichever team shouts the loudest, the pressure should not drive teams away from their focus

# 5. Escalation criterions

## Step 5: Escalation criterions

An important part of effective incident response and alerting is ensuring that there are escalation scenarios for when incidents occur and the designated team is unavailable to respond. If the initial team is unable to respond to the issue, escalations must be in place so the issue does not linger.



# 6. Collaboration and unified communications

## Step 6: Collaboration and unified communications

Teams need to think of response in terms of objectives beyond their individual team goals. As has been stated at other points in this document, teams need to have a sense of shared organizational goals and objectives. To enable teams to reach these objectives, teams need ways to collaborate and communicate during incidents

Strong collaboration platforms that enable communications once alerts are received are best. Ideally, the alerting and communications platforms are unified so that once alerted, teams do not need to switch devices to exchange messages with colleagues. The more robust the communications platform, the better. The ability to exchange voicemails, images and documents are all ideal as the need for these capabilities are often important in quick resolution of incidents.

# 7.
# Post mortems

## Step 7: Post mortems

Once the incident has been resolved, team members might feel that they can breath a sigh of relief that the issue has been resolved. However, once the incident is resolved team members have a unique opportunity to review and document their process. The ultimate goal of putting incident response under review is improvement of the process.

Post-incident analysis is an integral part of the process and can uncover knowledge that should have been available but was not known or was delayed and resulted in harm to a system. Without a post-mortem, improvement will be very difficult to achieve.

Reporting should also look at which systems were affected, and the number of users impacted as well as which notifications were issued. The resulting incident report should be reviewed by participants as well as key stakeholders. This process is where leaders engage the response team to help codify organizational lessons learned.

From this analysis, teams can also learn root causes of incidents and what might need to happen in the future to prevent incidents from occurring. The process will Also highlight faulty processes or knowledge that needs to be available next time.

# Conclusion

IT teams need to think of incident response as a process. If thought of as just one step then incident response will either not be as effective as it could be or will fail. Communication is the key underlying theme required for effective incident response. Incident management platforms like OnPage provide engineers in IT with the tools they need to organize their group, communicate between teams during incidents and report on incidents at the end.

To learn more about what OnPage can do for your IT team, give us a call

# Thanks!

CALL US!
Phone +1 (781) 916-0040
Or schedule a demo!