Critical Incident Management

ONPAGE

Table of contents

What’s Critical Incident Management

Critical incident management defines the alignment of company operations, services, and functions to manage high-priority assets and situations. Coordinated response between multiple teams requires critical incident management.

Critical incident management differs from regular incident management based on the severity of the incident.

Incident Severity

There are multiple severities that can describe an incident. Usually, IT teams will use “SEV” abbreviations. Severities can range from a severity five (SEV-5), which is a low-priority incident, to a severity one (SEV-1) incident which is high-priority event. Anything above a SEV-3 is considered a “major event” and becomes a critical incident requiring critical incident management.

Incident Severity Definitions

1

Incident Severity 1 (SEV-1):
Critical production issue that severely impacts use of the service. This type of situation has no workarounds. Severity one issues require a dedicated resource to work on the issue.

Action:

- High-priority alerts are sent to service team
- Multiple technicians are required to remedy the situation
- Use high-priority messages when exchanging information with colleagues
- Notify internal stakeholders

2

Incident Severity 2 (SEV-2):
Critical situations where functionality is impacted, or customer experience is seriously degraded. High impact to portions of the business and no reasonable workaround exists.

Action:

- High-priority alerts are sent to service team
- Multiple technicians are required to remedy the situation
- Use high-priority messages when exchanging information with colleagues

Incident Severity Definitions

3

Incident Severity 3 (SEV-3):
A partial loss of service with a medium-to-low impact on the business. Business is still able to function. Short-term workaround is available, but not scalable. Issue could escalate to SEV-2 if not managed properly.

Action:
- High-priority alerts are sent to service team
- Usually requires one engineer to work on issue although it is her top priority
- Continue to monitor situation in case it needs escalation

4

Incident Severity 4 (SEV-4):
Performance of systems is delayed but still functioning. Bug affects a small number of users. Acceptable workaround available.

Action:
- Low-priority alerts are sent to service team
- Engineer works on the issue as their top priority
- Monitors situation to ensure it doesn’t escalate

Incident Severity Definitions

5

Incident Severity 5 (SEV-5):
Systems experience minor issues that affect a small, limited number of users. SEV-5 issues are classified as low-priority events. They do not require immediate attention and resolution.

Action:

- Low-priority alerts are sent to service team
- Engineer works on the issue when possible
- Occasionally monitors situation to ensure it doesn’t escalate

Incident Severity Examples

Incident Severity 1 (SEV-1) – Internet service is down which prevents the application from running.

Incident Severity 2 (SEV-2) – Server is down preventing storage of new files or records.

Incident Severity 3 (SEV-3) – Part of a solution's functionality is unavailable.

Incident Severity 4 (SEV-4) – Website is slow in responding to requests.

Incident Severity 5 (SEV-5) – Users do not remember login credentials.

Managing Critical Incidents

Establish Workflows:

Establish a workflow for how incidents are handled by the IT operations team. Create a ticket and use the persistent alerting feature of the team's incident management platform.

Share Information:

Incidents are best managed by maintaining a constant flow of information. Engineers exchange text messages so that they can provide runbooks and advice to colleagues.

Analyze Incident:

After SEV-3, SEV-2, or SEV-1, teams should conduct a post-incident analysis as the final step of the critical incident management process.

Managing Critical Incidents with OnPage

OnPage ensures critical alerts are received by the right engineer securely with real-time incident management and priority alerting!

OnPage cuts through alert noise and prioritizes the most crucial alerts. The system triggers unique mobile alert tones for high and low-priority issues.

OnPage’s high-priority, persistent alerts ensure engineers manage high-severity incidents promptly. SEV-3, SEV-2, and SEV-1 issues will never go unnoticed.

OnPage Features

Bypass silent switch on all devices. Alerts cut through the noise and bring critical alerts to the forefront.

Schedule the on-call team as a group or as individuals, eliminating manual errors.

Escalate critical alerts to the next group or person if an engineer is not available.

Messages are SSL encrypted and can only be viewed by message participants.

Analyze incident response time with real-time reporting. Recognize incident trends.

Attach contextual media files to a high-priority alert. Provide more context into an incident.

About OnPage

OnPage's award-winning incident alert management system for IT, MSP and healthcare professionals provides the industry's only ALERT-UNTIL-READ notification capabilities, ensuring that critical messages are never missed. OnPage enables organizations to get the most out of their digital investments, so that sensors, monitoring systems, and people have a reliable way to escalate urgent communications to the right person immediately.

OnPage's escalation, redundancy, and scheduling features make the system infinitely more reliable and secure than emails, text messages and phone calls. OnPage shrinks resolution time by automating the notification process, reducing human errors and prioritizing critical messages to ensure fast response times.

Whether to minimize IT infrastructure downtime, or to reduce the response time of healthcare providers in life-and-death situations, organizations trust OnPage for all their secure, HIPAA-compliant, critical notification needs.

Contact Us For more information, visit www.onpage.com or contact the company at sales@onpagecorp.com or at (781) 916-0040